1. In an SQLi attack, what is the target, and what gets injected to facilitate the attack? Choose the best answer.

A. An SQL database is the target, and Brute Force password attacks are injected.
B. An LDAP server is the target, and a virus is injected.
C. A website is the target, and malformed SQL query statements are injected.
D. An SQL database is the target, and malformed SQL query statements are injected.
E. None of the above.

Correct answer: D.

Explanation: SQLi attacks can target any system where the attacker has access to database query syntax due to improper sanitized data. Though web pages are susceptible to SQLi, more broadly, any database without proper mitigation techniques can be targeted.

2. Which of the following, if any, are one of the security threats associated with social media access on corporate-owned devices? Select all that apply.

A. Decreased employee productivity.
B. Data leaks and a loss of trade secrets, intellectual property, corporate strategies, and proprietary data.
C. Embarrassing photos that may devalue the firm's reputation.
D. Password attacks designed to steal Facebook and Twitter login credentials.
E. None of the above.

Correct answer: B.

Explanation: Though many of the other answers are related to a loss of privacy and professionalism, the best answer is a loss of the firm's private information.

3. Virtualization technologies are not without their own flaws. While they do enhance security by isolating operating systems and services, they do carry certain risks. Which of the following are risks of virtualized servers? Select all that apply.

A. One virus can wipe out an entire cluster.
B. Implementation can take a lot longer since virtual servers require inordinately larger amounts of configuration than traditional servers.
C. Virtual servers are more susceptible to DoS attacks since they only have one network interface.
D. One hardware failure or issue can affect multiple services and hosts.
E. None of the above.

Correct answer: D.

Explanation: Virtualized servers are actually more secure than traditional servers due to OS isolation, though hardware issues can impact multiple machines simultaneously. However, most virtual servers use hardware redundancy to mitigate such an occurance.

4. Which of the following represent the best ways to protect and secure operating systems from viruses and malware? Select all that apply.

A. Install antimalware and antivirus software.
B. Keep the HIPS signatures updated.
C. Harden the software by turning off and disabling all unnecessary features and services.
D. Connect the system directly to a firewall's LAN port for increased security.
E. None of the above.

Correct answer: A, B, C.

Explanation: D is the only answer that is incorrect. It's actually pretty rare to connect hosts in a corporate environment directly to a firewall. Instead, routers and switches are used to segment the network.

5. Which of the following protocols is the most common way of accessing remote systems, such as Linux servers, routers, switches, and other networking devices securely? Choose all that apply.

A. Telnet.
B. Remote Desktop Protocol
C. SSH
D. Remote access software like LogMeIn and TeamViewer
E. None of the above

Correct answer: C.

Explanation: SSH is the most common command line tool used to remotely access devices via a terminal window. Telnet is antiquated because it doesn't secure the connection with encryption.

6. True or false? It is best to run multiple instances of antivirus and antimalware security software to drastically reduce the chance of a security breach.

A. True
B. False

Correct answer: B

Explanation: False. There are actually a lot of problems and issues that crop up when running multiple versions of security software. Not only will the software conflict with each other, but they can cause performance issues and generate more false positives.

7. Windows Defender should be utilized on Microsoft systems to mitigate the risk of malware, spyware, and viruses. True or false?

A. True
B. False

Correct answer: B.

Explanation: Windows Defender is Microsoft's answer to spyware and malware threats. However, it isn't as adept at handling, identifying, and removing threats as other third-party software. Because it can cause a lot of system conflicts, it should be disabled if you're running thrid-party antivirus tools.

8. You have recently setup new operating system environments for field agents at your firm and performed a fresh installation of the latest operating system. Which of the following should you do to further ensure that the computers are adequately protected from the latest threats? Select all that apply.

A. Create an initial backup image of the OS to provide the earliest recovery point.
B. Install the operating system's latest service pack, patches, and updates.
C. Record the users' login credentials in your personal password manager in case they forget their password.
D. Configure a software firewall to run in conjunction with antivirus software.
E. None of the above.
F. All of the above.

Correct answer: A, B, D.

Explanation: You shouldn't record any users' personal login passwords within your personal password manager. There are ways to access users' login accounts through authentication servers for administrative purposes.

9. Which of the following types of attacks, if any, can a virtualized web browser solution protect a user from? Select all that apply.

A. Social engineering attacks
B. Brute force password attacks
C. Malware
D. Malicious scripts
E. Session hijacking
F. None of the above
G. All of the above

Correct answer: C, D, E.

Explanation: Since the web browser is virtualized and not running as a traditional browser would on a local machine, malware and malicious scripts are mitigated. In addition, session hijacking is mitigated as well since the cookies aren't sent to the local OS.

10. Your firm has recently installed new virtualized servers, and most of the operating systems' applications and services are set to the default values. What should be done to minimize security risks from attacks that scan, identify, and make connections on open ports? Select all that apply.

A. Leave the settings at their default values, since an operating is most secure when it's newly installed.
B. Lock down access to the new servers to only one administrative user account.
C. Shut down all unnecessary servers and applications.
D. Use the software firewall to restrict connections for any ports and protocols that are not in use.
E. None of the above.

Correct answer: C, D.

Explanation: Frequently with new server installations, you'll find that a lot of ports and services are running that don't need to be. This is a massive problem because hackers can scan for open ports and try to make connections on them.

11. Which of the following options is *not* a typical part of a password policy? Select all that apply.

A. Forbid users to write their passwords down on paper and other physical mediums.
B. Require users to create complex passwords.
C. Require users to to regularly update their passwords in set intervals.
D. Require users to incorporate special characters into their passwords.
E. None of the above.

Correct answer: A.

Explanation: This was a bit of a trick question. It is poor security practice to write down passwords on sticky notes attached to desktop towers and monitors, since they violate clean desk policies and defeat the purpose of a password. But in some rare cases, it is acceptable to write down passwords, so long as they are stored in a safe location offsite, such as within a vault or safe.

12. You work for a medium-sized firm that keeps a lot of inventory on hand, as well as research and development data in an in-house server farm. Which of the following are needed to successfully monitor the premises?

A. Firewall logs that look for suspicious connections.
B. Wireless access point logs that record every MAC address of locally connected devices.
C. CCTV cameras to record on-site activity.
D. Security key cards and biometric scanners.
E. None of the above.

Correct answer: C.

Explanation: While the other options have desirable advantages, there is only one solution that helps to *monitor* the premises.

13. Windows is known for it's share of faults, and often crashes, especially when the system is strapped for hardware resources. If you needed to shut down malfunctioning processes without shutting down or rebooting the entire system, which of the following should you use or configure? Select all that apply.

A. Windows Defender
B. Windows Firewall
C. Task Manager
D. Ctrl + Alt + Delete
E. None of the above

Correct answer: C.

Explanation: The Task Manager is the only option that will actually allow you to shut down a process. The Ctrl + Alt + Delete key sequence, however, can be used to actually reach the Task Manager.

14. Windows is inherently flawed with it's default settings, and will allow file sharing on fresh systems. As an I.T. engineer and member of the security team, you have been tasked with making sure that no end-user workstations share files by default in a Windows environment. Where in the operating system should you make this configuration change? Choose the best answer.

A. The Control Panel
B. The Network and Sharing Center
C. The Task Manager
D. Windows Firewall
E. None of the above

Correct answer: B

Explanation: These changes should be made in the Network and Sharing Center. Though this is technically reachable via the Control Panel, the Control Panel is not the best answer. Also, Windows Firewall and the Task Manager don't have the ability to shut off file sharing.

15. Which of the following security qualities apply to the act of securing Internet connections when trying to prevent hackers and thieves from getting their hands on payment card information? Choose the best answer.

A. Authentication
B. Integrity
C. Hash
D. Confidentiality
E. Encryption
F. None of the above

Correct answer: D.

Explanation: Because you are trying to prevent others from seeing the payment card and account number, this is technically a protection of confidentiality. Authentication, data integrity, and encryption are all components of data security, but are not the best answer.

16. Which one of the following is the best option regarding the training end-users need to mitigate security risks? Choose the best answer.

A. How encryption works on a technical level.
B. How to install antivirus and antimalware software on their computers.
C. How to manually kill suspicious processes.
D. How to identify and react to social engineering attempts.
E. None of the above.

Correct answer: D.

Explanation: By and large, end users have no need or desire to learn how security concepts work on a technical level, and the last thing I.T. support staff want an end user doing is tinkering around with their operating system. Nevertheless, they should be trained to understand social engineering tactics and to respond accordingly.

17. You are troubleshooting a slowly running Linux system, and suspect that a process has a memory leak or is otherwise eating up an inordinate amount of system resources. What command would you enter into the BASH shell to view currently running processes?

A. ps aux
B. cd
C. ls -la
D. sudo apt-get process
E. None of the above

Correct answer: A.

Explanation: **ps aux** is the appropriate command to view running processes. Each process has a number, and you can append that number to the **kill** command to shut down a process. **Cd** is for changing your current working directory, **ls -la** is a version of the list command, and **sudo apt-get process** is a bogus command.

18. You notice that the DNS value on your firm's internal DHCP server isn't set to that of your private DNS server's address. Which of the following could be the problem? Select all that apply.

A. There was a DNS leak, and your users could be using your ISP's DNS servers.
B. There's no such thing as a private, internal DNS server; they are all public.
C. There has been a network intrusion, and an attacker setup their own bogus DNS server to spy on visited websites.
D. This is a common problem, colloquially called a “fetched server.”
E. None of the above.

Correct answer: A, C.

Explanation: DNS leaks are moderately common, but they need to happen immediately. What is most concerning is that this DNS value was set in the DHCP server, which most likely points to an attack. There is no such thing as a fetched server.

19. It's pretty common for users on a network to need to access many systems and services. Instead of needing to login each and every time, an authentication server can be used to simply the practice. After a user has been authenticated, what do they receive from the server as a proof of authentication? Choose the best answer.

A. A password hash
B. Token
C. Checksum
D. Ticket
E. None of the above

Correct answer: B.

Explanation: After successful authentication with the server, the user receives a token as verification of their authentication.

20. PAP is technologically superior to CHAP, since PAP is the new and improved version of CHAP. True or false?

A. True
B. False

Correct answer: B.

Explanation: CHAP is much more secure than PAP, and was designed to be more secure and improve upon PAP's shortcomings.