Franklin Nuth

CSC432 – A

Lab #7 – Web Server Security

8 March 2019

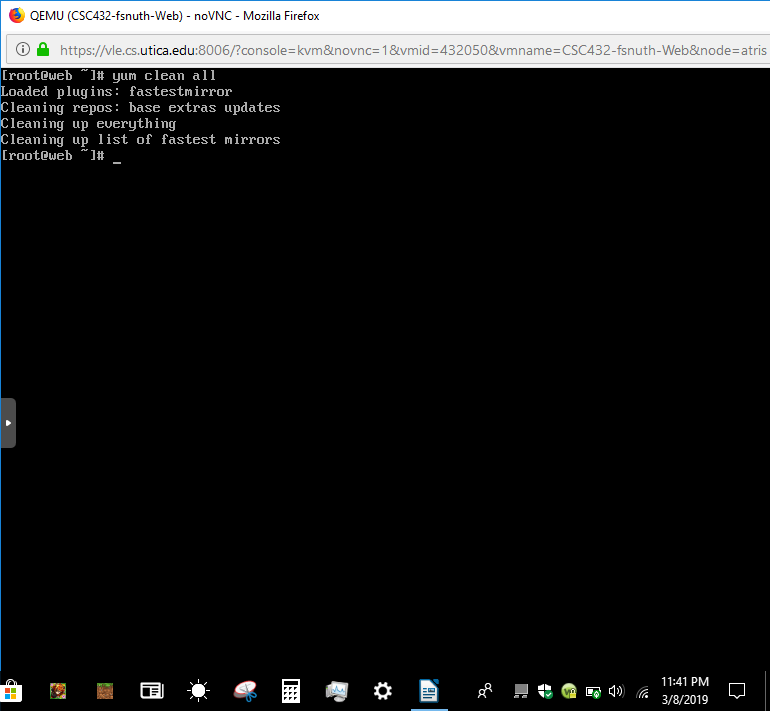
**Abstract**

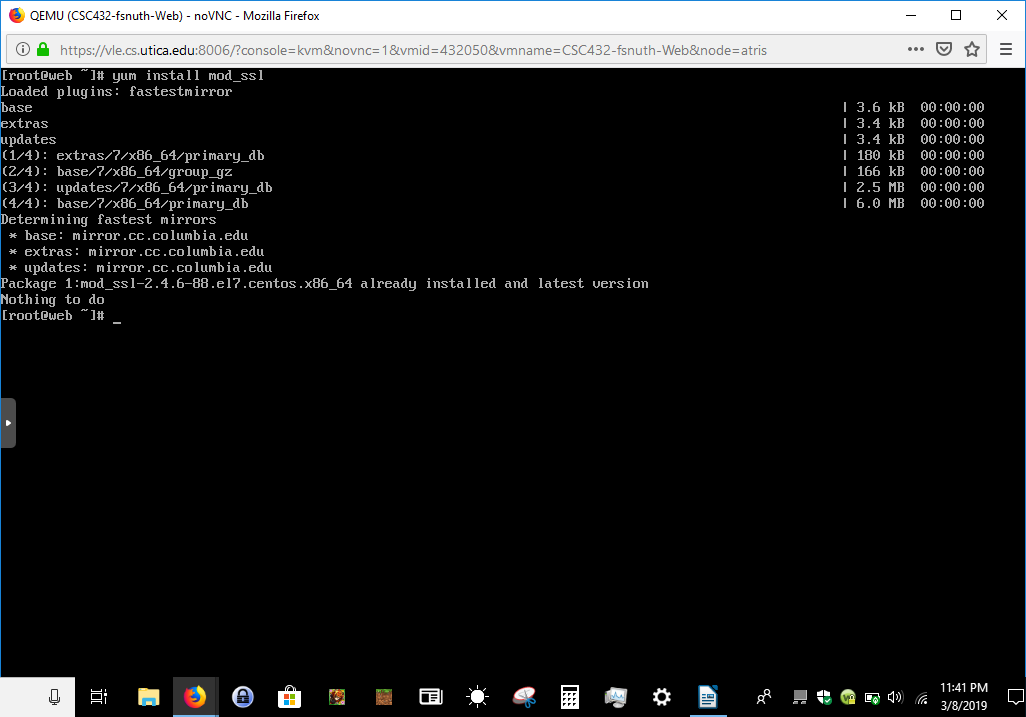
In this lab, I will be talking about how to configure the web server so that it will support encrypted web traffic over HTTPS as well as locking down web content with .htaccess files. I will be setting up the web server so that it supports encryption PKI certificates. I will also install an Apache HTTPS service so the web server can be modified for our own needs. The credential files created in the process shall be protected with a username and password for security.

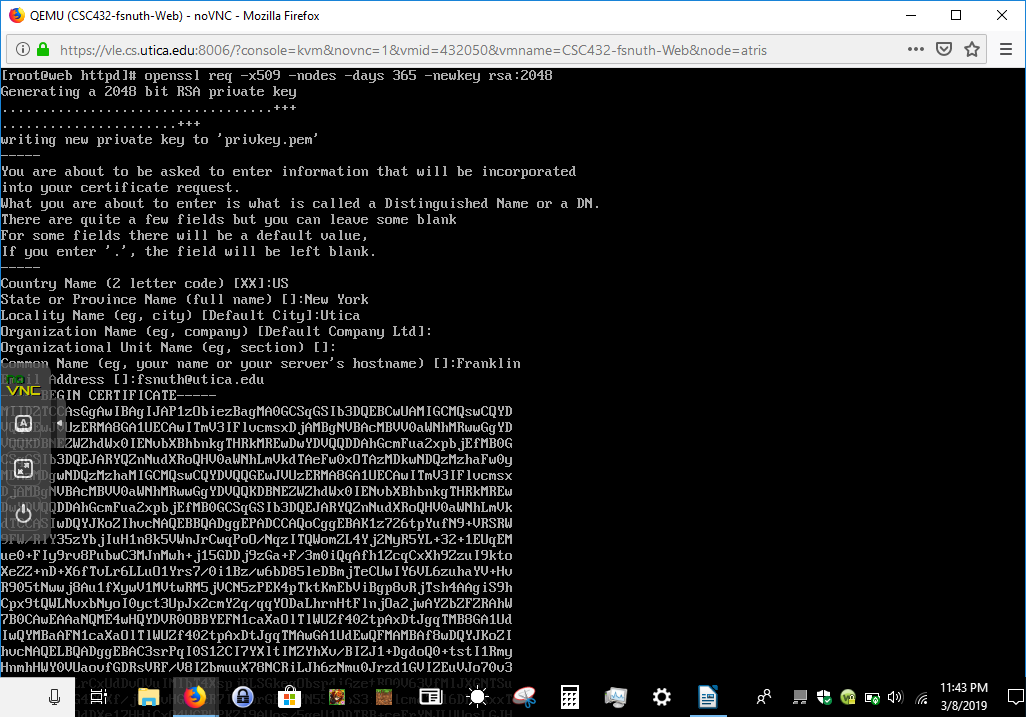
**Introduction**

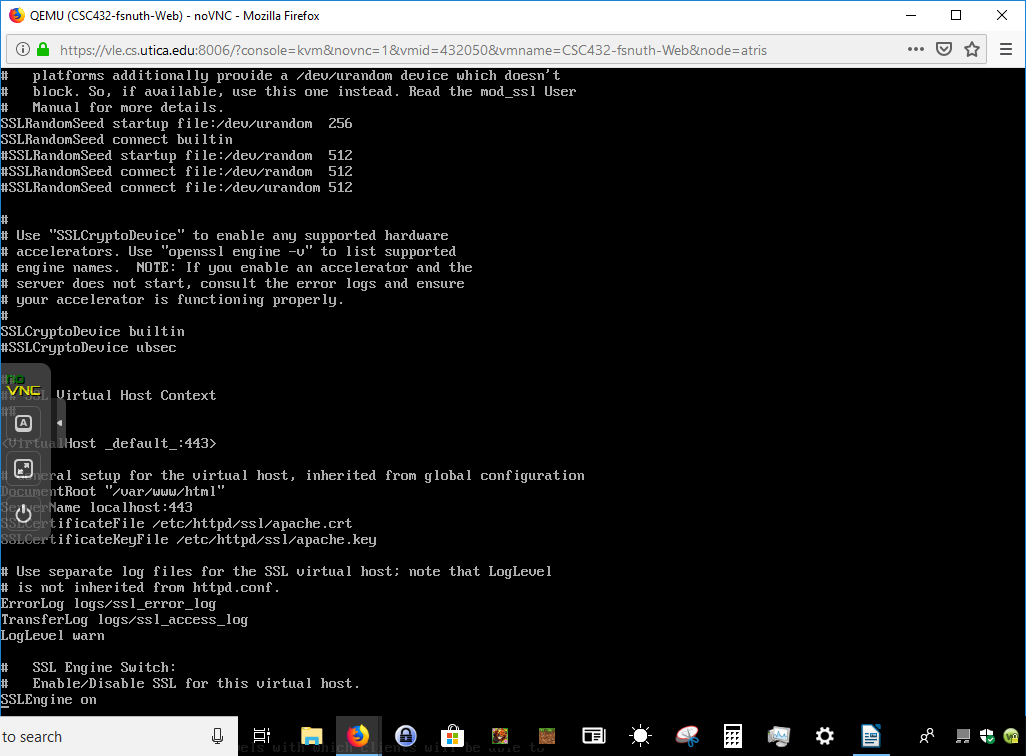
There is an abundant amount of web servers in the world out there today. They can be changed for serving as a giant library of sources and information like Google, or for entertainment purposes like Twitch. Another thing that these public web servers have in common is the high standard of security that is often changing with the times. Many changes must be made such as switching from Telnet to SSH, or seeing how many firewalls can be installed for maximum security. I will now experience the technical toil that these developers go through to reduce and eliminate the flaws in the security of their web servers.

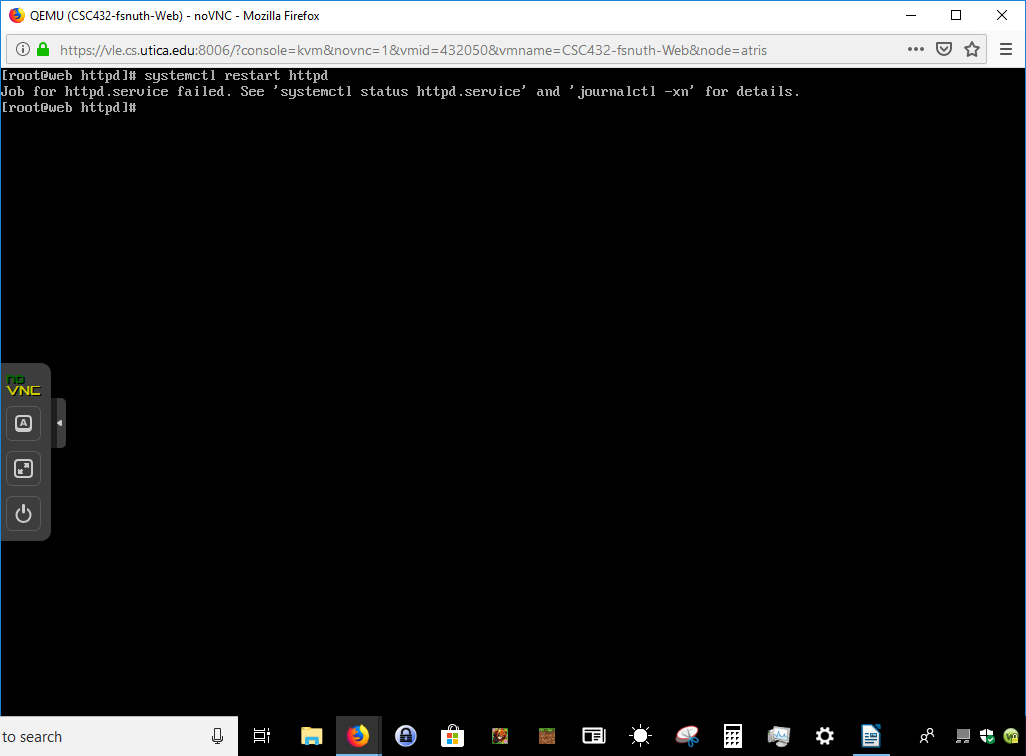
**Processes & Screenshots**



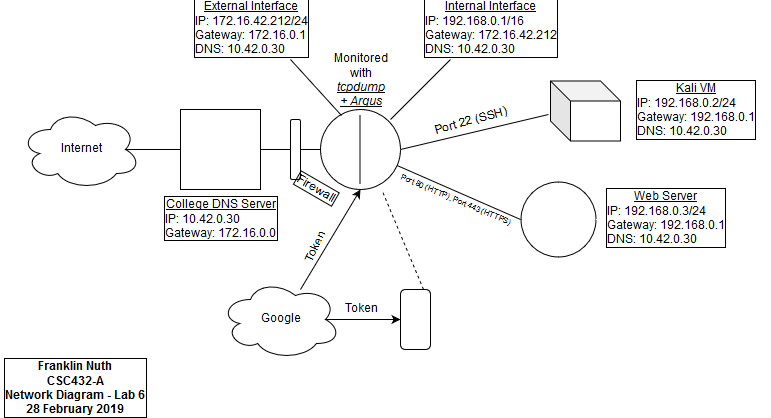
****

****

****

****

Apache Redirector with Valid SSL CERT

****

**Issues & Resolutions**

My one issue for this lab was that my web server was not working properly prior to this lab. When I enter the IP address of my web server in the Google Search bar, it said it was not working properly. I had to go back and redo my Lab 3 again so that my web server can be properly configured for installing Apache. My web server was still not up even when I made sure the configuration files were correct, so I had to lag behind a little bit to recheck everything again.

**Conclusion**

In this lab, I have installed Apache so that I can have the tools to configure my web server. I first made it more secure with a self-signed certificate, and allowed HTTPS service to run. I also updated my firewalls so that HTTPS is allowed through the router, as well as port-forward it to my web server. I have utilized .htaccess files so that users can have a place to store their usernames and passwords behind encrypted files. I then tested the web server to see if my credentials are stored and encrypted like it should be. This lab taught me that personal information can be handled responsibly with the right protcols and encryptions.