Assignment 0x02 - OSINT, Recon & Network Scanning

**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?
   1. site:adelaide.edu.au intitle:crucifixion filetype:pdf
   2. Felicity Harley

A screenshot of a computer

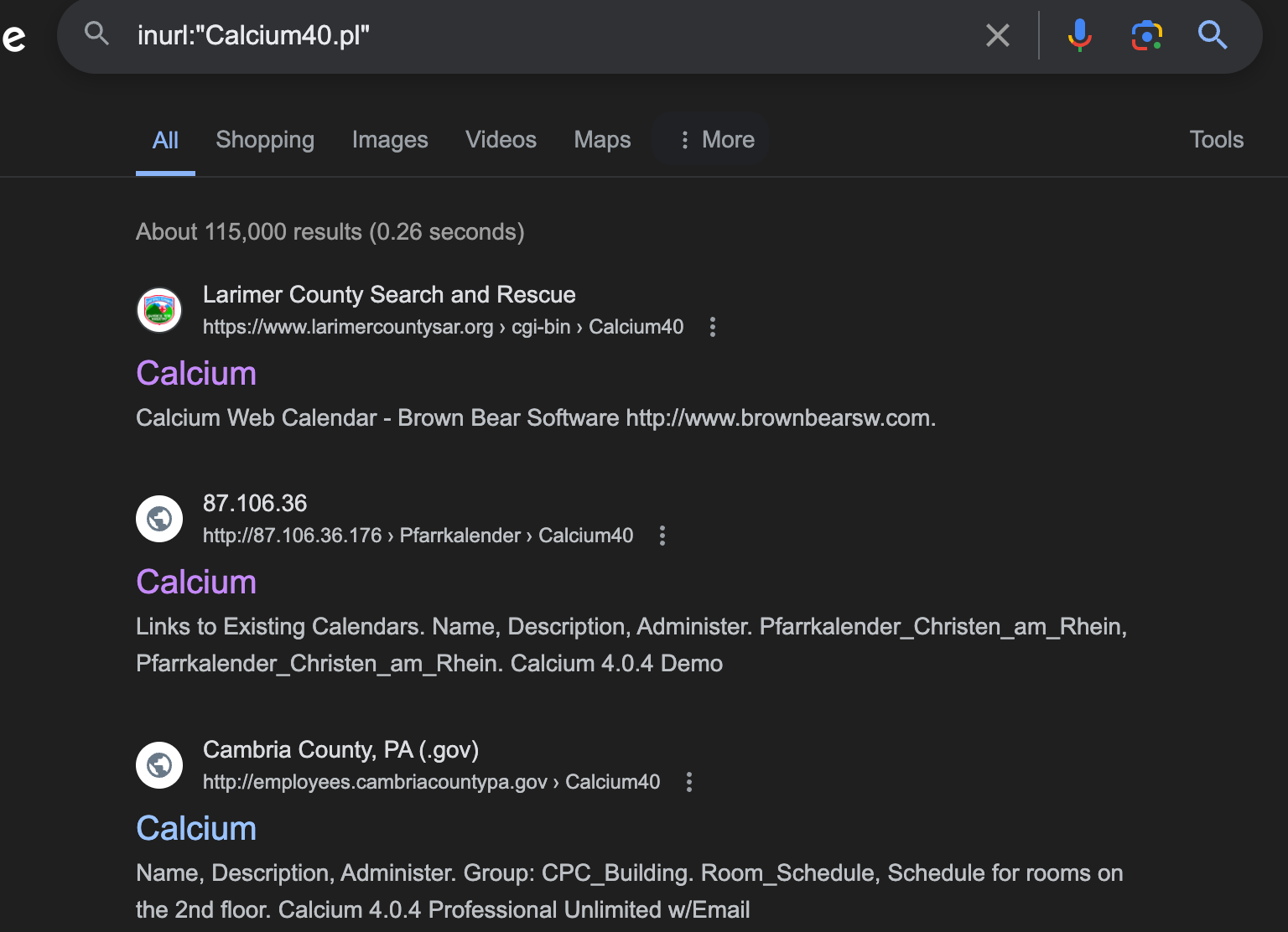
Description automatically generated

1. (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.

First of all, I perform a google search using the query “inurl:"calcium" intitle:" Brown Bear Software””, found the detail of “CVE-2008-2507” from the website <https://www.cvedetails.com/cve/CVE-2008-2507/>, noticed that “Calcium40.pl” is a key word of the vulnerability, then I use the query “inurl:"Calcium40.pl"” searched in Google and got the answer as followed, I picked the second one to perform the XSS vulnerability by adding “<script>alert(1)</script>” in the URL and succussed.

A screenshot of a computer

Description automatically generated





A black background with white text

Description automatically generated

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

Robert Nordland

A black screen with white text

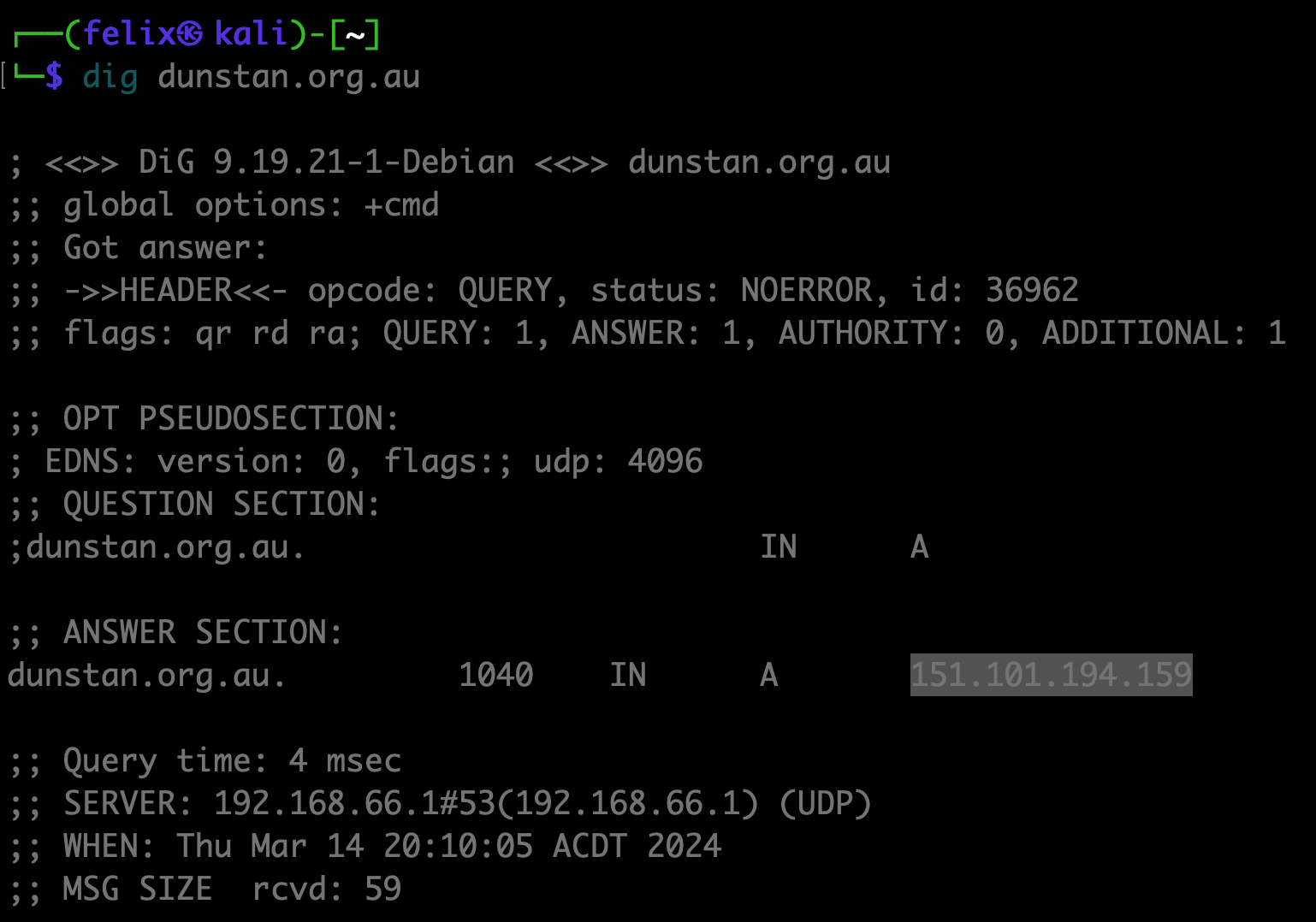
Description automatically generated

Just as what we have done in the workshop2, first, create a workspace using the command “workspaces create Assi2”, then, using the command “modules load whois\_pocs” to load the pre-installed “whois\_pocs” module. Insert the domain into the database using “db insert domains”, set the source URL as “x.com” using “options set SOURCE x.com”, run the module by typing the command “run”, finally, use the sql query “db query select \* from contacts where region = "Carson, CA"” to see the result.

1. (2 points) Use the techniques introduced in the workshop to complete the following table.

|  |  |
| --- | --- |
| **Question** | **Answer** |
| **dunstan.org.au** resolves to: | 151.101.194.159 |
| Other domain names that resolve to the same address | N/A “status: NXDOMAIN” |
| Owner of the IP address | Fastly, Inc. |
| 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 | 172.253.62.0-172.253.62.255 142.251.16.0-142.251.16.255  66.33.198.0-66.33.198.255  208.113.145.0-208.113.145.255  69.163.225.0-69.163.225.255  64.90.62.0-64.90.62.255  69.163.136.0-69.163.136.255  208.113.169.0-208.113.169.255 |

1. Use “dig dunstan.org.au” to find the A answer of the domain.



1. Can not find related domain.

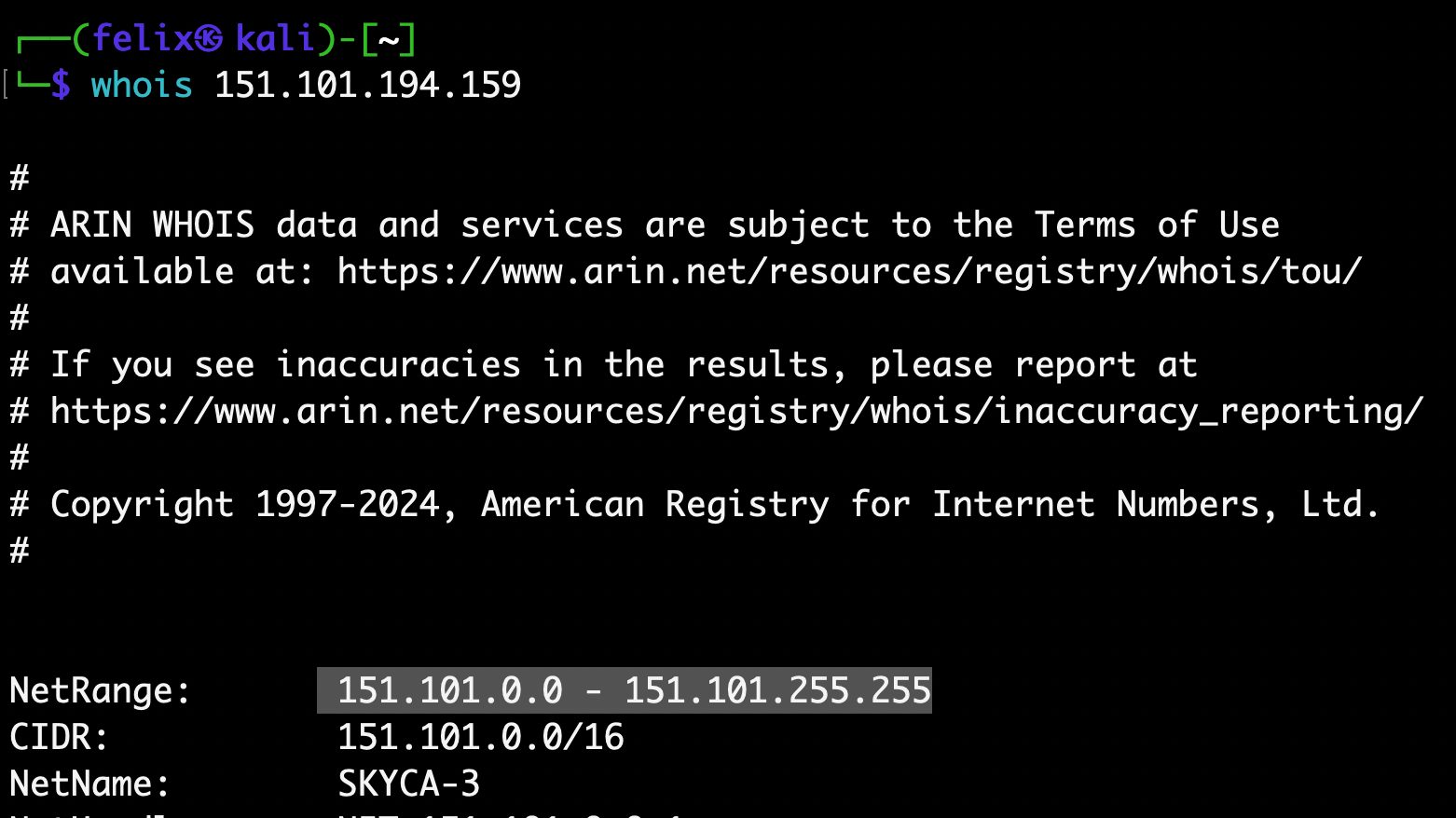
A screenshot of a computer

Description automatically generated

1. Organization name is Fastly, Inc.



1. IP address range is: 151.101.0.0 - 151.101.255.255



1. ASN number is: AS54113, by using “robtex” which introduced in the workshop.

A screenshot of a computer

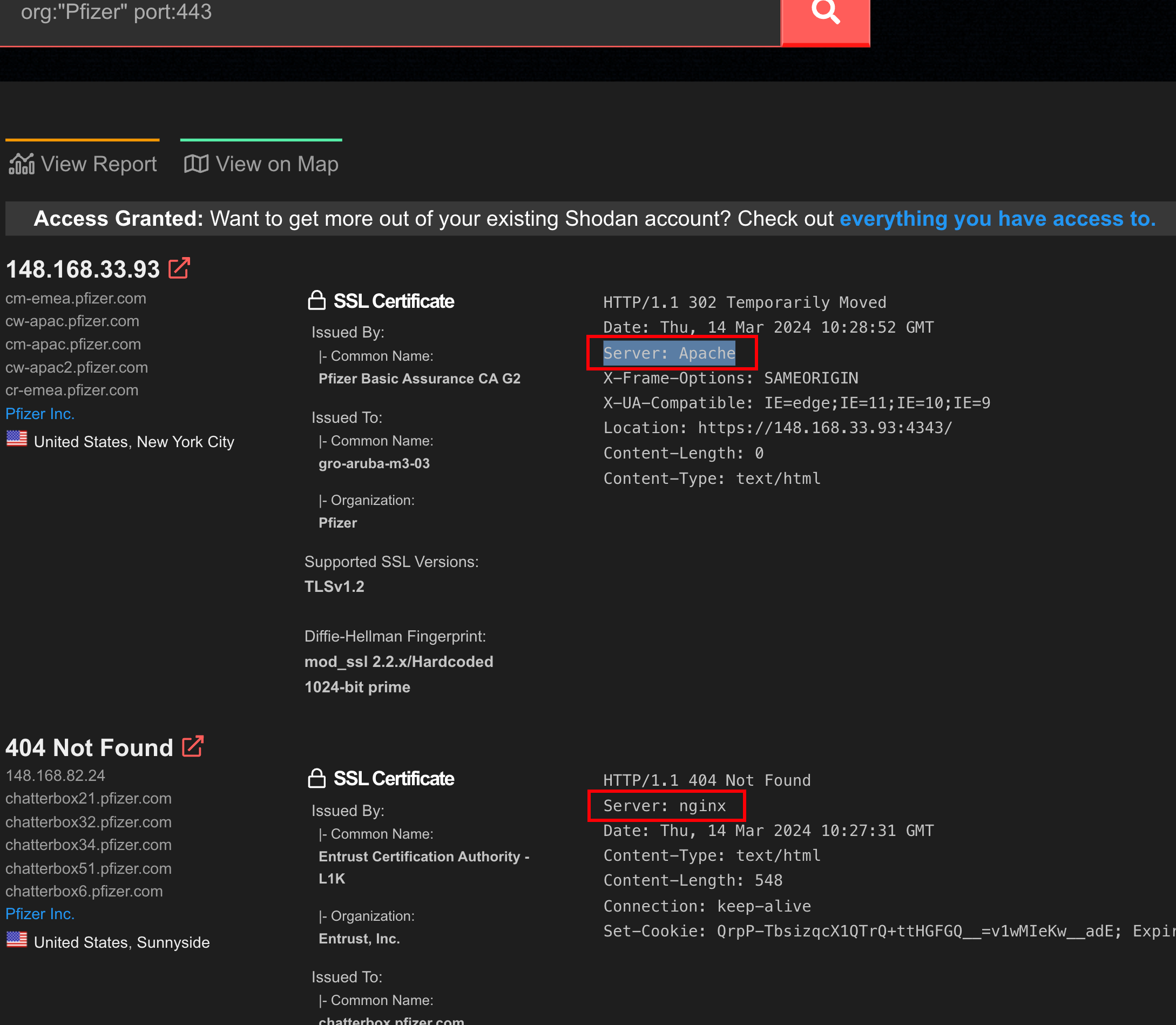
Description automatically generated

1. By following the instruction of “Maltego” in workshop2 to find other netblocks .A screenshot of a computer

   Description automatically generated
2. (2 points) Create a free account on shodan.io ([https://shodan.ioLinks to an external site.](https://shodan.io/)). 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.](https://thor-sec.com/cheatsheet/shodan/shodan_cheat_sheet/" \t "_blank)) . 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? | Nginx  Apache |
| What versions of OpenSSH are used by this company? | SSH-2.0-OpenSSH\_7.4 |
| According to Shodan, what are some of the vulnerabilities in one of the versions of the OpenSSH servers? | CVE-2023-51767  CVE-2023-51385  CVE-2023-51384  CVE-2023-48795  CVE-2023-38408  … |
| Choose the **most recent** vulnerability from above, and find the **CVSS2.0 string** for it by looking it up on nvd.nist.gov. | No CVSS2.0 string provided, only 3.0: “CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H” |

1. By using the query “org:"Pfizer" port:443” to search the web server(s) (port 443) of Pfizer company.

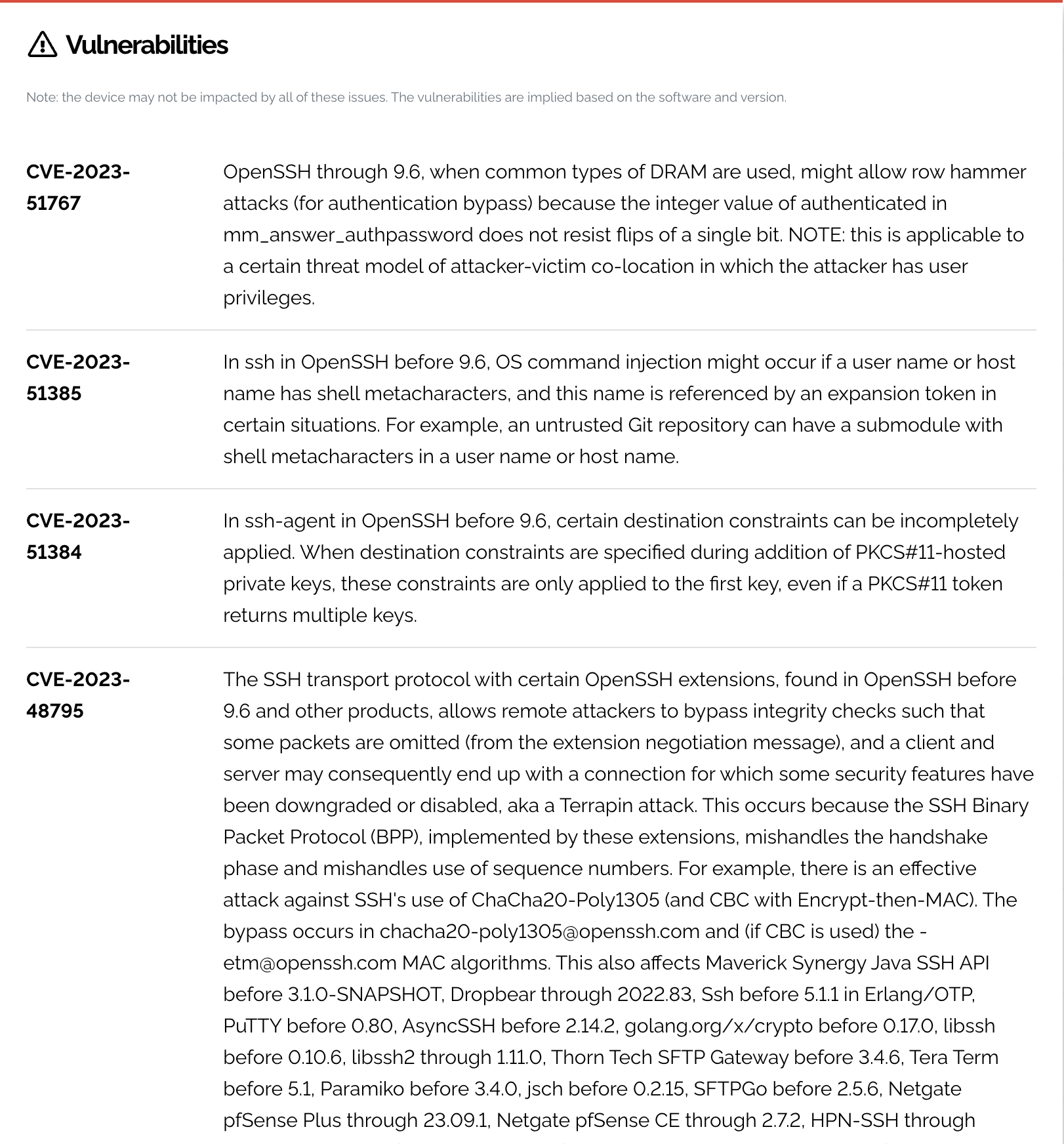


1. SSH default at port 22, so use the query “org:"Pfizer" port:22” to check the version of OpenSSH.

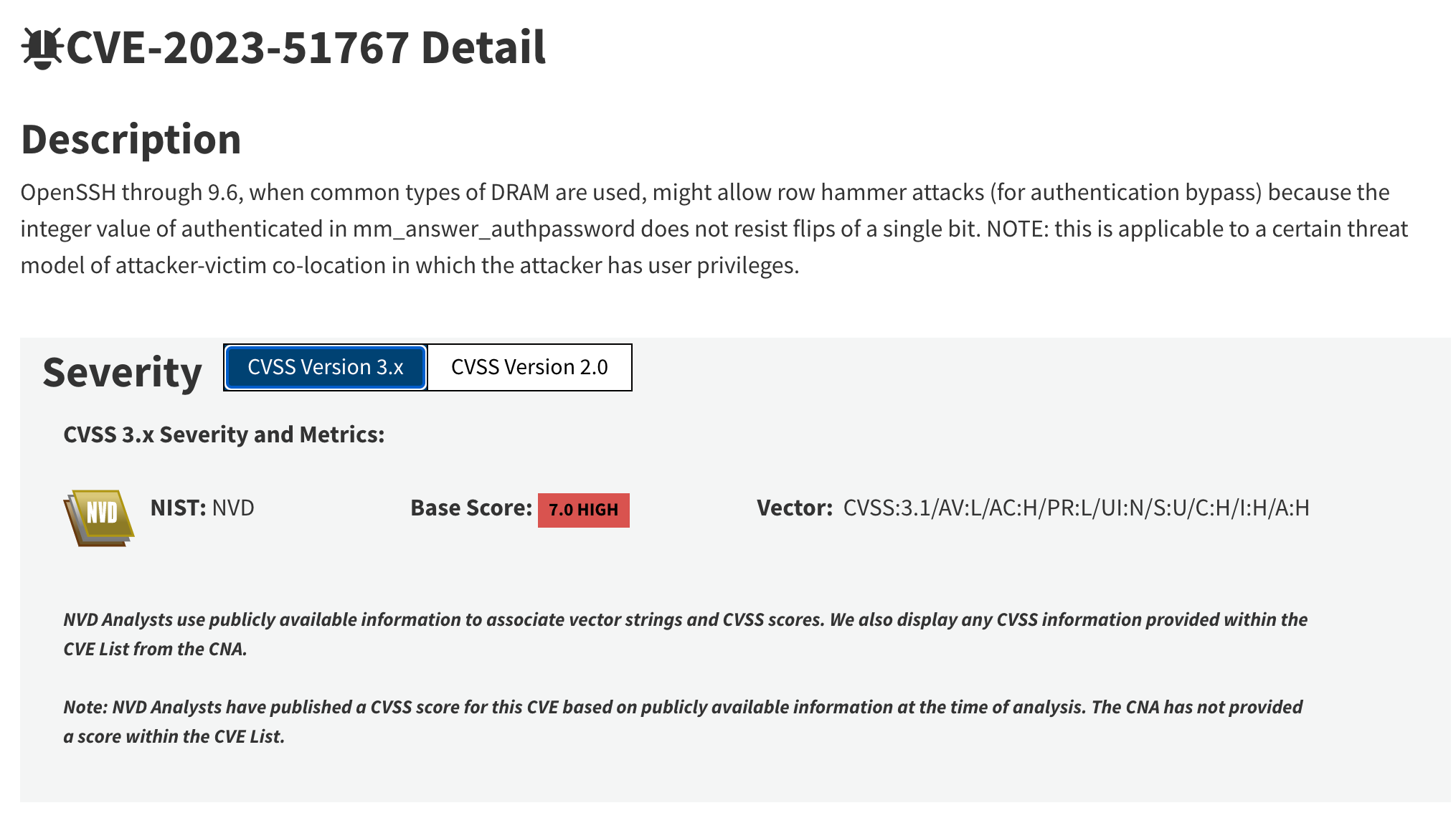
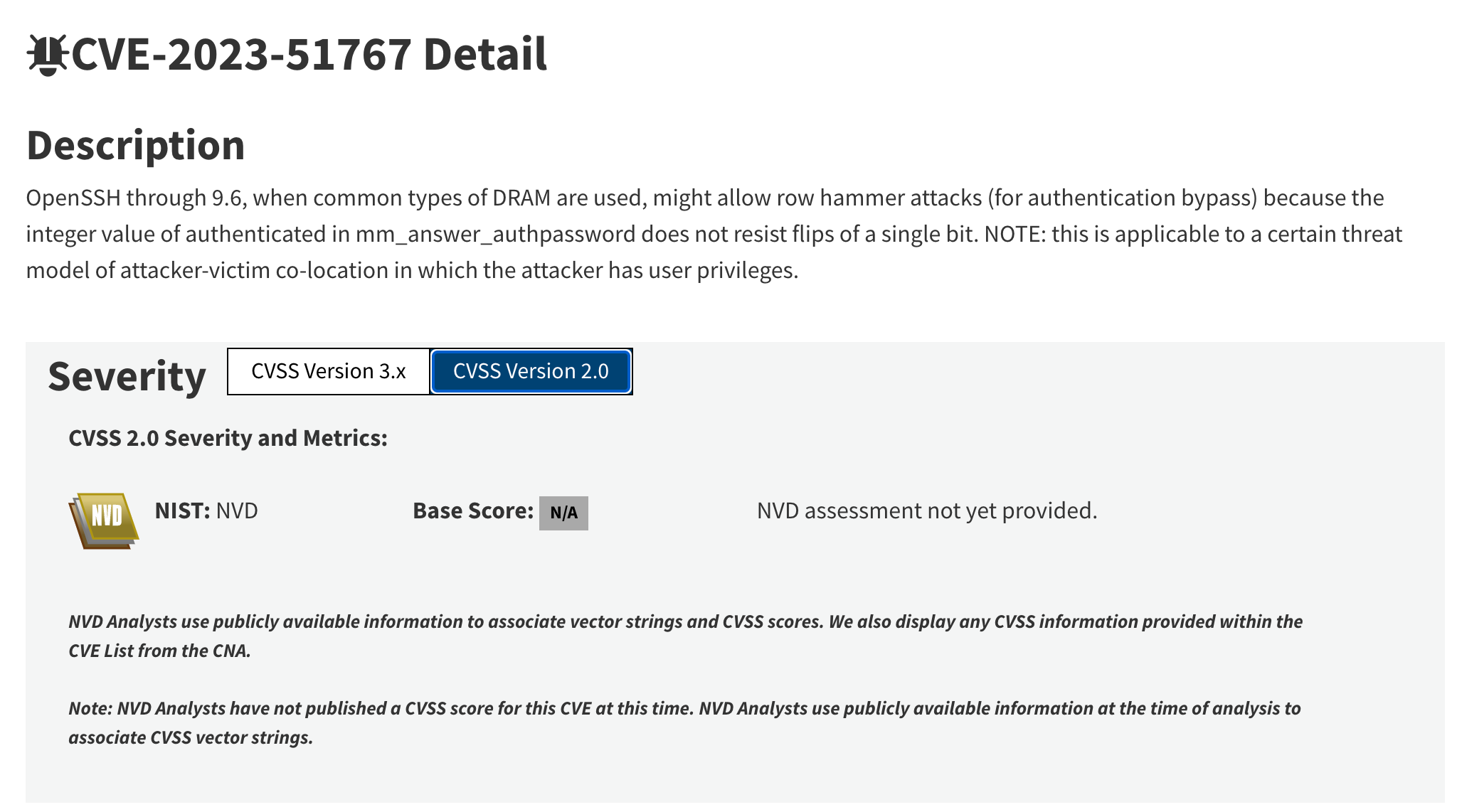
A screenshot of a computer

Description automatically generated

1. By click on the IP address, the vulnerabilities show below.



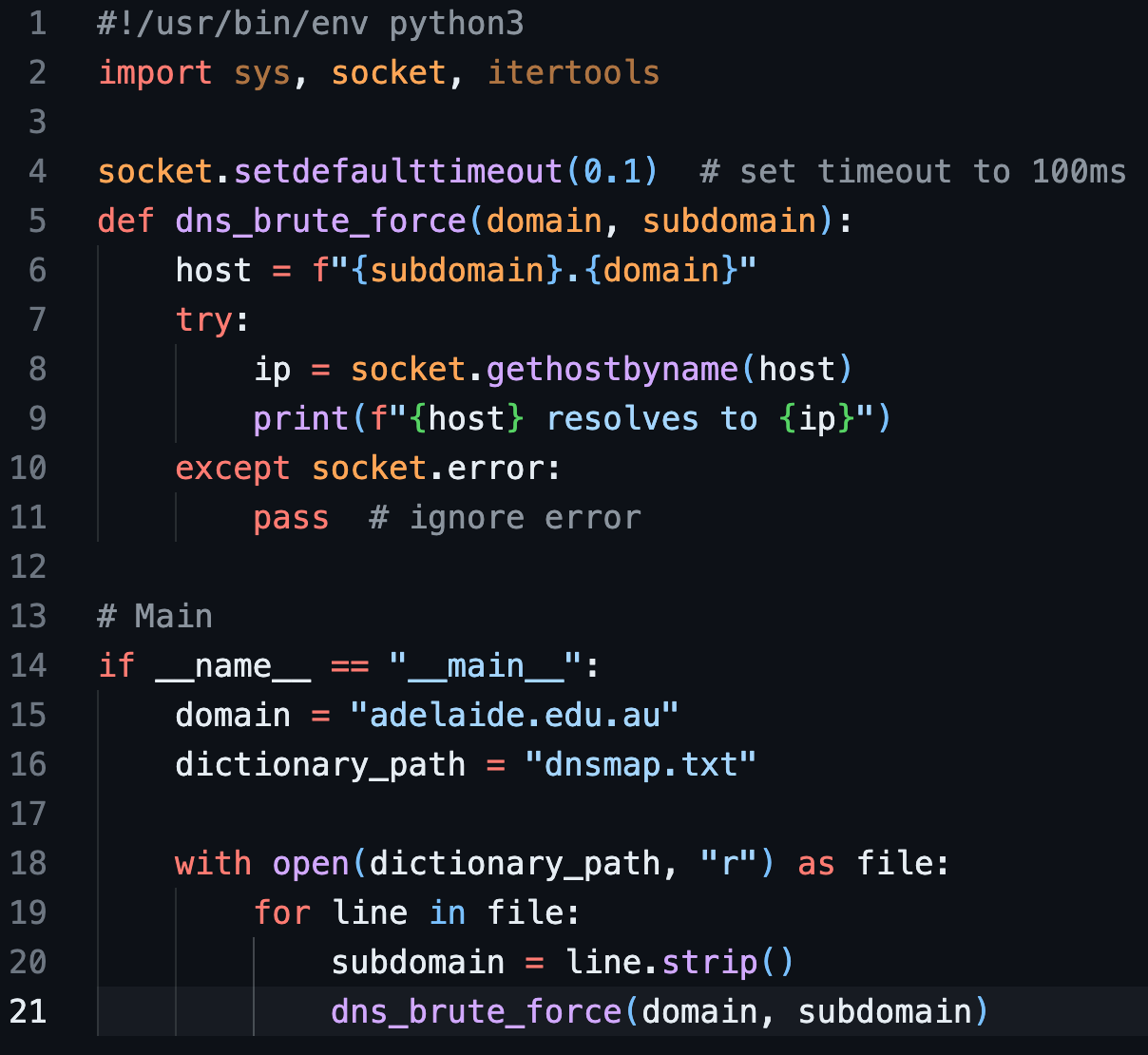
1. Just search the CVE on the website and get the CVSS string below:

1. (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](https://myuni.adelaide.edu.au/courses/95262/files/14689596?wrap=1)[Download this dictionary file](https://myuni.adelaide.edu.au/courses/95262/files/14689596/download?download_frd=1) (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

Script:



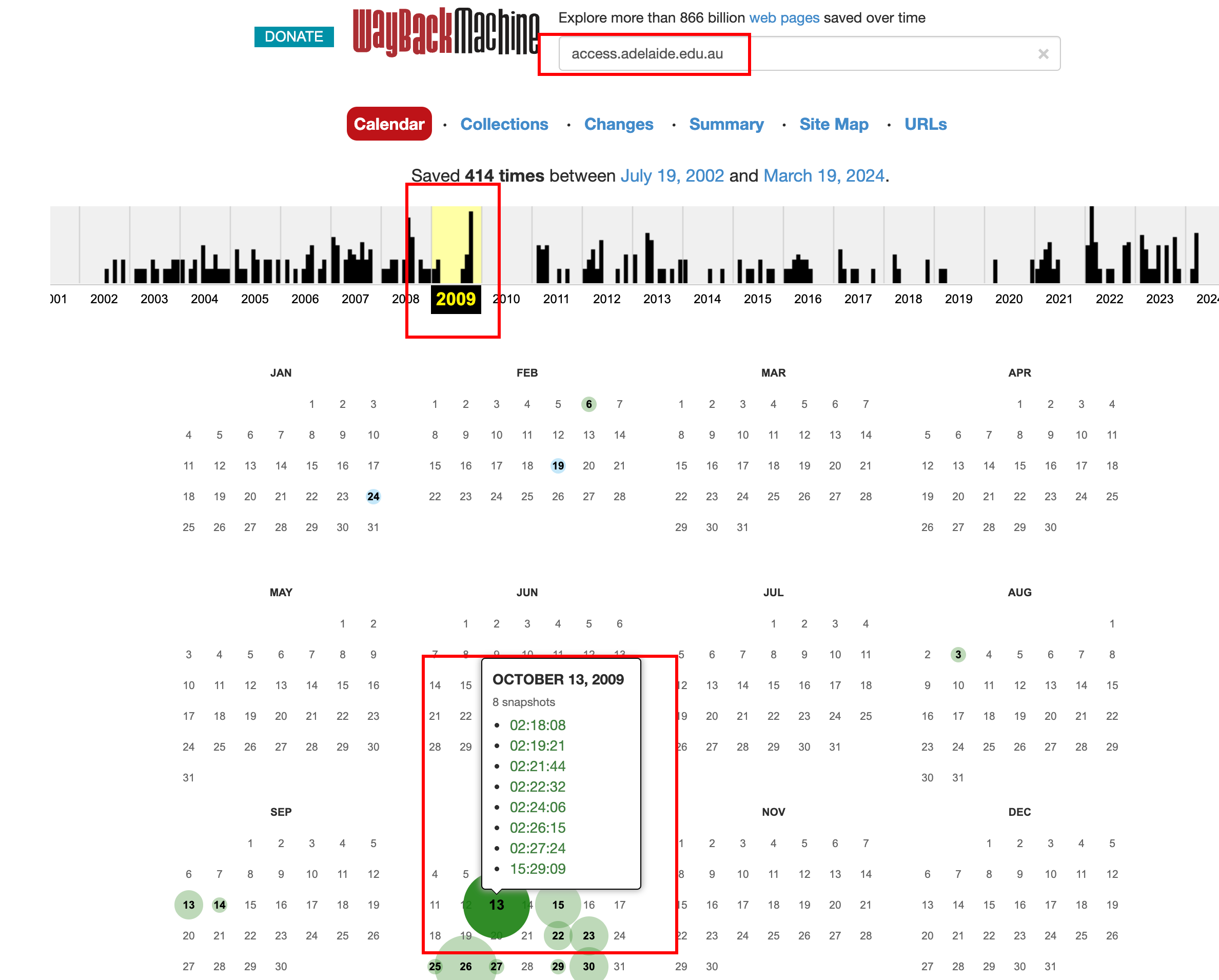
Result: (run with no result on my computer so tried on my own server)

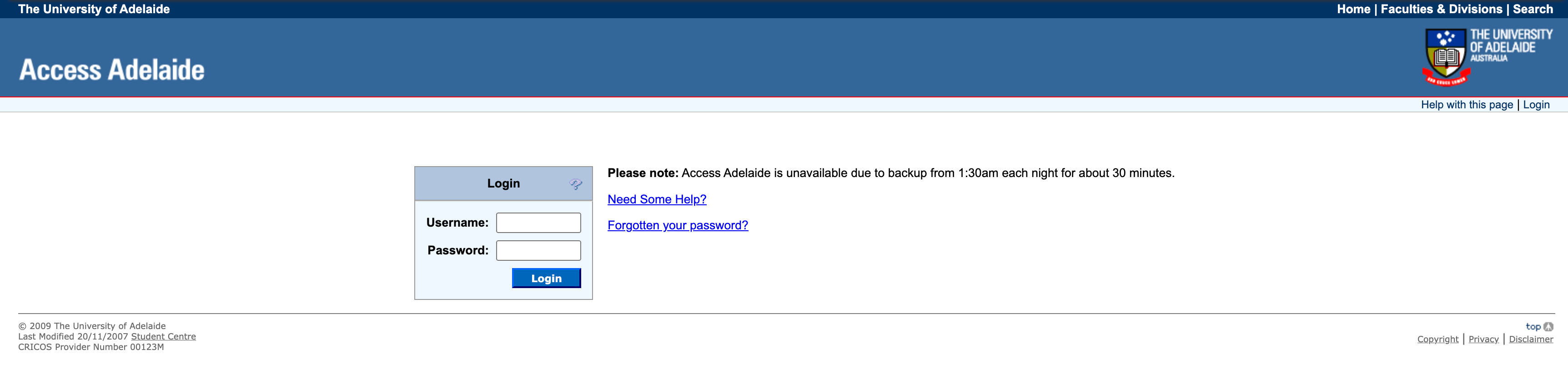


1. (1 point) Use the Wayback Machine to find out how Access Adelaide (access.adelaide.edu.au) looked like 10 years ago, in 2009. How does it look compared to the current Access Adelaide?

After I opened the Wayback Machine website, type the Access Adelaide website into the search box, then got a timeline. I chose the year 2009 and randomly chose a date to see the archive of the website in 2009.

Access Adelaide website 10 years ago is similar to nowadays.



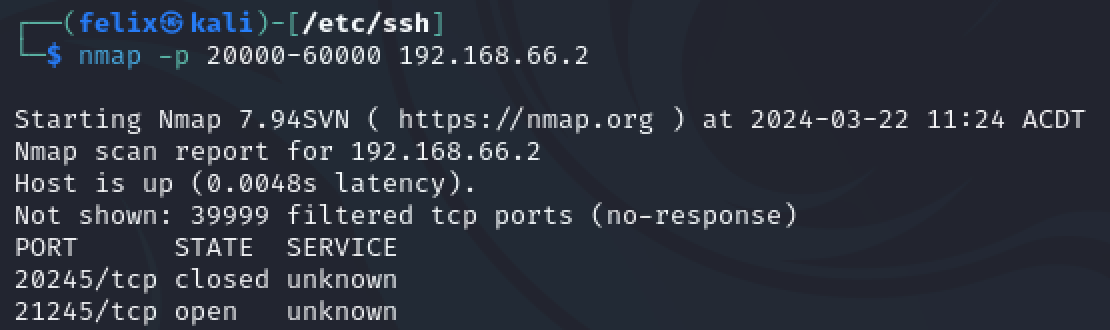


8.  (1 point) There is a network service running on the Hacklab VM behind a port somewhere between 20000 and 60000.

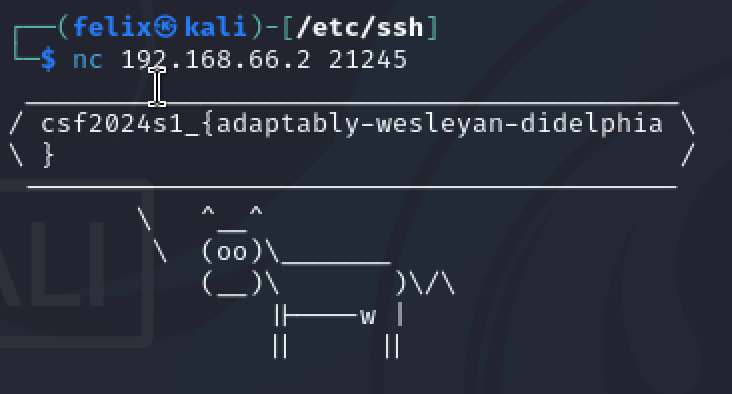
      a. Identify the port number and connect to it using netcat (“nc” or “netcat” command) to retrieve the secret.

Command: “nmap -p 20000-60000 192.168.66.2”, then “nc 192.168.66.2 21245”

Code: csf2024s1\_{adaptably-wesleyan-didelphia}



      b. Paste a screenshot showing the secret answer.



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

First, using “nmap” command to scan the port from 20000 to 60000 by using parameter “-p 20000-60000” and the HackLab’s ip address “192.168.66.2”.

Then, after waiting for a while, I got two answers, the first is port 20245 which is closed, and the second one is port **21245** which is opened.

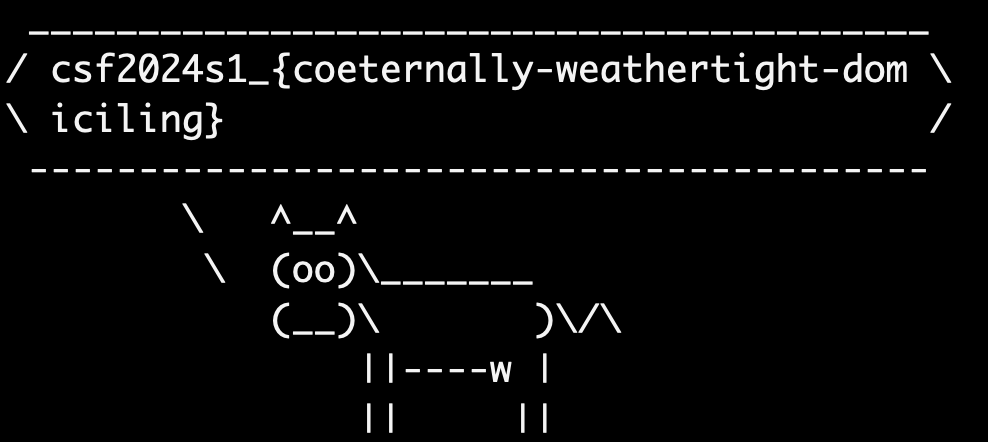
Finally, using the “nc” command connecting to port “21245” of ip address “192.168.66.2”.

 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.

A screen shot of a computer

Description automatically generated

     b. Paste a screenshot showing the secret answer.



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

Firstly, the question said to send a series of SYN packets to these 3 ports: 2201, 2211, 2234, I choose to use command “nmap” with the parameter “-sS” to send the SYN packets to those port, then, use the command “netcat” mentioned in question “a)” to get the secret answer.