Free Questions for 212-82 by vceexamstest

Shared by Walter on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Martin, a network administrator at an organization, received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. In which of the following threat-modeling steps did Martin evaluate the severity level of the threat?

Options:

A- Identify vulnerabilities

B- Application overview

C- Risk and impact analysis

D- Decompose the application

Answer:

C

Explanation:

Risk and impact analysis is the threat-modeling step in which Martin evaluated the severity level of the threat in the above scenario. Threat modeling is a process that involves identifying, analyzing, and mitigating threats and risks to a system or network. Threat modeling can be used to improve the security and resilience of a system or network by applying various methods or techniques, such as STRIDE, DREAD, PASTA, etc. Threat modeling consists of various steps or phases that perform different tasks or roles. Risk and impact analysis is a threat-modeling step that involves assessing the likelihood and consequences of threats and risks to a system or network . Risk and impact analysis can be used to evaluate the severity level of threats and risks and prioritize them for mitigation . In the scenario, Martin received breaching alerts for an application. He identified that a vulnerability in the application allowed attackers to enter malicious input. Martin evaluated the threat severity and extent of damage that could be caused by this vulnerability. He then escalated the issue to the security management team to determine appropriate mitigation strategies. This means that he performed risk and impact analysis for this purpose. Identify vulnerabilities is a threat-modeling step that involves finding and documenting the weaknesses or flaws in a system or network that can be exploited by threats or risks . Application overview is a threat-modeling step that involves defining and understanding the scope, architecture, components, and functionality of a system or network . Decompose the application is a threat-modeling step that involves breaking down a system or network into smaller and simpler elements, such as data flows, processes, assets, etc.

Question 2

Question Type: MultipleChoice

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. (Practical Question)

Options:

A- smith

B- attacker

C- roger

D- john

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.

Question 3

Question Type: MultipleChoice

in a security incident, the forensic investigation has isolated a suspicious file named "security_update.exe". You are asked to analyze the file in the Documents folder of the "Attacker Machine-1" to determine whether it is malicious. Analyze the suspicious file and identify the malware signature. (Practical Question)

Options:

A- Stuxnet

B- KLEZ

C- ZEUS

D- Conficker

Answer:

A

Explanation:

Stuxnet is the malware signature of the suspicious file in the above scenario. Malware is malicious software that can harm or compromise the security or functionality of a system or network. Malware can include various types, such as viruses, worms, trojans, ransomware, spyware, etc. Malware signature is a unique pattern or characteristic that identifies a specific malware or malware family.

Malware signature can be used to detect or analyze malware by comparing it with known malware signatures in databases or repositories. To analyze the suspicious file and identify the malware signature, one has to follow these steps:

Navigate to Documents folder of Attacker Machine-1.

Right-click on security_update.exe file and select Scan with VirusTotal option.

Wait for VirusTotal to scan the file and display the results.

Observe the detection ratio and details.

The detection ratio is 59/70, which means that 59 out of 70 antivirus engines detected the file as malicious. The details show that most antivirus engines detected the file as Stuxnet, which is a malware signature of a worm that targets industrial control systems (ICS). Stuxnet can be used to sabotage or damage ICS by modifying their code or behavior. Therefore, Stuxnet is the malware signature of the suspicious file. KLEZ is a malware signature of a worm that spreads via email and network shares. KLEZ can be used to infect or overwrite files, disable antivirus software, or display fake messages. ZEUS is a malware signature of a trojan that targets banking and financial systems. ZEUS can be used to steal or modify banking credentials, perform fraudulent transactions, or install other malware. Conficker is a malware signature of a worm that exploits a vulnerability in Windows operating systems. Conficker can be used to create a botnet, disable security services, or download other malware

Question 4

Question Type: MultipleChoice

Alex, a certified security professional, works for both aggressor and defender teams. His team's main responsibility involves enhancing protection and boosting the security standards of the organization. Identify Alex's team in this scenario.

Options:

A- White team

B- Purple learn

C- Blue team

D- Red team

Answer:

B

Explanation:

Purple team is the team that Alex works for in this scenario. A team is a group of people that work together to achieve a common goal or objective. A team can have different types based on its role or function in an organization or a project. A purple team is a type of team that works for both aggressor and defender teams. A purple team can be used to enhance protection and boost the security standards of an organization by performing various tasks, such as testing, evaluating, improving, or integrating the security measures implemented by the defender team or exploited by the aggressor team. In the scenario, Alex is a certified security professional who works for both aggressor and defender teams. His team's main responsibility involves enhancing protection and boosting the security standards of the

organization. This means that he works for a purple team. A white team is a type of team that acts as an observer or an arbitrator between the aggressor and defender teams. A white team can be used to monitor, evaluate, or adjudicate the performance or outcome of the aggressor and defender teams by providing feedback, guidance, or rules. A blue team is a type of team that acts as a defender or a protector of an organization's network or system. A blue team can be used to prevent, detect, or respond to attacks from external or internal threats by implementing various security measures, such as firewalls, antivirus, encryption, etc. A red team is a type of team that acts as an attacker or an adversary of an organization's network or system. A red team can be used to simulate realistic attacks from external or internal threats by exploiting various vulnerabilities, weaknesses, or gaps in the organization's security posture.

Question 5

Question Type: **MultipleChoice**

Camden, a network specialist in an organization, monitored the behavior of the organizational network using SIFM from a control room. The SIEM detected suspicious activity and sent an alert to the camer

a. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers.

Which of the following SIEM functions allowed Camden to view suspicious behavior and make correct decisions during a security incident?

Options:

A- Application log monitoring

B- Log Retention

C- Dashboard

D- Data aggregation

Answer:

C

Explanation:

Dashboard is the SIEM function that allowed Camden to view suspicious behavior and make correct decisions during a security incident. SIEM (Security Information and Event Management) is a system or software that collects, analyzes, and correlates security data from various sources, such as logs, alerts, events, etc., and provides a centralized view and management of the security posture of a network or system. SIEM can be used to detect, prevent, or respond to security incidents or threats. SIEM consists of various functions or components that perform different tasks or roles. Dashboard is a SIEM function that provides a graphical user interface (GUI) that displays various security metrics, indicators, alerts, reports, etc., in an organized and interactive manner. Dashboard can be used to view suspicious behavior and make correct decisions during a security incident. In the scenario, Camden monitored the behavior of the organizational network using SIEM from a control room. The SIEM detected suspicious activity and sent an alert to Camden. Based on the severity of the incident displayed on the screen, Camden made the correct decision and immediately launched defensive actions to prevent further exploitation by attackers. This means that he used the dashboard function of SIEM for this purpose. Application log monitoring is a SIEM function that collects and analyzes application logs, which are records of events or activities that occur within an

application or software. Log retention is an SIEM function that stores and preserves logs for a certain period of time or indefinitely for future reference or analysis. Data aggregation is an SIEM function that combines and normalizes data from different sources into a common format or structure.

Question 6

Question Type: MultipleChoice

Elliott, a security professional, was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network, Elliott monitored the firewall logs to

detect evolving threats And attacks; this helped in ensuring firewall security and addressing network issues beforehand.

in which of the following phases of firewall implementation and deployment did Elliott monitor the firewall logs?

Options:

A- Deploying

B- Managing and maintaining

C- Testing

D- Configuring

Answer:

B

Explanation:

Managing and maintaining is the phase of firewall implementation and deployment in which Elliott monitored the firewall logs in the above scenario. A firewall is a system or device that controls and filters the incoming and outgoing traffic between different networks or systems based on predefined rules or policies. A firewall can be used to protect a network or system from unauthorized access, use, disclosure, modification, or destruction . Firewall implementation and deployment is a process that involves planning, installing, configuring, testing, managing, and maintaining firewalls in a network or system . Managing and maintaining is the phase of firewall implementation and deployment that involves monitoring and reviewing the performance and effectiveness of firewalls over time . Managing and maintaining can include tasks such as updating firewall rules or policies, analyzing firewall logs , detecting evolving threats or attacks , ensuring firewall security , addressing network issues , etc. In the scenario, Elliott was tasked with implementing and deploying firewalls in the corporate network of an organization. After planning and deploying firewalls in the network, Elliott monitored the firewall logs to detect evolving threats and attacks; this helped in ensuring firewall security and addressing network issues beforehand. This means that he performed managing and maintaining phase for this purpose. Deploying is the phase of firewall implementation and deployment that involves installing and activating firewalls in the network or system according to the plan. Testing is the phase of firewall implementation and deployment that involves verifying and validating the functionality and security of firewalls before putting them into operation. Configuring is the phase of firewall implementation and deployment that involves setting up and customizing firewalls according to the requirements and specifications.

Question 7

Question Type: MultipleChoice

Elliott, a security professional, was appointed to test a newly developed application deployed over an organizational network using a Bastion host. Elliott initiated the process by configuring the nonreusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. identify the type of bastion host configured by Elliott in the above scenario.

Options:

A- External services hosts

B- Victim machines

C- One-box firewalls

D- Non-routing dual-homed hosts

Answer:

D

Explanation:

Non-routing dual-homed hosts are the type of bastion hosts configured by Elliott in the above scenario. A bastion host is a system or device that is exposed to the public internet and acts as a gateway or a proxy for other systems or networks behind it. A bastion host can be used to provide an additional layer of security and protection for internal systems or networks from external threats and attacks . A bastion host can have different types based on its configuration or functionality. A non-routing dual-homed host is a type of bastion host that has two network interfaces: one connected to the public internet and one connected to the internal network. A non-routing dual-homed host does not allow any direct communication between the two networks and only allows specific services or applications to pass through it . A non-routing dual-homed host can be used to isolate and secure internal systems or networks from external access . In the scenario, Elliott was appointed to test a newly developed application deployed over an organizational network using a bastion host. Elliott initiated the process by configuring the non-reusable bastion host. He then tested the newly developed application to identify the presence of security flaws that were not yet known; further, he executed services that were not secure. This means that he configured a non-routing dual-homed host for this purpose. An external services host is a type of bastion host that provides external services, such as web, email, FTP, etc., to the public internet while protecting internal systems or networks from direct access . A victim machine is not a type of bastion host, but a term that describes a system or device that has been compromised or infected by an attacker or malware . A one-box firewall is not a type of bastion host, but a term that describes a firewall that performs both packet filtering and application proxy functions in one device .

Question 8

Question Type: MultipleChoice

Juan, a safety officer at an organization, installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and Access any floor. Which of the following

types of physical locks did Juan install In this scenario?

Options:

A- Mechanical locks

B- Digital locks

C- Combination locks

D- Electromagnetic locks

Answer:

B

Explanation:

Digital locks are the types of physical locks that Juan installed in this scenario. A physical lock is a device that prevents or restricts access to a physical location or environment, such as a door, a cabinet, a drawer, etc. A physical lock can have different types based on its mechanism or technology. A digital lock is a type of physical lock that uses electronic or digital components, such as a keypad, a card reader, a fingerprint scanner, etc., to unlock or lock . A digital lock can be used to provide enhanced security and convenience to users, but it can also be vulnerable to hacking or tampering. In the scenario, Juan installed a physical lock at the entrance of each floor. All employees in the organization were allotted a smart card embedded in their ID cards, which had to be swiped to unlock doors and access any floor. This means that he installed digital locks for those doors. A mechanical lock is a type of physical lock that uses mechanical components, such as a key, a bolt, a latch, etc., to unlock or lock. A combination lock is a type of physical lock that uses a

sequence of numbers or symbols, such as a dial, a wheel, or a keypad, to unlock or lock. An electromagnetic lock is a type of physical lock that uses an electromagnet and an armature plate to unlock or lock.

To Get Premium Files for 212-82 Visit

https://www.p2pexams.com/products/212-82

For More Free Questions Visit

https://www.p2pexams.com/eccouncil/pdf/212-82