Chapter 7: Denial-of-Service Attacks

Denial-of-Service (DoS) Attack:

- An attack on some kind of service
- Categories are: Network bandwidth, system resources, application resources

Classic DoS Attacks:

- Flooding ping command: overwhels capacity of network connection to target. Source of the attack is easily identified unless spoofed. Network performance is affected.

Source Address Spoofing:

- Uses a forged source address through raw socket interface of operating system
- Attacker generates a large volume of packets with target as destination
- Requires network engineers to specifically query flow information

SYN Spoofing:

- Common DoS attack that attacks systems tables used to manage connection requests
- Legitimate users are denied access as network handling code of operating system is attacked

Flooding Attacks:

- Based on network protocol: ICMP, UDP, TCP SYN
- Overload network capacity on a link to server