**Chapter 7 – Denial-of-Service Attacks**

**TRUE/FALSE QUESTIONS:**

T F 1. A denial-of-service attack is an attempt to compromise availability by

hindering or blocking completely the provision of some service.

T F 2. DoS attacks cause damage or destruction of IT infrastructures.

T F 3. A DoS attack targeting application resources typically aims to overload

or crash its network handling software.

T F 4. The SYN spoofing attack targets the table of TCP connections on the

server.

T F 5. A cyberslam is an application attack that consumes significant

resources, limiting the server’s ability to respond to valid requests from

other users.

T F 6. The source of the attack is explicitly identified in the classic ping flood

attack.

T F 7. Given sufficiently privileged access to the network handling code on a

computer system, it is difficult to create packets with a forged source

address.

T F 8. SYN-ACK and ACK packets are transported using IP, which is an

unreliable network protocol.

T F 9. The attacker needs access to a high-volume network connection for a

SYN spoof attack.

T F 10. Flooding attacks take a variety of forms based on which network

protocol is being used to implement the attack.

T F 11. The best defense against being an unwitting participant in a DDoS

attack is to prevent your systems from being compromised.

T F 12. A SIP flood attack exploits the fact that a single INVITE request

triggers considerable resource consumption.

T F 13. Slowloris is a form of ICMP flooding.

T F 14. Reflector and amplifier attacks use compromised systems running the

attacker’s programs.

T F 15. There is very little that can be done to prevent a flash crowd.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_ relates to the capacity of the network links connecting a server to the wider Internet.

A. Application resource B. Network bandwidth

C. System payload D. Directed broadcast

1. A \_\_\_\_\_\_ triggers a bug in the system’s network handling software causing it to crash and the system can no longer communicate over the network until this software is reloaded.

A. echo B. reflection

C. poison packet D. flash flood

3. Using forged source addresses is known as \_\_\_\_\_\_\_\_\_.

A. source address spoofing B. a three-way address

C. random dropping D. directed broadcast

4. The \_\_\_\_\_\_ attacks the ability of a network server to respond to TCP connection requests by overflowing the tables used to manage such connections.

A. DNS amplification attack B. SYN spoofing attack

C. basic flooding attack D. poison packet attack

5. TCP uses the \_\_\_\_\_\_\_ to establish a connection.

A. zombie B. SYN cookie

C. directed broadcast D. three-way handshake

6. \_\_\_\_\_\_\_ bandwidth attacks attempt to take advantage of the disproportionally large resource consumption at a server.

A. Application-based B. System-based

C. Random D. Amplification

7. \_\_\_\_\_\_\_ is a text-based protocol with a syntax similar to that of HTTP.

A. RIP B. DIP

C. SIP D. HIP

8. Bots starting from a given HTTP link and then following all links on the provided Web site in a recursive way is called \_\_\_\_\_\_\_.

A. trailing B. spidering

C. spoofing D. crowding

9. \_\_\_\_\_\_ attempts to monopolize all of the available request handling threads on the Web server by sending HTTP requests that never complete.

A. HTTP B. Reflection attacks

C. SYN flooding D. Slowloris

10. A characteristic of reflection attacks is the lack of \_\_\_\_\_\_\_ traffic.

A. backscatter B. network

C. three-way D. botnet

11. In both direct flooding attacks and \_\_\_\_\_\_ the use of spoofed source addresses results in response packets being scattered across the Internet and thus detectable.

A. SYN spoofing attacks B. indirect flooding attacks

C. ICMP attacks D. system address spoofing

12. In a \_\_\_\_\_\_\_ attack the attacker creates a series of DNS requests containing the spoofed source address for the target system.

A. SYN flood B. DNS amplification

C. poison packet D. UDP flood

13. It is possible to specifically defend against the \_\_\_\_\_\_ by using a modified version of the TCP connection handling code.

A. three-way handshake B. UDP flood

C. SYN spoofing attack D. flash crowd

14. Modifying the system’s TCP/IP network code to selectively drop an entry for an incomplete connection from the TCP connections table when it overflows, allowing a new connection attempt to proceed is \_\_\_\_\_\_\_.

A. poison packet B. slashdot

C. backscatter traffic D. random drop

15. When a DoS attack is detected, the first step is to \_\_\_\_\_\_\_.

A. identify the attack B. analyze the response

C. design blocking filters D. shut down the network

**SHORT ANSWER QUESTIONS:**

1. The ICMP echo response packets generated in response to a ping flood using randomly spoofed source addresses is known as \_\_\_\_\_\_\_ traffic.
2. \_\_\_\_\_ attacks flood the network link to the server with a torrent of malicious packets competing with valid traffic flowing to the server.
3. The standard protocol used for call setup in VoIP is the \_\_\_\_\_\_\_\_ Protocol.
4. Requests and \_\_\_\_\_\_\_ are the two different types of SIP messages.
5. A \_\_\_\_\_\_\_ flood refers to an attack that bombards Web servers with HTTP requests.
6. During a \_\_\_\_\_\_ attack, the attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system and when the intermediary responds, the response is sent to the target.
7. In reflection attacks, the \_\_\_\_\_\_ address directs all the packets at the desired target and any responses to the intermediary.
8. \_\_\_\_\_\_ attacks are a variant of reflector attacks and also involve sending a packet with a spoofed source address for the target system to intermediaries.
9. The best defense against broadcast amplification attacks is to block the use of \_\_\_\_\_\_\_ broadcasts.
10. The four lines of defense against DDoS attacks are: attack prevention and preemption, attack detection and filtering, attack source traceback and identification and \_\_\_\_\_\_\_.
11. Since filtering needs to be done as close to the source as possible by routers or gateways knowing the valid address ranges of incoming packets, an \_\_\_\_\_\_\_ is best placed to ensure that valid source addresses are used in all packets from its customers.
12. A \_\_\_\_\_\_ is a graphical puzzle used to attempt to identify legitimate human initiated interactions.
13. To respond successfully to a DoS attack a good \_\_\_\_\_\_ plan is needed that includes details of how to contact technical personal for your ISP(s).
14. If an organization is dependent on network services it should consider mirroring and \_\_\_\_\_\_\_\_ these servers over multiple sites with multiple network connections.
15. A \_\_\_\_\_ is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units, memory, bandwidth, and disk space.