

Lab 02 Requirements

- ✓ Internet connectivity & VMware Workstation version 15.5.7 or above
 - ✓ Downloaded VMs from resources link under content on FOL
-

Part 01: Information Gathering

As discussed in this week's lecture, when you do passive information gathering, you are not introducing any traffic onto the target network

cewl

- Open a terminal and navigate to the **/usr/share/doc/cewl** directory
- Do an **ls -ail** to see the contents of the directory
- Open the **README** file to see the syntax you need to use to run this program
 - **gzip -cd README.md.gz | more**
- The syntax in its most basic form is **cewl target_website_name**
- Try running this scan against **transpirenetworks.com**
 - This could take a while, but when it finishes, cewl will return a list of keywords that could be used to increase the effectiveness of a dictionary attack
 - By default the command will be run and results will be output to your screen
- Simply running **cewl** gives you interesting results, but isn't very useful long term
- If you want to save the results for later use, you can export them to a file with an option that can be found in the **README.md.gz** file
- Use the correct option to send the output of the **cewl** command to a file called **transpire.txt**, and run it against **transpirenetworks.com**

Slide 01:

- Take a screenshot showing the results of **cewl** by using the **cat** command to display the contents of **transpire.txt**

whois

- Run the whois command against **transpirenetworks.com** with the following command:

whois transpirenetworks.com

Slide 02:

- Take a screenshot showing the results of the result of the **whois** command and highlight the **Registrar WHOIS Server** and place it into Slide 02

theHarvester (might need to run it more than once to get results)

- This tool will search a domain for email addresses, usernames and other relevant information
- This information could be used for social engineering attacks or to build a dictionary list
- Use locate and grep to find the README file for theharvester
- To see general information about theharvester you can view the **README** file

For a simple scan of the fanshawec.ca domain, using bing and limiting the results to 100, you can use the following syntax. (Use **theharvester ?** to view the help file so you understand what the options do)

theharvester -d fanshawec.ca -l 100 -b bing

As with many other commands you would output these results to a file with the redirection operator

theharvester -d fanshawec.ca -l 100 -b bing > emails.txt

Feel free to use Google or Yahoo, etc. if the Bing options doesn't find any results

Slide 03:

- Place the results of your findings into slide 03

SpiderFoot

SpiderFoot can be found under Information Gathering → OSINT Analysis

Open-source intelligence (OSINT) refers to passively gathering intelligence and analysing data that is made available publicly

We will look at what SpiderFoot can do when scanning our LAN network. SpiderFoot can be accessed through a CLI or a web browser if you run it in Web UI mode. In order to access it through a web browser, first start SpiderFoot and use the -l option while providing an IP address and Port that the web server should listen on for web requests:

spiderfoot -l 127.0.0.1:6065

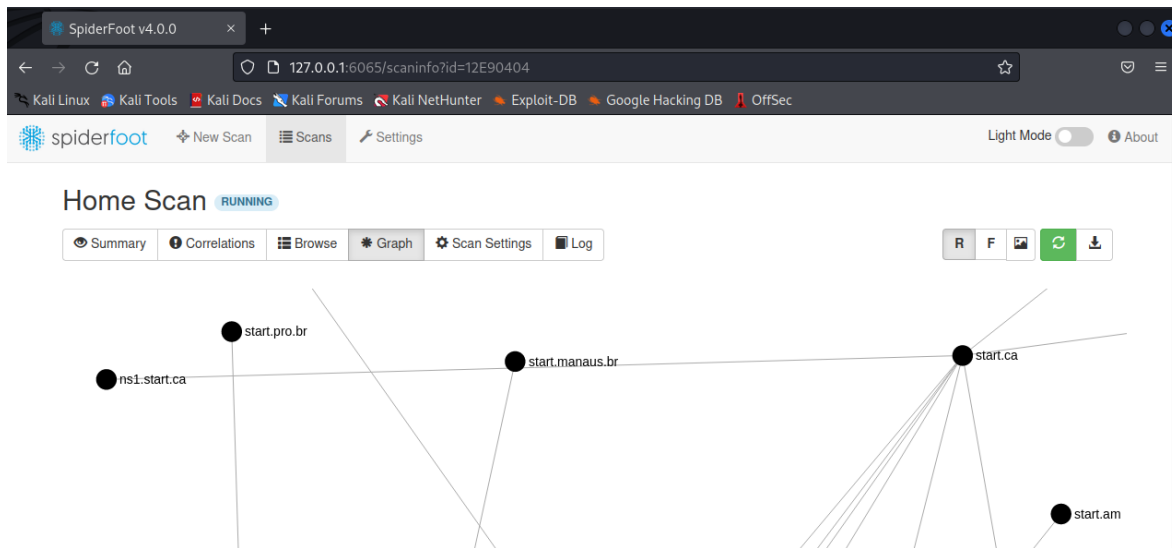
Once you execute the above command, the web server will start and listen on port 6065 for incoming connections. Use a web browser to access the Web UI running on 127.0.0.1:6065

Select a "New Scan"

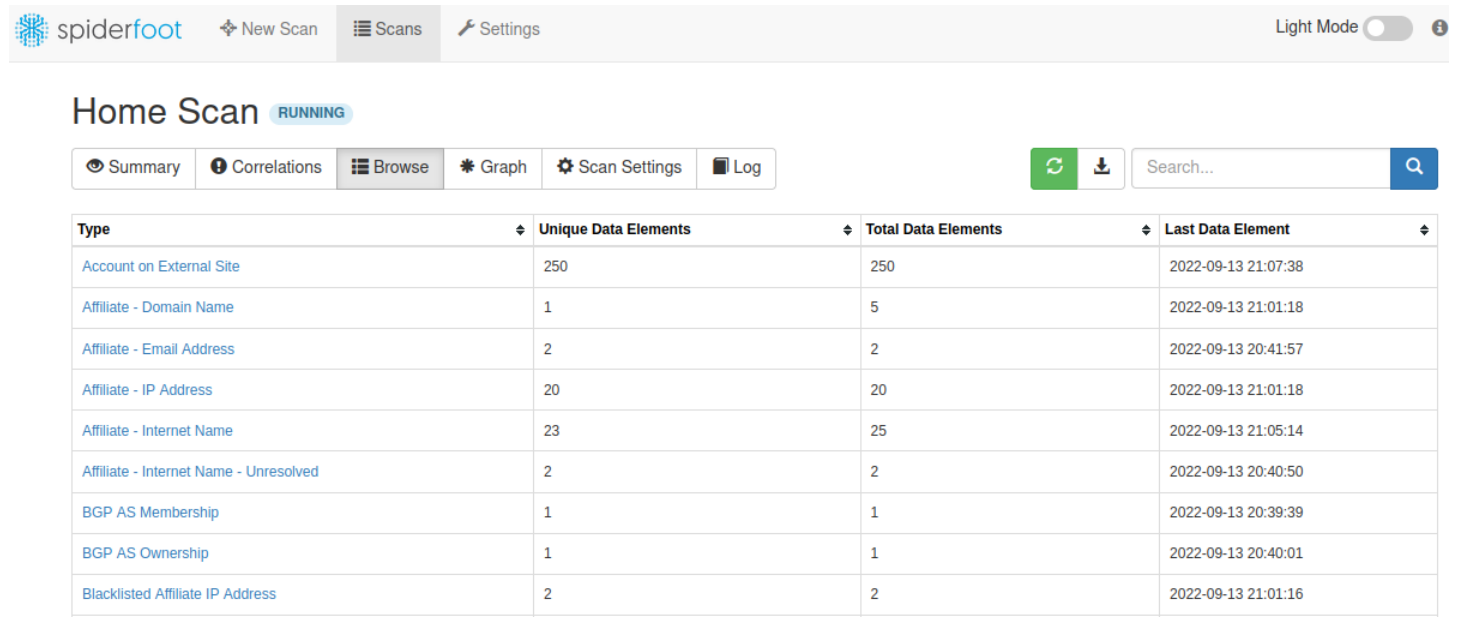
Name the scan **FOLusername-scan** with your FOLusername

For this exercise, you can select your home external IP address if you'd like or use something more generic like Google.ca

For my example, I scanned my external IP address at home and discovered information on my ISP



Once the scan has completed, click on the **Browse** tab, and show me your results as shown below:



The image shows the SpiderFoot v4.0.0 web interface with the 'Browse' tab selected. The 'Home Scan' is still 'RUNNING'. The 'Browse' tab displays a table of scan results. The table has four columns: 'Type', 'Unique Data Elements', 'Total Data Elements', and 'Last Data Element'. The results are as follows:

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	250	250	2022-09-13 21:07:38
Affiliate - Domain Name	1	5	2022-09-13 21:01:18
Affiliate - Email Address	2	2	2022-09-13 20:41:57
Affiliate - IP Address	20	20	2022-09-13 21:01:18
Affiliate - Internet Name	23	25	2022-09-13 21:05:14
Affiliate - Internet Name - Unresolved	2	2	2022-09-13 20:40:50
BGP AS Membership	1	1	2022-09-13 20:39:39
BGP AS Ownership	1	1	2022-09-13 20:40:01
Blacklisted Affiliate IP Address	2	2	2022-09-13 21:01:16

Slide 04:

- Select the Browse tab and place the results of a successful scan into slide 04
- Ensure that your **FOLusername** is shown as the name of the scan you created

Part 02: Scanning

Before proceeding, ensure you have all your VMs on a LAN segment in VMware called **INFO6065**

- ✓ You will need static IP assignments for LAN Segment network adapters

nmap (all your VMs need to be powered on at this point)

- If you enter the **nmap -h** command with no options you will be presented with all the options
- Find the following options and make note of what they do.
 - -sn
 - -T<0-5>
 - -O
 - -F
 - -A
 - -v
 - -vv
- We are going to run a simple scan with a timing level of 4, and fast mode

nmap -T4 -F your-LAN-network/24

- Make a note of the kind of information returned by the scan
 - Which host is showing the most open ports?

Slide 05:

- Take a screenshot of the output that is on the screen when the command finishes running
- Make sure you include the title bar

unicornscan

This is another powerful scanning tool. Use **unicornscan -h** or **man unicornscan** to investigate the features of this tool

- Build the command that will use unicornscan to:
 - Scan the in class address range (same one used with zenmap)
 - Scan only port 139
 - Set the packets sent per second to 200
 - Specify explicitly to display the results to the screen as they are generated
 - Don't use verbose, on some machines it hangs the program
 - Make the scan appear to be coming from a computer with an IP of other than yours
 - Must be a valid host on network, to work

Slide 06:

- Take a screenshot showing the results of your unicornscan, including a command prompt showing your hostname

***** Take a snapshot of all the VMs named After Lab 02 *****