Laboratory Exercise B1 – Footprinting using Search Engines and Web Services

Due Date: 09/14/2022
Points Possible: Number of points out of total course points or recommended percent of the course grade.

1. Overview

For this lesson, we will use the Cyber Range: Cyber Basics (2020.12) environment to perform passive footprinting on a target.

2. Resources required

This exercise requires a Kali Linux VM running in the Cyber Range.

[Note to instructors: This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Cyber Basics (2020.12) environment, then click "start" to start your environment and "join" to get to your Linux desktop login. Log in using these credentials:

Username: **`student`**
Password: **`student`**

4. Tasks

Task 1: Collect data on a target using Google Searches

Let's say we are an attacker who wants to find information on a new product that Google is releasing. The CEO is planning to present the product in six months. An attacker can use advanced Google Operators to gain as much information about the CEO. Open a Browser and navigate to the default Google page. See if you can answer the questions below. The Cyber Range may be needed for this part of the exercise depending on your school's access to restricted sites. Web filters will often block website that contain the information you need to answer the questions.

Answer the following questions:

1. Who is the CEO of Google? Sundar Pichai
2. Where and what did he study? Metallurgical Engineering, materials science, engineering
3. What are his interests? Cricket and football.
4. Where does he live? Los Altos Hills, Santa Clara County, California.
5. What is the phone number to his gatekeeper (home)? Could not find anything outside of his work phone for HQ.
6. What car does he drive? BMW 730Ld.

Task 2: Find files using Google Hacking advanced operators

Head back to the main Google page. Now let's try to find something we are not supposed to have. ***Just don't download it!*** Let's say we want to find some free mp3s someone put on a server somewhere. We can search site indexes by typing `intitle:index of .mp3`. Let's be more specific. Let's say we want to find a specific artist. You can choose your own artist. ***Again, don't download***. The search should look something like this: `intitle:index of Back in black .mp3`. Note that for this search, I was also able to obtain the server OS, domain, and port that it was using.

Answer the following questions:

1. What songs could you find? Staying Alive by Bee Gees, Closer Than close by Bee Gees, Reaching Out by Bee Gees.
2. What other data did you find? I was able to find a ton of other songs by the Bee Gees. It is a Russian hosted site.

Understanding Directory path traversals

Once you have entered a web servers file directory with a search like the one above, you can maneuver forward and backward through the directory. Click on the link at the top "parent directory" to travel one folder back in the file system. There is an example in the provided instructor video and in the screenshots below. This way of traversing through the index of a site is not damaging to the server.

Index of /sounds/mp3s/Rock/ACDC

Name	Last modified	Size	Description
Parent Directory		-	
AC-DC - Problem Chil..>	2016-10-20 19:20	5.0M	
AC-DC - Who Made Who..>	2016-10-20 19:22	2.8M	
AC-DC - You Shook Me..>	2016-10-20 19:25	6.4M	
ACDC - 05 - Mistress..>	2016-10-20 19:29	5.5M	
ACDC - Back In Black..>	2016-10-20 19:30	3.9M	
ACDC - Dirty Deeds D..>	2016-10-20 19:33	3.8M	
ACDC - Got you by th..>	2016-10-20 19:35	4.1M	
ACDC - Have A Drink ..>	2016-10-20 19:38	5.5M	
ACDC - Hells Bells.mp3	2016-10-20 19:41	4.8M	
ACDC - Highway to He..>	2016-10-20 19:43	3.2M	
ACDC - Jailbreak.mp3	2016-10-20 19:47	6.4M	
ACDC - Money Talks.mp3	2016-10-20 19:50	3.4M	
ACDC - Rock 'N Roll ..>	2016-10-20 19:53	6.0M	
ACDC - Rock Your Hea..>	2016-10-20 19:56	5.6M	
ACDC - Shoot to Thri..>	2016-10-20 19:59	4.9M	
ACDC - TNT.mp3	2016-10-20 20:06	3.3M	
ACDC - The Razors Ed..>	2016-10-20 20:02	4.2M	
ACDC - Thunderstruck..>	2016-10-20 20:04	4.5M	
favicon.ico	2018-07-11 23:21	43	

Apache Server at www.sinj.com Port 443

Index of /sounds/mp3s/Rock

Name	Last modified	Size	Description
Parent Directory		-	
(6) Radiohead - High..>	2016-10-20 12:42	3.9M	
(10)Nirvana - Scentl..>	2016-10-20 12:43	3.2M	
(Soul Coughing) Supe..>	2016-10-20 12:44	3.2M	
01 - Ambulance (1).mp3	2016-10-20 12:47	5.9M	
01-the_white_stripes..>	2016-10-20 12:49	5.3M	
01_-_lazlow_-_intro-..>	2016-10-20 12:49	1.9M	
04 - young liars.mp3	2016-10-20 12:54	8.8M	
06 - Santeria.mp3	2016-10-20 12:51	3.5M	
18 Snatch Soundtrack..>	2016-10-20 12:55	4.6M	
ACDC/	2018-07-11 23:21	-	
Adema - The Way You ..>	2016-10-20 12:57	3.4M	
Adema - Trust.mp3	2016-10-20 12:58	4.0M	
Aerosmith/	2019-01-28 21:22	-	
AlbumArtSmall.jpg	2016-10-20 12:57	2.2K	
Alice In Chains - I..>	2016-10-20 12:59	3.9M	
Alice In Chains - Ma..>	2016-10-20 13:01	4.4M	
American Beauty -03-..>	2016-10-20 13:02	4.0M	
Big Wreck - That Son..>	2016-10-20 13:06	4.6M	
Blur with Radiohead ..>	2016-10-20 13:07	3.7M	
Breeders - Cannonbal..>	2016-10-20 13:08	3.3M	
Broken Social Scene ..>	2016-10-20 13:10	4.7M	
C'mon C'mon.mp3	2016-10-20 13:10	3.0M	
Cake - The Distance.mp3	2016-10-20 13:12	2.7M	
Cardigans - My Favor..>	2016-10-20 13:13	4.1M	
Chris Cornell - Can'..>	2016-10-20 13:15	3.1M	

Filetype:

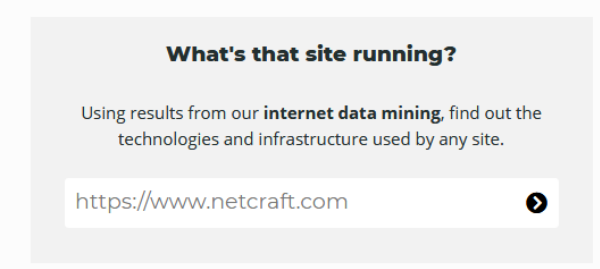
Filetype is another advanced Google Operator. Let's say you want to find documents in pdf format. Here is the basic syntax: `filetype:pdf <search words>`. If an attacker wanted to find company files, they may be able to search for pdf files containing important data. For example, `filetype:pdf <target> employee handbook`. In this case, the attacker is looking for the company's employee handbook. There is a lot of information that can be obtained from an employee handbook. Employee handbooks can list contact, emails, security policies, acceptable use policies, etc. Another

example is `filetype:pdf <target> login` this can return results for default instructions on how to login to a company system.

I was able to find The Home Depot's employee handbook this way.

Task 3: Find data using Netcraft (https://www.netcraft.com/)

Netcraft is a handy website tool that allows an attacker to gain data on a domain or web server. For example, if we type in the search box https://www.hackthissite.org/ and press enter, we get network information: how long the site has been up, encryption types, hashes, server name or owner, cipher and signature algorithms, etc. Be sure to scroll down the website page until you find the **what's that site running** submission box.



Answer the following question:

1. What is the IP of https://www.hackthissite.org?
   The IPv4 address is 137.74.187.104

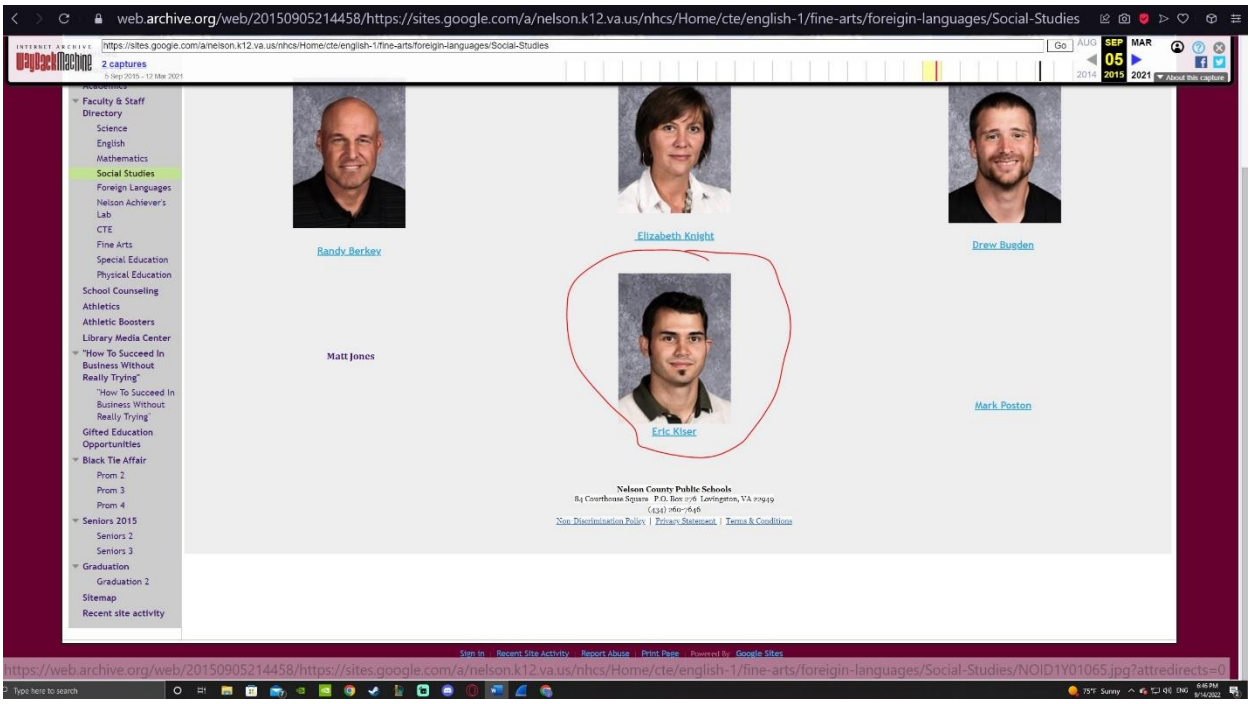
Task 4: Find target information using the Wayback Machine (https://web.archive.org/)

The Wayback Machine allows attackers to look at the cache of a website from previous years. Useful data can be obtained this way. Security practices were different 10, 20 plus years ago.

Complete the following task:

1. The current Nelson County High School website does not have a real picture of Mr. Kiser. See if you can find one.

   I went back 10 years, navigated to their staff directory, and found an Eric Kiser with a picture. It is on the next page:



Task 5 Explore Exploit Database (https://www.exploit-db.com/google-hacking-database)

The Exploit Database lists many advanced searches that can be performed using Google. The exploits are searchable as well. Not all are Google searches. The database holds a vast amount of other exploits. It also provides shellcodes that could be used to create backdoors. For this exercise, we will be using the Google Hacking Database. Let's see what we can find. **WARNING:** Only go as far as the search. **DO NOT ATTEMPT TO LOGIN** or crack any systems found. ***Do not download content***. **That would be illegal and punishable under the law as discussed in Module 1.**

1. Visit the Google Hacking Database in a browser.

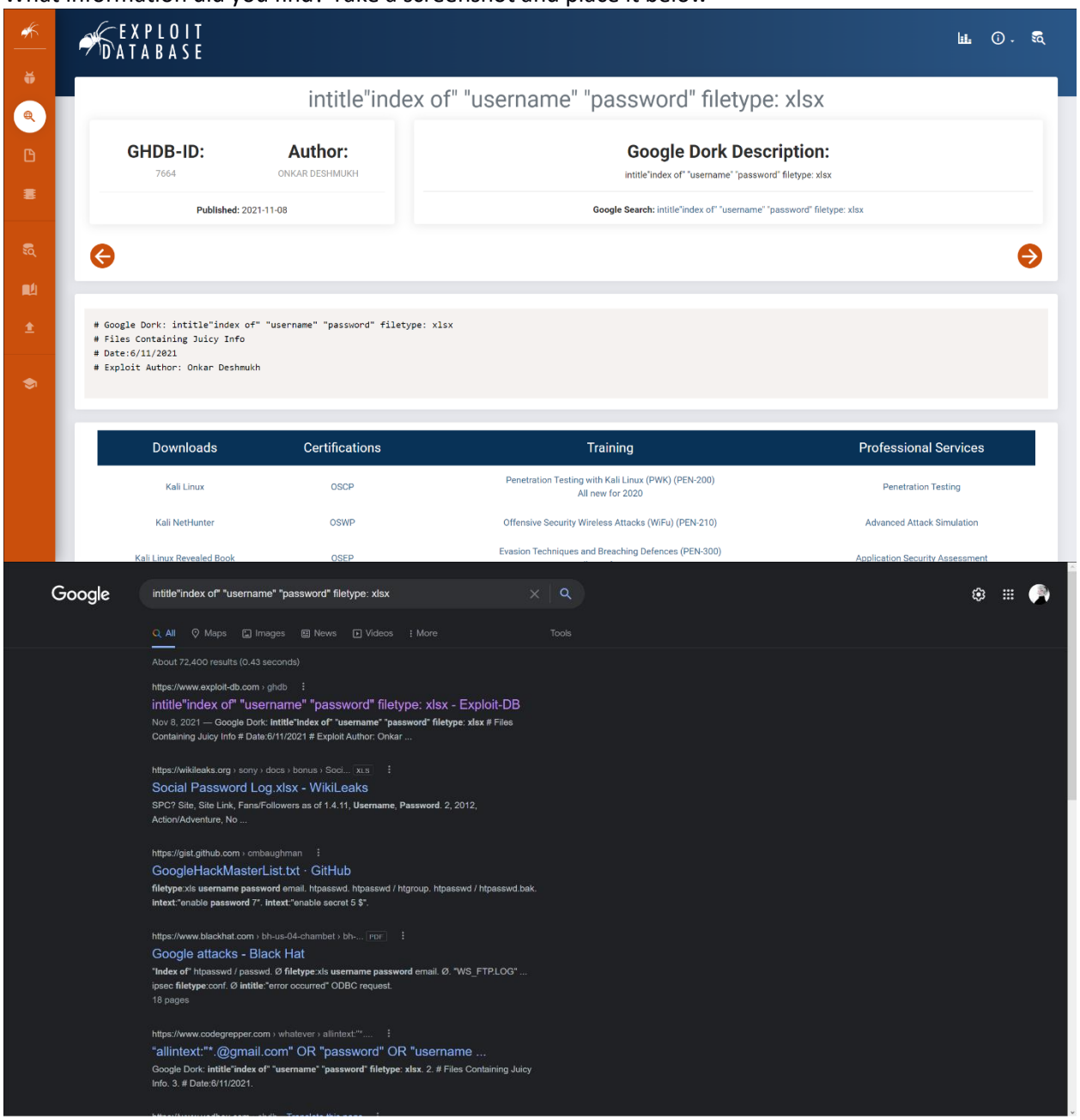
2. Type in the search box `username`.

3. Click on a link of your choice.
4. Click on the Google Search link.
5. View the results.

There are a lot of misconfigured web servers and devices on the internet. There is also a lot of information that should be protected such as usernames and passwords. Let this be a lesson, never place unencrypted data containing usernames and passwords online.

Answer the following questions:

1. What information did you find? Take a screenshot and place it below



2. How might attackers use this information?
   They might use it to gather username and password files. I saw multiple text files and xlsx.

Task 6: Explore CVE

The **CVE** website allows security professionals to analyze known vulnerabilities. According to the website, *"CVE provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample."*

Attackers can use this information as well. For example, if an attacker knows that a company is using the Linux Kernel version 2.6.32 - 4.13.1 they could search vulnerabilities such as CVE-2017-1000251. This is a Bluetooth stack attack resulting in remote code execution in kernel space.

Answer the following questions:

1. How many vulnerabilities are in Microsoft Products in 2015?
   514 vulnerabilities.
2. How many vulnerabilities are in Apple Products in 2015?
   658 vulnerabilities.
