UPGRADE YOUR SKILL

IT SECURITY PRACTICE TEST QUESTIONS

Practice Test 4

1. Which layer of the OSI model does a packet filtering firewall operate at? Select all that apply.

A. Packet filtering firewalls operate in layer 1 of the OSI model, the Physical layer.
B. Packet filtering firewalls operate in layer 2 of the OSI model, the Data-Link layer.
C. Packet filtering firewalls operate in layer 3 of the OSI model, the Network layer.
D. Packet filtering firewalls operate in layer 4 of the OSI model, the Transport layer.
E. Packet filtering firewalls operate in layer 5 of the OSI model, the Session layer.
F. Packet filtering firewalls operate in layer 6 of the OSI model, the Presentation layer.
G. Packet filtering firewalls operate in layer 7 of the OSI model, the Application layer.

---

2. Which of the following describes DPI, and it is possible to circumvent? Select the best answer.

A. DPI analyses data and header information to look for protocol compliance, spam, viruses, intrusions, and other criteria. It is possible to circumvent with certain encryption technologies.
B. DPI analyses data and header information to look for protocol compliance, spam, viruses, intrusions, and other criteria. It is not possible to circumvent.
C. DPI refers to the Dots Per Inch on a computer monitor, so circumventing DPI isn't applicable.
D. DPI refers to Datagram Packet Intrusions, which are a form of network-layer attack. They are possible to circumvent.
E. DPI refers to Datagram Packet Intrusions, which are a form of network-layer attack. They are not possible to circumvent.

---

3. Which of the following are mediums that a virus can travel through to infect hosts? Select all that apply.

A. Emails
B. Downloads
C. Network infrastructure
D. Encrypted hard drives
E. Public Wi-Fi
F. None of the above
G. All of the above

---

4. Which of the following accurately describes the term *phishing*? Choose the best answer.

A. Phishing is the practice of trying to attack systems on a LAN with session-hijacking software.
B. Phishing refers to using protocol analyzers and packet sniffers to mine sensitive data.
C. Phishing is a social engineering technique whereby an attacker calls a target and impersonates technical support personnel in order to trick the target into forfeiting their login credentials.
D. Phishing is the practice of setting up fake and malicious websites with bogus URLs that mimic real URLs in an attempt to capture login credentials before forwarding a user on to the correct URL.

---

5. True or false? XSS is a type of attack whereby the attacker injects malicious database code designed to break database systems with improperly sanitized data?

A. True.
B. False.

---

6. Which of the following, if any, describes the IEEE 802.1X specification?

A. 802.1X is the latest and greatest wireless connection standard as of 2016
B. 802.1X is the latest Ethernet standard, which supersedes 10Gigabit Ethernet with speeds as fast as 100Gb
C. 802.1X is the Extensible Authentication Protocol Over LAN, or EAPOL
D. 802.1X is the IEEE implementation of AES-256-bit encryption

---

7. Which of the following correctly lists the chronological development of IEEE wireless technologies, from oldest to newest? Select the correct answer.

A. 802.11A, 802.11B, 802.11G, 802.11AC, 802.11N
B. 802.11A, 802.11B, 802.11G, 802.11N, 802.11AC
C. 802.11B, 802.11A, 802.11G, 802.11AC, 802.11N
D. 802.11B, 802.11A, 802.11AC, 802.11G, 802.11N

---

8. True or false? NAT can only translate private RFC 1918 addresses to public addresses.

A. True.
B. False.

---

9. ARP spoofing is commonly employed to facilitate which types of attacks? Select all that apply.

A. MitM (Man in the Middle) attacks
B. Trojan virus propagation
C. Malicious DNS redirects
D. VLAN hopping-based attacks
E. Zero-day threats
F. SYN attacks

---

10. What is a flood guard, and what types of attacks do they help prevent? Select all that apply.

A. Flood guards is a preventative measure against DoS techniques, such as a SYN attack.
B. Flood guards are an STP feature, and help prevent broadcast storms.
C. Flood guards are a QoS mechanism, and help stop one computer from eating up all of a network's LAN bandwidth.
D. Flood guards are a QoS mechanism, and help stop one computer from eating up all of a network's WAN bandwidth.

---

11. Which of the following accurately describes LEAP and where it is commonly implemented? Select the best answer.

A. LEAP is a lightweight version of TLS proprietary to Juniper Networks, and it is commonly implemented in Ethernet connections.
B. LEAP is a lightweight version of EAP proprietary to Juniper Networks, and it is commonly implemented in wireless connections.
C. LEAP is a lightweight version of TLS proprietary to Cisco Systems, and it is commonly implemented in Ethernet connections.
D. LEAP is a lightweight version of EAP proprietary to Cisco Systems, and it is commonly

implemented in wireless connections.

---

12. What does the TKIP protocol acronym stand for, and what does it do? Select the best answer.

A. TKIP stands for Temporal Key Interchange Protocol, and it helps secure WAN connections.
B. TKIP stands for Temporal Key Integrity Protocol, and it helps secure wireless connections.
C. TKIP stands for Telemetry Key Interchange Protocol, and it provides encryption for TCP connections.
D. TKIP stands for Telemetry Key Integrity Protocol, and it is a hashing operating to check the validity and integrity of received data.

---

13. Which of the following accurately describes an SLA? Select the best answer.

A. An SLA is Simple LAN Authentication, and is a way of establishing secure connections on a local network.
B. An SLA is Symmetric Layer Algorithm, which provides security between two remote systems by establishing connections at the same layer of the OSI model – namely the Session and Presentation Layers.
C. An SLA is a contract between an ISP and a customer that outlines the expected level of service, such as uptime, raw bandwidth, QoS, and other parameters.
D. An SLA is a Service Level Agreement, and establishes the encryption key length during VPN tunnel negotiation.

---

14. Which of the following accurately describes Change Management and its role in an organization? Choose the best answer.

A. Change management is an I.T. security role in which the professional administers system updates whenever there is a change, such as a new zero-day threat discovery.
B. Change management refers to managing firewall configurations specifically, such as updates, edits, and deletions of any rule sets configured on the firewall.
C. Change management is an auditing process to record any system configuration changes made on a network to keep the security policy updated with the most recent threats.
D. Change management is a formal process defined by an organization in order to minimize any negative impacts of configuration changes.

15. Which of the following correctly lists data in its most volatile state to its least volatile state, according to forensics and the Order of Volatility? Select the best answer.

A. Memory, swap files, network processes, system process, file system data, raw disk blocks
B. System processes, memory, swap files, network process, raw disk blocks, file system data
C. Memory, swap files, network processes, file system data, raw disk blocks, system process
D. Swap files, network processes, system process, file system data, raw disk blocks, memory
E. Memory, network processes, system process, swap files. file system data, raw disk blocks

---

16. Which of the following are training and user awareness factors that need to be communicated to employees to strengthen the security of the workforce? Select all that apply.

A. Password strength
B. Data handling
C. XSS vulnerabilities
D. Clean desk policies
E. BYOD and personally owned devices
F. Antimalware operation

---

17. Which of the following are fault tolerance mechanisms designed to incorporate redundancy into computer systems to avoid catastrophic mission critical failure? Select all that apply.

A. RAID
B. Load balancers
C. Clustering
D. VPN concentrators
E. Personal external HDDs

---

18. Which of the following classify as a type of malicious software (e.g. malware). Select all that apply.

A. Viruses
B. Keyloggers
C. MitM attacks
D. Ransomware
E. Rootkits
F. Trojans
G. Adware

---

19. Which of the following accurately describes a botnet? Choose the best answer.

A. A botnet is a computer network that uses procedurally generated parameters such as automatic protocols like DHCP.
B. A botnet is a group of computers that are illegally controlled by an attacker, despite the owners' knowledge, to carry out other attacks such as propagating spam and malware and launching DDoS attacks.
C. A botnet is a network of computers that are used to host cloud services; the botnet only provides network functions as a platform to server higher level functions and only operates at the bottom layers of the OSI model (a bottom-network).
D. A botnet is a collection of computers that pool their resources through clustering for higher levels of power and efficiency.

---

20. Which of the following correctly describes spear phishing? Select the best answer.

an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data

A. Spear phishing is a penetration test designed to pinpoint a single system and scan for all available open ports on one host.
B. Spear phishing is a type of DoS attack that targets a single server or host system with precision.
C. Spear phishing is a technique used by attackers whereby they setup a fake website, which looks like a legitimate website, in order to capture login credentials before forwarding the user onto the appropriate legitimate website.
D. Spear phishing is an attempt by an attacker to gain unauthorized access to sensitive, personal, and confidential information by using dubious attack techniques through email, fraud, and spoofing to target a single organization.

1.
Correct answer: B, C, D, and E.

Explanation: Most packet filtering firewalls operate mainly in layers 2 through 4 of the OSI model. However, there are many advanced firewalls that can perform advanced types of inspection and even manipulate and filter data in higher levels, such as Session data. For instance, advanced firewall mechanisms can even rate limit transport protocols such as TCP/UDP connections via QoS.

2.
Correct answer: A.

Explanation: DPI stands for Deep Packet Inspection, and is an advanced feature of firewalls to make extremely intelligent decisions regarding forwarding, blocking, QoS, and other actions. Nevertheless, it is actually possible to circumvent DPI, especially with various types of encryption and VPN functionality.

3.
Correct answer: A, B, C, E.

Explanation: Though viruses can lie dormant on hard drives, HDDs (be they encrypted or not) aren't typically one of their transmission mediums. Instead, they are spread more readily through email, downloads (poisoned links, Bit Torrent, etc.), throughout LANs and networks, and even on a host-to-host basis over public Wi-Fi.

4.
Correct answer: D.

Explanation: Phishing consists of trying to setup a fake website that mirrors a legitimate site, only the URLs are slightly different. For instance, a fake website could use a '0' character instead of an 'o' character if they were trying to phish for 'faceb00k' passwords. Though not a necessity, the attacker will then usually forward the user onto the appropriate website to avoid arousing suspicion and meriting unwanted attention.

5.
Correct answer: False.

Explanation: False. Injecting malicious database code is an SQLi (SQL injection) attack. XSS is an attack, usually targeting websites, that works by running malicious scripts to access sensitive information.

6.
Correct answer: C.

Explanation: 802.1X is a security algorithm based on EAP, and it is used for LAN connections. Hence, it is aptly called EAPOL for short.

7.
Correct answer: B.

Explanation: 802.11AC is the latest and greatest wireless connection standard to date, though there is always another one looming around the corner as the IEEE ratifies new standards.

8.
Correct answer: B.

Explanation: False. It is true that one of the main driving reasons why NAT (Network Address Translation) was created was to slow the exhaustion of finite IPv4 addresses by allowing multiple private IP addresses to share a single public address. However, there are many types of NAT, and it is possible to translate one private address to another address as well as translate one public address to a different public IP address.

9.
Correct answer: A.

Explanation: MitM attacks occur when an attacker places their computer within the path of two other systems' transmissions. Because data flows through the attacker's network interface, they can capturer user data. On a LAN, an attacker can spoof their MAC address using ARP, causing the router to believe the attacker is the correct destination host, and tricking the target host into thinking the attacker's computer is the router.

10.
Correct answer: A.

Explanation: DoS attacks work by flooding a target with too many requests in order to overwhelm the host. Though there are many types of preventative measures to protect against DoS and DDoS attacks, flood guards are still an effective mitigation and prevention tool.

11.
Correct answer: D.

Explanation: LEAP is proprietary to Cisco Systems. LEAP is based of off Extensible Authentication Protocol, but LEAP was streamlined for better efficiency and use in wireless connections.

12.
Correct answer: B.

Explanation: TKIP is the Temporal Key Integrity protocol, and is used to help secure wireless connections. It is much more secure than older standards, and was created to fill the security gap that weak standards like WEP created.

13.
Correct answer: C.

Explanation: An SLA is a Service Level Agreement, and helps two parties determine levels of service quality when purchasing digital services, such as a leased WAN connection. The SLA often helps guide contracts, and can include topics such as policing, traffic shaping, Quality of Service parameters, bandwidth, protocol configurations, and uptime guarantees.

14.
Correct answer: D.

Explanation: Change management exists to ensure that no one accidentally makes a configuration that negatively impacts a customer's service. For instance, if I wanted to edit a VPN server

configuration at the behest of a higher-level authority within an organization, I would first need to go through the proper change management procedures to gain approval before making the configuration.

15.
Correct answer: A.

Explanation: The Order of Volatility helps to describe how easily data is lost dependent upon what type of data it is and the type of medium that it is stored on. Memory is highly volatile because it needs a constant flow of electricity to store data. Hard drives, on the other hand, don't need constant electricity because they use magnetic charges to store information, so HDDs have the lowest volatility ranking.

16.
Correct answer: A, B, D, E.

Explanation: The only two options that aren't typically used for training and general user awareness procedures are XSS vulnerabilities and antimalware operation. XSS and antimalware is usually the responsibility of an organization's I.T. department.

17.
Correct answer: A, B, C.

Explanation: The only two options that aren't truly fault tolerance mechanisms are VPN concentrators and personal external HDDs. Though HDDs do provide redundancy for personal data, they typically aren't implemented in business environment. Instead, cloud storage, storage, servers, and RAID configurations are used to securely store redundant copies of data to prevent data loss.

18.
Correct answer: A, B, D, E, F, G.

Explanation: MitM attacks are the only option listed that isn't truly a form of malware, though they are dangerous nevertheless. MitM attacks are typically a manual procedure, whereby an attacker personally operates software – though in some situations partial scripting could be used. All other options are types of code that, after infecting a host system, operate automatically as malware.

19.
Correct answer: B.

Explanation: Botnets are collections of 'zombie computers' that are controlled without the knowledge of the owner. The attacker can gain a lot of advantages from having these zombie computers do their bidding, such as being able to overwhelm resources from varied IP addresses (such as in a DDoS attack) or using their computing resources to spread viruses.

20.
Correct answer: D.

Explanation: Spear phishing is simply another type of phishing maneuver, though it targets a specific organization or network. C is incorrect because it simply describes traditional phishing.