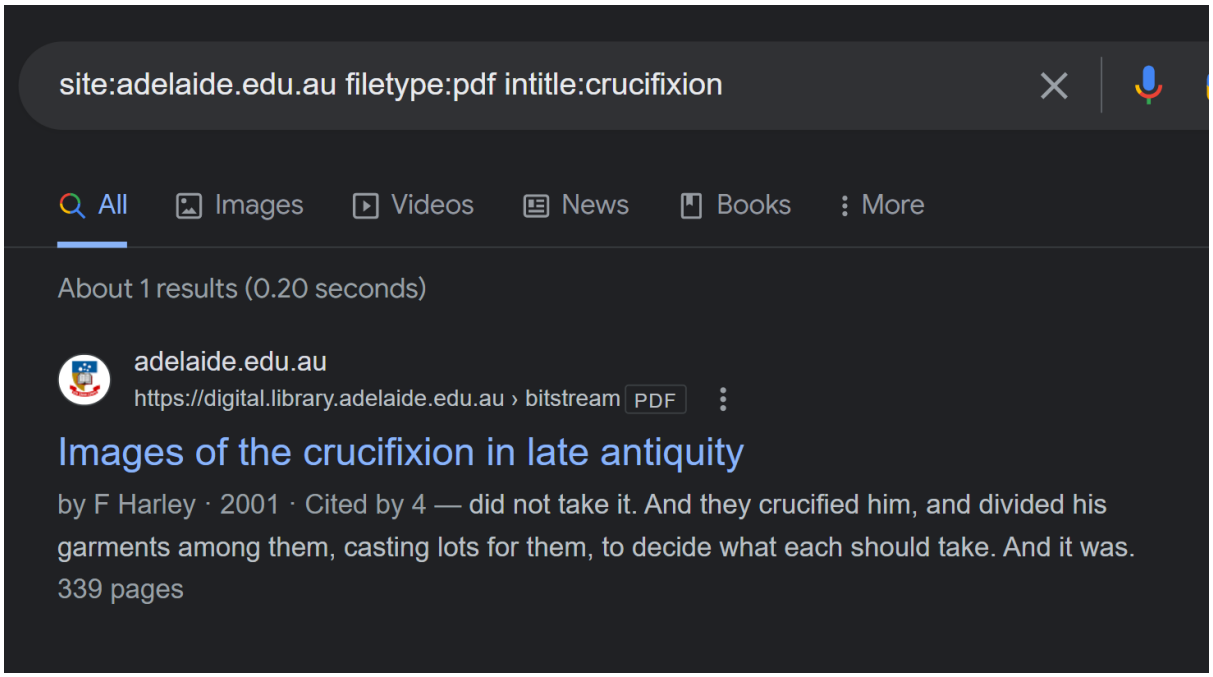
Part I - OSINT, Recon & Network Scanning

Question 1:

a) The Google search syntax is site:adelaide.edu.au filetype:pdf intitle:crucifixion.
b) The pdf author is F Harley.

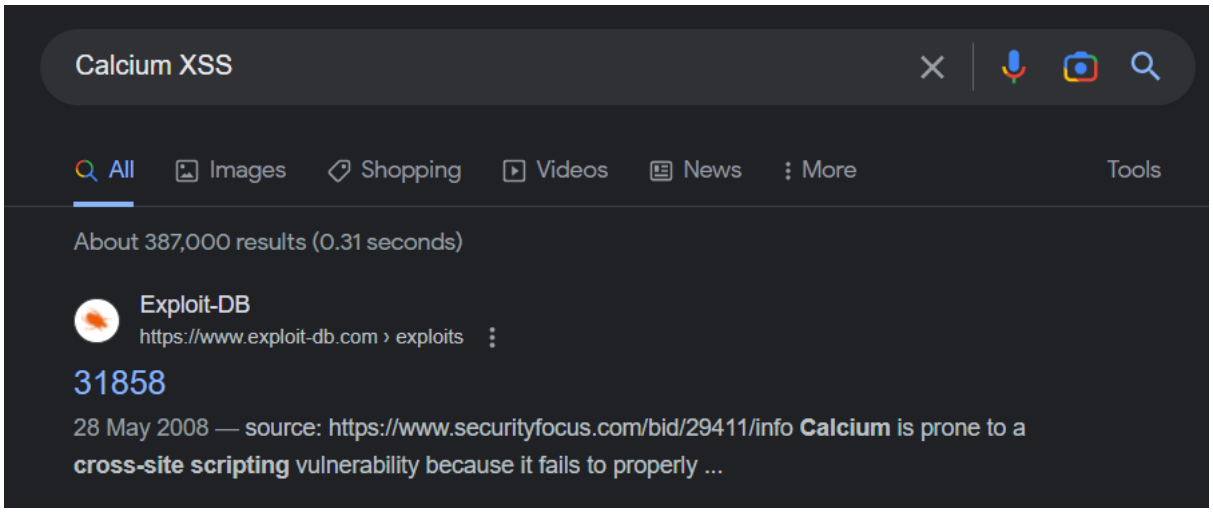
Screenshot:



Question 2:

Google search used to find websites is inurl:Calcium40.pl.

Screenshot:



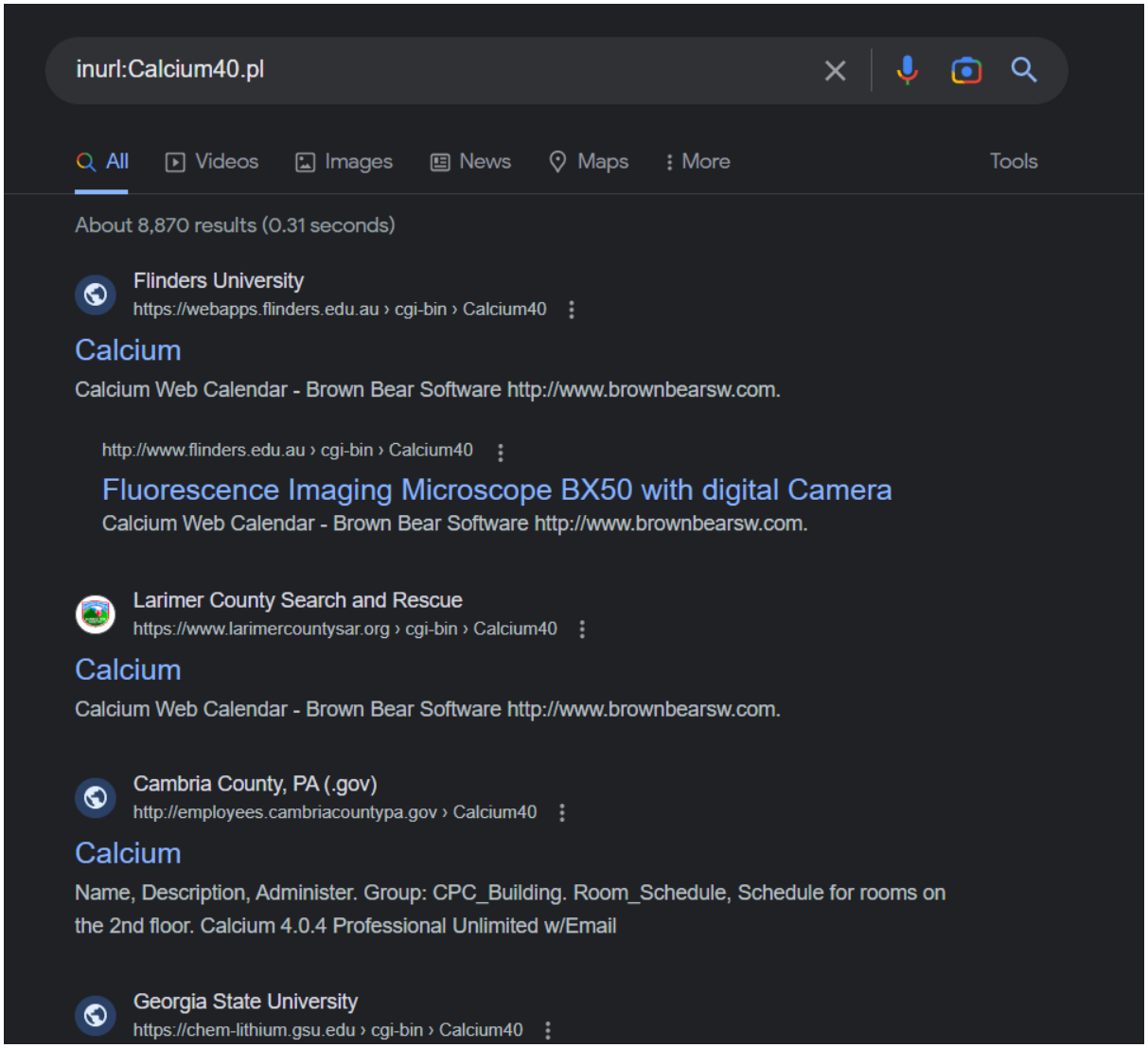
```
source: https://www.securityfocus.com/bid/29411/info

Calcium is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input.

An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the
attacker steal cookie-based authentication credentials and launch other attacks.

Calcium 4.0.4 and 3.10 are vulnerable; other versions may also be affected.

http://www.example.com/cgi-bin/Calcium40.pl?Op=ShowIt&CalendarName=[xss]
```



Comment:

From my quick research I used Exploit-DB (the resource provided in workshop 3) and found that for a site to have the vulnerability it needs to have Calcium40.pl in the url. So, the google search I used to find the websites with the vulnerability was inurl:Calcium40.pl.

Question 3:

Luz Castillo is the only contact from the list located in Miami, Florida.

Screenshot:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ recon-ng
[*] Version check disabled.
```

```
[recon-ng v5.1.2, Tim Tomes (@lanmaster
[*] No modules enabled/installed.
[recon-ng][default] > modules load whois_pocs
[!] Invalid module name.
[recon-ng][default] > marketplace install whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[recon-ng][default] > modules load whois_pocs
[recon-ng][default][whois_pocs] > db insert domains
domain (TEXT): bbc.co.uk
notes (TEXT):
```

```
[recon-ng][default][whois_pocs] > run
```

```
*] Phone: None
*] Region: Cg, FL
*] Title: Whois contact
*] ----------
*] URL: http://whois.arin.net/rest/poc/LCA68-ARIN
*] Country: United States
*] Email: luz.castillo@bbc.co.uk
*] First_Name: Luz
*] Last_Name: Castillo
*] Middle_Name: None
*] Notes: None
*] Phone: None
*] Region: Miami, FL
*] Title: Whois contact
*] ----------
*] URL: http://whois.arin.net/rest/poc/SOUTH100-ARIN
*] Country: United States
*] Email: rob.south@bbc.co.uk
*] First_Name: Rob
*] Last_Name: South
```

Comment:

I ran the command recon-ng in kali terminal and then I load the installed tool whois_pocs. Then I ran db insert domain code provided in workshop 3 to find the contacts list. The was only one contact located in Miami, FL.

Question 4:

Question	Answer
dunstan.org.au resolves to:	151.101.194.159
Other domain names that resolve to the same address	pri.authdns.ripe.net. dns.ripe.net 1680098523 3600 600 864000 3600
Owner of the IP address	Fastly
The IP address range which the IP address belongs	151.101.0.0 – 151.101.255.255
The Autonomous System Number (ASN) that contain the IP address	AS54113
Other netblocks registered under the same ASN	There are 502,128 under the same ASN

Screenshot:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig dunstan.org.au

; <<>> DiG 9.18.8-1-Debian <<>> dunstan.org.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1714
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
; COOKIE: 43b7edf841c862652ceb8c9564269aa5e5c40d58899be31c (good)
;; QUESTION SECTION:
;dunstan.org.au.                IN      A

;; ANSWER SECTION:
dunstan.org.au.         5       IN      A       151.101.194.159

;; AUTHORITY SECTION:
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ dig -x 151.101.194.159

; <<>> DiG 9.18.8-1-Debian <<>> -x 151.101.194.159
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 62876
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
; COOKIE: 4ba4f2846cd96becf3b5796e64269c4d5d605314034d31bf (good)
;; QUESTION SECTION:
;159.194.101.151.in-addr.arpa.  IN      PTR

;; AUTHORITY SECTION:
151.in-addr.arpa.       5       IN      SOA     pri.authdns.ripe.net. dns.ripe.net. 1680098523 3600 600 864000 3600

;; Query time: 43 msec
;; SERVER: 192.168.44.2#53(192.168.44.2) (UDP)
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whois -a  151.101.194.159
% This is the RIPE Database query serv
```

```
route:          151.101.19
descr:          Fastly
```

```
% Information related to '151.101.0.0 - 151.101.255.255'

inetnum:        151.101.0.0 - 151.101.255.255
```

```
descr:          Fastly
```

SuperTool Beta7

as54113 ASN Lookup

asn:as54113

Total amount of IPs for this ASN: **502,128**

As Number	As Name	CIDR Range
54113	Fastly, Inc.	23.154.64.0/24
54113	Fastly, Inc.	23.185.0.0/24
54113	Fastly, Inc.	23.235.32.0/23
54113	Fastly, Inc.	23.235.35.0/24
54113	Fastly, Inc.	23.235.36.0/23
54113	Fastly, Inc.	23.235.39.0/24
54113	Fastly, Inc.	23.235.45.0/24
54113	Fastly, Inc.	43.249.73.0/24

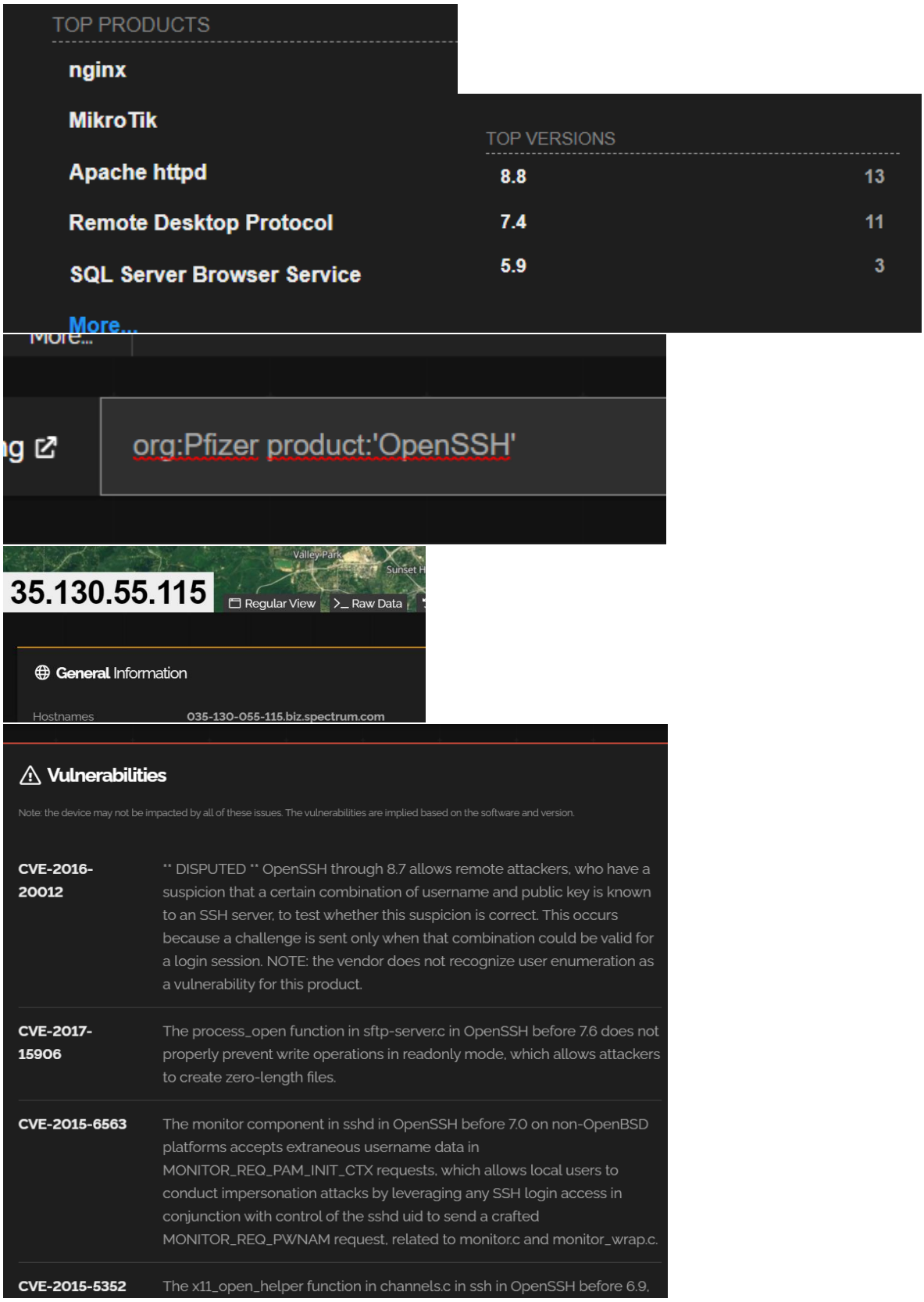
Comments:

The first two rows of the table I used basic commands such as dig in kali which I learnt from workshop. I then used the whois -a 151.101.194.159 and observed to find all information which helped in finding rows third, four, and five. The final row I used an online tool called mxtoolbox super tool and searched all the other ips using as54113 with the search asn:as54113.

Question 5:

Question	Answer
What web server(s) are used by this company?	Apache httpd, nginx, OpenSSH and more
What versions of OpenSSH are used by this company?	Three versions of OpenSSH: 8.8, 7.4, and 5.9
According to Shodan, what are some of the vulnerabilities in one of the versions of the OpenSSH servers?	In the version 5.9, vulnerabilities are: CVE-2016-20012, CVE-2017-15906, CVE-2015-6563 and more
Choose the most recent vulnerability from above, and find the CVSS2.0 string for it by looking it up on nvd.nist.gov.	Latest above is CVE-2016-20012 and its CVSS2.0 string is (AV:N/AC:M/Au:N/C:P/I:N/A:N)

Screenshot:


TOP PRODUCTS
nginx
MikroTik
Apache httpd
Remote Desktop Protocol
SQL Server Browser Service
More...
TOP VERSIONS
8.8 13
7.4 11
5.9 3
org:Pfizer product:'OpenSSH'
35.130.55.115
Regular View
Raw Data
General Information
Hostnames 035-130-055-115.biz.spectrum.com
Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2016-20012 ** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.
CVE-2017-15906 The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2015-6563 The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.
CVE-2015-5352 The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9,

CVE-2016-20012 Detail

Description

** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 4.3 MEDIUM **Vector:** (AV:N/AC:M/Au:N/C:P/I:N/A:N)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2016-20012
NVD Published Date:
09/15/2021
NVD Last Modified:
04/18/2022
Source:
MITRE

Comment:

I just learnt a bit about the Shodan search and answered row one, two (with search modifier), three by looking at the appropriate sections in the web pages. The fourth row I used the nvd nist gov website provided in the question to find the CVSS 2.0 version string.

Question 6:

Screenshot:

q6.py

```python
import sys, socket

socket.setdefaulttimeout(0.1) # set timeout to 100ms
host = "www.adelaide.edu.au"
with open("dnsmap.txt") as f:
    for line in f:
        try:
            base = line.strip() + "." + host
            ip = socket.gethostbyname(base)
            print(f"{base} resolves to {ip}")
        except:
            pass # ignore error
```

```
av.adelaide.edu.au resolves to 129.127.95.145
cp.adelaide.edu.au resolves to 129.127.149.31
cs.adelaide.edu.au resolves to 129.127.149.1
gg.adelaide.edu.au resolves to 129.127.144.5
gp.adelaide.edu.au resolves to 192.43.227.193
```

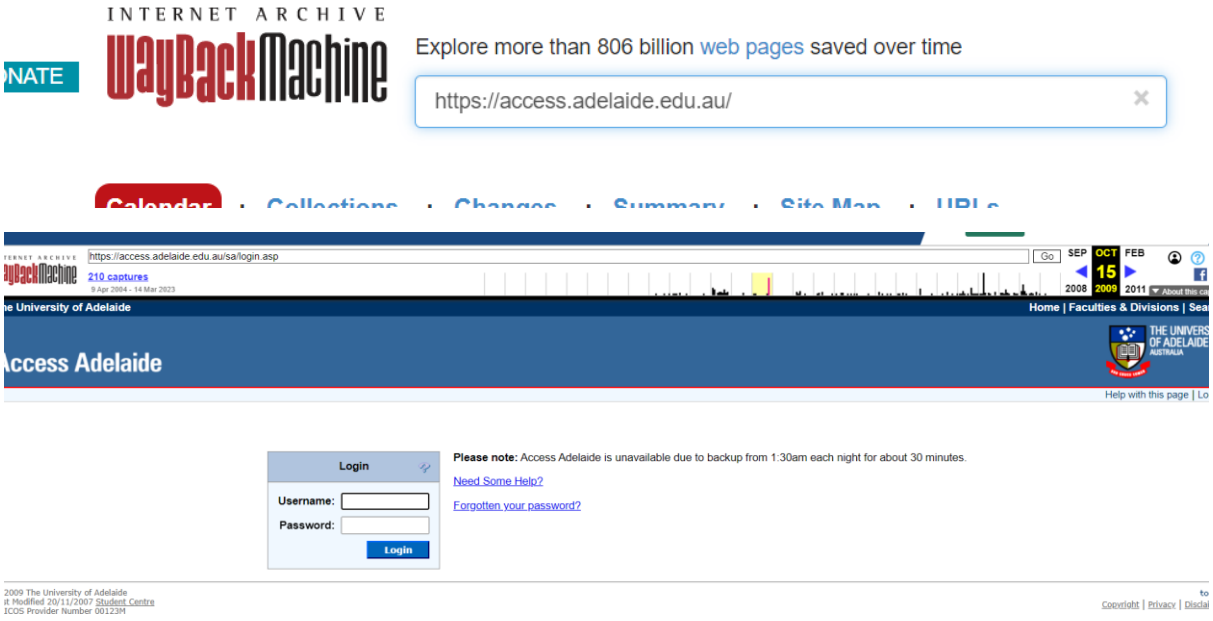
Comment:

The modified script has the file defined and a for loop to take each of the line in the file at a time with the host. So the print line now displays for every line in the dnsmap.txt file.

Question 7:

The 2009 version of the Access Adelaide webpage looks very similar to its latest version in 2023.

Screenshot:



Access Adelaide is currently unavailable, for one of the following reasons:

- The system is down for scheduled maintenance (see below)
- The system is under heavy load - please try again later

Scheduled downtime:

- *None*

Regular downtime:

- Nightly 1:30am to 2:00am for database backup.

For assistance, contact the student centre:
Telephone: +61 8 8303 5208
(Country and interstate callers toll free on 1800 061 459)
Email: student.centre@adelaide.edu.au

Comment:

I used the Wayback Machine search bar to find how the Access Adelaide login webpage looked like in October 15, 2009. All I did was search the URL and the selected the year specified in the question

and I got redirected to the old version. Some pages I opened were down versions of the page for example February, 2009 as seen above.

Question 8:

a) The port is 55554. b) The screenshot showing the secret answer is below. c) I identified by running the nmap command with -p to look for the port number. These commands were explained in workshop 4. Then I retrieved the secret answer based on the identified port. I used netcat command with the ip and the port number to display the secret.

Screenshot:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p 20000-60000 192.168.44.128
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 07:07 EDT
Nmap scan report for 192.168.44.128
Host is up (0.0011s latency).
Not shown: 40000 filtered tcp ports (no-response)
PORT      STATE SERVICE
55554/tcp open  unknown
MAC Address: 00:0C:29:CD:7A:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 174.57 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ netcat 192.168.44.128 55554
 ___________________________________________
/ hacklab_{enjoinment-sexdigitism-preveto \
\ es}                                     /
 -------------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

Question 9:

a) Connected to the port and the secret was hacklab_{nonirrevocable-mycoderm-checkpointed}.
b) Screenshot of answer below.
c) At first, I was getting timeout error when I did it in regular kali so I refereed back to workshop 4 and saw that we had to use root kali for SYN packet and I also saw about the command -sS which specifies SYN scan. Then with the addition of -sS, the addition of 1122,2233,3344 to -p and the && netcat port I was successfully able to display the secret.

Screenshot:

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p1122,2233,3344 192.168.44.128 && netcat 192.168.44.128 12345
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 08:05 EDT
Nmap scan report for 192.168.44.128
Host is up (0.00056s latency).

PORT     STATE    SERVICE
1122/tcp filtered availant-mgr
2233/tcp filtered infocrypt
3344/tcp filtered bnt-manager
MAC Address: 00:0C:29:CD:7A:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
 _____________________________________
/ hacklab_{nonirrevocable-mycoderm-checkp \
\ ointed}                                /
 _____________________________________
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```