Cybersecurity

Typosquatting Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Typosquatting

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

- Software tool used
  - **`wget`** (Linux Command Line Tool)
  - Leafpad (Linux application)

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.2 - Explain common threat vectors and attack surfaces.
    - Human vectors/ social engineering
      - Typo squatting

What is Typosquatting?

- Typosquatting is exploiting a user's misspelling
  - Could type www.facbook.com instead of www.facebook.com
  - What if a user goes to www.waether.com instead of www.weather.com
  - This is also known as cybersquatting
- A malicious user will buy one of these domain names in the hope that someone will visit this website accidentally

Typosquatting Lab Overview

1. Set up Environments
2. Find Kali's IP Address
3. Copy www.cyber.org
4. Access Website
5. Create Typosquatting Website
6. Create Malicious File
7. Edit the Typosquatting Website
8. Access Typosquatting Website

Set up Environments

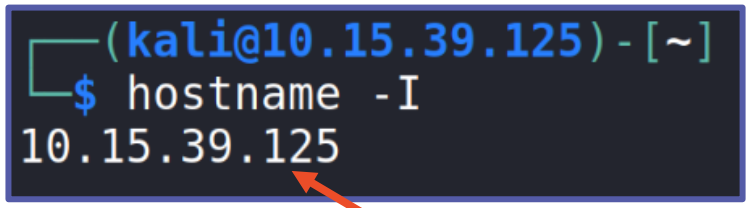
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

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



The IP Address

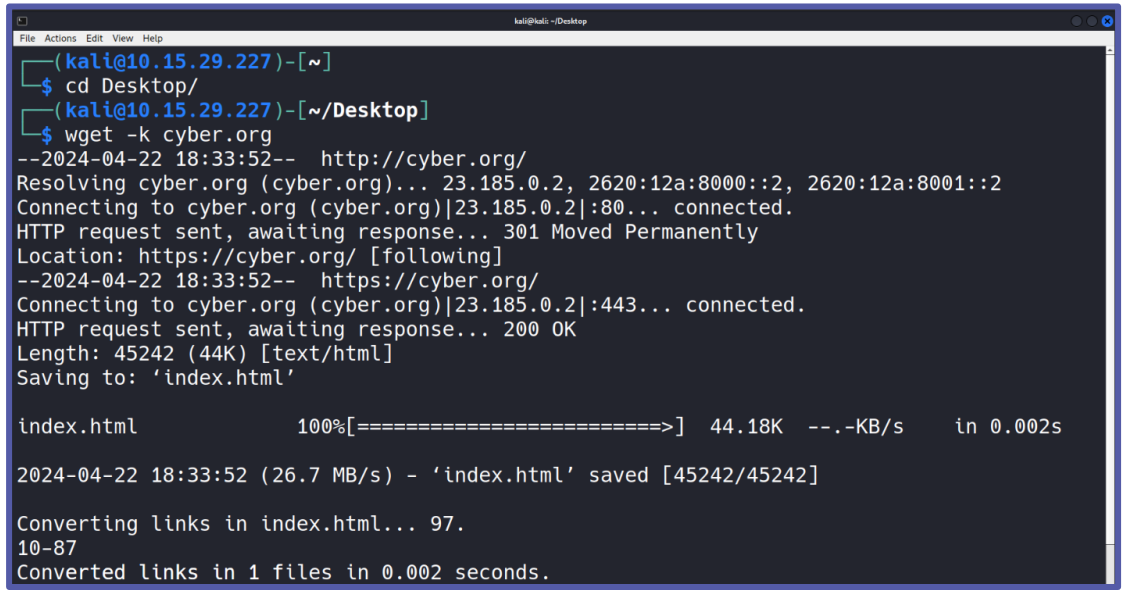
You need to screen print your result from
Running hostname –I
Save the file as
PX_lastname_IPAddress.
Be sure to drop it off into google classroom.

Copy www.cyber.org

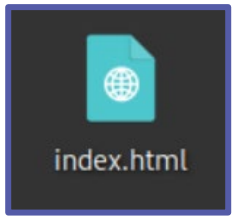
- Open a new Terminal in Kali
- Navigate to the Desktop

  `cd Desktop`
- Copy www.cyber.org's files/webpage

  `wget -k cyber.org`



You should see this folder appear on the Desktop that contains all of the files of www.cyber.org



CYBER.ORG

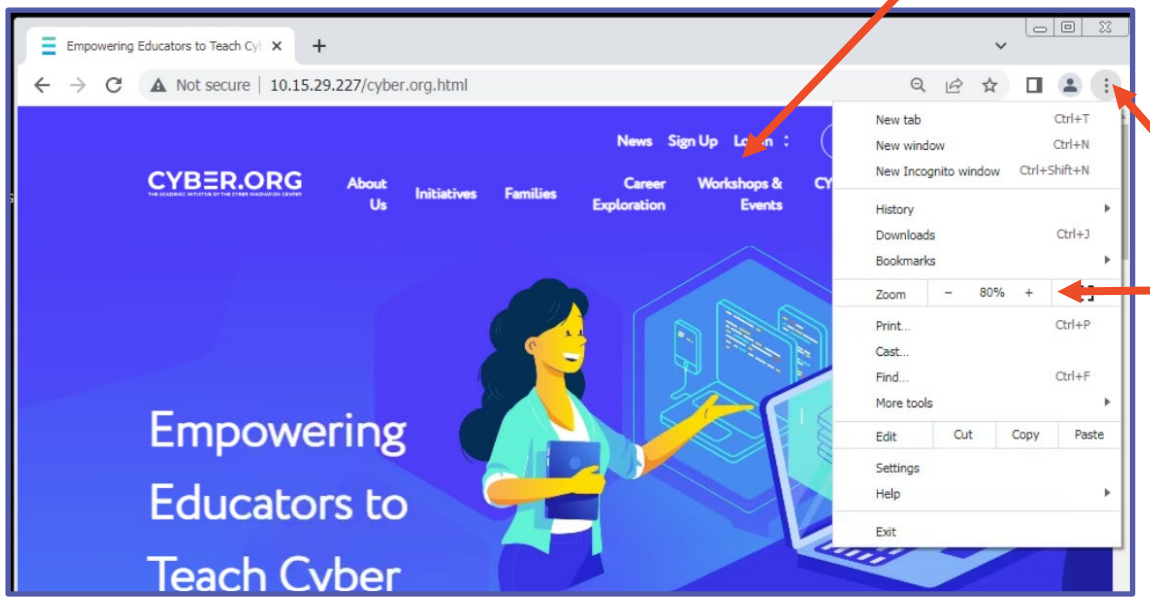
Access Website

- Rename the file
  - **`mv index.html "cyber.org".html`**
- Copy the cyber.org file to the Apache server
  - **`sudo cp cyber.org.html /var/www/html`**
- Start the Apache server
  - **`sudo service apache2 start`**

```
Converted links in 1 files in 0.002 seconds.
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ mv index.html "cyber.org".html
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ sudo cp cyber.org.html /var/www/html
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ sudo service apache2 start
┌──(kali@10.15.29.227)-[~/Desktop]
└─$
```

Access Website on Windows 7

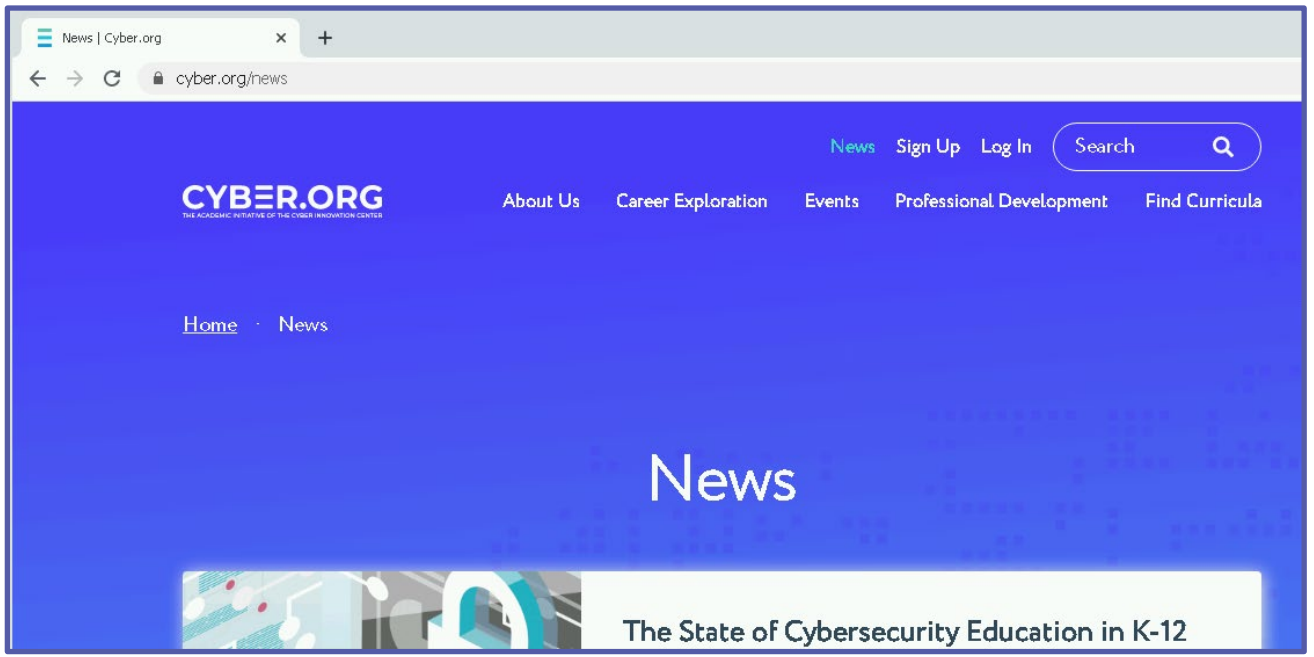
- Go to the Windows 7 Environment
- Open Google Chrome
- Click the settings button and zoom out to 80%
- Go to the following URL
  - <Your-Kali-IP-Address>/cyber.org.html



CYBER.ORG

Access News Website

- On the website, click on the “News” option at the top
- This should open cyber.org/news

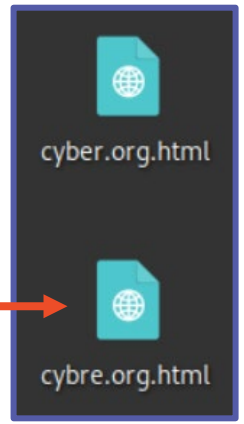


Create Typosquatting Website

- Now, create a malicious website
- Go back to the Kali machine, in the terminal copy the cyber.org.html file on the desktop to include the typo
  - **`cp cyber.org.html cybre.org.html`**

```
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ cp cyber.org.html cybre.org.html
```

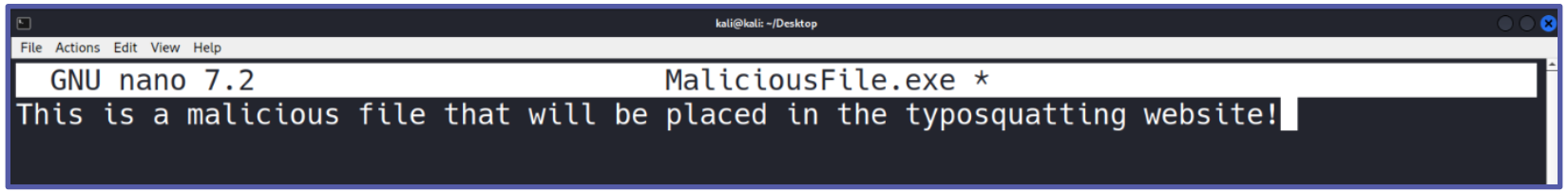
Here, the misspelling is going to be cybre.org instead of cyber.org



Create Malicious File

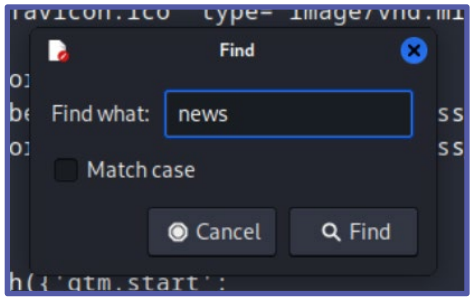
- Create a malicious file
  - **`touch MaliciousFile.exe`**
- Add some text to the MaliciousFile.exe
  - **`nano MaliciousFile.exe`**
  - Add some text
  - CTRL+X, y, ENTER to exit

```
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ touch MaliciousFile.exe
┌──(kali@10.15.29.227)-[~/Desktop]
└─$ nano MaliciousFile.exe
```



Edit the Typosquatting Website

- Open the cybre.org HTML file in Leafpad
  - **`leafpad cybre.org.html`**
- Find the code that controls the News link
  - Can search using CTRL+F for “news” to help find this line!



Find this line of code, this is the link for the News button

```
        <ul class="menu">
              <li class="menu-item">
    <a href="https://cyber.org/news">News</a>
        </li>
          <li class="menu-item">
    <a href="https://cyber.org/form/curricula-sign-up">Sign Up</a>
        </li>
          <li class="menu-item">
    <a href="https://cyber.instructure.com">Log In</a>
        </li>
    </ul>
```

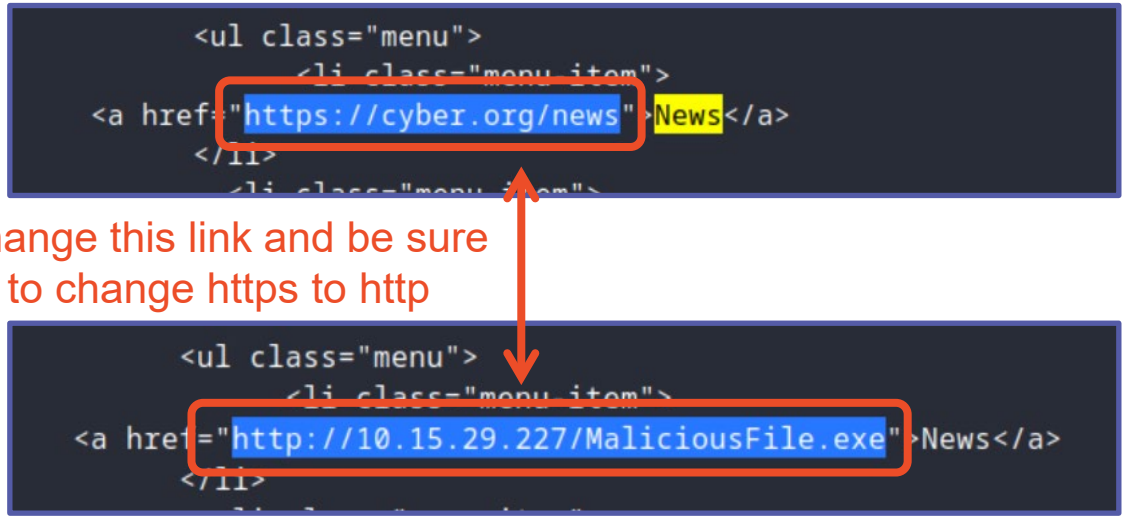
CYBER.ORG

Edit the Typosquatting Website News Link

- Change the “https://cyber.org/news” link to the following:

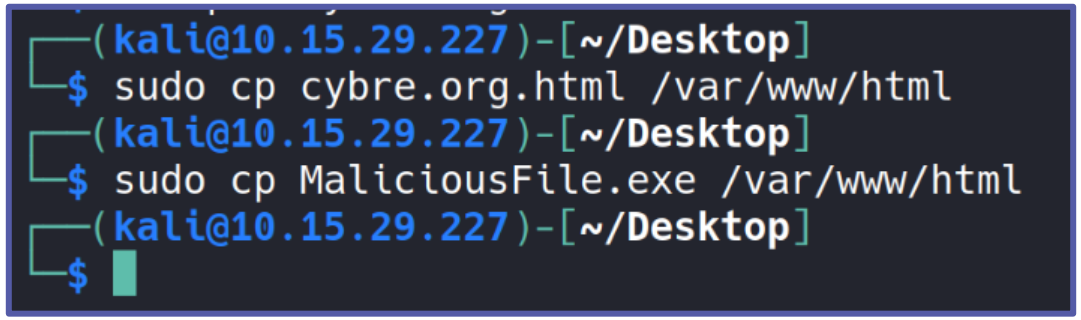
  `http://<Your-Kali-IP-Address>/MaliciousFile.exe`

- Click File, Save, and exit when you are finished



Move Typosquatting Website

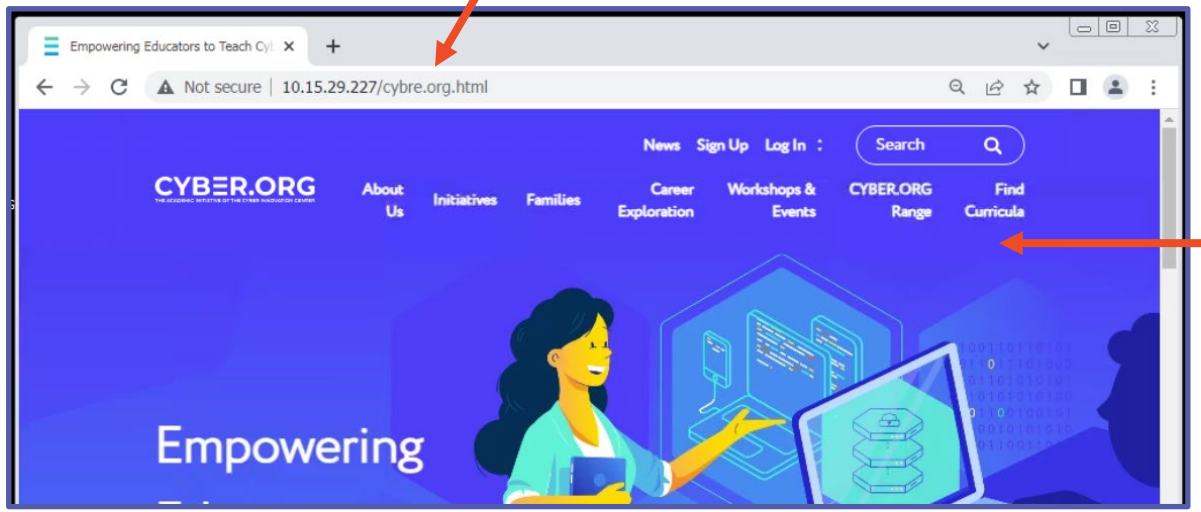
- Copy the files to the Apache server
  - **`sudo cp cybre.org.html /var/www/html`**
  - **`sudo cp MaliciousFile.exe /var/www/html`**



Access Typosquatting Website

- Go to the Windows 7 Environment
- Return to Google Chrome
- Go to the following URL
  - <Your-Kali-IP-Address>/cybre.org.html

Here, the user misspells cyber



You should see this website load, looks just like the original website

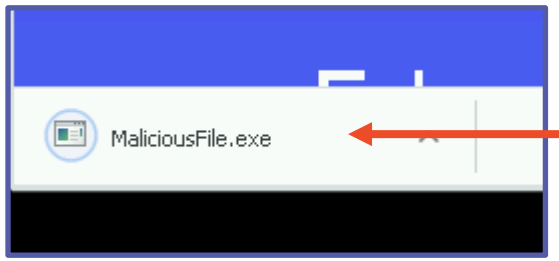
CYBER.ORG

Downloading the Malicious File

Page 18

- On the website, click on the “News” option
  - You may need to zoom out to 80% to see “News”
- You should see the MaliciousFile.exe download
- Obviously this MaliciousFile.exe is not harmful, but an unsuspecting user might trust this website because it looks exactly like the cyber.org website.
- In the real world, this file is probably going to be harmful to your system!

After you click on the news options, Screen print your screen to show you download the fake MaliciousFile.exe. File name should be PX_lastname_FakeMalicious.png



MaliciousFile.exe downloaded

CYBER.ORG

Defend Against Typosquatting

- Always check your domain names!
- Companies will actually purchase the domains of common typos to protect users
  - For example, go to www.gooogle.com
    - It will re-direct you to Google
  - Go to www.facbook.com
    - It will re-direct you to Facebook
  - Go to mikerowesoft.com
    - It will re-direct you to Microsoft's website