Security Assessment and Testing Domain 6 Practice Questions

Questions from the following topics are included in this domain:

- Designing and validating assessments and tests
- Conducting security control testing
- Collecting security process data
- Analyzing test output data and generating reports
- Conducting and facilitating security audits

To pass the CISSP exam, you must score high in the Security Assessment and Testing domain. Domain 6 has a 12% weighting on the exam and requires you to understand how to design and validate assessments and audits. Audits need to be done within the organization and, externally, acting as if a black hat hacker were performing them.

Security control testing includes vulnerability scanning and assessment, penetration testing, and observing activity through log files. It also covers understanding where management is involved in the security process, including disaster recovery and business continuity.

Code review and testing, misuse case testing, and running synthetic transactions on web applications will also be covered in this chapter. Understanding these software topics puts you a step ahead in preparing to pass the entire exam, since it is a primer to domain 8, Software Development Security.

Questions

1. The key difference between a vulnerability scan and a penetration test is which of the following?

   A. There is no difference between the two as they both search for vulnerabilities.

   B. Vulnerability testing is done only in physical environments to ensure the exit and safety doors are not vulnerable.

   C. Penetration testing is done only in logical environments to ensure firewalls are not vulnerable to attack.

   D. A vulnerability scan searches for vulnerabilities, but a penetration test exploits vulnerabilities.

2. Vivianne is a security tester working with management to determine which systems and departments to examine for an assessment. They also need to explain which processes need to be monitored. This is an example of which phase of the penetration test?

   A. Executing exploits

   B. Conducting documentation

   C. Defining the scope

   D. Running reconnaissance

3. Antoine is an auditor who needs to conduct an audit remotely from home because of a worldwide pandemic. An issue is discovered during the planning phase. What must be resolved?

   A. There is no such thing as a remote audit. All audits must be conducted onsite.

   B. Antoine currently uses dial-up internet at his home.

   C. Wireless internet at the company site is secure.

   D. The equipment operator does not like appearing on camera.

4. Which two of the following Service Organization Controls (SOC) reports are Type I and Type II reports? (Choose two.)

   A. SOC 1

   B. SOC 2

   C. SOC 3

   D. SOC 4

5. Sadio is the president of *Generic Plastics*. To win a bid with a Fortune 500 company, *Generic Plastics* are requesting their SOC 2 reports, stating they need more detail than the SOC 3 provides. SOC 2 reports are internal-only reports. What should he do?

   A. Inform the Fortune 500 company that SOC 2 reports are Generic Plastics-internal only.

   B. Provide the SOC 2 reports to the Fortune 500 company, but do not inform the board.

   C. Follow the policies of the Fortune 500 company.

D. Follow the policies of Generic Plastics.

6. Before auditing work begins, each organization must understand the Terms of Engagement (ToE). Which of the following is *NOT* part of the ToE?

   A. Pricing

   B. Scope

   C. Responsibilities

   D. Requirements

7. Pernille just ran a scan on her website and discovered that a hacker dropped files into her web server. The result of this test is considered which of the following?

   A. False positive

   B. False negative

   C. True positive

   D. True negative

8. Diego is an IT manager getting reports that three smaller departments have suffered from ransomware attacks. Because of the company having proper backups, no payments were made. What is his next *BEST* step?

   A. Pay the attackers.

   B. Run phishing exercises.

   C. Respond with ransomware attacks against the hackers.

   D. Have staff sign an agreement on not clicking on ransomware links.

9. As part of a physical audit, Wendie discovers several notes in wastebaskets revealing social security numbers, tax identification numbers, birth dates, and home addresses. Which attack did he execute to discover this issue?

   A. Social engineering

   B. Phishing simulation

   C. Wastebasket check

D. Dumpster diving

10. Level one merchants are required to conduct network scans how often to comply with PCI-DSS?

    A. Quarterly scans by an Approved Scanning Vendor (ASV)

    B. Bi-annual scans by internal auditors

    C. Annual scans by internal auditors

    D. Annual scans by an ASV

11. DeMarcus is an ethical hacker attacking *HART Hospital*, as authorized by their chief information security officer. Federal investigators notice the attack and raid DeMarcus' facility and arrest him. What is the *MOST LIKELY* reason for him being arrested?

    A. All hacking is against the law, including ethical hacking.

    B. He was attacking HERT Hospital instead of HART Hospital, which was unapproved.

    C. He was attacking the human resources department instead of the financial department, as per the agreement.

    D. He started the attack before getting his Get-Out-of-Jail-Free-Card document.

12. When attackers use Google searches, *WHOIS* results, and Wikipedia articles to learn about their potential victim, they are using what kinds of materials?

    A. Privately accessible

    B. Double-blind

    C. OSINT

    D. Library

13. A hacker dials multiple phone numbers, attempting to find modems and fax machines. What is this attack called?

    A. Sandstorm

    B. War dialing

    C. War driving

D. WarVOX

14. Good vulnerability reduction practices include all the following, *Except* for what?

    A. Patch updates

    B. New software

    C. Closing unused ports

    D. Firmware updates

15. *RMFco* announced they have resolved a zero day in their code. What should their clients do next?

    A. Wait to hear how early adopters are doing with the new security patch.

    B. Download the security patch, but do not install it until the CEO approves.

    C. Wait for RMFco to make a rollup patch with all their latest patches.

    D. Download the new security patch, test it, and install it on their production systems.

16. An application has been written where two processes are running at the same time. For process A to calculate properly, it needs data from process B. If process A calculates before process B completes, this is an example of which condition?

    A. Race condition

    B. Buffer overflow

    C. Process exhaustion

    D. Application development

17. The main difference between a business continuity plan (BCP) and a disaster recovery plan (DRP) is which of the following?

    A. The BCP requires testing, but the DRP does not because it is not as critical as business continuity.

    B. The DRP ensures the core business functions operate during a disaster; the BCP details steps to restore to normal operations after a disaster.

    C. The BCP ensures the core business functions operate during a disaster; the DRP details steps to restore to normal operations after a disaster.

D. There really is no difference because they both reduce downtime.

18. Which of the following SOC reports not only affirms that security controls are in place, but also lists the effectiveness of the security controls?

    A. SOC 2 – Type I

    B. SOC 2 – Type II

    C. SOC 3 – Type I

    D. SOC 3 – Type II

19. Virgil is a certified ethical hacker hired to find vulnerabilities in the GRC Bank website as if he were a malicious attacker. What type of testing is he conducting?

    A. Purple box testing

    B. Black box testing

    C. Gray box testing

    D. White box testing

20. The practice of conducting timely network vulnerability scans helps to discover which two exposures? (Choose two.)

    A. Open ports

    B. Poor passwords

    C. Unauthorized services

    D. File modifications

21. Amel is a security professional who believes hackers are within her network. She is concerned they are successfully covering their tracks by modifying log files. What are two steps she can take to mitigate altered log files? (Choose two.)

    A. Run consistent network scans.

    B. Install mantraps in the most vulnerable locations of the building.

    C. Write to WORM media.

    D. Periodically copy log files to remote locations.

22. Paul is a hardware technician who needs to replace the hard drive on the server. To complete this job, all users must be off the server. However, he has noticed that there are three users still on the system, since he has been checking remotely every 10 minutes. What is a better way for him to determine whether users are still logged on?

    A. Physically walk to each user's office and visibly determine whether they are still logged on to the server.

    B. Email all logged-on users, asking them to reply to the message once they are ready to log off the server.

    C. Text the users, asking them to call or text Paul once they have logged off the server.

    D. Create a synthetic transaction that polls for users every 5 minutes and then texts Paul when there are no users on the server.

23. Members of a software development team inspect each other's programming for bugs, bloat, and poor assumptions. This is an example of which activity? (Choose two.)

    A. Vericoding

    B. Code review

    C. Static code analysis

    D. Dynamic code analysis

24. A hacker compromises Kasey's account and uses malware to gain administrator rights. What is the term for when a hacker elevates their privileges?

    A. Verification

    B. Validation

    C. Privilege escalation

    D. Privilege creep

25. Frankie is taking 3 months of leave from *AMCO Inc.* to stay with his family because they just had a child. How should his accounts be managed while he is gone?

    A. Make no changes to his account access.

    B. Suspend his login credentials.

    C. Make no changes to his account access but enforce a password change upon his return.

D. Delete his account.

26. Tab is a systems administrator putting together a backup strategy to secure his files. Which of the following statements is correct?

    A. In general, differential backups are no different than incremental backups.

    B. In general, making full backups every day is not recommended.

    C. In general, differential backups require more tapes to restore, but daily differential backups are faster.

    D. In general, incremental backups require more tapes to restore, but daily incremental backups are faster.

27. Restoring systems back to standard operations after a disaster is known as disaster recovery. What is the process called where vital functions operate immediately after a disaster?

    A. Business continuity

    B. MTBF

    C. MTTR

    D. Disaster recovery

28. Kosovare runs a security training class for her team, teaching them to ask people "Did you forget your badge?" if they see someone wandering around the building without their badge. What can she do to be certain that staff are following their training?

    A. Run example scenarios in class, pretending someone does not have a badge.

    B. Hire an ethical hacker to wander around the building without a badge.

    C. Leave a badge lying in the parking lot and see if someone tries to use it.

    D. Ask security *not* to check for badges and allow anyone into the building.

29. Several signs and emails warn staff not to pick up and use USB drives found in parking lots, or elsewhere. These types of security notices fall under which category?

    A. Training

    B. Professional development

C. Awareness

D. Education

30. Sari just opened her new *SocCo* soccer warehouse business and is ready to take orders on her brand-new multi-function fax machine. A few months later, she receives several complaints that someone representing *SocCo* is demanding payments for fees already paid, and desires repayment by gift cards. What is the *MOST LIKELY* problem here?

    A. Attackers collected customer information by hacking her fax machine.

    B. Her bill collection company mistakenly called clients because they never reconciled payments with SocCo.

    C. The clients never paid their bills, and the bill collection is in order.

    D. One of her staff mistakenly called the clients, thinking their accounts were past due.

31. The practice of capturing and analyzing live user transactions from a website or application to monitor the user experience, or measure the performance of the application, is known as what?

    A. RPM

    B. DNF

    C. YUM

    D. RUM

32. Oguchi is a hacker who has crafted an email to collect bank account numbers from victims when they click the link inside it. He sends this email to the COOs and CFOs of *Standard Federal*. What type of attack is this?

    A. Whaling

    B. Spear phishing

    C. Vishing

    D. Phishing

33. *QWRK Inc.'s* software product has just released an update for their application. Soon, the hotline is overwhelmed with calls about a defect. What is the *MOST LIKELY* thing to have occurred?

A. Users have not upgraded to the latest release of the application.

B. A developer did not test the code before pushing it to the Git master branch.

C. QWRK's hotline is the victim of a Telephony Denial of Service (TDoS) attack.

D. Several hundred customers had their caps lock key on when they tried to enter their new passwords.

34. When an architect, designer, or developer reuses parts, components, or code instead of validating new replacements, the individual is engaged in which activity?

A. Band-aiding

B. Technical debt

C. Refactoring

D. Poor testing

35. Hedvig is a developer who just completed unit testing for her product. Once this test has passed, which test should she run to ensure the entire product is valid before releasing it to production? (Choose two.)

A. End-to-end testing

B. Performance testing

C. More unit testing

D. Integration testing

36. Integrating validating security with applications that are part of the DevOps cycle is also known as what? (Choose two.)

A. DevOps

B. Rugged DevOps

C. DevSecOps

D. Development

37. Gregg is a security manager crafting a preparedness audit for the company. To run the audit, he gets help from his staff and members of the human resources and legal departments. Which type of audit is this?

A. Internal

B. External

C. Third party

D. Combination

38. Which of the following is *NOT* a requirement of the payment card industry data security standard (PCI DSS)?

A. Protect stored cardholder data.

B. Collect the logins and passwords of each online customer.

C. Restrict physical access to cardholder data.

D. Regularly test security systems and processes.

39. When simulating an attack on an organization with penetration testing, which test should be done *FIRST*?

A. Both tests should be done at the same time.

B. External penetration test when done with automated tools; otherwise, internal penetration test is done first.

C. External penetration testing.

D. Internal penetration testing.

40. What is one of the *BEST* ways of ensuring the business continuity plan stays up to date?

A. Updating BCPs is not required if desk checks are done properly.

B. Keep the BCP updated as part of change management.

C. Conduct quarterly reviews of the BCP.

D. Conduct annual reviews of the BCP.

41. Which individual is responsible for data classification?

A. Data processor

B. Data custodian

C. Data user

D. Data owner

42. Paul is a security administrator reviewing audit logs from a security information and event management (SIEM) device. This activity would fall under which category?

    A. Detective

    B. Corrective

    C. Preventative

    D. Recovery

43. A computer job is running multiple threads. The value from thread A is passed to thread B a few seconds after the value is defined. If the value is altered within the few seconds before it reaches thread B, and thread B uses this new value, what kind of error occurs?

    A. Bug

    B. TOCTOU

    C. Docker

    D. Race condition

44. Irene is a network manager whose team has recently installed 50 IP cameras. Practicing good security, all default logins and passwords were changed to strong credentials. It is later discovered that one of the cameras is being used as an attack vector to breach the corporate network. What did the team miss?

    A. They forgot to change the credentials of the breached camera.

    B. A team member installed a 51st camera with the default credentials.

    C. Malware is within the cameras that go back to the manufacturer.

    D. The camera had a hardcoded password.

45. Steph is a security administrator who only wants to be notified of valid staff not gaining entry (false negative) when alerts reach three per minute. This level of notification would be considered a what?

    A. False negative counter

B. Control zone

C. Baseline

D. Clipping level

46. Mix is the chief security officer (CSO) of *MLX Corp*, and he is helping the security managers find the best security controls to protect their assets. Which technique does he advise the security managers to use to select the best controls?

A. Calculate single loss expectancies.

B. Rank threats and vulnerabilities.

C. Conduct risk analysis.

D. List all assets and recommended safeguards.

47. Carli is a security auditor providing results of her audit to the firm. A good audit report contains what types of data? (Choose two.)

A. Likely threats and vulnerabilities

B. A list of known attackers and locations

C. An estimate of repair fees that an auditor can provide

D. Probability and impact of the exploitation

48. Gyasi measures single loss expectancies, along with likelihoods, to evaluate whether he should purchase insurance or provide his own mitigations to protect corporate assets. These measurement indicators are known as what?

A. KCI

B. KGI

C. KRI

D. KPI

49. *XYZ bank* has been shut down due to a tornado that destroyed the building. Staff have attempted to call their managers on their cell phones, but a few numbers have changed, so they have reached the wrong people. Also, no one is familiar with first aid or CPR to assist the injured. How could the bank have been better prepared?

A. Hire an on-site nurse.

B. Keep the phone and extension lists updated.

C. Run a desk check.

D. Train the staff on the best escape routes.

50. Two programs that contain lists of known cybersecurity vulnerabilities, displaying an identification number of each vulnerability and description, would be which of the following? (Choose two.)

A. CVD

B. NVD

C. MITRE

D. NIST

51. Which of the following is *NOT* a requirement of the payment card industry data security standard (PCI DSS)?

A. Maintain a firewall to protect cardholder data.

B. Securely store credit card numbers and CVC codes.

C. Do not use default settings or default passwords.

D. Use and regularly update antivirus software.

52. Alyssa is a security system administrator taking a Linux class and learning how to hack networks with a utility called Kali. This type of learning falls under which category?

A. Awareness

B. Professional development

C. Training

D. Education

53. Which groups are *MOST* responsible for data leaks of personally identifiable information (PII)?

A. Hackers and script kiddies

B. External hacktivists

C. Nation-sponsored hackers

D. Employees and contractors

54. Arnie is a software developer and suggests to his supervisor to delay the project 1 week so that he can update the application with security mitigations. Why should his supervisor take this advice?

A. Because delays are normal in software development projects.

B. It costs significantly less to resolve security issues earlier in the process than later.

C. Customers are trained to expect projects to always be delayed.

D. You should always strive for perfect security.

55. An open sourced utility that runs vulnerability scans and penetration tests on a website is called what?

A. OWASP APPSEC

B. OWASP ZAP

C. OWASP API

D. OWASP WEBGOAT

56. Which of the following is *NOT* a risk of creating an application with open source components?

A. When developing under the LGPL license, the application must also be open sourced.

B. The developer may stop supporting the component.

C. The license may require fees if the primary application uses a for-profit model.

D. The open source code may contain some proprietary content.

57. Frances has just completed version 1.0.1 of their website and has switched over to the new version. Customers are complaining their purchases are failing. What is Frances' next *BEST* step?

A. Revert to version 0.99.1 of the website, even though it performs at 10% of normal operations.

B. Keep version 1.0.1 of the website running, quickly find a fix, and update the website to 1.0.1 when it's complete since the changes are minimal.

C. Revert to version 1.0.0 of the website and do further testing of 1.0.1 before uploading it.

D. Keep version 1.0.1 of the website running, quickly find a fix, and update the website to 1.0.2 when it's complete.

58. Bug number **535** was fixed with patch number 1. Bug number **435** was fixed with patch number 2. After customers installed patch number 2, several calls to support stated bug number **535** was returned. What type of testing was *NOT* done in this scenario?

A. Acceptance testing

B. Regression testing

C. Performance testing

D. Unit testing

59. What is a key problem with getting too many false positives and false negatives on a system?

A. Alerts eventually get ignored.

B. Such systems will not pass NIST standards for compliance.

C. The system is functional but requires extra attention.

D. The system is about to fail.

60. Which function assists administrators in determining how many shoppers did *NOT* complete a sale on the website?

A. User activity telemetry

B. Transaction telemetry

C. Application telemetry

D. Dependency telemetry

61. Maurice operates a website selling car parts. From time to time, customers click on the link for reporting a problem with the website. One customer wrote that she cannot find a part for her 1980 Chevy Chevette. What is the next step Maurice must take?

A. Ignore the message because it has nothing to do with a website issue.

B. Contact Chevy to see if he can get the part for her.

C. Ignore the message because he does not sell parts for Chevy cars.

D. Contact the customer.

62. You can monitor a website's storage, users, and system loads for effectiveness with which of the following utilities?

A. Alerts and logs

B. Events and logs

C. Metrics and logs

D. Thresholds and logs

63. A feature that's available in cloud systems monitors specific metrics to determine if more memory, CPU, or disk space is needed for an application to run efficiently. Once the loads return to normal, the system requirements return to normal. What is this feature called?

A. On-demand self-service

B. Autoscaling

C. Measured service

D. Resource pooling

64. Cloud vendors maintain data and applications using which life cycle steps?

A. Migrate --> secure --> monitor --> protect --> configure --> govern

B. Migrate --> secure --> protect --> monitor --> configure --> govern

C. Migrate --> secure --> protect --> monitor --> govern --> configure

D. Migrate --> protect --> secure --> monitor --> configure --> govern

65. In the arena of software development and using the principles of continuous integration (CI), developers work in which order before releasing finished code to production?

A. Test --> build --> code

B. Build --> code --> test

C. Code --> test --> build

D. Code --> build --> test

66. Sacha is a software developer in the area of research and development and requires beta application updates, and sometimes alpha releases. This would make him what type of user?

A. Early adopter

B. Mature user

C. Canary user

D. End user

67. What is the process called where one set of systems runs in a test environment, but gets switched to a production environment when testing completes? The systems that were running in production are now in the test environment.

A. Blue-green deployment

B. Purple deployment

C. Test-prod deployment

D. Red-blue deployment

68. Hugo runs the business continuity planning board. After completing other testing, he is ready to run a full test in the production environment. Which test should he choose to run?

A. Structured walkthrough test

B. Full interruption test

C. Desk check test

D. Checklist test

69. One key advantage of virtual machines related to security is which of the following?

A. The ability to run applications

B. The ability to take snapshots

C. The ability to run the Windows operating system

D. The ability to run the Linux operating system

70. Earnie is developing a website and has concerns that the website will look different on a smartphone, a computer, and a tablet. What kind of testing can he do to ensure the website will look good on all devices?

A. Website testing

B. Interface testing

C. Code review

D. Misuse case testing

71. Several engineers at *Desel Corp* are getting phone calls from a salesperson to make a $5,000 investment in gold. What caused this?

A. Vishing

B. War dialing

C. PhoneSweep

D. An engineer responded to an advertisement in a magazine.

72. Alejandro has noticed that a standard system file is missing. What utility can he use to help determine who deleted the file?

A. Folder auditing

B. Directory auditing

C. File auditing

D. Server auditing

73. What are two key differences between internal and external auditors? (Choose two.)

A. Internal auditors have a black box view of the organization.

B. External auditors are more effective because they are not affected by internal bias.

C. Internal auditors can measure effectiveness based on a recent baseline.

D. External auditors are more affected than internal auditors by the politics of the organization.

74. Two free, open source utilities that security administrators use to verify whether users are prone to phishing attacks are called what? (Choose two.)

A. Hak5

B. Gophish

C. Kali

D. King Phisher

75. What steps should be followed for an internal audit to ensure that the security study is beneficial?

A. Define audit --> Define threats --> Assess current status --> Resolve --> Prioritize

B. Define audit --> Define threats --> Prioritize --> Assess current status --> Resolve

C. Define threats --> Define audit --> Assess current status --> Prioritize --> Resolve

D. Define audit --> Define threats --> Assess current status --> Prioritize --> Resolve

76. Users have been split into two groups to test whether a single difference in a social media website keeps users more interested in the website and on it for longer. What is this testing called?

A. Negative testing

B. A/B testing

C. Red/blue teams

D. Penetration testing

77. Which of the following is *NOT* a software tool that analyzes source code for bugs and security vulnerabilities?

A. Compiler

B. SonarQube

C. WhiteSource

D. Veracode

78. Griedge is a network administrator who keeps router and switch firmware updated. She scans each update for malware and verifies the hash values. Users have noticed anomalies in the network and have discovered that hackers have gained entry. What caused this?

A. A hacker was able to infect the routers and switches with malware after the firmware updates.

B. A hacker was able to get malware installed in the firmware source code.

C. An inside attacker infected the routers and switches with malware after the firmware updates.

D. Untrained users unintentionally installed malware on their routers and switches after the firmware updates.

79. Yuki uses measurements based on all possible security alerts and monitors them weekly against her baseline and metrics to ensure she can reasonably protect the organization. These measurement indicators are known as what?

A. KCI

B. KGI

C. KRI

D. KPI

80. Ewa, a chief security officer (CSO), has just discovered that unreleased designs of their next-generation vehicle are in the *Car 'n' Driver* magazine. What can she do to mitigate future design leaks to the public?

A. Implement DLP.

B. Implement MAC.

C. Implement a forward proxy server.

D. Install and program a firewall.

81. Nilla is the manager of the business continuity plan board and wants to run a very simple, low-effort drill that ensures most of the vital pieces are in place in case of a disaster. Which test does she seek to run?

A. Full interruption test

B. Cutover test

C. Parallel test

D. Desk check test

82. Data remediation and reconciliation projects help keep records clean and consistent. Systems that monitor records for inconsistencies, and alert administrators of inefficiencies, are known as what?

A. Remediation systems

B. Reconciliation systems

C. Continuous auditing and analytics

D. Information governance

83. Nikita is a systems administrator who is in charge of recovering data on a server because the hard drive has crashed. She starts the recovery process and learns that the backup tapes are blank. What did the team neglect to do?

A. Test the RAID 0 (zero) system.

B. Perform backup verification.

C. Use the correct backup tape size.

D. Enable encrypted and compressed backups.

84. Debinha is an application developer who has completed a program that accepts credit cards. She simulates being a hacker, attempting to steal credit card information. This is an example of what kind of testing?

A. Normal case testing

B. Misuse case testing

C. Static code analysis

D. Code review

85. A centralized system that analyzes, correlates, and retains log files for the entire corporate network is known as which device?

A. TACACS

B. LDAP

C. Kerberos

D. SIEM

86. Jozy is a security analyst reviewing log files as part of a standard audit. He has noticed that apparent threats have attempted access at 2 A.M. on system A, but at 4 P.M. on system B. He checks the date on both systems and sees that it's incorrect on one of them. Which utility needs to be set up or tuned properly?

A. NTP

B. BIND

C. DNS

D. NAMED

87. Timely log reviews are conducted because they help security professionals uncover which kinds of issues? (Choose two.)

A. Detect attackers attempting to break into the network.

B. Zero days.

C. Whether users are using strong passwords.

D. Whether files are being modified via integrity checks.

88. Buffer overflow attacks occur because of poorly written applications. Attackers can exploit this vulnerability and can potentially gain access to the entire computer. They are called buffer overflow attacks because these attacks occur where?

A. Spaces on hard drives where files have been marked for removal

B. The main memory of the computer

C. Unused space in applications

D. Unused space within files

89. Cobi is a new business owner and has just purchased 100 prospect leads from *Glengary Leads*. The prospects are guaranteed to be interested in real estate opportunities. What is his *Greatest* risk?

    A. That only 90% of prospects will have interest in real estate opportunities.

    B. That only 50% of prospects will have interest in real estate opportunities.

    C. The lead list is stale because Glengary Leads has a poor reputation.

    D. That only 10% of prospects will have interest in real estate opportunities.

90. Tobin is a security manager and has learned that a new software management application has been introduced to the company. Staff are excited to use it because it will double production at half the cost of past methods. What is her *BEST* recommendation?

    A. Test the software for vulnerabilities before rolling into production.

    B. Because of past user testimonials, roll the application into production immediately.

    C. Because of user demand, roll the application into production immediately.

    D. Because of financial pressures, roll the application into production immediately.

91. Any testing that's performed where the evaluator has zero knowledge of the environment is also known as which kind of test?

    A. White box testing

    B. Red box testing

    C. Opaque testing

    D. Blind testing

92. Which *BEST* represents the five-step penetration testing process?

    A. Reconnaissance --> Assess vulnerabilities --> Scan --> Exploit --> Reporting

    B. Reconnaissance --> Scan --> Exploit --> Assess vulnerabilities --> Reporting

    C. Reconnaissance --> Scan --> Assess vulnerabilities --> Exploit --> Reporting

    D. Reconnaissance --> Exploit --> Assess vulnerabilities --> Scan --> Reporting

93. Dzsenifer is an ethical hacker who has been hired by *RCG Credit Union* to find security vulnerabilities as if she were a high-level executive at the bank. What type of testing is this?

    A. Gray box testing

    B. White box testing

    C. Black box testing

    D. Red box testing

94. Which two common vulnerabilities are typically found during internal scans?

    A. Wireshark results

    B. Open network ports

    C. Unpatched systems

    D. Nessus results

95. Which Service Organization Controls (SOC) reports related to security and privacy do *NOT* focus on financial controls? (Choose two.)

    A. SOC 1

    B. SOC 2

    C. SOC 3

    D. SOC 4

96. What are two aspects of compliance audits? (Choose two.)

    A. They prove that the auditee is following regulatory requirements.

    B. They must be exclusively performed by third-party auditors.

    C. They must be exclusively performed by internal auditors.

    D. They prove that the auditee is following their policies.

97. Internal audit teams have what advantage over third-party auditing?

    A. Internal auditors have the best understanding of the technology, people, and processes.

B. Internal auditors have exposure to other security methods that are used by other organizations.

C. Internal auditors are not concerned with the impact of submitting a negative audit.

D. Internal audits are looked at more favorably by regulators over third-party audits.

98. Davici is an auditor. As part of their inspection, they must review a room where no cameras are allowed due to the risk of a fire occurring. What is his next *BEST* step?

A. Conduct the audit within the room and shoot fewer pictures because the risk of a fire occurring is low.

B. Conduct the audit within the room and sketch drawings where required.

C. Skip the room; if the rest of the audit passes, provide a positive complete certification.

D. Cancel the audit and delay the final certification.

99. Rose has conducted an audit for *MMOH Enterprises*, but because of a missing part, she cannot complete the audit. The part will arrive next week. What is her next *BEST* step?

A. Pass MMOH as a completed audit and apply for the certificate of success.

B. Fail MMOH Enterprises and schedule the next 3-year audit.

C. Schedule a time when the audit can be completed.

D. Redefine the scope of the audit.

100. What is the next step of the audit process after conducting the audit?

A. Document the results.

B. Inform management.

C. Determine the goals.

D. Select audit team members.

Quick answer key

1. D	16. A	31. D	46. C	61. D	76. B	91. D
2. C	17. C	32. A	47. A D	62. A	77. A	92. C
3. B	18. B	33. B	48. C	63. B	78. B	93. B
4. A B	19. B	34. B	49. C	64. B	79. A	94. B C
5. D	20. A C	35. A D	50. A B	65. D	80. A	95. B C
6. A	21. C D	36. B C	51. B	66. C	81. D	96. A B
7. C	22. D	37. A B	52. C	67. A	82. C	97. A
8. B	23. B C	38. B	53. D	68. B	83. B	98. B
9. D	24. C	39. C	54. B	69. B	84. B	99. C
10. A	25. B	40. B	55. B	70. B	85. D	100. A
11. D	26. D	41. D	56. A	71. D	86. A	
12. C	27. A	42. A	57. C	72. C	87. A D	
13. B	28. B	43. B	58. B	73. B C	88. B	
14. B	29. C	44. D	59. A	74. B D	89. C	
15. D	30. A	45. D	60. A	75. D	90. A	

Answers with explanations

1. **Answer: D** Both types of testing are done in physical, logical, and administrative environments, and both search for vulnerabilities, but penetration testing takes the extra step of running exploits, ideally doing no harm.
2. **Answer: C** After defining the scope of an audit, penetration testing includes reconnaissance, enumeration, vulnerability analysis, launching the exploit, and documenting the final report for management.
3. **Answer: B** This question is intentionally vague because the real exam contains some questions like this where certain likely assumptions must be made; that is, to conduct a remote audit, there will need to be a live video feed. Dial-up internet is too slow for viewing the video stream from the audit site. Remote audits are allowed, if necessary, for example, during a worldwide pandemic. Corporate policies should cover whether an employee can be on camera. You can learn more about audits at https://iaf.nu/articles/FAQ/288.
4. **Answer: A and B** The SOC 3 report, which is provided by suppliers, contains general information that's usually posted on a website to prove that an organization practices good security protocols. SOC 4 reports do not exist.
5. **Answer: D** Policies may allow internal data to be released, depending on certain sized deals or relationships. If they have such a policy, they must provide the SOC 2 reports to the Fortune 500 company, so following Generic Plastics' policies is the best answer here.

6. **Answer: A** Pricing is part of the offer letter, after the terms of engagement (often called the rules of engagement) are completed. Scope, objective, definitions, responsibilities, how to handle changes, and requirements are all part of the written terms of engagement.
7. **Answer: C** A true negative rarely gives an alert because no problem has been detected. An example of a false positive is when a user attempts to download a file but is denied because the system incorrectly sees them as a threat. A false negative would not have reported a website breach. To learn more about true and false positives and how they work, visit https://bit.ly/3cTBFIU.
8. **Answer: B** Ransomware against hackers is considered a hack-back and is against the law. An employee agreement will not help. Most users are fooled into clicking ransomware links since they appear to be normal.
9. **Answer: D** Dumpster diving is more detailed than social engineering, even though dumpster diving is a type of social engineering. The wastebasket check is a false option. Phishing simulations are done via email.
10. **Answer: A** Approved scanning vendors (ASVs) are required to run penetration and internal scans, and then report the results to their acquiring financial institution. Level 1 merchants process more than 6 million credit card transactions annually, so they are desirable targets for hackers. Learn more here: https://semafone.com/blog/a-comprehensive-guide-to-pci-dss-merchant-levels/.
11. **Answer: D** Running approved penetration tests is not against the law. Once chief management has agreed to the test, they need to provide a *Penetration Test Approval* document to the ethical hacker in case they appear malicious to authorities. This includes the contact information of top management so that the authorities can contact them and ensure the hacking was approved.
12. **Answer: C Open source intelligence** (**OSINT**) uses common free, legal, and publicly available tools to learn about the target.
13. **Answer: B** Sandstorm's *PhoneSweep* and *WarVOX* are applications that are used to conduct war dialing. War driving is where you scan for Wi-Fi hotspots, usually while driving a car.
14. **Answer: B** New software generally contains bugs and needs to be updated and patched immediately. The others are good vulnerability reduction practices.
15. **Answer: D** Zero days are major security issues that hackers exploit, and there is no fix for the vulnerability yet. Once a fix is created, the update needs to occur as soon as possible.
16. **Answer: A** A buffer overflow attacks memory due to poor coding and allows the attacker to control the process. Process exhaustion occurs when a process hangs because it has run out of resources. Application development is basic computer coding and is not a negative condition.
17. **Answer: C** Business continuity plans and disaster recovery plans must be tested to ensure the organization can operate and recover after a major disaster, such as a fire or tornado.
18. **Answer: B** SOC 3 reports do not have differing types, and SOC 2 – Type I shows that security controls are in place.
19. **Answer: B** Malicious hackers have no internal knowledge of the environment. White box testing simulates an internal attacker because they have full knowledge of the

environment. Gray box means the hacker has some knowledge of the internal environment. Purple box is a false option.

20. **Answer: A and C** Poor password testing is done with tools such as *Cain & Abel* or *John the Ripper*. File modifications are checked with integrity checkers such as *Nessus*. Open ports are checked with tools such as *Nmap*.
21. **Answer: C and D Write-once read-many** (**WORM**) media cannot be modified once written. This media prevents attackers from deleting their entries. Also, hackers cannot delete entries from remote systems they cannot access. *Mantraps* lock a threat in a room until security staff arrives. *Network scans* search for open ports and services.
22. **Answer: D** This is a great case for using synthetic transactions. Physically walking to each user could take too much time because they could be 100 miles away from Paul. Email and texting are good, but the user might forget to contact Paul after logging off.
23. **Answer: B and C** Dynamic code analysis is where we validate results when users run the application. *Vericoding* is a false option.
24. **Answer: C** Verification ensures all the components are in place, while validation ensures that all the components are effective. Privilege creep is the accumulation of privileges that you might obtain as you move from department to department within an organization.
25. **Answer: B** Temporarily suspending access protects Frankie's data. At the same time, the account is not vulnerable to hackers since it has been temporarily closed. Timely password changes are important, but if the account is left open while he is gone, it is still vulnerable to attack.
26. **Answer: D** Many companies make daily full backups, which simplifies recoveries because only one tape is needed. Differential backups require fewer tapes to restore than incremental, but daily backups generally take longer.
27. **Answer: A Mean time between failure** (**MTBF**) is a prediction as to when hardware will fail. **Mean time to repair** (**MTTR**) is the average time it takes to repair an item after a failure. MTBF and MTTR are related to events or incidents, not business-wide disasters.
28. **Answer: B** Asking security not to check for badges leaves the entire building insecure; this should never be done. Leaving a badge in the parking lot to see if it will be abused is testing a different scenario; we are concerned with people *not* wearing a badge. Example scenarios in the class are good, but an ethical hacker runs a live case scenario and can provide a report on the experience.
29. **Answer: C** Professional development and education are formalized programs where students can obtain credit hours toward a certificate or degree. Training includes classes that are designed to teach an individual a new skill. Awareness is exposure to different subjects so that people can recognize security issues and respond to them better.
30. **Answer: A** Multi-function printers attached to company networks are vulnerable to attacks and can grant a hacker access to the entire network, where they can exploit customer records. Bill collection companies and staff would not request payment via gift cards.
31. **Answer: D Real-user monitoring** (**RUM**) measures user and application performance. **Yellowdog Updater, Modified** (**YUM**), **Red Hat Package Manager** (**RPM**), and **Dandified YUM** (**DNF**) are Linux package management tools.

32. **Answer: A** Spear phishing is close, but since he is targeting **Chief Operating Officers** (**COOs**) and **Chief Financial Officers** (**CFOs**), this is whaling because they are high-level executives that have more knowledge about the organization. Phishing is similar, but phishing attacks are sent to a broad community, and vishing is done by phone, not email.
33. **Answer: B** The hotline was not overwhelmed until the new software was released, so customers performed the update. The attacker behind a TDoS attack would not hang on the phone line long enough to open a service call about a defect. Most systems warn users that their *Caps Lock* key is on when entering their passwords.
34. **Answer: B** Poor testing, band-aiding, and code refactoring, such as reusing code and making small changes so that it works in the new software, are all components of technical debt. These quick fixes are left unvalidated and can end up costing much more to fix as the project moves closer to production.
35. **Answer: A and D** End-to-end testing checks the entire system, while integration testing validates that the different units work together. More unit testing is not necessary, and performance testing tests the product under varied loads, but not in terms of functionality.
36. **Answer: B and C** DevOps is the combination of development and operations, which includes testing and release to production. You can learn more about *rugged DevOps* here: https://insights.sei.cmu.edu/blog/build-devops-tough/.
37. **Answer: A** Internal audits are conducted by the organization's staff. External audits occur via a business supplier to ensure their security meets the policy. Since all the testers work for the organization, this is not a third-party audit because this requires hiring an outside organization to conduct the audit. A combination audit would be run by company resources and third-party resources. You can learn more here: https://quality-one.com/auditing/.
38. **Answer: B** Maintaining account information for online customers is not a requirement of PCI-DSS.
39. **Answer: C** External penetration testing simulates a threat from outside the company and helps expose vulnerabilities that can be exploited. Then, an internal penetration test is performed to simulate what an attacker can do after exploiting external vulnerabilities. The internal test also simulates an insider attack. These tests can be performed by corporate teams or professional third-party organizations.
40. **Answer: B** As new systems and software are added to the environment, always ask what effect this change will have on business continuity. This is normally done within the change management process. Most teams run change management weekly, so updates are frequent.
41. **Answer: D** Data users can access the data if they meet the correct classification level. The data custodian is in charge of making good backups. The data processor uses this information to send postal mail and emails. The data owner is legally accountable if the data is breached.
42. **Answer: A** SIEM devices are **Intrusion Detection Devices** (**IDS**), not **intrusion prevention devices** (**IPS**) such as firewalls. A corrective device corrects the asset state after an exploit; for example, a water sprinkler is a corrective device in case of a fire. Backup tapes are examples of recovery devices that return the asset to its normal state.
43. **Answer: B** This is a bug, but there is a more specific answer. **Time-of-check to time-of-use** (**TOCTOU**) is the result of a race condition where the value is *not* verified

immediately before it's used by the next computational thread. Docker is a utility that's used to clone a virtual machine image.

44. **Answer: D** Hardcoded passwords are written into the firmware. The best way to remove these is with a security firmware update from the manufacturer. They changed all the credentials, so they did not miss one. Also, they only installed 50 cameras according to the question. If malware was followed back to the manufacturer, several cameras would have been breached.
45. **Answer: D** A baseline is considered an expected normal level for alerts; this value could be higher or lower than the clipping level. False negative counters and control zones are both false options.
46. **Answer: C** Listing assets and safeguards, ranking threats and vulnerabilities, and calculating **single loss expectancies** (**SLEs**) are all phases of the risk analysis process.
47. **Answer: A and D** A good technical audit also lists the recommended actions to take to reduce the impact of exploitation. A list of attackers and locations is too numerous, and changes by the minute. The auditor must not be the repair person because this is poor separation of duties, and therefore insecure.
48. **Answer: C Key control indicators** (**KCIs**) are used to evaluate a security control and if it stays within a certain tolerance level. **Key risk indicators** (**KRIs**) measure whether risks fall within tolerances that have been measured against **SLEs**. **Key performance indicators** (**KPIs**) are a leading indicator for evaluating whether the organization is on target to achieving a goal. **Key goal indicators** (**KGIs**) are lagging indicators that are evaluated once a goal has been reached.
49. **Answer: C** Part of the desk checking process is to make sure phone numbers are updated, training programs are implemented on escape routes and first aid, and to determine whether everyone knows their role as part of a disaster.
50. **Answer: A and B** MITRE is a community-driven effort that tracks and provides the **common vulnerabilities and exposures** (**CVE**) list. The **national vulnerability database** (**NVD**), provided by NIST, syncs the CVE list of vulnerabilities to their list.
51. **Answer: B** The **card verification code** (**CVC**) that is on the back of most credit cards should *not* be saved by the merchant.
52. **Answer: C** Professional development and education are formalized programs where students can obtain credit hours toward a certificate or degree. Training includes classes that are designed to teach an individual a new skill. Awareness is exposure to different subjects so that people can recognize security issues and respond to them better.
53. **Answer: D** Nation-sponsored hackers and other hackers often persuade employees to leak data by offering them money or making threats. Script kiddies are people who are new to hacking and generally harm themselves more than others. Hacktivist are driven by a cause; for example, they may really want people to use stronger passwords. Learn more about data breaches here: https://www.pandasecurity.com/en/mediacenter/security/who-is-to-blame-data-breaches/.
54. **Answer: B** According to NIST and the Poleman Institute, repairs that might cost $80 to fix during development end up costing $240 to fix at build time. If you were to repair during the **quality assurance** (**QA**) process, it would cost $960, and after production, it would cost $7,600. You can learn more about defect costs here: https://owasp.org/www-pdf-archive/APAC13_Keynote_HyojinChoi.pdf.

55. **Answer: B** Features include an intercepting proxy server, automation tools, fuzz testing, and script support. OWASP *Webgoat* is an intentionally vulnerable website you can practice on with OWASP ZAP. OWASP AppSec Pipeline applies DevOps and Lean principles for designing secure applications. OWASP API Security Project focuses on mitigating vulnerabilities in **application programming interfaces** (**APIs**).
56. **Answer: A** Free software, although usually *free* of charge, allows users specific *freedoms* in terms of liberties; for example, the right to view the source code. The **Lesser General Public License** (**LGPL**) allows the developer to keep their source code closed, if desired, whereas the **General Public License** (**GPL**) requires that applications using GPL code must also open source their applications. The other risks can harm the developer financially. You can learn more here: https://www.gnu.org/licenses/lgpl-3.0.html.
57. **Answer: C** Revert to a known-good version so that the organization does not lose sales. The other options risk losing business and customer goodwill.
58. **Answer: B** Regression testing ensures no functionality is lost or that past fixed problems are not reintroduced into the system. Acceptance testing focuses on meeting requirements. Performance testing checks how the system responds to different loads. Unit testing checks an individual module; this usually results in regression problems because examiners do not continue with a full functional or integration test.
59. **Answer: A** All alerts, including true alerts, can eventually be ignored. The other options are not true because getting false alerts is common across common systems.
60. **Answer: A** User activity telemetry informs administrators of click streams that have been started and abandoned. Transaction telemetry is a false option; there is a feature called **transaction traceability** that monitors workloads. Application telemetry monitors error messages and the response times of web apps. Dependency telemetry monitors varied response times, such as networks or databases.
61. **Answer: D** The next step is to contact the customer to learn more about the issue and determine which part she needs. This is because if Maurice contacts Chevy first, he will not know which part to order. If Maurice ignores customers' issues, they will eventually feel like he does not care about them, and they will shop elsewhere.
62. **Answer: A** Alerts use thresholds and metrics to immediately inform administrators that a system requires attention. Events are entries that go into log files.
63. **Answer: B** On-demand self-service does not operate automatically but requires manual intervention when it comes to adding resources. Measured services can provide more services manually, but not automatically. Resource pooling allows multiple tenants to share resources; if one user overloads the system, it will affect all the users.
64. **Answer: B** Migration refers to moving data to the cloud vendor. Securing data is ensuring that the software can defend known threats. Protection ensures the data is always available; part of this is making backups. Monitoring tracks the health and availability of data. Configuring ensures that the application is set up to run efficiently. Governance ensures that applications correspond to the policy that has been set up.
65. **Answer: D** Coding, building, and testing are the correct steps to take when developing code before releasing it to production. Most releases start smaller with some form of beta testing before being released to a wider audience.
66. **Answer: C** Canary users desire bleeding-edge features as soon as possible. Early adopters use applications after some testing and may use higher generation beta software,

but not early releases. End users only use applications after thorough testing, often using older software versions because they do not trust newly released gamma software.

67. **Answer: A** The production systems may be on the green servers and being tested on the blue servers. Once testing is complete, blue gets switched to production, and green becomes the test environment. The other options are false options. Red-blue teams are used in ethical hacking exercises, where red is the threat and blue is the defender. Purple members maximize the effectiveness of the hacking exercise. You can learn more here: https://blog.christianposta.com/deploy/blue-green-deployments-a-b-testing-and-canary-releases/.
68. **Answer: B** Walkthroughs are what they sound like, where the team *walks through* a scenario without touching the production systems. Desk checks and checklist tests allow the team to discuss scenarios and make educated guesses as to how to best recover from disaster. Full interruption tests use live systems to evaluate responses to a disaster.
69. **Answer: B** Snapshots are instant backups. Virtual machines can make snapshots daily, or even more frequently. When data needs to be recovered, it is as simple as reverting to a snapshot, which is much faster than recovering from a backup tape.
70. **Answer: B** Website testing is too general an answer. Interface testing is specifically what needs to be done: testing the website with each device. A code review is where the source code is inspected by a team, while misuse testing is intentionally trying to break the software's security.
71. **Answer: D** The question asked what *caused* the attack, not the *type* of attack being performed. The technique the boiler room operators are using is known as war dialing. They dial through all the extensions the original investor *gave them* by responding to the advertisement. This is a type of vishing attack because the attackers are selling investments they do not own. *PhoneSweep* is a tool that's used for war dialing.
72. **Answer: C** Server, directory, and folder auditing are too broad for validating the entire server, directories, and folders, respectively. File auditing just validates files and informs Alejandro who modified, created, or deleted a file.
73. **Answer: B and C** Internal auditors have a white box view of the organization because they know all the details of the company. Internal auditors are more affected by organizational politics, and these relationships could cause them to alter the results so that they're more favorable to companies or business units.
74. **Answer: B and D** Hak5 and Kali provide security toolkits that contain phishing simulators, but these are general-purpose ethical hacking utilities. *Gophish* and *King Phisher* provide phishing simulators with GUI environments showing users that fell victim to the email.
75. **Answer: D** Internal security audits help mitigate data breaches. Conducting an audit at the best value involves the five steps provided in answer D. For more details, visit https://blog.dashlane.com/conduct-internal-security-audit/.
76. **Answer: B** A/B testing is a basic controlled experiment where a single difference is tested. Red and blue teams are used as part of penetration testing. The red team acts as the hacker, while the blue team acts as the defender. Negative testing hardens applications, checking to see how they will respond to unwanted input.
77. **Answer: A** A compiler converts source code into machine language and can find coding syntax errors. *SonarQube*, *WhiteSource*, and *Veracode* search for security vulnerabilities,

poorly written libraries, and licensing-related issues to keep the source code accurate and consistent.

78. **Answer: B** The update developer created a hash value in the code they believed was credible; therefore, the resulting hash gets marked as trusted, even though the code should be marked as untrusted. Malware protection scanners would have picked up issues in options A, C, and D.
79. **Answer: A KCIs** are used to evaluate security controls and whether they stay within a given threshold. **KRIs** measure whether risks fall within tolerances. **KPIs** are a leading indicator to evaluate whether the organization is on target to achieve the desired goals or objectives. **KGIs** are lagging indicators that are evaluated once a goal has been reached, and they measure how well the goal was achieved. You can learn more here: https://stratexsystemsadmin.squarespace.com/blog/2013/1/30/kpis-kris-kcis-are-they-different-if-so-does-it-really-matte.html.
80. **Answer: A Data loss prevention** (**DLP**) is the best solution for stopping insider attacks like this. **Mandatory access control** (**MAC**) can help, but the insider leaking the designs may have top-secret clearance. A proxy server enforces security policies, such as which websites can be viewed. A firewall blocks unwanted traffic from entering the corporate network.
81. **Answer: D** Full interruption and cutover tests simulate a disaster using production systems. Parallel tests build up systems that are identical to production systems and simulate a disaster on the secondary systems. A desk check involves the team reviewing and updating a checklist of items that are important in case a disaster occurs.
82. **Answer: C** Continuous auditing and analytics enforces good information governance, which includes remediation and reconciliation to keep records such as social security numbers, phone numbers, pricing, costing, and more clean and consistent.
83. **Answer: B** After encrypted and compressed backups are made, they must be tested. RAID 0 systems don't data mirroring like RAID 1 systems do. If the backup tapes did not physically fit, they would have discovered that much earlier.
84. **Answer: B** Normal case testing assumes that you are attempting to use the software in a normal manner, not as an attacker. Code review and static analysis involves other members of the team reviewing each other's source code for the application.
85. **Answer: D** A **security information and event management system** (**SIEM**) logs and tracks events over the entire network. **Kerberos**, **LDAP**, and **TACACS** are network-based authentication systems, and they only log authentication events.
86. **Answer: A** The **network time protocol** (**NTP**) ensures that all the systems are time-synchronized from a standard server. **Domain name service** (**DNS**), **NAMED**, and **BIND** are all domain name search utilities.
87. **Answer: A and D** Zero days are undiscovered vulnerabilities, so log reviews cannot detect these. Authentication tools force users to use strong passwords.
88. **Answer: B** Data that's written within unused space is called a SNOW attack, a type of steganography attack that hides attacks in plain sight.
89. **Answer: C** Cobi should validate and verify his suppliers before using them. Cobi starts calling the prospect leads that he bought, and several prospects complain to him that they wish the phone calls would stop because the same leads were sold to several others, and they are calling the same prospects. He will eventually find that Glengary Leads will not honor their guarantee because they will not respond to his requests for a refund.

90. **Answer: A** Applications must be tested and baselined before they are rolled into production; otherwise, the results may be a lot worse than a few unhappy users; for example, a financial shortfall.
91. **Answer: D** White box testing would mean the evaluator has full knowledge of the environment. Red box and opaque are false options.
92. **Answer: C** Reconnaissance allows the attacker to collect information about a target, such as their IP address and location. The scanning phase is where the attacker enumerates the devices that have been found. Next, they need to see which devices are vulnerable. Finally, an ethical hacker will launch exploits without causing harm and report the findings to management.
93. **Answer: B** A high-level executive has complete knowledge of the environment and demonstrates the biggest risk as an internal threat to an organization. A black box test simulates an external attacker having no knowledge of the environment. A gray box test simulates some knowledge of the organization, such as an administrator or engineer. Red box is a false option.
94. **Answer: B and C** *Wireshark* and *Nessus* are tools that are used to discover vulnerabilities.
95. **Answer: B and C** SOC 1 reports focus on financial services and policies, such as proper accounting and bookkeeping standards. SOC 4 reports do not exist.
96. **Answer: A and B** Compliance audits are performed because an organization such as a power plant or brokerage firm needs to show they are following the regulations for their industry.
97. **Answer: A** In general, options B, C, and D are advantages of third-party audits.
98. **Answer: B** Safety first, even when conducting an audit.
99. **Answer: C** Regulations may not allow the audit to be redefined, and audits must be completed before they are certified.
100. **Answer: A** The eight-step process is 1) Determine goals, 2) Choose business unit(s), 3) Determine scope, 4) Select the audit team, 5) Audit planning, 6) Conduct the audit, 7) Document results, and 8) Communicate the results.

Chapter 6
Security Assessment and Testing (Domain 6)

1. During a port scan, Susan discovers a system running services on TCP and UDP 137-139 and TCP 445, as well as TCP 1433. What type of system is she likely to find if she connects to the machine?
    1. A Linux email server
    2. A Windows SQL server
    3. A Linux file server
    4. A Windows workstation
2. Which of the following is a method used to design new software tests and to ensure the quality of tests?
    1. Code auditing
    2. Static code analysis

    3. Regression testing
    4. Mutation testing
3. During a port scan, Lauren found TCP port 443 open on a system. Which tool is best suited to scanning the service that is most likely running on that port?
    1. zzuf
    2. Nikto
    3. Metasploit
    4. sqlmap
4. What message logging standard is commonly used by network devices, Linux and Unix systems, and many other enterprise devices?
    1. Syslog
    2. Netlog
    3. Eventlog
    4. Remote Log Protocol (RLP)
5. Alex wants to use an automated tool to fill web application forms to test for format string vulnerabilities. What type of tool should he use?
    1. A black box
    2. A brute-force tool
    3. A fuzzer
    4. A static analysis tool
6. Susan needs to scan a system for vulnerabilities, and she wants to use an open-source tool to test the system remotely. Which of the following tools will meet her requirements and allow vulnerability scanning?
    1. Nmap
    2. OpenVAS
    3. MBSA
    4. Nessus
7. NIST Special Publication 800-53A describes four major types of assessment objects that can be used to identify items being assessed. If the assessment covers IPS devices, which type of assessment objects is being assessed?
    1. A specification
    2. A mechanism
    3. An activity
    4. An individual
8. Jim has been contracted to perform a penetration test of a bank's primary branch. In order to make the test as real as possible, he has not been given any information about the bank other than its name and address. What type of penetration test has Jim agreed to perform?
    1. A crystal box penetration test
    2. A gray box penetration test
    3. A black box penetration test
    4. A white box penetration test
9. Alex is using nmap to perform port scanning of a system, and he receives three different port status messages in the results. Match each of the numbered status messages with the appropriate lettered description. You should use each item exactly once.

    Status message

1. Open
2. Closed
3. Filtered

Description

4. The port is accessible on the remote system, but no application is accepting connections on that port.
5. The port is not accessible on the remote system.
6. The port is accessible on the remote system, and an application is accepting connections on that port.

10. In a response to a Request for Proposal, Susan receives an SSAE 18 SOC 1 report. If she wants a report that includes operating effectiveness detail, what should Susan ask for as follow-up and why?
    1. A SOC 2 Type II report, because Type I does not cover operating effectiveness
    2. A SOC 1 Type I report, because SOC 2 does not cover operating effectiveness
    3. A SOC 2 Type I report, because SOC 2 Type II does not cover operating effectiveness
    4. A SOC 3 report, because SOC 1 and SOC 2 reports are outdated
11. During a wireless network penetration test, Susan runs aircrack-ng against the network using a password file. What might cause her to fail in her password-cracking efforts?
    1. Use of WPA2 encryption
    2. Running WPA2 in Enterprise mode
    3. Use of WEP encryption
    4. Running WPA2 in PSK mode
12. A zero-day vulnerability is announced for the popular Apache web server in the middle of a workday. In Jacob's role as an information security analyst, he needs to quickly scan his network to determine what servers are vulnerable to the issue. What is Jacob's best route to quickly identify vulnerable systems?
    1. Immediately run Nessus against all of the servers to identify which systems are vulnerable.
    2. Review the CVE database to find the vulnerability information and patch information.
    3. Create a custom IDS or IPS signature.
    4. Identify affected versions and check systems for that version number using an automated scanner.
13. What type of testing is used to ensure that separately developed software modules properly exchange data?
    1. Fuzzing
    2. Dynamic testing
    3. Interface testing
    4. API checksums
14. Which of the following is not a potential problem with active wireless scanning?
    1. Accidently scanning apparent rogue devices that actually belong to guests
    2. Causing alarms on the organization's wireless IPS
    3. Scanning devices that belong to nearby organizations

4. Misidentifying rogue devices

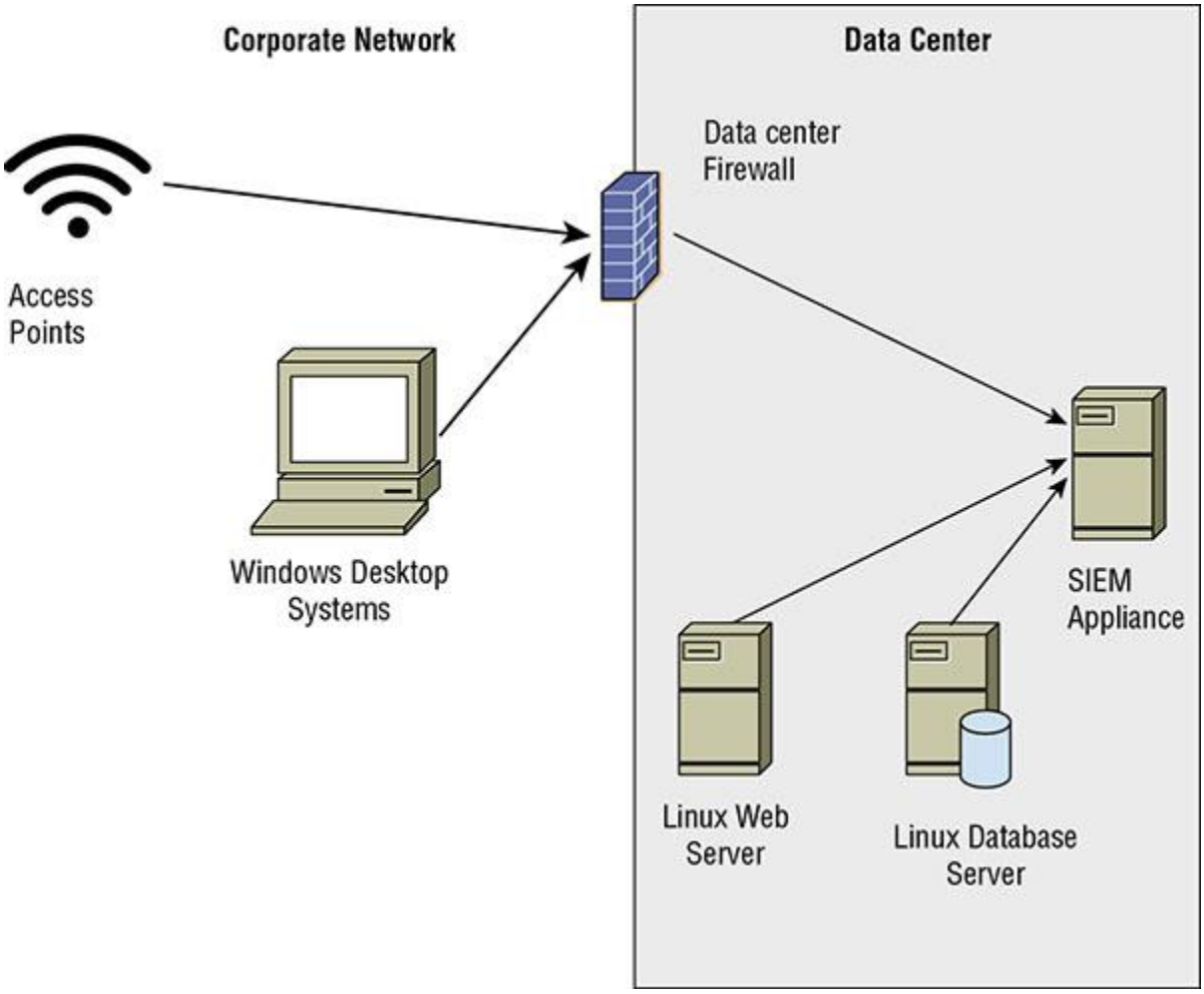
15. Ben uses a fuzzing tool that tests an application by developing data models and creating fuzzed data based on information about how the application uses data. What type of fuzzing is Ben doing?
    1. Mutation
    2. Parametric
    3. Generational
    4. Derivative
16. Saria wants to log and review traffic information between parts of her network. What type of network logging should she enable on her routers to allow her to perform this analysis?
    1. Audit logging
    2. Flow logging
    3. Trace logging
    4. Route logging
17. Jim has been contracted to conduct a gray box penetration test, and his clients have provided him with the following information about their networks so that he can scan them:
    - Data center: 10.10.10.0/24
    - Sales: 10.10.11.0/24
    - Billing: 10.10.12.0/24
    - Wireless: 192.168.0.0/16

    What problem will Jim encounter if he is contracted to conduct a scan from offsite?

    5. The IP ranges are too large to scan efficiently.
    6. The IP addresses provided cannot be scanned.
    7. The IP ranges overlap and will cause scanning issues.
    8. The IP addresses provided are RFC 1918 addresses.
18. Karen's organization has been performing system backups for years but has not used the backups frequently. During a recent system outage, when administrators tried to restore from backups, they found that the backups had errors and could not be restored. Which of the following options should Karen avoid when selecting ways to ensure that her organization's backups will work next time?
    0. Log review
    1. MTD verification
    2. Hashing
    3. Periodic testing

    For questions 19–21, please refer to the following scenario:

    The company that Jennifer works for has implemented a central logging infrastructure, as shown in the following image. Use this diagram and your knowledge of logging systems to answer the following questions.



19. Jennifer needs to ensure that all Windows systems provide identical logging information to the SIEM. How can she best ensure that all Windows desktops have the same log settings?
    0. Perform periodic configuration audits.
    1. Use Group Policy.
    2. Use Local Policy.
    3. Deploy a Windows syslog client.
20. During normal operations, Jennifer's team uses the SIEM appliance to monitor for exceptions received via syslog. What system shown does not natively have support for syslog events?
    0. Enterprise wireless access points
    1. Windows desktop systems
    2. Linux web servers
    3. Enterprise firewall devices
21. What technology should an organization use for each of the devices shown in the diagram to ensure that logs can be time sequenced across the entire infrastructure?
    0. Syslog
    1. NTP
    2. Logsync

3. SNAP

22. During a penetration test, Danielle needs to identify systems, but she hasn't gained sufficient access on the system she is using to generate raw packets. What type of scan should she run to verify the most open services?
    0. A TCP connect scan
    1. A TCP SYN scan
    2. A UDP scan
    3. An ICMP scan
23. During a port scan using nmap, Joseph discovers that a system shows two ports open that cause him immediate worry:
    - 21/open
    - 23/open

    What services are likely running on those ports?

    2. SSH and FTP
    3. FTP and Telnet
    4. SMTP and Telnet
    5. POP3 and SMTP
24. Saria's team is working to persuade their management that their network has extensive vulnerabilities that attackers could exploit. If she wants to conduct a realistic attack as part of a penetration test, what type of penetration test should she conduct?
    0. Crystal box
    1. Gray box
    2. White box
    3. Black box
25. What method is commonly used to assess how well software testing covered the potential uses of an application?
    0. A test coverage analysis
    1. A source code review
    2. A fuzz analysis
    3. A code review report
26. Testing that is focused on functions that a system should not allow are an example of what type of testing?
    0. Use case testing
    1. Manual testing
    2. Misuse case testing
    3. Dynamic testing
27. What type of monitoring uses simulated traffic to a website to monitor performance?
    0. Log analysis
    1. Synthetic monitoring
    2. Passive monitoring
    3. Simulated transaction analysis
28. Which of the following vulnerabilities is unlikely to be found by a web vulnerability scanner?
    0. Path disclosure

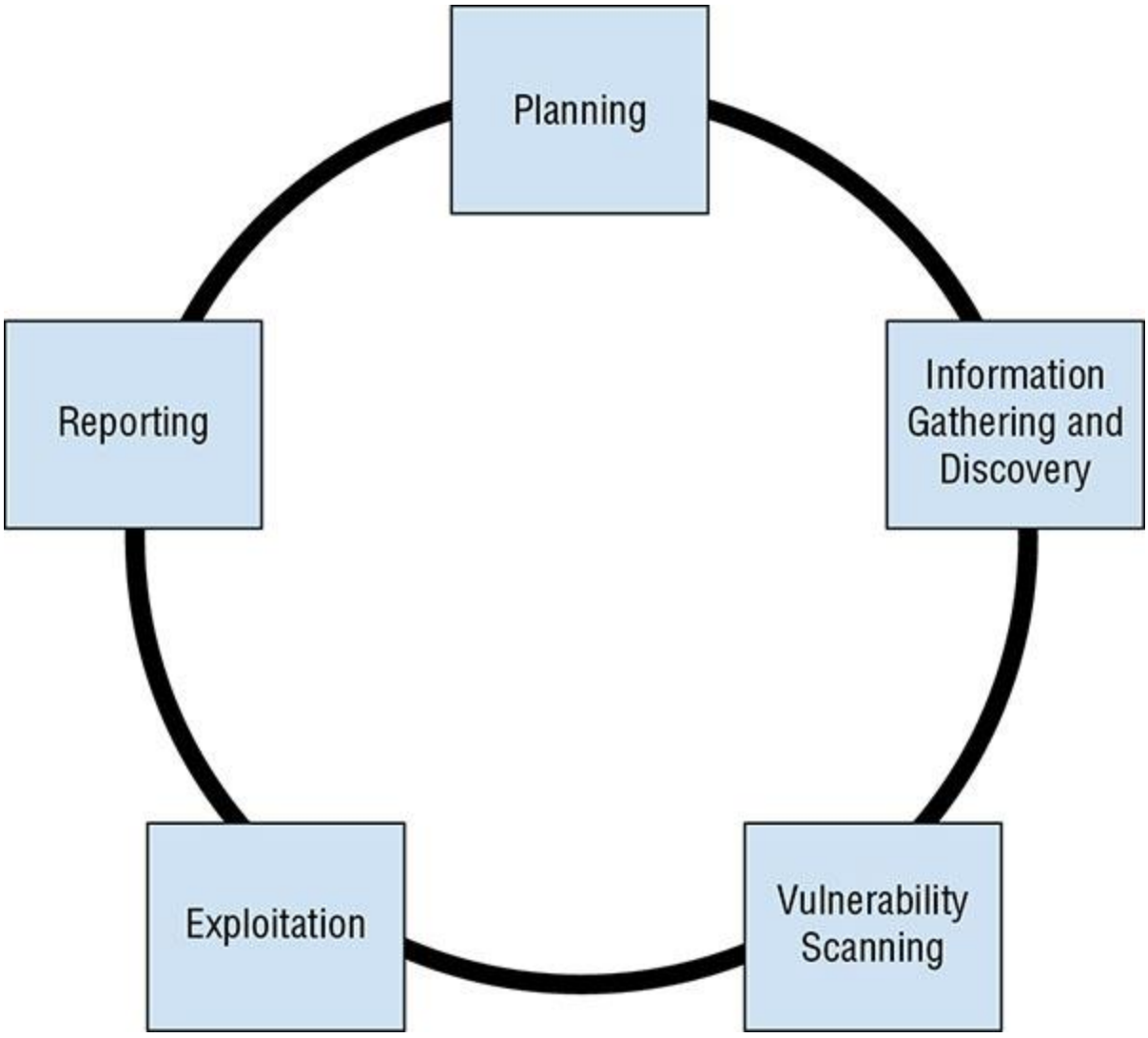
1. Local file inclusion
2. Race condition
3. Buffer overflow

29. Jim uses a tool that scans a system for available services and then connects to them to collect banner information to determine what version of the service is running. It then provides a report detailing what it gathers, basing results on service fingerprinting, banner information, and similar details it gathers combined with CVE information. What type of tool is Jim using?
    0. A port scanner
    1. A service validator
    2. A vulnerability scanner
    3. A patch management tool
30. Emily builds a script that sends data to a web application that she is testing. Each time the script runs, it sends a series of transactions with data that fits the expected requirements of the web application to verify that it responds to typical customer behavior. What type of transactions is she using, and what type of test is this?
    0. Synthetic, passive monitoring
    1. Synthetic, use case testing
    2. Actual, dynamic monitoring
    3. Actual, fuzzing
31. What passive monitoring technique records all user interaction with an application or website to ensure quality and performance?
    0. Client/server testing
    1. Real user monitoring
    2. Synthetic user monitoring
    3. Passive user recording
32. Earlier this year, the information security team at Jim's employer identified a vulnerability in the web server that Jim is responsible for maintaining. He immediately applied the patch and is sure that it installed properly, but the vulnerability scanner has continued to incorrectly flag the system as vulnerable due to the version number it is finding even though Jim is sure the patch is installed. Which of the following options is Jim's best choice to deal with the issue?
    0. Uninstall and reinstall the patch.
    1. Ask the information security team to flag the system as patched and not vulnerable.
    2. Update the version information in the web server's configuration.
    3. Review the vulnerability report and use alternate remediation options.
33. Angela wants to test a web browser's handling of unexpected data using an automated tool. What tool should she choose?
    0. Nmap
    1. zzuf
    2. Nessus
    3. Nikto
34. STRIDE, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, is useful in what part of application threat modeling?

0. Vulnerability assessment
1. Misuse case testing
2. Threat categorization
3. Penetration test planning

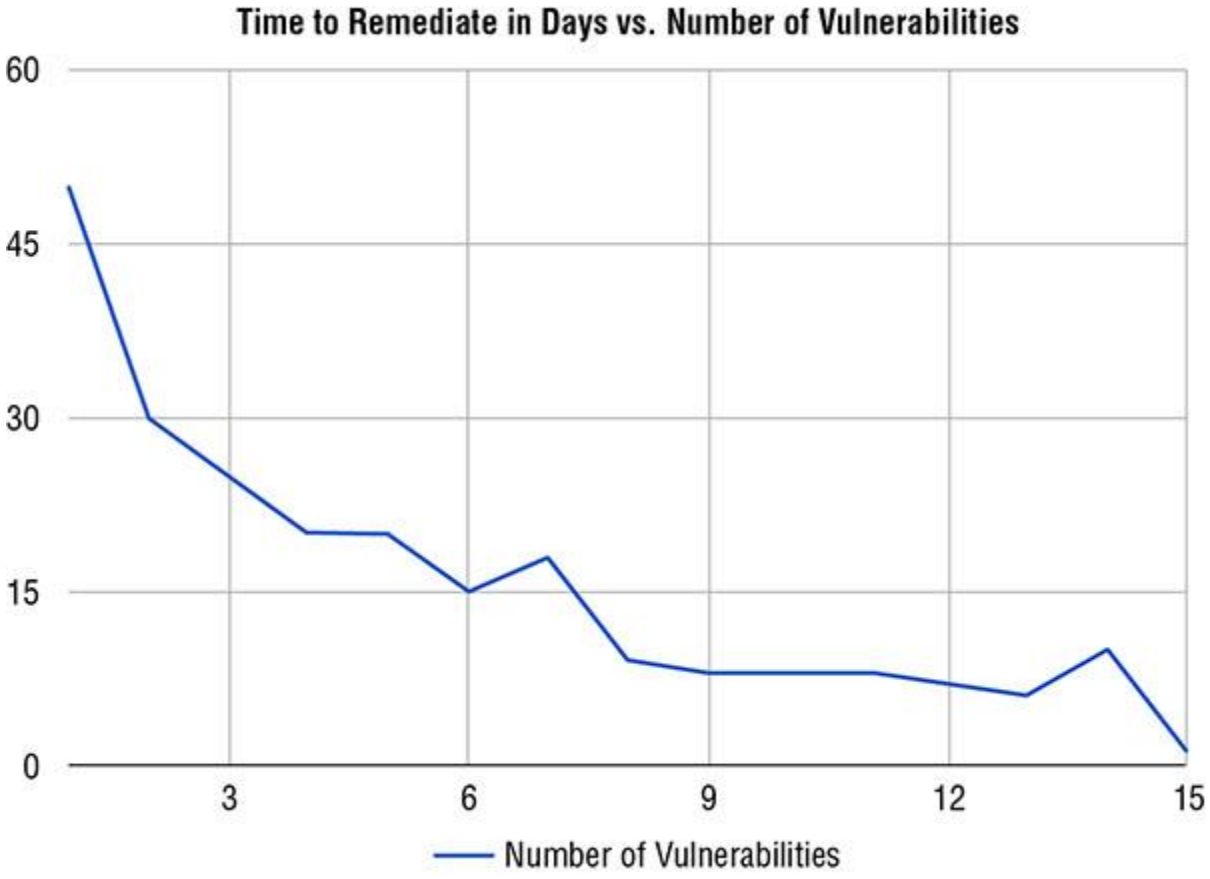
35. Why should passive scanning be conducted in addition to implementing wireless security technologies like wireless intrusion detection systems?
    0. It can help identify rogue devices.
    1. It can test the security of the wireless network via scripted attacks.
    2. Their short dwell time on each wireless channel can allow them to capture more packets.
    3. They can help test wireless IDS or IPS systems.
36. During a penetration test, Lauren is asked to test the organization's Bluetooth security. Which of the following is not a concern she should explain to her employers?
    0. Bluetooth scanning can be time-consuming.
    1. Many devices that may be scanned are likely to be personal devices.
    2. Bluetooth passive scans may require multiple visits at different times to identify all targets.
    3. Bluetooth active scans can't evaluate the security mode of Bluetooth devices.
37. What term describes software testing that is intended to uncover new bugs introduced by patches or configuration changes?
    0. Nonregression testing
    1. Evolution testing
    2. Smoke testing
    3. Regression testing
38. Which of the tools cannot identify a target's operating system for a penetration tester?
    0. Nmap
    1. Nessus
    2. Nikto
    3. sqlmap
39. Susan needs to predict high-risk areas for her organization and wants to use metrics to assess risk trends as they occur. What should she do to handle this?
    0. Perform yearly risk assessments.
    1. Hire a penetration testing company to regularly test organizational security.
    2. Identify and track key risk indicators.
    3. Monitor logs and events using a SIEM device.
40. What major difference separates synthetic and passive monitoring?
    0. Synthetic monitoring only works after problems have occurred.
    1. Passive monitoring cannot detect functionality issues.
    2. Passive monitoring only works after problems have occurred.
    3. Synthetic monitoring cannot detect functionality issues.

For questions 41–43, please refer to the following scenario. Chris uses the standard penetration testing methodology shown here. Use this methodology and your knowledge of penetration testing to answer questions about tool usage during a penetration test.



41. What task is the most important during Phase 1, Planning?
    0. Building a test lab
    1. Getting authorization
    2. Gathering appropriate tools
    3. Determining if the test is white, black, or gray box
42. Which of the following tools is most likely to be used during discovery?
    0. Nessus
    1. john
    2. Nmap
    3. Nikto
43. Which of these concerns is the most important to address during planning to ensure that the reporting phase does not cause problems?
    0. Which CVE format to use
    1. How the vulnerability data will be stored and sent
    2. Which targets are off-limits
    3. How long the report should be

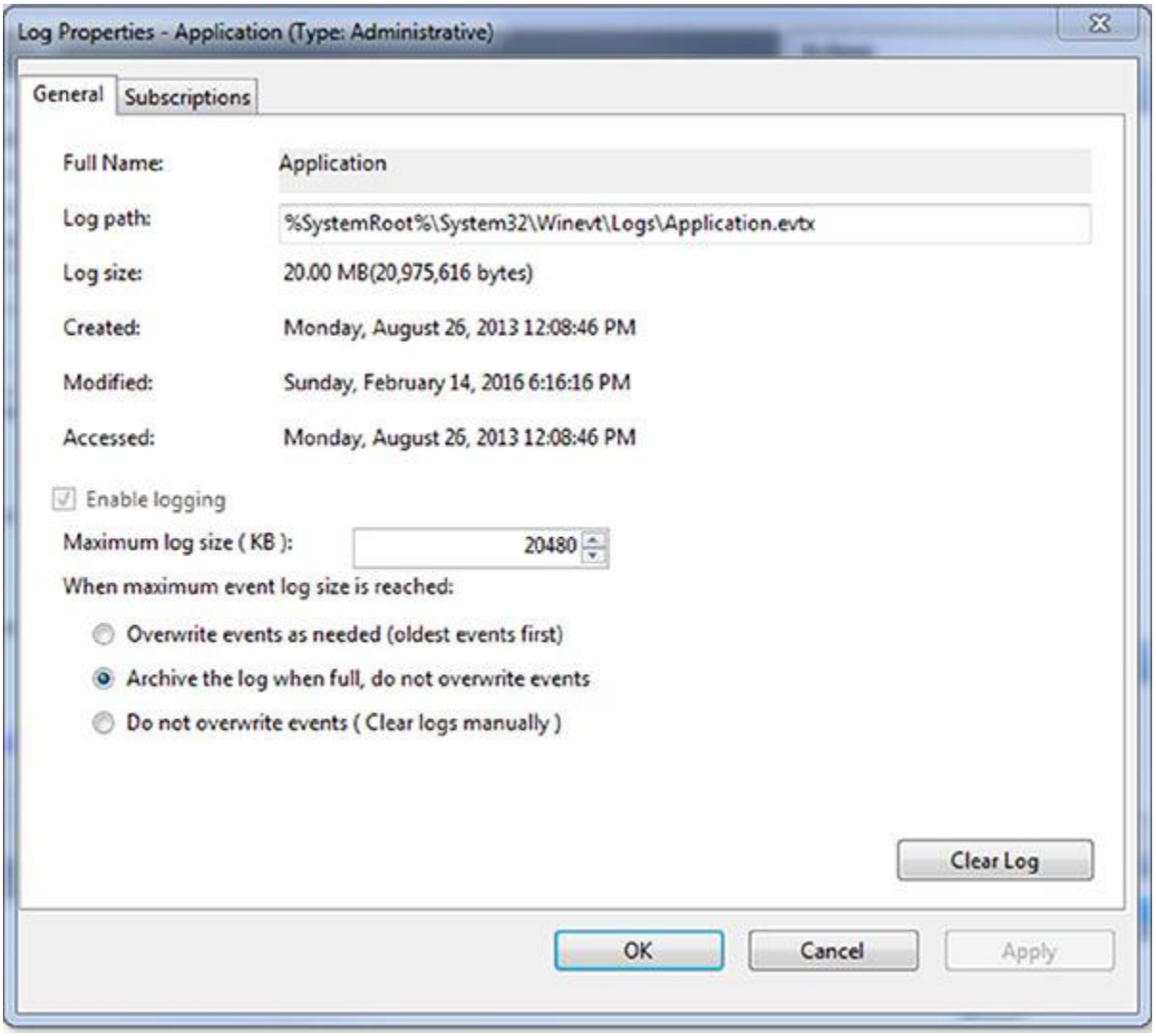
44. What four types of coverage criteria are commonly used when validating the work of a code testing suite?
    0. Input, statement, branch, and condition coverage
    1. Function, statement, branch, and condition coverage
    2. API, branch, bounds, and condition coverage
    3. Bounds, branch, loop, and condition coverage
45. As part of his role as a security manager, Jacob provides the following chart to his organization's management team. What type of measurement is he providing for them?



    0. A coverage rate measure
    1. A key performance indicator
    2. A time to live metric
    3. A business criticality indicator
46. What does using unique user IDs for all users provide when reviewing logs?
    0. Confidentiality
    1. Integrity
    2. Availability
    3. Accountability
47. Which of the following is not an interface that is typically tested during the software testing process?
    0. APIs
    1. Network interfaces

2. UIs
3. Physical interfaces

48. Alan’s organization uses the Security Content Automation Protocol (SCAP) to standardize its vulnerability management program. Which component of SCAP can Alan use to reconcile the identity of vulnerabilities generated by different security assessment tools?
    0. OVAL
    1. XCCDF
    2. CVE
    3. SCE
49. Misconfiguration, logical and functional flaws, and poor programming practices are all causes of what common security issue?
    0. Fuzzing
    1. Security vulnerabilities
    2. Buffer overflows
    3. Race conditions
50. Which of the following strategies is not a reasonable approach for remediating a vulnerability identified by a vulnerability scanner?
    0. Install a patch.
    1. Use a workaround fix.
    2. Update the banner or version number.
    3. Use an application layer firewall or IPS to prevent attacks against the identified vulnerability.
51. During a penetration test Saria calls her target’s help desk claiming to be the senior assistant to an officer of the company. She requests that the help desk reset the officer’s password because of an issue with his laptop while traveling and persuades them to do so. What type of attack has she successfully completed?
    0. Zero knowledge
    1. Help desk spoofing
    2. Social engineering
    3. Black box
52. In this image, what issue may occur due to the log handling settings?



0. Log data may be lost when the log is archived.
1. Log data may be overwritten.
2. Log data may not include needed information.
3. Log data may fill the system disk.

53. Which of the following is not a hazard associated with penetration testing?
    0. Application crashes
    1. Denial of service
    2. Exploitation of vulnerabilities
    3. Data corruption
54. Which NIST special publication covers the assessment of security and privacy controls?
    0. 800-12
    1. 800-53A
    2. 800-34
    3. 800-86
55. Match each of the numbered scanning types with the appropriate lettered description shown. You should use each item exactly once.

Scanning types

0. TCP Connect
1. TCP ACK
2. TCP SYN
3. Xmas

Scanning descriptions

4. Sends a request to open a new connection
5. Completes a three-way handshake
6. Sends a packet disguised as part of an active control
7. Sends a packet with the FIN, PSH, and URG flags set

Kara used nmap to perform a scan of a system under her control and received the results shown here. Refer to these results to answer questions 56 and 57.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-08 15:08 EST
Nmap scan report for myhost (192.168.107.9)
Host is up (0.033s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```

56. If Kara's primary concern is preventing eavesdropping attacks, which port should she block?
    0. 22
    1. 80
    2. 443
    3. 1433
57. If Kara's primary concern is preventing administrative connections to the server, which port should she block?
    0. 22
    1. 80
    2. 443
    3. 1433
58. During a third-party audit, Jim's company receives a finding that states, "The administrator should review backup success and failure logs on a daily basis, and take action in a timely manner to resolve reported exceptions." What is the biggest issue that is likely to result if Jim's IT staff need to restore from a backup?
    0. They will not know if the backups succeeded or failed.
    1. The backups may not be properly logged.
    2. The backups may not be usable.
    3. The backup logs may not be properly reviewed.

59. Jim is helping his organization decide on audit standards for use throughout their international organization. Which of the following is not an IT standard that Jim's organization is likely to use as part of its audits?
    0. COBIT
    1. SSAE-18
    2. ITIL
    3. ISO 27002
60. Which of the following best describes a typical process for building and implementing an Information Security Continuous Monitoring program as described by NIST Special Publication 800-137?
    0. Define, establish, implement, analyze and report, respond, review, and update
    1. Design, build, operate, analyze, respond, review, revise
    2. Prepare, detect and analyze, contain, respond, recover, report
    3. Define, design, build, monitor, analyze, react, revise
61. Lauren's team conducts regression testing on each patch that they release. What key performance measure should they maintain to measure the effectiveness of their testing?
    0. Time to remediate vulnerabilities
    1. A measure of the rate of defect recurrence
    2. A weighted risk trend
    3. A measure of the specific coverage of their testing
62. Which of the following types of code review is not typically performed by a human?
    0. Software inspections
    1. Code review
    2. Static program analysis
    3. Software walkthroughs

    For questions 63–65, please refer to the following scenario:

    Susan is the lead of a Quality Assurance team at her company. The team has been tasked with the testing for a major release of their company's core software product.

63. Susan's team of software testers are required to test every code path, including those that will only be used when an error condition occurs. What type of testing environment does her team need to ensure complete code coverage?
    0. White box
    1. Gray box
    2. Black box
    3. Dynamic
64. As part of the continued testing of their new application, Susan's quality assurance team has designed a set of test cases for a series of black box tests. These functional tests are then run, and a report is prepared explaining what has occurred. What type of report is typically generated during this testing to indicate test metrics?
    0. A test coverage report
    1. A penetration test report
    2. A code coverage report

3. A line coverage report

65. As part of their code coverage testing, Susan's team runs the analysis in a nonproduction environment using logging and tracing tools. Which of the following types of code issues is most likely to be missed during testing due to this change in the operating environment?
    0. Improper bounds checking
    1. Input validation
    2. A race condition
    3. Pointer manipulation
66. Robin recently conducted a vulnerability scan and found a critical vulnerability on a server that handles sensitive information. What should Robin do next?
    0. Patching
    1. Reporting
    2. Remediation
    3. Validation
67. Kathleen is reviewing the code for an application. She first plans the review, conducts an overview session with the reviewers and assigns roles, and then works with the reviewers to review materials and prepare for their roles. Next, she intends to review the code, rework it, and ensure that all defects found have been corrected. What type of review is Kathleen conducting?
    0. A dynamic test
    1. Fagan inspection
    2. Fuzzing
    3. A Roth-Parker review
68. Danielle wants to compare vulnerabilities she has discovered in her data center based on how exploitable they are, if exploit code exists, and how hard they are to remediate. What scoring system should she use to compare vulnerability metrics like these?
    0. CSV
    1. NVD
    2. VSS
    3. CVSS
69. During a port scan of his network, Alex finds that a number of hosts respond on TCP ports 80, 443, 515, and 9100 in offices throughout his organization. What type of devices is Alex likely discovering?
    0. Web servers
    1. File servers
    2. Wireless access points
    3. Printers
70. Nikto, Burp Suite, and Wapiti are all examples of what type of tool?
    0. Web application vulnerability scanners
    1. Code review tools
    2. Vulnerability scanners
    3. Port scanners
71. Place the following elements of a Fagan inspection code review in the correct order.
    0. Follow-up
    1. Inspection

2. Overview
3. Planning
4. Preparation
5. Rework

72. Jim is working with a penetration testing contractor who proposes using Metasploit as part of her penetration testing effort. What should Jim expect to occur when Metasploit is used?
    0. Systems will be scanned for vulnerabilities.
    1. Systems will have known vulnerabilities exploited.
    2. Services will be probed for buffer overflow and other unknown flaws.
    3. Systems will be tested for zero-day exploits.
73. Susan needs to ensure that the interactions between the components of her e-commerce application are all handled properly. She intends to verify communications, error handling, and session management capabilities throughout her infrastructure. What type of testing is she planning to conduct?
    0. Misuse case testing
    1. Fuzzing
    2. Regression testing
    3. Interface testing
74. Jim is designing his organization's log management systems and knows that he needs to carefully plan to handle the organization's log data. Which of the following is not a factor that Jim should be concerned with?
    0. The volume of log data
    1. A lack of sufficient log sources
    2. Data storage security requirements
    3. Network bandwidth
75. Ken is having difficulty correlating information from different security teams in his organization. Specifically, he would like to find a way to describe operating systems in a consistent fashion. What SCAP component can assist him?
    0. CVE
    1. CPE
    2. CWE
    3. OVAL
76. When a Windows system is rebooted, what type of log is generated?
    0. Error
    1. Warning
    2. Information
    3. Failure audit
77. During a review of access logs, Alex notices that Danielle logged into her workstation in New York at 8 a.m. daily but that she was recorded as logging into her department's main web application shortly after 3 a.m. daily. What common logging issue has Alex likely encountered?
    0. Inconsistent log formatting
    1. Modified logs
    2. Inconsistent timestamps
    3. Multiple log sources

78. What type of vulnerability scan accesses configuration information from the systems it is run against as well as information that can be accessed via services available via the network?
    0. Authenticated scans
    1. Web application scans
    2. Unauthenticated scans
    3. Port scans

    For questions 79–81, please refer to the following scenario:

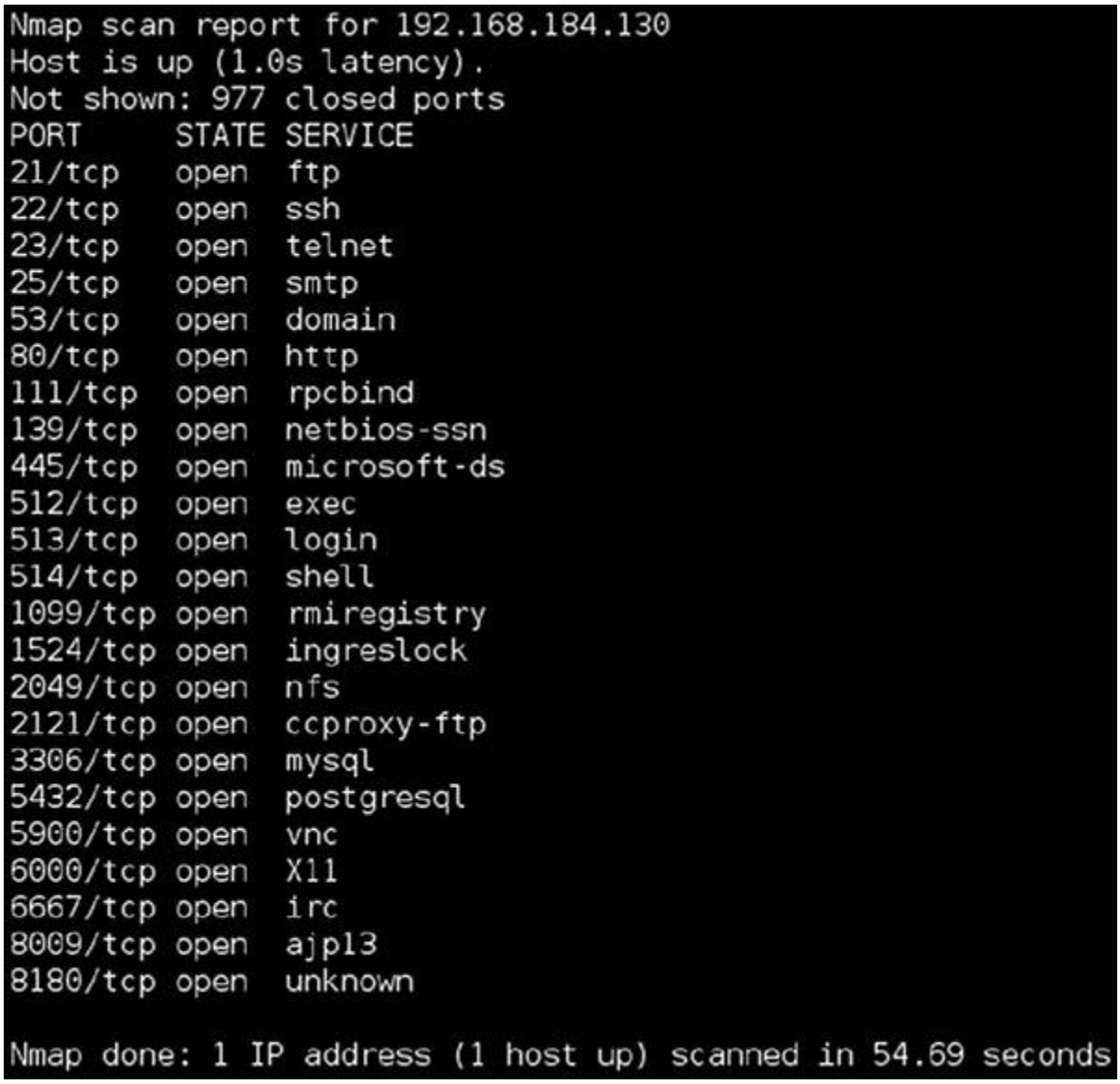
    Ben's organization has begun to use STRIDE to assess its software and has identified threat agents and the business impacts that these threats could have. Now they are working to identify appropriate controls for the issues they have identified.

79. Ben's development team needs to address an authorization issue, resulting in an elevation of privilege threat. Which of the following controls is most appropriate to this type of issue?
    0. Auditing and logging is enabled.
    1. Role-based access control is used for specific operations.
    2. Data type and format checks are enabled.
    3. User input is tested against a whitelist.
80. Ben's team is attempting to categorize a transaction identification issue that is caused by use of a symmetric key shared by multiple servers. What STRIDE category should this fall into?
    0. Information disclosure
    1. Denial of service
    2. Tampering
    3. Repudiation
81. Ben wants to prevent or detect tampering with data. Which of the following is not an appropriate solution?
    0. Hashes
    1. Digital signatures
    2. Filtering
    3. Authorization controls
82. Chris is troubleshooting an issue with his organization's SIEM reporting. After analyzing the issue, he believes that the timestamps on log entries from different systems are inconsistent. What protocol can he use to resolve this issue?
    0. SSH
    1. FTP
    2. TLS
    3. NTP
83. Ryan is considering the use of fuzz testing in his web application testing program. Which one of the following limitations of fuzz testing should Ryan consider when making his decision?
    0. They often find only simple faults.

1. Testers must manually generate input.
2. Fuzzers may not fully cover the code.
3. Fuzzers can't reproduce errors.

84. Ken is designing a testing process for software developed by his team. He is designing a test that verifies that every line of code was executed during the test. What type of analysis is Ken performing?
    0. Branch coverage
    1. Condition coverage
    2. Function coverage
    3. Statement coverage

For questions 85–87, please refer to the following scenario. During a port scan, Ben uses nmap's default settings and sees the following results.



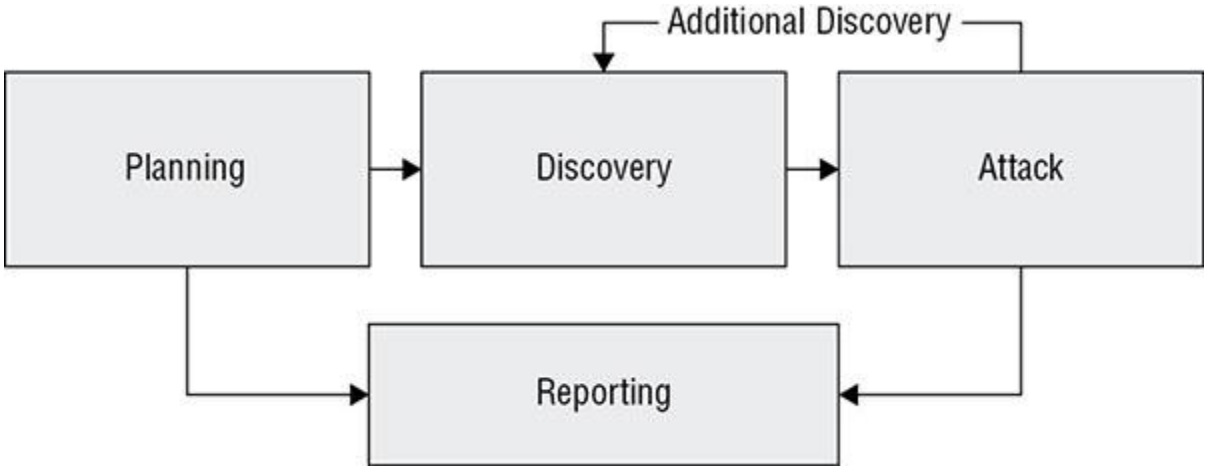
```
Nmap scan report for 192.168.184.130
Host is up (1.0s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 54.69 seconds
```

85. If Ben is conducting a penetration test, what should his next step be after receiving these results?
    0. Connect to the web server using a web browser.
    1. Connect via Telnet to test for vulnerable accounts.
    2. Identify interesting ports for further scanning.
    3. Use sqlmap against the open databases.
86. Based on the scan results, what operating system (OS) was the system that was scanned most likely running?
    0. Windows Desktop
    1. Linux
    2. Network device
    3. Windows Server
87. Ben's manager expresses concern about the coverage of his scan. Why might his manager have this concern?
    0. Ben did not test UDP services.
    1. Ben did not discover ports outside the "well-known ports."
    2. Ben did not perform OS fingerprinting.
    3. Ben tested only a limited number of ports.
88. What technique relies on reviewing code without running it?
    0. Fuzzing
    1. Black box analysis
    2. Static analysis
    3. Gray box analysis
89. Saria needs to write a request for proposal for code review and wants to ensure that the reviewers take the business logic behind her organization's applications into account. What type of code review should she specify in the RFP?
    0. Static
    1. Fuzzing
    2. Manual
    3. Dynamic
90. What type of diagram used in application threat modeling includes malicious users as well as descriptions like *mitigates* and *threatens*?
    0. Threat trees
    1. STRIDE charts
    2. Misuse case diagrams
    3. DREAD diagrams
91. What is the first step that should occur before a penetration test is performed?
    0. Data gathering
    1. Port scanning
    2. Getting permission
    3. Planning
92. Kevin is a database administrator and would like to use a tool designed to test the security of his databases. Which one of the following tools is best suited for this purpose?
    0. sqlmap
    1. nmap
    2. sqlthrash

3. Nessus

93. During a penetration test of her organization, Kathleen's IPS detects a port scan that has the URG, FIN, and PSH flags set and produces an alarm. What type of scan is the penetration tester attempting?
    0. A SYN scan
    1. A TCP flag scan
    2. An Xmas scan
    3. An ACK scan
94. Nmap is an example of what type of tool?
    0. Vulnerability scanner
    1. Web application fuzzer
    2. Network design and layout
    3. Port scanner
95. What type of vulnerabilities will not be found by a vulnerability scanner?
    0. Local vulnerabilities
    1. Service vulnerabilities
    2. Zero-day vulnerabilities
    3. Vulnerabilities that require authentication
96. MITRE's CVE database provides what type of information?
    0. Current versions of software
    1. Patching information for applications
    2. Vulnerability information
    3. A list of costs versus effort required for common processes
97. When designing an assessment following NIST SP 800-53A, which assessment component includes policies and procedures?
    0. Specifications
    1. Mechanisms
    2. Activities
    3. Individuals

For questions 98–100, please refer to the following scenario. NIST Special Publication 800-115, the Technical Guide to Information Security Testing and Assessment, provides NIST's process for penetration testing. Use this image as well as your knowledge of penetration testing to answer the questions.



Source: NIST SP 800-115.

98. Which of the following is not a part of the discovery phase?
    0. Hostname and IP address information gathering
    1. Service information capture
    2. Dumpster diving
    3. Privilege escalation
99. NIST specifies four attack phase steps: gaining access, escalating privileges, system browsing, and installing additional tools. Once attackers install additional tools, what phase will a penetration tester typically return to?
    0. Discovery
    1. Gaining access
    2. Escalating privileges
    3. System browsing
100. Which of the following is not a typical part of a penetration test report?
    0. A list of identified vulnerabilities
    1. All sensitive data that was gathered during the test
    2. Risk ratings for each issue discovered
    3. Mitigation guidance for issues identified

Chapter 6: Security Assessment and Testing (Domain 6)

1. B. TCP and UDP ports 137–139 are used for NetBIOS services, whereas 445 is used for Active Directory. TCP 1433 is the default port for Microsoft SQL, indicating that this is probably a Windows server providing SQL services.
2. D. Mutation testing modifies a program in small ways and then tests that mutant to determine if it behaves as it should or if it fails. This technique is used to design and test software tests through mutation. Static code analysis and regression testing are both means of testing code, whereas code auditing is an analysis of source code rather than a means of designing and testing software tests.
3. B. TCP port 443 normally indicates an HTTPS server. Nikto is useful for vulnerability scanning web servers and applications and is the best choice listed for a web server. Metasploit includes some scanning functionality but is not a purpose-built tool for vulnerability scanning. zzuf is a

fuzzing tool and isn't relevant for vulnerability scans, whereas sqlmap is a SQL injection testing tool.

4. A. Syslog is a widely used protocol for event and message logging. *Eventlog*, *netlog*, and *Remote Log Protocol* are all made-up terms.
5. C. Fuzzers are tools that are designed to provide invalid or unexpected input to applications, testing for vulnerabilities like format string vulnerabilities, buffer overflow issues, and other problems. A static analysis relies on examining code without running the application or code and thus would not fill forms as part of a web application. Brute-force tools attempt to bypass security by trying every possible combination for passwords or other values. A black box is a type of penetration test where the testers do not know anything about the environment.
6. B. OpenVAS is an open-source vulnerability scanning tool that will provide Susan with a report of the vulnerabilities that it can identify from a remote, network-based scan. Nmap is an open-source port scanner. Both the Microsoft Baseline Security Analyzer (MBSA) and Nessus are closed-source tools, although Nessus was originally open source.
7. B. An IPS is an example of a mechanism like a hardware-, software-, or firmware-based control or system. Specifications are document-based artifacts like policies or designs, activities are actions that support an information system that involves people, and an individual is one or more people applying specifications, mechanisms, or activities.
8. C. Jim has agreed to a black box penetration test, which provides no information about the organization, its systems, or its defenses. A crystal or white box penetration test provides all of the information an attacker needs, whereas a gray box penetration test provides some, but not all, information.
9. The status messages match with the descriptions as follows:
    1. Open: C. The port is accessible on the remote system and an application is accepting connections on that port.
    2. Closed: A. The port is accessible on the remote system, but no application is accepting connections on that port.
    3. Filtered: B. The port is not accessible on the remote system.
10. A. The key to answering this question correctly is understanding the difference between Type I and Type II audits. Type I audits only cover a single point in time and are based upon management descriptions of controls. They do not include an assessment of operating effectiveness. Type II audits cover a period of time and do include an assessment of operating effectiveness.
11. B. WPA2 enterprise uses RADIUS authentication for users rather than a preshared key. This means a password attack is more likely to fail as password attempts for a given user may result in account lockout. WPA2 encryption will not stop a password attack, and WPA2's preshared key mode is specifically targeted by password attacks that attempt to find the key. Not only is WEP encryption outdated, but it can also frequently be cracked quickly by tools like aircrack-ng.
12. D. In many cases when an exploit is initially reported, there are no prebuilt signatures or detections for vulnerability scanners, and the CVE database may not immediately have information about the attack. Jacob's best option is to quickly gather information and review potentially vulnerable servers based on their current configuration. As more information becomes available, signatures and CVE information are likely to be published. Unfortunately for Jacob, IDS and IPS signatures will only detect attacks and won't detect whether systems are vulnerable unless he sees the systems being exploited.
13. C. Interface testing is used to ensure that software modules properly meet interface specifications and thus will properly exchange data. Dynamic testing tests software in a running

environment, whereas fuzzing is a type of dynamic testing that feeds invalid input to running software to test error and input handling. API checksums are not a testing technique.

14. B. Not only should active scanning be expected to cause wireless IPS alarms, but they may actually be desired if the test is done to test responses. Accidentally scanning guests or neighbors or misidentifying devices belonging to third parties are all potential problems with active scanning and require the security assessor to carefully verify the systems that she is scanning.
15. C. Generational fuzzing relies on models for application input and conducts fuzzing attacks based on that information. Mutation-based fuzzers are sometimes called "dumb" fuzzers because they simply mutate or modify existing data samples to create new test samples. Neither *parametric* nor *derivative* is a term used to describe types of fuzzers.
16. B. Flows, also often called network flows, are captured to provide insight into network traffic for security, troubleshooting, and performance management. Audit logging provides information about events on the routers, route logging is not a common network logging function, and trace logs are used in troubleshooting specific software packages as they perform their functions.
17. D. The IP addresses that his clients have provided are RFC 1918 nonroutable IP addresses, and Jim will not be able to scan them from offsite. To succeed in his penetration test, he will have to either first penetrate their network border or place a machine inside their network to scan from the inside. IP addresses overlapping is not a real concern for scanning, and the ranges can easily be handled by current scanning systems.
18. B. Karen can't use MTD verification because MTD is the Maximum Tolerable Downtime. Verifying it will only tell her how long systems can be offline without significant business impact. Reviewing logs, using hashing to verify that the logs are intact, and performing periodic tests are all valid ways to verify that the backups are working properly.
19. B. Group Policy enforced by Active Directory can ensure consistent logging settings and can provide regular enforcement of policy on systems. Periodic configuration audits won't catch changes made between audits, and local policies can drift due to local changes or differences in deployments. A Windows syslog client will enable the Windows systems to send syslog to the SIEM appliance but won't ensure consistent logging of events.
20. B. Windows systems generate logs in the Windows native logging format. To send syslog events, Windows systems require a helper application or tool. Enterprise wireless access points, firewalls, and Linux systems all typically support syslog.
21. B. Network Time Protocol (NTP) can ensure that systems are using the same time, allowing time sequencing for logs throughout a centralized logging infrastructure. Syslog is a way for systems to send logs to a logging server and won't address time sequencing. Neither *logsync* nor *SNAP* is an industry term.
22. A. When a tester does not have raw packet creation privileges, such as when they have not escalated privileges on a compromised host, a TCP connect scan can be used. TCP SYN scans require elevated privileges on most Linux systems due to the need to write raw packets. A UDP scan will miss most services that are provided via TCP, and an ICMP is merely a ping sweep of systems that respond to pings and won't identify services at all.
23. B. Joseph may be surprised to discover FTP (TCP port 21) and Telnet (TCP port 23) open on his network since both services are unencrypted and have been largely replaced by SSH, and SCP or SFTP. SSH uses port 22, SMTP uses port 25, and POP3 uses port 110.
24. D. Black box testing is the most realistic type of penetration test because it does not provide the penetration tester with inside information about the configuration or design of systems, software, or networks. A gray box test provides some information, whereas a white or crystal box test provides significant or full detail.

25. A. A test coverage analysis is often used to provide insight into how well testing covered the set of use cases that an application is being tested for. Source code reviews look at the code of a program for bugs, not necessarily at a use case analysis, whereas fuzzing tests invalid inputs. A code review report might be generated as part of a source code review.
26. C. Testing how a system could be misused, or misuse testing, focuses on behaviors that are not what the organization desires or that are counter to the proper function of a system or application. Use case testing is used to verify whether a desired functionality works. Dynamic testing is used to determine how code handles variables that change over time, whereas manual testing is just what it implies: testing code by hand.
27. B. Synthetic monitoring uses emulated or recorded transactions to monitor for performance changes in response time, functionality, or other performance monitors. Passive monitoring uses a span port or other method to copy traffic and monitor it in real time. Log analysis is typically performed against actual log data but can be performed on simulated traffic to identify issues. *Simulated transaction analysis* is not an industry term.
28. C. Path disclosures, local file inclusions, and buffer overflows are all vulnerabilities that may be found by a web vulnerability scanner, but race conditions that take advantage of timing issues tend to be found either by code analysis or using automated tools that specifically test for race conditions as part of software testing.
29. C. Vulnerability scanners that do not have administrative rights to access a machine or that are not using an agent scan remote machines to gather information, including fingerprints from responses to queries and connections, banner information from services, and related data. CVE information is Common Vulnerability and Exposure information, or vulnerability information. A port scanner gathers information about what service ports are open, although some port scanners blur the line between port and vulnerability scanners. Patch management tools typically run as an agent on a system to allow them to both monitor patch levels and update the system as needed. Service validation typically involves testing the functionality of a service, not its banner and response patterns.
30. B. Emily is using synthetic transactions, which can use recorded or generated transactions, and is conducting use case testing to verify that the application responds properly to actual use cases. Neither *actual data* nor *dynamic monitoring* is an industry term. Fuzzing involves sending unexpected inputs to a program to see how it responds. Passive monitoring uses a network tap or other capture technology to allow monitoring of actual traffic to a system or application.
31. B. Real user monitoring (RUM) is a passive monitoring technique that records user interaction with an application or system to ensure performance and proper application behavior. RUM is often used as part of a predeployment process using the actual user interface. The other answers are all made up—synthetic monitoring uses simulated behavior, but synthetic user monitoring is not a testing method. Similarly, passive monitoring monitors actual traffic, but *passive user recording* is not an industry term or technique. Client/server testing merely describes one possible architecture.
32. B. Jim should ask the information security team to flag the issue as resolved if he is sure the patch was installed. Many vulnerability scanners rely on version information or banner information and may flag patched versions if the software provider does not update the information they see. Uninstalling and reinstalling the patch will not change this. Changing the version information may not change all of the details that are being flagged by the scanner and may cause issues at a later date. Reviewing the vulnerability information for a workaround may be a good idea but should not be necessary if the proper patch is installed; it can create maintenance issues later.

33. B. zzuf is the only fuzzer on the list, and zzuf is specifically designed to work with tools like web browsers, image viewers, and similar software by modifying network and file input to application. Nmap is a port scanner, Nessus is a vulnerability scanner, and Nikto is a web server scanner.
34. C. An important part of application threat modeling is threat categorization. It helps to assess attacker goals that influence the controls that should be put in place. The other answers all involve topics that are not directly part of application threat modeling.
35. A. Passive scanning can help identify rogue devices by capturing MAC address vendor IDs that do not match deployed devices, by verifying that systems match inventories of organizationally owned hardware by hardware address, and by monitoring for rogue SSIDs or connections.

    Scripted attacks are part of active scanning rather than passive scanning, and active scanning is useful for testing IDS or IPS systems, whereas passive scanning will not be detected by detection systems. Finally, a shorter dwell time can actually miss troublesome traffic, so balancing dwell time versus coverage is necessary for passive wireless scanning efforts.

36. D. Bluetooth active scans can determine both the strength of the PIN and what security mode the device is operating in. Unfortunately, Bluetooth scans can be challenging due to the limited range of Bluetooth and the prevalence of personally owned Bluetooth enabled devices. Passive Bluetooth scanning only detects active connections and typically requires multiple visits to have a chance of identifying all devices.
37. D. Regression testing, which is a type of functional or unit testing, tests to ensure that changes have not introduced new issues. Nonregression testing checks to see whether a change has had the effect it was supposed to, smoke testing focuses on simple problems with impact on critical functionality, and evolution testing is not a software testing technique.
38. D. Nmap, Nessus, and Nikto all have OS fingerprinting or other operating system identification capabilities. sqlmap is designed to perform automated detection and testing of SQL injection flaws and does not provide OS detection.
39. C. Key risk indicators are used to tell those in charge of risk management how risky an activity is and how much impact changes are having on that risk profile. Identifying key risk indicators and monitoring them can help to identify high-risk areas earlier in their lifecycle. Yearly risk assessments may be a good idea, but only provide a point-in-time view, whereas penetration tests may miss out on risks that are not directly security related. Monitoring logs and events using a SIEM device can help detect issues as they occur but won't necessarily show trends in risk.
40. C. Passive monitoring only works after issues have occurred because it requires actual traffic. Synthetic monitoring uses simulated or recorded traffic and thus can be used to proactively identify problems. Both synthetic and passive monitoring can be used to detect functionality issues.
41. B. Getting authorization is the most critical element in the planning phase. Permission, and the "get out of jail free card" that demonstrates that organizational leadership is aware of the issues that a penetration test could cause, is the first step in any penetration test. Gathering tools and building a lab, as well as determining what type of test will be conducted, are all important, but nothing should happen without permission.
42. C. Discovery can include both active and passive discovery. Port scanning is commonly done during discovery to assess what services the target provides, and nmap is one of the most popular tools used for this purpose. Nessus and Nikto might be used during the vulnerability

scanning phase, and john, a password cracker, can be used to recover passwords during the exploitation phase.

43. B. Penetration test reports often include information that could result in additional exposure if they were accidentally released or stolen. Therefore, determining how vulnerability data should be stored and sent is critical. Problems with off-limits targets are more likely to result in issues during the vulnerability assessment and exploitation phase, and reports should not be limited in length but should be as long as they need to be to accomplish the goals of the test.
44. B. Code coverage testing most frequently requires that every function has been called, that each statement has been executed, that all branches have been fully explored, and that each condition has been evaluated for all possibilities. API, input, and loop testing are not common types of code coverage testing measures.
45. B. Time to remediate a vulnerability is a commonly used key performance indicator for security teams. Time to live measures how long a packet can exist in hops, business criticality is a measure used to determine how important a service or system is to an organization, and coverage rates are used to measure how effective code testing is.
46. D. Unique user IDs provide accountability when paired with auditable logs to provide that a specific user took any given action. Confidentiality, availability, and integrity can be provided through other means like encryption, systems design, and digital signatures.
47. B. Application programming interfaces (APIs), user interfaces (UIs), and physical interfaces are all important to test when performing software testing. Network interfaces are not a part of the typical list of interfaces tested in software testing.
48. C. The Common Vulnerabilities and Exposures (CVE) database provides a consistent reference for identifying security vulnerabilities. The Open Vulnerability and Assessment Language (OVAL) is used to describe the security condition of a system. The Extensible Configuration Checklist Description Format (XCCDF) is used to create security checklists in a standardized fashion. The Script Check Engine (SCE) is designed to make scripts interoperable with security policy definitions.
49. B. Security vulnerabilities can be created by misconfiguration, logical or functional design or implementation issues, or poor programming practices. Fuzzing is a method of software testing and is not a type of issue. Buffer overflows and race conditions are both caused by logical or programming flaws, but they are not typically caused by misconfiguration or functional issues.
50. C. Simply updating the version that an application provides may stop the vulnerability scanner from flagging it, but it won't fix the underlying issue. Patching, using workarounds, or installing an application layer firewall or IPS can all help to remediate or limit the impact of the vulnerability.
51. C. Saria's social-engineering attack succeeded in persuading a staff member at the help desk to change a password for someone who they not only couldn't see, but who they couldn't verify actually needed their password reset. *Black box* and *zero knowledge* are both terms describing penetration tests without information about the organization or system, and *help desk spoofing* is not an industry term.
52. D. The menu shown will archive logs when they reach the maximum size allowed (20 MB). These archives will be retained, which could fill the disk. Log data will not be overwritten, and log data should not be lost when the data is archived. The question does not include enough information to determine if needed information may not be logged.
53. C. Penetration tests are intended to help identify vulnerabilities, and exploiting them is part of the process rather than a hazard. Application crashes; denial of service due to system, network, or application failures; and even data corruption can all be hazards of penetration tests.

54. B. NIST SP 800-53A is titled "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," and covers methods for assessing and measuring controls.

    NIST 800-12 is an introduction to computer security, 800-34 covers contingency planning, and 800-86 is the "Guide to Integrating Forensic Techniques into Incident Response."

55. The security controls match with the categories as follows:
    1. TCP Connect: B. Completes a three-way handshake.
    2. TCP ACK: C. Sends a packet disguised as part of an active control.
    3. TCP SYN: A. Sends a request to open a new connection.
    4. Xmas: D. Sends a packet with the FIN, PSH, and URG flags set.
56. B. Port 80 is used by the HTTP protocol for unencrypted web communications. If Kara wishes to protect against eavesdropping, she should block this port and restrict web access to encrypted HTTPS connections on port 443.
57. A. Port 22 is used by the Secure Shell (SSH) protocol for administrative connections. If Kara wishes to restrict administrative connections, she should block access on this port.
58. C. The audit finding indicates that the backup administrator may not be monitoring backup logs and taking appropriate action based on what they report, thus resulting in potentially unusable backups. Issues with review, logging, or being aware of the success or failure of backups are less important than not having usable backups.
59. C. ITIL, which originally stood for IT Infrastructure Library, is a set of practices for IT service management, and is not typically used for auditing. COBIT, or the Control Objectives for Information and Related Technology, ISO 27002, and SSAE-18, or the Statement on Standards for Attestation Engagements number 18, are all used for auditing.
60. A. NIST SP 800-137 outlines the process for organizations that are establishing, implementing, and maintaining an ISCM as define, establish, implement, analyze and report, respond, review, and update. Prepare, detect and analyze, contain, respond, recover, report is an incident response plan, and the others do not match the NIST process.
61. B. Lauren's team is using regression testing, which is intended to prevent the recurrence of issues. This means that measuring the rate of defect recurrence is an appropriate measure for their work. Time to remediate vulnerabilities is associated with activities like patching, rather than preparing the patch, whereas a weighted risk trend is used to measure risk over time to an organization. Finally, specific coverage may be useful to determine if they are fully testing their effort, but regression testing is more specifically covered by defect recurrence rates.
62. C. Static program reviews are typically performed by an automated tool. Program understanding, program comprehension, code review, software inspections and software walkthroughs are all human-centric methods for reviewing code.
63. A. In order to fully test code, a white box test is required. Without full visibility of the code, error conditions or other code could be missed, making a gray box or black box test an inappropriate solution. Using dynamic testing that runs against live code could also result in some conditions being missed due to sections of code not being exposed to typical usage.
64. A. A test coverage report measures how many of the test cases have been completed and is used as a way to provide test metrics when using test cases. A penetration test report is provided when a penetration test is conducted—this is not a penetration test. A code coverage report covers how much of the code has been tested, and a line coverage report is a type of code coverage report.

65. C. The changes from a testing environment with instrumentation inserted into the code and the production environment for the code can mask timing-related issues like race conditions. Bounds checking, input validation, and pointer manipulation are all related to coding issues rather than environmental issues and are more likely to be discoverable in a test environment.
66. D. Once a vulnerability scanner identifies a potential problem, validation is necessary to verify that the issue exists. Reporting, patching, or other remediation actions can be conducted once the vulnerability has been confirmed.
67. B. Fagan testing is a detailed code review that steps through planning, overview, preparation, inspection, rework, and follow-up phases. Dynamic tests test the code in a real runtime environment, whereas fuzzing is a type of dynamic testing that feeds invalid inputs to software to test its exception-handling capabilities. Roth-Parker reviews were made up for this question.
68. D. The Common Vulnerability Scoring System (CVSS) includes metrics and calculation tools for exploitability, impact, how mature exploit code is, and how vulnerabilities can be remediated, as well as a means to score vulnerabilities against users' unique requirements. NVD is the National Vulnerability Database, CSV is short for comma-separated values, and *VSS (Visual SourceSafe)* is an irrelevant term related to software development rather than vulnerability management.
69. D. Network-enabled printers often provided services via TCP 515 and 9100, and have both nonsecure and secure web-enabled management interfaces on TCP 80 and 443. Web servers, access points, and file servers would not typically provide service on the LPR and LPD ports (515 and 9100).
70. A. Nikto, Burp Suite, and Wapiti are all web application vulnerability scanners, tools designed specifically to scan web servers and applications. While they share some functionality with broader vulnerability scanners and port scanning tools, they have a narrower focus and typically have deeper capabilities than vulnerability scanners.
71. The correct order of steps in a Fagan inspection is:

- D. Planning
- C. Overview
- E. Preparation
- B. Inspection
- F. Rework
- A. Follow-up

72. B. Metasploit is an exploitation package that is designed to assist penetration testers. A tester using Metasploit can exploit known vulnerabilities for which an exploit has been created or can create their own exploits using the tool. While Metasploit provides built-in access to some vulnerability scanning functionality, a tester using Metasploit should primarily be expected to perform actual tests of exploitable vulnerabilities. Similarly, Metasploit supports creating buffer overflow attacks, but it is not a purpose-built buffer overflow testing tool, and of course testing systems for zero-day exploits doesn't work unless they have been released.
73. D. Susan is conducting interface testing. Interface testing involves testing system or application components to ensure that they work properly together. Misuse case testing focuses on how an attacker might misuse the application and would not test normal cases. Fuzzing attempts to send unexpected input and might be involved in interface testing, but it won't cover the full set of concerns. Regression testing is conducted when testing changes and is used to ensure that the application or system functions as it did before the update or change.
74. B. Not having enough log sources is not a key consideration in log management system design, although it may be a worry for security managers who can't capture the data they need. Log

management system designs must take into account the volume of log data and the network bandwidth it consumes, the security of the data, and the amount of effort required to analyze the data.

75. B. The Common Platform Enumeration (CPE) component of SCAP provides a consistent way to refer to operating systems and other system components. The Common Vulnerabilities and Exposures (CVE) component provides a consistent way to refer to security vulnerabilities. The Common Weaknesses Enumeration (CWE) component helps describe the root causes of software flaws. The Open Vulnerability and Assessment Language (OVAL) standardizes steps of the vulnerability assessment process.
76. C. Rebooting a Windows machine results in an information log entry. Windows defines five types of events: errors, which indicate a significant problem; warnings, which may indicate future problems; information, which describes successful operation; success audits, which record successful security accesses; and failure audits, which record failed security access attempts.
77. C. Inconsistent time stamps are a common problem, often caused by improperly set time zones or due to differences in how system clocks are set. In this case, a consistent time difference often indicates that one system uses local time, and the other is using Greenwich Mean Time (GMT). Logs from multiple sources tend to cause problems with centralization and collection, whereas different log formats can create challenges in parsing log data. Finally, modified logs are often a sign of intrusion or malicious intent.
78. A. Authenticated scans use a read-only account to access configuration files, allowing more accurate testing of vulnerabilities. Web application, unauthenticated scans, and port scans don't have access to configuration files unless they are inadvertently exposed.
79. B. Microsoft's STRIDE threat assessment model places threats into one of six categories:
    - Spoofing—threats that involve user credentials and authentication, or falsifying legitimate communications
    - Tampering—threats that involve the malicious modification of data
    - Repudiation—threats that cause actions to occur that cannot be denied by a user
    - Information disclosure—threats that involve exposure of data to unauthorized individuals
    - Denial of service—threats that deny service to legitimate users
    - Elevation of privilege—threats that provide higher privileges to unauthorized users

- Using role-based access controls (RBACs) for specific operations will help to ensure that users cannot perform actions that they should not be able to. Auditing and logging can help detect abuse but won't prevent it, and data type, format checks, and whitelisting are all useful for preventing attacks like SQL injection and buffer overflow attacks but are not as directly aimed at authorization issues.

80. D. Since a shared symmetric key could be used by any of the servers, transaction identification problems caused by a shared key are likely to involve a repudiation issue. If encrypted transactions cannot be uniquely identified by server, they cannot be proved to have come from a specific server.
81. C. Filtering is useful for preventing denial of service attacks but won't prevent tampering with data. Hashes and digital signatures can both be used to verify the integrity of data, and authorization controls can help ensure that only those with the proper rights can modify the data.

82. D. The Network Time Protocol (NTP) allows the synchronization of system clocks with a standardized time source. The Secure Shell (SSH) protocol provides encrypted administrative connections to servers. The File Transfer Protocol (FTP) is used for data exchange. Transport Layer Security (TLS) is an encryption process used to protect information in transit over a network.
83. B. Fuzz testers are capable of automatically generating input sequences to test an application. Therefore, testers do not need to manually generate input, although they may do so if they wish. Fuzzers can reproduce errors (and thus, "fuzzers can't reproduce errors" is not an issue) but typically don't fully cover the code—code coverage tools are usually paired with fuzzers to validate how much coverage was possible. Fuzzers are often limited to simple errors because they won't handle business logic or attacks that require knowledge from the application user.
84. D. Statement coverage tests verify that every line of code was executed during the test. Branch coverage verifies that every if statement was executed under all if and else conditions. Condition coverage verifies that every logical test in the code was executed under all sets of inputs. Function coverage verifies that every function in the code was called and returns results.
85. C. After scanning for open ports using a port scanning tool like nmap, penetration testers will identify interesting ports and then conduct vulnerability scans to determine what services may be vulnerable. This will perform many of the same activities that connecting via a web server will and will typically be more useful than trying to manually test for vulnerable accounts via Telnet. sqlmap would typically be used after a vulnerability scanner identifies additional information about services, and the vulnerability scanner will normally provide a wider range of useful information.
86. B. The system is likely a Linux system. The system shows X11, as well as login, shell, and nfs ports, all of which are more commonly found on Linux systems than Windows systems or network devices. This system is also very poorly secured; many of the services running on it should not be exposed in a modern secure network.
87. D. Nmap only scans 1000 TCP and UDP ports by default, including ports outside the 0–1024 range of "well-known" ports. By using the defaults for nmap, Ben missed 64,535 ports. OS fingerprinting won't cover more ports but would have provided a best guess of the OS running on the scanned system.
88. C. Static analysis is the process of reviewing code without running it. It relies on techniques like data flow analysis to review what the code does if it was run with a given set of inputs. Black and gray box analyses are not types of code review, although black box and gray box both describe types of penetration testing. Fuzzing provides unexpected or invalid data inputs to test how software responds.
89. C. A manual code review, which is performed by humans who review code line by line, is the best option when it is important to understand the context and business logic in the code. Fuzzing, dynamic, and static code review can all find bugs that manual code review might not but won't take the intent of the programmers into account.
90. C. Misuse case diagrams use language beyond typical use case diagrams, including *threatens* and *mitigates*. Threat trees are used to map threats but don't use specialized language like *threatens* and *mitigates*. STRIDE is a mnemonic and model used in threat modeling, and DREAD is a risk assessment model.
91. C. The most important first step for a penetration test is getting permission. Once permission has been received, planning, data gathering, and then elements of the actual test like port scanning can commence.
92. A. Sqlmap is a dedicated database vulnerability scanner and is well suited for Kevin's purposes. Nmap is a network port scanner that would not provide relevant results. Nessus is a network

vulnerability scanner and may detect issues with a database but would not be as effective as sqlmap. Sqlthrash does not exist.

93. C. A TCP scan that sets all or most of the possible TCP flags is called a Christmas tree, or Xmas, scan since it is said to "light up like a Christmas tree" with the flags. A SYN scan would attempt to open TCP connections, whereas an ACK scan sends packets with the ACK flag set. There is no such type of scan known as a TCP flag scan.
94. D. Nmap is a very popular open-source port scanner. Nmap is not a vulnerability scanner, nor is it a web application fuzzer. While port scanners can be used to partially map a network, and its name stands for Network Mapper, it is not a network design tool.
95. C. Vulnerability scanners cannot detect vulnerabilities for which they do not have a test, plug-in, or signature. Signatures often include version numbers, service fingerprints, or configuration data. They can detect local vulnerabilities as well as those that require authentication if they are provided with credentials, and of course, they can detect service vulnerabilities.
96. C. The Common Vulnerabilities and Exposures (CVE) dictionary provides a central repository of security vulnerabilities and issues. Patching information for applications and software versions are sometimes managed using central patch management tools, but a single central database is not available for free or public use. Costs versus effort is also not what CVE stands for.
97. A. Specifications are the documents associated with the system being audited. Specifications generally include policies, procedures, requirements, and designs.
98. D. Privilege escalation occurs during the attack phase of a penetration test. Host and service information gathering, as well as activities like dumpster diving that can provide information about the organization, its systems, and security, are all part of the discovery phase.
99. B. Once additional tools have been installed, penetration testers will typically use them to gain additional access. From there they can further escalate privileges, search for new targets or data, and once again, install more tools to allow them to pivot further into infrastructure or systems.
100. B. Penetration testing reports often do not include the specific data captured during the assessment, as the readers of the report may not be authorized to access all of the data, and exposure of the report could result in additional problems for the organization. A listing of the issues discovered, risk ratings, and remediation guidance are all common parts of a penetration test report.