kenet
Kenya Education Network

NETWORK SECURITY 2

KENET TRAINING

Transforming education through ICT

Layer 2 Security

- **WHY SECURE OUR SWITCHES**
  - Most vulnerabilities are inherent to the Layer 2 protocols from STP to IPV6 discovery
  - If Layer 2 is compromised, it is easier to build attacks on upper-layers protocols by using techniques such as man-in-the-middle (MITM) attacks
  - To exploit Layer 2 vulnerabilities, an attacker must usually be Layer 2 adjacent to the target.

Vulnerabilities exploited

- Defeating a Learning Bridge's Forwarding Process: MAC Flooding attacks
- Attacking the Spanning Tree Protocol: Yersinia
- Leveraging DHCP Weaknesses
- VLANS
- Information Leaks with Cisco Ancillary Protocols EG CDP,VTP,DTP

Defeating a learning bridge forwarding

- Mac flooding attacks-Forwarding table occupy memory therefore are finite;

  Macof-Sends Ethernet frames to random destination modifying SA each time

- Detecting Mac activity and notification
- Port security
- Unknown unicast flooding protection

Port Security

```
6K-2-S2# show port-security interface f8/4
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Maximum MAC Addresses      : 3
Total MAC Addresses        : 3
Configured MAC Addresses   : 0
Last Source Address        : 4428.6d15.b219
Security Violation Count   : 9
```

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 1

Switchport port-security violation restrict

Switchport port-security mac-address sticky

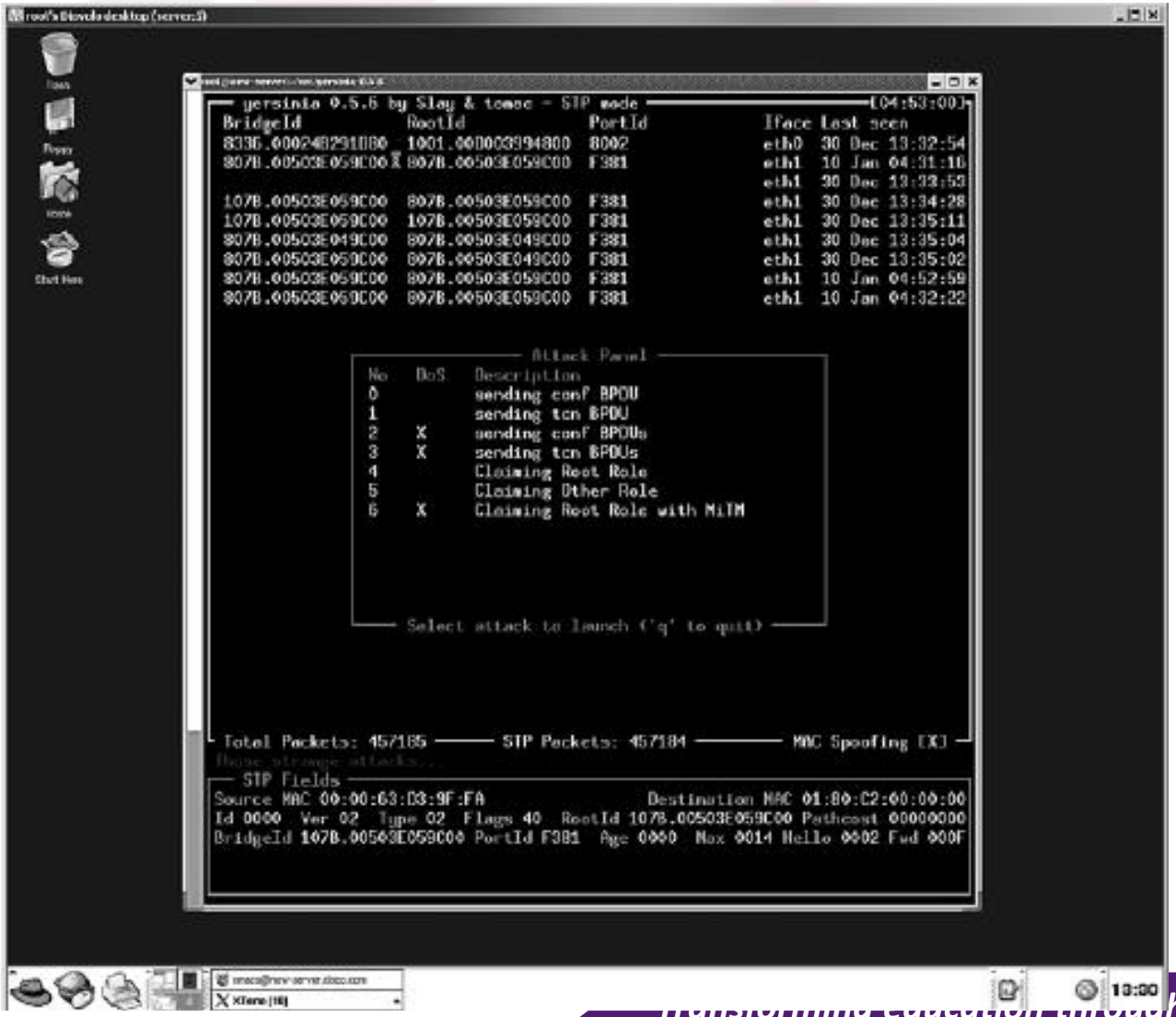
SPANNING TREE PROTOCOL

STP is trustful and does not provide any authentication mechanism

STP ATTACKS. (Yersinia)

- Taking over the root role
- Sending raw configuration BPDU
- DoS attacks sending raw BPDU

SPANNING TREE PROTOCOL Cont



SPANNING TREE PROTOCOL Cont

- **TAKING OVER THE ROOT ROLE**

Forging artificially low bride priorities

```
6K-2-S2#show spanning-tree vlan 123 interface f8/1 detail
 Port 897 (FastEthernet8/1) of VLAN0123 is root forwarding
   Port path cost 19, Port priority 240, Port Identifier 240.897.
   Designated root has priority 32891, address 0050.3e04.9c00
   Designated bridge has priority 32891, address 0050.3e04.9c00
   Designated port id is 240.897, designated path cost 0
   Timers: message age 15, forward delay 0, hold 0
   Number of transitions to forwarding state: 2
   Link type is point-to-point by default
   Loop guard is enabled by default on the port
   BPDU: sent 29, received 219
6K-2-S2#
! The previous command show the status of the port for a given VLAN, and
! the number of BPDU received on the port. Here, something abnormal is
! happening: a root port should typically be sending many more BPDUs than
! it is receiving. The opposite is taking place here, indicating suspicious
! activity.
6K-2-S2#sh spanning-tree bridge address ¦ inc VLAN0123
VLAN0123         0050.3e05.9c00
6K-2-S2#
6K-2-S2#sh spanning-tree vlan 123 root

                                        Root    Hello Max Fwd
Vlan                Root ID             Cost    Time  Age Dly  Root Port
---------------- ------------------- --------- ----- --- ---  ------------
VLAN0123         32891 0050.3e04.9c00        19    2   20  15  Fa8/1
6K-2-S2#
```

SPANNING TREE PROTOCOL Cont

- **DoS Attacks using a flood of configured BPDUs**
- Yersinia generates 25,000 BPDUs per second on test machine

```
6K-3-S720#remote command switch show proc cpu ¦ incl second
CPU utilization for five seconds: 99%/86%; one minute: 99%; five minutes: 76%
```

```
6K-3-S720#show spanning-tree vlan 123 interface f8/1 detail
 Port 897 (FastEthernet8/1) of VLAN0123 is root forwarding
   Port path cost 19, Port priority 240, Port Identifier 240.897.
   Designated root has priority 0, address 9838.9a38.3cf0
   Designated bridge has priority 52067, address 9838.9a38.3cf0
   Designated port id is 0.0, designated path cost 0
   Timers: message age 20, forward delay 0, hold 0
   Number of transitions to forwarding state: 4
   Link type is point-to-point by default, Peer is STP
   BPDU: sent 1191, received 7227590
```

- Logging-event spanning-tree status

```
5w2d: %SPANTREE-SP-6-PORT_STATE: Port Fa5/14 instance 1448 moving from blocking
  to blocking
5w2d: %SPANTREE-SP-6-PORT_STATE: Port Fa5/14 instance 1448 moving from blocking
  to forwarding
```

SPANNING TREE PROTOCOL Cont

- **Counter measures**
- **BPDU Guard**

```
6K-2-S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
6K-2-S2(config)#int f8/1
6K-2-S2(config-if)#spanning-tree bpduguard enable
6K-2-S2(config-if)#exit
6K-2-S2(config)#exit
6K-2-S2#
6K-2-S2(config)#errdisable recovery cause bpduguard
6K-2-S2(config)#errdisable recovery ?
  cause     Enable error disable recovery for application
  interval  Error disable recovery timer value

6K-2-S2(config)#errdisable recovery inter
6K-2-S2(config)#errdisable recovery interval ?
  <30-86400>  timer-interval(sec)

6K-2-S2(config)#errdisable recovery interval 30
```

- Immediately a BPDU is received on the ports, these messages are printed

```
Dec 30 18:23:58.685: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet8/1, changed state to down
Dec 30 18:23:58.683: %SPANTREE-SP-2-BLOCK_BPDUGUARD: Received BPDU on port
  FastEthernet8/1 with BPDU Guard enabled. Disabling port.
Dec 30 18:23:58.683: %PM-SP-4-ERR_DISABLE: bpduguard error detected on Fa8/1,
  putting Fa8/1 in err-disable state
```

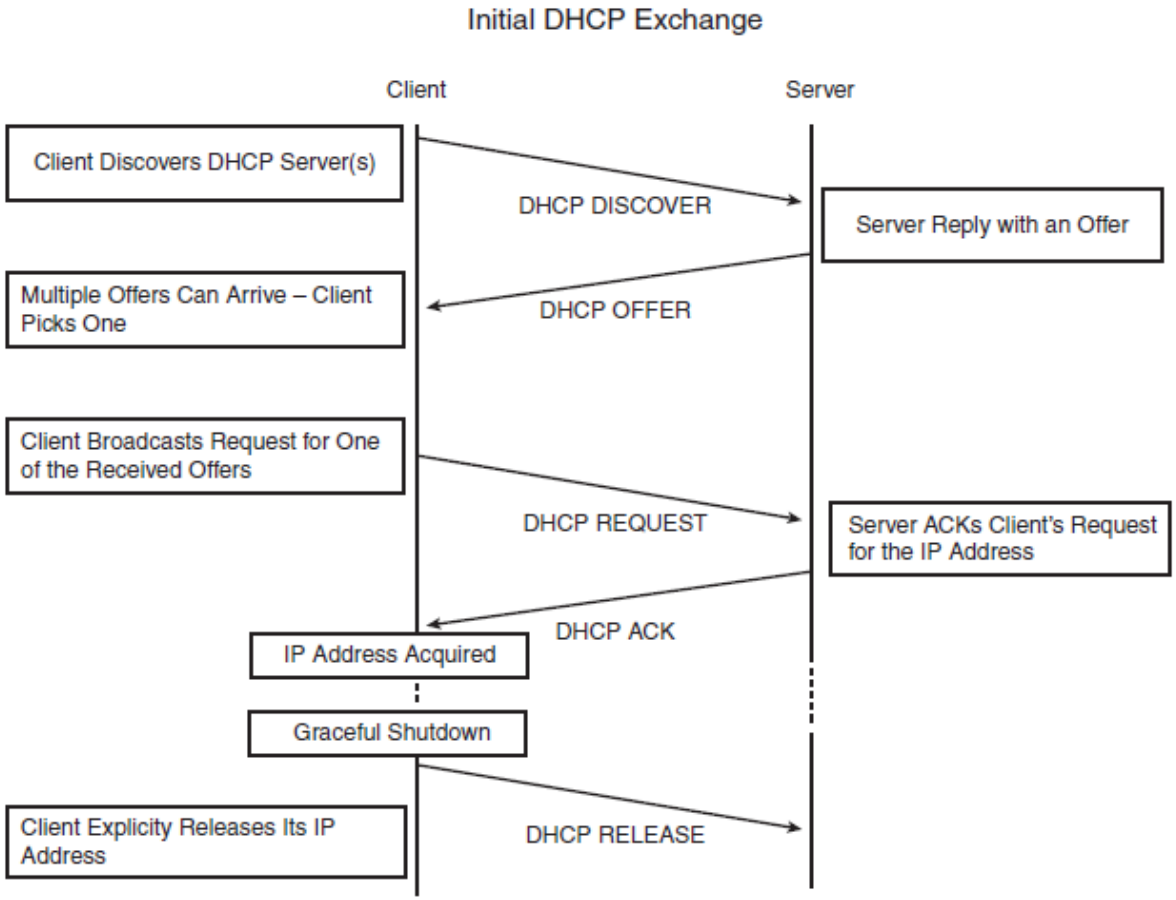
SPANNING TREE PROTOCOL Cont

- **Counter measures**
- **Root Guard**-Port in which root-guard is enabled is the Designated port
- Port put into a root-inconsistent state if it receives a superior BPDU

```
6K-2-S2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
6K-2-S2(config)# interface fastethernet 8/1
6K-2-S2(config-if)# spanning-tree rootguard
6K-2-S2(config-if)# ^Z
*Dec 30 18:25:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet8/1 VLAN 123.

Dec 30 18:33:41.677: %SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port Fa
stEthernet8/1 on VLAN0123.
6K-2-S2#sh spanning-tree vlan 123 ac

VLAN0123
  Spanning tree enabled protocol rstp
  Root ID    Priority    32891
             Address     0050.3e05.9c00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32891  (priority 32768 sys-id-ext 123)
             Address     0050.3e05.9c00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa8/1            Desg BKN*19        240.897  P2p *ROOT_Inc
Fa8/45           Desg FWD 19        128.941  P2p
Gi9/14           Desg FWD 4         128.1038 P2p
Gi9/15           Desg FWD 4         128.1039 Edge P2p

! "Desg" means designated port role; BKN means status blocking;
! FWD means forwarding. Notice the "ROOT Inc" status for port Fa8/1.
```

LEVERAGING DHCP WEAKNESSES

- **DHCP OVERVIEW**



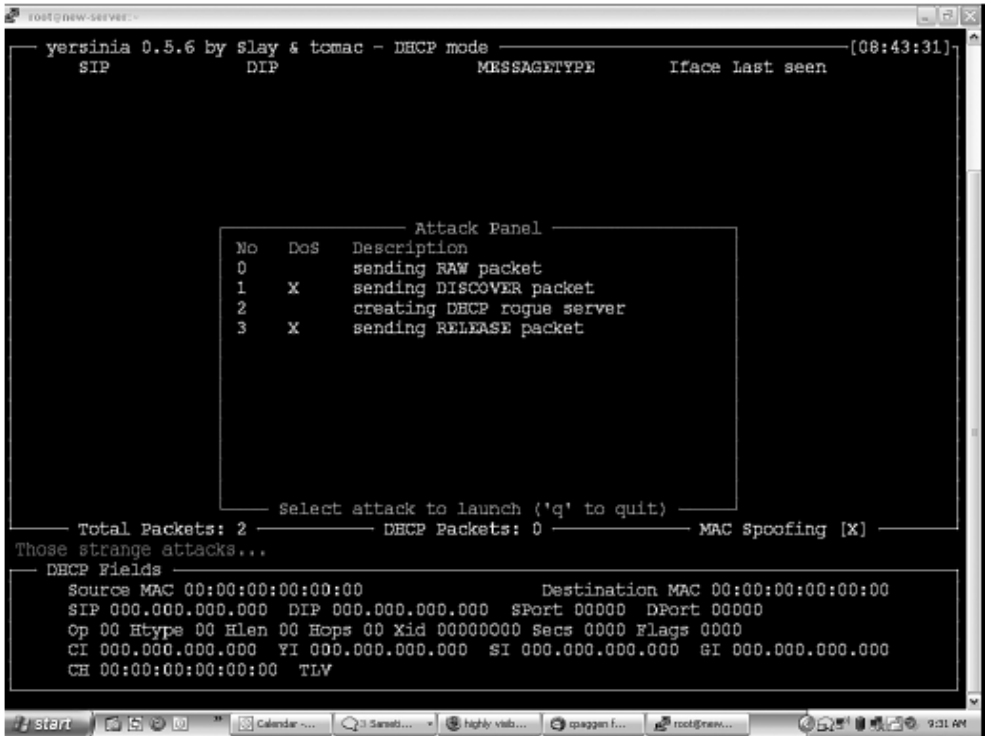
LEVERAGING DHCP WEAKNESSES

- **ATTACKS**
- DHCP SCOPE EXHAUSTION (Clients spoofs other clients)-Yersinia;client sends uniques packets with forged mac addresses for a DHCP discover
- Installation of a rogue DHCP server;Man in the middle attack

LEVERAGING DHCP WEAKNESSES

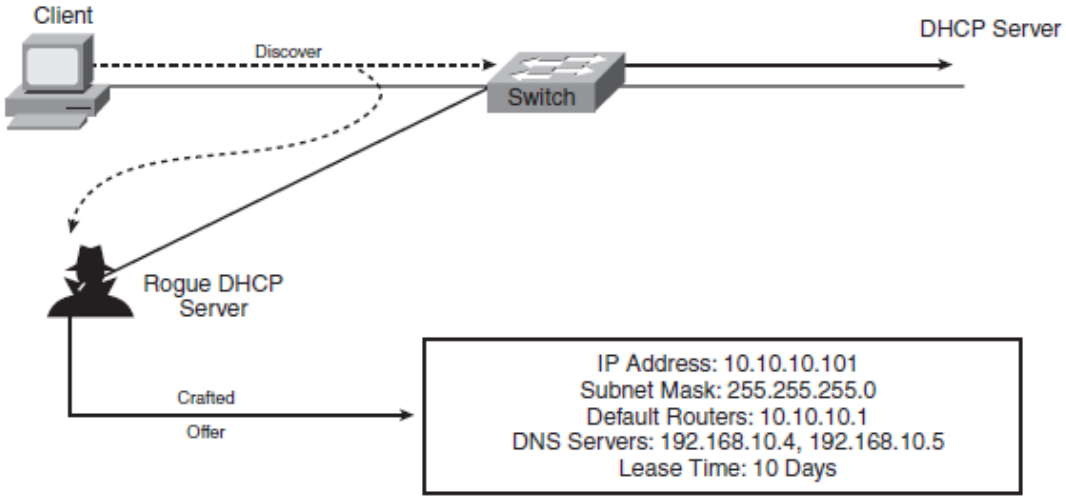
- **DHCP SCOPE EXHAUSTION /DoS attack against DHCP**

- Malicious client attempts to seize the entire range of IP addresses
- Uses random source mac addresses and then sending DHCPDISCOVER per forged mac address



LEVERAGING DHCP WEAKNESSES

- **Hijacking traffic using rogue DHCP server**



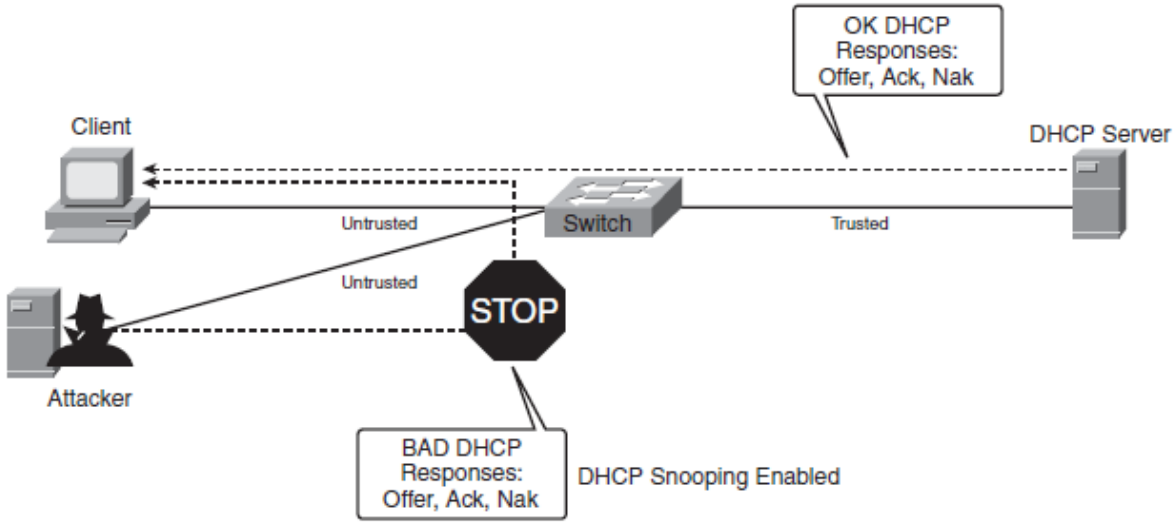
- **Counter measures**

Port security

DHCP Snooping-DPI on DHCP messages

LEVERAGING DHCP WEAKNESSES

- **DHCP snooping**
- Introduces concept of trusted and untrusted ports in a vlan
- Hosts have no reasons to generate DHCPOFFER or DHCPACK messages
- Rate-limits DHCP traffic from trusted and untrusted sources
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

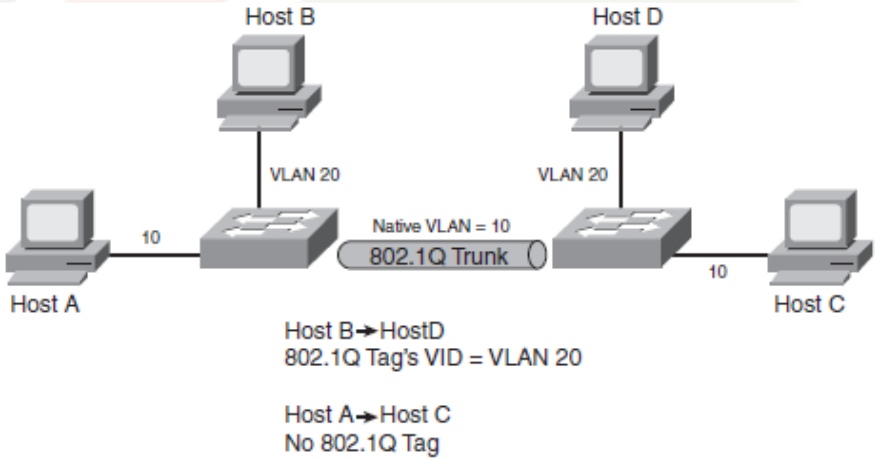


- **Router(config)# ip dhcp snooping**

VLAN SECURITY

VULNERABILITIES

Native VLAN concept

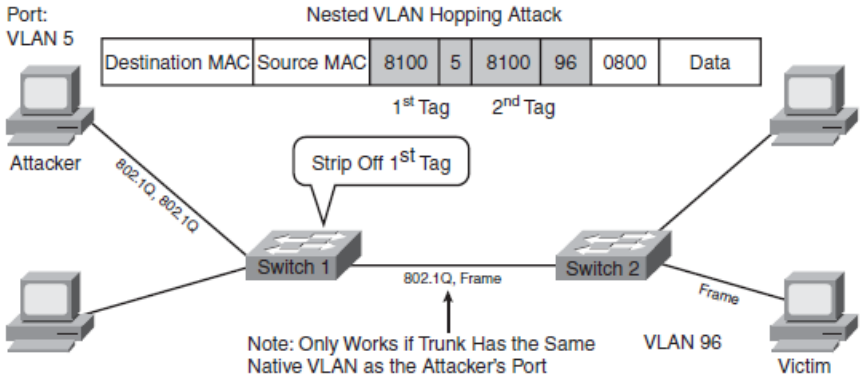


- Native Vlan and VLAN Hopping
- Double nested vlan attack (QnQ)

VLAN SECURITY

VULNERABILITIES

- Double nested vlan attack (QnQ)



Premises for this attack

- The attackers port is in VLAN 5
- The native VLAN of the trunk is VLAN 5

Counter measures

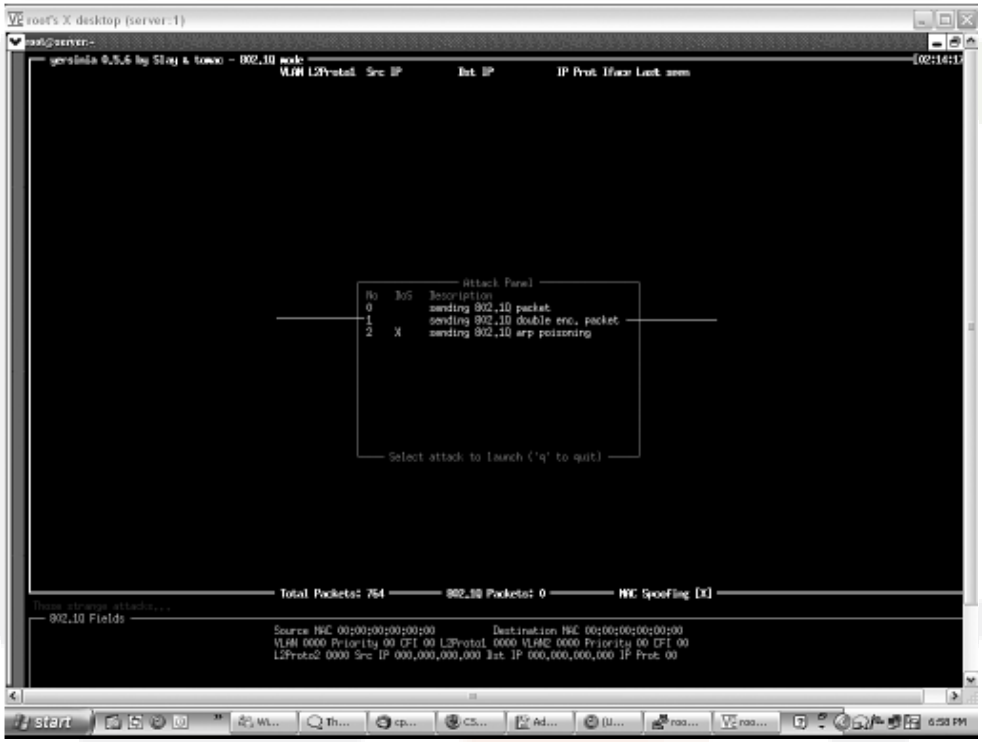
- Make sure no access port is a member of the trunk native vlan or force all traffic on the trunk to carry a tag

```
CiscoSwitch(config)#vlan dot1q tag native
or
CiscoSwitch(config)#interface GigabitEthernet2/1
CiscoSwitch(config-if)#switchport trunk native vlan tag
```

VLAN SECURITY

VULNERABILITIES

- Yersinia nested attack



INFORMATION LEAKS WITH CISCO PROTOCOLS (auto???)

- DTP-Cisco protocol that determines whether two switches connected want to create a trunk (Auto,Desirable,on,nonegotiate,off)

  Hard code everything!(Access ports,trunks)
- VTP-Reduces administrative overheads in a switched network (Server,client,transparent,off).Enable authentication or run VTP v3,enable only on trunks
- CDP-adjacent layer device discover each other

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.
- Example of a VACL on the distribution switches to prevent any client in Vlans 64 or 65 from performing Telnet sessions.

```
IP access-list extended TELNET_HOST 10
Permit IP 10.10.10.10 0.0.0.0 any any eq telnet

Vlan access-map NO_TELNET 10
Match IP address TELNET_HOST
Action forward

Vlan filter NO_TELNET vlan-list 64-65
```

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