Computer Security: Principles and Practice, 2nd Edition Chapter 7

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

|  |  |
| --- | --- |
|  | 1. The ICMP echo response packets generated in response to a ping flood using randomly spoofed source addresses is known as backscatter traffic. 2. Flooding 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 Session Initiation Protocol. 4. Requests and responses are the two different types of SIP messages. 5. A HTTP flood refers to an attack that bombards Web servers with HTTP requests. 6. During a reflection 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 spoofed source address directs all the packets at the desired target and any responses to the intermediary. 8. Amplification 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 IP-directed 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 attack reaction. 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 ISP is best placed to ensure that valid source addresses are used in all packets from its customers. 12. A captcha is a graphical puzzle used to attempt to identify legitimate human initiated interactions. 13. To respond successfully to a DoS attack a good incident response 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 replicating these servers over multiple sites with multiple network connections. 15. A denial-of-service 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. |