FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

SEMESTER 1 2021/2022

BITU3923 – WORKSHOP II

FINAL REPORT BITZ

GROUP 7: CYBER GUARD

PREPARED BY:

No	Student Name	Matric Number
1	Muhammad Izham bin Norhamadi	B032020039
2	Ooi Chiou Xiang	B032010388
3	Izzatul Hanani binti Kamarul Nizar	B031910032
4	Siti Aishah binti Mustafa	B031910420

SUPERVISOR'S NAME: PUAN KHADIJAH BINTI WAN MOHD GHAZALI

ACKNOWLEDGEMENTS

First of all, we would like to thank our supervisor, Puan Khadijah Binti Wan Mohd Ghazali, for her valuable guidance and advice. She inspired us to work on this project. Her willingness to motivate us contributed tremendously to our project. Also, we would like to thank our seniors and friends for showing us some examples related to the services in our project where it helped us a lot to understand each of the services, which allowed us to complete our project. We would also like to thank our evaluator for taking the time to evaluate our project. This evaluation gave us a deeper understanding of our services and network infrastructure.

Besides that, we would like to thank the authority of Universiti Teknikal Malaysia Melaka (UTeM) for providing us with good facilities to complete this project, such as a VNC connection. Finally, an honourable mention goes to our families for their understanding and support in completing this project. With the help mentioned above, we completed our project successfully.

ABSTRACT

In the Workshop II project, we must define, design, implement, and manage tasks that start from selecting a leader or project manager to lead this project from the beginning of the project. A task has been given to each member. It is essential to manage and organize every task to avoid any problems and errors later on.

Our main objective in this project is to complete the project successfully, and we can go through the challenges faced while completing the task given. We are grateful for this experience as it helped us be more prepared for our industrial training soon.

Our group had decided to use Windows 2012 as VM1, Ubuntu as VM2, and Ubuntu Desktop as VM3. We choose this server because it has many benefits. Our group were assigned to set up 12 services listed in the question. The 12 services listed are Active Directory, IDS with port mirroring and management console, IPsec VPN, Samba & Samba security services, DNS, DHCP, ACL Router, Router Authentication and Authorization (Radius), User authentication by integrating AD, VLAN and Port Security, Windows Server Hardening Vulnerability Report, and Linux Server Hardening Vulnerability Report.

During Workshop II, we faced several problems, such as the GNS3 was not functioning, but we still managed to overcome it and make this project successful.

ABSTRAK

Dalam projek Bengkel II ini, kita perlu menentukan, mereka, melaksanakan, dan menguruskan tugas-tugas yang dimana ia bermula dari memilih ketua atau pengurus projek untuk memimpin projek ini dari mula. Tugas-tugas telah diberikan kepada setiap ahli kumpulan. Ianya sangat penting untuk mengurus dan melaksanakan setiap tugas bagi mengelakkan sebarang masalah dan kesilapan nanti.

Objektif utama kami di dalam projek ini adalah untuk menyiapkan projek ini dengan berjaya dan kami dapat mengatasi segala cabaran yang dihadapi ketika menyelesaikan tugas yang diberi. Kami bersyukur untuk pengalaman ini kerana ia membantu kami untuk lebih bersedia dalam latihan perindustrian kami akan dating.

Kumpulan kami telah memutuskan untuk menggunakan Windows 2012 sebagai VM1, Ubuntu sebagai VM2, dan Desktop Ubuntu sebagai VM3. Kami memilih pelayan ini kerana ia mempunyai banyak kegunaan. Kumpulan kami juga ditugaskan untuk memasang 12 perkhidmatan yang telah disenaraikan di dalam soalan. 12 perkhidmatan yang disenaraikan adalah Active Directory, IDS with port mirroring and management console, IPsec VPN, Samba & Samba security services, DNS, DHCP, ACL Router, Router Authentication and Authorization (Radius), User authentication by integrating AD, VLAN and Port Security, Windows Server Hardening Vulnerability Report, dan Linux Server Hardening Vulnerability Report.

Semasa Bengkel II, kami menghadapi beberapa masalah seperti GNS3 tidak berfungsi dengan baik, tetapi kami masih dapat menangani masalah itu dan membuat projek ini berjaya.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1- Introduction

We have to set up a secure infrastructure that covers all networking functions for internal and external IT communications. This company is expanding its department with approximately 100 employees and setting up a new IT department. It will be divided into two departments: HQ site and Branch site. The HQ site is where the main server is homed and where the clients connect to, while the Branch site is the remote site. The sites are linked with a simple point-to-point internetworking that can be used to carry packets between the sites.

The company also wants to provide several services such as Active Directory, VLAN and Port Security, and more. Twelve services must be set up and running to ensure the entire network infrastructure will work properly. Before installing the services, we must develop and design a proper network design that includes physical and logical structures. We use Windows Server 2012, Ubuntu and Ubuntu for the server operating system as a platform for network implementation.

Twelve services need to be installed and configured such as Active Directory, IDS with port mirroring and management console, IPsec VPN server, Samba and Samba security services, DNS, DHCP, ACL Router, Router Authentication and Authorization (Radius), User authentication by integrating AD with Linux, VLAN and Port Security, Windows Server Hardening Vulnerability Report, and Linux Server Hardening Vulnerability Report. Every group member is assigned with their services.

1.2- Objective

The main objective of this project is to install a network service intro a different operating system server and develop an understanding of networking infrastructure, problem-solving techniques, and the concept of network security design. Besides that, solve a particular problem of twelve services in this network. Below is the list of objectives that uses to develop this project:

1. To ensure the security of the infrastructure that covers all the networking functions for internal and external, comprising several services have been set up.
2. To ensure that the network services infrastructure remains secure.
3. To ensure each staff has sufficient privileges to perform operations and avoid unauthorized use of data.

1.3- Project Planning / Schedule

In week one, we will be assigned to the supervisor, and in week two, we will discuss together to distribute our service tasks for each group member. After that, we start to propose our project to get approval from our supervisor. The proposal includes the details of the project such as introduction, logical and physical network design, Gantt chart, security policy and requirement analysis. We submitted the final proposal for approval at the end of week two. Then, we will contact the supervisor to make the VNC connection between the lab's PC and our laptop or PC so that it will be easier for students to install any software that needs ample storage. We start to install GNS3, VMware, Windows 2012, Ubuntu and Qradar on the PC.

Starting from week three to week five, we set up the services needed for this project. There are eight services that we plan to install during this period. At the same time, we prepare the Progress 1 meeting and logbook that will consist of the details of the setup and installation of the services. From week six to week ten, we plan to set up the four other

services and prepare for Progress 2 meeting that will consist of details. We must complete our project by the end of week eleven and set up the whole network and services required. At the same time, we need to prepare a video and a poster that shows one of the services that has been set up, which is Samba Security Service.

After completing the project, we will demonstrate the task to the supervisor and evaluator. In addition, we will be judged during the poster presentation by the juries. Finally, the completed final report and individual logbook will be submitted during week fifteen in the study week.

1.4- Gantt Chart

This Gantt chart will show the whole activities for this project. The details are shown in the table below:

No	Week / Activities	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
1	Project proposal • Proposal submission • Logbook review 1 • Test connection (VNC)															
2	Progress 1 (40% services must be done) • Progress 1 presentation • Logbook review 2															
3	Progress 2 (ALL services must be done) • Progress 2 presentation • Logbook review 3															
4	Video and poster (one service) • Evaluation and improvement • Submission for video and poster • Logbook review 4															
5	Demo to evaluator (Completed all services) • Progress report 3 presentation • Logbook review															
6	Poster Competition involved juries															
7	Document submission • Final report • Logbook • Peer assessment • Logbook review 5	DURING STUDY WEEK														

Figure 1 Gantt Chart

1.5- Conclusion

In conclusion, we can apply knowledge and experience from the previous subject that we have learnt, such as Operating System, Data Communication and Networking, Computer Network, Network Security Infrastructure and Design, and Network Security Project Management, into this project. In addition, we should understand how the security policy is developed in this project. We have practiced the theory of the entire subject to solve the problem that we been encountered during the development of this project.

Besides that, we have the experience to design the network infrastructure that we can maintain the security of the infrastructure and a good network environment. Plus, we need to realize that planning is essential for good implementation in the project. This process requires good collaboration from all in order to develop a network design with a secured connection.

CHAPTER 2: PROJECT REQUIREMENT

2.1- Introduction

The network that we need to develop will consist of three servers with different operating systems. We will use Windows Server 2012, Ubuntu and Ubuntu Desktop in our project. Furthermore, we need to set up twelve services, and it will distribute among the three servers. Ensuring the network system operates at the desired performance is very important.

2.2- Types of Operating System Used in the Project

An operating system (OS) is a program that manages a computer's resources, especially the allocation of those resources among the other programs. In order to let the user able to gain a good experience when they are operating the computer, high quality of the operating system is needed to integrate the network services to suit the network environment nowadays. Thus, the operating system used in the project are:

1. Windows Server 2012
2. Ubuntu Server
3. Ubuntu Desktop

2.3- Operating System Background

2.3.1- Windows Server 2012

Windows Server 2012 is an operating system built by Microsoft and is the successor of Windows Server 2008. Since September 2012, Windows Server 2012 has been offered as the server edition of Windows 8. Since October 2013, a minor update (Windows Server 2012 R2) has been provided. Various features, such as an updated version of Hyper-V, an IP address management role, a new version of Windows Task Manager, a new file system, were added or improved over Windows Server 2008 R2. Despite having the same controversial Metro-based user interface like Windows 8, Windows Server 2012 generally garnered positive reviews.

2.3.2- Ubuntu Server

Ubuntu is a Debian-based free and open-source Linux distribution. Ubuntu is available in three different editions: Desktop, Server, and Core (for IoT devices and robots). Ubuntu is a popular cloud computing operating system that includes OpenStack compatibility. Every six months, Ubuntu is updated, with long-term support (LTS) updates every two years.

2.3.3- Ubuntu Desktop

Ubuntu Desktop is a free and open-source graphical user interface. Even though it has a graphical user interface (GUI), this Linux distribution relies on the "terminal" command line. The bulk of commands that formerly required a terminal can now be executed using a GUI. Other popular desktop interfaces, such as Windows and Mac, have similar features.

Compared to other distributions, Ubuntu Desktop offers a lot more customisation choices. The "dash" panel and toolbar on the left side of Ubuntu Desktop are known as "dash" (dashboard). A home button appears on the dashboard, followed by customised icons for your favourite programmes.

2.4- Operating System Justification

2.4.1- Windows Server 2012

Windows Server 2012 is the sixth edition of the Windows server, and it is the server version of Windows 8. It is a version of Windows Server 2008 that has been upgraded. It came with several pre-release versions, including a beta version and a developer preview. One of the features that have been used is Server Manager.

Server Manager is a programme that allows you to manage your servers. The new server manager's multi-server capabilities are one of its most notable features since it makes it easier to deploy features and responsibilities remotely to virtual and real servers. A server group can manage many servers at the same time.

2.4.2- Ubuntu Server

Ubuntu Server comes with a variety of packages depending on the needs of the server. Both Apache2 and Bind9 are unique packages. Ubuntu Server packages provide client connectivity while keeping security in mind. As a result, Ubuntu Server can function as a web server, email server, samba server, and file server. In addition, because there is no need to run a desktop environment in Ubuntu Server, resources can be diverted to server activities, resulting in improved system performance.

2.4.3- Ubuntu Desktop

Ubuntu Desktop comes with several general-purpose applications preinstalled, including LibreOffice, an office productivity suite, Firefox, a web browser, and others. Also, the primary difference between Ubuntu Server and Ubuntu Desktop is the desktop environment.

The Ubuntu Desktop comes with several utilities preloaded. There is a list of some Ubuntu Desktop utilities that come preinstalled: Movie Player, LibreOffice, Thunderbird, Firefox, Gedit, Ubuntu One Music Store, and other applications are available. The Software Center also allows you to download various web repositories.

2.5- Hardware Requirement

2.5.1- Windows Server 2012

Windows Server is a server operating system Microsoft specifically created to run servers that provide resources for other computers. Windows Server 2012 requires a 64-bit processor. The table below outlines the minimum and recommended hardware requirements for Windows Server 2012.

Processor	1.4 GHz, x64
Memory	512 MB
Free disk space	32 GB

Table 1 Windows Server 2012 requirement

2.5.2- Ubuntu Server

Installing Ubuntu or Gnu & Linux should simply install a useable system with enough room to be comfortable using the Recommended Minimum System Requirements listed here. A fair "rule of thumb" is that machines that can run Windows XP, Vista, Windows 7, or x86 OS X will almost always be far faster with Ubuntu, even if their specs are lower than those listed below:

Processor	2 GHz dual-core processor
Memory	2 GB RAM (system memory)
Free disk space	25 GB of hard-drive space

Table 2 Ubuntu Server requirement

2.5.3- Ubuntu Desktop

Following are the minimum system requirements for Ubuntu Desktop:

Processor	2 GHz dual-core processor
Memory	4 GB RAM (system memory)
Free disk space	25 GB of hard-drive space

Table 3 Ubuntu Desktop requirement

2.6- Hardware Justification

2.6.1- Servers

There are three operating systems or servers. The first one will be installed with Windows Server 2012. Then, the next one will be installed with Ubuntu Server, and lastly, the last one will be installed with Ubuntu Desktop.

1) Windows Server 2012
    i. Domain Name System (DNS)
    ii. Active Directory
    iii. Router Authentication and Authorization (Radius)

2) Ubuntu Server
    i. Dynamic Host Configuration Protocol (DHCP)
    ii. IDS
    iii. Samba

3) Ubuntu Desktop
    i. Integrate AD with Linux

2.6.2- UTP (Unshielded Twisted Pair) Cable

This project makes use of a 15-meter UTP cable. UTP cable is a 100-ohm copper cable with 2 to 1800 unshielded twisted pairs encased in an outer jacket. They do not have a metal shield. As a result, the wire has a small diameter but is not protected against damage interference caused by electricity. The twist improves the device's resistance to electrical noise and EMI.

2.6.3- Switch

A network switch is a computer networking device that uses packet switching to connect devices on a computer network. It receives processes and forwards data to the target device. A network switch is a multiport network bridge that processes and forwards data at the OSI data link layer (layer 2) using hardware addresses. Certain switches can also process data at the network layer (layer 3) and Layer-3 switches by implementing routing functions, often known as multilayer switches.

In a computer network, a switch is a device that connects other devices. It facilitates communication between different networked devices, and multiple data connections are inserted into a switch. Switches control data flow across a network by sending a received network packet exclusively to one or more devices for whom it was intended.

2.6.4- Router

A router is a networking device that sends data packets from one computer network to another. On the Internet, routers oversee traffic direction. Data packets are used to send data over the internet, such as a web page or an email. A packet is sent from one router to another through the networks that make up an Internet connection until it reaches its destination node.

Two or more data lines from separate networks are linked to a router. The router scans the network address information in a data packet to determine the eventual destination when it arrives on one of the lines. The packet is then directed to the next network on its path using information from its routing table or routing policy. On this router, we will implement routing and ACL, AAA, and IPsec in this workshop II.

2.7- Conclusion

Finally, with all of the hardware and software requirements for Workshop II, we may now move on to the next phase of our project. We immediately research the hardware provided and the operating system we choose. With the completeness of the needs and the tools we have, the network can be working and running completely.

CHAPTER 3: DESIGN

3.1- Introduction

This project must define, design, build, and manage secure network infrastructure. In Workshop II, each group should implement their network design or infrastructure. Based on the network design that we accomplished, we need to build up a LAN (Local Area Network) that consists of three servers, routers, switches, and clients to meet the requirements of Workshop II. As previously said, our team built up a network with three servers: Windows Server 2012, Linux Ubuntu Server, and Linux Ubuntu Desktop.

3.2- Security Policy

Security policy is a written document outlining how to protect the organization from threats, including computer security threats, and how to handle the situations when they occur. The security policy was published to protect the computer network against any harmful actions or malicious activity by giving the guidelines to enforce, monitor, and maintain the computer network security. The secure network infrastructure is designed to ensure the CIA's confidentiality, integrity, and availability of the company's information are being protected. In addition, it is essential to protect the system and data from unauthorized access, unauthorized manipulation or modification, and protection against any cyber-attack in the company system.

- **Software Installation Policy**

  Most software nowadays is not freeware. Therefore, the cost of software is a consideration for their deployment. It is the organisation's responsibility to ensure the license are accurate and up to date. IT department is responsible for purchasing a software license for the following software categories:

  - Operating System Software.
  - Internet Software.
  - Productivity tools package.

The other software categories are the responsibility of the Head of Department in which they serve. The software installation policy is used to protect the organization from unauthorized software that sometimes has several viruses that can infect each computer and network.

- **Server Security Policy**

  Every Server Administrator at the organization must take reasonable security measures to secure their hosts as outlined in the policy. Servers should be placed in physically attached areas accessible only to authorized personnel. It is the responsibility of the administrator to:

  - Regularly scan all the servers using updated virus detection software.
  - The accounts must be periodically reviewed for inactivity and any dormant accounts disabled.
  - Ensure that logs of user activity must be retained for some time. Keep the records for at least six months.

- **Remote Access Policy**

  It is the responsibility of the organization requesters and approvers with remote access privileges to the corporate network to ensure that their access privileges are more minor or minimal to carry out the functions. The requirements for this policy are:

  - All the remote access should be strictly controlled.
  - Users with remote access privileges must ensure that their computer firewall settings shall be turned on and constantly running when connecting to the organization group.
  - No dial-in access shall be permitted to bypass the organization firewall.
  - No time should any user share their login or password to anyone else, including family members and close friends.
  - Password Protection Policy

Passwords are an essential aspect of computer security. A poorly chosen password may result in unauthorized access and exploitation. This policy aims to establish the standard for creating a strong password and protecting those passwords.

- Password creation is vital to protect from unauthorized access. To create a good password, you need to follow this guideline:
    i. The password cannot contain all or part of the user account name or ID.
    ii. The password must be at least eight characters in length.
    iii. The password must contain uppercase, lowercase, number, AND symbol.

- We need to protect the password because all passwords must be treated as sensitive and confidential data. To preserve the password, we must:
    i. Do not share the password with anyone, including family members.
    ii. Do not hint at the password format, such as "my family name."
    iii. Please do not write the passwords down and store them anywhere in the office.
    iv. Encrypt the password when we store it in a computer system or mobile device file.
    v. Do not use "Remember Password."

3.3- Physical Design

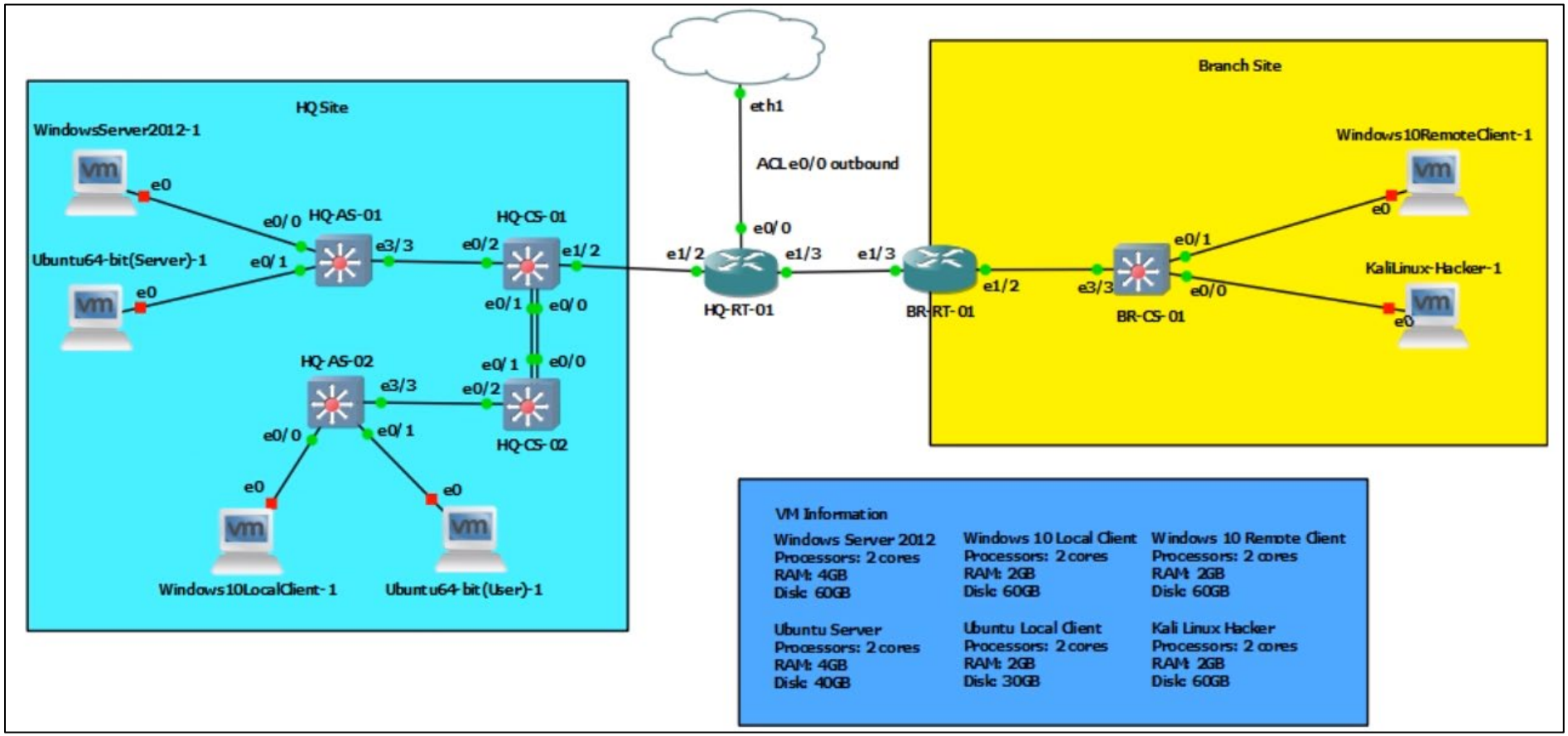

Figure 2 Physical Design

3.4- Logical Design

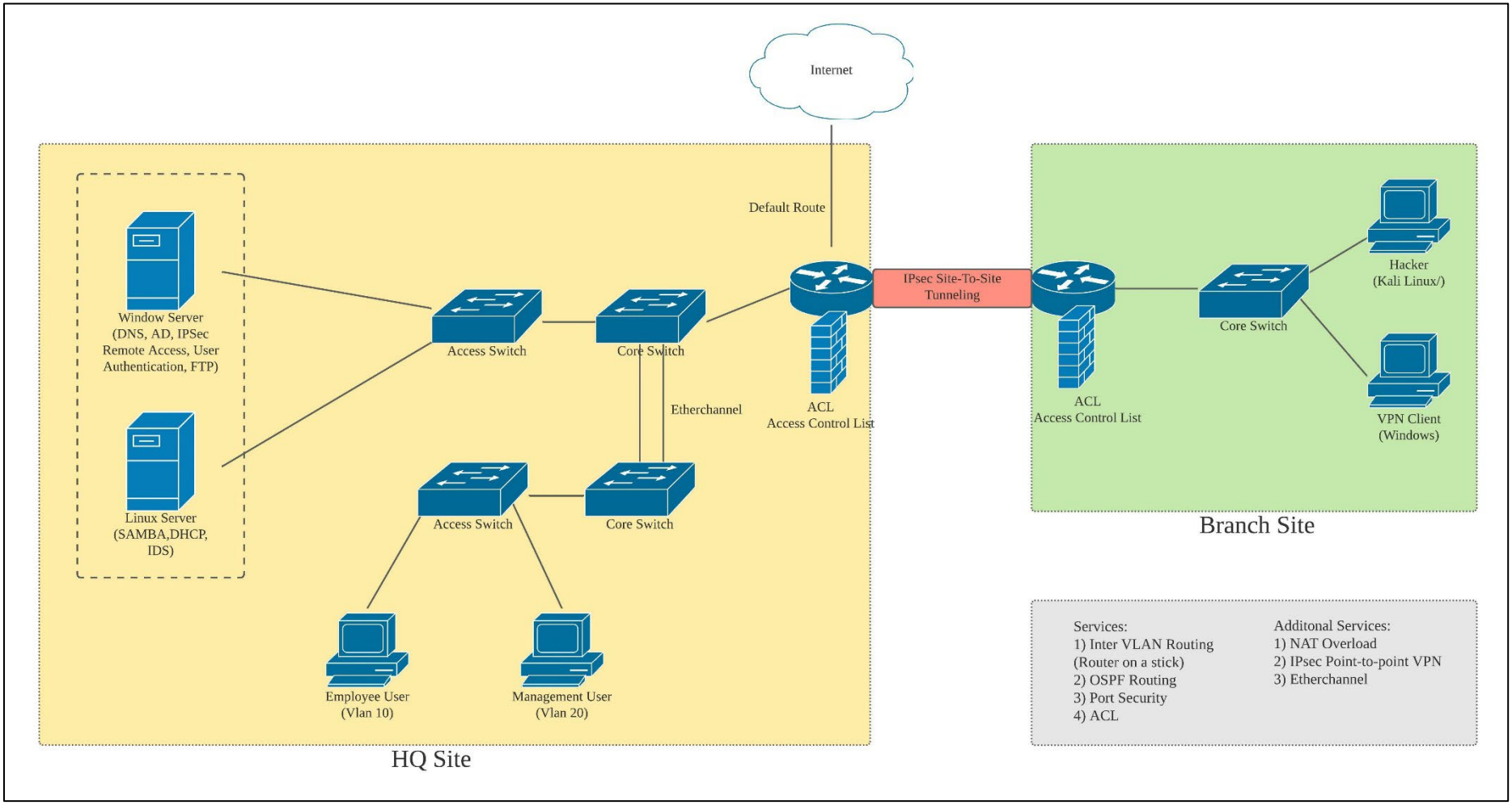

Figure 3 Logical Design

3.5- IP Addressing

HQ's Addressing Table

VLAN	VLAN Name	Network ID	Broadcast ID	Available IP
10	Employee	10.10.0.0/16	10.10.255.255/16	10.10.0.1 – 10.10.255.254 (65534 Hosts)
20	Management	10.20.0.0/18	10.20.63.255/18	10.20.0.1 – 10.20.63.254 (16382 Hosts)
30	Server	10.30.0.0/24	10.30.0.255/24	10.30.0.1 - 10.30.0.254 (254 Hosts)
40	Wireless	10.40.0.0/23	10.40.1.255/23	10.40.0.1 - 10.40.1.254 (510 Hosts)

Table 4 HQ's Addressing Table

Branch's Addressing Table

VLAN	VLAN Name	Network ID	Broadcast ID	Available IP
10	Employee	20.10.0.0/24	20.10.0.255/24	20.10.0.1 – 20.10.0.254 (254 Hosts)
20	Management	20.20.0.0/24	20.20.0.255/24	20.20.0.1 – 20.20.0.254 (254 Hosts)

Table 5 Branch's Addressing Table

3.6- Conclusion

Network design is crucial when it comes to building and developing a network. Without a network design, there is no way to know where to start with the network implementation of any project. The planning of network complexity must be in line with the network administrator, redundancy, standards, and maintenance issues are only a few of the primary factors to consider while adopting network design. These qualities must be present for the network to be deployable, extendable, and simple to manage.

CHAPTER 4: SERVICES

4.1- Introduction

In this chapter, we will show the list of services that we will include in this project and implement them. We will explain the overview of each of the services.

4.2- List of Services

a) Domain Name Server (DNS - IPv4)
b) Dynamic Host Configuration Protocol (DHCP – IPv4)
c) Access Control List Router
d) Router Authentication and Authorization (Radius)
e) User Authentication by integrating AD with Linux
f) VLAN and Port Security
g) Windows Server Hardening Vulnerability Report
h) Linux Server Hardening Vulnerability Report
i) Active Directory
j) IDS with port mirroring and management console
k) IPsec VPN
l) Samba and Samba security services

4.3- Brief of Overview for Services

4.3.1- Domain Name Server (DNS)

Domain Name Server, known as DNS, converts domain names into IP addresses. Each device in the network is assigned an IP address, which is required to locate the proper Internet device. When a user wishes to load a webpage, there must be a translation between what the user types into their web browser and what they see on the screen. A machine-friendly address is also required to locate the webpage.

4.3.2- Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol, known as DHCP, is a network management protocol that automates configuring devices on an IP network and allows them to use network services including DNS, NTP, and the UDP and TCP communication protocols. DHCP assigns each device on the network a dynamic IP address and other network setup parameters to communicate with other IP networks.

4.3.3- ACL Router

By regulating all incoming and outgoing data packets, the Access Control List known as ACL acts as the network's gatekeeper. The ACL follows a set of rules and examines every incoming and outgoing data to see if it complies with those criteria. Extended ACL and Standard ACL are the two forms of ACL. The standard ACL is the most basic ACL, which simply examines the source address to determine whether or not to allow data to pass. On the other hand, the Extended ACL is more advanced, as it can block entire networks and traffic depending on protocol details.

4.3.4- Router Authentication and Authorization (Radius)

Radius, or Remote Authentication Dial-In User Service, is an application layer client-server networking protocol. Radius Client and Radius Server are the two components. The Radius Client is a networking device that is used to verify a user's identity. On the other hand, Radius Server is a background process that runs on either UNIX or Windows Server. It enables you to keep track of user profiles in a central database.

4.3.5- User Authentication by integrating AD with Linux

Institutions and individuals worldwide utilise Microsoft's Active Directory to govern access to the organization's resources centrally. It allows you to manage users, passwords, and resources like computers and control who has access to what.

4.3.6- VLAN and Port Security

Port security enables us to restrict the number of MAC addresses on a port, preventing access by unauthorized MAC addresses. If a secure MAC address is secured on a port, that MAC address is not allowed to enter on any other port of VLAN.

4.3.7- Windows Server Hardening Vulnerability Report

Windows Server hardening involves identifying and remediating security vulnerabilities. It is used to reduce the risk of attackers compromising critical data and systems.

4.3.8- Linux Server Hardening Vulnerability Report

Many Linux server security issues we may experience occur because we do not arrive hardened out of the box. Further complicating matters, many of today's top security initiatives focus on the front office instead of the server rack. This provides more chances for malicious parties to acquire sensitive data, which can be devastating. A strategic protocol focused on risk prevention, and early mitigation can make all the difference.

4.3.9- Active Directory

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources. It can store the data as the object, which object is a single element such as a user and a device like a printer. Active Directory categorizes the directory object by name and attributes.

4.3.10- IDS with port mirroring and management console

An intrusion Detection System (IDS) can be used either as a software application or device that monitors the network from malicious activities. IDS with port mirroring means that the network switch can send a copy of network data packets transmitted over a switch port to network monitoring or inspection device. Any malicious activities will be reported centrally using security information and an event management system.

Port mirroring is the ability of a network switch to send a copy of network data packets being transferred over a switch port to a network monitoring or inspection device attached to the port mirror, a dedicated port on the switch.

Management console (Qradar) is the primary module for controlling log and flow views, reports, offenders, asset data, and administrative activities. The QRadar Console provides access to all modules through a single interface. The Qradar Console does not monitor data processing and storage for distributed systems. Instead, the Qradar Console allows users to make the calls they want, report them, and receive and interpret alarms based on the rules they define. Data collecting, processing, and storage are all done on a single appliance all in one system.

4.3.11- IPsec VPN

IPsec is a series of protocols that create encrypted connections between devices. IPsec is commonly used to create VPNs, and it encrypts IP packets while also authenticating the source of the packets. To build and maintain these encrypted connections, VPNs use the IPsec protocol.

4.3.12- Samba and Samba security services

Samba is free software that re-implementation of the SMB networking protocol. It provides file and print services for various Microsoft Windows clients and can integrate with the Microsoft Windows Server domain. There are only two types of security modes for Samba: share-level and user-level, which are known as security levels. Share-level can only be implemented in one way, whereas user-level can be implemented in four different ways.

4.4- Extra Services

a) Dynamic NAT (NAT Overload)
b) IPsec Point-To-Point VPN
c) EtherChannel

4.5- Brief of Overview for Extra Services

4.5.1- Dynamic NAT (NAT Overload)

Network Address Translation is a method that allows the translation of IP addresses while packets are traversing the network. NAT Overload, also known as PAT, Port Address Translation is essentially NAT with the TCP/UDP ports translation.

The primary purpose of NAT is to hide a client's private IP address to reserve the public address space. Other benefits of NAT include security and economical usage of the IP address ranges at hand. For example, a complete network with 100 hosts can have 100 private IP addresses and still be visible to the outside world (internet) as a single IP address.

4.5.2- IPsec Point-To-Point VPN

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g. HQ or branches). The VPN tunnel is created over the public Internet network and encrypted using several advanced encryption algorithms to protect the data transmitted between the two sites.

ISAKMP (Internet Security Association and Key Management Protocol) and IPSec are essential to building and encrypting the VPN tunnel. ISAKMP, also called IKE (Internet Key Exchange), is the negotiation protocol that allows two hosts to agree on building an IPsec security association. ISAKMP negotiation consists of two phases: Phase 1 and Phase 2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. IPSec then comes into play to encrypt the data using encryption algorithms and provides authentication, encryption and anti-replay services.

4.5.3- Etherchannel

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows several physical Ethernet links to create one logical Ethernet link to provide fault-tolerance and high-speed links between switches, routers, and servers.

Using an EtherChannel has numerous advantages, and probably the most desirable aspect is the bandwidth. It can be used with Ethernet running on twisted-pair wiring, single-mode and multimode fibre. Using the maximum of 8 active ports, a total bandwidth of 800 Mbit/s, 8 Gbit/s or 80 Gbit/s is possible depending on port speed. This assumes a traffic mixture, as those speeds do not apply to a single application only.

Because EtherChannel takes advantage of existing wiring, it makes it very scalable. It can be used at all levels of the network to create higher bandwidth links as the traffic needs of the network increase. All Cisco switches can support EtherChannel.

4.6- Conclusion

In this chapter, we understand the services we will implement in this chapter. It enables us to gain a better understanding of each service. In the industry world nowadays, these services are pretty widespread. As a result, having some fundamental knowledge will benefit us before going to industrial training and ensure we know what we are getting ourselves into.

CHAPTER 5: INSTALLATION AND CONFIGURATION

5.1- Introduction

In this chapter, each installed service will be listed and explained. The role of the service, the difficulties that are remedied by installing the service, the step on to install and configure the services, and the type of software or package used will all be explained.

5.2- Services and Person in Charge

Services	Group Member
a) VLAN and Inter VLAN Routing b) Port Security c) EtherChannel d) NAT e) IPSEC Site-to-Site VPN f) IPSEC Remote Access VPN g) ACL h) Router Radius Server Authentication	OOI CHIOU XIANG
a) Setup AD and Group Policy b) AD group and users c) DNS Server d) FTP Server e) Join Windows 10 PC with AD f) Integrating Linux with AD	MUHAMMAD IZHAM BIN NORHAMADI
a) DHCP b) Linux Hardening c) Launch Attack (MAC Address Flooding) d) IDS	IZZATUL HANANI BINTI KAMARUL NIZAR
a) Windows Hardening b) Samba Security	SITI AISHAH BINTI MUSTAFA

Table 6 Services and Person in Charge

5.3- Service Installation and Configuration

5.3.1 - VLAN and Inter VLAN Routing

1) Create VLAN on the switch.

```
HQ-CS-01(config)#vlan 10
HQ-CS-01(config-vlan)#name employee
HQ-CS-01(config-vlan)#exit
HQ-CS-01(config)#vlan 20
HQ-CS-01(config-vlan)#name Management
HQ-CS-01(config-vlan)#ex
HQ-CS-01(config)#vlan 30
HQ-CS-01(config-vlan)#name Server
HQ-CS-01(config-vlan)#exit
HQ-CS-01(config)#vlan 40
HQ-CS-01(config-vlan)#name Wireless
```

Figure 4 Configure VLAN

2) Assign the VLAN to switch ports.

```
HQ-CS-01(config)#int g0/0
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#switchport access vlan 10
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/1
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#switchport access vlan 20
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/2
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#switchport access vlan 30
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/3
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#switchport access vlan 40
```

Figure 5 Assign switch port

```
HQ-CS-01#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                                Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                                Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   employee                         active    Gi0/0
20   Management                       active    Gi0/1
30   Server                           active    Gi0/2
40   Wireless                         active    Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figure 6 Show VLAN brief output

3) Configure the trunk port on the port connected to another switch or router.

```
HQ-CS-01(config-if)#int g3/3
HQ-CS-01(config-if)#switchport trunk encapsulation dot1q
HQ-CS-01(config-if)#switchport mode trunk
HQ-CS-01(config-if)#no shut
```

Figure 7 Configure trunk port

4) Configure the router on the stick and IP address for each interface.

```
HQ-RT-01(config)#int e1/2.10
HQ-RT-01(config-subif)#encapsulation dot1q 10
HQ-RT-01(config-subif)#ip address 10.10.0.1 255.255.0.0
HQ-RT-01(config-subif)#no shut
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.20
HQ-RT-01(config-subif)#encapsulation dot1q 20
HQ-RT-01(config-subif)#ip address 10.20.0.1 255.255.192.0
HQ-RT-01(config-subif)#no shut
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.30
HQ-RT-01(config-subif)#encapsulation dot1q 30
HQ-RT-01(config-subif)#ip address 10.30.0.1 255.255.254.0
HQ-RT-01(config-subif)#no shut
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.40
HQ-RT-01(config-subif)#encapsulation dot1q 40
HQ-RT-01(config-subif)#ip address 10.40.0.1 255.255.255.0
HQ-RT-01(config-subif)#no shut
```

Figure 8 Configure Router on a stick

5.3.2- Port Security

1) Go to each switch port configure the port as an access port.

```
HQ-CS-01(config)#int g0/0
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/1
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/2
HQ-CS-01(config-if)#switchport mode access
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/3
HQ-CS-01(config-if)#switchport mode access
```

Figure 9 Configure access port

2) Enable dynamic port security with additional options configuration.

```
HQ-CS-01(config)#int g0/0
HQ-CS-01(config-if)#switchport port-security
HQ-CS-01(config-if)#switchport port-security mac-address sticky
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/1
HQ-CS-01(config-if)#switchport port-security
HQ-CS-01(config-if)#switchport port-security mac-address sticky
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/2
HQ-CS-01(config-if)#switchport port-security
HQ-CS-01(config-if)#switchport port-security mac-address sticky
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/3
HQ-CS-01(config-if)#switchport port-security
HQ-CS-01(config-if)#switchport port-security mac-address sticky
```

Figure 10 Configure dynamic port-security

3) Verify the VLAN port security with the show command.

```
HQ-CS-01#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Gi0/0             1            0                  0         Shutdown
      Gi0/1             1            0                  0         Shutdown
      Gi0/2             1            0                  0         Shutdown
      Gi0/3             1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Figure 11 Show port-security output

4) Set host limit can associate with port and security violation mode.

```
HQ-CS-01(config)#int g0/0
HQ-CS-01(config-if)#switchport port-security maximum 3
HQ-CS-01(config-if)#switchport port-security violation shutdown
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/1
HQ-CS-01(config-if)#switchport port-security maximum 3
HQ-CS-01(config-if)#switchport port-security violation shutdown
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/2
HQ-CS-01(config-if)#switchport port-security maximum 3
HQ-CS-01(config-if)#switchport port-security violation shutdown
HQ-CS-01(config-if)#
HQ-CS-01(config-if)#int g0/3
HQ-CS-01(config-if)#switchport port-security maximum 3
HQ-CS-01(config-if)#switchport port-security violation shutdown
```

Figure 12 Port security policy

5) Configure automatic re-enable error-disabled interface and its interval time.

```
HQ-CS-01(config)#errdisable recovery cause psecure-violation
HQ-CS-01(config)#errdisable recovery interval 300
```

Figure 13 Error recovery mode configuration

6) Check recovery mode is enabled and interval time left.

```
HQ-CS-01#sh errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Enabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

Figure 14 Error recovery configuration

5.3.3- ACL Router

1) Create the extended access control list.

```
HQ-RT-01(config)#ip access-list extended HQ_BRANCH
HQ-RT-01(config-ext-nacl)#
```

Figure 15 Create access control list

2) Create the access control list rules based on needs.

```
HQ-RT-01(config)#ip access-list extended HQ_BRANCH
HQ-RT-01(config-ext-nacl)#permit udp any any eq isakmp
HQ-RT-01(config-ext-nacl)#permit ahp any any
HQ-RT-01(config-ext-nacl)#permit esp any any
HQ-RT-01(config-ext-nacl)#permit udp any any eq non500-isakmp
HQ-RT-01(config-ext-nacl)#permit gre any any
HQ-RT-01(config-ext-nacl)#permit icmp any any echo-reply
HQ-RT-01(config-ext-nacl)#permit ospf any any
HQ-RT-01(config-ext-nacl)#permit icmp 20.20.0.0 0.0.0.255 any
```

Figure 16 Configure access control list

3) Apply the access list based on inbound or outbound traffic.

```
HQ-RT-01(config)#int e1/3
HQ-RT-01(config-if)#ip access-group HQ_BRANCH in
```

Figure 17 Apply access control list to port

4) Verify the access control list created.

```
HQ-RT-01#sh access-list
Extended IP access list HQ_BRANCH
    10 permit udp any any eq isakmp
    20 permit ahp any any
    30 permit esp any any
    40 permit udp any any eq non500-isakmp
    50 permit gre any any
    60 permit icmp any any echo-reply
    70 permit ospf any any
    80 permit icmp 20.20.0.0 0.0.0.255 any
```

Figure 18 Access control list configuration

5.3.4- IPsec VPN (Client-Server)

Windows Server 2012 L2

1) Open server manager, access the Manage menu and click on Add roles and features.

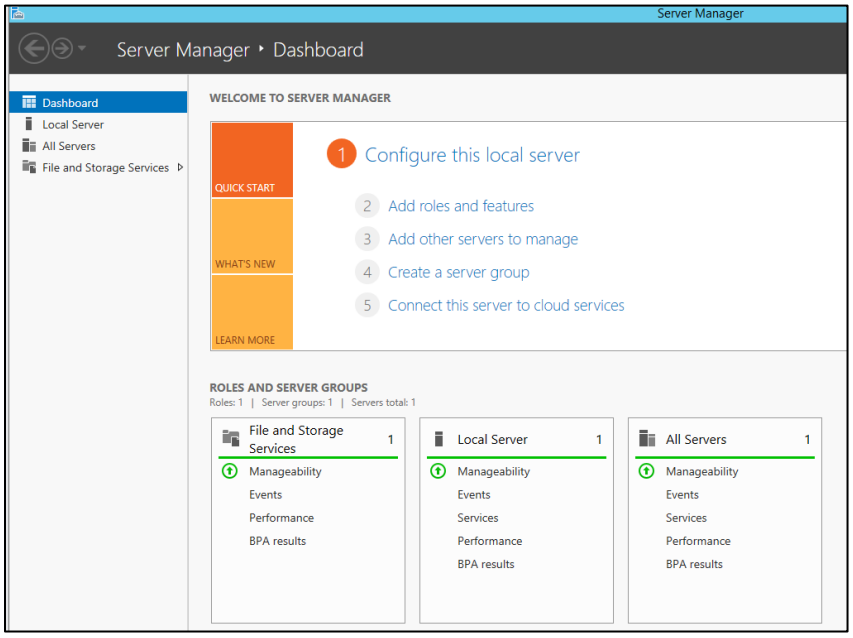

Figure 19 Server manager

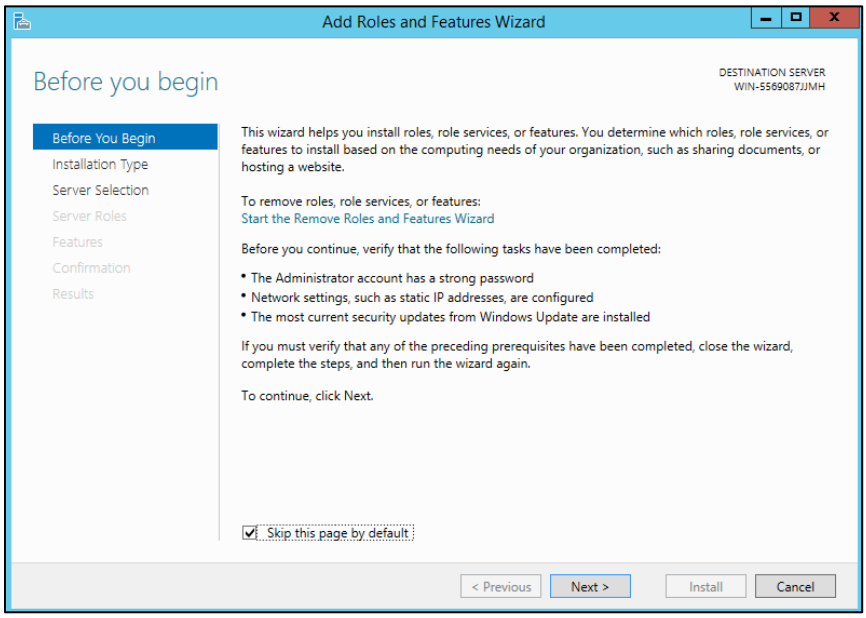

Figure 20 Add roles and features wizard

2) Follow the wizard setup

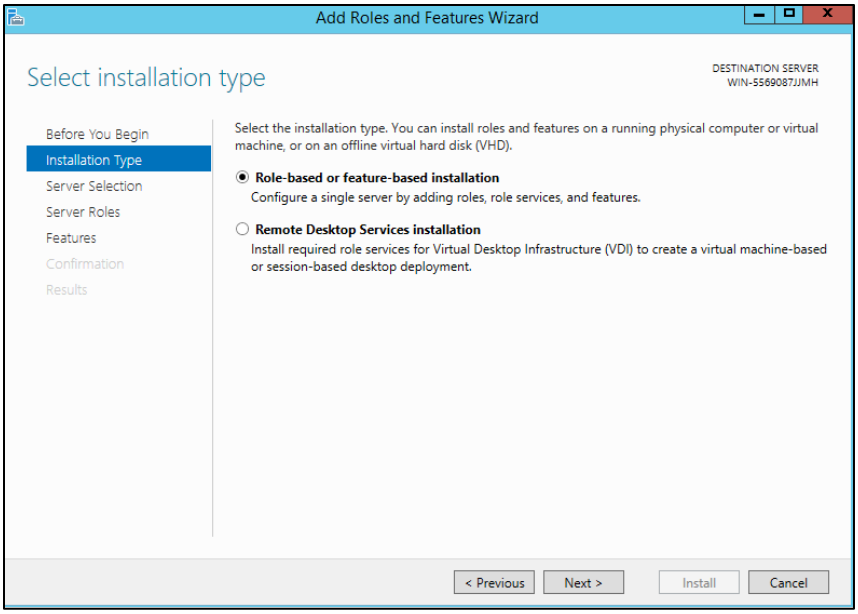

Figure 21 Wizard Installation type

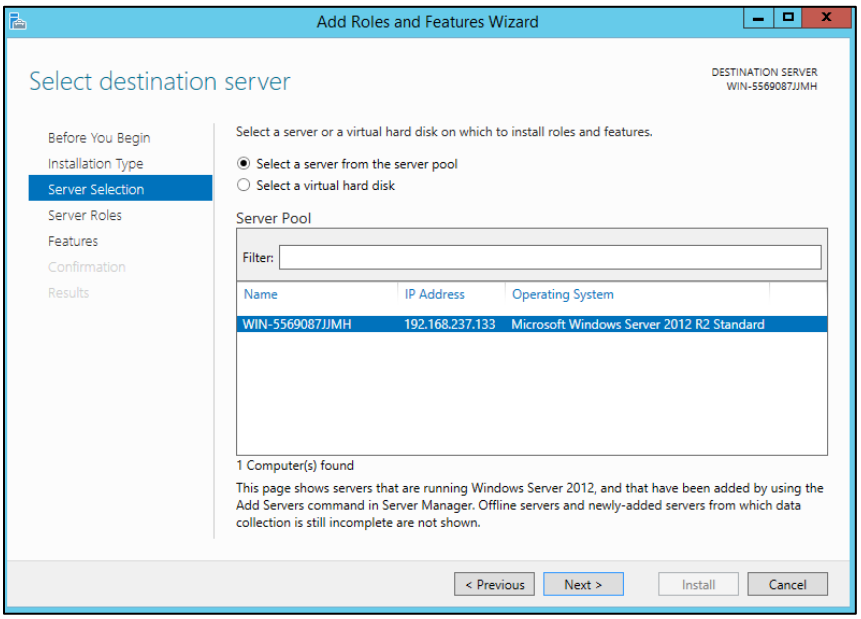

Figure 22 Wizard Server selection

3) Choose the Remote Access server role you would like to install.

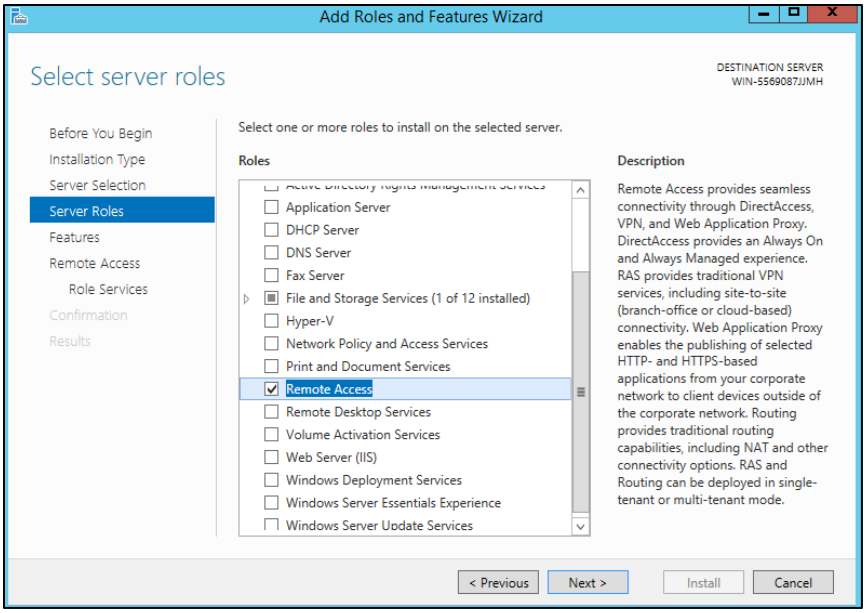

Figure 23 Wizard adds remote access role

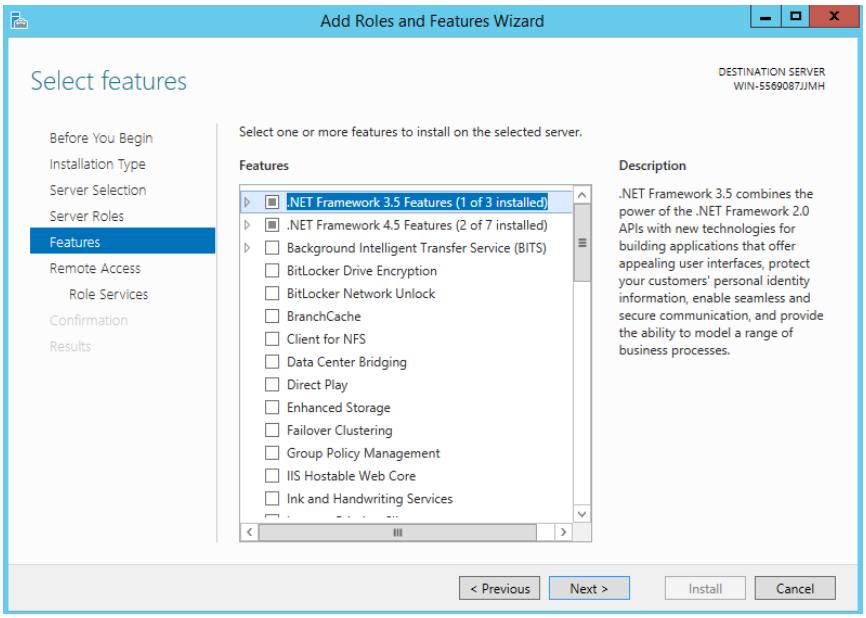

Figure 24 Wizard features

4) Select the Direct Access and VPN (RAS) role services.

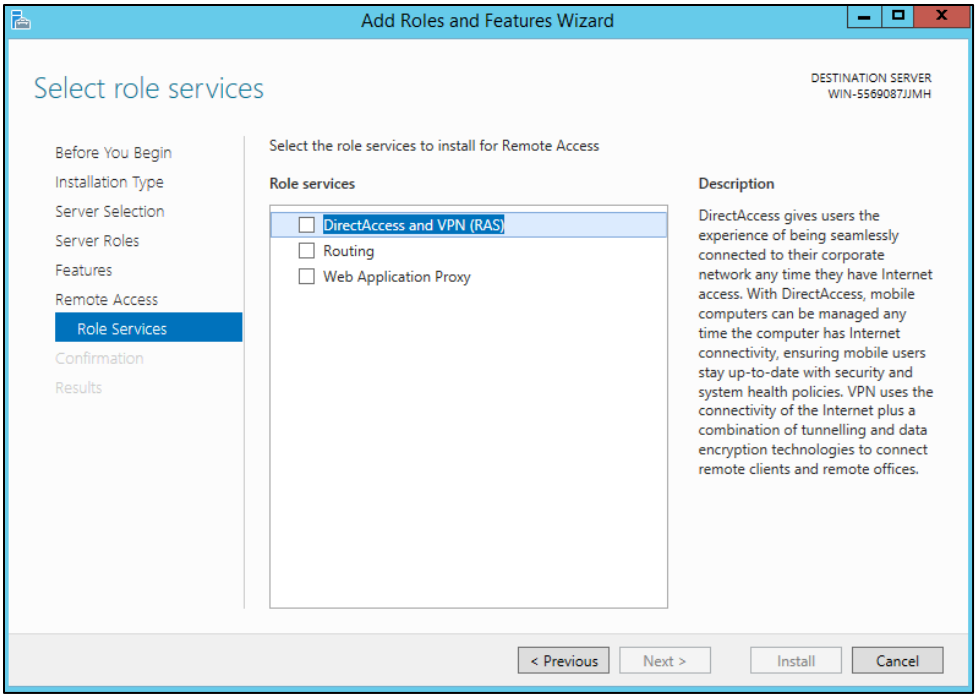

Figure 25 Wizard Role services

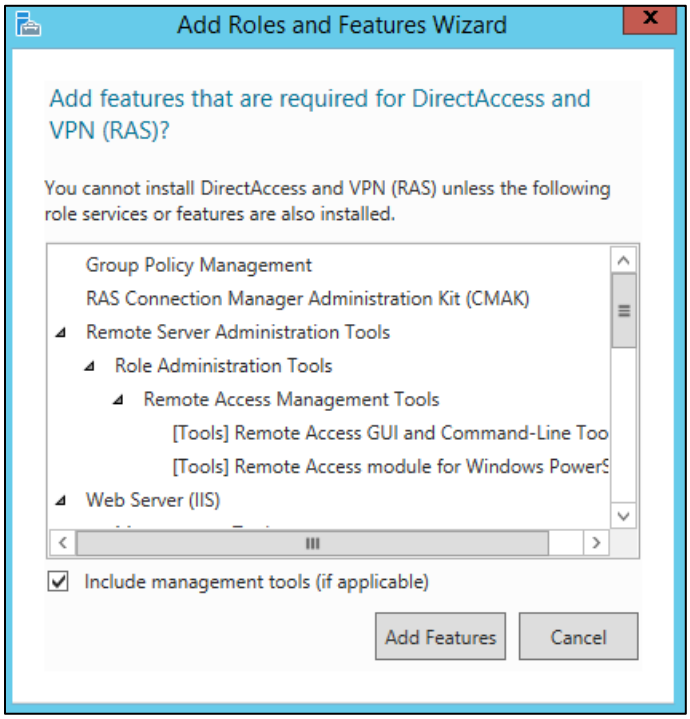

Figure 26 Add roles and features wizard final confirmation

5) Install the services.

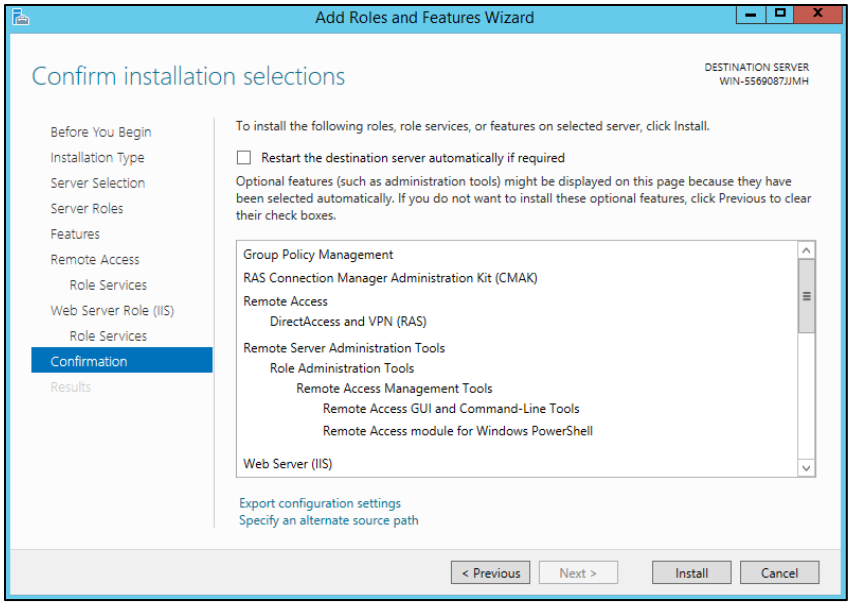

Figure 27 Wizard Install services

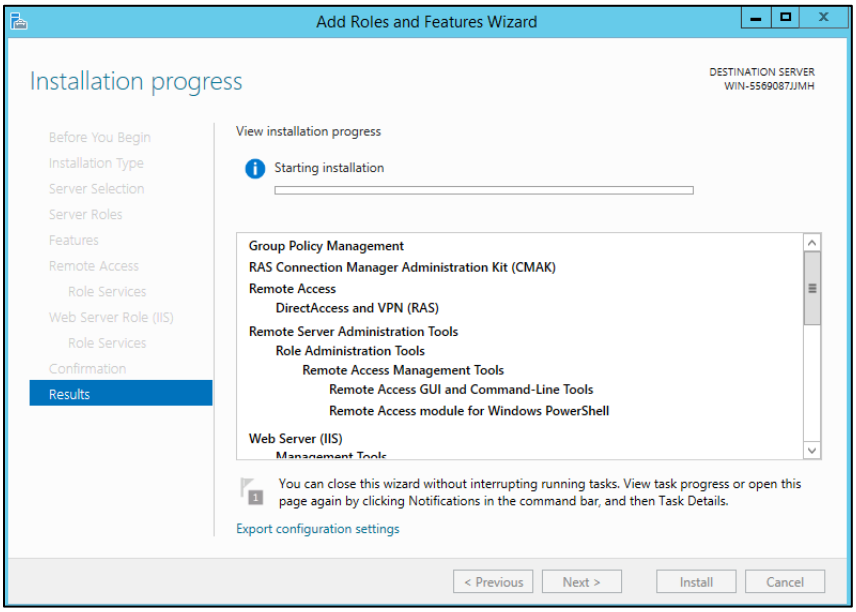

Figure 28 Wizard start install service

6) After installation is done, go to Configure Remote Access Wizard and click Open the Getting Started Wizard.

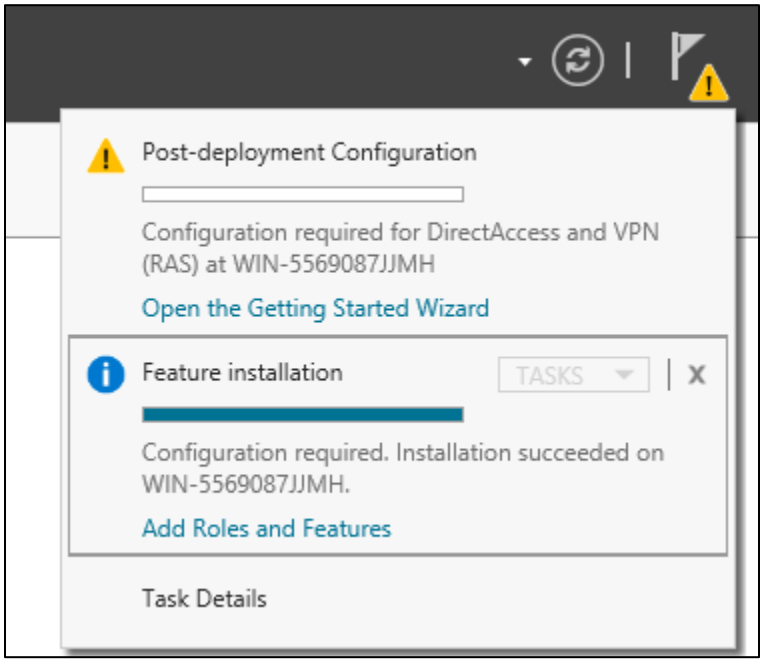

Figure 29 Installation successful

7) Click on Deploy VPN only.

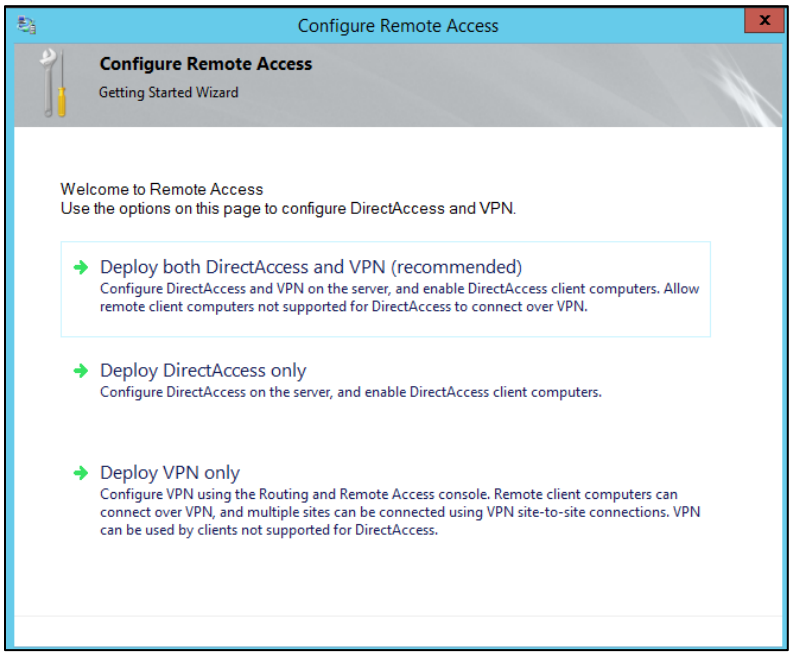

Figure 30 Configure remote access feature

8) Now the Routing and Remote Access configuration window show up.

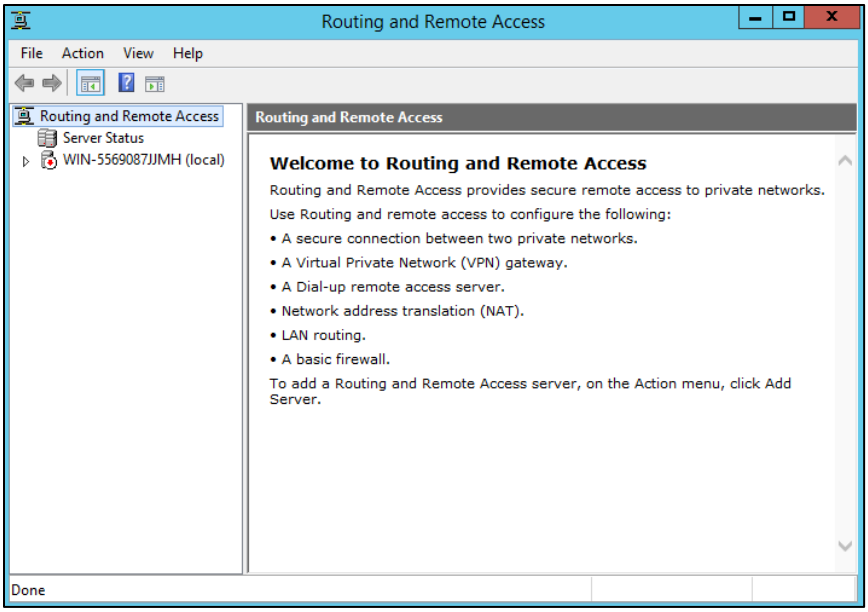

Figure 31 Routing and remote access dashboard

9) Right-click on the server name and choose Configure and Enable Routing and Remote Access.

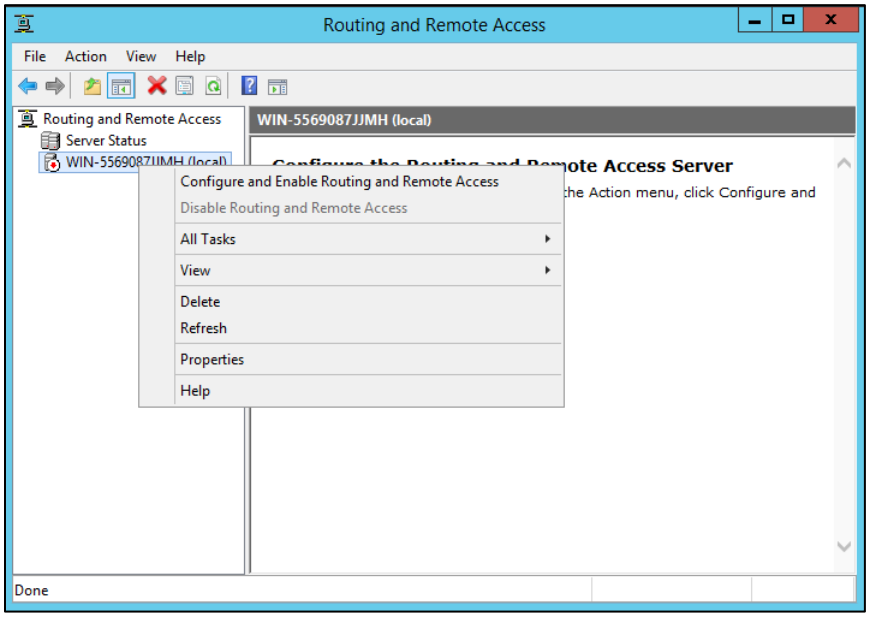

Figure 32 Configure routing and remote access

10) Follow the configuration wizard.

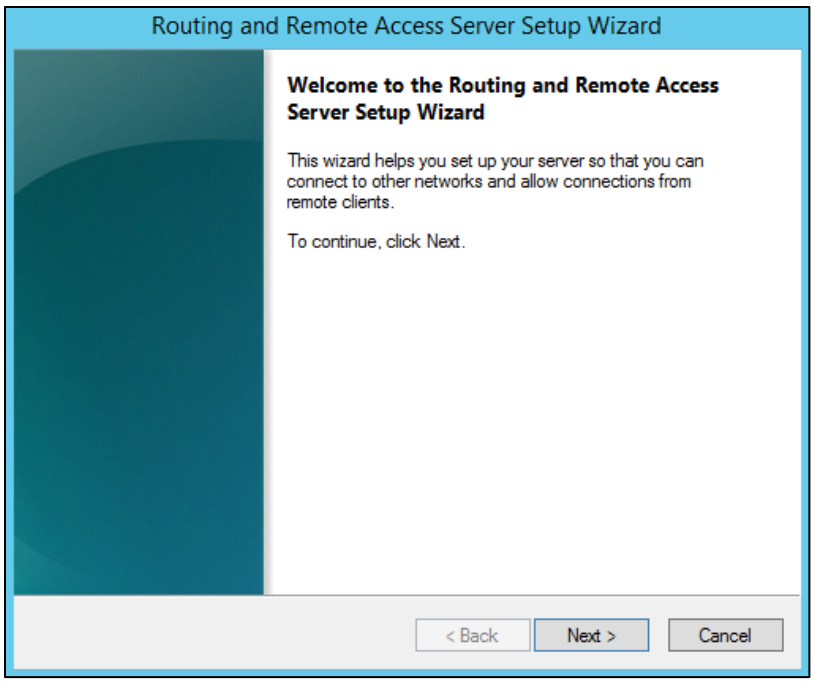

Figure 33 Routing and remote access server setup wizard

11) Click on Custom configuration.

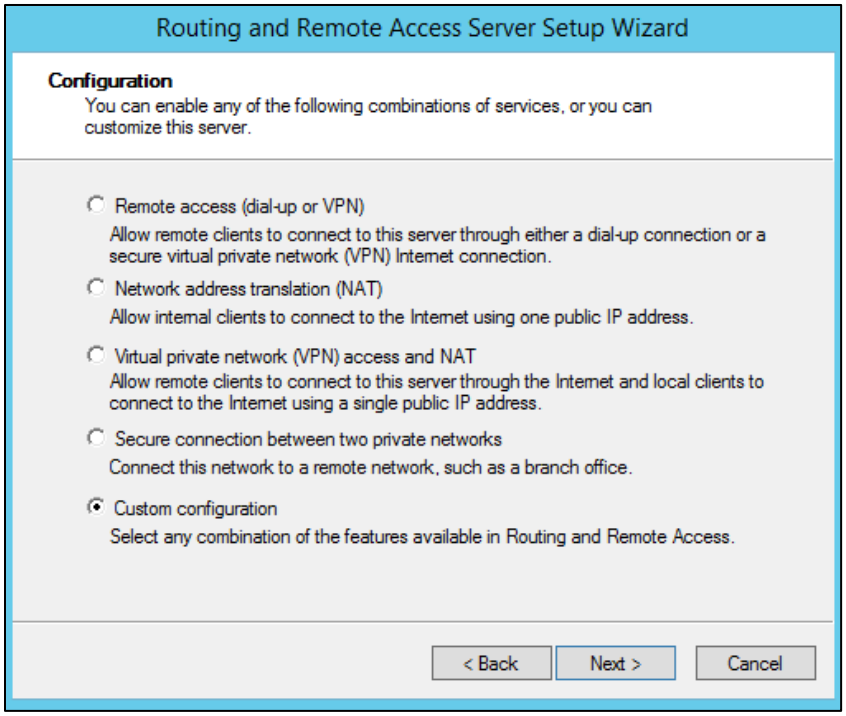

Figure 34 Routing and remote access server setup custom configuration

12) Tick only VPN access.

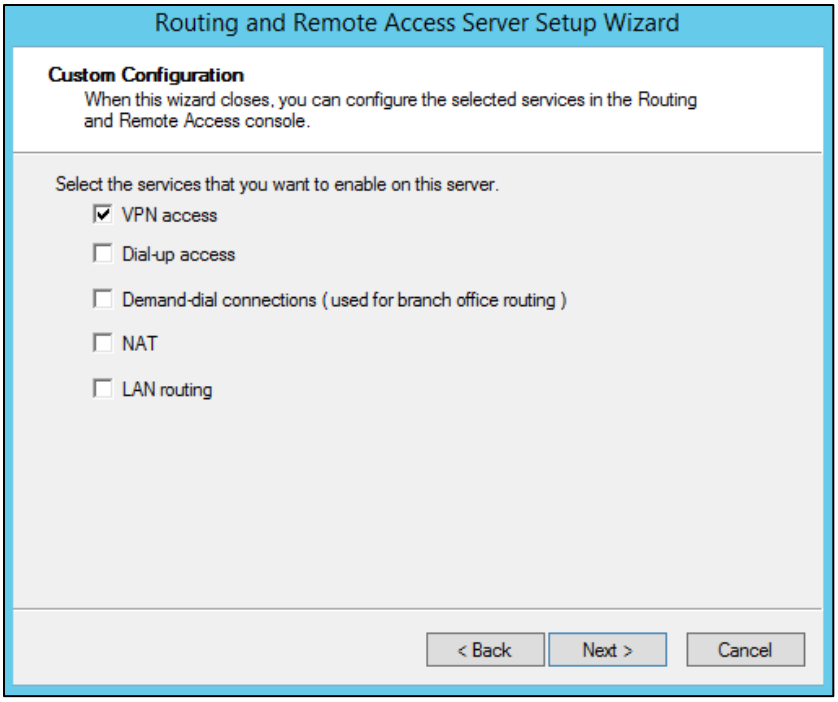

Figure 35 Select VPN access

13) Click on Start service to start the VPN access services.

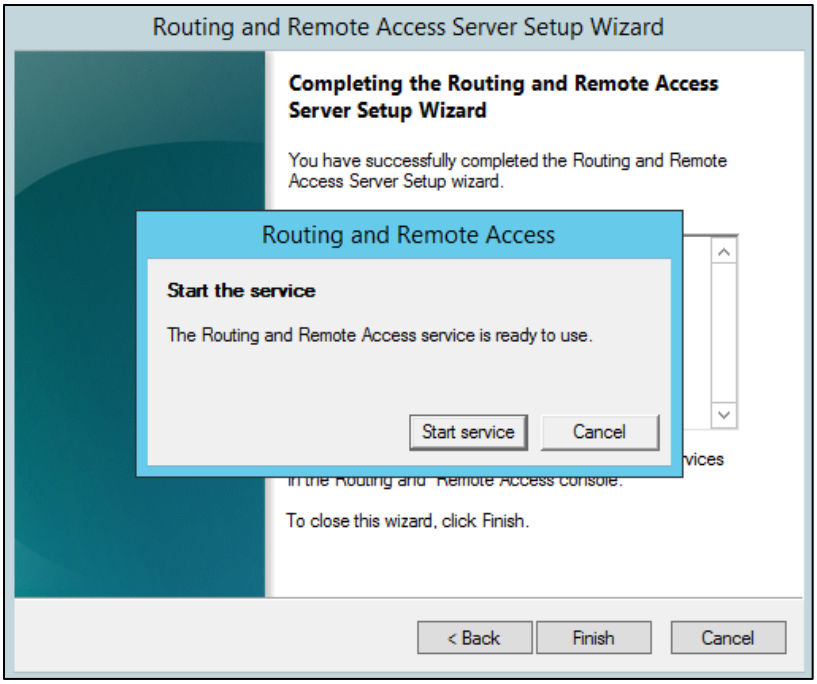

Figure 36 Start VPN access services

14) Now red-light changes to green indicate the remote access services is up.

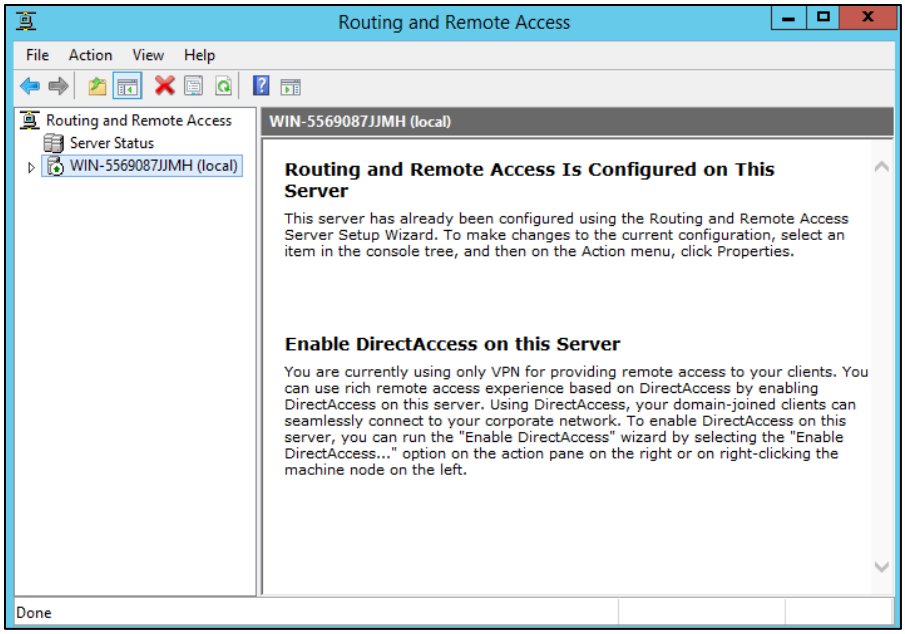

Figure 37 Routing and remote access dashboard

15) Right-click on the server name and go to Properties.

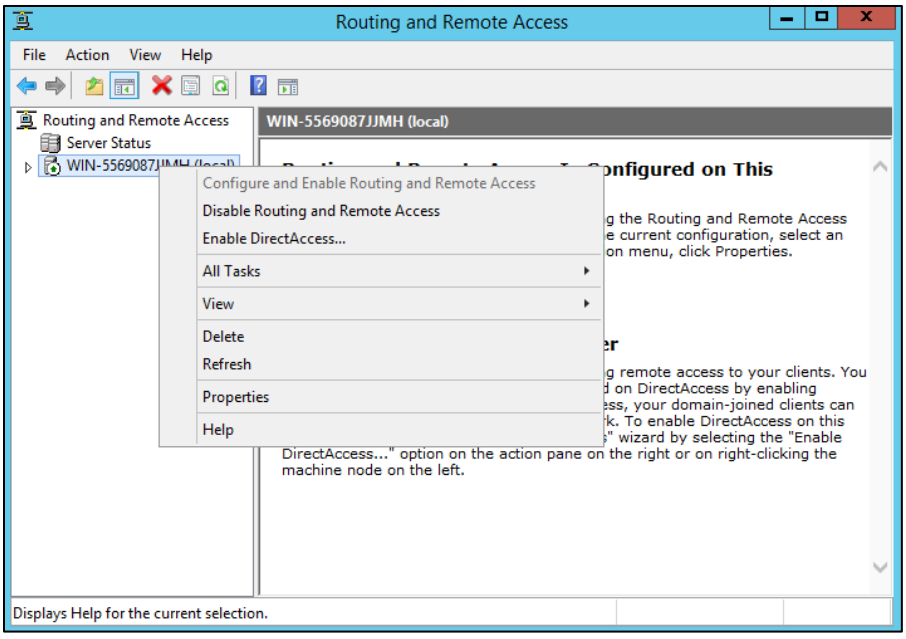

Figure 38 VPN server properties

16) In the properties, choose the IPv4 tab.

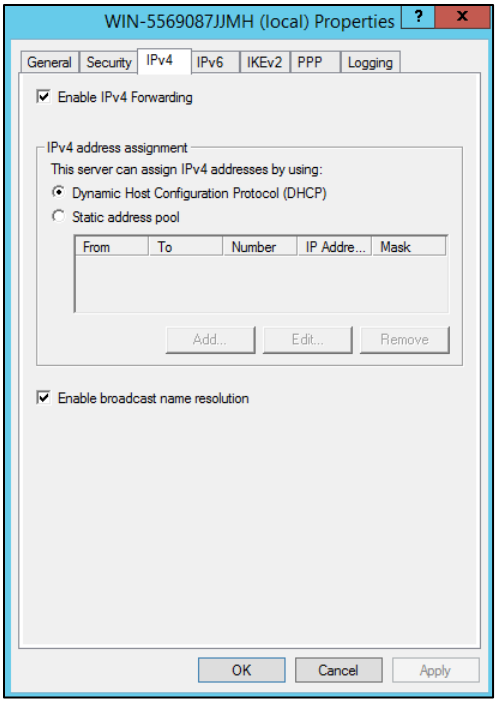

Figure 39 VPN server properties IPV4 tab

17) In the IPv4 address assignment, choose the Static address pool, then click on Add.

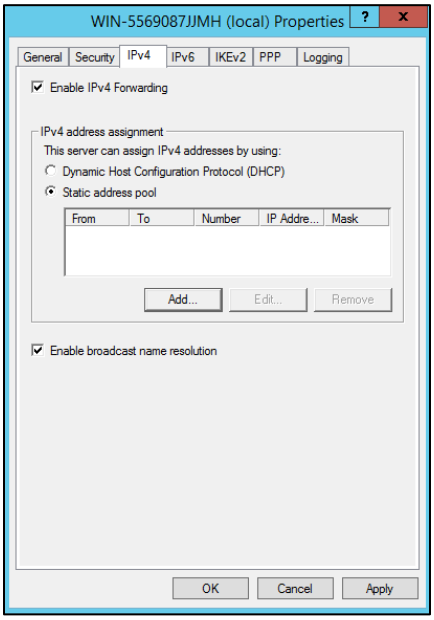

Figure 40 IPV4 address pool configuration

18) Give the remote client the start and end IP address when they establish the VPN.

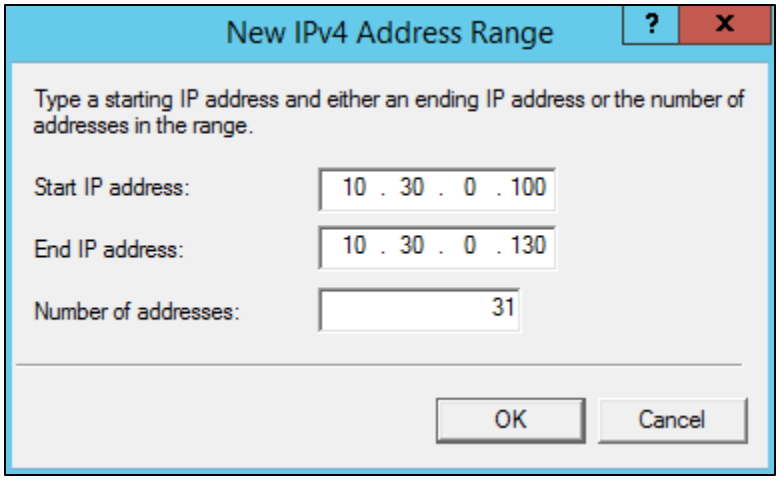

Figure 41 IPV4 address range configuration

19) Go to the Security tab, tick on Allow custom IPsec policy for L2TP/IKEv2 connection, assign the pre-shared key and apply the configuration.

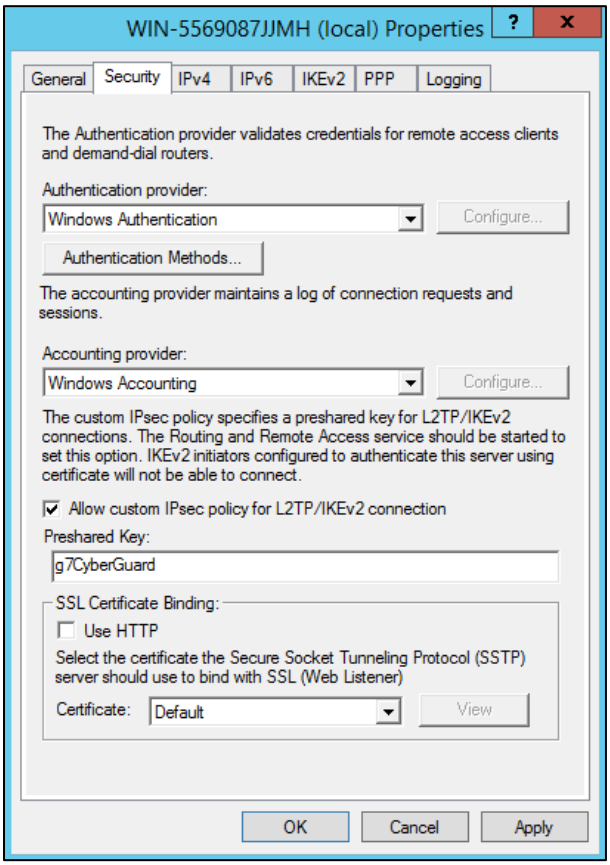

Figure 42 VPN server security tab

20) Go to the server's port option properties.

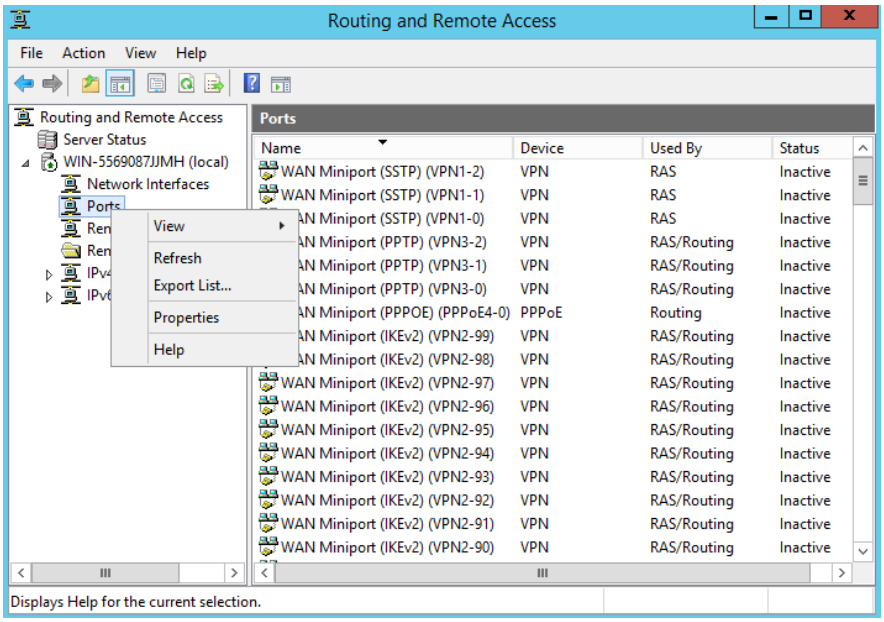

Figure 43 VPN server port option

21) Configure WAN Miniport (PPTP) maximum ports into 1 and apply the setting.

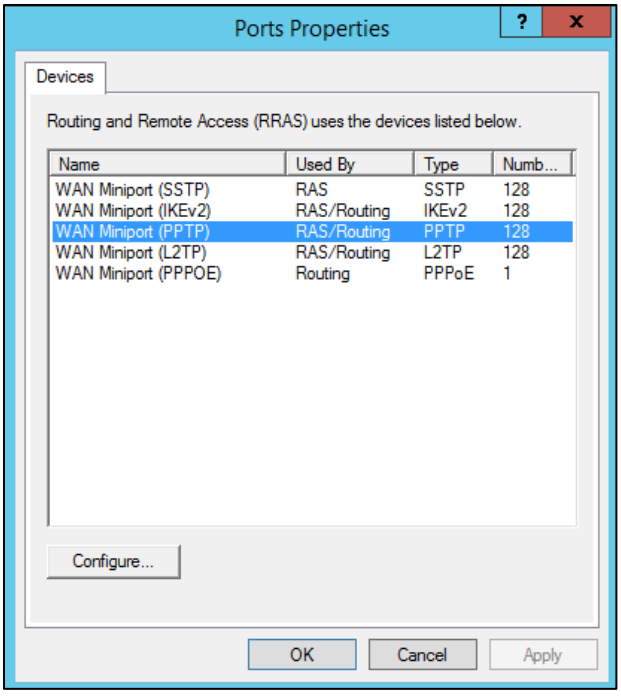

Figure 44 Port properties

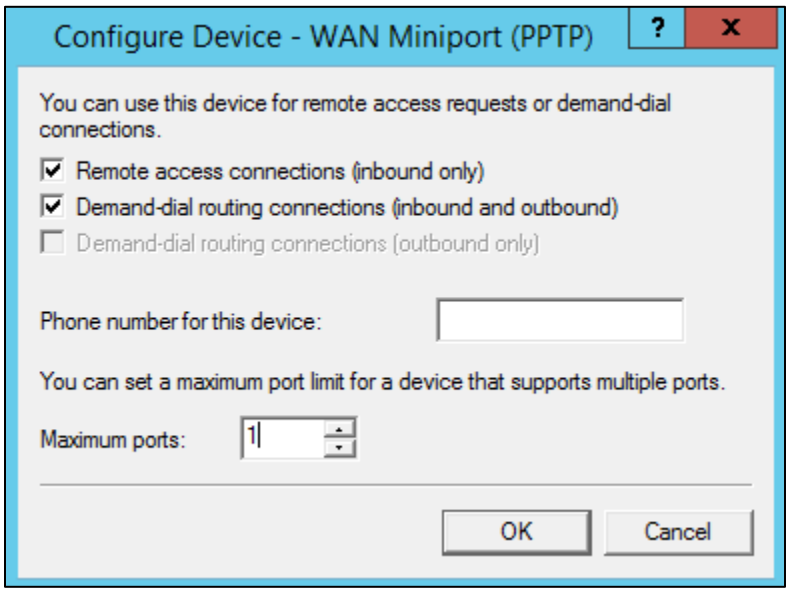

Figure 45 Configure device WAN Miniport

22) Now restart the remote access service.

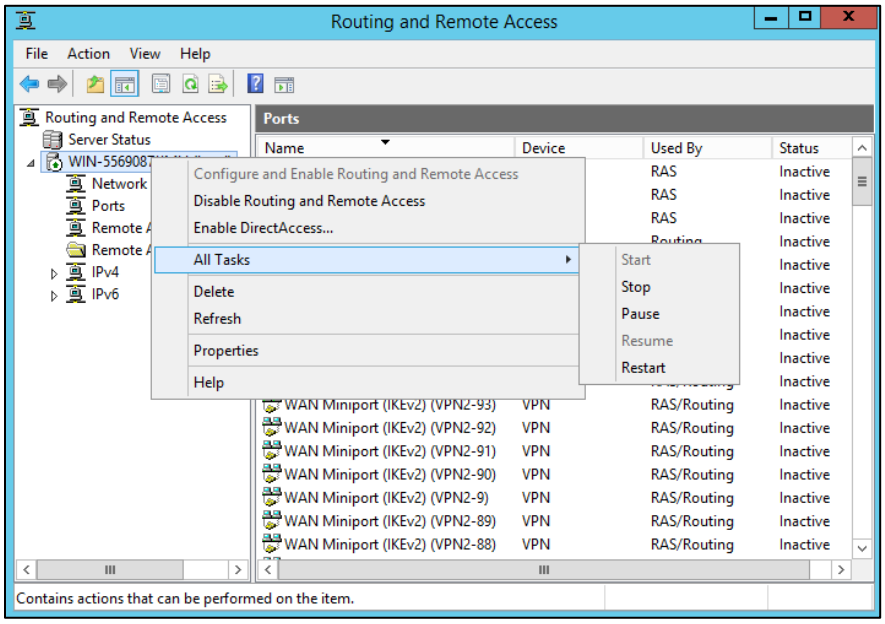

Figure 46 Restart VPN server

Windows 10 Remote Client

1) Open Network and Sharing Center and click on Set up a new connection or network.

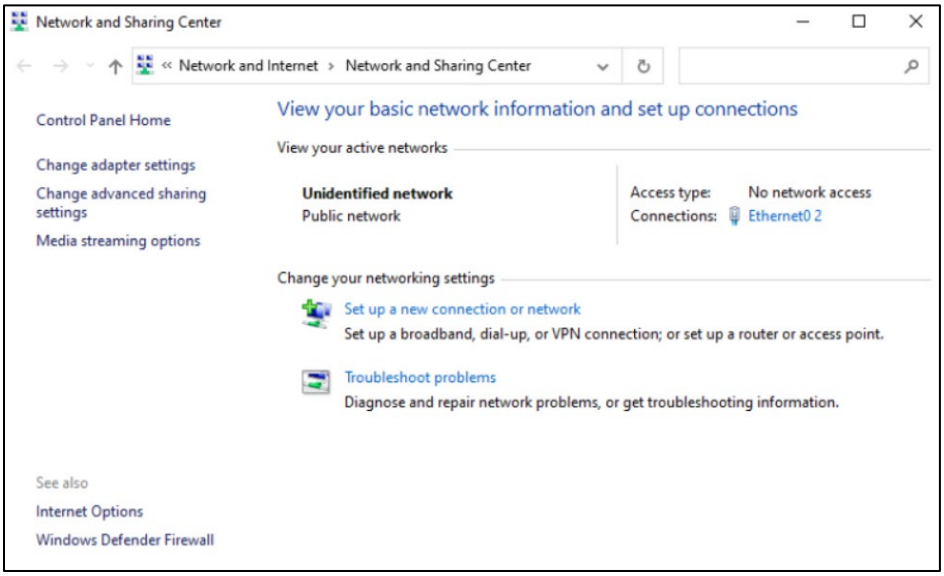

Figure 47 Network and sharing center

2) Select Connect to a workplace.

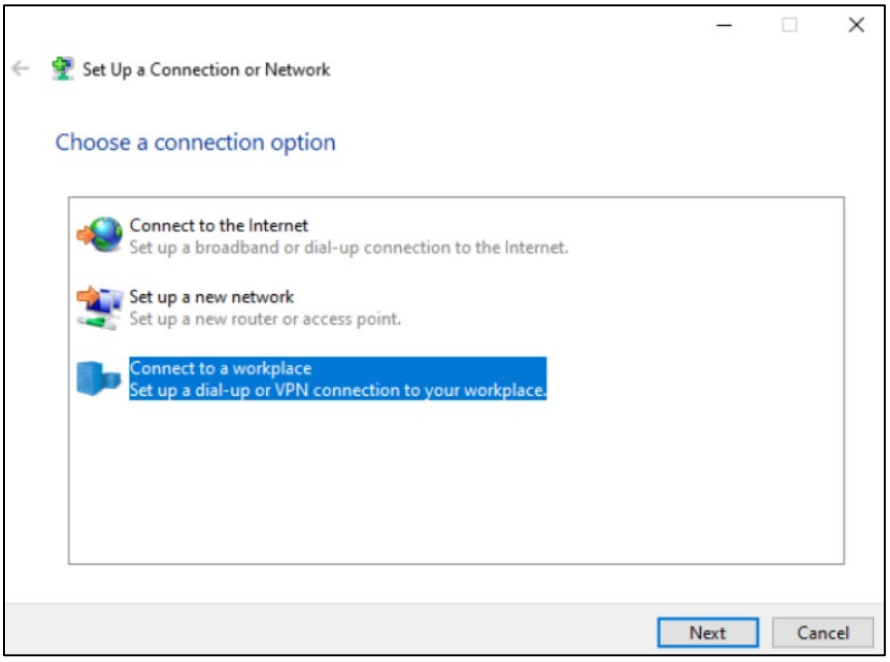

Figure 48 Setup connection or network interface

3) Select Use my Internet connection (VPN).

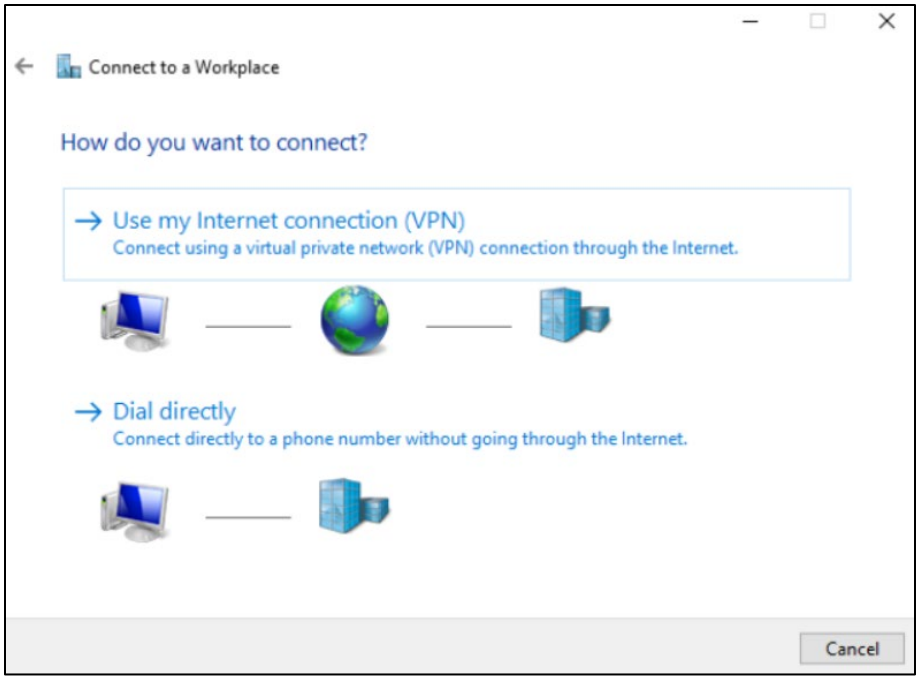

Figure 49 Setup VPN

4) Select I'll set up an Internet connection later.

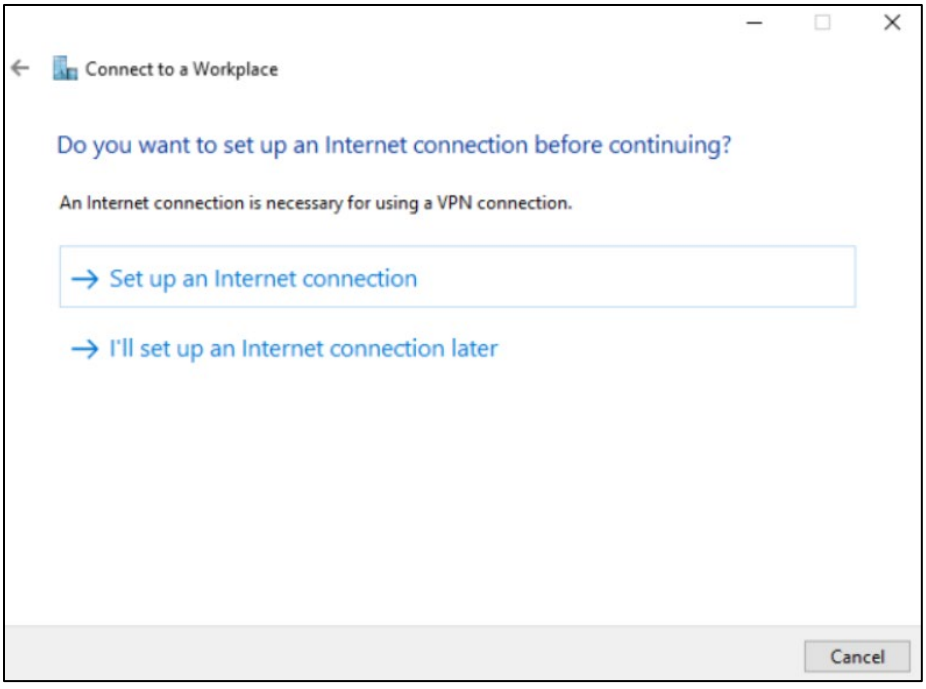

Figure 50 Setup VPN option

5) Assign the remote access server IP address, then click Create.

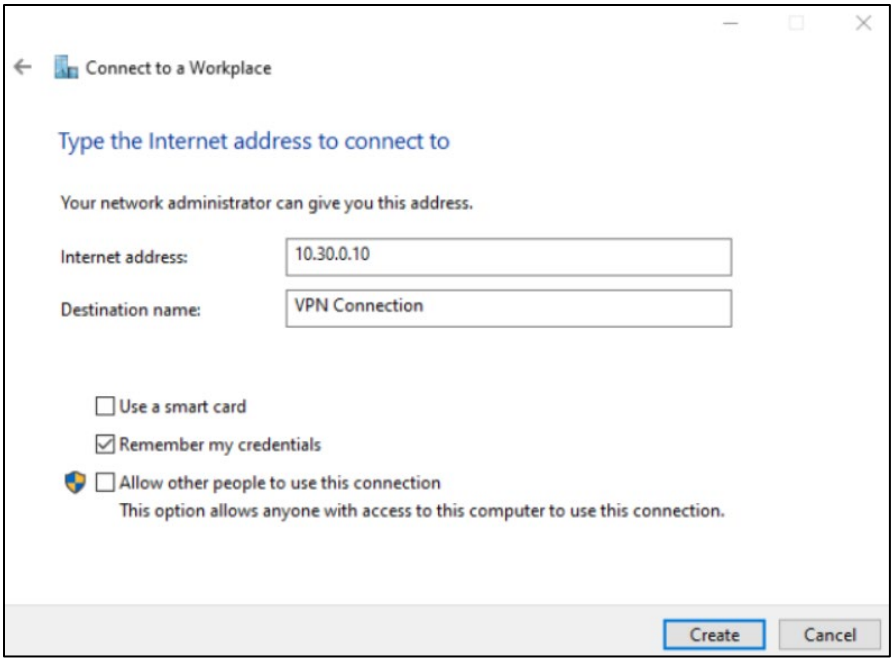

Figure 51 VPN server address configuration

6) Verify the created VPN adapter.

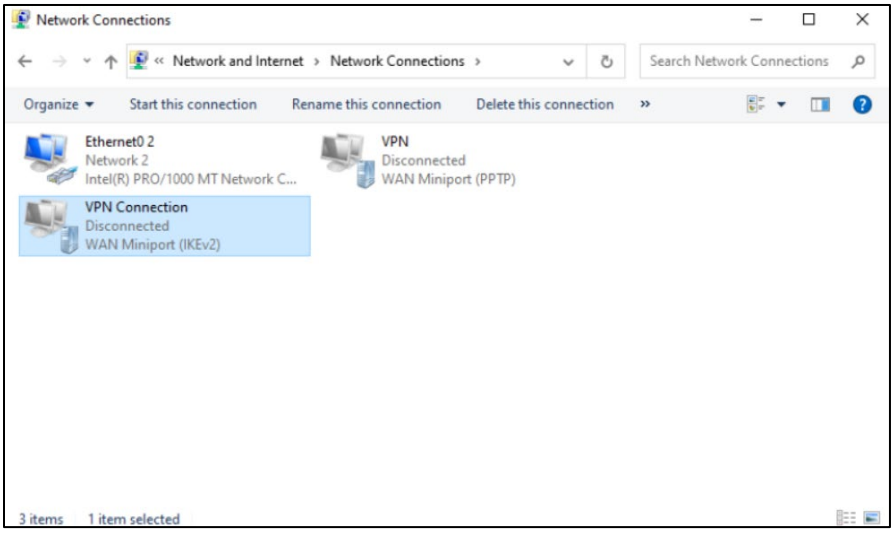

Figure 52 VPN adapter

7) Right-click on the VPN adapter and go to properties.

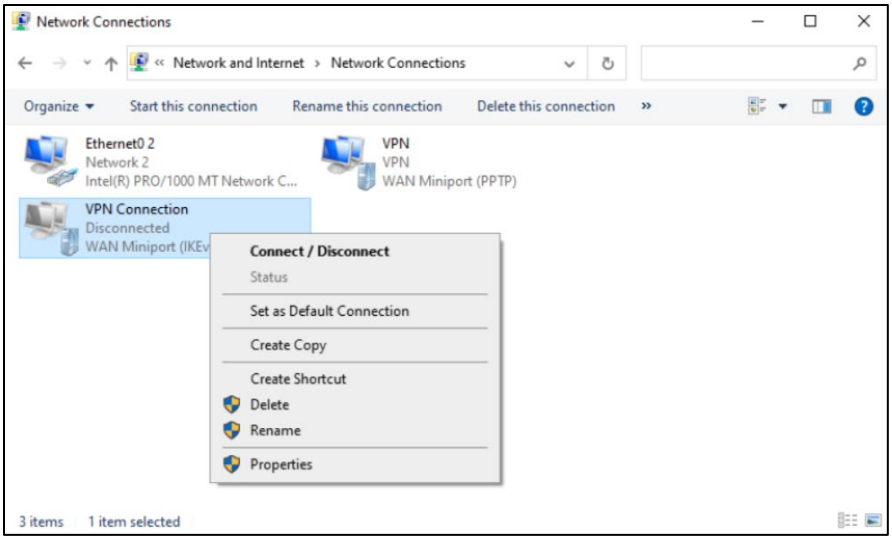

Figure 53 VPN adapter properties

8) In the adapter's properties, go to the Security tab.

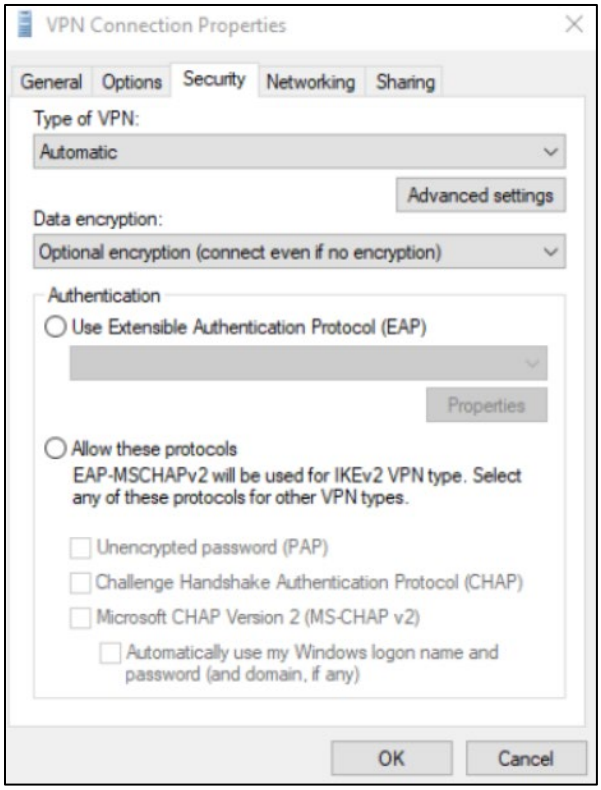

Figure 54 VPN properties security tab

9) In the Type of VPN, option choose L2TP from the drop-down menu.

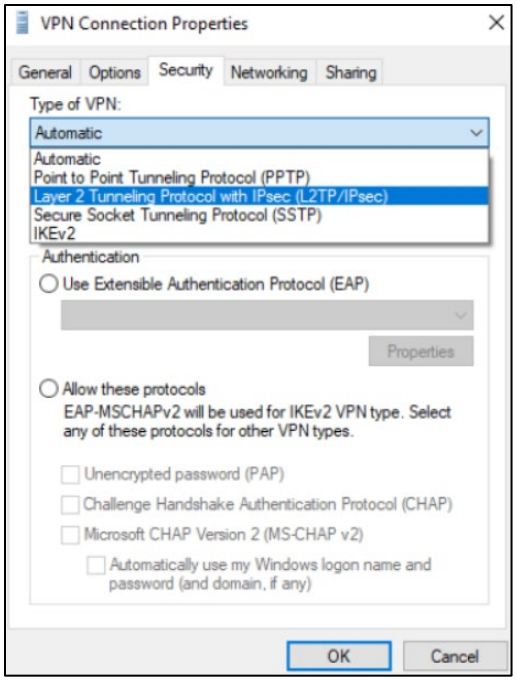

Figure 55 Choose VPN type setup

10) Then click on Advanced settings.

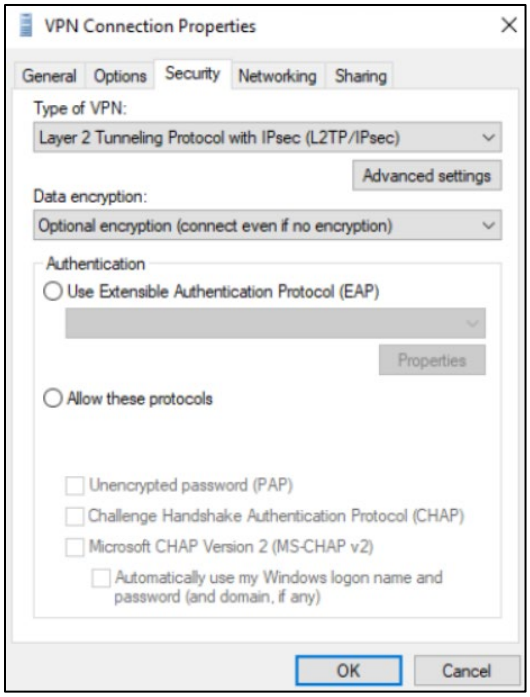

Figure 56 Confirm the setting

11) Choose to choose the preshared key for authentication and fill the key as specified previously.

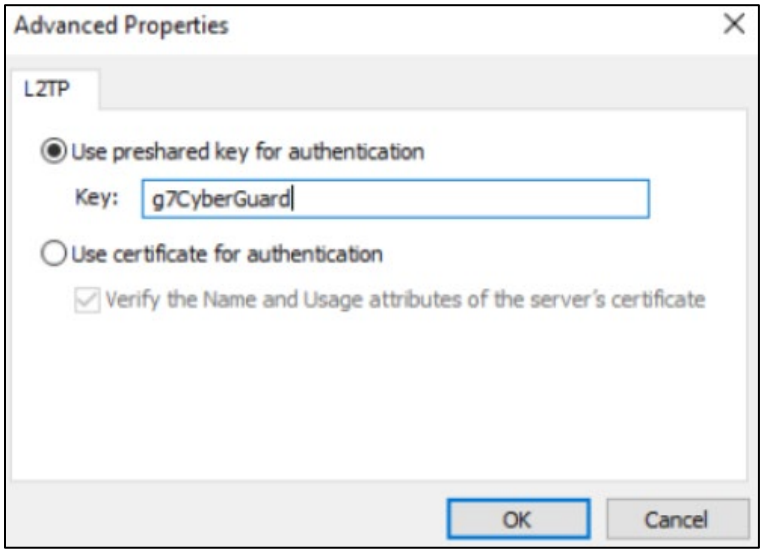

Figure 57 Configure preshared key

12) Try to establish the remote access VPN.

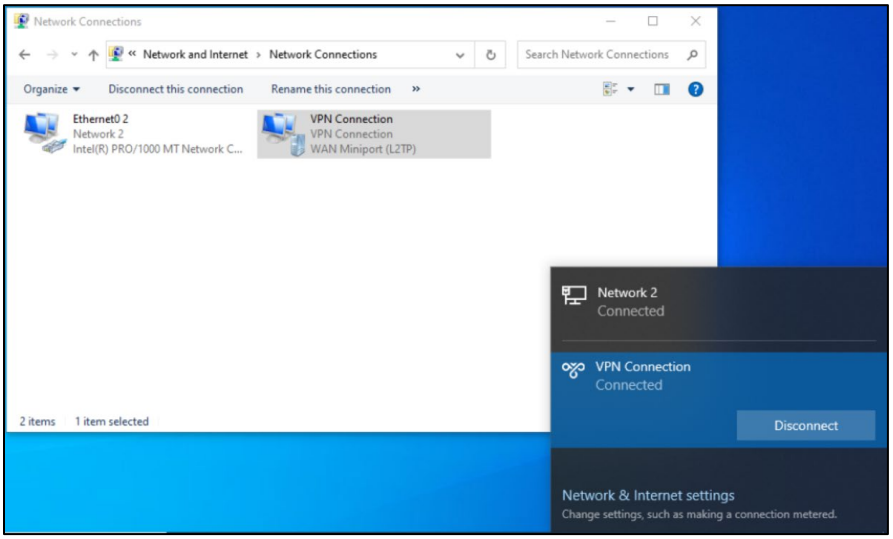

Figure 58 Establish VPN connection

13) Verify the protocol used for encryption, IPsec.

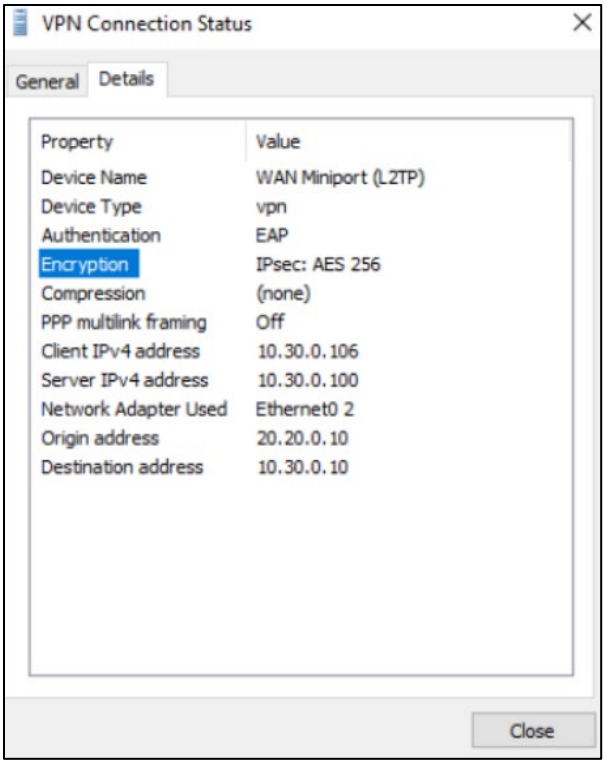

Figure 59 VPN adapter status

5.3.5- Radius Server Authentication & Authorization

Radius Server installation on Windows

1) Open the Server Manager application. Access the Manage menu and click on Add roles and features.

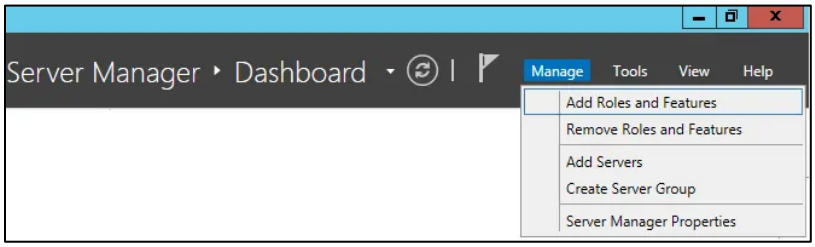

Figure 60 Server manager add roles and features

2) Access the Server roles screen select the Network Policy and Access Service option. Click on the Next button.

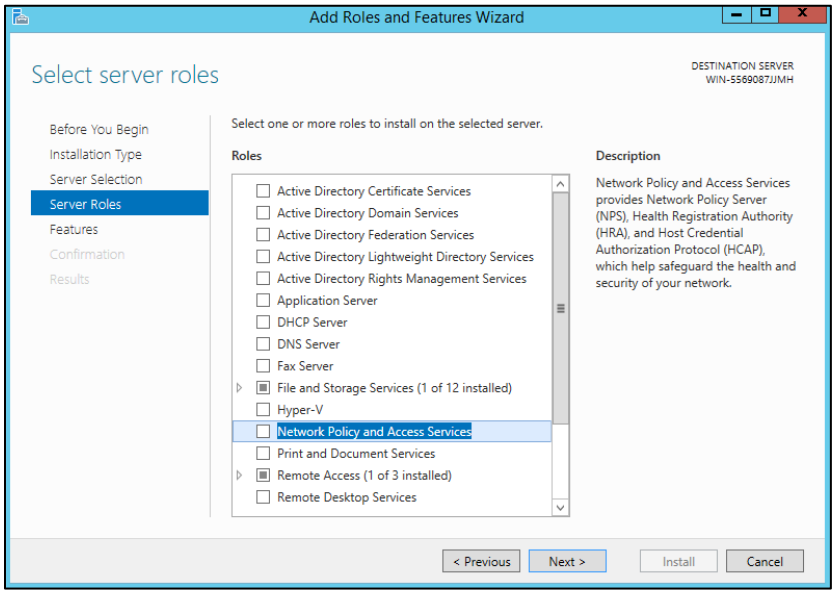

Figure 61 Add roles and features wizard server roles

3) On the following screen, click on the Add features button.

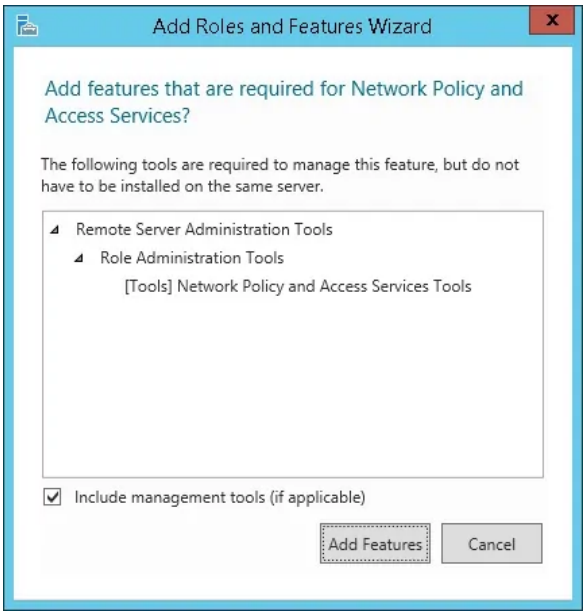

Figure 62 Add roles and features wizard final confirmation

4) On the Role service screen, click on the Next Button.

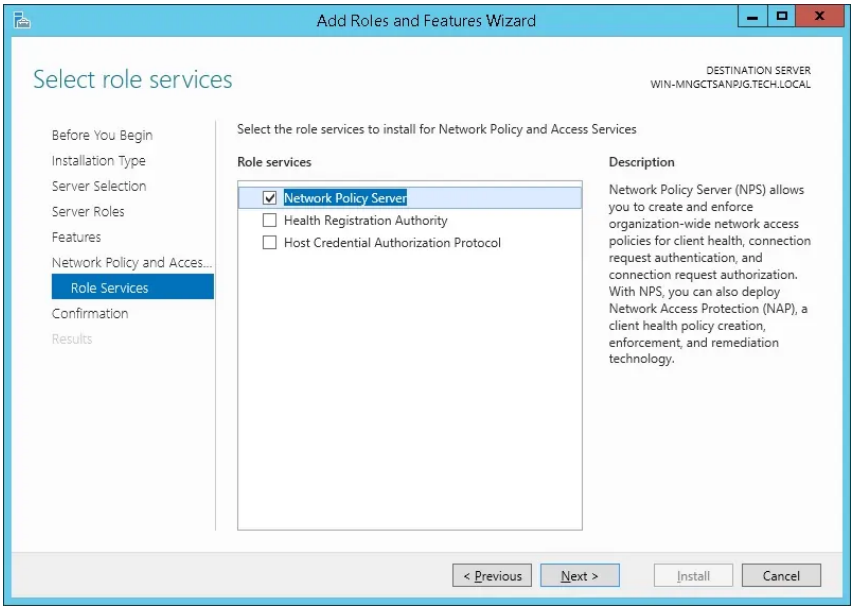

Figure 63 Add roles and features wizard role services

5) On the next screen, click on the Install button.

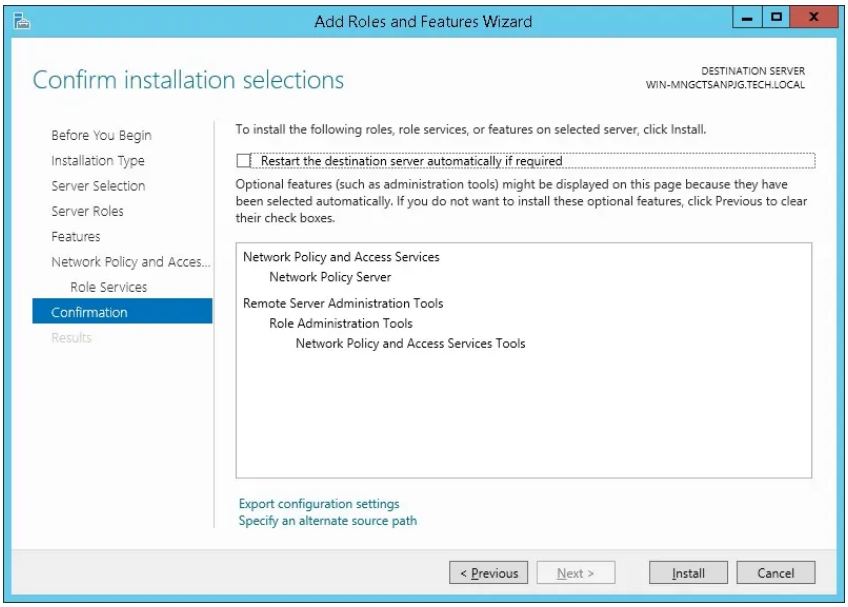

Figure 64 Confirm installation selections

6) Wait for installation. Radius server installation succeeded on Windows 2012.

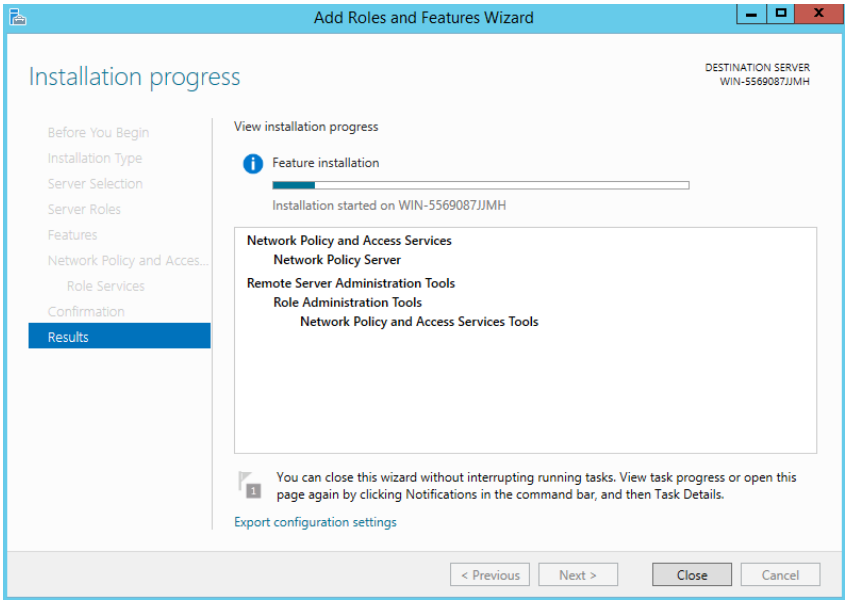

Figure 65 Installation begins

Active Directory integration

Next, create a group of authorized users to authenticate using Radius. The RADIUS-USERS group will list the user accounts allowed to authenticate on the radius server.

7) On the domain controller, open the Active Directory Users and Computers application. Create a new group inside the Users container.

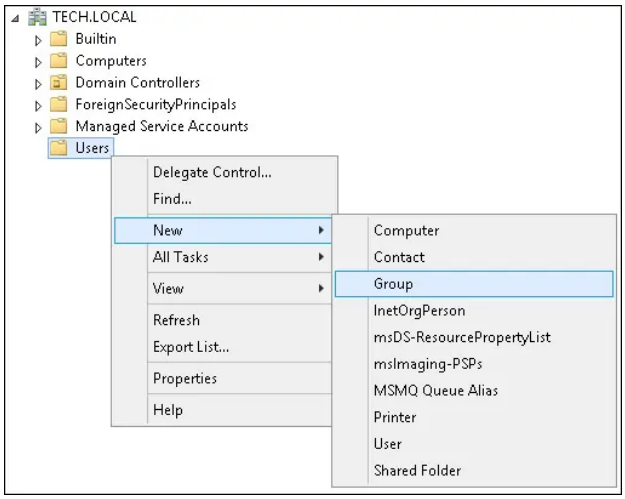

Figure 66 New group of users

8) Create a new group named: RADIUS-USERS. Members of this group will be allowed to authenticate on the Radius server.

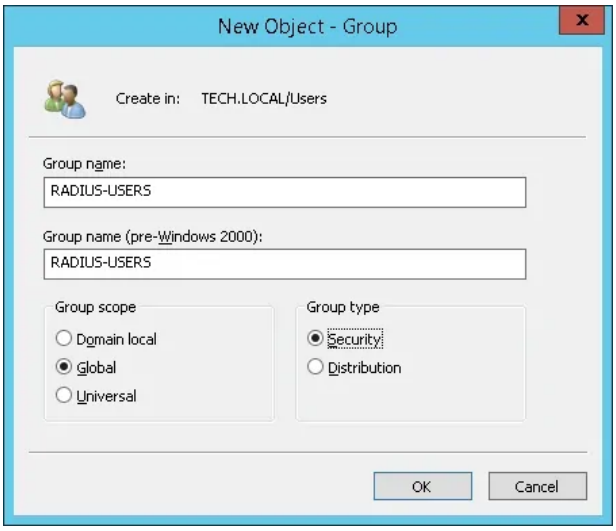

Figure 67 Group Configuration

9) Create a new user account inside the Users container.

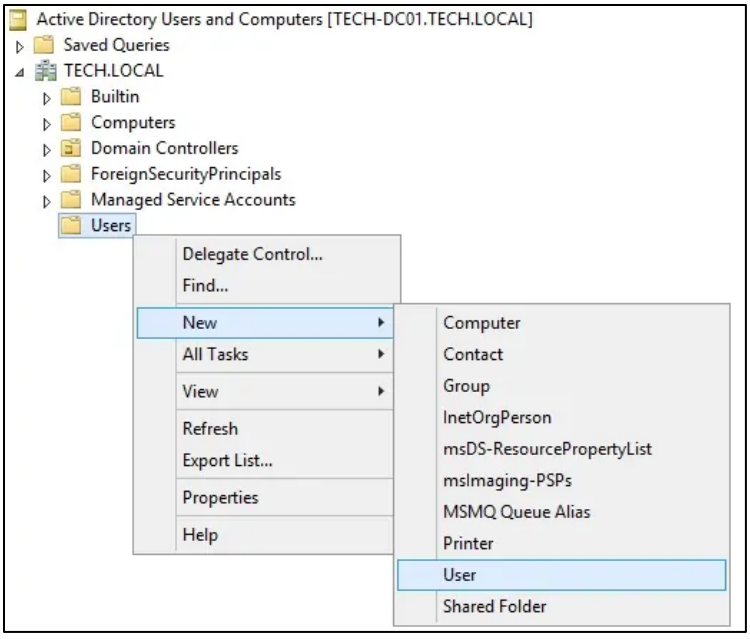

Figure 68 Create new user

10) Create a new user account named: VEGETA. The Vegeta user account will be allowed to authenticate on the Radius server.

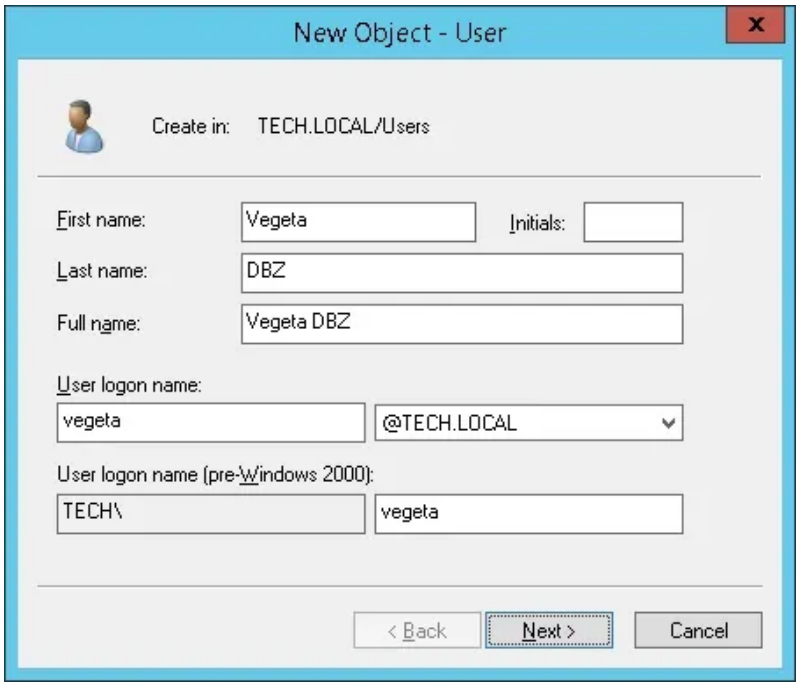

Figure 69 New user configuration

11) Set the Vegeta user account as a member of the RADIUS-USERS group.

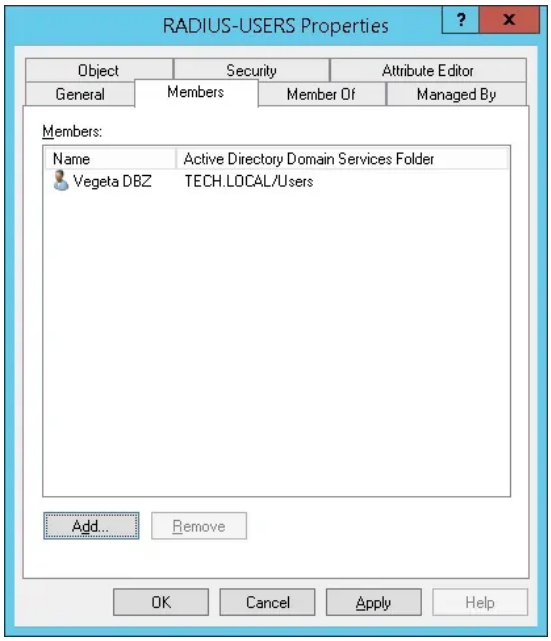

Figure 70 Assign new users in a new group

Add Client devices

On the Radius server, open the application named: Network Policy Server. It would help to authorise the Radius server on the Active Directory database.

12) Right-click on NPS(LOCAL) and select the Register server in the Active Directory option.

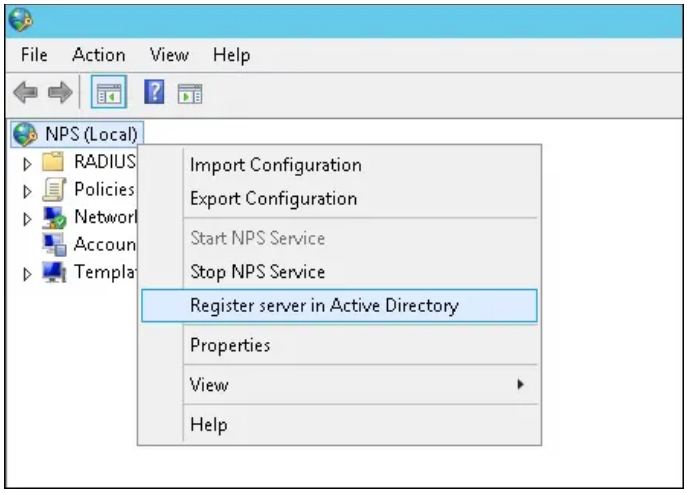

Figure 71 Register server in AD

13) On the confirmation screen, click on the OK button. Next, you need to configure Radius clients. (Friendly name, Device IP address, Device shared secret)

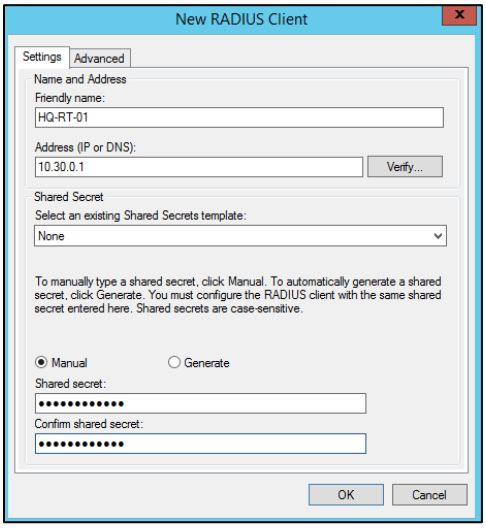

Figure 72 Radius client configuration

14) The radius client configuration finished

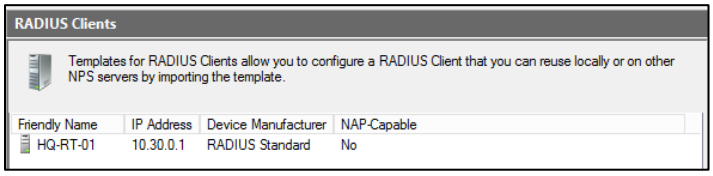

Figure 73 Radius clients list

Configure a Network Policy

Now, we need to create a Network Polity to allow authentication.

15) Right-click on the Network Policies folder and select the New option.

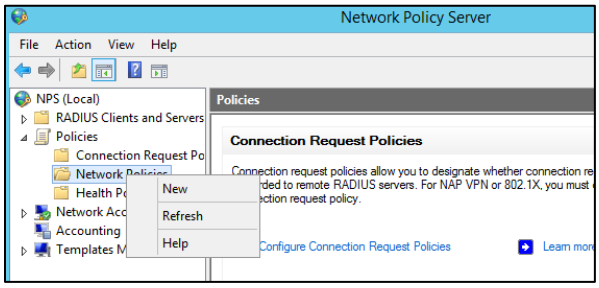

Figure 74 Network policy server dashboard

16) Enter a name to the network policy and click on the Next button.

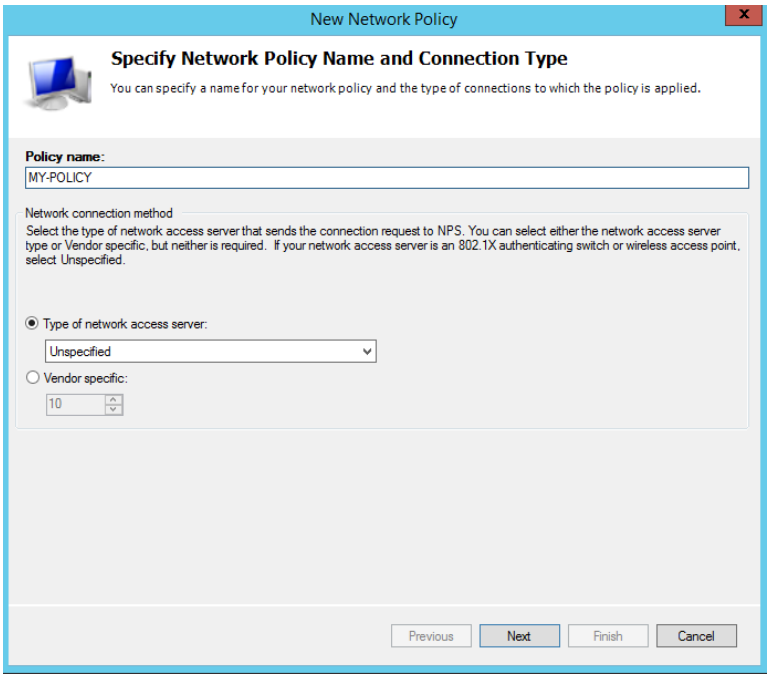

Figure 75 Create a new network policy

17) Click on the Add condition button. We are going to allow members of the RADIUS-SERS group to authenticate.

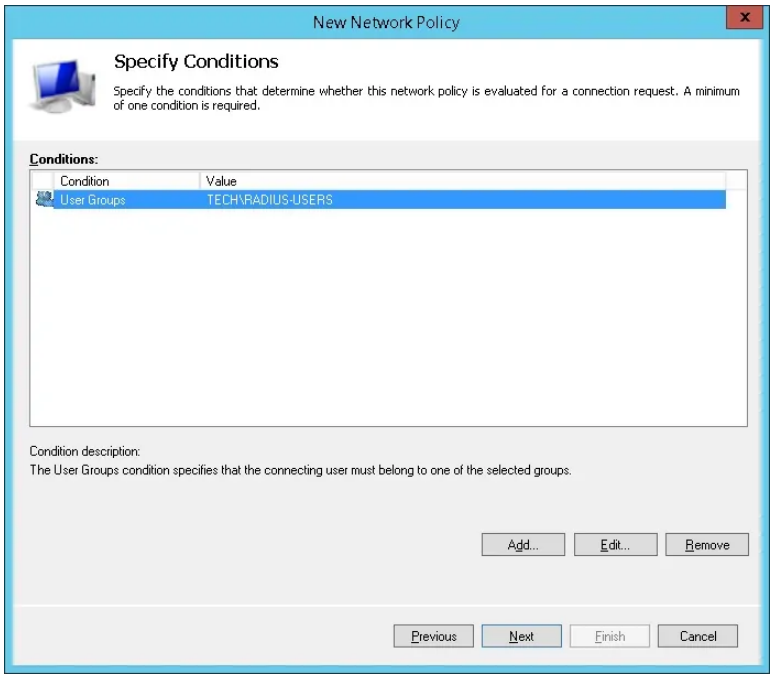

Figure 76 Assign group to network policy authentication

18) Select the User group option and click on the Add button.

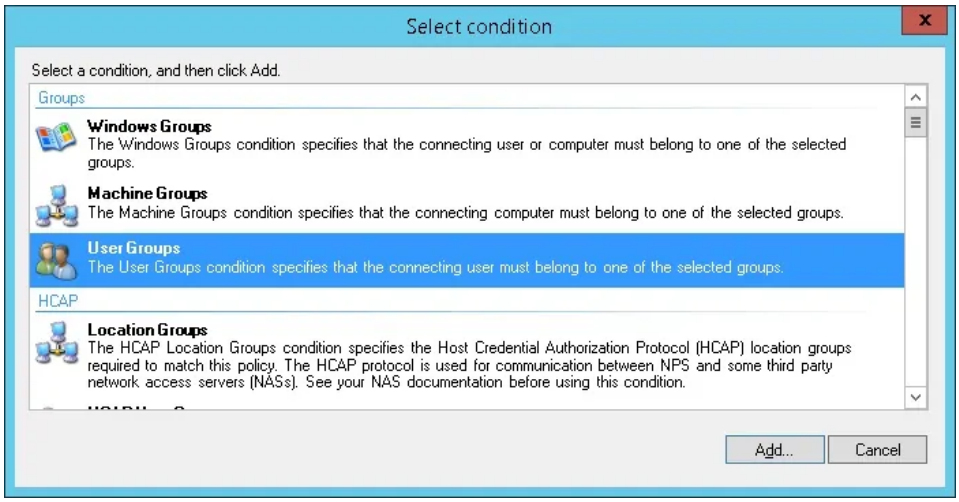

Figure 77 Select condition

19) Click on the Add Groups button and locate the RADIUS-USERS group.

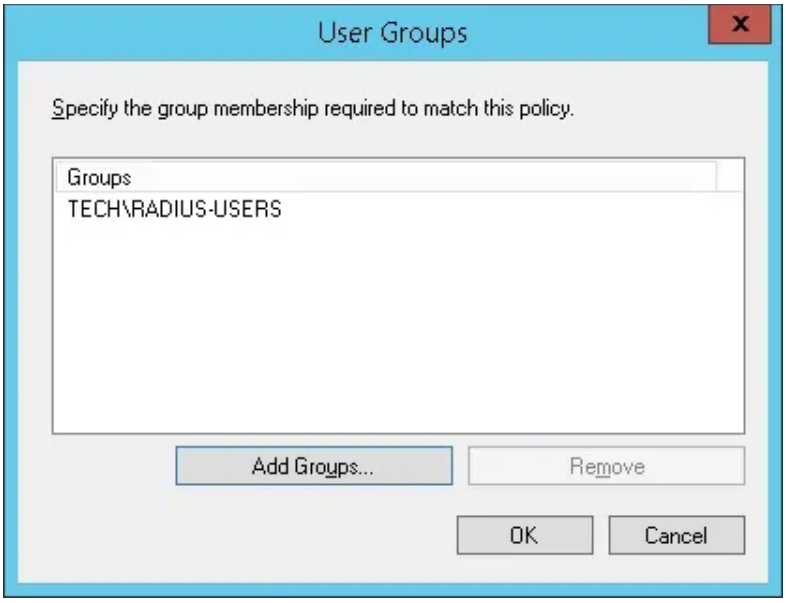

Figure 78 Assign group

20) Select the Access granted option and click on the Next button. This will allow members of the RADIUS-USERS group to authenticate on the Radius server.

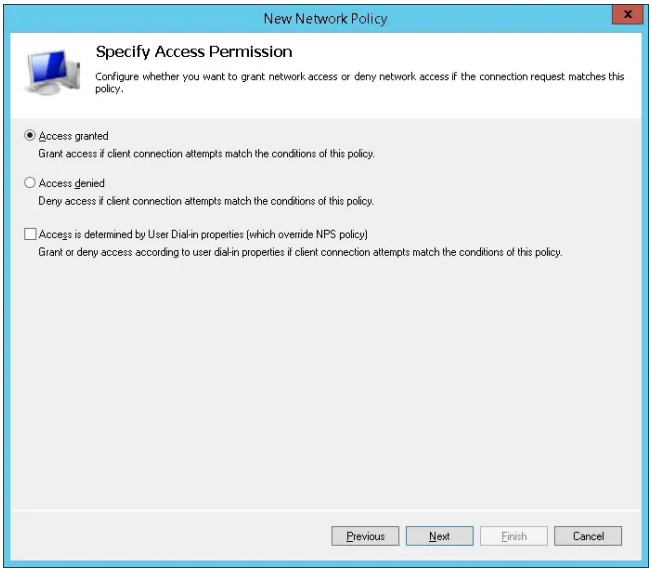

Figure 79 Network policy permission

21) Select the Unencrypted authentication (PAP, SPAP) option on the Authentication Methods screen.

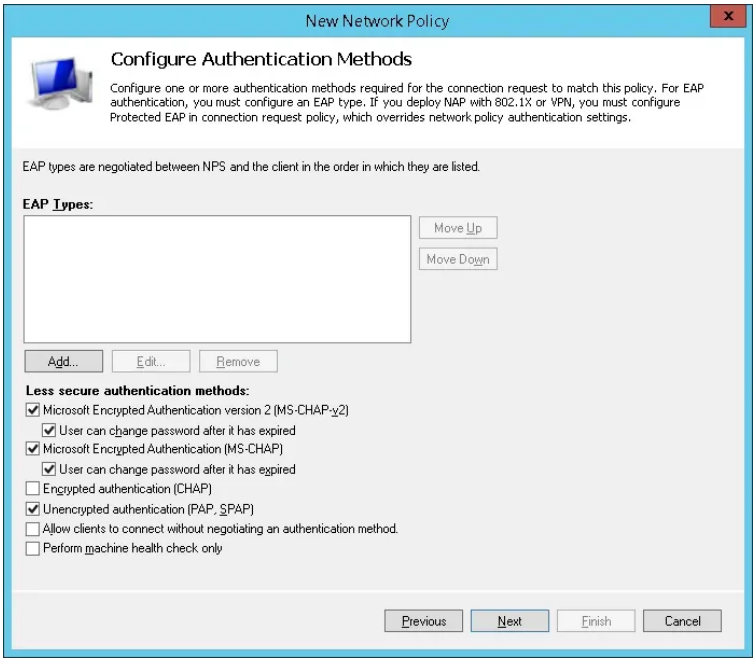

Figure 80 Network policy authentication encryption

22) If the following warning is presented, click on the No button.

Figure 81 Connection request policy pop-up

23) Verify the Radius server configuration summary and click on the Finish button.

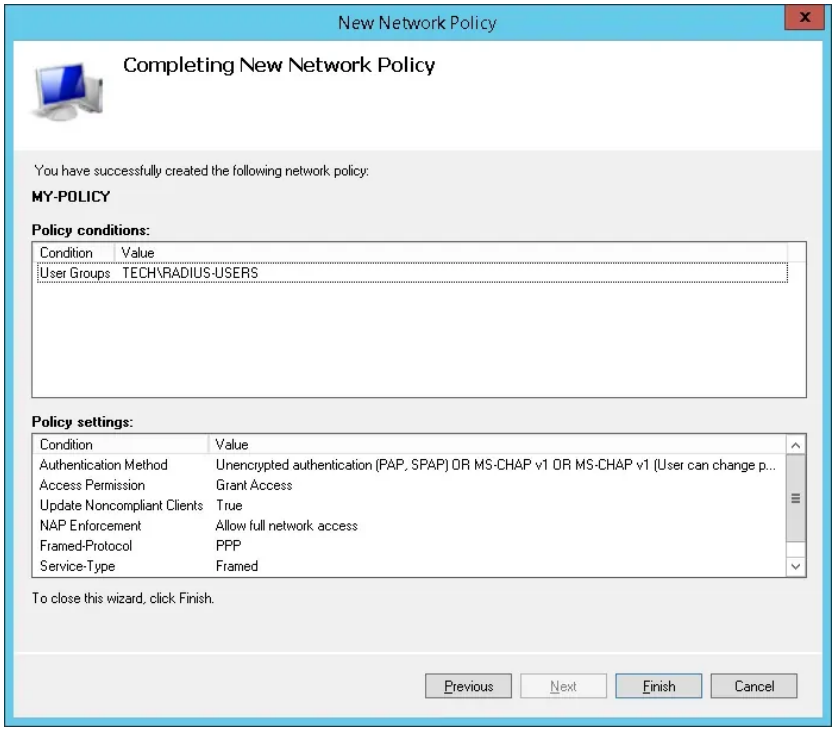

Figure 82 Radius server configuration summary

24) Radius server configuration finished.

Radius authentication configure on the router

1) Enable the new version of AAA authentication and specify the radius server and a group to use.

```
HQ-RT-01(config)#aaa new-model
HQ-RT-01(config)#aaa authentication login RADIUS-AUTHEN group radius local
```

Figure 83 Enable radius authentication

2) Specify which interface RADIUS will be accepting connections on.

```
HQ-RT-01(config)#ip radius source-interface e1/2.30
```

Figure 84 Assign port accept radius connection

3) Add radius-server host IP address and the key specified before at server.

```
HQ-RT-01(config)#radius-server host 10.30.0.10
HQ-RT-01(config)#radius-server key radiuspassword
```

Figure 85 Radius server IP and pre-shared key

4) Configure the same RADIUS group (RADIUS-AUTHEN) defined earlier under the vty lines as the authentication method to be used.

```
HQ-RT-01(config)#line con 0
HQ-RT-01(config-line)#login authentication RADIUS-AUTHEN
```

Figure 86 Enable radius authentication

5.3.6- DNS (IPv4)

1) Select DNS on the list of tools in Server Manager to open DNS manager

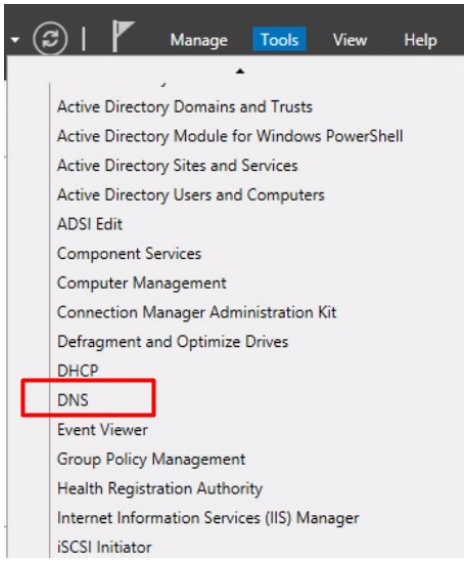

Figure 87 DNS in Server Manager

2) On DNS Manager, right-click the Forward Lookup Zone folder and select create New Zone

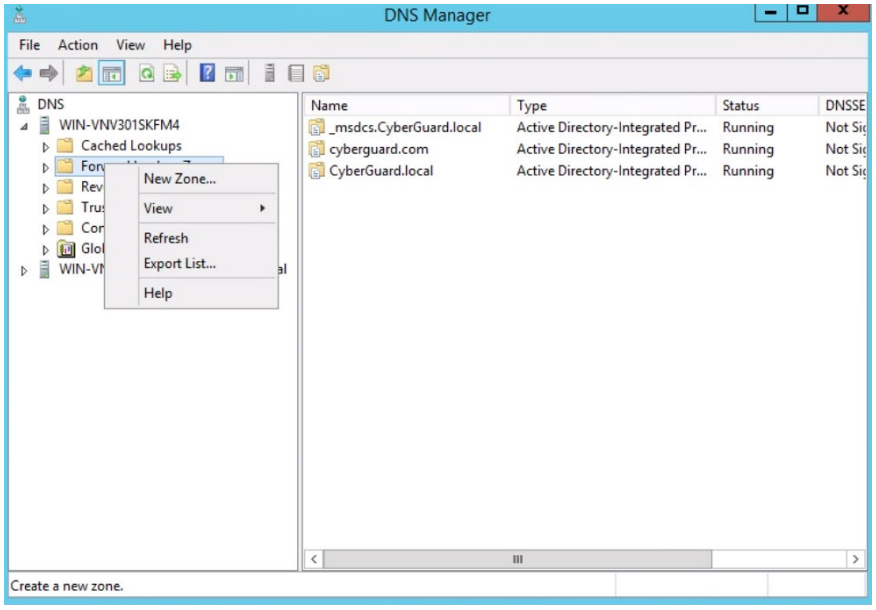

Figure 88 Forward Lookup Zone folder

3) A New Zone Wizard will appear that we can use to create a new zone

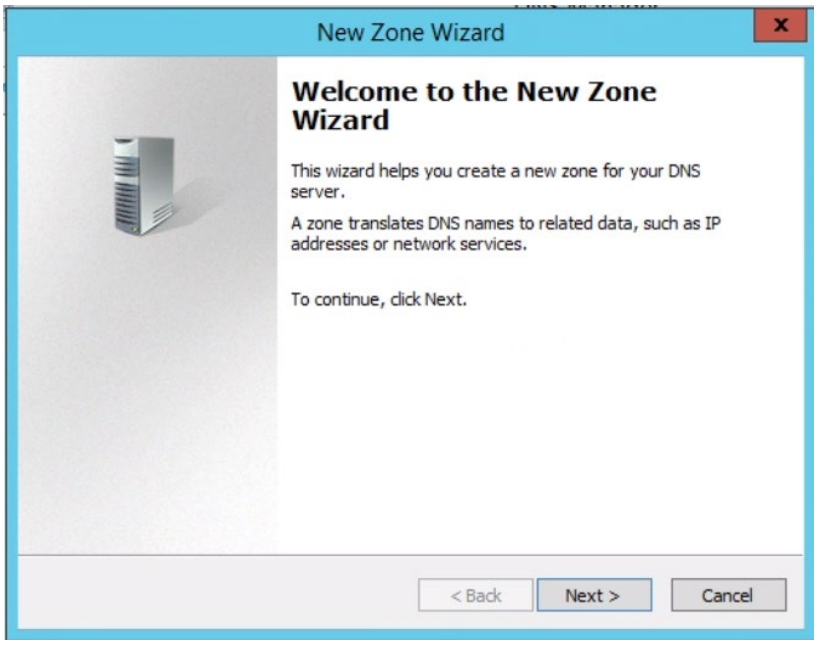

Figure 89 New Zone Wizard

4) Select primary zone and click next

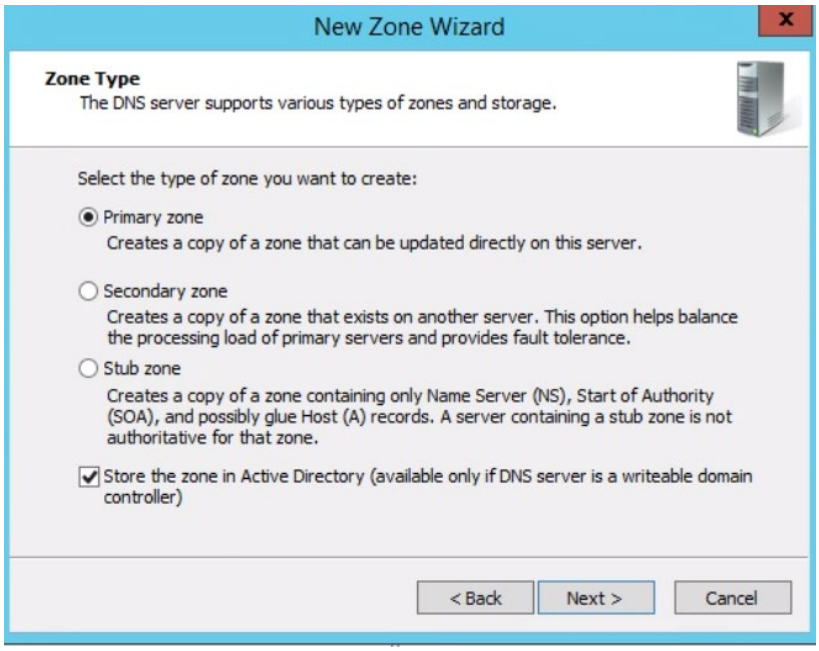

Figure 90 Zone Type

5) Select “To all DNS servers running on domain controllers in this domain” and click next

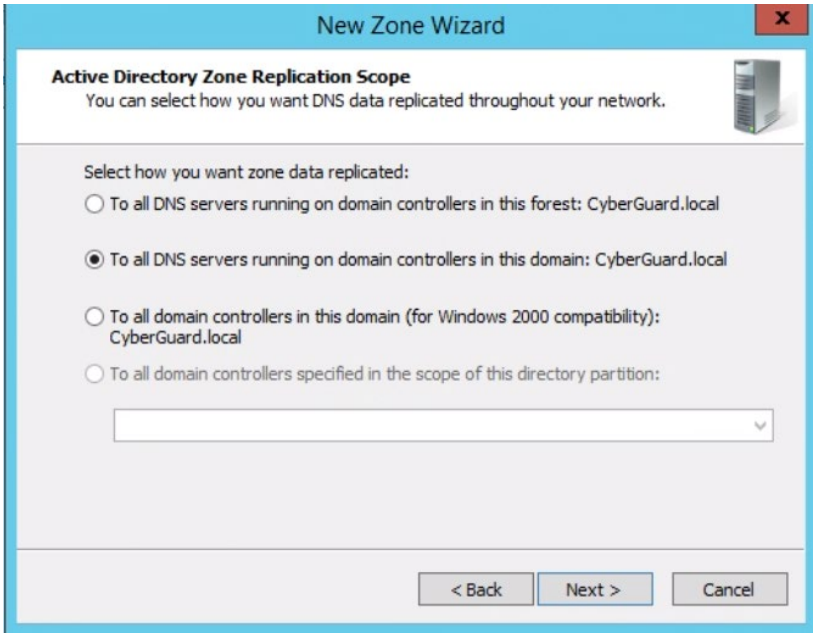

Figure 91 Active Directory Zone Replication Scope

6) Name the new zone, in our case it will be cyberguard.com, then click next

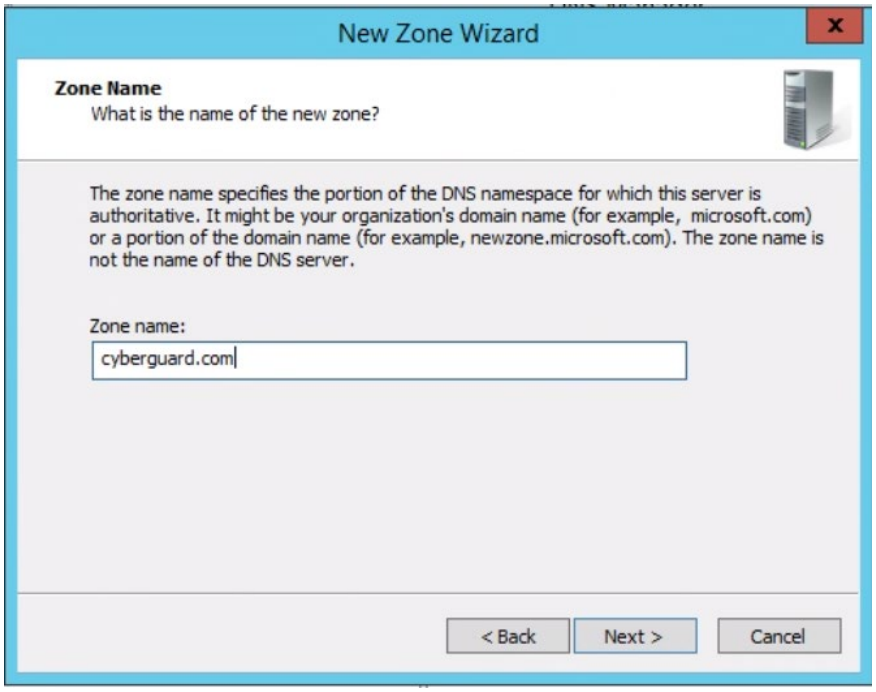

Figure 92 Zone Name

7) Select “Allow both nonsecure and secure dynamic updates” then click next

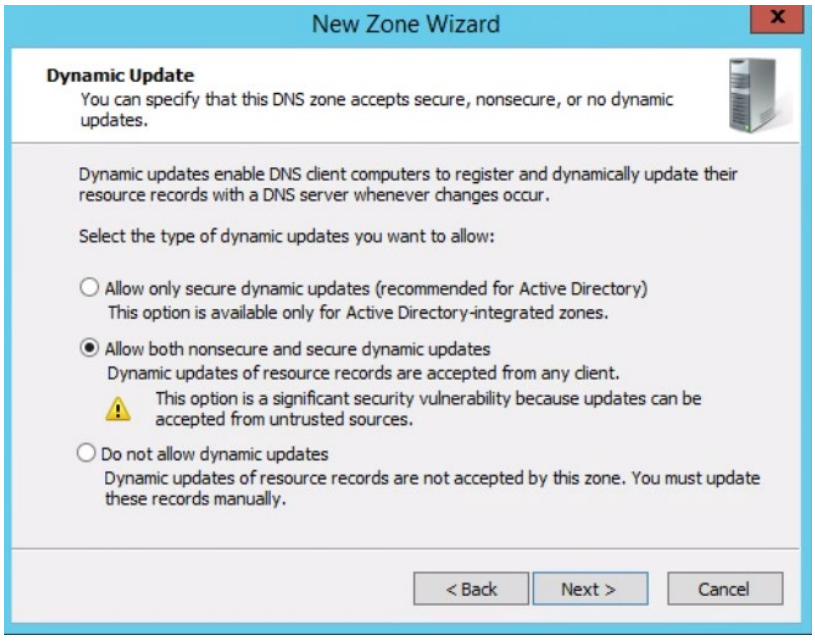

Figure 93 Dynamic Update

8) After checking the configuration, click finish

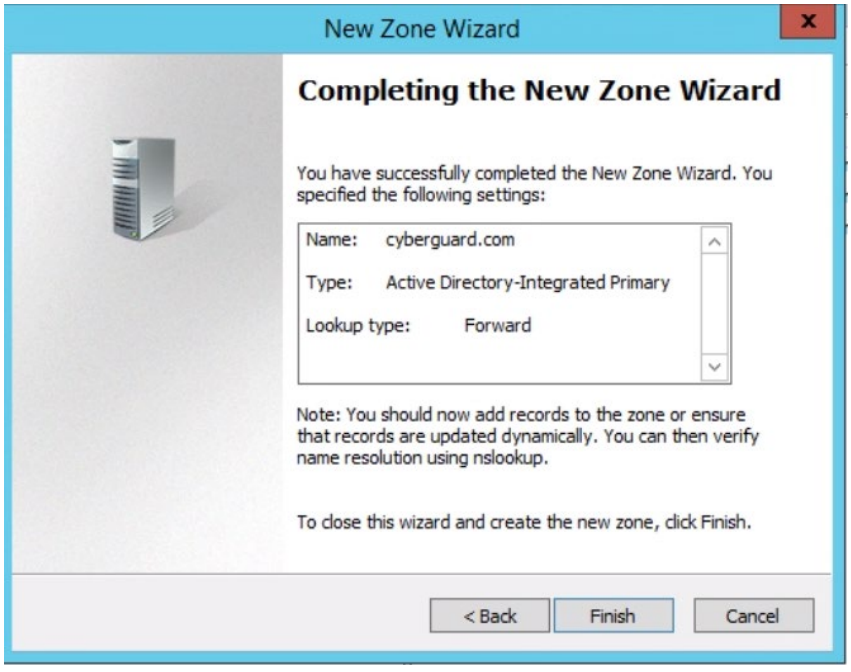

Figure 94 Completing the New Zone Wizard

9) Select the created lookup zone and right click in the displayed directory, select "New Host (A or AAAA)

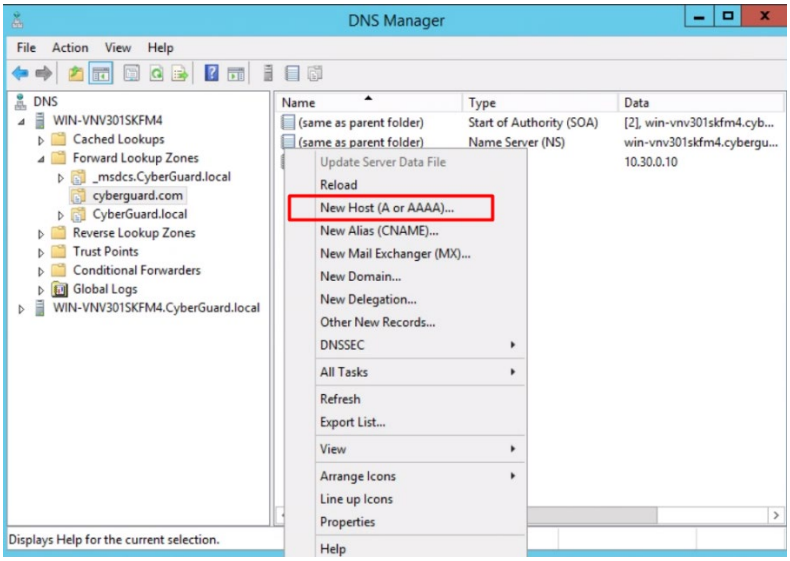

Figure 95 New DNS Host

10) Enter the name and IP address of the new host then click Add Host

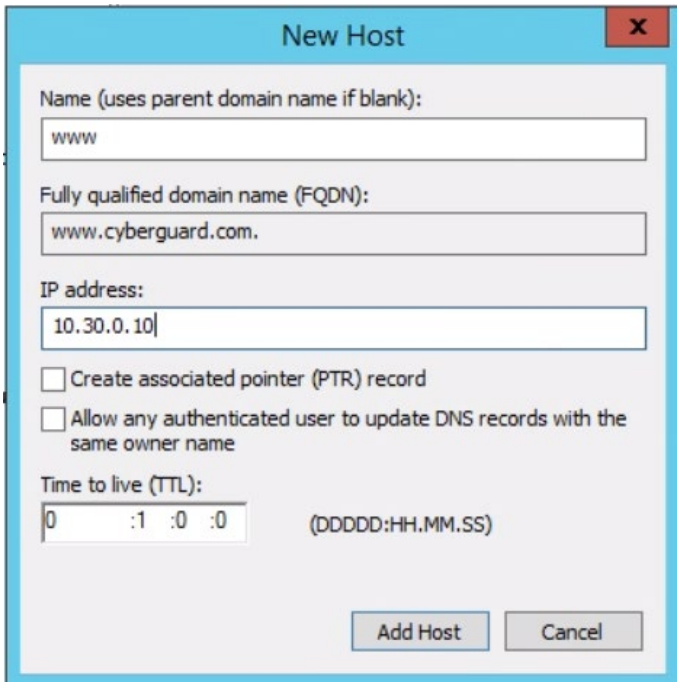

Figure 96 New Host

5.3.7- DHCP (IPv4)

Installation

1) Install the DHCP Server using the apt command as shown in the figure below

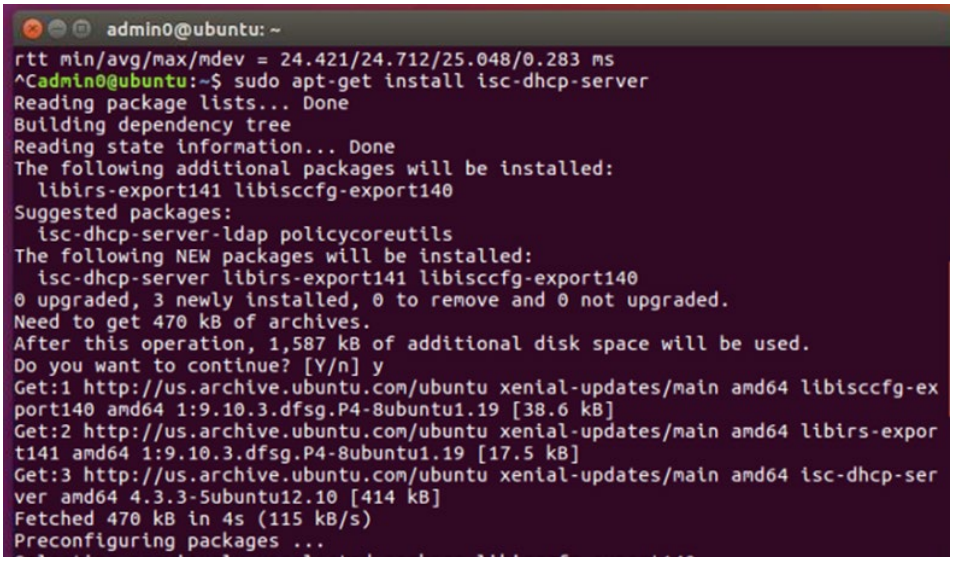

Figure 97 Installing DHCP Server using apt

Configuration

2) By using Gedit editor, open the configuration file.

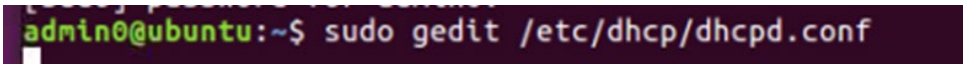

Figure 98 Open the configuration file using the editor

3) When the configuration file opens, assign a random IP Address range. The settings are the same as follows:

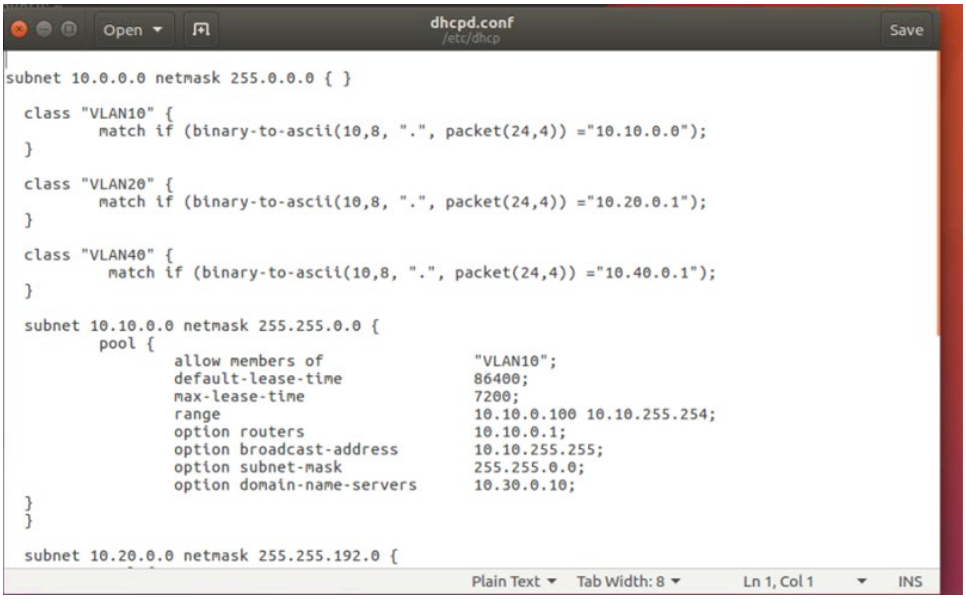

Figure 99 The range of IP address

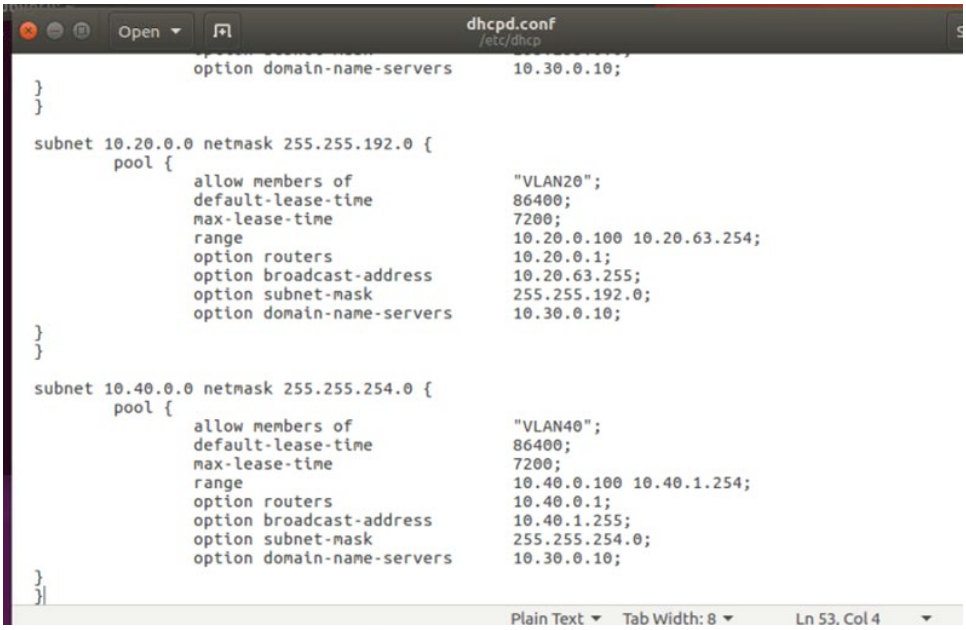

Figure 100 The range of IP address

According to this configuration:

- The default lease time for a client is 24 hours minutes (86400 seconds), and the maximum lease time is 2 hours (7200 seconds).
- The server will hand over the IP address from the range 10.10.0.100 to 10.10.255.254 for VLAN10, 10.20.0.100 to 10.20.63.254 for VLAN20, and 10.40.0.100 to 10.40.1.254 for VLAN40.
- The Domain Name Server (DNS) is the same, 10.30.0.10.

4) Save the configuration file by entering CTRL X and choosing Y to agree to change the configuration file. Then, click Enter.

5) Restart the DHCP Server to enable the changes in the configuration file.

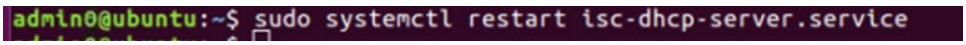

Figure 101 Restart the DHCP Server

6) Check the status of the DHCP Server.

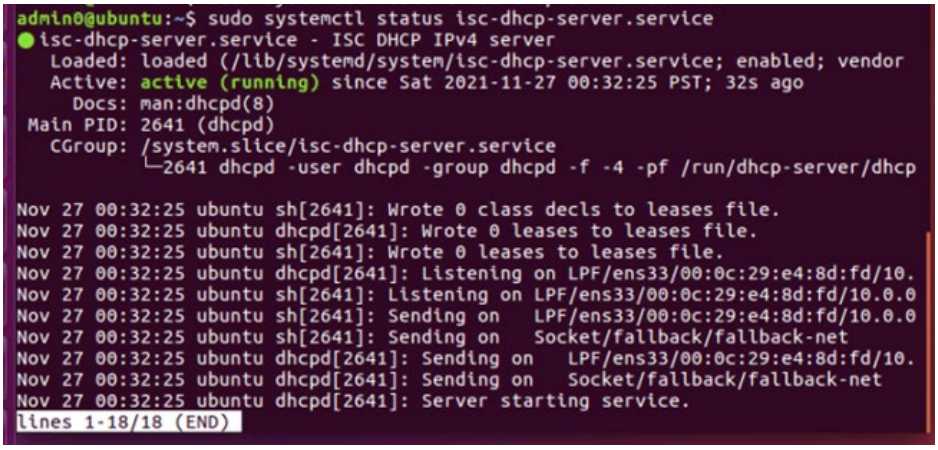

Figure 102 Status of DHCP Server

7) Do IP helper at the router HQ by typing these commands:

HQ-RT-01#conf t

HQ-RT-01(config)#int ethernet0/2.10

HQ-RT-01(config-subif) #ip helper-address 10.30.0.11

HQ-RT-01(config)#int ethernet0/2.20

HQ-RT-01(config-subif) #ip helper-address 10.30.0.11

HQ-RT-01(config)#int ethernet0/2.40

HQ-RT-01(config-subif) #ip helper-address 10.30.0.11

Note: Do IP helper for VLAN10, VLAN20, and VLAN40. VLAN30 does not require IP helper because it is static IP address.

```
!
interface Ethernet1/2.10
 encapsulation dot1Q 10
 ip address 10.10.0.1 255.255.0.0
 ip helper-address 10.30.0.11
 ip nat inside
 ip virtual-reassembly in
 nat64 enable
!
interface Ethernet1/2.20
 encapsulation dot1Q 20
 ip address 10.20.0.1 255.255.192.0
 ip helper-address 10.30.0.11
 ip nat inside
 ip virtual-reassembly in
 nat64 enable
!
interface Ethernet1/2.30
 encapsulation dot1Q 30
 ip address 10.30.0.1 255.255.255.0
 ip directed-broadcast
 ip nat inside
 ip virtual-reassembly in
 nat64 enable
!
interface Ethernet1/2.40
 encapsulation dot1Q 40
 ip address 10.40.0.1 255.255.254.0
 ip helper-address 10.30.0.11
 ip nat inside
 ip virtual-reassembly in
 nat64 enable
!
```

Figure 103 IP helper in HQ router

5.3.8- User Authentication by Integrating AD with Linux

Integrating Linux authentication with Active Directory

1) Specify the full domain controller name in /etc/hosts file using the command ‘sudo nano /etc/hosts’. Then, enter the domain controller IP address and domain name.

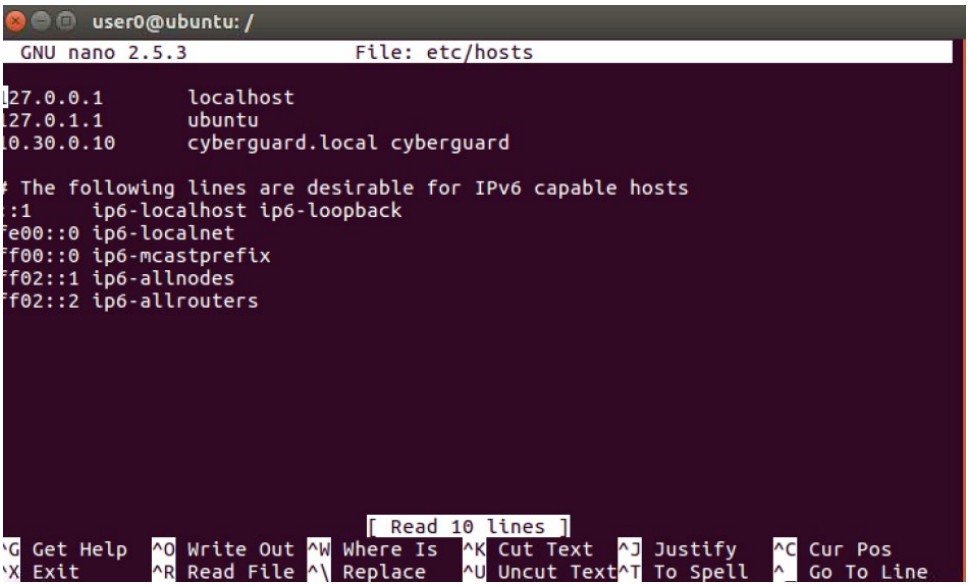

Figure 104 /etc/hosts file

2) Set a DNS server address on the linux machine with command ‘sudo nano /etc/resolvconf/resolv.conf.d/head’. Then, add the domain controller IP address, search address and nameserver.

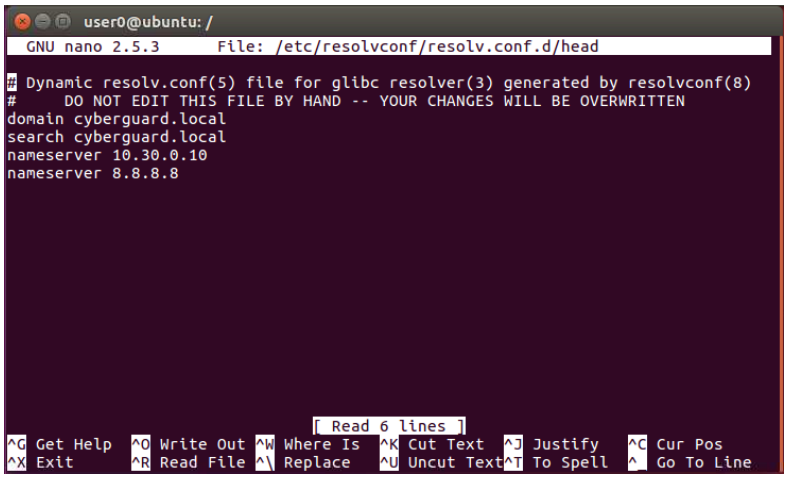

Figure 105 Setting DNS server address

3) Install all dependencies such as time synchronization NTP, Kerberos client, Samba, SSSD, and Winbind with the command 'sudo apt-get install ntp krb5-user libpam-krb5 libpam-ccreds auth-client-config samba winbind realmd sssd sssd-tools adcli samba-common-bin'

4) Upon installing Kerberos, this menu will pop up in the terminal. You can change this settings later in Kerberos configuration file but for now internet the domain name which is 'CYBERGUARD.LOCAL'

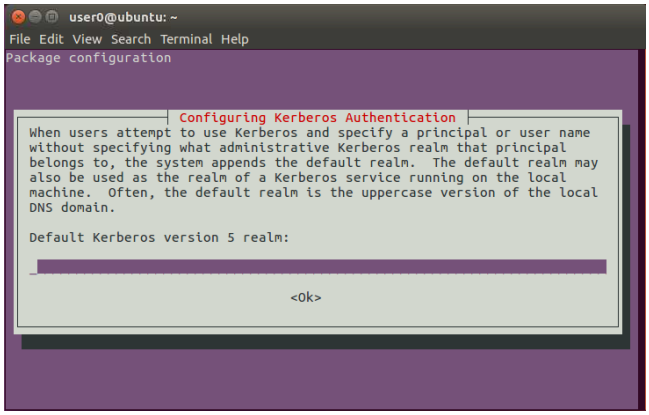

Figure 106 Configuring Kerberos Authentication

5) Configure the time synchronization NTP with the command 'sudo nano /etc/ntp.conf'. Specify the NTP server by inserting the line 'server www.cyberguard.com'. Then, restart the ntpd daemon with 'sudo /etc/init.d/ntp restart'.

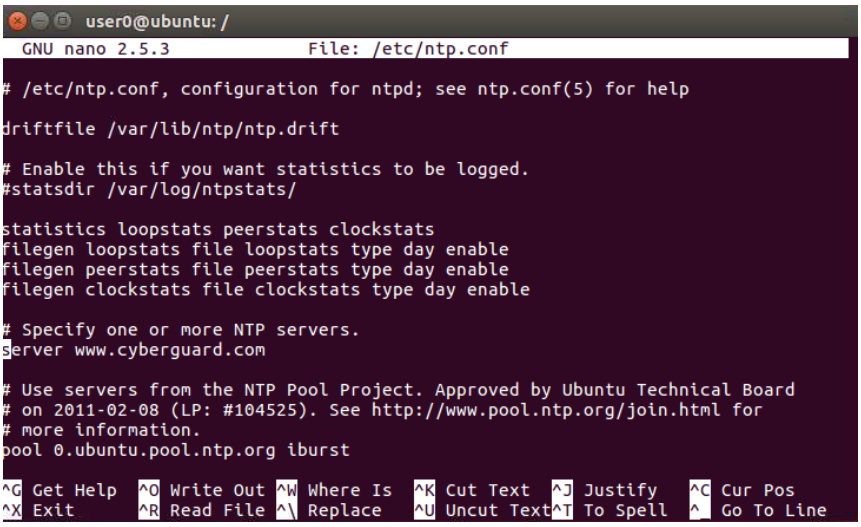

Figure 107 Configuring Time Synchronization

6) Edit Kerberos configuration file using the command 'sudo nano /etc/krb5.conf' and make sure to enter the domain controller name in the realm parameter.

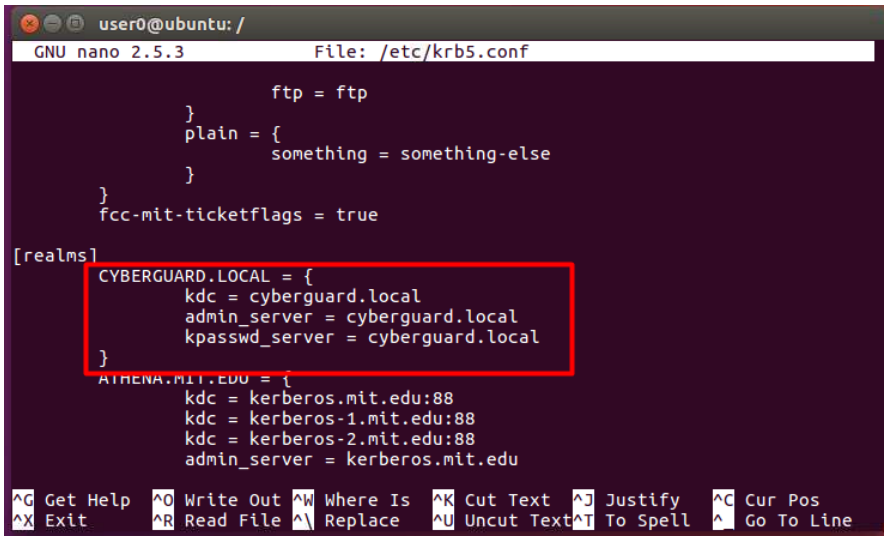

Figure 108 Entering controller name in Kerberos

7) Edit the samba configuration file with the command 'sudo nano /etc/samba/smb.conf'. Enter the following settings under the global parameter.

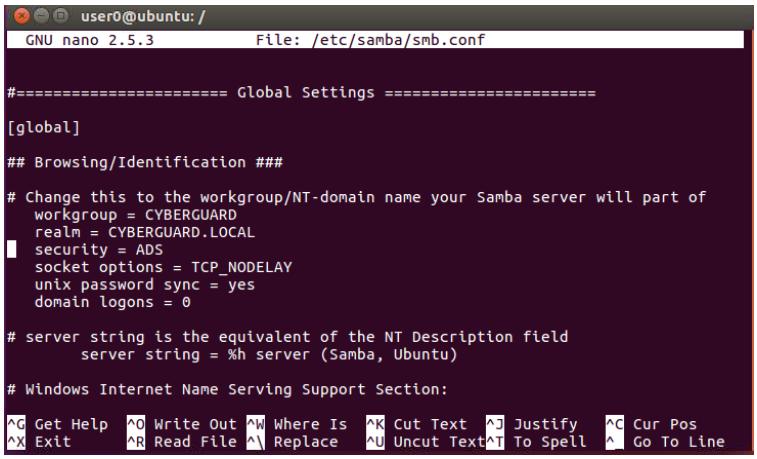

Figure 109 Editing Samba Configuration

8) Type in the command ‘realm list’ to list our Kerberos settings to make sure everything is in order.

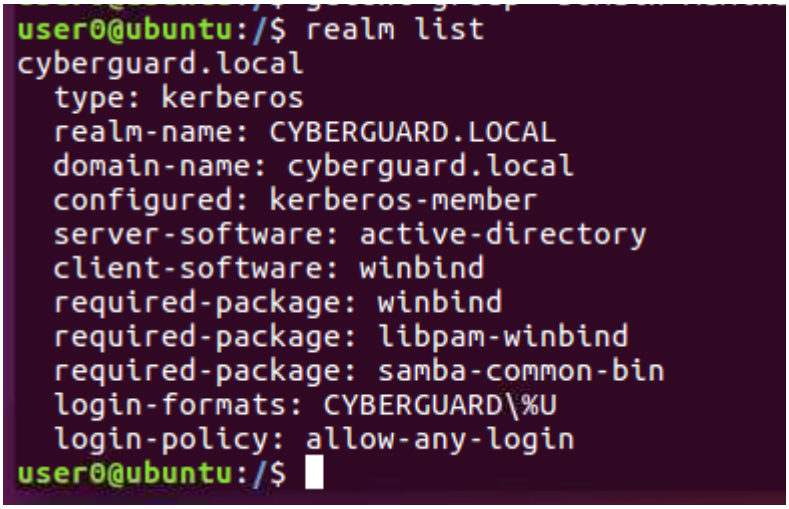

Figure 110 Realm List

5.3.9- Windows Server Hardening Vulnerability Report

Install Nmap

1) Click the Nmap Setup, and then a Nmap Setup window will appear. Click I Agree.

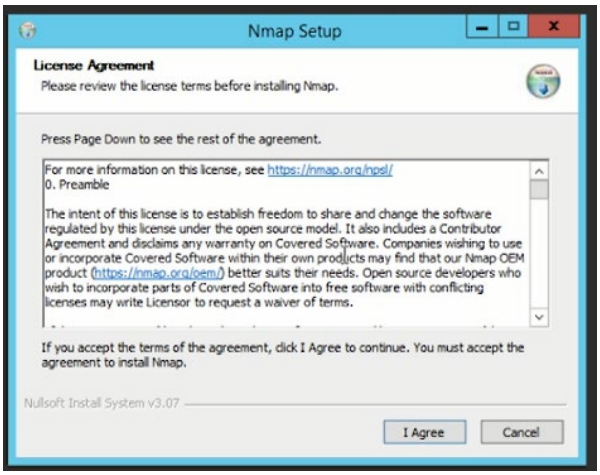

Figure 111 License Agreement for Nmap

2) Click Next button

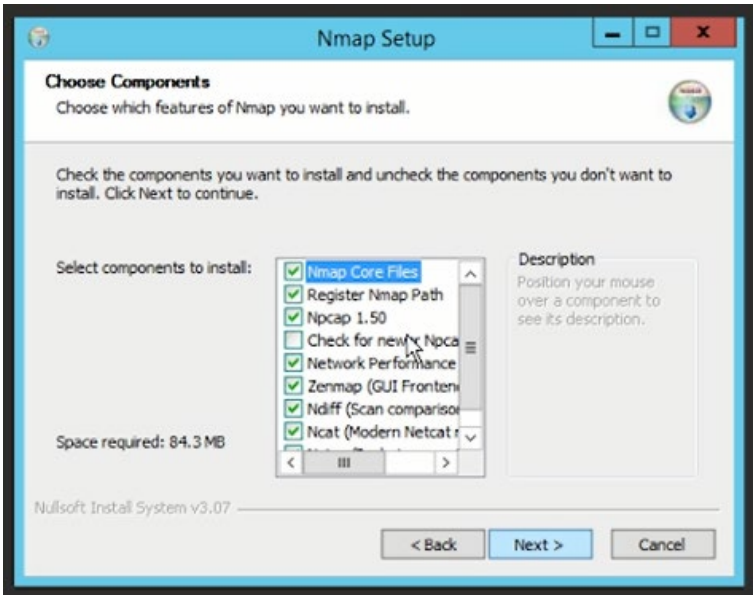

Figure 112 Choose Component

3) Choose where the location to install Nmap and click Install.

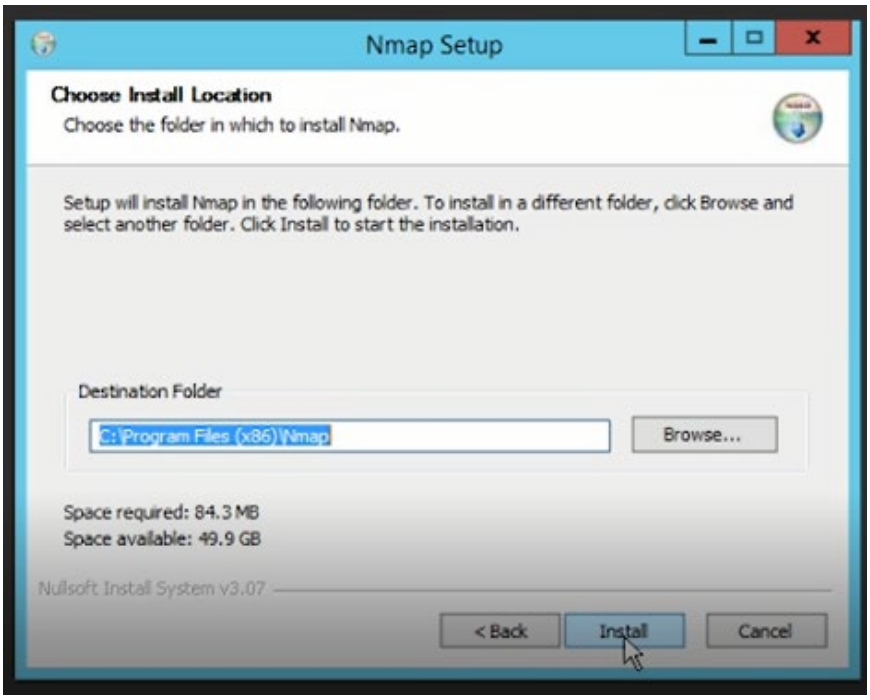

Figure 113 Choose a location to install Nmap

4) Wait for the installation to be complete.

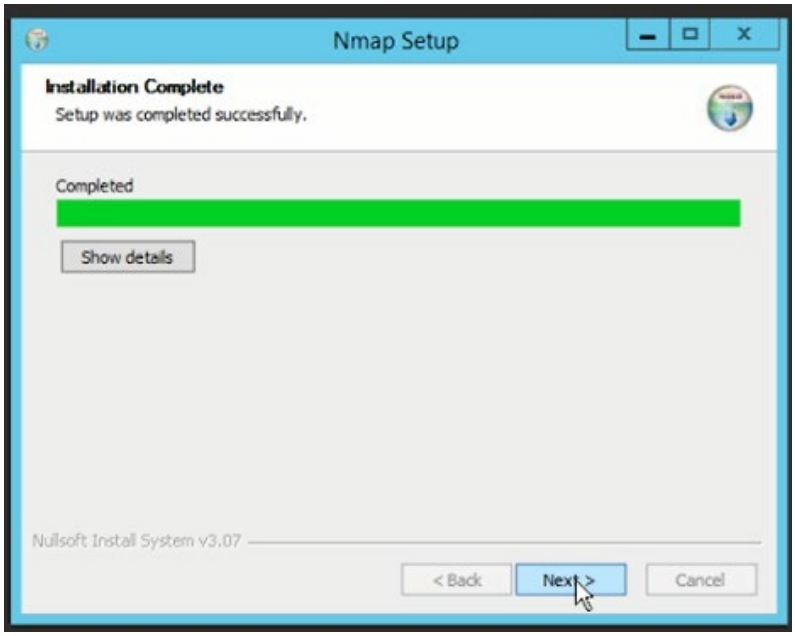

Figure 114 Nmap installation complete

5) After the installation has been complete, click the Finish button.

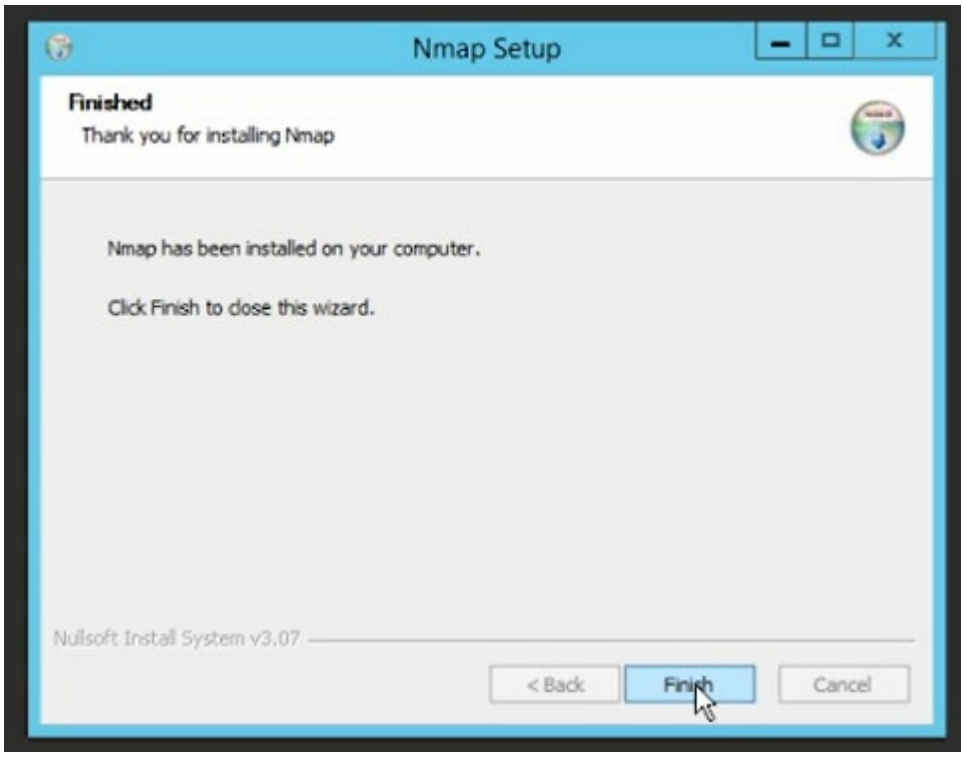

Figure 115 Nmap setup finish

6) Open Nmap. Insert Window Server IP address at the target column and start a Quick Scan to search for an open port.

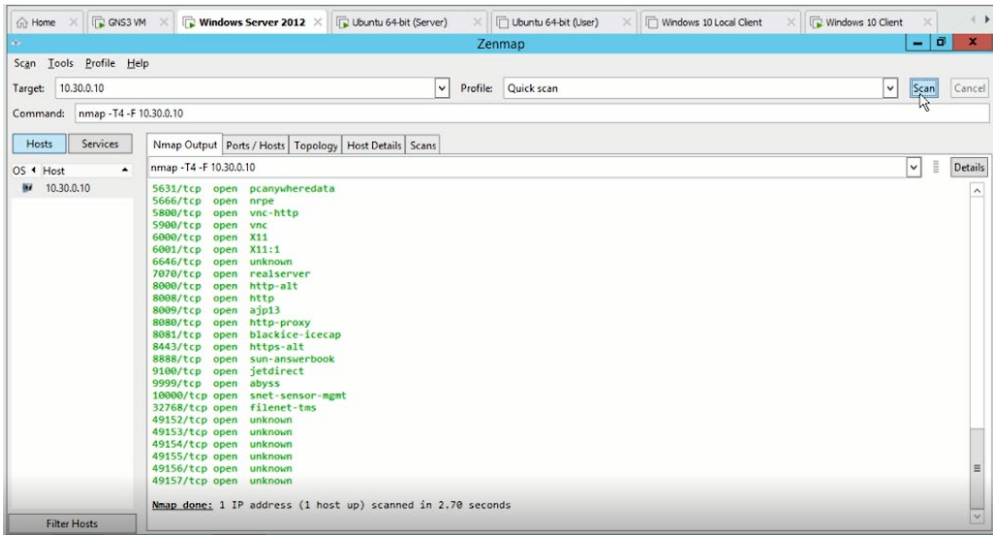

Figure 116 Nmap scanning

Updates patches

1) Search for Windows Update

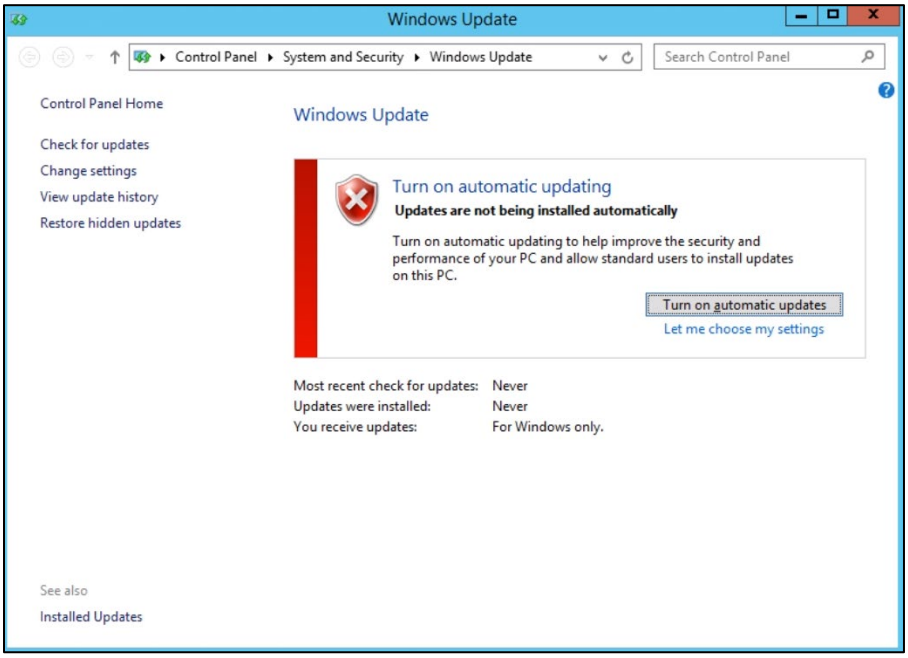

Figure 117 Check for Windows Update

2) Change settings to Install updates automatically and click OK.

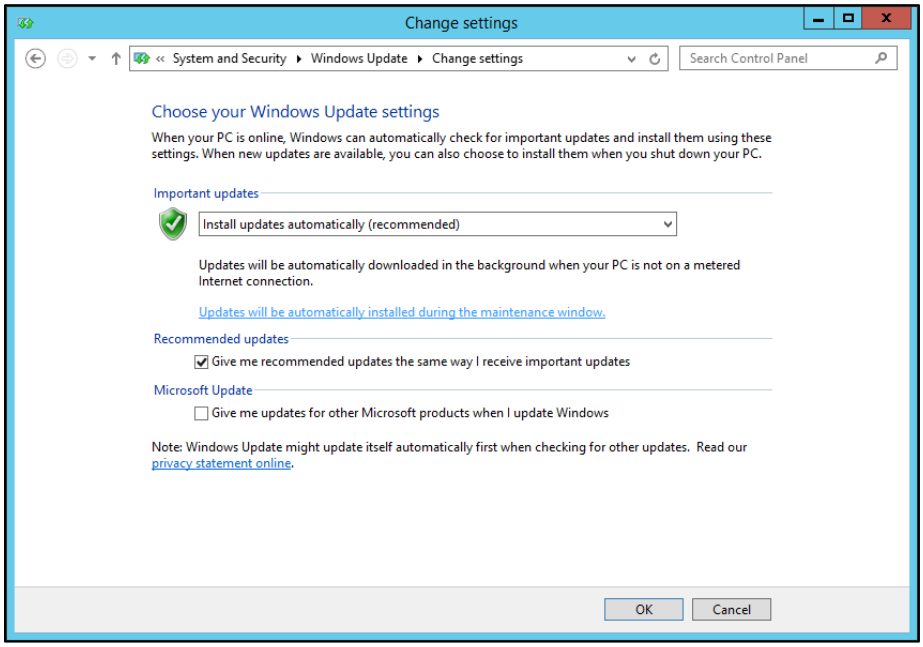

Figure 118 Turn on automatic updates

Enable account lockout policy

1) Go to Start > Administrative Tools > Group Policy Management.

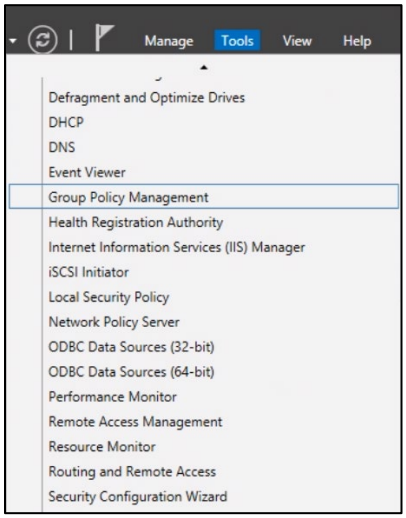

Figure 119 Open Group Policy Management

2) Expand Forest: CyberGuard.local > Domains> CyberGuard.local >right click Default Domain Policy and click edit.

3) Expand Computer Configuration> Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.

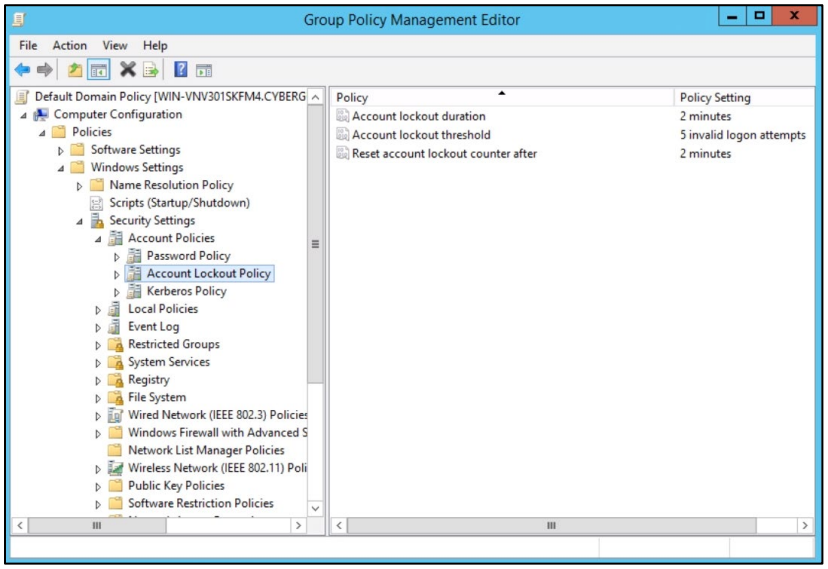

Figure 120 Account Lockout Policy

4) Set the Account lockout threshold Properties to Account will lockout after 3 invalid login attempts.

5) Set both Account lockout duration and reset account lockout counter after 2 minutes.

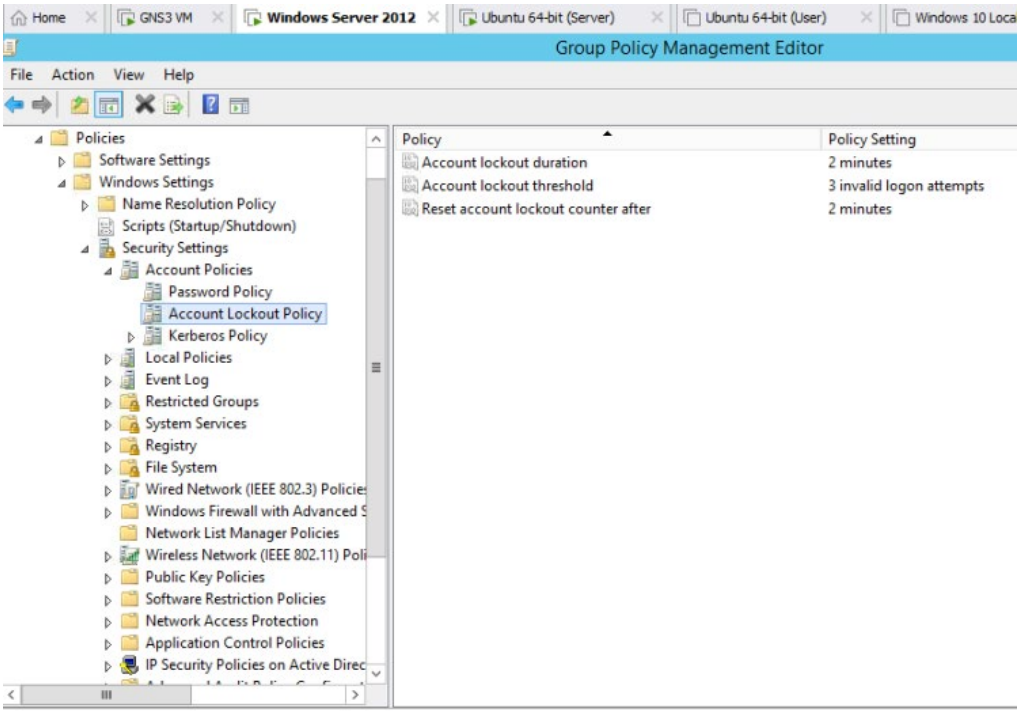

Figure 121 Show the new Account Lockout Policy

Enable Password Policy

1) Go to Start > Administrative Tools > Group Policy Management.

2) Expand Forest: CyberGuard.local > Domains> CyberGuard.local >right click Default Domain Policy and click edit.

3) Expand Computer Configuration> Policies > Windows Settings > Security Settings > Account Policies > Password Policy.

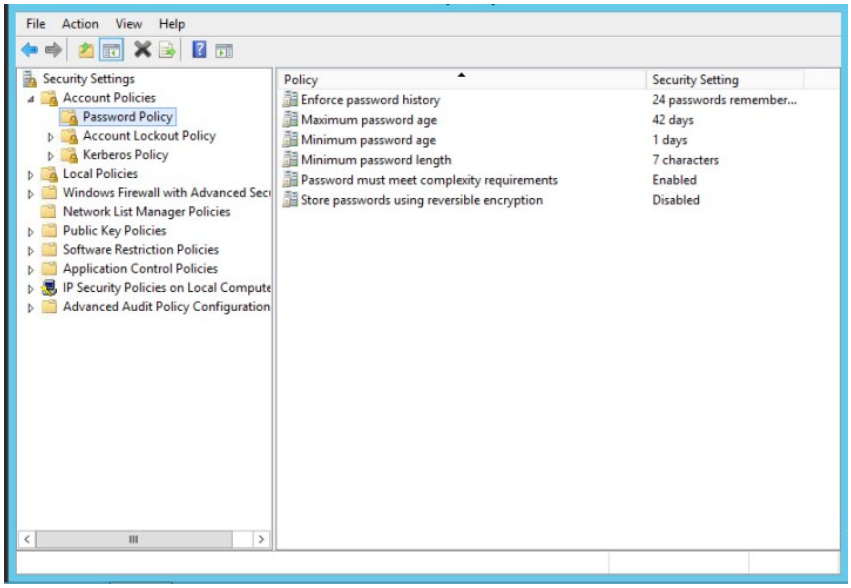

Figure 122 Unedited Password Policy

4) Set the enforce password history to 10, maximum password age to 80, minimum password age to 3, and minimum password length to 8.

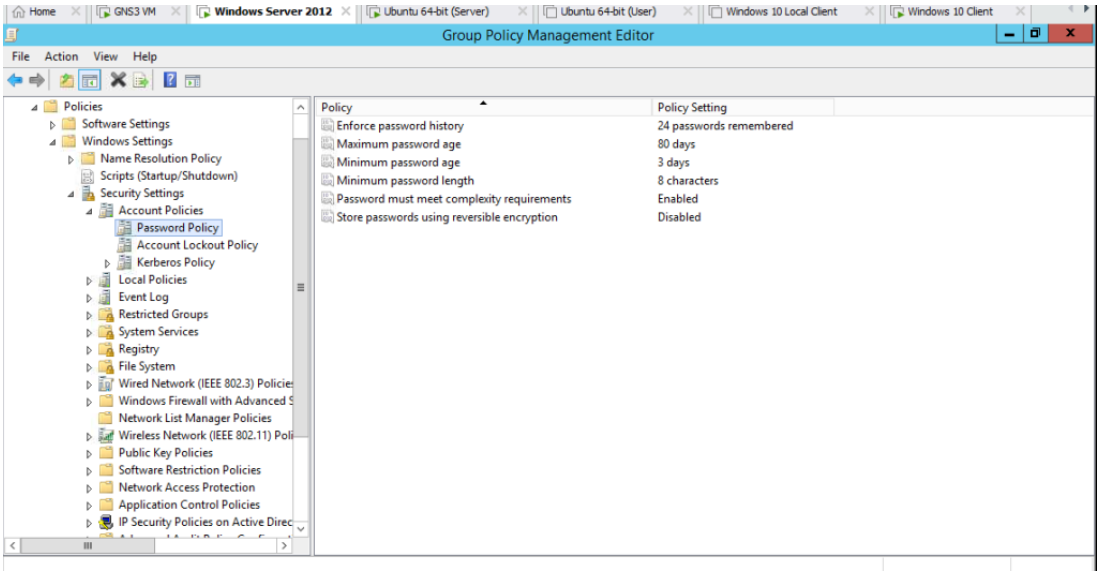

Figure 123 Password Policy

Enable Windows Firewall

1) Open Server Manager > Tools > click Windows Firewall with Advanced Security.

2) Change the Firewall for Domain, Private and Public to on and ensure all inbound connections are blocked.

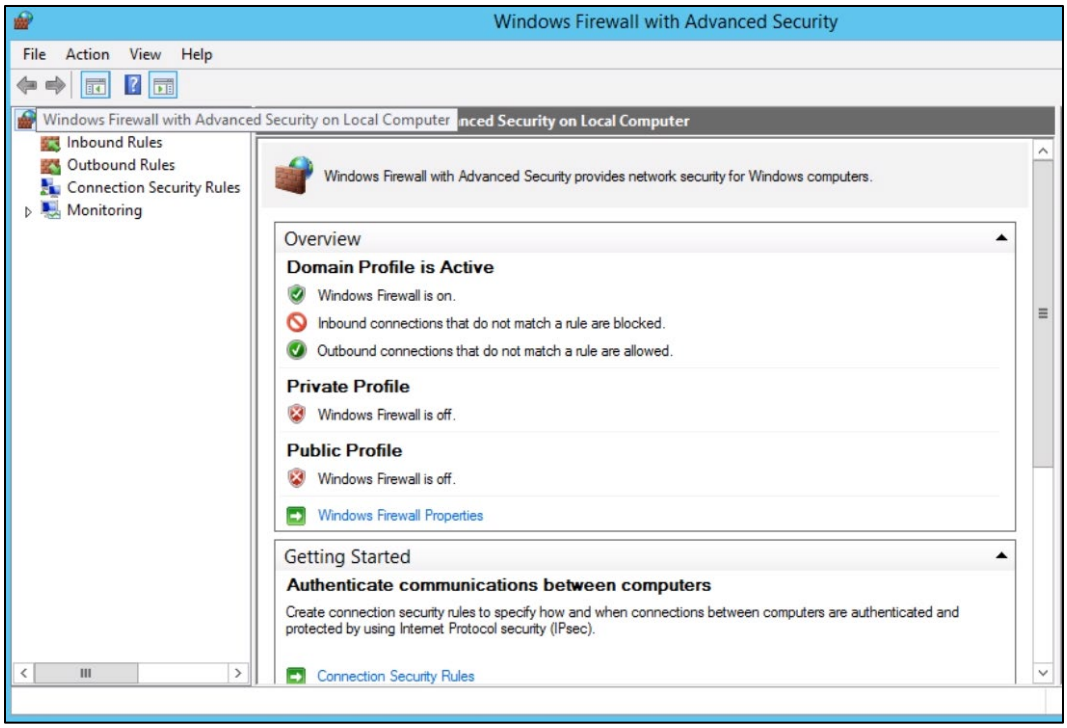

Figure 124 Firewall status

Configuring auditing

1) Go to Server Manager > Tools > Group Policy Management.

2) On the left side expend Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies.

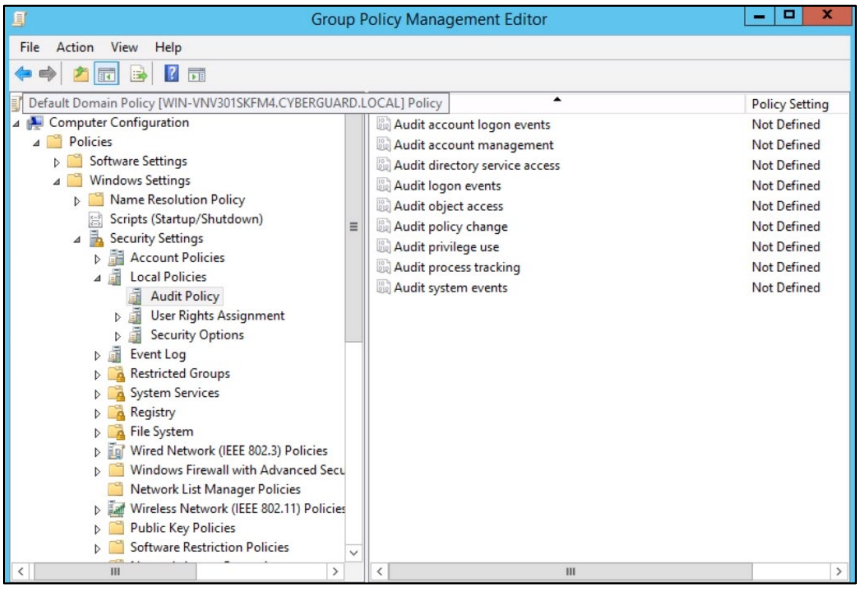

Figure 125 Audit Policy

3) Then modify the policies based on the audit's success and failure attempts.

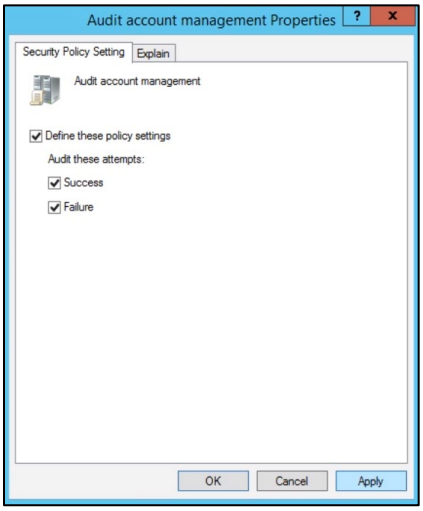

Figure 126 Audit account management properties

Disable automatic service

1) Open the Run dialogue box and type in “services.msc” to open Services.

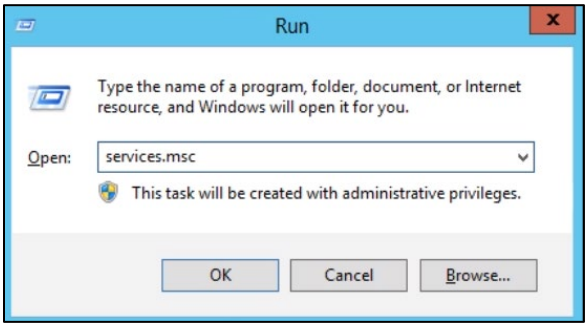

Figure 127 Run dialogue box

2) Change the start-up type of Distributed Transaction Coordinator Properties from Automatic to Disabled.

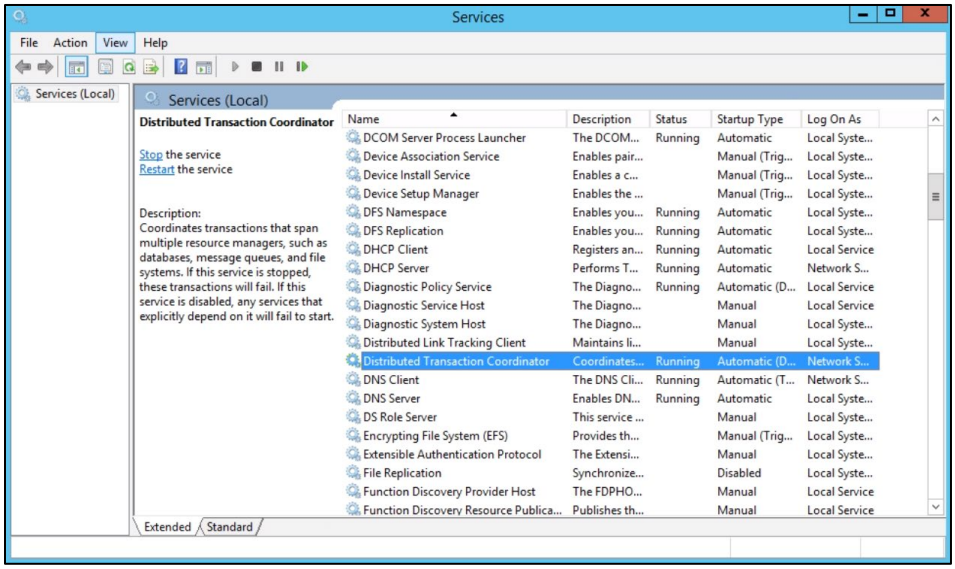

Figure 128 Distributed Transaction Coordinator

Reason: Coordinates transactions distributed across multiple computer systems and resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers. We are not using this service, so we just disabled it.

3) Stop the Print Spooler service and change its startup to ‘disabled.’

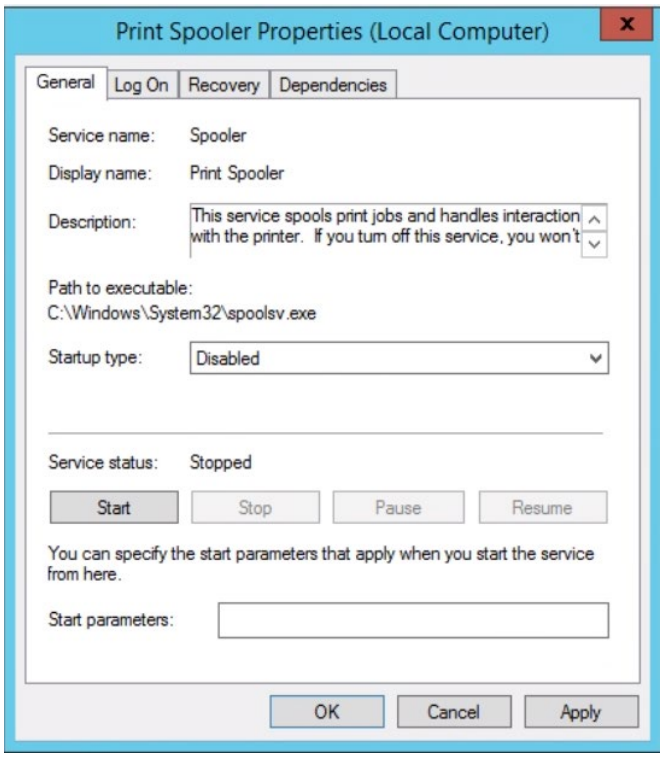

Figure 129 Print Spooler Properties

Reason: Since we are not using the Print Spooler service, we can disable it on our server. This service has a history of exploitable vulnerabilities, so that we will be turning this service off.

Disable or delete Unnecessary Accounts

1) Go to Server Manager > Tools > Active Domain Services and Computer.

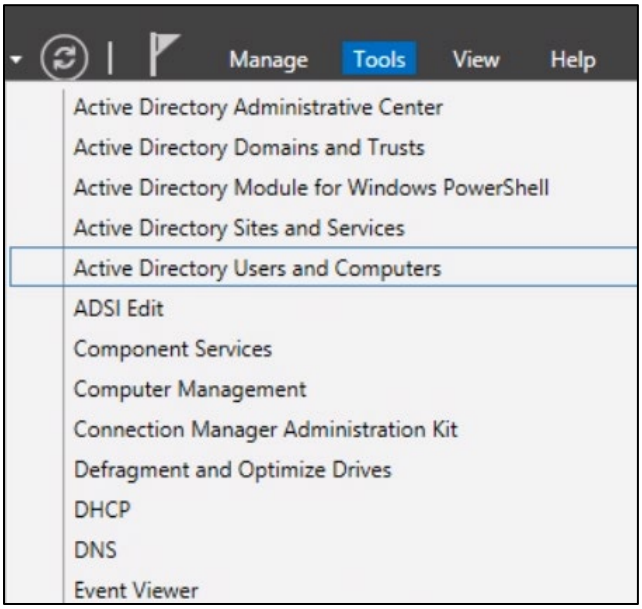

Figure 130 Active Directory Users and Computers

2) Right-click Guest account and choose Disable Account.

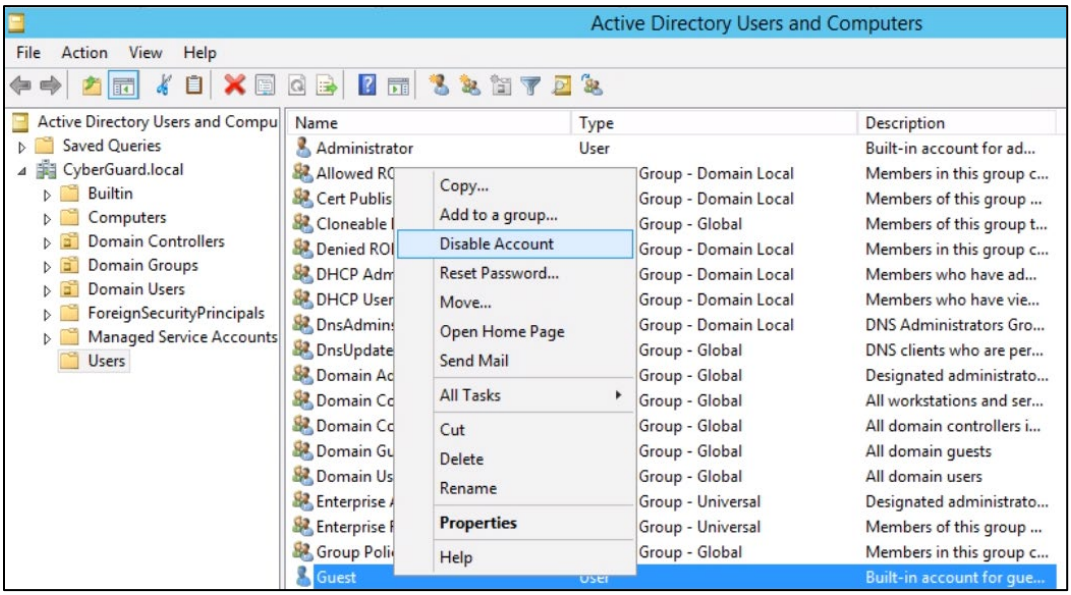

Figure 131 Disable Guest account

5.3.10- Linux Server Hardening Vulnerability Report

System Update

Keeping the system up to date is necessary after installing any operating system. This will reduce known vulnerabilities that are in our system.

Password Policy

1) Do password aging to all users by editing the configuration file. Use the command sudo nano /etc/login.defs to open the file. Lastly, save it.

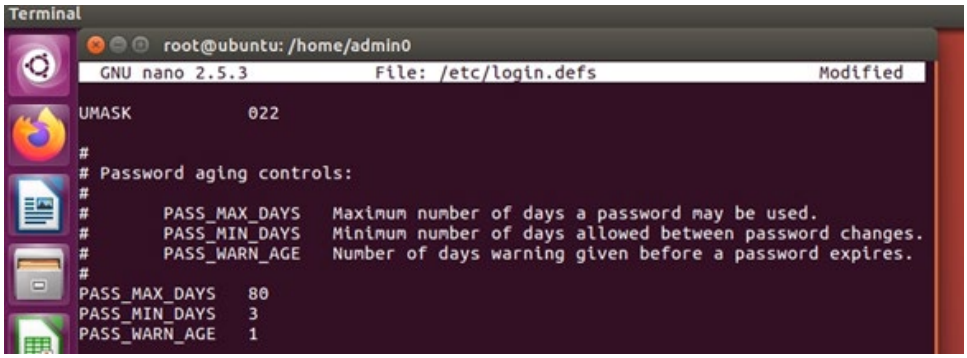

Figure 132 Password aging update login.defs file

Note: this will need every user to change their password once every 80 days and send the warning message 1 day before password expiration, and the system allows the user to change the password 3 days from the previous time.

2) Change user password expiry information (specific user). Open the terminal and type the following command.

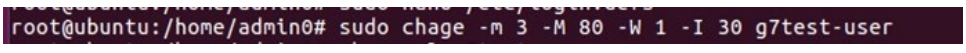

Figure 133 Change specify user password expiration

g7test-user password will expire on a specific date:

-m = minimum of 3 days between password change

-M = maximum of 80 days between password change

-W = set expiration warning days to 1 day

-I = set password inactive after expiration 30 days

Set Permission On Sensitive System File

1) Do system files only root by typing this command.

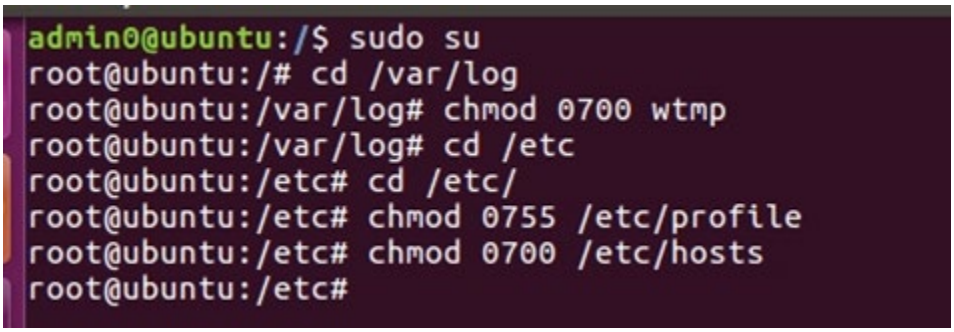

Figure 134 Change system files permission

Note:

- **/var/log/wtmp** show login and logout information.
- **/etc/profile** contains Linux wide environment and start-up programs. Normally, it is used to set path variables, user limits, and other user settings. It runs for login shell.
- **/etc/hosts** file is a plain text file that all operating systems use to translate hostname into IP address.

2) Users files. Type the following command in terminal.

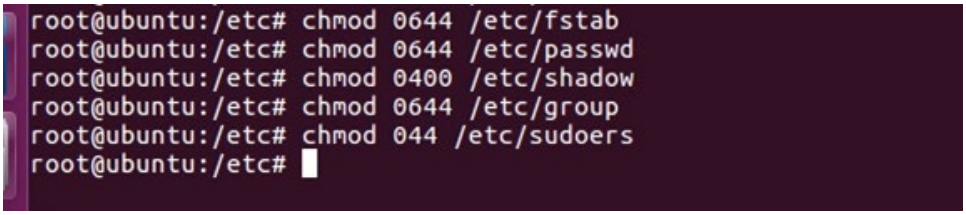

Figure 135 Change permission on user accessible file

- **/etc/fstab** is list of file systems to be mounted at BOOT time.
- **/etc/passwd** store essential information that required during login to the system. This file is owned by root user and must be readable by all users but it only the root user has access to write the file.
- **/etc/shadow** file stores actual password in encrypted format for additional properties related to user password.
- **/etc/group** is text file which defines the groups to which users belong under Linux.
- **/etc/sudoers** file is a file Linux administrators use to allocate system rights to system user. This allows the administrator to control who does what.

Check On Network Port

Note: Use multiple tools to discover network port.

1) Use Netstat. Install net-tools package to use netstat command.

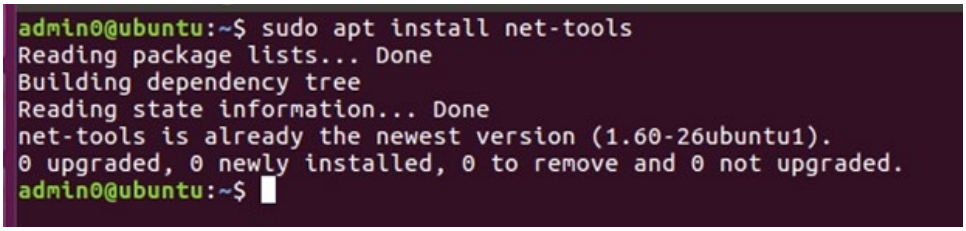

Figure 136 Install net-tools

2) Use Netstat to view all open ports and associated programs.

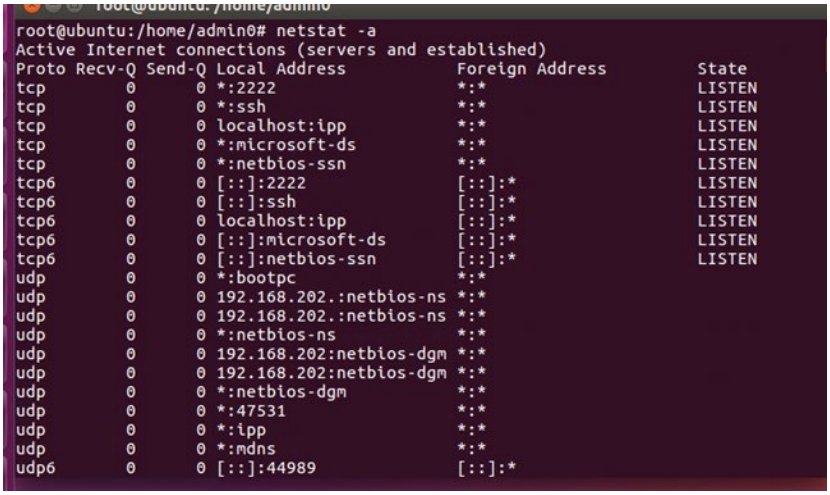

Figure 137 Use Netstat to discover listening port

Note: Netstat which known as network statistics is a command line tool for monitoring network connections in incoming and outgoing traffic. Netstat is one of the most basic network services debugging tools, tell what ports are open and whether any programs are listening on ports.

3) We are using Nmap. Install Nmap application.

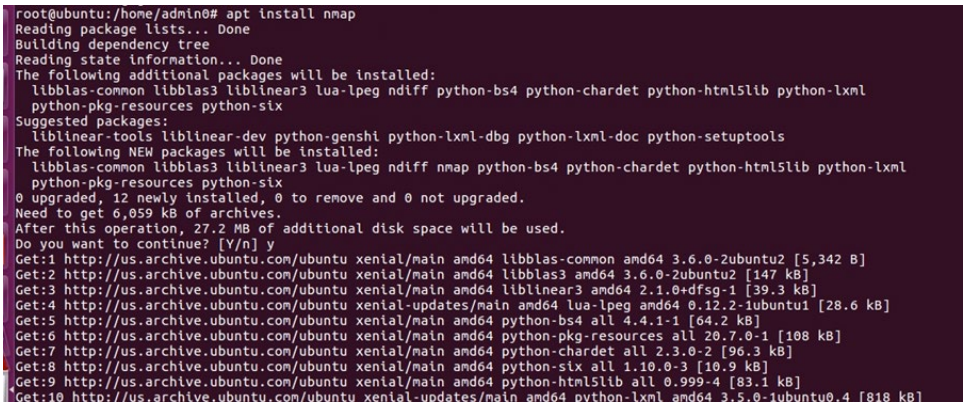

Figure 138 Installing Nmap

4) Discover all open ports. Use IP address Ubuntu server which 10.30.0.11.

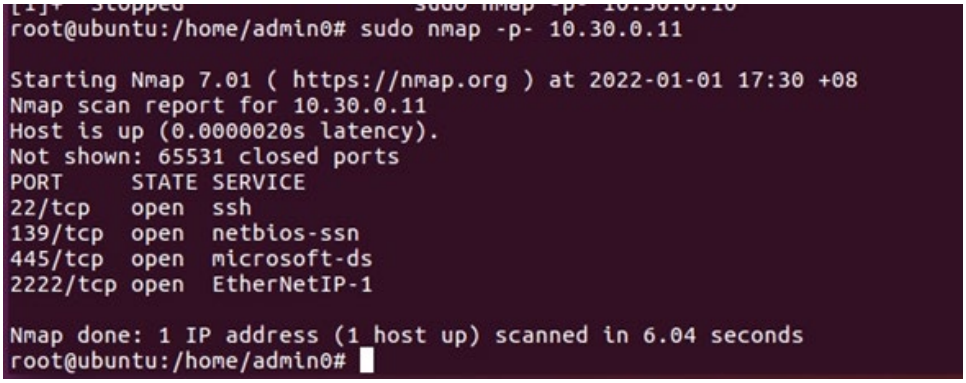

Figure 139 Discover opened port on Nmap

Note:

Port 22: Used for SSH service.

Port 139: Used for SMB dialects that communicate over NetBIOS.

Port 445: Used by newer version of SMB on top of TCP stack, allowing SMB to communicated over the Internet.

Note: Nmap which known as Network Mapper is a tool for network exploration and security auditing. It can scan large networks even though it works fine against single hists. Nmap is commonly used for security audits because most of network administrators find it useful for routine tasks such as manage service upgrade schedule, and monitoring host and service uptime.

5) Disable CUPS service.

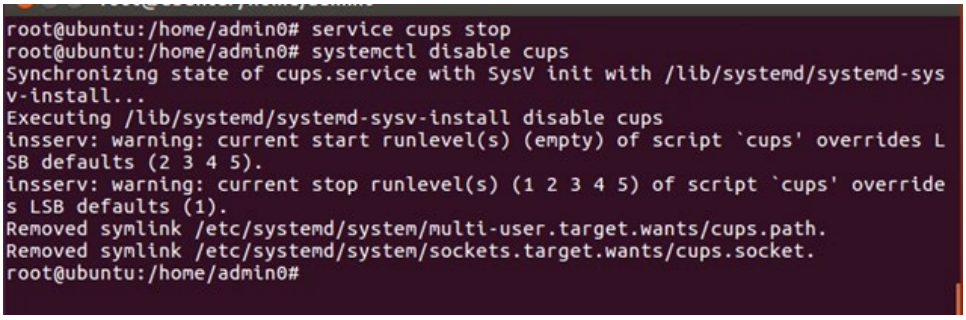

Figure 140 Stop CUPS service

Note: CUPS is a common Linux printing system. This application allows computer to act as print server.

Backup

1) Go to settings > search Backup and choose Backup.

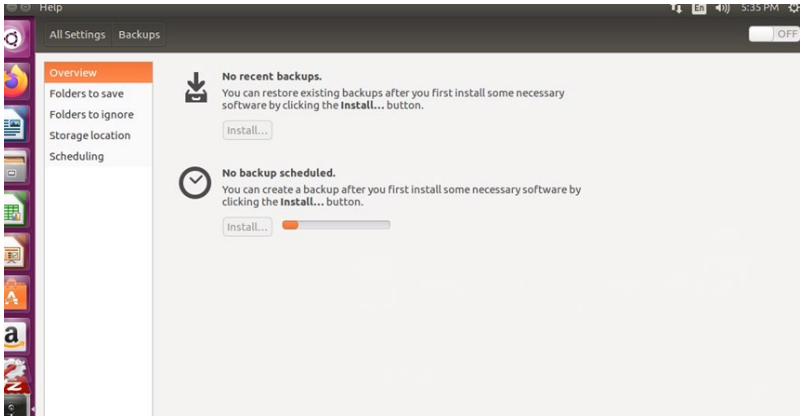

Figure 141 Backup interface

Note: Backup is one of the most important things in the system. If system is down, backup will save the important data in the system so that it can restore all the data without losing anything.

5.3.11- Active Directory

Installing Active Directory

1) Press the “Add Roles and Features” option on the Server Manager to open the installation wizard, click next

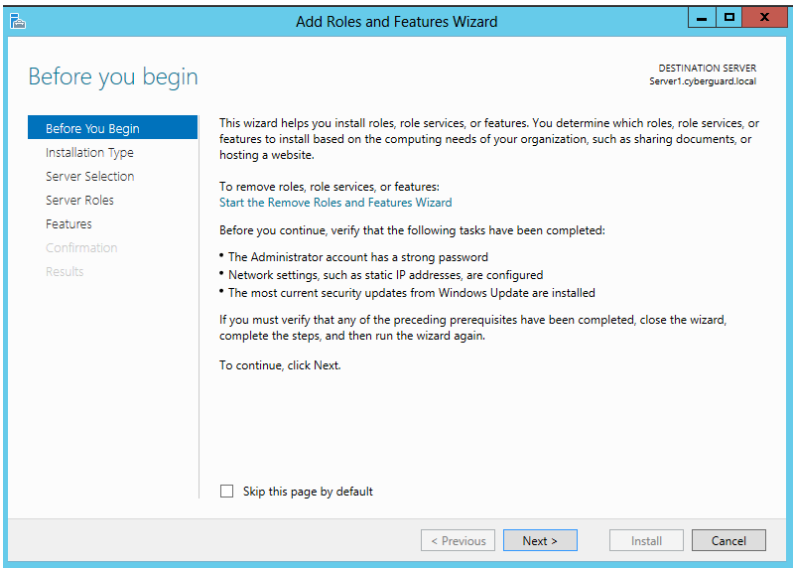

Figure 142 Add Roles and Features Wizard

2) Choose the ‘Role-based installation’ and click next

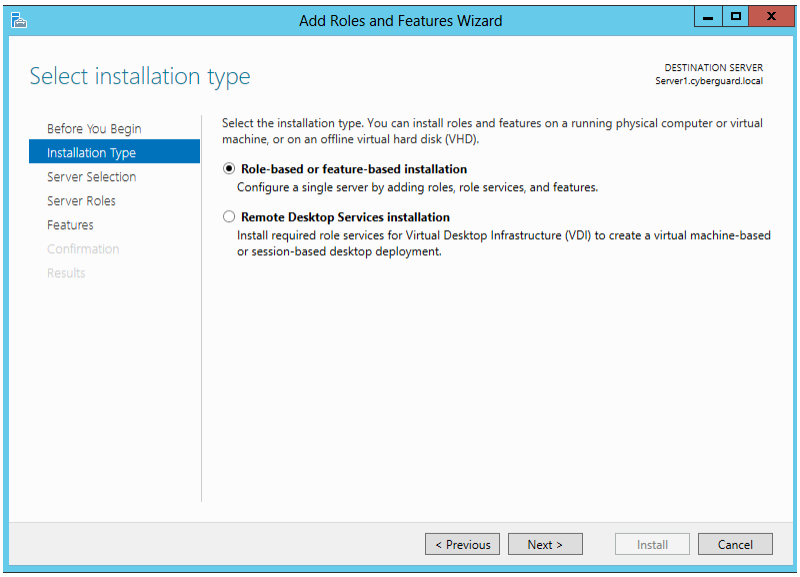

Figure 143 Installation Type

3) Make sure to select the current server from the server pool and click next

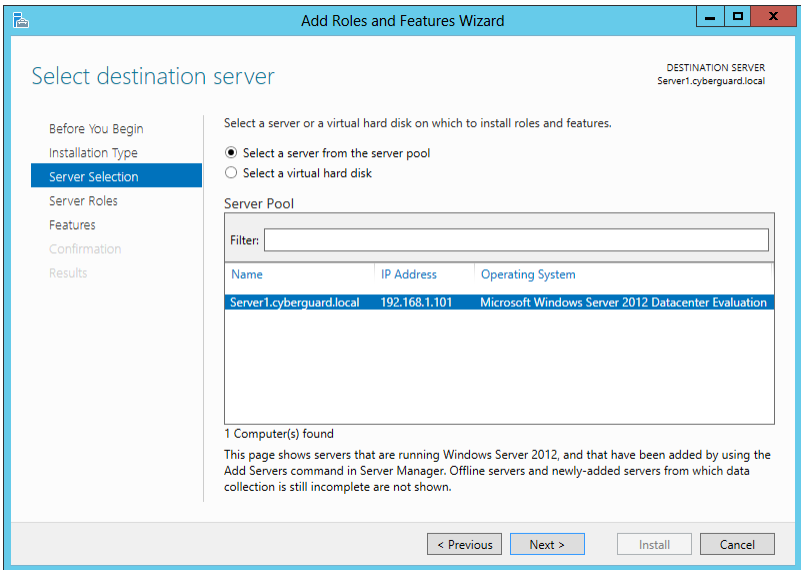

Figure 144 Selecting Server from Server Pool

4) Tick the 'Active Directory Domain Services' option and click next until the confirmation page appears

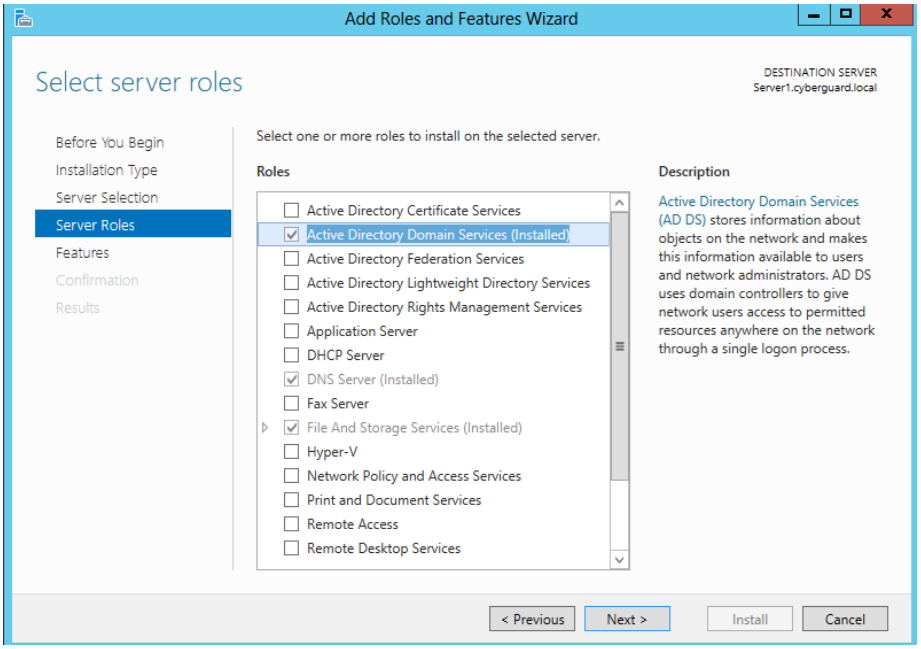

Figure 145 Server Roles

5) Make sure everything is in order and click install

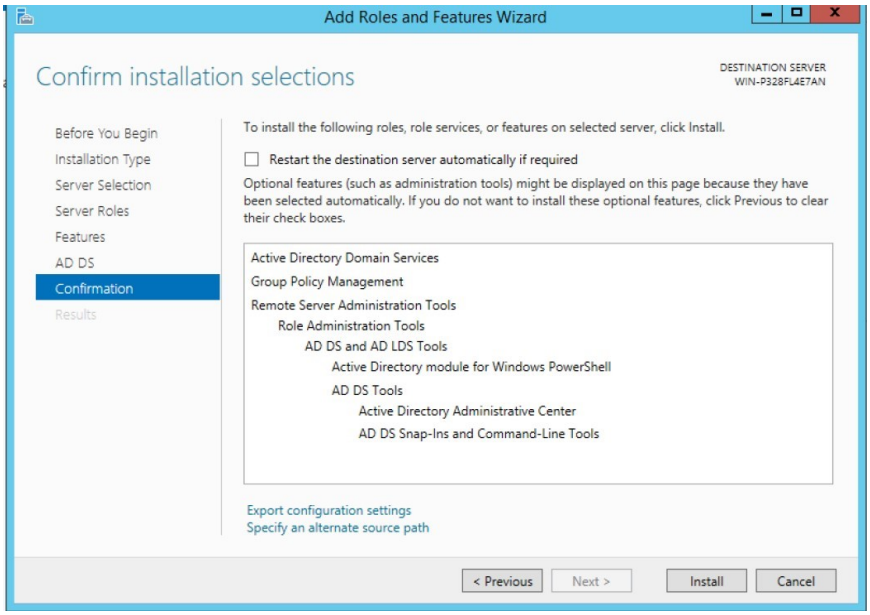

Figure 146 Confirm Installation

6) Before closing the wizard, click 'Promote this server to a domain controller' for the next steps

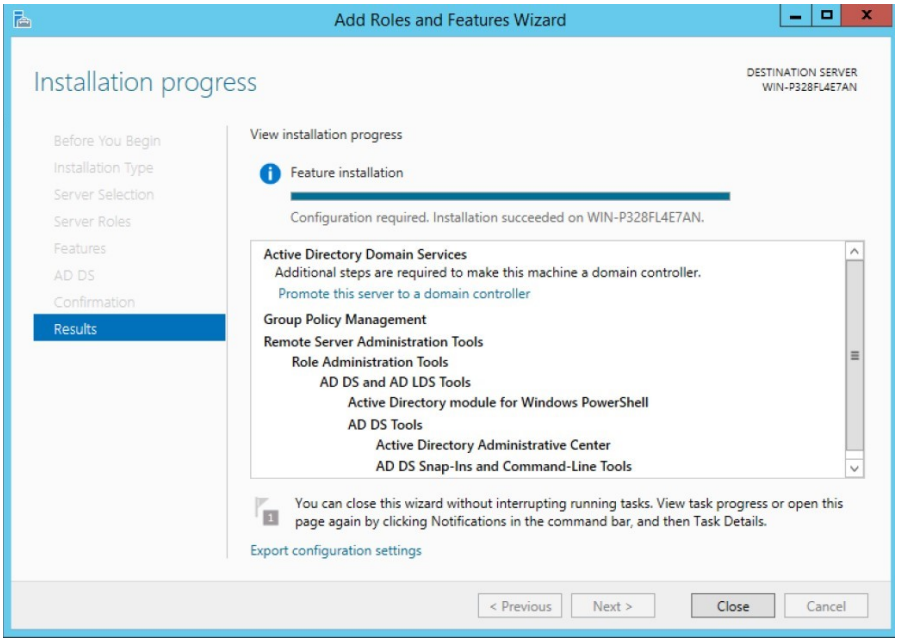

Figure 147 Closing Wizard

Promote Windows Server into Domain Controller

1) On the new configuration wizard, click 'Add a new forest' option and enter the desired root domain name

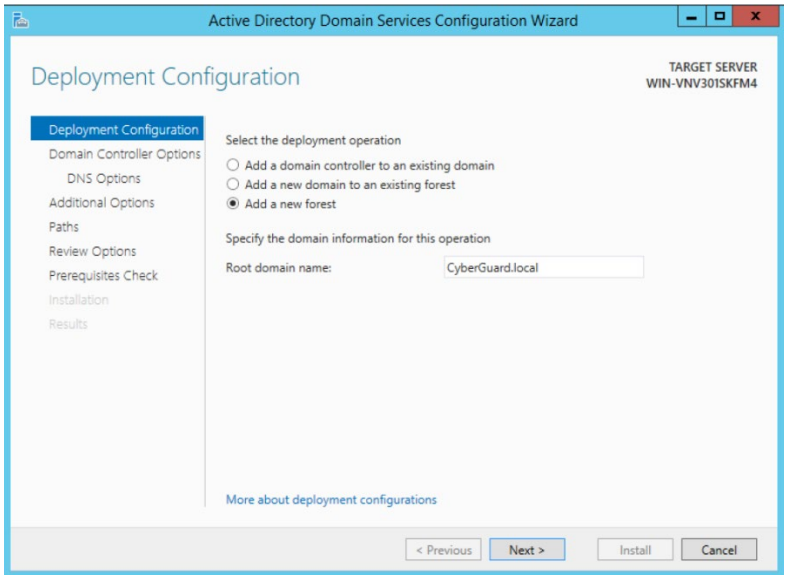

Figure 148 Adding CyberGuard.local domain name

2) Leave the options as the default and enter a password and password confirmation in the Directory Services Restore Mode (DSRM) password area

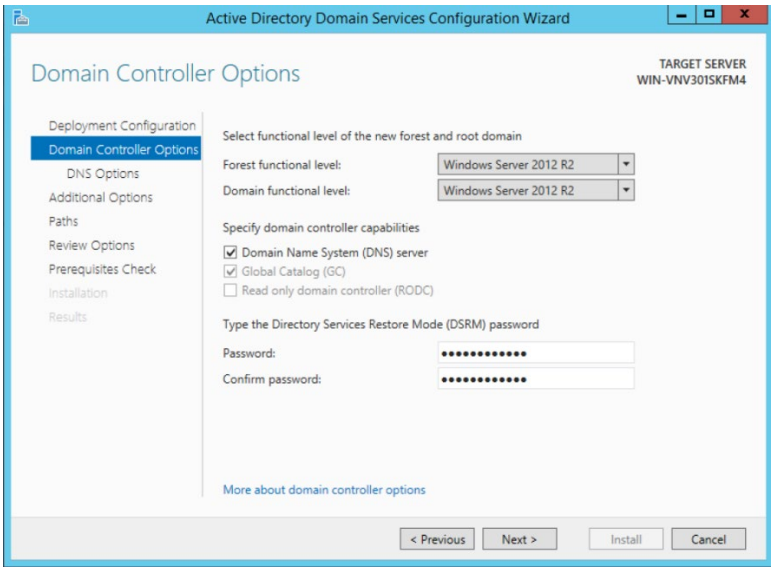

Figure 149 Entering DSRM password

3) You can change the domain name or change it, then click next

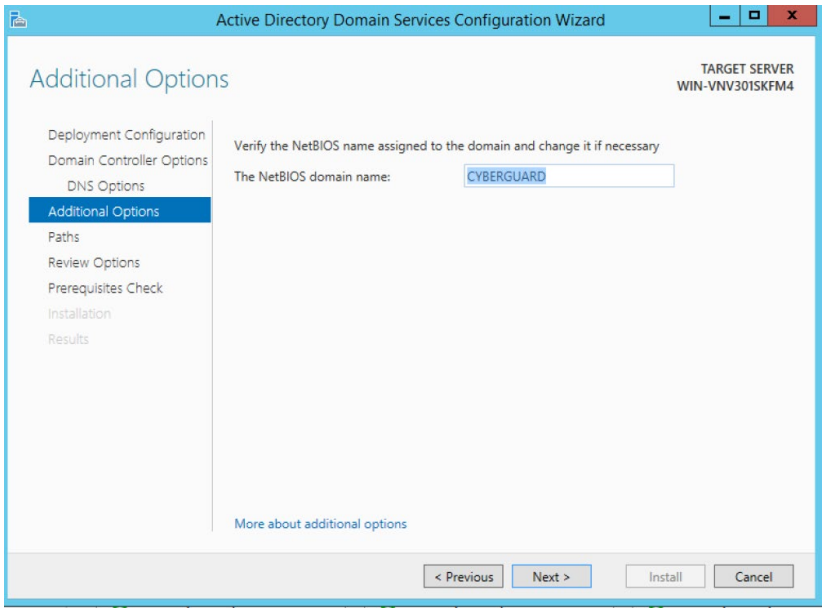

Figure 150 Enter NetBIOS domain name

4) You can specify the paths or leave it as defaults, then click next

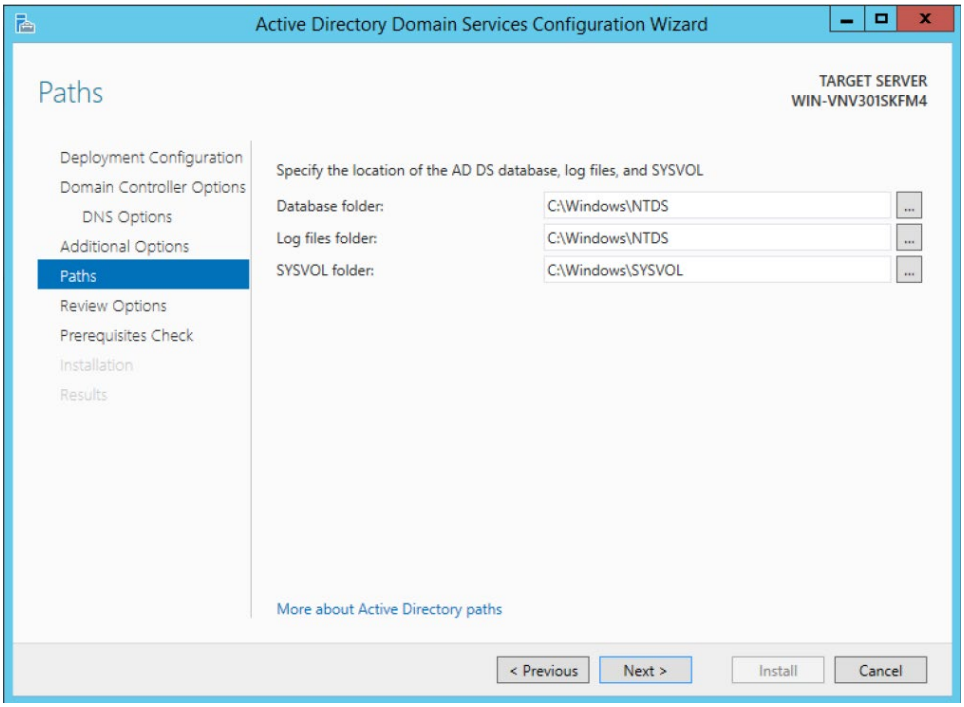

Figure 151 AD DS paths

5) Review your configurations and click next

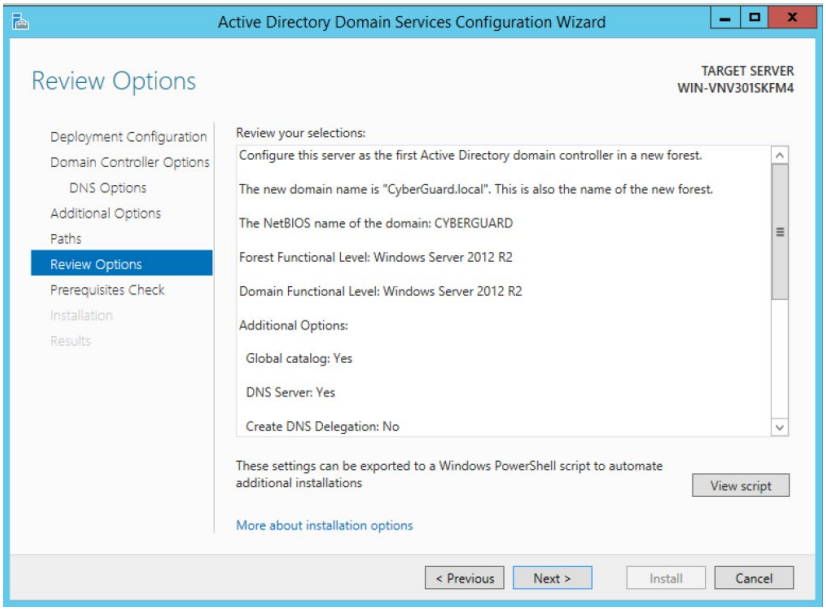

Figure 152 Review Configuration

6) On the prerequisites page, press install. Windows Server will restart automatically after the installation

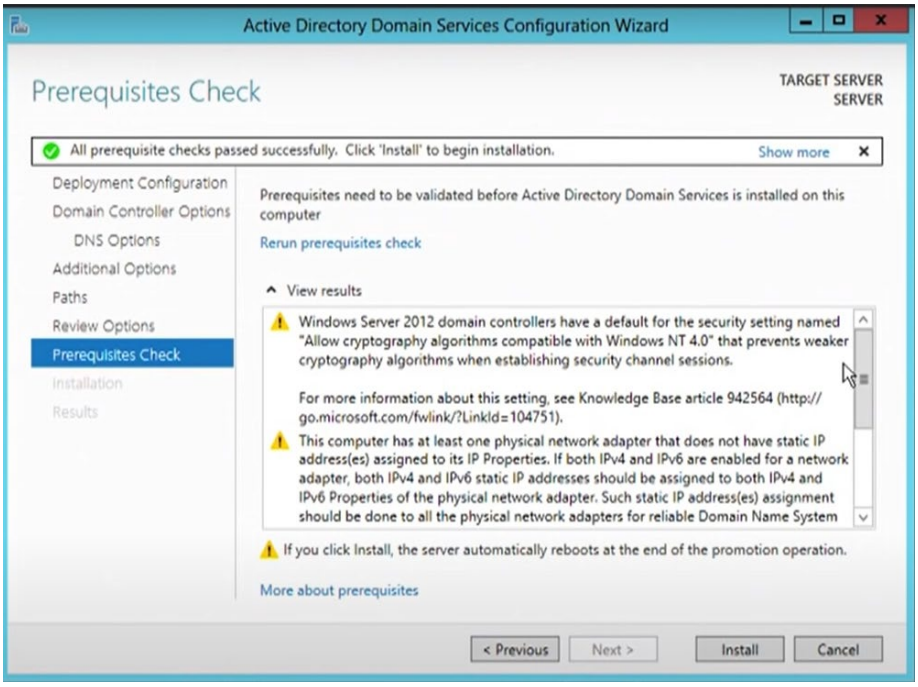

Figure 153 Prerequisites

Creating Users and Groups in Active Directory

In order to join the domain as a client or administer the domain, we need to have users created and stored in AD

1) In the Server Manager tools section, choose the 'Active Directory Users and Computers'

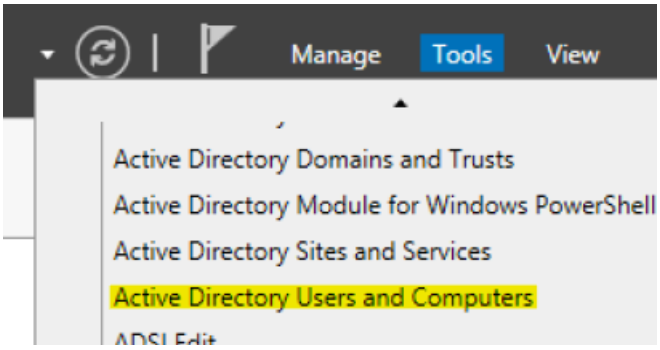

Figure 154 Active Directory Users and Computers

2) Choose to create a new Organizational Unit in the domain directory and enter name to store the users

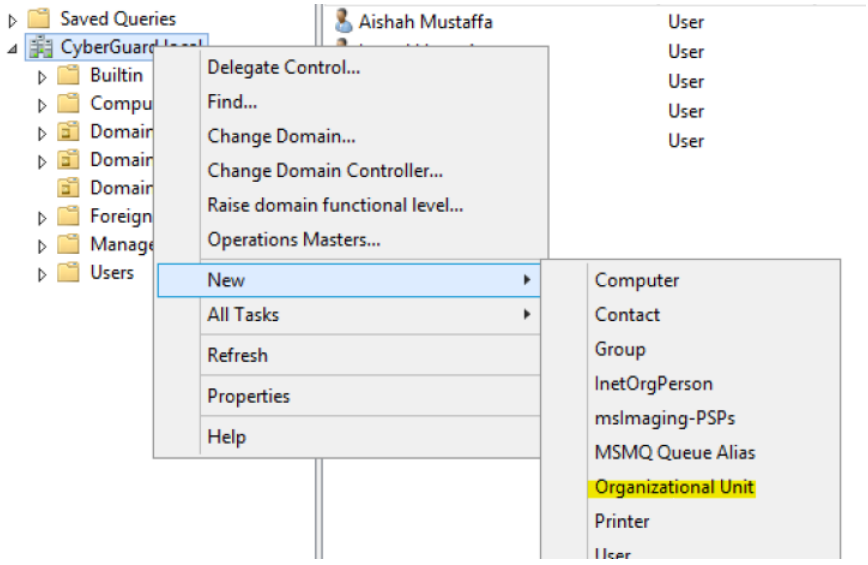

Figure 155 Create new Organizational Unit

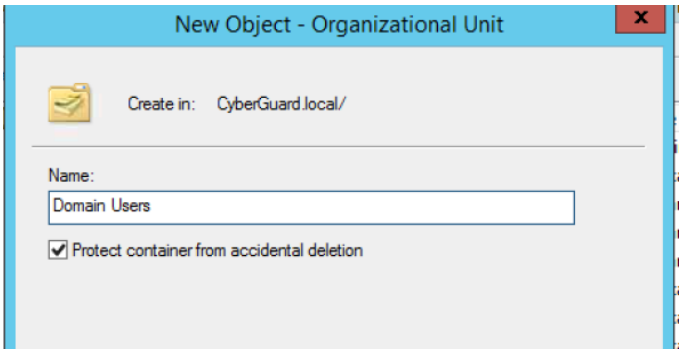

Figure 156 Name the new Organizational Unit

3) Click on the small user icon at the top to create a new User, and these users are used for logging in to the domain. Then, enter the appropriate credentials.

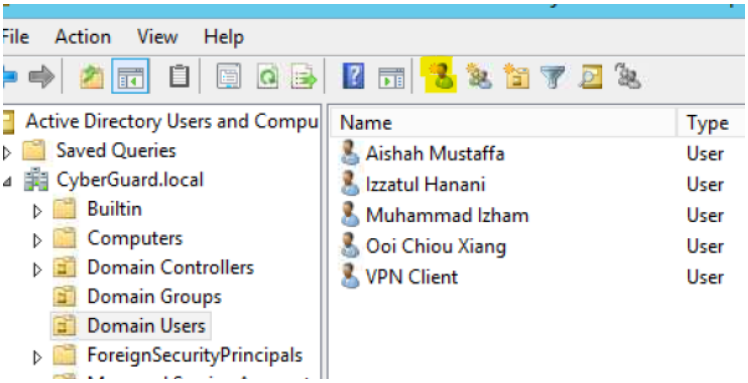

Figure 157 Domain Users folder

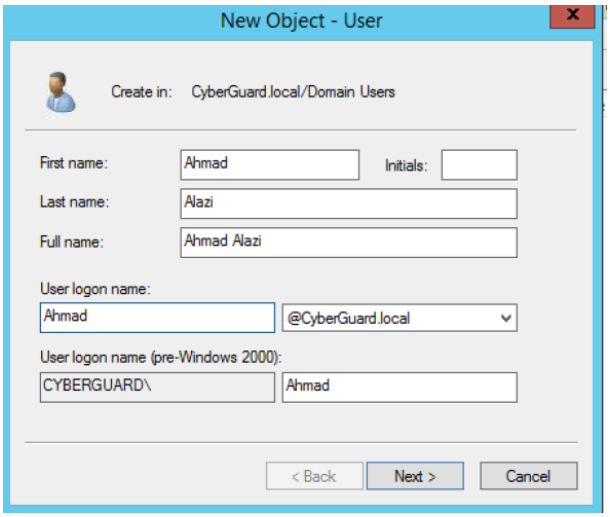

Figure 158 Creating New User

4) Next, we have to set the password. For best practices, make sure 'User must change password at next logon' ticked so that the user must change the default password, then click next.

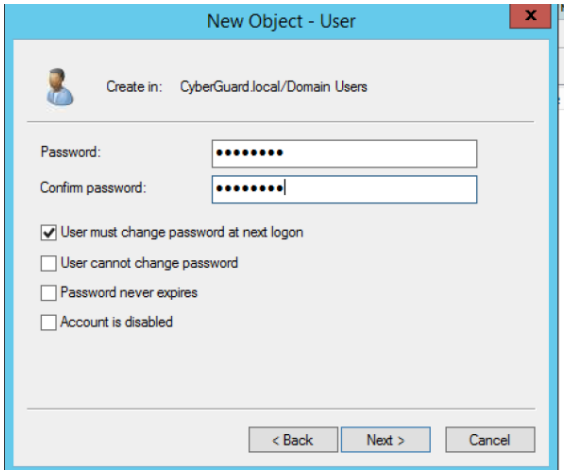

Figure 159 Entering Password for New User

5) Now that we created the user, we can include the user with pre-created domain groups to give the user permissions.

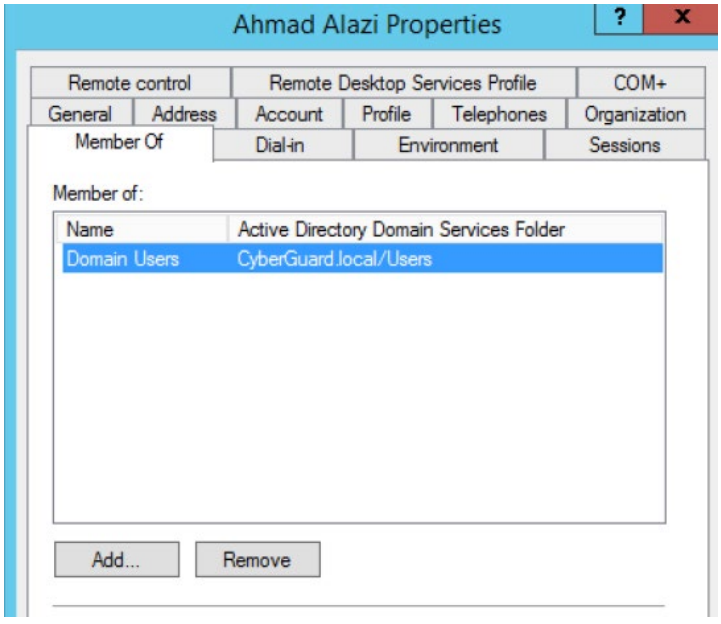

Figure 160 Member Of window

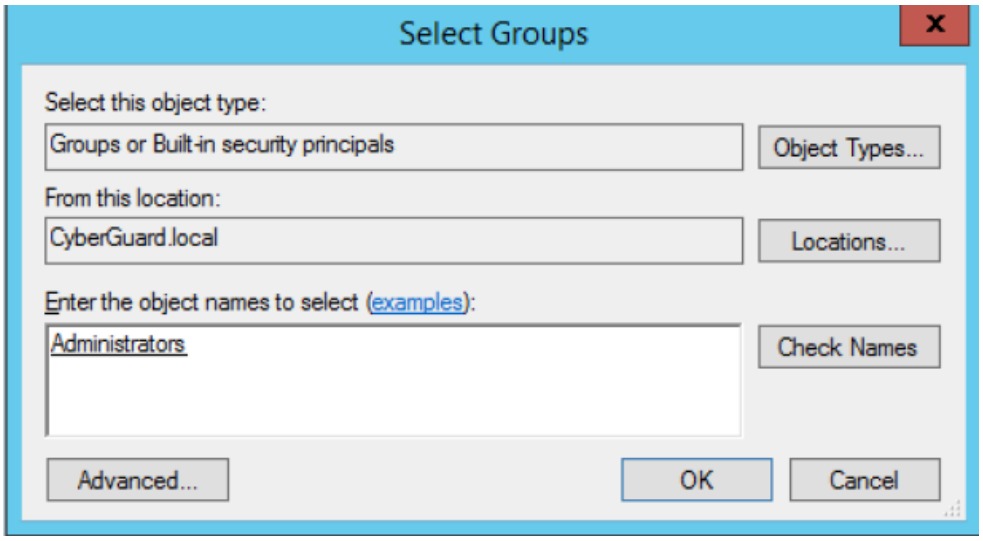

Figure 161 Joining User to a Group

6) Optionally, we can create our own domain groups and set the user as a member of said groups. Leave the Group scope and Group type as the default settings.

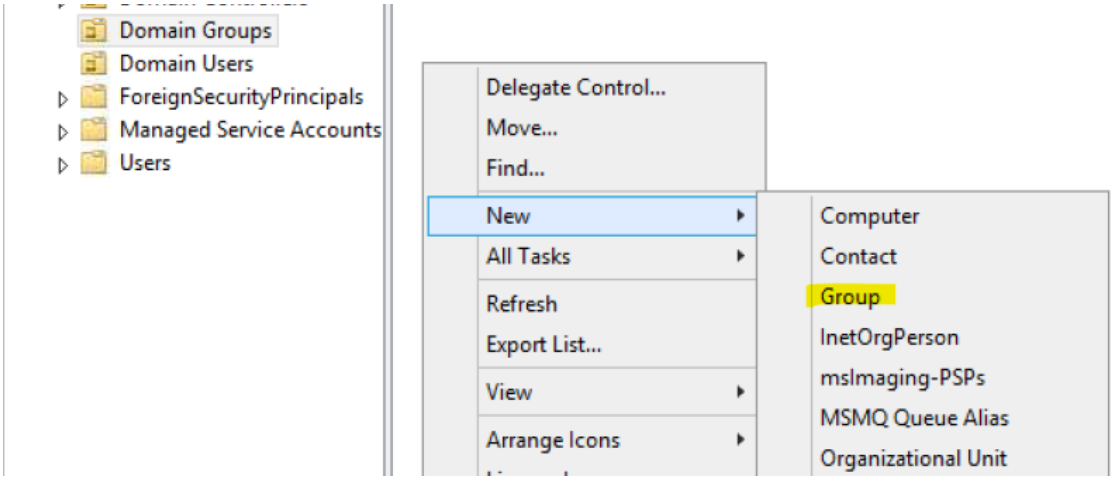

Figure 162 Creating new Group

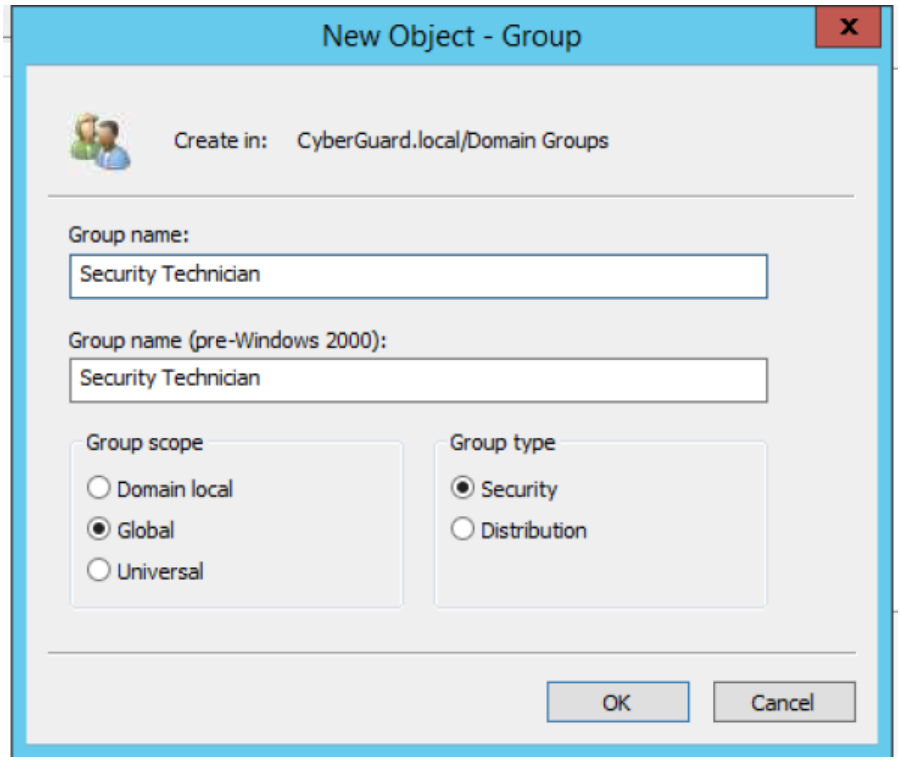

Figure 163 New Group Object Window

7) Now we can assign the user with the created group.

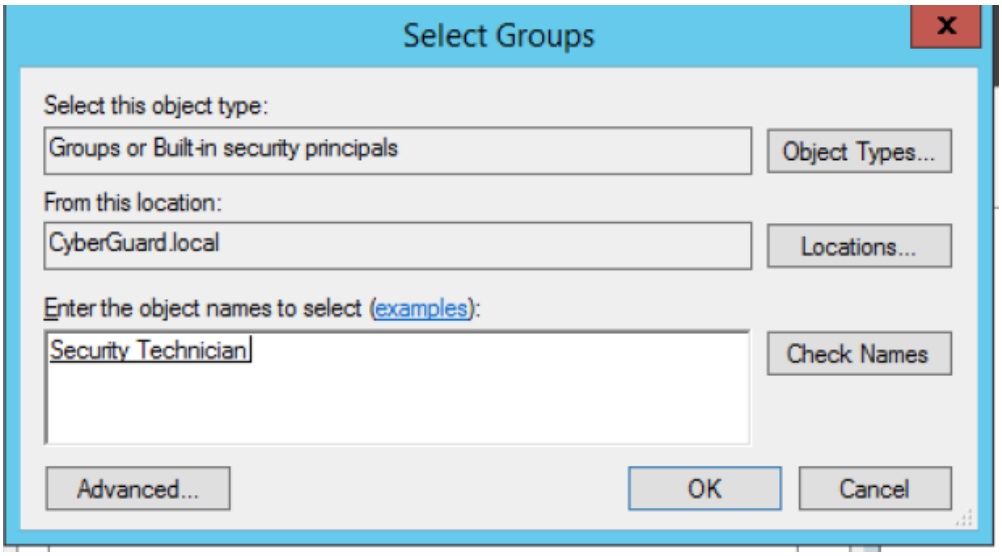

Figure 164 Joining User with New Group

5.3.12- IDS with Port Mirroring and Qradar

Install Snort

1) Install the required libraries

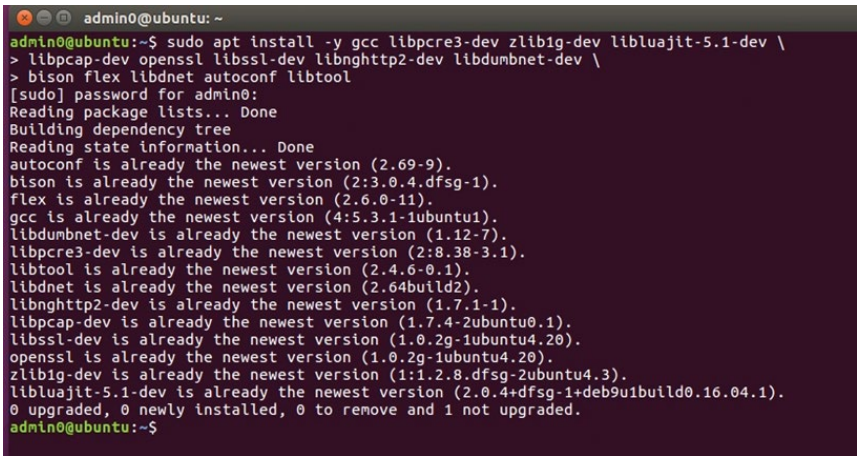

Figure 165 Required libraries has been installed

2) Create temporary folder for download in the home directory and change into it

Figure 166 Create folder and change into it ~/snort_src

3) Download the Data Acquisition Library (DAQ) source package from Snort website and replace the version number in the command.

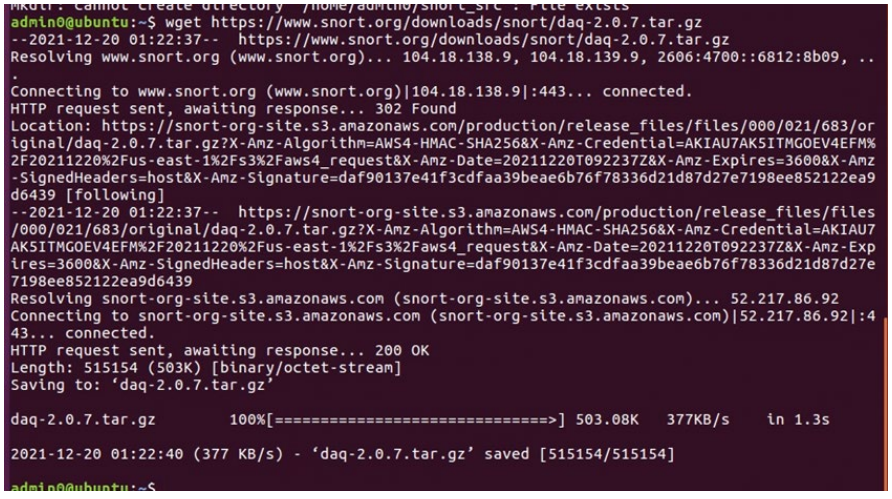

Figure 167 Successful download DAQ source package

4) Extract the source code

```
admin0@ubuntu:~$ tar -xvzf daq-2.0.7.tar.gz
daq-2.0.7/
daq-2.0.7/config.h.in
daq-2.0.7/config.guess
daq-2.0.7/api/
daq-2.0.7/api/daq.h
daq-2.0.7/api/Makefile.am
daq-2.0.7/api/daq_common.h
daq-2.0.7/api/daq_base.c
daq-2.0.7/api/daq_api.h
daq-2.0.7/api/daq_mod_ops.c
daq-2.0.7/api/Makefile.in
daq-2.0.7/config.sub
daq-2.0.7/ltmain.sh
daq-2.0.7/os-daq-modules/
daq-2.0.7/os-daq-modules/daq-modules-config.in
daq-2.0.7/os-daq-modules/daq_ipfw.c
daq-2.0.7/os-daq-modules/Makefile.am
daq-2.0.7/os-daq-modules/daq_static_modules.h
daq-2.0.7/os-daq-modules/daq_dump.c
daq-2.0.7/os-daq-modules/daq_ipq.c
daq-2.0.7/os-daq-modules/daq_static_modules.c
daq-2.0.7/os-daq-modules/daq_pcap.c
daq-2.0.7/os-daq-modules/daq_nfq.c
daq-2.0.7/os-daq-modules/daq_netmap.c
daq-2.0.7/os-daq-modules/daq_afpacket.c
daq-2.0.7/os-daq-modules/Makefile.in
daq-2.0.7/compile
daq-2.0.7/install-sh
```

Figure 168 the source code has been extracted

5) Change into the new directory

```
admin0@ubuntu:~$ cd daq-2.0.7
```

Figure 169 Change directory to DAQ folder

6) Auto reconfigures DAQ before running the configuration.

```
admin0@ubuntu:~/daq-2.0.7$ autoreconf -f -i
libtoolize: putting auxiliary files in '.'.
libtoolize: copying file './ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltsugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/lt~obsolete.m4'
configure.ac:12: installing './compile'
configure.ac:9: installing './missing'
api/Makefile.am: installing './depcomp'
```

Figure 170 Auto configuration command

7) Run configuration script using the default values and compile program with make and install DAQ.

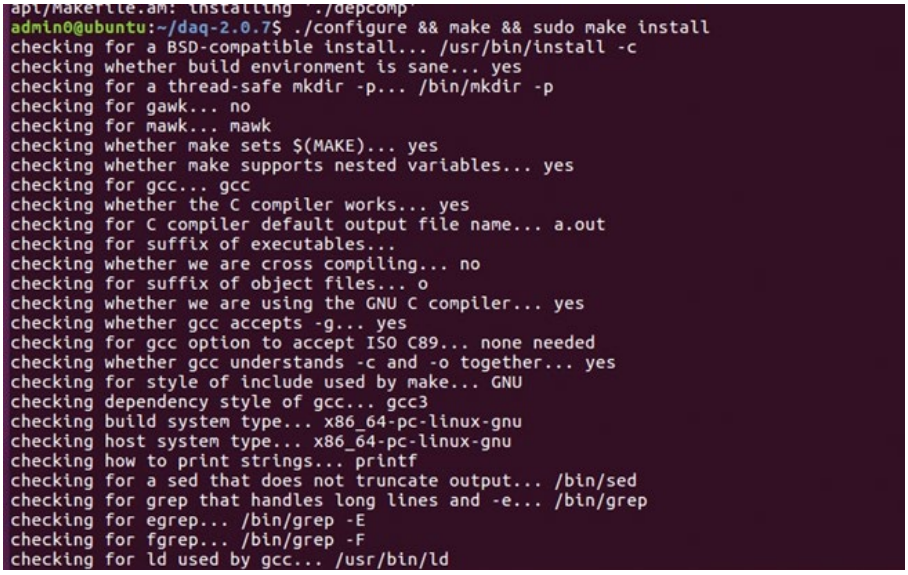

Figure 171 The program has been executed and installed

8) With DAQ installed, Snort can get started, change back to download folder.

Figure 172 Change back directory to ~/snort_src

9) Download Snort source code.

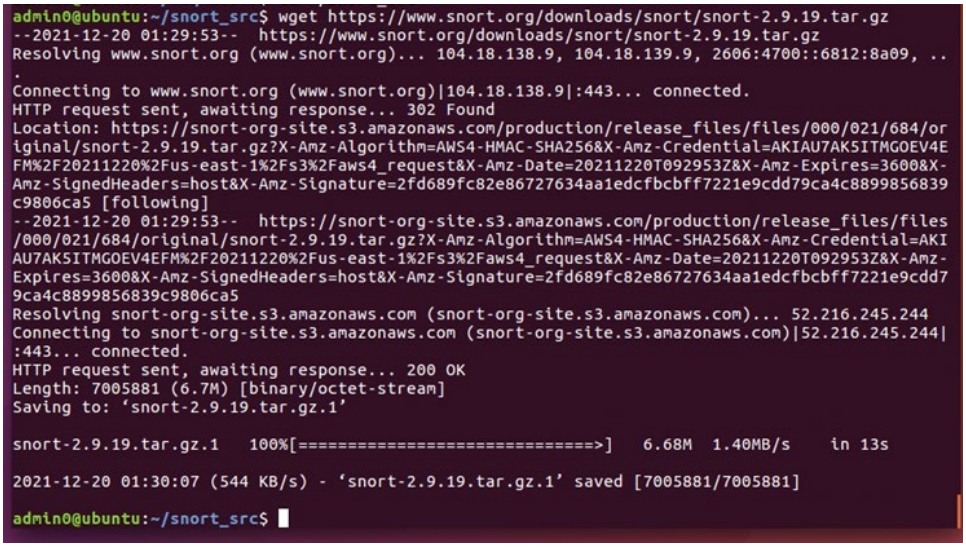

Figure 173 Snort version 2.9.19 has been installed

10) Extract the source code.

```
admin0@ubuntu:~/snort_src$ tar -xvzf snort-2.9.19.tar.gz
snort-2.9.19/
snort-2.9.19/snort.8
snort-2.9.19/install-sh
snort-2.9.19/snort.pc.in
snort-2.9.19/aclocal.m4
snort-2.9.19/config.guess
snort-2.9.19/compile
snort-2.9.19/config.h.in
snort-2.9.19/missing
snort-2.9.19/LICENSE
snort-2.9.19/config.sub
snort-2.9.19/COPYING
snort-2.9.19/templates/
snort-2.9.19/templates/sp_template.c
snort-2.9.19/templates/sp_template.h
snort-2.9.19/templates/spp_template.c
snort-2.9.19/templates/Makefile.in
snort-2.9.19/templates/Makefile.am
snort-2.9.19/templates/spp_template.h
snort-2.9.19/verstuff.pl
snort-2.9.19/Makefile.in
snort-2.9.19/etc/
snort-2.9.19/etc/file_magic.conf
snort-2.9.19/etc/unicode.map
snort-2.9.19/etc/gen-msg.map
snort-2.9.19/etc/attribute_table.dtd
snort-2.9.19/etc/Makefile.in
```

Figure 174 The source code has been extracted

11) Change into new directory.

```
admin0@ubuntu:~/snort_src$ cd snort-2.9.19
```

Figure 175 Change directory snort-2.9.19

Configuring Snort To Run In Nids Mode

12) Update the shared libraries.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo ldconfig
```

Figure 176 Update using this command

13) Snort on Ubuntu get installed to /usr/local/bin/snort directory, create symbolic link to /usr/sbin/snort.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figure 177 Create other symbolic links

14) Create new privileged user and new user group for daemon to run under. It is good and safe to run Snort on Ubuntu without root access.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo groupadd snort
groupadd: group 'snort' already exists
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g
snort
useradd: user 'snort' already exists
```

Figure 178 Snort group and user has been created

15) Create the folder structure for Snort configuration.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo mkdir -p /etc/snort/rules
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo mkdir /var/log/snort
mkdir: cannot create directory ‘/var/log/snort’: File exists
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo mkdir /usr/local/lib/snort_dynamicrules
mkdir: cannot create directory ‘/usr/local/lib/snort_dynamicrules’: File exists
```

Figure 179 The folders have been created

16) Change the permission of the new directories respectively.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /etc/snort
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /var/log/snort
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /etc/snort
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /var/log/snort
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicr
ules
```

Figure 180 Permission has been setup using these commands

17) Create new files for whitelist, blacklist, and local rules.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/white_list.rules
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/black_list.rules
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo touch /etc/snort/rules/local.rules
admin0@ubuntu:~/snort_src/snort-2.9.19$
```

Figure 181 Create new files using touch command

18) Copy the configuration files from download folder.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.conf* /etc/snort

admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo cp ~/snort_src/snort-2.9.19/etc/*.map /etc/snort
admin0@ubuntu:~/snort_src/snort-2.9.19$
```

Figure 182 Configuration files have been copied from download folder

Community Rules

19) Download the community rules.

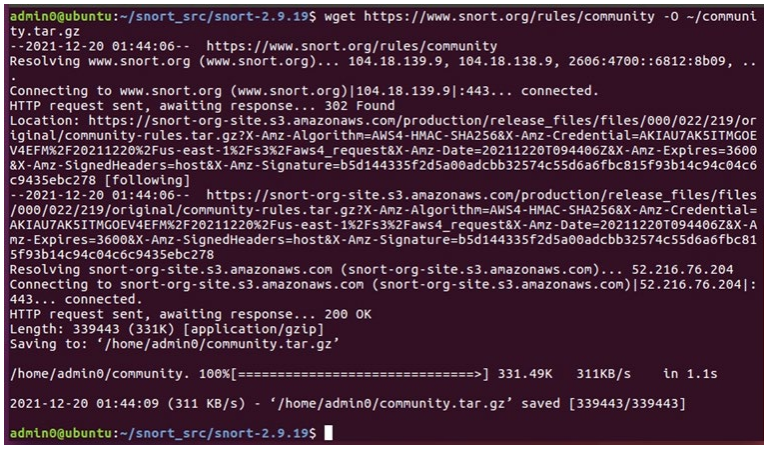

Figure 183 Community rules

20) Extract the rules.

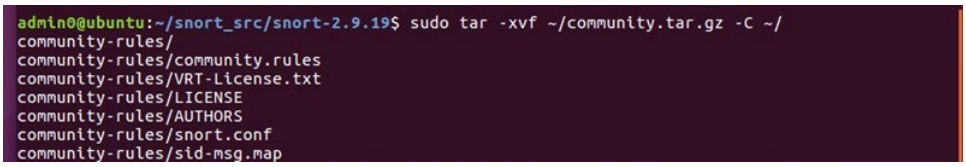

Figure 184 The rules have been extracted

21) Copy the to the configuration folder.

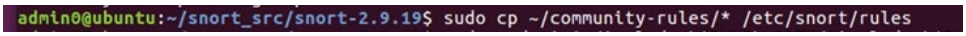

Figure 185 The rules have been copied to configuration file

22) Comment out the unnecessary line using this command.

By default, Snort on Ubuntu expects to find a number of different rule files which are not included in the community rules. So, comment out the unnecessary line easily by using sed command.

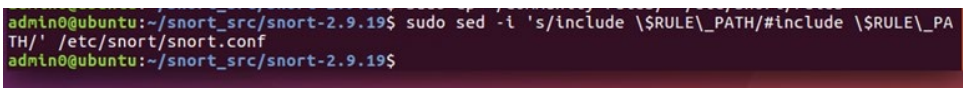

Figure 186 Comment out unnecessary line

Configuring Network And Rule Sets

23) Open configuration file in the text editor.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo nano /etc/snort/snort.conf
admin0@ubuntu:~/snort_src/snort-2.9.19$
```

Figure 187 Open configuration file using nano text editor

24) Find these keys in the configuration file and change the parameters, respectively.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.30.0.0/24
```

Figure 188 Change the network address we are protecting

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

Figure 189 Set the path to the rules files

```
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

Figure 190 Set absolute path

```
# unified2
# Recommended for most installs
output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types
```

Figure 191 Set the output for unified2 to log under filename of snort.log

```
# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules
```

Figure 192 Uncomment local.rules and add line for community rules

25) Edit Snort rules by opening text editor: **sudo nano /etc/snort/rules/local.rules**

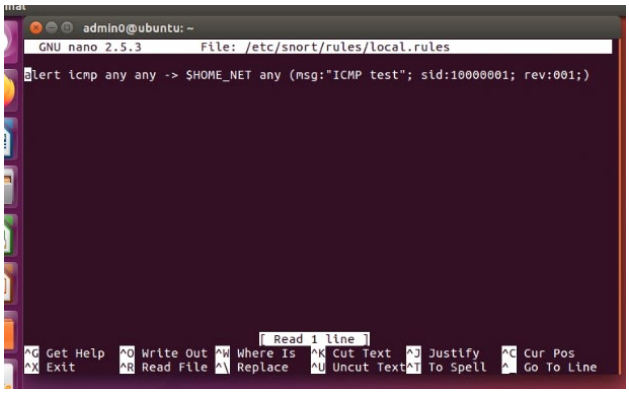

Figure 193 Add rules on the Snort rule file

26) Validate Snort Rules

Figure 194 Run Snort configuration test

After running Snort configuration test, the messages should appear.

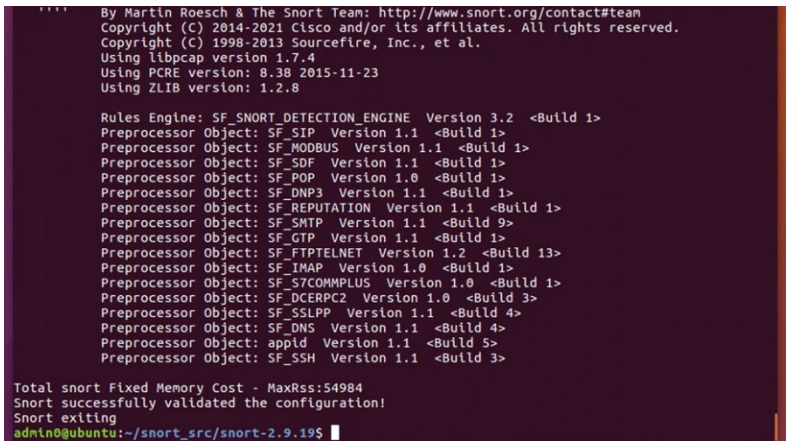

Figure 195 Messages show the version of Snort

Port Mirroring

1) Configure monitor session 1 on switch HQ-AS-01.

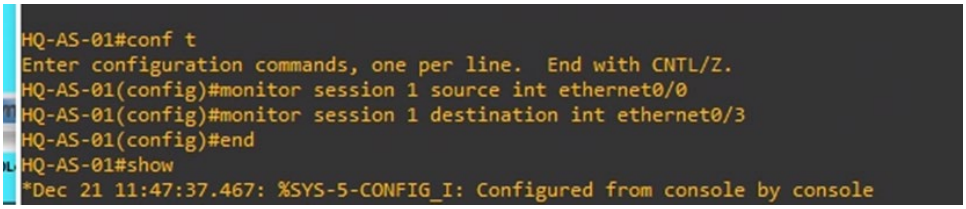

Figure 196 Create monitor session

2) Verify the monitor session that has been created.

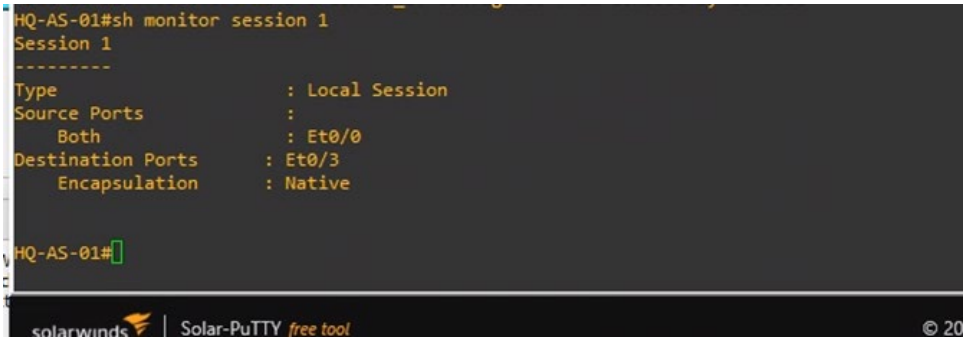

Figure 197 Verification of monitor session 1

QRadar Installation

1) Start QRadar on WM. Launch it and type the default username which is root. It requires you to fill in the new password.

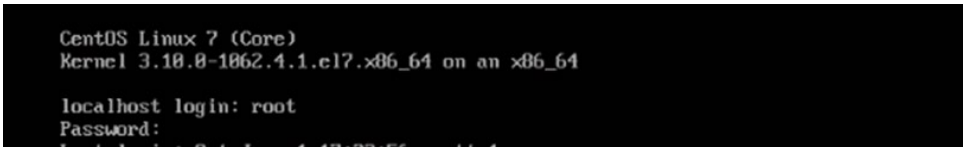

Figure 198 Type the password

2) Launch setup script and complete the setup process.
   Command: ./setup
3) Accept the CentOS 7 Linux EULA by entering Enter.
4) If it asks to continue the installation, press Y to proceed installation.

5) After the installation completed successfully, enter new admin password.

Figure 199 Enter strong password

Note: This is the password for admin user on QRadar CE web user interface.

Username: admin (fix name)

Password: g7CyberGuard (we decide)

6) Verify QRadar CE installation by typing the following command.

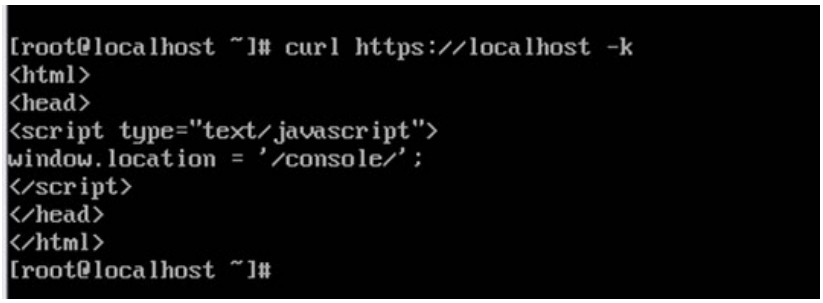

Figure 200 Verification QRadar installation

7) Use ifconfig command to quickly view the IP address. (**192.168.202.136)**

Figure 201 IP address shown in the interface of ens33

8) Open web browser in Ubuntu Server.

9) Enter the IP address 192.168.202.136

Figure 202 Enter IP address in web browser

10) Web browser will display the warning. Ignore this warning by clicking on **Advanced > Proceed to 192.168.202.136 (unsafe).**

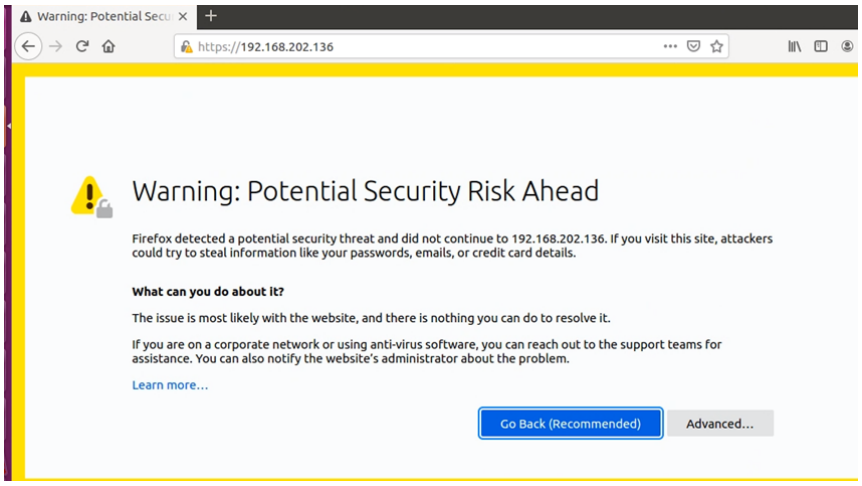

Figure 203 Warning message on web browser

11) **Step 11:** Log in with username **admin** and password that has been setup on the console during installation step.

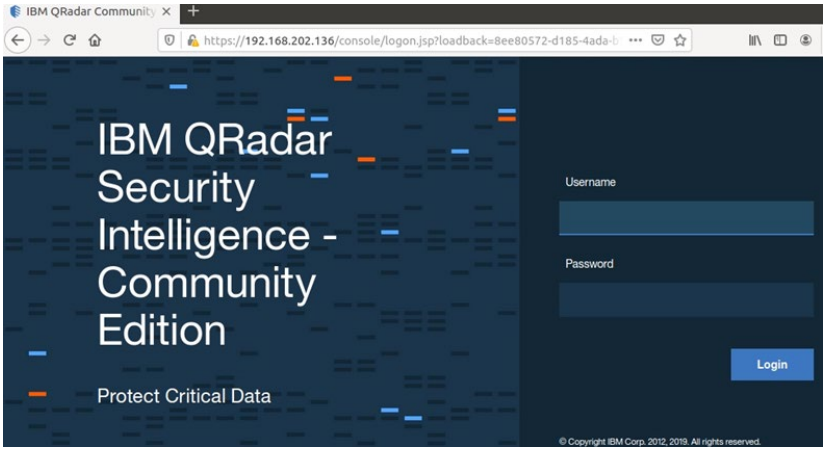

Figure 204 Login QRadar

12) Click Accept on QRadar Community Edition – License Agreement to continue.

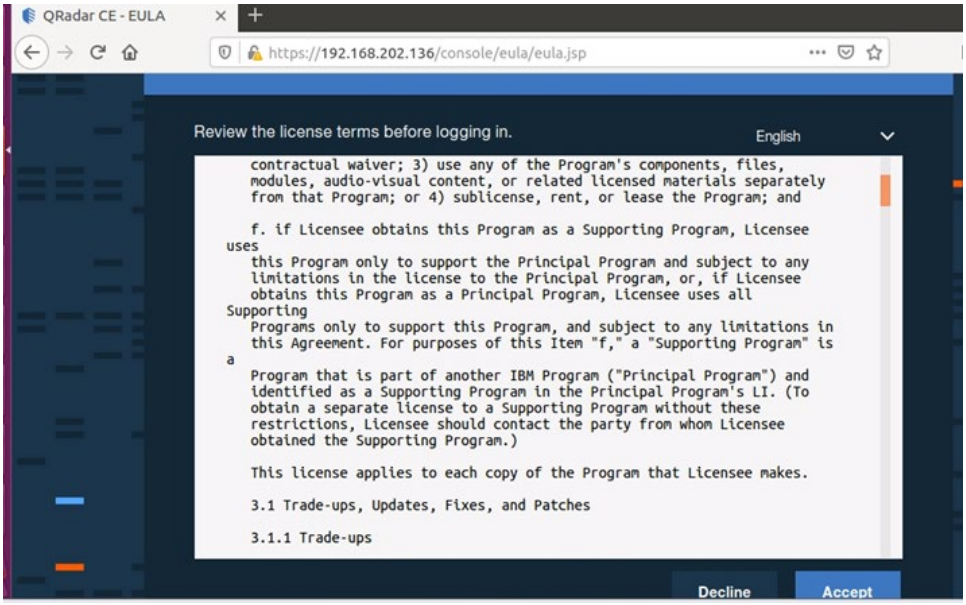

Figure 205 Accept the License Agreement

13) Dashboard view of QRadar CE.

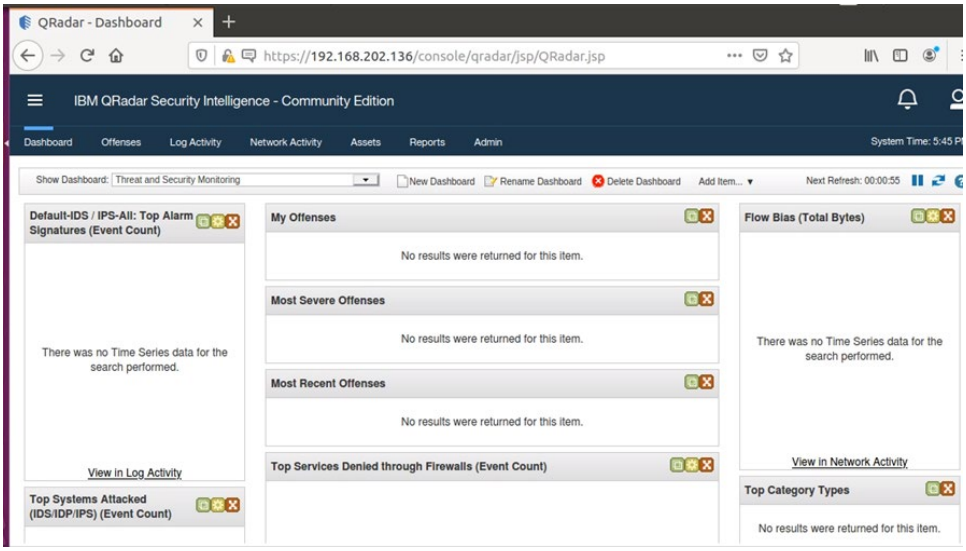

Figure 206 Dashboard QRadar

5.3.13- Samba Security

1) Check and update Ubuntu packages by using a command, **sudo apt-get update**.

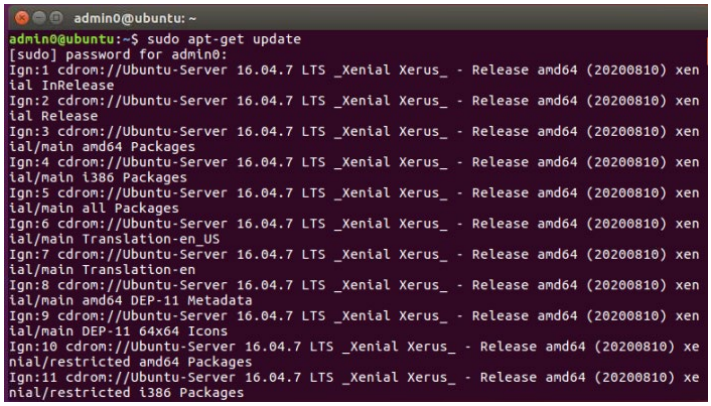

Figure 207 Install update

2) Install samba service by using command **sudo apt-get install samba**.

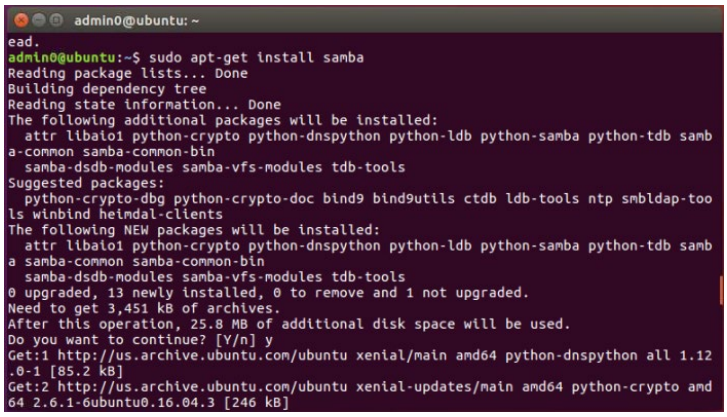

Figure 208 Install samba

3) Check the samba status using the command **sudo systemctl status smbd**.

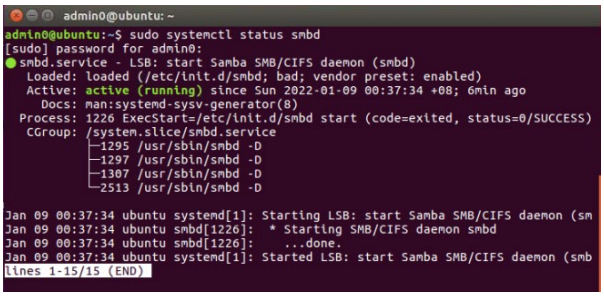

Figure 209 Check samba status

4) Firstly, we will create a folder named CyberGuard in the path we want by using the command **mkdir /home/admin0/CyberGuard**.

Figure 210 Create a directory

5) To check the file's existence, we can use the command **ls -l** or go to **search computer, type admin0, and the folder CyberGuard** will be there.

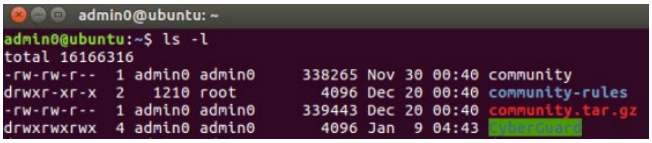

Figure 211 Check file existence using command

Figure 212 Check file existence using GUI

6) To add CyberGuard folder in the samba configuration file, use command **sudo mousepad /etc/samba/smb.conf**

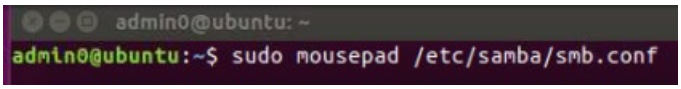

Figure 213 Open configuration file

7) Next, edit the **smb.conf** and press **CTRL + S** to save the file

Figure 214 Samba configuration file

8) To test the correctness of the configuration file, we will use the command **sudo testparm**

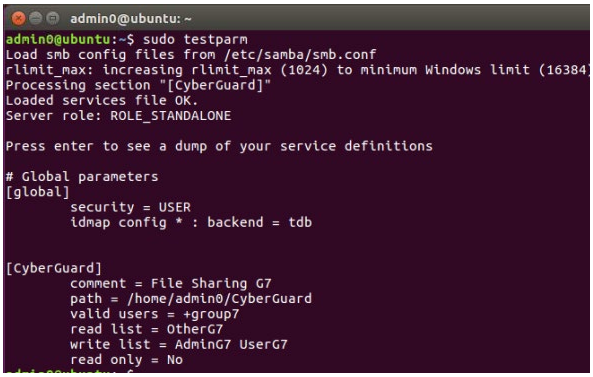

Figure 215 Check correctness of new configuration

9) After making changes in the smb.conf file, we need to restart the smbd and nmbd services by using the command **sudo /etc/init.d/smbd restart** and **sudo /etc/init.d/nmbd restart**

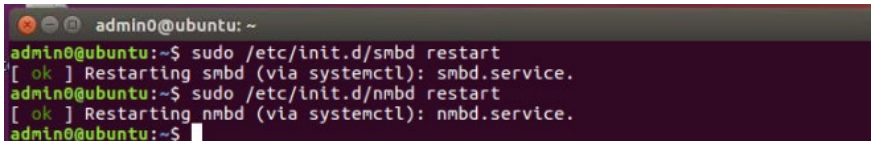

Figure 216 Restart services

10) Allow and update samba traffic by using the command **sudo ufw allow samba**.

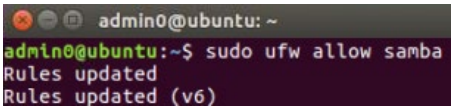

Figure 217 Allow samba in firewall

11) Next, we will add a user, set a password, and enable the user. The command is shown in the table.

Add User	Set Password	Enable User
sudo useradd AdminG7	sudo smbpasswd –a AdminG7	sudo smbpasswd –e AdminG7
sudo useradd UserG7	sudo smbpasswd –a UserG7	sudo smbpasswd –e UserG7
sudo useradd OtherG7	sudo smbpasswd –a OtherG7	sudo smbpasswd –e OtherG7

Table 7 Add. Enable and Set Password for user

After entering the command set password, enter the password and after that, you need to re-enter the password for confirmation.

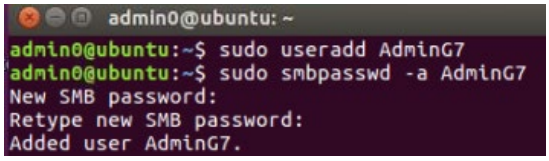

Figure 218 Add and Set Password for AdminG7

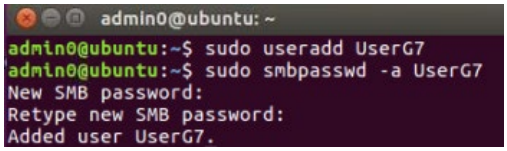

Figure 219 Add and Set Password for UserG7

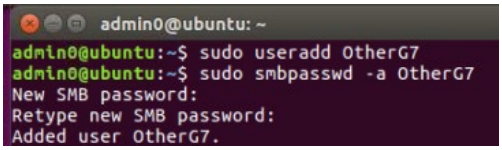

Figure 220 Add and Set Password for OtherG7

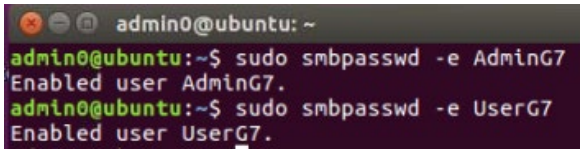

Figure 221 Enable AdminG7 and UserG7

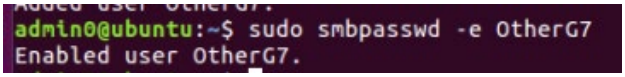

Figure 222 Enable OtherG7

12) Next, create a group and add the user into the group. We need to change the directory using the command **cd /home/admin0/CyberGuard.** To create a group, we will use the command **sudo addgroup group6**. To add the user into a group, use command **sudo adduser AdminG7 group7**, **sudo adduser UserG7 group7** and **sudo adduser OtherG7 group7**.

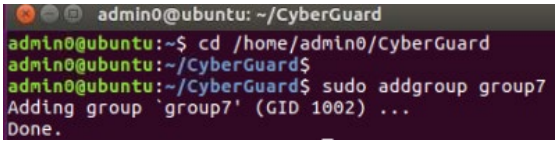

Figure 223 Create group

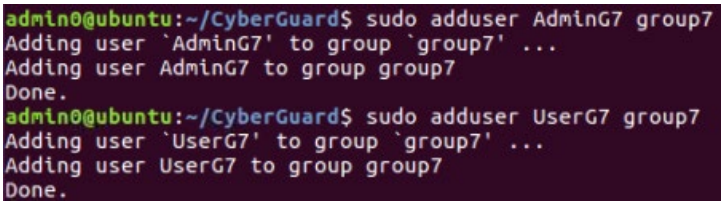

Figure 224 Add AdminG7 and UserG7 into the group

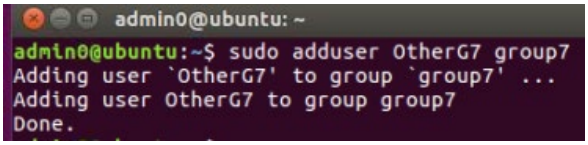

Figure 225 Add OtherG7 into the group

13) To check the list of users in the group, we use command **getent group group7**

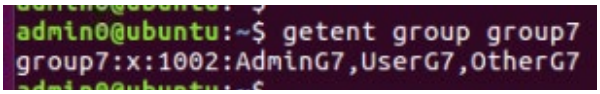

Figure 226 List users in the group

14) Create a file in the CyberGuard folder. We need to change the directory using the command **cd /home/admin0/CyberGuard**. Create a public and private file using the command **mkdir Public** and **mkdir Private**. To check and list files in the CyberGuard folder, use command **ls**. To know the list of files in CyberGuard with the permission, date and time, use command **ll**.

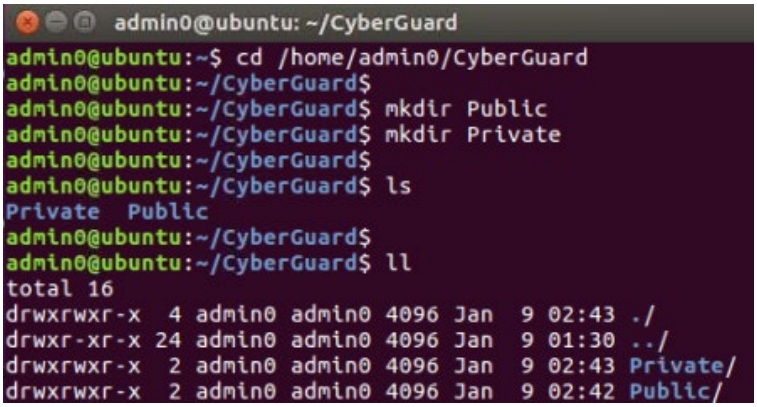

Figure 227 Create folder Public and Private then list file in Cyberguard

15) Next, create a text file in the folder Public and Private.

16) Change the directory to Private by using the command **cd Public** and create a text file using command **Cat > Secure.txt then type its contents, to save press Ctrl + C**. Use ls command to list the file and ll command to list file in detail.

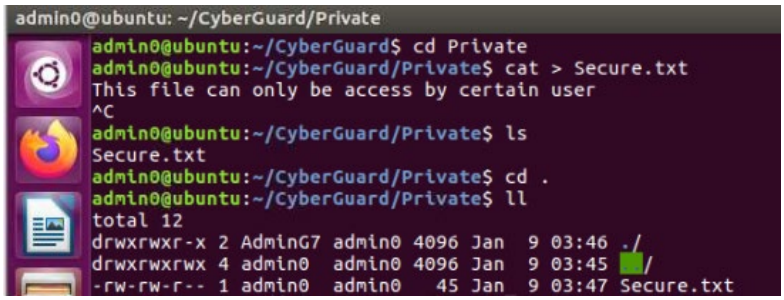

Figure 228 Create a text file in Private and then list the file

17) Change the directory to Public by using command **cd Public** and create a text file using command **Cat > g7.txt then type its contents, to save press Ctrl + C.** Use ls command from listing the file and ll command to list file in detail.

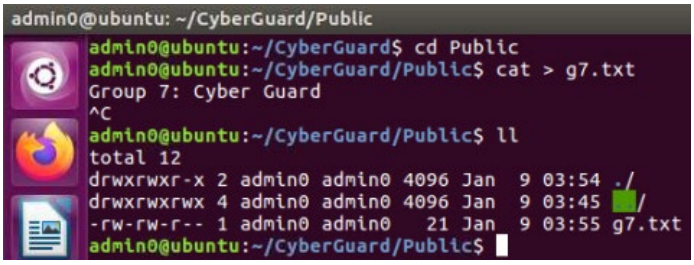

Figure 229 Create a text file in Public and then list the file

18) Change owner permission for file Public and Private. Use command **sudo chown AdminG7 Private** and **sudo chown AdminG7:UserG7 Public**. Next, change the file's permission from 775 to 740 using the command **sudo chmod 740 Private**.

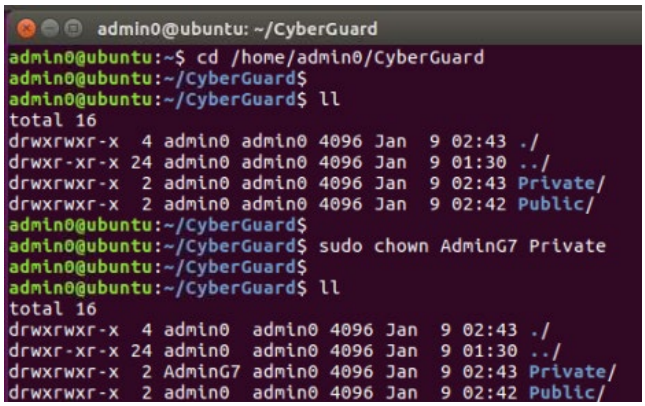

Figure 230 Change owner of Private file

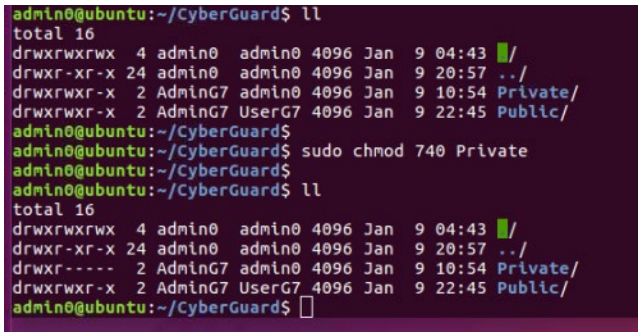

Figure 231 Change permission of the file

5.3.14- FTP Server

Deploying FTP Service in Windows Server

1) Press the “Add Roles and Features” option on the Server Manager to open the installation wizard. Click next until you reach the Server Roles section

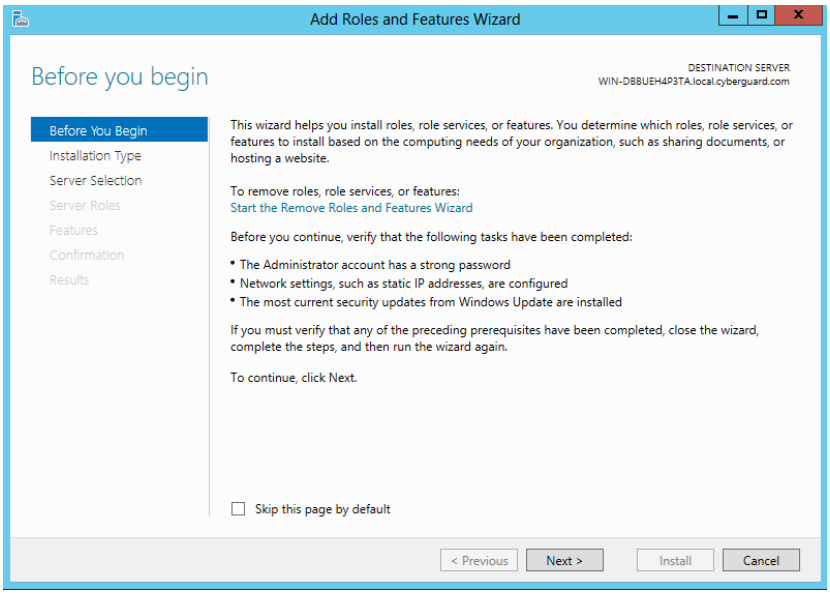

Figure 232 Add Roles and Features Wizard

2) Under Web Server (IIS), choose the FTP Server, then confirm the installation

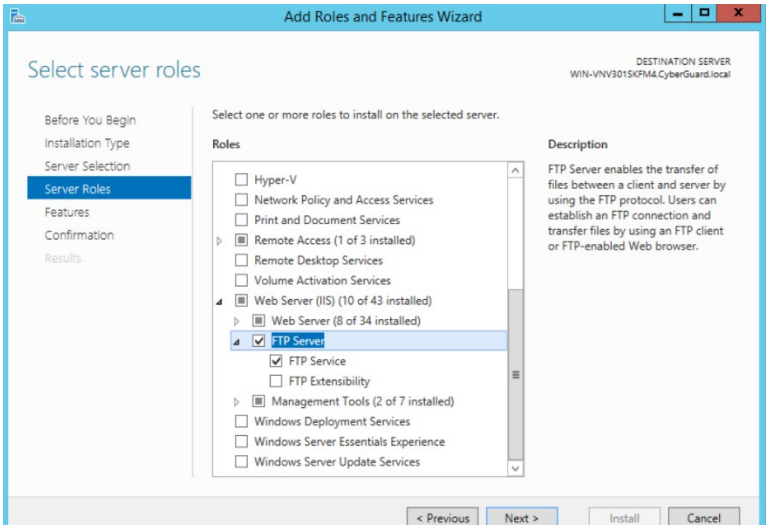

Figure 233 Select FTP Server in Server Roles

3) On the Server Manager, under the Tools option, choose IIS Manager

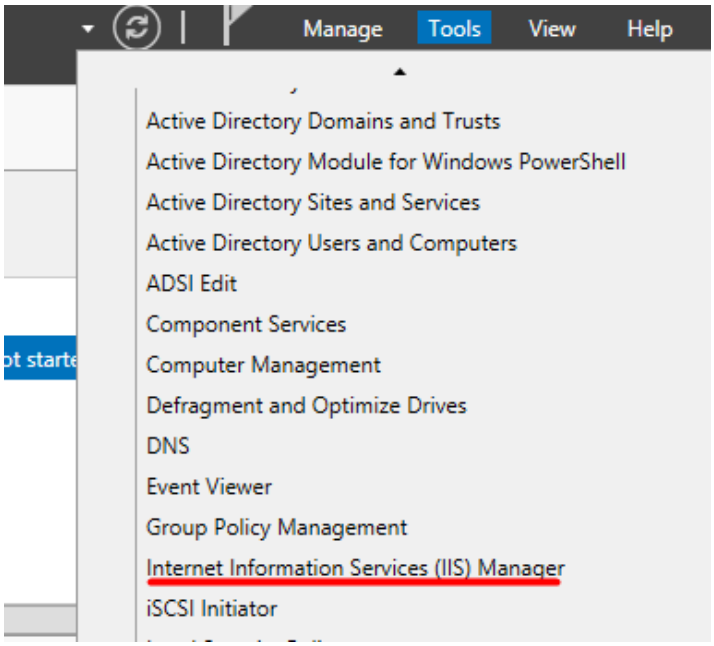

Figure 234 IIS Manager under Tools

4) On the IIS Manager, right-click the name of your server and choose Add FTP Site

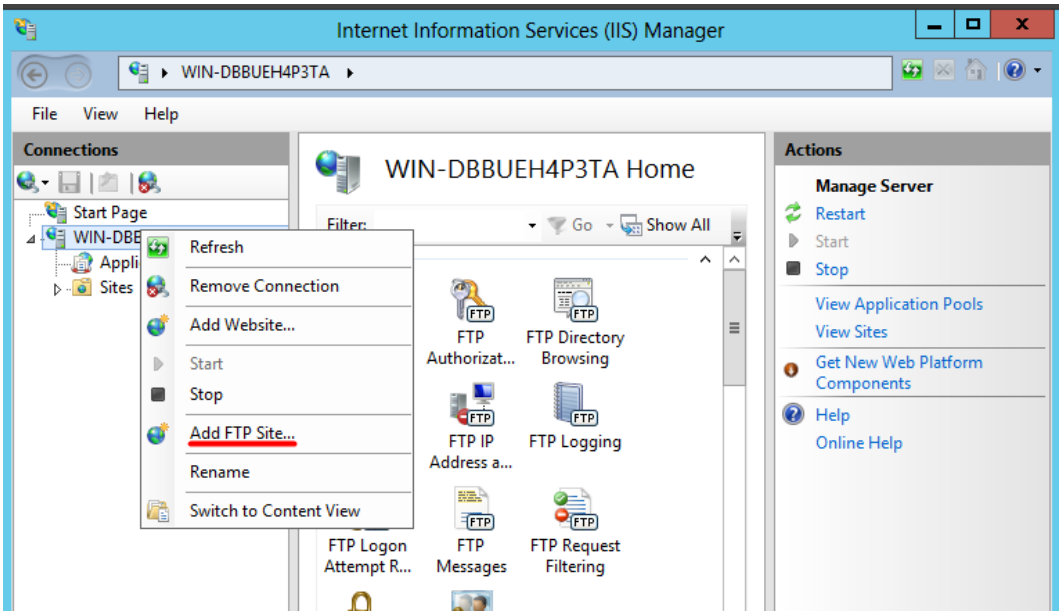

Figure 235 Adding FTP site

5) Enter a desired FTP site name and the content directory. It would be best if you created a new directory for this purpose

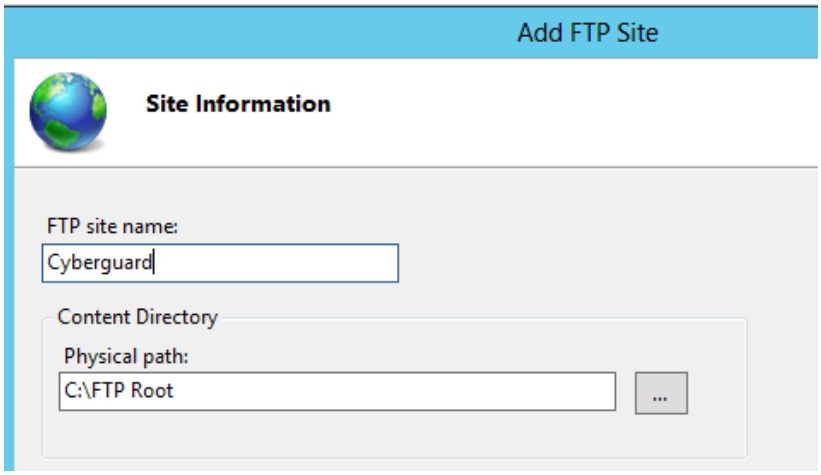

Figure 236 Enter FTP Site Name

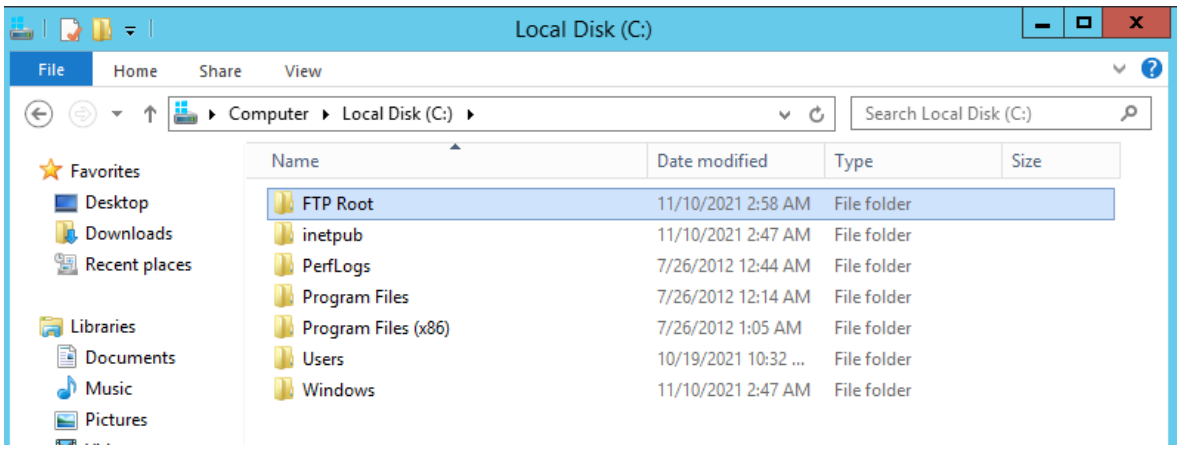

Figure 237 Setting FTP Root Folder

6) Choose the IP address of the server and choose No SSL certificate, then click next

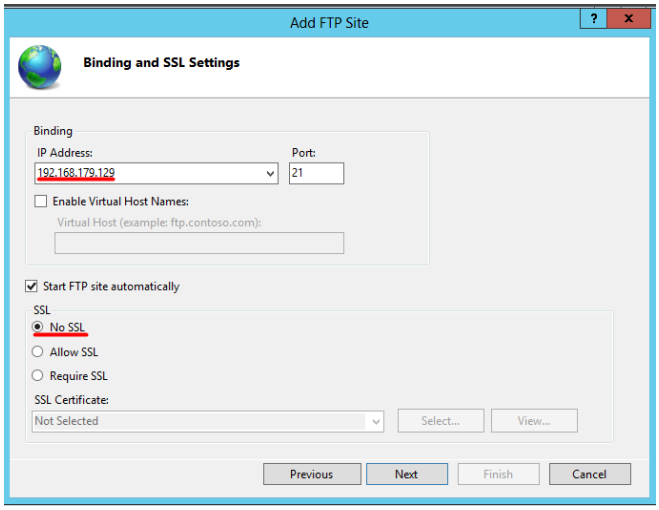

Figure 238 Binding and SSL Settings

7) Here we can set the authentication and authorization of the FTP service. For our usage, authorization will be set for all users and Read and Write permissions given

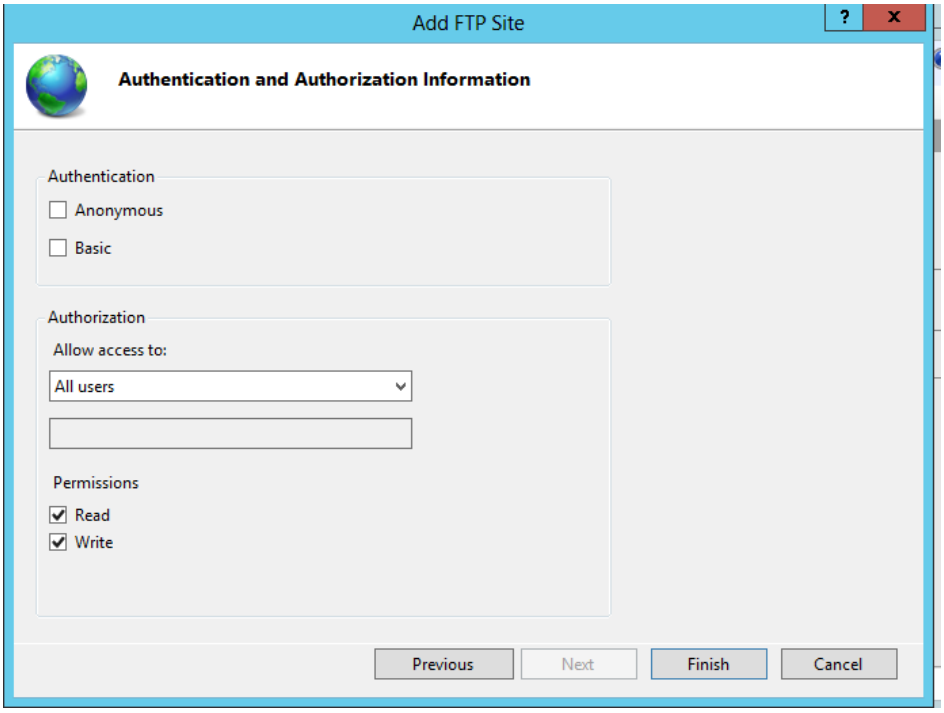

Figure 239 Authentication and Authorization Information

5.4- Extra Service Installation and Configuration

5.4.1- EtherChannel

1) Choose two interfaces to configure as EtherChannel.

```
HQ-CS-01(config)#int range e0/0-1
```

Figure 240 Interface range command

2) Enable the EtherChannel commands.

```
HQ-CS-01(config)#int range e0/0-1
HQ-CS-01(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
```

Figure 241 EtherChannel configuration

3) Verify the EtherChannel's port-channel created.

```
HQ-CS-01#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)           -        Et0/0(D)    Et0/1(D)
```

Figure 242 EtherChannel summary

5.4.2- Dynamic NAT (NAT Overload)

1) Define the NAT inside and outside interfaces.

```
HQ-RT-01(config)#int e0/0
HQ-RT-01(config-if)#ip nat outside
HQ-RT-01(config-if)#
HQ-RT-01(config-if)#int e1/2.10
HQ-RT-01(config-subif)#ip nat inside
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.20
HQ-RT-01(config-subif)#ip nat inside
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.30
HQ-RT-01(config-subif)#ip nat inside
HQ-RT-01(config-subif)#
HQ-RT-01(config-subif)#int e1/2.40
HQ-RT-01(config-subif)#ip nat inside
```

Figure 243 Assign inside and outside the port

2) Create an Access Control List (ACL) that will include local (private) hosts or network(s).

```
HQ-RT-01(config)#ip access-list standard NAT
HQ-RT-01(config-std-nacl)#permit 10.10.0.0 0.0.255.255
HQ-RT-01(config-std-nacl)#permit 10.20.0.0 0.0.63.255
HQ-RT-01(config-std-nacl)#permit 10.30.0.0 0.0.0.255
HQ-RT-01(config-std-nacl)#permit 10.40.0.0 0.0.1.255
```

Figure 244 NAT's ACL configuration

3) Enable NAT overload and bind it to the outside interface previously selected.

```
HQ-RT-01(config)#ip nat inside source list NAT interface e0/0 overload
```

Figure 245 Enable NAT service

4) Verifying NAT overload operation with show commands.

#show ip nat statistics

```
HQ-RT-01#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet1/2.10, Ethernet1/2.20, Ethernet1/2.30, Ethernet1/2.40
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT interface Ethernet0/0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Figure 246 NAT statistics

5.4.3- IPsec Point-To-Point VPN

1) Configure an ISAKMP Phase 1 policy.

```
HQ-RT-01(config)#crypto isakmp policy 10
HQ-RT-01(config-isakmp)#encr aes 256
HQ-RT-01(config-isakmp)#authentication pre-share
HQ-RT-01(config-isakmp)#group 5
```

Figure 247 ISAKMP policy

2) Define a pre-shared key for authentication with our peers.

```
HQ-RT-01(config)#crypto isakmp key secretkey address 209.165.100.2
```

Figure 248 Pre-shared key configuration

3) Create an access list and define the traffic that would like the router to pass through the VPN tunnel.

```
HQ-RT-01(config)#access-list 100 permit ip 10.0.0.0 0.255.255.255 20.0.0.0 0.2$
```

Figure 249 ACL configuration

4) Create the transform set used to protect data.

```
HQ-RT-01(config)#crypto ipsec transform-set HQ-BR esp-aes 256 esp-sha-hmac
HQ-RT-01(cfg-crypto-trans)# mode tunnel
```

Figure 250 Transform set configuration

5) Create a crypto map that connects the previously defined ISAKMP and IPSec configuration.

```
HQ-RT-01(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ-RT-01(config-crypto-map)# set peer 209.165.100.2
HQ-RT-01(config-crypto-map)# set security-association lifetime seconds 86400
HQ-RT-01(config-crypto-map)# set transform-set HQ-BR
HQ-RT-01(config-crypto-map)# set pfs group5
HQ-RT-01(config-crypto-map)# match address 100
```

Figure 251 Crypto map configuration

6) Apply crypto map to the public interface.

```
HQ-RT-01(config)# interface Ethernet1/3
HQ-RT-01(config-if)# ip address 209.165.100.1 255.255.255.0
HQ-RT-01(config-if)# crypto map IPSEC-MAP
HQ-RT-01(config-if)#
*Dec  4 05:16:36.719: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure 252 Assign a crypto map

7) Establishing and verifying the IPsec VPN tunnel and encrypted packets.

#show crypto isakmp sa

```
HQ-RT-01#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.100.2   209.165.100.1   QM_IDLE           1001 ACTIVE
```

Figure 253 Tunnel established

#show crypto ipsec sa

```
HQ-RT-01#show crypto ipsec sa

interface: Ethernet1/3
    Crypto map tag: IPSEC-MAP, local addr 209.165.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (20.0.0.0/255.0.0.0/0/0)
   current_peer 209.165.100.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

Figure 254 Packets sent and received

5.5- Conclusion

Before the test, the services in the testing phase complete the installation and configuration procedures. Because the required method varies, installation of a programme is the act of putting the programme onto a computer system so that it can be run. Many programmes come with a general-purpose or customised installer for each programme and each computer. This step must be completed to ensure that the service can function properly throughout the testing phase. The installation tutorial will assist in getting up and running quickly.

CHAPTER 6: TESTING

6.1- Introduction

Different methodologies and approaches have been used to test all the services processes. This section will explain how to test all the services that have been installed and configured. It is critical to test the services to isolate them and demonstrate that the various components are correct. Furthermore, testing allows you to demonstrate the services are successfully up and running. Excellent testing is when errors occur and are recognised, we will locate the source of the error. Also, find the solutions to fix the flaws and create improvements in order to achieve the most satisfactory performance.

6.2- Services Testing

6.2.1 - VLAN and Inter VLAN Routing

1) Verify the VLAN created.

```
HQ-CS-01#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                                 Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                                 Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   employee                          active    Gi0/0
20   Management                        active    Gi0/1
30   Server                            active    Gi0/2
40   Wireless                          active    Gi0/3
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Figure 255 Show VLAN brief output

2) Verify the VLAN routing connectivity with the ping command.

Ping from Vlan 10 to Vlan 20

```
HQ-RT-01#ping 10.20.0.1 source 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Figure 256 Ping Vlan 10 to Vlan 20

Ping from Vlan 10 to Vlan 30

```
HQ-RT-01#ping 10.30.0.1 source 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Figure 257 Ping Vlan 10 to Vlan 30

Ping from Vlan 10 to Vlan 40

```
HQ-RT-01#ping 10.40.0.1 source 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.40.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Figure 258 Ping Vlan 10 to Vlan 40

6.2.2- Port Security

1) Verify the VLAN port security with the show command.

```
HQ-CS-01#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
     Gi0/0              1            0                  0         Shutdown
     Gi0/1              1            0                  0         Shutdown
     Gi0/2              1            0                  0         Shutdown
     Gi0/3              1            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Figure 259 Show port-security output

2) Check recovery mode is enabled and interval time left.

```
HQ-CS-01#sh errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Enabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

Figure 260 Show error recovery output

6.2.3- ACL Router

1) Verify the access control list created.

```
HQ-RT-01#sh access-list
Extended IP access list HQ_BRANCH
    10 permit udp any any eq isakmp
    20 permit ahp any any
    30 permit esp any any
    40 permit udp any any eq non500-isakmp
    50 permit gre any any
    60 permit icmp any any echo-reply
    70 permit ospf any any
    80 permit icmp 20.20.0.0 0.0.0.255 any
```

Figure 261 Show access-list output

6.2.4- IPsec VPN (Client-Server)

1) Verify the remote access VPN successful to HQ check IP addresses assigned to the VPN Client. To check IP address assigned, use command “ipconfig” in the cmd. The IP address should get the HQ internal IP address.

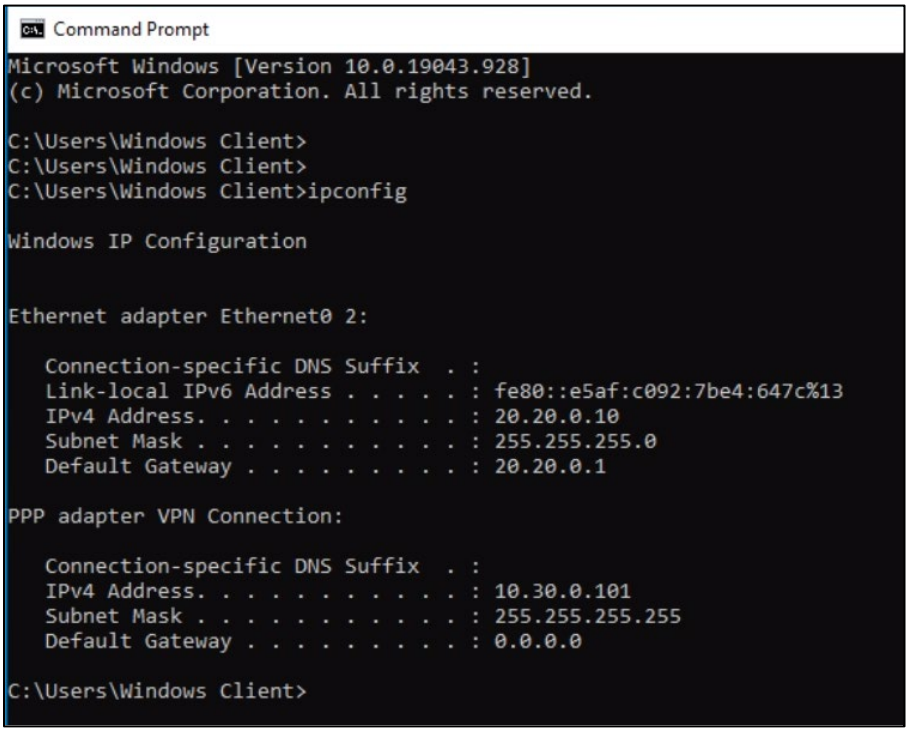

Figure 262 Ipconfig output

2) To show the connection is encrypted with IPSEC. Check the VPN network adapter here, which is L2TP, also known as IPSEC.

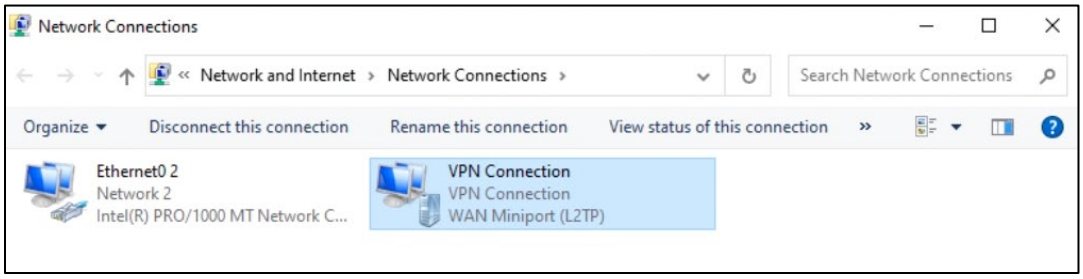

Figure 263 VPN adapter

3) Or check in Details, Encryption is using IPSEC.

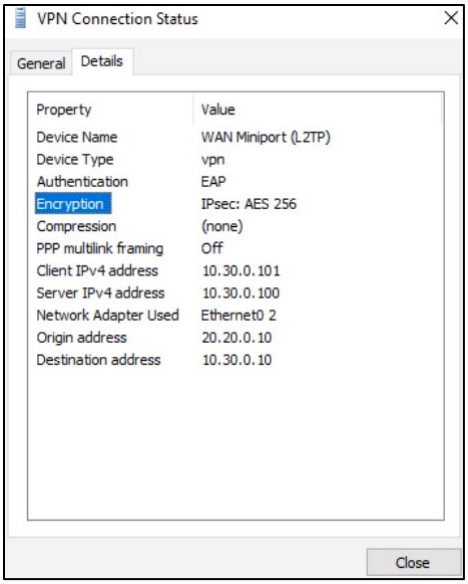

Figure 264 VPN adapter status

4) Go to firewall (ctrl+r) wf.msc, go to "Monitoring", "Security Associations", "Main Mode". Show the authentication mode, using preshared key. Preshared key for authentication means IPsec encryption. Prove the encryption is IPSEC.

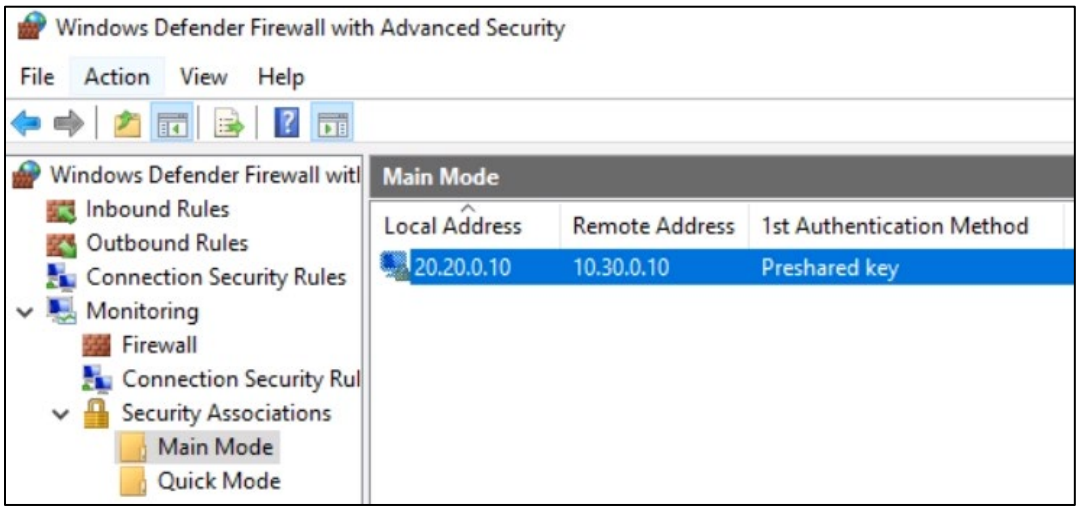

Figure 265 VPN server-client list

5) Check from the server, go to routing and remote access, show remote access client, double click on the client, show the frame in and frame out. bytes in and bytes out.

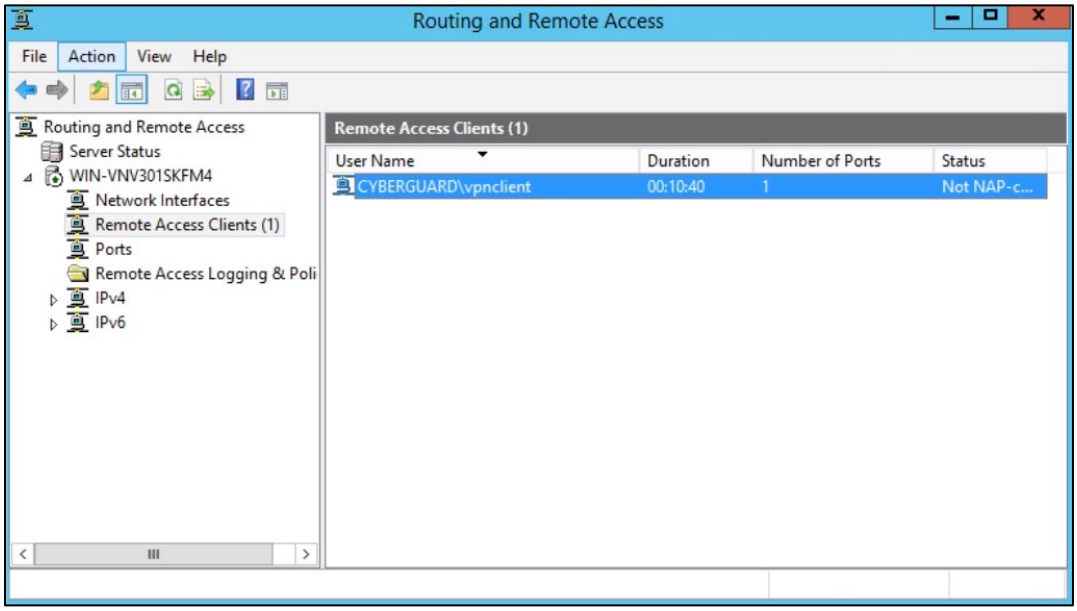

Figure 266 Remote access client list

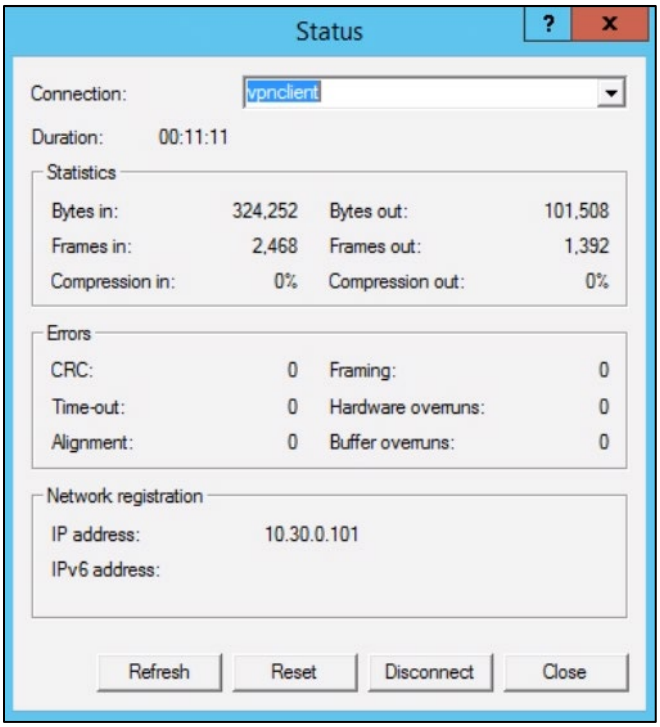

Figure 267 VPN connection status

6.2.5- Radius Server Authentication & Authorization

1) Exit from the router configuration terminal and login with the radius server user credential. Username: radiusadmin, Password: g7CyberGuard.

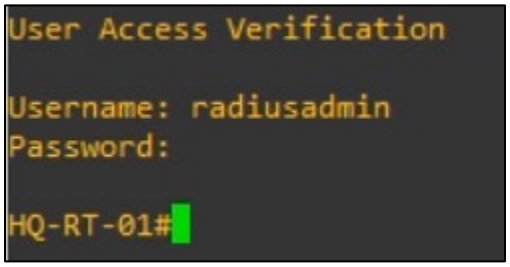

Figure 268 Radius authentication login

6.2.6- DNS (IPv4)

1) Our created DNS is up and running and can be tested by pinging the DNS

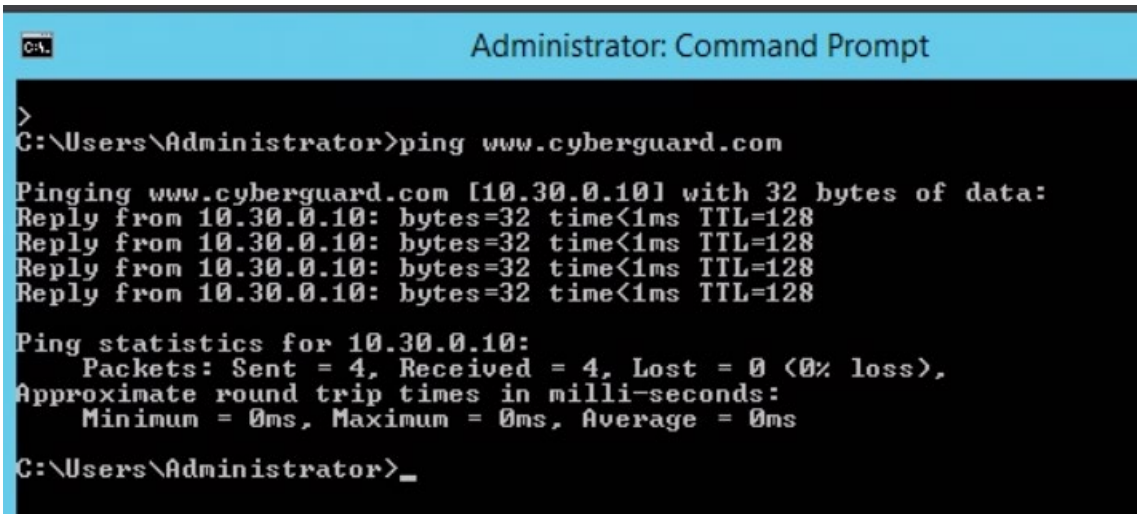

Figure 269 Pinging www.cyberguard.com DNS

6.2.7- DHCP (IPv4)

Test Using Windows 10 Local Client

1) Go to Windows 10 Local Client
2) Search for Network Connections and click on View network connections.

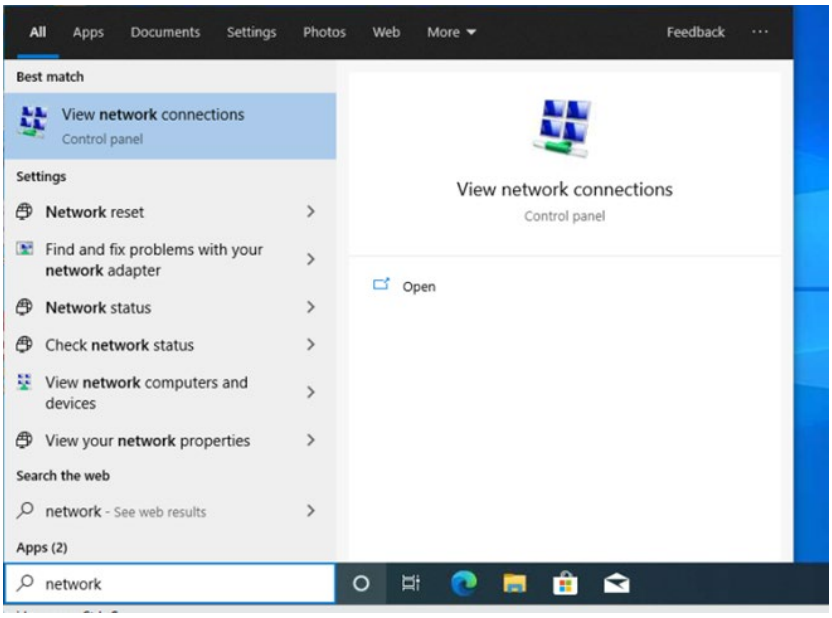

Figure 270 View Network Connections in Windows

3) Right-click on Ethernet0 2 and choose Properties.

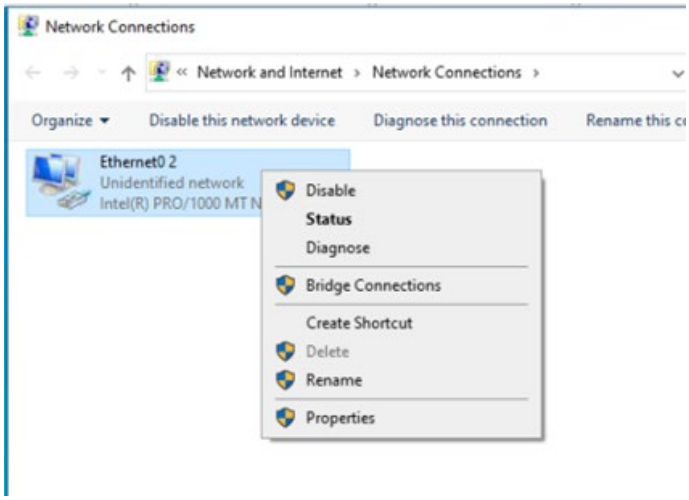

Figure 271 Network Connections page

4) Click on Internet Protocol Version 4 (TCP/IPv4) and choose Properties.

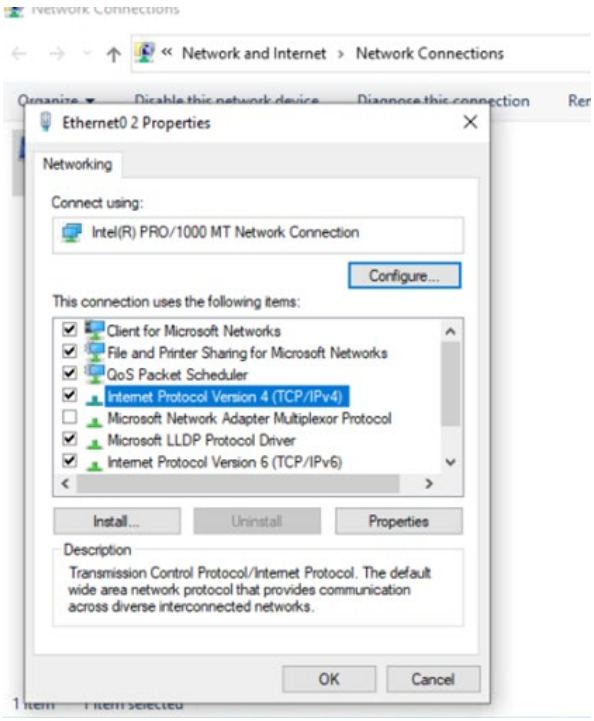

Figure 272 Ethernet0 2 Properties

5) Choose to obtain IP address automatically. Then, click OK.

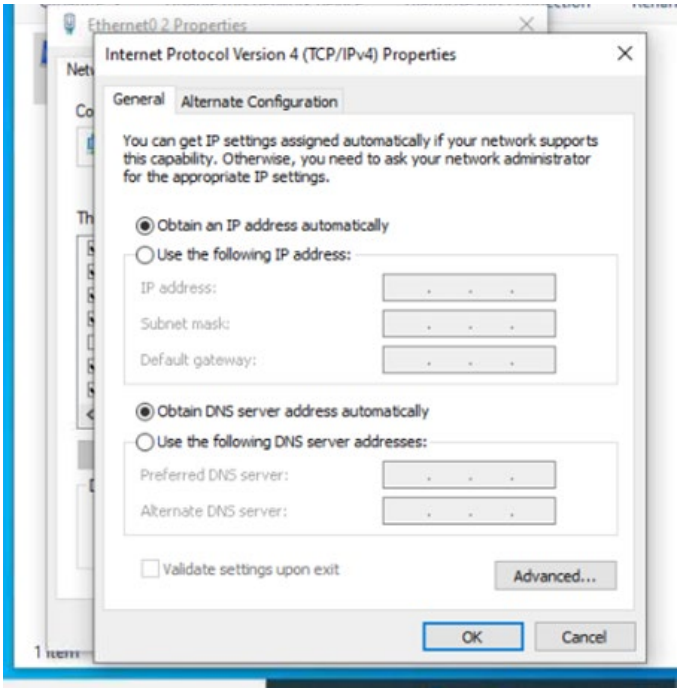

Figure 273 Internet Protocol Version 4 (TCP/IPv4) Properties

6) Open Command Prompt. Using command ipconfig will show the IP address assigned to this Windows 10 Local Client.

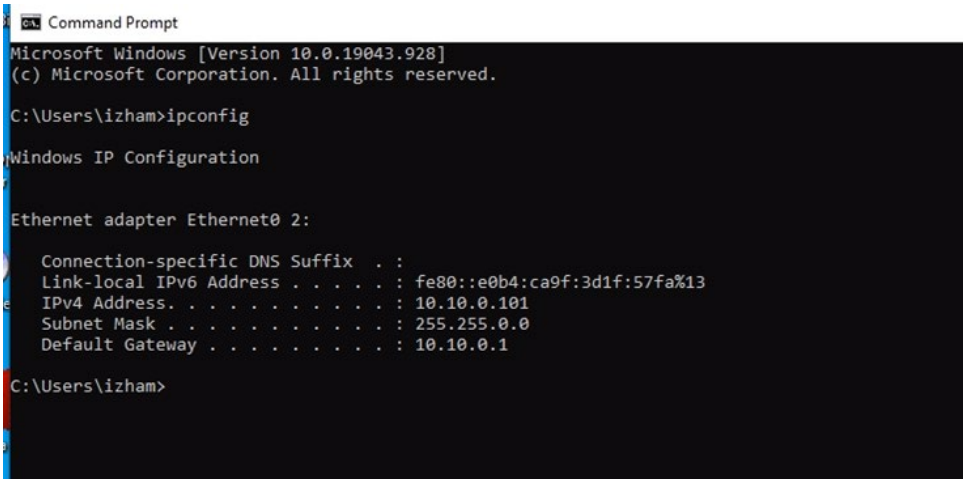

Figure 274 IP address assigned to Windows 10 Local Client

7) To view the detailed information, use the command ipconfig /all.

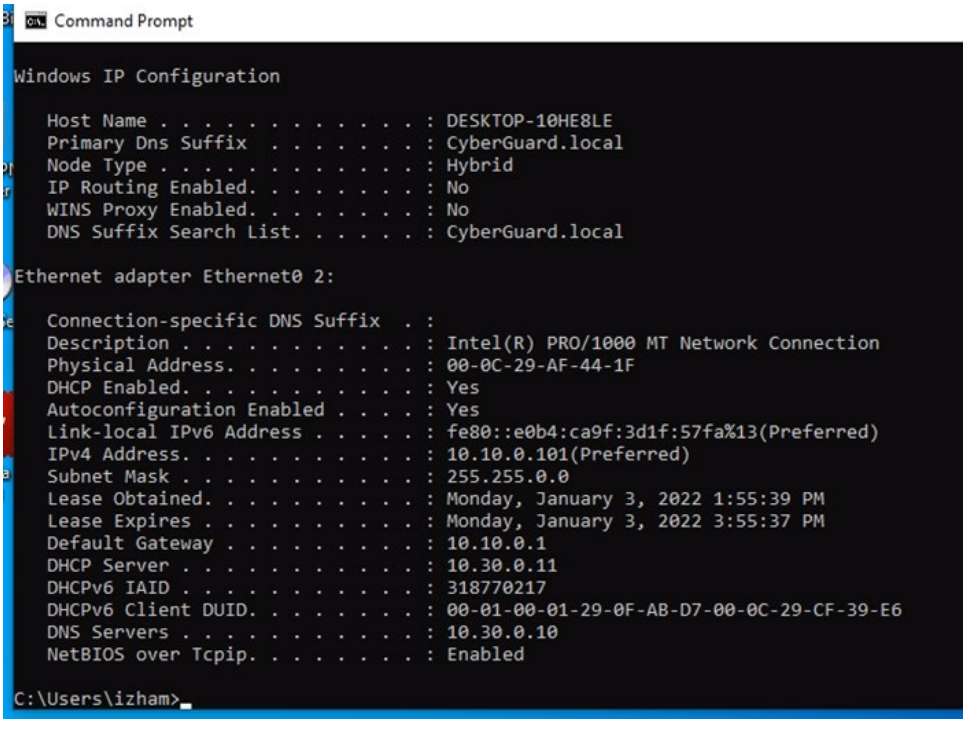

Figure 275 Details of IP address

Test Using Ubuntu (User)

1) Go to Ubuntu (User) and start the VM.
2) Open the terminal and search for IP address by typing command ifconfig.

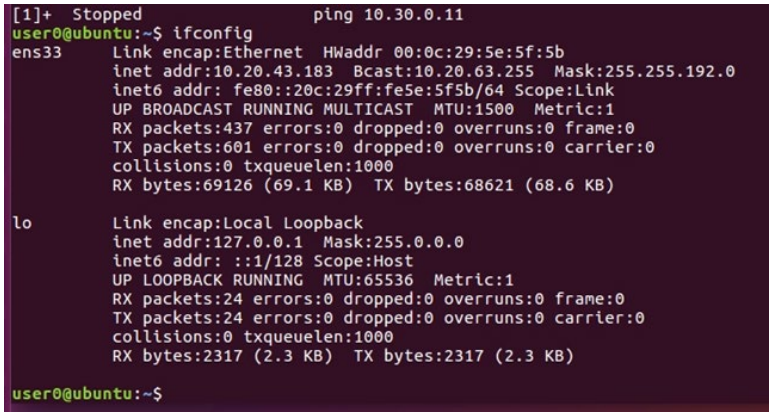

Figure 276 The IP address assigned to Ubuntu (User)

6.2.8- User Authentication by Integrating AD with Linux

1) To join the domain as administrator, enter the command 'kinit Administrator' and enter the password for the account. Type in the command 'klist' to list our authentication ticket and the expiry time.

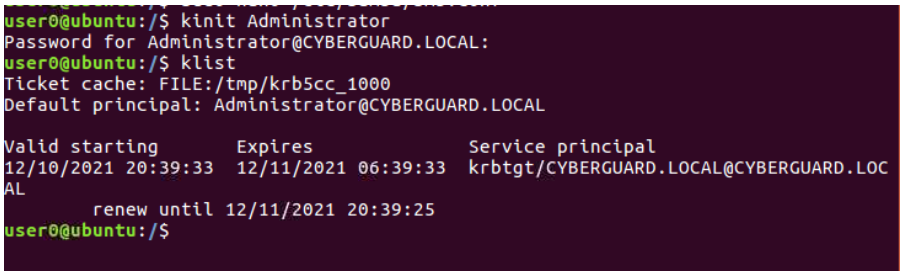

Figure 277 Joining AD as Administrator

2) To ensure our Linux machine has successfully logged into Active Directory, use the command 'realm join cyberguard.local –user=Administrator' and if prompted, enter the appropriate password.

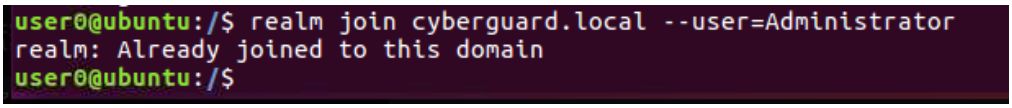

Figure 278 Checking if successfully logged in

6.2.9- Windows Server Hardening Vulnerability Report

Testing

1) Scan for open port using Nmap. Disable any unused port to minimize risk.

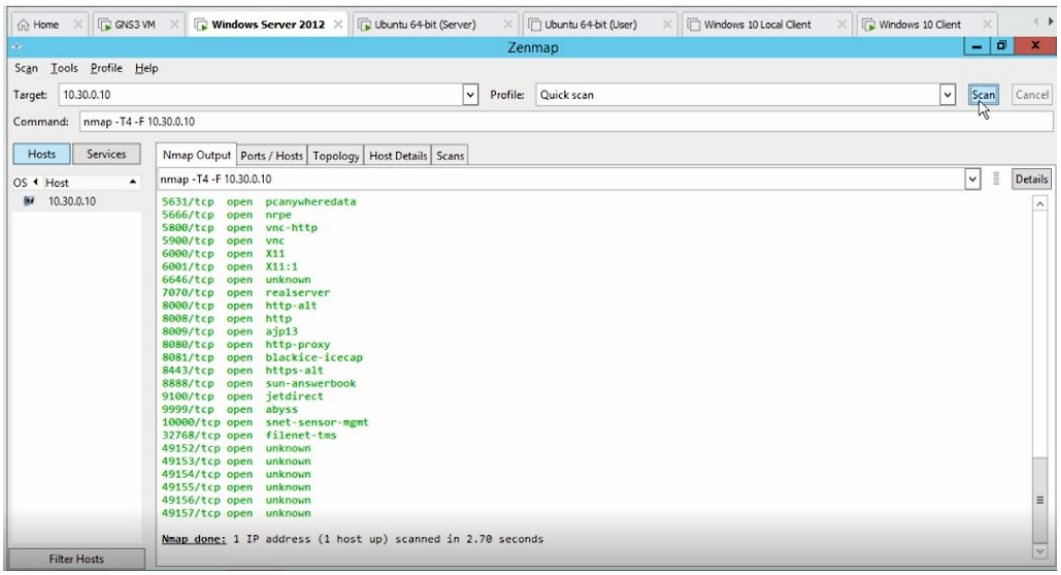

Figure 279 Scan for open port

2) Ensure that the status of the update is set to automatically updates

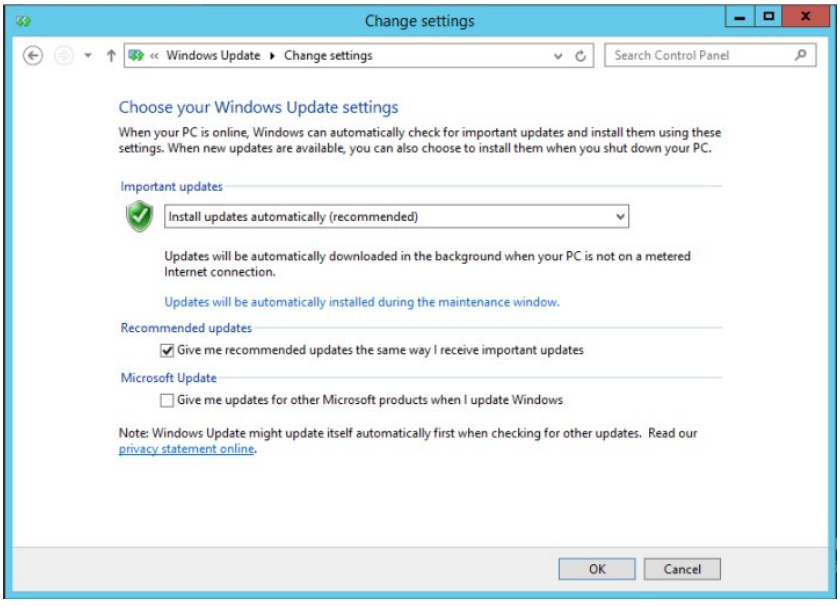

Figure 280 Setting for Windows Update

3) Check and updates the patches

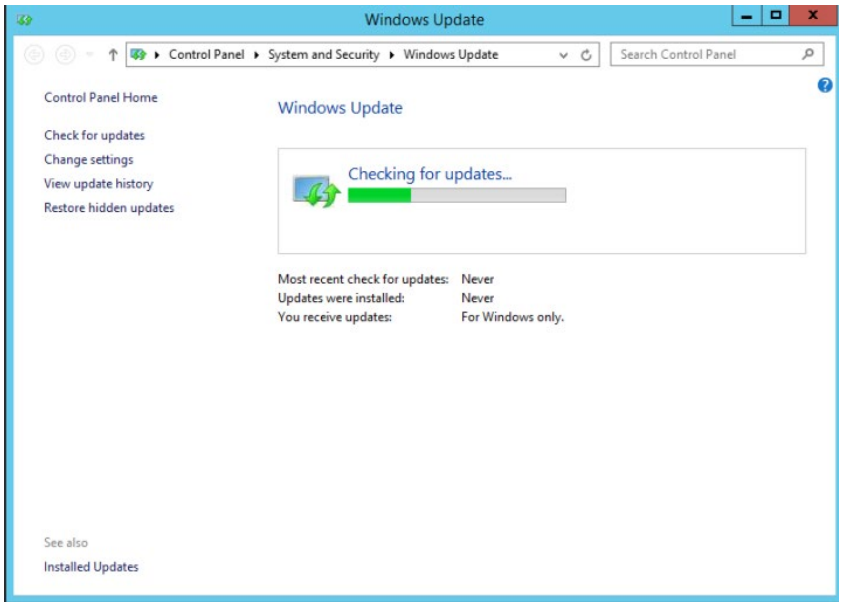

Figure 281 Check for any updates

4) Check the security settings for Password Policy after enabling the password requirements.

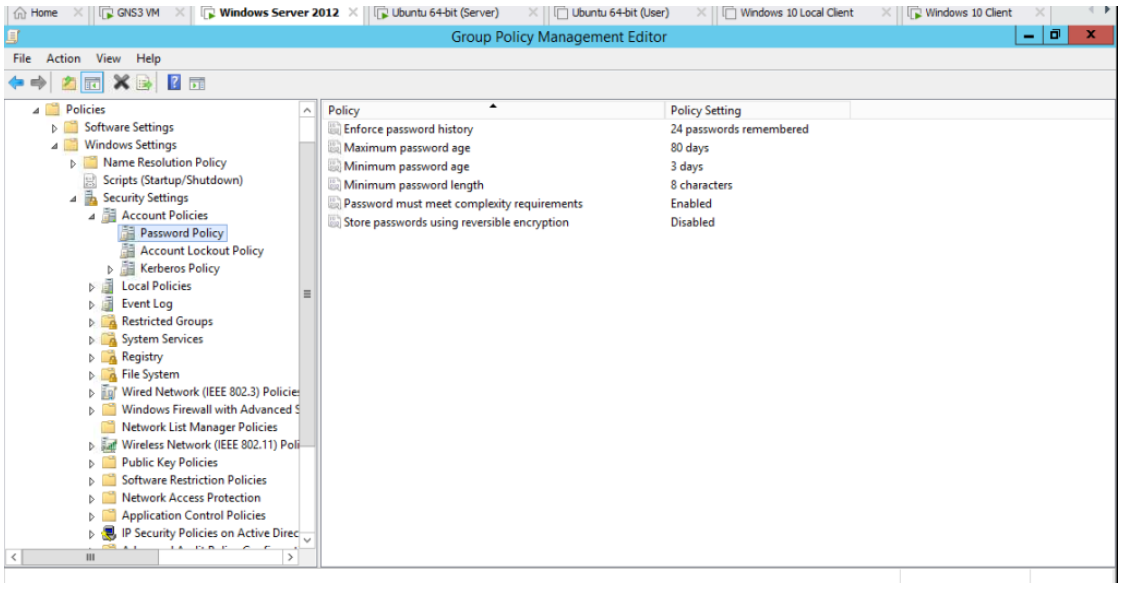

Figure 282 Password Policy

5) Check the security settings for the Account Lockout Policy.

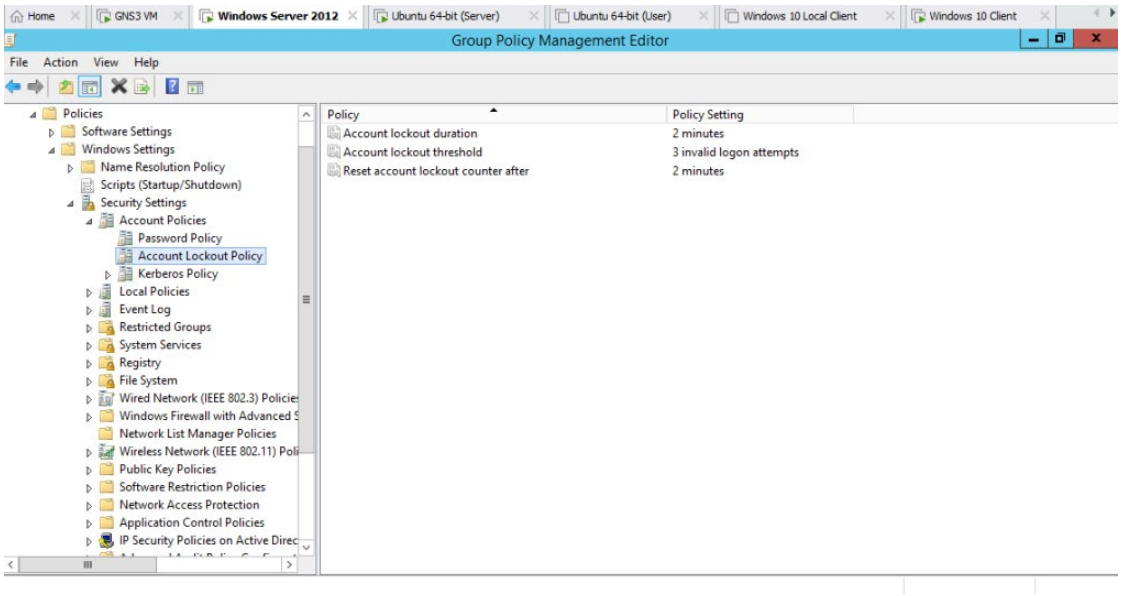

Figure 283 Account Lockout Policy

6) If user insert 3 invalid password, the account will be lockout.

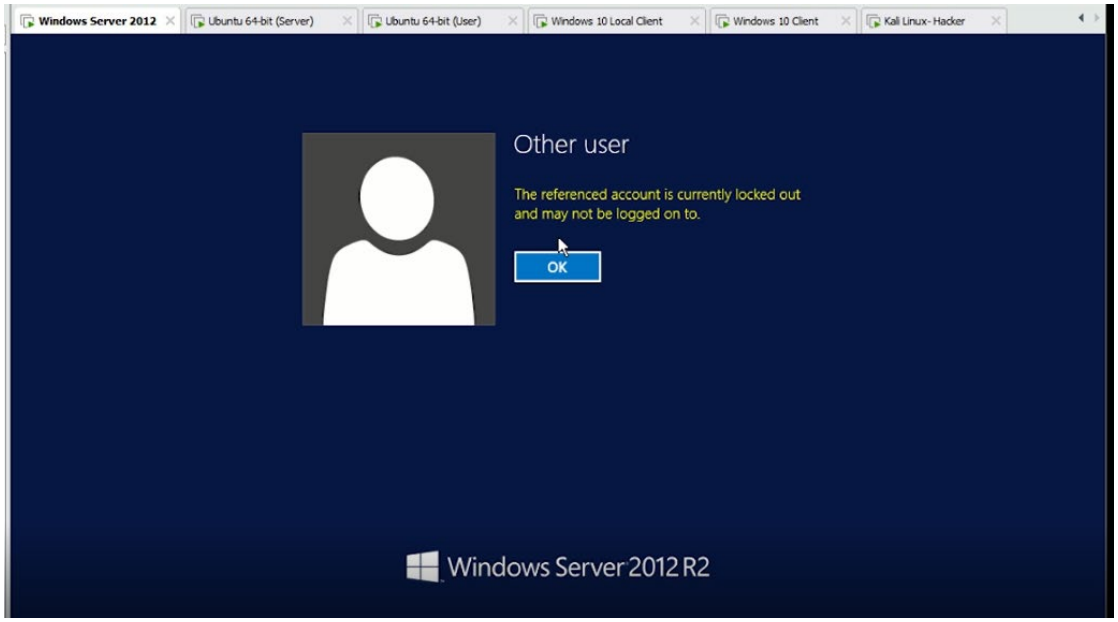

Figure 284 Show an account that has been locked due to 3 invalid attempt

7) Security Banner

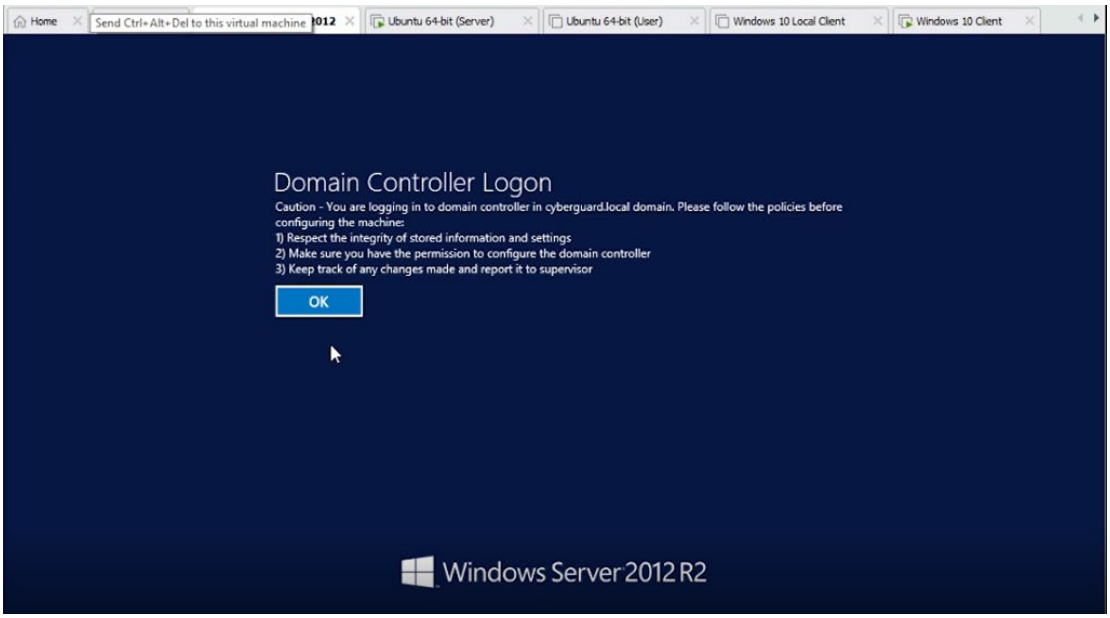

Figure 285 Security banner before login

8) Every time login must click CTRL + ALT + DELETE

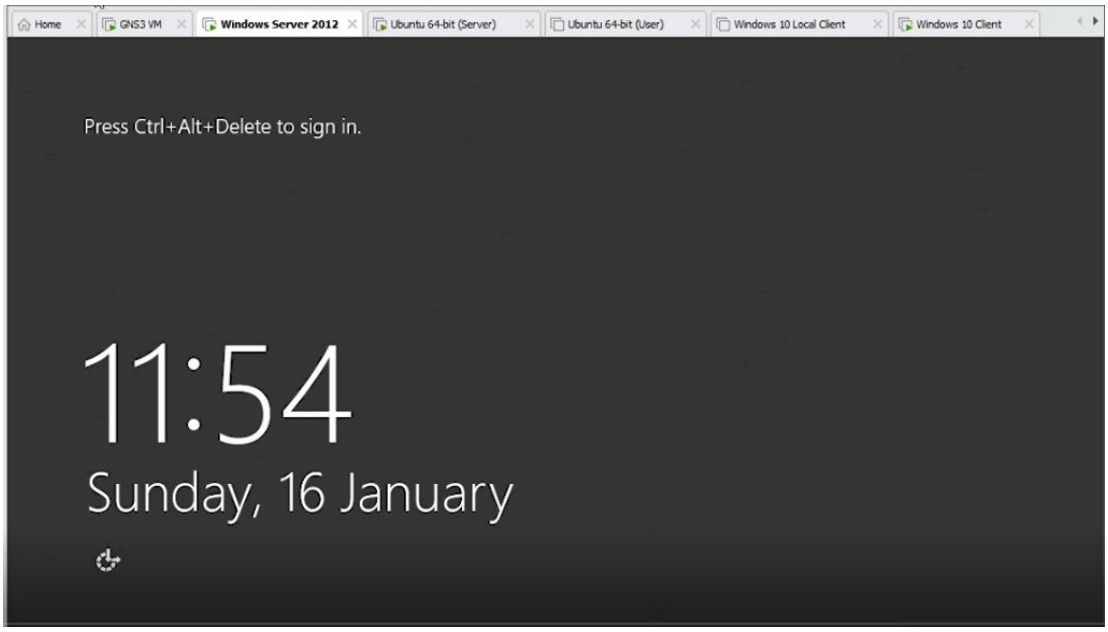

Figure 286 Login interface of Windows Server 2012

9) Disable the unnecessary guest account.

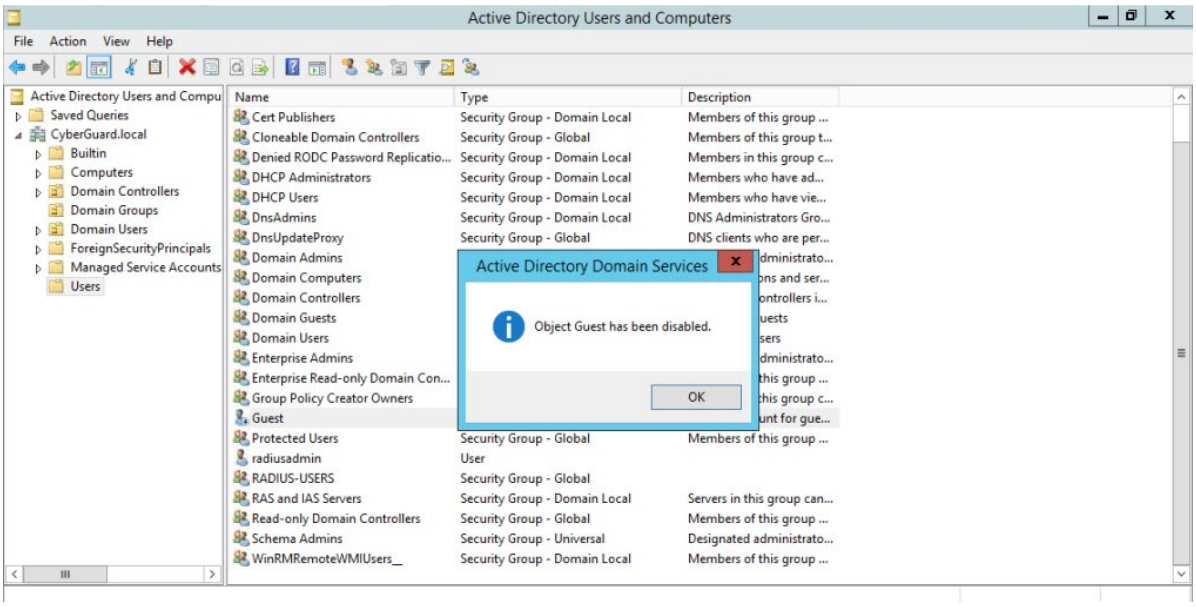

Figure 287 Disable the guest account

10) Check the security settings for Audit Policy in Local Security Policy. Make sure all the policy setting is Success, Failure.

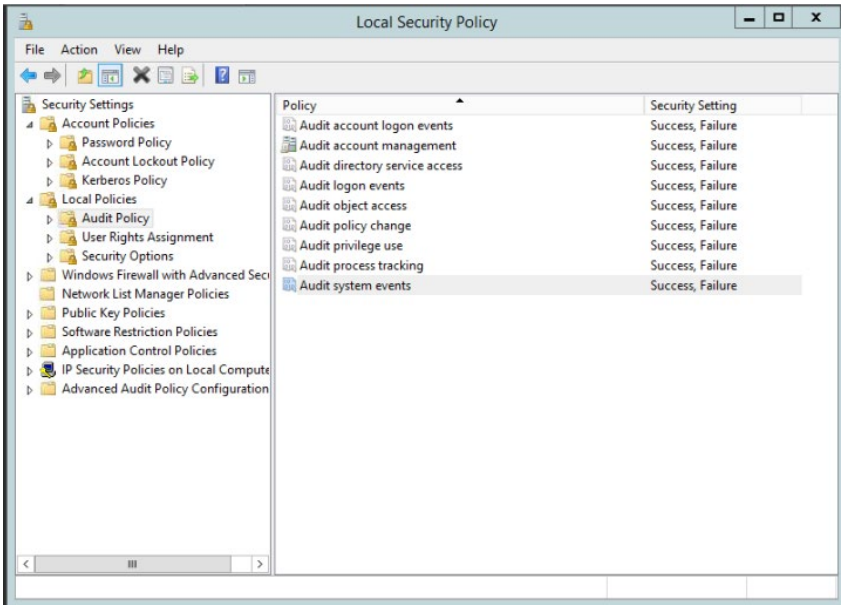

Figure 288 Audit Policy that has been configured

11) Check the Firewall status, make sure all firewall for Domain, Private and Public is ON.

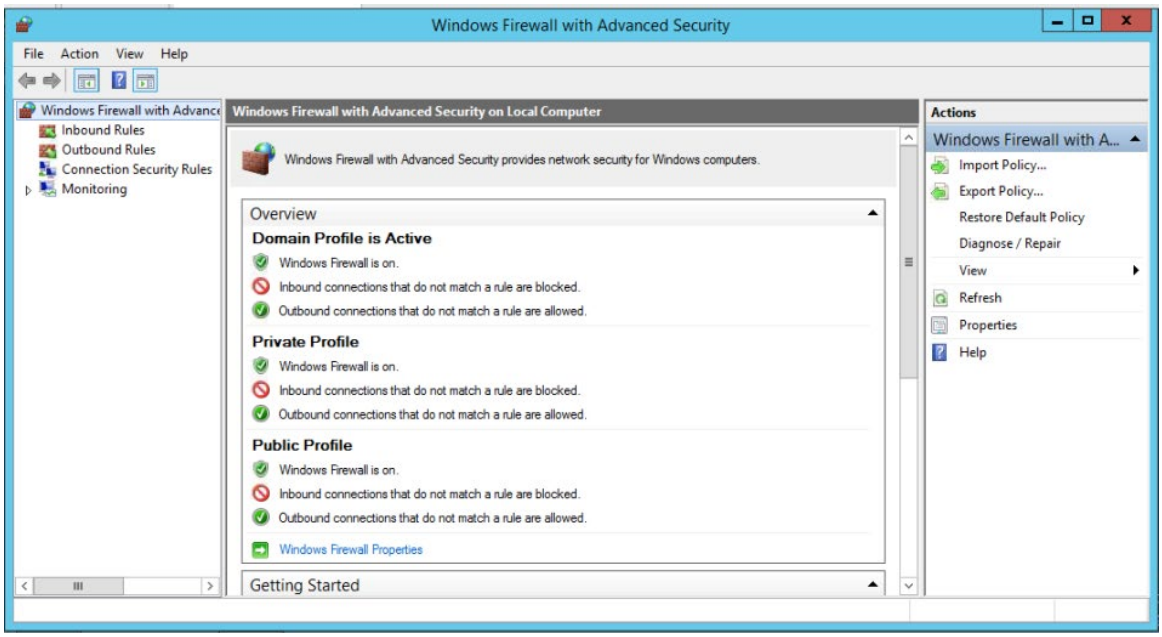

Figure 289 The status of the firewall

6.2.10- Linux Server Hardening Vulnerability Report

Testing

1) Open the terminal and go to root. Type chage -l <username> to check password aging.

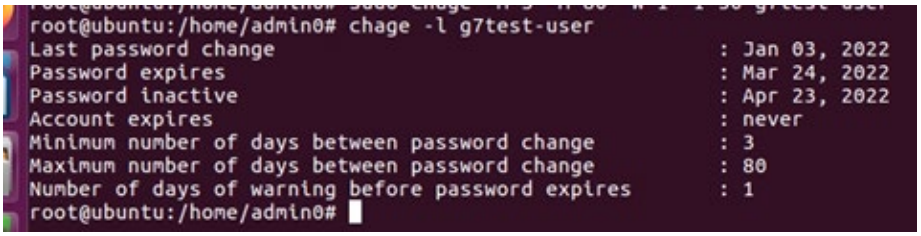

Figure 290 Verification of password aging

2) Set permission on Sensitive System File only root verification.

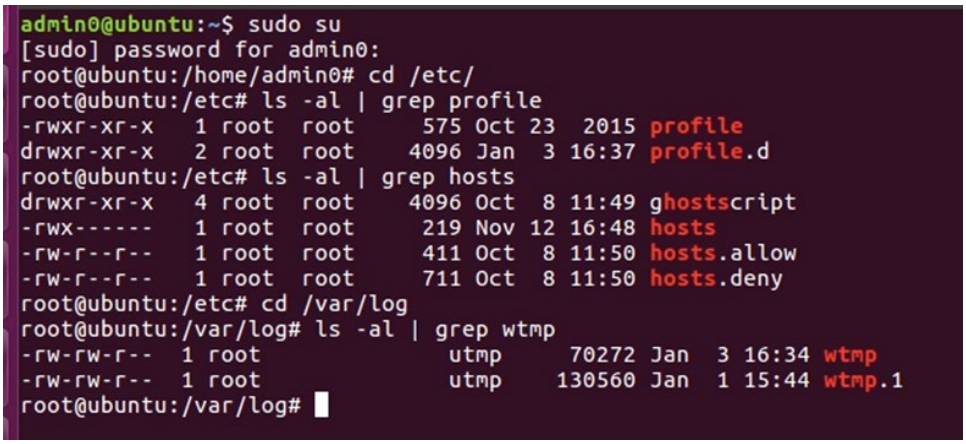

Figure 291 Verify on system file permission

3) Set permission on Sensitive System File for user files verification.

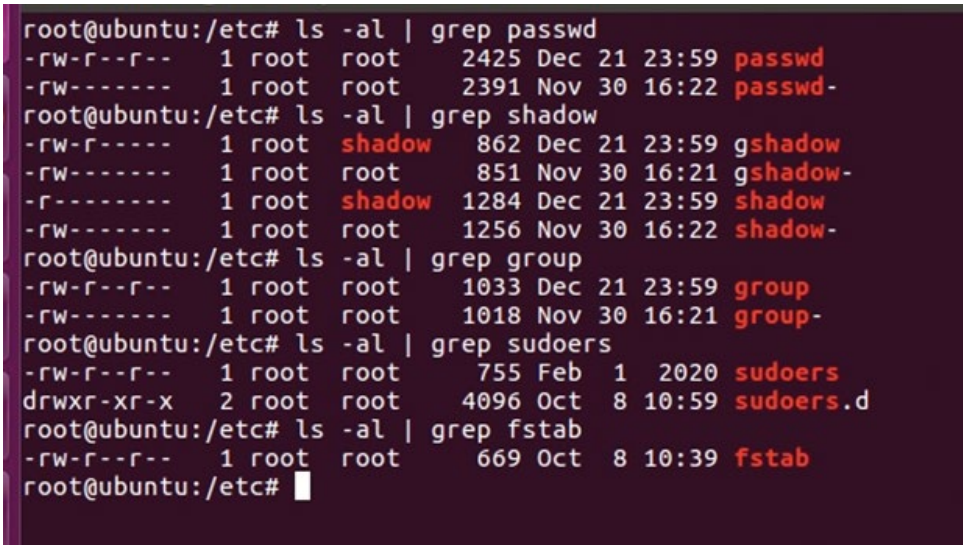

Figure 292 Verify on users accessible file permission

4) Verify on the CUPS port that has been stopped.

```
SB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (1 2 3 4 5) of script `cups' override
s LSB defaults (1).
root@ubuntu:/home/admin0# netstat -tlpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
2043/smbd
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
2008/sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
2008/sshd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
2043/smbd
tcp6       0      0 :::139                  :::*                    LISTEN
2043/smbd
tcp6       0      0 :::2222                 :::*                    LISTEN
2008/sshd
tcp6       0      0 :::22                   :::*                    LISTEN
2008/sshd
tcp6       0      0 :::445                  :::*                    LISTEN
2043/smbd
root@ubuntu:/home/admin0#
```

Figure 293 CUPS port stopped

5) Verify on disabled CUPS service.

```
root@ubuntu:/home/admin0# service cups status
● cups.service - CUPS Scheduler
   Loaded: loaded (/lib/systemd/system/cups.service; disabled; vendor preset: en
   Active: inactive (dead) since Mon 2022-01-03 16:45:09 +08; 49s ago
     Docs: man:cupsd(8)
 Main PID: 789 (code=exited, status=0/SUCCESS)

Jan 03 16:34:25 ubuntu systemd[1]: Started CUPS Scheduler.
Jan 03 16:45:09 ubuntu systemd[1]: Stopping CUPS Scheduler...
Jan 03 16:45:09 ubuntu systemd[1]: Stopped CUPS Scheduler.
lines 1-9/9 (END)
```

Figure 294 Disabled service CUPS displayed

6.2.11- Active Directory

Setting Group Policy for Windows Server 2012

1) To set our first group policy, open the Group Policy Management tool on the Server Manager.

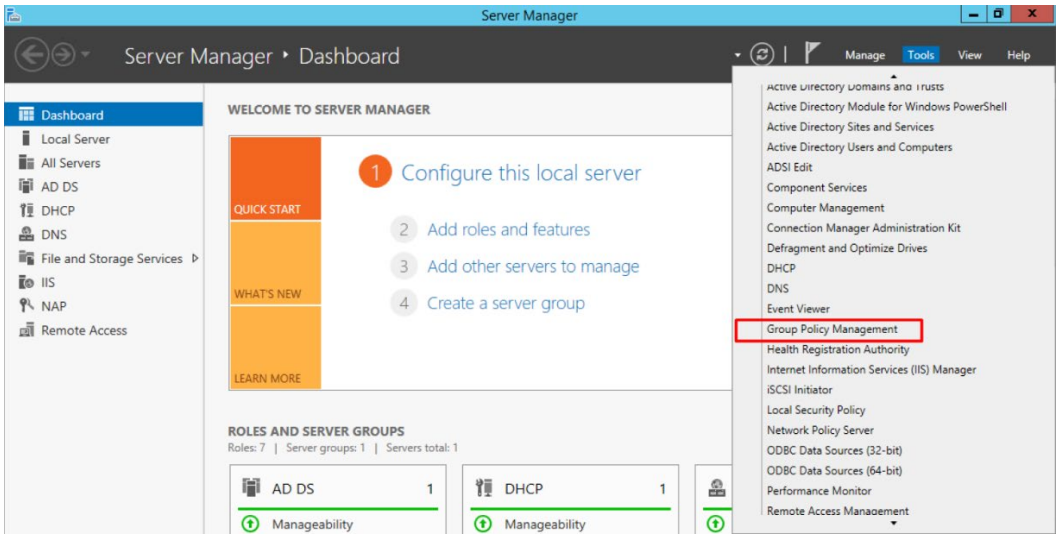

Figure 295 Group Policy Manager under Tools

2) Navigate to Group Policy Object and click edit on Default Domain Policy

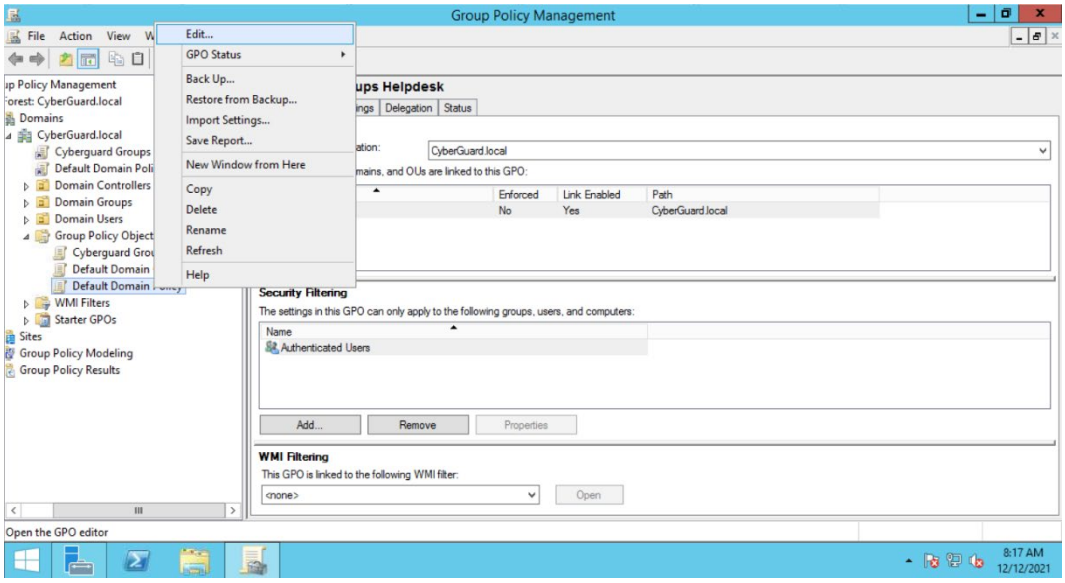

Figure 296 Group Policy Management Window

3) Navigate to Security Settings and click on Account Lockout Policy

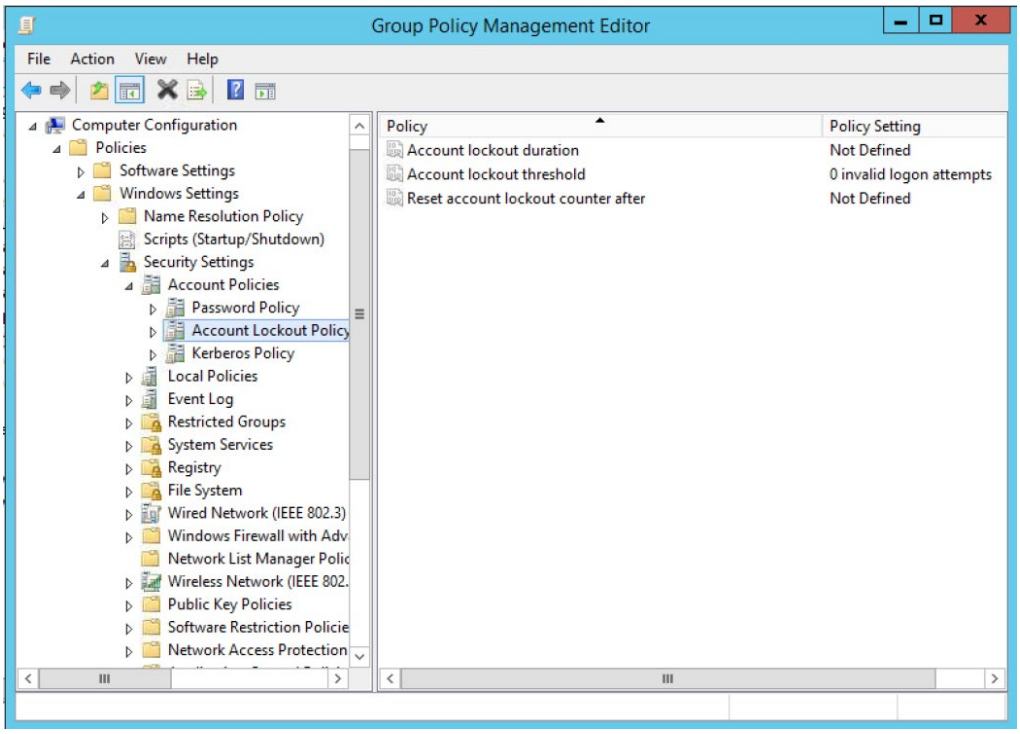

Figure 297 Group Policy Management Editor

4) Double click the Account Lockout Threshold and click the Define this policy setting. Set the account lock out after 5 invalid logon attempts.

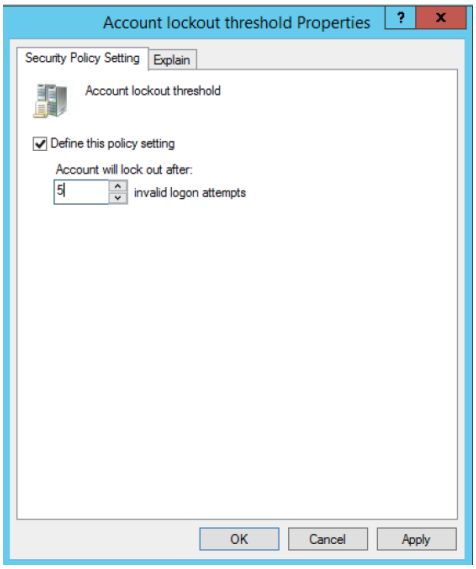

Figure 298 Setting Account Lockout Threshold

5) When the Suggested Value Changes pop up, select ok

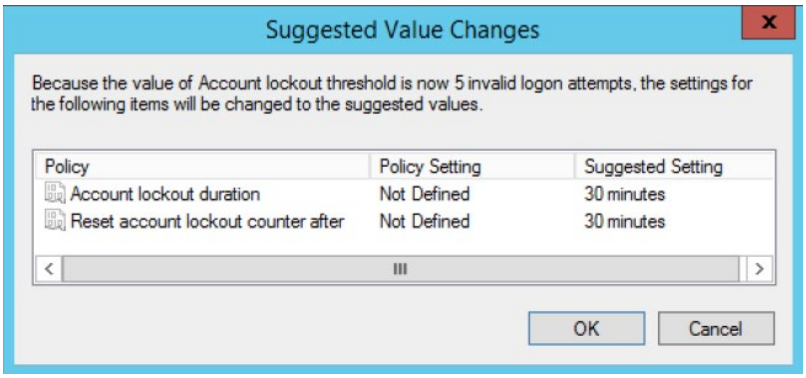

Figure 299 Suggested Value Changes

6) Next, adjusts the Account Lockout Duration setting to lock out account for 2 minutes.

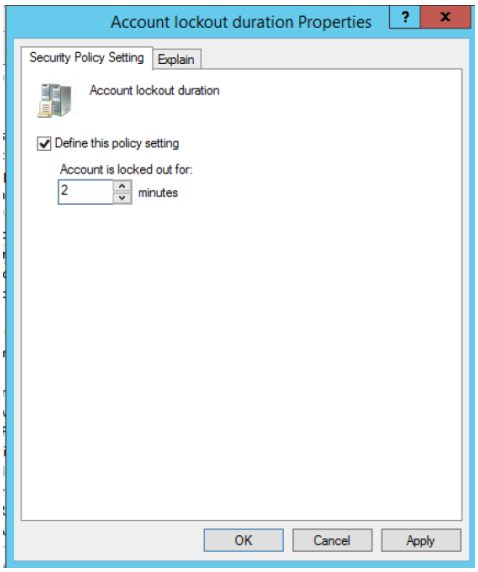

Figure 300 Account Lockout Duration

7) Next, adjust the Reset Account Lockout Counter after 2 minutes.

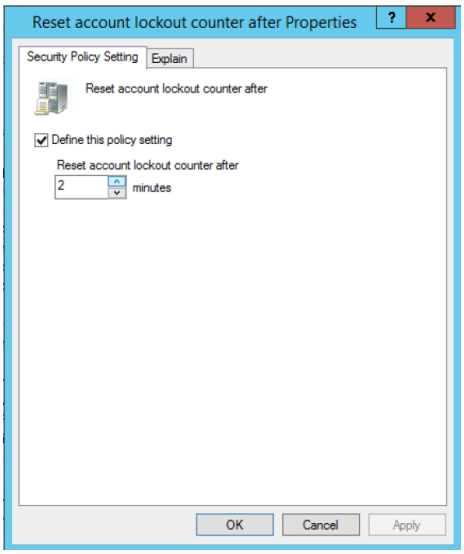

Figure 301 Reset Account Lockout Counter

8) Our first Group Policy has been created, we can check the report of the policies on the settings tab

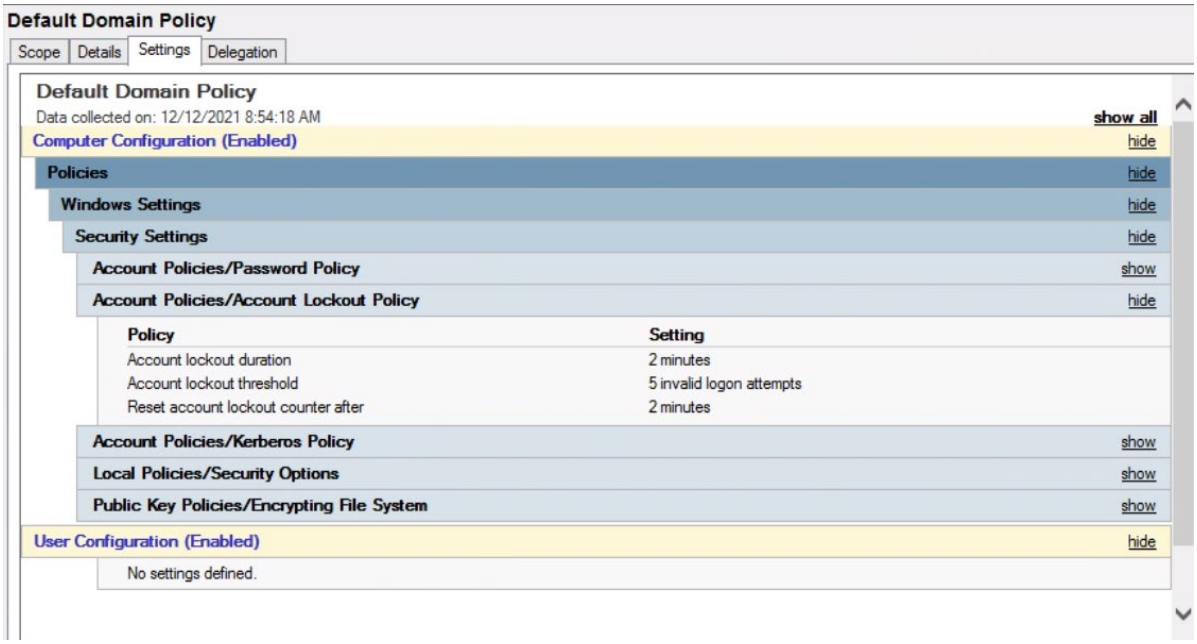

Figure 302 Default Domain Policy Report

9) To create our second Group Policy, right-click on our domain name and click Create a GPO in this domain

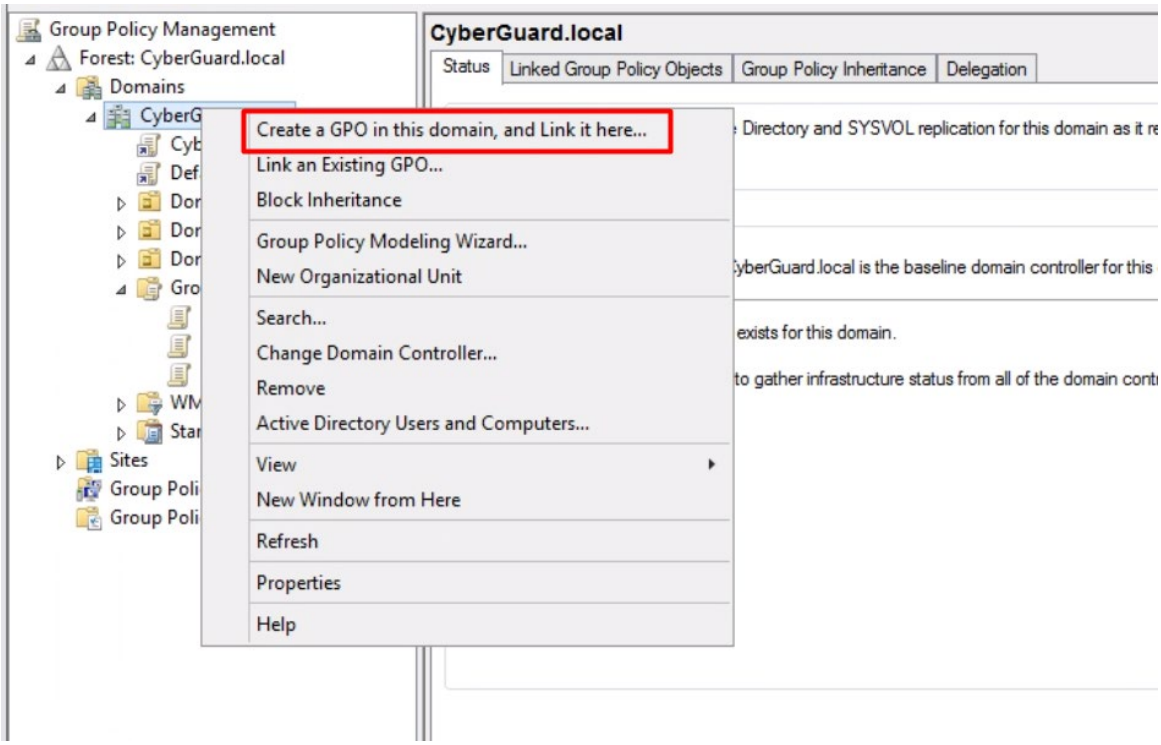

Figure 303 Creating a GPO in domain

10) Name our new GPO as Cyberguard Logon Banner

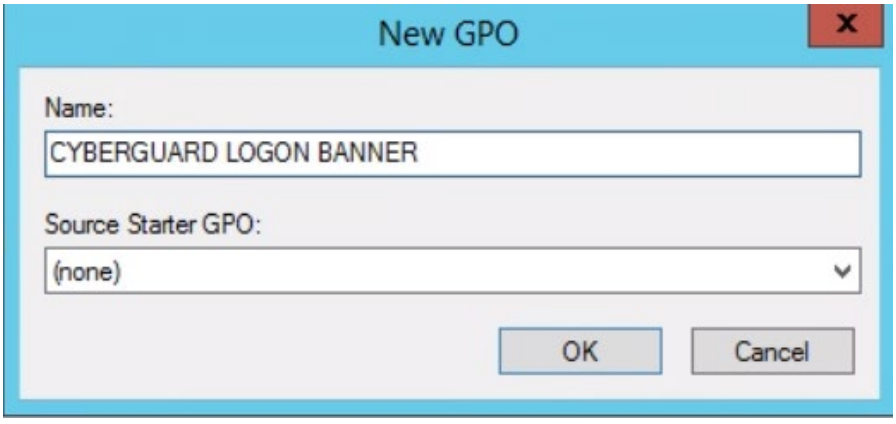

Figure 304 Naming New GPO

11) Right-click the created GPO and click edit

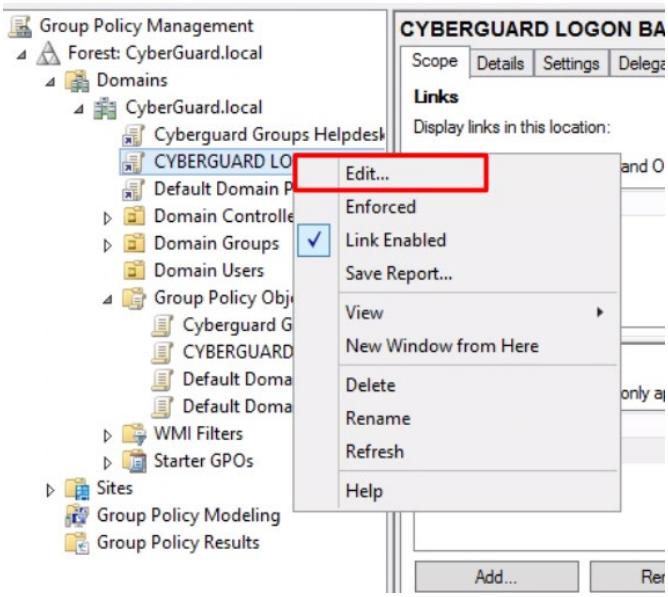

Figure 305 Editing new GPO

12) Navigate to Local Policies, then Security Options, then scroll down to Interactive Logon section.

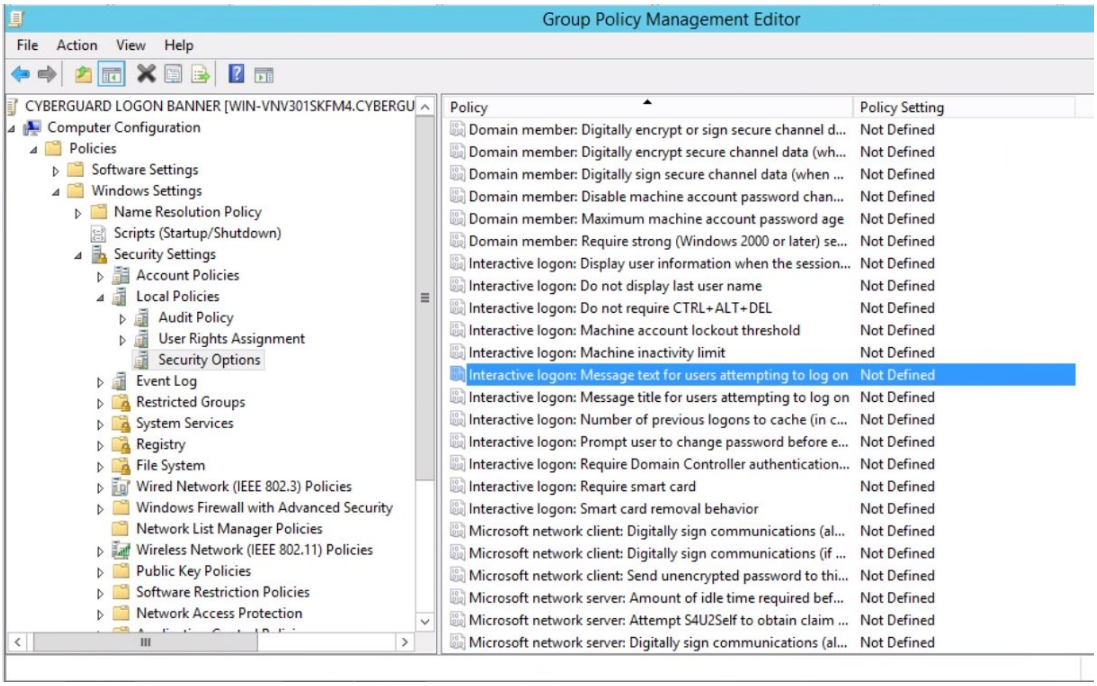

Figure 306 Security Options

13) Double click the Interactive Logon: Message text and define the policy setting that will show when user attempting to logon

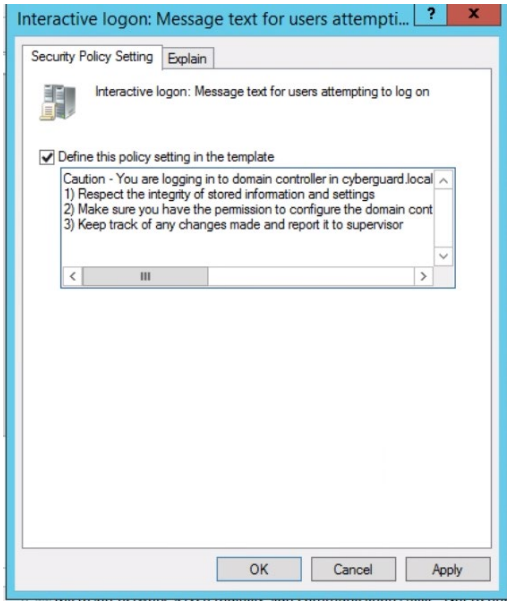

Figure 307 Defining Interactive Logon Text

14) Next, double click the Interactive Logon: Message title and define the policy setting too

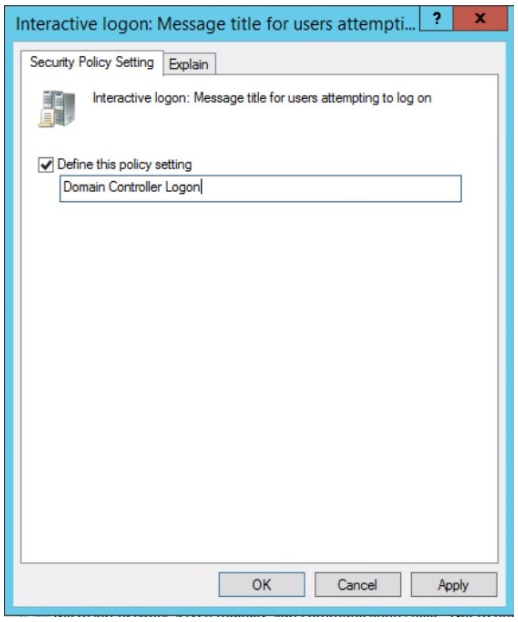

Figure 308 Defining Interactive Logon Title

15) Our second Group Policy has been configured and will be shown when user attempting to logon

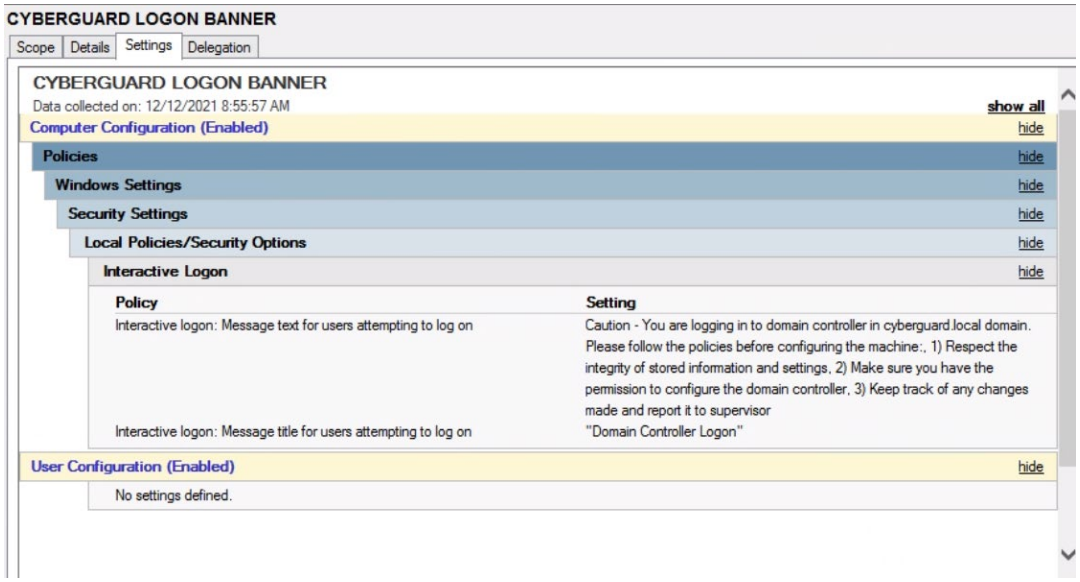

Figure 309 Cyberguard Logon Banner Report

Figure 310 Interactive Logon Banner before Login

6.2.12- IDS with Port Mirroring and Qradar

1) Reload systemctl daemon.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo systemctl daemon-reload
```

Figure 311 Reload Daemon

2) Snort can then be run with the configuration that has been set up by using the start command.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo systemctl start snort
```

Figure 312 Start the snort to run Snort

3) Check the status of the Snort by using the command below.

```
admin0@ubuntu:~/snort_src/snort-2.9.19$ sudo systemctl status snort
● snort.service - Snort NIDS Daemon
   Loaded: loaded (/lib/systemd/system/snort.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-12-19 22:13:42 PST; 4h 0min ago
 Main PID: 3131 (snort)
   CGroup: /system.slice/snort.service
           └─3131 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

Dec 19 22:13:42 ubuntu systemd[1]: Started Snort NIDS Daemon.
Dec 20 02:14:07 ubuntu systemd[1]: Started Snort NIDS Daemon.
admin0@ubuntu:~/snort_src/snort-2.9.19$
```

Figure 313 Status of Snort service

4) Start Snort –A console option to print the alerts.

```
ws Server 2012 | Ubuntu 64-bit (Server) | Ubuntu 64-bit (User) | Windows 10 Local Client | Windows 10 Client
@ubuntu: ~
Reload thread starting...
Reload thread started, thread 0x7f276a146700 (2346)
Decoding Ethernet

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.19 GRE (Build 85)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''    Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.38 2015-11-23
           Using ZLIB version: 1.2.8

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Commencing packet processing (pid=2344)
```

Figure 314 Open console and detect alerts

5) Ping Ubuntu Server (10.30.0.11) from Windows Server.

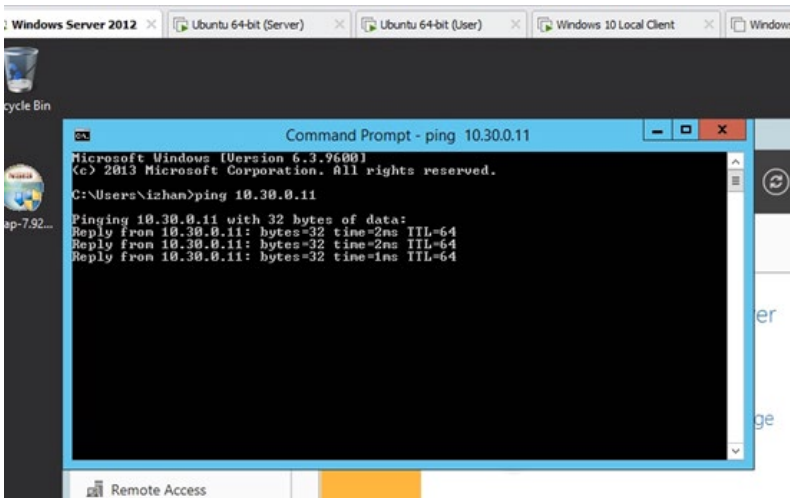

Figure 315 Ping Windows Server

6) Snort detects Windows Server ping to Ubuntu Server and alerts.

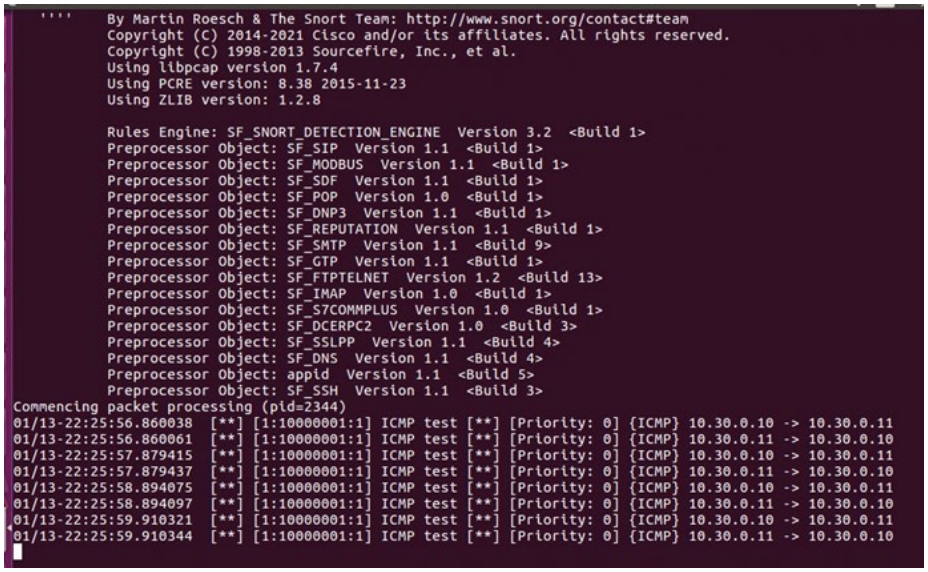

Figure 316 Snort activation

7) Ping Ubuntu Server (10.30.0.11) from Ubuntu User. But make sure Ubuntu User receive IP Address from DHCP Server.

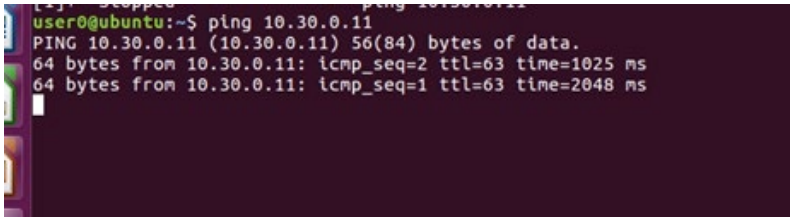

Figure 317 Ping Ubuntu Server from Ubuntu User (HQ client)

8) Do not stop the ping at Ubuntu User and start Snort –A console options to print the alerts.

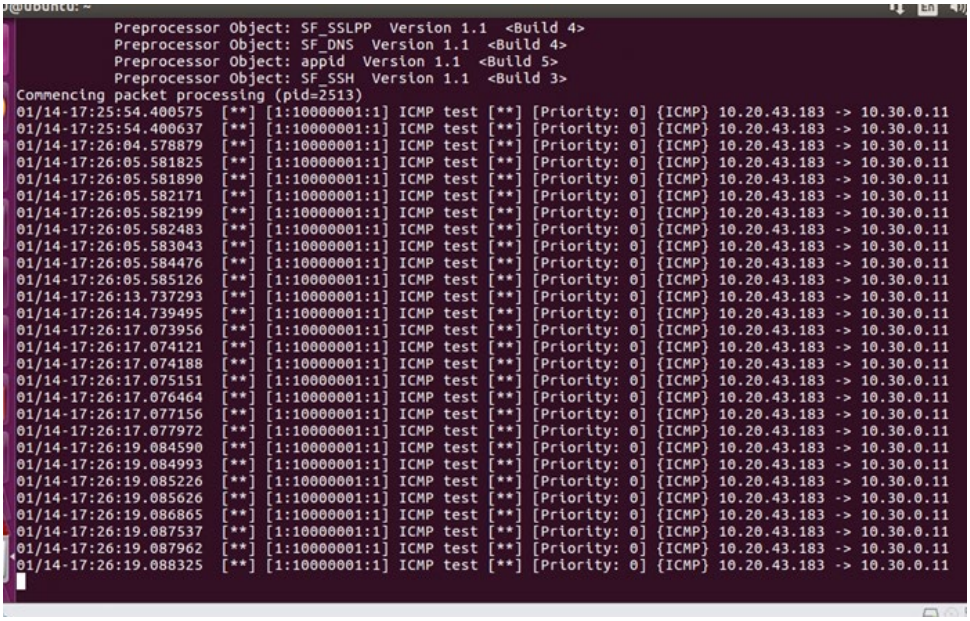

Figure 318 Snort activation

6.2.13- Samba Security

1. Check IP address of Ubuntu Server by using command **ifconfig**. The IP address is **10.30.0.11**

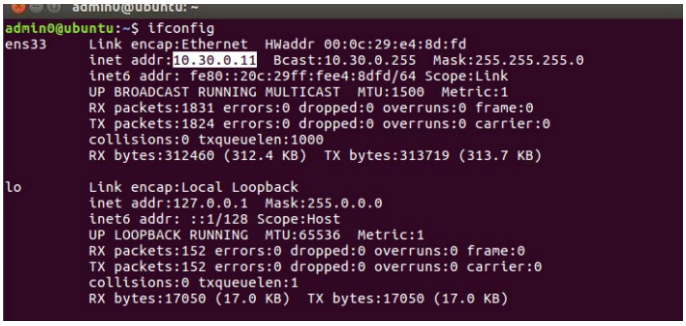

Figure 319 Check IP address of Ubuntu Server

2. Access samba file from **Windows Server** using users **OtherG7**

   i. Go to **Start** and type **Run**, enter **\\10.30.0.11** and click **OK**.

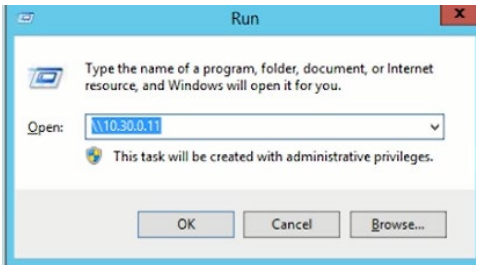

Figure 320 Access samba from Windows Server

   ii. We need to enter the username and password that have been registered, and we will log in as OtherG7.

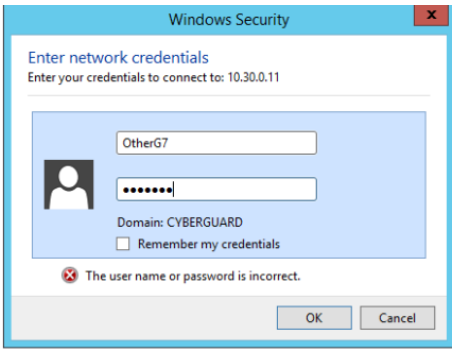

Figure 321 Login using OtherG7

iii. The folder CyberGuard can be accessed by a user named OtherG7

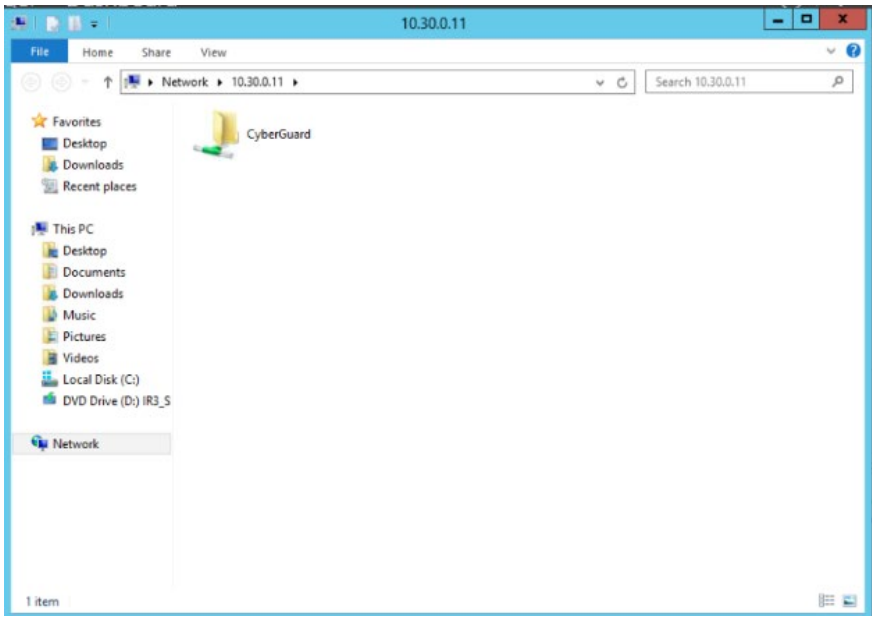

Figure 322 OtherG7 accessing CyberGuard folder

iv. Open the CyberGuard folder, and there is file name Private and Public

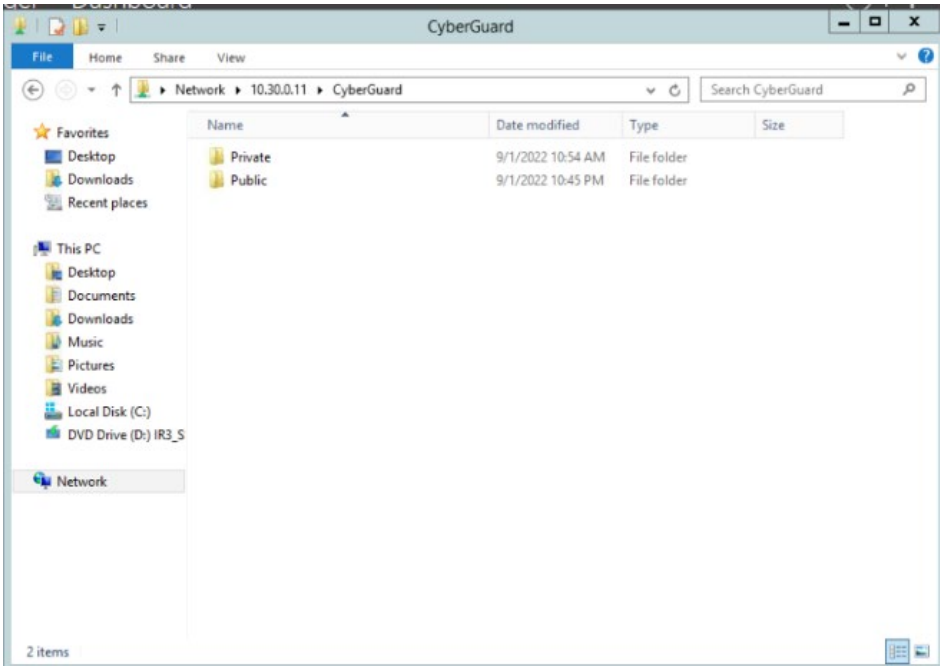

Figure 323 OtherG7 open CyberGuard folder and see folder named Private and Public

v. Try to access the Private file. The file cannot be accessed by user OtherG7.

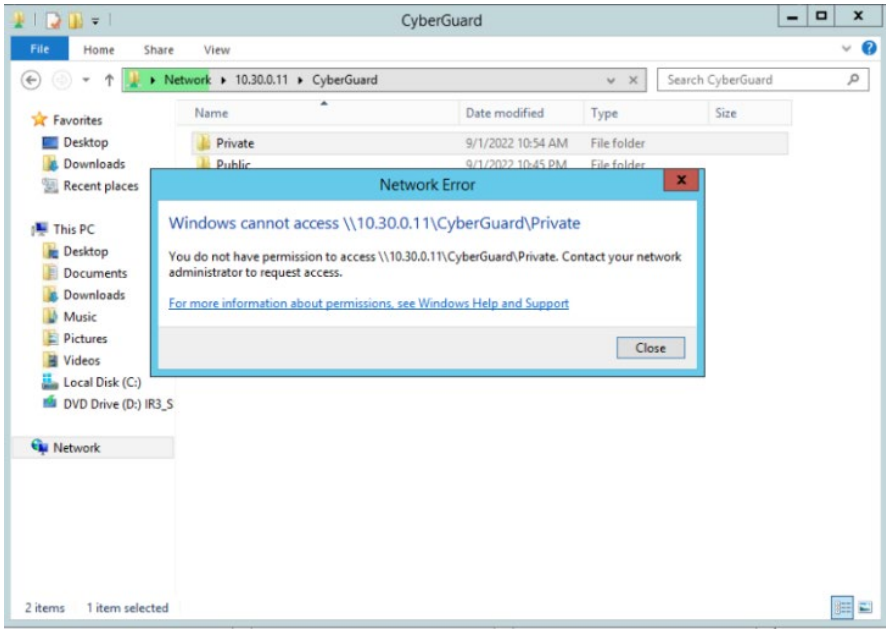

Figure 324 OtherG7 cannot access Private folder

vi. Try to access the **Public** file. The file can be accessed and, in the file, have the text file name g7.txt.

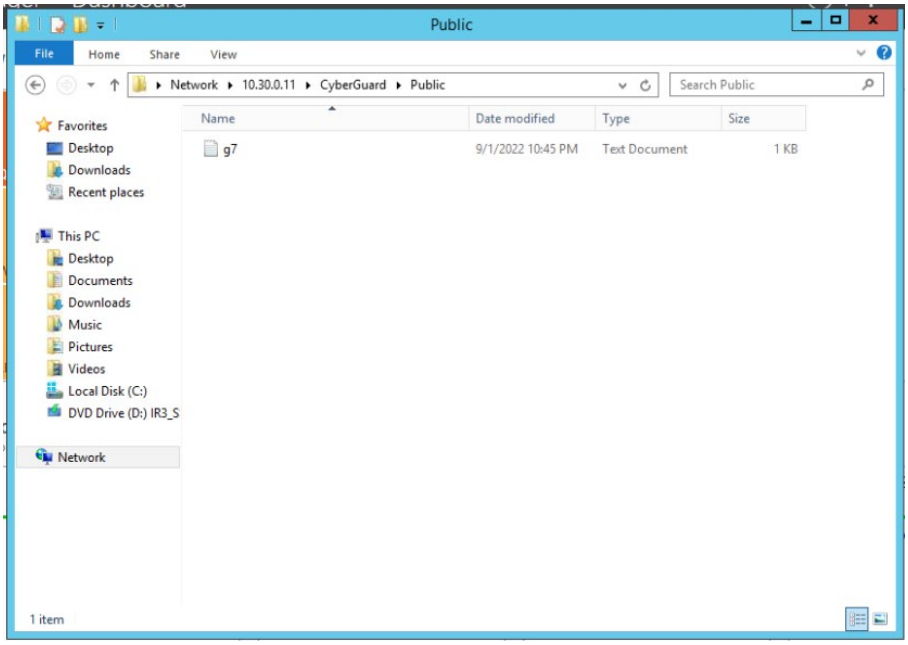

Figure 325 OtherG7 can access Public folder

vii. Try to add a new file in the Public folder. User OtherG7 cannot add a file.

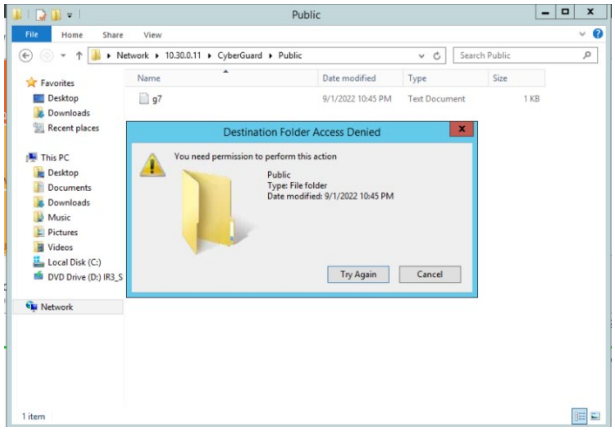

Figure 326 OtherG7 cannot add file

viii. Try to open file g7.txt. The file can be open but cannot be edited by user OtherG7.

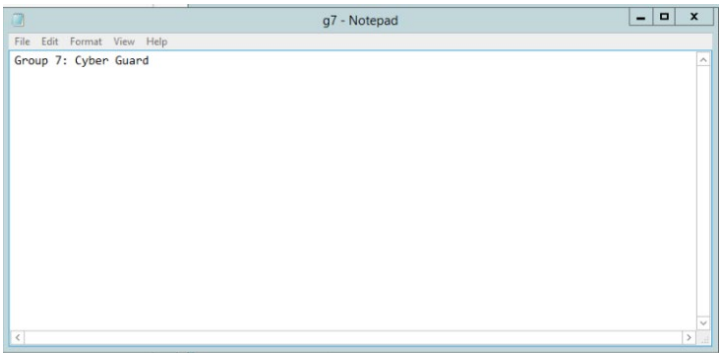

Figure 327 OtherG7 try to edit text file and save

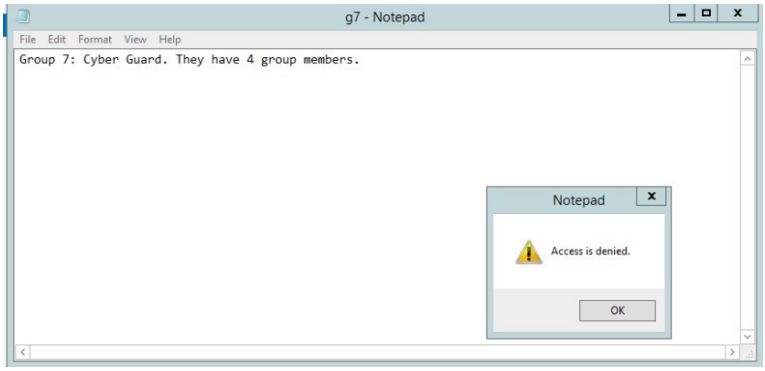

Figure 328 OtherG7 cannot edit a text file

3. Access samba file from **Ubuntu user** using users **UserG7**

   i. Go to **Home,** click **Connect to Server**, enter **smb://10.30.0.11/** and click **Connect**.

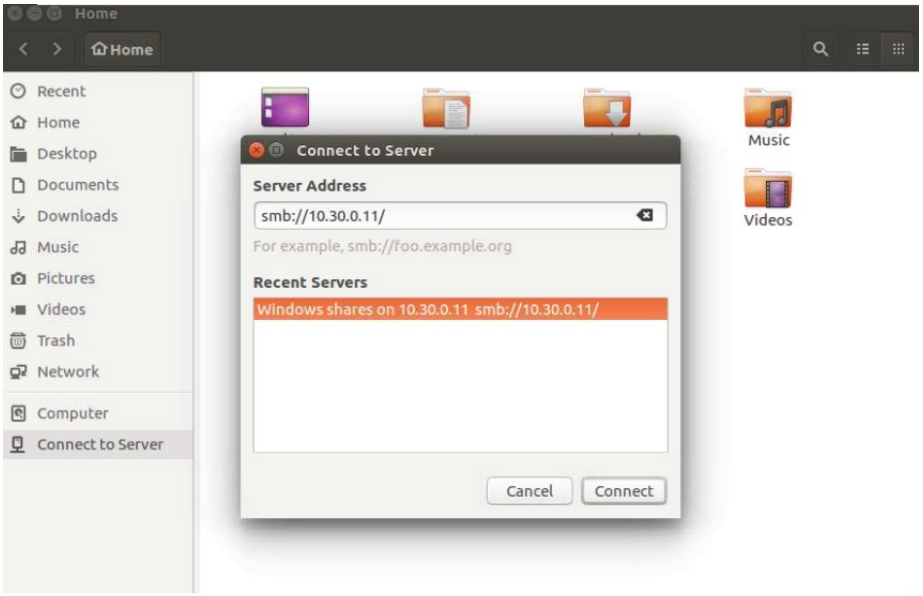

Figure 329 Access samba from Ubuntu user

   ii. We need to enter the username and password that have been registered, and we will log in as UserG7.

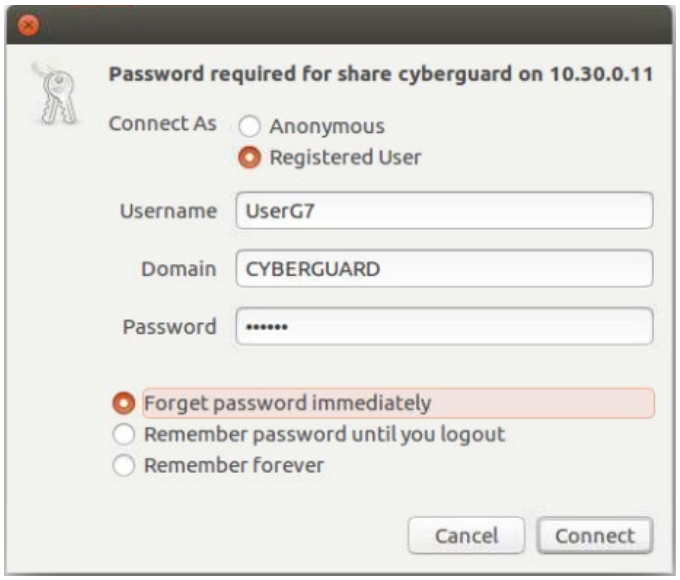

Figure 330 Login using UserG7

iii. The folder CyberGuard can be accessed by user UserG7, and there is file name Private and Public

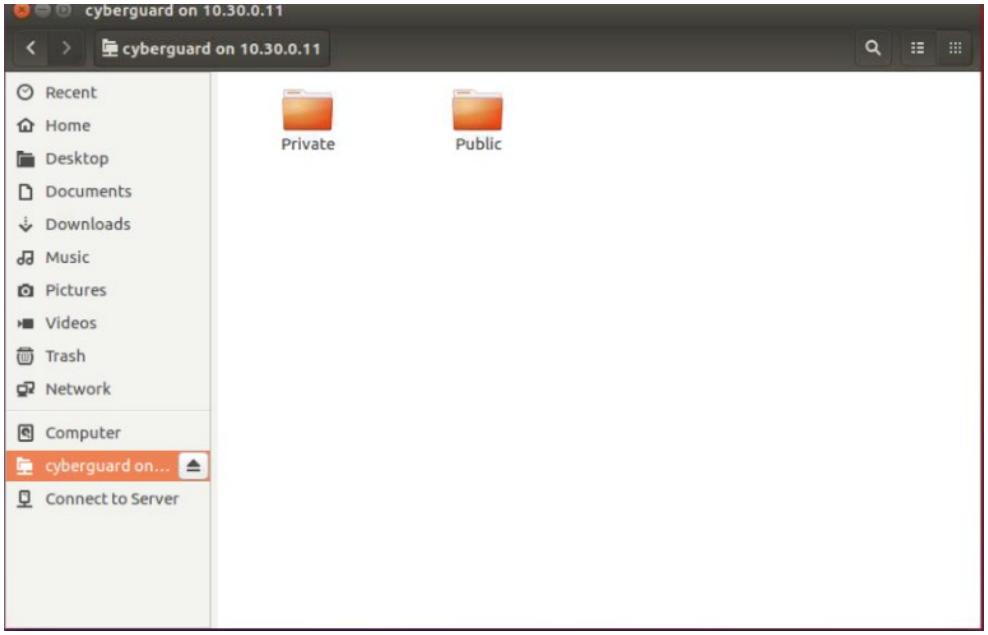

Figure 331 UserG7 can access the CyberGuard folder

iv. Try to access the Private file. The file cannot be accessed by user UserG7.

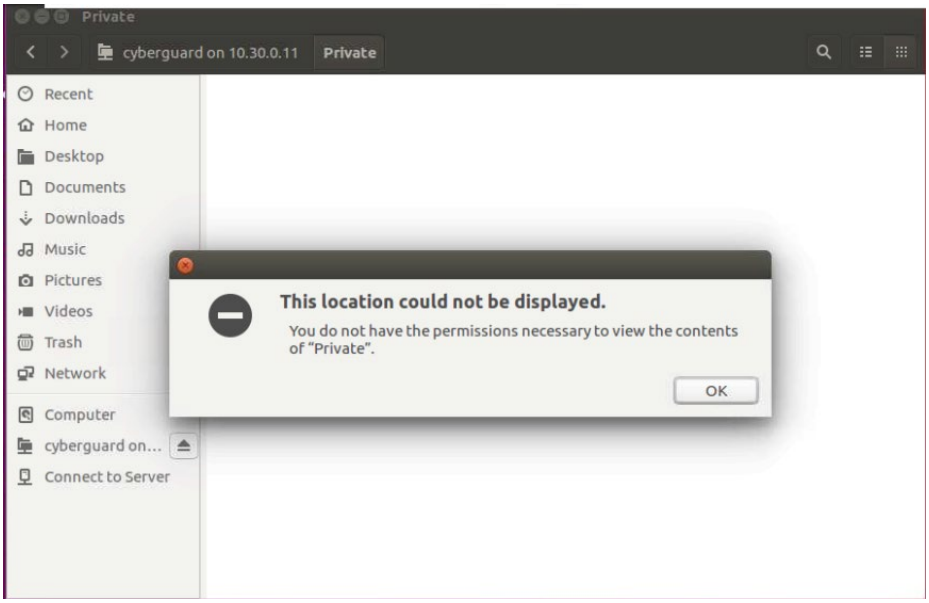

Figure 332 UserG7 cannot access Private file

v. Try to access the **Public** file. The file can be accessed and, in the file, have the text file name g7.txt.

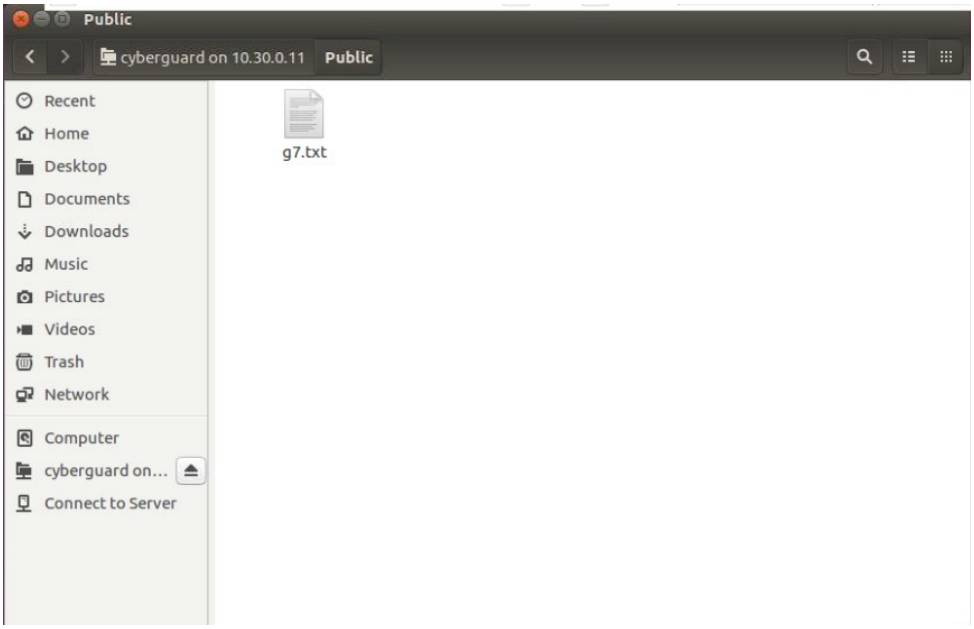

Figure 333 UserG7 can access Public file

vi. Try to add a new file in the Public folder. UserG7 can add the file. The new file name TestUserG7

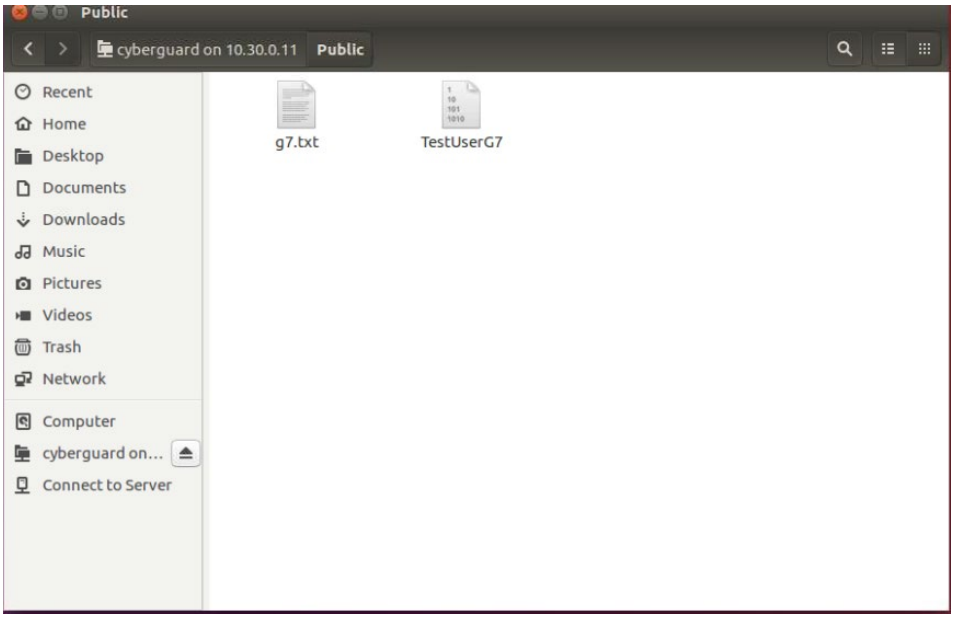

Figure 334 UserG7 can create new file

vii. Try to open file g7.txt. The file can be open and can be edited by user UserG7.

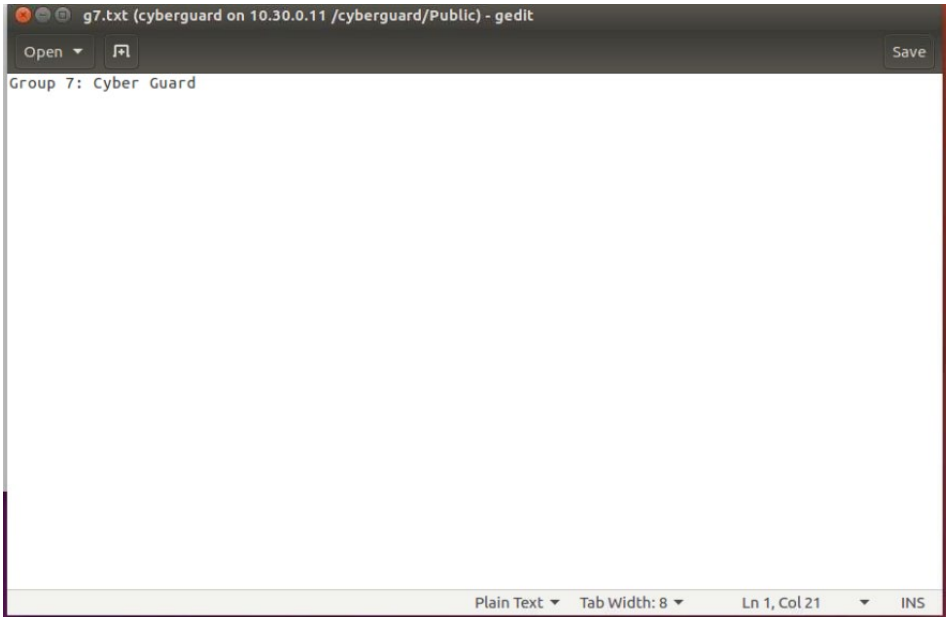

Figure 335 UserG7 try to edit the text file

viii. The file g7.txt that has been edited and saved is shown below.

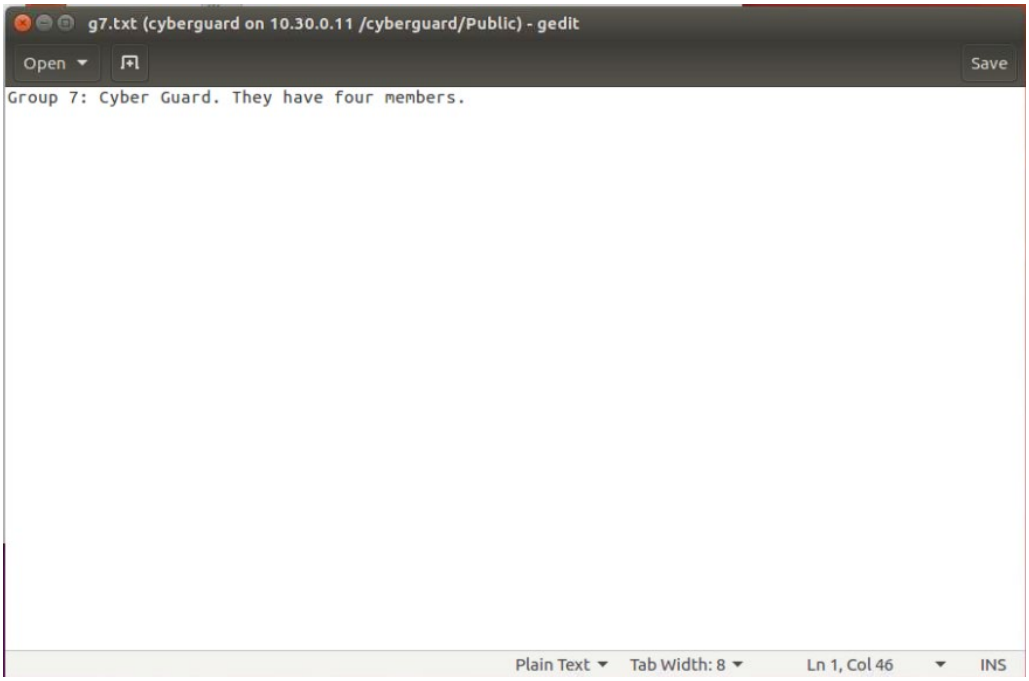

Figure 336 UserG7 can save the edited text file

4. Access samba file from **Windows 10 Client** using users **AdminG7**

   i. Go to **Start** and type **Run**, enter **\\10.30.0.11** and click **OK**.

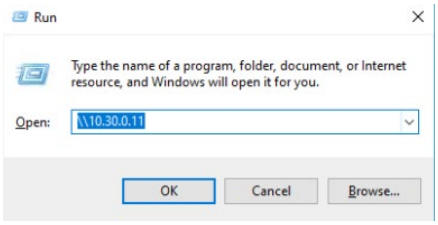

Figure 337 Access samba using Windows 10 Client

   ii. We need to enter username and password that have been registered and we will log in as AdminG7.

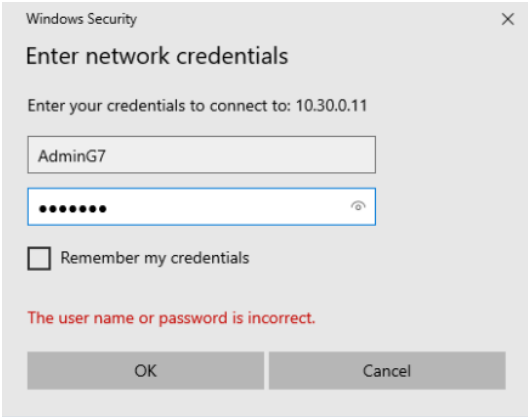

Figure 338 Login using AdminG7

   iii. The folder CyberGuard can be accessed by user AdminG7, and there is file name Private and Public

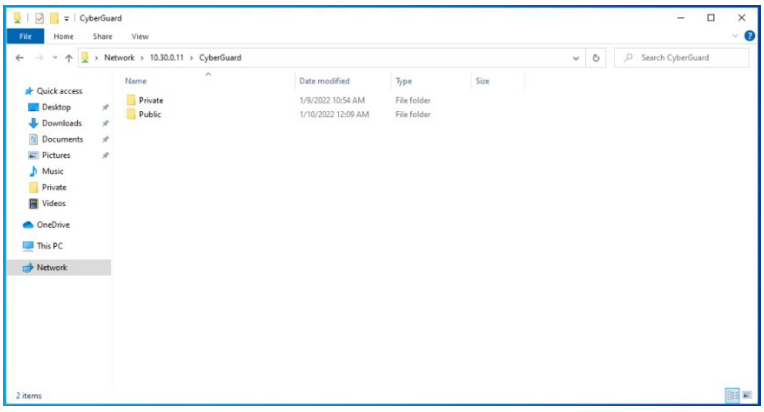

Figure 339 AdminG7 can access CyberGuard folder

iv. Try to access the Private file. AdminG7 can access the file, and there is a text file named Secure.txt.

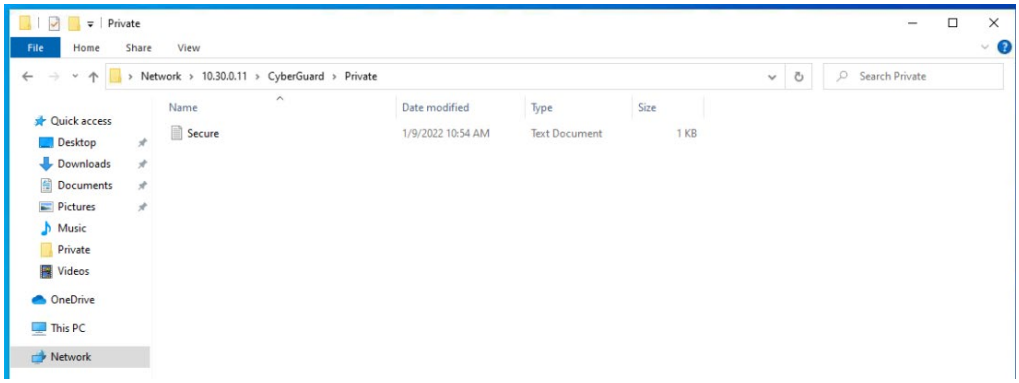

Figure 340 AdminG7 can access Private file

v. Try to add a new file named Test. AdminG7 can add the file in the Private folder.

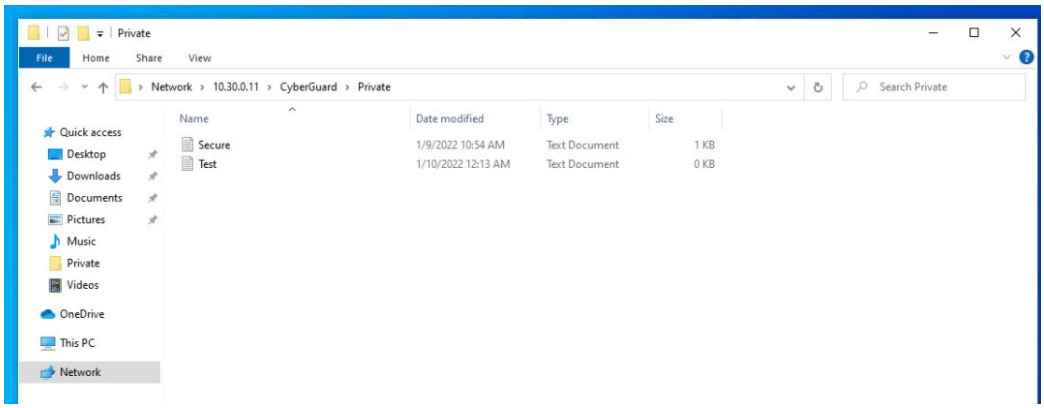

Figure 341 AdminG7 can create a new file

vi. Try to edit the Secure.txt file.

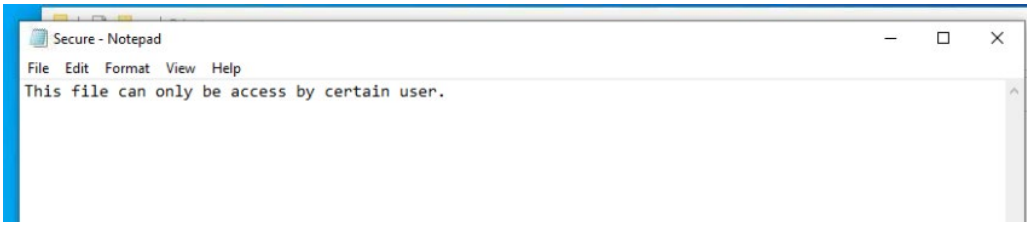

Figure 342 AdminG7 try to edit text file

vii. AdminG7 can edit and save Secure.txt file

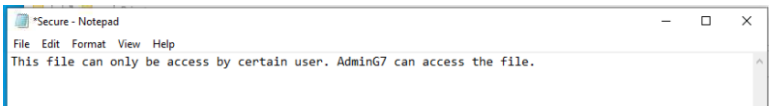

Figure 343 AdminG7 can edit the text file in Private folder

viii. Try to access the **Public** file. The file can be accessed and, in the file, have text file name g7.txt. and TestUserG7 that has been added by user name UserG7.

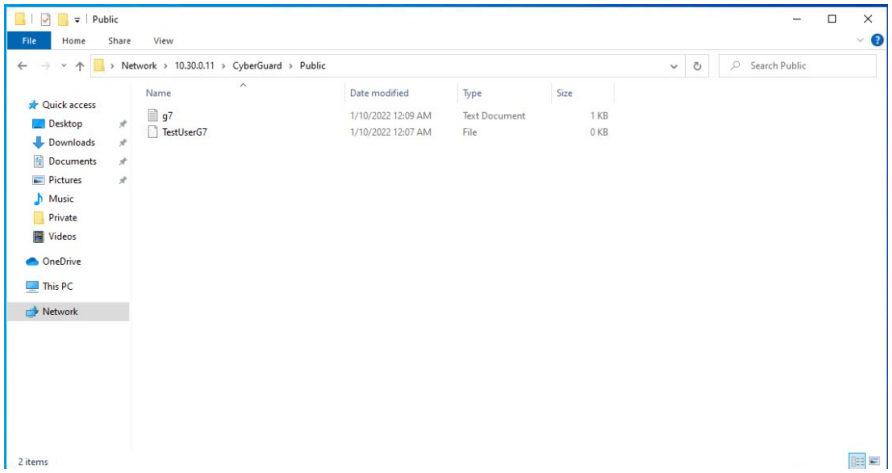

Figure 344 AdminG7 can access Public folder

ix. Try to add a new file in the Public folder. AdminG7 can add the file. The new file name TestAdminG7

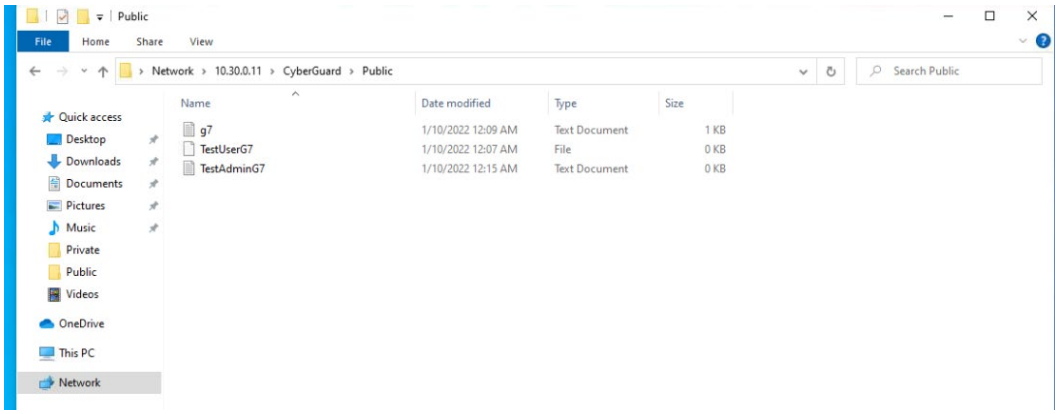

Figure 345 AdminG7 can create new file in Public folder

x. Try to open file g7.txt. The file can be open a user named AdminG7.

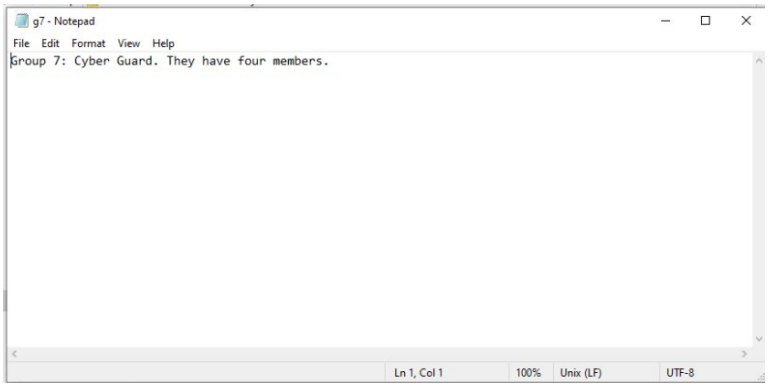

Figure 346 AdminG7 try to edit a text file in Public folder

xi. The file g7.txt cannot be edited by a user named AdminG7.

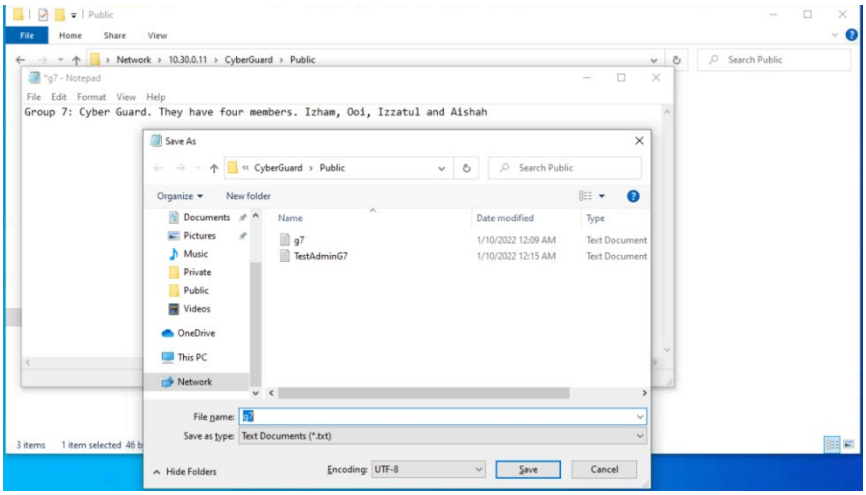

Figure 347 AdminG7 try to save the edited file

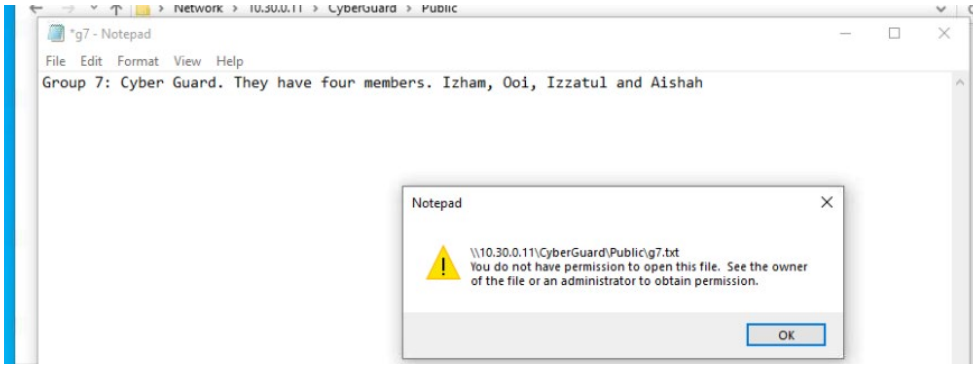

Figure 348 AdminG7 cannot save the edited file

5. The Public file has been edited by other users from the user's view named UserG7.

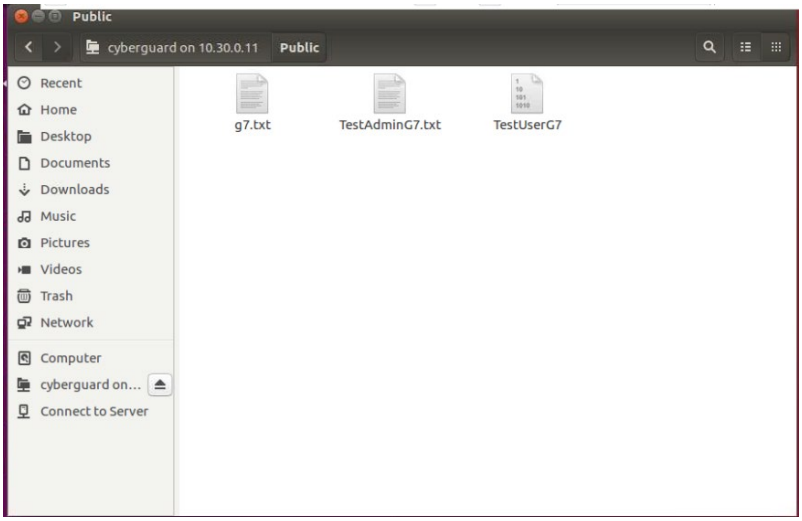

Figure 349 View from UserG7 after AdminG7 make changes

6. The Public file has been edited by another user from the view of a user named OtherG7.

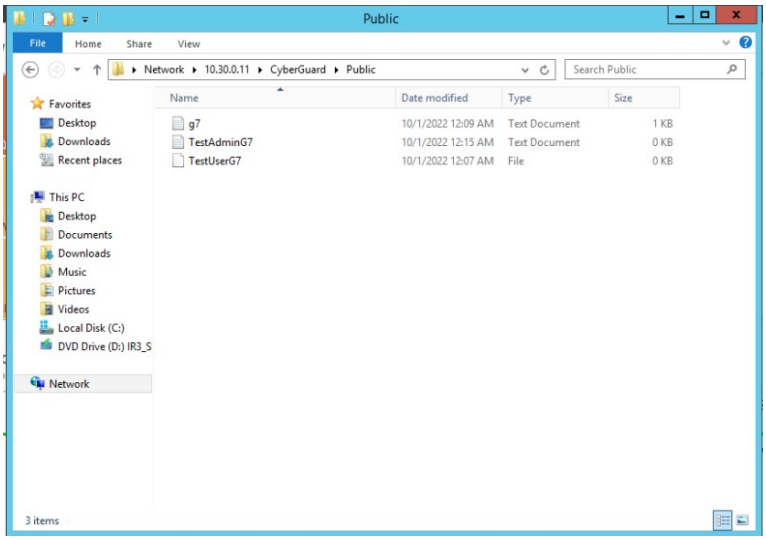

Figure 350 View from OtherG7 after AdminG7 and UserG7 make changes

6.2.14- FTP Server

1) To connect to the FTP server from other devices, download and install other FTP client software such as FileZilla, then enter the appropriate credentials to access the server files.

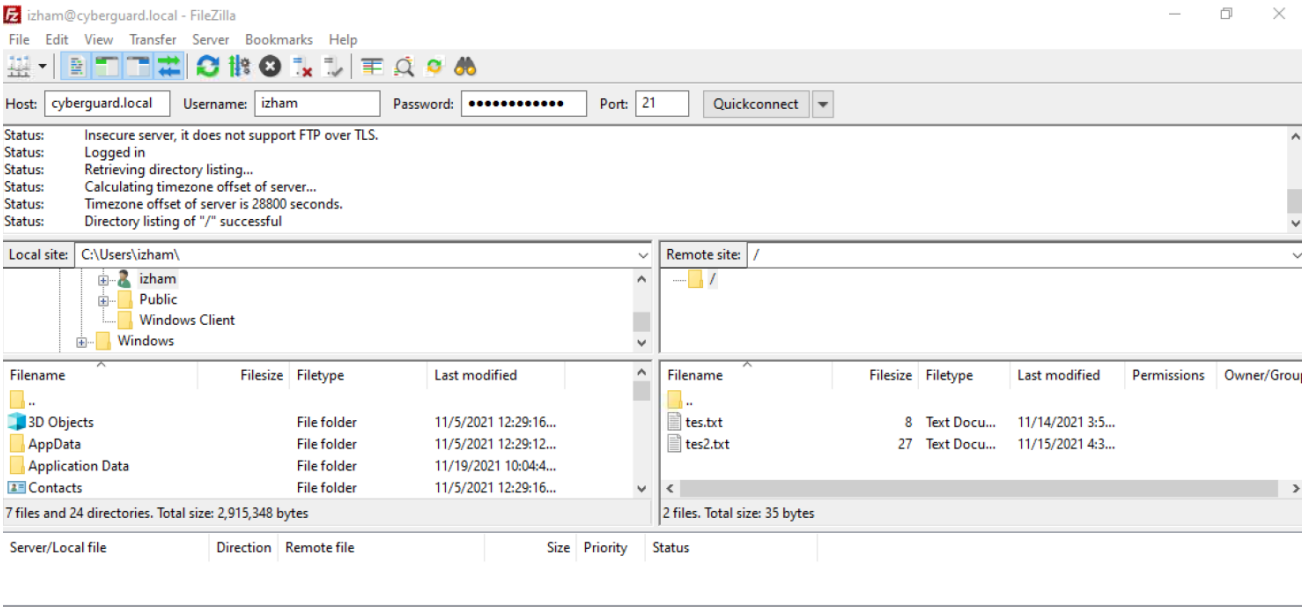

Figure 351 Filezilla on Windows client

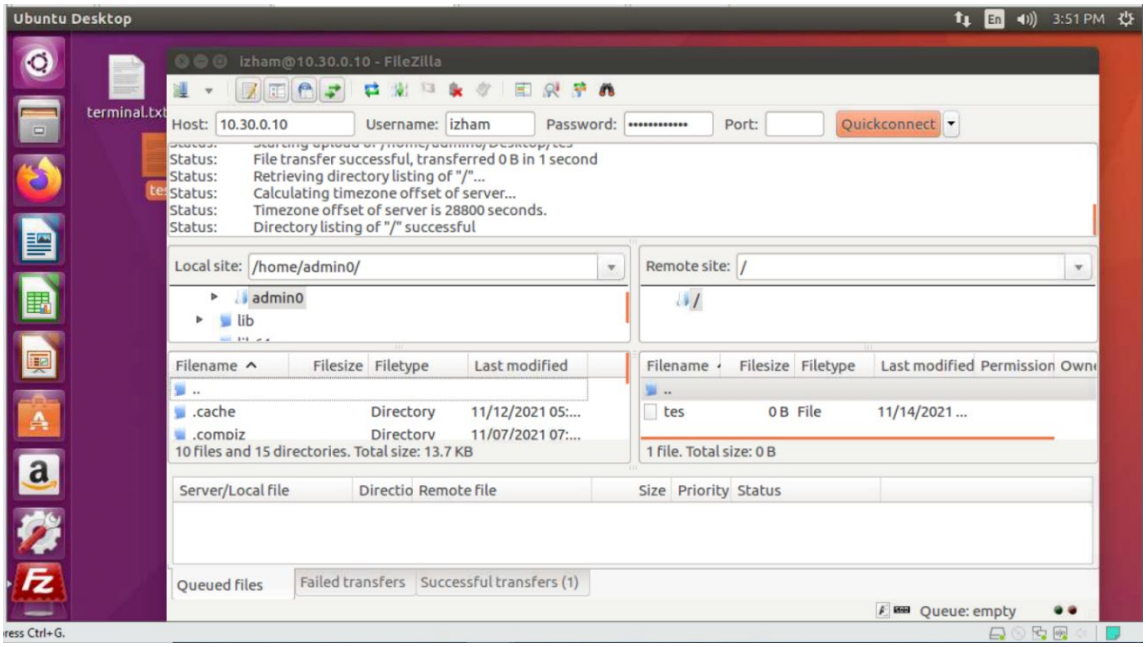

Figure 352 Filezilla on Linux Client

6.3- Extra Services Testing

6.3.1- EtherChannel

1) Verify the EtherChannel's port channel created.

```
HQ-CS-01#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)          -        Et0/0(D)    Et0/1(D)
```

Figure 353 Show EtherChannel summary output

6.3.2- Dynamic NAT (NAT Overload)

1) Verifying NAT overload operation with show commands.

   #show ip nat statistics

```
HQ-RT-01#sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet1/2.10, Ethernet1/2.20, Ethernet1/2.30, Ethernet1/2.40
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT interface Ethernet0/0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Figure 354 Show ip nat statistics output

6.3.3- IPsec Point-To-Point VPN

1) Establishing and verifying the ipsec vpn tunnel and encrypted packets.

#show crypto isakmp sa

```
HQ-RT-01#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.100.2   209.165.100.1   QM_IDLE           1001 ACTIVE
```

Figure 355 Show crypto isakmp session output

#show crypto ipsec sa

```
HQ-RT-01#show crypto ipsec sa

interface: Ethernet1/3
    Crypto map tag: IPSEC-MAP, local addr 209.165.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (20.0.0.0/255.0.0.0/0/0)
   current_peer 209.165.100.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

Figure 356 Show crypto IPsec session output

6.4- Conclusion

Testing is the process of making objective judgments about how well a system device meets, exceeds, or falls short of stated goals. A good testing program will enable administrators to identify issues and make changes to improve performance. In addition, testing is required for risk evaluation. As a result, all services will be subjected to testing.

CHAPTER 7: CONCLUSION

7.1- Introduction

Workshop 2 act as a platform for students to prepare the technical part for the final year project and industrial training, especially in the future. Through Workshop 2, we learned many things, including network setup, service configuration, troubleshooting, and problem-solving. We apply all the subjects learnt in previous semesters in Workshop 2 to implement the project and solve the problem or error. It is an excellent opportunity for students to gain real-world experience, practice, and apply information from previously learned disciplines. Students can also learn from their failures and how to address challenges.

The group leader leads the group well. Starting from the beginning of Workshop 2, the planning, implementation and testing phase, we discuss together if we have a problem. Tasks have been distributed for each group member to make sure everyone is involved in this project. As a result, planning and management are critical to ensuring that tasks are done on time and that the danger of a problem is minimized. Even though some issues arise during the project implementation, everything is completed successfully within the time frame.

The Workshop 2 project services include DHCP, DNS, FTP, and many more, the essential network services and important elements in a network. This Workshop 2 project is suitable for small organisations because it is easy to manage and implement. The summary, we are grateful for the opportunities to learn and grow. This subject has provided us with the knowledge to assist us, especially in industrial training soon.

7.2- Project Advantages

There are a lot of benefits of doing Workshop 2, such as:

- Gain knowledge on how to design a secure network infrastructure.
- Gain knowledge on how to set up the network successfully.
- Gain knowledge on how to install and configure the services given.
- Gain knowledge on how to use different operating systems.
- Gain knowledge on how to troubleshoot problems and errors.
- Gain knowledge on maintaining the network so that it has no bugs.
- Gain knowledge on how to tolerate each other in groups.
- Gain knowledge on how to work in the real environment of network security.

7.3- Project Disadvantages

Even though there are a lot of benefits, there are some lacks in the project, such as:

- Group members do not know or lack knowledge about some of the services.
- Some command cannot be used in the different versions of the same operating system.
- The time we need to complete this project is longer than expected.
- We cannot refer to many references for some of the services.

7.4- Project Limitation

Because of some limitations in this project, we must work hard to succeed. The limitations are:

- Not suitable to implement more extensive and more complex network design.
- The connection between the VNC server and VNC client sometimes is not very good.

7.5- Conclusion

Workshop 2 provided a good platform for students to experience a real work atmosphere and real hands-on activities that they could not learn in class. During the completion of Workshop 2, students should be able to set up, install, configure, test, maintain, monitor, and troubleshoot their own network infrastructure under various conditions. More network security information is gained as a result of this.

Design, installation, configuration, testing, monitoring, and maintenance are needed to complete the project. We may also apply the subjects that have been taken in the previous semester to complete the project successfully, such as Network Security Infrastructure and Design, Cyber Law, Computer Networking, Operating System, and others.

Thus, the Workshop 2 and 12 network services have been completed on time with the cooperation from each group member, guidance from the supervisor, and other lecturers.

APPENDIX

Windows Server Hardening Checklist

Server Information

IP Address:	10.30.0.10
Machine Name:	Windows Server 2012 R2
Asset Tag:	VM1
Check by:	Siti Aishah binti Mustaffa
Date:	17 January 2022

Checklist

Step	To Do	Status
Preparation and Installation		
1.	Install Nmap scanning tools to scan for open ports	/
Updates and Patches		
2.	Install the latest updates for Windows	/
3.	Enable automatic notification of patch availability	/
User Account Policies		
4.	Enforce password history	/
5.	Set maximum password age	/
6.	Set minimum password age	/
7.	Set minimum password length	/
8.	Enable password complexity requirements	/
9.	Do not store passwords using reversible encryption	/
10.	Configure account lockout policy	/
Security Settings		
11.	Place the University warning banner in the Message Text for users attempting to log on.	/
12.	Disable the guest account	/

13.	Require Ctrl+Alt+Del for interactive logins	/
Network Security Settings		
14.	Enable the Windows Firewall in all profiles (domain, private, public)	/
15.	Configure the Windows Firewall in all profiles to block inbound traffic by default.	/
Audit Policy Settings		
16.	Configure Account Logon audit policy.	/
17.	Configure Account Management audit policy.	/
18.	Configure Logon/Logoff audit policy.	/
19.	Configure Policy Change audit policy.	/
20.	Configure Privilege Use audit policy.	/
Additional Security Protection		
21.	Disable or uninstall unused services.	/
22.	Disable or delete unused users.	/