Lab 12 Requirements

- Internet connectivity & VMware Workstation version 14.0.0 or above
- A web browser with default settings

Part 01: Social Media Search

Search Google for your name and see what information comes up

- Are there any pictures of you that come up in the search results?
- Are there any social media accounts that come up in the search results?

Search popular sites such as Facebook, LinkedIn, YouTube, etc. to see what information about you is publicly available

- What personal information where you able to come up with?
- Could someone find out where you live?
- Could someone find out where you work?
- Could someone find out where you go to school?
- What other information is available?
  - Marital Status
  - Sex
  - Age
  - DOB
  - Etc.

Look through Google Alerts:

https://www.google.ca/alerts

Has an account associated with your email address been compromised?

https://haveibeenpwned.com/

Slide 01:
Place the answers to the above questions into slide 01

Part 02: Create a robots.txt file

On your Ubuntu Web Server VM, create the following directories in your /var/www/html directory

- FOLusername01
- FOLusername02
- FOLusername03

Inside the FOLusername01 directory, create a new HTML document with the following content:

```
<html>
<head>
<title>FOLusername01</title>
</head>
<body>
<h1>This is the FOLusername01 contact us page</h1>
</body>
</html>
```

Save it as contactus.html

Inside the FOLusername02 directory, create a new HTML document with the following content:

```
<html>
<head>
<title>FOLusername02</title>
</head>
<body>
<h1>This is the FOLusername02 site map page</h1>
</body>
</html>
```

Save it as sitemap.html

Inside the FOLusername03 directory, create a new HTML document with the following content:

```
<html>
<head>
<title>FOLusername03</title>
</head>
<body>
<h1>This is the FOLusername03 private page</h1>
</body>
</html>
```

Save it as private.html

Create a robots.txt file in the root of the web directory that will do the following:

- Allow the Google News Spider to index the contactus.html page
- Allow the Yahoo Spider to crawl the site map page
- Disallow Google, Yahoo, and MSN to crawl private.html, but not any others
- Disallow Facebook access to the contactus.html page
- Allow all user-agents access to the /mutillidae directory

Slide 02:
Take a screenshot showing the contents of your robots.txt file and place it into slide 02

Part 03: Display the routes of the Facebook bots

On the Ubuntu Web server, install whois and issue the following command *with the output being redirected* to a file named robotindex.txt

```
whois -h whois.radb.net -- '-i origin AS32934' | grep ^route
```

Use nano to display the contents of the file and take a screenshot of your results

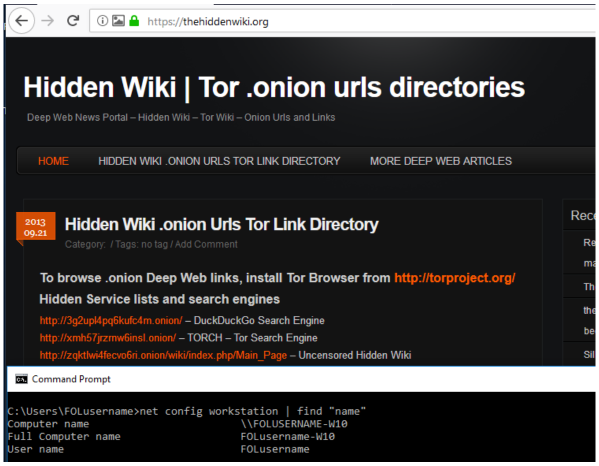
Slide 03:
Take a screenshot showing the robotindex.txt file and place it into slide 03

Part 04: Download and Install the TOR Browser

On your Windows 10 VM, navigate to www.torproject.org and download the appropriate file to install TOR

Once installed, start the TOR Browser and **Connect to TOR**

Navigate to https://thehiddenwiki.org



https://thehiddenwiki.org
HOME
HIDDEN WIKI .ONION URLS TOR LINK DIRECTORY
MORE DEEP WEB ARTICLES
2013
09.21
Category: / Tags: no tag / Add Comment
Rec
Command Prompt

Hidden Wiki | Tor .onion urls directories

Deep Web News Portal – Hidden Wiki – Tor Wiki – Onion Urls and Links

Hidden Wiki .onion Urls Tor Link Directory

To browse .onion Deep Web links, install Tor Browser from http://torproject.org/

Hidden Service lists and search engines

http://3g2upl4pq6kufc4m.onion/ – DuckDuckGo Search Engine
http://xmh57jrzrnw6insl.onion/ – TORCH – Tor Search Engine
http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page – Uncensored Hidden Wiki

```
C:\Users\FOLusername>net config workstation | find "name"
Computer name                        \\FOLUSERNAME-W10
Full Computer name                   FOLusername-W10
User name                            FOLusername
```

Slide 04:
Take a screenshot showing the hidden wiki page and the output of net config workstation filtered to “name” and place it into slide 04

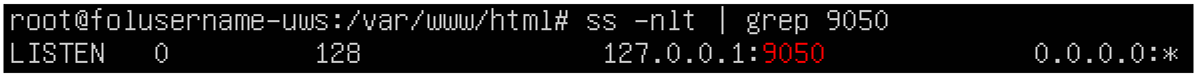
Part 05: Configure the Ubuntu Server to use Hidden Services

**** Take a snapshot of your Ubuntu Web Server VM before proceeding ****

On your Ubuntu Web Server, install the TOR service

```
apt install tor
```

Check that TOR is listening on the default port of 9050 on a localhost address



```
root@folusername-uws:/var/www/html# ss -nlt | grep 9050
LISTEN    0          128                    127.0.0.1:9050              0.0.0.0:*
```

We are going to configure this server to host a web service over the TOR network. Add the HTTP service to the /etc/tor/torrc file with the following lines:

```
HiddenServiceDir /var/lib/tor/hidden_service/http
```

```
HiddenServicePort 80 127.0.0.1:80
```

Restart the TOR service

Check your external IP address

```
wget -qO - https://api.ipify.org; echo
```

Try to obtain an external IP address over the TOR network (Might not work over the college network)

```
torsocks wget -qO - https://api.ipify.org; echo
```

In order to enable your commands in the current shell to use the TOR network, issue the following command:

```
source torsocks on
```

This will activate the TOR mode. In order to enable TOR's control port, start with establishing a password of your ***FOLusername***

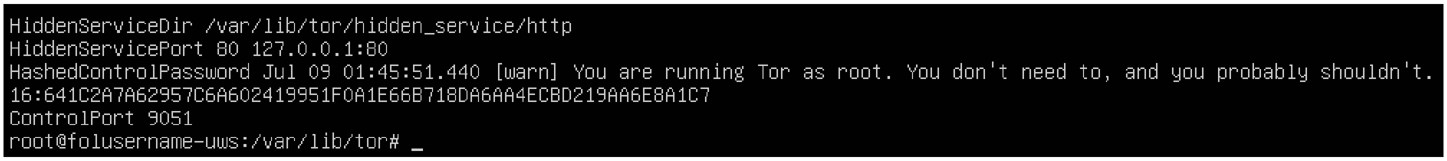
```
torpass=$(tor --hash-password "folusername")
```

Insert the hashed password

```
printf "HashedControlPassword $torpass\nControlPort 9051\n" | sudo tee -a
/etc/tor/torrc
```

Your /etc/tor/torrc file should have been updated with the entry

Unfortunately we are limited by the network firewalls in establishing a TOR connection. If you have control of the network, you can adjust the firewall rules.



```
HiddenServiceDir /var/lib/tor/hidden_service/http
HiddenServicePort 80 127.0.0.1:80
HashedControlPassword Jul 09 01:45:51.440 [warn] You are running Tor as root. You don't need to, and you probably shouldn't.
16:641C2A7A62957C6A602419951F0A1E66B718DA6AA4ECBD219AA6E8A1C7
ControlPort 9051
root@folusername-uws:/var/lib/tor# _
```

Slide 05:
Take a screenshot showing the contents of /etc/tor/torrc as shown above and place it into slide 05