EC-COUNCIL.212-89.v2025-07-10.q180

Exam Code:	212-89
Exam Name:	EC Council Certified Incident Handler (ECIH v3)
Certification Provider:	EC-COUNCIL
Free Question Number:	180
Version:	v2025-07-10
# of views:	156
# of Questions views:	1800
https://www.exam-tests.com/212-89-exam/EC-COUNCIL.212-89.v2025-07-10.q180.html	

NEW QUESTION: 1
Raven is a part of an IH&R team and was info med by her manager to handle and lead the removal of the root cause for an incident and to close all attack vectors to prevent similar incidents in the future. Raven notifies the service providers and developers of affected resources.
Which of the following steps of the incident handling and response process does Raven need to implement to remove the root cause of the incident?
A. Evidence gathering and forensic analysis
B. Incident triage
C. Containment
D. Eradication
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which stage of the incident response and handling process involves auditing the system and network log files?
A. Containment
B. Incident triage
C. Incident disclosure
D. Incident eradication
Answer: (SHOW ANSWER)
Auditing the system and network log files is a crucial step in the incident triage phase of the incident response and handling process. During incident triage, incident handlers assess and prioritize incidents based on their severity, impact, and the urgency of the response required. Part of this assessment involves reviewing log files to understand the nature of the incident, its scope, and the systems or networks affected. This information helps in categorizing the incident and deciding on the appropriate response actions. Unlike

containment, which aims to limit the damage, incident disclosure, which involves communicating about the incident, or incident eradication, which focuses on removing the threat, incident triage is about evaluating and prioritizing the incident based on detailed log analysis among other factors.References:The Incident Handler (ECIH v3) courses and study guides emphasize the role of incident triage in the early stages of the incident response process, highlighting the importance of log file analysis in assessing and prioritizing incidents.

NEW QUESTION: 3
Which of the following terms refers to the personnel that the incident handling and response (IH&R) team must contact to report the incident and obtain the necessary permissions?
A. Civil litigation
B. Ticketing
C. Criminal referral
D. Point of contact
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Jason is setting up a computer forensics lab and must perform the following steps: 1. physical location and structural design considerations; 2. planning and budgeting; 3. work area considerations; 4. physical security recommendations; 5. forensic lab licensing; 6. human resource considerations. Arrange these steps in the order of execution.
A. 2 -> 1 -> 3 -> 6 -> 4 -> 5
B. 2->3->l ->4->6->5
C. 5-> 2-> l-> 3-> 4-> 6
D. 3 .> 2 -> 1 -> 4-> 6-> 5
Answer: (SHOW ANSWER)
Setting up a computer forensics lab involves several critical steps that need to be executed in a logical and efficient order. The correct sequence starts with planning and budgeting(2), as it is essential to understand the scope, resources, and financial commitment required for the lab. The next step involves considering the physical location and structural design (1) to ensure the lab meets operational needs and security requirements.
Work area considerations (3) follow, focusing on the layout and functionality of the workspace. Human resource considerations (6) are crucial next, to ensure the lab is staffed with qualified personnel. Physical security recommendations (4) are then implemented to protect the lab and its resources. Finally, forensic lab licensing (5) ensures the lab operates within legal and regulatory frameworks.
References:The ECIH v3 course materials from EC-Council outline the foundational steps for setting up a computer forensics lab, stressing the importance of thorough planning and adherence to best practices in lab design and operation.

NEW QUESTION: 5
Which of the following is not called volatile data?
A. Open sockets er open ports
B. The dale a no Lime of the system
C. Creation dates of files
D. State of the network interface
Answer: (SHOW ANSWER)
Volatile data refers to information that is stored temporarily and is lost when a computer is turned off or restarted, such as RAM contents, including open sockets and open ports, the date and time of the system, and the state of the network interface. The creation dates of files, however, are considered non-volatile data because they are preserved on the hard drive and remain available after the system is restarted or turned off.
Non-volatile data is stored on persistent storage mediums like hard drives, SSDs, and magnetic tapes, where it remains until it is deleted or overwritten.References:The Incident Handler (ECIH v3) certification emphasizes the distinction between volatile and non-volatile data in the context of digital forensics and incident response, highlighting the importance of understanding what data may be lost upon system shutdown and what data persists.

NEW QUESTION: 6
In which of the following confidentiality attacks attackers try to lure users by posing themselves as authorized AP by beaconing the WLAN's SSID?
A. Masqueradin
B. Session hijacking
C. Honeypot AP
D. Evil twin AP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
Removing or eliminating the root cause of the incident is called:
A. Incident Protection
B. Incident Classification
C. Incident Containment
D. Incident Eradication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
Bit stream image copy of the digital evidence must be performed in order to:
A. Copy all disk sectors including slack space
B. Copy the FAT table

C. All the above
D. Prevent alteration to the original disk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
Which of the following techniques helps incident handlers to detect man-in-the-middle attack by finding the new APs and trying to connect an already established channel, even if the spoofed AP consists similar IP and MAC addresses as of the original AP?
A. Access point monitoring
B. General wireless traffic monitoring
C. Wireless client monitoring
D. Network traffic monitoring
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
SWA Cloud Services added PKI as one of their cloud security controls. What does PKI stand for?
A. Public key information
B. Private key infrastructure
C. Public key infrastructure
D. Private key in for ma lion
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
During the vulnerability assessment phase, the incident responders perform various steps as below:
1. Run vulnerability scans using tools
2. Identify and prioritize vulnerabilities
3. Examine and evaluate physical security
4. Perform OSINT information gathering to validate the vulnerabilities
5. Apply business and technology context to scanner results
6. Check for misconfigurations and human errors
7. Create a vulnerability scan report
Identify the correct sequence of vulnerability assessment steps performed by the incident responders.
A. 4-->1-->2->3->6->5-->7
B. 3-->6-->1->2->5->4-->7
C. 1-->3-->2->4->5->6-->7
D. 2-->1-->4->7->5->6-->3
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
According to the Evidence Preservation policy, a forensic investigator should make at least ..... image copies of the digital evidence.
A. Two image copies
B. Three image copies
C. Four image copies
D. One image copy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
Michael is an incident handler at CyberTech Solutions. He is performing detection and analysis of a cloud security incident. He is analyzing the file systems, slack spaces, and metadata of the storage units to find hidden malware and evidence of malice.
Identify the cloud security incident handled by Michael.
A. Server-related incident
B. Storage-related incident
C. Application-related incident
D. Network-related incident
Answer: (SHOW ANSWER)

NEW QUESTION: 14
An organization named Sam Morison Inc. decided to use cloud-based services to reduce the cost of maintenance. The organization identified various risks and threats associated with cloud service adoption and migrating business-critical data to thirdparty systems. Hence, the organization decided to deploy cloud-based security tools to prevent upcoming threats.
Which of the following tools help the organization to secure the cloud resources and services?
A. Nmap
B. Alert Logic
C. Burp Suite
D. Wireshark
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
In a qualitative risk analysis, risk is calculated in terms of:
A. Probability of Loss X Loss
B. (Attack Success + Criticality) -(Countermeasures)
C. Asset criticality assessment - (Risks and Associated Risk Levels)
D. (Countermeasures + Magnitude of Impact) - (Reports from prior risk assessments)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues.
Which of the following documents helps in protecting evidence from physical or logical damage:
A. Network and host log records
B. Chain-of-Custody
C. Forensic analysis report
D. Chain-of-Precedence
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Which of the following is a technique used by attackers to make a message difficult to understand through the use of ambiguous language?
A. Steganography
B. Spoofing
C. Encryption
D. Obfuscation
Answer: D (LEAVE A REPLY)
Obfuscation is a technique used to make data or code difficult to understand. It is often employed by attackers to conceal the true intent of their code or communications, making it harder for security professionals, automated tools, and others to analyze or detect malicious activity. Obfuscation can involve the use of ambiguous or misleading language, as well as more technical methods such as encoding, encryption, or the use of nonsensical variable names in source code to hide its true functionality.
References:The ECIH v3 program discusses various techniques attackers use to evade detection, including obfuscation, highlighting how it complicates the analysis and understanding of malicious payloads.

NEW QUESTION: 18

The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could
be:
A. System files become inaccessible
B. All the above
C. Increase in the number of e-mails sent and received
D. Antivirus software detects the infected files
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
John is performing a memory dump analysis in order to find traces of malware. He has employed Volatility tool in order to achieve his objective.
Which of the following volatility framework command she will use in order to analyze the running process from the memory dump?
A. python vol.py pslist-profile=Win2008SP1x86 -f/root/Desktop/memdump.mem
B. python vol.py hivelist-prof le=Win2008SP1x86 -f/root Desktop/memdump.mem
C. python vol.py svcscan--profile=Win2008SP1x86 -f/root/Desktop/memdump.mem | more
D. python vol.py imageinfo -f/root/Desktop/memdump.mem
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Sam, an employee of a multinational company, sends emails to third-party organizations with a spoofed email address of his organization.
How can you categorize this type of incident?
A. Denial-of-service incident
B. Unauthorized access incident
C. Network intrusion incident
D. Inappropriate usage incident
Answer: (SHOW ANSWER)

NEW QUESTION: 21
A user downloaded what appears to be genuine software. Unknown to her, when she installed the application, it executed code that provided an unauthorized remote attacker access to her computer.
What type of malicious threat displays this characteristic?
A. Backdoor
B. Spyware
C. Trojan
D. Virus
Answer: (SHOW ANSWER)

NEW QUESTION: 22
The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:
A. Incident Response
B. Incident Handling
C. Incident Management
D. Incident Recovery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Which of the following terms refers to vulnerable account management functions, including account update, recovery of forgotten or lost passwords, and password reset, that might weaken valid authentication schemes?
A. SQL injection
B. Broken account management
C. Directory traversal
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
The term "broken account management" refers to vulnerabilities in the account management functions of web applications, which can weaken valid authentication schemes. This can include issues with how accounts are created, updated, managed, and deleted, as well as how users recover forgotten passwords or perform password resets. Poorly implemented account management functions can allow attackers to bypass authentication, elevate privileges, or assume the identity of another user. This weakness is a significant security concern because it directly impacts the ability of a system to safeguard user data and maintain operational integrity.
References:In its training materials, the ECIH v3 program addresses various web application vulnerabilities, including broken account management, emphasizing the importance of secure development practices and regular security assessments to prevent such issues.

NEW QUESTION: 24
They type of attack that prevents the authorized users to access networks, systems, or applications by
exhausting the network resources and sending illegal requests to an application is known as:
A. Denial of Service attack
B. Man in the Middle attack
C. SQL injection attack
D. Session Hijacking attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:
A. Handlers
B. Zombies
C. Honey Pots
D. Relays
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
In which of the following phases of incident handling and response (IH&R) process the identified security incidents are analyzed, validated, categorized, and prioritized?
A. Containment
B. Incident triage
C. Notification
D. Incident recording and assignment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
Network Ned is the security administrator for a company. He is going to place the company's new web server into production.
Into which of the following zones should he place the server to best protect the company's network?
A. Sandbox
B. Intranet
C. Honeypot
D. DMZ
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
A colleague wants to minimize their security responsibility because they are in a small organization. They are evaluating a new application that is offered in different forms. Which form would result in the least amount of responsibility for the colleague?
A. laaS
B. PaaS
C. saaS
D. On-prom installation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

The process of rebuilding and restoring the computer systems affected by an incident to normal operational
stage including all the processes, policies and tools is known as:
A. Incident Management
B. Incident Response
C. Incident Recovery
D. Incident Handling
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 30
During the vulnerability assessment phase, the incident responders perform various steps as below:
1. Run vulnerability scans using tools
2. Identify and prioritize vulnerabilities
3. Examine and evaluate physical security
4. Perform OSINT information gathering to validate the vulnerabilities
5. Apply business and technology context to scanner results
6. Check for misconfigurations and human errors
7. Create a vulnerability scan report
Identify the correct sequence of vulnerability assessment steps performed by the incident responders.
A. 4-->1-->2-->3-->6-->5-->7
B. 2-->1-->4-->7-->5-->6-->3
C. 1-->3-->2-->4-->5-->6-->7
D. 3-->6-->1-->2-->5-->4-->7
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
An organization implemented an encoding technique to eradicate SQL injection attacks. In this technique, if a user submits a request using single-quote and some values, then the encoding technique will convert it into numeric digits and letters ranging from a to f. This prevents the user request from performing SQL injection attempt on the web application. Identify the encoding technique used by the organization.
A. URL encoding
B. Hex encoding
C. Base64 encoding
D. Unicode encoding
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Bran is an incident handler who is assessing the network of the organization. In the process, he wants to detect ping sweep attempts on the network using Wireshark tool.
Which of the following Wireshark filter he must use to accomplish this task?
A. icmp.seq
B. icmp.redir_gw
C. icmp.type==8
D. icmp.ident
Answer: C (LEAVE A REPLY)
In Wireshark, the filtericmp.type==8is used to detect ping sweep attempts. ICMP type 8 messages are echo requests, which are used in ping operations to check the availability of a network device. A ping sweep involves sending ICMP echo requests to multiple addresses to discover active devices on a network. By filtering for ICMP type 8 messages in Wireshark, Bran can identify these echo requests, helping to pinpoint ping sweep activities on the network.
References:Wireshark, as a network protocol analyzer, is frequently discussed in the ECIH v3 program, with particular emphasis on its utility in detecting network reconnaissance activities like ping sweeps through specific filter usage.

NEW QUESTION: 33
Patrick is doing a cyber forensic investigation. He is in the process of collecting physical evidence at the crime scene.
Which of the following elements he must consider while collecting physical evidence?
A. Open ports, services, and operating system (OS) vulnerabilities
B. DNS information including domain and subdomains
C. Published name servers and web application source code
D. Removable media, cable, and publications
Answer: D (LEAVE A REPLY)
In the context of collecting physical evidence during a cyber forensic investigation, Patrick must consider items like removable media, cables, and publications. These items can contain crucial information related to the crime, such as data storage devices (USB drives, external hard drives), cables connected to potentially relevant devices, and any printed materials that might have information or clues about the incident. Open ports, services,

and OS vulnerabilities, DNS information, and published name servers and web application source code, while important in digital forensics, do not constitute physical evidence in the traditional sense.References:Incident Handler (ECIH v3) study guides and courses detail the process of evidence collection in cyber forensic investigations, emphasizing the importance of securing physical evidence that could support digital forensic analysis.

NEW QUESTION: 34
James is a professional hacker and is employed by an organization to exploit their cloud services. In order to achieve this, James created anonymous access to the cloud services to carry out various attacks such as password and key cracking, hosting malicious data, and DDoS attacks. Which of the following threats is he posing to the cloud platform?
A. Insufficient duo diligence
B. Abuse end nefarious use of cloud services
C. Data breach/loss
D. Insecure interface and APIs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 35
According to NITS, what are the 5 main actors in cloud computing?
A. Provider, carrier, auditor, broker, and seller
B. Buyer, consumer, carrier, auditor, and broker
C. None of these
D. Consumer, provider, carrier, auditor, ano broker
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and removed the malware completely. Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident.
Which of the following stages in IH&R process is James working on?
A. Notification
B. Evidence gathering and forensics analysis
C. Post-incident activities
D. Eradication
Answer: C (LEAVE A REPLY)
James is working on the post-incident activities stage of the Incident Handling and Response (IH&R) process.

After containing the spread of the infection and removing the malware, the focus shifts to assessing the impact of the incident on the organization and preparing a detailed report. This phase involves analyzing the extent of the damage, determining the cost of the attack, evaluating how well the incident was managed, and identifying lessons learned to improve future response efforts. The objective is to restore systems to normal operation, ensure no remnants of the threat remain, and implement measures to prevent recurrence.References:Incident Handler (ECIH v3) courses and study guides outline the IH&R process, emphasizing the importance of post-incident activities for organizational recovery and improvement of future security measures.

NEW QUESTION: 37
You are a systems administrator for a company. You are accessing your file server remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either. You can ping the file serverbut not connect to it via RDP. You check the Active Directory Server, and all is well. You check the email server and find that emails are sent and received normally. What is the most likely issue?
A. An e-mail service issue
B. The file server has shut down
C. A denial-of-service issue
D. An admin account issue
Answer: C (LEAVE A REPLY)
In this scenario, the inability to access the file server via Remote Desktop Protocol (RDP), despite the server being pingable and other services functioning normally, suggests a service-specific disruption rather than a complete system shutdown or broader network issue. This pattern is indicative of a denial-of-service (DoS) attack targeted at the file server's RDP service or network congestion that specifically affects RDP connectivity. A DoS attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. The fact that other services (like email) are operational rules out broader system or admin account issues, pointing towards a specific problem with accessing the file server, most likely due to a denial-of-service condition.References:Incident Handler (ECIH v3) courses teach systems administrators and security professionals to diagnose and respond to various security incidents, including DoS attacks, by understanding symptoms and isolating issues based on the services affected.

NEW QUESTION: 38
Which of the following is defined as the identification of the boundaries of an IT system along with the resources and information that constitute the system?
A. System characterization

B. Threat ioenLificalion
C. Vulnerability identification
D. Control analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
BadGuy Bob hid files in the slack space, changed the file headers, hid suspicious files in executables, and changed the metadata for all types of files on his hacker laptop. What has he committed?
A. Anti-forensics
B. Adversarial mechanics
C. Felony
D. Legal hostility
Answer: A (LEAVE A REPLY)
Anti-forensics refers to techniques used to hinder the forensic analysis of a computer system. By hiding files in slack space, changing file headers, embedding suspicious files in executables, and altering metadata, BadGuy Bob is attempting to make it difficult for forensic analysts to find, analyze, and attribute the malicious activities and data on his laptop. These actions are designed to conceal evidence, manipulate digital artifacts, and obstruct investigations, making them clear examples of anti-forensic techniques. While such actions could be part of broader criminal activities, constituting a felony, and could be seen as adversarial mechanics or legal hostility in specific contexts, the most accurate classification of these techniques is anti-forensics.References:The ECIH v3 certification program includes discussions on forensic analysis and the challenges posed by anti-forensic techniques, teaching incident handlers how to recognize and counteract attempts to obstruct investigations.

NEW QUESTION: 40
Francis received a spoof email asking for his bank information. He decided to use a tool to analyze the email headers. Which of the following should he use?
A. EventLog Analyzer
B. MxToolbox
C. Email Checker
D. PoliteMail
Answer: (SHOW ANSWER)
MxToolbox is a comprehensive tool designed for analyzing email headers and diagnosing various email delivery issues. When Francis received a spoofed email asking for his bank information, using MxToolbox to analyze the email headers would be appropriate. This tool helps in examining the source of the email, tracking the email's path across the internet from the sender to the receiver, and identifying any signs of email spoofing or malicious activity. It provides detailed information about the email servers encountered along the way

and can help in verifying the authenticity of the email sender. Other options like EventLog Analyzer, Email Checker, and PoliteMail are tools used for different purposes such as analyzing system event logs, checking email address validity, and managing email communications, respectively, and do not specifically focus on analyzing email headers to the extent required for investigating a spoofed email incident.References:The use of MxToolbox in incident handling and email security analysis is commonly recommended in Incident Handler (ECIH v3) study materials as a practical tool for email header analysis and spoofing investigation.

NEW QUESTION: 41
If the browser does not expire the session when the user fails to logout properly, which of the following OWASP Top 10 web vulnerabilities is caused?
A. A7: Cross-site scripting
B. A3: Sensitive- data exposure
C. A2: Broken authentication
D. A5: Broken access control
Answer: (SHOW ANSWER)
When a browser does not expire a session after the user fails to logout properly, it is indicative of a vulnerability related to broken authentication. Broken authentication is a security issue where attackers can exploit flaws in the authentication mechanism to impersonate other users or take over their sessions. Failure to properly manage session lifetimes, such as not expiring sessions on logout, can allow an attacker to reuse old sessions or session IDs, potentially gaining unauthorized access to user accounts. This vulnerability is classified under A2: Broken Authentication in the OWASP Top 10, which lists the most critical web application security risks. The OWASP Top 10 serves as a guideline for developers and web application providers to understand and mitigate common security risks.References:The OWASP Top 10 is a widely recognized standard for web application security, often referenced in cybersecurity training and certifications, including the EC-Council's Incident Handler (ECIH v3) curriculum, which covers identification and mitigation of various web application vulnerabilities, including broken authentication.

NEW QUESTION: 42
Which of the following risk management processes identifies the risks, estimates the impact, and determines sources to recommend proper mitigation measures?
A. Risk assessment
B. Risk assumption
C. Risk mitigation
D. Risk avoidance
Answer: (SHOW ANSWER)

Risk assessment is the risk management process that involves identifying risks, estimating their impact on the organization, and determining the sources of those risks to recommend appropriate mitigation measures. The goal of a risk assessment is to understand the nature of potential threats, vulnerabilities, and the consequences of those risks materializing, allowing an organization to make informed decisions about how to address them effectively. Risk assumption involves accepting the potential impact of a risk, risk mitigation focuses on reducing the likelihood or impact of risks, and risk avoidance involves taking actions to avoid the risk entirely.References:The ECIH v3 course materials include discussions on risk management processes, outlining the importance of risk assessment in identifying and preparing for potential security threats.

NEW QUESTION: 43
Which of the following does NOT reduce the success rate of SQL injection?
A. Close unnecessary application services and ports on the server.
B. Limit the length of the input field.
C. Constrain legitimate characters to exclude special characters.
D. Automatically lock a user account after a predefined number of invalid login attempts within a predefined interval.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following is NOT part of the static data collection process?
A. Evidence acquisition
B. Evidence oxa mi nation
C. Password protection
D. System preservation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
Investigator Ian gives you a drive image to investigate. What type of analysis are you performing?
A. Real-time
B. Static
C. Dynamic
D. Live
Answer: B (LEAVE A REPLY)

NEW QUESTION: 46
US-CERT and Federal civilian agencies use the reporting timeframe criteria in the federal agency reporting

categorization. What is the timeframe required to report an incident under the CAT 4 Federal Agency category?
A. Within four (4) hours of discovery/detection if the successful attack is still ongoing and agency is unable to
successfully mitigate activity
B. Within two (2) hours of discovery/detection
C. Monthly
D. Weekly
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
In which of the following phases of incident handling and response (IH&R) process are the identified security incidents analyzed, validated, categorized, and prioritized?
A. Incident recording and assignment
B. Containment
C. Incident triage
D. Notification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following techniques against insider threats identifies events that are related to suspicious activity?
A. Correlation
B. Pattern discovery
C. Anomaly detection
D. Normalization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
The correct sequence of Incident Response and Handling is:
A. Incident Identification, recording, initial response, containment and communication
B. Incident Identification, recording, initial response, communication and containment

C. Incident Identification, initial response, communication, recording and containment
D. Incident Identification, communication, recording, initial response and containment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 50
John, a professional hacker, is attacking an organization, and is trying to destroy the connectivity between an AP and client to make the target unavailable to other wireless devices.
Which of the following attacks is John performing in this case?
A. Denial-of-service
B. Routing attack
C. Disassociation attack
D. EAP failure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
Clark, a professional hacker, exploited the web application of a target organization by tampering the form and parameter values. He successfully exploited the web application and gained access to the information assets of the organization.
Identify the vulnerability in the web application exploited by the attacker.
A. SQL injection
B. Broken access control
C. Sensitive data exposure
D. Security misconfiguration
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
SWA Cloud Services added PKI as one of their cloud security controls. What does PKI stand for?
A. Private key infrastructure
B. Private key in for ma lion
C. Public key information
D. Public key infrastructure
Answer: D (LEAVE A REPLY)
Public Key Infrastructure (PKI) is a framework used to manage digital certificates and public-key encryption.
It enables secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email. PKI is fundamental to the management of encryption keys and digital certificates, ensuring the secure exchange of data over networks and verification of identity.

References:The ECIH v3 program covers the importance of PKI in cloud security controls, emphasizing its role in establishing and maintaining a secure cloud computing environment.

NEW QUESTION: 53
Joseph is an incident handling and response (IH&R) team lead in Toro Network Solutions Company. As a part of IH&R process, Joseph alerted the service providers, developers, and manufacturers about the affected resources.
Identify the stage of IH&R process Joseph is currently in.
A. Containment
B. Recovery
C. Eradication
D. Incident triage
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
A computer Risk Policy is a set of ideas to be implemented to overcome the risk associated with computer security incidents. Identify the procedure that is NOT part of the computer risk policy?
A. Procedure for the ongoing training of employees authorized to access the system
B. Procedure to identify security funds to hedge risk
C. Procedure to monitor the efficiency of security controls
D. Provisions for continuing support if there is an interruption in the system or if the system crashes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
Eve is an incident handler in ABC organization. One day, she got a complaint about an email hacking incident from one of the employees of the organization. As a part of incident handling and response process, she must follow a number of recovery steps in order to recover from the incident impact and maintain business continuity.
What is the first step that she must do to secure the employee's account?
A. Restore the email services and change the password
B. Disabling automatic filesharing between the systems
C. Enable two-factor authentication
D. Enable scanning of links and attachments in all the emails
Answer: (SHOW ANSWER)

NEW QUESTION: 56
Otis is an incident handler working in an organization called Delmont. Recently, the organization faced several setbacks in business, whereby its revenues are decreasing.

Otis was asked to take charge and look into the matter. While auditing the enterprise security, he found traces of an attack through which proprietary information was stolen from the enterprise network and passed onto their competitors. Which of the following information security incidents did Delmont face?

A. Email-based abuse

B. Espionage

C. Network and resource abuses

D. Unauthorized access

Answer: B (LEAVE A REPLY)

NEW QUESTION: 57

An attacker traced out and found the kind of websites a target company/individual is frequently surfing and tested those particular websites to identify any possible vulnerabilities. When the attacker detected vulnerabilities in the website, the attacker started injecting malicious script/code into the web application that can redirect the webpage and download the malware onto the victim's machine. After infecting the vulnerable web application, the attacker waited for the victim to access the infected web application.

Identify the type of attack performed by the attacker.

A. Watering hole

B. Obfuscation application

C. Directory traversal

D. Cookie/Session poisoning

Answer: A (LEAVE A REPLY)

The described attack is a "Watering hole" attack. This type of attack targets specific groups of users by infecting websites they are known to frequently visit. The attacker first identifies websites that are popular with the target group, then finds vulnerabilities in those websites to inject malicious code. When the victims visit the compromised site, the code redirects them to other sites or automatically downloads malware onto their machines. This attack leverages the trust users have in regularly visited sites to distribute malware.

Unlike obfuscation application, directory traversal, or cookie/session poisoning attacks, watering hole attacks specifically aim to compromise a commonly used and trusted website to target its users.References:The ECIH v3 certification materials discuss various cyber attack strategies, including watering hole attacks, and provide insights into how attackers exploit trusted relationships between websites and their users.

NEW QUESTION: 58

XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and

removed the malware completely. Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident.
Which of the following stages in IH&R process is James working on?
A. Notification
B. Evidence gathering and forensics analysis
C. Post-incident activities
D. Eradication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Which of the following email security tools can be used by an incident handler to prevent the organization against evolving email threats?
A. Mx Toolbox
B. Email Header Analyzer
C. G Suite Toolbox
D. Gpg4win
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
You are a systems administrator for a company. You are accessing your file server remotely for maintenance. Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either. You can ping the file server but not connect to it via RDP. You check the Active Directory Server, and all is well. You check the email server and find that emails are sent and received normally. What is the most likely issue?
A. The file server has shut down
B. An admin account issue
C. An e-mail service issue
D. A denial-of-service issue
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
As an IT security officer, what is the first step you will take after discovering a successful email compromise?
A. Test the infected system to ensure security
B. Report the incident to the organization's computer incident response team.
C. Investigate similar hosts to determine whether the attacker has compromised other systems.
D. Isolate the compromised system or take steps to contain the attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Which of the following is an appropriate flow of the incident recovery steps?
A. System Validation-System Operation-System Restoration-System Monitoring
B. System Restoration-System Monitoring-System Validation-System Operations
C. System Operation-System Restoration-System Validation-System Monitoring
D. System Restoration-System Validation-System Operations-System Monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Identify the malicious program that is masked as a genuine harmless program and gives the attacker unrestricted access to the user's information and system. These programs may unleash dangerous programs that may erase the unsuspecting user's disk and send the victim's credit card numbers and passwords to a stranger.
A. Worm
B. Adware
C. Virus
D. Trojan
Answer: D (LEAVE A REPLY)
A Trojan, or Trojan horse, is a type of malware that disguises itself as a legitimate, harmless program or file to trick users into downloading and installing it. Once activated, a Trojan can perform a range of malicious activities, including giving attackers unauthorized access to the infected system. This can lead to the theft of sensitive information, such as credit card numbers and passwords, and can also allow the attacker to install additional malware, potentially leading to further damage, such as the erasure of data. Unlike viruses and worms, Trojans do not replicate themselves but rely on the deception of users to spread.
References:The Incident Handler (ECIH v3) course materials cover various types of malware, including Trojans, and their characteristics. The curriculum emphasizes the importance of understanding how different types of malicious software operate to effectively manage and respond to security incidents involving such threats.

NEW QUESTION: 64
Francis received a spoof email asking for his bank information. He decided to use a tool to analyze the email headers.
Which of the following should he use?
A. Polite Mail
B. Email Checker
C. EventLog Analyzer
D. Mx Toolbox
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
John is a professional hacker who is performing an attack on the target organization where he tries to redirect the connection between the IP address and its target server such that when the users type in the Internet address, it redirects them to a rogue website that resembles the original website. He tries this attack using cache poisoning technique.
Identify the type of attack John is performing on the target organization.
A. War driving
B. Pharming
C. Skimming
D. Pretexting
Answer: (SHOW ANSWER)
Pharming is a cyber attack intended to redirect a website's traffic to another, bogus website. By poisoning a DNS server's cache, attackers can redirect users from the site they intended to visit to one that is malicious, without the user's knowledge or any action on their part, such as clicking a deceptive link. This technique is particularly insidious because it can affect well-intentioned users who type the correct URL into their browsers but are still redirected. War driving involves searching for wireless networks from a moving vehicle, skimming refers to stealing credit card information using a device placed on ATMs or point-of-sale terminals, and pretexting is a form of social engineering where the attacker lies to obtain privileged data.References:The Incident Handler (ECIH v3) certification program covers a variety of cyber attacks and techniques, including DNS poisoning and pharming, explaining how attackers exploit vulnerabilities to redirect users to fraudulent sites.

NEW QUESTION: 66
If a hacker cannot find any other way to attack an organization, they can influence an employee or a disgruntled staff member. What type of threat is this?
A. Phishing attack
B. Insider attack
C. Footprinting
D. Identity theft

Answer: (SHOW ANSWER)
If a hacker influences an employee or a disgruntled staff member to gain access to an organization's resources or sensitive information, this is classified as an insider attack.Insider attacks are perpetrated by individuals within the organization, such as employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems. The threat from insiders can be intentional, as in the case of a disgruntled employee seeking to harm the organization, or unintentional, where an employee is manipulated or coerced by external parties without realizing the implications of their actions.
Phishing attacks, footprinting, and identity theft represent different types of cybersecurity threats where the attacker's method or objective differs from that of insider attacks.References:The ECIH v3 certification program addresses various types of threats, including insider threats, emphasizing the importance of recognizing and mitigating risks posed by individuals within the organization.

NEW QUESTION: 67
Performing Vulnerability Assessment is an example of a:
A. Post Incident Management
B. Incident Response
C. Pre-Incident Preparation
D. Incident Handling
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Your manager hands you several items of digital evidence and asks you to investigate them in the order of volatility. Which of the following is the MOST volatile?
A. Cache
B. Disk
C. Emails
D. Temp files
Answer: A (LEAVE A REPLY)
In the context of digital evidence investigation, volatility refers to how quickly data can change or be lost when power is removed or systems are altered. Among the options provided, cache is the most volatile because it is temporary storage that is designed to speed up access to data and is frequently overwritten. Cache data resides in RAM and includes things like memory buffers, system and network information, and process execution data, which are lost upon reboot or power loss. This contrasts with disks, emails, and temp files, which are considered less volatile because they are stored on permanent or semi-permanent media and are less likely to be immediately lost or overwritten.References:The Incident Handler (ECIH v3) curriculum includes principles of digital evidence handling, which emphasizes the importance of collecting evidence in

descending order of volatility to ensure that the most ephemeral data is preserved before it's lost.

NEW QUESTION: 69
The steps followed to recover computer systems after an incident are:
A. System validation, restoration, operation and monitoring
B. System monitoring, validation, operation and restoration
C. System restoration, validation, operation and monitoring
D. System restoration, operation, validation, and monitoring
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
An organization implemented an encoding technique to eradicate SQL injection attacks. In this technique, if a user submits a request using single-quote and some values, then the encoding technique will convert it into numeric digits and letters ranging from a to f. This prevents the user request from performing SQL injection attempt on the web application. Identify the encoding technique used by the organization.
A. Unicode encoding
B. Base64 encoding
C. Hex encoding
D. URL encoding
Answer: C (LEAVE A REPLY)
Hex encoding (also known as hexadecimal encoding) involves converting binary data into hexadecimal representation. In the context described, when a user submits a request with potentially malicious input (such as a single quote and other characters in an attempt to perform SQL injection), the encoding technique converts this input into a string of hexadecimal digits (ranging from 0 to 9 and A to F). This prevents the direct interpretation of the input as SQL commands by the database, thereby mitigating the risk of SQL injection attacks. This method is a form of input sanitization that helps ensure that user input cannot be used to manipulate database queries directly.
References:The use of hex encoding as a technique to prevent SQL injection attacks is discussed in the ECIH v3 course materials. This includes an explanation of how encoding user input can protect web applications from injection and other forms of attacks by ensuring that inputs are treated as data rather than executable code.

NEW QUESTION: 71
Which of the following information security personnel handles incidents from management and technical point of view?
A. Network administrators
B. Incident manager (IM)
C. Threat researchers

D. Forensic investigators
Answer: (SHOW ANSWER)
In the context of information security, the Incident Manager (IM) plays a crucial role in handling incidents from both a management and technical perspective. The Incident Manager is responsible for overseeing the entire incident response process, coordinating with relevant stakeholders, ensuring that incidents are analyzed, contained, and eradicated efficiently, and that recovery processes are initiated promptly. They are pivotal in ensuring communication flows smoothly between technical teams and upper management and that all actions taken are aligned with the organization's broader security policies and objectives. Unlike network administrators, threat researchers, or forensic investigators who may play more specialized roles within the incident response process, the Incident Manager has a broad oversight role that encompasses both technical and managerialaspects to ensure a comprehensive and coordinated response to security incidents.References:Incident Handler (ECIH v3) courses and study guides emphasize the role of the Incident Manager as integral to the incident handling process, underscoring their importance in bridging the gap between technical response actions and strategic management decisions.

NEW QUESTION: 72
Jason is an incident handler dealing with malware incidents. He was asked to perform a memory dump analysis in order to collect the information about the basic functionality of any program. As apart of his assignment, he needs to perform string search analysis to search for the malicious string that could determine the harmful actions that a program can perform.
Which of the following string-searching tools does Jason need to use to perform the intended task?
A. Bin Text
B. Process Explorer
C. PE View
D. Dependency Walker Information about the resource is in the response body.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 73
For analyzing the system, the browser data can be used to access various credentials. Which of the following tools is used to analyze the history data files in Microsoft Edge browser?
A. ChromeHistoryView
B. BrowsingHistoryView
C. MZCacheView
D. MZHistoryView
Answer: B (LEAVE A REPLY)

BrowsingHistoryView is a tool designed to collect and analyze history data from various web browsers, including Microsoft Edge. It allows users to view the browsing history stored by their browsers in one unified interface. This includes URLs visited, page titles, visit times, and the number of visits to each page. While ChromeHistoryView is specific to Google Chrome, BrowsingHistoryView supports multiple browsers, making it versatile for analyzing history data across different platforms. MZCacheView and MZHistoryView do not exist as tools recognized for this purpose in the context of Microsoft Edge or other browser history analysis.References:Incident Handler (ECIH v3) courses and study guides emphasize the importance of using digital forensic tools, such as BrowsingHistoryView, for analyzing web browser data during investigations.

NEW QUESTION: 74
You area systems administrator for a company. You are accessing your fileserver remotely for maintenance.
Suddenly, you are unable to access the server. After contacting others in your department, you find out that they cannot access the file server either.
You can ping the file server but not connect to it via RD. You check the Active Directory Server, and all is well.
You check the email server and find that emails are sent and received normally.
What is the most likely issue?
A. A denial-of-service issue
B. An admin account issue
C. An email service issue
D. The fileserver has shutdown
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-prof le executives of the company.
What type of phishing attack is this?
A. Spear phishing
B. Whaling
C. Puddle phishing
D. Pharming
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
In NIST risk assessment/ methodology; the process of identifying the boundaries of an IT system along with the resources and information that constitute the system is known as:
A. Asset valuation

B. Asset Identification
C. System characterization
D. System classification
Answer: C (LEAVE A REPLY)

NEW QUESTION: 77
Which of the following service(s) is provided by the CSIRT:
A. Development of security tools
B. Vulnerability handling
C. All the above
D. Technology watch
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
James is a professional hacker and is employed by an organization to exploit their cloud services. In order to achieve this, James created anonymous access to the cloud services to carry out various attacks such as password and key cracking, hosting malicious data, and DDoS attacks. Which of the following threats is he posing to the cloud platform?
A. Insecure interface and APIs
B. Data breach/loss
C. Insufficient duo diligence
D. Abuse end nefarious use of cloud services
Answer: (SHOW ANSWER)
James's activities, including creating anonymous access to cloud services to carry out attacks such as password and key cracking, hosting malicious data, and conducting DDoS attacks, exemplify the abuse and nefarious use of cloud services. This threat involves exploiting cloud computing resources to conduct malicious activities, which can impact the cloud service provider as well as other users of the cloud services. This abuse ranges from using the cloud platform's resources for computationally intensive tasks like cracking passwords or encryption keys to conducting DDoS attacks that can disrupt services for legitimate users.References:The Incident Handler (ECIH v3) certification emphasizes understanding cloud-specific security challenges, including the abuse of cloud services,

and recommends strategies for mitigating such risks, highlighting the need for comprehensive security measures to protect cloud environments.

NEW QUESTION: 79
John, a professional hacker, is attacking an organization, where he is trying to destroy the connectivity between an AP and client to make the target unavailable to other wireless devices.
Which of the following attacks is John performing in this case?
A. Routing attack
B. EAP failure
C. Disassociation attack
D. Denial-of-service
Answer: C (LEAVE A REPLY)
In a disassociation attack, the attacker sends disassociation frames to a wireless access point (AP) using a spoofed MAC address of a client or to the client pretending to be the AP. This forces the target to disconnect and often reconnect, causing a disruption in the wireless connectivity. Such attacks can be used to create a denial-of-service condition for the client, making the network resource unavailable. The primary objective of this attack is not to eavesdrop but to disrupt the normal operation of the wireless connection between the client and the AP.
References:The concept of disassociation attacks and their impact on wireless network connectivity is covered in cybersecurity training materials and incident response courses, including those related to the ECIH v3 certification. These materials explain the techniques used in various network attacks, including how disassociation attacks are performed and mitigated.

NEW QUESTION: 80
Which of the following terms refers to the personnel that the incident handling and response (IH&R) team must contact to report the incident and obtain the necessary permissions?
A. Civil litigation
B. Point of contact
C. Criminal referral
D. Ticketing
Answer: (SHOW ANSWER)
In the context of incident handling and response (IH&R), the term "Point of contact" refers to individuals or departments within an organization that are designated to be contacted by the IH&R team in case of an incident. These personnel are crucial for the reporting process and for obtaining the necessary permissions to proceed with incident response activities. They serve as the liaison between the incident response team and other parts of the organization, external agencies, or partners involved in the incident response process. The

point of contact is responsible for facilitating communication, coordinating actions, and ensuring that the appropriate stakeholders are engaged in the response to an incident. This role is pivotal in ensuring a swift and effective response to security incidents, minimizing damage, and restoring operations.
References:Incident Handler (ECIH v3) courses and study guides typically emphasize the importance of clearly defined roles and responsibilities within the incident response process, including the designation of points of contact.

NEW QUESTION: 81
Andrew, an incident responder, is performing risk assessment of the client organization. As a part of risk assessment process, he identified the boundaries of the IT systems, along with the resources and the information that constitute the systems.
Identify the risk assessment step Andrew is performing.
A. System characterization
B. Control analysis
C. Likelihood determination
D. Control recommendations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82
CERT members can provide critical support services to first responders such as:
A. Immediate assistance to victims
B. A + C
C. Organizing spontaneous volunteers at a disaster site
D. Consolidated automated service process management platform
Answer: B (LEAVE A REPLY)

NEW QUESTION: 83
James has been appointed as an incident handling and response (IH&R) team lead and he was assigned to build an IH&R plan along with his own team in the company.
Identify the IH&R process step James is currently working on.
A. Eradication
B. Recovery
C. Preparation
D. Notification
Answer: C (LEAVE A REPLY)
In the context of incident handling and response (IH&R), the preparation phase is the initial step where teams and resources are organized to effectively respond to potential security incidents. This phase involves building the IH&R team, developing incident response plans and policies, setting up communication channels, and ensuring that the team has the necessary tools and authority to act. James, being assigned to build an IH&R plan and

organize his team, is engaging in the preparation step of the incident response process. This foundational step is crucial for ensuring a coordinated and efficient response to incidents when they occur.
References:The importance of the preparation phase in the incident response lifecycle is emphasized in various cybersecurity frameworks and guidelines, including those covered in ECIH v3 certification materials, which detail the roles, responsibilities, and planning necessary to establish an effective incident response capability.

NEW QUESTION: 84
Sam received an alert through an email monitoring tool indicating that their company was targeted by a phishing attack. After analyzing the incident, Sam identified that most of the targets of the attack are high-profile executives of the company. What type of phishing attack is this?
A. Pharming
B. Whaling
C. Puddle phishing
D. Spear phishing
Answer: B (LEAVE A REPLY)
Whaling is a specific type of phishing attack that targets high-profile executives or individuals within an organization, often with the intent to steal sensitive information or gain access to their accounts for financial fraud. The term "whaling" is used because it targets the "big fish" of an organization. Given that Sam identified the targets of the attack as high-profile executives, the described scenario is indicative of a whaling attack.
References:The ECIH v3 curriculum includes a section on different types of phishing attacks, including whaling, emphasizing the strategies attackers use to target individuals based on their roles within an organization.

NEW QUESTION: 85
A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to
propagate is called:
A. Trojan
B. Worm
C. RootKit
D. Virus
Answer: D (LEAVE A REPLY)

NEW QUESTION: 86
An organization named Sam Morison Inc. decided to use cloud-based services to reduce the cost of their maintenance. They first identified various risks and threats associated with

cloud service adoption and migrating critical business data to third party systems. Hence, the organization decided to deploy cloud-based security tools to prevent upcoming threats. Which of the following tools would help the organization to secure cloud resources and services?

A. Nmap

B. Burp Suite

C. Wire shark

D. Alert Logic

Answer: D (LEAVE A REPLY)

NEW QUESTION: 87

Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall. They then use any software or hardware access point to perform an attack. Which of the following is this type of attack?

A. Malware attack

B. Rogue- access point attack

C. Password-based attack

D. Email infection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 88

Ross is an incident manager (IM) at an organization, and his team provides support to all users in the organization who are affected by threats or attacks. David, who is the organization's internal auditor, is also part of Ross's incident response team. Which of the following is David's responsibility?

A. Perform the- necessary action to block the network traffic from the suspectoc intruder.

B. Identify and report security loopholes to the management for necessary action.

C. Coordinate incicent containment activities with the information security officer (ISO).

D. Configure information security controls.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 89

BadGuy Bob hid files in the slack space, changed the file headers, hid suspicious files in executables, and changed the metadata for all types of files on his hacker laptop.
What has he committed?

A. Legal hostility

B. Adversarial mechanics

C. Anti-forensics

D. Felony

Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
The main feature offered by PGP Desktop Email is:
A. End-to-end email communications
B. Email service during incidents
C. End-to-end secure email service
D. None of the above
Answer: C (LEAVE A REPLY)

NEW QUESTION: 91
Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :
A. All the above
B. Threat-source motivation and capability
C. Nature of the vulnerability
D. Existence and effectiveness of the current controls
Answer: (SHOW ANSWER)

NEW QUESTION: 92
James has been appointed as an incident handling and response (IH&R) team lead and he was assigned to build an IH&R plan along with his own team in the company.
Identify the IH&R process step James is currently working on.
A. Eradication
B. Preparation
C. Notification
D. Recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
James is a professional hacker and is employed by an organization to exploit their cloud services. In order to achieve this, James created anonymous access to the cloud services to carryout various attacks such as password and key cracking, hosting malicious data, and DDoS attacks.
Which of the following threats is he posing to the cloud platform?

A. Insufficient due diligence
B. Insecure interface and APIs
C. Abuse and nefarious use of cloud services
D. Data breach/loss
Answer: (SHOW ANSWER)

NEW QUESTION: 94
Smith employs various malware detection techniques to thoroughly examine the network and its systems for suspicious and malicious malware files. Among all techniques, which one involves analyzing the memory dumps or binary codes for the traces of malware?
A. Live system
B. Static analysis
C. Dynamic analysis
D. Intrusion analysis
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95
What is the best staffing model for an incident response team if current employees' expertise is very low?
A. Fully insourced
B. Partially outsourced
C. Fully outsourced
D. All the above
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which is the incorrect statement about Anti-keyloggers scanners:
A. Software tools
B. Run in stealthy mode to record victims online activity
C. Detect already installed Keyloggers in victim machines
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Eve's is an incident handler in ABC organization. One day, she got a complaint about email hacking incident from one of the employees of the organization. As a part of incident handling and response process, she must follow many recovery steps in order to recover from incident impact to maintain business continuity.
What is the first step that she must do to secure employee account?
A. Enable two-factor authentication
B. Enable scanning of links and attachments in all the emails
C. Restore the email services and change the password

D. Disabling automatic file sharing between the systems
Answer: A (LEAVE A REPLY)

NEW QUESTION: 98
Bran is an incident handler who is assessing the network of the organization. He wants to detect ping sweep attempts on the network using Wireshark. Which of the following Wireshark filters would Bran use to accomplish this task?
A. icmp.ident
B. icmp.redir_gw
C. icmp.scq
D. icmp.lype==8
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
Bran is an incident handler who is assessing the network of the organization. He wants to detect ping sweep attempts on the network using Wireshark. Which of the following Wireshark filters would Bran use to accomplish this task?
A. icmp.scq
B. icmp.lype==8
C. icmp.ident
D. icmp.redir_gw
Answer: B (LEAVE A REPLY)
In the context of using Wireshark, a popular network protocol analyzer, to detect ping sweep attempts on a network, the filtericmp.type==8is used. ICMP (Internet Control Message Protocol) is utilized for sending error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP type 8 messages are echo requests, which are used by the ping command to test the reachability of a host on an IP network. A ping sweep consists of ICMP echo requests sent to multiple hosts to find which ones are alive. By applying theicmp.type==8filter in Wireshark, Bran can isolate and examine the echo request messages, helping to identify ping sweep attempts, which are characterized by a high volume of ICMP echo requests over a broad range of IP addresses in a short period.
References:The ECIH v3 program by EC-Council covers network monitoring and analysis techniques, including the use of Wireshark and its filters to detect various types of network scanning activities, such as ping sweeps.

NEW QUESTION: 100
Marley was asked by his incident handing and response (IH&R) team lead to collect volatile data such as system information and network information present in the registries, cache, and RAM of victim's system.
Identify the data acquisition method Marley must employ to collect volatile data.

A. Validate data acquisition
B. Live data acquisition
C. Static data acquisition
D. Remote data acquisition
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Zaimasoft, a prominent IT organization, was attacked by perpetrators who directly targeted the hardware and caused irreversible damage to the hardware. In result, replacing or reinstalling the hardware was the only solution.
Identify the type of denial-of-service attack performed on Zaimasoft.
A. DRDoS
B. PDoS
C. ddos
D. DoS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following techniques prevent or mislead incident-handling process and may also affect the collection, preservation, and identification phases of the forensic investigation process?
A. Enumeration
B. Anti-forensics
C. Scanning
D. Footprinting
Answer: B (LEAVE A REPLY)

NEW QUESTION: 103
To effectively describe security incidents, it is necessary to adopt a common set of terminology and to categorize the incidents.
According to ECIH text, in which category would you place an incident that involves illegal file download by a suspected or unknown user?
A. Middle level
B. Ultra High Level
C. Low Level
D. High level
Answer: D (LEAVE A REPLY)

NEW QUESTION: 104
Which of the following is NOT one of the techniques used to respond to insider threats:
A. Disabling the computer systems from network connection

B. Preventing malicious users from accessing unclassified information
C. Placing malicious users in quarantine network, so that attack cannot be spread
D. Blocking malicious user accounts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 105
When an employee is terminated from his or her job, what should be the next immediate step taken by an organization?
A. All access rights of the employee to physical locations, networks, systems, applications and data should be disabled
B. The organization should enforce separation of duties
C. The organization should monitor the activities of the system administrators and privileged users who have permissions to access the sensitive information
D. The access requests granted to an employee should be documented and vetted by the supervisor
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
Stanley works as an incident responder at a top MNC based out of Singapore. He was asked to investigate a cybersecurity incident that recently occurred in the company. While investigating the crime, he collected the evidence from the victim systems. He must present this evidence in a clear and comprehensible manner to the members of jury so that the evidence explains the facts clearly and further helps in obtaining an expert opinion on the same to confirm the investigation process.
In the above scenario, what is the characteristic of the digital evidence Stanley tried to preserve?
A. Complete
B. Admissible
C. Believable
D. Authentic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following best describes an email issued as an attack medium, in which several messages are sent to a mailbox to cause overflow?
A. Smurf attack
B. Masquerading
C. Spoofing
D. Email-bombing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:
A. It helps in reconstructing the events after a problem has occurred
B. It helps calculating intangible losses to the organization due to incident
C. It helps tracking individual actions and allows users to be personally accountable for their actions
D. It helps in compliance to various regulatory laws, rules,and guidelines
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Shiela is working at night as an incident handler. During a shift, servers were affected by a massive cyberattack. After she classified and prioritized the incident, she must report the incident, obtain necessary permissions, and perform other incident response functions. What list should she check to notify other responsible personnel?
A. HR log book
B. Point of contact
C. Email list
D. Phone number list
Answer: B (LEAVE A REPLY)
In the context of incident handling, the "point of contact" list is essential for ensuring that Sheila, the incident handler working at night, can quickly notify the responsible personnel within the organization about the cyberattack. This list typically includes the contact information of key stakeholders and decision-makers who need to be informed about security incidents, allowing for timely communication, decision-making, and response coordination.
References:Incident Handler (ECIH v3) courses and study guides stress the importance of having a well-maintained point of contact list as part of an organization's incident response plan to facilitate efficient and effective communication during and after cybersecurity incidents.

NEW QUESTION: 110
While analyzing a file, Ryan discovered that an attacker used an anti-forensics method, wherein the attacker embedded a hidden message inside an image file.
What type of method is this?
A. Password protection
B. Steganography
C. Golden ticket
D. Program packers
Answer: (SHOW ANSWER)

NEW QUESTION: 111
Who is mainly responsible for providing proper network services and handling network-related incidents in each cloud service model?
A. Cloud auditor
B. Cloud service provider
C. Cloud consumer
D. Cloud brokers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following is an attack that attempts to prevent the use of systems, networks, or applications by the intended users?
A. Denial of service (DoS) attack
B. Fraud and theft
C. Unauthorized access
D. Malicious code or insider threat attack
Answer: A (LEAVE A REPLY)
A Denial of Service (DoS) attack aims to make a computer resource, network, or application unavailable to its intended users, thereby preventing legitimate users from using the service. This is achieved by overwhelming the target with a flood of internet traffic or sending information that triggers a crash. In contrast, fraud and theft involve the unauthorized acquisition of data or assets, unauthorized access refers to gaining entry into systems without permission, and malicious code or insider threat attacks relate to software designed to cause harm or unauthorized actions by trusted users within the organization. The specific intent of a DoS attack is to disrupt service, making it a distinct category focused on denial of availability.References:The Incident Handler (ECIH v3) certification materials discuss various types of cybersecurity threats, including DoS attacks, outlining their methods, objectives, and impacts on targeted systems or networks.

NEW QUESTION: 113

James is working as an incident responder at Cyber Sol Inc. The management instructed James to invest gate a cybersecurity incident that recently happened in the company. As a part of the investigation process, James started collecting volatile information from a system running on Windows operating system.
Which of the following commands helps James in determining all the executable files for running processes?
A. dos key/history
B. top
C. netstat-ab
D. date/t&time/t
Answer: C (LEAVE A REPLY)

NEW QUESTION: 114
A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:

A. Control analysis
B. System characterization
C. Threat identification
D. Identification Vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 115
Incident management team provides support to all users in the organization that are affected by the threat or
attack. The organization's internal auditor is part of the incident response team. Identify one of the
responsibilities of the internal auditor as part of the incident response team:
A. Coordinate incident containment activities with the information security officer
B. Identify and report security loopholes to the management for necessary actions
C. Configure information security controls
D. Perform necessary action to block the network traffic from suspected intruder
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
A self-replicating malicious code that does not alter files but resides in active memory and duplicates itself,

spreads through the infected network automatically and takes advantage of file or information transport
features on the system to travel independently is called:
A. RootKit
B. Trojan
C. Worm
D. Virus
Answer: (SHOW ANSWER)

NEW QUESTION: 117
To whom should an information security incident be reported?
A. Human resources and Legal Department
B. It should not be reported at all and it is better to resolve it internally
C. It should be reported according to the incident reporting & handling policy
D. Chief Information Security Officer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following is not the responsibility of first responders?
A. Protecting the crime scene
B. Packaging and transporting the electronic evidence
C. Identifying the crime scene
D. Preserving temporary and fragile evidence and then shutdown or reboot the victim's computer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 119
Agencies do NOT report an information security incident is because of:
A. Afraid of negative publicity
B. Have full knowledge about how to handle the attack internally
C. Do not want to pay the additional cost of reporting an incident
D. All the above
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
Stanley works as an incident responder at a top MNC based in Singapore. He was asked to investigate a cybersecurity incident that recently occurred in the company. While investigating the incident, he collected evidence from the victim systems. He must present this evidence in a clear and comprehensible manner to the members of a jury so that the evidence clarifies the facts and further helps in obtaining an expert opinion on the incident

to confirm the investigation process. In the above scenario, which of the following characteristics of the digital evidence did Stanley attempt to preserve?

A. Completeness

B. Authenticity

C. Admissibility

D. Believability

Answer: B (LEAVE A REPLY)

NEW QUESTION: 121

A self-replicating malicious code that does not alter files but resides in active memory and duplicates itself, spreads through the infected network automatically and takes advantage of file or information transport features on the system to travel independently is called:

A. Trojan

B. RootKit

C. Worm

D. Virus

Answer: C (LEAVE A REPLY)

NEW QUESTION: 122

Which of the following is not a best practice to eliminate the possibility of insider attacks?

A. Always leave business details over voicemail or email broadcast message

B. Monitor employee behaviors and the computer systems used by employees

C. Disable the users from installing unauthorized software or accessing malicious websites using the corporate network

D. Implement secure backup and disaster recovery processes for business continuity

Answer: (SHOW ANSWER)

NEW QUESTION: 123

Lack of forensic readiness may result in:

A. System downtime

B. All the above

C. Loss of clients thereby damaging the organization's reputation

D. Data manipulation, deletion, and theft
Answer: (SHOW ANSWER)

NEW QUESTION: 124
A Malicious code attack using emails is considered as:
A. Email attack
B. Inappropriate usage incident
C. Multiple component attack
D. Malware based attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 125
Contingency planning enables organizations to develop and maintain effective methods to handle emergencies. Every organization will have its own specific requirements that the planning should address. There are five major components of the IT contingency plan, namely supporting information, notification activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution plan?
A. To restore the original site, tests systems to prevent the incident and terminates operations
B. To provide the introduction and detailed concept of the contingency plan
C. To define the notification procedures, damage assessments and offers the plan activation
D. To provide a sequence of recovery activities with the help of recovery procedures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by anti-
spyware tools is most likely called:

A. Software Key Grabber
B. Hardware Keylogger
C. USB adapter

D. Anti-Keylogger
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 127
Stenley is an incident handler working for Texa Corp. located in the United States. With the growing concern of increasing emails from outside the organization, Stenley was asked to take appropriate actions to keep the security of the organization intact. In the process of detecting and containing malicious emails, Stenley was asked to check the validity of the emails received by employees.
Identify the tools he can use to accomplish the given task.
A. EventLog Analyzer
B. PoliteMail
C. PointofMail
D. Email Dossier
Answer: D (LEAVE A REPLY)

NEW QUESTION: 128
Miko was hired as an incident handler in XYZ company. His first task was to identify the PING sweep attempts inside the network. For this purpose, he used Wireshark to analyze the traffic. What filter did he use to identify ICMP ping sweep attempts?
A. icrrip.lype == icmp
B. tcp.typc == icmp
C. icmp.type == 8 or icmp.type ==0
D. udp.lype - 7
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following best describes an email issued as an attack medium, in which several messages are sent to a mailbox to cause overflow?
A. Email-bombing
B. Masquerading
C. Spoofing
D. Smurf attack
Answer: A (LEAVE A REPLY)
Email-bombing refers to the attack where the attacker sends a massive volume of emails to a specific email address or mail server in order to overflow the mailbox or overwhelm the server, potentially causing it to fail or deny service to legitimate users. This attack can disrupt communications and, in some cases, lead to the targeted email account being disabled. Masquerading involves pretending to be another legitimate user, spoofing is the creation of emails (or other communications) with a forged sender address, and a smurf

attack is a specific type of Distributed Denial of Service (DDoS) attack that exploits Internet Protocol (IP) and Internet Control Message Protocol (ICMP) to flood a target with traffic. Email-bombing specifically targets email services with the goal of causing disruption by overflowing inboxes.References:ECIH v3 courses and study guides often include discussions on various attack vectors used by cybercriminals, including email-based threats and their impact on organizational security.

NEW QUESTION: 130
Khai was tasked with examining the logs from a Linux email server. The server uses Sendmail to execute the command to send emailsand Syslog to maintain logs. To validate the data within email headers, which of the following directories should Khai check for information such as source and destination IP addresses, dates, and timestamps?
A. /Var/log/mailog
B. /ar/log/sendmail
C. /va r/log/mai11og
D. /va r/log/sendmail/mailog
Answer: A (LEAVE A REPLY)
In a Linux environment, email servers such as Sendmail log events, including details about sent and received emails, in a specific log file. The correct directory and file for examining email logs, particularly for Sendmail and using Syslog for logging, is /Var/log/maillog. Thisfile contains vital information for forensic and incident response purposes, including source and destination IP addresses, email addresses, timestamps, and other data relevant to the email traffic handled by the server. By analyzing this log, incident responders can gather evidence related to email-based incidents, trace the source of malicious emails, and understand the scope of an incident. It's crucial for individuals like Khai, who are tasked with examining logs, to know the correct log file locations and their contents to effectively validate and analyze email header information and other relevant data.
References:Incident Handler (ECIH v3) study materials often cover the logging mechanisms of common services and applications on Linux systems, including email servers like Sendmail, and the importance of log files like /var/log/maillog in incident investigation and response activities.

NEW QUESTION: 131
Alice is a disgruntled employee. She decided to acquire critical information from her organization for financial benefit.
To accomplish this, Alice started running a virtual machine on the same physical host as her victim's virtual machine and took advantage of shared physical resources (processor cache) to steal data (cryptographic key/plaintext secrets) from the victim machine. Identify the type of attack Alice is performing in the above scenario.
A. SQL injection attack

B. Man-in-the-cloud attack
C. Service hijacking
D. Side channel attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
Which of the following is a correct statement about incident management, handling and response:
A. Incident response is on the functions provided by incident handling
B. Triage is one of the services provided by incident response
C. Incident handling is on the functions provided by incident response
D. Incident response is one of the services provided by triage
Answer: (SHOW ANSWER)

NEW QUESTION: 133
They type of attack that prevents the authorized users to access networks, systems, or applications by exhausting the network resources and sending illegal requests to an application is known as:
A. Denial of Service attack
B. Session Hijacking attack
C. SQL injection attack
D. Man in the Middle attack
Answer: (SHOW ANSWER)

NEW QUESTION: 134
A Host is infected by worms that propagates through a vulnerable service; the sign(s) of the presence of the
worm include:
A. All the above
B. Decrease in network usage
C. Established connection attempts targeted at the vulnerable services
D. System becomes instable or crashes
Answer: (SHOW ANSWER)

NEW QUESTION: 135
Which of the following terms refers to vulnerable account management functions, including account update, recovery of forgotten or lost passwords, and password reset, that might weaken valid authentication schemes?
A. SQL injection
B. Directory traversal
C. Broken account management

D. Cross-site scripting
Answer: (SHOW ANSWER)

NEW QUESTION: 136
The ability of an agency to continue to function even after a disastrous event, accomplished through the
deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup
and recovery strategy is known as:
A. Contingency Planning
B. Disaster Planning
C. Business Continuity Plan
D. Business Continuity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
Qual Tech Solutions is a leading security services enterprise. Dickson, who works as an incident responder with this firm, is performing a vulnerability assessment to identify the security problems in the network by using automated tools for identifying the hosts, services, and vulnerabilities in the enterprise network.
In the above scenario, which of the following types of vulnerability assessment is Dickson performing?
A. Internal assessment
B. Active assessment
C. External assessment
D. Passive assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Joseph is an incident handling and response (IH&R) team lead in Toro Network Solutions Company. As a part of the IH&R process, Joseph alerted the service providers,

developers, and manufacturers about the affected resources. Identify the stage of IH&R process Joseph is currently in.

A. Recovery

B. Containment

C. Eradication

D. Incident triage

Answer: B (LEAVE A REPLY)

NEW QUESTION: 139

Investigator Ian gives you a drive image to investigate. What type of analysis are you performing?

A. Real-time

B. Static

C. Dynamic

D. Live

Answer: (SHOW ANSWER)

When Investigator Ian gives you a drive image to investigate, the type of analysis you are performing is static analysis. Static analysis involves examining the contents of a drive, file, or binary without executing the system or the application. It's about analyzing the data at rest. This type of analysis is crucial for forensics investigations because it allows for the examination of files, directories, and system information without altering any state or data, thereby preserving the integrity of the evidence. Static analysis is contrasted with dynamic analysis, which involves analyzing a system in operation (real-time or live) or executing the application to observe its behavior.References:Incident Handler (ECIH v3) courses and study guides highlight the importance of static analysis in digital forensics, detailing methods for examining disk images, files, and other digital artifacts to gather evidence without compromising its integrity.

NEW QUESTION: 140

A colleague wants to minimize their security responsibility because they are in a small organization. They are evaluating a new application that is offered in different forms. Which form would result in the least amount of responsibility for the colleague?

A. On-prom installation

B. saaS

C. laaS

D. PaaS

Answer: B (LEAVE A REPLY)

Software as a Service (SaaS) offers the least amount of security responsibility for the end-user or organization, as the service provider manages the underlying infrastructure, software maintenance, security patching, and updates. Choosing a SaaS application means the colleague's organization would not be responsible for the physical servers,

operating systems, or the application's security configurations, making it the best option for minimizing their security responsibilities.
References:In the Certified Incident Handler (ECIH v3) course materials, the various cloud service models (IaaS, PaaS, SaaS) are discussed with a focus on their implications for security responsibilities and management.

NEW QUESTION: 141
Alexis works as an incident responder at XYZ organization. She was asked to identify and attribute the actors behind an attack that occurred recently. For this purpose, she is performing a type of threat attribution that deals with the identification of a specific person, society, or country sponsoring a well-planned and executed intrusion or attack on its target.
Which of the following types of threat attributions is Alexis performing?
A. Nation-state attribution
B. True attribution
C. Campaign attribution
D. Intrusion set attribution
Answer: A (LEAVE A REPLY)

NEW QUESTION: 142
Which one of the following is the correct flow of the stages in an incident handling and response (IH&R) process?
A. Incident triage -> Eradication -> Containment -> Incident recording -> Preparation -> Recovery -> Post-incident activities
B. Incident recording -> Preparation -> Containment -> Incident triage -> Recovery > Eradication -> Post-incident activities
C. Preparation -> Incident recording -> Incident triage -> Containment -> Eradication -> Recovery -> Post-incident activities
D. Containment -> Incident recording -> Incident triage -> Preparation -> Recovery -> Eradication -> Post-incident activities
Answer: C (LEAVE A REPLY)

NEW QUESTION: 143
Electronic evidence may reside in the following:
A. Data Files
B. Other media sources
C. Backup tapes
D. All the above
Answer: (SHOW ANSWER)

NEW QUESTION: 144

Matt is an incident handler working for one of the largest social network companies, which was affected by malware. According to the company's reporting timeframe guidelines, a malware incident should be reported within 1 h of discovery/detection after its spread across the company. Which category does this incident belong to?

A. CAT 1

B. CAT 4

C. CAT 2

D. CAT 3

Answer: (SHOW ANSWER)

In incident response protocols, incidents are categorized based on their severity, impact, and the urgency of the response required. The categorization helps in prioritizing incident response activities and allocating resources accordingly. A CAT 1 (Category 1) incident is typically considered the highest priority, involving significant threats that require immediate response. Given the scenario where a malware incident in one of the largest social network companies must be reported within 1 hour of discovery/detection, this indicates a high-priority incident due to the potential widespread impact and the need for a rapid response to contain and mitigate the malware's spread. The urgency of the reporting timeframe suggests that the incident is considered critical, aligning with the characteristics of a CAT 1 incident, which necessitates immediate action to prevent significant damage or disruption to the company's operations and services.References:The Incident Handler (ECIH v3) curriculum emphasizes the importance of incident categorization and the establishment of clear reporting and response protocols based on the severity and urgency of incidents. This framework enables organizations to respond effectively to incidents like malware attacks by ensuring that high-priority threatsare quickly identified and addressed.

NEW QUESTION: 145

Based on the some statistics; what is the typical number one top incident?

A. Phishing

B. Policy violation

C. Un-authorized access

D. Malware

Answer: A (LEAVE A REPLY)

NEW QUESTION: 146

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of

the following steps focus on limiting the scope and extent of an incident?

A. Data collection

B. Eradication

C. Identification

D. Containment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 147
A computer virus hoax is a message warning the recipient of an on-existent computer virus threat. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know.
Which of the following is not a symptom of virus hoax message?
A. The message prompts the user to install Anti-virus
B. The message from a known email id is caught by SPAM filters due to change in filter settings
C. The message prompts the end user to forward it to his/her email contact list and gain monetary benefits in doing so
D. The message warns to delete certain files if the user does not take appropriate action
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
The following steps describe the key activities in forensic readiness planning:
1. Train the staff to handle the incident and preserve the evidence
2. Create a special process for documenting the procedure
3. Identify the potential evidence required for an incident
4. Determine the source of the evidence
5. Establish a legal advisory board to guide the investigation process
6. Identify if the incident requires full or formal investigation
7. Establish a policy for securely handling and storing the collected evidence
8. Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption Identify the correct sequence of steps involved in forensic readiness planning.
A. 2-->3-->1-->4-->6-->5-->7-->8
B. 3-->4-->8-->7-->6-->1-->2-->5
C. 3-->1-->4-->5-->8-->2-->6-->7
D. 1-->2-->3-->4-->5-->6-->7-->8
Answer: (SHOW ANSWER)
The correct sequence of steps involved in forensic readiness planning, based on the activities described, is as follows:
* Identify the potential evidence required for an incident.
* Determine the source of the evidence.
* Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption.
* Establish a policy for securely handling and storing the collected evidence.
* Identify if the incident requires full or formal investigation.
* Train the staff to handle the incident and preserve the evidence.

* Create a special process for documenting the procedure.
* Establish a legal advisory board to guide the investigation process.This sequence ensures that an organization is prepared to handle incidents efficiently, with a focus on identifying relevant evidence and the legal context of its collection, followed by staff training and the establishment of guiding policies and advisory boards.References:Incident Handler (ECIH v3) courses and study guides include discussions on forensic readiness planning, highlighting the importance of preparing organizations for effective legal and technical handling of incidents.

NEW QUESTION: 149
James is working as an incident responder at CyberSol Inc. The management instructed James to investigate a cybersecurity incident that recently happened in the company. As a part of theinvestigation process, James started collecting volatile information from a system running on Windows operating system.
Which of the following commands helps James in determining all the executable files for running processes?
A. cate A &. time ,/t
B. netstat -ab
C. top
D. doskey/history
Answer: B (LEAVE A REPLY)
Thenetstat -abcommand is useful in Windows operating systems for displaying all connections and listening ports, along with the executable involved in creating each connection or listening port. This can be particularly valuable for an incident responder like James when attempting to determine which processes are running on a system and how they are communicating over the network. This information can help identify malicious processes, unauthorized connections, or other signs of compromise on the system.
Whilenetstat -abdoes not exclusively list executable files for running processes, it ties processes to network activity, which is a critical part of collecting volatile information during a cybersecurity incident investigation.
References:The Certified Incident Handler (ECIH v3) course by EC-Council covers various commands and tools that can be used to collect volatile data from systems as part of incident response activities, highlighting the importance of understanding network connections and the processes responsible for them.

NEW QUESTION: 150
Khai was tasked with examining the logs from a Linux email server. The server uses Sendmail to execute the command to send emails and Syslog to maintain logs.
To validate the data within email headers, which of the following directories should Khai check for information such as source and destination IP addresses, dates, and timestamps?

A. /var/log/mailog
B. /var/log/sendmail
C. /var/log/mailog
D. /var/log/sendmail/mailog
Answer: (SHOW ANSWER)

NEW QUESTION: 151
Which of the following techniques prevent or mislead incident-handling process and may also affect the collection, preservation, and identification phases of the forensic investigation process?
A. Scanning
B. Footprinting
C. Enumeration
D. Anti-forensics
Answer: (SHOW ANSWER)
Anti-forensics techniques are designed to prevent, mislead, or interfere with the incident handling process, affecting the collection, preservation, and identification phases of the forensic investigation process. These techniques include methods to erase, encrypt, or alter information, make data recovery difficult, hide data (e.g., steganography), or otherwise obstruct forensic analysis and investigation efforts. Anti-forensics can significantly challenge the efforts of incident responders and forensic investigators in establishing the facts of a security incident or crime.References:The Incident Handler (ECIH v3) courses and study guides discuss various challenges in digital forensics, including anti-forensics methods and their impact on the effectiveness of forensic investigations.
Top of Form

NEW QUESTION: 152
QualTech Solutions is a leading security services enterprise. Dickson works as an incident responder with this firm. He is performing vulnerability assessment to identify the security problems in the network, using automated tools to identify the hosts, services, and vulnerabilities present in the enterprise network.

Based on the above scenario, identify the type of vulnerability assessment performed by Dickson.

A. Internal assessment

B. Active assessment

C. Passive assessment

D. External assessmen

Answer: B (LEAVE A REPLY)

An active assessment involves using automated tools to scan and probe the network actively to identify hosts, services, and vulnerabilities. This type of assessment directly interacts with the network components to gather information about the existing security posture, unlike passive assessments, which analyze traffic without sending packets to the target systems. Dickson's approach, employing automated tools to identify the network's hosts, services, and vulnerabilities, fits the definition of an active assessment. This method provides a more immediate understanding of the network's vulnerabilities, allowing for timely remediation actions.

References:The ECIH v3 program includes discussions on vulnerability assessment techniques, highlighting the differences between active and passive assessments and their applicability in identifying network security issues.

NEW QUESTION: 153

Investigator Ian gives you a drive image to investigate.

What type of analysis are you performing?

A. Static

B. Dynamic

C. Live

D. Real-time

Answer: A (LEAVE A REPLY)

NEW QUESTION: 154

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

A. Spear Phishing

B. An Adware

C. A Virus Hoax

D. Mail bomb

Answer: (SHOW ANSWER)

NEW QUESTION: 155

Which of the following is a common tool used to help detect malicious internal or compromised actors?

A. Syslog configuration

B. Log forward ng
C. User behavior analytics
D. SOC2 compliance report
Answer: C (LEAVE A REPLY)

NEW QUESTION: 156
Chandler is a professional hacker who is targeting an organization called Technote. He wants to obtain important organizational information that is being transmitted between different hierarchies. In the process, he sniffs the data packets transmitted through the network and then analyzes them to gather packet details such as network, ports, protocols, devices, issues in network transmission, and other network specifications.
Which of the following tools can Chandler employ to perform packet analysis?
A. shARP
B. Omni peek
C. BeEf
D. IDA Pro
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
Mr.Smith is a lead incident responder of a small financial enterprise, which has a few branches in Australia. Recently, the company suffered a massive attack losing$5MM through an inter-banking system.
After an in-depth investigation, it was found that the incident occurred because 6 months ago the attackers penetrated the network through a minor vulnerability and maintained the access without any user being aware of it. They then tried to delete users' fingerprints and performed a lateral movement to the computer of a person with privileges in the inter-banking system. The attackers finally gained access and performed the fraudulent transactions.
Based on the above scenario, identify the most accurate kind of attack.
A. Denial-of-service attack
B. Phishing
C. Ransom ware attack
D. APT attack
Answer: (SHOW ANSWER)

NEW QUESTION: 158
Dan is a newly appointed information security professional in a renowned organization. He is supposed to follow multiple security strategies to eradicate malware incidents.
Which of the following is not considered as a good practice for maintaining information security and eradicating malware incidents?
A. Do not click on web browser pop-up windows

B. Do not open files with file extensions such as.bat, .com, .exe, .p if, .vbs, and soon
C. Do not download or execute applications from third-party sources
D. Do not download or execute applications from trusted sources
Answer: D (LEAVE A REPLY)

NEW QUESTION: 159
The USB tool (depicted below) that is connected to male USB Keyboard cable and not detected by anti-spyware tools is most likely called:

A. Software Key Grabber
B. Anti-Keylogger
C. Hardware Keylogger
D. USB adapter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 160
What is the name of the type of malicious software or malware designed to deny access to a computer system or data until money is paid?
A. Virus
B. Spyware
C. Ransomware
D. Adware
Answer: C (LEAVE A REPLY)

NEW QUESTION: 161
_____ record(s) user's typing.
A. Malware
B. Virus
C. adware
D. Spyware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
Which of the following has been used to evade IDS and IPS?

A. Fragmentation
B. TNP
C. HTTP
D. SNMP
Answer: A (LEAVE A REPLY)
Fragmentation is a technique used by attackers to evade detection by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). By breaking down packets into smaller fragments, attackers can make it more difficult for these security systems to detect malicious payloads or signature-based patterns associated with known attacks. This method exploits the fact that some IDS/IPS solutions may not properly reassemble packet fragments for analysis, thereby allowing malicious fragments to pass through undetected. References:In its coverage of network security mechanisms and evasion techniques, the ECIH v3 certification details how attackers exploit vulnerabilities in the implementation of IDS and IPS systems, including the use of packet fragmentation.

NEW QUESTION: 163
Which of the following forensic investigation phases should occur first?
A. Create two-bitstream copies of the evidence.
B. Preform the first responder procedure.
C. Transport the evidence to the forensic laboratory.
D. Collect preliminary evidence.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164
Ensuring the integrity, confidentiality and availability of electronic protected health information of a patient is known as:
A. Social Security Act
B. Health Insurance Portability and Privacy Act
C. Gramm-Leach-Bliley Act
D. Sarbanes-Oxley Act
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following is an attack that occurs when a malicious program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated?
A. SQL injection
B. Cross-site request forgery
C. Cross-site scripting
D. Insecure direct object references
Answer: (SHOW ANSWER)

NEW QUESTION: 166
The very well-known free open source port, OS and service scanner and network discovery utility is called:
A. Nmap (Network Mapper)
B. Snort
C. SAINT
D. Wireshark
Answer: A (LEAVE A REPLY)

NEW QUESTION: 167
Ikeo Corp, hired an incident response team to assess the enterprise security. As part of the incident handling and response process, the IR team is reviewing the current security policies implemented by the enterprise. The IR team finds that employees of the organization do not have any restrictions on Internet access: they are allowed to visit any site, download any application, and access a computer or network from a remote location. Considering this as the main security threat, the IR team plans to change this policy as it can be easily exploited by attackers. Which of the following security policies is the IR team planning to modify?
A. Promiscuous policy
B. Prudent policy
C. Permissive policy
D. Paranoic policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
ADAM, an employee from a multinational company, uses his company's accounts to send e-mails to a third
party with their spoofed mail address. How can you categorize this type of account?
A. Inappropriate usage incident
B. Network intrusion incident
C. Denial of Service incident

D. Unauthorized access incident
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Oscar receives an email from an unknown source containing his domain name oscar.com. Upon checking the link, he found that it contains a malicious URL that redirects to the website evilsite.org. What type of vulnerability is this?
A. Unvalidated redirects and forwards
B. Bolen
C. Malware
D. SQL injection
Answer: (SHOW ANSWER)

NEW QUESTION: 170
Drake is an incident handler in Dark CLoud Inc. He is intended to perform log analysis in order to detect traces of malicious activities within the network infrastructure.
Which of the following tools Drake must employ in order to view logs in real time and identify malware propagation within the network?
A. Splunk
B. HULK
C. Hydra
D. LOIC
Answer: (SHOW ANSWER)
Splunk is a powerful tool for log analysis, capable of collecting, analyzing, and visualizing data from various sources in real time. For an incident handler like Drake, intending to detect traces of malicious activities within the network infrastructure, Splunk can efficiently parse large volumes of log data, enabling the identification of patterns and anomalies that may indicate malware propagation or other security incidents. Its real-time analysis capabilities make it an ideal tool for monitoring network activities and responding to incidents promptly.

NEW QUESTION: 171
Which one of the following is the correct sequence of flow of the stages in an incident response:
A. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
B. Preparation - Identification - Containment - Eradication - Recovery - Follow-upà
C. Identification - Preparation - Containment - Recovery - Follow-up - Eradication
D. Containment - Identification - Preparation - Recovery - Follow-up - Eradication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172

Alexis works as an incident responder at XYZ organization. She was asked to identify and attributethe actors behind an attack that occurred recently. For this purpose, she is performing a type of threat attribution that deals with the identification of a specific person, society, or country sponsoring a well-planned and executed intrusion or attack on its target. Which of the following types of threat attributions is Alexis performing?

A. Campaign attribution

B. True attribution

C. Nation-state attribution

D. Intrusion set attribution

Answer: C (LEAVE A REPLY)

Nation-state attribution involves identifying a specific country or government as the sponsor behind a cyber-attack or intrusion. This type of threat attribution is focused on determining the involvement of state actors in cyber operations against specific targets, which often involves sophisticated, well-planned, and executed cyber campaigns. Alexis's efforts to identify and attribute the actors behind the attack to a specific nation-state fall under this category, as she seeks to uncover the geopolitical motives and the extent of state sponsorship behind the incident. Nation-state attribution requires analyzing a variety of indicators, including technical evidence, tactics, techniques, and procedures (TTPs), and contextual intelligence. This is distinct from campaign attribution, which focuses on linking attacks to a specific campaign or operation, true attribution, which aims at identifying the actual individuals behind an attack, and intrusion set attribution, which involves attributing a set of malicious activities to a particular threat actor or group.References:The Incident Handler (ECIH v3) certification program includes discussions on various types of threat attributions, highlighting the challenges and methodologies involved in attributing cyber-attacks to specific actors, including nation-states.

NEW QUESTION: 173

An insider threat response plan help san organization minimize the damage caused by malicious insiders.

One of the approaches to mitigate these threats is setting up controls from the human resources department.

Which of the following guidelines can the human resources department use?

A. Access granted to users should be documented and vetted by a supervisor.

B. Disable the default administrative account to ensure accountability.

C. Implement a person-to-person rule to secure the backup process and physical media.

D. Monitor and secure the organization's physical environment.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 174

If the browser does not expire the session when the user fails to logout properly, which of the following OWASP Top 10 web vulnerabilities is caused?

A. A5: Broken access control
B. A2: Broken authentication
C. A7: Cross-site scripting
D. A3: Sensitive data exposure
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
Contingency planning enables organizations to develop and maintain effective methods to handle
emergencies. Every organization will have its own specific requirements that the planning should address.
There are five major components of the IT contingency plan, namely supporting information, notification
activation, recovery and reconstitution and plan appendices. What is the main purpose of the reconstitution
plan?
A. To define the notification procedures, damage assessments and offers the plan activation
B. To provide a sequence of recovery activities with the help of recovery procedures
C. To restore the original site, tests systems to prevent the incident and terminates operations
D. To provide the introduction and detailed concept of the contingency plan
Answer: (SHOW ANSWER)

NEW QUESTION: 176
Miko was hired as an incident handler in XYZ company. His first task was to identify the PING sweep attempts inside the network. For this purpose, he used Wireshark to analyze the traffic. Whatfilter did he use to identify ICMP ping sweep attempts?
A. tcp.typc == icmp
B. icrrip.lype == icmp
C. icmp.type == 8 or icmp.type ==0
D. udp.lype - 7
Answer: C (LEAVE A REPLY)
In Wireshark, to identify ICMP ping sweep attempts, the filtericmp.type == 8 or icmp.type ==0is used. This filter captures ICMP echo requests and echo replies, which are indicative of ping commands. Type 8 represents an echo request used when a source sends a ping, and type 0 represents an echo reply, which is the response from the target. By filtering for these ICMP types, Miko can detect a surge in ping requests across the network, which could indicate a ping sweep attempt-an exploratory activity often used by attackers to discover active hosts on a network by sending ping requests to multiple addresses.References:Incident Handler (ECIH v3) courses and study guides often

incorporate training on using network analysis tools like Wireshark, including how to use filters to detect specific types of network activities and potential threats.

NEW QUESTION: 177
Alex is an incident handler for Tech-o-Tech Inc. and is tasked to identify any possible insider threats within his organization. Which of the following insider threat detection techniques can be used by Alex to detect insider threats based on the behavior of a suspicious employee, both individually and in a group?
A. behaviorial analysis
B. Physical detection
C. Profiling
D. Mole detection
Answer: (SHOW ANSWER)
Behavioral analysis is a technique used to detect insider threats by analyzing the behavior of employees, both individually and in group settings, to identify any actions that deviate from the norm. This method relies on monitoring and analyzing data related to user activities, access patterns, and other behaviors that could indicate malicious intent or a potential security risk from within the organization. Behavioral analysis can detect unusual access to sensitive data, abnormal data transfer activities, and other indicators of insider threats. This approach is proactive and can help in identifying potential insider threats before they result in significant harm to the organization.References:The Incident Handler (ECIH v3) certification materials cover various insider threat detection techniques, including the importance of behavioral analysis as a key method for identifying potential security risks posed by insiders.

NEW QUESTION: 178
Stenley is an incident handler working for Texa Corp. located in the United States. With the growing concern of increasing emails from outside the organization, Stenley was asked to take appropriate actions to keep the security of the organization intact. In the process of detecting and containing malicious emails, Stenley was asked to check the validity of the emails received by employees.
Identify the tools he can use to accomplish the given task.
A. PointofMail
B. Email Dossier
C. PoliteMail
D. EventLog Analyzer
Answer: B (LEAVE A REPLY)
Email Dossier is a tool designed to perform detailed investigations on email messages to verify their authenticity and trace their origin. It can analyze email headers and provide information about the route an email has taken, the servers it passed through, and potentially malicious links or origins. For an incident handler like Stenley, tasked with

verifying the validity of emails and containing malicious email threats, Email Dossier serves as a practical tool for analyzing and validating emails received by employees. By using this tool, Stenley can identify fraudulent or suspicious emails, thereby helping to protect the organization from phishing attacks, malware distribution, and other email-based threats. References:In the context of managing and mitigating the risks associated with email communications, ECIH v3 study materials outline various tools and techniques for email analysis and validation. These resources recommend the use of tools like Email Dossier for incident handlers to effectively scrutinize incoming emails for security threats.

NEW QUESTION: 179
Zaimasoft, a prominent IT organization, was attacked by perpetrators who directly targeted the hardware and caused irreversible damage to the hardware. In result, replacing or reinstalling the hardware was the only solution. Identify the type of denial-of-service attack performed on Zaimasoft.
A. DDoS
B. PDoS
C. DoS
D. DRDoS
Answer: (SHOW ANSWER)

NEW QUESTION: 180
Which of the following tools helps incident handlers to view the filesystem, retrieve deleted data, perform timeline analysis, web art facts, etc., during an incident response process?
A. netstat
B. nbtstat
C. Autopsy
D. Process Explorer
Answer: (SHOW ANSWER)