Cybersecurity 701

Phishing Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Phishing Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

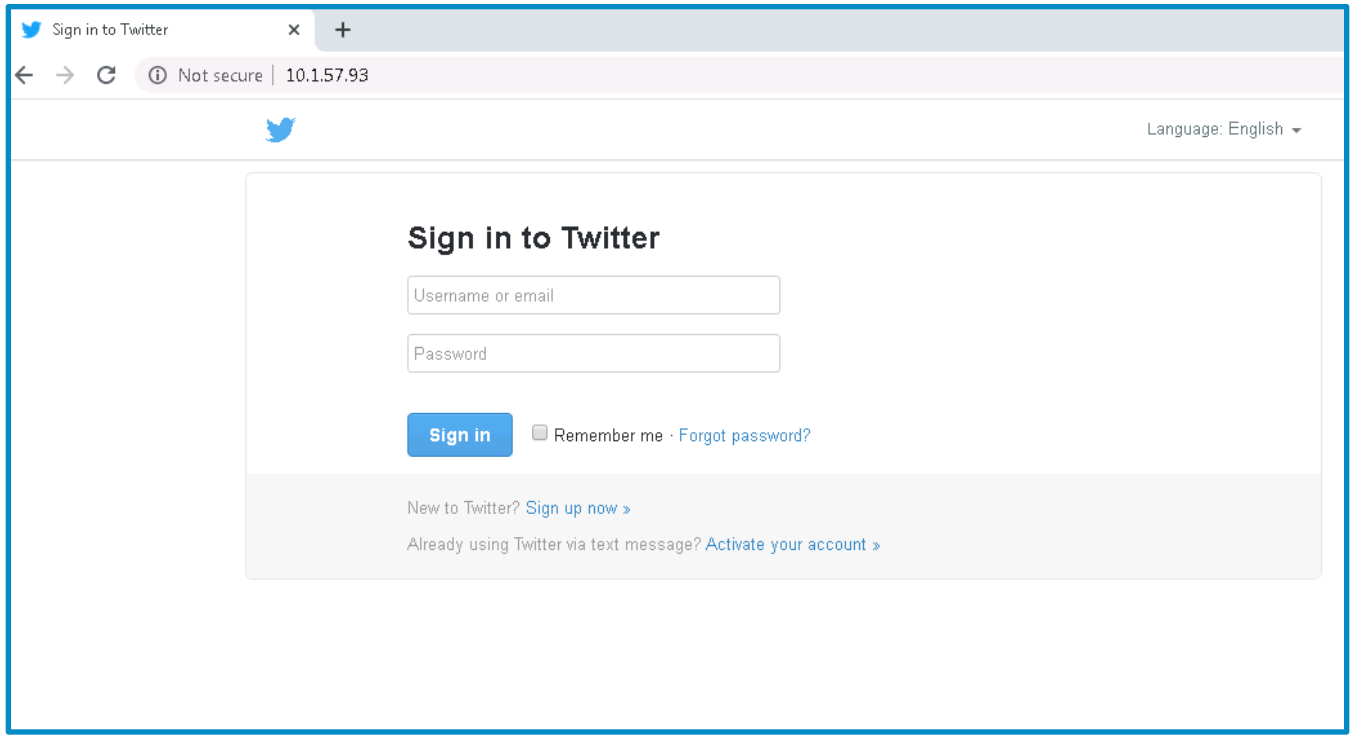
- Software Tools used (On the Kali Linux OS)
  - **`phishery`**
    - Linux application from the APT repository

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 5.6 – Given a scenario, implement security awareness practices.
    - Phishing

What is a Phishing Attack?

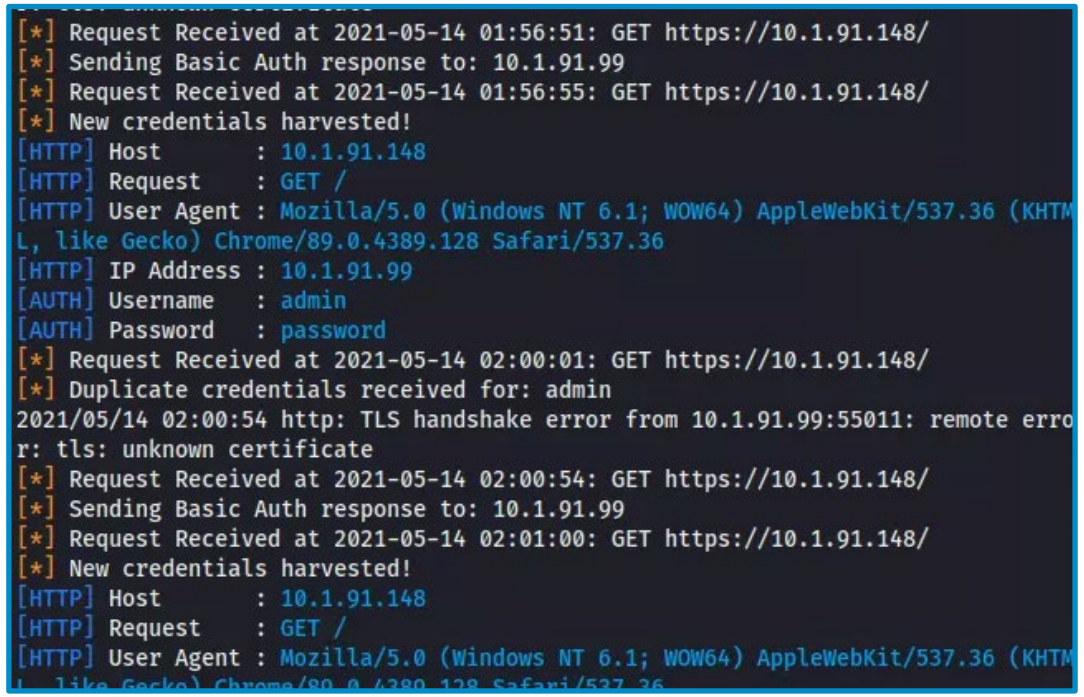
- Attempting to get information from someone in a malicious manner
- An example, a phishing attack can send someone to a fake website to try and have them use credentials for the real website



Here, this website is made to look like the log-in page for Twitter, but notice the URL

Phishing Lab Overview

1. Set up Environments
2. Find IP Address
3. Setup Phishing email
4. Start Server
5. Play the Victim
6. See the Attack



Set up Environments

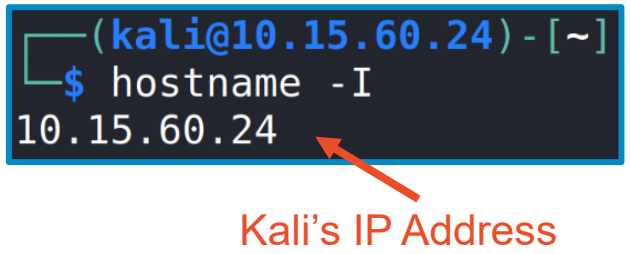
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

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

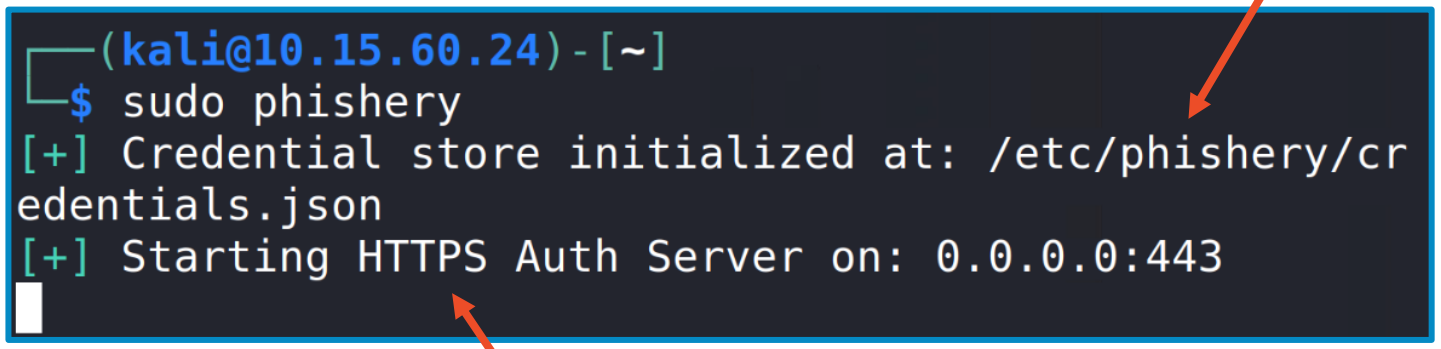


Launch Phishery

- Start the Phishery application
- Launch Phishery

  `sudo phishery`

Notice that Phishery starts a server on port 443



Phishery is using HTTPS

Please Note: Leave this Terminal open as we setup the email on the Apache2 server in a different Terminal

Set up the Phishing “Email”

Create a phishing Email*

- Open a new Terminal
- Navigate to the Desktop

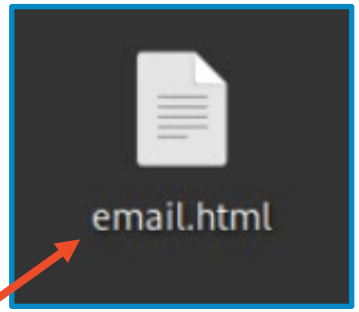
  `cd Desktop`

- Create an email file on the Desktop

  `touch email.html`

*Please Note: This will not be an actual email, but a website made to look like an email. In the real world, this would be email to the victims

```
┌──(kali@10.15.60.24)-[~]
└─$ cd Desktop

┌──(kali@10.15.60.24)-[~/Desktop]
└─$ touch email.html
```



Verify that the email.html page appears on the Desktop

Set up the Phishing “Email”

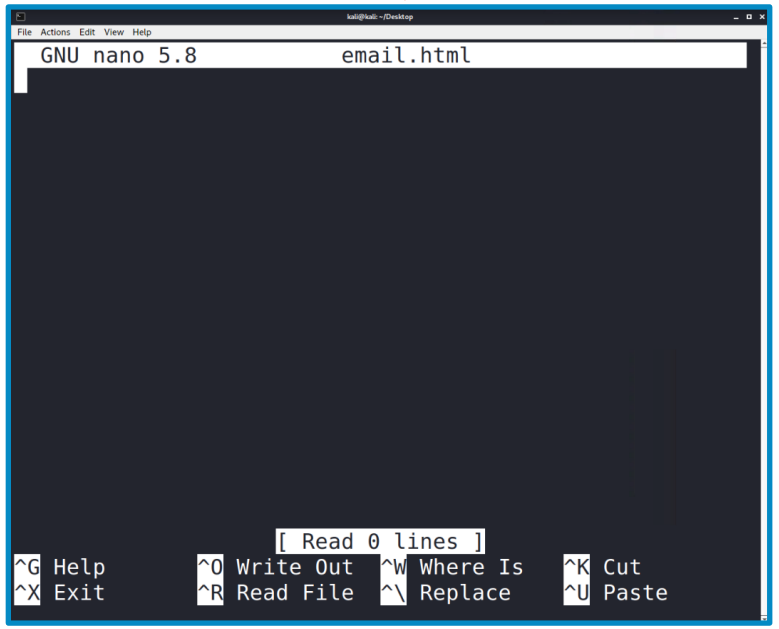
Edit the phishing Email*

- Open the file in the nano editor

```
nano email.html
```

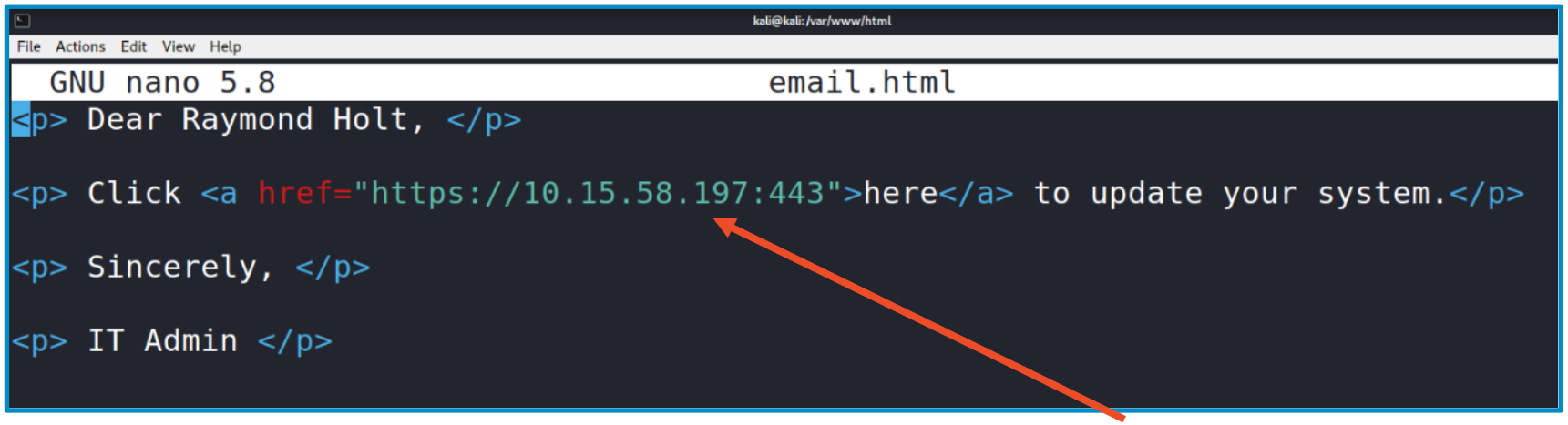
```
┌──(kali@10.15.60.24)-[~/Desktop]
└─$ nano email.html
```

This should open email.html in the nano editor



Set up the Phishing “Email”

Create the email in the Nano editor (similar to below)



This should be your specific Kali IP Address
NOTE: “:443” is the default port for SSL connections (HTTPS)

When finished, CTRL+X to exit and Y to save the changes

Start Apache2 Server

- Save the email.html and exit nano
- Move the email to the Apache server

  `sudo mv email.html /var/www/html`

- Start the Apache server

  `sudo service apache2 start`

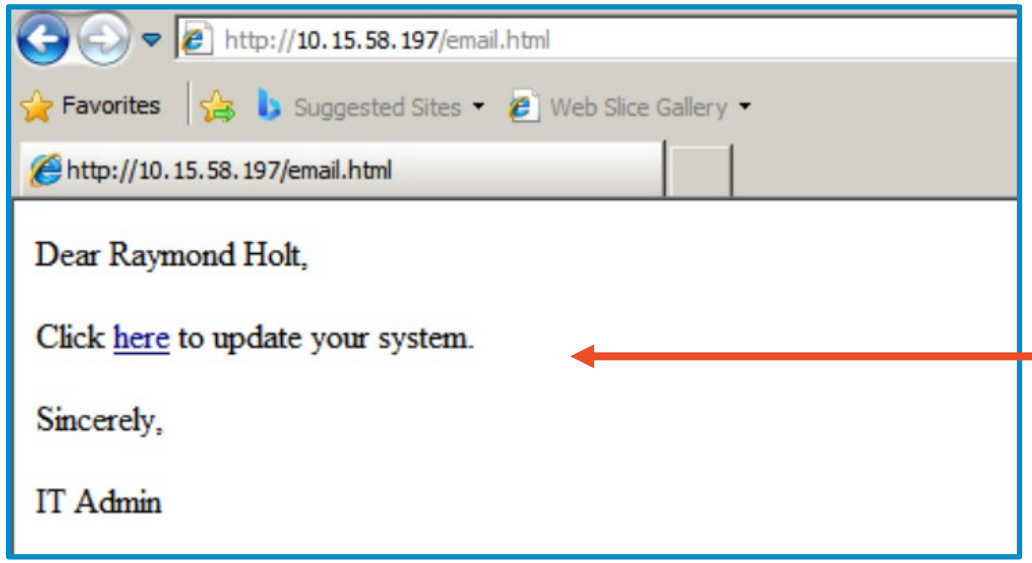
```
┌──(kali@10.15.60.24)-[~/Desktop]
└─$ sudo mv email.html /var/www/html

┌──(kali@10.15.60.24)-[~/Desktop]
└─$ sudo service apache2 start
```

Verify that the email.html file moved from the Desktop

Playing the Victim

- In the Windows environment, open Internet Explorer
- Go to the following website

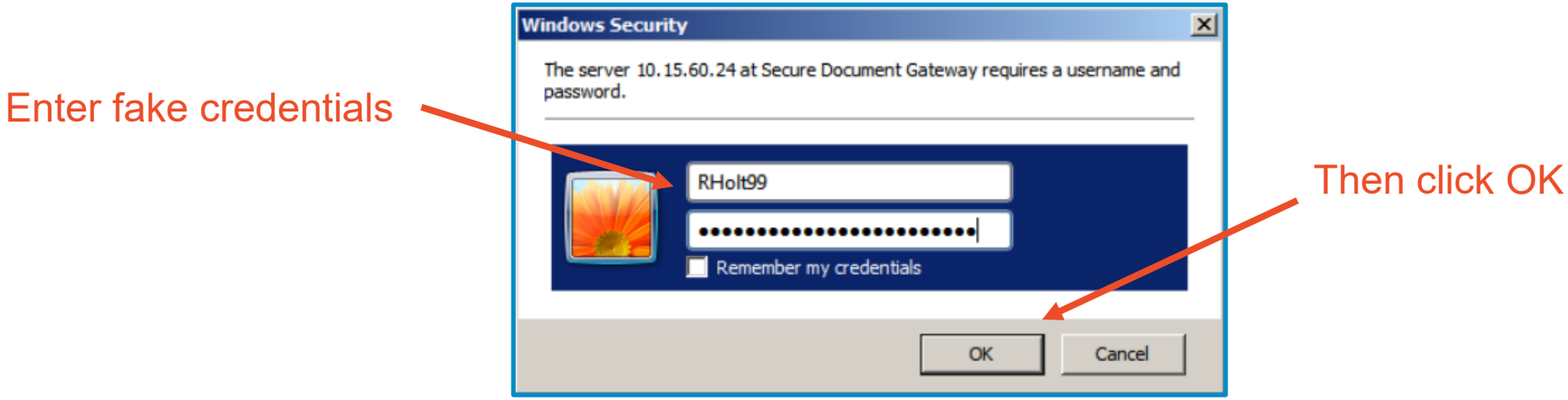
  `http://kali-IP-Address/email.html`



Verify that you see the email made in Nano

Playing the Victim

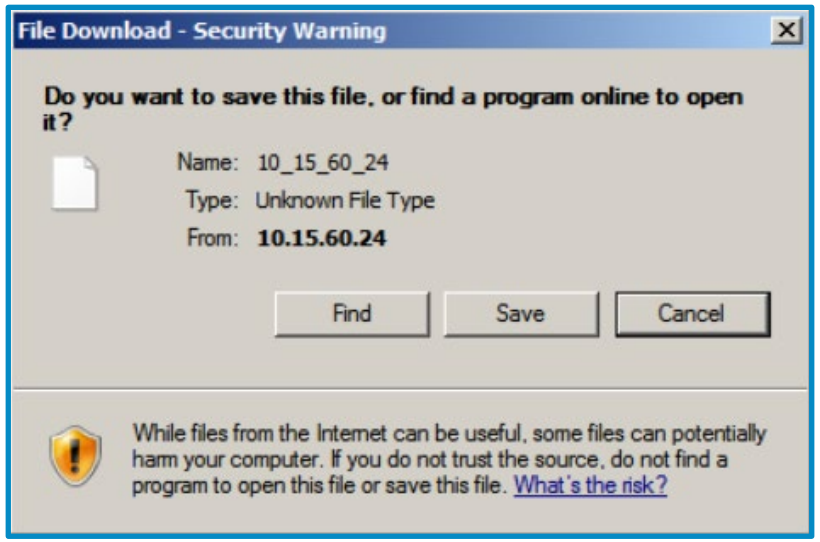
- Click on the **here** link
  - If there is a problem, click “Continue to this website”
- Notice that a Windows Security feature appears
- Enter false credentials and select **OK**



Playing the Victim

- Notice that a file tries to download

Either Save or Cancel the download



This is just to make the victim think this is the update file

Seeing the Attack

- Go back to the Kali Machine
- View the credentials

```
[*] Request Received at 2023-07-05 17:51:41: GET http
s://10.15.60.24/
[*] Sending Basic Auth response to: 10.15.6.114
[*] Request Received at 2023-07-05 17:53:19: GET http
s://10.15.60.24/
[*] New credentials harvested!
[HTTP] Host       : 10.15.60.24
[HTTP] Request    : GET /
[HTTP] User Agent : Mozilla/4.0 (compatible; MSIE 8.0
; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; M
edia Center PC 6.0; .NET4.0C; .NET4.0E)
[HTTP] IP Address : 10.15.6.114
[AUTH] Username   : RHolt99
[AUTH] Password   : ICaughtTheDiscoStrangler
```

Notice the Windows Victim's credentials

How to Defend Against a Phishing 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 are all the same...
- Two-Factor Authentication
  - Why would these help secure your password?
- What are some other ways of defending against a phishing attack?