CCIE Security Version 5
Advanced Technologies Class

TCP Intercept

What is the TCP intercept?

What should be taken into account when deploying it?

TCP Intercept Overview

- A network device will be configured to
  - Intercept TCP sessions (act like a TCP proxy/MiTM)
- TCP Intercept is pseudo-defined in RFC 4987

TCP Intercept Overview

- With TCP intercept active, there will be two TCP sessions in the beginning
  - First between the attacker and the network device
  - Second between the network device and the victim
- If the three-way handshake of first session is established
  - The network device joins the two TCP sessions together
  - Outcome is one legit end-to-end TCP session, between client and server

TCP Intercept Overview

- If the three-way handshake of first session is not established
  - The network device should kill the half-open/embryonic TCP session

TCP Intercept Overview

- The router will start killing embryonic sessions
  - When the upper limit of configured embryonic sessions has been reached
- The router will stop killing embryonic sessions
  - When the lower limit of configured embryonic sessions has been reached

TCP Intercept Overview

- It can be configured
  - As a standalone feature
  - As part of CBAC and Zone-Based Policy Firewall

TCP Intercept Overview

- If the victim does not respond
  - The router will probe it repeatedly using en exponential algorithm
  - SYN is retransmitted after 1,2,4,8,16 seconds and if no SYN ACK is received, session is terminated
- When the upper limit of embryonic sessions is reached
  - The above algorithm happens twice faster

TCP Intercept Functional Modes

- The standalone option can be implemented in two modes
  - Intercept mode
  - Watch mode

TCP Intercept in Intercept Mode

- Running in Intercept mode
  - The network device will proxy for all TCP sessions
  - It will join together valid sessions and kill embryonic sessions as configured
- Problem is that the victim becomes the router now
  - Router's CPU has less performance in general than a server's CPU (different architecture)

TCP Intercept in Watch Mode

- Running in Watch mode
  - The network device will passively monitor all TCP sessions
  - The network device kicks-in to proxy for TCP sessions only when upper limit of embryonic has been reached
  - It will join together valid sessions and kill embryonic sessions as configured
- It's more CPU friendly with the network device
  - Safer to implement

IOS TCP Intercept

- IOS TCP Intercept implementation steps
  - Configure the TCP intercept functional mode
  - Configure embryonic session thresholds
  - Configure the drop mode for embryonic sessions
  - Verify its functionality