

EECS 3482 – LAB 1

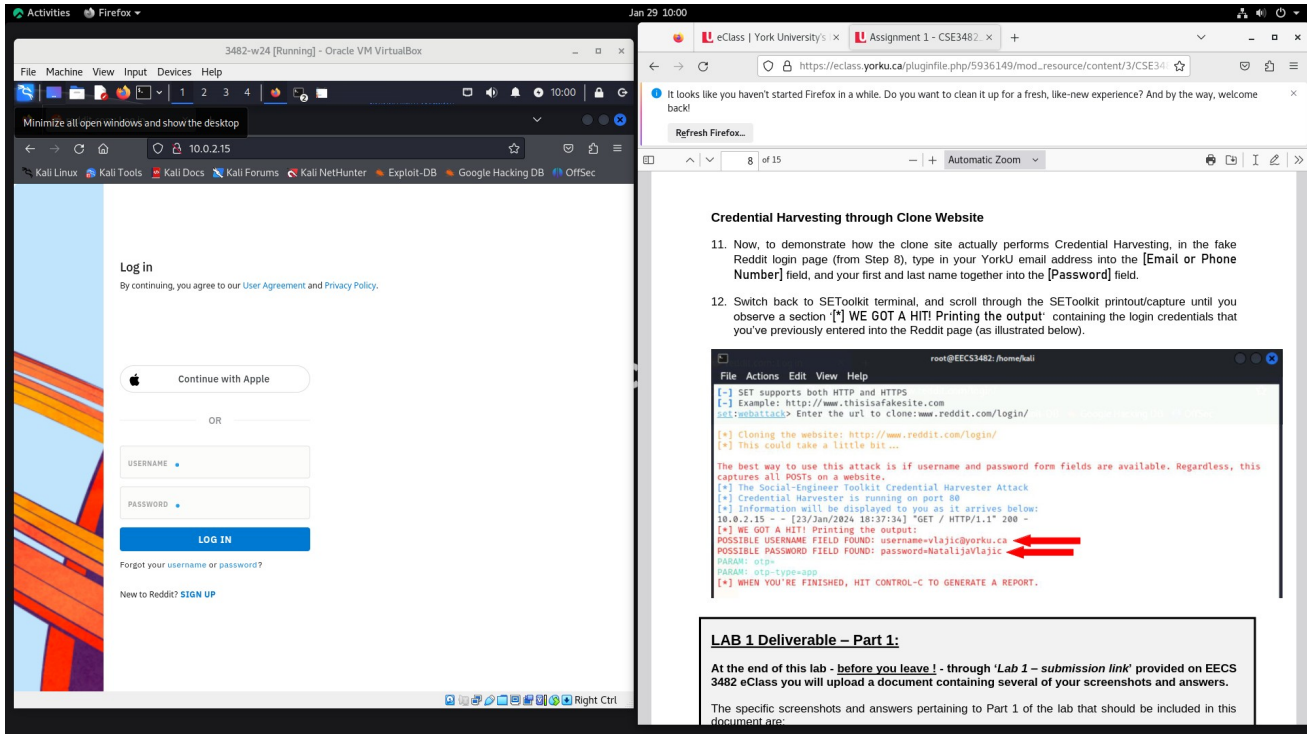
NAME: Stuti Parmar

STUDENT ID: 218516625

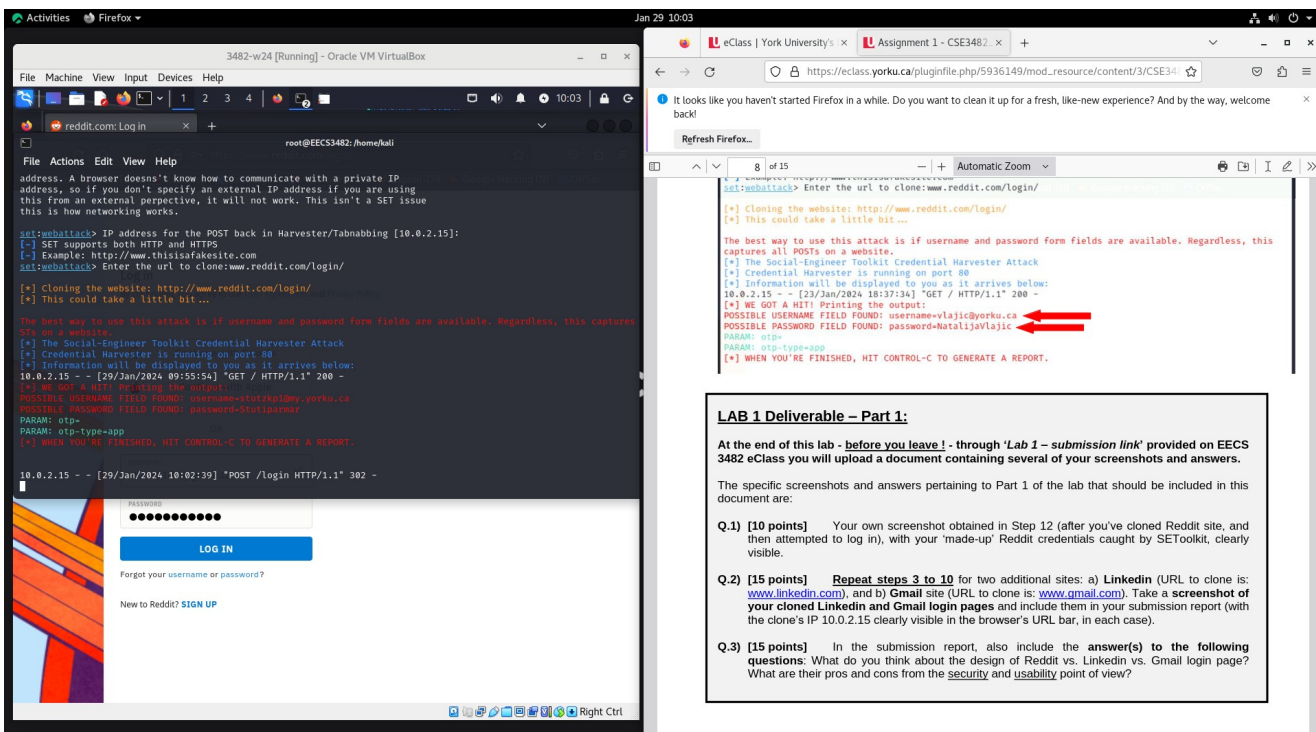
PART 1

Q.1)

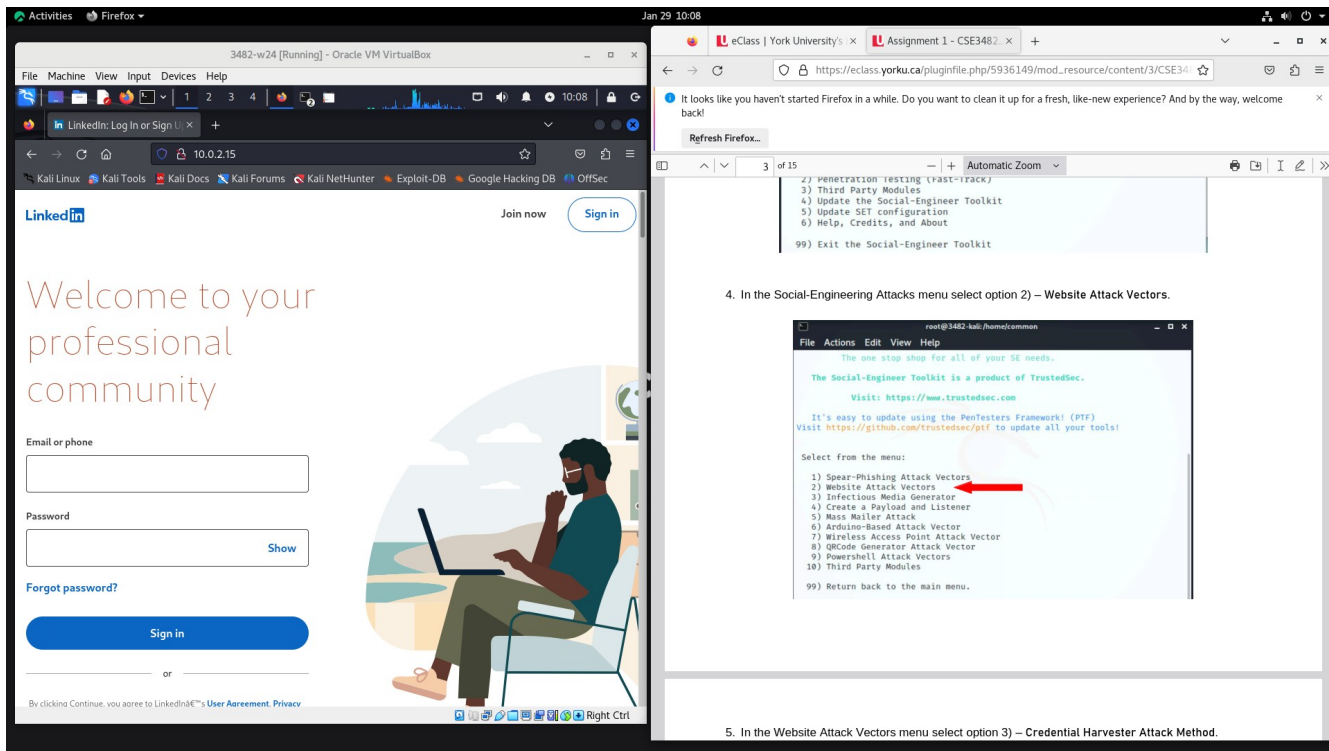
Screenshot of Reddit website login page:



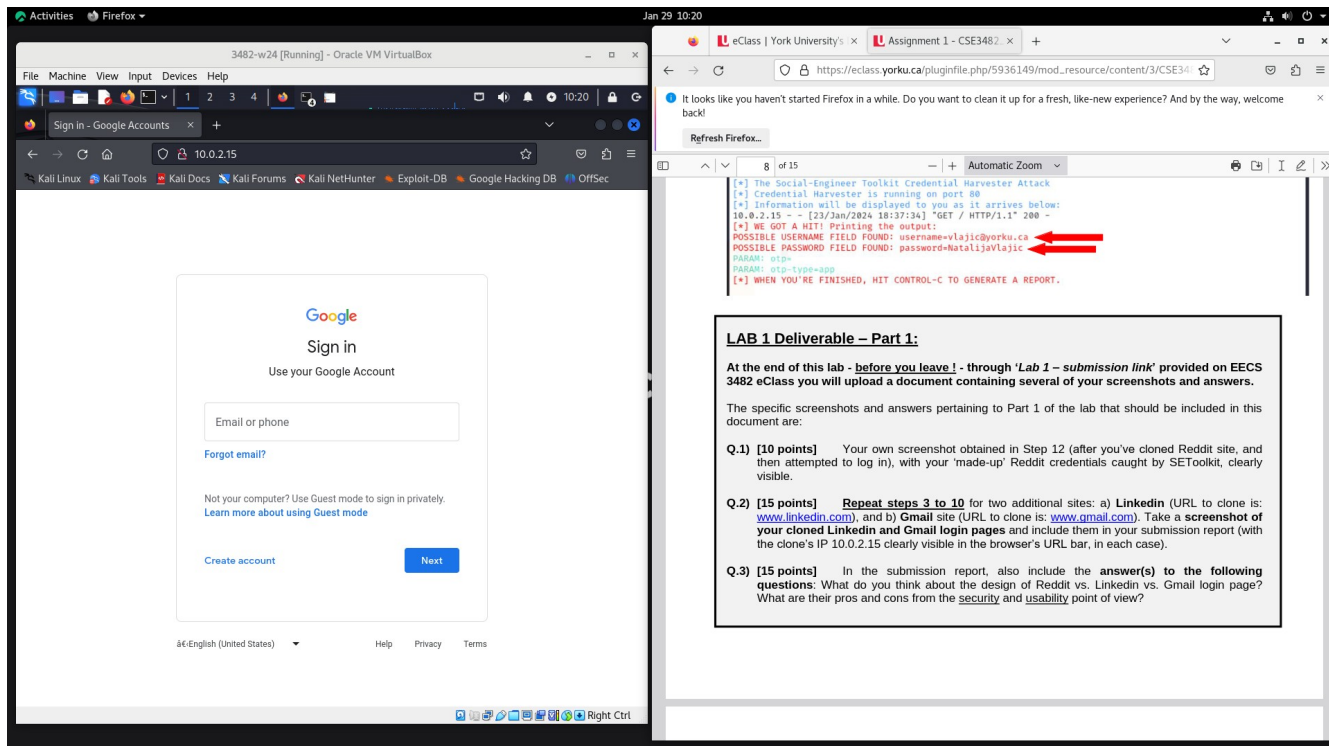
Screenshot of Step 12:



Q.2) Screenshot of LinkedIn login page:



Screenshot of Gmail Login Page:



Q.3) What do you think about the design of Reddit vs. LinkedIn vs. Gmail login page? What are their pros and cons from the security and usability point of view?

- According to me the LinkedIn and Gmail login pages look more real and genuine than reddit login page.
- One thing to notice about Gmail login page is the symbol beside 'English (United States)' which doesn't appear in real login page of gmail.
- For the fake linkedin login page, the fonts for "welcome to your professional community" is different from the real login page.
- And for Reddit fake login page, there is no option for 'Continue with google' as it appears in real login page of reddit.
- Pros in points of security for the fake login pages are that you get the person's username and password as soon as they enter it on such websites which can be easily used to exploit the vulnerabilities. Cons in terms of security would be that sensitive information is leaked because of real looking login pages which leads to data breach.
- Usability means the user's experience when interacting with the websites. So in terms of pros, they are quite real looking but in terms of cons there are little details that can identify them as fake websites (as mentioned above).

PART-2

Q.1) Here the IP address of web-server host is – 130.63.94.24 and the IP address of email address is – 130.63.94.75. As the IP addresses are different, the web server and the email server run on different physical host/machine.

Q.2) It is an Apache software/program and the version of EECS's Web Server is –
cpe:/a:apache:http_server:2.4.58

Q.3) The most recent CVE vulnerability is – CVE-{2023}-{5678}

Q.4) Screenshot of www.mcmaster.ca :

The screenshot shows the Maltego Community Edition 4.4.1 interface. The main window displays a graph with various entities, including domains, IP addresses, and machines. The graph is titled "New Graph (1)" and shows a complex network of relationships. The left sidebar contains a search bar and a list of entities. The right sidebar shows a "Detail View" for a selected entity. A browser window in the foreground displays a lab assignment titled "LAB 1 Deliverable – Part 2:" with the following content:

LAB 1 Deliverable – Part 2:

In addition to the screenshots and answers from Part 1, the following screenshots and answers pertaining to Part 2 of the lab should also be included in your submission document:

Q.1) [10 points] Based on your Maltego analysis of EECS Web-domain, does it appear that EECS web-server and email server run on the same physical host/machine? (Hint: what is the IP address of the web-server host and what is the IP address of the email server host? Include these in your report.)

Q.2) [10 points] What is the program/software type and version of EECS's Web server (e.g., Apache vs IIS)?

Q.3) [15 points] Out of the CVE vulnerabilities that Maltego identified on the host machine of EECS server, which one is the most recent (i.e., most recently added to the CVE database, and thus the least likely to be patched)?
Hint: CVE vulnerability identifiers follow the format CVE-{year}-{ID}, where the ID is sequentially increased in each year for every newly discovered/reported vulnerability.

Q.4) [25 points] Repeat Steps 3 to 9 (except Step 7) for the following two domains: www.mcmaster.ca (McMaster University) and www.uwaterloo.ca (University of Waterloo) to obtain the respective Footprint L2 Maltego graphs. Include a snapshot of the final graph for each university.
Based on these graphs (and as per our in-class discussion on DDoS defences), if you were an attacker interested in conducting a DDoS attack on one of the two domains, which one do you think would be easier to successfully DDoS? Explain!

Screenshot of www.uwaterloo.ca:

The screenshot shows the Maltego Community Edition 4.4.1 interface. The main window displays a graph with various entities, including domains, IP addresses, and machines. The graph is titled "New Graph (1)" and shows a complex network of relationships. The left sidebar contains a search bar and a list of entities. The right sidebar shows a "Detail View" for a selected entity. A browser window in the foreground displays a lab assignment titled "Assignment 1 - CSE3482" with the following content:

More information about the nature of various footprint options in Maltego can be found from: <https://www.maltego.com/blog/network-footprinting-with-machines-in-maltego/>

7. Now, right-click on mail.eecs.yorku.ca email entity (icon C). In the Run Transforms window select All Transforms (click on + symbol to see all sub-options), and then click on To IP Addresses [DNS] sub-option. This will reveal the IP address of the actual machine on which EECS's email server runs, which will also help you determine whether the main Web and the main email server of EECS domain are hosted on the same physical machine, which would be helpful if one is to perform a simultaneous attack on both the web and email server of www.eecs.yorku.ca domain.

8. Next, right-click on the machine / IP entity affiliated with www.eecs.yorku.ca domain icon (icon B). In the Run Transforms window select All Transforms (click on + symbol) -> To Location [city, country] option. This will reveal the geographic location at which the given machine is situated.

9. Again right-click on the machine / IP entity affiliated with www.eecs.yorku.ca. In the Run Transforms window, move the mouse to To Vulnerabilities [Shodan Internet DB] (as shown below left), and click on the arrow at the right-end of this option (Run All – as shown below left, observe the location of red arrow). This will generate a graph (as shown below right) which contains icons representing the instances of software running on the given machine (including their version), the open port numbers, as well as their known associated CVE vulnerabilities. (Note: the machine may not be impacted by all the enlisted vulnerabilities. The vulnerabilities are implied based on the software installed/found on the machine and their version.)

Activities Firefox Jan 29 11:34

3482-w24 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Maltego Community Edition 4.4.1

Investigate View Entities Collections Transforms Machines Collaboration Import Screenshot taken

Number of Results Privacy Mode Quick Find Find in Files Entity Selection

Entity ... X Home New Graph (1) * New Graph (1) * New Graph (1) * Overview X

Search: Recent... Layout Domain An internet Infrastru... DNS Nam Domain Na Domain An internet STIK2 Do... The Domai Run Vi... X

Freeze View View

<No Selection>

Entity Selection

Machine completed

runASNumberToCompel Machine completed with

Detail View X

<No Selection>

X Hub Tra...

<No Properties>

37 entities, 51 links

FOOD FOR THOUGHT

More information about the nature of various footprint options in Maltego can be found from: <https://www.maltego.com/blog/network-footprinting-with-machines-in-maltego/>

7. Now, right-click on mail.eecs.yorku.ca email entity (icon C). In the Run Transforms window select All Transforms (click on + symbol to see all sub-options), and then click on To IP Addresses [DNS] sub-ption. This will reveal the IP address of the actual machine on which EECS's email server runs, which will also help you determine whether the main Web and the main email server of EECS domain are hosted on the same physical machine, which would be helpful if one is to perform a simultaneous attack on both the web and email server of www.eecs.yorku.ca domain.

8. Next, right-click on the machine / IP entity affiliated with www.eecs.yorku.ca domain icon (icon B). In the Run Transforms window select All Transforms (click on + symbol) -> To Location [city, country] option. This will reveal the geographic location at which the given machine is situated.

9. Again right-click on the machine / IP entity affiliated with www.eecs.yorku.ca. In the Run Transforms window, move the mouse to To Vulnerabilities [Shodan Internet DB] (as shown below left), and click on the arrow at the right-end of this option (Run All - as shown below left, observe the location of red arrow). This will generate a graph (as shown below right) which contains icons representing the instances of software running on the given machine (including their version), the open port numbers, as well as their known associated CVE vulnerabilities. (Note, the machine may not be impacted by all the enlisted vulnerabilities. The vulnerabilities are implied based on the software installed/found on the machine and their version.)

Page 4 of 4 324 words, 1,902 characters Default Page Style

Assignment 1 - CSE3482

https://eclass.yorku.ca/pluginfile.php/5936149/mod_resource/content/3

14 of 15 Automatic Zoom

Highlight All Match Case Match Diacritics Whole Words 17

Activities Firefox Jan 29 11:34

3482-w24 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Maltego Community Edition 4.4.1

Investigate View Entities Collections Transforms Machines Collaboration Import Screenshot taken

Number of Results Privacy Mode Quick Find Find in Files Entity Selection

Entity ... X Home New Graph (1) * New Graph (1) * New Graph (1) * Overview X

Search: Recent... Layout Domain An internet Infrastru... DNS Nam Domain Na Domain An internet STIK2 Do... The Domai Run Vi... X

Freeze View View

<No Selection>

Entity Selection

Machine completed

runASNumberToCompel Machine completed with

Detail View X

<No Selection>

X Hub Tra...

<No Properties>

37 entities, 51 links

FOOD FOR THOUGHT

More information about the nature of various footprint options in Maltego can be found from: <https://www.maltego.com/blog/network-footprinting-with-machines-in-maltego/>

7. Now, right-click on mail.eecs.yorku.ca email entity (icon C). In the Run Transforms window select All Transforms (click on + symbol to see all sub-options), and then click on To IP Addresses [DNS] sub-ption. This will reveal the IP address of the actual machine on which EECS's email server runs, which will also help you determine whether the main Web and the main email server of EECS domain are hosted on the same physical machine, which would be helpful if one is to perform a simultaneous attack on both the web and email server of www.eecs.yorku.ca domain.

8. Next, right-click on the machine / IP entity affiliated with www.eecs.yorku.ca domain icon (icon B). In the Run Transforms window select All Transforms (click on + symbol) -> To Location [city, country] option. This will reveal the geographic location at which the given machine is situated.

9. Again right-click on the machine / IP entity affiliated with www.eecs.yorku.ca. In the Run Transforms window, move the mouse to To Vulnerabilities [Shodan Internet DB] (as shown below left), and click on the arrow at the right-end of this option (Run All - as shown below left, observe the location of red arrow). This will generate a graph (as shown below right) which contains icons representing the instances of software running on the given machine (including their version), the open port numbers, as well as their known associated CVE vulnerabilities. (Note, the machine may not be impacted by all the enlisted vulnerabilities. The vulnerabilities are implied based on the software installed/found on the machine and their version.)

Page 4 of 4 324 words, 1,902 characters Default Page Style

Assignment 1 - CSE3482

https://eclass.yorku.ca/pluginfile.php/5936149/mod_resource/content/3

14 of 15 Automatic Zoom

Highlight All Match Case Match Diacritics Whole Words 17

I would be more successful in doing the DDoS attack for the mcmaster server as it is easier. It only has 1 server.