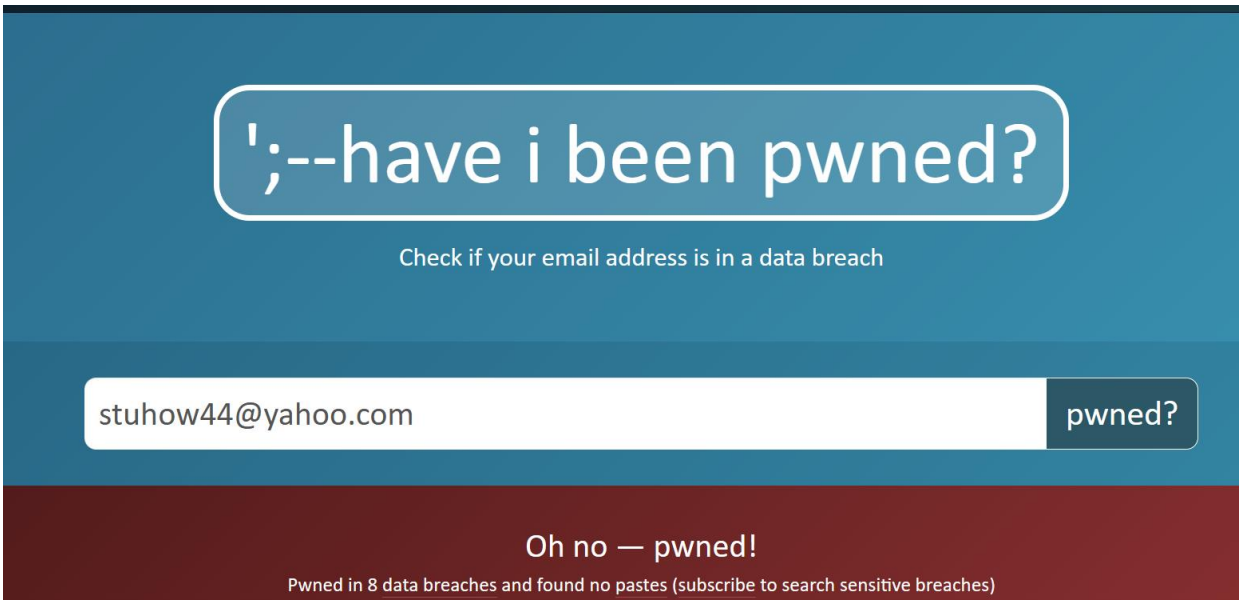
CYSE 450 - Introduction to Ethical Hacking & Penetration Testing
Assignment 2

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

Task 1 (50 points): Reconnaissance and Scanning

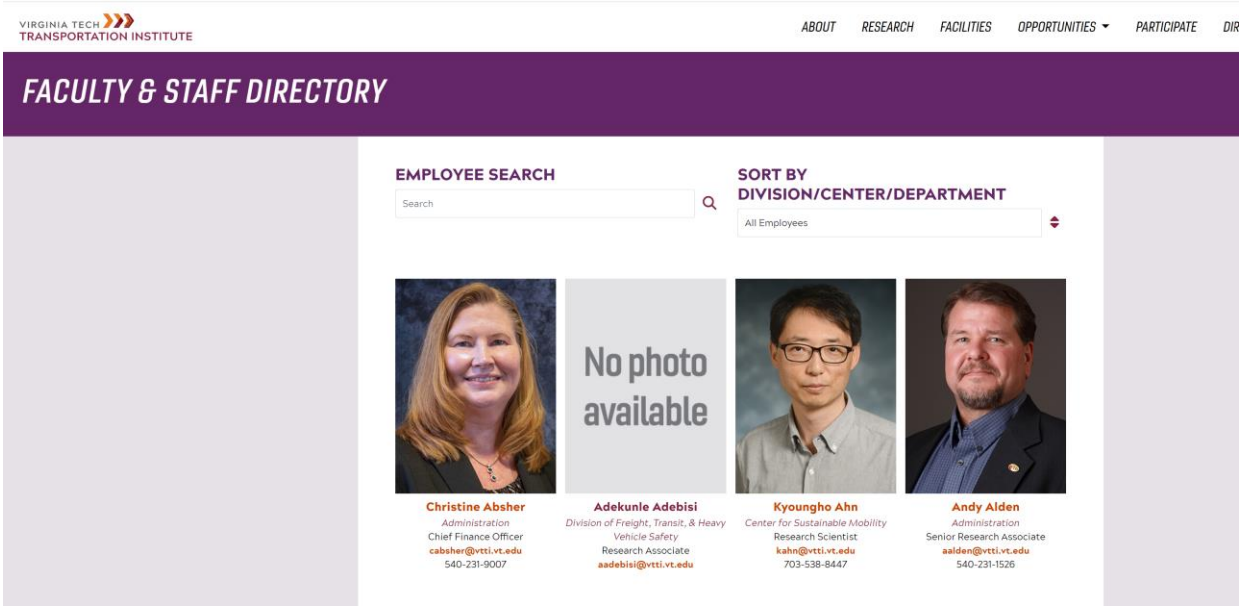
1.1. Your password is for sale!

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



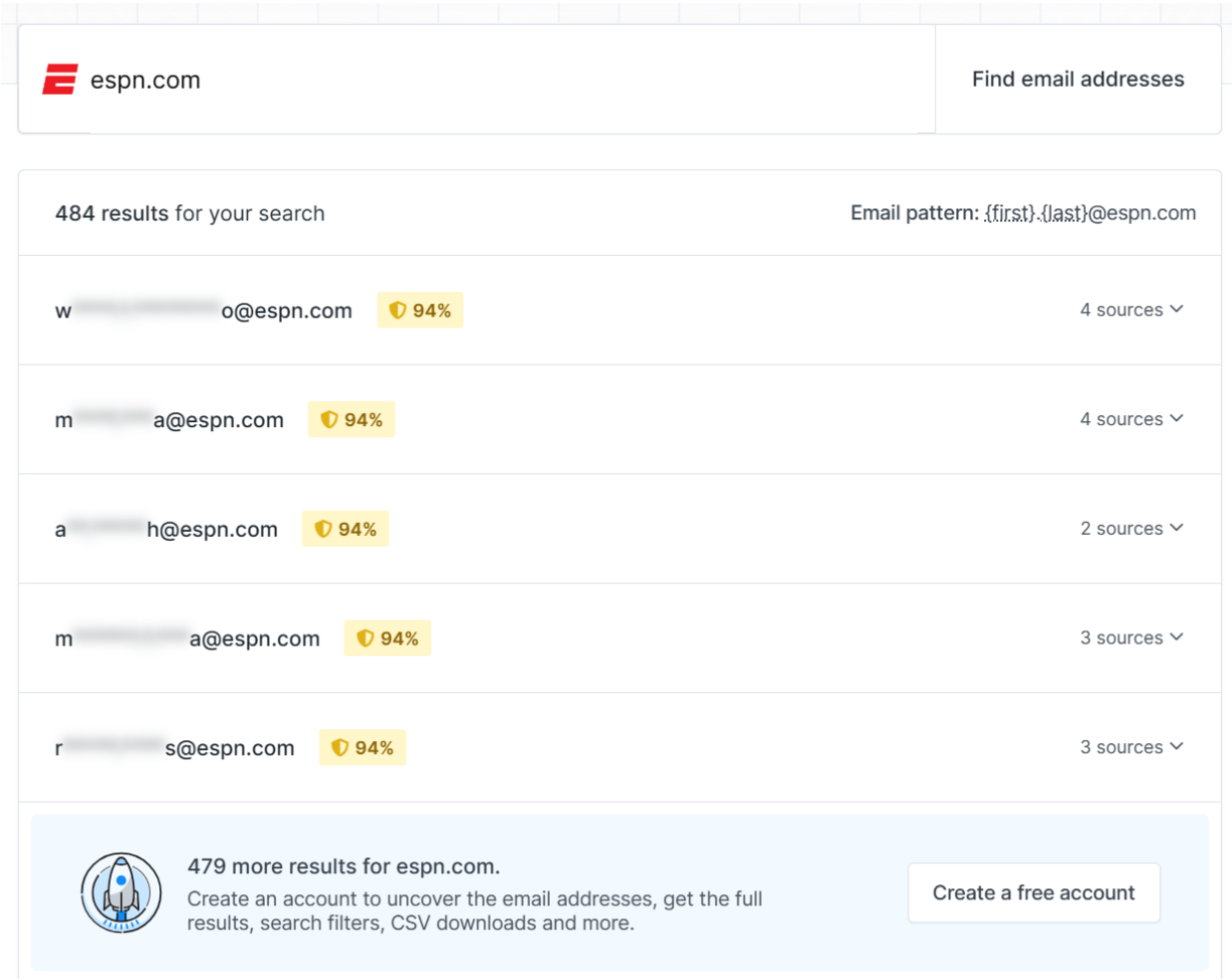
1.2. Make good use of Google search.

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.

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!

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

CVE stands for Common Vulnerabilities and Exposures. It lists publicly disclosed information security vulnerabilities and exposures that affect software and firmware. CVE was launched in 1999 by the MITRE corporation with funding from the U.S. Department of Homeland Security. CVE aims to identify and categorize vulnerabilities in a standardized way and provide a standard reference for security tools and solutions.

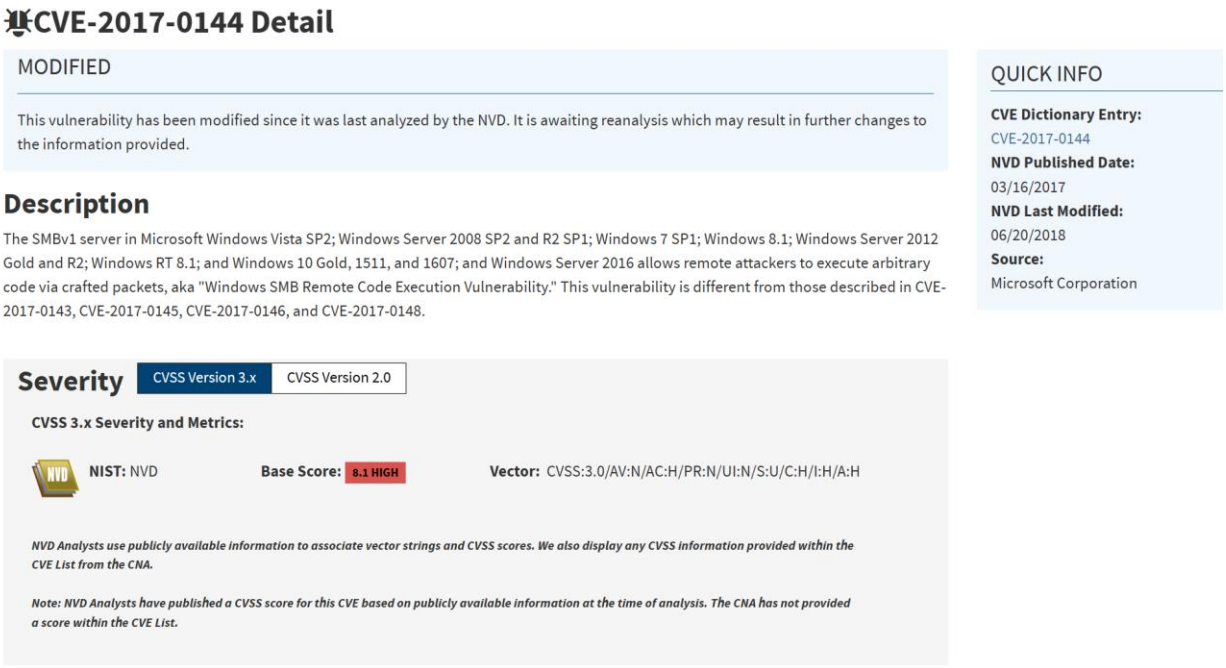
A CVE entry consists of a unique identifier, a brief description, and references to other sources of information. The identifier has the format CVE-YYYY-NNNNN, where YYYY is the year of discovery, and NNNNN is a sequence number. For example, CVE-2023-12345 is a CVE entry for a buffer overflow vulnerability in a web server application.

A CVE entry does not include technical details, risk assessments, or remediation advice. Other databases, such as the U.S. National Vulnerability Database (NVD), the CERT/CC Vulnerability Notes Database, and various vendor and researcher websites, provide those details. CVE entries are linked to these databases by their identifiers, which enable users to find more information about a specific vulnerability easily.

CVE entries are assigned by CVE Numbering Authorities (CNAs), organizations with the authority to issue CVE identifiers for vulnerabilities in their products or domains. There are about 100 CNAs representing major IT vendors, security companies, and research organizations. The MITRE corporation also assigns CVE identifiers for vulnerabilities not covered by CNA[2].

CVE is an essential resource for cybersecurity professionals, as it helps them discover, prioritize, and address system vulnerabilities. CVE also facilitates the coordination and collaboration among different stakeholders in the cybersecurity community, such as vendors, researchers, users, and regulators[1]. CVE is a free and open service that anyone can access and use.

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

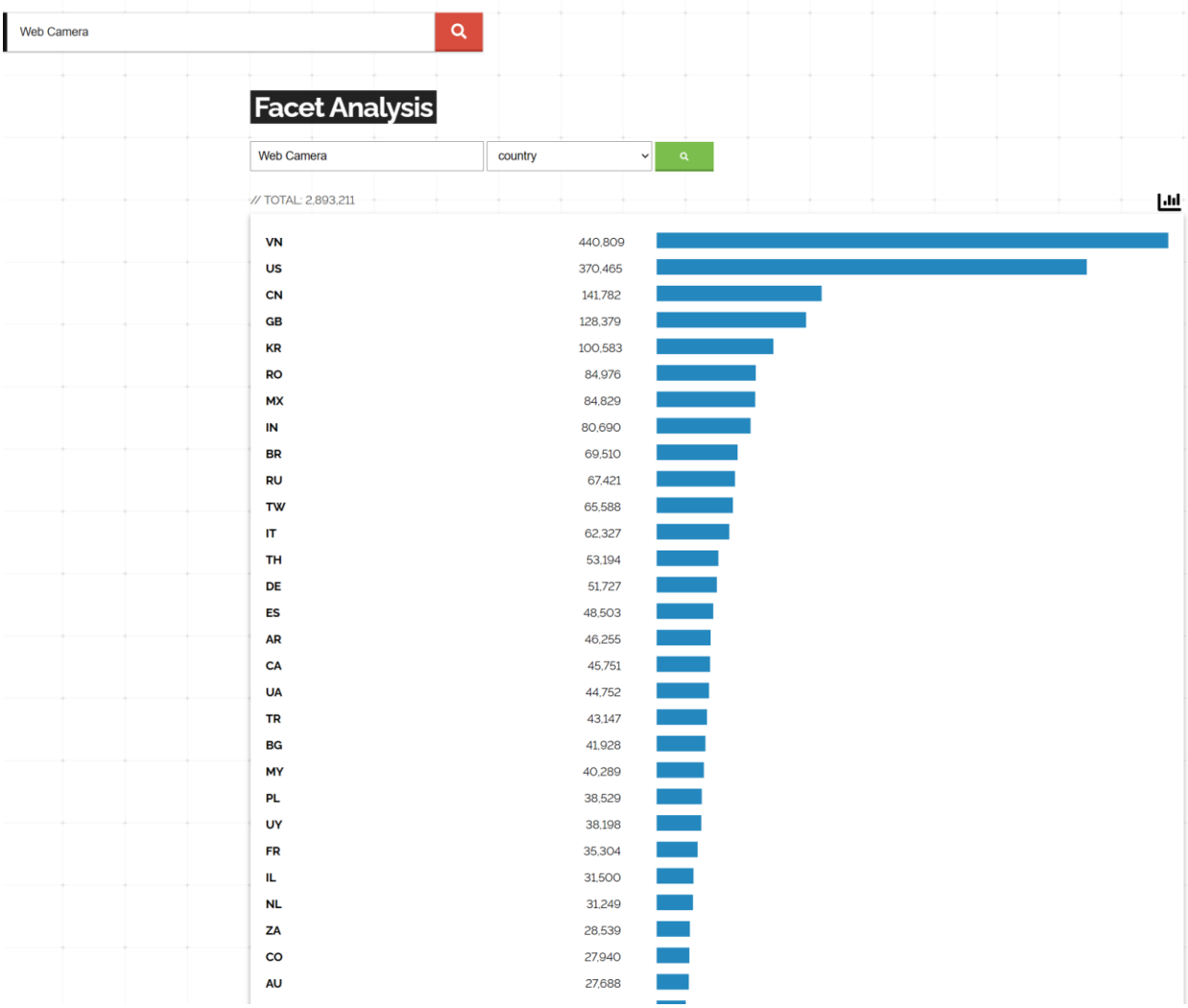


2.2. Search open web cameras!

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.



Web Camera

Facet Analysis

Web Camera | port

// TOTAL: 2,893,355