Implementing Secure Converged Wide Area Networks (ISCW)

Network Security Strategies & Cisco Device Hardening

http://www.INE.com

Attack Mitigation Overview

- Layer 2 attack review
  - VLAN hopping
  - CAM attacks
  - DHCP starvation
  - Rogue DHCP
  - ARP poisoning
  - IP/MAC spoofing
- What about layer 3 and above?

Reconnaissance Attacks

- Used to map the network and discover resources
  - What are the routers, links, routing tables, hosts, etc.
- Common methods
  - Packet capture (sniffers)
  - Ping sweeps
  - Port scans
  - DNS queries

Control Plane Attacks

- Disrupt the routing & management protocols of the network
- Common methods
  - Prefix injection/withdrawal
  - BGP reset
  - Telnet passwords
  - SNMP community strings
  - NTP spoofing

Access Attacks

- Used to gain unauthorized access to resources
- Common methods
  - Brute force password attacks
  - Redirection
  - Layer 3 Man-in-the-Middle (MiM)

DoS/DDoS Attacks

- Used to overwhelm links and servers to the point they are unusable
- Common methods
  - IP spoofing
  - Smurf
  - Fraggle
  - TCP SYN flooding

Application Attacks

- Targeted at software vulnerabilities
- Common methods
  - Buffer overflows
  - Worms
  - Viruses
  - Trojans
  - etc.

Reconnaissance Mitigation

- How are they mapping the network in the first place?
  - ICMP
    - Echo-reply
    - Unreachable
    - Mask reply
    - Redirect
  - Proxy ARP
  - CDP
- How to mitigate?
  - Disable unneeded services
  - IPS

Control Plane Attack Mitigation

- Why is the control vulnerable?
  - No routing authentication
  - Promiscuous routing neighbors
  - Clear text telnet & SNMP passwords
  - No NTP authentication
- How to mitigate
  - Routing authentication
  - Unicast updates
  - SSH
  - SNMPv3
  - NTP authentication

Access Attack Mitigation

- Why is access vulnerable?
  - Lenient password retry policy
  - Clear text strings in protocol payloads
  - Hosts vulnerable to redirection
- How to mitigate?
  - AAA & lockouts
  - SSL/IPsec
  - HIPS

DoS/DDoS Attack Mitigation

- Why are we vulnerable?
  - TCP stack connection limits
  - Flood attack amplification
  - Input packets not RPF checked
- How to mitigate
  - Half-open session monitoring
  - Disable directed broadcasts
  - RFC 3704 / BOGON / URPF

Application Attacks

- Why are we vulnerable?
  - Patch application not enforced
  - Virus scan updates not enforced
- How to mitigate?
  - NAC

Disabling Unneeded Services Examples

- Manually via CLI
- Auto-secure
- SDM audit & lockdown

Securing the Control Plane Examples

- Passwords, privileges, & AAA
- Role based CLI
- Disabling Telnet
- Enabling SSH
- Disabling SMNP v1/v2
- NTP authentication
- Logging sequence numbers
- Banners

DoS Mitigation Examples

- URPF
- BOGON filtering
- TCP Intercept / CBAC
- Disabling directed broadcasts

Q&A