kenet
Kenya Education Network

NETWORK SECURITY 1

KENET TRAINING

Transforming education through ICT

Layer 2 Security

- The BP recommendations for switch port security depend on the following characterizations
  - Unused ports
  - User ports
  - Trusted ports/trunk ports

Strategies: Used and Unsed Ports

- Disable unneeded dynamic protocols like CDP and DTP
- Disable trunking
- Enable BPDU Guard and Root Guard to prevent STP attacks
- Enable DAI or Private VLANs
- Enable port security. Limit Mac adresses
- Use 802.1X user authentication
- Use DHCP snooping and IP Source Guard to prevent DHCP DoS and man in the middle attacks

Additional Recommendations

- 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

Counter Measures

- Shutdown unused ports
- Enable only specific mac- addresses on specific ports
- Configure port security violation
- Specify specific on all trunk links

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

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

VLAN SECURITY

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.

Using DTP configurations whose DTP trunking mode is Dynamic desirable

Counter Measures

- Don’t use VLAN 1 for management
- Propagate the Management VLAN on links that connect to your switches only
- 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. If you have to use VTP then upgrade the switch IOS and use VTP version 3
- Disable automatic trunking. Make the interfaces either DTP Protocol negotiate or non-negotiate. Hard code the interfaces whenever possible.

VLAN SECURITY Cont.

Counter Measures

- Don’t use VLAN 1 for management
- Propagate the Management VLAN on links that connect to your switches only Combine PVLANs with Router ACLs
- Generally best to disable VTP or set on transparent mode, password protected. If you have to use VTP then upgrade the switch IOS and use VTP version 3
- Disable automatic trunking. Make the interfaces either DTP Protocol negotiate or non-negotiate. Hard code the interfaces whenever possible.
- 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

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.

Counter Measures

- 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
- STP bridge assurance
- STP dispute
- Configuration setting. Switch(config-if)# spanning-tree guard root

SPANNING TREE PROTOCOL Cont

- **UDLD** – Uni-Directional Link Detection puts unidirectional links into blocking state and prevents forwarding loops.
- **BPDU Guard** – disables ports that receive a BPDU frame; useful for edge ports that should never be connected to another switch.
- **Loop Guard** – Protects against ports where the link becomes unidirectional. It operates differently than the UDLD function.
- **Root Guard** – Prevents a port from becoming a root port or a blocked port.
- **EtherChannel Guard** – Prevents inconsistent configuration of EtherChannel that creates loops between two switches.
- **Bridge Priority** – Defines the root bridge in an STP domain

Bridge Assurance

Bridge Assurance only runs in RSTP or MST networks. It makes sure that a neighboring switch does not malfunction and begin forwarding frames when it shouldn't. It does this by monitoring receipt of BPDUs on point-to-point links. When the BPDUs stop being received, the port is put into blocking state (actually a port inconsistent state, which stops forwarding). When BPDUs restart, the port resumes normal RSTP or MST modes. This handles unidirectional links as well as the malfunction of a neighboring switch where STP stops sending BPDUs but the switch continues to forward frames.

STP DISPUTE

Currently, this feature is not present in the IEEE MST standard, but it is included in the standard-compliant implementation. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops.

When a designated port detects a conflict, it keeps its role, but reverts to a discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

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

COUNTERMEASURES

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

kenet
Kenya Education Network

Questions

kenet
Kenya Education Network

Transforming education through ICT

Thank You

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500