Chapter 1 - Network Security Fundamentals

TRUE/FALSE

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

   ANS: F PTS: 1 REF: 3

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

   ANS: T PTS: 1 REF: 5

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

   ANS: T PTS: 1 REF: 12

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

   ANS: F PTS: 1 REF: 17

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

   ANS: T PTS: 1 REF: 19

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

   ANS: C PTS: 1 REF: 3

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

   ANS: A PTS: 1 REF: 5

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

   ANS: C PTS: 1 REF: 5

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
   c. back door

b. macro
d. Trojan

ANS: B PTS: 1 REF: 6

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

ANS: D PTS: 1 REF: 6

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

ANS: B PTS: 1 REF: 7

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

ANS: A PTS: 1 REF: 7

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

ANS: C PTS: 1 REF: 8

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

ANS: A PTS: 1 REF: 10

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

ANS: D PTS: 1 REF: 11

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

ANS: C PTS: 1 REF: 11

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

ANS: B PTS: 1 REF: 12

13. Which security layer verifies the identity of a user, service, or computer?

a. authentication c. physical security
b. repudiation d. authorization

ANS: A PTS: 1 REF: 12

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 c. biometrics
b. challenge/response d. signature

ANS: B PTS: 1 REF: 13

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 c. quarantine
b. recycle bin d. demilitarized zone

ANS: C PTS: 1 REF: 13

16. Which of the following is NOT information that a packet filter uses to determine whether to block a packet?

a. checksum c. IP address
b. port d. protocol

ANS: A PTS: 1 REF: 13

17. Which type of firewall policy calls for a firewall to deny all traffic by default?

a. permissive policy c. restrictive policy
b. perimeter policy d. demilitarized policy

ANS: C PTS: 1 REF: 14

18. Which security tool works by recognizing signs of a possible attack and sending notification to an administrator?

a. DiD c. VPN
b. DMZ d. IDPS

ANS: D PTS: 1 REF: 15-16

19. What tool do you use to secure remote access by users who utilize the Internet?

a. VPN c. DMZ
b. IDS d. DiD

ANS: A PTS: 1 REF: 16-17

20. With which access control method do system administrators establish what information users can share?

a. discretionary access control c. administrative access control
b. mandatory access control d. role-based access control

ANS: B PTS: 1 REF: 19

COMPLETION

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.

   ANS: Viruses

   PTS: 1 REF: 5

2. _______________ do not require user intervention to be launched; they are self-propagating.

   ANS: Worms

   PTS: 1 REF: 5

3. A _______________ is reserved for a program that runs in the background to listen for requests for the service it offers.

   ANS: port

   PTS: 1 REF: 5

4. ________________________ is the capability to prevent a participant in an electronic transaction from denying that it performed an action.

   ANS: Nonrepudiation

   PTS: 1 REF: 11

5. _________________ events usually track the operations of the firewall or IDPS, making a log entry whenever it starts or shuts down.

   ANS: System

   PTS: 1 REF: 17

MATCHING

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.

1.	ANS: D	PTS: 1
2.	ANS: A	PTS: 1
3.	ANS: H	PTS: 1
4.	ANS: F	PTS: 1
5.	ANS: C	PTS: 1
6.	ANS: I	PTS: 1
7.	ANS: G	PTS: 1
8.	ANS: B	PTS: 1
9.	ANS: J	PTS: 1
10.	ANS: E	PTS: 1

SHORT ANSWER

1. List and describe two motivations attackers have to attack a network.

   ANS:
   Status—Some attackers attempt to take over computer systems just for the thrill of it. They like to count the number of systems they have accessed as notches on their belt.

   Revenge—Disgruntled current or former employees might want to retaliate against an organization for policies or actions they consider wrong. They can sometimes gain entry through an undocumented account (back door) in the system.

   Financial gain—Other attackers have financial profit as their goal. Attackers who break into a network can gain access to financial accounts. They can steal individual or corporate credit card numbers and make unauthorized purchases.

   Industrial espionage—Proprietary information is often valuable enough that it can be sold to competing companies or other parties.

   PTS: 1 REF: 2

2. What is a script kiddie?

   ANS:
   The term script kiddie is often used to describe relatively unskilled programmers who spread viruses and other malicious scripts to exploit weaknesses in computer systems. Script kiddies lack the ability to create viruses or Trojan programs on their own, but they can usually find these programs online.

   PTS: 1 REF: 3

3. Compare and contrast virus and worm.

ANS:
A virus is executable code that can replicate itself from one place to another surreptitiously and perform actions that range from benign to harmful. Viruses 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. Viruses can attach to other executables or replace them in order to spread or execute. Viruses require user intervention to run.

A worm creates files that copy themselves repeatedly and consume disk space. Worms do not require user intervention to be launched; they are self-propagating. Some worms can install back doors—a way of gaining unauthorized access to a computer or other resource, such as an unused port or terminal service, that makes it possible for attackers to gain control over the computer.

PTS: 1 REF: 5

4. What is social engineering?

ANS:
One common way that attackers gain access to an organization's resources cannot be prevented with hardware or software. The vulnerability in this case is well-meaning but gullible employees who attackers fool into giving out passwords or other access codes. This is called social engineering. To protect itself against personnel who do not observe accepted security practices or who willfully abuse them, an organization needs a strong and consistently enforced security policy and a rigorous training program.

PTS: 1 REF: 6

5. What is malicious port scanning and how can you defend against it?

ANS:
Malicious port scanning is when an attacker looks for open ports to infiltrate a network.

To defend against malicious port scanning, install and configure a firewall, which is hardware and/or software designed to filter out unwanted network traffic and protect authorized traffic.

PTS: 1 REF: 7

6. Discuss scripting and how it relates to network security.

ANS:
A widespread network intrusion that is increasing in frequency and severity is the use of scripts—executable code attached to e-mail messages or downloaded files that infiltrates a system. It can be difficult for a firewall or intrusion-detection system (IDS) to block all such files; specialty firewalls and other programs should be integrated with existing security systems to keep scripts from infecting a network.

PTS: 1 REF: 8

7. What are the three primary goals of information security? Describe them.

ANS:

The three primary goals of information security are data confidentiality, data integrity, and data availability. It is hard to imagine any aspect of information technology that has no responsibility for ensuring one or more of these three fundamental goals. Confidentiality is the prevention of intentional or unintentional disclosure of communications between a sender and recipient. Integrity ensures the accuracy and consistency of information during all processing (creation, storage, and transmission). Availability is the assurance that authorized users can access resources in a reliable and timely manner.

PTS: 1 REF: 11

8. Discuss defense in depth.

ANS:
The components and approaches to security should be arranged to provide layers of network defense. This layering approach to network security is often called defense in depth (DiD). The National Security Agency (NSA) originally designed DiD as a best practices strategy for achieving information assurance.
When beginning with an unprotected system, the first layer of defense added is always the most effective. As more layers are stacked on the first, potential attackers must successfully breach each layer to gain access to the next one. However, adding layers also adds increasing complexity for system administrators. Security enhancements must be balanced against the cost to maintain and monitor defenses. DiD does eventually reach a point where the cost of implementing additional security outweighs the potential benefits.

PTS: 1 REF: 12

9. What is virus scanning and how does it work?

ANS:
Virus scanning refers to the process of examining files or e-mail messages for filenames, file extensions such as .exe (for executable code) or .zip (for zipped files), and other indications that viruses are present. Many viruses have suspicious file extensions, but some seem innocuous. Antivirus software uses several methods to look for malware, including comparisons to the software’s current signature files, which contain a pattern of known viruses. Signature files are the primary reason for keeping your antivirus software updated; antivirus software vendors frequently create updates and make them available for customers to download.
When antivirus software recognizes the presence of viruses, it deletes them from the file system or places them in a storage area called a quarantine where they cannot replicate themselves or do harm to other files.

PTS: 1 REF: 13

10. Discuss permissive versus restrictive firewall policies.

ANS:
Permissive policy—Calls for a firewall and associated security components to allow all traffic through the network gateway by default and then to block services on a case-by-case basis.
Restrictive policy—Calls for a firewall and associated network security components to deny all traffic by default. The first rule denies all traffic on any service and using any port. To allow a specific type of traffic, a new rule must be placed ahead of the “deny all” rule.

PTS: 1 REF: 14