Google Basics

Google is an extremely powerful search engine. With some practice, it can be utilized to discover a wealth of resources. First, we will cover some basics. Please review the information on the following sites:

Basic Search Help
https://support.google.com/websearch/answer/134479?hl=en&ref_topic=3036132
Refine Web Searches
https://support.google.com/websearch/answer/2466433?hl=en&ctx=cb&src=cb&cbid=-1p5t0py707x2h&cbrank=1&visit_id=637338138192366256-3316279017&rd=1

Google Operators

Google Operators can be used to refine your searches. Add one of these symbols to your search terms in the Google search box to gain more control over the results that you see. While there are many search operators, here are a few of the most common ones:

Search for an exact word or phrase "*search query*"	Use quotes to search for an exact word or set of words in a specific order, without normal improvements such as spelling corrections and synonyms. This option is handy when searching for song lyrics or a line from literature. ["imagine all the people"] ***Tip:*** Only use this if you're looking for a very precise word or phrase, because otherwise you could be excluding helpful results by mistake.
Exclude a word *-query*	Add a dash (-) before a word to exclude all results that include that word. This is especially useful for synonyms like Jaguar the car brand and jaguar the animal. [jaguar speed -car] ***Tip:*** You can also exclude results based on other operators, like excluding all results from a specific site. [pandas -site:wikipedia.org]
Include similar words *~query*	Normally, synonyms might replace some words in your original query. Add a tilde sign (~) immediately in front of a word to search for that word as well as even more synonyms. [~food facts] includes results for "nutrition facts"
Search within a site or domain *site: query*	Include "site:" to search for information within a single website like all mentions of "Olympics" on the New York Times website. [Olympics site:nytimes.com] ***Tip:*** Also search within a specific top-level domain like .org or .edu or country top-level domain like .de or .jp. [Olympics site:.gov]

Include a "fill in the blank" *query * query*	Use an asterisk (*) within a query as a placeholder for any unknown or "wildcard" terms. Use with quotation marks to find variations of that exact phrase or to remember words in the middle of a phrase.

	["a * saved is a * earned"]
Search for either word *query OR query*	If you want to search for pages that may have just one of several words, include OR (capitalized) between the words. Without the OR, your results would typically show only pages that match *both* terms. You can also use the | symbol between words for the same effect. [olympics location 2014 OR 2018] ***Tip:*** Enclose phrases in quotes to search for either one of several phrases. ["world cup 2014" OR "olympics 2014"]
Search for a number range *number..number*	Separate numbers by two periods (with no spaces) to see results that contain numbers in a given range of things like dates, prices, and measurements. [camera $50..$100] ***Tip:*** Use only one number with the two periods to indicate an upper maximum or a lower minimum. [world cup winners ..2000]

http://support.google.com/websearch/bin/answer.py?hl=en&answer=136861&ctx=cb&src=cb&cbid=-1p5t0py707x2h&cbrank=1

Advanced Google Operators

Locate text at the top of a webpage. *Intitle: “query” “query”*	Use “inititle:” to search for text that is found with HTML Title tags. If using multiple queries, Google results will show results if 1 or more queries are in the title.
Locate text at the top of a webpage. *Allintitle: “query” “query”*	Use “allinititle:” to search for text that is found with HTML Title tags. If using multiple queries, Google results will show results if ALL queries are in the title.
Search by filetype. *“query” filetype: “extension”*	Use “filetype:” to search for a specific filetype such as: • Microsoft Word: filetype:doc • Microsoft Excel: filetype:xls • PDF: filetype:pdf • …and many more

References/Resources

Google Support: www.google.com/support
Google Hacking Database: http://www.hackersforcharity.org/ghdb/
Long, Johnny. Google Hacking for Penetration Testing: 2nd Edition. Syngress Publishing

Lab 0: Google Hacking

Objectives:

- Locate useful information using the Google Search engine
- Use Google's built-in functionality to locate sensitive information about a targeted company

Tools Needed:

- Internet Browser
- Google Search Engine

Grading: 100 points total

- Part 1 – 20 points (2 points per question)
- Part 2 – 80 points (4 points per question)

Part 1: Generic Information Search [2 points each]

It is important to be able to locate a variety of information freely available on the Internet using the Google search engine. Use your Google Hacking skills to locate the following information.

Question	Answer
What computer worm was used to sabotage Iran's nuclear program?	Stuxnet
What entity established the AES specification?	U.S. National Institute of Standards of Technology
What language was the ILOVEYOU worm written in?	Visual Basic Scripting (VBS) which originated in the Philippines
What are the names of the two Trojans that were found to be inserted in CCleaner 5.33 in 2017?	Floxif and Trojan
Which Microsoft security patch fixed the Sandworm vulnerability?	Sandworm
What is the CVE for the Heartbleed vulnerability?	CVE-2014-0160
Which versions of OpenSSL are affected by the Heartbleed vulnerability?	OpenSSL 1.0.1 through 1.0.1f
What is a passing score on the CompTIA Security+ certification exam?	750/900
What Act requires every U.S. Federal agency to create and implement an information security program to protect the information systems the agency uses?	Federal Information Security Management Act
What is the SHA256Sum of Offensive Security's 2020.3 Kali Linux VMWare 64-bit Image?	Due to the length of this answer, place it the box below.

-- lab continues on next page --

Part 2: Targeted Company Search – Anne Arundel Community College (AACC)

Google Hacking can also be used to locating information about specific target companies. For instance, about an organization that has hired you, and given you written approval, to perform a penetration test. For this portion of the lab, please use Google to locate information specifically about Anne Arundel Community College. You do NOT have permission to attack AACC. You are **performing passive information gathering** – which means you will not interact with the organization. You will just be using the Google search engine to gather information.

Note: you are not authorized to contact AACC, or any of its employees, to locate this information. You must obtain all of the answers using Google searches.

General Information [4 points each]
When you are hired to perform a penetration test, it is important to learn more about your client. In this section, we will learn more about our “pretend” client, Anne Arundel Community College.

1. What year was Anne Arundel Community College founded?
   1961
2. How many acres is AAAC’s Arnold, Maryland campus?
   230
3. Is the CALT building located on AACC’s East Campus or AACC’s West Campus?
   West
4. Is the Truxal Library located on AACC’s East Campus or AACC’s West Campus?
   East
5. Which parking lot is closest to the Florestano Building? A, B, C, D, E, F, G or H?
   E
6. A Footbridge connects which 2 AACC parking lots? Answer with two letters – i.e. A & B
   G & H

Personnel [4 points each]
When performing a penetration test, you will find that knowing more about the individuals that work at the target organization can be very advantageous. These names often provide insight to user account on the system that you may need to access. In this section, you will seek out information about important personnel at AACC.

7. Who was the first President of Anne Arundel Community College?
   Dr. Andrew G. Truxal
8. Who is the current President of Anne Arundel Community College?
   Dawn Lindsay
9. What is the current President’s AACC email address?
   presidentsline@aacc.edu
10. What is the name of AACC’s Chief Technology Officer?
   Shirin Goodarzi

a. List the Google Search you entered to locate this information.

Name of aacc's chief technology officer

b. List the URL at which you found this information.

https://www.aacc.edu/media/college/leadership/Board-of-Trustees-Public-Session-Minutes_-June-12_-2018.pdf

c. List the date you know this information to be accurate. If for instance, if you found the information in a newspaper article/press release/meeting minutes, list the date of the that resource. If you found this information in a current directory on AACC's website or another website, list the date in which you accessed the website containing this information.

June 12, 2018

11. What is the name of the Director of Information Security at AACC?

John Williams

a. List the Google Search you entered to locate this information.

Name of the director of information security at aacc

b. List the URL at which you found this information.

https://www.linkedin.com/in/john-williams-1b06a56/

c. List the date you know this information to be accurate. If for instance, if you found the information in a newspaper article/press release/meeting minutes, list the date of the that resource. If you found this information in a current directory on AACC's website or another website, list the date in which you accessed the website containing this information.

9/8/2020

12. What is AACC's Director of Information Security's email address?

linkedin.com/in/john-williams-1b06a56

a. List the Google Search you entered to locate this information.

Name of director of information security at aacc

b. List the URL at which you found this information.

https://www.linkedin.com/in/john-williams-1b06a56/

13. What is the location of AACC's Director of Information Security's office?
Note: your answer should include a building code and room number – i.e. CALT 338
Hint: Access AACC's Staff Directory

CRSC 252B

14. Who's office is **CRSC 252Y**?
Hint: Access AACC's Staff Directory

Terence Crane

15. What is title of Terence Crane's position at AACC?

System Administrator

Authentication [4 points each]

Authentication is how users prove they are genuine, and not an imposter. Gaining information about a target organizations authentication method is critical in penetration testing. In this section, you will explore the authentication used by our “pretend” client, Anne Arundel Community College.

16. Locate an image of an AACC student ID card. Insert a copy of the image below.

a. List the URL that contains the image

https://www.google.com/search?q=image+of+aacc+student+id+card&source=lnms&tbm=isch&sa=X&ved=2ahUKEwihldz4otvrAhXlI3IEHWdwC2wQ_AUoAXoECAwQAw&biw=958&bih=959#imgrc=4JYU_HeUFtGULM

17. Locate AACC’s Password Policies.

a. What is the minimum password length for AACC accounts?

8

b. Which NINE special characters does AACC specifically state that users **CANNOT** use in their passwords?

! @ ^ % $ # ? ‘ / [ ] \ | { }

c. List the Google Search you entered to locate this information.

Aacc's password policy

d. List the URL at which you found this information.

https://www.google.com/search?source=hp&ei=J19YX7fmJeyJytMP0_CS4AY&q=aacc%27s+password+policy&oq=aacc%27s+password+policy&gs_lcp=CgZwc3ktYWIQAzIFCCEQqwI6CAgAELEDEIMBOgUIABCxAzoCCAA6BAgAEB46BggAEAoQHjoICAAQFhAKEB46BggAEBYQHjoFCCEQoAE6BwghEAoQoAFQ6QFYyRdg9hhoAHAAeACAAUyIAZkLkgECMjKYAQCgAQGqAQdnd3Mtd2l6&sclient=psy-ab&ved=0ahUKEwj3lcmPo9vrAhXshHIEHVO4BGwQ4dUDCAk&uact=5

Other [4 points each]
In this section, you will explore other pieces of data that might prove to be helpful as we explore the steps in the penetration testing process.

18. On what two days of each month do students in the Federal Work Study program receive paychecks?
Note: You will list two days of the month. For instance, the 1st & 15th
Hint: The Federal Work Study program is a part of the Student Employment Programs

7th and 22nd of each month

a. List the Google Search you entered to locate this information.

when do students get paid in federal work study program at aacc

b. List the URL at which you found this information.

https://www.google.com/search?ei=nWBYX-W9Je2g_QaDrp2QDw&q=when+do+students+get+paid+in+federal+work+study+program+at+aacc&oq=when+do+students+get+paid+in+federal+work+study+program+at+aacc&gs_lcp=CgZwc3ktYWIQAzoHCAAQRxCwAzoFCCEQoAE6BQghEKsCUOifAVjvqAFg4KkBaAFwAHgAgAGMAYgBywWSAQM3LjGYAQCgAQGqAQdnd3Mtd2l6wAEB&sclient=psy-ab&ved=0ahUKEwilgPTBpNvrAhVtUN8KHQNXB_IQ4dUDCA0&uact=5

19. What is the fine in US dollars for parking on the grass at AACC?

$15

20. What anti-spam firewall does AACC use?
Hint: On January 20, 2012, this information was located at address below
https://www.aacc.edu/technology/file/infoTech_Feb10.pdf
This link no longer works. If you visit the page, you will get a 404 – Page Not Found notice. Use the WayBack Machine to see what the page looked link on January 20, 2012.

Barracuda