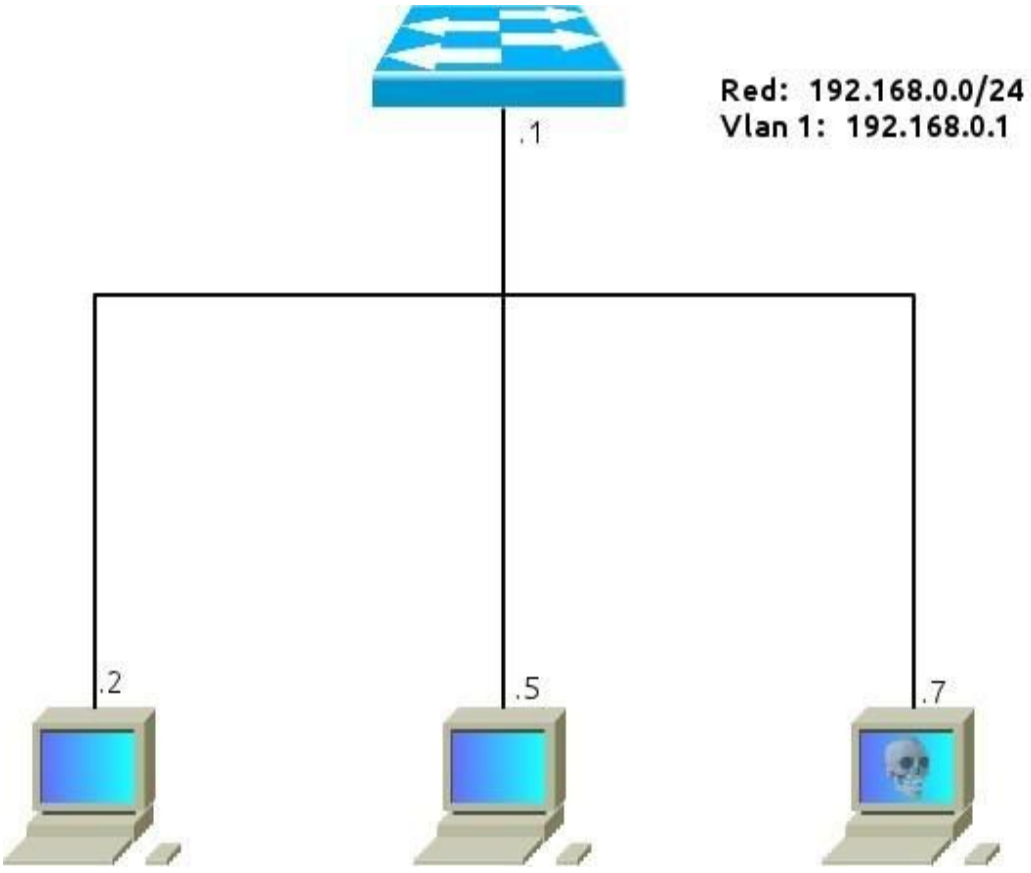
Practica 1 (Mac Flooding Attack)

4.1.1. ESCENARIO.



HARWARE

- 3 terminales con sistema Operativo linux.
- Switch Catalyst Cisco 2960.

4.1.1.2. Batería

- Macof

Paso 1: Ejecutamos nuestro terminal en “Open device”
Paso 2: En la casilla input tipeamos enable para poner nuestro Switch en modo EXEC.()
Switch> enable

Paso 3: Configuramos el Switch

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname ALS1 (Nombre del

switch ALS1) ALS1(config)#interface vlan 1

(entramos a configurar Vlan 1)

ALS1(config-if)#ip address 192.168.0.1 255.255.255.0 (Le asignamos una ip y su respectiva máscara)

ALS1(config-if)#no shutdown (Activamos Vlan 1)
%LINK-5-CHANGED: Interface Vlan1,
changed state to up ALS1(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,

changed state to up ALS1(config-if)#end Salimos del modo de

configuración.

%SYS-5-CONFIG_I: Configured from

console by console ALS1#

4.1.1.3.2. ***Dsniff***

Es una colección de herramientas para auditar la red y pruebas de penetración. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean la red de forma pasiva para recopilar datos de interés. (contraseñas, correos electrónicos, archivos, etc). arpspoof, dnsspoof, y macof facilitan facilitan la intercepción del tráfico de red normalmente inaccesible para un atacante (Por ejemplo. Debido a los switches de capa 2). sshmitm y webmitm implementan ataques activos man-in-the-middle contra redirección de sesiones SSH[14] y HTTPS[15] por explotación de enlaces débiles en PKI ad-hoc[16].

4.1.1.3.2.1. Para Monitorear La Red De Forma Pasiva.

Dsniff.captura de contraseñas para FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft, SMB, Oracle SQL*Net, Sybase y Microsoft SQL. **Filesnarf**. Vertederos de todos los archivos enviados vía NFS.
Mailsnarf. Vertederos de e-mail en formato leible de SMTP y POP.

Msgsnarf. Vertederos de mensajes instantáneos

Urlsnarf. Captura url's en http.

Webspy. Espejos de páginas web buscadas por un usuario en tiempo real.

Macof. Inunda switches con MAC's hasta hacerlos fallar y convertirlos en hub.

4.1.1.3.2.2. instalación Dsniff

Paso 4: Desde root en fedora digitamos el comando:

*[root@labdisca04 ~]# **yum install** dsniff*

-------Desde Ubuntu

root@labdisca:/home/labdisca# **apt-get install** dsniff

4.1.1.3.2.3. Ejecutando dsniff.

Paso 5: Desde el switch observamos nuestra tabla mac addres-table count ue nos muestra la cantidad de macs asignadas.

show MAC address-table count

Este comando nos muestra el número de direcciones MAC utilizadas y el total de direcciones MAC disponibles:

Para el ataque por inundamiento de MAC's usaremos la herramienta macof de dsniff

¡Importante!. Este ataque puede colapsar una red por eso debemos asegurarnos que la interfaz que vamos a usar sea una red creada por nosotros para ello ejecutamos el comando "ifconfig" y nos aseguramos de usar la interfaz correcta. En mi caso use la interfaz eth3.

Paso6: Como root en nuestra consola de comandos digitamos el comando:

[root@labdisca04 ~]# macof -i eth3

Aquí comienza nuestro ataque

53:1e:43:4c:35:c8 2f:b2:30:7e:ee:c 0.0.0.0.30486 > 0.0.0.0.49942: S 961023746:961023746(0) win 512

2a:4f:5b:10:25:36 65:81:6c:35:7a:6c 0.0.0.0.21499 > 0.0.0.0.3740: S 1055267698:1055267698(0) win 512

b9:5e:3a:6f:e2:9b a7:92:e7:49:a6:49 0.0.0.0.35379 > 0.0.0.0.64005: S 1362531159:1362531159(0)

win 512

da:24:9:17:23:cf f2:d8:e5:59:42:ec 0.0.0.0.63081 > 0.0.0.0.21289: S 188090032:188090032(0) win 512

a7:f0:4:22:6c:71 56:0:84:74:7d:c9 0.0.0.0.55353 > 0.0.0.0.45537: S 1922743052:1922743052(0) win 512

be:1c:fc:d:9a:7b b0:e1:c4:6c:49:7 0.0.0.0.32637 > 0.0.0.0.53107: S 401293249:401293249(0) win 512

7e:2e:99:b:90:93 23:7c:c:37:ef:6c 0.0.0.0.48063 > 0.0.0.0.30270: S 830091504:830091504(0) win 512

c6:f2:2b:42:17:75 30:ee:e1:50:cc:29 0.0.0.0.18647 > 0.0.0.0.5838: S 1146686082:1146686082(0) win 512

a3:af:bd:19:95:79 ad:c5:6b:2c:d5:97 0.0.0.0.30076 > 0.0.0.0.32859: S 1165148507:1165148507(0) win 512

3f:d8:27:c:e5:40 c:f5:ac:6b:96:97 0.0.0.0.42711 > 0.0.0.0.59796: S 375668839:375668839(0) win 512

44:21:f6:15:bd:8b f4:da:65:23:4d:76 0.0.0.0.37701 > 0.0.0.0.32353: S 1362788995:1362788995(0) win 512

d:c3:d2:31:1e:9d e3:b6:d2:24:f9:e6 0.0.0.0.7764 > 0.0.0.0.10864: S 1101044559:1101044559(0) win 512

98:a4:0:53:56:c1 c2:51:45:14:52:d8 0.0.0.0.14560 > 0.0.0.0.32709: S 729141755:729141755(0) win 512

b8:9:50:7f:ab:34 eb:3d:7d:5d:62:7 0.0.0.0.50256 > 0.0.0.0.48702: S 1408858971:1408858971(0)

dentro de la consola de vemos como el atacante envía paquetes con direcciones MAC aleatóriamente.

Paso 7: Vamos al switch y observamos que se muestran mensajes aceptando peticiones MAC.

Paso 8: Ahora vamos a ver qué sucedido con nuestra tabla MAC para ello abrimos consola, se muestran mensajes donde el switch continúa aprendiendo la nueva tabla cuando su tabla llega al límite de direcciones MAC colapsa. Ejecutamos el comando:

show MAC address-table count

Después del ataque observamos en la tabla que las direcciones MAC dinámicas fueron asignadas en su totalidad y el switch ya no acepta mas asociaciones por tanto este enviará por todos los puertos adquiriendo el comportamiento de un hub.

Práctica (Mitigación Usando Port Security)

Paso 9: Ahora vamos a proteger todos los puertos de nuestro Switch usando Port security. Desde la terminal cutecom vamos a ejecutar los siguientes comandos.

ALS1$ enable

ALS1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ALS1(config)#interface range fa0/1 – 10 (entramos al modo de configuración de los

puertos 1 al 10) ALS1(config-if-range)#switchport port-security

Command rejected: FastEthernet0/1 is a

dynamic port. Command rejected:

FastEthernet0/2 is a dynamic port.

Esto quiere decir que el puerto no puede ser configurado como puerto seguro si se encuentra de forma dinámica, sólo se puede cuando el puerto está en modo “static acces” o modo “trunk”.

ALS1(config-if-range)#switchport

mode access

ALS1(config-if-range)#switchport

port security

Si se ingresa solamente el comando básico, se asumen los valores por defecto: solo permite una dirección MAC en el puerto, que será la primera que se conecte al mismo, en caso de que otra dirección MAC intente conectarse utilizando el mismo puerto, este será deshabilitado o bloqueado. Claro esta que todos estos parámetros son modificables.

Switch(config-ig)#switchport port-security maximum [cantidad de MAC permitidas]

Esta opción permite definir el número de direcciones MAC que está permitido que se conecten a través de la interfaz del swtich. El número máximo de direcciones permitidas por puerto va desde 1 a 132. Es importante tener presente que este feature (rasgo) también limita la posibilidad de un ataque de seguridad por inundación de la tabla CAM (ver definiciones) del switch. El siguiente ejemplo ilustra la configuración sobre los de los puertos 1 al 10 para

que solo acepten solo 1 direccion MAC como máxima posible.

ALS1(config-if-range)#switchport port-security maximum 1

Ettercap es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

ALS1(config-if)# switchport port-security violation [shutdown restrict protect]

Este comando establece la acción que tomará el switch en caso de que se supere el número de direcciones MAC que se establece con el comando anterior. Las opciones son deshabilitar el puerto, alertar al Administrador de la Red o permitir exclusivamente el tráfico de la MAC que se registró inicialmente. En el siguiente ejemplo trabajando con los puerto 1 al 10 del switch, podemos especificar qué hacer si ese número de direcciones MAC es superado (por default deshabilitar el puerto)

Que deje de prender:

Switch(config-if)# switchport port-security violation protect

Que envíe alertas administrativas:

Switch(config-if)# switchport port-security violation restrict

Que deshabilite el puerto del switch:

Switch(config-if)# switchport port-security violation shutdown

Paso 10: Para nuestro caso vamos a hacer que el switch deshabilite el puerto cuando se presente el ataque.

ALS1(config-if)# switchport port-security violation shutdown

Posterior al haber deshabilitado el puerto del switch, este se puede volver habilitar con el siguiente comando previa autorización del Administrador de la Red:

Switch(config-if)# switchport port-security
mac-address Switch(config-if)# shutdown
Switch(config-if)# no shutdown

switchport port-security mac-address [MAC address]

Esta opción permite definir manualmente la dirección MAC que se permite conectar a través de ese puerto, o dejar que la aprenda dinámicamente varias direcciones MAC. Ejemplo:
ALS1(config)#interface range FastEthernet 0/1 - 10

(Dentro del modo configuración del puerto a configurar)

Switch(config-if)# switchport port-security mac-address sticky

(esta opcion leera y aprendera la primera mac-address que se conecte)

Switch(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

(este comando te permitirá definir una mac-address estática) es decir:

1. Con la primera línea de comando le digo que agregue las MACs que va aprendiendo a la lista de MACs seguras.
2. Con la segunda línea de comando, que agregue la MAC xx:xx:xx:xx:xx a la lista de MACs seguras.
3. Si no agrego una segunda MAC, la primera MAC que escuche distinta a xx:xx:xx:xx:xx:xx será agregada a la lista de MACs seguras.

Atención..! Este comando no debe ser configurado en un puerto troncal o de backbone, ya que por estos puertos circulan tramas con múltiples direcciones MAC, diferentes de origen. Esto daría como resultaría el bloqueo del puerto.

Paso 10: A continuación configuraremos los puertos del 1 al 10 para que el switch proteja sus puertos aprendiendo las direcciones MAC que se conecten:

ALS1#configure terminal

Enter configuration commands, one per line. End with

CNTL/Z. ALS1(config)#interface range fa0/1 - 10

ALS1(config-if-range)#switchport port-security

mac-address sticky

ALS1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down administratively down

ALS1(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Paso 11: Ahora vamos a monitorizar el estado de los puertos.
ALS1#show port-security address

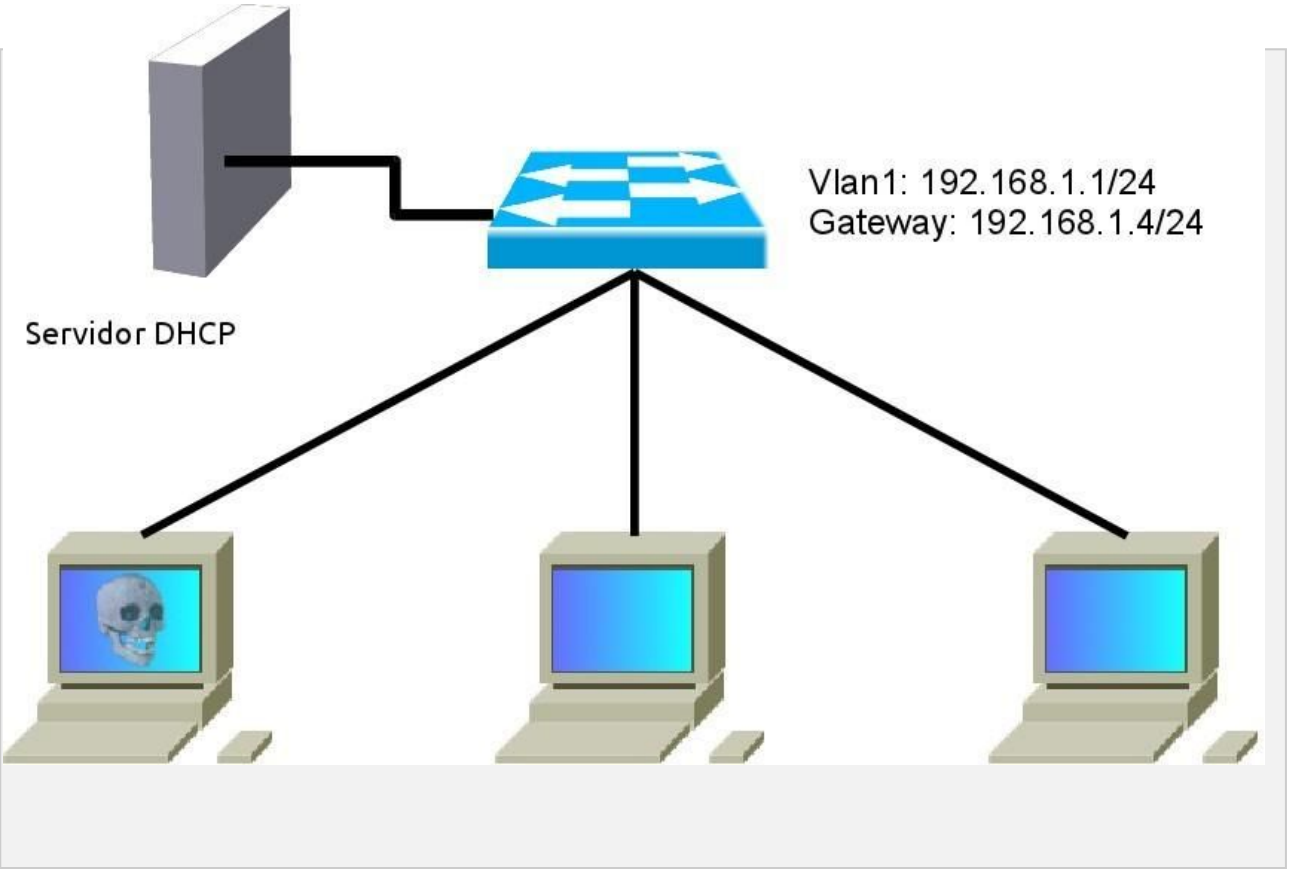
Secure Mac Address Table

Vlan	*Mac Address*	*Type*	*Ports*	*Remaining Age (mins)*
1	*0267.E422.11B4*	*SecureSticky*	*FastEthernet0/1*	*-*
1	*001E.683F.C8E0*	*SecureSticky*	*FastEthernet0/2*	*-*
1	*0800.E454.415B*	*SecureSticky*	*FastEthernet0/5*	*-*

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 6021

Práctica Ataque DHCP STARVATION (Agotamiento De Direcciones).



4.5.1. Escenario

4.5.1.1. DESCRIPCIÓN

DHCP starvation es un ataque que consiste en inundar con peticiones DHCP_REQUEST al servidor DHCP, con direcciones MAC falseadas y con el objetivo de agotar su espacio de direcciones asignables. El objetivo es que el servidor DHCP no sea capaz de responder a otros clientes y así realizar otro tipo de ataques (DHCP rogue).

4.5.1.2. HERRAMIENTAS

4.5.1.2.1. Hardware

- Servidor DHCP 3 host
- 1 switch

4.5.1.2.2. Software

- Yersinia

Yersinia es una herramienta de red diseñada para tomar ventaja de algunas debilidades en los diferentes protocolos de red. Pretende ser un framework sólido para analizar y probar redes y sistemas.

En la actualidad, hay algunos protocolos de red implementado, pero otros están por venir.
Los ataques de los siguientes protocolos de red se pueden implementar.

- Spanning Tree Protocol (STP) Cisco Discovery
- Protocol (CDP) Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP) Hot
- Standby Router Protocol (HSRP)
- IEEE 802.1Q IEEE 802.1X
- Inter-Switch Link Protocol (ISL) VLAN Trunking
- Protocol (VTP)

4.5.1.2.2.1. INSTALACIÓN

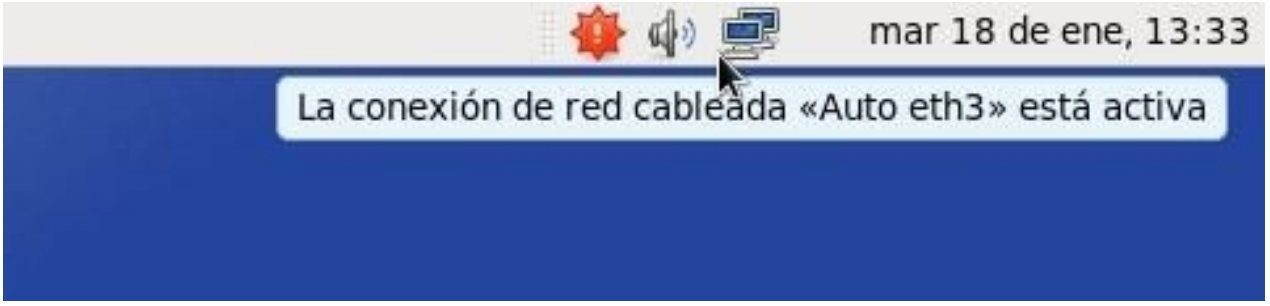
Para Fedora:
yum install yersinia

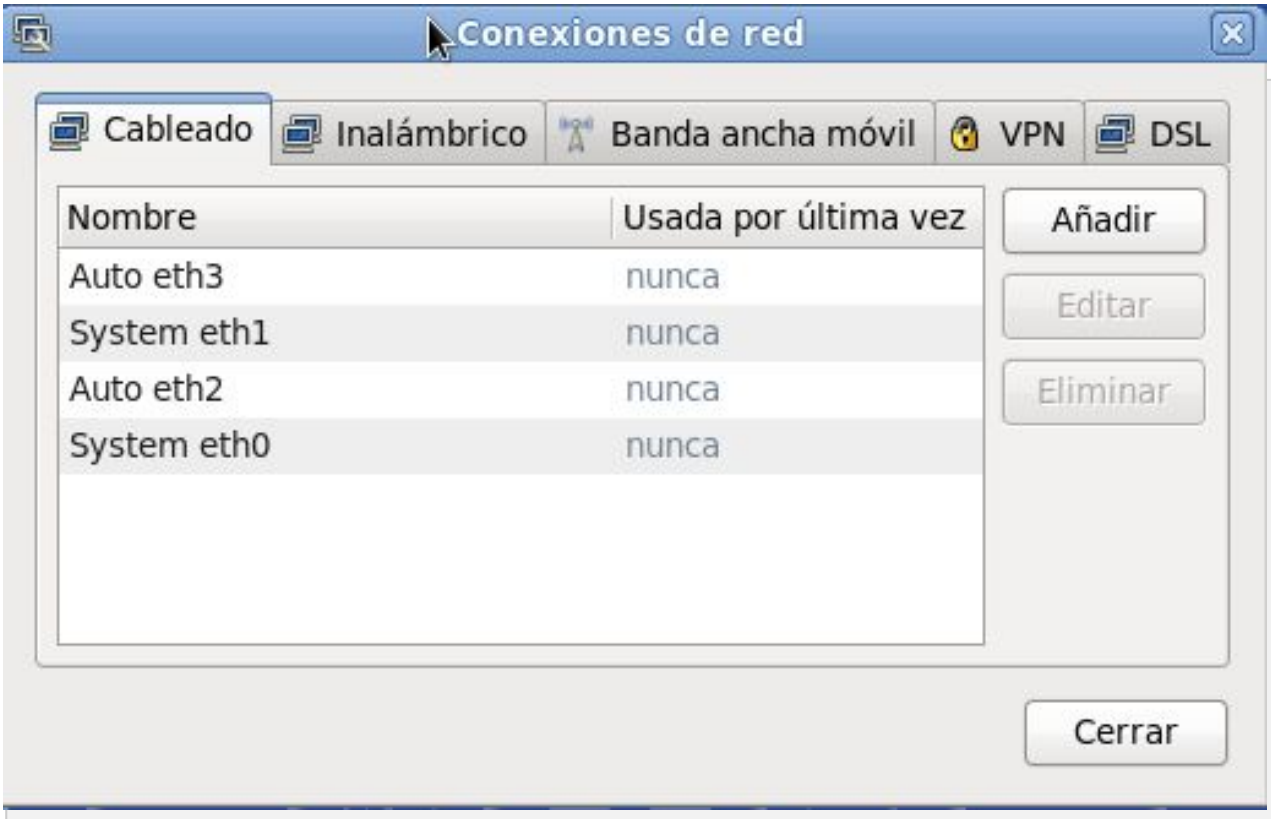
Para Ubuntu:
apt-get install yersinia

4.5.1.3. CONFIGURACIÓN DE LA IP DINÁMICA

Una vez conectado y configurado el servidor DHCP al Switch procedemos a la configuración de la IP dinámica en cada una de las terminales.

Paso 1: Hacemos click derecho sobre el icono de conexiones de red y seleccionamos Editar las conexiones.





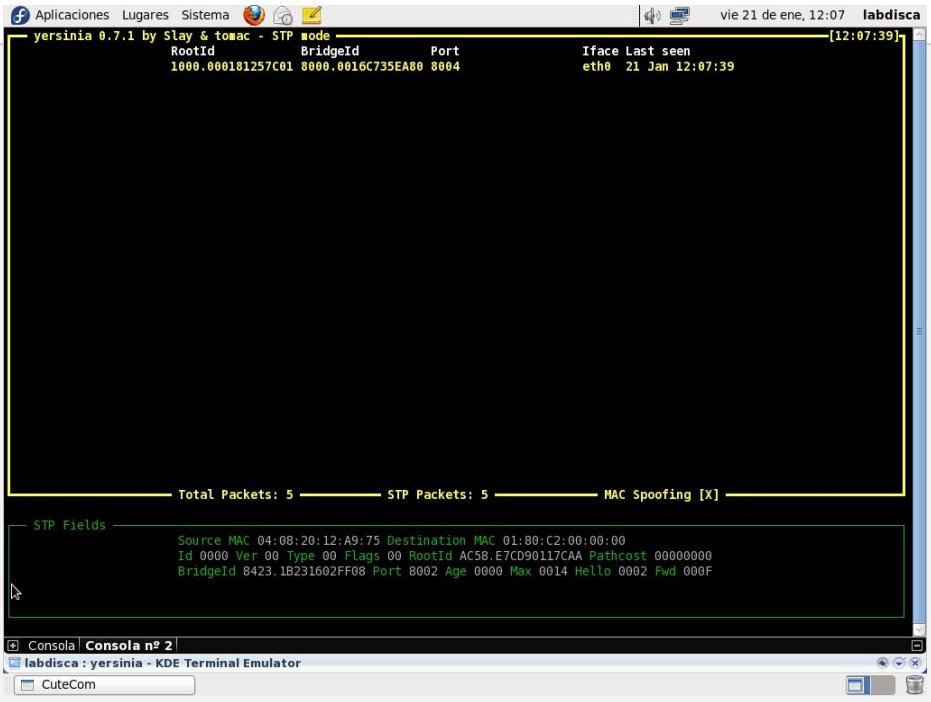
Paso 2: En la ventana de conexiones de red seleccionamos nuestro puerto que está conectada al Switch en este caso eth3 y la editamos.

Paso 3: En ajustes de Ipv4 seleccionamos Método - Automático (DHCP)

Paso 4: Hacemos click en Aplicar introducimos contraseña de administrador y cerramos conexiones de red. Revisamos configuración. (Figura 4.33)

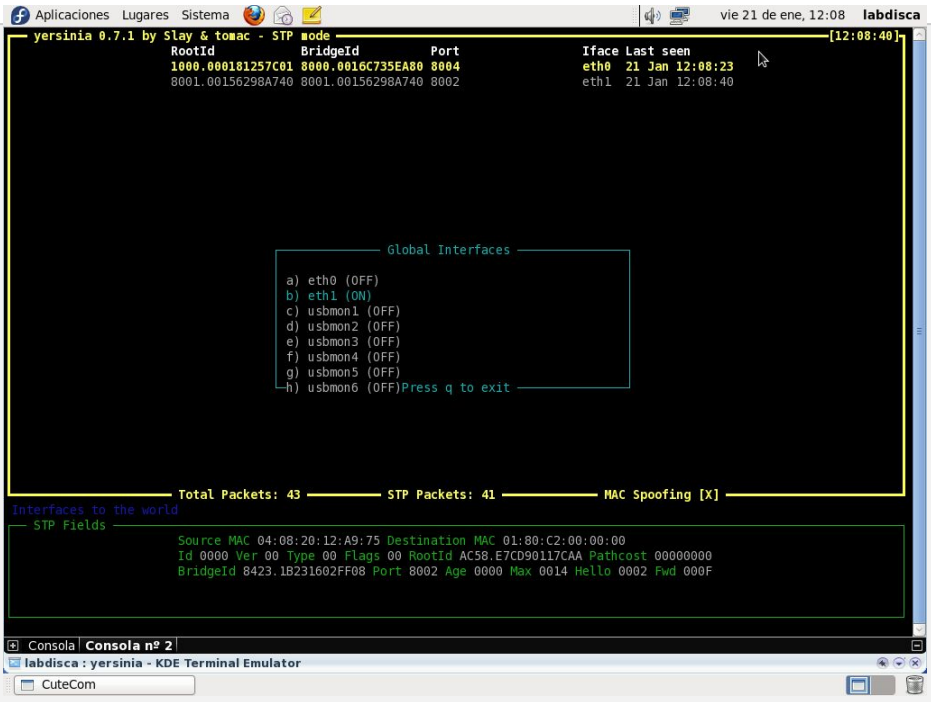
4.5.2. DHCP Starvation Con Yersinia

Paso 5:

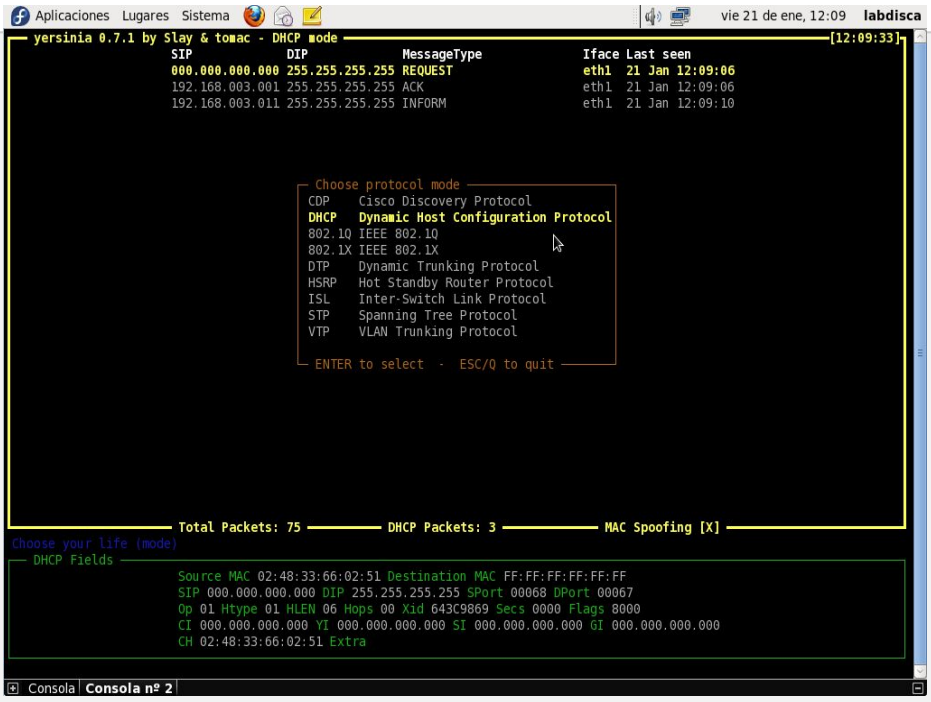


Ejecutamos yersinia con digitando el comando yersinia -I. (Figura 4.34)

Paso 6: Seleccionamos la NIC que deseemos usar presionando i por defecto el toma la



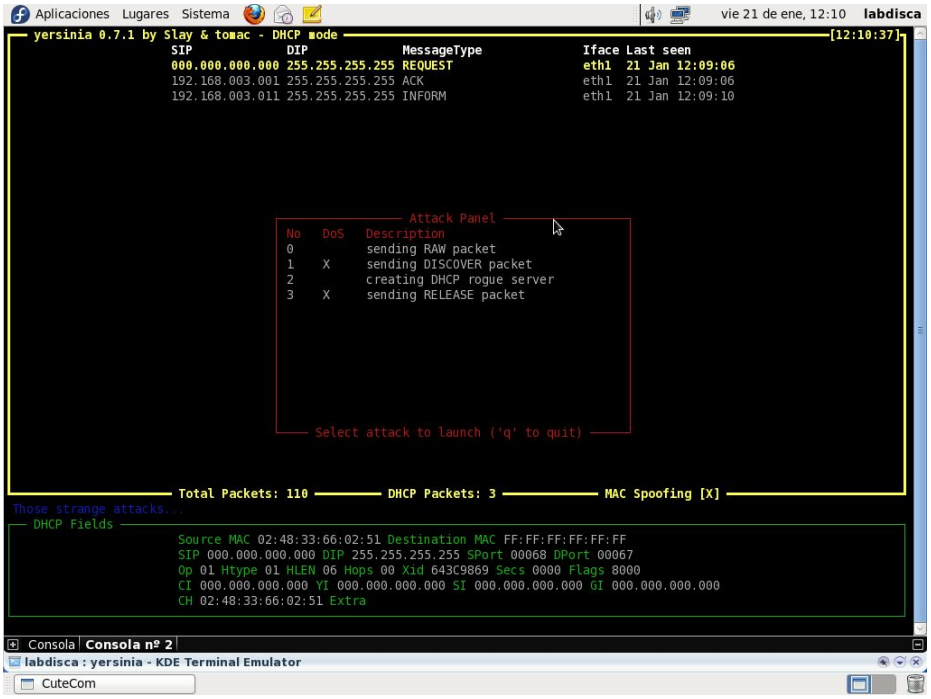
primera interface que es eth0 presionamos la letra que corresponda a la NIC en este caso la “a” para seleccionarla y seleccionamos eth1 presionando la tecla “b” para seleccionarla y luego presionamos la tecla “q” para salir.



Paso 7: Luego presionamos la tecla “g” para cargar el ataque, seleccionamos DHCP con “flecha arriba/abajo”. Y presionamos ENTER para seleccionar. (Figura 4.36)

Paso 8: Presionamos “x” para abrir el menú de ataques. Figura 4.37

Paso 9: Presionamos 1 para iniciar nuestro ataque.



Aquí ya hemos ejecutado nuestro ataque DHCP starvation.

Mitigación de DHCP Starvation.

Para evitar este ataque vamos a usar DHCP snooping.

Paso 10: Borramos la información del switch consultar “Anexos. Borrar la información de un Switch o Router Cisco.”

Paso 11: Accedemos al switch. Digitamos los siguientes comandos:

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch#hostname ALS1

ALS1(config)#ip dhcp snooping

ALS1(config)# ALS1(config)#interface fa 0/2

ALS1(config-if)#

ALS1(config-if)#ip dhcp snooping trust

ALS1(config-if)#ip arp inspection trust

Hasta aquí ya hemos mitigado el ataque DHCP Starvation y nuestro switch comienza a filtrar mensajes de los puertos no confiables.

Ataque DHCP Rouge.

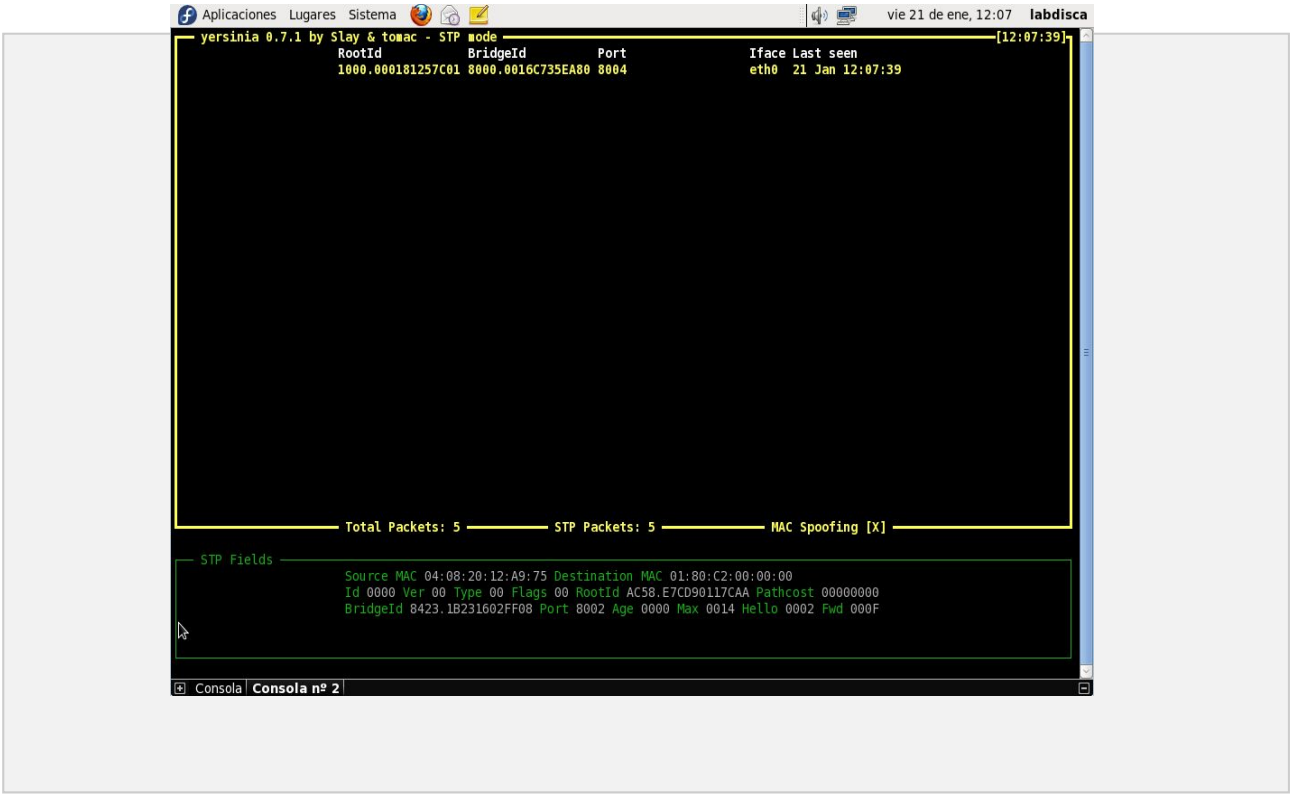
4.6.1. Descripción.

Configurando un Servidor DHCP rogue es una de las técnicas en las que un atacante puede usar para ganar acceso al trafico de red. Este es alcanzado por respuestas spoofing que pueden ser enviadas por un Servidor DHCP autorizado.

4.6.2. Escenario.

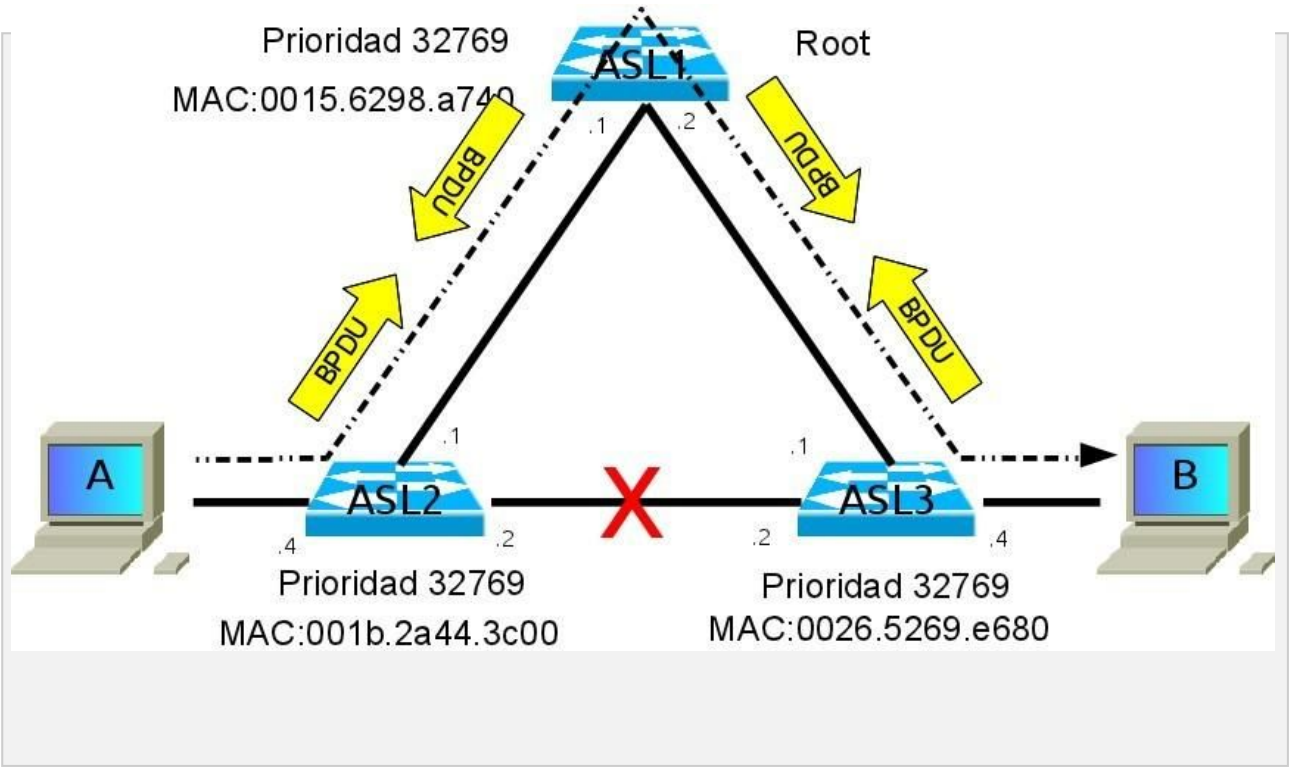
El mismo que en DHCP Starvation.

Paso 1: Para este ataque continuamos desde el paso 5 del ataque DHCP starvatión



Accedemos al Switch y borramos el Vlan.dat y el startup-config

Practica Ataque Spanning Tree.



4.8.1. Escenario: Ataque STP Face 1

Para este ataque haremos el montaje mostrado en el diagrama.

- Necesitamos tres Switches.
- 2 Host
- Un Host con 2 tarjetas de red el cual va actuar como atacante.

Vamos a nombrar a los Switches ALS1, ALS2 y ALS3.

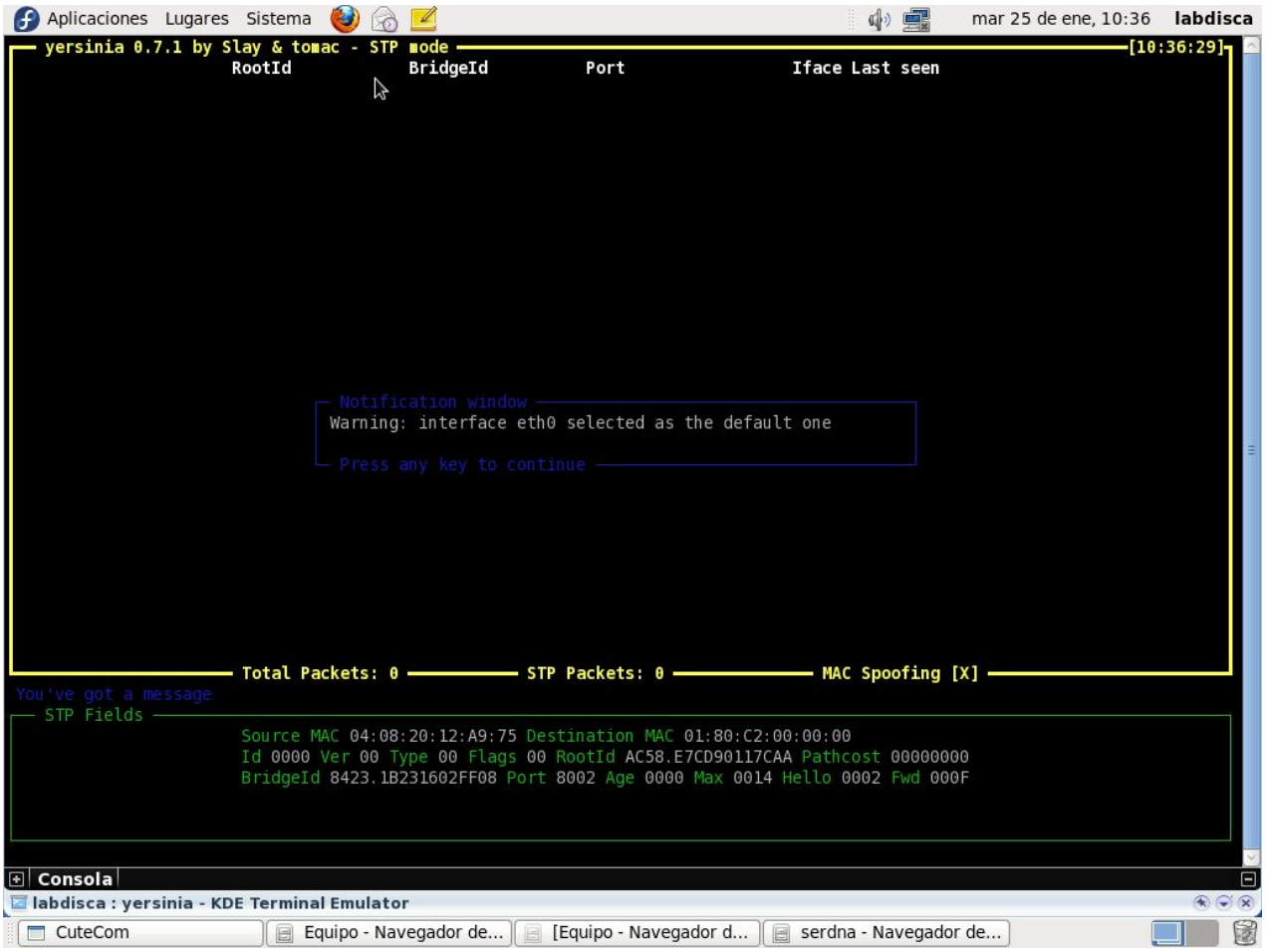
Paso 1: Borramos la información del switch consultar “Anexos. Borrar la información de un Switch o Router Cisco.”

Paso 2: Ingresamos a Cutecom y configuramos cada uno de los Switches (Configuración inicial)

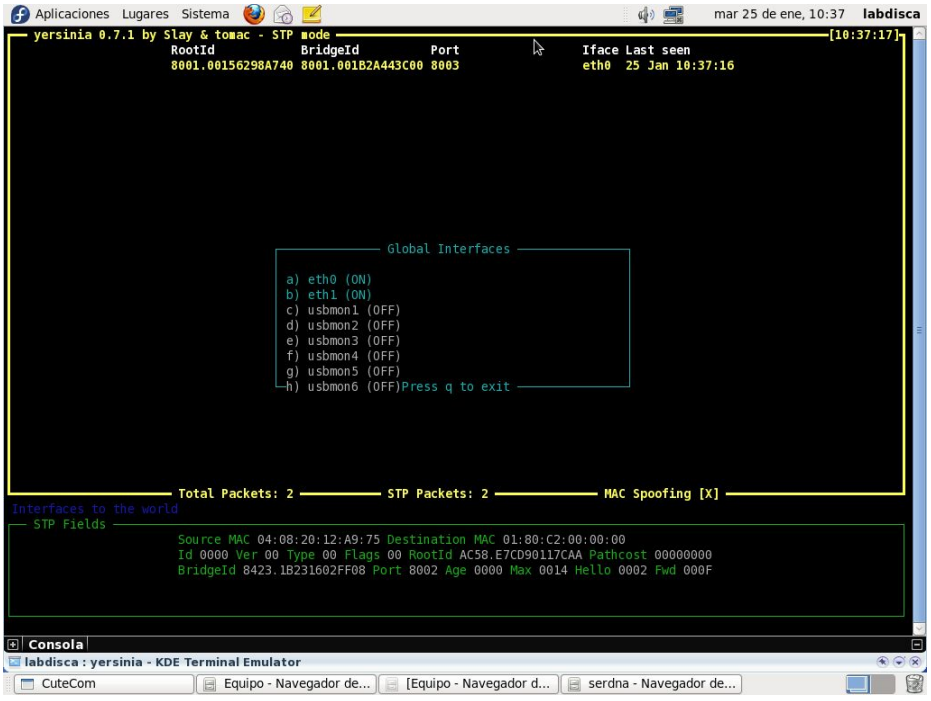
Paso 3: Observamos como queda configurado el STP en cada uno de los switches.

Implementando Un Ataque STP Con Yersinia.

Paso 4: [root@labdisca04 ~]# Yersinia -I

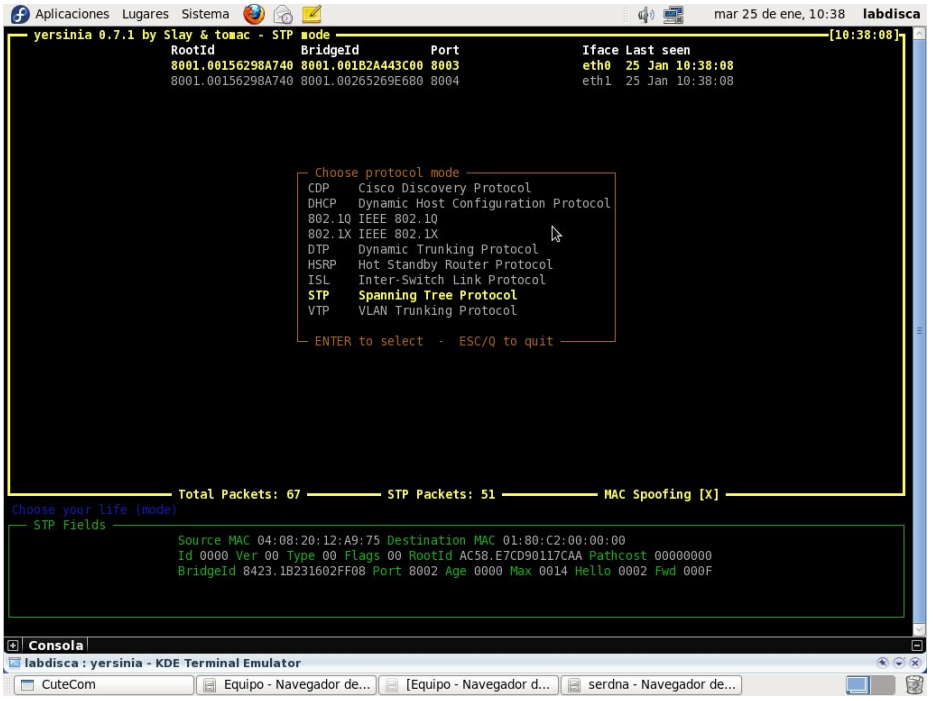

Aplicaciones Lugares Sistema
mar 25 de ene, 10:36 labdisca
yersinia 0.7.1 by Slay & tomac - STP mode
[10:36:29]
RootId BridgeId Port Iface Last seen
Notification window
Warning: interface eth0 selected as the default one
Press any key to continue
Total Packets: 0
STP Packets: 0
MAC Spoofing [X]
You've got a message
STP Fields
Source MAC 04:08:20:12:A9:75 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId AC58.E7CD90117CAA Pathcost 00000000
BridgeId 8423.1B231602FF08 Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
Consola
labdisca : yersinia - KDE Terminal Emulator
CuteCom
Equipo - Navegador de...
[Equipo - Navegador d...
serdna - Navegador de...

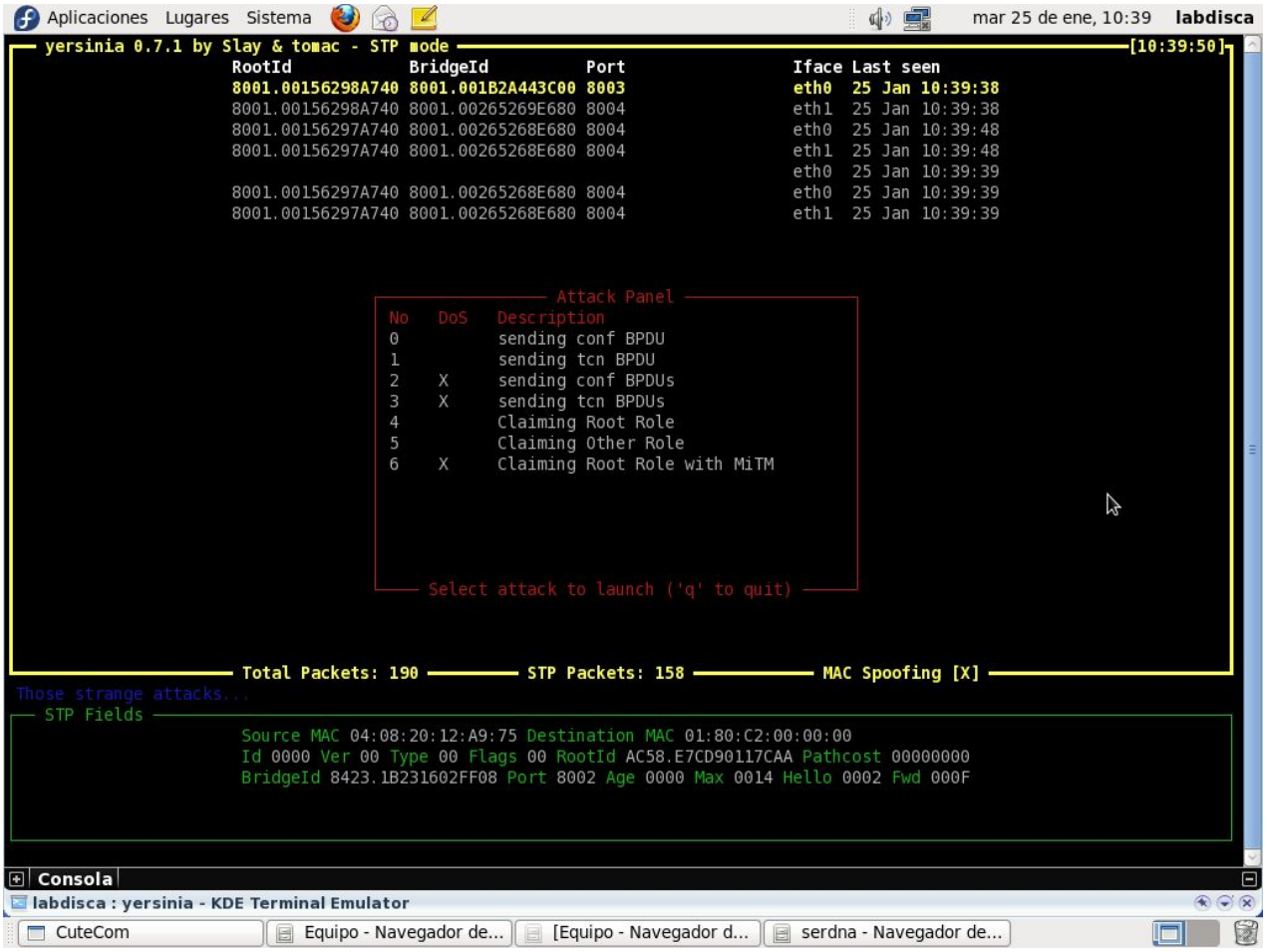
Paso 5: Digitamos i en el teclado y elegimos tanto eth0 como eth1, estos corresponden a los puertos eth2 y eth3 de nuestro atacante pulsamos solamente b para elegir eth1 ya que eth0 está por defecto.



Paso 6: Movemos Flecha arriba/ abajo y escogemos STP Spanning tree Protocol.

Paso 7: Tecleamos x para entrar al menú de ataques y elegimos la opción 6 pulsando 6 en el teclado. Para convertirnos en Root





Interface Role Sts Cost Prio.Nbr Type

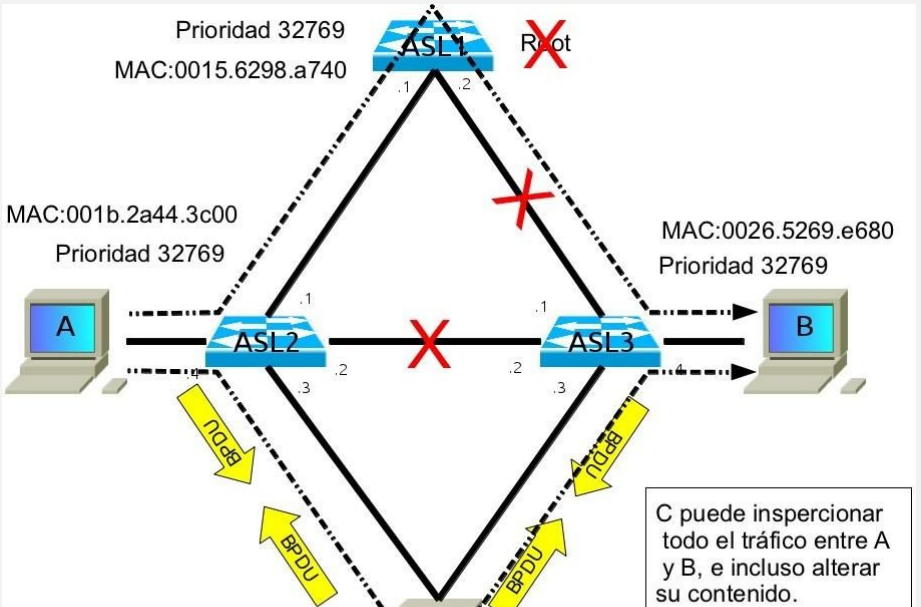
---------- ---- --- --------- -------- --------------------------------

Fa0/1 Desg FWD 19 128.2 P2p

Fa0/2 Altn BLK 19 128.3 P2p

Fa0/3 Root FWD 19 128.4 P2p

Fa0/4 Desg FWD 19 128.5 P2p



Si nos damos cuenta la configuración del STP ha cambiado. Y el ALS1 dejó de ser root la configuración nueva se muestra en el gráfico

Practica 10: Mitigación Ataque STP: Root Guard

Para mitigar el ataque STP vamos a usaremos BPDU Guard en cada uno de los los puertos donde estén conectados nuestros host.

Paso 9: Ingresamos a cutecom y configuramos ALS2 y ALS3 con RootGuard. Que es donde tenemos conectados nuestras terminales.

ALS2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ALS2(config)#interface range fastEthernet 0/3 - 4

ALS2(config-if-range)#spanning-tree guard root

ALS2(config-if-range)#end ALS2#

ALS3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ALS3(config)#interface range fastEthernet 0/3 - 4

ALS3(config-if-range)#spanning-tree guard root

ALS3(config-if-range)#end ALS3#

En un campo real es recomendable configurar Root guard en todos los puertos que no estén conectados a otros switches.

Paso 9: verificamos nuevamente el Spanning-Tree en cada uno de los Switches.

show spanning-tree

CONCLUSIONES

- Hasta este punto se tiene la capacidad para distinguir los ataques básicos que se pueden presentar a nivel de capa 2 y como prevenirlos

- Se tiene la capacidad de mejorar la seguridad en la red, de acuerdo a su configuración y montaje.

- Se tiene la capacidad de manejar diferentes herramientas de ataque y como emplearlas

  Se tiene la capacidad de emplear diferentes herramientas de Seguridad Dispositivos Cisco de acuerdo a su montaje en la red.