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?**

I was a victim of a previous cyber breach. In May 2019, and massive SMS spam operation know as "ApexSMS" leaked over 80 million records of email address, along with names, phone numbers, and IP addresses.

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!

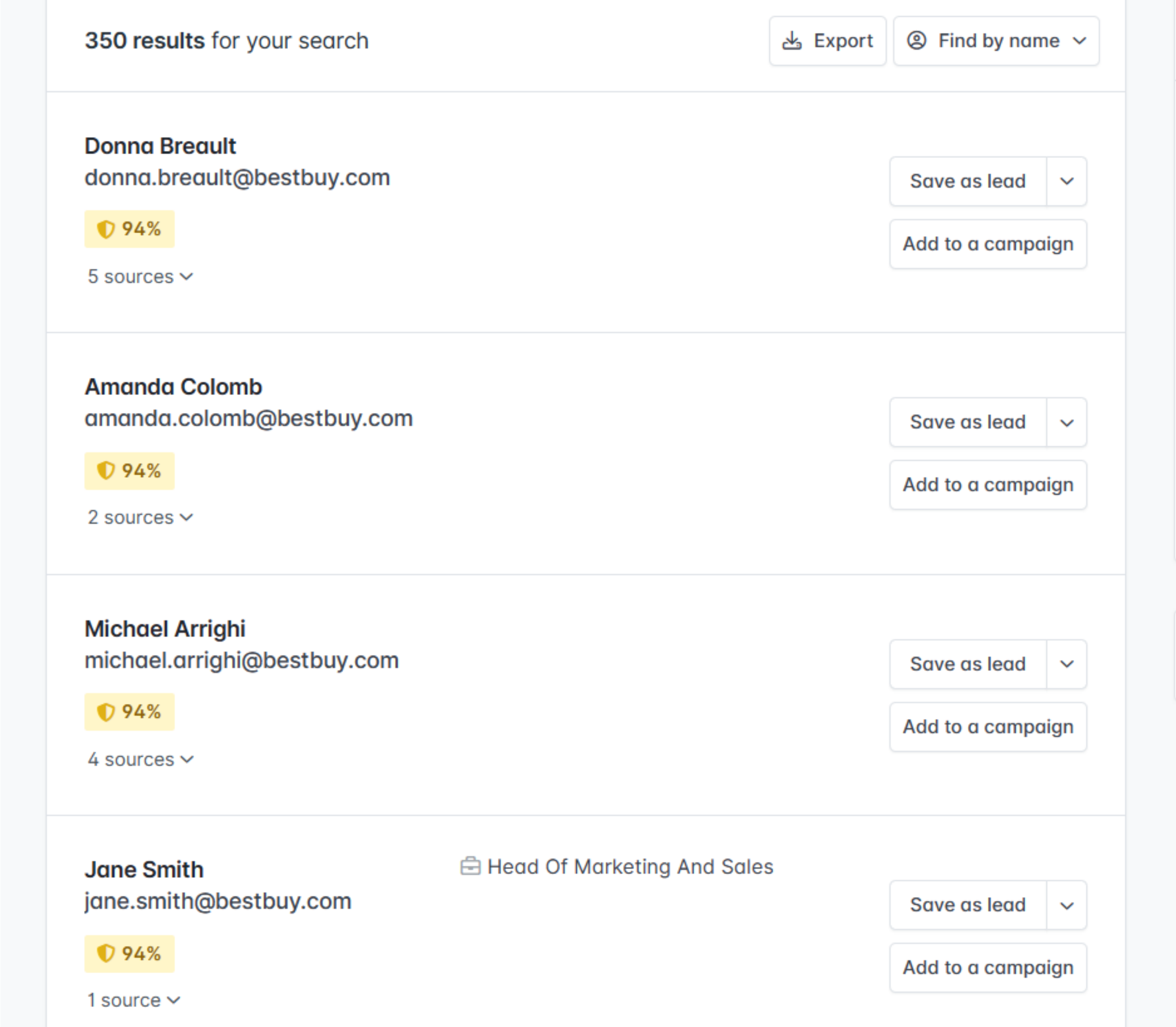
Question 2 (10 points). **Please use Google Search to find out any known person from any Technological University (e.g. ODU) and his/her email address.**

I found Stephanie Jenelle who is the associate vice president for budget & Financial Planning
Email Address: sjennelle@odu.edu

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.**



350 results for your search

Donna Breault
donna.breault@bestbuy.com
94%
5 sources

Amanda Colomb
amanda.colomb@bestbuy.com
94%
2 sources

Michael Arrighi
michael.arrighi@bestbuy.com
94%
4 sources

Jane Smith — Head Of Marketing And Sales
jane.smith@bestbuy.com
94%
1 source

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?

CVE stands for common vulnerabilities and Exposures. It is a glossary that classifies vulnerabilities.

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

The SMBv1 server in Microsoft Vista SP2, Windows Server 2008 SP2, Windows 8.1, Windows Server 2012 Gold, and Windows 10 Gold allowed remote attackers to execute malicious code by crafted packets (Windows SMB Remote Code Execution Vulnerability).

2.2. Search open web cameras!

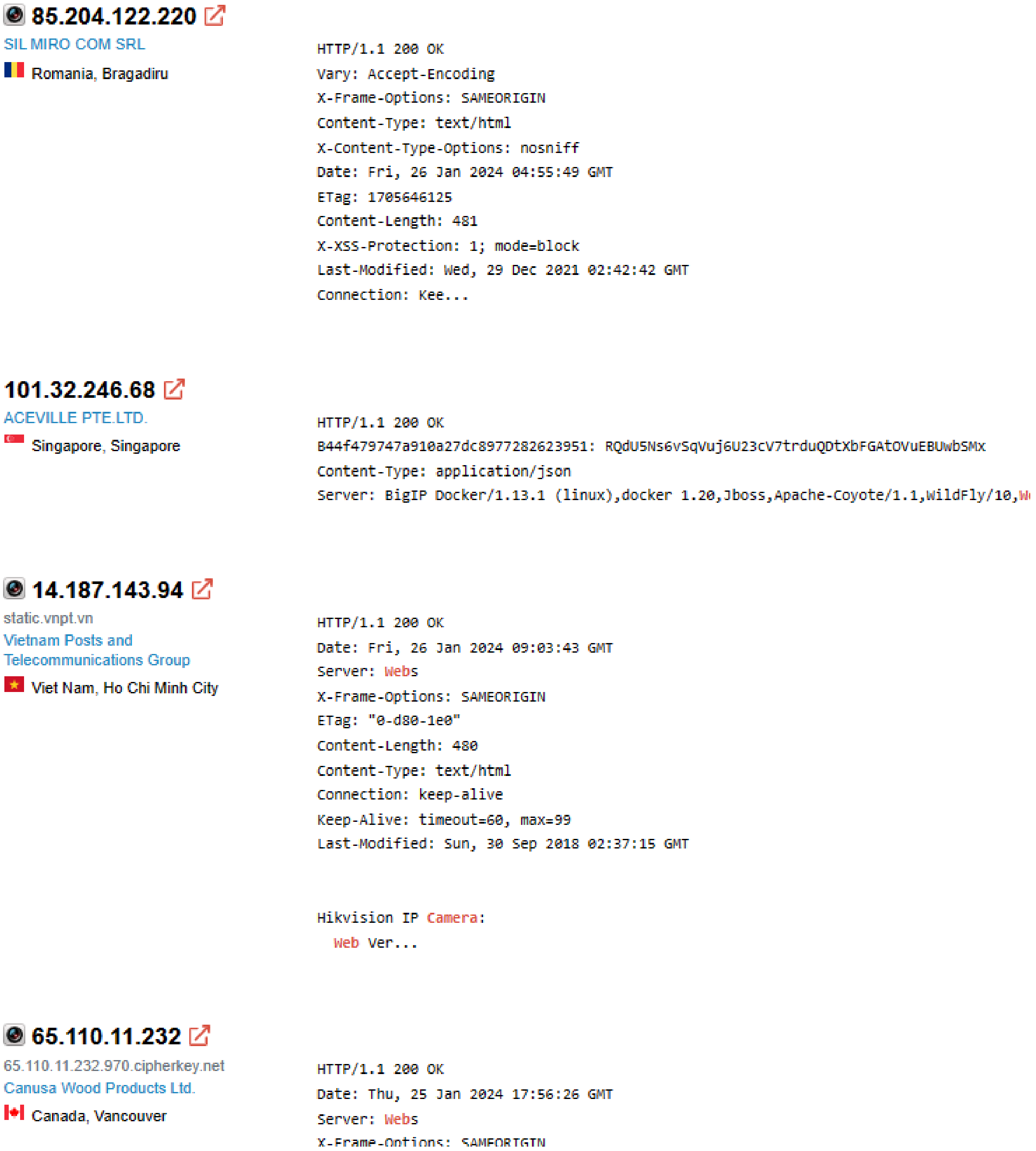
Please visit the following websites to search open web cameras**:**

- 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.

I did find open web cameras. In terms of which country they came from I got some from Romania, Singapore, Vietnam, Mexico, and Canada.



85.204.122.220

SIL MIRO COM SRL

Romania, Bragadiru

```
HTTP/1.1 200 OK
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
X-Content-Type-Options: nosniff
Date: Fri, 26 Jan 2024 04:55:49 GMT
ETag: 1705646125
Content-Length: 481
X-XSS-Protection: 1; mode=block
Last-Modified: Wed, 29 Dec 2021 02:42:42 GMT
Connection: Kee...
```

101.32.246.68

ACEVILLE PTE.LTD.

Singapore, Singapore

```
HTTP/1.1 200 OK
B44f479747a910a27dc8977282623951: RQdU5Ns6vSqVuj6U23cV7trduQDtXbFGAtOVuEBUwbSMx
Content-Type: application/json
Server: BigIP Docker/1.13.1 (linux),docker 1.20,Jboss,Apache-Coyote/1.1,WildFly/10,W
```

14.187.143.94

static.vnpt.vn

Vietnam Posts and Telecommunications Group

Viet Nam, Ho Chi Minh City

```
HTTP/1.1 200 OK
Date: Fri, 26 Jan 2024 09:03:43 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN
ETag: "0-d80-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
Last-Modified: Sun, 30 Sep 2018 02:37:15 GMT


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

65.110.11.232

65.110.11.232.970.cipherkey.net

Canusa Wood Products Ltd.

Canada, Vancouver

```
HTTP/1.1 200 OK
Date: Thu, 25 Jan 2024 17:56:26 GMT
Server: Webs
X-Frame-Options: SAMEORIGIN
```