CCIE Security Version 5
Advanced Technologies Class

DoS and DDoS Attacks

What is a DoS/DDoS attack?

What are the identification and mitigation tools?

DoS and DDoS Overview

- Denial Of Service (DoS) attacks
  - Aimed to disrupt network/host/service availability
  - Sourced from a single system or a small number
  - Less common nowadays, as it's no longer effective
  - Usually it's a simple attack

DoS and DDoS Overview

- Distributed Denial Of Service (DDoS) attacks
  - Aimed to disrupt network/host/service availability
  - Sourced from large number of sources (botnets)
  - More common nowadays, very effective
  - Usually it's a complex attack, or a mix of multiple

DoS and DDoS Overview

- DoS and DDoS can be of three types
  - Volume based
  - Protocol based
  - Application based
- Cisco uses another categorization
  - http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html#13

Volume Based Attacks

- Volume based (most common)
  - Victim is flooded with a high volume of connections and/or packets
  - Attacker's scope is to saturate the bandwidth of the victim
  - It is measured in bits per second
- Examples
  - ICMP and UDP floods
  - NTP and DNS reflection/amplification attacks

Volume Based Attacks

- Reflection attack
  - The attacker spoofs the victim's IP address
  - The attacker initiates a large amount of requests with spoofed source
  - Responder's will reply to the victim, flooding it, causing a DDoS
- Amplification attack
  - An enhanced version of the reflection attack
  - The attacker's request will force a large/big reply

Protocol Based Attacks

- Protocol based
  - Victim is flooded with a high volume of connections and/or packets
  - Attacker's scope is to consume actual server resources or network equipment resources (firewall, balancers)
  - It is measured in packets per second
- Examples
  - TCP SYN floods, IP fragmentation attacks, Ping of Death

Application Based Attacks

- Application based
  - Victim receives legitimate requests that are aimed to exploit protocol/application vulnerability
  - Attacker's scope is to crash the server/service by forcing the application to allocate maximum resources per request
  - It is measured in requests per second
- Examples
  - Low and slow attacks like HTTP GET/POST floods

DoS and DDoS Mitigation

- In DoS and DDoS mitigation we always have two steps
  - Attack identification
  - Attack mitigation
- Attack identification and mitigation tools
  - http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html#44

DoS and DDoS Evolution

- Due to more and more unsecure devices being connected to the Internet (IoT)
  - More botnets showed up, which facilitated volume-based attacks
  - http://thehackernews.com/2013/03/worlds-biggest-ddos-attack-that-almost.html
  - http://thehackernews.com/2014/02/NTP-Distributed-Denial-of-Service-DDoS-attack.html
  - http://thehackernews.com/2016/01/biggest-ddos-attack.html
  - http://thehackernews.com/2016/09/ddos-attack-iot.html

Malware As A Service