VLAN Hijacking

Objective: In this lab I used the Yersinia tool to take advantage of default settings on a switch. By enabling DTP (Dynamic Trunking Protocol) I was able to make the switch form a trunk link with my Kali Linux. This allowed my Kali Linux to receive traffic from different VLANs, including one I wasn't originally part of. The goal was to show how attackers can use weak or default configurations to gain access to network traffic they shouldn't normally see.

Equipment: Kali Linux, 2811 Router, 2960 Switch, and Mac

Steps:

1. **Create a DHCP pool for VLAN 2**

```
ip routing
ip dhcp excluded-address 192.168.2.254
!
ip dhcp pool Home
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.254
```

2. Keep **interface g1/0/1 on VLAN 1 and move g1/0/2-3 to VLAN 2**

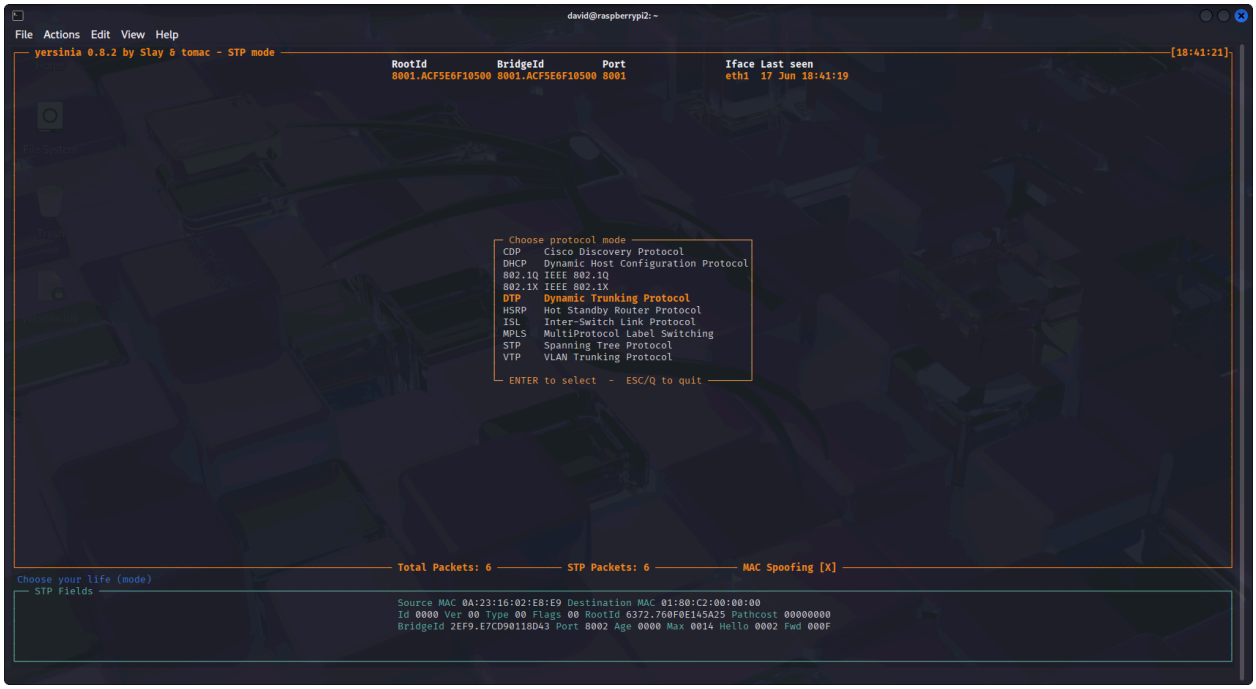
```
switcha#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi1/0/1, Gi1/0/4, Gi1/0/5
                                                 Gi1/0/6, Gi1/0/7, Gi1/0/8
                                                 Gi1/0/9, Gi1/0/10, Gi1/0/11
                                                 Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                 Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                 Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                 Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                 Gi1/0/24, Gi1/0/25, Gi1/0/26
                                                 Gi1/0/27, Gi1/0/28, Gi1/0/29
                                                 Gi1/0/30, Gi1/0/31, Gi1/0/32
                                                 Gi1/0/33, Gi1/0/34, Gi1/0/35
                                                 Gi1/0/36, Gi1/0/37, Gi1/0/38
                                                 Gi1/0/39, Gi1/0/40, Gi1/0/41
                                                 Gi1/0/42, Gi1/0/43, Gi1/0/44
                                                 Gi1/0/45, Gi1/0/46, Gi1/0/47
                                                 Gi1/0/48, Gi1/0/49, Gi1/0/50
                                                 Gi1/0/51, Gi1/0/52
2    VLAN0002                          active    Gi1/0/2, Gi1/0/3
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
switcha#
```

3. With default configurations or poor configurations, **the interface is on auto negotiation**

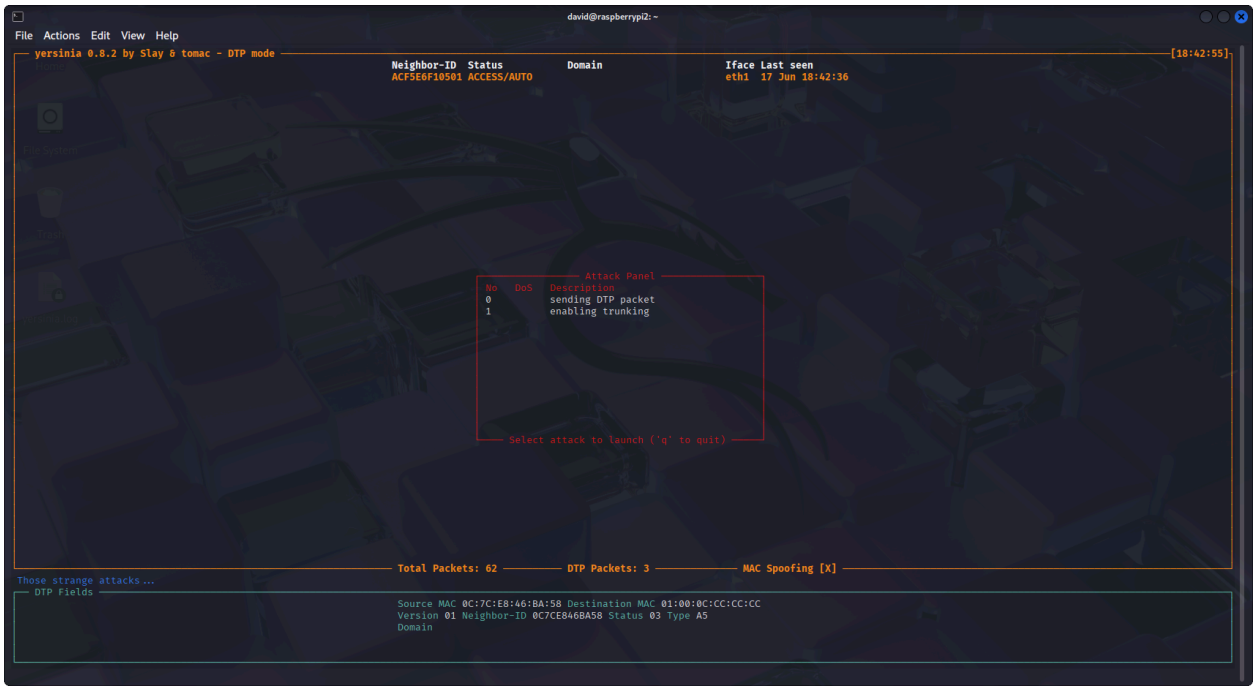
```
switcha>en
switcha#show int g1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
switcha#
```

4. Go to my Kali Linux to set up the **Yersinia** attack

5. Select the **DTP attack**



6. **Form the trunk link**



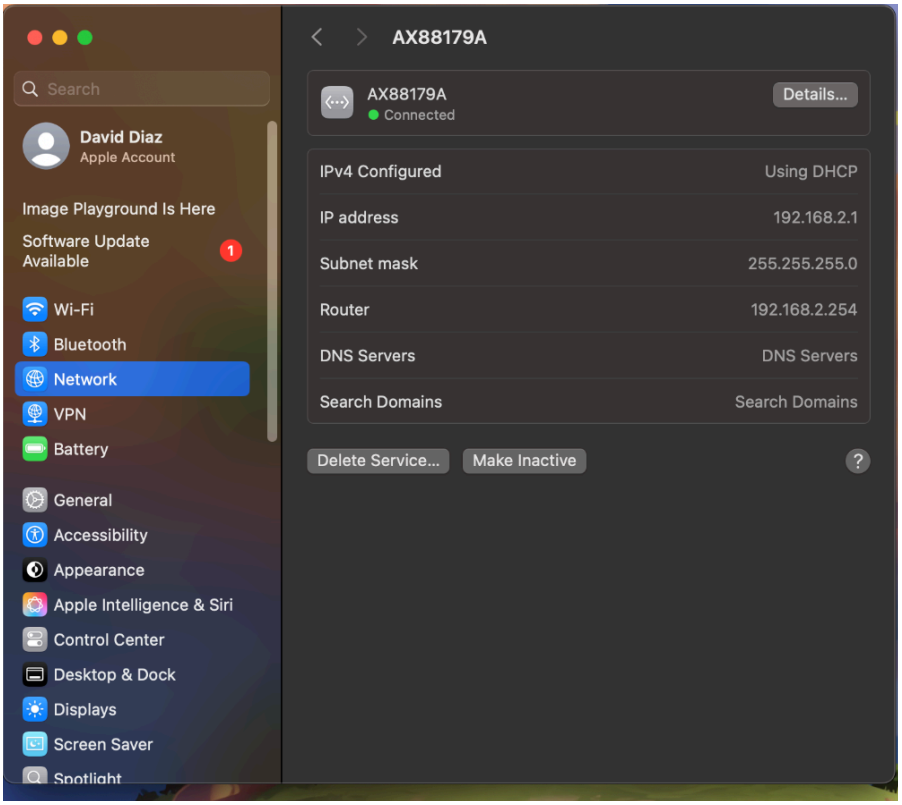
7. Verify it works by **looking for any changes on my CLI**

```
switcha#
Jun 20 12:11:51.548: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Jun 20 12:11:52.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down
Jun 20 12:11:55.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
Jun 20 12:12:24.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

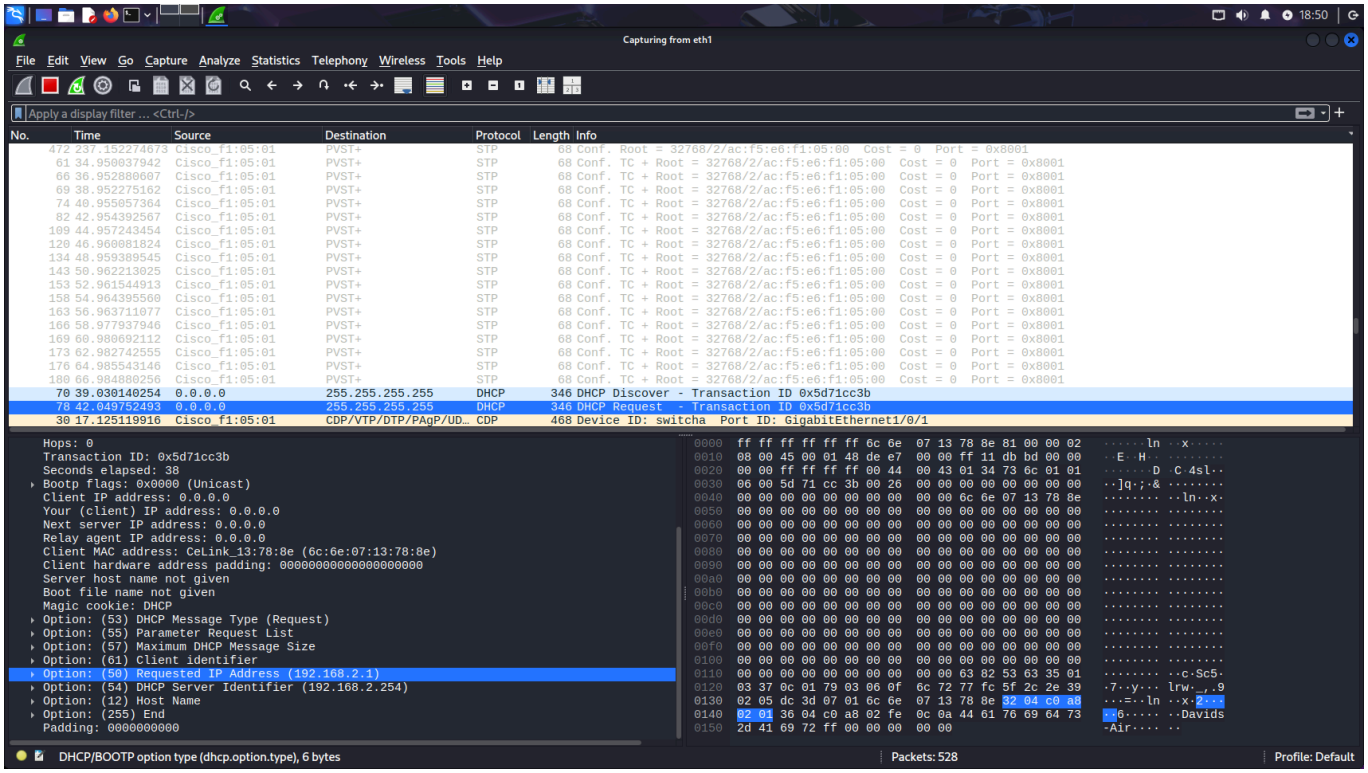
8. **Check my interfaces trunk**

```
switcha#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Gi1/0/1     1-4094

Port        Vlans allowed and active in management domain
Gi1/0/1     1-2

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     1-2
switcha#
```

9. On VLAN 2 I connect my Mac to the network and **do a DHCP request**

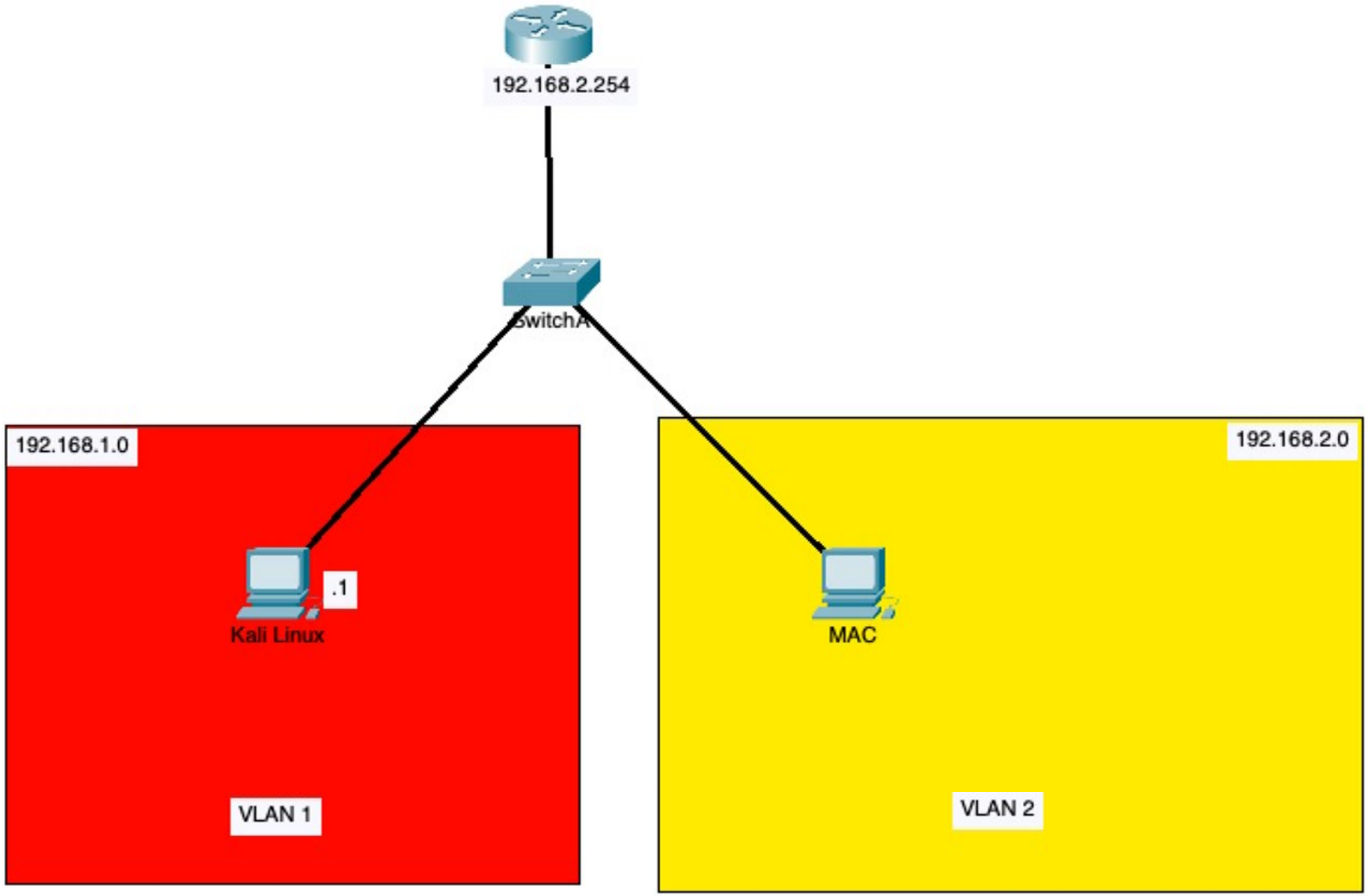


10. I use **wireshark to snoop on traffic and capture the DHCP request**, while being on VLAN 1



11. In order to stop this attack, **I have to configure my port with no negotiation** (in real world situations, it should be applied to every interface). **This ensures that no DTP can be performed**

```
switcha(config)#int g1/0/1
switcha(config-if)#switchport nonegotiate
switcha(config-if)#do sh int g1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
switcha(config-if)#
```


192.168.2.254
SwitchA
192.168.1.0
.1
Kali Linux
VLAN 1
192.168.2.0
MAC
VLAN 2