Guía Práctica de Pentesting en Redes

Introducción: Esta guía está diseñada para que los alumnos realicen tres tipos de pruebas de penetración en un entorno controlado. Los ejercicios se enfocan en el uso de herramientas clave: Nmap, Hydra (con SSH) y un ataque de denegación de servicio (DoS) en Kali Linux. Es importante realizar estas actividades en un ambiente de laboratorio seguro y con autorización.

1. Exploración de Red con Nmap

Objetivo: Identificar dispositivos, puertos abiertos y servicios en una red.

1. Configurar el entorno:
   - Inicia Kali Linux.
   - Asegúrate de estar en la misma red que el objetivo.

2. Ejecutar Nmap para un escaneo básico:

```
nmap <dirección_IP_objetivo>
```

- Observa los puertos abiertos y los servicios listados.

3. Escaneo avanzado con identificación de sistemas operativos:

```
nmap -A <dirección_IP_objetivo>
```

- Verifica el sistema operativo y versiones de servicios.

4. Guardar los resultados en un archivo:

```
nmap -oN resultado_nmap.txt <dirección_IP_objetivo>
```

- Revisa el archivo con: `cat resultado_nmap.txt`

2. Fuerza Bruta con Hydra (SSH)**

Objetivo: Comprobar la fortaleza de contraseñas en un servicio SSH.

1. Configurar el entorno:
   - Identifica un objetivo con servicio SSH habilitado (puerto 22).

2. Ejecutar Hydra:

```
hydra -l <usuario> -P <ruta_lista_contraseñas> ssh://<dirección_IP_objetivo>
```

- `-l`: Especifica el nombre de usuario.
- `-P`: Indica el archivo de contraseñas (ejemplo: `/usr/share/wordlists/rockyou.txt`).

3. Ataque de Denegación de Servicio (DoS)

Objetivo: Simular un ataque DoS para evaluar la resiliencia del sistema.

1. Configurar el entorno:
   - Identifica un servidor objetivo.
   - Utiliza un servidor web local o virtualizado para pruebas.

2. Ejecutar el ataque con hping3:

   hping3 -S --flood -V -p <puerto_objetivo> <dirección_IP_objetivo>

   - `-S`: Envia paquetes SYN.
   - `--flood`: Envía paquetes de forma continua.
   - `-V`: Muestra los detalles del ataque.
   - `-p`: Especifica el puerto objetivo.

3. Monitorear el impacto:
   - Usa herramientas como `top` o `iftop` en el servidor para observar el consumo de recursos.

4. Detener el ataque:
   - Presiona `Ctrl + C` para interrumpir el ataque.