Chapter 7

Denial of Service Attacks
DoS attack:

“An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.”
Denial-of-Service (DoS)

- An attack on the availability of some service
- Categories of resources that could be attacked are:
  - network bandwidth
  - system resources
  - application resources
Classic Denial-of-Service Attacks

- Ping flooding command
  - overwhelm the capacity of the network connection to the target organization
  - traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
  - source of the attack is clearly identified unless a spoofed address is used
  - network performance is noticeably affected
Source Address Spoofing

- Use forged source addresses
  - usually via the raw socket interface on operating systems
  - makes attacking systems harder to identify
- Attack generates large volumes of packets that have the target system as the destination address
- Congestion results in the router connected to the final lower capacity link
- Requires network engineers to specifically query flow information from their routers
- Backscatter traffic
  - advertise routes to unused IP addresses to monitor attack traffic
SYN Spoofing

- Common DoS attack
- An attack on system resources, specifically the network handling code in the operating system
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
  - Goal → legitimate users are denied access to the server
Figure 7.2  TCP Three-Way Connection Handshake
**Figure 7.3** TCP SYN Spoofing Attack

1. **Attacker** sends SYN with spoofed src (seq = x)
2. **Server** sends SYN-ACK (seq = y, ack = x+1)
3. **Spoofed Client** resends SYN-ACK after timeouts
4. Assume failed connection request
5. SYN-ACK’s to non-existent client discarded
Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used
Flooding Attacks

- **ICMP flood**
  - ping flood using ICMP echo request packets
  - traditionally network administrators allow such packets into their networks because ping is a useful diagnostic tool

- **UDP flood**
  - uses UDP packets directed to some port number on the target system

- **TCP SYN flood**
  - sends TCP packets to the target system
  - total volume of packets is the aim of the attack
Distributed Denial of Service Attacks (DDoS)

- Use of multiple systems to generate attacks

- Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

- Large collections of such systems under the control of one attacker’s control can be created
  - E.g. forming a botnet
Figure 7.4 DDoS Attack Architecture
Figure 7.5  SIP INVITE Scenario
Hypertext Transfer Protocol (HTTP) Based Attacks

- **HTTP flood**
  - attack that bombards Web servers with HTTP requests
  - consumes considerable resources
  - *spidering*: bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

- **Slowloris**
  - attempts to monopolize by sending HTTP requests that never complete
  - eventually consumes Web server’s connection capacity
  - utilizes legitimate HTTP traffic
  - existing intrusion detection and prevention solutions that rely on signatures to detect attacks will generally not recognize Slowloris
Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- Basic defense against these attacks is blocking spoofed-source packets
DNS Reflection Attacks

Figure 7.6 DNS Reflection Attack
Amplification Attacks

Figure 7.7 Amplification Attack
DNS Amplification Attacks

- Packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source
DoS Attack Defenses

● These attacks cannot be prevented entirely

Why?

High traffic volumes may be legitimate

○ high publicity about a specific site
○ activity on a very popular site
○ described as slashdotted, flash crowd, or flash event
Defense against DDoS attacks

- Attack prevention and preemption
  - before attack
- Attack detection and filtering
  - during the attack
- Attack source traceback and identification
  - during and after the attack
- Attack reaction
  - after the attack
DoS Attack Prevention

- Block spoofed source addresses
  - on routers as close to source as possible

Filters may be used to ensure path back to the claimed source address is the one being used by the current packet

- filters must be applied to traffic before it leaves the ISP’s network or at the point of entry to their network
DoS Attack Prevention

- Use modified TCP connection handling code
  - cryptographically encode critical information in a cookie that is sent as the server’s initial sequence number
  - legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - drop an entry for an incomplete connection from the TCP connections table when it overflows
DoS Attack Prevention

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Follow general system security practices
- Use of mirrored and replicated servers when high-performance and reliability is required
Responding to DoS Attacks

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns
- Good Incident Response Plan
  - details on how to contact technical personnel for ISP
  - needed to impose traffic filtering upstream
  - details of how to respond to the attack
Responding to DoS Attacks

- Identify the type of the attack
  - capture and analyze packets
  - design filters to block attack traffic upstream
  - identify and correct system/application bug

- Have ISP trace packet flow back to source
  - may be difficult and time consuming
  - necessary if planning legal action
Responding to DoS Attacks

● Implement a contingency plan
  ○ switch to alternate backup servers
  ○ commission new servers at a new site with new addresses

● Update incident response plan
  ○ analyze the attack and the response for future handling
Summary

● Denial-of-service (DoS) attacks
  ○ network bandwidth
  ○ system resources
  ○ application resources
  ○ overwhelm capacity of network
  ○ forged source addresses (spoofing)
  ○ SYN spoofing/TCP connection requests

● Flooding attacks
  ○ ICMP flood
  ○ UDP flood
  ○ TCP SYN flood

● Distributed denial-of-service attacks (DDoS)
  ○ reflection attacks
  ○ amplification attacks
  ○ DNS amplification attacks

● Application-based bandwidth attacks
  ○ SIP flood
  ○ HTTP-based attacks

● Reflector and amplifier attacks
  ○ Reflection attacks
  ○ Amplification attacks
  ○ DNS amplification attacks