UPGRADE YOUR SKILL

IT SECURITY PRACTICE TEST QUESTIONS

Practice Test 3

1. Which of the following identifies a wireless network, and *usually* (though not always) corresponds with a single VLAN or subnet? Select all that apply.

A. Channel Number (1-13)
B. VLAN Identification Number
C. Wireless Fidelity Identification
D. Extended Service Set
E. Service Set Identifier
F. Basic Service Set

---

2. Why would a network engineer or security professional want to disable the setting that allows a wireless access point or wireless router from broadcasting its SSID? Select all that apply.

A. Disabling SSID broadcast makes the wireless network harder to discover and 'hidden,' so it is less likely to be targeted in an attack.
B. Disabling SSID broadcast saves power, which is crucial in today's green network policies.
C. Disabling SSID broadcast prevents unencrypted transmissions, thereby strengthening security.
D. Disabling SSID broadcast will stop wireless clients from connecting to the wireless device.

---

3. Which of the following wireless security algorithms provides the strongest security? Select the best answer.

A. WPA2
B. SSH
C. WPA
D. WEP
E. WAP
F. WAP2
G. WEP2

---

4. Which of the following wireless security algorithms are so antiquated that it shouldn't be used in any real-world implementation, owing to the fact that it can be easily broken in a short amount of

time? Select all that apply.

A. WPA2
B. Wi-Fi Encryption 1.0
C. WEP
D. Extensible Authentication Protocol
E. AES-256
F. GRE

---

5. Which of the following protocols and algorithms combine TLS (Transport Layer Security) with EAP (Extensible Authentication Protocol), thereby improving the connection with enhanced encryption and authentication? Select all that apply.

A. GRE
B. TLS/IPsec
C. PEAP
D. EAPv2
E. EAPv3
F. None of the above.
G. All of the above.

---

6. Network engineers and security professionals need to be extremely mindful of wireless antenna placement and direction, especially to prevent which of the following threats? Select the best 2 answers.

A. Rogue AP sniffing
B. War driving
C. War chalking
D. Promiscuous wireless captures
E. Other AP's placed in Monitor mode

---

7. Which of the following protocols and algorithms are commonly used to provide authentication functions on both point-to-point connections as well as wireless connections? Select all that apply.

A. PPPoE (Point-to-Point tunneling Protocol over Ethernet)
B. EAP
C. PPP (Point-to-Point tunneling Protocol)
D. LDAP
E. Active Directory
F. L2TP/IPsec
G. TLS

---

8. Is it possible (on most wireless access points) to change the wireless range? If so, which settings would allow a professional to extend the range of the wireless signal? Select the best answer.

A. No, it is not possible.
B. Yes, simply perform a 30/30/30 reset on the router to unlock greater signal range.
C. Yes, simply switch the channel number to a higher number, ranging from 1-13.
D. Yes, simply configure the power level controls.
E. None of the above.

---

9. Which of the following terms describes actions and configurations a network administrator can take to secure physical connections, such as by implementing NAC based on each network card's globally unique physical 48-bit address? Select the best 2 answers.

A. Port security
B. Time-delimited NAC
C. Lock-and-key admission control
D. MAC filtering
E. ACL
F. Time-based ACL
G. IP address filtering

---

10. If an IDS detects network traffic and labels it as an intrusion, though the traffic is actually legitimate, what would this situation be called? Select all that apply.

A. Anomaly
B. False negative

C. False positive
D. Error

---

11. Which of the following outlines best practices regarding personal data and its management in a secure fashion? Choose the best answer.

A. Privacy policy
B. Acceptable use policy
C. Terms of service
D. Security policy
E. Threat mitigation policy
F. Social engineering mitigation policy

---

12. Which of the following are vital components of cryptographic protocols? Select all that apply.

A. Authentication mechanisms
B. Integrity checks
C. Symmetric encryption keys
D. Public keys
E. Shared secrets
F. None of the above
G. All of the above

---

13. True or false? It is not only advised, but rather a *necessity*, to make sure that users within an organization connect to web servers using HTTPS every time they load a web page, regardless of what information they are accessing online.

A. True.
B. False.

---

14. Which of the following correctly identifies bluesnarfing? Choose the best answer.

theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other device

A. Bluesnarfing is the theft of personal data by taking advantage of free public Wi-Fi as the attack's medium.
B. Bluesnarfing is the theft of personal data by taking advantage of an open Bluetooth connection.
C. Bluesnarfing is like war driving, but instead of trying to break into wireless networks, hackers try to break into bluetooth networks.
D. Bluesnarfing is the practice of targeting lonely or sad employees (e.g. 'blue' employees) with social engineering techniques to steal sensitive login credentials.

---

15. Which of the following correctly describes a rogue access point? Choose the best answer.

A. A rogue access point is an access point that has been infected with a virus, and is trying to maliciously harm and control other access points as a result of the infection. l
B. A rogue access point is a WAP that has been added to the network without the knowledge and permission of the I.T. department.
C. Rogue access points are wireless networks that aren't visible because they don't broadcast their SSID.
D. Rogue access points are any access points without any wireless encryption or those that use outdated protocols such as WEP.

---

16. What is the difference between a vulnerability and an exploit? Choose the best answer.

A. A vulnerability represents a flaw in a computing system that could be taken advantage of, but an exploit is the act of preying upon the weakness in a definable way.
B. A vulnerability exists when a hacker installs viruses remotely, but an exploit is the code running in the background that infects the target system.
C. A vulnerability is any method that can be used to break into another system, and an exploit is a way to patch up security flaws.
D. Vulnerabilities are temporal whereas exploits are static.

17. Which of the following statements is true regarding RSA? Select the best answer.

A. RSA uses a public key, its encryption key is different from the decryption key, and has the ability to use keys 2048-bits long.
B. RSA uses a private key only, its encryption key is different from the decryption key, and has the ability to use keys only 256-bits long.
C. RSA uses a public key, its encryption key is identical to the decryption key, and has the ability to use keys 128-bits long.
D. RSA uses a private key only, its encryption key is identical to the decryption key, and has the ability to use keys 1998-bits long.

---

18. Which of the following correctly states one of the main ways TCP is different from UDP? Select all that apply.

A. TCP has an encryption mode to provide transport-layer security. UDP does not.
B. UDP has an encryption mode to provide transport-layer security. TCP does not.
C. UDP uses acknowledgements, which is a system to ensure that every packet of data is successfully received by the end system without corrupted data. TCP does not.
D. TCP uses acknowledgements, which is a system to ensure that every packet of data is successfully received by the end system without corrupted data. UDP does not.

---

19. Which of the following lists units of data, starting at the bottom of the OSI model and working towards higher levels, in correct order? Choose the best answer.

A. Bit, byte, frame, segment, packet
B. Bit, frame, packet, segment
C. Packet, segment, frame, byte, bit
D. Segment, packet, frame, bit
E. Frame, bit, segment, packet
F. Packet, segment, bit, frame
G. None of the above

---

20. FTPS is intended to be a more secure version of FTP (File Transfer Protocol). What features does it improve upon standard FTP, and what underlying technologies provide these functions? Select all that apply.

A. FTPS adds encryption to the connection by using TLS and SSL.
B. FTPS adds encryption to the connection by using an L2TP tunnel.
C. FTPS adds encryption to the connection by using an L2TP/IPsec tunnel.
D. FTPS adds authentication to the connection by using SHA-256.
E. FTPS adds authentication to the connection by using SHA-128.
F. FTPS adds authentication to the connection by using 9-factor authentication.
G. None of the above

1.

Correct answer: E.

Explanation: SSID, or **S**ervice **S**et **ID**entifier, helps humans identify a wireless network by naming it with characters which are easily understood and remembered by humans. Most typically, a single SSID will correspond with a single VLAN or subnet, though there are some rare exceptions to the rule. The channel number, though important, only helps to keep multiple wireless signals from interfering with each other. Answers B and C are fictional, and answers D and F are simply incorrect.

2.
Correct answer: A.

3.

Correct answer: A.

Explanation: Several of the answers aren't even wireless security algorithms, such as SSH, WAP, WEP2, and WAP2. Of the remaining answers, only WPA2, WPA, and WEP are wireless security algorithms. WEP is the oldest and least secure, and it can be easily cracked using simple tools in Kali Linux for free. WPA2 is the latest wireless security standard listed above, and it is the most secure.

4.

Correct answer: C.

Explanation: WEP, or Wired Equivalent Privacy, is antiquated, outdated, and deprecated. Even teenagers can crack WEP encryption with little to no background in computer systems by using simple tutorials and downloading free Kali Linux wireless cracking tools.

5.

Correct answer: C.

Explanation: Protected EAP improves upon EAP by adding encryption using SSL and TLS. The other options are either bogus protocols or tunneling options that don't even provide encryption (e.g. GRE).

6.
Correct answer: B, C.

Explanation: War driving consists of driving around, looking for weak points in wireless infrastructures – especially for weaker protocols like WEP security as to crack it and gain entry to the network. War chalking is the practice of using special chalk symbols to let others know about Wi-Fi access and possibly credentials. If wireless signals are strong enough in unintended areas, it will be possible for attackers to engage in these practices.

7.

Correct answer: B.

Explanation: EAP is the only protocol listed above that works on wireless connections as well as point-to-point connections. The other options either don't work on both types of connections, don't provide authentication, or aren't true network protcols in the case of Active Directory.

8.
Correct answer: D.

Explanation: Power level controls can be configured on most routers, even in home settings though especially with business-class hardware. These settings can be used to increase power and adjust the strength and signal range of wireless connections.

9.
Correct answer: A, D.

Explanation: Port security and MAC filtering are both techniques used to control who or what devices can access a physical switch port. MAC addresses are, of course, 48 bits in length. If an administrator filtered all MAC addresses on an interface except one, no other computer could use that port unless they were somehow able to obtain the correct MAC address and spoof it.

10.
Correct answer: C.

Explanation: antivirus too When the alarm bell sounds but no emergency is present, it's known as a false positive. However, false positives aren't only prevalent in network intrusion and detection devices. They are commonly found with antivirus and antimalware programs, especially regarding PUPs (potentially unwanted programs).

11.

Correct answer: B.

Explanation: The acceptable use policy helps define how end users should use their devices, personal data, and the network resources.

12.
Correct answer: G.

Explanation: All of the options are components that make up cryptographic protocols.

13.
Correct answer: B.

Explanation: Though it would be nice if all web server connections were secured with HTTPS, it simply isn't feasible because HTTPS isn't implemented with every web server, so requiring users to secure their connections with HTTPS isn't feasible. However, Google has made HTTPS a ranking signal to their search results algorithm, which drastically encourages its use by web administrators.

14.
Correct answer: B.

Explanation: All other options are illegitimate. Unsecured Bluetooth connections represent a

gaping security hole, so Bluetooth should be turned off when not in use for greater security.

15.
Correct answer: B.

Explanation: Rogue access points impose a large security risk for a network because they are often installed by non-technical users who simply want their own personal Wi-Fi signal. Often they are configured to use little to no wireless security, and unknowing end users can select protocols such as WEP instead of WPA2.

16.
Correct answer: A.

Explanation: A vulnerability is a flaw that leaves the door open for a potential attack. An exploit is either the act of taking advantage of a vulnerability or a well-defined procedure for attacking a vulnerability.

17.
Correct answer: A.

Explanation: The RSA algorithm can use a public key where the encryption key is different than the decryption key. Also, though there are different key lengths, you'll find that longer keys (such as 2048-bits) are more secure than shorter keys.

18.

Correct answer: D.

Explanation: Though there are several differences between UDP and TCP, the largest difference is that TCP uses acknowledgements and sequence numbers to account for each an every piece of data sent. If a packet gets drop during times of congestion through the Internet (or for other reasons), TCP can notice that the data didn't reach it's destination and resend the lost data. That's one reason why UDP is a faster protocol that's more appropriate for voice and real-time applications.

19.
Correct answer: B.

Explanation: Bits exist at the physical layer, frames are units of data at the Data-Link layer, packets are units of data at the network layer, and segments are units of data sent at the transport layer. Each unit of data is packaged in the next-lowest layer's data type like a Russian nesting doll before being forwarded, and then unpacked in the reverse direction on the receiving machine.

20.
Correct answer: A.

Explanation: The only valid answer is that FTPS, or FTP-Secure, adds encryption using SSL/TLS. Doing so helps protect the file's data from being intercepted and stolen by hackers, attackers, and eavesdroppers.