CCIE Security Version 5
Advanced Technologies Class

ICMP Attacks

What is the ICMP attack?

What IOS tools can be used to mitigate it?

ICMP Attacks Overview

- ICMP is unidirectional and connectionless (except ping)
  - It was designed to help diagnose and troubleshoot network/service issues
  - Because of its nature, it's a powerful attack vector
  - http://resources.infosecinstitute.com/icmp-attacks/#gref

ICMP Attacks Overview

- Port Scanning and OS fingerprinting
  - Relies on ICMP Port Unreachable and ICMP Echo-Request/Echo-Reply
- Network Topology Discovery
  - Relies on traceroute
- Smurf Attacks
  - Relies on spoofed ICMP Echo-Request sent to the broadcast address of the subnet
  - Among the first reflection attacks

ICMP Attacks Overview

- Host routing table modification for MiTM attacks
  - Relies on ICMP Redirects, ICMP Router Discovery messages
- Smurf Attacks
  - Relies on spoofed ICMP Echo-Request sent to the broadcast address of the subnet
  - Among the first reflection attacks
- ICMP Tunneling
  - Relies on data injection into ICMP Echo-Request/Echo-Reply payload

ICMP Attack Mitigation

- IOS Mitigation Tools
  - Ensure directed broadcast is disabled (Smurf attack)
  - ACL Filtering
  - Rate-limit (CAR – Committed Access Rate)
  - Policing (successor of CAR)
  - Unconditional packet discard via MQC (ACL/NBAR)
  - uRPF
  - Zone-Based Policy Firewall

NBAR2 Resources

- NBAR2
  - http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_c67-697963.html
  - https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76539&backBtn=true

ICMP Attack Mitigation

- MQC Mitigation Implementation Steps
  - Classify the traffic via NBAR/NBAR2 (class-map)
  - Configure policy to drop traffic (policy-map)
  - Apply the policy at the interface-level (service-policy)
  - Enable NBAR at the interface level
  - Verify its functionality