Assignment 2

Wednesday, 20 March 2024 3:45 PM

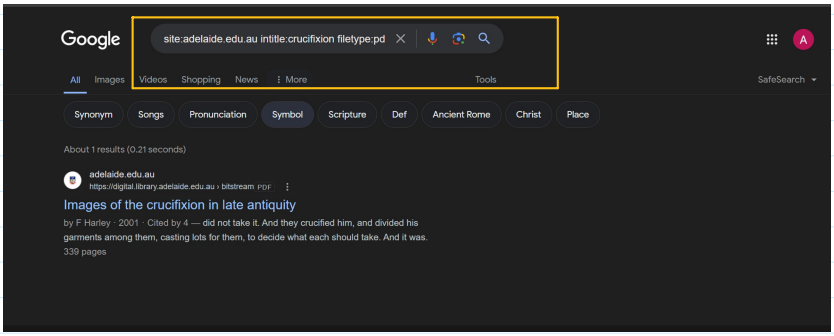
Part I - OSINT, Recon & Network Scanning

1. **(1 point) Search on the University of Adelaide domain for a PDF document containing the word "crucifixion" in the title of the document.**
   (a) What is the Google search syntax and
   (b) who is the author of the PDF file?

   The google search syntax is site:adelaide.edu.au intitle:crucifixion filetype:pdf.
   The search parameter **site** specifies that we want to search for adelaide.edu.au and the **intitle** parameter specifies that we want to search for a specific word in the title. We can then narrow down our search further by specifying the **file type** which is a pdf in our case.

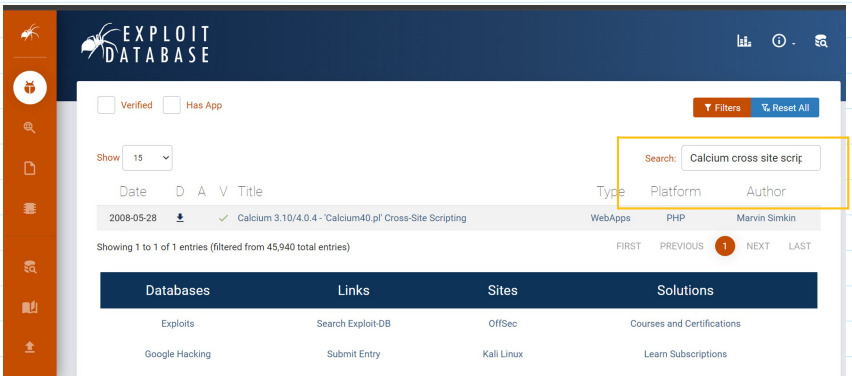
   Upon inspecting the file after downloading it, the author is Felicity Harley.

   A screenshot of this command can be seen below.

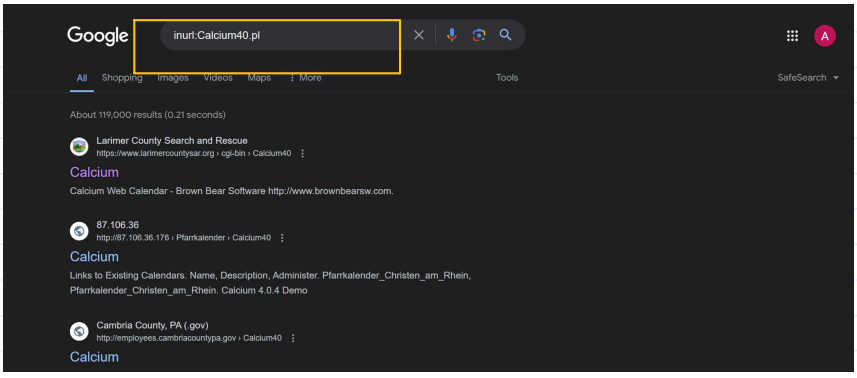


2. **(1 point) Google dorks are good at finding vulnerabilities in websites. Do a quick research for the cross-site scripting (XSS) vulnerability in a product called Calcium by Brown Bear Software (you will learn about XSS in subsequent modules). What google search would you perform to find websites running Calcium? Perform the search, and paste a screenshot of the results.**

   The following screenshot shows the vulnerability. Reading the article, it appears that the parameter **CalenderName** is suspectable to java script injection. This was found by searching for 'Calcium cross site scripting'.



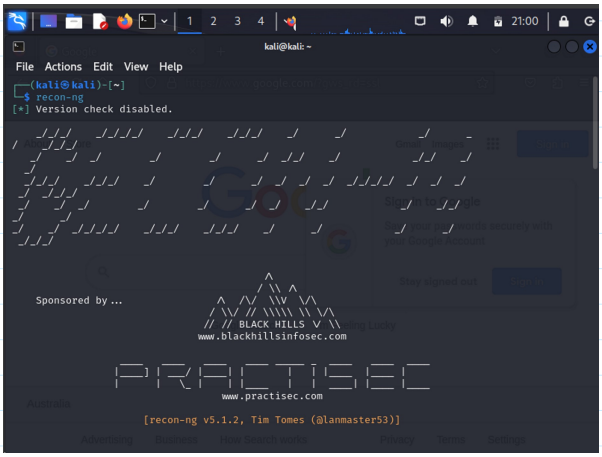
   Websites running Calcium can be found by running the **inurl** parameter.



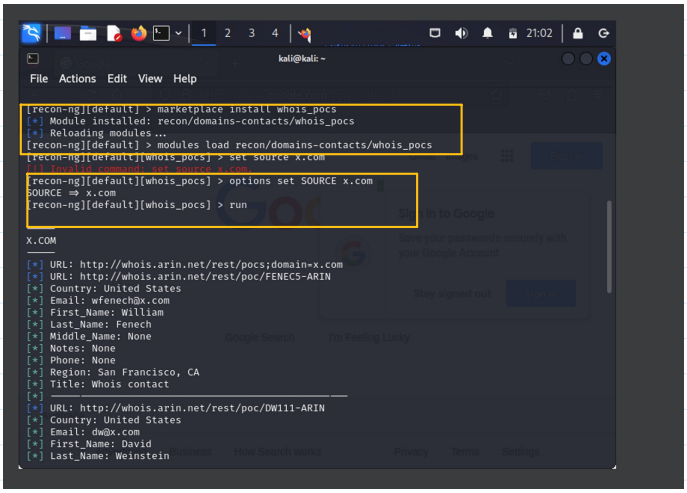
3. **(1 point) Use the whois_pocs module in recon-ng to list some contacts for x.com. Who is located in Carson, CA?**

   The Following steps were used to find out the contact located in Carson, CA.

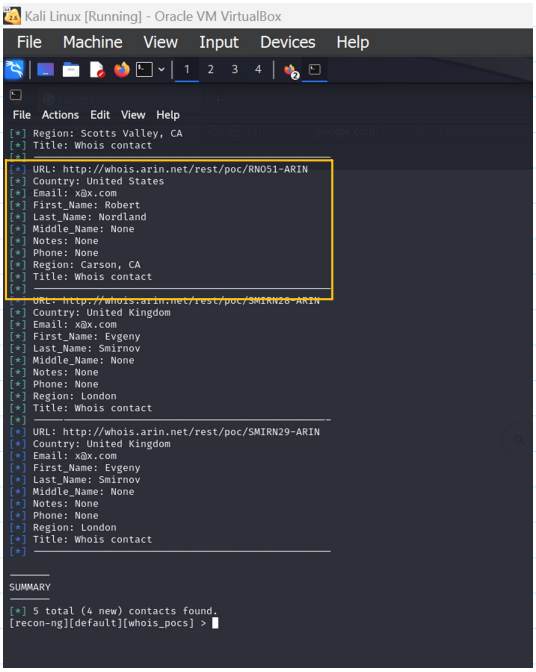
   - Load recon-ng using the command **recon-ng.**



- Install the module using the command "**Marketplace install whois_pocs**"
- Load the module using the command "**load recon/domains-contacts/whois-pocs**"
- Set the souce using command "**set SOURCE x.com**"
- Run the module using "**run**"



- Scrolling through the output, it can then be seen that there is only one contact in Carson, CA who is Robert Nordland as seen in the screenshot below.

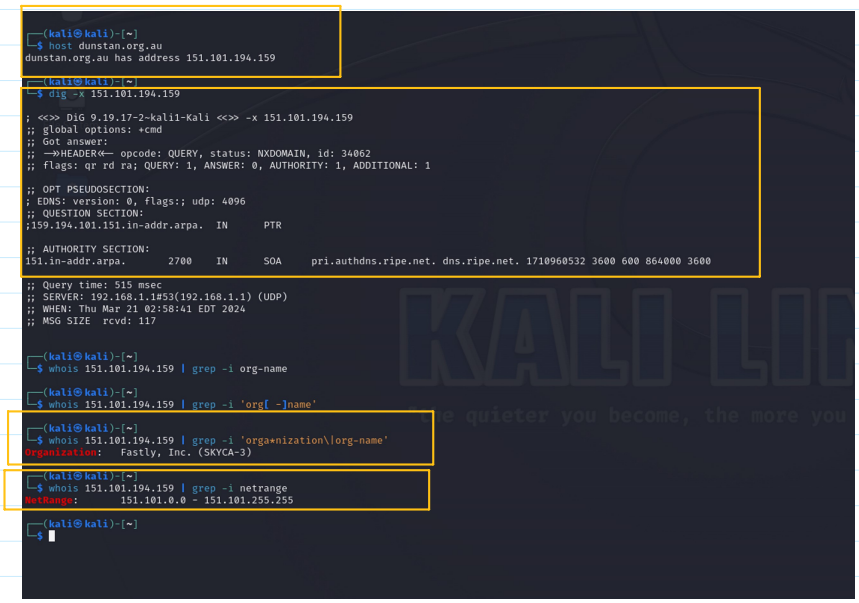


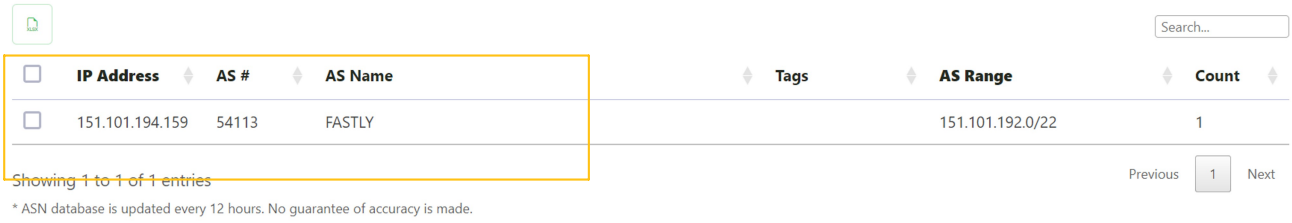
Question 4: (2 points) Use the techniques introduced in the workshop to complete the following table.

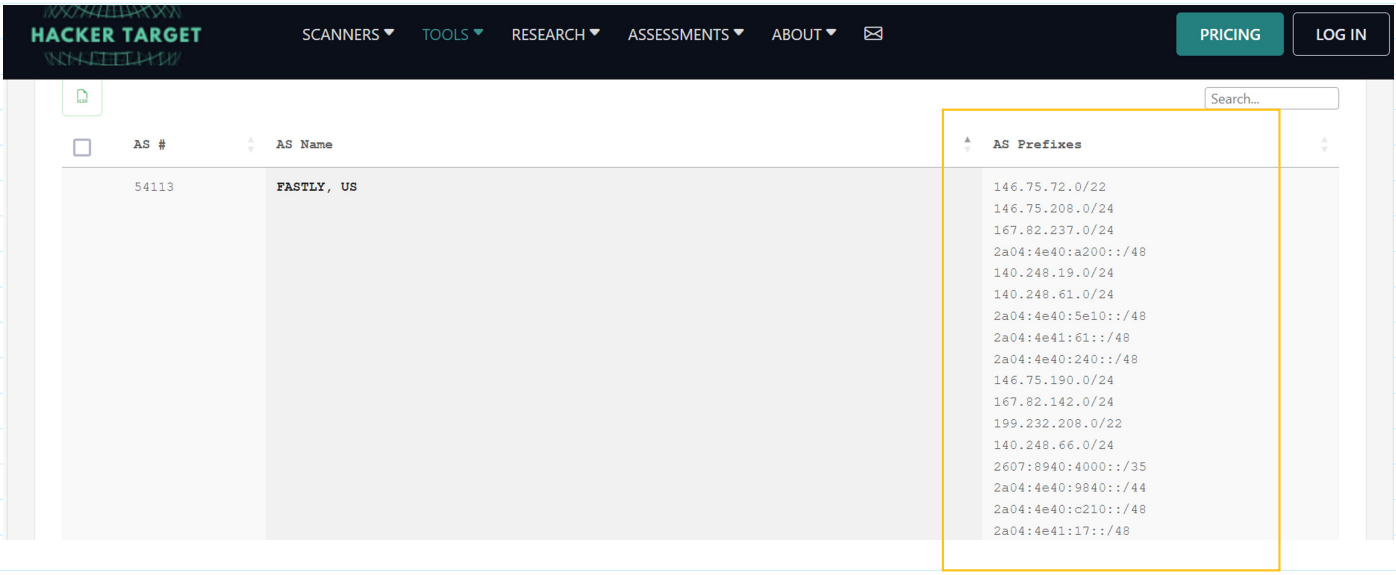
Question	Answer	
dunstan.org.au resolves to:	(IP address)	The ip address dunstan.org.au resolves to is 151.101.194.159.
Other domain names that resolve to the same address	(List a subset of other domain names that resolve to the same IP address as above)	Other domain names that resolve to the same address are 1. pri.authdns.ripe.net and 2. dns.ripe.net
Owner of the IP address	(Organisation name according to whois)	Owner of the ip address is Fastly Inc.
The IP address range which the IP	(Netblock IP range according to whois)	151.101.0.0 - 151.101.255.255

address belongs		
The Autonomous System Number (ASN) that contain the IP address	(ASN that contains the IP address range. e.g. AS1234)	54113
Other netblocks registered under the same ASN	(List of netblocks/ip address ranges)	The list can be viewed in the screenshot below.

*All answers populated in table above are highlighted in the screenshot below with commands used.



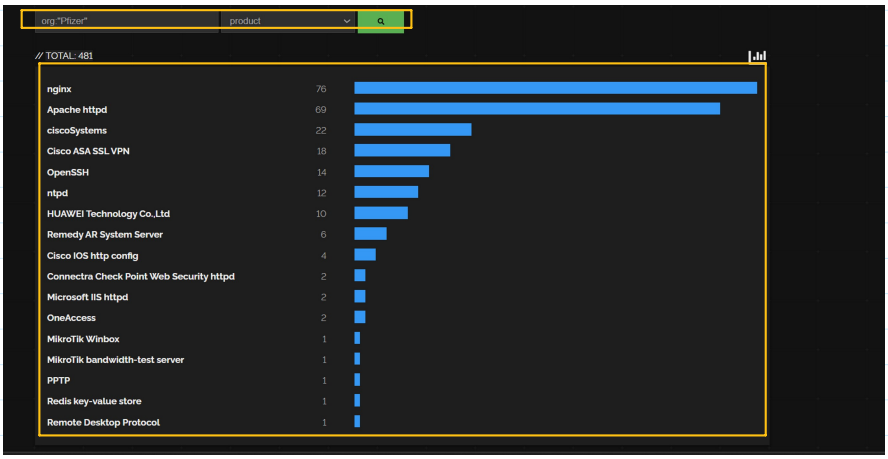




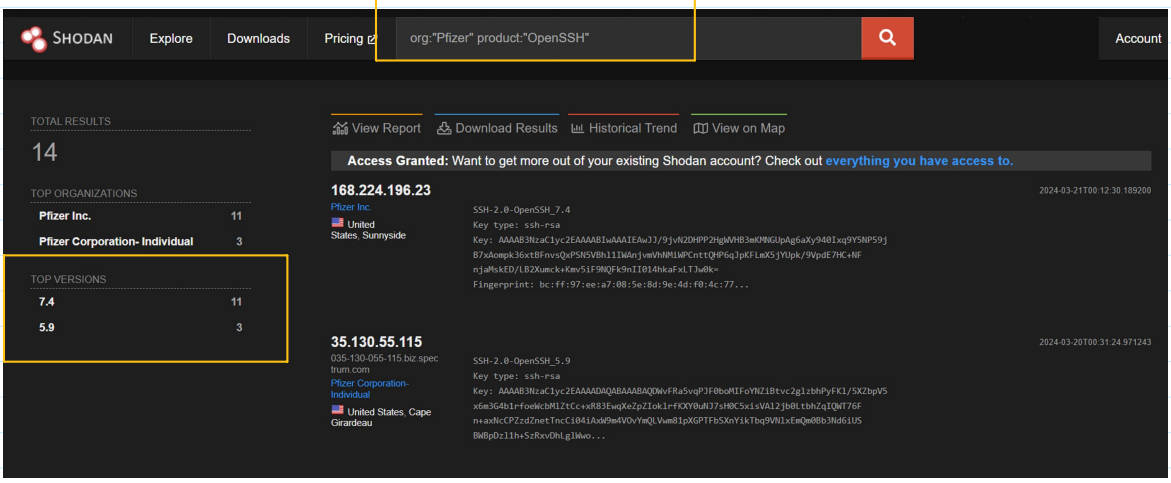
5. **(2 points) Create a free account on shodan.io (https://shodan.ioLinks to an external site.). You will be entitled to an academic upgrade if you register using your @student.adelaide.edu.au or @adelaide.edu.au account. Learn a bit about the Shodan search modifiers, similar to the Google ones (e.g., see hereLinks to an external site.) . Search for information on hosts under the company "Pfizer" and answer the following questions. Start with the "org:" modifier.**

Question	Answer
What web server(s) are used by this company?	Some of the main web servers used are niginx, Apache httpd and openSSH, other can be seen in the screenshot belo.
What versions of OpenSSH are used by this company?	7.4 and 5.9
According to Shodan, what are some of the vulnerabilities in one of the versions of the OpenSSH servers?	seen in the screenshot below
Choose the **most recent** vulnerability from above, and find the **CVSS2.0 string** for it by looking it up on nvd.nist.gov.	**Vector:** CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

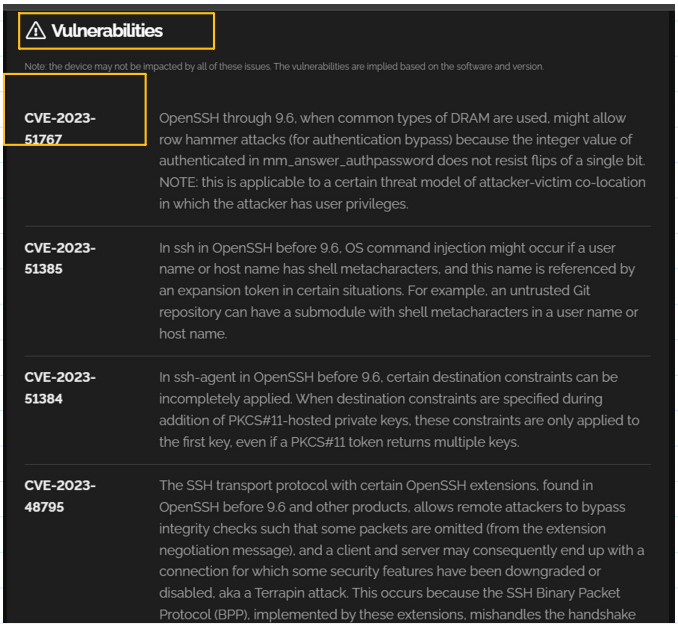
- Servers used by the organisation 'Pfizer'



- Version of 'OpenSSH' used by 'Pfizer'



- Vulnerabilities, boxed is the latest one



- Using the nvd.nist.gov website, vector/string of the latest vulnerability can be found.

Description

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.0 HIGH

Vector:
CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

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.

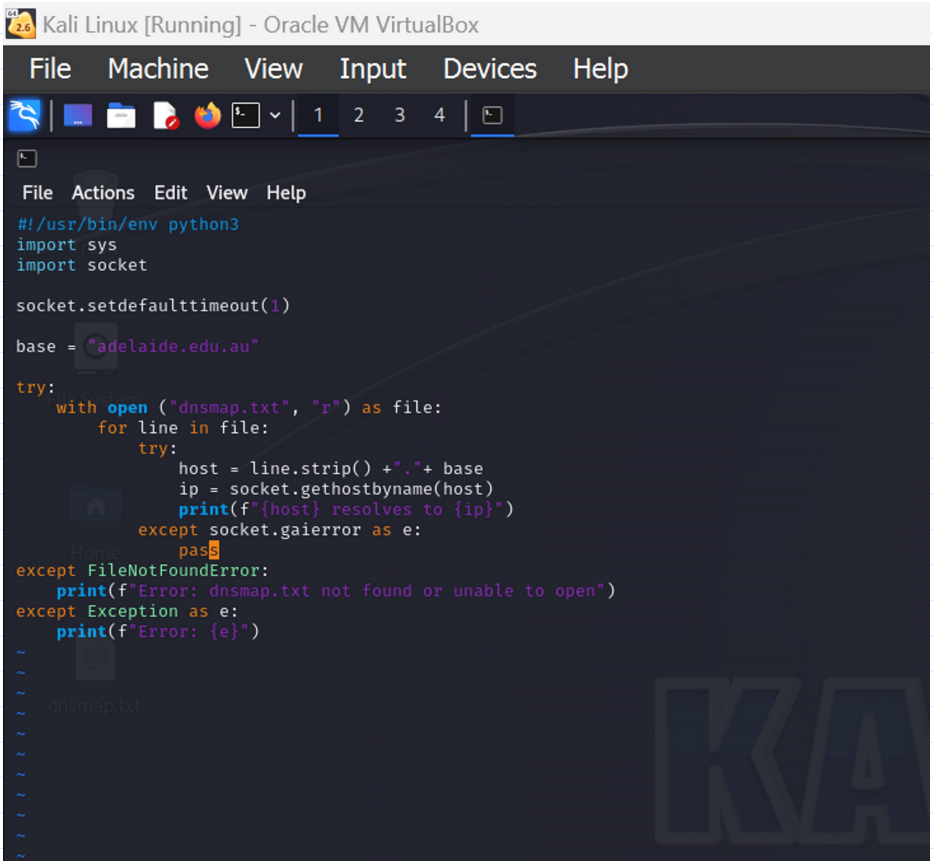
QUICK INFO

CVE Dictionary Entry:
CVE-2023-51767
NVD Published Date:
12/24/2023
NVD Last Modified:
02/27/2024
Source:
MITRE

6. (2 points) Write a simple DNS brute-force script in your language of choice to enumerate hostnames under a given domain and an input dictionary. Run the code against **adelaide.edu.au** using this dictionary file (this file contains the entire 3-character permutations - please unzip before use). ***Running the whole list will take a long time, so you can stop after a few minutes.*** Paste some preliminary results.
Here is a sample code for Python3:

```
#!/usr/bin/env python3
import sys, socket
socket.setdefaulttimeout(0.1) # set timeout to 100ms
host = "www.adelaide.edu.au"
try:
    ip = socket.gethostbyname(host)
    print(f"{host} resolves to {ip}")
except:
    pass # ignore error
```

The following python script is used to enumerate hostnames. A loop is used to read the dnsmap.txt file line by line and a for loop is then used to resolve the host to its ip address using the parameter gethostbyname(). Exception handling is done as well to ensure error messages can be interrupted.



The script is then run using python3 which shows domains resolving to their ip addresses.

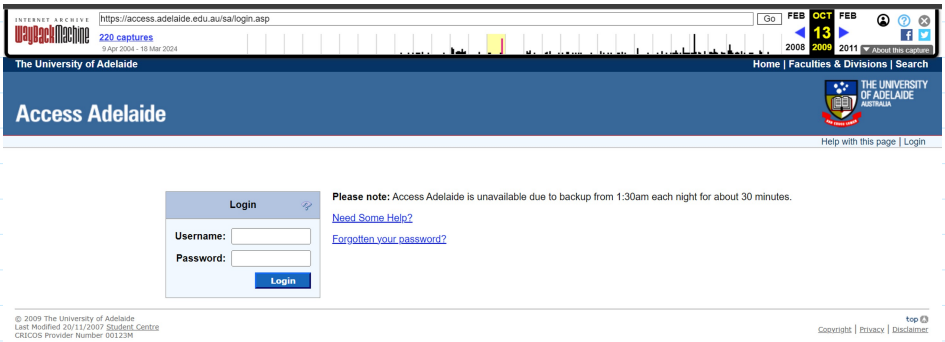
```
~
~
~
```

The script is then run using python3 which shows domains resolving to their ip addresses.

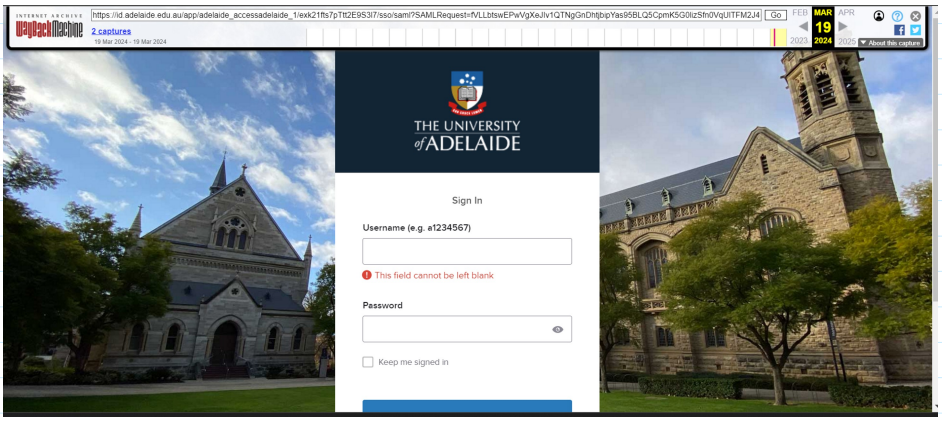
```
┌──(kali㉿kali)-[~]
└─$ python3 en.py
m.adelaide.edu.au resolves to 129.127.149.1
av.adelaide.edu.au resolves to 129.127.95.145
cp.adelaide.edu.au resolves to 129.127.149.31
cs.adelaide.edu.au resolves to 129.127.149.1
gg.adelaide.edu.au resolves to 129.127.144.5
gp.adelaide.edu.au resolves to 192.43.227.193
id.adelaide.edu.au resolves to 52.223.1.182
ks.adelaide.edu.au resolves to 129.127.43.66
mw.adelaide.edu.au resolves to 129.127.144.69
ns.adelaide.edu.au resolves to 129.127.40.3
pc.adelaide.edu.au resolves to 129.127.178.166
sb.adelaide.edu.au resolves to 129.127.144.69
aml.adelaide.edu.au resolves to 129.127.9.104
ams.adelaide.edu.au resolves to 52.255.35.249
api.adelaide.edu.au resolves to 129.127.149.154
apm.adelaide.edu.au resolves to 10.160.19.1
apr.adelaide.edu.au resolves to 129.127.149.1
asb.adelaide.edu.au resolves to 129.127.144.60
asp.adelaide.edu.au resolves to 129.127.149.1
awx.adelaide.edu.au resolves to 129.127.149.178
bsl.adelaide.edu.au resolves to 129.127.194.23
cbs.adelaide.edu.au resolves to 10.230.0.47
cdm.adelaide.edu.au resolves to 10.33.23.13
cms.adelaide.edu.au resolves to 10.33.78.12
cwa.adelaide.edu.au resolves to 129.127.44.182
edm.adelaide.edu.au resolves to 54.183.0.47
eeg.adelaide.edu.au resolves to 129.127.149.1
ees.adelaide.edu.au resolves to 129.127.149.1
eft.adelaide.edu.au resolves to 129.127.125.210
elc.adelaide.edu.au resolves to 129.127.149.27
elm.adelaide.edu.au resolves to 10.130.4.78
emu.adelaide.edu.au resolves to 129.127.149.1
eng.adelaide.edu.au resolves to 192.43.228.130
erm.adelaide.edu.au resolves to 20.37.196.197
eso.adelaide.edu.au resolves to 192.43.228.152
faq.adelaide.edu.au resolves to 129.127.144.9
fcs.adelaide.edu.au resolves to 129.127.194.26
fin.adelaide.edu.au resolves to 10.230.0.20
ftp.adelaide.edu.au resolves to 192.43.228.177
gpo.adelaide.edu.au resolves to 129.127.40.3
gsm.adelaide.edu.au resolves to 129.127.149.1
^Z
zsh: suspended  python3 en.py

┌──(kali㉿kali)-[~]
└─$
```

7. **(1 point) Use the Wayback Machine to find out how Access Adelaide (access.adelaide.edu.au) looked like in 2009. How does it look compared to the current Access Adelaide web page?**

   The screenshot below shows the Access Adelaide site from 2009. This looks completely different to the new page now. The fonts are different and the layout of the web page is different as well.



   The new Access Adelaide page is as below. The only similarity between the two is the content, both still have a login section with username and password. Both also still have options to reset your password and an option for more help. The new webpage has a background showing the university of Adelaide grounds. The old one just has a white plain background.



8. **(1 point) There is a network service running on the Hacklab VM behind a port somewhere between 20000 and 60000.**

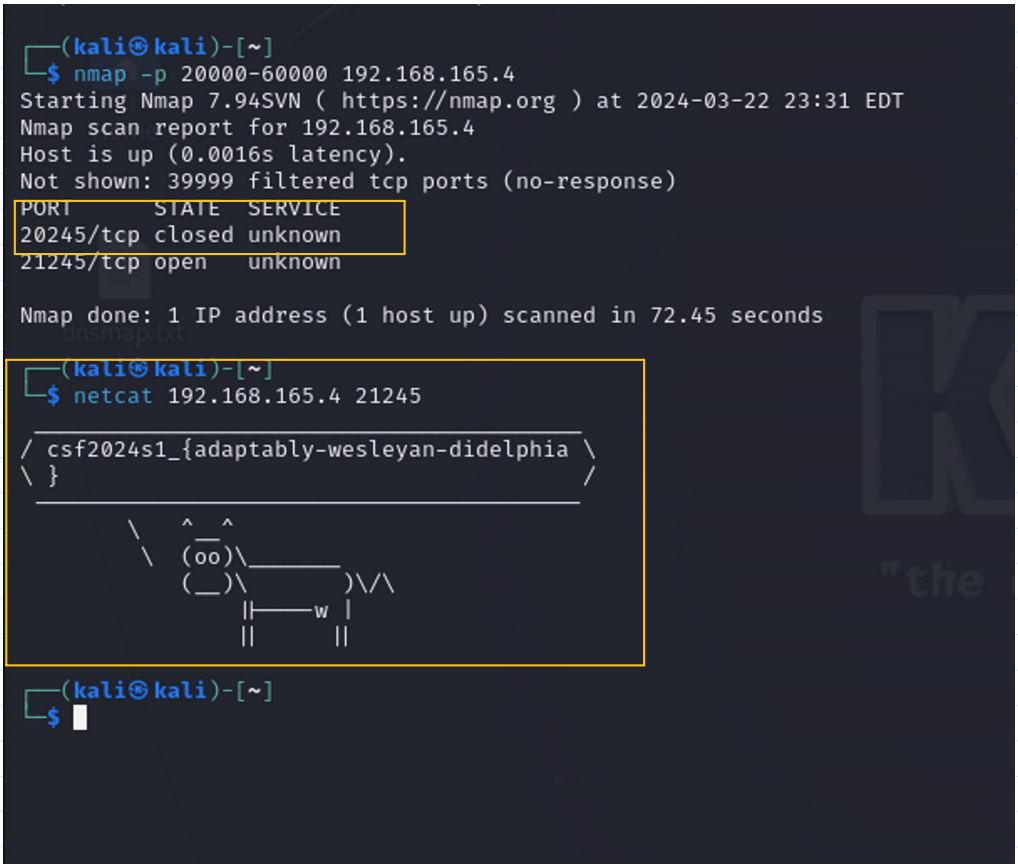
   a. Identify the port number and connect to it using netcat (“nc” or “netcat” command) to retrieve the secret.

   b. Paste a screenshot showing the secret answer.

   c. Explain how you identified and retrieved the secret answer.

The port number open can be found that using the nmap command and the -p flag. The -p flag allows us to scan multiple ports between 20000 and 60000. The output then shows an open port which is port 21245.

The netcat command can then be used with your hack lab vm ip address to retrieve the secret message as displayed in the screenshot below.



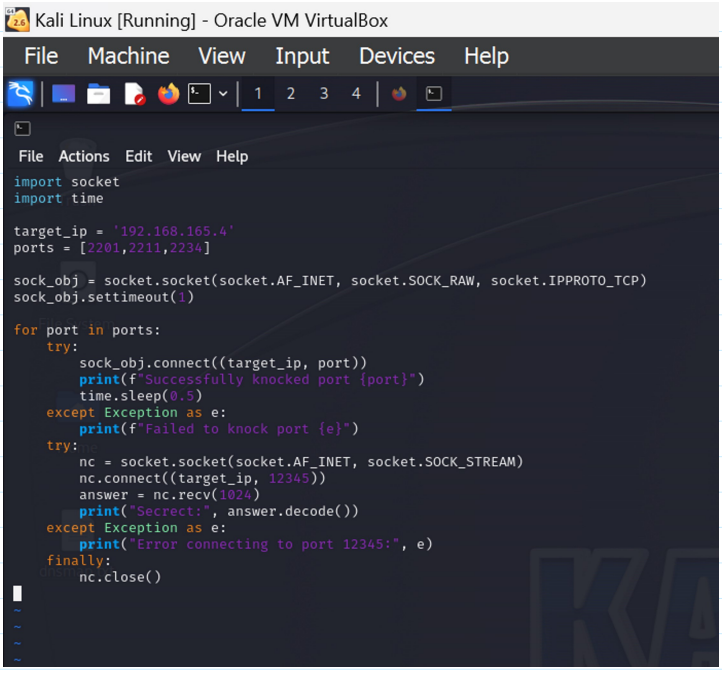
9. (1 point) The Hacklab VM is running what's known as a "port knocking" that opens a previously closed port 12345 for a limited time if you send a series of SYN packets to these 3 ports: 2201, 2211, 2234 (be careful, there is a timeout of 15 seconds, so you may have to write a simple script).

a. Connect to port 12345 using netcat to get the secret.

b. Paste a screenshot showing the secret answer.

c. Explain how you identified and retrieved the secret answer.

The following script was used to knock the ports sequentially in order to connect to port 12345. As seen in the screenshots below, the ports are successfully knocked however the connection was not able to be made.



```
┌──(kali㉿kali)-[~]
└─$ sudo python3 question9.py
[sudo] password for kali:
Failed to knock port [Errno 101] Network is unreachable
Error connecting to port 12345: [Errno 101] Network is unreachable
Failed to knock port [Errno 101] Network is unreachable
Error connecting to port 12345: [Errno 101] Network is unreachable
Failed to knock port [Errno 101] Network is unreachable
Error connecting to port 12345: [Errno 101] Network is unreachable
```

Hence the question could not be completed.