

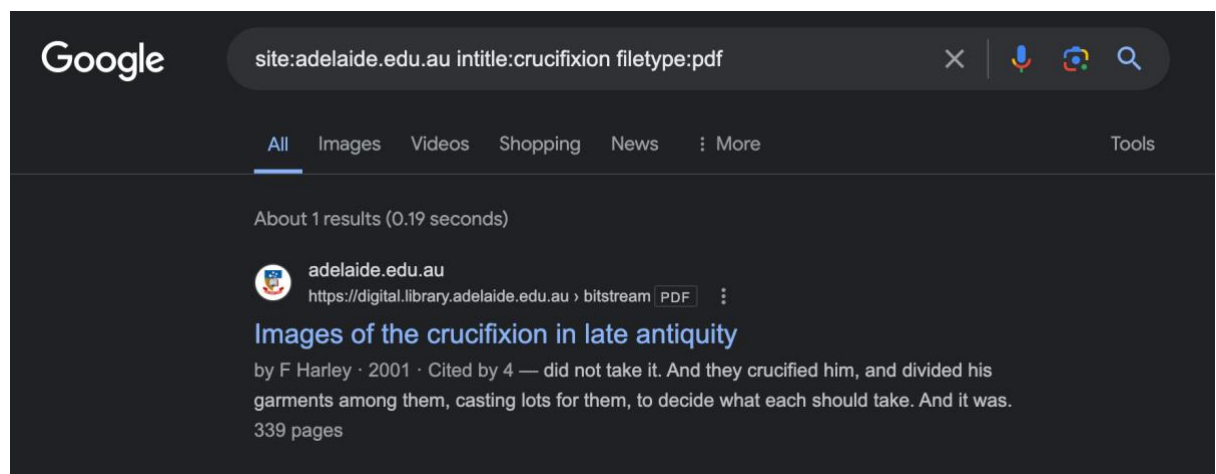
Assignment 0x02 - OSINT, Recon & Network Scanning

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?

(a) site:adelaide.edu.au intitle:crucifixion filetype:pdf

(b) Felicity Harley



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.

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 succeeded.

Documentation

CVEdetails.com
powered by SecurityScorecard

- Vulnerabilities
 - By Date
 - By Type
 - Known Exploited
 - Assigners
 - CVSS Scores
 - EPSS Scores
 - Search
- Vulnerable Software
 - Vendors
 - Products
 - Version Search
- Vulnerability Intel.
 - Newsfeed
 - Open Source Vuls
 - Emerging CVEs
 - Feeds
 - Exploits
 - Advisories
 - Code Repositories
 - Code Changes
- Attack Surface
 - My Attack Surface
 - Digital Footprint
 - Discovered Products
 - Detected Vuls
 - IP Search
- Other
 - Metasploit Modules
 - Port Closures

Vulnerability Details : CVE-2008-2507

Cross-site scripting (XSS) vulnerability in Calcium40.pl in Brown Bear Software Calcium 3.10 and 4.0.4 allows remote attackers to inject arbitrary web script or HTML via the CalendarName parameter in a ShowIt action.

Published 2008-05-29 23:32:00 Updated 2018-10-11 20:41:45 Source MITRE [View at NVD](#), [CVE.org](#)

Vulnerability category: Cross site scripting (XSS)

Exploit prediction scoring system (EPSS) score for CVE-2008-2507

Probability of exploitation activity in the next 30 days: **0.19%**

Percentile, the proportion of vulnerabilities that are scored at or less: **55%** [EPSS Score History](#) [EPSS FAQ](#)

CVSS scores for CVE-2008-2507

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
4.3	MEDIUM	AVN/AC:M/Au/N/CN/PP/AN	5.8	2.5	NIST

CWE ids for CVE-2008-2507

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
Assigned by: nvd@nist.gov (Primary)

References for CVE-2008-2507

- <http://www.securityfocus.com/bid/29411> Exploit
- <https://exchange.xforce.ibmcloud.com/vulnerabilities/42704>
- <http://www.securityfocus.com/archive/1/492719/100/0/threaded>

[All](#) [Shopping](#) [Images](#) [Videos](#) [Maps](#) [More](#) [Tools](#)

About 115,000 results (0.26 seconds)

Larimer County Search and Rescue
<https://www.larimercountysar.org> > cgi-bin > Calcium40

Calcium
Calcium Web Calendar - Brown Bear Software <http://www.brownbearsw.com>.

87.106.36
<http://87.106.36.176> > Pfarrkalender > Calcium40

Calcium
Links to Existing Calendars. Name, Description, Administer. Pfarrkalender_Christen_am_Rhein, Pfarrkalender_Christen_am_Rhein. Calcium 4.0.4 Demo

Cambria County, PA (.gov)
<http://employees.cambriacountypa.gov> > Calcium40

Calcium
Name, Description, Administer. Group: CPC_Building. Room_Schedule, Schedule for rooms on the 2nd floor. Calcium 4.0.4 Professional Unlimited w/Email

Not Secure [http://87.106.36.176/cgi-bin/Pfarrkalender/Calcium40.pl?Op=ShowIt&CalendarName=<script>alert\(1\)</script>](http://87.106.36.176/cgi-bin/Pfarrkalender/Calcium40.pl?Op=ShowIt&CalendarName=<script>alert(1)</script>) ☆

87.106.36.176 says
1

3. (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

```
[recon-ng][Assi2][whois_pocs] > db query select * from contacts where region = "Carson, CA"

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| first_name | middle_name | last_name | email | title | region | country | phone | notes | module |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Robert | | Nordland | x@x.com | Whois contact | Carson, CA | United States | | | whois_pocs |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

[*] 1 rows returned
```

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.

4. (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.

```

(felix@kali)-[~]
└─$ dig dunstan.org.au

; <<> DiG 9.19.21-1-Debian <<> dunstan.org.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36962
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dunstan.org.au.                IN      A

;; ANSWER SECTION:
dunstan.org.au.                1040    IN      A      151.101.194.159

;; Query time: 4 msec
;; SERVER: 192.168.66.1#53(192.168.66.1) (UDP)
;; WHEN: Thu Mar 14 20:10:05 ACDT 2024
;; MSG SIZE rcvd: 59

```

2) Can not find related domain.

```

(felix@kali)-[~]
└─$ dig -x 151.101.194.159

; <<> DiG 9.19.21-1-Debian <<> -x 151.101.194.159
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47486
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;159.194.101.151.in-addr.arpa.  IN      PTR

;; AUTHORITY SECTION:
151.in-addr.arpa.              1713    IN      SOA      pri.authdns.ripe.net. dns.ripe.net. 1710372718 3600 600 864000 3600

;; Query time: 7 msec
;; SERVER: 192.168.66.1#53(192.168.66.1) (UDP)
;; WHEN: Thu Mar 14 20:26:26 ACDT 2024
;; MSG SIZE rcvd: 117

```

3) Organization name is Fastly, Inc.

```

(felix@kali)-[~]
└─$ whois 151.101.194.159

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:      151.101.0.0 - 151.101.255.255
CIDR:          151.101.0.0/16
NetName:       SKYCA-3
NetHandle:     NET-151-101-0-0-1
Parent:        RIPE-ERX-151 (NET-151-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization:  Fastly, Inc. (SKYCA-3)
RegDate:       2016-02-01
Updated:       2021-12-14
Ref:           https://rdap.arin.net/registry/ip/151.101.0.0

OrgName:       Fastly, Inc.
OrgId:         SKYCA-3
Address:       PO Box 78266
City:          San Francisco
StateProv:     CA
PostalCode:    94107
Country:       US
RegDate:       2011-09-16
Updated:       2022-11-16
Ref:           https://rdap.arin.net/registry/entity/SKYCA-3

```

- 4) IP address range is: 151.101.0.0 - 151.101.255.255

```

(felix@kali)-[~]
└─$ whois 151.101.194.159

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

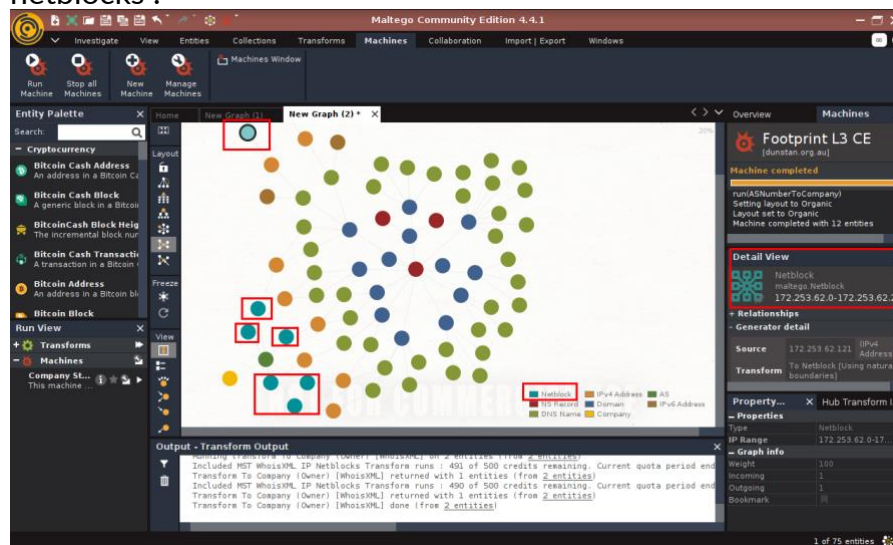
NetRange:      151.101.0.0 - 151.101.255.255
CIDR:          151.101.0.0/16
NetName:       SKYCA-3

```

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

RECORDS	
Hierarchical analysis of the entity	
151.101.194.159	whois Fastly (SKYCA-3)
route 151.101.192.0/22	
bgp AS54113	
asname Fastly Fastly, Inc.	
descr Fastly	
location San Francisco, United States	

6) By following the instruction of “Maltego” in workshop2 to find other netblocks .



5. (2 points) Create a free account on shodan.io (<https://shodan.io>Links 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 [here](#)Links 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?	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

	<p>CVE-2023-48795</p> <p>CVE-2023-38408</p> <p>...</p>
<p>Choose the most recent vulnerability from above, and find the CVSS2.0 string for it by looking it up on nvd.nist.gov.</p>	<p>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”</p>

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

The screenshot shows Shodan search results for the query "org:”Pfizer” port:443". The search bar at the top contains the query. Below the search bar, there are two main results displayed side-by-side.

Result 1: 148.168.33.93

- IP: 148.168.33.93
- Location: United States, New York City
- SSL Certificate:
 - Issued By: Pfizer Basic Assurance CA G2
 - Issued To: gro-aruba-m3-03
 - Organization: Pfizer
 - Supported SSL Versions: TLSv1.2
 - Diffie-Hellman Fingerprint: mod_ssl 2.2.x/Hardcoded 1024-bit prime
- HTTP/1.1 302 Temporarily Moved
 - Date: Thu, 14 Mar 2024 10:28:52 GMT
 - Server: Apache
 - X-Frame-Options: SAMEORIGIN
 - X-UA-Compatible: IE=edge;IE=11;IE=10;IE=9
 - Location: https://148.168.33.93:4343/
 - Content-Length: 0
 - Content-Type: text/html

Result 2: 404 Not Found

- IP: 148.168.82.24
- Location: United States, Sunnyside
- SSL Certificate:
 - Issued By: Entrust Certification Authority - L1K
 - Issued To: chatterbox pfizer.com
 - Organization: Entrust, Inc.
- HTTP/1.1 404 Not Found
 - Date: Thu, 14 Mar 2024 10:27:31 GMT
 - Server: nginx
 - Content-Type: text/html
 - Content-Length: 548
 - Connection: keep-alive
 - Set-Cookie: QrpP-TbsizqcX1QTr0+ttHGFGQ__=v1wMieKw__adE; Expires=...

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

The screenshot shows Shodan search results for the query "org:”Pfizer” port:22". The search bar at the top contains the query. Below the search bar, there is one main result displayed.

Result: 148.168.82.87

- IP: 148.168.82.87
- Location: United States, Sunnyside
- SSH-2.0-OpenSSH_7.4
 - Key type: ssh-rsa
 - Key: AAAAB3NzaC1yc2EAAAABIwAAQEAxN78fPr6AG82CqfdxS/7BeePzXJ+Pk+rhduW77y8IsyXwe83hMm2q9n0eF2zzKfMNAj7nqKwePnZ+vbjR4kaYo5fTAgoI0KUZAew/Gfn/m/g1Rok+Axwac29ApbXVES4F3myttQvLwLps7x/mjq3ixQWe/SbH10VtoTFszvD23306mLwPxyx9v9gm7gyRRP1xscZewgmqQ0f8TerFmbDQ7WY4dGd...

- 3) By click on the IP address, the vulnerabilities show below.

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-51767	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.
CVE-2023-51385	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
CVE-2023-51384	In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.
CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGO before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through

4) Just search the CVE on the website and get the CVSS string below:


CVE-2023-51767 Detail

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.


CVE-2023-51767 Detail

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 2.0 Severity and Metrics:

 **NIST:** NVD **Base Score:** N/A NVD assessment not yet provided.

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 not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

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](#) Download 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
```

Script:

```
1  #!/usr/bin/env python3
2  import sys, socket, itertools
3
4  socket.setdefaulttimeout(0.1) # set timeout to 100ms
5  def dns_brute_force(domain, subdomain):
6      host = f"{subdomain}.{domain}"
7      try:
8          ip = socket.gethostbyname(host)
9          print(f"{host} resolves to {ip}")
10     except socket.error:
11         pass # ignore error
12
13 # Main
14 if __name__ == "__main__":
15     domain = "adelaide.edu.au"
16     dictionary_path = "dnsmap.txt"
17
18     with open(dictionary_path, "r") as file:
19         for line in file:
20             subdomain = line.strip()
21             dns_brute_force(domain, subdomain)
```

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

```
xio@instance-20240115-0610:~/temp$ python3 brute-force.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
```

7. (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.

Wayback Machine

Explore more than 866 billion web pages saved over time

access.adelaide.edu.au

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved 414 times between July 19, 2002 and March 19, 2024.

2009

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

OCTOBER 13, 2009

- 8 snapshots
- 02:18:08
- 02:19:21
- 02:21:44
- 02:22:32
- 02:24:06
- 02:26:15
- 02:27:24
- 15:29:09

The University of Adelaide

Access Adelaide

Home | Faculties & Divisions | Search

Help with this page | Login

Please note: Access Adelaide is unavailable due to backup from 1:30am each night for about 30 minutes.

Need Some Help?

Forgot your password?

© 2009 The University of Adelaide
Last modified: 2011/1/2007 Student Centre
CRICOS Provider Number 001234

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}

```
(felix@kali)-[/etc/ssh]
$ nmap -p 20000-60000 192.168.66.2

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 11:24 ACDT
Nmap scan report for 192.168.66.2
Host is up (0.0048s latency).
Not shown: 39999 filtered tcp ports (no-response)
PORT      STATE SERVICE
20245/tcp  closed unknown
21245/tcp  open  unknown
```

b. Paste a screenshot showing the secret answer.

```
(felix@kali)-[/etc/ssh]
$ nc 192.168.66.2 21245

/ csf2024s1_{adaptably-wesleyan-didelfhia } \
\ }

      ^ ^
      (oo)\_____
      ( _ )\_____)\\
      ||____w  ||
      ||      ||
```

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.

```

(felix@kali)-[~]
└─$ cat port_knock.sh
#!/bin/bash

# Target IP address
IP="192.168.66.2"

# Port knocking sequence
sudo nmap -sS $IP -p 2201
sudo nmap -sS $IP -p 2211
sudo nmap -sS $IP -p 2234

# Connect to the opened port using netcat
nc $IP 12345

```

b. Paste a screenshot showing the secret answer.

```

-----
/ csf2024s1_{coeternally-weather-tight-dom \
\ iciling} /
-----
      ^__^
      (oo)\_______
          (__)\       )\/\
              ||----w |
              ||     ||

```

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.