Network Security Fundamentals

TRUE/FALSE

1. A packet monkey is an unskilled programmer who spreads viruses and other malicious scripts to exploit computer weaknesses.

2. A worm creates files that copy themselves repeatedly and consume disk space.

3. Physical security protects a system from theft, fire, or environmental disaster.

4. Reviewing log files is a time-consuming task and therefore should only be done when an attack on the network has occurred.

5. With discretionary access control, network users can share information with other users, making it more risky than MAC.

MULTIPLE CHOICE

1. A hactivist can best be described as which of the following?
   a. an unskilled programmer that spreads malicious scripts
   b. consider themselves seekers of knowledge
   c. use DoS attacks on Web sites with which they disagree
   d. deface Web sites by leaving messages for their friends to read

2. Malware that creates networks of infected computers that can be controlled from a central station is referred to as which of the following?
   a. botnet
   b. Trojan
   c. logic bomb
   d. packet monkey

3. What is a program that appears to do something useful but is actually malware?
   a. virus
   b. logic bomb
   c. Trojan
   d. back door

4. Which of the following is a type of script that automates repetitive tasks in an application such as a word processor but can also be programmed to be a virus?
   a. worm
   b. macro
   c. back door
   d. Trojan

5. Which term is best described as an attack that relies on the gullibility of people?
   a. malicious code
   b. script kiddie
   c. back door
   d. social engineering

6. Which type of attack works by an attacker operating between two computers in a network and impersonating one computer to intercept communications?
   a. malicious port scanning
   b. man-in-the-middle
   c. denial of service
   d. remote procedure call

7. Which type of attack causes the operating system to crash because it is unable to handle arbitrary data sent to a port?
   a. RPC attacks
   b. ICMP message abuse
   c. malicious port scanning
   d. SYN flood

8. What can an attacker use a port scanner to test for on a target computer?
   a. invalid IP addresses
   b. SYN flags
   c. open sockets
   d. ping floods

9. What is a VPN typically used for?
   a. secure remote access
   b. detection of security threats
   c. block open ports
   d. filter harmful scripts

10. Why might you want your security system to provide nonrepudiation?
    a. to prevent a user from capturing packets and viewing sensitive information
    b. to prevent an unauthorized user from logging into the system
    c. to trace the origin of a worm spread through email
    d. so a user can't deny sending or receiving a communication

11. Which of the following is NOT one of the three primary goals of information security?
    a. confidentiality
    b. integrity
    c. impartiality
    d. availability

12. Defense in depth can best be described as which of the following?
    a. a firewall that protects the network and the servers
    b. a layered approach to security
    c. antivirus software and firewalls
    d. authentication and encryption

13. Which security layer verifies the identity of a user, service, or computer?
    a. authentication
    b. repudiation
    c. physical security
    d. authorization

14. In which form of authentication does the authenticating device generate a random code and send it to the user who wants to be authenticated?
    a. basic
    b. challenge/response
    c. biometrics
    d. signature

15. What is the name of a storage area where viruses are placed by antivirus software so they cannot replicate or do harm to other files?
    a. firewall
    b. recycle bin
    c. quarantine
    d. demilitarized zone

16. Which of the following is NOT information that a packet filter uses to determine whether to block a packet?
    a. checksum
    b. port
    c. IP address
    d. protocol

17. Which type of firewall policy calls for a firewall to deny all traffic by default?
    a. permissive policy
    b. perimeter policy
    c. restrictive policy
    d. demilitarized policy

18. Which security tool works by recognizing signs of a possible attack and sending notification to an administrator?
    a. DiD
    b. DMZ
    c. VPN
    d. IDPS

19. What tool do you use to secure remote access by users who utilize the Internet?
    a. VPN
    b. IDS
    c. DMZ
    d. DiD

20. With which access control method do system administrators establish what information users can share?
    a. discretionary access control
    b. mandatory access control
    c. administrative access control
    d. role-based access control

FILL IN THE BLANKS

1. __________________ are spread by several methods, including running executable code, sharing disks or memory sticks, opening e-mail attachments, and viewing infected or malicious Web pages.
2. ______________ do not require user intervention to be launched; they are self-propagating.

3. A ______________ is reserved for a program that runs in the background to listen for requests for the service it offers.
4. ______________________ is the capability to prevent a participant in an electronic transaction from denying that it performed an action.
5. ________________ events usually track the operations of the firewall or IDPS, making a log entry whenever it starts or shuts down.

MATCH THE OPTIONS TO THE CORRESPONDING STATEMENTS.

a. auditing
b. biometrics
c. DMZ
d. DDoS attack
e. packet filters
f. port
g. RBAC
h. signatures
i. socket
j. worm

1. An attack in which many computers are hijacked and used to flood the target with so many false requests that the server cannot process them all, and normal traffic is blocked
2. The process of recording which computers are accessing a network and what resources are being accessed, and then recording the information in a log file
3. Signs of possible attacks that include an IP address, a port number, and the frequency of access attempts; an IDPS uses signatures to detect possible attacks
4. An area in random access memory (RAM) reserved for the use of a program that “listens” for requests for the service it provides
5. A semitrusted subnet that lies outside the trusted internal network but is connected to the firewall to make services publicly available while still protecting the internal LAN
6. A network connection consisting of a port number combined with a computer’s IP address
7. An access control method that establishes organizational roles to control access to information
8. A method of authenticating a user using physical information, such as retinal scans, fingerprints, or voiceprints
9. Computer files that copy themselves repeatedly and consume disk space or other resources
10. Hardware or software tools that allow or deny packets based on specified criteria, such as port, IP address, or protocol.

PROVIDE SHORT ANSWERS TO THE FOLLOWING.

1. List and describe two motivations attackers have to attack a network.
2. What is a script kiddie?
3. Compare and contrast virus and worm.
4. What is social engineering?
5. What is malicious port scanning and how can you defend against it?
6. Discuss scripting and how it relates to network security.
7. What are the three primary goals of information security? Describe them.
8. Discuss defense in depth.
9. What is virus scanning and how does it work?
10. Discuss permissive versus restrictive firewall policies.