

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	1
1.1. Enumeración de Interfaces	1
2. Gestión del Estado de la Interfaz y Escalado de Privilegios	1
2.1. Intento sin privilegios	1
2.2. Ejecución con privilegios	1
2.3. Verificación de conectividad	2
2.4. Reactivación	2
2.4.1. Comandos adicionales	2
2.5. Resultados	2
3. Configuración de Direcciones IP Estáticas	2
3.1. Objetivo	2
3.2. Asignación Temporal	2
3.3. Configuración Persistente	2
4. Verificación de la Pila TCP/IP y Conectividad Externa	3
4.1. Objetivo	3
4.2. Desarrollo	3
4.2.1. Prueba de Loopback	3
4.2.2. Prueba de Conectividad Externa	3
4.3. Análisis de Resultados	3
5. Análisis de la Caché del Protocolo ARP	3
5.0.1. Comando tradicional	3
5.0.2. Alternativa moderna	3
5.1. Resultados	3
6. Inspección de la Tabla de Enrutamiento	3
6.1. Análisis	4
7. Trazado de Ruta de Red (Traceroute)	4
7.1. Objetivo	4
7.2. Desarrollo	4
7.3. Resultados	4
8. Escaneo de Puertos Locales con Nmap	4
8.1. Objetivo	4
8.2. Desarrollo	4
8.3. Análisis	4
9. Análisis de Sockets y Conexiones de Red	4
9.1. Objetivo	4
9.2. Desarrollo	5

9.2.1. Comando tradicional	5
9.2.2. Herramienta moderna	5
9.3. Análisis	5
10. Resolución de Nombres DNS (NSLookup)	5
10.1. Objetivo	5
10.2. Desarrollo	5
10.3. Documentación	5
11. Interacción de Red con Netcat (nc)	5
11.1. Objetivo	5
11.2. Desarrollo	5
11.2.1. Revisión de opciones	5
11.2.2. Sintaxis clave	6
12. Reconocimiento DNS Avanzado con dnsenum	6
12.1. Objetivo	6
12.2. Desarrollo	6
12.3. Análisis	6
13. Análisis de Tráfico en Terminal con tcpdump	6
13.1. Objetivo	6
13.2. Desarrollo	6
13.2.1. Explicación de flags	6
13.3. Observaciones	7

1. Análisis y Configuración de Interfaces de Red

Ejecutar el comando para listar todas las interfaces de red:

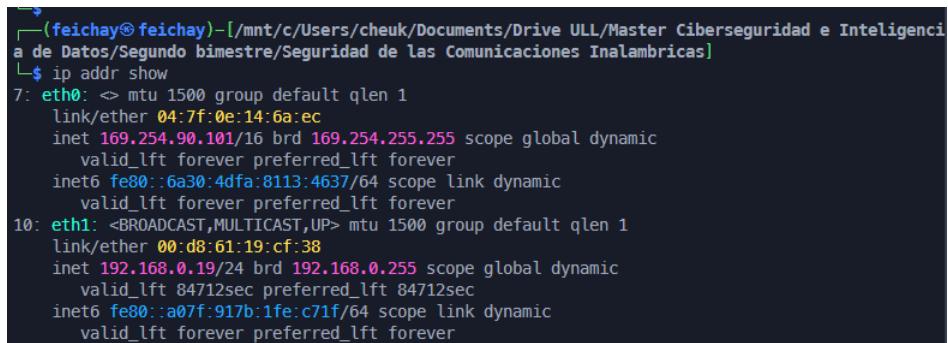
```
ip addr show
```

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`



```
(feichay@feichay) [/mnt/c/Users/cheuk/Documents/Drive ULL/Master Ciberseguridad e Inteligencia de Datos/Segundo bimestre/Seguridad de las Comunicaciones Inalambricas]
$ ip addr show
7: eth0: <mtu 1500 group default qlen 1
    link/ether 04:7f:0e:14:6a:ec
    inet 169.254.90.101/16 brd 169.254.255.255 scope global dynamic
        valid_lft forever preferred_lft forever
    inet6 fe80::6a30:4dfa:8113:4637/64 scope link dynamic
        valid_lft forever preferred_lft forever
10: eth1: <BROADCAST,MULTICAST,UP> mtu 1500 group default qlen 1
    link/ether 00:d8:61:19:cf:38
    inet 192.168.0.19/24 brd 192.168.0.255 scope global dynamic
        valid_lft 84712sec preferred_lft 84712sec
    inet6 fe80::a07f:917b:1fe:c71f/64 scope link dynamic
        valid_lft forever preferred_lft forever
```

Figura 1.1: Salida del comando `ip addr show`

2. Gestión 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.

2.2. Ejecución con privilegios

Ejecutar con `sudo`:

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

2.3. Verificación de conectividad

Confirmar que la interfaz está inactiva:

```
ip a
```

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

2.4. Reactivación

Restaurar la interfaz:

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

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

2.4.1. Comandos adicionales

1. Cambiar IP de `eth0`:

```
sudo ip addr add 192.168.1.200/24 dev eth0
```

2. Asignar nueva máscara: Se incluye en la notación CIDR (/24)

3. Configuración persistente: Editar `/etc/network/interfaces`

2.5. Resultados

[Documentar los resultados obtenidos]

3. Configuración de Direcciones IP Estáticas

3.1. Objetivo

Comprender la diferencia entre configuración temporal y persistente.

3.2. Asignación Temporal

La configuración con `ip` es volátil:

```
sudo ip addr add 192.168.1.200/24 dev eth0
```

Esta configuración se pierde al reiniciar.

3.3. Configuración Persistente

En sistemas Debian/Kali, editar el fichero `/etc/network/interfaces` para definir:

- IP estática
- Máscara de red
- Puerta de enlace (gateway)

Nota: Este apartado es informativo y no requiere entrega.

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

4.1. Objetivo

Validar la correcta inicialización de la pila TCP/IP local y la conectividad externa.

4.2. Desarrollo

4.2.1. Prueba de Loopback

Ping a la interfaz de loopback:

```
ping -c 4 127.0.0.1
```

4.2.2. Prueba de Conectividad Externa

Verificar resolución DNS y conectividad WAN:

```
ping -c 4 www.ull.es
```

4.3. Análisis de Resultados

Documentar:

1. **Estadísticas de paquetes:** Transmitidos, recibidos, pérdida
2. **RTT (Round-Trip Time):** Mínimo, promedio, máximo

5. Análisis de la Caché del Protocolo ARP

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

5.0.1. Comando tradicional

```
arp -a
```

5.0.2. Alternativa moderna

Usando el comando ip:

```
ip neigh
```

5.1. Resultados

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

6. 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`

6.1. Análisis

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

7. Trazado de Ruta de Red (Traceroute)

7.1. Objetivo

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

7.2. Desarrollo

Realizar trazados de ruta:

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

7.3. Resultados

Documentar:

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

8. Escaneo de Puertos Locales con Nmap

8.1. Objetivo

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

8.2. Desarrollo

Escaneo con detección de versión:

```
nmap -sV localhost
```

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

8.3. Análisis

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

9. Análisis de Sockets y Conexiones de Red

9.1. Objetivo

Enumerar conexiones activas y puertos abiertos.

9.2. Desarrollo

9.2.1. Comando tradicional

```
netstat -tulpn
```

9.2.2. Herramienta moderna

Usando **ss** (socket statistics):

```
ss -tulpn
```

9.3. Análisis

Buscar puertos abiertos inesperados o conexiones remotas ESTABLISHED sospechosas.

10. Resolución de Nombres DNS (NSLookup)

10.1. Objetivo

Realizar consultas DNS para resolver nombres de dominio.

10.2. Desarrollo

Consultas con nslookup:

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

10.3. Documentación

Identificar y documentar:

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

11. Interacción de Red con Netcat (nc)

11.1. Objetivo

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

11.2. Desarrollo

11.2.1. Revisión de opciones

```
nc -h
```

11.2.2. Sintaxis clave

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

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

2. **Modo Cliente:**

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

12. Reconocimiento DNS Avanzado con dnsenum

12.1. Objetivo

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

12.2. Desarrollo

Ejecutar `dnsenum`:

```
dnsenum tecnomobile.com
```

12.3. 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

13. Análisis de Tráfico en Terminal con tcpdump

13.1. Objetivo

Analizar paquetes de red en línea de comandos.

13.2. Desarrollo

Captura básica (requiere privilegios):

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

13.2.1. Explicación de flags

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

13.3. Observaciones

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