



**UNIVERSITY of INFORMATION
TECHNOLOGY and MANAGEMENT
in Rzeszow, POLAND**

**SUBJECT: Major threat on Virtual Lan Networks
– Hopping Attacks.**

Lecturer:

dr. Nataliia Poliakova

Student:

Jash Vaidya (W63847)

Tangirbergen Bolganbay (W61784)

Class:

Cybersecurity Essentials

Field of study:

(IT)

Rzeszów 2022

Table of Contents

Introduction.....	3
1. Threat analysis of VLAN attacks.....	4
1.1. What is a Virtual Local Area Network (VLAN) and how it works?.....	4
1.2. What is VLAN attack?.....	5
1.2.1 Switch Spoofing/Basic VLAN Hopping Attack VLAN hopping attacks.....	6
1.2.2 Double Tagging/Double Encapsulation VLAN Hopping Attack.....	7
2. Planning countermeasures against VLAN double-tagging and VLAN Switch Spoofing	10
2.1 Access Control Lists ACLs.....	10
2.2 Countermeasures for VLAN double-tagging.....	11
2.3 Countermeasures for VLAN Switch Spoofing	12
3. An experiment to verify the effectiveness of protection	13
Scenario 1 - Switch Spoofing Attack	13
Scenario 2 - Double Tagging Attack.....	16
Conclusion.....	19
List of Sources	20

Introduction

A virtual local area network is a logical subnetwork that groups a collection of devices from different physical LANs. Large business computer networks often set up VLANs to re-partition a network for improved traffic management. Several kinds of physical networks support virtual LANs, including Ethernet and Wi-Fi.

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.

The majority of Layer 2 (data link layer) attacks exploit the inability of a switch to track an attacker, because the switch has no inherent mechanism to detect that an attack is occurring. This inability to detect an attacker means that this same attacker can perform malicious acts against the network path, altering the path and exploiting the change without detection.

1. Threat analysis of VLAN attacks.

1.1. What is a Virtual Local Area Network (VLAN) and how it works?

A **virtual** local area network (VLAN) enables administrators to separate networks based on function, project team, or application, independent of the user's or device's actual location. Devices inside a VLAN operate independently, even if they share infrastructure with other VLANs. Any switch port can be assigned to a VLAN, and unicast, broadcast, and multicast packets are sent to and saturate only the terminal stations on the VLAN from which they originated. Each VLAN is treated as a distinct logical network. Packets destined for stations outside the VLAN must be routed through a routing device.

What happens if we need a virtual connection between two stations belonging to two different physical LANs? A virtual local area network (VLAN) is defined as a local area network configured by software not by physical wiring. [1]

Virtual LANs (VLANs) have recently developed into an integral feature of switched LAN solutions from every major LAN equipment vendor. In networking, a LAN has a single broadcast domain and the traffic from a workstation reaches other workstations on the LAN through the broadcast. This is not desirable as certain classified information can be received by unauthorized parties. Also, if the broadcast is not well-contained, it can lead to a collision in the network [1]

Virtual LAN technology is used in the design of internal networks of universities, organizations, and enterprise networks. VLAN is a data link layer technology for building multiple logical networks on the top of logical networks. The LAN network is divided into different logical segments called broadcast domains. The workstation division is based on the functions, platforms and teams. Virtual network is nothing but a group of devices that are connected virtually but may or may not physically connected. VLAN allows network engineers and network administrators to make logical network from physical network. This technology is used to segment a complex network into smaller networks for better manageability, improved performance and security [1]

1.2. What is VLAN attack?

When people talk about Virtual LANs (VLANs), they tend not to focus on the security features of this versatile network topology. However, there are several tangible security vulnerabilities that can increase business risk if they are not properly understood and mitigated. [2]

Attacks on VLANs are easier to perpetrate than you might think. And typically, there are several known applications that provide potential attackers with the tools to penetrate VLANs and cause chaos. Easy to find and download from the Internet, these tools show people how to exploit badly configured networks and physical weaknesses in the LAN, making it depressingly easy for them to launch a devastating VLAN attack. VLANs are implemented at layer 2 of the OSI network model. The majority of layer 2 (data link layer) attacks exploit the inability of a switch to track an attacker, because the switch has no inherent mechanism to detect that an attack is occurring. This weakness means that this same attacker can perform malicious acts against the network path, altering the path and exploiting the change without detection. While the number of possible attack vectors is large, here is a list of what I believe to be the top ten threats for organizations using VLANs in no particular order. [2]

Well known types of VLAN attacks,

1. CAM Table Overflow/Media Access Control (MAC) Attack.
2. Address Resolution Protocol (ARP) attack.
3. VLAN Management Policy Server (VMPS)/ VLAN Query Protocol (VQP) attack
4. Multicast Brute-Force Attack.

In this project, we will talk about **major threat on Virtual Lan Networks – Hopping Attacks.**

- 1) Switch Spoofing/Basic VLAN Hopping Attack VLAN hopping attacks.
- 2) Double Tagging/Double Encapsulation VLAN Hopping Attack.

1.2.1 Switch Spoofing/Basic VLAN Hopping Attack VLAN hopping attacks.

There are a number of different types of VLAN attacks in modern switched networks. The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. It is important to understand the general methodology behind these attacks and the primary approaches to mitigate them. [3]

VLAN hopping enables traffic from one VLAN to be seen by another VLAN.

Switch spoofing is a type of VLAN hopping attack that works by taking advantage of an incorrectly configured trunk port. By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches.

In a basic switch spoofing attack, the attacker takes advantage of the fact that the default configuration of the switch port is dynamic auto. The network attacker configures a system to spoof itself as a switch. This spoofing requires that the network attacker be capable of emulating 802.1Q and DTP messages. By tricking a switch into thinking that another switch is attempting to form a trunk, an attacker can gain access to all the VLANs allowed on the trunk port. [3]

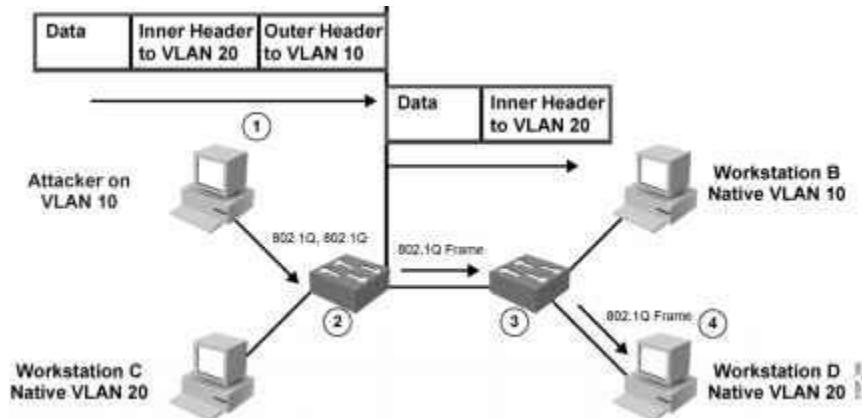


Image 1: Switch Spoofing attack (www.ccexpert.us)

Switch Spoofing Sequence of Events,[4]

Step 1. Attacker gains access to a switch port and sends DTP negotiation frames toward a switch with DTP running and auto negotiation turned on (often, the default settings).

Step 2. Attacker and switch negotiate trunking over the port.

Step 3. Switch allows all VLANs (default) to traverse the trunk link.

Step 4. Attacker sends data to, or collects it from, all VLANs carried on that trunk.

1.2.2 Double Tagging/Double Encapsulation VLAN Hopping Attack.

Another type of VLAN attack is a double-tagging (or double-encapsulated) VLAN hopping attack. This type of attack takes advantage of the way that hardware on most switches operates. Most switches perform only one level of 802.1Q de-encapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify as shown in **Image 2**. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link. [3]

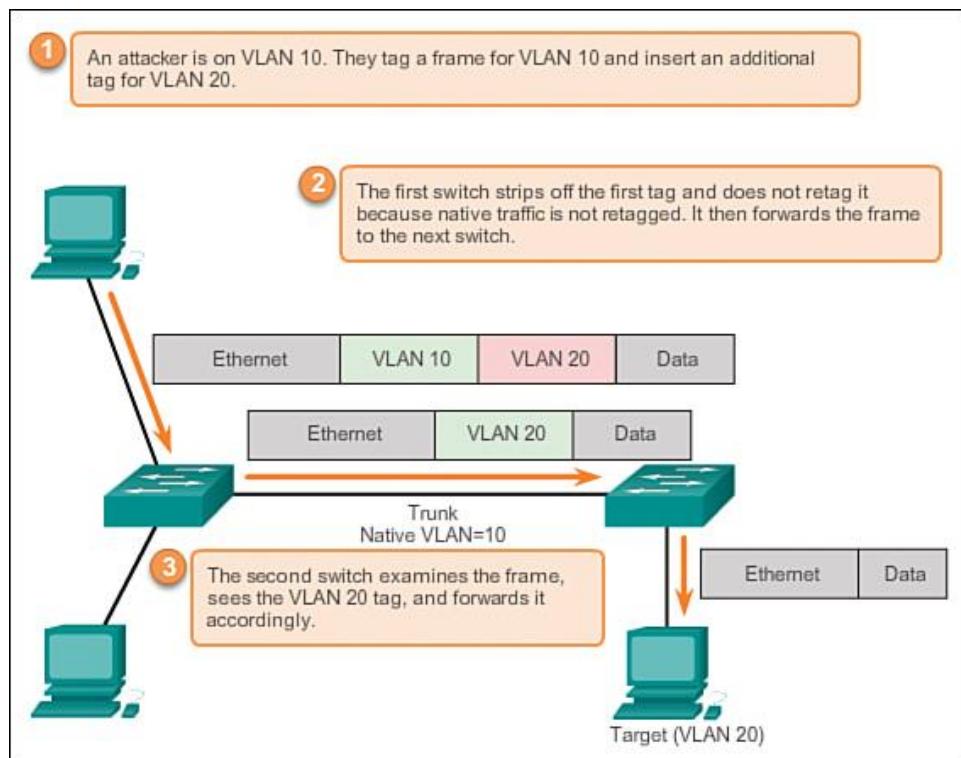


Image 2: Double-Tagging Attack (www.ciscopress.com)

Step 1. The attacker sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the attacker, which is the same as the native VLAN of the trunk port. The assumption is that the switch processes the frame received from the attacker as if it were on a trunk port or a port with a voice VLAN. (A switch should not receive a tagged Ethernet frame on an access port.) For the purposes of this example, assume that the native VLAN is VLAN 10. The inner tag is the victim VLAN; in this case, it is VLAN 20.

Step 2. The frame arrives on the switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for VLAN 10, which is the native VLAN. The switch forwards the packet out on all VLAN 10 ports after stripping the VLAN 10 tag. On the trunk port, the VLAN 10 tag is stripped, and the packet is not retagged because it is part of the native VLAN. At this point, the VLAN 20 tag is still intact and has not been inspected by the first switch.

Step 3. The second switch looks only at the inner 802.1Q tag that the attacker sent and sees that the frame is destined for VLAN 20, the target VLAN. The second switch sends the frame on to

the victim port or floods it, depending on whether there is an existing MAC address table entry for the victim host.

This type of attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port. Thwarting this type of attack is not as easy as stopping basic VLAN hopping attacks. [3]

The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports. In fact, it is considered a security best practice to use a fixed VLAN that is distinct from all user VLANs in the switched network as the native VLAN for all 802.1Q trunks. [3]

2. Planning countermeasures against VLAN double-tagging and VLAN Switch Spoofing

The measures to defend the network from VLAN hopping are a series of best practices for all switch ports and parameters to follow when establishing a trunk port. [4]

- Configure all unused ports as access ports so that trunking cannot be negotiated across those links.
- Place all unused ports in the shutdown state and associate them with a VLAN designed for only unused ports, carrying no user data traffic.
- When establishing a trunk link, purposefully configure arguments so that:
 - The native VLAN will be different from any data VLANs
 - Trunking is set up as "on," rather than as "negotiated"
 - The specific VLAN range will be carried on the trunk

2.1 Access Control Lists ACLs

Access control lists (ACLs) are useful for controlling access in a multilayer switched network. This topic describes VACLs and their purpose as part of VLAN security.[4]

Cisco Systems multilayer switches support three types of ACLs:

- Router access control lists (RACLs): Supported in the TCAM hardware on Cisco multilayer switches. In Catalyst switches, RACL can be applied to any routed interface, such as a switch virtual interface (SVI) or Layer 3 routed port.
- Port access control list (PACL): Filters traffic at the port level. PACLs can be applied on a Layer 2 switch port, trunk port, or EtherChannel port.
- VACLs: Supported in software on Cisco multilayer switches.

Catalyst switches support four ACL lookups per packet: input and output security ACL and input and output quality of service (QoS) ACL. [4]

Catalyst switches use two methods of performing a merge: order independent and order dependent. With order-independent merge, ACLs are transformed from a series of order

dependent actions to a set of order-independent masks and patterns. The resulting access control entry (ACE) can be very large. The merge is processor and memory intensive.[4]

Order-dependent merge is a recent improvement on some Catalyst switches in which ACLs retain their order-dependent aspect. The computation is much faster and is less processor-intensive.[4]

RACLs are supported in hardware through IP standard ACLs and IP extended ACLs, with permit and deny actions. ACL processing is an intrinsic part of the packet forwarding process. ACL entries are programmed in hardware. Lookups occur in the pipeline, whether ACLs are configured or not. With RACLs, access list statistics and logging are not supported.[4]

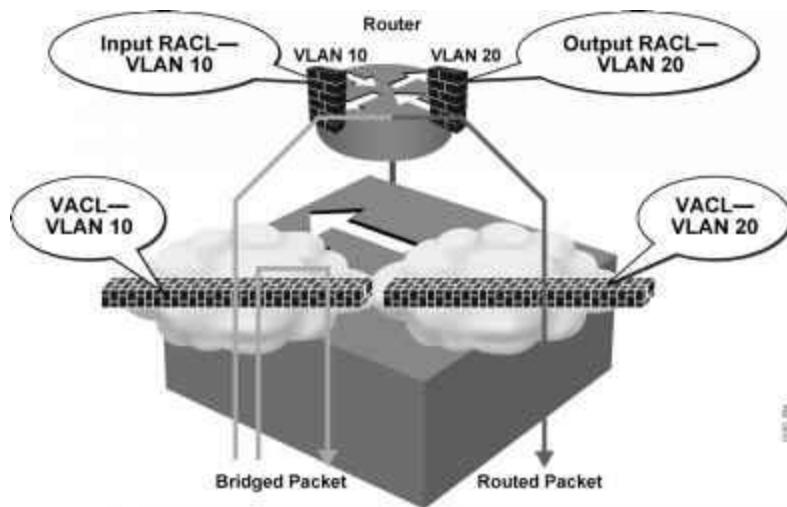


Image 3: Switch (www.ccexpert.us)

2.2 Countermeasures for VLAN double-tagging

Double tagging is a method involves tagging transmitted frames with two 802.1q headers, one of the headers is used for Victim switch and another is used for the attacker's switch.

The simplest way to prevent a VLAN Hopping attack is by disabling Dynamic Trunk protocol (DTP) on all untrusted ports.

For example:

```
ciscoswitch# conf t  
ciscoswitz(config)# int gi1/10  
ciscoswitch(config-if)# switchportnonegotiate
```

From the example “switchportnonegotiate” disables the DTP.

2.3 Countermeasures for VLAN Switch Spoofing

The simplest way to prevent a VLAN Switch Spoofing attack is by disabling Dynamic Trunk protocol (DTP) on all untrusted ports. From the example “switchportnonegotiate” disables the DTP. IEEE 802.1Q helps to create smaller networks out of large networks.

3. An experiment to verify the effectiveness of protection

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.

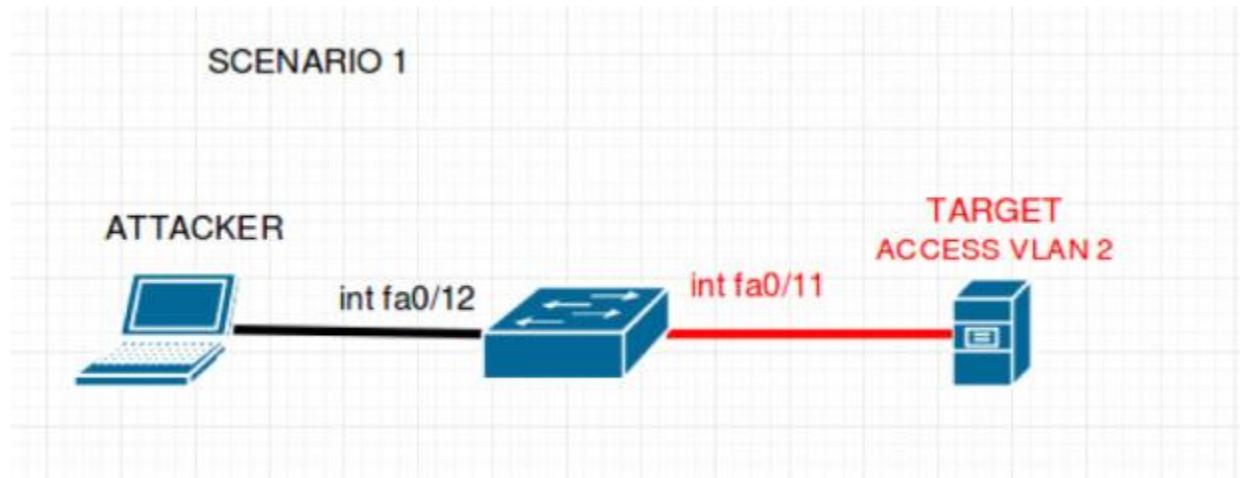


Image 4: Overview of Spoofing attack (cybersecurity.att.com)

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

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:

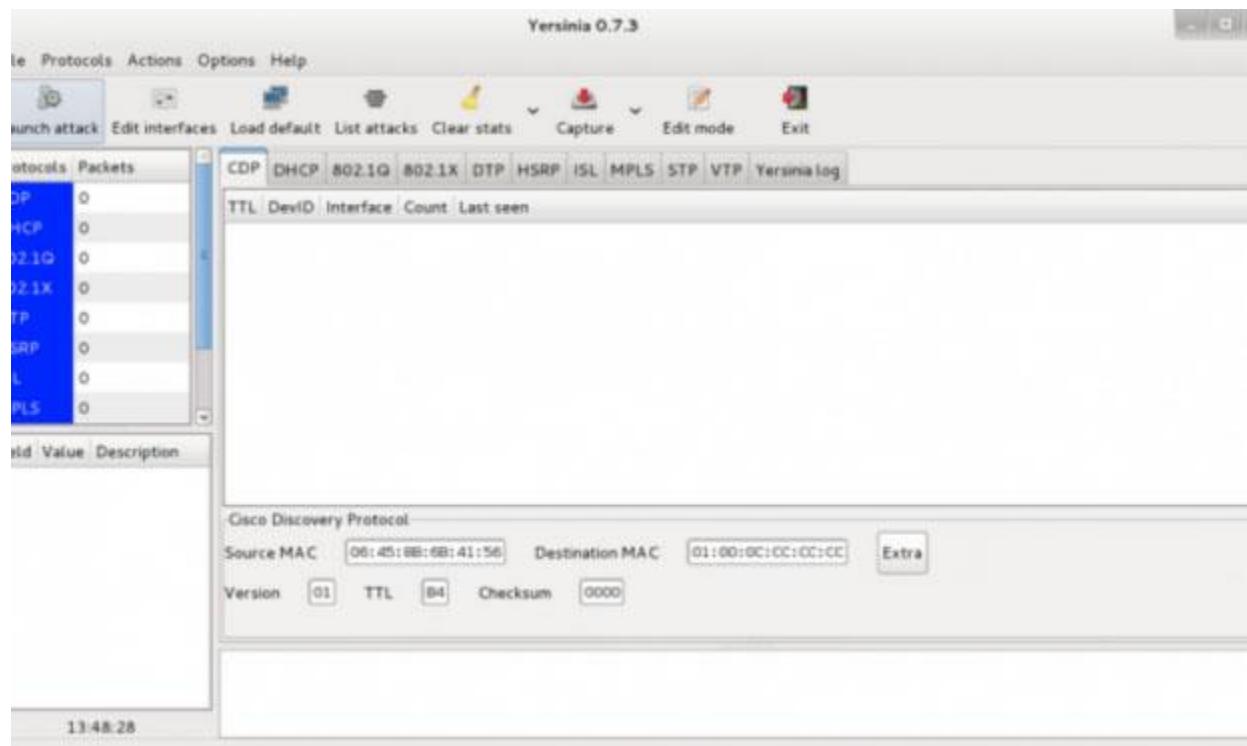


Image 5: Screenshot of GUI

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 GUI

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

click "Launch attack"

click the tab "DTP"

click "enable trunking"

click "ok"

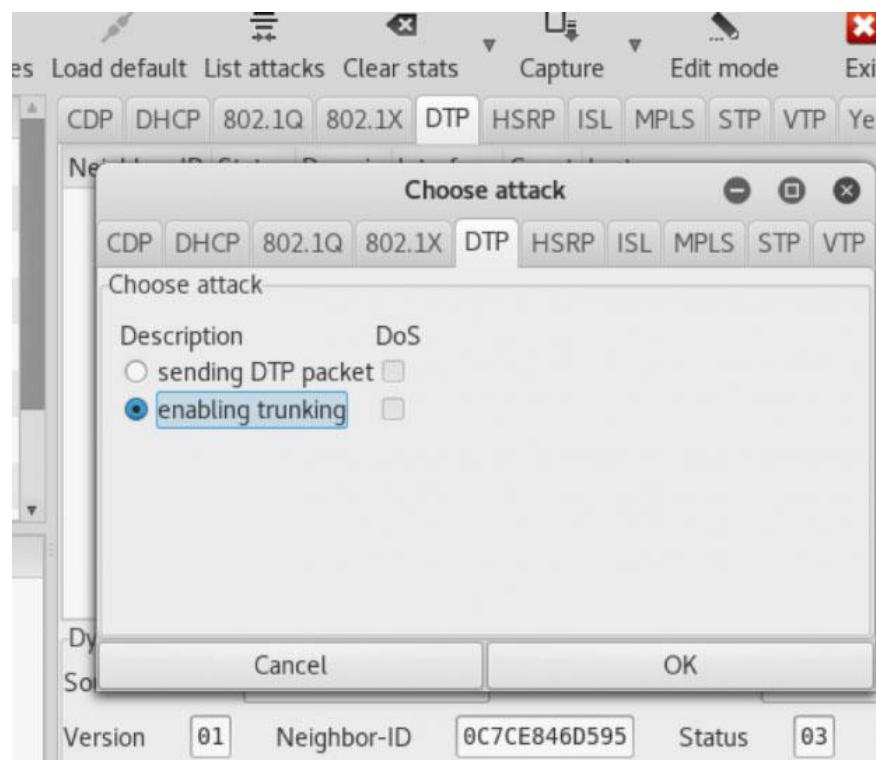


Image 6: Screenshot of enabling trunking

Yersinia will send out a DTP message and within a few seconds, a trunking link will be established VLAN

Yersinia will 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.

Yersinia will send out a DTP a trunking link will be established

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.

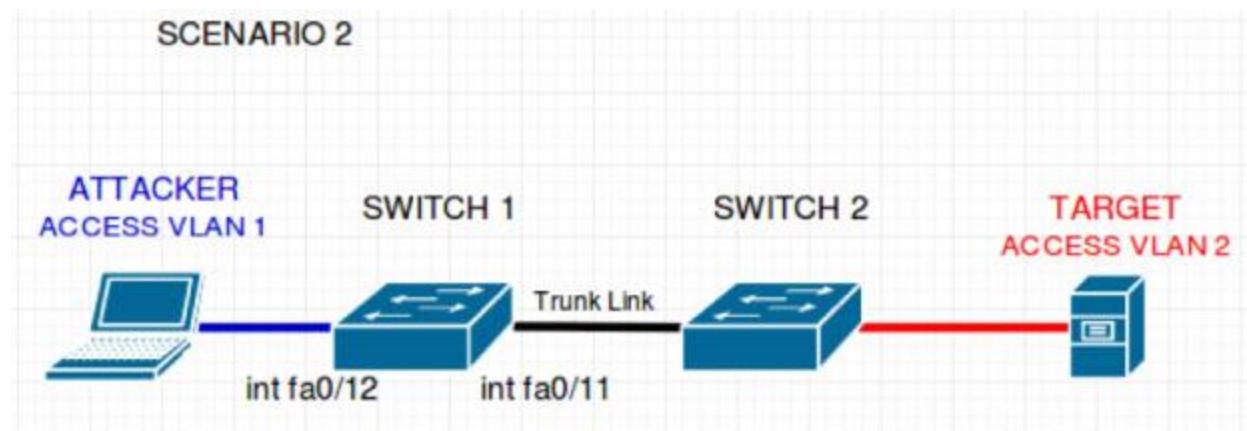


Image 7:: Overview of Double Tagging Attack 2 switches, and a target server
(cybersecurity.att.com)

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.

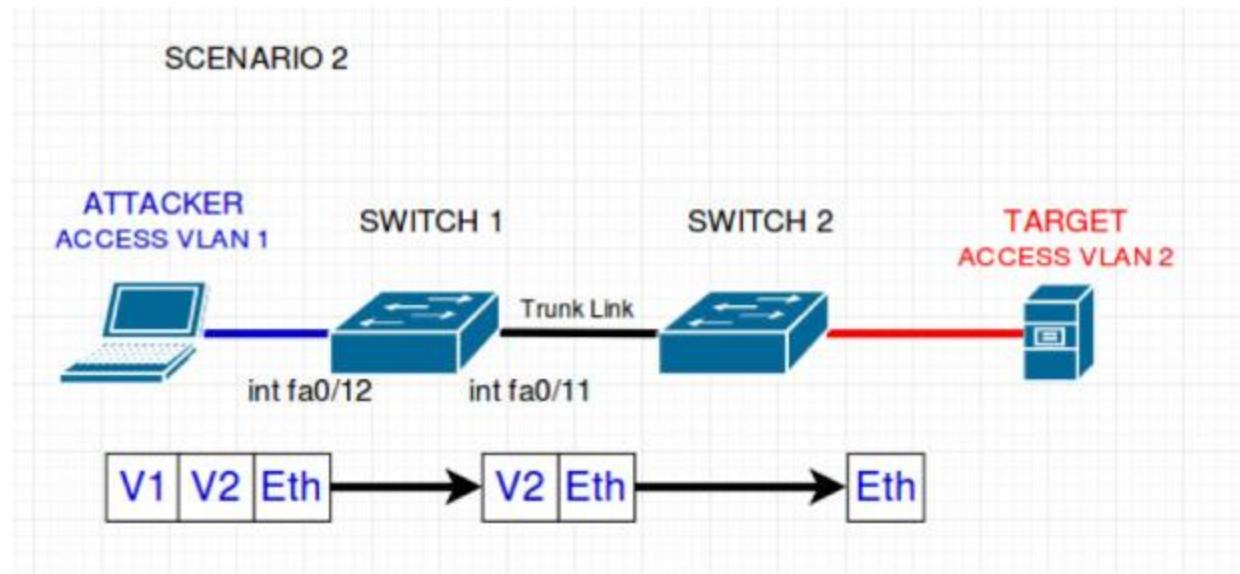


Image 8: Double Tagging Attack Process (cybersecurity.att.com)

switch 1 reads removes only the outside tag. 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

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.

Conclusion

I hope this helps understand various VLAN attacks and makes the concept simpler. On other hand, attacking a Vlan is tough. And never forget to change the default settings of your devices.

A few points for the administrators would be:

- Manage switches in as secure a manner
- The native VLAN ID should not be used for trunking. Always use a dedicated VLAN ID for all trunk ports.
- Set all user ports to non trunking
- Do configure port-security feature in the switch for more protection. (Note: be careful about configuring the port-security feature.)
- Avoid using VLAN 1
- Deploy port-security where possible for user ports
- Enable BPDU Guard for STP attack mitigation
- Use private VLAN where appropriate to further divide L2 networks
- If VTP is used, use MD5 authentication.
- Unused ports can be disabled.

List of Sources

1. Johannes Fernandes Andry, Design and Simulation VLAN Using Cisco Packet Tracer: A Case Study (2016), 66-67.
2. Simon Heron, <https://www.redscan.com/news/ten-top-threats-to-vlan-security/> (2022)
3. Cisco Networking Academy's Introduction to VLANs, <https://www.ciscopress.com/> (2014)
4. Multilayer-Switched, [Switch Spoofing - Multilayer Switched - Cisco Certified Expert \(ccexpert.us\)](#), (2022)
5. VLAN Hopping, https://en.wikipedia.org/wiki/VLAN_hopping, (2022)