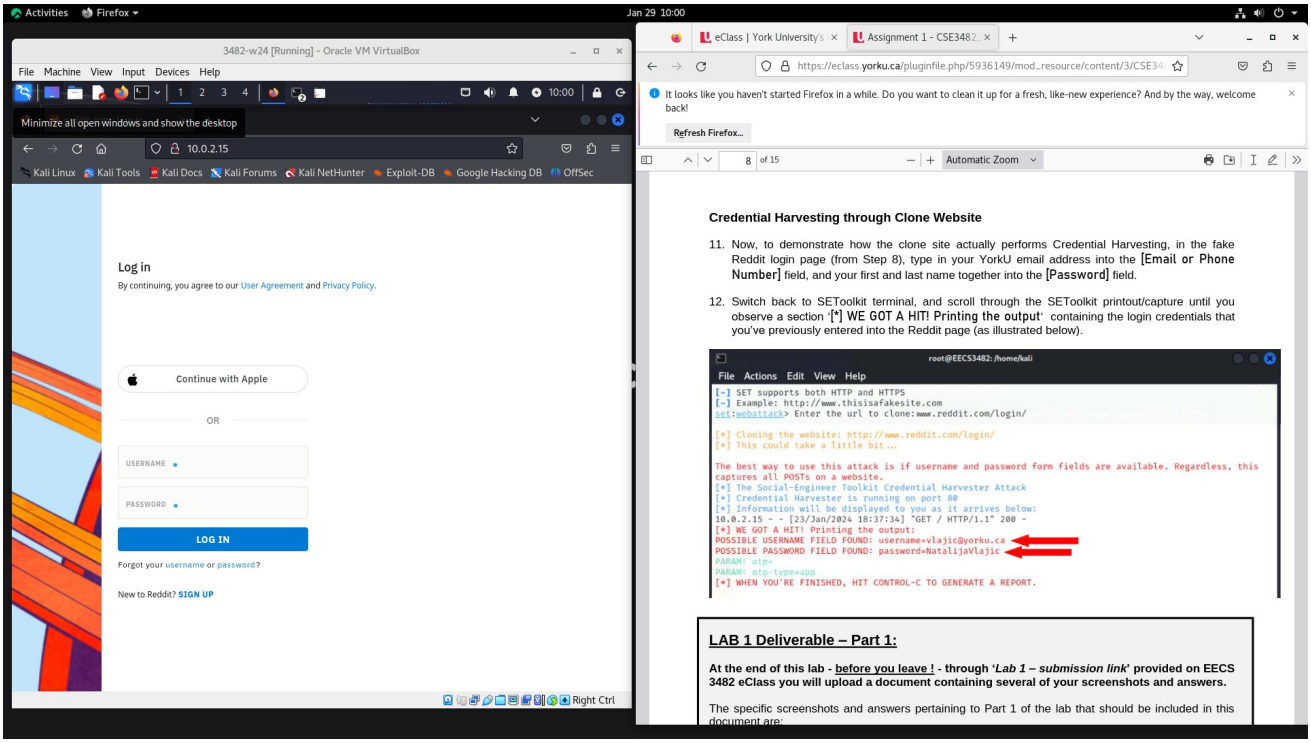
EECS 3482 – LAB 1

NAME: Stuti Parmar
STUDENT ID: 218516625

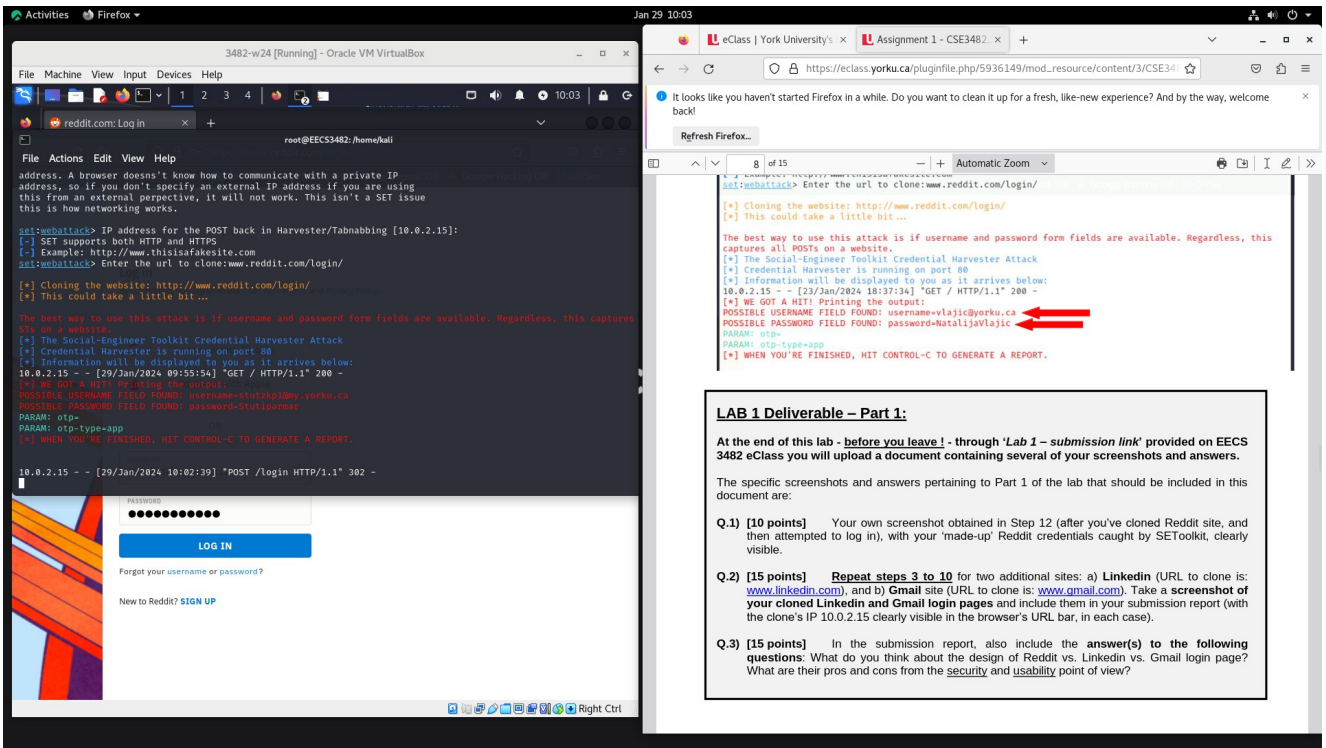
PART 1

Q.1)

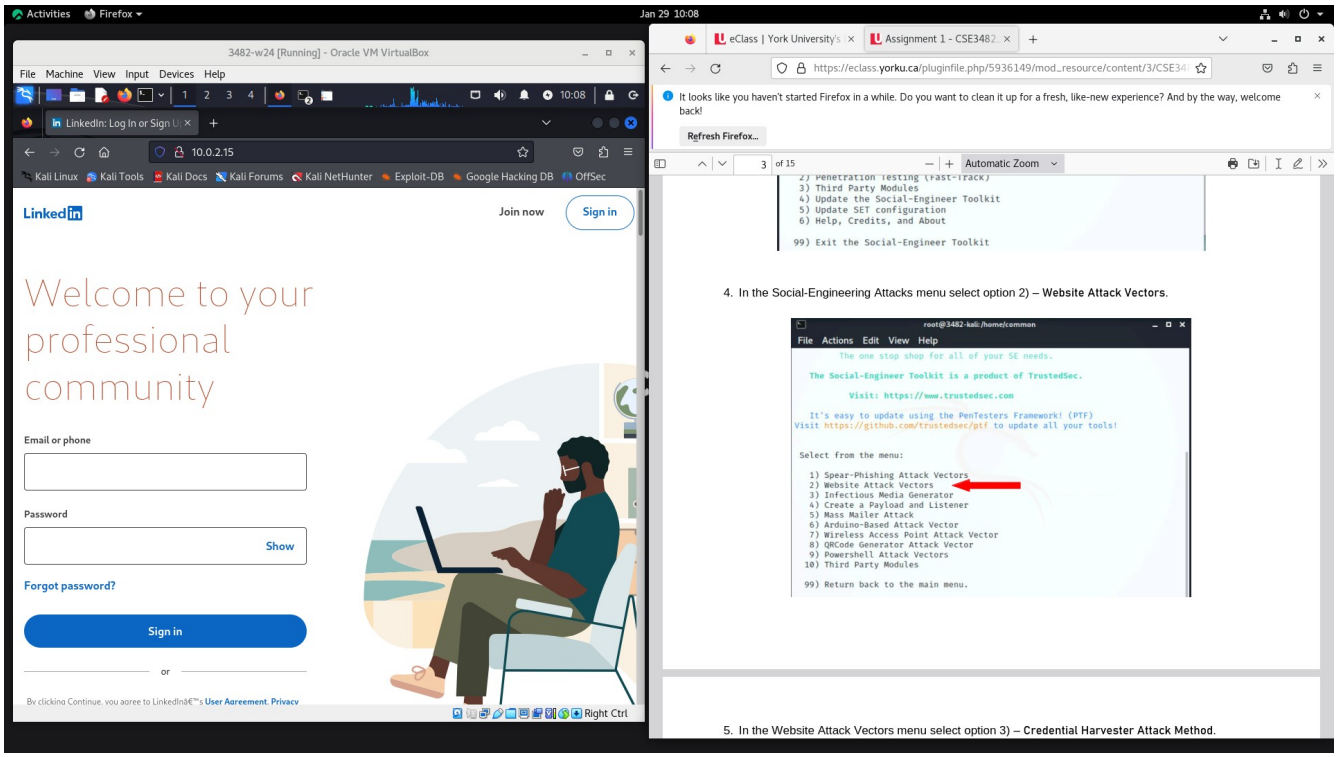
Screenshot of Reddit website login page:



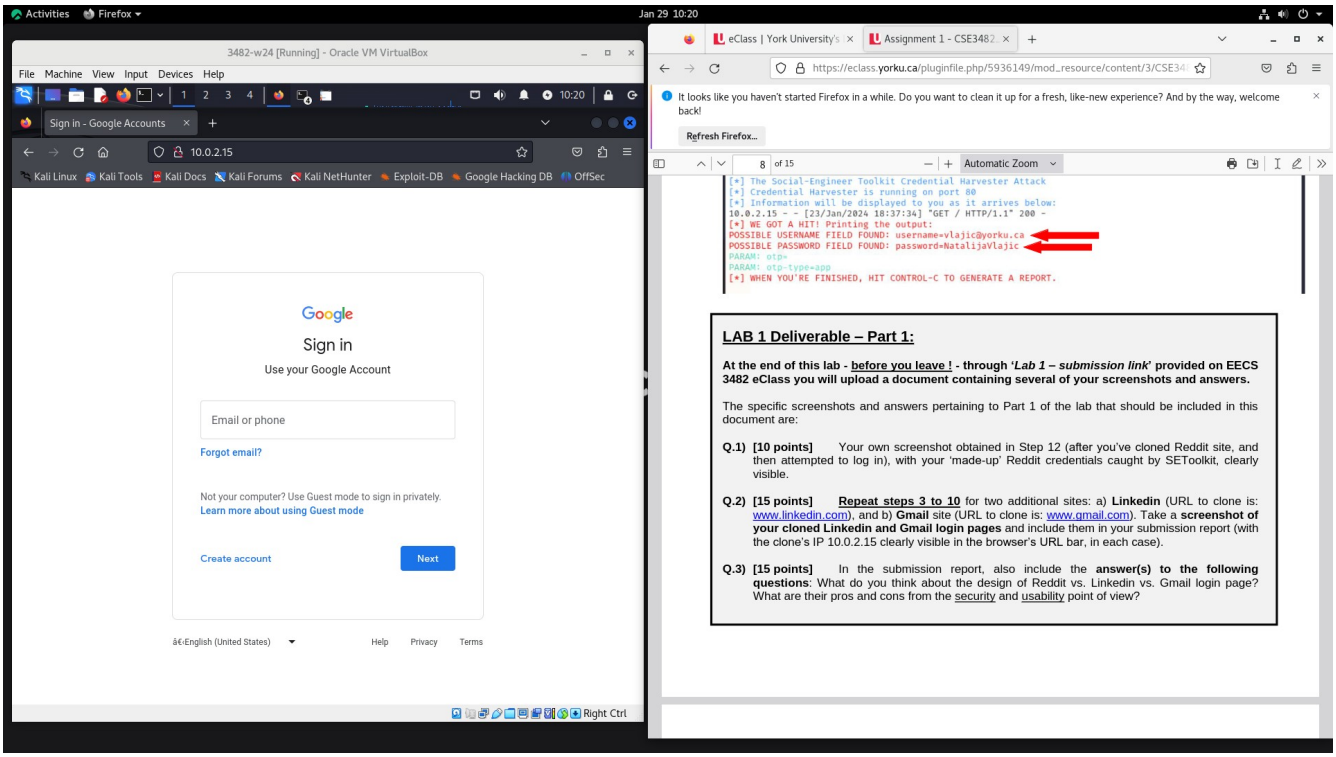
Screenshot of Step 12:



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 LinkedId 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).

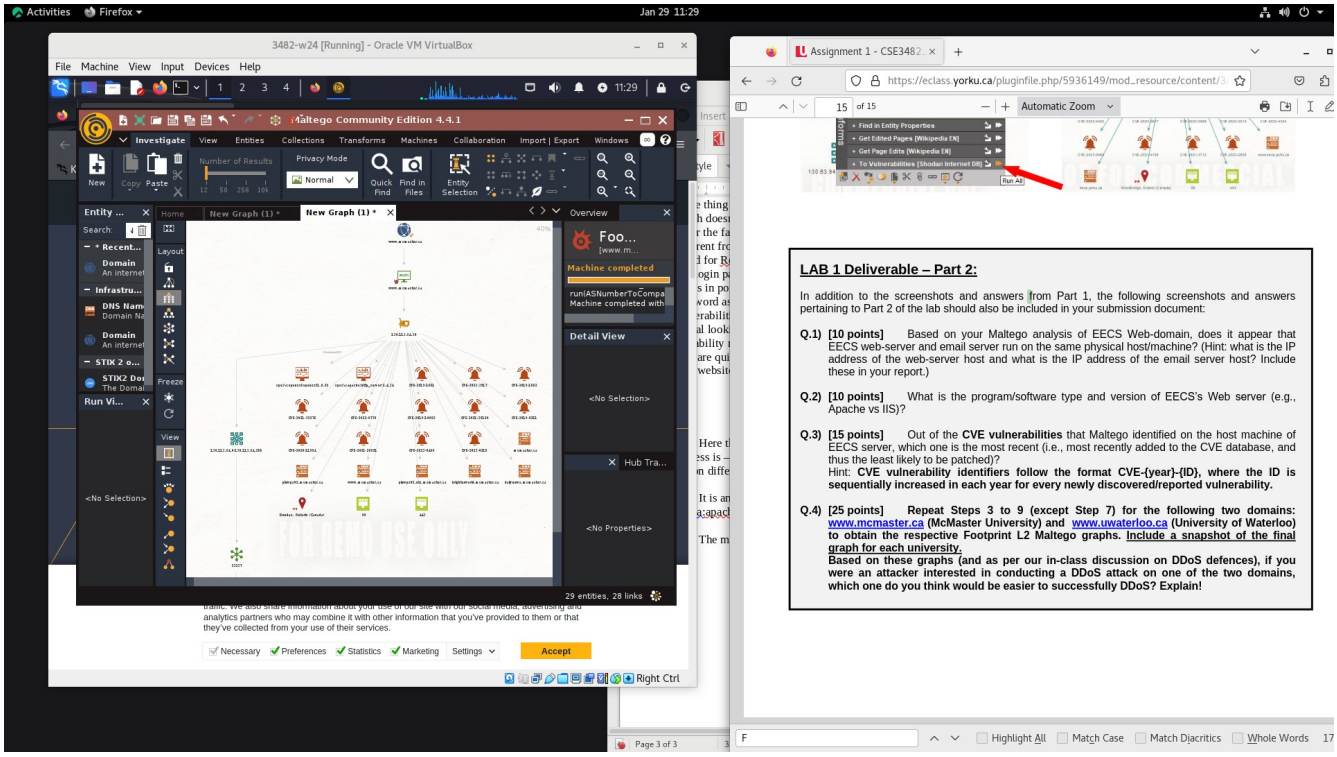
PART-2

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.

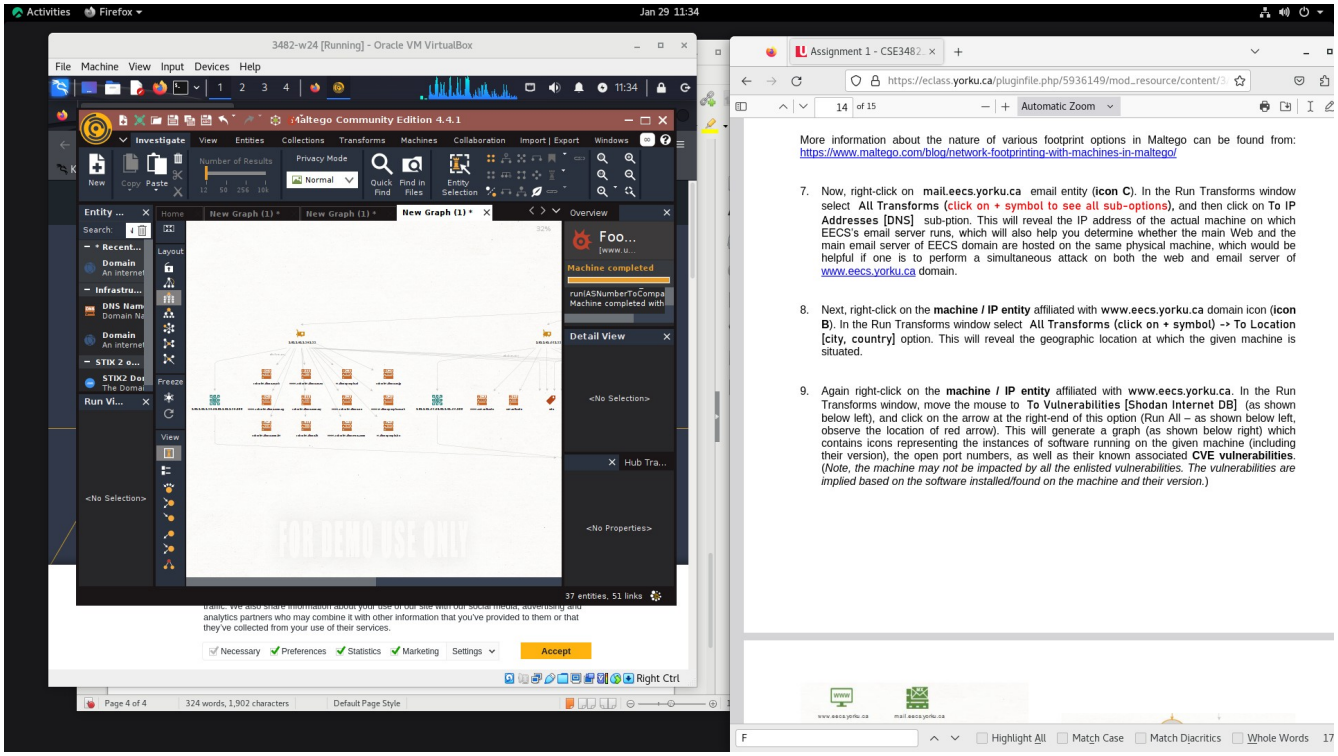
Q.2) It is an Apache software/program and the version of EECS's Web Server is – cpe:/a:apache:http_server:2.4.58

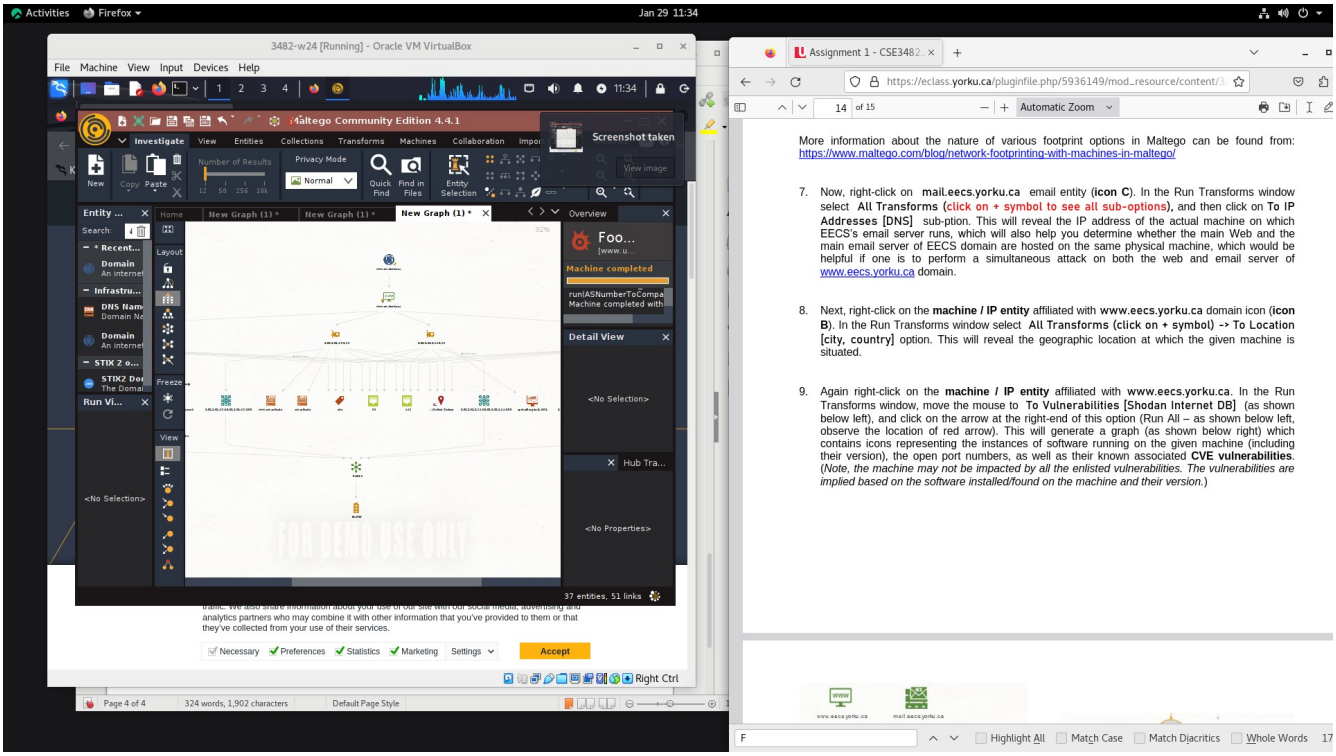
Q.3) The most recent CVE vulnerability is – CVE-{2023}-{5678}

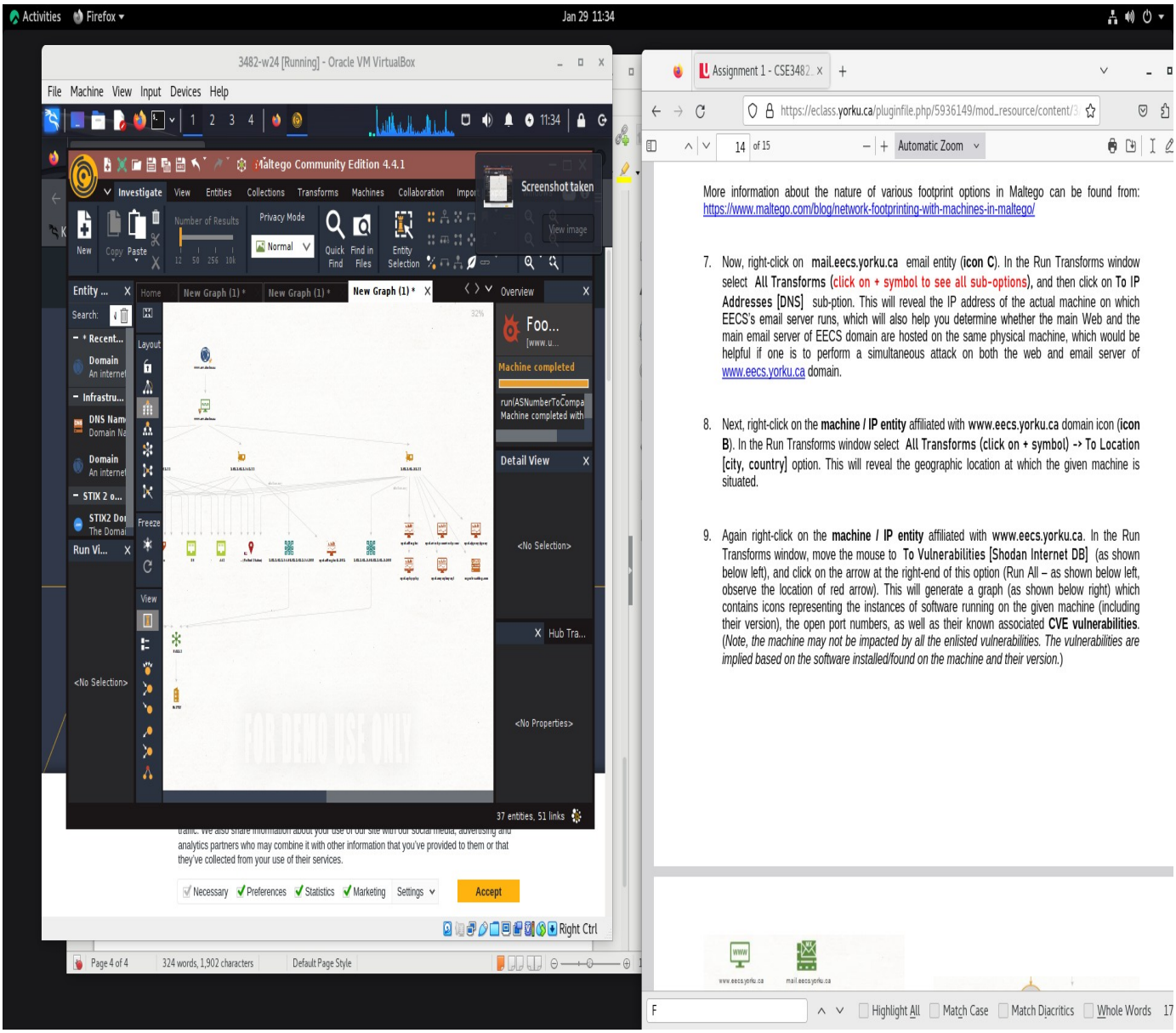
Q.4) Screenshot of www.mcmaster.ca :



Screenshot of www.uwaterloo.ca:




Activities
Firefox
Jan 29 11:34
3482-w24 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Maltego Community Edition 4.4.1
Screenshot taken
FOR DEMO USE ONLY
Assignment 1 - CSE3482
https://eclass.yorku.ca/pluginfile.php/5936149/mod_resource/content/3
14 of 15
Automatic Zoom
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.)
Highlight All
Match Case
Match Diacritics
Whole Words


Activities
Firefox
Jan 29 11:34
3482-w24 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Maltego Community Edition 4.4.1
Screenshot taken
FOR DEMO USE ONLY
Assignment 1 - CSE3482
https://eclass.yorku.ca/pluginfile.php/5936149/mod_resource/content/3
14 of 15
Automatic Zoom
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.)
Highlight All
Match Case
Match Diacritics
Whole Words

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