

CYSE 450 - Introduction to Ethical Hacking & Penetration Testing

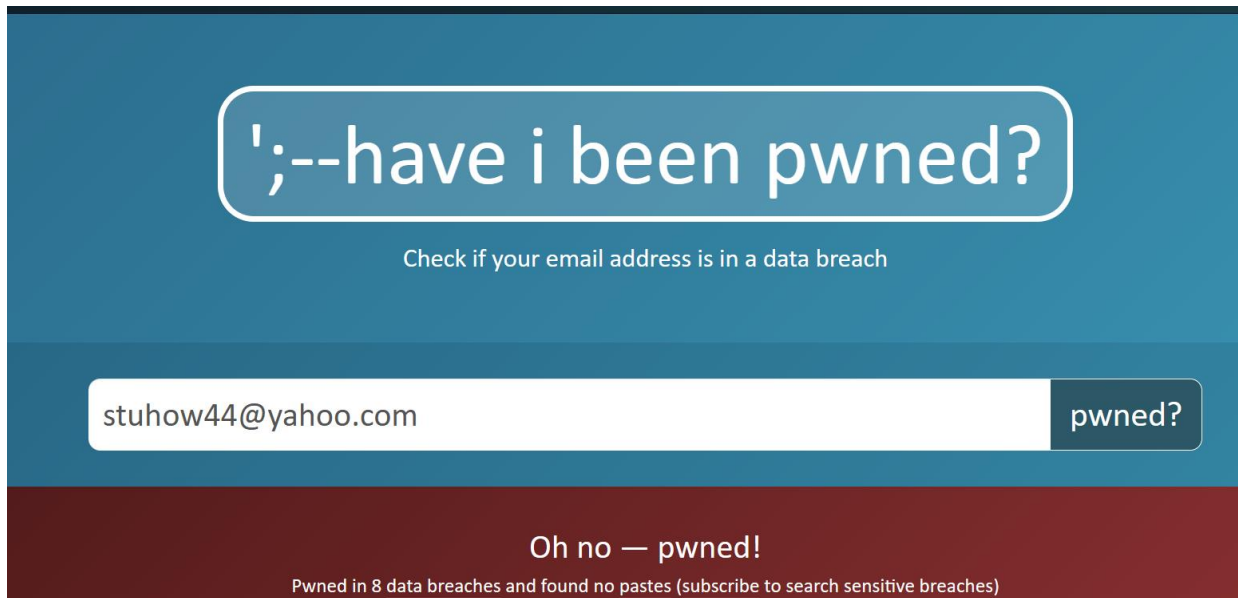
Assignment 2

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?



The screenshot shows the 'have i been pwned?' website interface. At the top, the title is 'have i been pwned?' in a large, white, rounded box on a blue background. Below the title, it says 'Check if your email address is in a data breach'. There is a search input field containing 'stuhow44@yahoo.com' and a button labeled 'pwned?'. Below the search results, it says 'Oh no — pwned!' and 'Pwned in 8 data breaches and found no pastes (subscribe to search sensitive 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.

FACULTY & STAFF DIRECTORY

EMPLOYEE SEARCH

SORT BY DIVISION/CENTER/DEPARTMENT



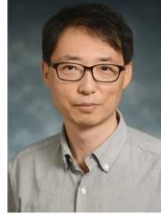
Christine Absher

Administration
Chief Finance Officer
cabsher@vtti.vt.edu
540-231-9007

No photo
available

Adekunle Adebisi

Division of Freight, Transit, & Heavy
Vehicle Safety
Research Associate
aadebisi@vtti.vt.edu



Kyoungho Ahn

Center for Sustainable Mobility
Research Scientist
kahn@vtti.vt.edu
703-538-8447




Andy Alden

Administration
Senior Research Associate
aalden@vtti.vt.edu
540-231-1526

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.



espn.com

Find email addresses

484 results for your search

Email pattern: {first}-{last}@espn.com

w	o@espn.com	94%	4 sources
m	a@espn.com	94%	4 sources
a	h@espn.com	94%	2 sources
m	a@espn.com	94%	3 sources
r	s@espn.com	94%	3 sources



479 more results for espn.com.

Create an account to uncover the email addresses, get the full results, search filters, CSV downloads and more.

Create a free account

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-NNNN, where YYYY is the year of discovery, and NNNN 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 CNA².

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 regulators¹. 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.

CVE-2017-0144 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

QUICK INFO

CVE Dictionary Entry:
CVE-2017-0144
NVD Published Date:
03/16/2017
NVD Last Modified:
06/20/2018
Source:
Microsoft Corporation

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **8.1 HIGH**

Vector: CVSS:3.0/AV:N/AC:H/PR:N/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.

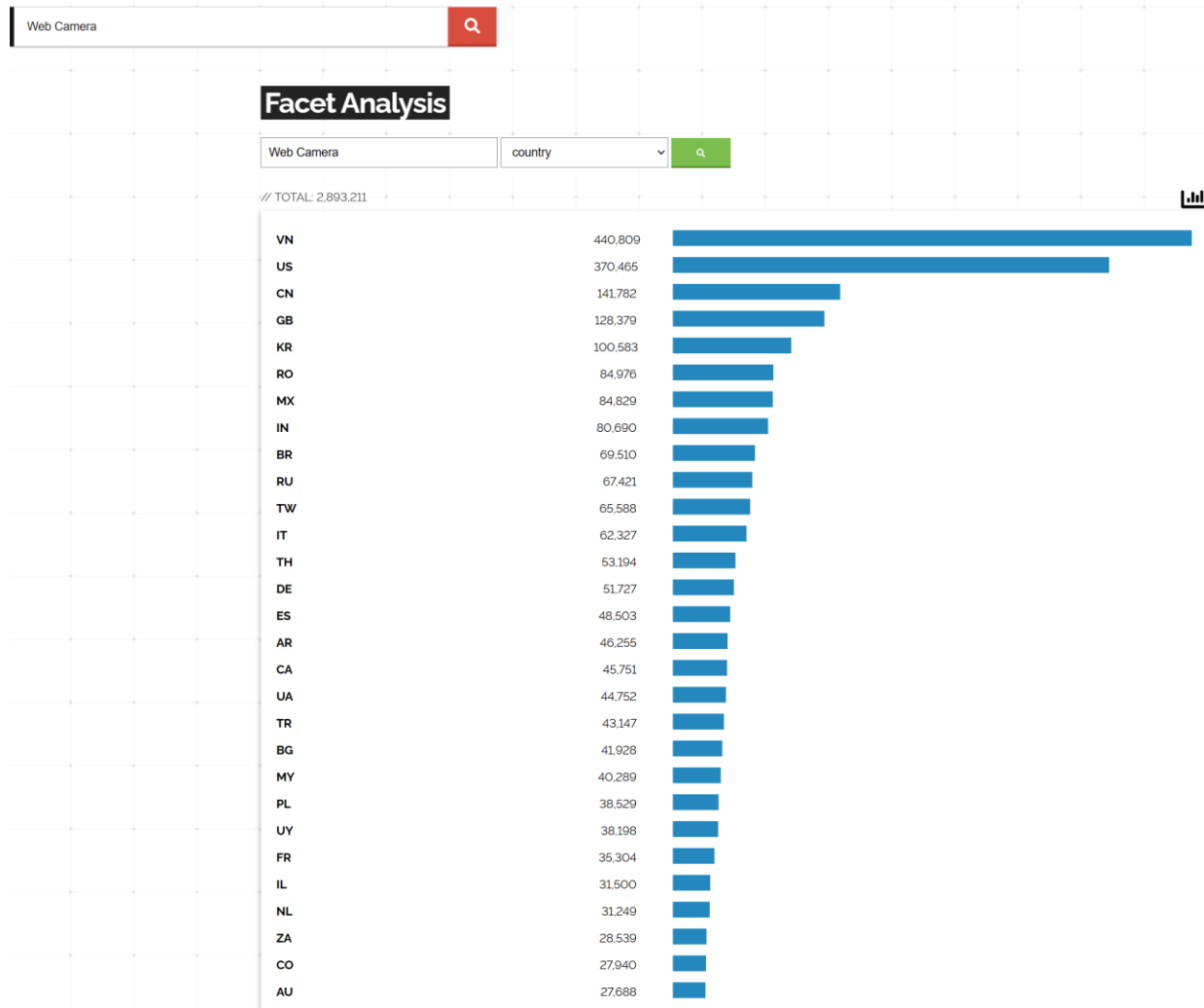
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

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.





Facet Analysis

Web Camera

port



// TOTAL: 2,893,355

