Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Práctica 1: Ataque por denegación de servicios

Seguridad de las comunicaciones por Internet

Autor: Cheuk Kelly Ng Pante (alu0101364544@ull.edu.es)

Fecha: 24 de noviembre de 2025

Índice general

1. Análisis y Configuración de Interfaces de Red

Ejecutar el comando para listar todas las interfaces de red:

```
ip addr show
```

Forma abreviada: `ip a`

1.1. Enumeración de Interfaces

Para cada interfaz activa (eth0, lo, wlan0), documentar:

- **Dirección MAC:** Valor `link/ether`
- **Direcciones IP:** `inet` (IPv4) e `inet6` (IPv6)
- **Dirección Broadcast:** Valor `brd`
- **Estado:** `STATE UP` o `STATE DOWN`
- **MTU:** Valor numérico `mtu`

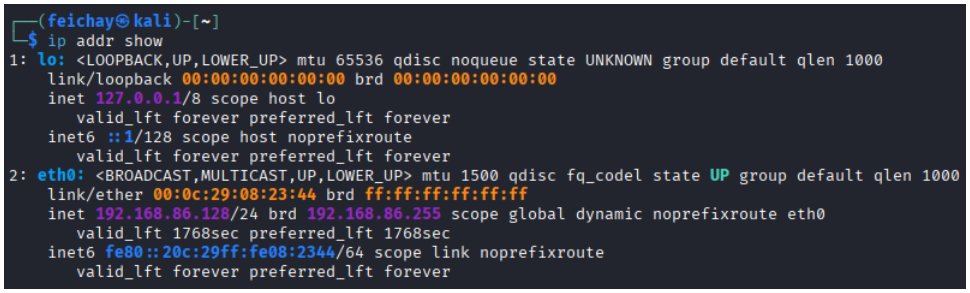

Figura 1.1: Salida del comando `ip addr show`

2. Gesión del Estado de la Interfaz y Escalado de Privilegios

2.1. Intento sin privilegios

Intentar deshabilitar la interfaz eth0:

```
ip link set eth0 down
```

Resultado esperado: Error de permiso denegado.

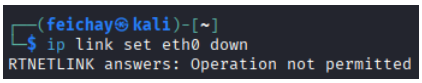

Figura 2.1: Error al intentar deshabilitar eth0 sin privilegios

2.2. Ejecución con privilegios

Ejecutar con `sudo`:

```
sudo ip link set eth0 down
```

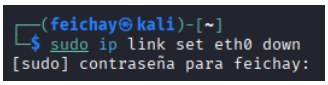

Figura 2.2: Deshabilitación exitosa de eth0 con privilegios

2.3. Verificación de conectividad

Confirmar que la interfaz está inactiva:

```
ip a
```

Intentar acceder a un sitio web para verificar pérdida de conectividad.

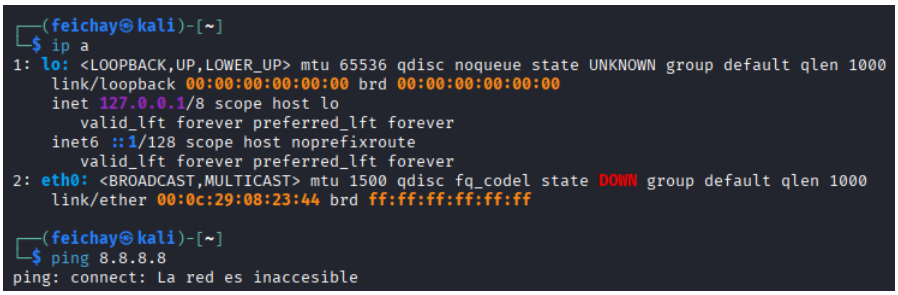

Figura 2.3: Verificación de estado inactivo de eth0

2.4. Reactivación

Restaurar la interfaz:

```
sudo ip link set eth0 up
```

Validar la restauración con `ip a` y verificar conectividad a Internet.

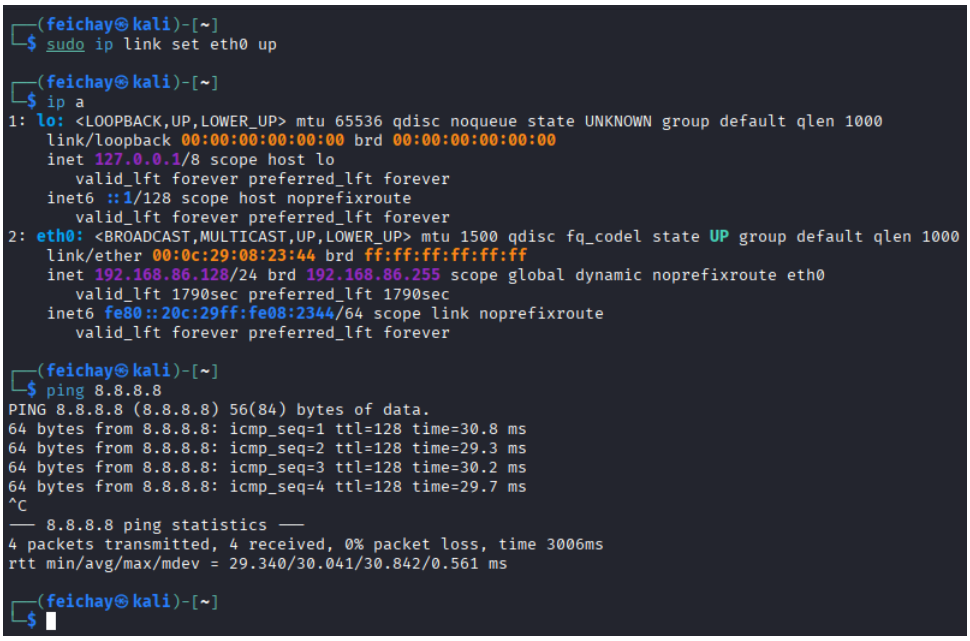

Figura 2.4: Reactivación exitosa de eth0

2.4.1. Comandos adicionales

`sudo ip addr add 192.168.1.200/24 dev eth0`

Figura 2.5: Asignación temporal de nueva IP a eth0

Al hacer esto el cambio es temporal y se pierde al reiniciar. Para hacerlo persistente hay que editar el fichero `/etc/network/interfaces`.

```
┌──(feichay㉿kali)-[~]
└─$ sudo vi /etc/network/interfaces

┌──(feichay㉿kali)-[~]
└─$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.1.200
        netmask 255.255.255.0

┌──(feichay㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:08:23:44 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.200/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe08:2344/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figura 2.6: Verificación de nueva IP asignada a eth0

3. Verificación de la Pila TCP/IP y Conectividad Externa

3.1. Prueba de Loopback

Ping a la interfaz de loopback:

`ping -c 4 127.0.0.1`

```
┌──(feichay㉿kali)-[~]
└─$ ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.053 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.036/0.042/0.053/0.006 ms
```

Figura 3.1: Prueba de conectividad a loopback

3.2. Prueba de Conectividad Externa

Verificar resolución DNS y conectividad WAN:

`ping -c 4 www.ull.es`

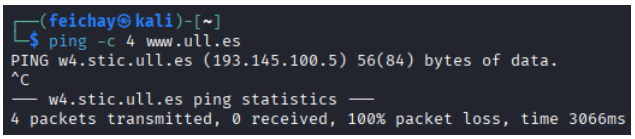

Figura 3.2: Prueba de conectividad a www.ull.es

A continuación se documentan los resultados obtenidos tras ejecutar el comando de diagnóstico de red hacia el dominio de la Universidad de La Laguna.

a. Estadísticas de Paquetes Basado en la línea final: *4 packets transmitted, 0 received, 100 % packet loss.*

- **Transmitidos:** 4
- **Recibidos:** 0
- **Pérdida (%):** 100 %

b. Estadísticas de RTT (Round-Trip Time) Debido a que la pérdida de paquetes fue total (ningún paquete retornó), el sistema no pudo calcular los tiempos de viaje.

- **Mínimo:** N/A (No disponible)
- **Promedio (Avg):** N/A (No disponible)
- **Máximo:** N/A (No disponible)

Observación: El fallo en la recepción de paquetes (100 % de pérdida) sugiere que el host destino (`193.145.100.5`) está inactivo o, lo más probable, que existe un firewall bloqueando las solicitudes ICMP.

4. Análisis de la Caché del Protocolo ARP

Inspeccionar la traducción de direcciones IP a MAC en la LAN.

4.0.1. Comando tradicional

```
arp -a
```

4.0.2. Alternativa moderna

Usando el comando `ip`:

```
ip neigh
```

4.1. Resultados

Anotar las entradas que mapean IP-MAC de dispositivos en la red, especialmente la puerta de enlace (router).

5. Inspección de la Tabla de Enrutamiento

Analizar cómo el sistema decide dónde enviar el tráfico. Para mostrar la tabla de enrutamiento:

```
ip route show
```

Forma abreviada: `ip r`

5.1. Análisis

Identificar la ruta por defecto (`default via ...`) que indica la IP de la puerta de enlace.

6. Trazado de Ruta de Red (Traceroute)

6.1. Objetivo

Determinar los saltos (routers intermedios) entre la máquina y un destino.

6.2. Desarrollo

Realizar trazados de ruta:

```
traceroute www.ull.es
traceroute www.net.berkeley.edu
```

6.3. Resultados

Documentar:

- Número total de saltos para cada destino
- Latencia en cada nodo

7. Escaneo de Puertos Locales con Nmap

7.1. Objetivo

Identificar puertos que están escuchando y servicios asociados en la máquina local.

7.2. Desarrollo

Escaneo con detección de versión:

```
nmap -sV localhost
```

El flag `-sV` intenta determinar la versión del servicio.

7.3. Análisis

Esto simula un reconocimiento inicial desde la perspectiva de un atacante en la misma red.

8. Análisis de Sockets y Conexiones de Red

8.1. Objetivo

Enumerar conexiones activas y puertos abiertos.

8.2. Desarrollo

8.2.1. Comando tradicional

```
netstat -tulpn
```

8.2.2. Herramienta moderna

Usando `ss` (socket statistics):

```
ss -tulpn
```

8.3. Análisis

Buscar puertos abiertos inesperados o conexiones remotas `ESTABLISHED` sospechosas.

9. Resolución de Nombres DNS (NSLookup)

9.1. Objetivo

Realizar consultas DNS para resolver nombres de dominio.

9.2. Desarrollo

Consultas con `nslookup`:

```
nslookup www.ull.es
nslookup www.w3c.org
```

9.3. Documentación

Identificar y documentar:

- Servidor DNS que resuelve la consulta (indicado como `Server`)
- Registros A (IPv4) resueltos para cada dominio

10. Interacción de Red con Netcat (nc)

10.1. Objetivo

Comprender el uso de Netcat para depuración y explotación de redes.

10.2. Desarrollo

10.2.1. Revisión de opciones

```
nc -h
```

10.2.2. Sintaxis clave

1. **Modo Escucha (Listener):**

   ```
   nc -l -p 1234
   ```

2. **Modo Cliente:**

   ```
   nc <IP_remota> <puerto>
   ```

11. Reconocimiento DNS Avanzado con dnsenum

11.1. Objetivo

Recopilar inteligencia de fuentes abiertas (OSINT) sobre un dominio.

11.2. Desarrollo

Ejecutar `dnsenum`:

```
dnsenum tecnomobile.com
```

11.3. Análisis

Extraer información clave:

1. Registros de Host (A/AAAA)
2. Servidores de Nombres (NS)
3. Servidores de Correo (MX)
4. Sub-enumeración de subdominios

12. Análisis de Tráfico en Terminal con tcpdump

12.1. Objetivo

Analizar paquetes de red en línea de comandos.

12.2. Desarrollo

Captura básica (requiere privilegios):

```
sudo tcpdump -i eth0 -n -c 20
```

12.2.1. Explicación de flags

- `-i eth0`: Escucha en la interfaz eth0
- `-n`: No resuelve nombres DNS/IPs
- `-c 20`: Captura 20 paquetes y se detiene

12.3. Observaciones

Observar el flujo de tráfico en tiempo real y documentar los datos relevantes.