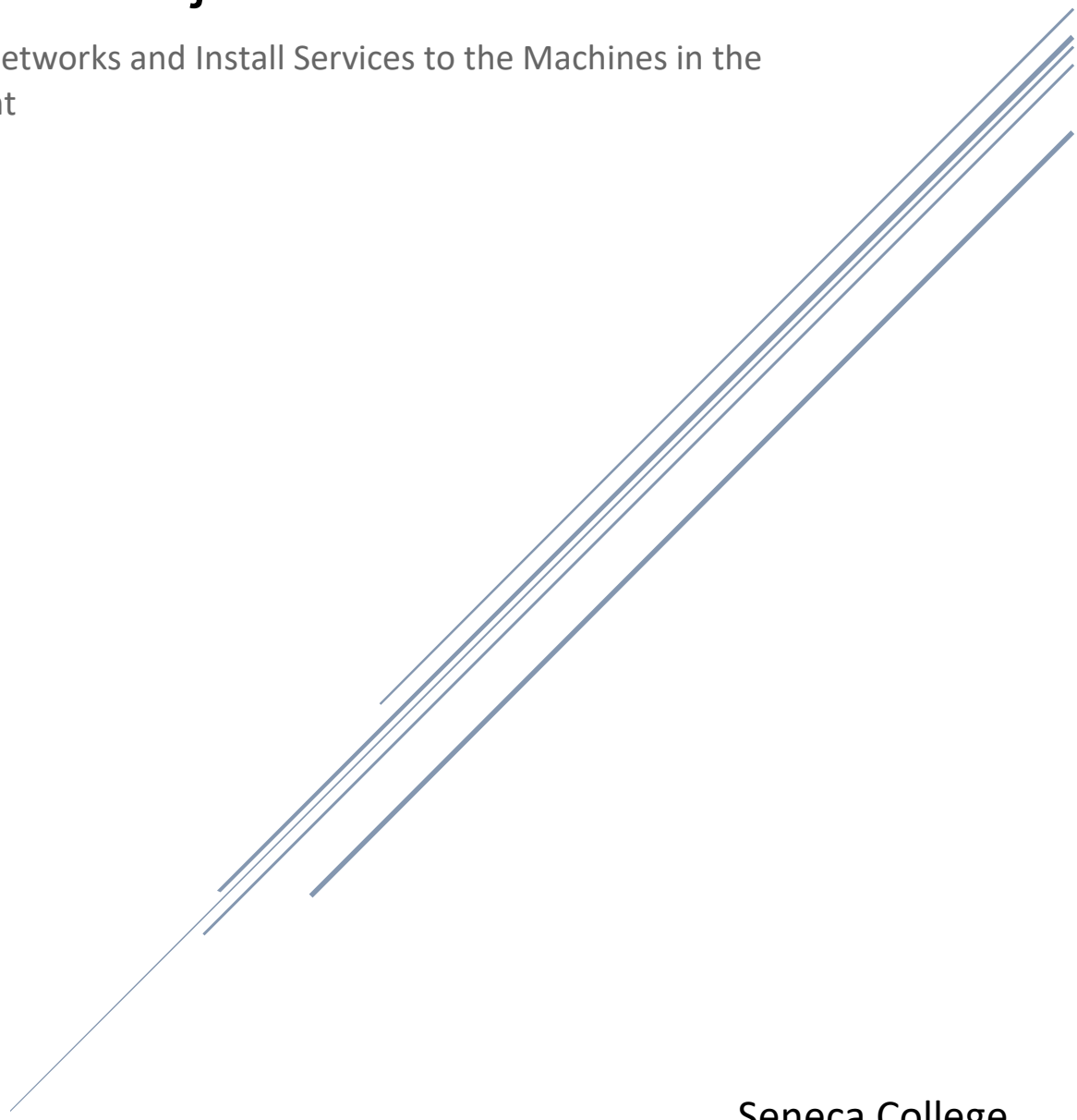
SRT 411 Project Phase 1

Configure Networks and Install Services to the Machines in the Environment



Seneca College

Group Members Associated with Configuring Project Phase 1

Professor Asma Paracha

Members

Ali Abdulkarim: 150706166

Murad Okasa: 108741208

Buwaneka Hettiarachchi: 104376165

College: Seneca College

Table of Contents

Introduction

This is the first of three phases of the final project deliverable of the SRT 411 course. This phase mainly focuses on the configuration of the virtual server environment and the installation of the many services into the virtual machines. Since this is the first phase of the report, our team faced many issues regarding setting up some services within the Lab Environment, these instances will be later discussed within the report. The Lab environment consists of six different virtual machines, Machine 1 is preinstalled with the CentOS software, and we are needed to install the snort service into the environment. Machine 2 runs as the Metasploitable machine, this machine doesn't need any services to be installed since it will act mainly as a vulnerable machine that can be used as a platform for various attacks. Machine 3 is another CentOS machine that needs to be installed with the LAMP server. Machine 4 is another CentOS machine that requires us to install the DVWA and WordPress into its platform. Machine 5 is the Kali Linux machine, this machine that comes with preinstalled OpenVAS and Nessus services, but we are required to configure the Nessus running on our Environment. Machine 6 is the Windows Machine which will be used as the machine that will host the Elasticsearch services. The Primary goal in this project phase is to complete and configure as much as we can.

IP configurations

The Table below shows all the configuration that took place in all the machines. The Machines are configured in three different interfaces, with all the machines running in the Repo Interface while some machines are configured in both the Attacker interface and the Log Interface.

Machine Number	Attack Interface IP	Repo Interface IP	Log Interface
1	Port Mirror	172.20.14.1	192.100.200.2
2	172.20.21.1	172.20.14.2	N/A
3	172.20.21.2	172.20.14.3	N/A
4	172.20.21.3	172.20.14.4	N/A
5	172.20.21.10	172.20.14.10	N/A
6	N/A	172.20.14.5	192.100.200.1

Table 1: Table showing the IP configurations

Machine 1 - Configurations

Machine 1 requires us to configure the IP addresses and install snort in its system. For this case I ran the script to configure the IP addresses provided from the script given to us. As shown in the configuration table, we configured the IP addresses on Both the Repo interface and the Log Interface.

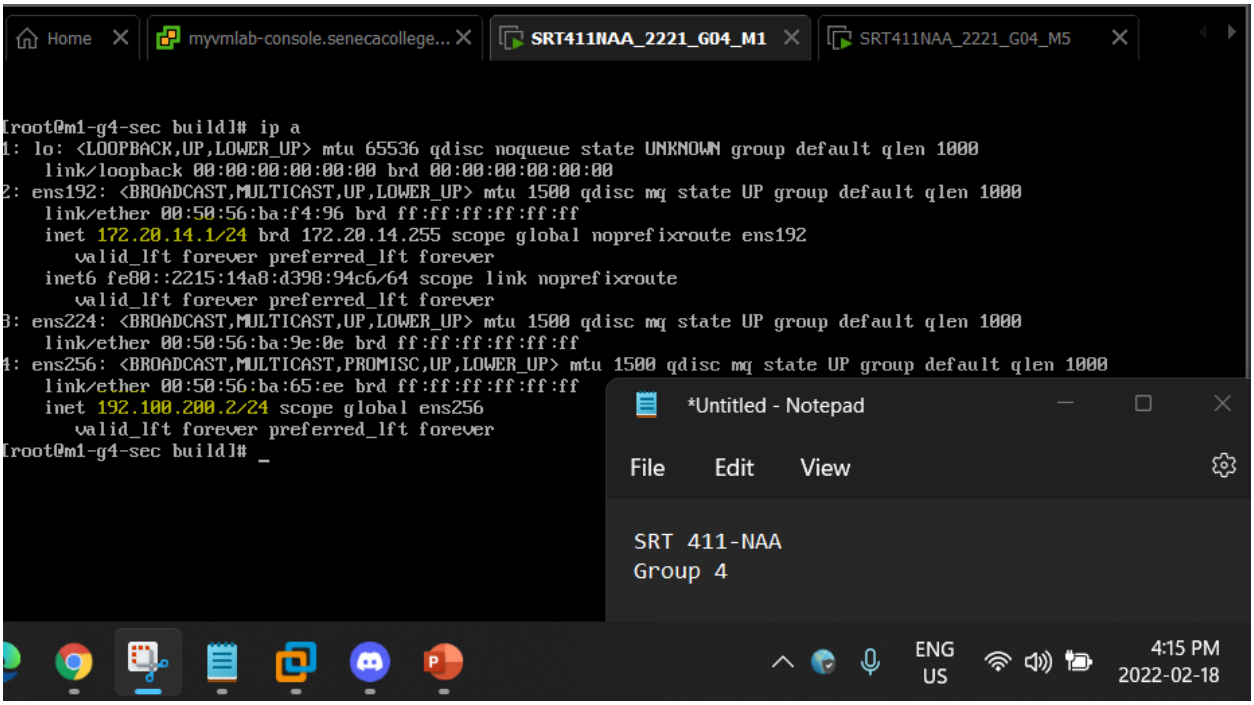


Figure 1: Ip configuration for Machine 1

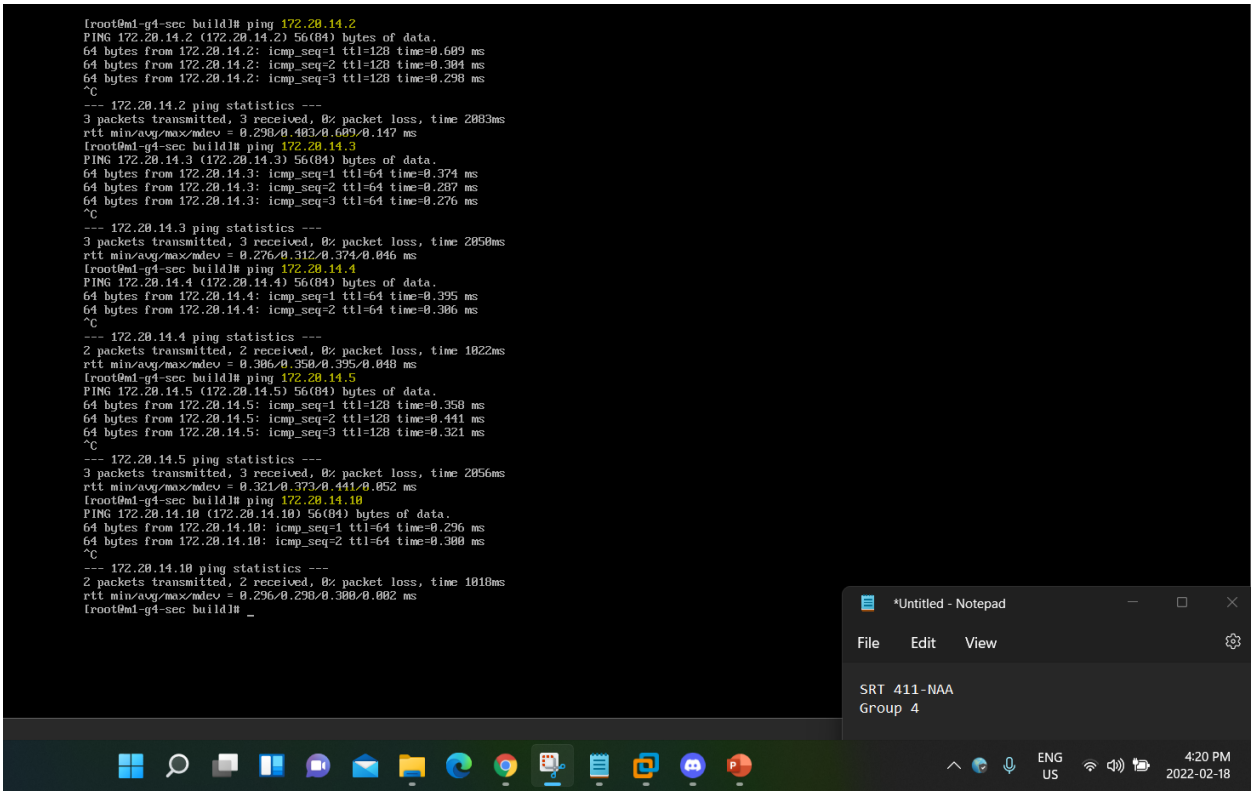


Figure 2: Machine 1 can ping all the machines within the Repo Interface

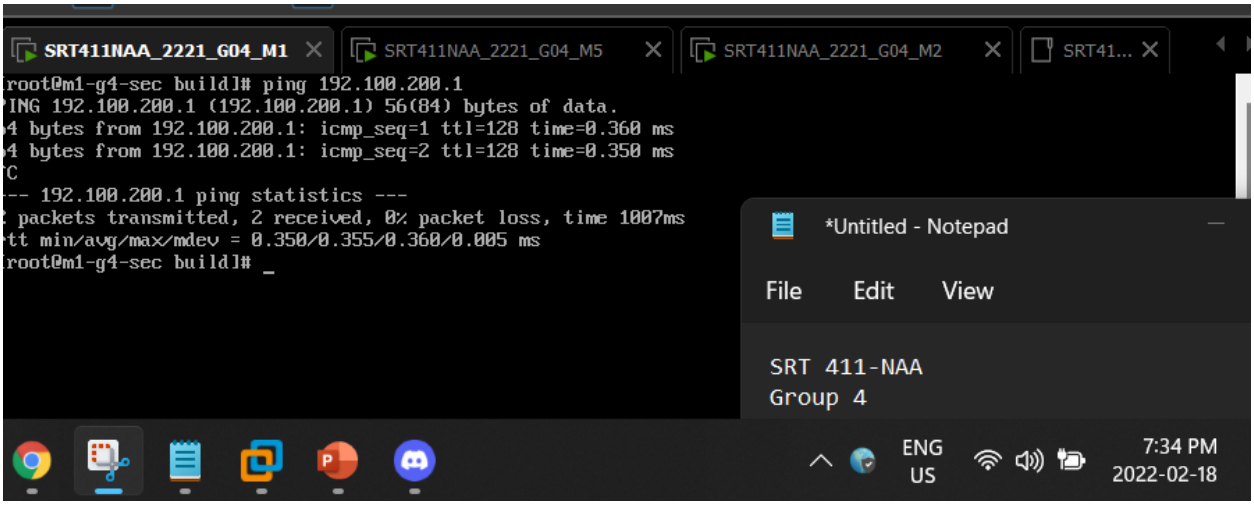


Figure 3: Machine 1 can communicate with machine 6 though the Log interface

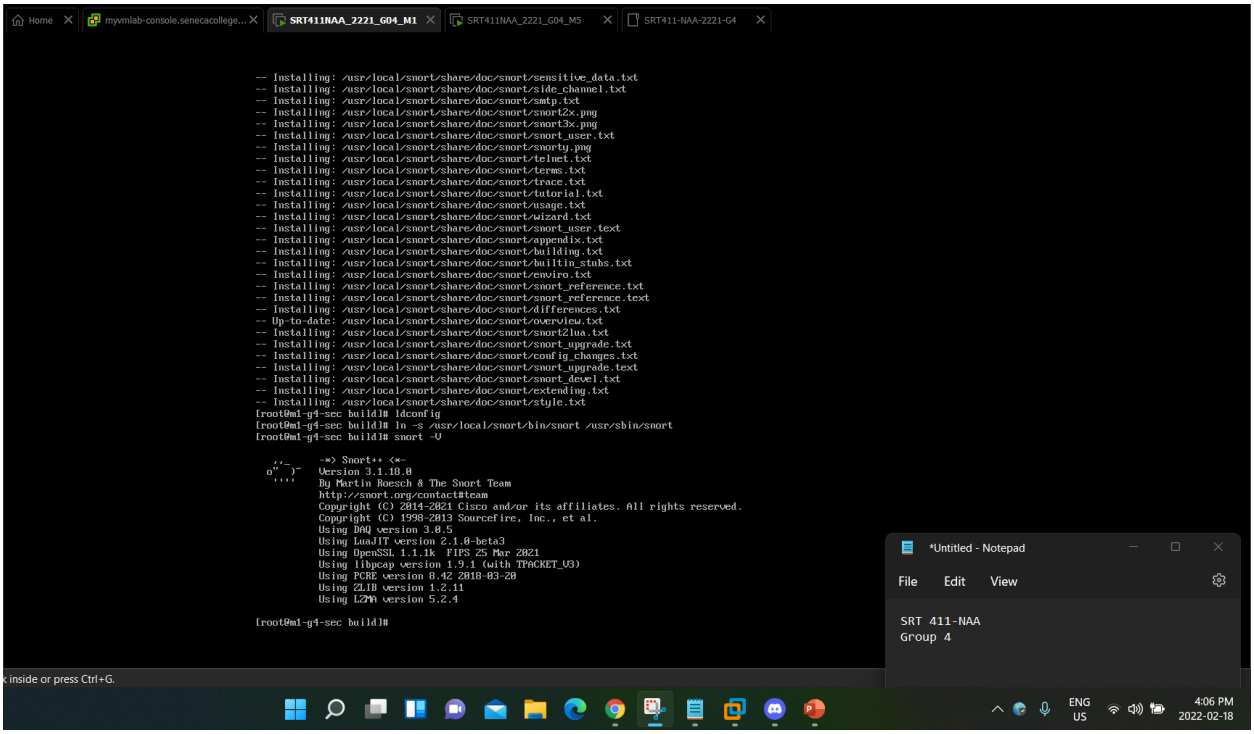


Figure 4: Snort Intrusion Detection System is successfully installed in the Machine 1 Environment

The above Figure shows that we were able to successfully install snort in our machine and that we will have the ability to pass logs into the Windows machine (Machine 6). The snort version that we installed was the third version of Snort, and it has already been configured with the dependencies such as Libdaq and Daq. For this phase we only installed and configured snort in our environment and we will use this in the future phases of our final project deliverable.

Machine 2 - Configurations

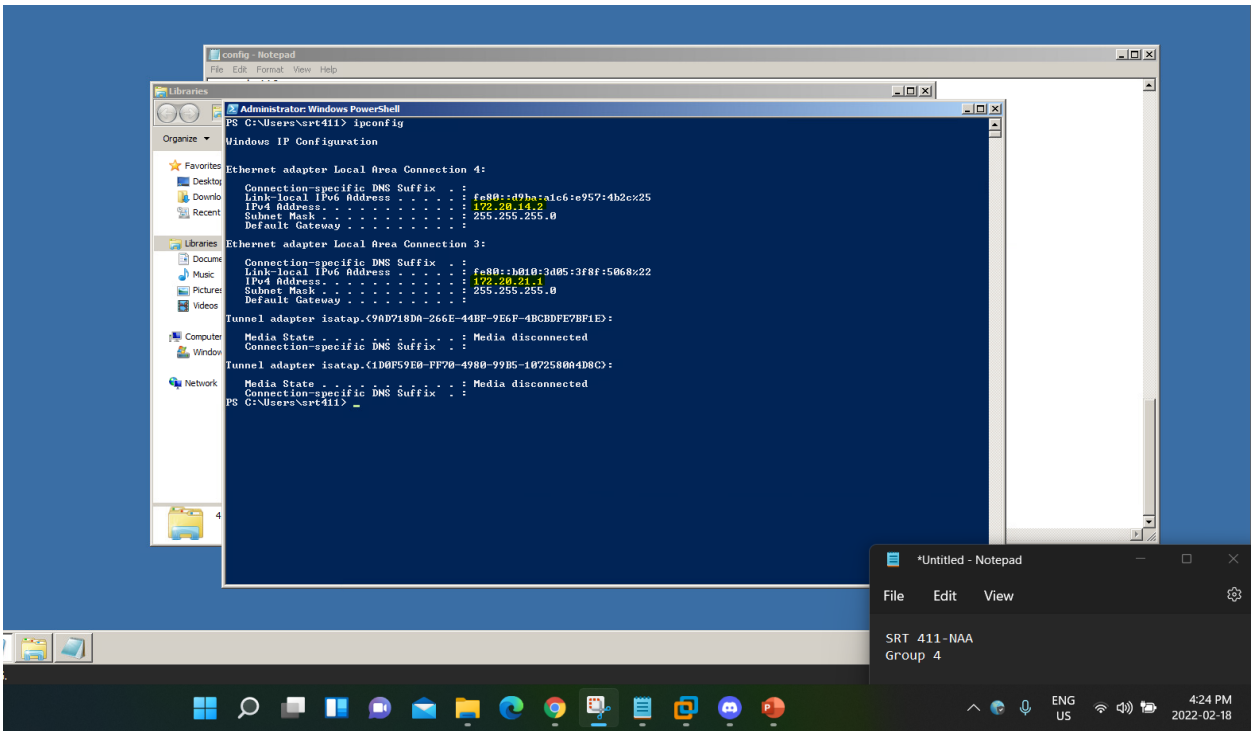


Figure 5: IP configurations for Machine 2

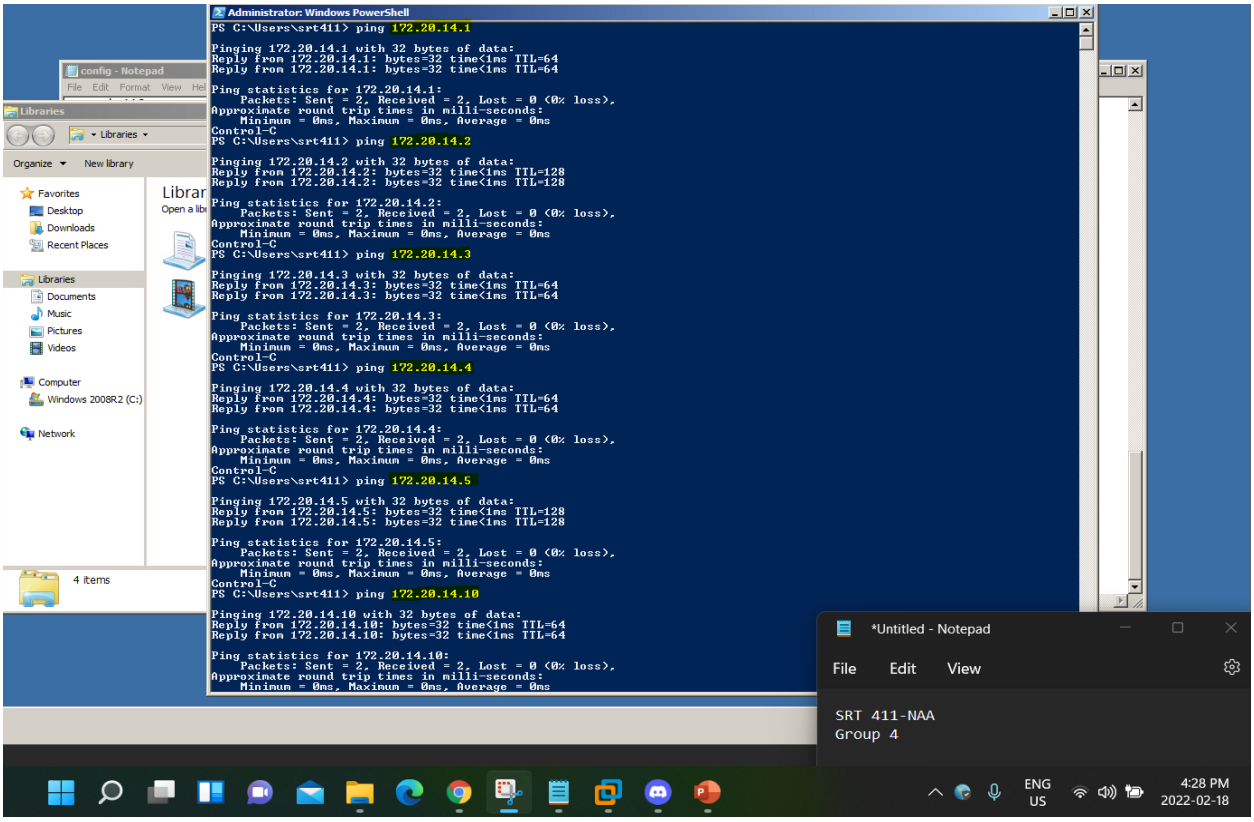


Figure 6: Machine 2 can ping all the machines within the Repo interface

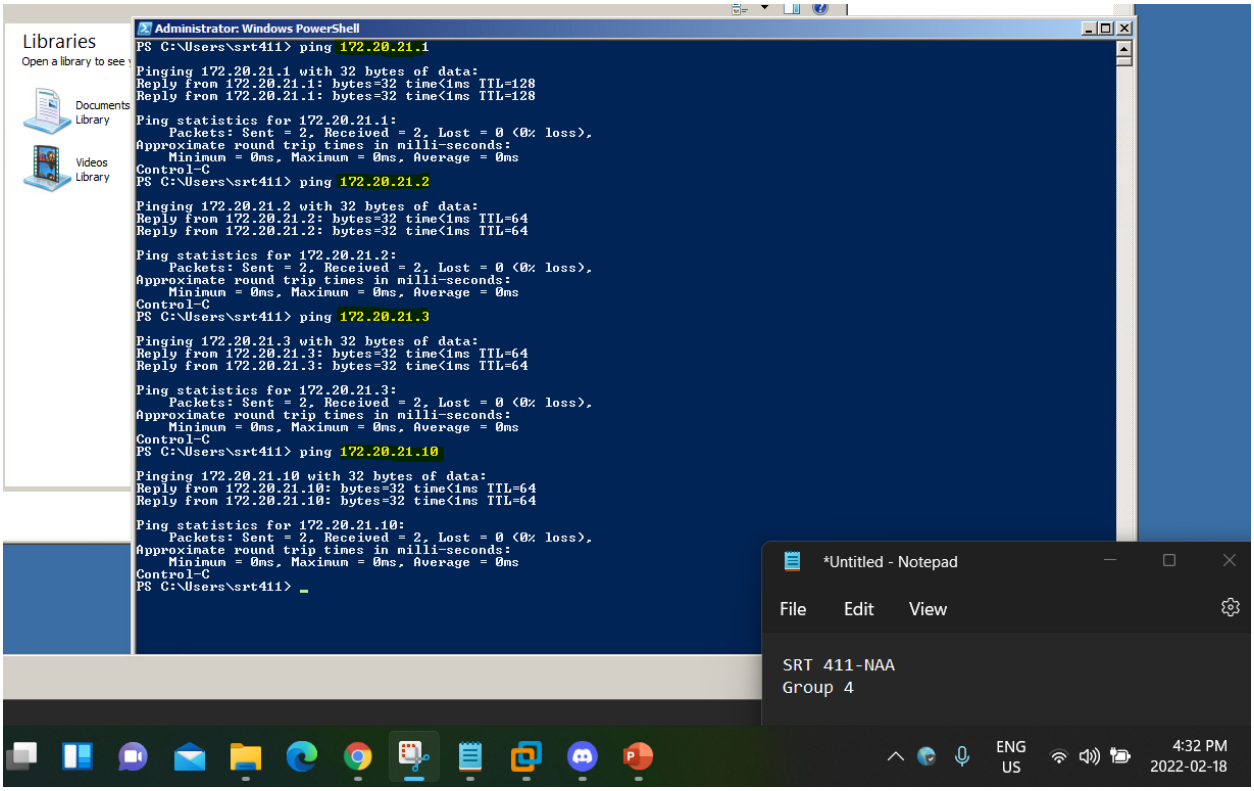


Figure 7: Machine 2 can communicate with all the machines from the attacker interface

Machine 2 is the Metasploitable 3 machine, for this case, we only needed to configure the IP addresses running within the environment, this machine is configured for both the Attacking Interface and the Repo interface. The Main purpose of this machine is to act as a vulnerable environment where we can perform various exploits and attacks within the environment. In this phase, the only requirement for this machine was to configure the IP addresses and check to see if the machine can access the repository environment and connect to the other machines, as shown in the above figures, the machine can successfully connect to the other machines and the repository environment. This machine also had a script that needed to be executed so that we can get the actual IP configurations on to the Machine.

Machine 3 - Configurations

This Machine runs as the LAMP server in our project Environment, the LAMP server is an acronym for Linux, Apache, MySQL, and PHP-MariaDB. As the name suggests, we are required to install all the services for Machine 3, excluding Linux, because CentOS is installed in the environment by default, and we are supposed to only install the other Requirements into the Machine. If you successfully install all the services, then your services should be present when you input the command to see whether these services are running or not. And As shown in the Figures below, we successfully configured and installed those services within the environment, and similarly to the machines before, we had to configure the IP addresses using the script provided to us, and this Machine also have two adapters running on the Attacker interface and the Repo interface.

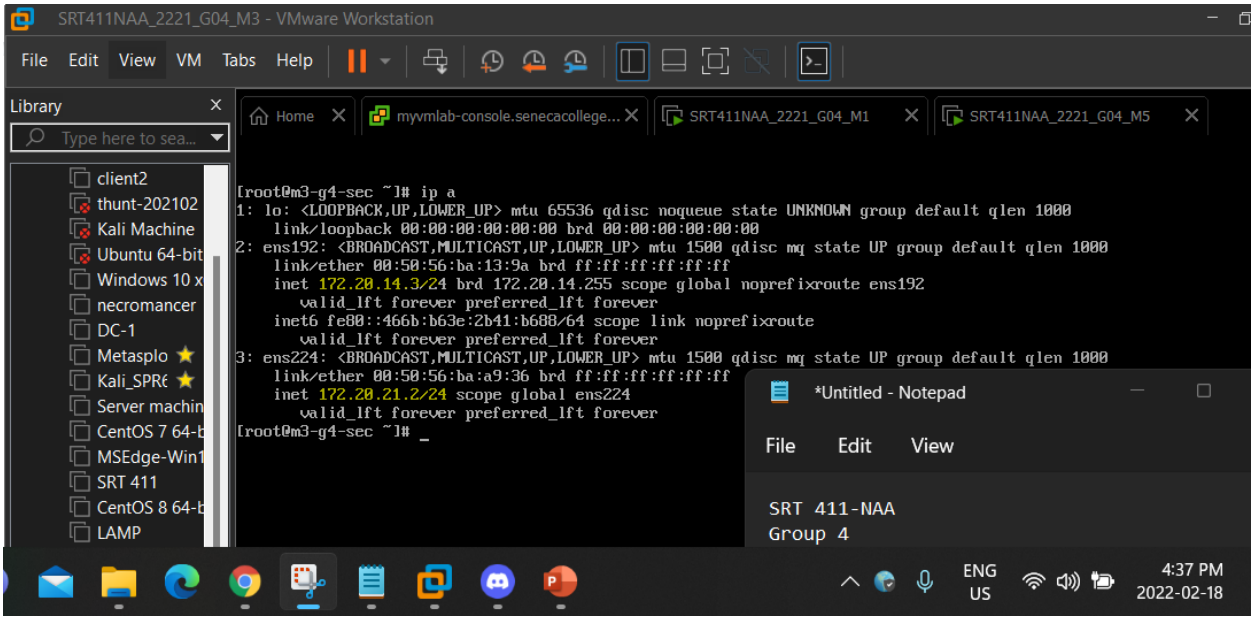


Figure 8: IP configurations for Machine 3

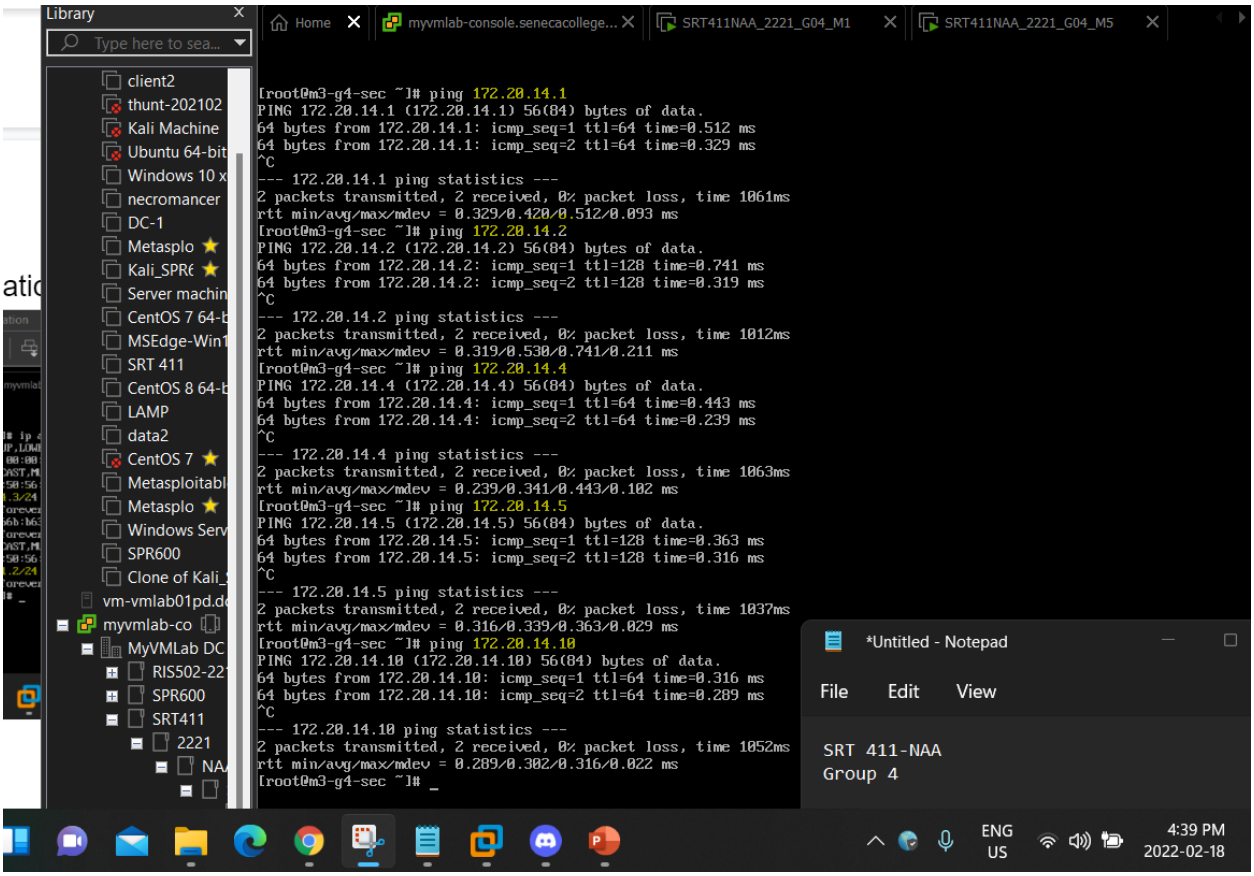


Figure 9: Machine 3 can Successfully communicate with the machines in the repo interface

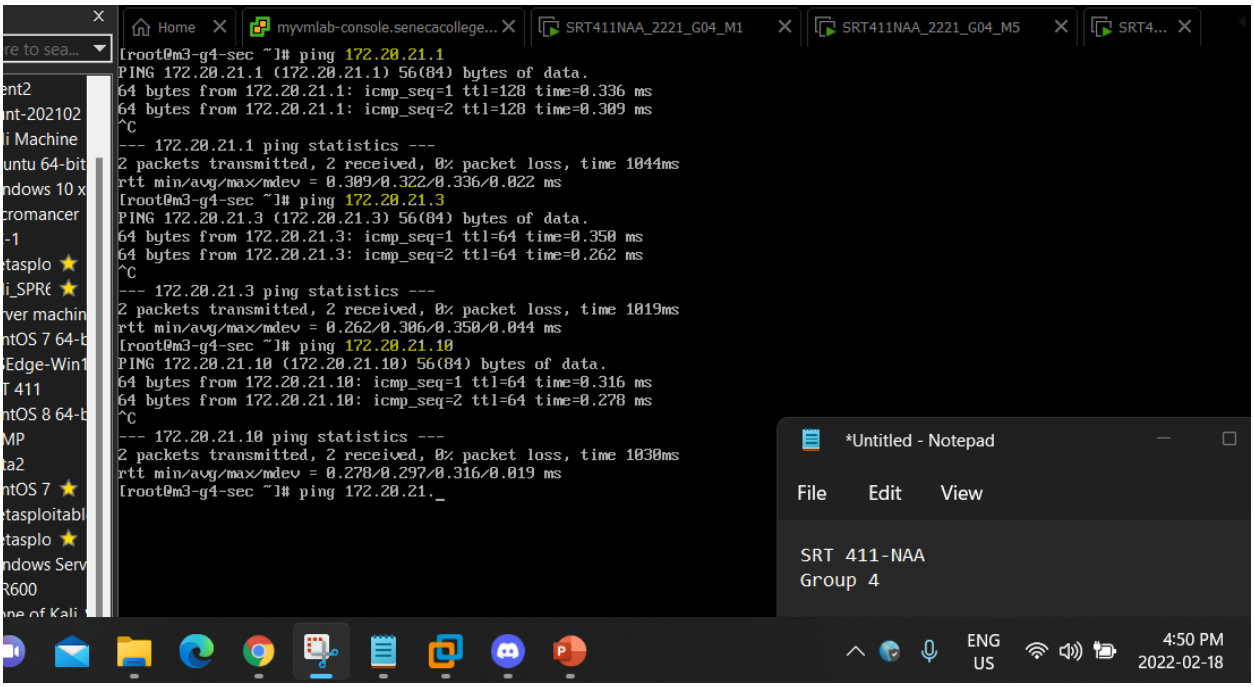


Figure 10: Machine 3 can successfully communicate other machines in the Attack interface

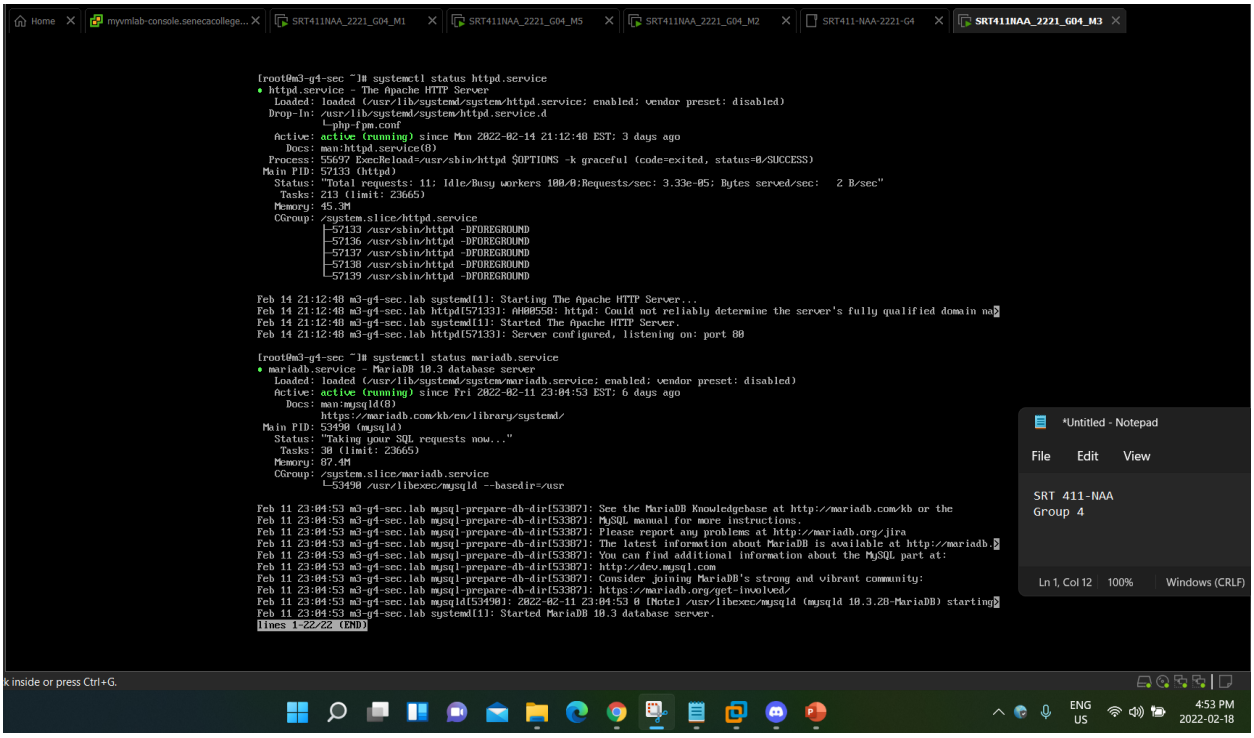


Figure 11: Both Apache and PHP are successfully configured and running in the Machine environment

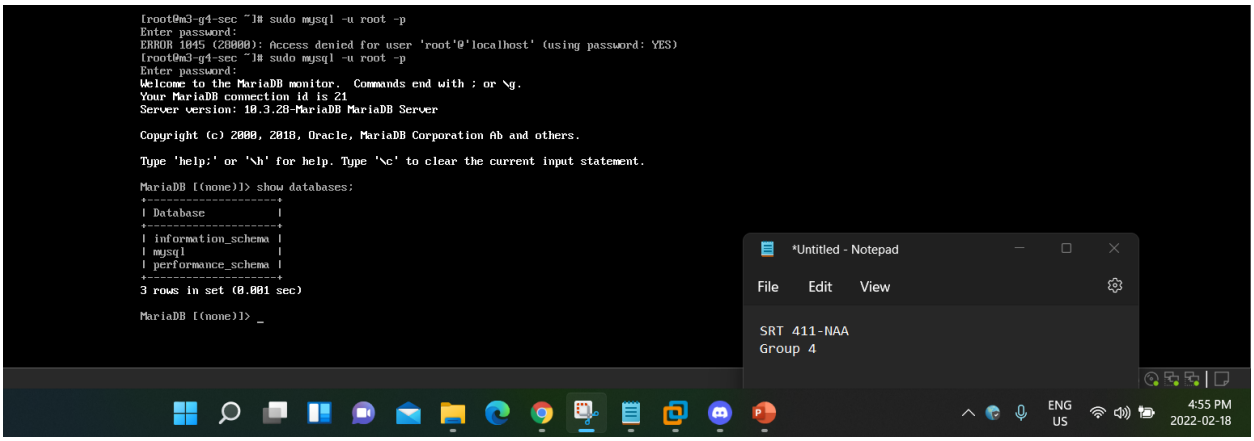


Figure 12: My SQL is running in Machine 3

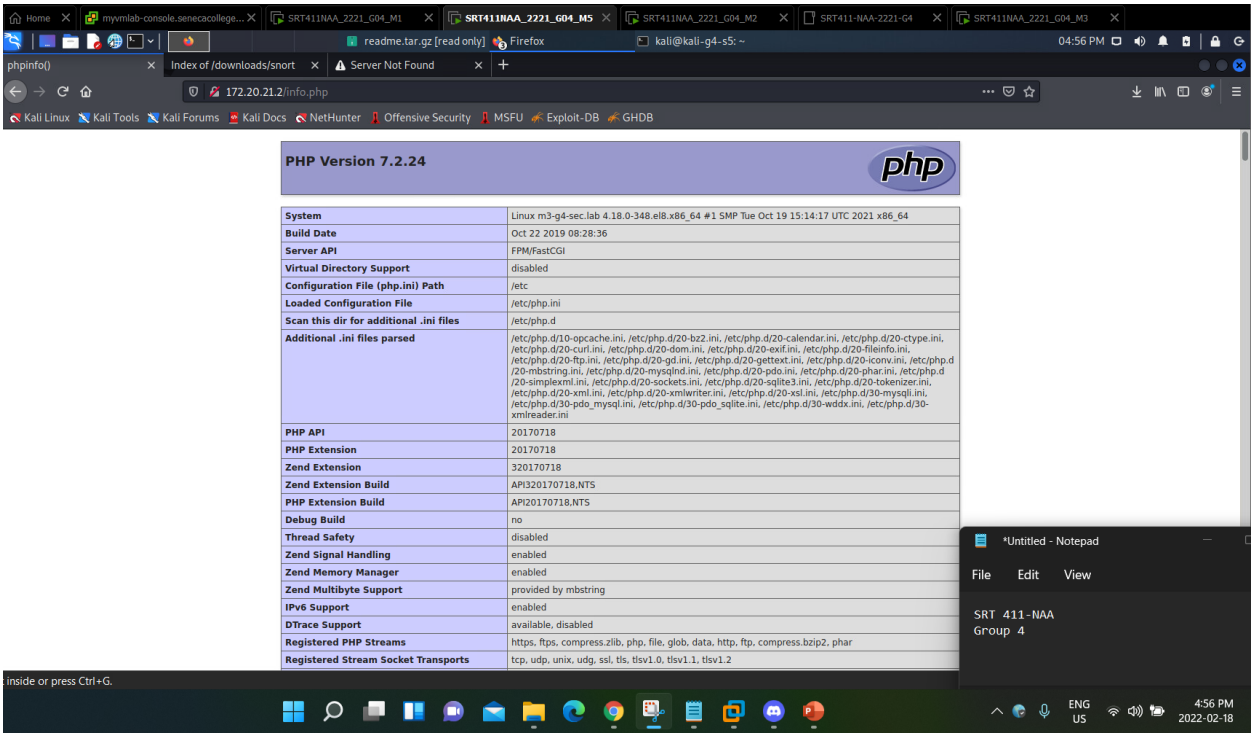


Figure 13: Successfully configured the LAMP server in Machine 3

Machine 4 - Configurations

This machine acts as the DVWA and Wordpress Server. The main purpose in this machine is to set up the above two servers within the Environment. Even though our group was able to successfully install both DVWA and Wordpress in our machine Environment, we weren't able to successfully open the server environments within the browsers, these limitations are further explained under the Limitations in Configurations heading. But similarly to the above machines, we ran a script to configure the IP addresses and both the Network Adapters in this Machine runs within the Attacker Interface and the Repo interface.

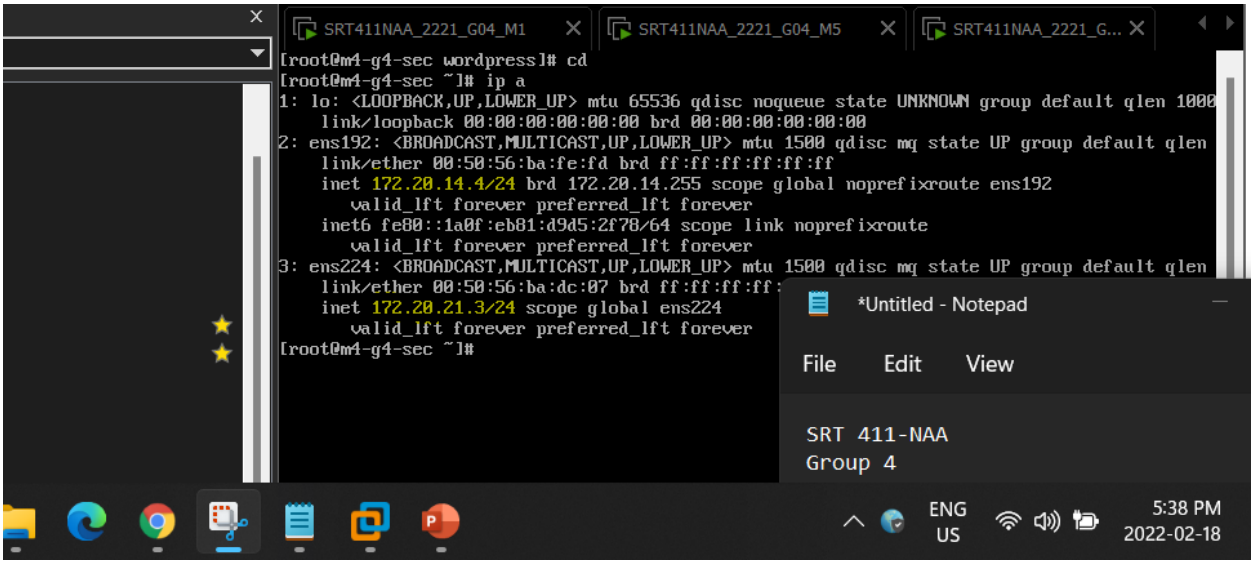


Figure 14: IP configurations for Machine 4

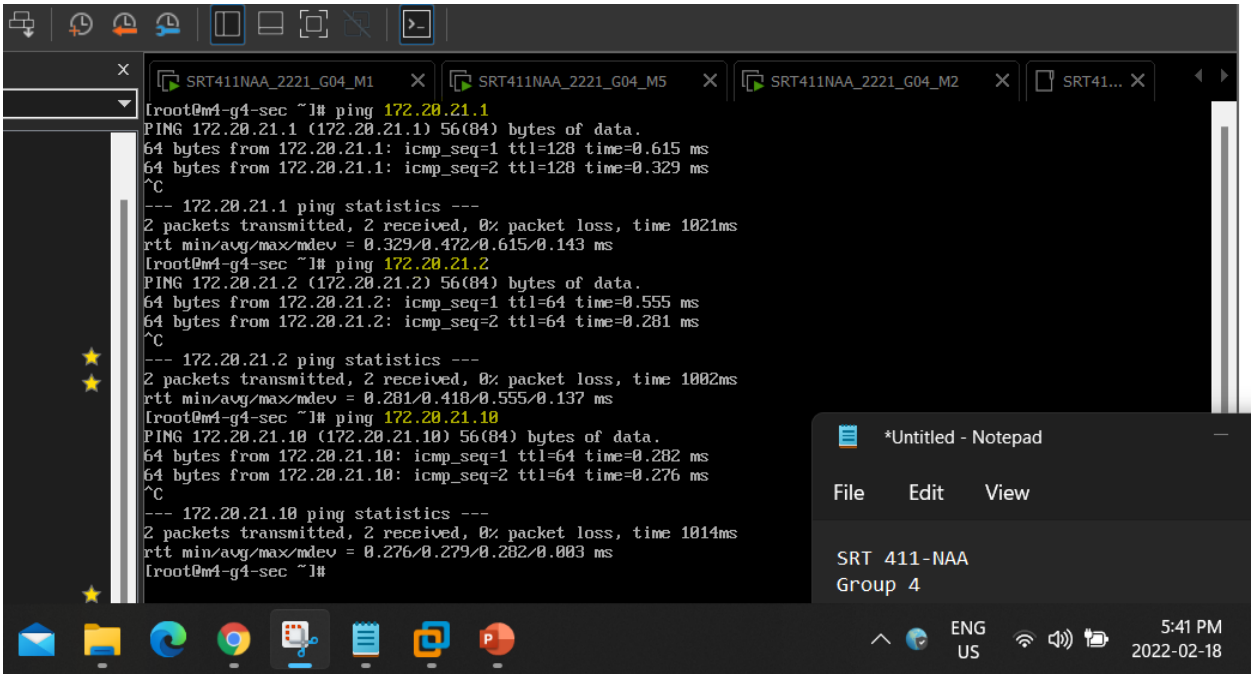


Figure 15: Machine 4 successfully connects to all the other machines in the attack interface

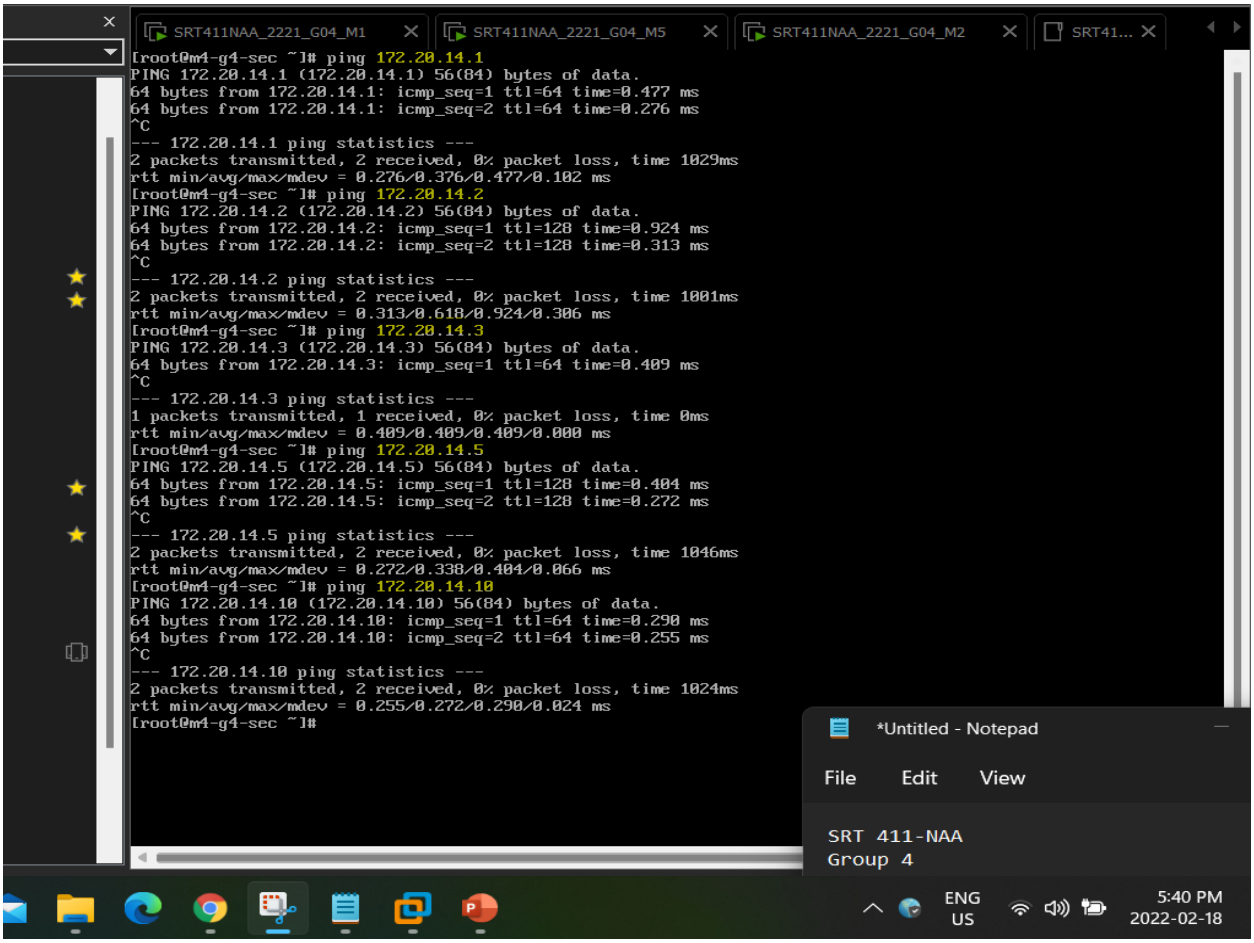


Figure 16: Machine 4 can successfully connect all the other machines in the repo interface

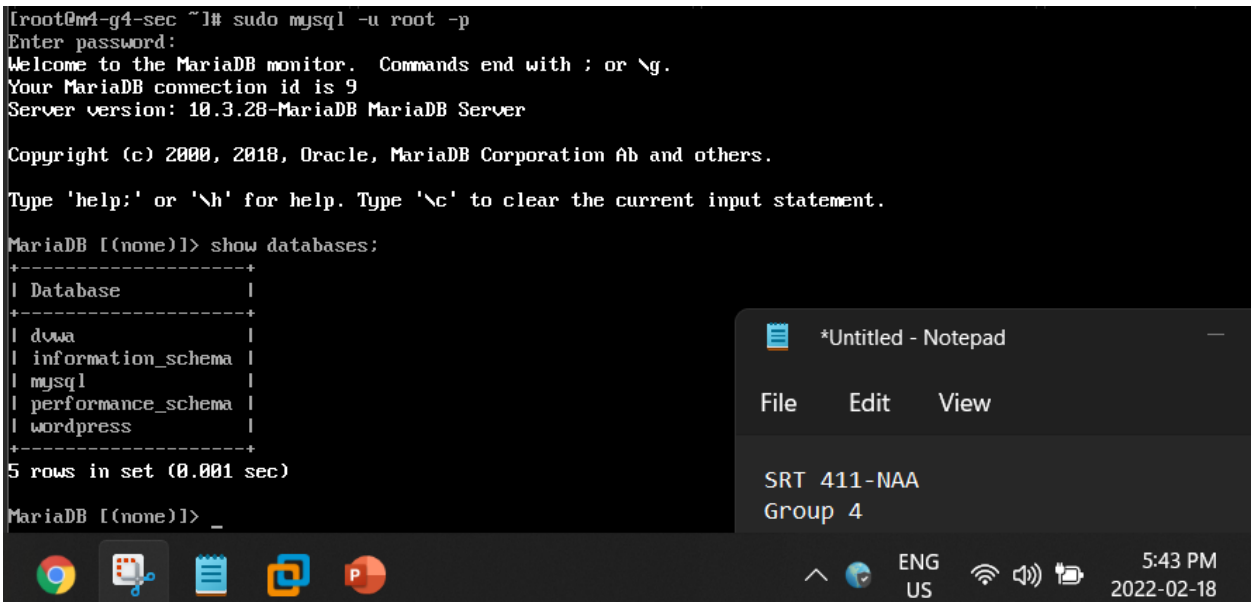


Figure 17: Created a database for both DVWA and WordPress in MySQL

Machine 5 - Configurations

This machine is the Kali Linux machine, and this machine will most likely used as the attacker machine because in later phases of this project, we will be looking at various different attacks that are produced and explained through the use of greenbone OpenVAS system, which is already installed in the Machine,the only requirement, we need to configure on this machine is to install Nessus, which we were successfully able to work on. In terms of Installing Nessus, we require an Activation Key, and since we had no Internet connection, we had to use a challenge code to get a configuration key that would give us the access to reach the Nessus server. This machine also requires us to use NMAP, which is already configured in this working environment. The other configuration was to configure the IP addresses of the environment and configure the Interfaces. This machine runs again in both the Attacker interface and the Repo interface. And This machine also had a script that configured the IP addresses into the machine.

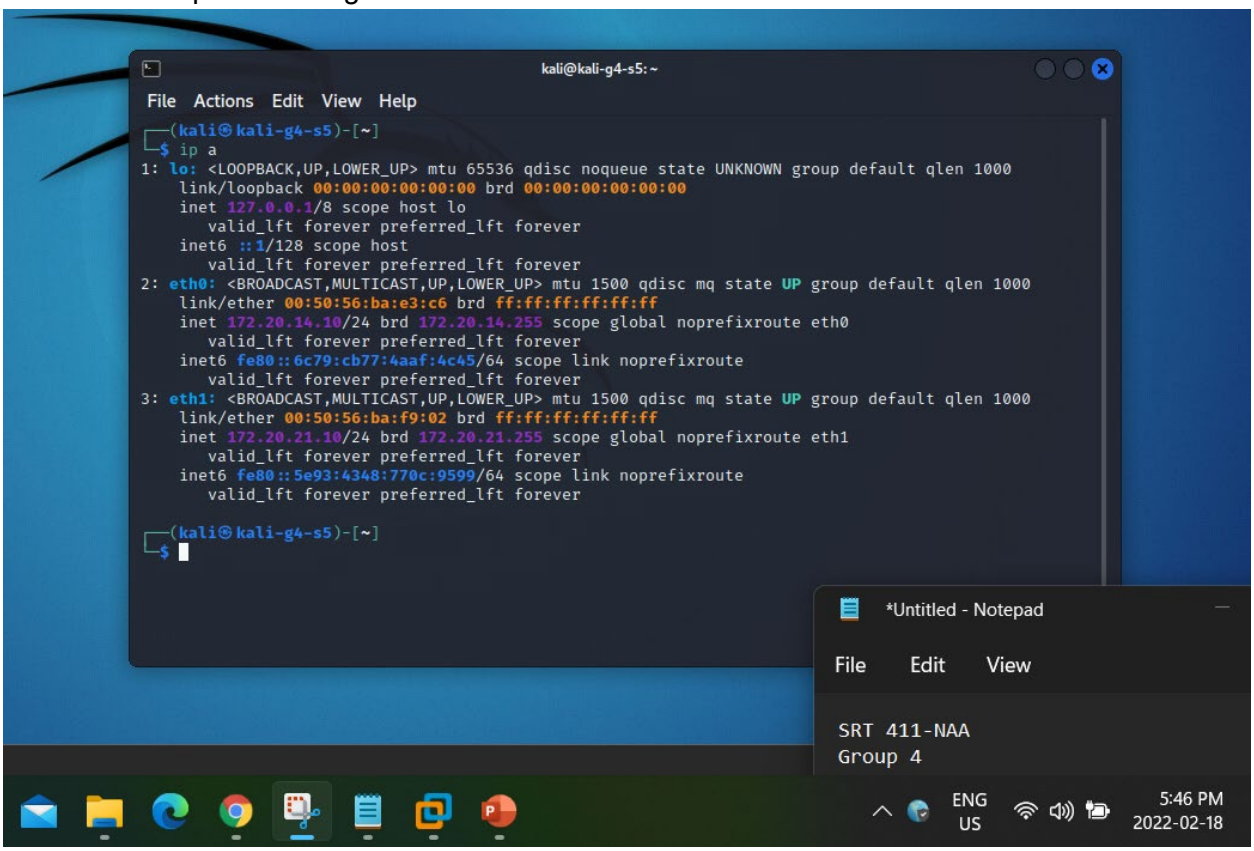


Figure 18: IP configurations for Machine 5

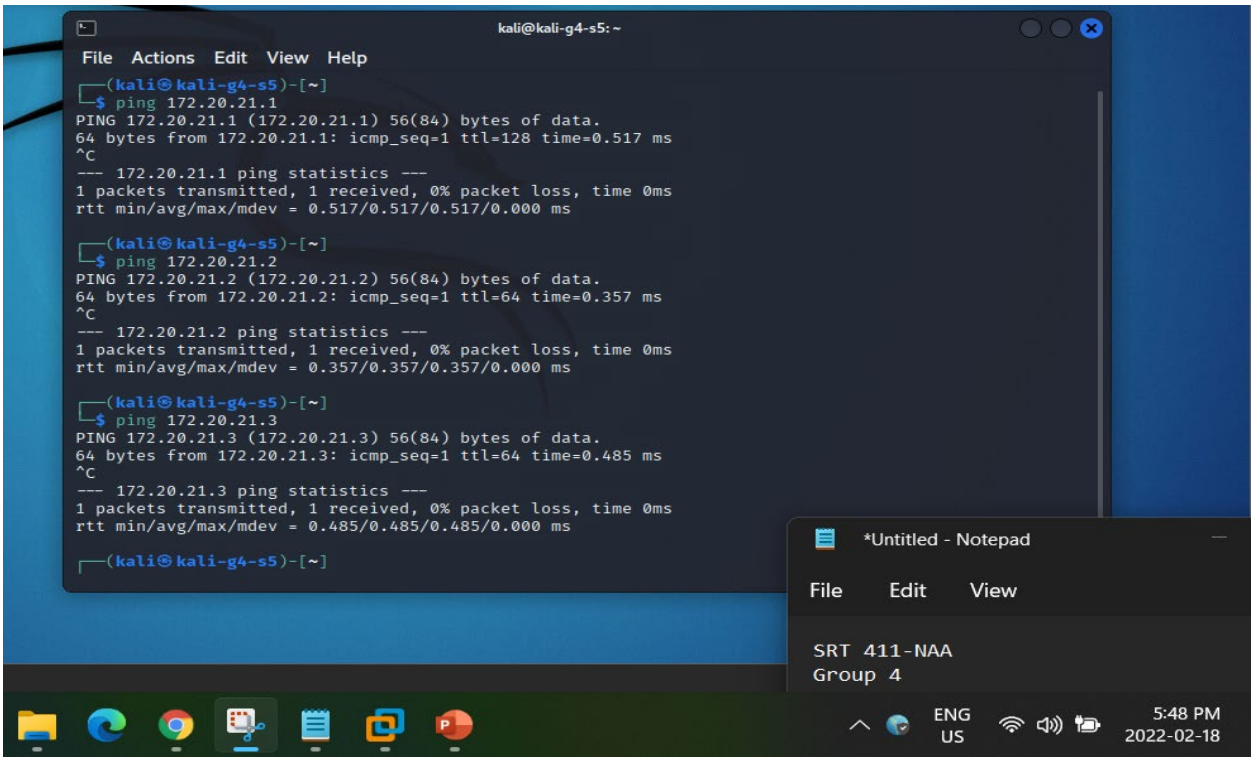


Figure 19: Machine 5 communicating with all the machines in the Attack interface

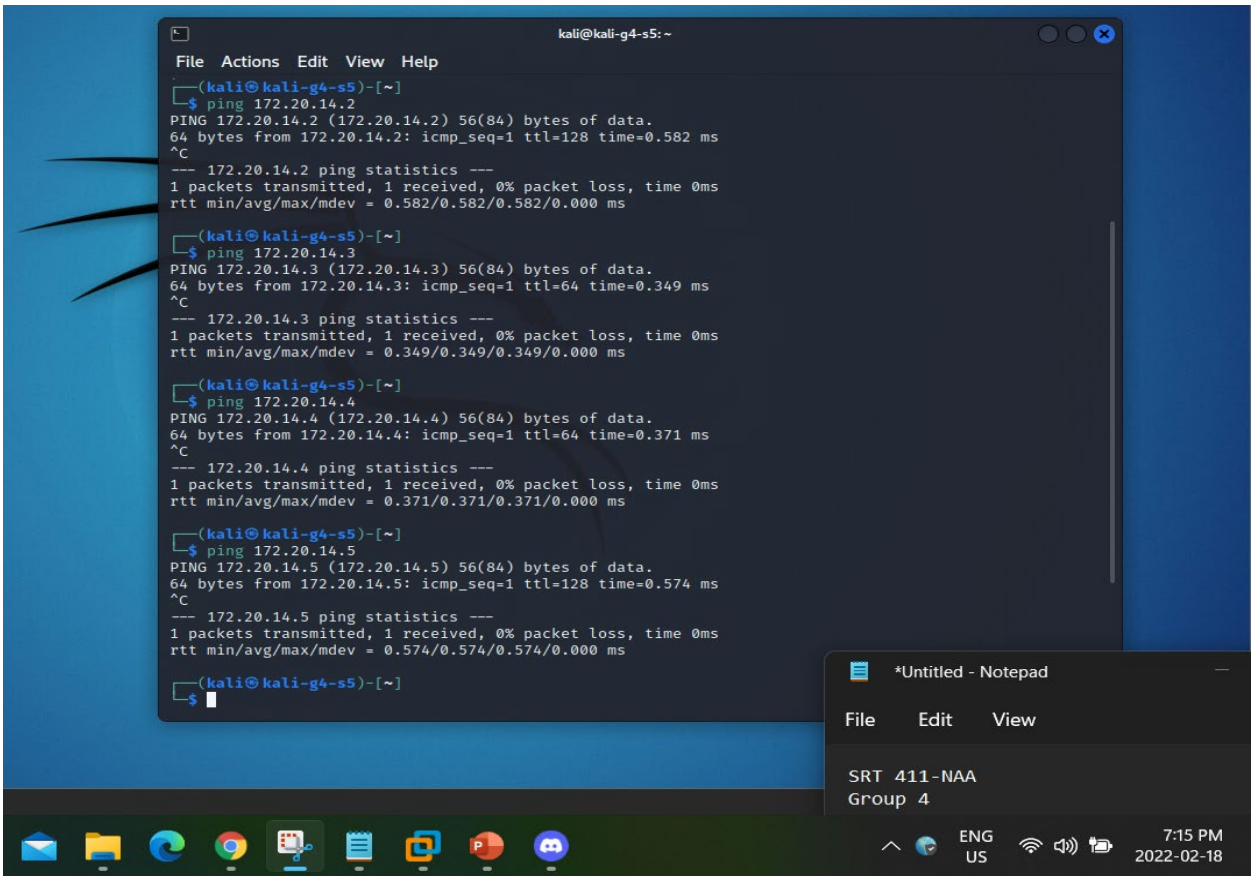


Figure 20: Machine 5 can communicate with all the machines in the Repo interface

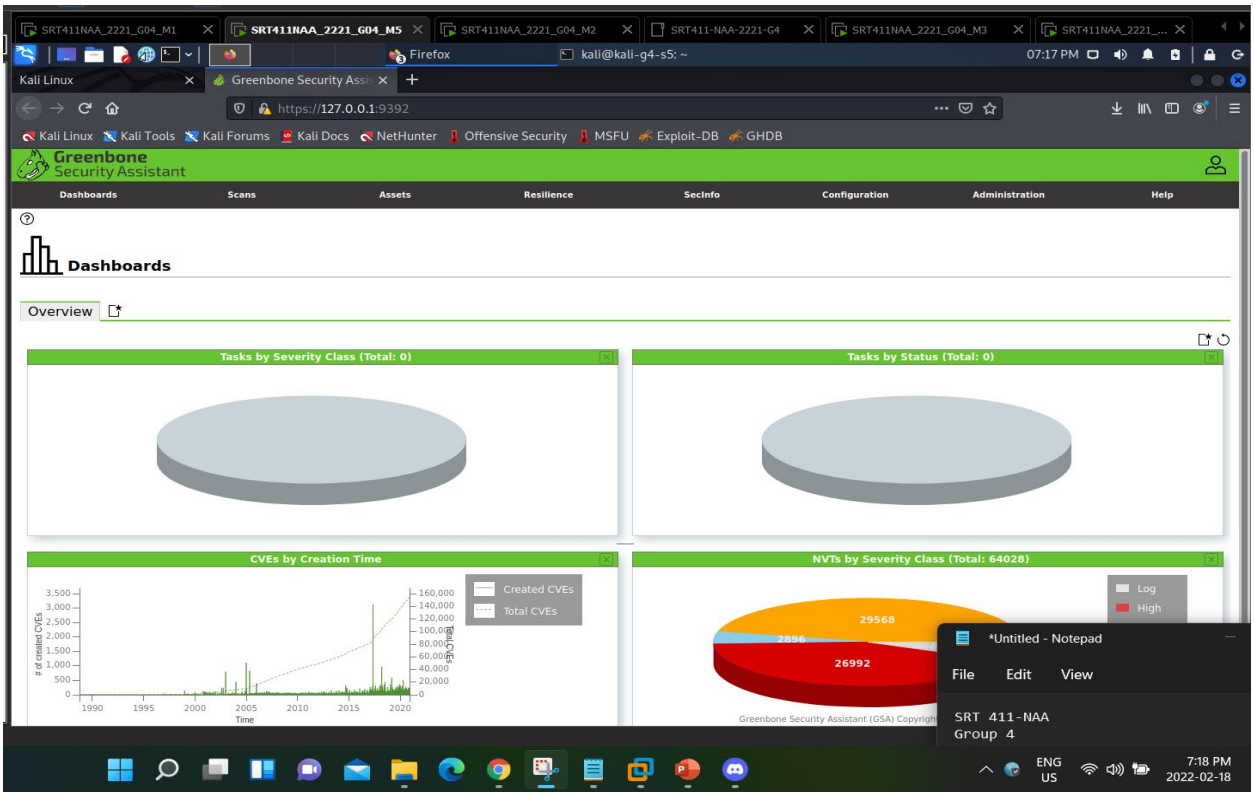


Figure 21: OpenVAS installed and running in the environment

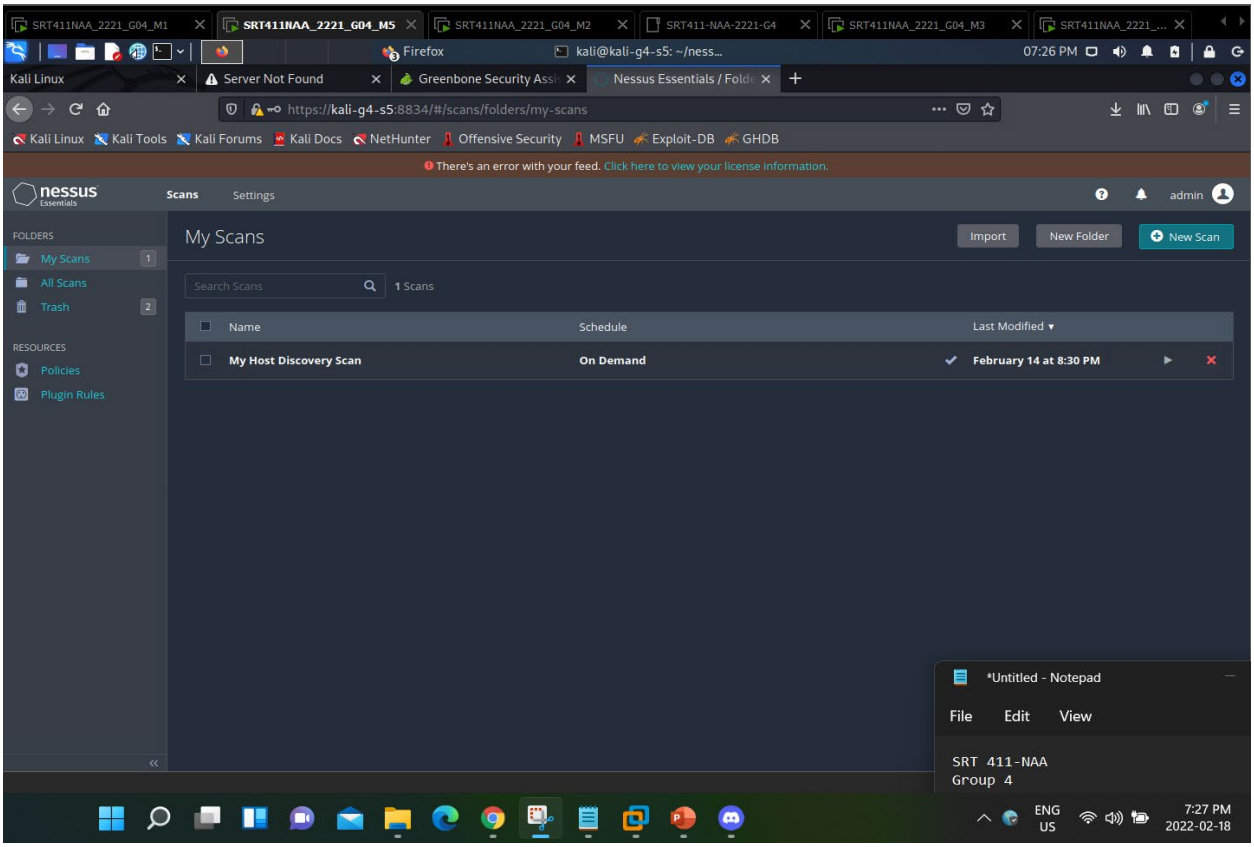


Figure 22: Nessus installed and running in the environment

Machine 6 - Configurations

Machine 6 acts as the ELK stack machine, this machine has two Interfaces where one interface is used for the Attacking interface while the other interface is used in the Log interface because this machine's log interface will communicate with Machine 1 where Snort from Machine 1 will send in the collected logs into the ELK environment. This was another machine we had some issues with because when we tried to install and run the ELasticsearch in our environment, we weren't able to successfully perform that, this event will be further explained in Limitations in configurations heading. The primary goal in this machine is to install Elasticsearch, Kibana, and Logstash, so that it will act as a Event Log environment with capabilities of displaying indexes, ingesting various different logs and visualizing these logs within a dashboard Environment.

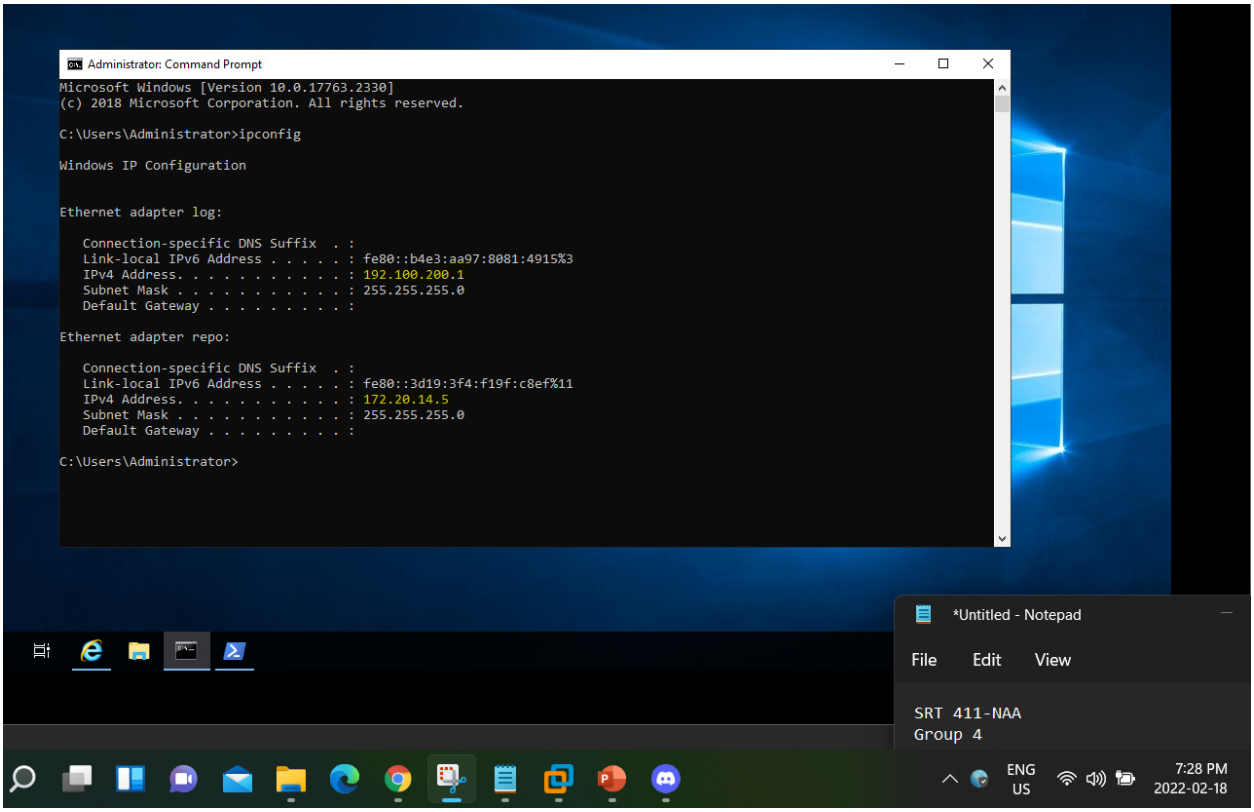


Figure 23: IP configurations for Machine 6

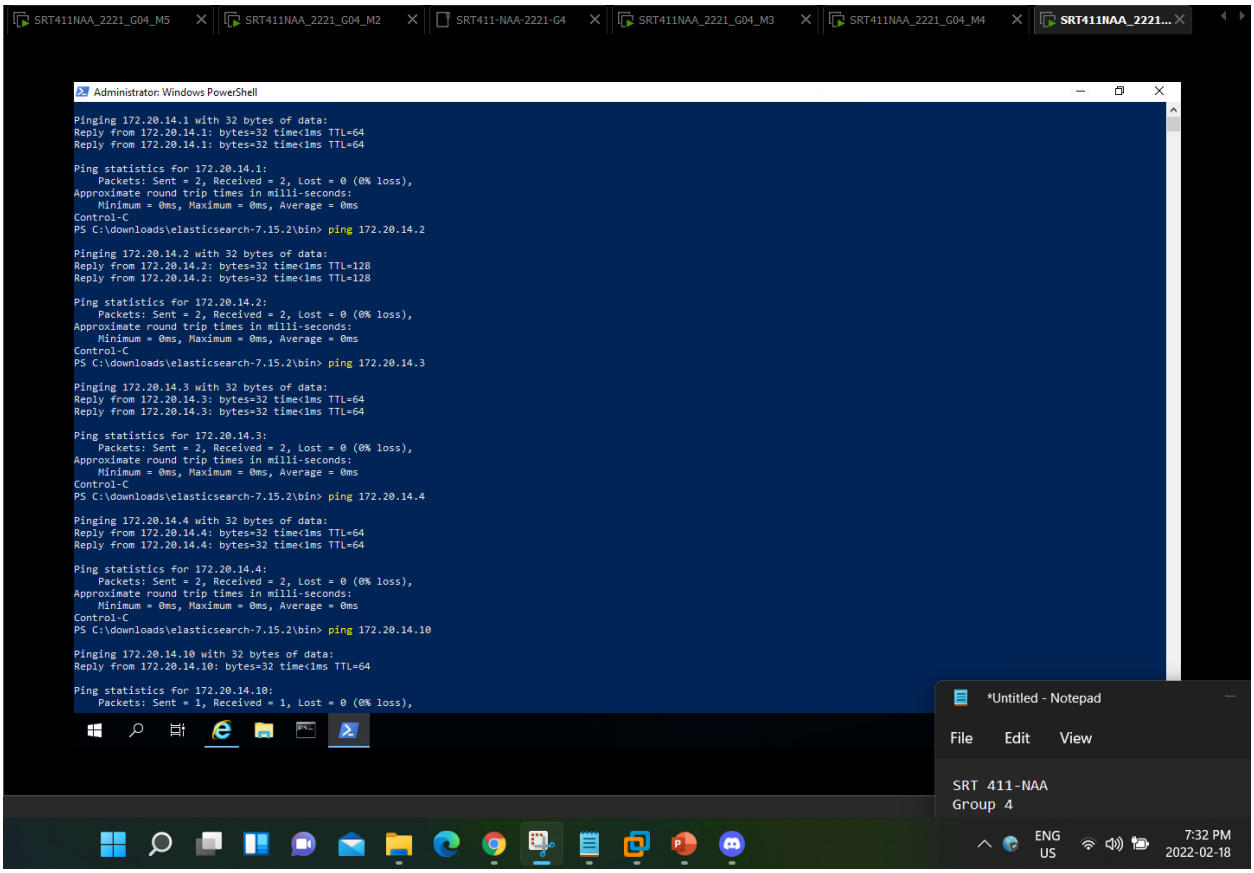


Figure 24: Machine 6 can successfully communicate with all the Machines in the repo environment

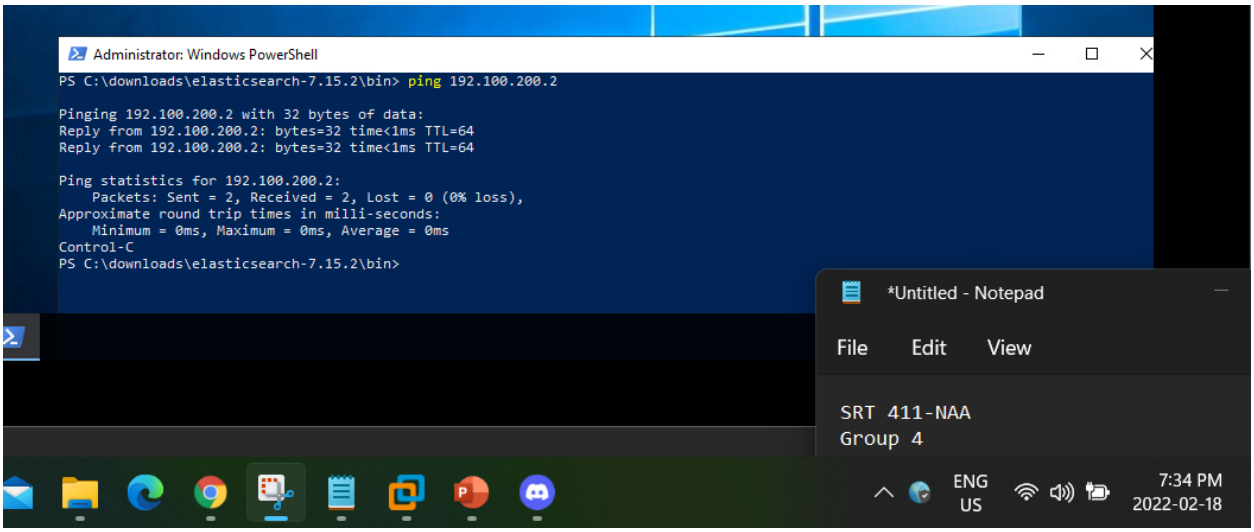


Figure 25:Machine 6 can successfully communicate with Machine 1 through the Log Interface

Limitations in configurations

Some of the limitations we had with configuring in the environment was the configuration of services such as WordPress, DVWA agent, and installing the ELK environment within the project

environment. The problem with both the DVWA agent and WordPress were that when we were trying to reach these servers, which are web servers, we weren't able to reach the setup and configurations of these files due to some errors shown in the Figures below. Like always, there is a reason we might be getting issues like this, it might either be related to the method we used to install the services within the environment, or the Environment provided to us might have limitations that need to be configured. To overcome these issues, we need to properly configure these installations to further proceed into the next phases in the project.

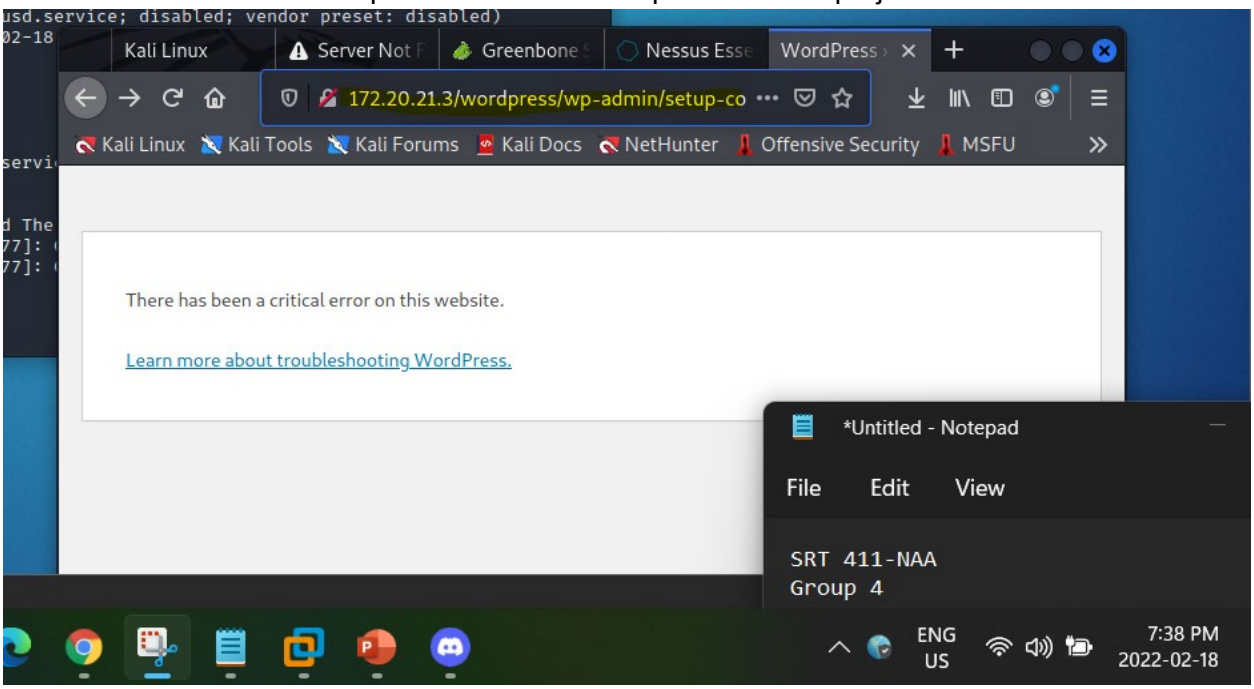


Figure 26: Issues regarding with WordPress setup

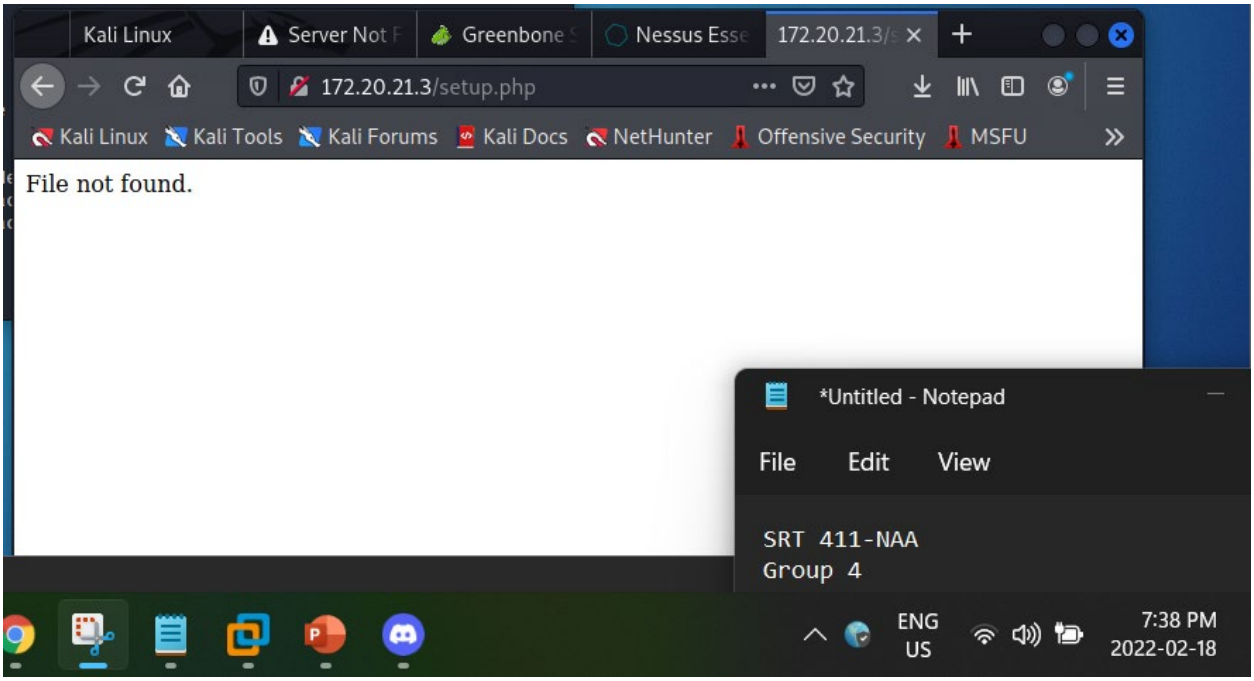


Figure 27: DVWA issue that our group faced

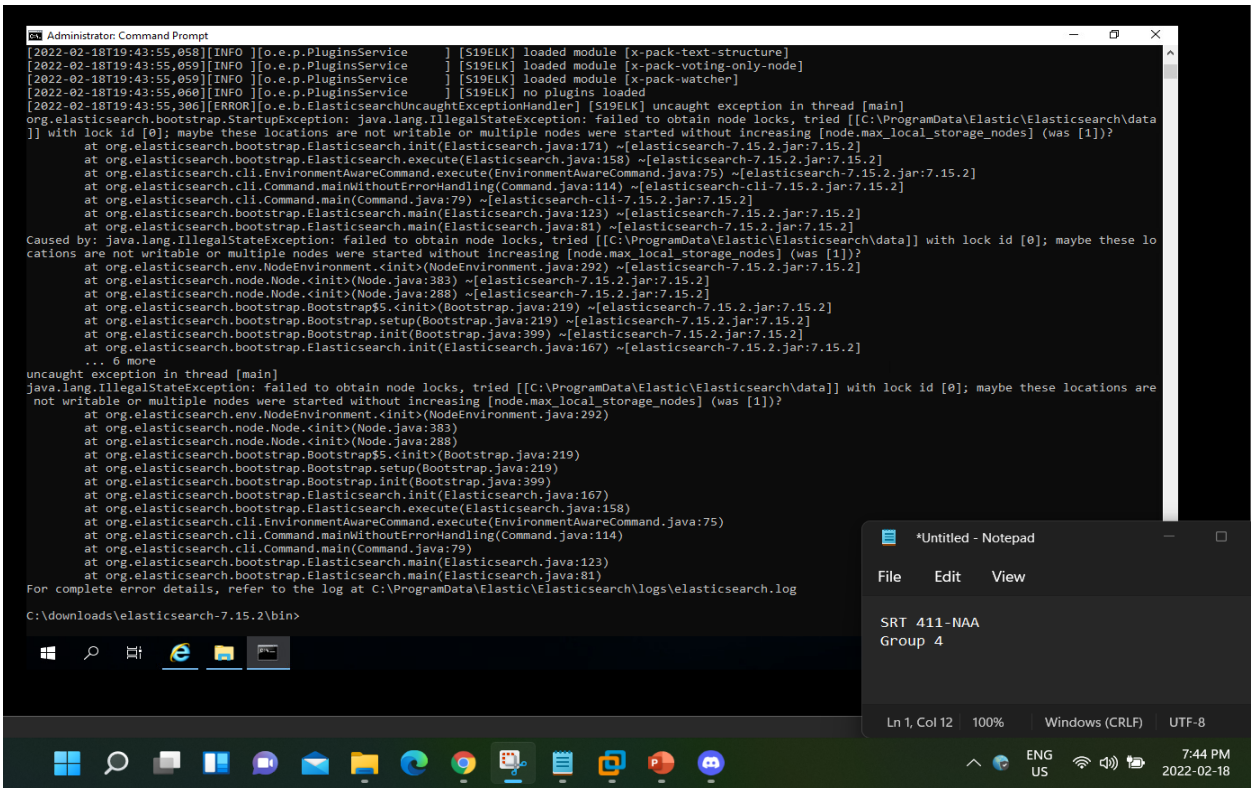


Figure 28: Issue regarding elasticsearch installation

In terms of the issue that we are dealing with elasticsearch is that it isn't properly installing the elasticsearch services in the environment, hence giving us error messages which seems to be related to specified misconfigurations regarding the Java executions. Since this issue occurred, we weren't able to properly open elasticsearch in our browser environment and only opens in JSON format.

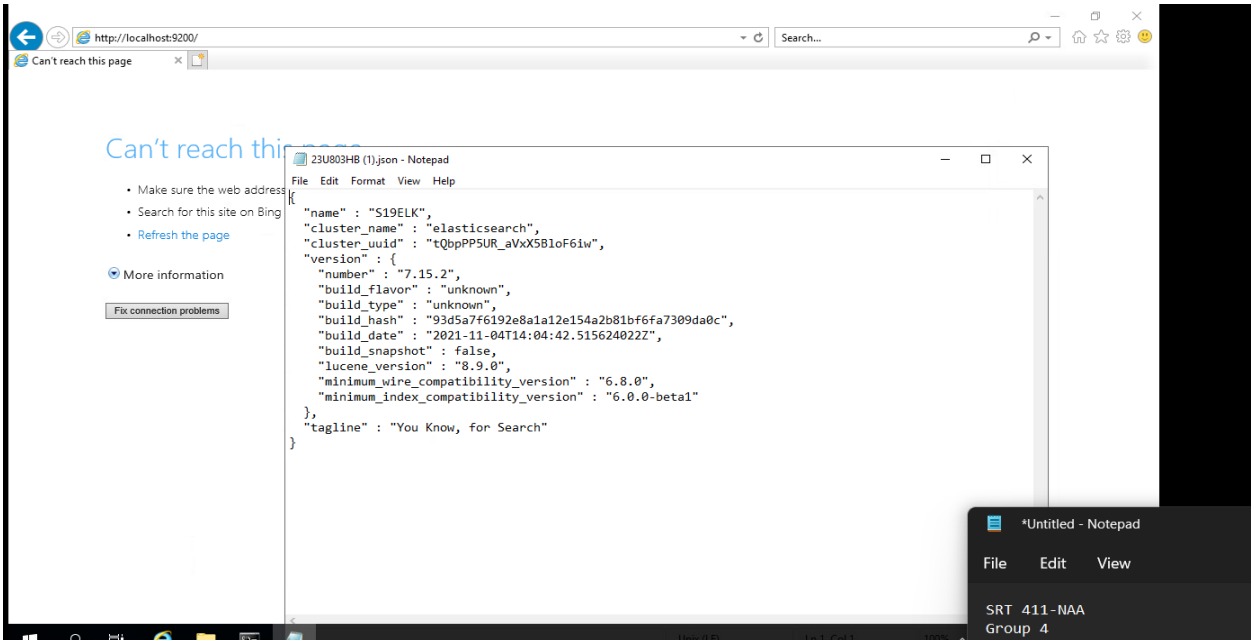


Figure 29: Elasticsearch doesn't open in the browser

Conclusion

In conclusion, this phase of the project seems to be fairly successful with our team managing to configure as much as we were able to within the Project environment. Mainly the IP configurations had slight issues as well, due to the fact of misconfigured information within the script environments provided to us. But we were able to identify the mistakes and were able to successfully configure them. But when it comes to service installations, we had few mistakes and limitations that lead us into some services not properly installed or configured. But this concludes our phase 1 of the project and in the upcoming phases we are required to do the changes that will prepare our project environment into the upcoming phases of this final Project.

References

R. (2020, October 31). How To Install WordPress with Nginx on CentOS 8 / RHEL 8. ITzGeek. https://www.itzgeek.com/how-tos/linux/centos-how-tos/how-to-install-wordpress-with-nginx-on-centos-8-rhel-8.html

Jethva, H. (2021, June 4). How to Install Damn Vulnerable Web Application on CentOS 8. HowtoForge. https://www.howtoforge.com/how-to-install-damn-vulnerable-web-application-on-centos-8/

Guoan, X. (2021, April 28). How to Install LAMP Stack on CentOS 8/RHEL 8. LinuxBabe. https://www.linuxbabe.com/redhat/install-lamp-stack-centos-8-rhel-8

Ruostemaa, J., & Ruostemaa, J. (2022, January 10). How to install Snort on CentOS. UpCloud. https://upcloud.com/community/tutorials/installing-snort-on-centos/