Server & Cloud Security

SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Cyber Security & Forensics

Diploma in Information Technology

GROUP ASSIGNMENT

Duration: Weeks 5 -17

Weightage: 20% out of Total 50%

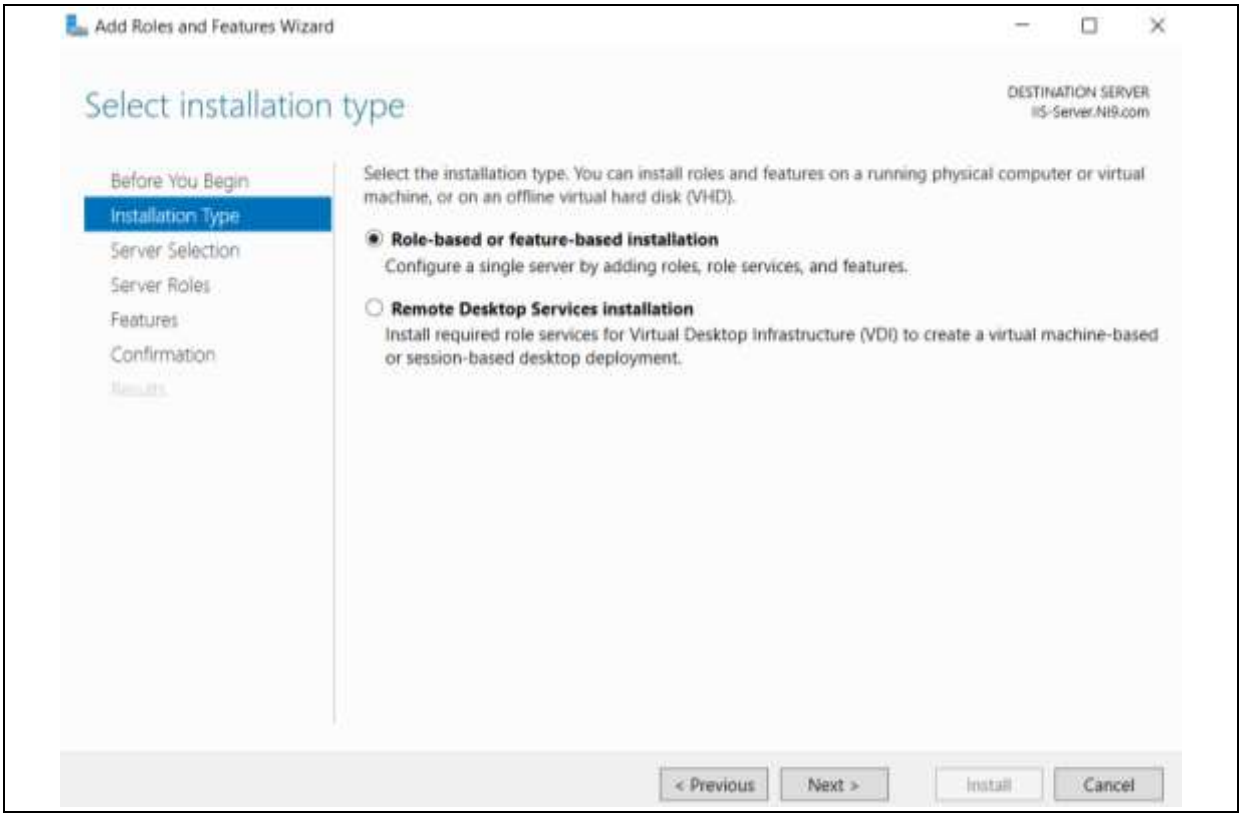
Tutorial Group: T03 Team Number: __ Team Grade: _____

Student Name	Student Number
NG CHIN TIONG RYAN	S10196904C
HANNAH LEONG JIA WEN	S10195094B
EZRA HO JINCHENG	S10194982A
MATTHIAS WEN-ZHONG BRUNO-JEAN MOREL GAN	S10197146D

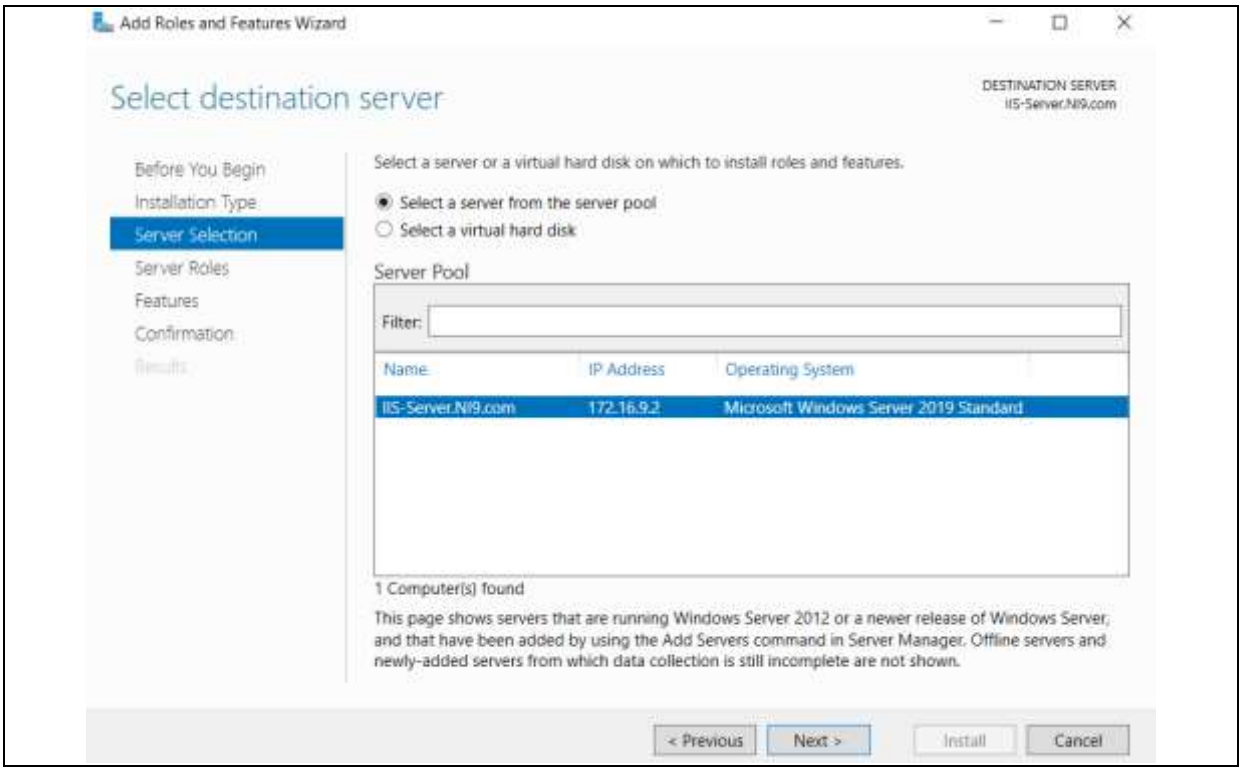
Contents

Installing File Server in Windows Server 2019

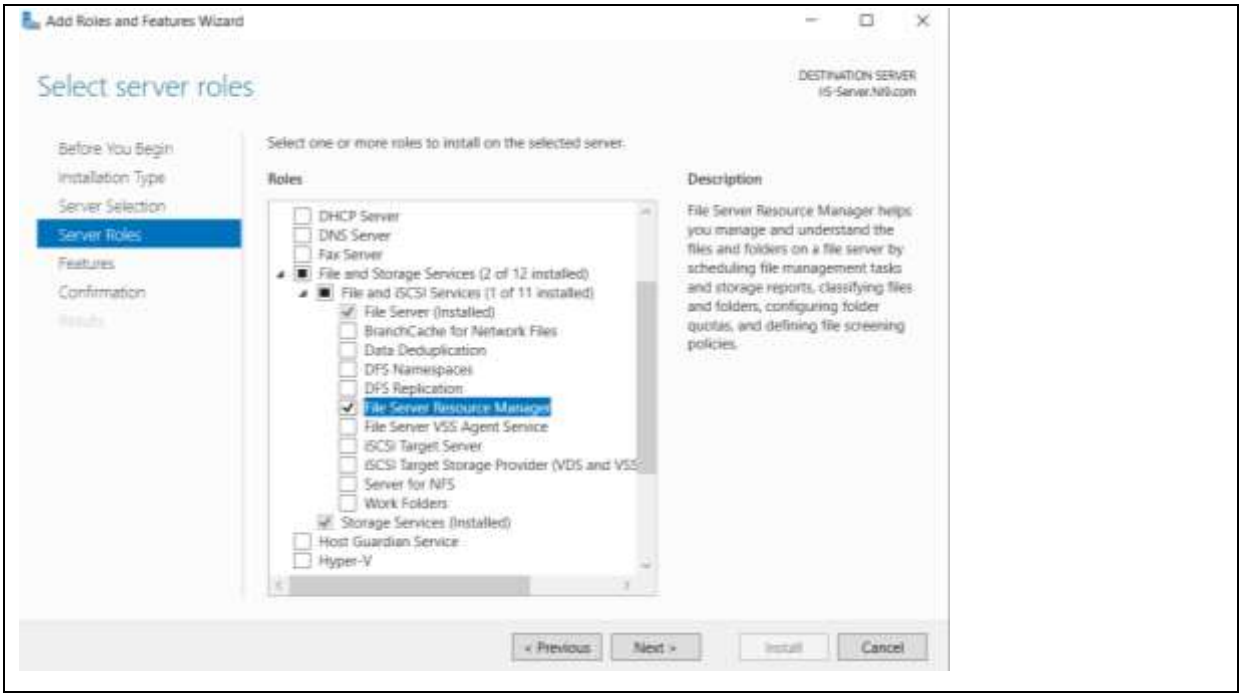
Step 1: Click on “Role-based or feature-based installation” and click “Next >”.



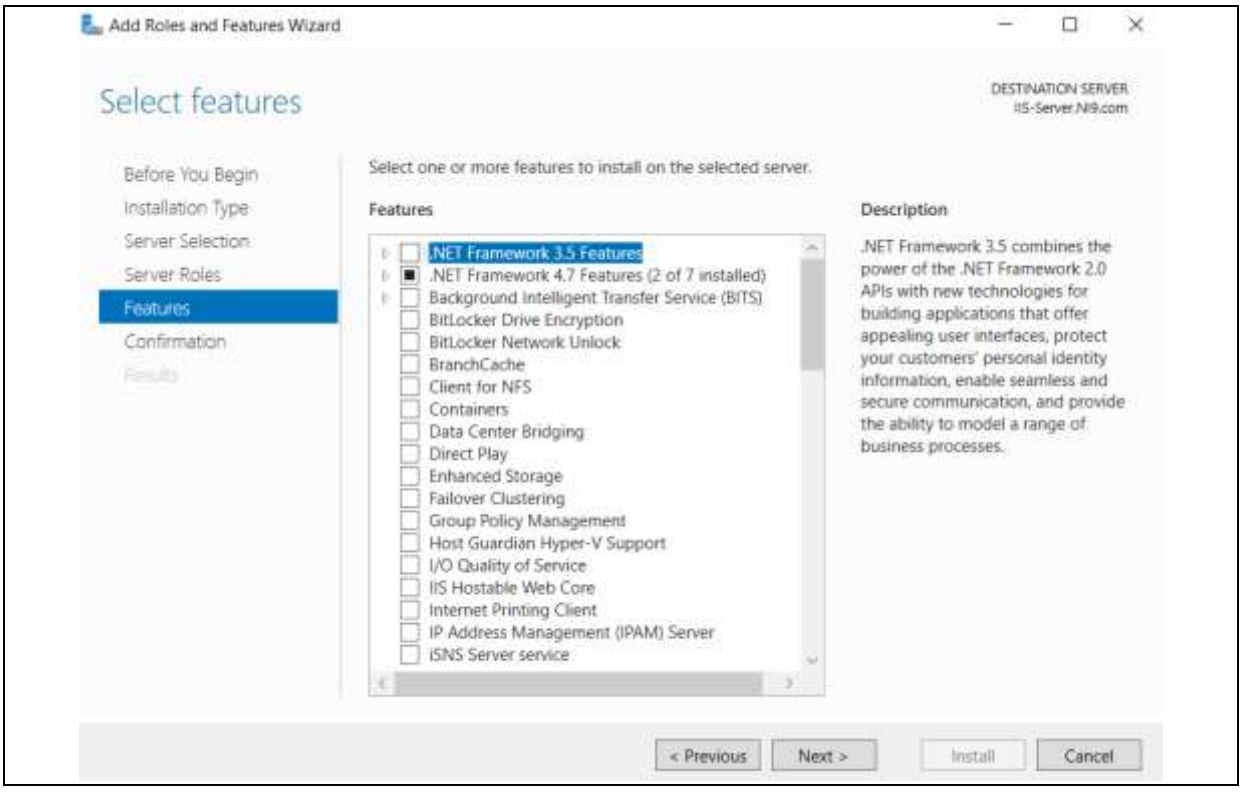
Step 2: Click on “Select a server from the server pool” and click “Next >”.



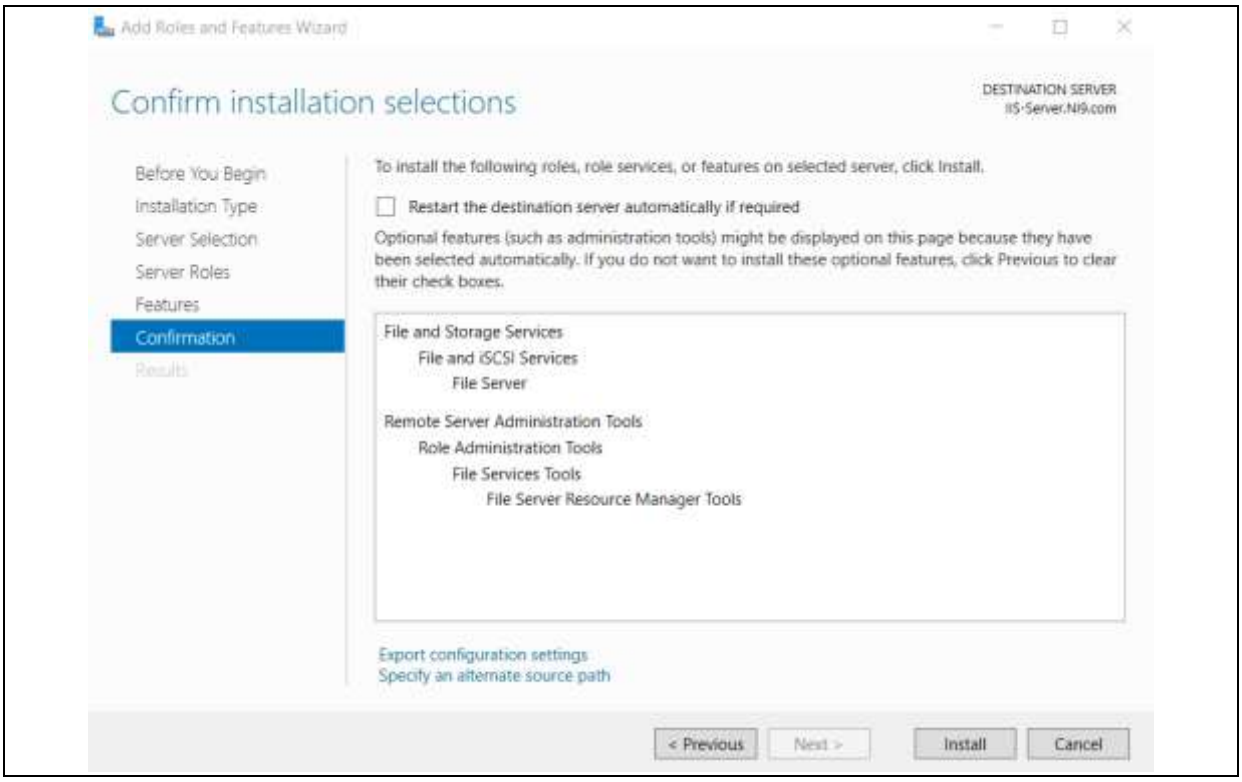
Step 3: Scroll down and click on “File and Storage Services > File and iSCSI Services”. Click on the dropdown options “File Server” and “File Server Resource Manager”. Click “Next >” to continue to the last step of the installation process.



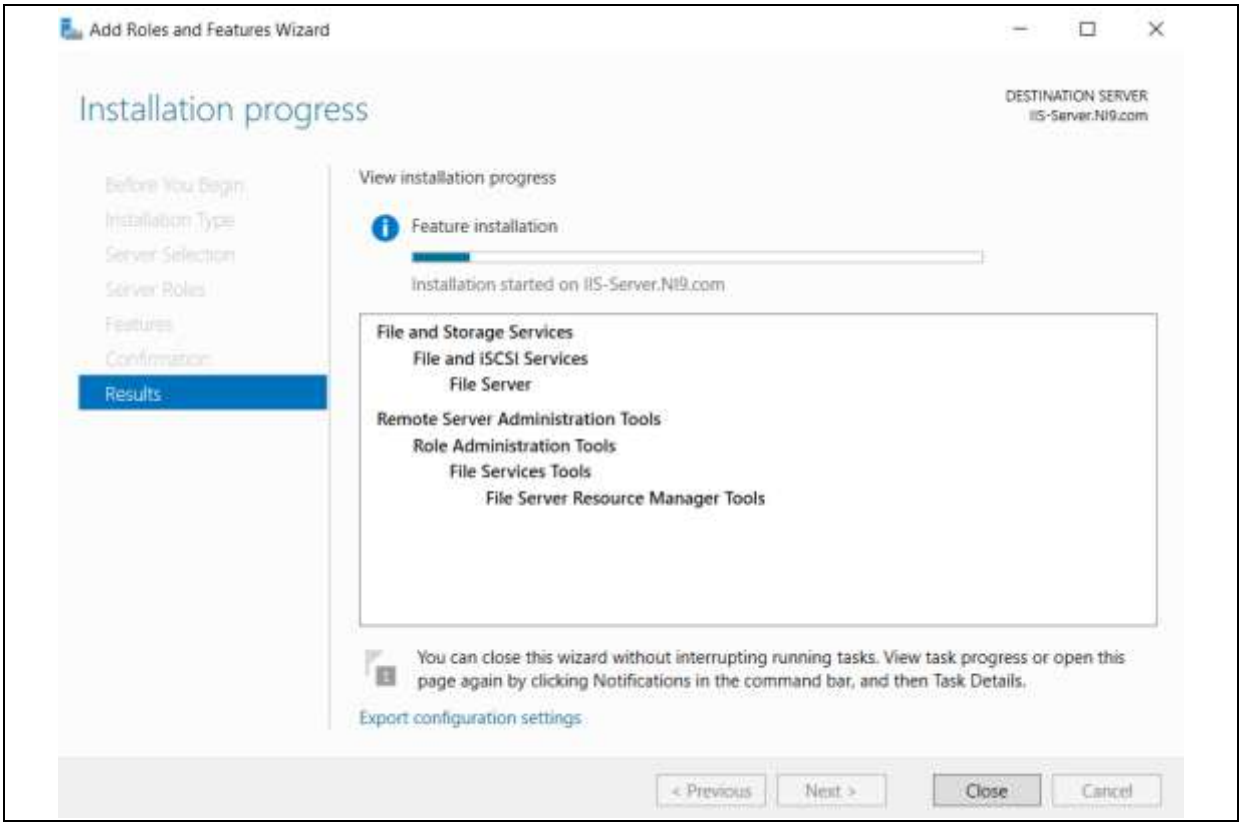
Step 4: Click on “.NET Framework 4.7 Features” and proceed to click “Next >”.



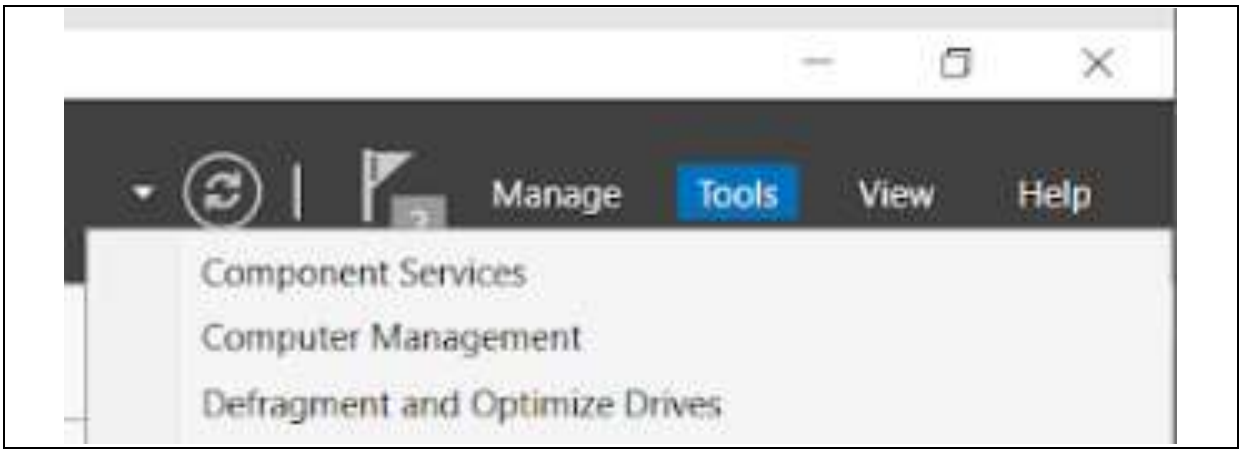
Step 5: Click on “Install”.



Step 6: Please wait for the installation process to be completed before performing other tasks.

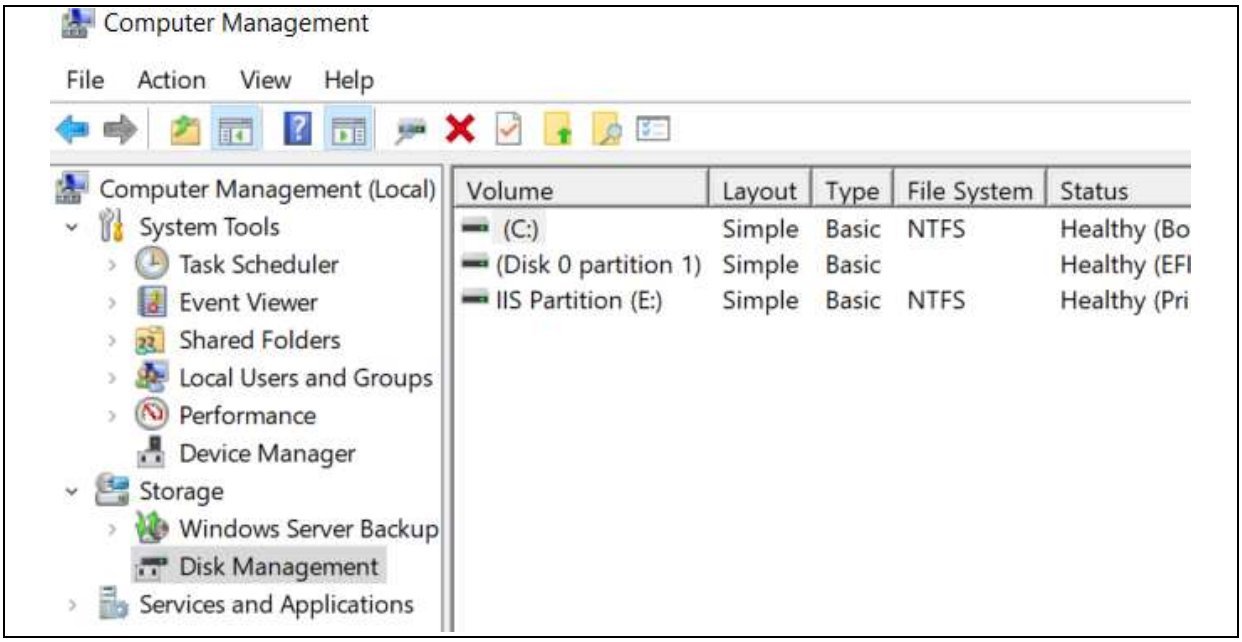


Step 7: Once installation is complete, please go to “Server Manager > File and Storage Services > Shares”. On the top right, please click on “Tools > Computer Management”.

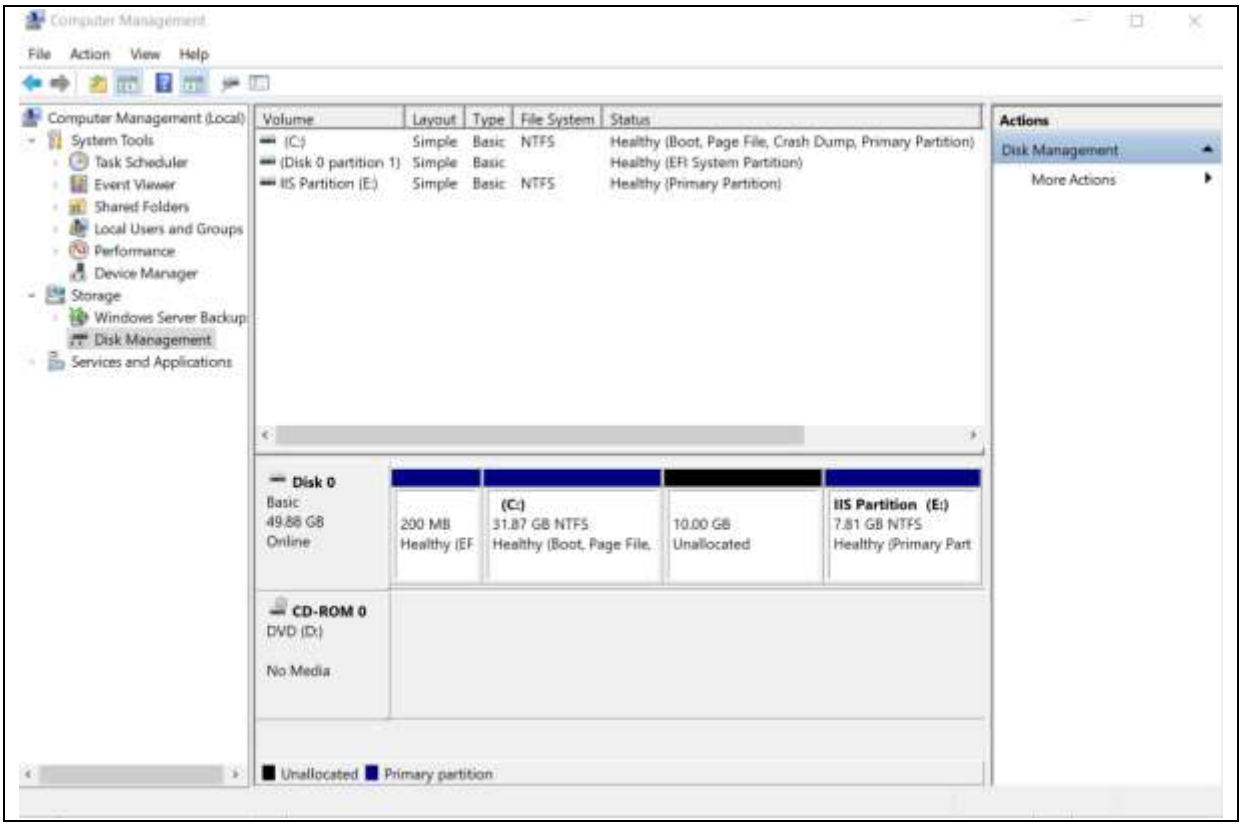


Next, we will be setting up another partition which we will use later on for file sharing. This is to enable a somewhat isolated environment from the boot disk and allows the share folder to be secured later on using the security tools that we will be putting into place.

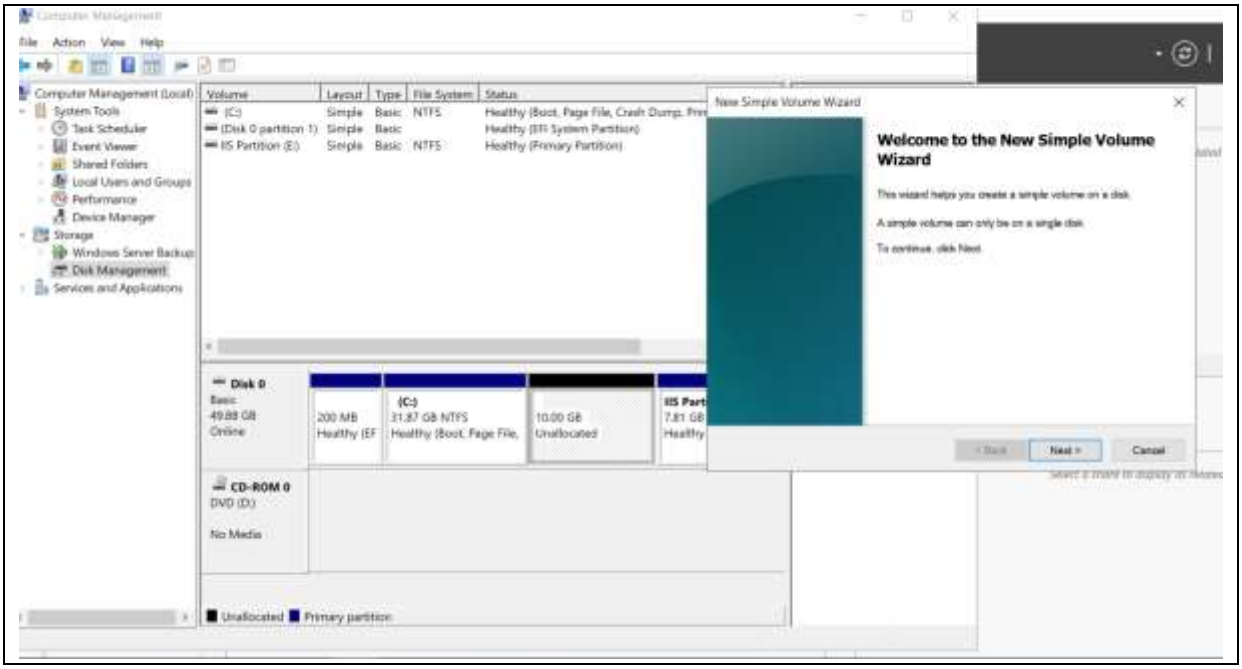
Step 8: Open Disk Management and it will show the disks of the system.



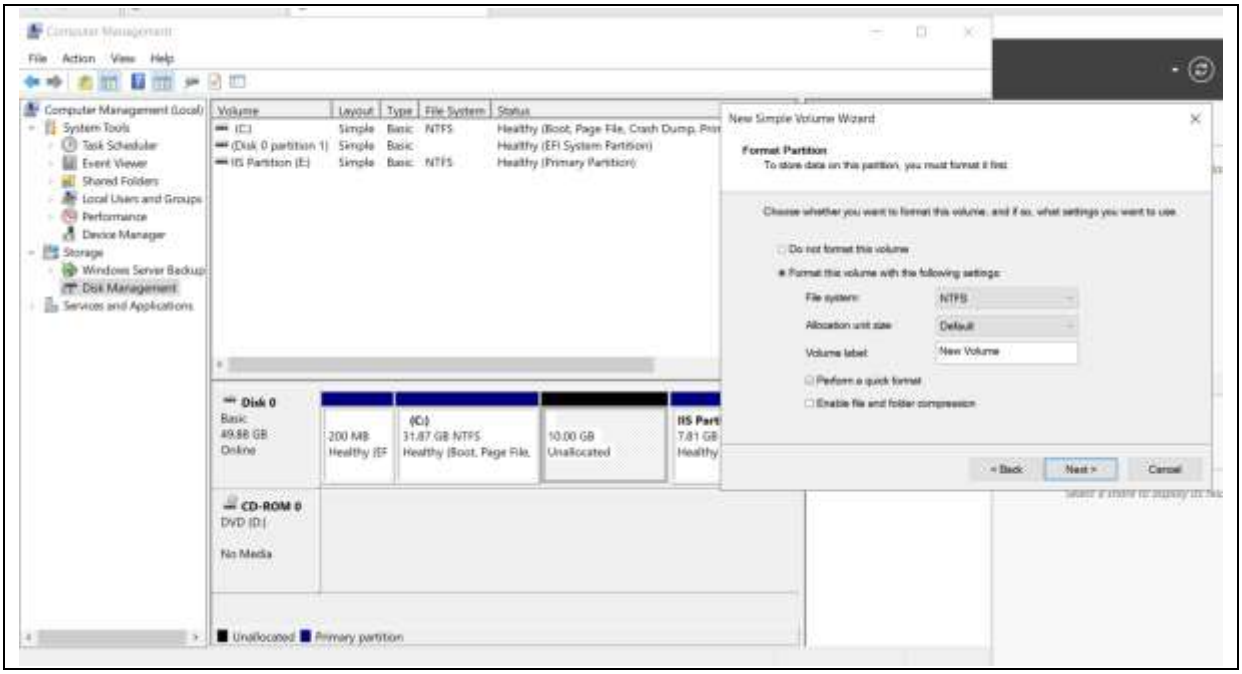
Step 9: Populate the disk which was unallocated in the beginning.



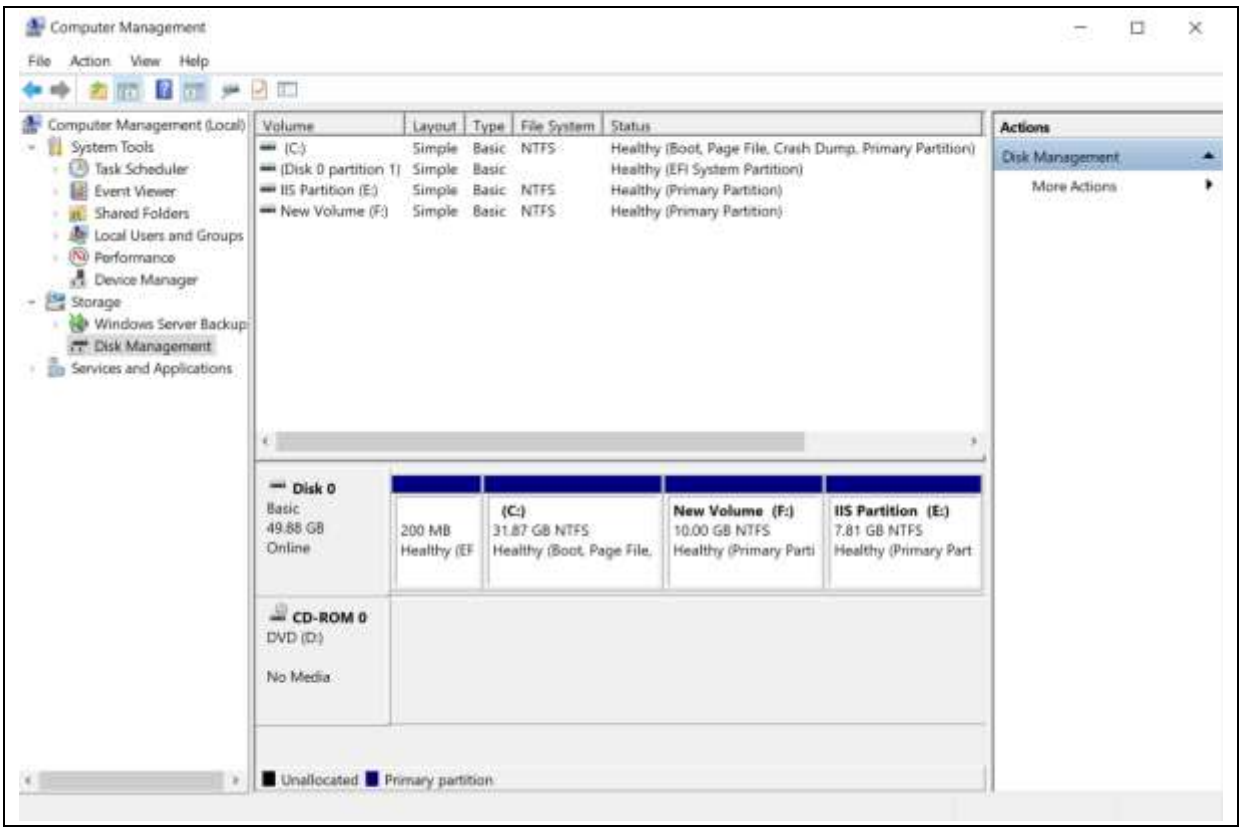
Step 10: A pop-up wizard will appear and proceed to click on “Next >” to continue the creation of the simple volume.



Step 11: Please only change the Volume Label to be the name of the allocated volume. Click “Next >” to continue.

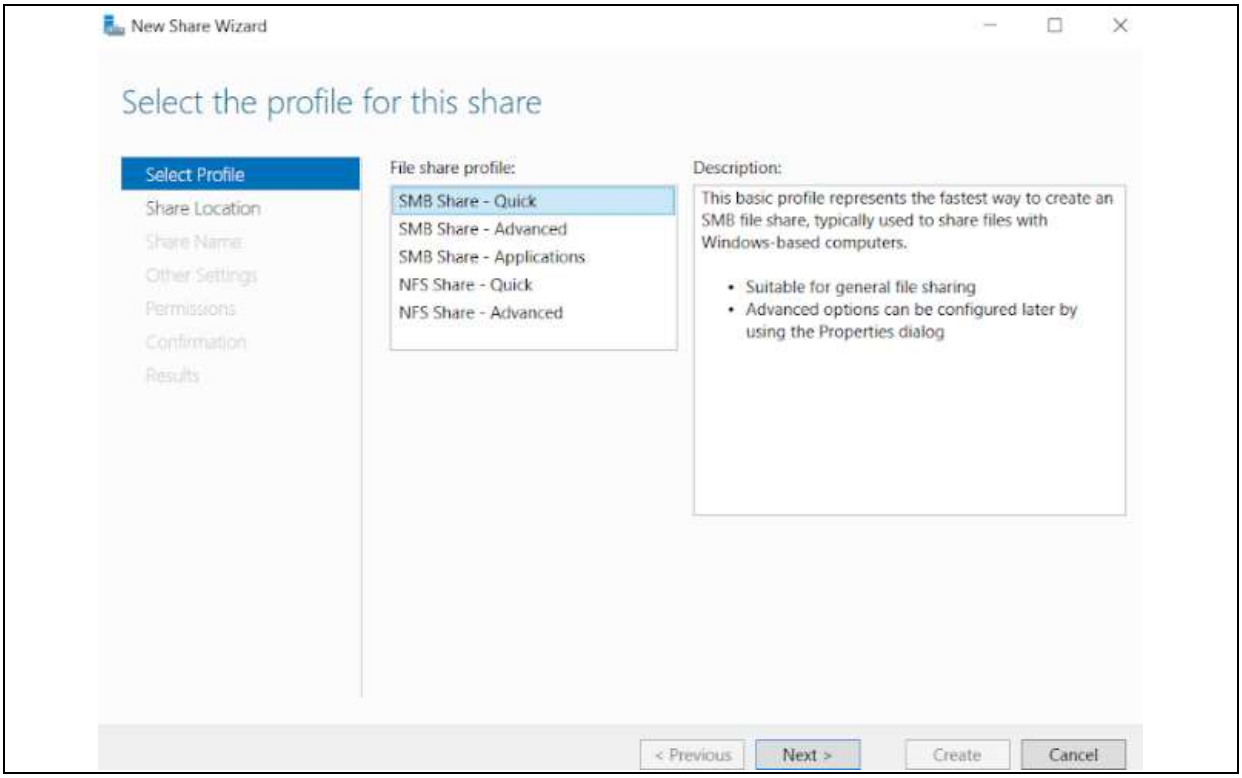


Step 12: Once the process is completed, the colour of the allocated space will be blue in colour. In our scenario, we kept the name of the volume as “New Volume”, which is shown as “10.00GB NTFS” in the image below. Close the window once the process is complete and a new volume has been allocated.

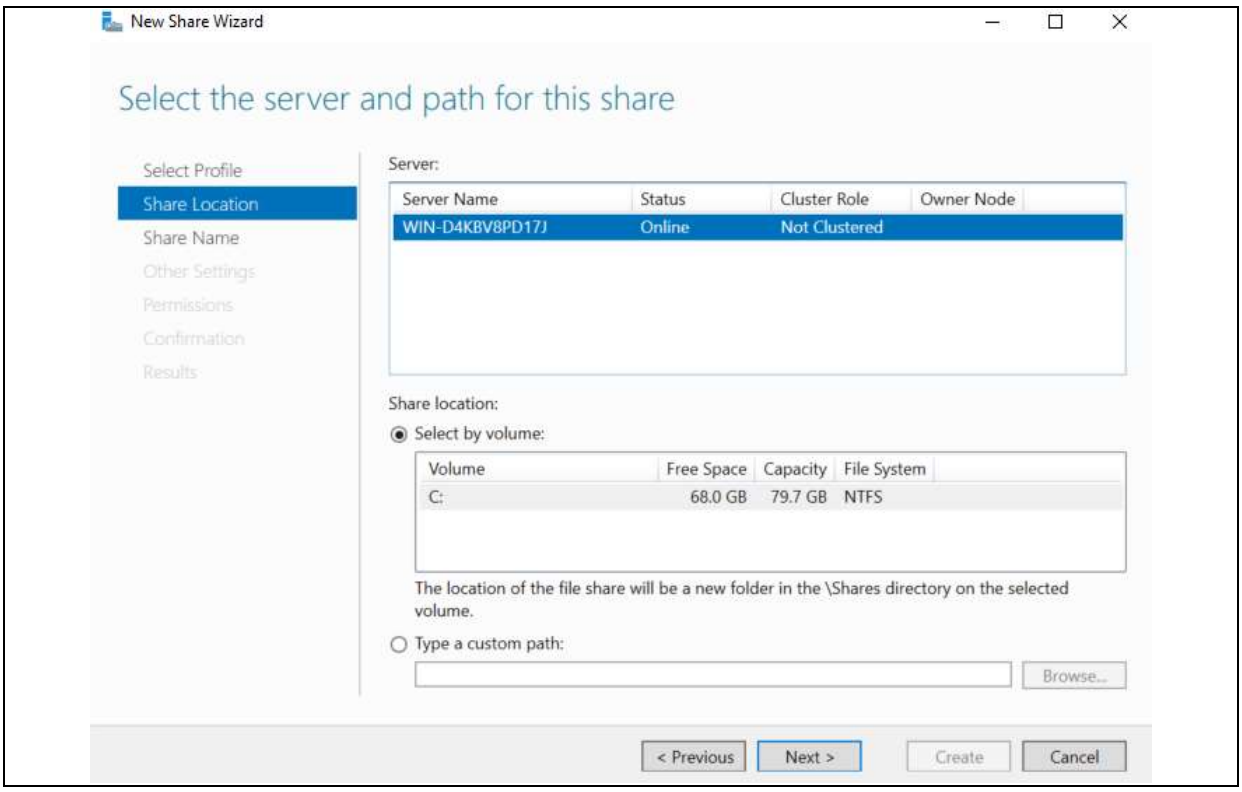


Step 13: Go to the directory “Server Manager > File and Storage Services > Shares” and click on “TASKS > New Share”.

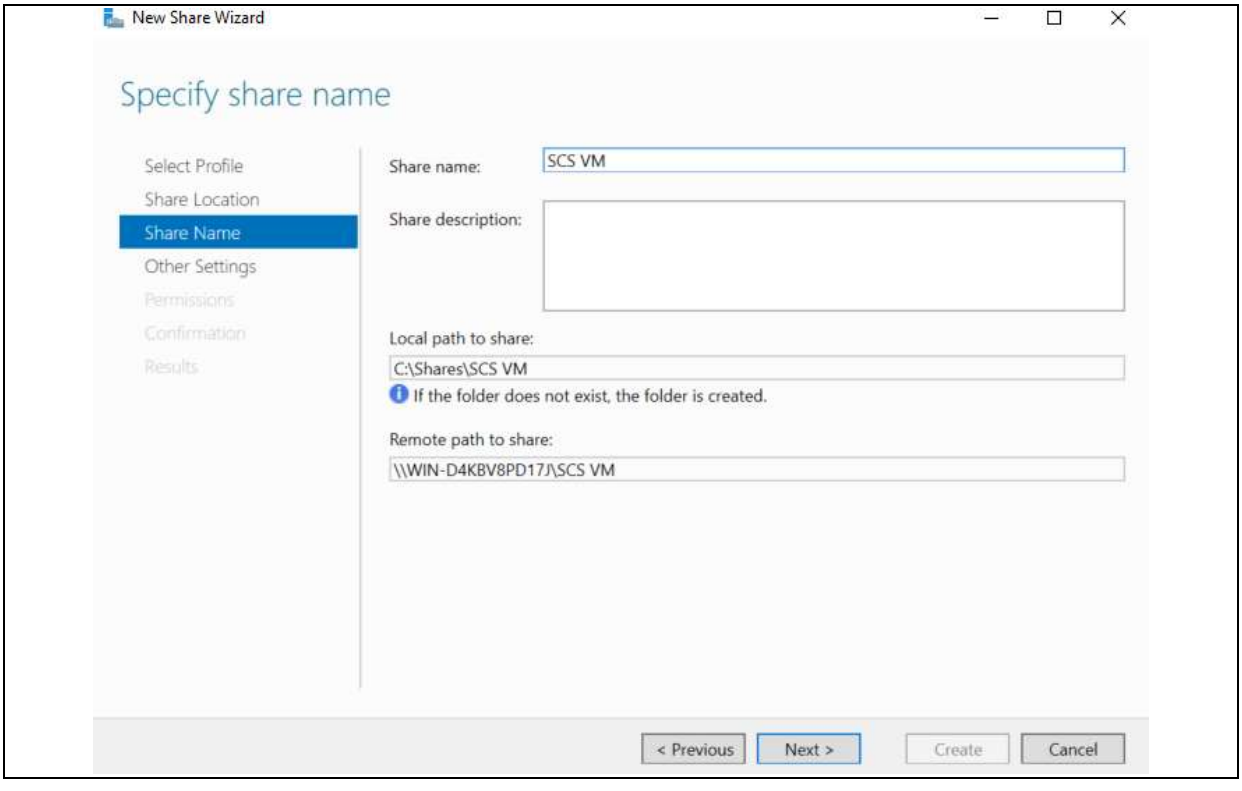
Step 14: This window will pop up and click on “SMB Share – Quick” since it is the fastest way to create share files. Click “Next >” to continue.



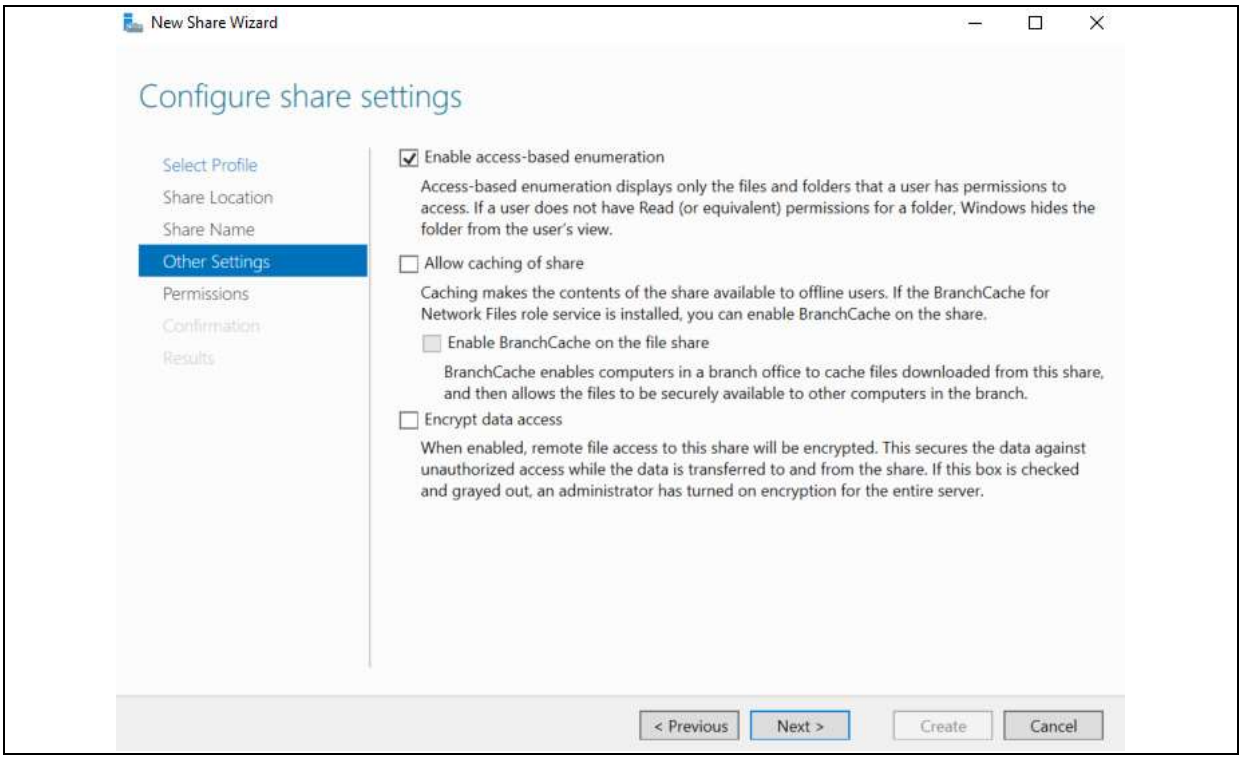
Step 15: Click on the name of the server that is going to be shared. Select the location (E.g. Volume C) and click “Next >”.



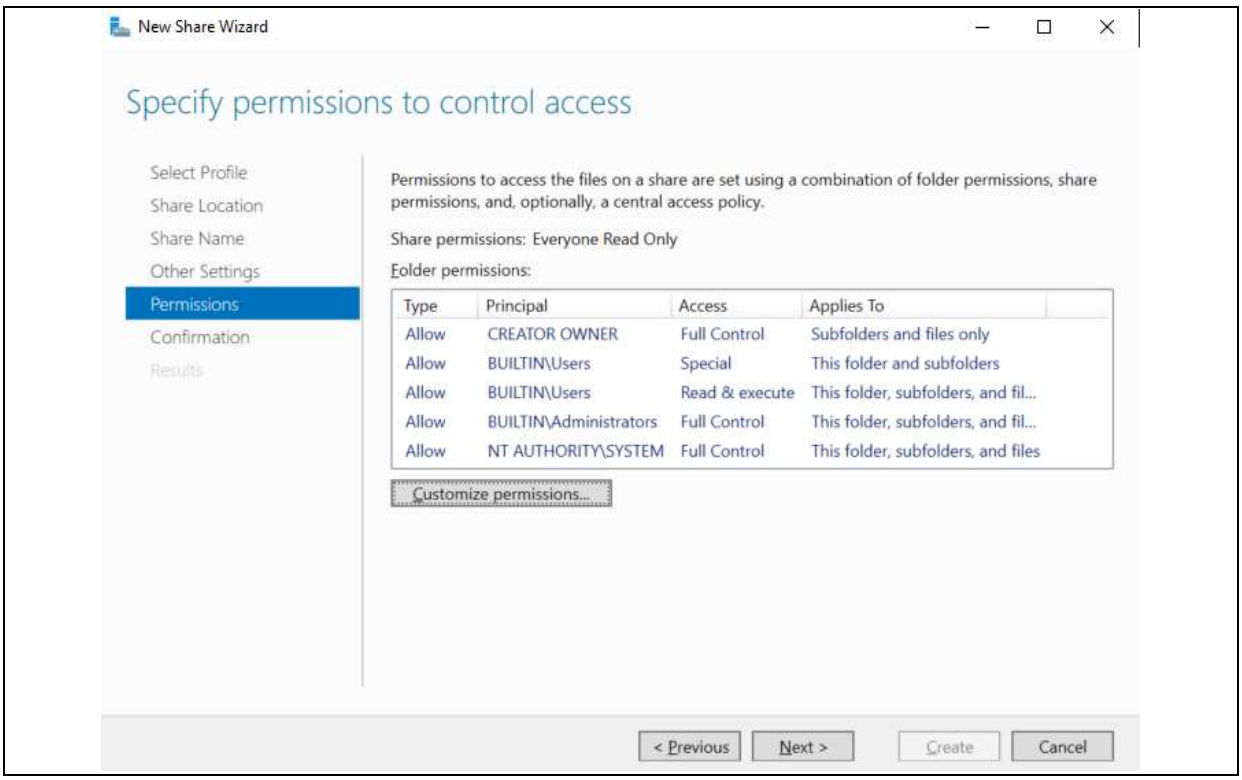
Step 16: Enter the name which the share network file will be called. Ours is called “SCS VM”. Click “Next >” to continue the process.



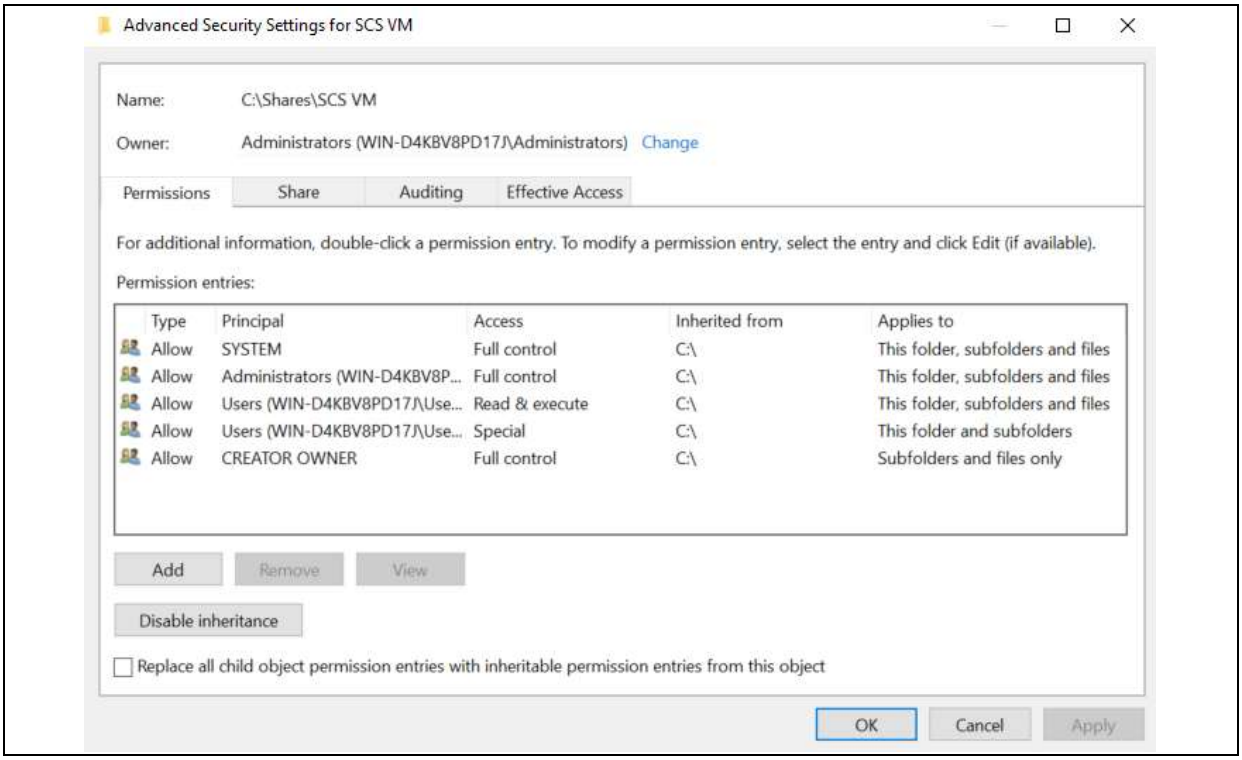
Step 17: Click on “Enable access-based enumeration” to only allow authorized users to view the files that they have permissions to. Click “Next >” to continue.



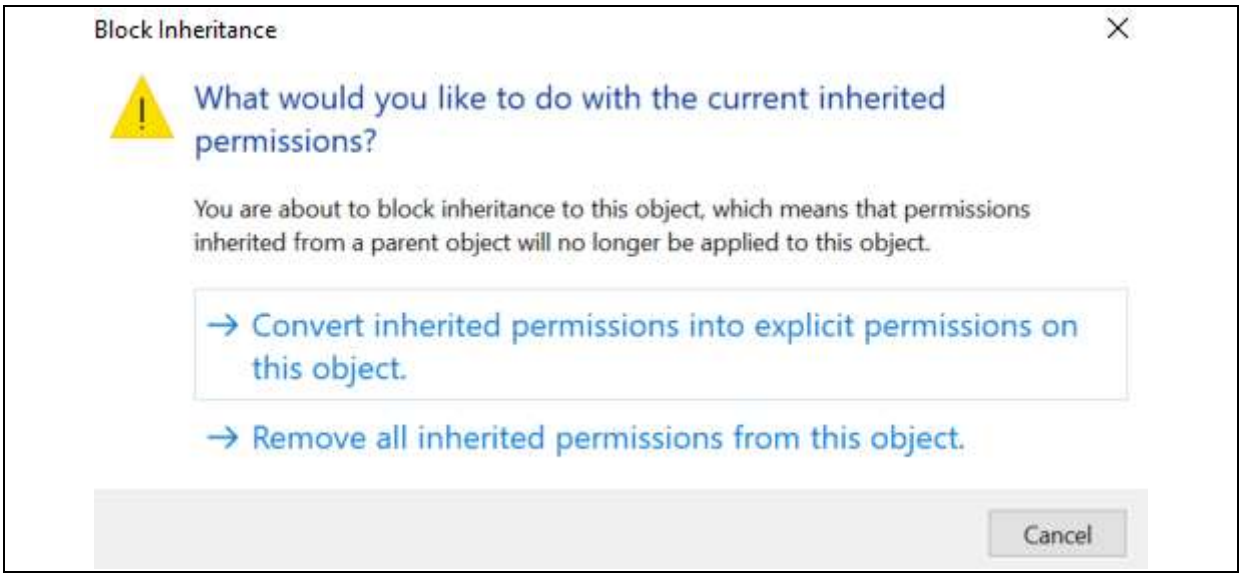
Step 18: This image shows the permission for each principal. Click on “Customize permissions…” to customize the permissions.



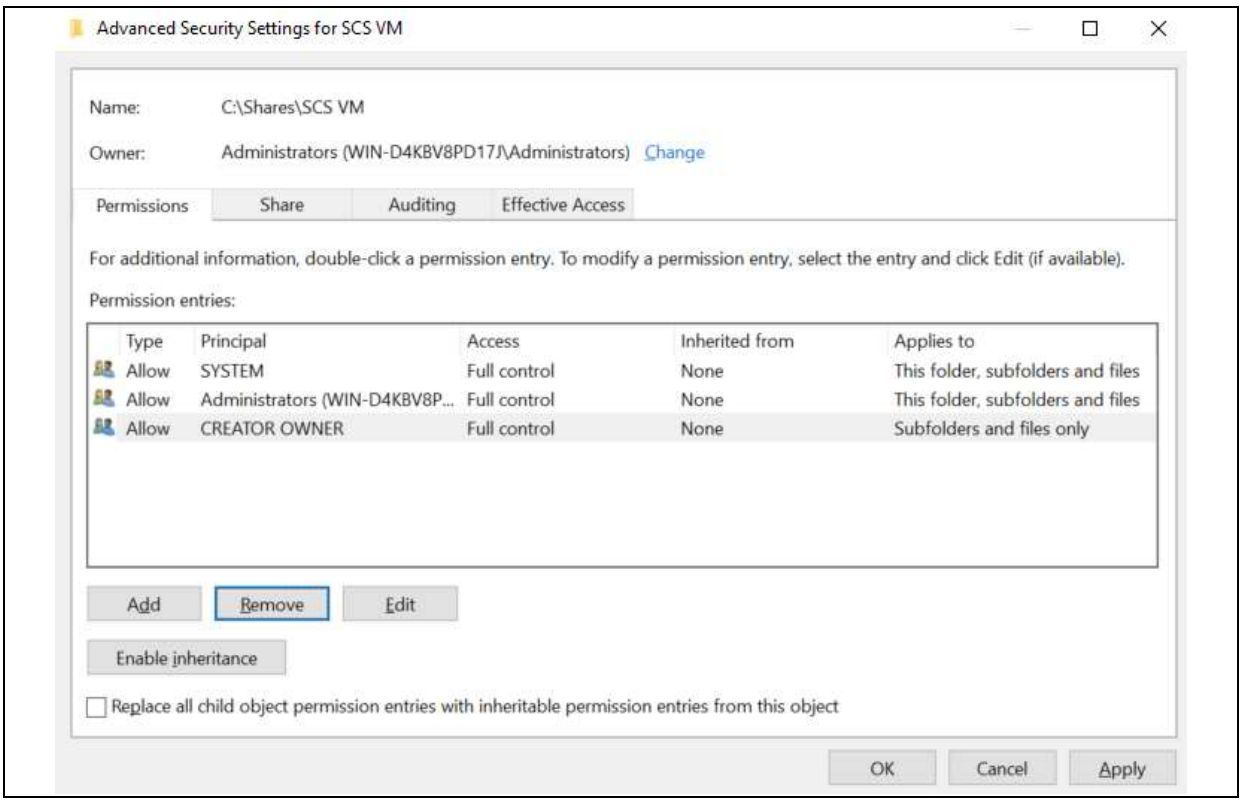
Step 19: Click on “Disable Inheritance”.



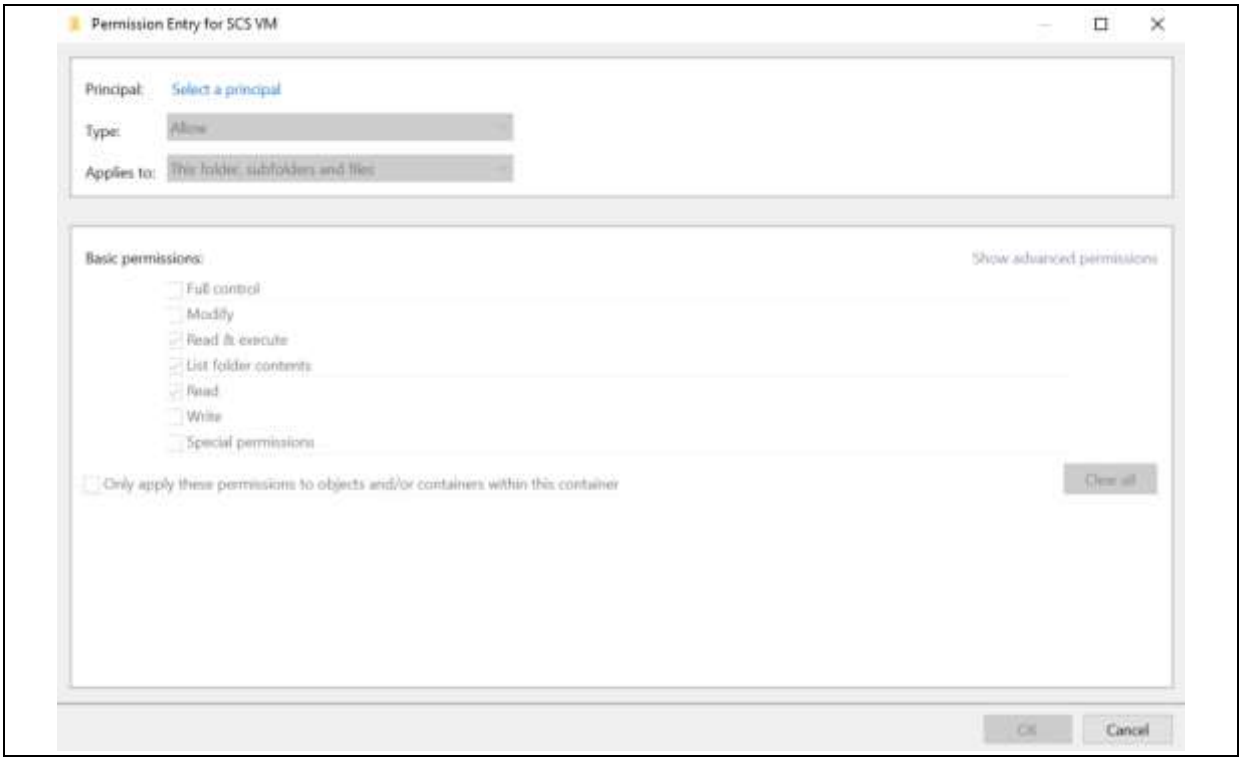
Step 20: This pop-up alert would be displayed, click on the top option, “Convert inherited permissions into explicit permissions on this object.”.



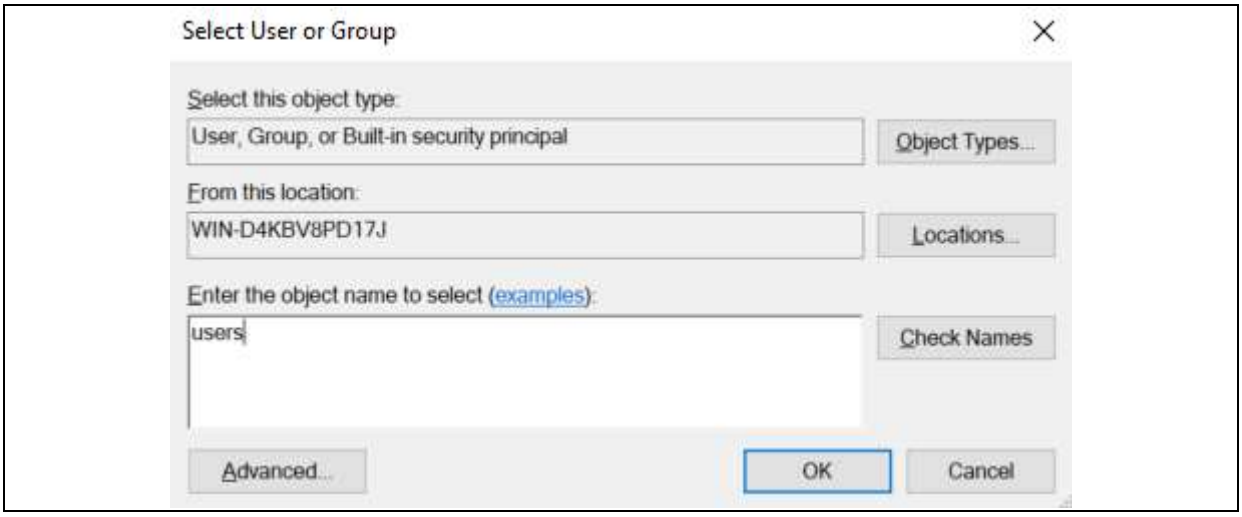
Step 21: Proceed to remove the Users principals. Once done, click on “Add” to create new principals”



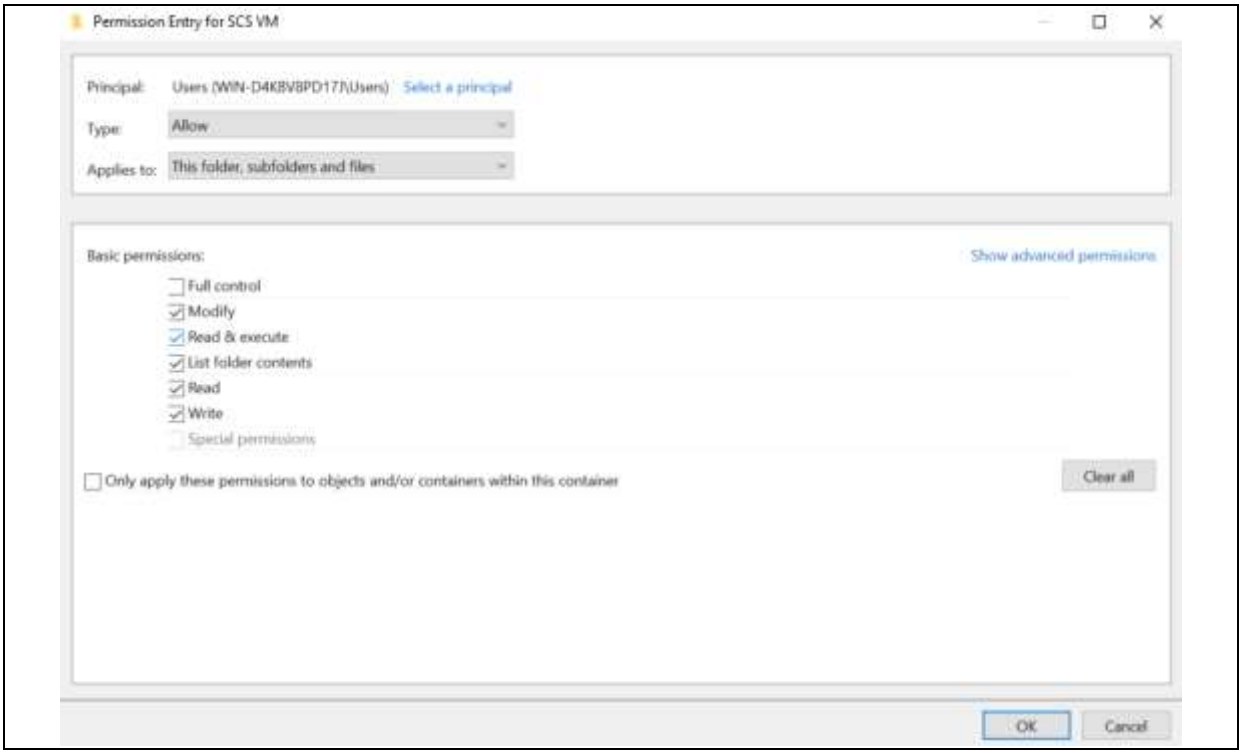
Step 22: This window would pop up. Click on “Select a principal”.



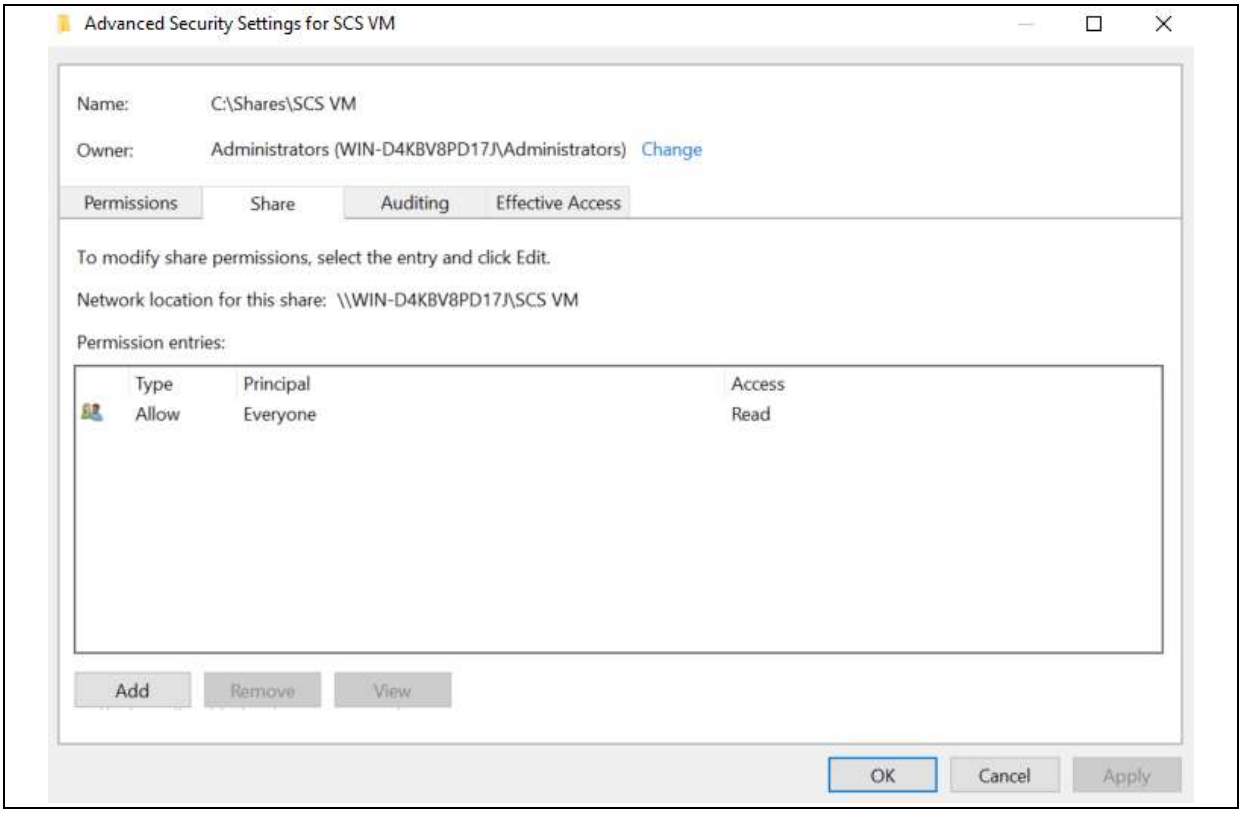
Step 23: Enter “users” on the textbox allocated and click “OK”.



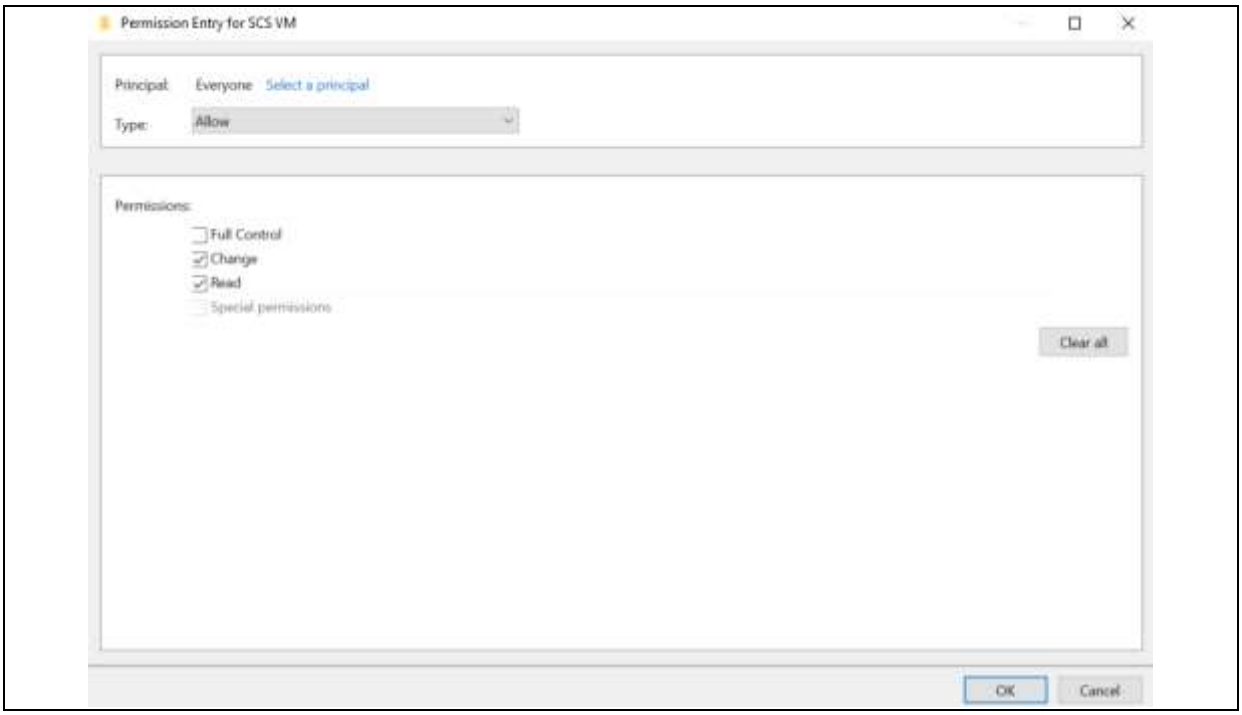
Step 24: Ensure that “Modify”, “Read & Execute”, “List folder contents”, “Read” and “Write” are all checked before clicking “OK”.



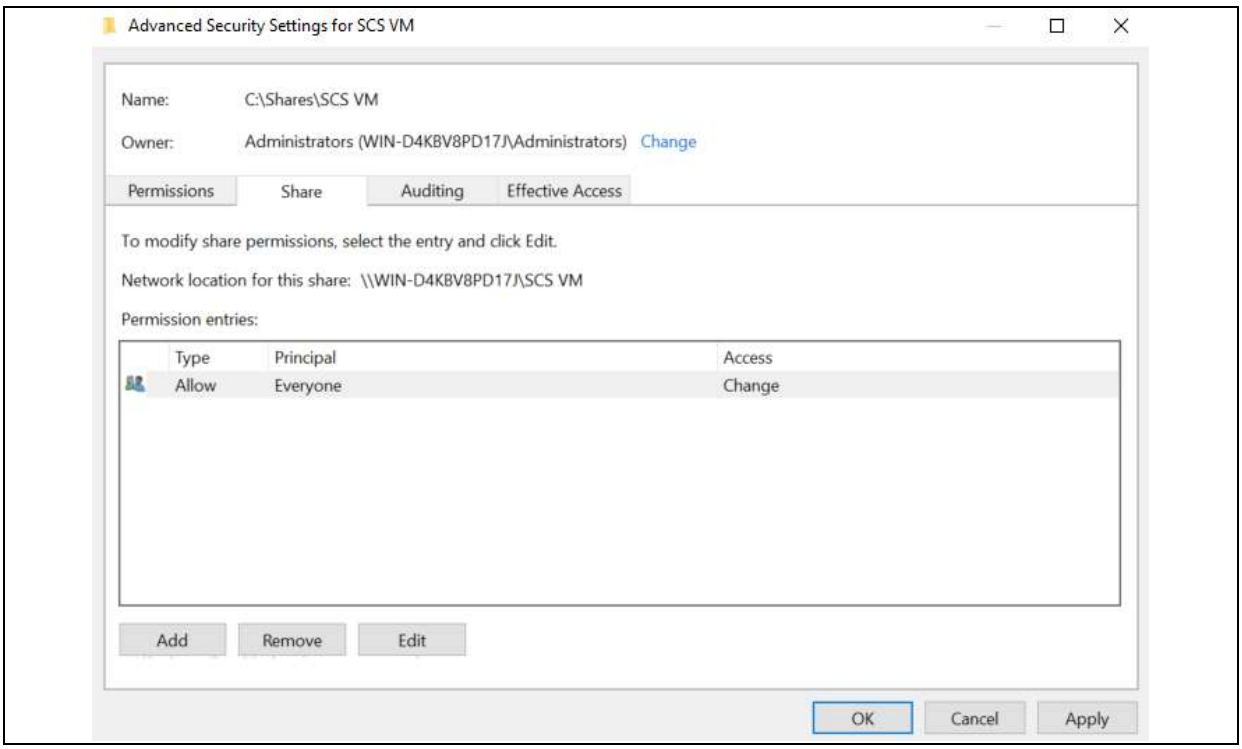
Step 25: Click on “Share” to see this page. Double click on “Everyone”.



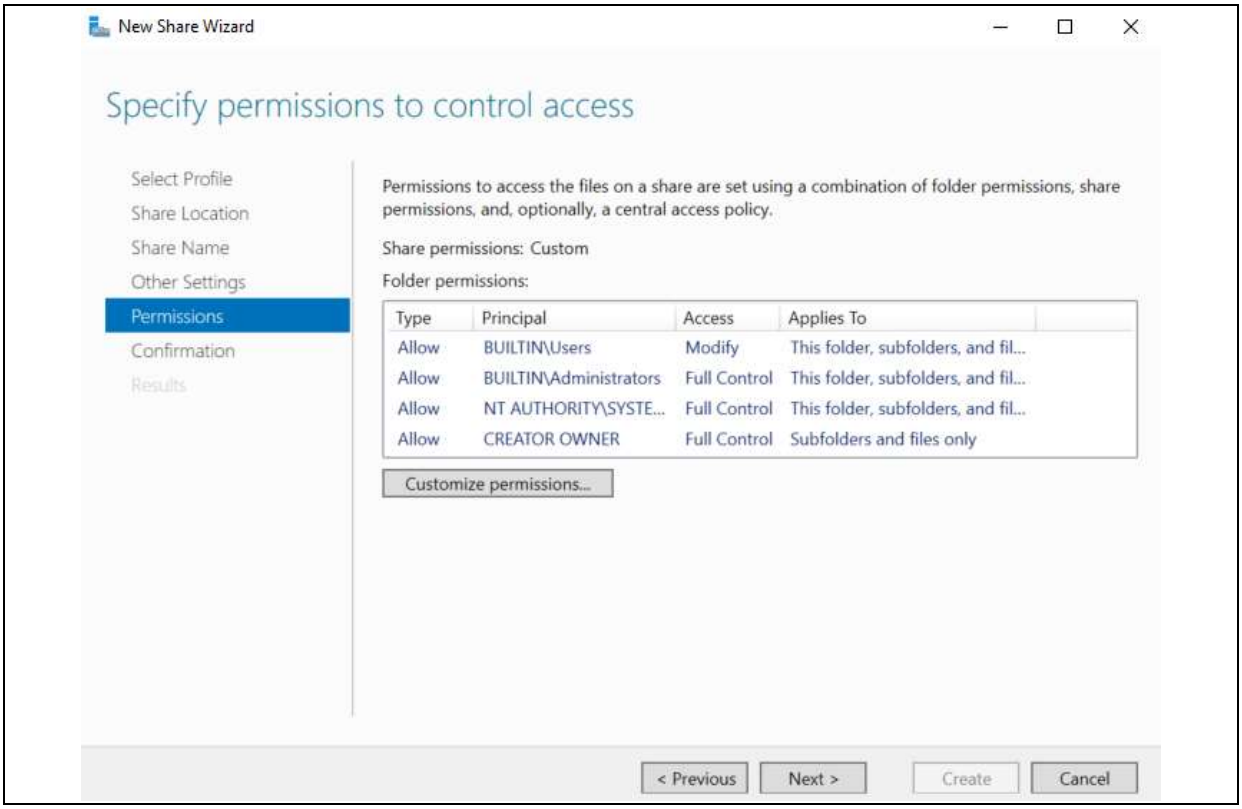
Step 26: This page would be shown, ensure that “Change” and “Read” is checked before clicking “OK”.



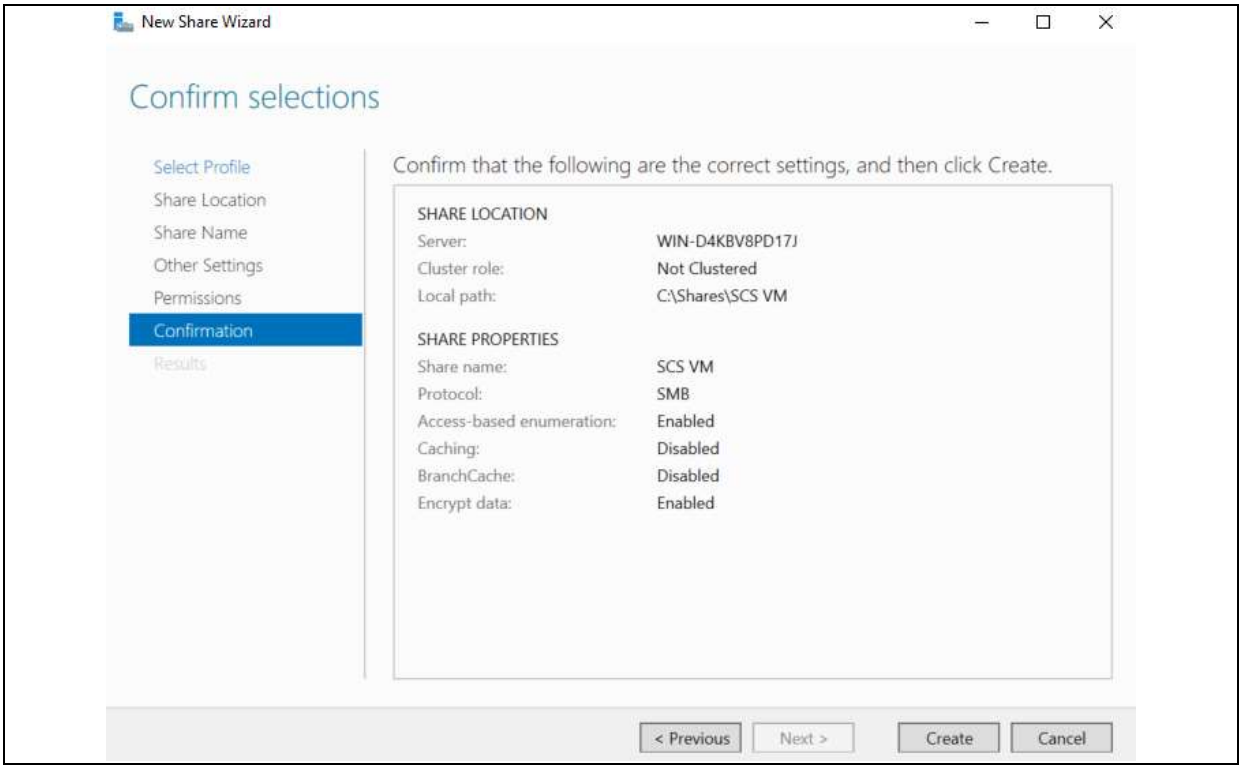
Step 27: The screen should now display the access as “Change” instead of “Read”. Click “Apply” then “OK”.



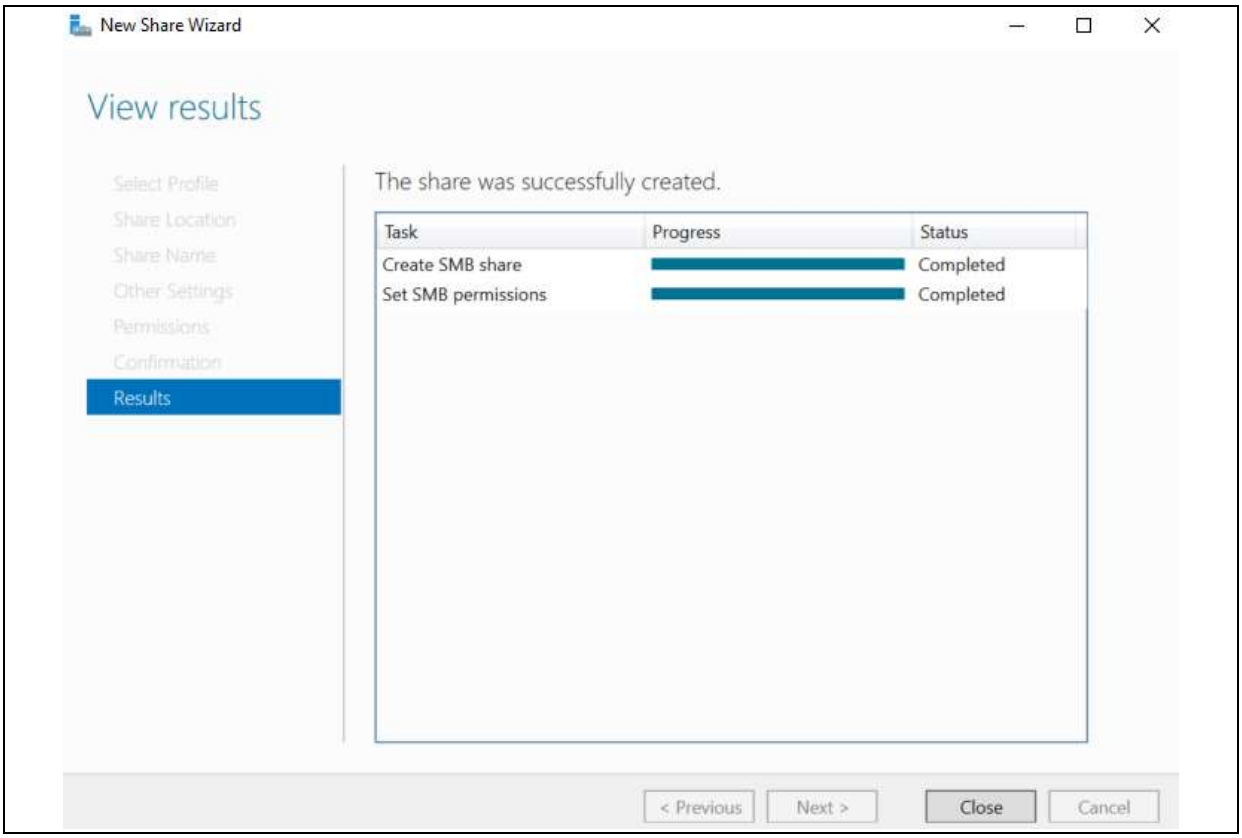
Step 28: The screen would now show this screen, click on “Next >”.



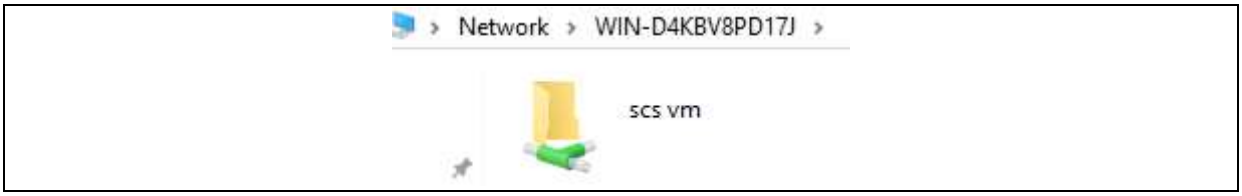
Step 29: Click on “Create” to create the network file sharing folder.



Step 30: This screen will be displayed once the folder has been successfully created.



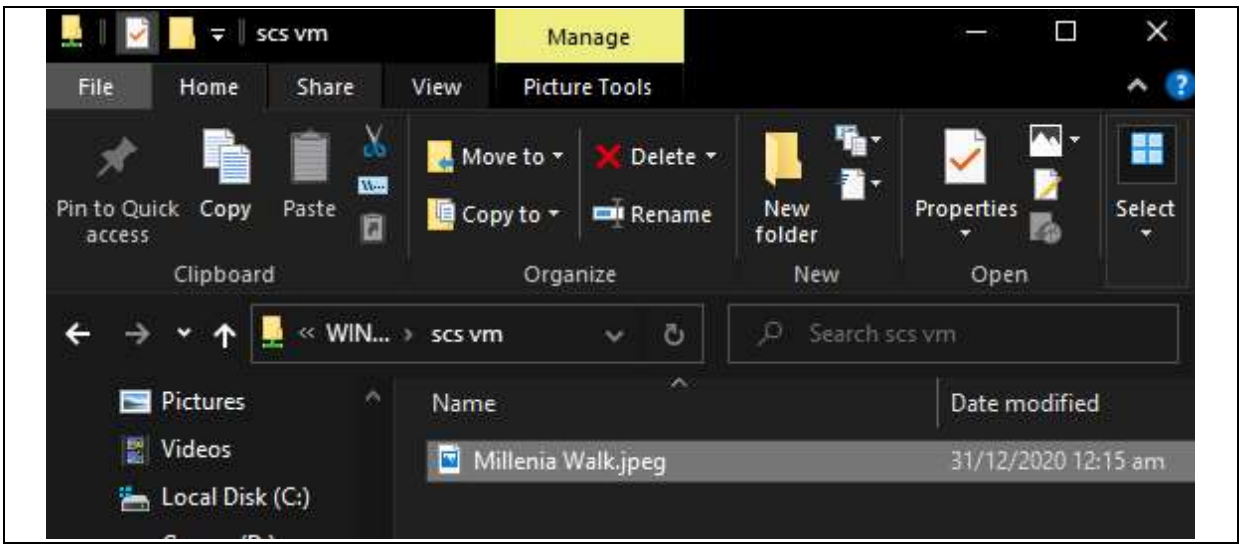
Step 31: This is the folder as seen on Windows Server 2019.



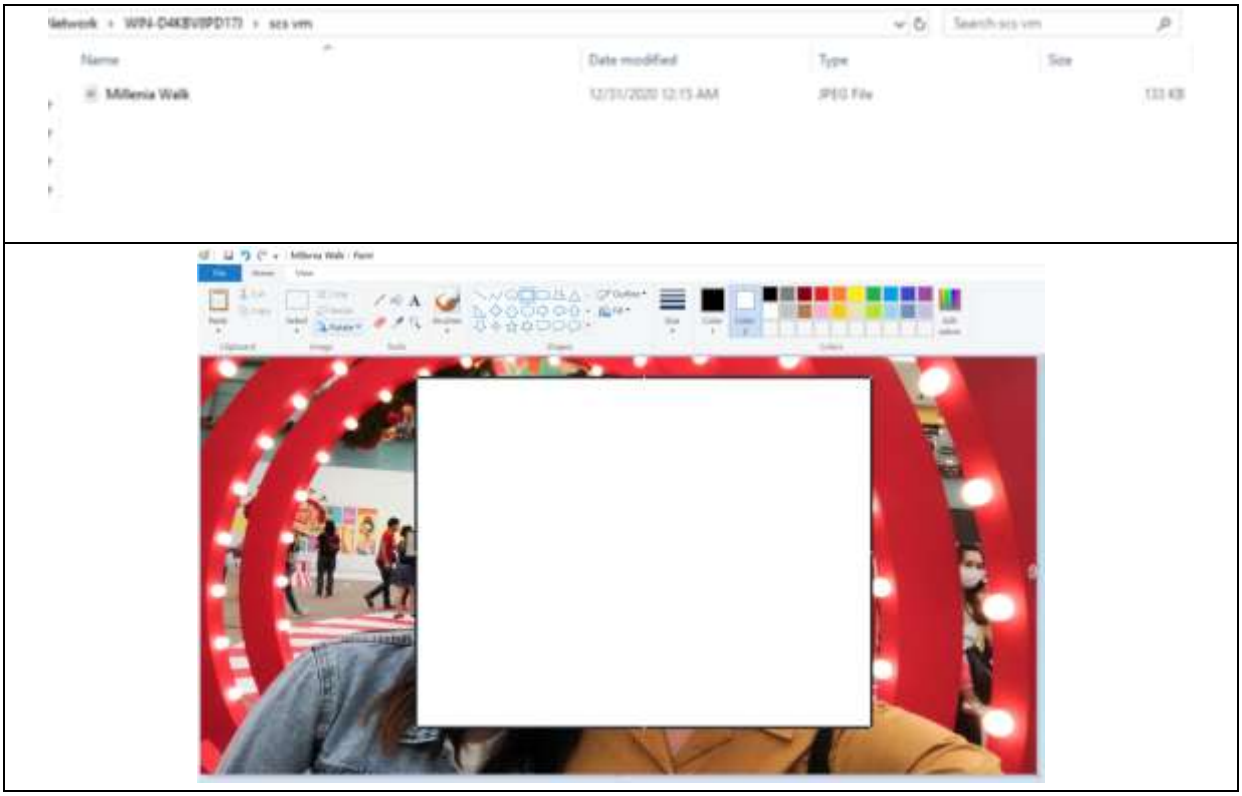
Step 32: This is the same folder shown on my personal desktop using Windows 10.

Testing Network File Server Connectivity

Step 1: I copied an image from my personal desktop and pasted it into the network folder. The image shows the outcome shown on my personal desktop.

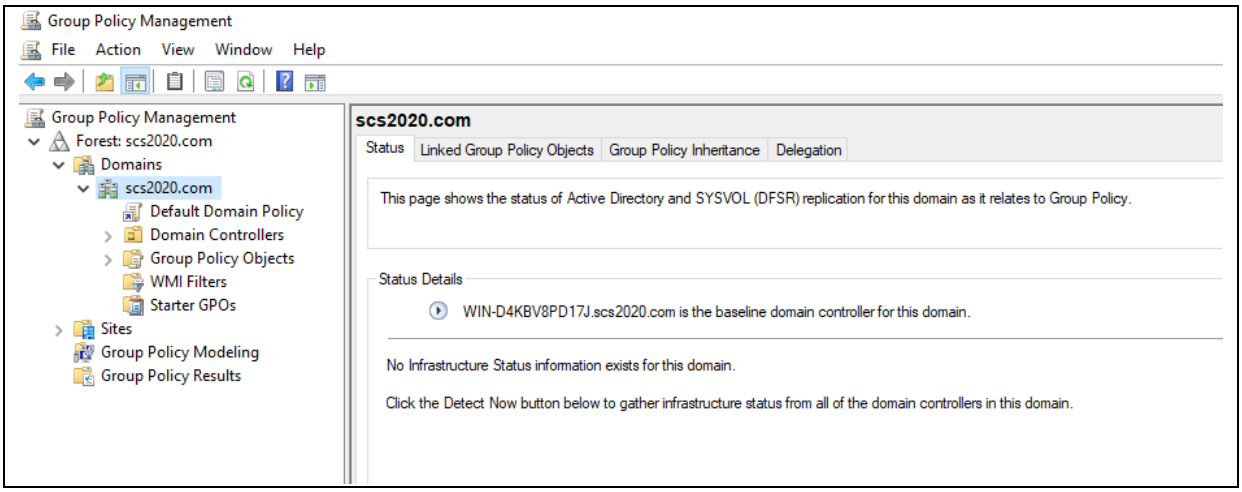


Step 2: The image shown below shows the same image displayed on Windows Server 2019. Thus, proving that the network folder works. I can even open the image to display the contents as shown.

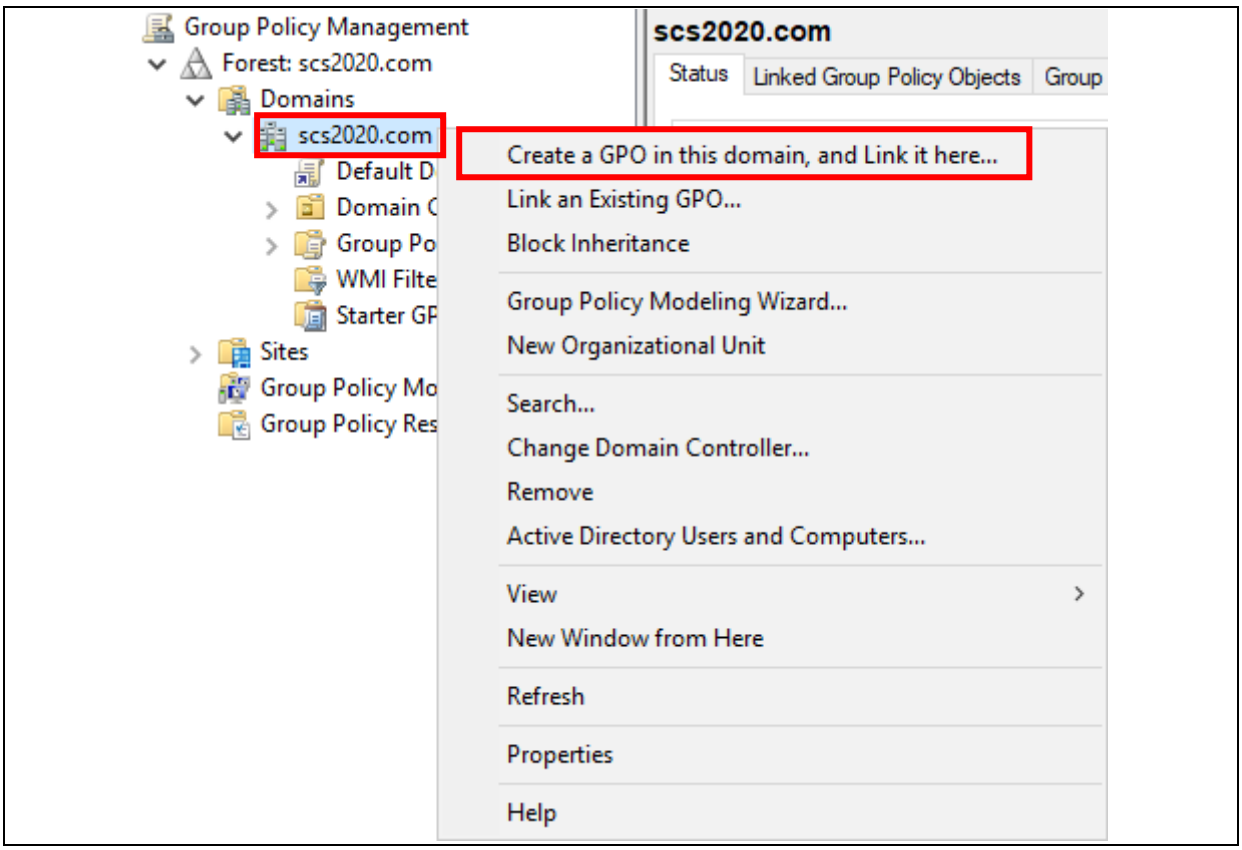


Configure Group Policy Object

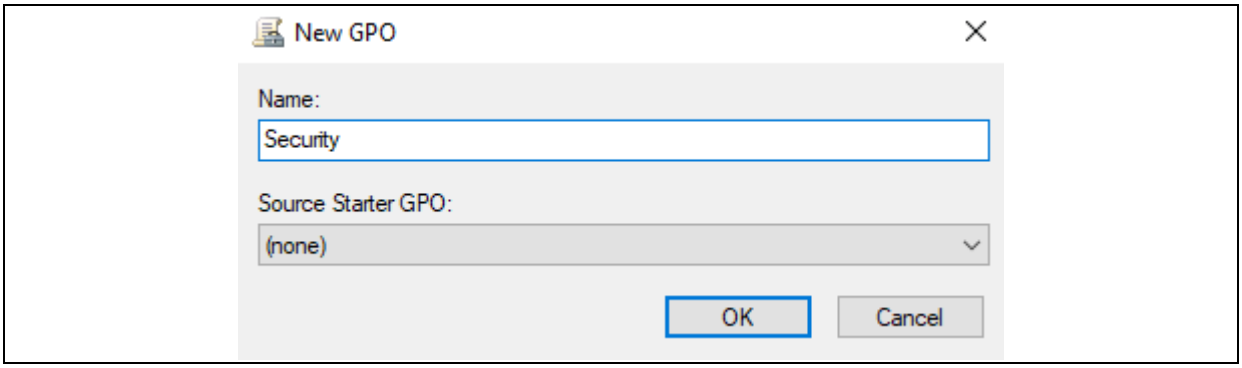
Step 1: Open Group Policy Management after creating a forest and adding in the user's desktop into the forest after logging into the administrator account.



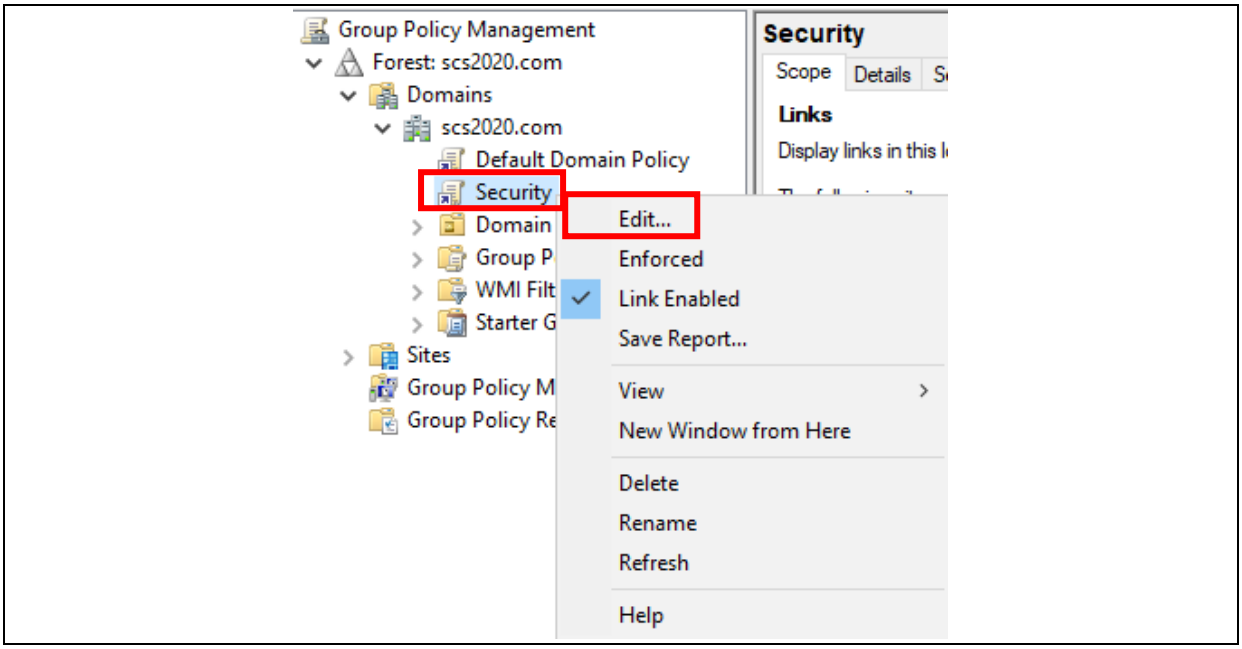
Step 2: Right-click the domain and click on “Create a GPO in this domain, and Link it here” to create a group policy object (GPO).



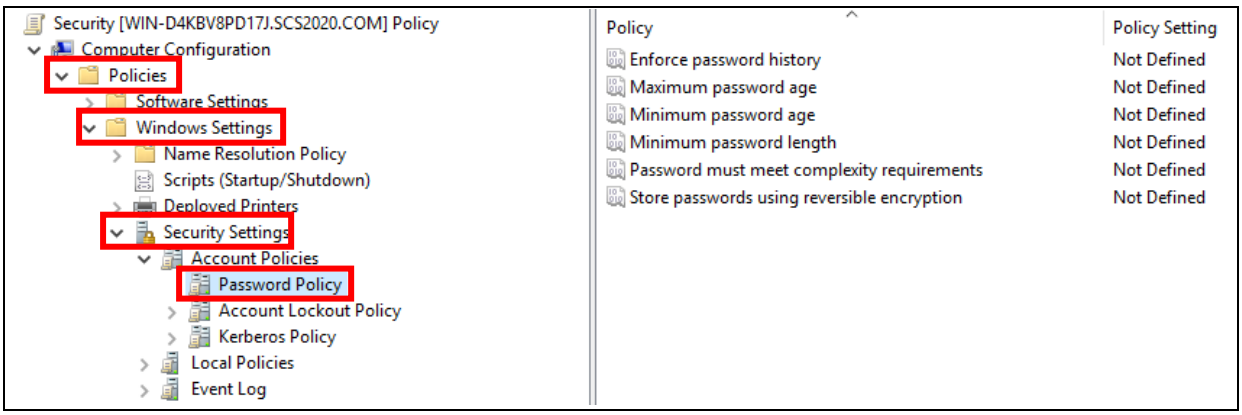
Step 3: Change the name to the name you would like to have as your GPO name. We set it to “Security” for our case.



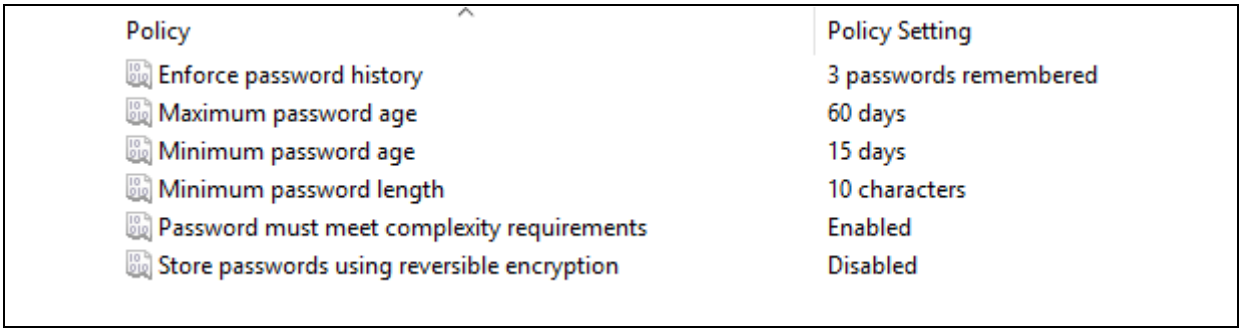
Step 4: Right-click the newly created GPO and click on “Edit”.



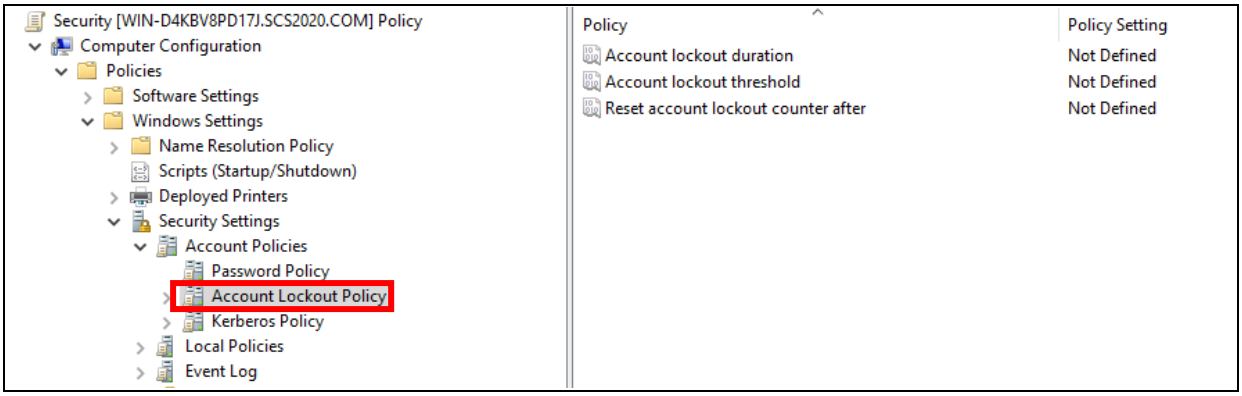
Step 5: Go to Policies > Windows Settings > Security Settings > Password Policy.



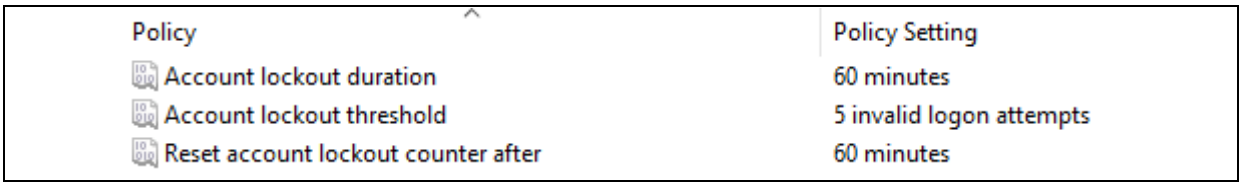
Step 6: Set the policy settings accordingly by right clicking the policy settings and setting the options for each.



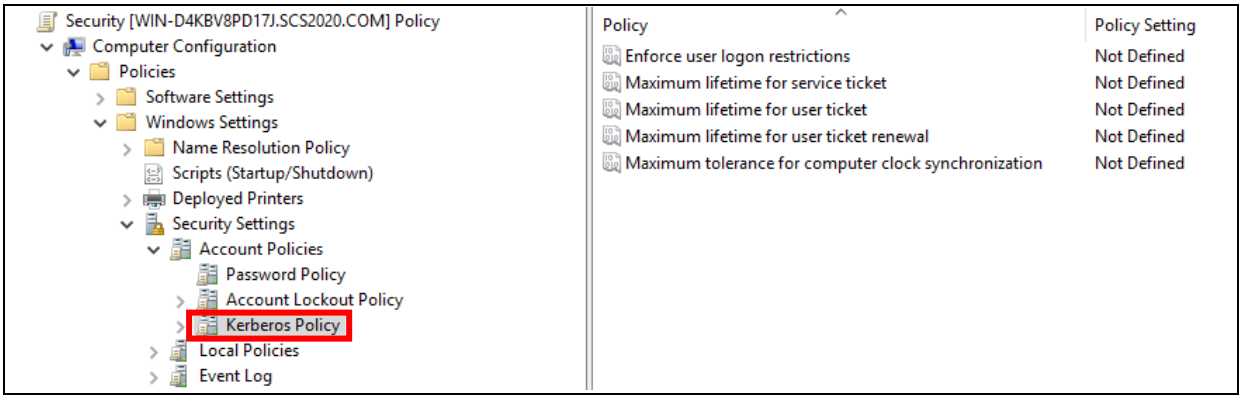
Step 7: Next, Account Lockout Policy will be configured.



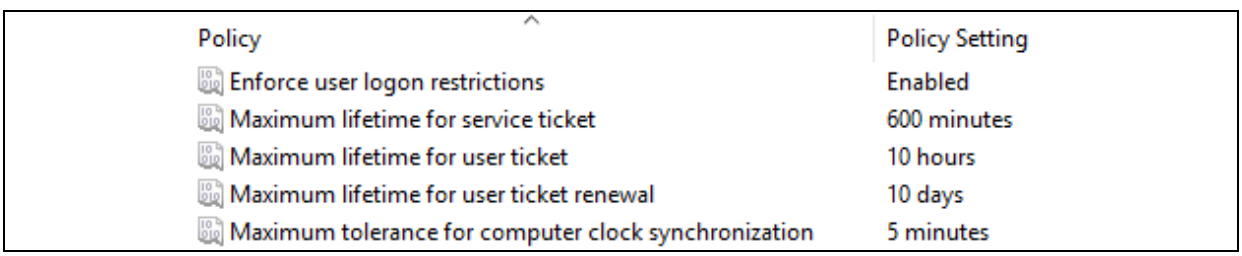
Step 8: Set the policy settings accordingly by right clicking the policy settings and setting the options for each.



Step 9: Next, Kerberos Policy will be configured.



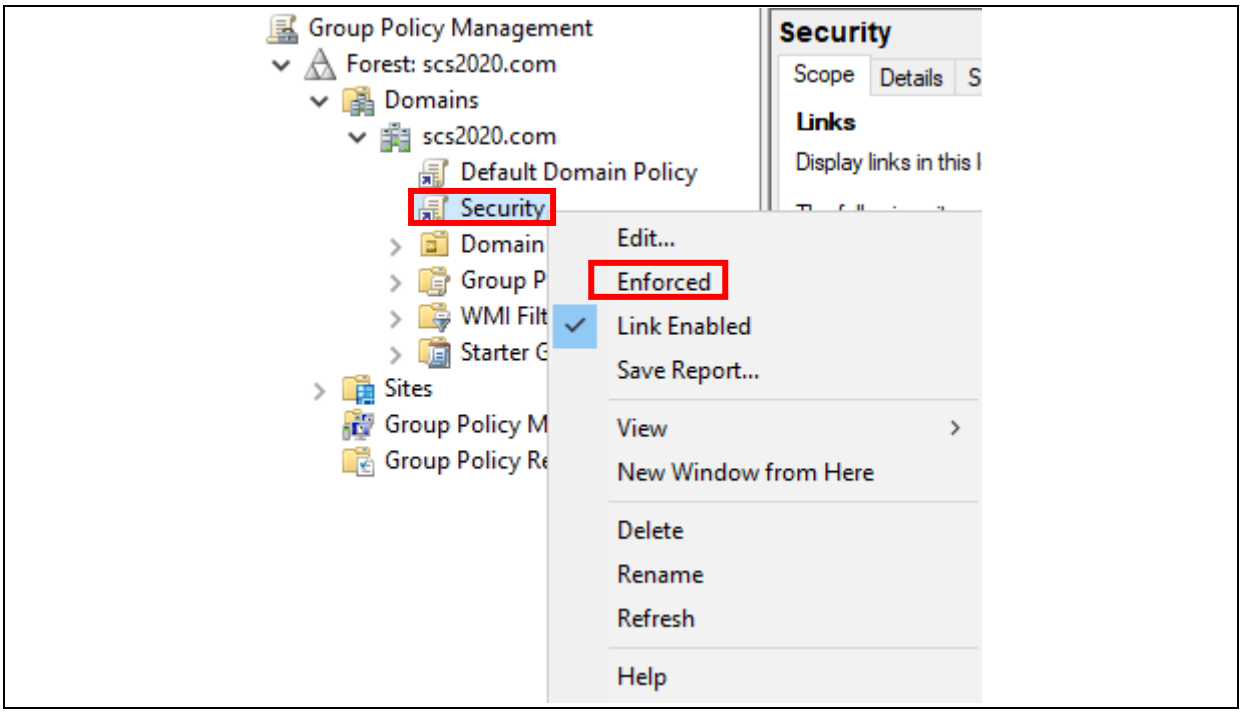
Step 10: Set the policy settings accordingly by right clicking the policy settings and setting the options for each.



These are the following policy explanations and why they should be used:

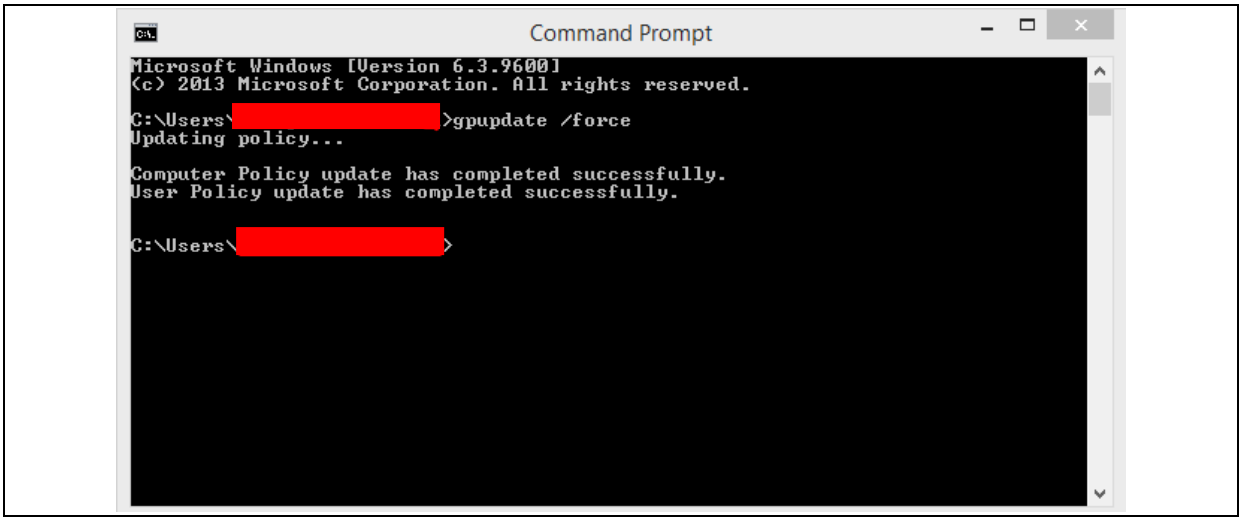
1. Enforce user logon restrictions:
    - This policy determines whether the Kerberos Version 5 Key Distribution Center (KDC) validates every request for a session ticket and compares it against the rights policy of the user account.
2. Maximum Lifetime for a service ticket:
    - This determines the maximum time in minutes, that a granted session ticket can be used for a particular service.
3. Maximum Lifetime for a user ticket:
    - This determines the maximum time in hours, that a user's ticket-granting ticket can be used.
4. Maximum lifetime for user ticket renewal:
    - This determines the period of time in days, during which a user's ticket-granting ticket can be renewed.
5. Maximum tolerance for computer clock synchronization
    - The amount of time that Kerberos Version 5 tolerates between the time on client clock and the time on the Domain Controller.

Step 11: Enforce the group policies by right clicking on the group policy object and clicking "Enforce".



By clicking on “Enforce” it enforces the policy and apply to all the organizational units (OUs) followed in the Active Directory (AD). This setting will also override any OU with the Block Inheritance. The default time to update all clients is 90 minutes, meaning that every 90 minutes, it will contact the Active Directory to check if there are any policy changes applicable to all or any specific clients.

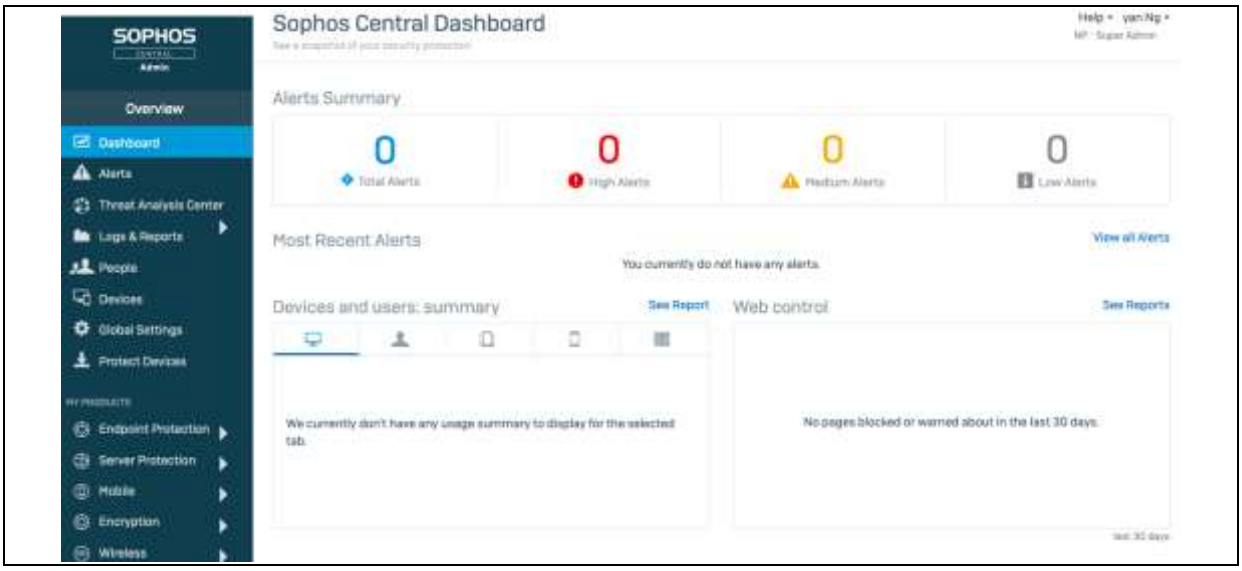
To update it immediately, use the *gpupdate/force* command in the clients which will perform checks with the AD and update to the most recent policy settings.



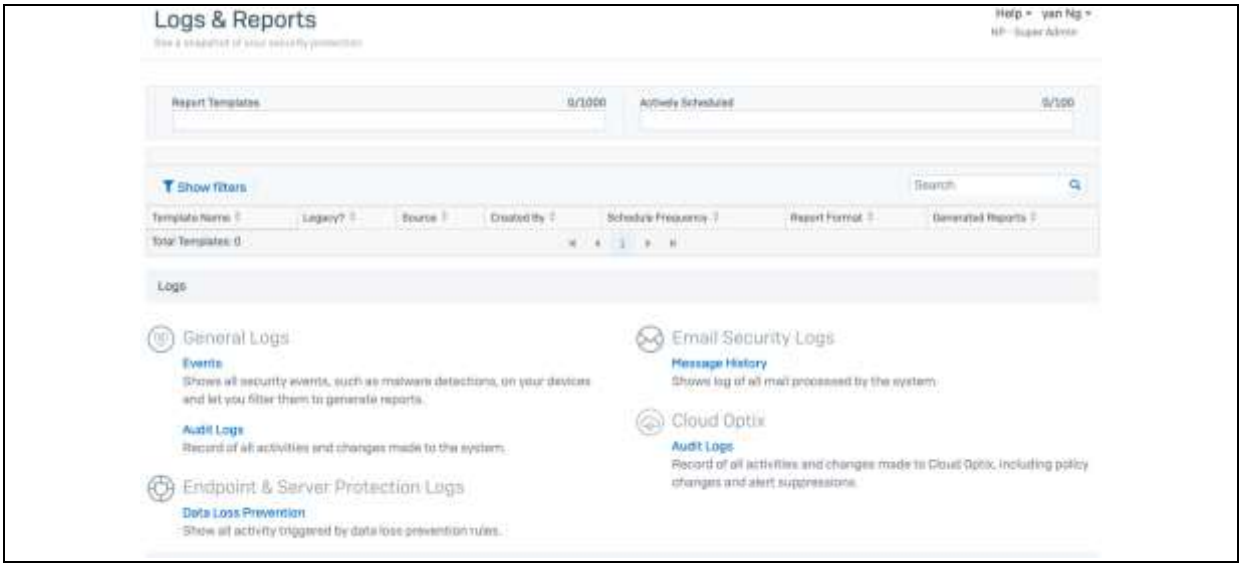
Sophos Server Protection

For the antimalware protection, we chose to use Sophos Server Protection. Sophos is a reputable anti-virus company which provides various software to enhance the security posture of both individuals and enterprises.

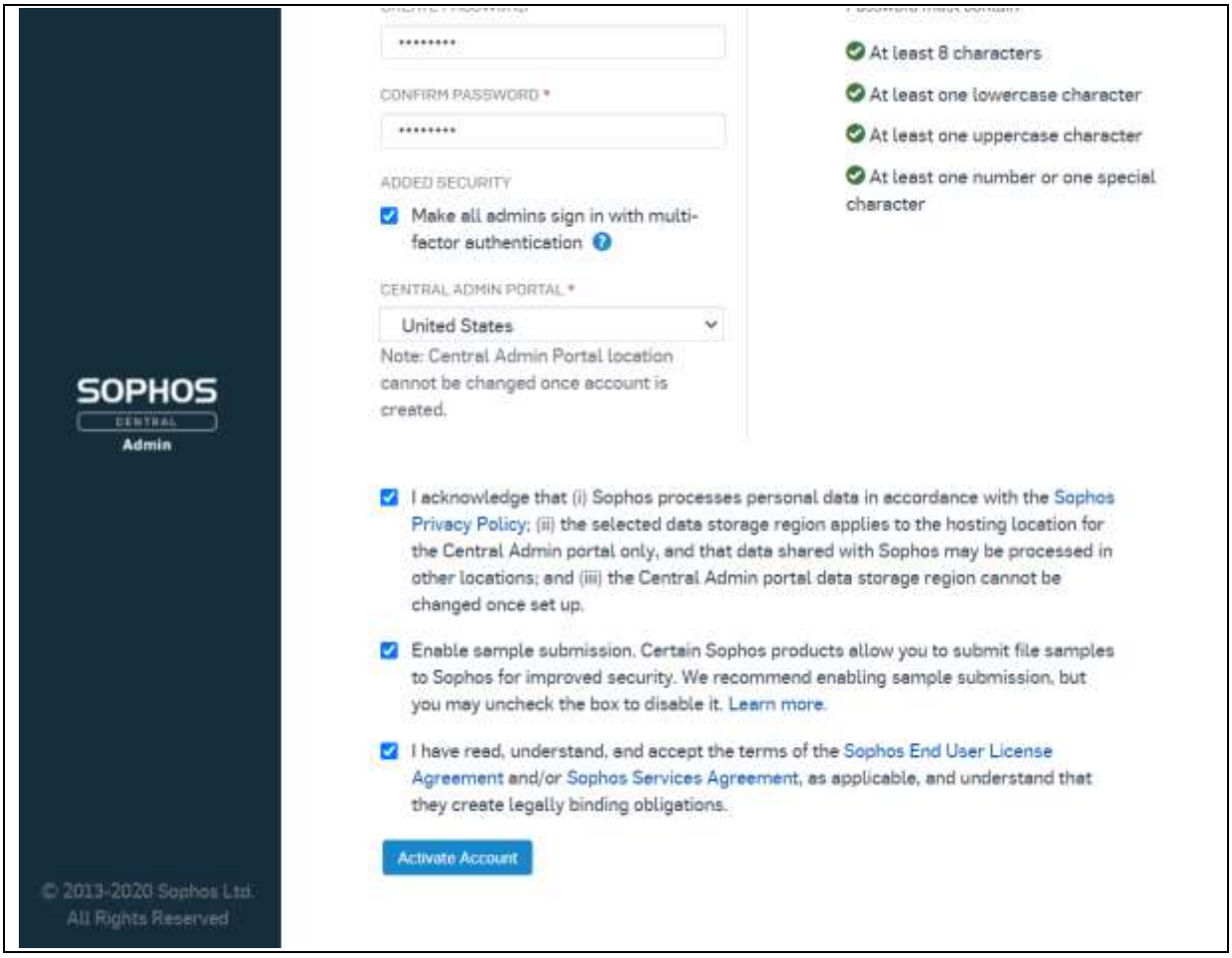
For this exercise, we decided to get the 30-day Free Trial of the Sophos Central, which is a centralised dashboard allowing system administrators to monitor objects like individual endpoint devices, servers, and users.

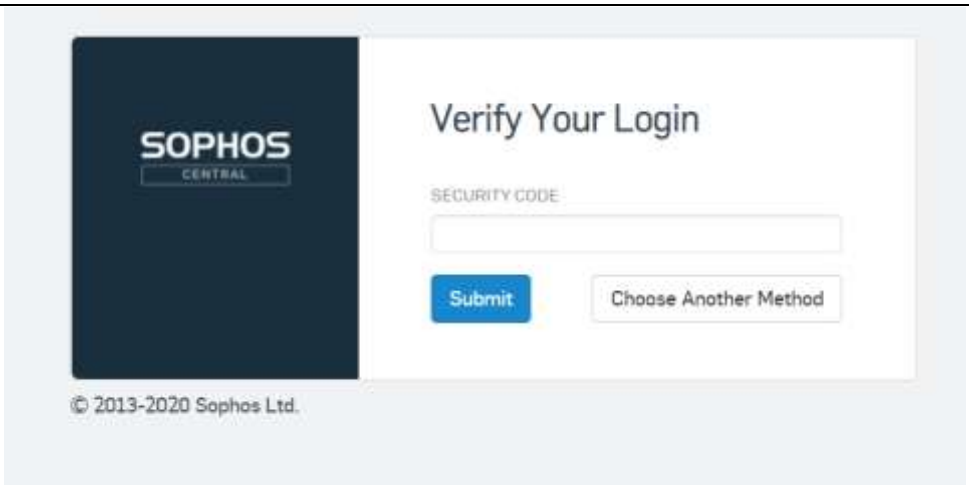


It also offers admins the option to look at various types on logs that are generated by the endpoint software.



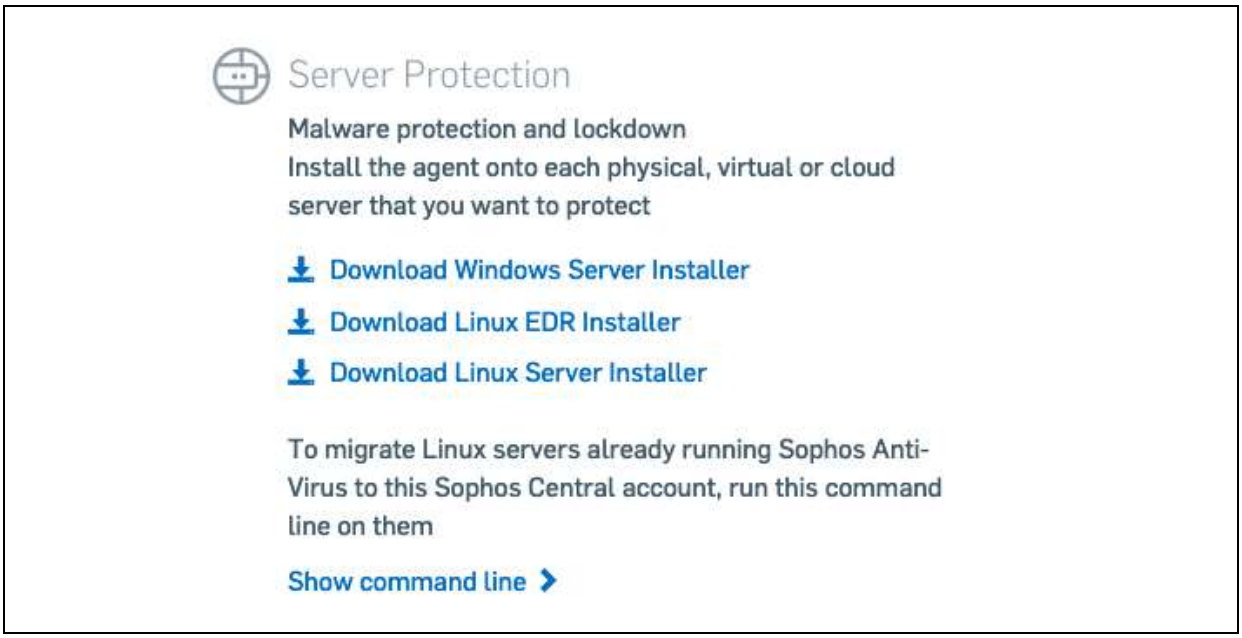
Sophos Central has 2FA configurable to be automatically enabled, thus the administrator will need to use Google Authenticator application to Login, which provides an additional layer of security on top of the password.



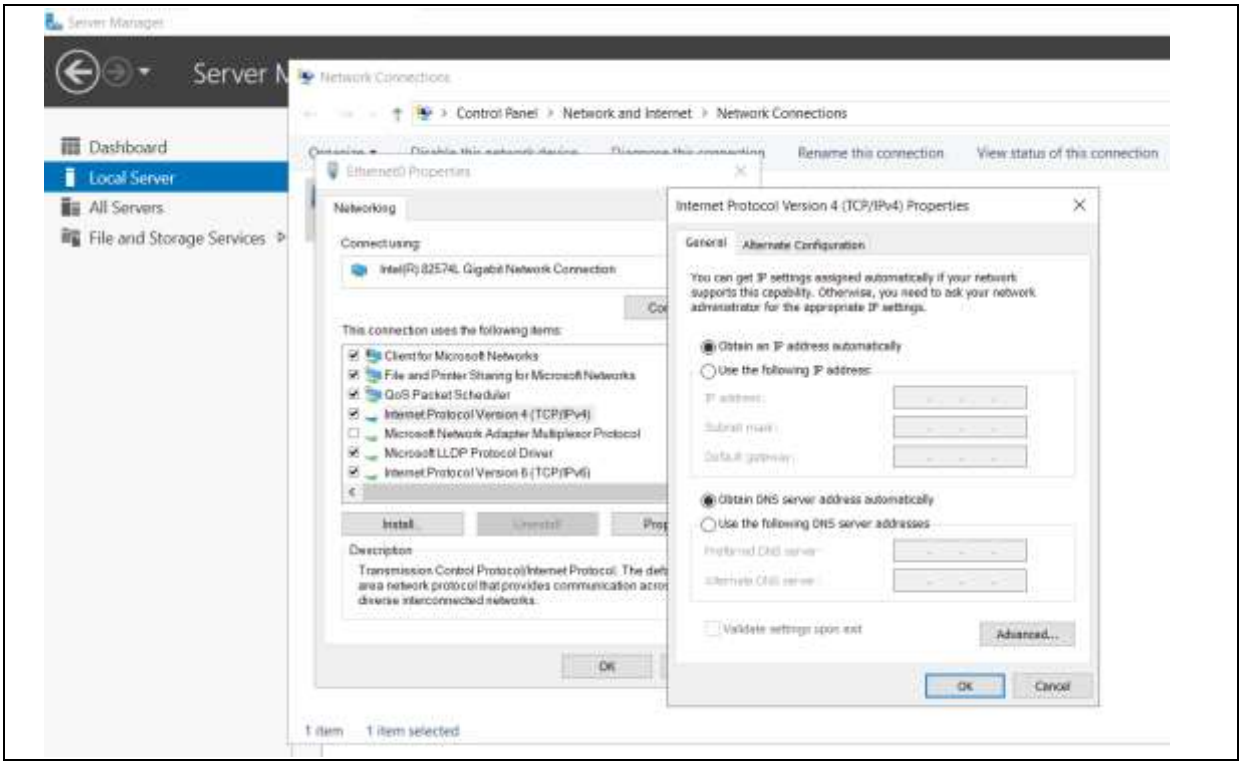


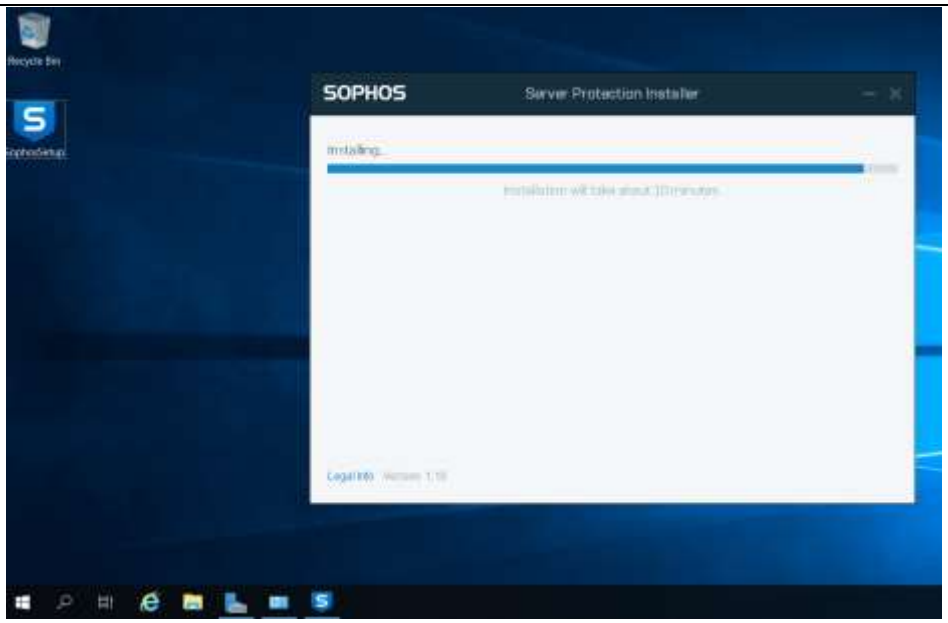
Installation

Since we will be securing the Windows File Server in this instance, we will be downloading the Windows Server Installer.

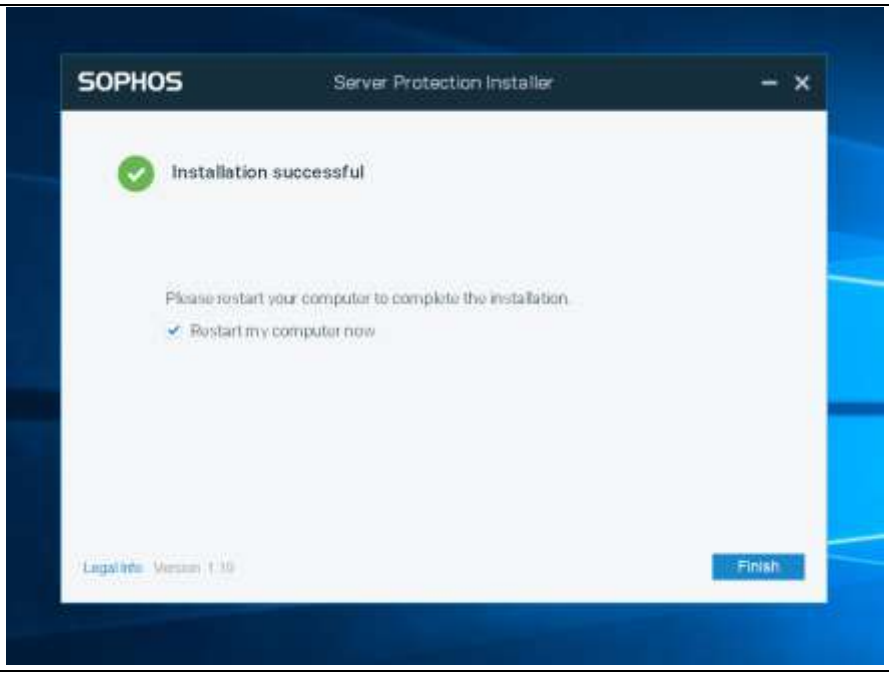


After the setup executable is installed, the DNS settings need to be changed and NAT should be enabled on the file server to allow for the AV program to be installed. In this case DHCP is configured and thereafter disabled after successful installation.

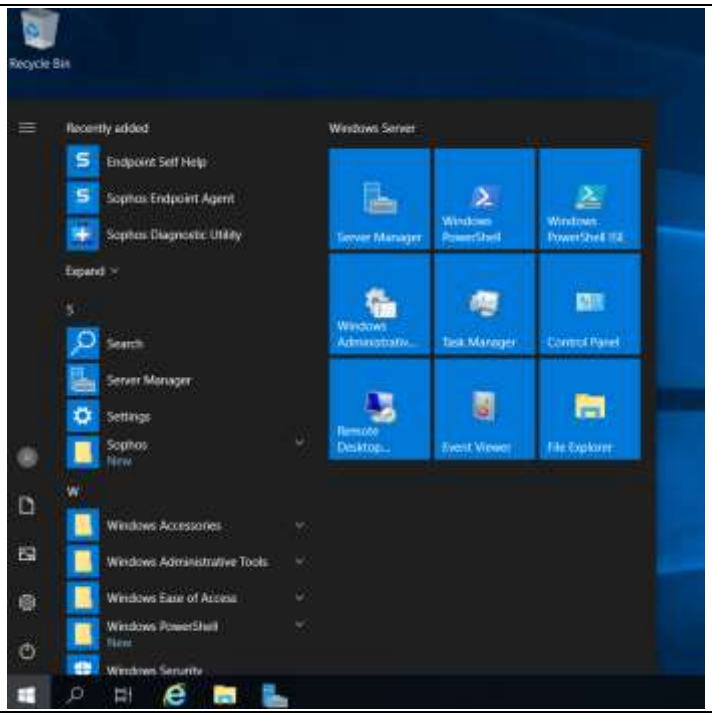




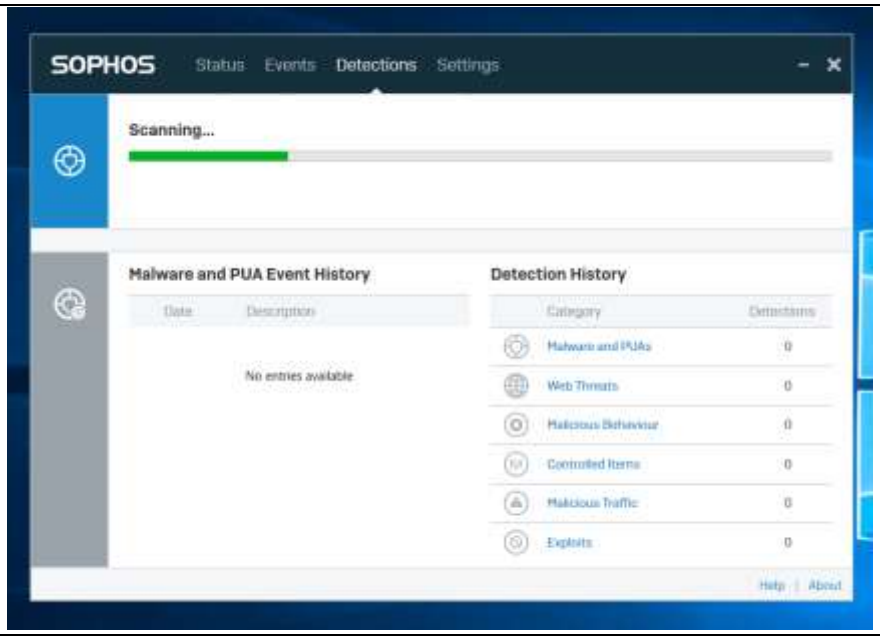
The screenshot above shows the endpoint application being installed. Once the install is completed, a machine restart is required.



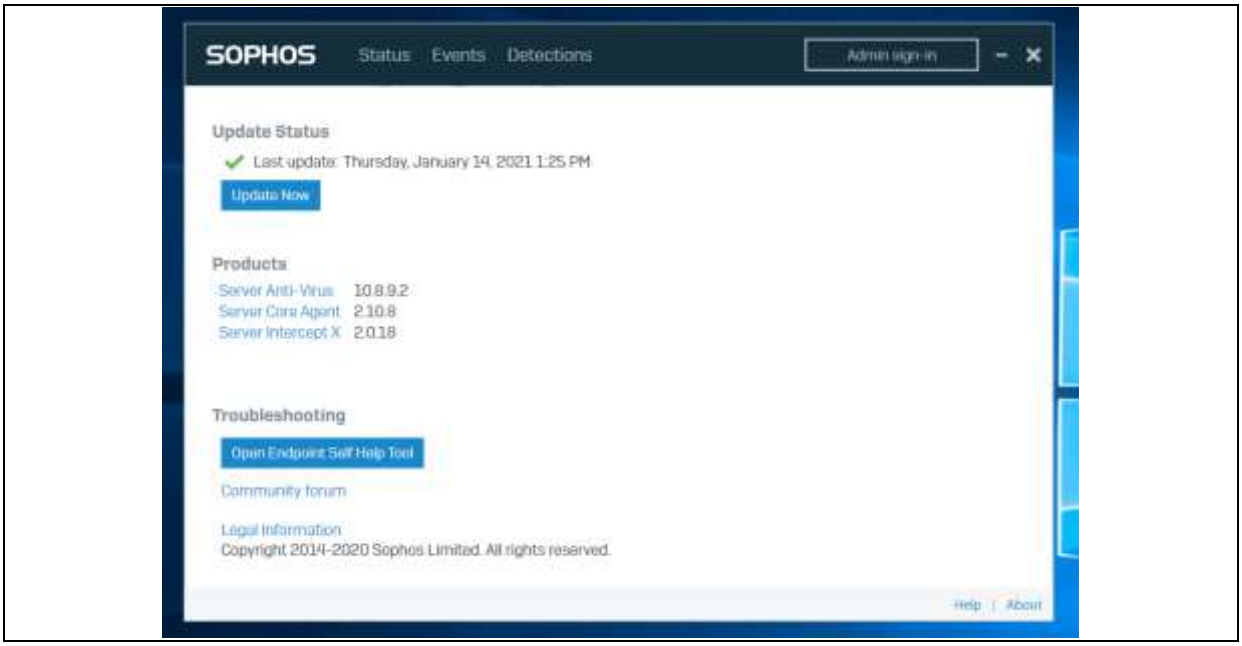
Thereafter, the product can be launch using the Windows Start Menu.



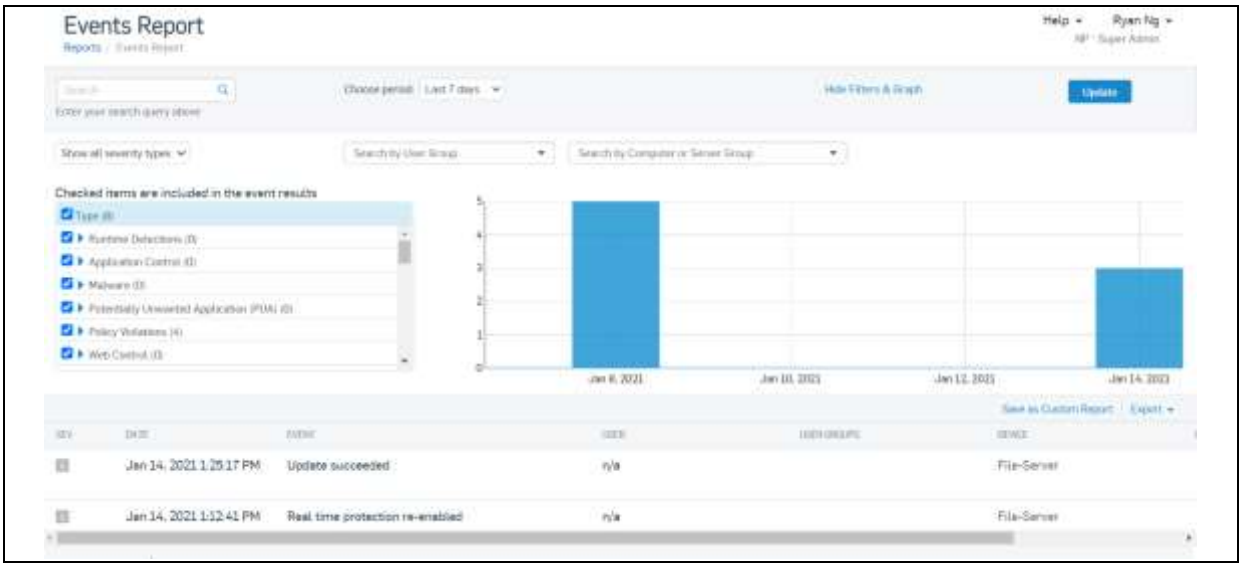
Manual scanning can take place as shown below. The antivirus software uses a combination of signature and anomaly-based scanning to identify malware, web threats (supposing the administrator/another user uses the browser), malicious behaviour and traffic and exploits that have yet to be patched on the server, which would be a useful tool in conducting preliminary vulnerability scanning before using a dedicated tool later on like Nessus to do more in-depth scanning.



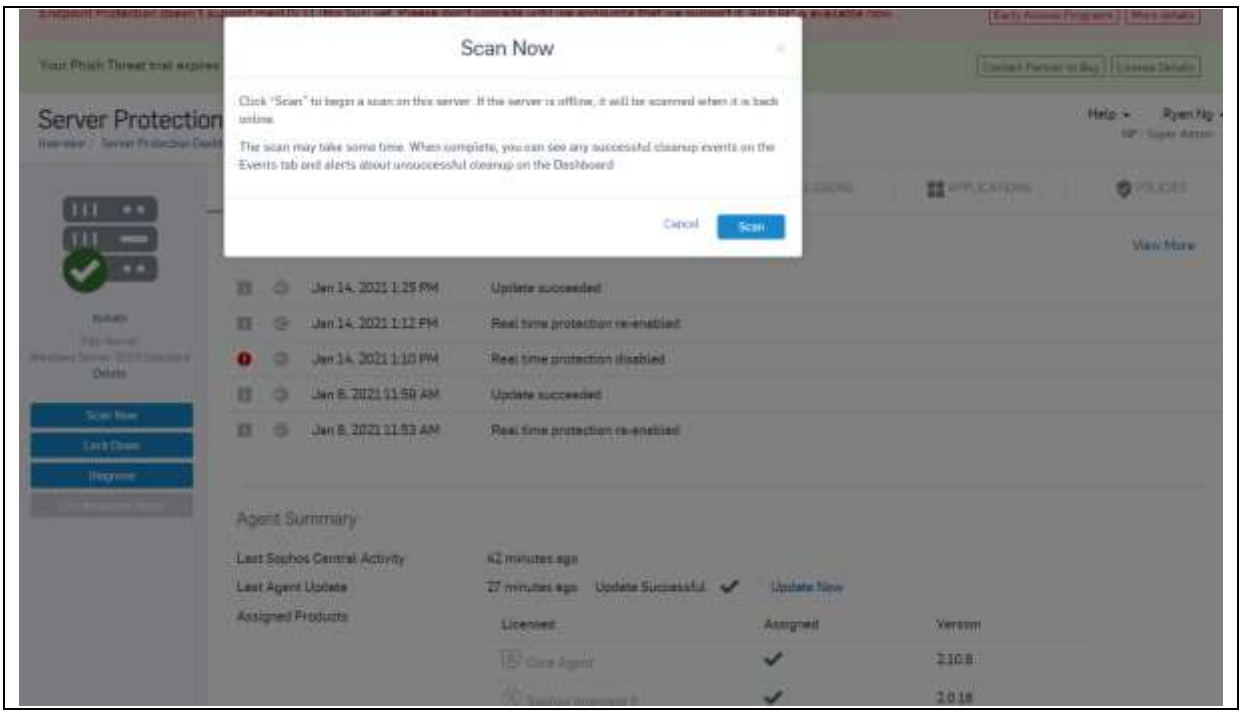
Under the “About” pane on the bottom left corner, the update status, installed products as well as the list of install products and plugins.



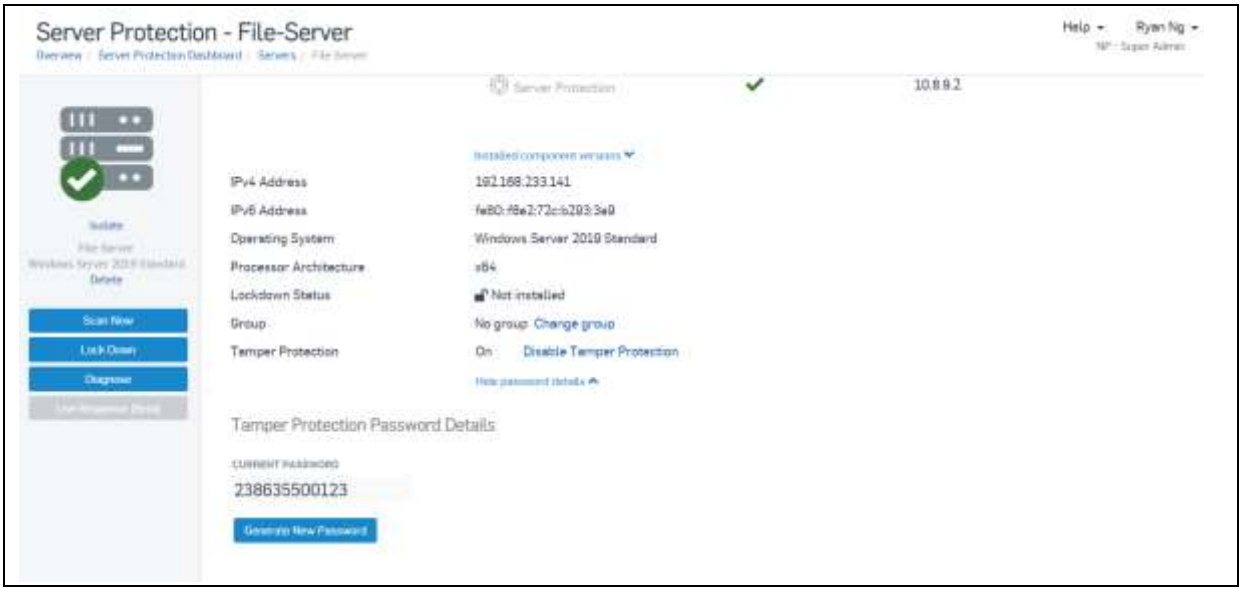
In Sophos Central dashboard, various reports about the device’s security will be generated. For the server variant of the antivirus software, additional information such as policy violations and application control logs can be displayed.



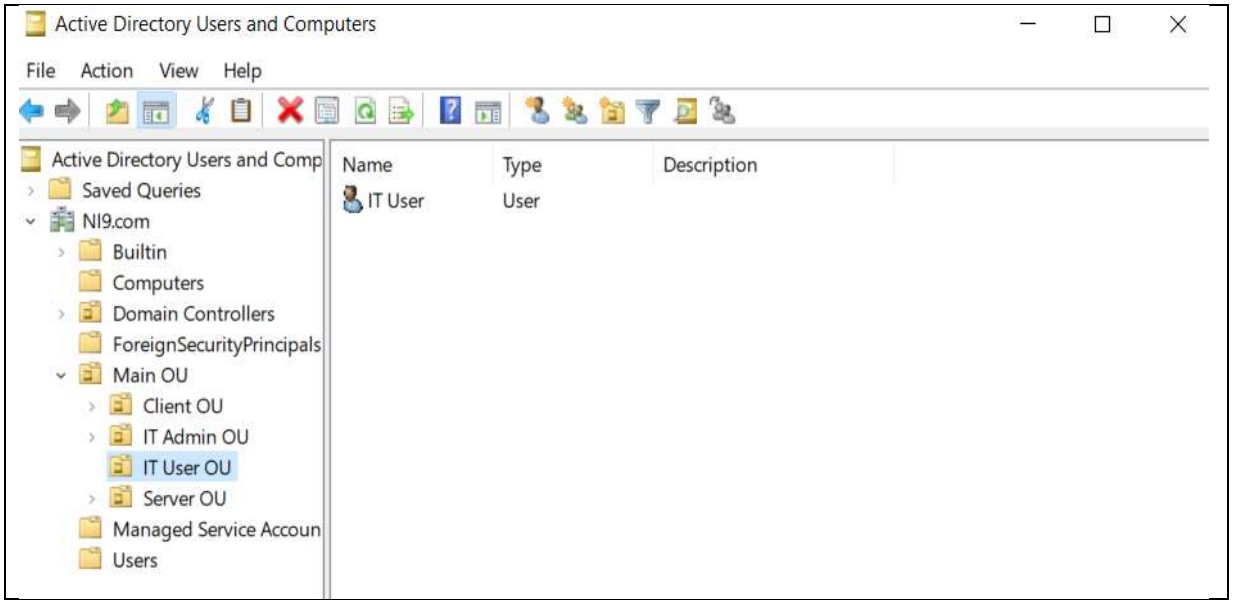
The administrator can configure the antimalware product to scan for malware on the software automatically via the dashboard or manually after logging into the server.



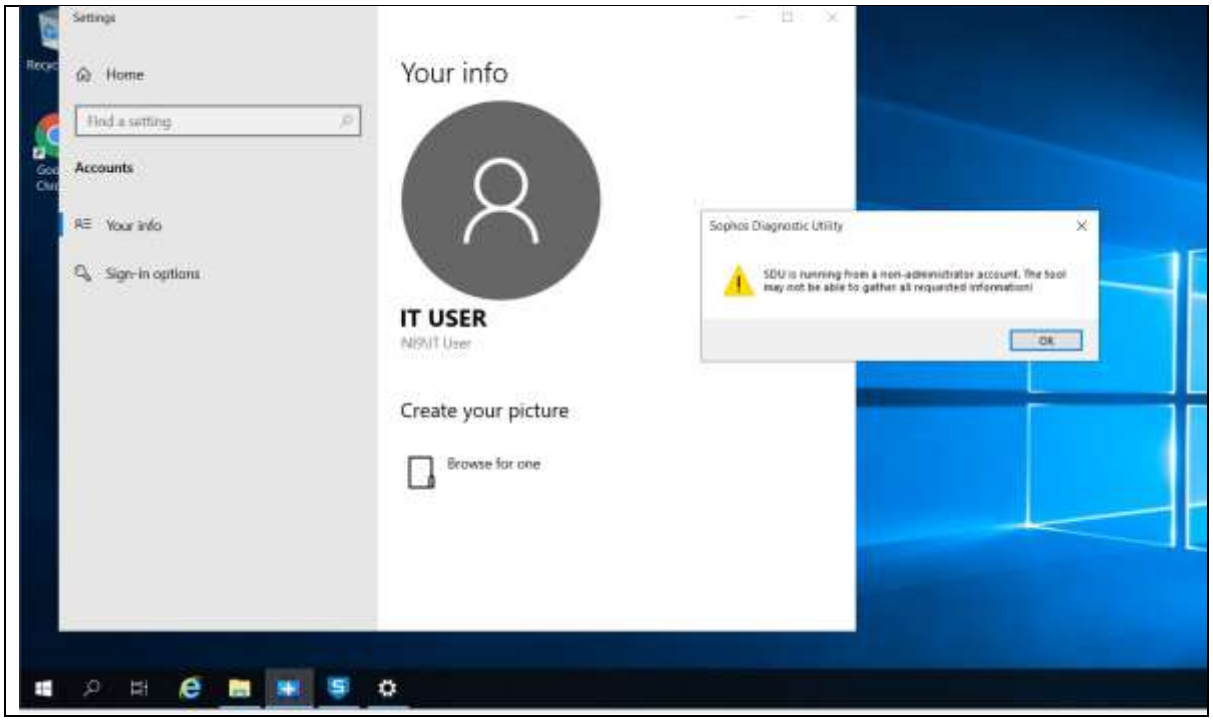
There is also the option to view the general information about the server once it is connected to the Sophos Central such as the IP Address, Operating System, and additional features such as machine lockdown and tamper protection (prevents non-admin users from deleting or modifying the AV software).



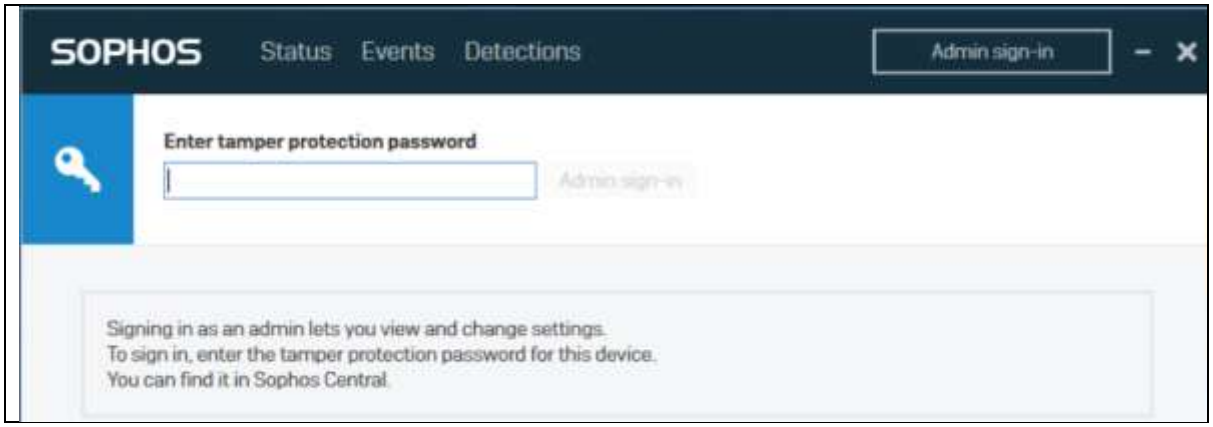
In the instance of my file server, I have an IT User (who is not an admin), as a regular user object configured in the Active Directory Users and Computers



When trying to run the Sophos Diagnostic Tool using the IT user's account, this is not possible.

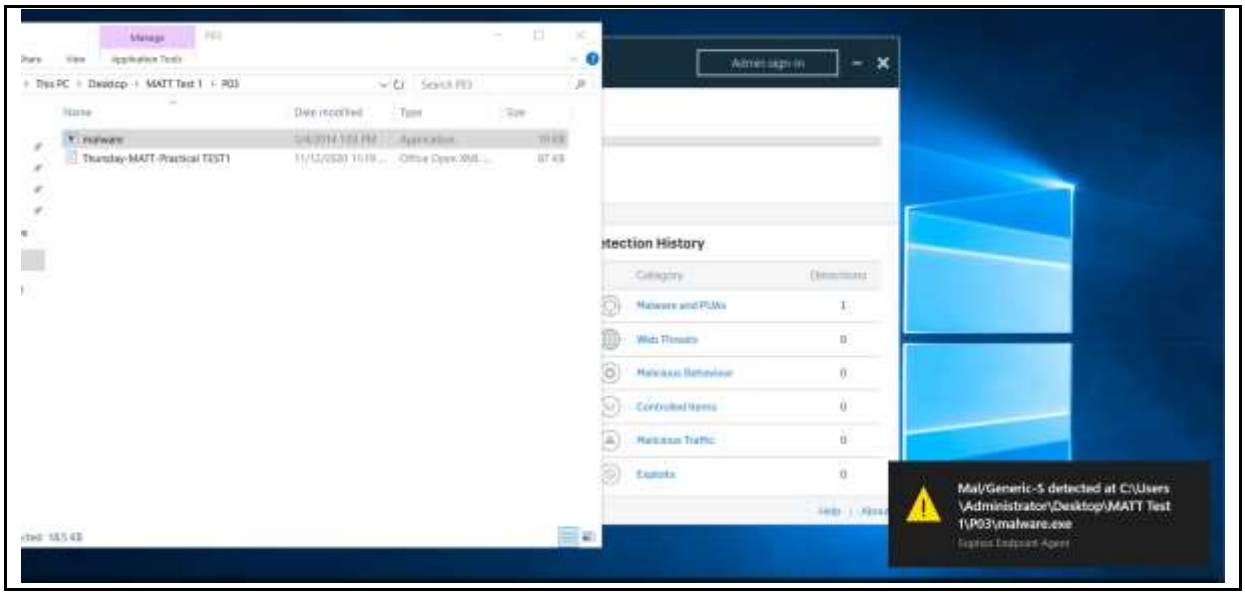


Furthermore, the tamper protection password, which should be only available to the administrator of the domain NI9.com in Sophos Central means that the user will not be able to change important settings within the application itself.



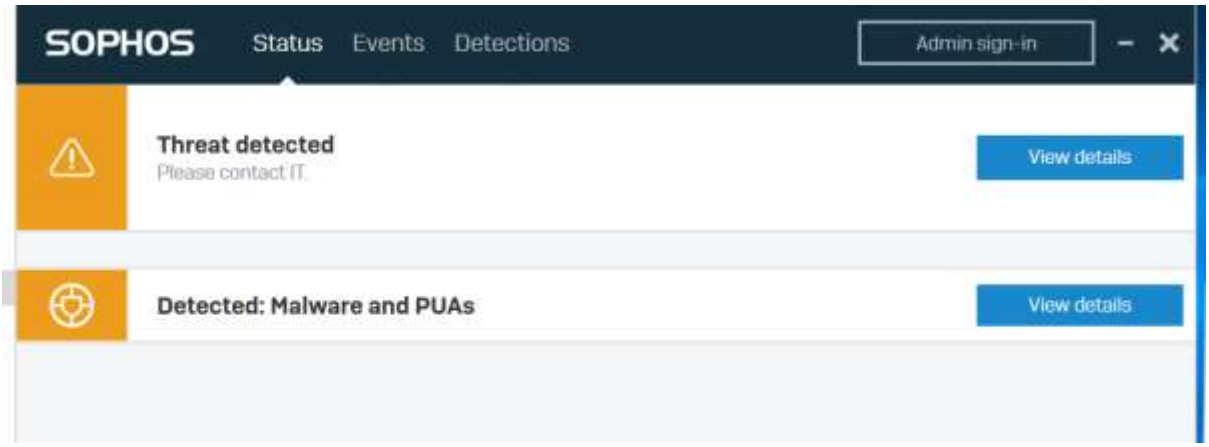
Automatic updates to the server endpoint AV tool can also be configured and scheduled, which is useful in an enterprise environment (allows for centralised updates to all servers).

Evaluation of Effectiveness of Antimalware Software

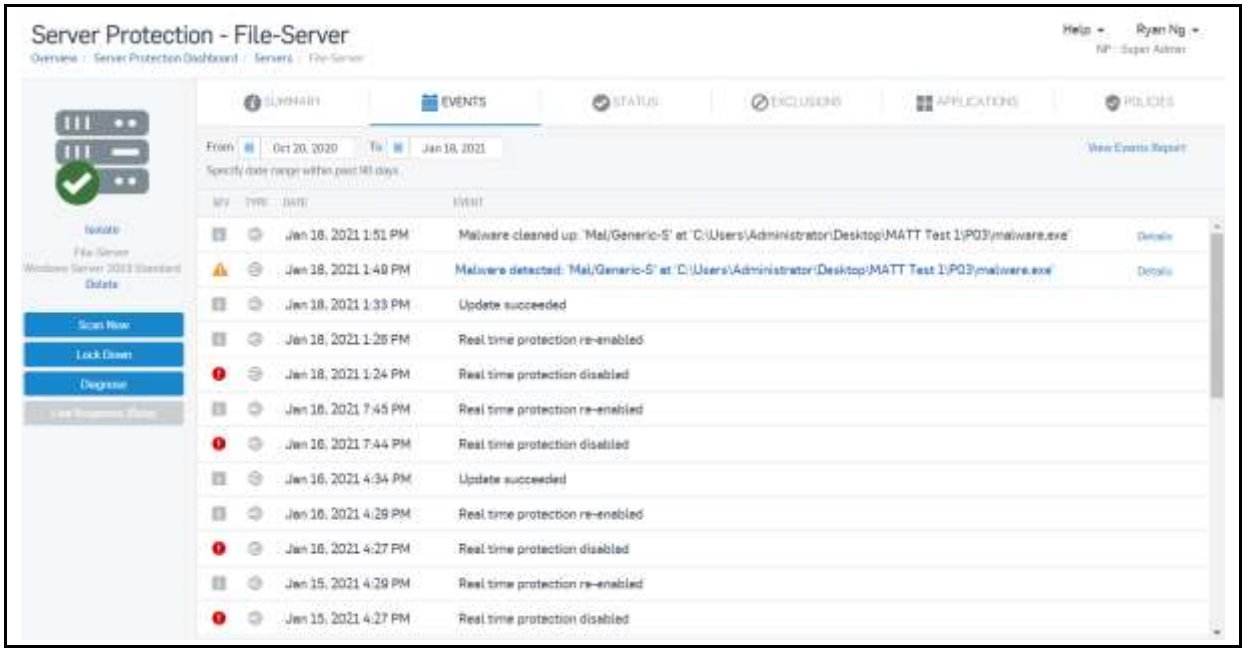


To test the effectiveness of the antivirus, we used a Windows 10 malware from a MATT assessment (Windows Executable). Sophos managed to pick up and warn us about the file after it had been unzipped. Thereafter the AV removed the malware.

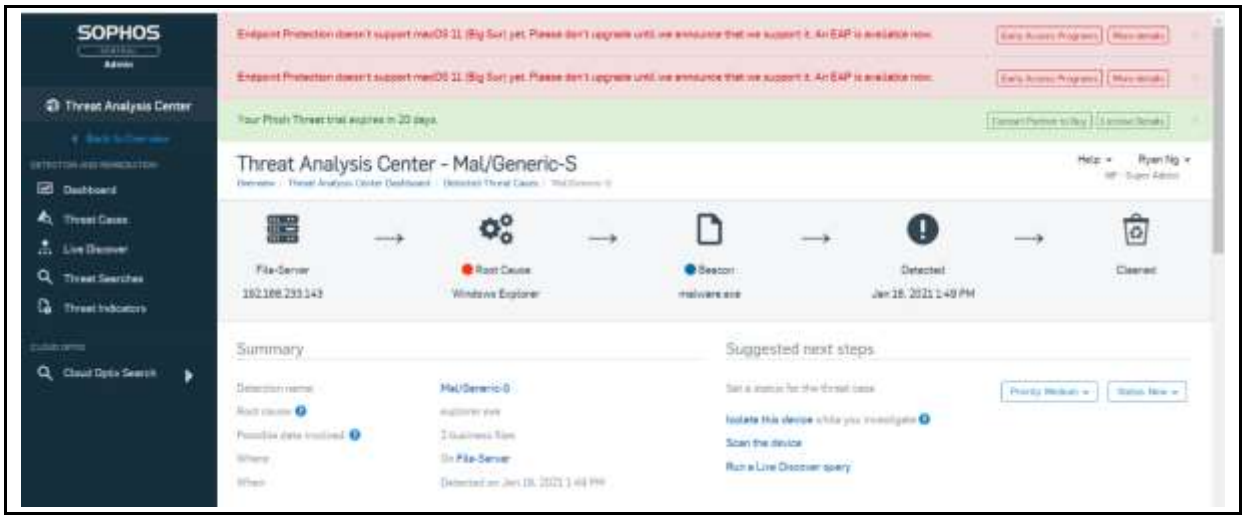
The AV also managed to pick up a malicious pdf file after it had been unzipped as shown below.



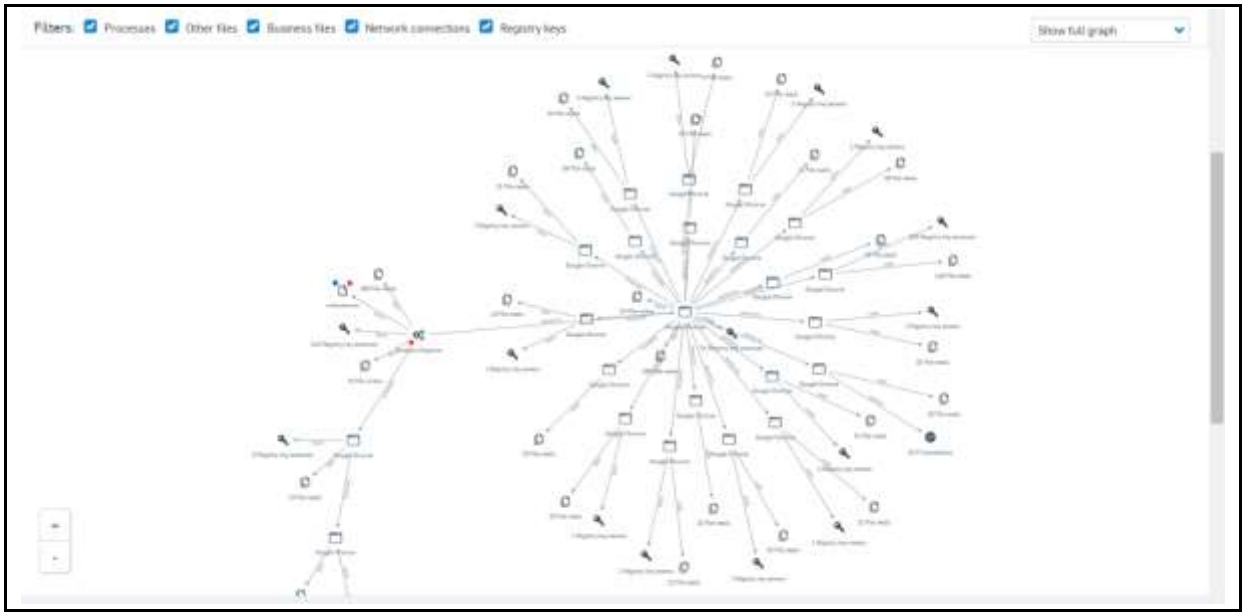
When the endpoint cannot remove the malicious file, it will prompt for IT support to be given and the similar notifications will be reflected on the Sophos Central dashboard indicating that the situation requires further attention of the administrator if the Sophos Server Endpoint Agent is unable to remove it.



The server event log shows the AV-related incidents happening on the server itself, including updates, real time protection and malware detection. This form of automated logging helps companies in audits and comply with legislation and company policies.

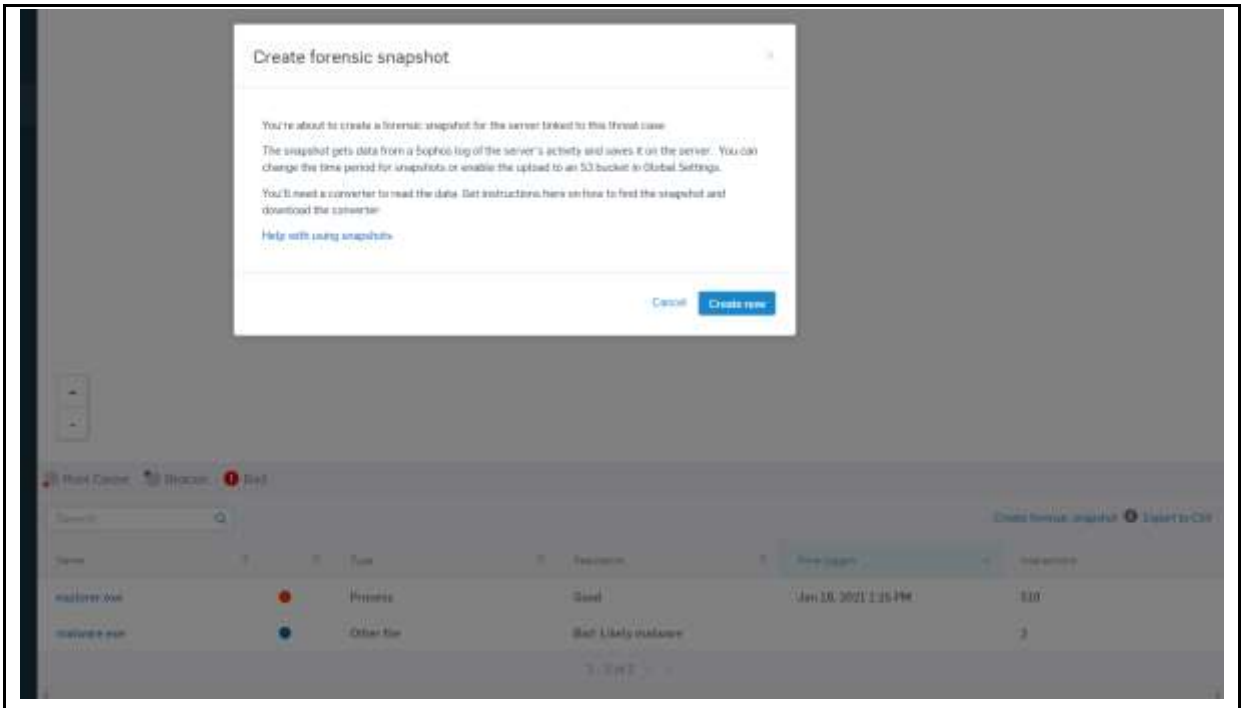


The successful malware detection (for the first case involving malware.exe) is also available and logged in Sophos Central as shown above. A detailed report including network connections can also be generated as shown below.



Sophos Central has in built Data Loss Prevention Policies, but not specific to Singapore, thus other DLP software need to be used to configure Singapore-specific policies to comply with regulations such as PDPA.

Forensic snapshots can also be taken in case a forensic investigation is needed later on, which can be useful in responding to incidents involving the server.


Create forensic snapshot
Cancel
Create new

Data Loss Prevention

In any file server, a DLP is an essential tool that must be implemented. DLP can be implemented at the endpoint (user) to ensure sensitive data is not shared with others, in motion (network) to ensure data is not visible by others and goes only to the specified users, at rest (data storage) to ensure contents are not modified in disruptions.

For this assignment, we are implementing the DLP tool on our file server. Therefore, we will use a DLP for data at rest. Although, our Sophos Server Protection already has its own built-in DLP, it is best practice to install a standalone software for each security function. By having a diversity of sources, we are able to minimise the effect of a breach of a single software provider by maintaining the rest of our security functions.

We first searched online for DLP software for servers. We came across a few such as CoCoSys, Symantec, MacAfee, Check Point, SecureTrust and SolarWinds. The majority of them offer custom solutions and require prospective customers to contact them for a quote. For the few which claim to offer free trials, these ended up to be sales pitches via email and an offer to demonstrate the software over video conferencing. SolarWinds was the only vendor which allowed downloads for a free trial. However, given the recent security lapses and controversies regarding SolarWinds, we decided not to use their software.

We instead ventured online to find an open source DLP tool. We came across MyDLP and OpenDLP. However, as MyDLP is no longer open source, we decided to go with OpenDLP.

OpenDLP is a free and open source, agent-based, centrally managed DLP tool. OpenDLP works as a web application on Linux which then remotely scans the Windows target machine.

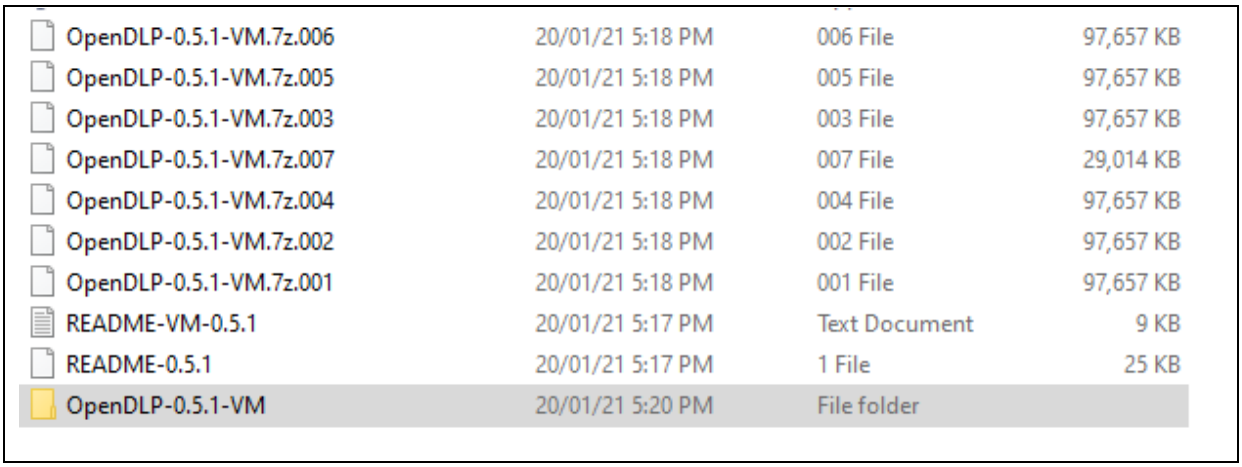
Unlike the other tools we used for this assignment, which are generally plug and play, easy to install and configure using GUI, OpenDLP is not installed on the file server. Instead, it is installed as a virtual machine on a separate computer and then used to remotely scan our server as an agent.

OpenDLP Installation Process

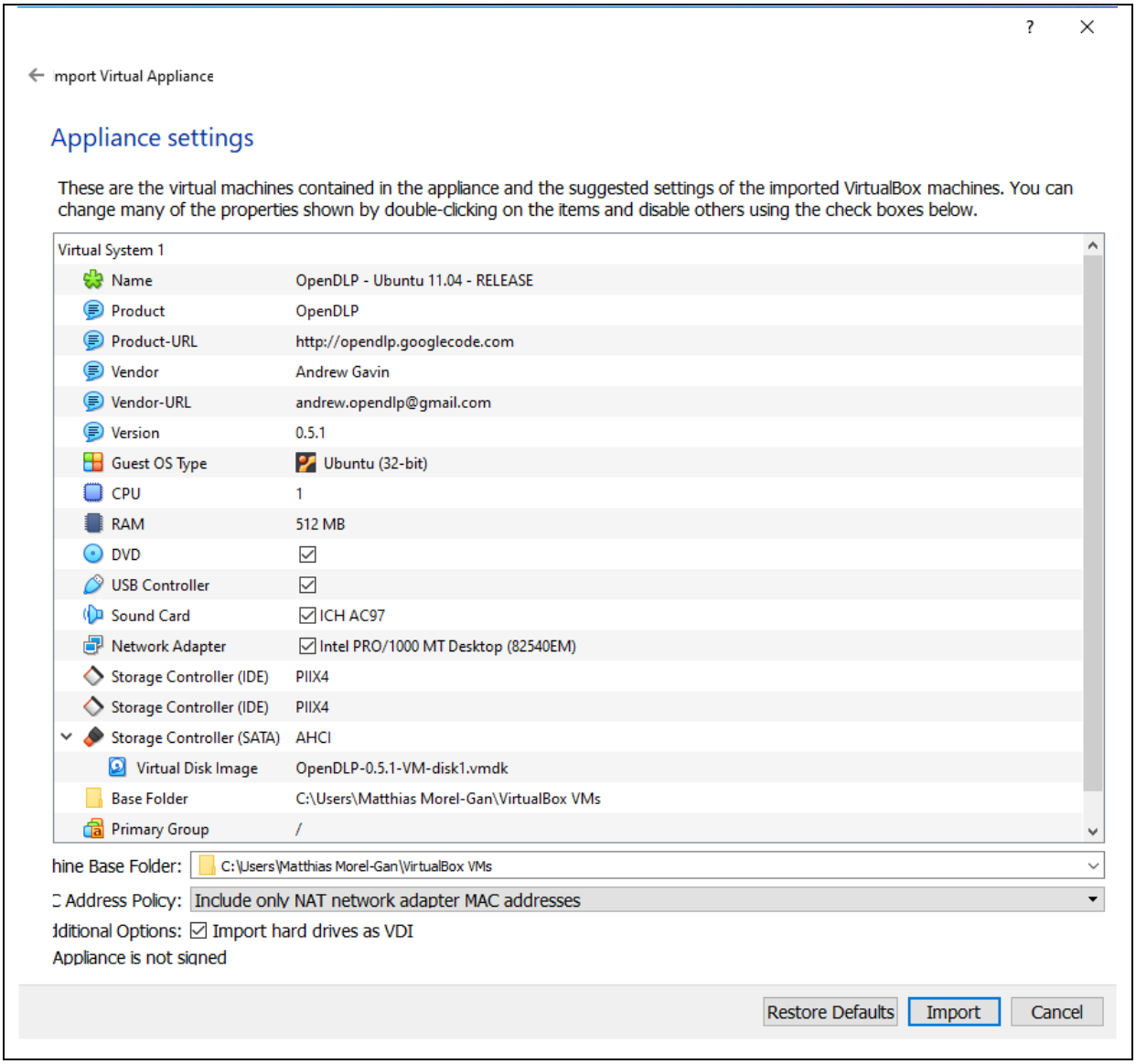
Step 1: In order to install OpenDLP, we must first install VirtualBox which can be downloaded from virtualbox.org.

Step 2: Download the Virtual Machine files from https://code.google.com/archive/p/opendlp/downloads

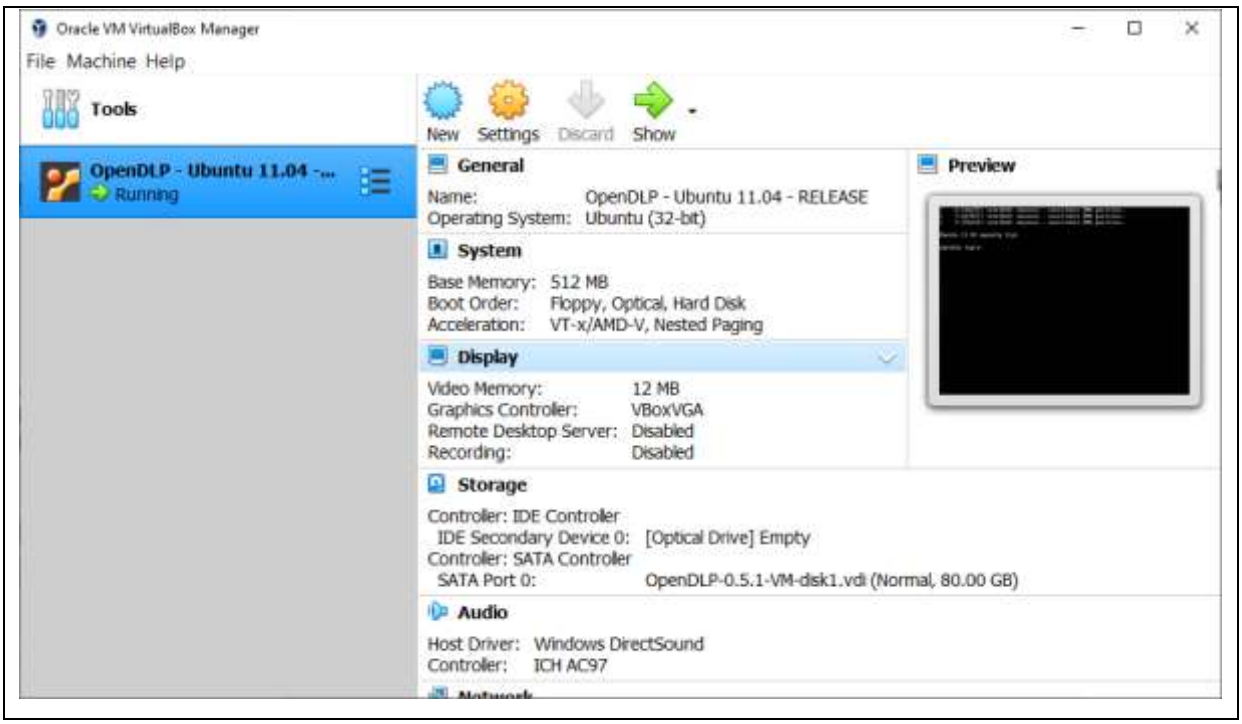
Step 3: Extract the 7 VM files into a single folder using 7-zip



Step 4: Launch VBox, click File, Import Appliances. Select the folder with the VM image. Check through the settings and click import.



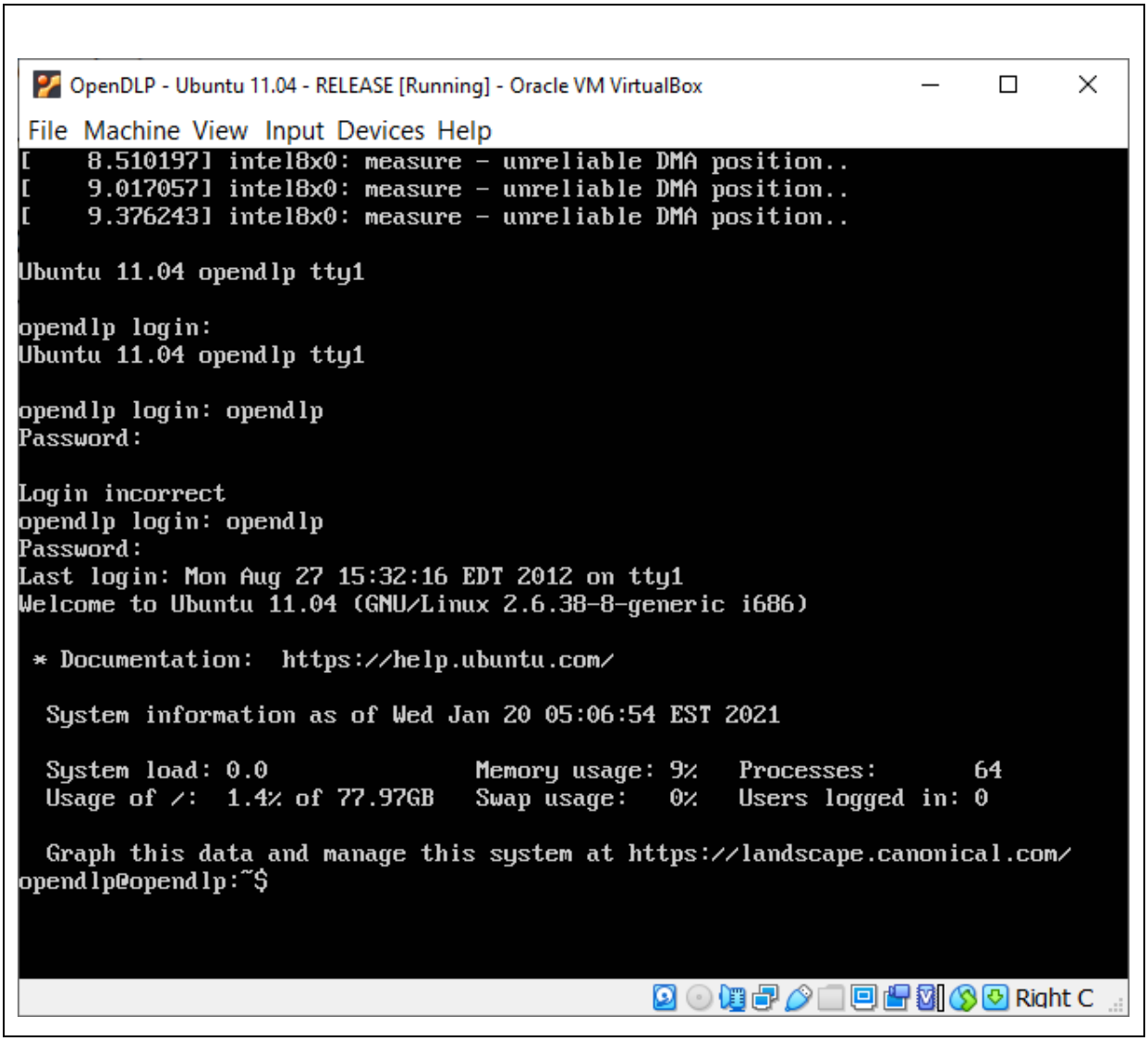
Step 5: The virtual machine will now appear in the VBox manager. Start the Virtual Machine.



Step 6: After starting up, the virtual machine will then ask for your login credentials. The defualt credentials are:

Username: opendlp

Password: opendlp



Step 7: If you do not see an IP Address, run the following commands to reset the network adapters:

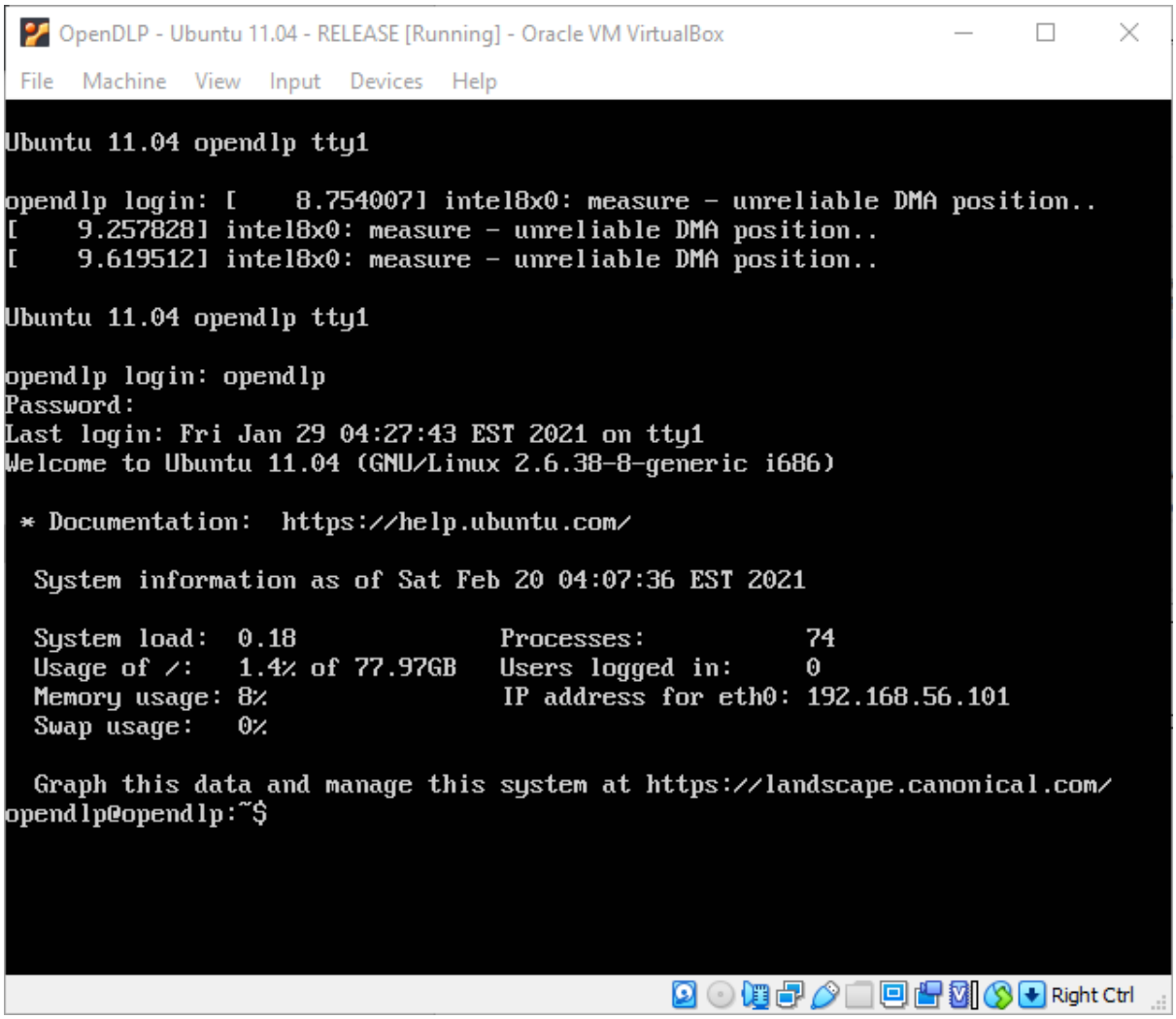
cd /etc/udev/rules.d

sudo rm 70-persistent-cd.rules

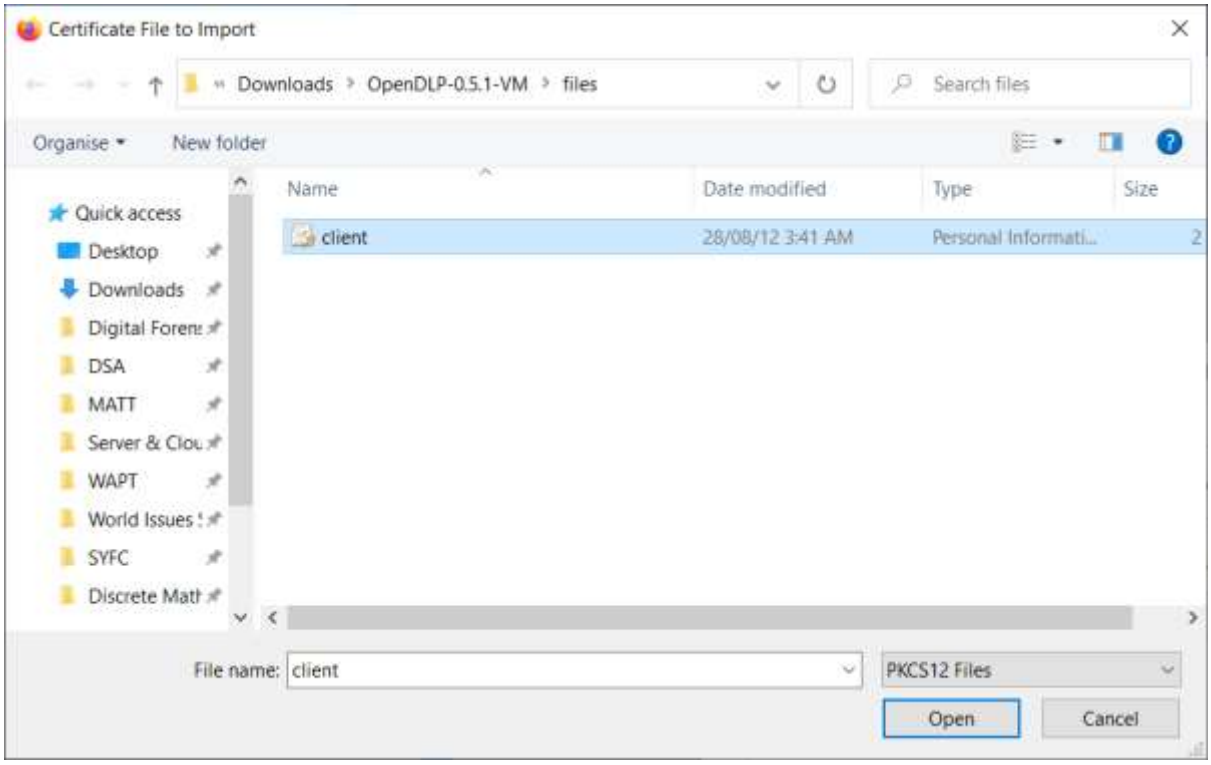
sudo rm 70-persistent-net.rules

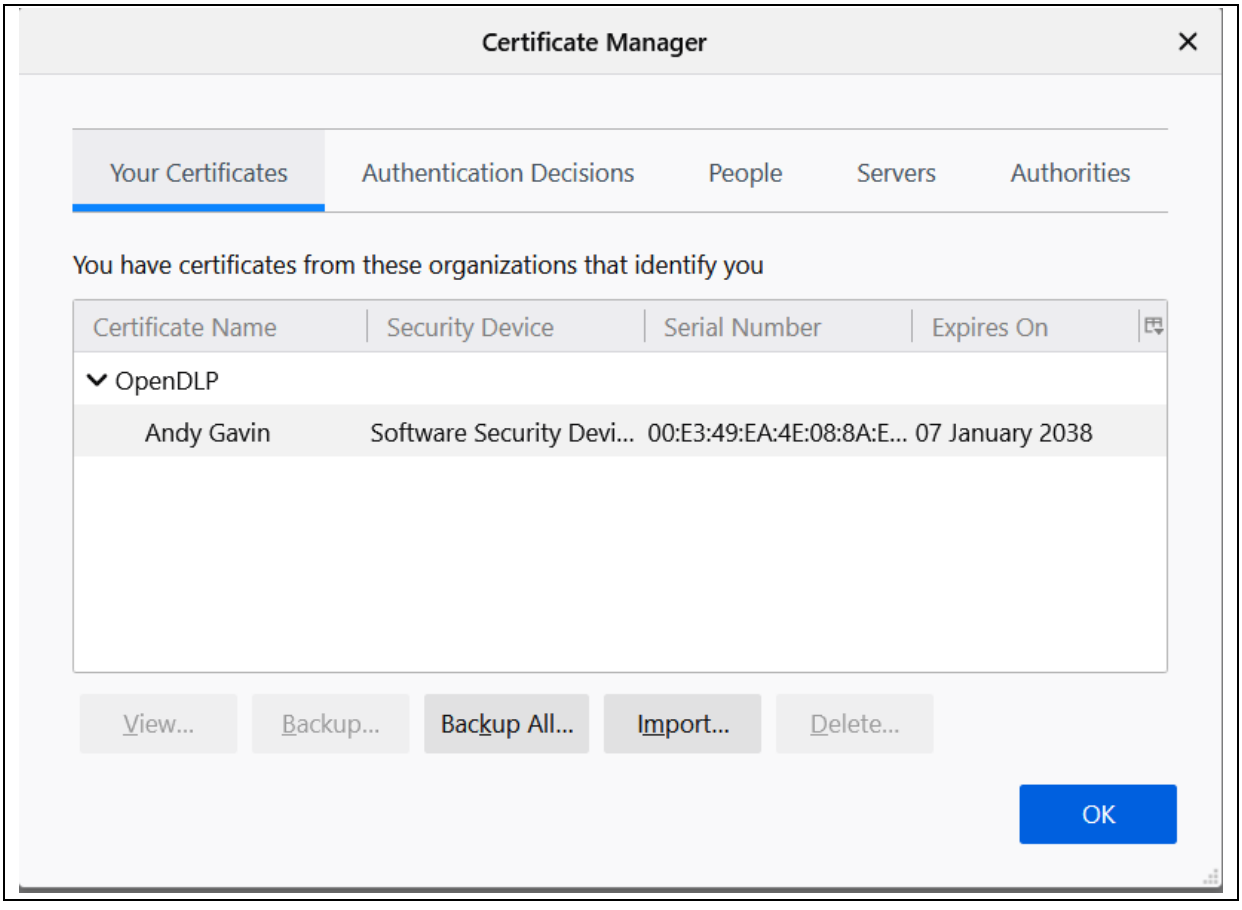
sudo reboot now

After which, you should be able to see an IP address as seen below:

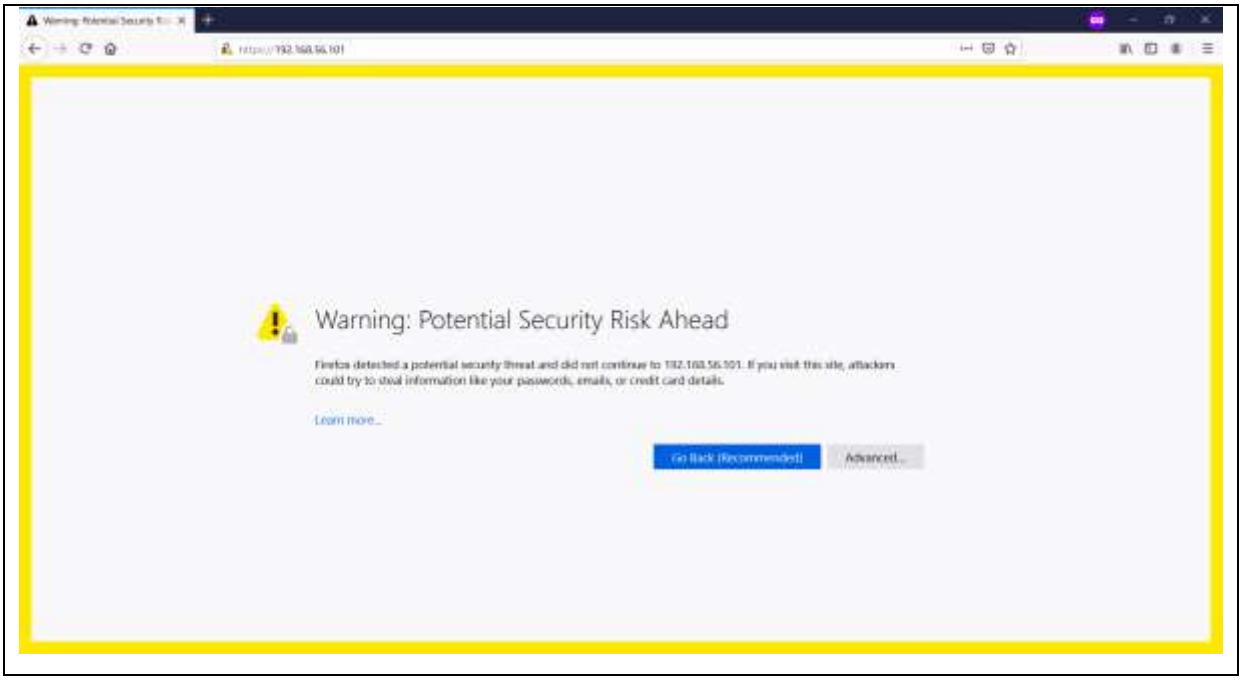


Step 8: Import the certificate to Firefox (on any machine)

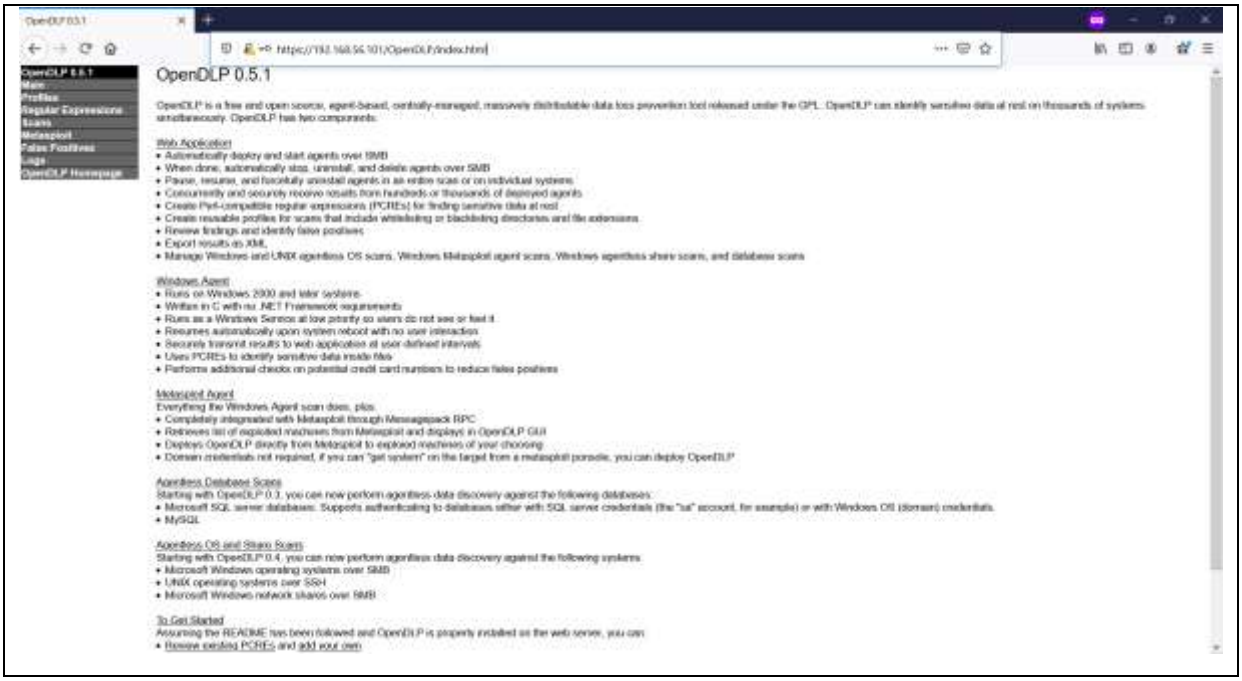




Step 7: Now, we can try connecting to our VM. Click Advanced, then enable TLS 1.0

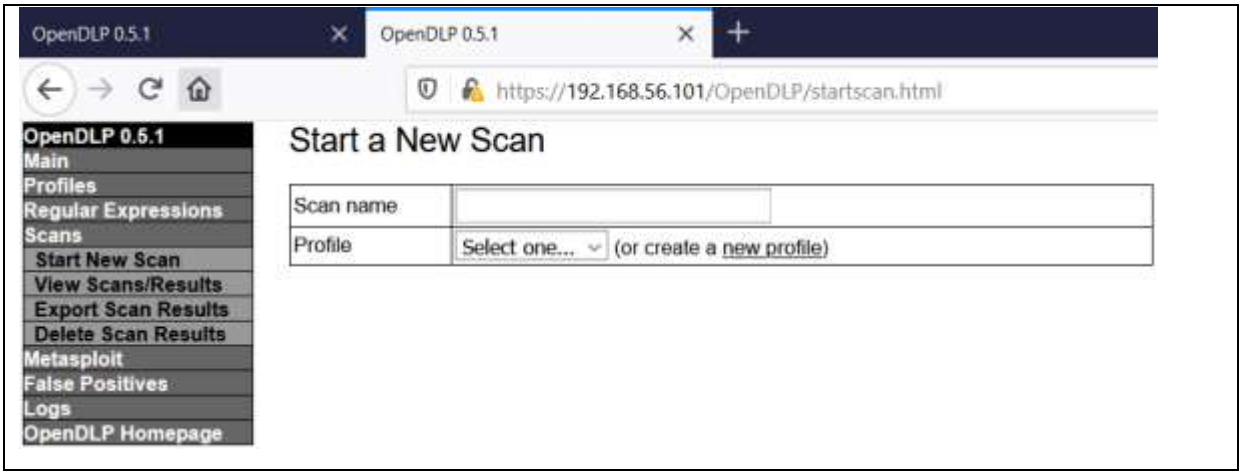


Go to **ip of vm/OpenDLP/index.html**

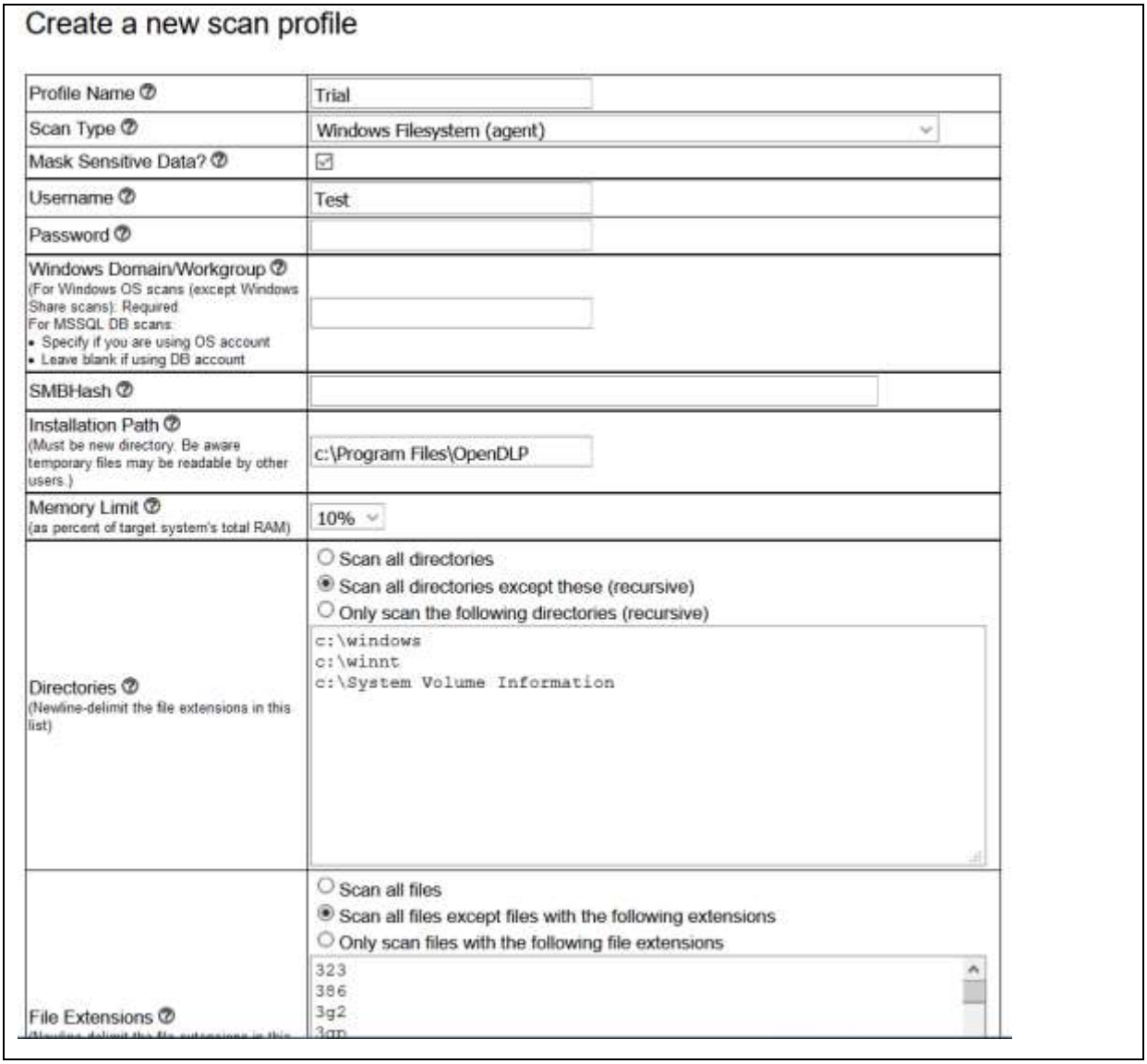


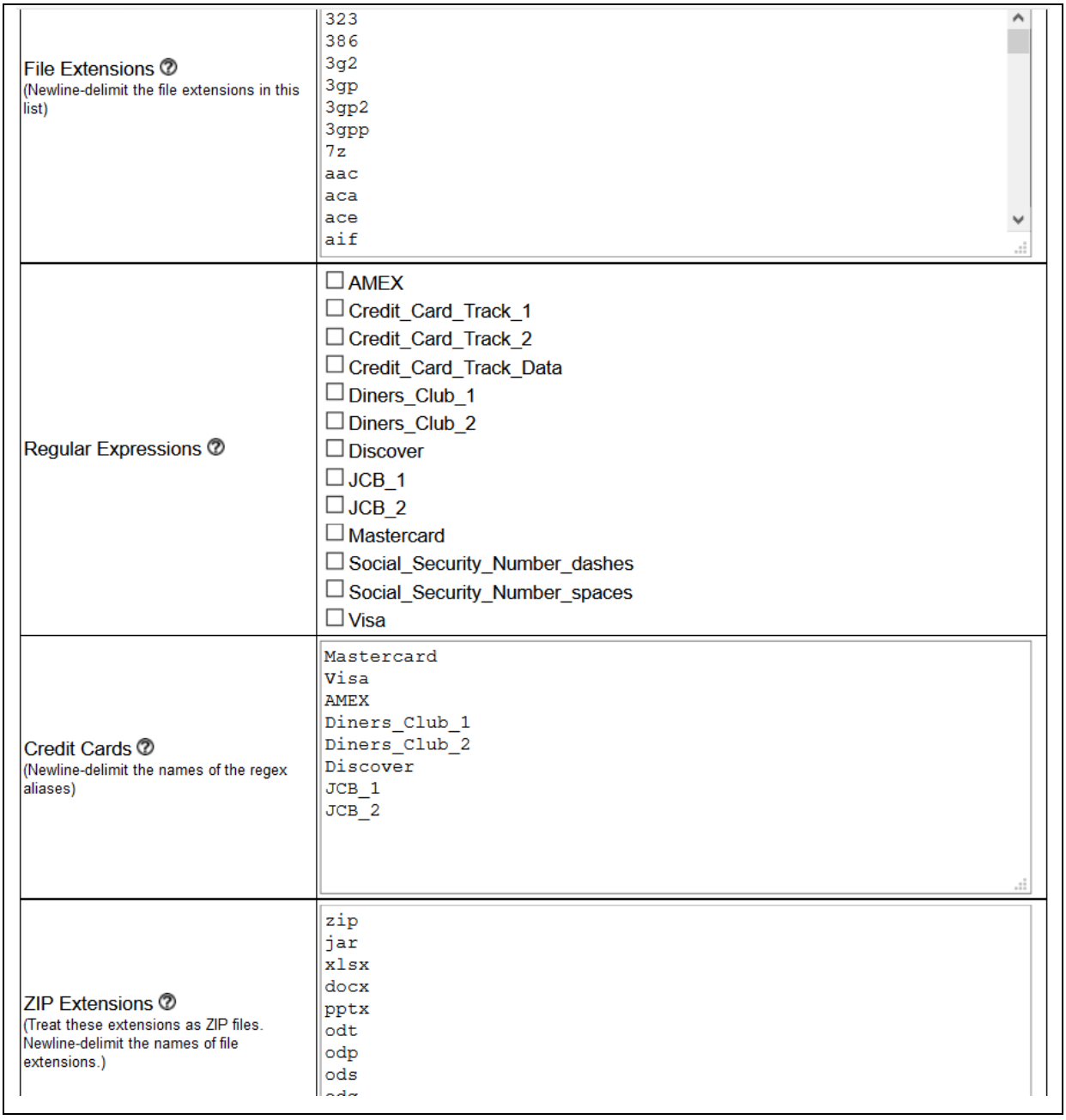
OpenDLP Scanning Process

Step 1: Go to **ip of vm/OpenDLP/startscan.html**



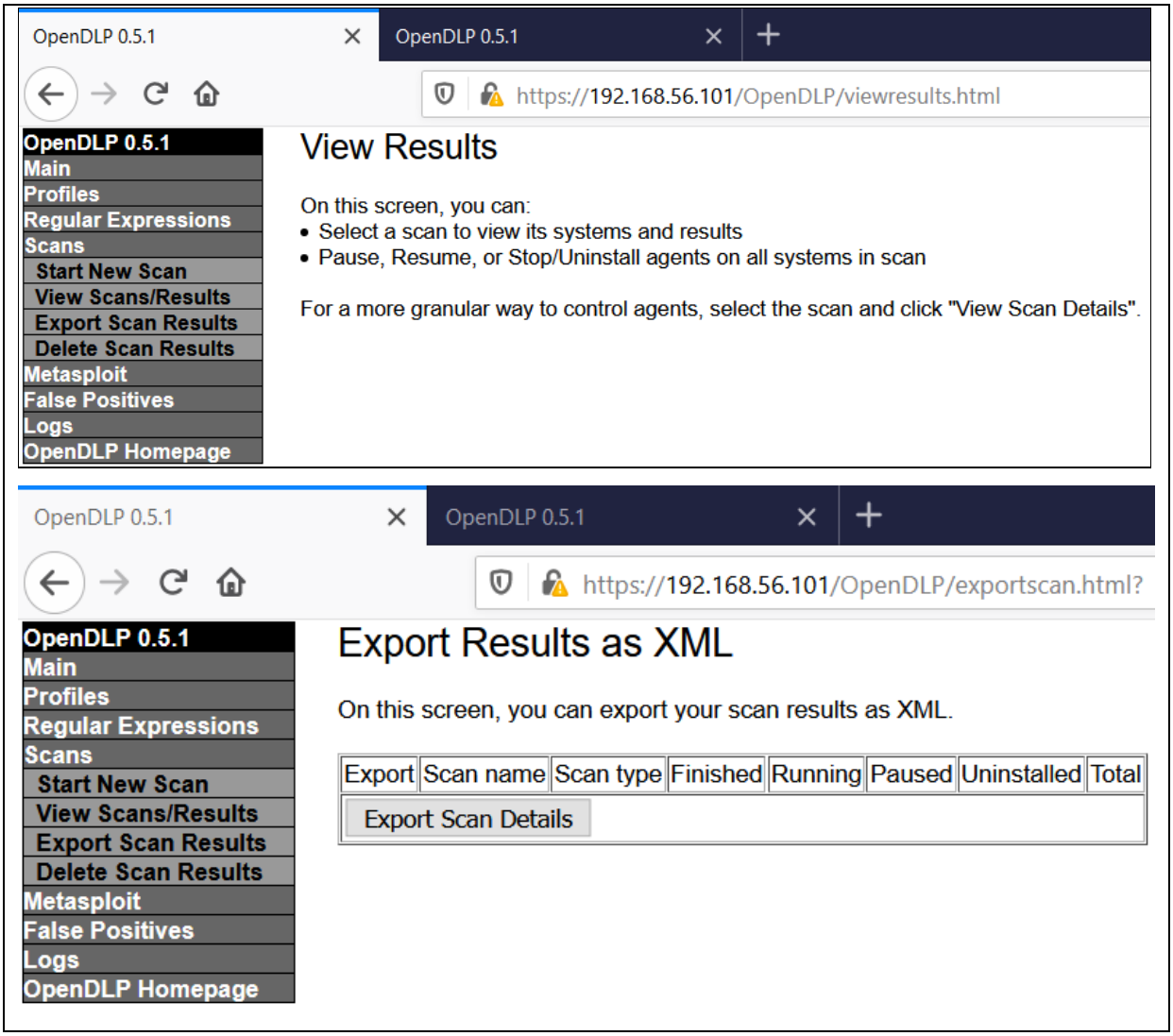
Step 2: Create a new profile (you will be re-directed to **OpenDLP/profiles.html**)





The user is able to select the directories they wish to be scanned.

Step 4: After scanning, the user is able to view the results and export them as XML.



In practice, OpenDLP is unable to scan our server as it relies on TLS 1.0 which is outdated and blocked by most computers.

OpenDLP Evaluation

I would say that finding and installing a Data Loss Prevention software on a non-enterprise set-up such as ours is a very frustrating experience. Firstly, when we attempt to get a trial of a DLP from reputable sources such as Checkpoint, Symantec, we instead get an email from a sales representative offering to schedule an appointment where they can demonstrate the software over video conferencing. This forced us to source for an open-source DLP instead.

Installing OpenDLP is a very frustrating experience, there were many times where I thought I could not install it and wanted to give up. In particular, I had to reset the network adapters on my host and OpenDLP multiple times. There were also some weird errors such as OpenDLP being able to ping our host but our host not being able to ping OpenDLP. I also had to enable TLS 1.0 on my host in order to connect to OpenDLP.

From a security standpoint, I seriously do not recommend installing OpenDLP and using it as a Data Loss Prevention software. I would say that you are better off not using any DLP than OpenDLP. As OpenDLP is an open-source software, it may carry inherent risks such as not being patched for known security flaws, or having hidden security flaws known only by a select few for malicious purposes. Furthermore, the use of outdated protocols such as TLS 1.0, and a self-signed certificate for connectivity, it is hard to have confidence in OpenDLP.'s security on its own.

From a usability standpoint, I would also say that OpenDLP has limited functionality. It only scans the file system directories and other regular expressions in the C:/ drive. It does not scan partitions or perform signature-based analysis to check for more minute changes.

In conclusion, I do not recommend using OpenDLP as it has limited functionality and we are unable to have confidence in its security. I would recommend enterprises to purchase a full-fledged DLP from a reputable source such as Symantec. For individuals and small businesses, I would say that it is safe to use the server with standard antivirus installed and storing sensitive information such as credit card numbers as hashes instead. Furthermore, it is hard to justify the business case of a DLP due to high cost and the need for custom solutions in most business settings.

Nessus Essentials Vulnerability Scanning Tool

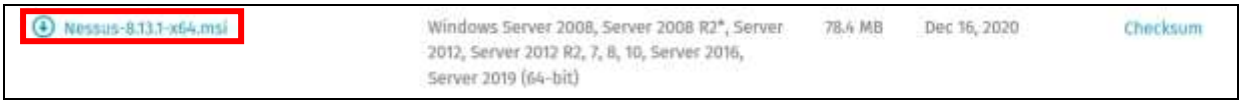
Nessus Essentials is part of the Nessus family; however, Nessus Essentials is a free vulnerability assessment tool which has limited testing capabilities. It can perform daily scheduled scans of different areas such as vulnerability scanning or malware. When performing daily scans, it can generate reports shows the administrator exactly what vulnerabilities were detected within the server and what are the recommended procedures to fix those issues.

Downloading Nessus requires some steps involving the workplace email, email verification and a registration key which is sent to the email upon registration. On the download screen, download the Nessus Essentials as this is the version used in this report.

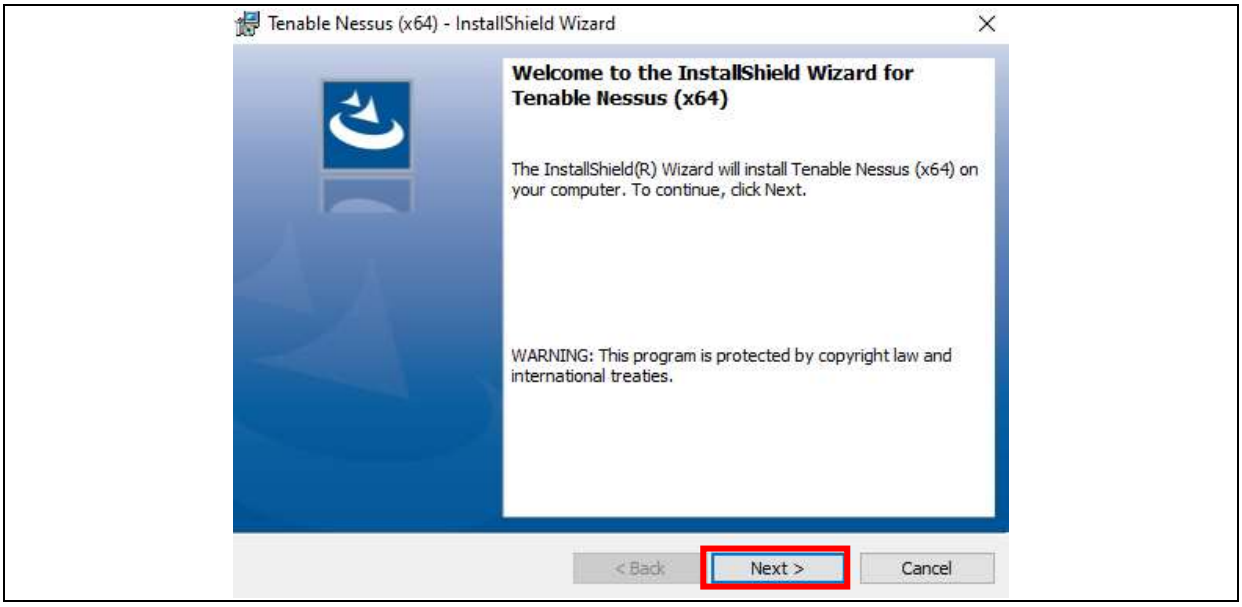
The reason why I choose Nessus to be used as a vulnerability scanner is because it has the advantage for quickly identifying and accurately identify vulnerabilities and recommend solutions and methods as to how to proceed to ensure that the system is kept safe.

Nessus Installation Process

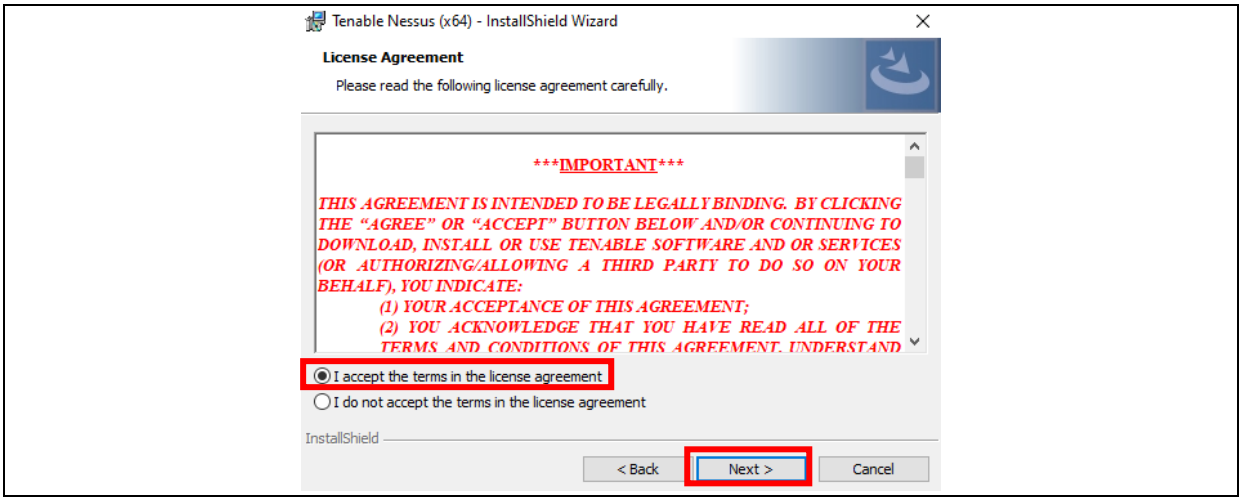
Step 1: Go to this website and download the latest version of Nessus for Windows Server. We downloaded “Nessus-8.13.1-x64.msi” as it was the latest version as of this assignment.



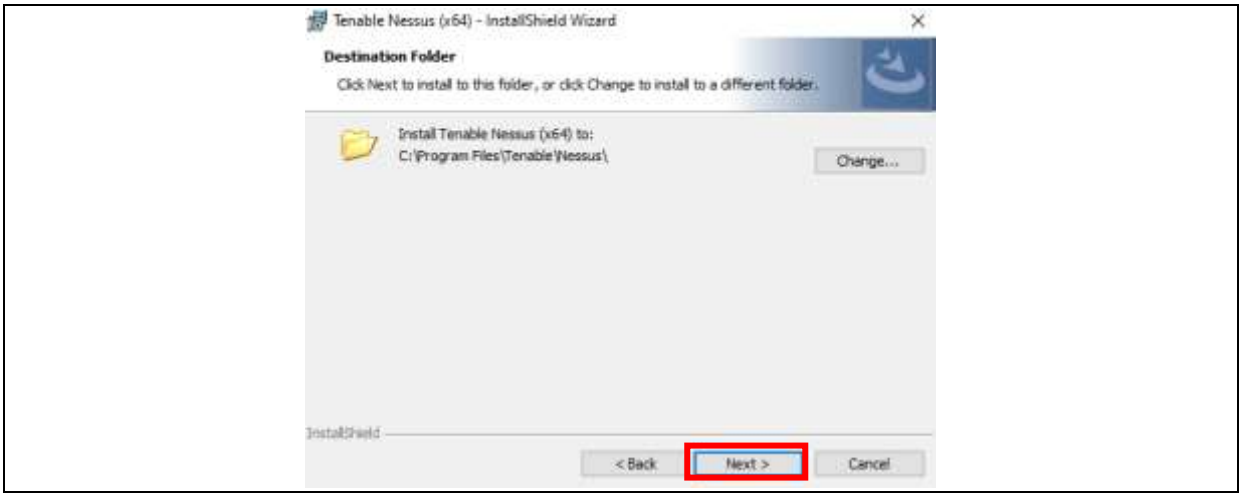
Step 2: Run the program and click “Next >”.

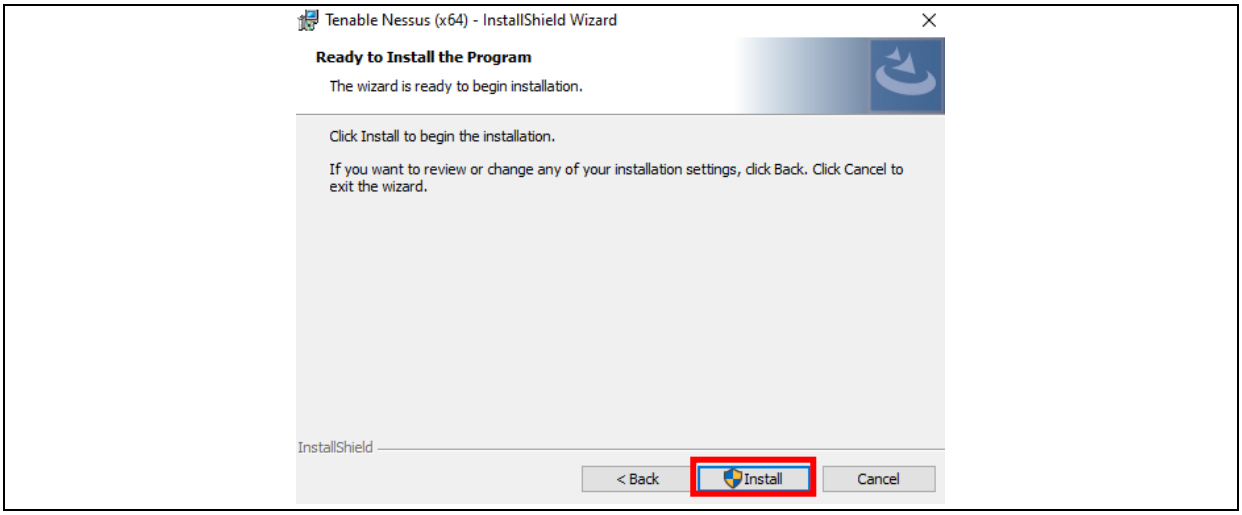


Step 3: Click on “I accept the terms in the license agreement” and click “Next >”.

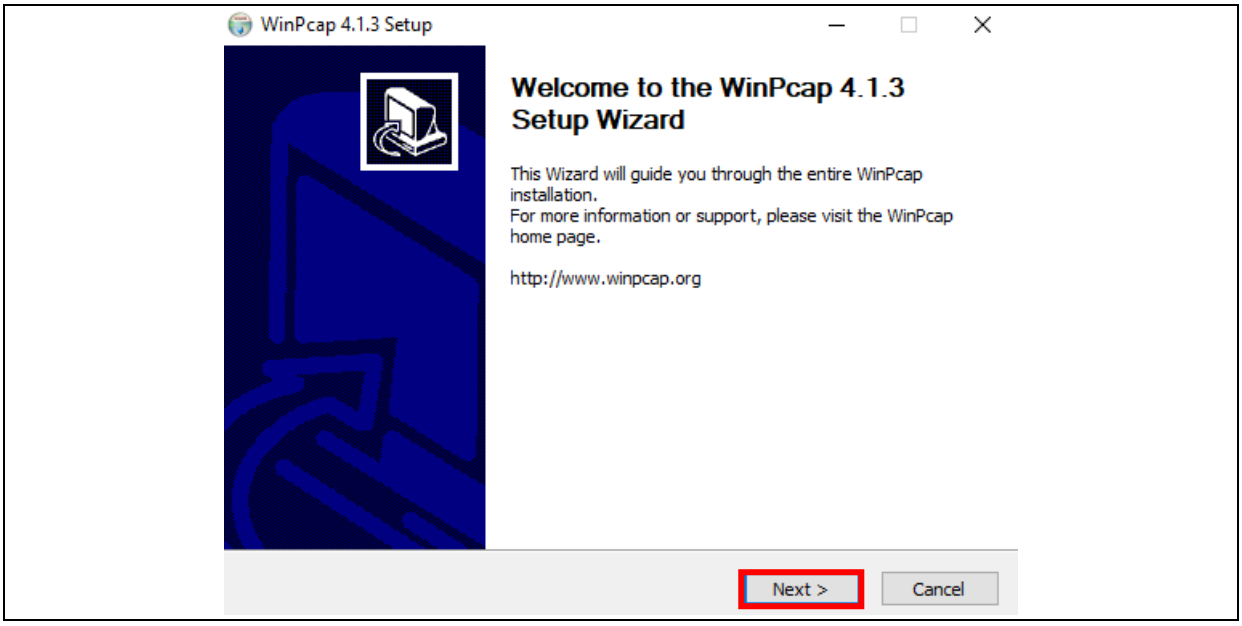


Step 4: Configure where the program should be installed and click “Next >” then “Install”.

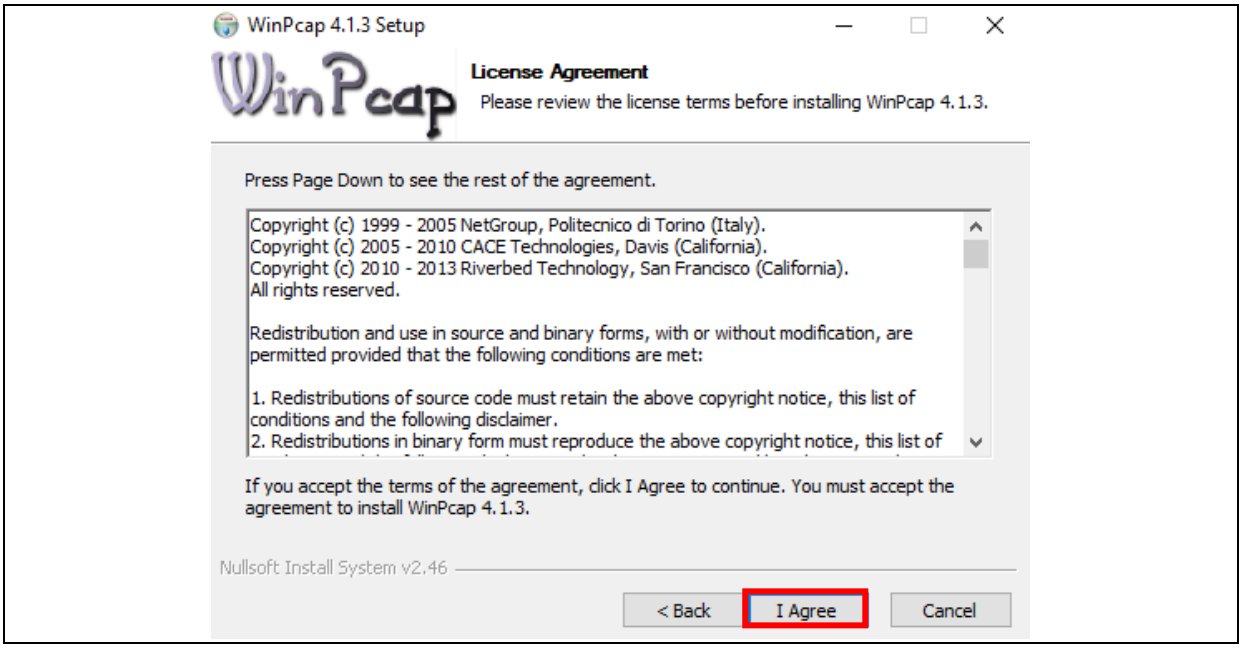




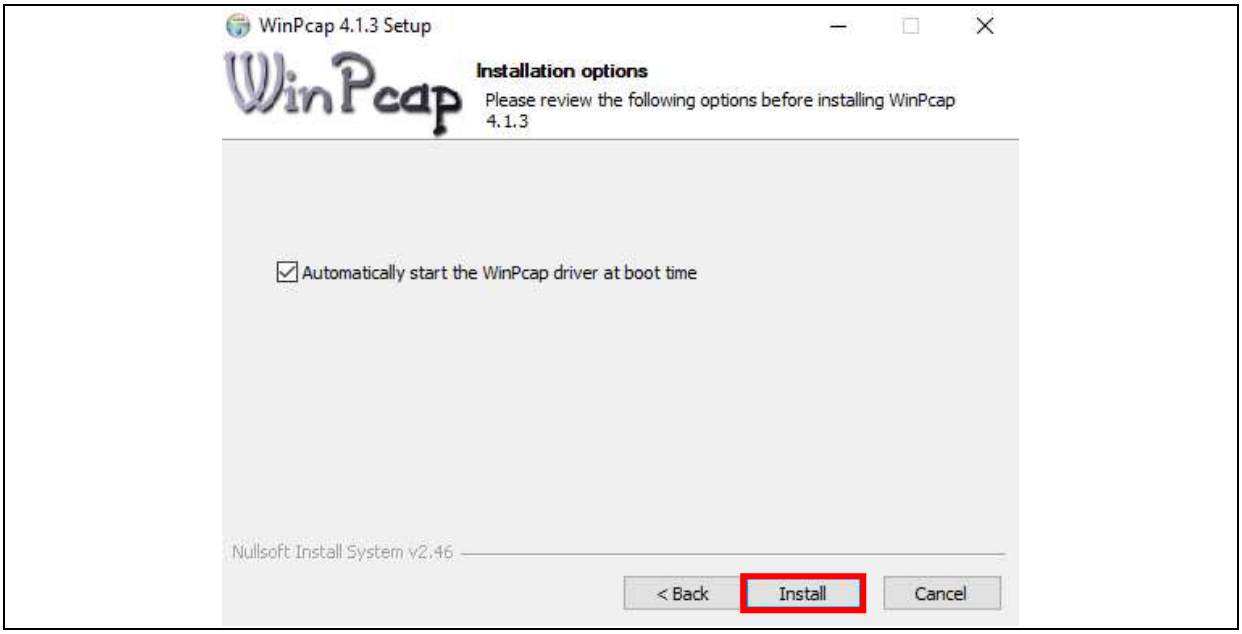
Step 5: There will be a pop-up to download WinPcap. Click on “Next >” to begin the installation.



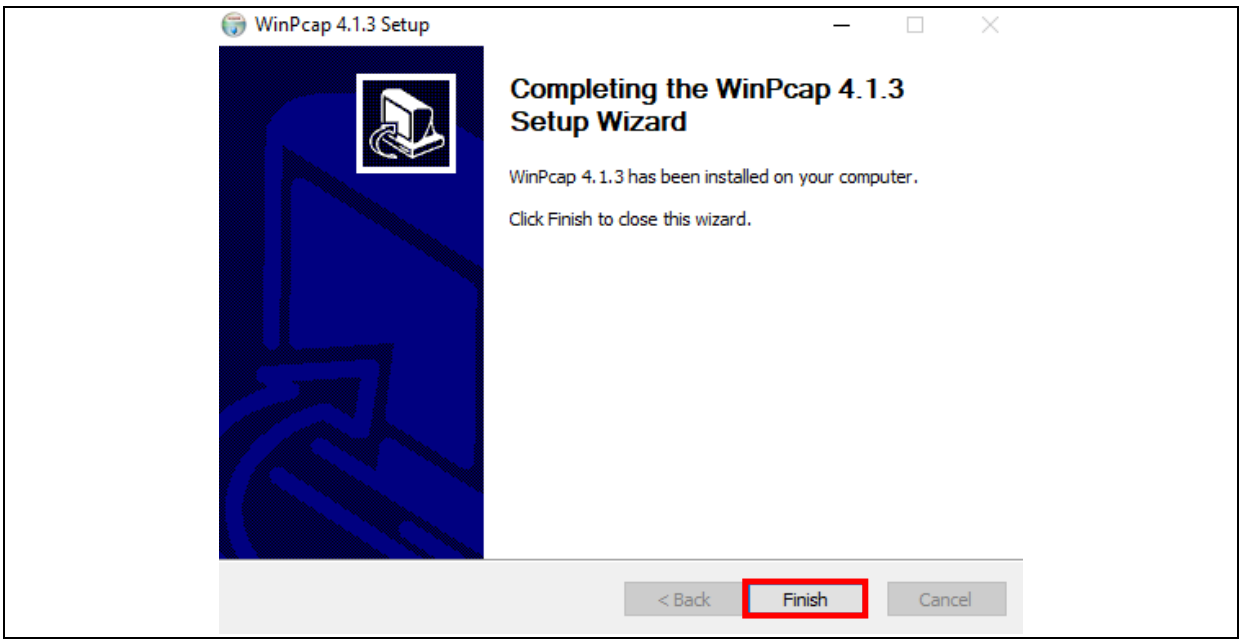
Step 6: Click on “I Agree” to continue the installation.



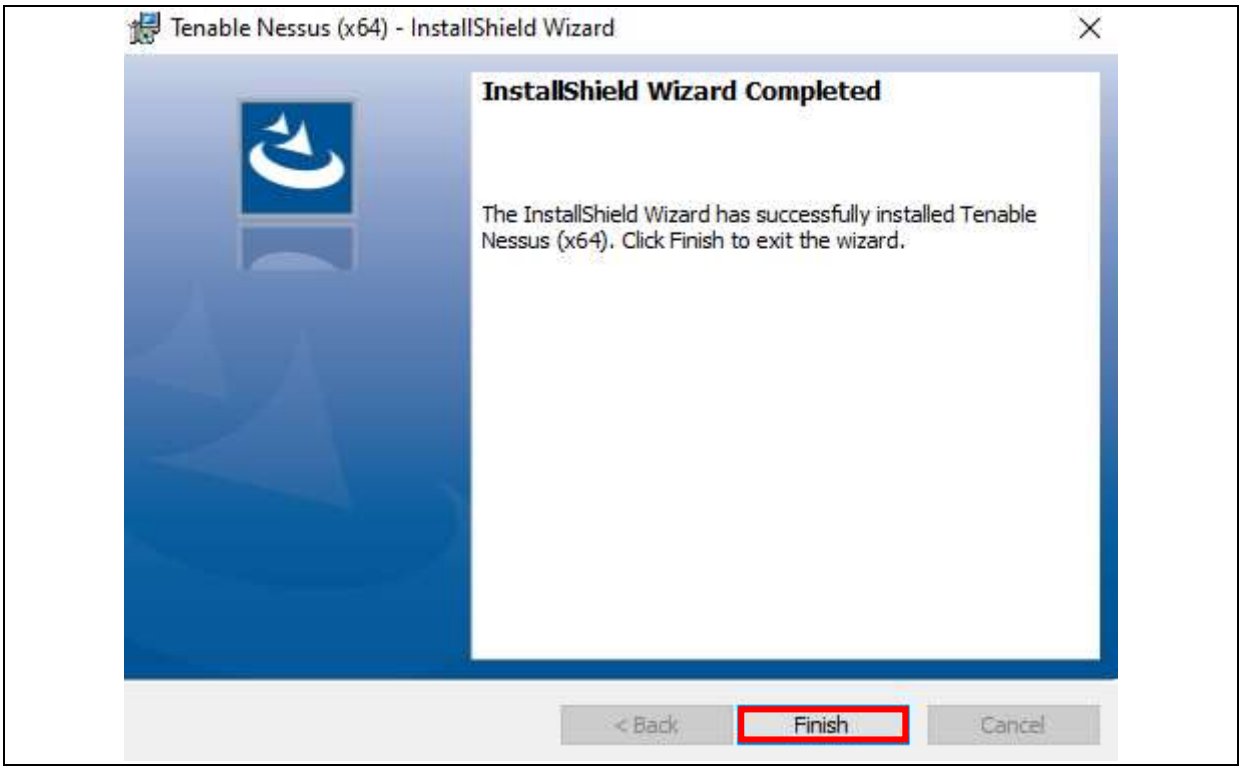
Step 7: Enable WinPcap driver to automatically start at boot time. And click “Install”.



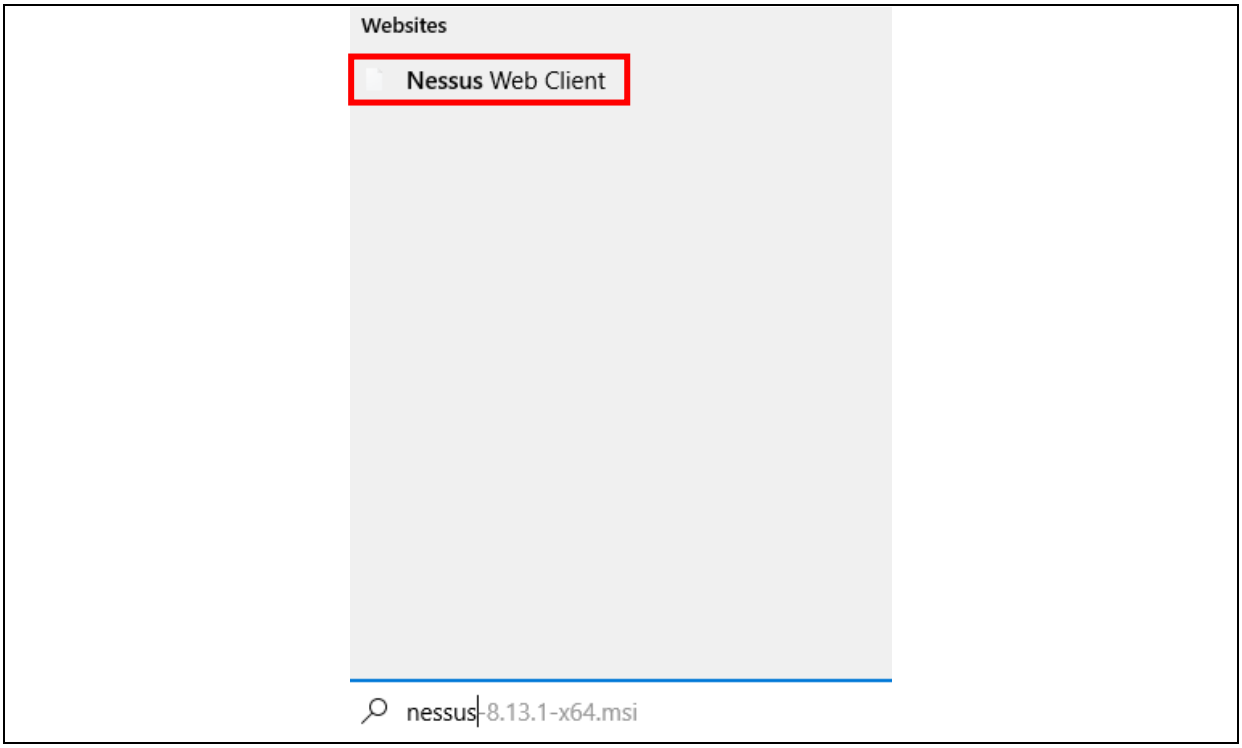
Step 8: Click “Finish” to complete the setup and installation for WinPcap.



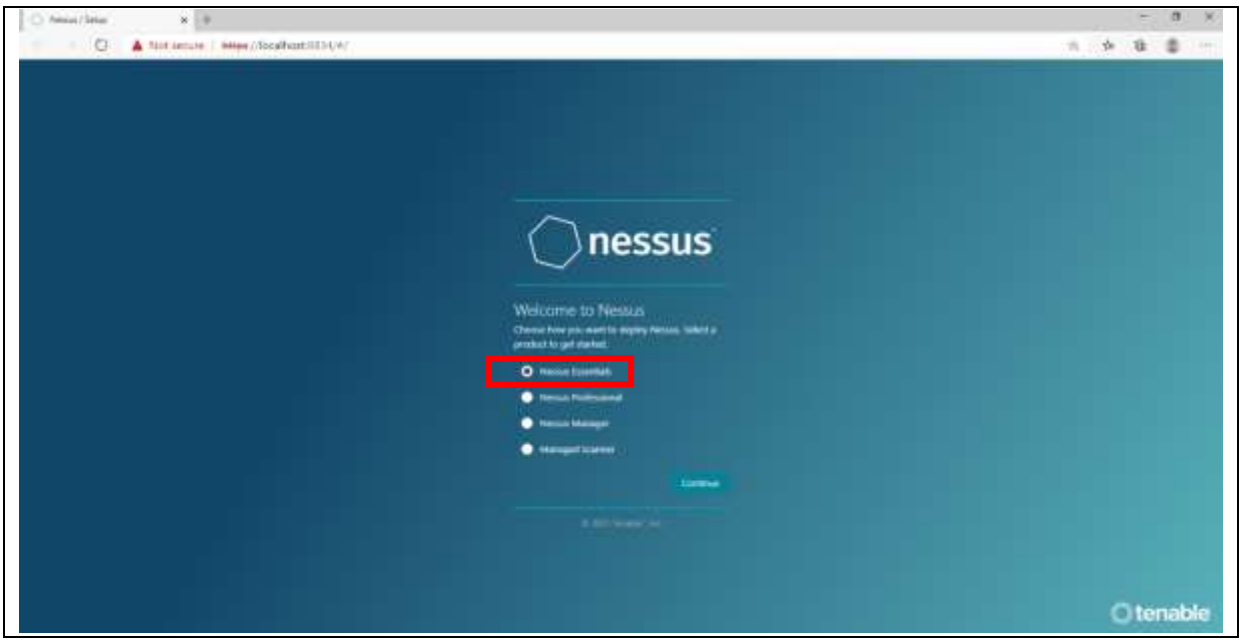
Step 9: Click “Finish” to complete the installation of Nessus.



Step 10: Open Windows Start Menu and type in “Nessus”, please open “Nessus Web Client” by clicking it as shown by the image below.



Step 11: The internet browser may state that it is unsafe as it is an insecure connection. Please ignore it and continue until the page shown below can be seen.

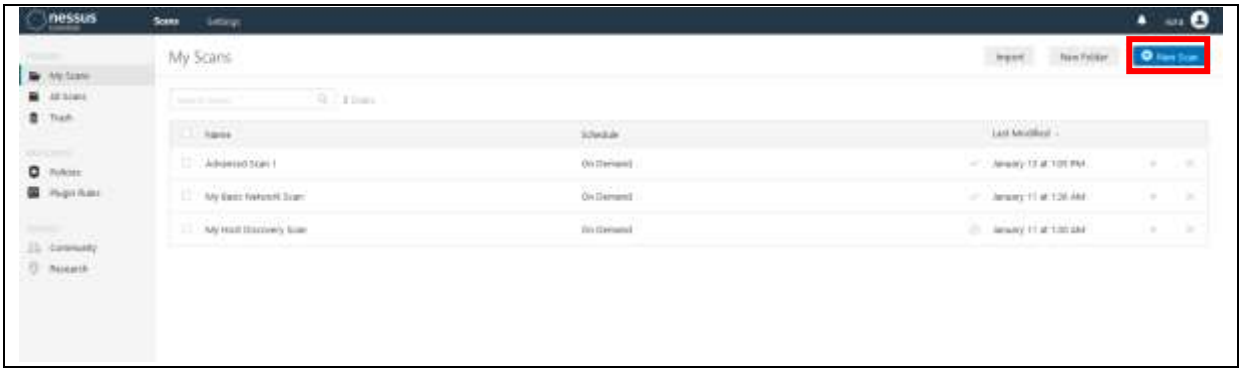


Step 12: For this assignment, we will be using Nessus Essentials as it is free, while the other versions of Nessus are paid. However, the functionality of Nessus Essentials is similar to the other versions such as Nessus Manager. Please click on “Nessus Essentials” and click “Continue” to view this page.

Step 13: Please enter your details to obtain an activation code to log into your Nessus account. Please visit your email to retrieve the activation code and paste on the next page as shown below.

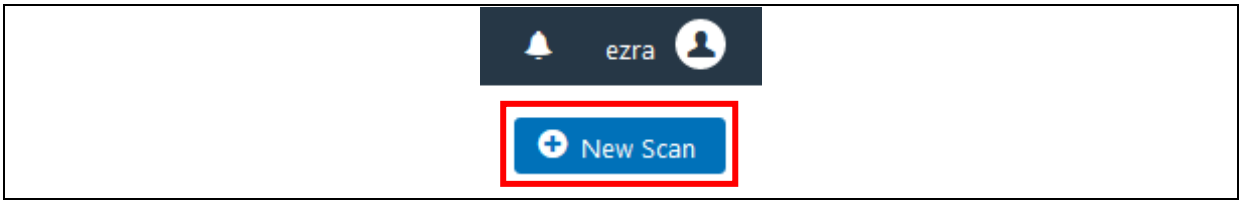
Step 14: Please create a new user account and password and click “Submit”. It will take several minutes to load the configuration.

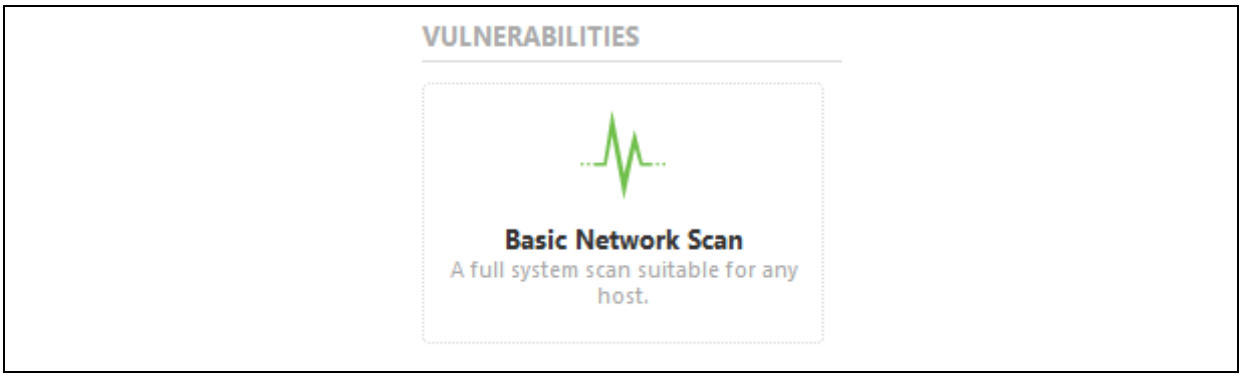
Step 15: Once the page has loaded, this is what it will show.



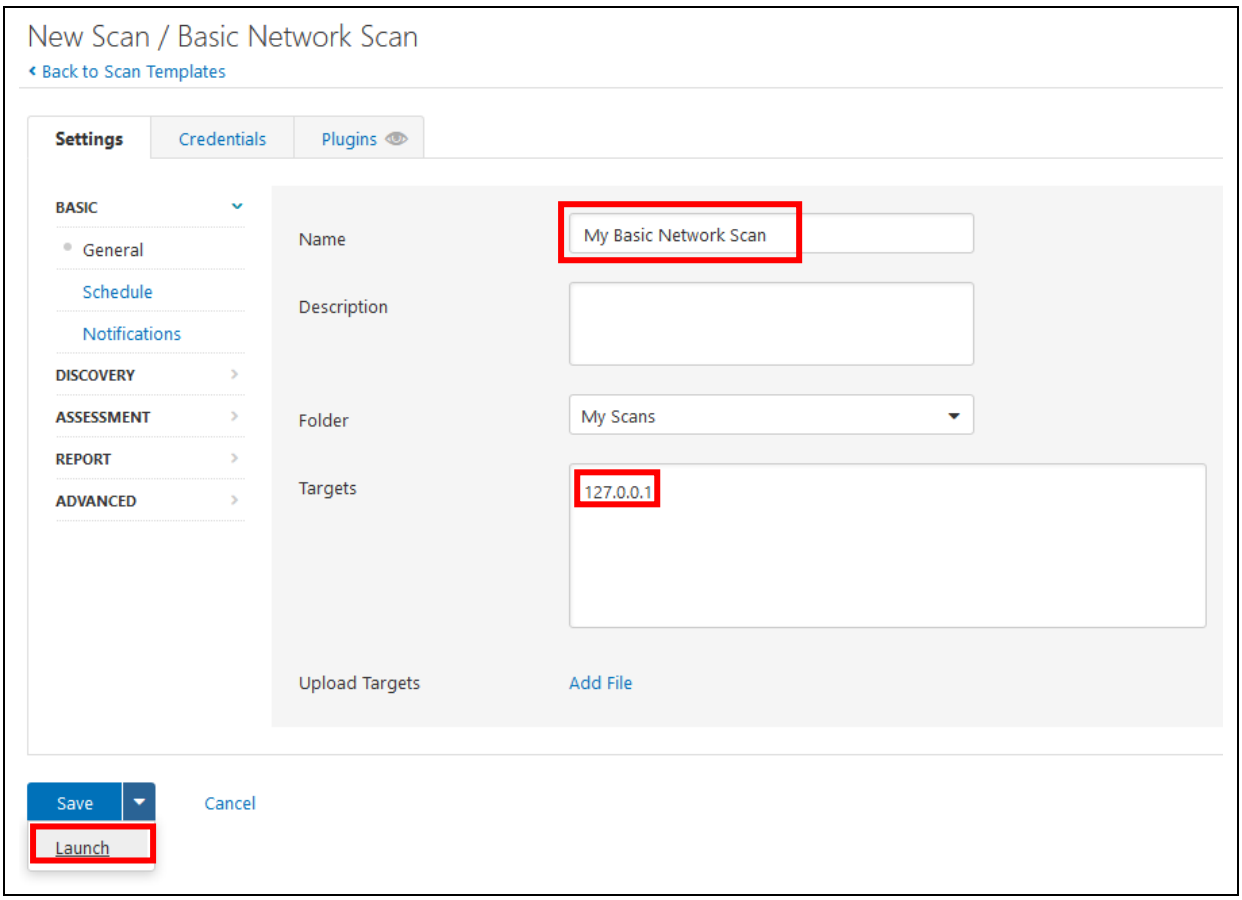
Nessus Scanning Process

Step 1: To run the first scan, please click on New Scan > Basic Network Scan.





Step 2: Enter the name of the scan and the targets to be scanned. In this case, we will scan the loopback address to check for any vulnerabilities on the server itself. Then once all is configured, click on the dropdown menu on the bottom left corner and click on “Launch”. This will automatically run the scanner.



Step 3: Click on the name of the scan to view the results. Here are some of the findings.

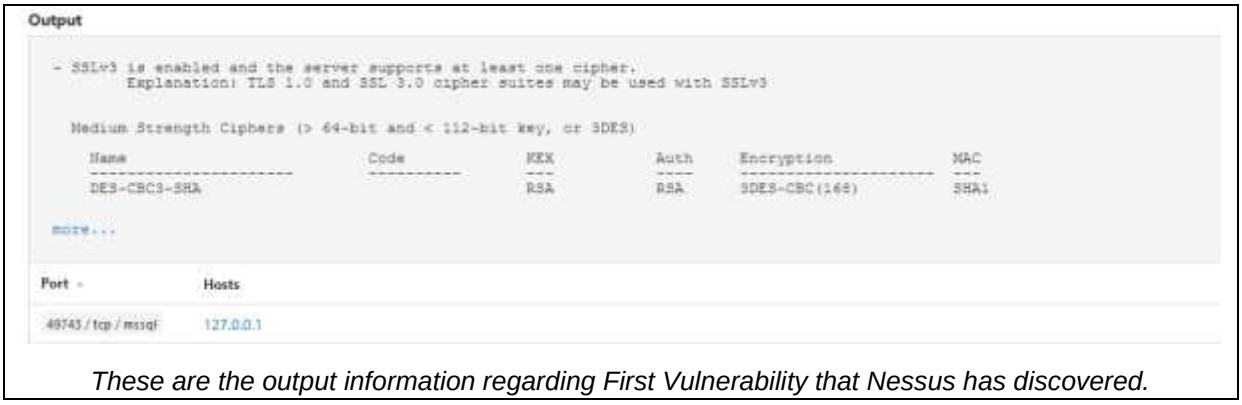
There were a few issues highlighted in purple, orange and yellow as shown in the image above. The ones highlighted blue are just information. More vulnerabilities will be shown in the performance and evaluation section of the report below.

Nessus Performance and Evaluation

First Vulnerability:

The one with the orange highlight states that it discovered SSL Version 2 and 3 Protocol Detection, where it summarized that these versions of SSL have been affected by several cryptographic flaws such as insecure padding scheme with CBC ciphers and insecure session renegotiation and resumption schemes.

This flaw could potentially lead to an attacker exploiting this to perform man-in-the-middle attack and decrypt communications between the affected clients and the service. It then concludes with recommending a better alternative to this protocol, which is the TLS 1.2. It recommends this version and higher as it is a stable and much safer alternative to its predecessor, SSL protocol, and previous versions of TLS 1.0, TLS 1.1.



These are the output information regarding First Vulnerability that Nessus has discovered.

Plugin Details

Severity:	High
ID:	20007
Version:	1.33
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	May 6, 2020

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 7.5

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:N/S:U/C:H/I:N/A:N

CVSS Base Score: 7.1

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N

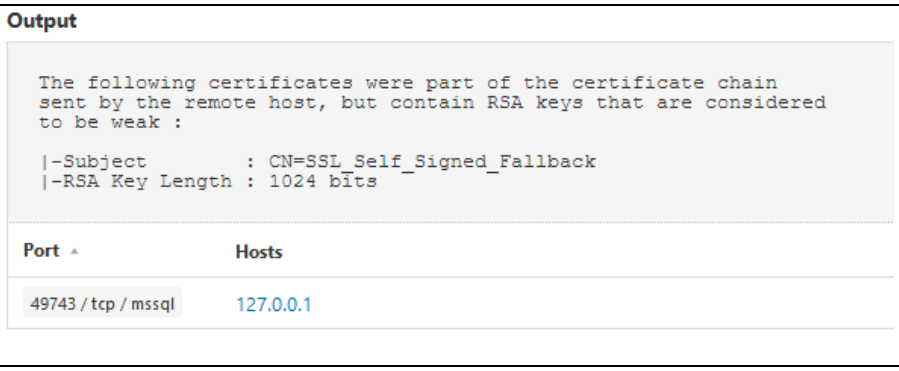
Vulnerability Information

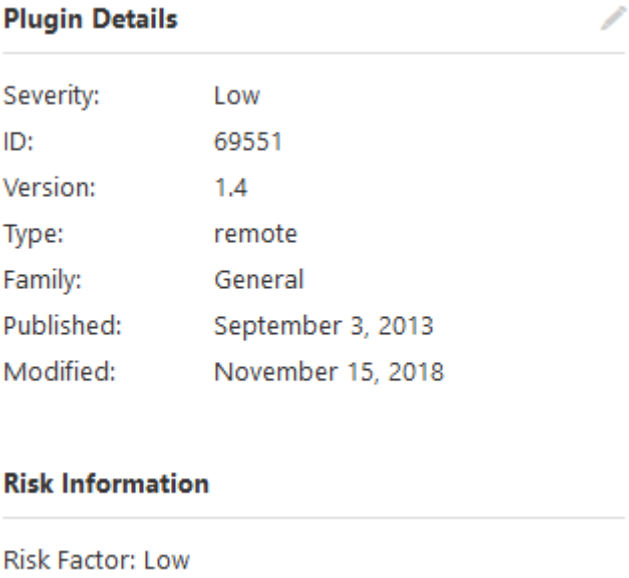
In the news: true

These are the output information regarding First Vulnerability that Nessus has discovered.

Second Vulnerability:

Another such example of details found is one which states that SSL Certificate Chain contains RSA Keys less than 2048 bits. This vulnerability was highlighted green, which indicates that this is a low-level vulnerability. It brings up that some browsers may reject keys with less than 2048 bits after January 1st, 2014. It brings up the solution that users should reissue the certificates with RSA keys of 2048 bits or lesser.



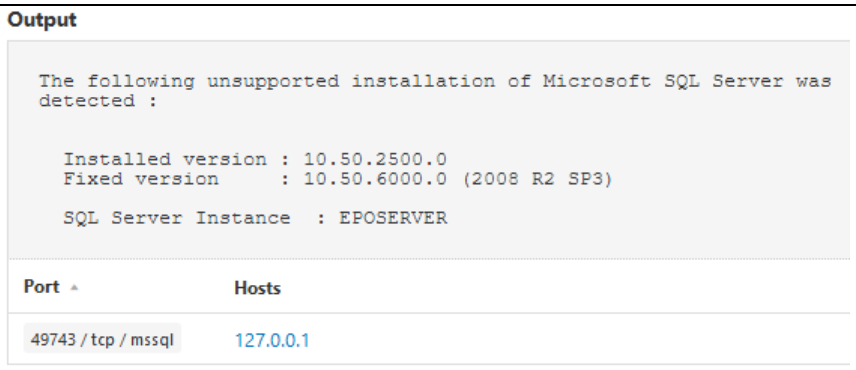


These are the output information regarding Third Vulnerability that Nessus has discovered.

Third Vulnerability

This vulnerability was intentionally placed into the server for the vulnerability scanner to detect. The highlight indicator was red, meaning that it is a critical error which could lead to potentially huge damage. The software, McAfee ePolicy Orchestrator 5.30, was downloaded into the Windows server machine to see the capabilities of Nessus when it comes to vulnerability scanning. It summarized that the version of Microsoft SQL Server on the remote host is no longer supported and received no new security patches, hence would most likely contain security vulnerabilities.

It then suggested to upgrade to a version of Microsoft SQL Server that is supported. However, McAfee ePolicy Orchestrator 5.3.0 has been out since 19th May 2015, which is why Nessus was able to detect that the Microsoft SQL Server needed an update instead of completely deleting the old software.



These are the output information regarding Third Vulnerability that Nessus has discovered.

Plugin Details

Severity:	Critical
ID:	73756
Version:	1.17
Type:	remote
Family:	Databases
Published:	April 29, 2014
Modified:	December 2, 2020

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:N/S:C/C:H/I:H/A:H

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/a:microsoft:sql_server

Unsupported by vendor: true

These are the output information regarding Third Vulnerability that Nessus has discovered.

Windows Firewall with Advanced Security

Firewall is an essential part of the security system, as without it, the device and network are vulnerable and open to threats. A firewall keeps disruptive and destructive forces out, controlling the incoming and outgoing network traffic connections based on the security parameters controlled by the user.

Access the Windows Firewall with Advanced Security > Inbound Security > BranchCache Content Retrieval (HTTP-in). Right-click and click on “Enable Rule” to enable the rule.

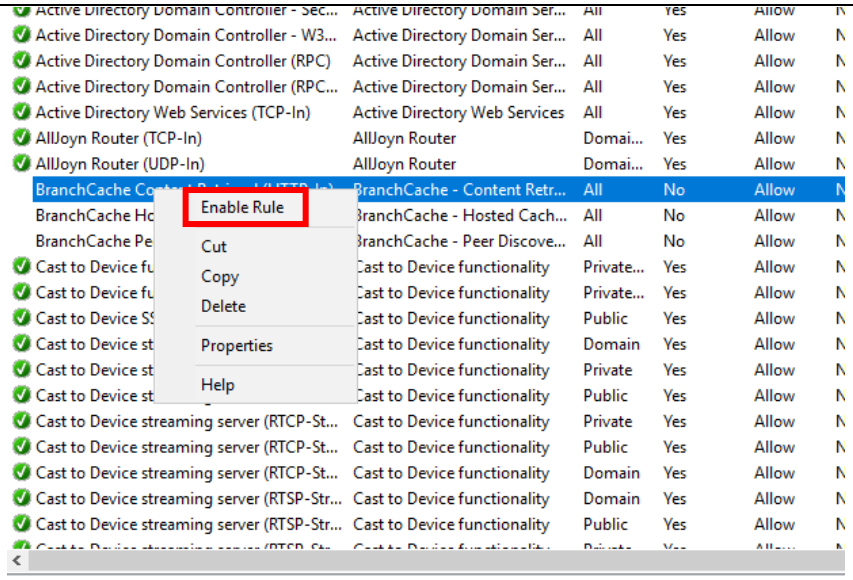


Image of enabling BranchCache Content Retrieval (HTTP-in)

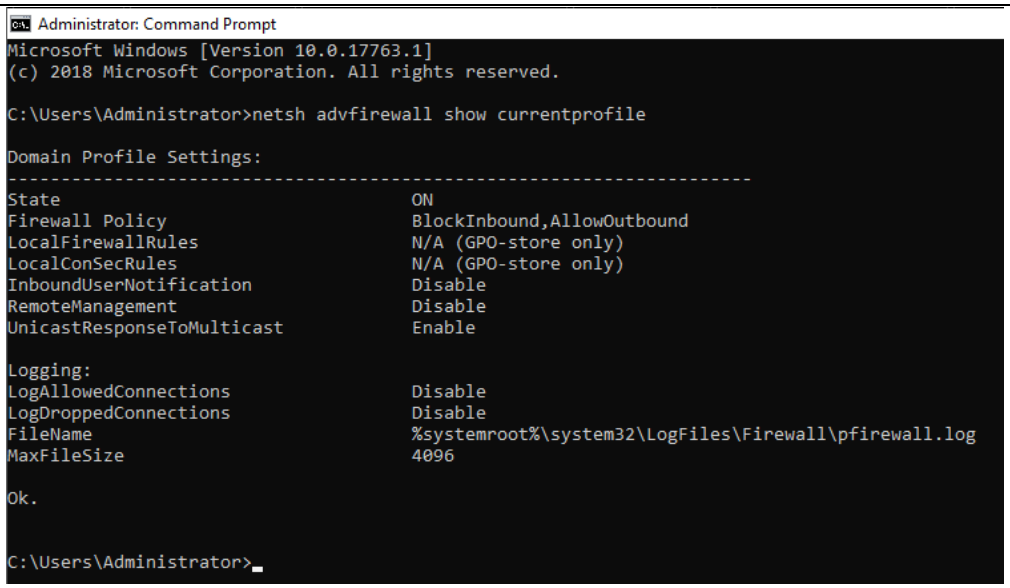


Image of current profile of firewall in Windows Server

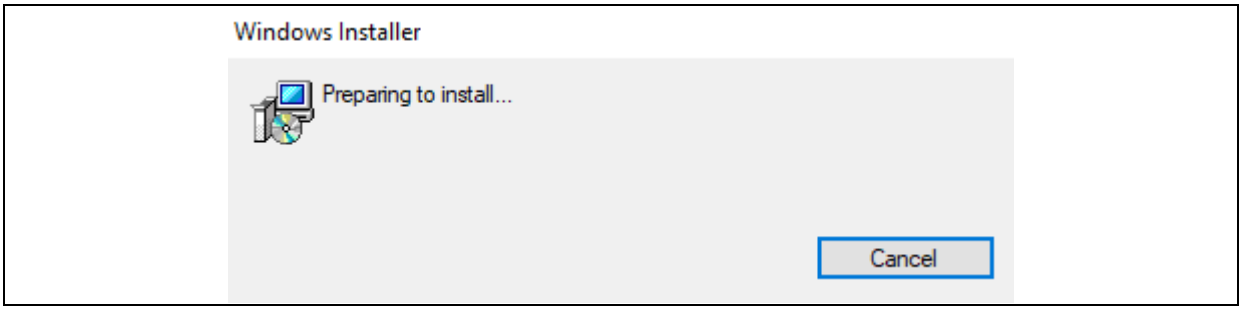
TinyWall Firewall

Tinywall is a small, simple, and easy to use firewall software that can allow or block both incoming and outgoing ports. It also passes all the port scans and other web-based tests. It is also stealthy, making it invisible to attackers outside.

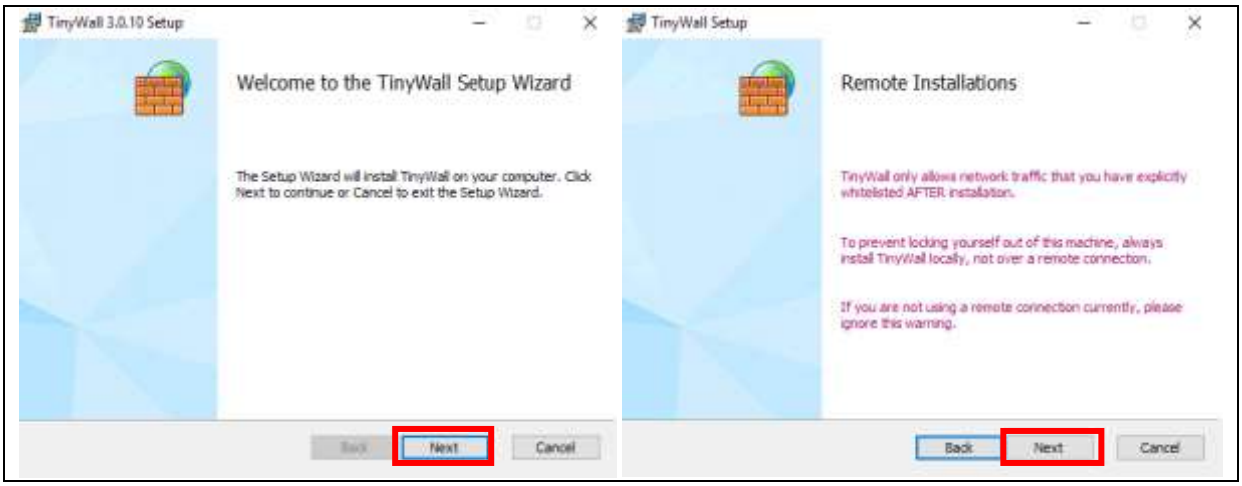
Step 1: Please access this website to download TinyWall executable file.

https://tinywall.pados.hu/download.php

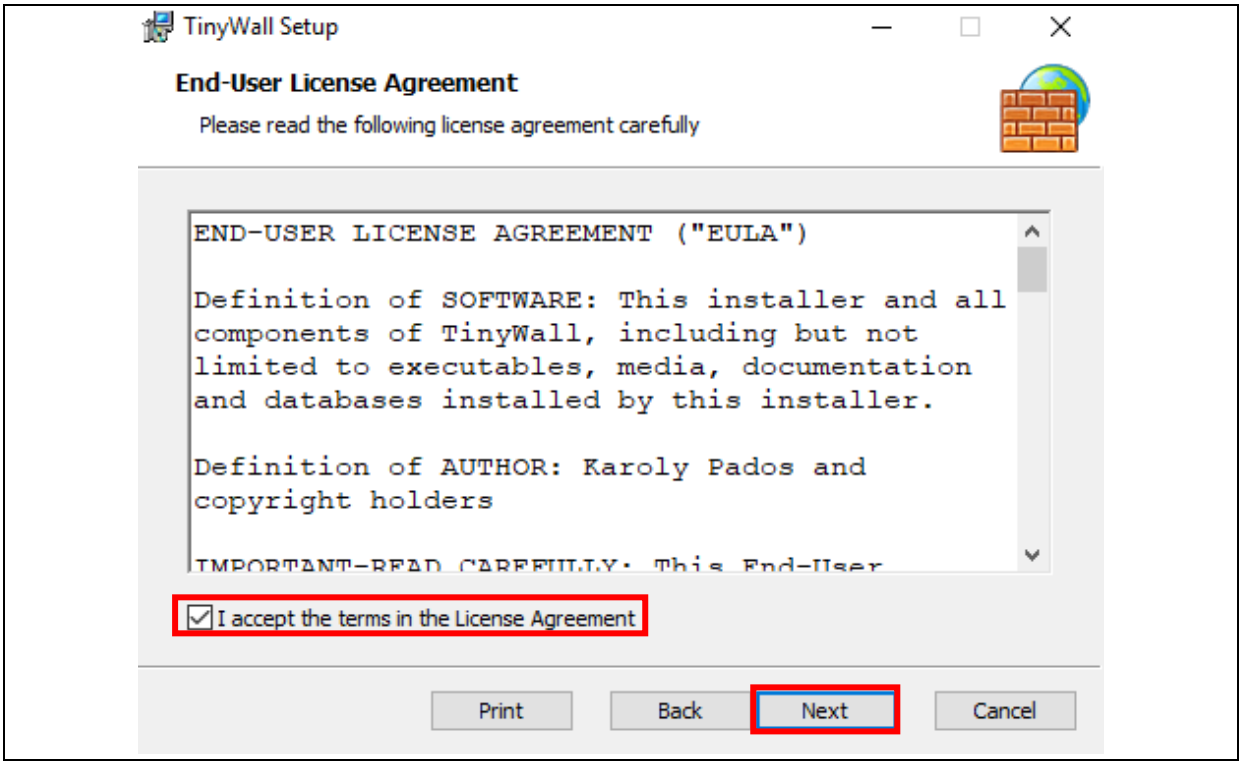
Step 2: Double click on the downloaded file and wait until the setup pop-up appears.



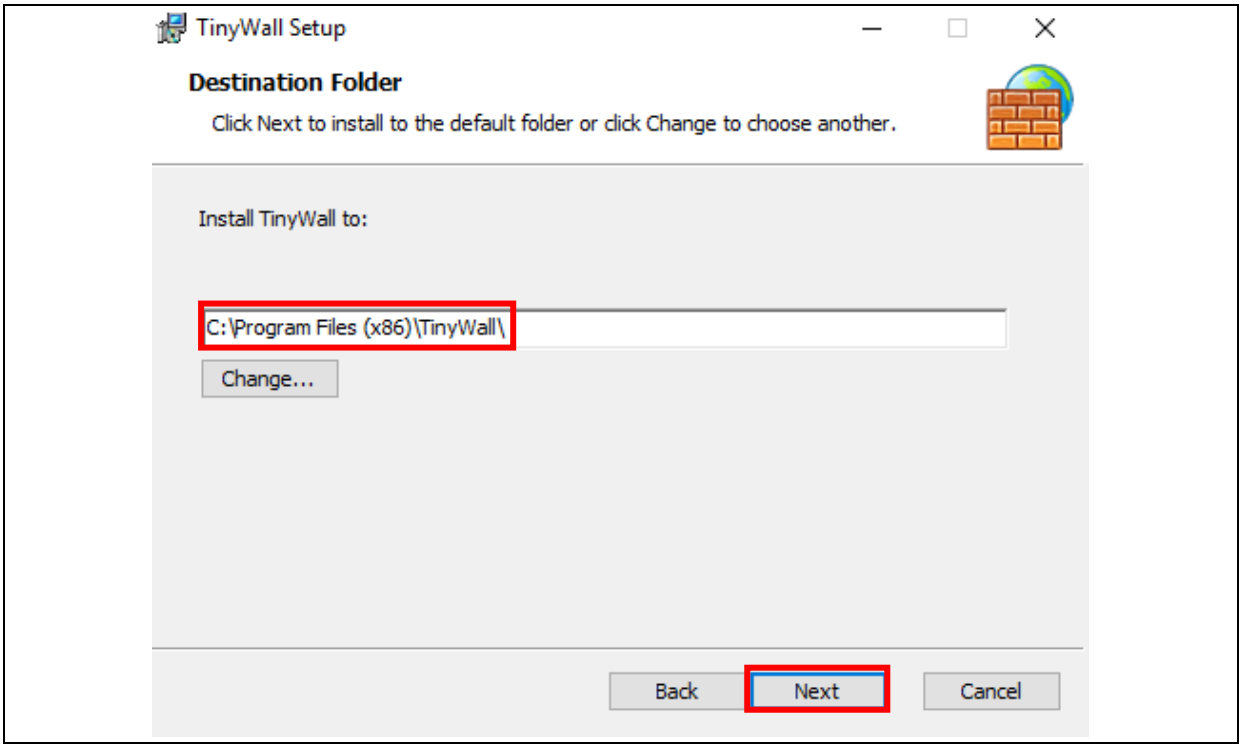
Step 3: Click on “Next” to proceed with the installation.



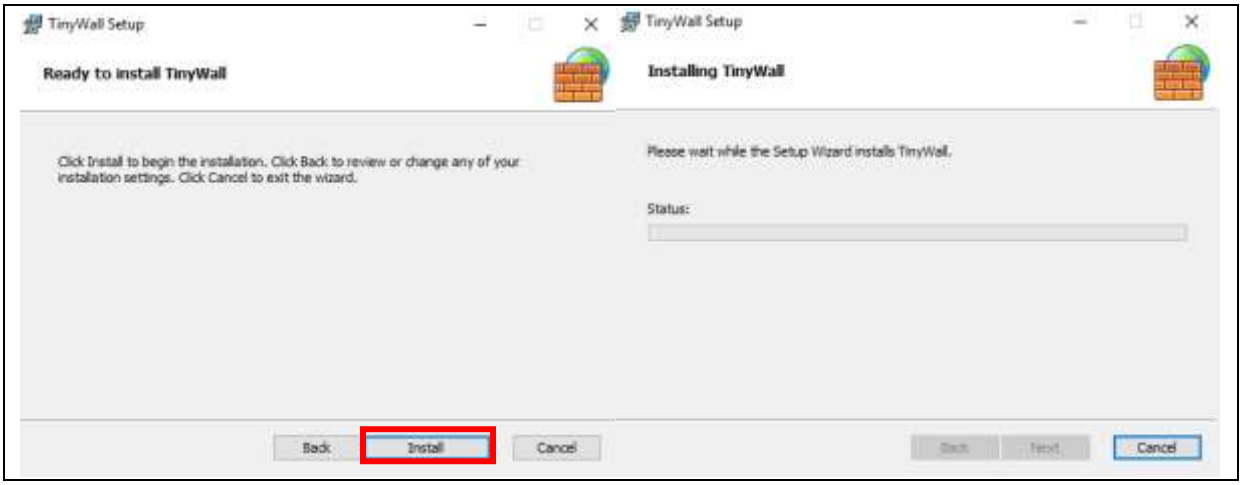
Step 4: Check the box and click “Next” to proceed with the installation.



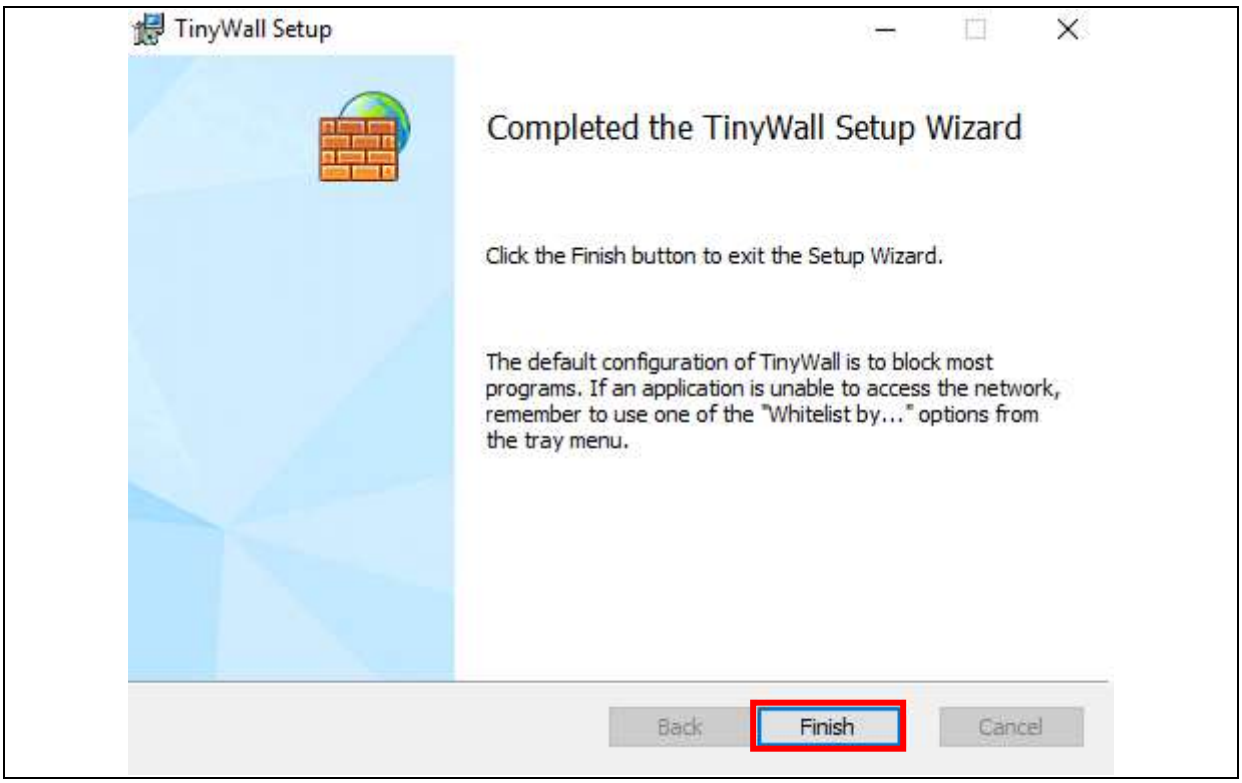
Step 5: Check the destination where this app will be downloaded and click “Next”.



Step 6: Click on “Install” and wait a few moments for the installation of the software.

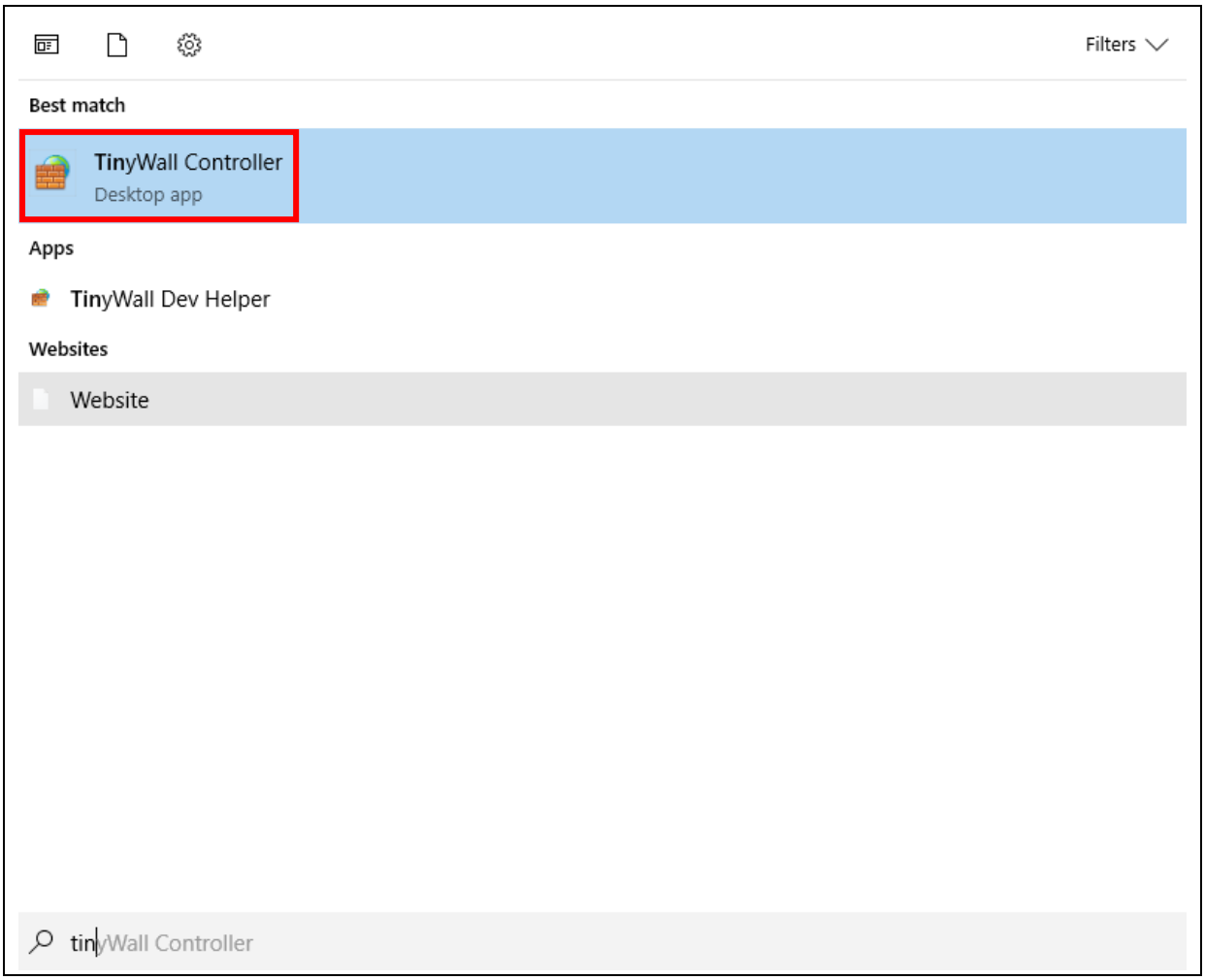


Step 7: Click on “Finish” to complete the installation.

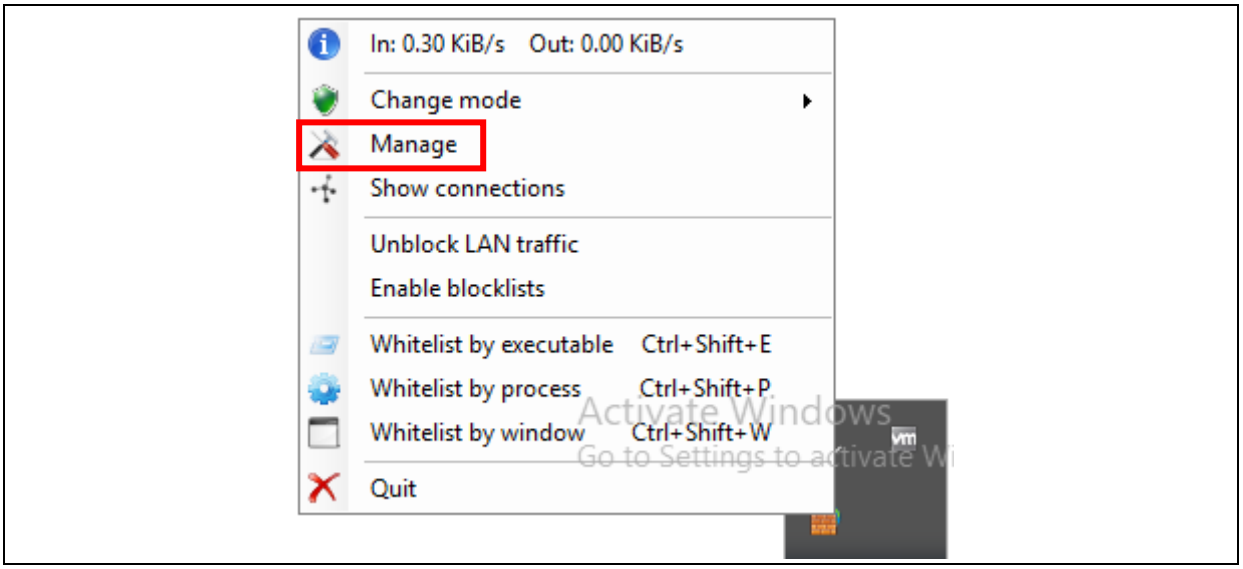


Using TinyWall Firewall

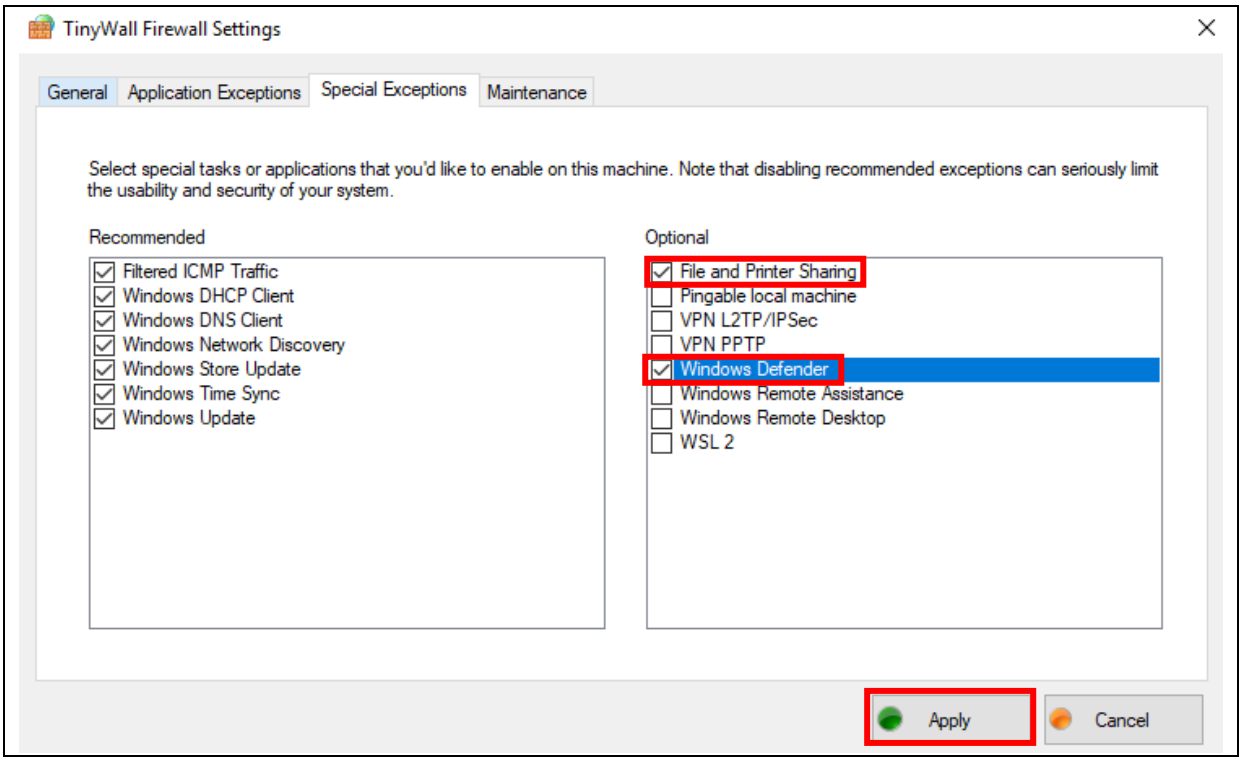
On the start menu, search for TinyWall and click on it to launch it in the background. This will open a background task instead of displaying a window for the users.



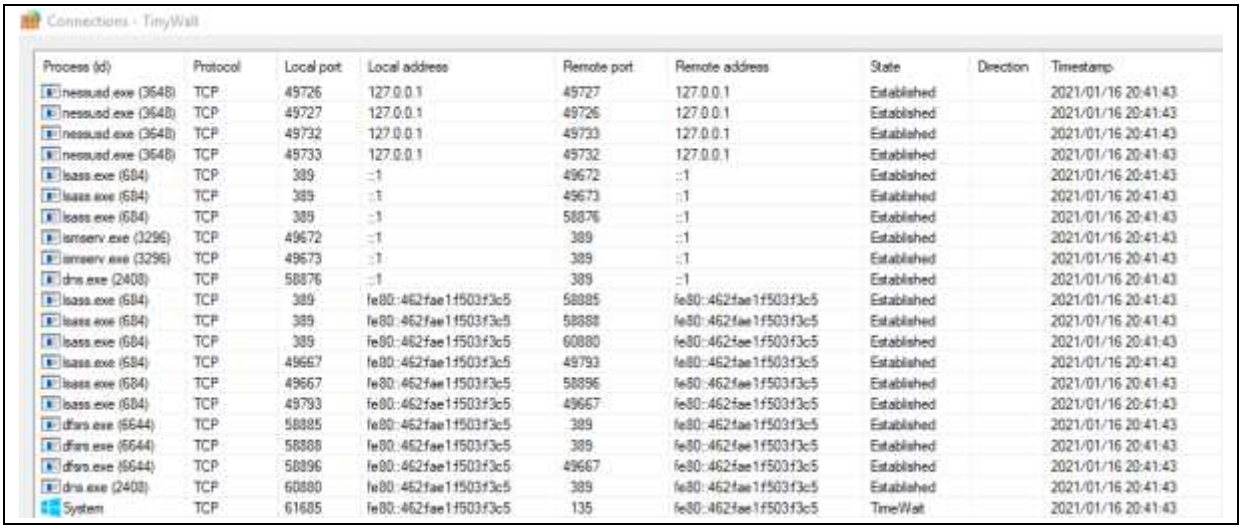
Right click on the task bar TinyWall icon and click “Manage” to show a window which allows users to manage what kind of apps will be whitelisted or blacklisted from the firewall.



Click on “Special Exceptions” and check the boxes “File and Printer Sharing” and “Windows Defender”. This will allow these processes to continue running and working as per normal when TinyWall firewall is activated.



Right click on the TinyWall firewall taskbar icon and click on show connections. This will display the connections that is being received by the Windows Server at the moment. From the image of the connections below, it can be said that a few applications are running in the background which requires constant network connection such as Nessus.



Process (id)	Protocol	Local port	Local address	Remote port	Remote address	State	Direction	Timestamp
nessusd.exe (3648)	TCP	49726	127.0.0.1	49727	127.0.0.1	Established		2021/01/16 20:41:43
nessusd.exe (3648)	TCP	49727	127.0.0.1	49726	127.0.0.1	Established		2021/01/16 20:41:43
nessusd.exe (3648)	TCP	49732	127.0.0.1	49733	127.0.0.1	Established		2021/01/16 20:41:43
nessusd.exe (3648)	TCP	49733	127.0.0.1	49732	127.0.0.1	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	::1	49672	::1	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	::1	49673	::1	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	::1	58876	::1	Established		2021/01/16 20:41:43
ismserv.exe (3296)	TCP	49672	::1	389	::1	Established		2021/01/16 20:41:43
ismserv.exe (3296)	TCP	49673	::1	389	::1	Established		2021/01/16 20:41:43
dns.exe (2408)	TCP	58876	::1	389	::1	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	fe80::462fae1f503f3c5	58885	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	fe80::462fae1f503f3c5	58888	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	389	fe80::462fae1f503f3c5	60880	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	49667	fe80::462fae1f503f3c5	49793	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	49667	fe80::462fae1f503f3c5	58896	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
lsass.exe (684)	TCP	49793	fe80::462fae1f503f3c5	49667	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
dfsrs.exe (6644)	TCP	58885	fe80::462fae1f503f3c5	389	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
dfsrs.exe (6644)	TCP	58888	fe80::462fae1f503f3c5	389	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
dfsrs.exe (6644)	TCP	58896	fe80::462fae1f503f3c5	49667	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
dns.exe (2408)	TCP	60880	fe80::462fae1f503f3c5	389	fe80::462fae1f503f3c5	Established		2021/01/16 20:41:43
System	TCP	61685	fe80::462fae1f503f3c5	135	fe80::462fae1f503f3c5	TimeWait		2021/01/16 20:41:43

Testing Firewalls (TinyWall & Windows Firewall)

An attempt to ping Windows Server fail as all incoming traffic was blocked by the firewall. Hence, the Windows 10 desktop was not able to ping successfully to Windows Server as the packets were dropped immediately. “Request timed out” indicated that the Windows 10 machine was not able to successfully ping the server, indicating that the firewall did manage to block all incoming connection.

Windows Server IP Configuration

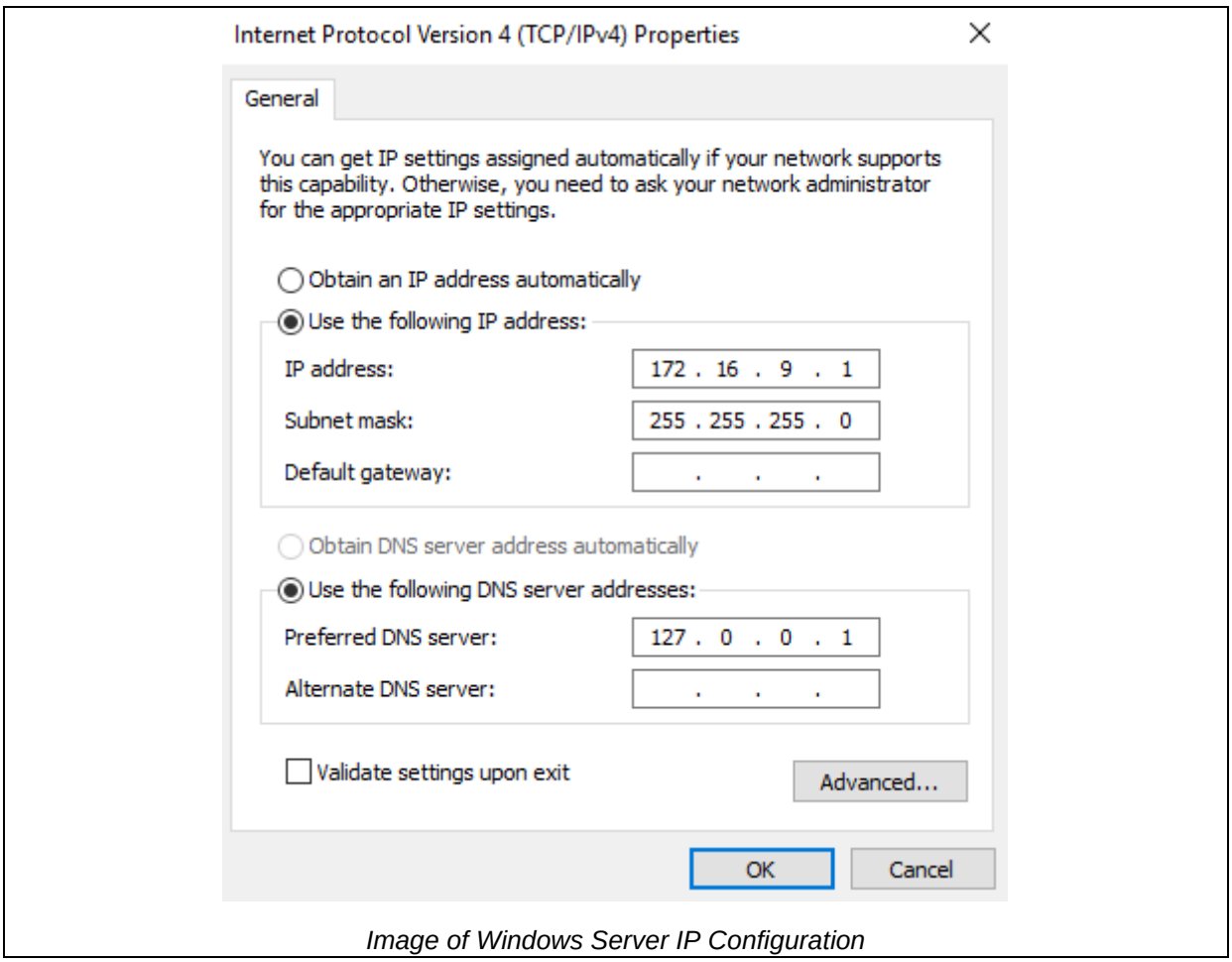


Image of Windows Server IP Configuration

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::462:fae1:f503:f3c5%12
   IPv4 Address. . . . . . . . . . . : 172.16.9.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Image of Command Prompt screenshot of Windows Server IP Configuration

Windows 10 Configuration

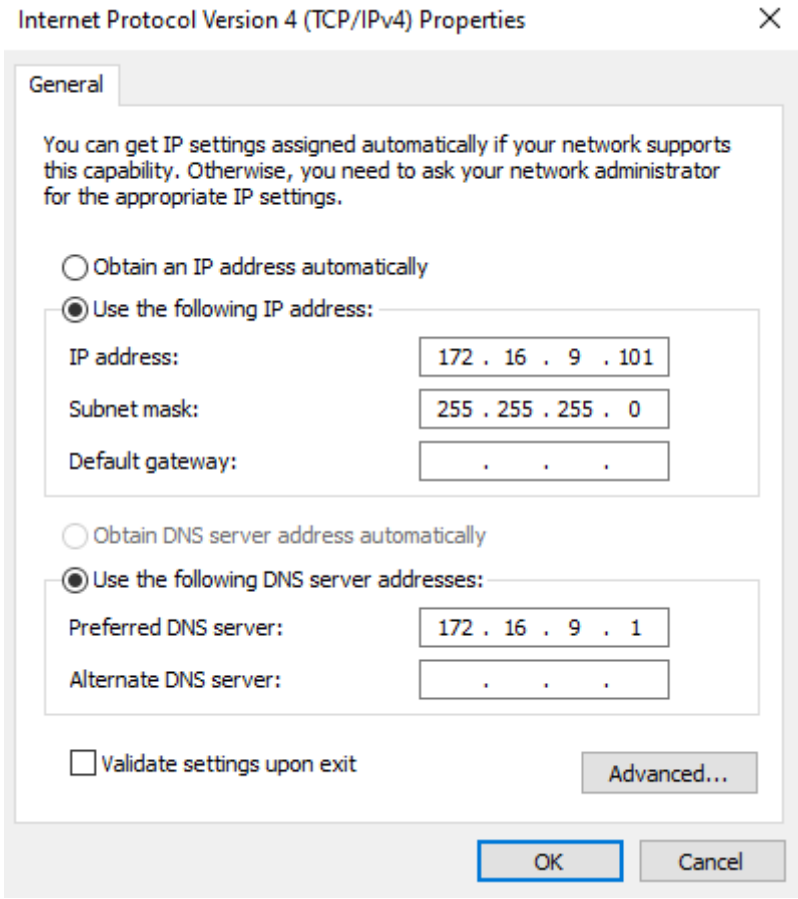


Image of Windows 10 IP Configuration

Pinging Windows Server from Windows 10

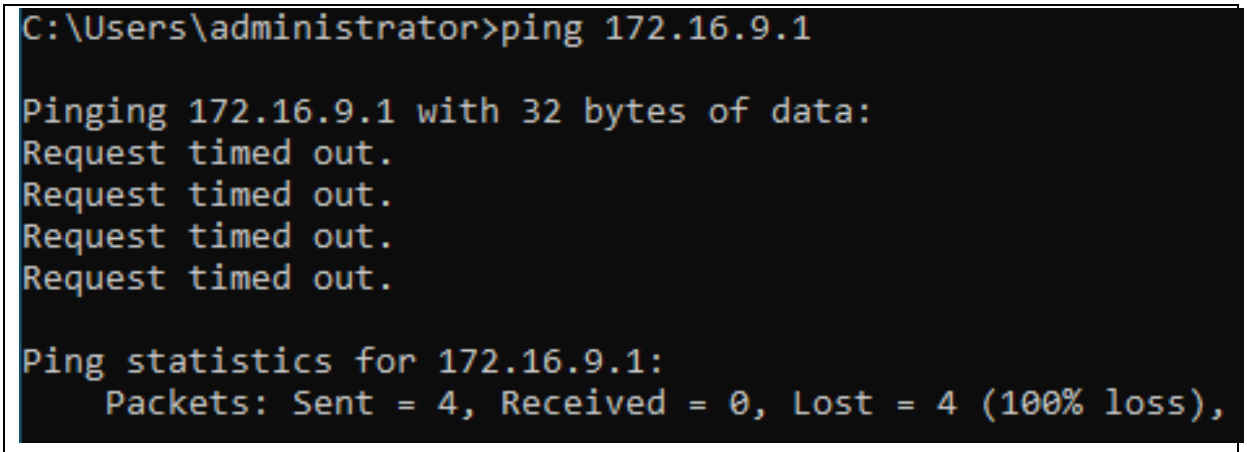


Image of pinging Windows Server from Windows 10

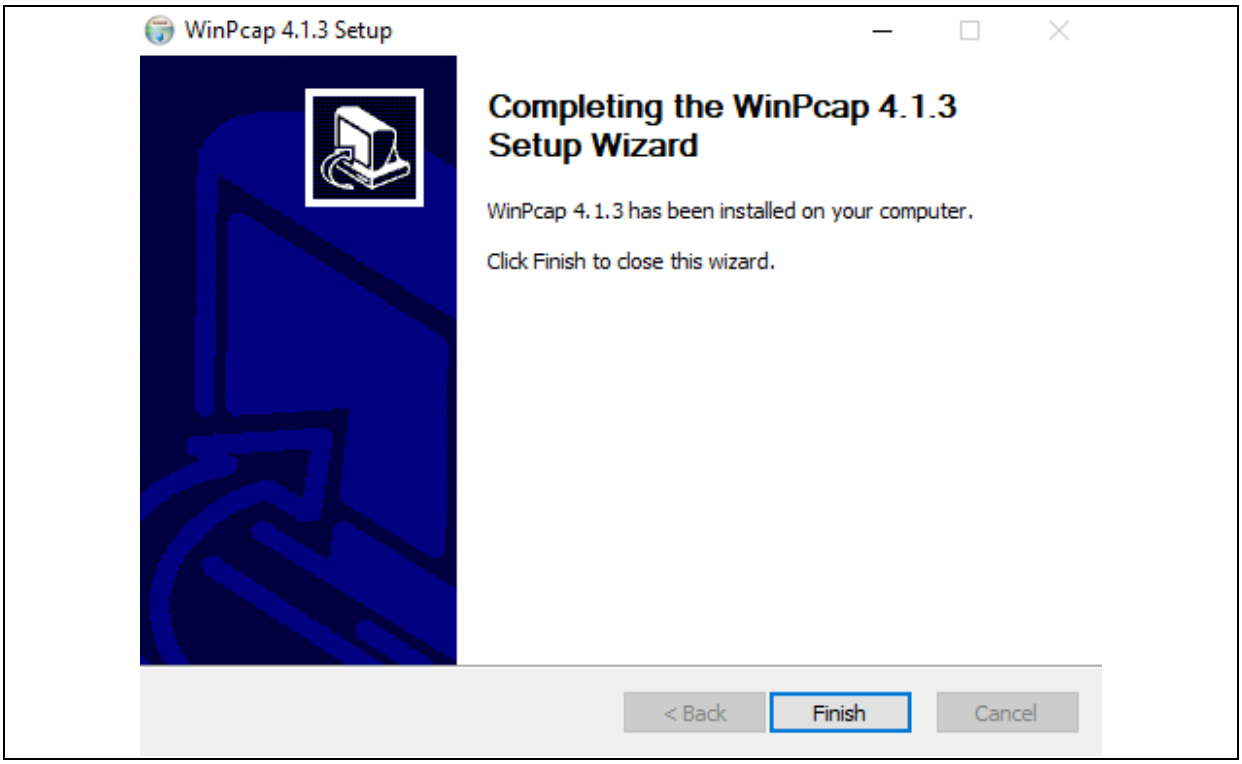
Snort

Snort is an open-source network intrusion detection system (NIDS), it is a packet sniffer that monitors network traffic in real time, inspecting each packet closely to detect dangerous payloads or suspicious anomalies.

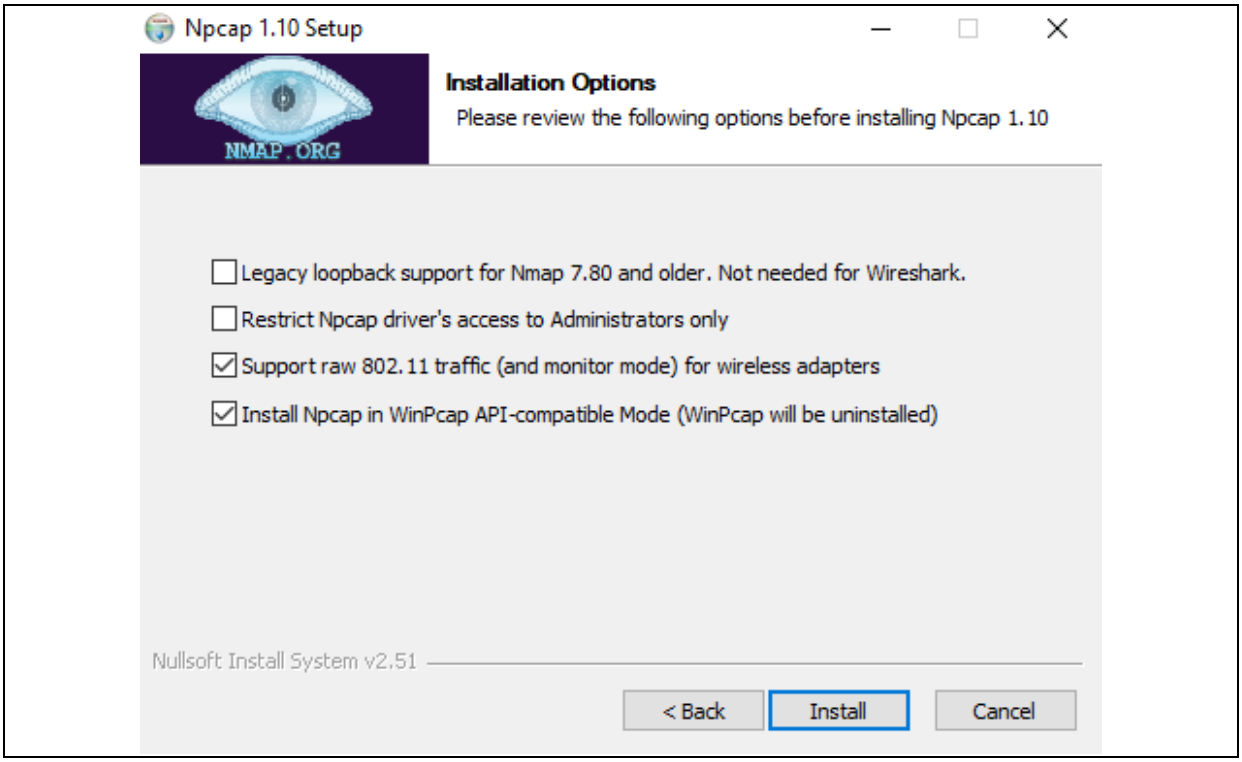
In addition to Snort, we'll also be using WinPcap and Npcap, which are packet sniffing libraries for Windows.

We will also need the Snort Rules which can be downloaded from their website and since we are using snort version 2.9.17, we will download "snortrules-snapshot-29170.tar.gz"

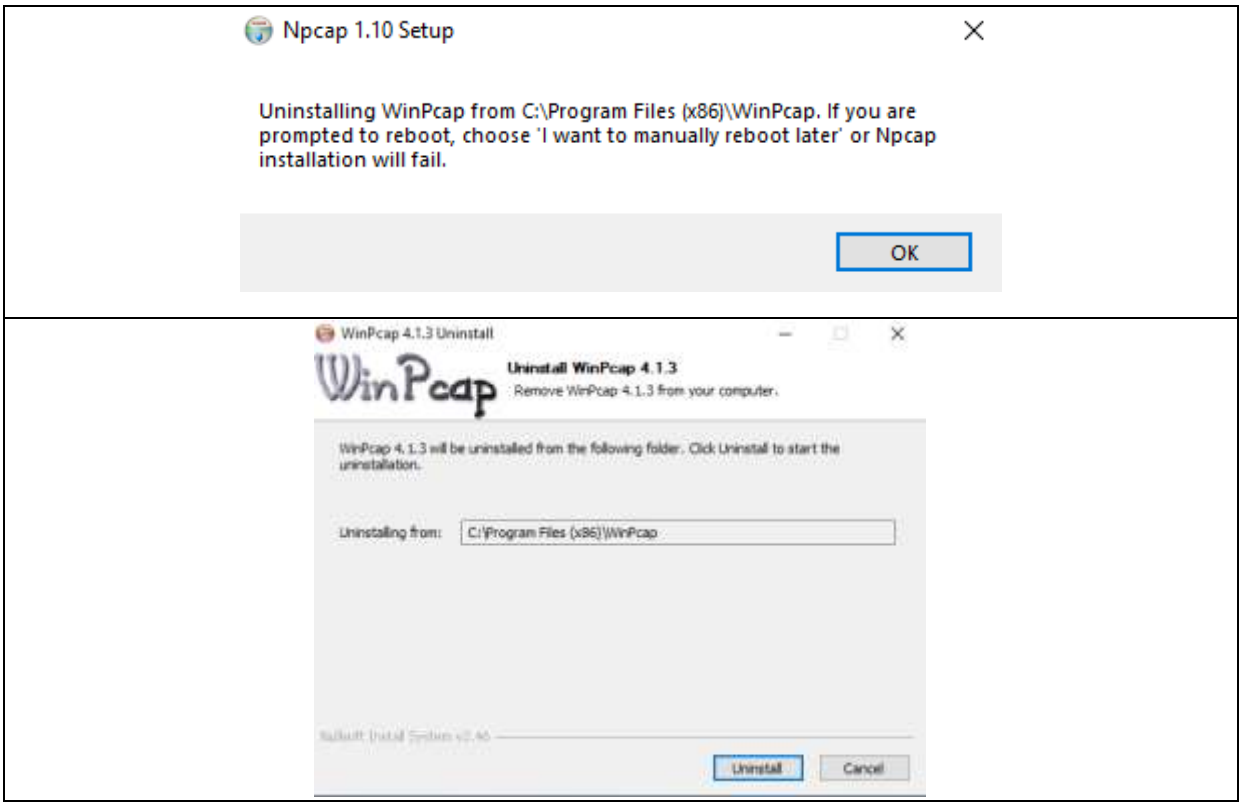
Step 1: Install WinPcap, make sure to check the box "Automatically start the WinPcap driver at boot time"



Step 2: Install Npcap, make sure to check the 2 boxes as shown in the picture.

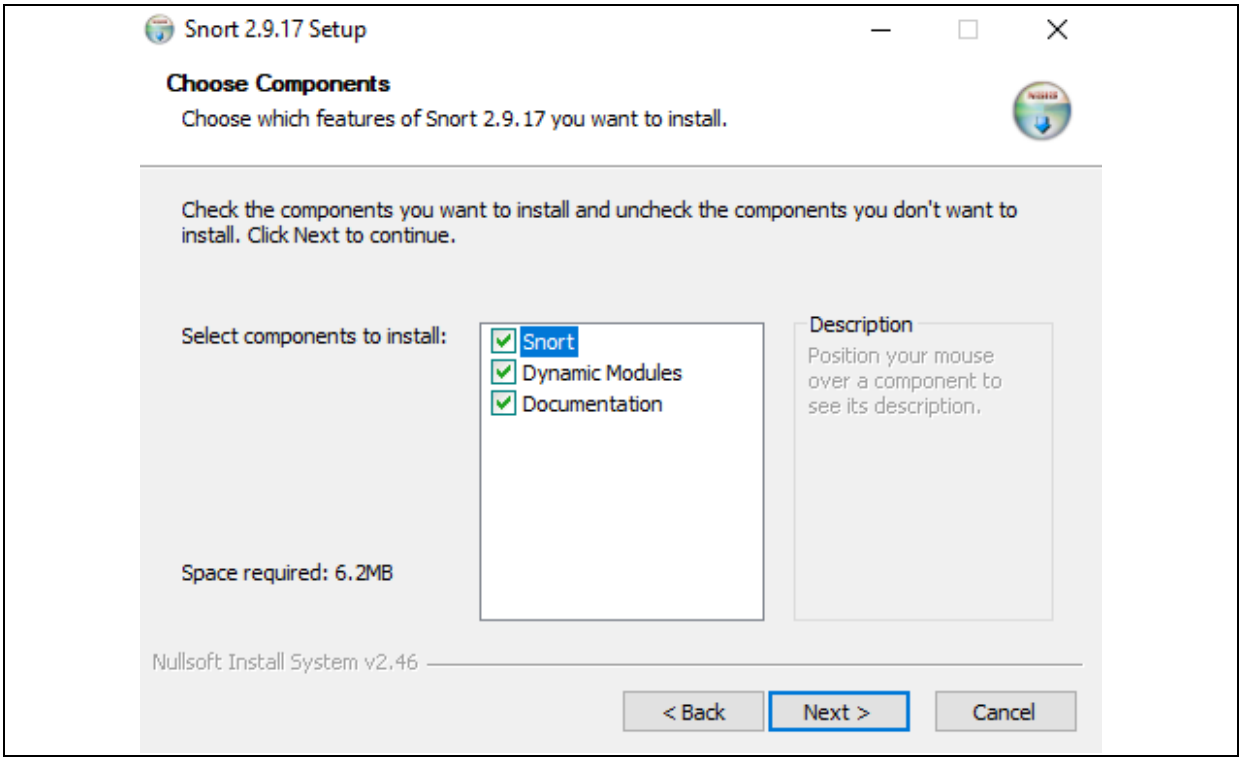


Step 3: There will be a prompt to uninstall WinPcap. Click OK. Then uninstall. (Npcap seems to use some files from WinPcap.)

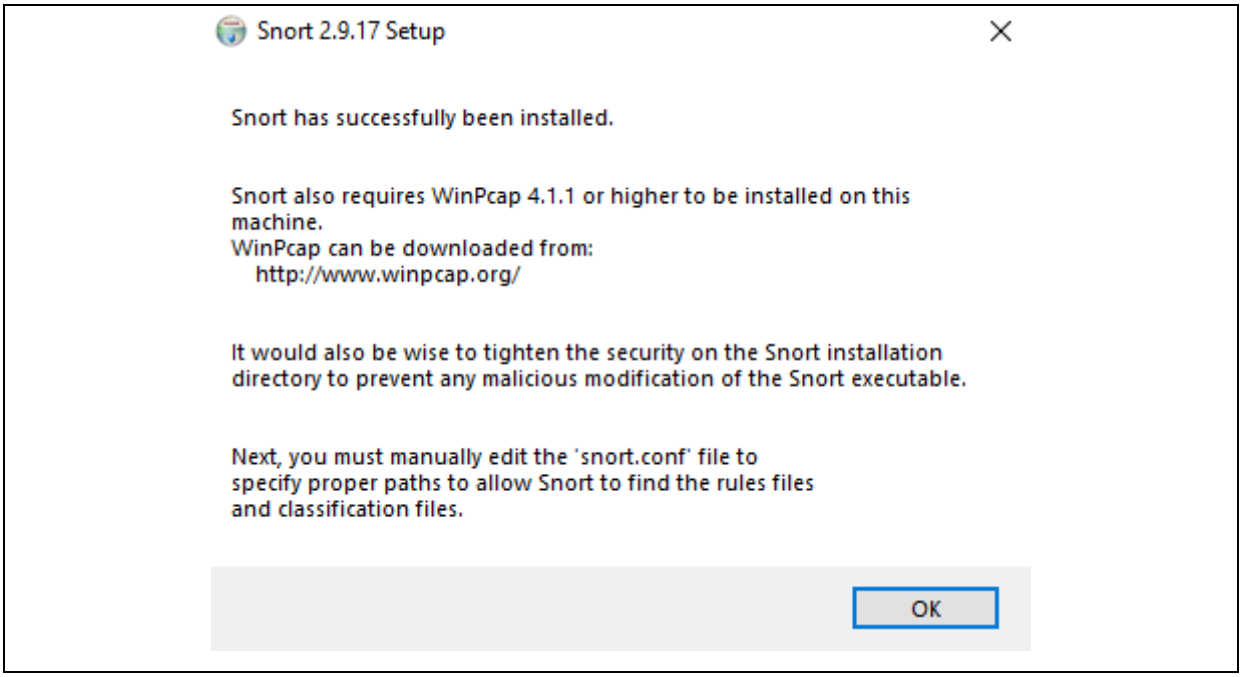


Step 4: Install Snort. Check all 3 boxes.

Step 5: At “Choose Install Location” Click “Next”

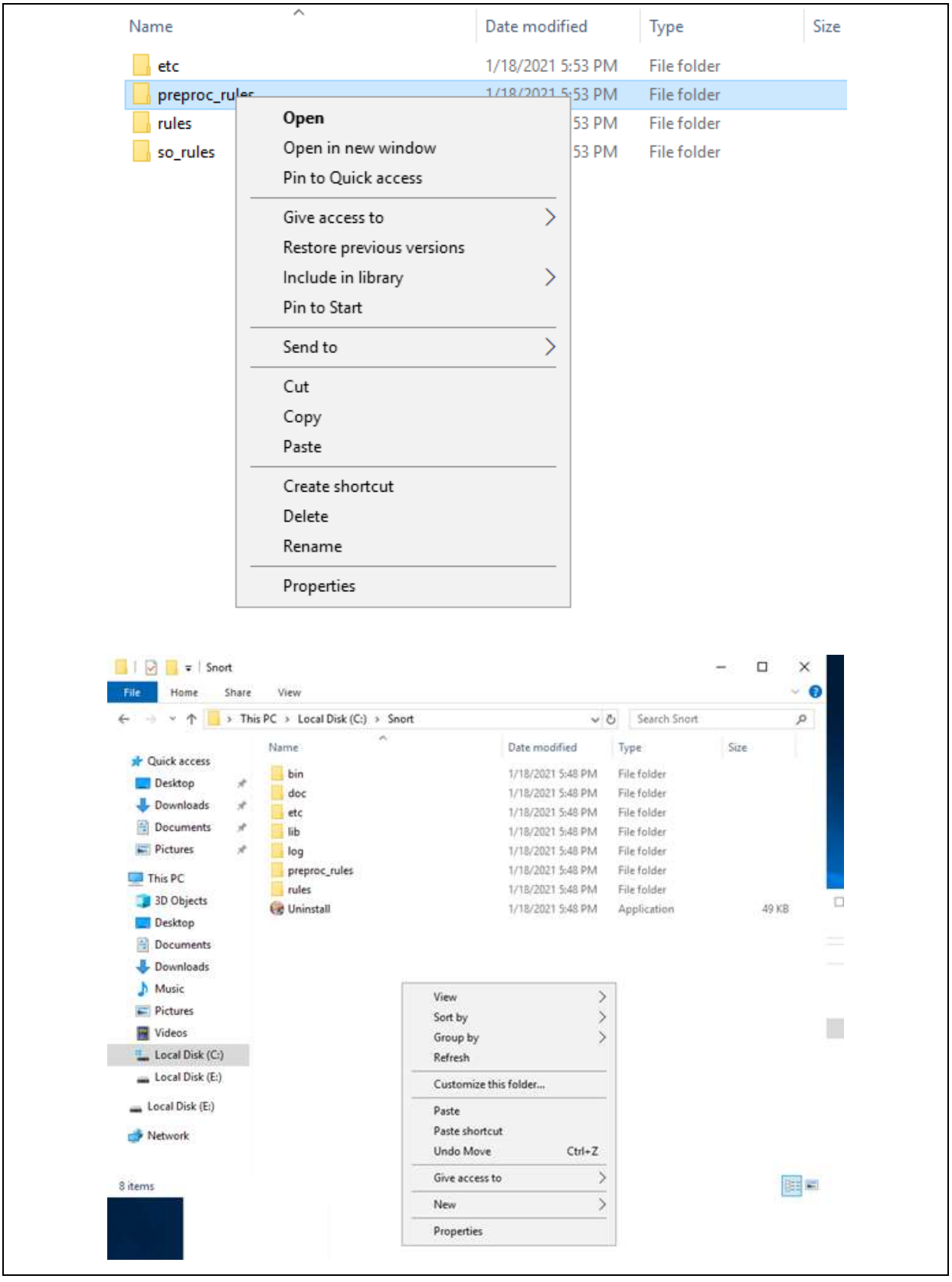


Step 6: Click OK on the pop up.

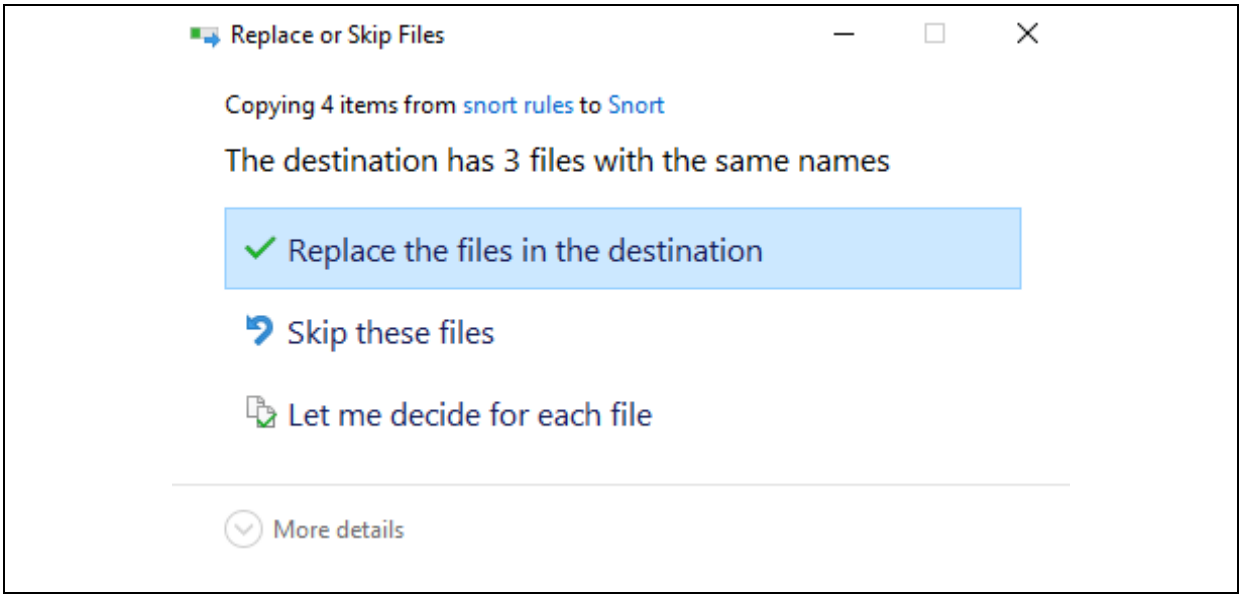


Step 7: Unzip the snort rules folder and put it in a new folder.

Step 8: Copy “preproc_rules” into the Snort Folder “C:\Snort”

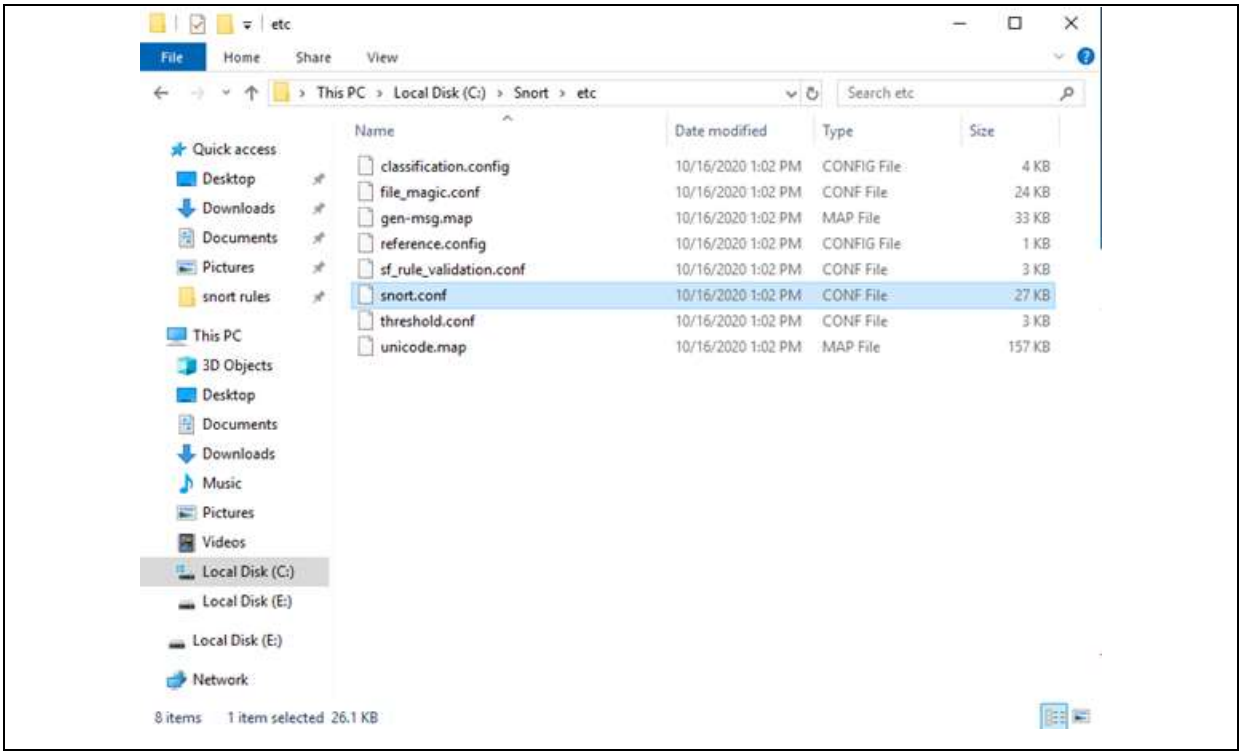


If there is a prompt to Replace or skip files Click “Replace the files in the destination.

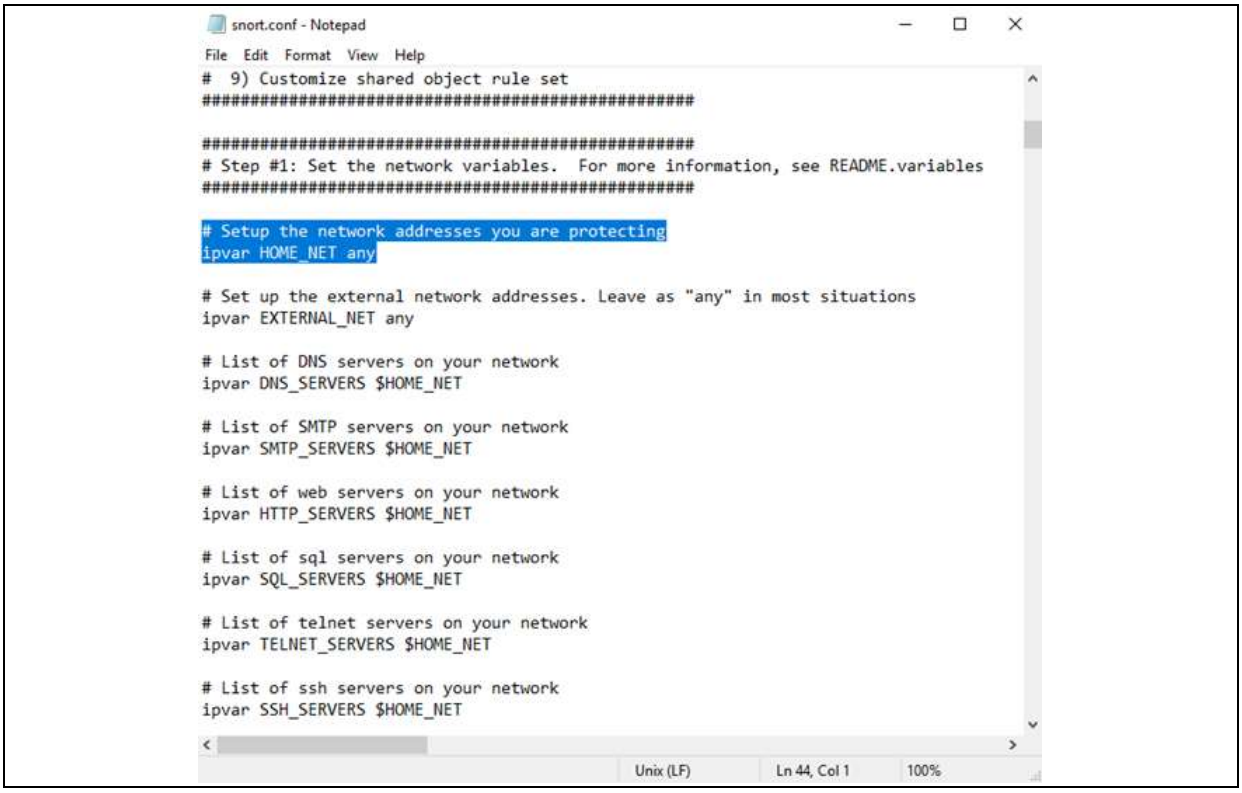


Step 9: Do the same for the rules folder.

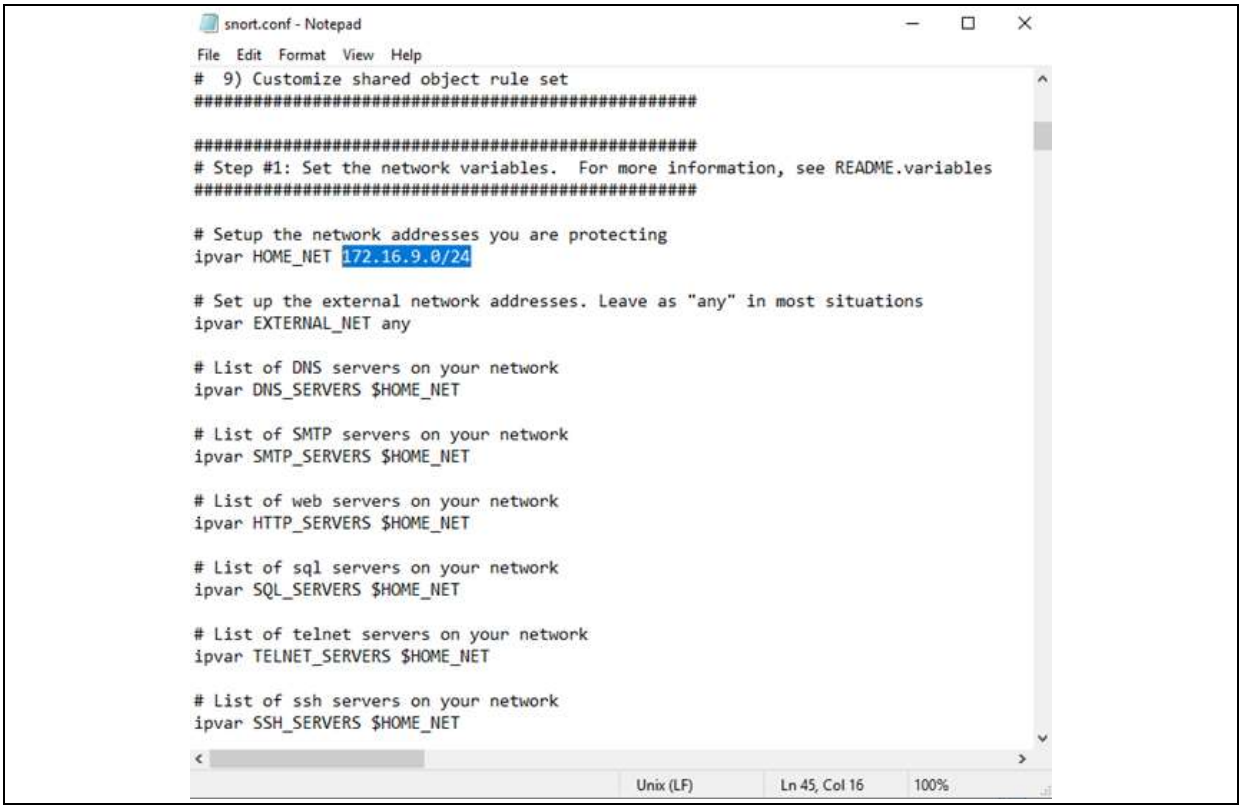
Step 10: Configure Snort. Go to “C:\Snort\etc”. Find “snort.conf” and open with Notepad or Notepad++.



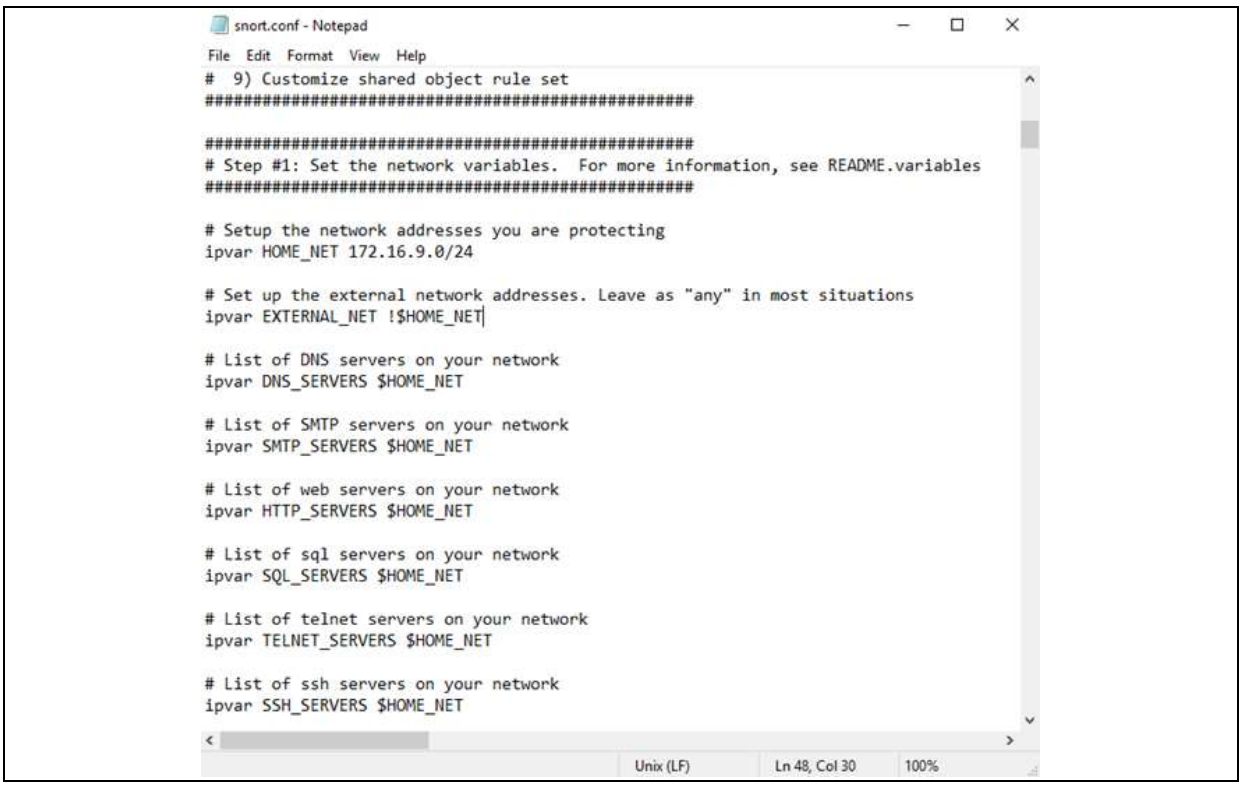
Step 11: Once in snort.conf look for “ipvar HOME_NET any”.



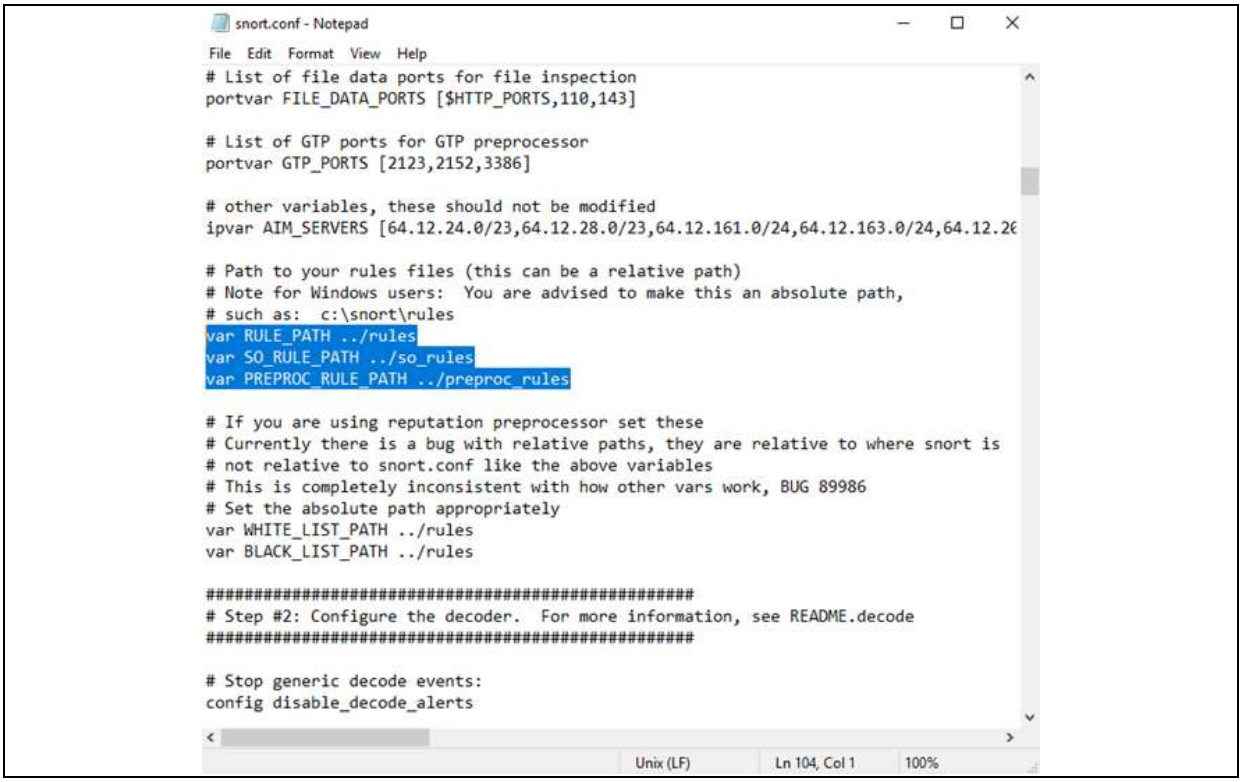
Step 12: Input the network IP as shown in the picture.



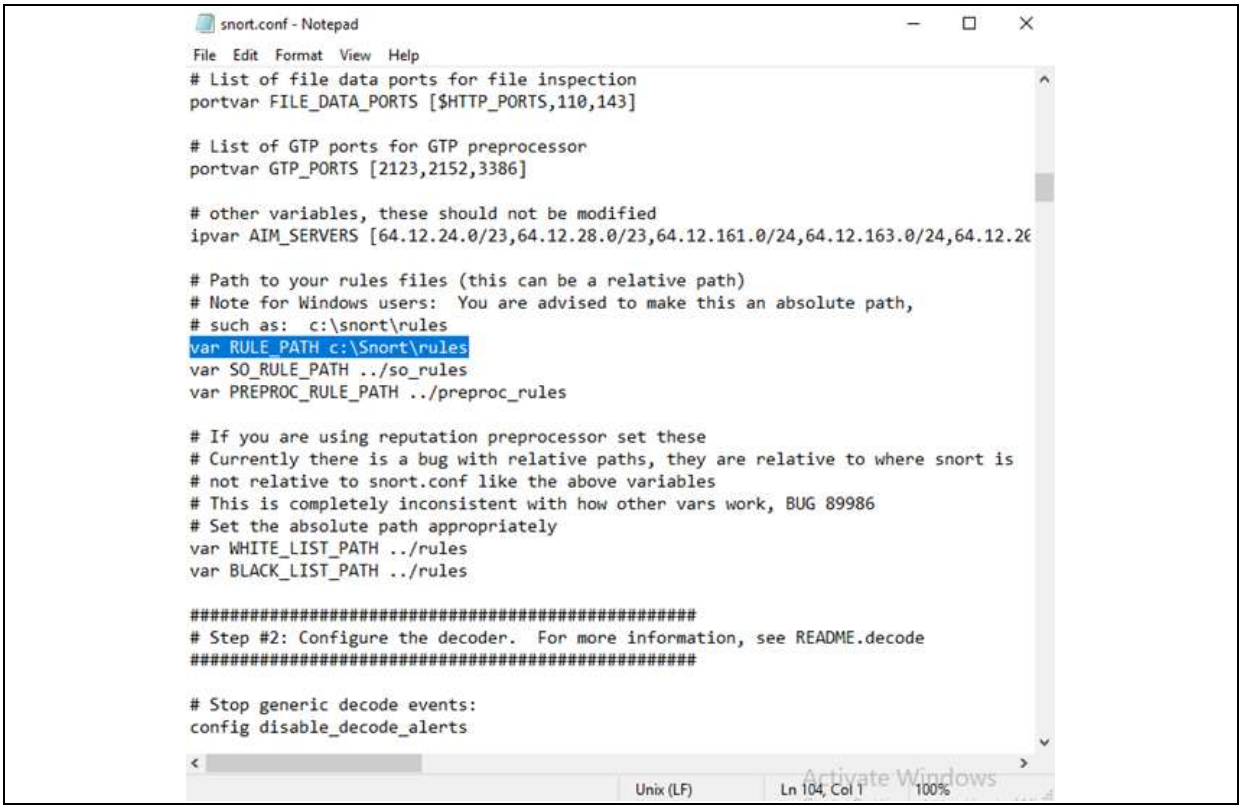
Step 13: On the Next line “ipvar EXTERNAL_NET any” input “!$HOME_NET” as shown in the picture.



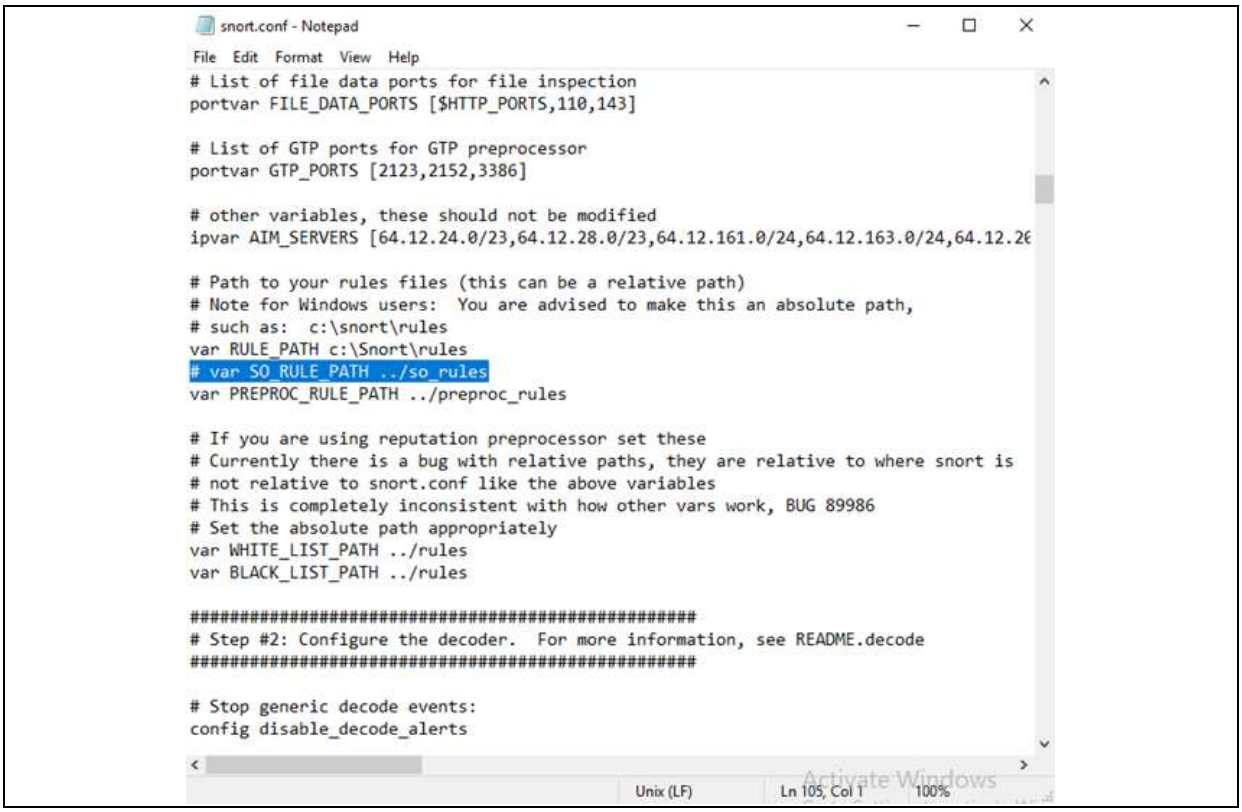
Step 14: Look for these 3 variables as shown in the picture (line 104).



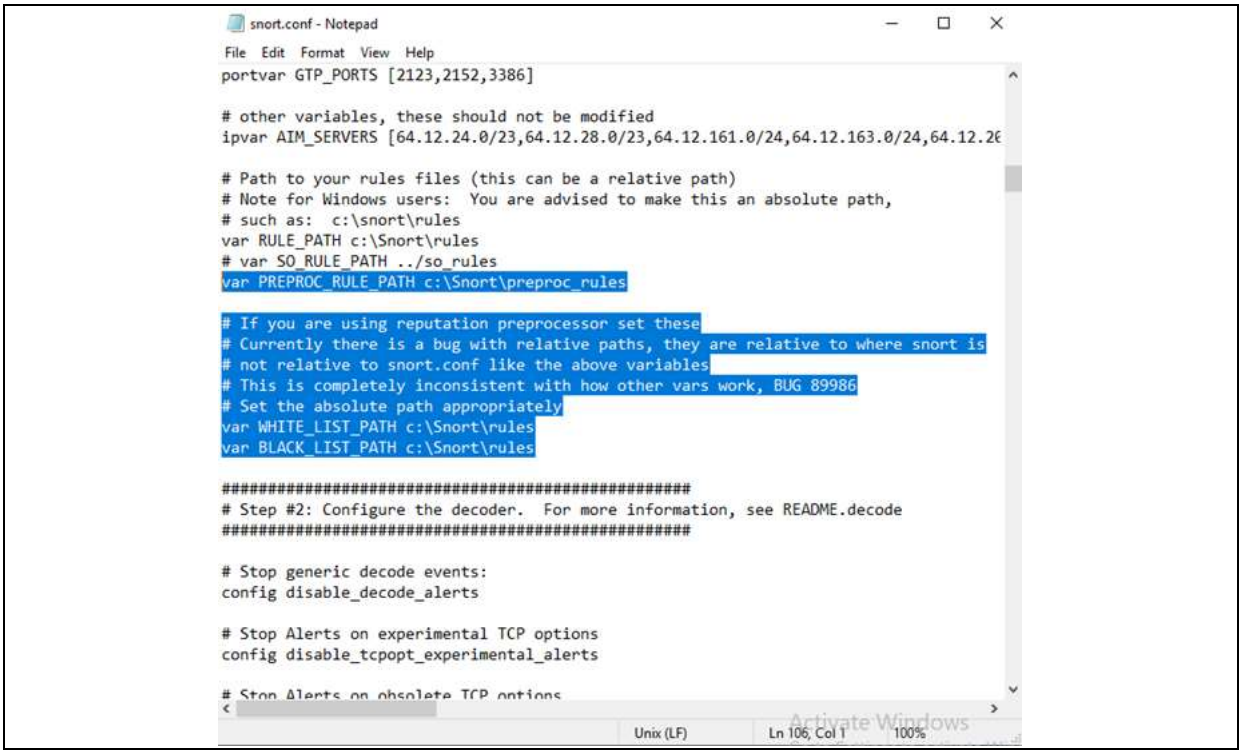
Step 15: Change “var RULE_PATH ../rules” to “var RULE_PATH c:\Snort\rules”.



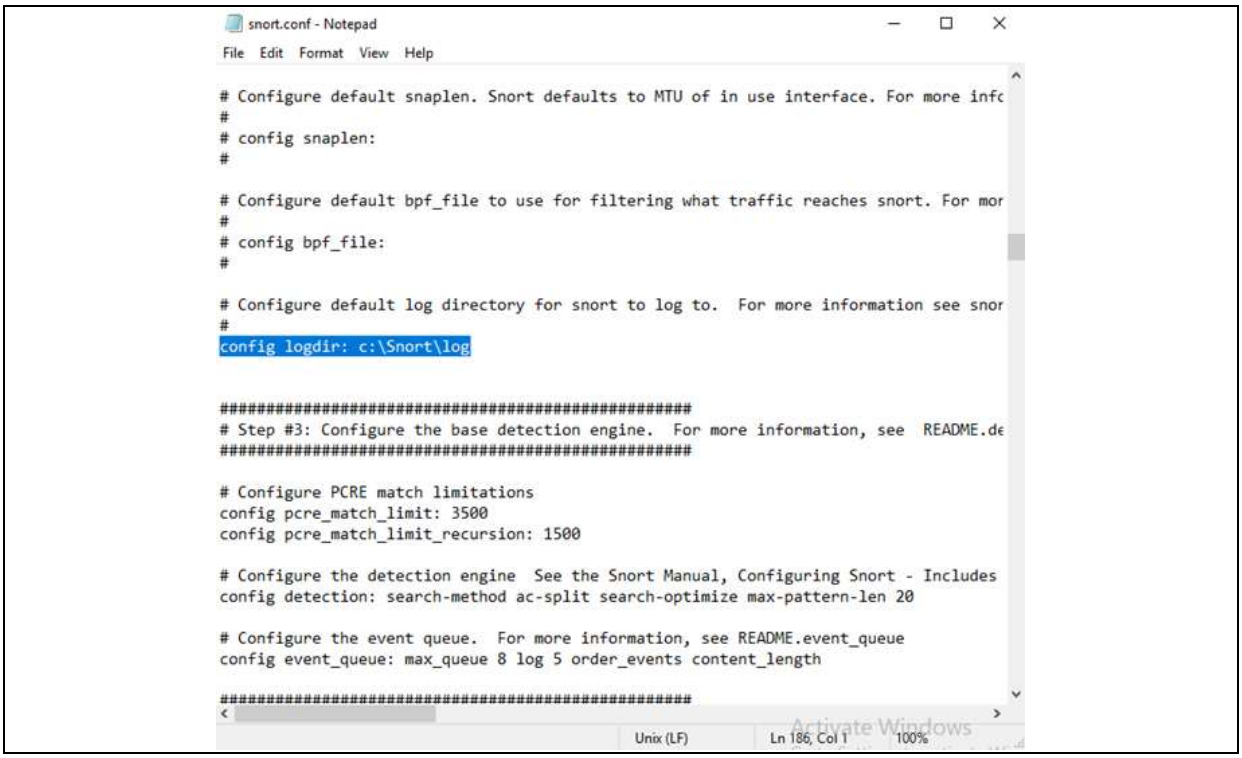
Step 16: Comment out “var SO_RULE_PATH ../so_rules” using # (it is for linux)



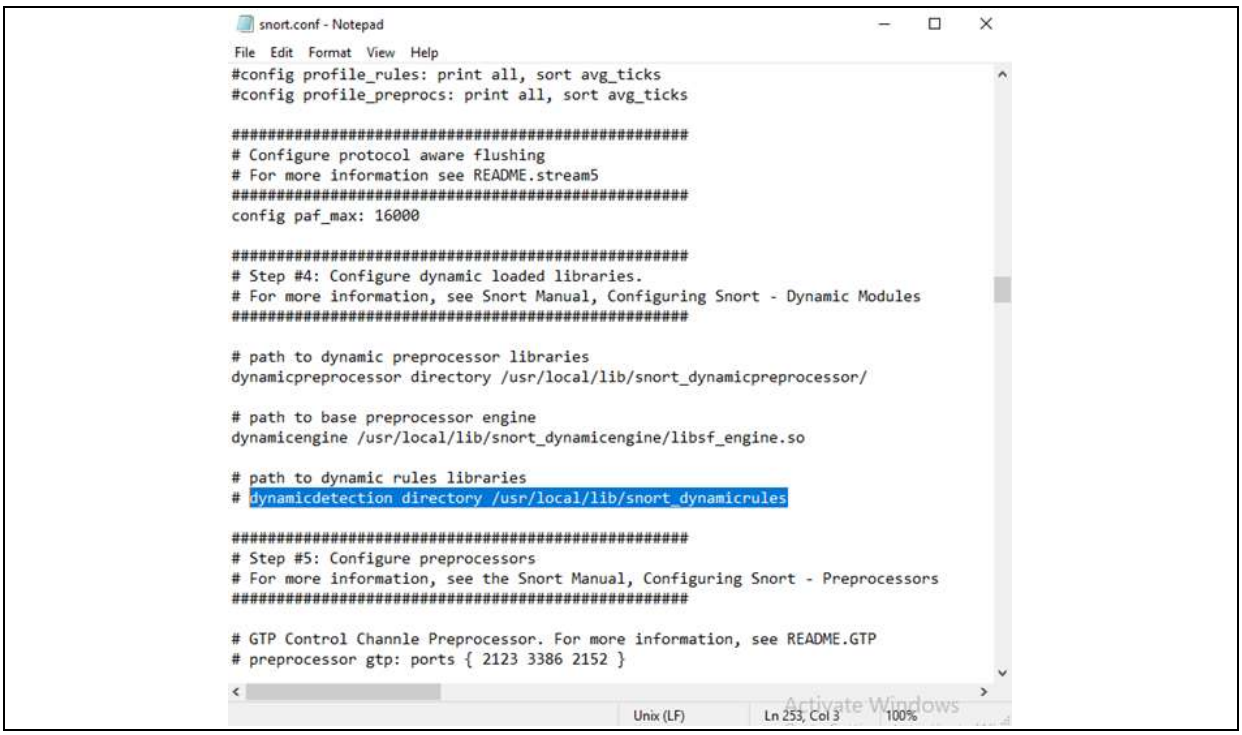
Step 17: Change "var PREPROC_RULE_PATH ../preproc_rules" to "var PREPROC_RULE_PATH c:\Snort\preproc_rules". Do the same for "var WHITE_LIST_PATH" (line 113) and "var BLACK_LIST_PATH" (line 114)



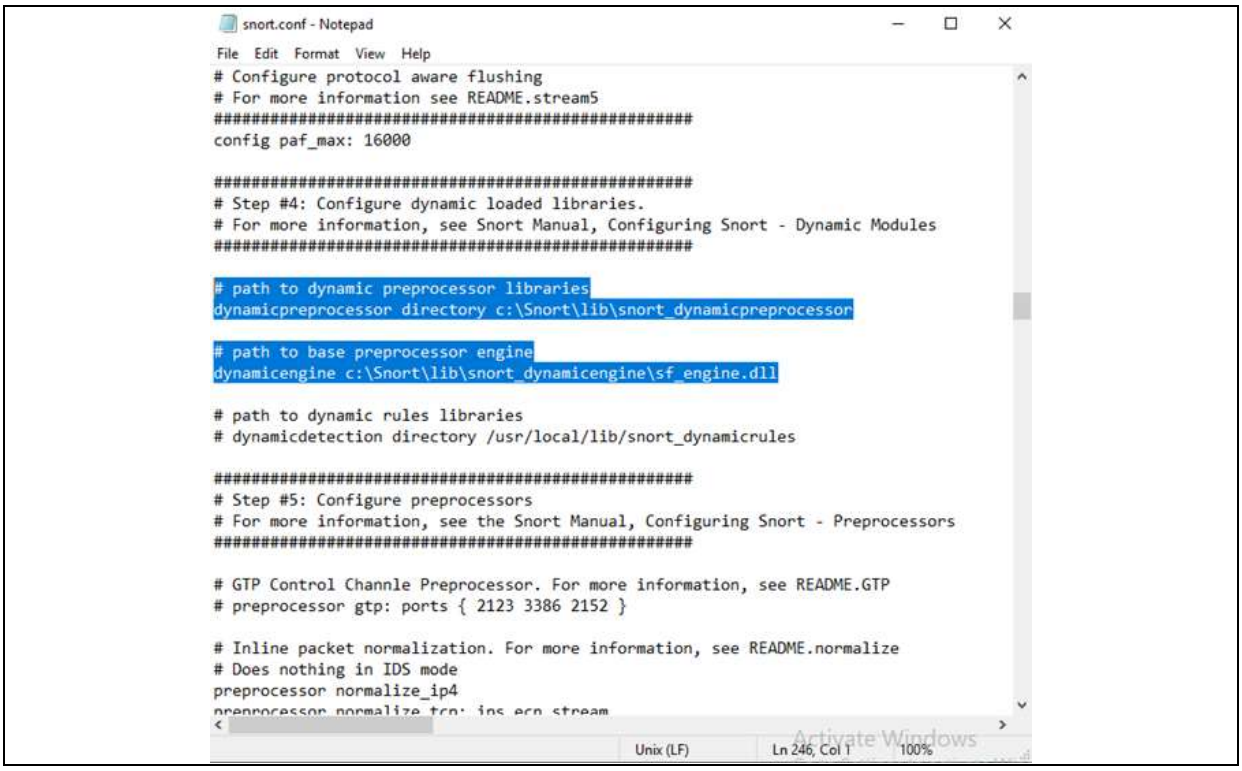
Step 18: Assign the config log directory (line 186). Make sure to delete the #.



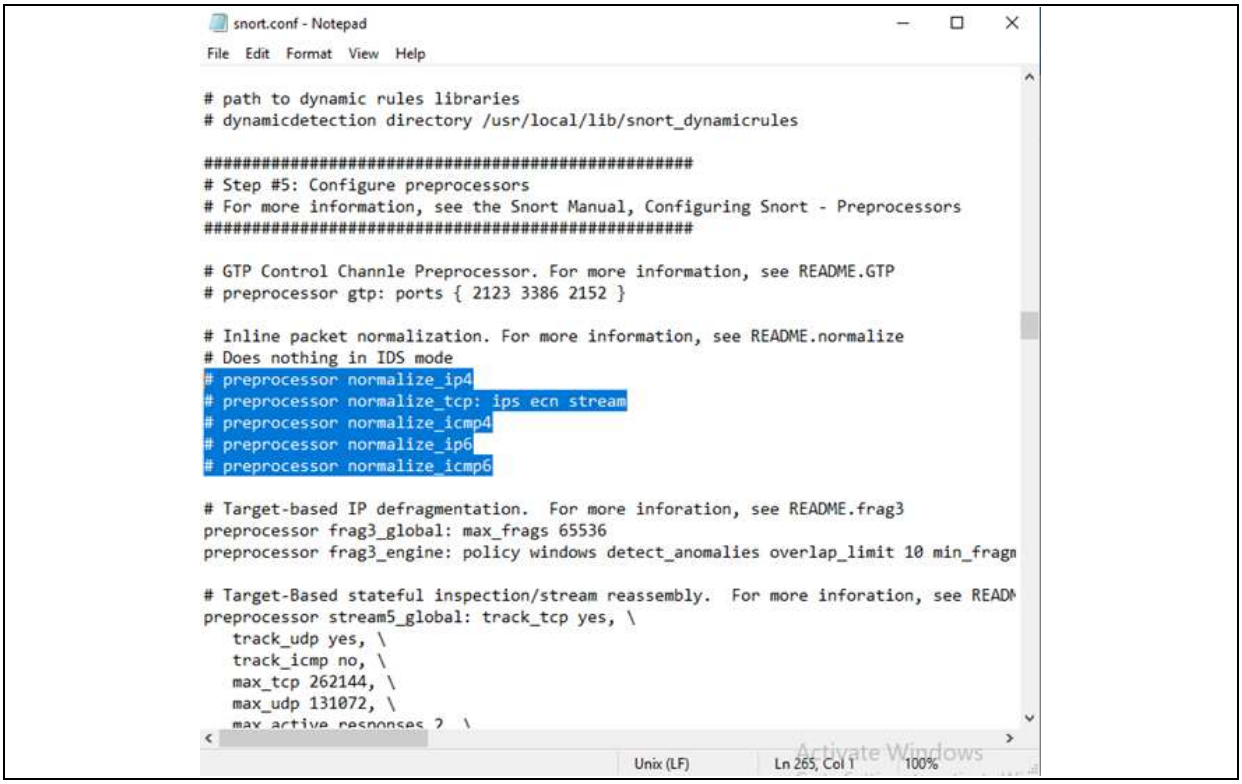
Step 18: Comment out line 253 “dynamicdetection directory /usr/local/lib/snort_dynamicrules”



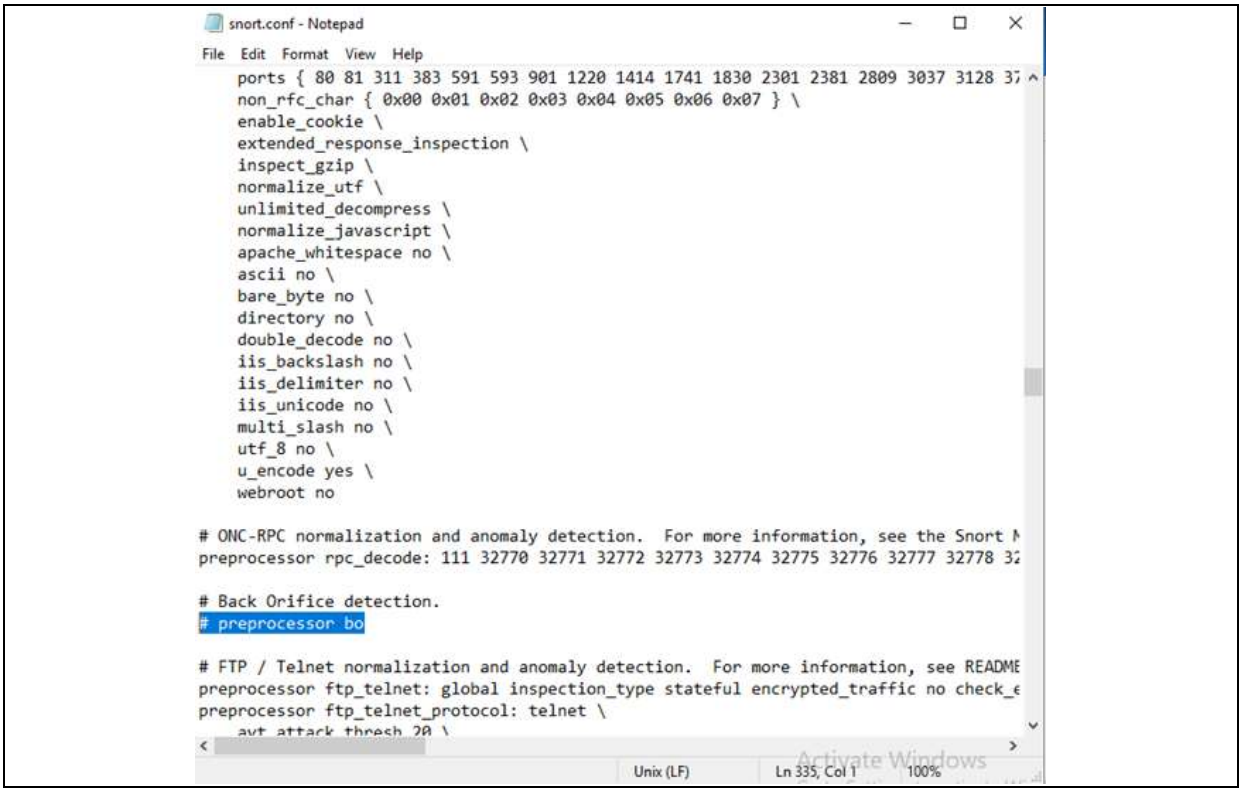
Step 19: Assign the path to dynamic preprocessor libraries and base preprocessor engine.



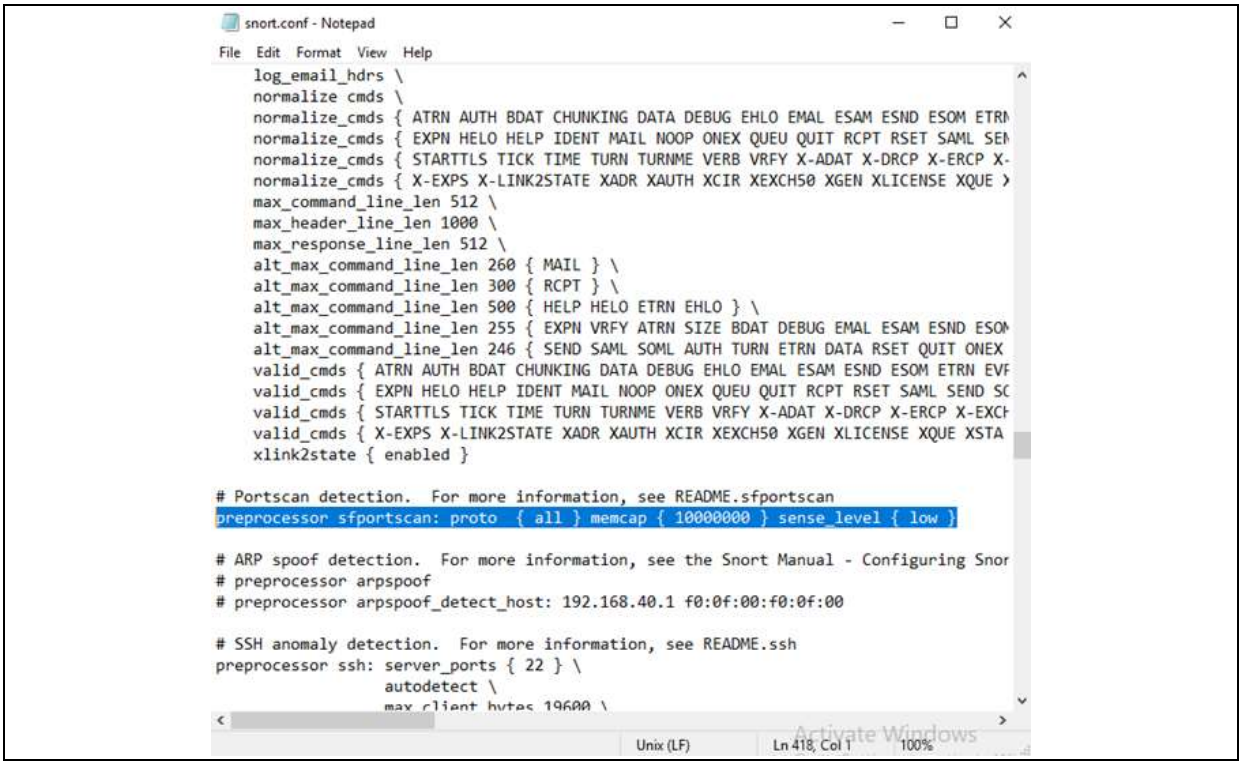
Step 20: Comment out using #, lines 265 to 269



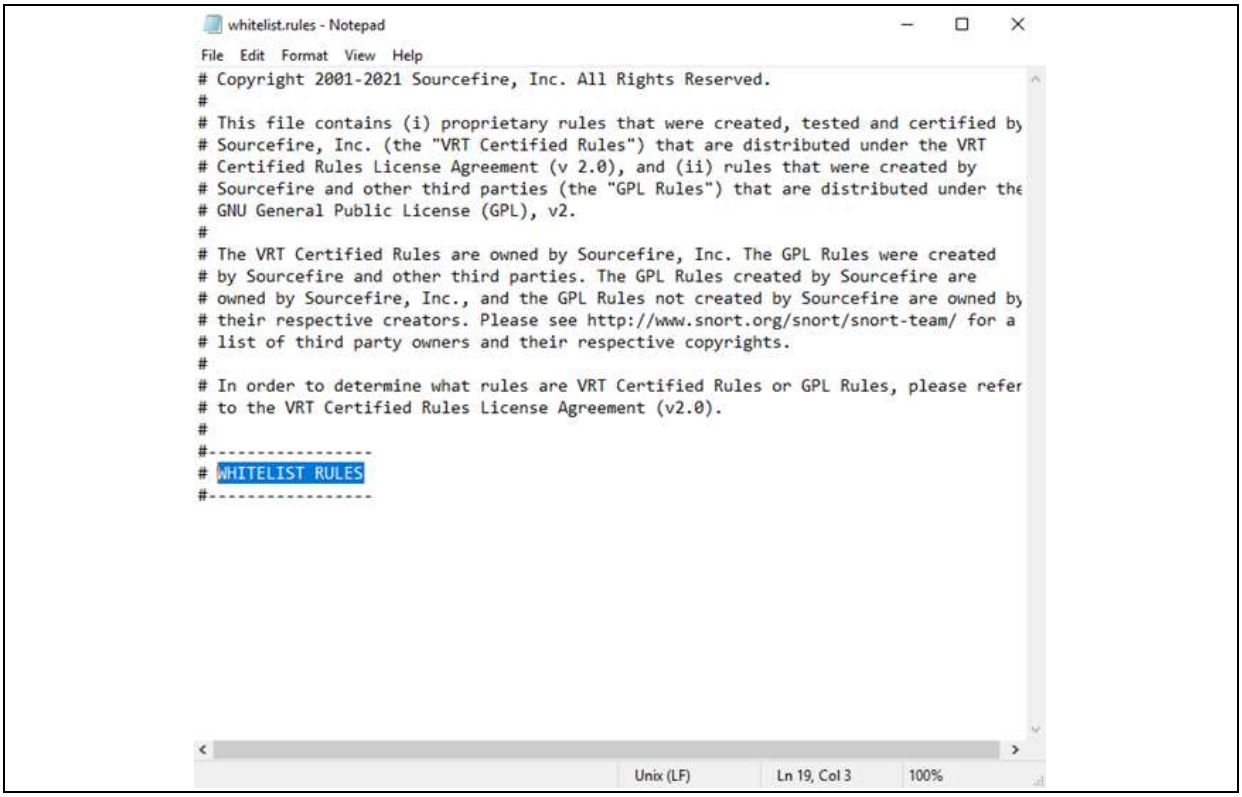
Step 21: Comment out line 335.



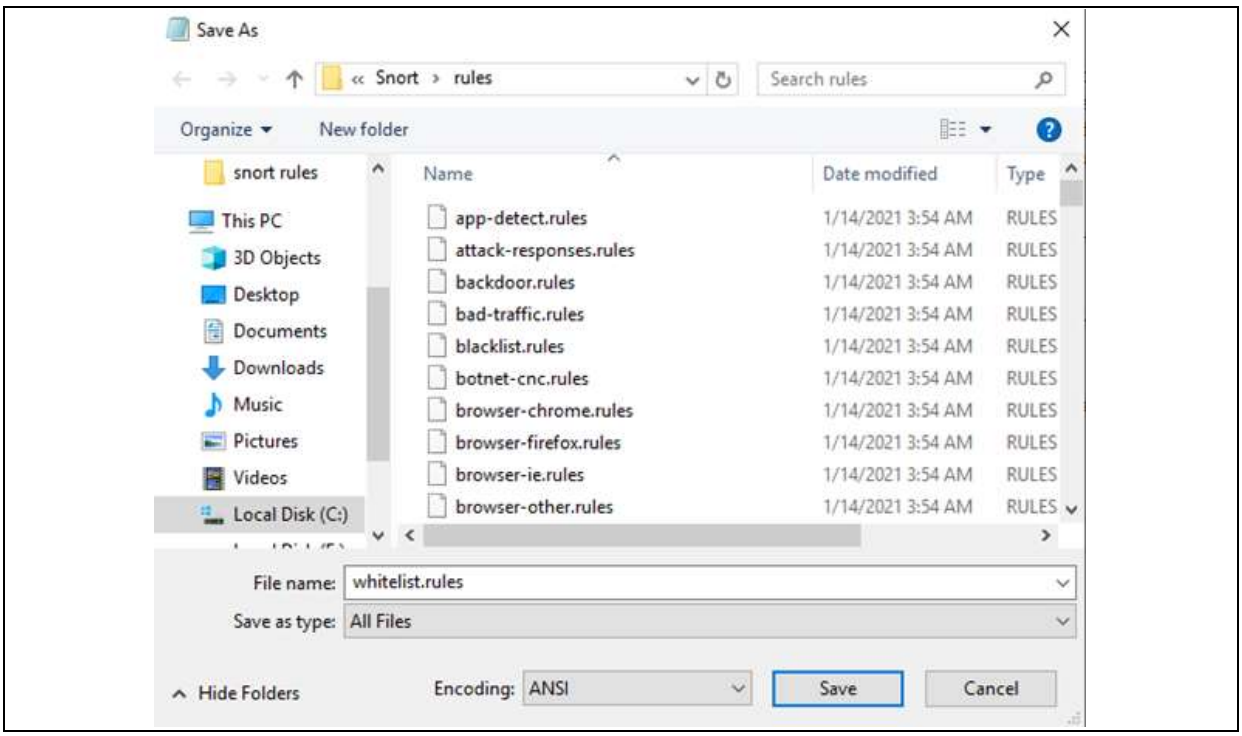
Step 22: Remove the # from line 418.



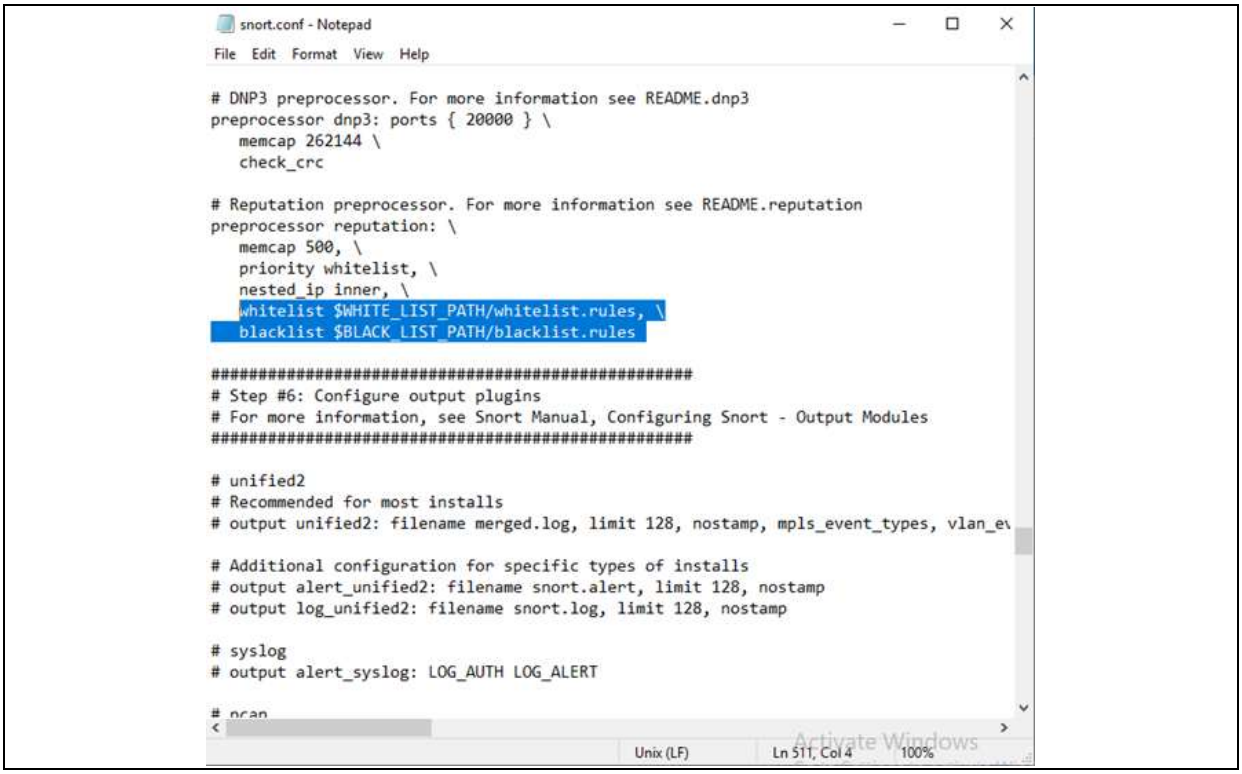
Step 23: Open blacklist.rules using notepad and change “BLACKLIST” to “WHITELIST”.



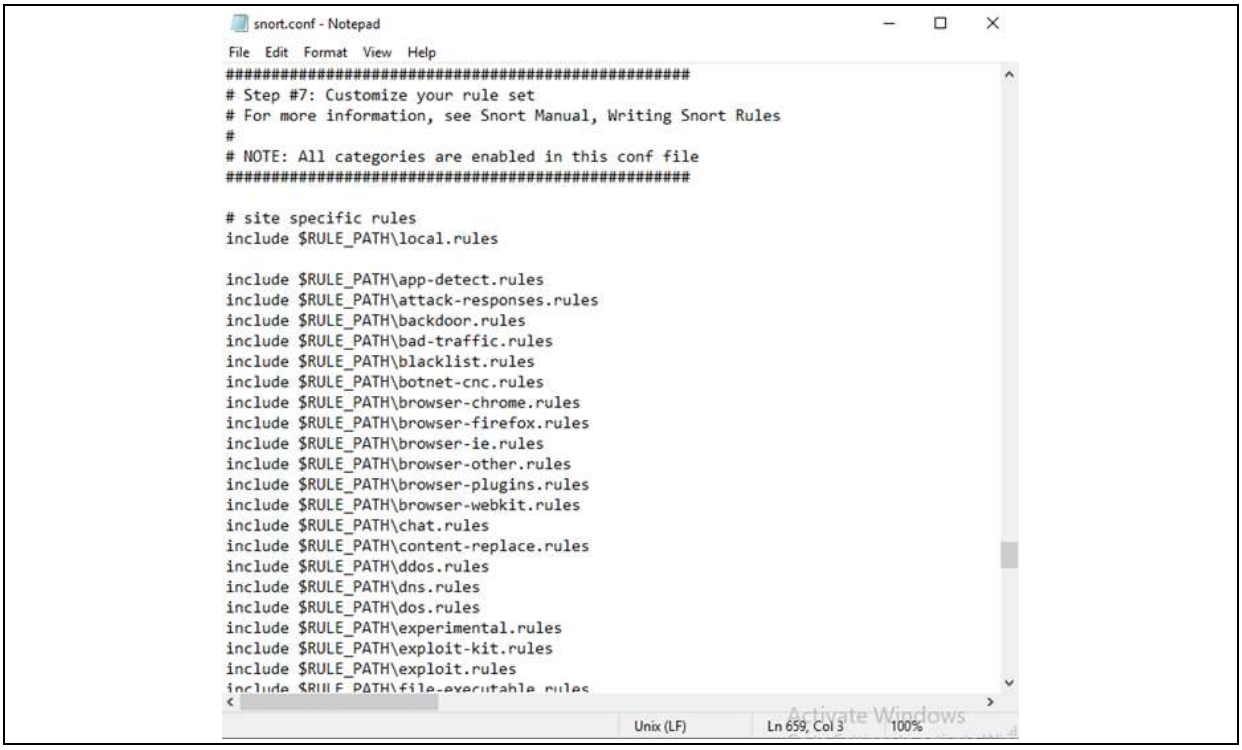
Step 24: Click “Files” and “Save As”. Name the file “whitelist.rules” and then click save. Make sure “Save as type” is in “All Files”.



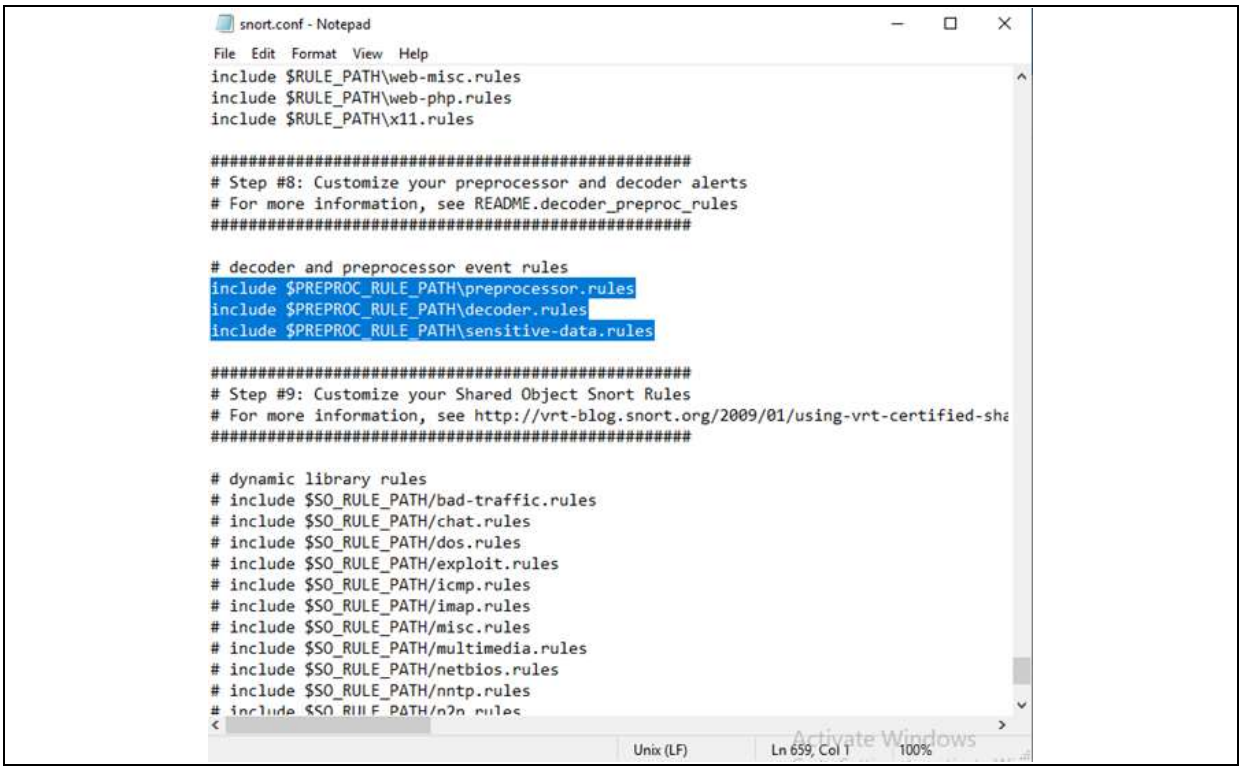
Step 25: Change the file name to match the file name in rules in line 511 and 512. Make sure to change the / to a \.



Step 26: Change all the / from line 546 to 661 to \.

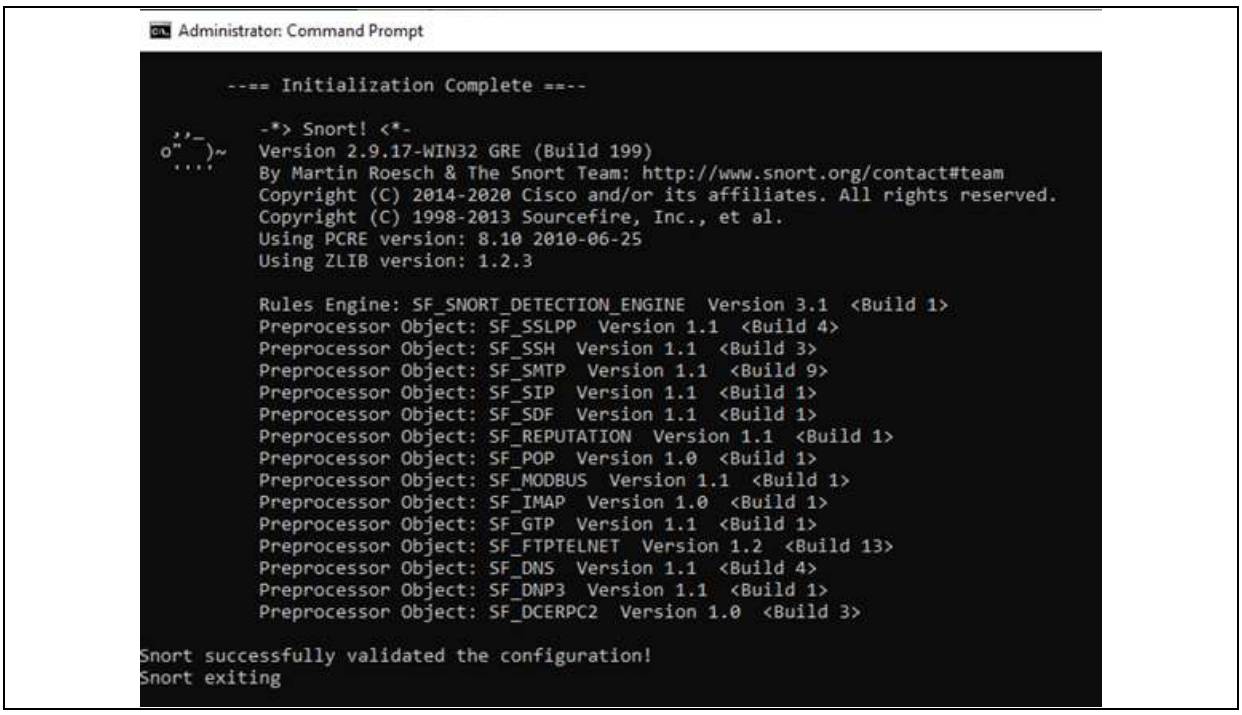


Step 27: Remove the # from line 659 to 661.



Step 28: Save the .conf file.

Step 29: Test .conf file by going to administrator command prompt, go to C:\Snort\bin and then typing the command “snort -i 1 -c c:\Snort\etc\snort.conf -T”



Testing Snort

We will be doing DoS and DDoS attacks to replicate a real-world setting; we used a kali linux virtual machines to perform the attacks by using the hping3 package in kali linux.

hping is a command-line oriented TCP/IP packet assembler/analyzer, it is able to send ICMP echo requests, supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode and the ability to send files between a covered channel.

A DoS attack is where the attacker seeks to make the machine or the network unavailable to its intended users by temporarily. This attack is typically accomplished by flooding the target with unnecessary requests, attempting to overload the system and prevent some or all legitimate requests from being fulfilled. This attack is typically characterized by an explicit attempt by attackers to prevent the legitimate use of a service.

A DDoS is where the attacker uses more than 1 unique IP address, often thousands of them. Since the incoming traffic flooding the victim originates from many different sources, it is impossible to stop the attack simply by using ingress filtering. It makes it difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

Before we could test Snort against these attacks, we needed to set the rules in which Snort will use to identify the attack. To create these rules we go to “c:\Snort\etc\rules\local.rules”. This is where we will write the rules, this first rule we will be writing is to enable snort to detect an ICMP flooding attack.

Here we type the following:

alert icmp any any -> $HOME_NET any (msg:"ICMP flood"; sid:1000001; rev:1; classtype:icmp-event; detection_filter:track by_dst, count 500, seconds 3;)

Syntax of this rule:

Rule header:

- Alert – Rule Action. Snort will generate an alert when the conditions set are met.
- Any – Source IP
- Any – Source port
- -> - Direction from source to destination
- $HOME_NET – Destination IP address. This is the value in the snort.conf file.
- Any – Destination port

Rule Options:

- Msg: “ICMP flood” - A message in the alert
- sid:1000001 – Snort rule ID
- Rev:1 – revision number, allowing easier rule maintenance
- Classtype:icmp-event – Categorises the rule as an “icmp-event”
- Detection_filter: track by_dst – Snort tracks the destination IP for detection.
- Seconds 3 – sampling period

- Count 500 – if Snort detects more than 500 requests during the sampling period, an alert will be received.

This second rule is to detect SYN flooding and this is the rule:

alert tcp any any -> $HOME_NET 80 (flags: S; msg:"Possible DoS Attack Type : SYN flood"; flow:stateless; sid:3; detection_filter:track by_dst, count 20, seconds 10;)

Here we change the protocol to TCP and set the destination port to 80. The keyword flag checks if specific TCP flag bits are present, in this case it would be SYN flag. Sampling duration is set to 10 seconds and if there are more than 20 requests detected then we will receive an alert.

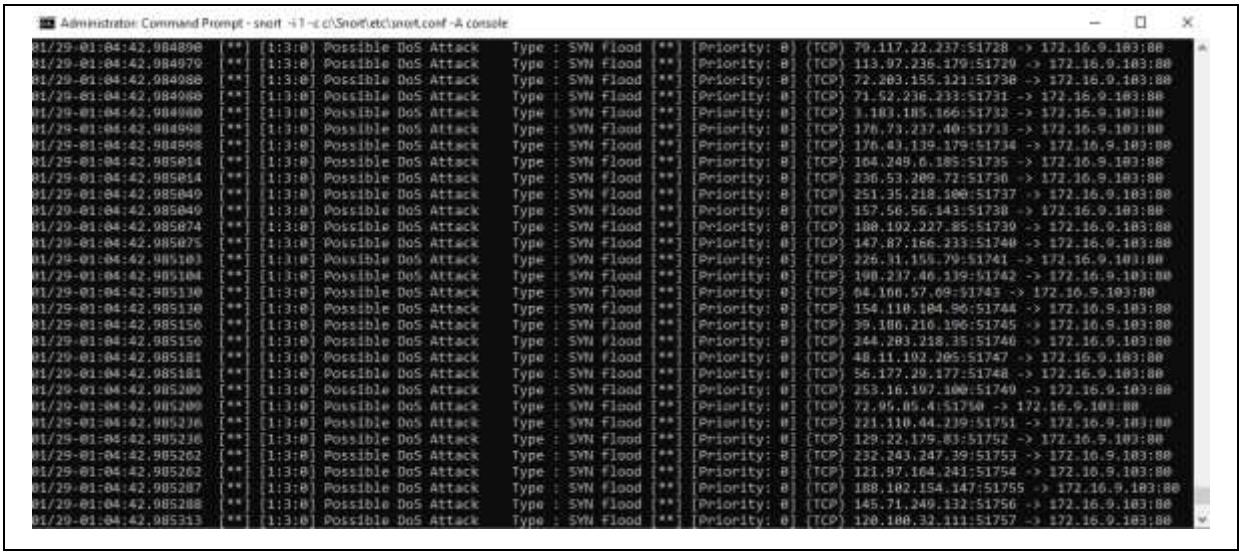
After setting saving those rules in “local.rules” we can now perform testing. Firstly we have to start Snort in IDS mode and tell it to display the alert to the console:

snort -i 1 -c c:\Snort\etc\snort.conf -A console

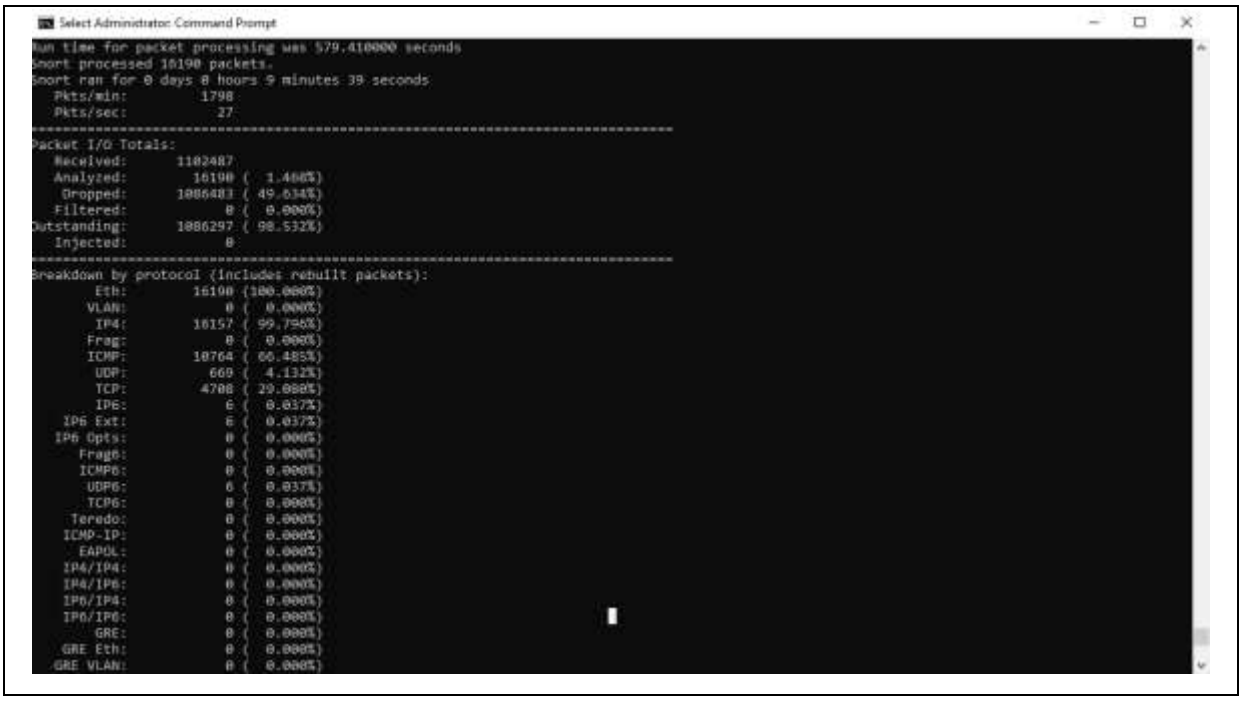
Using hping3 I input a command to simulate a SYN flood attack:

sudo hping3 --rand-source 172.16.9.103 -S -q -p 80 –flood

This is a SYN flood attack against port 80 and when we check back to the file server, we can see that there are a bunch of alerts popping up warning about a SYN flood attack.



In the picture below we can also see the summary while Snort was running.



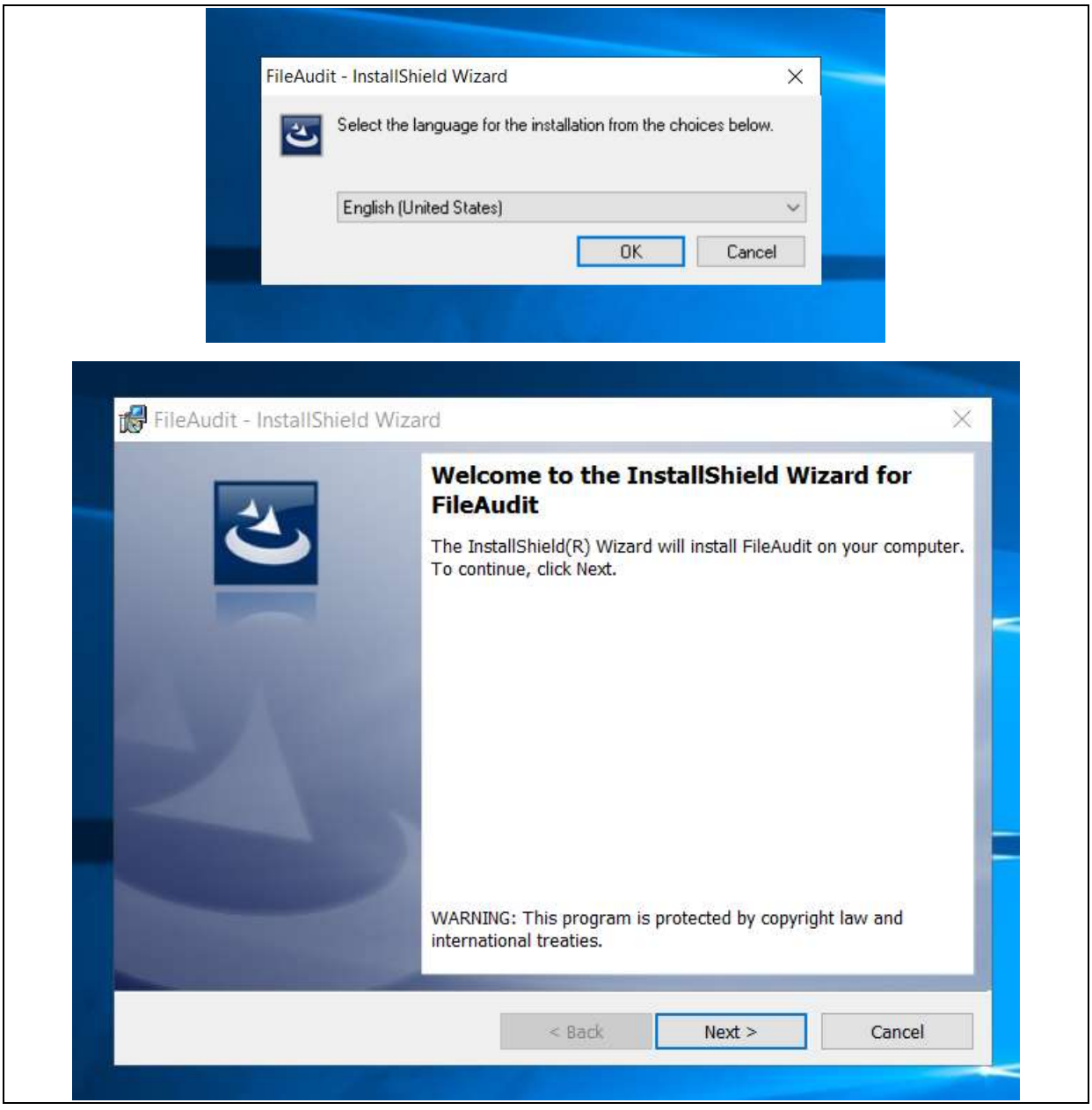
FileAudit

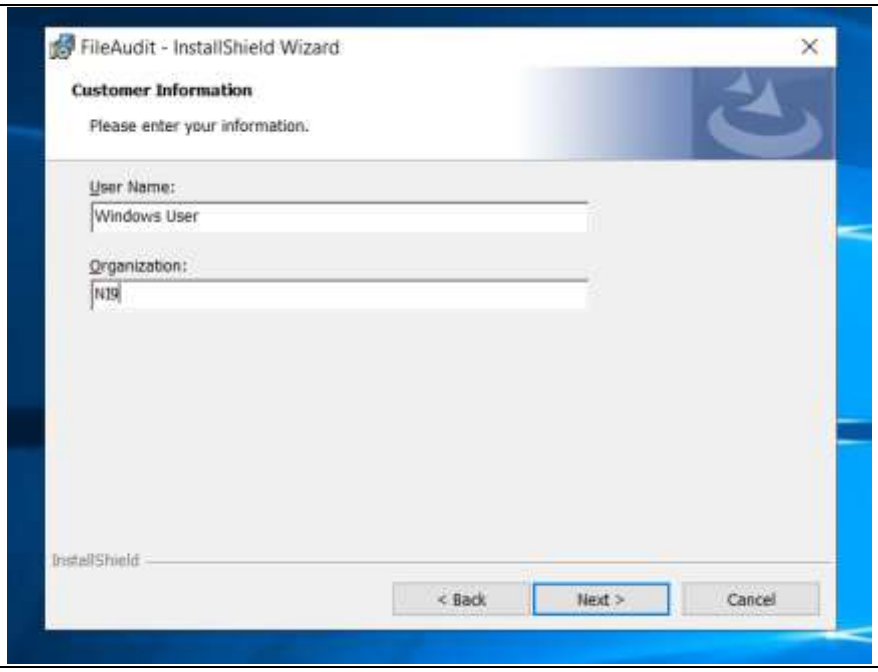
The audit tool can be downloaded from this link:

File Audit allows for automated generation of logs according to predefined alerts that can be configured within the application. We decided to use this tool as opposed to using the GPO to configure Windows Logs since this may be rather tedious for administrators and FileAudit's dashboard provides an intuitive and easy to use interface for easy navigation and configuration of various settings.

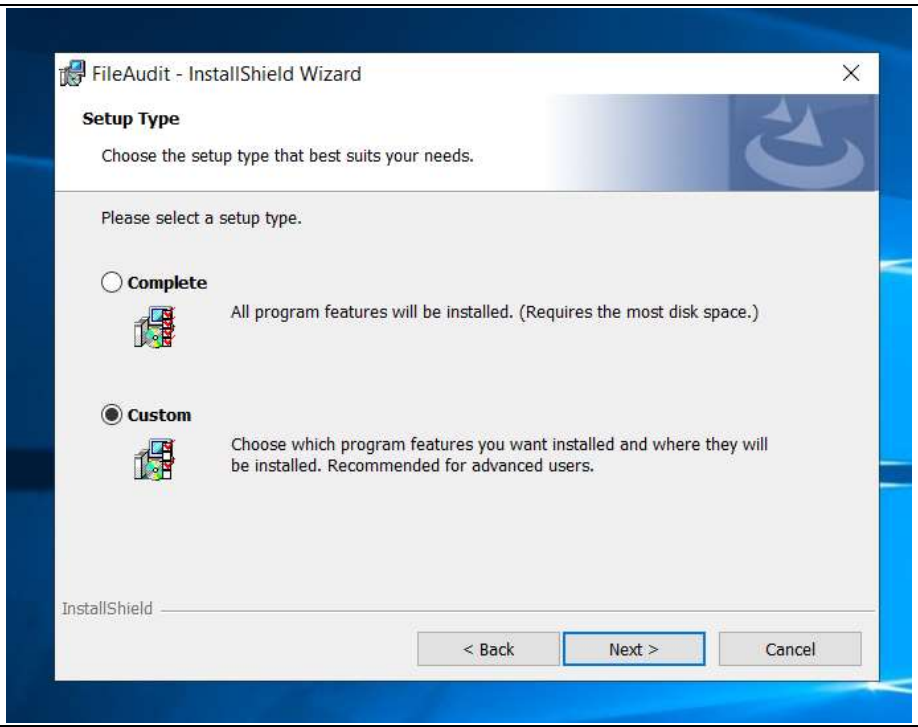
FileAudit Installation

Install FileAudit with all default options on the File Server.





This name and Organization do not have to be the same as the original domain name NI9.com, instead, any Organization Identifier can be used and username if being configured in a larger enterprise with multiple file servers for easy identification.

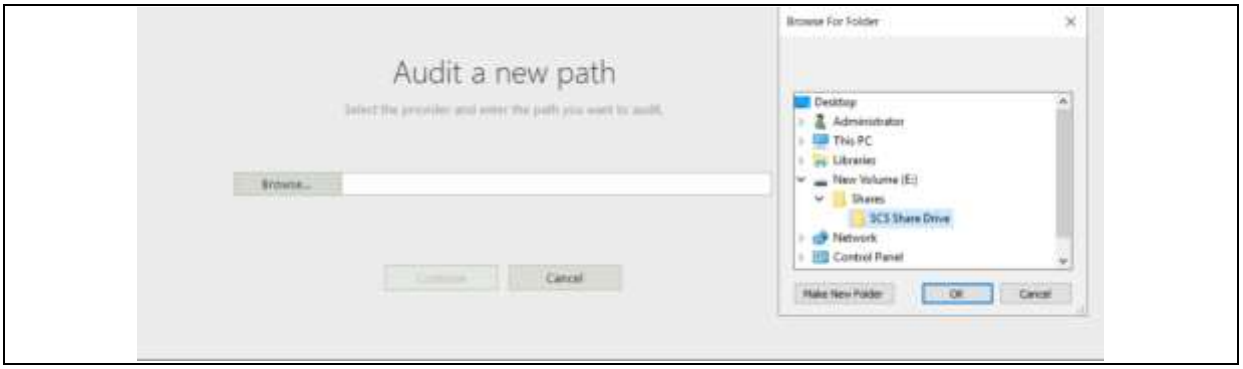


In this case complete or custom installation can be chosen. I explored with the Custom option and ended up going with the default Complete option instead.

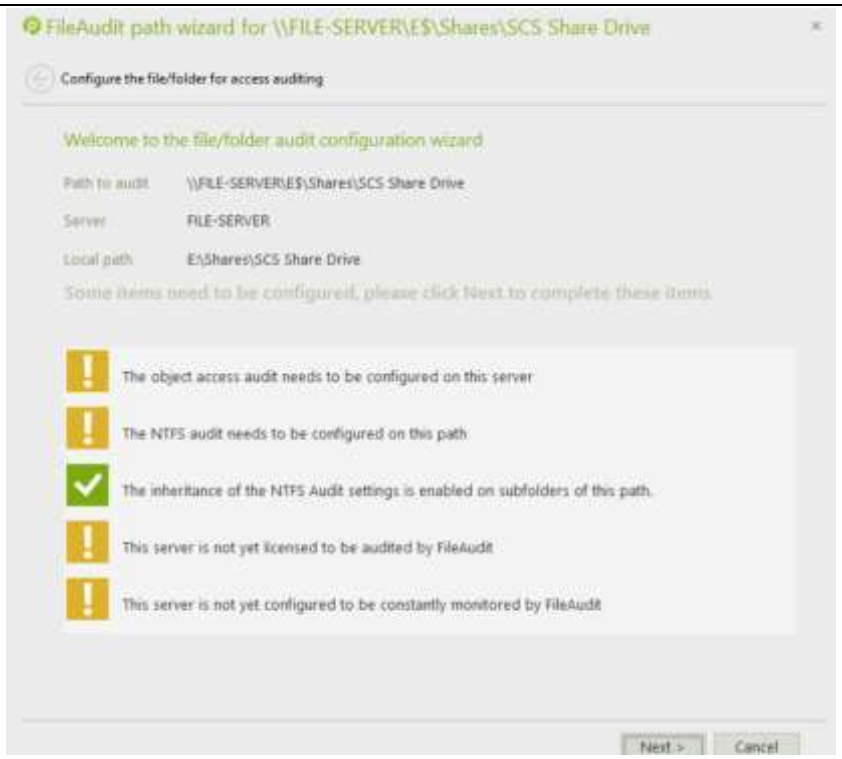
Configuration of FileAudit Tool

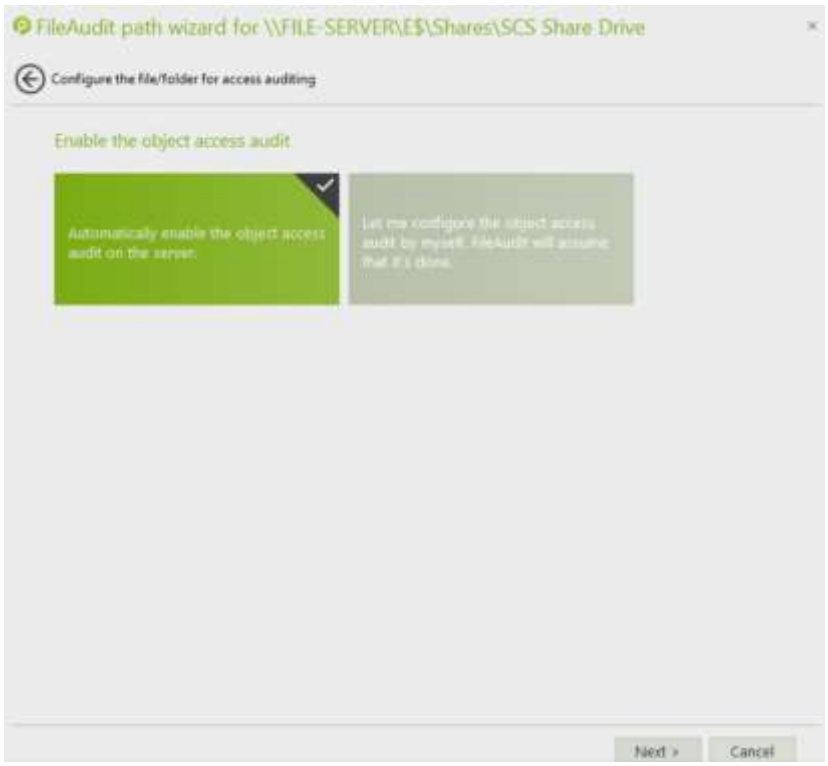
After installing the tool, the central dashboard will be displayed. Thereafter, we can proceed to configure the settings in the tool to do active monitoring of activities. Navigate to Windows Audit > Audit Paths and click on add a path.

Thereafter there is the option to indicate the file path (in this case we specify our shared folder at E:\\Shares\SCS Share Drive) and then click continue to allow an entry to be created so that the application can start tracking changes made in that particular path.

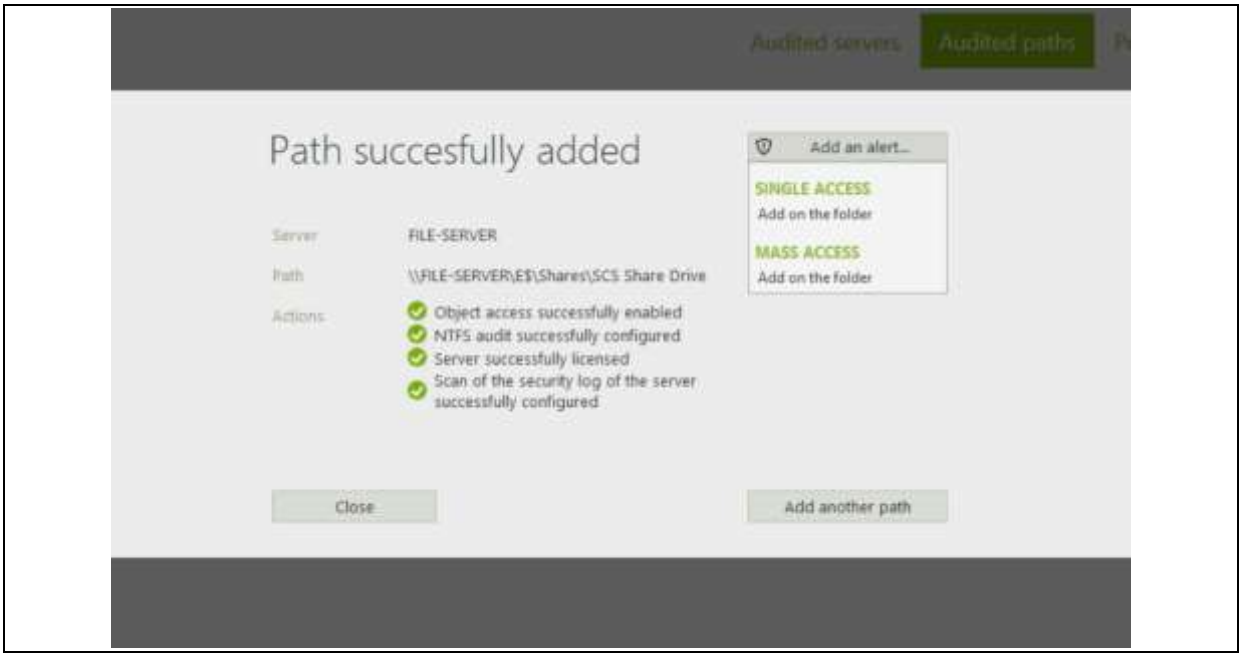


If some of the objects are not configured manually already through GPO (object access audit etc.), the application will prompt for further action and give the option for the issues to be resolved automatically or manually configured (we will choose automatic resolution in this case).

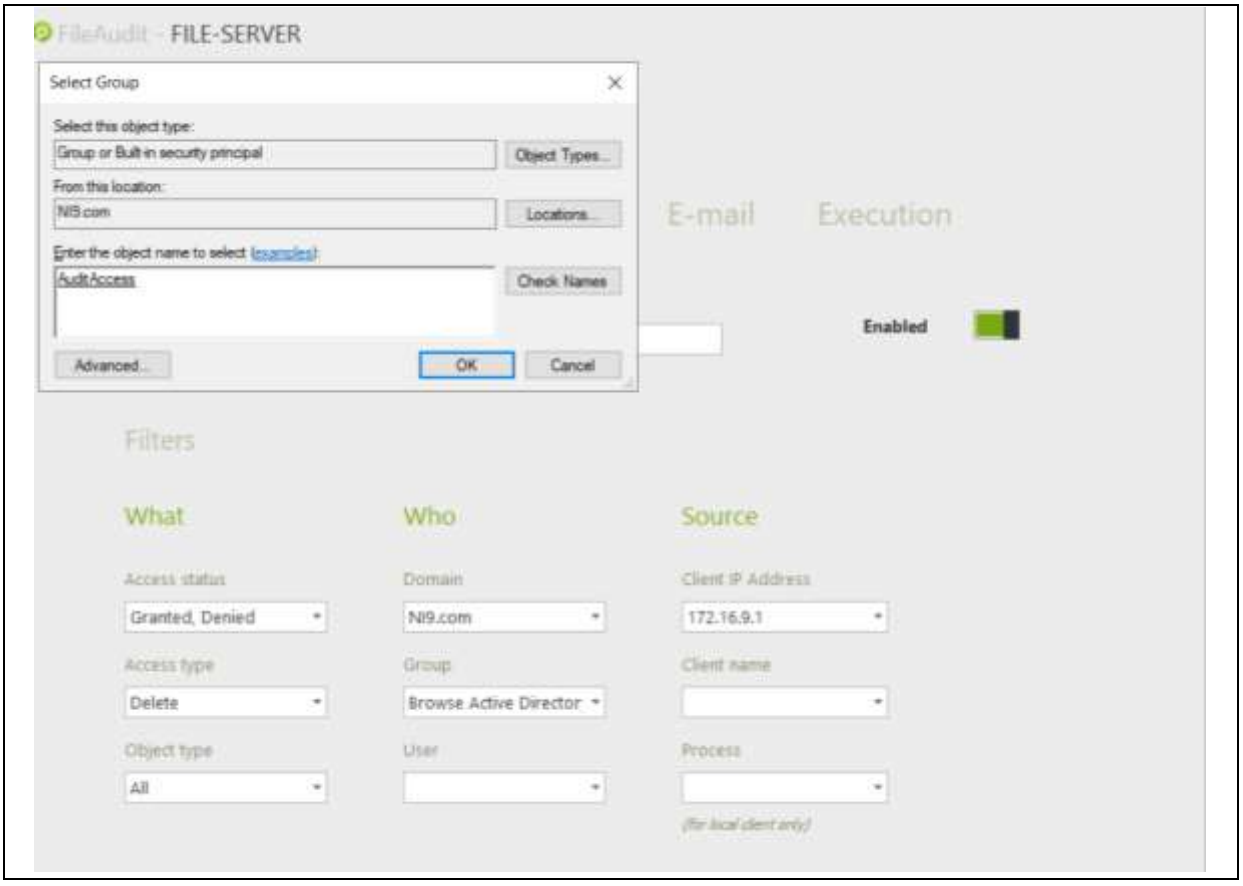




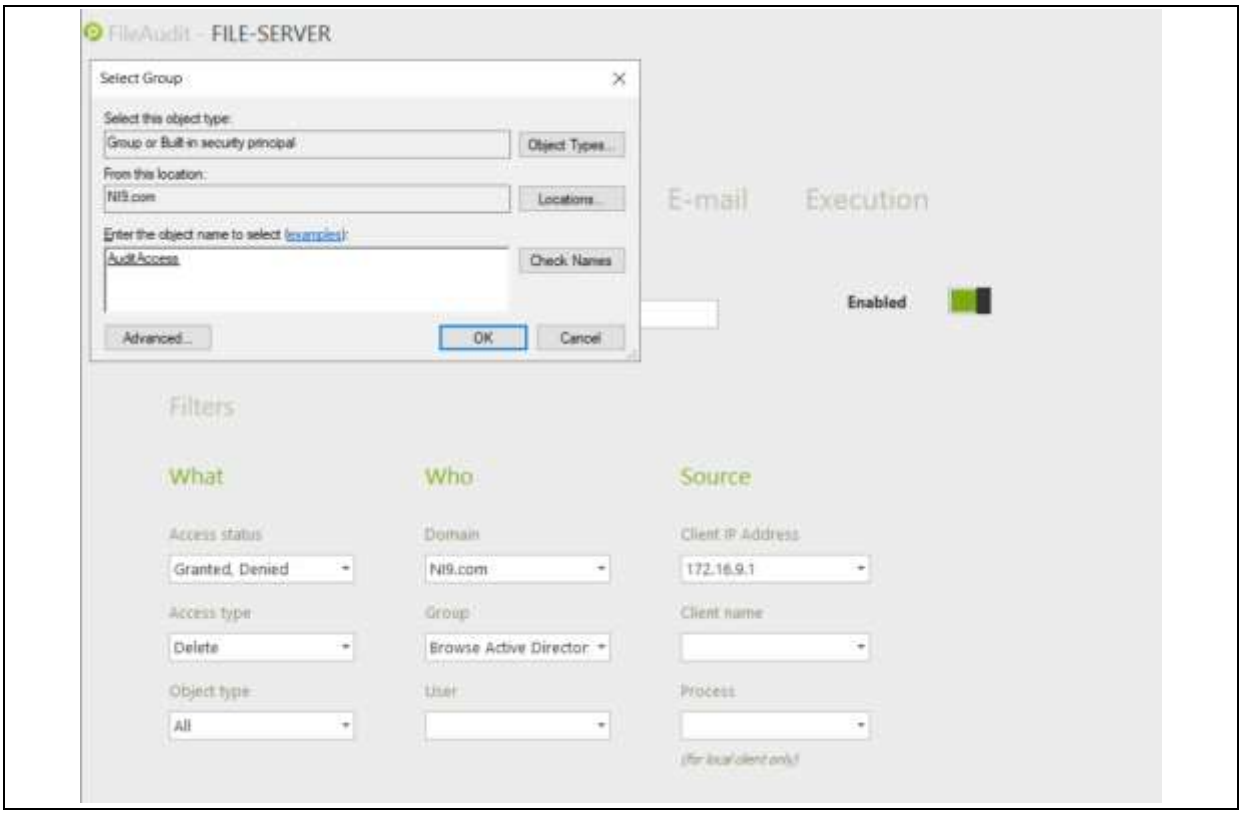
Once this is completed a success popup will appear indicating that the path has been successfully configured and will be monitored. There is also an option to configure alerts for single access (every time an action is conducted) and mass access (i.e. potential DDoS of the shared drive).



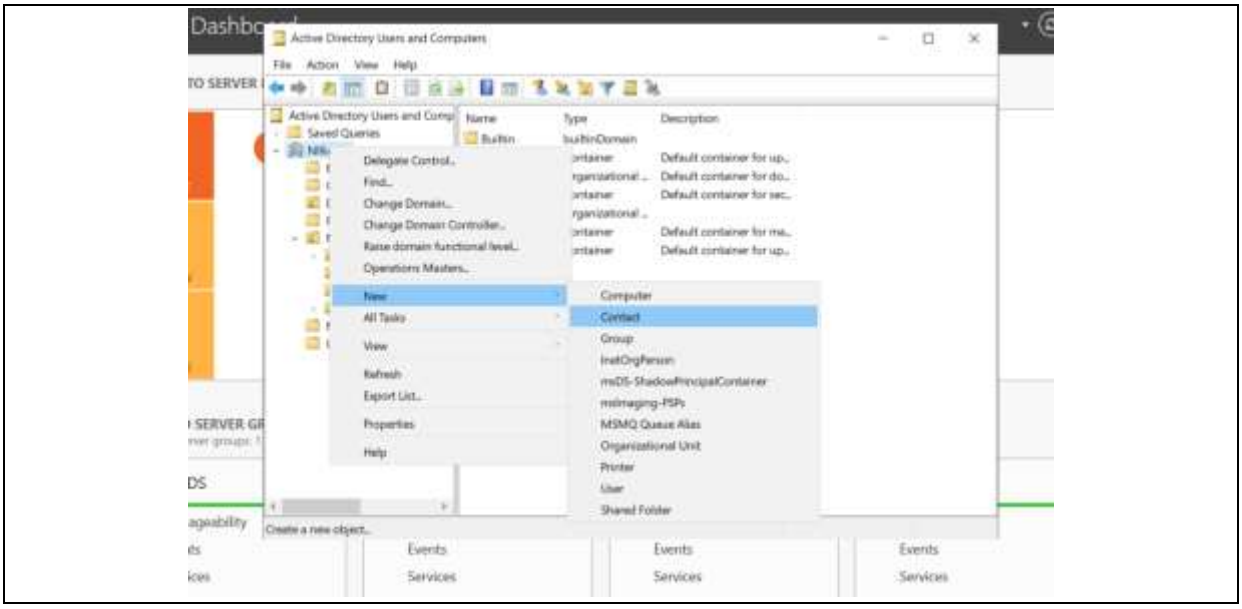
In this case we will be exploring the Single Access option. We are then prompted to fill in a few options as shown below.



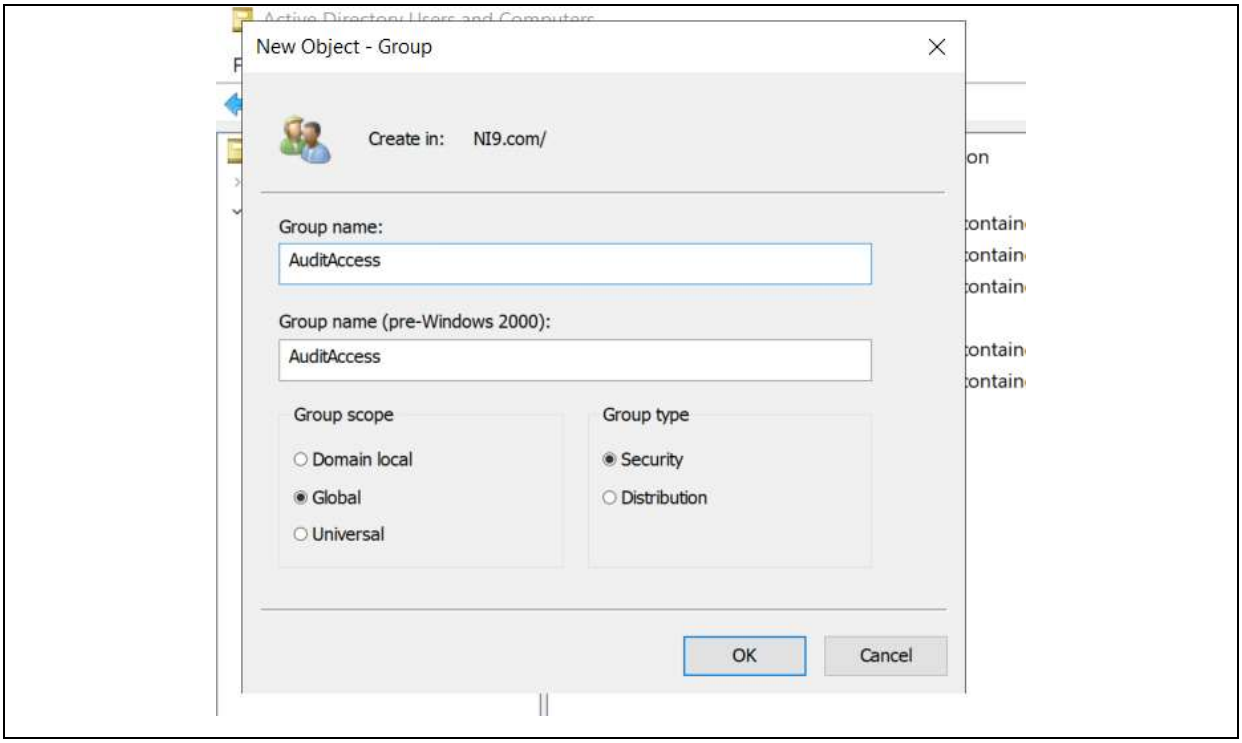
We are able to specify the Client IP to specify the target IP which will be used to access the resources in the shared folder. We can specify the access status (whether we want to track both Users who are Granted and/or Denied Permissions to the shared folder), access type (further narrow down the scope of what we are capturing—i.e. Read, Write Execute instances etc.).



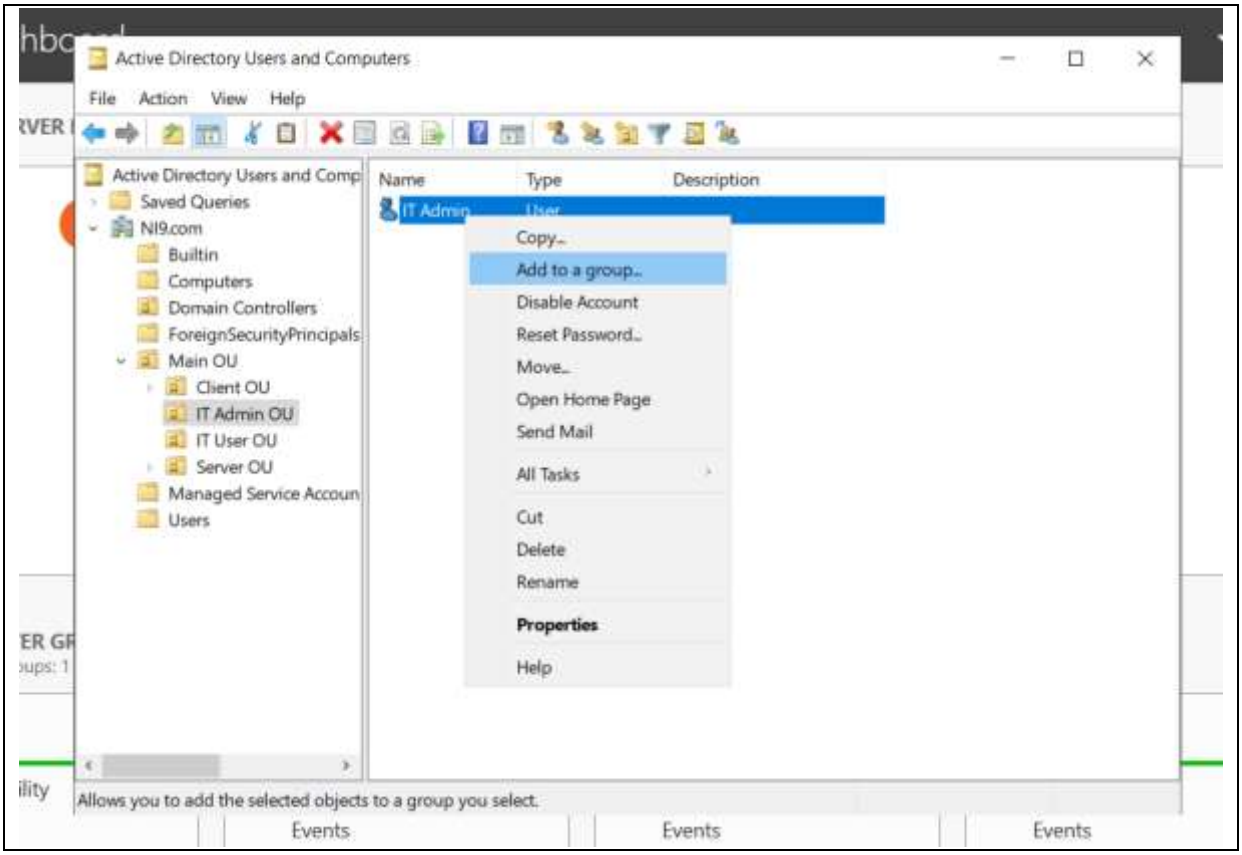
In this case, the Server would need to be connected to the active directory and since only Group or Built in Objects are permitted (and we cannot directly add a user), so we will have to create groups using the Active Directory Users and Computers. In the ADUC as shown below, right click on the domain NI9.com and select **New > Group**.



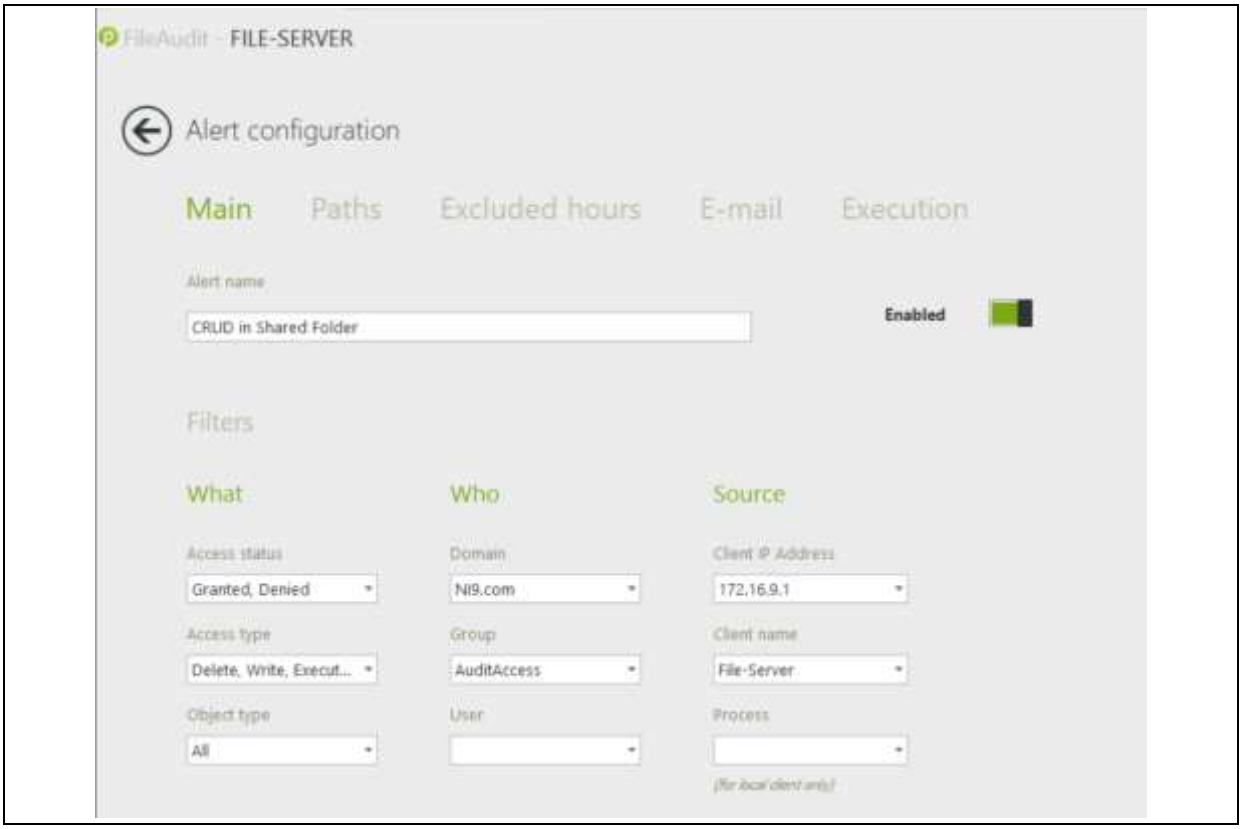
Make sure the group has a Global Group Scope so that it can added as part of the Access Control Listing and security group is selected (not distribution as we are not running an email service in the Active Directory Domain).



Thereafter, add the IT Admin user to the AuditAccess group just created so that the user activity will be captured in the logs.



The resultant page should look like this once the Group is properly configured and added. This alert logs entries for Create, Read, Update and Delete options



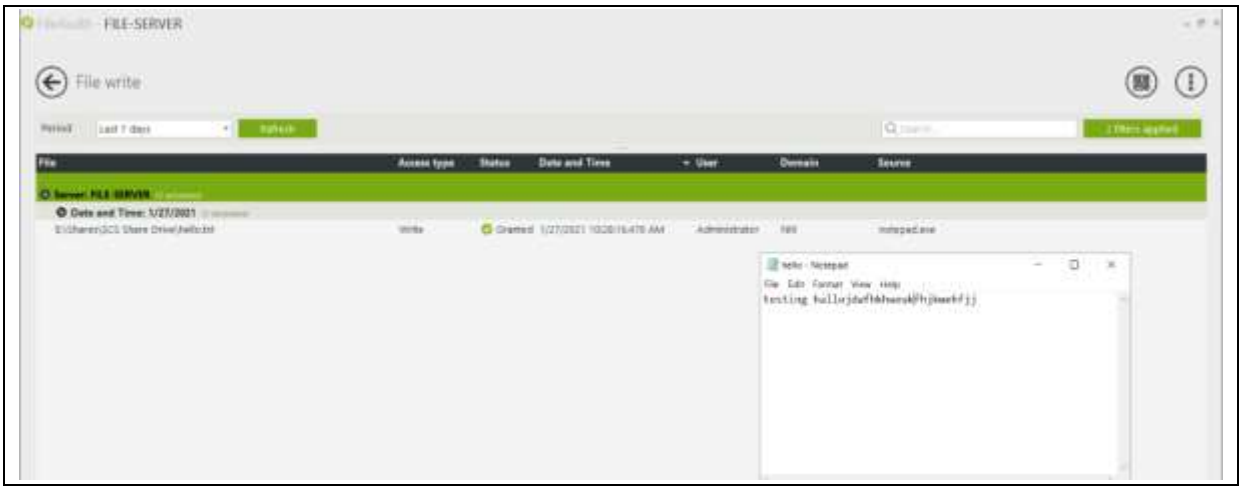
The FileAudit software has the option of narrowing down to specific actions after the alerts have been configured.

Testing and Evaluation of FileAudit

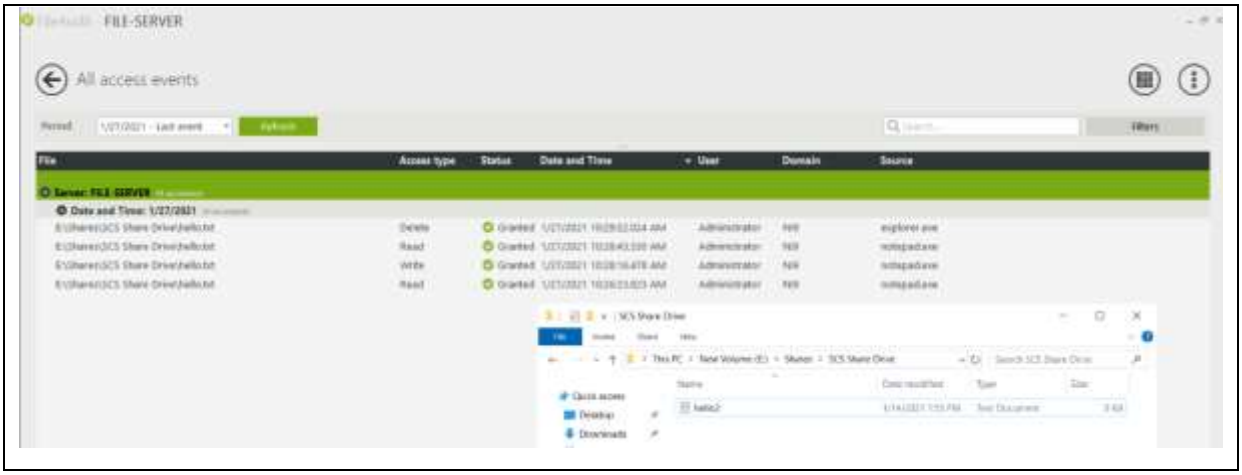
Test 1: File modification and deletion using the Domain Controller (172.16.9.1) and File Server itself.

Documents that existed in the folder before the test: hello.txt and hello2.txt

For this test, I first opened up an existing document and wrote some content to it (using the administrator account on the domain controller) and it got logged in the File Write Section Under reports as an entry to write to the file hello.txt using the notepad.exe application.

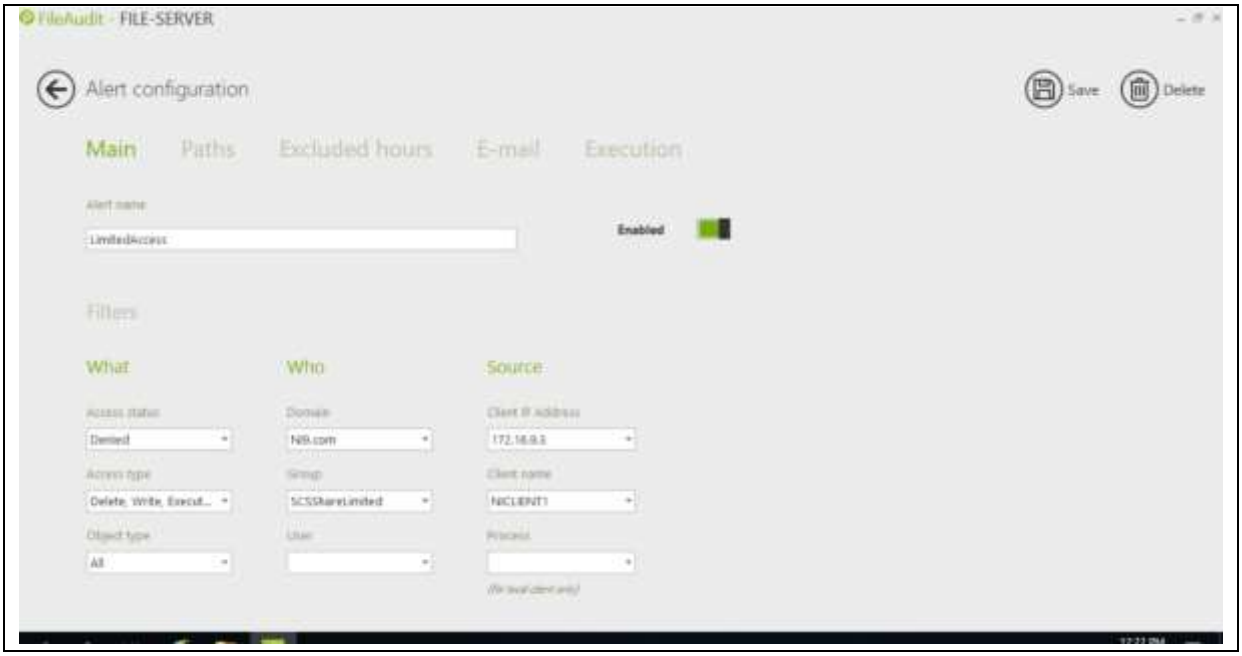


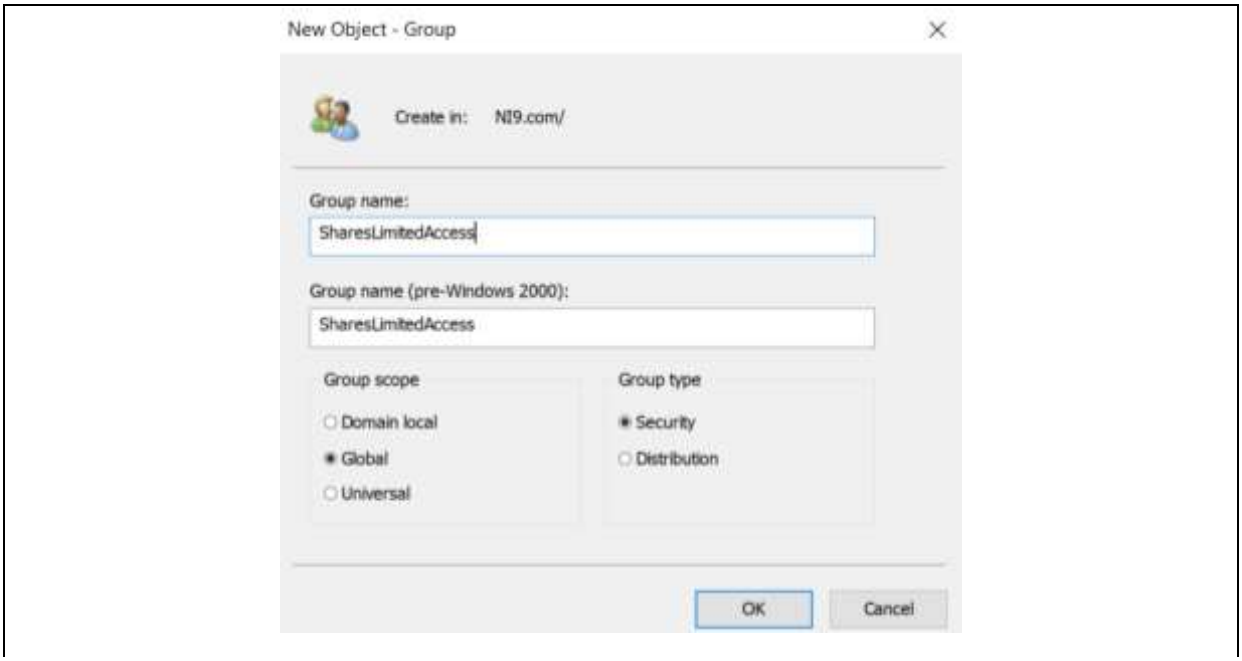
I thereafter opened up the All-access events and thereafter deletion of hello.txt and this also got logged as a deletion using the explorer.exe process (using the File Server this time).

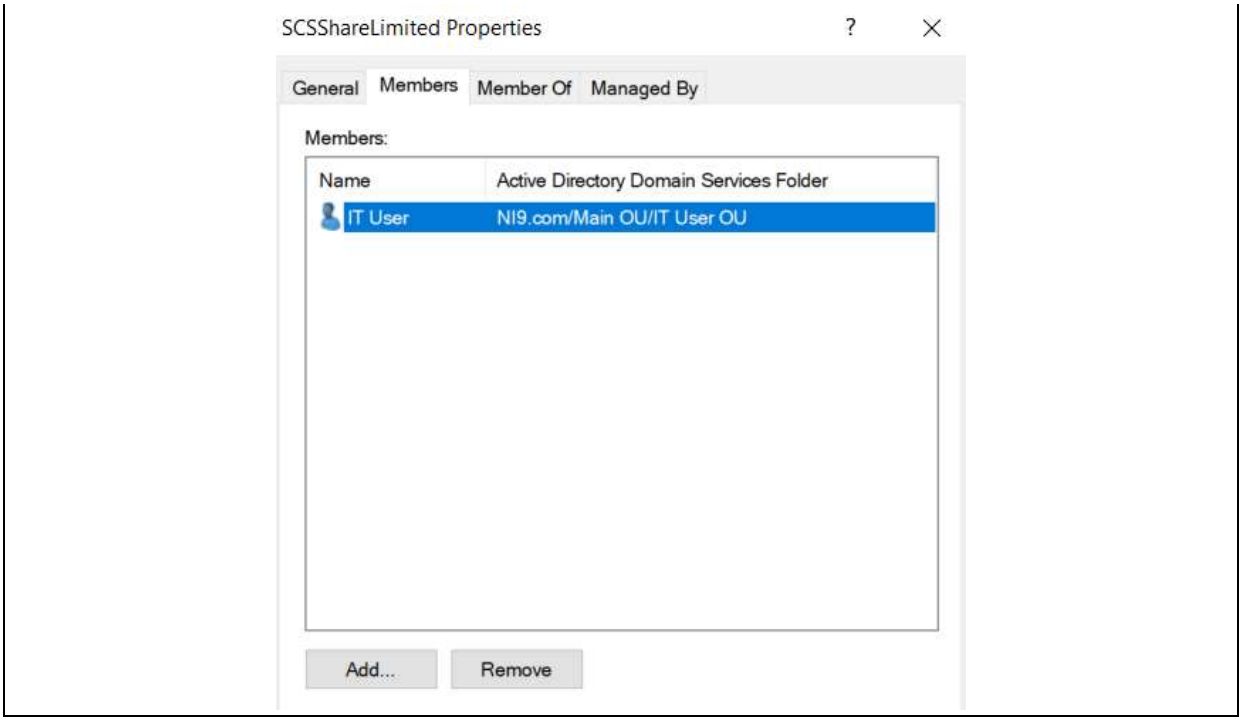


Test 2: Denial of Write Access to the folder for Client

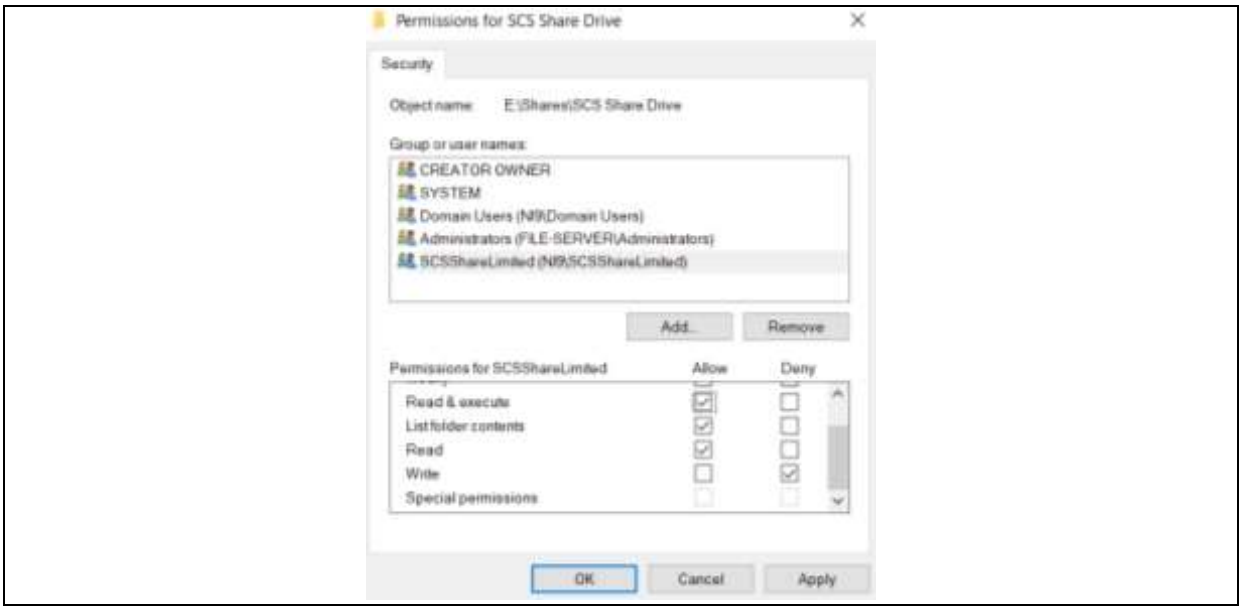
For this test case, I configured an additional policy to log only failures from the Client Machine in the Active Directory Domain as shown below. To do this, I had to create another group using the ADUC tool on the domain controller and add the user “IT User” to the group.



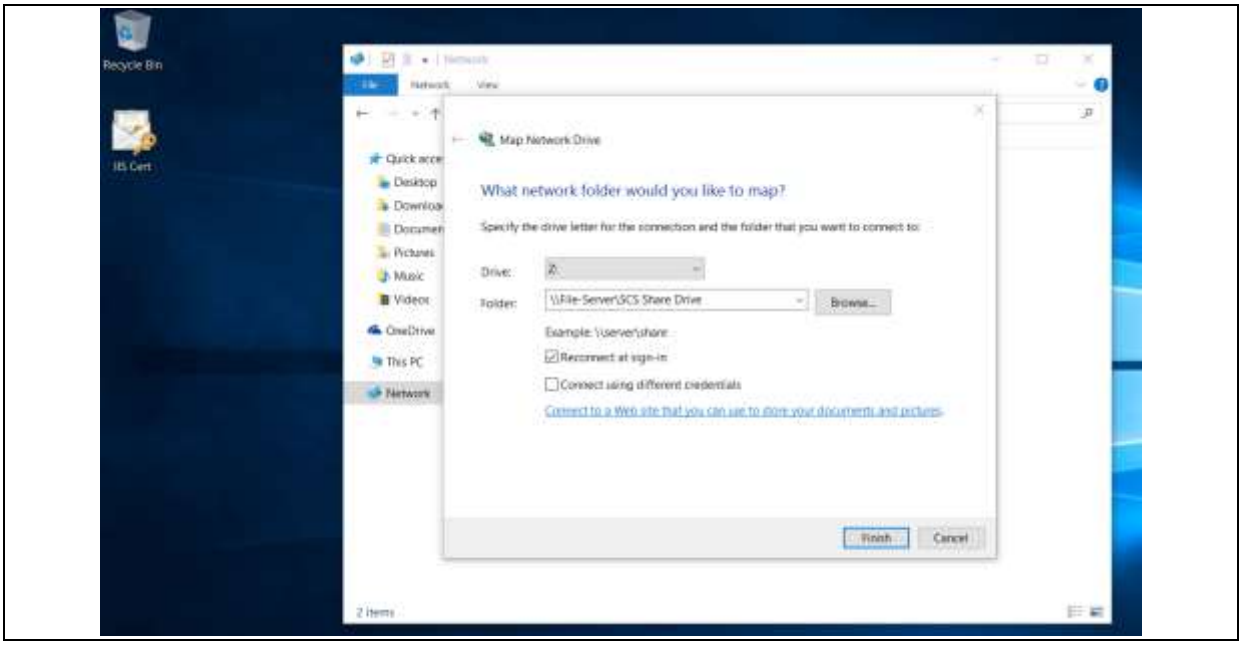




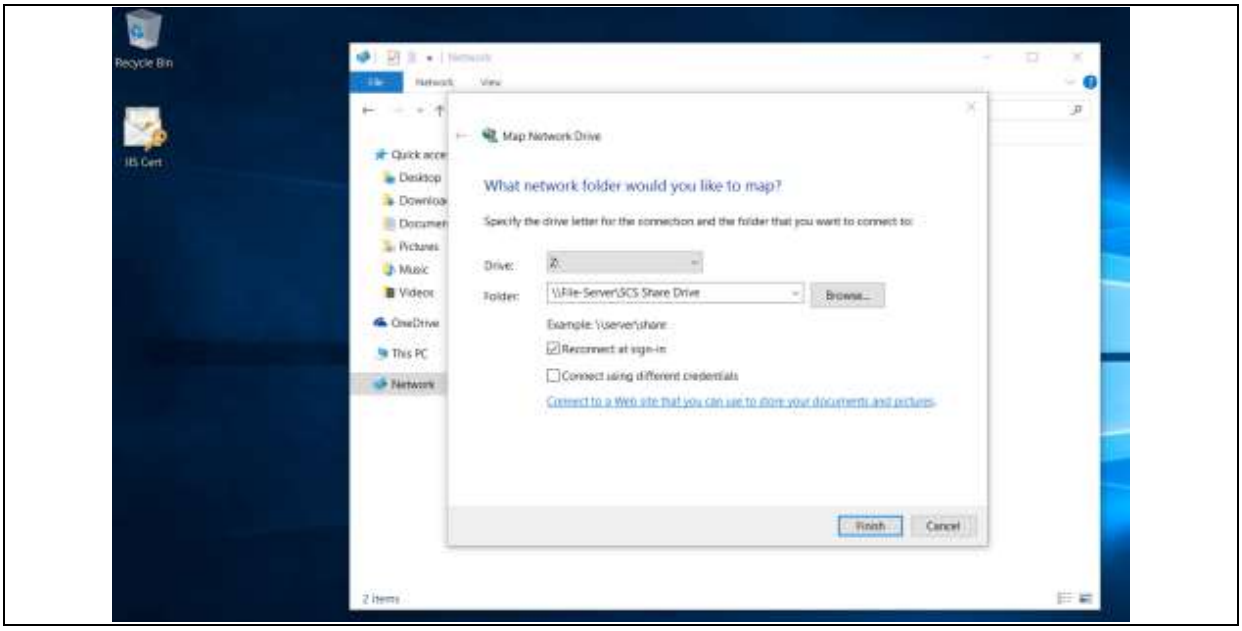
Thereafter, I had to create a new permissions entry for the IT User to deny write permissions on the File Server.



After logging into to client machine using the credentials of the IT User, I attempted to map the network drive where the shared folder was located.



Opening up hello2.txt went fine. However, when I attempted to modify and save the file, an error message appeared detailing that the action was prohibited and confirming that the permissions and domain group was configured correctly.



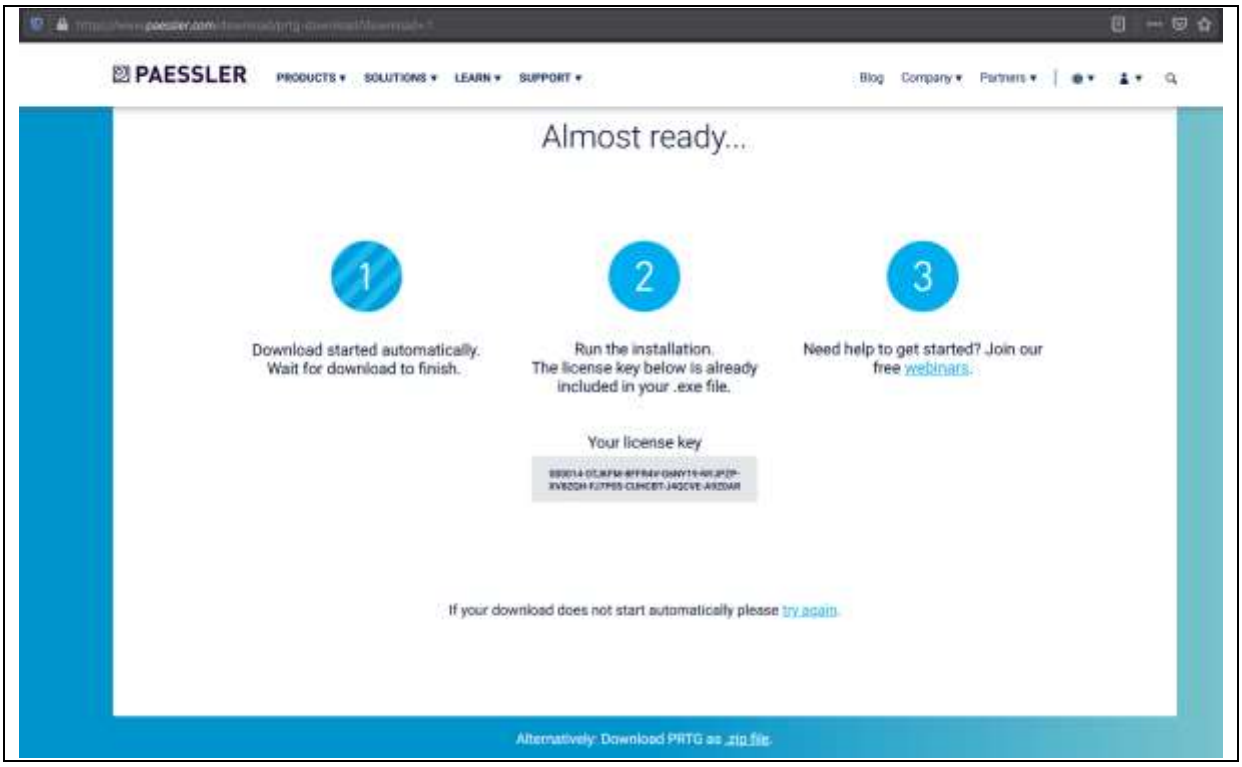
Thereafter, I went back to All access events and found the entry of the deletion being logged, as well as the permissions being changed and the corresponding IP address and Client name.

There is also the option to view a summary of the events that occurred using the Statistics screen, which allows categorizing of information according to topmost access files, Users and Data Sources that are being tracked using the alert tool.

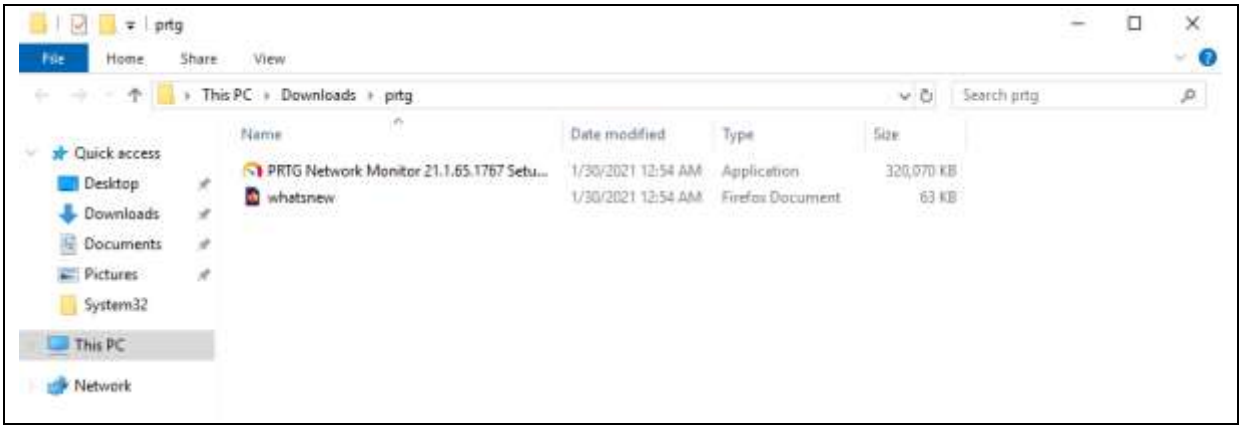
Paessler PRTG Network Monitor

The reason why this software was chosen was because it is a powerful and easy to use solution, suitable for all business sizes. It is capable of monitoring all systems, devices, traffic, and application in the IT infrastructure. Some of the key features are the Maps and Dashboards, which visualized the network using real-time maps with live status information. It also has an alerting function, customizable to the needs and requirements of the client and Integrated Technology such as WMI and Windows Performance Counters to track the performance of the windows system and how much a software or process could affect the performance of the system.

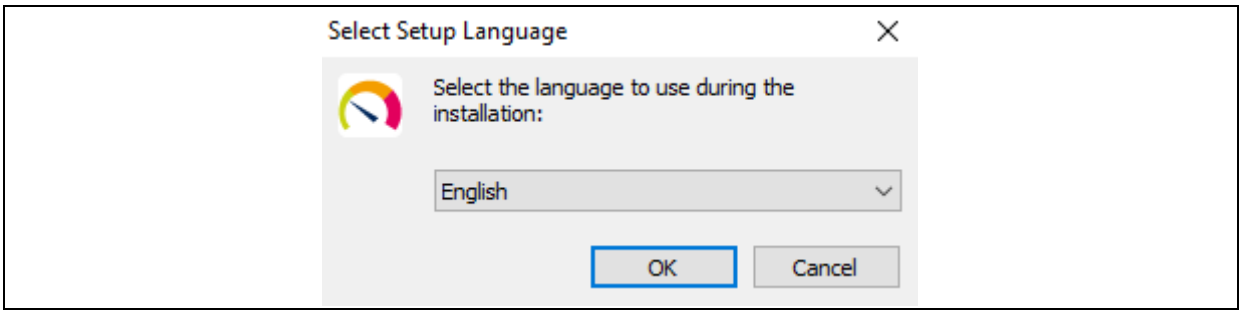
Download Process



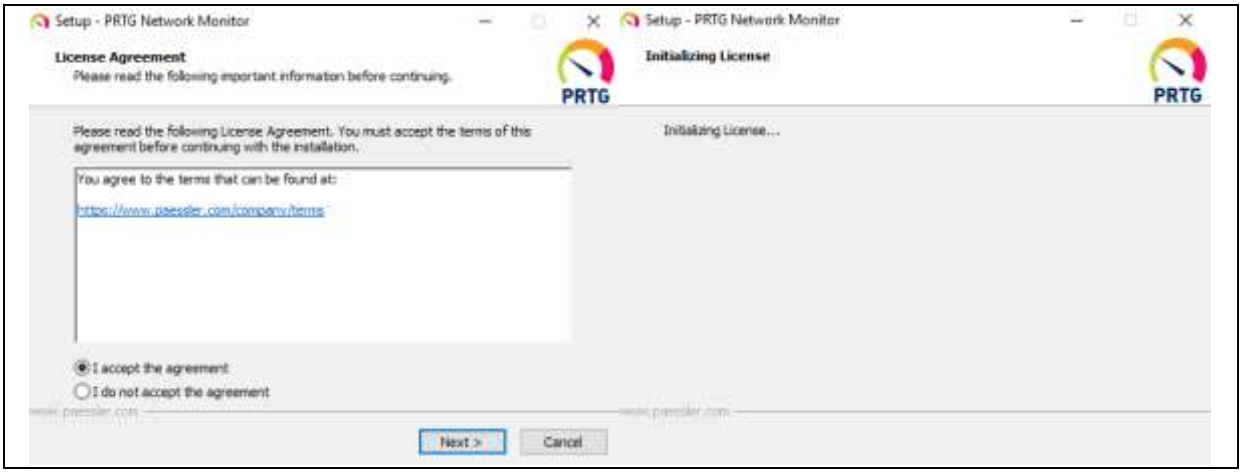
Go to the website and download the zip file as listed below the website.



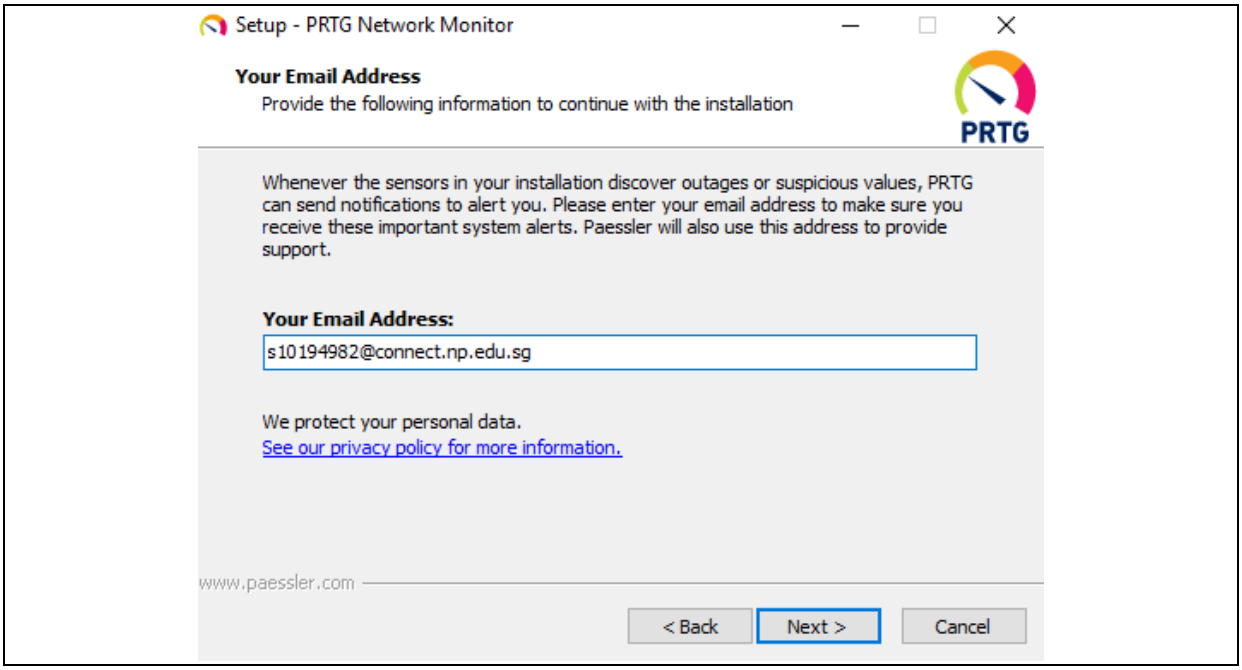
Unzip the downloaded file and click on the application.



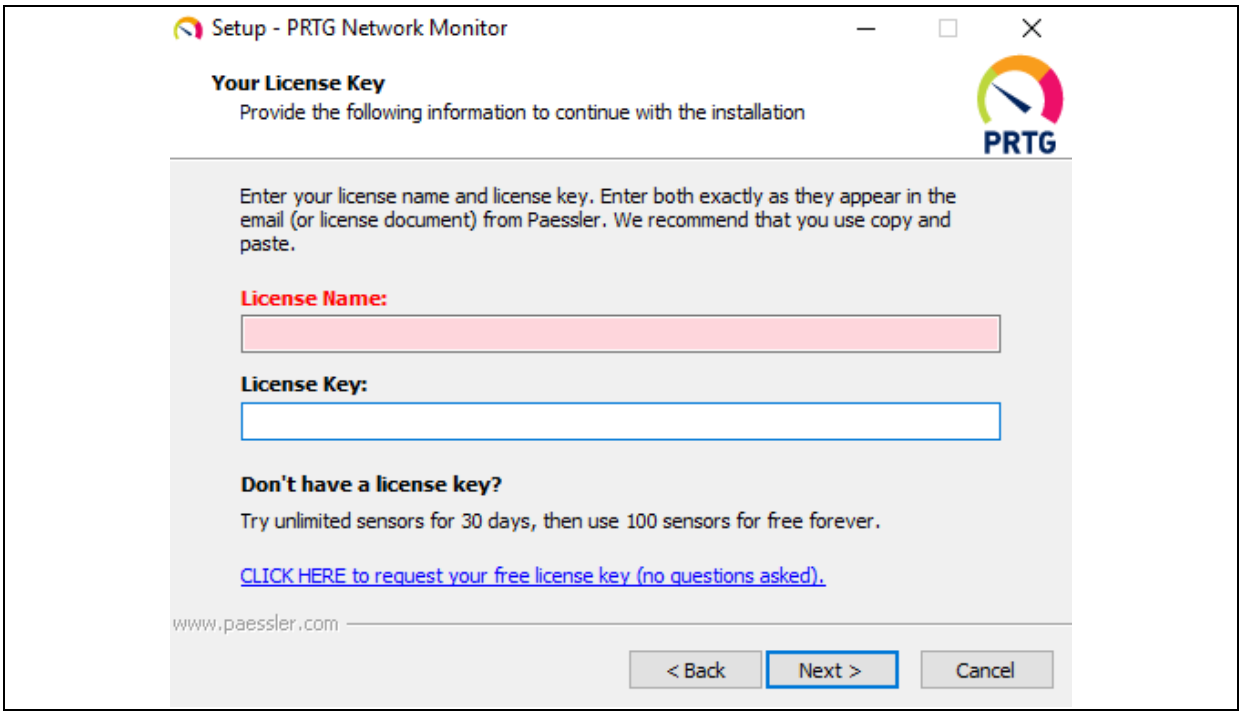
Select the language of choice and click “OK”.



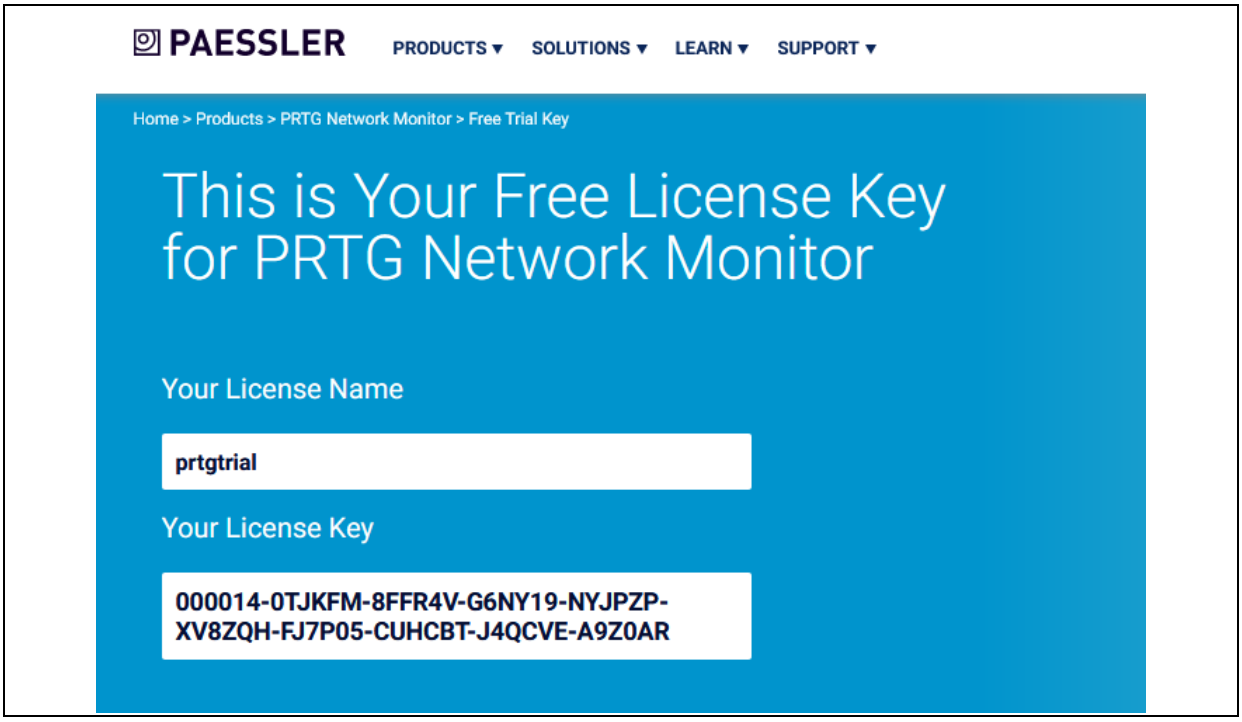
Accept the terms and agreement and wait for the software to initialize.



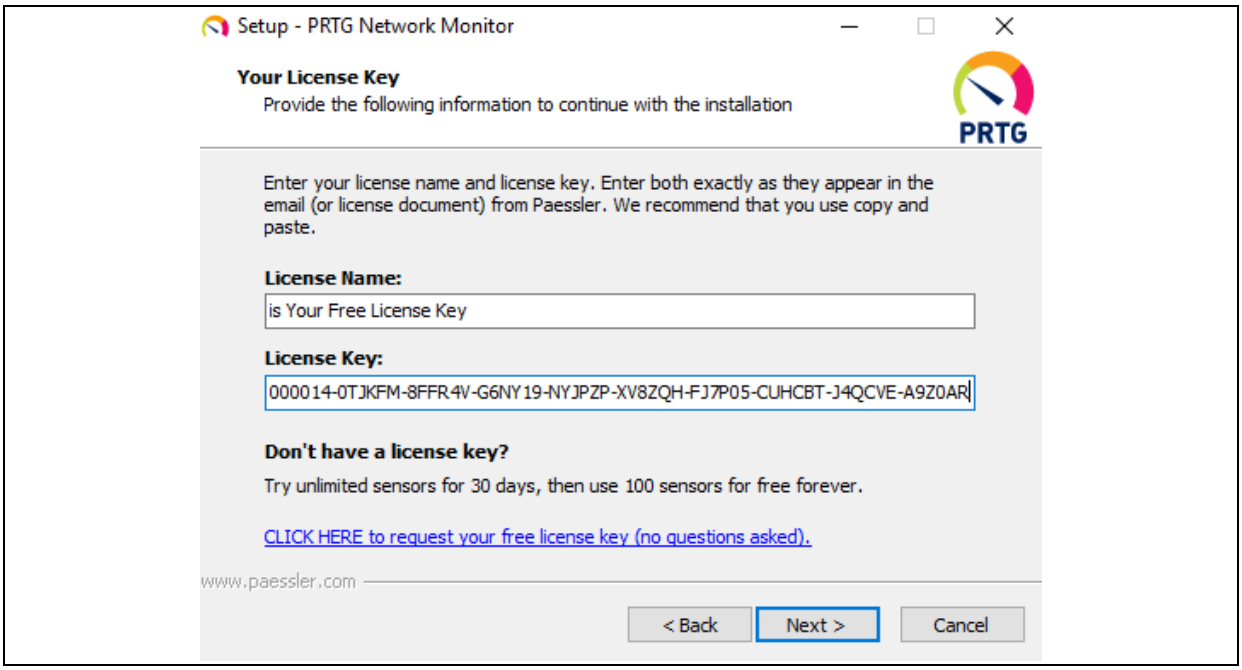
Enter your email address. In this case, I used my school email address as the email for this.



It will then request for the License Name and License Key. Please click the link below to obtain the free License Name and License Key.



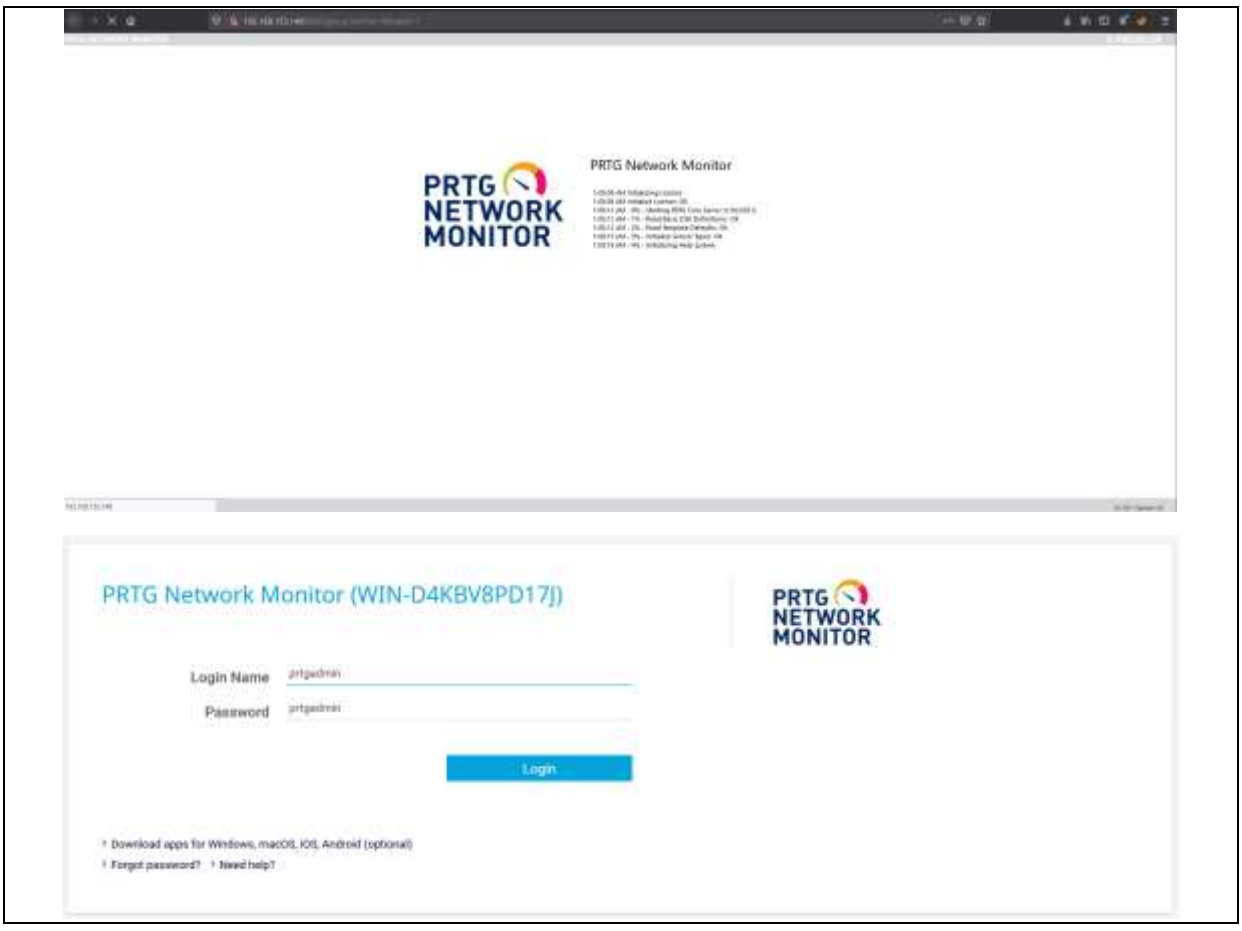
It will lead to this page, copy, and paste the License Name and License Key and paste them in the respective text boxes in the previous image.



This shows the filled text boxes.

Wait for the software to unpack, install, and start the clean-up process.

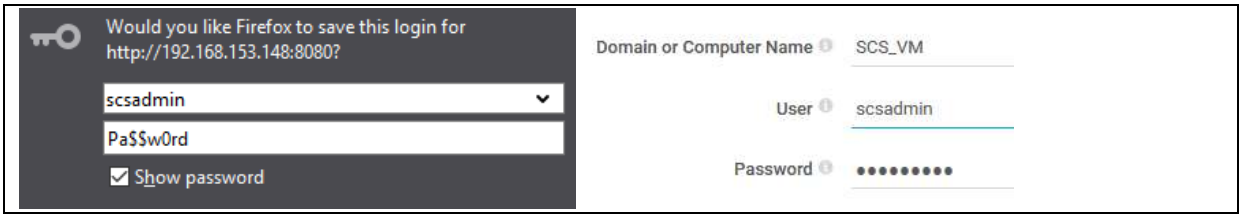
The configurations



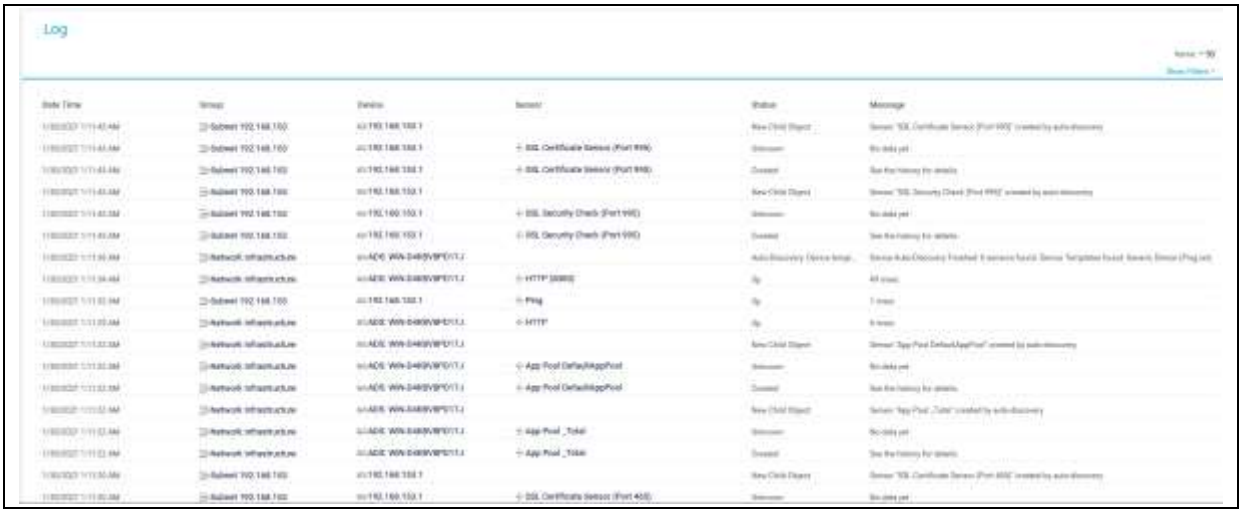
Let the page load and click “Login” without changing the default login name and password on the screen.

The image above the image of all the main menu options available to the users.

It will then guide the user to set the domain / computer name, the user and password for the software.

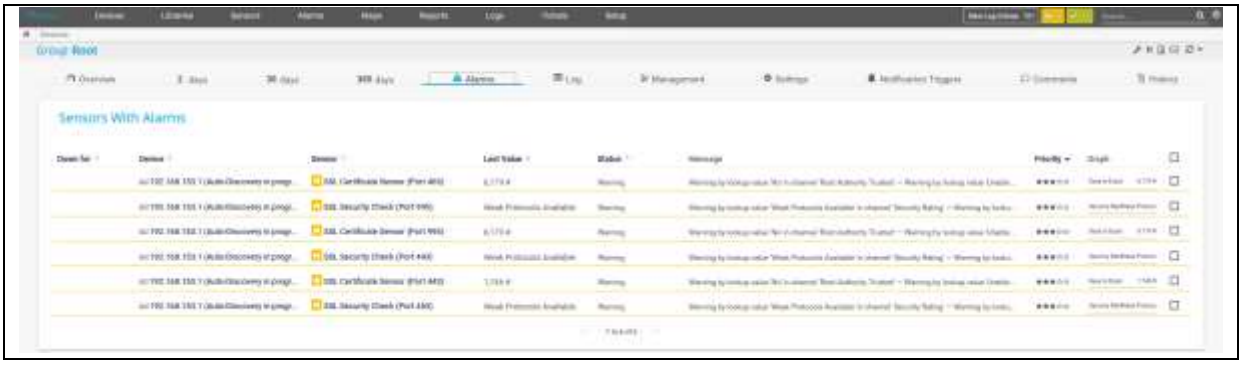


This shows the configuration used for this software.



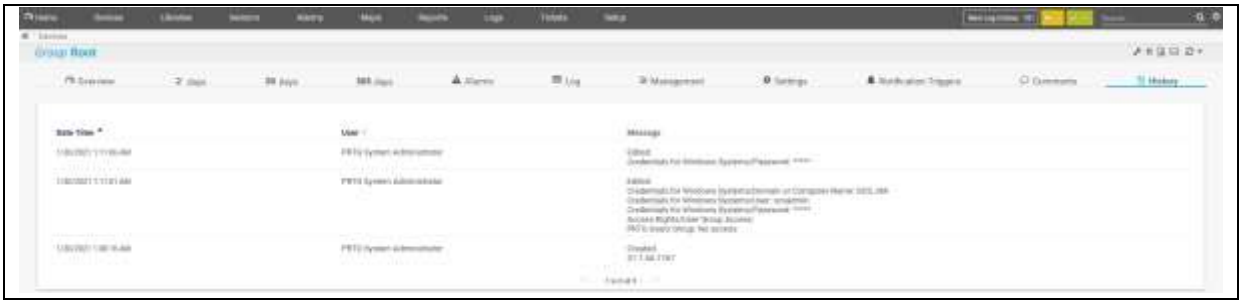
The image above shows the logs the software captures and logs it accordingly to ensure a systematic formal approach.

The image above shows the timeline of the system health by days, indicating whether it is down, up, or how much resource was used by the system.

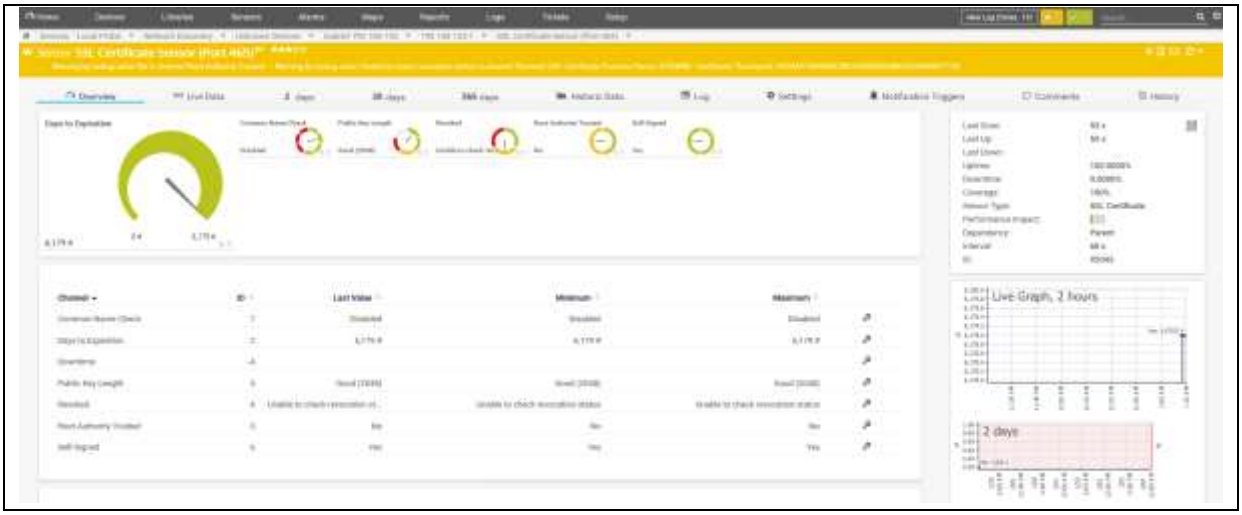


This image shows all the sensors with alarms deployed by the software.

The notification triggers can be used to notify the users by email if there happens to be any failure in the network.



The history tab shows the changes that users have done to the software. This is some sort of internal auditing for the software such that unauthorized changes can be tracked.



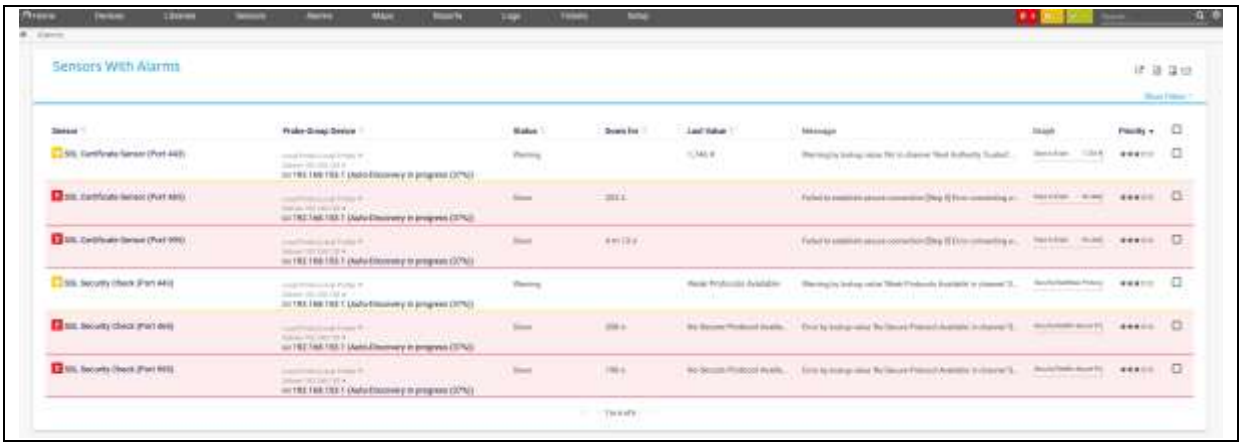
The overview shows the health of the port and provides users with a graphical interface.

Test case for Paessler PRTG Network Monitor

```
C:\Users\25ezr>ping 192.168.153.148 -t -l 65500

Pinging 192.168.153.148 with 65500 bytes of data:
Reply from 192.168.153.148: bytes=65500 time=9ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=2ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=2ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=3ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=2ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=2ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=2ms TTL=128
Reply from 192.168.153.148: bytes=65500 time=1ms TTL=128
```

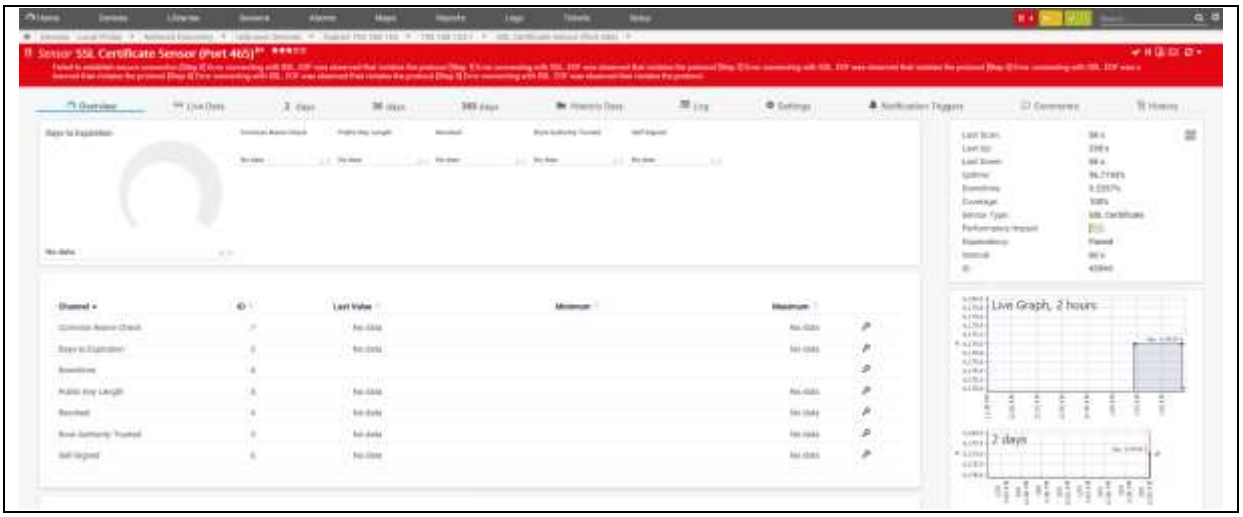
Firstly, I used the Ping of Death, meaning constant ping to the Windows Server with a packet size of 65500 bytes using the commands *ping 192.168.153.148 -t -l 65500*.



A few moments passed and the network monitor started to get errors and high alerts, indicating that something has happened. Turns out, the Ping of Death has caused some of the ports to close and are down as of conducting the test case. The reason why this could be possible is due to the amount of traffic being passed was too much, hence crashing.

There was a total of 2 ports that crashed, and 2 different types of alerts was given. The ports involved were Port 995 and Port 465. The errors were “Failed to establish secure connection [Step 0]” and “Error by lookup value “No Secure Protocol Available” in channel “Security Rating”.

Sensor SSL Certificate Sensor error

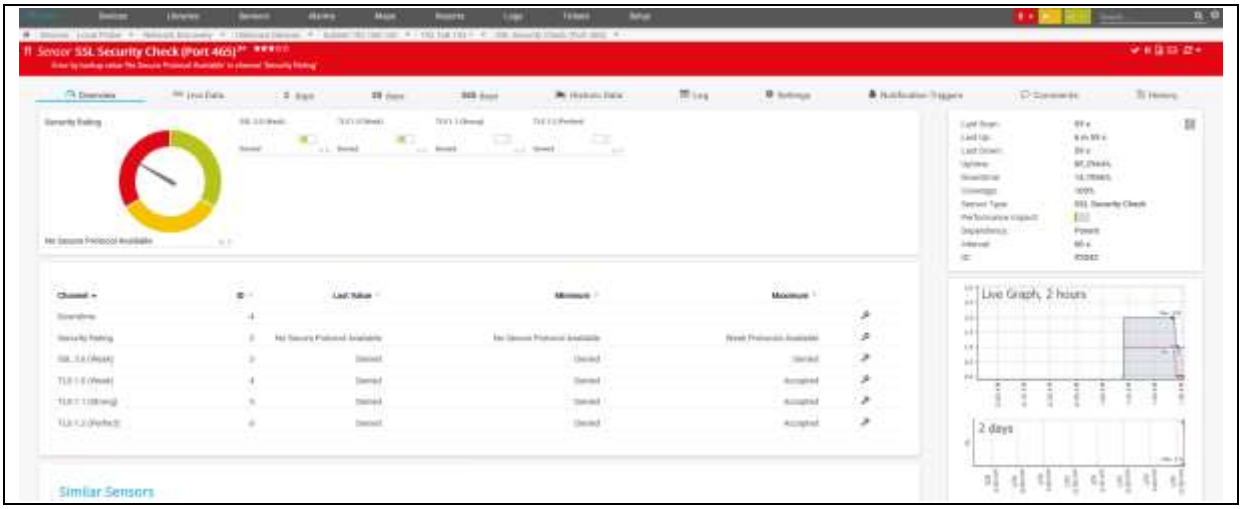


The image below and the next few will indicate the Sensor SSL Certificate Sensor error. This is similar on both port 465 and 995. On the overall look, it does not show any details and the graphs at the right-hand side also indicated that the port is down and is not functional.

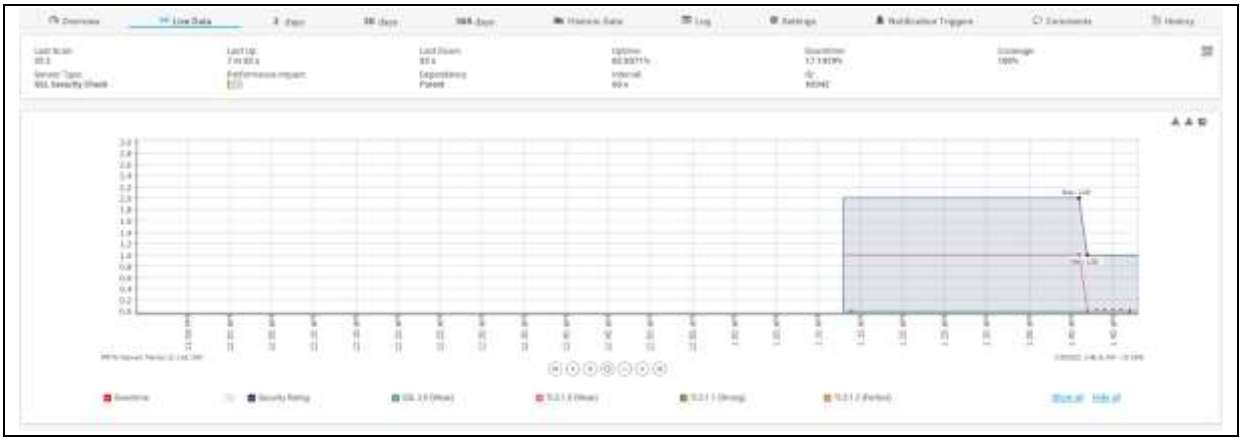
A closer inspection of the timeline shows that the port was working as per usual until just after 1.40am, which was the time where I started the Ping of Death. This shows that the network was able to record, monitor and analyse the network of the server accurately and with a lot of details.

The log tab also shows the exact date and time that the port went down and the message alongside it, which provides the error and reason to justify the port status.

Sensor SSL Security Check error



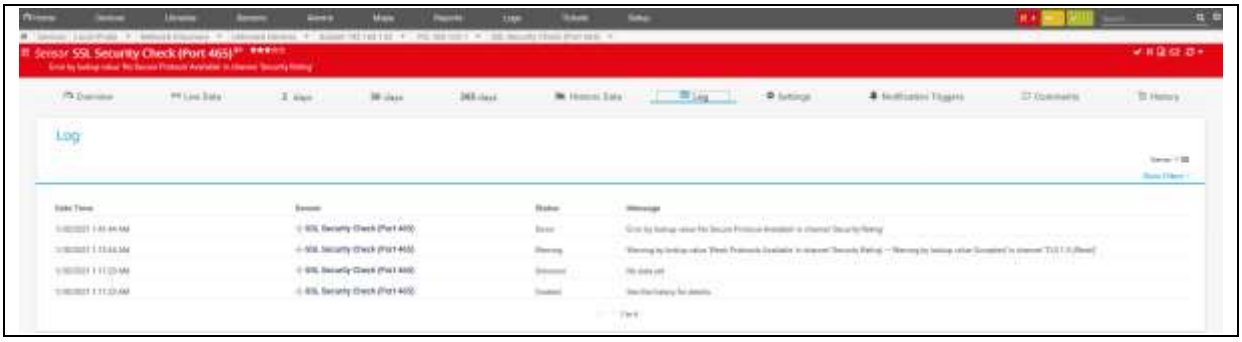
The overview of the Sensor SSL Security Check error still shows data to the user instead of having no value / data for the user to analyse at all. The above described the accepted protocols through the port. Since most are denied, the only ones accepted are TLS 1.0 (Weak), TLS 1.1 (Strong) and TLS 1.2 (Perfect). It represents a warning status, an unknown status, and an unknown status respectively to the protocols mentioned above.



The graph above shows the timeline of the port and the amount of time it was open. As shown in the image above, the port did experience downtime, however, the security rating of the port dropped by half, from 2.00 to 1.00. Security ratings are a measurement of an organization's security posture, providing a quantitative measure of credit risk. This aims to provide a quantitative measure of cyber risk. The lower the security rating, the lower the measurement of an organization's security posture.

Date Time *	Security Rating (Only Strong Protocols Available)	SSL 3.0 (Weak) (Denied)	TLS 1.0 (Weak) (Denied)	TLS 1.1 (Strong) (Accepted)	TLS 1.2 (Perfect) (Accepted)	Downtime	Coverage
Averages (of 37 values)						19 %	100 %
1/30/2021 1:48:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:47:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:46:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:45:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:44:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:43:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:42:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	100 %	100 %
1/30/2021 1:41:44 AM	No Secure Protocol Available	Denied	Denied	Denied	Denied	0 %	100 %
1/30/2021 1:40:44 AM	Weak Protocols Available	Denied	Accepted	Accepted	Accepted	0 %	100 %
1/30/2021 1:39:44 AM	Weak Protocols Available	Denied	Accepted	Accepted	Accepted	0 %	100 %

As shown, the protocols have all been denied since the Ping of Death was started, as it overloaded the Windows Server.



The log can be used to check the date and time of the incident and can be used to tell if any changes has occurred to the port by looking at the changes of the state of the port.

Contributions

Name	Feature
Ryan	1. Anti-malware (Sophos) Installation 2. Anti-malware Configuration and Evaluation 3. FileAudit Installation 4. FileAudit Configuration and Evaluation
Ezra	1. Setting Up File Server 2. Testing File Server 3. Configuring Group Object Policy 4. Testing Group Object Policy 5. Nessus Essential Vulnerability Scanning Tool 6. Testing Nessus Vulnerability Scanning Tool Configuration and Evaluation 7. Windows Firewall with Advanced Security 8. Tinywall Firewall 9. Testing Firewall Configuration and Evaluation 10. Paessler PRTG Network Monitor 11. Testing Paessler PRTG Network Monitor 12. Formatting
Matthias	Data Loss Prevention: - Sourcing for workable DLP - Set-up and installation of OpenDLP - OpenDLP Testing - OpenDLP Evaluation
Hannah	Snort: 1. Installing Snort 2. Configuring Snort 3. Testing and Evaluation of Snort