CCIE Security Version 5 Advanced Technologies Class

TCP Attacks

What is the TCP attack?

What IOS tools can be used to mitigate it?

TCP Attacks Overview

▷TCP is connection-oriented by design

- A three-way handshake needs to be established before session is opened
- TCP consumes more resources on the end-hosts, which makes it a great attack vector

TCP Session Hijacking Overview

- ▷TCP sequence number guessing/spoofing
  - Attacker identifies the TCP sequence numbering of a TCP sessions and hijacks the session
  - It can inject spoofed payload or RST/FIN the session

TCP Session Hijacking Overview

- There are two methods
  - Non-blind spoofing (attacker is in the transit path of the TCP session)
  - Blind spoofing (attacker needs to break the TCP sequence number algorithm) http://thehackernews.com/2016/08/linux-tcp-packet-hacking.html

TCP Session Hijacking Mitigation

- Specific only to this attack
  - Sequence number randomization by a transit firewall (like ASA firewall)

TCP SYN Flood Overview

▷TCP SYN Flood

- Victim is flooded with large amount of TCP SYN packets, but attacker never finishes the three-way handshake
- Victim consumes all resources with half-opened/ embryonic TCP sessions

TCP SYN Flood Mitigation

- Specific only to this attack
  - TCP Intercept
  - http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html

TCP Attack Mitigation

▷IOS Mitigation Tools

- ACL Filtering
- Rate-limit (CAR – Committed Access Rate)
- Policing (successor of CAR)
- Unconditional packet discard via MQC (ACL/NBAR)
- uRPF
- Zone-Based Policy Firewall

Knowledge is Power!