**Chapter 5 Review Questions**

1. The residential lock most often used for keeping out intruders is the \_\_\_\_\_\_\_.

a. privacy lock

b. passage lock

c. keyed entry lock – PG163

d. encrypted key lock

2. A lock that extends a solid metal bar into the door frame for extra security is the \_\_\_\_\_\_.

a. deadman’s lock

b. full bar lock

c. deadbolt lock – PG163-164

d. triple bar lock

3. A mantrap \_\_\_\_\_\_\_\_.

a. is illegal in the United States

b. monitors and controls two interlocking doors to a room – PG167-168

c. is a special keyed lock

d. requires the use of a cipher lock

4. Which of the following cannot be used along with fencing as a security perimeter?

a. Vapor barrier – PG169

b. Rotating spikes

c. Roller barrier

d. Anti-climb paint

5. A \_\_\_\_\_\_\_\_ can be used to secure a mobile device.

a. cable lock – PG168-169

b. mobile chain

c. security tab

d. mobile connector

6. Which of the following is not used to secure a desktop computer?

a. Data encryption

b. Screen locking

c. Remote wipe/sanitation – PG170

d. Strong passwords

7. Which is the first step in securing an operating system?

a. Implement patch management.

b. Configure operating system security and settings.

c. Perform host software baselining.

d. Develop the security policy. – PG171

8. A typical configuration baseline would include each of the following except \_\_\_\_\_\_.

a. changing any default settings that are insecure

b. eliminating any unnecessary software

c. enabling operating system security features

d. performing a security risk assessment – PG172

9. Which of the following is NOT a Microsoft Windows setting that can be configured through a security template?

a. Account Policies

b. User Rights

c. Keyboard Mapping – PG172

d. System Services

10. \_\_\_\_\_\_\_\_ allows for a single configuration to be set and then deployed to many or all users.

a. Group Policy – PG172

b. Active Directory

c. Snap-In Replication (SIR)

d. Command Configuration

11. A \_\_\_\_\_\_\_ addresses a specific customer situation and often may not be distrib- uted outside that customer’s organization.

a. rollup

b. service pack

c. patch

d. hotfix – PG173

12. Which of the following is NOT an advantage to an automated patch update service?

a. Administrators can approve or decline updates for client systems, force updates to install by a specific date, and obtain reports on what updates each computer needs.

b. Downloading patches from a local server instead of using the vendor’s online update service can save bandwidth and time because each computer does not have to connect to an external server.

c. Users can disable or circumvent updates just as they can if their computer is configured to use the vendor’s online update service. – PG174

d. Specific types of updates that the organization does not test, such as hotfixes, can be automatically installed whenever they become available.

13. Each of the following is a type of matching used by anti-virus software except .

a. string scanning

b. wildcard scanning

c. match scanning – PG176

d. mismatch scanning

14. How does heuristic detection detect a virus?

a. A virtualized environment is created and the code is executed in it. – PG176

b. A string of bytes from the virus is compared against the suspected file.

c. The bytes of a virus are placed in different “piles” and then used to create a profile.

d. The virus signature file is placed in a suspended chamber before streaming to the CPU.

15. A cross-site request forgery (XSRF) \_\_\_\_\_\_\_\_.

a. is used to inherit the identity and privileges of the victim – PG183

b. is identical to cross-site scripting (XSS)

c. cannot be blocked

d. can only be used with a Web-based e-mail client

16. Which of the following is a list of approved e-mail senders?

a. whitelist – PG176

b. blacklist

c. greylist

d. greenlist

17. A(n) \_\_\_\_\_\_\_\_\_\_ can provide details regarding requests for specific files on a system.

a. audit log

b. access log – PG178

c. report log

d. file log

18. Errors that occur while an application is running are called

a. exceptions – PG182

b. faults

c. liabilities

d. conventions

19. Which is the preferred means of trapping user input for errors?

a. Input validation

b. On-Trap input

c. Escaping – PG183

d. Fuzz testing

20. Each of the following is true about data loss prevention (DLP) except

a. it can only protect data in use – PG185

b. it can scan data on a DVD

c. it can read inside compressed files

d. a policy violation can generate a report or block the data

**Chapter 6 Review Questions**

1. Which of the following is true about subnetting?

a. It requires the use of a Class B network.

b. It divides the network IP address on the boundaries between bytes.

c. It provides very limited security protection.

d. It is also called subnet addressing. – PG228

2. A virtual LAN (VLAN) allows devices to be grouped \_\_\_\_\_\_\_.

a. based on subnets

b. logically – PG231

c. directly to hubs

d. only around core switches

3. Which of the following devices is easiest for an attacker to take advantage of to capture and analyze packets?

a. hub – PG209

b. switch

c. router

d. load balancer

4. Which of the following is not an attack against a switch?

a. MAC flooding

b. ARP address impersonation – PG211

c. ARP poisoning

d. MAC address impersonation

5. Which of the following is not true regarding a demilitarized zone (DMZ)?

a. It provides an extra degree of security.

b. It typically includes an e-mail or Web server.

c. It can be configured to have one or two firewalls.

d. It contains servers that are used only by internal network users. – PG228

6. Which of the following is true about network address translation (NAT)?

a. It substitutes MAC addresses for IP addresses.

b. It removes private addresses when the packet leaves the network. – PG224-225

c. It can be found only on core routers.

d. It can be stateful or stateless.

7. Which of the following is not an advantage of a load balancer?

a. The risk of overloading a desktop client is reduced. – PG212

b. Network hosts can benefit from having optimized bandwidth.

c. Network downtime can be reduced.

d. DoS attacks can be detected and stopped.

8. Which of the following is another name for a packet filter?

a. proxy server

b. reverse proxy server

c. DMZ

d. firewall – PG214

9. A \_\_\_\_\_\_\_\_ firewall allows the administrator to create sets of related parameters that together define one aspect of the device’s operation.

a. rule-based

b. host-based

c. signature-based

d. settings-based – PG214

10. A(n) \_\_\_\_\_\_\_\_\_ intercepts an internal user request and then processes that request on behalf of the user.

a. content filter

b. host detection server

c. proxy server – PG215

d. intrusion prevention device

11. A reverse proxy \_\_\_\_\_\_\_\_\_\_.

a. only handles outgoing requests

b. is the same as a proxy server

c. must be used together with a firewall

d. routes incoming requests to the correct server – PG216

12. Which is the preferred location for a spam filter?

a. Install the spam filter with the SMTP server. – PG217-218

b. Install the spam filter on the POP3 server.

c. Install the spam filter on the proxy server.

d. Install the spam filter on the local host client.

13. A \_\_\_\_\_\_\_\_\_ watches for attacks and sounds an alert only when one occurs.

a. network intrusion prevention system (NIPS)

b. proxy intrusion device

c. network intrusion detection system (NIDS) – PG223-224

d. firewall

14. A multipurpose security device is known as a(n) \_\_\_\_\_\_\_\_.

a. unified attack management system (UAMS)

b. intrusion detection/prevention device

c. all-in-one network security appliance – PG224

d. proxy security system (PSS)

15. Each of the following can be used to hide information about the internal network except \_\_\_\_\_\_\_.

a. a protocol analyzer

b. a proxy server – PG216

c. network address translation (NAT) – PG225

d. subnetting – PG230-231

16. What is the difference between a network intrusion detection system (NIDS) and a network intrusion prevention system (NIPS)?

a. A NIPS can take actions quicker to combat an attack. – PG224

b. A NIDS provides more valuable information about attacks.

c. A NIPS is much slower because it uses protocol analysis.

d. There is no difference because a NIDS and a NIPS are equal.

17. A variation of NAT that is commonly found on home routers is \_\_\_\_\_\_\_.

a. port address translation (PAT) – PG225

b. network proxy translation (NPT)

c. network address IP transformation (NAIPT)

d. subnet transformation (ST)

18. If a device is determined to have an out-of-date virus signature file, then Network Access Control (NAC) can redirect that device to a network by \_\_\_\_\_\_\_\_.

a. a Trojan horse

b. TCP/IP hijacking

c. Address Resolution Protocol (ARP) poisoning – PG227

d. DHCP man-in-the-middle

19. Each of the following is an option in a firewall rule except \_\_\_\_\_\_\_\_\_.

a. prompt

b. block

c. delay – PG212

d. allow

20. A firewall using \_\_\_\_\_\_\_ is the most secure type of firewall.

a. stateful packet filtering – PG214

b. network intrusion detection system replay

c. stateless packet filtering

d. reverse proxy analysis

.