1.INTRODUCTION

1.1 Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

- Provides More than 600 penetration testing tools.
- OS Family - Unix like
- Working State - Active
- Platforms - x86, x86-64, armel, armhf
- Kernel Type - Monolithic kernel (Linux)
- Default UI - GNOME
- Latest Release – 2019.1a March 4, 2019

1.2 PENETRATION TESTING

Penetration testing which is also called pen testing is refers to the process of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit and make use of it. Pen tests can be performed manually or it can be done automatically through software applications. In either way, the process includes collecting information about the target before the test (reconnaissance), identifying possible loop holes (entry points), attempting to break in (either virtually or for real) and reporting back the findings. The main objective of penetration testing is to determine security weaknesses.

Different Strategies

- Targeted testing - Testing team working together.
- External testing - Targets externally visible servers or devices.
- Internal testing - Attack behind the firewall.
- Blind testing - Simulates the actions of a real attacker.

Targeted testing: This testing is performed by the organization's IT testing team and the penetration testing team working together. It's sometimes referred to as a "lights-turnedon" approach because everyone can see and know the test being carried out.

External testing: This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing: This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing: A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Benefits of Penetration Testing

- Intelligently manage vulnerabilities.
- Avoid the cost of network downtime.
- Meet regulatory requirements and avoid fines.
- Preserve corporate image and customer loyalty.

1.3 SQL INJECTION

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

2.0 ANDRORAT 2.1 INDRODUCTION

AndroRat (Android Remote Administration Tool) is one of the Client or Server applications written using the basic language of Android or Java. By using the AndroRat application, you can fully control other people's Smartphones through computer devices. This is certainly quite useful if you want to know the activities of children using a Smartphone.

While to be able to use the AndroRat Application, you just have to install the application on the victim's Smartphone. The good news, when the hacking process is done the victim will not see what you are doing on their Smartphone. If the AndroRat Application has been installed on the victim's Smartphone and you have successfully configured the application via a computer, then

when the targeted Android smartphone is connected to the internet network you can do the following operations through a computer device.

2.2 FEATURES

- Take a picture with the camera

- Location by GPS/Network
- Do vibrate the phone
- Send a text message
- Streaming video (for activity based client only) ▪ Get contacts and all their information.
- Stream sound from the microphone (or other sources..)
- Open a URL in the default browser
- Monitoring received messages in live
- Get all messages
- Get call logs(History)
- Monitoring phone state in live (call received, call sent, call missed..)
- Do a toast

2.3 STEPS

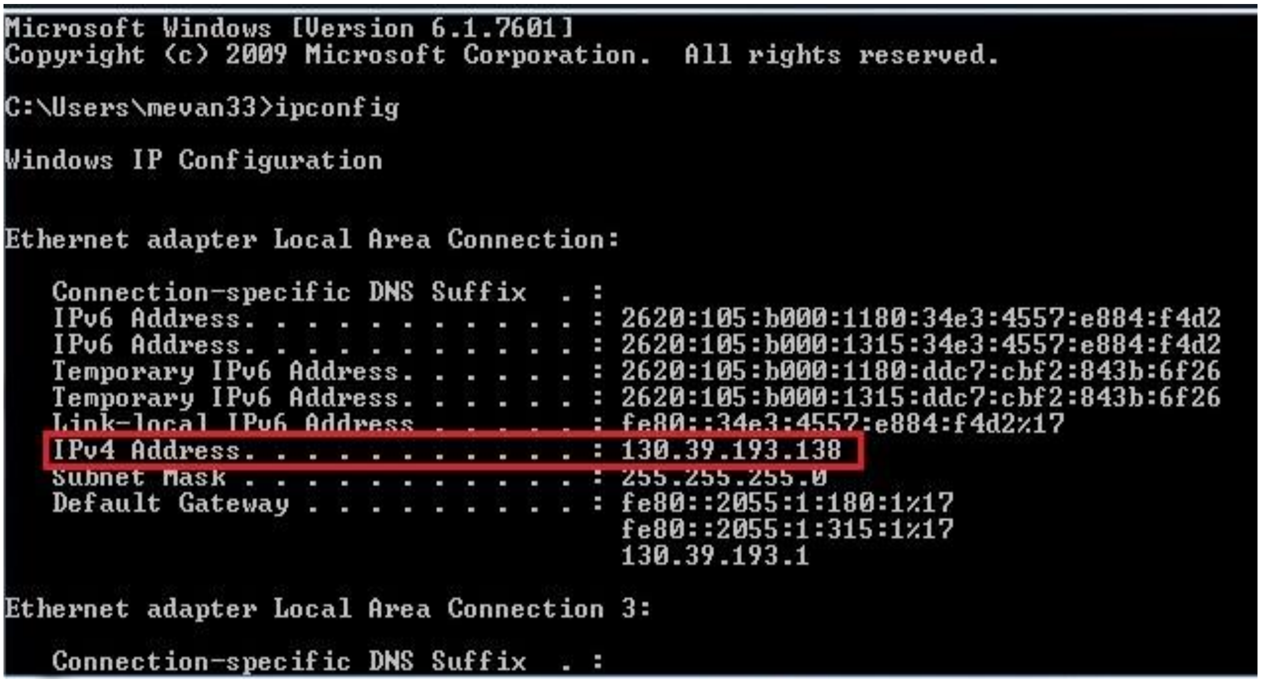
Before you can use the AndroRat application, there are some materials that are needed, as follows.

- Java must be installed on the computer.
- Router Port forwarder.
- Antivirus and firewall must be turned off.
- A computer desktop/laptop.
- An Andriod phone to deploy the client app.
- A wireless router.
- Fast internet connection

- If you have prepared all of the above materials, then it's time you learn how to use androrat on adroid device and here are some steps-by-step needed.

3.0 WORKING OF ANDRORAT

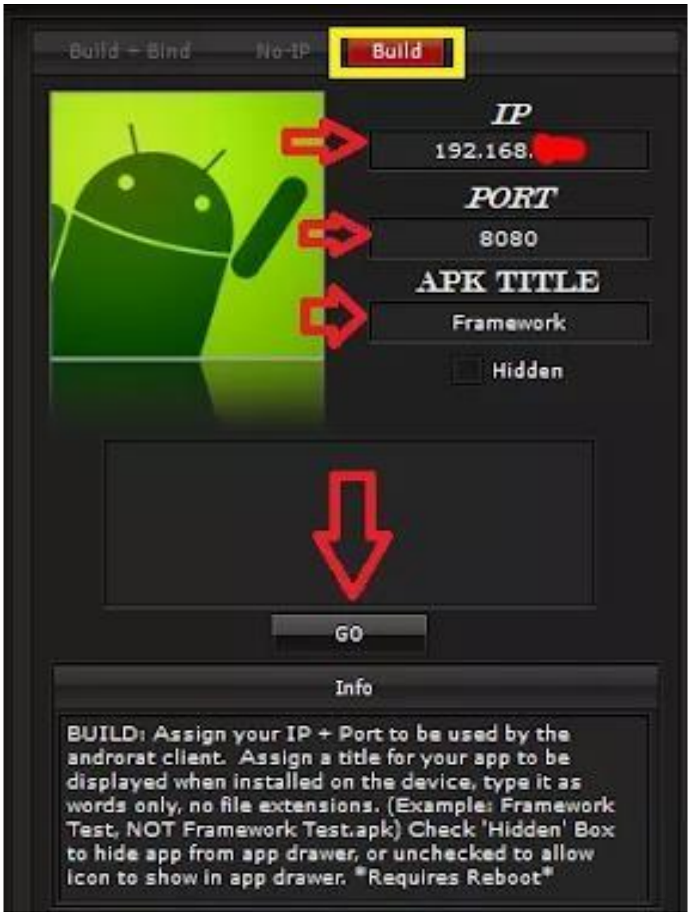
Step one, To be able to use the Port Router Forwarder you must know the IPv4 address. For that, open Command Promt (CMD) and type ipconfig then press enter. You will find an Ipv4 address, please copy the address



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\mevan33>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2620:105:b000:1180:34e3:4557:e884:f4d2
   IPv6 Address. . . . . . . . . . . : 2620:105:b000:1315:34e3:4557:e884:f4d2
   Temporary IPv6 Address. . . . . . : 2620:105:b000:1180:ddc7:cbf2:843b:6f26
   Temporary IPv6 Address. . . . . . : 2620:105:b000:1315:ddc7:cbf2:843b:6f26
   Link-local IPv6 Address . . . . . : fe80::34e3:4557:e884:f4d2%17
   IPv4 Address. . . . . . . . . . . : 130.39.193.138
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::2055:1:180:1%17
                                       fe80::2055:1:315:1%17
                                       130.39.193.1

Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
```

The second step, you need an application to be installed on the victim's Android device. For that you can create your own application using AndroRat APK Binder. Please go to AndroRat folder, and open the AndroRat Binder then select the Build option to create your own application.

- In the IP column enter your IPv4 address, fill Port with 8080, and click Go then wait for the application creation process.



IP

192.168.[redacted]

PORT

8080

APK TITLE

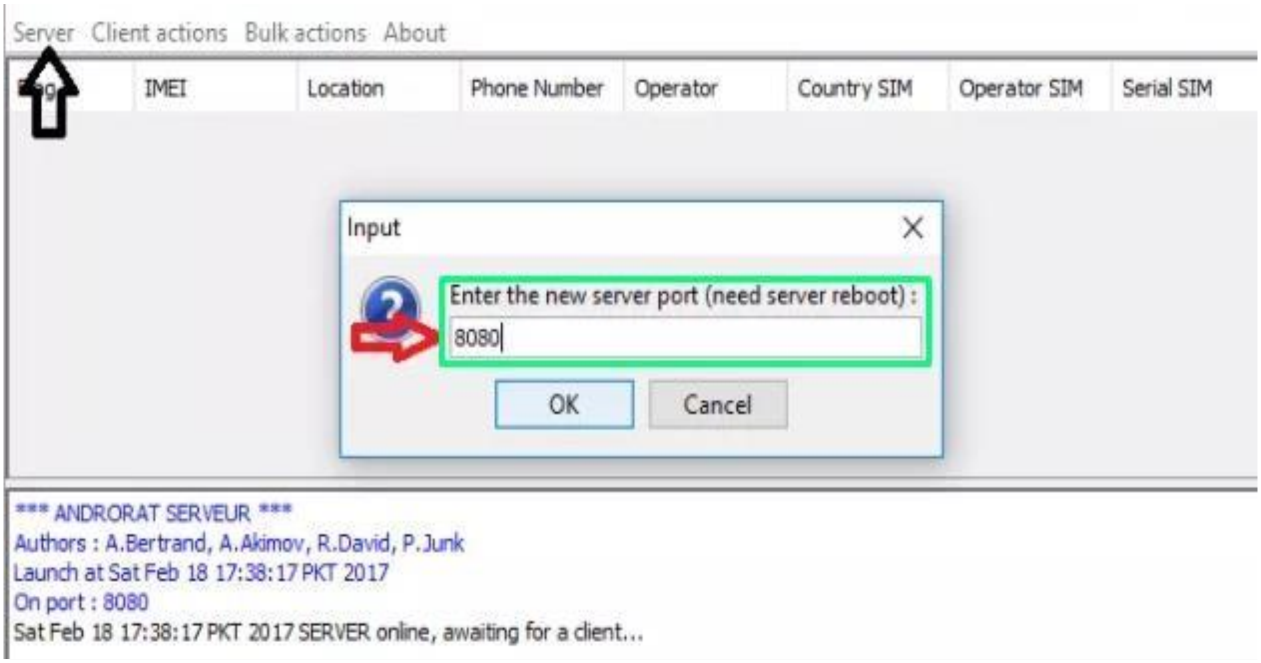
Framework

□ Hidden

BUILD: Assign your IP + Port to be used by the androrat client. Assign a title for your app to be displayed when installed on the device, type it as words only, no file extensions. (Example: Framework Test, NOT Framework Test.apk) Check 'Hidden' Box to hide app from app drawer, or unchecked to allow icon to show in app drawer. *Requires Reboot*

Up here, you will find a Frame.apk file in the same AndroRat folder. Please install the Frame.apk application on the target Smartphone.

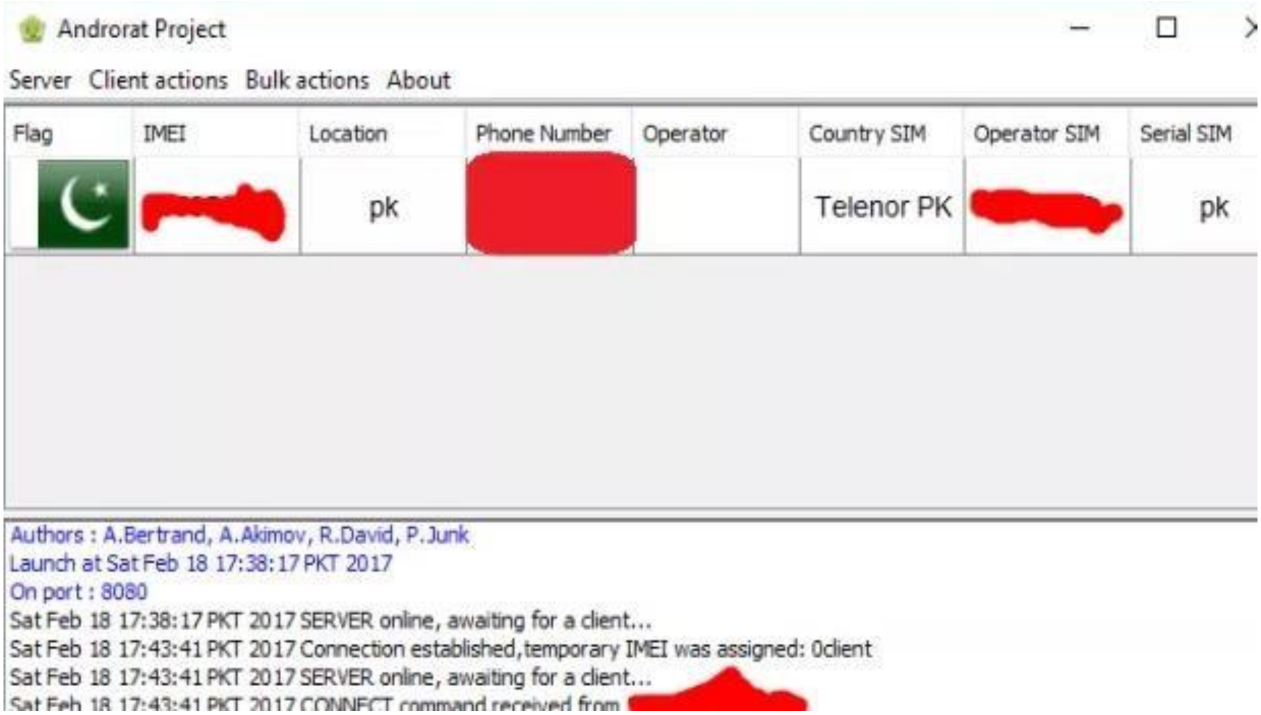
Step third- After all the steps above are passed, now you can control your target Smartphone in full Completely. Then enter the AndroRat folder, then you will see other AndroRat folders. Open and launch the AndroRat Server application. Enter the Server menu, select Port and enter 8080 according to port forwarding, then click OK. Close the application and then open it again



Enter the new server port (need server reboot) : 8080

```
*** ANDRORAT SERVEUR ***
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Sat Feb 18 17:38:17 PKT 2017
On port : 8080
Sat Feb 18 17:38:17 PKT 2017 SERVER online, awaiting for a client...
```

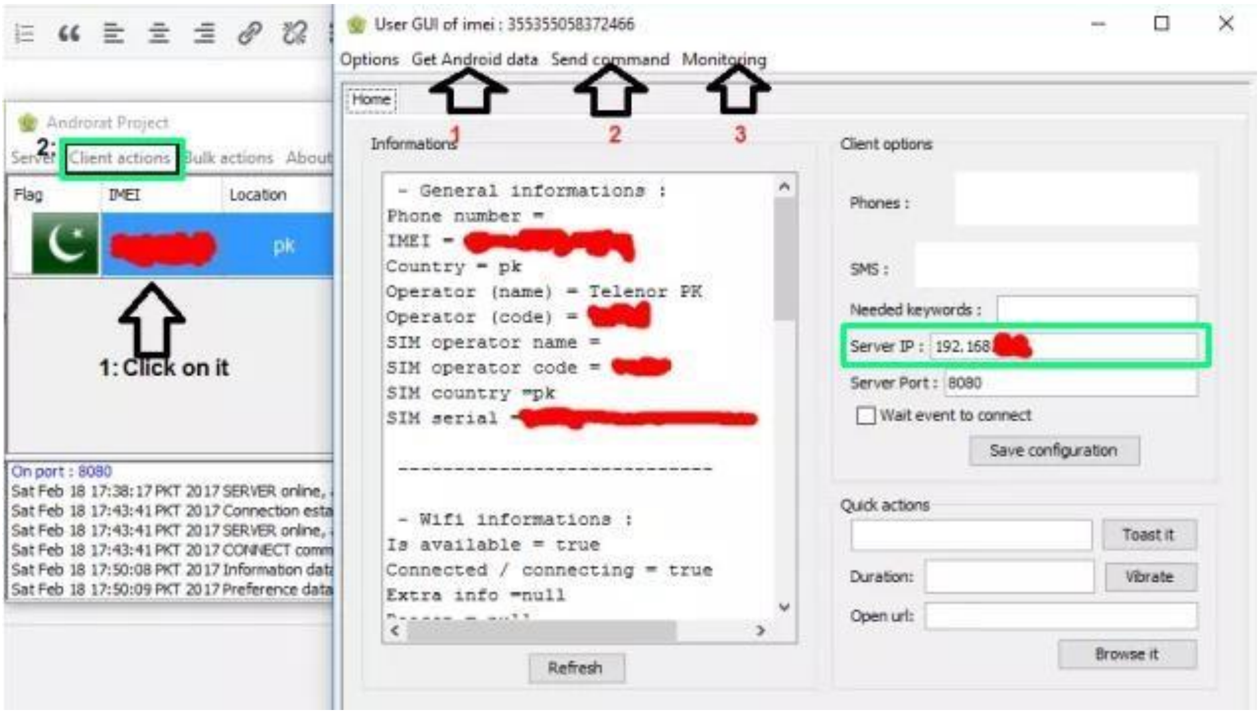
- After the application opens, wait until the application is connected to the Smartphone that is being targeted



Flag	IMEI	Location	Phone Number	Operator	Country SIM	Operator SIM	Serial SIM
	[redacted]	pk	[redacted]		Telenor PK	[redacted]	pk

```
Authors : A.Bertrand, A.Akimov, R.David, P.Junk
Launch at Sat Feb 18 17:38:17 PKT 2017
On port : 8080
Sat Feb 18 17:38:17 PKT 2017 SERVER online, awaiting for a client...
Sat Feb 18 17:43:41 PKT 2017 Connection established,temporary IMEI was assigned: 0client
Sat Feb 18 17:43:41 PKT 2017 SERVER online, awaiting for a client...
Sat Feb 18 17:43:41 PKT 2017 CONNECT command received from [redacted]
```

- Select an Android Smartphone by clicking on it, Please go and click Client and select the User Interface menu



Flag	IMEI	Location
	[redacted]	pk

```
On port : 8080
Sat Feb 18 17:38:17 PKT 2017 SERVER online,
Sat Feb 18 17:43:41 PKT 2017 Connection esta
Sat Feb 18 17:43:41 PKT 2017 SERVER online,
Sat Feb 18 17:43:41 PKT 2017 CONNECT comm
Sat Feb 18 17:50:08 PKT 2017 Information data
Sat Feb 18 17:50:09 PKT 2017 Preference data
```

```
 - General informations :
Phone number =
IMEI = [redacted]
Country = pk
Operator (name) = Telenor PK
Operator (code) = [redacted]
SIM operator name =
SIM operator code = [redacted]
SIM country =pk
SIM serial =[redacted]

 -----------------------------

 - Wifi informations :
Is available = true
Connected / connecting = true
Extra info =null
```

Phones :

SMS :

Needed keywords :

Server IP : 192.168[redacted]

Server Port : 8080

☐ Wait event to connect

Duration:

Open url:

Explanation :

1. Monitoring: In this menu, you can find out and monitor all incoming and outgoing calls and messages
2. Send Command: You can send messages and make voice calls
3. Get Android Data: With this you have access and can use the camera, microphone, contacts, SMS, call history and others

4.0 NEW PROBLEM CONCEPT

Port forwarding with ngrok.

5.0 CONCLUSION

Androrat is a solid remote administration tool, with a good spread of features and modules for nearly any type of penetration test. It works on a variety of systems and is worthy of inclusion in hacker toolkits everywhere. It does not use metasploit framework for penetration. It is still in development so it may not be as effective as metasploit framework. For advanced users, the way that payloads are generated and managed make this tool a contender for automated attacks. But there are issues creating a apk file based payload file at present and the developers has taken initiative to resolve it.

6.0 REFERENCES

https://www.apkglobe.net/app/androrat/
https://geekviews.tech/androrat/
https://www.malavida.com/en/soft/androrat/
https://github.com/DesignativeDave/androrat