CYSE 450 - Introduction to Ethical Hacking & Penetration Testing

Assignment 2

(Total: 100 points)

Goal: This lab will introduce you to some basic ethical hacking tools and techniques.

Please submit the answers for all 6 questions in a word or pdf file on canvas.

Task 1 (50 points): Reconnaissance and Scanning

1.1. Your password is for sale!

Please visit the following website: •
https://haveibeenpwned.com/

This is a website which allows you to find password leaking information.
Please search your own email address if you used that email address to register online accounts.

Question 1 (20 points). **Visit https://haveibeenpwned.com/. Are you a victim of previous cyber breaches?**

1.2. Make good use of Google search.

You can use Google search to find many useful information about the target.

For example, hackers can find out the President of Old dominion University and his/her email address. Then hackers can send phishing emails to the President!

Question 2 (10 points). **Please use Google Search to find out any known person from any Technological University (e.g. ODU) and his/her email address.**

1.3. Get bulk email addresses for free.

You can get bulk email addresses for free from http://hunter.io
Hackers could misuse those email addresses by sending bulk phishing emails.

Question 3 (20 points). **Visit** http://hunter.io, **search for any domain of your choice and report a couple of email addresses you found. You may submit the screenshot as an alternative.**

Task 2 (50 points): Privilege Escalation with Vulnerabilities

2.1. Search vulnerability information!

Please visit the following websites to search vulnerability information for **CVE- 2017-0144:** •
exploit-db.com

- cve.mitre.org Use the keyword

2017-0144 for search.

Question 4 (10 points). **What is CVE in cybersecurity?**

Question 5 (20 points). **Visit http://exploit-db.com and http://cve.mitre.org, briefly explain what vulnerability CVE-2017-0144 is.**

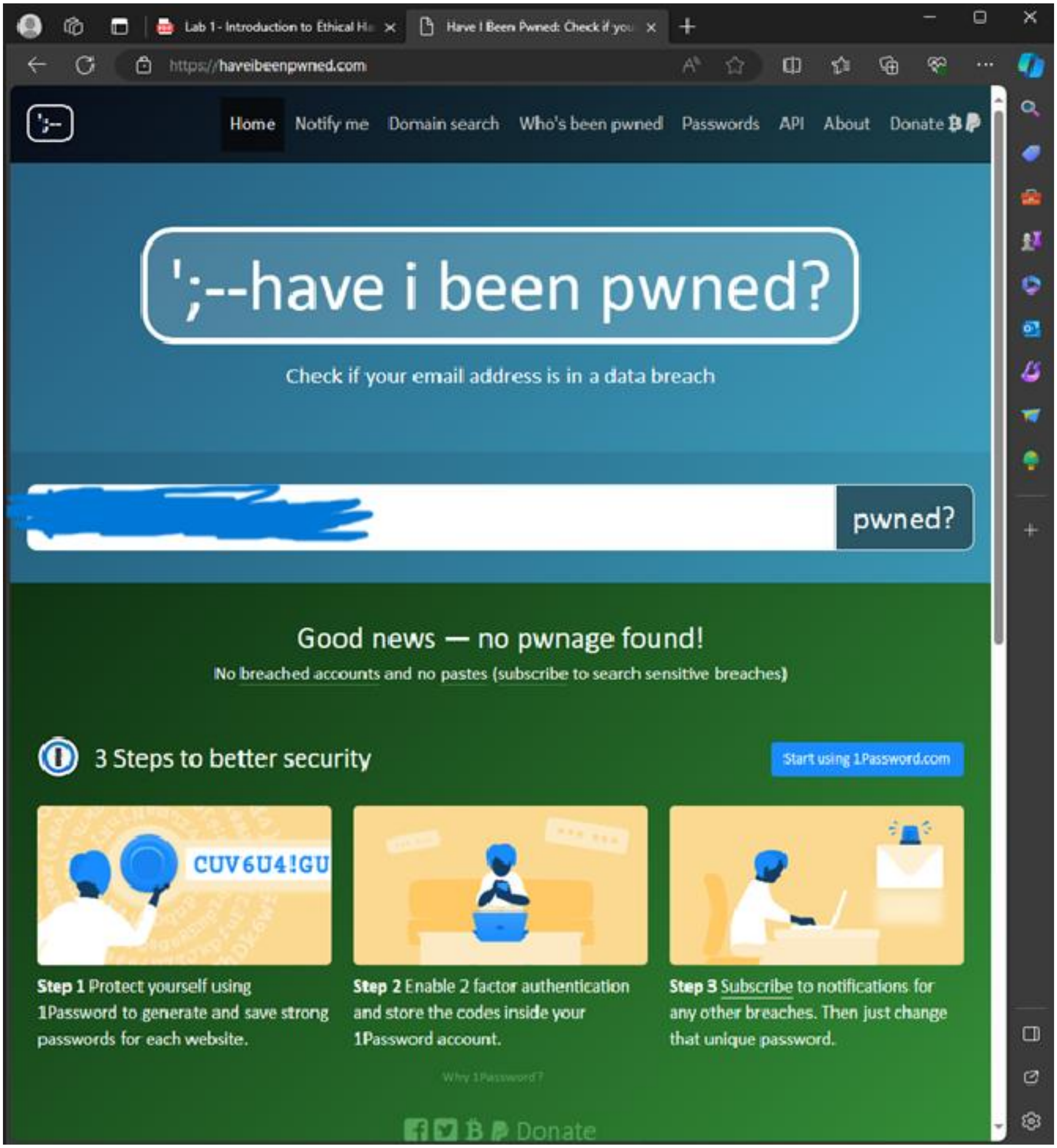
2.2. Search open web cameras!

Please visit the following websites to search open web cameras:

- shodan.io Use the keyword **Web**

Camera for search.

Question 6 (20 points). **Visit http://shodan.io. Do you find any open web cameras? Which countries do they come from? Give a couple of examples.**


Lab 1 - Introduction to Ethical Ha
Have I Been Pwned: Check if you
https://haveibeenpwned.com
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
pwned?
Start using 1Password.com
CUV6U4!GU
Why 1Password?
Donate

[redacted]

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

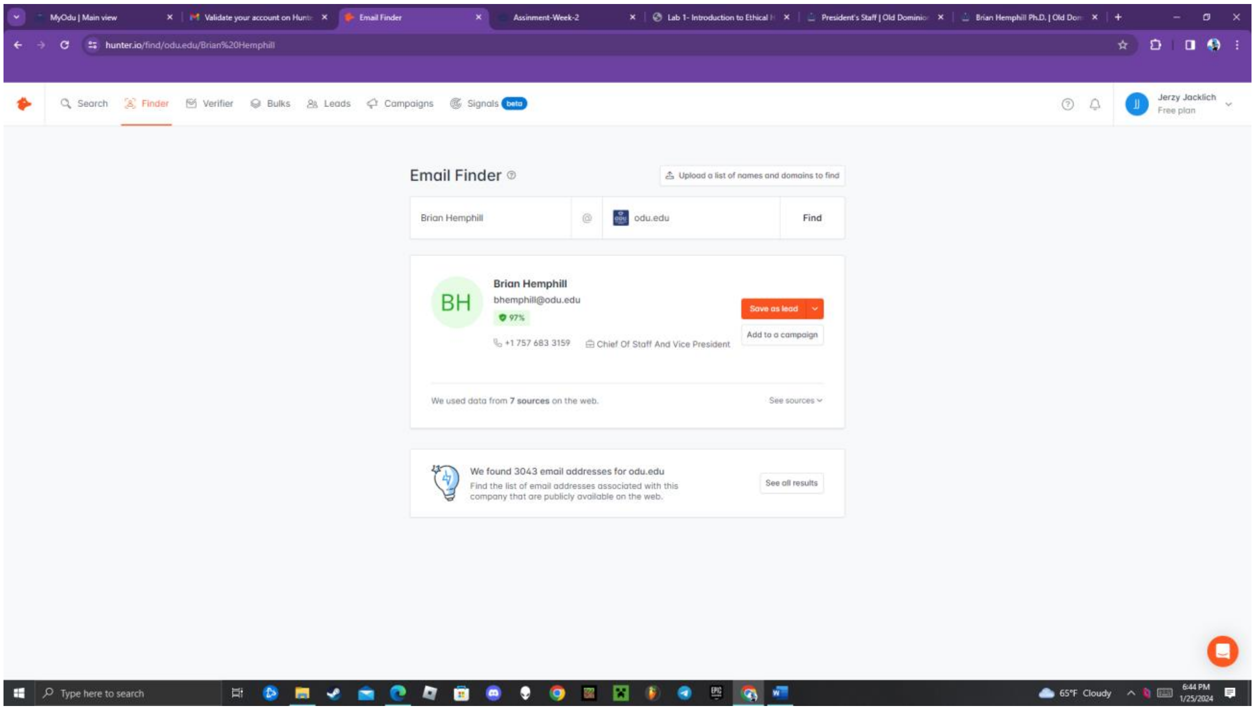
3 Steps to better security

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

1. I am not a victim of any of the cyber breaches known to haveibeenpwned.com

2. 

Email Finder

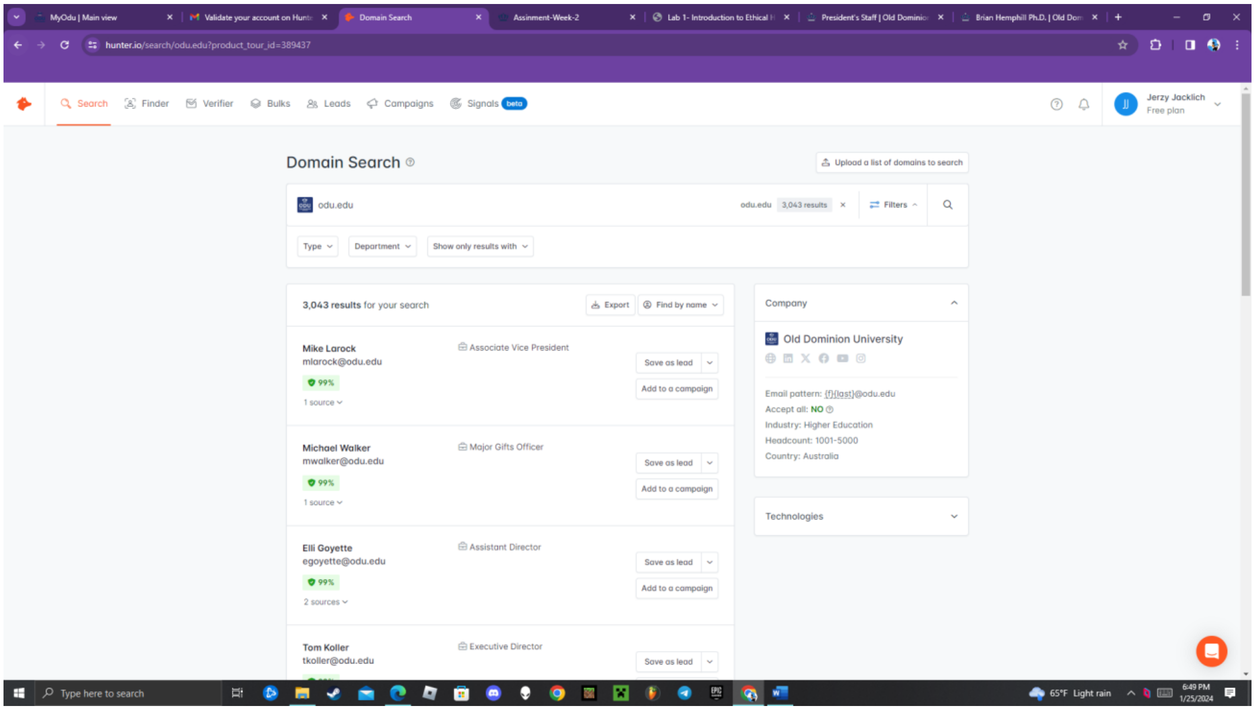
Brian Hemphill @ odu.edu

Brian Hemphill
bhemphill@odu.edu
97%
+1 757 683 3159
Chief Of Staff And Vice President

We used data from **7 sources** on the web.

We found 3043 email addresses for odu.edu
Find the list of email addresses associated with this company that are publicly available on the web.

I chose ODU's president, his email is bhemphill@odu.edu. I also found this address on the ODU website but I wanted to check multiple locations to see if I could find any others.

3. 

Domain Search

odu.edu

odu.edu 3,043 results

3,043 results for your search

Mike Larock
mlarock@odu.edu
99%
1 source
Associate Vice President

Michael Walker
mwalker@odu.edu
99%
1 source
Major Gifts Officer

Elli Goyette
egoyette@odu.edu
99%
2 sources
Assistant Director

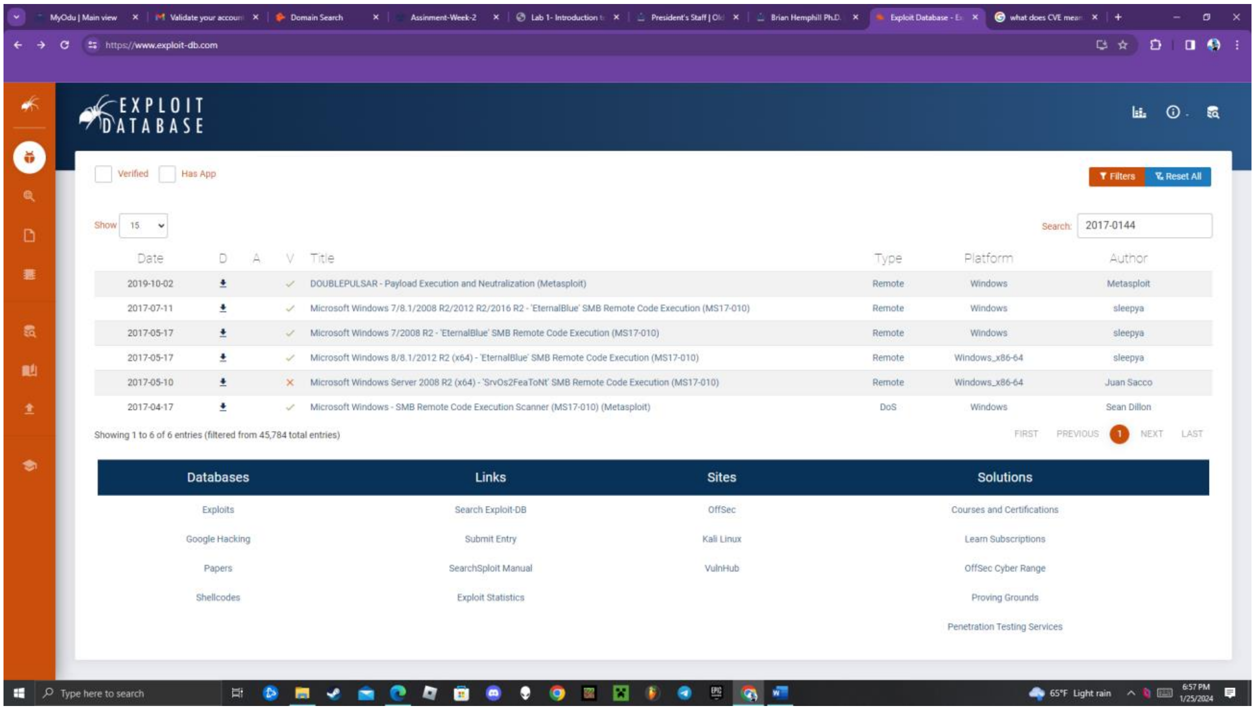
Tom Koller
tkoller@odu.edu
Executive Director

Old Dominion University

Email pattern: {f}{last}@odu.edu
Accept all: NO
Industry: Higher Education
Headcount: 1001-5000
Country: Australia

Some of the emails I found include mlarock@odu.edu, mwalker@odu.edu, egoyette@odu.edu, and tkoller@odu.edu.

4.



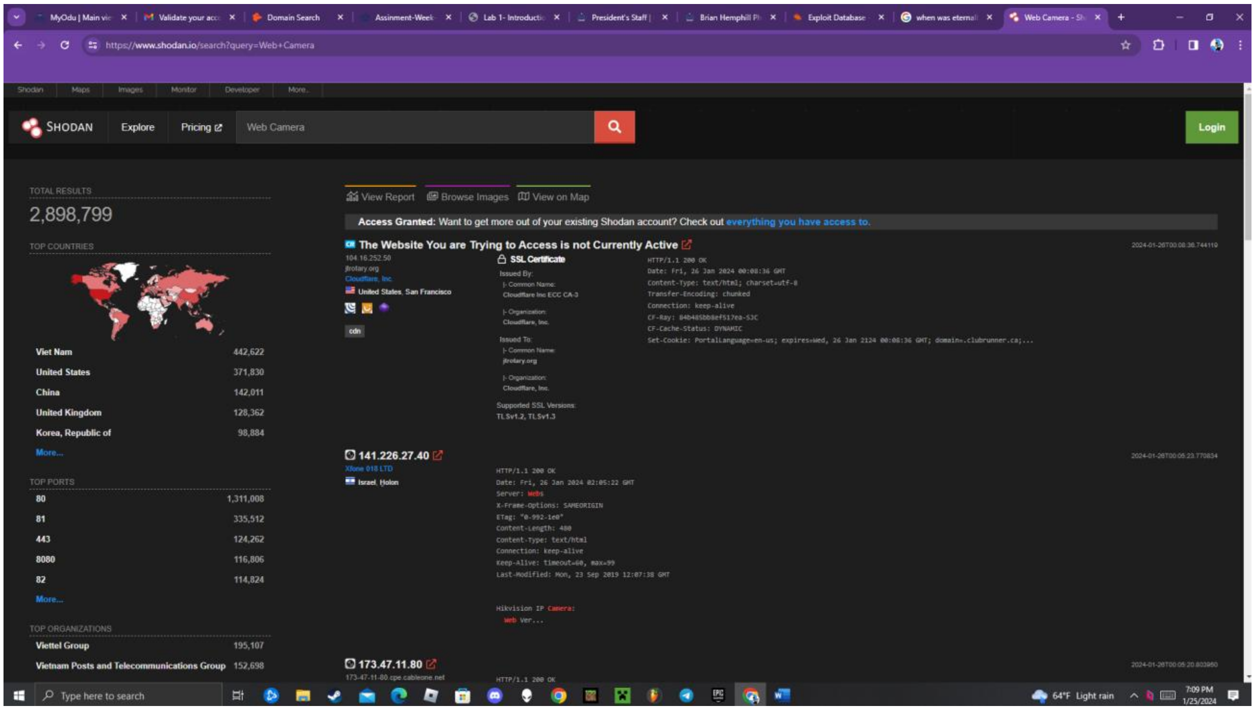
Date	D	A	V	Title	Type	Platform	Author
2019-10-02	⬇		✓	DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit)	Remote	Windows	Metasploit
2017-07-11	⬇		✓	Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows	sleepya
2017-05-17	⬇		✓	Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	sleepya
2017-05-10	⬇		✗	Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	Remote	Windows_x86-64	Juan Sacco
2017-04-17	⬇		✓	Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	DoS	Windows	Sean Dillon

Showing 1 to 6 of 6 entries (filtered from 45,784 total entries)

CVE means "Common Vulnerabilities and Exposures" and is essentially just noting that an exploit is part of this glossary of exploits. For example, CVE- 2017-0144.

5. CVE-2017-0144, otherwise known as eternalblue, is a remote code execution vulnerability that was found in 2017. It exploited a server message block vulnerability and would allow an attacker to run code remotely.

6.



TOTAL RESULTS

2,898,799

TOP COUNTRIES

Viet Nam	442,622
United States	371,830
China	142,011
United Kingdom	128,362
Korea, Republic of	98,884
More...	

TOP PORTS

80	1,311,008
81	335,512
443	124,262
8080	116,806
82	114,824
More...	

TOP ORGANIZATIONS

Viettel Group	195,107
Vietnam Posts and Telecommunications Group	152,698

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

The Website You are Trying to Access is not Currently Active 2024-01-26T00:08:36.744119

104.16.252.50
jlrotary.org
Cloudflare, Inc.
United States, San Francisco
cdn

SSL Certificate
Issued By:
|- Common Name:
Cloudflare Inc ECC CA-3
|- Organization:
Cloudflare, Inc.
Issued To:
|- Common Name:
jlrotary.org
|- Organization:
Cloudflare, Inc.
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Fri, 26 Jan 2024 00:08:36 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
CF-Ray: 84b485bb8ef517ea-SJC
CF-Cache-Status: DYNAMIC
Set-Cookie: PortalLanguage=en-us; expires=Wed, 26 Jan 2124 00:08:36 GMT; domain=.clubrunner.ca;...
```

141.226.27.40 2024-01-26T00:05:23.770834

Xfone 018 LTD
Israel, Holon

```
HTTP/1.1 200 OK
Date: Fri, 26 Jan 2024 02:05:22 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN
ETag: "0-992-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Mon, 23 Sep 2019 12:07:38 GMT


Hikvision IP Camera:
 Web Ver...
```

173.47.11.80 2024-01-26T00:05:20.803950

173-47-11-80.cpe.cableone.net

```
HTTP/1.1 200 OK
```

There are several hundred thousand web cameras open currently. They come from Vietnam, the US, China, Korea, etc. There is an open camera from Israel with an IP address of 141.226.27.40 and a webcam from Twin Falls in the US with an IP address of 173.47.11.80. There are many more examples but those are two for the purpose of this assignment.