Appendix B
Answers to Review Questions and Practice Exam

Chapter 1: Today's Cybersecurity Analyst

1. B. The three primary objectives of cybersecurity professionals are confidentiality, integrity, and availability.
2. B. In this scenario, Tommy identified a deficiency in the security of his web server that renders it vulnerable to attack. This is a security vulnerability. Tommy has not yet identified a specific risk because he has not identified a threat (such as a hacker) that might exploit this vulnerability.
3. C. The NIST risk assessment process says that organizations should identify threats before identifying vulnerabilities or determining the likelihood and impact of risks.
4. D. Widespread infrastructure failures, such as those affecting the power grid or telecommunications circuits, are considered man-made disasters and fall under the category of environmental threats.
5. A. Adversarial threat analysis requires examining the capability of the threat source, the intent of the threat source, and the likelihood that the threat will target the organization.
6. D. In an availability attack, the attacker disrupts access to information or a service by legitimate users. In this attack, the attacker disrupted access to the organization's website, violating the principle of availability.
7. D. Penetration tests are an example of an operational security control. Encryption software, network firewalls, and antivirus software are all examples of technical security controls.

8. A. Any action that an organization takes to reduce the likelihood or impact of a risk is an example of risk mitigation. In this case, Paul chose to implement a technical control—a network firewall—to mitigate the likelihood of a successful attack.
9. B. Network access control (NAC) solutions are able to verify the security status of devices before granting them access to the organization's network. Devices not meeting minimum security standards may be placed on a quarantine network until they are remediated.
10. D. The Remote Access Dial-In User Service (RADIUS) is an authentication protocol used for communications between authenticators and the authentication server during the 802.1x authentication process.
11. A. Any device that wishes to join an 802.1x network must be running an 802.1x supplicant that can communicate with the authenticator before joining the network.
12. D. The Secure HTTP (HTTPS) protocol uses TCP port 443 for communications between web browsers and the web server.
13. A. Next-generation firewalls (NGFWs) incorporate contextual information about users, applications, and business processes in their decision-making process.
14. B. Port 23, used by the Telnet protocol, is unencrypted and insecure. Connections should not be permitted to the jump box on unencrypted ports. The services running on ports 22 (SSH), 443 (HTTPS), and 3389 (RDP) all use encryption.
15. A. Administrators may use Group Policy Objects (GPOs) to control a wide variety of Windows settings and create different policies that apply to different classes of system.
16. A. During the planning phase of a penetration test, the testers should confirm the timing, scope, and authorization for the test in writing.
17. A. After the completion of the discovery phase, penetration testers first seek to gain access to a system on the targeted network and then may use that system as the launching point for additional attacks.
18. A. The red team plays the role of the attacker and uses reconnaissance and exploitation tools to attempt to gain access to the protected network.

19. D. Sandboxing is an approach used to detect malicious software based on its behavior rather than its signatures. Sandboxing systems watch systems and the network for unknown pieces of code and, when they detect an application that has not been seen before, immediately isolate that code in a special environment known as a sandbox where it does not have access to any other systems or applications.
20. B. Web application firewalls (WAFs) are specialized firewalls designed to protect against web application attacks, such as SQL injection and cross-site scripting.

Chapter 2: Using Threat Intelligence

1. B. While higher levels of detail can be useful, it isn'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. STIX is an XML-based language, allowing it to be easily extended and modified while also using standard XML-based editors, readers, and other tools.
3. D. Threat intelligence dissemination or sharing typically follows threat data analysis. The goal is to get the threat data into the hands of the organizations and individuals who need it.
4. A. Understanding what your organization needs is important for the requirements gathering phase of the intelligence cycle. Reviewing recent breaches and compromises can help to define what threats you are currently facing. Current vulnerability scans can identify where you may be vulnerable but are less useful for threat identification. Data handling standards do not provide threat information, and intelligence feed reviews list new threats, but those are useful only if you know what type of threats you're likely to face so that you can determine which ones you should target.
5. D. The U.S. government created the information sharing and analysis centers (ISACs). ISACs help infrastructure owners and operators share

threat information, as well as provide tools and assistance to their members.

6. A. Nation-state actors are government sponsored and typically have the greatest access to resources, including tools, money, and talent.
7. A. Hacktivists execute attacks for political reasons, including those against governments and businesses. The key element in this question is the political reasons behind the attack.
8. B. Attack vectors, or the means by which an attacker can gain access to their target, can include things like USB key drops. You may be tempted to answer this question with adversary capability, but remember the definition: the resources, intent, or ability of the likely threat actor. Capability here doesn't mean what they can do, but their ability to do so. The attack surface might include the organization's parking lot in this example, but this is not an example of an attack surface, and there was no probability assessment included in this problem.
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 context of the actions performed such as after-hours logins, misuse of credentials, logins from abnormal locations or in abnormal patterns, other behavioral indicators are often used.
10. D. TAXII, the Trusted Automated Exchange of Indicator Information protocol, is specifically designed to communicate cyber threat information at the application layer. OpenIOC is a compromise indicator framework, and STIX is a threat description language.
11. C. The installation phase of the Cyber Kill Chain focuses on providing persistent backdoor access for attackers. Delivery occurs when the tool is put into action either directly or indirectly, whereas exploitation occurs when a vulnerability is exploited. Command and control (C2) uses two-way communications to provide continued remote control.
12. C. The Kill Chain includes actions outside the defended network which many defenders cannot take action on, resulting in one of the common criticisms of the model. Other criticisms include the focus on a tradi-

tional perimeter and on antimalware-based techniques, as well as a lack of focus on insider threats.

13. B. Patching against zero-day attacks won't stop a command and control capability, although it might stop the initial exploit that results in the installation of C2 tools. Network hardening, deploying additional capabilities to detect C2 traffic, and staying ahead of the latest in C2 methods and technology so that detections and hardening match them are all common techniques.
14. C. The confidence level of your threat information is how certain you are of the information. A high confidence threat assessment will typically be confirmed either by multiple independent and reliable sources or via direct verification.
15. A. ISACs were introduced in 1998 as part of a presidential directive, and they focus on threat information sharing and analysis for critical infrastructure owners.
16. D. STRIDE, PASTA, and LINDDUN are all examples of threat classification tools. LINDDUN focuses on threats to privacy, STRIDE is a Microsoft tool, and PASTA is an attacker-centric threat modeling tool.
17. A. The threat indicators built into OpenIOC are based on Mandiant's indicator list. You can extend and include additional indicators of compromise beyond the 500 built-in definitions.
18. B. Advanced persistent threats (APTs) are most commonly associated with nation-state actors. The complexity of their operations and the advanced tools that they bring typically require significant resources to leverage fully.
19. B. The ATT&CK framework specifically defines threat actor tactics in standardized ways. The Diamond Model is useful for guiding thought processes about threats, and the Cyber Kill Chain is most useful for assessing threats based on a set of defined stages. The Universal Threat Model was made up for this question!
20. C. Forensic data is very helpful when defining indicators of compromise (IOCs). Behavioral threat assessments can also be partially defined by forensic data, but the key here is where the data is most frequently used.

Chapter 3: Reconnaissance and Intelligence Gathering

1. D. DNS zone transfers provide a method to replicate DNS information between DNS servers, but they are also a tempting target for attackers due to the amount of information that they contain. A properly secured DNS server will only allow zone transfers to specific, permitted peer DNS servers. DNSSEC is a suite of DNS security specifications, AXR is a made-up term (AXFR is the zone transfer command), and DNS registration is how you register a domain name.
2. C. Nmap's operating system identification flag is –o and it enables OS detection. –A also enables OS identification and other features. –osscan with modifiers like –limit and –guess set specific OS identification features. –os and –id are not nmap flags.
3. B. Traceroute (or tracert on Windows systems) is a command-line tool that uses ICMP to trace the route that a packet takes to a host. Whois and nslookup are domain tools, and routeview is not a command-line tool.
4. B. Exif (Exchangeable Image Format) data often includes location and camera data, allowing the images to be mapped and identified to a specific device or type of camera.
5. A. Log level 0 is used for emergencies in Cisco's logging level scheme. Log level 7 is for debugging information and is at the bottom of the scale.
6. C. UDP connections are not shown by netstat because UDP is a connectionless protocol. Active TCP connections, executables that are associated with them, and route table information are all available via netstat.
7. D. Although it is possible that a system named “db1” with a hostname “sqldb1” is not a Microsoft SQL Server, the most likely answer is that it is a Microsoft SQL Server.
8. B. Microsoft Windows security logs can contain information about files being opened, created, or deleted if configured to do so. Configuration and httpd logs are not a type of Windows logs, and sys-

tem logs contain information about events logged by Windows components.

9. D. The Internet Assigned Numbers Authority manages the global IP address space. ARIN is the American Registry for Internet Numbers, WorldNIC is not an IP authority, and NASA tackles problems in outer space, not global IP space.
10. C. Metadata scrubbing removes hidden information about a file such as the creator, creation time, system used to create the file, and a host of other information. The other answers are made up.
11. C. Heuristic analysis focuses on behaviors, allowing a tool using it to identify malware behaviors instead of looking for a specific package. Trend analysis is typically used to identify large-scale changes from the norm, and it is more likely to be useful for a network than for a single PC. Regression analysis is used in statistical modeling.
12. B. Registering manually won't prevent DNS harvesting, but privacy services are often used to prevent personal or corporate information from being visible via domain registrars. CAPTCHAs, rate limiting, and blacklisting systems or networks that are gathering data are all common anti-DNS harvesting techniques.
13. D. The axfr flag indicates a zone transfer in both the dig and host utilities.
14. C. A packet capture can't provide plausible deniability, as it provides evidence of action. Packet capture is often used to document work, including the time that a given scan or process occurred, and it can also be used to provide additional data for further analysis.
15. D. Operating system detection often uses TCP options support, IP ID sampling, and window size checks, as well as other indicators that create unique fingerprints for various operating systems. Service identification often leverages banners since TCP capabilities are not unique to a given service. Fuzzing is a code testing method, and application scanning is usually related to web application security.
16. B. Netflow is a Cisco network protocol that collects IP traffic information that allows analysis of traffic flow and volume. Netstat provides information about local connections, which applications have made them, and other useful local system information. Libpcap is the Linux

packet capture library and would not be used alone. Pflow is a made-up term.

17. B. Zone transfers are intended to allow DNS database replication, but an improperly secured DNS server can also allow third parties to request a zone transfer, exposing all of their DNS information. Traceroute is used to determine the path and latency to a remote host, whereas dig is a useful DNS query tool. DNS sync is a made-up technical term.
18. A. The Internet Archive maintains copies of sites from across the Internet, and it can be used to review the historical content of a site. WikiLeaks distributes leaked information, whereas the Internet Rewinder and TimeTurner are both made-up names.
19. B. Social media can be a treasure trove of personal information. Company websites and forums are usually limited in the information they provide, and Creepy is a geolocation tool that gathers data from social media and geotagging.
20. C. Whois provides information that can include the organization's physical address, registrar, contact information, and other details. Nslookup will provide IP address or hostname information, whereas host provides IPv4 and IPv6 addresses as well as email service information. Traceroute attempts to identify the path to a remote host as well as the systems along the route.

Chapter 4: Designing a Vulnerability Management Program

1. C. The Federal Information Security Management Act (FISMA) requires that federal agencies implement vulnerability management programs for federal information systems.
2. D. The Federal Information Security Management Act (FISMA) requires vulnerability management programs for all federal information systems, regardless of their assigned impact rating.
3. A. An asset inventory supplements automated tools with other information to detect systems present on a network. The asset inventory

provides critical information for vulnerability scans.

4. D. PCI DSS requires that organizations conduct vulnerability scans on at least a quarterly basis, although many organizations choose to conduct scans on a much more frequent basis.
5. B. Qualys, Nessus, and OpenVAS are all examples of vulnerability scanning tools. Snort is an intrusion detection system.
6. A. PCI DSS requires that organizations conduct vulnerability scans quarterly, which would have Bethany's next regularly scheduled scan scheduled for June. However, the standard also requires scanning after any significant change in the payment card environment. This would include an upgrade to the point-of-sale system, so Bethany must complete a new compliance scan immediately.
7. 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.
8. C. Common Platform Enumeration (CPE) is an SCAP component that provides standardized nomenclature for product names and versions.
9. D. Internal scans completed for PCI DSS compliance purposes may be conducted by any qualified individual.
10. C. The Federal Information Security Management Act (FISMA) requires that government agencies conduct vulnerability scans. HIPAA, which governs hospitals and doctors' offices, does not include a vulnerability scanning requirement, nor does GLBA, which covers financial institutions. Banks may be required to conduct scans under PCI DSS, but this is a contractual obligation and not a statutory requirement.
11. C. Control enhancement number 4 requires that an organization determine what information about the system is discoverable by adversaries. This enhancement only applies to FISMA high systems.
12. B. The organization's risk appetite is its willingness to tolerate risk within the environment. If an organization is extremely risk averse, it may choose to conduct scans more frequently to minimize the amount of time between when a vulnerability comes into existence and when it is detected by a scan.
13. D. Scan schedules are most often determined by the organization's risk appetite, regulatory requirements, technical constraints, business con-

straints, and licensing limitations. Most scans are automated and do not require staff availability.

14. B. If Barry is able to limit the scope of his PCI DSS compliance efforts to the isolated network, then that is the only network that must be scanned for PCI DSS compliance purposes.
15. 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.
16. C. Although reporting and communication are an important part of vulnerability management, they are not included in the life cycle. The three life-cycle phases are detection, remediation, and testing.
17. A. Continuous monitoring incorporates data from agent-based approaches to vulnerability detection and reports security-related configuration changes to the vulnerability management platform as soon as they occur, providing the ability to analyze those changes for potential vulnerabilities.
18. B. Systems have a moderate impact from a confidentiality perspective if the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
19. A. The Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security vulnerabilities. Jessica could use this scoring system to prioritize issues raised by different source systems.
20. B. While any qualified individual may conduct internal compliance scans, PCI DSS requires the use of a scanning vendor approved by the PCI SSC for external compliance scans.

Chapter 5: Analyzing Vulnerability Scans

1. B. Although the network can support any of these protocols, internal IP disclosure vulnerabilities occur when a network uses Network Address Translation (NAT) to map public and private IP addresses but

a server inadvertently discloses its private IP address to remote systems.

2. C. The privileges required (PR) metric indicates the type of account access the attacker must have.
3. C. An attack complexity of "low" indicates that exploiting the vulnerability does not require any specialized conditions.
4. D. A value of High (H) for an impact metric indicates the potential for complete loss of confidentiality, integrity, and/or availability.
5. D. Version 3.1 of CVSS is currently available but is not as widely used as the more common CVSS version 2.0.
6. B. The CVSS exploitability score is computed using the attack vector, attack complexity, privileges required, and user interaction metrics.
7. B. Vulnerabilities with CVSS base scores between 4.0 and 6.9 fit into the medium risk category.
8. A. A false positive error occurs when the vulnerability scanner reports a vulnerability that does not actually exist.
9. B. It is unlikely that a database table would contain information relevant to assessing a vulnerability scan report. Logs, SIEM reports, and configuration management systems are much more likely to contain relevant information.
10. A. Microsoft discontinued support for Windows Server 2003, and it is likely that the operating system contains unpatchable vulnerabilities.
11. 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.
12. B. In October 2016, security researchers announced the discovery of a Linux kernel vulnerability dubbed Dirty COW. This vulnerability, present in the Linux kernel for nine years, was extremely easy to exploit and provided successful attackers with administrative control of affected systems.
13. D. Telnet is an insecure protocol that does not make use of encryption. The other protocols mentioned are all considered secure.

14. D. TLS 1.1 is a secure transport protocol that supports web traffic. The other protocols listed all have flaws that render them insecure and unsuitable for use.
15. B. Digital certificates are intended to provide public encryption keys, and this would not cause an error. The other circumstances are all causes for concern and would trigger an alert during a vulnerability scan.
16. D. In a virtualized datacenter, the virtual host hardware runs a special operating system known as a *hypervisor* that mediates access to the underlying hardware resources.
17. A. 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 on the resources assigned to a different virtual machine.
18. B. Intrusion detection systems (IDSs) are a security control used to detect network or host attacks. The Internet of Things (IoT), supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICSs) are all associated with connecting physical world objects to a network.
19. D. In a cross-site scripting (XSS) attack, an attacker embeds scripting commands on a website that will later be executed by an unsuspecting visitor accessing the site. The idea is to trick a user visiting a trusted site into executing malicious code placed there by an untrusted third party.
20. A. In a SQL injection attack, the attacker seeks to use a web application to gain access to an underlying database. Semicolons and apostrophes are characteristic of these attacks.

Chapter 6: Cloud Security

1. C. One of the key characteristics of cloud computing is that customers can access resources on-demand with minimal service provider inter-

action. 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.

2. A. Under the shared responsibility model, the customer only bears responsibility for operating system security in IaaS environments. In all other environments, the service provider is responsible for securing the operating system.
3. B. Helen is using IaaS services to create her payroll product. She is then offering that payroll service to her customers as an SaaS solution.
4. 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.
5. B. ScoutSuite is the only cloud assessment tool listed here that performs security scans of Azure environments. Inspector and Prowler are AWS-specific tools. Pacu is an exploitation framework used in penetration testing.
6. C. This is an example of function as a service (FaaS) computing, a subset of platform as a service (PaaS). Although both terms may be used to describe the service Kevin uses, the best answer is FaaS, because it is more specific.
7. D. In the shared responsibility model, the customer always retains either full or partial responsibility for data security. Responsibility for hardware and physical datacenters is the cloud provider's responsibility under all models. Responsibility for applications is the customer's responsibility under IaaS, the provider's responsibility under SaaS, and a shared responsibility under PaaS.
8. B. AWS Lambda, Google Cloud Functions, and Microsoft Azure Functions are all examples of function as a service (FaaS) computing. AWS DeepLens is an AI-enabled camera.
9. 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.

10. 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.
11. C. DevOps approaches to software development and technology operations increase the frequency of releases by automating software testing and release processes. The other options are characteristic of legacy approaches to technology.
12. C. Infrastructure as code 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.
13. D. All of these issues are security vulnerabilities that should be addressed. Cloud assessment tools would be able to identify most of these issues, but they would have no way of knowing that two or more developers are sharing an API key.
14. 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.
15. C. Community cloud deployments may offer IaaS, PaaS, and/or SaaS solutions. Their defining characteristic is that access is limited to members of a specific community.
16. D. Cloud service providers bear sole responsibility for datacenter security in all cloud service models.
17. C. Inline CASB solutions require either network reconfiguration or the use of a software agent. They intercept requests from users to cloud providers and, by doing so, are able to both monitor activity and enforce policy.
18. B. API keys are used to identify and authenticate the user, system, or application that is connecting to an API.

19. D. Pacu is an AWS-specific exploitation framework. It is particularly well suited to identifying the permissions available to an account during a penetration test. ScoutSuite, Inspector, and Prowler are all assessment tools that would not directly provide the information that Gina seeks.
20. 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.

Chapter 7: Infrastructure Security and Controls

1. D. Jump boxes are used to access and manage devices that are in another security zone from where the user is. This means they have connectivity into both zones, either via a VPN or similar technology. Option A may be tempting, but jump boxes aren't only used for DMZs. Remember this when you're studying—often questions will have a likely looking answer that isn't fully correct.
2. C. Ben has set up a honeypot, a system intended to be attractive to attackers, allowing defenders to observe their behavior while gathering information and potentially capturing copies of their tools. Sinkholes are systems or devices that are used as a destination for redirected traffic. Often, this is used defensively to redirect traffic via DNS. Blackholes and beehives are not common terms.
3. A. Polymorphic techniques change malware each time it infects a system, making simple hashing unable to be used to check if the malware matches. More advanced techniques include behavior monitoring–based techniques as well as other more in-depth analytical techniques that identify components of the malware package.
4. B. Ric's best option is to implement backup Internet connectivity using a different make and model of router. This reduces the chance of the same exploit being able to take down both types of device while re-

moving the single point of failure for connectivity. Adding a second identical router in either active/active or active/passive mode does not work around the flaw since an attacker could immediately repeat the attack to take down the matching router. A firewall might help, but in many cases attacks against routers take place on a channel that is required for the router to perform its function.

5. C. Whitelisting technologies can be used to only allow programs that have been preapproved to run on systems that use it. Blacklisting prevents specific programs from running. An antivirus uses a number of techniques to identify malicious software and might even include blacklisting and whitelisting capabilities, but we cannot assume that is the case. VDI provides virtualized desktops and can be useful for controlling systems but does not specifically provide this capability.
6. B. A multitier firewall is least likely to be an effective security control when Susan's organization deals with compromised credentials. Multifactor authentication would require the attacker to have the second factor in addition to the password, an awareness program may help Susan's employees avoid future scams, and a SIEM monitoring for logins that are out of the ordinary may spot the attacker logging in remotely or otherwise abusing the credentials they obtained.
7. D. Retirement is the last step at the end of the life cycle for a standard or process. Of course, this means that if the process is retired, a final update to it is not needed! The standards for other, currently maintained operating systems should undergo regular scheduled review, and staff who support them may participate in a continuous improvement process to keep the standards up to date.
8. A. Example Corporation is using network segmentation to split their network up into security zones based on their functional requirements. They may use multiple-interface firewalls for this, and they may try to avoid single points of failure, but the question does not provide enough information to know if that is the case. Finally, zoned routing is a made-up term—zone routing is an actual technical term, but it is used for wireless networks.
9. B. Firewalls are commonly used to create network protection zones, to protect network borders, and at the host level to help armor the host

against attacks. Encryption at rest is most frequently used at the host layer, whereas DMZs are typically used at the edge of a network for publicly accessible services. Antivirus is sometimes used at each layer but is most commonly found at the host layer.

10. C. Data loss prevention (DLP) tools attempt to identify sensitive or controlled data and to prevent it from being removed from systems or the local network. In this case, Jason's answer should be to use a DLP and to tag sensitive data to help ensure that another sensitive database is not stolen. He should also make sure that management is aware that a DLP cannot always detect all data that might leave, and that encrypted or otherwise obscured data may still be at risk.
11. A. This diagram shows two potential single points of failure, but only one that meets Michelle's goals: the single connection to the Internet from the ISP is an immediate concern at Point A. Point D shows single connections to each edge switch, which would result in the devices connected to that switch failing, but that would not result in the impact to the core network that Michelle is concerned about. Points B and C both have fully redundant network devices with heartbeat connections.
12. C. Sending logs to a remote log server or bastion host is an appropriate compensating control. This ensures that copies of the logs exist in a secure location, allowing them to be reviewed if a similar compromise occurred. Full-disk encryption leaves files decrypted while in use and would not secure the log files from a compromise, whereas log rotation simply means that logs get changed out when they hit a specific size or timeframe. TLS encryption for data (including logs) in transit can keep it private and prevent modification but wouldn't protect the logs from being deleted.
13. B. While each of the items listed can help as part of a comprehensive security architecture, using centralized patch management software will typically have the largest impact in an organization's handling of vulnerabilities related to software updates. Vulnerability scanning can help detect issues, and an IPS with the appropriate detections enabled may help prevent exploits, but both are less important than patching

itself. Similarly, standards for patching help guide what is done but don't ensure that the patching occurs.

14. B. Since Ben must assume that data that leaves may be exposed, his best option is to enforce encryption of files that leave the organization. Mandatory data tagging and DLP monitoring can help catch data that is accidentally sent, and network segmentation can help reduce the number of points he has to monitor, but encryption is the only control that can have a significant impact on data that does leave.
15. B. Trend analysis using historical data will show James what his network traffic's behavior has been. James may notice an increase since a new storage server with cloud replication was put in, or he may notice that a DMZ host has steadily been increasing its outbound traffic. Automated reporting might send an alarm if it has appropriate thresholds set, and log aggregation is the foundation of how a SIEM gathers information, but neither will individually give James the view he needs. BGP is a routing protocol, and graphing it won't give James the right information either.
16. C. File integrity checking tools like Tripwire can notify an administrator when changes are made to a file or directory. Angela can implement file integrity monitoring for her critical system files, thus ensuring she is warned if they change without her knowledge. Antimalware tools only detect behaviors like those of malware and may not detect manual changes or behaviors that don't match the profile they expect. Configuration management tools can control configuration files but may not note changes that are made, and logging utilities often don't track changes to files.
17. A. A web application firewall (WAF) can provide protection against unknown threats and zero-day exploits by restricting attacks based on behavior or by implementing custom protection based on known exploit behavior. A patch from the vendor is often not immediately available, an IDS cannot stop an attack—at best it will report the attack—and least privilege for accounts may limit the impact of an attack but won't stop it.
18. A. Mike reduced the organization's attack surface. This occurs when the number of potential targets is reduced. Since the question de-

scribes only one security activity, we don't know that defense-in-depth has been implemented. The firewall may be a corrective control, but the question does not specify whether it's there as part of a response or to deal with a specific problem, and firewalls are technical controls rather than administrative controls.

19. A. Port security is a switch layer 2 security option that will allow only specific MAC addresses to access the port.
20. C. Tony is using a sinkholing technique by causing traffic that would normally go to a malicious site to go to another host. One common option is to send traffic like this to an internally controlled site that lets users know they would have gone somewhere dangerous.

Chapter 8: Identity and Access Management Security

1. B. While it may seem like Gabby has implemented three different factors, both a PIN and a passphrase are knowledge-based factors and cannot be considered distinct factors. She has implemented two distinct factors with her design. If she wanted to add a third factor, she could replace either the password or the PIN with a fingerprint scan or other biometric factor.
2. B. An individual's job title is an attribute, which means that attribute-based access control is the appropriate answer. Titles may be used to help identify a role, but they do not necessarily match roles directly, meaning that role-based access control is not the right choice. Discretionary access control empowers users to make decisions about rights, and mandatory access control enforces access control at the system level.
3. B. The nightmare scenario of having a compromised Kerberos server that allows attackers to issue their own ticket-granting tickets (TGTs), known as golden tickets, would result in attackers being able to create new tickets, perform account changes, and even to create new accounts and services. A KDC is a Kerberos key distribution center; MGT and master tickets were both made up for this question.

4. B. The NT LAN Manager (NTLM) security protocols are associated with Active Directory. SAML, OAuth, and RADIUS do not use NTLM.
5. D. Privilege creep occurs as staff members change roles but their rights and permissions are not updated to match their new responsibilities. This violates the concept of least privilege. Rights mismanagement and permission misalignment are both terms made up for this question.
6. A. OAuth redirect exploits are a form of impersonation attack, allowing attackers to pretend to be a legitimate user. Session hijacking would take advantage of existing sessions, whereas man-in-the-middle (MitM) attacks take advantage of being in the path of communications. Protocol analysis is a networking term used when reviewing packet contents.
7. C. Breaches of passwords stored in easily recoverable or reversible formats paired with user IDs or other identifying information create significant threats if users reuse passwords. Attackers can easily test the passwords they recover against other sites and services. Poor password reset questions are a threat even without a breach, and unencrypted password storage is an issue during breaches, but this type of breach is enabled by poor storage, rather than a result of the breach. Use of federated credentials are not a critical concern in cases like this.
8. B. Context-based authentication allows authentication decisions to be made based on information about the user, the system they are using, or other data like their geographic location, behavior, or even the time of day. Token-based authentication uses a security token to generate a onetime password or value, and NAC (network access control) is a means of validating systems and users that connect to a network. System-data contextual is a made-up answer for this question.
9. C. Common attacks against Kerberos include attacks aimed at administrative accounts, particularly those that attempt to create a ticket-granting ticket (TGT). Ticket reuse attacks are also common. Open redirect-based attacks are associated with OAuth rather than Kerberos.
10. B. LDAP is sometimes used for single sign-on (SSO) but is not a shared authentication technology. OpenID Connect, OAuth, and Facebook Connect are all examples of shared authentication technologies.

11. B. LDAP access control lists (ACLs) can limit which accounts or users can access objects in the directory. LDAP replication may help with load issues or denial-of-service attacks, TLS helps to protect data in transit, but MD5 storage for secrets like passwords is a bad idea!
12. D. TACACS+ should be run on an isolated management network to protect it from attackers. It does not provide built-in encryption, TACACS++ does not exist, and while enabling auditing features is a good idea, it won't stop attacks from occurring.
13. A. Jason's exploit is a form of privilege escalation, which uses a flaw to gain elevated privileges. Local users have a far greater ability to attempt these attacks in most organizations, since flaws that are only exploitable locally often get less attention from administrators than those that can be exploited remotely. A zero-day attack would use previously unknown flaws to exploit a system, rootkits are aimed at acquiring and maintaining long term access to systems, and session hijacking focuses on taking over existing sessions.
14. C. Chris has identified a problem with the maintenance and modification processes his organization uses. He should review how employee accounts are reviewed and how changes are requested when employees change positions in the organization.
15. B. CAPTCHAs, login throttling, and locking out accounts after a set number of failed logins are all useful techniques to stop or delay brute-force password guessing attacks. Some sites also use unique URLs, or limit the IP ranges that systems can authenticate from. Returning an HTTP error actually works in the attacker's favor, as they can key off of that error to try their next login attempt!
16. C. Identity providers (IDPs) make assertions about identities to relying parties and service providers in a federation. CDUs and APs are not terms used in federated identity designs.
17. C. NIST SP 800 63-3 recommends that SMS be deprecated due to issues with VoIP, including password reuse and the ability to redirect SMS sent via VoIP calls. In addition, SMS itself is relatively insecure, allowing attackers with the right equipment to potentially intercept it. The good news is that SMS can send unique tokens, they're just text!

18. C. Ben successfully conducted a session hijacking attack by copying session information and using the existing session. If he had impersonated a legitimate user, it would have been an impersonation attack, whereas an MitM attack would require being in the flow of traffic between two systems or services. Privilege escalation attacks focus on acquiring higher levels of privilege.
19. D. Gabby is attempting a privilege escalation attack. After acquiring the web server's privileges, she is now attempting to gain root (administrative) privileges.
20. B. Michelle's security token is an example of a possession factor, or “something you have.” A password or PIN would be a knowledge factor or “something you know,” and a fingerprint or retina scan would be a biometric, or inherence, factor.

Chapter 9: Software and Hardware Development Security

1. B. A Trusted Platform Module (TPM) stores encryption keys to be used for hardware authentication. Hardware security models (HSMs) are used to create, manage, and store encryption keys and to offload cryptographic processing. SED stands for self-encrypting drive, and a trusted foundry is a trusted validated secure microelectronics supplier or manufacturer.
2. D. During the rework stage of Fagan inspection, issues may be identified that require the process to return to the planning stage and then proceed back through the remaining stages to re-review the code.
3. 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.
4. B. Sam is conducting a regression test, which verifies that changes have not introduced new issues to his application. Code review focuses on the application code, whereas stress testing verifies that the application will perform under load or other stress conditions. Whiffing isn't a term used in this type of review.

5. C. Tiffany is stress testing the application. Stress testing intentionally goes beyond the application's normal limits to see how it responds to extreme loads or other abnormal conditions beyond its normal capacity. Unit testing tests individual components of an application, and regression testing is done to ensure that new versions don't introduce old bugs. Fagan testing is a formal method of code inspection.
6. 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.
7. D. A source control management tool like Subversion or Git can help prevent old code from being added to current versions of an application. Developer practices still matter, but knowing what version of the code you are checking in and out helps! Stress testing would help determine whether the application can handle load, a WAF or web application firewall can protect against attacks, but neither would resolve this issue. Pair programing might detect the problem, but the question specifically asks for a tool, not a process.
8. 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.
9. C. User acceptance testing (UAT) is the process of testing to ensure that the users of the software are satisfied with its functionality. Stress testing verifies that the application will perform when under high load or other stress, and unit testing validates individual components of the application. CNA is not a term associated with application development.
10. A. Bus encryption protects data in transit between the processor and other devices. An HSM is used to create, store, and manage crypto-

graphic keys as well as to offload cryptographic processing, and a TPM chip is used to store cryptographic keys. LAMP encryption is made up for this question.

11. D. TLS satisfies the “protect data” best practice by ensuring that network traffic is secure. Parameterizing queries uses prebuilt SQL, while encoding data removes control characters that could be used for cross-site scripting attacks and other exploits. Validating all inputs requires treating all user input as untrusted.
12. B. Pass-around reviews normally rely on email to move code between developers. In Kristen's case, a pass-around review will exactly meet her needs. Pair programming and over-the-shoulder review both require developers to work together, whereas tool-assisted reviews require implementation of a tool to specifically support the review.
13. D. `strcpy` does not include size information for the data it accepts, making it a popular target for buffer overflow attacks.
14. A. RESTful designs are the most common and popular for modern web services because of their flexibility. SOAP remains in use, but is not broadly used for public APIs. SAML is a security assertion markup language and would be useful for making security assertions, not for building a general use SOA. RAD is an application development model.
15. 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. Although this could be caused by a default configuration issue, there is nothing in the question to point to that problem.
16. D. Load testing is used to validate the performance of an application under heavy loads like high numbers of concurrent user sessions. Fuzzing, fault injection, and mutation testing are all types of code review and testing.
17. A. Interception proxies are designed to allow testers to intercept, view, and modify traffic sent from web browsers and are often used for penetration testing and web application security testing. Fuzzers are used

for application testing by sending invalid data to the application, a WAF is a web application firewall, and a sniffer is useful for monitoring traffic, but not for modifying web traffic in a live, easy-to-use manner.

18. D. Fault injection directly inserts faults into the error handling paths for an application to verify how it will handle the problem. Stress testing focuses on application load, dynamic code analysis describes any type of live application testing, and fuzzing sends invalid data to applications to ensure that they can deal with it properly.
19. B. The application has a race condition that occurs when multiple operations cause undesirable results due to their order of completion. Dereferencing would occur if a memory location was incorrect, 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.
20. B. While this example includes continuous integration, the key thing to notice is that the code is then delivered/deployed into production. This means that Susan is operating in a continuous delivery/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 an Agile.

Chapter 10: Security Operations and Monitoring

1. A. DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a protocol that combines SPF and DKIM to prove that a sender is who they claim to be. DKIM validates that a domain is associated with a message, whereas SPF lists the servers that are authorized to send from your domain. POP3 is an email protocol but does not perform the function described.
2. D. A disassembler can translate binary machine code into assembly code, allowing it to be far more human readable. Once he has run a disassembler against the binary, Ben can perform further analysis of the program and its functions.

3. B. The syslog file is found in `/var/log` on most Linux hosts.
4. C. Charles is performing trend analysis. He has noticed a consistent change in pattern and has checked it over a period of time. His next step will likely be to look at the source and destination of the traffic, as well as details like the port and protocol associated with the traffic. With that information, he can determine if there is any security concern.
5. A. Piping output to `more` will break it up into pages, allowing Ian to page through the output from the top one at a time. `grep` would be useful for searching if he provided search terms. Neither of the flags shown will paginate `top`'s output.
6. C. Ben's best option is a workflow orchestration system that can define and manage the logical flow of his business processes. A continuous deployment (CD) pipeline can ensure that rules are deployed, but there is no mention of continuous integration, which is important for testing in addition to implementation. Finally, a SIEM is a security information and event management tool, and a fuzzer is used to test software by inserting random data. Neither will help Ben with this issue.
7. A. NetFlow does not capture the packet payload, and Chris will not be able to see this.
8. B. A user and entity behavior analytics (UEBA) tool will be her best bet. UEBA tools monitor end-user behavior using agents and focus on detection of anomalous behavior paired with analytics and correlation capabilities. A network analyzer would be useful for reviewing packets, antimalware with heuristics can detect malware but aren't focused on user behavior in most cases, and a DMARC tool would help with email security configuration.
9. B. Chris can block many known malicious links by implementing a DNS blackhole that is fed by a DNS reputation service. Blocking all links in email is likely to cause significant business impact, SPF and DKIM will not have an impact on links in email, and a proxy can filter web traffic. However, determining which URLs are from email links and which may have been browsed for or manually entered isn't likely to be able to be implemented in any reasonable way.

10. D. The analyst is performing data enrichment, the process of enhancing or improving data. In this case, the threat feeds and syslog input review will improve the overall quality of both the SIEM's threat feed and the data it is used to analyze.
11. B. The key entry here is the note inside the file that says, “This program cannot be run in DOS mode.” This indicates that the file is actually an executable, and that it is not actually a TIFF file. Michelle will need to do more investigation!
12. B. Elaine should check `/var/log/auth.log` , which is the default collection point for authentication logs for Linux systems. Red Hat and Centos logs for authentication go to `/var/log/secure` , but since that isn't listed, `auth.log` is the best and only correct answer among those listed.
13. A. Joseph hasn't taken into account the impact to the organization that the server being down may have, and he likely needs to assess whether the files were also uploaded or otherwise exposed. This means that he has looked at the localized impact to just the system and the immediate impact by noting what the impact is at the moment instead of what longer-term issues may arise.
14. B. While IP reputation tools can be useful, much like any automated blacklisting tool, they can also result in desired sites and services being blocked. Attacks that rely on popular services like Google Forms can result in services being blocked until they are manually whitelisted or fall out of the blacklist.
15. A. Tripwire and OSSEC are both open source options that provide host intrusion detection capabilities, including filesystem monitoring. The other answers were made up for this question.
16. C. The `-v` flag for `grep` returns any line that doesn't match the string. In this case, it will search for all logs in `/var/log/boot.log` without the string `"error"` in them. Charlene likely needs a better search string, since most of the `boot.log` file won't include the string error!
17. D. DMARC relies on both SPF and DKIM being set up properly, so Megan may need to walk their email administrator through all three steps to be able to use DMARC with them.

18. C. User agent information can include useful information about the originating device. In this case we can clearly see that the user agent lists Android 9 on a Samsung SM-N950U device. If you were to search for that term, you'd find out that the user was using a Galaxy Note 8. There is additional extraneous data about WebKit browsers, but the key element here is the clearly identified Samsung Android device.
19. C. The `/var/log/faillog` log file contains failed login attempts on Linux systems.
20. C. All Tony needs to verify that an email is from Mal is Mal’s public key. The email will be signed with Mal's private key. If the public key works, then Mal signed it.

Chapter 11: Building an Incident Response Program

1. D. A former employee crashing a server is an example of a computer security incident because it is an actual violation of the availability of that system. An intruder breaking into a building may be a security event, but it is not necessarily a computer security event unless they perform some action affecting a computer system. A user accessing a secure file and an administrator changing file permission settings are examples of security events but are not security incidents.
2. A. Organizations should build solid, defense-in-depth approaches to cybersecurity during the preparation phase of the incident response process. The controls built during this phase serve to reduce the likelihood and impact of future incidents.
3. C. A security information and event management (SIEM) system correlates log entries from multiple sources and attempts to identify potential security incidents.
4. C. The definition of a medium functional impact is that the organization has lost the ability to provide a critical service to a subset of system users. That accurately describes the situation that Ben finds himself in. Assigning a low functional impact is only done when the organization can provide all critical services to all users at diminished effi-

ciency. Assigning a high functional impact is only done if a critical service is not available to all users.

5. C. The containment protocols contained in the containment, eradication, and recovery phases are designed to limit the damage caused by an ongoing security incident.
6. D. The National Archives General Records Schedule requires that all federal agencies retain incident handling records for at least three years.
7. C. In a proprietary breach, unclassified proprietary information is accessed or exfiltrated. Protected critical infrastructure information (PCII) is an example of unclassified proprietary information.
8. A. The Network Time Protocol (NTP) provides a common source of time information that allows the synchronizing of clocks throughout an enterprise.
9. A. An organization's incident response policy should contain a clear description of the authority assigned to the CSIRT while responding to an active security incident.
10. D. A web attack is an attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or redirect to a site that exploits a browser vulnerability and installs malware.
11. A. CSIRT members do not normally communicate directly with the perpetrator of a cybersecurity incident.
12. A. The incident response policy provides the CSIRT with the authority needed to do their job. Therefore, it should be approved by the highest possible level of authority within the organization, preferably the CEO.
13. A. Detection of a potential incident occurs during the detection and analysis phase of incident response. The other activities listed are all objectives of the containment, eradication, and recovery phase.
14. C. Extended recoverability effort occurs when the time to recovery is unpredictable. In those cases, additional resources and outside help are typically needed.
15. D. An attrition attack employs brute-force methods to compromise, degrade, or destroy systems, networks, or services—for example, a DDoS

attack intended to impair or deny access to a service or application or a brute-force attack against an authentication mechanism.

16. C. Lessons learned sessions are most effective when facilitated by an independent party who was not involved in the incident response effort.
17. D. Procedures for rebuilding systems are highly technical and would normally be included in a playbook or procedure document rather than an incident response policy.
18. B. An impersonation attack involves the replacement of something benign with something malicious—for example, spoofing, man-in-the-middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
19. C. Incident response playbooks contain detailed, step-by-step instructions that guide the early response to a cybersecurity incident. Organizations typically have playbooks prepared for high-severity and frequently occurring incident types.
20. A. The event described in this scenario would not qualify as a security incident with measurable information impact. Although the laptop did contain information that might cause a privacy breach, that breach was avoided by the use of encryption to protect the contents of the laptop.

Chapter 12: Analyzing Indicators of Compromise

1. B. The df command will show you a system's current disk utilization. Both the top command and the ps command will show you information about processes, CPU, and memory utilization, whereas lsof is a multifunction tool for listing open files.
2. C. Perfmon, or Performance Monitor, provides the ability to gather detailed usage statistics for many items in Windows. Resmon, or Resource Monitor, monitors CPU, memory, and disk usage, but does not provide information about things like USB host controllers and other detailed instrumentation. Statmon and winmon are not Windows built-in tools.

3. D. Flow data provides information about the source and destination IP address, protocol, and total data sent and would provide the detail needed. Syslog, WMI, and resmon data is all system log information and would not provide this information.
4. A. Network access control (NAC) can be set up to require authentication. Port security is limited to recognizing MAC addresses, making it less suited to preventing rogue devices. PRTG is a monitoring tool, and NTP is the network time protocol.
5. A. A monitoring threshold is set to determine when an alarm or report action is taken. Thresholds are often set to specific values or percentages of capacity.
6. C. Active monitoring is focused on reaching out to gather data using tools like ping and iPerf. Passive monitoring using protocol analyzers collects network traffic and router-based monitoring using SNMP, and flows gather data by receiving or collecting logged information.
7. A. Beaconing activity (sometimes called heartbeat traffic) occurs when traffic is sent to a botnet command and control system. The other terms are made up.
8. C. Log analysis, flow monitoring, and deploying an IPS are all appropriate solutions to help detect denial-of-service attacks. iPerf is a performance testing tool used to establish the maximum bandwidth available on a network connection.
9. D. Hardware vendor ID codes are part of MAC addresses and can be checked for devices that have not had their MAC address changed. It is possible to change MAC addresses, so relying on only the MAC address is not recommended.
10. B. Locating a rogue AP is often best done by performing a physical survey and triangulating the likely location of the device by checking its signal strength. If the AP is plugged into the organization's network, nmap may be able to find it, but connecting to it is unlikely to provide its location (or be safe!). NAC would help prevent the rogue device from connecting to an organizational network but won't help locate it.
11. A. Microsoft Endpoint Configuration Manager provides non-real-time reporting for disk space. Resmon, perfmon, and SCOM can all provide

real-time reporting, which can help to identify problems before they take a system down.

12. B. The best way to deal with memory leaks is to patch the application or service. If a patch is not available, restarting the service or the underlying operating system is often the only solution. Buffer overflow and stack smashing prevention both help deal with memory-based attacks rather than memory leaks, and monitoring can help identify out-of-memory conditions but don't directly help deal with a memory leak.
13. A. A blacklisting application or tool can allow Sayed to specifically prevent specific files or applications from being installed. Microsoft Endpoint Configuration Manager could be used to uninstall files, and SCOM could be used to monitor machines for files, but neither is as well suited. Whitelisting works in the opposite manner by listing allowed files.
14. C. The most likely answer is that the link has failed. Incorrectly set sampling rates will not provide a good view of traffic, and a DDoS attack is more likely to show large amounts of traffic. SNMP is a monitoring tool and would not result in flow data changing.
15. B. SNMP alerts are called SNMP traps, and they are sent from endpoints to a central management system or collector where they are typically stored and analyzed. The rest of the answers were made up for this question.
16. B. The service --status command is a Linux command. Windows service status can be queried using sc, the Services snap-in for the Microsoft Management Console, or via a PowerShell query.
17. D. Protocol analysis, using heuristic (behavior)-based detection capabilities, and building a network traffic baseline are all common techniques used to identify unexpected network traffic. Beaconing occurs when a system contacts a botnet command and control system, and it is likely to be a source of unexpected traffic.
18. C. SNMP will not typically provide specific information about a system's network traffic that would allow you to identify outbound connections. Flows, sniffers (protocol analyzers), and an IDS or IPS can all provide a view that would allow the suspect traffic to be captured.

19. A. Whitelisting software prevents software that is not on a preapproved list from being installed. Blacklists prevent specific software from being installed, whereas heuristic and signature-based detection systems focus on behavior and specific recognizable signatures, respectively.
20. B. The top command in Linux provides an interactive interface to view CPU utilization, memory usage, and other details for running processes. df shows disk usage, tail displays the end of a file, and cpugrep is a made-up command.

Chapter 13: Performing Forensic Analysis and Techniques

1. B. dd creates files in RAW, bit-by-bit format. EN01 is the EnCase forensic file format, OVF is virtualization file format, and ddf is a made-up answer.
2. B. Slack space is the space that remains when only a portion of a cluster is used by a file. Data from previous files may remain in the slack space since it is typically not wiped or overwritten. Unallocated space is space on a drive that has not been made into part of a partition. Outer space and non-Euclidean space are not terms used for filesystems or forensics.
3. C. Event logs do not typically contain significant amounts of information about file changes. The Master File Table and file indexes (INDX files) both have specific information about files, whereas volume shadow copies can help show differences between files and locations at a point in time.
4. C. Write blockers ensure that no changes are made to a source drive when creating a forensic copy. Preventing reads would stop you from copying the drive, drive cloners may or may not have write blocking capabilities built in, and hash validation is useful to ensure contents match but don't stop changes to the source drive from occurring.
5. B. A legal hold is a process used to preserve all data related to pending legal action, or when legal action may be expected. A retainer is paid

to a lawyer to keep them available for work. The other two terms were made up for this question.

6. D. Core dumps and hibernation files both contain an image of the live memory of a system, potentially allowing encryption keys to be retrieved from the stored file. The MFT provides information about file layout, and the Registry contains system information but shouldn't have encryption keys stored in it. There is no hash file or encryption log stored as a Windows default file.
7. A. Timelines are one of the most useful tools when conducting an investigation of a compromise or other event. Forensic tools provide built-in timeline capabilities to allow this type of analysis.
8. D. Since Danielle did not hash her source drive prior to cloning, you cannot determine where the problem occurred. If she had run MD5sum prior to the cloning process as well as after, she could verify that the original disk had not changed.
9. D. The Volatility Framework is designed to work with Windows, macOS, and Linux, and it provides in-depth memory forensics and analysis capabilities. LiME and fmem are Linux tools, whereas DumpIt is a Windows-only tool.
10. D. Windows installer logs are typically kept in the user's temporary app data folder. Windows does not keep install log files, and System32 does not contain an Installers directory.
11. B. Windows crash dumps are stored in %SystemRoot%\MEMORY.DMP and contain the memory state of the system when the system crash occurred. This is her best bet for gathering the information she needs without access to a live image. The Registry and System Restore point do not contain this information, and WinDbg is a Windows debugger, not an image of live memory.
12. D. Manual access is used when phones cannot be forensically imaged or accessed as a volume or filesystem. Manual access requires that the phone be reviewed by hand, with pictures and notes preserved to document the contents of the phone.
13. A. CCleaner is a PC cleanup utility that wipes Internet history, destroys cookies and other cached data, and can impede forensic investigations. CCleaner may be an indication of intentional antiforensic activi-

ties on a system. It is not a full disk encryption tool or malware packer, nor will it modify MAC times.

14. B. Unallocated space is typically not captured during a live image, potentially resulting in data being missed. Remnant data from the tool, memory and drive contents changing while the image is occurring, and malware detecting the tool are all possible issues.
15. D. Jeff did not create the image and cannot validate chain of custody for the drive. This also means he cannot prove that the drive is a copy of the original. Since we do not know the checksum for the original drive, we do not have a bad checksum or a hash mismatch—there isn't an original to compare it to. Anti-forensics activities may have occurred, but that is not able to be determined from the question.
16. A. Imaging the system while the program is live has the best probability of allowing Jeff to capture the encryption keys or decrypted data from memory. An offline image after the system is shut down will likely result in having to deal with the encrypted file. Brute-force attacks are typically slow and may not succeed, and causing a system crash may result in corrupted or nonexistent data.
17. A. The tcpdump utility is a command-line packet capture tool that is found on many Linux systems. Wireshark is a GUI tool available for most operating systems. Netdd and snifman were made up for this question.
18. A. Ben is maintaining chain-of-custody documentation. Chris is acting as the validator for the actions that Ben takes, and acts as a witness to the process.
19. D. While AES does have a hashing mode, MD5, SHA1, and built-in hashing tools in FTK and other commercial tools are more commonly used for forensic hashes.
20. B. Both cloud and virtualized environments are often temporary (ephemeral) and thus can be difficult to perform forensics on. If you have a cloud, virtualized, or containerized environment, make sure you have considered how you would perform forensics, and what data preservation techniques you may need to use.

Chapter 14: Containment, Eradication, and Recovery

1. A. The containment, eradication, and recovery phase of incident response includes active undertakings designed to minimize the damage caused by the incident and restore normal operations as quickly as possible.
2. C. NIST recommends using six criteria to evaluate a containment strategy: the potential damage to resources, the need for evidence preservation, service availability, time and resources required (including cost), effectiveness of the strategy, and duration of the solution.
3. C. In a segmentation approach, the suspect system is placed on a separate network, where it has very limited access to other networked resources.
4. B. In the isolation strategy, the quarantine network is directly connected to the Internet or restricted severely by firewall rules so that the attacker may continue to control it but not gain access to any other networked resources.
5. D. In the removal approach, Alice keeps the systems running for forensic purposes but completely cuts off their access to or from other networks, including the Internet.
6. A. Sandboxes are isolation tools used to contain attackers within an environment where they believe they are conducting an attack but, in reality, are operating in a benign environment.
7. C. Tamara's first priority should be containing the attack. This will prevent it from spreading to other systems and also potentially stop the exfiltration of sensitive information. Only after containing the attack should Tamara move on to eradication and recovery activities. Identifying the source of the attack should be a low priority.
8. D. CompTIA includes patching, permissions, security scanning, and verifying logging/communication to monitoring in the set of validation activities that cybersecurity analysts should undertake in the aftermath of a security incident.

9. C. Understanding the root cause of an attack is critical to the incident recovery effort. Analysts should examine all available information to help reconstruct the attacker's actions. This information is crucial to remediating security controls and preventing future similar attacks.
10. C. Lynda should consult the disposal flowchart. Following that chart, the appropriate disposition for media that contains high security risk information and will be reused within the organization is to purge it.
11. B. New firewall rules, if required, would be implemented during the eradication and recovery phase. The validation phase includes verifying accounts and permissions, verifying that logging is working properly, and conducting vulnerability scans.
12. D. The primary purpose of eradication is to remove any of the artifacts of the incident that may remain on the organization's network. This may include the removal of any malicious code from the network, the sanitization of compromised media, and the securing of compromised user accounts.
13. B. There are many potential uses for written incident reports. First, it creates an institutional memory of the incident that is useful when developing new security controls and training new security team members. Second, it may serve as an important record of the incident if there is legal action that results from the incident. These reports should be classified and not disclosed to external parties.
14. D. Malware signatures would not normally be included in an evidence log. The log would typically contain identifying information (e.g., the location, serial number, model number, hostname, MAC addresses and IP addresses of a computer), the name, title and phone number of each individual who collected or handled the evidence during the investigation, the time and date (including time zone) of each occurrence of evidence handling, and the locations where the evidence was stored.
15. D. Even removing a system from the network doesn't guarantee that the attack will not continue. In the example given in this chapter, an attacker can run a script on the server that detects when it has been removed from the network and then proceeds to destroy data stored on the server.

16. A. The data disposition flowchart directs that any media containing highly sensitive information that will leave the control of the organization must be destroyed. Joe should purchase a new replacement device to provide to the contractor.
17. B. Incident reports should include a chronology of events, estimates of the impact, and documentation of lessons learned, in addition to other information. Incident response efforts should not normally focus on uncovering the identity of the attacker, so this information would not be found in an incident report.
18. D. NIST SP 800-61 is the Computer Security Incident Handling Guide. NIST SP 800-53 is Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-88 is Guidelines for Media Sanitization. NIST SP 800-18 is the Guide for Developing Security Plans for Federal Information Systems.
19. A. Resetting a device to factory state is an example of a data clearing activity. Data purging activities include overwriting, block erase, and cryptographic erase activities when performed through the use of dedicated, standardized device commands.
20. A. Only removal of the compromised system from the network will stop the attack against other systems. Isolated and/or segmented systems are still permitted access to the Internet and could continue their attack. Detection is a purely passive activity that does not disrupt the attacker at all.

Chapter 15: Risk Management

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 percent) 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. C. Top Secret is the highest level of classification under the U.S. system and, therefore, requires the highest level of security control.
13. 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.
14. D. The principle of data sovereignty says that data is subject to the legal restrictions of any jurisdiction where it is collected, stored, or processed.
15. C. Red team members are the attackers who attempt to gain access to systems. Sofia's team is fulfilling this role.

16. B. White team members are the observers and judges. They serve as referees to settle disputes over the rules and watch the exercise to document lessons learned from the test.
17. D. Blue team members are the defenders who must secure systems and networks from attack. The blue team also monitors the environment during the exercise, conducting active defense techniques.
18. 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.
19. A. Classification policies create different categories of data used within an organization and then specify the level of security control required for each classification level. Using classifications helps users understand the type of protection necessary for each data type they encounter.
20. D. Once an employee leaves the organization, they would no longer be subject to any of the technical controls that Alfonso might implement. These include intrusion prevention systems (IPSs), data loss prevention (DLP) systems, and digital rights management (DRM) systems. The best way to protect against unauthorized sharing of information by former employees is through the use of nondisclosure agreements (NDAs).

Chapter 16: Policy and Compliance

1. B. The key word 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. A. The Health Insurance Portability and Accountability Act (HIPAA) includes security and privacy rules that affect healthcare providers, health insurers, and health information clearinghouses.
4. B. The five security functions described in the NIST Cybersecurity Framework are identify, protect, detect, respond, and recover.
5. B. The International Organization for Standardization (ISO) publishes ISO 27001, a standard document titled “Information technology—Security techniques—Information security management systems—Requirements.”
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. 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.
8. B. The Sarbanes–Oxley (SOX) Act applies to the financial records of publicly traded companies and requires that those companies have a strong degree of assurance around the IT systems that store and process those records.
9. C. The code of conduct is often used as a backstop for employee behavior issues that are not addressed directly by another policy.
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. D. Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process. Examples of managerial controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices.
12. D. The Information Technology Infrastructure Library (ITIL) is a framework that offers a comprehensive approach to IT service management (ITSM) within the modern enterprise. ITIL covers five core activities: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

13. 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.
14. D. The data retention policy outlines what information the organization will maintain and the length of time different categories of information will be retained prior to destruction.
15. D. The description provided matches the definition of a Tier 4 (Adaptive) organization's risk management practices under the NIST Cybersecurity Framework.
16. D. Guidelines are the only element of the security policy framework that is optional. Compliance with policies, standards, and procedures is mandatory.
17. 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.
18. 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.
19. 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.
20. D. Procedures provide checklist-style sets of step-by-step instructions guiding how employees should react in a given circumstance. Procedures commonly guide the early stages of incident response.

Practice Exam Answers

1. D. Compensating controls are used to fulfill the same control objective as a required control when it is not feasible to implement that required control. The scenario describes a need for a compensating control. This control may be technical, operational, and/or administrative in nature.
2. C. Zero-day exploits take advantage of a security vulnerability that is not known until the exploit has been used—there is no time (zero days) between the discovery and the attack.
3. A. Threat hunting activities presume that a compromise has already taken place and search for indicators of that compromise. Vulnerability scanning activities probe systems for known vulnerabilities. Juan's activity could be described as intrusion detection, but not as intrusion prevention because he is not taking any action to block future attacks. Data mining is a generic term used in machine learning activities and Juan is not leveraging data mining in this work.
4. B. Honeypots are decoy systems used to attract the attention of intruders so that they may be monitored in a controlled environment. Mandatory access controls (MACs) are used to enforce system security policies. Intrusion prevention systems are designed to detect and block malicious activity. Rogue access points provide an unauthorized means of wireless access.
5. B. This is an example of delivering the payload to the victim, so it is from the Delivery stage of the Cyber Kill Chain.
6. A. A jump box is a system designed to accept remote connection requests and act as an intermediary between those remote systems and local hosts. Virtual machines, honeypots, and firewalls may all exist in the DMZ but do not have the express purpose of providing remote administrative access.
7. D. Port 1433 is used for Microsoft SQL Server and should not be exposed on a web server. Ports 22, 80, and 443 are required for SSH, HTTP, and HTTPS connectivity, respectively.
8. B. Sampling is often used to retain flow visibility while reducing the overall flow rates to a reasonable level. Rates of 1:10, 1:100, or 1:1000 can significantly decrease the load that flows create while providing useful visibility. RMON does not provide visibility into flow data.

Decreasing the number of flows per user would require reducing users' ability to use the network, much like using packet shaping to reduce traffic rates would cause the network to be less usable—not a desirable option in almost any network!

9. D. Infrastructure as a service (IaaS) is the only cloud service model where customers would configure operating systems themselves. In platform as a service (PaaS), function as a service (FaaS), and software as a service (SaaS) models, the cloud service provider is responsible for operating system configuration.
10. A. This is an example of a captive portal network access control (NAC) solution, which is an in-band NAC because it inserts a device between Barry and the Internet. Out-of-band solutions, such as 802.1x, require that Barry's system communicate with the network switch to support NAC. Agent-based solutions would require the installation of software on Barry's computer.
11. A. A network access control (NAC) system can allow Charles to require network authentication while performing security posture assessments on the systems that connect. This will allow his team to authenticate and use the network if they have secure systems.
12. D. The Trusted Platform Module (TPM) is a hardware chip found inside most modern computers that is used to store disk encryption keys. Hardware security modules (HSMs) also store encryption keys, but they are dedicated, costly devices. Trusted foundries are trusted sources for hardware, and the root of trust is a concept used to describe how trust flows through the components of a secure system.
13. C. Destruction is both the most effective and the costliest option identified in the NIST Guidelines for Media Sanitization. Clearing by using logical methods to clear addressable storage locations and using overwriting and cryptographic erase techniques for purging are both cheaper and easier to perform. Obliteration is not an option in the NIST listing.
14. A. Next-generation firewalls (NGFWs) are able to incorporate contextual information about a connection attempt when making access control decisions. This capability is not available in packet filters or state-

ful inspection firewalls. While an NGFW may be a perimeter firewall, not all perimeter firewalls have next-generation capabilities.

15. C. During a network attack simulation, the blue team is responsible for securing the targeted environment and keeping the attacking (red) team out. The white team serves as referees. There is no black team during a network attack simulation.
16. A. The three pillars of information security are confidentiality, integrity, and availability. Attacks against confidentiality seek to disclose sensitive information. Attacks against integrity seek to alter information in an unauthorized manner. Attacks against availability seek to prevent legitimate use of information or systems.
17. D. Segmentation occurs in the containment phase in the CompTIA incident response process. Bear in mind that CompTIA's incident response process differs from the NIST standard, and places sanitization, reconstruction/re-imaging, and secure disposal in the eradication and recovery phase.
18. D. Environmental threats are natural or man-made disasters outside the control of the organization. Accidental threats occur when an inadvertent action jeopardizes security. Adversarial threats occur when someone is actively seeking to attack the organization. Structural threats occur when there is an exhaustion of available resources.
19. B. PCI DSS is an information security standard required by major payment card brands for organizations that use their cards. HIPAA, SOX, and FERPA are all U.S. laws.
20. C. For most organizations, CSIRT activities initially involve internal resources. Law enforcement is involved only when it is believed that a crime has been committed, requiring participation of law enforcement officers.
21. B. Network reconnaissance normally takes place during the discovery phase of a penetration test. The attack phase consists of gaining access, escalating privileges, system browsing, and installing additional tools.
22. D. Under the risk management matrix used by most organizations, a risk with a medium likelihood and high impact would be considered a high risk.

23. C. Bandwidth consumption, beaconing, and unexpected traffic are all common network issues that you should monitor for. Link aggregation refers to combining links to create a higher throughput link.
24. D. Distributed denial-of-service (DDoS) attacks can be detected in many ways, including use of SIEM devices, IDSs and IPSs, network bandwidth and connection monitoring tools, and performance monitoring utilities. Fuzzers are used to send unexpected data to applications and won't help detect a DDoS.
25. A. Application programming interfaces (APIs) are used to programmatically integrate systems, including SaaS platforms. Security orchestration, automation, and response (SOAR) does integrate systems but specifically in the security, not productivity, space. The Security Content Automation Protocol (SCAP) also is used to integrate security, not productivity, systems. Continuous integration/continuous delivery (CI/CD) is an operational philosophy and not a specific technology.
26. C. Although the bandwidth used for active monitoring is typically relatively low, it does add to the total network traffic load. If the monitoring traffic is not prioritized, information is available less quickly than desired, and if it is prioritized, it may compete with other important traffic.
27. C. Nmap is a network port scanner and generated the output shown in the question: a list of network ports. Nessus is a vulnerability scanner and would produce a detailed report of vulnerabilities. Traceroute determines the path between two points on a network. Syslog is a logging facility on Linux systems.
28. A. Signature analysis uses a fingerprint or signature to detect threats or other events. This means that a signature has to exist before it can be detected, but if the signature is well designed, it can reliably detect the specific threat or event.
29. C. Wireshark is a protocol analyzer and can be used to capture network traffic in a standard format. Nessus and Nmap are vulnerability scanners. Nikto is a web application security scanner.
30. B. The Netstat tool shows all open connections on a system. Tcpdump and Wireshark are capable of capturing traffic from open connections

but will not display connections that are silent during the capture period. Traceroute shows the path between two systems.

31. D. There are many reasons to avoid imaging live machines if it is not absolutely necessary, but one advantage that imaging a live machine has is the ability to directly capture the contents of memory. Risks of capturing images from live machines include inadvertent modification of the systems, changes that may occur on the machine during imaging, the potential for malware to attack the imaging system or to detect and avoid it, and the fact that most live images don't capture unallocated space.
32. D. Organizational change management processes are often bypassed during an incident response process due to the urgency of the need to make quick changes. Once the incident response has been completed, changes are often filed as catch-up documentation as part of the postincident activities.
33. B. Brian is developing potential scenarios that might result in a successful attack. This is an example of establishing a threat-hunting hypothesis. Next, Brian should look for evidence of such an attack in an attempt to confirm or refute his hypothesis.
34. C. Multifactor authentication like token-based authentication can help prevent phishing attacks that result in stolen credentials resulting in attackers accessing systems. As long as attackers do not also acquire the token (often an app on a smartphone or a physical device kept in the user's pocket), the attacker will not have all the factors they need to authenticate. Context-aware authentication might help if attackers log in from places that legitimate users don't, but enhanced password requirements and shorter password lifespans have a relatively small impact, if any.
35. B. Unit testing tests the smallest testable parts of an application or program, ensuring that each component works properly before they are put together. UAT is user acceptance testing, Fagan inspection is a form of formal code review, and code segmentation is not a term used in software engineering or development.
36. C. Once a security incident has been detected and analyzed, CSIRTs move into an active phase of containment, eradication, and recovery.

Active measures seek to limit the damage, gather evidence, identify the attackers and systems they are using, and eradicate the effects of the incident.

37. B. This is most likely a port scan being used to conduct reconnaissance and determine what ports are open on the server. A DoS attack would more likely use requests to a service allowed through the firewall. SQL injection and cross-site scripting would be successful only against a web server that was allowed to receive connections through the firewall.
38. A. Cisco uses log level 0 for emergency situations. Log level 1 is for alerts. Log level 6 is for information, and log level 7 is for debugging.
39. D. Since Angela already knows the MAC addresses of all the devices due to her systems inventory, she can simply search for associated MAC addresses that do not match the list.
40. C. When existing controls are insufficient, do not resolve the issue, or are too difficult to implement, a compensating control is often put in place. It is important to document compensating controls, because they differ from the expected or typical control that would normally be in place.
41. A. The image shows a screenshot of network traffic captured using the Wireshark protocol analyzer.
42. D. The `-sV` flag reports banner and version information. The `-oG` flag generates greppable output. The `-sS` flag requests a TCP SYN scan. The `-b` flag is used to detect servers supporting FTP bounce.
43. B. Encrypting a drive with strong encryption like AES256 will make the loss of a drive less of an issue. In general, strong encryption with a key that has not also been exposed can make confidentiality risks like this negligible. Both MD5 and SHA1 are not encryption methods—they are hashes. DES is an older, weaker encryption method, and it would not provide strong protection for the drive.
44. A. It can be easy to forget how important policies and the standards and practices that derive from them are, but policies make up the foundation of an organization's security practices. When combined with awareness training, it is far more likely that the employees that Cynthia works with will avoid bad practices like taking unencrypted

drives home or neglecting to use web application security development best practices.

45. D. Cynthia's design should include an intrusion prevention system (IPS). An in-line IPS with the right signatures installed can detect and stop attacks, including SQL injection, cross-site scripting, and even denial-of-service (DoS) attacks. An intrusion detection system (IDS) could detect the attacks but can't stop them, whereas data loss prevention (DLP) systems are designed to prevent data from exiting an organization. A PRNG, or pseudo-random number generator, is not a security technology.
46. B. Port 1433 is used by Microsoft SQL Server, so Kevin is most likely scanning a database server.
47. A. The Secure Shell (SSH) protocol uses encryption by default. HTTP, MySQL, and SMTP do not use encryption unless configured to do so.
48. A. The key difference between a shared authentication model and a single sign-on (SSO) model is that shared authentication systems require users to enter credentials when authenticating to each site. Single sign-on only requires a single sign-on—exactly as the name says!
49. B. In NIST's classification scheme, this is a privacy breach, involving personally identifiable information. NIST defines four ratings: none, privacy breaches, proprietary information breaches, and integrity loss. Proprietary information breaches involve unclassified proprietary information, such as protected critical infrastructure information. Integrity losses occur when sensitive or proprietary information is changed or deleted. NIST does not use the broad term *confidentiality breaches*, instead preferring more specific definitions.
50. A. Port 53 is reserved for the Domain Name Service (DNS), which does not normally run on web servers. Ports 80 and 443 are used for HTTP and HTTPS, respectively. Ports in the range of 80xx are commonly used for web services running on nonstandard ports.
51. B. Perfmon (Performance Monitor) provides the ability to perform detailed data collection, unlike resmon's (Resource Monitor) high-level view, which does not include the use of counters. Winmon is a name

typically associated with malware, and sysctl is a Linux tool used for changing kernel parameters at runtime.

52. A. The DNS server that answered Kyle's request is identified in the first line of the response. The IP addresses that appear at the bottom are the server's response to Kyle's query.
53. B. Chain-of-custody tracking indicates who has access to and authority over drives, devices, and forensic data throughout their life cycle. This is a critical element in investigations that may end up in court or that will involve law enforcement.
54. C. Ryan has created an MD5 hash of his image file. This can be compared to the original, or if it is the original, it can be compared to figure copies to validate their integrity.
55. D. Hashes are compared to verify that the files are the same. Since MD5 returns a warning that the checksum did not match, we know that the files are different.
56. B. NTP (Network Time Protocol) is used to ensure that events that are logged and other actions taken that use system time line up properly. Without NTP enabled, it may be significantly more difficult to determine when events occurred, making the chronological view of events harder, or even impossible, to build.
57. C. The most important criteria when making decisions about the scope of vulnerability management programs are regulatory requirements, corporate policy, asset classification, and data classification.
58. D. PCI DSS only requires that internal scans be conducted by a qualified individual. External scans must be conducted by an approved scanning vendor (ASV).
59. C. Common Vulnerabilities and Exposures (CVE) provides a standard nomenclature for describing security-related software flaws. Common Vulnerability Scoring System (CVSS) provides a standardized approach for measuring and describing the severity of security-related software flaws. Common Platform Enumeration (CPE) provides a standard nomenclature for describing product names and versions. Open Vulnerability and Assessment Language (OVAL) is a language for specifying low-level testing procedures used by checklists.

60. D. DumpIt is a Windows-only memory forensics tool. LiME and fmem are both Linux kernel modules that allow access to physical memory, and the Volatility Framework is a multiplatform tool with support for a broad range of memory forensics activities.
61. B. The three steps in the vulnerability management life cycle are detection, remediation, and testing.
62. A. NIST uses three critical measures to determine an organization's tier in the framework: how mature their risk management process is, whether there is an integrated risk management program, and if the organization is effectively participating with external partners.
63. D. Credentialed scanning should always be performed with a read-only account to limit the potential impact on the system should the scanner malfunction or the account become compromised.
64. B. The system should be rated as moderate impact for confidentiality if "the unauthorized disclosure of information stored on the system could have a serious adverse impact on organizational operations, organizational assets, or individuals," according to FIPS 199.
65. B. Kerberos generating tickets, also known as golden tickets, can be created if attackers are able to gain domain administrator or local administrator access to the AD controller. This would allow attackers to set arbitrary ticket lifespans and to act as any user in the domain or forest.
66. D. LDAP attacks often focus on insecure binding methods, harvesting directory information by taking advantage of improper ACLs, LDAP injection, or denial-of-service attacks. Silver ticket attacks are associated with Kerberos, where the term is used to describe compromised service account credentials.
67. B. The most commonly accepted criteria for vulnerability prioritization include criticality of the systems and information affected by the vulnerability, difficulty of remediating the vulnerability, severity of the vulnerability, and exposure of the vulnerability.
68. A. The Federal Information Security Management Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS) both require the use of vulnerability scanning. The Gramm–Leach–Bliley Act

(GLBA) and Health Insurance Portability and Accountability Act (HIPAA) have no such requirement.

69. D. Testing code by running it is known as dynamic code analysis. Static code analysis looks at the source code for an application. Runtime is when a program is running, but runtime inspection is not a common term used in software engineering. There is no Run/Test method.
70. C. This scenario describes a false positive error—the condition where a scanner reports a vulnerability but that vulnerability does not actually exist.
71. D. Technical subject matter experts, IT support staff, legal counsel, human resources staff members, and public relations and marking staff are all frequently part of the CSIRT. Comptrollers are rarely part of the response process.
72. B. IPS and firewall devices can detect scans and probes, and may have built-in detection methods. A SIEM can pull data from multiple sources, identifying scans and probes against a variety of devices. SNMP traps provide information about the state of a device but are not useful when attempting to detect network scans or probes.
73. A. Regression testing focuses on ensuring that changes have not reintroduced problems or created new issues. Olivia has asked her team to do regression testing to make sure that the patches have not created new problems or brought an old problem back.
74. C. Fault injection directly injects faults into the error handling paths of an application and focuses on areas that might otherwise be missed. Fuzzing sends unexpected data, whereas mutation testing modifies the program itself to see how it handles unexpected behaviors. Fagan inspection is a formal inspection process.
75. A. Windows captures quite a bit of useful data about USB devices when they are connected, but it does not capture the device's capacity. The device name, serial number, vendor, brand, and even the user ID of the currently logged-in user when it was plugged in are captured.
76. D. This process shows a Fagan inspection, which consists of six phases: Planning, Overview, Preparation, Meeting, Rework and Follow-Up.
77. D. Windows workstations can be a treasure trove of forensic information. Volume shadow copies are manual or automatic copies of files or

volumes kept by Windows systems for backup.

78. A. This vulnerability is in the SSH protocol, which uses TCP port 22, as shown in the bottom portion of the graphic.
79. B. The most effective defense against SQL injection is the use of input validation. Firewall rules would not likely be effective because the web server likely requires access from the outside world. Honeypots and patching would not serve as a defense against a SQL injection attack.
80. C. Buffer overflow vulnerabilities in an operating system require a vendor-supplied patch to correct. Input validation would not be an effective defense. While firewalls and intrusion prevention systems may block an attack, they would not resolve the underlying problem.
81. D. None of these protocols should be used on a secure network. All versions of SSL contain unfixable vulnerabilities, as do TLS versions earlier than 1.2.
82. B. The most effective defense against cross-site scripting is the use of input validation. Firewall rules would not likely be effective because the web server likely requires access from the outside world. Honeypots and operating system patching would not serve as a defense against a SQL injection attack.
83. C. Network segmentation is a strong security control for ICS networks. Chelsea does not have access to the source code so she cannot rewrite it. No patch is available because the vendor no longer provides support. Encryption would not provide a defense against a buffer overflow attack.
84. A. In a virtualized datacenter, the virtual host hardware runs a special operating system known as a hypervisor that mediates access to the underlying hardware resources.
85. C. The most likely scenario is that the hotel is running a captive portal and the user must authenticate before trying to access other websites. While the other scenarios are possible, they are not as likely. If the error was with the company's certificate, other users would be reporting the same problem. It is possible that another hotel guest is attempting to trick the user into accepting a false certificate, but this is unlikely.