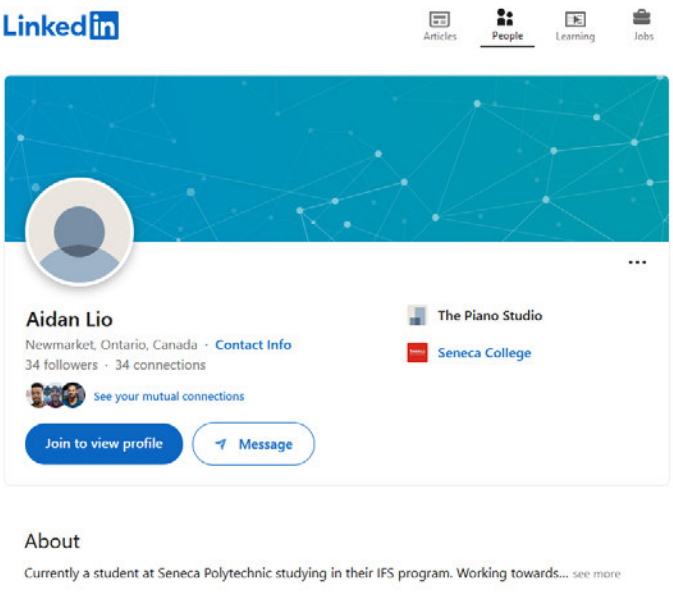
Lab Activities

Part 1A: Information Gathering

- What is the difference between passive and active information gathering?
    - Passive information gathering can be referred to as Open Source Intellgience (OSINT) or Information Gathering and is the act of gathering information using only publicly available resources. In the paper published by Mike Czumak, examples of this includes identifying IP addresses and sub-domains, people, technology, content of interests, and vulnerabilities
- Provide examples of each
    - Passive Information Gathering – Learning information about a target based on information from public LinkedIn profiles. For me, this would include town of residence (Newmarket, ON), the most recent previous work experience (The Piano Studio), how many connections I have, as well as that I attend or have attended Seneca Polytechnic. This is also seen from the screenshot below



    - Active Information Gathering – Utilizes tools to garner information that is not publically available, thus a tool like nmap and running a scan is an example of active information gathering.
- Assuming we are not engaged in criminal activity, what are the ethical and legal considerations we must be aware of when gathering information about a target?
    - Legal considerations can encompass the ownership of said information, especially if the information would be compromised, utilizing information gathering, means that we have information about someone that is not legally ours's, can be confidential which means that proper channels must be utilized to protect this information, or there can be legal ramifications for the use of said information. Moreover, from an ethical standpoint, is it okay to have this information on the target? This question is very nuanced and in terms of passive information gathering, I believe an argument can be made that it is more justifiable as we did not utilize channels other than publicly available information to create a profile. However, regarding active gathering, this can be harder to determine.

Often when cybersecurity professionals engage in active information gathering, we have received permissions to use these tools and gather the information. However, the ethical dilemma of, should I have this data, still exists.

Part 1B: IP Address & Domain ID

Table 2-3. All bolded text was already in table.

IP Address	FQDN	Point of Contact	Location
129.119.70.169	www.smu.edu	Information Security Office abuse@smu.edu 214-768-9999 Network Operations Center noc@smu.edu 214-768-4357	6185 Airline, 4th Floor, Dallas, TX, United States
162.12.1.112	www.td.com	Anthony Paleologus anthony.paleologus@td.com 856-470-3236 Irwin Chan irwin.chan@td.com 647-964-3402	27777 Inkster Road, Farmington Hills, MI, United States
104.247.81.52	**www.dj.com.ve**	Network Operations Centre 1-800-461-0585 noc@nextdimensioninc.com Oussman Jebbe ojebbe@nextdimensioninc.com 519-945-2032 Jeevan Reddy Kodur jkodur@nextdimensioninc.com 416-688-2568	1163 Goyeau Street, Windsor, ON, N9A 1H9, Canada
70.86.89.34	www.ibm.com	Chris chrisp@us.ibm.com Curtis curtis1977@us.ibm.com 214-42-0600 (Office)	4849 Alpha Road, Dallas, TX, United States
	www.hackthestack.com		
211.64.175.201	www.cernet.edu.cn	Jianping Wu jianping@cernet.edu.cn 86-10-6278-5933 Ling Zhang ling@scut.edu.cn 86-20-8711-0596 Xing Li	Network Research Center (Main Building) Tshinghua University Beijing China

		xing@certnet.edu.cn 86-10-6278-6983	

Most information was obtained from utilizing whois, especially in the instances of Point of Contact and Location. For www.dj.com.ve and www.hackthestack.com I utilized ping to get the IP address which worked for www.dj.come.ve but not hackthestack. Nslookup and dig also did not yield results.

To defend against this type of information gathering, we can utilize a few measures. The information provided by whois can be detrimental to untrained personnel in regard to social engineering attempts. For instance, from my research I know the first name and last name of support for www.td.com. This can be leveraged for attacks where I target the email of the support with bots to file their inbox, cause DoS or other social engineering techniques.

One of the means that we can protect ourselves is by using proxy names, emails, and phone numbers when providing information for ARIN or IANA to minimize the chance of social engineering. Moreover, all communications to the given contact information can be filtered to ensure whatever is necessary is sent to the proper channels. Moreover, knowing that certain IP addresses are available through this type of information gathering should guide security plans to ensure these resources are protected appropriately. Perhaps firewall rules to deny dig/nslookup/traceroute requests to limit the amount of information that is passively or actively available.

Part 1C: DNS

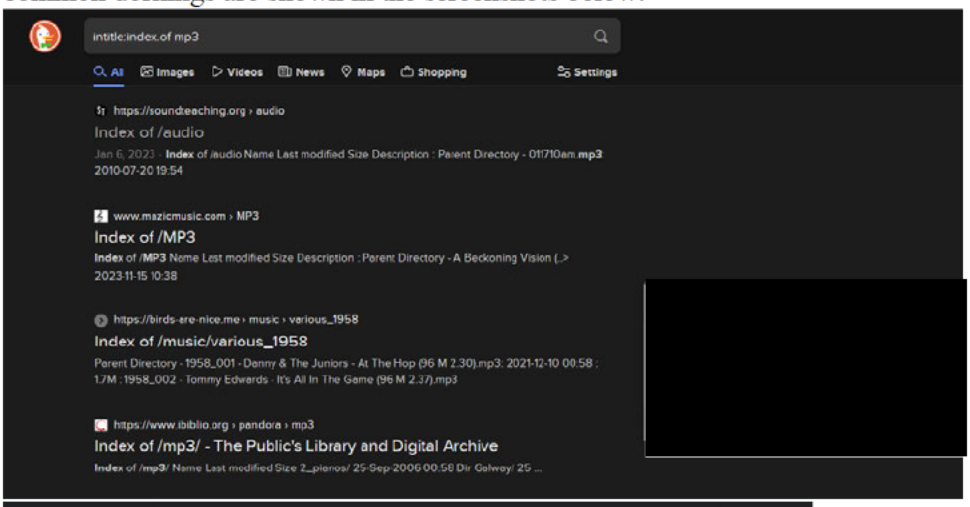
Chosen Company: Reddit

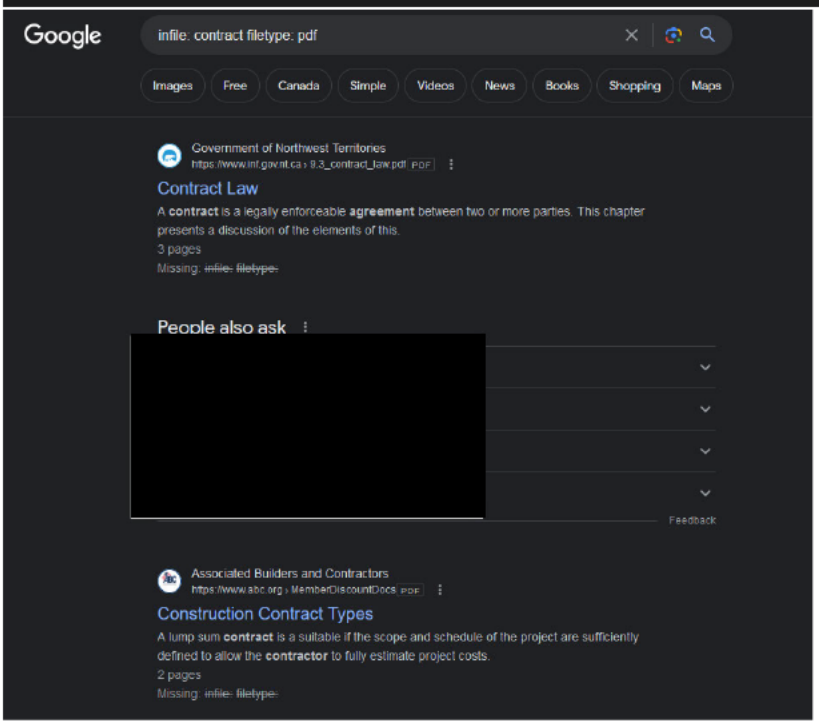
Item	Description and Findings
Domain Name	www.reddit.com
Address and Phone # of Corporate Headquarters	303 Second St. San Francisco, CA, 94107, US
Location of Internet Presence	151.101.1.140 151.101.193.140 151.101.65.140 151.101.129.140
Co-location or branches	Canadian Branch – 1 University Avenue, Toronto, M5J 2P1
Types of technology used	Python
Name of CEO	Steve Huffman (Also Co-Founder)
Home address of CEO	Not Available
Background of CEO	Degree in Computer Science, born in 1983 or 1984 (it is unconfirmed), once divorced
CEO Alma Mater	University of Virginia
Job Listing	https://www.redditinc.com/careers
Other Information	Goes by online name of u/spez on Reddit

Part 1D: Google Hacking

As will be discussed when looking at the included chart, the first portion of the page introduces concept relating to dorking and the basic formula (inurl:”domain”/”dorks”), the common search operators

(these being intitle, allintitle, inurl, allinurl, filetype, ext, intext, allintext, site). A few examples of common dorkings are shown in the screenshots below.

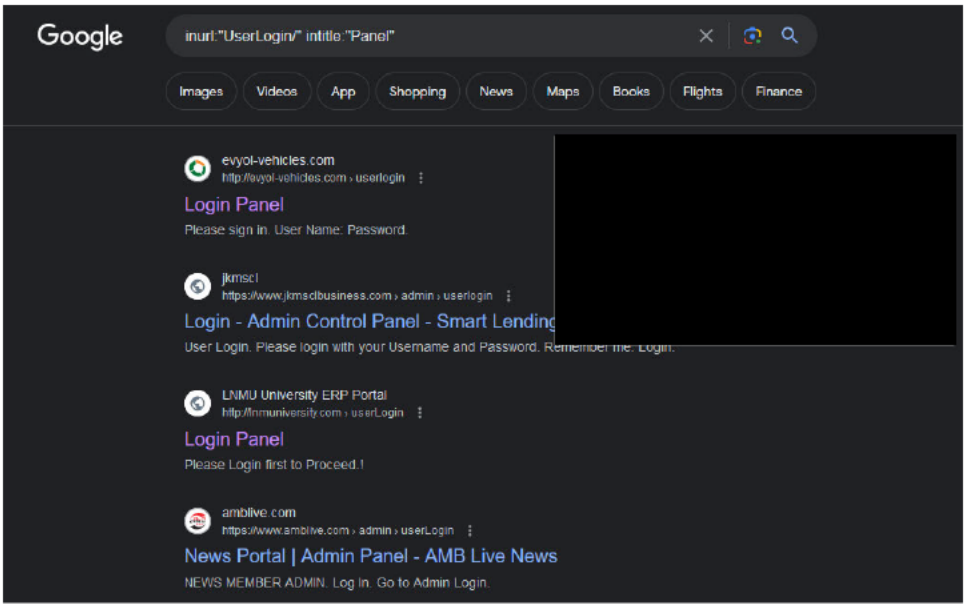




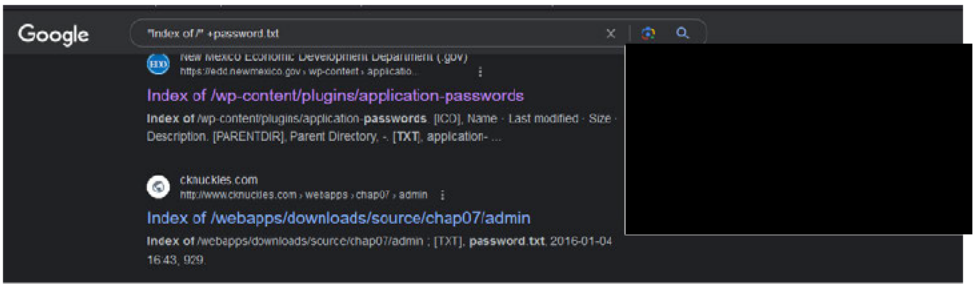
Resources for Dorking

- Google Hacking Database: https://www.exploit-db.com/google-hacking-database/
- Google Dorking: http://www.google-dorking.com/
- What Is Google Dorking?: https://www.simplilearn.com/tutorials/cyber-security-tutorial/google-dorking

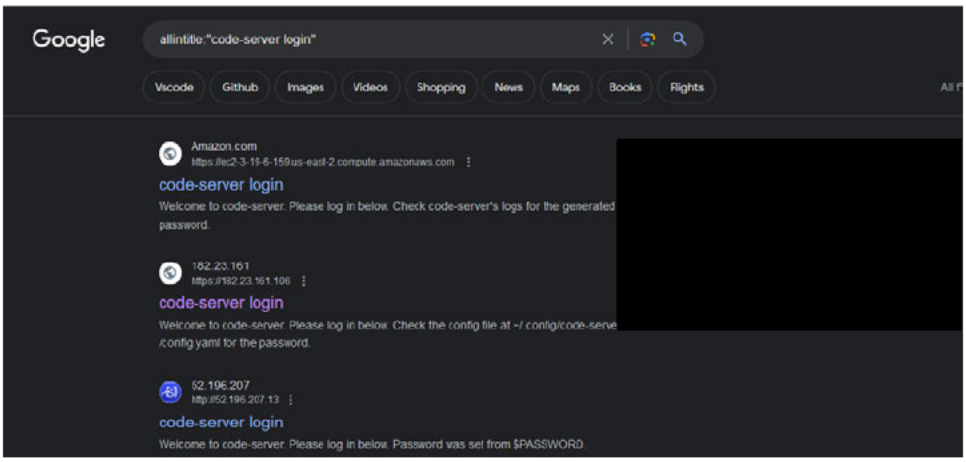
Utilizing the links referenced above, a few more complex examples are shown.



This first example looks for UserLogin in the url and Panel in the title



In this second example, using the “index of/” +password.txt finds pages that contain index of as well as something like password.txt which is very effective as the clicked-on link, had extension information available publicly.

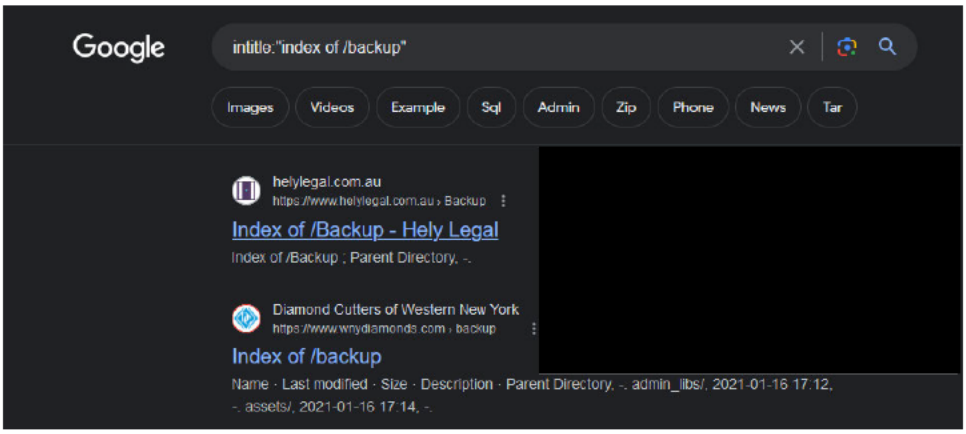


In this last example, using the search of allintitle: “code-server login” we have the login pages of various front-facing servers that direct us to passwords. The clicked link was of interest as it shows the directory that stores the password which could be utilized in a directory escape.

Understand the following examples:

Directive	Example	Description
intext	intext:password filetype:xlsx	Displays hits within page text
intitle	intitle:"index of /backup"	Displays hits within the page title
inurl	inurl:dyn_sensors.htm	Displays hits within the page URL
filetype	filetype:log intext:password	Return results with a specific file type (e.g., passwords within log files)
site	site:edu filetype:key intext:private	Show resultswithin a particular domain (e.g., RSA private keys within the EDU top-level domain)

These examples make some of the cornerstone terms/searches for dorking. As explained in the description column, they all provide fundamental tools that we can utilize to access publicaly available, albeit accidentally public, information. Utilizing an example provides invaluable resources to a hacker / someone trying to gather information.



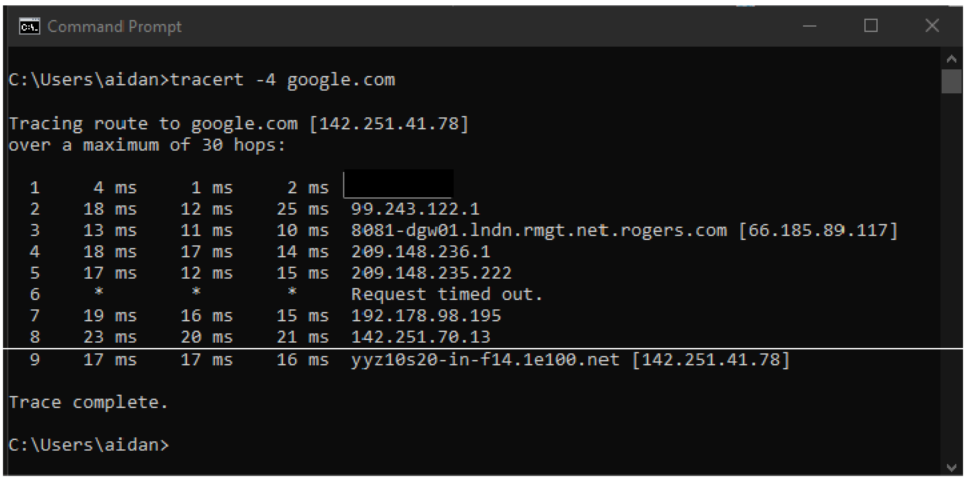
Part 1E: Banner Grabbing

Banner grabbing can be utilized as information gathering to gather information regarding web servers. The text utilized both telnet and netcat to gather information however, nmap can also be used with the –script banner option.

The information that can be gathered this way depends on the type of server and security setup on the targetted server.

Part 1F: TraceRoute

Traceroute or tracert is a powerful tool that is often utilized in conjunction with tools like ping to test network connectivity between the host and the chosen IP or FQDN. Within the context of information acquisition, people can use traceroute to learn information about the targeted website. Data like IPv4 or IPv6 can be utilized to pinpoint location of servers using visualization tools as well as possible points of interest



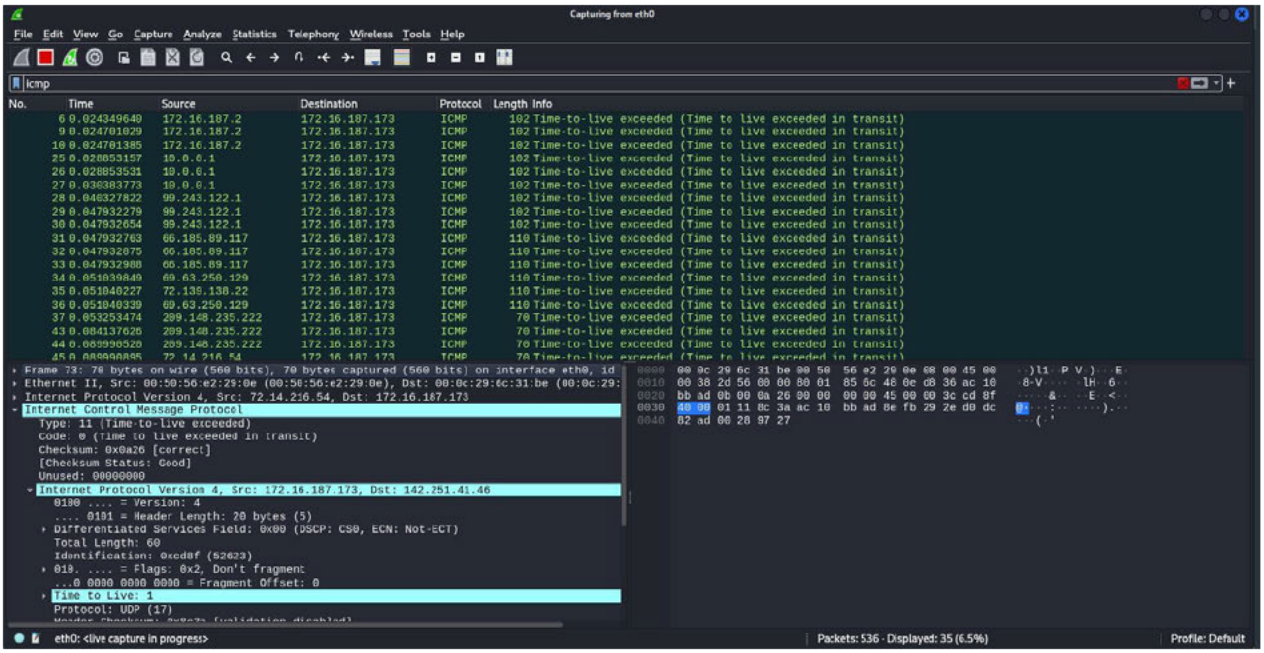
[redacted]

```
C:\Users\aidan>tracert learn.senecapolytechnic.ca

Tracing route to learn-prod-5c082fb7a0cdb-11455896.us-east-1.elb.amazonaws.com [54.211
.190.21]
over a maximum of 30 hops:

  1     4 ms     3 ms     2 ms
  2    12 ms    19 ms    14 ms
  3    15 ms    14 ms    11 ms
  4    43 ms    12 ms    22 ms
230.169]
  5    14 ms    14 ms    17 ms  209.148.235.222
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
```

In this second example, I used tracert on learn.senecapolytechnic.ca, as with the previous screenshot, information can be gathered about my network. We can also see that Seneca utilizes Amazon's AWS service to host BlackBoard. An interesting instance occurred where the tracert packets were delayed leaving 209.148.235.222 on both tracert examples. This can be a point of interest but also suggests that 209.148.235.222 is a busy server and prioritizes tracert lower than other traffic. Moreover, the device at 52.93.3.63 may be configured to drop traceroute packets as both attempts of tracert stalled and failed at this point.

Wireshark and Tracert

When analyzing the traffic of traceroute on Wireshark, some things of note arise, ICMP is the protocol utilized by tracert, therefore we can ensure we are capturing the traceroute by filtering by icmp. Below is a screenshot of the Wireshark output.

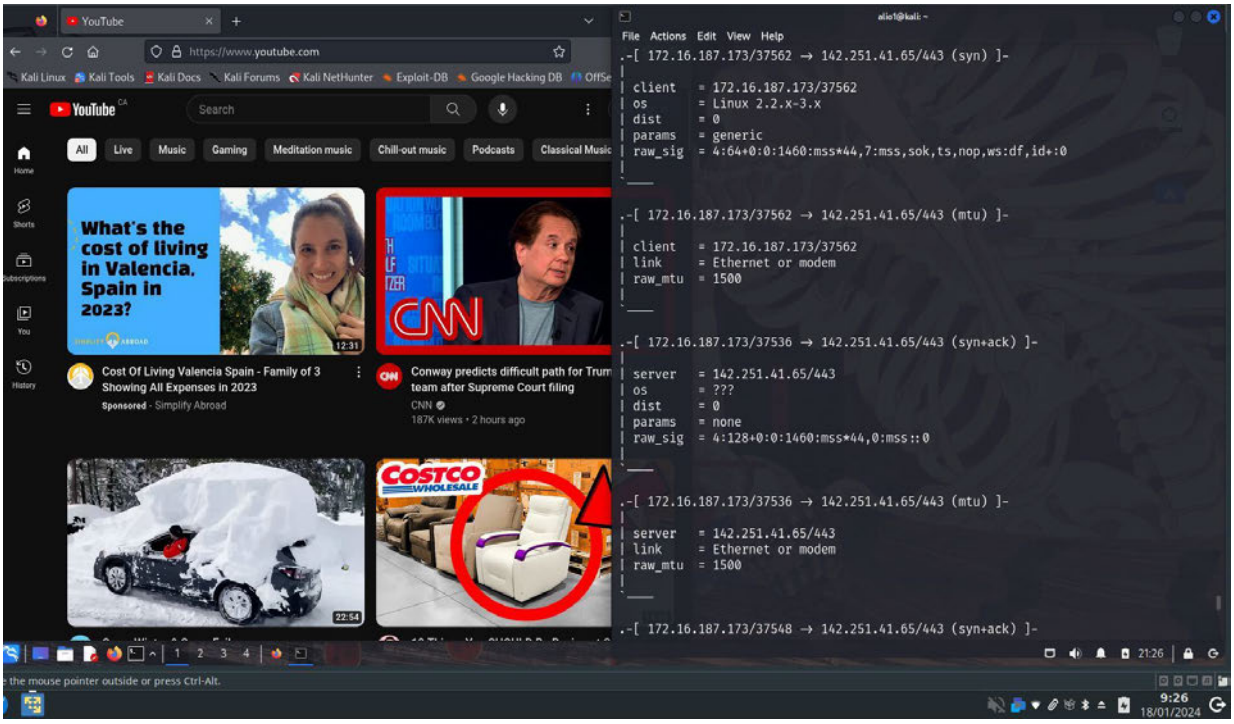


Analyzing the packets, a few things of note arise, we can see the route the data is taking from the source IP addresses that are contacting the host IP (172.16.187.173). We can also see that UDP is also being utilized.

Part 1G: Useful tools which can be found on Kali Linux

p0f

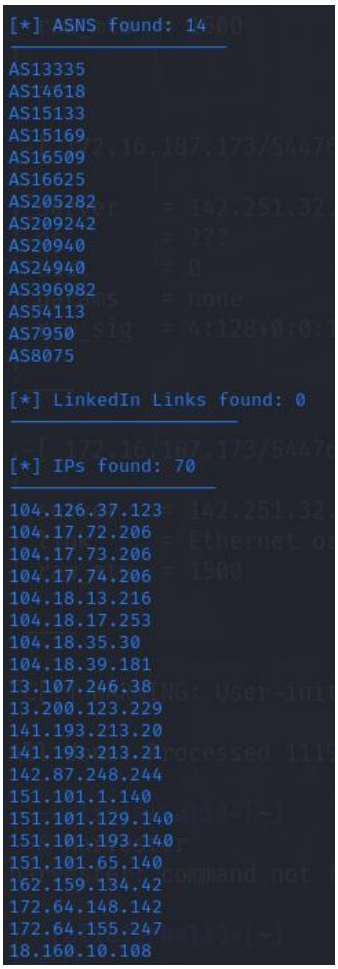
As a tool p0f provides the user with decoded network traffic information. For the subsequent screenshot p0f was run using the command *sudo p0f –i eth0* which told p0f to listen on interface eth0. p0f provides the user with information about the device that sends the packet, we can see any packet that leaves the Kali VM shows Linux 2.2.x-3.x, flags are also shown (syn+ack, mtu) as well host change. In other scans, information like uptime would be available or information like http_request from a specific browser.



theHarvester

Harvester is a powerful tool that gathers OSINT and publicly available information. It uses various search engines (duckduckgo, bing, google), and APIs to gather information about email addresses, domain names, and more. TheHarvester features the ability to use the –b command to specify search platforms or –all to use all, which requires certain API keys for tools like Shodan. To showcase the ability a prompt was run using *theHarvester –d Reddit.com -b all* as well as a second scan using *theHarvester –d cernet.edu.cn -b duckduckgo* to showcase the differences in all and a specific search like google, in addition to comparing the information pulled with the information I gathered using other tools in previous sections of this lab.

-d Reddit.com -b all



This scan often ran into the error of “Got more than 13000 bytes when reading Header value” which occurred frequently. However, a few tools like sitedossier’s parent domain yielded 400 domains associated with reddit.com, many of which link to specific subreddits. 14 ASNS were found as well as 70 associated IP addresses and took roughly 10 minutes

-d www.cernet.edu.cn -b duckduckgo

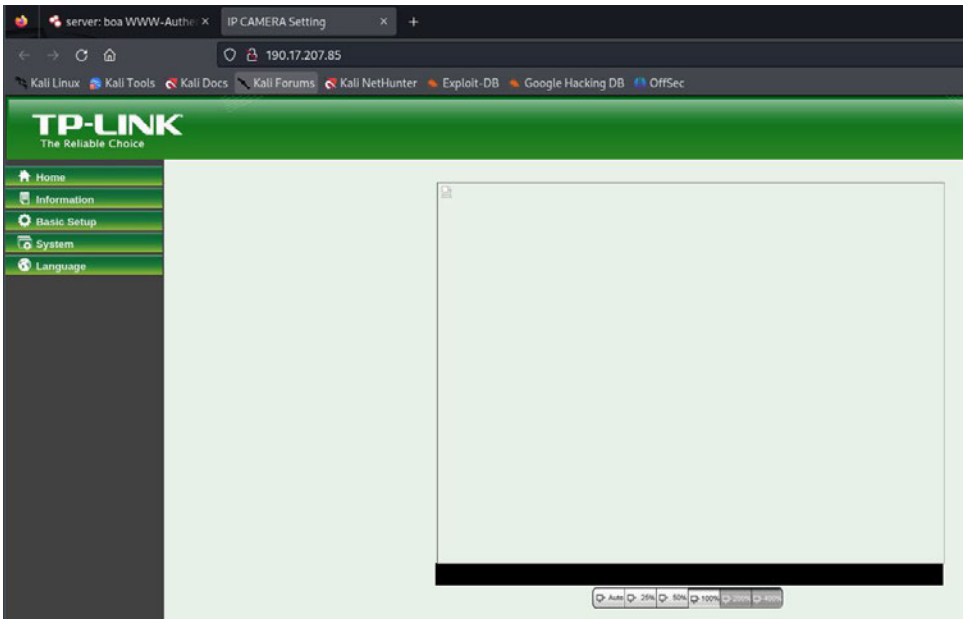
-d www.cernet.edu.cn -b urlscan

Shodan:

As a tool Shodan acts as an index for most devices connected to the internet (like routers, webcams) and catalogs them. Shodan can be utilized via the command line or with a GUI website that both act similarly. This can be goldmine for hackers that use a tool like Shodan to find specific devices, for instance a webcam that has a known exploit and try to leverage that to attack a device or network.

Moreover, due to the nature of Shodan we can also find devices that do not have any security measures in place, meaning that these devices can be compromised and utilized as zombies for C2s and DoS/DDoS attacks. In the video provided, the host found an open satellite link which was password protected, but utilized the setup guide to find the default login and use that to gain access.

In the subsequent screenshot, I clicked on a webcam from the GUI shodan and was able to access the settings using admin:admin


server: boa WWW-Authe
IP CAMERA Setting
190.17.207.85
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
TP-LINK
The Reliable Choice
Home
Information
Basic Setup
System
Language