

Intro to Cybersecurity

2.1.1 - Social Engineering Toolkit



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Getting Started

- In this lab we will use the Social Engineering Toolkit (SET) to create a fake website and use it to capture login credentials. This is an example of one technique used in many phishing emails

```
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
```



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Social Engineering Toolkit Lab

- Materials needed
 - Kali Linux Virtual Machine
 - Windows 7 Virtual Machine
- Software Tools used
 - SET



GALANTECH —with—
GARDEN STATE CYBER

Setup Environment

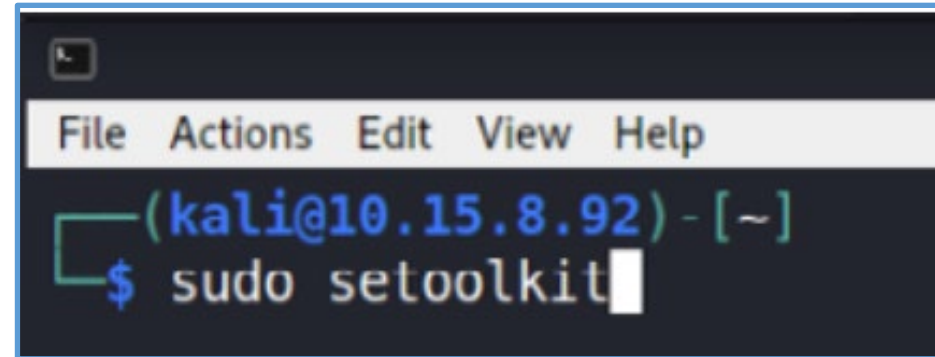
- Log into your range
- Open the Kali Linux Environment
 - You should be on your Kali Linux Desktop



GALANTECH —with—
GARDEN STATE CYBER

Launch SET

- Open a terminal
- Type `sudo setoolkit`



```
File Actions Edit View Help
(kali@10.15.8.92) - [~]
$ sudo setoolkit
```

- When presented with the terms of service, enter “y”

```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y
```



SET

- The Social-Engineering Toolkit will start, showing a menu

```
kali@kali: ~  
File Actions Edit View 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) 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> |
```



GALANTECH —with—
GARDEN STATE CYBER

Setting up the Attack

- From the SET menu, follow these selections
 - #1 Social Engineering Attacks
 - #2 Website Attack Vectors
 - #3 Credential Harvester Method
 - #1 Web Templates
 - The following will appear (with a different IP address), just press enter

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.15.7.174]:
```

- Select the Twitter web template.

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

set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

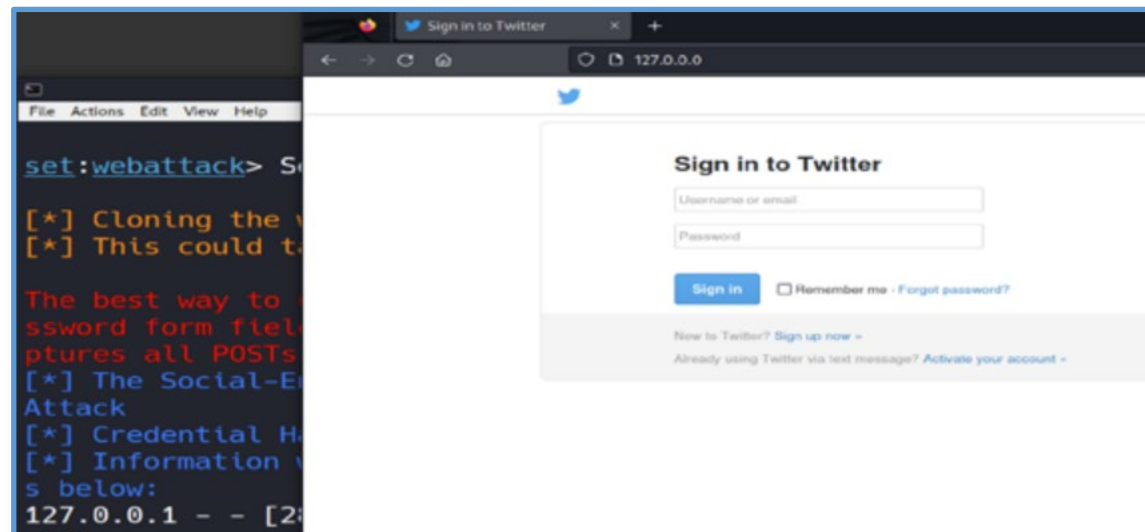
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```



GALANTECH —with—
GARDEN STATE CYBER

Playing the Victim

- Open a web browser (Firefox button to the left of the terminal in the toolbar)
- Type in 127.0.0.1
- You'll see a fake version of Twitter
- Enter a FAKE username and password and click login



Playing the Victim

- It will look like the login and webpage failed. This is because the fake webpage harvested your login information and then redirected to the real Twitter website, which will appear as blocked as it is not on the allow list for the CYBER.ORG Range
- Return to SET (in the terminal) and you should see that your username and password were captured

```
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=pascal@cyber.org  
POSSIBLE PASSWORD FIELD FOUND: session[password]=pandabear
```



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Let's Review

- Attacker uses SET to set up a fake version of a popular website login page
- Attacker takes URL link of fake page and sends it in a phishing email to lots of victims OR puts the link in a social media post
- The victim clicks the link to login to the website, not realizing this is not the real login page
- The victim enters their username and password and is redirected to the real website



GALANTECH —with—
GARDEN STATE CYBER

Let's Review

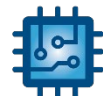
- Thinking the user typed their information incorrectly, they try again and successfully log in
- Every time a victim logs into the fake website, the attacker receives their username and password
- In the terminal running SET, press CTRL+C to shut down the current process and return to the SET menu
- If desired, try this again with Google



GALANTECH —with—
GARDEN STATE CYBER

Closure Discussion

- What kind of situations have you seen where this technique could be used?
- How could a user protect themselves against this type of attack?



GALANTECH —with—
GARDEN STATE CYBER