212-82$^{Q\&As}$

Certified Cybersecurity Technician(C|CT)

Pass EC-COUNCIL 212-82 Exam with 100% Guarantee

QUESTION 1

A software company is developing a new software product by following the best practices for secure application development. Dawson, a software analyst, is checking the performance of the application on the client\\'s network to determine whether end users are facing any issues in accessing the application.

Which of the following tiers of a secure application development lifecycle involves checking the performance of the application?

A. Development

B. Testing

C. Quality assurance (QA)

D. Staging

Correct Answer: B

Explanation: The testing tier of a secure application development lifecycle involves checking the performance of the application on the client\\'s network to determine whether end users are facing any issues in accessing the application. Testing is a crucial phase of software development that ensures the quality, functionality, reliability, and security of the application. Testing can be done manually or automatically using various tools and techniques, such as unit testing, integration testing, system testing, regression testing, performance testing, usability testing, security testing, and acceptance testing

QUESTION 2

A text file containing sensitive information about the organization has been leaked and modified to bring down the reputation of the organization. As a safety measure, the organization did contain the MD5 hash of the original file. The file which has been leaked is retained for examining the integrity. A file named "Sensitiveinfo.txt" along with OriginalFileHash.txt has been stored in a folder named Hash in Documents of Attacker Machine-1. Compare the hash value of the original file with the leaked file and state whether the file has been modified or not by selecting yes or no.

A. No

B. Yes

Correct Answer: B

Explanation: Yes is the answer to whether the file has been modified or not in the above scenario. A hash is a fixed-length string that is generated by applying a mathematical function, called a hash function, to a piece of data, such as a file or a message. A hash can be used to verify the integrity or authenticity of data by comparing it with another hash value of the same data . A hash value is unique and any change in the data will result in a different hash value . To compare the hash value of the original file with the leaked file and state whether the file has been modified or not, one has to follow these steps: Navigate to Hash folder in Documents of Attacker-1 machine. Open OriginalFileHash.txt file with a text editor. Note down the MD5 hash value of the original file as 8f14e45fceea167a5a36dedd4bea2543 Open Command Prompt and change directory to Hash folder using cd command. Type certutil -hashfile Sensitiveinfo.txt MD5 and press Enter key to generate MD5 hash value of leaked file. Note down the MD5 hash value of leaked file as 9f14e45fceea167a5a36dedd4bea2543 Compare both MD5 hash values. The MD5 hash values are different , which means that the file has been modified.

QUESTION 3

Nicolas, a computer science student, decided to create a guest OS on his laptop for different lab operations. He adopted a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS.

Which of the following virtualization approaches has Nicolas adopted in the above scenario?

A. Hardware-assisted virtualization

B. Full virtualization

C. Hybrid virtualization

D. OS-assisted virtualization

Correct Answer: A

Explanation: Hardware-assisted virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment. The virtual machine manager (VMM) will directly interact with the computer hardware, translate commands to binary instructions, and forward them to the host OS. Hardware-assisted virtualization relies on special hardware features in the CPU and chipset to create and manage virtual machines efficiently and securely34. Full virtualization is a virtualization approach in which the guest OS will not be aware that it is running in a virtualized environment, but the VMM will run in software and emulate all the hardware resources for each virtual machine5. Hybrid virtualization is a virtualization approach that combines hardware-assisted and full virtualization techniques to optimize performance and compatibility6. OS-assisted virtualization is a virtualization approach in which the guest OS will be modified to run in a virtualized environment and cooperate with the VMM to access the hardware resources

QUESTION 4

An organization hired a network operations center (NOC) team to protect its IT infrastructure from external attacks. The organization utilized a type of threat intelligence to protect its resources from evolving threats. The threat intelligence helped the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors.

Identify the type of threat intelligence consumed by the organization in the above scenario.

A. Operational threat intelligence

B. Strategic threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Correct Answer: C

Explanation: Technical threat intelligence is a type of threat intelligence that provides information about the technical details of specific attacks, such as indicators of compromise (IOCs), malware signatures, attack vectors, and vulnerabilities. Technical threat intelligence helps the NOC team understand how attackers are expected to perform an attack on the organization, identify the information leakage, and determine the attack goals as well as attack vectors. Technical threat intelligence is often consumed by security analysts, incident responders, and penetration testers who need to analyze and respond to active or potential threats.

QUESTION 5

As a cybersecurity technician, you were assigned to analyze the file system of a Linux image captured from a device that has been attacked recently. Study the forensic image \\'Evidenced.img" in the Documents folder of the "Attacker Machine-1" and identify a user from the image file.

A. smith

B. attacker

C. roger

D. john

Correct Answer: B

Explanation: The attacker is a user from the image file in the above scenario. A file system is a method or structure that organizes and stores files and data on a storage device, such as a hard disk, a flash drive, etc. A file system can have

different types based on its format or features, such as FAT, NTFS, ext4, etc. A file system can be analyzed to extract various information, such as file names, sizes, dates, contents, etc. A Linux image is an image file that contains a copy or a

snapshot of a Linux-based file system . A Linux image can be analyzed to extract various information about a Linux-based system or device . To analyze the file system of a Linux image captured from a device that has been attacked recently

and identify a user from the image file, one has to follow these steps:

Navigate to Documents folder of Attacker Machine-1. Right-click on Evidenced.img file and select Mount option. Wait for the image file to be mounted and assigned a drive letter. Open File Explorer and navigate to the mounted drive. Open

etc folder and open passwd file with a text editor.

Observe the user accounts listed in the file.

The user accounts listed in the file are:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/

var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:

systemd-network:x: systemd-resolve:x: systemd-bus-proxy:x: syslog:x: _apt:x:

messagebus:x: uuidd:x: lightdm:x: whoopsie:x: avahi-autoipd:x: avahi:x: dnsmasq:x:

colord:x: speech-dispatcher:x: hplip:x: kernoops:x: saned:x: nm-openvpn:x: nm- openconnect:x: pulse:x: rtkit:x: sshd:x: attacker::1000 The user account that is not a system or service account is attacker, which is a user from the image file.