

# EC-Council

## Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)



#### NEW QUESTION 1

Maisie, a new employee at an organization, was given an access badge with access to only the first and third floors of the organizational premises. Maisie tried scanning her access badge against the badge reader at the second-floor entrance but was unsuccessful. Identify the short-range wireless communication technology used by the organization in this scenario.

- A. RFID
- B. Li-Fi
- C. Bluetooth
- D. Wi-Fi

**Answer:** A

#### Explanation:

RFID (Radio Frequency Identification) is a short-range wireless communication technology that uses radio waves to identify and track objects. RFID tags are attached to objects and RFID readers scan the tags to obtain the information stored in them. RFID is commonly used for access control, inventory management, and identification. References: What is RFID?

#### NEW QUESTION 2

Anderson, a security engineer, was instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.

Identify the type of attack signature analysis performed by Anderson in the above scenario.

- A. Context-based signature analysis
- B. Atomic-signature-based analysis
- C. Composite-signature-based analysis
- D. Content-based signature analysis

**Answer:** D

#### Explanation:

Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities. Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

#### NEW QUESTION 3

Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.

Identify the type of event logs analyzed by Tenda in the above scenario.

- A. Application event log
- B. Setup event log
- C. Security event log
- D. System event log

**Answer:** C

#### Explanation:

Security event log is the type of event log analyzed by Tenda in the above scenario. Windows Event Viewer is a tool that displays logged data about various events that occur on a Windows system or network. Windows Event Viewer categorizes event logs into different types based on their source and purpose. Security event log is the type of event log that records events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies. Security event log can help identify attempted or successful unauthorized activities on a Windows system or network. Application event log is the type of event log that records events related to applications running on a Windows system, such as errors, warnings, or information messages. Setup event log is the type of event log that records events related to the installation or removal of software or hardware components on a Windows system. System event log is the type of event log that records events related to the operation of a Windows system or its components, such as drivers, services, processes, etc.

#### NEW QUESTION 4

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

**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 8f14e45fceeaa167a5a36dedd4bea2543
  - ? 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 9f14e45fceeaa167a5a36dedd4bea2543
  - ? Compare both MD5 hash values.
- The MD5 hash values are different , which means that the file has been modified.

#### NEW QUESTION 5

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Quid pro quo
- B. Diversion theft
- C. Elicitation
- D. Phishing

**Answer:** A

#### Explanation:

Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Quid pro quo is a social engineering method that involves offering a service or a benefit in exchange for information or access. Quid pro quo can be used to trick victims into believing that they are receiving help or assistance from a legitimate source, while in fact they are compromising their security or privacy. In the scenario, Johnson performed quid pro quo by claiming himself to represent a technical support team from a vendor and offering to help sibertech.org with a server issue, while in fact he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. If you want to learn more about social engineering techniques, you can check out these resources:

? [1] A guide to different types of social engineering attacks and how to prevent

them: [<https://www.csoonline.com/article/2124681/what-is-social-engineering.html>]

? [2] A video that explains how quid pro quo works and how to avoid falling for it: [<https://www.youtube.com/watch?v=3Yy0gZ9xw8g>]

? [3] A quiz that tests your knowledge of social engineering techniques and scenarios: [<https://www.proprofs.com/quiz-school/story.php?title=social-engineering-quiz>]

#### NEW QUESTION 6

Myles, a security professional at an organization, provided laptops for all the employees to carry out the business processes from remote locations. While installing necessary applications required for the business, Myles has also installed antivirus software on each laptop following the company's policy to detect and protect the machines from external malicious events over the Internet.

Identify the PCI-DSS requirement followed by Myles in the above scenario.

- A. PCI-DSS requirement no 1.3.2
- B. PCI-DSS requirement no 1.3.5
- C. PCI-DSS requirement no 5.1
- D. PCI-DSS requirement no 1.3.1

**Answer:** C

#### Explanation:

The correct answer is C, as it identifies the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS is a set of standards that aims to protect cardholder data and ensure secure payment transactions. PCI-DSS has 12 requirements that cover various aspects of security such as network configuration, data encryption, access control, vulnerability management, monitoring, and testing. PCI-DSS requirement no 5.1 states that "Protect all systems against malware and regularly update anti-virus software or programs". In the above scenario, Myles followed this requirement by installing antivirus software on each laptop to detect and protect the machines from external malicious events over the Internet. Option A is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.2 states that "Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet". In the above scenario, Myles did not follow this requirement, as there was no mention of outbound traffic or cardholder data environment. Option B is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.5 states that "Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment". In the above scenario, Myles did not follow this requirement, as there was no mention of inbound or outbound traffic or cardholder data environment. Option D is incorrect, as it does not identify the PCI-DSS requirement followed by Myles in the above scenario. PCI-DSS requirement no 1.3.1 states that "Implement a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data". In the above scenario, Myles did not follow this requirement, as there was no mention of firewall configuration or publicly accessible servers or system components storing cardholder data.

References: Section 5.2

#### NEW QUESTION 7

The incident handling and response (IH&R) team of an organization was handling a recent cyberattack on the organization's web server. Fernando, a member of the IH&P team, was tasked with eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. For this purpose, Fernando applied the latest patches to the web server and installed the latest security mechanisms on it. Identify the IH&R step performed by Fernando in this scenario.

- A. Notification
- B. Containment
- C. Recovery
- D. Eradication

**Answer:** D

#### Explanation:

Eradiation is the IH&R step performed by Fernando in this scenario. Eradication is a step in IH&R that involves eliminating the root cause of the incident and closing all attack vectors to prevent similar incidents in future. Eradication can include applying patches, installing security mechanisms, removing malware,

restoring backups, or reformatting systems.  
References: [Eradication Step in IH&R]

#### NEW QUESTION 8

Cairo, an incident responder, was handling an incident observed in an organizational network. After performing all IH&R steps, Cairo initiated post-incident activities. He determined all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Identify the post-incident activity performed by Cairo in this scenario.

- A. Incident impact assessment
- B. Close the investigation
- C. Review and revise policies
- D. Incident disclosure

**Answer:** A

#### Explanation:

Incident impact assessment is the post-incident activity performed by Cairo in this scenario. Incident impact assessment is a post-incident activity that involves determining all types of losses caused by the incident by identifying and evaluating all affected devices, networks, applications, and software. Incident impact assessment can include measuring financial losses, reputational damages, operational disruptions, legal liabilities, or regulatory penalties<sup>1</sup>. References: Incident Impact Assessment

#### NEW QUESTION 9

Finley, a security professional at an organization, was tasked with monitoring the organizational network behavior through the SIEM dashboard. While monitoring, Finley noticed suspicious activities in the network; thus, he captured and analyzed a single network packet to determine whether the signature included malicious patterns. Identify the attack signature analysis technique employed by Finley in this scenario.

- A. Context-based signature analysis
- B. Atomic-signature-based analysis
- C. Composite signature-based analysis
- D. Content-based signature analysis

**Answer:** D

#### Explanation:

Content-based signature analysis is the attack signature analysis technique employed by Finley in this scenario. Content-based signature analysis is a technique that captures and analyzes a single network packet to determine whether the signature included malicious patterns. Content-based signature analysis can be used to detect known attacks, such as buffer overflows, SQL injections, or cross-site scripting<sup>2</sup>. References: Content-Based Signature Analysis

#### NEW QUESTION 10

Gideon, a forensic officer, was examining a victim's Linux system suspected to be involved in online criminal activities. Gideon navigated to a directory containing a log file that recorded information related to user login/logout. This information helped Gideon to determine the current login state of cyber criminals in the victim system, identify the Linux log file accessed by Gideon in this scenario.

- A. /var/rlog/mysql
- B. log
- C. /var/rlog/wtmp
- D. /ar/log/boot.iog
- E. /var/log/httpd/

**Answer:** B

#### Explanation:

/var/log/wtmp is the Linux log file accessed by Gideon in this scenario.

/var/log/wtmp is a log file that records information related to user login/logout, such as username, terminal, IP address, and login time. /var/log/wtmp can be used to determine the current login state of users in a Linux system. /var/log/wtmp can be viewed using commands such as last, lastb, or utmpdump<sup>1</sup>. References: Linux Log Files

#### NEW QUESTION 10

Tristan, a professional penetration tester, was recruited by an organization to test its network infrastructure. The organization wanted to understand its current security posture and its strength in defending against external threats. For this purpose, the organization did not provide any information about their IT infrastructure to Tristan. Thus, Tristan initiated zero-knowledge attacks, with no information or assistance from the organization.

Which of the following types of penetration testing has Tristan initiated in the above scenario?

- A. Black-box testing
- B. White-box testing
- C. Gray-box testing
- D. Translucent-box testing

**Answer:** A

#### Explanation:

Black-box testing is a type of penetration testing where the tester has no prior knowledge of the target system or network and initiates zero-knowledge attacks, with no information or assistance from the organization. Black-box testing simulates the perspective of an external attacker who tries to find and exploit vulnerabilities without any insider information. Black-box testing can help identify unknown or hidden vulnerabilities that may not be detected by other types of testing. However, black-box testing can also be time-consuming, costly, and incomplete, as it depends on the tester's skills and tools.

#### NEW QUESTION 15

RAT has been setup in one of the machines connected to the network to steal the important Sensitive corporate docs located on Desktop of the server, further

investigation revealed the IP address of the server 20.20.10.26. Initiate a remote connection using thief client and determine the number of files present in the folder.

Hint: Thief folder is located at: Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.

- A. 2
- B. 4
- C. 3
- D. 5

**Answer: C**

**Explanation:**

3 is the number of files present in the folder in the above scenario. A RAT (Remote Access Trojan) is a type of malware that allows an attacker to remotely access and control a compromised system or network. A RAT can be used to steal sensitive data, spy on user activity, execute commands, install other malware, etc. To initiate a remote connection using thief client, one has to follow these steps:

- ? Navigate to the thief folder located at Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Thief of Attacker Machine-1.
- ? Double-click on thief.exe file to launch thief client.
- ? Enter 20.20.10.26 as IP address of server.
- ? Enter 1234 as port number.
- ? Click on Connect button.
- ? After establishing connection with server, click on Browse button.
- ? Navigate to Desktop folder on server.
- ? Count number of files present in folder. The number of files present in folder is 3, which are:
  - ? Sensitive corporate docs.docx
  - ? Sensitive corporate docs.pdf
  - ? Sensitive corporate docs.txt

**NEW QUESTION 16**

Hayes, a security professional, was tasked with the implementation of security controls for an industrial network at the Purdue level 3.5 (IDMZ). Hayes verified all the possible attack vectors on the IDMZ level and deployed a security control that fortifies the IDMZ against cyber-attacks. Identify the security control implemented by Hayes in the above scenario.

- A. Point-to-point communication
- B. MAC authentication
- C. Anti-DoS solution
- D. Use of authorized RTU and PLC commands

**Answer: D**

**Explanation:**

The use of authorized RTU and PLC commands is the security control implemented by Hayes in the above scenario. RTU (Remote Terminal Unit) and PLC (Programmable Logic Controller) are devices that control and monitor industrial processes, such as power generation, water treatment, oil and gas production, etc. RTU and PLC commands are instructions that are sent from a master station to a slave station to perform certain actions or request certain data. The use of authorized RTU and PLC commands is a security control that fortifies the IDMZ (Industrial Demilitarized Zone) against cyber-attacks by ensuring that only valid and authenticated commands are executed by the RTU and PLC devices. Point-to-point communication is a communication method that establishes a direct connection between two endpoints. MAC authentication is an authentication method that verifies the MAC (Media Access Control) address of a device before granting access to a network. Anti-DoS solution is a security solution that protects a network from DoS (Denial-of-Service) attacks by filtering or blocking malicious traffic.

**NEW QUESTION 18**

Arabella, a forensic officer, documented all the evidence related to the case in a standard forensic investigation report template. She filled different sections of the report covering all the details of the crime along with the daily progress of the investigation process.

In which of the following sections of the forensic investigation report did Arabella record the "nature of the claim and information provided to the officers"?

- A. Investigation process
- B. Investigation objectives
- C. Evidence information
- D. Evaluation and analysis process

**Answer: B**

**Explanation:**

Investigation objectives is the section of the forensic investigation report where Arabella recorded the "nature of the claim and information provided to the officers" in the above scenario. A forensic investigation report is a document that summarizes the findings and conclusions of a forensic investigation. A forensic investigation report typically follows a standard template that contains different sections covering all the details of the crime and the investigation process. Investigation objectives is the section of the forensic investigation report that describes the purpose and scope of the investigation, the nature of the claim and information provided to the officers, and the questions or issues to be addressed by the investigation. Investigation process is the section of the forensic investigation report that describes the steps and methods followed by the investigators, such as evidence collection, preservation, analysis, etc. Evidence information is the section of the forensic investigation report that lists and describes the evidence obtained from various sources, such as devices, media, witnesses, etc. Evaluation and analysis process is the section of the forensic investigation report that explains how the evidence was evaluated and analyzed using various tools and techniques, such as software, hardware, etc.

**NEW QUESTION 22**

Richard, a professional hacker, was hired by a marketer to gather sensitive data and information about the offline activities of users from location data. Richard employed a technique to determine the proximity of a user's mobile device to an exact location using CPS features. Using this technique, Richard placed a virtual barrier positioned at a static location to interact with mobile users crossing the barrier, identify the technique employed by Richard in this scenario.

- A. Containerization

- B. Over-the-air (OTA) updates
- C. Full device encryption
- D. Geofencing

**Answer:** D

**Explanation:**

Geofencing is a technique that uses GPS features to determine the proximity of a user's mobile device to an exact location. Geofencing can be used to create a virtual barrier positioned at a static location to interact with mobile users crossing the barrier. Geofencing can be used for marketing, security, and tracking purposes.

References: What is Geofencing?

**NEW QUESTION 25**

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?

- 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.

**NEW QUESTION 26**

Kayden successfully cracked the final round of interviews at an organization. After a few days, he received his offer letter through an official company email address. The email stated that the selected candidate should respond within a specified time. Kayden accepted the opportunity and provided an e-signature on the offer letter, then replied to the same email address. The company validated the e-signature and added his details to their database. Here, Kayden could not deny the company's message, and the company could not deny Kayden's signature.

Which of the following information security elements was described in the above scenario?

- A. Availability
- B. Non-repudiation
- C. Integrity
- D. Confidentiality

**Answer:** B

**Explanation:**

The correct answer is B, as it describes the information security element that was described in the above scenario. Non-repudiation is an information security element that ensures that a party cannot deny sending or receiving a message or performing an action. In the above scenario, non-repudiation was described, as Kayden could not deny company's message, and company could not deny Kayden's signature. Option A is incorrect, as it does not describe the information security element that was described in the above scenario. Availability is an information security element that ensures that authorized users can access and use information and resources when needed. In the above scenario, availability was not described, as there was no mention of access or use of information and resources. Option C is incorrect, as it does not describe the information security element that was described in the above scenario. Integrity is an information security element that ensures that information and resources are accurate and complete and have not been modified by unauthorized parties. In the above scenario, integrity was not described, as there was no mention of accuracy or completeness of information and resources. Option D is incorrect, as it does not describe the information security element that was described in the above scenario. Confidentiality is an information security element that ensures that information and resources are protected from unauthorized access and disclosure. In the above scenario, confidentiality was not described, as there was no mention of protection or disclosure of information and resources.

References: , Section 3.1

**NEW QUESTION 30**

Wilson, a security specialist in an organization, was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. Identify the method used by Wilson to achieve cloud network security in this scenario.

- A. Virtual private cloud (VPC)
- B. Public and private subnets
- C. Transit gateways
- D. VPC endpoint

**Answer:** C

**Explanation:**

Transit gateways are the method used by Wilson to achieve cloud network security in this scenario. Cloud network security is a branch of cybersecurity that

focuses on protecting and securing the network infrastructure and traffic in a cloud environment. Cloud network security can involve various methods or techniques, such as encryption, firewall, VPN, IDS/IPS, etc. Transit gateways are a method of cloud network security that provide a network routing solution that establishes and manages communication between on-premises consumer networks and VPCs (Virtual Private Clouds) via a centralized unit. Transit gateways can be used to simplify and secure the connectivity between different networks or VPCs in a cloud environment. In the scenario, Wilson was instructed to enhance its cloud network security. To achieve this, Wilson deployed a network routing solution that established and managed communication between the on-premises consumer network and VPCs via a centralized unit. This means that he used transit gateways for this purpose. A virtual private cloud (VPC) is not a method of cloud network security, but a term that describes an isolated and private section of a public cloud that provides exclusive access to cloud resources to a single organization or entity. A VPC can be used to create and configure virtual networks in a cloud environment. Public and private subnets are not methods of cloud network security, but terms that describe segments of a VPC that have different levels of accessibility or visibility. A public subnet is a segment of a VPC that can be accessed from the internet or other networks. A private subnet is a segment of a VPC that cannot be accessed from the internet or other networks. A VPC endpoint is not a method of cloud network security, but a term that describes an interface that allows private connectivity between a VPC and other AWS (Amazon Web Services) services or resources.

#### NEW QUESTION 35

An FTP server has been hosted in one of the machines in the network. Using Cain and Abel the attacker was able to poison the machine and fetch the FTP credentials used by the admin. You're given a task to validate the credentials that were stolen using Cain and Abel and read the file flag.txt

- A. white@hat
- B. red@hat
- C. hat@red
- D. blue@hat

**Answer:** C

#### Explanation:

hat@red is the FTP credential that was stolen using Cain and Abel in the above scenario. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. FTP requires a username and a password to authenticate the client and grant access to the server. Cain and Abel is a tool that can perform various network attacks, such as ARP poisoning, password cracking, sniffing, etc. Cain and Abel can poison the machine and fetch the FTP credentials used by the admin by intercepting and analyzing the network traffic. To validate the credentials that were stolen using Cain and Abel and read the file flag.txt, one has to follow these steps:

- ? Navigate to the Documents folder of Attacker-1 machine.
- ? Double-click on Cain.exe file to launch Cain and Abel tool.
- ? Click on Sniffer tab.
- ? Click on Start/Stop Sniffer icon.
- ? Click on Configure icon.
- ? Select the network adapter and click on OK button.
- ? Click on + icon to add hosts to scan.
- ? Select All hosts in my subnet option and click on OK button.
- ? Wait for the hosts to appear in the list.
- ? Right-click on 20.20.10.26 (FTP server) and select Resolve Host Name option.
- ? Note down the host name as ftpserver.movieabc.com
- ? Click on Passwords tab.
- ? Click on + icon to add items to list.
- ? Select Network Passwords option.
- ? Select FTP option from Protocol drop-down list.
- ? Click on OK button.
- ? Wait for the FTP credentials to appear in the list.
- ? Note down the username as hat and the password as red
- ? Open a web browser and type ftp://hat:red@ftpserver.movieabc.com
- ? Press Enter key to access the FTP server using the stolen credentials.
- ? Navigate to flag.txt file and open it.
- ? Read the file content.

#### NEW QUESTION 36

Jordan, a network administrator in an organization, was instructed to identify network-related issues and improve network performance. While troubleshooting the network, he received a message indicating that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host, which of the following network issues did Jordan find in this scenario?

- A. Time exceeded message
- B. Destination unreachable message
- C. Unreachable networks
- D. Network cable is unplugged

**Answer:** B

#### Explanation:

Destination unreachable message is the network issue that Jordan found in this scenario. Destination unreachable message is a type of ICMP message that indicates that the datagram could not be forwarded owing to the unavailability of IP-related services (such as FTP or web services) on the target host. Destination unreachable message can be caused by various reasons, such as incorrect routing, firewall blocking, or host configuration problems<sup>1</sup>.

References: Destination Unreachable Message

#### NEW QUESTION 38

Karter, a security professional, deployed a honeypot on the organization's network for luring attackers who attempt to breach the network. For this purpose, he configured a type of honeypot that simulates a real OS as well as the applications and services of a target network. Furthermore, the honeypot deployed by Karter only responds to pre-configured commands.

Identify the type of Honeypot deployed by Karter in the above scenario.

- A. Low-interaction honeypot
- B. Pure honeypot
- C. Medium-interaction honeypot

D. High-interaction honeypot

**Answer:** A

**Explanation:**

A low-interaction honeypot is a type of honeypot that simulates a real OS as well as the applications and services of a target network, but only responds to pre-configured commands. It is designed to capture basic information about the attacker, such as their IP address, tools, and techniques. A low-interaction honeypot is easier to deploy and maintain than a high-interaction honeypot, which fully emulates a real system and allows the attacker to interact with it. A pure honeypot is a real system that is intentionally vulnerable and exposed to attackers. A medium-interaction honeypot is a type of honeypot that offers more functionality and interactivity than a low-interaction honeypot, but less than a high-interaction honeypot.

**NEW QUESTION 40**

Richards, a security specialist at an organization, was monitoring an IDS system. While monitoring, he suddenly received an alert of an ongoing intrusion attempt on the organization's network. He immediately averted the malicious actions by implementing the necessary measures. Identify the type of alert generated by the IDS system in the above scenario.

- A. True positive
- B. True negative
- C. False negative
- D. False positive

**Answer:** A

**Explanation:**

A true positive alert is generated by an IDS system when it correctly identifies an ongoing intrusion attempt on the network and sends an alert to the security professional. This is the desired outcome of an IDS system, as it indicates that the system is working effectively and accurately

**NEW QUESTION 44**

Kaison, a forensic officer, was investigating a compromised system used for various online attacks. Kaison initiated the data acquisition process and extracted the data from the systems DVD-ROM. Which of the following types of data did Kaison acquire in the above scenario?

- A. Archival media
- B. Kernel statistics
- C. ARP cache
- D. Processor cache

**Answer:** A

**Explanation:**

Archival media is the type of data that Kaison acquired in the above scenario. Archival media is a type of data that is stored on removable media such as DVD-ROMs, CD-ROMs, tapes, or flash drives. Archival media can be used to backup or transfer data from one system to another. Archival media can be acquired using forensic tools that can read and copy the data from the media. References: Archival Media

**NEW QUESTION 48**

An attacker with malicious intent used SYN flooding technique to disrupt the network and gain advantage over the network to bypass the Firewall. You are working with a security architect to design security standards and plan for your organization. The network traffic was captured by the SOC team and was provided to you to perform a detailed analysis. Study the Synflood.pcapng file and determine the source IP address.

Note: Synflood.pcapng file is present in the Documents folder of Attacker-1 machine.

- A. 20.20.10.180
- B. 20.20.10.19
- C. 20.20.10.60
- D. 20.20.10.59

**Answer:** B

**Explanation:**

20.20.10.19 is the source IP address of the SYN flooding attack in the above scenario. SYN flooding is a type of denial-of-service (DoS) attack that exploits the TCP (Transmission Control Protocol) three-way handshake process to disrupt the network and gain advantage over the network to bypass the firewall. SYN flooding sends a large number of SYN packets with spoofed source IP addresses to a target server, causing it to allocate resources and wait for the corresponding ACK packets that never arrive. This exhausts the server's resources and prevents it from accepting legitimate requests. To determine the source IP address of the SYN flooding attack, one has to follow these steps:

- ? Navigate to the Documents folder of Attacker-1 machine.
- ? Double-click on Synflood.pcapng file to open it with Wireshark.
- ? Click on Statistics menu and select Conversations option.
- ? Click on TCP tab and sort the list by Bytes column in descending order.
- ? Observe the IP address that has sent the most bytes to 20.20.10.26 (target server).

The IP address that has sent the most bytes to 20.20.10.26 is 20.20.10.19, which is the source IP address of the SYN flooding attack.

**NEW QUESTION 51**

Giovanni, a system administrator, was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. Identify the type of account created by Giovanni in this scenario.

- A. Third-party account
- B. Group-based account
- C. Shared account
- D. Application account

**Answer:** B

**Explanation:**

Group-based account is the type of account created by Giovanni in this scenario. An account is a set of credentials, such as a username and a password, that allows a user to access a system or network. An account can have different types based on its purpose or usage. A group-based account is a type of account that allows multiple users to access a system or network with the same credentials and permissions. A group-based account can be used to simplify the management of users and resources by assigning them to groups based on their roles or functions. In the scenario, Giovanni was tasked with configuring permissions for employees working on a new project. His organization used active directories (ADs) to grant/deny permissions to resources. Giovanni created a folder for AD users with the required permissions and added all employees working on the new project in it. This means that he created a group-based account for those employees. A third-party account is a type of account that allows an external entity or service to access a system or network with limited permissions or scope. A shared account is a type of account that allows multiple users to access a system or network with the same credentials but different permissions. An application account is a type of account that allows an application or software to access a system or network with specific permissions or functions.

**NEW QUESTION 55**

You have been assigned to perform a vulnerability assessment of a web server located at IP address 20.20.10.26. Identify the vulnerability with a severity score of 8.0. You can use the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password for this challenge. (Practical Question)

- A. TCP timestamps
- B. FTP Unencrypted Cleartext Login
- C. Anonymous FTP Login Reporting
- D. UDP timestamps

**Answer:** A

**Explanation:**

TCP Timestamps is the vulnerability with a severity score of 8.0. This can be verified by performing a vulnerability assessment of the web server located at IP address 20.20.10.26 using the OpenVAS vulnerability scanner, available with the Parrot Security machine, with credentials admin/password. To perform the vulnerability assessment, one can follow these steps:

Launch the Parrot Security machine and open a terminal.

Enter the command `sudo openvas-start` to start the OpenVAS service and wait for a few minutes until it is ready.

Open a web browser and navigate to `https://127.0.0.1:9392` to access the OpenVAS web interface.

Enter the credentials admin/password to log in to OpenVAS.

Click on Scans -> Tasks from the left menu and then click on the blue icon with a star to create a new task.

Enter a name and a comment for the task, such as "Web Server Scan". Select "Full and fast" as the scan config from the drop-down menu. Click on the icon with a star next to Target to create a new target. Enter a name and a comment for the target, such as "Web Server". Enter 20.20.10.26 as the host in the text box and click on Save.

Select "Web Server" as the target from the drop-down menu and click on Save.

Click on the green icon with a play button next to the task name to start the scan and wait for it to finish.

Click on the task name to view the scan report and click on Results from the left menu to see the list of vulnerabilities found.

Sort the list by Severity in descending order and look for the vulnerability with a severity score of 8.0. The screenshot below shows an example of performing these steps: The vulnerability with a severity score of 8.0 is TCP Timestamps, which is an option in TCP packets that can be used to measure round-trip time and improve performance, but it can also reveal information about the system's uptime, clock skew, or TCP sequence numbers, which can be used by attackers to launch various attacks, such as idle scanning, OS fingerprinting, or TCP hijacking<sup>1</sup>. The vulnerability report provides more details about this vulnerability, such as its description, impact, solution, references, and CVSS score<sup>2</sup>. References: Screenshot of OpenVAS showing TCP Timestamps vulnerability, TCP Timestamps Vulnerability, Vulnerability Report

**NEW QUESTION 56**

You are Harris working for a web development company. You have been assigned to perform a task for vulnerability assessment on the given IP address 20.20.10.26. Select the vulnerability that may affect the website according to the severity factor.

Hint: Greenbone web credentials: admin/password

- A. TCP timestamps
- B. Anonymous FTP Login Reporting
- C. FTP Unencrypted Cleartext Login
- D. UDP timestamps

**Answer:** C

**Explanation:**

FTP Unencrypted Cleartext Login is the vulnerability that may affect the website according to the severity factor in the above scenario. A vulnerability is a weakness or flaw in a system or network that can be exploited by an attacker to compromise its security or functionality. A vulnerability assessment is a process that involves identifying, analyzing, and evaluating vulnerabilities in a system or network using various tools and techniques. Greenbone is a tool that can perform vulnerability assessment on various targets using various tests and scans. To perform a vulnerability assessment on the given IP address 20.20.10.26, one has to follow these steps:

? Open a web browser and type 20.20.10.26:9392

? Press Enter key to access the Greenbone web interface.

? Enter admin as username and password as password.

? Click on Login button.

? Click on Scans menu and select Tasks option.

? Click on Start Scan icon next to IP Address Scan task.

? Wait for the scan to complete and click on Report icon next to IP Address Scan task.

? Observe the vulnerabilities found by the scan.

The vulnerabilities found by the scan are:

Name	Severity
TCP timestamps	Low
Anonymous FTP Login Reporting	Low
FTP Unencrypted Cleartext Login	Medium
UDP timestamps	Low

The vulnerability that may affect the website according to the severity factor is FTP Unencrypted Cleartext Login, which has a medium severity level. FTP Unencrypted Cleartext Login is a vulnerability that allows an attacker to intercept or sniff FTP login credentials that are sent in cleartext over an unencrypted connection. An attacker can use these credentials to access or modify files or data on the FTP server. TCP timestamps and UDP timestamps are vulnerabilities that allow an attacker to estimate the uptime of a system or network by analyzing the timestamp values in TCP or UDP packets. Anonymous FTP Login Reporting is a vulnerability that allows an attacker to access an FTP server anonymously without providing any username or password.

#### NEW QUESTION 58

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.

- A. White team
- B. Purple team
- 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.

#### NEW QUESTION 61

Identify a machine in the network with SSH service enabled. Initiate an SSH Connection to the machine, find the file, ttag.txt. in the machine, and enter the file's content as the answer. The credentials for SSH login are sam/adm(admin@123. {Practical Question}

- A. sam@bob
- B. bob2@sam
- C. sam2@bob
- D. bobt@sam

**Answer: D**

#### Explanation:

bob1@sam is the file's content as the answer. To find the machine with SSH service enabled, one can use a network scanning tool such as Nmap to scan the network for port 22, which is the default port for SSH. For example, the command `nmap -p 22 192.168.0.0/24` will scan the network range 192.168.0.0/24 for port 22 and display the results. To initiate an SSH connection to the machine, one can use a command-line tool such as ssh or an SSH client such as PuTTY to connect to the machine using the credentials sam/admin@123. For example, the command `ssh sam@192.168.0.10` will connect to the machine with IP address 192.168.0.10 using the username sam and prompt for the password admin@123. To find the file flag.txt in the machine, one can use a file searching tool such as find or locate to search for the file name in the machine's file system. For example, the command `find / -name flag.txt` will search for the file flag.txt from the root directory (/) and display its location. To enter the file's content as the answer, one can use a file viewing tool such as cat or less to display the content of the file flag.txt. For example, the command `cat /home/sam/flag.txt` will display the content of the file flag.txt located in /home/sam/ directory. The screenshot below shows an example of performing these steps: [Screenshot of performing these steps] References: Nmap Tutorial, SSH Tutorial, Find Command Tutorial, Cat Command Tutorial, [Screenshot of performing these steps]

#### NEW QUESTION 62

Andre, a security professional, was tasked with segregating the employees' names, phone numbers, and credit card numbers before sharing the database with clients. For this purpose, he implemented a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (\*) and hashes (#).

Which of the following techniques was employed by Andre in the above scenario?

- A. Tokenization
- B. Masking
- C. Hashing
- D. Bucketing

**Answer: B**

#### Explanation:

Masking is the technique that Andre employed in the above scenario. Masking is a deidentification technique that can replace the critical information in database fields with special characters such as asterisks (\*) and hashes (#). Masking can help protect sensitive data from unauthorized access or disclosure, while preserving the format and structure of the original data. Tokenization is a deidentification technique that can replace the critical information in database fields with

random tokens that have no meaning or relation to the original data. Hashing is a deidentification technique that can transform the critical information in database fields into fixed-length strings using a mathematical function. Bucketing is a deidentification technique that can group the critical information in database fields into ranges or categories based on certain criteria.

#### NEW QUESTION 64

Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user- specified decodes. Identify the Wireshark menu Leilani has navigated in the above scenario.

- A. Statistics
- B. Capture
- C. Main toolbar
- D. Analyze

**Answer: B**

#### Explanation:

Capture is the Wireshark menu that Leilani has navigated in the above scenario. Wireshark is a network analysis tool that captures and displays network traffic in real-time or from saved files. Wireshark has various menus that contain different items and options for manipulating, displaying, and analyzing network data. Capture is the Wireshark menu that contains items to start, stop, restart, or save a live capture of network traffic. Capture also contains items to configure capture filters, interfaces, options, and preferences. Statistics is the Wireshark menu that contains items to display various statistics and graphs of network traffic, such as packet lengths, protocols, endpoints, conversations, etc. Main toolbar is the Wireshark toolbar that contains icons for quick access to common functions, such as opening or saving files, starting or stopping a capture, applying display filters, etc. Analyze is the Wireshark menu that contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, and configure user-specified decodes.

#### NEW QUESTION 65

Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them. What is the technique used by Kevin to evade the IDS system?

- A. Desynchronization
- B. Obfuscating
- C. Session splicing
- D. Urgency flag

**Answer: B**

#### Explanation:

Obfuscating is the technique used by Kevin to evade the IDS system in the above scenario. Obfuscating is a technique that involves encoding or modifying packets or data with various methods or characters to make them unreadable or unrecognizable by an IDS (Intrusion Detection System). Obfuscating can be used to bypass or evade an IDS system that relies on signatures or patterns to detect malicious activities. Obfuscating can include encoding packets with Unicode characters, which are characters that can represent various languages and symbols. The IDS system cannot recognize the packet, but the target web server can decode them and execute them normally. Desynchronization is a technique that involves creating discrepancies or inconsistencies between the state of a connection as seen by an IDS system and the state of a connection as seen by the end hosts. Desynchronization can be used to bypass or evade an IDS system that relies on stateful inspection to track and analyze connections. Desynchronization can include sending packets with invalid sequence numbers, which are numbers that indicate the order of packets in a connection. Session splicing is a technique that involves splitting or dividing packets or data into smaller fragments or segments to make them harder to detect by an IDS system. Session splicing can be used to bypass or evade an IDS system that relies on packet size or content to detect malicious activities. Session splicing can include sending packets with small MTU (Maximum Transmission Unit) values, which are values that indicate the maximum size of packets that can be transmitted over a network. An urgency flag is a flag in the TCP (Transmission Control Protocol) header that indicates that the data in the packet is urgent and should be processed immediately by the receiver. An urgency flag is not a technique to evade an IDS system, but it can be used to trigger an IDS system to generate an alert or a response.

#### NEW QUESTION 66

Ayden works from home on his company's laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. Which of the following PCI-DSS requirements is demonstrated in this scenario?

- A. PCI-DSS requirement no 5.3
- B. PCI-DSS requirement no 1.3.1
- C. PCI-DSS requirement no 5.1
- D. PCI-DSS requirement no 1.3.2

**Answer: A**

#### Explanation:

PCI-DSS requirement no 5.3 is the PCI-DSS requirement that is demonstrated in this scenario. PCI-DSS (Payment Card Industry Data Security Standard) is a set of standards that applies to entities that store, process, or transmit payment card information, such as merchants, service providers, or payment processors. PCI-DSS requires them to protect cardholder data from unauthorized access, use, or disclosure. PCI-DSS consists of 12 requirements that are grouped into six categories: build and maintain a secure network and systems, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. PCI-DSS requirement no 5.3 is part of the category "maintain a vulnerability management program" and states that antivirus mechanisms must be actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. In the scenario, Ayden works from home on his company's laptop. During working hours, he received an antivirus software update notification on his laptop. Ayden clicked on the update button; however, the system restricted the update and displayed a message stating that the update could only be performed by authorized personnel. This means that his company's laptop has an antivirus mechanism that is actively running and cannot be disabled or altered by users, which demonstrates PCI-DSS requirement no 5.3.

#### NEW QUESTION 70

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **212-82 Practice Exam Features:**

- \* 212-82 Questions and Answers Updated Frequently
- \* 212-82 Practice Questions Verified by Expert Senior Certified Staff
- \* 212-82 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 212-82 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 212-82 Practice Test Here](#)**