**Module 10: Denial of Service**

**Basic Categories of DoS/DDOS Attack Vector**

* Volumetric Attacks:
  + Consume the bandwidth of a target network or service.
  + The magnitude of attack is measured in **bits-per-second (bps)**
  + Types of bandwidth depletion attacks
    - **Flood attacks**: Zombies send large volumes of traffic to the victim’s system to exhaust the bandwidth of these systems
    - **Amplification attacks:** The attacker or zombies transfer messages to a boradcast IP address. This method amplifies malicious traffic that consumes the bandwidth of the victim’s system
  + Techniques:
    - UDP flood attack
    - ICMP flood attack
    - Ping of Death attack
    - Smurf attack
    - Pulse wave attack
    - Zero-day attack
    - Malformed IP packet flood attack
    - Spoofed IP packet flood attack
* Protocol Attacks
  + Consume other types of resources like **connection state tables** present in network infrastructure component such as **load-balander, firewalls, and application servers**
  + The magnitude of attack is measured in **packets-per-second (pps)**
  + Techniques:
    - Syn flood attack
    - Fragmentation attack
    - Spoofed session flood attack
    - ACK flood attack
    - RST attack
    - TCP state exhaustion attack
    - TCP connection flood attack
* Application Layer Attacks
  + Consume the resources or services of an application, thereby making the application unavailable to other legitimate users
  + The magnitude of attack is measured in requests-per-second (rps)
  + Techniques:
    - HTTP GET/POST attack
    - Slowloris attack
    - UDP application layer flood attack

**DoS/DDoS Attack Techniques**

* **UDP flood attack**
  + An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a larget src IP range
  + The flooding of UDP packets causes the server to repeatedly check for **non-existent applications** at the ports
  + Legitimate apps are inaccessible by the system and give an error reply with an ICMP “Destination Unreachable” packet
* **ICMP flood attack**
  + A type of attack in which attackers send large volumes of **IMCP echo request packets** to a victim system directly or through relection networks
  + To protect against this attack, set a threshold limit that invokes an ICMP attack protection feature when exceeded
* **PoD (Ping of Death) attack**
  + An attacker tries to crash,destabilize, of freeze the targeted system or service by sending malformed or oversized packets using a simple ping command
  + Ex: Send a packet which has a size of 65538 bytes
* **Smurf attack**
  + Spoof the source IP address with the victim’s IP address and sends a large number of ICMP echo request packets to an IP broadcast network
  + Cause all the hosts on the broadcast network to respond to the received ICMP echo request.
* **Pulse wave attack**
  + Attackers send a **highly repetitive periodic train of packets as pulses** to the target victim every 10 minutes, and each specific attack session can last for a few hours to days.
  + A single pulse (300 Gbps or more) is sufficient to ccrowd a network pipe
* **Zero-day attack**
  + This attack is delivered before the DDoS vulnerabilities of a system have been patched of effective defensive mechanisms are implemented
* **SYN flood attack**
  + Send a large number of SYN requests with fake source IP addresses to the target
  + Take advantage of a flaw in the implementation of the TCP three-way-handshake in most hosts
  + When server receives the SYN request, it must keep track of the partially opened connection is a listen queue for at least **75 seconds.**
  + Countermeasures: Poper packet filtering
* **Fragmentation attack**
  + Stop a victim from being able to re-assemble fragmented packets by flooding the traget system with TCP or UDP fragments. Attackers send a larger number of fragmented packets to a target web server with a relatively small packet rate
  + Ressembling and inspecting these large fragmented packets cinsumes excessive resources. Morever, the content in the packet fragments will be randomized by the attacker, which in turn makes the process consume more resources
* **ACK flood attack**
* **TCP state exhaustion attack**
* **Spoofed session flood attack**
  + Attackers **create fake or spoofed TCP sessions** by carring multiple **SYN, ACK,** and **RST or FIN packets**
  + Attackers employ this attack to bypass firewalls and perform DDoS attacks against target network, exhausting its network resources
  + Multiple SYN-ACK Spoofed Session Flood Attack: Create a fake session with **multiple SYN and muiltiple ACK packets** along with **one or more RST or FIN packets**
  + Multiple ACK Spoofed Session Flood Attack: Attackers create a fake session by **completely skipping the SYN packets** and using only multiple ACK packets along with **one or more RST or FIN packets**
* **HTTPS GET/POST attack**
  + HTTP GET attack: Use a time-delayed HTTP header to maintain HTTP connection and exhauste web server resources
  + HTTP POST attack: Send HTTP requests with complete headers but with incomplete message bodies to the target, prompting the server to wait for the rest of the message body,
* **Slowloris attack**
  + Send partial HTTP requests to the target
  + Upon receiving the partial HTTP requests, the target opens multiple open connections and keeps waiting for the request to complete
  + These requests will not be complete, and the target server’s maximum concurrent connection pool will be exhausted, and additional connection attemps will be denied.
* **UDP application layer flood attack**
  + SSDP
  + NTP
  + VoIP
  + TFTP
  + RPC
  + …
* Multi-vector attack
  + Use **combinations** of vollumetric, protocol, and application-layer attacks to disable the target
* **Peer-to-peer attack**
  + Attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim’s fake website
  + Exploits flaws found in the network using the DC++ (Direct Connect) protocol, which is used for sharing all types of files between instant messaging clients
  + Attacks launch massive DoS and compromise websites.
* **Permanent DoS (PDoS) attack**
  + **Phlashing:** Permanent DoS, also known as plashing, refers to attacks that cause ireversible damage to system hardware
  + **Sabotage:** Unlike other DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware
  + **Bricking a system:** This attack is carried out using a method known as bricking a system. Using this method, attackers send fraudulent hardware updates to the victims
* **Distributed relection DoS (DRDoS) attack**
  + Also known as a spoofed attack, involves the **use of multiple imtermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
  + Launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn **reflect the attack traffic to the target,**
  + Adv: The primary target seems to be directly attacked by the secondary victim rather than the actual attacker. Multiple intermediary victim servers are used, which results in an increase in attack bandwidth
  + **Countermeasure:** Turn off the CHARGEN (Character Generator Protocol) service to stop this attack method.

**Botnets**

* Software apps that **run automated tasks** over the Internet and perform simple repetitive tasks.
* A huge network of compromised systems and can be used for launching DoS

**Scanning methods for finding vulnerable machines**

* **Random Scanning:** The infected machine probes IP addresses randomly from the target network IP range and checks for vulnerabilities
* **Hit-list scanning:** First collects a list of potentially vulnerable machines and then scans them to find vulnerable machines
* **Topological Scanning:** Use information obtained from an infected machine to find new vulnerable machines
* **Local Subnet Scanning:** The infected machine looks for new vulnerable machines in its own local network
* **Permutation Scanning:** Use a pseudorandom permutation list of IP addresses to find new vulnerable machines

**How Does Malicious Code Propagate?**

* **Central Source Propagation:** Place an attack toolkit on the central source, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system
* **Back-chaining Propagation:** Place an attack toolkit on his own system, and a copy of the attack toolkit is transferred to the newly discovered vulnerable system
* **Autonomous Propagation:** Host itself transfers the attack toolkit to the newly discovered vulnerable system at the exact time that it breaks into that system

**DDos Case Study: DDoS attack on github**

* The world’s largest DDoS attack ever recorded
* Take place on Wed,28 Feb 2018
* Make github’s service unavailable for 4 min
* An amplification attack using a Memcached-based approach that peaked at 1.35Tbps

**Tools**

* **HOIC (High Orbit Ion Cannon):** Carry out a DDoS to attack any IP with a user selected port and a user selected protocol
* **LOIC (Low Orbit Ion Cannon):** Can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests wit hthe intention of disrupting the service of a particular host

**Detection Techniques**

* Based on identifying and discriminating illegitimate traffic increases and flash events from legitmate packet traffic
* **Activity Profiling:** Based on the average packet rate for a network flow
* **Sequential Change-Point Detection:** Use Cusum (Cumulative Sum) algorithm to identify and locate DoS attacks. Can also be used to identify the typical scanning activities of network worms
* **Wavelet-Based Signal Analysis:** Describe an input signal in terms of spectral components. Analyzing each spectral window’s energy determines the presence of anomalies. Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise.

**DoS Countermeasure Strategies**

* Absorbing the Attack
* Degrading Service
* Shutting Down the Services
* Countermeasures:
  + Protect Secondary victims
  + Detect and neutralize handlers
  + Prevent potential attacks
    - Egress filtering
    - Ingress filtering
    - TCP intercept
    - Rate limiting
  + Deflect attacks:
    - Set up honeypots
    - Tool: **KFSenso**r acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans.
  + Mitigate attacks
    - **Load Balancing**
    - **Throttling:** Set routers to access a server with a logic that throttles incoming traffic levels to be safe for the server. Help in preventing damage to servers by controlling DoS traffic. Help router manage heavy incoming traffic. Filter legitimate user traffic from fake DDoS attack traffic
    - **Drop requests**
  + Post-attack forensics
    - Traffic Pattern Analysis
    - Packet Traceback
    - Zombie Zapper Tool
    - Event Log Analysis

**Techniques to Defend against Botnets**

* **RFC 3704 Filtering:** Limit the impack by denying traffic with spoofed address.
* **Cisco IPS Source IP Reputation Filtering:** Help in determining if an IP or a service is a source of threat. Cisco IPS regularly updates its database with known threats such as botnets…
* **Black Hole Filtering:** Refer to a network node where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient.
* **DDoS Prevention Offerings from ISP of DDoS Service:** Enable IP Source Guard or similar features in other routers to filter traffic based on the DHCP snooping binding database or…

**Advanced DDoS Protection Appliances**

* FortiDDoS-1200B
* DDoS Protector
* Terabit DDoS Protection System
* A10 Thunder TPS
* Tools: Imperva Incapsula DDoS Protection
* Services: Akamai DDoS Protection