**Justin Ciocoi**

**Feb. 15, 2024**

# CSCI 400 Textbook Notes

## Chapter 7: Denial of Service Attacks

### 7.1: Denial of Service (DoS) Attacks

- NIST 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
- A DoS is an attack on availability and can affect any of the following resources
    - Network bandwidth
    - System resources
    - Application resources
- **Classic DoS Attacks**
    - Flooding ping command, which repeatedly sends pings in hopes of overwhelming the receiving server and rendering the network unavailable
    - Source address spoofing used the flooding ping command with a spoofed IP address to mask the source of the attack
    - SYN spoofing exploits the TCP handshake to similarly render a network unavailable
    - You can do a similar attack using UDP packets instead of TCP handshake packets

### 7.2: Flooding Attacks

- Flooding attacks are classified based on the network protocol that is used
- The intent of these attacks is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used
- **ICMP Flood**, which is a ping flood using ICMP echo request packets

- **UDP Flood**, where UDP packets are directed to some port number on the target system
- **TCP SYN Flood**, which sends TCP Packets to the target system

## 7.3: Distributed DoS (DDoS) Attacks

- A DDoS Attack is similar to a DoS attack, but leverages multiple systems or a botnet to generate attacks
- The attacker will use a flaw in an OS or a common application to gain access and install their program on the system
- This makes DoS far more potent due to the much higher resource capabilities of a botnet when compared to a single system

## 7.4: Application-Based Bandwidth Attacks

- **HTTP Based Attacks**
    - **HTTP Flood**
        - These attacks bombard servers with HTTP requests
        - consume considerable resources
        - They will follow all links on the web in a recursive manner
    - **Slowloris**
        - Attempts to monopolize by sending HTTP requests that never complete, which eventually consumes the web server's connection capacity
        - Utilizes legitimate HTTP traffic
        - Intrusion detection relying on signatures will generally not recognize this attack

## 7.5: Reflector and Amplifier Attacks

- **Reflection Attacks**
    - In a reflection attack, an attacker will send packets to a known service on an intermediary with a spoofed source address of the actual target system
    - When the response is received, it is sent to the target
    - The intermediary *reflects* the attack and acts as a **reflector**

    - The goal is to generate enough packet volume to flood the link to the target system without alerting the intermediary
    - The basic defense against these attacks is to block spoofed-source packets
- **DNS Amplification Attacks**
    - Use packets directed at a legitimate DNS server as the intermediary system, and the attacker creates a series of requests containing the spoofed address of the target system
    - Attacker will then exploit the DNS behavior to amplify the response volume and flood the target with DNS responses
- **DoS Attack Prevention**
    - Block spoofed source addresses
    - Use a modified TCP connection handling code
    - Block suspicious services

## 7.6: Defenses against DoS

- There is no way to entirely prevent DoS attacks considering there is always a chance that there will be entirely legitimate high traffic volumes
- There are four lines of defense against DDoS attacks
    - Before the attack, prevention and preemption
    - During the attack, detection and filtering
    - During and after the attack, source traceback and identification
    - After the attack, reaction
- There are a number of ways in which you can help prevent DoS attacks
    - Blocking spoofed source addresses on routers as close to the source as possible
    - Filters can be used to make sure that the path the packet is claiming to have taken is the actual path taken by the packet
    - Use modified TCP connection handling code such that TCP SYN flooding becomes infeasible

    - Block IP directed broadcasts
    - Block suspicious services and combinations
    - Manage application attacks with a form of graphical puzzle (i.e. captcha) to distinguish legitimate human requests
    - Use mirrored and replicated servers when high-performance and reliability is required

## 7.7: Responding to a DoS

- A good incident response plan has details for the ISP to contact technical personnel, as well as details of how to respond to the attack itself
- Ideally, network monitors are in place to detect abnormal traffic patterns
- Identification of the attack
    - Packets must be captured and analyzed
    - Filters should be used to block attack traffic upstream
- Have ISP trace packet flow back to source
    - This may be difficult and time consuming
    - This theoretically finds the source of the attacker and is a necessary step if legal action is to be pursued
- Implement a contingency plan
    - Backup servers should be in place
    - New servers at a new site with new addresses should be commissioned
- Update the incident response plan and analyze what failures may have led to the attack that was experienced