Eccouncil

(312-38)

Certified Network Defender

Total: **718 Questions**

Link:

MYEXAM.FR

through the normal authentication process. The main advantage of this type of attack is that the network traffic moves from inside a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically the least restrictive, as companies are more concerned about what comes into a network, rather than what leaves it. It, therefore, becomes hard to detect backdoors.

Question: 3

FILL BLANK -
Fill in the blank with the appropriate term. _____ is the complete network configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Answer: NetRanger

Explanation:
NetRanger is the complete network configuration and information toolkit that includes the following tools: a Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the
Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

Question: 4

FILL BLANK -
Fill in the blank with the appropriate term. A _____device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Answer: biometric

Explanation:
A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits.
Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.
Biometric characteristics can be divided into two main classes:
1. Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent.
2. Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

Question: 5

Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

A. Wireless sniffer

Question: 9

FILL BLANK -
Fill in the blank with the appropriate term. _____ is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.

Answer:

Network reconnaissance

Explanation:
Network reconnaissance is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.
Network reconnaissance is increasingly used to exploit network standards and automated communication methods. The aim is to determine what types of computers are present, along with additional information about those computers such as the type and version of the operating system. This information can be analyzed for known or recently discovered vulnerabilities that can be exploited to gain access to secure networks and computers. Network reconnaissance is possibly one of the most common applications of passive data analysis. Early generation techniques, such as TCP/IP passive fingerprinting, have accuracy issues that tended to make it ineffective. Today, numerous tools exist to make reconnaissance easier and more effective.

Question: 10

FILL BLANK -
Fill in the blank with the appropriate term. The _____is an application layer protocol that is used between workstations and routers for transporting SNA/
NetBIOS traffic over TCP sessions.

Answer: DCAP

Explanation:
The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/
NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues.

Question: 11

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:
`It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.`
Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd
B. Kismet
C. AirSnort
D. Cain

B. Fire Suppression System: Similar to the fire sprinkler, fire suppression systems are designed for controlling and extinguishing fires using various agents (foam, chemicals, etc.). However, like sprinklers, they do not have a detection capability but rather a reactive extinguishing function, rendering them inadequate as a means to recognize fire origin or presence.

D. Gaseous Fire Suppression: These systems deploy inert gas to suppress fires in sensitive environments (e.g., data centers). While very effective for controlling fire after its presence has been established, they do not engage in the detection phase, as their main role is to mitigate damage once a fire has begun.

For comprehensive insights into fire alarm systems and their functionalities, one can refer to the following authoritative references:

1. https://www.nfpa.org/Codes-and-Standards/Resources/Fire-safety-in-the-home/Smoke-alarm-facts-and-figures
2. https://www.firesafety.gov/what-are-fire-alarms
3. https://www.nfpa.org/-/media/Files/Training/Fire-Safety/FireAlarmSystemsFactSheet.ashx

Question: 14

Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?

A. IPS
B. HIDS
C. DMZ
D. NIDS

Answer: B

Explanation:

B is correct because a Host Intrusion Detection System (HIDS) specifically monitors the internal activities of a computing system rather than external network traffic.

In detail, HIDS operates by analyzing system logs, file integrity, and process behavior to detect irregularities or potential security breaches. This detection occurs at the endpoint level, providing deep insights into the operating system's health and security status. It is particularly effective in identifying unauthorized access, malware, and system anomalies that network-based systems cannot efficiently correlate.

Evaluation of Other Options:

A. IPS (Intrusion Prevention System): IPS is primarily designed to detect and actively prevent network intrusions by inspecting network packets and stopping malicious activities before they reach the target systems. It operates at the network layer, focusing on traffic rather than the internal workings of the host.

C. DMZ (Demilitarized Zone): A DMZ is a secure area of a network that acts as a buffer zone between an internal network and an external one. While it is a network architecture used to enhance security, it does not provide monitoring or analysis of system internals.

D. NIDS (Network Intrusion Detection System): NIDS monitors network traffic to identify suspicious activities by analyzing packets flowing through the network. It focuses on network-level activities rather than the detailed internal operations of host systems, making it less effective for detecting internal compromises.

C. Email spoofing

D. Email jamming

Answer: AB

Explanation:

A. E-mail spam and B. Junk mail accurately describe the practice of sending unsolicited e-mail messages, often with commercial intentions, to numerous recipients without their consent.

E-mail spam refers to unsolicited bulk messages that typically aim to promote products or services, creating a nuisance for recipients. The classification of such communications as "spam" is well-established within both legal frameworks and IT security practices, as it poses significant operational and legal challenges for individuals and organizations alike. Junk mail, while sometimes viewed as physical correspondence, has become synonymous with digital spam in online contexts, indicating unwanted advertising or promotional content delivered via e-mail.

Conversely, option C, Email spoofing, involves altering the sender's address in an e-mail to deceive recipients into believing the message is from a trusted source, but does not inherently relate to the mass distribution of unsolicited content. This tactic often complements phishing attacks but is distinct from the act of sending spam itself. Option D, Email jamming, refers to the intentional disruption of email communication channels, which also diverges from the concept of unsolicited advertising as it centers around interference rather than distribution practices.

Thus, only A and B embody the established definitions applicable within the domain of unsolicited electronic communications.

References:

https://www.cisco.com/c/en/us/products/collateral/security/email-security/index.html
https://www.spamhaus.org/consumer/dictionary/
https://www.icann.org/resources/pages/spam-2012-02-25-en

Question: 19

FILL BLANK -
Fill in the blank with the appropriate word. The _____risk analysis process analyzes the effect of a risk event deriving a numerical value.

Answer: quantitative

Explanation:
Quantitative risk analysis is a process to assess the probability of achieving particular project objectives, to quantify the effect of risks on the whole project objective, and to prioritize the risks based on the impact to the overall project risk. The quantitative risk analysis process analyzes the effect of a risk event deriving a numerical value. It also presents a quantitative approach to build decisions in the presence of uncertainty. The inputs for quantitative risk analysis are as follows:

Organizational process assets -

Project scope statement -

Risk management plan -

Explanation:

The correct answers are A and C because both client-server computing and client-server networking partition tasks between service providers (servers) and service requesters (clients).

Justification for A and C: Client-server architectures inherently involve a structured division of roles where the server provides resources or services (data, processing power) while the client requests these services. This clear delineation of responsibilities exemplifies a distributed application architecture, efficiently managing workloads and enhancing resource use (Bhanot et al., 2016). Both "client-server computing" and "client-server networking" emphasize this division, facilitating scalability and centralized management, which are pivotal in distributed systems.

Evaluation of B and D: Peer-to-peer (P2P) computing (B) and peer-to-peer networking (D) operate on a decentralized model where each participant can act as both a service provider and a service requester simultaneously. This negates the traditional client-server model's explicit partitioning of tasks, as every node in a P2P environment shares equivalent responsibilities, ultimately leading to a more collaborative rather than a hierarchically organized workload distribution (Babaoglu, 2008). Therefore, while P2P models excel in resource sharing and fault tolerance, they do not conform to the definition of a distributed system focused on clear service provision hierarchies.

Additionally, terms 'client-server computing' and 'client-server networking' point towards a specific architecture that supports scalability through centralized structure, which is not representative in peer-to-peer arrangements.

References:

https://www.researchgate.net/publication/313983591_Distributed_Computing_Environment_for_the_Grid_Based_C
Server_Computing
https://link.springer.com/chapter/10.1007/978-3-030-50853-0_17
https://ieeexplore.ieee.org/document/6536482

Question: 23

Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?

A. Website defacement
B. Zero-day attack
C. Spoofing
D. Buffer overflow

Answer: A

Explanation:

A. Website defacement is correct because it directly alters the appearance of a website, undermining its integrity and eroding user trust.

Website defacement is primarily characterized by malicious entities altering the visual presentation of a site, typically to convey a political message or to demonstrate vulnerabilities. The implications of such attacks extend beyond immediate visual changes; they can lead to long-term reputational damage, loss of user confidence, and financial repercussions. When visitors perceive a website as compromised, it significantly influences their willingness to return or engage with the services provided, thereby impacting the site's

presence and quality of these networks. This strategic practice benefits users by facilitating the discovery of accessible connections in urban areas without the need for extensive searching. It stands out in the context of network security and wireless communications because it aligns with both advertising and community resource sharing.

Evaluation of Incorrect Options:

A. Spamming: This term refers to the indiscriminate sending of unsolicited emails, primarily for advertising products or services. It does not relate to advertising Wi-Fi networks and lacks the visual symbolic representation characteristic of Warchalking.

B. War driving: While War driving involves searching for unsecured Wi-Fi networks by moving through areas, it focuses on network discovery rather than publicizing them. Therefore, it lacks the tangible element of drawing symbols associated with Warchalking.

C. War dialing: This technique entails dialing a list of phone numbers to discover any modems connected to them. It falls within the realm of voice communication rather than wireless networking, distinguishing it from the visual signaling inherent in Warchalking.

In summary, Warchalking uniquely encapsulates the act of visually marking open Wi-Fi spots, while the other options are irrelevant to the concept of public advertisement for wireless networks.

References:

https://www.wired.com/2003/08/warchalking/
https://www.networkworld.com/article/3235172/the-history-and-tech-of-war-driving.html
https://www.cs.cmu.edu/~chuck/lennapg/whatis/cybersecurity/whatiswarchalking.html

Question: 28

Which of the following is a standard protocol for interfacing external application software with an information server, commonly a Web server?

A. DHCP
B. IP
C. CGI
D. TCP

Answer: C

Explanation:

C is correct because CGI (Common Gateway Interface) serves as a standard protocol enabling external application software to interact with web servers to generate dynamic content.

CGI acts as an intermediary, allowing web servers to execute external programs and return their output to clients. This interaction is crucial for developing dynamic web applications where content can be generated in response to user input. The flexibility of CGI supports various programming languages, enhancing its utility in web development environments.

Evaluation of Other Options:

A. DHCP: Dynamic Host Configuration Protocol (DHCP) is primarily used for assigning IP addresses dynamically to devices on a network. It does not facilitate application interaction with web servers but rather

Question: 31

Which of the following devices allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards?

A. Express card
B. WAP
C. WNIC
D. Wireless repeater
E. None

Answer: B

Explanation:

The correct answer is B, as the Wireless Access Point (WAP) facilitates the connection of wireless communication devices to a wireless network using Wi-Fi and other related standards.

A WAP functions as a bridge between wired and wireless networks, serving to extend network accessibility by allowing multiple devices to connect to a network without physical cabling. Its function is critical in environments where mobility and flexibility of device connectivity are paramount, such as in offices, homes, and public areas.

Evaluation of Other Options:

A. Express card: This is a form of interface used primarily in laptops to add extra functionalities, connecting peripheral devices. It does not inherently provide wireless connectivity itself, distinguishing it from WAPs which establish wireless networks.

C. WNIC (Wireless Network Interface Card): While a WNIC allows a device to connect to a wireless network, it is not a networking device that enables other devices to connect. Rather, it is specific to the device itself, functioning at the client side rather than as an access point.

D. Wireless repeater: Although it enhances the range of a wireless signal, a wireless repeater does not create a new access point for devices to connect to; instead, it extends the reach of an existing network. This is a critical distinction, as repeaters do not manage connections but merely amplify existing signals.

E. None: As a choice, this does not apply since WAP is indeed a valid option. The existence of a well-defined function for WAP directly negates this option as an answer.

In summary, a WAP is indispensable for establishing a wireless network and allowing diverse devices to connect seamlessly, an ability not mirrored by the other listed options.

References:

https://www.networkworld.com/article/3495344/what-is-a-wireless-access-point.html
https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-access-points/white-paper-list.html
https://www.computerhope.com/jargon/w/wireless-access-point.htm

Question: 32

Which of the following protocols uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets?

portals.

B. Temporary Internet Folder: This is also a valid choice. It holds cached versions of web pages, allowing an investigator to find remnants of emails or email attachments that may have been viewed or downloaded.

C. Cookies Folder: Although this folder contains data regarding user sessions and preferences, it does not provide direct evidence about specific email interactions or contents. Thus, it is less relevant in a focused investigation of email usage.

D. Download Folder: This is indeed relevant, as it may contain files that the employee downloaded from their email, further solidifying evidence of their online behavior.

Ultimately, the combination of CAB provides a comprehensive view of the employee's online email usage while each of these specific locations serves a different investigative purpose.

References:

https://www.forensicswiki.org/wiki/Internet_Artifact_Evidence
https://www.oss-online.org/guide-computer-forensics
https://www.cyberforensicator.com/forensic-analysis-of-email-evidence

Question: 36

Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?

A. Transport layer
B. Link layer
C. Internet layer
D. Application layer

Answer: A

Explanation:

A is correct because the Transport layer is responsible for ensuring data integrity, order, and reliability in message delivery.

The Transport layer, specifically protocols such as TCP (Transmission Control Protocol), utilizes sequence numbers and acknowledgments to maintain the order and delivery of data packets, thus preventing loss and duplication. By employing checksums and retransmission strategies, it guarantees that received data is accurate, creating an essential foundation for reliable communication across networks. The mechanisms in place within this layer not only establish connections but also manage congestion, enhancing the performance and integrity of data transmission.

In contrast, the other options are incorrect for the following reasons:

B. Link Layer: The Link layer primarily deals with node-to-node data transfer within a single segment. It is tasked with framing, addressing, and error detection, but it does not provide end-to-end reliability or the ordering of packets across multiple networks.

C. Internet Layer: The Internet layer, which includes the IP (Internet Protocol), is responsible for routing packets between devices across different networks. While it handles addressing and forwarding, it does not ensure reliability or packet ordering, which are features exclusive to the Transport layer.

https://www.cisa.gov/insights/articles/2021/11/refining-your-organization-password-policy
https://www.nist.gov/itl/publications/nist-special-publication-800-63b
https://www.cyber.gov.au/acsc/view-all-content/publications/what-strong-password

Question: 39

Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?

A. Facial recognition device
B. Iris camera
C. Voice recognition voiceprint
D. Fingerprint reader

Answer: D

Explanation:

D is correct because a fingerprint reader specifically captures the unique patterns of friction ridges found on the fingers.

Biometric authentication leverages distinct physiological characteristics for identification. Fingerprint readers utilize sensors to scan and digitize the minutiae patterns on the skin's surface, which serve as reliable identifiers due to individuality and persistence throughout a person's life. This technology underpins a broad array of security applications, facilitating accurate user identification and access control.

Critical Evaluation of Other Options:

A. **Facial recognition device**: This technology relies on the analysis of facial features, such as the distance between eyes or jawline contours, rather than the unique skin patterns found on fingertips. While effective in identifying individuals, it lacks the specificity and reliability inherent to fingerprint recognition.

B. **Iris camera**: Although iris recognition provides a high level of accuracy due to the uniqueness of the iris, it is fundamentally different from fingerprint readers, which focus specifically on the friction ridge patterns of fingers, making it unsuitable for the context of the question.

C. **Voice recognition voiceprint**: This biometric utilizes vocal characteristics to distinguish individuals. It primarily captures audio patterns, which can be influenced by numerous factors such as environmental conditions or emotional state, thus offering less reliability compared to the permanent features captured by fingerprint readers.

In conclusion, fingerprint readers are uniquely designed to capture and analyze the friction ridges on fingers, distinguishing them from other biometric technologies that cater to different physiological traits.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6488186/
https://www.researchgate.net/publication/313833706_Fingerprints_and_their_Applications_in_Authentication
https://www.sciencedirect.com/science/article/pii/S1877050920303681

Question: 40

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses.

gain access or information.

6. **Message Repudiation (E)**: This entails a sender denying sending a message, stressing the importance of non-repudiation in secure communication.

Evaluation of Incorrect Options:

Message Digest (D): While important for ensuring data integrity through hash functions, it is a preventative measure rather than a direct security risk itself. It does not inherently relate to vulnerabilities in communications and email but rather to how integrity is maintained.

In conclusion, the selected answers comprehensively outline the critical vulnerabilities in communication and email systems, while the rejected option focuses on a technology used to combat, not illustrate, security problems.

References:

https://www.sans.org/white-papers/88/
https://www.cisecurity.org/white-papers/eavesdropping-and-its-prevention/
https://www.infosecurity-magazine.com/opinions/understanding-replay-attacks/

Question: 44

Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?

A. Application layer
B. Internet layer
C. Link layer
D. Transport Layer
E. None

Answer: C

Explanation:

C is correct because the Link layer is responsible for facilitating communication between network interfaces on the same physical network segment.

The TCP/IP model comprises four layers: Application, Transport, Internet, and Link. The Link layer specifically handles the transfer of data packets over the physical media. It encompasses protocols and standards that ensure reliable communication over local links, such as Ethernet and Wi-Fi, managing frame encapsulation, addressing, and error detection. The Link layer operates directly with the hardware and is crucial in the packet delivery process between hosts on the same local network.

Evaluation of Incorrect Options:

A. **Application Layer:** This layer is concerned with end-user data and applications, providing protocols for specific data communications but does not deal with packet movement between interfaces.

B. **Internet Layer:** While it handles packet routing and forwarding across networks, it does not manage the actual movement of packets within a local link, which is the Link layer's responsibility.

D. **Transport Layer:** This layer is responsible for end-to-end communication, flow control, and error correction, but it abstracts away the underlying mechanics of packet delivery on a local link, focusing instead on data

D. Warkitting is a less common term that often refers to connecting to an unsecured network or system remotely. Like warchalking, it is not associated with the scanning of telephone numbers and is distinct from the automated scanning process involved in war dialing.

In summary, war dialing uniquely captures the essence of utilizing modems to systematically scan telephone numbers, underlining its importance within the cybersecurity domain.

References:

https://www.csoonline.com/article/3381600/how-war-dialing-works-and-what-it-can-do-for-your-security-efforts.html
https://www.sans.org/white-papers/15427/
https://www.techopedia.com/definition/7255/war-dialing

Question: 48

FILL BLANK -
Fill in the blank with the appropriate file system. Alternate Data Streams (ADS) is a feature of the_____ file system, allowing more than one data stream to be associated with a filename.

Answer: NTFS

Explanation:
Alternate Data Streams (ADS) is a feature of the NTFS file system that allows more than one data stream to be associated with a filename, using the filename format "filename:streamname". Alternate streams are not listed in Windows Explorer, and their size is not included in the file size. ADS provides the hacker a place to hide root kits or hacker tools, which can be executed without being detected by the system administrator. Alternate Data Streams are strictly a feature of the
NTFS file system. Alternate Data Streams may be used as a method of hiding executables or proprietary content.

Question: 49

Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?

A. User policy
B. IT policy
C. Issue-Specific Security Policy
D. Group policy

Answer: C

Explanation:

C is correct because the Issue-Specific Security Policy (ISSP) provides tailored security guidelines that address specific issues, ensuring clarity and enhancing the organization's overall security posture.

The ISSP is crucial for delineating security measures concerning particular topics, such as remote access, acceptable use, and incident response, thereby reducing ambiguity and inefficiency in operations. By setting precise standards, it allows organizations to adapt to dynamic security threats while ensuring compliance with broader policies.

D is correct as a Network Intrusion Detection System (NIDS) analyzes network traffic for suspicious patterns or signatures, effectively identifying potential threats.

NIDS operates at the network level, monitoring all incoming packets in real-time to detect suspicious activities. By utilizing signature-based detection methods, it can identify known threats based on predefined patterns, providing a proactive security measure against intrusions. This capacity to read and process each packet allows NIDS to perform effectively in environments where extensive traffic analysis is necessary to uphold network integrity and security.

Evaluation of Other Options:

A. **HIDS (Host Intrusion Detection System)**: HIDS operates at the host level rather than monitoring all incoming packets across a network. It analyzes the system's internal state, looking for signs of malicious activity, which does not align with the real-time packet examination characteristic of NIDS.

B. **IPS (Intrusion Prevention System)**: While an IPS can also inspect packets to detect signatures, it differs by not merely detecting but actively preventing intrusions. The question specifies the detection aspect, making NIDS the more fitting answer as it is solely focused on identifying suspicious patterns rather than implementing active countermeasures.

C. **DMZ (Demilitarized Zone)**: A DMZ refers to a network configuration used to enhance security by isolating external servers from the internal network. It is a network architecture rather than a detection tool, hence irrelevant in the context of identifying signatures in network traffic.

In summary, NIDS specializes in analyzing packets for threats through signature-based methods, distinguishing it from HIDS, IPS, and DMZ.

References:

1. https://www.cisco.com/c/en/us/products/security/what-is-intrusion-detection-system-ids.html
2. https://www.varonis.com/blog/intrusion-detection-system
3. https://www.paloaltonetworks.com/cybersecurity-101/intrusion-detection-system-ids

Question: 55

Fill in the blank with the appropriate term. The_____ is typically considered as the top InfoSec officer in the organization and helps in maintaining current and appropriate body of knowledge required to perform InfoSec management functions.

Answer: CISO

Explanation:
The Chief InfoSec Officer (CISO) is typically considered as the top InfoSec officer in the organization, though the CISO is usually not an executive-level position and commonly reports to the CIO. Following are the job competencies for the Chief InfoSec Officer (CISO):
Maintaining current & appropriate body of knowledge required to perform InfoSec management functionsEffectively applying InfoSec management knowledge for improving security of open network and associated systems and services Maintaining working knowledge of external legislative & regulatory initiativesInterpreting and translating requirements for implementationDeveloping appropriate InfoSec policies, standards, guidelines, and proceduresProviding meaningful input, preparing effective presentations, and communicating InfoSec objectivesParticipating in short and long term planning

Question: 56

Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission.

Question: 60

FILL BLANK -
Fill in the blank with the appropriate term. The _____is a communication protocol that communicates information between the network routers and the multicast end stations.

Answer: IGMP

Explanation:
The Internet Group Management Protocol (IGMP) is a communication protocol that communicates information between the network routers and the multicast end stations. It allows the receivers to request a multicast data stream from a specific group address. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. The IGMP allows an end station to connect to a multicast group and leave it, while being connected to the group address. It can be effectively used for gaming and showing online videos. Although it does not actually act as a transport protocol, it operates above the network layer. It is analogous to ICMP for unicast connections. It is susceptible to some attacks, so firewalls commonly allow the user to disable it if not needed.

Question: 61

Which of the following can be performed with software or hardware devices in order to record everything a person types using his or her keyboard?

A. Warchalking
B. Keystroke logging
C. War dialing
D. IRC bot

Answer: B

Explanation:

B. Keystroke logging is the correct answer as it involves capturing each keystroke made by a user through software or hardware devices.

Keystroke logging is an established technique used primarily for monitoring and recording input from keyboards, thereby providing insights into user behavior, applications used, or even gathering sensitive information such as passwords. This technique can be implemented using various means, including software installed on the target machine or dedicated hardware devices intercepting the keyboard input directly.

Evaluation of other options:

A. Warchalking refers to the practice of marking on the sidewalk or using symbols to indicate the availability of wireless networks. While it relates to network security, it does not involve recording keystrokes, making it irrelevant to the context of keystroke logging.

Question: 67

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. Read-Only Memory (ROM) is an example of volatile memory.
B. The content is stored permanently, and even the power supply is switched off.
C. The volatile storage device is faster in reading and writing data.
D. It is computer memory that requires power to maintain the stored information.

Answer: DC

Explanation:

DC is correct because volatile memory is characterized by its need for power to retain information and its faster read/write capabilities compared to non-volatile memory.

Justification of Correct Options:

1. **C**: Volatile storage devices, such as RAM, are designed for speed, allowing for rapid read and write operations. This is essential for active processes and applications in computing, providing performance advantages over non-volatile types which access data more slowly.
2. **D**: By definition, volatile memory requires continuous power to maintain its stored information. Once power is lost, all data is erased, distinguishing it from non-volatile memory types that retain data without power.

Evaluation of Incorrect Options:

1. **A**: Read-Only Memory (ROM) is not classified as volatile memory. Rather, it is non-volatile because its contents remain intact even when the power is turned off, allowing it to store firmware and essential system instructions.
2. **B**: The statement that content is stored permanently contradicts the essence of volatile storage. By definition, volatile memory loses its data with a power interruption, while permanent data storage is a characteristic of non-volatile memory types.

To summarize, the key attributes of volatile memory are its dependency on power for data retention and its speed in processing, which are not applicable to the features of ROM or the permanence suggested in the other option.

References:

https://en.wikipedia.org/wiki/Volatile_memory
https://www.techopedia.com/definition/20180/volatile-memory
https://www.ibm.com/docs/en/zos/2.4.0?topic=concepts-volatile-and-non-volatile-storage

Question: 68

Which of the following firewalls are used to track the state of active connections and determine the network packets allowed to enter through the firewall? Each correct answer represents a complete solution. Choose all that apply.

IP Phones look exactly like the traditional phones, but they differ in that they have RJ-45 Ethernet connectors, instead of RJ-11 phone connectors, for connecting to the computers.

Computer To Computer -
This is the easiest way to use VoIP. For this, we need software, microphone, speakers, sound card and an Internet connection through a cable or a DSL modem.

Soft Phones -
Soft phone is a software application that can be loaded onto a computer and used anywhere in the broadband connectivity area.

Question: 71

FILL BLANK -
Fill in the blank with the appropriate term. The _____ protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.

Answer: Sliding Window

Explanation:
The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame sequences sent, and their respective acknowledgements received, by both the users. Its additional feature over a simpler protocol is that can allow multiple packets to be "in transmission" simultaneously, rather than waiting for each packet to be acknowledged before sending the next.In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgment is received or before a specified event occurs.An example of a sliding window is one in which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender "slides" the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes called acknowledgment delay period.

Question: 72

FILL BLANK -
Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.

Answer: rootkit

Explanation:
A rootkit is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers. A rootkit requires root access to be installed in the Linux operating system, but once installed, the attacker can get root access at any time. Rootkits have the following features:
They allow an attacker to run packet sniffers secretly to capture passwords.
They allow an attacker to set a Trojan into the operating system and thus open a backdoor for anytime access.
They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
They provide utilities for installing Trojans with the same attributes as legitimate programs.

Conversely, the **RST** (B) flag is not typically used in an Xmas tree scan; it is usually employed to reset connections. Sending an RST packet would not initiate a scan, as it generally signals an error or an attempt to terminate a session, rather than probe for open ports. Thus, it does not fulfill the methodological intent of an Xmas tree scan.

In summary, the flags FIN, URG, and PUSH are employed together to probe for open ports in this technique, while RST serves a different operational purpose unrelated to the Xmas tree scanning methodology.

References:

https://www.cyberciti.biz/faq/how-to-use-nmap-xmas-tree-scanning/
https://www.sans.org/white-papers/1998/
https://www.csoonline.com/article/3031981/understanding-network-scanning.html

Question: 77

Network security is the specialist area, which consists of the provisions and policies adopted by the Network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. For which of the following reasons is network security needed? Each correct answer represents a complete solution. Choose all that apply.

A. To protect information from loss and deliver it to its destination properly
B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
C. To protect private information on the Internet
D. To prevent a user from sending a message to another user with the name of a third person

Answer: CBAD

Explanation:

The options C, B, A, and D correctly highlight the multifaceted importance of network security in protecting valuable information and sustaining network integrity.

Firstly, option C correctly addresses the need for network security to safeguard private information online. As digital communications proliferate, the loss of confidentiality can lead to significant personal and organizational repercussions, including identity theft and data breaches. Thus, rigorous protections are essential to maintain trust and safeguard sensitive data.

Secondly, option B emphasizes the necessity of preventing unauthorized editing of information. This aspect is crucial in ensuring data integrity, as both accidental and intentional modifications can severely impact decision-making processes and operational reliability. Network security measures such as access control and checksum verification directly contribute to maintaining the authenticity of data within systems.

Option A concerns the delivery and proper handling of information; while it is important, its focus on the transportation process may not fully encompass the protective measures required to prevent unauthorized access and alteration, making it slightly less critical compared to options C and B.

Lastly, option D refers to the prevention of impersonation through message spoofing, which technically falls under network security. However, it is less relevant than the foundational need to protect against unauthorized access and modification, as impersonation is often a side effect of broader systemic security issues rather than a primary motivator for network security policies.

In summary, options C, B, A, and D collectively underline critical facets of network security; however, C and B are more fundamental to the core objectives of safeguarding data integrity and confidentiality.

Critique of Alternatives:

None of the options presented are incorrect as they all represent critical responsibilities of the disaster recovery team; thus, there are no alternatives that challenge the validity of A, B, C, and D.

References:

https://www.cio.com/article/221977/disaster-recovery-best-practices.html
https://www.isc2.org/News-and-Events/Blog/PostID/1560
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5414468/