This assignment uses a GCU-provided virtual machine that will be specified by your instructor.

Websites are the most vulnerable services on an organization's network. Performing a vulnerability assessment on these services is critical. Often a compromised website/server is the perfect jumping off point for an attacker to pivot into the rest of a network.

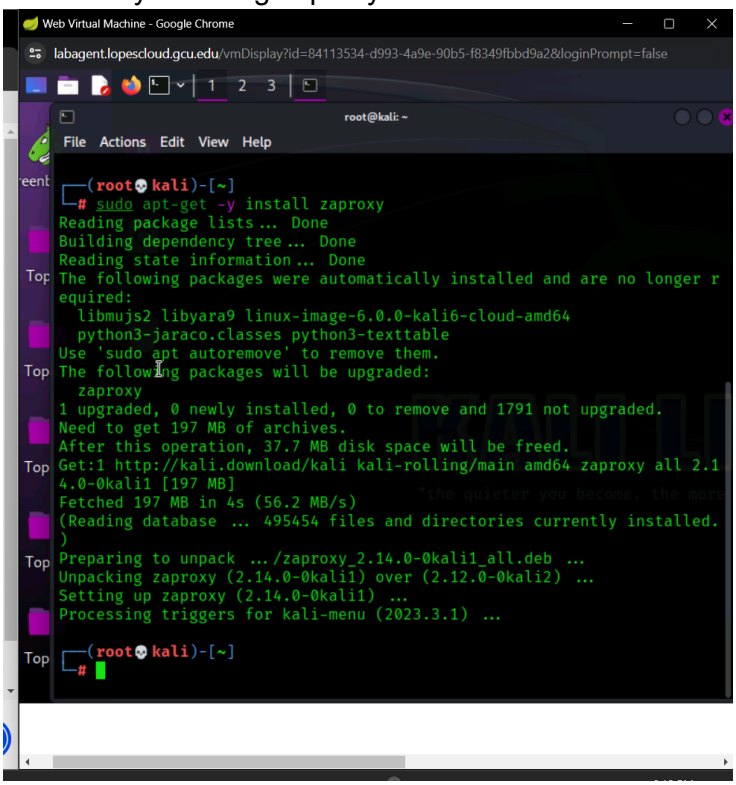
1. Using the GCU-provided virtual machine and OWASP ZAP or other website vulnerability assessment tool available in Kali Linux, perform a website vulnerability assessment on the Metasploitable 2 VM.
2. Document your findings under Phase Testing in the "ITT-340 PEN Testing Report Guidelines," located in Class Resources. Refer to "Writing a Penetration Testing Report," by the SANS Institute, located in Class Resources, for examples of PEN testing reports.
3. Append this assignment to the PEN testing report and resubmit the report (Passive Corporate Recon + Automating Information RECON + NMap Scan + Vulnerability Assessment + Applied Exploitation using Metasploit + Custom Payload + Website Vulnerability Assessment).

While APA style is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.

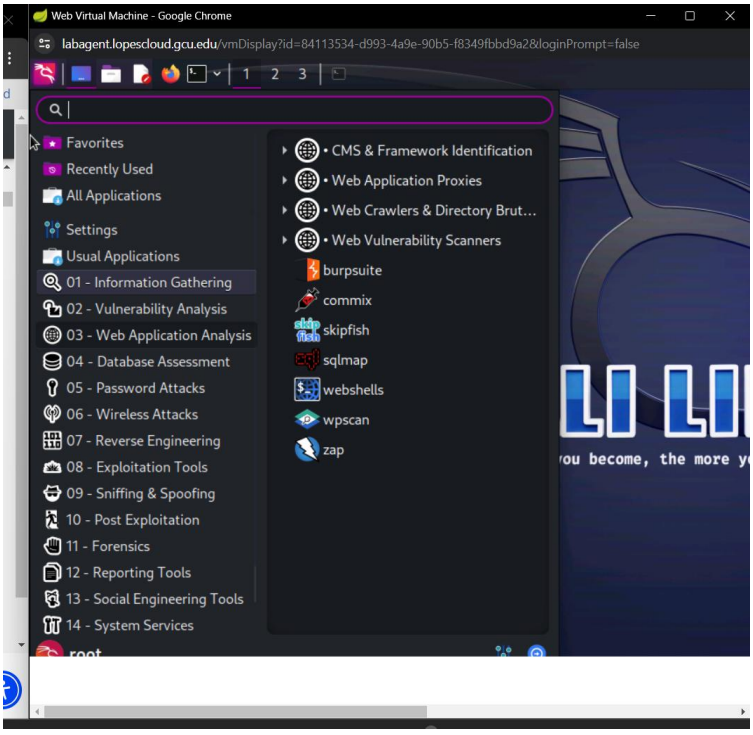
This assignment uses a rubric. Please review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are not required to submit this assignment to LopesWrite.

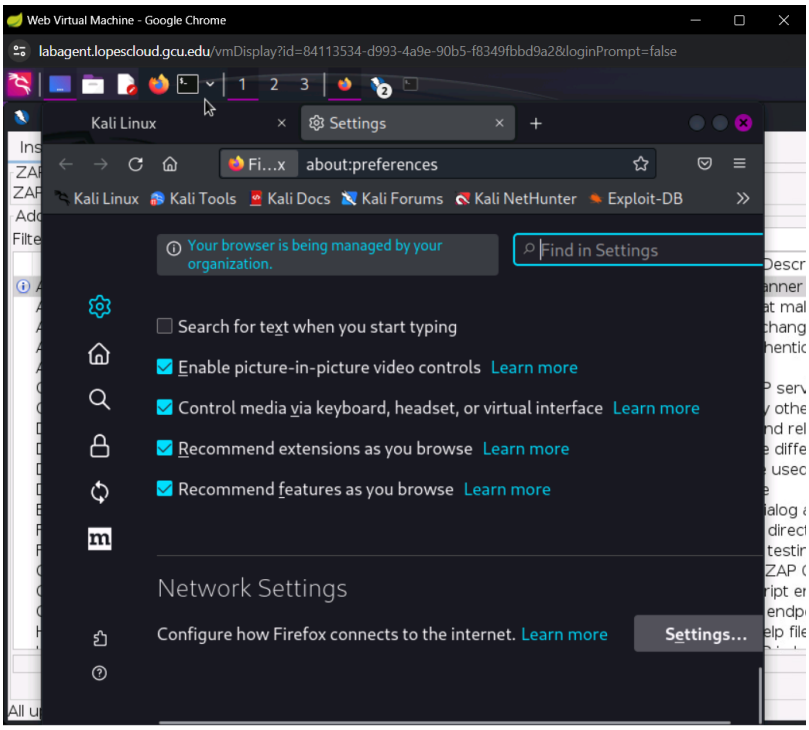
I started by installing zaproxy:

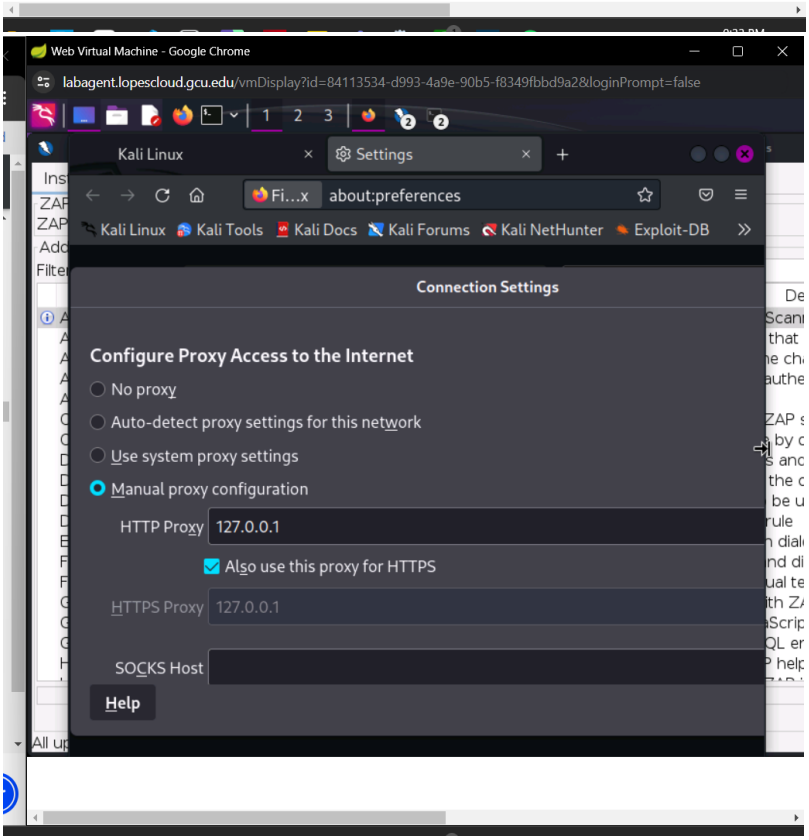


I then opened the application and my browser:



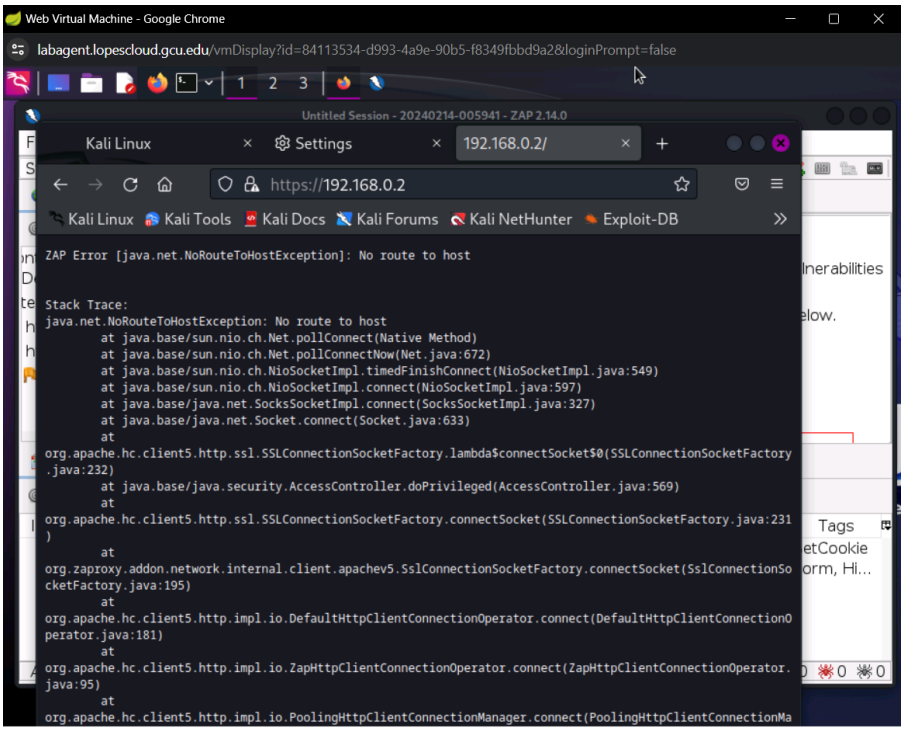
Before proceeding to any other steps I needed to make sure that the network settings were properly configured so that the LHOST was set my VM's local host: 127.0.0.1 and port 8080



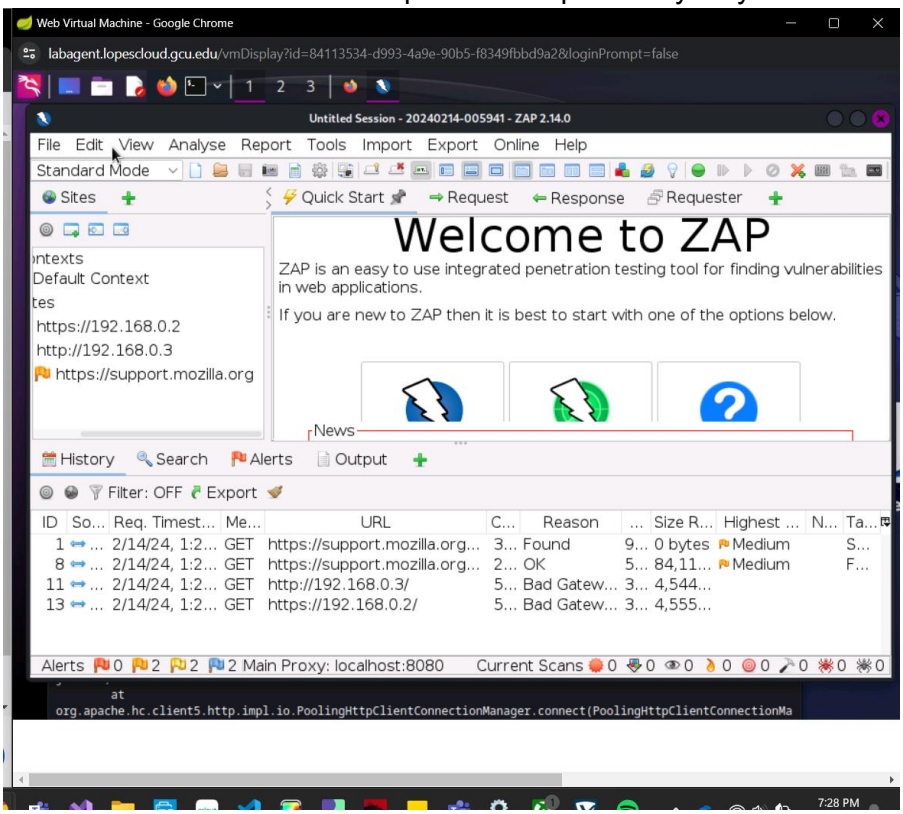


After configuring the settings I opened a new tab to go to the ip address for the metasploitable 2: 192.168.0.2.

After going to advanced and accepting the risk and continuing it led this error:



We are now able to see the requests on zap but they only showed the failed requests:



I checked my settings once again and even tried to restart my LopesCloud and restart the browser but it still led to the same failures- I am thinking the lab was malfunctioning or just down

when trying to connect. I also tried different IP addresses just to makes sure it wasn't the one website. (192.168.0.3 and 192.168.0.2 and 192.168.122.148):