312-50V12$^{\text{Q\&As}}$

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

QUESTION 1

Jim\\'s company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim\\'s company keeps the backup tapes in a safe in the office. Jim\\'s company is audited each year, and the results from this year\\'s audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and transport them in a lock box.

B. Degauss the backup tapes and transport them in a lock box.

C. Hash the backup tapes and transport them in a lock box.

D. Encrypt the backup tapes and use a courier to transport them.

Correct Answer: A

QUESTION 2

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. Nessus

C. OpenVAS

D. tcptraceroute

Correct Answer: A

QUESTION 3

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?

A. Key derivation function

B. Key reinstallation

C. A Public key infrastructure

D. Key stretching

Correct Answer: D

QUESTION 4

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

A. verification

B. Risk assessment

C. Vulnerability scan

D. Remediation

Correct Answer: D

QUESTION 5

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

A. The program is a Trojan; the tearm should regularly update antivirus software and install a reliable firewall

B. The program is spyware; the team should use password managers and encrypt sensitive data

C. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software

D. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups

Correct Answer: C

A keylogger is a type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. Keyloggers are a common tool for cybercriminals, who use them to capture passwords, credit card numbers, personal information, and other sensitive data. Keyloggers can be installed on a device through various methods, such as phishing emails, malicious downloads, or physical access. To confirm the type of program, the security team can use a web search tool, such as Bing, to look for keylogger programs and compare their features and behaviors with the suspicious program they encountered. Alternatively, they can use a malware analysis tool, such as Malwarebytes, to scan and identify the program and its characteristics. To prevent the same attack from occurring in the future, the security team should employ intrusion detection systems (IDS) and regularly update the system software. An IDS is a system that monitors network traffic and system activities for signs of malicious or unauthorized behavior, such as keylogger installation or communication. An IDS can alert the security team of any potential threats and help them respond accordingly. Regularly updating the system software can help patch any vulnerabilities or bugs that keyloggers may exploit to infect the device. Additionally, the security team should also remove the keylogger program from the affected computers and change any compromised passwords or credentials. References: Keylogger | What is a Keylogger? How to protect yourself How to Detect and Remove a Keylogger From Your Computer Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) What is a Keylogger? | Keystroke Logging Definition | Avast Keylogger Software: 11 Best Free to Use in 2023