EC-Council

Exam Questions 212-82

Certified Cybersecurity Technician(C|CT)

NEW QUESTION 1
A software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. Which of the following tiers of the secure application development lifecycle involves
checking the application
performance?

A. Development
B. Staging
C. Testing
D. Quality assurance (QA)

Answer: C

Explanation:
Testing is the tier of the secure application development lifecycle that involves checking the application performance in the above scenario. Secure application development is a process that involves designing, developing, deploying, and maintaining software applications that are secure and resilient to threats and attacks. Secure application development can be based on various models or frameworks, such as SDLC (Software Development Life Cycle), OWASP (Open Web Application Security Project), etc. Secure application development consists of various tiers or stages that perform different tasks or roles. Testing is a tier of the secure application development lifecycle that involves verifying and validating the functionality and security of software applications before releasing them to end users. Testing can include various types of tests, such as unit testing, integration testing, system testing, performance testing, security testing, etc. Testing can be used to check the application performance and identify any errors, bugs, or vulnerabilities in the software applications. In the scenario, a software company develops new software products by following the best practices for secure application development. Dawson, a software analyst, is responsible for checking the performance of applications in the client's network to determine any issue faced by end users while accessing the application. This means that he performs testing for this purpose. Development is a tier of the secure application development lifecycle that involves creating and coding software applications according to the design and specifications. Staging is a tier of the secure application development lifecycle that involves deploying software applications to a simulated or pre-production environment for testing or evaluation purposes. Quality assurance (QA) is a tier of the secure application development lifecycle that involves ensuring that software applications meet the quality standards and expectations of end users and stakeholders

NEW QUESTION 2
Jase. a security team member at an organization, was tasked with ensuring uninterrupted business operations under hazardous conditions. Thus, Jase implemented a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Which of the following business continuity and disaster recovery activities did Jase perform in this scenario?

A. Prevention
B. Response
C. Restoration
D. Recovery

Answer: A

Explanation:
Prevention is the business continuity and disaster recovery activity performed by Jase in this scenario. Prevention is an activity that involves implementing a deterrent control strategy to minimize the occurrence of threats, protect critical business areas, and mitigate the impact of threats. Prevention can include measures such as backup systems, firewalls, antivirus software, or physical security1. References: Prevention Activity in BCDR

NEW QUESTION 3
Rhett, a security professional at an organization, was instructed to deploy an IDS solution on their corporate network to defend against evolving threats. For this purpose, Rhett selected an IDS solution that first creates models for possible intrusions and then compares these models with incoming events to make detection decisions.
Identify the detection method employed by the IDS solution in the above scenario.

A. Not-use detection
B. Protocol anomaly detection
C. Anomaly detection
D. Signature recognition

Answer: C

Explanation:
Anomaly detection is a type of IDS detection method that involves first creating models for possible intrusions and then comparing these models with incoming events to make a detection decision. It can detect unknown or zero-day attacks by looking for deviations from normal or expected behavior

NEW QUESTION 4
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 5
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

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

NEW QUESTION 6
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 7
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-po int 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 8
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 9
Riley sent a secret message to Louis. Before sending the message, Riley digitally signed the message using his private key. Louis received the message, verified the digital signature using the corresponding key to ensure that the message was not tampered during transit.
Which of the following keys did Louis use to verify the digital signature in the above scenario?

A. Riley's public key
B. Louis's public key
C. Riley's private key
D. Louis's private key

Answer: A

Explanation:
Riley's public key is the key that Louis used to verify the digital signature in the above scenario. A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document. A digital signature is created by applying a hash function to the message or document and then encrypting the hash value with the sender's private key. A digital signature can be verified by decrypting the hash value with the sender's public key and comparing it with the hash value of the original message or document . Riley's public key is the key that corresponds to Riley's private key, which he used to sign the message. Louis's public key is the key that corresponds to Louis's private key, which he may use to encrypt or decrypt messages with Riley. Louis's private key is the key that only Louis knows and can use to sign or decrypt messages. Riley's private key is the key that only Riley knows and can use to sign or encrypt messages.

NEW QUESTION 10
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?

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.

NEW QUESTION 10
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 11
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 16
Dany, a member of a forensic team, was actively involved in an online crime investigation process. Dany's main responsibilities included providing legal advice on conducting the investigation and addressing legal issues involved in the forensic investigation process. Identify the role played by Dany in the above scenario.

A. Attorney
B. Incident analyzer
C. Expert witness
D. Incident responder

Answer: A

Explanation:
Attorney is the role played by Dany in the above scenario. Attorney is a member of a forensic team who provides legal advice on conducting the investigation and addresses legal issues involved in the forensic investigation process. Attorney can help with obtaining search warrants, preserving evidence, complying with laws and regulations, and presenting cases in court3. References: Attorney Role in Forensic Investigation

NEW QUESTION 20
A threat intelligence feed data file has been acquired and stored in the Documents folder of Attacker Machine-1 (File Name: Threatfeed.txt). You are a cybersecurity technician working for an ABC organization. Your organization has assigned you a task to analyze the data and submit a report on the threat landscape. Select the IP address linked with http://securityabc.s21sec.com.

A. 5.9.200.200
B. 5.9.200.150
C. 5.9.110.120
D. 5.9.188.148

Answer: D

Explanation:
5.9.188.148 is the IP address linked with http://securityabc.s21sec.com in the above scenario. A threat intelligence feed is a source of data that provides information about current or potential threats and attacks that can affect an organization’s network or system. A threat intelligence feed can include indicators of compromise (IoCs), such as IP addresses, domain names, URLs, hashes, etc., that can be used to detect or prevent malicious activities. To analyze the threat intelligence feed data file and determine the IP address linked with http://securityabc.s21sec.com, one has to follow these steps:
? Navigate to the Documents folder of Attacker-1 machine.
? Open Threatfeed.txt file with a text editor.
? Search for http://securityabc.s21sec.com in the file.
? Observe the IP address associated with the URL.
The IP address associated with the URL is 5.9.188.148, which is the IP address linked with http://securityabc.s21sec.com.

NEW QUESTION 24
Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN. To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. Identify the type of wireless encryption employed by Charlie in the above scenario.

A. TKIP
B. WEP
C. AES

D. CCMP

Answer: B

Explanation:
WEP is the type of wireless encryption employed by Charlie in the above scenario. Wireless encryption is a technique that involves encoding or scrambling the data transmitted over a wireless network to prevent unauthorized access or interception. Wireless encryption can use various algorithms or protocols to encrypt and decrypt the data, such as WEP, WPA, WPA2, etc. WEP (Wired Equivalent Privacy) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer

. WEP can be used to provide basic security and privacy for wireless networks, but it can also be easily cracked or compromised by various attacks . In the scenario, Charlie, a security professional in an organization, noticed unauthorized access and eavesdropping on the WLAN (Wireless Local Area Network). To thwart such attempts, Charlie employed an encryption mechanism that used the RC4 algorithm to encrypt information in the data link layer. This means that he employed WEP for this purpose. TKIP (Temporal Key Integrity Protocol) is a type of wireless encryption that uses the RC4 algorithm to encrypt information in the data link layer with dynamic keys . TKIP can be used to provide enhanced security and compatibility for wireless networks, but it can also be vulnerable to certain attacks . AES (Advanced Encryption Standard) is a type of wireless encryption that uses the Rijndael algorithm to encrypt information in the data link layer with fixed keys . AES can be used to provide strong security and performance for wireless networks, but it can also require more processing power and resources . CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is a type of wireless encryption that uses the AES algorithm to encrypt information in the data link layer with dynamic keys .

CCMP can be used to provide robust security and reliability for wireless networks, but it can also require more processing power and resources

NEW QUESTION 27
Mark, a security analyst, was tasked with performing threat hunting to detect imminent threats in an organization's network. He generated a hypothesis based on the observations in the initial step and started the threat-hunting process using existing data collected from DNS and proxy logs.
Identify the type of threat-hunting method employed by Mark in the above scenario.

A. Entity-driven hunting
B. TTP-driven hunting
C. Data-driven hunting
D. Hybrid hunting

Answer: C

Explanation:
A data-driven hunting method is a type of threat hunting method that employs existing data collected from various sources, such as DNS and proxy logs, to generate and test hypotheses about potential threats. This method relies on data analysis and machine learning techniques to identify patterns and anomalies that indicate malicious activity. A data-driven hunting method can help discover unknown or emerging threats that may evade traditional detection methods. An entity-driven hunting method is a type of threat hunting method that focuses on specific entities, such as users, devices, or domains, that are suspected or known to be involved in malicious activity. A TTP-driven hunting method is a type of threat hunting method that leverages threat intelligence and knowledge of adversary tactics, techniques, and procedures (TTPs) to formulate and test hypotheses about potential threats. A hybrid hunting method is a type of threat hunting method that combines different approaches, such as data-driven, entity-driven, and TTP-driven methods, to achieve more comprehensive and effective results.

NEW QUESTION 32
Initiate an SSH Connection to a machine that has SSH enabled in the network. After connecting to the machine find the file flag.txt and choose the content hidden in the file. Credentials for SSH login are provided below:
Hint: Username: sam
Password: admin@l23

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

Answer: C

Explanation:
Quid pro quo is the social engineering technique that Johnson employed in the above scenario. Social engineering is a technique that involves manipulating or deceiving people into performing actions or revealing information that can be used for malicious purposes. Social engineering can be performed through various methods, such as phone calls, emails, websites, etc. 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. Diversion theft is a social engineering method that involves diverting the delivery or shipment of goods or assets to a different location or destination. Elicitation is a social engineering method that involves extracting information from a target by engaging them in a conversation or an interaction. Phishing is a social engineering method that involves sending fraudulent emails or messages that appear to come from a trusted source, such as a bank, a company, or a person, and asking the recipient to click on a link, open an attachment, or provide personal or financial information.

NEW QUESTION 33
An MNC hired Brandon, a network defender, to establish secured VPN communication between the company's remote offices. For this purpose, Brandon employed a VPN topology where all the remote offices communicate with the corporate office but communication between the remote offices is denied.
Identify the VPN topology employed by Brandon in the above scenario.

A. Point-to-Point VPN topology
B. Star topology
C. Hub-and-Spoke VPN topology
D. Full-mesh VPN topology

Answer: C

Explanation:

A hub-and-spoke VPN topology is a type of VPN topology where all the remote offices communicate with the corporate office, but communication between the remote offices is denied. The corporate office acts as the hub, and the remote offices act as the spokes. This topology reduces the number of VPN tunnels required and simplifies the management of VPN policies. A point-to-point VPN topology is a type of VPN topology where two endpoints establish a direct VPN connection. A star topology is a type of VPN topology where one endpoint acts as the central node and connects to multiple other endpoints. A full-mesh VPN topology is a type of VPN topology where every endpoint connects to every other endpoint.

NEW QUESTION 38

George, a security professional at an MNC, implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. Identify the type of Internet access policy implemented by George in this scenario.

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

Answer: A

Explanation:

Permissive policy is the type of Internet access policy implemented by George in this scenario. An Internet access policy is a policy that defines the rules and guidelines for accessing the Internet from a system or network. An Internet access policy can be based on various factors, such as security, productivity, bandwidth, etc. An Internet access policy can have different types based on its level of restriction or control. A permissive policy is a type of Internet access policy that allows users to access any site, download any application, and access any computer or network without any restrictions. A permissive policy can be used to provide maximum flexibility and freedom to users, but it can also pose significant security risks and challenges. In the scenario, George implemented an Internet access policy that allowed employees working from a remote location to access any site, download any application, and access any computer or network without any restrictions. This means that he implemented a permissive policy for those employees. A paranoid policy is a type of Internet access policy that blocks or denies all Internet access by default and only allows specific sites, applications, or computers that are explicitly authorized. A prudent policy is a type of Internet access policy that allows most Internet access but blocks or restricts some sites, applications, or computers that are deemed inappropriate, malicious, or unnecessary. A promiscuous policy is not a type of
Internet access policy, but a term that describes a network mode that allows a network interface card (NIC) to capture all packets on a network segment, regardless of their destination address.

NEW QUESTION 41

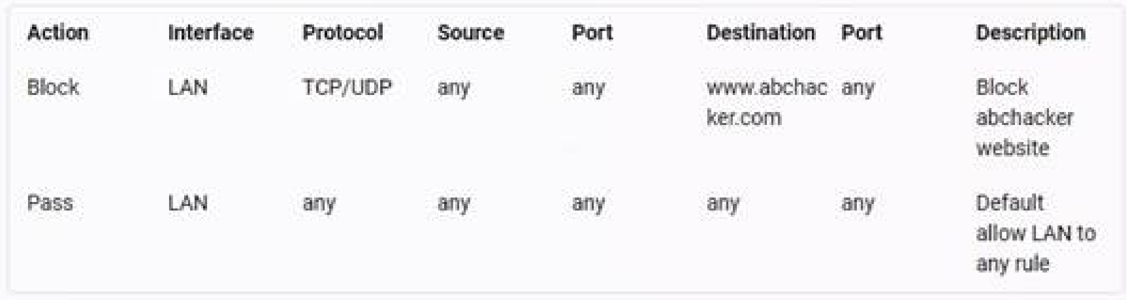
A pfSense firewall has been configured to block a web application www.abchacker.com. Perform an analysis on the rules set by the admin and select the protocol which has been used to apply the rule.
Hint: Firewall login credentials are given below: Username: admin
Password: admin@l23

A. POP3
B. TCP/UDP
C. FTP
D. ARP

Answer: B

Explanation:

TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com in the above scenario. pfSense is a firewall and router software that can be installed on a computer or a device to protect a network from various threats and attacks. pfSense can be configured to block or allow traffic based on various criteria, such as source, destination, port, protocol, etc. pfSense rules are applied to traffic in the order they appear in the firewall configuration . To perform an analysis on the rules set by the admin, one has to follow these steps:
? Open a web browser and type 20.20.10.26
? Press Enter key to access the pfSense web interface.
? Enter admin as username and admin@l23 as password.
? Click on Login button.
? Click on Firewall menu and select Rules option.
? Click on LAN tab and observe the rules applied to LAN interface.
The rules applied to LAN interface are:



Action	Interface	Protocol	Source	Port	Destination	Port	Description
Block	LAN	TCP/UDP	any	any	www.abchacker.com	any	Block abchacker website
Pass	LAN	any	any	any	any	any	Default allow LAN to any rule

The first rule blocks any traffic from LAN interface to www.abchacker.com website using TCP/UDP protocol. The second rule allows any traffic from LAN interface to any destination using any protocol. Since the first rule appears before the second rule, it has higher priority and will be applied first. Therefore, TCP/UDP is the protocol that has been used to apply the rule to block the web application www.abchacker.com. POP3 (Post Office Protocol 3) is a protocol that allows downloading emails from a mail server to a client device. FTP (File Transfer Protocol) is a protocol that allows transferring files between a client and a server over a network. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC (Media Access Control) addresses on a network.

NEW QUESTION 45

......