1. A former employee who worked as a part of the in-house I.T. staff recently found employment at a new firm. However, he still has the ability to log into crucial networks systems, such as firewalls, routers, servers, and other networking equipment. Which one of the following best practices should be observed to stop such a massive security risk from happening in the first place?

A. Delete all traces of the user's account from access servers, such as RADIUS credentials.
B. Leave things as they are in case the user returns to their former role.
C. Regularly run audits to identify vulnerabilities and enforce proper access control.
D. Update the system to use AAD (Automatic Account Deletion).

Correct answer: C.

Explanation: It's inadvisable to permanently delete the user's account because they will need to log into various network resources in their new role. Leaving things the same is also inadvisable because the user would have access to data and systems they no longer have any business accessing. In addition, there's no such thing as AAD, so it's best to run regular permissions audits.

2. There was recently a successful security attack against your employer's network devices and servers. Fortunately, through prudent planning and best practices, a myriad of information was gathered such as network statistics, logs from a security audit, and IDS/IPS logs. What is the name of the concept that describes maintaining possession of these types of evidence legally?

A. Chain of custody
B. Custodial law
C. The EU Data Directive
D. Federal Data Communications Act of 2004
E. There is no concept to describe this event; it simply belongs to your firm since they own the devices that generated the data
F. Statute of limitations
G. None of the above

Correct answer: A.

Explanation: Most of the incorrect answers are simply made up. However, the statute of limitations concerns whether or not a crime happened to far in the past to go to court, and custodial law concerns guardianship and parental rights.

3. Your employer backs up mission critical data in a variety of ways including with safeguards such as disaster recovery, offsite backups, and weekly/monthly,quarterly backups. With exception to keeping vigilant backups on a regular basis, what else must be done to ensure that the mission critical data doesn't suffer from a catastrophic vulnerability?

A. Always keep backup files, even if they're decades old, to ensure that no file ever goes missing.
B. Once in a while (perhaps once per quarter), try to restore data from the backups to ensure the restore procedure works as expected.
C. Save all of the backups on servers running RAID 10 to ensure data isn't lost.
D. Invest in a business account with a service like Dropbox to provide an extra layer of redundancy and protection.

Correct answer: B.

Explanation: It is absolutely critical to test the restore process. If something went wrong or there was a flaw in the restore procedure of the backup software that caused a restore to fail, all of the backups would essentially be worthless. Furthermore, Dropbox is incredibly insecure, and it often isn't necessary to keep every single backup job.

4. The head of security at your firm has recently decided to implement browser extensions that force employees to use HTTPS when available to mitigate data leaks and loss of sensitive information, such as login credentials. When one of the employees connects to another system with the HTTPS protocol, what is the *first* thing that happens?

A. A 9-way handshake is completed.
B. The web browser asks the user if they want to proceed and visit the link.
C. A public key is sent from the browser to the server.
D. A private key is sent from the server to the browser.
E. The web browser looks up the certificate information to discern the link's identity.
F. None of the above.

Correct answer: E.

Explanation: The first thing the browser does is download the certificate from the server to check its validity. HTTPS does not use a 9-way handshake, and it doesn't start exchanging keys until the certificate has been verified.

5. You have recently been transferred to the security department of a large firm, and tasked with the maintenance of your company's digital certificate from a Certificate Authority (CA). However, the first thing you notice is that the certificate is going to expire by the end of the month. When *can* you renew the certificate, and when *should* you renew the certificate?

A. On the date that it expires, since it is impossible to renew beforehand.
B. Within a 30-day window prior to expiration.
C. Certificates can not be renewed; a new one must be created, purchased, and activated.
D. After the certificate has expired.
E. None of the above.

Correct answer: B.

Explanation: It's pretty common for Certificate Authorities to send renewal reminders one month prior to expiration. It is intolerable to let the certificate expire, and to let the server run without a certificate.

6. There have been a myriad of breaches and data loss at your firm. After careful inspection of IDS and IPS logs, it was determined by the security department that the attacks were, in part, carried out by using password cracking techniques. Of these techniques, it was determined that Brute Force was used to target weak passwords. Which of the following are especially suited for mitigating the risk of Brute Force attacks? Select all that apply.

A. Make the use of password managers mandatory to prevent password theft.
B. Impose strict guidelines concerning the structure, characters, and length of passwords to make it harder for Brute Force attacks to find the right combination of characters.
C. Force users to change their passwords every 7 days.
D. Lock accounts or bar further login attempts for a certain period of time after 3 failed login attempts.
E. None of the above.

Correct answer: D.

Explanation: Brute Force attacks succeed because they are able to guess thousands upon thousands of password combinations. By restricting them to only 3 login attempts, it becomes virtually impossible for a Brute Force attack to succeed. While the other options are generally good practices concerning password security, they don't help to mitigate Brute Force attempts.

7. You work for a large business with over 4500 employees as an I.T. engineer. To help lock down system access and provide authentication, you have been tasked with implementing network-wide directory authentication via SSO (Single Sign-On). For a firm of this size, which of the following would be most appropriate? Select all that apply.

A. A RADIUM server.
B. Implement Single Sign-On by leveraging the implementation of an LDAP server.
C. Install password managers on all of the end-user workstations.
D. Implement biometric scanners.
E. None of the above.
F. Options A and B.

Correct answer: B.

Explanation: There is no such thing as a RADIUM server in the context of Single Sign-On. LDAP, or Lightweight Directory Access Protocol, is the preferred solution.

8. You work in the I.T. department of a large firm, and you have been tasked with performing a risk assessment to weigh the advantages and disadvantages of implementing virtualization technologies. Which, if any, of the following describe the advantages of virtualization with regards to tradeoffs between cost and security?

A. Virtualization helps to separate services and operating systems in separate zones, thus reducing the chance that a single virus or vulnerability will cause the entire system to crash.
B. Physical security breaches are mitigated since the attacker can't find the hardware tied to the virtual machine (obfuscation).
C. Virtualization applies automatic patches and code updates to the entire system, reducing the chance that an individual OS will fail to load the latest updates.
D. Virtualization technologies don't provide security benefits at all, and instead make service more vulnerable to attack without the right firewall solution.
E. None of the above.

Correct answer: A.

Explanation: Virtual machines are inherently isolated from one another, which reduces the chance of a single bug or problem affecting other servers and services. Furthermore, virtualization saves money by eliminating the need to purchase hardware for each individual operating system instance.

9. There have been numerous attacks against your corporation's network over the last week, and it was determined by the security department that DoS attacks were used to disrupt network services. To mitigate the next attack, an engineer creates a firewall policy that discards traffic from the source IP address of the attacker. Nevertheless, the attacks still continue, despite the new firewall rule. What could be the root problem? Select all that apply.

A. The firewall rule should have been configured to block both the source *and* destination IP addresses of incoming DoS packets.
B. The firewall rule failed to account for IPv6 addresses.
C. The attacker found a way to break into the firewall system, thus allowing packets to be forwarded despite the firewall policy.
D. It's not a DoS attack at all; rather, it's a Distributed Denial of Service attack (DdoS).
E. None of the above.

Correct answer: D.

Explanation: Standard DoS attacks only originate from one source, but distributed attacks come from numerous source IP addresses. To successfully mitigate the attack, the other source IP addresses must be blocked as well.

10. Is it possible to tighten security on wireless networks with MAC filtering, or is MAC filtering only possible on wired networks? Also, what does MAC address filtering do on a network? Select all that apply.

A. Yes, MAC address filtering is possible on wireless networks. It works by using FCP (Firewall Communication Protocol) to download lists of firewall rules and policies to make decisions.
B. Yes, MAC address filtering is possible on wireless networks. It works by blocking connection attempts from individual MAC addresses.
C. Yes, MAC address filtering is possible on wireless networks. It filters IP address bindings to disallow hosts from connecting to WiFi.
D. No, MAC address filtering is not possible on wireless networks. It is only possible on Ethernet conenctions.
E. No, MAC address filtering is not possible on wireless networks. Wireless routers and access points don't have hardware capable of filtering addresses.
F. None of the above.

Correct answer: B.

Explanation: To setup MAC address filtering, an I.T. engineer simply needs to gather a list of MAC addresses not allowed to connect. Alternatively (and more practically), an engineer can setup a rule that bars all MAC addresses from connecting with exception to handful of permitted devices. There is no such protocol as Firewall Communication Protocol.

11. To combat malware and other similar threats, the security section of the I.T. department for a large firm has tasked you with installing antivirus software on users' workstations, and then to subsequently scan the systems. You notice that one system scan identified a virus 30 minutes after installation. What caused the virus to appear? Choose the best answer.

A. The virus infected the host system while you were in the process of installing the software.
B. The virus had likely existed beforehand, but wasn't discovered until the first scan was run.
C. The virus isn't really a virus at all, and is likely a false positive because you haven't had a chance to update the antivirus signatures.
D. The antivirus software you are installing is corrupted, and a virus piggy-backed on its installation.
E. None of the above.

Correct answer: B.

Explanation: While it's certainly possible that the virus is a false positive or is the result of a network-wide worm or virus, the most probable explanation is that the virus had already infected the computer beforehand. It simply wasn't discovered until a scan was run.

12. A high-profile leader of your firm is traveling with corporate-owned devices, such as a company laptop. The data contained on the laptop is highly sensitive and mission critical in nature, and it must be protected at all costs. What can you do to ensure that the leader's laptop is secured? Select the best answer.

A. Encrypt the hard drive to prevent data theft
B. Setup a BIOS password to prevent attackers from using a live-boot utility to access the hard drive
C. Ensure the user always uses a VPN tunnel when connecting to the Internet, especially when using public Wi-Fi
D. Update the OS with the latest service pack, updates, and patches
E. None of the above
F. All of the above

Correct answer: F.

Explanation: All of the above should be performed to secure the laptop and its mission-critical data. Interestingly enough, many people forget to setup a BIOS password, which allows attackers to change the boot order of a device and subsequently boot into the machine with live hard drive utilities, such as Linux.

13. Recently, a lot of the leaders of your organization gathered at their annual conference, and discovered that one of the links populated by the DNS server of the local WiFi turned out to be a link to a phishing site. What is this type of attack called? Choose the best answer.

A. Phishing
B. Fishing
C. Whaling
D. Grumming
E. None of the above

Correct answer: C.

Explanation: Whaling is the practice of targeting high-ranking members of an organization with phishinhg attacks.

14. If you wanted to allow traffic through a firewall, despite the existing configuration and policy rules, which of the following would you create to ensure that the traffic isn't discarded? Choose the best answer.

A. Exception
B. Policy
C. Access control
D. Session
E. None of the above

Correct answer: A.

Explanation: Creating a firewall exception “excepts” traffic from the other rules desitned to discard packets. Thus, the traffic is allowed through the firewall unharmed.

15. Which one of the following options does not represent a biometric-based system of authentication? Choose all that apply.

A. Keycard
B. Voice authentication
C. Fingerprint reader
D. Retina reader
E. None of the above

Correct answer: A.

Explanation: Though most people tend to think of biometric authentication systems as primarily based on eyes and fingerprints, your voice can also be used. Thus, a keycard is the only option that isn't a biometric scanner.

16. There have been numerous data sniffing attacks at your local firm, and it has been decided that the firm's security profile needs to be bolstered with the latest encryption technologies. They decide to consider algorithms that only use PKI. What type of encryption does a PKI system use? Choose the best answer.

A. Symmetric
B. Asymmetric
C. Two-way
D. Private
E. Public
F. None of the above

Correct answer: B.

Explanation: Though it does use both a public and a private key, PKI uses asymmetric encryption.

17. Which of the following types of network devices are extremely vulnerable to data capture software and sniffers, making it a simple matter for an attacker to capture data that wasn't intended to be sent to their computer? Choose the best answer.

A. Firewall
B. Switch
C. Router
D. Hub
E. None of the above

Correct answer: D.

Explanation: A hub doesn't segment a network. Rather, it represents a single network segment that broadcasts data among all connected devices, much like a wireless network. As such, an attacker connected to a hub can capture data from all devices transmitting over that medium.

18. Many times the best defense is a strong offense, so your firm has decided to create a fake network target designed to attract hackers and malicious users, thereby drawing them away from genuinely sensitive data. What is this type of strategy, technique, and implementation known as? Choose the best answer.

A. Cookie
B. Honeypot
C. Scarecrow
D. Dummy-data
E. None of the above

Correct answer: B.

Explanation: A honeypot is a device designed to absorb, identify, or counteract people trying to access systems they have no authorization to access. Usually a honeypot consists of false data that *looks* like a real part of a system, but is in fact, a fake target.

19. You work for a large firm, and they have decided to invest heavily in a consulting firm to come and try to hack into their network. Why on Earth would a company pay another firm to hack into their network? Choose the best answer.

A. To prove to customers and partners that the network is, in fact, truly safe.
B. No business would ever do this in their right mind.
C. To entice other hackers to do the same in an effort to catch them red-handed.
D. To find weak points in the security strategy to identify areas of improvement.
E. None of the above.

Correct answer: D.

Explanation: The whole idea of penetration testing is to find the weakest parts of a security strategy. Then, the white hat hacker, or penetration tester, can give recommendations for how to plug up the security holes.

20. Which one of the following types of attacks is really a type of social engineering attack? Choose the best answer.

A. Honeynet
B. DDoS
C. DoS
D. Vishing
E. None of the above

Correct answer: D.

Explanation: Vishing is a form of voice phishing, whereby the attacker tries to wheedle sensitive information out of unsuspecting users.