Chapter 1: Security fundamentals

Module A: Security concepts

Assessment: Security concepts

1. Someone put malware on your computer that records all of your keystrokes What aspect of security was primarily attacked? Choose the best response.

   - **Confidentiality**
   - Integrity
   - Availability

2. What type of control would a security assessment procedure be? Choose the best response.

   - Management
   - **Operational**
   - Physical
   - Technical

3. Malware is a common example of a threat vector. True or false?

   - **True**
   - False

4. Which controls primarily protect data integrity? Choose all that apply.

   - **Backups**
   - Encryption
   - Fault tolerance
   - **Hashing**
   - Need to know

5. A security program alerts you of a failed logon attempt to a secure system. On investigation, you learn the system's normal user accidentally had caps lock turned on. What kind of alert was it? Choose the best response.

   - True positive
   - True negative
   - **False positive**
   - False negative

Module B: Risk management

Assessment: Risk management

1. Order the steps of a complete risk assessment.

    1. Identify assets at risk
    2. Conduct a threat assessment
    3. Analyze business impact
    4. Evaluate threat probability
    5. Prioritize risks
    6. Create a mitigation strategy

2. Qualitative risk assessment is generally best suited for tangible assets. True or false?

    - True
    - **False**

3. You're shopping for a new A/C unit for your server room, and are comparing manufacturer ratings. Which combination will minimize the time you'll have to go without sufficient cooling? Choose the best response.

    - High MTBF and high MTTR
    - **High MTBF and low MTTR**
    - Low MTBF and high MTTR
    - Low MTBF and low MTTR

4. Your company has long maintained an email server, but it's insecure and unreliable. You're considering just outsourcing email to an external company who provides secure cloud-based email services. What risk management strategy are you employing? Choose the best response.

    - Risk acceptance
    - Risk avoidance
    - Risk deterrence
    - Risk mitigation
    - **Risk transference**

5. What element of your risk mitigation strategy helps keep future additions to your network from introducing new security vulnerabilities? Choose the best response.

    - **Change management**
    - Incident management
    - Security audits
    - Technical controls

Module C: Vulnerability assessment

Assessment: Vulnerability assessments

1. A vulnerability scan can be intrusive or non-intrusive. True or false?
   - **True**
   - False
2. What steps might be taken as part of a vulnerability scan? Choose all that apply.
   - Bypassing security controls
   - Exploiting vulnerabilities
   - **Finding open ports**
   - **Identifying vulnerabilities**
   - **Passively testing security controls**
3. What element of a vulnerability assessment compares security performance to existing security configuration documents? Choose the best response.
   - Architecture review
   - **Baseline review**
   - Code review
   - Design review?
4. What kind of penetration test involves a tester with full knowledge of your network configuration? Choose the best response.
   - Black box
   - Black hat
   - **White box**
   - White hat
5. Vulnerability scanners are a good way to determine a network's attack surface. True or false?
   - **True**
   - False
6. While conducting a penetration test you've just managed to get access to an important server. The main problem is that you got it through a session hijacking attack that took both luck and precise timing, and might be cut off at any time. Given limited time, what should your next step be? Choose the best response.
   - Escalate privileges
   - **Establish persistence**
   - Perform reconnaissance
   - Pivot

Chapter 2: Understanding attacks

Module A: Understanding attackers

Assessment: Understanding attackers

1. What category of attackers are defined by their limited sophistication and reliance on pre-packaged tools? Choose the best response.

   - APTs
   - Hacktivists
   - Organized criminals
   - **Script kiddies**

2. What kind of attacker is an APT most commonly associated with? Choose the best response.

   - Business competitors
   - Hacktivists
   - **Nation states**
   - Script kiddies

3. What category of attacker might also be called cyberterrorists? Choose the best response.

   - **Hacktivists**
   - Nation states
   - Organized criminals
   - Script kiddies

Module B: Social engineering

Assessment: Social engineering

1. What kind of attack is most likely when you're doing sensitive work on your laptop at a coffee shop? Choose the best response.

   - Piggybacking
   - Dumpster diving
   - **Shoulder surfing**
   - Smurfing

2. Impersonation is a core element to most social engineering attacks. True or false?

   - **True**
   - False

3. Several coworkers in the sales department received email claiming to be from you. Each message was personally addressed, and contained a link to a "test site" and a request to log in with normal user credentials. You never sent it, and on examination the supposed test site is a phishing scam. Just what variant of phishing is this? Choose the best response.

   - Pharming
   - **Spear phishing**
   - Vishing
   - Whaling

4. What security controls can protect against tailgating? Choose all that apply.

   - Alarm systems
   - Clean desk policy
   - **Mantraps**
   - **Security guards**
   - Spam filters

5. Social engineering attacks are most commonly either in person or over electronic media rather than on the phone. True or false?

   - True
   - **False**

Module C: Malware

Assessment: Malware

1. A user complains that every time they open their Internet browser, it no longer goes to their preferred home page and advertisements pop up in dialog boxes that they have to close. What is the likely cause? Choose the best response.

   - **Spyware**
   - Trojan
   - Virus
   - Worm

2. A user logs into their computer and is presented with a screen showing a Department of Justice logo indicating the computer has been locked due to the user being in violation of federal law. The screen gives several details of the violation and indicates that the user must pay a fine of $500 within 72 hours or a warrant will be issued for their arrest. The user cannot unlock their system. What type of malware is likely infecting the computer? Choose the best response.

   - Keylogger
   - **Ransomware**
   - Rootkit
   - Trojan
   - Worm

3. What kind of malware can spread through a network without any human interaction? Choose the best response.

   - Polymorphic virus
   - Trojan horse
   - Virus
   - **Worm**

4. You've traced some odd network activity to malware that's infected a whole department's computers. They're processing a distributed task using spare CPU cycles, communicating with a remote server, and sending email to random targets. What kind of malware is it? Choose the best response.

   - **Botnet**
   - Rootkit
   - Spyware
   - Trojan

5. You've found a computer infected by stealth malware. The program installed itself as part of the computer's boot process so that it can gain access to the entire operating system and hide from antimalware software. What kind of malware is it? Choose the best response.

   - Armored virus
   - Backdoor
   - **Rootkit**
   - Spyware

Module D: Network attacks

Assessment: Network attacks

1. Complex passwords that are combinations of upper and lower case letters, numbers, and special characters protect your system from which types of attacks?

   - Birthday
   - **Brute force**
   - **Dictionary**
   - Man-in-the-middle
   - Zero-day

2. As a user, what can you do to protect yourself from man-in-the-middle attacks? Choose the best response.

   - **Avoid connecting to open WiFi routers.**
   - Avoid following links in emails when possible.
   - Enable Firewall protection.
   - Install only the application software you need.
   - Use complex passwords that are combinations of upper and lower case letters, numbers, and special characters.

3. What tools allow amplification of a DoS attack? Choose all that apply.

   - Bluesnarfing
   - **Botnets**
   - **Malformed packets**
   - **Reflection**
   - VLAN hopping

4. Evil twins are mostly used as part of what kind of attack? Choose the best response.

   - Denial of service
   - **Man-in-the-middle**
   - Phishing
   - Trojan horse

5. What kind of attack is against a software vulnerability which hasn't been patched yet? Choose the best response.
   - DDoS
   - Pharming
   - Smurf
   - **Zero day**

Module E: Application attacks

Assessment: Application attacks

1. An attack on your web application began with a long string of numbers sent to a field that's only supposed to hold a four-digit variable. What kind of attack was it? Choose the best response.
   - **Buffer overflow**
   - Integer overflow
   - LDAP injection
   - XSRF
2. What application attacks directly target the database programs sitting behind web servers? Choose all that apply.
   - Command injection
   - Cross-site scripting
   - Session hijacking
   - **SQL injection**
   - **XML injection**
3. What SQL injection technique relies on unfiltered semicolons?
   - Blind injection
   - Signature evasion
   - **Stacked query**
   - XSRF
4. Blocking and cleaning Flash cookies is much the same as for any other browser cookies. True or false?
   - True
   - **False**
5. What XSS techniques don't require anything to actually be stored on the target server? Choose all that apply.
   - **DOM based**
   - Persistent
   - **Reflective**
   - XSRF

6. What application vulnerability can be exploited by providing a series of normal data inputs with a specific sequence and timing? Choose the best response.

   - Buffer overflow
   - Injection
   - **Race condition**
   - Request forgery

Chapter 3: Cryptography

Module A: Cryptography concepts

Assessment: Cryptography concepts

1. Which type of cryptography is most commonly used for key exchange? Choose the best response.
   - **Asymmetric encryption**
   - Hashing
   - One-Time Pad
   - Symmetric encryption
2. What type of cryptography is usually used for password storage? Choose the best response.
   - Asymmetric encryption
   - **Hashing**
   - One-Time Pad
   - Symmetric encryption
3. Order the following encryption ciphers from weakest to strongest.
   1. DES
   2. 3DES
   3. Blowfish
   4. AES
4. Which of the following was originally designed as a stream cipher? Choose the best response.
   - AES
   - Blowfish
   - **RC4**
   - Twofish
5. What asymmetric algorithm uses complex new mathematical approaches to create relatively short but very secure and high-performance keys? Choose the best response.
   - DH
   - **ECC**
   - RIPEMD
   - RSA

6. According to NIST, what is the *effective* strength of a 168-bit 3DES key? Choose the best response.
   - 56-bit
   - **80-bit**
   - 112-bit
   - 168-bit
7. What process gives integrity, authenticity, and non-repudiation? Choose the best response.
   - Diffie-Hellmann key exchange
   - **Digital signature**
   - Hashing
   - HMAC
8. You've received an assortment of files along with accompanying hashes to guarantee integrity. Some of the hash values are 256-bit and some are 512-bit. Assuming they all use the same basic algorithm, what might it be? Choose the best response.
   - MD5
   - RIPEMD
   - SHA-1
   - **SHA-2**

Module B: Public key infrastructure

Assessment: Public key infrastructure

1. What is true of a digital certificate, but not true of a digital signature? Choose all that apply.
   - **Has a valid starting and ending date**
   - Proves the authenticity of a message
   - **Proves the authenticity of a person or system**
   - Provides non-repudiation
2. What defines an EV certificate? Choose the best response.
   - It applies to more than one domain
   - It lasts longer than a normal certificate
   - **It requires a stricter identity verification process on application**
   - It uses stronger cryptography
3. What's generally seen as the most modern and flexible way to find out if a certificate has been revoked?
   - ASN.1
   - CRL
   - CSR
   - **OCSP**

4. Your employer demands a copy of all private keys used on devices you use for work, since regulatory requirements require them to be able to decrypt any official communications when legally requested. What is this an example of?

   - **Key escrow**
   - Key recovery
   - PKI hierarchy
   - Revocation

5. What certificate formats commonly use the web of trust model? Choose the best response.

   - ASN.1
   - Bridge
   - **OpenPGP**
   - X.509

6. What certificate encoding is intended for use in secure email? Choose the best response.

   - CER
   - DER
   - **PEM**
   - PFX

7. An attacker's gotten a fraudulent certificate attesting to be for your bank and is planning to intercept your transactions in a man-in-the-middle attack. The certificate hasn't been revoked yet, but what technology could still let you know something is wrong?

   - Escrow
   - **Pinning**
   - OCSP
   - Stapling

Chapter 4: Network fundamentals

Module A: Network components

Assessment: Network components

1. Order the OSI layers from bottom to top.

    1. Physical
    2. Data Link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application

2. What kind of WAP is designed for use with a central WAN controller? Choose the best response

    - Controllerless
    - Fat
    - Mesh
    - **Thin**

3. What happens to a non-tagged frame on a VLAN trunk?

    - It's flooded to all VLANs the trunk carries.
    - It's forwarded to the lowest-numbered VLAN.
    - **It's forwarded to the trunk's native VLAN.**
    - It's dropped without an error message.

4. What protocol would an echo request packet use?

    - ARP
    - **ICMP**
    - TCP
    - UDP

5. Which storage option is just a refinement of traditional file servers?

    - iSCSI
    - **NAS**
    - SAN

6. You want to create a point-to-point wireless link between two buildings. Your goals are to keep a strong signal between the two transceivers while minimizing the area in which eavesdroppers can access network traffic. What antenna style should you use for each? Choose the best response.

    - Dipole
    - Monopole
    - Patch
    - **Yagi**

Module B: Network addressing

Assessment: Network addressing

1. What might a router using PAT change on packets passing through? Choose all that apply.

    - **Destination port for incoming packets**
    - Destination port for outgoing packets
    - **Destination address for incoming packets**
    - Source address for incoming packets
    - Source port for incoming packets
    - **Source port for outgoing packets**

2. What protocol is used to find the MAC address of a given IP address? Choose the best response.

    - **ARP**
    - DHCP
    - APIPA
    - DNS

3. For a local server, you might not need the full domain name to perform a DNS lookup. True or false?

    - **True**
    - False

4. Which IPv4 address might be valid on the Internet? Choose the best response.

    - 127.0.0.1
    - **150.50.101.32**
    - 169.254.121.68
    - 192.168.52.52

5. What network attack can only be used on local network segments?

    - **ARP poisoning**
    - DNS poisoning
    - DNS spoofing
    - Man in the middle

6. What protocol can be used to prevent DNS poisoning? Choose the best response.

- DHCP
- **DNSSEC**
- FQDN
- PAT

Module C: Network ports and applications

Assessment: Network ports and applications

1. Match the network protocols with their default ports

Telnet	23
SSH	22
SNMP	161
SMTP	25
FTP	21
LDAPS	636
DNS	53
POP	110
IMAP	143

2. You want to securely connect to a server via a command line terminal interface. What protocol should you use? Choose the best answer.

- FTP
- LDAP
- **SSH**
- Telnet

3. How many total packets need to be exchanged for a TCP handshake? Choose the best response.

- 2
- **3**
- 4
- 5

4. What kind of communications would be suitable for UDP? Choose all that apply.

   - **DNS requests**
   - File transfers
   - **Online games**
   - **Streaming video**
   - Website connections

5. Your company's custom server software application needs a TCP port to listen on. What port range should it be configured to use?

   - Private
   - System
   - **User**

6. What protocol would you use to connect to a shared drive on another Windows system? Choose the best answer.

   - AFP
   - FTP
   - **SMB**
   - SNMP

7. HTTPS adds security to HTTP and uses a different port, but otherwise is fundamentally the same. True or false?

   - **True**
   - False

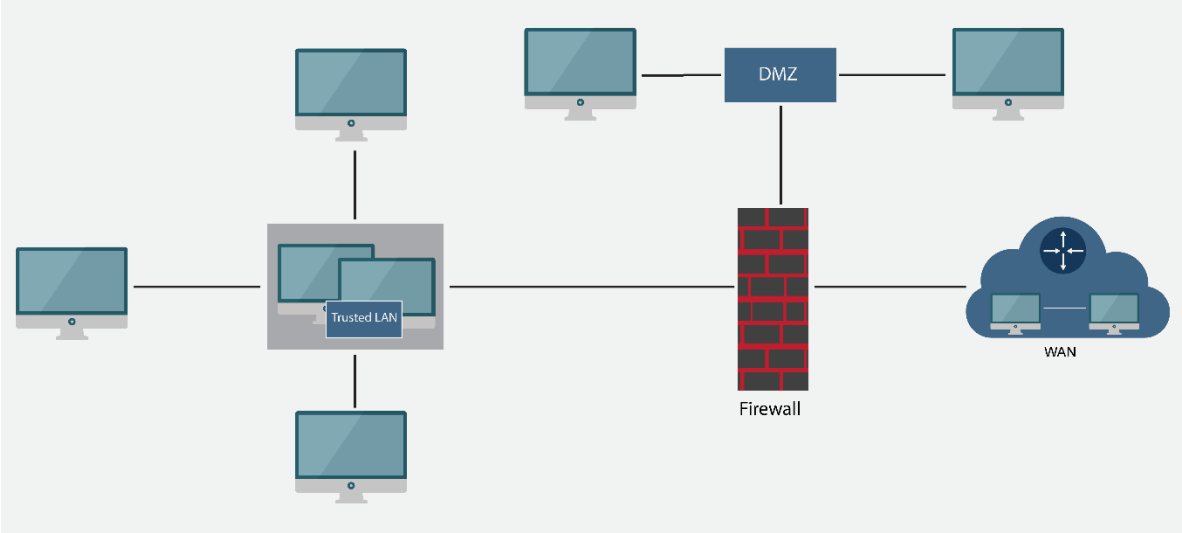
Chapter 5: Securing networks

Module A: Network security components

Assessment: Network security components

1. ACLs are based on which assumption? Choose the best response.
   - Explicit Allow
   - Explicit Deny
   - Implicit Allow
   - **Implicit Deny**
2. When configuring an IDS you might want to allow a few false positives to make sure you never get any false negatives, but not the opposite. True or false?
   - **True**
   - False
3. You're configuring a router, and want it to check the properties of incoming traffic before passing it on. What will this require? Choose the best response.
   - **Configuring ACLs**
   - Configuring routing tables
   - Either would have the same effect
   - Only a fully featured firewall can do this.
4. What kind of proxy would you use to mediate communications between Internet-based clients and LAN-based servers?
   - Anonymous
   - Forward
   - **Reverse**
   - Transparent

5. What DMZ topology is displayed? Choose the best response.



- Bastion Host
- Dual firewall
- **Three-homed firewall**
- UTM firewall

6. NIST defines the standards for UTM devices. True or false?

- True
- False

7. Which of the following is an example of a load balancer scheduling method? Choose the best response.

- Active-active
- Active-passive
- **Round robin**
- Virtual IP

Module B: Transport encryption

Assessment: Transport encryption

1. Order WAP encryption methods from most to least secure.

    1. WPA2-AES
    2. WPA-AES
    3. WPA2-TKIP
    4. WPA-TKIP
    5. WEP

2. Your WAP is currently secured with WPA Personal encryption, using a shared key. Which of the following is true? Choose the best response.
   - Enabling WPS could increase security, but enabling 802.1X would reduce it.
   - **Enabling 802.1X could increase security, but enabling WPS would reduce it.**
   - Enabling either WPS or 802.1X could increase security.
   - Enabling either WPS or 802.1X would reduce security.
3. On an IPsec VPN, what protocol negotiates security associations? Choose the best response.
   - AH
   - ESP
   - **IKE**
   - L2TP
4. What secure protocols add SSL/TLS security to protocols which were insecure on their own? Choose all that apply.
   - **FTPS**
   - **HTTPS**
   - SFTP
   - **SNMPv3**
   - SSH
5. What VPN type is secure, compatible with nearly any application, and supported by most operating systems?
   - **L2TP/IPsec**
   - PPTP
   - SSH
   - SSL/TLS
6. You can use a VPN to securely encrypt all of your network communication even on an open Wi-Fi network. True or false?
   - **True**
   - False
7. What security appliance is similar to a MitM attack, but designed to enhance network security rather than disrupt it? Choose the best response.
   - Split tunnel
   - SSL accelerator
   - **SSL decryptor**
   - VPN concentrator

8. You have a lingering problem with mobile users who connect to untrusted Wi-Fi networks without enabling their VPN, out of forgetfulness or lack of technical knowledge. What technology might help solve the problem? Choose the best response.

   - **Always-on VPN**
   - ESP
   - Full tunneling
   - Secure shell

Module C: Hardening networks

Assessment: Hardening networks

1. A perimeter network needs most of the same security precautions as a trusted network, just with a few extra concerns. True or false?

   - **True**
   - False

2. It's a safe assumption that an attacker with physical access to a system can compromise any other security measures given time. True or false?

   - **True**
   - False

3. What's the most essential tool for segmenting broadcast domains? Choose the best response.

   - Bridges
   - **Routers**
   - Switches
   - VLANs

4. What feature primarily helps to protect against DoS attacks? Choose the best response.

   - Authentication systems
   - DMZ
   - **Loop protection**
   - SNMPv3

5. If there are two firewalls between the internet and the interior network, they should be from different vendors. True or false?

   - **True**
   - False

6. What security feature is especially important for preventing rogue devices on the network? Choose the best response.
   - DMZ
   - Loop protection
   - **Port security**
   - VPN
7. Which Wi-Fi feature should you disable to improve security? Choose the best response.
   - 802.1X
   - MAC filtering
   - WPA2
   - **WPS**
8. A critical network service is hosted on a legacy server running an obsolete operating system, and you can't replace it until next fiscal year. You just learned it is extremely vulnerable to a new worm that's appeared on other computers on your network, but you can't update the server or install software that will protect it. What can you place between the server and the rest of the network to protect it? Choose the best response.
   - Airgap
   - Firewall
   - HIDS
   - **NIPS**

Module D: Monitoring and detection

Assessment: Monitoring and detection

1. An interface monitor is likely to be one part of a larger monitoring tool. True or false?
   - **True**
   - False
2. What SNMP component is a database for a particular device? Choose the best response.
   - Agent
   - Manager
   - **MIB**
   - OID
3. Even though Syslog has been around a very long time, it hasn't always been a well-defined standard. True or false?
   - True
   - **False**

4. What SIEM software feature finds broader trends and relationships formed by individually insignificant events? Choose the best response.

   - Aggregation
   - **Correlation**
   - Deduplication
   - Synchronization

5. What kind of tool is often called a sniffer? Choose the best response.

   - Database vulnerability tester
   - Network mapper
   - **Protocol analyzer**
   - Wireless analyzer

Chapter 6: Securing hosts and data

Module A: Securing data

Assessment: Securing data

1. Which Windows encryption tool can protect the entire system volume? Choose the best response.
   - **BitLocker**
   - Encrypting File System
   - Both
   - Neither
2. Your organization has a degausser in the basement. What media can you use it to securely destroy? Choose all that apply.
   - **Backup tapes**
   - CDs and DVDs
   - **Hard drives**
   - Paper documents
   - SSDs
3. What cryptographic tool is commonly built into a motherboard?
   - FDE
   - DLP
   - HSM
   - **TPM**
4. What might protect users from copying sensitive files to external media?
   - FDE
   - **DLP**
   - HSM
   - TPM
5. "Big data" shouldn't be confused with "cloud storage"? True or false?
   - **True**
   - False

6. Your organization has a critical database full of customer PII, and a new employee was just authorized to use it. How would you best describe the role of the system administrator who configures user permissions in the database software?

   - **Data custodian**
   - Data owner
   - Data steward
   - Privacy officer

Module B: Securing hosts

Assessment: Securing hosts

1. What was the first version of Windows to include real-time antivirus scanning? Choose the best response.

   - Windows XP Service Pack 2
   - Windows Vista
   - Windows 7
   - **Windows 8**
   - Windows 8.1

2. In general, you should leave the Guest account in Windows disabled. True or false?

   - **True**
   - False

3. A company configures workstations only to run software on an approved list. What is this an example of? Choose the best response.

   - Blacklisting
   - Hardening
   - Sandboxing
   - **Whitelisting**

4. A service pack is generally a more major update than a maintenance release. True or false?

   - **True**
   - False

5. Downgrades are often more difficult than upgrades. True or false?

   - **True**
   - False

6. What security feature makes it more difficult for an attacker to trick you into installing a fraudulent Ethernet driver that reports on your network activities? Choose the best response.

   - **Code signing**
   - Firewall
   - HIDS
   - Trusted hardware

7. What potential security risk does an SD card pose that a USB thumb drive does not? Choose the best response.

   - Data exfiltration
   - Malware
   - Photographs of sensitive areas
   - Wireless attacks

Module C: Mobile device security

Assessment: Mobile device security

1. What kind of application centrally manages security policy on all company mobile devices? Choose the best answer.

   - Asset tracking
   - BYOD
   - GPS
   - **MDM**

2. Both iOS and Android include a built-in feature to find and secure a lost device. True or false?

   - **True**
   - False

3. Both iOS and Android enable data encryption on most devices by default. True or false?

   - True
   - **False**

4. What are important security steps on all mobile devices? Choose all that apply.

   - Configuring antivirus software
   - **Configuring remote backup features**
   - Installing a firewall app
   - **Regularly applying operating system updates**
   - Using biometric authentication

5. What kind of policy governs a user-owned device on the corporate network? Choose the best response.

   - Acceptable Use
   - **BYOD**
   - MDM
   - Offboarding

6. Your company allows you to use the same smartphone for both personal and work purposes, but only if it's one of a half-dozen different models on an approved list. If you don't have an approved device, the company will pay for part of your upgrade. What kind of deployment model does the company use? Choose the best response.

   - BYOD
   - COBO
   - COPE
   - **CYOD**

7. What kind of policy governs removal of sensitive data and credentials when a user device is no longer used for company business?

   - Asset tracking
   - **Offboarding**
   - Onboarding
   - Storage segmentation

8. What connection type is very similar to Bluetooth but used by more specialized devices?

   - **ANT**
   - GSM
   - NFC
   - SATCOM

Chapter 7: Securing network services

Module A: Securing applications

Assessment: Securing applications

1. What technique tests an application's responses to random input? Choose the best response.
   - Escaping
   - **Fuzzing**
   - Sanitization
   - Validation
2. What kind of attack do synchronizer tokens help prevent?
   - Buffer overflow
   - SQL injection
   - XSS
   - **XSRF**
3. What does the software assurance process do? Choose the best response.
   - Ensure applications are up to date.
   - Ensure applications are regularly audited.
   - Ensure applications are securely configured.
   - **Ensure applications are securely designed.**
4. You're reviewing a web application. Which of these features are security warning signs? Choose all that apply.
   - **Input errors are logged and clearly displayed to users in full detail.**
   - The web server and database software are on separate physical servers, both similarly secured.
   - **Input validation is performed more rigorously on the client side than the server side.**
   - The HTTPOnly flag is set on session cookies.
   - **Secret cookies are used to prevent XSRF attacks.**
5. Even just blocking or sanitizing the < and > characters used by HTML tags can prevent many attacks. True or false?
   - **True**
   - False

6. What DevOps practice keeps code created by multiple developers from diverging or conflicting? Choose the best response.
   - Baselining
   - **Continuous integration**
   - Immutable systems
   - Infrastructure as code

Module B: Virtual and cloud systems

Assessment: Virtual and cloud systems

1. What model would describe a cloud accounting service? Choose the best response.
   - IaaS
   - PaaS
   - **SaaS**
   - SDN
2. All else being equal, bare metal hypervisors are more efficient than hosted ones. True or false?
   - **True**
   - False
3. As long as the host machine has antimalware protection, VMs are protected as well. True or false?
   - True
   - **False**
4. What cloud model is likely to provide access to a software environment you can use to develop and host web-based applications, but not the applications themselves? Choose the best response.
   - IaaS
   - **PaaS**
   - SaaS
   - Any of the above
5. When you use a cloud service, the security controls used by fellow customers could endanger your own security. True or false?
   - **True**
   - False
6. What kind of virtualization relies on a "master image?" Choose the best response.
   - Bare metal
   - Container
   - **Non-persistent VDI**
   - Persistent VDI

7. Your organization has decided to outsource a number of IT services to a cloud provider. They're hosted outside your enterprise network, but you want to centrally manage all authentication, encryption, activity logging, and other security policies for connections between local computers and the cloud. What security solution would address these issues?

   - On-premise policies
   - Private deployment
   - Security as a Service
   - **Security broker**

Chapter 8: Authentication

Module A: Authentication factors

Assessment: Authentication factors

1. What AAA element specifies the exact resources a given principal is allowed to access? Choose the best response.

   - Accounting
   - Authentication
   - **Authorization**
   - Identification

2. You require your users to log on using a user name, password, and rolling 6-digit code sent to a key fob device. They are then allowed computer, network, and email access. What type of authentication have you implemented? Choose all that apply.

   - Basic single-factor authentication
   - Federated identity management
   - **Multi-factor authentication**
   - Principle of least privilege
   - **Single sign-on**

3. What are good examples of two-factor authentication? Choose all that apply.

   - A credit card and a photo ID
   - **A credit card and a security code**
   - **A credit card and a signature**
   - A password followed by a security question
   - **A password followed by a PIN texted to your phone**

4. What authentication standard is used by active duty US military personnel?

   - **CAC**
   - PIV
   - OTP
   - SIM

5. A secure records room installed a new iris scanner, chosen for its low crossover error rate. What does that mean it has? Choose the best response.

   - A high false acceptance rate and a high false rejection rate
   - A high false acceptance rate and a low false rejection rate
   - A low false acceptance rate and a high false rejection rate
   - **A low false acceptance rate and a low false rejection rate**

6. Federated identity management allows authentication systems to be shared across multiple directly associated systems or networks. True or false?

   - True
   - **False**

7. You've been instructed to implement two-factor authentication for a secure system. What of the following would qualify? Choose all that apply.

   - **Password and OTP**
   - Smart card and OTP
   - **Smart card and fingerprint scan**
   - Iris scan and fingerprint scan
   - **Password and iris scan**

Module B: Authentication protocols

Assessment: Authentication protocols

1. Which protocol is more of a message framework than an authentication method in itself? Choose the best response.

   - CHAP
   - **EAP**
   - MS-CHAP
   - PAP

2. Your wireless network is configured in 802.1X mode. What kind of server does it most likely use as a back end? Choose the best response.

   - KERBEROS
   - **RADIUS**
   - TACACS+
   - TKIP

3. Your remote access system currently uses RADIUS, but one administrator is proposing replacing it with TACACS+. What benefits might this provide?. Choose all that apply.

   - **Better able to support non-IP protocols**
   - **Better suited to large networks**
   - Less complicated to administer
   - **More secure**
   - More focused on user authentication

4. You've been asked to help consult for security on an application that's designed to interoperate with Google and Salesforce SSO systems. What protocol should you study first? Choose the best answer.

   - Kerberos
   - LDAP
   - RADIUS
   - **SAML**

5. Unlike LDAP, LDAPS _____? Choose all that apply.

   - **Includes SSL or TLS encryption**
   - Is compatible with Unix-based operating systems
   - Is safe for use on the public internet
   - Uses port 389
   - **Uses port 636**

6. Your company is developing a custom web app for the sales team. It should be able to access a list of Salesforce contacts, but for security reasons the app shouldn't be able to access the actual Salesforce account. What standard would allow this? Choose the best response.

   - Kerberos
   - **OAuth**
   - OpenID Connect
   - SAML

Chapter 9: Access control

Module A: Access control principles

Assessment: Access control principles

1. Secure access control models are based on which assumption? Choose the best response.
   - Explicit Allow
   - Explicit Deny
   - Implicit Allow
   - **Implicit Deny**
2. What access control model was popularized by military usage? Choose the best response.
   - Discretionary
   - **Mandatory**
   - Role-based
   - Rule-based
3. What access control model is used by network hardware such as routers?
   - Discretionary
   - Mandatory
   - Role-based
   - **Rule-based**
4. What identifies a security principal in an NTFS file system?
   - ACE
   - DACL
   - LBAC
   - **SID**
5. What group permissions would a Linux file have if its permissions displayed as `-rwxrw-r--`?
   - **Read and write**
   - Read only
   - Read, write, and execute
   - Write only

6. You want to implement an access control model that lets you easily assign users to a combination of multiple roles, and also restrict access to some actions based on the time of day and physical location of the user. Which model is the best fit? Choose the best response.

   - **ABAC**
   - DAC
   - MAC
   - Role-based access control

Module B: Account management

Assessment: Account management

1. What order does Windows process GPOs in?

   1. Local GPO
   2. Site GPO
   3. Domain GPO
   4. Organizational Unit GPO
   5. Child OU GPO

2. Where is the best place to assign permissions?

   - **A domain local group**
   - A global group
   - An individual user
   - A universal group

3. When you enforce password complexity in Windows, you can't edit the precise complexity requirements True or false?

   - **True**
   - False

4. During a discussion of user account policies, someone suggests lowering the account lockout threshold on the Windows domain. What would be the net effect of this change? Choose the best response.

   - Less secure, and less trouble for users
   - Less secure, but more trouble for users
   - More secure, but less trouble for users
   - **More secure and more trouble for users**

5. When it's so important to change passwords regularly, why would you set a minimum password age? Choose the best response.

   - To keep users from choosing simple passwords
   - **To keep users from bypassing history requirements**
   - To prevent attackers from easily cracking passwords
   - To make sure users change their passwords regularly

Chapter 10: Organizational security

Module A: Security policies

Assessment: Security policies

1. What policy document generally describes mutual goals between organizations? Choose the best response.
   - BPA
   - ISA
   - **MOU**
   - SLA
2. Which policy is focused on preventing data loss? Choose the best response.
   - AUP
   - **Clean desk policy**
   - Mandatory vacation
   - Separation of duties
3. Experts agree that very demanding password policies are the best way to maintain security. True or false?
   - True
   - **False**
4. What are the benefits of a job rotation policy? Choose all that apply.
   - Allows employees to discover each other's mistakes in multi-step processes
   - **Helps detect fraudulent activity over time**
   - Minimizes permissions given to any one employee
   - Prevents data loss
   - **Trains employees more broadly**
5. Your company has signed a BPA with a business partner. What most likely isn't a part of it? Choose the best response.
   - How liability is shared for a loss of shared assets
   - **Technical requirements for secured data connections between the two companies**
   - What happens to informational assets when the agreement is dissolved
   - Who is responsible for maintaining informational assets

Module B: User training

Assessment: User training

1. What kind of security training is most important for a company executive? Choose the best response.
   - Identifying malware symptoms
   - **Overall awareness of the organization's assets and threats to them**
   - Recognizing social engineering attacks
   - Regular updates on evolving network threats
2. What standards do you need to use when handling credit card data? Choose the best response.
   - HIPAA
   - NIST
   - **PCI-DSS**
   - PKI
3. Users should have both permission and need to access sensitive data, whether technically able to or not. True or false?
   - **True**
   - False
4. What kind of employee is most likely to need extra training about social engineering attacks? Choose the best response.
   - Department manager
   - Maintenance technician
   - Network administrator
   - **Receptionist**

Module C: Physical security and safety

Assessment: Physical security and safety

1. You need to install a new fire extinguisher next to the server closet. What class would be most useful? Choose the best response.
   - Class A
   - Class B
   - **Class C**
   - Class D

2. What qualifies as both a preventive and a detective control? Choose the best response.
   - A locked door
   - A motion detector
   - **A security guard**
   - A surveillance camera
3. What are hot and cold aisles designed to assist? Choose the best response.
   - **Air circulation in the server room**
   - Defining routes for evacuating employees and incoming emergency workers
   - Preventing EMI
   - Preventing the spread of fires
4. One server closet has particularly sensitive equipment that's suffering EMI due to a nearby electrical motor. You can't really move either the equipment or the motor, so what option might help? Choose the best response.
   - Airgap
   - Cold aisle
   - **Faraday cage**
   - Mantrap
5. Fail-close door locks are _____. Choose the best response.
   - Good for safety and security
   - Good for safety but bad for security
   - **Bad for safety but good for security**
   - Bad for safety and security
6. In a building floor plan you see lines representing a Protected Distribution System. What is it used for? Choose the best response.
   - Backup power
   - Encrypted data
   - HVAC Controls
   - **Unencrypted data**

Chapter 11: Disaster planning and recovery

Module A: Business continuity

Assessment: Business continuity

1. What document specifically covers moving operations to a temporary site? Choose the best response.
   - BCP
   - BIA
   - **COOP**
   - DRP
2. Which document is a business most likely to have more than one of? Choose the best response.
   - BCP
   - BIA
   - COOP
   - **DRP**
3. What is also known as a "structured walkthrough?" Choose the best response.
   - Checklist test
   - ISCP
   - Simulation test
   - **Tabletop exercise**

Module B: Fault tolerance and recovery

Assessment: Fault tolerance and recovery

1. Which of the following RAID levels incorporates disk striping?
   - **RAID 0**
   - RAID 1
   - **RAID 5**
   - **RAID 10**
2. The process of rebuilding a RAID drive from parity data can cause a RAID drive to fail.
   - **True.**
   - False.

3. If you have a RAID implementation with data parity, you don't need data backups.

   - True.
   - **False.**

4. You have a critical database server that constantly backs its files up to the cloud, but its software environment is so finicky that if it encountered a critical failure it would take a long time to get it working again. How would you describe your recovery plan for that service?

   - High RPO and high RTO
   - High RPO and low RTO
   - **Low RPO and high RTO**
   - Low RPO and low RTO

5. Clustering is similar to load balancing, but tends to use tighter integration between redundant systems. True or false?

   - **True**
   - False

6. Your company rents a spare server room in a secondary location. It has all necessary hardware, software, and network services, and you just need to load the latest backups to get it in operation. What is it? Choose the best answer.

   - **Hot site**
   - Hot spare
   - Cold site
   - Cold spare

7. In terms of time, how does a differential backup plan generally differ from an incremental backup plan?

   - It's quicker both to create backups and to restore data
   - It's quicker to create backups, but slower to restore data
   - **It's slower to create backups, but quicker to restore data**
   - It's slower both to create backups and to restore data

8. What backup type might require specific operating system support? Choose the best response.

   - Differential
   - Full
   - Incremental
   - **Snapshot**

Module C: Incident response

Assessment: Incident response

1. Order the steps of the incident response process.

    1. Preparation
    2. Identification
    3. Containment
    4. Investigation
    5. Eradication
    6. Recovery
    7. Follow-up

2. What is eDiscovery? Choose the best answer.

    - A process for identifying security incidents.
    - **A process for sharing electronic forensic data.**
    - A standard for forensic backup software.
    - A software application used to track security incidents.

3. You should start choosing an incident response team as soon as you've identified an incident. True or false?

    - True
    - **False**

4. After a security incident you rush to take a screenshot of a telltale running process before you leisurely take a backup of suspicious files on the hard drive. What forensic principle are you exercising? Choose the best response

    - Audit trail
    - Chain of custody
    - eDiscovery
    - **Order of volatility**

5. Why is it important to record a time offset when collecting evidence?

    - To compensate for logging systems that don't record precise times
    - **To compensate for time differences between multiple systems**
    - To document the precise order of events
    - To document the precise timing of events