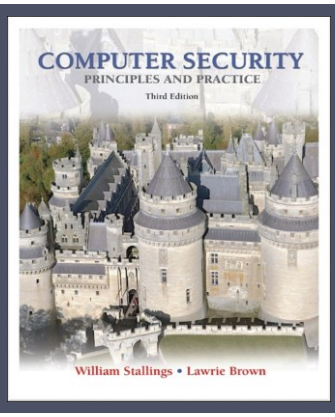


Chapter 7

Denial-of-Service Attacks

Denial-of-Service (DoS) Attack

The NIST Computer Security Incident Handling Guide defines a DoS attack as:

"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)

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:

Network bandwidth	System resources	Application resources
Relates to the capacity of the network links connecting a server to the Internet For most organizations this is their connection to their Internet Service Provider (ISP)	Aims to overload or crash the network handling software	Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

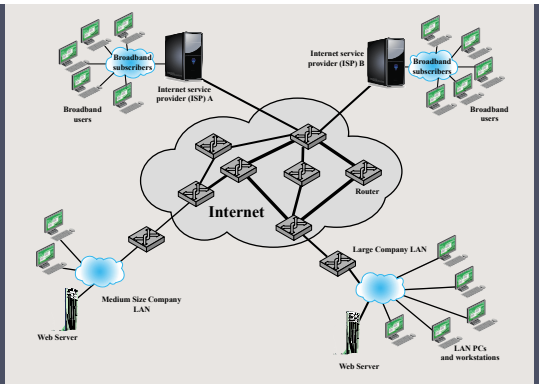


Figure 7.1 Example Network to Illustrate DoS Attacks

Classic DoS Attacks

- Flooding ping command
  - Aim of this attack is to 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
- Attacker generates large volumes of packets that have the target system as the destination address
- Congestion would result 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
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in the operating system

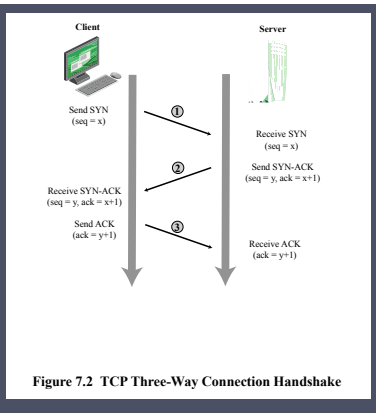


Figure 7.2 TCP Three-Way Connection Handshake

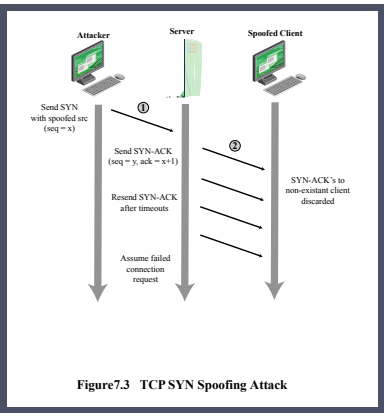


Figure7.3 TCP SYN Spoofing Attack

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

ICMP flood	• Ping flood using ICMP echo request packets • Traditionally network administrators allow such packets into their networks because ping is a useful network 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 rather than the system code

Distributed Denial of Service DDoS Attacks

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, forming a botnet

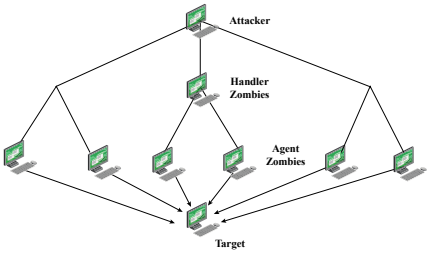


Figure 7.4 DDoS Attack Architecture

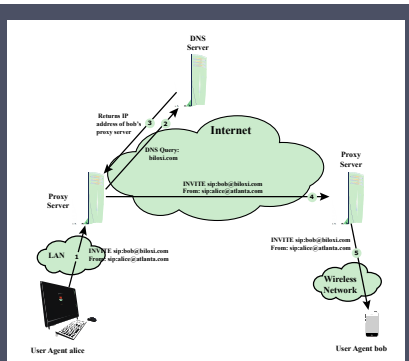


Figure 7.5 SIP INVITE Scenario

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
- The basic defense against these attacks is blocking spoofed-source packets

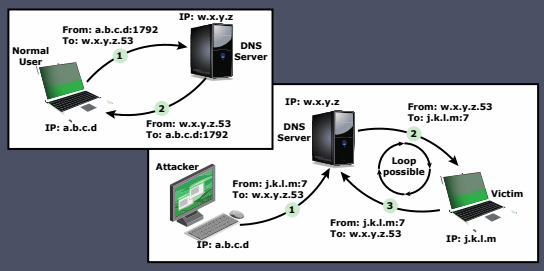


Figure 7.6 DNS Reflection Attack

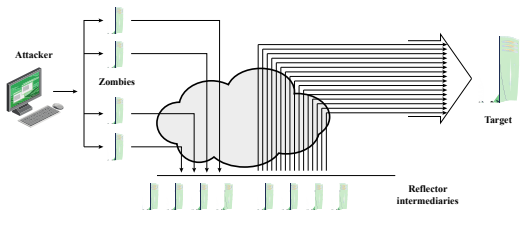


Figure 7.7 Amplification Attack

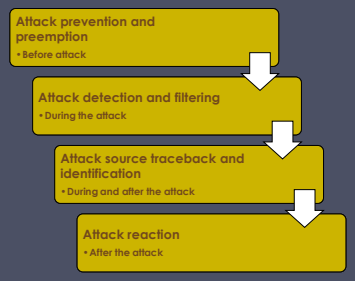
DNS Amplification Attacks

- Use 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 addresses

DoS Attack Defenses

- These attacks cannot be prevented entirely
- 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*

Four lines of defense against DDoS attacks



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
- 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
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks

Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

Responding to DoS Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or 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
- Implement 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 attacks
  - The nature of denial-of-service attacks
  - Classic denial-of-service attacks
  - Source address spoofing
  - SYN spoofing
- Flooding attacks
  - ICMP flood
  - UDP flood
  - TCP SYN flood
- Defenses against denial-of-service attacks
- Responding to a denial-of-service attack

- Distributed denial-of-service attacks
- Application-based bandwidth attacks
  - SIP flood
  - HTTP-based attacks
- Reflector and amplifier attacks
  - Reflection attacks
  - Amplification attacks
  - DNS amplification attacks