Vendor: EC-Council

Exam Code: 212-89

Exam Name: EC-Council Certified Incident Handler v3

Version: DEMO

QUESTION 1
Malicious Micky has moved from the delivery stage to the exploitation stage of the kill chain. This malware wants to find and report to the command center any useful services on the system. Which of the following recon attacks is the MOST LIKELY to provide this information?

A. IP range sweep
B. Packet sniffing
C. Session hijack
D. Port scan

Answer: D
Explanation:
When malware moves from the delivery stage to the exploitation stage in the cyber kill chain, its objective often shifts to identifying exploitable vulnerabilities within the targeted system. A port scan is a technique used to discover services that are listening on ports within a system. By scanning the system's ports, the malware can identify open ports and the services running on them, providing valuable information about potential entry points for further exploitation. This type of reconnaissance attack is aimed at gathering intelligence on the target system's network services, which can then be reported back to a command and control center for further malicious activity planning.
Port scanning is more relevant than IP range sweeps, packet sniffing, or session hijacking for identifying useful services on a system because it directly targets the discovery of accessible network services and their corresponding ports. While the other methods can also be part of the reconnaissance phase, they serve different purposes: IP range sweeps aim to identify active IP addresses, packet sniffing intercepts data packets to gather information, and session hijacking involves taking over a valid user session. In contrast, port scanning is specifically designed to enumerate services that could be exploited.

QUESTION 2
Raven is a part of an IH&R team and was informed 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. Eracicotion
C. Containment
D. Incident triage

Answer: B
Explanation:
Eradication is the step in the incident handling and response process where the root cause of an incident is removed, and measures are taken to close all attack vectors to prevent similar incidents in the future. After an incident has been properly contained to stop it from spreading or causing further damage, the eradication phase focuses on eliminating the source of the incident. This could involve removing malware, closing vulnerabilities, or implementing stronger security measures to address the exploitation paths used by the attacker.
In the scenario with Raven, notifying service providers and developers of affected resources is part of the actions taken to address the root cause of the incident. This ensures that any vulnerabilities or issues that contributed to the incident are fixed. By working to remove the root cause and secure the system against similar attacks, Raven is effectively implementing the eradication step of the incident handling process.

QUESTION 3
According to NITS, what are the 5 main actors in cloud computing?

A. Provider, carrier, auditor, broker, and seller
B. Consumer, provider, carrier, auditor, ano broker
C. Buyer, consumer, carrier, auditor, and broker
D. None of these

Answer: B
Explanation:
According to the National Institute of Standards and Technology (NIST), which is a primary source for cloud computing standards and guidelines, the five main actors in cloud computing are Consumer, Provider, Carrier, Auditor, and Broker. These roles are defined as follows:
Consumer: The person or organization that uses cloud computing services.
Provider: The entity that provides the cloud services to consumers.
Carrier: The organization that offers connectivity and transport services to cloud providers and consumers.
Auditor: An independent party that assesses and verifies the cloud services, security controls, and operations.
Broker: An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud providers and consumers.
These actors play critical roles in the ecosystem of cloud computing, ensuring the services are delivered and used securely, efficiently, and effectively.

QUESTION 4
Which of the following is an Inappropriate usage incident?

A. Access-control attack
B. Reconnaissance attack
C. Insider threat
D. Denial-of-service attack

Answer: C
Explanation:
An Inappropriate Usage incident refers to instances where computing resources are misused or abused, often violating organizational policies or laws. While access-control attacks, reconnaissance attacks, and denial-of-service (DoS) attacks represent different types of external threats or methods of attack, an Insider Threat is an example of inappropriate usage. Insider threats come from individuals within the organization, such as employees or contractors, who misuse their access to harm the organization's interests. This can include stealing confidential information, intentionally disrupting systems, or other malicious activities that leverage their legitimate access to the organization's resources.

QUESTION 5
Which of the following is the ECIH phase that involves removing or eliminating the root cause of an incident and closing all attack vectors to prevent similar incidents in the future?

A. Recovery
B. Containment
C. Eradication
D. Vulnerability management phase

Answer: C
Explanation:
Eradication is the phase in the incident response process where the root cause of an incident is removed or eliminated, and all attack vectors are closed to prevent similar incidents in the future. This step follows the containment phase, where the immediate threat is isolated to prevent further damage, and precedes the recovery phase, where normal operations are restored. Eradication involves thoroughly removing malware, unauthorized access mechanisms, or any other elements used in the attack, and securing any vulnerabilities that were exploited. The goal is to ensure that the threat cannot re-emerge and that the systems are secure before they are returned to operational status.

QUESTION 6
An insider threat response plan helps an 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
Explanation:
One of the key approaches to mitigating insider threats is ensuring that access control policies are strictly implemented and monitored. This includes the guideline that access granted to users should be thoroughly documented and vetted by a supervisor. This control helps ensure that users have only the access necessary to perform their job functions, reducing the risk of inappropriate access or misuse of information. Proper documentation and supervisor approval also ensure accountability and traceability of access decisions, which is crucial for detecting and responding to insider threats. The human resources department plays a vital role in this process, working closely with IT and security teams to enforce access control policies, conduct regular reviews of access rights, and manage the onboarding and offboarding process to ensure that access rights are appropriately updated.

QUESTION 7
Alice is an incident handler and she has been informed by her lead that the data on affected systems must be backed up so that it can be retrieved if it is damaged during the incident response process. She was also told that the system backup can also be used for further investigation of the incident. In which of the following stages of the incident handling and response (IH&R) process does Alice need to do a complete backup of the infected system?

A. Containment
B. Incident recording
C. Incident triage
D. Eradication

Answer: A
Explanation:
In the incident handling and response (IH&R) process, backing up the data on affected systems is a critical step that usually falls under the Containment phase. The Containment phase is crucial for limiting the scope and severity of an incident, ensuring that it does not spread further or affect

additional systems. Backing up affected systems during containment is essential for several reasons:
it preserves a snapshot of the system in its current state for forensic analysis, ensures that data is not lost if the system needs to be wiped or altered during the response process, and helps in the recovery process if data is corrupted or lost.
By performing a complete backup of the infected system during the Containment phase, Alice ensures that there is a reliable copy of all data and system states before any major actions, such as eradication or deeper forensic analysis, are taken. This step is also preparatory for the potential use of the backup in analyzing how the incident occurred and in restoring system functionality after the incident is resolved.

QUESTION 8
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. Trojan
C. Spyware
D. Virus

Answer: B
Explanation:
The scenario described is characteristic of a Trojan. A Trojan is a type of malware that disguises itself as legitimate software but performs malicious actions once installed. Unlike viruses, which can replicate themselves, or worms, which can spread across networks on their own, Trojans rely on the guise of legitimacy to trick users into initiating their execution. In this case, the user believed they were downloading and installing genuine software, but the reality was that the application contained a Trojan. The malicious code executed upon installation provided unauthorized remote access to the user's computer, which could be used by an attacker to control the system, steal data, install additional malware, or carry out other malicious activities. Trojans can come in many forms and can be used to achieve a wide range of malicious objectives, making them a versatile and dangerous type of cyber threat. The deceptive nature of Trojans, exploiting the trust users have in what appears to be legitimate software, is what makes them particularly effective and widespread.

QUESTION 9
Finn is working in the eradication phase, wherein he is eliminating the root cause of an incident that occurred in the Windows operating system installed in a system. He ran a tool that can detect missing security patches and install the latest patches on the system and networks. Which of the following tools did he use to detect the missing security patches?

A. Microsoft Cloud App Security
B. Offico360 Advanced Throat Protection
C. Microsoft Advanced Threat Analytics
D. Microsoft Baseline Security Analyzer

Answer: D
Explanation:
The Microsoft Baseline Security Analyzer (MBSA) is a tool designed to assess a computer or network's security state by checking for missing security updates and common security misconfigurations. In the scenario with Finn, who is working in the eradication phase of an incident response process, the use of MBSA makes sense. The tool's ability to detect missing

security patches and recommend the installation of the latest patches is crucial for eliminating vulnerabilities in the Windows operating system that could be the root cause of the incident. MBSA scans the system for missing security updates, misconfigurations, and other vulnerabilities and provides detailed reports and recommendations for remediation. This step is vital in the eradication phase, where the goal is to remove the root causes of the incident and secure the system against future attacks. By ensuring that all necessary patches are applied, Finn is addressing any security gaps that could be exploited by attackers.

QUESTION 10
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
Explanation:
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.

QUESTION 11
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. Paranoic policy
B. Prudent policy
C. Promiscuous policy
D. Permissive policy

Answer: D
Explanation:
A permissive security policy is one that allows employees broad freedoms in terms of internet access, application downloads, and remote access capabilities. In the scenario described, the incident response team identifies that the lack of restrictions is a significant security threat that could be exploited by attackers, indicating that the current policy is permissive. Modifying this policy would involve implementing more stringent controls on what sites can be visited, what applications can be downloaded, and how remote access is granted, moving towards a more controlled and secure environment. This approach contrasts with paranoic, prudent, and promiscuous policies, each of which has its own characteristics and applications in cybersecurity frameworks.

QUESTION 12
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. 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
Explanation:
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.

QUESTION 13
Nervous Nat often sends emails with screenshots of what he thinks are serious incidents, but they always turn out to be false positives. Today, he sends another screenshot, suspecting a nation-state attack. As usual, you go through your list of questions, check your resources for information to determine whether the screenshot shows a real attack, and determine the condition of your network. Which step of IR did you just perform?

A. Recovery
B. Preparation
C. Remediation
D. Detection anc analysis (or identification)

Answer: D
Explanation:
When you receive a screenshot from Nervous Nat and go through a list of questions, check resources for information to determine the nature of the screenshot, and assess the condition of your network, you are engaging in the Detection and Analysis (or Identification) phase of Incident Response (IR). This phase is about identifying potential security incidents based on reported concerns, anomalies detected by security tools, or through the analysis of security alerts. In this scenario, despite the historical context of false positives, each report is treated seriously, requiring you to collect and analyze information to determine whether a real attack is happening. This involves verifying the validity of the incident, assessing its nature, scope, and impact, and deciding on the appropriate next steps. The detection and analysis phase is critical for determining the course of the IR process, including whether escalation is needed and what response measures should be initiated.

QUESTION 14
Which of the following does NOT reduce the success rate of SQL injection?

A. Close unnecessary application services and ports on the server.
B. Automatically lock a user account after a predefined number of invalid login attempts within a predefined interval.
C. Constrain legitimate characters to exclude special characters.
D. Limit the length of the input field.

Answer: A
Explanation:
Reducing the success rate of SQL injection attacks is focused on minimizing vulnerabilities within the application's database interactions, rather than the broader server or network services. SQL injection prevention techniques typically involve input validation, parameterized queries, and the use of stored procedures, rather than changes to the network or server configuration. A) Closing unnecessary application services and ports on the server is a general security best practice to reduce the attack surface but does not directly impact the success rate of SQL injection attacks. This action limits access to potential vulnerabilities across the network and server but doesn't address the specific ways SQL injection exploits input handling within web applications. B) Automatically locking a user account after a predefined number of invalid login attempts within a predefined interval can help mitigate brute force attacks but has no direct effect on preventing SQL injection, which exploits code vulnerabilities to manipulate database queries. C) Constraining legitimate characters to exclude special characters and D) Limiting the length of the input field are both direct methods to reduce the risk of SQL injection. They focus on controlling user input, which is the vector through which SQL injection attacks are launched. By restricting special characters that could be used in SQL commands and limiting input lengths, an application can reduce the potential for malicious input to form a part of SQL queries executed by the backend database.

QUESTION 15
Rica works as an incident handler for an international company. As part of her role, she must review the present security policy implemented. Upon inspection, Rica finds that the policy is wide open, and only known dangerous services/attacks or behaviors are blocked. Which of the following is the current policy that Rica identified?

A. Prudent policy
B. Paranoic policy
C. Permissive policy
D. Promiscuous policy

Answer: C
Explanation:
A permissive security policy is characterized by allowing all activities except those that are explicitly blocked. This approach starts with a default state of allowing access and functionality, with restrictions applied only to known dangerous services, attacks, or behaviors. Such a policy can lead to a wider attack surface because it assumes services and behaviors are safe unless proven otherwise. A prudent policy would typically involve more conservative security measures, applying necessary restrictions to protect against identified and potential threats. A paranoic policy would be at the extreme end of security measures, possibly blocking more than necessary to ensure the highest level of security, often at the expense of usability or functionality. A promiscuous policy, in contrast, would be even more open than a permissive policy, essentially allowing nearly all traffic or actions with minimal restrictions, which is not what Rica observed.

QUESTION 16
An organization's customers are experiencing either slower network communication or unavailability of services. In addition, network administrators are receiving alerts from security tools such as IDS/IPS and firewalls about a possible DoS/DDoS attack. In result, the organization requests the incident handling and response (IH&R) team further investigates the incident. The IH&R team decides to use manual techniques to detect DoS/DDoS attack. Which of the following commands helps the IH&R team to manually detect DoS/DDoS attack?

A. netstat -r
B. nbtstat /c
C. netstat an
D. nbtstat/S

Answer: C
Explanation:
The netstat -an command is used to display network connections, routing tables, and a number of network interface statistics. It is particularly useful for identifying unusual volumes of traffic to and from a system, which can be indicative of a DoS/DDoS attack. The option -a shows all active connections and the TCP and UDP ports on which the computer is listening, and -n displays addresses and port numbers in numerical form. This can help the incident handling and response (IH&R) team to identify suspicious patterns, such as a large number of connections from a single source or to a specific port, which are common during DoS/DDoS attacks.

QUESTION 17
Which of the following is a volatile evidence collecting tool?

A. Netstat
B. HashTool
C. FTK Images
D. ProDiscover Forensics

Answer: A
Explanation:
Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface (and network protocol) statistics. It is considered a volatile evidence collecting tool because it gathers information that exists in the system's memory, which is lost upon shutdown or reboot. This makes it invaluable for collecting evidence of active connections and processes that are present at the time of the incident response but does not persistently store data that can be recovered later. This contrasts with tools like FTK Imager or ProDiscover Forensics, which are used for acquiring digital evidence in a non-volatile manner, such as disk imaging, and HashTool, which is used for validating the integrity of collected digital evidence through hashing.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**