

Lab 05 – Searching and Filtering

Raymond Ng: JQG999
IS 1003 Spring 2021
April 25, 2021

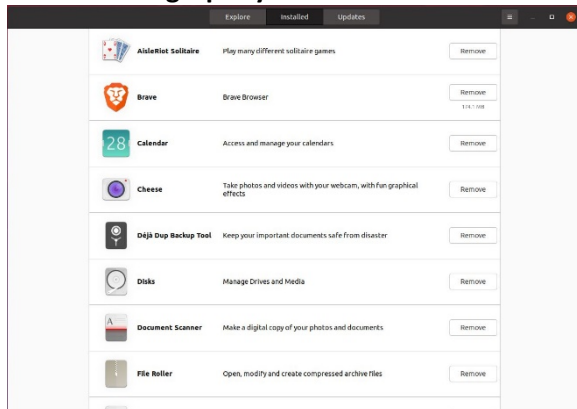
INTRODUCTION

The purpose of this lab was to execute the following:

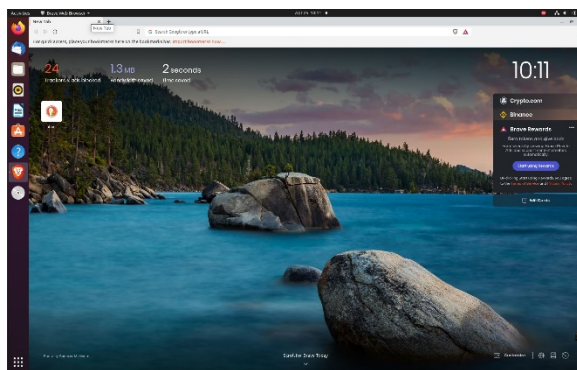
- Secure a browsing environment by using Brave web browser with the DuckDuckGo search engine extension on a Virtual Machine (VM).
- Check to see if my email(s) and password(s) have been discovered via HavIBeenPwned and to establish better password protocols.
- Search my online presence using Google Dorking operators and familiarize with the use of these operators.
- Use and familiarize with the use of the `grep` command and regular expressions (regexes) to filter the Slack workspace.

PROCESS

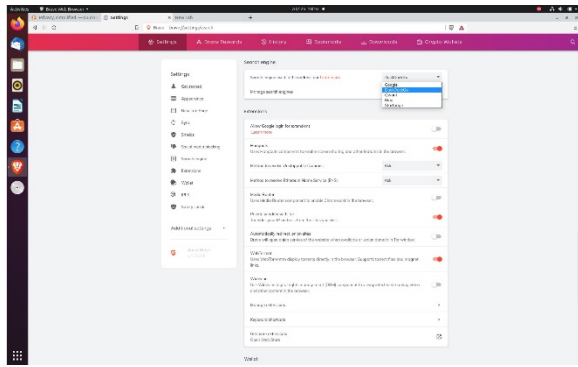
Part 1: Setting Up My Environment



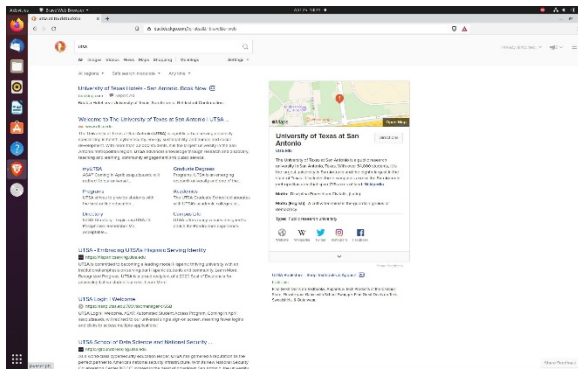
Per the initial block of instructions, I downloaded the Brave browser from the Ubuntu Software Center on my VM. In this lab, I continued using Ubuntu 20.04.2.0 LTS OS that I downloaded via VirtualBox from Lab01.



The installation of Brave took less a minute to install. After the installation was complete, I fired up the browser. There was a walkthrough before I got to the main screen that you see from this screenshot asking simple introductory questions include setting the Brave browser as my default browser.

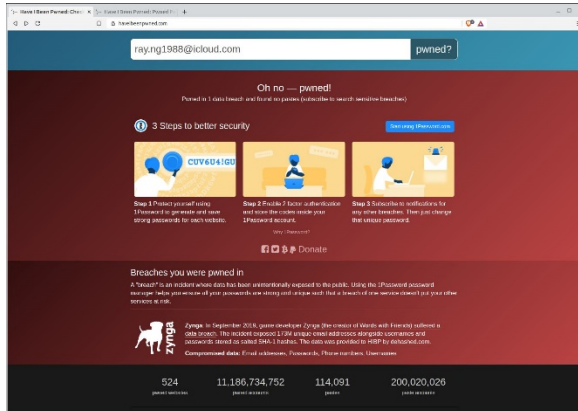


Next, I went to the DuckDuckGo.com and followed the instruction to add the DuckDuckGo extension to my Brave browser. When I clicked on the option to add the extension it prompted a window indicating to go to my search engine settings via the browser to switch it to DuckDuckGo.

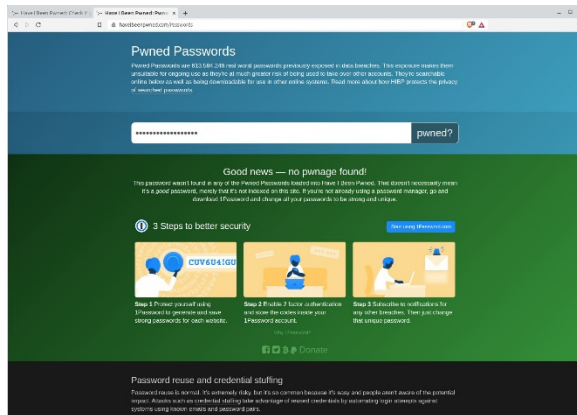


Executed a search via DuckDuckGo search engine. The results page looked identical to Google's search engine results. Everything appeared very simple and as expected from a search engine.

Part 2: Password and E-mail Checks

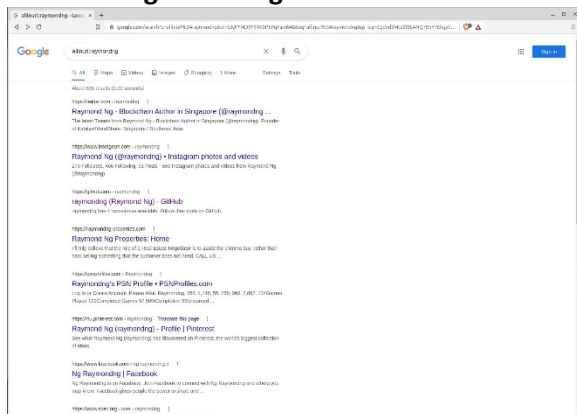


Using HaveIBeenPwned, I check to see if my personal email had been *pwned*. From the results, apparently my email was part of a data breach that happened back in September 2019 affecting the company Zynga that designs gaming applications. I'm was not too worried about it because the one gaming app I downloaded I used a fake alias as my player name and did not provide any information that would identify myself.

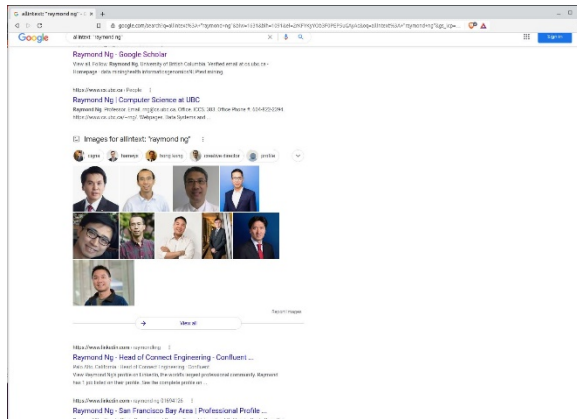


In the second part of this block of instructions I checked my password. The results indicated *no pwnage* was found. It recommended that I used 1Password.com, but I felt it was unnecessary because I have a password manager I use regularly (both mac and windows). Further, from my experience working in a secured environment, I usually change my password every 90 days using the upper/lower case, alphanumeric combinations, with at least one special character.

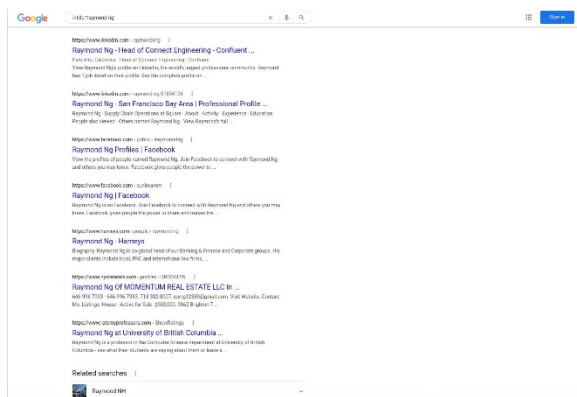
Part 3: Google Hacking



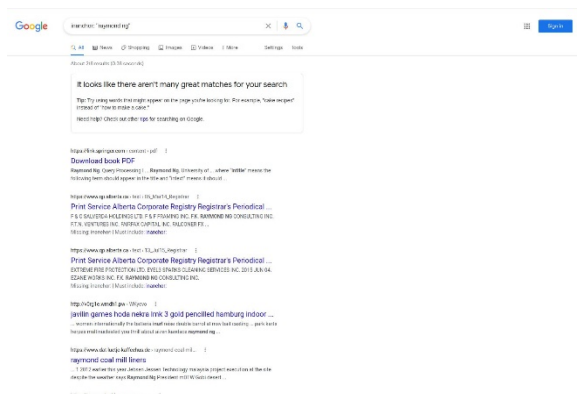
I used the `allinurl` Google Dork operator for a search of my name. It yielded results whose URL contained my name *RaymondNg*. I'm always happy to see that there are so many of me out there via the world wide web. I investigated the results that matched in social media platforms (facebook, Instagram, LinkedIn etc). None of the results were associated with my identity. (Borges, 2021)



I wanted to continue investigating instances of my name, Raymond Ng, so I used the `allintext` Google Dork operator to locate pages that contained my name inside their text. I investigated the sites on the first two pages just to see if any of them would match my identity. None of them were me. (Borges, 2021)



Here, I used the `allintitle` operator, specifically typed `allintitle:"raymond ng"`, to search for instances of my name in titles. (Borges, 2021)



Executed the `inanchor` operator to search anchor text associated with my name. Yielded no results in relation to my identity. (Borges, 2021)


```

raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -R '<https:'.
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-02-1
5.json:      "text": "Update on Friday, February 19, 5:14 PM: Based on <http
s://www.utsa.edu/today/2021/02/story/campus-closure-extended-weekend.html
> [this message from UTSA], Module 02 assignments now have a suggested deadline
of Monday, February 22 (0N1) and Tuesday, February 23 (001 and 002), and a hard
deadline of March 7 at 11:59 PM (all sections). Professor Collazo and I conferr
ed earlier today and have revised future module and lab dates as well. An update
d syllabus and schedule are posted on Blackboard in all sections. Take care.",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-02-1
5.json:      "text": "Hi all: Checking in ... how is everyone doing? Folks in
lower Texas may experience rotating power outages today and tomorrow. Here is so
me info from <https://www.ksa.com/cps-energy-customers-may-experience-rotati
ng-power-outages/IKISA>. Also, dress in layers, try not to get wet, and move ar
ound. More CDC tips are <https://emergency.cdc.gov/poweroutage/pdf/powerout
age.pdf|here>. Take care.",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-02-1
5.json:      "text": "<@U01JVM8PR3P> <https://is-1003-spring-2021.slack.com/
/archives/C01JCU5H2P/p1613393750232200>",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-01-2
6.json:      "text": "Hi all: I found a potentially more straightforward way t
o obtain a licensed Windows 10 operating system from UTSA: <https://www.utsa.e
du/techsolutions/students/software/windows.html>. Caveat: You can only downl
oad one of these, so it might be worth considering when you want to take UTSA up
on its offer. Also, note that you do not need a Win 10 VM for this class (but y
ou may for a couple of later classes).",

```

Grabbed all the links in the workspace by searching on '<https:'. Typed in `grep -R '<https:'`. I only captured a minimized screen of all the output from the command.

```

raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -R '"text":'.
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "And here is the book in a PDF: <https://is-1003-spring-2021.slack.com/files/U01KZCMB708/F01KB40EQ4F/sandworm.pdf>.",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "And here is the book in a PDF: ",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": ".",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "Last thing for now...although you are not req
uired to post anywhere else, feel free to read other posts on module and lab ch
annels and to contribute whenever you'd like.",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "Last thing for now...although you are not req
uired to post anywhere else, feel free to read other po
sts on module and lab channels and to contribute whenever you'd like.",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "Thank your Dr. Mitra and hello Joseph! I have
a lot of catching up to do, but I look forward to our conversations on this th
read! ",
IS-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/sandworm-studies
/2021-02-03.json:      "text": "Thank your Dr. Mitra
and hello Joseph! I have a lot of catching up to do, but I look forward to our
conversations on this thread! ",
raymond-ng@raymondng-VirtualBox: ~/Downloads$

```

Here I saved all the text of the workspace using the "text" keyword. Typed in `grep -R '"text":'`.

```

raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -R '[gG]it lab-03'
raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -R '[gG]it lab-03'
>

```

Attempted to execute `grep -R '[gG]it lab-03` to find instances of the words "git" or "Git" in the lab-03 folder, but yielded no results. I tried adding a '[' at the end of syntax, but that did not work either. I did notice that if I simply just typed in `grep -R '[gG]it'` it depicted all instances of the words "git" and "Git".

```

raymond-ng@raymondng-VirtualBox: ~/Downloads/IS-1003-Spring-2021 Slack Export Jan
10 2021 - Apr 17 2021 (1)/lab-03$ grep -R '[gG]it'
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15,
16, and 17? And you see no updates on timestamps on GitHub and/or git for any o
f the steps?",
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15, 16, and 17? And you see no updates on timestamps on GitHub
and/or git for any of the steps?",
2021-03-27.json:      "text": "Is it possible to have the \"git Bash\" install w
ithin the virtual machine? ",
2021-03-27.json:      "text": "Is it possible to have the \"git Bash\" install within the virtual machine? ",
2021-03-27.json:      "text": "On step 19 it shows my branch is already up to
date...did I do something in github incorrectly or did I just do the same thing b
ut a different way?",
2021-03-27.json:      "text": "On step 19 it shows my branch is already up to date...did I do something in github incorrectly or did I
just do the same thing but a different way?",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If
you completed the operations, then you should be fine (you may have executed you
r pull from GitHub, for example).",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If you completed the operations, then you should be fine (y

```

Later, I realized that I had forgot a '[' after [gG]it so the it should have read `grep -R '[gG]it'` lab-03'. However, the output indicated that the lab-03 directory could not be found. Instead, I changed the directory (using the `cd` command) I was working under to the lab-03 folder from the Slack workspace and ran the `grep -R '[gG]it' lab-03` command again and it searched for all instances of "git" and "Git".

```

raymond-ng@raymondng-VirtualBox: ~/Downloads/15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/lab-03$ grep -R '[gG]itHub'
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15, 16, and 17? And you see no updates on timestamps on github and/or git for any of the steps?",
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15, 16, and 17? And you see no updates on timestamps on github and/or git for any of the steps?",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If you completed the operations, then you should be fine (you may have executed your pull from github, for example).",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If you completed the operations, then you should be fine (you may have executed your pull from github, for example).",
2021-03-29.json:      "text": "On the step 1 setup part for Git are there instructions on what the particular selection to make during the setup because I've read the instructions and don't see any and when I try to access hello world git Hub guidelines under tutorial it gives me a broken link",
2021-03-29.json:      "text": "On the step 1 setup part for Git are there instructions on what the particular selection to make during the setup because I've read the instructions and don't see any and when I try to access hello world github guidelines under tutorial it gives me a broken link"

```

Remaining in the lab-03 file, I search for all instances of the word “GitHub” in my Slack workspace by executing `grep -R '[gG]itHub'` command. The screenshot does not capture the entire output.

```

raymond-ng@raymondng-VirtualBox: ~/Downloads/15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/lab-03$ grep -R '[gG]it[hH]*u*b*'
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15, 16, and 17? And you see no updates on timestamps on github and/or git for any of the steps?",
2021-03-27.json:      "text": "Do you mean that nothing happened at steps 15, 16, and 17? And you see no updates on timestamps on github and/or git for any of the steps?",
2021-03-27.json:      "text": "Is it possible to have the git Bash" install within the virtual machine?",
2021-03-27.json:      "text": "Is it possible to have the git Bash" install within the virtual machine?",
2021-03-27.json:      "text": "On step 19 it shows my branch is already up to date..did I do something in github incorrectly or did I just do the same thing but a different way?",
2021-03-27.json:      "text": "On step 19 it shows my branch is already up to date..did I do something in github incorrectly or did I just do the same thing but a different way?",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If you completed the operations, then you should be fine (you may have executed your pull from github, for example).",
2021-03-27.json:      "text": "There are many ways to achieve these tasks. If you completed the operations, then you should be fine (you may have executed your pull from github, for example).",

```

This is a screenshot of part of the output from the executing a command using wildcards, specifically the “*” wildcard. Here I typed in `grep -R '[gG]it[hH]*u*b*'` into the terminal. The screenshot does not capture the entire output.

```

raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -ri "word".
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-04/2021-03-26.json:      "text": "I dare you a little to figure this one out :slight ly_smiling_face: Please read the first error message and check the spelling of the key words mentioned in it (compare to other similar words in the code and try to find the error). Every character counts...",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-04/2021-03-26.json:      "text": "Please read the first error message and check the spelling of the key words mentioned in it (compare to other similar words in the code and try to find the error). Every character counts...",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-02-08.json:      "text": "I didn't read the instructions carefully and forgot to include my name in my virtual machine's admin username. I attempted to change it, but it required me to put in my complex password in less than a second. I, a slow typer, am now stuck with a username based on memes (and doesn't include my name). Would this lead to points off?",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-02-08.json:      "text": "I didn't read the instructions carefully and forgot to include my name in my virtual machine's admin username. I attempted to change it, but it required me to put in my complex password in less than a second. I, a slow typer, am now stuck with a username based on memes (and doesn't include my name). Would this lead to points off?",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-01-19.json:      "text": "so for the responses do we have a word minimum??",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-01-19.json:      "text": "so for the responses do we have a word minimum??",
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/general/2021-01-19.json:      "text": "<@U01JMBDVP1>: I'm editing this response after checking into Packback a bit more. There is a word minimum of 20 words to activate the AI. Overall, Packback scores on the quality of your post and its credibility."

```

I wanted try searching for the word “word” in the Slack workspace without case distinctions. So I typed in `grep -ri “word”`. This screenshot does not capture the entire output of the command. (Gite, 2016)

```

raymond-ng@raymondng-VirtualBox: ~/Downloads$ grep -r -l "syntax".
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-04/2021-03-20.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-04/2021-03-23.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-04/2021-03-22.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/lab-01/2021-02-09.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-06/2021-04-11.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/lab-02/2021-03-07.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/lab-02/2021-03-06.json
15-1003-Spring-2021 Slack Export Jan 10 2021 - Apr 17 2021 (1)/module-03/2021-02-23.json

```

Lastly, I wanted to search for the word “syntax”, but instead of listing all instances of the word in the output I only wanted to see, which files the word would be found in. (Gite, 2016)

CONCLUSION

In conclusion I attempted to secure a safe browsing environment via VM. Additionally, checked to see if my email and passwords have been discovered/compromised. Further, I learned and familiarized myself

with Google Dorking and utilization of the grep command (and regexes) to search and filter in directories in the terminal of linux machines.

This lab felt a little more abstract than the previous ones, particularly when I got to Google Dorking. However, it was great forcing function to research and explore on my own to gain a better understanding. I can see how the combination of the lines of efforts in this lab can help cybersecurity analysts debug in the real world.

REFERENCES

Internet Resources

Borges, E. (2021). *Exploring Google Hacking Techniques - Top Google Dorks*. Retrieved from Security Trails: <https://securitytrails.com/blog/google-hacking-techniques>

Gite, V. (2016, October 8). *Linux / UNIX Recursively Search All Files For A String*. Retrieved from Cyberciti: <https://www.cyberciti.biz/faq/howto-recursively-search-all-files-for-words/>

Smart Search with GoogleDorking. (2017, May 29). Retrieved from Exposing The Invisible: <https://exposingtheinvisible.org/en/guides/google-dorking/>

Collaboration

I attempted to collaborate via Slack, by posting the issue I encountered in Step 4, Part 5 concerning the specific search for a word in a specific lab folder. The instructor noticed I was missing a character in my syntax; however, it did not remedy the issue. I ended debugging on my own by reviewing the `cd` command from a previous lab and the issues was corrected.