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: 19 de noviembre de 2025

Índice general

1. Análisis y Configuración de Interfaces de Red

1.1. Objetivo

Arrancar la máquina virtual de Kali Linux y analizar las interfaces de red utilizando comandos modernos.

1.2. Desarrollo

1.2.1. Inicio de sesión

Usuario: `kali`, Contraseña: `kali`

1.2.2. Comando principal

Ejecutar el comando para listar todas las interfaces de red:

```
ip addr show
```

Forma abreviada: `ip a`

1.2.3. 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`

1.3. Resultados

[Aquí se deben incluir las capturas de pantalla y los datos obtenidos]

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

2.1. Objetivo

Comprender cómo modificar el estado de las interfaces de red requiere privilegios elevados.

2.2. Desarrollo

2.2.1. Intento sin privilegios

Intentar deshabilitar la interfaz eth0:

```
ip link set eth0 down
```

Resultado esperado: Error de permiso denegado.

2.2.2. Ejecución con privilegios

Ejecutar con `sudo`:

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

2.2.3. Verificación de conectividad

Confirmar que la interfaz está inactiva:

```
ip a
```

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

2.2.4. Reactivación

Restaurar la interfaz:

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

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

2.2.5. 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`

2.3. 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

5.1. Objetivo

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

5.2. Desarrollo

5.2.1. Comando tradicional

```
arp -a
```

5.2.2. Alternativa moderna

Usando el comando `ip`:

```
ip neigh
```

5.3. 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

6.1. Objetivo

Analizar cómo el sistema decide dónde enviar el tráfico.

6.2. Desarrollo

Mostrar la tabla de enrutamiento:

```
ip route show
```

Forma abreviada: `ip r`

6.3. 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.