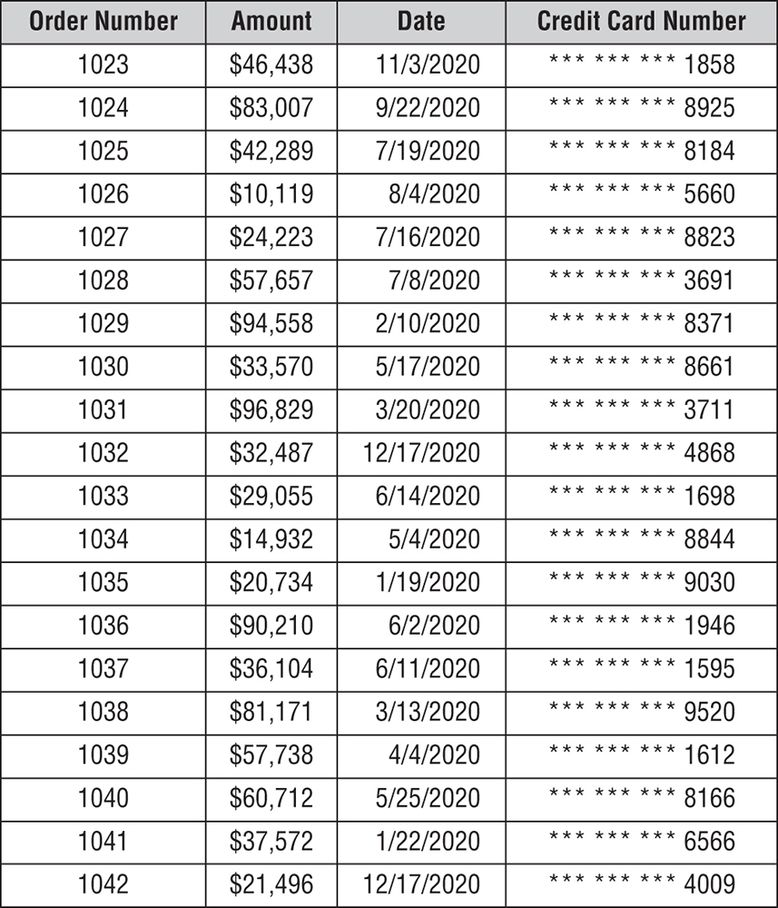
Ch 1:

**Review Questions**

1. Matt is updating the organization's threat assessment process. What category of control is Matt implementing?
   1. Operational
   2. Technical
   3. Corrective
   4. Managerial
2. Jade's organization recently suffered a security breach that affected stored credit card data. Jade's primary concern is the fact that the organization is subject to sanctions for violating the provisions of the Payment Card Industry Data Security Standard. What category of risk is concerning Jade?
   1. Strategic
   2. Compliance
   3. Operational
   4. Financial
3. Chris is responding to a security incident that compromised one of his organization's web servers. He believes that the attackers defaced one or more pages on the website. What cybersecurity objective did this attack violate?
   1. Confidentiality
   2. Nonrepudiation
   3. Integrity
   4. Availability
4. Gwen is exploring a customer transaction reporting system and discovers the table shown here. What type of data minimization has most likely been used on this table?

Larger View

* 1. Destruction
  2. Masking
  3. Tokenization
  4. Hashing

1. Tonya is concerned about the risk that an attacker will attempt to gain access to her organization's database server. She is searching for a control that would discourage the attacker from attempting to gain access. What type of security control is she seeking to implement?
   1. Preventive
   2. Detective
   3. Corrective
   4. Deterrent
2. Greg is implementing a data loss prevention system. He would like to ensure that it protects against transmissions of sensitive information by guests on his wireless network. What DLP technology would best meet this goal?
   1. Watermarking
   2. Pattern recognition
   3. Host-based
   4. Network-based
3. What term best describes data that is being sent between two systems over a network connection?
   1. Data at rest
   2. Data in transit
   3. Data in processing
   4. Data in use
4. Tina is tuning her organization's intrusion prevention system to prevent false positive alerts. What type of control is Tina implementing?
   1. Technical control
   2. Physical control
   3. Managerial control
   4. Operational control
5. Which one of the following is not a common goal of a cybersecurity attacker?
   1. Disclosure
   2. Denial
   3. Alteration
   4. Allocation
6. Tony is reviewing the status of his organization's defenses against a breach of their file server. He believes that a compromise of the file server could reveal information that would prevent the company from continuing to do business. What term best describes the risk that Tony is considering?
   1. Strategic
   2. Reputational
   3. Financial
   4. Operational
7. Which one of the following data elements is not commonly associated with identity theft?
   1. Social Security number
   2. Driver's license number
   3. Frequent flyer number
   4. Passport number
8. What term best describes an organization's desired security state?
   1. Control objectives
   2. Security priorities
   3. Strategic goals
   4. Best practices
9. Lou mounted the sign below on the fence surrounding his organization's datacenter. What control type *best* describes this control?

Larger View

Source: Gabriel Cassan / Adobe Stock

* 1. Compensating
  2. Detective
  3. Physical
  4. Deterrent

1. What technology uses mathematical algorithms to render information unreadable to those lacking the required key?
   1. Data loss prevention
   2. Data obfuscation
   3. Data minimization
   4. Data encryption
2. Greg recently conducted an assessment of his organization's security controls and discovered a potential gap: the organization does not use full-disk encryption on laptops. What type of control gap exists in this case?
   1. Detective
   2. Corrective
   3. Deterrent
   4. Preventive
3. What compliance regulation most directly affects the operations of a health-care provider?
   1. HIPAA
   2. PCI DSS
   3. GLBA
   4. SOX
4. Nolan is writing an after action report on a security breach that took place in his organization. The attackers stole thousands of customer records from the organization's database. What cybersecurity principle was most impacted in this breach?
   1. Availability
   2. Nonrepudiation
   3. Confidentiality
   4. Integrity
5. Which one of the following objectives is not one of the three main objectives that information security professionals must achieve to protect their organizations against cybersecurity threats?
   1. Integrity
   2. Nonrepudiation
   3. Availability
   4. Confidentiality
6. Which one of the following data protection techniques is reversible when conducted properly?
   1. Tokenization
   2. Masking
   3. Hashing
   4. Shredding
7. Which one of the following statements is not true about compensating controls under PCI DSS?
   1. Controls used to fulfill one PCI DSS requirement may be used to compensate for the absence of a control needed to meet another requirement.
   2. Controls must meet the intent of the original requirement.
   3. Controls must meet the rigor of the original requirement.
   4. Compensating controls must provide a similar level of defense as the original requirement.

Ch 2

**Review Questions**

1. Which of the following measures is not commonly used to assess threat intelligence?
   1. Timeliness
   2. Detail
   3. Accuracy
   4. Relevance
2. Which one of the following motivations is most commonly attributed to hacktivists?
   1. War
   2. Financial gain
   3. Political/philosophical beliefs
   4. Ethical
3. Kolin is a penetration tester who works for a cybersecurity company. His firm was hired to conduct a penetration test against a health-care system, and Kolin is working to gain access to the systems belonging to a hospital in that system. What term best describes Kolin's work?
   1. Authorized attacker
   2. Unauthorized attacker
   3. Unknown attacker
   4. Semi-authorized attacker
4. Which one of the following attackers is most likely to be associated with an APT?
   1. Nation-state actor
   2. Hacktivist
   3. Unskilled
   4. Insider
5. Which organization did the U.S. government help create to share knowledge between organizations in specific verticals?
   1. DHS
   2. SANS
   3. CERTS
   4. ISACs
6. Which of the following threat actors typically has the greatest access to resources?
   1. Nation-state actors
   2. Organized crime
   3. Hacktivists
   4. Insider threats
7. Of the threat vectors shown here, which one is most commonly exploited by attackers who are at a distant location?
   1. Email
   2. Direct access
   3. Wireless
   4. Removable media
8. Which one of the following is the best example of a hacktivist group?
   1. Chinese military
   2. U.S. government
   3. Russian mafia
   4. Anonymous
9. What type of assessment is particularly useful for identifying insider threats?
   1. Behavioral
   2. Instinctual
   3. Habitual
   4. IoCs
10. Cindy is concerned that her organization may be targeted by a supply chain attack and is conducting a review of all of her vendor and supplier partners. Which one of the following organizations is least likely to be the conduit for a supply chain attack?
    1. Hardware provider
    2. Software provider
    3. Managed service provider
    4. Talent provider
11. Greg believes that an attacker may have installed malicious firmware in a network device before it was provided to his organization by the supplier. What type of threat vector best describes this attack?
    1. Supply chain
    2. Removable media
    3. Cloud
    4. Direct access
12. Ken is conducting threat research on Transport Layer Security (TLS) and would like to consult the authoritative reference for the protocol's technical specification. What resource would best meet his needs?
    1. Academic journal
    2. Internet RFCs
    3. Subject matter experts
    4. Textbooks
13. Wendy is scanning cloud-based repositories for sensitive information. Which one of the following should concern her most, if discovered in a public repository?
    1. Product manuals
    2. Source code
    3. API keys
    4. Open source data
14. Which one of the following threat research tools is used to visually display information about the location of threat actors?
    1. Threat map
    2. Predictive analysis
    3. Vulnerability feed
    4. STIX
15. Vince recently received the hash values of malicious software that several other firms in his industry found installed on their systems after a compromise. What term best describes this information?
    1. Vulnerability feed
    2. IoC
    3. TTP
    4. RFC
16. Ursula recently discovered that a group of developers are sharing information over a messaging tool provided by a cloud vendor but not sanctioned by her organization. What term best describes this use of technology?
    1. Shadow IT
    2. System integration
    3. Vendor management
    4. Data exfiltration
17. Tom's organization recently learned that the vendor is discontinuing support for their customer relationship management (CRM) system. What should concern Tom the most from a security perspective?
    1. Unavailability of future patches
    2. Lack of technical support
    3. Theft of customer information
    4. Increased costs
18. Which one of the following information sources would not be considered an OSINT source?
    1. DNS lookup
    2. Search engine research
    3. Port scans
    4. WHOIS queries
19. Edward Snowden was a government contractor who disclosed sensitive government documents to journalists to uncover what he believed were unethical activities. Which of the following terms best describe Snowden's activities? (Choose two.)
    1. Insider
    2. State actor
    3. Hacktivist
    4. APT
    5. Organized crime
20. Renee is a cybersecurity hobbyist. She receives an email about a new web-based grading system being used by her son's school and she visits the site. She notices that the URL for the site looks like this:

www.myschool.edu/grades.php&studentID=1023425

She realizes that 1023425 is her son's student ID number and she then attempts to access the following similar URLs:

www.myschool.edu/grades.php&studentID=1023423

www.myschool.edu/grades.php&studentID=1023424

www.myschool.edu/grades.php&studentID=1023426

www.myschool.edu/grades.php&studentID=1023427

When she does so, she accesses the records of other students. She closes the records and immediately informs the school principal of the vulnerability. What term best describes Renee's work?

* 1. Authorized hacking
  2. Unknown hacking
  3. Semi-authorized hacking
  4. Unauthorized hacking

Ch 3

**Review Questions**

1. Ryan wants to prevent logic bombs created by insider threats from impacting his organization. What technique will most effectively limit the likelihood of logic bombs being put in place?
   1. Deploying antivirus software
   2. Using a code review process
   3. Deploying endpoint detection and response (EDR) software
   4. Disabling autorun for USB drives
2. Yasmine believes that her organization may be dealing with an advanced rootkit and wants to write IoC definitions for it. Which of the following is not likely to be a useful IoC for a rootkit?
   1. File hashes
   2. Command and control domains
   3. Pop-ups demanding a ransom
   4. Behavior-based identifiers
3. Nathan works at a school and notices that one of his staff appears to have logged in and changed grades for a single student to higher grades, even in classes that staff member is not responsible for. When asked, the staff member says that they did not perform the action. Which of the following is the most likely way that a student could have gotten access to the staff member's password?
   1. A keylogger
   2. A rootkit
   3. Spyware
   4. A logic bomb
4. Amanda notices traffic between her systems and a known malicious host on TCP port 6667. What type of traffic is she most likely detecting?
   1. Command and control
   2. Spyware
   3. A worm
   4. A hijacked web browser
5. Mike discovers that attackers have left software that allows them to have remote access to systems on a computer in his company's network. How should he describe or classify this malware?
   1. A worm
   2. Crypto malware
   3. A trojan
   4. A backdoor
6. What is the primary impact of bloatware?
   1. Consuming resources
   2. Logging keystrokes
   3. Providing information about users and devices to third parties
   4. Allowing unauthorized remote access
7. What type of malware is used to gather information about a user's browsing habits and system?
   1. A Trojan
   2. Bloatware
   3. Spyware
   4. A rootkit
8. Matt uploads a malware sample to a third-party malware scanning site that uses multiple antimalware and antivirus engines to scan the sample. He receives multiple different answers for what the malware package is. What has occurred?
   1. The package contains more than one piece of malware.
   2. The service is misconfigured.
   3. The malware is polymorphic and changed while being tested.
   4. Different vendors use different names for malware packages.
9. Nancy is concerned that there is a software keylogger on the system she's investigating. What best describes data that may have been stolen?
   1. All files on the system
   2. All keyboard input
   3. All files the user accessed while the keylogger was active
   4. Keyboard and other input from the user
10. A system in Elaine's company has suddenly displayed a message demanding payment in Bitcoin and claiming that the data from the system has been encrypted. What type of malware has Elaine likely encountered?
    1. Worms
    2. A virus
    3. Ransomware
    4. Rootkit
11. Rick believes that a system he is responsible for has been compromised with malware that uses a rootkit to obtain and retain access to the system. When he runs an antimalware tool's scanner, the system doesn't show any malware. If he has other data that indicates the system is infected, what should his next step be if he wants to determine what malware may be on the system?
    1. Rerun the antimalware scan.
    2. Mount the drive on another system and scan it that way.
    3. Disable the systems antivirus because it may be causing a false negative.
    4. The system is not infected and he should move on.
12. A recently terminated developer from Jaya's organization has contacted the organization claiming that they left code in an application that they wrote that will delete files and bring the application down if they are not employed by the company. What type of malware is this?
    1. Ransomware
    2. Extortionware
    3. A logic bomb
    4. A Trojan
13. Selah wants to ensure that malware is completely removed from a system. What should she do to ensure this?
    1. Run multiple antimalware tools and use them to remove all detections.
    2. Wipe the drive and reinstall from known good media.
    3. Use the delete setting in her antimalware software rather than the quarantine setting.
    4. There is no way to ensure the system is safe and it should be destroyed.
14. What is the key difference between a worm and a virus?
    1. What operating system they run on
    2. How they spread
    3. What their potential impact is
    4. The number of infections
15. Ben wants to analyze Python code that he believes may be malicious code written by an employee of his organization. What can he do to determine if the code is malicious?
    1. Run a decompiler against it to allow him to read the code
    2. Open the file using a text editor to review the code
    3. Test the code using an antivirus tool
    4. Submit the Python code to a malware testing website
16. Which of the following defenses is most likely to prevent Trojan installation?
    1. Installing patches for known vulnerabilities
    2. Preventing downloads from application stores
    3. Preventing the use of USB drives
    4. Disabling autorun from USB drives
17. Jason's security team reports that a recent WordPress vulnerability seems to have been exploited by malware and that their organization's entire WordPress service cluster has been infected. What type of malware is most likely involved if a vulnerability in the software was exploited over the network?
    1. A logic bomb
    2. A Trojan
    3. A worm
    4. A rootkit
18. Hui's organization recently purchased new Windows computers from an office supply store. The systems have a number of unwanted programs on them that load at startup that were installed by the manufacturer. What type of software is this?
    1. Viruses
    2. Trojans
    3. Spyware
    4. Bloatware
19. What type of malware connects to a command and control system, allowing attackers to manage, control, and update it remotely?
    1. A bot
    2. A drone
    3. A vampire
    4. A worm
20. Randy believes that a system that he is responsible for was infected after a user picked up a USB drive and plugged it in. The user claims that they only opened one file on the drive to see who might own it. What type of malware is most likely involved?
    1. A virus
    2. A worm
    3. A trojan
    4. A spyware tool

Ch 4

**Review Questions**

1. Joseph receives an email notifying him that he needs to change his password due to a recent account issue. He notices that the email links him to a website using the domain [amaz0n.com](http://amaz0n.com/). What type of attack should he describe this as?
   1. Typosquatting
   2. Phishing
   3. Smishing
   4. A watering hole attack
2. When you combine phishing with voicemail, it is known as:
   1. Whaling
   2. Spoofing
   3. Spooning
   4. Vishing
3. While reviewing her logs, Michele notices that a remote system has attempted to log into her server via SSH using the username admin and a variety of passwords like “password” and “ninja.” What type of attack has Michele noticed?
   1. A brute-force attack
   2. Shoulder surfing
   3. An on-path attack
   4. Pretexting
4. Joanna wants to detect password spraying attacks. What type of rule should she deploy through her security systems?
   1. Match attempts to log into many systems with the same username and password.
   2. Match multiple attempts to log into the same user account using different passwords.
   3. Match repeated use of the same password during failed login attempts for multiple usernames.
   4. Match all attempts to use passwords with slight changes for the same account.
5. One of the staff at Susan's organization has reported that a critical vendor has contacted them about an unpaid invoice. After Susan investigates, she discovers that the invoice was sent from an email account that was not typically a contact and that the invoice requested payment to a PayPal account. What type of social engineering attack has Susan most likely discovered?
   1. Smishing
   2. Business email compromise
   3. Disinformation
   4. Typosquatting
6. Selah infects the ads on a website that users from her target company frequently visit with malware as part of her penetration test. What technique has she used?
   1. A watering hole attack
   2. Vishing
   3. Whaling
   4. Typosquatting
7. Ben wants to determine if brute-force password attacks are being used against his company. What log information is least likely to be useful when working to detect brute-force attacks?
   1. Source IP address or hostname
   2. Failed login logs
   3. The password that was used for each attempt
   4. The geographic location of system being logged into
8. Melissa receives a call and the caller informs her a senior manager in her organization needs her to buy gift cards for an event that starts in an hour. The caller says that the senior leader forgot to get the cards, and that the event is critical to her organization. Melissa buys the cards and sends them to the Gmail address the caller says that the senior leader needs them sent to. What type of attack has Melissa fallen for?
   1. Phishing
   2. Pretexting
   3. Business email compromise
   4. Carding
9. Alaina wants to determine if a password spraying attack was used against her organization. Which of the following indicators would be most useful as part of her investigation?
   1. The time the login attempts happened
   2. The passwords used for failed attempts
   3. The source IP address of the attempts
   4. The number of failed attempts for each user
10. Which of the following human vectors is primarily associated with nation-state actors?
    1. Misinformation campaigns
    2. Watering hole attacks
    3. Business email compromise
    4. Password spraying
11. Nicole accidentally types [www.smazon.com](http://www.smazon.com/) into her browser and discovers that she is directed to a different site loaded with ads and pop-ups. Which of the following is the most accurate description of the attack she has experienced?
    1. DNS hijacking
    2. Pharming
    3. Typosquatting
    4. Hosts file compromise
12. Devon is a penetration tester and sets up malicious tools on his target organization's primary internal website. What type of attack is he conducting?
    1. A misinformation campaign
    2. A watering hole attack
    3. A typosquatting attack
    4. A disinformation campaign
13. Phishing emails sent pretending to be from a company that recipients are familiar with and likely to respond to is what type of attack?
    1. Phishing
    2. Pharming
    3. Brand impersonation
    4. Pretexting
14. When a caller was recently directed to Amanda, who is a junior IT employee at her company, the caller informed her that they were the head of IT for her organization and that she needed to immediately disable the organization's firewall. After Amanda made the change, she discovered that the caller was not the head of IT, and that they were actually a penetration tester hired by her company. What social engineering attack best describes this?
    1. Smishing
    2. Pretexting
    3. Impersonation
    4. Vishing
15. Fred is concerned about text message–based attacks. Which of the following attacks relies on text messages as its primary focus?
    1. Impersonation
    2. Watering hole attacks
    3. Smishing
    4. Business email compromise
16. Sharif notices that his authentication logs have many different usernames showing failed logins with the same password. What type of attack has he discovered?
    1. Credential harvesting
    2. Impersonation
    3. BEC
    4. Spraying
17. Naomi receives a report of smishing. What type of attack should she be looking for?
    1. Compressed files in phishing
    2. Text message–based phishing
    3. Voicemail-based phishing
    4. Server-based phishing
18. Jack's organization wants to prevent typosquatting. What option should he select to address this issue?
    1. Copyright the domain name
    2. Purchase the most common typos for his organization's domain
    3. Trademark the domain name
    4. Disable typo resolution for the domain
19. Gwyne's company has been contacted by customers asking about a new social media account operating under the company's brand. The social media account is advertising cryptocurrency, which Gwyne's organization does not sell or work with. What type of attack best describes what Gwyne's organization has encountered?
    1. Impersonation
    2. Brand impersonation
    3. Mis-branding
    4. Crypto-phishing
20. Nation-state-driven social media campaigns about the trustworthiness of the U.S. election in 2016 are an example of what type of social engineering?
    1. Smishing
    2. Pretexting
    3. Disinformation
    4. Spraying

Ch 5

**Review Questions**

1. Which one of the following security assessment techniques assumes that an organization has already been compromised and searches for evidence of that compromise?
   1. Vulnerability scanning
   2. Penetration testing
   3. Threat hunting
   4. War driving
2. Renee is configuring her vulnerability management solution to perform credentialed scans of servers on her network. What type of account should she provide to the scanner?
   1. Domain administrator
   2. Local administrator
   3. Root
   4. Read-only
3. Ryan is planning to conduct a vulnerability scan of a business-critical system using dangerous plug-ins. What would be the best approach for the initial scan?
   1. Run the scan against production systems to achieve the most realistic results possible.
   2. Run the scan during business hours.
   3. Run the scan in a test environment.
   4. Do not run the scan to avoid disrupting the business.
4. Which one of the following values for the CVSS attack complexity metric would indicate that the specified attack is simplest to exploit?
   1. High
   2. Medium
   3. Low
   4. Severe
5. Tara recently analyzed the results of a vulnerability scan report and found that a vulnerability reported by the scanner did not exist because the system was actually patched as specified. What type of error occurred?
   1. False positive
   2. False negative
   3. True positive
   4. True negative
6. Brian ran a penetration test against a school's grading system and discovered a flaw that would allow students to alter their grades by exploiting a SQL injection vulnerability. What type of control should he recommend to the school's cybersecurity team to prevent students from engaging in this type of activity?
   1. Confidentiality
   2. Integrity
   3. Alteration
   4. Availability
7. Which one of the following security assessment tools is least likely to be used during the reconnaissance phase of a penetration test?
   1. Nmap
   2. Nessus
   3. Metasploit
   4. Nslookup
8. During a vulnerability scan, Brian discovered that a system on his network contained this vulnerability:

Larger View

What security control, if deployed, would likely have addressed this issue?

* 1. Patch management
  2. File integrity monitoring
  3. Intrusion detection
  4. Threat hunting

1. Which one of the following tools is most likely to detect an XSS vulnerability?
   1. Static application test
   2. Web application vulnerability scanner
   3. Intrusion detection system
   4. Network vulnerability scanner
2. During a penetration test, Patrick deploys a toolkit on a compromised system and uses it to gain access to other systems on the same network. What term best describes this activity?
   1. Lateral movement
   2. Privilege escalation
   3. Footprinting
   4. OSINT
3. Zian is a cybersecurity leader who is coordinating the activities of a security audit. The audit is being done to validate the organization's financial statements to investors and involves a review of cybersecurity controls. What term best describes this audit?
   1. External audit
   2. Penetration test
   3. Internal audit
   4. Informal audit
4. Which one of the following assessment techniques is designed to solicit participation from external security experts and reward them for discovering vulnerabilities?
   1. Threat hunting
   2. Penetration testing
   3. Bug bounty
   4. Vulnerability scanning
5. Kyle is conducting a penetration test. After gaining access to an organization's database server, he installs a backdoor on the server to grant himself access in the future. What term best describes this action?
   1. Privilege escalation
   2. Lateral movement
   3. Maneuver
   4. Persistence
6. Which one of the following techniques would be considered passive reconnaissance?
   1. Port scans
   2. Vulnerability scans
   3. WHOIS lookups
   4. Footprinting
7. Which element of the SCAP framework can be used to consistently describe vulnerabilities?
   1. CPE
   2. CVE
   3. CVSS
   4. CCE
8. Bruce is conducting a penetration test for a client. The client provided him with full details of their systems in advance. What type of test is Bruce conducting?
   1. Partially known environment test
   2. Detailed environment test
   3. Known environment test
   4. Unknown environment test
9. Lila is working on a penetration testing team and she is unsure whether she is allowed to conduct social engineering as part of the test. What document should she consult to find this information?
   1. Contract
   2. Statement of work
   3. Rules of engagement
   4. Lessons learned report
10. Grace would like to determine the operating system running on a system that she is targeting in a penetration test. Which one of the following techniques will most directly provide her with this information?
    1. Port scanning
    2. Footprinting
    3. Vulnerability scanning
    4. Packet capture
11. Kevin recently identified a new security vulnerability and computed its CVSS base score as 6.5. Which risk category would this vulnerability fall into?
    1. Low
    2. Medium
    3. High
    4. Critical
12. Which one of the CVSS metrics would contain information about the type of account access that an attacker must have to execute an attack?
    1. AV
    2. C
    3. PR
    4. AC

Ch 6

**Review Questions**

1. Adam is conducting software testing by reviewing the source code of the application. What type of code testing is Adam conducting?
   1. Mutation testing
   2. Static code analysis
   3. Dynamic code analysis
   4. Fuzzing
2. Charles is worried about users conducting SQL injection attacks. Which of the following solutions will best address his concerns?
   1. Using secure session management
   2. Enabling logging on the database
   3. Performing user input validation
   4. Implementing TLS
3. Precompiled SQL statements that only require variables to be input are an example of what type of application security control?
   1. Parameterized queries
   2. Encoding data
   3. Input validation
   4. Appropriate access controls
4. During a web application test, Ben discovers that the application shows SQL code as part of an error provided to application users. What should he note in his report?
   1. Improper error handling
   2. Code exposure
   3. SQL injection
   4. A default configuration issue
5. The application that Scott is writing has a flaw that occurs when two operations are attempted at the same time, resulting in unexpected results when the two actions do not occur in the expected order. What type of flaw does the application have?
   1. Dereferencing
   2. A race condition
   3. An insecure function
   4. Improper error handling
6. Every time Susan checks code into her organization's code repository, it is tested and validated, and then if accepted, it is immediately put into production. What is the term for this?
   1. Continuous integration
   2. Continuous delivery
   3. A security nightmare
   4. Agile development
7. Tim is working on a change to a web application used by his organization to fix a known bug. What environment should he be working in?
   1. Test
   2. Development
   3. Staging
   4. Production
8. Ricky is concerned that developers in his organization make use of third-party code in their applications, which may introduce unknown vulnerabilities. He is concerned about the risk of the organization running code that it is not aware it is using. Which one of the following activities would best address this risk?
   1. Web application firewalls
   2. Package monitoring
   3. Static analysis
   4. Dynamic analysis
9. Which one of the following is not an advantage of automation in cybersecurity operations?
   1. Enforcing baselines
   2. Technical debt
   3. Employee retention
   4. Standardizing infrastructure configurations
10. Chris is creating a script that will automatically screen any user requests and flag those that exceed normal thresholds for manual review. What term best describes this automation use case?
    1. User provisioning
    2. Guard rails
    3. Ticket creation
    4. Escalation
11. Which one of the following is not a common drawback of automating cybersecurity operations?
    1. Reducing employee satisfaction
    2. Creating single points of failure
    3. Costs
    4. Complexity
12. Frank is investigating a security incident where the attacker entered a very long string into an input field, which was followed by a system command. What type of attack likely took place?
    1. Cross-site request forgery
    2. Server-side request forgery
    3. Command injection
    4. Buffer overflow
13. What type of attack places an attacker in the position to eavesdrop on communications between a user and a web server?
    1. On-path attack
    2. Session hijacking
    3. Buffer overflow
    4. Meet-in-the-middle
14. Tom is a software developer who creates code for sale to the public. He would like to assure his users that the code they receive actually came from him. What technique can he use to best provide this assurance?
    1. Code signing
    2. Code endorsement
    3. Code encryption
    4. Code obfuscation
15. Chris is reviewing evidence of a cross-site scripting attack where the attacker embedded JavaScript in a URL that a user clicked. The web page then sent the JavaScript to the user in the displayed page. What term best describes this attack?
    1. Reflected XSS
    2. Stored XSS
    3. Persistent XSS
    4. DOM-based XSS
16. Joe checks his web server logs and sees that someone sent the following query string to an application running on the server:
17. www.mycompany.com/servicestatus.php?serviceID=892&serviceID=892’%20;DROP%20TABLE%20Services;--

What type of attack was most likely attempted?

* 1. Cross-site scripting
  2. Session hijacking
  3. Parameter pollution
  4. On-path

1. Upon further inspection, Joe finds a series of thousands of requests to the same URL coming from a single IP address. Here are a few examples:
2. www.mycompany.com/servicestatus.php?serviceID=1
3. www.mycompany.com/servicestatus.php?serviceID=2
4. www.mycompany.com/servicestatus.php?serviceID=3
5. www.mycompany.com/servicestatus.php?serviceID=4
6. www.mycompany.com/servicestatus.php?serviceID=5
7. www.mycompany.com/servicestatus.php?serviceID=6

What type of vulnerability was the attacker likely trying to exploit?

* 1. Insecure direct object reference
  2. File upload
  3. Unvalidated redirect
  4. Session hijacking

1. Joe's adventures in web server log analysis are not yet complete. As he continues to review the logs, he finds the request:
2. www.mycompany.com/../../../etc/passwd

What type of attack was most likely attempted?

* 1. SQL injection
  2. Session hijacking
  3. Directory traversal
  4. File upload

1. Wendy is a penetration tester who wishes to engage in a session hijacking attack. What information is crucial for Wendy to obtain if her attack will be successful?
   1. Session ticket
   2. Session cookie
   3. Username
   4. User password
2. Joe is examining the logs for his web server and discovers that a user sent input to a web application that contained the string WAITFOR. What type of attack was the user likely attempting?
   1. Timing-based SQL injection
   2. HTML injection
   3. Cross-site scripting
   4. Content-based SQL injection

Ch 7

**Review Questions**

1. Mike is sending David an encrypted message using a symmetric encryption algorithm. What key should he use to encrypt the message?
   1. Mike's public key
   2. Mike's private key
   3. David's public key
   4. Shared secret key
2. Shahla recently discovered an attack where the attacker managed to force a network user to use weak encryption and was then able to decrypt that content. What term best describes this attack?
   1. Downgrade
   2. Collision
   3. Homomorphic encryption
   4. Birthday attack
3. Norm is using full-disk encryption technology to protect the contents of laptops against theft. What goal of cryptography is he attempting to achieve?
   1. Integrity
   2. Non-repudiation
   3. Authentication
   4. Confidentiality
4. Brian discovers that a user suspected of stealing sensitive information is posting many image files to a message board. What technique might the individual be using to hide sensitive information in those images?
   1. Steganography
   2. Homomorphic encryption
   3. Replay attack
   4. Birthday attack
5. Which one of the following statements about cryptographic keys is incorrect?
   1. All cryptographic keys should be kept secret.
   2. Longer keys are better than shorter keys when the same algorithm is used.
   3. Asymmetric algorithms generally use longer keys than symmetric algorithms.
   4. Digital certificates are designed to share public keys.
6. What type of cipher operates on one character of text at a time?
   1. Block cipher
   2. Bit cipher
   3. Stream cipher
   4. Balanced cipher
7. Vince is choosing a symmetric encryption algorithm for use in his organization. He would like to choose the strongest algorithm from these choices. What algorithm should he choose?
   1. DES
   2. 3DES
   3. RSA
   4. AES
8. Kevin is configuring a web server to use digital certificates. What technology can he use to allow clients to quickly verify the status of those certificates without contacting a remote server?
   1. CRL
   2. OCSP
   3. Certificate stapling
   4. Certificate pinning
9. Acme Widgets has 10 employees and they all need the ability to communicate with one another using a symmetric encryption system. The system should allow any two employees to securely communicate without other employees eavesdropping. If an 11th employee is added to the organization, how many new keys must be added to the system?
   1. 1
   2. 2
   3. 10
   4. 11
10. Referring to the scenario in question 9, if Acme Widgets switched to an asymmetric encryption algorithm, how many keys would be required to add the 11th employee?
    1. 1
    2. 2
    3. 10
    4. 11
11. What type of digital certificate provides the greatest level of assurance that the certificate owner is who they claim to be?
    1. DV
    2. OV
    3. UV
    4. EV
12. Glenn recently obtained a wildcard certificate for \*.[mydomain.com](http://mydomain.com/). Which one of the following domains would not be covered by this certificate?
    1. [mydomain.com](http://mydomain.com/)
    2. core.mydomain.com
    3. dev. [www.mydomain.com](http://www.mydomain.com/)
    4. mail.mydomain.com
13. Which one of the following servers is almost always an offline CA in a large PKI deployment?
    1. Root CA
    2. Intermediate CA
    3. RA
    4. Internal CA
14. Which one of the following certificate formats is closely associated with Windows binary certificate files?
    1. DER
    2. PEM
    3. PFX
    4. P7B
15. What type of security solution provides a hardware platform for the storage and management of encryption keys?
    1. HSM
    2. IPS
    3. SIEM
    4. SOAR
16. What type of cryptographic attack attempts to force a user to reduce the level of encryption that they use to communicate with a remote server?
    1. Birthday
    2. Frequency
    3. Downgrade
    4. Collision
17. David would like to send Mike a message using an asymmetric encryption algorithm. What key should he use to encrypt the message?
    1. David's public key
    2. David's private key
    3. Mike's public key
    4. Mike's private key
18. When Mike receives the message that David encrypted for him, what key should he use to decrypt the message?
    1. David's public key
    2. David's private key
    3. Mike's public key
    4. Mike's private key
19. If David wishes to digitally sign the message that he is sending Mike, what key would he use to create the digital signature?
    1. David's public key
    2. David's private key
    3. Mike's public key
    4. Mike's private key
20. When Mike receives the digitally signed message from David, what key should he use to verify the digital signature?
    1. David's public key
    2. David's private key
    3. Mike's public key
    4. Mike's private key

Ch 8

**Review Questions**

1. Angela has chosen to federate with other organizations to allow use of services that each organization provides. What role does Angela's organization play when they authenticate their users and assert that those users are valid to other members of the federation?
   1. Service provider
   2. Relying party
   3. Authentication provider
   4. Identity provider
2. Which of the following technologies is the least effective means of preventing shared accounts?
   1. Password complexity requirements
   2. Requiring biometric authentication
   3. Requiring one-time passwords via a token
   4. Requiring a one-time password via an application
3. What major difference is likely to exist between on-premises identity services and those used in a cloud-hosted environment?

A.Account policy control will be set to the cloud provider's standards.

B.The cloud service will provide account and identity management services.

C.Multifactor authentication will not be supported by the cloud vendor.

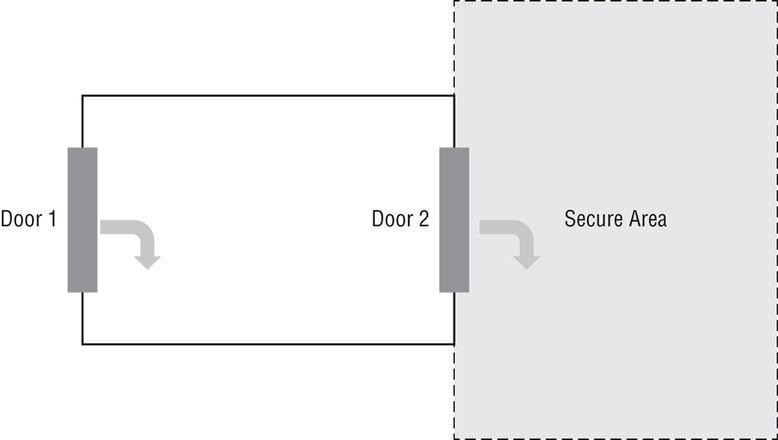
D.None of the above.

1. Amitoj wants to ensure that her organization's password policy does not allow users to reset their password multiple times until they can reuse their current password. What setting is used to prevent this?
   1. Complexity
   2. Length
   3. Expiration
   4. Age
2. Which type of multifactor authentication is considered the least secure?
   1. HOTP
   2. SMS
   3. TOTP
   4. Biometric
3. Geeta has been issued a USB security key as part of her organization's multifactor implementation. What type of implementation is this?
   1. A hard token
   2. A biometric token
   3. A soft token
   4. An attestation token
4. Michelle enables the Windows picture password feature to control logins for her laptop. Which type of attribute will it provide?
   1. Somewhere you are
   2. Something you know
   3. Something you are
   4. Someone you know
5. What purpose would Linux file permissions set to rw-r—r-- serve?
   1. To allow the owner to read and write the file, and for the owner's group and others to be able to read it
   2. To allow all users to read and write the file, and for the group and owner to be able to read it
   3. To allow system administrators to read and write the file, and for users and all others to be able to read it
   4. To prevent reading and writing for all users, and to prevent reading by groups and a specific user
6. Theresa wants to implement an access control scheme that sets permissions based on what the individual's job requires. Which of the following schemes is most suited to this type of implementation?
   1. ABAC
   2. DAC
   3. RBAC
   4. MAC
7. Which of the following biometric technologies is most broadly deployed due to its ease of use and acceptance from end users?
   1. Voice print recognition
   2. Gait recognition
   3. Retina scanners
   4. Fingerprint scanner
8. Adam want to increase his organization's passwords resistance to attacks in the event that the password hash database is stolen by attackers. Which of the following password security settings has the largest impact on password cracking if his organization's current passwords are 8 characters long?
   1. Password complexity
   2. Password length
   3. Password reuse limitations
   4. Preventing the use of common words in passwords
9. A PIN is an example of what type of factor?
   1. Something you know
   2. Something you are
   3. Something you have
   4. Something you set
10. Marie is implementing a PAM solution and wants to ensure that root passwords are available in the event of an outage. Which PAM-related tool is most likely to be useful in this situation?
    1. Ephemeral accounts
    2. Just-in-time permissions
    3. Password vaulting
    4. Token-based authentication
11. Jill sets her files on a Windows file share to allow Fred to access the files. What type of access control system is she using?
    1. Mandatory access control
    2. Rule-based access control
    3. Attribute-based access control
    4. Discretionary access control
12. Lisa sets up an account on a website that allows her to log in with Google. When she logs in, Google provides an access token to the website that confirms that she is who she says she is but doesn't provide the site with her password. Which of the following technologies has she used?
    1. LDAP
    2. OAuth
    3. MITRE
    4. RADIUS
13. Kyle has been asked to provide his government-issued ID as part of the creation of his user account. What process should he assume it is being used for?
    1. Biometric enrollment
    2. Just-in-time permission creation
    3. Identity proofing
    4. Federation
14. What key concept below best describes only providing the permissions necessary to perform a role?
    1. Least privilege
    2. Best practice
    3. Ephemeral accounts
    4. Mandatory access control
15. Nina has recently left her organization. What should the organization do with her account?
    1. Transfer it to her replacement.
    2. Reprovision it for another user.
    3. Deprovision her account.
    4. Change the password and preserve the account.
16. A person's name, age, location, or job title are all examples of what?
    1. Biometric factors
    2. Identity factors
    3. Attributes
    4. Account permissions
17. What type of access control scheme best describes the Linux filesystem?
    1. MAC
    2. RBAC
    3. DAC
    4. ABAC

Ch 9

**Review Questions**

1. Naomi wants to handle increasing load by scaling cloud-hosted resources as needed while having the change remain transparent to users. She also wants to allow for upgrades and system replacements transparently. What solution should she select?
   1. Load balancing
   2. Clustering
   3. Geographic diversity
   4. A hot site
2. Rick performs a backup that captures the changes since the last full backup. What type of backup has he performed?
   1. A new full backup
   2. A snapshot
   3. An incremental backup
   4. A differential backup
3. What type of recovery site has some or most systems in place but does not have the data needed to take over operations?
   1. A hot site
   2. A warm site
   3. A cloud site
   4. A cold site
4. Ben wants to test his warm site to verify that it will take over operations successfully. What type of testing is this?
   1. Parallel processing
   2. Simulation
   3. Failover
   4. A tabletop exercise
5. Felix wants to clone a virtual machine. What should he do to capture a live machine, including the machine state?
   1. A full backup
   2. A snapshot
   3. A differential backup
   4. Live boot media
6. Sally is working to restore her organization's operations after a disaster took her datacenter offline. What critical document should she refer to as she restarts systems?
   1. The restoration order documentation
   2. The TOTP documentation
   3. The HOTP documentation
   4. The last-known good configuration documentation
7. Mike wants to stop vehicles from traveling toward the entrance of his building. What physical security control should he implement?
   1. An air gap
   2. A hot aisle
   3. A robotic sentry
   4. A bollard
8. Alecia wants to ensure that her backups cannot be accessed by third parties while stored in an offsite storage location. What should she do to secure her backups?
   1. Hash the backup data.
   2. Avoid the use of offsite storage locations.
   3. Employ security guards.
   4. Encrypt the backup data.
9. Fred wants to be able to recover his database transactions at any point in time if a physical disaster occurs involving his datacenter. His organization uses daily backups. What additional solution should he select to support this need?
   1. Onsite journaling
   2. Onsite snapshots
   3. Offsite journaling
   4. Offsite snapshots
10. Ellen is concerned about her company's resilience and wants to ensure it can handle either changing loads or support disaster recovery and business continuity efforts if a primary location or datacenter were taken offline. Which of the following should she primarily focus on during her capacity planning?
    1. People, technology, and infrastructure
    2. A generator and a UPS
    3. RAID 0, 1, 5, and 10
    4. Incremental, differential, and full backups
11. Madhuri has deployed a replication tool that copies data over to a secondary hot site in real time. What type of replication has she deployed?
    1. Synchronous replication
    2. Journaled replication
    3. Asynchronous replication
    4. Snapshot-based replication
12. What factor is a major reason organizations do not use security guards?
    1. Reliability
    2. Training
    3. Cost
    4. Social engineering
13. Megan wants to deploy a sensor that is inexpensive, yet will allow her to detect humans entering and moving in a secured room. Which of the following should she select?
    1. An infrared sensor
    2. A microwave sensor
    3. An ultrasonic sensor
    4. A pressure sensor
14. Kathleen wants to discourage potential attackers from entering the facility she is responsible for. Which of the following is *not* a common control used for this type of preventive defense?
    1. Fences
    2. Lighting
    3. Platform diversity
    4. Video surveillance
15. How does technology diversity help ensure cybersecurity resilience?
    1. It ensures that a vulnerability in a single company's product will not impact the entire infrastructure.
    2. If a single vendor goes out of business, the company does not need to replace its entire infrastructure.
    3. It means that a misconfiguration will not impact the company's entire infrastructure.
    4. All of the above.
16. Scott sends his backups to a company that keeps them in a secure vault. What type of backup solution has he implemented?
    1. Nearline
    2. Safe
    3. Onsite
    4. Offsite
17. Gabby wants to detect physical brute-force attempts against her organization. What solution is best suited to this?
    1. Security guards
    2. Locks
    3. Access badges
    4. An intrusion detection system (IDS)
18. Florian wants to test his high-availability designs but does not want to interrupt his organization's normal work. Which of the following is the least disruptive testing scenario?
    1. A failover exercise
    2. A tabletop exercise
    3. A partial failover exercise
    4. A simulation
19. What type of physical security control is shown here?

Larger View

* 1. A Faraday cage
  2. An access control vestibule
  3. A bollard
  4. An air gap

1. Gurvinder identifies a third-party datacenter provider over 90 miles away to run his redundant datacenter operations. Why has he placed the datacenter that far away?
   1. Because it is required by law
   2. Network traffic latency concerns
   3. Geographic dispersion
   4. Geographic tax reasons

Ch 10

**Review Questions**

1. Kevin discovered that his web server was being overwhelmed by traffic, causing a CPU bottleneck. Using the interface offered by his cloud service provider, he added another CPU to the server. What term best describes Kevin's action?
   1. Elasticity
   2. Horizontal scaling
   3. Vertical scaling
   4. High availability
2. Fran's organization uses a Type I hypervisor to implement an IaaS offering that it sells to customers. Which one of the following security controls is least applicable to this environment?
   1. Customers must maintain security patches on guest operating systems.
   2. The provider must maintain security patches on the hypervisor.
   3. The provider must maintain security patches on the host operating system.
   4. Customers must manage security groups to mediate network access to guest operating systems.
3. In what cloud security model does the cloud service provider bear the most responsibility for implementing security controls?
   1. IaaS
   2. FaaS
   3. PaaS
   4. SaaS
4. Greg would like to find a reference document that describes how to map cloud security controls to different regulatory standards. What document would best assist with this task?
   1. CSA CCM
   2. NIST SP 500-292
   3. ISO 27001
   4. PCI DSS
5. Wanda is responsible for a series of seismic sensors placed at remote locations. These sensors have low-bandwidth connections, and she would like to place computing power on the sensors to allow them to preprocess data before it is sent back to the cloud. What term best describes this approach?
   1. Edge computing
   2. Client-server computing
   3. Fog computing
   4. Thin client computing
6. Which one of the following statements about cloud computing is incorrect?
   1. Cloud computing offers ubiquitous, convenient access.
   2. Cloud computing customers store data on hardware that is shared with other customers.
   3. Cloud computing customers provision resources through the service provider's sales team.
   4. Cloud computing resources are accessed over a network.
7. Helen designed a new payroll system that she offers to her customers. She hosts the payroll system in AWS and her customers access it through the web. What tier of cloud computing best describes Helen's service?
   1. PaaS
   2. SaaS
   3. FaaS
   4. IaaS
8. Which cloud computing deployment model requires the use of a unifying technology platform to tie together components from different providers?
   1. Public cloud
   2. Private cloud
   3. Community cloud
   4. Hybrid cloud
9. Which one of the following would not commonly be available as an IaaS service offering?
   1. CRM
   2. Storage
   3. Networking
   4. Computing
10. Which one of the following is *not* an example of infrastructure as code?
    1. Defining infrastructure in JSON
    2. Writing code to interact with a cloud provider's API
    3. Using a cloud provider's web interface to provision resources
    4. Defining infrastructure in YAML
11. Brian is selecting a CASB for his organization, and he would like to use an approach that interacts with the cloud provider directly. Which CASB approach is most appropriate for his needs?
    1. Inline CASB
    2. Outsider CASB
    3. Comprehensive CASB
    4. API-based CASB
12. In which of the following cloud categories are customers typically charged based on the number of virtual server instances dedicated to their use?
    1. IaaS only
    2. SaaS only
    3. IaaS and PaaS
    4. IaaS, SaaS, and PaaS
13. Brian would like to limit the ability of users inside his organization to provision expensive cloud server instances without permission. What type of control would best help him achieve this goal?
    1. Resource policy
    2. Security group
    3. Multifactor authentication
    4. Secure web gateway
14. Ursula would like to link the networks in her on-premises datacenter with cloud VPCs in a secure manner. What technology would help her best achieve this goal?
    1. Transit gateway
    2. HSM
    3. VPC endpoint
    4. SWG
15. What component of a virtualization platform is primarily responsible for preventing VM escape attacks?
    1. Administrator
    2. Guest operating system
    3. Host operating system
    4. Hypervisor
16. Ryan is selecting a new security control to meet his organization's objectives. He would like to use it in their multicloud environment and would like to minimize the administrative work required from his fellow technologists. What approach would best meet his needs?
    1. Third-party control
    2. Internally developed control
    3. Cloud-native control
    4. Any of the above
17. Kira would like to implement a security control that can implement access restrictions across all of the SaaS solutions used by her organization. What control would best meet her needs?
    1. Security group
    2. Resource policy
    3. CASB
    4. SWG
18. Howard is assessing the legal risks to his organization based on its handling of PII. The organization is based in the United States, handles the data of customers located in Europe, and stores information in Japanese datacenters. What law would be most important to Howard during his assessment?
    1. Japanese law
    2. European Union law
    3. U.S. law
    4. All should have equal weight.
19. Brenda's company provides a managed incident response service to its customers. What term best describes this type of service offering?
    1. MSP
    2. PaaS
    3. SaaS
    4. MSSP
20. Tony purchases virtual machines from Microsoft Azure exclusively for use by his organization. What model of cloud computing is this?
    1. Public cloud
    2. Private cloud
    3. Hybrid cloud
    4. Community cloud

Ch 11

**Review Questions**

1. Lin's hardware manufacturer has stopped selling the model of device that Lin's organization uses and has also stopped providing security or other updates. What phase of the hardware life cycle is the device in?
   1. End-of-life
   2. Legacy
   3. End-of-sales
   4. Senescence
2. Naomi has discovered the following TCP ports open on a system she wants to harden. Which ports are used for unsecure services and thus should be disabled to allow their secure equivalents to continue to be used?
   1. 21, 22, and 80
   2. 21 and 80
   3. 21, 23, and 80
   4. 22 and 443
3. Frank's organization is preparing to deploy a data loss prevention (DLP) system. What key process should they undertake before they deploy it?
   1. Define data life cycles for all nonsensitive data.
   2. Encrypt all sensitive data.
   3. Implement and use a data classification scheme.
   4. Tag all data by creator or owner.
4. Oliver wants to store and manage secrets in his cloud service provider's environment. What type of solution should he look for as part of their offerings?
   1. A TPM
   2. A secure enclave
   3. A KMS
   4. A Titan M
5. What is the key difference between EDR and XDR solutions?
   1. The variety of malware it can detect
   2. The number of threat feeds that are used
   3. The breadth of the technology stack that is covered
   4. The volume of logs that can be processed
6. Michelle wants to prevent unauthorized applications from being installed on a Windows system. What type of tool can she use to stop applications from being installed?
   1. Antivirus
   2. A GPO
   3. An EDR
   4. A HIPS
7. What term is used to describe tools focused on detecting and responding to suspicious activities occurring on endpoints like desktops, laptops, and mobile devices?
   1. EDR
   2. IAM
   3. FDE
   4. ESC
8. Fred has recently purchased a network router and is preparing to deploy it. Which of the following is a common step in deploying new routers?
   1. Disabling unwanted services
   2. Removing unnecessary software
   3. Installing antivirus
   4. Changing default passwords
9. Charlene wants to prevent attacks against her system that leverage flaws in the services that it provides while still keeping the services accessible. What hardening technique should she use?
   1. A host-based firewall
   2. A host-based IPS
   3. Encryption
   4. An EDR
10. Allan is preparing to harden his organization's network switches. Which of the following is not a common hardening technique for network devices?
    1. Removing unnecessary software
    2. Installing patches
    3. Administrative VLANs
    4. Changing default passwords
11. Helen's organization is planning to deploy IoT devices across their buildings as part of a HVAC system. Helen knows that the vendor for the IoT devices does not provide regular security updates to the device's web interfaces that are used to manage the devices. What security control should she recommend to help protect the devices on the network?
    1. Install host-based firewalls.
    2. Deploy the IoT devices to a protected VLAN.
    3. Install host-based IPS.
    4. Disable the web interfaces for the IoT devices.
12. What is the primary reason to remove unnecessary software during hardening efforts?
    1. To reduce the attack footprint of the device
    2. To reduce the number of patches that are installed
    3. To reduce the number of firewall rules required for the device
    4. To support incident response (IR) activities
13. Brian has deployed a system that monitors sensors and uses that data to manage the power distribution for the power company that he works for. Which of the following terms is commonly used to describe this type of control and monitoring solution?
    1. SCADA
    2. SIM
    3. HVAC
    4. AVAD
14. The organization that Lynn works for wants to deploy an embedded system that needs to process data as it comes in to the device without processing delays or other interruptions. What type of solution does Lynn's company need to deploy?
    1. An MFP
    2. A HIPS
    3. An SoC
    4. An RTOS
15. Which of the following is not a common constraint of an embedded system?
    1. Compute
    2. Cost
    3. Network
    4. Authentication
16. Jim configures a Windows machine with the built-in BitLocker full-disk encryption tool that uses a TPM chip. When is the machine least vulnerable to having data stolen from it?
    1. When the machine is off
    2. When the machine is booted and logged in but is locked
    3. When the machine is booted and logged in but is unlocked
    4. When the machine is booted and logged in but is asleep
17. Olivia wants to install a host-based security package that can detect attacks against the system coming from the network, but she does not want to take the risk of blocking the attacks since she fears that she might inadvertently block legitimate traffic. What type of tool could she install that will meet this requirement?
    1. A host firewall
    2. A host-based intrusion detection system
    3. A host-based intrusion prevention system
    4. A data loss prevention tool
18. Anita wants to enforce security settings across her organization's Windows Active Directory domain. What tool can she use to do this?
    1. EDR
    2. Group Policy
    3. XDR
    4. SELinux
19. Chris wants systems that connect to his network to report their boot processes to a server where they can be validated before being permitted to join the network. What technology should he use to do this on the workstations?
    1. UEFI/Trusted boot
    2. BIOS/Trusted boot
    3. UEFI/Measured boot
    4. BIOS/Measured boot
20. Elaine wants to securely erase the contents of a tape used for backups in her organization's tape library. What is the fastest secure erase method available to her that will allow the tape to be reused?
    1. Using a degausser
    2. Wiping the tape by writing a random pattern of 1s and 0s to it
    3. Incinerating the tape
    4. Wiping the tape by writing all 1s or all 0s to it

Ch 12

**Review Questions**

1. A system that Tony manages sends an SNMP trap. What type of information should Tony expect to receive?
   1. Notification of a vulnerability
   2. Notification of a patch being installed
   3. Notification of an issue
   4. Notification of user being created
2. Ben wants to observe malicious behavior targeted at multiple systems on a network. He sets up a variety of systems and instruments to allow him to capture copies of attack tools and to document all the attacks that are conducted. What has he set up?
   1. A honeypot
   2. A beartrap
   3. A honeynet
   4. A tarpit
3. Valerie wants to replace the telnet access that she found still in use in her organization. Which protocol should she use to replace it, and what port will it run on?
   1. SFTP, port 21
   2. SSH, port 22
   3. HTTPS, port 443
   4. RDP, port 3389
4. Jill wants to use DNS filtering to prevent users in her organization from visiting potentially malicious sites. What type of service should she use to obtain this information?
   1. An OSINT service
   2. A STP feed
   3. An ACL monitoring service
   4. A reputation service
5. Chuck wants to provide access to a protected network from a less trusted network. What type of solution is commonly implemented to provide a secure, monitored access method?
   1. A proxy server
   2. A jump server
   3. A VLAN
   4. An air gap
6. Kathleen wants to deploy a firewall that can handle large amounts of network traffic while performing advanced firewalling tasks. What type of device should she select?
   1. A NGFW
   2. A WAF
   3. A UTM
   4. A SD-FW
7. Mark wants to prevent DNS poisoning attacks. What technology should he implement to counter them most effectively?
   1. DNSSEC
   2. SDNS
   3. SASE
   4. SD-WAN
8. Casey wants to replace her organization's MPLS-based external connectivity using commodity technologies. What technology should she select to help her manage this?
   1. IPSec VPN
   2. SASE
   3. SD-WAN
   4. TLS VPN
9. What protocol is used to securely wrap many otherwise insecure protocols?
   1. ISAKMP
   2. SSL
   3. IKE
   4. TLS
10. Valentine wants to deploy a secure version of DHCP for her organization. What should she implement?
    1. S-DHCP
    2. DHCP over TLS
    3. DHCPS
    4. There is no secured version of DHCP.
11. What component of a zero-trust architecture forwards requests from subjects and acts on whether subjects are allowed to access resources?
    1. Policy administrators
    2. Policy enforcement points
    3. Policy engines
    4. Policy gateways
12. Gary wants to use secure protocols for email access for his end users. Which of the following groups of protocols should he implement to accomplish this task?
    1. DKIM, DMARC, HTTPS
    2. SPF, POPS, IMAPS
    3. POPS, IMAPS, HTTPS
    4. DMARC, DKIM, SPF
13. Gary wants to prevent his organization's most sensitive data from being accessed by network-based attackers at any cost. What solution should he implement to ensure this?
    1. An air gap
    2. Firewall rules
    3. An IPS
    4. IPSec
14. Madhuri is designing a load-balancing configuration for her company and wants to keep a single node from being overloaded. What type of design will meet this need?
    1. A daisy chain
    2. Active/active
    3. Duck-duck-goose
    4. Active/passive
15. What type of NAC will provide Isaac with the greatest amount of information about the systems that are connecting while also giving him the most amount of control of systems and their potential impact on other systems that are connected to the network?
    1. Agent-based, preadmission NAC
    2. Agentless, postadmission NAC
    3. Agent-based NAC, postadmission NAC
    4. Agentless, postadmission NAC
16. Danielle's organization has implemented a tool that combines SD-WAN, a CASB, and Zero Trust, among other security functions, to provide security regardless of where her organization's devices are. What type of solution has her organization implemented?
    1. A UTM
    2. An NGFW
    3. IPSec
    4. SASE
17. Wayne is concerned that an on-path attack has been used against computers he is responsible for. What artifact is he most likely to find associated with this attack?
    1. A compromised router
    2. A browser plug-in
    3. A compromised server
    4. A modified hosts file
18. Elle has scanned her organization from an external IP address and has identified all of the services that are visible from the public Internet. What does this enable her to describe?
    1. If the organization is a fail-open organization
    2. Her organization's OSINT report
    3. Her organization's attack surface
    4. If the organization is a fail-closed organization
19. What technique is used to ensure that DNSSEC-protected DNS information is trustworthy?
    1. It is digitally signed.
    2. It is sent via TLS.
    3. It is encrypted using AES256.
    4. It is sent via an IPSec VPN.
20. Fred wants to ensure that the administrative interfaces for the switches and routers are protected so that they cannot be accessed by attackers. Which of the following solutions should he recommend as part of his organization's network design?
    1. NAC
    2. Trunking
    3. Out-of-band management
    4. Port security

Ch 13

**Review Questions**

1. Alyssa wants to harden iOS devices her organization uses. What set of guidelines can she follow to align to common industry security practices?
   1. OWASP
   2. CIS benchmarks
   3. NIST 800-103
   4. NIST 800-111
2. Fred's company issues devices in a BYOD model. That means that Fred wants to ensure that corporate data and applications are kept separate from personal applications on the devices. What technology is best suited to meet this need?
   1. Biometrics
   2. Full-device encryption
   3. Context-aware authentication
   4. Containerization
3. Michelle has deployed iPads to her staff who work her company's factory floor. She wants to ensure that the devices work only in the factory and that if they are taken home they cannot access business data or services. What type of solution is best suited to her needs?
   1. Context-aware authentication
   2. Geofencing
   3. Geolocation
   4. Unified endpoint management (UEM)
4. Ivan is running an enterprise wireless network and his heatmap shows that two access points are likely conflicting with each other. What will the enterprise access controller most likely do to handle this conflict?
   1. Increase the broadcast power of one of the access points.
   2. Change the SSID for one of the access points.
   3. Disable one of the access points.
   4. Decrease the broadcast power of the access points.
5. Chris wants to use geolocation technology to find where phones issued by his organization are located. Which of the following is not commonly used as part of geolocation techniques?
   1. Bluetooth
   2. GPS
   3. NFC
   4. Wi-Fi
6. Daniel knows that WPA3 has added a method to ensure that brute-force attacks against weak preshared keys are less likely to succeed. What is this technology called?
   1. SAE
   2. CCMP
   3. PSK
   4. WPS
7. Isabelle needs to select the EAP protocol that she will use with her wireless network. She wants to use a secure protocol that does not require client devices to have a certificate, but she does want to require mutual authentication. Which EAP protocol should she use?
   1. EAP-FAST
   2. EAP-TTLS
   3. PEAP
   4. EAP-TLS
8. Theresa has implemented a technology that keeps data for personal use separate from data for her company on mobile devices used by members of her staff. What is this concept called?
   1. Storage segmentation
   2. Multifactor storage
   3. Full-device encryption
   4. Geofencing
9. A member of Jake's team tells him that he sideloaded applications on his Android-based company owned phone. What has occurred?
   1. Malware was installed on the phone.
   2. The phone was rooted to allow administrative access.
   3. Applications were installed by copying them instead of via an app store.
   4. The organization's MDM was disabled to avoid its management controls.
10. Madhuri disables SMS, MMS, and RCS on phones in her organization. What has she prevented from being sent?
    1. Phone calls and texts
    2. Text messages and multimedia messages
    3. Text messages and firmware updates
    4. Phone calls and multimedia messages
11. What is the most frequent concern that leads to GPS tagging being disabled by some companies via an MDM tool?
    1. Chain of custody
    2. The ability to support geofencing
    3. Privacy
    4. Context-aware authentication
12. Bart wants to use a cellular hotspot to provide Internet connectivity via Wi-Fi. What type of network has he set up for his laptop and phone to connect to?
    1. Ad-hoc
    2. NFC
    3. Point-to-point
    4. RFID
13. Susan wants to ensure that the threat of a lost phone creating a data breach is minimized. What two technologies should she implement to do this?
    1. Wi-Fi and NFC
    2. Remote wipe and FDE
    3. Containerization and NFC
    4. Geofencing and remote wipe
14. What are the two most commonly deployed biometric authentication solutions for mobile devices?
    1. Voice recognition and face recognition
    2. Fingerprint recognition and gait recognition
    3. Face recognition and fingerprint recognition
    4. Voice recognition and fingerprint recognition
15. Alaina wants to modify operating system settings and features on her iOS device and to install applications that are not permitted or available via the Apple App Store. What would she need to do to accomplish this?
    1. Deploy an MDM tool to the phone.
    2. Jailbreak the phone.
    3. Keymod the phone.
    4. Install a third-party operating system.
16. Jerome wants to allow guests to use his organization's wireless network, but he does not want to provide a preshared key. What solution can he deploy to gather information such as email addresses or other contact information before allowing users to access his open network?
    1. WPS capture mode
    2. Kerberos
    3. WPA2
    4. A captive portal
17. Amanda wants to create a view of her buildings that shows Wi-Fi signal strength and coverage. What is this type of view called?
    1. A channel overlay
    2. A PSK
    3. A heatmap
    4. A SSID chart
18. Megan wants to prevent access to phones that are misplaced by members of her organization. Which of the following MDM control options is least likely to help her protect phones that are misplaced?
    1. PINs
    2. Device encryption
    3. Remote wipe
    4. Application management
19. Gurvinder wants to select a mobile device deployment method that provides employees with devices that they can use as though they're personally owned to maximize flexibility and ease of use. Which deployment model should he select?
    1. CYOD
    2. COPE
    3. BYOD
    4. MOTD
20. Octavia discovers that the contact list from her phone has been acquired via a wireless attack. Which of the following is the most likely culprit?
    1. Bluejacking
    2. An evil maid
    3. Bluesnarfing
    4. An evil twin

Ch 14

**Review Questions**

1. The following figure shows the Security+ incident response cycle. What item is missing?

Larger ViewA diagram of a process

Description automatically generated

* 1. Planning
  2. Reporting
  3. Monitoring
  4. Preparation

1. Michael analyzes network traffic, including packet content, as part of his incident response process. What tool should he use?
   1. Syslog
   2. NetFlow
   3. Packet capture
   4. A SIEM
2. Susan wants to create a dashboard that shows her aggregated log events related to logins from different geographic regions. Her goal is to identify impossible travel scenarios. Which of the following solutions should she select to accomplish that goal?
   1. IPS
   2. OS logs
   3. SIEM
   4. Vulnerability scan data
3. Selah wants to ensure that users in her organization can only install applications that are evaluated and approved by the organization's security team. What should she use?
   1. A SIEM
   2. An application deny list
   3. An application allow list
   4. sFlow
4. What is the primary concern with sFlow in a large, busy network?
   1. It may allow buffer overflow attacks against the collector host.
   2. sFlow is not designed for large or complex networks.
   3. sFlow puts extreme load on the flow collector host.
   4. sFlow samples only network traffic, meaning that some detail will be lost.
5. Mark unplugs the network connection from a system that is part of an incident and places tape over its Ethernet jack with a sign that says, “Do not reconnect without approval from IR team.” How is this method best described?
   1. Containment
   2. Isolation
   3. Segmentation
   4. Zoning
6. The company that Ben works for wants to test its incident response plan. Ben gathers the incident response team in a room and walks through a scenario to validate the organization's processes and procedures. What type of event has Ben hosted?
   1. A checklist exercise
   2. A simulation
   3. A tabletop exercise
   4. A fail-over exercise
7. Madhuri wants to check a PNG-formatted photo for GPS coordinates. Where can she find that information if it exists in the photo?
   1. In the location.txt file appended to the PNG
   2. On the original camera
   3. In the photo's metadata
   4. In the photo as a steganographically embedded data field
8. Alyssa has identified malware on a system. She removes the system from the network to ensure that it cannot impact other systems. What technique has she used to deal with this system?
   1. Quarantine
   2. Segmentation
   3. Converted it to agentless
   4. Deny listing
9. Kristen discovers missing logs as part of her threat hunting activities. What has most likely happened?
   1. The logs hit the end of their life cycle and were rotated.
   2. The system is a newly deployed system.
   3. An attacker wiped the logs to hide evidence.
   4. An attacker encrypted the logs as part of their process.
10. Ian has been receiving hundreds of false positive alerts from his SIEM every night when scheduled jobs run across his datacenter. What should he adjust on his SIEM to reduce the false positive rate?
    1. Trend analysis
    2. Sensitivity
    3. Correlation rules
    4. Dashboard configuration
11. Which team member acts as a primary conduit to senior management on an IR team?
    1. Communications and public relations
    2. Information security
    3. Management
    4. Technical expert
12. Dana is reviewing her system's application logs and notices that a full backup of the application was done at 10 a.m. She knows that the job that runs the backup process is set to run overnight. What indicator should she flag this as?
    1. Unexpected logs
    2. Resource consumption
    3. Resource inaccessibility
    4. Out-of-cycle logging
13. Jim wants to view log entries that describe actions taken by applications on a Red Hat Linux system. Which of the following tools can he use on the system to view those logs?
    1. logger
    2. syslog-ng
    3. journalctl
    4. tail
14. Megan wants to ensure that logging is properly configured for her organization's Windows workstations. What could she use to ensure that logging best practices are configured?
    1. SIEM
    2. Benchmarks
    3. Syslog
    4. Agents
15. Chris has turned on logon auditing for a Windows system. Which log will show them?
    1. The Windows Application log
    2. The Windows Security log
    3. The Windows System log
    4. All of the above
16. Jayne wants to determine why a ransomware attack was successful against her organization. She plans to conduct a root cause analysis. Which of the following is not a typical root cause analysis method?
    1. Root/branch review
    2. Five whys
    3. Event analysis
    4. Diagramming
17. Hitesh wants to keep a system online but limit the impact of the malware that was found on it while an investigation occurs. What method from the following list should he use?
    1. Containment
    2. Isolation
    3. Segmentation
    4. Black holing
18. What phase in the incident response process leverages indicators of compromise and log analysis as part of a review of events?
    1. Preparation
    2. Containment
    3. Eradication
    4. Identification
19. Henry wants to check to see if services were installed by an attacker. What commonly gathered organizational data can he use to see if a new service appeared on systems?
    1. Registry dumps from systems throughout his organization
    2. Firewall logs
    3. Vulnerability scans
    4. Flow logs

Ch 15

**Review Questions**

1. Felix wants to make an exact copy of a drive using a Linux command-line tool as part of a forensic acquisition process. What command should he use?
   1. df
   2. cp
   3. dd
   4. ln
2. Greg is preparing a forensic report and needs to describe the tools that were used. What should he report about the tools in addition to their names?
   1. The type of system the tools were installed or run on
   2. The training level or certifications of the team that uses the tools
   3. Any known limitations or issues with the tools
   4. The patch level or installed version of the tools
3. Gabby is preparing chain-of-custody documentation and identifies a gap in hand-off documentation for an original source forensic drive. What issue should she expect to encounter due to this gap?
   1. The evidence may not be admissible in court.
   2. The forensic activities may need to be repeated.
   3. The staff involved may have to re-create the missed log.
   4. The chain of custody may need to be edited to note the problem.
4. Mike's organization has recently moved to a SaaS cloud service and needs to collect forensic data from the cloud service. What process can Mike use to gather the information he needs?
   1. Install forensic imaging software on the cloud service's servers.
   2. Identify the log information available and request any other desired information from the cloud service provider.
   3. Engage law enforcement to acquire the forensic data.
   4. Request the forensic information from third-party auditors.
5. Charles wants to obtain a forensic copy of a running virtual machine. What technique should he use to capture the image?
   1. Run dd from within the running machine.
   2. Use FTK Imager from the virtual machine host.
   3. Use the VM host to create a snapshot.
   4. Use WinHex to create a copy from within the running machine.
6. Melissa wants to capture network traffic for forensic purposes. What tool should she use to capture it?
   1. A forensic suite
   2. Wireshark
   3. dd
   4. WinHex
7. Frank is concerned about the admissibility of his forensic data. Which of the following is not an element he should be concerned about?
   1. Whether the forensic source data has remained unaltered
   2. Whether the practices and procedures would survive review by experts
   3. Whether the evidence is relevant to the case
   4. Whether the forensic information includes a time stamp
8. What is the document that tracks the custody or control of a piece of evidence called?
   1. Evidence log
   2. Audit log
   3. Event report
   4. Chain of custody
9. Isaac is performing a forensic analysis on two systems that were compromised in the same event in the same facility. As he performs his analysis, he notices that the event appears to have happened almost exactly one hour earlier on one system than the other. What is the most likely issue he has encountered?
   1. The attacker took an hour to get to the second system.
   2. One system is set to an incorrect time zone.
   3. The attacker changed the system clock to throw off forensic practitioners.
   4. The forensic tool is reading the time stamps incorrectly.
10. What legal concept determines the law enforcement agency or agencies that will be involved in a case based on location?
    1. Nexus
    2. Nonrepudiation
    3. Jurisdiction
    4. Admissibility
11. Michael wants to acquire the firmware from a running device for analysis. What method is most likely to succeed?
    1. Use forensic memory acquisition techniques.
    2. Use disk forensic acquisition techniques.
    3. Remove the firmware chip from the system.
    4. Shut down the system and boot to the firmware to copy it to a removable device.
12. Charles needs to know about actions an individual performed on a PC. What is the best starting point to help him identify those actions?
    1. Review the system log.
    2. Review the event log.
    3. Interview the individual.
    4. Analyze the system's keystroke log.
13. Maria has acquired a disk image from a hard drive using dd, and she wants to ensure that her process is forensically sound. What should her next step be after completing the copy?
    1. Securely wipe the source drive.
    2. Compare the hashes of the source and target drive.
    3. Securely wipe the target drive.
    4. Update her chain-of-custody document.
14. Alex has been handed a flash media device that was quick-formatted and has been asked to recover the data. What data will remain on the drive?
    1. No data will remain on the drive.
    2. Files will remain but file indexes will not.
    3. File indexes will remain, but the files will be gone.
    4. Files and file indexes will remain on the drive.
15. Naomi is preparing to migrate her organization to a cloud service and wants to ensure that she has the appropriate contractual language in place. Which of the following is not a common item she should include?
    1. Right-to-audit clauses
    2. Right to forensic examination
    3. Choice of jurisdiction
    4. Data breach notification timeframe
16. Alaina wants to maintain chain-of-custody documentation and has created a form. Which of the following is not a common element on a chain-of-custody form?
    1. Item identifier number
    2. Signature of the person transferring the item
    3. Signature of the person receiving the item
    4. Method of transport
17. Henry is following the EDRM model and is preparing to review data. What two key tasks occur during this stage?
    1. Validating that time stamps match between systems and that data is properly hashed to confirm that original data is sent
    2. Validating that the legal hold request is valid and that all documented items are included
    3. Validating that the desired data is included and that information that should not be shared is not included
    4. Validating that chain of custody is ensured and that malicious files are not included
18. Theresa's organization has received a legal hold notice for their files and documents. Which of the following is *not* an action she needs to take?
    1. Ensure that changes to existing documents related to the case are tracked and that originals can be provided.
    2. Preserve all existing documents relevant to the case.
    3. Delete all sensitive documents related to the case.
    4. Prevent backups that contain files related to the case from being overwritten on their normal schedule.
19. Gurvinder wants to follow the order of volatility to guide his forensic data acquisition. Which of the following is the least volatile?
    1. RAM
    2. Data on the hard drive
    3. Backups
    4. Remote logs
20. What is the key difference between hashing and checksums?
    1. Both can validate integrity, but a hash also provides a unique digital fingerprint.
    2. A hash can be reversed, and a checksum cannot be.
    3. Checksums provide greater security than hashing.
    4. Checksums have fewer message collisions than a hash.

Ch 16

**Review Questions**

1. Joe is authoring a document that explains to system administrators one way in which they might comply with the organization's requirement to encrypt all laptops. What type of document is Joe writing?
   1. Policy
   2. Guideline
   3. Procedure
   4. Standard
2. Which one of the following statements is not true about compensating controls under PCI DSS?
   1. Controls used to fulfill one PCI DSS requirement may be used to compensate for the absence of a control needed to meet another requirement.
   2. Controls must meet the intent of the original requirement.
   3. Controls must meet the rigor of the original requirement.
   4. Compensating controls must provide a similar level of defense as the original requirement.
3. What law creates privacy obligations for those who handle the personal information of European Union residents?
   1. HIPAA
   2. FERPA
   3. GDPR
   4. PCI DSS
4. Which one of the following is *not* one of the five core security functions defined by the NIST Cybersecurity Framework?
   1. Identify
   2. Contain
   3. Respond
   4. Recover
5. What ISO standard provides guidance on privacy controls?
   1. 27002
   2. 27001
   3. 27701
   4. 31000
6. Which one of the following documents must normally be approved by the CEO or similarly high-level executive?
   1. Standard
   2. Procedure
   3. Guideline
   4. Policy
7. Greg would like to create an umbrella agreement that provides the security terms and conditions for all future work that his organization does with a vendor. What type of agreement should Greg use?
   1. BPA
   2. MOU
   3. MSA
   4. SLA
8. What organization is known for creating independent security benchmarks covering hardware and software platforms from many different vendors?
   1. Microsoft
   2. Center for Internet Security
   3. Cloud Security Alliance
   4. Cisco
9. What do many organizations use to schedule and coordinate changes for information systems?
   1. Impact analysis
   2. Backout plans
   3. Maintenance windows
   4. Version control
10. Which one of the following would *not* normally be found in an organization's information security policy?
    1. Statement of the importance of cybersecurity
    2. Requirement to use AES-256 encryption
    3. Delegation of authority
    4. Designation of responsible executive
11. Alice, an IT security manager at Acme Corporation, decides to conduct an exercise to test the employees' ability to recognize phishing emails. She creates fake phishing messages and sends them to the employees. When employees click on the links in the fake messages, they are redirected to a training program. What is the primary purpose of the exercise that Alice is conducting?
    1. To penalize the employees who click on the phishing links
    2. To reward employees who identify the fake phishing messages
    3. To test employees' ability to recognize phishing messages and help them improve
    4. To gather data for a report on the most gullible departments
12. Tonya discovers that an employee is running a side business from his office, using company technology resources. What policy would most likely contain information relevant to this situation?
    1. NDA
    2. AUP
    3. Data ownership
    4. Data classification
13. What compliance obligation applies to merchants and service providers who work with credit card information?
    1. FERPA
    2. SOX
    3. HIPAA
    4. PCI DSS
14. Mike is an information security manager at TechRise Solutions. The company has been experiencing an increase in security incidents, and senior management is concerned about the security posture of the organization. They have asked Mike to take proactive measures to strengthen the company's security culture. What should be Mike's primary role in enhancing the security awareness and training at TechRise Solutions?
    1. To delegate all security responsibilities to the HR department
    2. To establish, promote, and maintain security training and awareness programs
    3. To create and distribute security awareness posters
    4. To personally conduct security training sessions for all employees
15. Colin would like to implement a security control in his accounting department that is specifically designed to detect cases of fraud that are able to occur despite the presence of other security controls. Which one of the following controls is best suited to meet Colin's need?
    1. Separation of duties
    2. Least privilege
    3. Dual control
    4. Mandatory vacations
16. Which one of the following security policy framework components does not contain mandatory guidance for individuals in the organization?
    1. Policy
    2. Standard
    3. Procedure
    4. Guideline
17. Rachel is the Head of Security at WebCraft Inc. She wants to create both security training and awareness programs. Which statement best captures the difference between these programs?
    1. Security training requires time to learn new material, whereas awareness efforts use techniques like posters and emails to remind employees of security lessons.
    2. Security training involves giving rewards to employees, whereas awareness efforts involve punishments.
    3. There is no difference; both terms can be used interchangeably.
    4. Security training is for security team members only, whereas security awareness is for all employees.
18. Allan is developing a document that lists the acceptable mechanisms for securely obtaining remote administrative access to servers in his organization. What type of document is Allan writing?
    1. Policy
    2. Standard
    3. Guideline
    4. Procedure
19. Which one of the following is not a common use of the NIST Cybersecurity Framework?
    1. Describe the current cybersecurity posture of an organization.
    2. Describe the target future cybersecurity posture of an organization.
    3. Communicate with stakeholders about cybersecurity risk.
    4. Create specific technology requirements for an organization.
20. Which one of the following items is *not* normally included in a request for an exception to security policy?
    1. Description of a compensating control
    2. Description of the risks associated with the exception
    3. Proposed revision to the security policy
    4. Business justification for the exception

Ch 17

**Review Questions**

1. Jen identified a missing patch on a Windows server that might allow an attacker to gain remote control of the system. After consulting with her manager, she applied the patch. From a risk management perspective, what has she done?
   1. Removed the threat
   2. Reduced the threat
   3. Removed the vulnerability
   4. Reduced the vulnerability
2. You notice a high number of SQL injection attacks against a web application run by your organization, so you install a web application firewall to block many of these attacks before they reach the server. How have you altered the severity of this risk?
   1. Reduced the magnitude
   2. Eliminated the vulnerability
   3. Reduced the probability
   4. Eliminated the threat
3. Questions 3–7 refer to the following scenario:

Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm’s customers. He expects that a compromise of that database would result in $500,000 of fines against his firm.

Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent chance of a successful attack in any given year.

What is the asset value (AV)?

* 1. $5,000
  2. $100,000
  3. $500,000
  4. $600,000

1. What is the exposure factor (EF)?
   1. 5%
   2. 20%
   3. 50%
   4. 100%
2. What is the single loss expectancy (SLE)?
   1. $5,000
   2. $100,000
   3. $500,000
   4. $600,000
3. What is the annualized rate of occurrence (ARO)?
   1. 0.05
   2. 0.20
   3. 2.00
   4. 5.00
4. What is the annualized loss expectancy (ALE)?
   1. $5,000
   2. $25,000
   3. $100,000
   4. $500,000
5. Questions 8–11 refer to the following scenario:

Grace recently completed a risk assessment of her organization’s exposure to data breaches and determined that there is a high level of risk related to the loss of sensitive personal information. She is considering a variety of approaches to managing this risk.

Grace's first idea is to add a web application firewall to protect her organization against SQL injection attacks. What risk management strategy does this approach adopt?

* 1. Risk acceptance
  2. Risk avoidance
  3. Risk mitigation
  4. Risk transference

1. Business leaders are considering dropping the customer activities that collect and store sensitive personal information. What risk management strategy would this approach use?
   1. Risk acceptance
   2. Risk avoidance
   3. Risk mitigation
   4. Risk transference
2. Grace's company decided to install the web application firewall and continue doing business. They are still worried about other risks to the information that were not addressed by the firewall and are considering purchasing an insurance policy to cover those risks. What strategy does this use?
   1. Risk acceptance
   2. Risk avoidance
   3. Risk mitigation
   4. Risk transference
3. In the end, Grace's risk managers found that the insurance policy was too expensive and opted not to purchase it. They are taking no additional action. What risk management strategy is being used in this situation?
   1. Risk acceptance
   2. Risk avoidance
   3. Risk mitigation
   4. Risk transference
4. Under the European Union's GDPR, what term is assigned to the individual who leads an organization's privacy efforts?
   1. Data protection officer
   2. Data controller
   3. Data steward
   4. Data processor
5. Helen's organization maintains medical records on behalf of its customers, who are individual physicians. What term best describes the role of Helen's organization?
   1. Data processor
   2. Data controller
   3. Data owner
   4. Data steward
6. Gene recently conducted an assessment and determined that his organization can be without its main transaction database for a maximum of two hours before unacceptable damage occurs to the business. What metric has Gene identified?
   1. MTBF
   2. MTTR
   3. RTO
   4. RPO
7. Tina works for a hospital system and manages the system's patient records. What category of personal information best describes the information that is likely to be found in those records?
   1. PCI
   2. PHI
   3. PFI
   4. PII
8. Asa believes that her organization is taking data collected from customers for technical support and using it for marketing without their permission. What principle is most likely being violated?
   1. Data minimization
   2. Data retention
   3. Purpose limitation
   4. Data sovereignty
9. Which one of the following U.S. government classification levels requires the highest degree of security control?
   1. Secret
   2. Confidential
   3. Top Secret
   4. Unclassified
10. Which type of analysis uses numeric data in the analysis, resulting in assessments that allow the very straightforward prioritization of risk?
    1. Qualitative
    2. One-time
    3. Recurring
    4. Quantitative
11. What term is given to an individual or organization who determines the reasons for processing personal information?
    1. Data steward
    2. Data controller
    3. Data processor
    4. Data custodian
12. Brian recently conducted a risk mitigation exercise and has determined the level of risk that remains after implementing a series of controls. What term best describes this risk?
    1. Inherent risk
    2. Control risk
    3. Risk appetite
    4. Residual risk

ANSWERS

**Appendix: Answers to Review Questions**

**Chapter 1: Today's Security Professional**

1. D. Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Threat assessment is an example of one of these activities.
2. B. The breach of credit card information may cause many different impacts on the organization, including compliance, operational, and financial risks. However, in this scenario, Jade's primary concern is violating PCI DSS, making his concern a compliance risk.
3. C. The defacement of a website alters content without authorization and is, therefore, a violation of the integrity objective. The attackers may also have breached the confidentiality or availability of the website, but the scenario does not provide us with enough information to draw those conclusions.
4. B. In this case, the first 12 digits of the credit card have been removed and replaced with asterisks. This is an example of data masking.
5. D. Deterrent controls are designed to prevent an attacker from attempting to violate security policies in the first place. Preventive controls would attempt to block an attack that was about to take place. Corrective controls would remediate the issues that arose during an attack. Detective controls detect issues or indicators of issues.
6. D. In this case, Greg must use a network-based DLP system. Host-based DLP requires the use of agents, which would not be installed on guest systems. Greg may use watermarking and/or pattern recognition to identify the sensitive information, but he must use network-based DLP to meet his goal.
7. B. Data being sent over a network is data in transit. Data at rest is stored data that resides on hard drives, tapes, in the cloud, or on other storage media. Data in processing, or data in use, is data that is actively in use by a computer system.
8. A. Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.
9. D. The three primary goals of cybersecurity attackers are disclosure, alteration, and denial. These map directly to the three objectives of cybersecurity professionals: confidentiality, integrity, and availability.
10. A. The risk that Tony is contemplating could fit any one of these categories. However, his primary concern is that the company may no longer be able to do business if the risk materializes. This is a strategic risk.
11. C. Although it is possible that a frequent flyer account number, or any other account number for that matter, could be used in identity theft, it is far more likely that identity thieves would use core identity documents. These include drivers' licenses, passports, and Social Security numbers.
12. A. As an organization analyzes its risk environment, technical and business leaders determine the level of protection required to preserve the confidentiality, integrity, and availability of their information and systems. They express these requirements by writing the control objectives that the organization wishes to achieve. These control objectives are statements of a desired security state.
13. D. This question is a little tricky. The use of an actual guard dog could be considered a deterrent, physical, or detective control. It could even be a compensating control in some circumstances. However, the question asks about the presence of a *sign* and does not state that an actual dog is used. The sign only has value as a deterrent control. Be careful when facing exam questions like this to read the details of the question.
14. D. Encryption technology uses mathematical algorithms to protect information from prying eyes, both while it is in transit over a network and while it resides on systems. Encrypted data is unintelligible to anyone who does not have access to the appropriate decryption key, making it safe to store and transmit encrypted data over otherwise insecure means.
15. D. The use of full-disk encryption is intended to prevent a security incident from occurring if a device is lost or stolen. Therefore, this is a preventive control gap.
16. A. Although a health-care provider may be impacted by any of these regulations, the Health Insurance Portability and Accountability Act (HIPAA) provides direct regulations for the security and privacy of protected health information and would have the most direct impact on a health-care provider.
17. C. The disclosure of sensitive information to unauthorized individuals is a violation of the principle of confidentiality.
18. B. The three primary objectives of cybersecurity professionals are confidentiality, integrity, and availability.
19. A. Tokenization techniques use a lookup table and are designed to be reversible. Masking and hashing techniques replace the data with values that can't be reversed back to the original data if performed properly. Shredding, when conducted properly, physically destroys data so that it may not be recovered.
20. A. PCI DSS compensating controls must be “above and beyond” other PCI DSS requirements. This specifically bans the use of a control used to meet one requirement as a compensating control for another requirement.

**Chapter 2: Cybersecurity Threat Landscape**

1. B. Although higher levels of detail can be useful, they aren't a common measure used to assess threat intelligence. Instead, the timeliness, accuracy, and relevance of the information are considered critical to determining whether you should use the threat information.
2. C. Hacktivists are defined by the motivation behind their actions—advancing their political or philosophical beliefs. They engage in cyberattacks that they believe will advance their causes.
3. A. Attacks that are conducted as part of an authorized penetration test are white-hat hacking attacks, regardless of whether they are conducted by internal employees or an external firm. Kolin is, therefore, engaged in white-hat hacking. If he were acting on his own, without authorization, his status would depend on his intent. If he had malicious intent, his activity would be considered black-hat hacking. If he simply intended to report vulnerabilities to the hospital, his attack would be considered gray hat and he would likely be semi-authorized.
4. A. Advanced persistent threats (APTs) are most commonly associated with nation-state actors. It is unlikely that an APT group would leverage the unsophisticated services of an unskilled script kiddie type attacker. It is also unlikely that a hacktivist would have access to APT resources. Although APTs may take advantage of insider access, they are most commonly associated with nation-state actors.
5. D. The U.S. government created the Information Sharing and Analysis Centers (ISACs). ISACs help infrastructure owners and operators share threat information, and provide tools and assistance to their members.
6. A. Nation-state actors are government sponsored, and they typically have the greatest access to resources, including tools, money, and talent.
7. A. Email is the most common threat vector exploited by attackers who use phishing and other social engineering tactics to gain access to an organization. The other vectors listed here, direct access, wireless, and removable media, all require physical proximity to an organization and are not easily executed from a remote location.
8. D. The Chinese military and U.S. government are examples of nation-state actors and advanced persistent threats (APTs). The Russian mafia is an example of a criminal syndicate. Anonymous is the world's most prominent hacktivist group.
9. A. Behavioral assessments are very useful when you are attempting to identify insider threats. Since insider threats are often hard to distinguish from normal behavior, the context of the actions performed—such as after-hours logins, misuse of credentials, logins from abnormal locations, or abnormal patterns—and other behavioral indicators are often used.
10. D. Supply chain attacks are typically associated with vendors and suppliers that provide technology infrastructure or services that may be compromised. This would include hardware and software providers as well as managed service providers (MSPs). Talent providers, who help with staffing solutions, are generally not considered common avenues for supply chain attacks.
11. A. Tampering with equipment before it reaches the intended user is an example of a supply chain threat. It is also possible to describe this attack as a direct access attack because it involved physical access to the device, but supply chain is a more relevant answer. You should be prepared to select the best possible choice from several possible correct answers when you take the exam. Security+ questions often use this type of misdirection.
12. B. All of these resources might contain information about the technical details of TLS, but Internet Request for Comments (RFC) documents are the definitive technical standards for Internet protocols. Consulting the RFCs would be Ken's best option.
13. C. All of these items could be concerning, depending on the circumstances. However, API keys should *never* be found in public repositories because they may grant unauthorized individuals access to information and resources.
14. A. Threat maps are graphical tools that display information about the geographic locations of attackers and their targets. These tools are most often used as interesting marketing gimmicks, but they can also help identify possible threat sources.
15. B. Specific details of attacks that may be used to identify compromises are known as indicators of compromise (IoCs). This data may also be described as an adversary tactics, techniques, and procedures (TTP), but the fact that it is a set of file signatures makes it more closely match the definition of an IoC.
16. A. The developers in question are using unapproved technology for business purposes. This is the classic definition of shadow IT. It is possible to describe this as data exfiltration, but there is no indication that the data security has been compromised, so shadow IT is a better description here. Remember, you will often be asked to choose the best answer from multiple correct answers on the exam.
17. A. Tom's greatest concern should be that running unsupported software exposes his organization to the risk of new, unpatchable vulnerabilities. It is certainly true that they will no longer receive technical support, but this is a less important issue from a security perspective. There is no indication in the scenario that discontinuing the product will result in the theft of customer information or increased costs.
18. C. Port scans are an active reconnaissance technique that probe target systems and would not be considered open source intelligence (OSINT). Search engine research, DNS lookups, and WHOIS queries are all open source resources.
19. A, C. As a government contractor, Snowden had authorized access to classified information and exploited this access to make an unauthorized disclosure of that information. This clearly makes him fit into the category of an insider. He did so with political motivations, making him fit the category of hacktivist as well.
20. C. Renee was not authorized to perform this security testing, so her work does not fit into the category of white-hat hacking, or authorized hacking. However, she also does not have malicious intent, so her work cannot be categorized as an unauthorized, or black-hat attack. Instead, it fits somewhere in between the two extremes and would best be described as semi-authorized, or gray-hat hacking.

**Chapter 3: Malicious Code**

1. B. Logic bombs are embedded in code, so Ryan's organization would get the most benefit from a code review process for any code that goes into production. Antivirus and EDR are unlikely to detect logic bombs created by staff in Ryan's organization.
2. C. Rootkits are intended to be stealthy, and a pop-up demanding ransom works against that purpose. File hashes, command and control details, and behavior-based identifiers are all useful IoCs likely to be relevant to a rootkit.
3. A. Nathan should check the staff member's computer for a keylogger, which would have captured their username and password. A student could have then used the staff member's credentials to make the changes described. A rootkit would be used to retain access, spyware gathers a variety of data but is not specifically aimed at capturing keystrokes like this, and logic bombs have specific events or triggers that cause them to take action.
4. A. Amanda has most likely discovered a botnet's command and control channel, and the system or systems she is monitoring are probably using IRC as the command and control channel. Spyware is likely to simply send data to a central server via HTTP/HTTPS, worms spread by attacking vulnerable services, and a hijacked web browser would probably operate on common HTTP or HTTPS ports (80/443).
5. D. Remote access to a system is typically provided by a backdoor. Backdoors may also appear in firmware or even in hardware. None of the other items listed provide remote access by default, although they may have a backdoor as part of a more capable malware package.
6. A. Bloatware is typically not a significant security threat, but it consumes resources like disk space, CPU, and memory. Unfortunately, some bloatware can be vulnerable and may not get regularly patched, meaning it's both useless and a potential risk!
7. C. Spyware is specifically designed to gather information about users and systems and to send that data back to a central collector. Trojans pretend to be useful software and include malicious components, bloatware is preinstalled software that isn't needed, and rootkits are used to conceal malicious software and retain a foothold on compromised systems.
8. D. One of the challenges security practitioners can face when attempting to identify malware is that different antivirus and antimalware vendors will name malware packages and families differently. This means that Matt may need to look at different names to figure out what he is dealing with.
9. D. While keyloggers often focus on keyboard input, other types of input may also be captured, meaning Nancy should worry about any user input that occurred while the keylogger was installed. Keyloggers typically do not target files on systems, although if Nancy finds a keylogger, she may want to check for other malware packages with additional capabilities.
10. C. Ransomware demands payment to be made while typically using encryption to make data inaccessible. Worms, viruses, and rootkits are not defined by behavior like this.
11. B. Rootkits are designed to hide from antimalware scanners and can often defeat locally run scans. Mounting the drive in another system in read-only mode or booting from a USB drive and scanning using a trusted, known good operating system can be an effective way to determine what malware is on a potentially infected system.
12. C. Jaya's former employee is describing a logic bomb, malicious code that will cause harm when a trigger or specific action occurs. In this case, the former employee is claiming that the trigger is them not being employed at the company. Jaya will need to assess all of the code that the employee wrote to determine if a logic bomb exists. Ransomware is a type of malicious software that typically uses encryption to extort a ransom. Extortionware is not a commonly used term. Trojans appear to be useful or desirable software but contain malicious code.
13. B. In most malware infection scenarios, wiping the drive and reinstalling from known good media is the best option available. If the malware has tools that can infect the system BIOS/UEFI, even this may not be sufficient, but BIOS/UEFI resident malware is relatively uncommon. Multiple antivirus and antimalware tools, even if they are set to delete malware, may still fail against unknown or advanced malware packages. Destroying systems is uncommon, expensive, and unlikely to be acceptable to most organizations as a means of dealing with a malware infection.
14. B. The key difference between worms and viruses is how they spread. Worms spread themselves, whereas viruses rely on human interaction.
15. B. Python is an interpreted rather than a compiled language, so Ben doesn't need to use a decompiler. Instead, his best bet is to open the file and review the code to see what it does. Since it was written by an employee, it is unlikely that it will match an existing known malicious package, which means antivirus and antimalware tools and sites will be useless.
16. B. Trojans are often found in application stores where they appear to be innocuous but desirable applications or are listed in confusingly similar ways to legitimate applications. Many organizations choose to lock down the ability to acquire applications from app stores to prevent this type of issue. Since Trojans do not self-spread and rely on user action, patching typically won't prevent them. While users may try to transfer files via USB, this isn't the most common means for modern Trojans to spread.
17. C. Worms often spread via networks, taking advantage of vulnerabilities to install themselves on targeted systems and then to propagate further. Trojans require human interaction to install software that appears desirable. Logic bombs are embedded in code and perform actions when triggers like a date or event occur. Rootkits are used to hide malware and to conceal attacker's actions.
18. D. Unwanted, typically preinstalled programs are known as bloatware. They take up space and resources without providing value, and many organizations either uninstall them or install clean operating system images to avoid them. There is no indication of malicious activity in the question, so these are most likely not viruses, Trojans, or spyware.
19. A. Bots connect to command and control (C&C) systems, allowing them to be updated, controlled, and managed remotely. Worms spread via vulnerabilities, and drones and vampires aren't common terms for malware.
20. A. Randy knows that viruses spread through user interaction with files on thumb drives. A worm would spread itself, a Trojan would look like a useful or desirable file, and there is no indication of spyware in the question.

**Chapter 4: Social Engineering and Password Attacks**

1. B. This email is an attempt to get account information and is a phishing email. Joseph did not enter the URL himself, which is the behavior that a typosquatter relies on. A smishing attack relies on SMS, and a watering hole attack uses a frequently visited website.
2. D. Vishing is a form of phishing done via voice phones call or voicemail. Whaling focuses on targeting important targets for phishing attacks, whereas spoofing is a general term that means faking things. Spooning is not a technical term used for security practices.
3. A. Michele has discovered a brute-force attack, which relies on trying a large number of passwords, often combined with a list of usernames to try. Shoulder surfing attacks involve an attacker watching as a user enters information like a password or credit card data. On-path attacks intercept data sent via a network, and pretexting is a social engineering attack that relies on a believable reason for attackers to need a victim to take action.
4. C. Password spraying involves the use of the same password to attempt to log into multiple accounts. Joanna should search for uses of the same password for different accounts.
5. B. Susan has most likely discovered a business email compromise and should reach out to the impacted organization to inform them of the potentially compromised account. Smishing would occur via SMS, there is nothing in the question to indicate a disinformation campaign was part of this, and there is no URL mentioned and thus typosquatting can be dismissed as well.
6. A. Watering hole attacks rely on compromising or infecting a website that targeted users frequently visit, much like animals will visit a common watering hole. Vishing is phishing via voice, whaling is a targeted phishing attack against senior or important staff, and typosquatting registers similar URLs that are likely to be inadvertently entered in order to harvest clicks or conduct malicious activity.
7. D. The source IP or hostname; the failed login logs with time, date, username, and other information; and the password that was used for each failed attempt would be useful for watching for brute-force attempts. Knowing where the system being logged into is located isn't useful when tracking brute-force attempts.

Logging failed passwords can be problematic as it can reveal actual passwords by allowing log reviewers to see failures driven by typos, so Ben may want to avoid that sort of log even though it can be useful!

1. B. The caller is using pretexting, providing Melissa with a story that relies on urgency and perceived authority to get her to take actions she might normally question. This social engineering attack is not a phishing attack aimed at gathering information or credentials, it does not involve business email accounts being compromised, and carding is not a topic covered in the Security+ exam outline.
2. B. Password spraying attempts try to use a single common password for many user accounts. Determining if a single password is being used over and over can help catch basic password spraying attempts. The time, source IP, or number of failed attempts do not indicate password spraying.
3. A. Misinformation and disinformation campaigns are primarily associated with nation-state actors, but are increasingly used by other organizations and even individuals as well. Watering hole attacks, business email compromise, and password spraying are broadly used attacks.
4. C. Typosquatting uses misspellings and common typos of websites to redirect traffic for profit or malicious reasons. Fortunately in reality, if you visit [smazon.com](http://smazon.com/), you'll be redirected to the actual [amazon.com](http://amazon.com/) website, as Amazon knows about and works to prevent this type of issue. DNS hijacking and hosts file modifications both attempt to redirect traffic to actual URLs or hostnames to different destinations, and pharming does redirect legitimate traffic to fake sites, but typosquatting is the more specific answer.
5. B. Devon is conducting a watering hole attack that leverages a frequently visited site to deploy malware. There is no description of misinformation or disinformation in the question, and there is not a typo described that would lead to a typosquatting attack being successful.
6. C. Brand impersonation attacks are designed to appear to be from a company that recipients are likely to be familiar with, and thus are more likely to elicit a response. While these are a type of phishing, the more specific answer of brand impersonation is the best answer. Pretexting is a social engineering concept that provides a reason for the request. Pharming attacks redirect traffic intended to be sent to a legitimate site to a fake website typically designed to simulate the real one.
7. C. This is an example of an impersonation attack. The pentester impersonated the head of IT in order to achieve their goals. The good news is that it was a penetration tester! Smishing is phishing via SMS, vishing is phishing via voice or voicemail, and pretexting provides a reason that the target should perform an action. Here the attack relied on the authority that Amanda believed the caller had.
8. C. Smishing attacks are SMS-based. Impersonation attacks could use texts but don't specifically rely on them. Watering hole attacks use frequently visited websites, whereas business email compromise attacks focus on gaining access to business email accounts to use in follow-up attacks.
9. D. Sharif has discovered a spraying attack that uses the same password—often a default or common password—with many usernames. Credential harvesting is the process of gathering credentials like usernames and passwords. Impersonation is a social engineering technique used when an attacker pretends to be someone else. BEC, or business email compromise, involves attackers posing as a trusted individual and asking for actions to be performed.
10. B. Smishing is a type of phishing that occurs via text (SMS) message.
11. B. While it's nearly impossible to prevent typosquatting, purchasing and registering the most common typos (typo-domains) related to your organization's domain and redirecting them to your real domain is the most effective option available. Copyrighting or trademarking the domain name does not prevent typosquatting, and typo resolution is not a feature or capability that is available.
12. B. Using an organization's brand in this way is an example of brand impersonation. While this is also an impersonation attack, the more specific description is the best answer here. Misbranding and crypto-phishing were both made up for this question and aren't commonly used terms.
13. C. Disinformation campaigns are used to shift public opinion or to accomplish other goals. They are not limited to nation-state actors but are an increasingly heavily used social engineering tactic at a broad scale. Smishing relies on SMS messages, pretexting involves using a reason that creates urgency or importance in a request from a social engineer, and spraying is a type of password brute forcing.

**Chapter 5: Security Assessment and Testing**

1. C. Threat hunting is an assessment technique that makes an assumption of compromise and then searches the organization for indicators of compromise that confirm the assumption. Vulnerability scanning, penetration testing, and war driving are all assessment techniques that probe for vulnerabilities but do not assume that a compromise has already taken place.
2. D. Credentialed scans only require read-only access to target servers. Renee should follow the principle of least privilege and limit the access available to the scanner.
3. C. Ryan should first run his scan against a test environment to identify likely vulnerabilities and assess whether the scan itself might disrupt business activities.
4. C. An attack complexity of “low” indicates that exploiting the vulnerability does not require any specialized conditions.
5. A. A false positive error occurs when the vulnerability scanner reports a vulnerability that does not actually exist.
6. B. By allowing students to change their own grades, this vulnerability provides a pathway to unauthorized alteration of information. Brian should recommend that the school deploy integrity controls that prevent unauthorized modifications.
7. C. Nmap is a port scanning tool used to enumerate open network ports on a system. Nessus is a vulnerability scanner designed to detect security issues on a system. Nslookup is a DNS information gathering utility. All three of these tools may be used to gather information and detect vulnerabilities. Metasploit is an exploitation framework used to execute and attack and would be better suited for the Attacking and Exploiting phase of a penetration test.
8. A. This vulnerability is corrected by a patch that was released by Microsoft in 2017. A strong patch management program would have identified and remediated the missing patch.
9. B. Intrusion detection systems do not detect vulnerabilities; they detect attacks. The remaining three tools could all possibly discover a cross-site scripting (XSS) vulnerability, but a web application vulnerability scanner is the most likely to detect it because it is specifically designed to test web applications.
10. A. Moving from one compromised system to other systems on the same network is known as lateral movement. Privilege escalation attacks increase the level of access that an attacker has to an already compromised system. Footprinting and OSINT are reconnaissance techniques.
11. A. Audits performed to validate an organization's financial statements are very formal audits that are performed by independent third-party auditors. This makes them external audits. Internal audits may be more or less formal than external audits but they are generally done only to provide assurance to internal parties and not to investors. Penetration tests may be done as part of an audit but they are not audits themselves.
12. C. Bug bounty programs are designed to allow external security experts to test systems and uncover previously unknown vulnerabilities. Bug bounty programs offer successful testers financial rewards to incentivize their participation.
13. D. Backdoors are a persistence tool, designed to make sure that the attacker's access persists after the original vulnerability is remediated. Kyle can use this backdoor to gain access to the system in the future, even if the original exploit that he used to gain access is no longer effective.
14. C. WHOIS lookups use external registries and are an example of open source intelligence (OSINT), which is a passive reconnaissance technique. Port scans, vulnerability scans, and footprinting all require active engagement with the target and are, therefore, active reconnaissance.
15. B. Common Vulnerabilities and Exposures (CVE) provides a standard nomenclature for describing security-related software flaws. Common Platform Enumeration (CPE) provides a standard nomenclature for describing product names and versions. The Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security-related software flaws. Common Configuration Enumeration (CCE) provides a standard nomenclature for discussing system configuration issues.
16. C. Known environment tests are performed with full knowledge of the underlying technology, configurations, and settings that make up the target. Unknown environment tests are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems like an attacker would. Partially known environment tests are a blend of unknown environment and known environment testing. Detailed environment tests are not a type of penetration test.
17. C. The rules of engagement provide technical details on the parameters of the test. This level of detail would not normally be found in a contract or statement of work (SOW). The lessons learned report is not produced until after the test.
18. B. All of these techniques might provide Grace with information about the operating system running on a device. However, footprinting is a technique specifically designed to elicit this information.
19. B. Vulnerabilities with CVSS base scores between 4.0 and 6.9 fit into the medium risk category. Vulnerability scores between 0.1 and 3.9 would be low, between 7.0 and 8.9 would be high, and those between 9.0 and 10.0 would be in the critical risk category.
20. C. The privileges required (PR) metric indicates the type of system access that an attacker must have to execute the attack.

**Chapter 6: Application Security**

1. B. Adam is conducting static code analysis by reviewing the source code. Dynamic code analysis requires running the program, and both mutation testing and fuzzing are types of dynamic analysis.
2. C. Charles should perform user input validation to strip out any SQL code or other unwanted input. Secure session management can help prevent session hijacking, logging may provide useful information for incident investigation, and implementing TLS can help protect network traffic, but only input validation helps with the issue described.
3. A. A parameterized query (sometimes called a prepared statement) uses a prebuilt SQL statement to prevent SQL-based attacks. Variables from the application are fed to the query, rather than building a custom query when the application needs data. Encoding data helps to prevent cross-site scripting attacks, as does input validation. Appropriate access controls can prevent access to data that the account or application should not have access to, but they don't use precompiled SQL statements. Stored procedures are an example of a parameterized query implementation.
4. A. Improper error handling often exposes data to users and possibly attackers that should not be exposed. In this case, knowing what SQL code is used inside the application can provide an attacker with details they can use to conduct further attacks. Code exposure is not one of the vulnerabilities we discuss in this book, and SQL code being exposed does not necessarily mean that SQL injection is possible. While this could be caused by a default configuration issue, there is nothing in the question to point to that problem.
5. B. The application has a race condition, which occurs when multiple operations cause undesirable results due to their order of completion. De-referencing accesses or uses a memory pointer, an insecure function would have security issues in the function itself, and improper error handling would involve an error and how it was displayed or what data it provided.
6. B. Although this example includes continuous integration, the key thing to notice is that the code is then deployed into production. This means that Susan is operating in a continuous deployment environment, where code is both continually integrated and deployed. Agile is a development methodology and often uses CI/CD, but we cannot determine if Susan is using Agile.
7. B. Developers working on active changes to code should always work in the development environment. The test environment is where the software or systems can be tested without impacting the production environment. The staging environment is a transition environment for code that has successfully cleared testing and is waiting to be deployed into production. The production environment is the live system. Software, patches, and other changes that have been tested and approved move to production.
8. B. All of the activities listed here may reduce the risk of the vulnerabilities created by the code. However, Ricky is specifically concerned about the fact that the organization may not be aware of all of the code that it is running. Package monitoring would inventory and monitor these third-party libraries, so that is the best answer here.
9. B. The main benefits of automation are efficiency and time savings, enforcing baselines, standardizing infrastructure configurations, scaling in a secure manner, retaining employees, reducing reaction time, and serving as a workforce multiplier. Technical debt is one of the potential drawbacks of automation.
10. B. This is an example of the guard rails use case for automation. Cybersecurity professionals can use scripting to automatically review user actions and block any that are outside of normal parameters.
11. A. Automation normally increases employee retention. The common drawbacks to automation include complexity, cost, creating single points of failure, incurring technical debt, and creating challenges to ongoing supportability.
12. D. Buffer overflow attacks occur when an attacker manipulates a program into placing more data into an area of memory than is allocated for that program's use. The goal is to overwrite other information in memory with instructions that may be executed by a different process running on the system.
13. A. In an on-path attack, the attacker fools the user into thinking that the attacker is actually the target website and presenting a fake authentication form. They may then authenticate to the website on the user's behalf and obtain the cookie. This is slightly different from a session hijacking attack, where the attacker steals the cookie associated with an active session.
14. A. Code signing provides developers with a way to confirm the authenticity of their code to end users. Developers use a cryptographic function to digitally sign their code with their own private key, and then browsers can use the developer's public key to verify that signature and ensure that the code is legitimate and was not modified by unauthorized individuals.
15. A. This is an example of a reflected attack because the script code is contained within the URL. A persistent or stored attack places the content on a web page or other location where a victim may later access it. DOM-based XSS attacks hide the attack code within the Document Object Model.
16. C. This query string is indicative of a parameter pollution attack. In this case, it appears that the attacker was waging a SQL injection attack and tried to use parameter pollution to slip the attack past content filtering technology. The two instances of the serviceID parameter in the query string indicate a parameter pollution attempt.
17. A. The series of thousands of requests incrementing a variable indicate that the attacker was most likely attempting to exploit an insecure direct object reference vulnerability.
18. C. In this case, the .. operators are the telltale giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the /etc/passwd file on the server.
19. B. Websites use HTTP cookies to maintain sessions over time. If Wendy is able to obtain a copy of the user's session cookie, she can use that cookie to impersonate the user's browser and hijack the authenticated session.
20. A. The use of the SQL WAITFOR command is a signature characteristic of a timing-based SQL injection attack.

**Chapter 7: Cryptography and the PKI**

1. D. In symmetric encryption algorithms, both the sender and the receiver use a shared secret key to encrypt and decrypt the message, respectively.
2. A. Downgrade attacks try to remove or lower the strength of encryption to allow the decryption of sensitive information. Birthday attacks find collisions where two different inputs produce the same hash value output, but there is no discussion of that in this scenario. Homomorphic encryption is not an attack but a technology that protects privacy by encrypting data in a way that preserves the ability to perform computation on that data.
3. D. Norm's actions are designed to protect against the unauthorized disclosure of sensitive information. This is a clear example of protecting confidentiality.
4. A. Steganography is the art of using cryptographic techniques to embed secret messages within another file.
5. A. All of these statements are correct except for the statement that all cryptographic keys should be kept secret. The exception to this rule are public keys used in asymmetric cryptography. These keys should be freely shared.
6. C. Stream ciphers operate on one character or bit of a message (or data stream) at a time. Block ciphers operate on “chunks,” or blocks, of a message and apply the encryption algorithm to an entire message block at the same time.
7. D. AES is the successor to 3DES and DES and is the best choice for a symmetric encryption algorithm. RSA is a secure algorithm, but it is asymmetric rather than symmetric.
8. C. The Online Certificate Status Protocol (OCSP) provides real-time checking of a digital certificate's status using a remote server. Certificate stapling attaches a current OCSP response to the certificate to allow the client to validate the certificate without contacting the OCSP server. Certificate revocation lists (CRLs) are a slower, outdated approach to managing certificate status. Certificate pinning is used to provide an expected key, not to manage certificate status.
9. C. When the 11th employee joins Acme Widgets, they will need a shared secret key with every existing employee. There are 10 existing employees, so 10 new keys are required.
10. B. In an asymmetric encryption algorithm, each employee needs only two keys: a public key and a private key. Adding a new user to the system requires the addition of these two keys for that user, regardless of how many other users exist.
11. D. Extended validation (EV) certificates provide the highest available level of assurance. The CA issuing an EV certificate certifies that they have verified the identity and authenticity of the certificate subject.
12. C. Wildcard certificates protect the listed domain as well as all first-level subdomains. dev.[www.mydomain.com](http://www.mydomain.com/) is a second-level subdomain of [mydomain.com](http://mydomain.com/) and would not be covered by this certificate.
13. A. Root CAs are highly protected and not normally used for certificate issuance. A root CA is usually run as an offline CA that delegates authority to intermediate CAs that run as online CAs.
14. C. The PFX format is most closely associated with Windows systems that store certificates in binary format, whereas the P7B format is used for Windows systems storing files in text format.
15. A. Hardware security modules (HSMs) provide an effective way to manage encryption keys. These hardware devices store and manage encryption keys in a secure manner that prevents humans from ever needing to work directly with the keys.
16. C. A downgrade attack is sometimes used against secure communications such as TLS in an attempt to get the user or system to inadvertently shift to less secure cryptographic modes. The idea is to trick the user into shifting to a less secure version of the protocol, one that might be easier to break.
17. C. When encrypting a message using an asymmetric encryption algorithm, the person performing the encryption does so using the recipient's public key.
18. D. In an asymmetric encryption algorithm, the recipient of a message uses their own private key to decrypt messages that they receive.
19. B. The sender of a message may digitally sign the message by encrypting a message digest with the sender's own private key.
20. A. The recipient of a digitally signed message may verify the digital signature by decrypting it with the public key of the individual who signed the message.

**Chapter 8: Identity and Access Management**

1. D. Angela's organization is acting as an identity provider (IdP). Other members of the federation may act as a service provider or relying party when they allow her users to access their services. Authentication provider is not a named role in typical federation activities.
2. A. Password complexity requirements do not prevent sharing of complex passwords, making it the least effective option from the list. Biometric authentication measures will require the enrolled user to be there, although in some cases such as fingerprint systems, multiple users could each enroll a valid fingerprint for a single account. Both types of one-time passwords could be shared but make it harder and less convenient to share accounts.
3. B. Most cloud services provide identity and authorization tools for their services. Most, although not all, allow customers to set some or even many of the account policies they will use, and most major vendors support some form of multifactor capability.
4. D. Password age is set to prevent users from resetting their password enough times to bypass reuse settings. Complexity, length, and expiration do not influence this.
5. B. SMS messages are not secure and could be accessed by cloning a SIM card or redirecting VoIP traffic, among other possible threat models. Both HOTP and TOTP tokens and applications as well as biometric factors are generally considered more secure than an SMS-based factor.
6. A. A USB security key is an example of a hard, or physical, token. An application is an example of a soft token. A biometric factor might be a fingerprint or faceprint. Attestation is a formal verification that something is true. Attestation tokens were made up for this question.
7. B. Picture password asks users to click on specific, self-defined parts of a picture. This means that clicking on those points is something you know. Something you are involves biometric traits, and somewhere you are relies on geographic locations.
8. A. Linux file permissions are read left to right, with the first three characters indicating read, write, and execute permissions (rwx) for the owner of the file, the second three apply to the group, and the last three to all other users. Any indicated with a – are not allowed for that set.
9. C. Role-based access control (RBAC) sets permissions based on an individual's role, which is typically associated with their job. Attribute-based access control (ABAC) is typically matched to other attributes than the job role. Discretionary access control (DAC) and mandatory access control (MAC) are commonly implemented at the operating system level.
10. D. Fingerprint scanners are found on many mobile devices and laptops, making them one of the most broadly deployed biometric technologies. Facial recognition is also broadly deployed, but it is not mentioned in this question or offered as an option.
11. B. Password length has the largest impact on preventing password cracking. When paired with a strong password hash algorithm and proper use of technology like salting, long passwords are much harder to crack. Complexity is the next most important option, as preventing simple repeated characters and similar problematic passwords helps reduce the probability of easily cracked passwords being used. Reuse limitations and preventing common words are less useful.
12. A. PINs and passwords are both examples of something you know. Something you set is not a type of factor. Biometric factors are an example of something you are, and a physical USB token would be a common example of something you have.
13. C. Password vaulting, which stores passwords for use with proper authentication and rights, is the most appropriate solution for Marie's needs. Ephemeral accounts and just-in-time permissions are typically used under normal circumstances to provide least privilege access as needed. Token-based authentication is not specifically a PAM solution.
14. D. Jill is able to make decisions about the rights she grants on her files, meaning this is a discretionary access control system. A mandatory access control system relies on labels to set access control rules. Rule-based access control systems rely on rules to define access, and attribute-based access control systems grant access based on attributes like job roles or locations.
15. B. OAuth is an authentication protocol that allows services to receive authentication tokens from an identity provider without needing the user's password. LDAP is a directory service and is often used as part of SSO processes. MITRE is a nonprofit organization, and RADIUS is an authentication technology.
16. C. Kyle can assume that his government-issued ID is being used as part of an identity proofing process to validate that he is who he claims to be. Biometric enrollment typically requires interaction with an enrollment process to scan or capture biometric information. Just-in-time permission creation is done when access is requested and does not require government ID, and federation connects identity providers with service providers, which is not described here.
17. A. The principle of least privilege means that users should only be given the permissions necessary to perform their role. Best practice is a general term describing commonly recommended and accepted industry practices. Temporal accounts are ephemeral, or short-lived accounts. Mandatory access control is an access control scheme.
18. C. Without other factors that would require the account to be retained, deprovisioning accounts that belonged to users who have left the organization is a best practice. Transferring accounts or reprovisioning them may expose data to new users or provide them with rights that they should not have.
19. C. A person's name, age, location, job title, and even things like their height or their hair color are all attributes that may be associated with a person's identity. None of these describe biometric factors used for authentication, and identity factors are something you are, something you have, or somewhere you are. Account permissions determine what you can do, not attributes like these.
20. C. Linux users can change who can read, write, or execute files and directories they own, which is discretionary access control (DAC). Mandatory access control (MAC) would enforce settings set by the systems administrator without users having the rights to make their own decisions. While role-based access control is involved, DAC best describes the access control scheme. ABAC is not a default method for setting rights for the Linux filesystem.

**Chapter 9: Resilience and Physical Security**

1. A. Naomi should select a load balancing solution. Load balancers allow multiple systems or services to appear like a single resource and can take systems out of the load-balanced pool to allow for upgrades or changes in resources required. Clustering is used to allow groups of computers to perform the same task, but without a load balancer cannot provide the same transparent service appearing as the same system. Geographic diversity and hot sites are concepts used to provide resilience but don't provide this capability.
2. D. Differential backups back up the changes since the last full backup. Incremental backups back up changes since the last backup, and snapshots are a live copy of a system. This is not a full backup, because it is capturing changes since a full backup.
3. B. Warm sites have systems, connectivity, and power but do not have the live or current data to immediately take over operations. A hot site can immediately take over operations, whereas a cold site has space and power, and likely connectivity, but will require that systems and data be put in place to be used. Cloud sites are not one of the three common types of recovery sites.
4. C. Testing that involves an actual failover to another site or service is failover testing. Parallel processing runs both sites or services at the same time; simulation and tabletops both review what would happen without making the actual change.
5. B. Virtual machine snapshots capture the machine state at a point in time and will allow Felix to clone the system. A full backup and a differential backup can be used to capture the disk for the machine but typically will not capture the memory state and other details of the system state. Live boot media allows you to boot and run a nonpersistent system from trusted media.
6. A. A documented restoration order helps ensure that systems and services that have dependencies start in the right order and that high-priority or mission-critical services are restored first. TOTP and HOTP are types of one-time password technology, and last-known good configurations are often preserved with a snapshot or other technology that can allow a system to return to a known good status after an issue such as a bad patch or configuration change.
7. D. Bollards are physical security controls that prevent vehicles from accessing or ramming doors or other areas. They may look like pillars, planters, or other innocuous objects. An air gap is a physical separation of technology environments; a hot aisle is the aisle where systems in a datacenter exhaust warm air; and unlike in movies, robotic sentries are not commonly deployed and aren't ready to stop vehicles in most current circumstances.
8. D. Encryption is commonly used to ensure that backup media or data that is exposed is not accessible to third parties. This does mean that Alecia must carefully secure the encryption keys for the backup. Hashing that data would not keep it secure, and if only hashes were stored the data would be unrecoverable. Security guards are expensive and not a complete solution if data is inadvertently exposed, and offsite, secure storage locations are a useful and common solution for organizations that want to have remote backups.
9. C. Offsite journaling will allow transactions to be recorded and to remain available if a significant event occurred that involved his datacenter. Snapshots are useful at a point in time but do not retain a transaction log between snapshots.
10. A. Resilience requires capacity planning to ensure that capacity—including staff, technology, and infrastructure—is available when is needed. Although a generator, UPS, various RAID levels, and backups have their place in disaster recovery and contingency planning, they are not the primary focus of resiliency and capacity planning.
11. A. Synchronous replication occurs in real time, whereas asynchronous replication occurs after the fact but more regularly than a backup. Journaled and snapshot-based replication are not specific types of replication.
12. C. Security guards can be one of the costliest physical security controls over time, making the cost of guards one of the most important deciding factors guiding when and where they will be employed. Reliability, training, and the potential for social engineering are all possible issues with security guards, but none of these is the major driver in the decision process.
13. A. Infrared sensors balance lower cost with the ability to detect humans entering and moving in a space. Microwave sensors are more expensive but can provide better coverage, including traveling through some barriers. Ultrasonic sensors are rarely used for this purpose, and pressure sensors are limited to the pad where they are deployed, making them expensive and challenging to use for rooms or larger spaces.
14. C. Fences, lighting, and video surveillance can all help discourage potential malicious actors from entering an area, although a determined adversary will ignore or bypass all three. Platform diversity can help make it harder for attackers to succeed, but this is primarily a resilience tactic, and remains more costly to maintain and implement.
15. D. Technology diversity helps ensure that a single failure—due to a vendor, vulnerability, or misconfiguration—will not impact an entire organization. Technology diversity does have additional costs, including training, patch management, and configuration management.
16. D. Scott has implemented an offsite backup scheme. His backups will take longer to retrieve because they are at a remote facility and will have to be sent back to him, but they are likely to survive any disaster that occurs in his facility or datacenter. Onsite backups are kept immediately accessible, whereas nearline backups can be retrieved somewhat more slowly than online backups but faster than offline backups. “Safe backups” is not an industry term.
17. A. Security guards who can monitor for and understand the signs of a physical brute-force attempt are the most useful control listed. Locks may show signs of attempts but require careful inspection, access badges would require log review and additional information to detect brute-force attacks, and an IDS is useful for network attacks.
18. B. A tabletop exercise is the least disruptive form of exercise. Even simulations have some risk if an employee does not fully realize that the scenario is simulated and takes action. Failover, even partial, involves the potential for disruption.
19. B. An access control vestibule uses a pair of doors. When an individual enters, the first door must be closed and secured before the second door can be opened. This helps prevent tailgating, since the person entering will notice anybody following them through the secured area. A Faraday cage is used to stop electromagnetic interference (EMI), a bollard prevents vehicular traffic, and an air gap is a physical separation of networks or devices.
20. C. Geographic dispersion helps ensure that a single natural or human-made disaster does not disable multiple facilities. This distance is not required by law; latency increases with distance; and though there may be tax reasons in some cases, this is not a typical concern for a security professional.

**Chapter 10: Cloud and Virtualization Security**

1. C. This is an example of adding additional capacity to an existing server, which is also known as vertical scaling. Kevin could also have used horizontal scaling by adding additional web servers. Elasticity involves the ability to both add and remove capacity on demand, and though it does describe this scenario, it's not as good a description as vertical scaling. There is no mention of increasing the server's availability.
2. C. Type I hypervisors, also known as bare-metal hypervisors, run directly on top of the physical hardware and, therefore, do not require a host operating system.
3. D. The cloud service provider bears the most responsibility for implementing security controls in an SaaS environment and the least responsibility in an IaaS environment. This is due to the division of responsibilities under the cloud computing shared responsibility model.
4. A. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a reference document designed to help organizations understand the appropriate use of cloud security controls and map those controls to various regulatory standards. NIST SP 500-292 is a reference model for cloud computing and operates at a high level. ISO 27001 is a general standard for cybersecurity, and PCI DSS is a regulatory requirement for organizations involved in processing credit card transactions.
5. A. This approach may be described as client-server computing, but that is a general term that describes many different operating environments. The better term to use here is edge computing, which involves placing compute power at the client to allow it to perform preprocessing before sending data back to the cloud. Fog computing is a related concept that uses IoT gateway devices that are located in close physical proximity to the sensors.
6. C. One of the key characteristics of cloud computing is that customers can access resources on-demand with minimal service provider interaction. Cloud customers do not need to contact a sales representative each time they wish to provision a resource but can normally do so on a self-service basis.
7. B. Helen is using IaaS services to create her payroll product. She is then offering that payroll service to her customers as a SaaS solution.
8. D. Hybrid cloud environments blend elements of public, private, and/or community cloud solutions. A hybrid cloud requires the use of technology that unifies the different cloud offerings into a single, coherent platform.
9. A. Customer relationship management (CRM) packages offered in the cloud would be classified as software-as-a-service (SaaS), since they are not infrastructure components. Storage, networking, and computing resources are all common IaaS offerings.
10. C. Infrastructure as code (IaC) is any approach that automates the provisioning, management, and deprovisioning of cloud resources. Defining resources through JSON or YAML is IaC, as is writing code that interacts with an API. Provisioning resources through a web interface is manual, not automated, and therefore does not qualify as IaC.
11. D. API-based CASB solutions interact directly with the cloud provider through the provider's API. Inline CASB solutions intercept requests between the user and the provider. Outsider and comprehensive are not categories of CASB solutions.
12. C. Customers are typically charged for server instances in both IaaS environments, where they directly provision those instances, and PaaS environments, where they request the number of servers needed to support their applications. In an SaaS environment, the customer typically has no knowledge of the number of server instances supporting their use.
13. A. Cloud providers offer resource policies that customers may use to limit the actions that users of their accounts may take. Implementing resource policies is a good security practice to limit the damage caused by an accidental command, a compromised account, or a malicious insider.
14. A. Cloud providers offer VPC endpoints that allow connections of VPCs to each other using the cloud provider’s secure network. Cloud transit gateways extend this model even further, allowing the direct interconnection of cloud VPCs with on-premises VLANs for hybrid cloud operations. Secure web gateways (SWGs) provide a layer of application security for cloud-dependent organizations. Hardware security modules (HSMs) are special-purpose computing devices that manage encryption keys and also perform cryptographic operations in a highly efficient manner.
15. D. Virtual machine (VM) escape vulnerabilities are the most serious issue that can exist in a virtualized environment, particularly when a virtual host runs systems of differing security levels. In an escape attack, the attacker has access to a single virtual host and then manages to leverage that access to intrude upon the resources assigned to a different virtual machine. The hypervisor is supposed to prevent this type of access by restricting a virtual machine's access to only those resources assigned to that machine.
16. A. Controls offered by cloud service providers have the advantage of direct integration with the provider's offerings, often making them cost-effective and user-friendly. Third-party solutions are often more costly, but they bring the advantage of integrating with a variety of cloud providers, facilitating the management of multicloud environments.
17. C. Cloud access security brokers (CASBs) are designed specifically for this situation: enforcing security controls across cloud providers. A secure web gateway (SWG) may be able to achieve Kira's goal, but it would be more difficult to do so. Security groups and resource policies are controls used in IaaS environments.
18. D. The principle of data sovereignty states that data is subject to the legal restrictions of any jurisdiction where it is collected, stored, or processed. In this case, Howard needs to assess the laws of all three jurisdictions.
19. D. Brenda's company is offering a technology service to customers on a managed basis, making it a managed service provider (MSP). However, this service is a security service, so the term managed security service provider (MSSP) is a better description of the situation.
20. A. This is an example of public cloud computing because Tony is using a public cloud provider, Microsoft Azure. The fact that Tony is limiting access to virtual machines to his own organization is not relevant because the determining factor for the cloud model is whether the underlying infrastructure is shared, not whether virtualized resources are shared.

**Chapter 11: Endpoint Security**

1. B. Legacy hardware is unsupported and no longer sold. End-of-life typically means that the device is no longer being made but is likely to still have support for a period of time. End-of-sales means the device is no longer being sold, but again, may have support for some time. Senescence is not a term typically used in hardware life cycles.
2. C. The services listed are:
   * 21—FTP
   * 22—SSH
   * 23—Telnet
   * 80—HTTP
   * 443—HTTPS

Of these services, SSH (Port 22) and HTTPS (port 443) are secure options for remote shell access and HTTP. Although secure mode FTP (FTP/S) may run on TCP 21, there is not enough information to know for sure, and HTTPS can be used for secure file transfer if necessary. Thus, Naomi's best option is to disable all three likely unsecure protocols: FTP (port 21), Telnet (port 23), and HTTP (port 80).

1. C. Protecting data using a DLP requires data classification so that the DLP knows which data should be protected and what policies to apply to it. Defining data life cycles can help prevent data from being kept longer than it should be and improves data security by limiting the data that needs to be secured, but it isn't necessary as part of a DLP deployment. Encrypting all sensitive data may mean the DLP cannot recognize it and may not be appropriate for how it is used. Tagging all data with a creator or owner can be useful but is not required for a DLP rollout—instead, knowing the classification of the data is more important.
2. C. Oliver should look for a key management system, or KMS, which will allow him to securely create, store, and manage keys in a cloud environment. TPMs, secure enclaves, and Google's Titan M are all local hardware solutions.
3. C. XDR is similar to EDR but has a broader perspective covering not only endpoints but also cloud services, security platforms, and other components. Thus, the breadth of coverage of the technology stack is broader for XDR solutions.
4. B. A Windows Group Policy Object (GPO) can be used to control whether users are able to install software. Antivirus will not stop this, nor will EDR or a HIPS.
5. A. Endpoint detection and response (EDR) systems provide monitoring, detection, and response capabilities for systems. EDR systems capture data from endpoints and send it to a central repository, where it can be analyzed for issues and indicators of compromise or used for incident response activities. IAM is identity and access management, FDE is full-disk encryption, and ESC is not a commonly used security acronym.
6. D. Network devices as well as many other devices like printers come with default passwords set. Fred should change the default password as part of the process of setting up his new router.
7. B. A host-based intrusion prevention system (HIPS) can detect and prevent attacks against services while allowing the service to be accessible. A firewall can only block based on port, protocol, and IP; encryption won't prevent this; and an EDR is primarily targeted at malicious software and activity, not at network-based attacks on services.
8. A. Unlike computers and mobile devices, switches and other network devices typically do not have additional software that can be removed. Installing patches, placing administrative interfaces on protected VLANs, and changing default passwords are all common hardening techniques for network devices like switches.
9. B. Since the web interfaces are needed to manage the devices, Helen's best option is to place the IoT devices in a protected VLAN. IoT devices will not typically allow additional software to be installed, meaning that adding firewalls or a HIPS won't work.
10. A. Removing unnecessary software helps to reduce the attack surface of the devices. Not all software runs a service or opens a network port, but installed software provides additional opportunities for attackers to find vulnerabilities. That means that reducing firewall rules is not a primary purpose. While removing it may reduce the number of patches required by a device, that is not the primary driver. Finally, while incident response efforts may point to a need for further hardening to prevent future incidents, removing unnecessary software is not a typical step in support of IR activities.
11. A. SCADA (supervisory control and data acquisition) is a system architecture that combines data acquisition and control devices with communications methods and interfaces to oversee complex industrial and manufacturing processes, just like those used in utilities. A SIM (subscriber identity module) is the small card used to identify cell phones; HVAC stands for heating, ventilation, and air-conditioning; and AVAD was made up for this question.
12. D. A real-time operating system (RTOS) is an OS that is designed to handle data as it is fed to the operating system, rather than delaying handling it as other processes and programs are run. Real-time operating systems are used when processes or procedures are sensitive to delays that might occur if responses do not happen immediately. An MFP is a multifunction printer, a HIPS is a host intrusion prevention system, and an SoC is a system on a chip—which is hardware, which might run an RTOS, but the option does not mention what type of OS the SoC is running.
13. B. Embedded systems are available at many price points. Understanding constraints that limited resources create for embedded systems helps security professionals identify appropriate security controls and options.
14. A. Jim knows that once a BitLocker-enabled machine is booted, the drive is unlocked and could be accessed. He would be least worried if the machine were off and was stolen, or if the drive itself were stolen from the machine, since the data would not be accessible in either of those cases.
15. B. Olivia should install a host-based intrusion detection system (HIDS). An HIDS can detect and report on potential attacks but does not have the ability to stop them. A host-based intrusion prevention system (HIPS) can be configured to report only on attacks, but it does have the built-in ability to be set up to block them. Firewalls can block known ports, protocols, or applications, but they do not detect attacks—although advanced modern firewalls blur the line between firewalls and other defensive tools. Finally, a data loss prevention (DLP) tool focuses on preventing data exposures, not on stopping network attacks.
16. B. Group Policy deployed via Active Directory will allow Anita to set security settings across her domain managed systems. EDR and XDR are useful for detecting and responding to malware and malicious actors but not for deploying security configurations. SELinux is a Linux kernel-based security module that provides additional security capabilities and options on top of existing Linux distributions.
17. C. Chris knows that BIOS-based systems do not support either of these modes, and that trusted boot validates every component before loading it, whereas measured boot logs the boot process and sends it to a server that can validate it before permitting the system to connect to the network or perform other actions.
18. A. A degausser is a quick and effective way to erase a tape before it is reused. Wiping a tape by writing 1s, 0s, or a pattern of 1s and 0s to it will typically be a slow operation and is not a common method of destroying data on a tape. Incinerating the tape won't allow it to be reused!

**Chapter 12: Network Security**

1. C. SNMP traps can be configured to provide additional information, but typical SNMP traps provide information about issues such as links going down, authentication failures, and reboots.
2. C. A honeynet is a group of systems that intentionally exposes vulnerabilities so that defenders can observe attacker behaviors, techniques, and tools to help them design better defenses.
3. B. Telnet provides remote command-line access but is not secure. SSH is the most common alternative to telnet, and it operates on port 22.
4. D. DNS reputation services can provide Jill with an automated feed of malicious sites that she can include in her DNS filter. OSINT (open source intelligence) is gathered without scans but typically won't provide DNS block lists. STP (Spanning Tree Protocol) prevents loops in networks and is not relevant to DNS filtering, and an access control monitoring service will not be either.
5. B. Jump servers are used to provide secure, monitored access to a protected network. Users log in to the jump server, which then has access to the network. Proxies are used to filter or manage traffic and might be used in this scenario, but jump servers are the preferred answer for most organizations and uses. A VLAN (virtual LAN) is used to logically separate network segments. An air gap is a physical disconnection between networks or devices.
6. A. A next-generation firewall (NGFW) device is typically designed and built to be more capable at high speeds and throughput than a universal threat management device. Since UTM devices provide such a wide array of services that consume CPU and memory resources, this performance gap can also sometimes be due to the broad set of services that a UTM device provides. A WAF (web application firewall) is specialized in web traffic, and SD-FW was made up for this question.
7. A. DNSSEC validates both the origin of DNS information and ensures that DNS responses have not been modified, making it the best option to help prevent DNS poisoning attacks. SDNS was made up for this question. SASE is used to secure networks in complex multilocation environments, and SD-WAN allows for dynamic wide area networks defined by software, but neither provides this type of DNS security.
8. C. SD-WAN (software-defined wide area network) is commonly used to replace MPLS (Multiprotocol Label Switching) networks, which are typically higher cost than other connectivity options. IPSec and TLS-based VPNs are used to connect through untrusted networks, but they do not provide the functionality required. SASE uses SD-WAN and other technologies to ensure secure connectivity in complex network infrastructures with endpoints in many locations.
9. D. Transport Layer Security (TLS) is commonly used to wrap (protect) otherwise insecure protocols. In fact, many of the secure protocols simply add TLS to protect them. ISAKMP and IKE are both used for IPSec and can be used to wrap insecure protocols, but they aren't used alone. SSL is no longer used; TLS has almost entirely replaced it, although SSL is still often casually referred to as TLS.
10. D. While many protocols have a secure version, DHCP does not have a secure option, and protection must be handled by using detection and response mechanisms, rather than an encrypted protocol.
11. B. Policy enforcement points communicate with policy administrators to forward requests from subjects and to receive instructions from them about connections to allow or end. Policy administrators are components that establish or remove the communication path between subjects and resources, including creating session-specific authentication tokens or credentials as needed. Policy engines make policy decisions based on both rules and external systems. Policy gateways are not reference components for zero-trust designs.
12. C. End users may use secure POP (POPS), secure IMAP (IMAPS), and secure HTTP (HTTPS) to retrieve email. SPF, DKIM, and DMARC are used to identify and validate email servers, not to access email by end users.
13. A. Physical isolation like an air gap is used when the additional work to manually transfer files is an acceptable trade-off against the potential for a security event caused by potential network-based attackers. Firewall rules, an IPS, or the use of IPSec to protect traffic will not sufficiently address this issue if any services remain accessible on the system.
14. B. Active/active designs spread traffic among active nodes, helping ensure that a single node will not be overwhelmed. Active/passive designs are useful for disaster recovery and business continuity, but they do not directly address heavy load on a single node. There are many load-balancing schemes, but daisy chains and duck-duck-goose are not among them.
15. A. Agent-based, preadmission NAC will provide Isaac with the greatest amount of information about a machine and the most control about what connects to the network and what can impact other systems. Since systems will not be connected to the network, even to a quarantine or preadmission zone, until they have been verified, Isaac will have greater control.
16. D. SASE (Secure Access Service Edge) combines network security and device security by leveraging SD-WAN with security tools like Zero Trust, firewalls, and cloud access security brokers (CASBs). Both UTM and NGFW are advanced firewalls but do not provide this full functionality, and IPSec is a protocol used to provide encryption and authentication for network traffic.
17. B. Browser on-path attacks take advantage of malicious browser plug-ins or proxies to modify traffic at the browser level. They do not involve compromised routers or servers, and a modified hosts file is more likely to be involved in an on-path attack.
18. C. Understanding what services your organization offers to the outside world is an important step in describing the organization's attack surface. Fail open and fail closed describe what happens when devices or systems fail, not vulnerability and service availability information. OSINT is a passive process and scanning is not a passive activity.
19. A. DNSSEC does not encrypt data but does rely on digital signatures to ensure that DNS information has not been modified and that it is coming from a server that the domain owner trusts. DNSSEC does not protect confidentiality, which is a key thing to remember when discussing it as a security option. TLS, an IPSec VPN, or encryption via AES are all potential solutions to protect the confidentiality of network data.
20. C. Out-of-band management places the administrative interface of a switch, router, or other device on a separate network or requires direct connectivity to the device to access and manage it. This ensures that an attacker who has access to the network cannot make changes to the network devices. NAC and port security help protect the network itself, whereas trunking is used to combine multiple interfaces, VLANs, or ports together.

**Chapter 13: Wireless and Mobile Security**

1. B. The Center for Internet Security (CIS) provides hardening guidelines known as CIS benchmarks that Alyssa can use as a guide to secure her organization's iOS devices. OWASP does not provide these, and NIST provides general guidance, not OS- or device-specific configuration guides.
2. D. Using a containerization system can allow Fred's users to run corporate applications and to use corporate data in a secure environment that cannot be accessed by other applications outside of the container on the device. Containerization schemes for mobile devices typically use encryption and other isolation techniques to ensure that data and applications do not cross over. Biometrics and context-aware authentication are useful for ensuring that the right user is using a device but don't provide this separation. Full-device encryption helps reduce the risk of theft or loss of a device resulting in a data breach.
3. B. Geofencing will allow Michelle to determine what locations the device should work in. The device will then use geolocation to determine when it has moved and where it is. In this case, the correct answer is therefore geofencing—simply having geolocation capabilities would not provide the solution she needs. Context-aware authentication can help by preventing users from logging in when they aren't in the correct location, but a device that was logged in may not require reauthentication. Finally, UEM, much like mobile device management, can be used to enforce these policies, but the most correct answer is geofencing.
4. D. When access points conflict, enterprise wireless network management tools will typically decrease the power for both access points until the issue is resolved. Simply increasing power will cause more conflicts, changing the SSID would not serve typical enterprise models that use a single SSID to allow roaming, and disabling an access point may leave coverage gaps.
5. C. Nearfield communication (NFC) is not typically used for geolocation because of its extremely short range. Geolocation services may use GPS, Wi-Fi, and Bluetooth to identify areas, access points, Bluetooth beacons, and other items that help with location services.
6. A. Simultaneous Authentication of Equals (SAE) is used to establish a secure peering environment and to protect session traffic. Since the process requires additional cryptographic steps, it causes brute-force attacks to be much slower and thus less likely to succeed while also providing more security than WPA2's preshared key (PSK) mode. WPS is Wi-Fi Protected Setup, a quick setup capability; CCMP is the encryption mode used for WPA2 networks. WPA3 moves to 128-bit encryption for Personal mode and can support 192-bit encryption in Enterprise mode.
7. C. Isabelle should select PEAP, which doesn't require client certificates but does provide TLS support. EAP-TTLS provides similar functionality but requires additional software to be installed on some devices. EAP-FAST focuses on quick reauthentication, and EAP-TLS requires certificates to be deployed to the endpoint devices.
8. A. Storage segmentation is the concept of splitting storage between functions or usage to ensure that information that fits a specific context is not shared or used by applications or services outside of that context. Full-device encryption encrypts the entire device, geofencing is used to determine geographic areas where actions or events may be taken by software, and multifactor storage was made up for this question.
9. C. Sideloading is the process of copying files between two devices like a phone and a laptop, desktop, or storage device. Jake's team member has loaded an application without using the Android application store. Sideloading does not necessarily imply malware, rooting, or disabling an MDM, although an MDM may be configured to prevent sideloading.
10. B. SMS (Short Message Service) is used to send text messages, and MMS and RCS provide additional multimedia features. Neither provides phone calls or firmware updates.
11. C. Geotagging places a location stamp in documents and pictures that can include position, time, and date. This can be a serious privacy issue when pictures or other information are posted, and many individuals and organizations disable GPS tagging. Organizations may want to enforce GPS tagging for some work products, meaning that the ability to enable or disable it in an MDM tool is quite useful. Chain of custody is a forensic concept, the ability to support geofencing does not require GPS tagging, and context-aware authentication may need geolocation but not GPS tagging.
12. A. This is an ad-hoc network set up to allow devices to connect to the access point provided by the cellular modem. NFC is a short range, low bandwidth connection method used for payments and similar purposes. Point-to-point connections are used to bridge two networks together or for single connections, this is a multi-device network. RFID uses tags and readers.
13. B. Susan's best options are to use a combination of full-device encryption (FDE) and remote wipe. If a device is stolen and continues to be connected to the cellular network, or reconnects at any point, the remote wipe will occur. If it does not, or if attackers attempt to get data from the device and it is locked, the encryption will significantly decrease the likelihood of the data being accessed. Of course, cracking a passcode, PIN, or password remains a potential threat. NFC and Wi-Fi are wireless connection methods and have no influence on data breaches due to loss of a device. Geofencing may be useful for some specific organizations that want to take action if devices leave designated areas, but it is not a general solution. Containerization may shield data, but use of containers does not immediately imply encryption or other protection of the data but simply that the environments are separated.
14. C. Current mobile device implementations have focused heavily on facial recognition via services like Apple's Face ID and fingerprint recognition like Android's fingerprint scanning and Apple's Touch ID. Gait recognition is not a widely deployed biometric technology and would be difficult for most mobile device users to use. Voice recognition as a biometric authenticator has not been broadly deployed for mobile devices, whereas voice-activated services are in wide usage.
15. B. Jailbreaking will allow Alaina to obtain administrator access to the underlying phone operating system and to modify operating system settings and options as well as to install applications that are not available via the App Store. Deploying an MDM does not permit all of this, keymodding is not a term used in this context, and installing a third-party OS would allow access but would change the OS.
16. D. Jerome should deploy a captive portal that requires users to provide information before being moved to a network segment that allows Internet access. WPS capture mode was made up for this question, Kerberos is used for enterprise authentication, and WPA2 supports open, enterprise, or PSK modes but does not provide the capability Jerome needs by itself.
17. C. Amanda wants to create a heatmap, which shows the signal strength and coverage for each access point in a facility. Heatmaps can also be used to physically locate an access point by finding the approximate center of the signal. This can be useful to locate rogue access points and other unexpected or undesired wireless devices. PSK stands for preshared key, a channel overlay is not a commonly used term (although channel overlap is a concern for channels that share bandwidth), and SSID chart was made up for this question.
18. D. Managing applications won't help protect a misplaced phone from being accessed. PINs, device encryption, and remote wipe will all help keep her organization's data and devices secure.
19. B. Gurvinder's requirements fit the COPE (corporate-owned, personally enabled) mobile device deployment model. Choose your own device (CYOD) allows users to choose a device but then centrally manages it. BYOD allows users to use their own device, rather than have the company provide it, and MOTD means message of the day, and is not a mobile device deployment scheme.
20. C. Bluesnarfing is the theft of information from a Bluetooth enabled device. If Octavia left Bluetooth on and had not properly secured her device, then an attacker may have been able to access her contact list and download its contents. A bluejacking attack occurs when unwanted messages are sent to a device via Bluetooth. Evil twins are malicious access points configured to appear to be legitimate access points, and an evil maid attack is an in-person attack where an attacker takes advantage of physical access to hardware to acquire information or to insert malicious software on a device.

**Chapter 14: Monitoring and Incident Response**

1. D. The first item in the incident response cycle used by the Security+ exam is preparation.
2. C. Packet capture will allow Michael to see all the content of packets that are captured to analyze them. NetFlow simply shows source, destination, protocol, and traffic volume. Syslog and a SIEM don't capture packet content, and instead focus on logs and events.
3. C. A SIEM with correlation rules for geographic IP information as well as user IDs and authentication events will accomplish Susan's goals. An IPS may detect attacks, but it isn't well suited to detecting impossible travel. OS logs would need to be aggregated, and vulnerability scan data won't show this at all.
4. C. Application allow lists are used to ensure that only allowed applications are installable on systems. A deny list specifically identifies programs that aren't allowed. A SIEM doesn't provide application management capabilities, and sFlow is a flow tool like NetFlow.
5. D. The primary concern for analysts who deploy sFlow is often that it samples only data, meaning some accuracy and nuance can be lost in the collection of flow data. Sampling, as well as the implementation methods for sFlow, means that it scales well to handle complex and busy networks. Although vulnerabilities may exist in sFlow collectors, a buffer overflow is not a primary concern for them.
6. B. Mark has isolated the system by removing it from the network and ensuring that it cannot communicate with other systems. Containment would limit the impact of the incident and might leave the system connected but with restricted or protected access. Segmentation moves systems or groups of systems into zones that have similar purposes, data classification, or other restrictions on them.
7. C. Ben's organization is conducting a tabletop exercise. Tabletop exercises are conducted with more flexibility—team members are given a scenario and asked how they would respond and what they would do to accomplish tasks they believe would be relevant. Checklist exercises are not a specific type of exercise. A simulation exercise attempts to more fully re-create an actual incident to test responses. Fail-over exercises are conducted by actually failing a datacenter over to a hot location.
8. C. If the photo includes GPS data, it will be included in the photo's metadata. Madhuri can use a tool like ExifTool to review the metadata for useful information. None of the other options are places where data is stored for a PNG image as a normal practice.
9. A. Alyssa's has quarantined the machine, ensuring it cannot reach other systems or impact the rest of her organization. Segmentation would involve putting the system in protected network zone. Agentless tools are used to send data without a separate program or agent deployed to allow that. Deny lists are used to prevent specific programs or files from being used or deployed to systems.
10. C. Missing logs are often associated with an attacker attempting to hide evidence of their actions. Log rotation will typically remove the oldest log items and replace them with new log items rather than wiping a log, or will archive the old log file and create a new one. A newly deployed system typically has at least some logs from booting and running. Encrypting logs would leave a file in place even if it couldn't be read.
11. B. Ian's first step should be changing the sensitivity for his alerts. Adjusting the alerts to ignore safe or expected events can help reduce false positives. Correlation rules may then need to be adjusted if they are matching unrelated items. Dashboards are used to visualize data, not for alerting, and trend analysis is used to feed dashboards and reports.
12. C. Members of management or organizational leadership act as a primary conduit to senior leadership for most incident response teams. They also ensure that difficult or urgent decisions can be made without needing escalated authority. Communications and PR staff focus on internal and external communications but are typically not the direct conduit to leadership. Technical and information security experts do most of the incident response work itself.
13. D. This is an example of out-of-cycle logging, or logging that occurs at a different time than expected. This may be because an attacker is using the backup tool to acquire data. Unexpected logs are not an indicator found on the Security+ exam outline. There is no indication of resource consumption or inaccessibility in the question.
14. C. Red Hat Enterprise uses journalctl to view journal logs that contain application information. Jim should use journalctl to review the logs for the information he needs. The tool also provides functionality that replicates what head and tail can do for logs. Syslog-ng is a logging infrastructure, and though logs may be sent via syslog-ng, it is not mentioned here. logger is a logging utility used to make entries in the system log.
15. B. Benchmarks often include logging settings and configurations. SIEM is used to gather and analyze logs. Syslog is a standard for logging and sending logs. Agents are used to send logs for systems that don't have a logging capability.
16. B. The Windows Security log records logon events when logon auditing is enabled. The Application and System logs do not contain these events.
17. A. Five whys, event analysis, and diagramming are all common methods of performing root cause analysis. Root/branch review is not a typical process for this.
18. A. Containment activities focus on preventing further malicious actions or attacks. In this case, Hitesh might opt to prevent the malware from spreading but leave the system online due to a critical need or a desire to preserve memory and other artifacts for investigation. Isolation walls a system or systems off from the rest of the world, whereas segmentation is frequently used before incidents occur to create zones or segments of a network or system with different security levels and purposes.
19. D. The Analysis phase focuses on using various techniques to analyze events to identify potential incidents. Preparation focuses on building tools, processes, and procedures to respond to incidents. Eradication involves the removal of artifacts related to the incident, and containment limits the scope and impact of the incident.
20. C. Vulnerability scans are the best way to find new services that are offered by systems. In fact, many vulnerability scanners will flag new services when they appear, allowing administrators to quickly notice unexpected new services. Registry information is not regularly dumped or collected in most organizations. Firewall logs and flow logs could show information about the services being used by systems whose traffic passes through them, but this is a less useful and accurate way of identifying new services and would work only if those services were also being used.

**Chapter 15: Digital Forensics**

1. C. dd is a copying and conversion command for Linux and can be used to create a forensic image that can be validated using an MD5sum or SHA1 hash. The other commands are df for disk usage, cp for copying files, and ln to link files.
2. C. If there are known limitations or issues with the tools used, this should be included in the report. The type of system the tool was installed on may influence performance but should not influence the report or output. Training and certification may be listed as part of a team description but are not required as part of tool description. Finally, patch levels or installed versions are not critical unless there are known issues that would have been described as such.
3. A. If forensic evidence was not properly handled, it may not be admissible in court. Repeating forensic activities won't reverse mishandling, staff can't go back and re-create logs, and noting the issue will not resolve it.
4. B. Mike's best option is to identify the log information available from the provider and to request any additional information knowing that he may not receive more detail unless there is contractual language that specifies it. SaaS vendors typically won't allow installation of forensic tools, law enforcement does not perform forensic acquisition for third parties upon request, and auditors don't provide forensic data acquisition either.
5. C. Creating a snapshot will provide a complete copy of the system, including memory state that can then be analyzed for forensic purposes. Copying a running system from a program running within that system can be problematic, since the system itself will change while it is trying to copy itself. FTK Imager can copy drives and files, but it would not handle a running virtual machine.
6. B. Even though Wireshark is not a dedicated network forensic tool, since network traffic is ephemeral, capturing it with a packet sniffer like Wireshark is Melissa's best option. Forensic suites are useful for analyzing captured images, not capturing network traffic, and dd and WinHex are both useful for packet capture, but not for network traffic analysis.
7. D. Forensic information does not have to include a time stamp to be admissible, but time stamps can help build a case that shows when events occurred. Files without a time stamp may still show other information that is useful to the case or may have other artifacts associated with them that can provide context about the time and date.
8. D. Chain-of-custody documentation tracks evidence throughout its life cycle, with information about who has custody or control and when transfers happened, and continues until the evidence is removed from the legal process and disposed of. The other terms are not used for this practice.
9. B. The most common cause of an hour of difference between two systems in an environment is an incorrectly set time zone. Isaac should check the time zone settings, and then correct his findings based on the time zones set on the systems if necessary.
10. C. Jurisdiction is the legal authority over an area or individuals based on laws that create the jurisdiction. Nexus defines whether a relationship or connection exists, such as a local branch or business location. Non-repudiation ensures that evidence or materials can be connected to their originator. Admissibility determines whether evidence can be used in court.
11. A. Firmware can be challenging to access, but both memory forensic techniques and direct hardware interface access are viable means in some cases. Firmware is not typically stored on the disk and instead is stored in a BIOS or UEFI chip. Removing the chip from the system will leave it unable to run and thus this is not a preferred method. Also, many chips are not removable. Shutting down the device and booting it to the firmware does not provide a means of copying the firmware for most devices. Although the firmware is likely to allow updates, most do not allow downloads or copying.
12. C. Although it may be tempting to use a technical answer, interviewing the individual involved is the best starting point when a person performed actions that need to be reviewed. Charles can interview the staff member, and then move on to technical means to validate their responses. System and event logs may have some clues to what occurred, but normal systems do not maintain a keystroke log. In fact, the closest normal element is the command log used by both Windows and Linux to allow command-line input to be recalled as needed.
13. B. Once a copy is made, hashes for the original and target drive should be compared to ensure that the copy was successful. After that, the chain-of-custody document can be updated to note that a copy was made and will be tracked as it is analyzed while the original is preserved. Wiping either drive after a copy is not part of the process, although a target drive may be wiped after a case is complete.
14. B. Quick-formatting a drive removes the file indexes but leaves the file content on the drive. Recovery tools look for those files on the drive and piece them back together using metadata, headers, and other clues that help to recover the files.
15. B. Contracts commonly include right to audit, choice of jurisdiction, and data breach notification time frame clauses, but a right to forensically examine a vendor's systems or devices is rarely included. Naomi may want to ask about their incident response process and for examples of previous breach notification and incident documentation shared with customers instead.
16. D. Chain of custody tracks who has an item, how it is collected, where it is stored and how, how it is secured or protected, who collected it, and transfers, but it does not typically include how the items were transported because that is not relevant if the other data is provided.
17. C. It is important to ensure that data prepared for e-discovery only contains what it is supposed to, and that information that should not be shared is not included. Time stamps, hashing, chain of custody, and ensuring malicious files are not included are not part of the EDRM model. Validating that a legal hold is valid should happen before preservation, but validating that documented items from the hold are included if they exist should occur.
18. C. Removing information relevant to a legal hold is exactly what the hold is intended to prevent. Theresa's organization could be in serious legal trouble if they were to intentionally purge or change related information.
19. C. Backups are the least volatile of these options according to the order of volatility. Backups will be kept until they are aged out, which may be days, weeks, or even months in some cases. From most to least volatile, these are RAM, data on the hard drive, remote logs, and then backups.
20. A. Although both a checksum and a hash can be used to validate message integrity, a hash has fewer collisions than a checksum and will also provide a unique fingerprint for a file. Checksums are primarily used as a quick means of checking that that integrity is maintained, whereas hashes are used for many other purposes such as secure password validation without retaining the original password. A checksum would not be useful for proving a forensic image was identical, but it could be used to ensure that your work had not changed the contents of the drive.

**Chapter 16: Security Governance and Compliance**

1. B. The key phrase in this scenario is “one way.” This indicates that compliance with the document is not mandatory, so Joe must be authoring a guideline. Policies, standards, and procedures are all mandatory.
2. A. PCI DSS compensating controls must be “above and beyond” other PCI DSS requirements. This specifically bans the use of a control used to meet one requirement as a compensating control for another requirement.
3. C. The General Data Protection Regulation (GDPR) implements privacy requirements for handling the personal information of EU residents. The Health Insurance Portability and Accountability Act (HIPAA) includes security and privacy rules that affect health-care providers, health insurers, and health information clearinghouses. The Family Educational Rights and Privacy Act (FERPA) applies to educational institutions. The Payment Card Industry Data Security Standard (PCI DSS) applies to credit and debit card information.
4. B. The five security functions described in the NIST Cybersecurity Framework are identify, protect, detect, respond, and recover.
5. C. The International Organization for Standardization (ISO) publishes ISO 27701, covering privacy controls. ISO 27001 and 27002 cover cybersecurity, and ISO 31000 covers risk management.
6. D. Policies require approval from the highest level of management, usually the CEO. Other documents may often be approved by other managers, such as the CISO.
7. C. Master service agreements (MSAs) provide an umbrella contract for the work that a vendor does with an organization over an extended period of time. The MSA typically includes detailed security and privacy requirements. Each time the organization enters into a new project with the vendor, they may then create a statement of work (SOW) that contains project-specific details and references the MSA.
8. B. All of these organizations produce security standards and benchmarks. However, only the Center for Internet Security (CIS) is known for producing independent benchmarks covering a wide variety of software and hardware.
9. C. Many organizations use scheduled maintenance windows to coordinate changes to information systems. These windows are preplanned and announced times when all non-emergency changes will take place and often occur on evenings and weekends. A change management process ensures that personnel can perform a security impact analysis. Experts evaluate changes to identify any security impacts before personnel deploy the changes in a production environment. A backout plan allows personnel to undo the change and return the system to its previous state if necessary. Version control ensures that developers and users have access to the latest versions of software and that changes are carefully managed throughout the release process.
10. B. Security policies do not normally contain prescriptive technical guidance, such as a requirement to use a specific encryption algorithm. This type of detail would normally be found in a security standard.
11. C. Alice's exercise is designed to evaluate how well employees can identify phishing messages and, if they fail to do so, redirect them to a training program that is meant to help them get better at recognizing such messages.

The exercise is meant for educational purposes and not for penalizing employees. It is intended to help them improve their skills in recognizing phishing emails.

While rewarding employees for identifying phishing emails could be a component of a security awareness program, the exercise described is primarily educational and is focused on helping those who fail to recognize the phishing messages.

While data might be collected for analysis and understanding areas where improvement is needed, the intention is not to label departments as gullible.

1. B. An organization's acceptable use policy (AUP) should contain information on what constitutes allowable and unallowable use of company resources. This policy should contain information to help guide Tonya's next steps.
2. D. The Payment Card Industry Data Security Standard (PCI DSS) provides detailed rules about the storage, processing, and transmission of credit and debit card information. PCI DSS is not a law but rather a contractual obligation that applies to credit card merchants and service providers.
3. B. As an information security manager, Mike's primary role would be to establish an effective security training and awareness program, promote it within the organization, and ensure it is maintained effectively to foster a security-conscious culture among employees. This aligns with a proactive approach to reducing security incidents.

Mike should take an active role in security training and awareness, rather than delegating all responsibilities to another department. While HR may be involved, Mike's expertise is crucial in establishing effective programs.

Although security awareness posters and training sessions are two components of security awareness efforts, Mike's role should be much broader, encompassing the establishment, promotion, and maintenance of comprehensive training and awareness programs.

1. D. Mandatory vacations are designed to force individuals to take time away from the office to allow fraudulent activity to come to light in their absence. The other controls listed here (separation of duties, least privilege, and dual control) are all designed to prevent, rather than detect, fraud.
2. D. Guidelines are the only element of the security policy framework that is optional. Compliance with policies, standards, and procedures is mandatory.
3. A. Security training typically involves structured and formal programs where employees learn new security concepts and practices. In contrast, security awareness efforts are more informal and aim to keep security principles top-of-mind for employees through reminders, without requiring them to engage in formal learning.

The idea that security training involves giving rewards to employees and awareness efforts involve punishments is not accurate. Security training is meant to educate employees on security concepts and practices, not to serve as a platform for rewards. Similarly, awareness efforts are not punitive; they serve to remind and reinforce security principles among employees. The statement that there is no difference between security training and awareness efforts and that both terms can be used interchangeably is also incorrect. There is a distinct difference between the two in terms of their structure and purpose, as explained in the correct answer. Lastly, the notion that security training is only for security team members while security awareness is for all employees is not true. Security training is important for all employees, depending on their roles and responsibilities, to ensure they understand the security protocols and policies. Security awareness, on the other hand, is a continual reminder for all employees, including the security team, to stay vigilant and informed about security practices.

1. B. Standards describe specific security controls that must be in place for an organization. Allan would not include acceptable mechanisms in a high-level policy document, and this information is too general to be useful as a procedure. Guidelines are not mandatory, so they would not be applicable in this scenario.
2. D. The NIST Cybersecurity Framework is designed to help organizations describe their current cybersecurity posture, describe their target state for cybersecurity, identify and prioritize opportunities for improvement, assess progress, and communicate with stakeholders about risk. It does not create specific technology requirements.
3. C. Requests for an exception to a security policy would not normally include a proposed revision to the policy. Exceptions are documented variances from the policy because of specific technical and/or business requirements. They do not alter the original policy, which remains in force for systems not covered by the exception.

**Chapter 17: Risk Management and Privacy**

1. C. By applying the patch, Jen has removed the vulnerability from her server. This also has the effect of eliminating this particular risk. Jen cannot control the external threat of an attacker attempting to gain access to her server.
2. C. Installing a web application firewall reduces the probability that an attack will reach the web server. Vulnerabilities may still exist in the web application and the threat of an external attack is unchanged. The impact of a successful SQL injection attack is also unchanged by a web application firewall.
3. C. The asset at risk in this case is the customer database. Losing control of the database would result in a $500,000 fine, so the asset value (AV) is $500,000.
4. D. The attack would result in the total loss of customer data stored in the database, making the exposure factor (EF) 100 percent.
5. C. We compute the single loss expectancy (SLE) by multiplying the asset value (AV) ($500,000) and the exposure factor (EF) (100%) to get an SLE of $500,000.
6. A. Aziz's threat intelligence research determined that the threat has a 5 percent likelihood of occurrence each year. This is an ARO of 0.05.
7. B. We compute the annualized loss expectancy (ALE) by multiplying the SLE ($500,000) and the ARO (0.05) to get an ALE of $25,000.
8. C. Installing new controls or upgrading existing controls is an effort to reduce the probability or magnitude of a risk. This is an example of a risk mitigation activity.
9. B. Changing business processes or activities to eliminate a risk is an example of risk avoidance.
10. D. Insurance policies use a risk transference strategy by shifting some or all of the financial risk from the organization to an insurance company.
11. A. When an organization decides to take no further action to address remaining risk, they are choosing a strategy of risk acceptance.
12. A. Under the GDPR, the data protection officer (DPO) is an individual assigned direct responsibility for carrying out an organization's privacy program.
13. A. In this case, the physicians maintain the data ownership role. They have chosen to outsource data processing to Helen's organization, making that organization a data processor.
14. C. The Recovery Time Objective (RTO) is the amount of time that the organization can tolerate a system being down before it is repaired. That is the metric that Gene has identified in this scenario.
15. B. This is a tricky question, as it is possible that all of these categories of information may be found in patient records. However, they are most likely to contain protected health information (PHI). PHI could also be described as a subcategory of personally identifiable information (PII), but PHI is a better description. It is also possible that the records might contain payment card information (PCI) or personal financial information (PFI), but that is less likely than PHI.
16. C. Organizations should only use data for the purposes disclosed during the collection of that data. In this case, the organization collected data for technical support purposes and is now using it for marketing purposes. That violates the principle of purpose limitation.
17. C. Top Secret is the highest level of classification under the U.S. system and, therefore, requires the highest level of security control.
18. D. Quantitative risk analysis uses numeric data in the analysis, resulting in assessments that allow the very straightforward prioritization of risks. Qualitative risk analysis substitutes subjective judgments and categories for strict numerical analysis, allowing the assessment of risks that are difficult to quantify. A one-time risk assessment offers the organization a point-in-time view of its current risk state. Recurring risk assessments are performed at regular intervals, such as annually or quarterly.
19. B. Data controllers are the entities who determine the reasons for processing personal information and direct the methods of processing that data. This term is used primarily in European law, and it serves as a substitute for the term *data owner* to avoid a presumption that anyone who collects data has an ownership interest in that data.
20. D. The residual risk is the risk that remains after an organization implements controls designed to mitigate, avoid, and/or transfer the inherent risk.