VLAN

A **virtual local area network** (VLAN) is used to share the physical network while creating virtual segmentations to divide specific groups. For example, a host on VLAN 1 is separated from any host on VLAN 2. Any packets sent between VLANs must go through a router or other layer 3 devices. Security is one of the many reasons network administrators configure VLANs. However, with an exploit known as 'VLAN Hopping', an attacker is able to bypass these security implementations. Learn more about network segmentation and VLANs here.

VLAN Hopping

This type of exploit allows an attacker to bypass any layer 2 restrictions built to divide hosts. With proper switch port configuration, an attacker would have to go through a router and any other layer 3 devices to access their target. However, many networks either have poor VLAN implementation or have misconfigurations which will allow for attackers to perform said exploit. In this article, I will go through the two primary methods of VLAN hopping, known as 'switched spoofing', and 'double tagging'. I will then discuss mitigation techniques.

Switched Network

It is crucial we understand how switches operate if we would like to find and exploit their vulnerabilities. We are not necessarily exploiting the device itself, but rather the protocols and configurations instructing how they operate.

On a switch, a port is either configured as an access port or a trunking port. An access port is typically used when connecting a host to a switch. With the implementation of VLANs, each access port is assigned to only one VLAN. A trunking port is used when connecting two switches or a switch and a router together. Trunking ports allow for traffic from multiple VLANs.

A trunk port can be configured manually or created dynamically using Dynamic Trunking Protocol (DTP).

DTP is a Cisco proprietary protocol where one use is to dynamically establish a trunk link between two switches.

Switched Spoofing VLAN Attack

An attacker acts as a switch in order to trick a legitimate switch into creating a trunking link between them. As mentioned before, packets from any VLAN are allowed to pass through a trunking link. Once the trunk link is established, the attacker then has access to traffic from any VLAN. This exploit is only successful when the legitimate switch is configured to negotiate a trunk. This occurs when an interface is configured with either "dynamic desirable", "dynamic auto" or "trunk" mode. If the target switch has one of those modes configured, the attacker then can generate a DTP message from their computer and a trunk link can be formed.

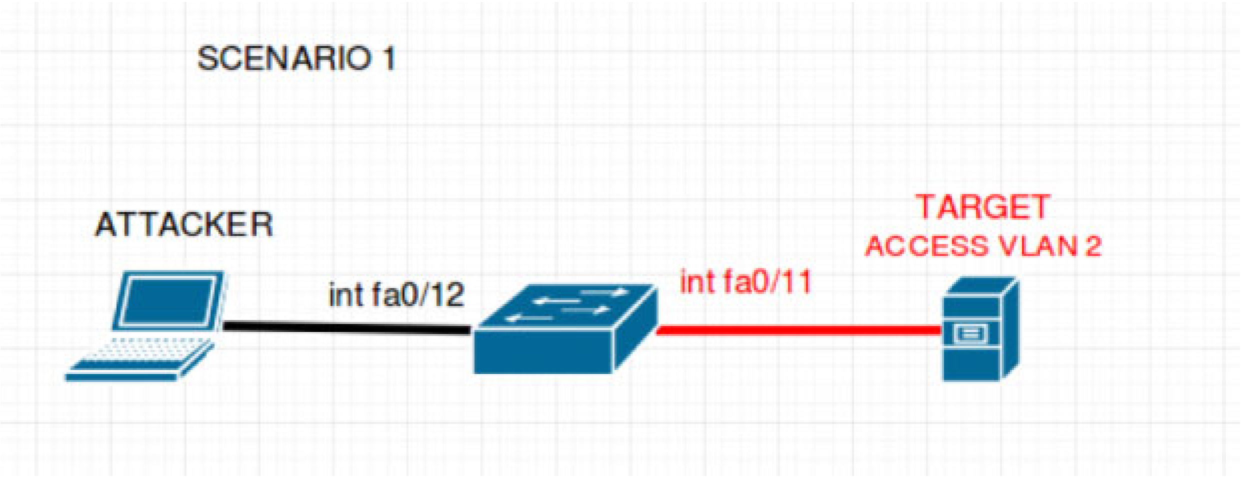
Double Tagging

Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link. Another important point is, this attack is strictly one way as it is impossible to encapsulate the return packet.

VLAN Hopping Exploit

Scenario 1 - Switch Spoofing Attack

In this scenario there exists the attacker, a switch, and the target server. The attacker is attached to the switch on interface FastEthernet 0/12 and the target server is attached to the switch on interface FastEthernet 0/11 and is a part of VLAN 2. Take a look at the following topology.



Once you are familiar with the topology, take a look at a few of the configurations set for the switch:

```
interface FastEthernet0/11

switchport mode access

switchport mode nonegotiate

switchport access vlan 2

!
```

```
interface FastEthernet0/12

switchport mode dynamic auto
```

Hopefully, you can see the configuration issue with interface fa0/12. This port is set to accept incoming negotiations to determine whether the port is for access or trunking. Which means an attacker is able to perform a Switch Spooking attack. Once the attacker connects to the port they can then send a DTP message and a trunking link will be established.

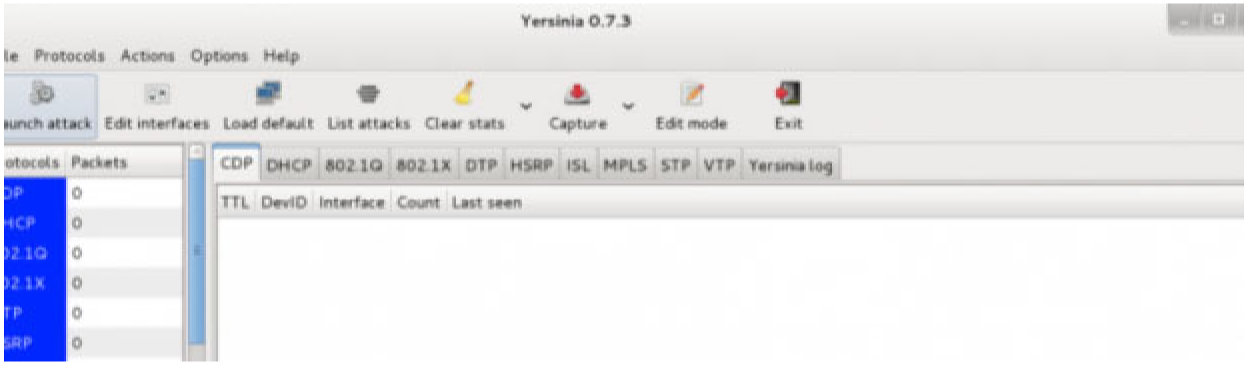
An attacker can use the program Yersinia to craft and send a DTP message. Yersinia is a penetration testing framework built to attack many protocols that reside on layer 2. It comes pre-installed with kali Linux and has an easy to use graphical user interface (GUI).

Yersinia Homepage - http://www.yersinia.net/

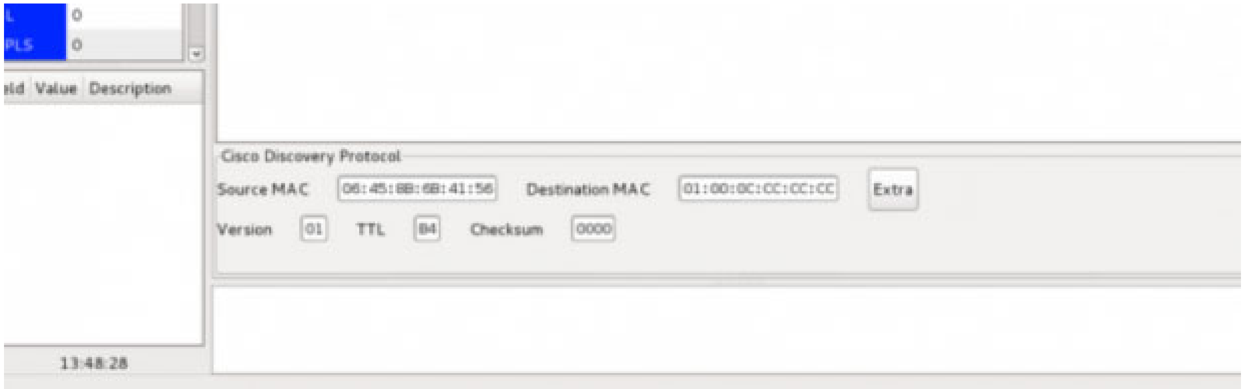
To launch Yersinia:

```
    yersinia -G
```

Here is a quick look at the GUI:



otocols	Packets
DP	0
HCP	0
02.1Q	0
02.1X	0
TP	0
SRP	0



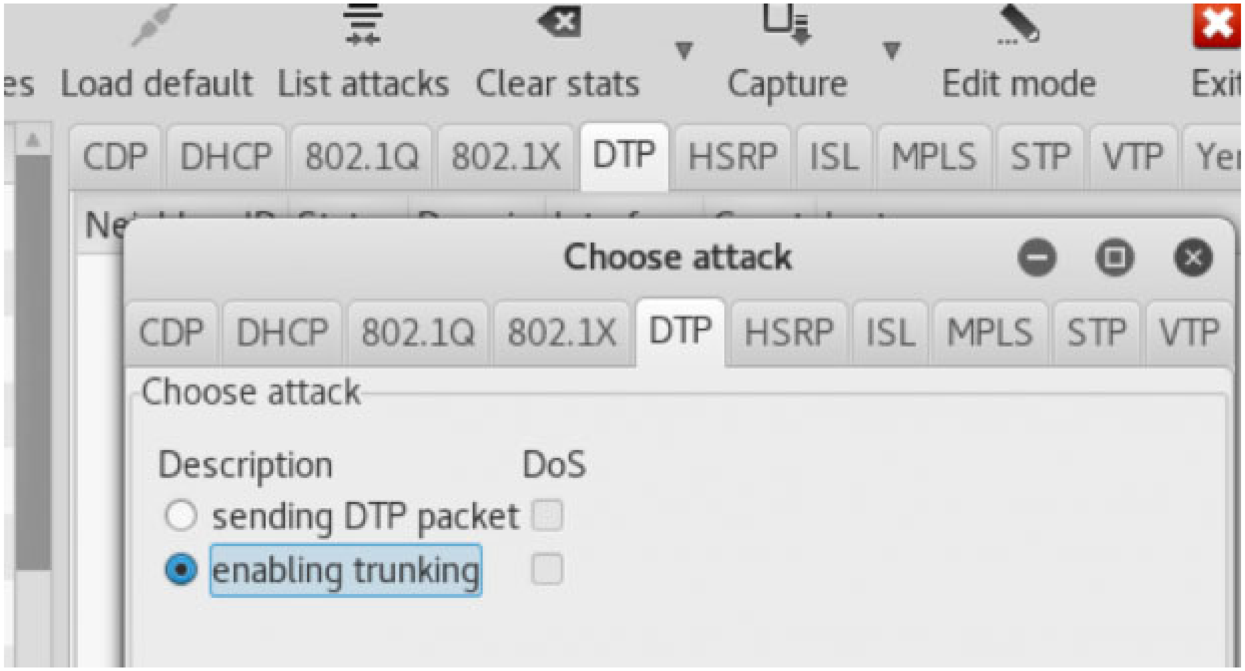
Cisco Discovery Protocol

Source MAC 06:45:8B:6B:41:56 Destination MAC 01:00:0C:CC:CC:CC

Version 01 TTL B4 Checksum 0000

Now to send a DTP message is as simple as the following 4 steps:

1. ***click "Launch attack"***
2. ***click the tab "DTP"***
3. ***click "enable trunking"***
4. ***click "ok"***



es
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yer
Ne
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP

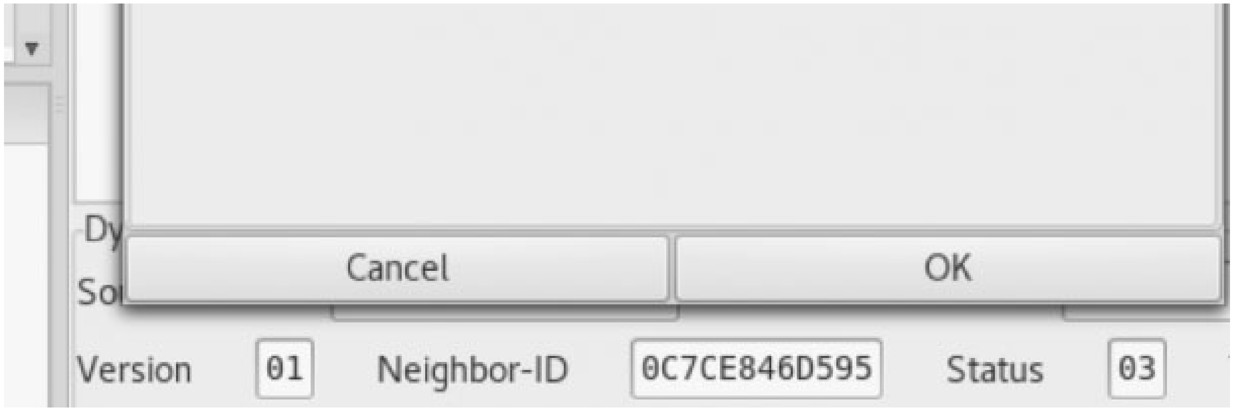
Choose attack

Choose attack

Description DoS

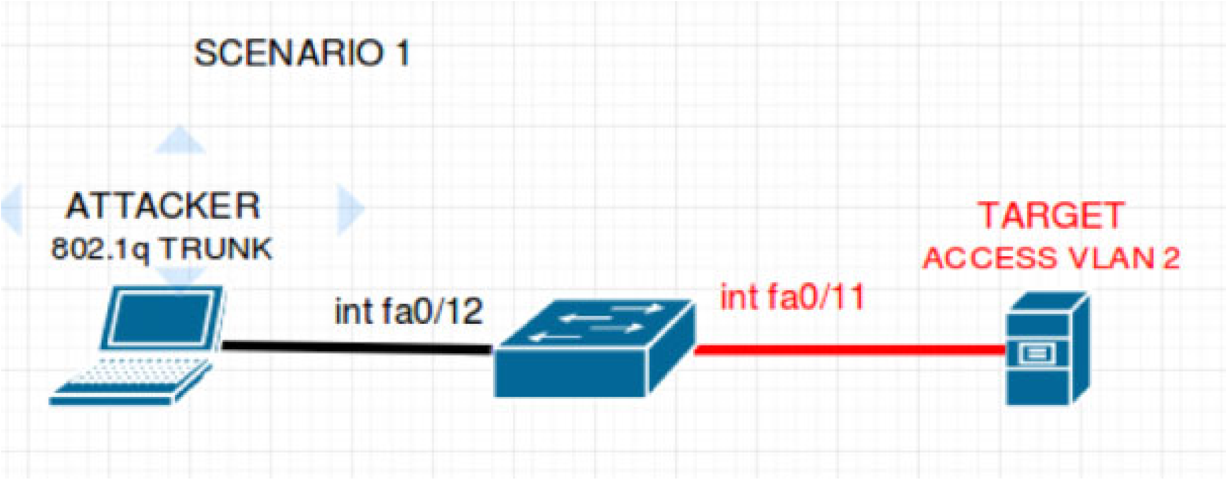
○ sending DTP packet □

● enabling trunking □



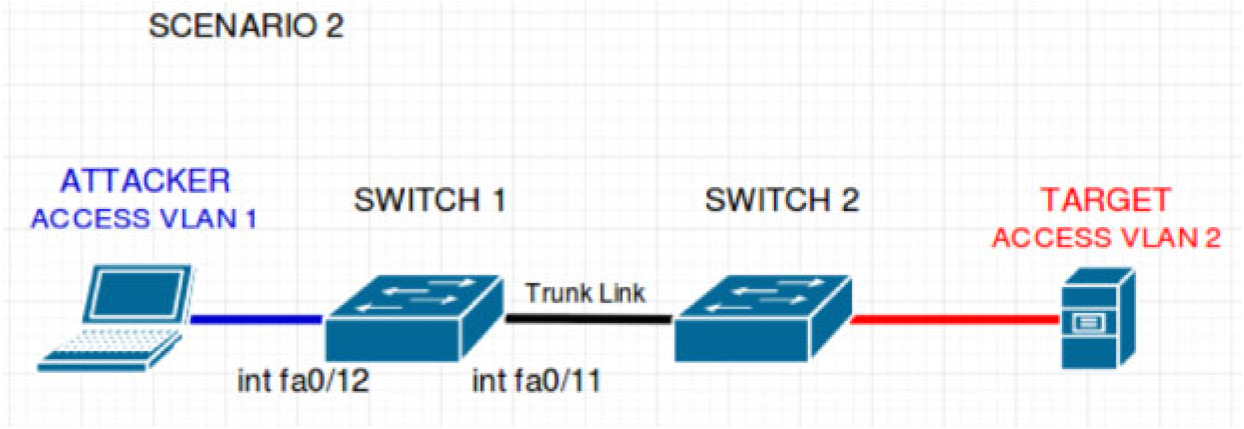
Version 01 Neighbor-ID 0C7CE846D595 Status 03

Yersinia will the send out a DTP message and within a few seconds, a trunking link will be established. In our scenario, the attacker will then have access to all traffic flowing through VLAN 2 and can directly attack without going through any layer 3 devices.



Scenario 2 - Double Tagging Attack

In this scenario, there exists an attacker, 2 switches, and a target server. The attacker is attached to switch 1. Switch 1 is attached to switch 2 and finally, our target is attached to switch 2. Take a look at the following topology.



Once you are familiar with the topology, take a look at a few of the configurations set for switch 1.

```
interface FastEthernet0/12
 switchport mode access
 switchport nonegotiate
 switchport access vlan 1
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 1
```

From these configurations, we see that an attacker would be unable to perform a switch spoofing attack. However, we see that the attacker belongs to the native VLAN of the trunk port. Which means this topology is vulnerable to a Double Tagging attack.
An attacker can use the program Scapy, to create the specially crafted frames needed for processing this attack. Scapy is a Python program created to manipulate packets.

Scapy Homepage - https://scapy.net/

Scapy Documentation - http://scapy.readthedocs.io/en/latest/usage.html

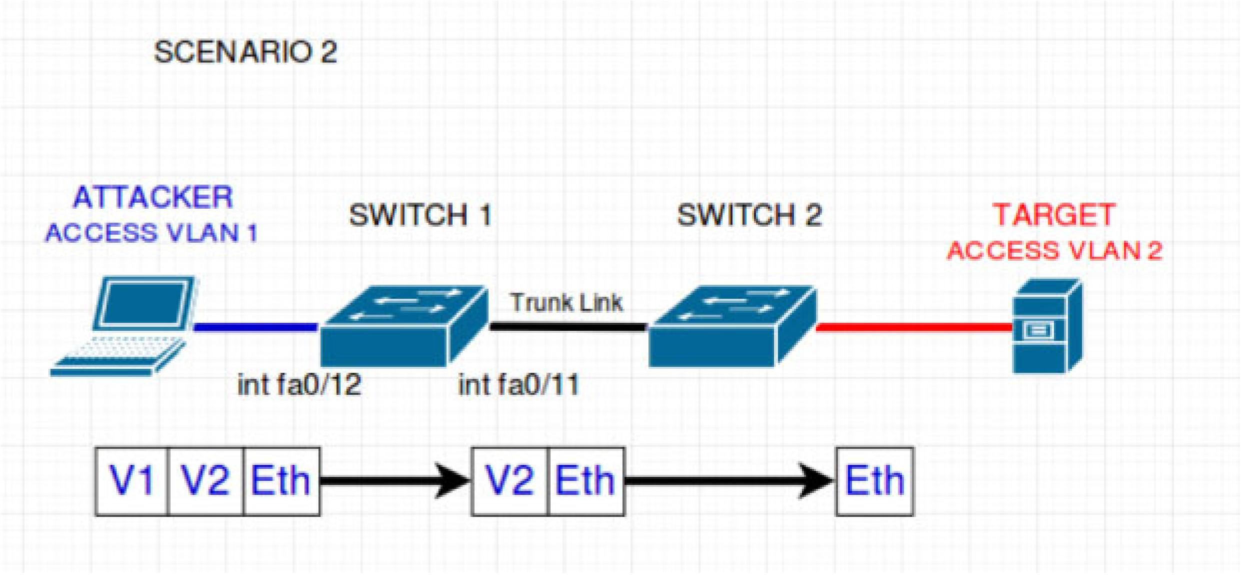
Start Scapy:

```
    sudo ./scapy
```

Using the sendp() function to craft a packet:

```
>>>sendp(Ether()/Dot1Q(vlan=1)/Dot1Q(vlan=2)/IP(dst='" )="" icmp())
```

This will generate a double 802.1q encapsulated packet for the target on VLAN 2. Take a look at the following topology to view how the switches manage this frame.



From the picture, we can see that switch 1 reads and removes only the outside tag. It checks that the host is part of the stated VLAN and forwards the packet to all native VLAN ports (VLAN

1). Switch 2 then receives the packet with only one header left. It assumes the frame belongs to the stated VLAN on this tag (VLAN 2) and forwards to all ports configured for VLAN 2. The target then receives the packet sent by the attacker.

VLAN = HOPPED.
Due to the nature of this attack, it is strictly one way. Please also note that this attack may not work on new switches.

Mitigation for VLAN Hopping

Switched Spoofing

To prevent a Switched Spoofing attack, there are a few steps you should take:

1. ***Do not configure any access points with either of the following modes: "dynamic desirable", "dynamic auto", or "trunk".***
2. ***Manually configure access ports and disable DTP on all access ports.***
   switchport mode access
   switchport mode nonegotiate
3. ***Manually configure all trunk ports and disable DTP on all trunk ports.***
   switchport mode trunk
   switchport mode nonegotiate
4. ***Shutdown all interfaces that are not currently in use.***

Double Tagging

To prevent a Double Tagging attack, keep the native VLAN of all trunk ports different from user VLANs.

Final Note

Switches were not built for security. However, it is important to utilize security measures at every level. If you are to take the time to segment your network, make sure it is done properly and securely. Be diligent when configuring your network.