SWITCHING SECURITY

PRESENTED BY: Michelle Opiyo

Switching security

- Port Security
- Understanding Switch Security Issues
- Protecting Against VLAN Attacks
- Protecting Against Spoofing Attacks
- Securing Network Services
- Secure Network Switches to Mitigate Security Attack

PORT SECURITY

VULNERABILITIES

- A switch that does not provide port security allows an attacker to attach a system to an unused, enabled port and to perform information gathering or attacks.

COUNTERMEASURES

- Shutdown unused ports
- Enable only specific mac- addresses on specific ports

e.g, **switchport port-security mac-address sticky**

errdisable recovery cause psecure-violation global config to unshut a port

VLAN ATTACKS

VULNERABILITIES

- By default all ports are on VLAN 1
- Private VLANs (P-VLANs) separated on layer 2 but not necessarily layer 3
- VTP allows the addition, deletion and renaming of VLANs on a network-wide basis within a VTP management domain.

COUNTERMEASURES

- Don’t use VLAN for management
- Don’t trunk the management VLAN off the switch. Use dedicated switch for that
- Combine PVLANs with Router ACLs
- Generally best to disable VTP or set on transparent mode, password protected

CONT’D…

VULNERABILITIES

- Using DTP whose default setting is dynamic desirable

COUNTERMEASURES

- Set switch-port as either trunk or access not auto negotiate
- Allow only specific VLANS on the trunk
- Use unique native VLAN for each trunk on a switch

SPANNING TREE PROTOCOL

VULNERABILITIES

- A vulnerability associated with STP is that a system within the network can actively modify the STP topology. There is no authentication that would prevent such an action. The bridge ID, a combination of priority (less is best) and MAC address(lower is best), determines the root bridge within a network.

COUNTERMEASURES

- Using portfast BPDU guard to enforce STP topology. Global or port configuration. spanning-tree portfast bpduguard default spanning-tree portfast bpduguard default
- Using spanning tree root guard. Allows participation in STP unless port attempts to become a root port. Switch(config-if)# spanning-tree guard root

ACCESS CONTROL LISTS

VULNERABILITIES

- Lack of ACLs or very permissive ACLs. Remember that ACLs deny or permit access based on the 1st ACL statement that the packet macthes.
- Poorly designed ACLs can also affect services that use protocols such as SIP, H.323 etc

COUNTERMEASUERS

- Categorize systems attached to the switches into groups that use the same network services. Grouping systems this way helps reduce the size and complexity of associated ACLs.

LOGGING AND DEBUGGING

VULNERABILITES

- Poor configuration and monitoring leads to inadequate information on attacks

COUNTERMEASURES

- Enable logging
- Configure appropriate trap levels
- Set up a separate logging server
- Ensure you have a good NTP server

QUESTIONS?