LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS6P05NI Final Year Project

Assessment Weightage & Type

40% FYP Final Report

Year and Semester

2021 Autumn

Student Name:

London Met ID:

College ID:

Internal Supervisor:

External Supervisor:

Assignment Due Date: 27th April 2022
Assignment Submission Date: 27th April 2022

Word Count (Where required): 9067

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

Firstly, I would like to express my gratitude to Islington College and its university partner London Metropolitan University for providing a conducive environment and course material, such as Final Year Project (CS6P05NI), in which I was able to learn about real-time project planning, development, testing, implementation, and documentation. I am also grateful for the learning materials they give; they came in handy as I was putting up my report. To achieve the goal of this report, I had to seek the assistance and advice of various well-respected individuals, all of whom deserve my sincere appreciation.

I am grateful and like to thank Mr. Saroj Lamichhane, my External Supervisor, and Mr. Sathyam Pradhan, my Internal Supervisor, for their assistance, consistent monitoring, and help in finishing my final report.

I would also like to thank my parents for their encouragement, assistance, and support. And finally, I would like to express my deepest appreciation to my friends for their willingness to provide a hand when I needed it every time.

Abstract

The final report shows the development of a network monitoring tool project. The constant study of a network in order to detect and fix any functioning problems is known as network monitoring. This Network monitoring tool includes gathering statistics from the network in order to assess the network's service quality. Routing, firewalls, PCs, switches, servers, and Wi-Fi are all monitored and reviewed on a regular basis as part of the network's continuous monitoring and evaluation.

This report illustrates innovative solutions that can visualize all the data inside the dashboard of a Nagios server. This also includes new features like doing the Nmap scan in this tool which helps us to see all the open ports inside an organization and helps to keep it secure. Network monitoring tool may be used not just by businesses, but also by individuals who wish to protect their privacy, data, and other personal information. The project can track Windows host status and event logs, Linux host status and event logs, router and switch status and its event logs, network open ports, remote machine temperature, and server status.

This tool supports us in identifying the location of a network problem or confirming that the network is not the issue. Continuous monitoring can benefit in the detection of potential problems before they arise. It means we can address issues before they affect users so this what the network monitoring tool does and helps in different business organizations to keep their business safe and secure and run continuously without facing and future problems.

Table of Contents

Table of Figures

Figures of Table

List of Abbreviation

Acronyms	**Full Forms**
IT	Information Technology
VM	Virtual Machine
OS	Operating System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSH	Secure Socket Shell
RAM	Random Access Memory
CPU	Central Processing Unit
XAMPP	An abbreviation for cross-platform, Apache, MySQL, PHP, and Perl
GNS	Get Nearest Server
PUTTY	An application which can act as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols.
WinSCP	Windows Secure Copy
IP	Internet Protocol
NMAP	Network Mapper
LINUX	Lovable Intellect Not Using XP
CentOS	Community Enterprise Linux Operating System

PING	Packet Internet or Inter-Network Groper
DB	Database

Table 1 List of Abbreviation

1. Introduction

1.1. Project Description

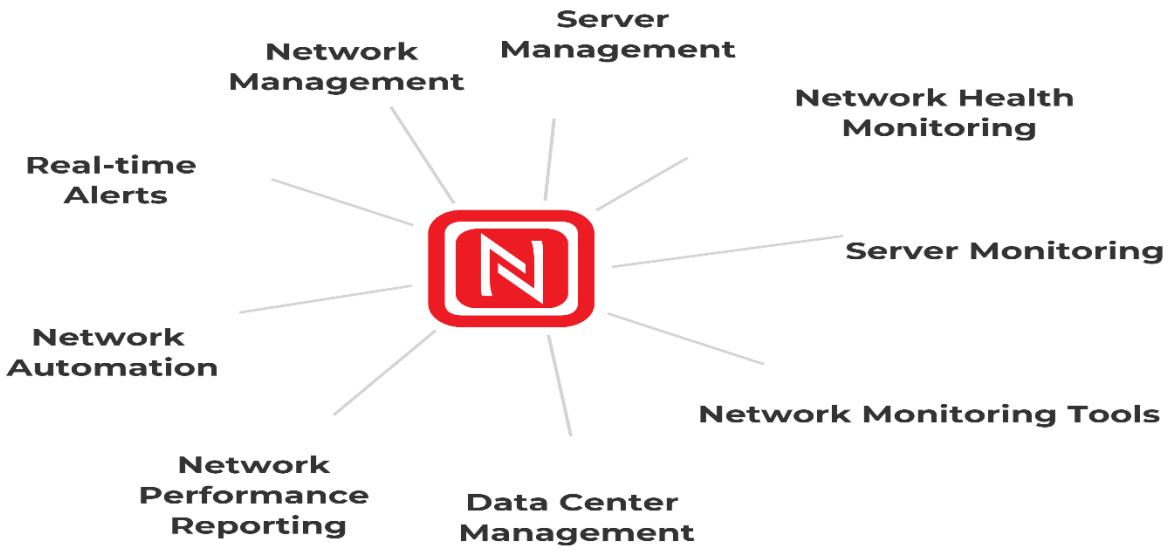


Figure 1 Uses of Network Monitoring tools *(Pat Research, 2021)**.***

A business network's network monitoring is a crucial IT activity that may save money on network performance, employee productivity, and infrastructure cost overruns. A network monitoring system (NMS) monitors an internal network for faults. It can locate and assist with the execution of tasks like Overloaded, crashed servers, unstable network connections, and other devices can cause slow Web page downloads, lost-in-space e-mail, suspicious user behaviour, and file delivery (Behr, 2007).

Network monitoring software provides historical data on how equipment has behaved over time, allowing you to justify network improvements. Trends analysis can help you figure out whether your present technology can scale to meet your company's goals or whether you need to invest in modern technology (Helpsystems, 2021).

The technique of determining whether ports on a target machine are open is known as port scanning. Secondly, one of the most typical outcomes of this phase is determining what services are operating on these ports. Sales associates, for example, enter through the front door, while owners enter by the garage door and friends enter through the side door. We expect salespeople to come in via the front door, and we expect services to use specific computer ports. HTTP traffic is typically sent over port 80, whereas HTTPS traffic is sent over port 443. If ports 80 and 443 are open, we may assume that HTTP and HTTPS are active, and that the computer is a web server. This tool not only monitors the up and down status of the hosts it also helps to scall all the open ports of that host and help an organization in many ways (Pauli, 2013).

Administrators can receive a comprehensive image of all the devices connected to the network by using network monitoring. View the flow of data between them and rapidly discover and resolve issues that might jeopardize performance or cause disruptions. Modern business depends on a host of internet-based, mission-critical services. This comprises cloud service providers, ISPs, CDNs, SaaS, UCaaS, VPNs, and SECaaS providers, as well as SaaS, UCaaS, VPNs, and SECaaS providers. Because each service is based on the internet, it is vulnerable to performance swings caused by network outages or routing difficulties. We can monitor issues that may affect employees or customers by having visibility into network components outside of your control. Network monitoring systems use hardware and software to decrease IT teams' human effort. As a result, the organization's valued IT professionals will have more time to dedicate to important tasks (Cisco, 2021).

1.2. Current Scenario

Figure 2 Network Monitoring *(Yoram Ehrlich, 2020)**.***

The task of organizing and presenting an enormous amount of data in a meaningful way becomes more difficult with cloud-based monitoring. Monitoring tools convergences between NetFlow and Packet monitoring are the result of a requirement to reduce tool sprawl. Machine learning (ML) and artificial intelligence (AI) are included into network monitoring systems to better control data volume (LiveAction, 2022).

Nagios Core is a network monitoring and system administration program that is free and open source. It keeps an eye on the hosts and services we provide, notifying us when something goes wrong and when things improve. Nagios Core was developed with

Linux in mind; however, it should run on most other operating systems (Core, 2022). Nagios Core comes with several functionalities which includes:

- Network services are monitored (SMTP, POP3, HTTP, NNTP, PING, etc.).
- Host resource monitoring (processor load, disk usage, etc).
- Users may quickly create their own service checks thanks to a simple plugin design.
- Service checks that run in parallel.
- The ability to create a network host hierarchy using "parent" hosts, allowing for the detection and differentiation of down and inaccessible hosts.
- When service or host issues arise and are remedied, we will receive alerts (via email, pager, or user-defined method).
- Ability to design event handlers that will be executed during service or host events to solve problems before they occur.
- Log file rotation is automated.
- Implementing multiple monitoring hosts are supported.
- Optional online interface to see current network status, notification and problem history, log file, and other information (Core, 2022).

1.3. Problem Statement and Project as a Solution

1.3.1. Problem Domain

The need of environmental equipment monitoring is sometimes overlooked. The failure to monitor the performance of our HVAC or environmental sensors, as well as the lack of a backup plan, can quickly result in network outages. Home network and corporate network gets and send lot of data and information. The ability to see what is going on one the network gives control. But modern network monitoring tools are tailored towards the IT specialist and technical person. With this project a simple and easy to use home/corporate network monitoring tools using open-source software is created. Which will help common people to understand network better. The user can easily see all the output logs and reports understandable easily in graphs.

Port scanning is the process of identifying "listening" TCP or UDP ports on a computer or network and extracting as much information about the device as possible from the listening ports. TCP and UDP applications and services make use of a number of well-known ports that are available. To extract information, the hacker uses his knowledge of often used ports.

SSH, for example, uses port 22 by default. If the hacker discovers that port open and listening on the system, he/she might assume that SSH is enabled. He/she can then attempt to get into the system, for example, by brute-forcing the password and gets all the information of an organization or a private network/home network.

1.3.2. Project as a solution

This project will assist in resolving the problem stated above. The user will be able to readily access all the network output log and report files, as well as understand what the report means, with the help of this program or tool all the reports can be seen in a graph and makes the user easy to understand and see all the reports from a week to months. The normal peoples will also be able to see the logs by staying at home and using the home network. With the help of this tool anyone that uses the tool will know to use it properly because of its simple UI. The UI is so normal that anyone can monitor the network to which they are connected.

The tool will be able to scan networks of a particular address, identify all the vulnerabilities, scan all the open port, and help an organization to make all the ports close or secured. The port scanning feature will help an organization to list all the open ports and help to get secure all the information of that organization by securing the open port or closing all the open ports which will not allow any hackers to get into the system of the organization and save them from big problems. The tool lists all the active and inactive hosts and services. So, if the tool scans all the above-mentioned components the user will be able to monitor his/her network and see all the logs and reports in an understandable way in a graph and monitor the network in a real time and can fix all the errors before occurring any big problems or before getting any effects.

1.4. Aims and Objectives

The aim of this project is to develop a network monitoring tool which is user friendly and can be used easily and do the monitoring of the network. Some of the aims and objectives of the project are as follows:

1.4.1. Aim

The main aim of the project is to understand all the working mechanism of the Network monitoring tools, learn what all the logs and report mean and represent all the report in the graph and scan all the open ports and their services. Add different hosts and services, router and switches for monitoring their data and suppress all the problem of the tool for the users of the particular tool known as Nagios Core.

1.4.2. Objectives

- To learn how all the tools work and check all its available features.
- To Research on Python, Perl, C programming language and other hardware and software components.
- To figure out where the project can be used.
- To make the tool run user-friendly.
- To make all the output logs and reports in a graph and make it understandable by the user easily.
- To add different new features in the tool.
- To add different type of host and services and monitor it in real time.
- To learn to use different tools and software used to add all the required features and monitor the network.
- To make the tool able to scan all the open ports and services used by the ports.

1.5. Structure of the Report

1.5.1. Background

The background section of this report provides better way of understanding of the project and all of the features, requirements and all the description of the project. And it also shows all the similar projects to give the details of its features and all of its components.

1.5.2. Development

The development section explains how the project will be developed using the methodologies that have been studied and chosen, as well as the many phases of analysis and methodologies that have been chosen. In addition, it reflects the project's work breakdown structure (WBS). that are being carried out and will be carried out according to a schedule (Gantt chart).

1.5.3. Testing and Analysis

First, unit testing was completed, followed by system testing via the creation of a test strategy and test cases in this part. Finally, the test results are carefully examined in order to obtain the most useful information. The project explanation is verified, and the progress to date is analysed. It displays the current status of development as well as reviews. With the dashboard, it indicates how the system is progressing. It also demonstrates how the backstage work was completed according to the Gantt chart's plan.

1.5.4. Conclusion

This part displays a report's conclusion by analysing legal, ethical, and societal concerns, project benefits and challenges, and the system's future potential. Overall, it gives a broad overview of the system, its applications, and its consequences.

2. Background

2.1. About the End Users

This project is for network security experts and new commers who want to monitor or capture network data. Analysts can use the analytic data to understand more about the resource's targeted features, which can later be more precisely maintained in the real system. This project's monitoring and analytics infrastructure may be utilized for research and business proposals. Because this is an open-source project, any of the new features can be added to it. However, I have also downloaded the Nagios tool and added some additional features to it that will make it easier for users to understand the reports and keep a record of all open ports in any of the remote device or nearby devices and helps an organization to keep all the data and information secured from the hackers by securing the open ports.

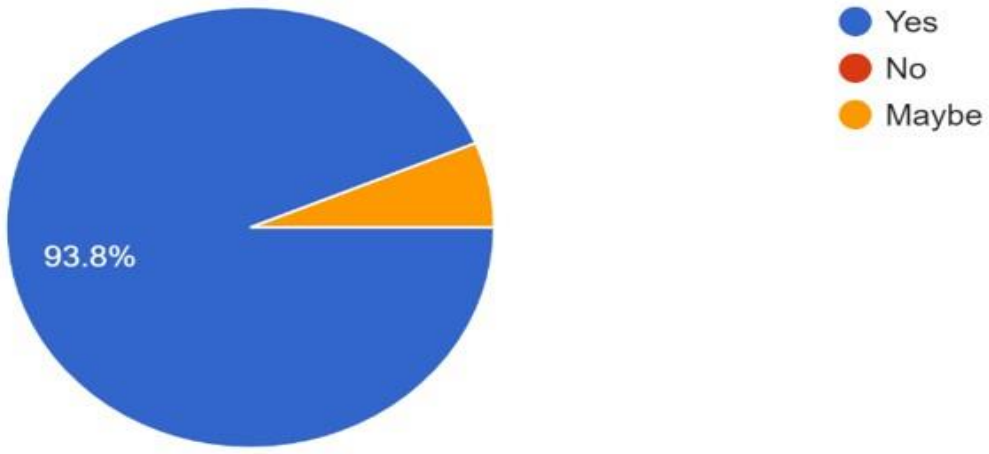


Figure 3 Graph of interested users in Network Monitoring (Primarily end users)

2.2. Understanding the Solution

2.2.1. Overview of the system

The project ScanNet is a tool which is slightly modified from the opensource tool named as Nagios and added different new features in it, through which we can monitor different types of host logs, services logs, router and switches logs, windows event logs easily by doing different configuration of the hosts that we need to monitor and all that logs can be shown clearly in the Nagios Dashboard. All the logs that are generated will be sent to the Ngaios Dashboard through different agents and monitored for real-time visualization.

2.2.2. Project Elaboration

The project would be a tool with a dashboard and other many features on it. Which will contain various hosts and services and different logs of the it by using NSClient++, SNMP, etc. all the data and information can be fetched from host machine, Linux machines, Router and Switches and other different network devices and will be shown in Nagios Dashboard. Which will make the user easy and help to analyse real-time network ups and down and all the logs of the system and networks. All the logs like CPU Usages, ping, Storage, Open Ports, and other different things can be monitored and can be shown in the Nagios Dashboard. The tool will also check whether the host and services are alive or not and will notify the user about its status. All the open ports, storage, CPU usages can be easily detected and seen in the Nagios dashboard which can help to solve all the problems in the right time before everything goes out of control.

2.2.3. Project Deliveries

The project is specifically designed to assist security companies and network companies such as banks and other businesses. Any anyone who wishes to monitor their own network and system logs, behaviour, and other services can benefit from the project. This will help in the analysis of real-time visualization of their system as well as all open ports in a network. Organizations such as "Banks" might profit from this project by using it to monitor their internal and external networks of all the branches and to examine their real-time server status. This will help them in analysing the problem and resolving it in a timely manner without risking client relationships.

2.2.4. Network Description

SNMP and NSClient++ are used to monitor hosts and services, as well as to track network protocols. They maintain track of all hosts and services, response times, open ports, disk usages, CPU usages, and many other things. SNMP helps in the understanding, collection, and organization of data regarding managed devices over IP networks, as well as the modification of that data to modify device behaviour. Cable modems, routers, switches, servers, workstations, printers, and other devices commonly support SNMP. It will submit its data and logs to Nagios server after analysing network devices and logs, and it will appear on Nagios Dashboard.

2.2.5. Security

The host and Linux machine's data and logs, as well as any open ports, will be retrieved and shown in the Nagios dashboards. It would help the concerned team in analysing real-time logs and numerous services for that host and services. This will help security teams in analysing real-time cyber-attacks via open ports and system performance. Cyber-attacks such as failed login attempts, illegal login, Brute force attacks, and unusual network behaviour may all be recognized and reported to users. This will assist them in resolving concerns in a timely manner and avoiding major harm.

2.2.6. Programming

The port scanning feature in this project is developed PERL programming language. The main component is written in the Perl programming language, which includes features like conditional statements, loops, modules, and basic functions, among others. The program scans all the open ports in that network and displays all the open ports in network. And the temperature scanning feature is written in Python programming language which scans all the available temperature of the host machines.

2.3. Similar Project

2.3.1. Cacti

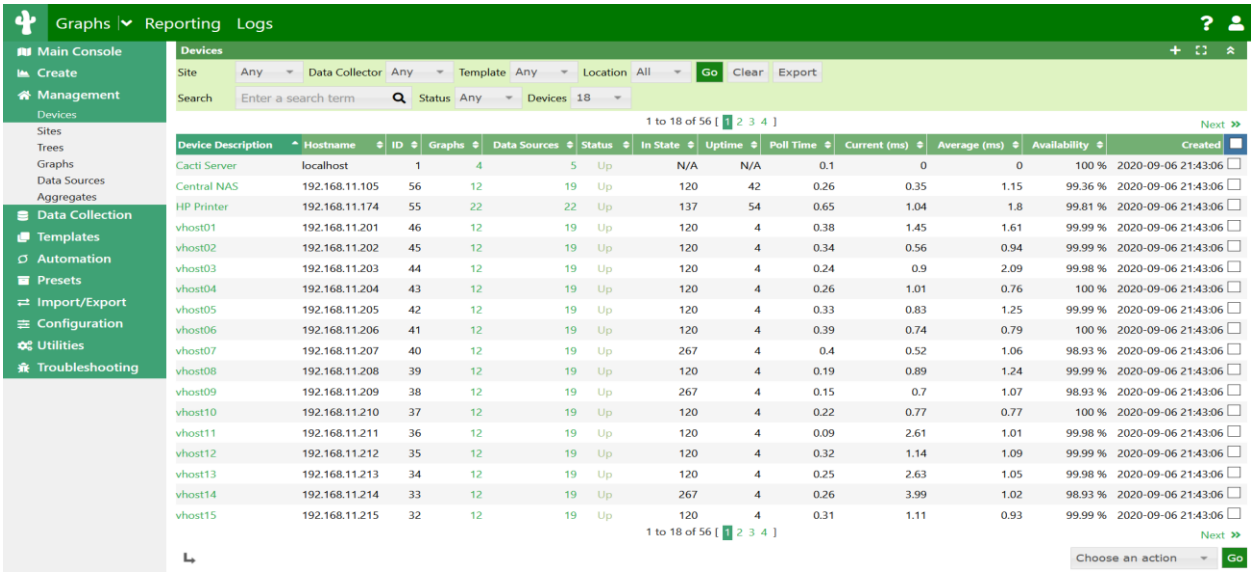


Figure 4 Cacti *(Cacti, 2021)*

For users across the world, Cacti offers a strong and adaptable operational monitoring and fault management system. Is also a full network graphing solution that makes use of RRDtool data storing and graphing capabilities. Cacti comes with a fully distributed and fault-tolerant data collection framework, advanced template-based automation features for Devices, Graphs, and Trees, multiple data acquisition methods, the ability to be extended through Plugins, role-based User, Group, and Domain management features, a theming engine, and multi-language support out of the box. All of this is packaged in a simple, intuitive UI that works for small LANs to large networks with tens of thousands of devices (Cacti, 2021).

2.3.2. Zabbix

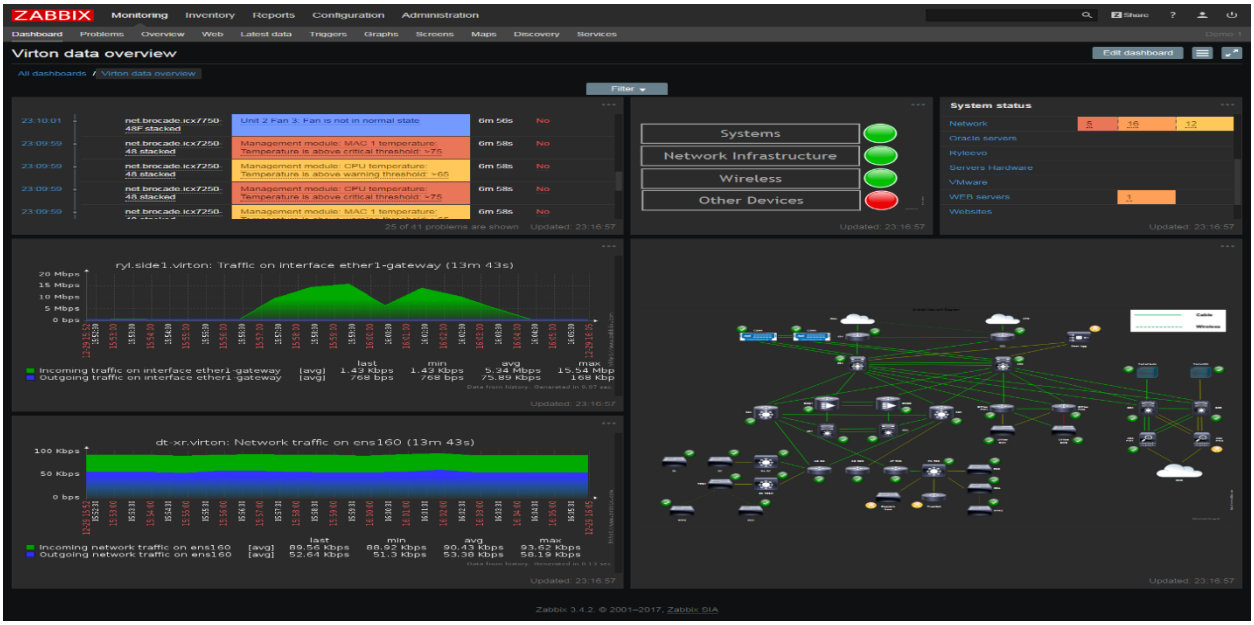


Figure 5 Zabbix *(Zabbix, 2021)*

Alexei Vladishev founded Zabbix, which is now actively developed and supported by Zabbix SIA. Zabbix is an open-source distributed monitoring system for businesses (Zabbix, 2021).

Zabbix is network monitoring software that checks the health and integrity of servers, virtual machines, applications, services, databases, websites, and the cloud, among other things. Zabbix has a versatile notification system that lets users to up e-mail-based notifications for almost any occurrence. This enables a quick response to server issues. Based on the recorded data, Zabbix provides strong reporting and data visualization options. Zabbix is therefore suitable for capacity planning (Zabbix, 2021).

Zabbix offers highly versatile and sophisticated threshold definition choices to its consumers. While a trigger threshold might be as basic as "larger than x," statistical analysis of historical data can take advantage of the full capability of supporting functions and operators (Zabbix, 2021).

2.3.3. Observium

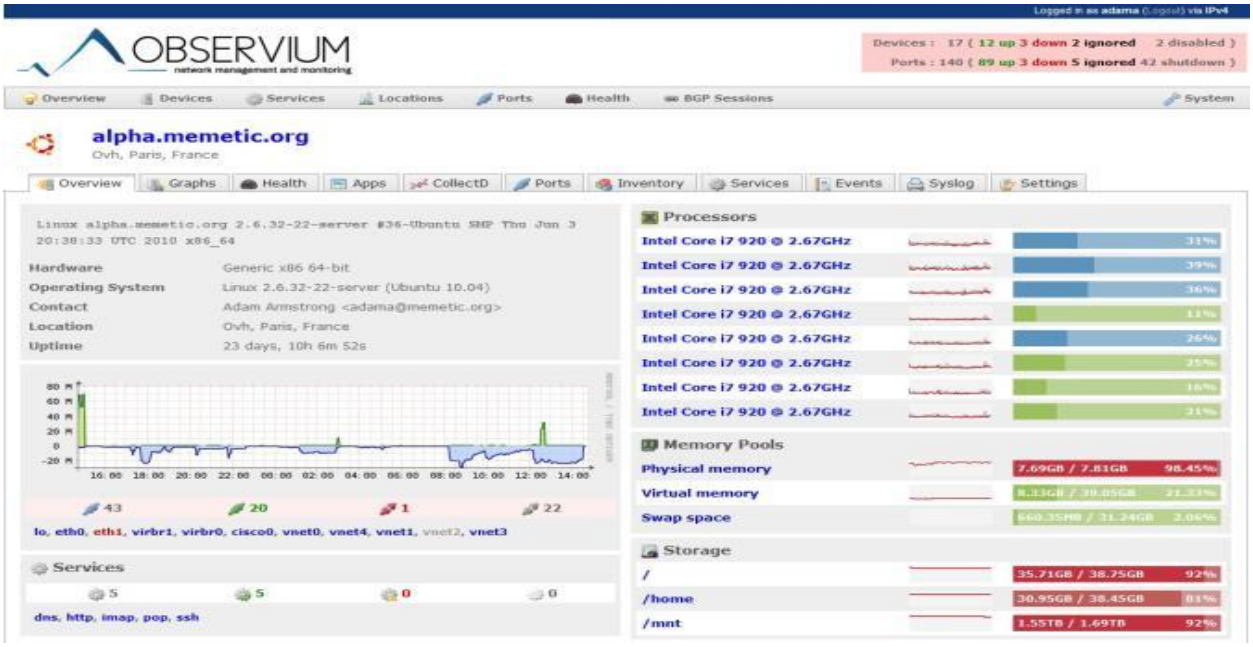


Figure 6 Observium *(Tecmint, 2015)*

Observium is a PHP/MySQL-based network observation and monitoring tool that works with a variety of operating systems and hardware platforms, including Linux, Windows, FreeBSD, Cisco, HP, Dell, NetApp, and others. It aims to provide a reliable and straightforward online interface for monitoring your network's health and performance (Tecmint, 2015).

With the aid of SNMP, Observium collects data from devices and displays it in a graphical pattern through a web interface. The RRDtool package is extensively

used. Its design aims include gathering as much history information on devices as possible, being completely auto discovered with little or no user intervention and having a quite simple yet powerful interface (Tecmint, 2015).

2.4. Comparison

2.4.1. Comparison Table

S. N	Features	Project 1	Project 2	Project 3	This Project
1.	Business use	×	×	×	✓
2.	License	✓	✓	✓	✓
3.	Alert system via email	×	×	×	✓
4.	Easy to use	✓	✓	✓	✓
5.	Dashboard	✓	✓	✓	✓
6.	Monitor applications, services, and systems.	×	×	✓	✓
7.	Port Scanning	×	×	×	✓
8.	Cost effective	✓	✓	✓	✓
9.	Real-time data visualization	✓	✓	✓	✓
10.	Live update	×	×	×	✓
11.	Technical expert requirement	×	×	×	✓

12.	Features to add new hosts and services	×	×	×	✓
13.	Features to check up/down time of the host and services	×	×	×	✓
14.	Remote data accessibility	×	×	×	✓
15.	Windows event logs monitor	×	×	×	✓

Table 2 Comparison of Similar Project

2.4.2. The Conclusion from Similar Projects

When we analyse all of the features offered by similar projects, we can see that the purposed system gives all of the features at an extremely low cost. With less complexity, it performs brilliantly. None of the projects had port scanning, application, service, or system monitoring, or a clear dashboard, all of which are critical for anybody to utilize in real-time. The system allows for remote access to analyse host and service logs, router and switch logs, and open port monitoring. The system also includes an alarm system that is unique among comparable initiatives and comes at an extremely low cost. In addition, the project's simple UI and dashboard make it more helpful in a number of ways.

3. Development

3.1. Considered Methodologies

3.1.1. Waterfall Methodology

The first Process Model to be introduced was the Waterfall Model. The Waterfall model is the most basic SDLC technique for software development. The waterfall model depicts the software development process as a sequential flow of events. This indicates that any step of the development process may start only after the preceding one has finished. The entire software development process is separated into several phases in "The Waterfall" technique. Typically, the output of one phase serves as the input for the following step in this Waterfall approach (Tutorialspoint, 2022). It is not possible for this project due to the possibility of future needs changing. The several phases of the Waterfall Model are depicted in the following diagram:

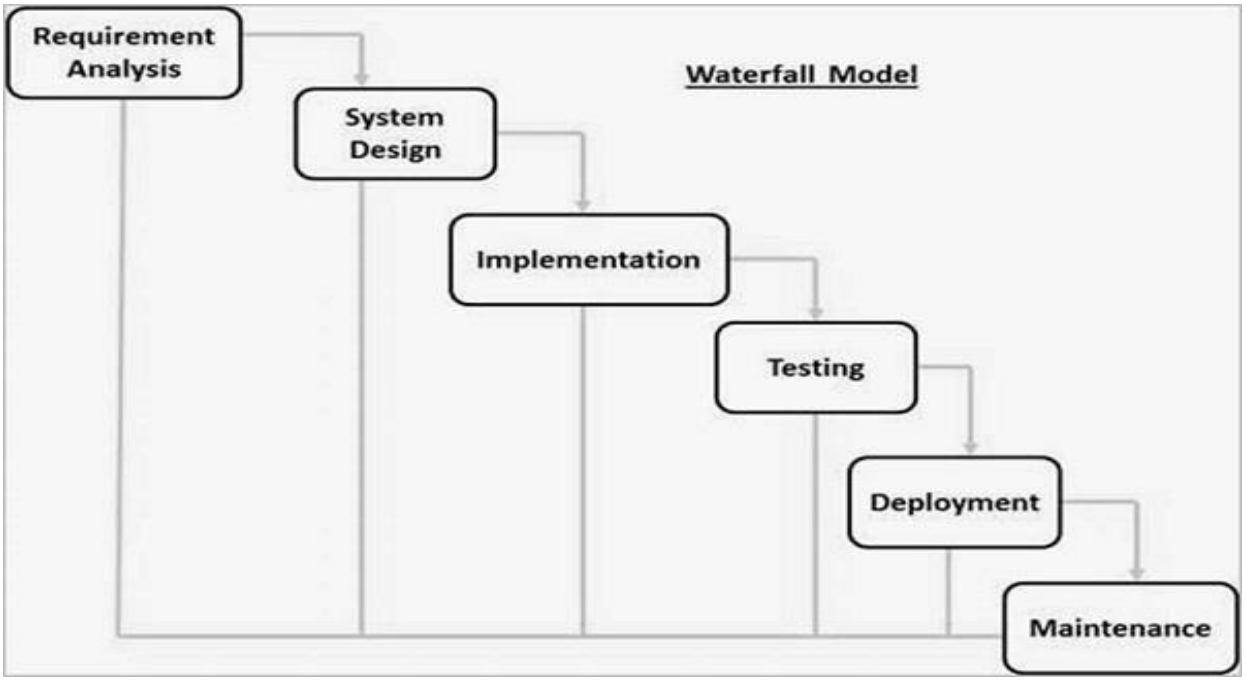


Figure 7 Waterfall Model *(Tutorialspoint, 2022)**.***

3.1.2. Spiral Model

The spiral model is one of the most important Software Development Life Cycle models for risk management. It resembles a spiral with several loops in diagrammatic depiction. The spiral's precise number of loops is unclear, and it varies from project to project. The project manager plays an essential role in developing a product utilizing the spiral model since the number of stages is constantly determined by the project manager. The spiral's radius at any point symbolizes the project's costs (cost) thus far, while the angular dimension represents the current phase's progress (GeekforGeeks, 2022). The process of obtaining information, gathering requirements, risk analysis, and providing feedback is beneficial, but it might be costly and time consuming. Risk analysis necessitates a prominent level of skill and is ineffective for small projects with minor risk and difficult to establish major objectives, milestones, and verifiable outcomes. The phases of the Spiral Model are depicted in the diagram below: –

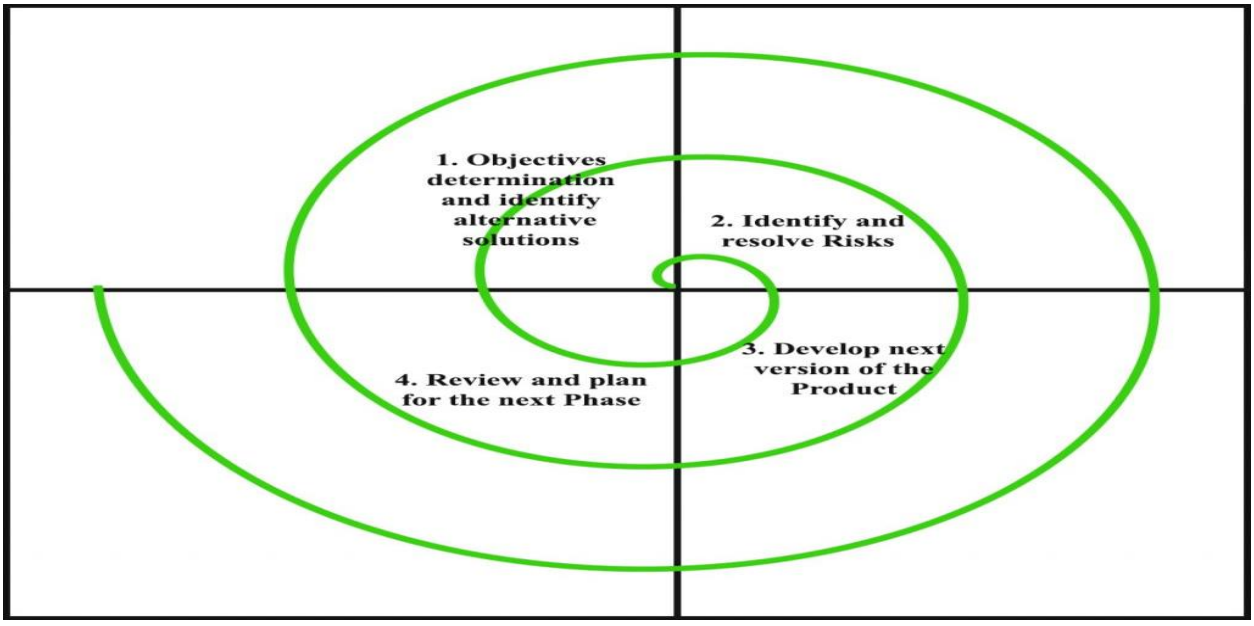


Figure 8 Spiral Model *(GeekforGeeks, 2022)**.***

3.2. Selected Methodology

3.2.1. Scrum Methodology

In this project, Scrum Methodology is used. Scrum is an iterative and incremental software development method. Scrum methodology is built on a set of well-defined principles and responsibilities that must be followed throughout the software development process. It is a flexible technique that recognizes the use of the 12 agile principles in a context that is agreed upon by all product team members. Scrum is carried out in short, periodic chunks known as Sprints, which normally last between two and four weeks and are used for feedback and reflection (Digite, 2021).

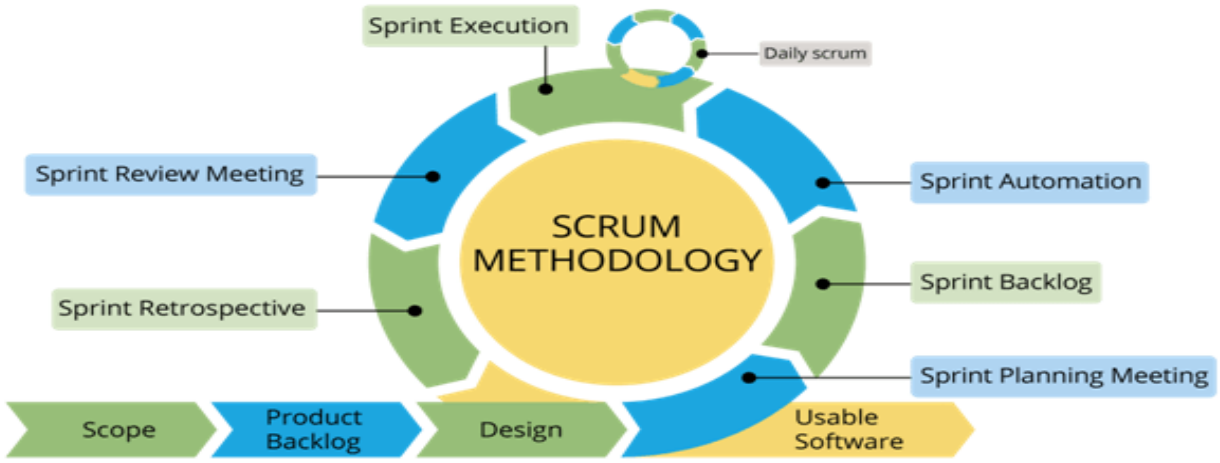


Figure 9 SCRUM Methodology *(Zaynabzahrablog, 2017)*

Compared to other agile development methods, Scrum has several benefits. In the software industry, it is now the most widely used and respected reference framework. Some of the well-known Scrum advantages are as follow:

- Risks are reduced.
- Prediction made at the right time.

- Software of higher quality.
- Reduced time to market.
- Easy to change.
- Scalable to any size.
- Expectations are also being reached.

3.3. Phases of Methodology

This project has 5 phases in it, which are as follows:

3.3.1. Project Initiation

This phase identifies the important level of scope, approval to begin the project by understanding users, and risks/constraints/assumptions.

3.3.2. Project Planning

To construct a project management strategy, specialists gather detailed needs and assumptions. The project's WBS (Work Breakdown Structure), timeline, budget, and resources are then decided.

3.3.3. Project Execution

Project resource management, project change approval, quality assurance, and communication with the are all completed.

3.3.4. Project Monitoring and Control

Measures project cost, quality, schedule controls, project threats and updating those risks, as well as interacting with experts and supervisors about the project.

3.3.5. Project Closure

Customer satisfaction is measured, all project reports and papers are finalized, ownership of deliverables is transferred, and the final project report is sent.

3.4. Survey Results

3.4.1. Pre-Survey Results

For the pre-requirement collection procedure, a pre-survey was performed. It benefited in the evaluation of the system's features and functions. This survey was conducted among 15 persons of various ages, vocations, and genders (80 percent male and 20 percent female). Seven of them were students from the Islington College, and eight of them worked in the IT specialist in Sanima Bank, Naxal.

93.8 percent of them knew about the Network Monitoring tools and 17.2 percent of them did not knew about it. 43.8 percent of the total users used the network monitoring tools sometimes, 25 percent of the total users did not use the network monitoring tools yet and 31.3 percent of the total users used the network monitoring tools almost regularly where most of the users were from the bank's IT department.75 percent of the total users preferred the Nagios as their favourite tool for monitoring the network, 12.5 percent preferred to use Zabbix as their favourite tool, 0 percent of them preferred Cacti and 12.5 percent of the total users preferred other tools as their favourite network monitoring tool. 43.8 percent of the total users were interested to check their network's down/up time, 12.5 percent of the total users have not checked or not interested to check their network's up/down time and 43.8 percent of the total users were interested

to check their network's up/down time in the future. 93.8 percent of the total users were thinking that the tool's simple UI and the reports generated in graphs can be useful for everyone to keep the network safe. 0 percent users marked as "No" which means that the feature will be useful, and 17.2 percent of the total users marked "Maybe" the feature will be useful. Other different information is shown in the Appendix section and can be found by clicking in the following link.

3.4.2. Post-Survey Results

For the post-requirement collection procedure, a pro-survey was performed. It benefited in the evaluation of the system's features and functions. This survey was conducted among 21 persons of various ages, vocations, and genders (85.7 percent male and 14.3 percent female). Fourteen of them were students from the Islington College, and three of them worked in the IT specialist in Sanima Bank, Naxal and four of them were mine other close friends from other college.

90.5 percent of them knew about the Network Monitoring tools and they thought that the tool is user-friendly and 9.5 percent of them did not knew about it and marked as maybe. 66.7 percent of the total users used the network monitoring tools sometimes and they think the tool will monitor the host and services as does port scanning in an excellent way, 23.8 percent of the total users marked as Good, and 9.5 percent of the total users marked as Fair. 42.9 percent of the total users rated the ScanNet tool 9/10, and 33.3 percent of the users rated it as 10/10 and other remaining users rated 5,6,7

and 8 out of 10. 57.1 percent of the users marked Excellent and think this feature added in Nagios to display the logs in graphs and does open port scanning works well. 33.3 percent of the marked as Good and 9.5 percent of the remaining users marked as Fair. 38.1 percent of the users rated the Open Port Scanning features as 10/10, 28.6 percent of the users rated 9/10, 23.8 percent of the users rated 8/10, 4.8 percent rated 7/10 and 4.8 percent user rated 4/10. Other different information is shown in the Appendix section and can be found by clicking in the following link.

3.5. Requirement Analysis

All the requirements analysis is done as per the research and inquiries done with the IT professionals and the features are developed for the Nagios according to that. The requirements and features are elaborated and specified below:

3.5.1. The system should be able to monitor logs of host machine and Linux machine:

The project should be able to track the information and show the Okay, Critical, and Warning logs created by the Windows hosts and Linux host system.

3.5.2. The system should be able to monitor all the open port of the hosts:

The project must be able to monitor all the open ports through the script to analyse real-time open ports in the system or network.

3.5.3. The system should be able to check the up/down time of the hosts and services:

The project must display the host and services according to the configurations made for them in the Nagios and monitor the down/up state of the host and services.

3.5.4. Display:

All the hosts and services that are added inside the Nagios configuration file through the medium of different agents should be displayed in the dashboard of the Nagios core. And this can help the user to make incidence plan to any of the errors or problems.

3.5.5. Cost-effective:

This project is developed with different programming languages and different software and is cost-effective and can easily help in any business organizations.

3.6. Design

3.6.1. Use Case Diagram

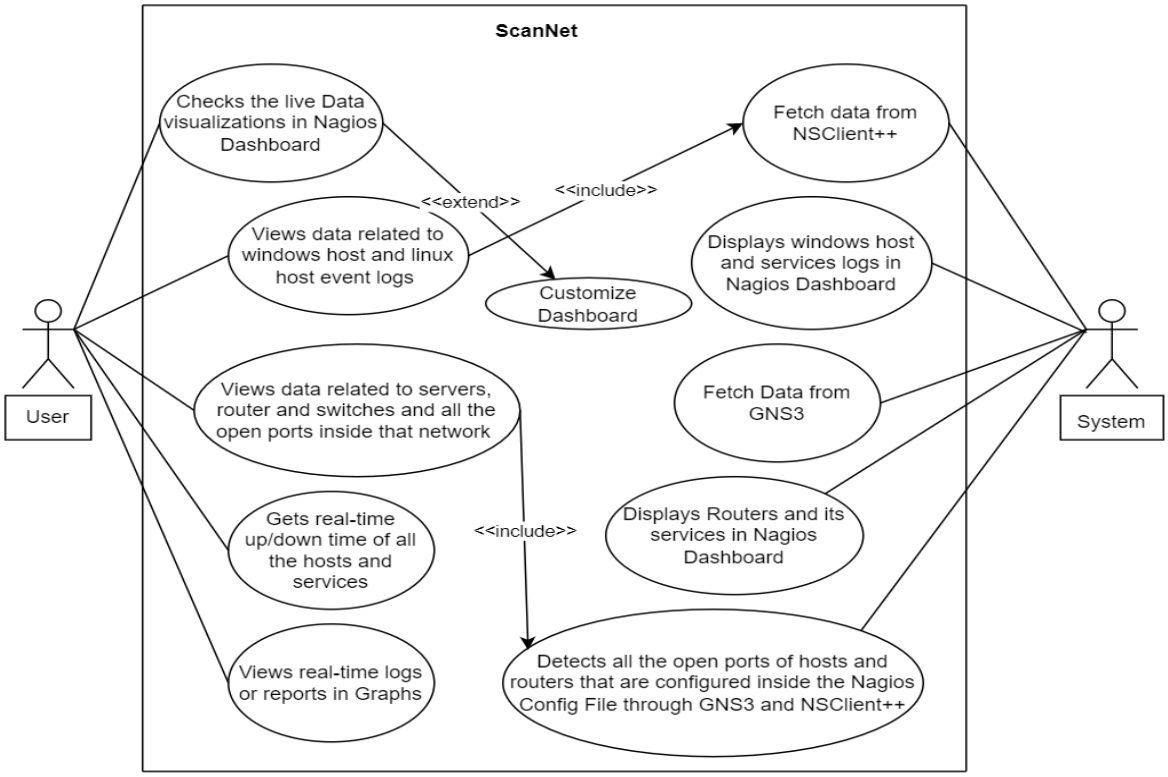


Figure 10 Use Case Diagram.

3.6.2. Block Diagram

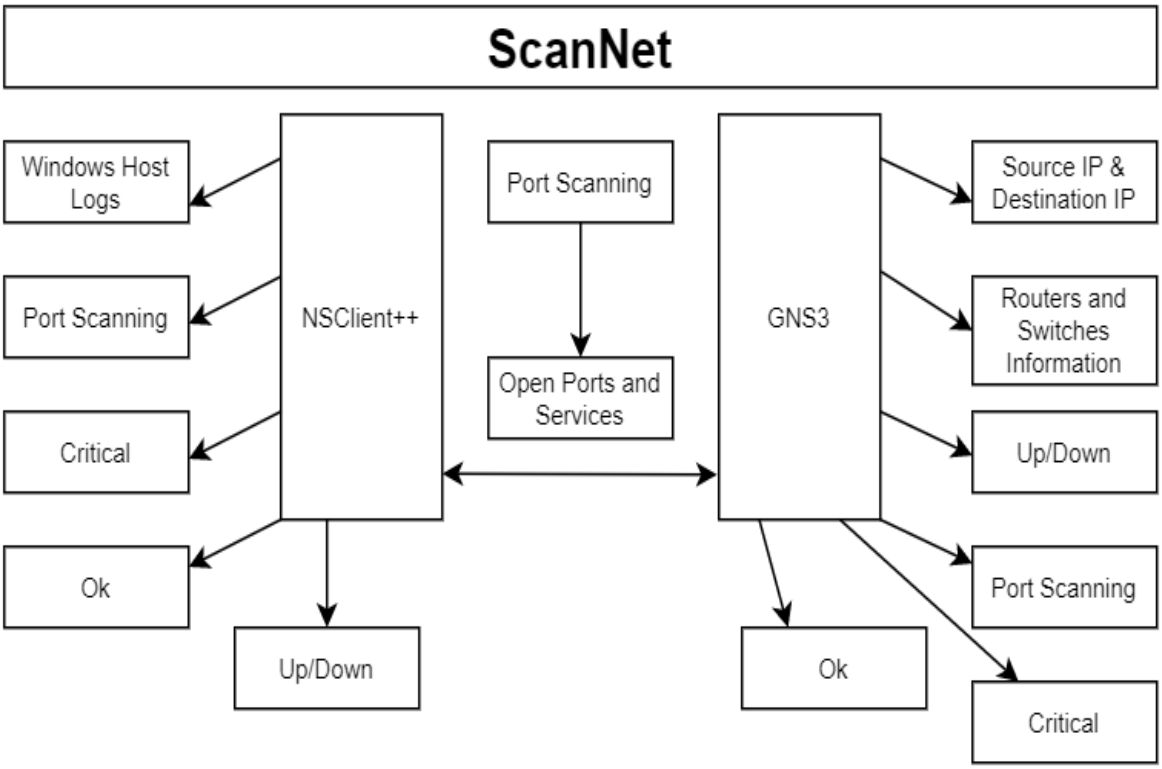


Figure 11 Block Diagram

3.6.3. Flowchart

3.6.3.1. Flowchart of ScanNet

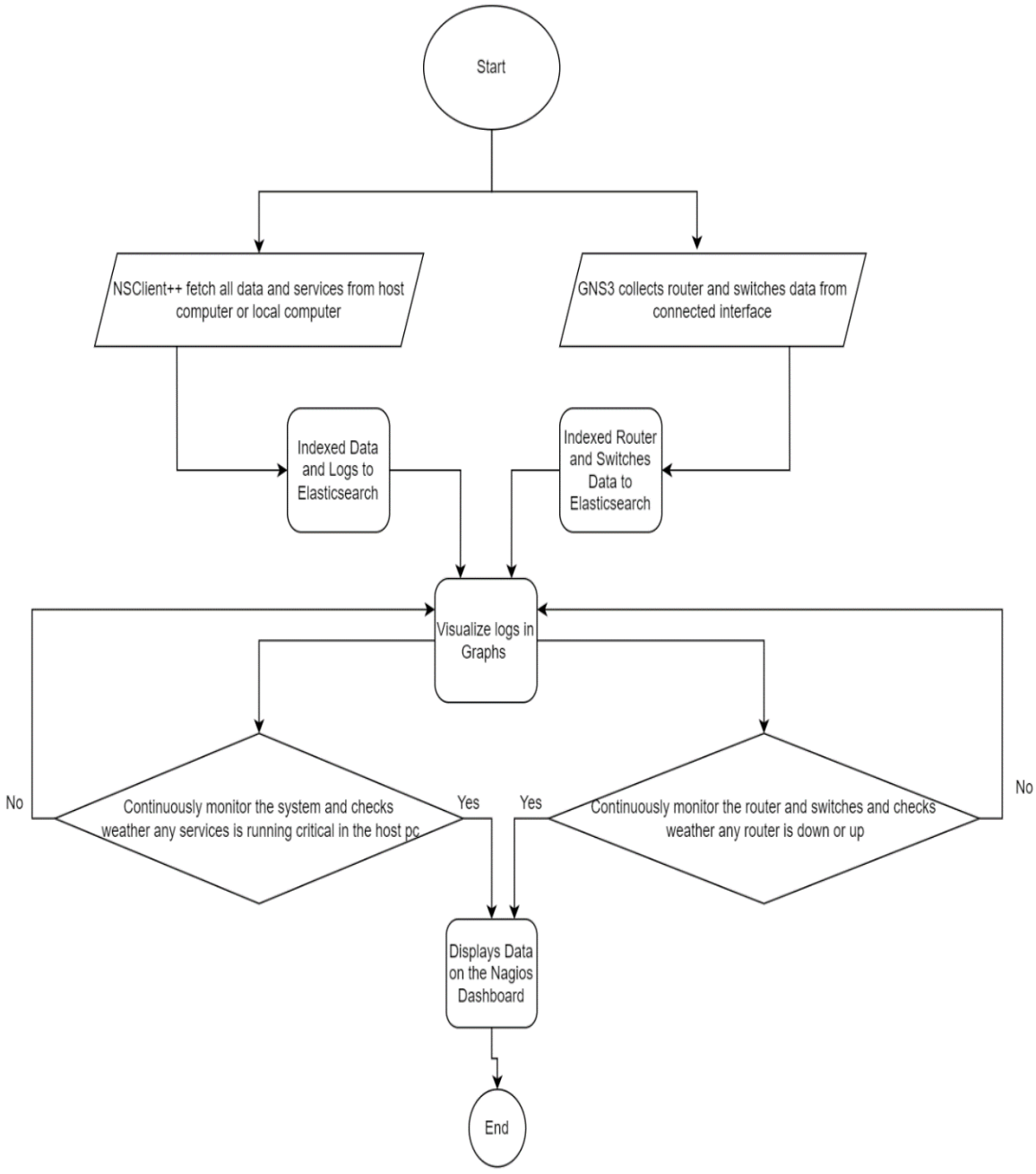


Figure 12 Flowchart of ScanNet

3.6.3.2. Flowchart of the Port Scanning feature to Check the Open Ports inside a Network.

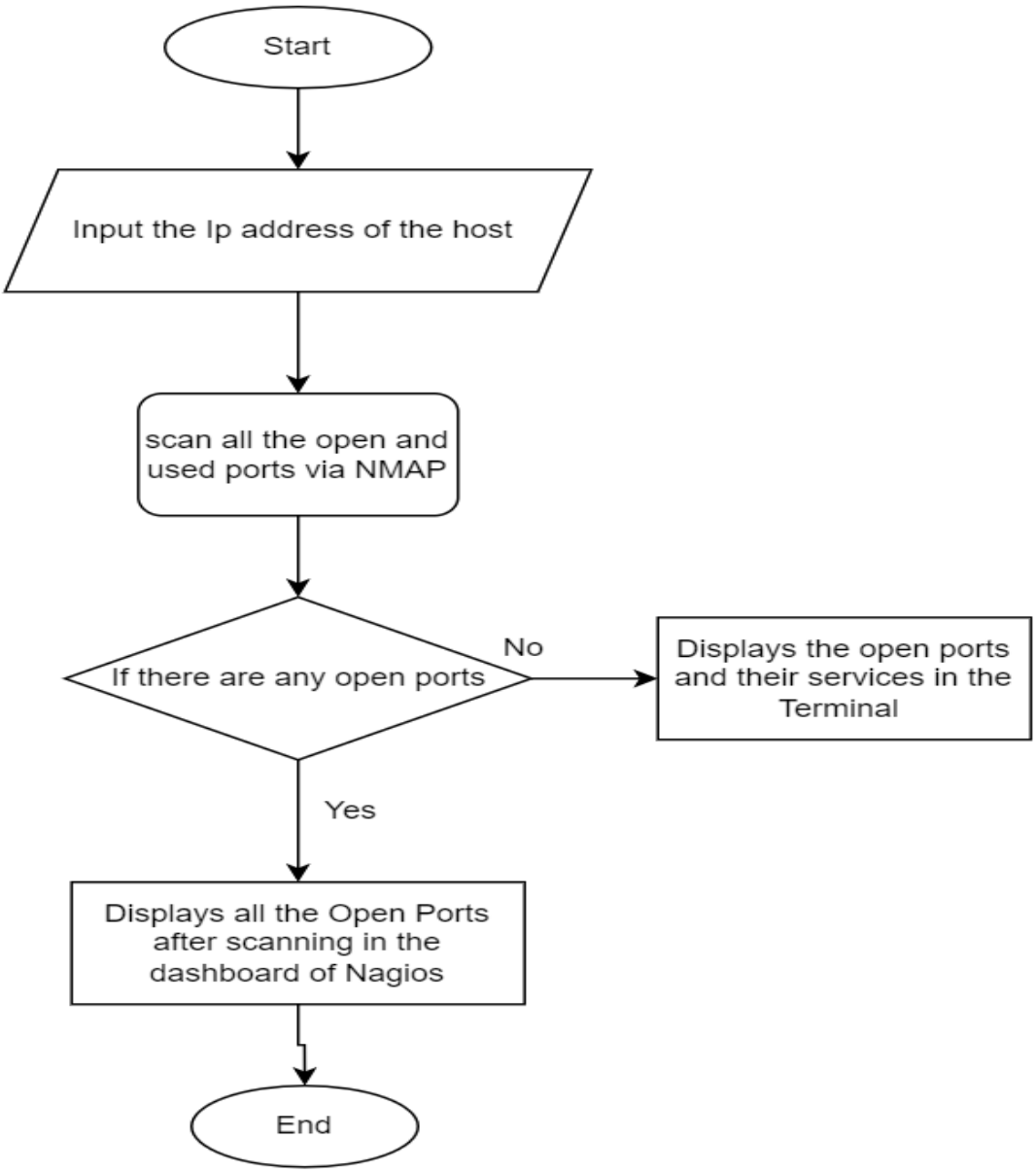


Figure 13 Flowchart of the Port Scanning feature to Check the Open Ports inside a Network.

3.7. Implementation

The project's implementation is carried out utilizing a variety of tools and methodologies. These tools and processes support in the system's development and implementation. The implementation is thoroughly demonstrated by showing screenshots to describe the software and technologies utilized.

3.7.1. Primary Components

i. Oracle VM VirtualBox

VirtualBox is a strong x86 and AMD64/Intel64 virtualization tool that can be used in both the workplace and at home. VirtualBox now supports a wide range of guest operating systems, including Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x, and 4.x), Solaris and Open Solaris, OS/2, and OpenBSD (Virtualbox, 2022). Some more screenshots of it can be found in the link below:

8.3.2.1. Screenshots of Oracle VM Virtual box

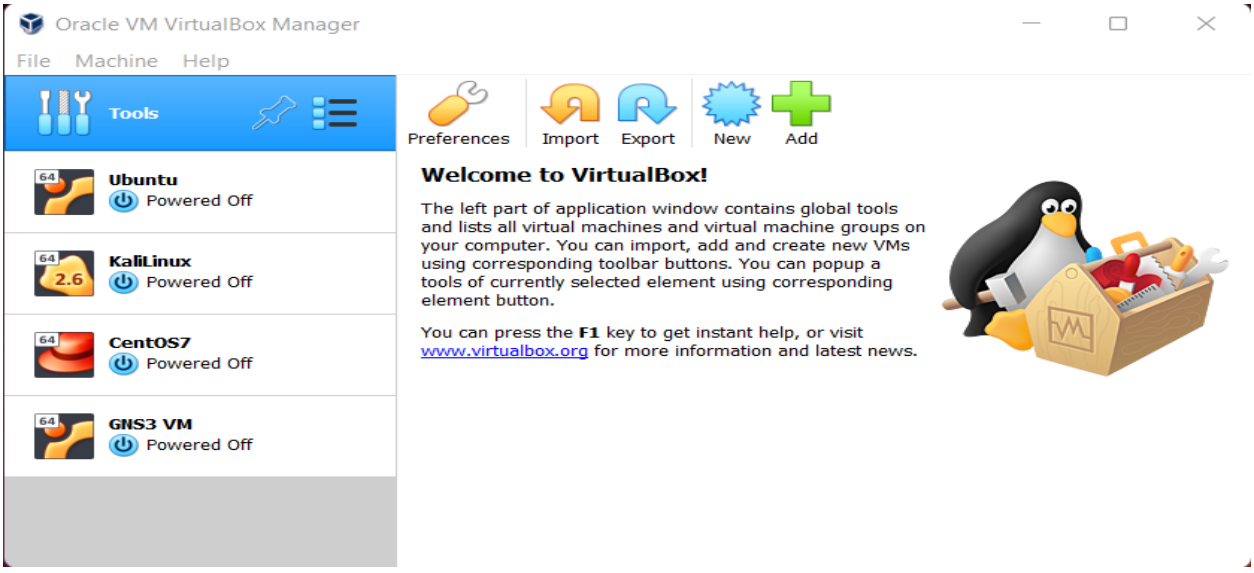


Figure 14 Oracle VM VirtualBox

ii. CentOS

CentOS Linux is a community-supported distribution based on Red Hat or CentOS git for Red Hat Enterprise Linux sources that are freely available to the public (RHEL). As a result, CentOS Linux aspires to be functionally equivalent to Red Hat Enterprise Linux (RHEL). The CentOS Project modifies packages to remove upstream vendor branding and artwork. CentOS Linux is a free and open-source operating system that may be redistributed without charge (CentOS, 2022). Some more screenshots of it can be found in the link below:

8.3.2.2. Screenshots of CentOS

Figure 15 Starting CentOS

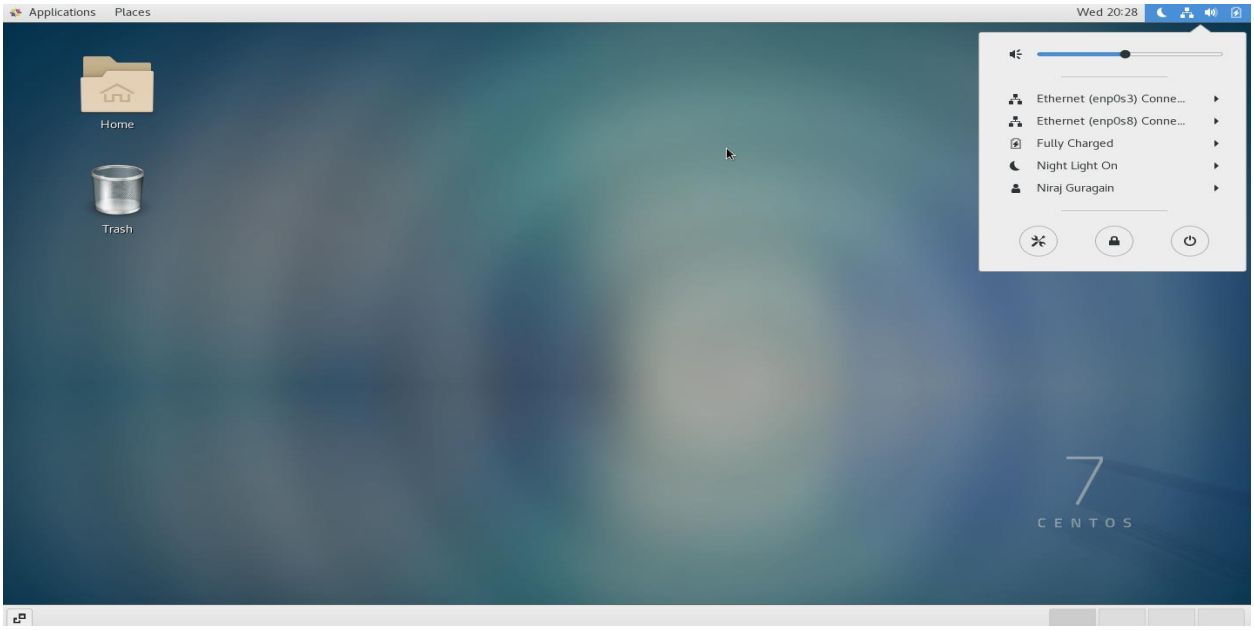


Figure 16 CentOS

iii. Putty

PuTTY is a telnet and SSH client for Windows that was created by Simon Tatham. PuTTY is free, open-source software that is created and maintained by volunteers (Putty, 2022).

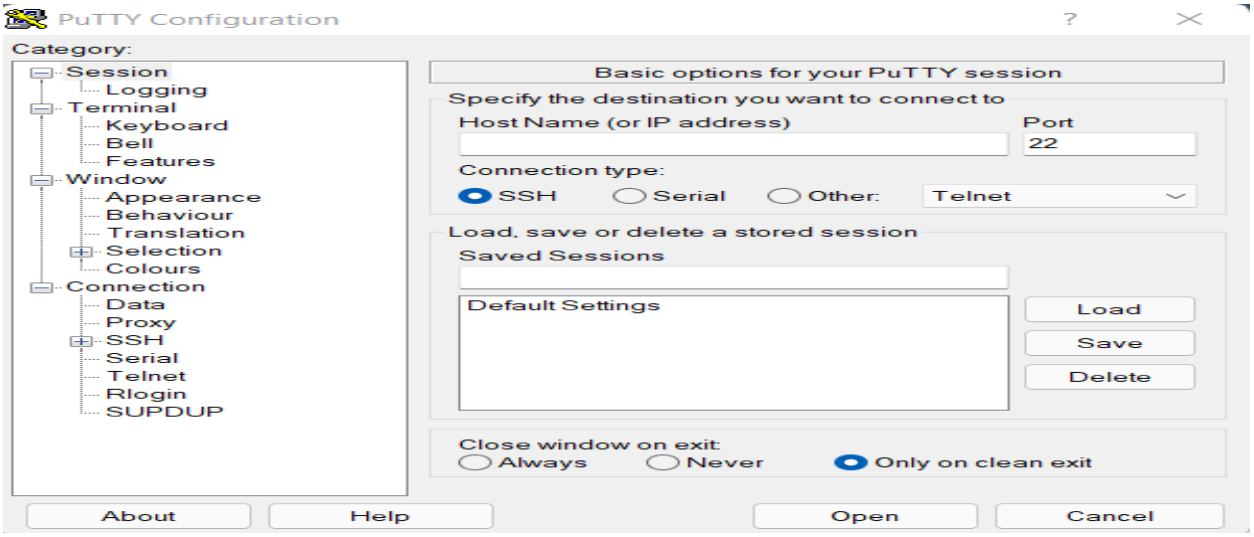


Figure 17 UI of Putty

iv. Nagios Core

Nagios Core is a network monitoring and system administration program that is free and open source. It keeps an eye on the hosts and services we provide, notifying us when something goes wrong and when things improve. Nagios Core was developed with Linux in mind; however, it should run on most other operating systems (Core, 2022). Some more screenshots of it can be found in the link below:

7.3.2.4. Screenshots of Nagios Core

7.4.2. Configurations made for router and services in Nagios Server.

7.4.1. Configuration made for Host and Services in Nagios Server.

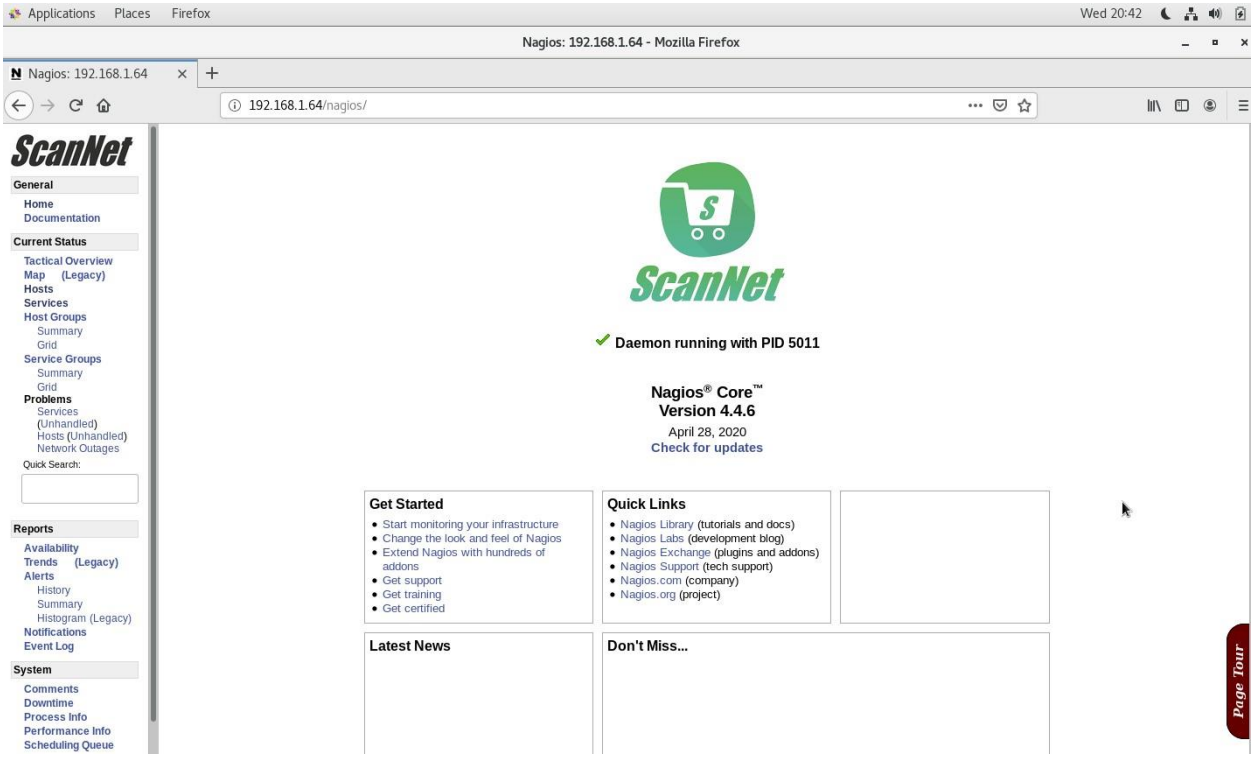


Figure 18 Home page of Nagios

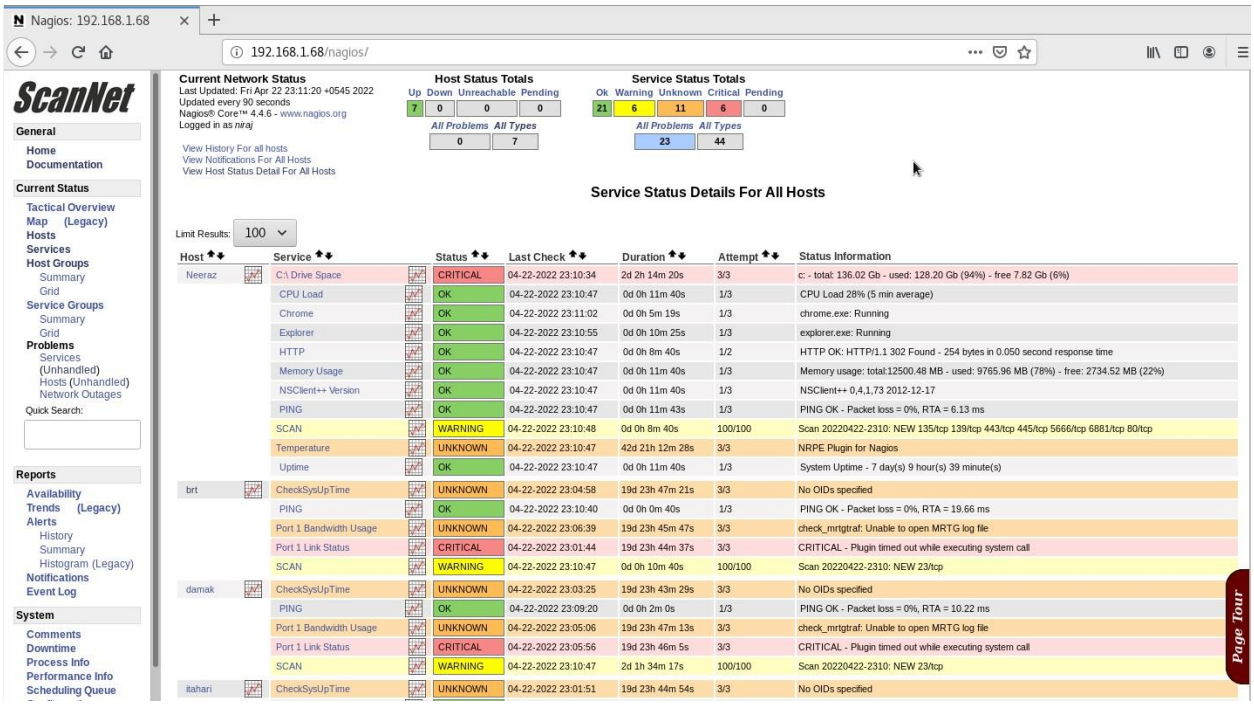


Figure 19 Monitoring all the services in Nagios Dashboard

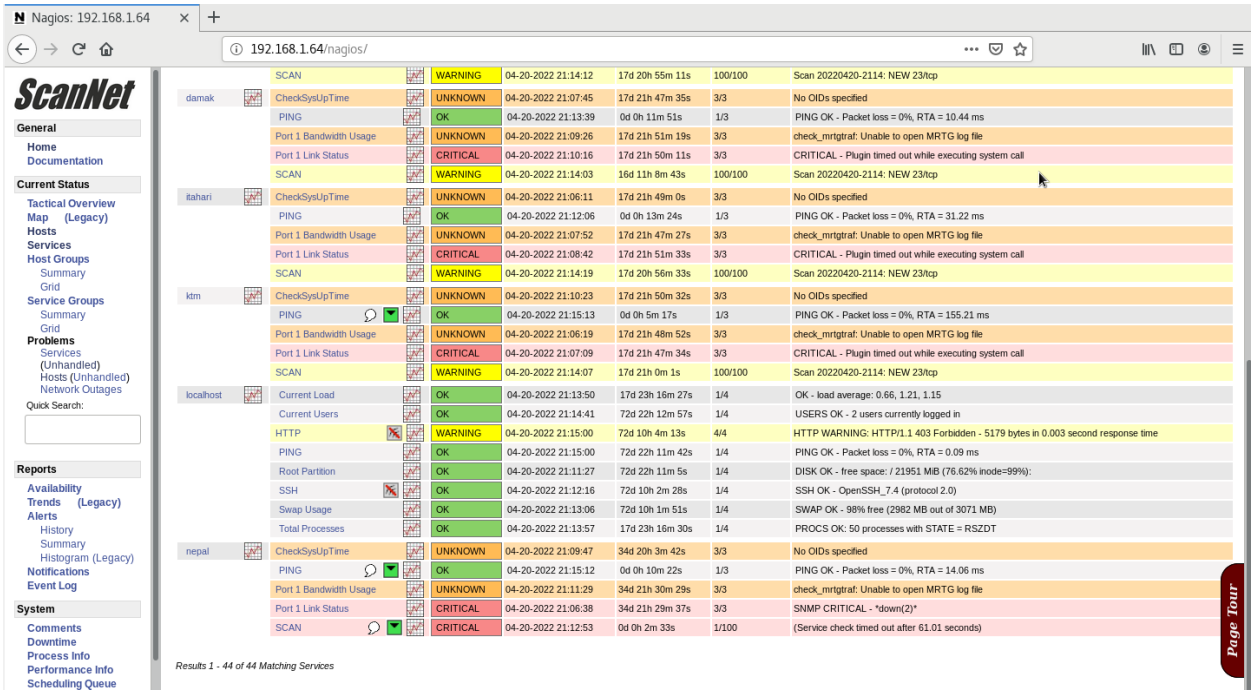


Figure 20 Monitoring all the services in Nagios Dashboard

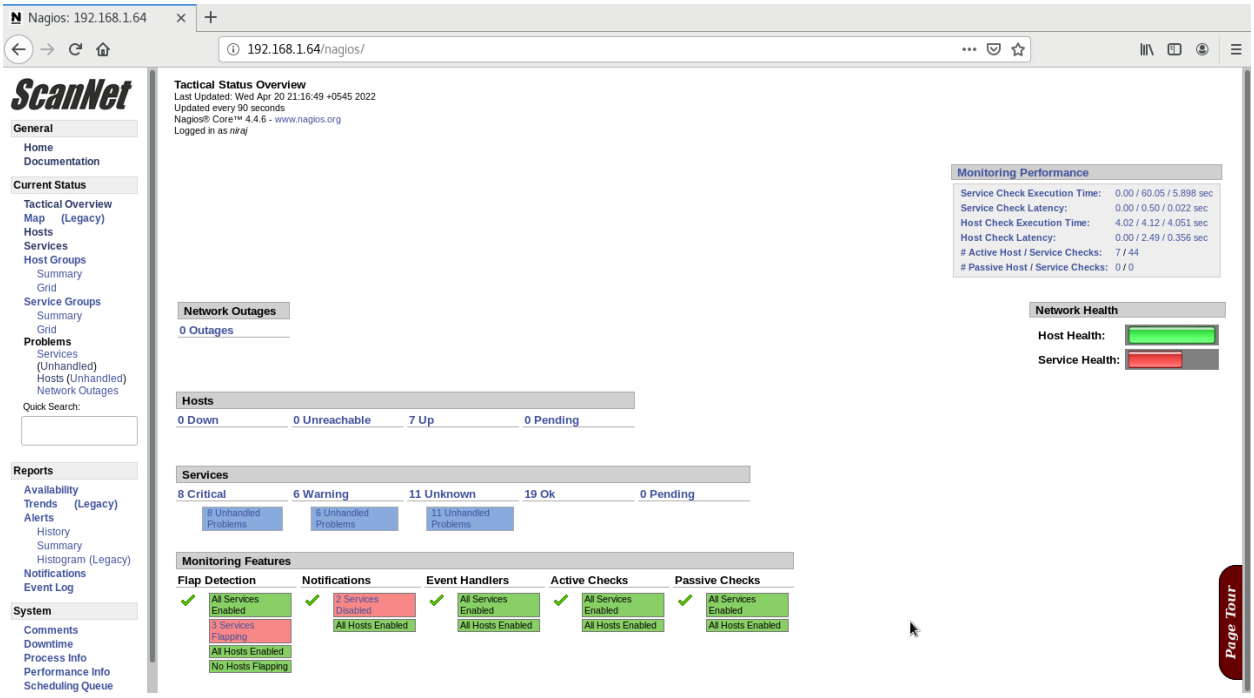


Figure 21 Tactical Status Overview of Hosts and Services

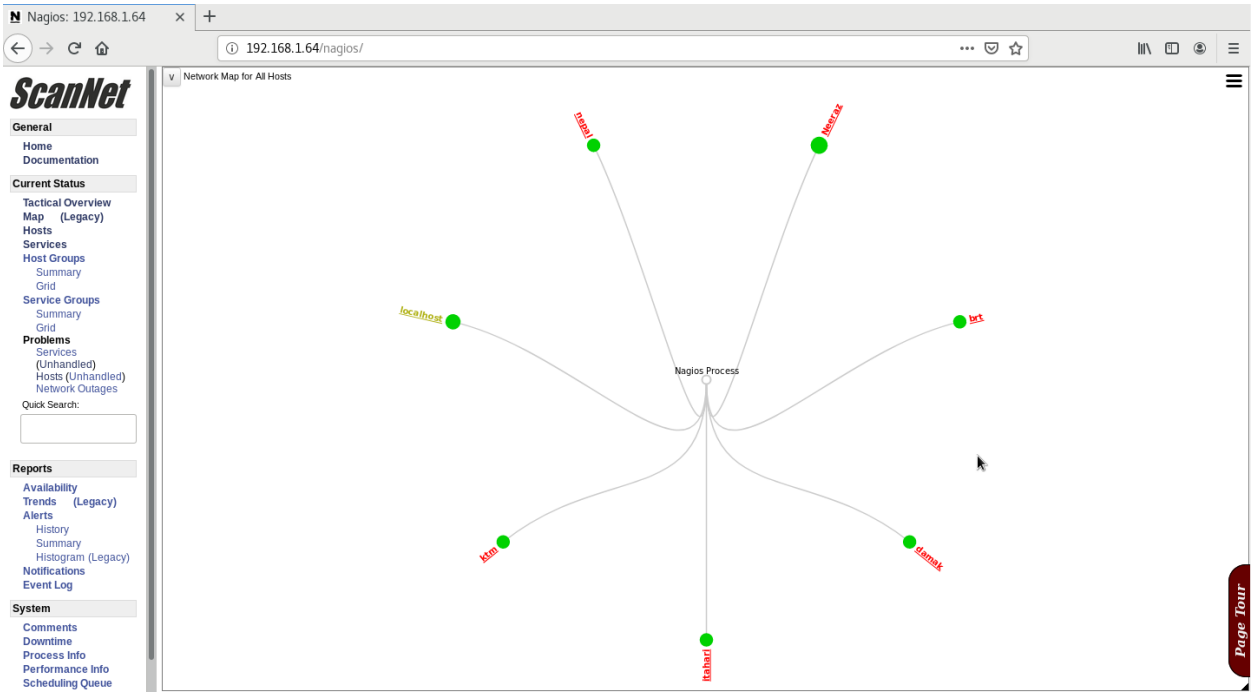


Figure 22 Map of the connected hosts in Nagios

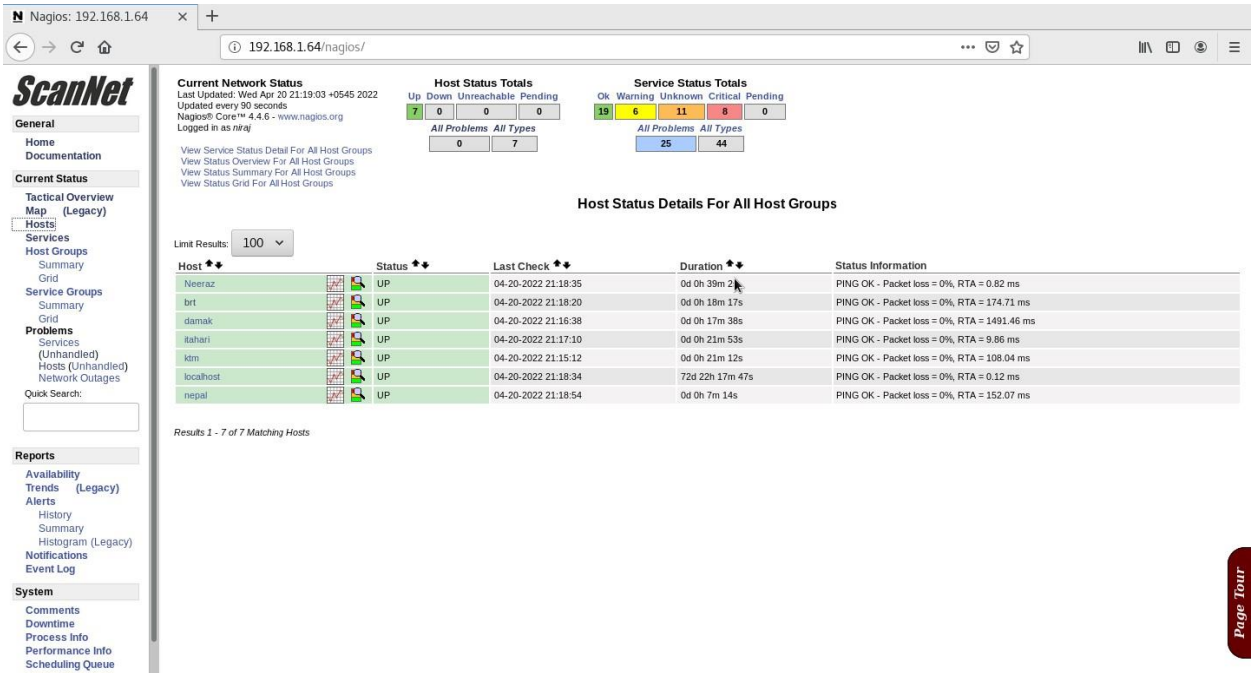


Figure 23 Host status details

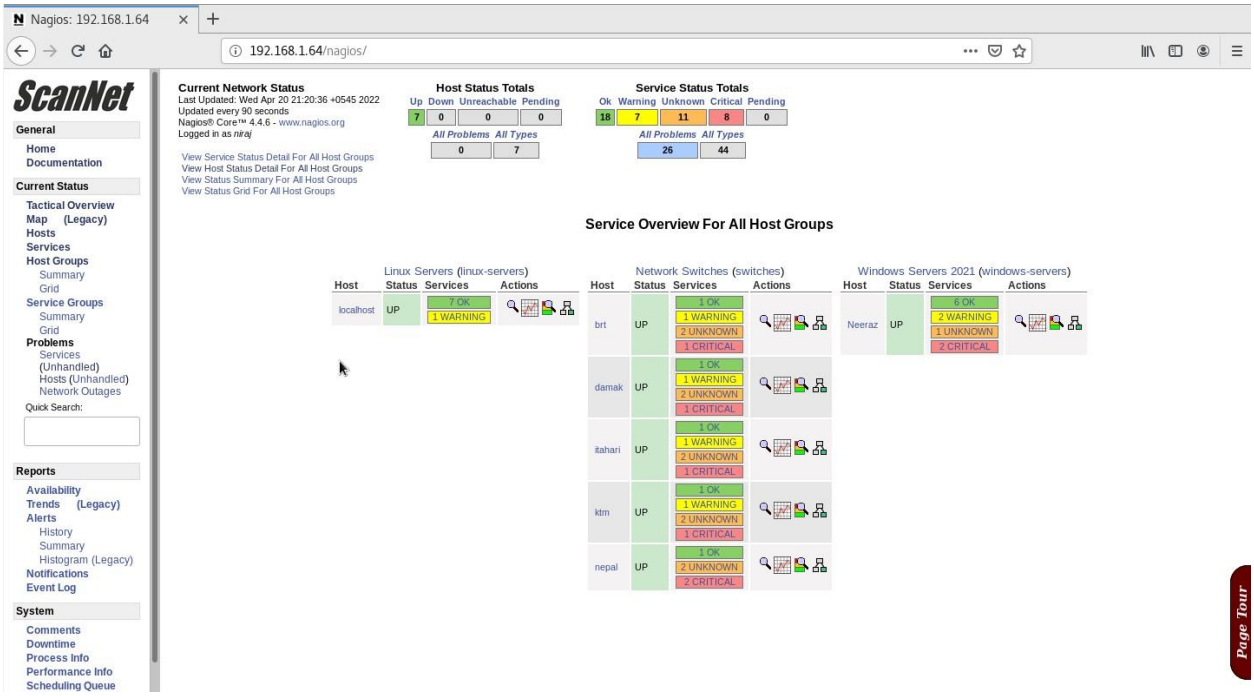


Figure 24 Service Overview for all host groups

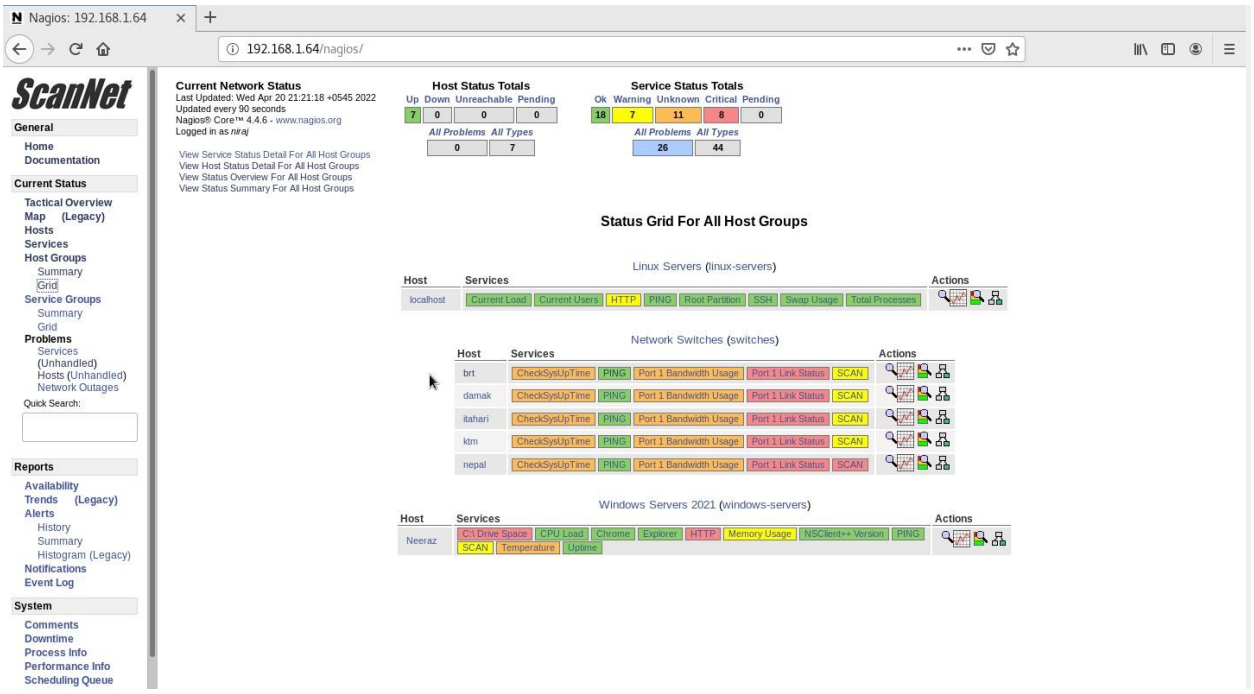


Figure 25 Status grid for all host groups

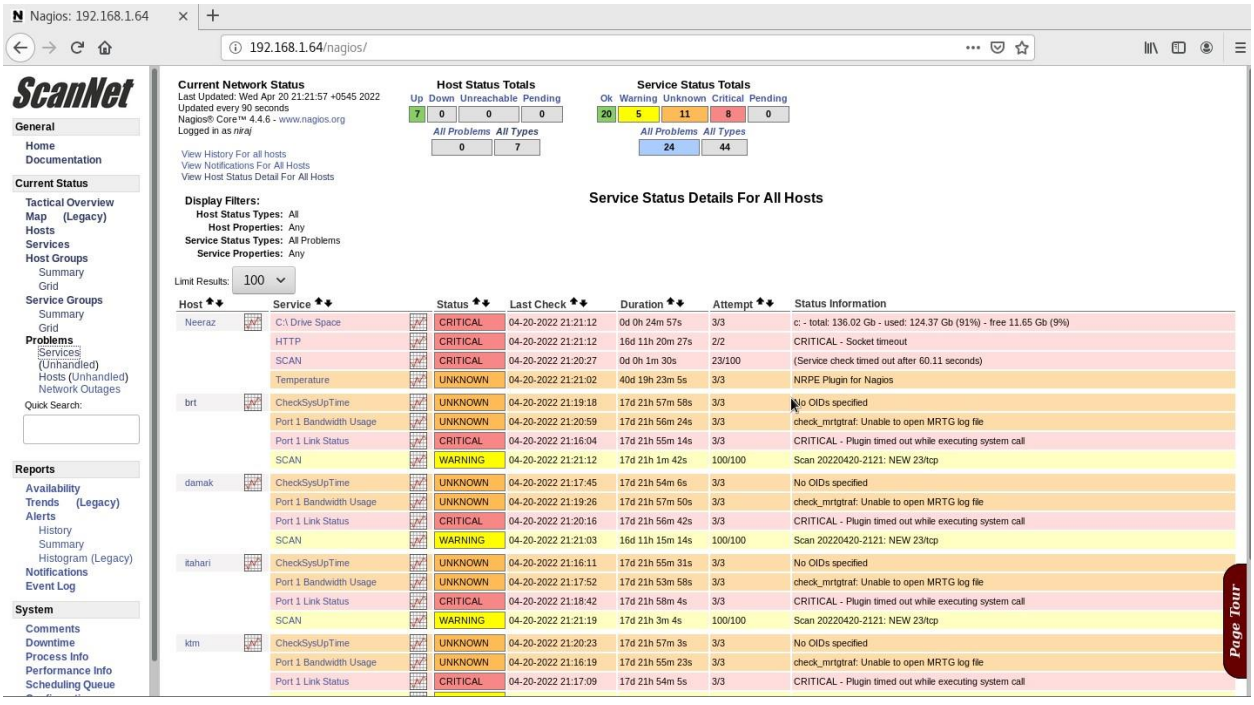


Figure 26 Unhandled services details for all hosts

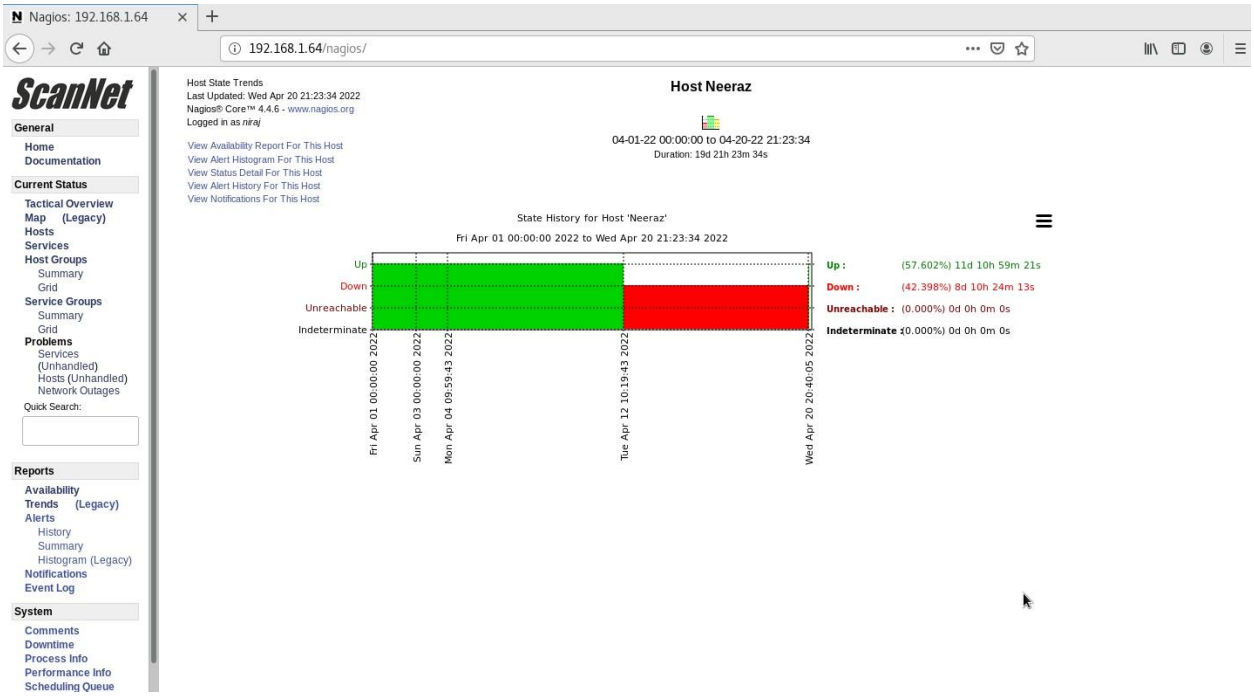


Figure 27 State History of Host 'Neeraz' in 1 months

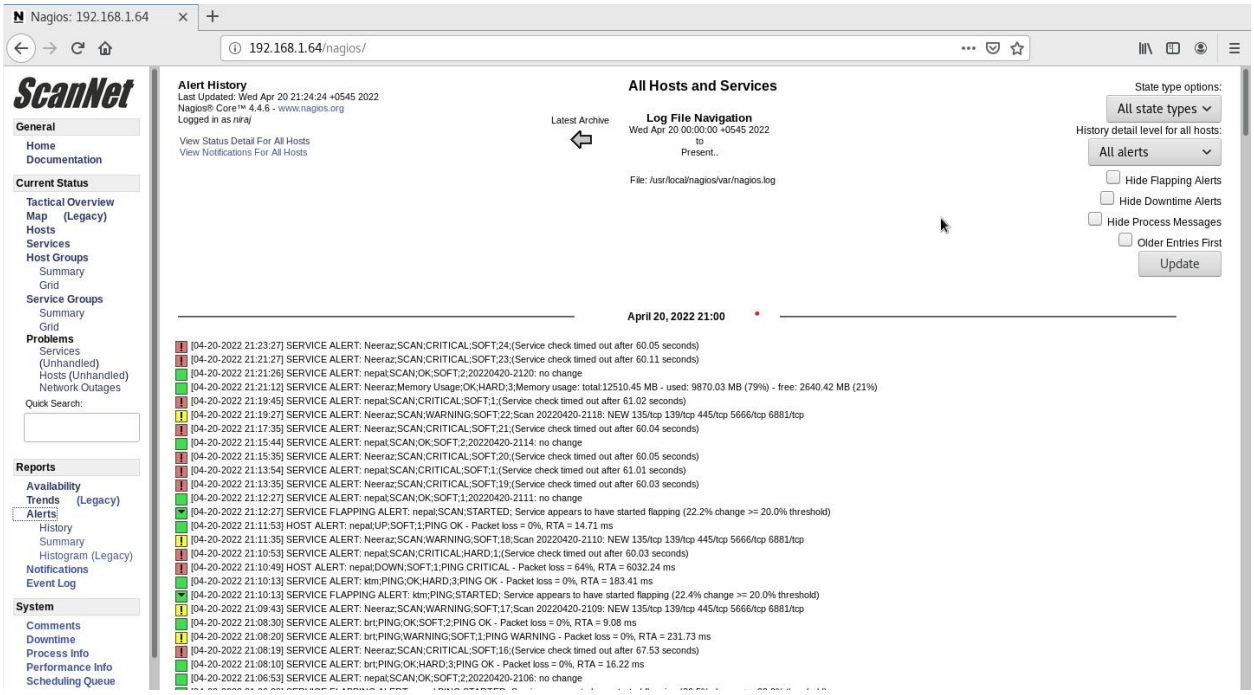


Figure 28 All the Alerts

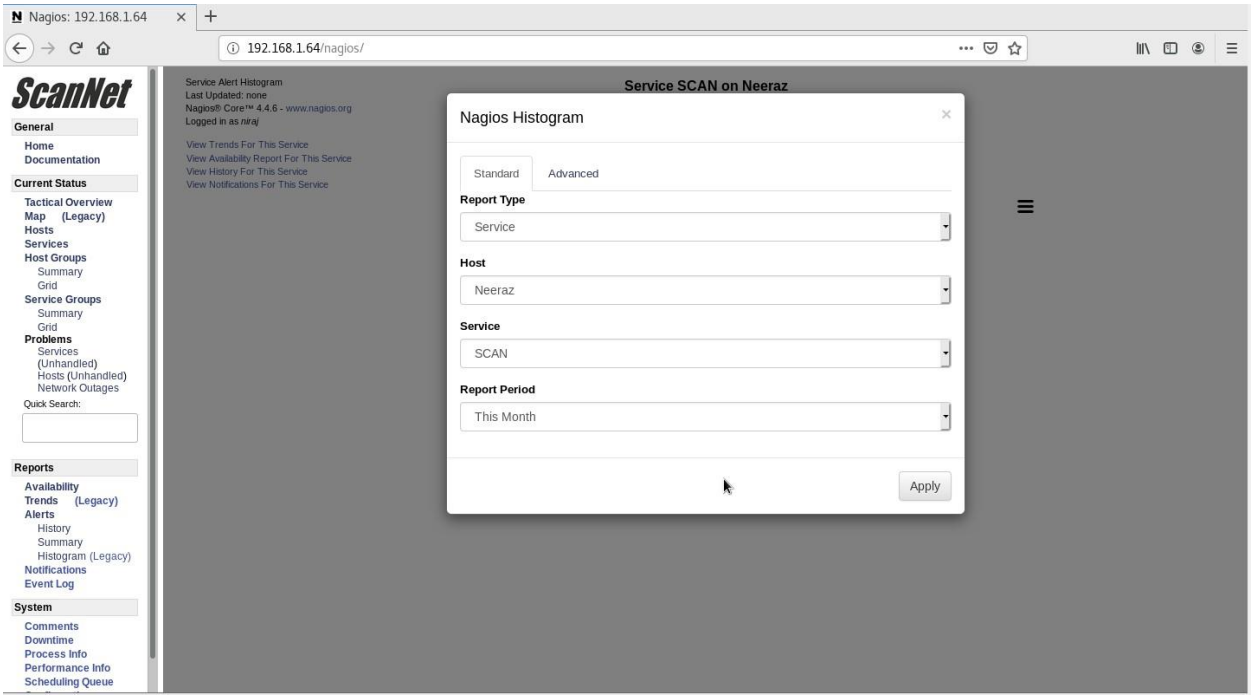


Figure 29 Displaying histogram of 'SCAN' service running in 'Neeraz' host

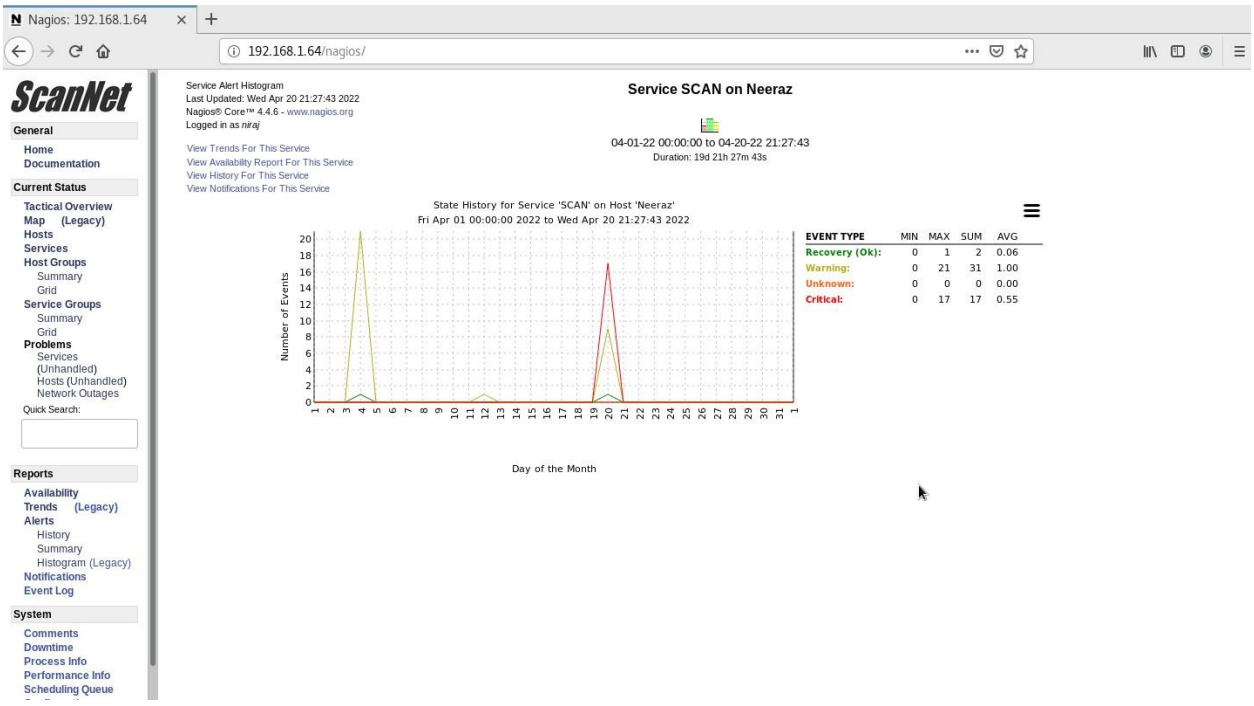


Figure 30 State History of 'SCAN' in 1 months

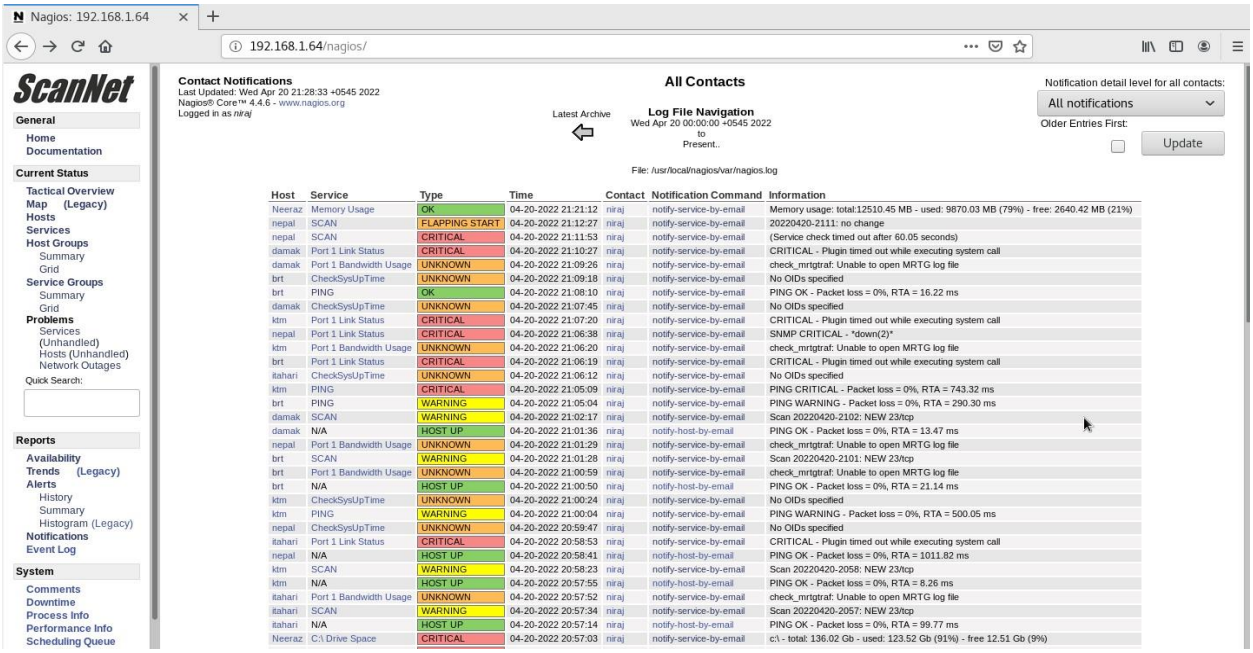


Figure 31 Notifications from beginning to present time

v. WinSCP

WinSCP is a free SFTP, FTP, WebDAV, S3 and SCP client for Windows that is available as an open-source project. File transfer between a local and a distant computer is its primary function. WinSCP also has scripting and a simple file management (WinSCP, 2022). Some more screenshots of it can be found in the link below:

[7.3.2.5. Screenshots of WinSCP]

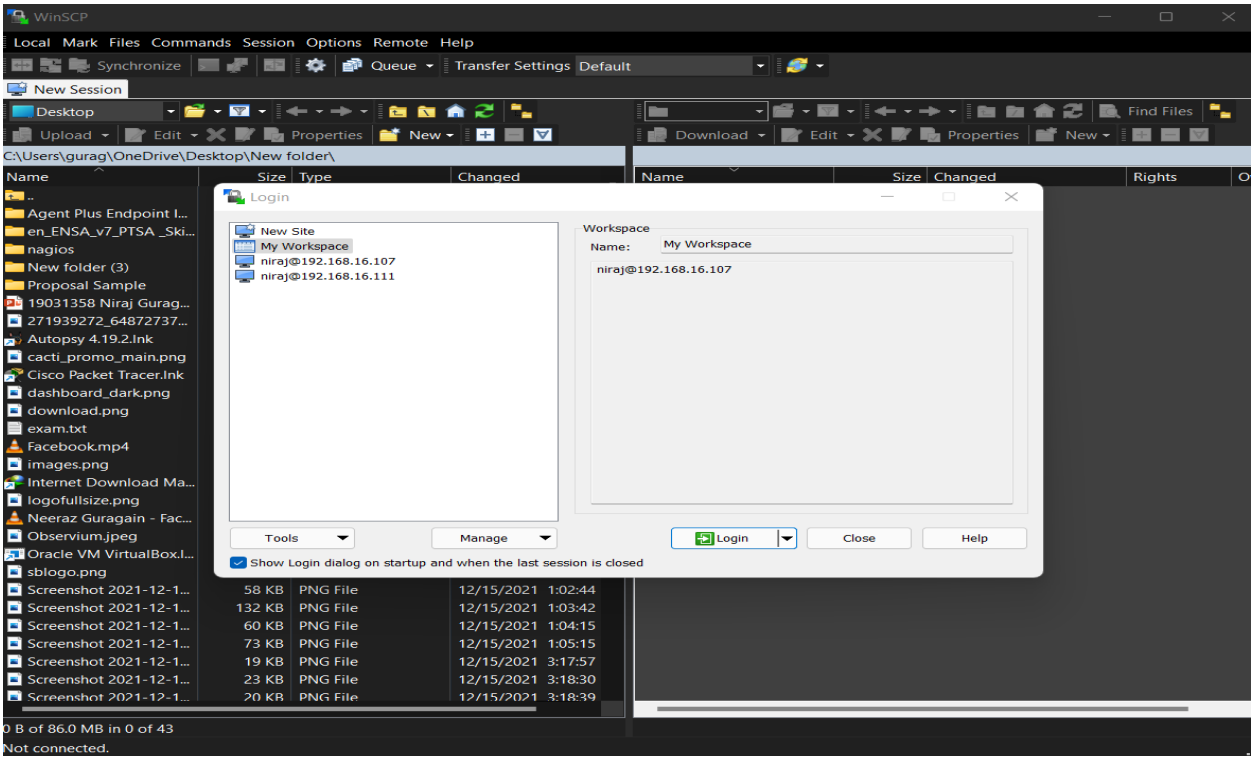


Figure 32 Starting WinSCP

vi. NSClient++

NSClient++ (nscp) is a monitoring daemon that strives to be simple to use while yet being strong and secure. It was created for Nagios/Icinga/Neamon, but there is nothing in the daemon that is particular to Nagios/Icinga/Neamon, and it may be used in a variety of scenarios where check metrics are received and distributed. Allow a distant machine (the monitoring server) to send instructions to this machine (the monitored machine) that report the machine's status. Send the same findings to a distant location (monitoring server). Act and finish the things you have set out for us. To a central repository, provide measurements and real-time data (NSClient++, 2022). Some more screenshots of it can be found in the link below:

[7.4.3. Configuration made inside NSClient++ for monitoring windows host and logs.]

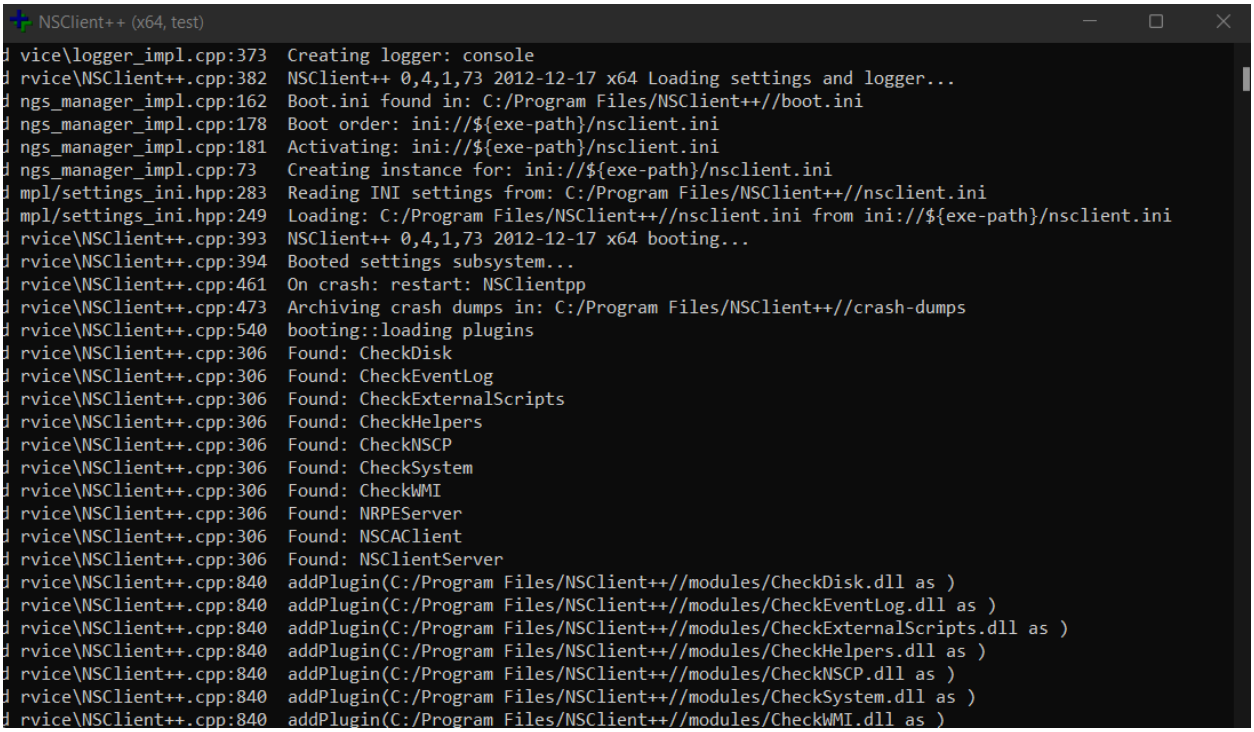


Figure 33 Starting NSClient++

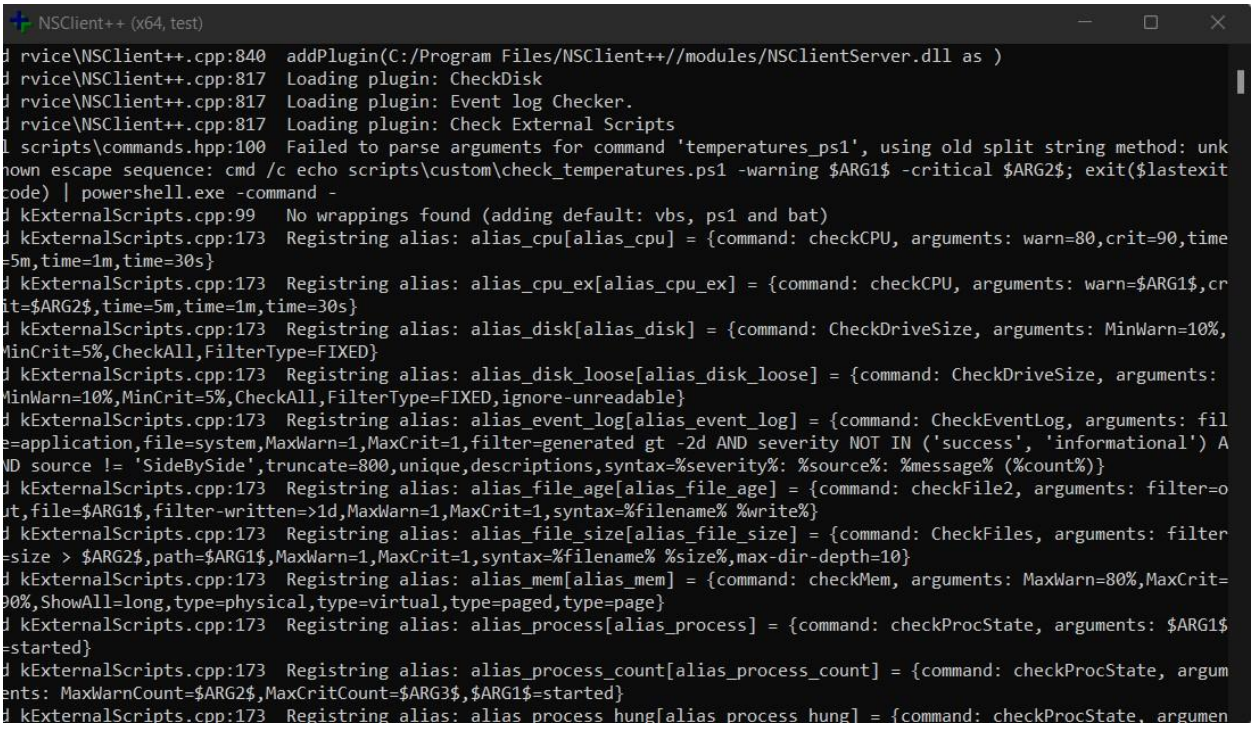


Figure 34 Starting NSClient++

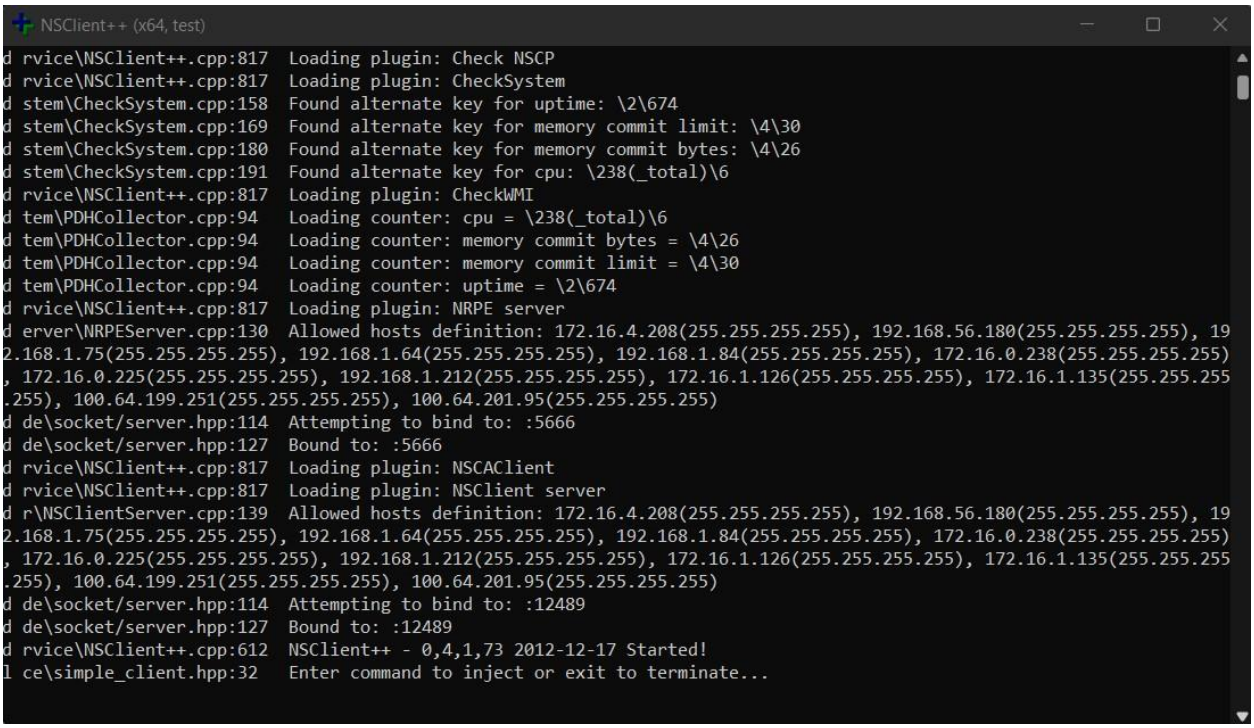


Figure 35 Starting NSClient++

vii. GNS3

GNS3 is a tool which supports all the cisco devices and helps in configuring the devices in real-time. GNS allows us to run a small and a big topology which allows us to host multiple servers, router, and switches. Some more screenshots of it can be found in the link below:

[7.3.2.6. Screenshots of GNS3]

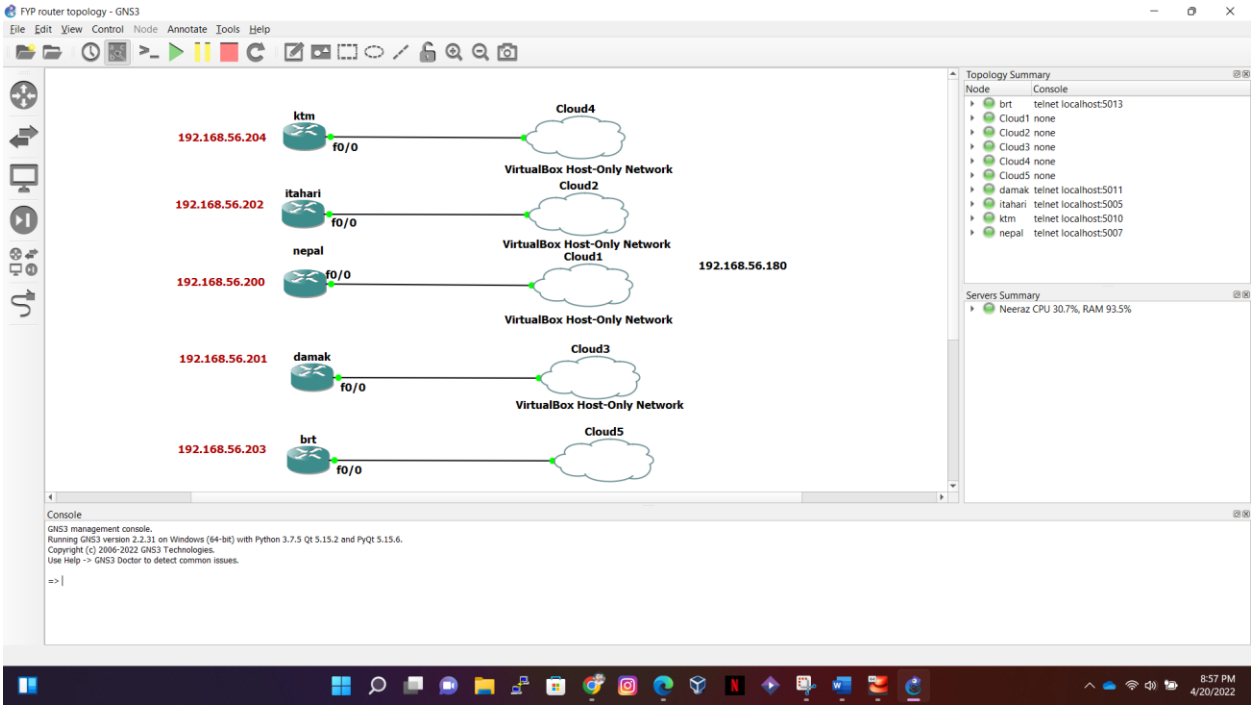


Figure 36 Topology of routers connected to cloud for monitoring

viii. NMAP

NMAP is a tool or an open-source tool which helps us to scan all the open ports in a network. Some more screenshots of it can be found in the link below:

7.3.2.7. Screenshots of Nmap

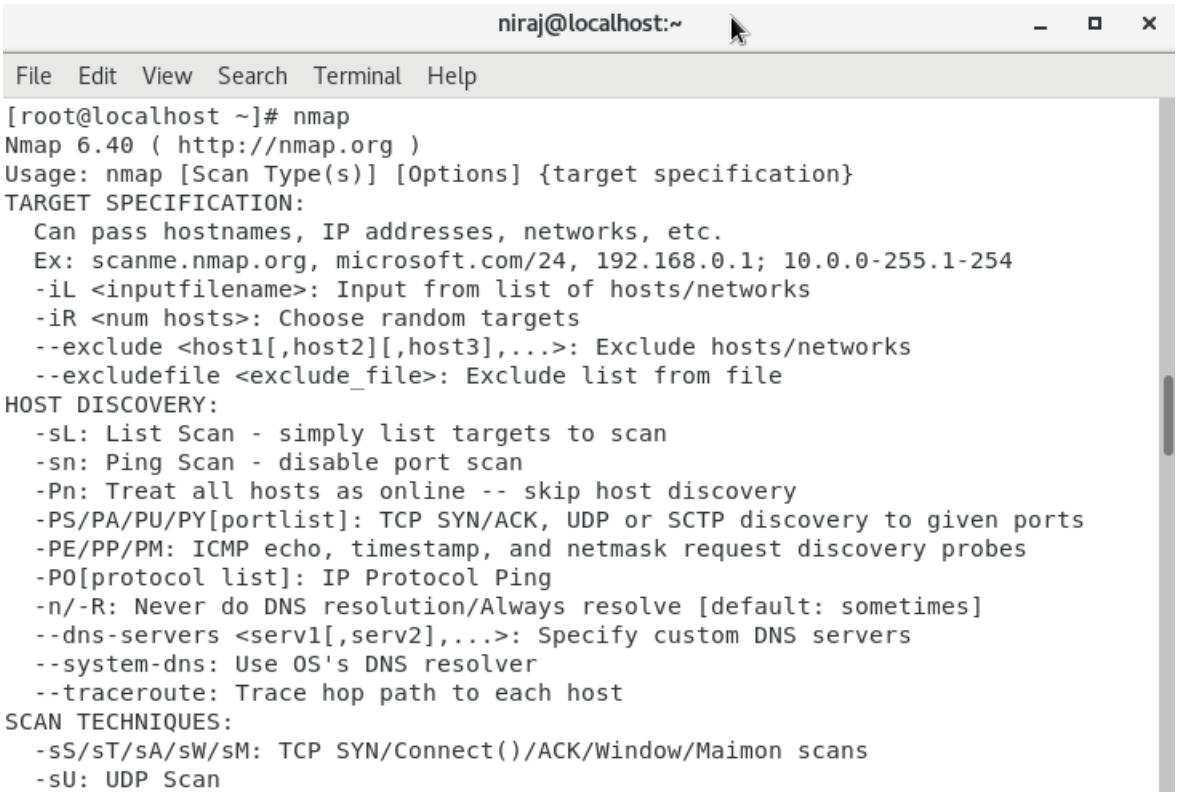


Figure 37 Installing NMAP

ix. PNP4Nagios

PNP4Nagios is a Nagios add-on that analyses and stores performance data from plugins in RRD-databases (Round Robin Databases, see RRD Tool). Some more screenshots of it can be found in the link below:

7.3.2.9. Screenshots of PNP4Nagios

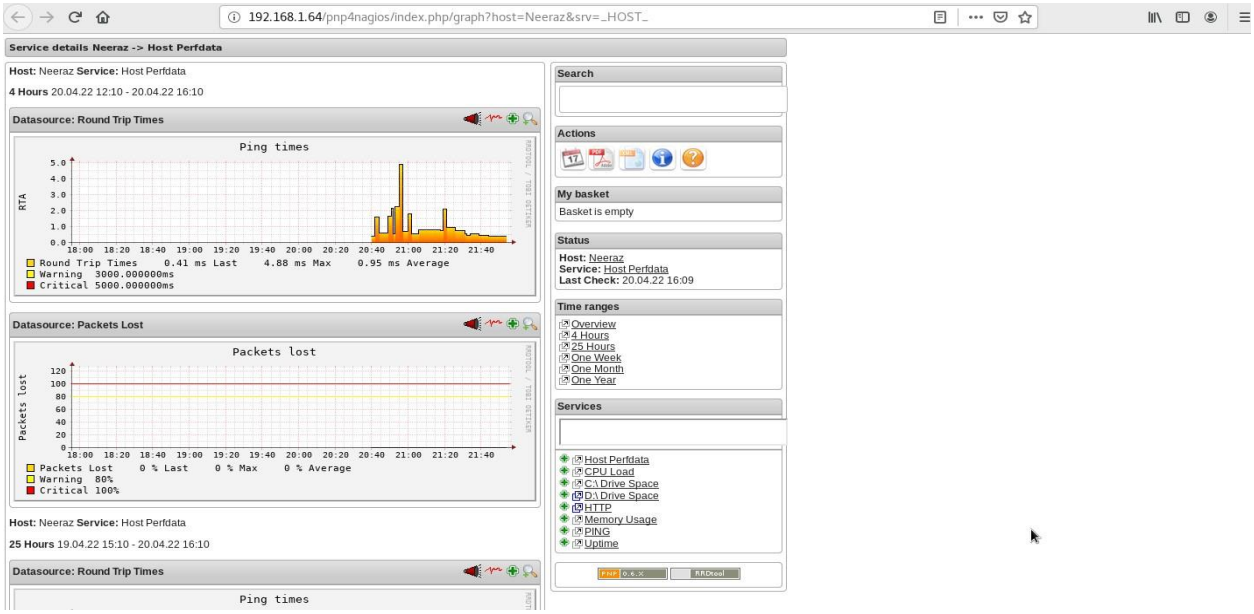


Figure 38 Displayed graph from PNP4Nagios

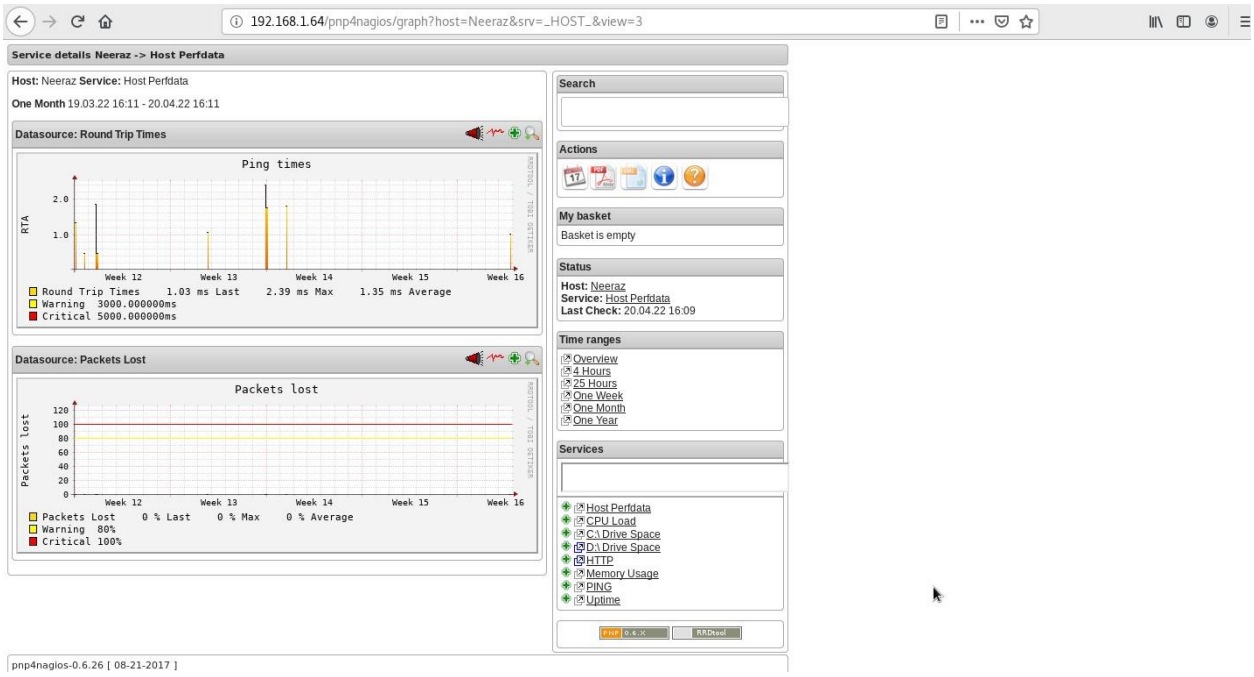


Figure 39 Displayed graph from PNP4Nagios

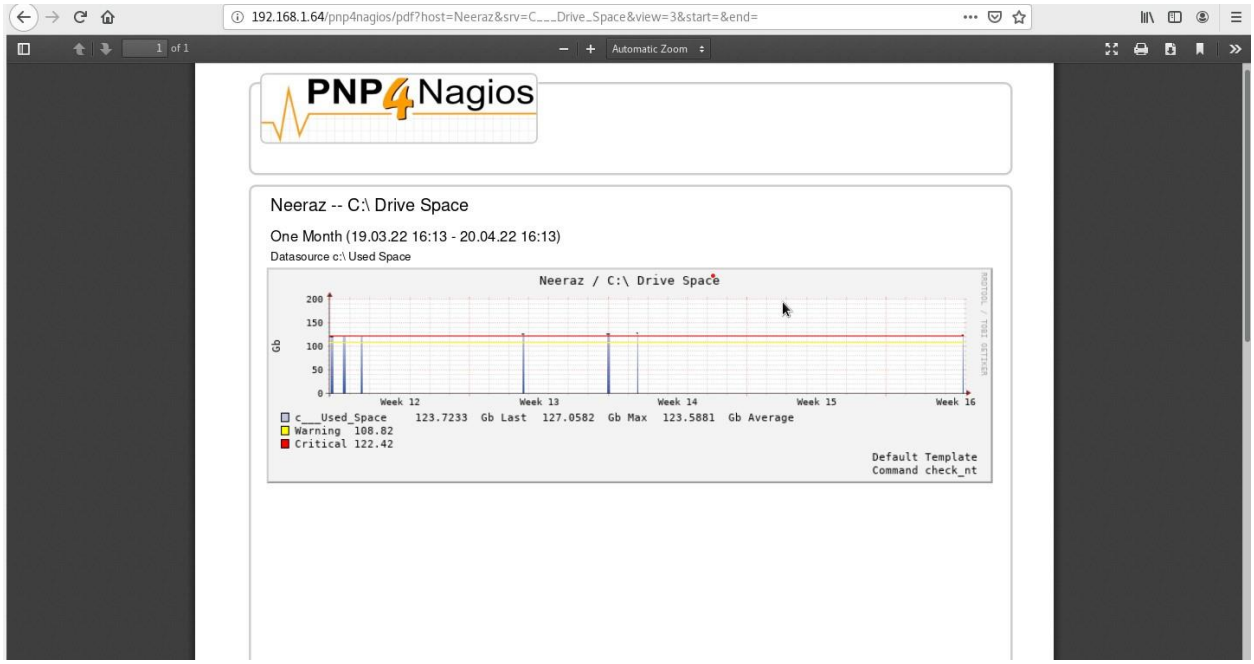


Figure 40 Displayed graph from PNP4Nagios in PDF

x. check_scan.sh

This code is written in Perl Programming Language which is used to display all the open ports in a network which is displayed after performing a Nmap scan. This will help in a business organization in finding all the open and venerable ports that may be the cause of future harm in the organization. Some more screenshots of it can be found in the link below:

7.4.4. Sample code for the Port Scanning feature.

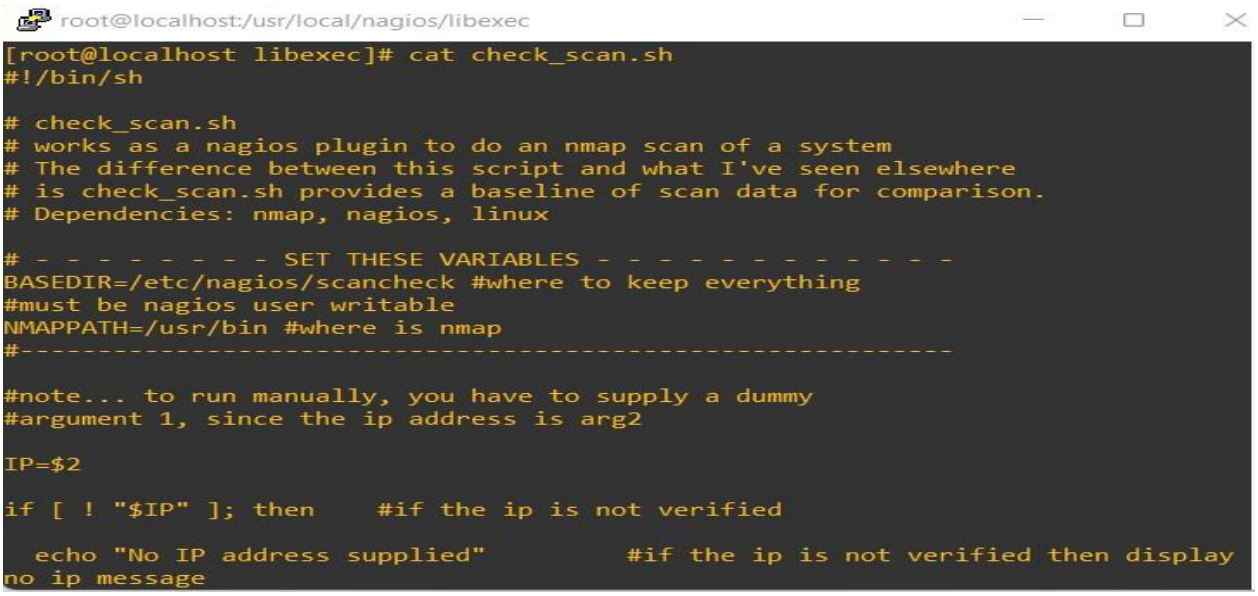


Figure 41 check_scan.sh code (Port Scanner)

Figure 42 check_scan.sh code (Port Scanner)

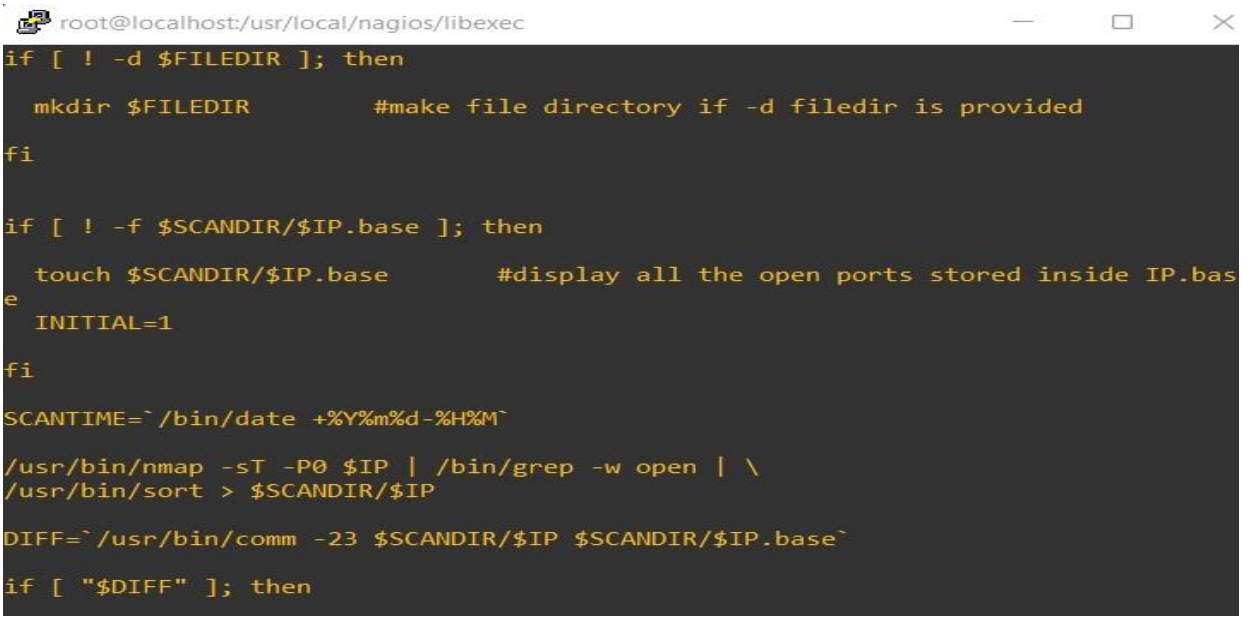


Figure 43 check_scan.sh code (Port Scanner)

root@localhost:/usr/local/nagios/libexec

```
if [ "$DIFF" ]; then

  CHANGED=1
  DIFFSTR=`echo "$DIFF" | /usr/bin/awk '{print $1}' | \
    /usr/bin/paste -s -d " " -`

fi

if [ $INITIAL -eq 1 ]; then

  /bin/cat $SCANDIR/$IP > $SCANDIR/$IP.base     #combine both scandir IP and IP.
base for displaying the ports
  echo "Initial scan"
  exit 0

fi

if [ $CHANGED -eq 1 ]; then

  echo "Scan $SCANTIME: NEW $DIFFSTR"   #display all the open ports after doint
cat IP > IP.base
  exit 1

else
```

Figure 44 check_scan.sh code (Port Scanner)

root@localhost:/usr/local/nagios/libexec

```
if [ $INITIAL -eq 1 ]; then

  /bin/cat $SCANDIR/$IP > $SCANDIR/$IP.base     #combine both scandir IP and IP.
base for displaying the ports
  echo "Initial scan"
  exit 0

fi

if [ $CHANGED -eq 1 ]; then

  echo "Scan $SCANTIME: NEW $DIFFSTR"   #display all the open ports after doint
cat IP > IP.base
  exit 1

else

  echo "$SCANTIME: no change"   #output all the ports
  exit 0

fi

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 45 check_scan.sh code (Port Scanner)

xi. XAMPP

Many individuals have learned the hard way that setting up an Apache web server is difficult, and that adding MariaDB, PHP, and Perl to the mix makes it even more difficult. XAMPP's mission is to create an easy-to-install Apache distribution for developers. XAMPP is set up with all features switched on to make it easier for developers to use. Please refer to the product licensing in the event of business usage; nonetheless, commercial use of XAMPP is also free. Currently, Windows, Linux, and OS X distributions are available (XAMPP, 2022). Some more screenshots of it can be found in the link below:

[7.3.2.8. Screenshots of XAMPP]

Figure 46 XAMPP control panel

4. Testing and Analysis

4.1. Test Plan

4.1.1. Unit Testing Test Plan

4.1.1.1. CentOS Test Plan

Test Case	Objectives
1	To test whether the CentOS is properly running or not.
2	To test whether the Nagios Core is properly running or not.

Table 3 CentOS Test Plan

4.1.1.2. Windows Hosts and Services Logs Monitoring Test Plan

Test Case	Objectives
1	To test whether the NSClient++ is properly running or not.
2	To test whether the Windows Hosts and Services Logs are monitored and displayed in Nagios dashboard or not.
3	To test if the warnings are shown or not.

Table 4 Windows Hosts and Services Logs Monitoring Test Plan

4.1.1.3. Router Status Monitoring Test Plan

Test Case	Objectives
1	To test whether the GNS3 is properly running or not.
2	To test whether the Routers and Cloud are properly functioning or not.
3	To test whether the configurations done of the router in Nagios server is right or not.
4	To test whether the Router Logs and status are monitored and displayed in Nagios dashboard or not.
5	To test whether the router's IP are pinged through Nagios Server or not and vice versa.

Table 5 Router Status Monitoring Test Plan

4.1.1.4. Graphs of Host Test Plan

Test Case	Objectives
1	To test whether the PNP4Ngaios is properly running or not.
2	To test whether the Graphs are properly functioning or not.
3	To test whether the configurations done of the Hosts and Services of PNP4Nagios in Nagios server is right or not.
4	To test whether the Graph sign are displayed in Nagios dashboard in each host and services or not.

Table 6 Graphs of Host Test Plan

4.1.1.5. Port Scanning Feature Test Plan

Test Case	Objectives
1	To test whether the NMAP is working or not.
2	To test whether the Open Ports are scanned or not.
3	To test whether the open ports are displayed in the Nagios Dashboard or not.
4	To test whether the feature can scan routers and other devices open ports or not.

Table 7 Port Scanning Feature Test Plan

4.1.2. System Testing, Test Plan

Test Case	Objectives
1	To test the windows and Linux host and their services logs as a whole.
2	To test the Routers log and status as a whole.
3	To test the Port Scanning feature as a whole.
4	To test the Graph feature as a whole.

Table 8 System Testing, Test Plan

4.2. Unit Testing

4.2.1. Nagios Server Test Case

Test Case 1	
Objective	To test whether the CentOS is properly running or not.
Action	Start the CentOS machine from Oracle VM Virtual box.
Expected Test Result	The CentOS machine should start up with all the useable features running in it.
Actual Test Result	The CentOS machine started up with all the useable features running in it.
Conclusion	Test Successful.

Table 9 Nagios Server Test Case

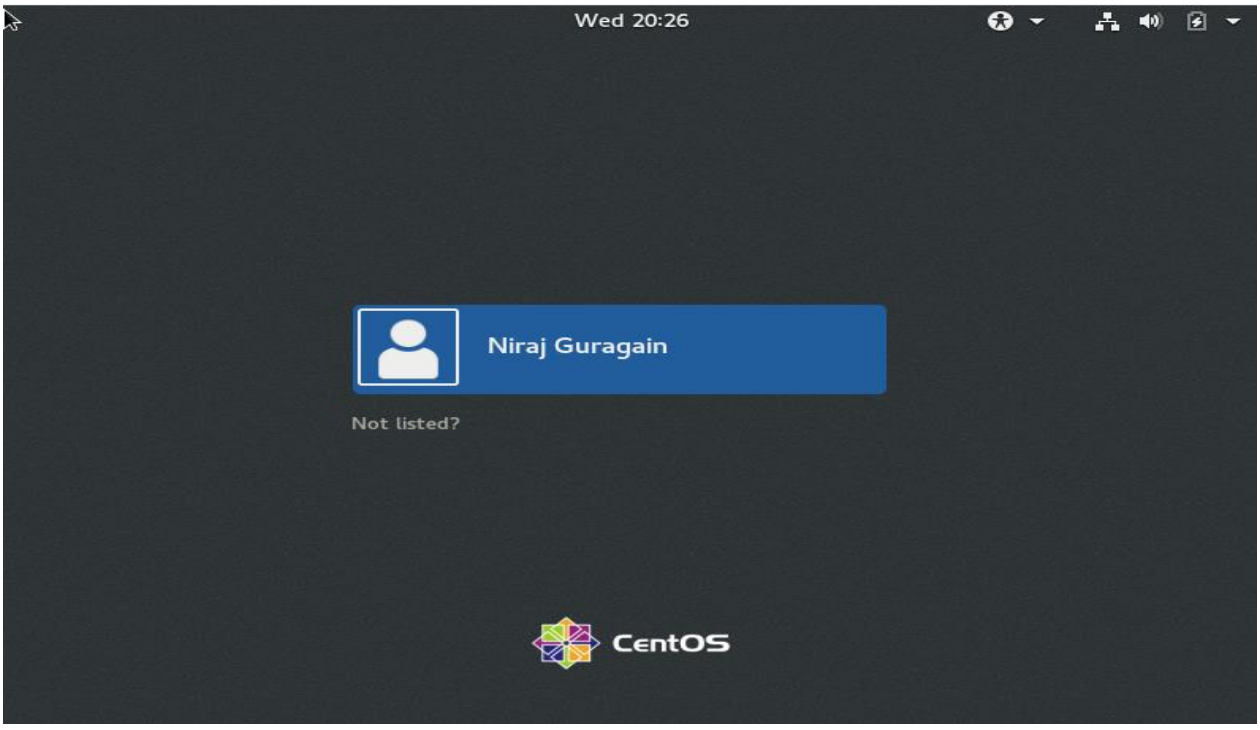


Figure 47 Starting up CentOS

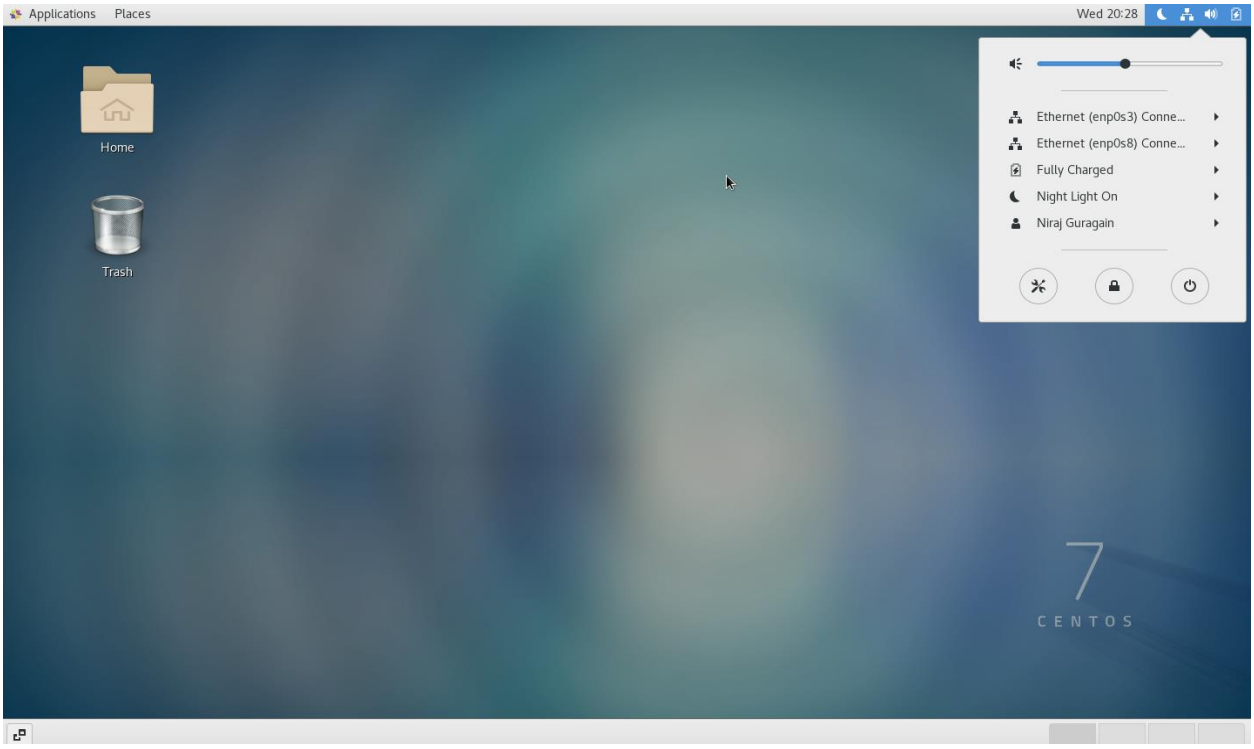


Figure 48 CentOS Successfully Running on Oracle VM Virtual box

Test Case 2	
Objective	To test whether the Nagios is properly running or not.
Action	Start the Nagios Core from CentOS machine.
Expected Test Result	The Nagios Core should start up with all the useable features running in it and show all the status of host in its Dashboard.
Actual Test Result	The Nagios Core ran with all the useable features running in it including the status of hosts in its Dashboard.
Conclusion	Test Successful.

Table 10 Nagios Server Test Case 2

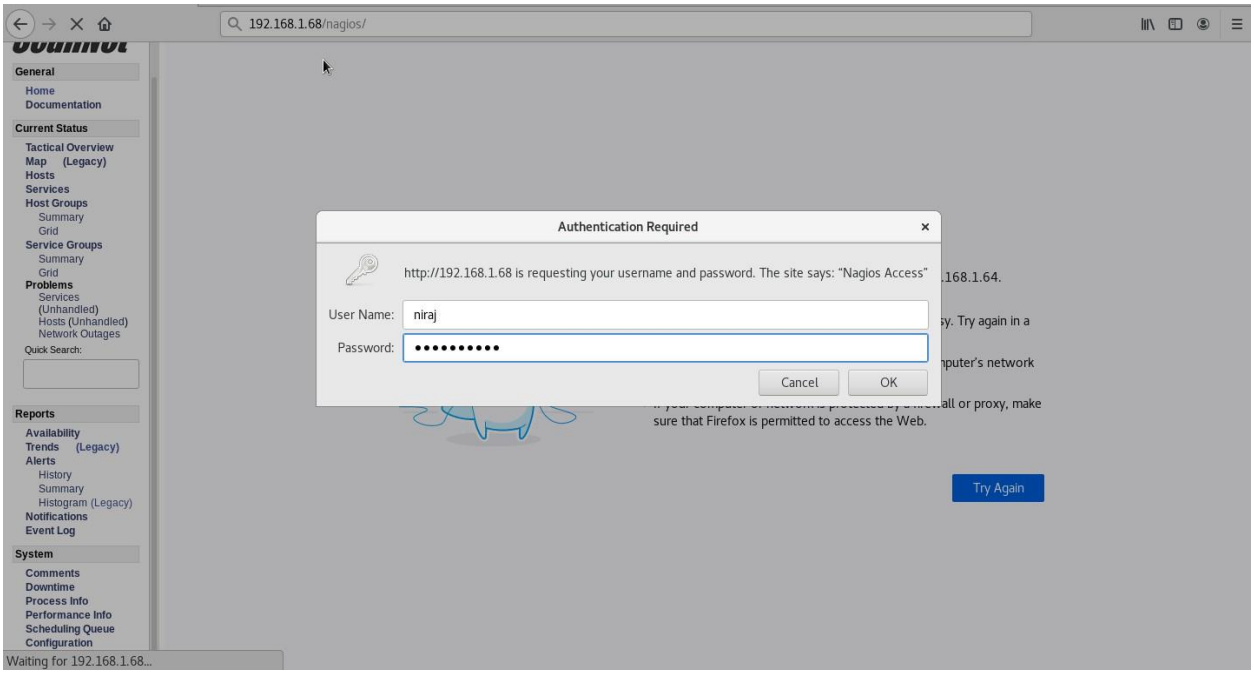


Figure 49 Starting Nagios Core Running on CentOS on Ethernet 08 IP.

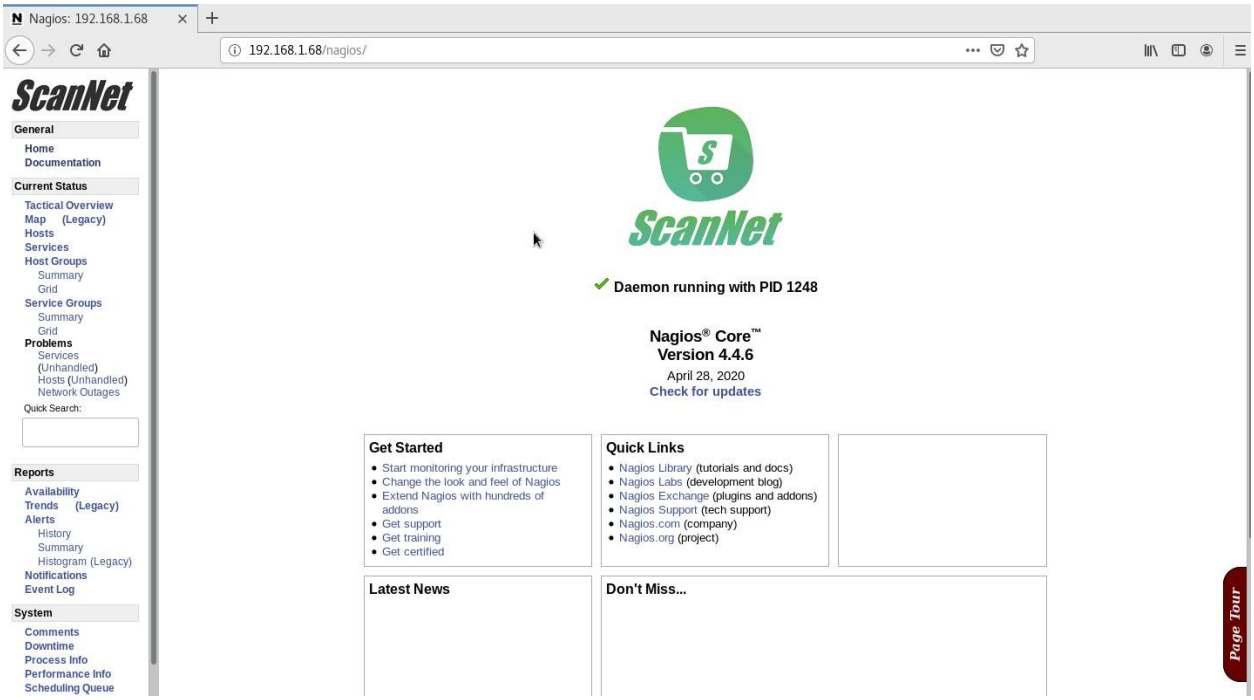


Figure 50 Nagios Dashboard successfully displayed.

4.2.2. Windows Hosts and Services Logs Monitoring Test Case

Test Case 1	
Objective	To test whether the NSClient++ is properly running or not.
Action	Start the NSClient++ on windows host machine.
Expected Test Result	The NSClient++ should start up with all the useable features running in it in ethernet 08's IP and show all the status of host in Nagios Dashboard.
Actual Test Result	The NSClient++ ran with all the useable features running in it including the status of hosts and its services in Nagios Dashboard.
Conclusion	Test Successful.

Table 11 Windows Hosts and Services Logs Monitoring Test Case 1

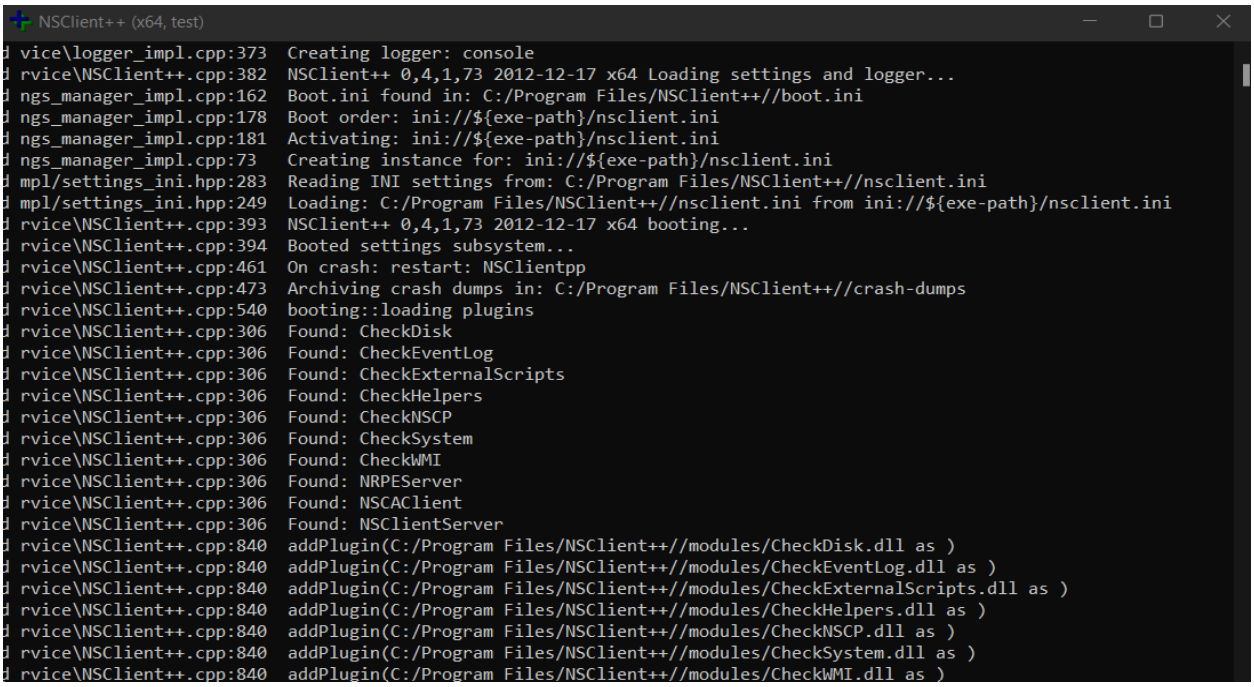


Figure 51 Starting NSClient++

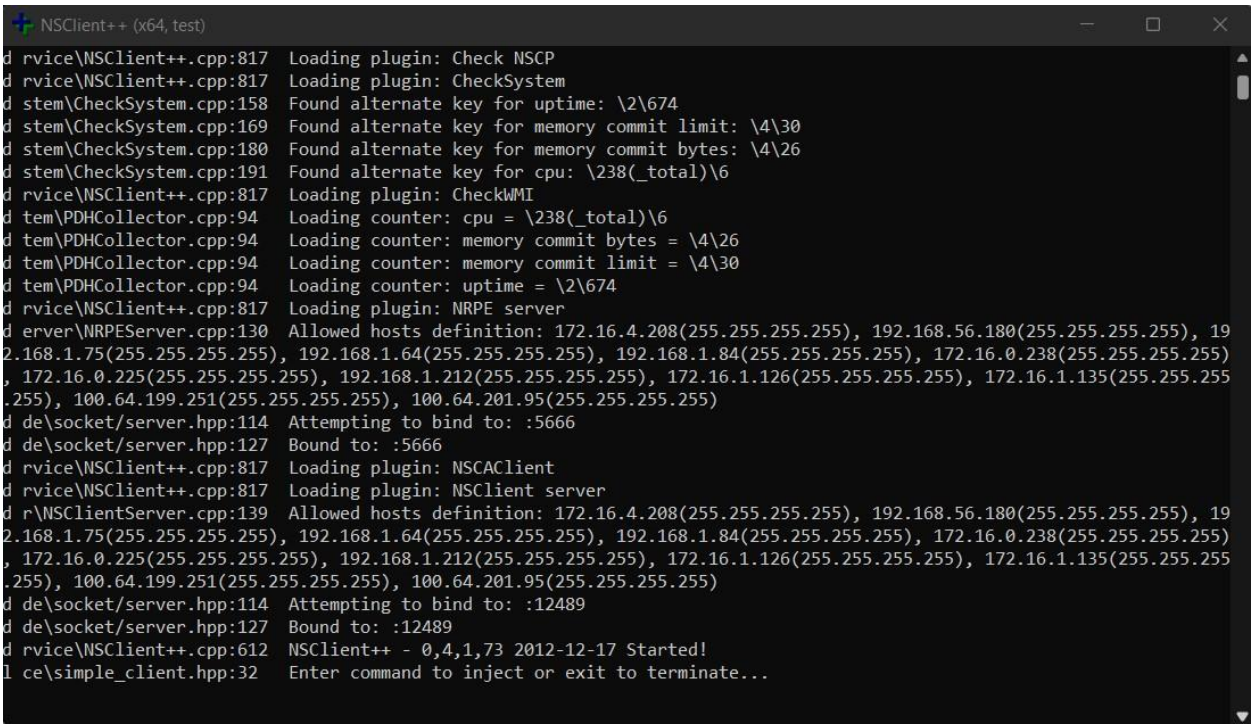


Figure 52 NSClient++ running on windows host machine.

Test Case 2	
Objective	To test whether the windows host and services are monitored and displayed in Nagios or not.
Action	Start the Nagios Core and Click on windows host named as “Neeraz.”
Expected Test Result	The Dashboard should display the host status and all its services.
Actual Test Result	The Dashboard displayed the host status and all its services.
Conclusion	Test Successful.

Table 12 Windows Hosts and Services Logs Monitoring Test Case 2

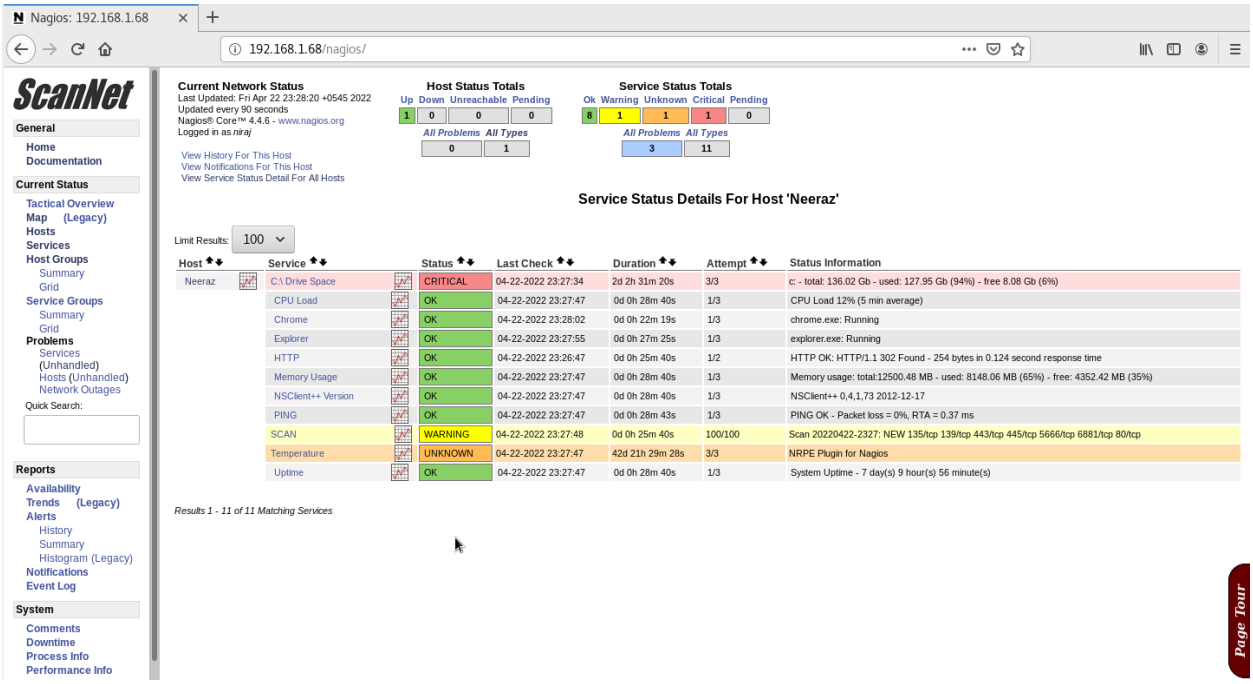


Figure 53 Windows Host and Services Status Successfully Displayed in Nagios Dashboard.

Test Case 3	
Objective	To test whether the windows host and services logs and notifications are displayed in Nagios or not.
Action	Start the Nagios Core and Click on windows host named as “Neeraz” and click on “View Status Detail.”
Expected Test Result	The Dashboard should display the host status and all its services and their status and logs and all notifications.
Actual Test Result	The Dashboard displayed the host status and all its services and their status and logs and all the notifications.
Conclusion	Test Successful.

Table 13 Windows Hosts and Services Logs Monitoring Test Case 3

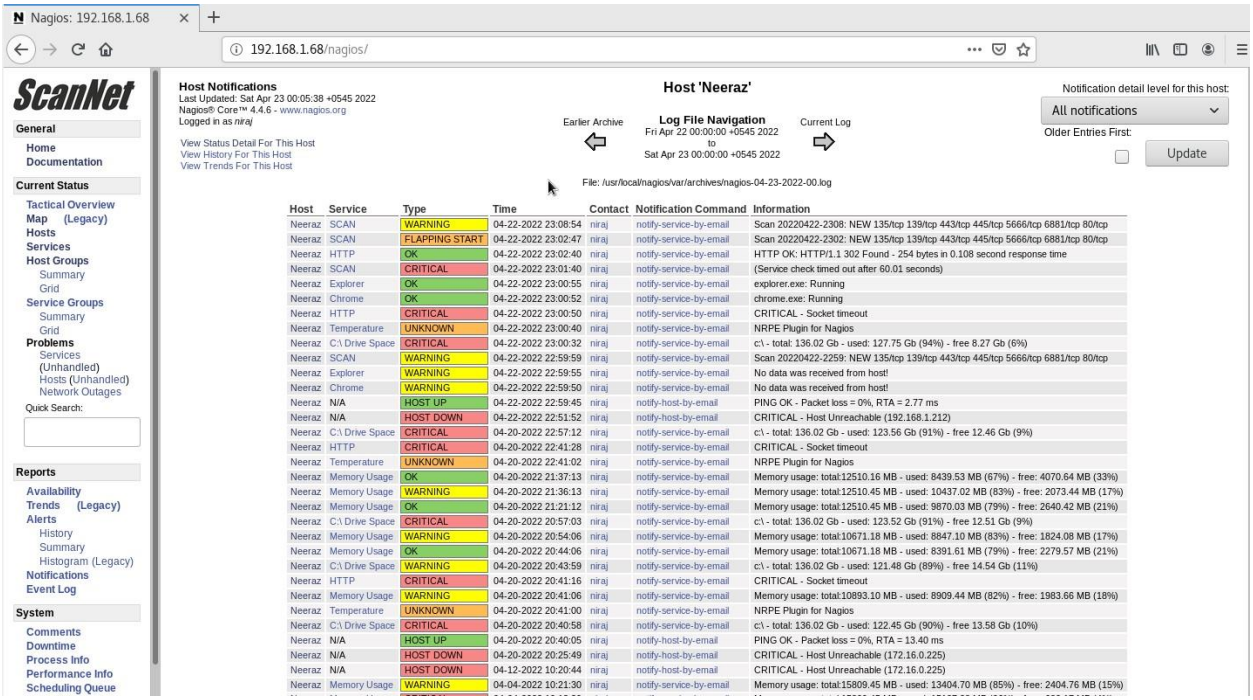


Figure 54 Displaying the Host status and all its services and their status and logs and all the notifications in Nagios dashboard.

4.2.3. Routers Status Monitoring Test Case

Test Case 1	
Objective	To test whether the GNS3 is running on windows host or not.
Action	Start the GNS3 and configure all the routers with IP addresses.
Expected Test Result	The routers inside the GNS3 should all run successfully.
Actual Test Result	The routers inside the GNS3 successfully ran successfully.
Conclusion	Test Successful.

Table 14 Routers Status Monitoring Test Case 1

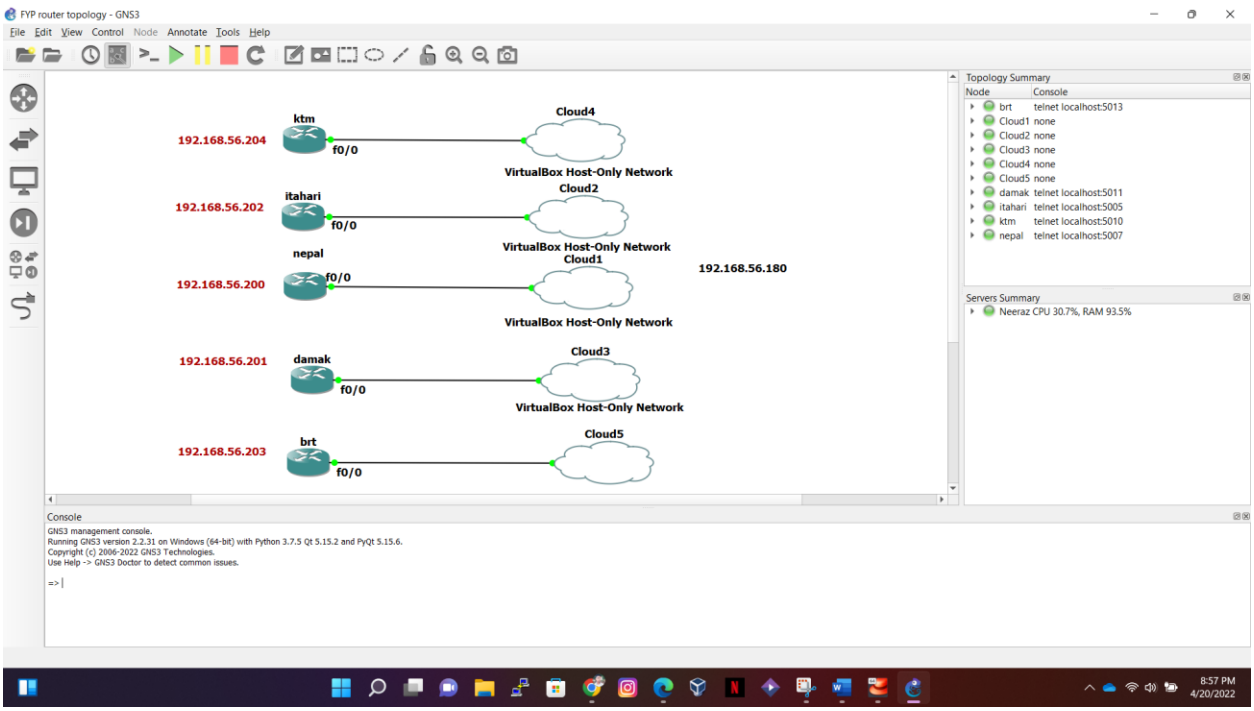


Figure 55 Topology of routers and clouds in GNS3.

Test Case 2	
Objective	To test whether the GNS3 is running on windows host and able to ping the Nagios Server or not.
Action	Start the GNS3 and start all the routers connected with the cloud.
Expected Test Result	The routers inside the GNS3 should all run and be able to ping with all the routers and Nagios Server.
Actual Test Result	The routers inside the GNS3 ran and was able to ping with all the routers and Nagios Server successfully.
Conclusion	Test Successful.

Table 15 Routers Status Monitoring Test Case 2

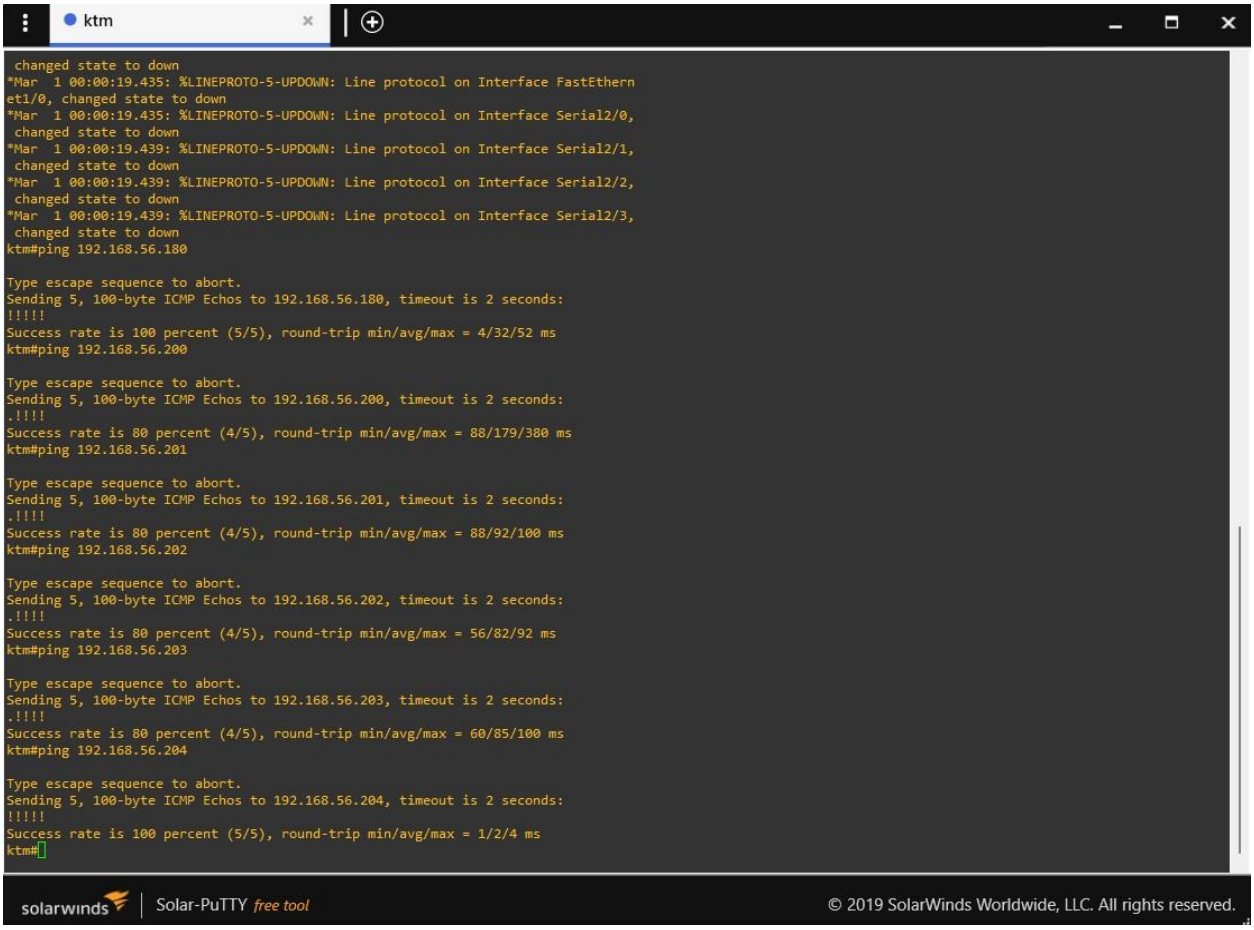


Figure 56 Pinging with all the routers and the Nagios Server.

4.2.4. Graphs Status Monitoring Test Case

Test Case 1	
Objective	To test whether the PNP4Nagios is installed on Nagios Server or not.
Action	Start the Nagios Server and check the Graphs Logo on the side of hosts and services.
Expected Test Result	The Graph Logo created by PNP4Nagios should appear in the side of all the hosts and all the services.
Actual Test Result	The Graph Logo was created by PNP4Nagios and appeared in the side of all the hosts and all the services successfully.
Conclusion	Test Successful.

Table 16 Graphs Status Monitoring Test Case 1

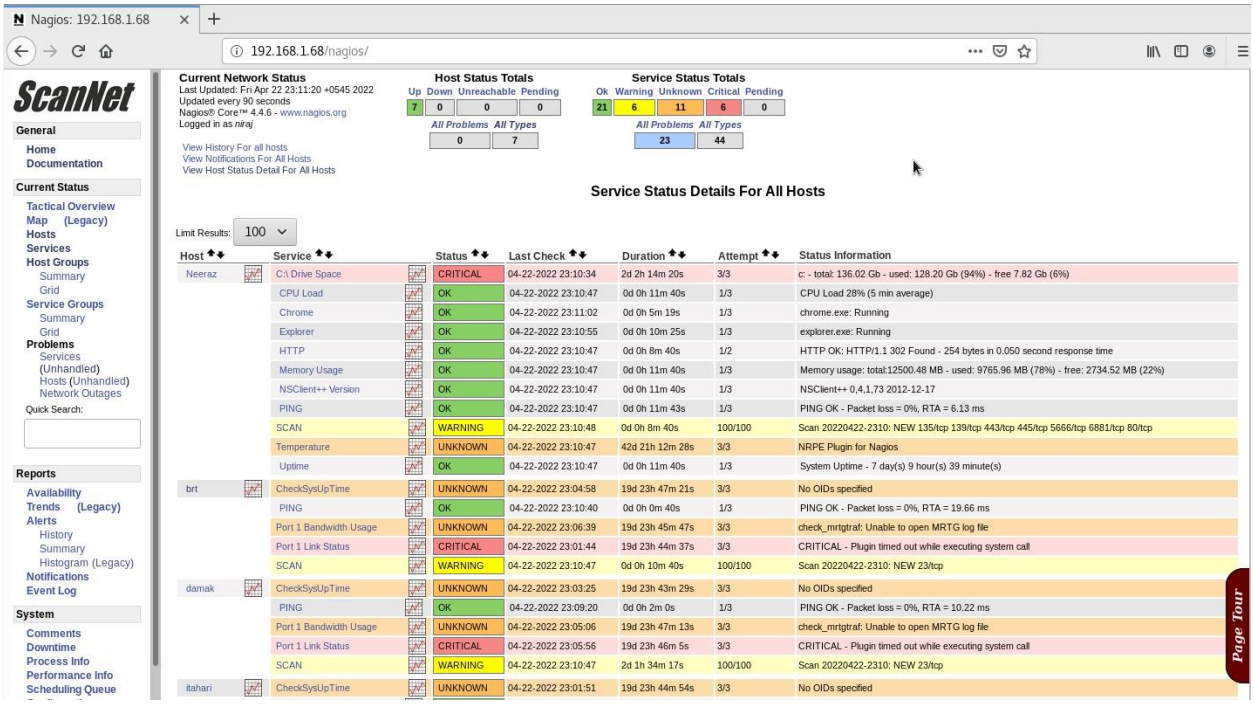


Figure 57 Checking the Graph logos in each host and services.

Test Case 2	
Objective	To test whether the PNP4Nagios is running on Nagios Server or not.
Action	Start the Nagios Server and check the Graphs Logo on the side of hosts and services and click on it.
Expected Test Result	The Graph Logo created by PNP4Nagios should appear in the side of all the hosts and all the services and should display graphs for all the logs of them.
Actual Test Result	The Graph Logo was created by PNP4Nagios and appeared in the side of all the hosts and all the services and also displayed graphs for all the logs of them.
Conclusion	Test Successful.

Table 17 Graphs Status Monitoring Test Case 2

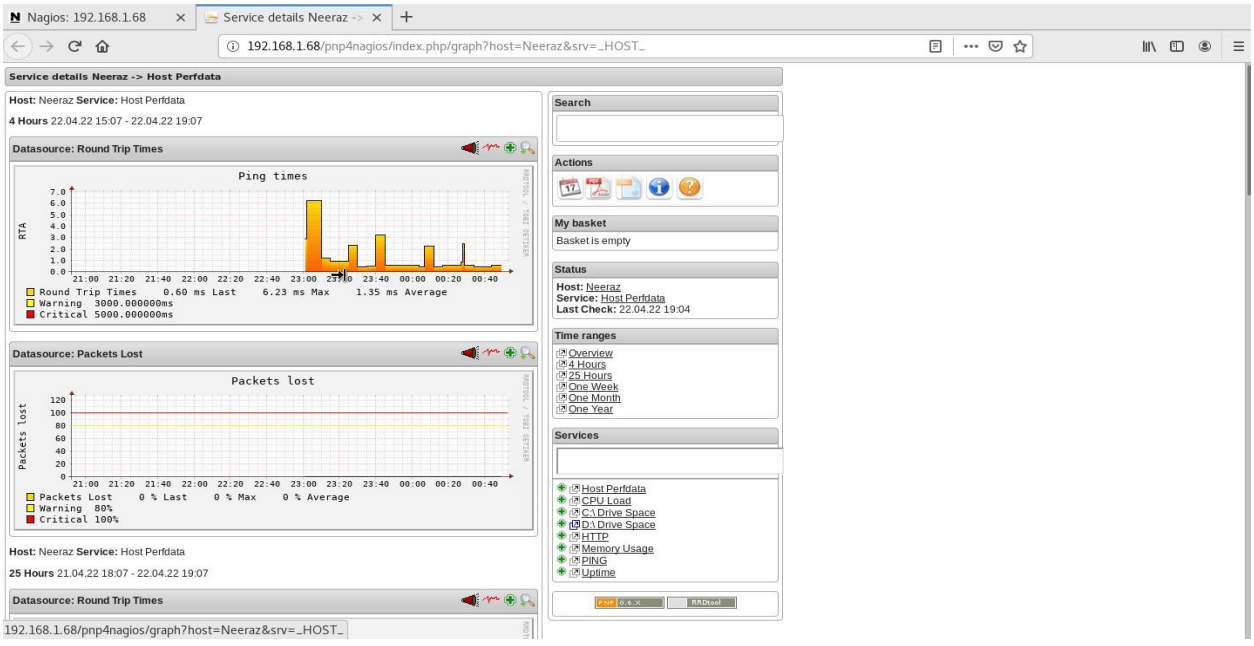


Figure 58 Graph of logs of Host "Neeraz" in 4 hrs.

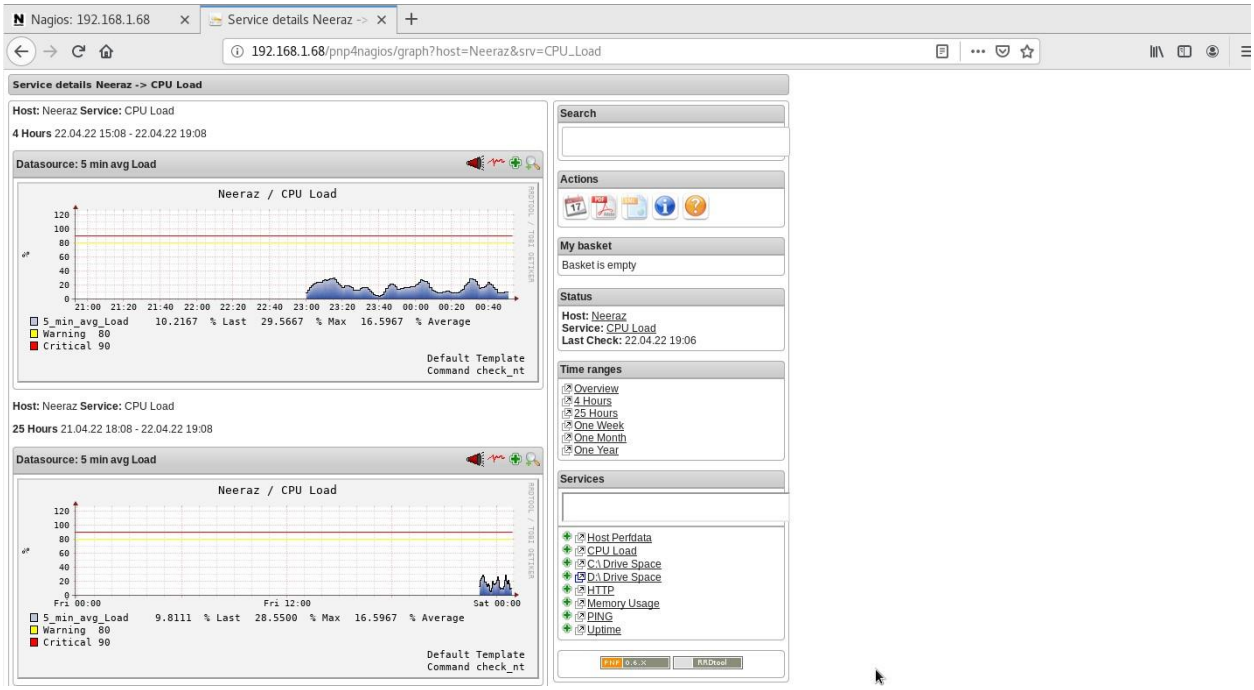


Figure 59 Graph of logs of services "CPU Load" in 4 hrs.

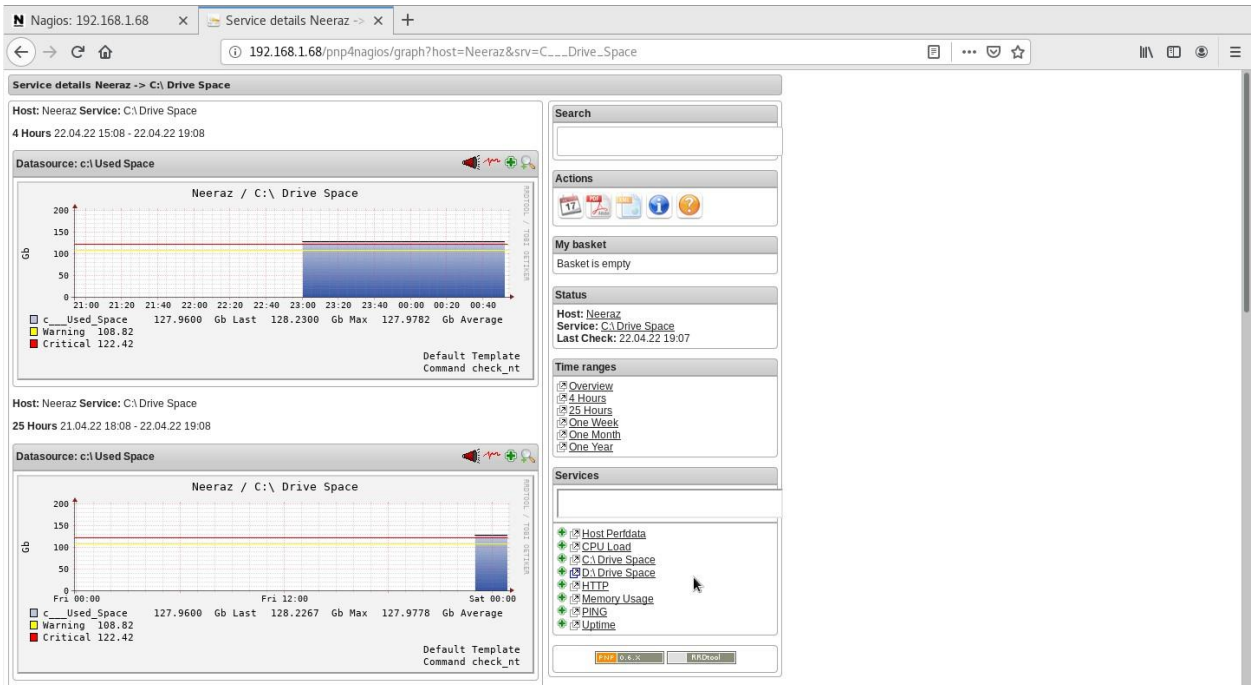


Figure 60 Graph of logs of services "C:|Drive Space" in 4 hrs.

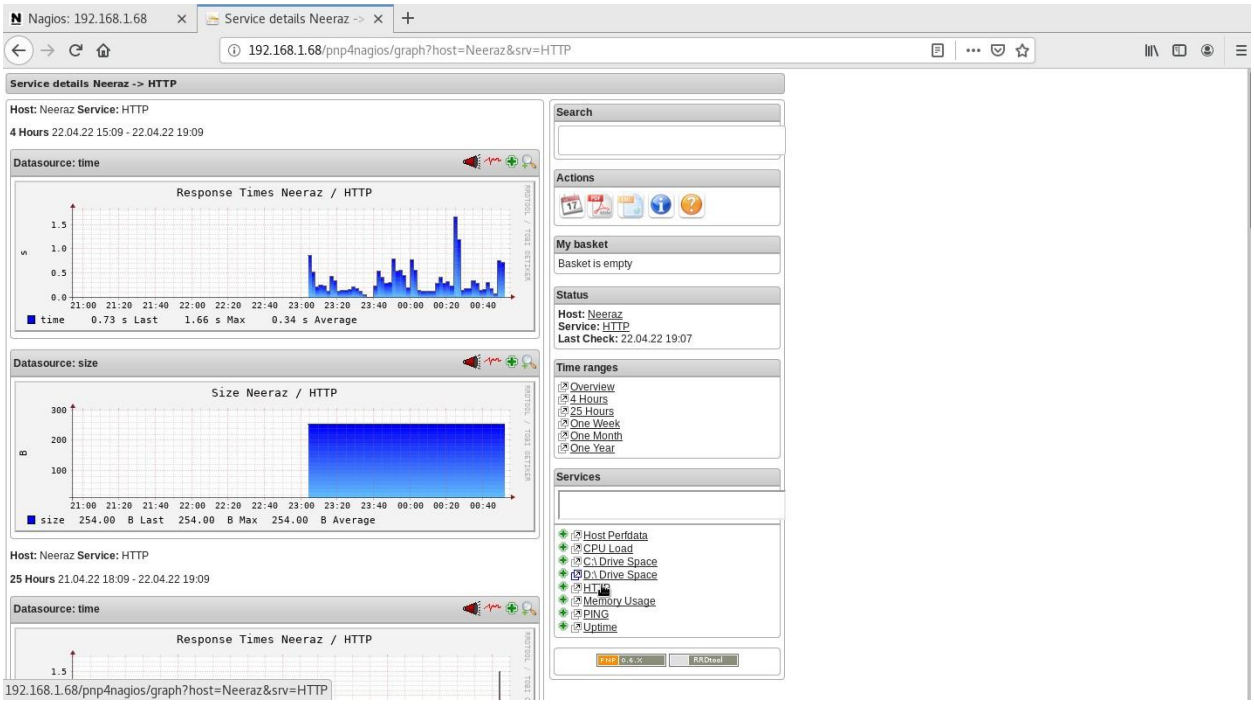


Figure 61 Graph of logs of services "HTTP" in 4 hrs.

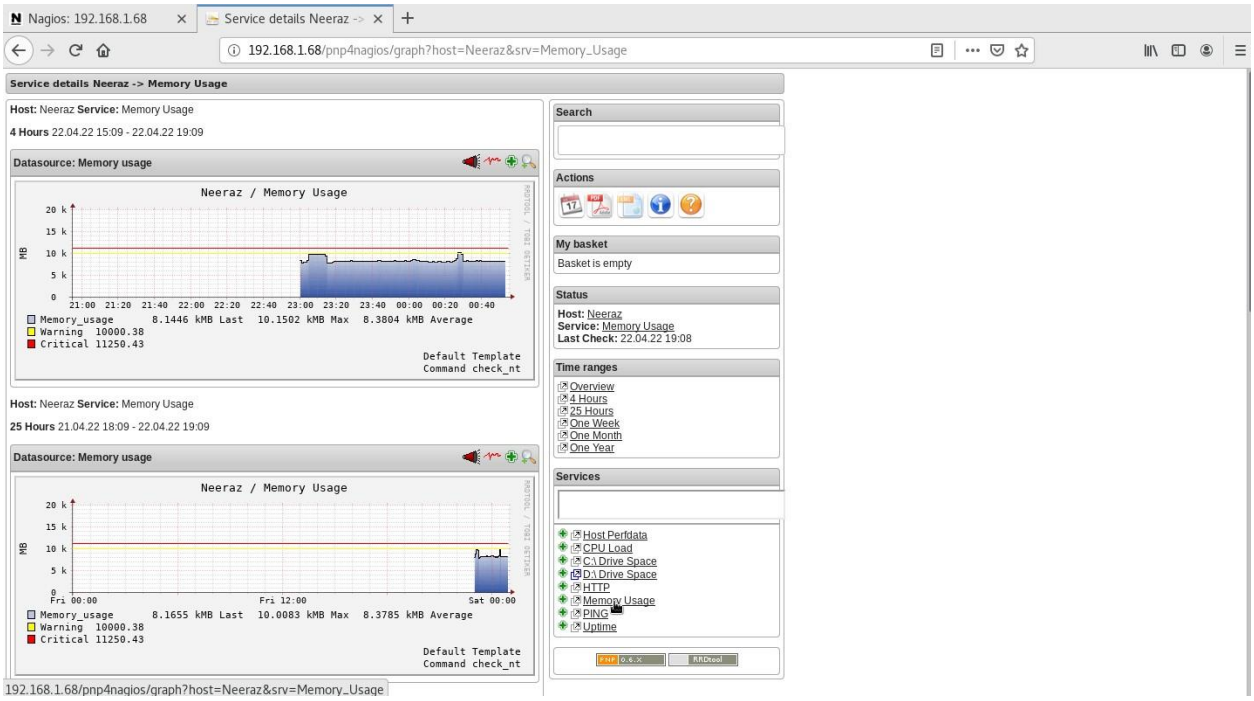


Figure 62 Graph of logs of services "Memory Usage" in 4 hrs.

4.2.5. Open Ports Monitoring Test Case

Test Case 1	
Objective	To test the Nmap tool as a whole.
Action	Start the Putty and SSH to the Nagios Servers IP and do a Nmap scan see the result.
Expected Test Result	The tool should automatically display all the open ports after performing the Nmap scanning in the particular networks IP and show the services used by it in the terminal.
Actual Test Result	The tool automatically displayed all the open ports after performing the Nmap scanning in the particular networks IP and showed the services used by it in the terminal.
Conclusion	Test Successful.

Table 18 Open Ports Monitoring Test Case 1

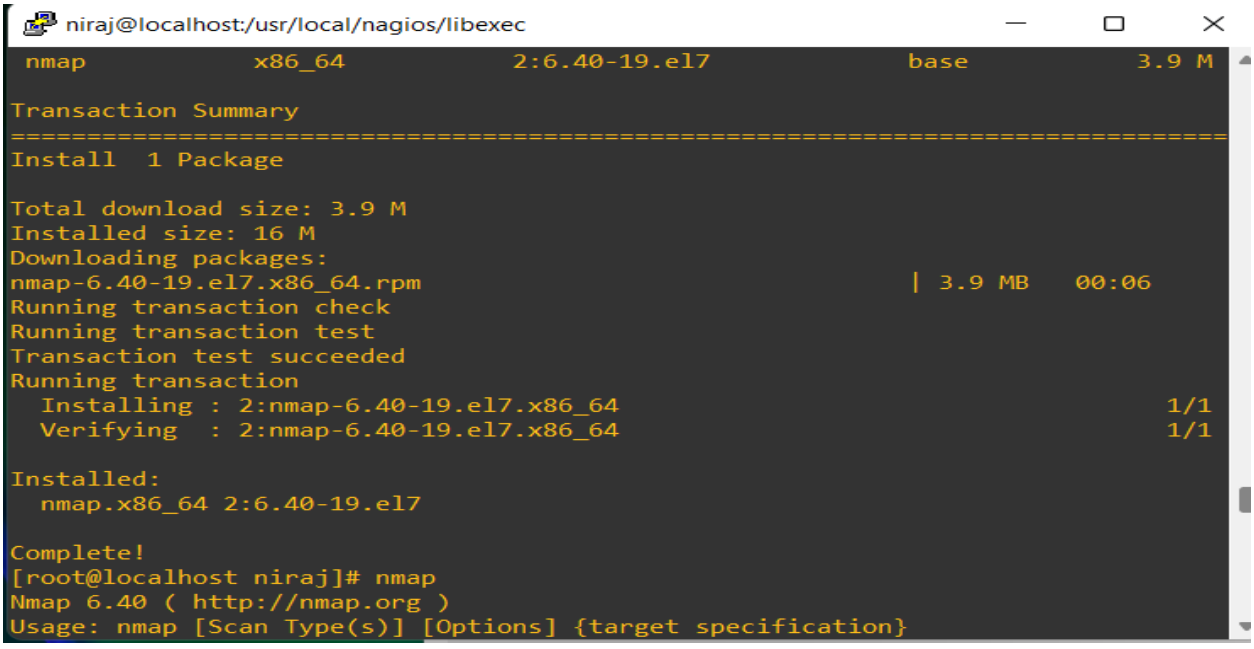


Figure 63 Nmap installation Successful.

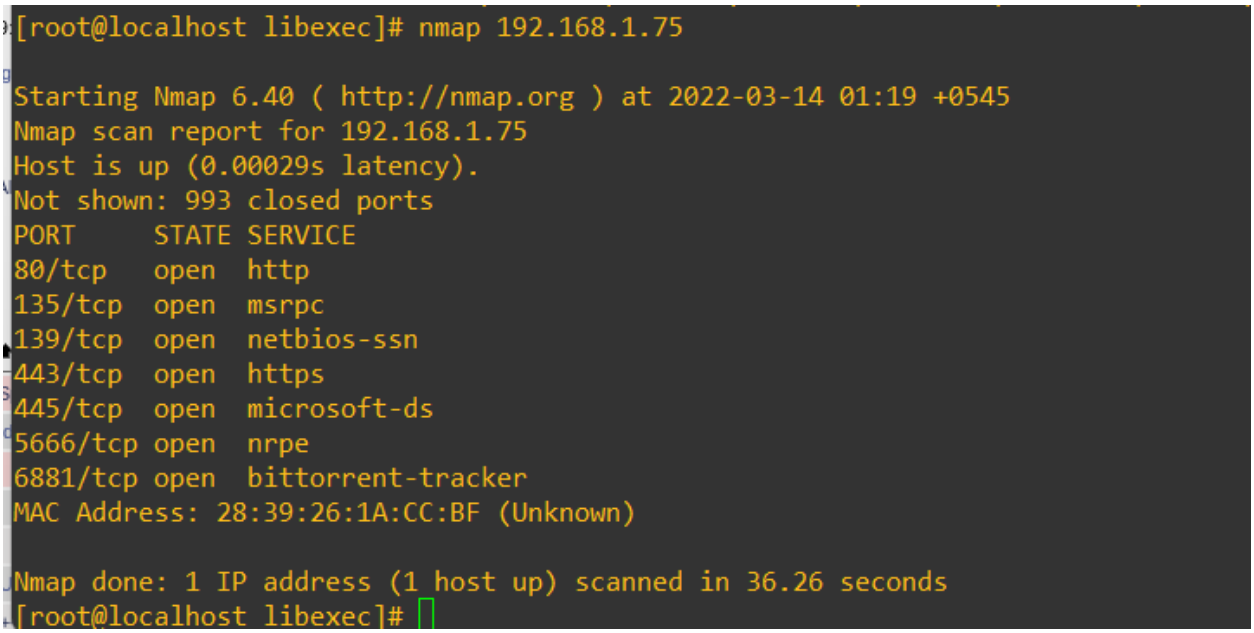


Figure 64 Nmap scan successfully done.

Test Case 2	
Objective	To test the Port Scanning feature as a whole.
Action	Start the Putty and SSH to the Nagios Servers IP and do a Nmap scan and run the code check_scan.sh which is stored inside Nagios Server inside Libexec and see the result.
Expected Test Result	The program should automatically display all the open ports after performing the port scanning in the particular networks IP and show the services used by it and display it in the Nagios dashboard.
Actual Test Result	The program automatically displayed all the open ports after performing the port scanning in the particular networks IP and

	showed the services used by it and displayed it in the Nagios dashboard.
Conclusion	Test Successful.

Table 19 Open Ports Monitoring Test Case 2

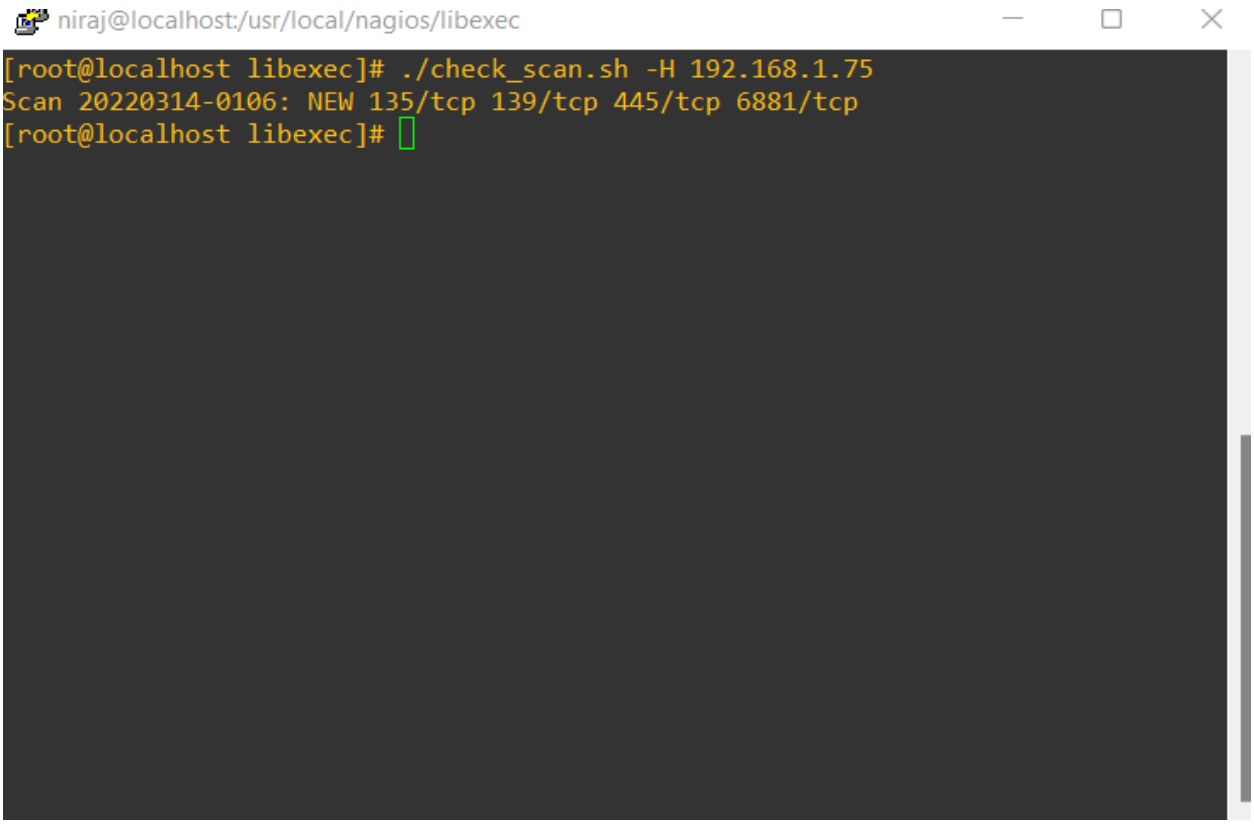


Figure 65 Doing Port Scanning through the Code and all open ports are displayed.

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Neeraz	C:\ Drive Space	CRITICAL	03-14-2022 01:12:19	6d 15h 7m 40s	2/2	c: - total: 136.02 Gb - used: 126.99 Gb (93%) - free 9.03 Gb (7%)
	CPU Load	OK	03-14-2022 01:12:41	0d 0h 1m 27s	1/2	CPU Load 3% (5 min average)
	Chrome	CRITICAL	03-14-2022 01:13:02	0d 1h 17m 26s	2/2	Chrome.exe: not running
	Explorer	OK	03-14-2022 01:13:24	0d 0h 2m 44s	1/2	explorer.exe: Running
	HTTP	OK	03-14-2022 01:13:56	0d 0h 0m 12s	1/2	HTTP OK: HTTP/1.1 302 Found - 254 bytes in 0.024 second response time
	Memory Usage	OK	03-14-2022 01:13:58	0d 0h 2m 10s	1/2	Memory usage: total:14714.43 MB - used: 6194.91 MB (42%) - free: 8519.52 MB (58%)
	NSClient++ Version	OK	03-14-2022 01:13:58	0d 0h 2m 10s	1/2	NSClient++ 0,4,1,73 2012-12-17
	PING	OK	03-14-2022 01:13:58	0d 0h 8m 10s	1/2	PING OK - Packet loss = 0%, RTA = 2.59 ms
	SCAN	WARNING	03-14-2022 01:13:08	0d 0h 4m 20s	4/100	Scan 20220314-0113: NEW 135/tcp 139/tcp 445/tcp 6881/tcp
	Temperature	UNKNOWN	03-14-2022 01:13:58	2d 23h 15m 16s	3/3	NRPE Plugin for Nagios
	Uptime	OK	03-14-2022 01:12:31	0d 0h 1m 37s	1/2	System Uptime - 2 day(s) 6 hour(s) 45 minute(s)

Figure 66 All the open ports that were scanned are displayed in the Nagios Dashboard.

4.4. Critical Analysis

4.4.1. Test Summary

The whole system's unit and system testing have both been completed successfully. The Scrum Methodology was used to create the system. The testing step benefited the system in identifying a variety of logical and practical issues that had previously gone unnoticed. The system unit was planned, created, tested, and assessed first. Each system feature was created individually and then unified as a single system for the final development of this project. The entire system was tested and reviewed when it was completed. The testing is carried out in order to make graphs and real-time port scanning more accessible to business organizations.

4.4.2. Evaluation

The system evaluation is based on the goals it claimed to fulfil as well as business requirements. The main goal of this project is to mitigate modern cyber threats by monitoring real-time system logs and detecting various intrusions that come through port scanning inside or outside of the system by displaying those logs and open ports in Nagios Dashboard in a clear graph visualization that the system can do perfectly. In addition, the project will be able to eliminate the issues associated with traditional Log Monitoring and Port Scanning methods, as well as create a cost-effective and efficient manner of operation. The Windows Event Log monitoring system can keep track of a wide range of events and send out warnings when anything important happens. Monitoring logs is useful for a variety of purposes, including diagnosing critical issues, identifying cyber criminals, finding open ports, and assisting with incident response. The

essence of log analysis might be automating the monitoring of events and incidents. The system functions as a single unit with remarkable success.

4.4.2.1. Evaluation of Project Deliverables

System Requirements, System Design, Project Feasibility Report, Practical Implementation, Test Plan & Test Cases with Results, and a final fully functional prototype system are the primary deliverables of the report. While working on various stages of the project, all of the above deliverables were completed successfully.

4.4.2.2. System Evaluation

All of the necessary criteria, functional requirements, and initially promised features of modern business organizations have been achieved. The system was created utilizing a variety of tools and technologies, and it is now being implemented. The Windows Status and Event Logs, Routers Status and Logs, and Port Scanning functions, as well as the Alert features, operate flawlessly together, and it also includes some extra features like monitoring several types of hosts and services. All of the assignments and milestones were met on schedule.

5. Conclusion

Servers, networking devices, IoT devices, and operating systems all create logs that may be captured by Nagios to better understand the performance and critical status of such equipment. However, because certain system logs are machine readable and disorganized, organizations use Nagios and add analytics behavioural that allows them to view data in dashboards, make reports, and send alerts to system analysts if any errors occur.

The tool effectively analyses system logs and detects faults using SNMP technology. The system is built with technology that allows us to monitor more data than before. The Windows and Linux Servers Security Events & Logs, as well as the Routers Status and Logs, are monitored by the system, which was added from GNS3. The system also discovers and monitors all of the network's open ports, as well as their services. The system identifies issues such as critical, warnings, and status okay, among others. As It also identifies various ports in the system, which can be important in preventing any attacks before they have a chance to cause harm. The program also helps in the creation of log graphs and reports for the host and services. These data are tracked and shown in real time on the Nagios Dashboard. If something goes wrong with the system's normal operations, the system displays all notifications quickly.

5.1. Legal, Social and Ethical Issues

5.1.1. Legal Issues

All of the tools and technologies used in this project's development are open-source, trial versions, or come pre-installed with the Windows operating system. This project does not contain any cracked or pirated software. The project is being created in accordance with the Nepal Electronic Transaction Act 2063 (2008) and does not violate any of its provisions. The system's development, testing, and installation activities are all done in accordance with all applicable laws in the nation, and there are no legal issues. Approximately 80 provisions of the Nepal Electronic Transaction Act 2063 have been completely reviewed and updated. The system does not include any dangerous code or viruses and respects the privacy and security of its users.

5.1.2. Social Issues

The user's data and privacy are respected by the ScanNet Tool. While transmitting, receiving, creating, displaying, and modifying the data, no data or privacy is leaked or compromised. The system's major goal is to assist the user by offering an SNMP solution as well as behavioural analytics that allow users to view data in dashboards, produce reports, and get warnings from system analysts if any security issues are detected. The goal of the project is to have a good influence on the IT sector and company by monitoring network traffic and detecting anomalous spikes, non-communication sources, and open ports in the network. The system's potential for social issues has already been addressed. Furthermore, the project's system or documentation contains no religious or political content, and it has no impact on any

individual's self-respect or self-esteem. The system's report has no social aspects that might lead to a social issue.

5.1.3. Ethical Issues

All data relating to Windows events and network traffic is sent to the Nagios dashboard, whose permissions may be changed to allow unwanted access. Furthermore, all ethical issues have been taken into account to ensure that no data falls into the hands of an unauthorized individual. For monitoring open ports and services in a network, the system uses the Perl programming language. There is no virus in any of the scripts, and no new code or backdoor with malicious purpose is injected into the system. The system is set up in a fair manner and for fair use. The technology gives me complete control over my data, which can only be edited or viewed by others with my permission. Also, the system does not replicate any source code or information from anyplace without giving acknowledgment, and it is the creator's original concept (myself). The project documentation has all of the necessary references and citations, so there is no room for error. The documentation's content has been verified and updated to ensure that there is no plagiarism. The system and report were created in accordance with the London Metropolitan University's rules and regulations, as well as the supervisors' instructions. The report and process do not breach any ethical standards, hence there is no ethical issues. The program protects the user's data and does not compromise on the user's intellectual property.

5.2. Advantages

The system was designed to fix issues with existing methods of network monitoring, log monitoring in graphs, and port scanning. As a result, all of the system's features and capabilities are benefits over traditional network monitoring methods. Even when compared to other similar projects, this project offers a lot more benefits. Different advantages of the project are as follows:

- Advanced Visualizations and Graphs
- Graphs of Performance and Capacity Planning
- Wizards for configuring your system.
- Infrastructure Management at its Finest.
- Archive of configuration snapshots.
- Advanced User Administration.
- Reports on Service-Level Agreements (SLAs).
- Architecture that can be expanded.
- Server, service, process, and application availability have all improved.
- Network and server outages, as well as protocol issues, are quickly detected.
- Failed servers, services, processes, and batch operations are quickly detected.
- Open Ports are detected quickly.
- Examine the event logs of various hosts and services.
- System of Notification.
- Simple to Use.

5.3. Limitations

Because it was created for a college final year project, the Network Monitoring, Log Monitoring in Graphs, and Port Scanning is just a prototype SNMP solution with several restrictions. The unique approach is designed to cost-effectively reduce some drawbacks of previous network monitoring methods, so there is plenty of room for improvement. The following are some of the system's key limitations:

- Nagios open-source monitoring has hidden expenses.
- Functionality of the product.
- There are security risks.
- There is not much assistance.
- While exploring the web, the user interface could be improved.
- There is a need to increase assistance and availability.
- Monitoring plugins might be managed in a more centralized and consistent manner.
- To use this program, we must have some understanding of Linux.
- The first setup is a little challenging.
- False positive warnings are difficult to locate and correct.

5.4. Future Work

The application of SNMP technology in the IT business is seen as a topic with a lot of potential, and the IT industry is moving in that direction. SNMP solutions are available on the market now in a variety of forms. This is only a final year project aimed at providing a minor upgrade to Nagios Core by implementing some new functionality. It is designed to meet the needs of the new organizations, but there is plenty of room for future enhancements and upgrades. To make this system more advanced and market ready, many alternative features and approaches might be implemented. Additionally, if the system is properly upgraded, the project might have a big business potential. The following are some of the new elements that might be included in the future to help the system advance:

- Phone-based alerting for improved security notifications in real time, SMS can be used.
- To store additional logs and resolve dashboard crashes and hangs, enough RAM and storage device may be installed.
- Long-term data retention can be accomplished using big data architecture and unlimited scalability technologies
- In order for additional corporate personnel to access the dashboard, user access control and group policy can be created.
- By comparing older data with current data in the system, machine learning and artificial intelligence approaches may be utilized to detect unknown patterns.
- In the future, features to monitor the temperature of various servers and hosts might be added.

6. Bibliography

Behr, A., 2007. *network monitoring,* s.l.: s.n.

Cacti, 2021. *About Cacti.* [Online] Available at: https://www.cacti.net/ [Accessed 15 12 2021].

CentOS, 2022. *CentOS.* [Online] Available at: https://wiki.centos.org/ [Accessed 20 04 2022].

Cisco, 2021. *Network Automation.* [Online] Available at: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html#~benefits [Accessed 25 11 2021].

Core, N., 2022. *Nagios Core Overview.* [Online] Available at: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#:~:text=What%20Is%20Nagios%20Core%3F,most%20other%20unices%20as%20well. [Accessed 11 04 2022].

Digite, 2021. *Scrum Methodology & Scrum Project Management.* [Online] Available at: https://www.digite.com/agile/scrum-methodology/ [Accessed 24 11 2021].

GeekforGeeks, 2022. *Software Engineering | Spiral Model.* [Online] Available at: https://www.geeksforgeeks.org/software-engineering-spiral-model/ [Accessed 18 04 2022].

Helpsystems, 2021. *Challenges with Network Monitoring: Preventing Outages.* [Online] Available at: https://www.helpsystems.com/intermapper/resources/articles/prevent-outages-with-network-monitoring-software
[Accessed 25 11 2021].

LiveAction, 2022. *Network Monitoring Tools.* [Online] Available at: https://www.liveaction.com/resources/blog/a-brief-history-of-network-monitoring-tools/
[Accessed 11 04 2022].

NSClient++, 2022. *About NSClient++.* [Online] Available at: https://docs.nsclient.org/
[Accessed 20 04 2022].

Pat Research, 2021. *Network Monitoring Software.* [Online] Available at: https://www.predictiveanalyticstoday.com/top-free-premium-network-monitoring-software/
[Accessed 11 04 2022].

Pauli, J., 2013. Tools and Techniques to Attack the Web. In: T. E. Scott White, ed. *The Basics of Web Hacking.* s.l.:s.n., pp. 19-40.

Putty, 2022. *Putty.* [Online] Available at: https://www.putty.org/
[Accessed 20 04 2022].

TechTarget, 2021. *MySQL.* [Online] Available at: https://searchoracle.techtarget.com/definition/MySQL
[Accessed 15 12 2021].

Tecmint, 2015. *Observium.* [Online]
Available at: https://www.tecmint.com/install-observium-in-centos/
[Accessed 15 12 2021].

Tutorialspoint, 2022. *SDLC - Waterfall Model.* [Online]
Available at: https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm
[Accessed 18 04 2022].

Virtualbox, 2022. *Virtualbox.* [Online]
Available at: virtualbox.org
[Accessed 20 04 2022].

WinSCP, 2022. *WinSCP.* [Online]
Available at: https://winscp.net/eng/docs/introduction
[Accessed 20 04 2022].

XAMPP, 2022. *XAMPP.* [Online]
Available at: https://www.apachefriends.org/about.html
[Accessed 20 04 2022].

Yoram Ehrlich, 2020. *Network Tool Sprawl: Enabling Flexibility While Managing Chaos.* [Online]
Available at: https://www.networkcomputing.com/networking/overcome-network-tool-sprawl
[Accessed 11 04 2022].

Zabbix, 2021. *Zabbix.* [Online]
Available at: https://www.zabbix.com/network_monitoring
[Accessed 15 12 2021].

Zaynabzahrablog, 2017. *SCRUM Methodology.* [Online] Available at: https://zaynabzahrablog.wordpress.com/2017/10/07/scrum-methodology/ [Accessed 24 11 2021].

7. References

Behr, A., 2007. *network monitoring,* s.l.: s.n.

Cacti, 2021. *About Cacti.* [Online] Available at: https://www.cacti.net/ [Accessed 15 12 2021].

CentOS, 2022. *CentOS.* [Online] Available at: https://wiki.centos.org/ [Accessed 20 04 2022].

Cisco, 2021. *Network Automation.* [Online] Available at: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html#~benefits [Accessed 25 11 2021].

Core, N., 2022. *Nagios Core Overview.* [Online] Available at: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html#:~:te

xt=What%20Is%20Nagios%20Core%3F,most%20other%20unices%20as%20well.

[Accessed 11 04 2022].

Digite, 2021. *Scrum Methodology & Scrum Project Management.* [Online] Available at: https://www.digite.com/agile/scrum-methodology/

[Accessed 24 11 2021].

GeekforGeeks, 2022. *Software Engineering | Spiral Model.* [Online] Available at: https://www.geeksforgeeks.org/software-engineering-spiral-model/

[Accessed 18 04 2022].

Helpsystems, 2021. *Challenges with Network Monitoring: Preventing Outages.* [Online] Available at: https://www.helpsystems.com/intermapper/resources/articles/prevent-outages-with-network-monitoring-software

[Accessed 25 11 2021].

LiveAction, 2022. *Network Monitoring Tools.* [Online] Available at: https://www.liveaction.com/resources/blog/a-brief-history-of-network-monitoring-tools/

[Accessed 11 04 2022].

NSClient++, 2022. *About NSClient++.* [Online] Available at: https://docs.nsclient.org/

[Accessed 20 04 2022].

Pat Research, 2021. *Network Monitoring Software.* [Online] Available at: https://www.predictiveanalyticstoday.com/top-free-premium-network-monitoring-software/

[Accessed 11 04 2022].

Pauli, J., 2013. Tools and Techniques to Attack the Web. In: T. E. Scott White, ed. *The Basics of Web Hacking.* s.l.:s.n., pp. 19-40.

Putty, 2022. *Putty.* [Online] Available at: https://www.putty.org/ [Accessed 20 04 2022].

TechTarget, 2021. *MySQL.* [Online] Available at: https://searchoracle.techtarget.com/definition/MySQL [Accessed 15 12 2021].

Tecmint, 2015. *Observium.* [Online] Available at: https://www.tecmint.com/install-observium-in-centos/ [Accessed 15 12 2021].

Tutorialspoint, 2022. *SDLC - Waterfall Model.* [Online] Available at: https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm [Accessed 18 04 2022].

Virtualbox, 2022. *Virtualbox.* [Online] Available at: virtualbox.org [Accessed 20 04 2022].

WinSCP, 2022. *WinSCP.* [Online] Available at: https://winscp.net/eng/docs/introduction [Accessed 20 04 2022].

XAMPP, 2022. *XAMPP.* [Online] Available at: https://www.apachefriends.org/about.html [Accessed 20 04 2022].

Yoram Ehrlich, 2020. *Network Tool Sprawl: Enabling Flexibility While Managing Chaos.* [Online]
Available at: https://www.networkcomputing.com/networking/overcome-network-tool-sprawl
[Accessed 11 04 2022].

Zabbix, 2021. *Zabbix.* [Online]
Available at: https://www.zabbix.com/network_monitoring
[Accessed 15 12 2021].

Zaynabzahrablog, 2017. *SCRUM Methodology.* [Online]
Available at: https://zaynabzahrablog.wordpress.com/2017/10/07/scrum-methodology/
[Accessed 24 11 2021].

8. Appendix

8.1. Appendix A: Pre-Survey

8.1.1. Pre-Survey Form

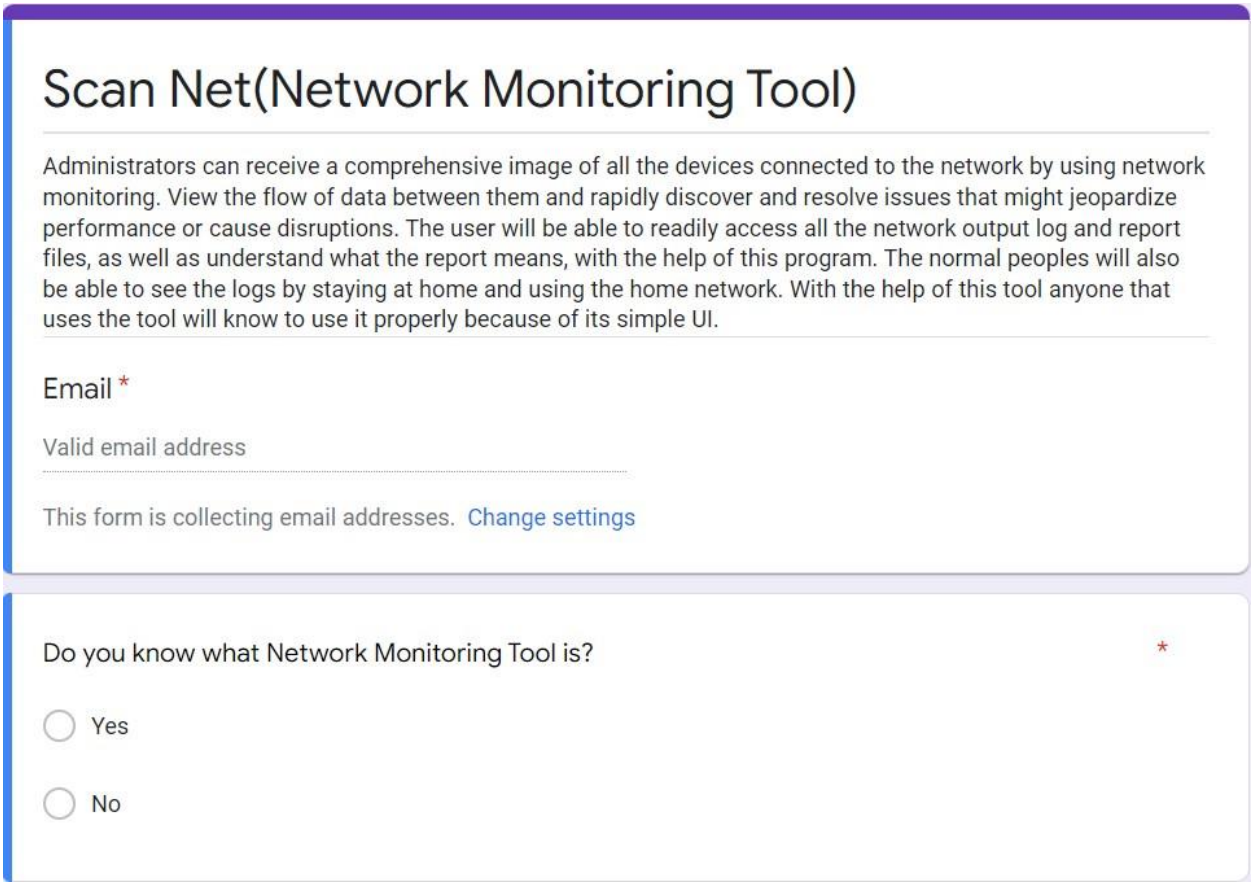


Figure 67 Pre-survey form figure 1

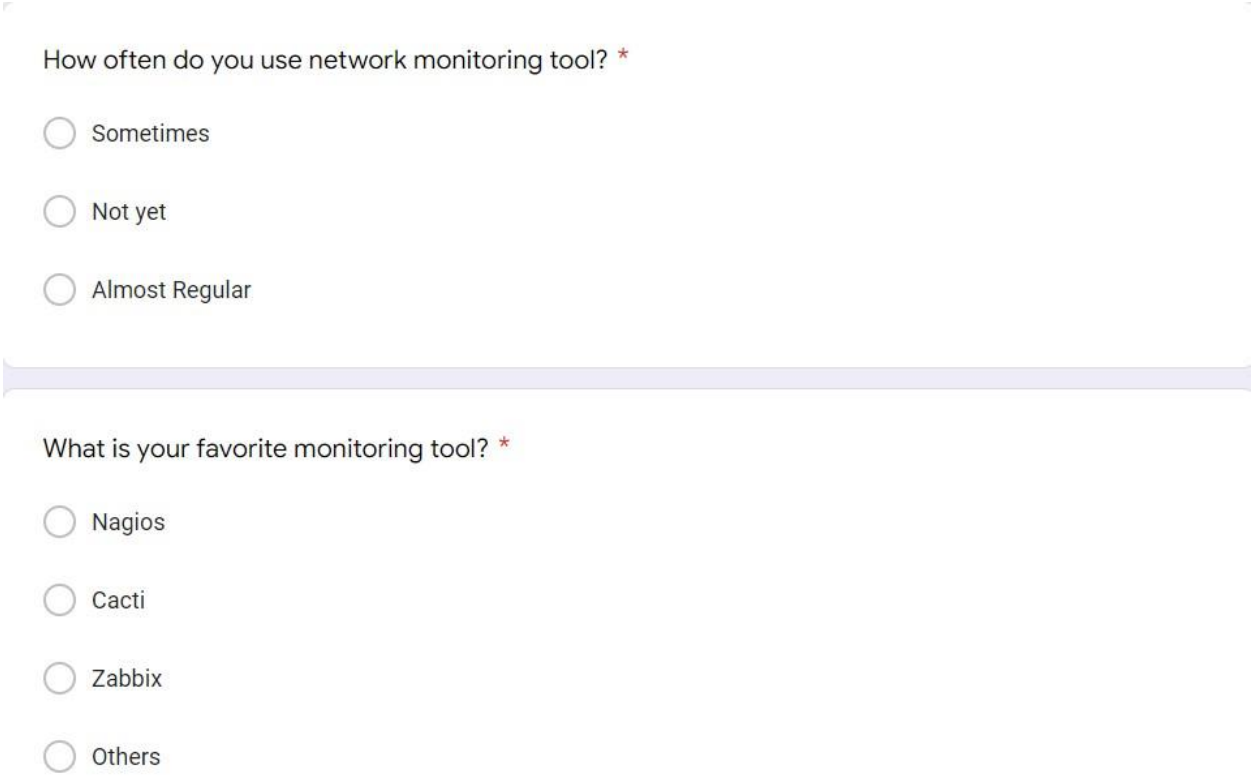


Figure 68 Pre-survey form figure 2

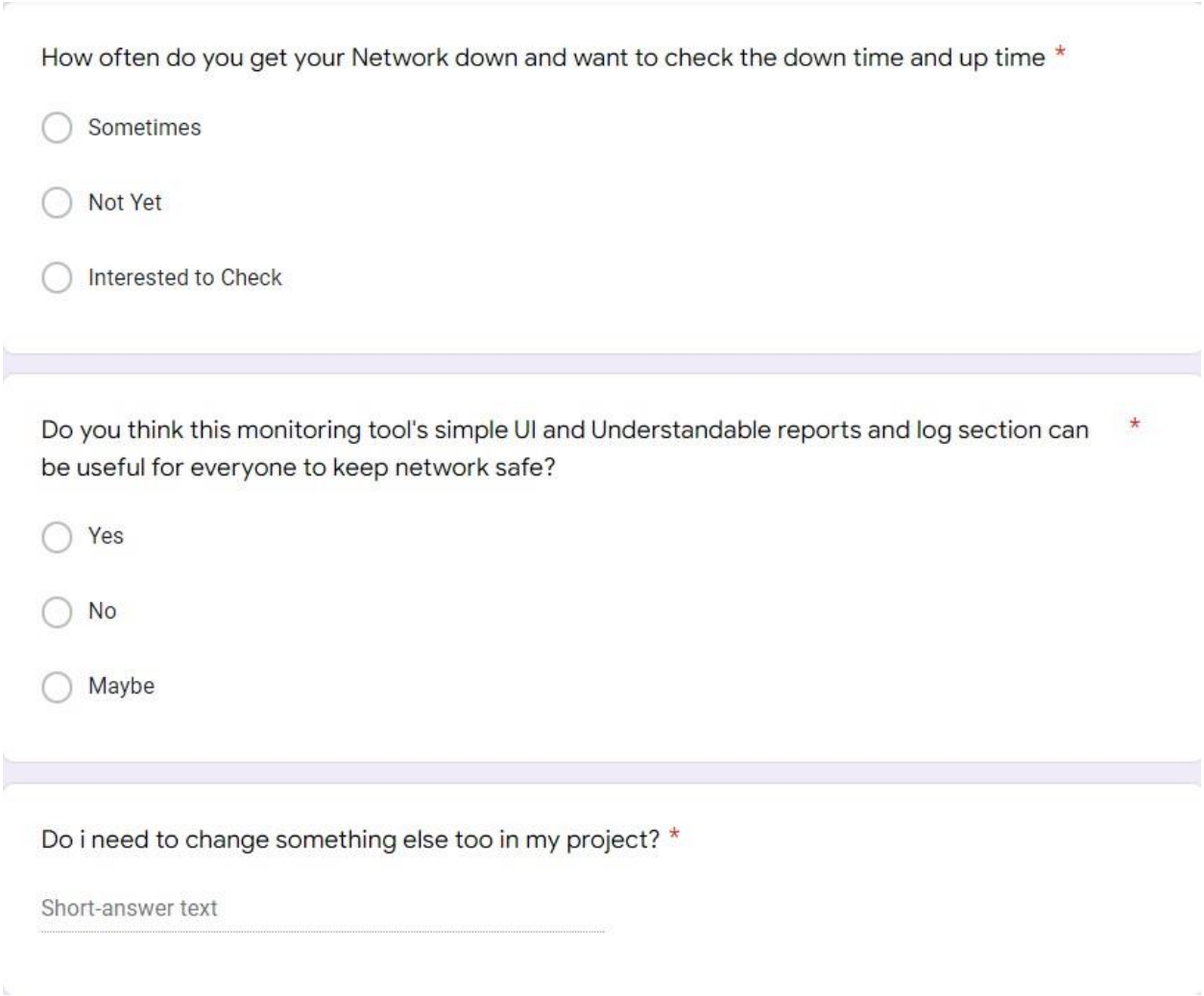


Figure 69 Pre-survey form figure 3

8.1.2. Sample of Filled Pre-Survey Form

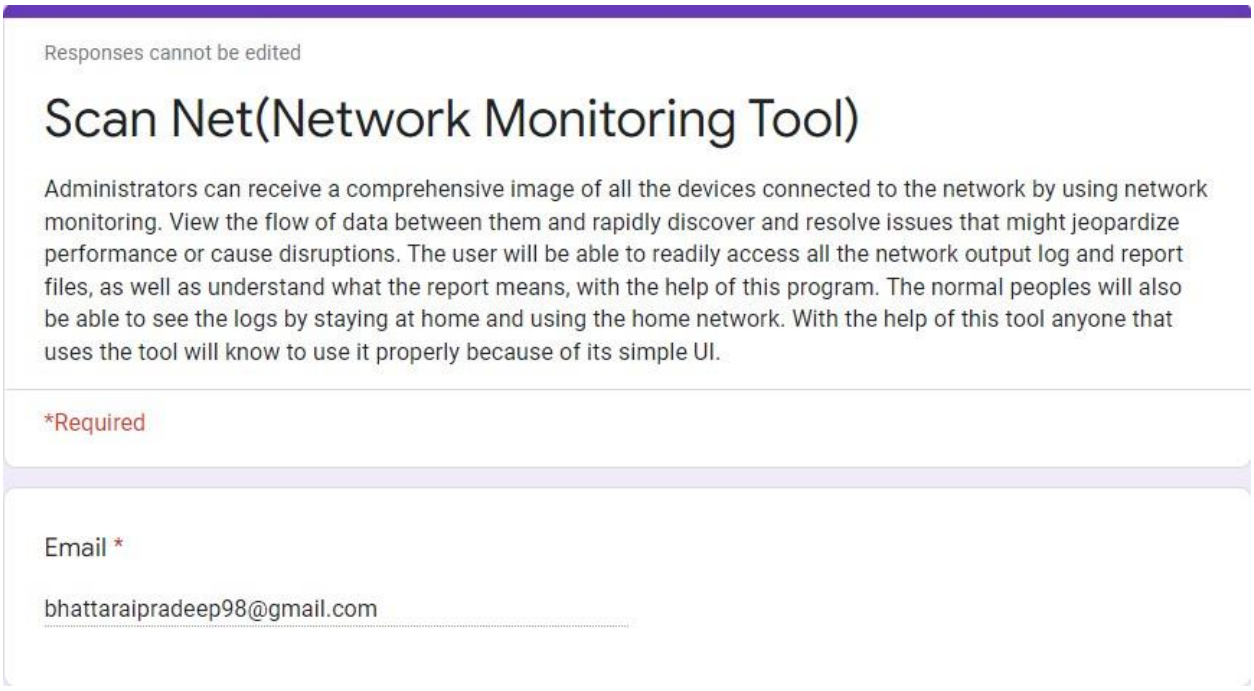


Figure 70 Pre-survey result sample figure 1

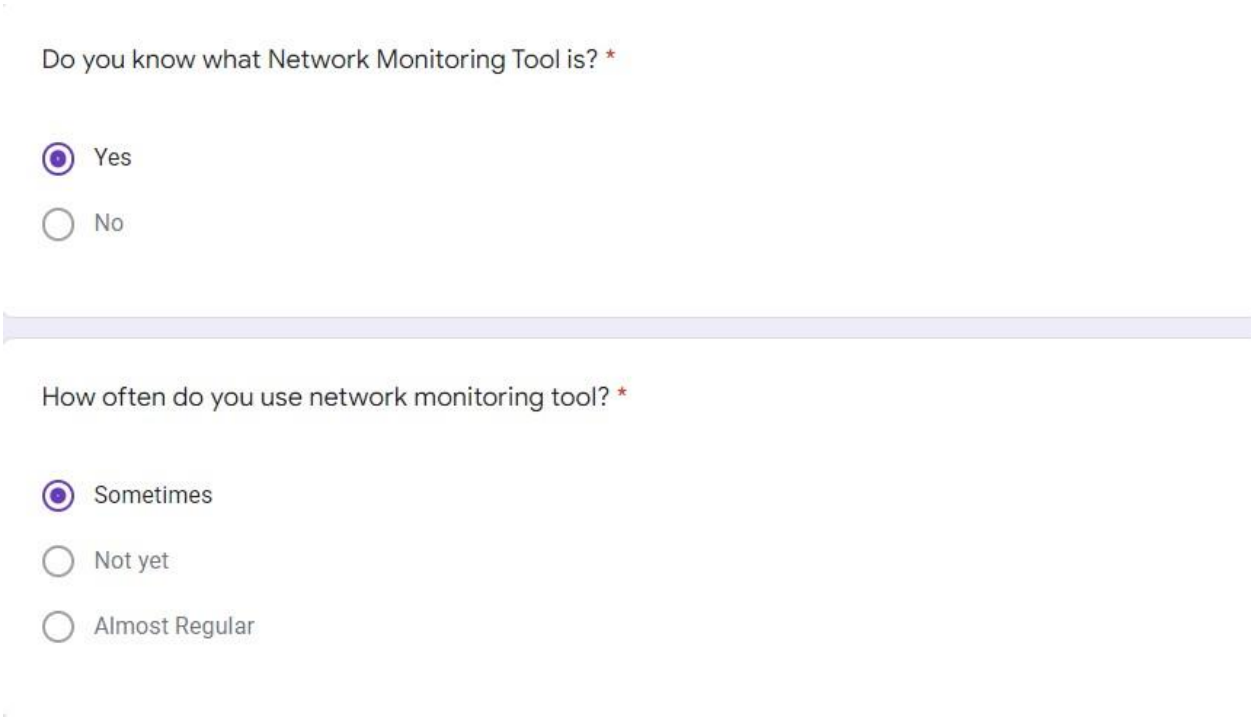


Figure 71 Pre-survey result sample figure 2

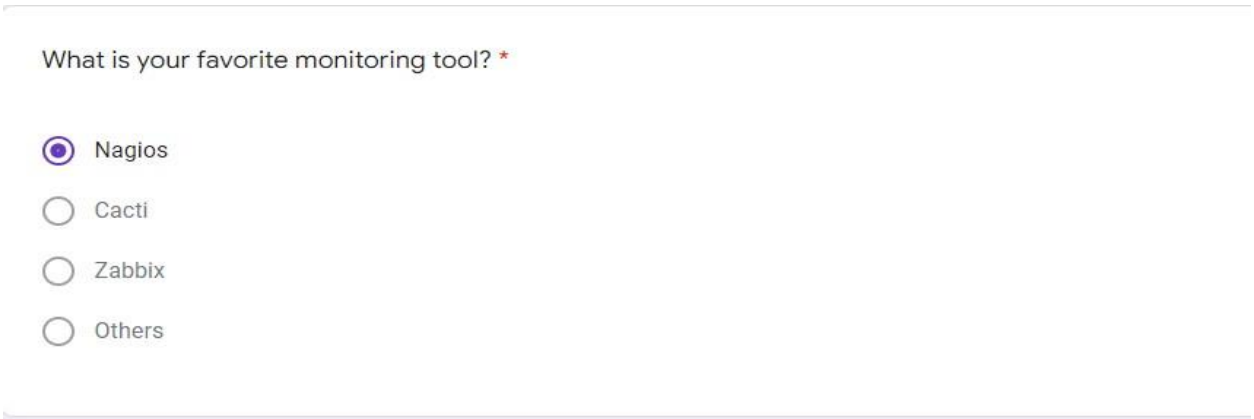


Figure 72 Pre-survey result sample figure 3

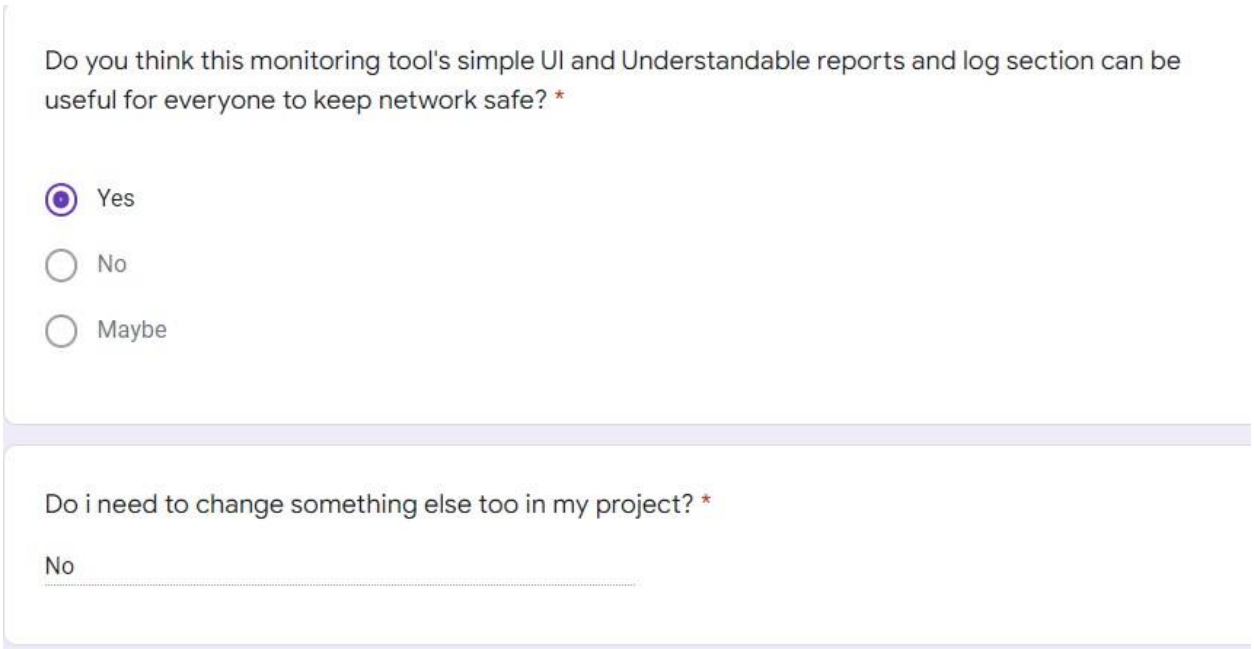


Figure 73 Pre-survey result sample figure 4

8.1.3. Pre-Survey Result

Please Enter Your Name.	Please Enter Your Email Address.	What is Your Current Position?
Mohan Guro	pyare.guro@gmail.com	IT Professional
Pradeep Bhattarai	bhattaraipradeep98@gmail.com	IT Student
Sourav KC	souravkc00@gmail.com	IT Student
Madhukar Pant	gppantha2014@gmail.com	IT Professional
Rabin Subedi	rbnsubedi01@gmail.com	IT Professional
Ayush Shrestha	ayushxhrextha@gmail.com	IT Student
Nishan Thapa	nishan.thapa024@gmail.com	IT Student
Nilesh Niroula	np01nt4s200038@islingtoncollege.edu.np	IT Student
Pranjil Thapa	pranjil001@gmail.com	IT Student
Pratik Yadav	np01nt4s210054@islingtoncollege.edu.np	IT Student
Bibek Chaudhary	np01nt4a190073@islingtoncollege.edu.np	IT Student
Gyan Bd. Tamang	gtamang47@gmail.com	IT Professional

Table 20 Pre-Survey Participants Detail Information.

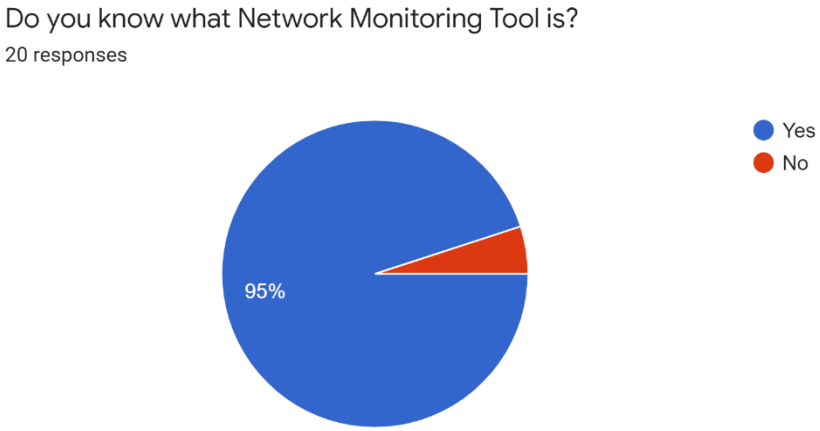


Figure 74 Pre-Survey result figure 1

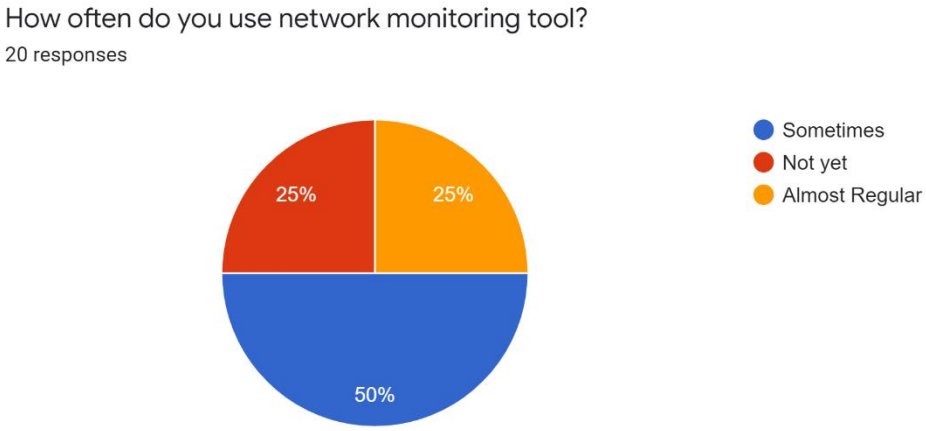


Figure 75 Pre-Survey result figure 2

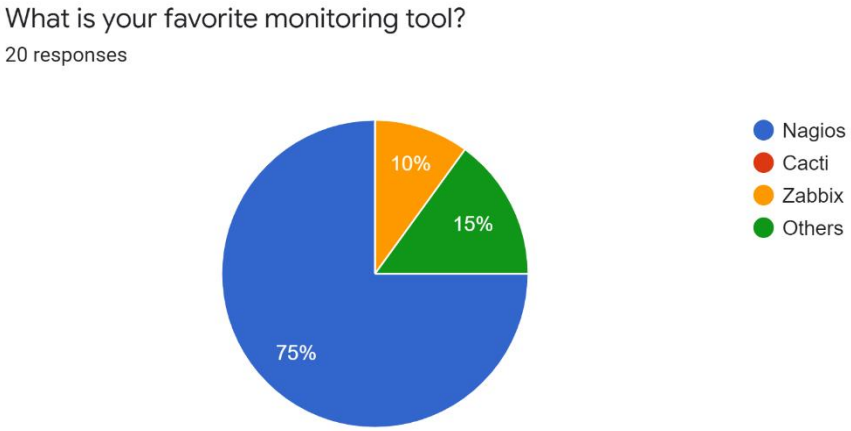


Figure 76 Pre-Survey result figure 3

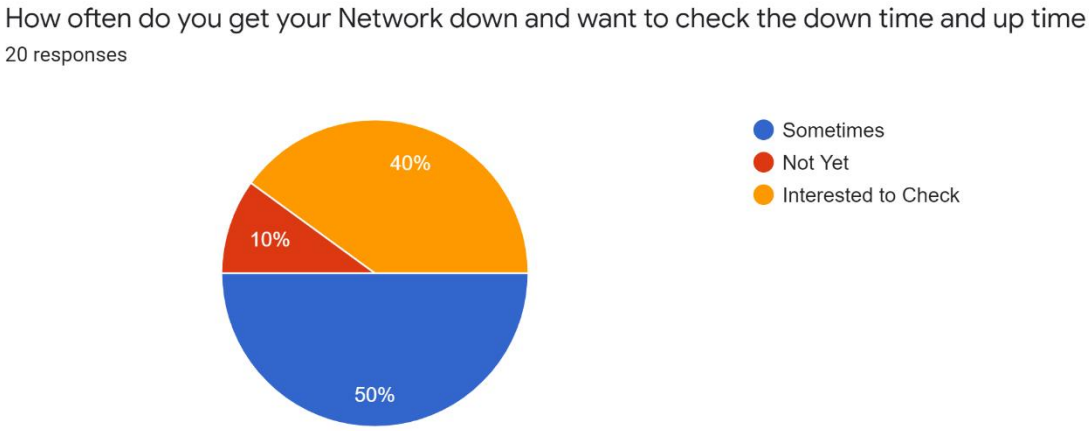


Figure 77 Pre-Survey result figure 4

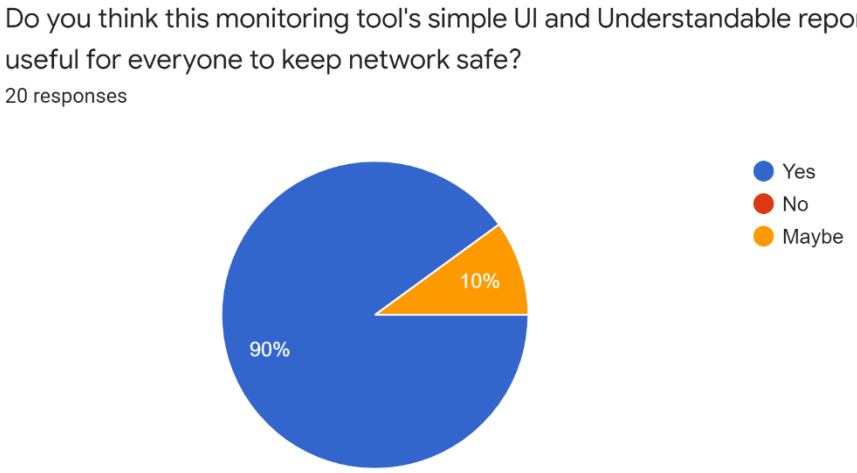


Figure 78 Pre-Survey result figure 5

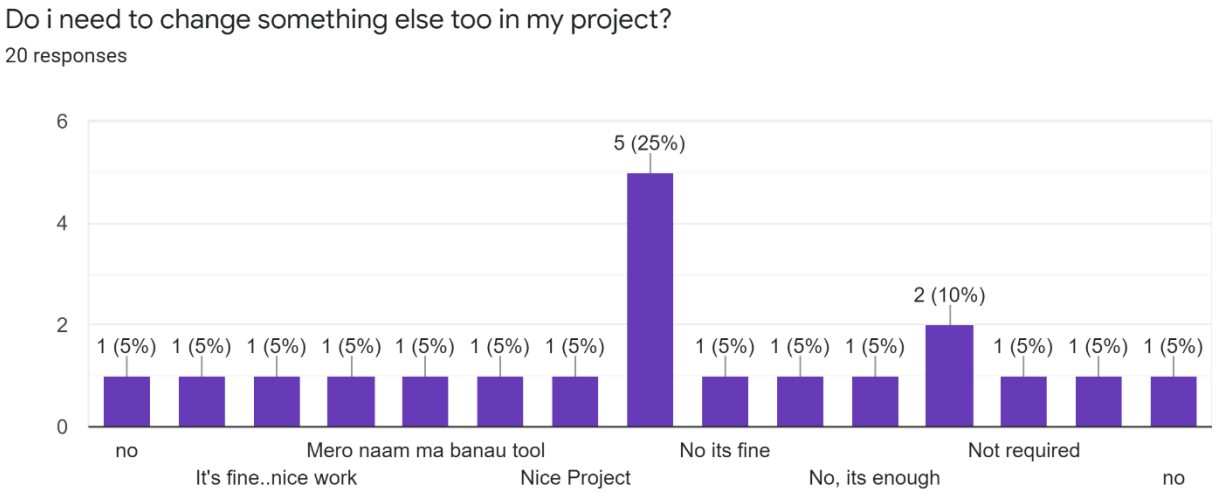


Figure 79 Pre-Survey result figure 6

8.2. Appendix B: Post-Survey

8.2.1. Post-Survey Form

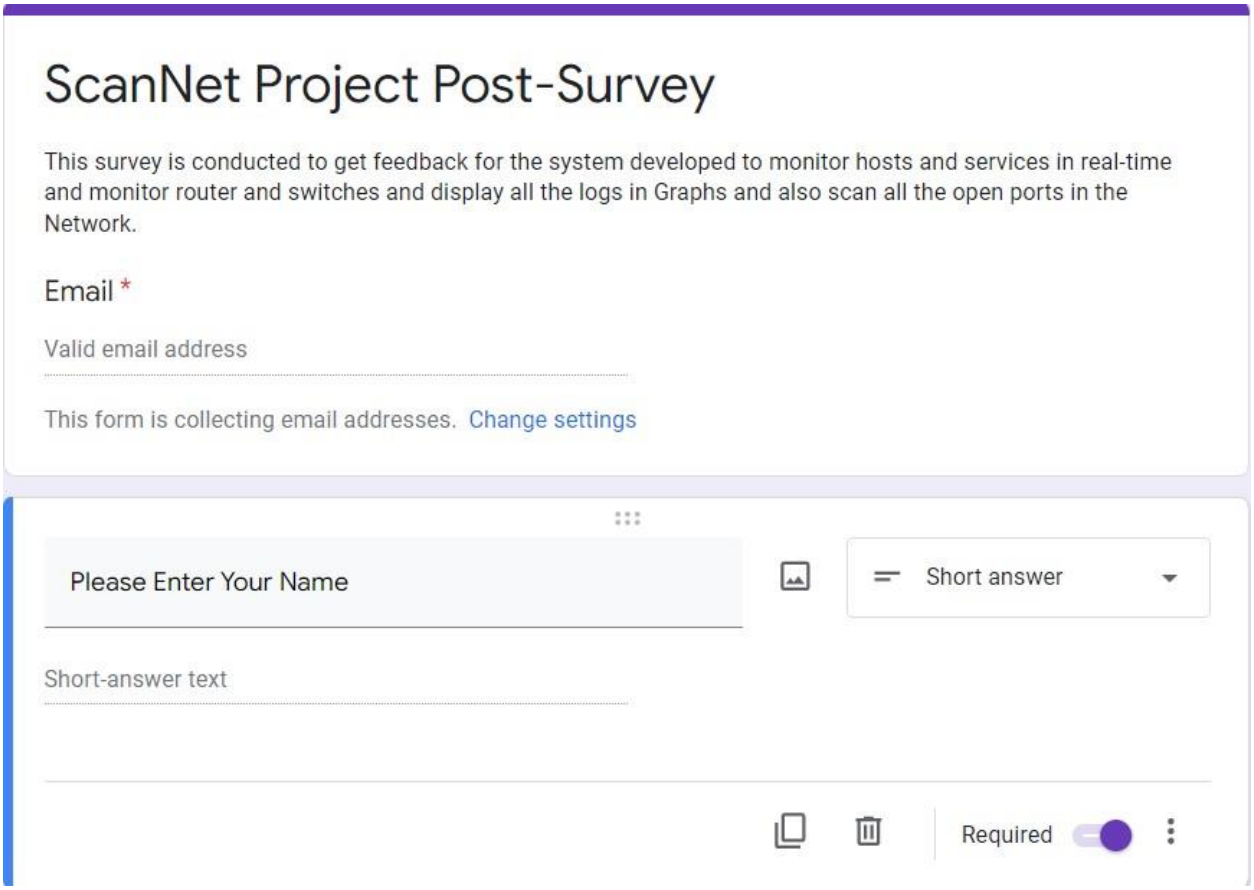


Figure 80 post-survey form figure 1

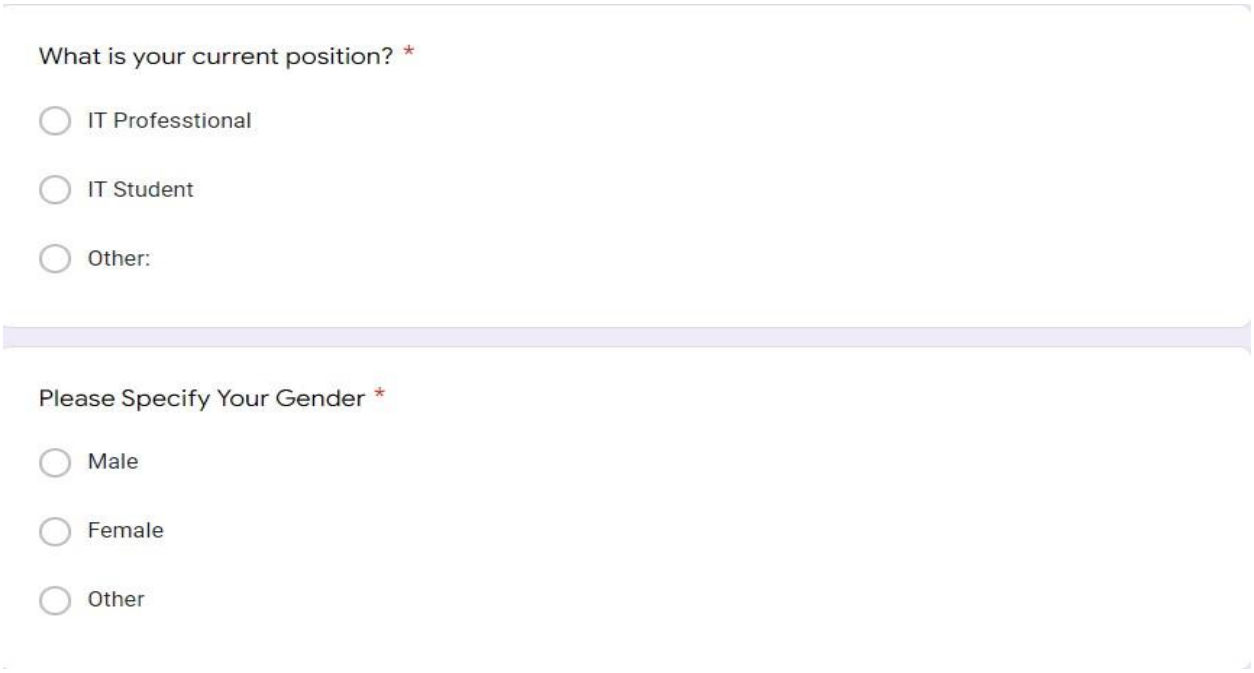


Figure 81 post-survey form figure 2

Figure 82 post-survey form figure 3

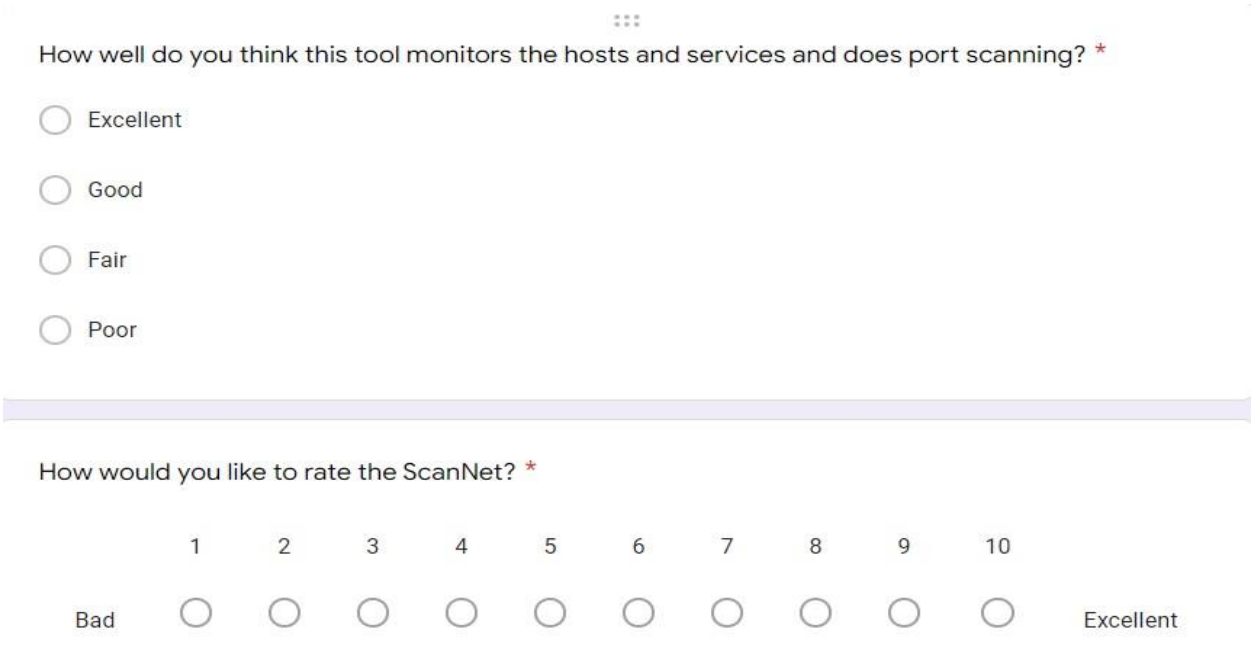


Figure 83 post-survey form figure 4

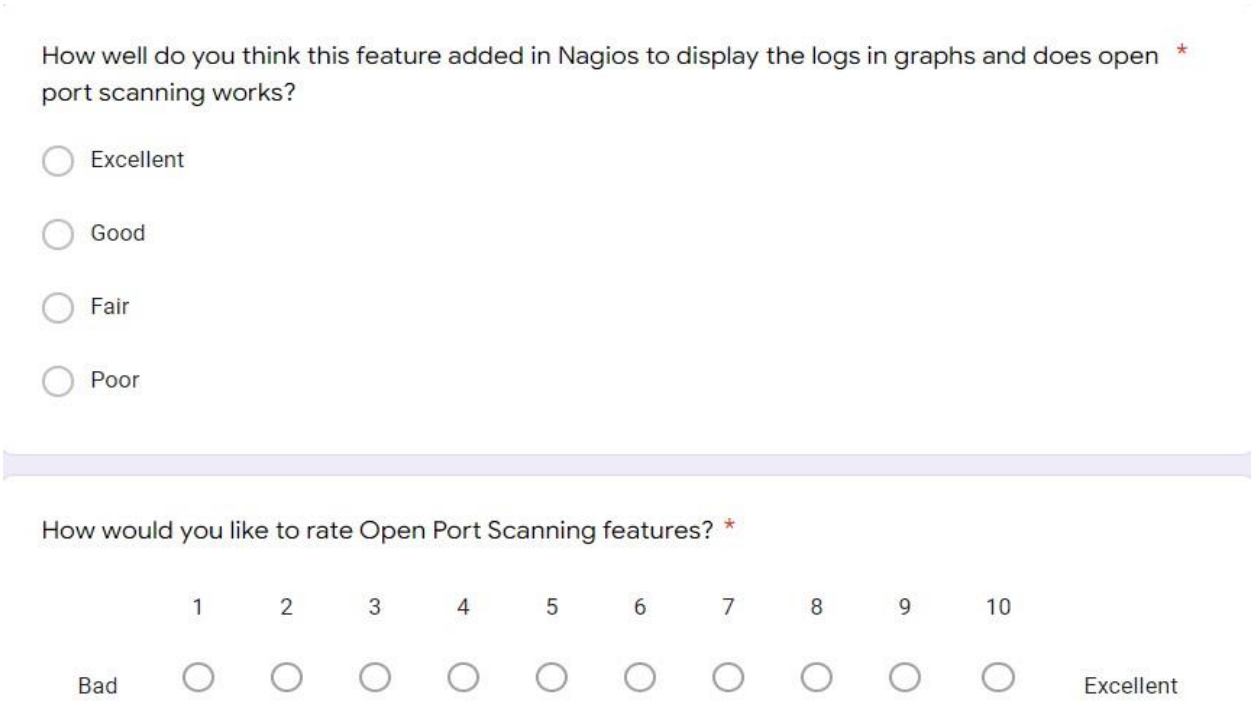


Figure 84 post-survey form figure 5

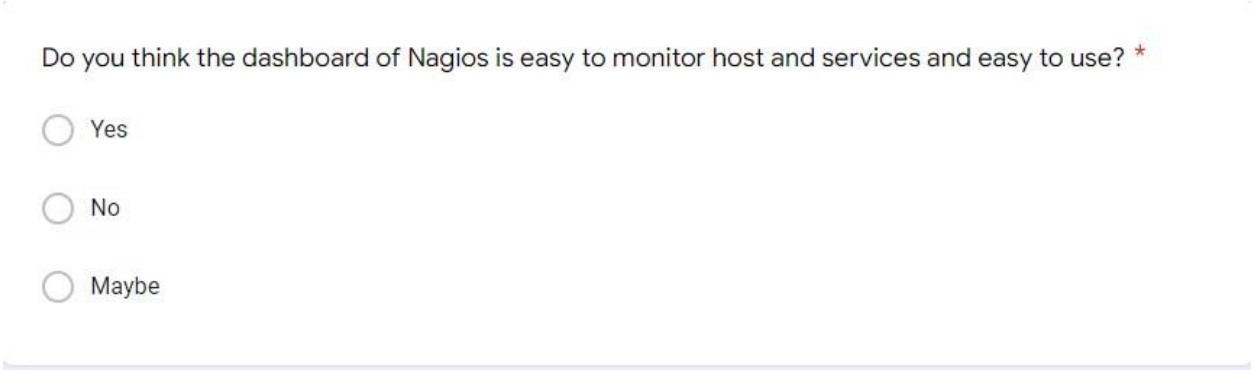


Figure 85 post-survey form figure 6

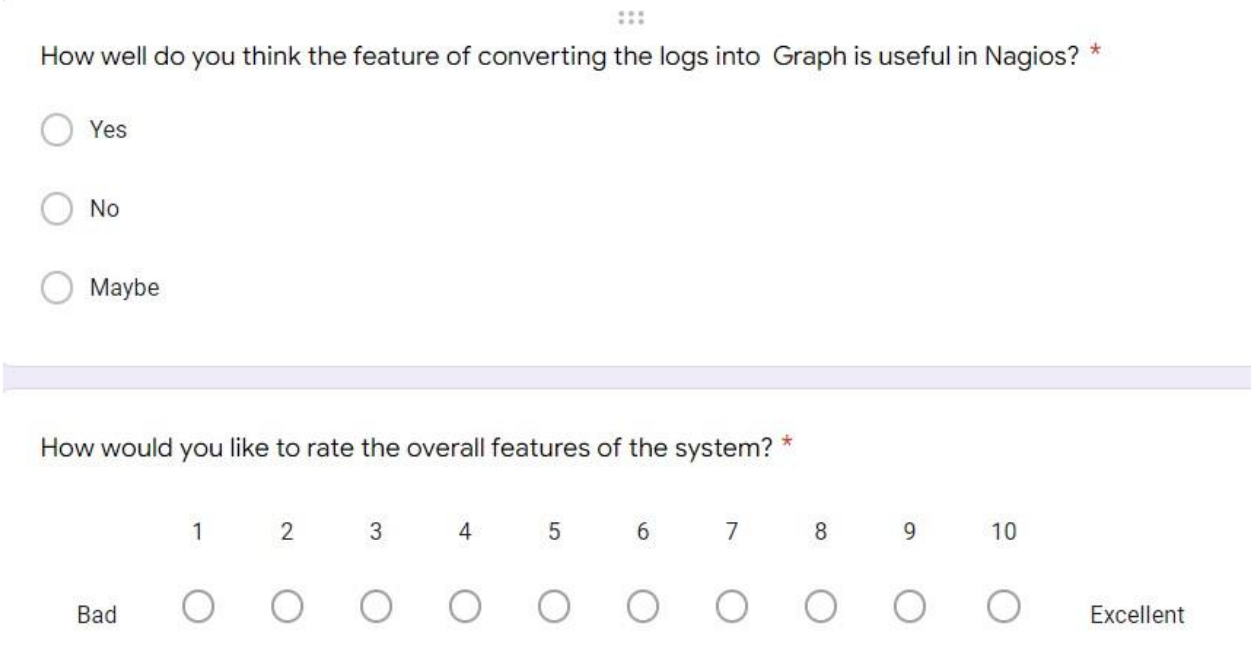


Figure 86 post-survey form figure 7

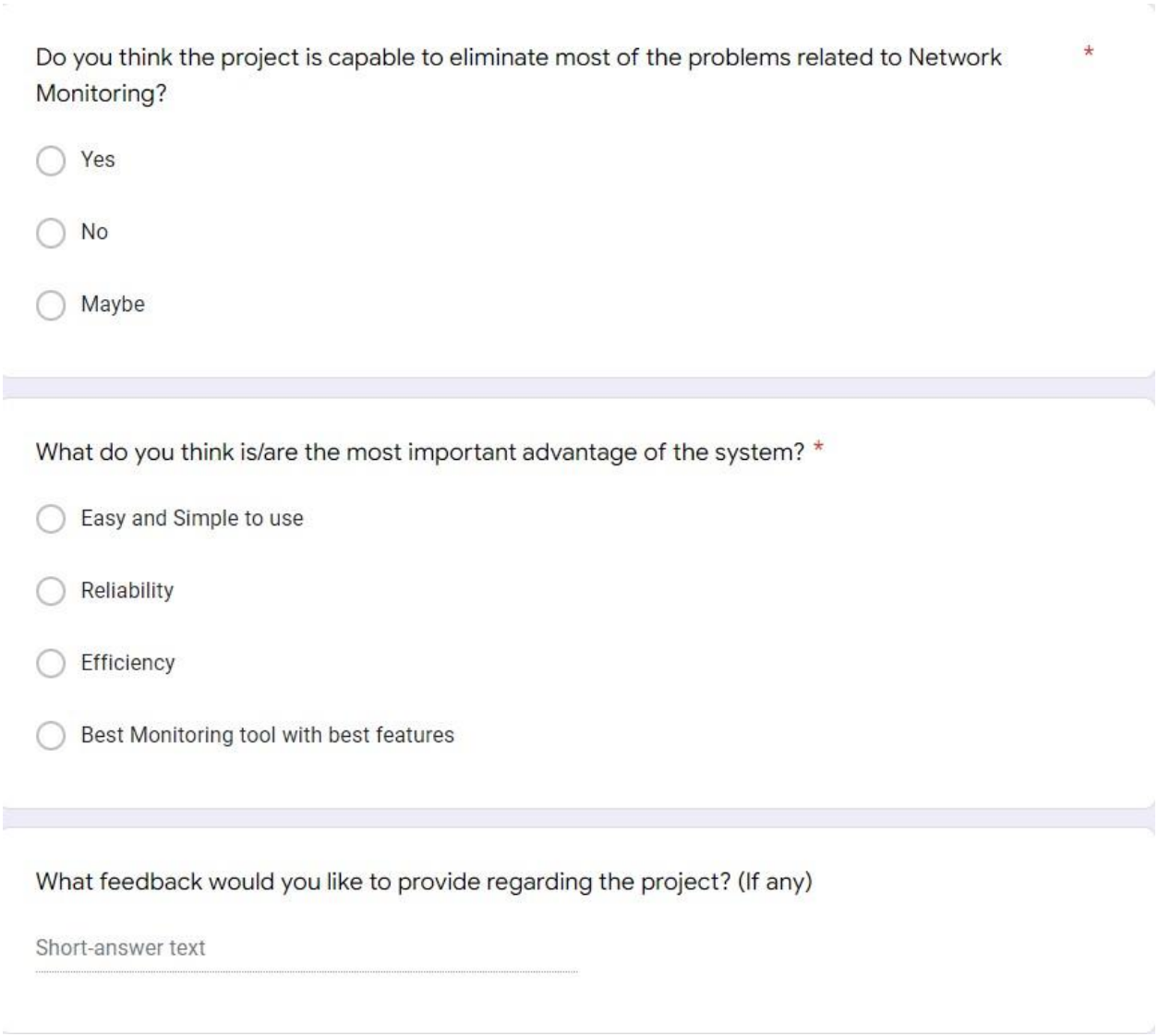


Figure 87 post-survey form figure 8

8.2.2. Sample of Filled Post-Survey Form

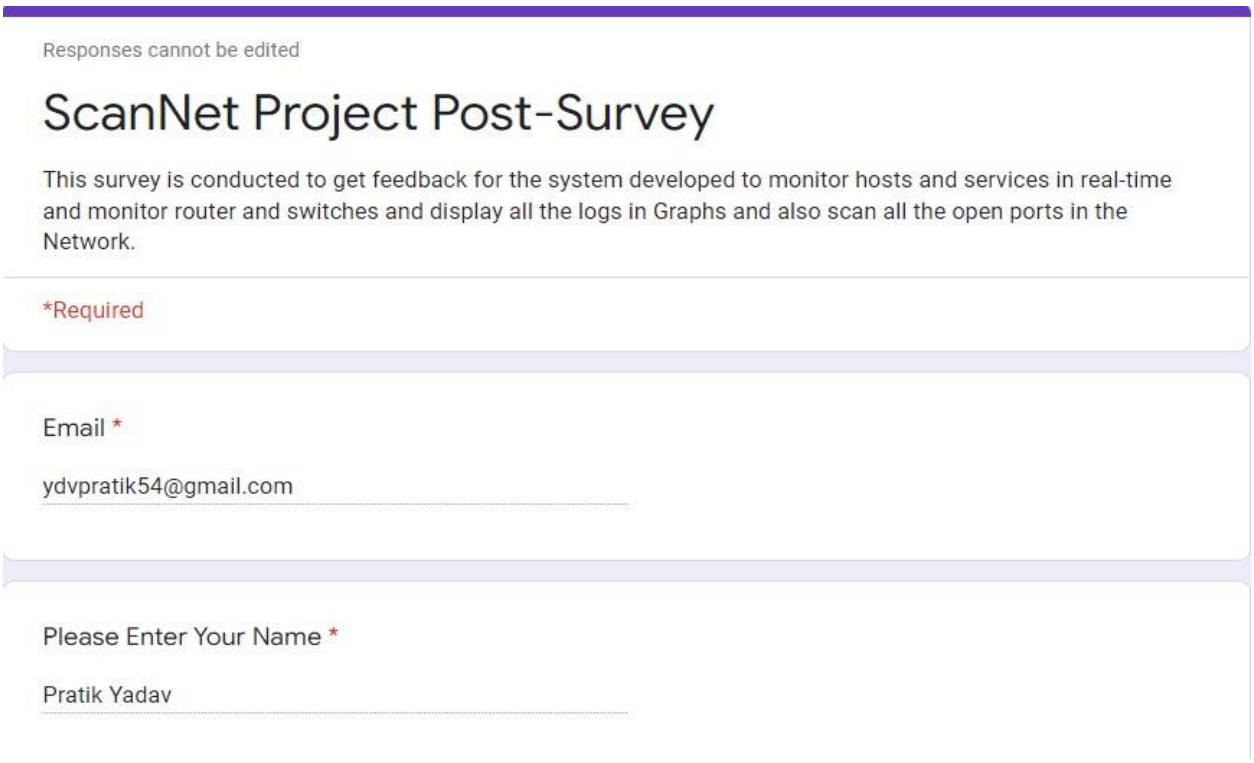


Figure 88 post-survey result sample figure 1

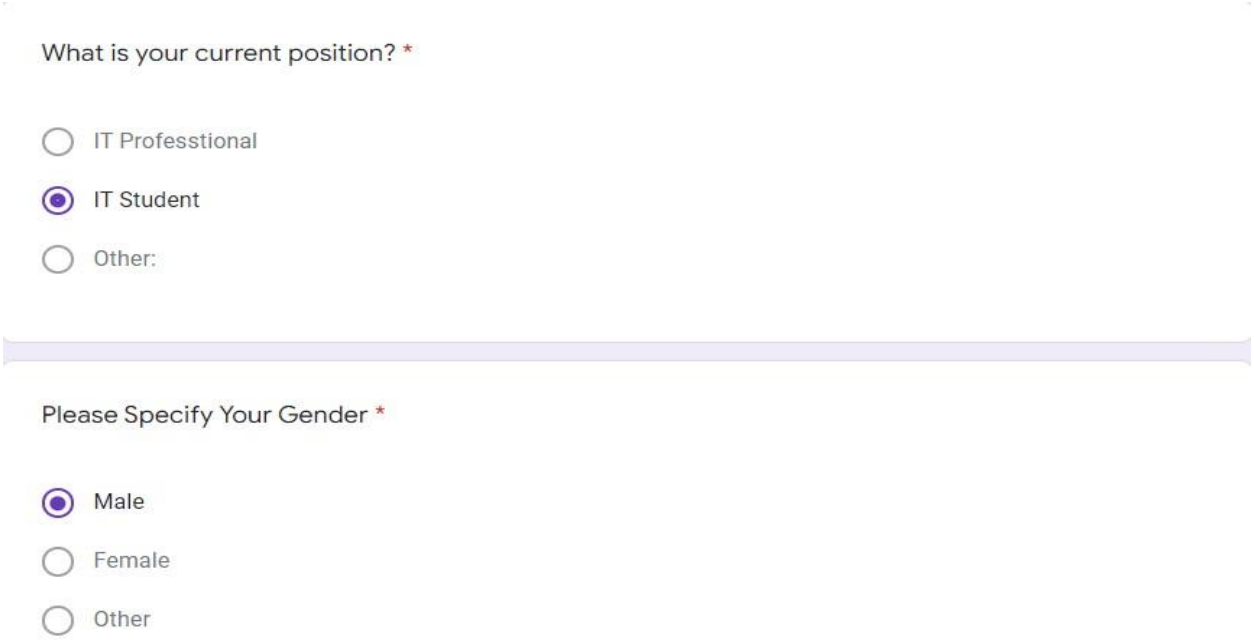


Figure 89 post-survey result sample figure 2

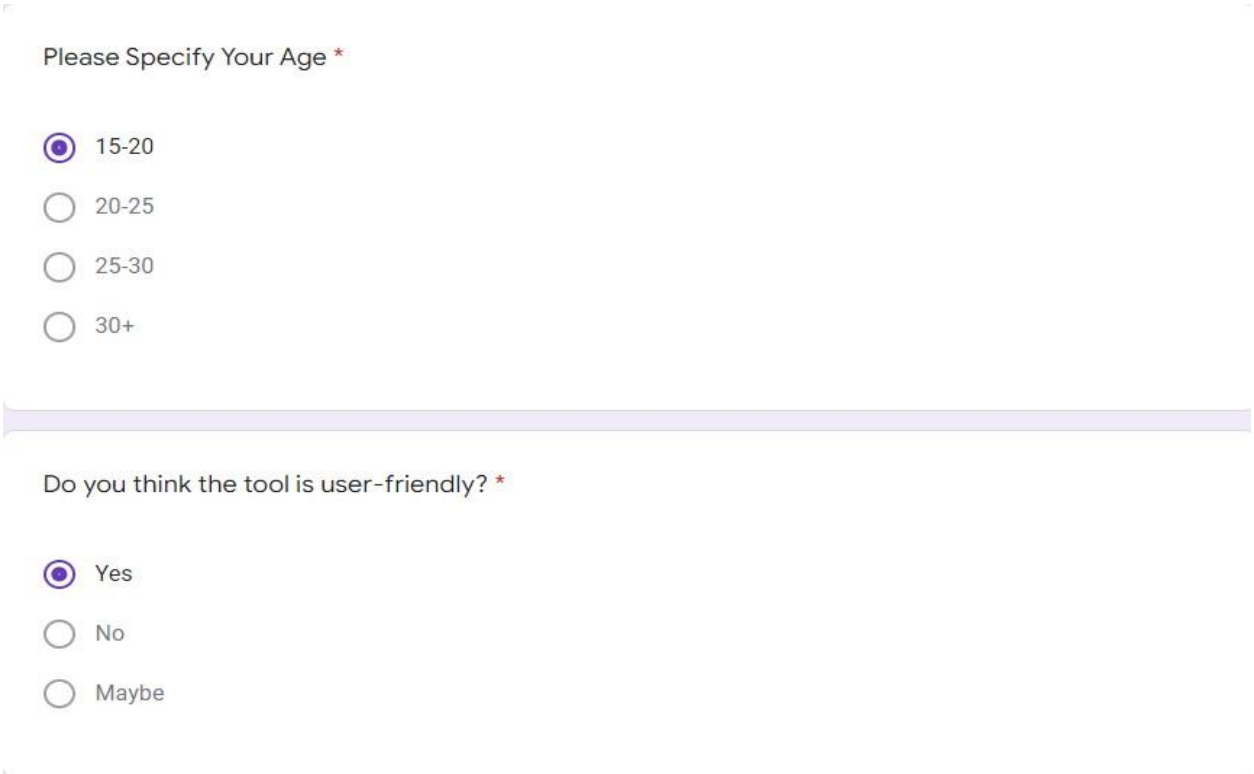


Figure 90 post-survey result sample figure 3

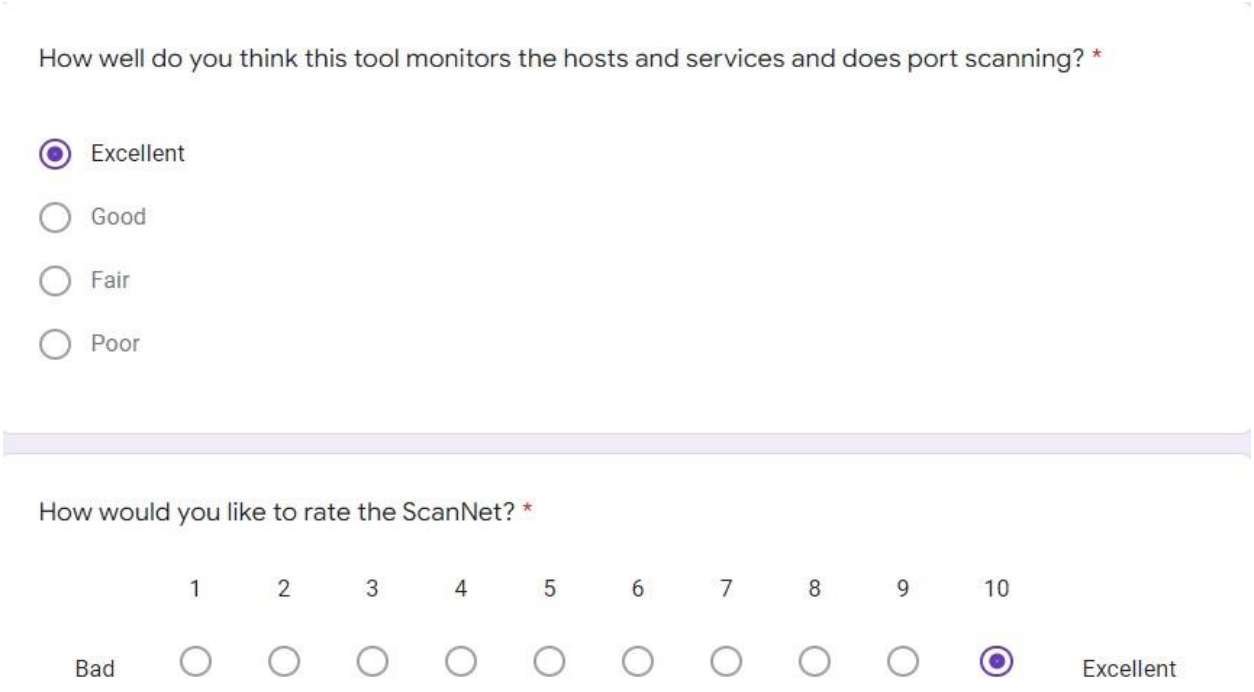


Figure 91 post-survey result sample figure 4

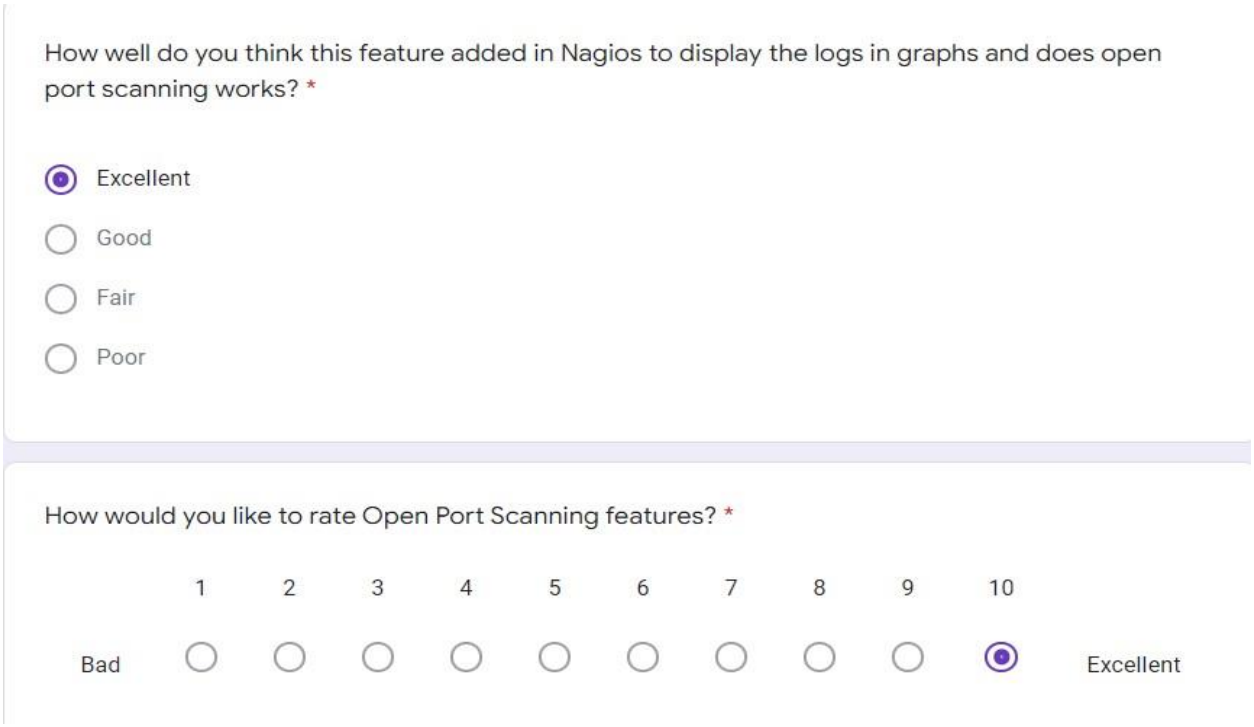


Figure 92 post-survey result sample figure 5

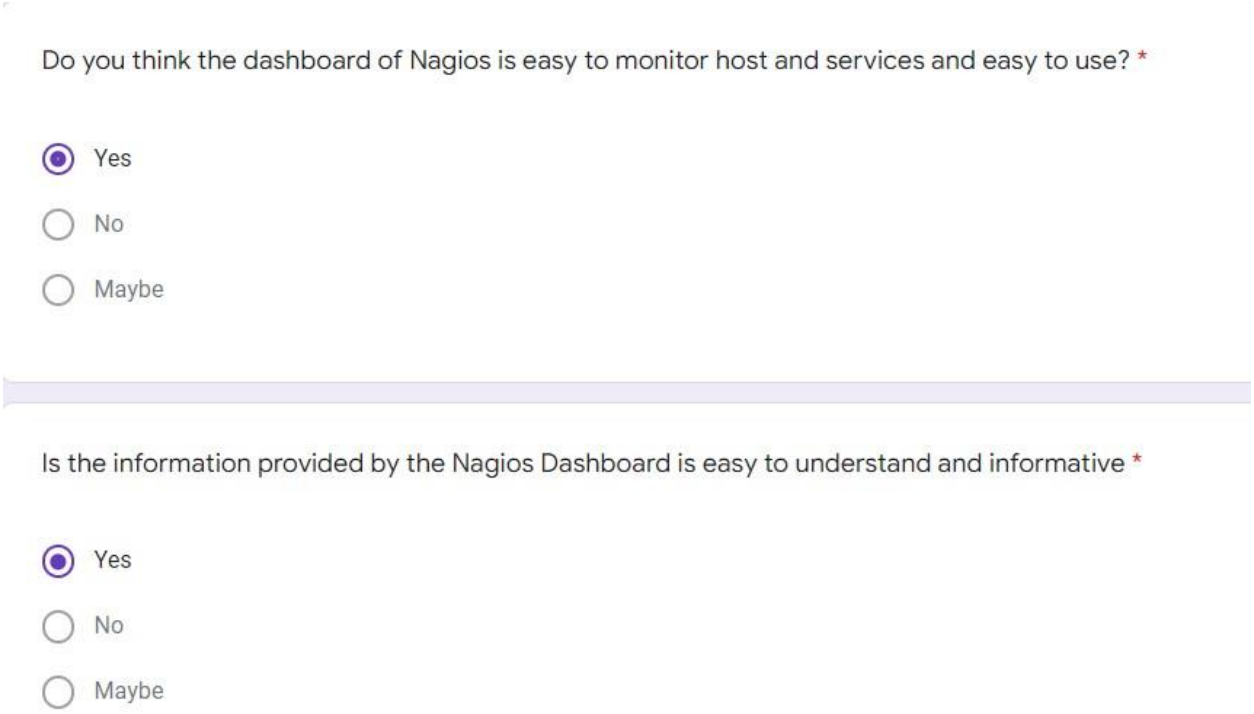


Figure 93 post-survey result sample figure 6

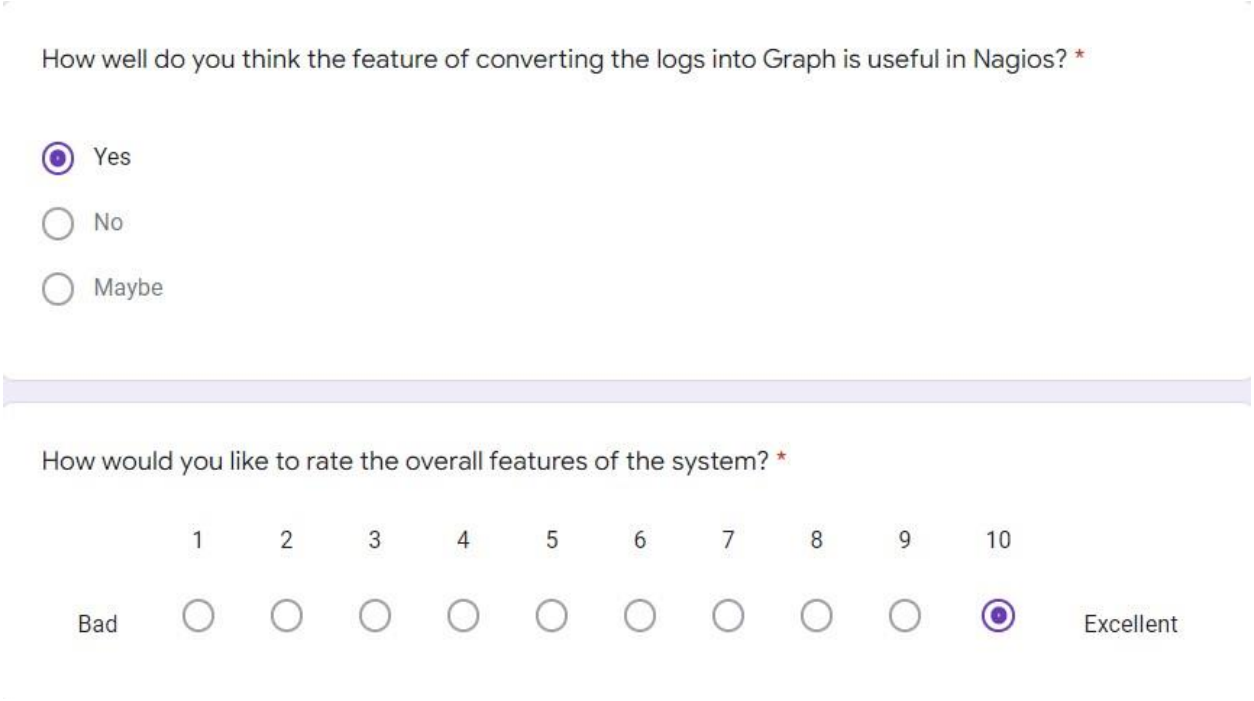


Figure 94 post-survey result sample figure 7

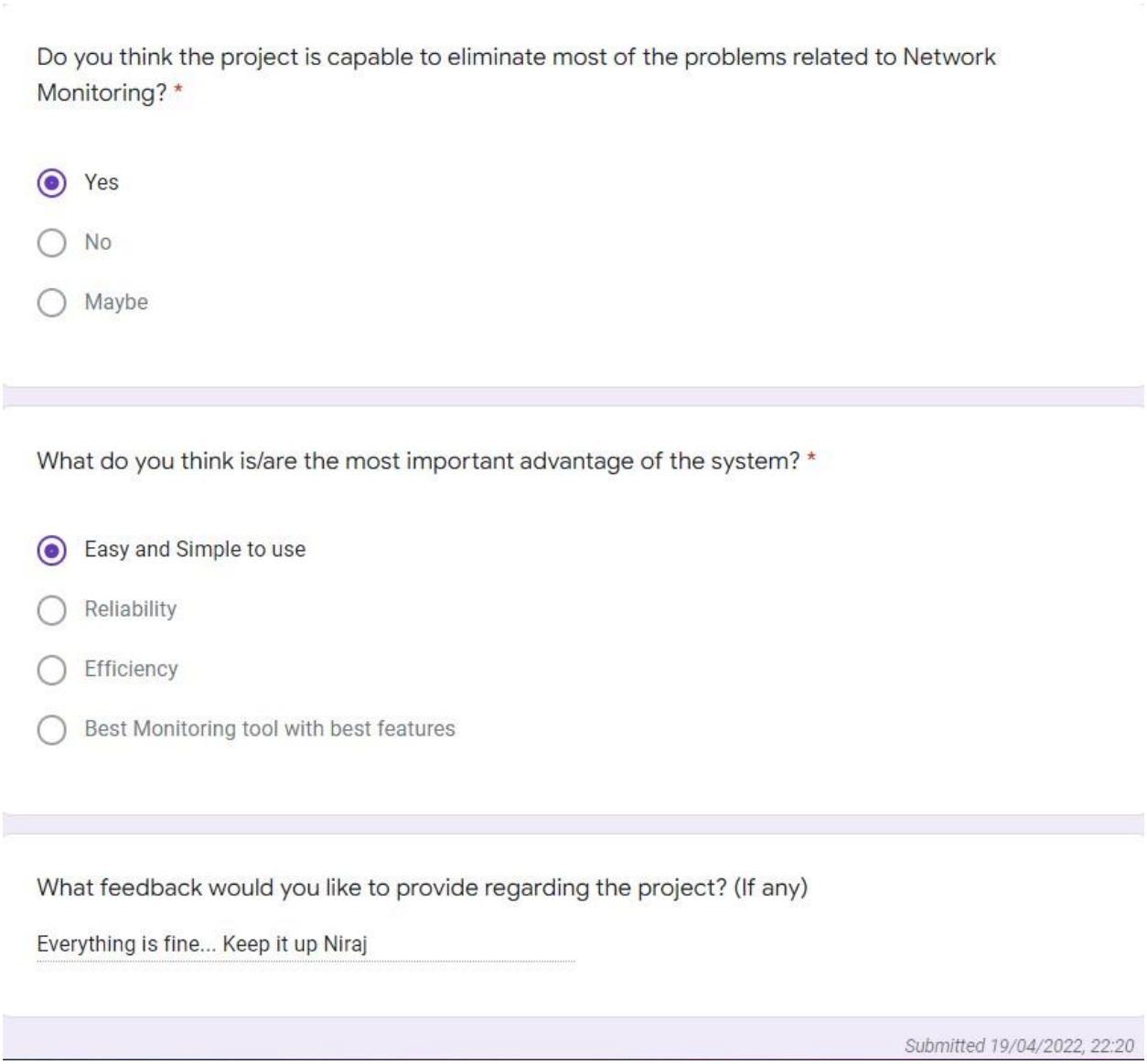


Figure 95 post-survey result sample figure 8

8.2.3. Post-Survey Result

Please Enter Your Name.	Please Enter Your Email Address.	What is Your Current Position?
Pratik Yadav	ydvpratik54@gmail.com	IT Student
Ishwor Dhakal	iswordhakal00@gmail.com	IT Student
Karsang Gurung	gurungjacob99@gmail.com	IT Student
Ujwal Bhattarai	ujwal.bhattarai61@gmail.com	IT Student
Kamal Pokharel	kamalpokharel234@gmsil.com	IT Student
Diwash Rijal	diwashrijal233@gmail.com	IT Student
Aayush Neupane	aayush.sg8@gmail.com	IT Student
Dipesh Acharya	np01nt4a190003@islingtoncollege.edu.np	IT Student
Gyan Bd. Tamang	gtamang47@gmail.com	IT Professional
Yuvaraj Niroula	yuviniroula01@gmail.com	IT Professional
Binam Karki	webcoder716@gmail.com	IT Student
Amrit Ghale	amrit18ho@gmail.com	IT Professional
Manoj Bam	mjbam72@gmail.com	IT Professional
Bibek Chaudhary	np01nt4a190188@islingtoncollege.edu.np	IT Student
Yubaraj Raya	yubarajraya12345@gmail.com	IT Student
Seekha Shrestha	shrestha.seekha2001@gmail.com	IT Student
Deepak Bokati	deepakbokati777@gmail.com	IT Student
Shreeya Shrestha	shreeya.shrestha20s@gmail.com	IT Student
Sudip Thapa	sudipthapa376@gmail.com	Others

Mandip Thapa	mandipthapa777@gmail.com	IT Student
Sapna Acharya	acharyasapna055@gmail.com	Others

Table 21 Post-Survey Participants Detail Information

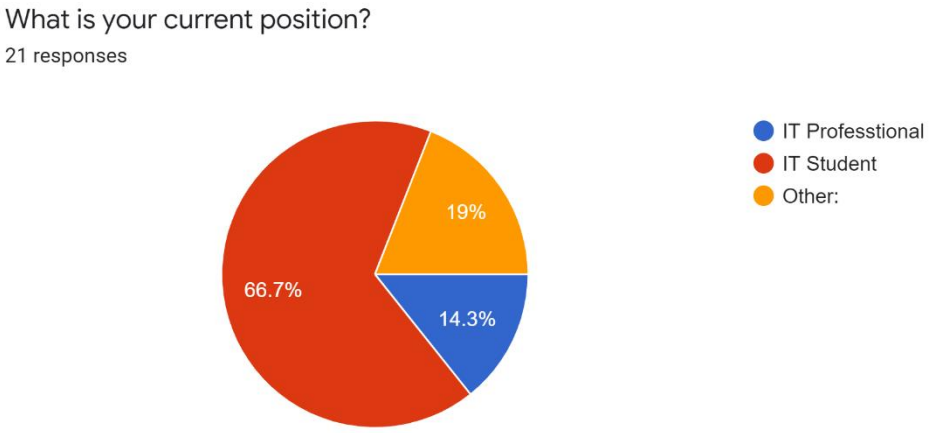


Figure 96 post-survey result figure 1

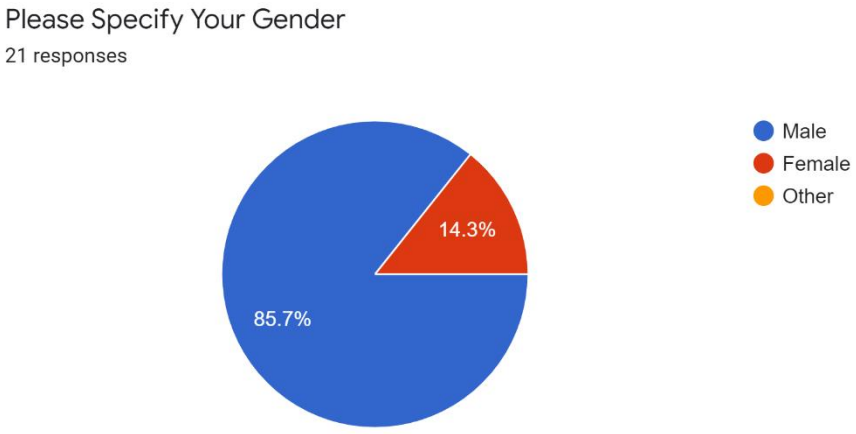


Figure 97 post-survey result figure 2

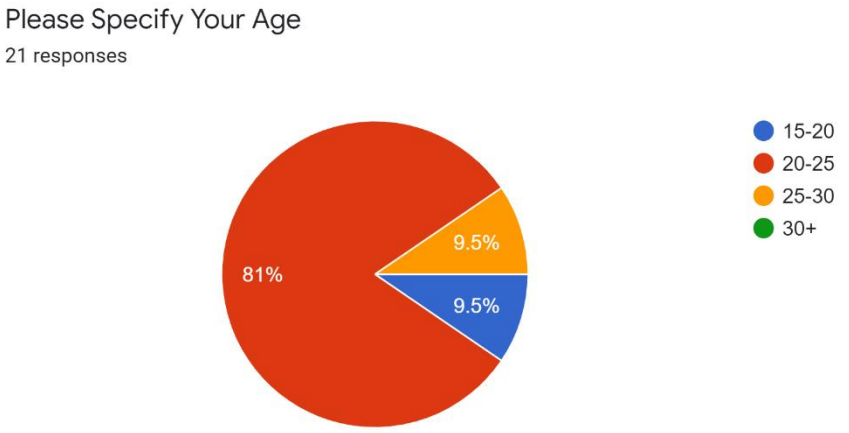


Figure 98 post-survey result figure 3

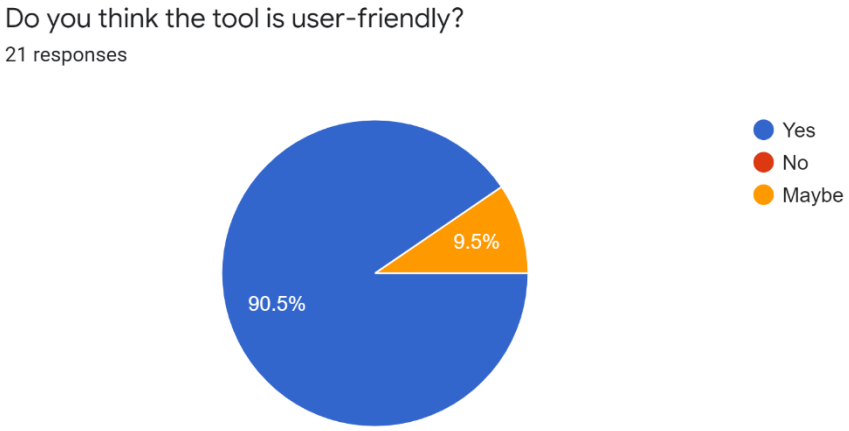


Figure 99 post-survey result figure 4

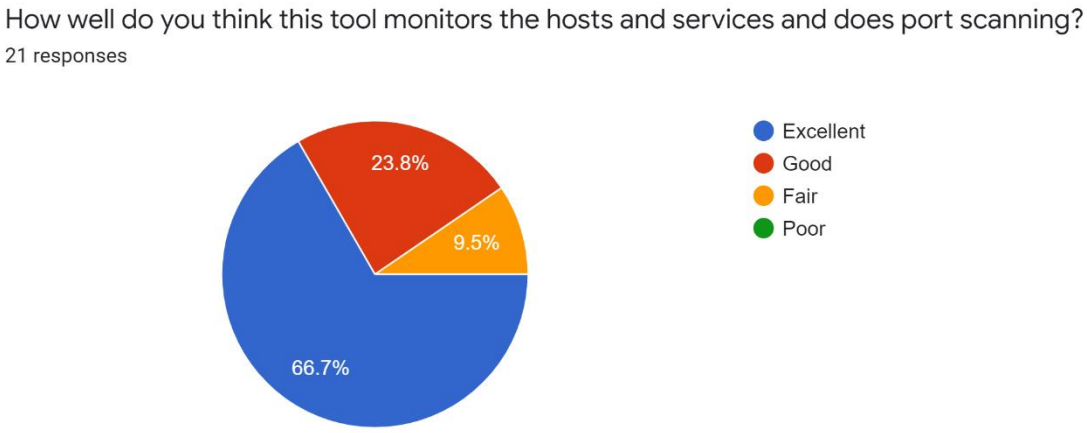


Figure 100 post-survey result figure 5

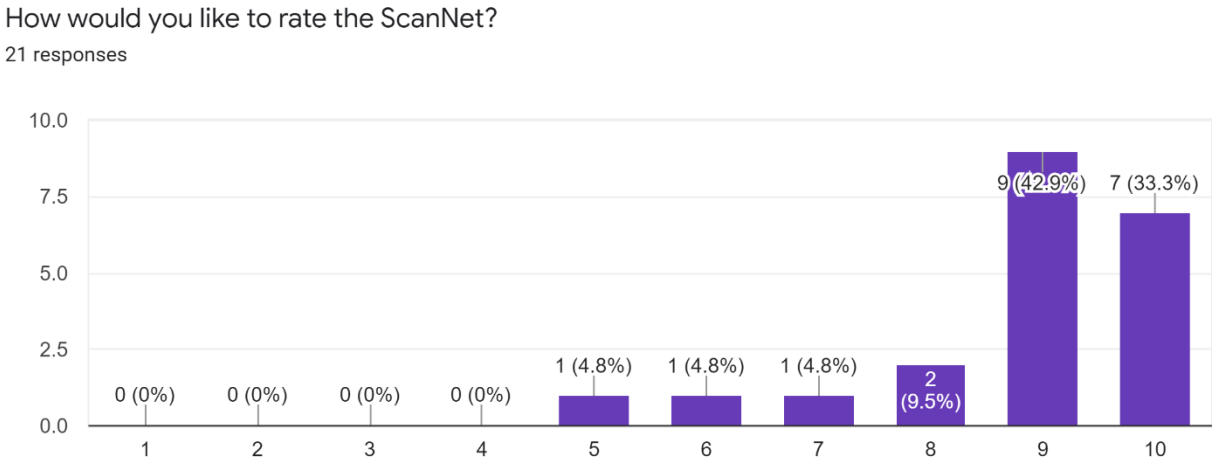


Figure 101 post-survey result figure 6

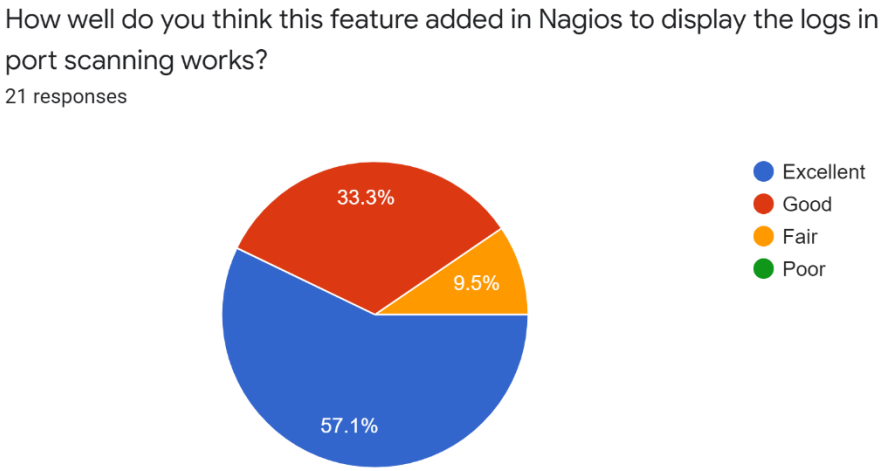


Figure 102 post-survey result figure 7

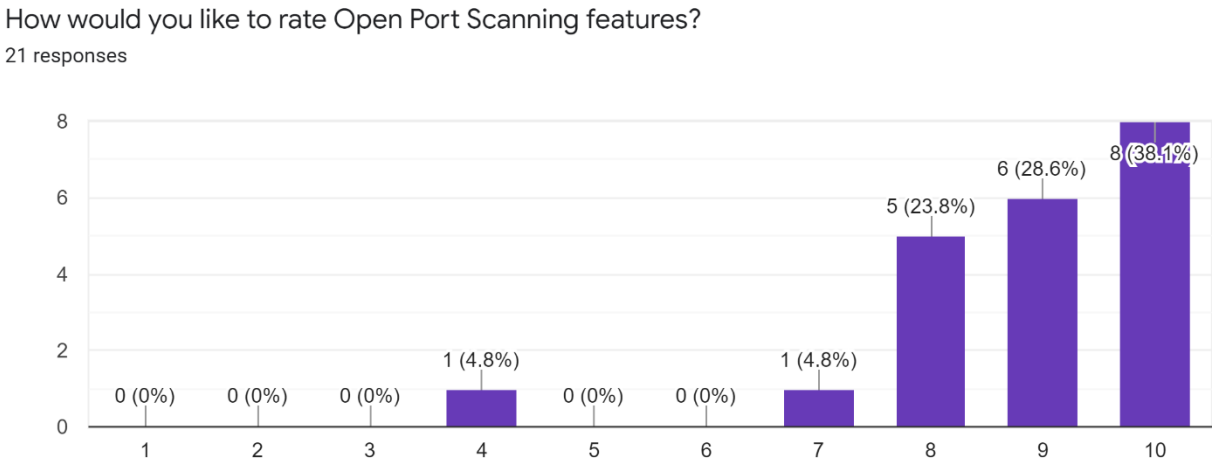


Figure 103 post-survey result figure 8

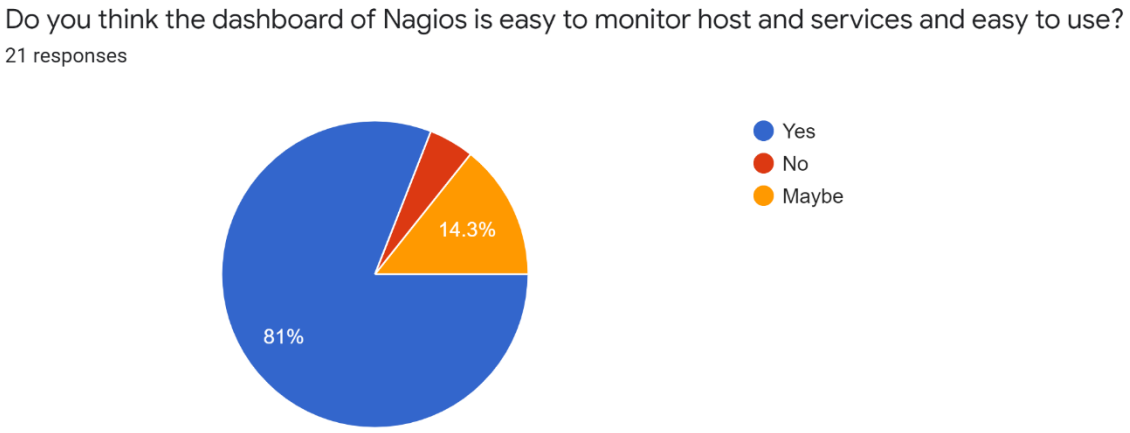


Figure 104 post-survey result figure 9

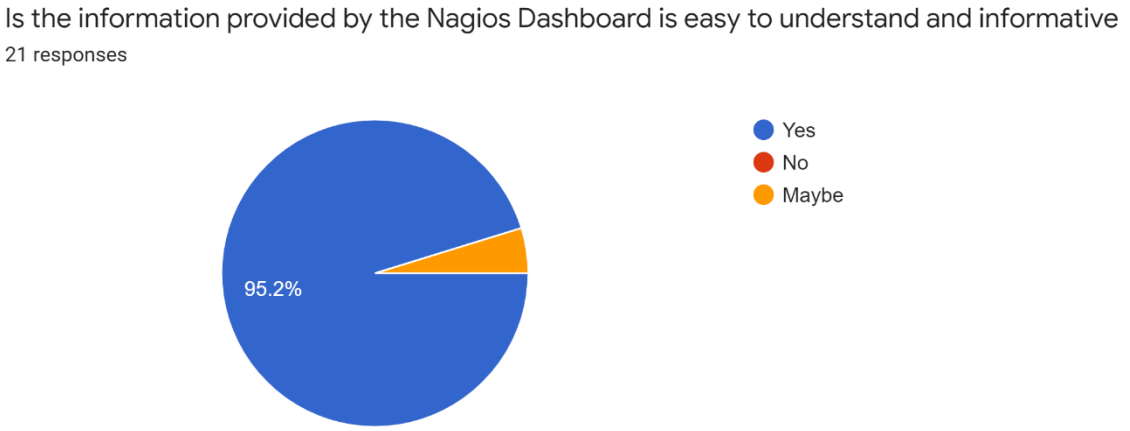


Figure 105 post-survey result figure 10

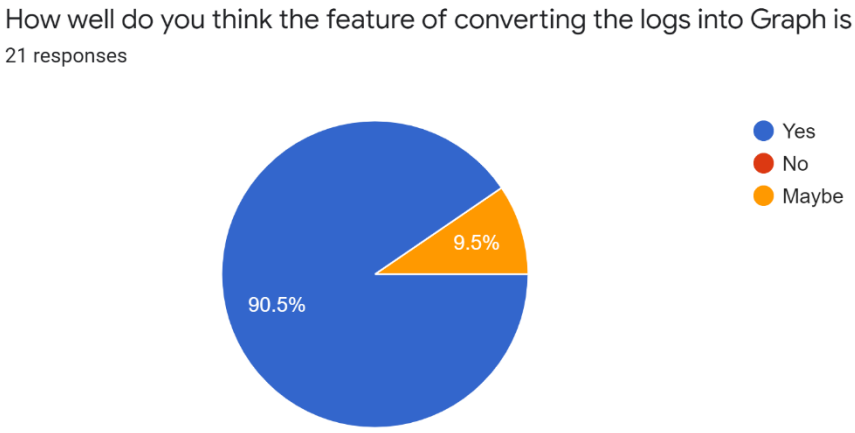


Figure 106 post-survey result figure 11

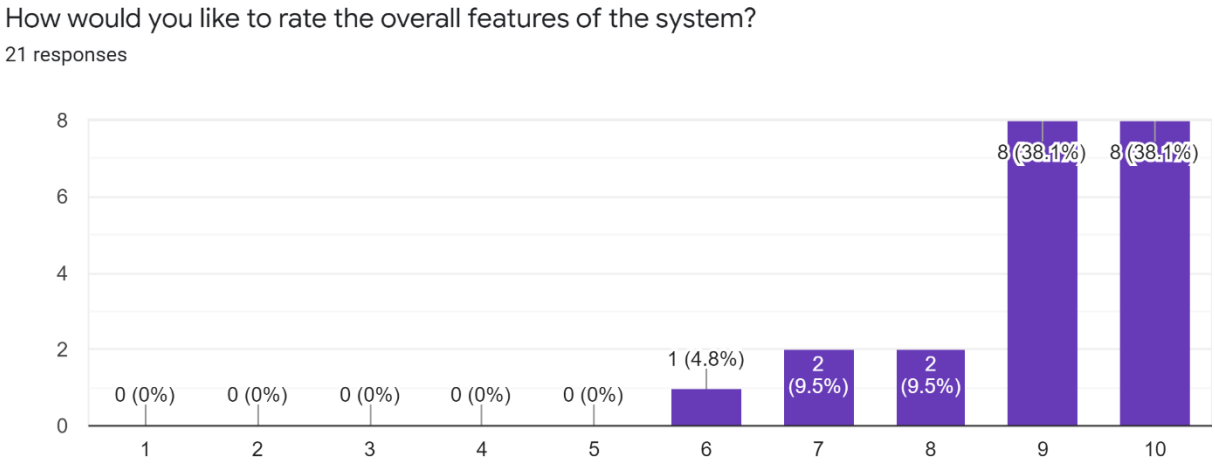


Figure 107 post-survey result figure 12

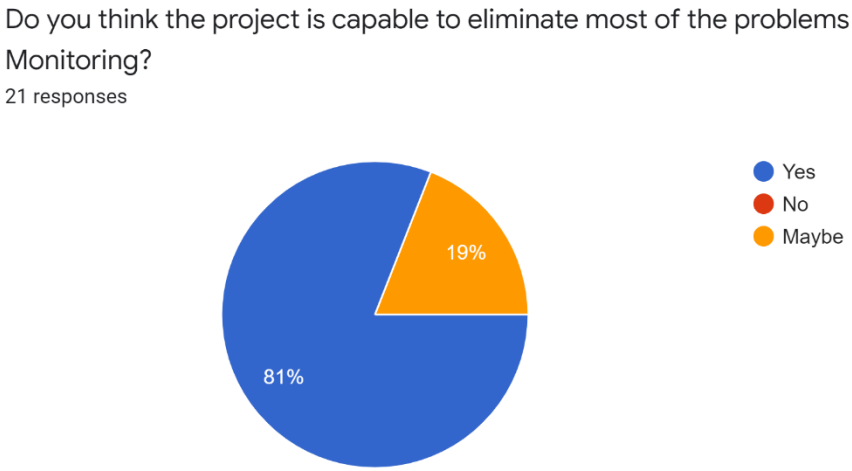


Figure 108 post-survey result figure 13

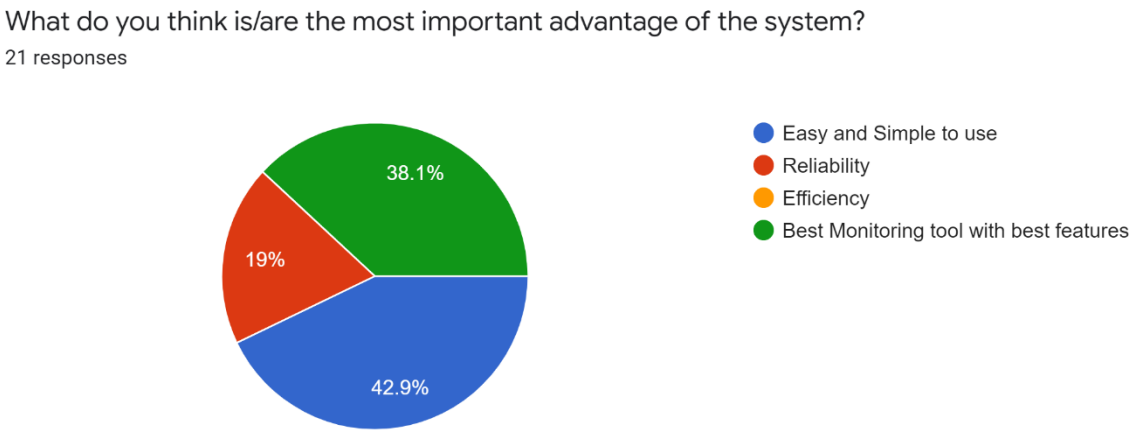


Figure 109 post-survey result figure 14

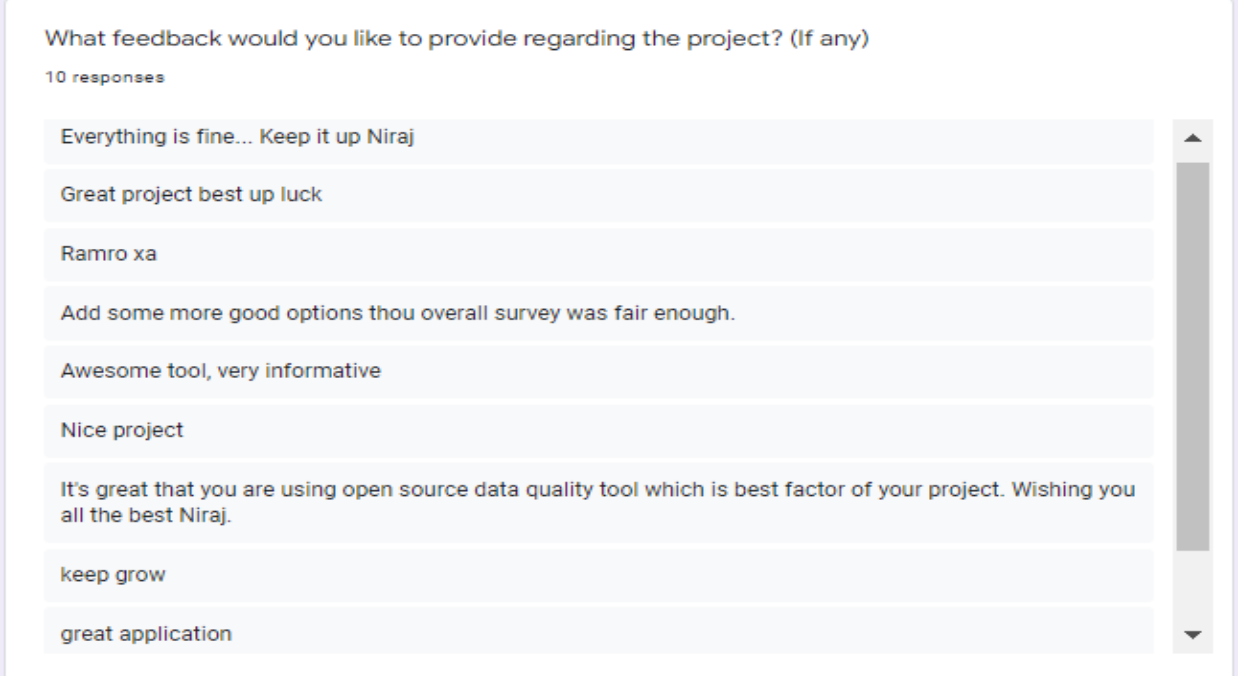


Figure 110 post-survey result figure 15

8.3. Appendix C: Resource Requirements

8.3.1. Hardware

Although no specific hardware is required for the development of this project, it will require a laptop or desktop computer to install and setup software as well as to document the essential project information. Designing the dashboard and conducting research are also essential. It is necessary to have a computer with sufficient RAM, storage, processor, and a decent internet connection.

8.3.2. Software

Oracle VM Virtual box	Oracle VM Virtual box is used to install different Linux machines and windows machines in it.
CentOS	CentOS is a Linux machine that is installed inside the Virtual box.
Putty	Putty is used to do telnet, SSH to remote devices.
Nagios Core	Nagios Core is a network monitoring tool which uses SNMP protocol and can be used to monitor different network devices and also used to visualize all the data and logs inside its dashboard
WinSCP	WinSCP is used to change different

	information through telnet or SSH like photos.
NSClient++	Allow a distant machine (the monitoring server) to send instructions to this machine (the monitored machine) that report the machine's status. Send the same findings to a distant location (monitoring server).
GNS3	GNS3 is a tool which supports all the cisco devices and helps in configuring the devices in real-time. GNS allows us to run a small and a big topology which allows us to host multiple servers, router, and switches
NMAP	NMAP is a tool or an open-source tool which helps us to scan all the open ports in a network.
PNP4Nagios	PNP4Nagios is a Nagios add-on that analyses and stores performance data from plugins in RRD-databases (Round Robin Databases, see RRD Tool).
check_scan.sh	This code is written in Perl Programming Language which is used to display all the

	open ports in a network which is displayed after performing a Nmap scan.
XAMPP	XAMPP's mission is to create an easy-to-install Apache distribution for developers. XAMPP is set up with all features switched on to make it easier for developers to use.

Table 22 Software Requirements

8.3.2.1. Screenshots of Oracle VM Virtual box

Figure 111 Installation Process of Oracle VM Virtual box 1

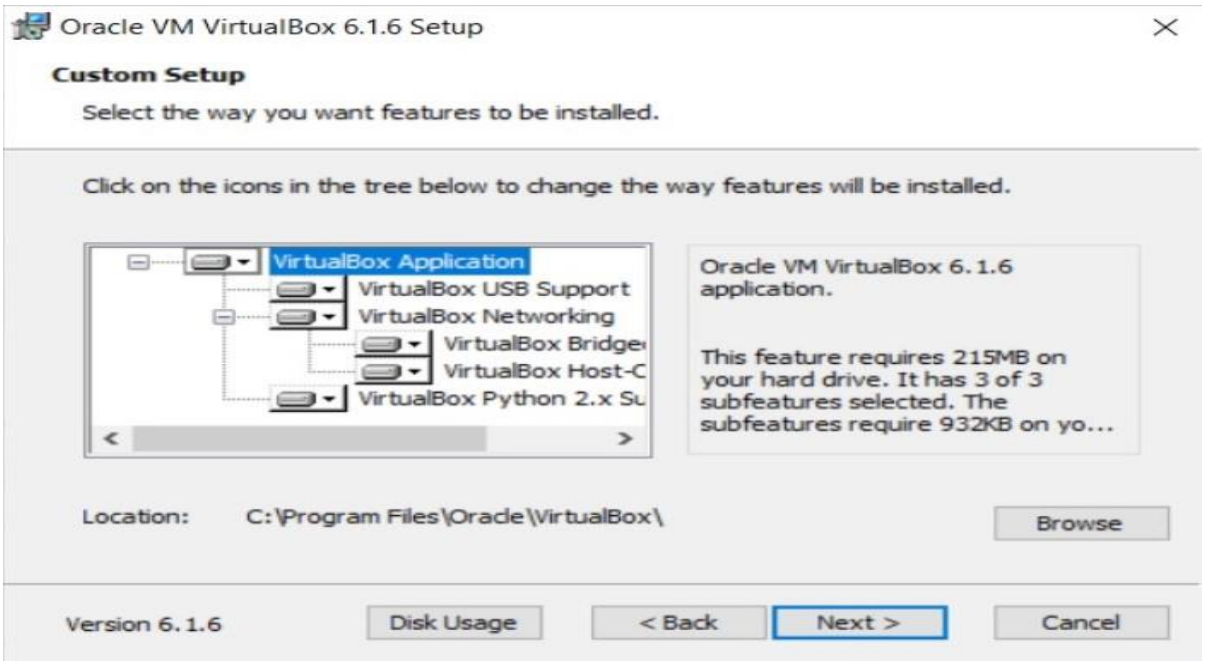


Figure 112 Installation Process of Oracle VM Virtual box 2

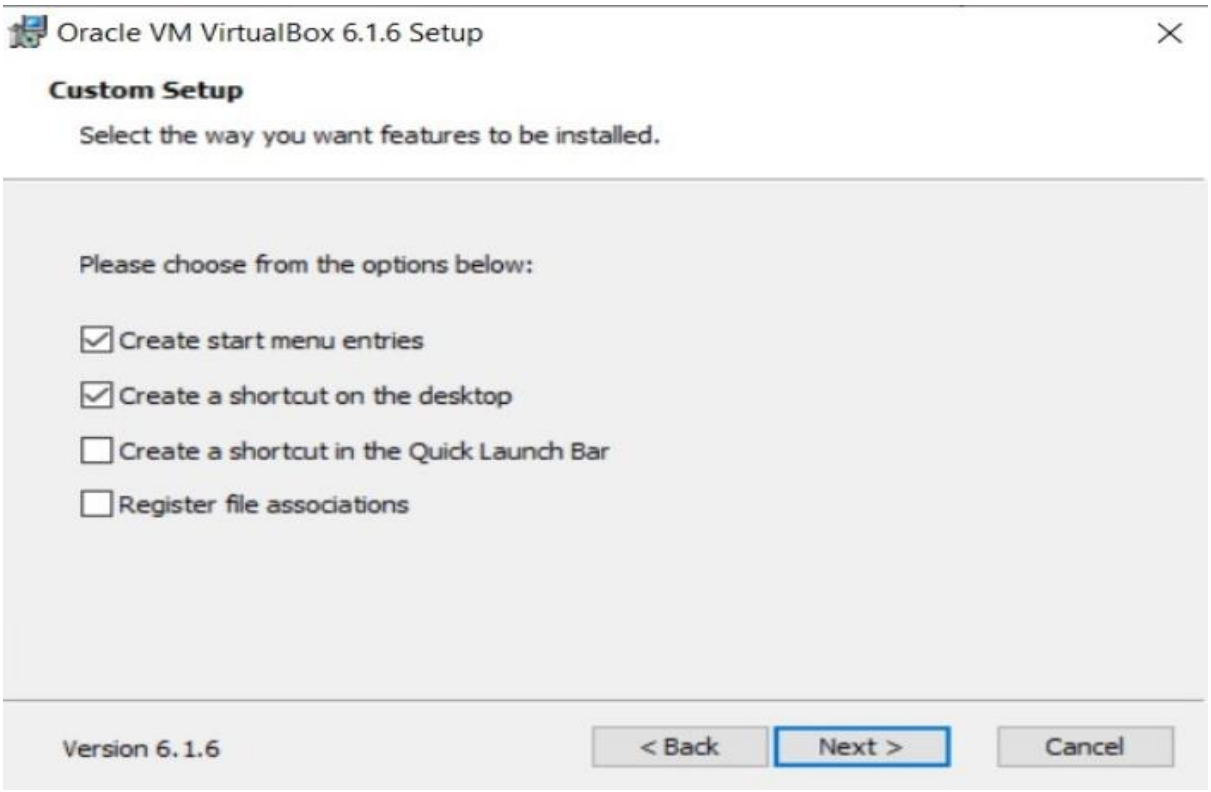


Figure 113 Installation Process of Oracle VM Virtual box 3

Figure 114 Installation Process of Oracle VM Virtual box 4

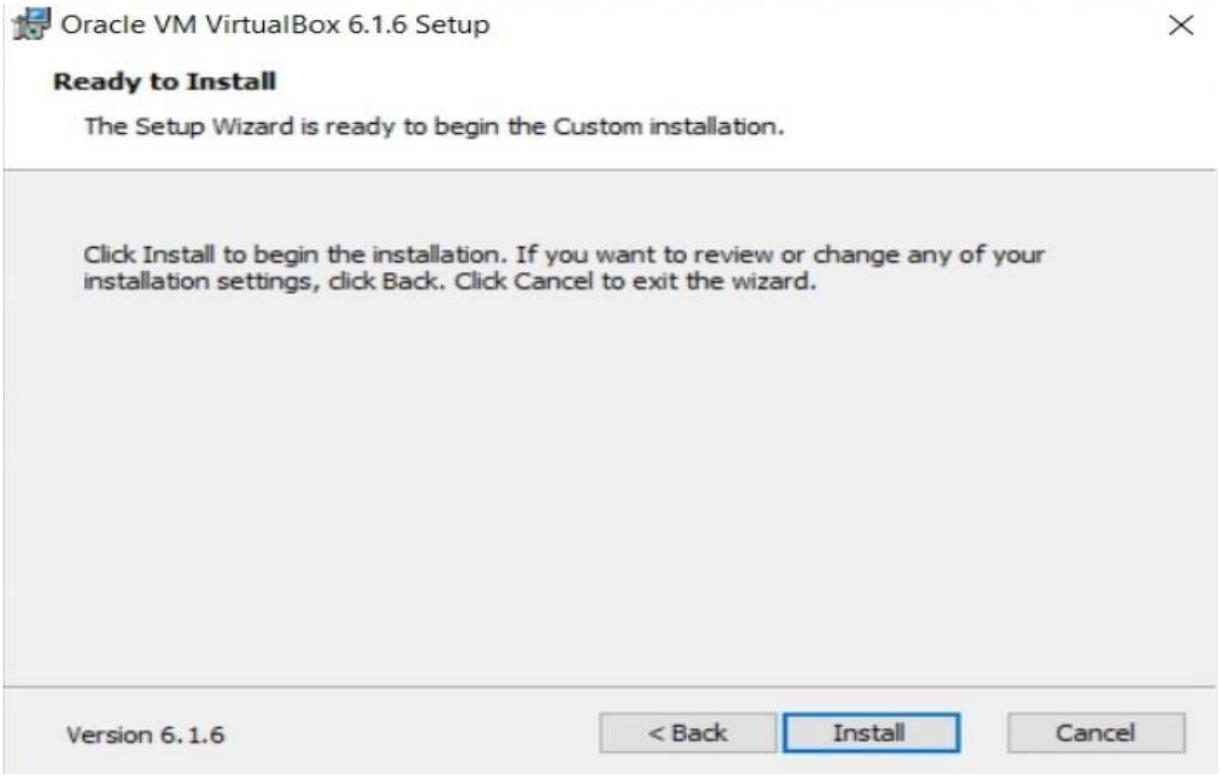


Figure 115 Installation Process of Oracle VM Virtual box 5

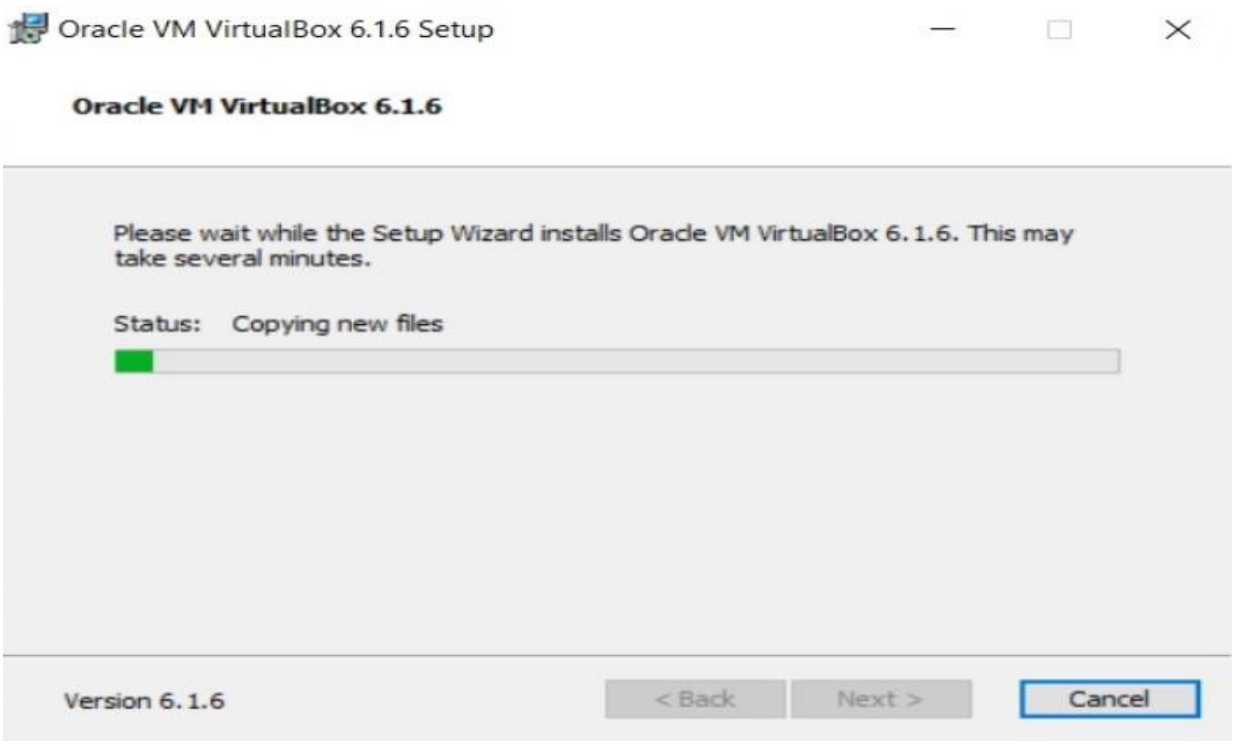


Figure 116 Installation Process of Oracle VM Virtual box 6

Figure 117 Installation Process of Oracle VM Virtual box 7

8.3.2.2. Screenshots of CentOS

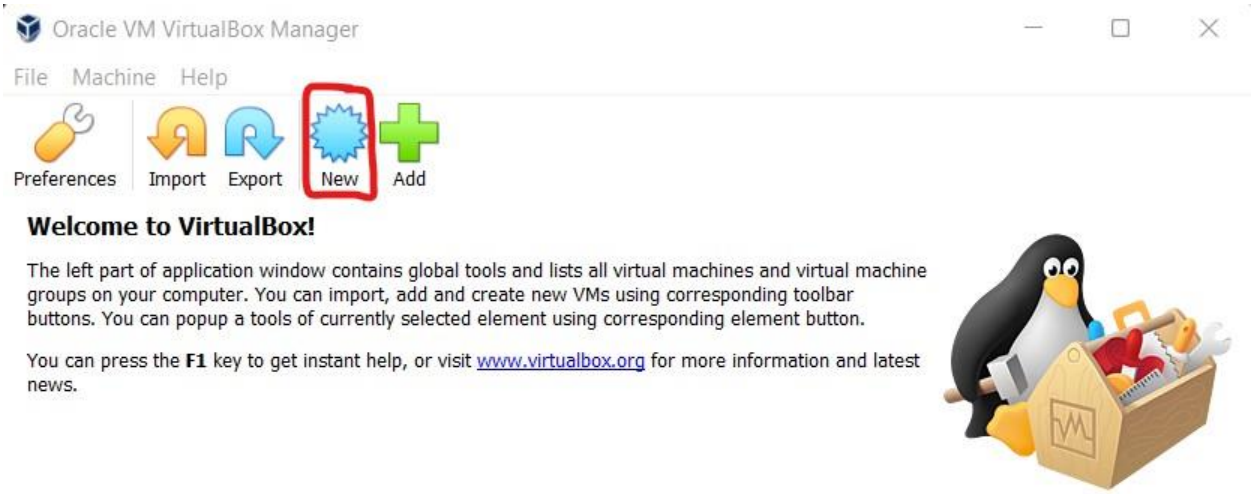


Figure 118 Installation Process of CentOS7 1

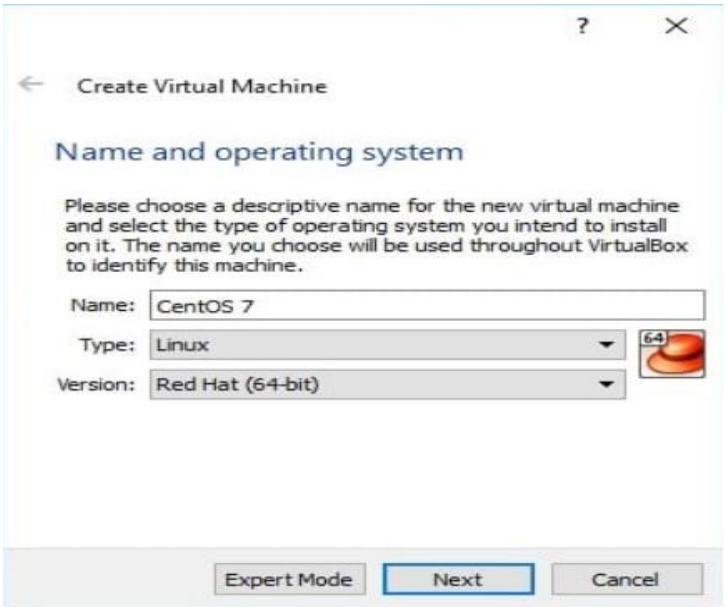


Figure 119 Installation Process of CentOS7 2

Figure 120 Installation Process of CentOS7 3

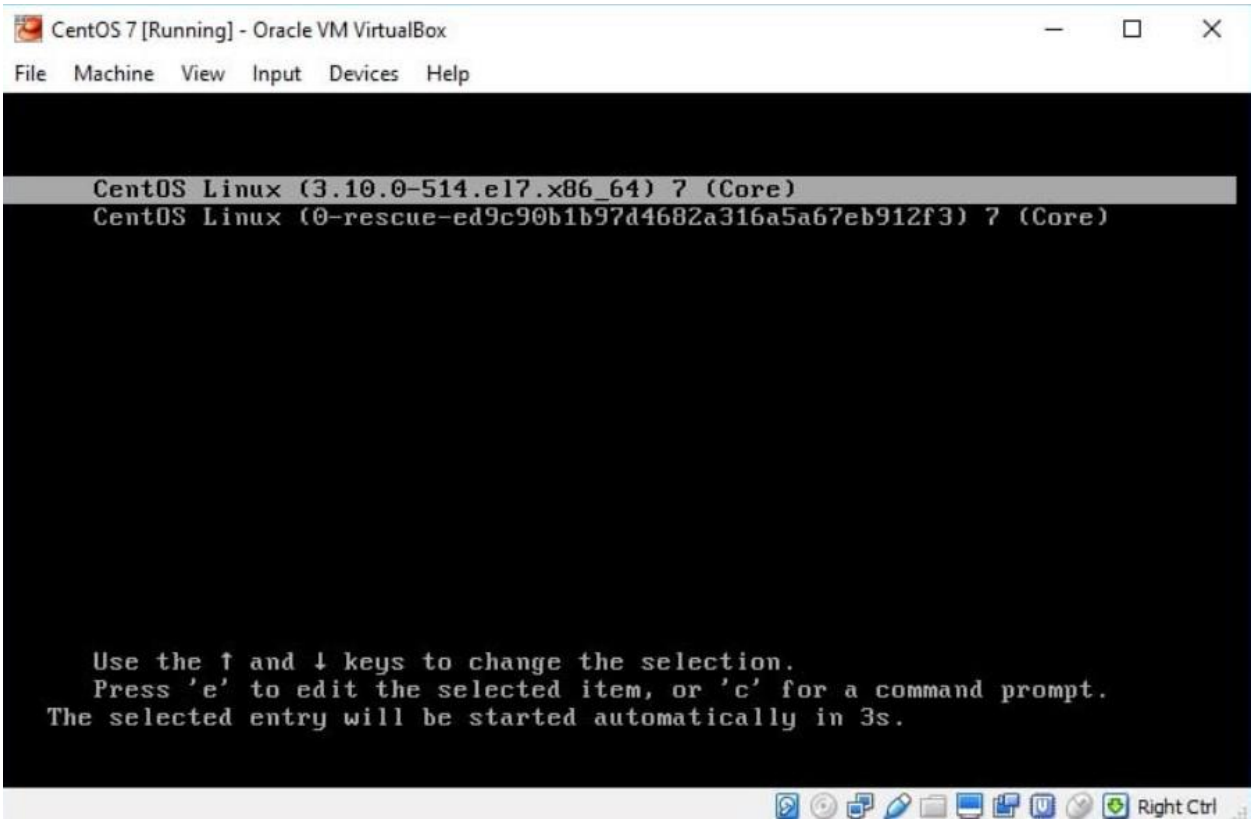


Figure 121 Starting Process of CentOS7 1

Figure 122 Starting Process of CentOS7 2

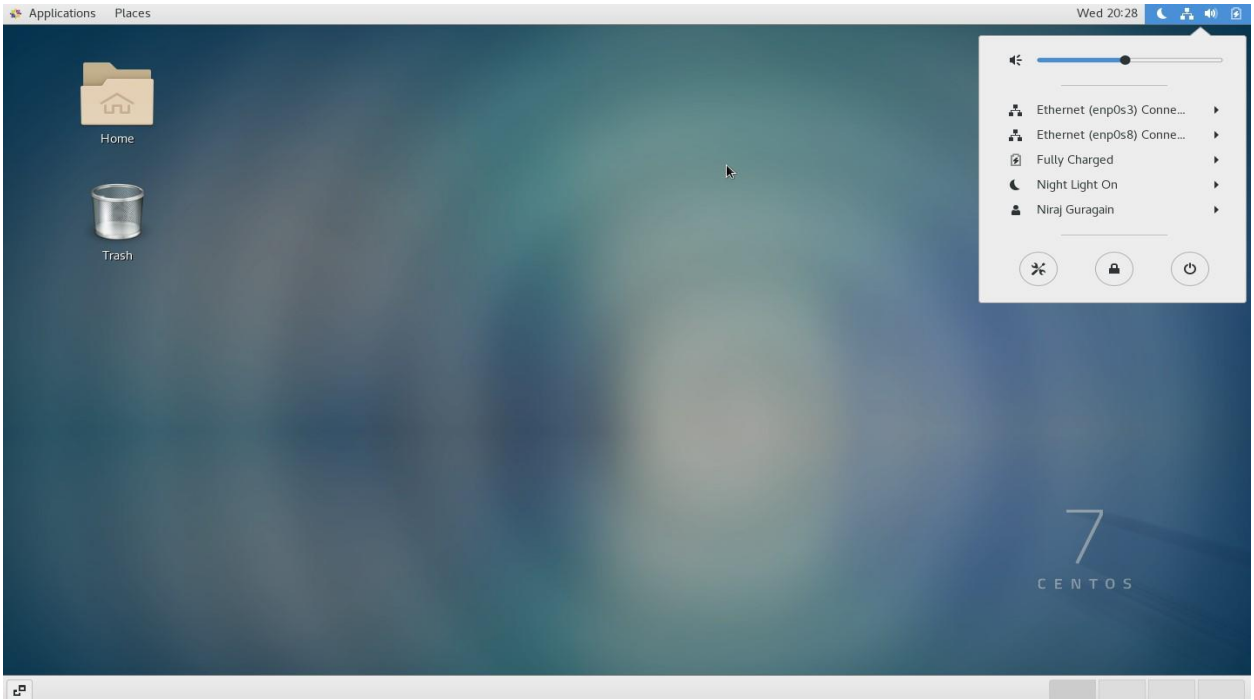


Figure 123 Starting Process of CentOS7 3

8.3.2.3. Screenshots of Putty

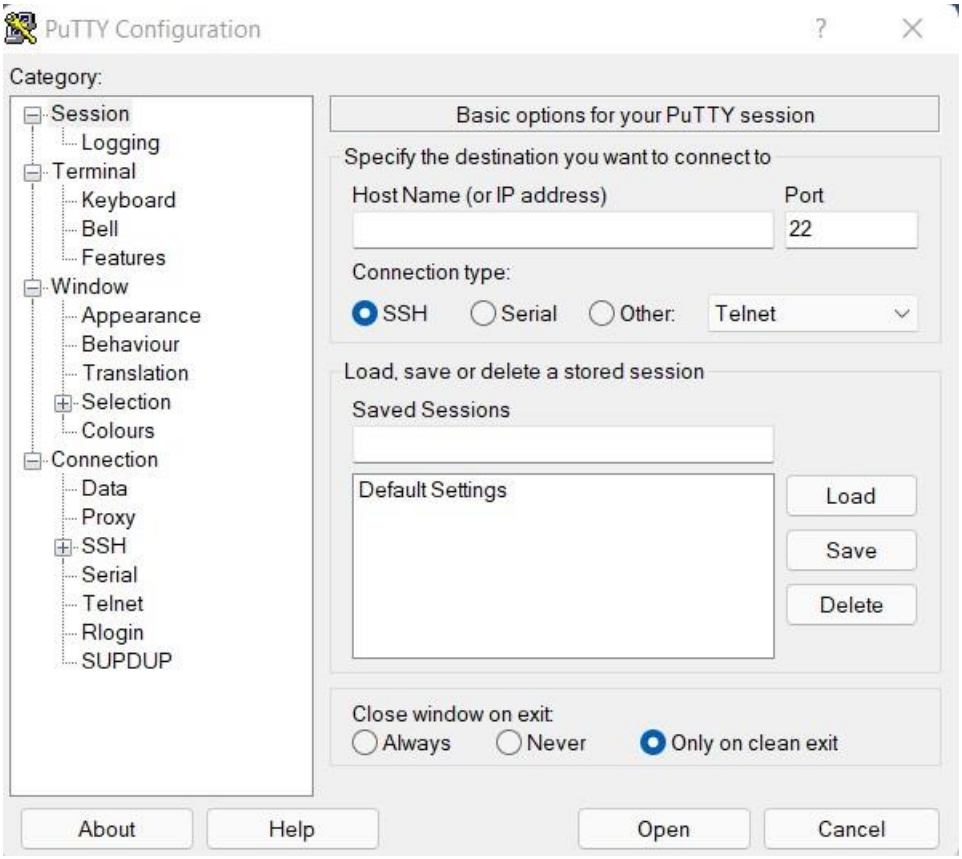


Figure 124 Putty

8.3.2.4. Screenshots of Nagios Core

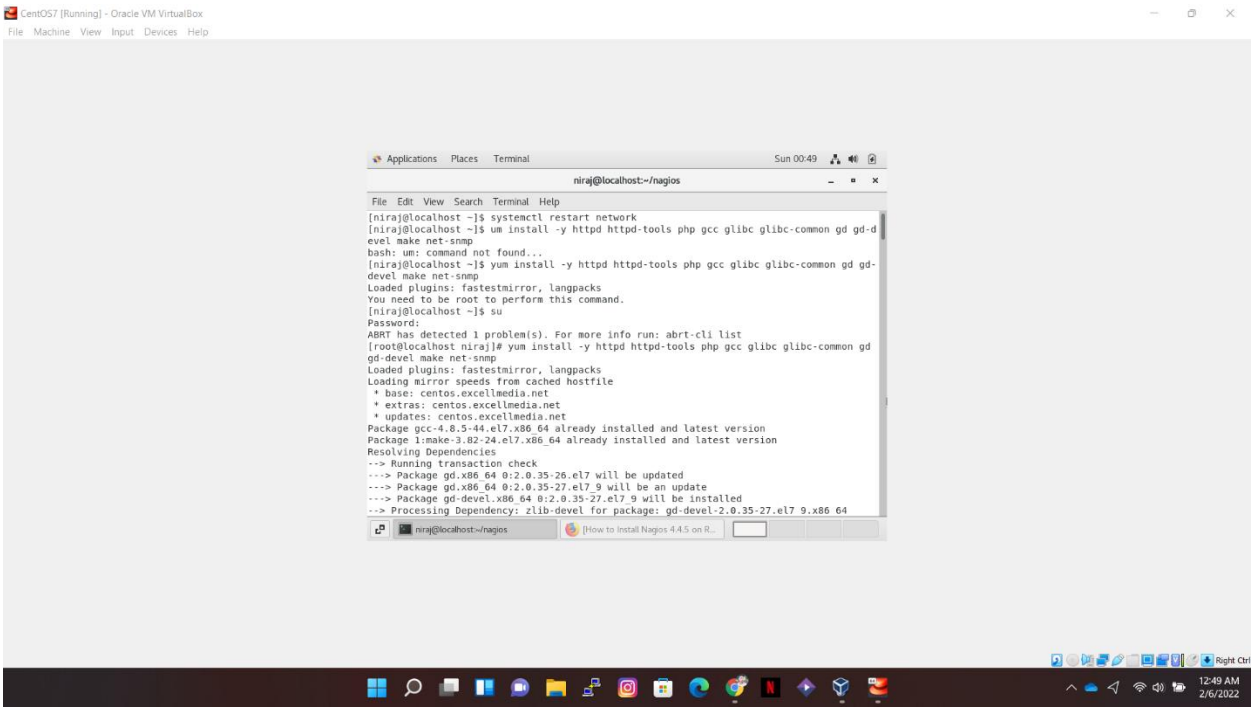


Figure 125 Installing Nagios Core on CentOS Process 1

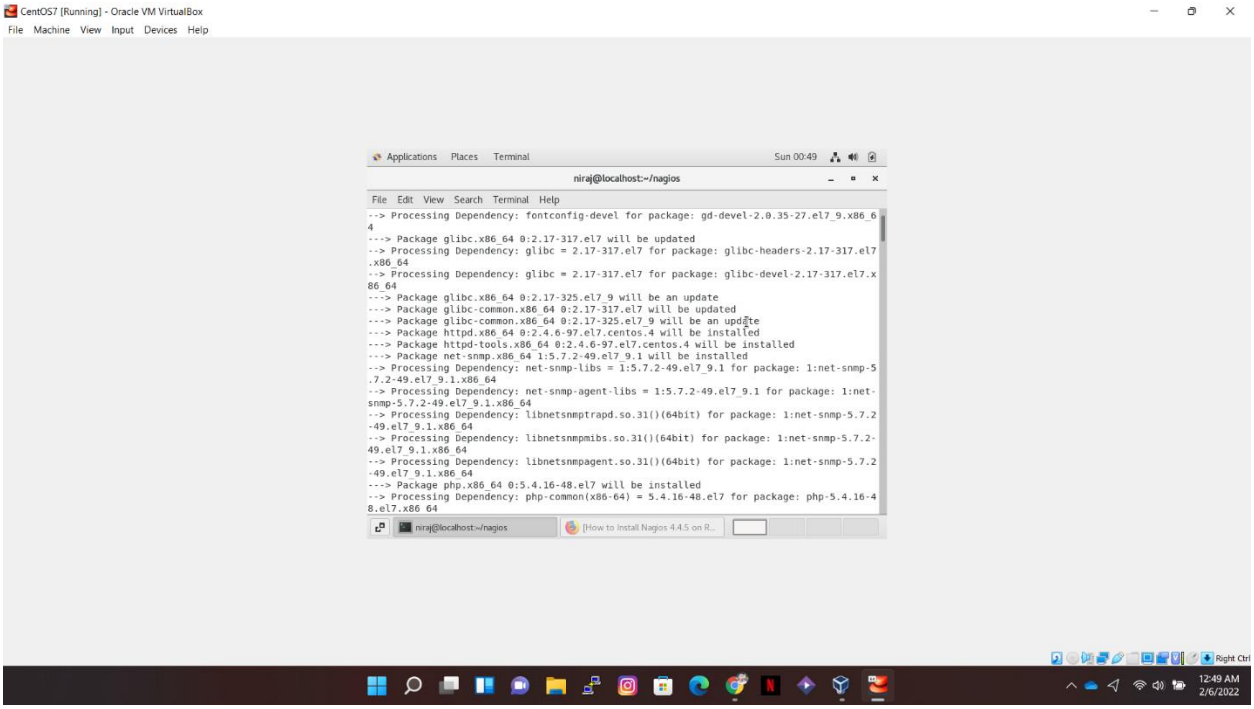


Figure 126 Installing Nagios Core on CentOS Process 2

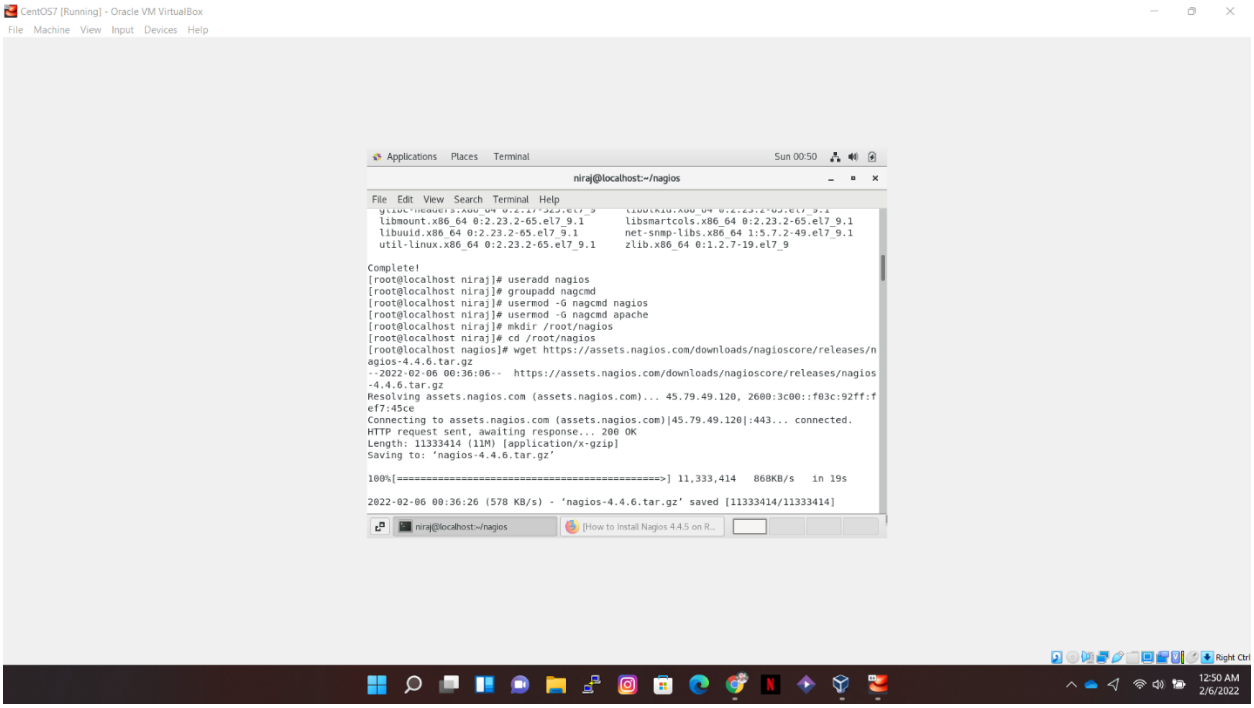


Figure 127 Installing Nagios Core on CentOS Process 3

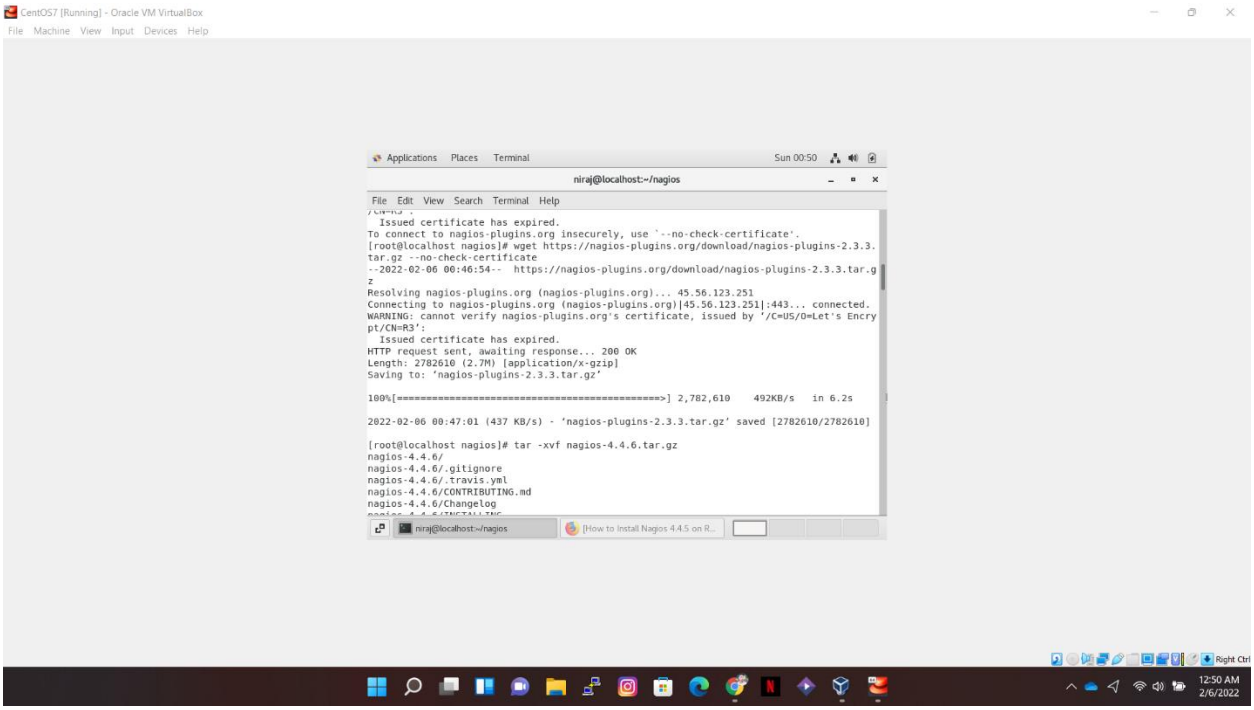


Figure 128 Installing Nagios Core on CentOS Process 4

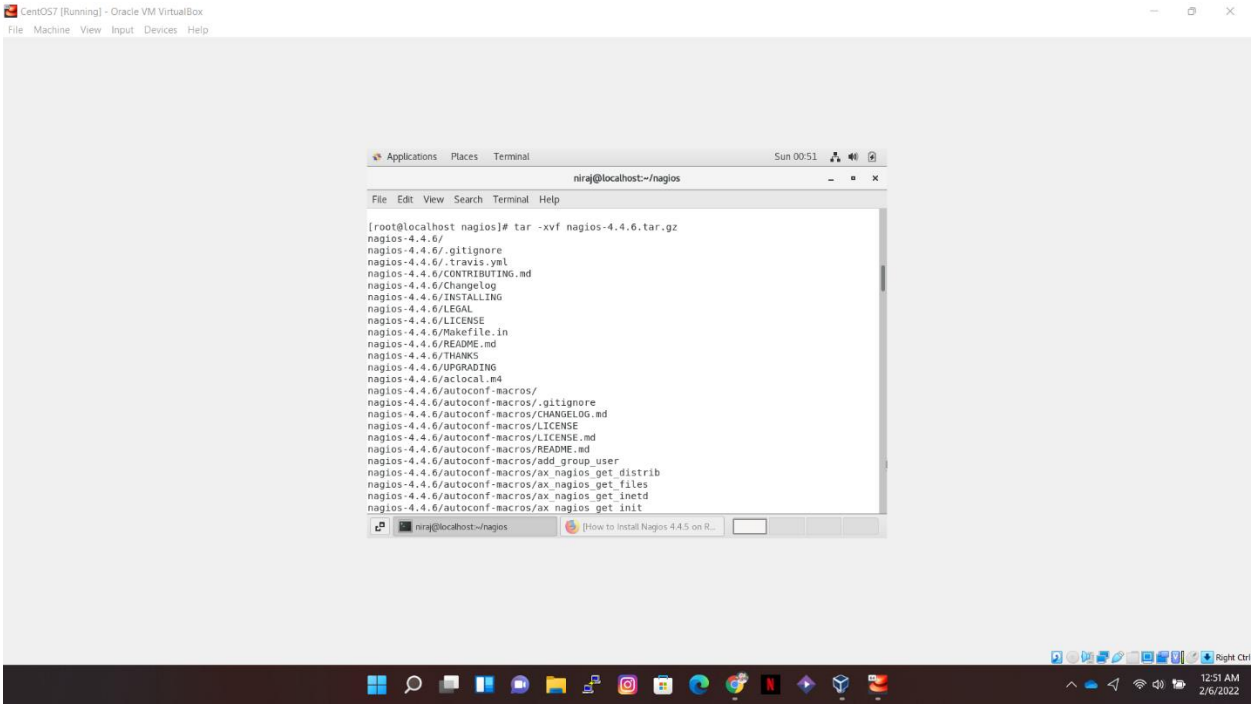


Figure 129 Installing Nagios Core on CentOS Process 5

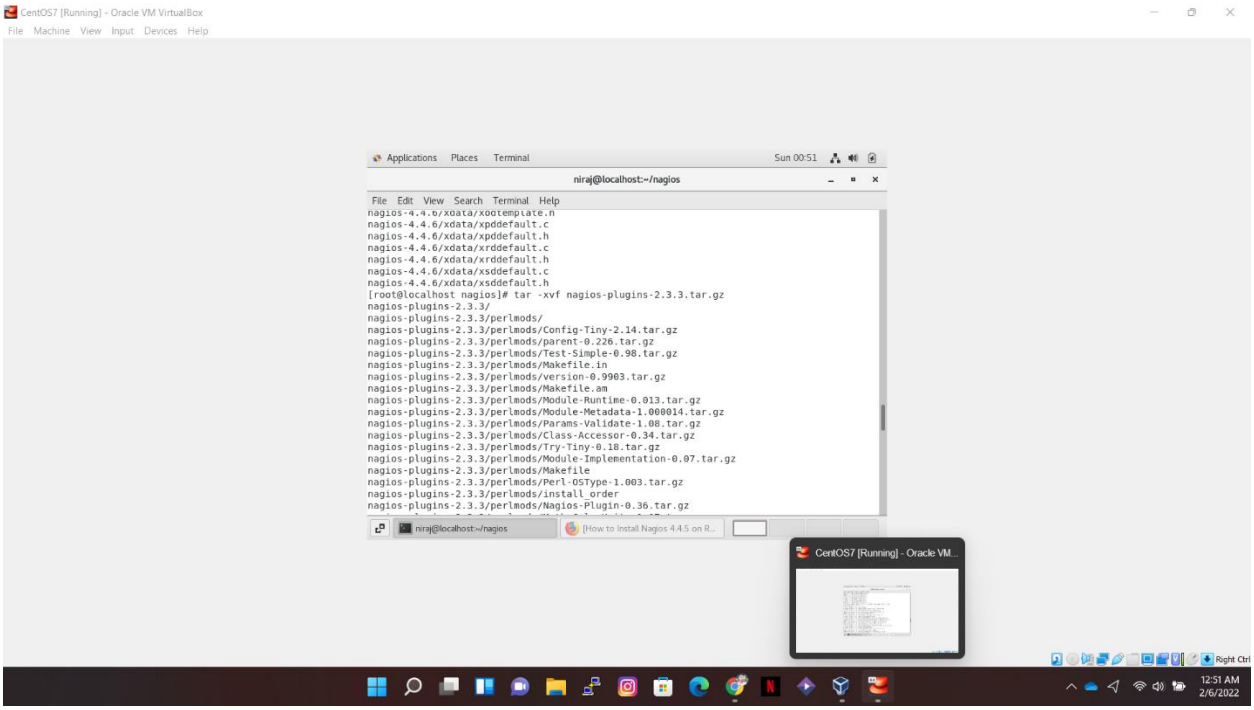


Figure 130 Installing Nagios Core on CentOS Process 6

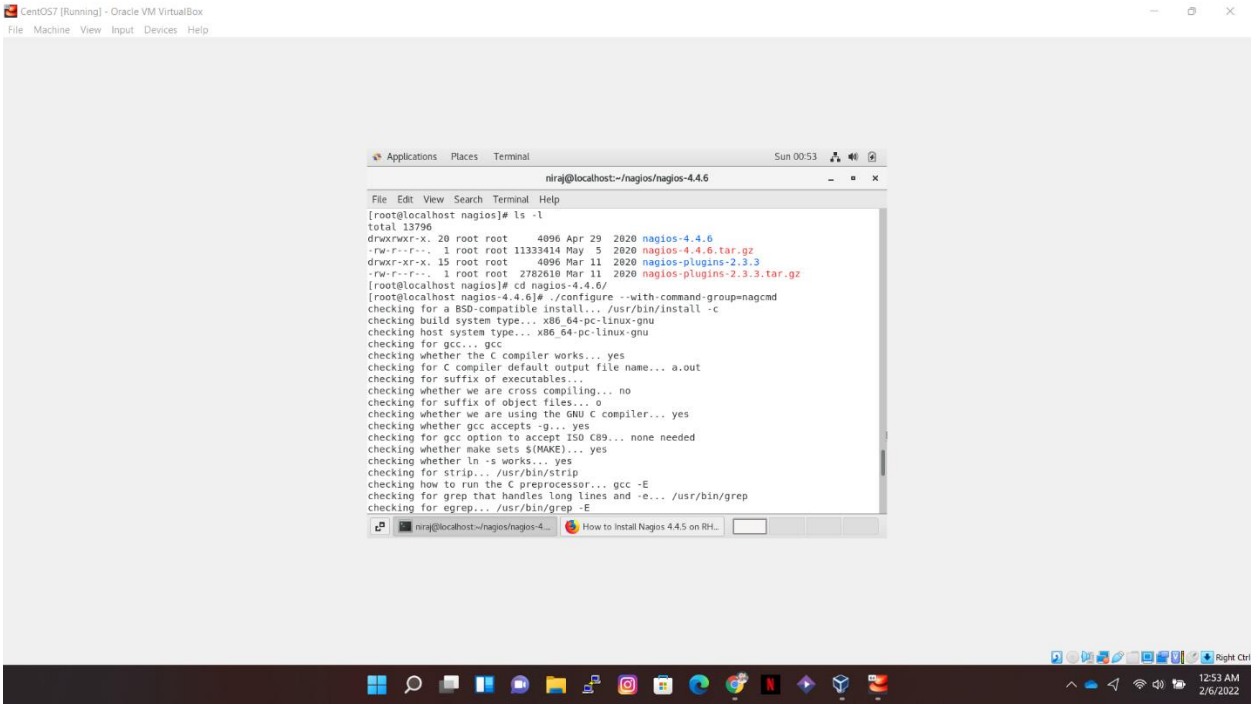


Figure 131 Installing Nagios Core on CentOS Process 7

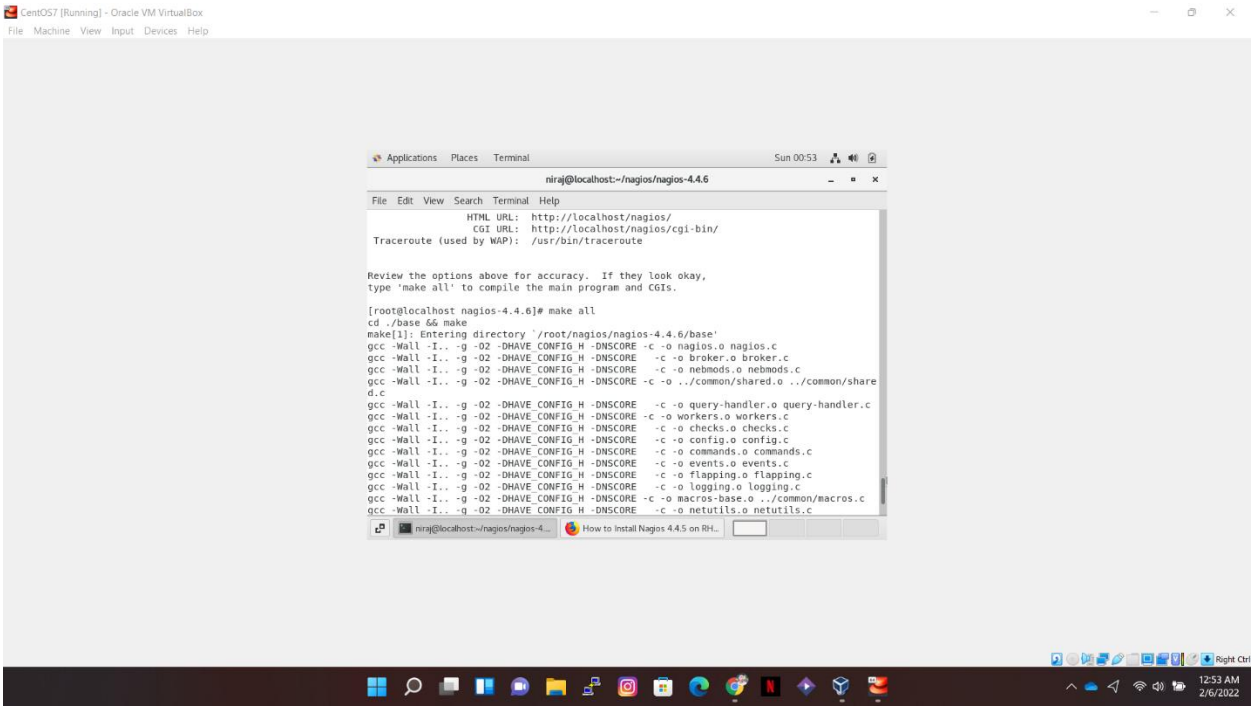


Figure 132 Installing Nagios Core on CentOS Process 8

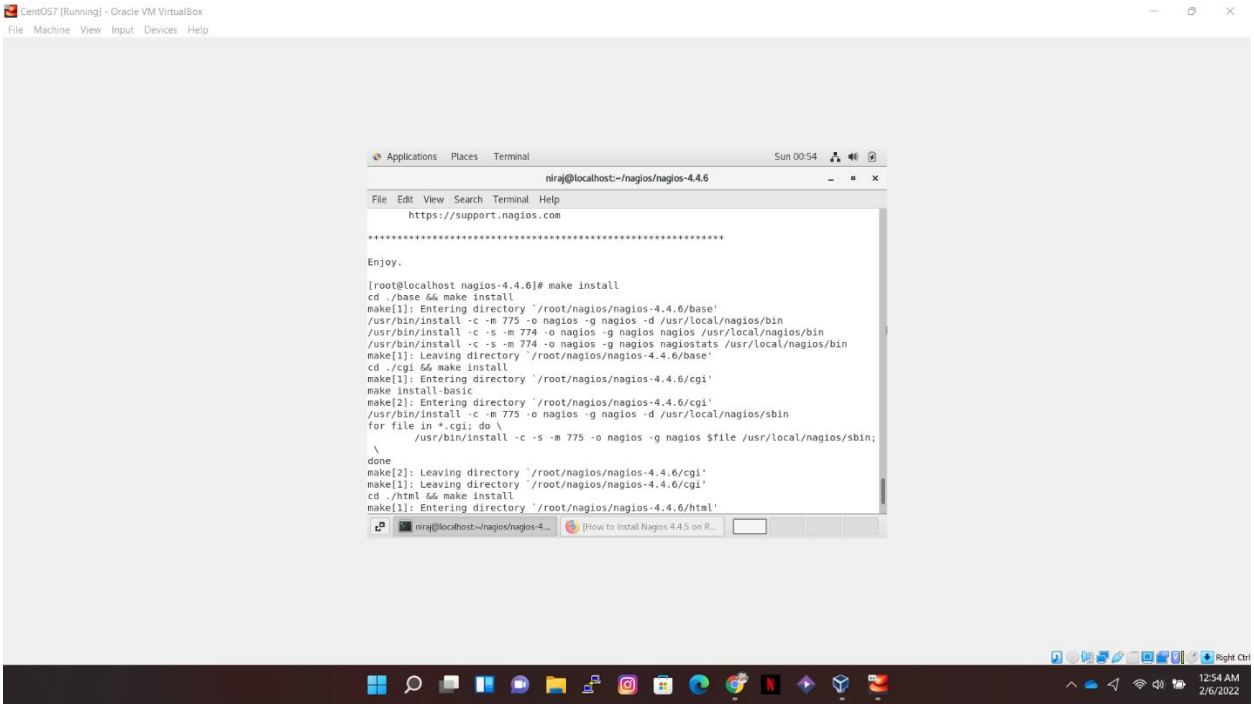


Figure 133 Installing Nagios Core on CentOS Process 9

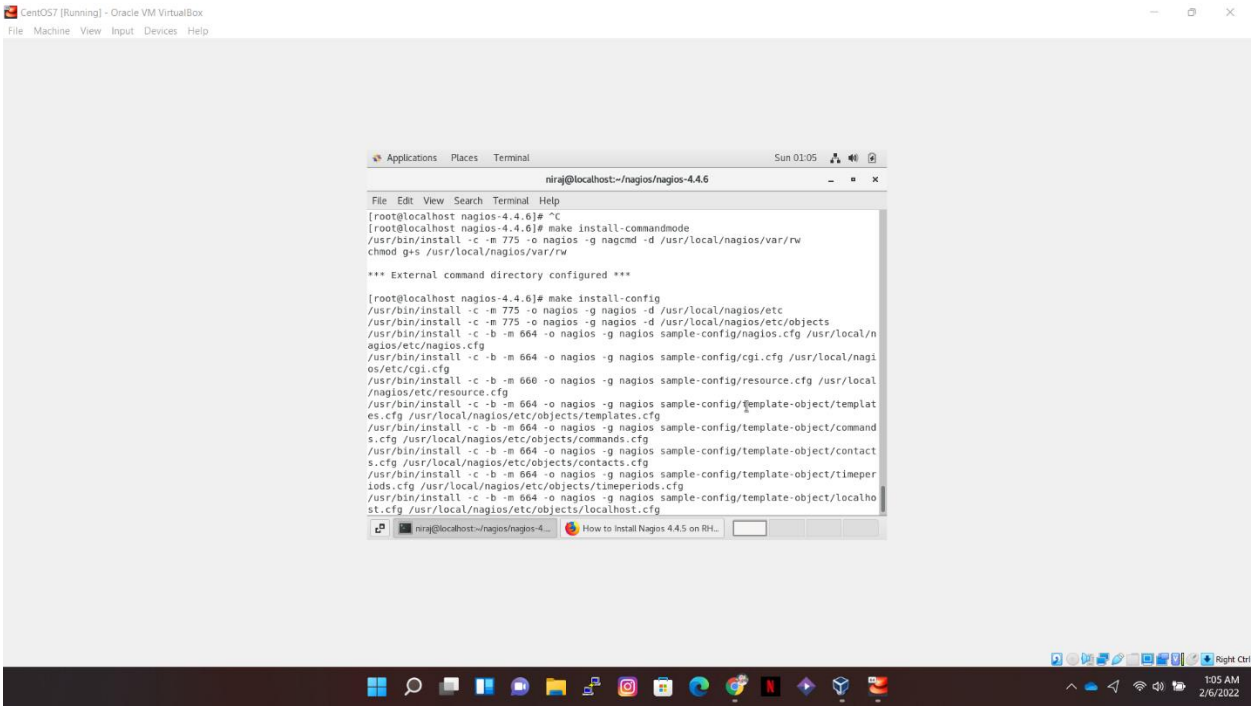


Figure 134 Installing Nagios Core on CentOS Process 10

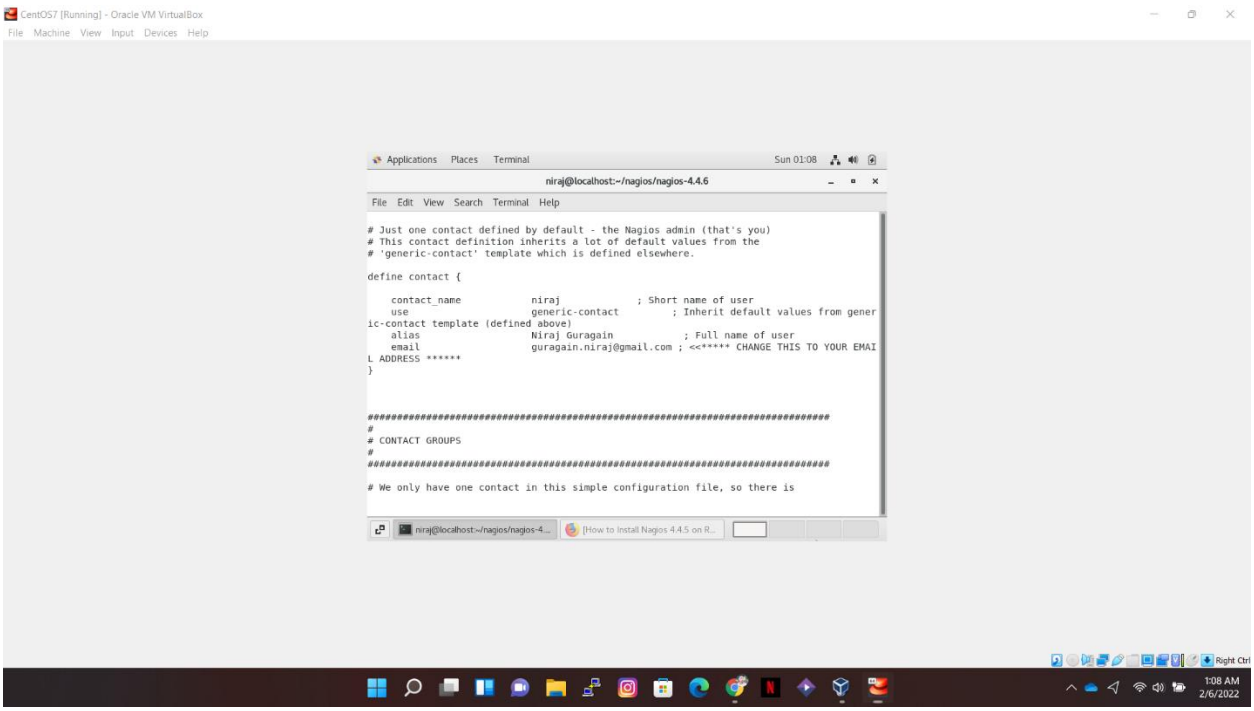


Figure 135 Installing Nagios Core on CentOS Process 11

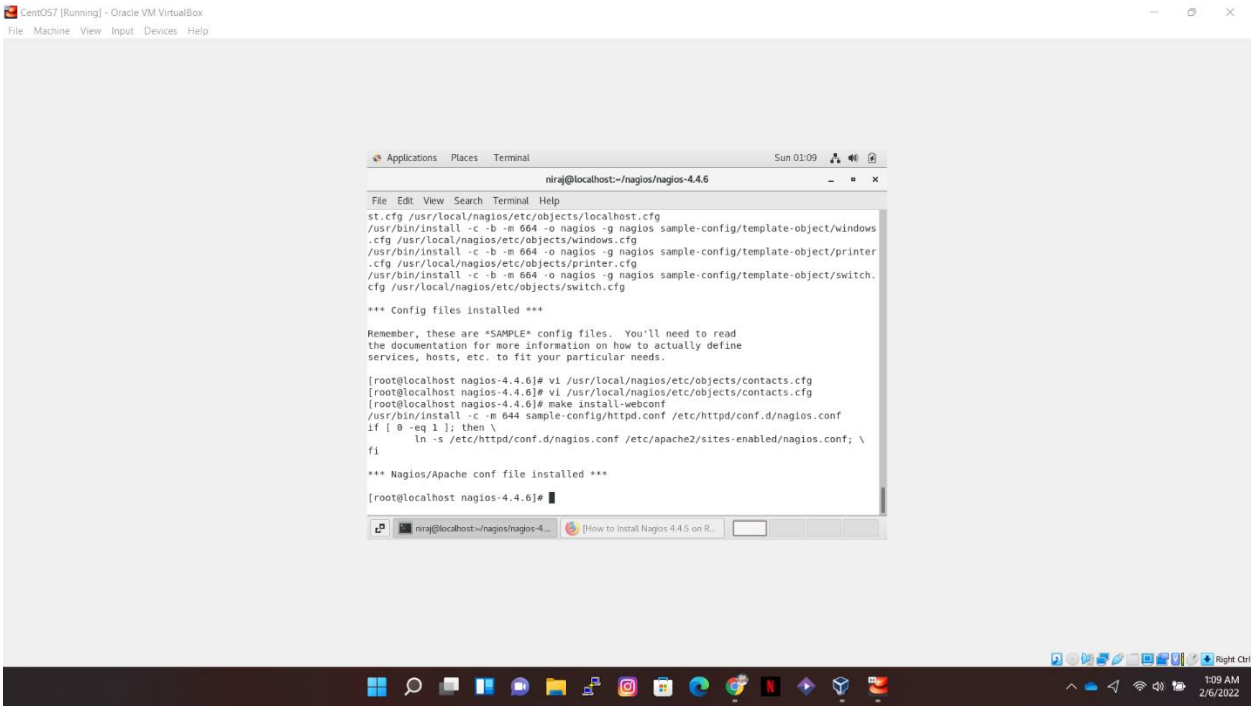


Figure 136 Installing Nagios Core on CentOS Process 12

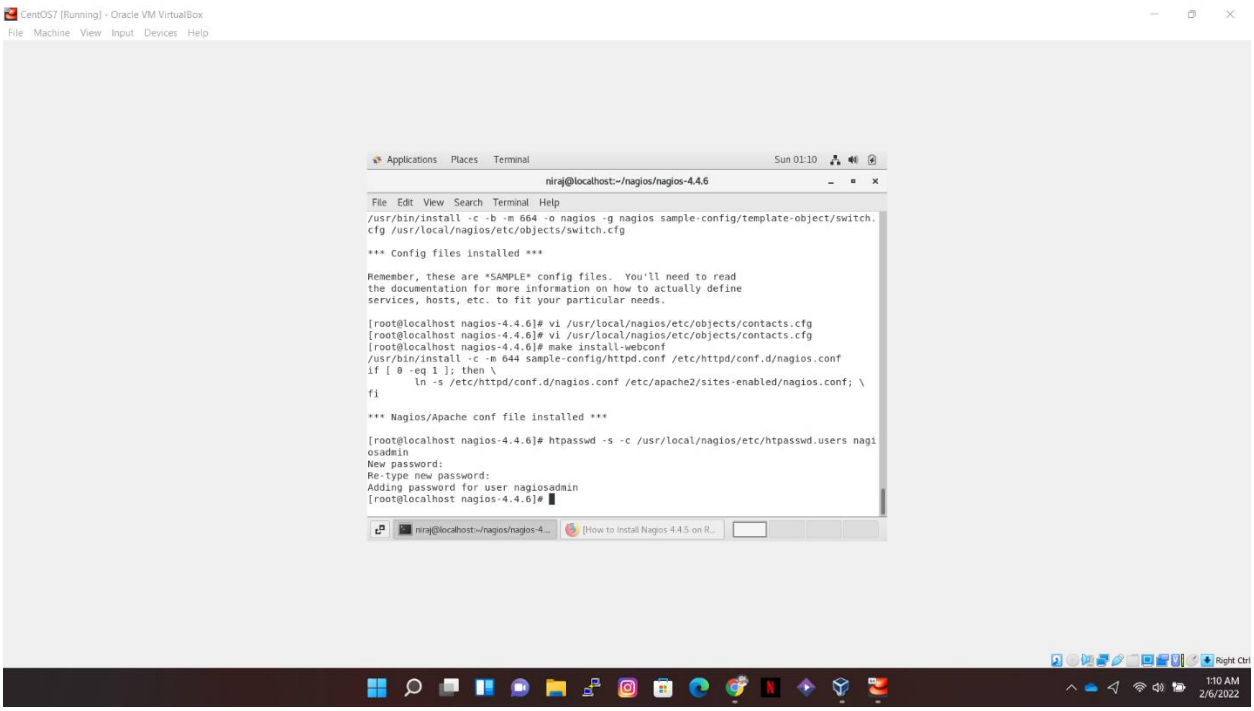


Figure 137 Installing Nagios Core on CentOS Process 13

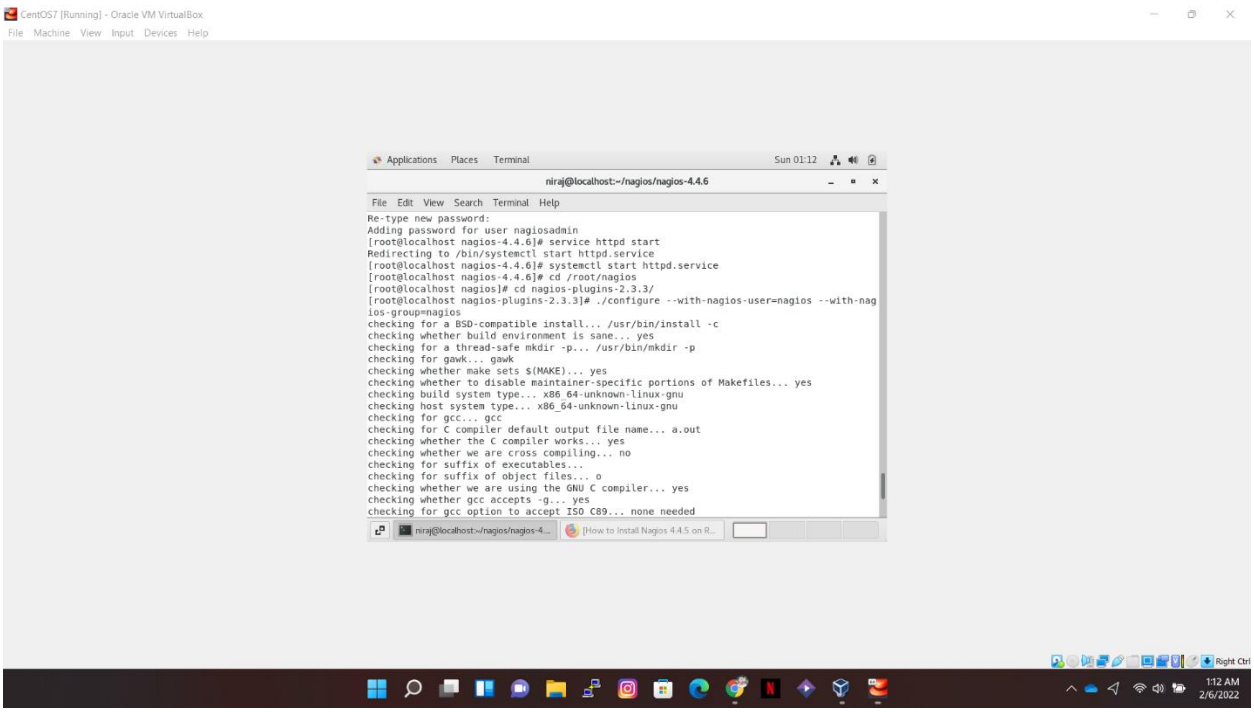


Figure 138 Installing Nagios Core on CentOS Process 14

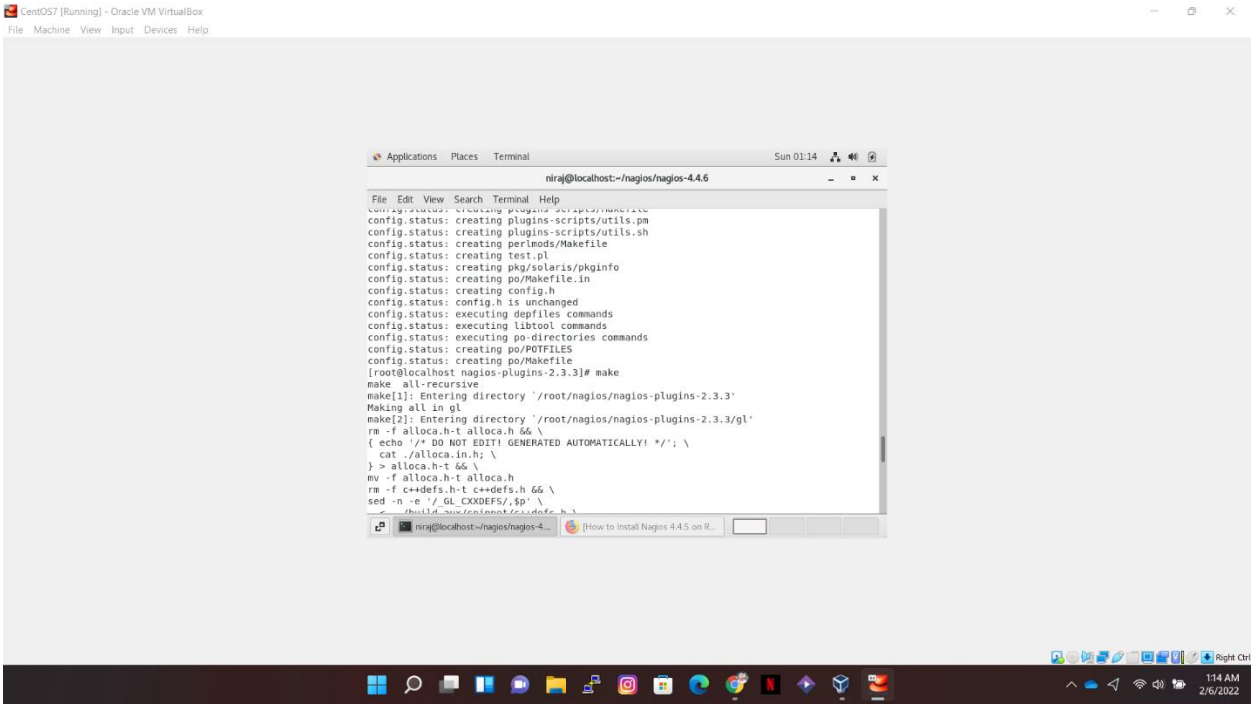


Figure 139 Installing Nagios Core on CentOS Process 15

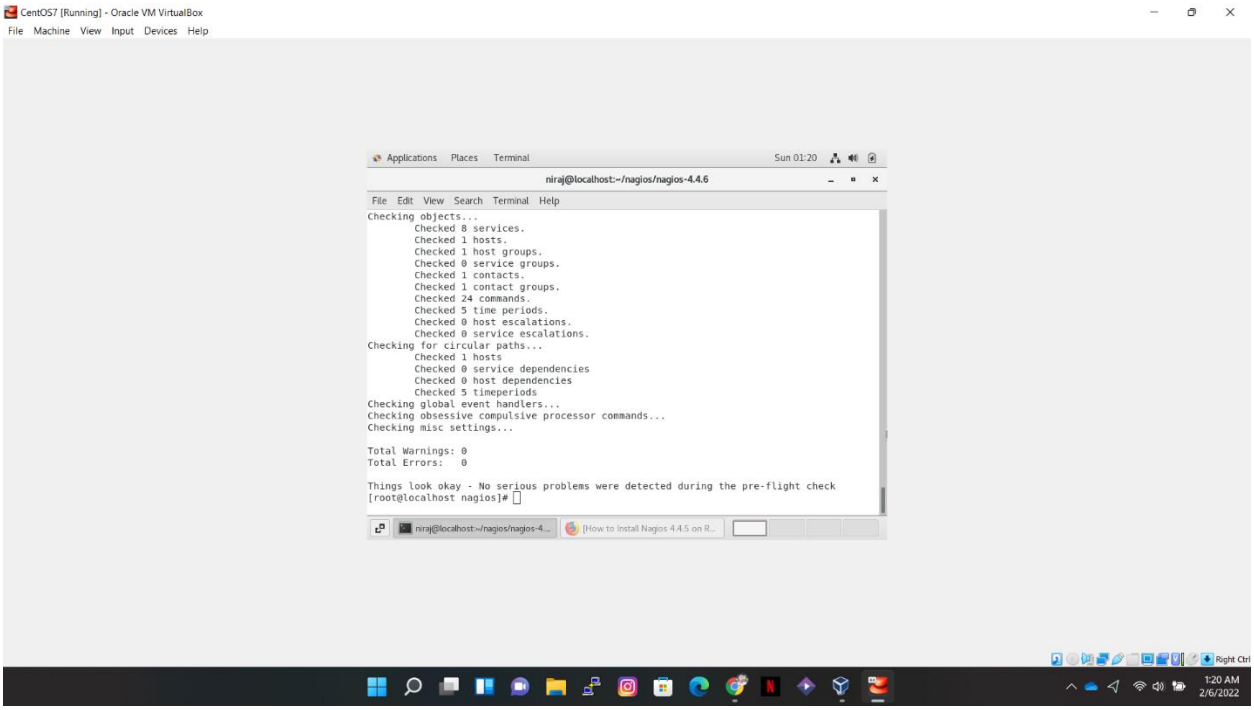


Figure 140 Installing Nagios Core on CentOS Process 16

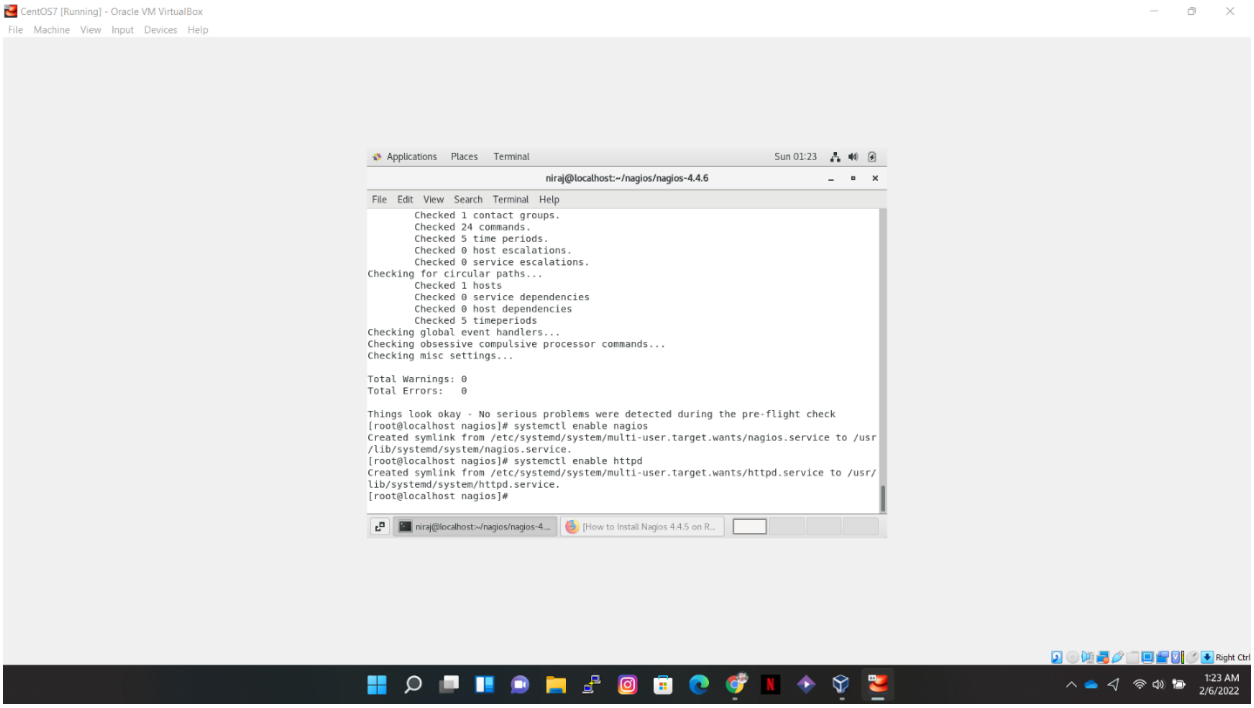


Figure 141 Installing Nagios Core on CentOS Process 17

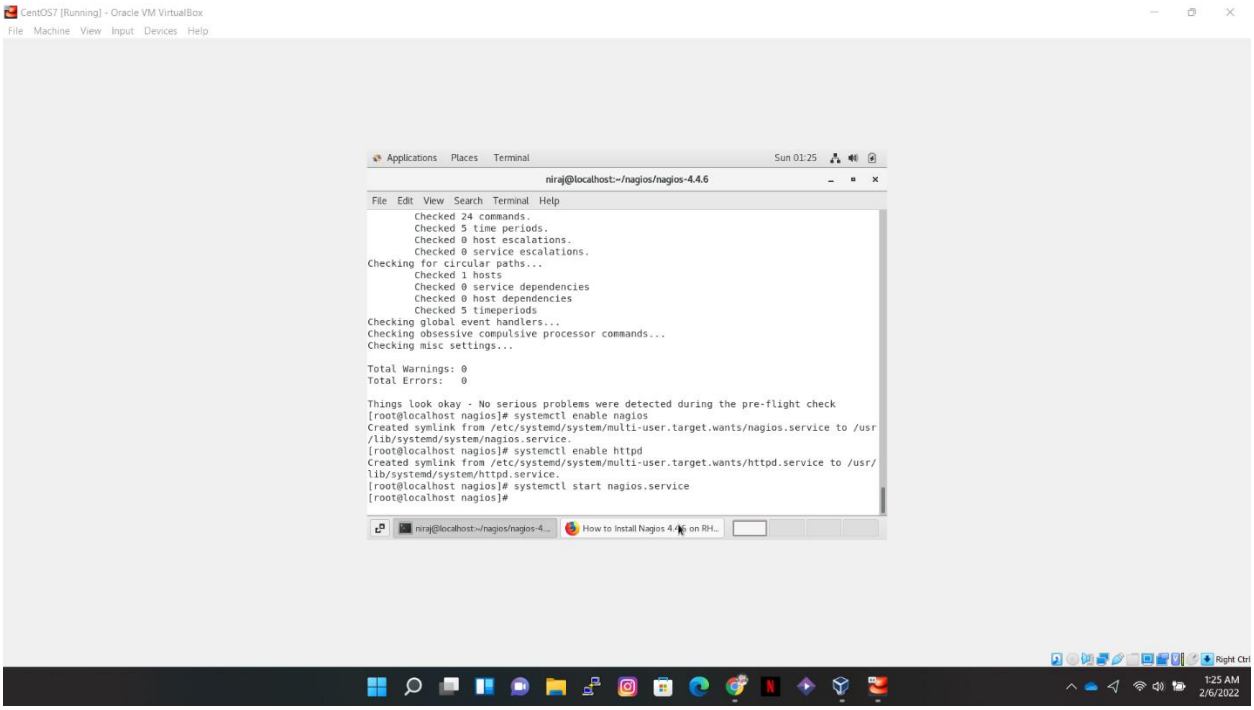


Figure 142 Installing Nagios Core on CentOS Process 18

8.3.2.5. Screenshots of WinSCP

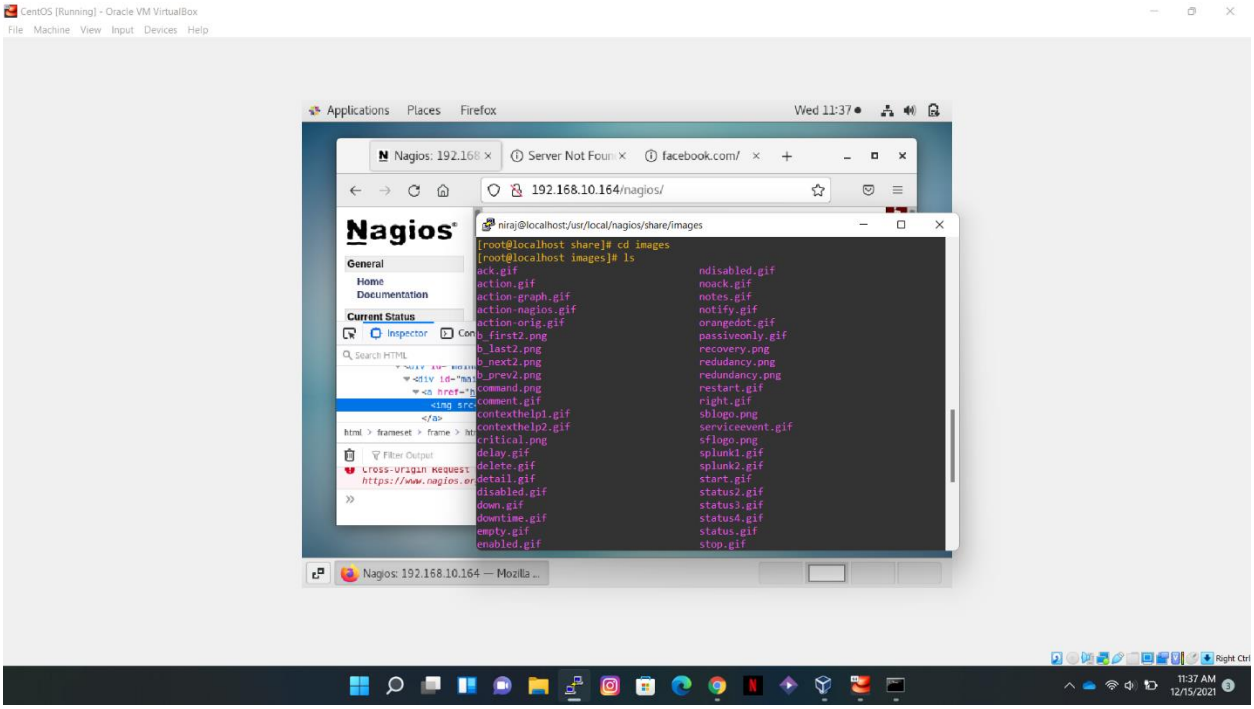


Figure 143 Changing Nagios Logo Process 1

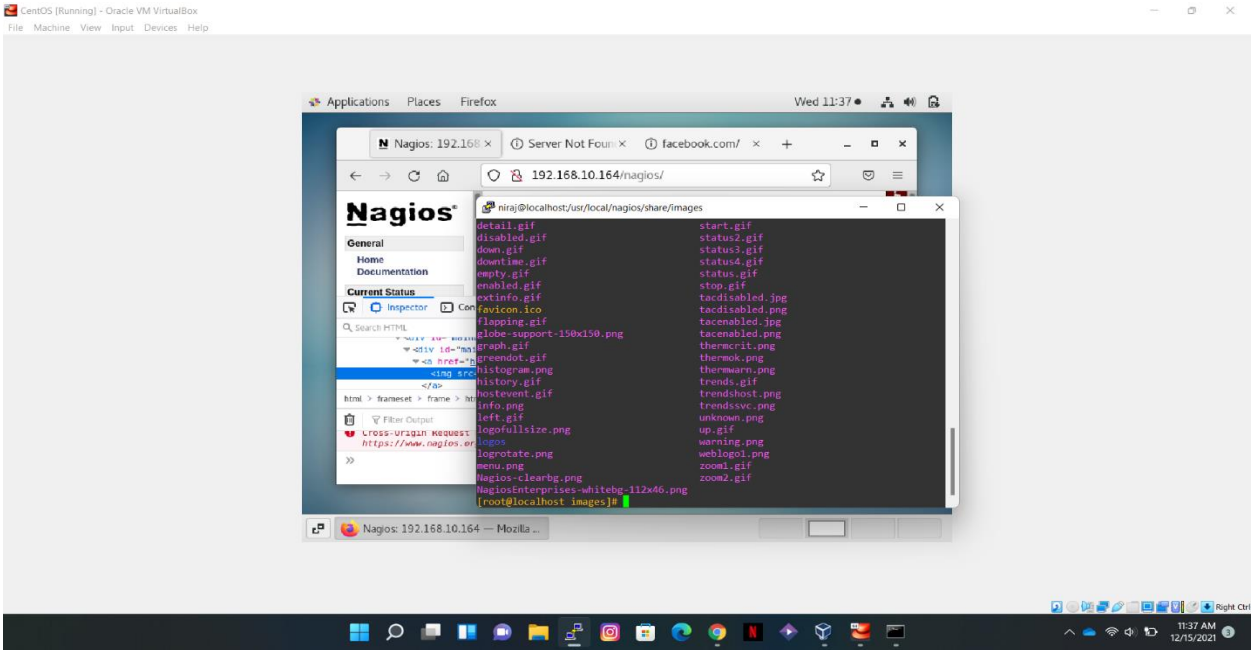


Figure 144 Changing Nagios Logo Process 2

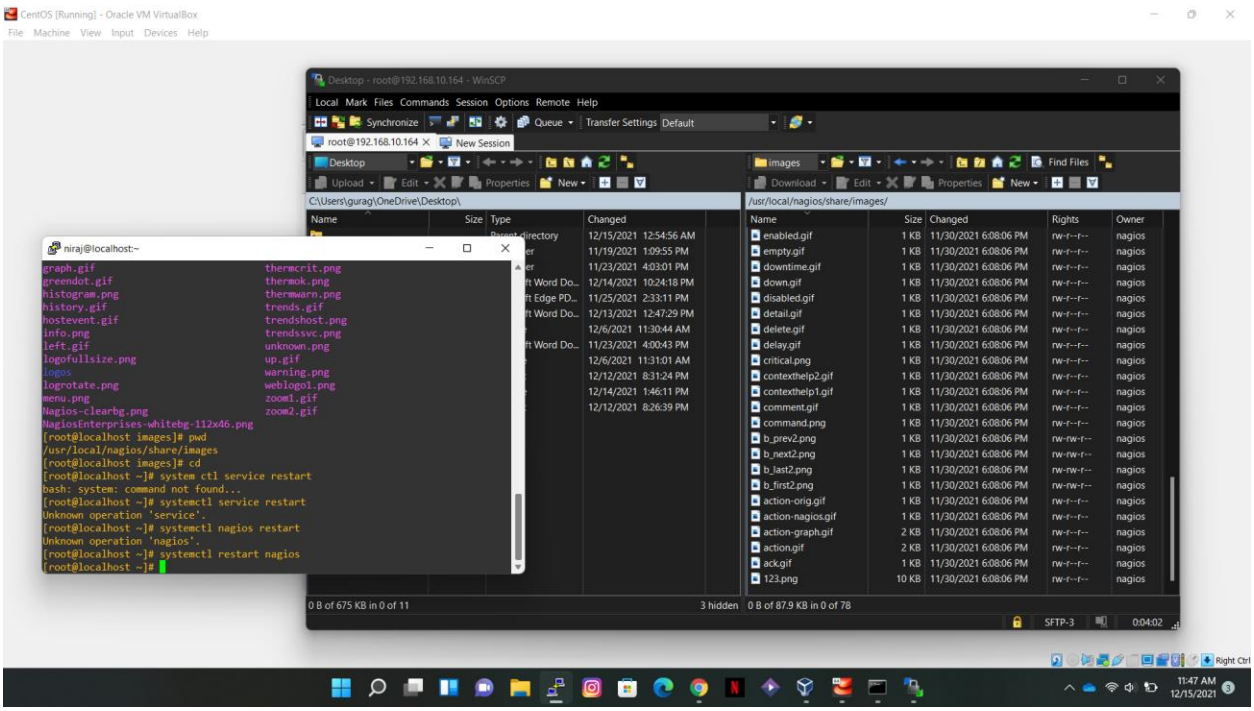


Figure 145 Changing Nagios Logo Process 3

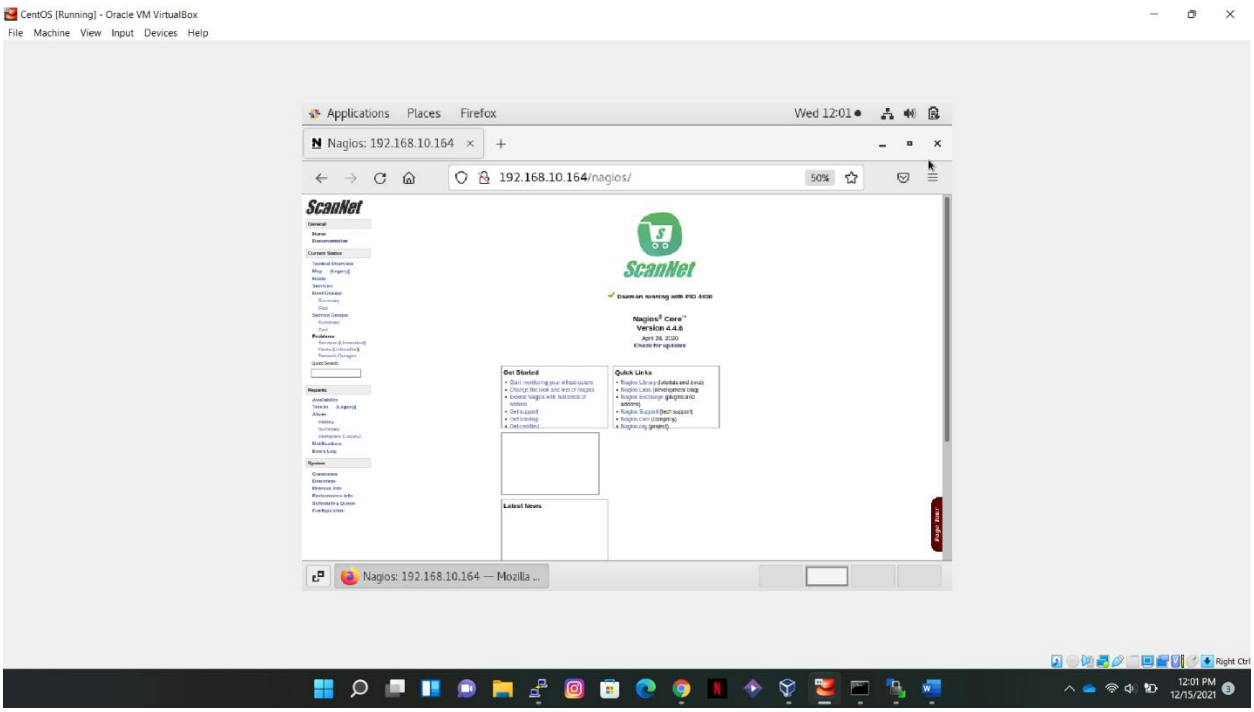


Figure 146 Successfully Changed Nagios Logo Process

8.3.2.6. Screenshots of GNS3

Figure 147 GNS3 installation process 1

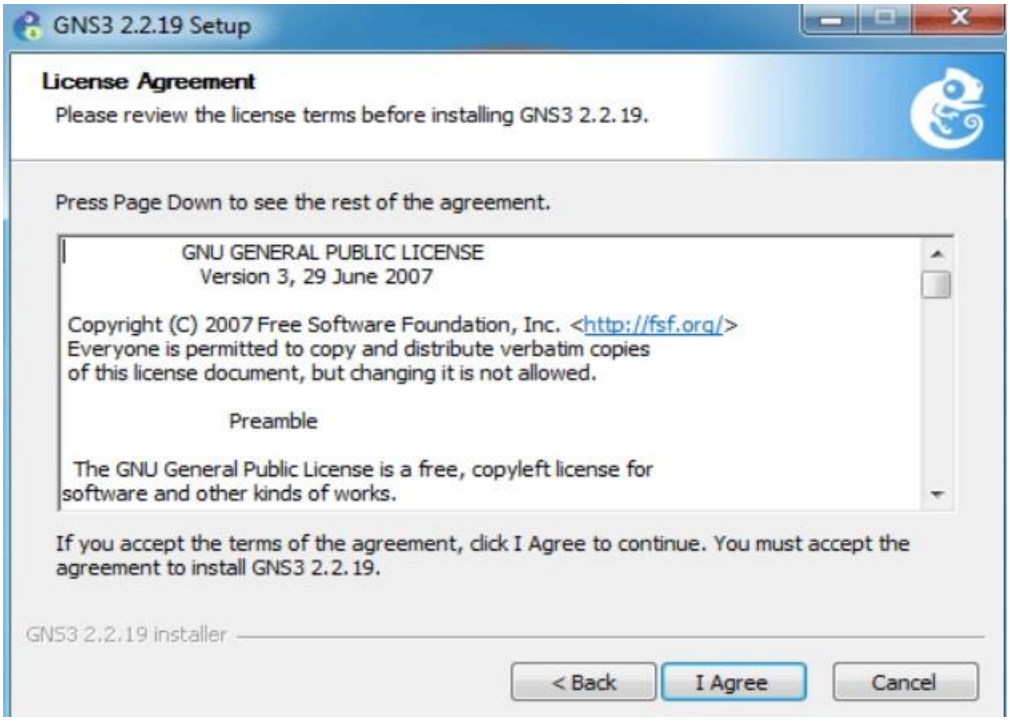


Figure 147 GNS3 installation process 2

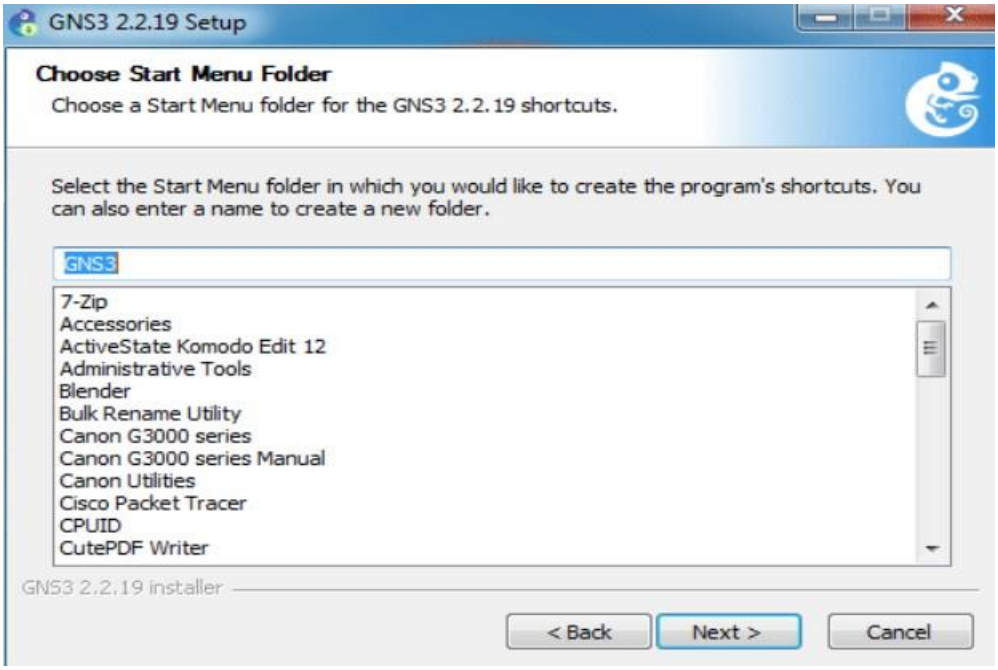


Figure 148 GNS3 installation process 3

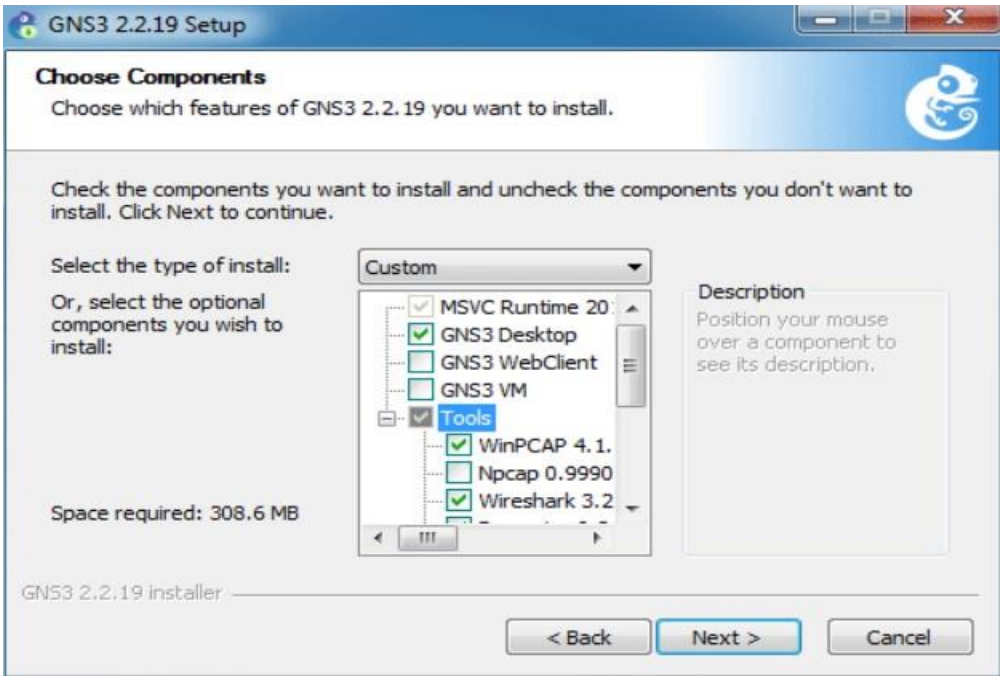


Figure 149 GNS3 installation process 4

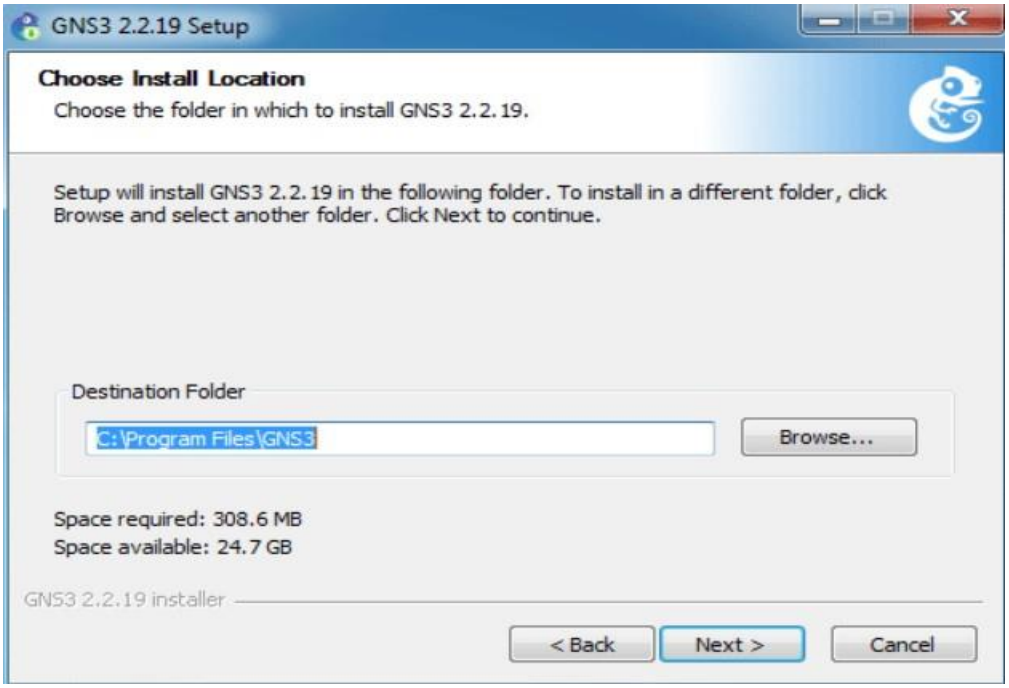


Figure 150 GNS3 installation process 5

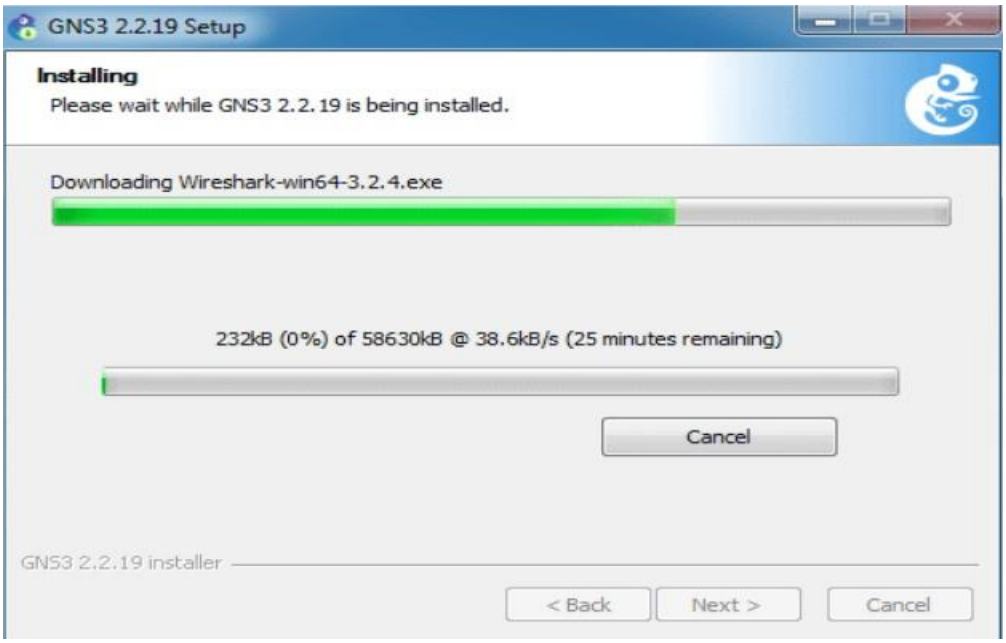


Figure 151 GNS3 installation process 6

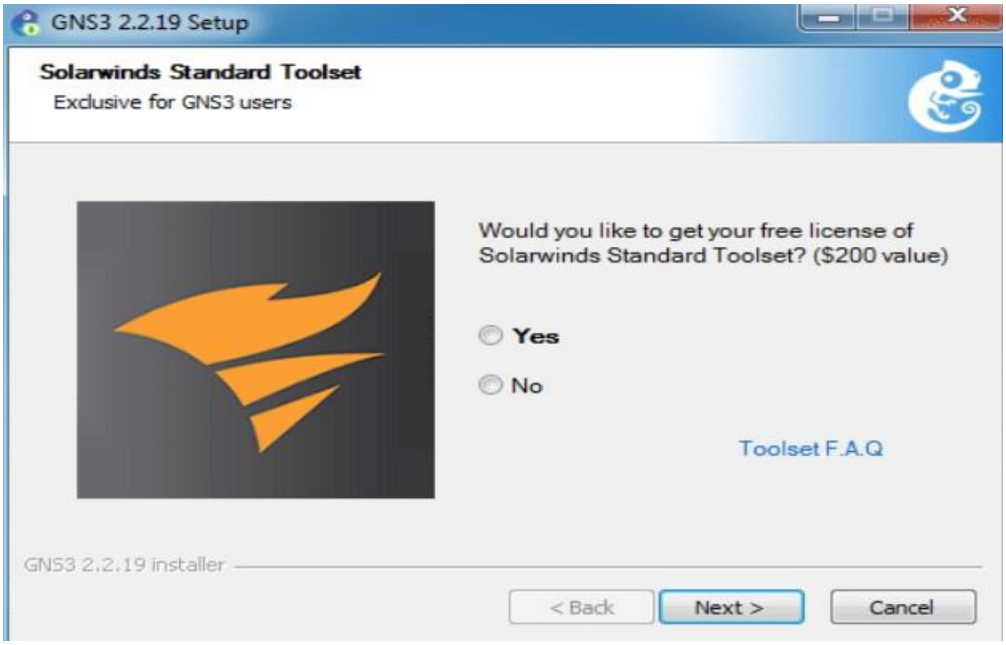


Figure 152 GNS3 installation process 7

Figure 148 GNS3 installation process 8

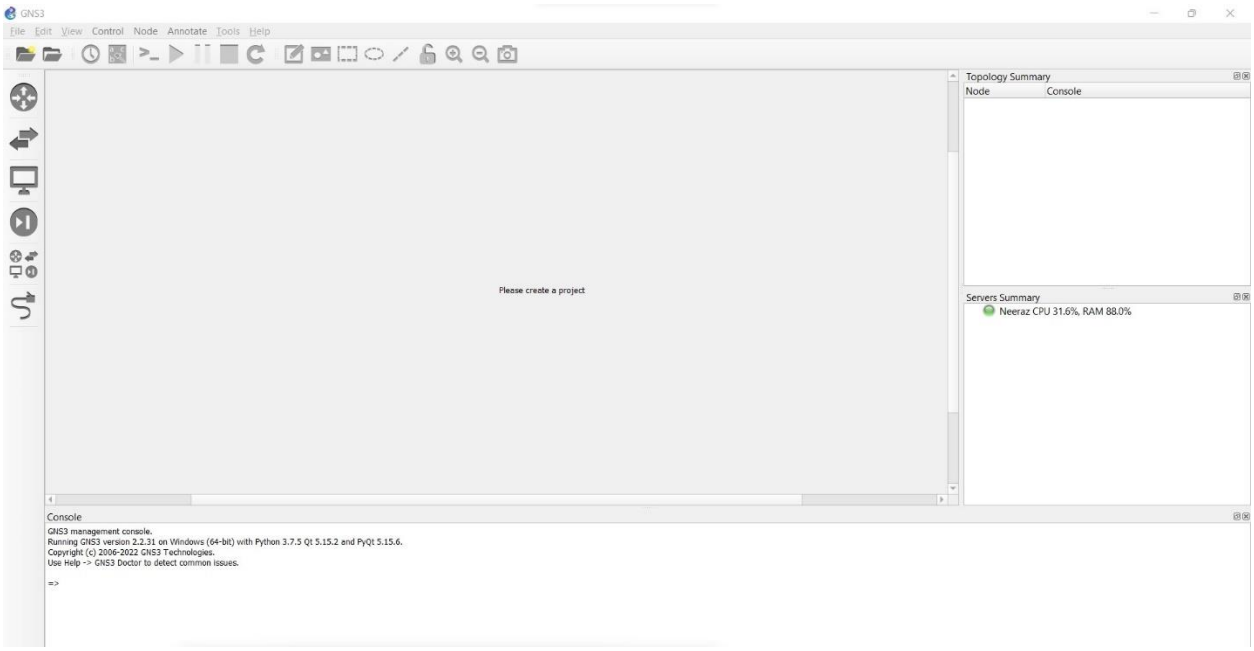


Figure 149 GNS3 installation successful

8.3.2.7. Screenshots of Nmap

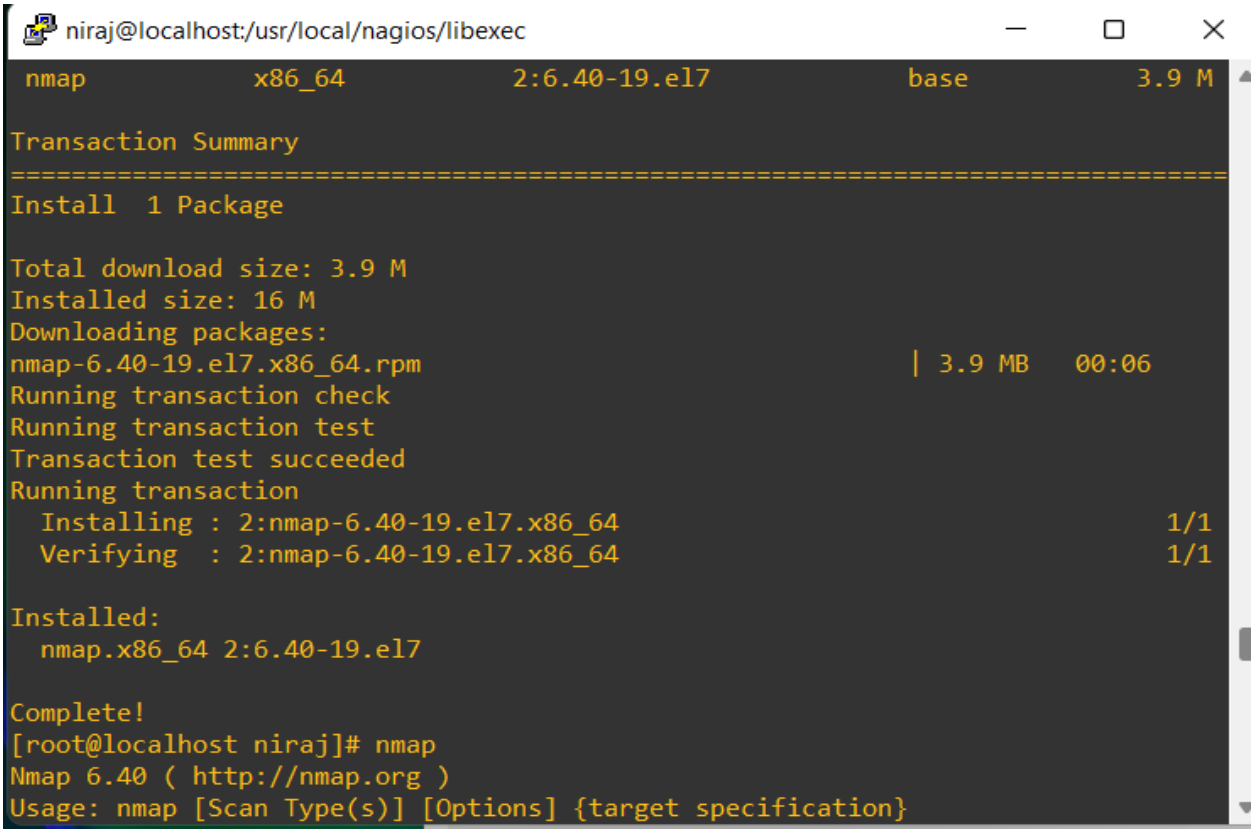


Figure 150 Nmap installation on Nagios Server

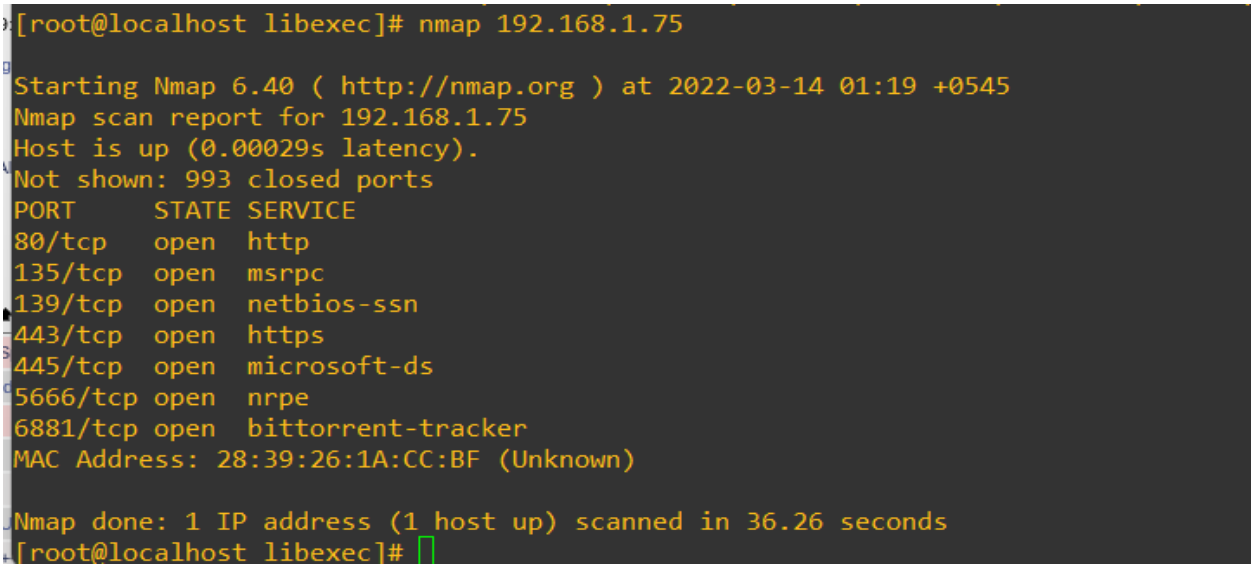


Figure 151 Scanning port through Nmap

8.3.2.8. Screenshots of PNP4Nagios

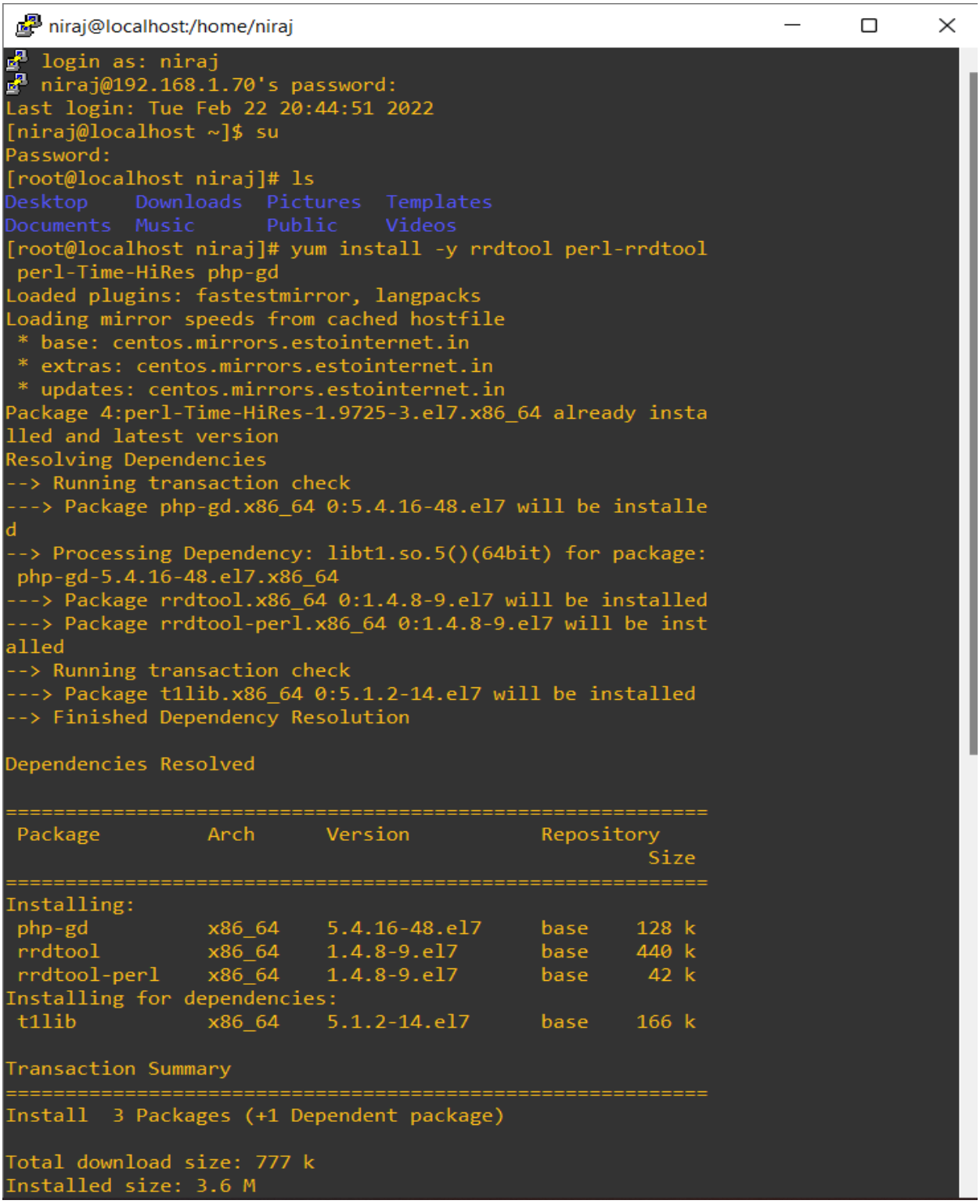


Figure 152 Installing PNP4Nagios 1

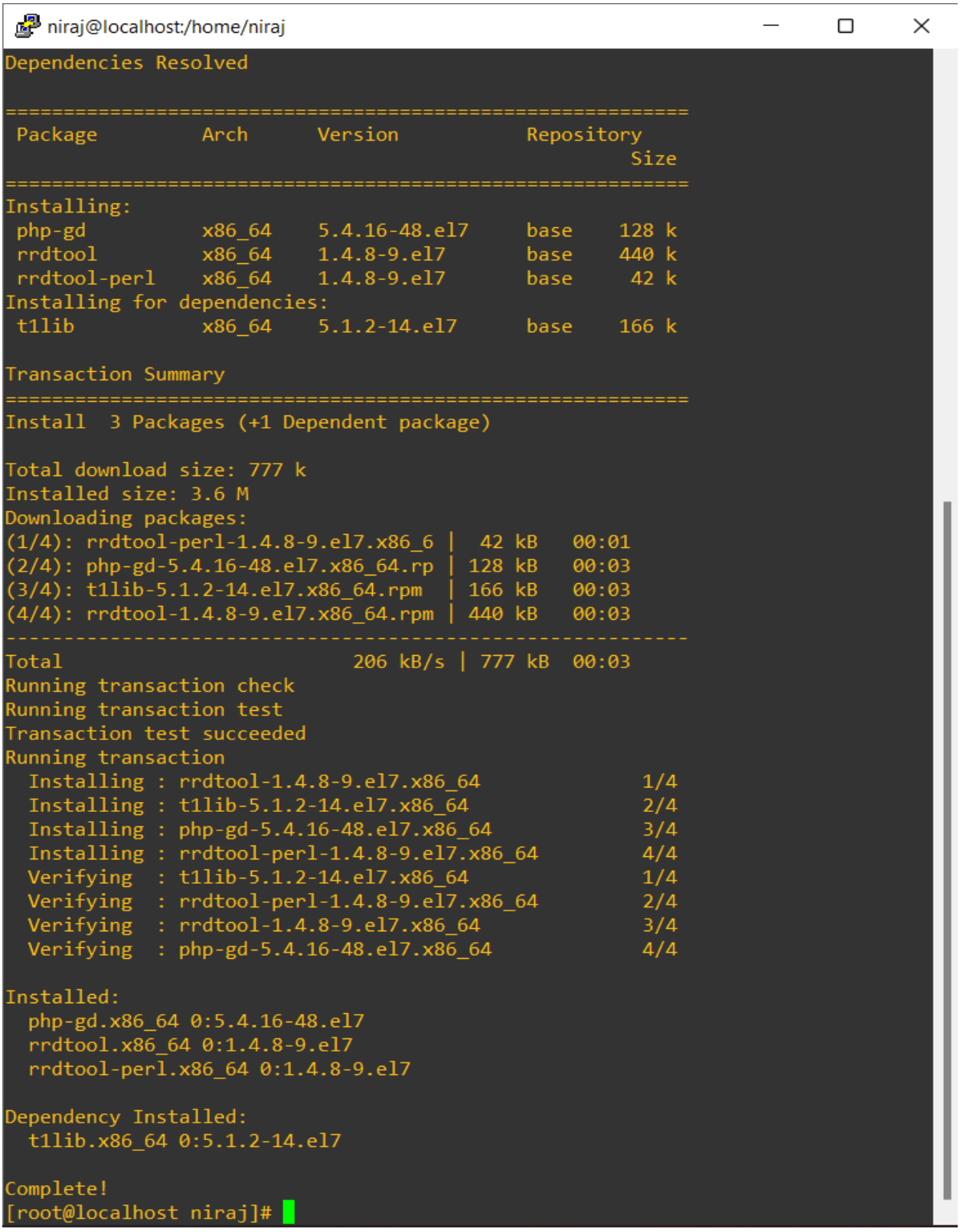


Figure 153 Installing PNP4Nagios 2

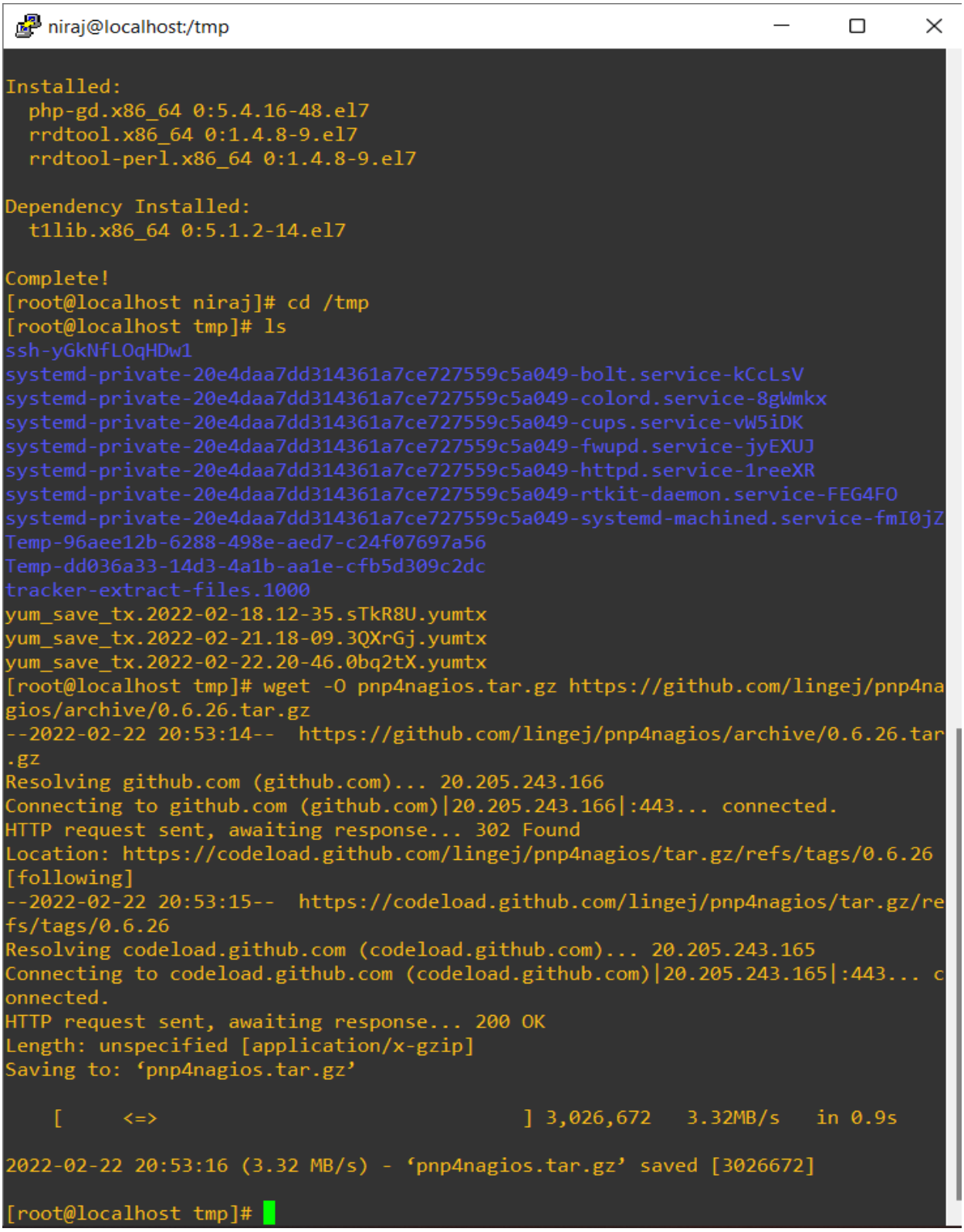


Figure 154 Installing PNP4Nagios 3

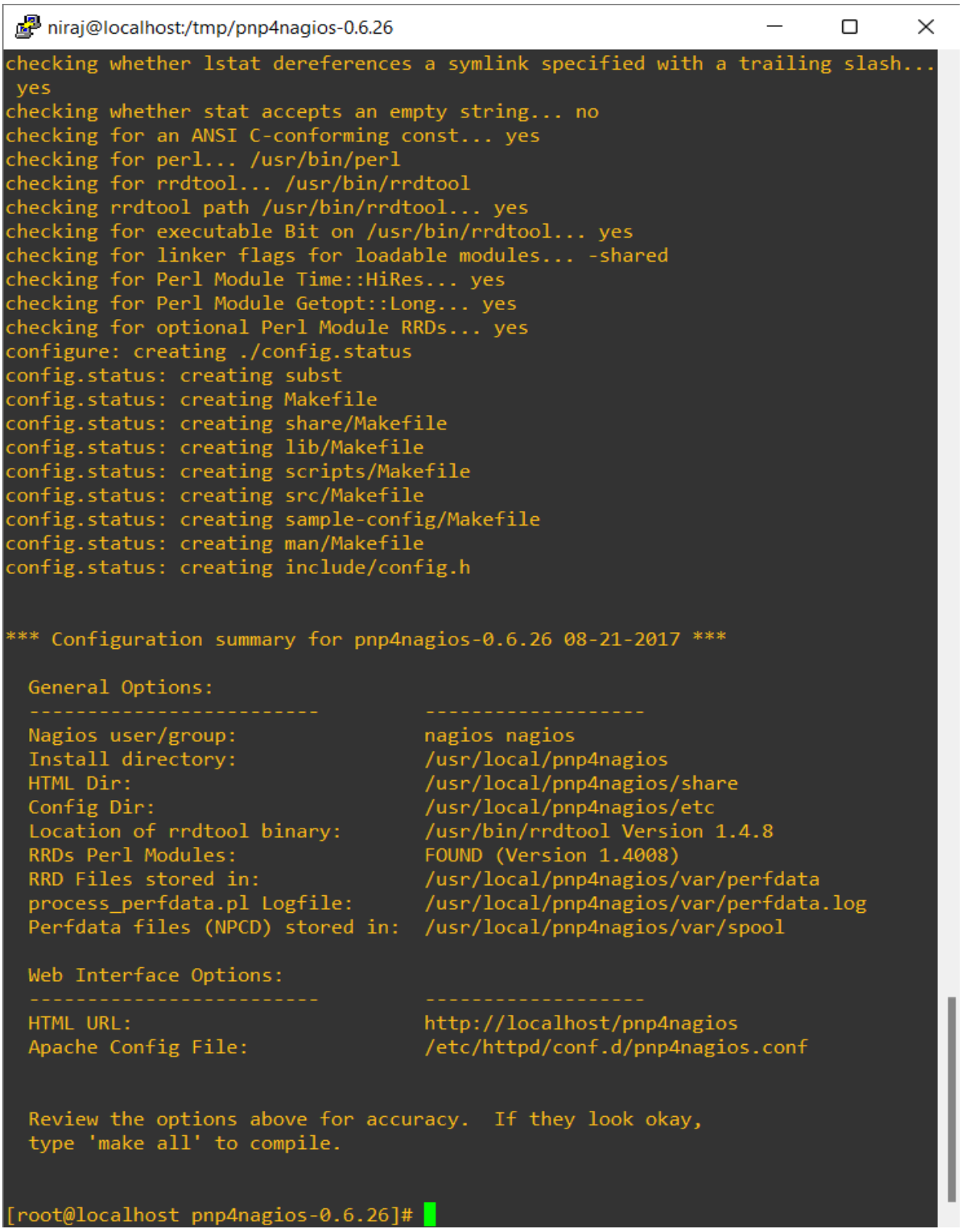


Figure 155 Installing PNP4Nagios 4

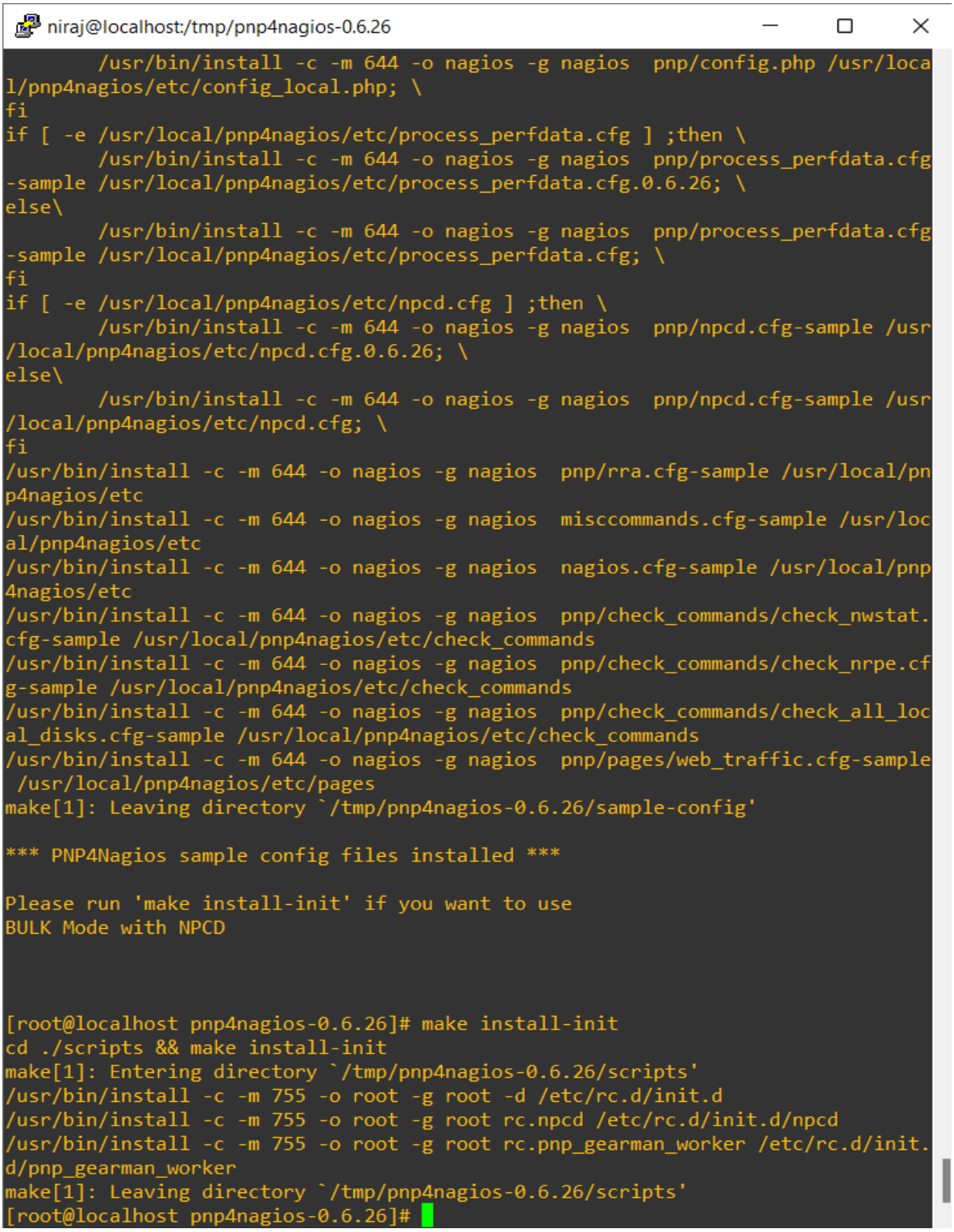


Figure 156 Installing PNP4Nagios 5

Figure 157 Installing PNP4Nagios 6

Figure 158 Installing PNP4Nagios 7

```
define command {
    command_name    process-service-perfdata-file-bulk-npcd
    command_line    /bin/mv /usr/local/pnp4nagios/var/service-perfdata
/usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$
    }

define command {
    command_name    process-host-perfdata-file-bulk-npcd
    command_line    /bin/mv /usr/local/pnp4nagios/var/host-perfdata
/usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$
    }
systemctl enable npcd.service
systemctl start npcd.service
systemctl restart httpd.service
/usr/local/pnp4nagios/bin/npcd -d -f /usr/local/pnp4nagios/etc/npcd.cfg
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
systemctl restart nagios.service
```

Figure 159 Configuring PNP4Nagios 1

```
define host {
   name       host-pnp
   action_url /pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=_HOST_
   register   0
}

define service {
   name       service-pnp
   action_url /pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=$SERVICEDESC$
   register   0
}
```

Figure 160 Configuring PNP4Nagios 2

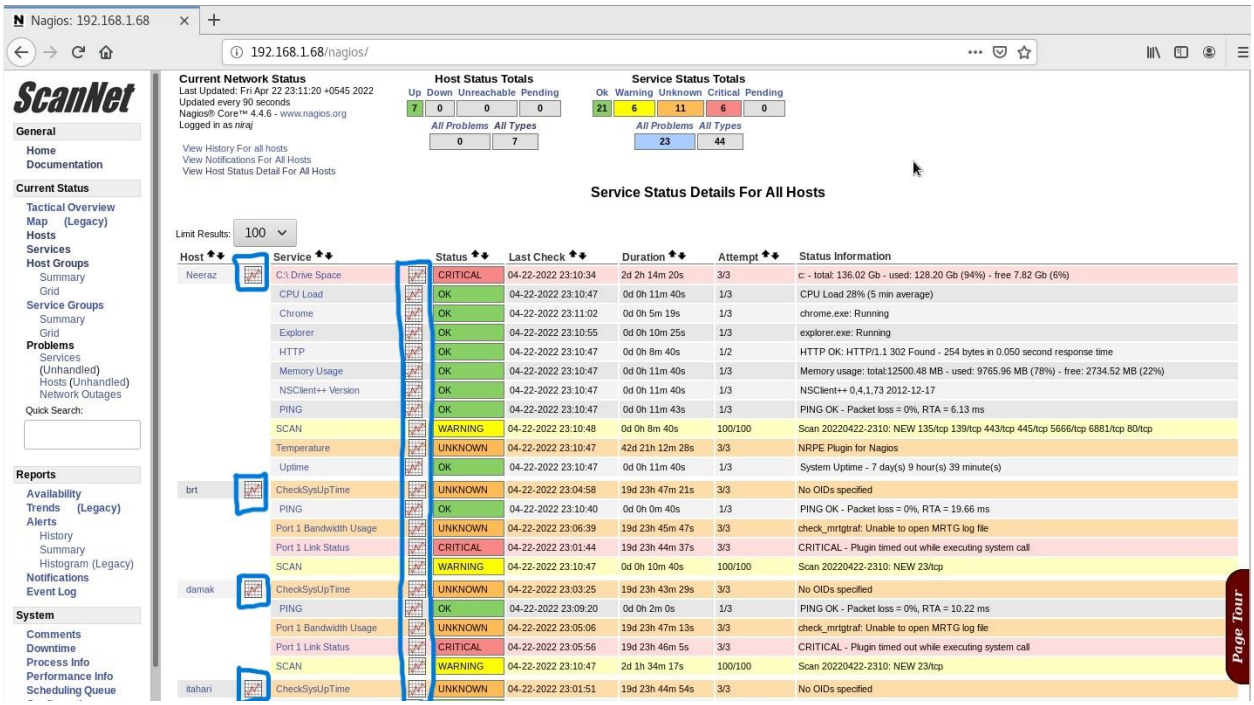


Figure 161 PNP4Nagios successfully installed 1

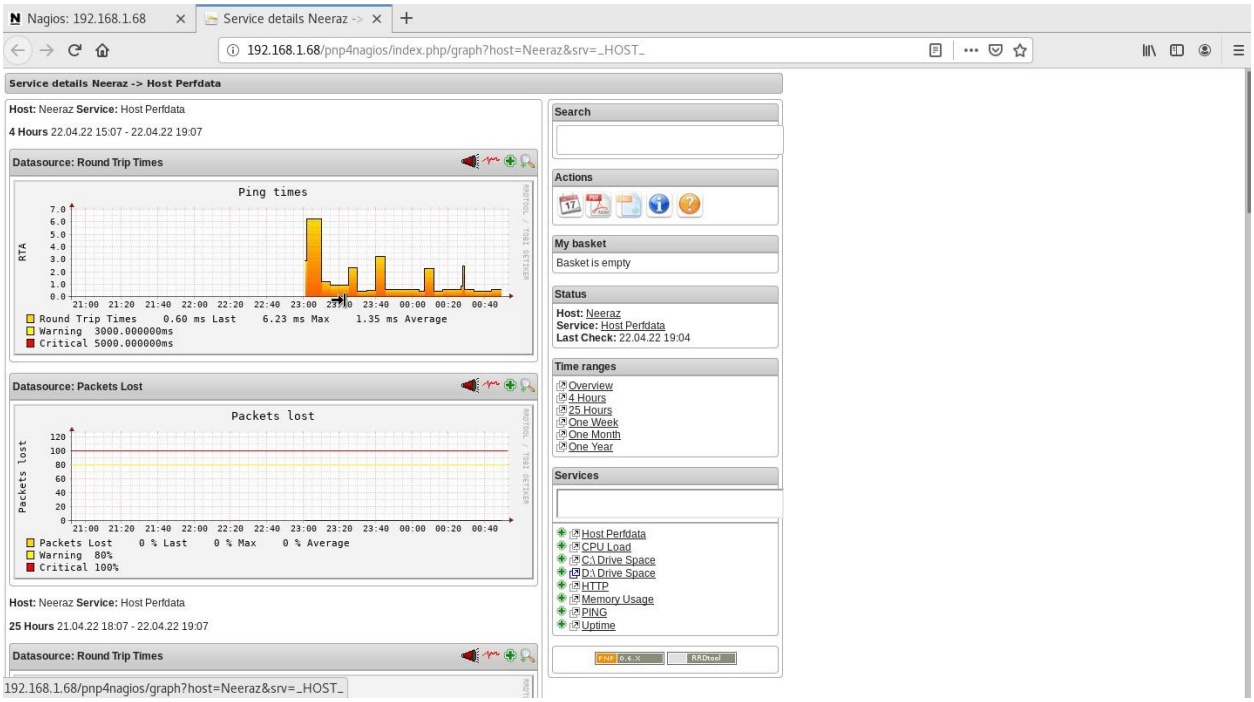


Figure 162 PNP4Nagios successfully installed 2

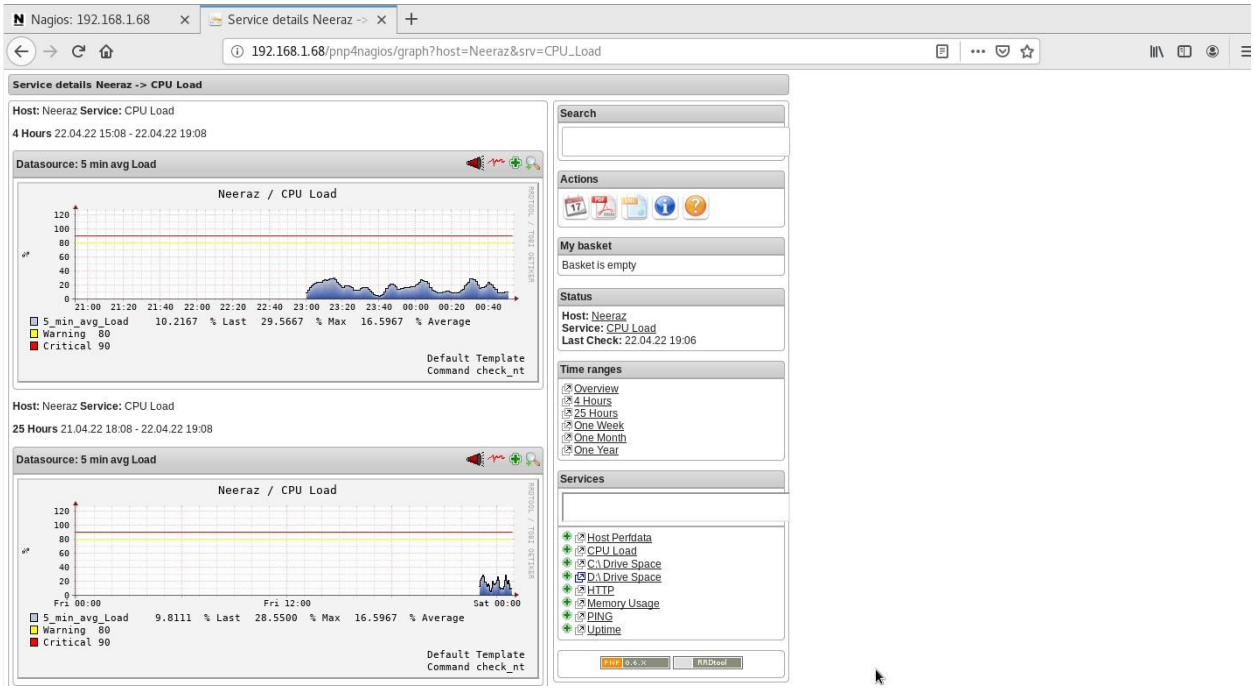


Figure 163 PNP4Nagios successfully installed 2

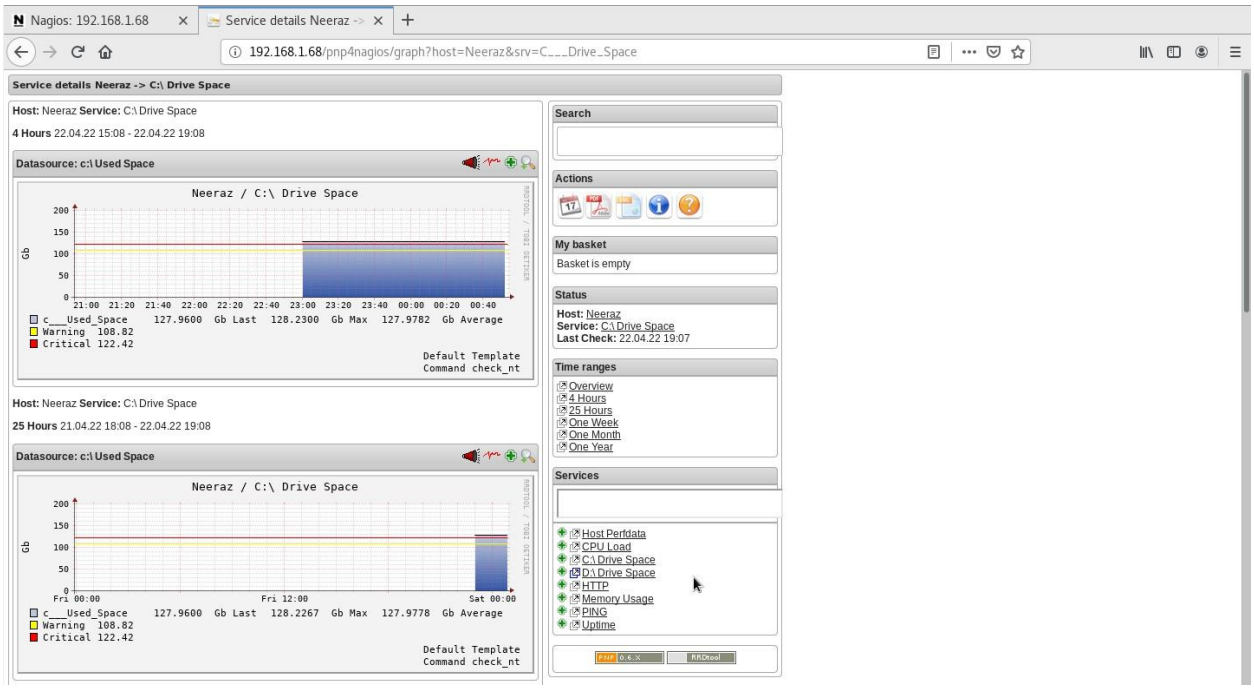


Figure 164 PNP4Nagios successfully installed 3

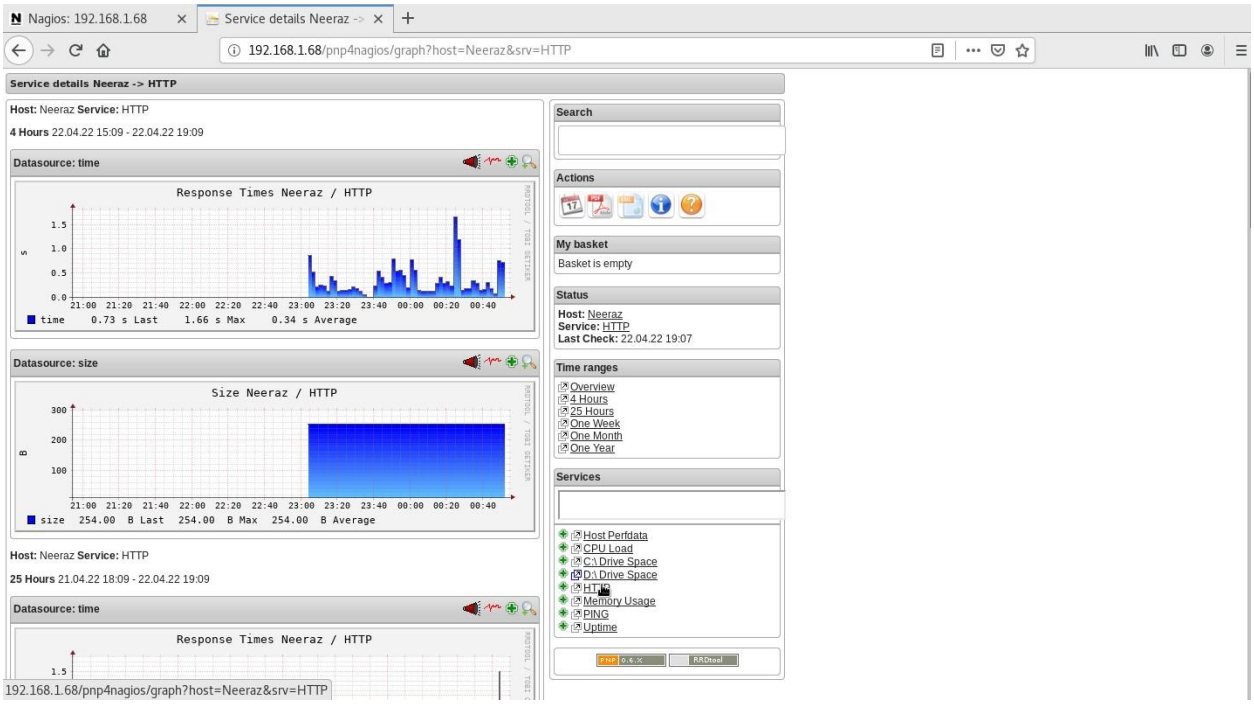


Figure 165 PNP4Nagios successfully installed 4

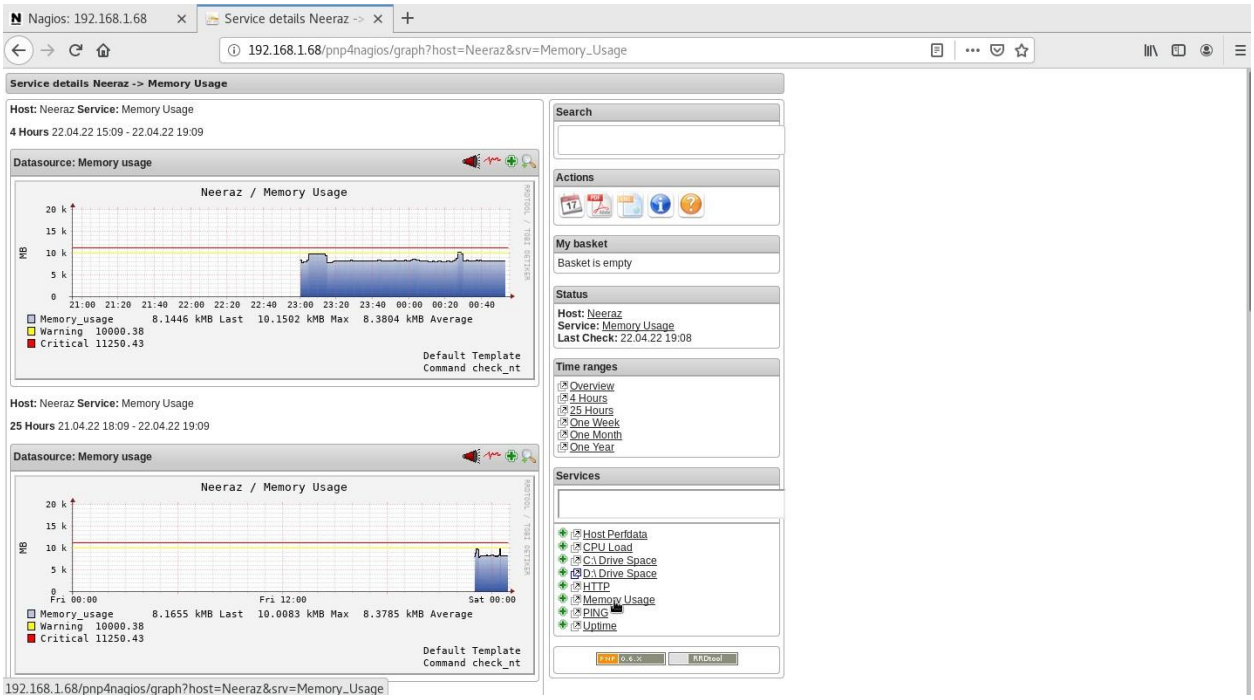


Figure 166 PNP4Nagios successfully installed 5

8.3.2.8. Screenshots of XAMPP

Figure 167 Installation process of XAMPP 1

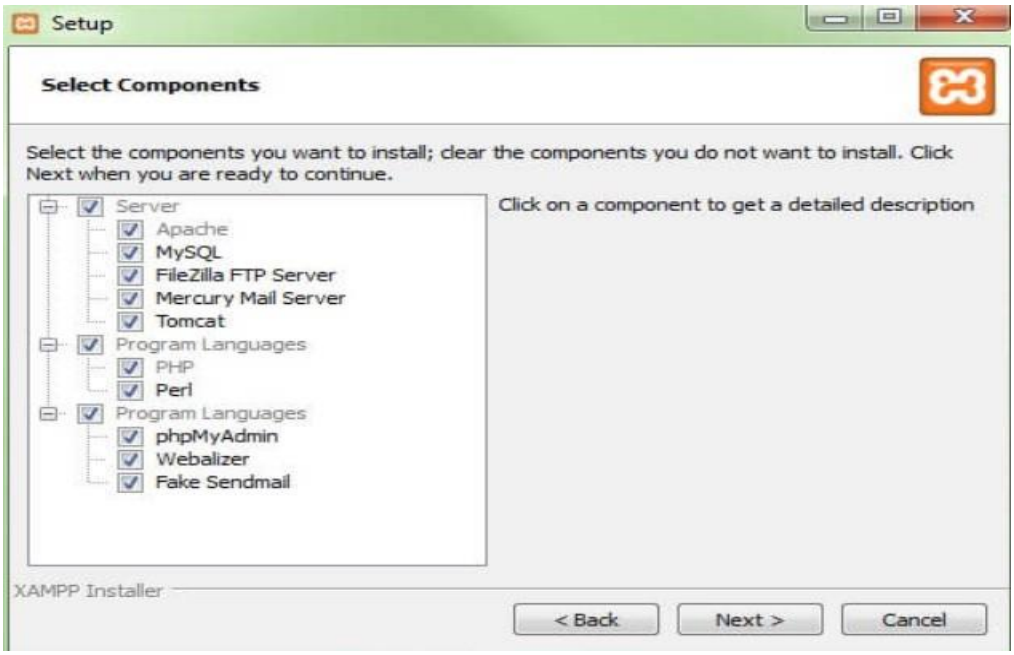


Figure 168 Installation process of XAMPP 2

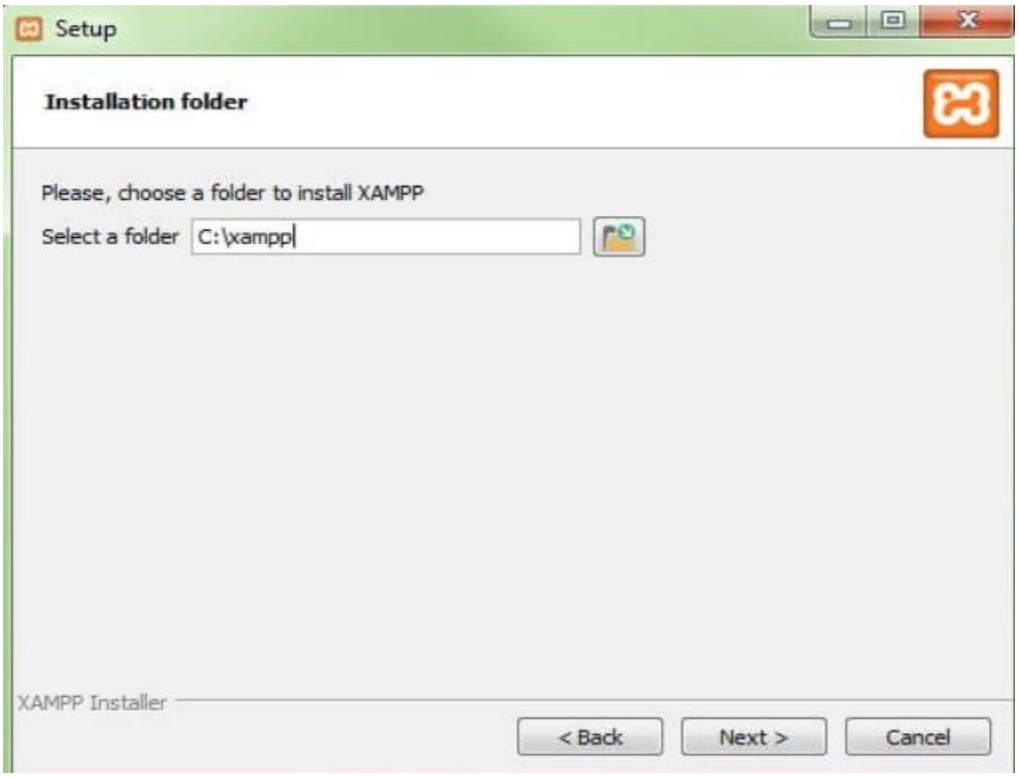


Figure 169 Installation process of XAMPP 3

Figure 170 Installation process of XAMPP 4

Figure 171 Installation process of XAMPP 5

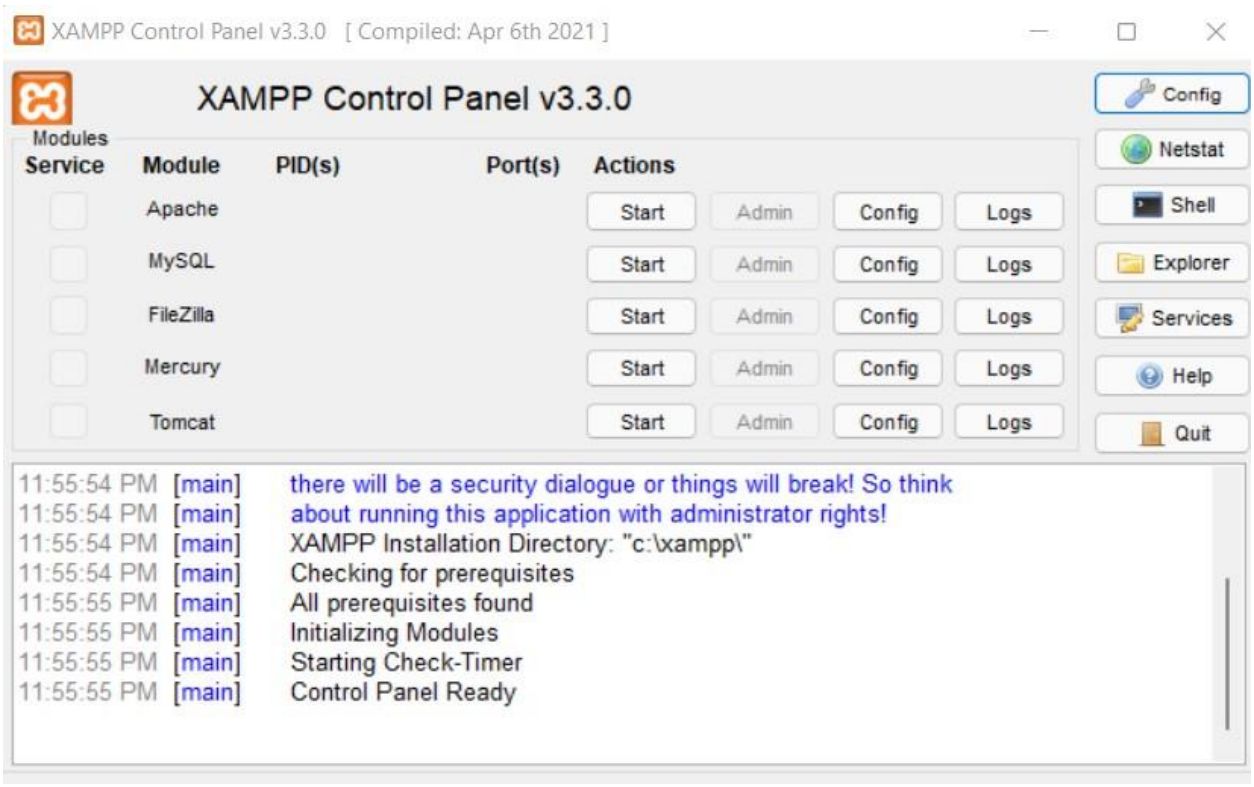


Figure 172 XAMPP successfully installed

8.4. Appendix D: Sample Codes

8.4.1. Configuration made for Host and Services in Nagios Server.

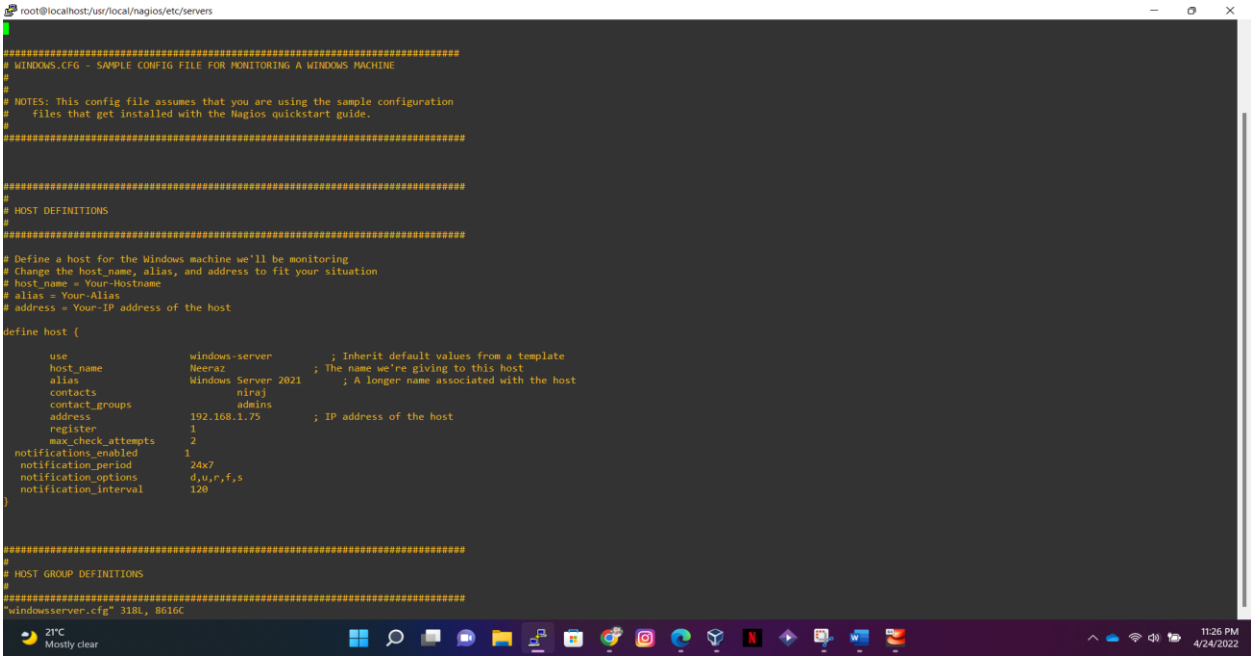


Figure 173 Configuring Windows Host and Services in Nagios Server 1

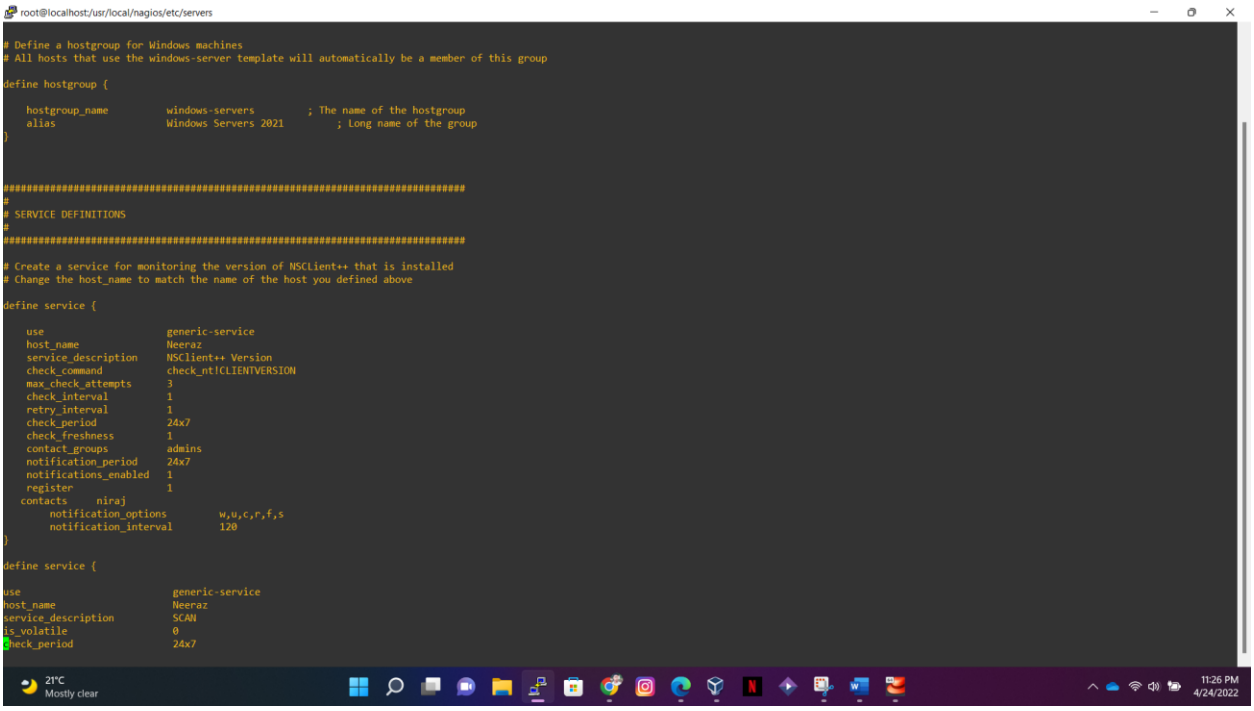


Figure 174 Configuring Windows Host and Services in Nagios Server 2

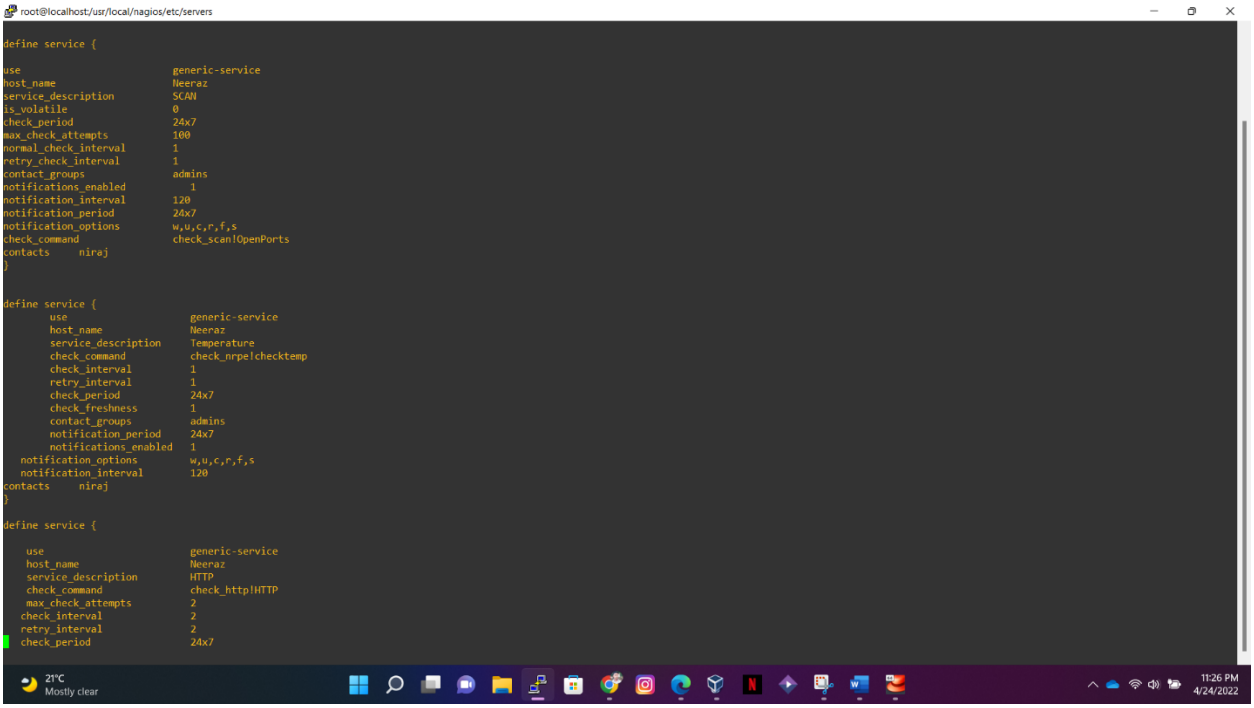


Figure 175 Configuring Windows Host and Services in Nagios Server 3

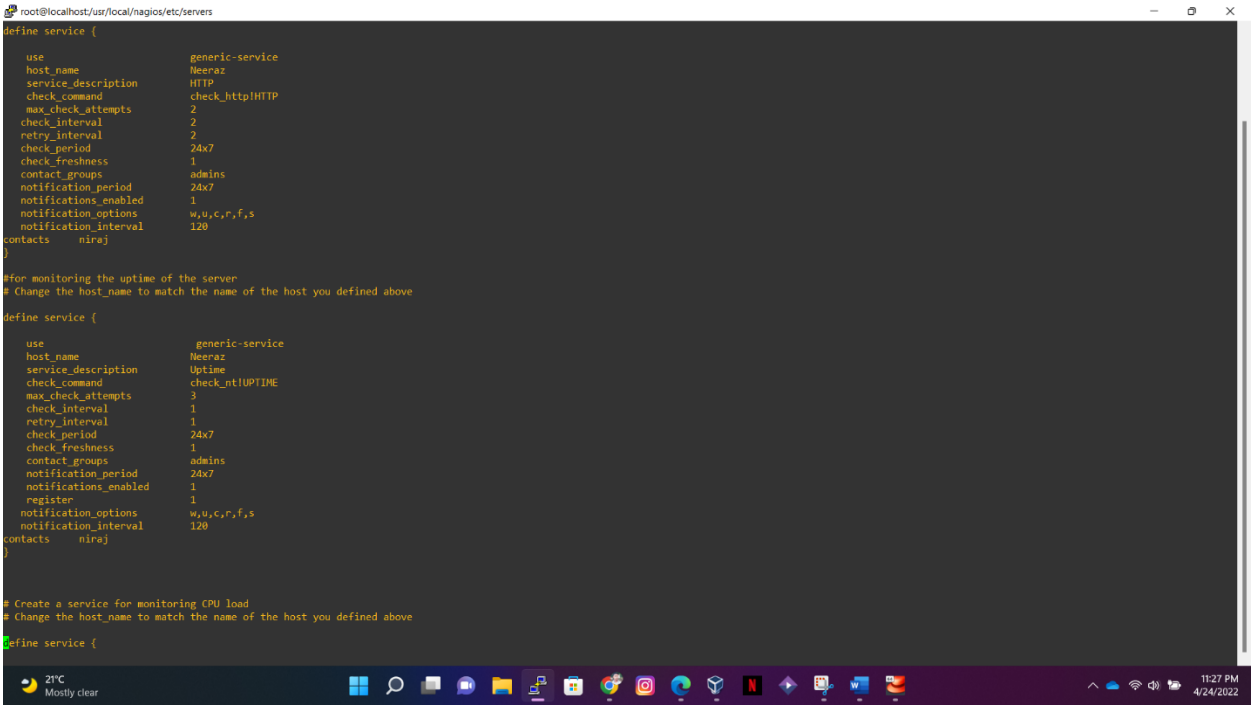


Figure 176 Configuring Windows Host and Services in Nagios Server 4

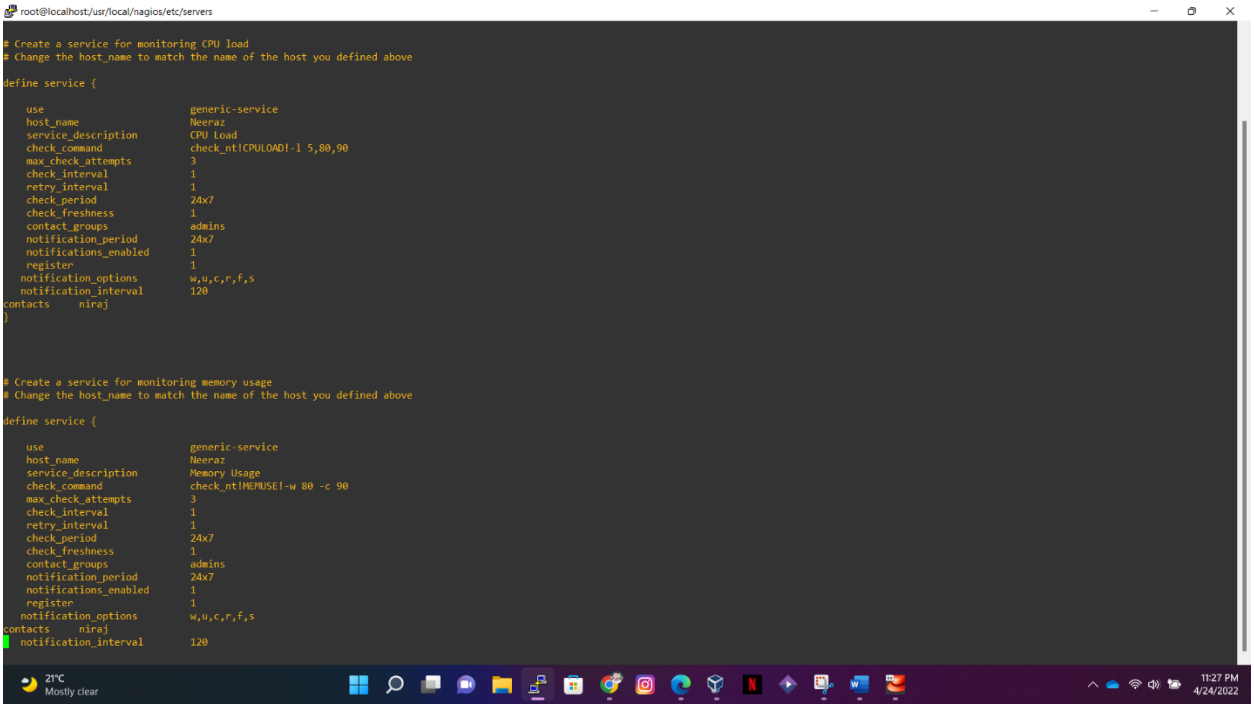


Figure 177 Configuring Windows Host and Services in Nagios Server 5

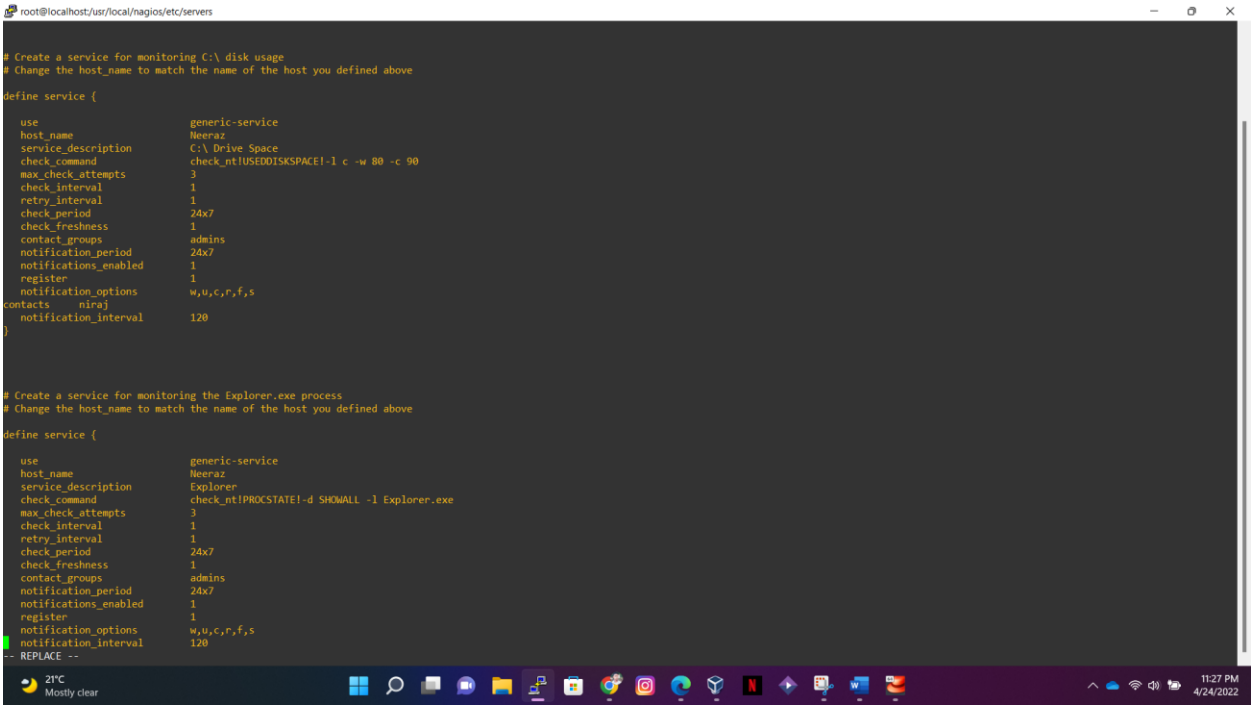


Figure 178 Configuring Windows Host and Services in Nagios Server 6

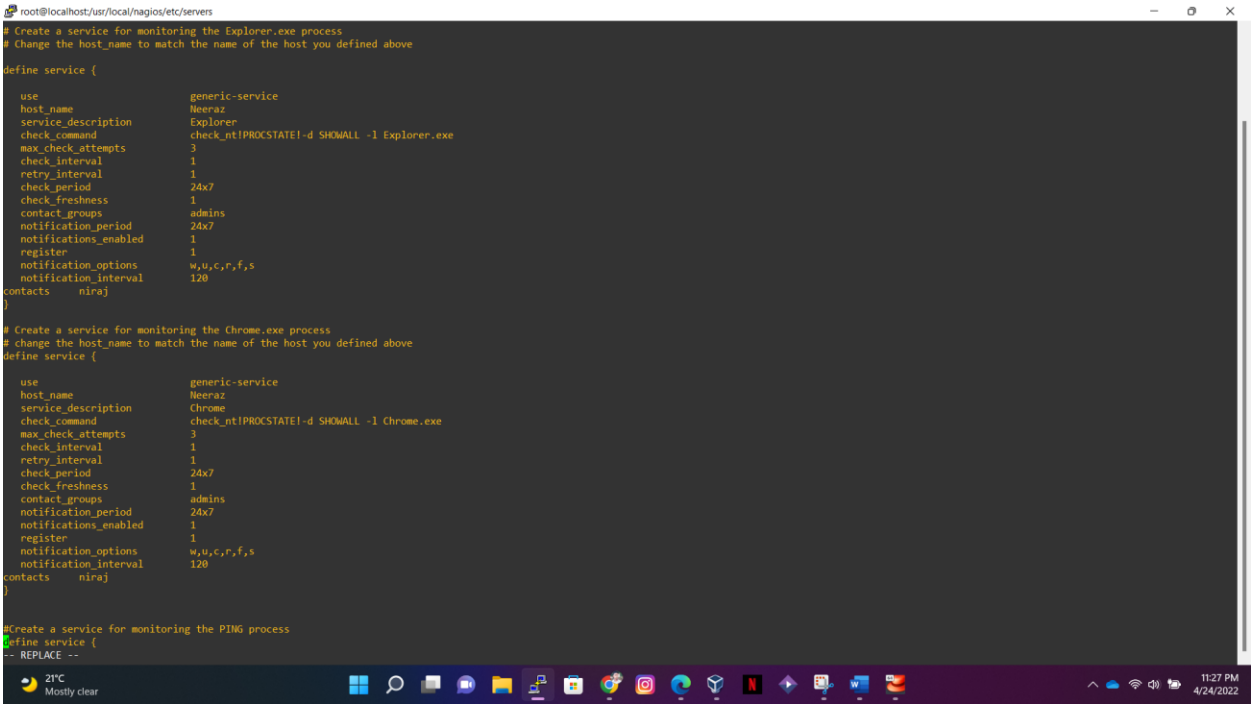


Figure 179 Configuring Windows Host and Services in Nagios Server 7

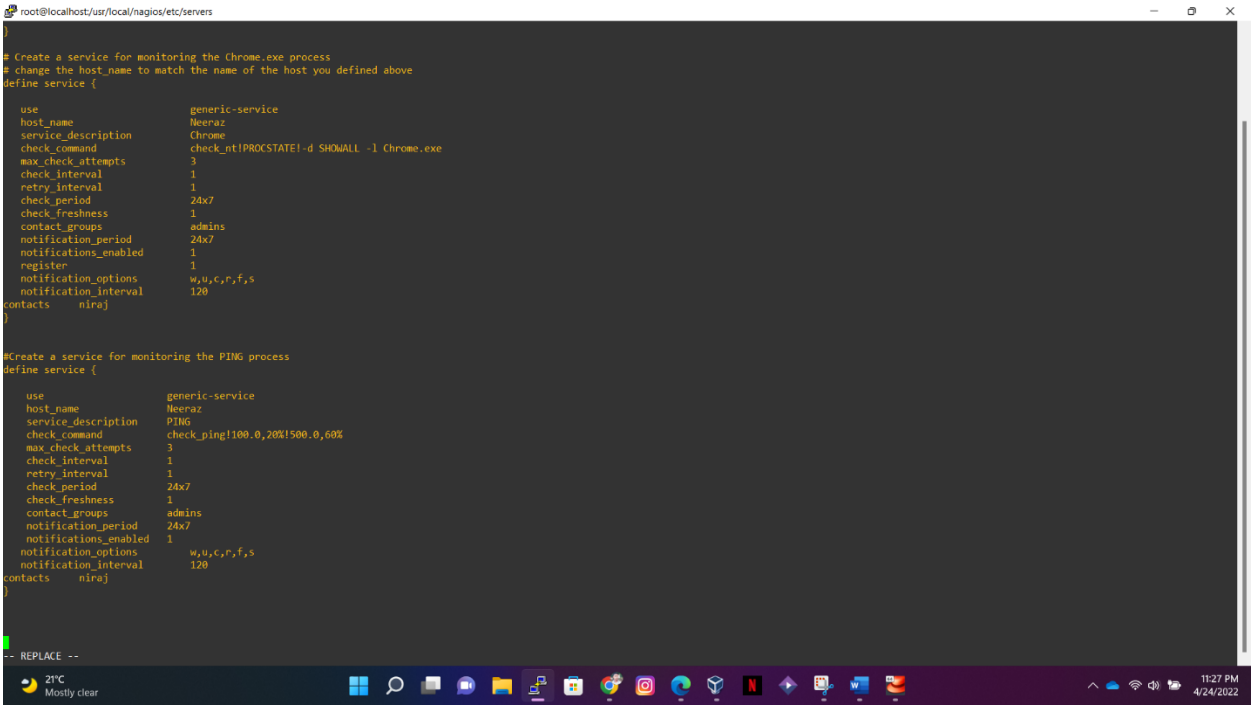


Figure 180 Configuring Windows Host and Services in Nagios Server 8

8.4.2. Configurations made for router and services in Nagios Server.

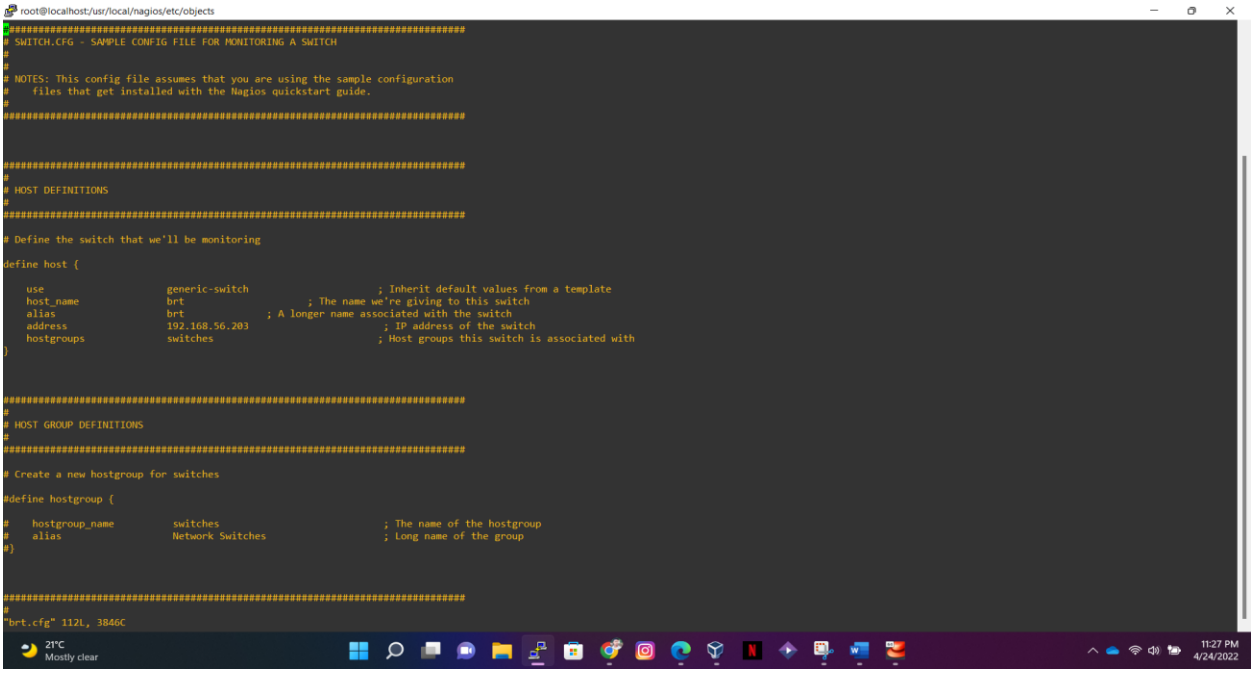


Figure 181 Configuring brt router and its services in Nagios Server 1

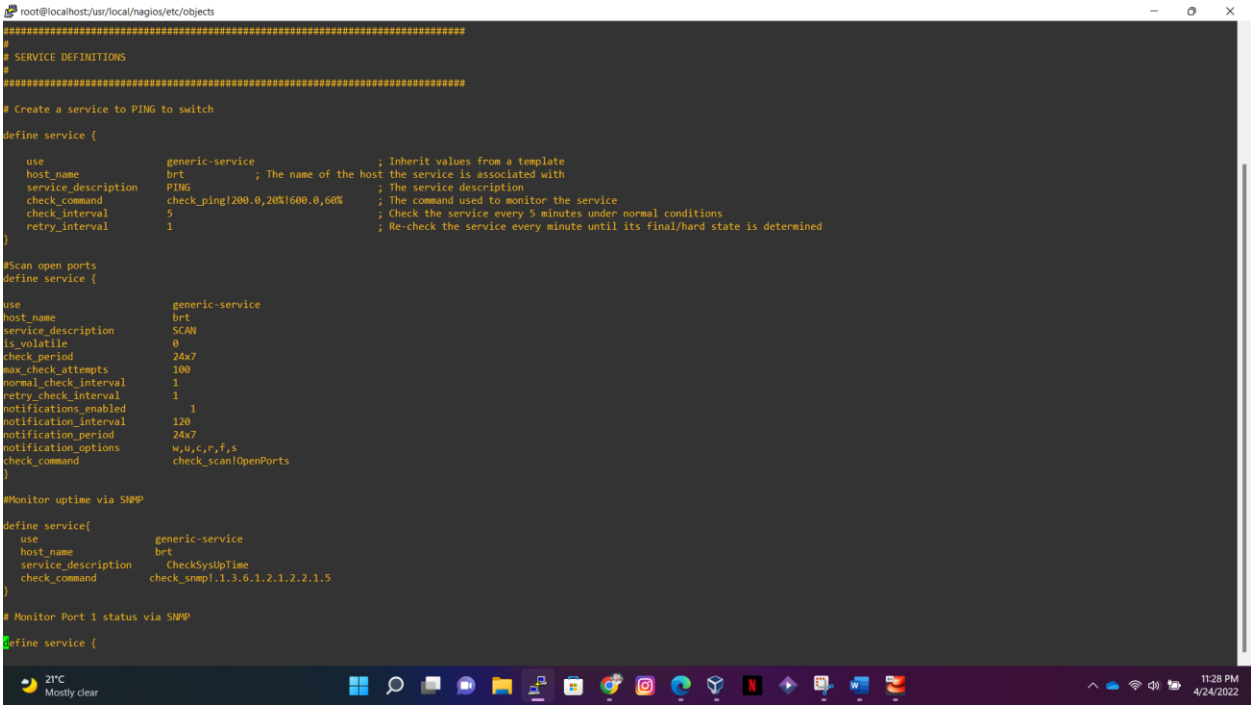


Figure 182 Configuring brt router and its services in Nagios Server 2

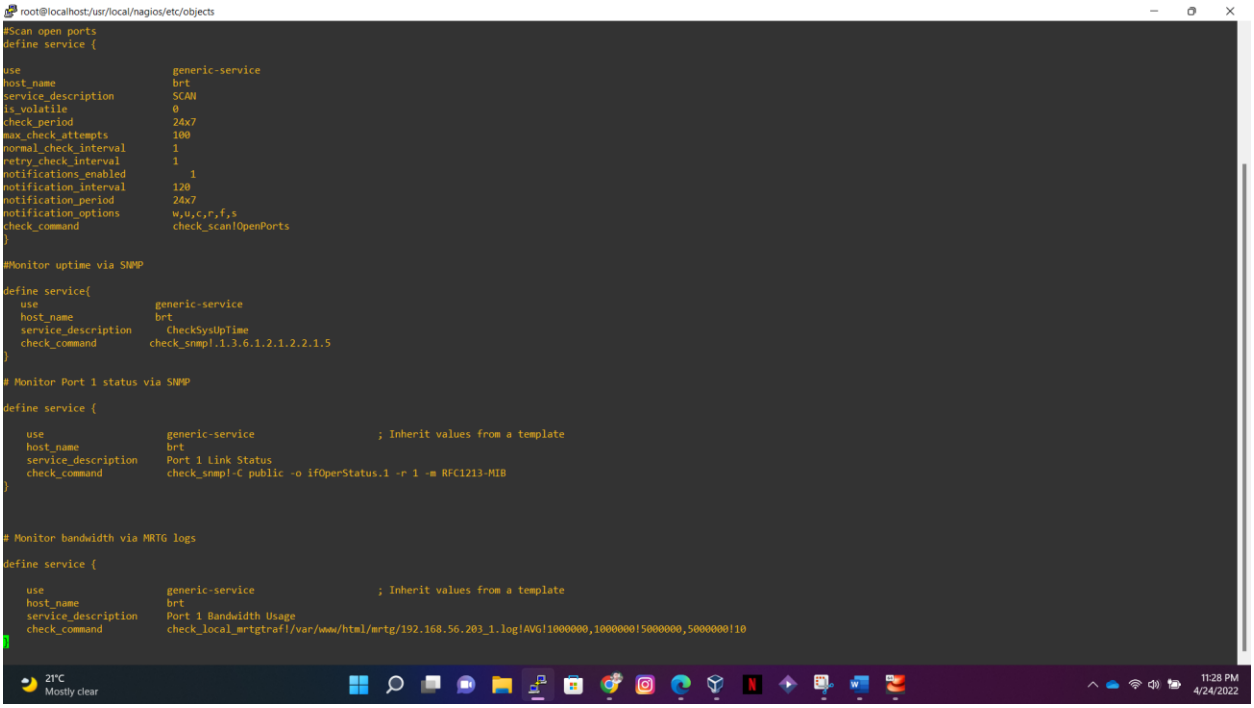


Figure 183 Configuring brt router and its services in Nagios Server 3

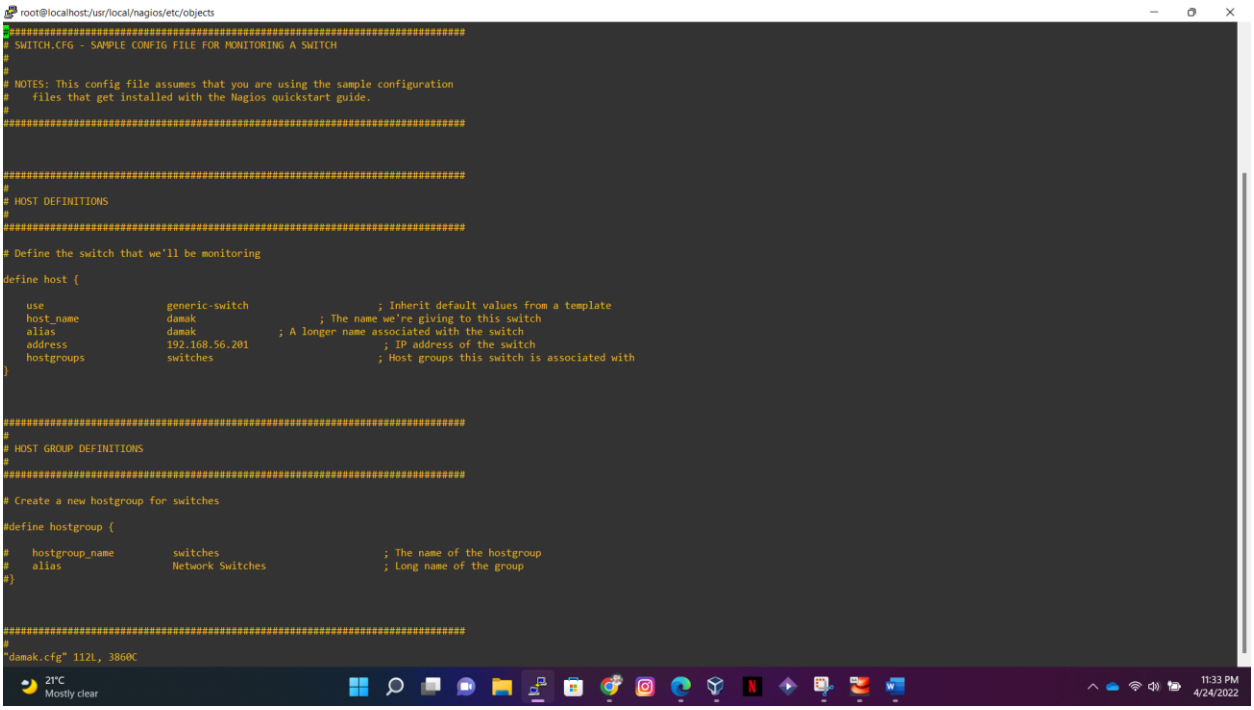


Figure 184 Configuring damak router and its services in Nagios Server 1

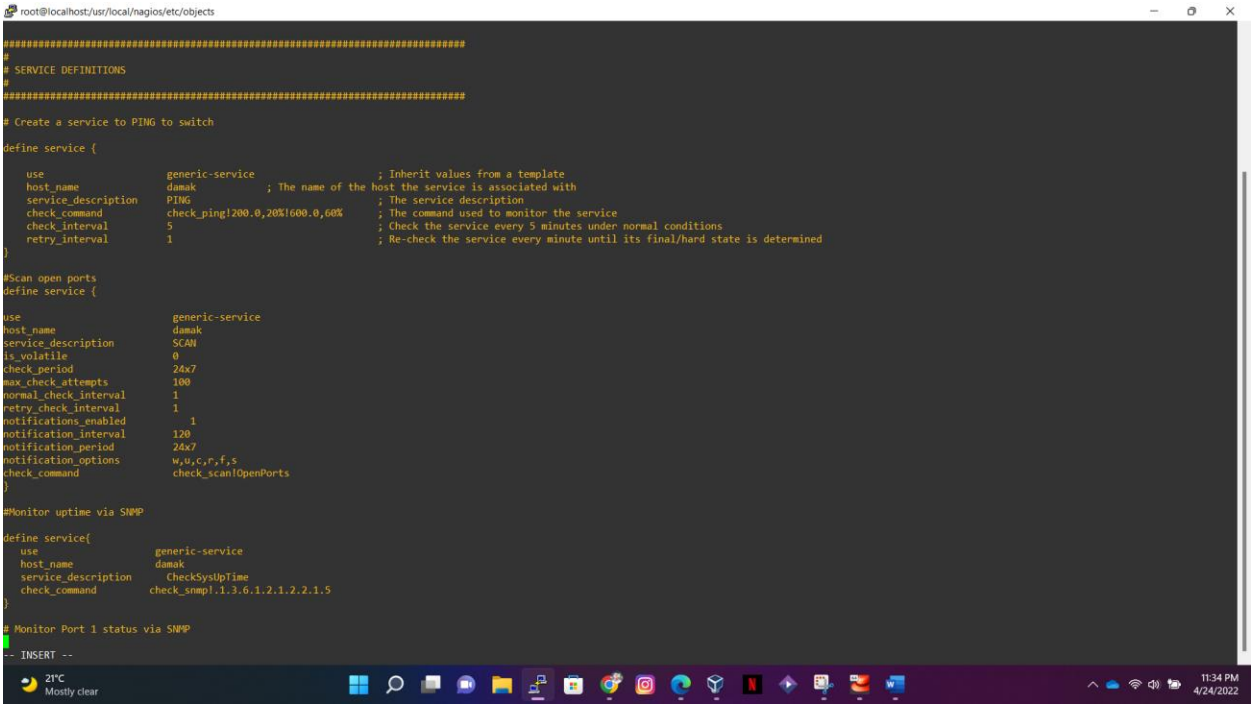


Figure 185 Configuring damak router and its services in Nagios Server 2

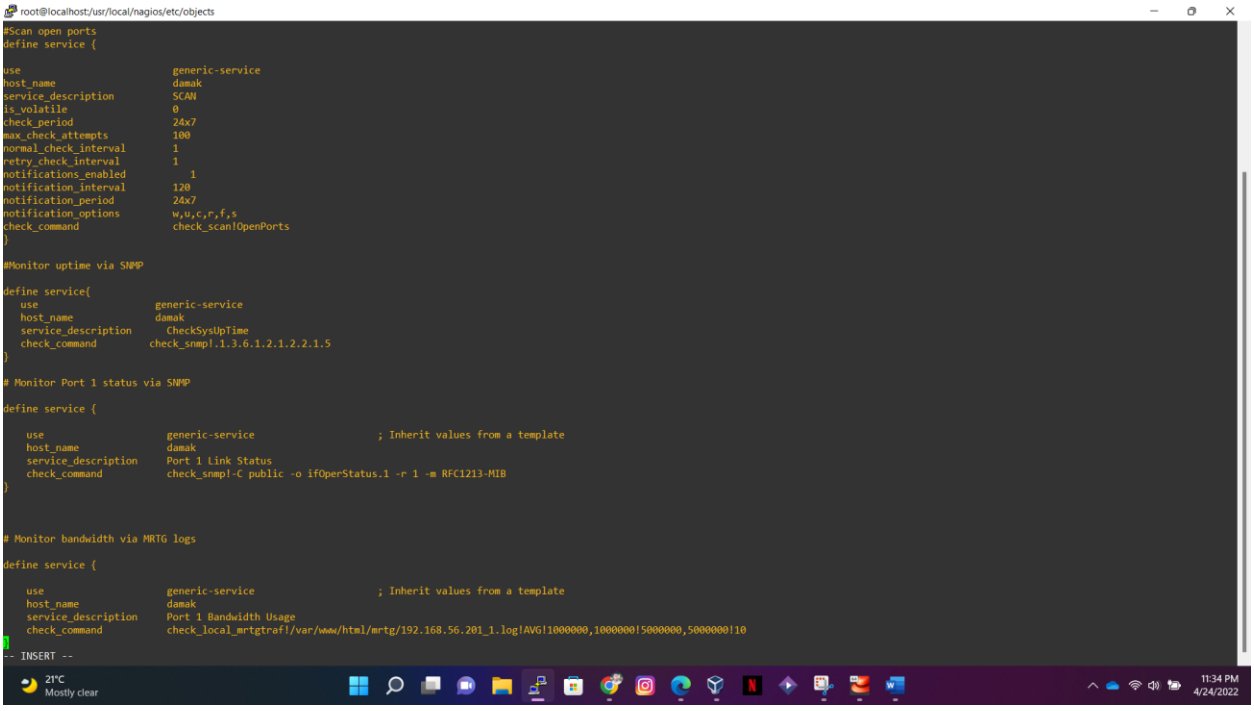


Figure 186 Configuring damak router and its services in Nagios Server 3

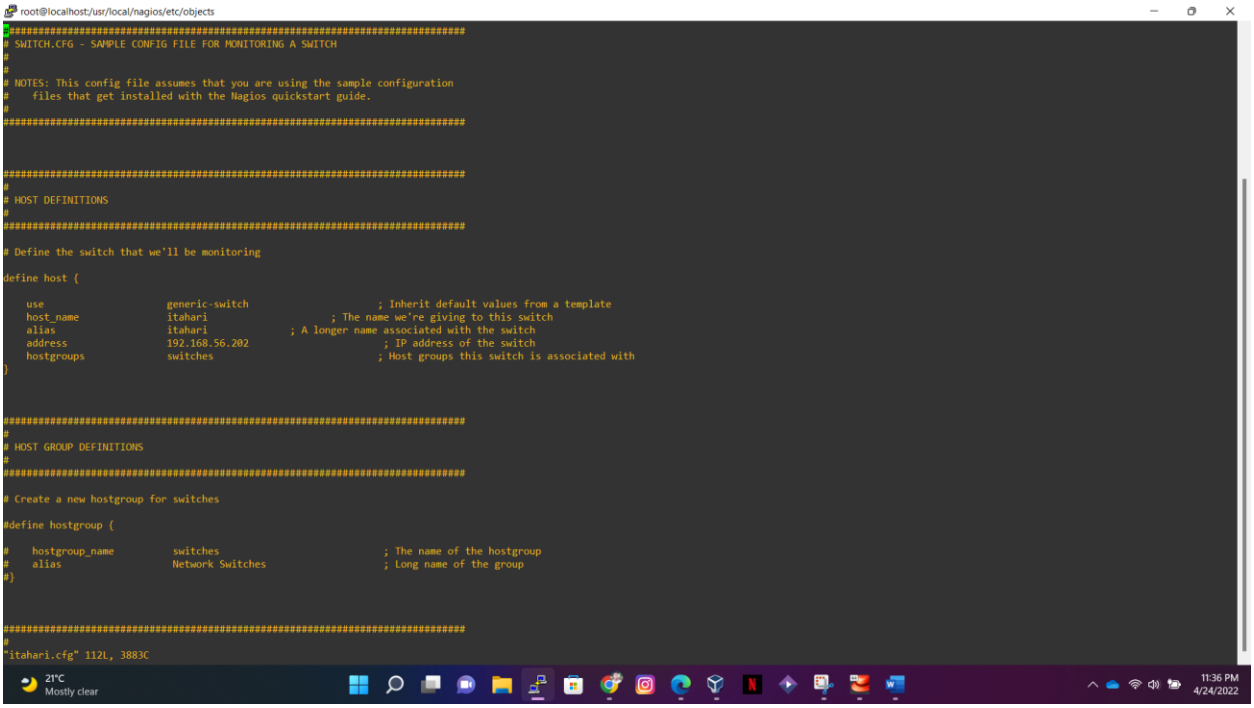


Figure 187 Configuring itahari router and its services in Nagios Server 1

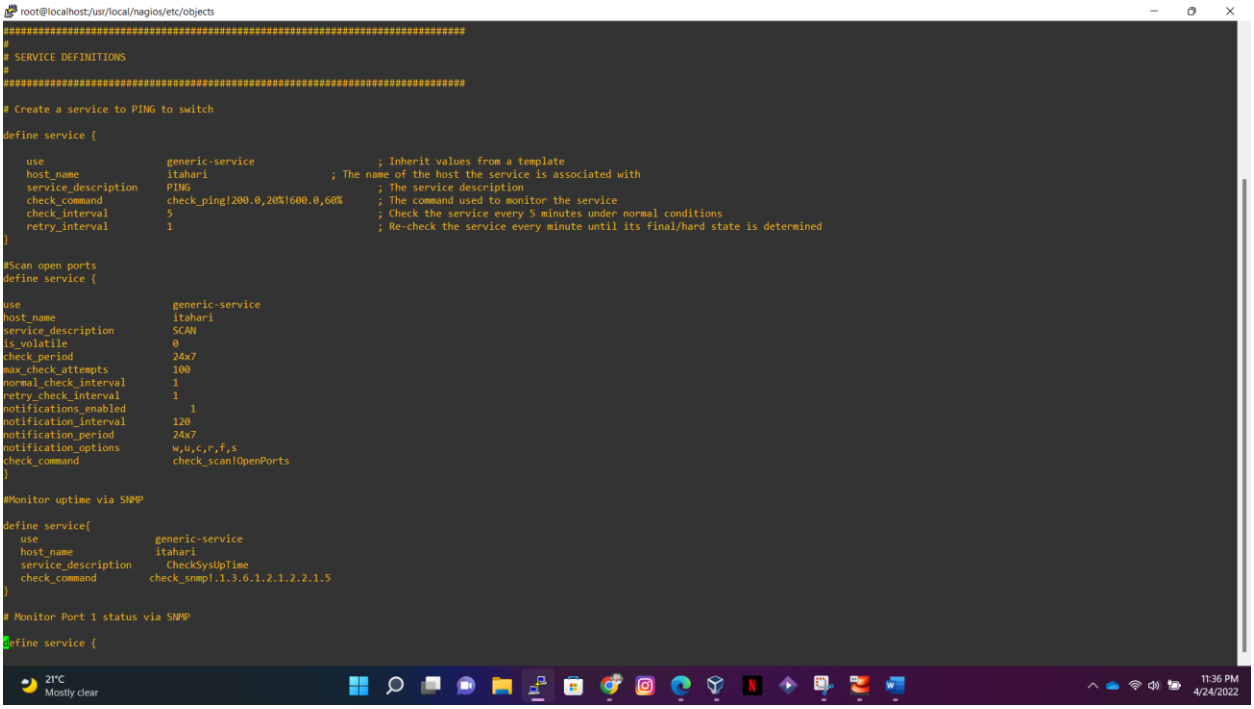


Figure 188 Configuring itahari router and its services in Nagios Server 2

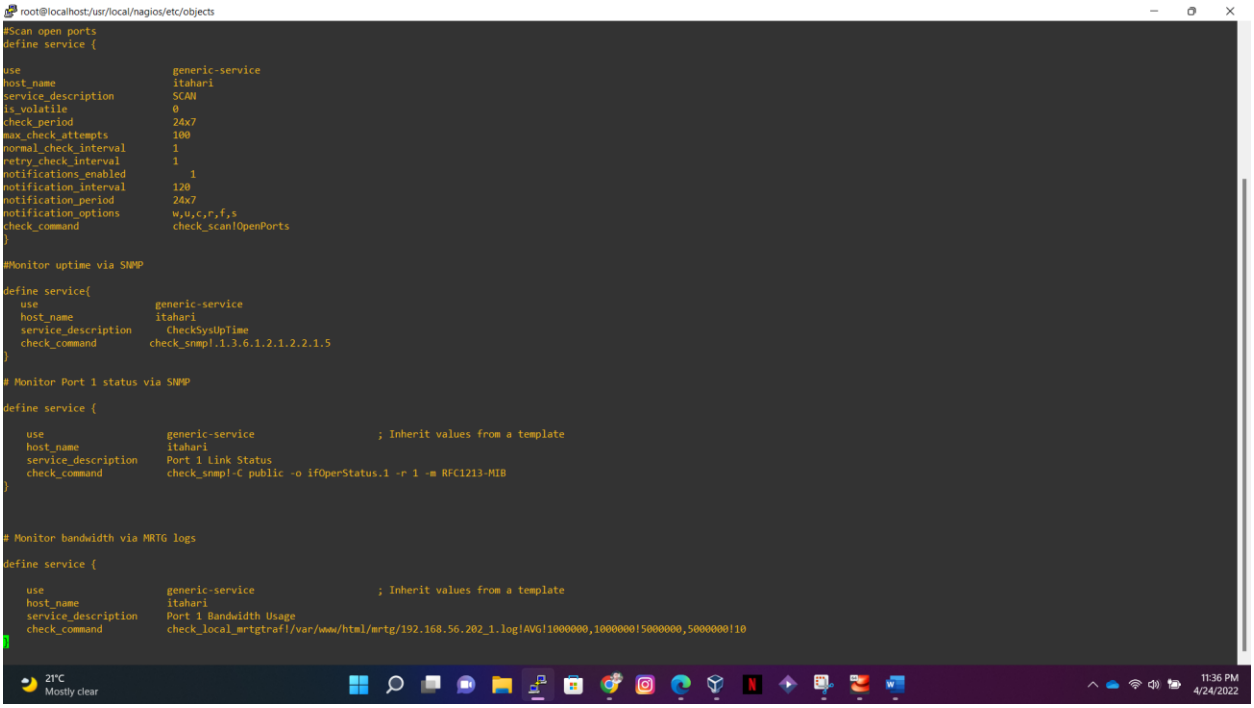


Figure 189 Configuring itahari router and its services in Nagios Server 3

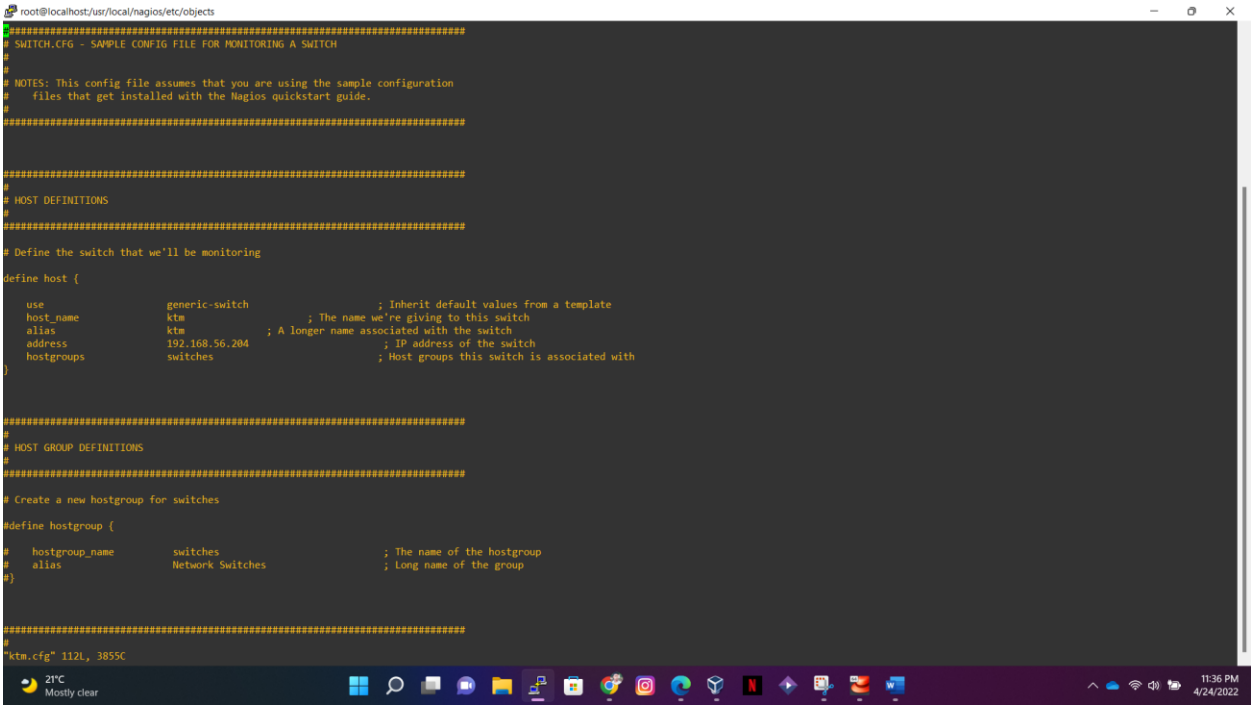


Figure 190 Configuring ktm router and its services in Nagios Server 1

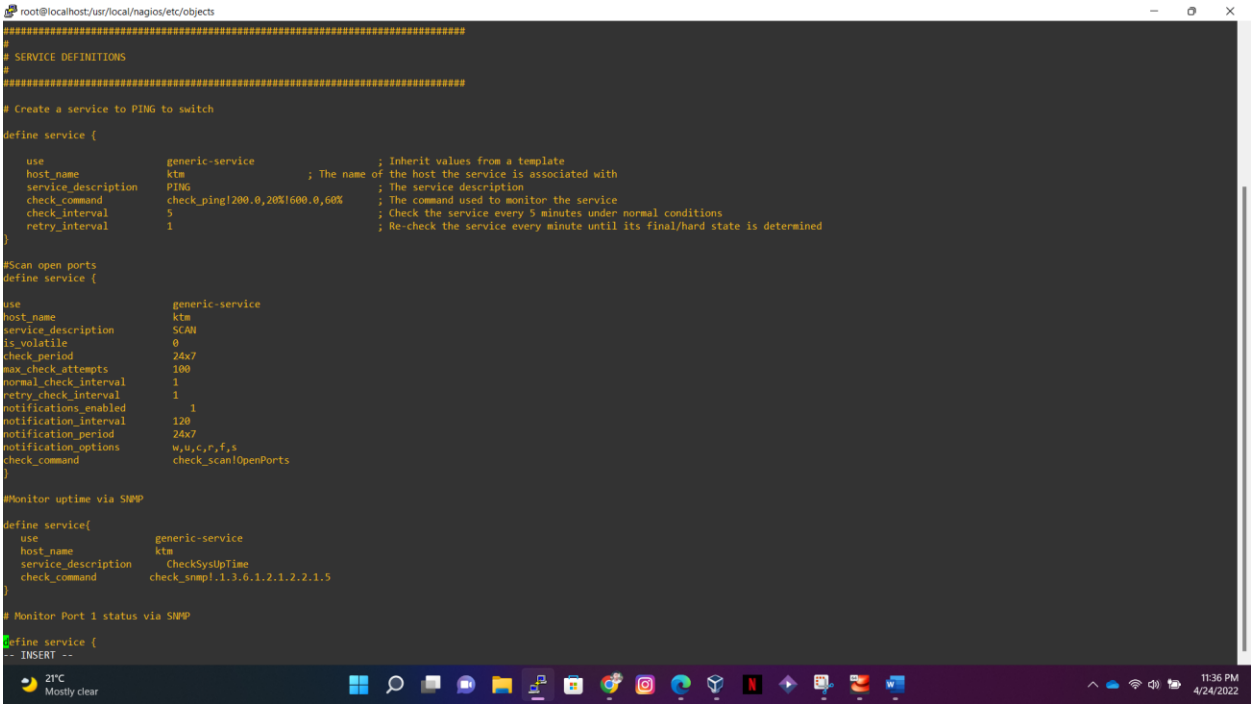


Figure 191 Configuring ktm router and its services in Nagios Server 2

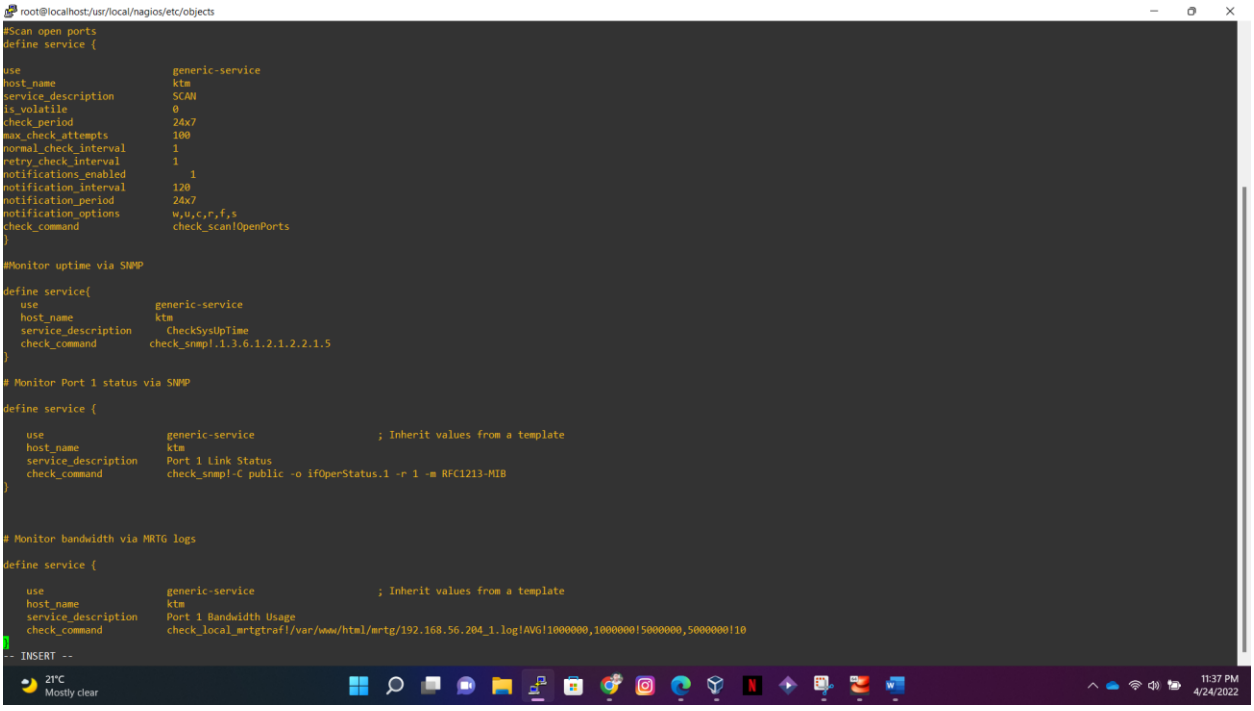


Figure 192 Configuring ktm router and its services in Nagios Server 3

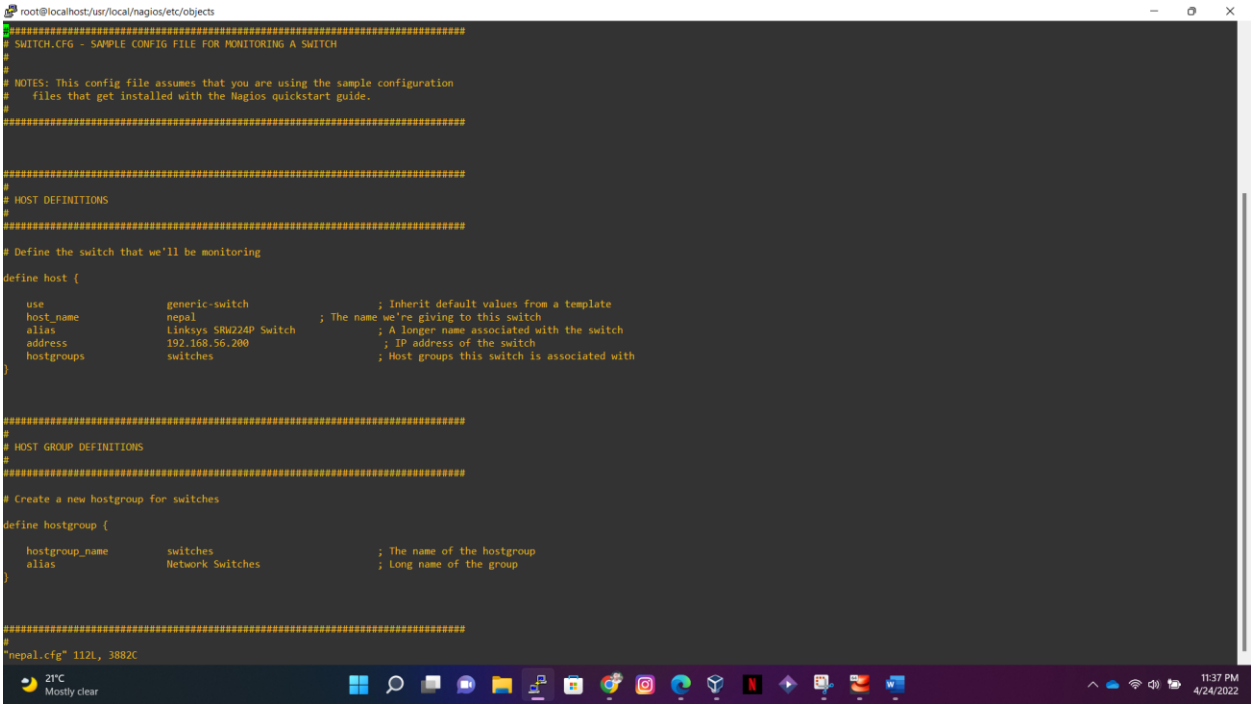


Figure 193 Configuring nepal router and its services in Nagios Server 1

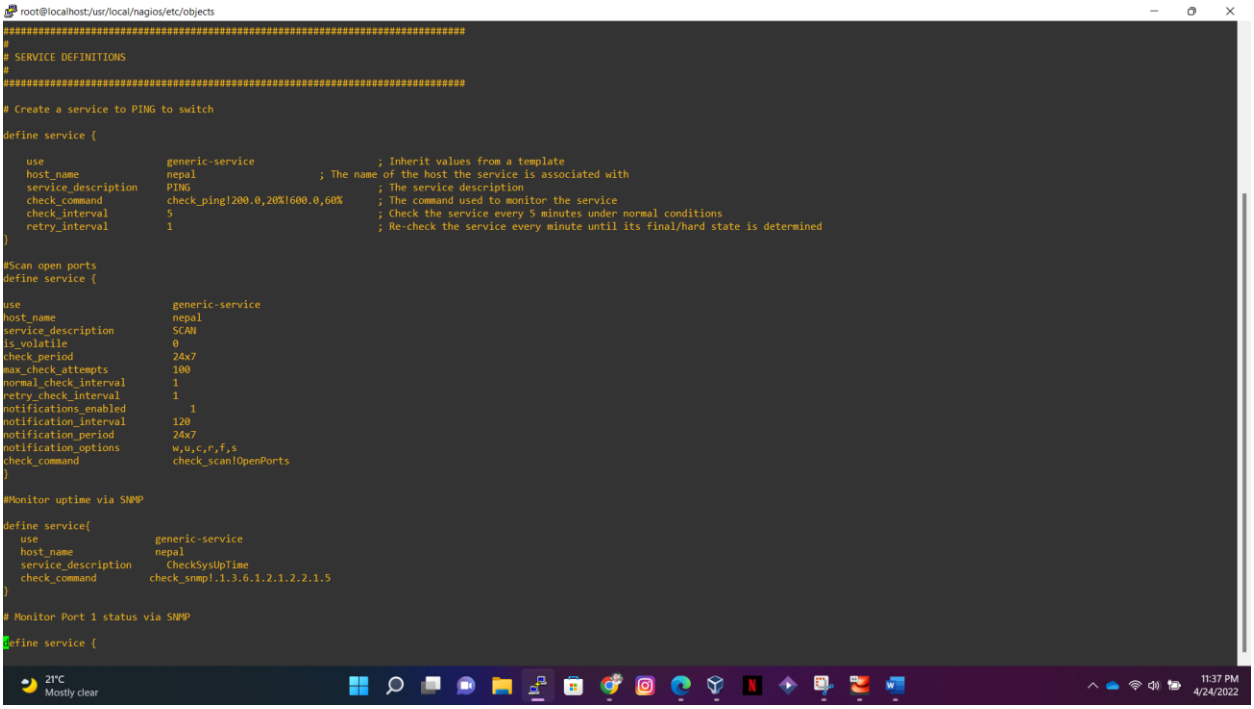


Figure 194 Configuring nepal router and its services in Nagios Server 2

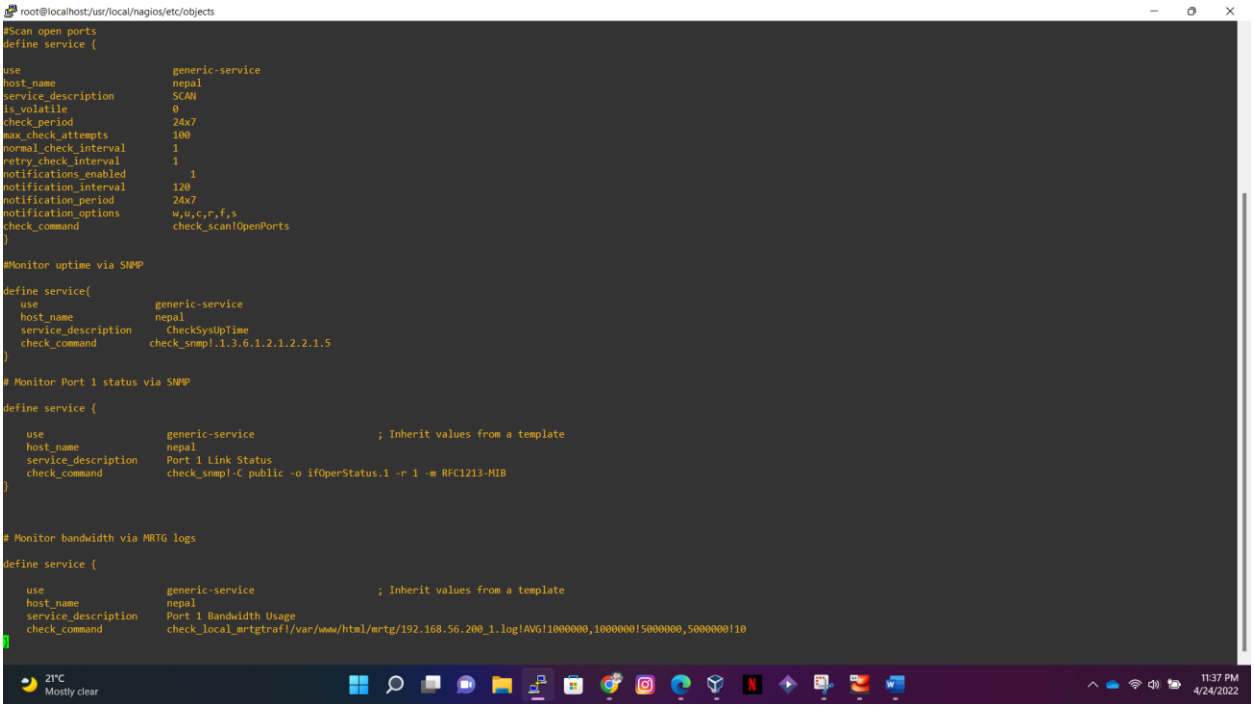


Figure 195 Configuring nepal router and its services in Nagios Server 3

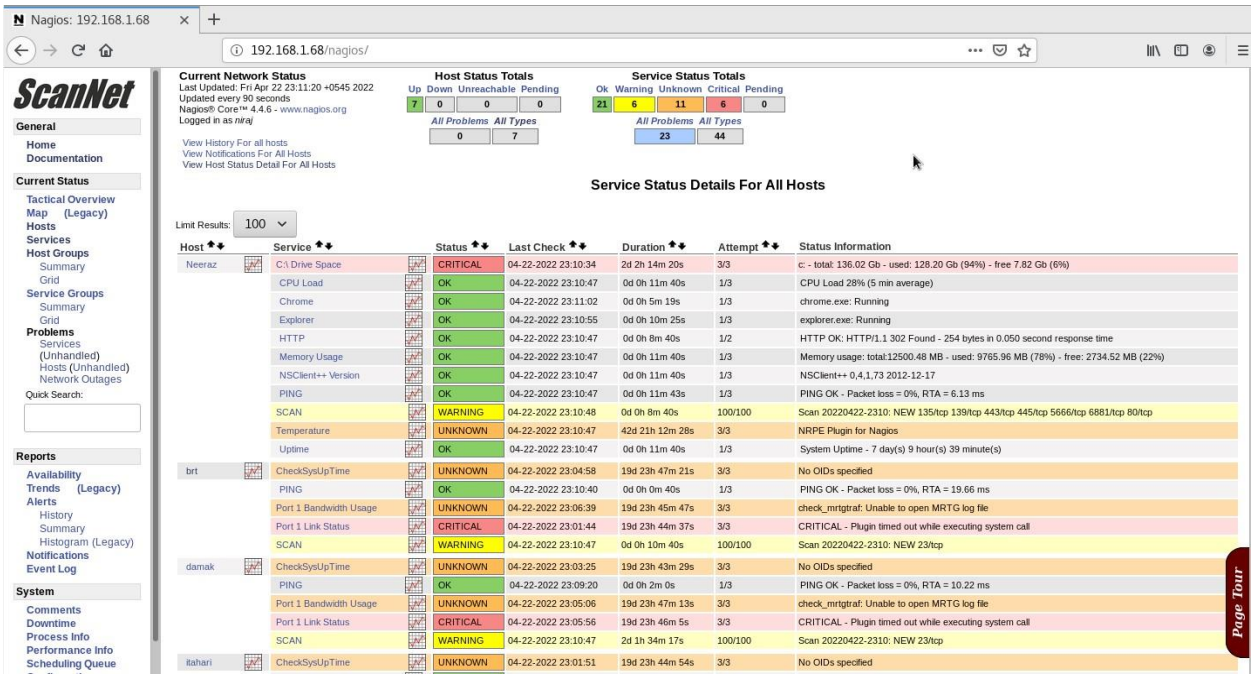
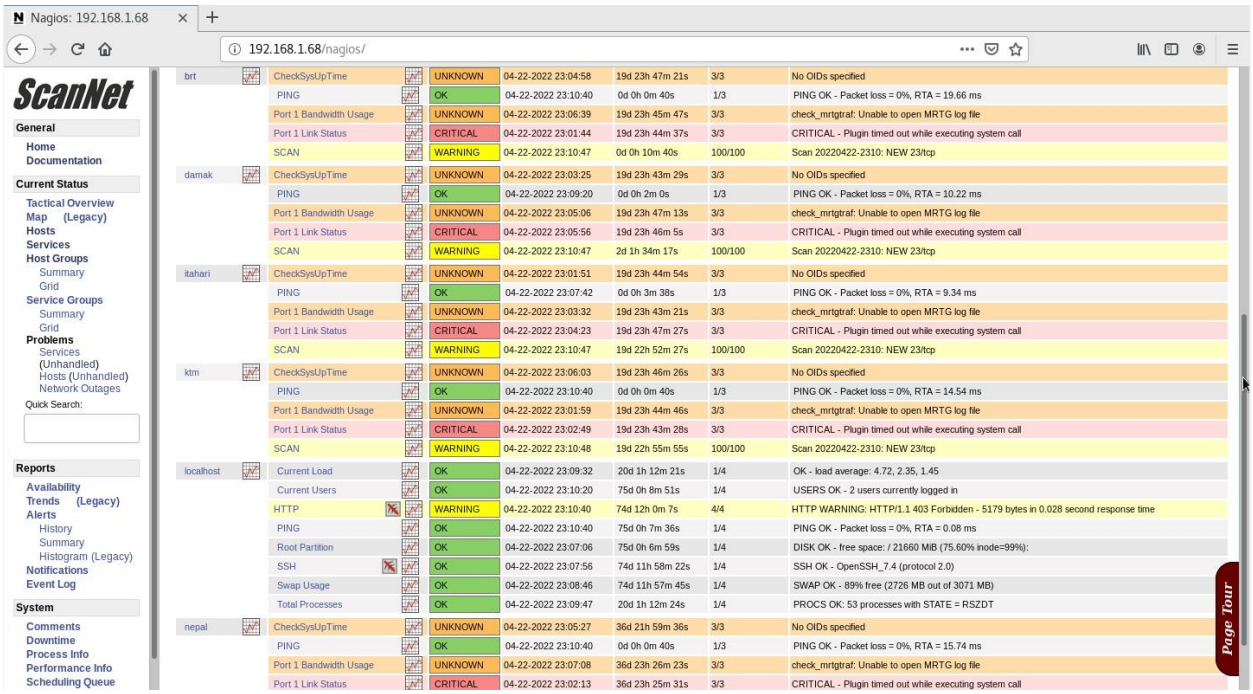


Figure 196 Displaying all the host and services in Nagios dashboard that are configured in Nagios Server 1



brt	CheckSysUpTime	UNKNOWN	04-22-2022 23:04:58	19d 23h 47m 21s	3/3	No OIDs specified
	PING	OK	04-22-2022 23:10:40	0d 0h 0m 40s	1/3	PING OK - Packet loss = 0%, RTA = 19.66 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-22-2022 23:06:39	19d 23h 45m 47s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-22-2022 23:01:44	19d 23h 44m 37s	3/3	CRITICAL - Plugin timed out while executing system call
	SCAN	WARNING	04-22-2022 23:10:47	0d 0h 10m 40s	100/100	Scan 20220422-2310: NEW 23/tcp
damak	CheckSysUpTime	UNKNOWN	04-22-2022 23:03:25	19d 23h 43m 29s	3/3	No OIDs specified
	PING	OK	04-22-2022 23:09:20	0d 0h 2m 0s	1/3	PING OK - Packet loss = 0%, RTA = 10.22 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-22-2022 23:05:06	19d 23h 47m 13s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-22-2022 23:05:56	19d 23h 46m 5s	3/3	CRITICAL - Plugin timed out while executing system call
	SCAN	WARNING	04-22-2022 23:10:47	2d 1h 34m 17s	100/100	Scan 20220422-2310: NEW 23/tcp
itahari	CheckSysUpTime	UNKNOWN	04-22-2022 23:01:51	19d 23h 44m 54s	3/3	No OIDs specified
	PING	OK	04-22-2022 23:07:42	0d 0h 3m 38s	1/3	PING OK - Packet loss = 0%, RTA = 9.34 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-22-2022 23:03:32	19d 23h 43m 21s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-22-2022 23:04:23	19d 23h 47m 27s	3/3	CRITICAL - Plugin timed out while executing system call
	SCAN	WARNING	04-22-2022 23:10:47	19d 22h 52m 27s	100/100	Scan 20220422-2310: NEW 23/tcp
ktm	CheckSysUpTime	UNKNOWN	04-22-2022 23:06:03	19d 23h 46m 26s	3/3	No OIDs specified
	PING	OK	04-22-2022 23:10:40	0d 0h 0m 40s	1/3	PING OK - Packet loss = 0%, RTA = 14.54 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-22-2022 23:01:59	19d 23h 44m 46s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-22-2022 23:02:49	19d 23h 43m 28s	3/3	CRITICAL - Plugin timed out while executing system call
	SCAN	WARNING	04-22-2022 23:10:48	19d 22h 55m 55s	100/100	Scan 20220422-2310: NEW 23/tcp
localhost	Current Load	OK	04-22-2022 23:09:32	20d 1h 12m 21s	1/4	OK - load average: 4.72, 2.35, 1.45
	Current Users	OK	04-22-2022 23:10:20	75d 0h 8m 51s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	04-22-2022 23:10:40	74d 12h 0m 7s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5179 bytes in 0.028 second response time
	PING	OK	04-22-2022 23:10:40	75d 0h 7m 36s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
	Root Partition	OK	04-22-2022 23:07:06	75d 0h 6m 59s	1/4	DISK OK - free space: / 21660 MiB (75.60% inode=99%):
	SSH	OK	04-22-2022 23:07:56	74d 11h 58m 22s	1/4	SSH OK - OpenSSH_7.4 (protocol 2.0)
	Swap Usage	OK	04-22-2022 23:08:46	74d 11h 57m 45s	1/4	SWAP OK - 89% free (2726 MB out of 3071 MB)
	Total Processes	OK	04-22-2022 23:09:47	20d 1h 12m 24s	1/4	PROCS OK: 53 processes with STATE = RSZDT
nepal	CheckSysUpTime	UNKNOWN	04-22-2022 23:05:27	36d 21h 59m 36s	3/3	No OIDs specified
	PING	OK	04-22-2022 23:10:40	0d 0h 0m 40s	1/3	PING OK - Packet loss = 0%, RTA = 15.74 ms
	Port 1 Bandwidth Usage	UNKNOWN	04-22-2022 23:07:08	36d 23h 26m 23s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	04-22-2022 23:02:13	36d 23h 25m 31s	3/3	CRITICAL - Plugin timed out while executing system call

Figure 197 Displaying all the host and services in Nagios dashboard that are configured in Nagios Server 2

8.4.3. Configuration made inside NSClient++ for monitoring windows host and logs.

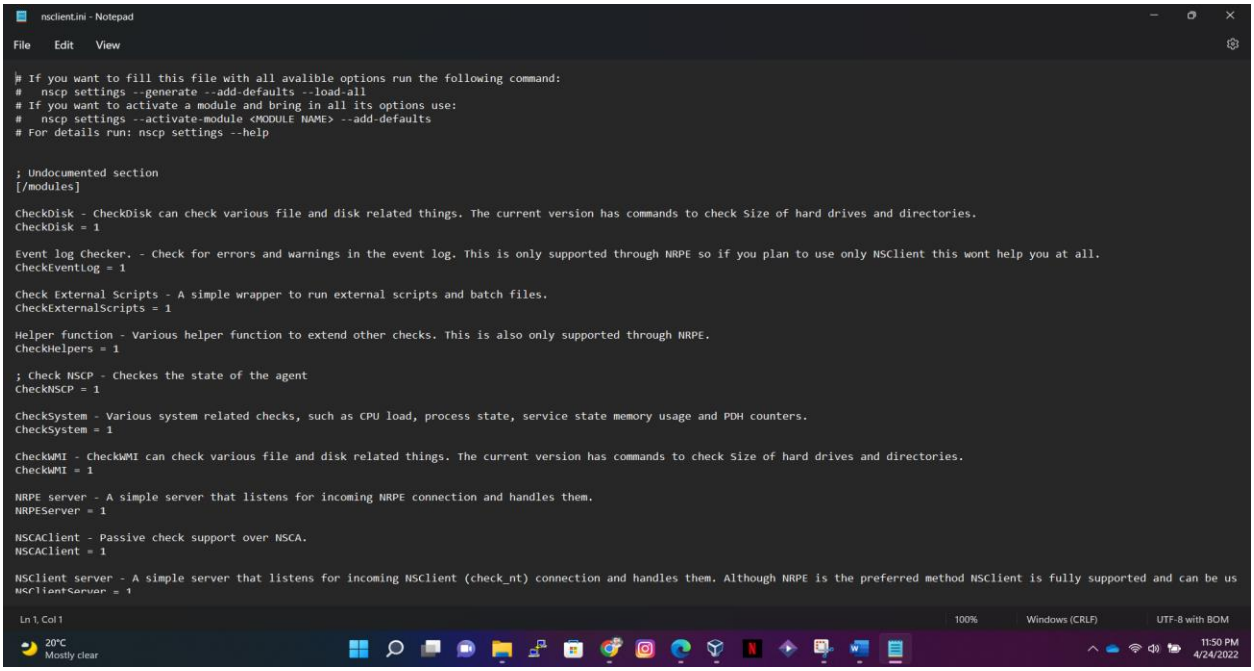


Figure 198 Configurations done inside nsclient.ini 1

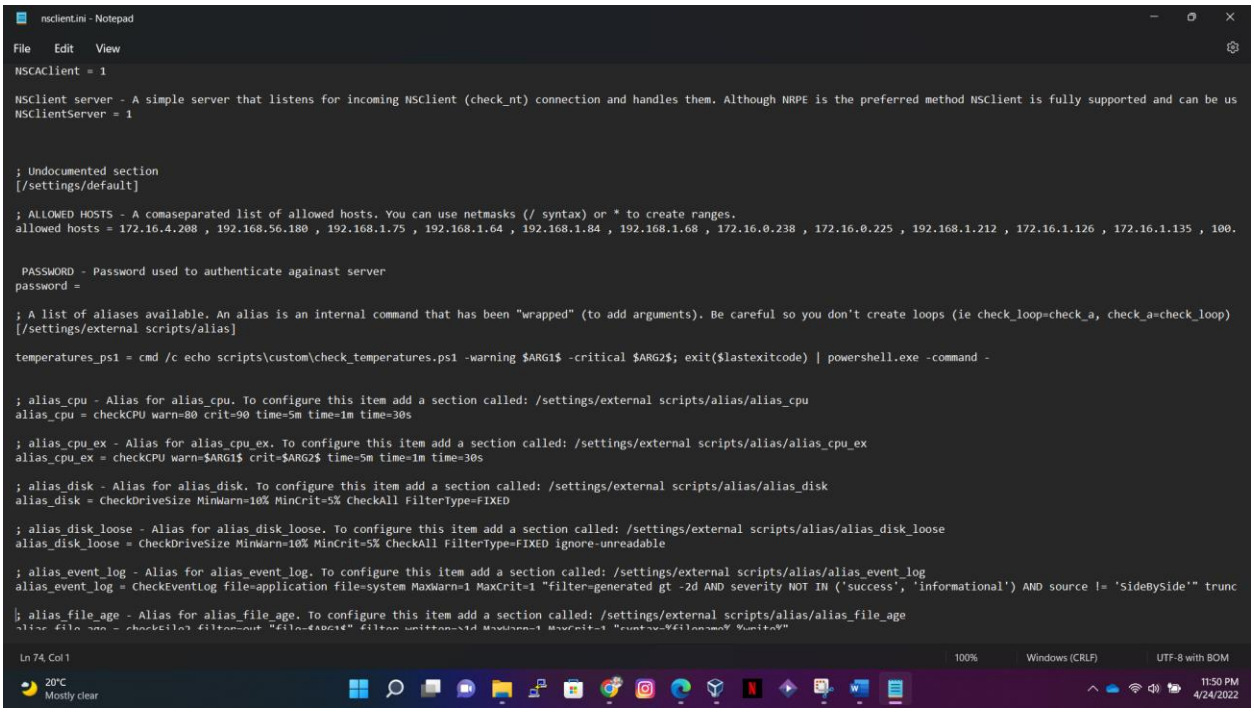


Figure 199 Configurations done inside nsclient.ini 2

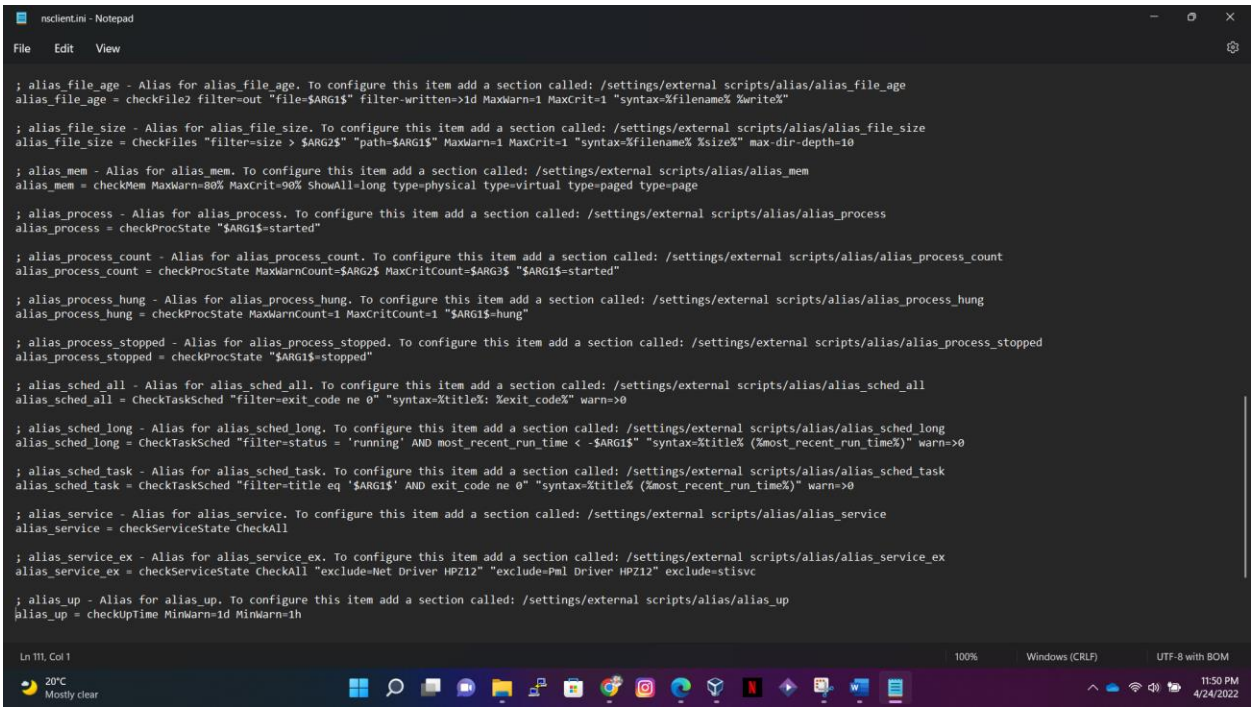


Figure 200 Configurations done inside nsclient.ini 3

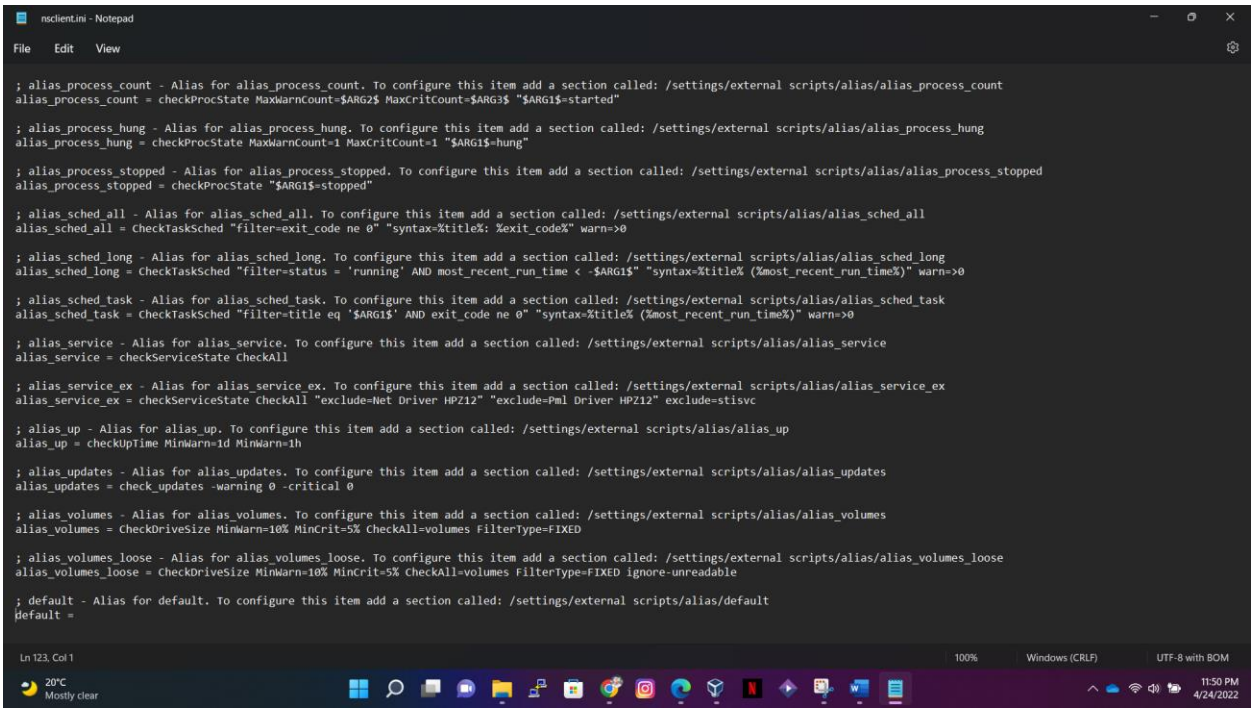


Figure 201 Configurations done inside nsclient.ini 4

8.4.4. Sample code for the Port Scanning feature.

root@localhost:/usr/local/nagios/libexec

```
[root@localhost libexec]# cat check_scan.sh
#!/bin/sh

# check_scan.sh
# works as a nagios plugin to do an nmap scan of a system
# The difference between this script and what I've seen elsewhere
# is check_scan.sh provides a baseline of scan data for comparison.
# Dependencies: nmap, nagios, linux

# - - - - - - - - - SET THESE VARIABLES - - - - - - - - - - - -
BASEDIR=/etc/nagios/scancheck #where to keep everything
#must be nagios user writable
NMAPPATH=/usr/bin #where is nmap
#-------------------------------------------------------------

#note... to run manually, you have to supply a dummy
#argument 1, since the ip address is arg2

IP=$2

if [ ! "$IP" ]; then    #if the ip is not verified

  echo "No IP address supplied"         #if the ip is not verified then display
no ip message
```

Figure 202 check_scan.sh code for port scanning 1

root@localhost:/usr/local/nagios/libexec

```
  exit 0

fi


SCANDIR=$BASEDIR/scans          #directory of the scan
FILEDIR=$BASEDIR/files          #directory of the files
CHANGED=0
INITIAL=0


if [ ! -d $BASEDIR ]; then

  mkdir $BASEDIR        #make base directory if -d basedir is provided

fi


if [ ! -d $SCANDIR ]; then

  mkdir $SCANDIR        #make scan directory if -d scandir is provided

fi
```

Figure 203 check_scan.sh code for port scanning 2

root@localhost:/usr/local/nagios/libexec

```
if [ ! -d $FILEDIR ]; then

  mkdir $FILEDIR        #make file directory if -d filedir is provided

fi


if [ ! -f $SCANDIR/$IP.base ]; then

  touch $SCANDIR/$IP.base       #display all the open ports stored inside IP.bas
e
  INITIAL=1

fi

SCANTIME=`/bin/date +%Y%m%d-%H%M`

/usr/bin/nmap -sT -P0 $IP | /bin/grep -w open | \
/usr/bin/sort > $SCANDIR/$IP

DIFF=`/usr/bin/comm -23 $SCANDIR/$IP $SCANDIR/$IP.base`

if [ "$DIFF" ]; then
```

Figure 204 check_scan.sh code for port scanning 3

root@localhost:/usr/local/nagios/libexec

```
if [ "$DIFF" ]; then

  CHANGED=1
  DIFFSTR=`echo "$DIFF" | /usr/bin/awk '{print $1}' | \
    /usr/bin/paste -s -d " " -`

fi

if [ $INITIAL -eq 1 ]; then

  /bin/cat $SCANDIR/$IP > $SCANDIR/$IP.base     #combine both scandir IP and IP.
base for displaying the ports
  echo "Initial scan"
  exit 0

fi

if [ $CHANGED -eq 1 ]; then

  echo "Scan $SCANTIME: NEW $DIFFSTR"   #display all the open ports after doint
cat IP > IP.base
  exit 1

else
```

Figure 205 check_scan.sh code for port scanning 4

root@localhost:/usr/local/nagios/libexec

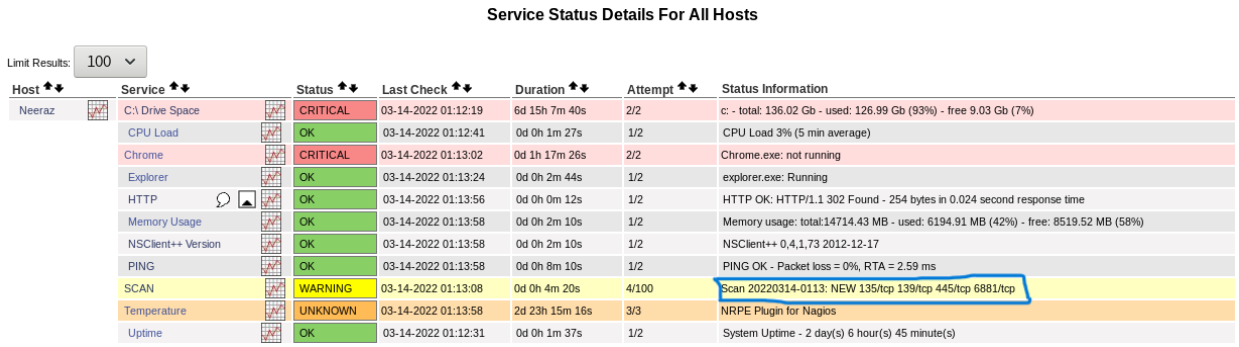
```
if [ $INITIAL -eq 1 ]; then

  /bin/cat $SCANDIR/$IP > $SCANDIR/$IP.base     #combine both scandir IP and IP.
base for displaying the ports
  echo "Initial scan"
  exit 0

fi

if [ $CHANGED -eq 1 ]; then

  echo "Scan $SCANTIME: NEW $DIFFSTR"   #display all the open ports after doint
cat IP > IP.base
  exit 1

else

  echo "$SCANTIME: no change"   #output all the ports
  exit 0

fi

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 206 check_scan.sh code for port scanning 5

niraj@localhost:/usr/local/nagios/libexec

```
[root@localhost libexec]# ./check_scan.sh -H 192.168.1.75
Scan 20220314-0106: NEW 135/tcp 139/tcp 445/tcp 6881/tcp
[root@localhost libexec]#
```

Figure 207 check_scan.sh working fine and displaying all open ports



Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Neeraz	C:\ Drive Space	CRITICAL	03-14-2022 01:12:19	6d 15h 7m 40s	2/2	c: - total: 136.02 Gb - used: 126.99 Gb (93%) - free 9.03 Gb (7%)
	CPU Load	OK	03-14-2022 01:12:41	0d 0h 1m 27s	1/2	CPU Load 3% (5 min average)
	Chrome	CRITICAL	03-14-2022 01:13:02	0d 1h 17m 26s	2/2	Chrome.exe: not running
	Explorer	OK	03-14-2022 01:13:24	0d 0h 2m 44s	1/2	explorer.exe: Running
	HTTP	OK	03-14-2022 01:13:56	0d 0h 0m 12s	1/2	HTTP OK: HTTP/1.1 302 Found - 254 bytes in 0.024 second response time
	Memory Usage	OK	03-14-2022 01:13:58	0d 0h 2m 10s	1/2	Memory usage: total:14714.43 MB - used: 6194.91 MB (42%) - free: 8519.52 MB (58%)
	NSClient++ Version	OK	03-14-2022 01:13:58	0d 0h 2m 10s	1/2	NSClient++ 0,4,1,73 2012-12-17
	PING	OK	03-14-2022 01:13:58	0d 0h 8m 10s	1/2	PING OK - Packet loss = 0%, RTA = 2.59 ms
	SCAN	WARNING	03-14-2022 01:13:08	0d 0h 4m 20s	4/100	Scan 20220314-0113: NEW 135/tcp 139/tcp 445/tcp 6881/tcp
	Temperature	UNKNOWN	03-14-2022 01:13:58	2d 23h 15m 16s	3/3	NRPE Plugin for Nagios
	Uptime	OK	03-14-2022 01:12:31	0d 0h 1m 37s	1/2	System Uptime - 2 day(s) 6 hour(s) 45 minute(s)

Figure 208 check_scan.sh working fine and displaying all open ports in Nagios dashboard

8.5. Appendix E: Designs

8.5.1. Gantt Chart

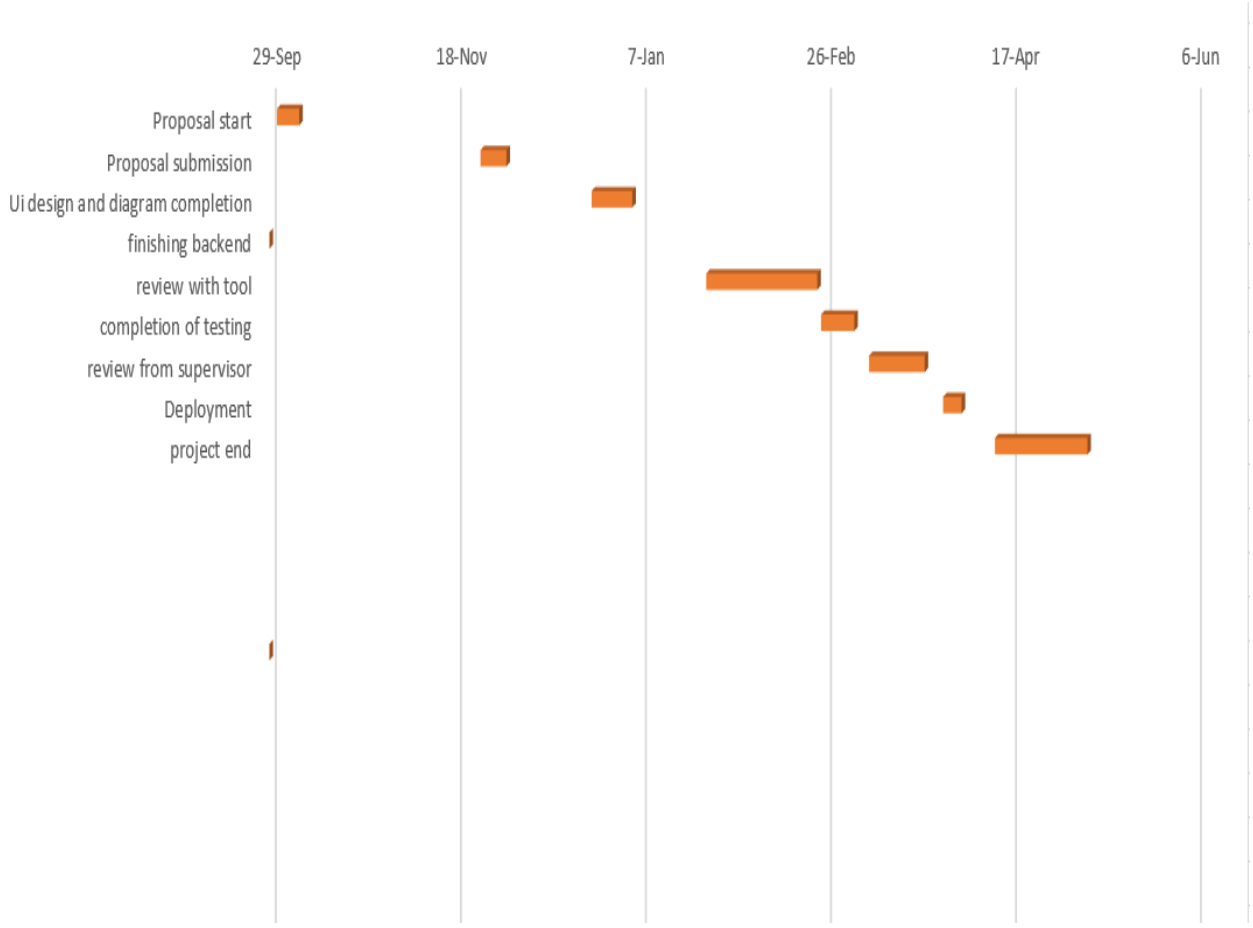


Figure 209 Gantt Chart

8.5.2. Work Breakdown Structure

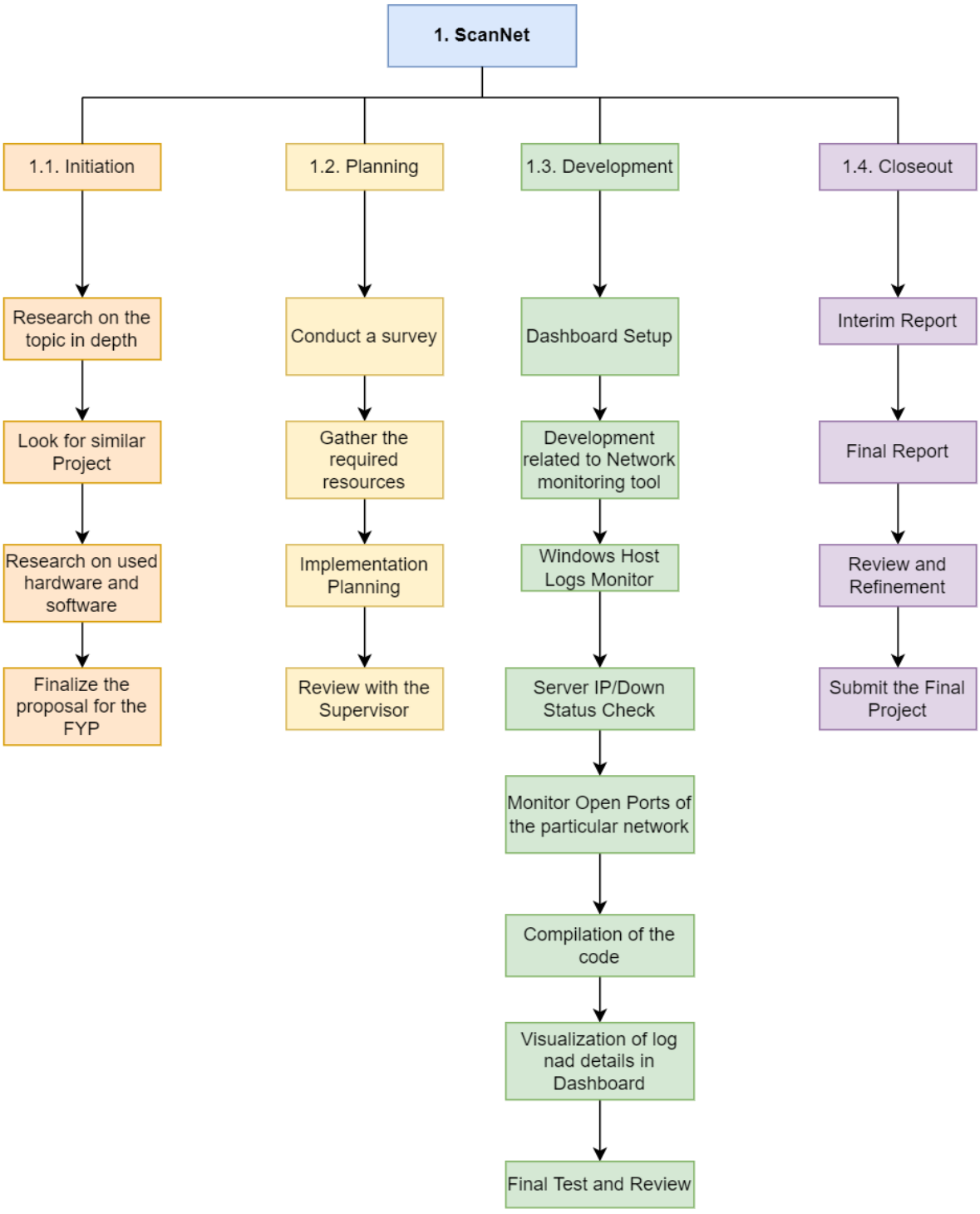


Figure 210 Work Breakdown Structure

8.6. Appendix F: Screenshots of the System

Screenshot of the system can be seen from the following link:

3.7.1. Primary Components

8.7. Appendix G: User Feedback

8.7.1. User feedback form

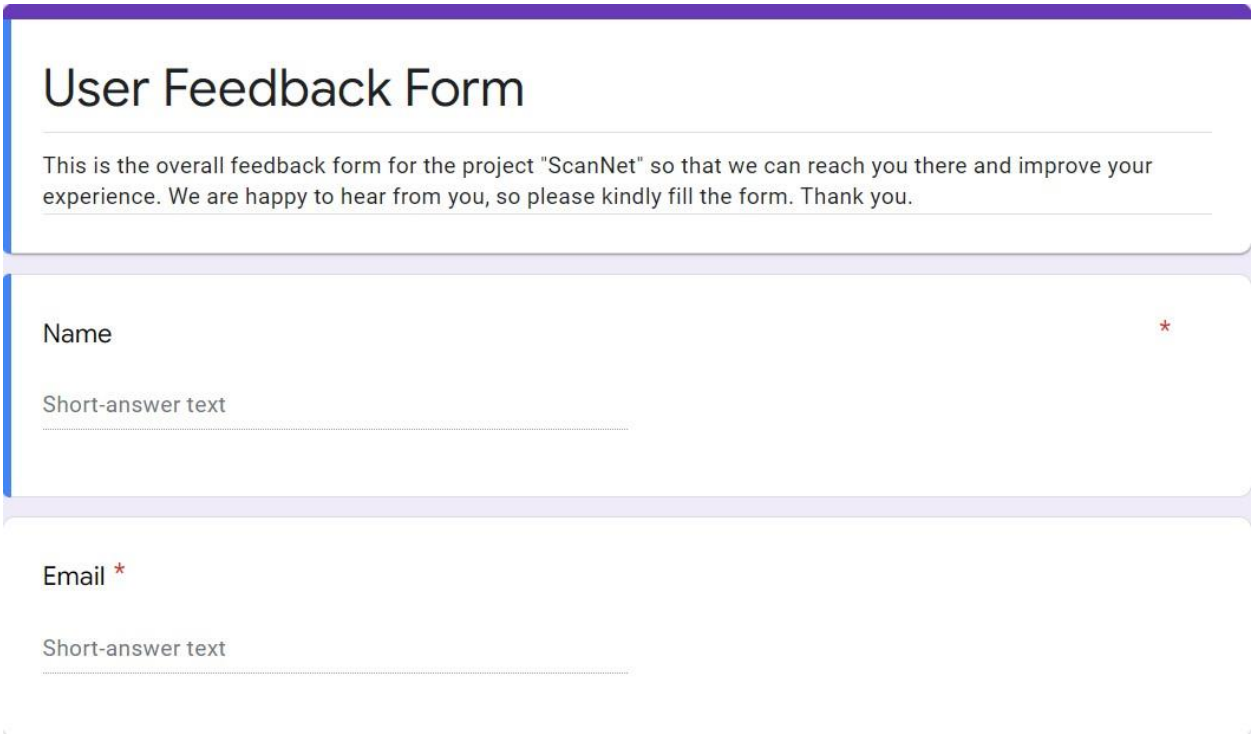


Figure 211 User Feedback Form 1

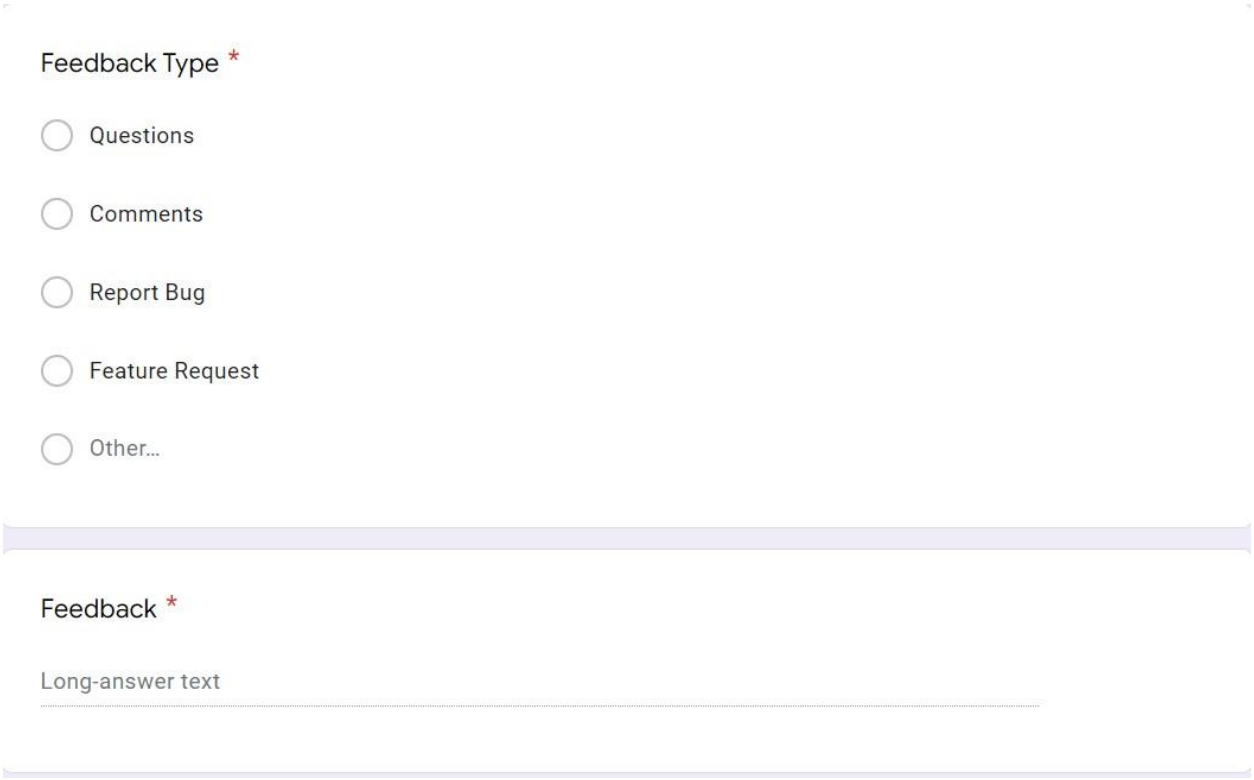


Figure 212 User Feedback Form 2

Figure 213 User Feedback Form 3

8.7.2. Sample of Filled User Feedback Form

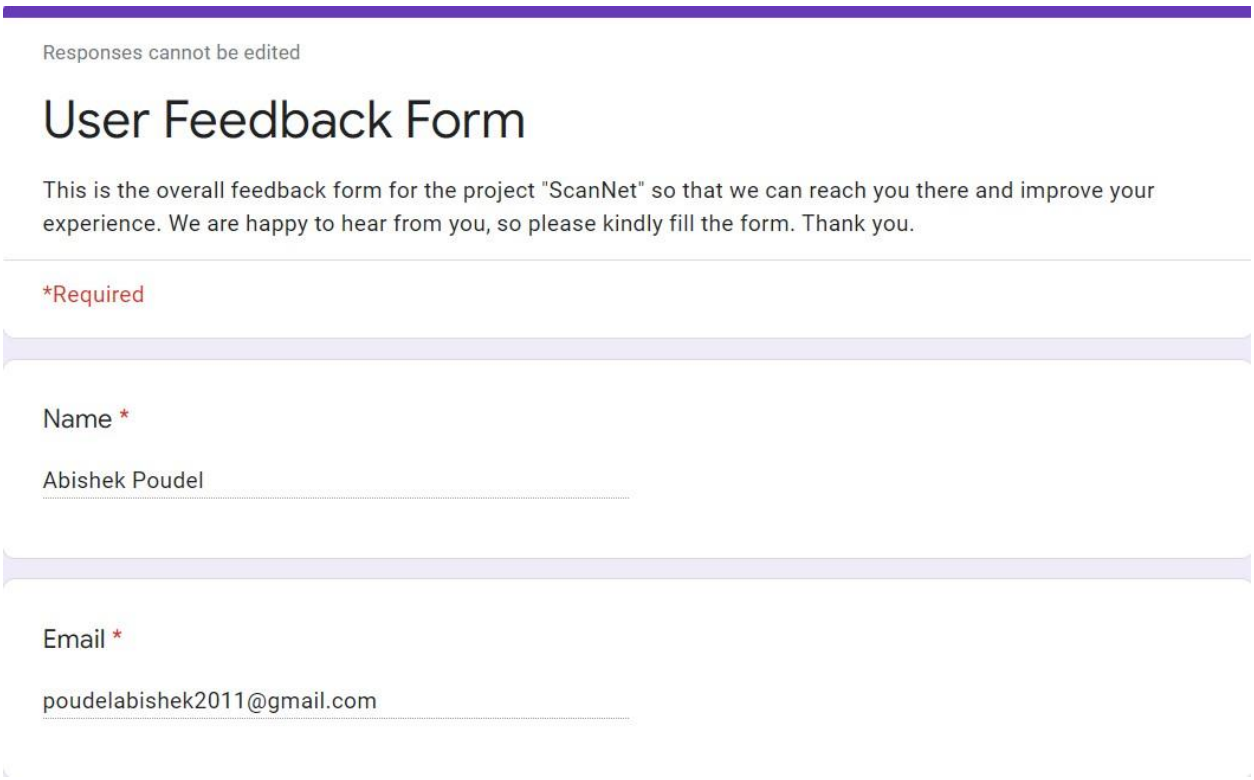


Figure 214 User feedback sample figure 1

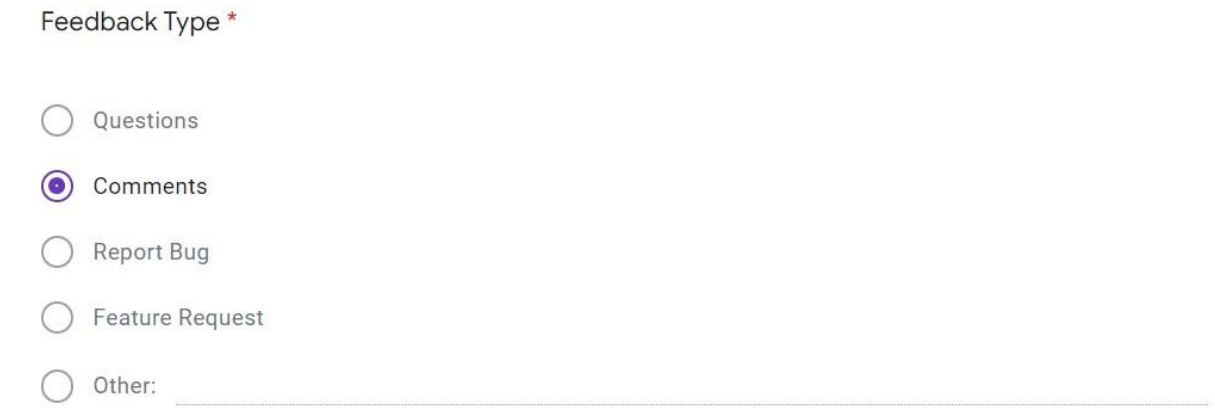


Figure 215 User feedback sample figure 2

Feedback *

The overall system developed by Mr. Niraj Guragain is very clear and important in network monitoring. The system is user-friendly, cost-effective, reliable and very easy to use. All the features implemented in the system are perfect and working. The Windows hosts and services logs monitoring feature and port scanning features are quite effective and helpful for our business organizations. This system will help us to monitor our internal and external networks and also help us to build good relations with customers. The port scanning feature implemented in the system is very good in protecting our organizations from various cyber threats. This will also help us to give an incident response plan to those threats in real-time.

Suggestion for improvement *

The port scanning and graphing features implemented in the system are very useful for now, but it would be much better if we could get temperatures of all the Windows host servers, routers, switches, and other different network devices. Thank you very much.

Figure 216 User feedback sample figure 3

8.8. Appendix H: Future Work

8.8.1. Readings For Future Work

The more details of future work are given below:

- **Phone-based alerting for improved security notifications in real time, SMS can be used.**

  The system just sends an email alert to the admin but adding features like SMS alerts might make the system more efficient since it would warn a user at the very next step and allow them to take Incident Action at the very same time.

- **To store additional logs and resolve dashboard crashes and hangs, enough RAM and storage device may be installed.**

  The current system lacks sufficient RAM and storage capacity, however future development might address the issue of dashboard crashes and hangs by adding sufficient RAM and storage.

- **Long-term data retention can be accomplished using big data architecture and unlimited scalability technologies.**

  When a system generates a big volume of syslog that is sophisticated, the syslog server may be unaware of it. As a result, deploying big data infrastructure and infinite scalability technologies will assist in the resolution of these issues as well as the long-term storage of data.

- **In order for additional corporate personnel to access the dashboard, user access control and group policy can be created.**

  Using features like User Access Control and Group Policy, additional employees may access the dashboard and system at the same time. This might also offer an additional degree of protection by granting different levels of access to the system.

- **By comparing older data with current data in the system, machine learning and artificial intelligence approaches may be utilized to detect unknown patterns.**

  By comparing historical and present threats in the system, machine learning and artificial intelligence approaches might be more successful in finding undiscovered patterns and anomaly detection.

- **In the future, features to monitor the temperature of various servers and hosts might be added.**

  By using the same Perl Programming language or python programming language in future we can write a code and make a plugin to also scan the temperature of the different windows host server and other different networking devices.

8.9. Appendix I: Progress Review Table

SN	Task	Status	Progress (%)
1	Topic Selection	Completed	100%
2	Research on similar projects	Completed	100%
3	Technical Research	Partially Completed	100%
4	Finalize Proposal	Completed	100%
5	Conduct a Pre-Survey	Completed	100%
6	Finalize Interim report	Completed	100%
7	Develop ScanNet by adding different new features on it (Network Monitoring Tool)	Completed	100%
8	Compilation and testing	Completed	100%
9	Optimize Software	Completed	100%
10	Testing	Completed	100%
11	Conduct a Post-Survey	Completed	100%
11	Final FYP Report	Completed	100%
12	Review and refinement	Completed	100%

Table 23 Progress Review Table

9. Milestones

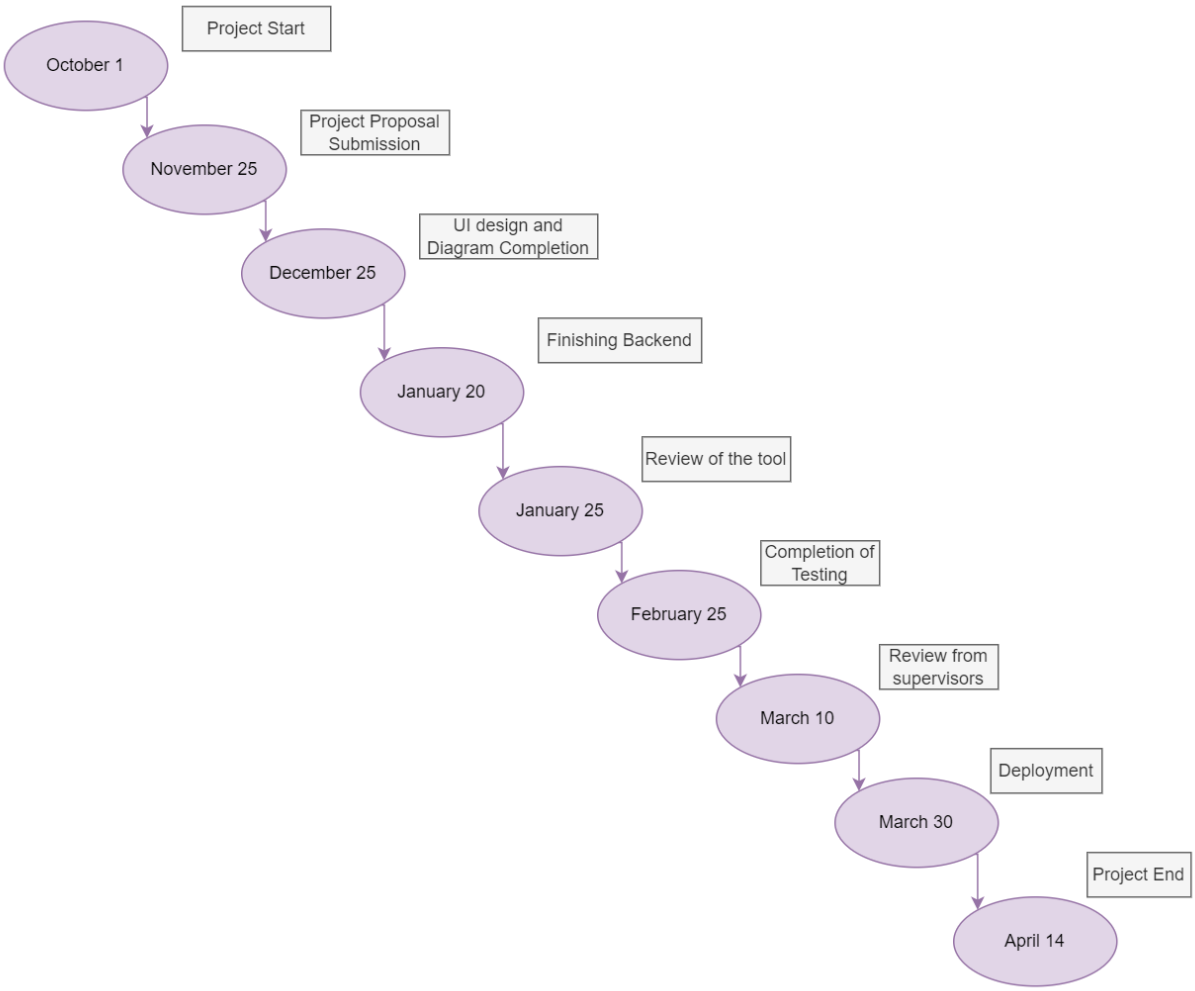


Figure 217 Milestones of the project