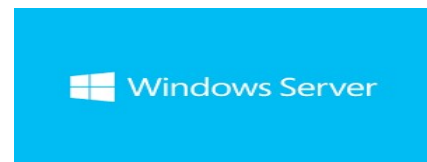




# SOC (Cybersecurity Analyst Program)

## Build Book



**Student: Keerthana Tirumalaraju**

**Instructor: Talha Iqbal**

**Nov 2022**

## Contents

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <b>1. Security Overview .....</b>                                  | <b>4</b>  |
| <b>2. About the Program.....</b>                                   | <b>6</b>  |
| 2.1 Lab Design.....                                                | 6         |
| 2.2 Hardware requirements for host.....                            | 6         |
| <b>3.Virtualization .....</b>                                      | <b>7</b>  |
| 3.1 Oracle's VM Virtual Box .....                                  | 9         |
| 3.2 Installing Oracle VM VirtualBox.....                           | 10        |
| <b>4. Installing Windows 2016 Server on VirtualBox.....</b>        | <b>13</b> |
| 4.1 Download ISO Windows 2016 .....                                | 13        |
| 4.2 Download ISO Windows 10 Pro .....                              | 14        |
| 4.3 Windows 2016 Server Installation .....                         | 21        |
| <b>5. Installing Windows Client (Windows 10 Pro) .....</b>         | <b>29</b> |
| 5.1 Virtual machine configuration .....                            | 29        |
| 5.2 Windows 10 Pro Installation.....                               | 31        |
| <b>6. Active Directory (AD).....</b>                               | <b>37</b> |
| 6.1 Why do we need AD? .....                                       | 37        |
| 6.2 Active Directory setup.....                                    | 39        |
| 6.3 Creating a new user in Active Directory .....                  | 42        |
| <b>7. Event Viewer .....</b>                                       | <b>47</b> |
| <b>8. Security Information &amp; Event Management (SIEM) .....</b> | <b>53</b> |
| 8.1 SIM vs SEM vs SIEM.....                                        | 53        |
| 8.2 Setting up Sumo Logic .....                                    | 55        |
| 8.3 Downloading and Installing Sumo Logic Collector .....          | 57        |
| 8.4 Collect Windows Logs.....                                      | 59        |
| 8.5 Searching Event Logs .....                                     | 61        |
| 8.6 Parse the Event Code .....                                     | 62        |
| 8.7 Creating Alert for Windows Event .....                         | 63        |
| <b>9. Firewalls.....</b>                                           | <b>65</b> |
| 9.1 What is firewall?.....                                         | 65        |
| Advantages of Firewall.....                                        | 65        |
| Disadvantages of Firewall .....                                    | 65        |
| 9.2 Installing pfSense on VirtualBox .....                         | 66        |
| 9.3 Installing Snort Package .....                                 | 81        |
| <b>10. Endpoint Security .....</b>                                 | <b>85</b> |
| Why Is Endpoint Security Important? .....                          | 86        |
| 10.1 SOPHOS installation .....                                     | 87        |
| <b>11. Incident Response .....</b>                                 | <b>95</b> |

|                                                                                    |            |
|------------------------------------------------------------------------------------|------------|
| <b>12. Importance of Vulnerability scan .....</b>                                  | <b>100</b> |
| <b>Vulnerability Examples .....</b>                                                | <b>100</b> |
| 1. Hardware.....                                                                   | 100        |
| 2. Software .....                                                                  | 100        |
| 3. Network.....                                                                    | 101        |
| 4. Personnel .....                                                                 | 101        |
| 5. Physical site.....                                                              | 101        |
| 6. Organizational.....                                                             | 101        |
| <b>12.1 NESSUS Installation .....</b>                                              | <b>101</b> |
| <b>12.2 Deploying a dummy web server (BadStore).....</b>                           | <b>108</b> |
| <b>13 CIS Critical Security Controls .....</b>                                     | <b>115</b> |
| <b>CIS Control 1 - Inventory and Control of Enterprise Assets .....</b>            | <b>115</b> |
| <b>CIS Control 2 - Inventory and Control of Software Assets .....</b>              | <b>115</b> |
| <b>CIS Control 3 - Data Protection .....</b>                                       | <b>115</b> |
| <b>CIS Control 4 - Secure Configuration of Enterprise Assets and Software.....</b> | <b>115</b> |
| <b>CIS Control 5 - Account Management .....</b>                                    | <b>116</b> |
| <b>CIS Control 6 - Access Control Management.....</b>                              | <b>116</b> |
| <b>CIS Control 7 - Continuous Vulnerability Management .....</b>                   | <b>116</b> |
| <b>CIS Control 8 - Audit Log Management.....</b>                                   | <b>116</b> |
| <b>CIS Control 9 - Email and Web Browser Protections .....</b>                     | <b>116</b> |
| <b>CIS Control 10 - Malware Defenses .....</b>                                     | <b>116</b> |
| <b>CIS Control 11 - Data Recovery.....</b>                                         | <b>116</b> |
| <b>CIS Control 12 - Network Infrastructure Management .....</b>                    | <b>116</b> |
| <b>CIS Control 13 - Network Monitoring and Defense .....</b>                       | <b>117</b> |
| <b>CIS Control 14 - Security Awareness and Skills Training.....</b>                | <b>117</b> |
| <b>CIS Control 15 - Service Provider Management.....</b>                           | <b>117</b> |
| <b>CIS Control 16 - Application Software Security.....</b>                         | <b>117</b> |
| <b>CIS Control 17 - Incident Response Management .....</b>                         | <b>117</b> |
| <b>CIS Control 18 - Penetration Testing.....</b>                                   | <b>117</b> |
| <b>14. Cyber Security Questions &amp; Answers .....</b>                            | <b>118</b> |

## 1. Security Overview

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ cyber security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

Security system complexity, created by disparate technologies and a lack of in-house expertise, can amplify these costs. But organizations with a comprehensive cybersecurity strategy, governed by best practices and automated using advanced analytics, artificial intelligence (AI) and machine learning, can fight cyberthreats more effectively and reduce the lifecycle and impact of breaches when they occur.



Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

**Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

**Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

**Information security** protects the integrity and privacy of data, both in storage and in transit.

**Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

**Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

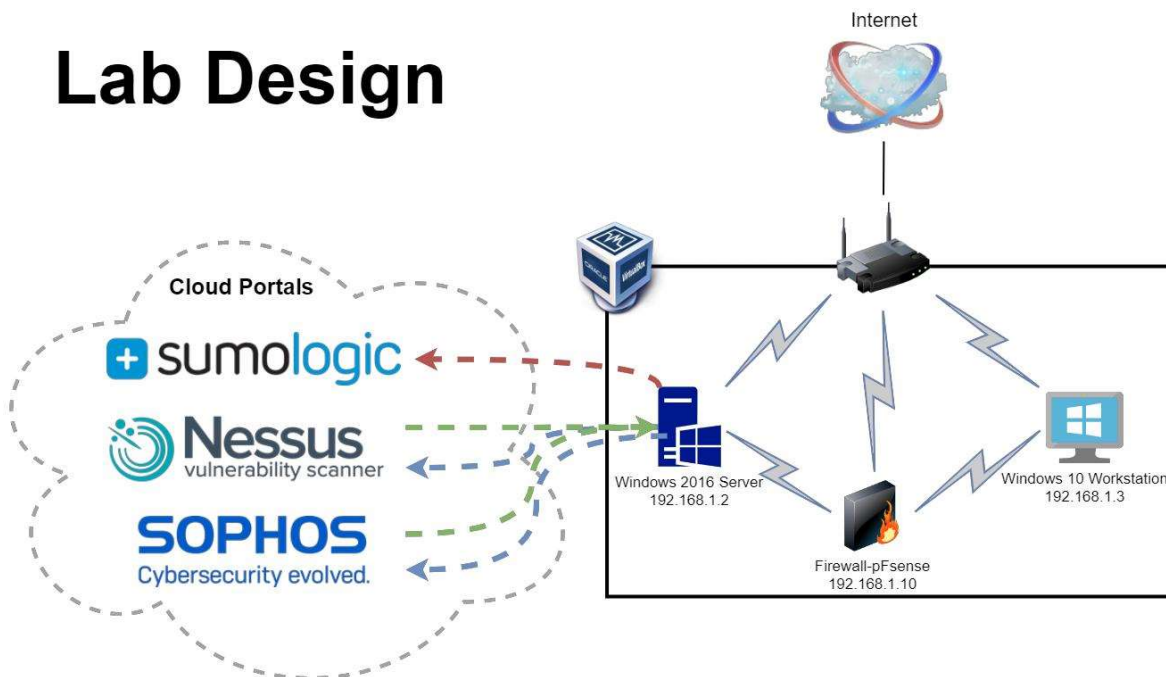
**End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

## 2. About the Program

Cybersecurity is one of the fastest growing segments in IT. Through practical training, skill development and employment support, this program will prepare you for a career as a SOC Cybersecurity Analyst in this high demand field. Professional training by Cyberwall. SOC Cybersecurity Analyst Certificate (upon successful completion).

### 2.1 Lab Design

# Lab Design



### 2.2 Hardware requirements for host

Laptop with Windows 10 Pro (allow virtualization in Bios)

RAM 8 G

Disk – at least 100GB free space

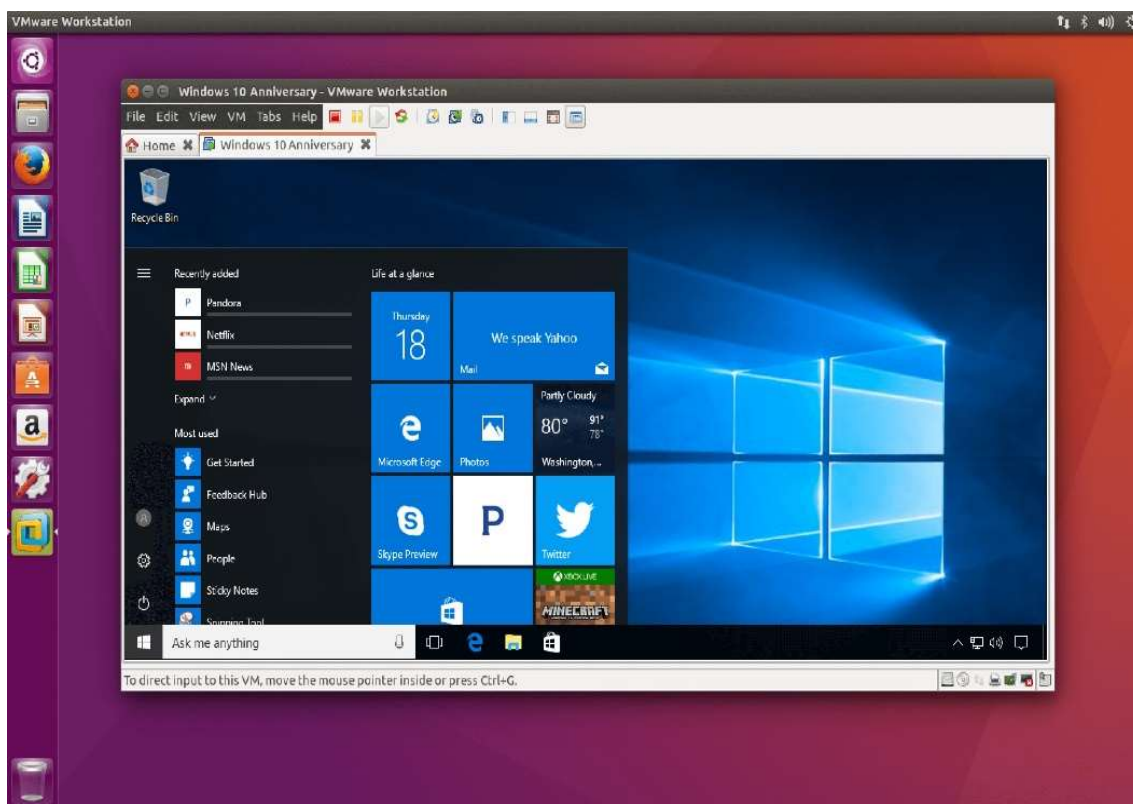
Web Camera

### 3. Virtualization

#### What is Virtualization?

Virtualization is where we create a virtual computer or 'virtual machine' out of software that behaves like a separate computer. All the hardware components of that virtual machine are actual software. The software that is the virtual machine uses the hardware resources of the computer it is running on. This is achieved using a hypervisor, which creates a thin layer that breaks the traditional 1:1 relationship between an operating system and the hardware. There are various types of hypervisors we will cover in more depth later.

Put simply, we can build a virtual computer out of software, and use that to run a different operating system on top of our main operating system. Imagine running Windows at the same time as running Mac OS X for example. Or even running Windows while running Linux. All this and more are possible with virtualization.



Here we have a Linux system running VMware (a popular virtualization software); the operating system inside the virtual machine is Windows 10.

#### Host Operating System

We call the operating system that runs the virtualization software the host operating system. It is the master, the operating system that loads when you first turn on your

physical computer.

## Guest Operating System

We call the operating system that runs inside the virtual machine the 'guest operating system'. The Guest operating system is separate from the host operating system cannot directly access the resources on the host. For example, if you were running Windows as the host operating system and Linux as the guest, the Linux guest is not able to access files on your Windows desktop directly. This separation is a key use case for virtualization. If you are analysing a computer virus, you will want to be doing it in a virtual machine to prevent it from spreading to your host operating system and potentially escaping out onto the internet from there.

## The Hypervisor

Before we talk about the different types of virtualizations, we have to talk about the hypervisor. The hypervisor is the layer of code that allows multiple operating systems to share the same hardware resources. Essentially, it's the bit of code that directs traffic, deciding which bits of memory are used for which virtual machines, where the hard disk for that virtual machine is kept in storage, and so on.

## Type 2 Hypervisor

The first type of virtualization we'll talk about is the type 2 hypervisor. This type of virtualization is where the virtualization is done by a software program that runs on an operating system. This is the kind of virtualization we'll be using throughout this course. Several software programs can be used to perform this; the most popular ones are VMware Workstation and VirtualBox.

## Type 1 Hypervisor

The second type of virtualization is the type 1 hypervisor. This type of virtualization is where the virtualization occurs at the firmware level. This is still software, but there is no host operating system. The virtualization software in effect is the host operating system. This is commonly used in server environments such as data centers, particularly ones that form 'the cloud'. It is a more efficient setup than a type 2 hypervisor, but it isn't convenient for people to use on their personal computers. Some examples are VMware vSphere and Proxy

## Uses of Virtualization

Virtualization sounds pretty niche, so why is it so important? Well, you might be surprised to learn that a large proportion of the internet runs on virtualised servers. Ever heard of the cloud? Well, most of that is run off of Type 1 hypervisors. The fact of the matter is virtualization offers huge efficiency improvements for large-scale applications.

Imagine if you have a website which is usually quiet, but often it will suddenly get a huge deluge of users accessing it all at once. You need a server that can handle the maximum number of users, but that will leave your server doing nothing most of the time when it's quiet. With virtualization, you can run the site off one small virtual machine, and have new virtual machines come online during peak times to load balance your traffic across the multiple servers. When it becomes quiet again, you can delete some of the virtual machines and go back to having only one serving the website. Cloud hosting providers such as Amazon AWS offer this functionality using virtualization.

### 3.1 Oracle's VM Virtual Box

**Oracle VM VirtualBox** (formerly **Sun VirtualBox**, **Sun xVM VirtualBox** and **Innotek VirtualBox**) is a type-2 hypervisor for x86 virtualization developed by Oracle Corporation.

VirtualBox was originally created by Innotek GmbH, which was acquired by Sun Microsystems in 2008, which was in turn acquired by Oracle in 2010.

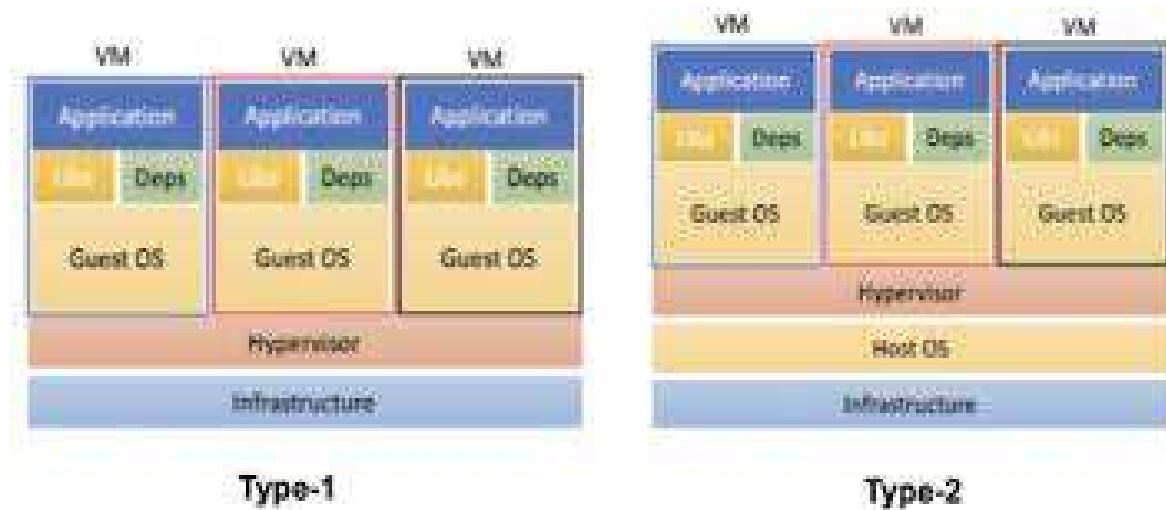
VirtualBox may be installed on Microsoft Windows, macOS, Linux, Solaris and OpenSolaris. there are also ports to FreeBSD and Genode. It supports the creation and management of guest virtual machines running Windows, Linux, BSD, OS/2, Solaris, Haiku, and OSx86, as well as limited virtualization of macOS guests on Apple hardware.

#### Version 6.1

- Support for importing virtual machines from Oracle Cloud
- Added nested virtualization support for Intel CPUs (it was already available for AMD CPUs) starting with Intel Core i5 Broadwell
- Experimental support for file transfers via drag-n-drop only for Windows host and guests (disabled by default, must be enabled using VBoxManage)
- Support for virtio-scsi for hard disks and optical drives, including boot support
- Support for hosts with up to 1024 CPUs
- DXVA (hardware accelerated video decoding) support for Windows guests
- NVRAM support for EFI which improves compatibility with many guest OSes
- Software keyboard for entering any keys to a guest
- Guest CPU use monitoring
- Dropped support for software CPU virtualization: a CPU with hardware virtualization support is now required
- Dropped support for PCI passthrough for Linux hosts
- Soft (virtual) keyboard

## Hypervisor

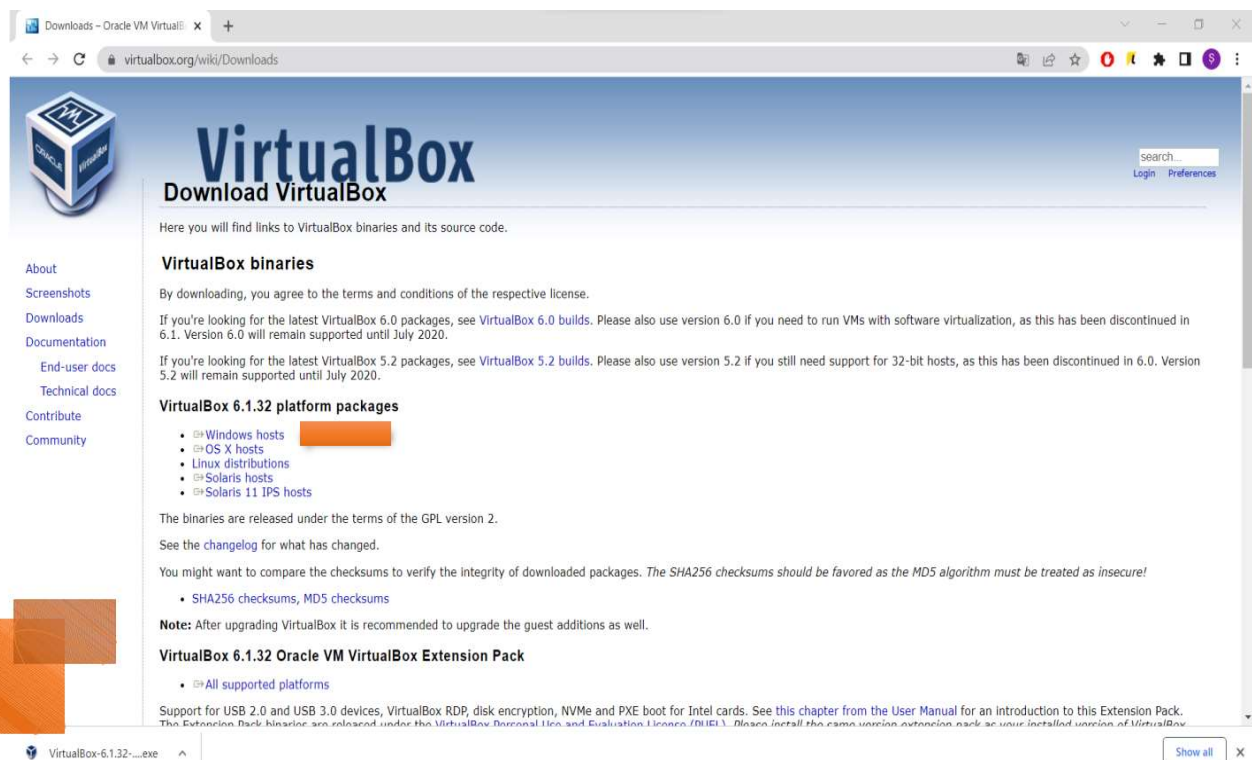
A hypervisor is a computer software, firmware or hardware that creates and runs Virtual Machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.



## 3.2 Installing Oracle VM VirtualBox

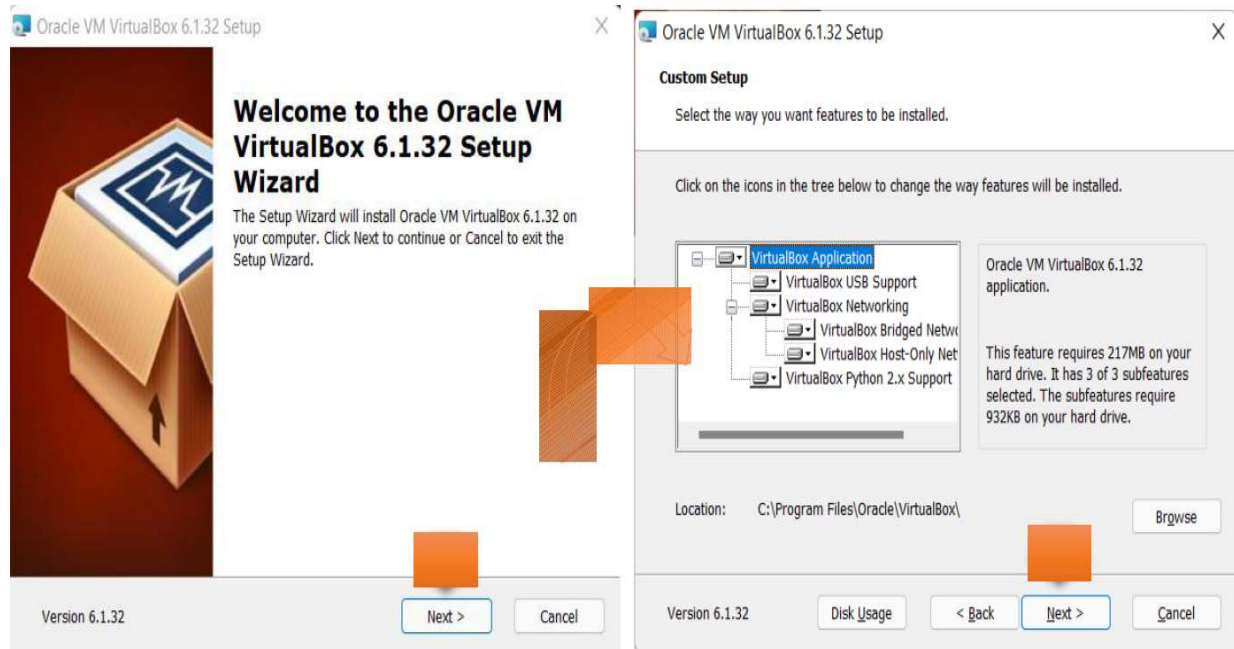
To download go to <https://www.virtualbox.org/wiki/Downloads>

Select "Windows hosts". It'll give you the option to Run or Save. Click Run.



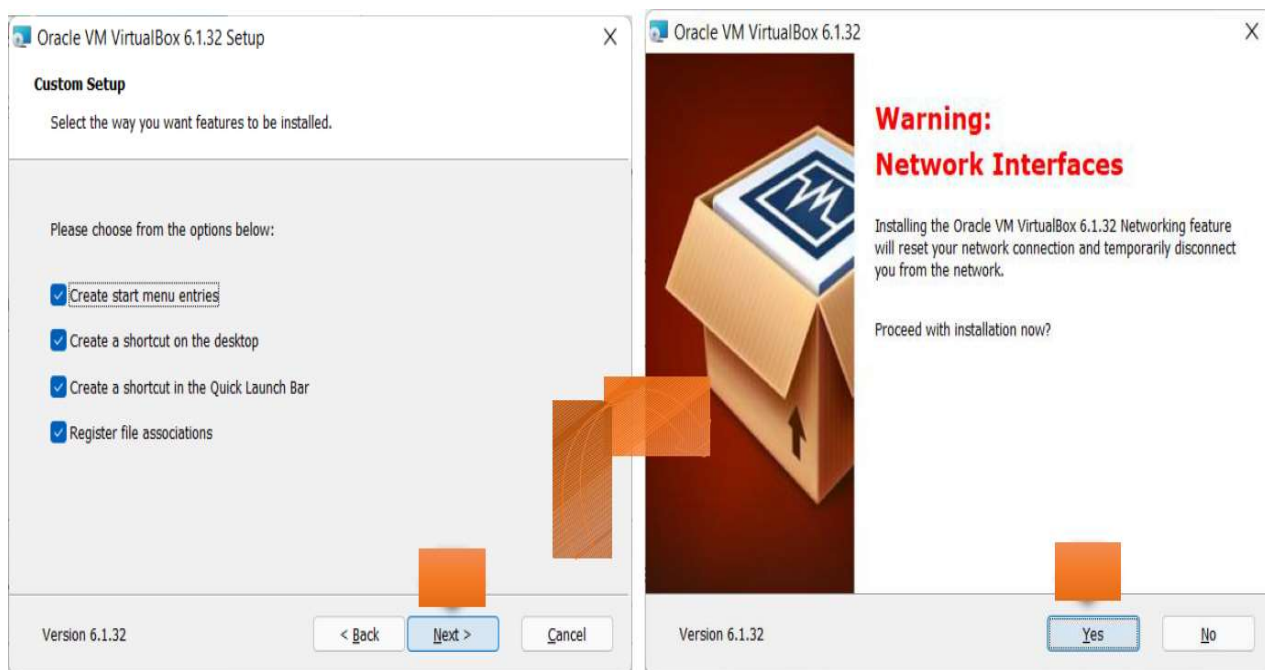
The installation window will appear. Click “Next”

Custom setup screen will come up. Click “Next”



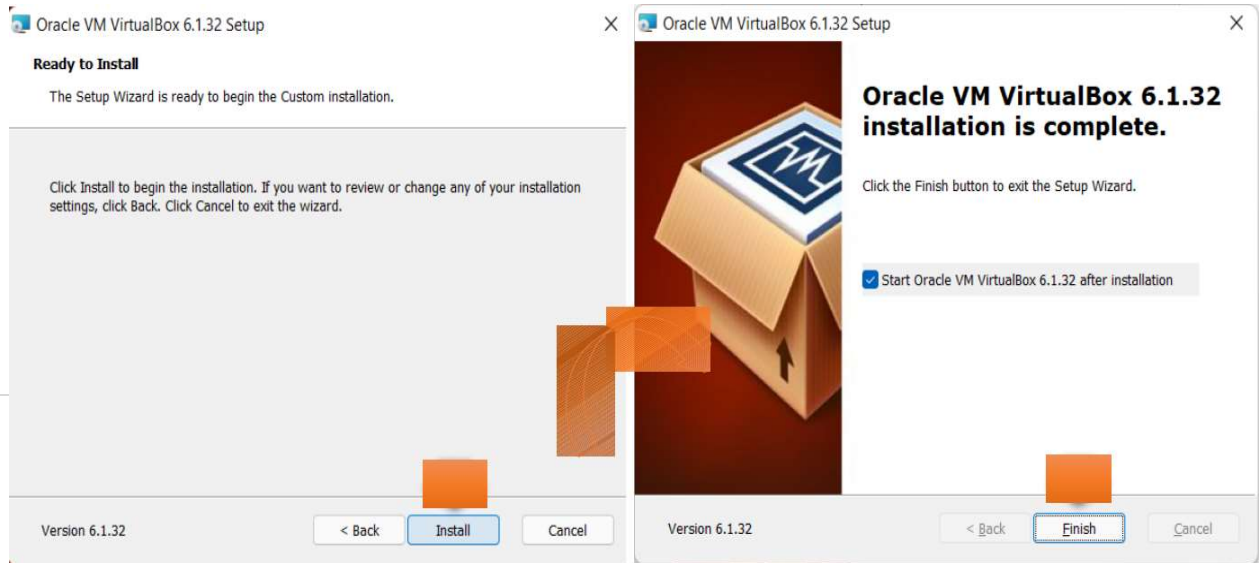
Click Select options which you want and then click “Next”

It'll warn you about the temporary network disconnection. Click “Yes”



Click "Install" on next screen.

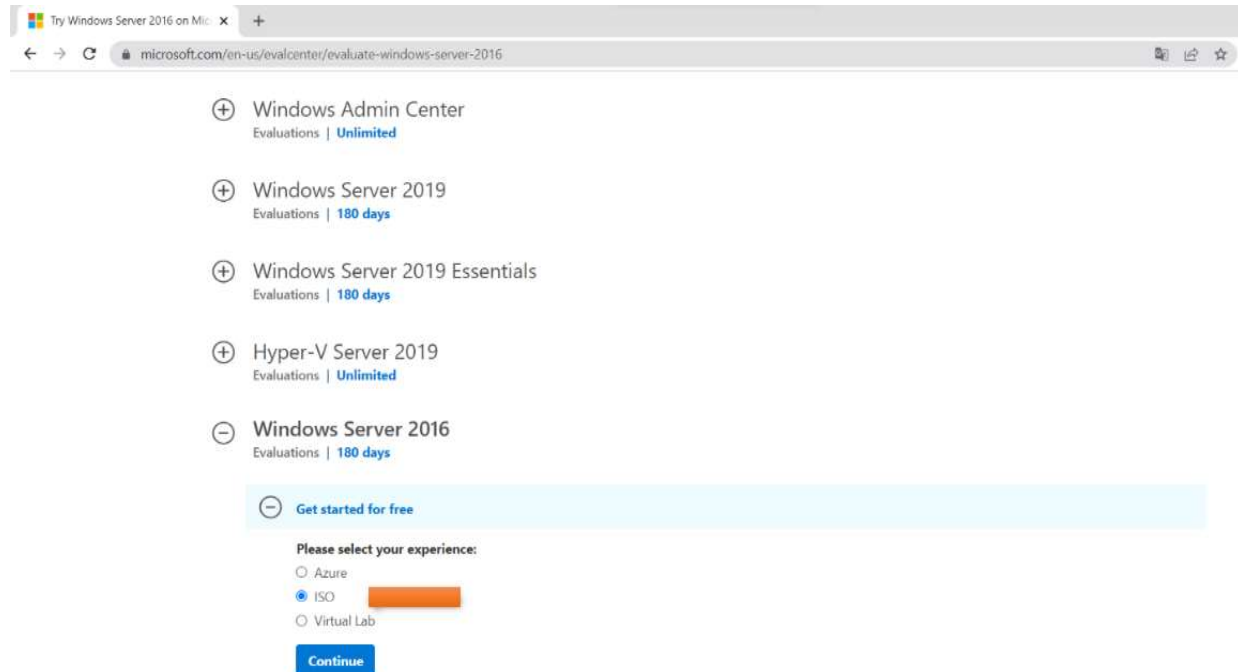
Click "Finish". It'll close the installation window



## 4. Installing Windows 2016 Server on VirtualBox

### 4.1 Download ISO Windows 2016

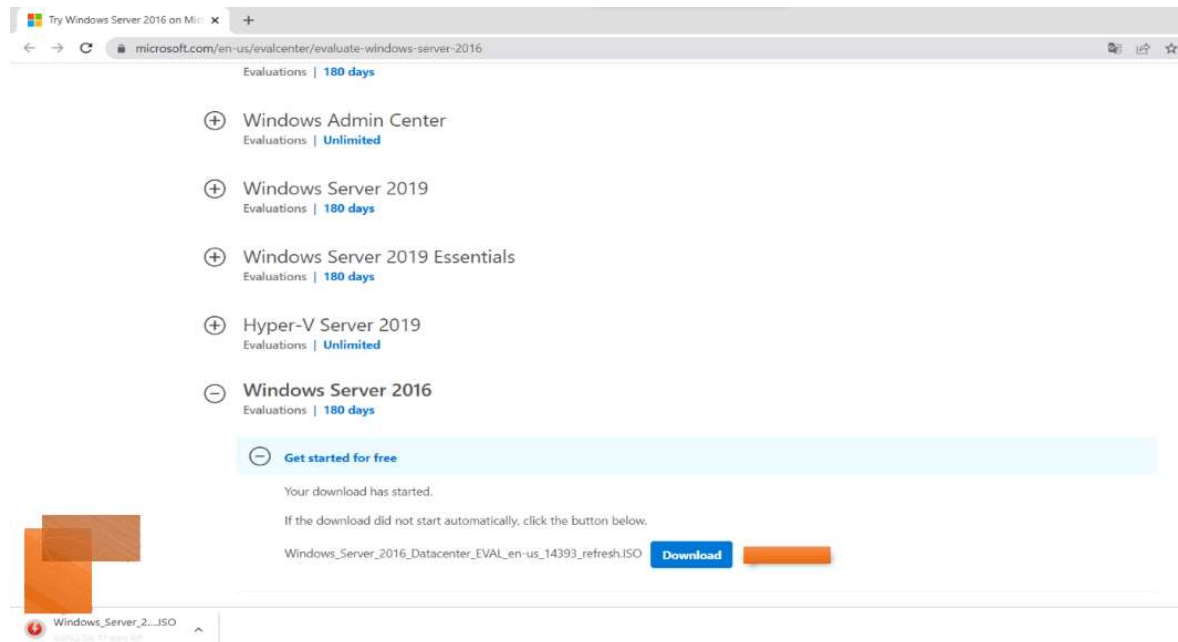
Go to <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016> in your computer's internet browser. Select ISO and click "Continue".



It'll ask for your details. Fill in all the required information and click Continue

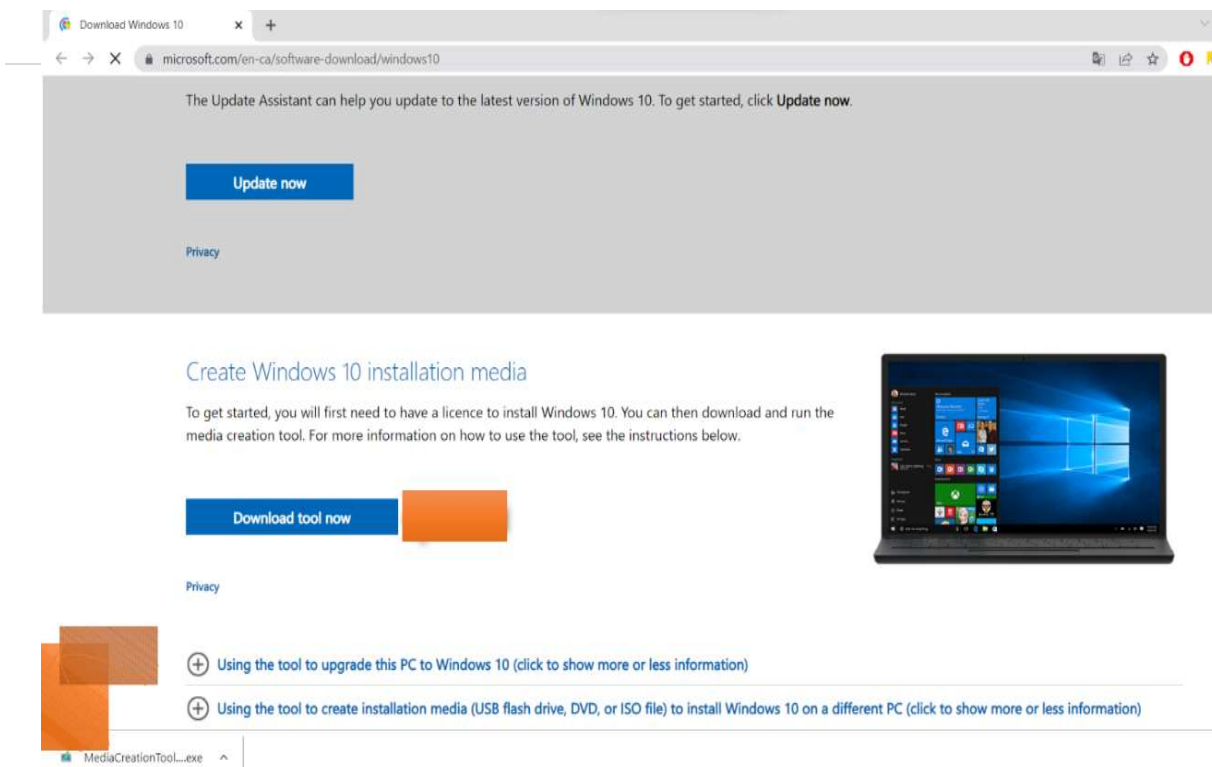
A screenshot of the registration form for Windows Server 2016 evaluation. The form is titled "Get started for free" and asks the user to complete the form to continue. It contains several required fields marked with an asterisk: First name, Last name, Company name, Company size, Job title, Work email address, Work phone number, and Country/region. Each field has a corresponding input box. Below the fields, there is a checkbox for "Yes" and a "Continue" button. A "Back" button is also visible. At the bottom, there is a consent statement: "I would like to hear from Microsoft and its family of companies via email and phone about Solutions for Businesses and Organizations and other Microsoft products and services. To withdraw consent or manage your contact preferences, visit the Promotional Communications Manager. Privacy Statement." The "Yes" checkbox is checked.

Next select language from drop down and click “Download”. Save the file on your hard drive.



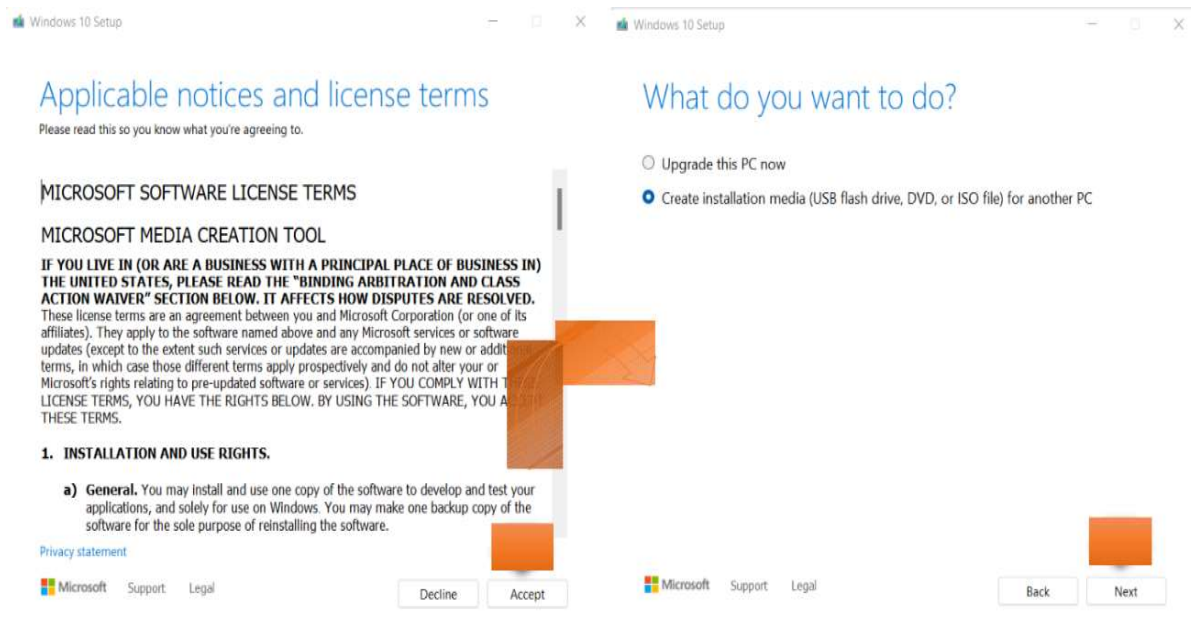
## 4.2 Download ISO Windows 10 Pro

In our lab, we are going to use Windows 10 as client machine. Download Windows 10 Image from <https://www.microsoft.com/en-ca/software-download/windows10>



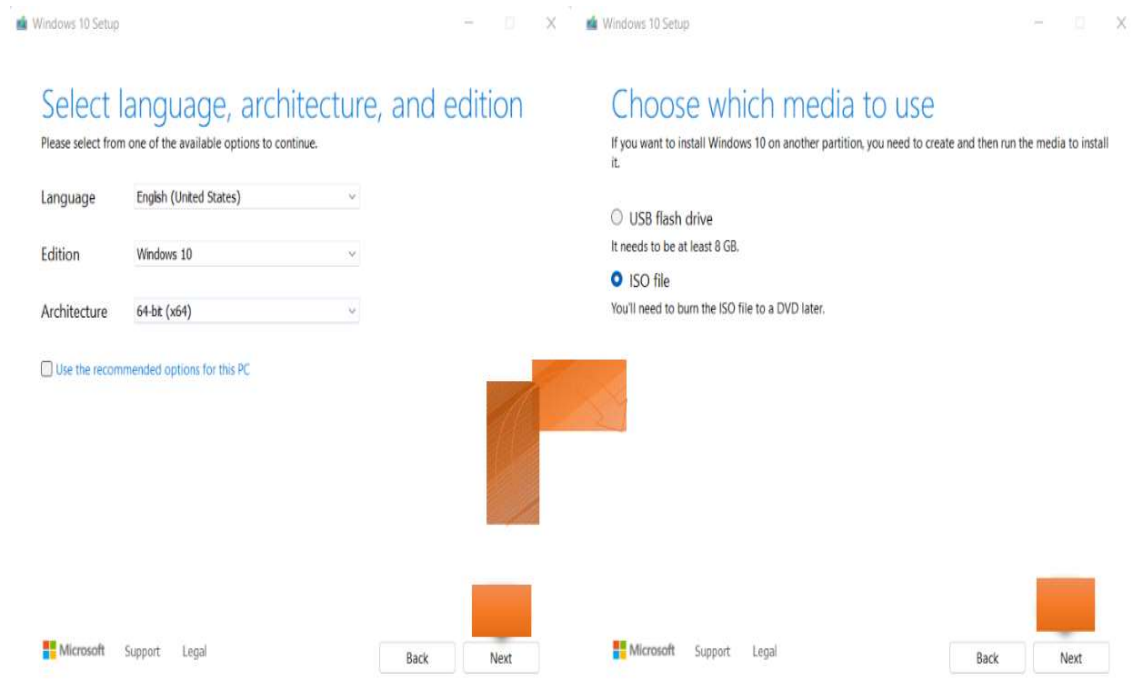
The installation window will appear. Click “Accept”

Custom setup screen will come up. Click “Create installation media...” and after Click “Next”



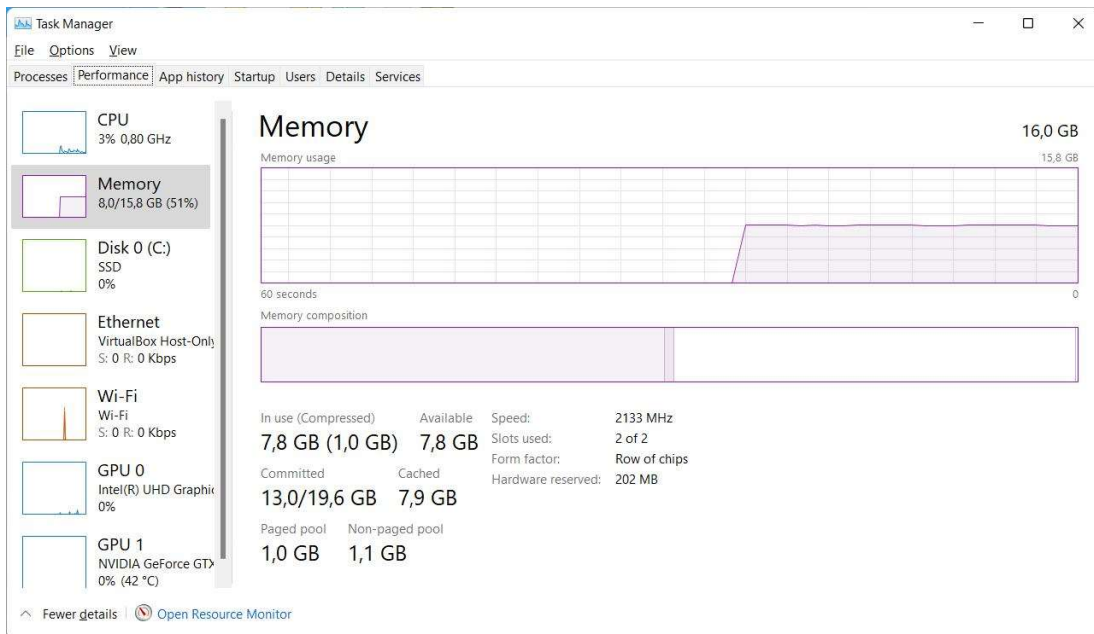
Select options which you want and then click “Next”

Custom setup screen will come up. Click “ISO file” and after Click “Next”



Finally, we have 2 Optical disc image (ISO) files that we use to install OC

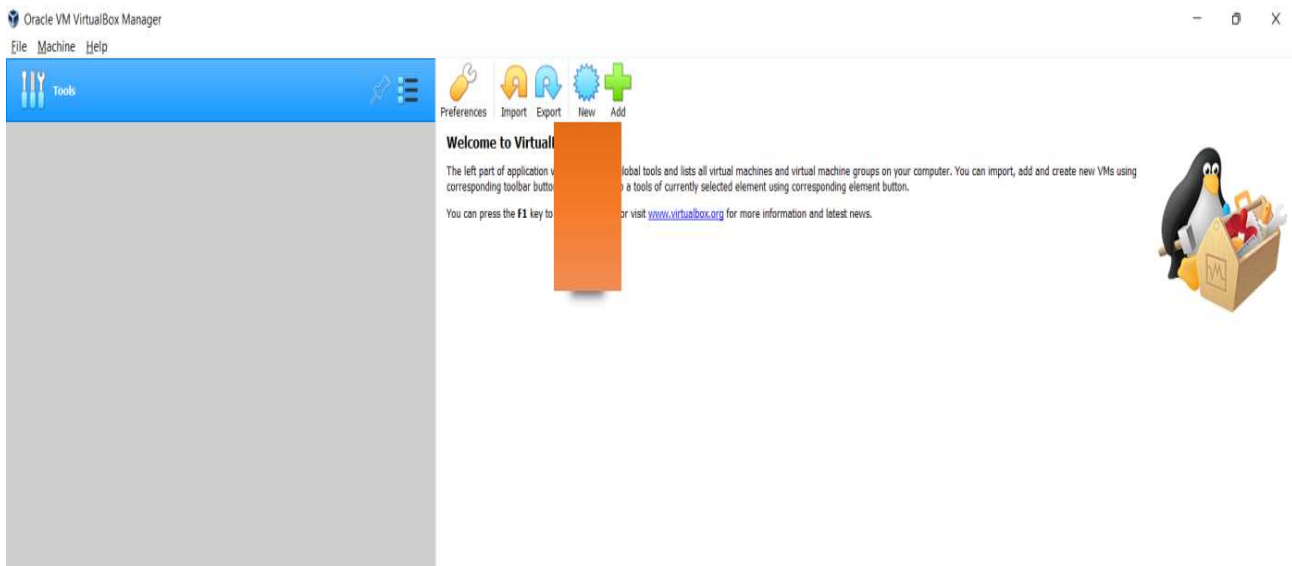
Check the available resources to set up the virtual machine with the optimal parameters for good work.



See the official pages for hardware requirements

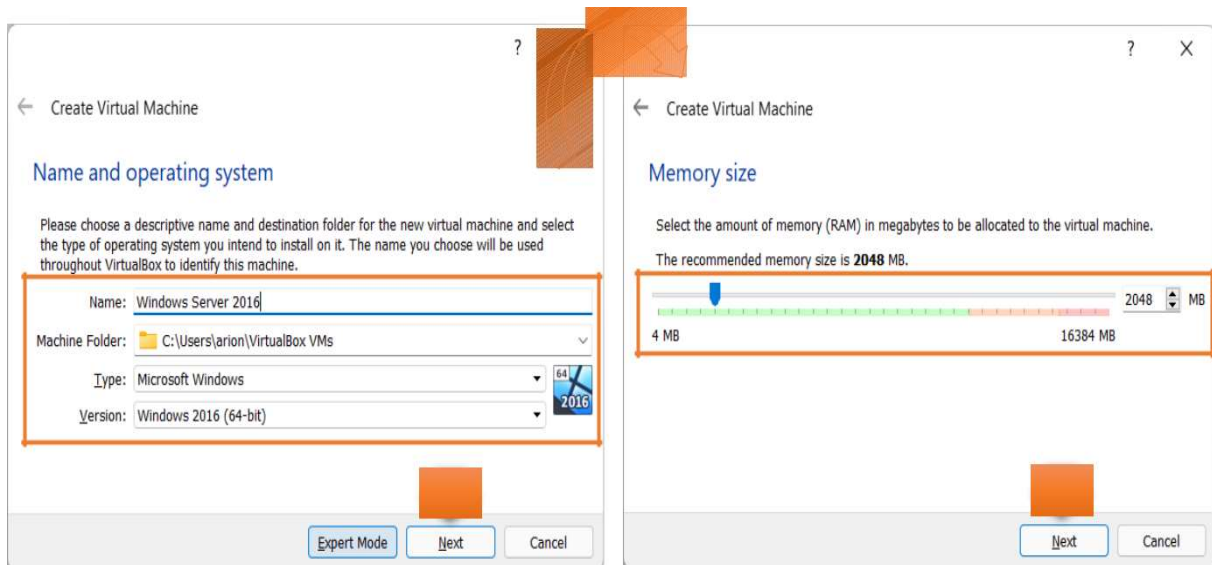
The screenshot shows the Microsoft Docs page for 'Hardware requirements for Windows Server'. The page title is 'Hardware requirements for Windows Server' with a sub-header 'Article • 12/23/2021 • 4 minutes to read • 2 contributors'. The main content area starts with an 'Important' callout: 'The highly diverse scope of potential deployments makes it unrealistic to state recommended hardware requirements that would be generally applicable. Consult documentation for each of the server roles you intend to deploy for more details about the resource needs of particular server roles. For the best results, conduct test deployments to determine appropriate hardware requirements for your particular deployment scenarios.' Below this, the 'Processor' section states: 'Processor performance depends not only on the clock frequency of the processor, but also on the number of processor cores and the size of the processor cache. The following are the processor requirements for this product: Minimum: 1.4 GHz 64-bit processor, Compatible with x64 instruction set, Supports NX and DEP, Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW, Supports Second Level Address Translation (EPT or NPT)'. The 'RAM' section states: 'The following are the estimated RAM requirements for this product: Minimum: 512 MB (2 GB for Server with Desktop Experience installation option)'. A 'Download PDF' button is visible at the bottom left.

Start VirtualBox from start menu. Click on “New”



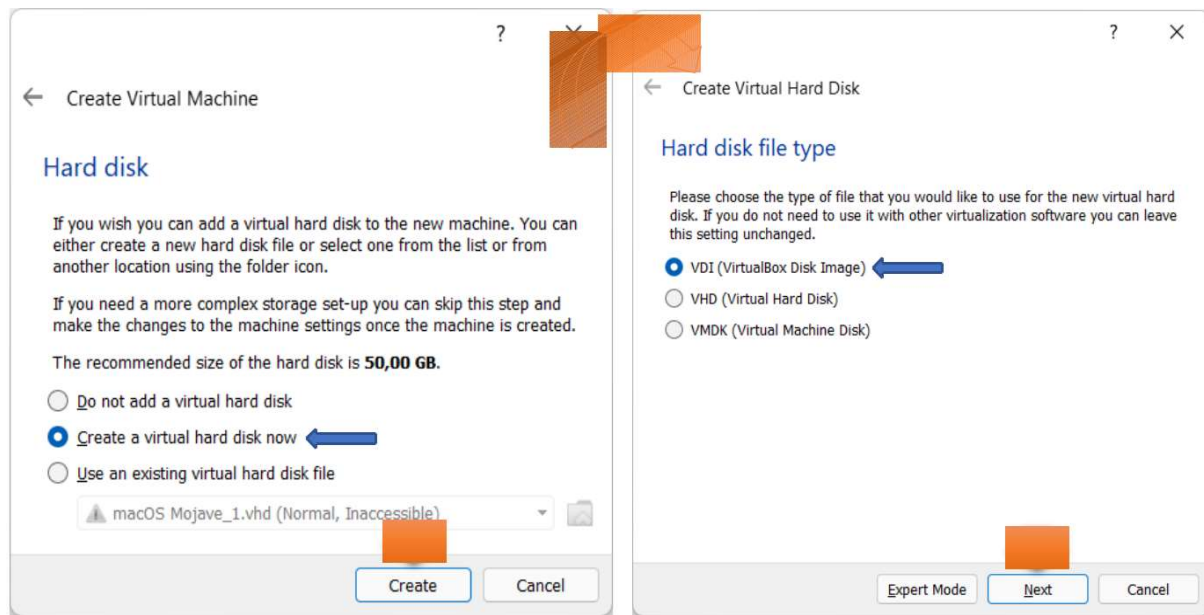
Put in desired name. We'll use “Windows 2016 Server”. It'll change the version automatically, if not, select Windows 2016 (64-bit). Click “Next”:

Next, it'll ask for memory size allocation, leave it default and click “Next”.

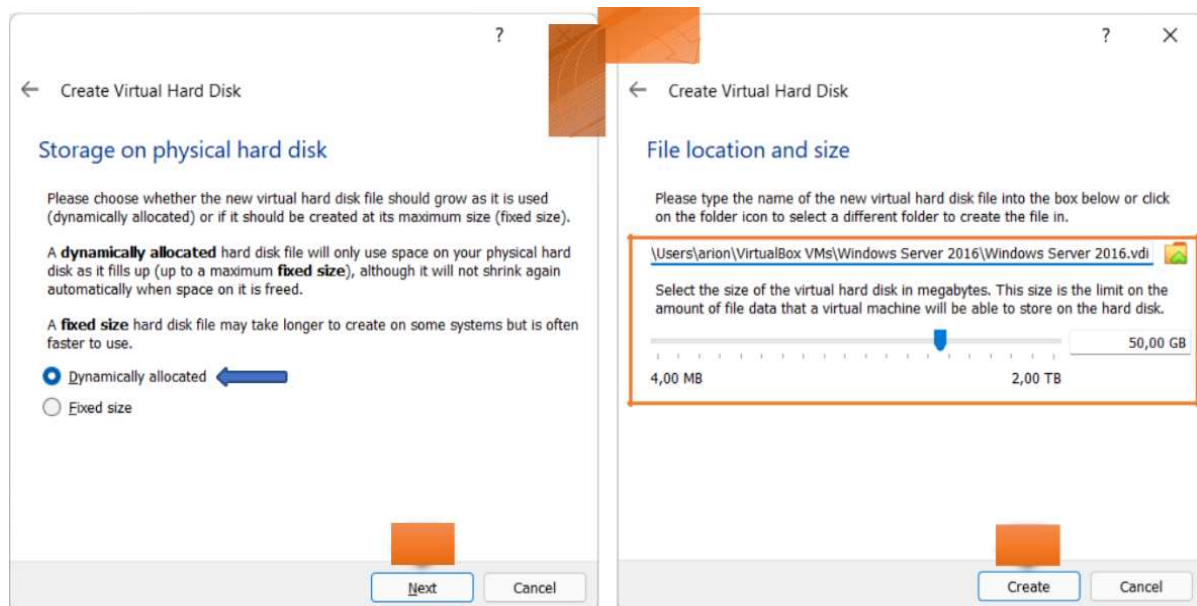


Select “Create a virtual hard disk now” and click “Create”.

Next, it'll ask for Hard disk type. VHD and VMDK options are there if you want to use this space with other virtualization software. We are not going to use other software, so we'll select “VDI (VirtualBox Disk Image)” option. Click “Next”.

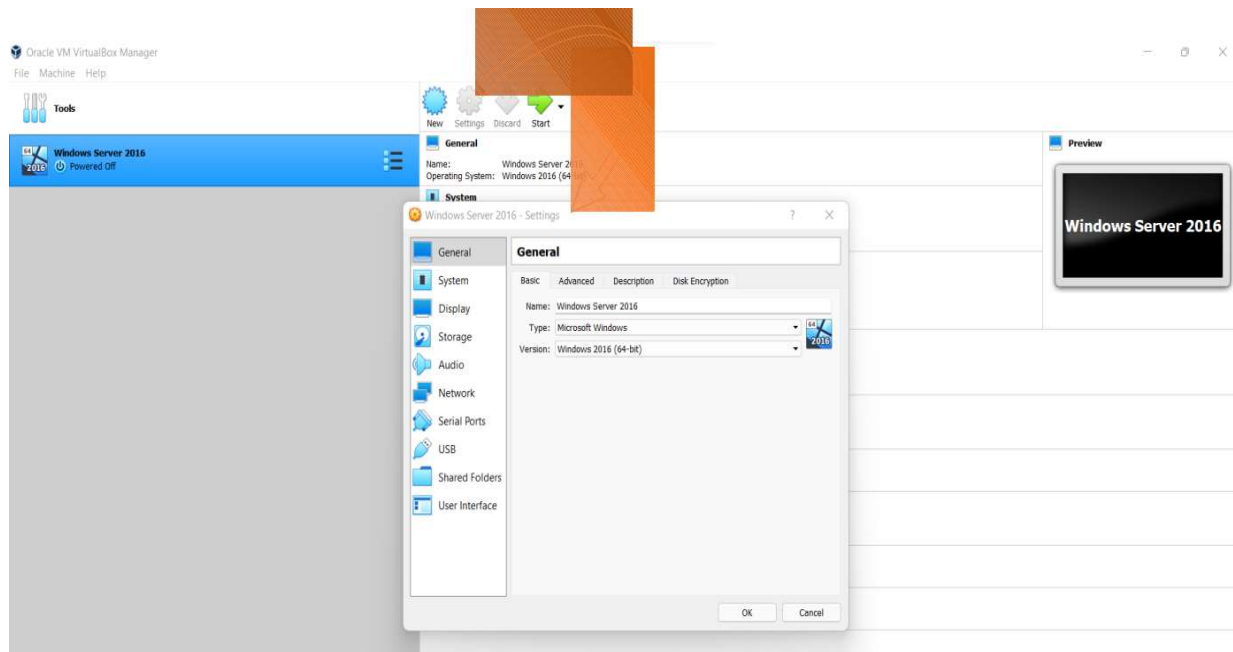


Next option is about storage on physical drive. Select “Dynamically allocated” option and then click “Next”. File location and size is next. Default is 50.00 GB. We’ll use the default option. Click “Create”

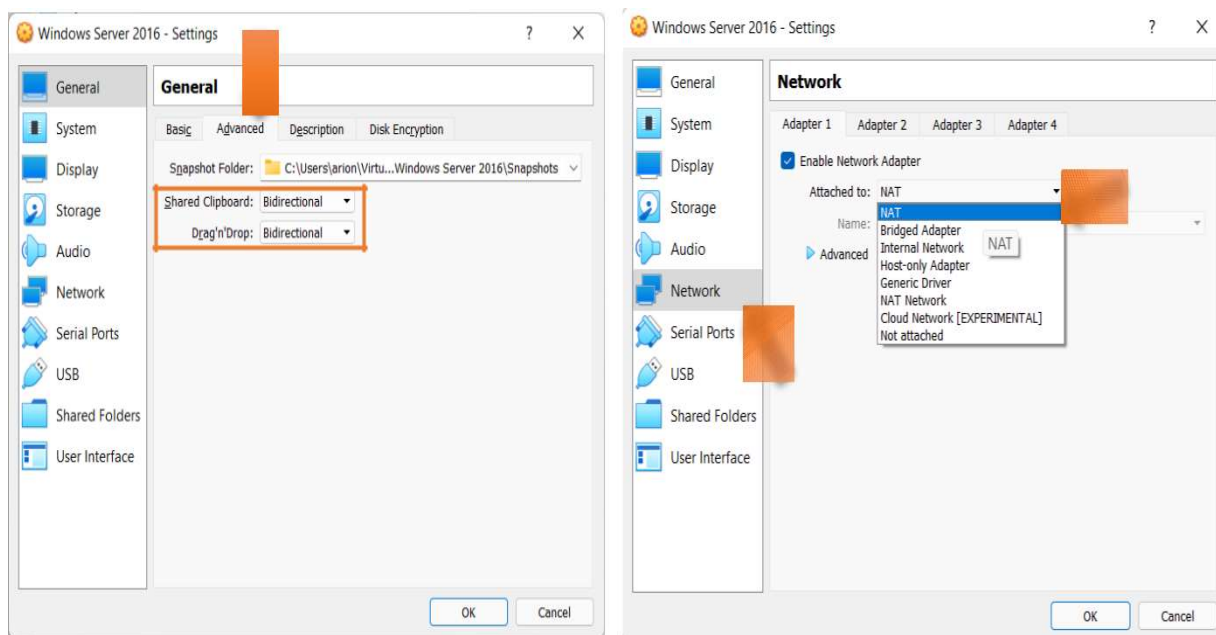


Windows 2016 Server will appear under Tools. Click “Settings” button.

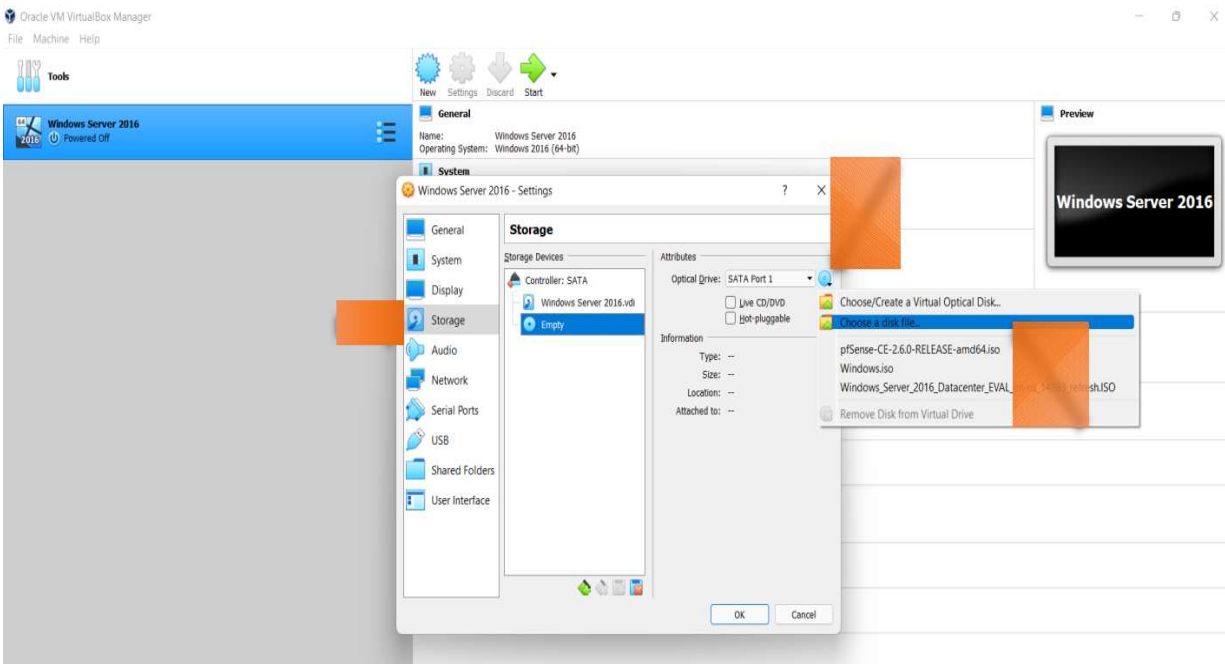
Windows 2016 Server settings will popup



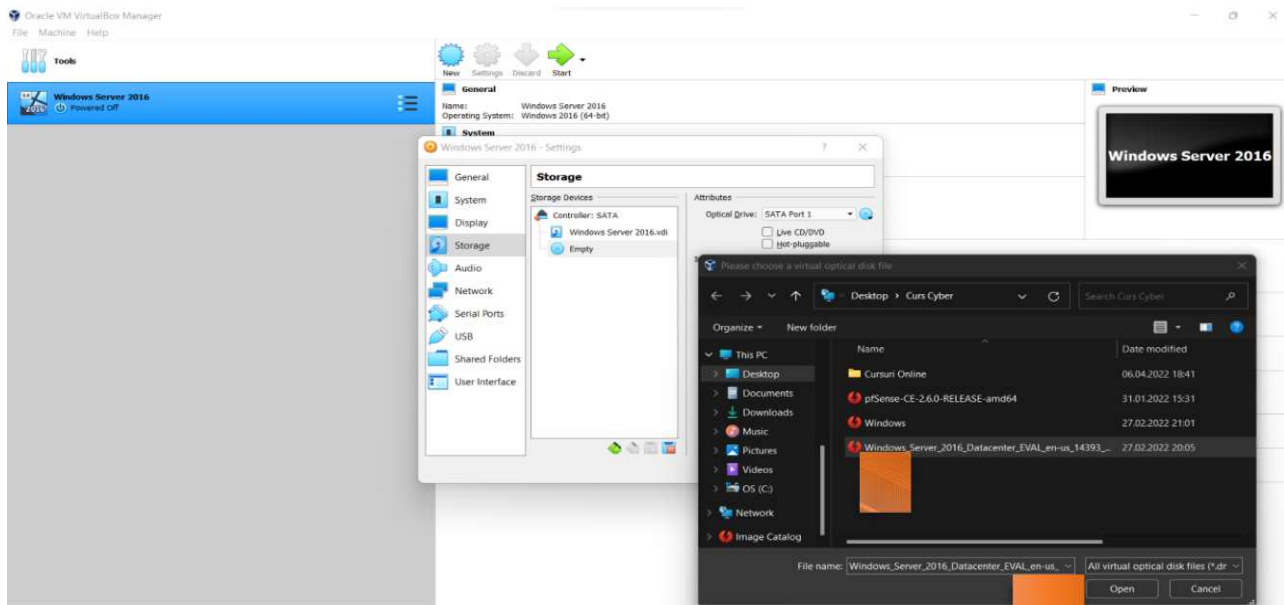
Go to General ----> Advanced. Change "Shared Clipboard" and "Drag'n'Drop" options from Disabled to Bidirectional Select Network. Under Adapter 1, go to "Attached to" option and from drop down box select "Host-only Adapter"



Now go to Storage option. Under Controller: SATA, select Empty. Then click on CD icon on far right. Select "Choose a disk file....." option

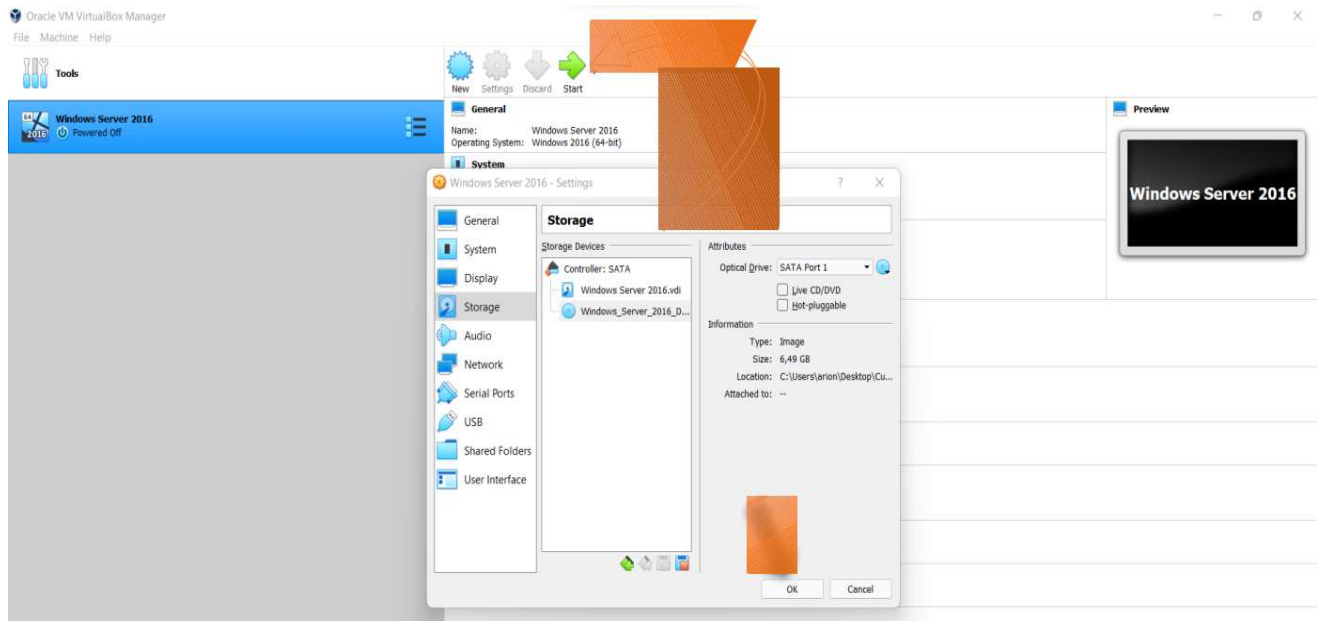


Select the folder where you have downloaded Windows 2016 Server ISO file. Select the file and click “Open”.

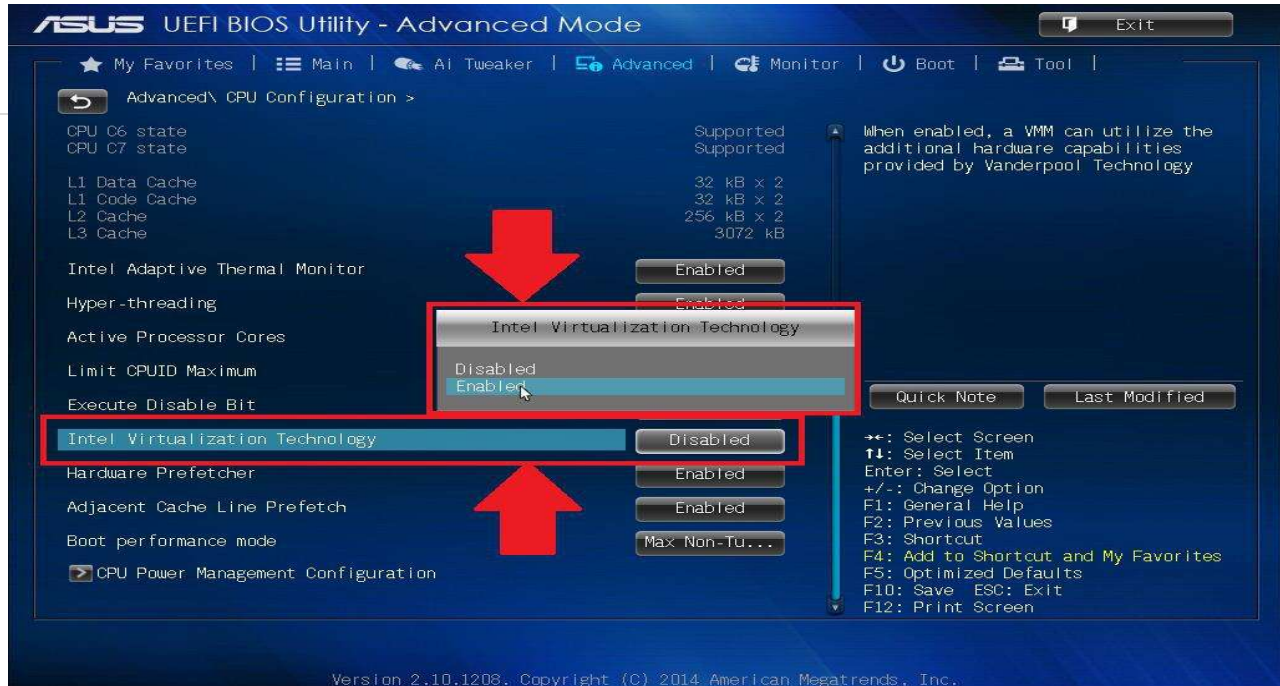


### 4.3 Windows 2016 Server Installation

Click “Start” from main VirtualBox window.

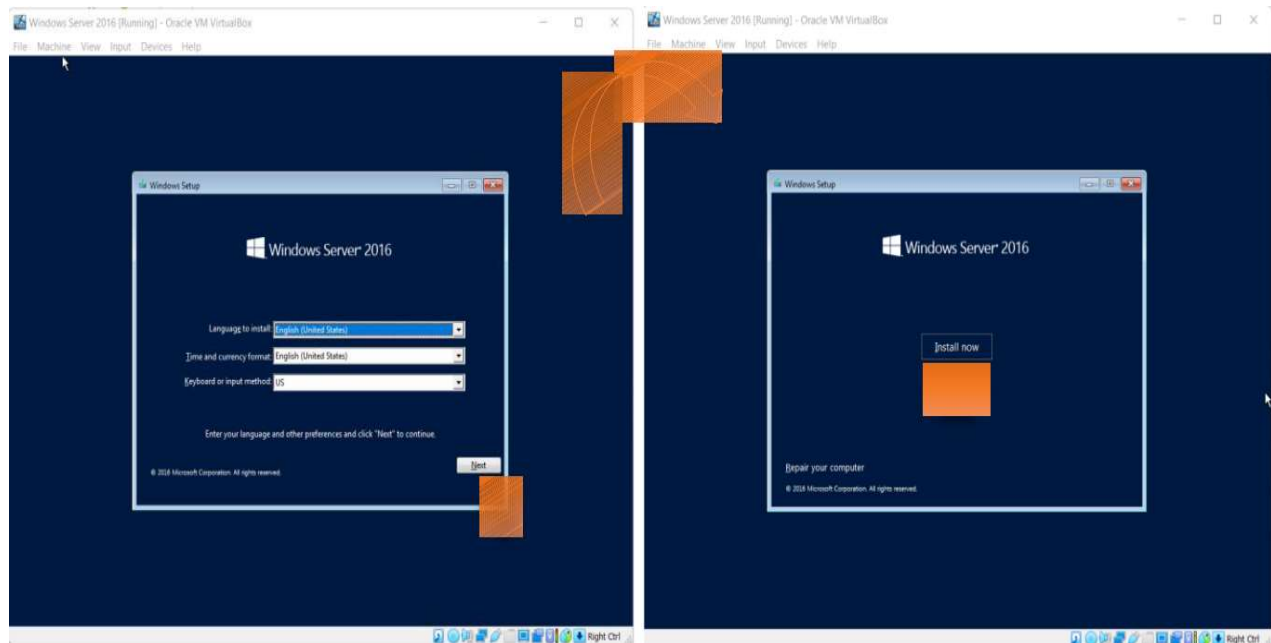


If an error occurs at Startup, then the computer is turned off then the bios menu is accessed and virtualization is activated.

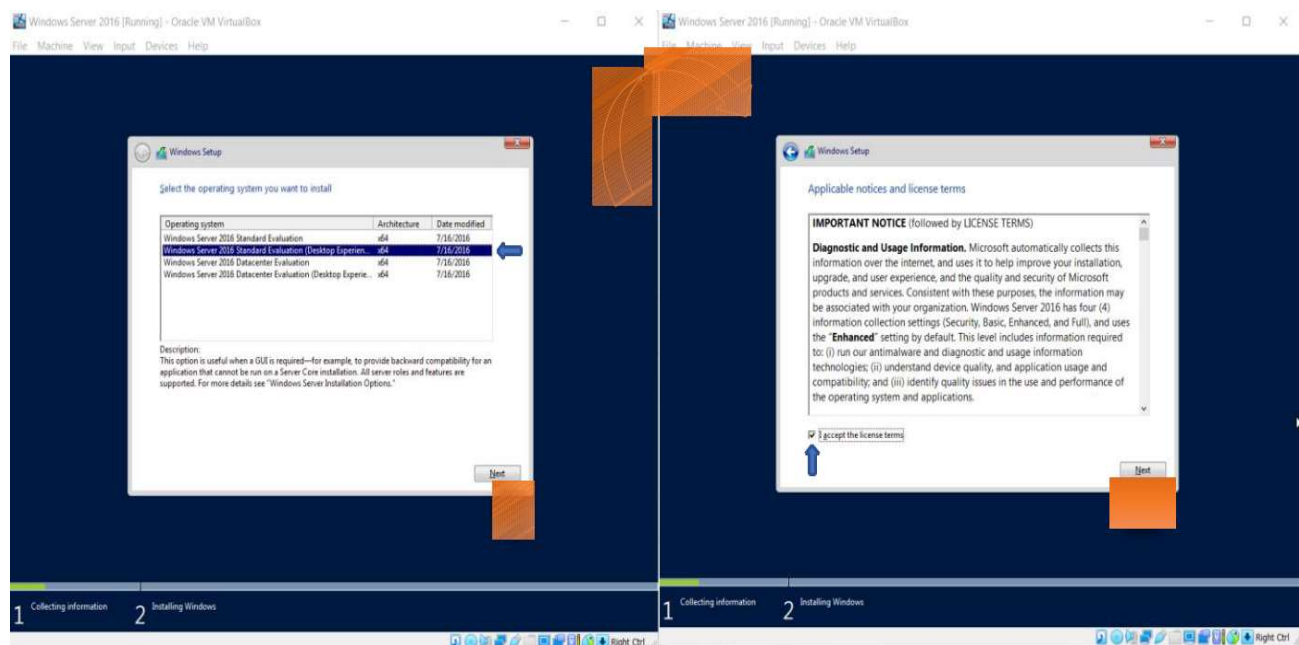


Click “Start” on next screen. If it doesn’t have Windows Server 2016 option, click drop down menu and select it.

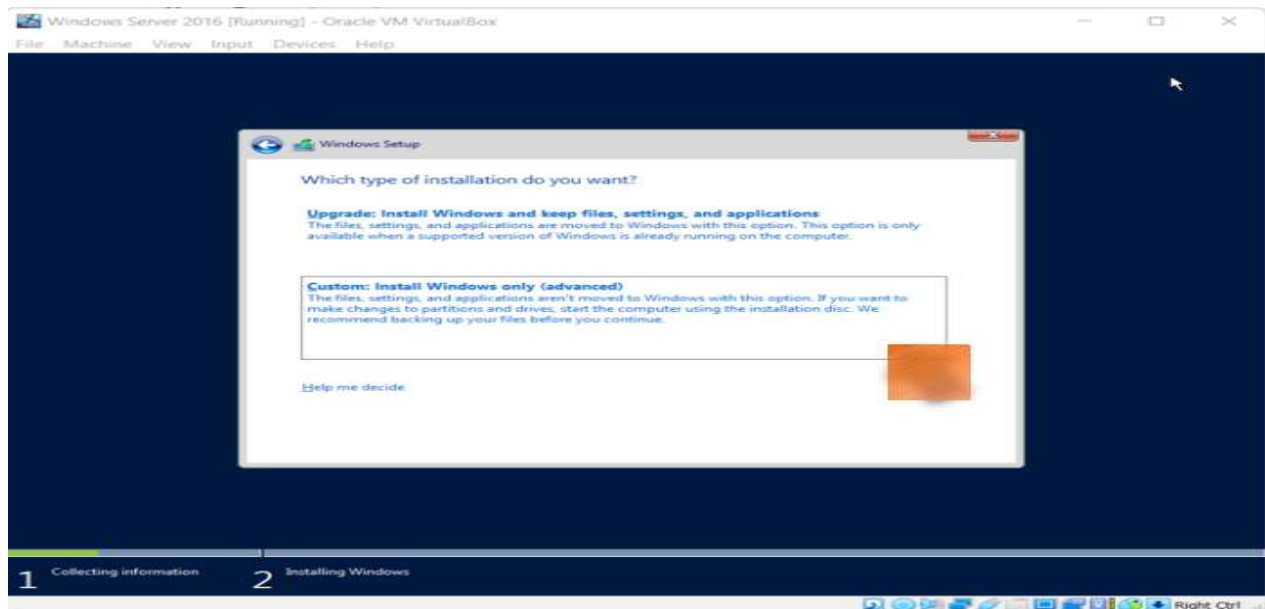
Select Language, Time & Currency, and input method from drop down. Click “Next”. Click “Install Now”



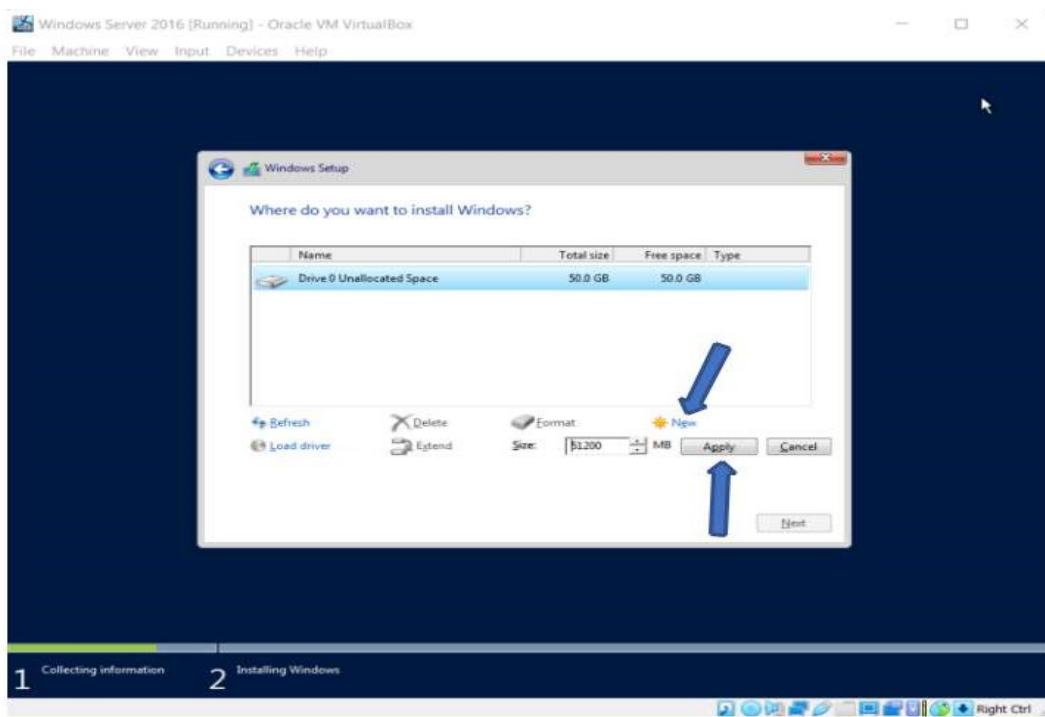
Select "Windows Server 2016 Standard Evaluation (Desktop Experience)". Click "Next".  
Select "I accept the license terms" check box and click "Next".



Select "Custom: Install Windows only (advanced)"



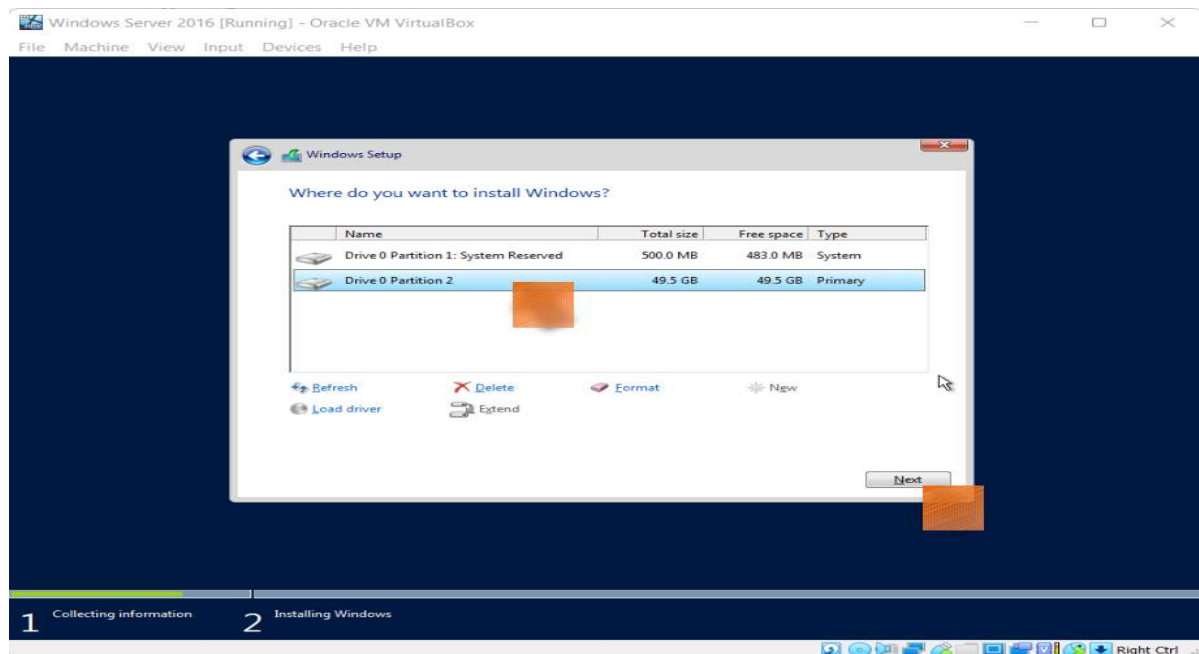
Click "New". Click "Apply".



Windows pop will appear. Click "OK"

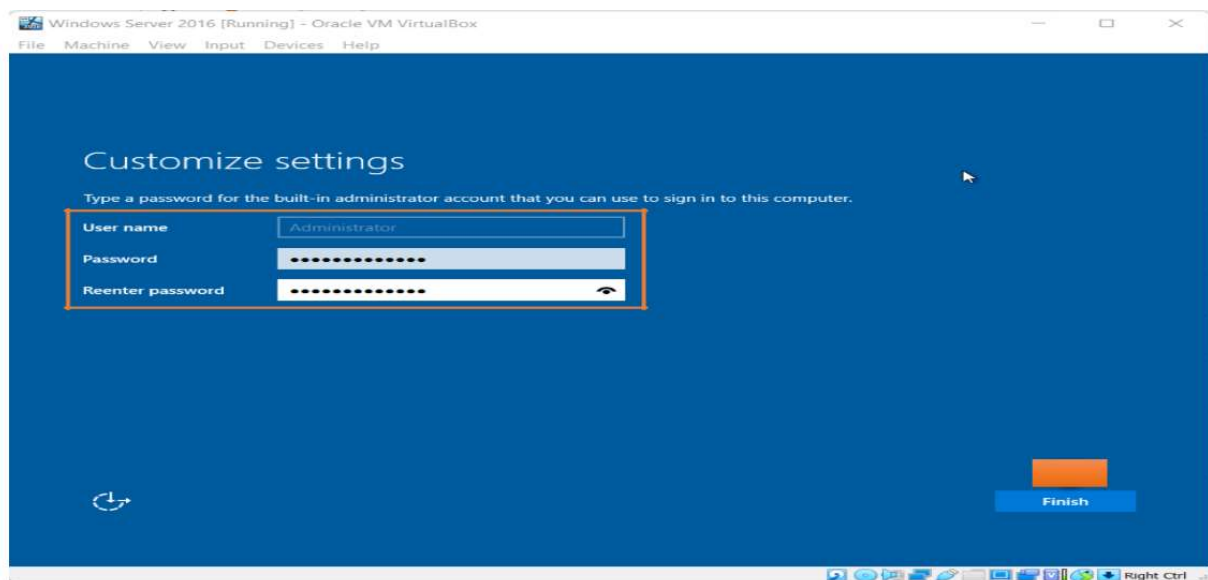
Click on Partition 2 and then click "Next"

Windows installation will start.

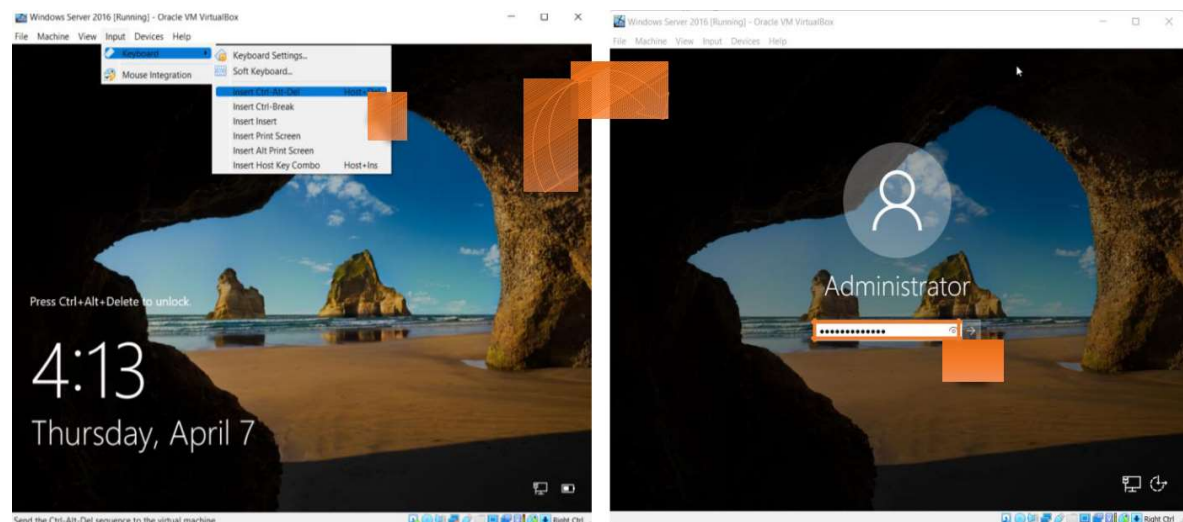


Once done, it'll reboot.

Create Administrator password and click "Finish".

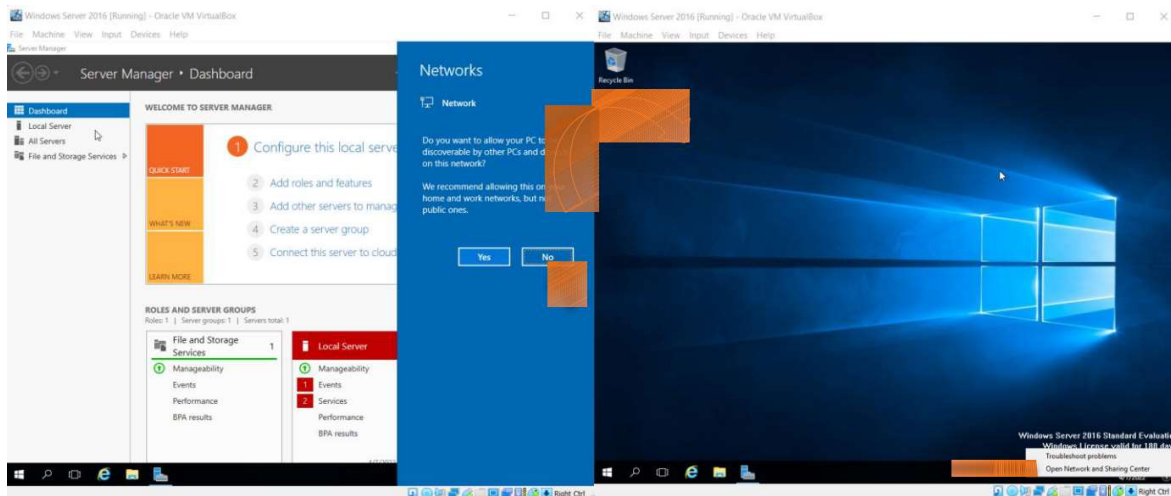


Select: Input ----> Keyboard ----> Insert Ctrl-Alt-Del.

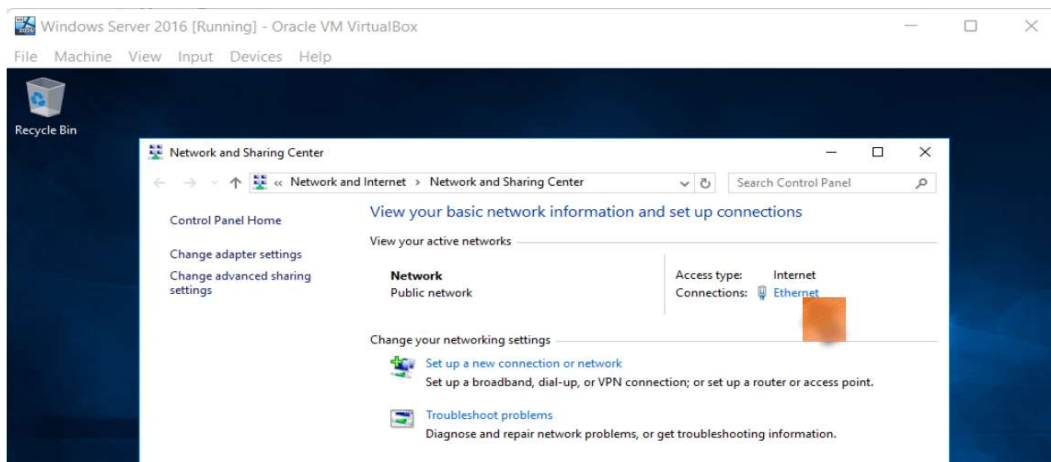


After logging in, it'll open the Server Manager. This screen means server is installed.

We do not allow other PCs to find this one. Right click on small monitor icon on right bottom side of screen, beside clock. Select "Open Network and Sharing Center".

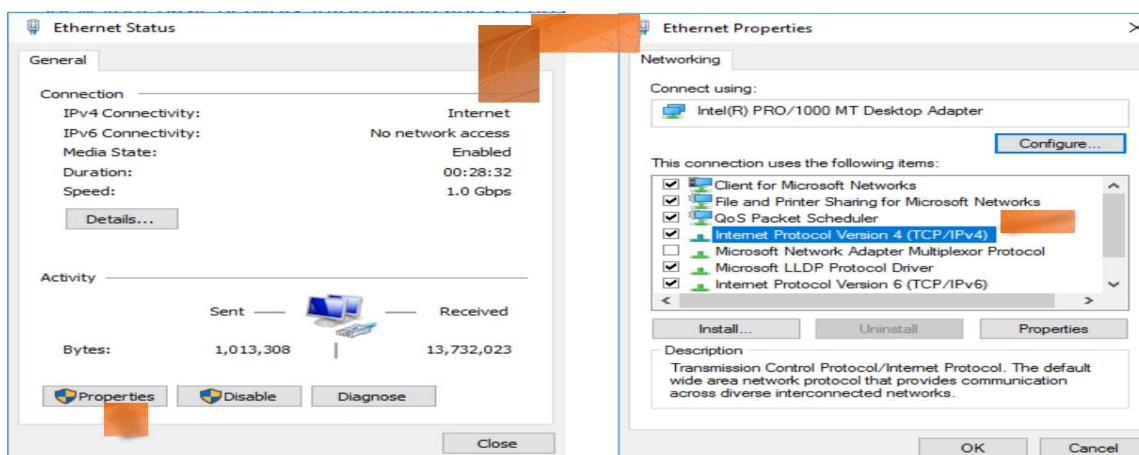


Network and Sharing Center screen will appear. Click "Ethernet"



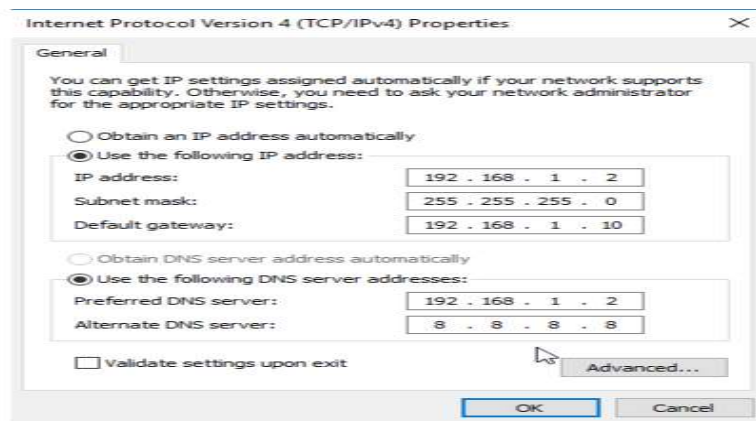
Ethernet Status screen will popup. Click "Properties" button.

Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".



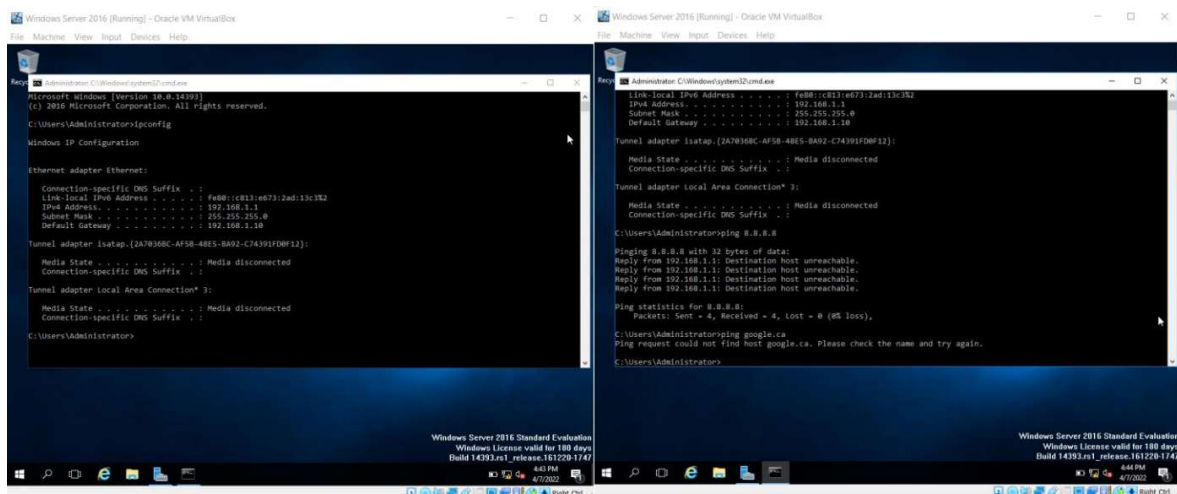
Select "Use the following IP address:"

radio button and fill in the required information. We used the following information. Click "OK". Select "Close" on next 2 screens.

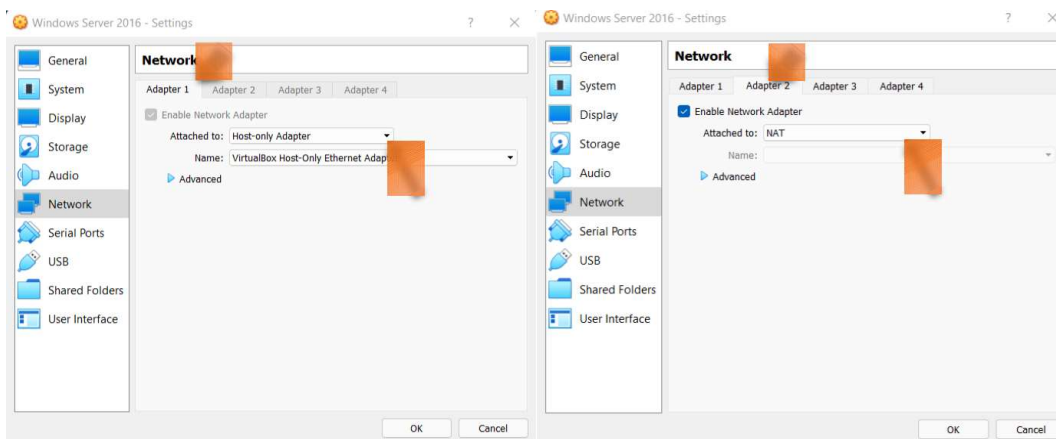


Through the command line we check if the network settings have been applied using the "IPCONFIG" command.

We apply the "ping" command to the google.ca site to check the internet access.



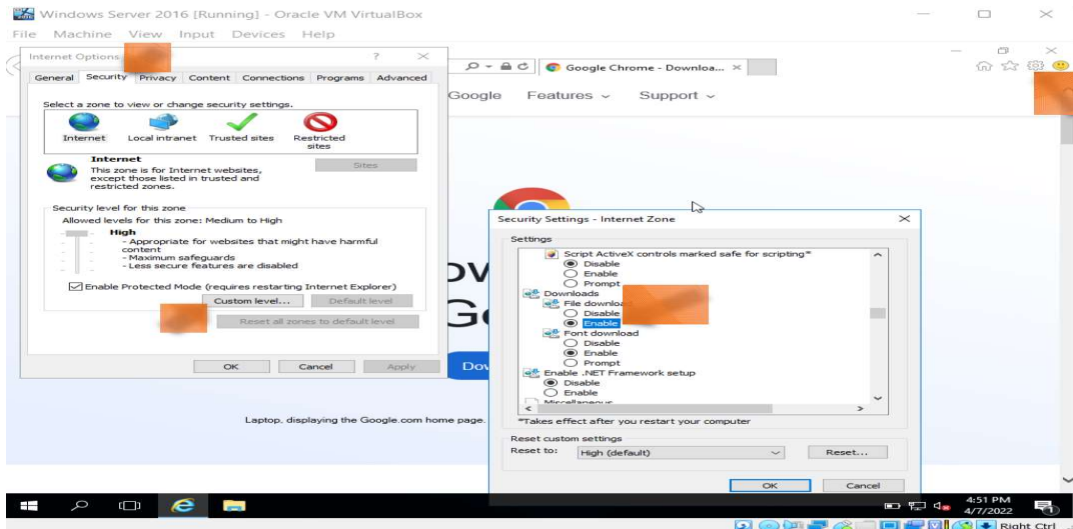
The settings for the top network are used to connect to the firewall. But now I am temporarily activating the second adapter with NAT (Network Address Translation) settings for temporary internet access. We shut down the operating system and change the system settings. Activate the 2nd adapter



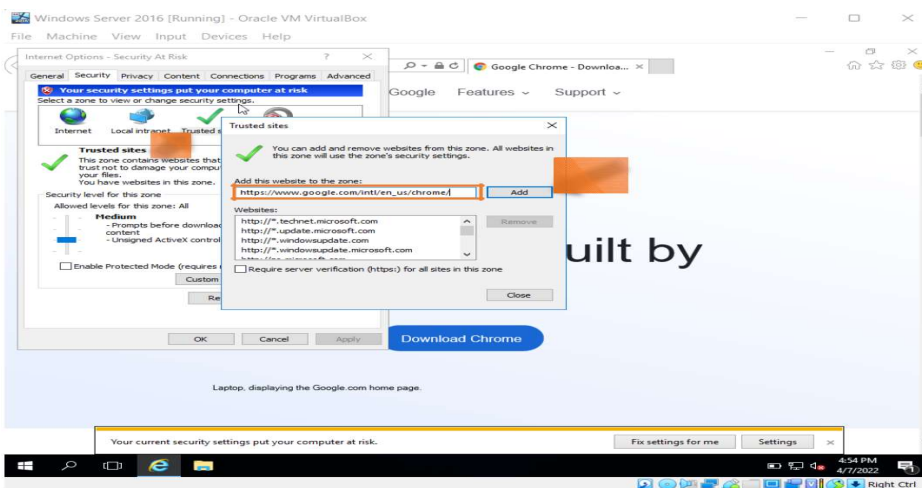
## Install Google Chrome browser

We access the Internet Explorer browser, and enter the site

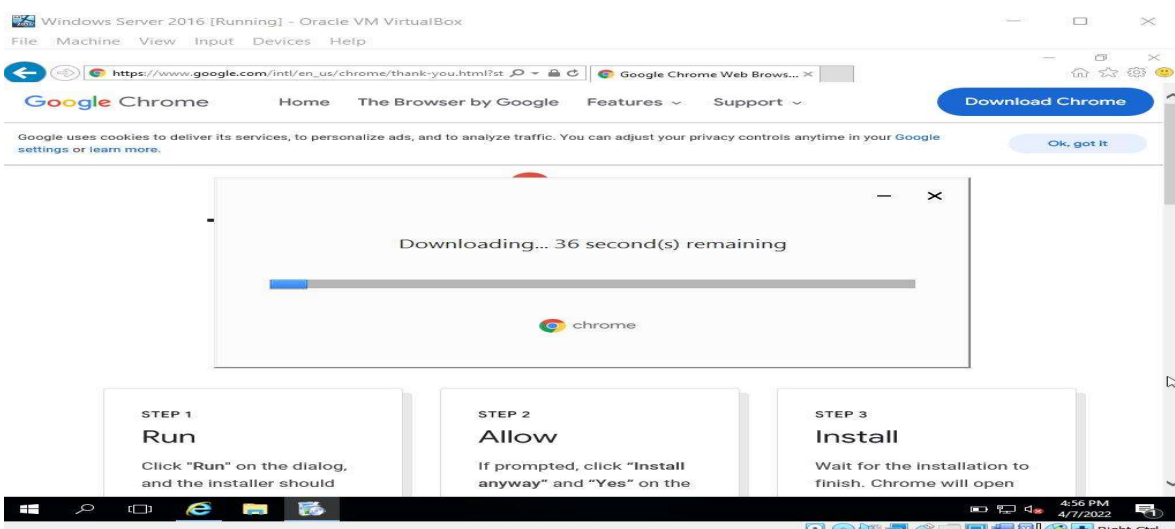
[https://www.google.com/intl/en\\_us/chrome/](https://www.google.com/intl/en_us/chrome/) Then in the internet settings it allows you to download the files



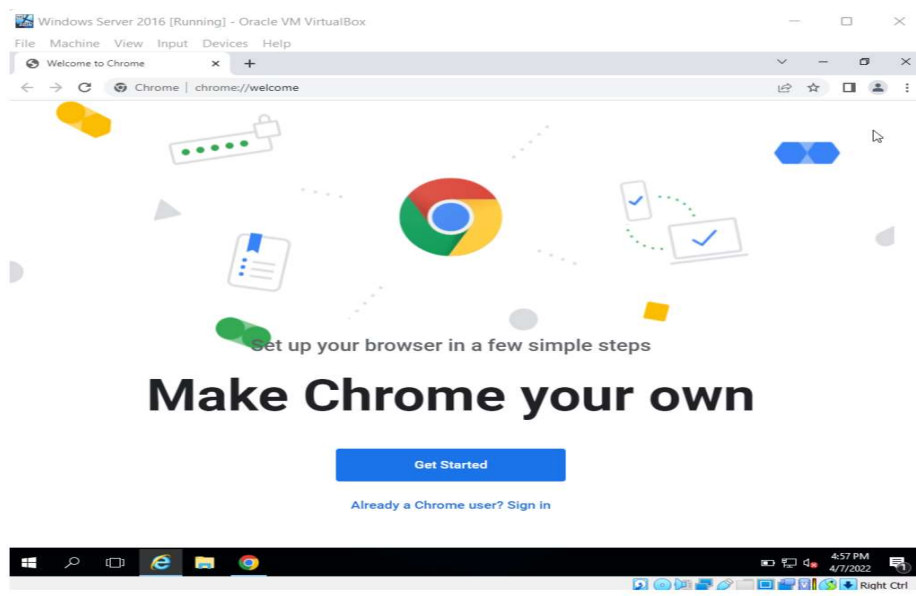
We apply the download site as trusted so that it can be accessed



Download and install the browser following the steps.



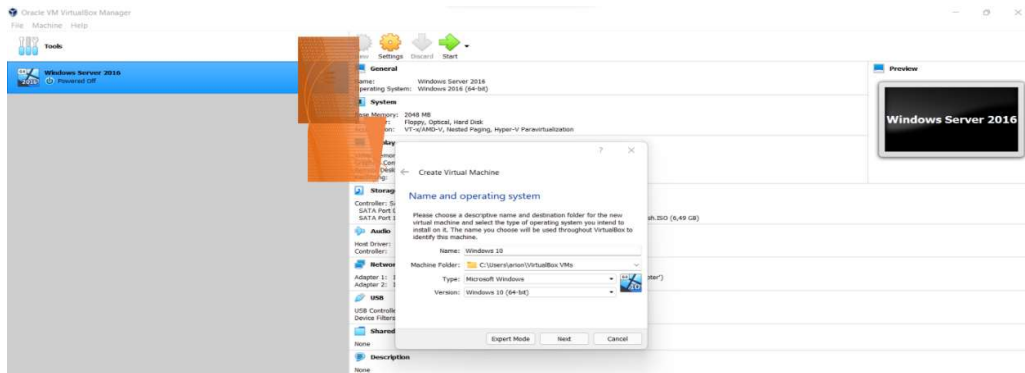
Final Browser is installed. We use this browser because it is faster and has the necessary extensions to open most sites.



## 5. Installing Windows Client (Windows 10 Pro)

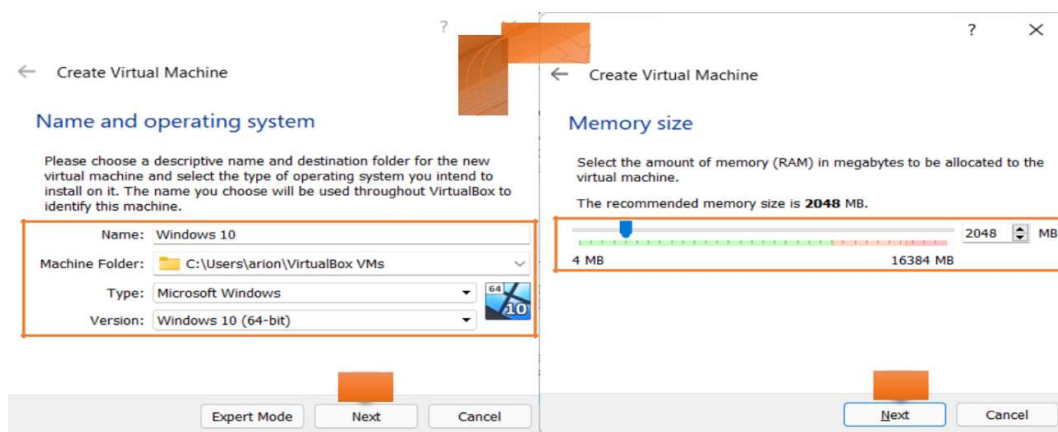
### 5.1 Virtual machine configuration

Start VirtualBox from start menu. Click on “New”



Put in desired name. We'll use “Windows 10”. It'll change the version automatically, if not, Select Windows 10 (64-bit). Click “Next”:

Next, it'll ask for memory size allocation, leave it default and click “Next”.



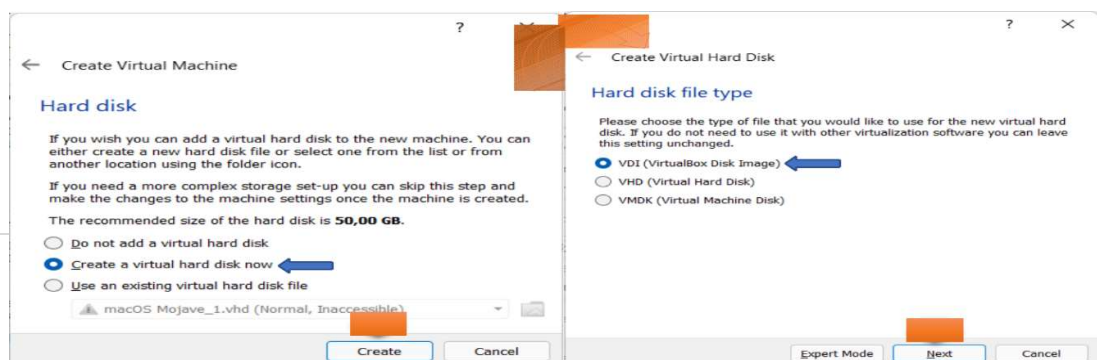
Select “Create a virtual hard disk now” and click “Create”.

Next, it'll ask for Hard disk type.

VHD and VMDK options are there if you want to use this space with other virtualization software.

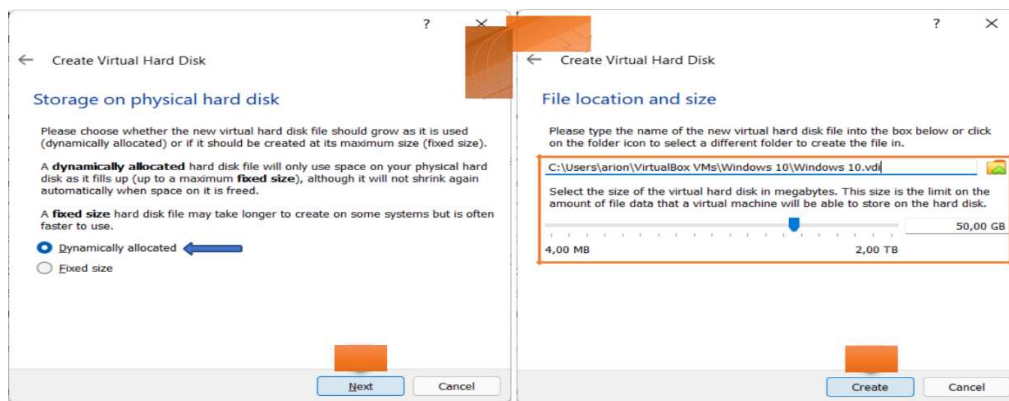
We are not going to use other software, so we'll select “VDI (VirtualBox Disk Image)” option.

Click “Next”.

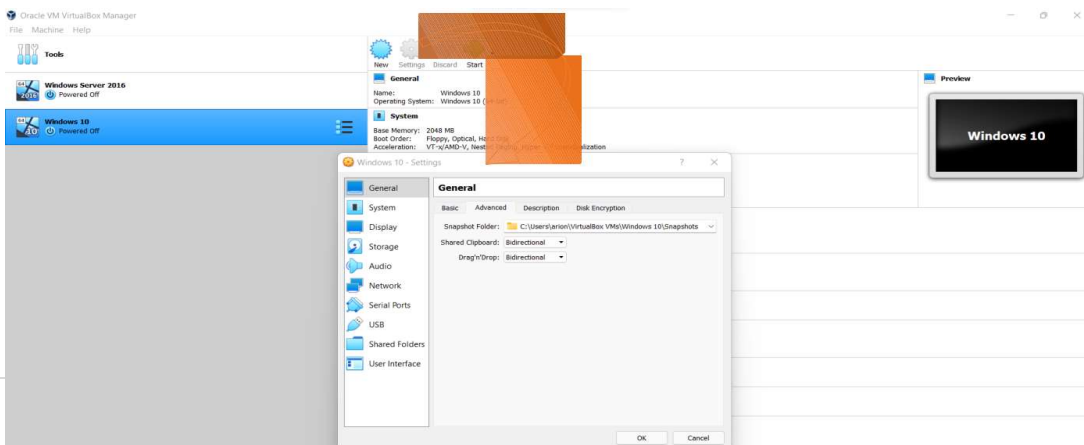


Next option is about storage on physical drive. Select “Dynamically allocated” option and then click “Next”.

File location and size is next. Default is 50.00 GB. We’ll use the default option. Click “Create”

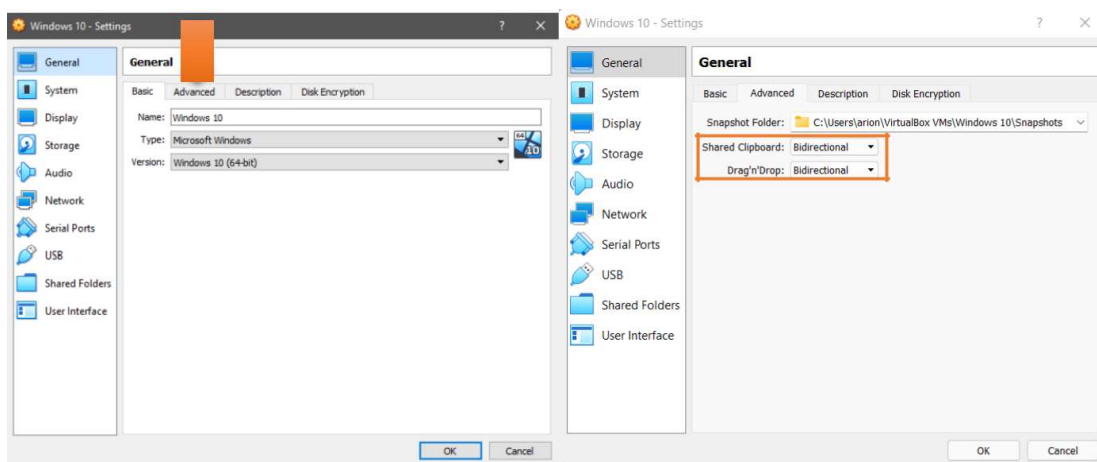


Windows 10 will appear under Tools. Click “Settings” button.

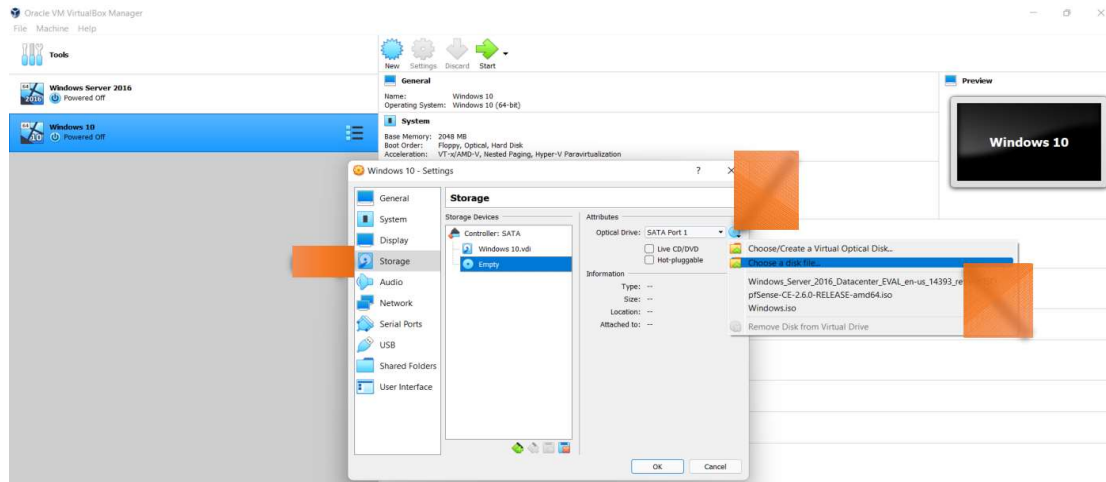


Windows 10 settings will popup.

Go to General ----> Advanced. Change “Shared Clipboard” and “Drag’n’Drop” options from Disabled to Bidirectional.

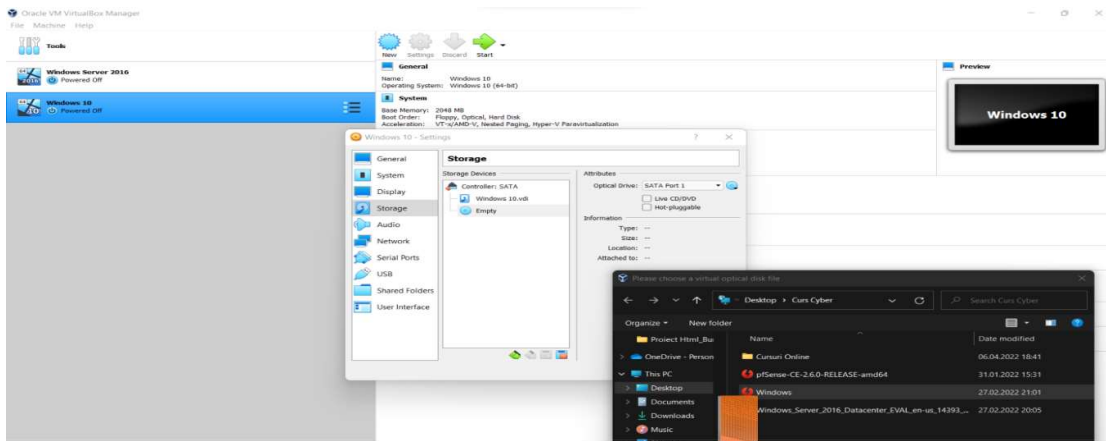


Now go to Storage option. Under Controller: SATA, select Empty. Then click on CD icon on far-right side. Select “Choose a disk file....” option.



Select the folder where you have downloaded Windows 10 ISO file.

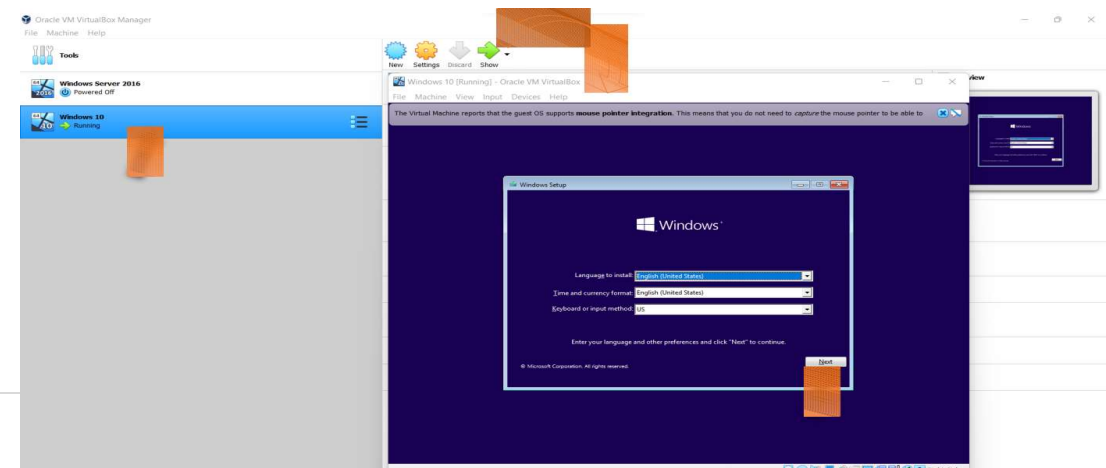
Select the file and click "Open" Press "OK" on main settings window.



## 5.2 Windows 10 Pro Installation

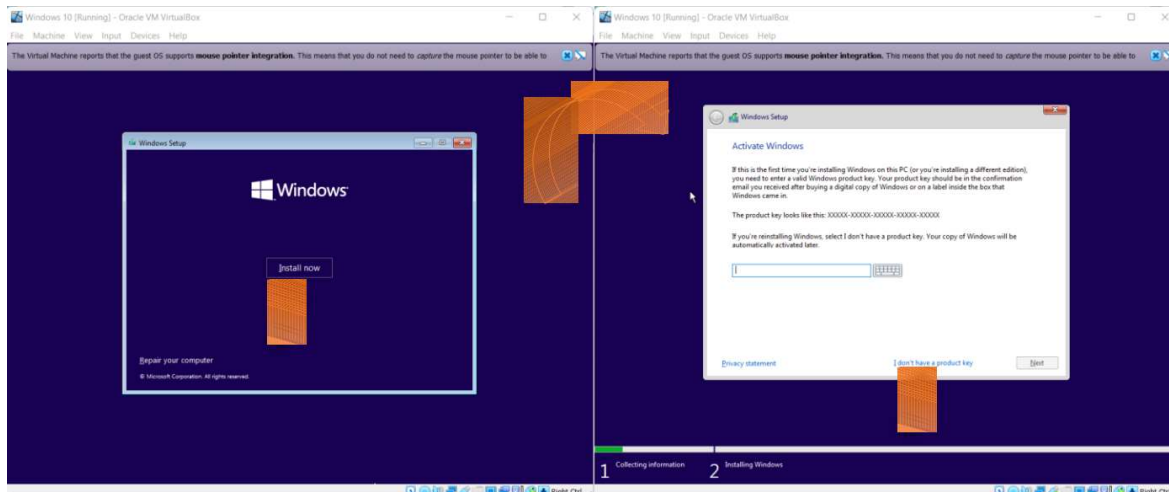
Select Windows 10 from left panel and then click “Start”.

Click "Start" on next screen. If it doesn't have Windows 10 option, click drop down menu and select it. Select Language and other preference and click "Next".



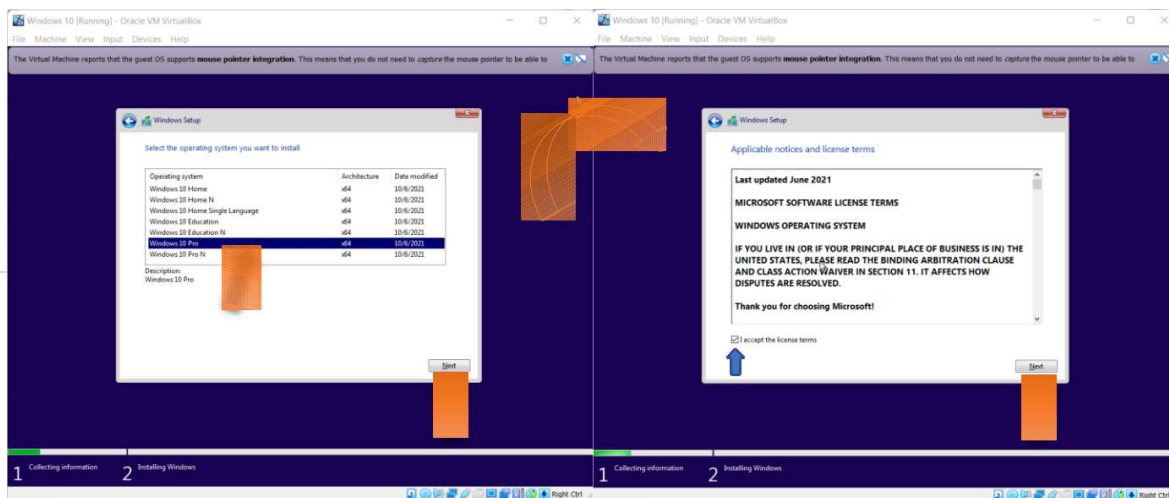
Click "Install now"

Select "I don't have a product key" and click "Next"

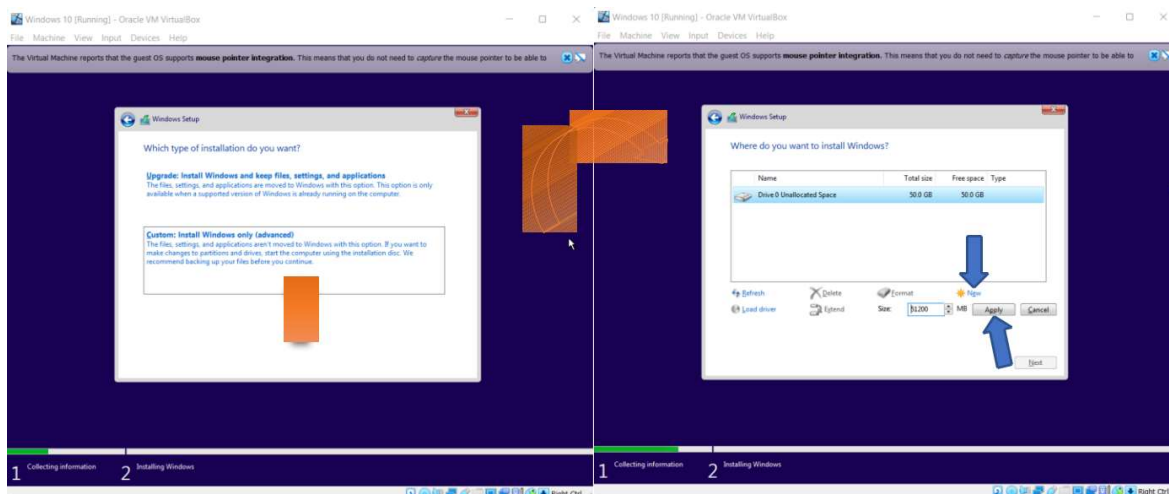


Select "Windows 10 Pro" and click "Next"

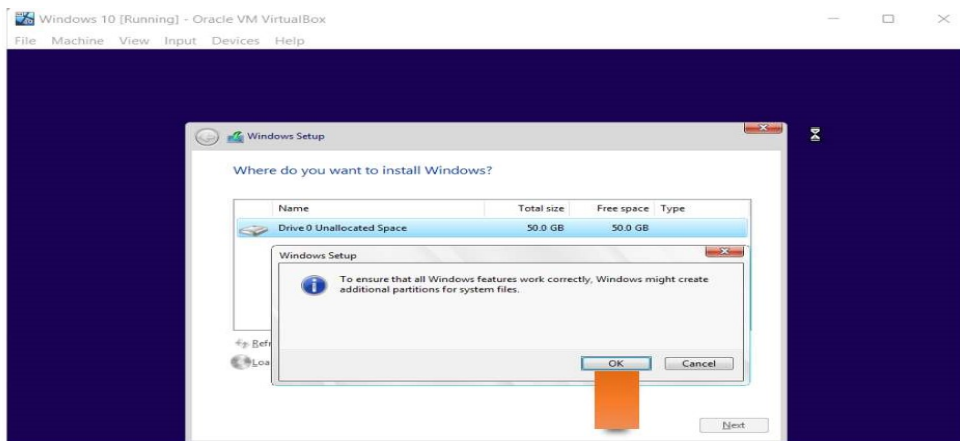
Select check box "I accept the license terms" and click "Next".



Click on "Custom: Install Windows only (advanced)". Click "New". Click "Apply".

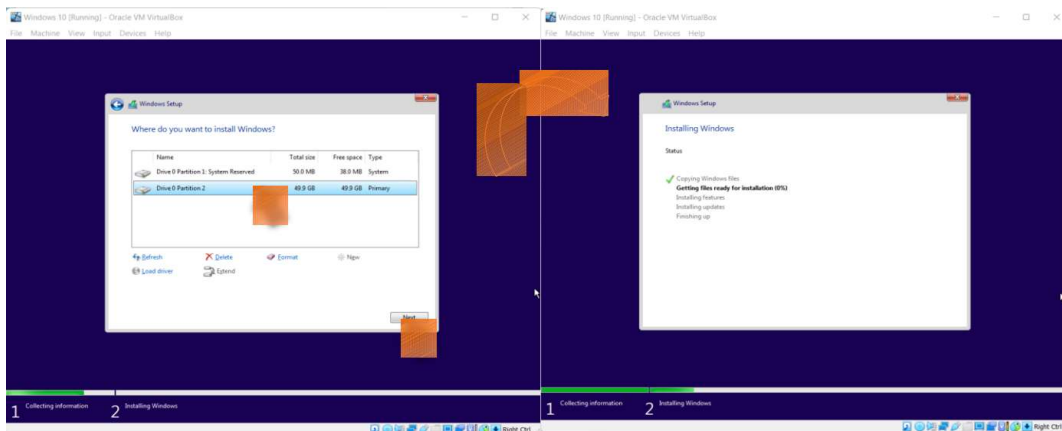


Windows pop will appear. Click “OK”



Click on Partition 2 and then click “Next”

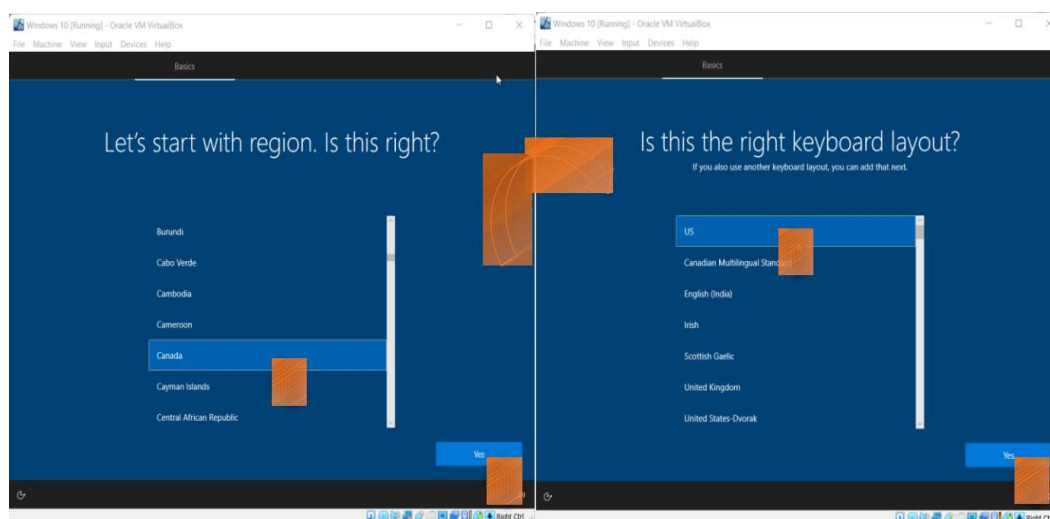
Windows installation will start.



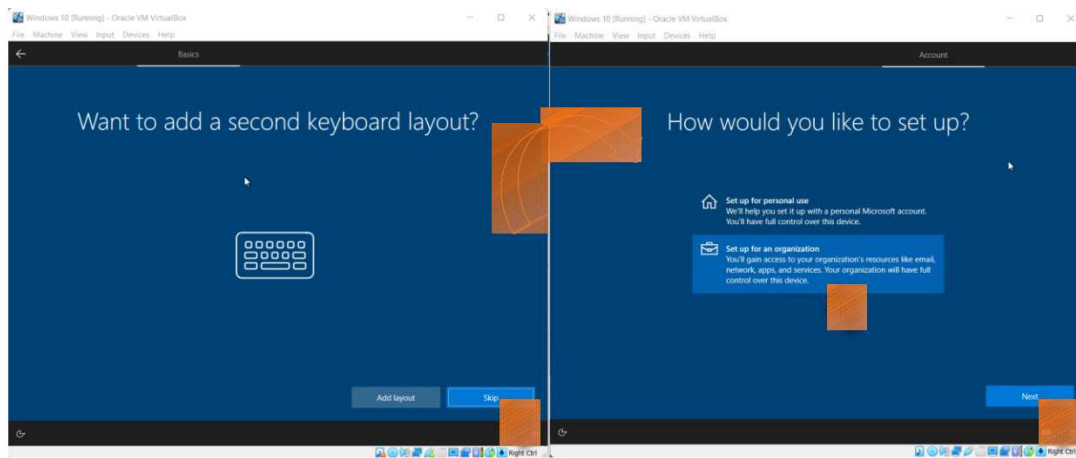
Once done, it'll reboot.

Select the desired region and click “Yes”

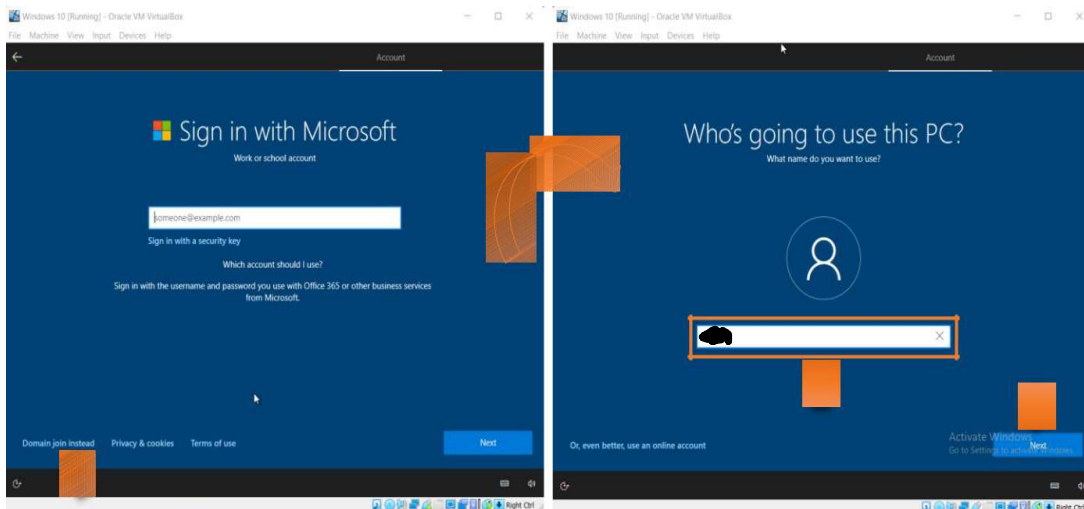
Select the right keyboard layout and click “Yes”



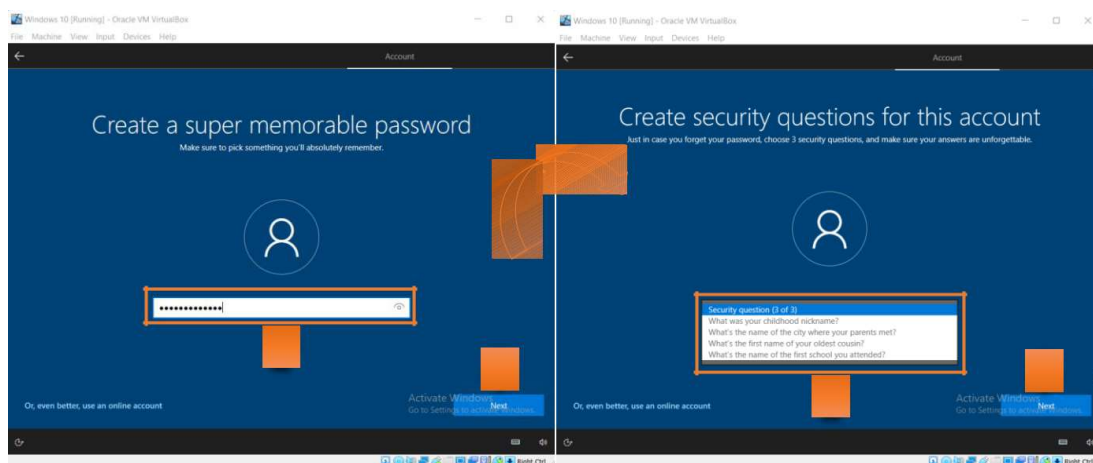
## Complete the optional items on next screens



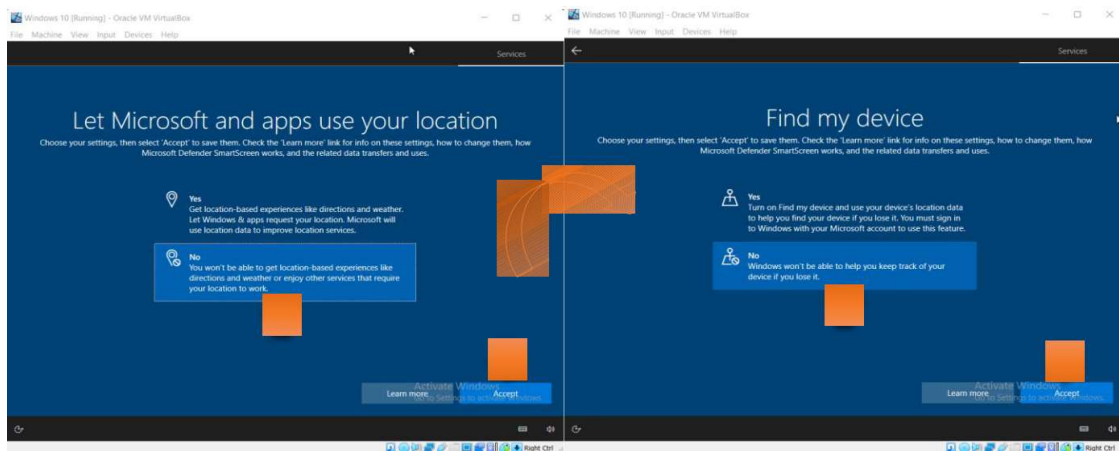
Select "Domain join instead" for offline account. Enter the default username.



Create a new password. Choose questions and answer for security.



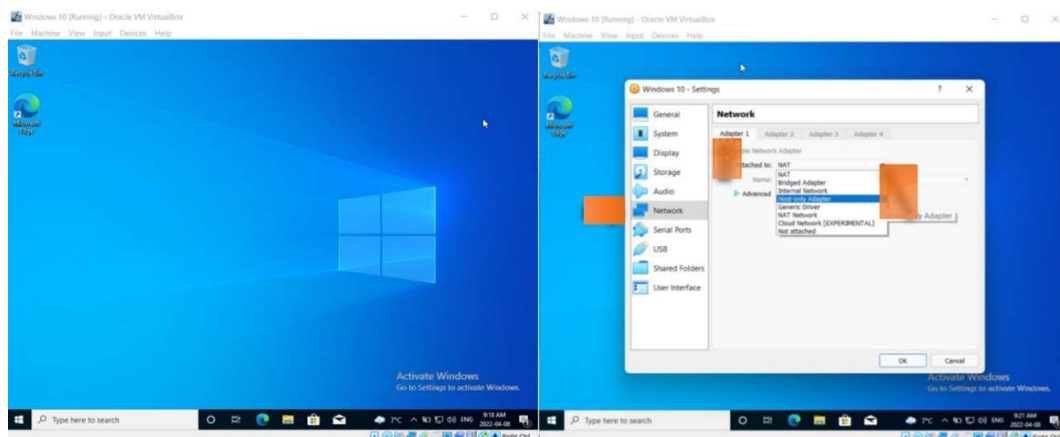
## Deny all features for optimal OC work



Once completed it'll show you the Welcome screen. Windows 10 installation is completed.

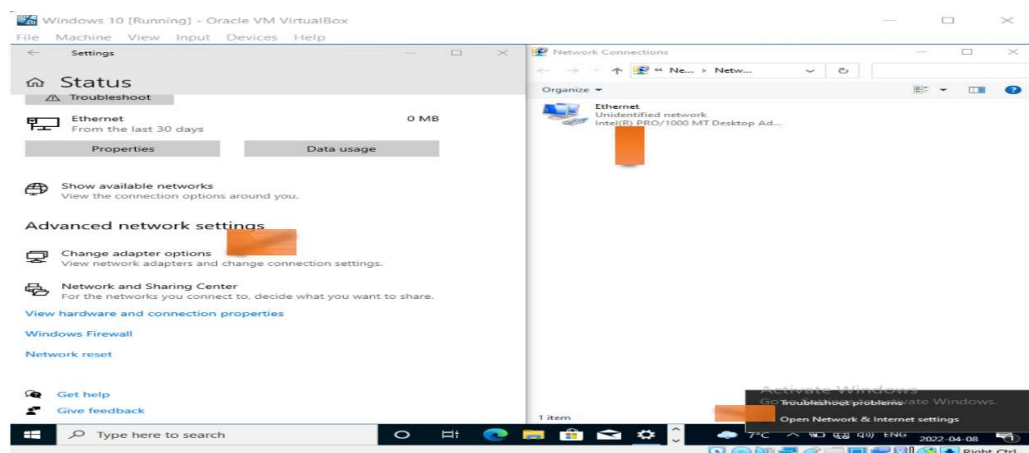
Windows 10 will appear under Machine. Click "Settings" button. Select Network.

Under Adapter 1, go to "Attached to" option and from drop down box select "Host-only Adapter"



Right click on small monitor icon on right bottom side of screen, beside clock. Select "Open Network and Sharing Center".

Network and Sharing Center screen will appear. Click "Change adapter options". Click "Ethernet"



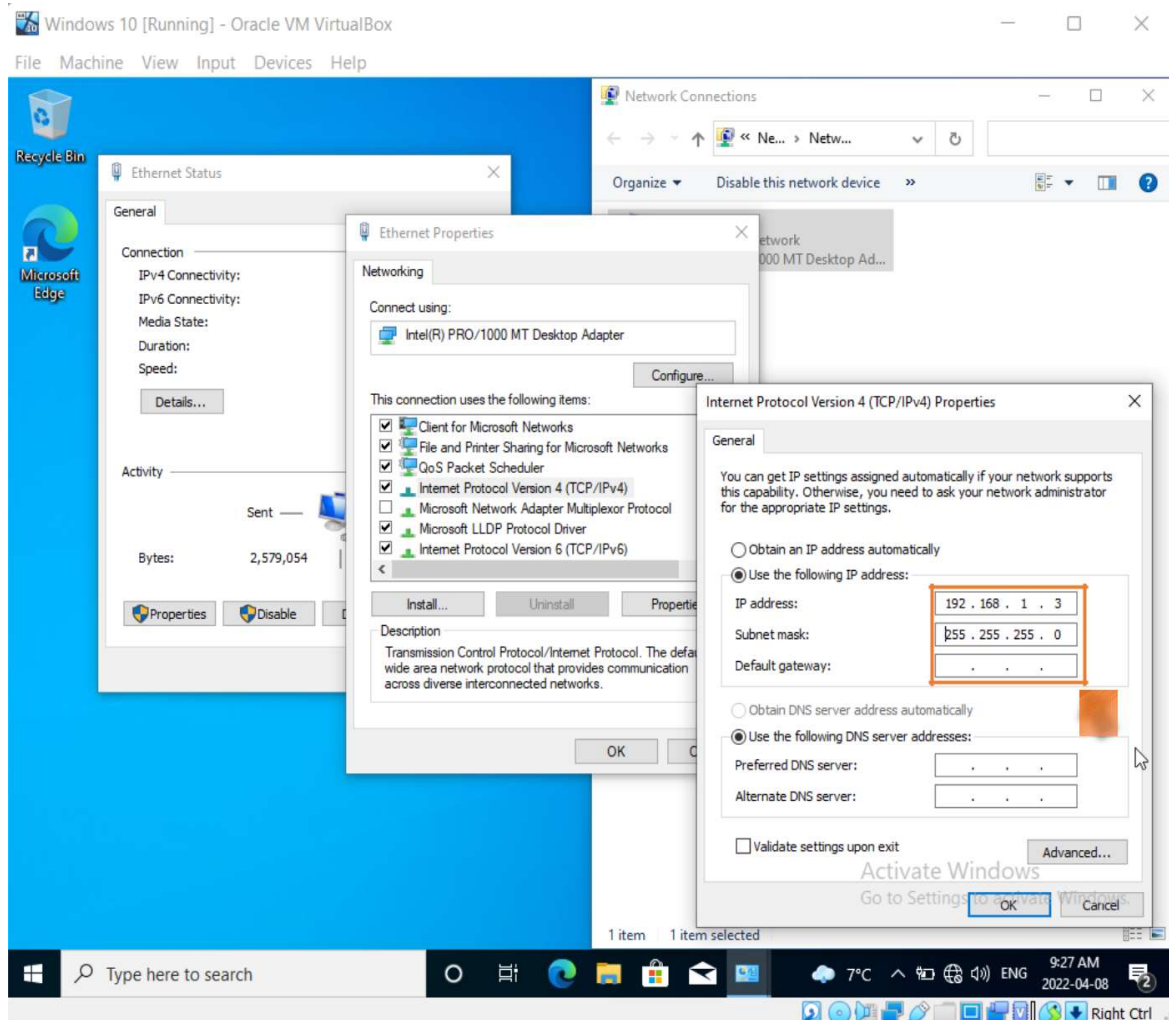
Ethernet Status screen will popup. Click "Properties" button.

Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".

Select "Use the following IP address:" radio button and fill in the required information.

We used the following information. Click "OK".

Select "Close" on next 2 screens.



## 6. Active Directory (AD)

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

This data store, also known as the directory, contains information about Active Directory objects. These objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. For more information about the Active Directory data store, see [Directory data store](#).

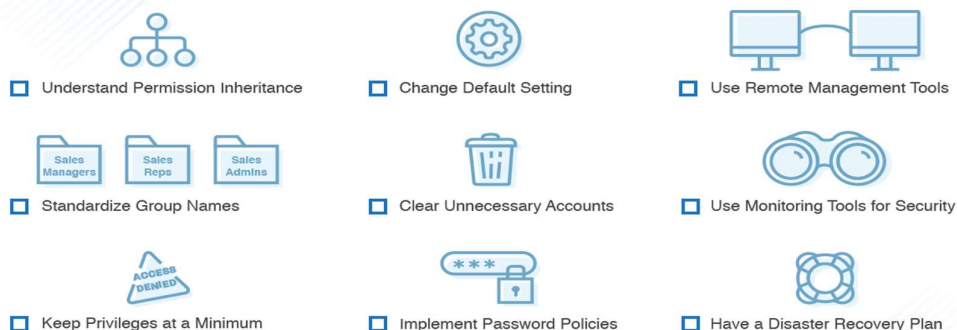
Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network. For more information about Active Directory security, see [Security overview](#).

### 6.1 Why do we need AD?

There are several benefits to using AD DS for your basic network user and computer management.

- You can customize how your data is organized to meet your companies needs
- You can manage AD DS from any computer on the network, if necessary
- AD DS provides built in replication and redundancy: if one Domain Controller (DC) fails, another DC picks up the load
- All access to network resources goes through AD DS, which keeps network access rights management centralized

### Active Directory Best Practices



Even if you don't know what Active Directory ("AD") is, you've probably seen it in action at some point in your career. You've also, perhaps wondered how specific tasks occur. There are many benefits to implanting Active Directory in your office, even if you don't think you are big enough to utilize it.

### **Company Security Policy Management**

Precisely, with Active Directory, employees must adhere to password security protocols. These include the complexity, length, and how often they must update their password within the system. By setting this at a system-wide level, you can be sure that it is happening, not just being an overlooked policy.

### **Ease of Computer Use**

Ever wondered how users can log in to any computer at an organization? Active Directory. When all the users are loaded, they have access to the network. Meaning, they can log into the conference room computer and find all their information without having to use USB drives to transport data. All the data is stored in one location and allows all devices registered to the network access to the files, based on the permission level you set.

### **Security Controls**

If you're tired of manually setting up files that some people have access to and others don't, "AD" is the solution for you! It allows you to stick people in groups and then apply the security access to the entire team, rather than just a single person at a time.

### **Protection**

When configured correctly, users only have access to data that is pertinent to them. What this means is your company files are more protected. People without access can't accidentally delete data they shouldn't. If a virus gets into a network, that virus (typically) won't be able to infect a file that it can't access.

### **Ease of Program Installs**

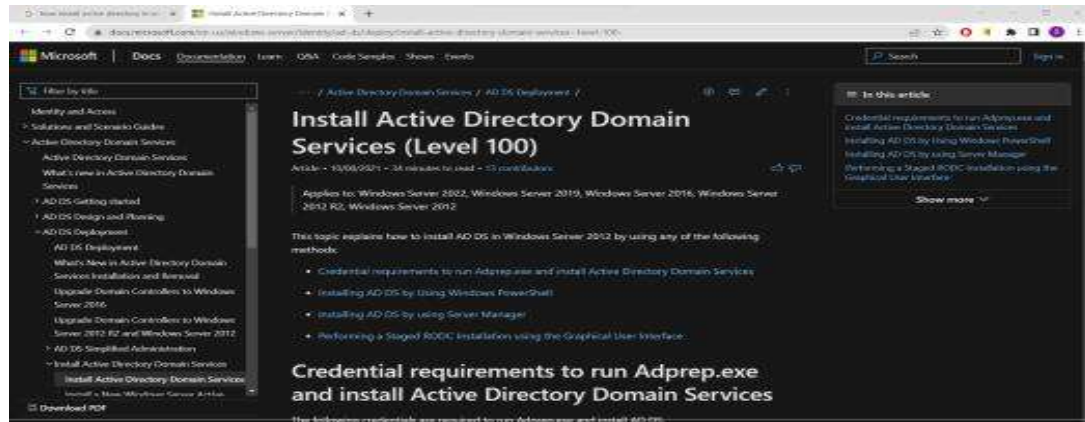
Instead of installing antivirus one-by-one on each computer, you can send that installation out via Active Directory. "AD" will keep your equipment protected without having to remember which machines got what programs.

### **Your Directory Transfers**

Smart all-in-one printers are great, except when you have to set them up. Active Directory speaks to the LDAP (Lightweight Directory Access Protocol) allowing your user's email addresses to be synced with your new printer so users can quickly scan to themselves.

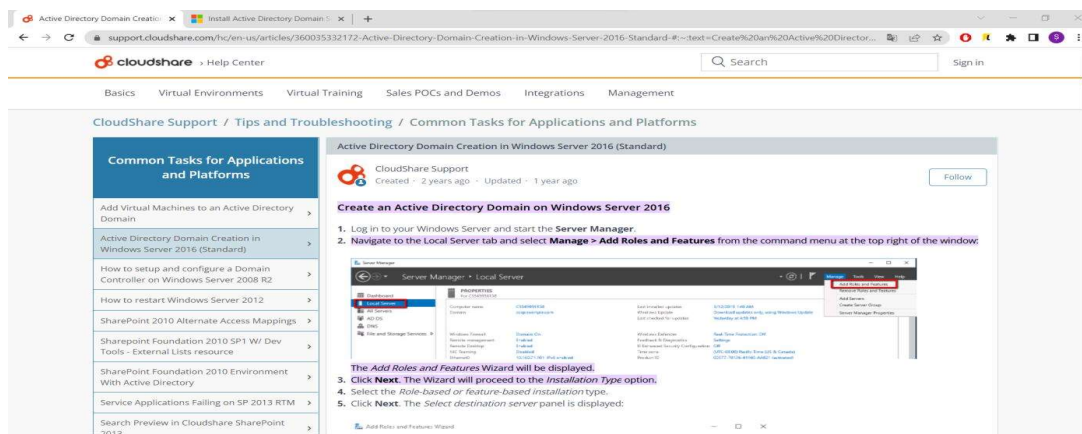
## 6.2 Active Directory setup

It initially informs you according to the official website <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100->



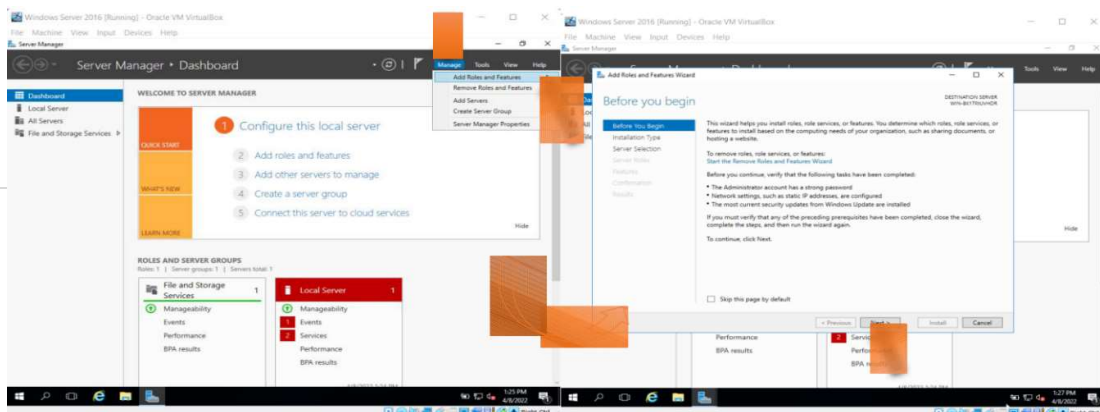
Informs you about creating Active Directory Domain on Windows Server 2016

<https://support.cloudshare.com/hc/en-us/articles/360035332172-Active-Directory-Domain-Creation-in-Windows-Server-2016-Standard-#:~:text=Create%20an%20Active%20Directory%20Domain%20on%20Windows%20Server%202016&text=Navigate%20to%20the%20Local%20Server,to%20the%20Installation%20Type%20option.>



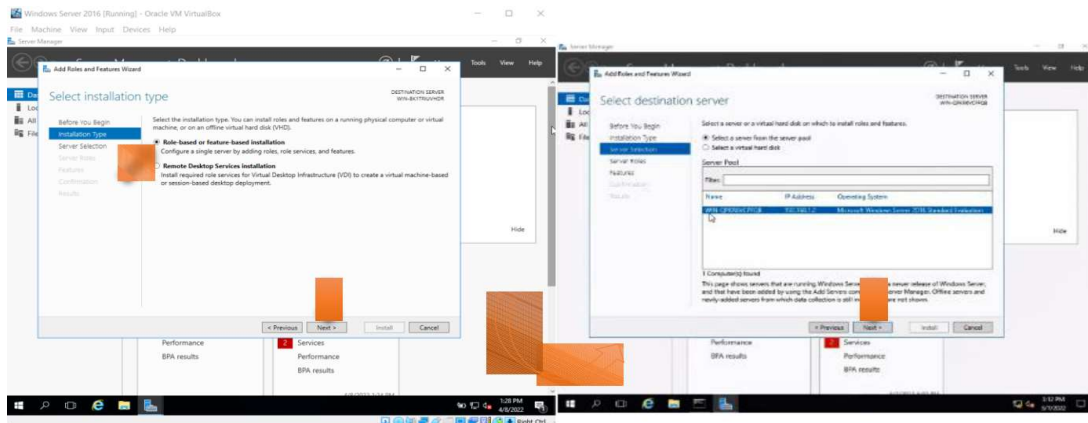
Go to Server Manager Dashboard. Click on “Add roles and features”.

Click “Next” to continue next screen.

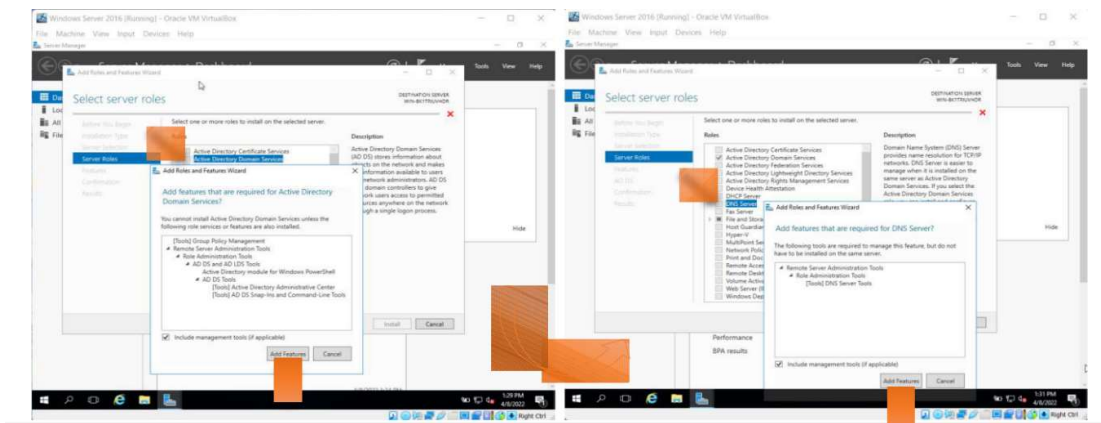


Select “Role-based or feature-based installation” radio button and click “Next”.

Select the server you installed in previous slides. Click “Next”

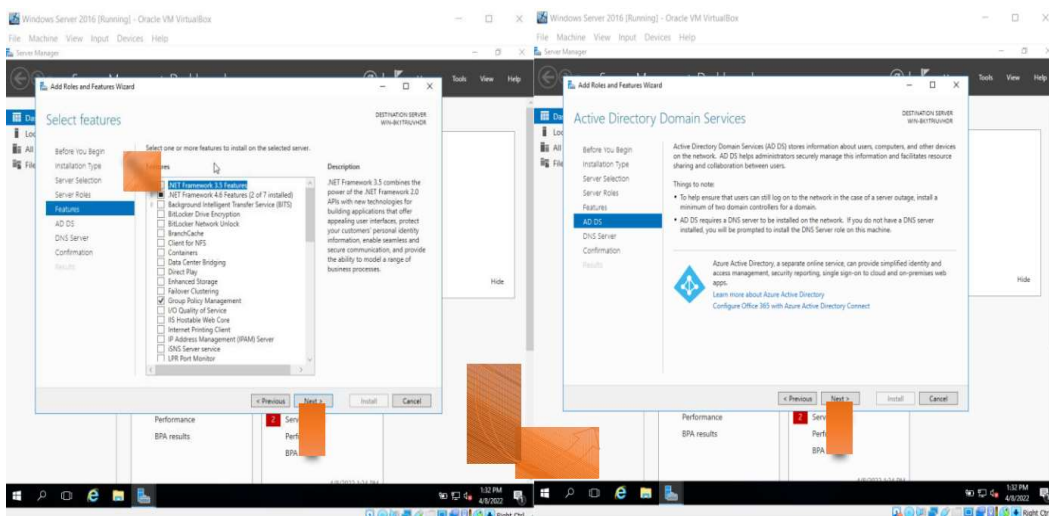


Select “Active Directory Domain Services” and “DNS Server” from the list. Click “Add Features”.

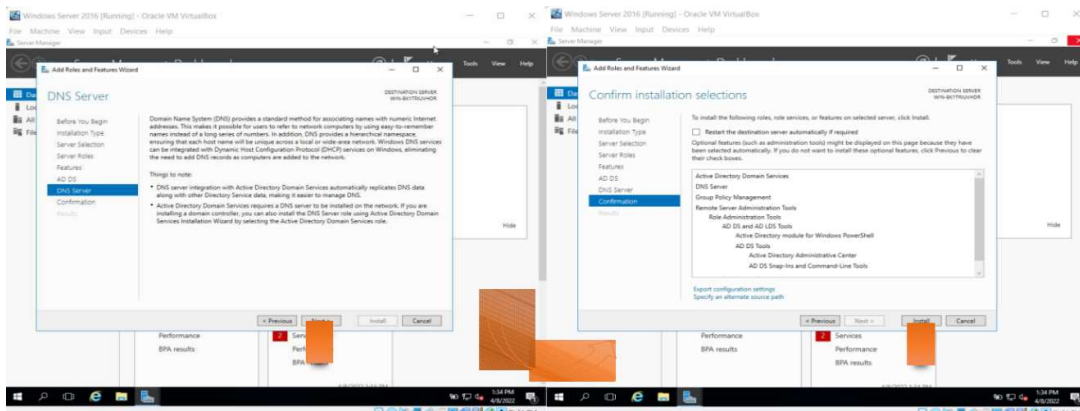


Next is to select features. Make sure.

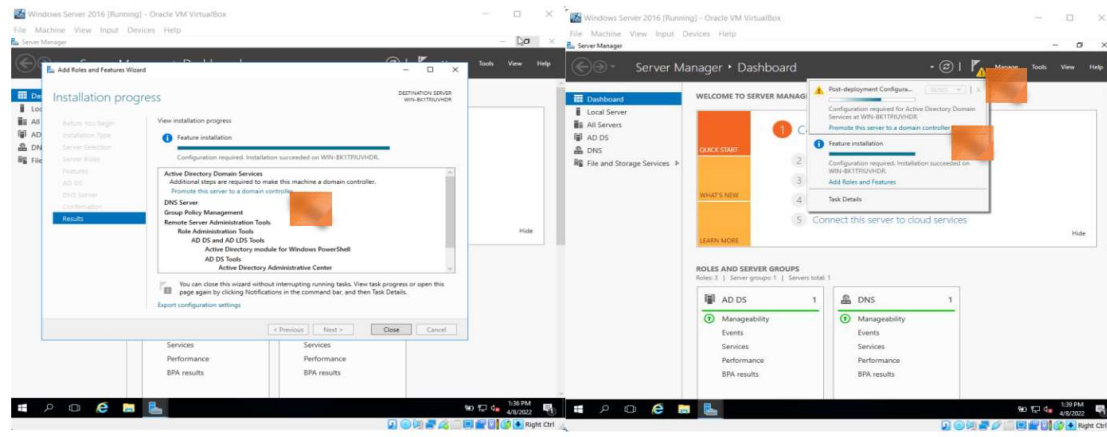
Net Framework check box should be BOLD. Click “Next” Click “Next” to confirm AD Domain Services.



Click “Next” to confirm DNS Server. Click “Install” to begin AD installation.

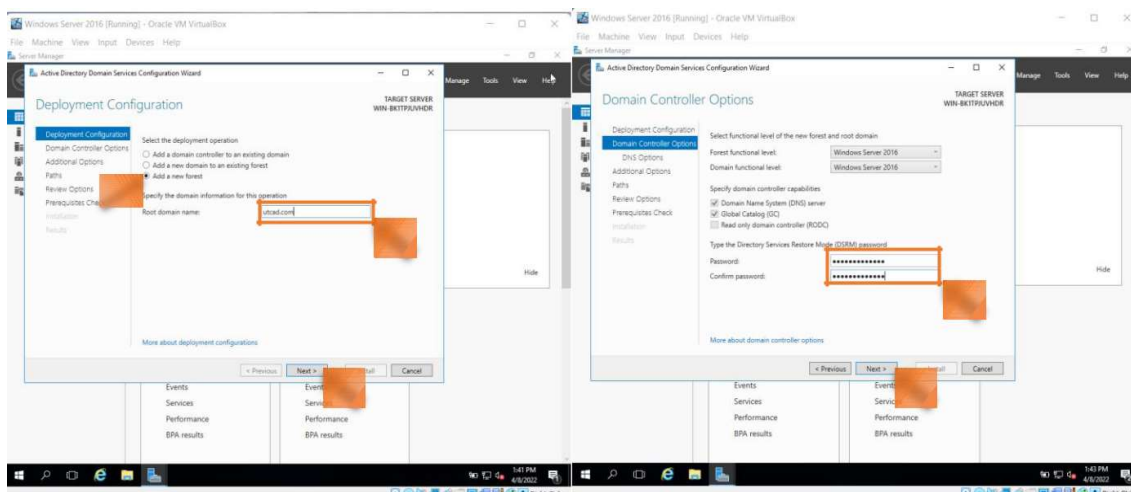


Once completed, it'll show Installation succeeded. Click “Promote this server to a domain controller”.

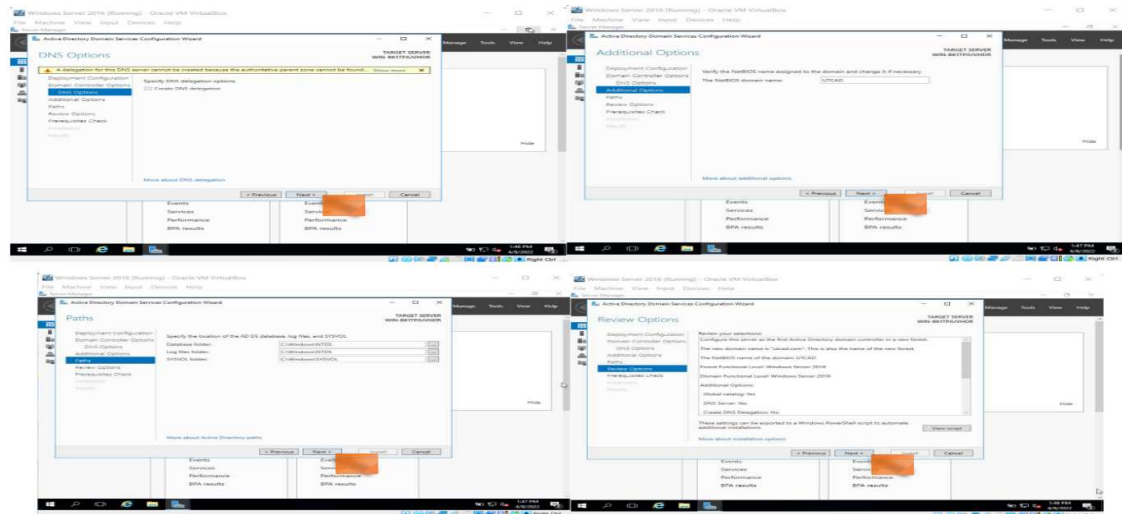


A new Deployment Configuration Window will open. Select “Add a new forest” radio button and put in Root domain name. It could be any name which you like to use. Click “Next”

Leave all default option. Type in a new DSRM password. Remember this is not the administrator password. This is to recover the Directory Services. Click “Next”

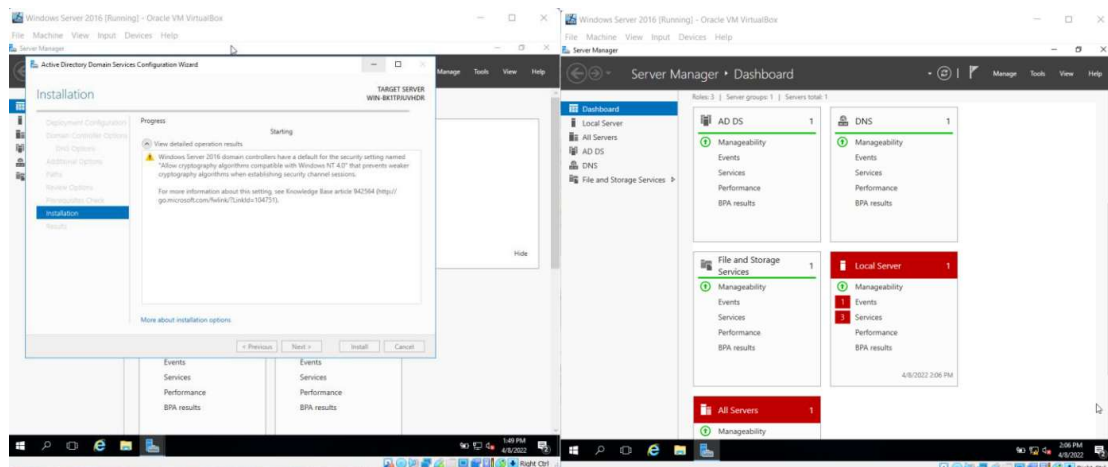


Leave default values on DNS Options and click “Next”. Click “Next” on next 3 screens leaving default values.



Click “Install” to begin deployment.

Once completed a restart warning will popup. Click Close. Server will reboot.

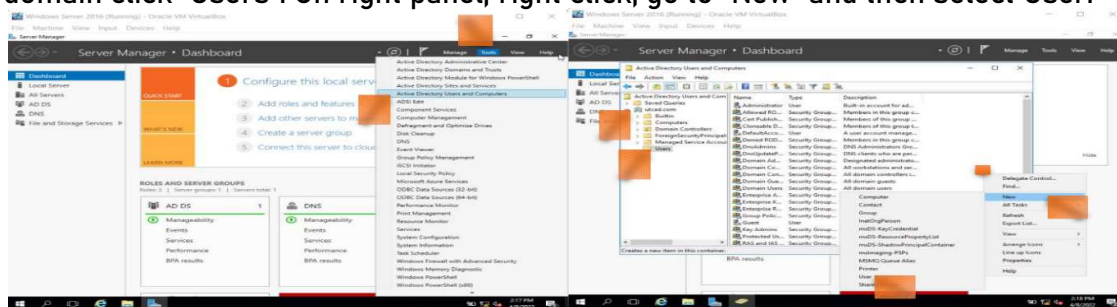


## 6.3 Creating a new user in Active Directory

Let's create a new user on AD. Open Server Manager Dashboard. Click “Tools” on top right corner and select “Active Directory Users and Computers”.

In left Panel, select your newly created Domain.

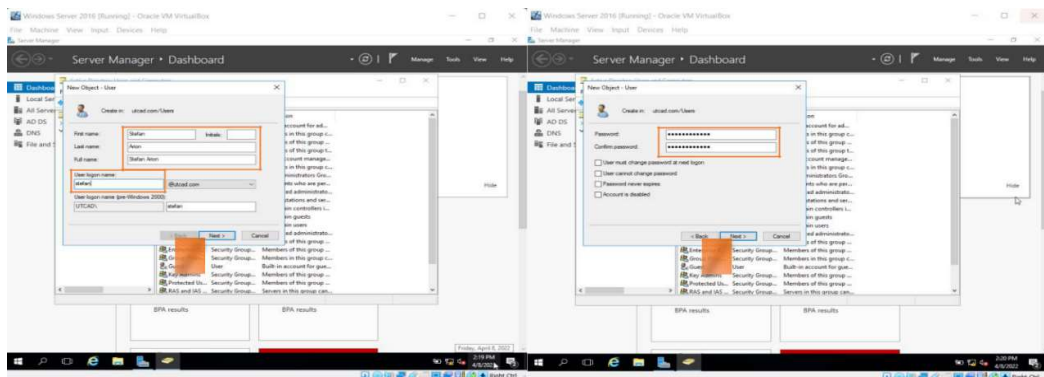
Under domain click “Users”. On right panel, right click, go to “New” and then select User.



A new popup will appear. Fill in the details and click “Next”.

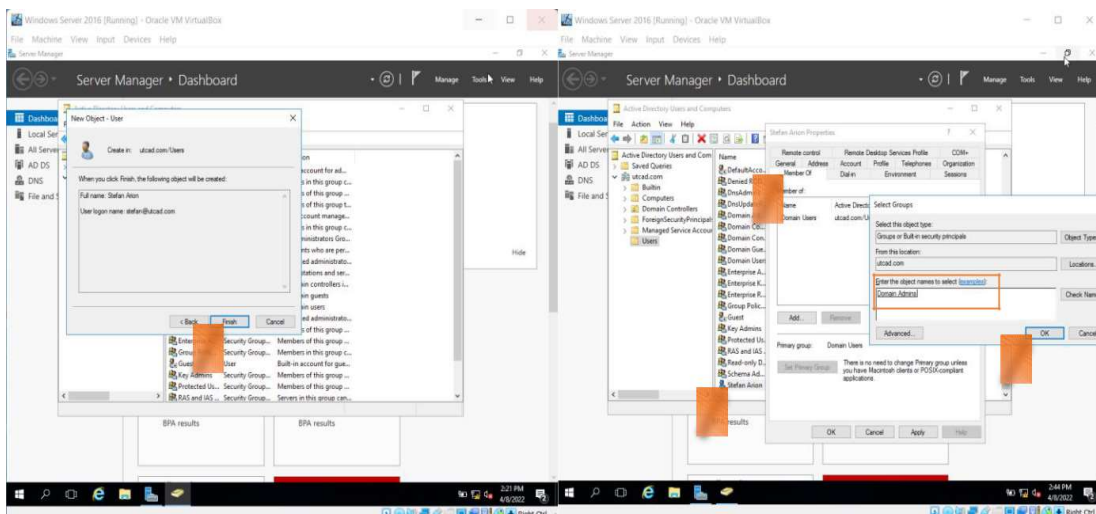
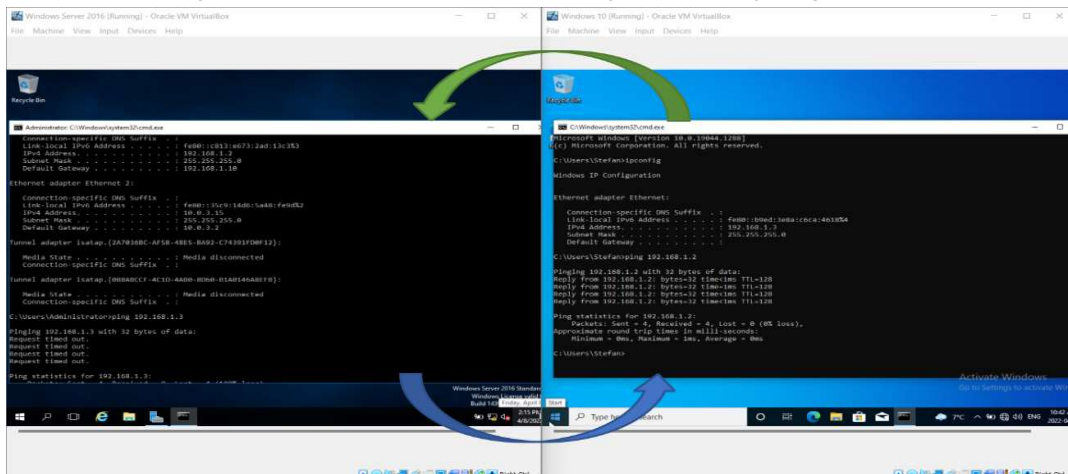
Create a new password for that user. Select the desired boxes as per your policies.

Just for the sake of lab, we didn't select any option. Click “Next”.



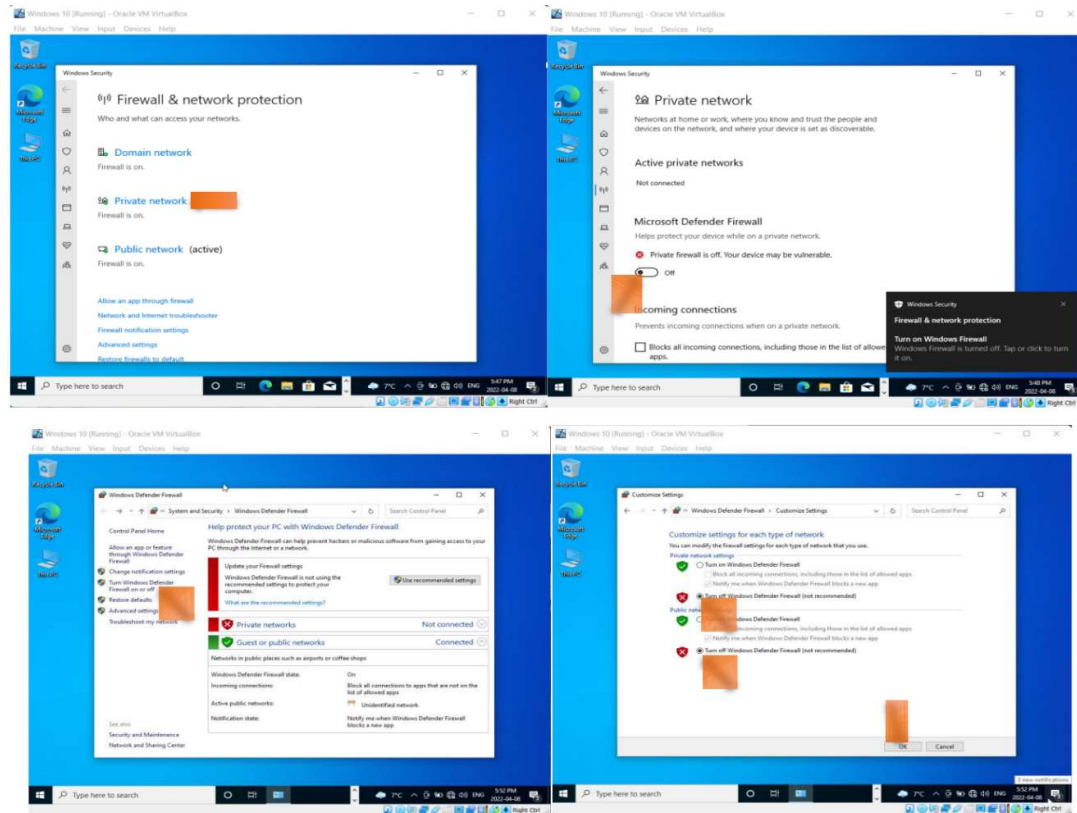
Click “Finish”. Your new user has been created.

In the "member of" option, enter the name of the object in the group. "Domain Admins"

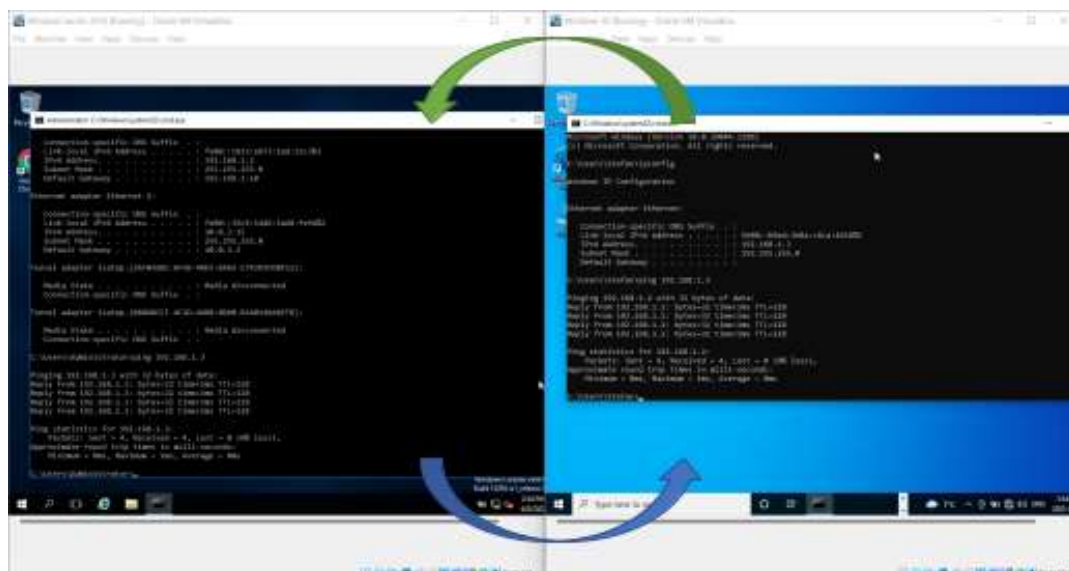


Then activate both virtual machines and access the command line. Enter the "Ping" command from server to client at 192.168.1.3. Then from client to server at 192.168.1.2. We notice that we cannot access the data packets from the client. The internal firewall installed in the client blocks access from foreign sources. Must be disabled

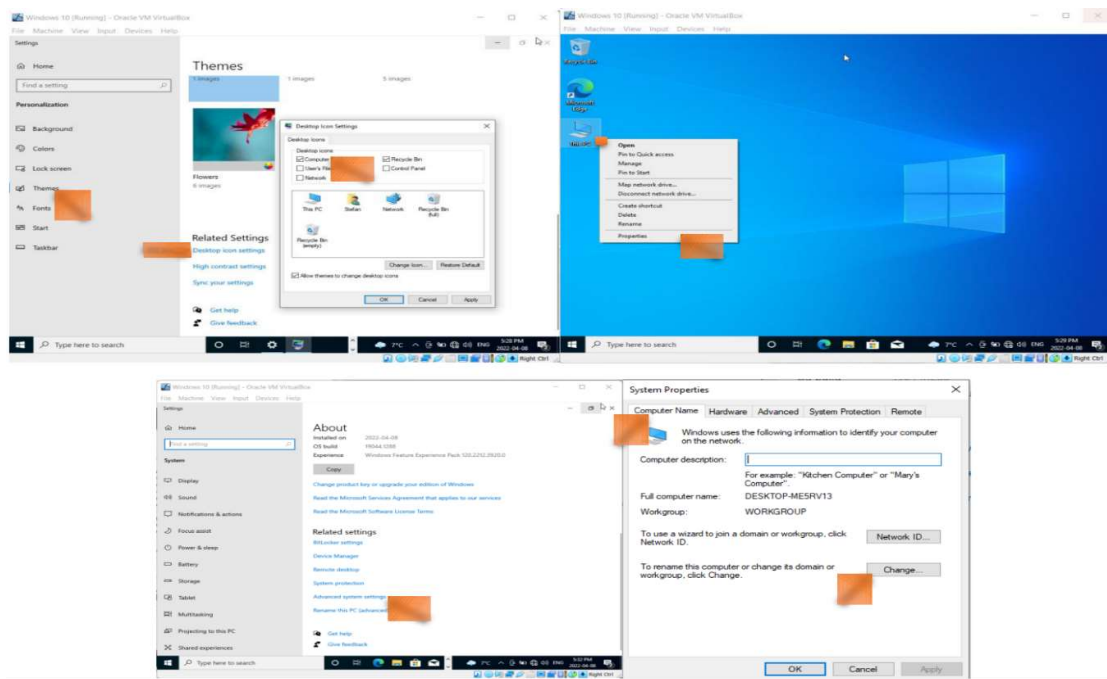
Search for Firewall on client. in our case it is Windows 10. And we disconnect the firewall



Check the transfer and reception correspondence between the server and the client. You notice that the packets are sent and received successfully. The result is that the connection is accessed.



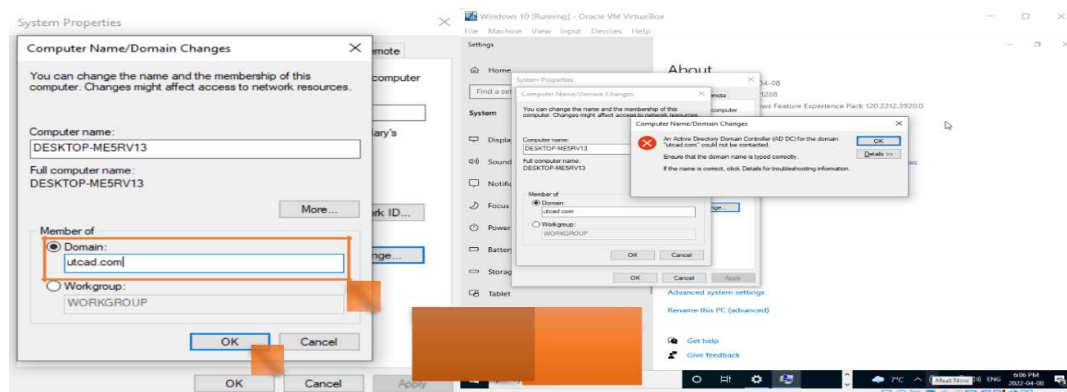
We hang the "This PC" icon on the desktop for quick access to the properties.



Change the "Computer name:" to some meaningful name.

Click on "Domain" radio button and put in your domain name.

Click "OK". Error appears! We do not have access to the domain...



In the command line we send the "ping" command to the domain name.

Domain is not recognized because we do not have access to the Domain Name System (DNS).



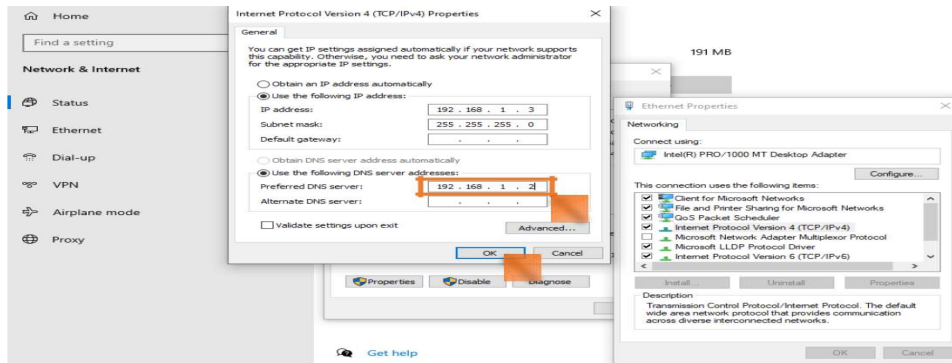
Ethernet Status screen will popup. Click "Properties" button.

Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".

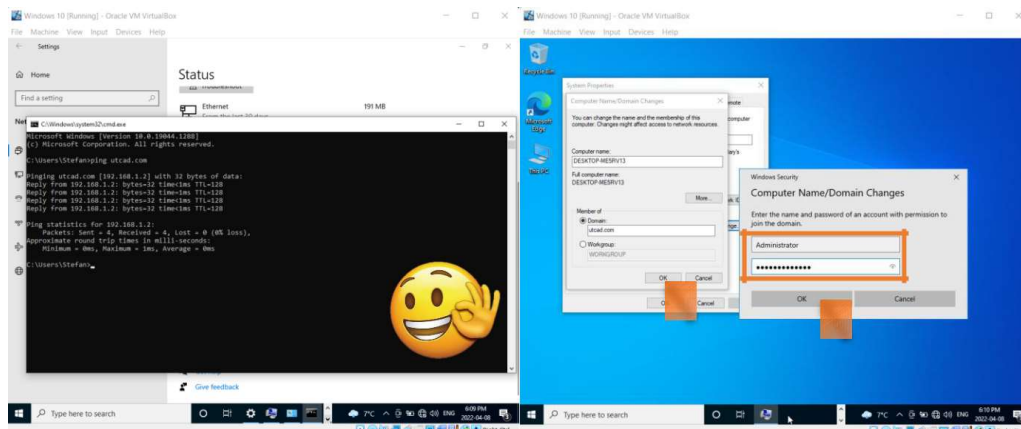
Select "Use the following IP address:"

Radio button and fill in the required information.

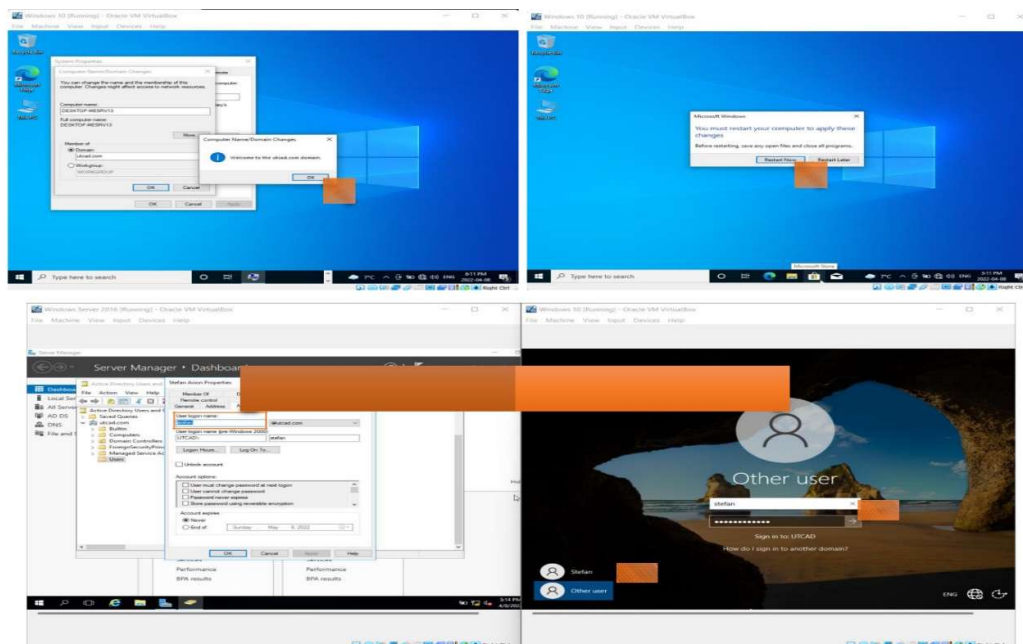
We used the following information. Click "OK". Select "Close" on next 2 screens.



Click "OK". Enter the domain access password, the server.



Welcome domain popup will appear. You might need to reboot the PC. Log on Client.



## 7. Event Viewer

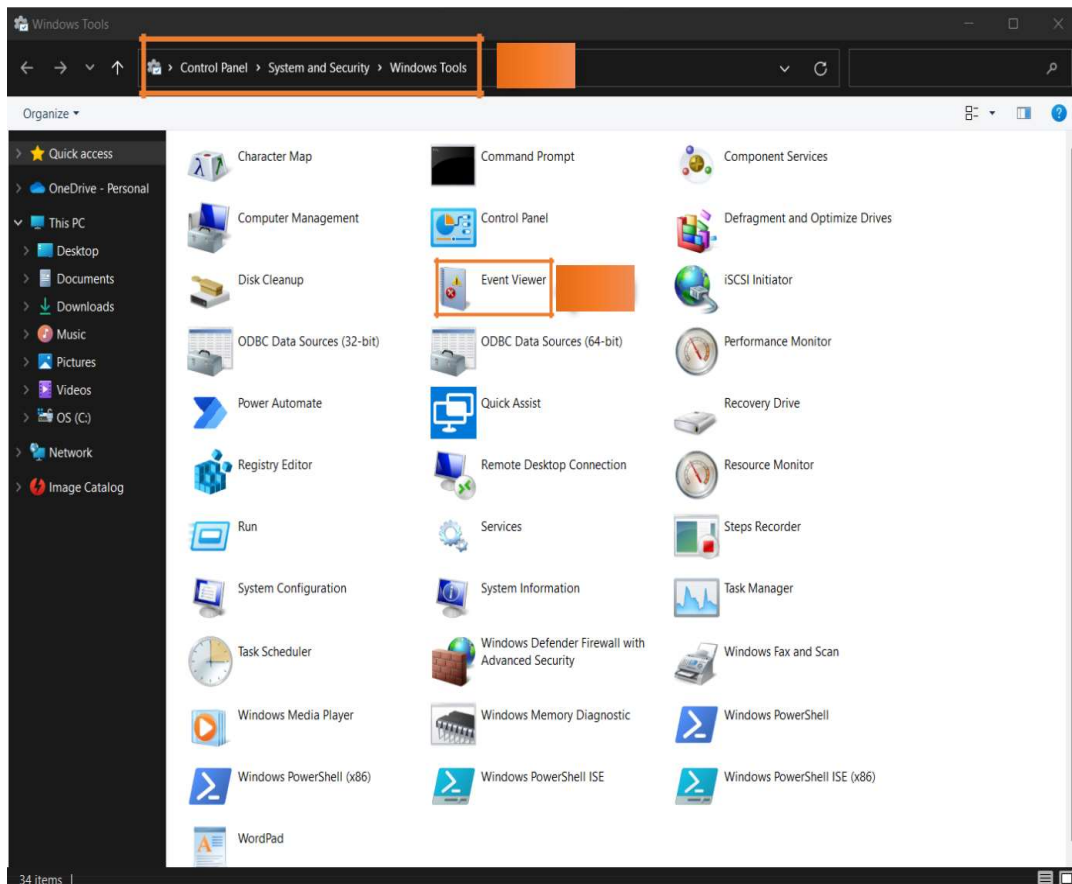
The Windows Event Viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems.

Note that even a properly functioning system will show various warnings and errors in the logs you can comb through with Event Viewer. Scammers even use this fact on occasion to deceive people into believing their system has a problem only the scammer can fix. In one infamous scam, a person claiming to be from Microsoft phones someone up and instructs them to open the Event Viewer. The person is sure to see error messages here, and the scammer will ask for the person's credit card number to fix them.

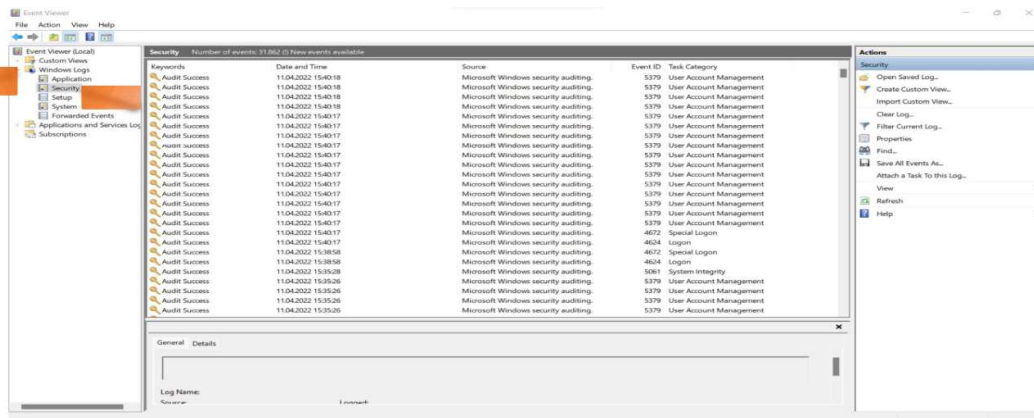
As a rule of thumb, assuming your PC is working properly, you can pretty much ignore the errors and warnings that appear in the Event Viewer. That said, it's worth having a basic working knowledge of the tool and knowing when it can be useful to you.



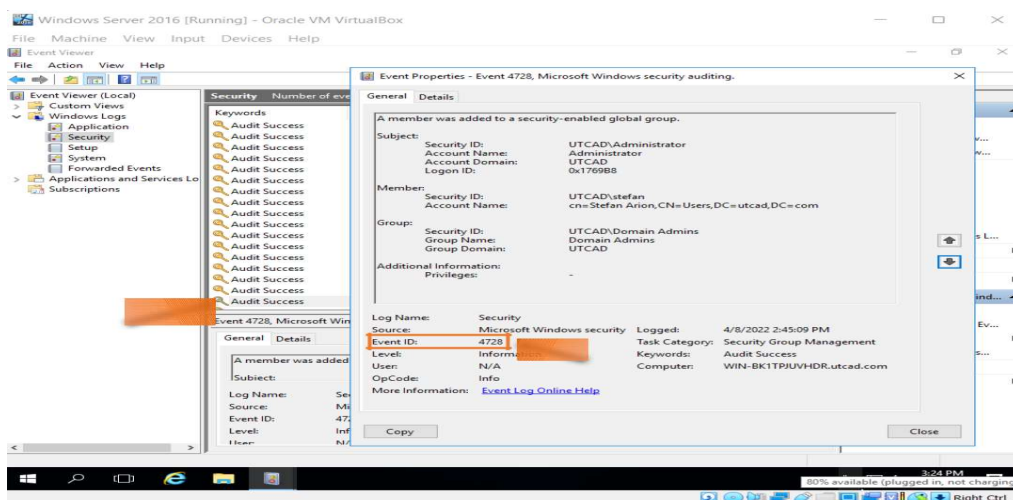
Open Control Panel and search for Windows Tool, then open Event Viewer. Or search for "Event Viewer"



## Access Windows Logs, and look at Security Logs



Next identify the Log IDs and their meaning. Depending on the ID, the user's activity can be seen in the description.

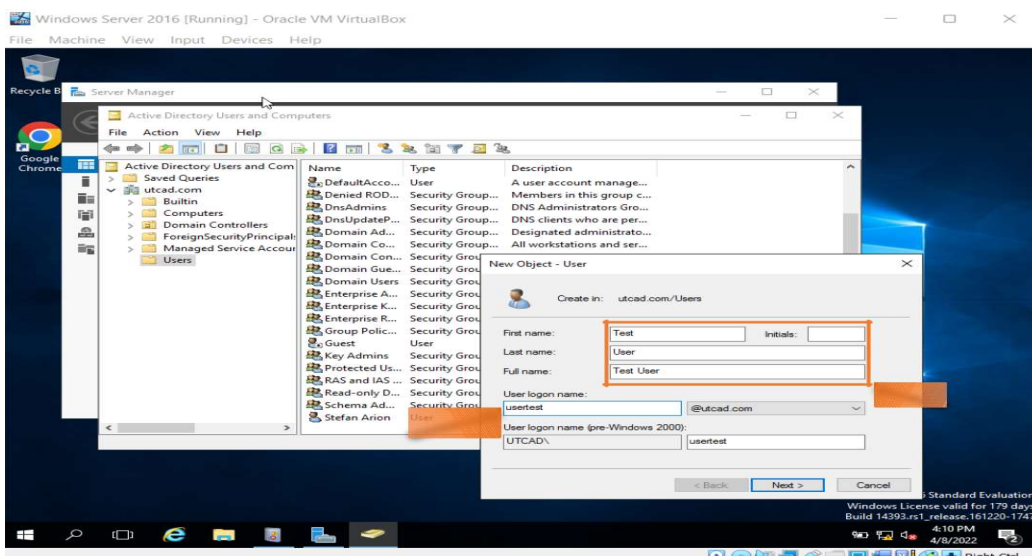


Let's create a new user on AD. Open Server Manager Dashboard.

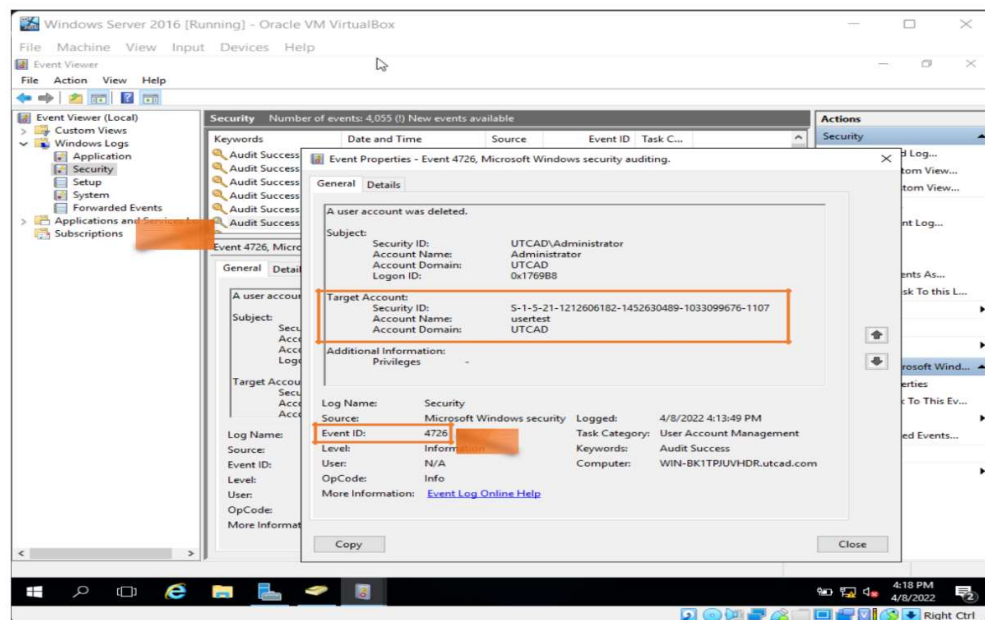
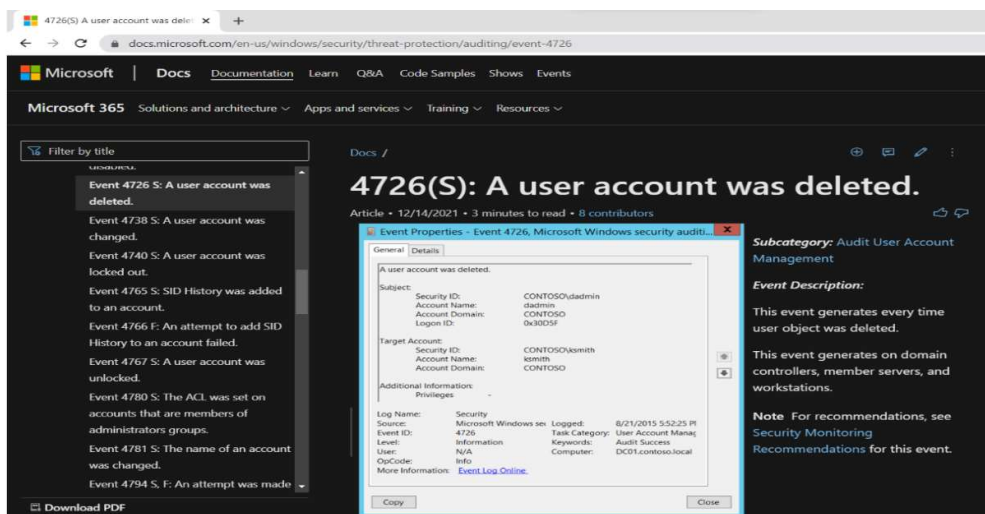
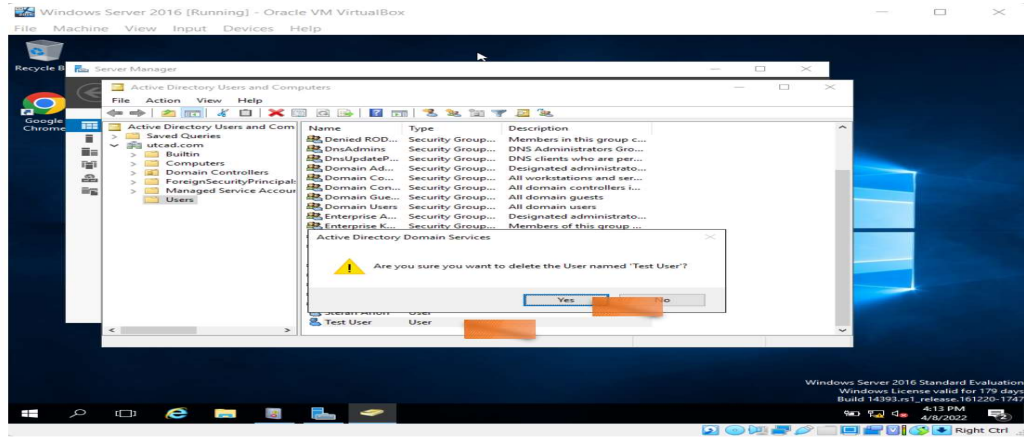
Click "Tools" on top right corner and select "Active Directory Users and Computers".

In left Panel, select your newly created Domain. Under domain click "Users".

On right panel, right click, go to "New" and then select User.



## Delete the created user



4720(S) A user account was created

docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720

Microsoft | Docs | Documentation | Learn | Q&A | Code Samples | Shows | Events

Microsoft 365 | Solutions and architecture | Apps and services | Training | Resources

Filter by title

- Event 4720(S): A user account was created.
- Event 4722 S: A user account was enabled.
- Event 4723 S, F: An attempt was made to change an account's password.
- Event 4724 S, F: An attempt was made to reset an account's password.
- Event 4725 S: A user account was disabled.
- Event 4726 S: A user account was deleted.
- Event 4738 S: A user account was changed.
- Event 4740 S: A user account was locked out.
- Event 4765 S: SID History was added to an account.

Download PDF

## 4720(S): A user account was created.

Article • 12/14/2021 • 18 minutes to read • 9 contributors

Event Properties - Event 4720, Microsoft Windows security auditing

General Details

A user account was created.

Subject:

- Security ID: CONTOSO\dadmin
- Account Name: dadmin
- Account Domain: CONTOSO
- Logon ID: 0x30DC2

New Account:

- Security ID: CONTOSO\ksmith
- Account Name: ksmith
- Account Domain: CONTOSO

Attributes:

- SAM Account Name: ksmith
- Display Name: Ken Smith
- User Principal Name: ksmith@contoso.local
- Home Directory: -
- Home Drive: -
- Script Path: -
- Profile Path: -
- User Workstations: -
- Password Last Set: <never>
- Account Expires: <never>
- Primary Group ID: 513
- Allowed To Delegate To: -
- Old UAC Value: 0x0
- New UAC Value: 0x15
- User Account Control: Account Disabled

Subcategory: Audit User Account Management

Event Description:

This event generates every time a new user object is created.

This event generates on domain controllers, member servers, and workstations.

Note For recommendations, see [Security Monitoring Recommendations](#) for this event.

Windows Server 2016 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
  - Applications and Services Logs

Security Number of events

- Audit Success 4
- Audit Success 4
- Audit Success 4
- Audit Success 4
- Audit Success 4
- Audit Success 4

Event 4720, Microsoft Windows security auditing

General Details

A user account was created.

Subject:

- Security ID: UTCAD\Administrator
- Account Name: Administrator
- Account Domain: UTCAD
- Logon ID: 0x1769B8

New Account:

- Security ID: S-1-5-21-1212606182-1452630489-1033099676-1107
- Account Name: userstest
- Account Domain: UTCAD

Attributes:

- SAM Account Name: userstest
- Display Name: Test User
- User Principal Name: userstest@utcad.com
- Home Directory: -
- Home Drive: -
- Script Path: -
- Profile Path: -
- User Workstations: -
- Password Last Set: <never>

Log Name: Security

Source: Microsoft Windows security

Event ID: 4720

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 4/8/2022 4:12:27 PM

Task Category: User Account Management

Keywords: Audit Success

Computer: WIN-BK1TPJUVHDR.utcad.com

Copy

Close

4:21 PM 4/8/2022

Right Ctrl

4625(F) An account failed to log on

docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625

Microsoft | Docs | Documentation | Learn | Q&A | Code Samples | Shows | Events

Microsoft 365 | Solutions and architecture | Apps and services | Training | Resources

Filter by title

Event 4625 F: An account failed to log on.

Audit User/Device Claims

Audit Group Membership

Audit IPsec Extended Mode

Audit IPsec Main Mode

Audit IPsec Quick Mode

Audit Logoff

Audit Logon

Audit Network Policy Server

Audit Other Logon/Logoff Events

Audit Special Logon

Audit Application Generated

Audit Certification Services

Audit Detailed File Share

Audit File Share

Audit File System

Download PDF

## 4625(F): An account failed to log on.

Article • 01/04/2022 • 13 minutes to read • 14 contributors

Event Properties - Event 4625, Microsoft Windows security auditing

General Details

An account failed to log on.

Subject:

|                 |         |
|-----------------|---------|
| Security ID:    | SYSTEM  |
| Account Name:   | DC01\$  |
| Account Domain: | CONTOSO |
| Logon ID:       | 0x3E7   |

Logon Type: 2

Account For Which Logon Failed:

|                 |          |
|-----------------|----------|
| Security ID:    | NULL SID |
| Account Name:   | Auditor  |
| Account Domain: | CONTOSO  |

Failure Information:

|                 |                     |
|-----------------|---------------------|
| Failure Reason: | Account locked out. |
| Status:         | 0xC0000234          |
| Sub Status:     | 0x0                 |

Process Information:

|                      |                                  |
|----------------------|----------------------------------|
| Caller Process ID:   | 0x1bc                            |
| Caller Process Name: | C:\Windows\System32\winlogon.exe |

Network Information:

|                         |           |
|-------------------------|-----------|
| Workstation Name:       | DC01      |
| Source Network Address: | 127.0.0.1 |
| Source Port:            | 0         |

Detailed Authentication Information:

Windows 10 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Event Viewer

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

|                 |                   |
|-----------------|-------------------|
| Security ID:    | SYSTEM            |
| Account Name:   | DESKTOP-MESRV13\$ |
| Account Domain: | UTCAD             |
| Logon ID:       | 0x3E7             |

Logon Type: 2

Account For Which Logon Failed:

|                 |          |
|-----------------|----------|
| Security ID:    | NULL SID |
| Account Name:   | stefan   |
| Account Domain: | UTCAD    |

Failure Information:

|                 |                                    |
|-----------------|------------------------------------|
| Failure Reason: | Unknown user name or bad password. |
| Status:         | 0xC000006D                         |
| Sub Status:     | 0xC000006A                         |

Process Information:

|                      |                                 |
|----------------------|---------------------------------|
| Caller Process ID:   | 0x3e0                           |
| Caller Process Name: | C:\Windows\System32\svchost.exe |

Network Information:

|                   |                 |
|-------------------|-----------------|
| Workstation Name: | DESKTOP-MESRV13 |
|-------------------|-----------------|

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 2022-04-08 4:34:00 PM

Task Category: Logon

Keywords: Audit Failure

Computer: DESKTOP-MESRV13.utcad.com

Type here to search

4:40 PM 2022-04-08

Right Ctrl

4624(S) An account was successfully logged on. x +

docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

Microsoft | Docs Documentation Learn Q&A Code Samples Shows Events

Microsoft 365 Solutions and architecture Apps and services Training Resources

Filter by title

- Event 4624 S: An account was successfully logged on.
- Event 4625 F: An account failed to log on.
- Event 4648 S: A logon was attempted using explicit credentials.
- Event 4675 S: SIDs were filtered.
- Audit Network Policy Server
- > Audit Other Logon/Logoff Events
- > Audit Special Logon
- Audit Application Generated
- Audit Certification Services
- > Audit Detailed File Share
- > Audit File Share
- > Audit File System
- > Audit Filtering Platform Connection
- > Audit Filtering Platform Packet Drop

Download PDF

## 4624(S): An account was successfully logged on.

Article • 12/14/2021 • 14 minutes to read • 13 contributors

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: SYSTEM
- Account Name: WIN-GG82ULGC9G0
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:

- Logon Type: 2
- Restricted Admin Mode: No
- Virtual Account: No
- Elevated Tokens: Yes

Impersonation Level: Impersonation

New Logons:

- Security ID: CONTOSO\Administrator
- Account Name: Administrator
- Account Domain: WIN-GG82ULGC9G0
- Logon ID: 0x4DCDC
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x44c
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: WIN-GG82ULGC9G0
- Source Network Address: 127.0.0.1
- Source Port: 0

Windows Server 2016 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

Account Name: stelan

Account Domain: UTCAD.COM

Logon ID: 0x31DAFA

Linked Logon ID: 0x0

Network Account Name: -

Network Account Domain: -

Logon GUID: {9ab928a4-cfd4-8aea-d87d-db13d1442cbb}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: 192.168.1.3
- Source Port: 49713

Detailed Authentication Information:

- Logon Process: Kerberos
- Authentication Package: Kerberos
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 4/8/2022 4:34:06 PM

Task Category: Logon

Keywords: Audit Success

Computer: WIN-BK1TPJUVHDR.utcad.com

Copy Close

## 8. Security Information & Event Management (SIEM)

### 8.1 SIM vs SEM vs SIEM

First, let's clear up some confusion about acronyms that you may come across. You may have come across SIM, SEM, and SIEM. SIM means Security Information Management; SEM means Security Event Management. Combine the two together, and we get SIEM Security Information and Event Management. So, what role do they play? Let's break their value down a little further.

Simply put, they refer to a type of tool that will store and process logs or event data. The quick difference is that SIM deals with storing log data for long term analysis, whereas SEM is concerned with live-action processing. Combined and you get one neat tool that deals with both, SIEM.

#### SIM

SIMs are tools or platforms used to collect and store all the security data that is logged within an organization. There is a considerable amount of data ranging across the entire IT platform. Depending on your technology choices and how well configured the collection process is, they would collect data from things such as:

- Web servers (if in house)
- Firewalls
- IDS and IPS logs
- Router information
- Terminal commands
- Changes to an employee's computer
- Antivirus logs
- DNS servers
- Authentication servers
- Database access

Basically, all the information from any software and how it's being used, including changes to the operating system. This could get very big very quickly! It is therefore not uncommon for collection to be a little more selective. All of these stored log's amount to far too much data for any human to process. Enter SEM.

#### SEM

These tools provide real-time analysis of all the SIM data with the added benefit of sending alerts about any security anomalies. Imagine combing and sorting through all the data listed above and then parsing it. This would then output to a console so that a human gets an alert to be investigated. This can be used to trip alerts, but also provide bigger picture insights into the network and trends. The console tends to have displays such as charts and pictorial representation of the data to make it easy for the network administrators to see what is happening. Log data can provide an invaluable insight into what attackers are doing on the network. The ability to analyse this data quickly as opposed to in 30 days, could make the difference between stopping an attacker quickly, or giving them significant dwell time in your network!

#### SIEM

Rather than having two separate tools that do practically the same thing, why not combine them into one platform? This is precisely what a SIEM does and has become quite the default. These

SIEM systems automate much of this process and come pre- packaged with rules and hows designed to make processing data and reacting to it mucheasier.

This integrated platform is useful to security but can also be very beneficial when auditors come and check how compliant the company has been. This is for things like Information Security management systems and ISO 27000 certificates. Demonstrating control over your logs and understanding of events in your network is key to such processes.

As mentioned, before you can process a huge volume of data with these systems. Simply imagine every endpoint streaming continuous log data about a given software update or configuration change! Retention policies to limit what matters and filtering rules that focus on the data of consequence is key, or data can become a gigantic monolith.

In most businesses there are typical things you want to log, so there are default setups to arrange collection for common technology or platforms. However, some configuration is often needed. SIEM tools do often come with a set of rules or triggers but customizing them for your environment is typically required. SIEM platforms are not just installed in the network, they can be cloud based too! In this setup you can benefit from management by a vendor, and continual software updates or features, but there can be a tradeoff of handing your event data to a third party.

These platforms include more and more clever techniques to react to data, and baselining with machine learning or heuristic mechanisms is finding more suspicious entries than ever before. In short, this means that if a hacker wants to get through the network, they will have to look like regular traffic.

A great SIEM setup will help organizations react to breaches, but also understand what happened and investigate retrospectively.

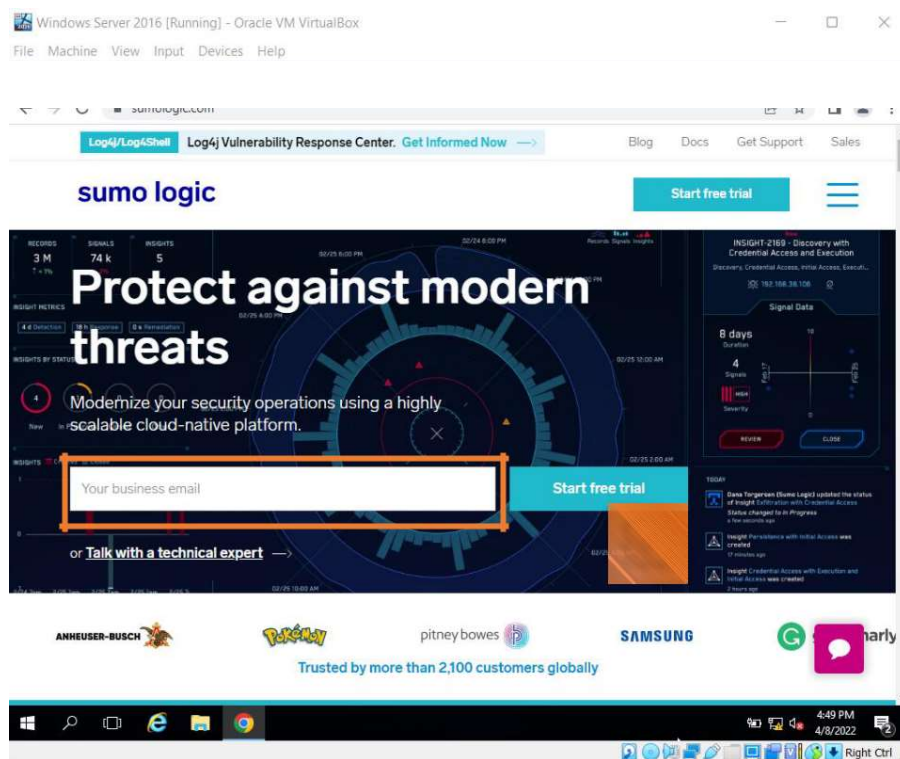
## 8.2 Setting up Sumo Logic

Sumo Logic is a cloud-based SaaS security platform that provides organizations continuous, real-time security intelligence essential for protecting modern network environments. Whereas traditional SIEM systems struggle to monitor and protect distributed cloud environments effectively, Sumo Logic was designed for scalability and built to cover rapidly expanding attack surfaces. The platform was built with modern IT environments in mind, including cloud infrastructure, tools, and modern application architectures.

Sumo Logic provides customizable dashboards used to display security metrics, performance data, and other key information across the network for a bird's-eye view into a company's network security efforts in real-time.

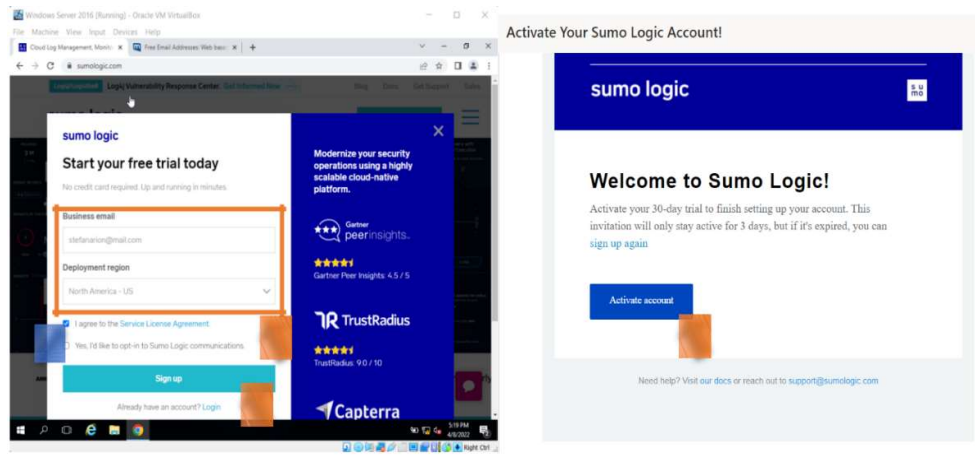


For this lab, first we need to register for the free trial. On your Windows server 2016, go to <https://www.sumologic.com/> and click on Start free trial.

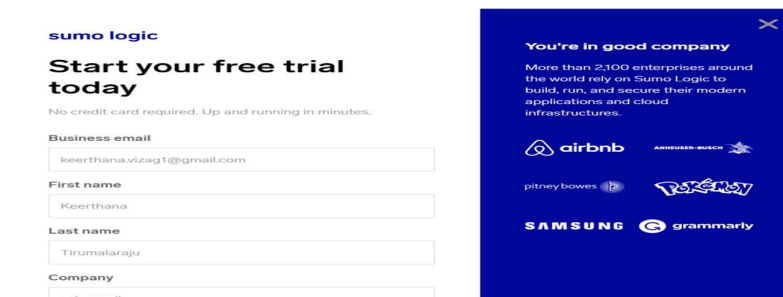


Put in your business email, select the region, select “I agree to the Service License Agreement”, and click sign up.

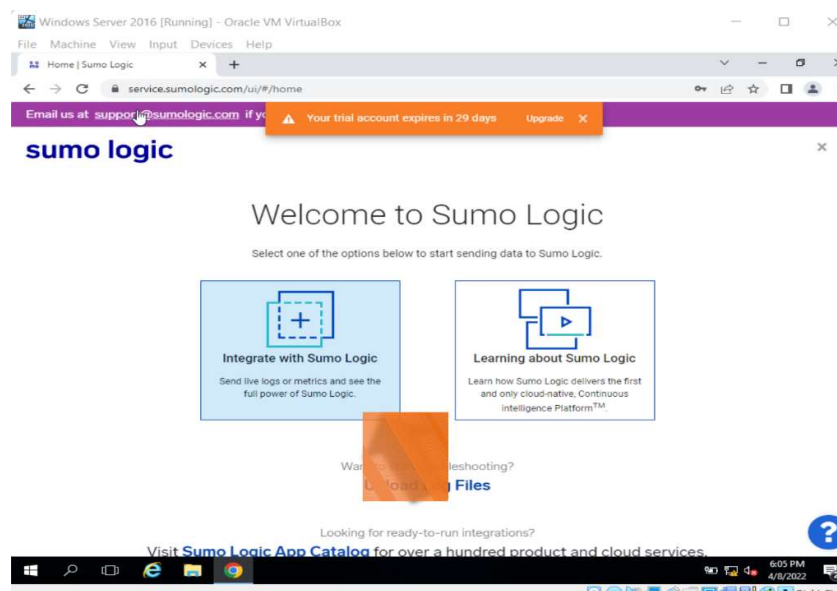
You'll receive an email with Activation. Click on “Activate account”



It'll ask you for some details. Put in all the required details and click “Activate”



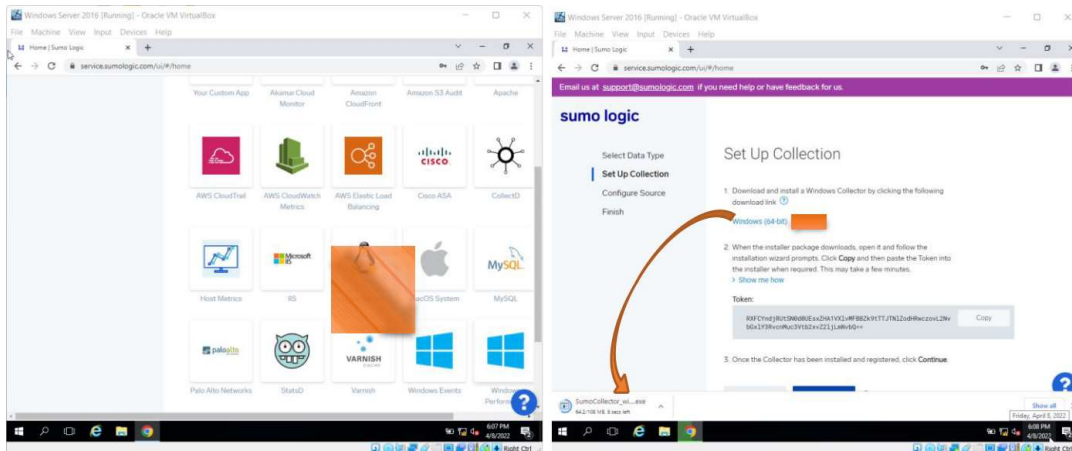
Click “Integrate with Sumo Logic”.



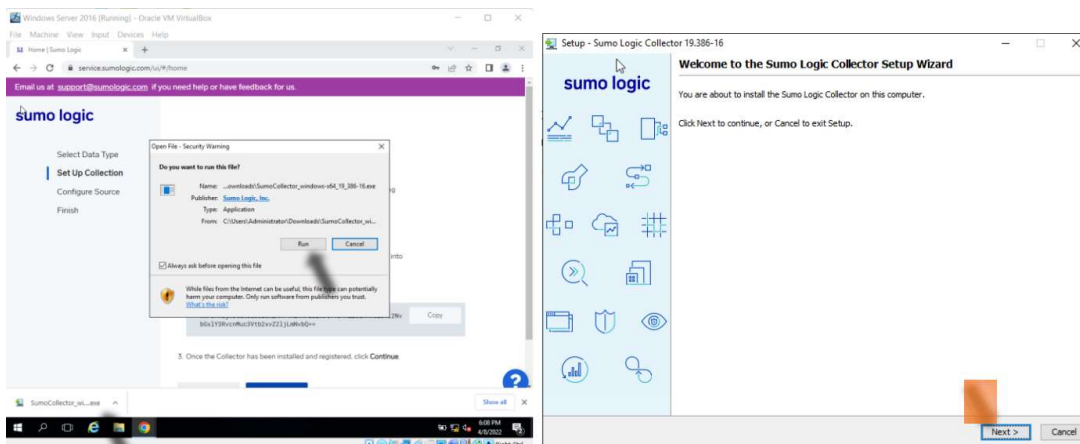
## 8.3 Downloading and Installing Sumo Logic Collector

At first setup, it provides a list of applications.

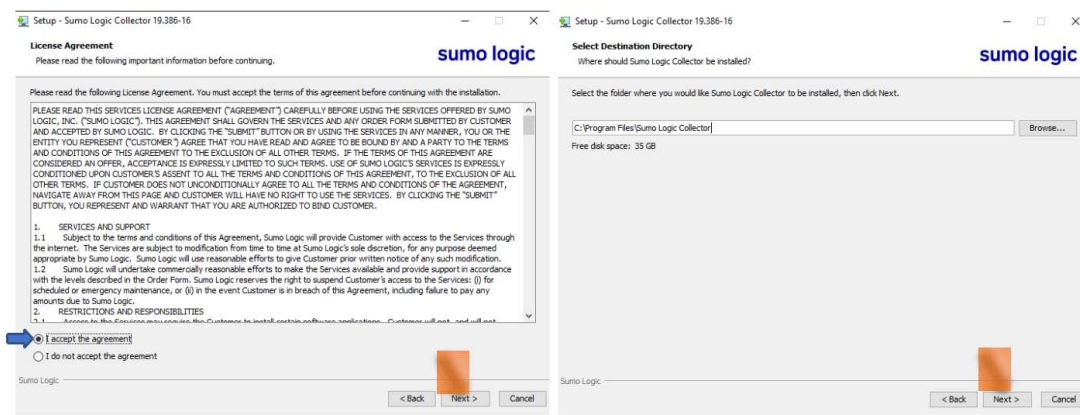
Select "Windows Events" Download and install the application following the steps below. Copy Token key.

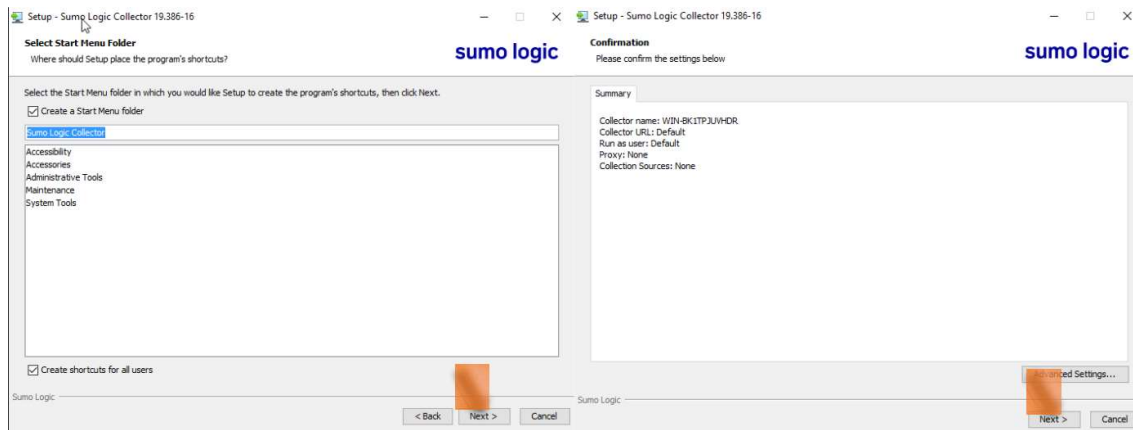


It'll start the Sumo Logic Collector setup. Click "Next"

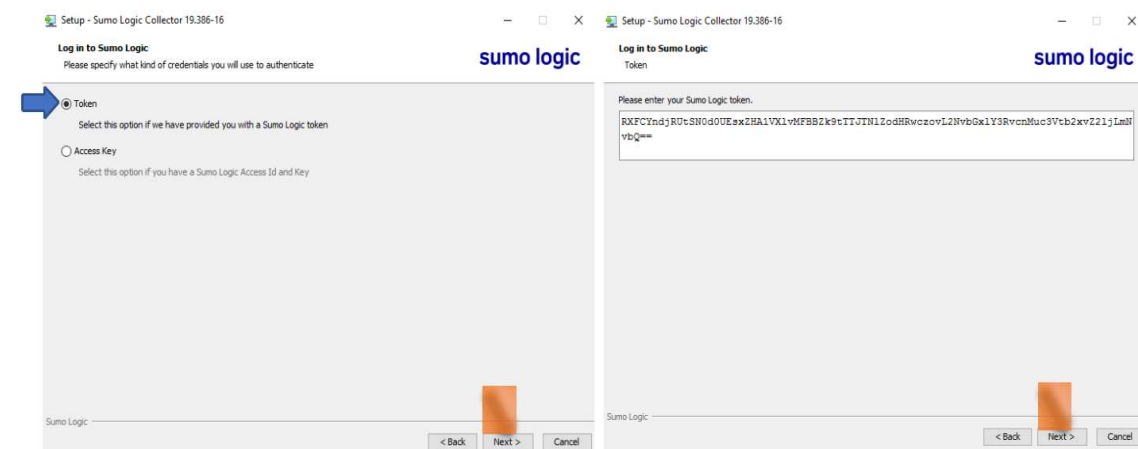
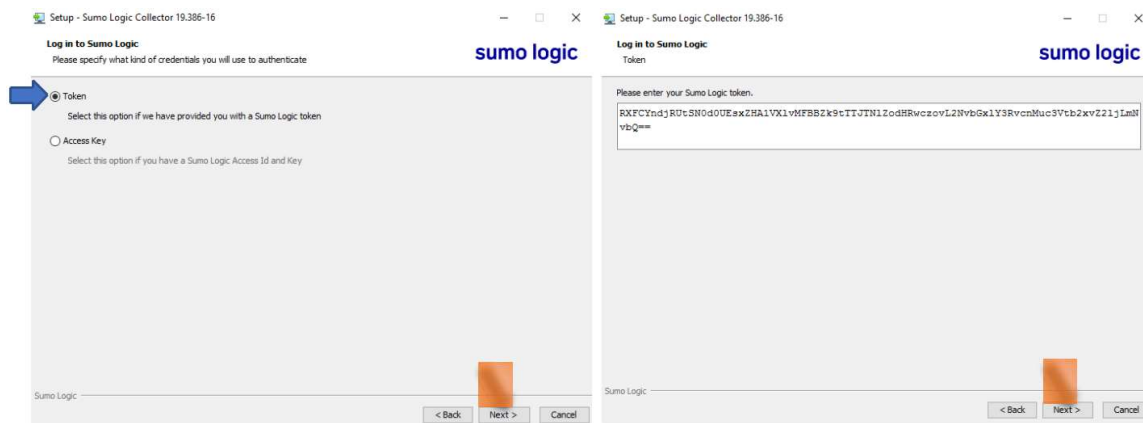


Select "I accept the agreement" and click "Next". Leave the default value on next two screens and select "Next >"



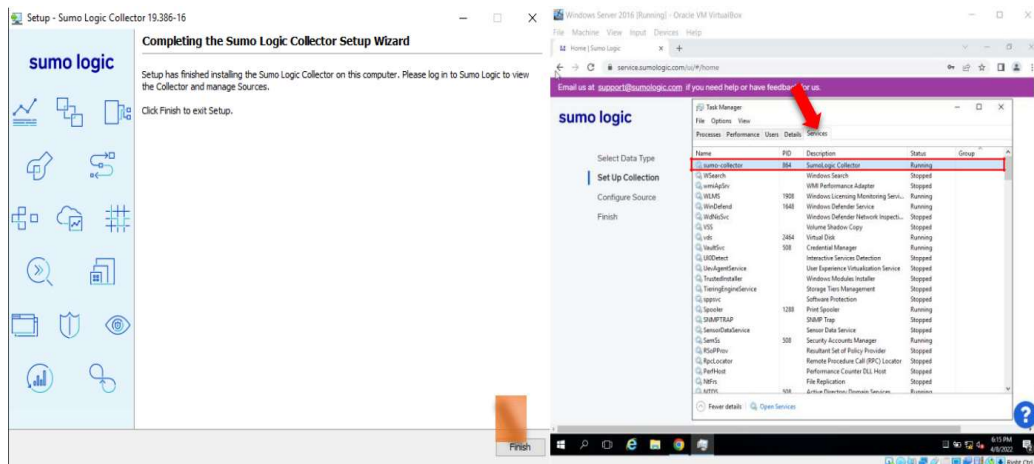


Select token and put pasta in the next window. Then click "next"

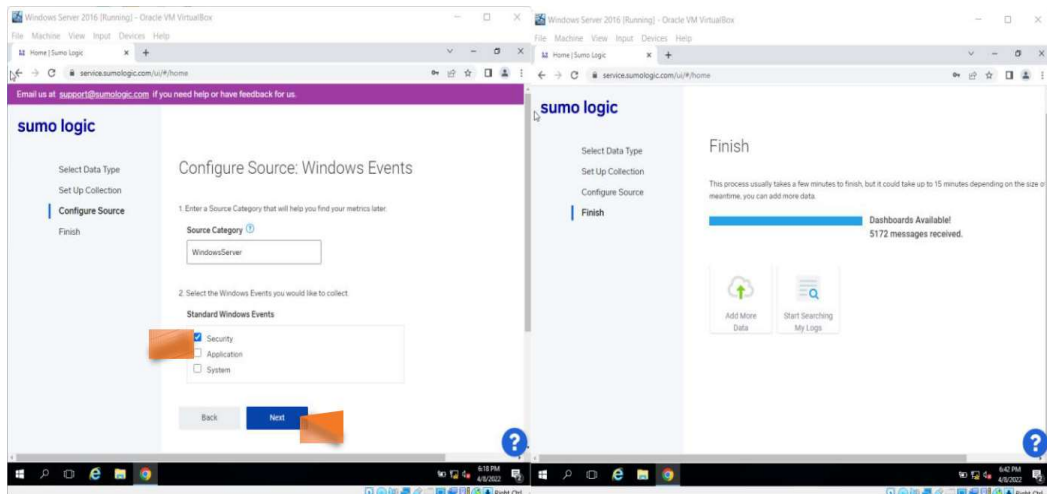


It'll initialize collector. Once completed, click "Finish"

Check in the task manager if the sumo-collector process is running.

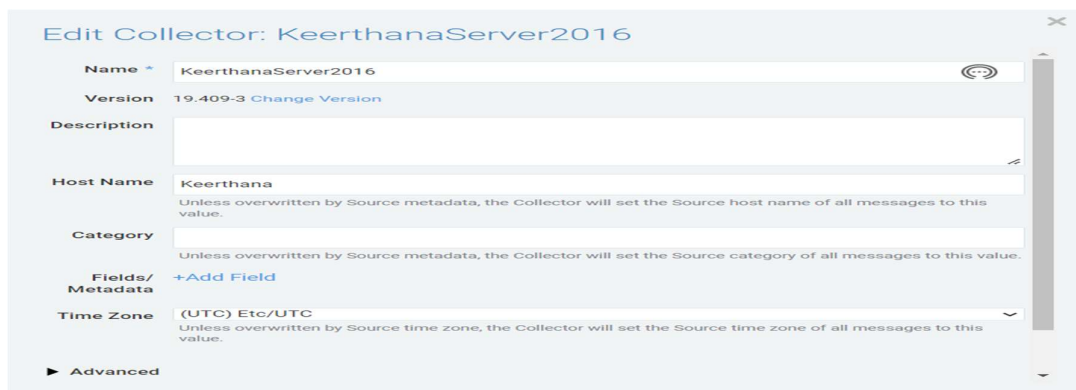


Configure the source by selecting only security logs. Finish configuration.



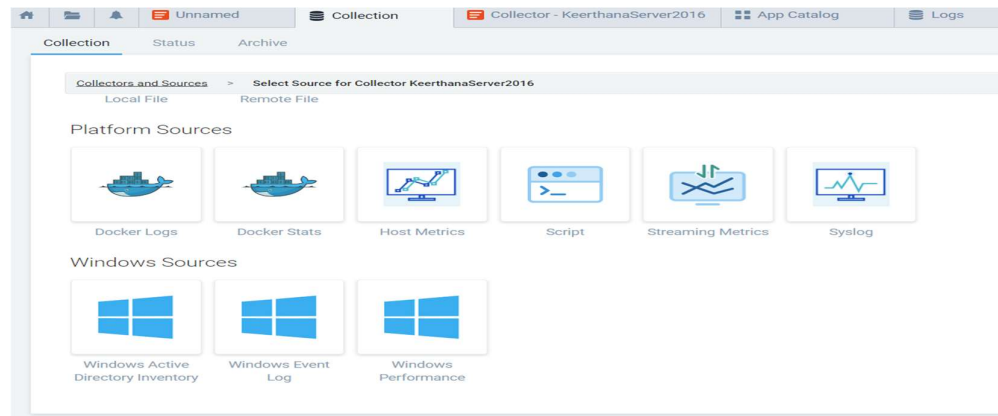
## 8.4 Collect Windows Logs

Under Collection, go to the right-hand side of screen and click "Edit" in front of your server and change the collector's name to be easily identified.



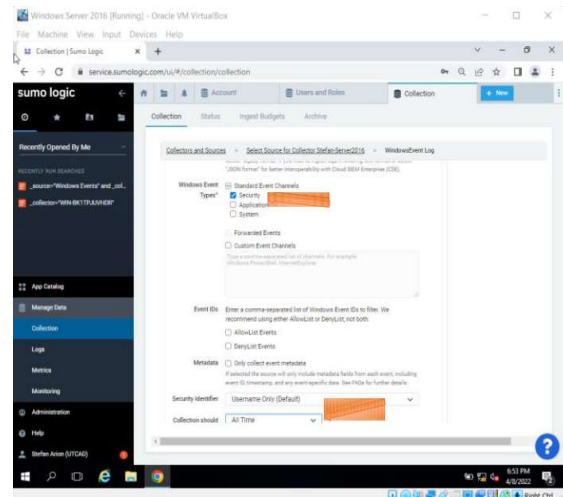
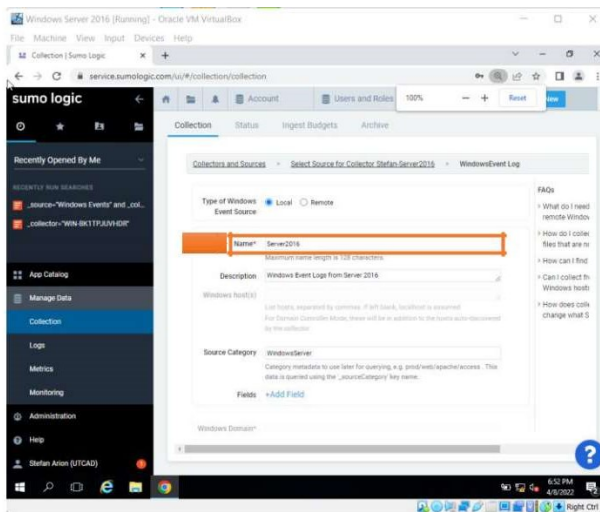
Under Collection, go to the right-hand side of screen and click “Add” in front of your server. Select “Add source”

It'll give you some options. Click on “Windows Event Log” icon.



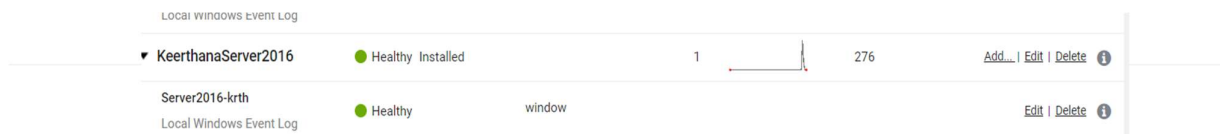
Put in a Name. We used “Server2016”. In description write “Windows Event Logs from Server 2016” or you can use your own. Assign a Source Category, in our case we used Windows.

Types we selected only “Security” so we won't run out of free trial space. Select “All time” for Collection should from drop down. Leave other options as default. Click “Save”

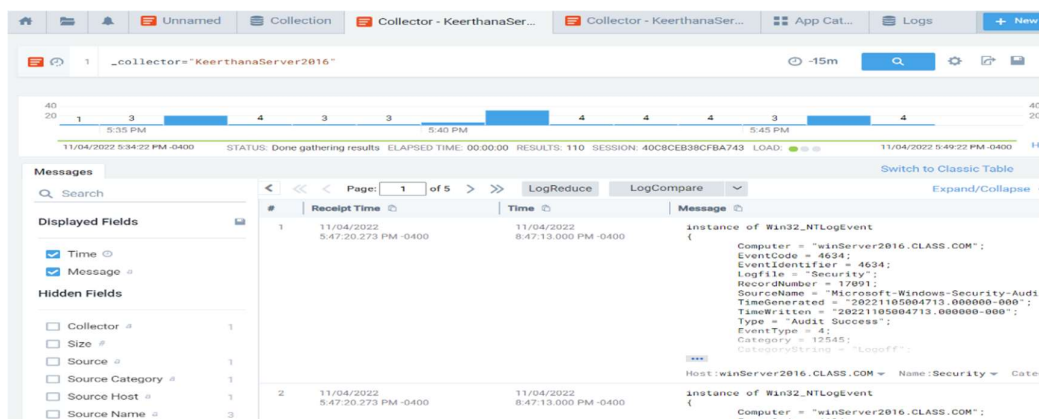


## 8.5 Searching Event Logs

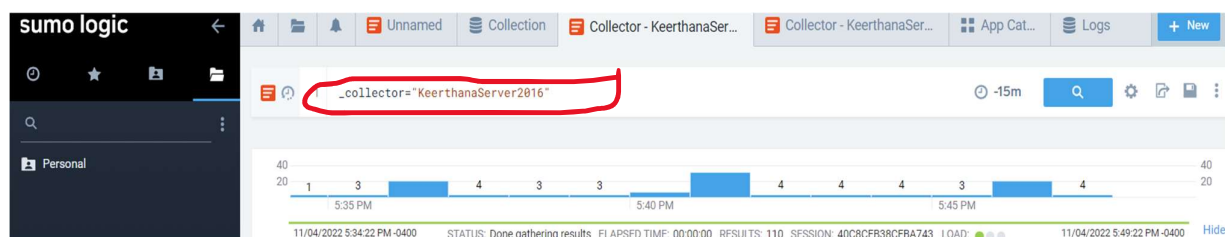
Now go back to Server Manager and create a new user and delete it. You can follow the procedure to create user defined before. Go to Sumo Logic portal. Under Collection, hover mouse over your server's name. There'll appear a blue icon (pointed by red arrow), click that icon.



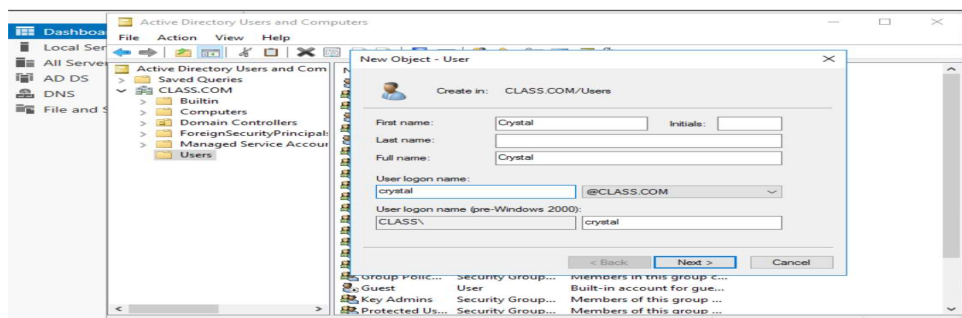
It'll open the Collector window. In search bar, in front of the existing query select the length of time ("Use Receipt Time") to display the logs. Press the search magnifier button.



In search bar, in front of the existing query type keywords such as "user test and deleted". Select "Use Receipt Time" and click "Magnifier" button.

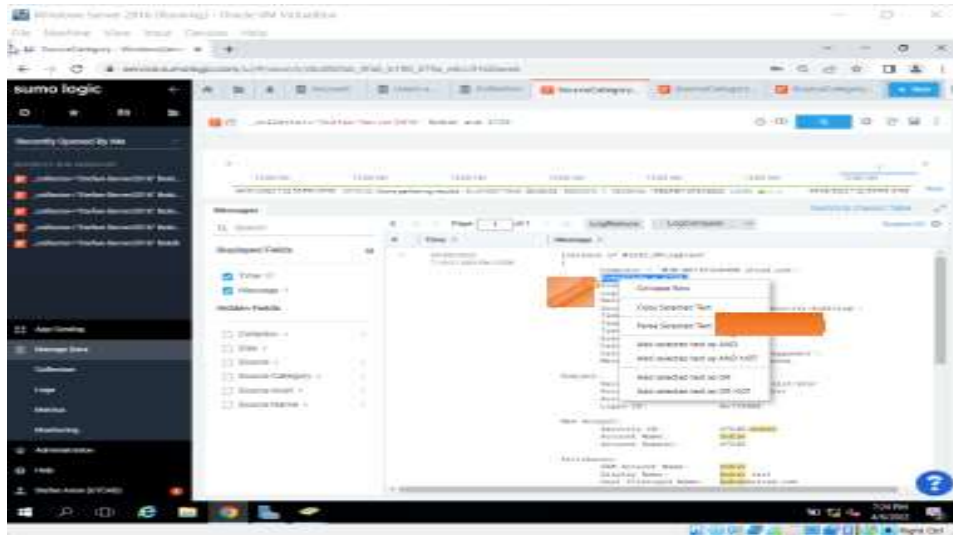


In the active directory application, in left Panel, select your newly created Domain. Under domain click "Users". On right panel, right click, go to "New" and then select User.

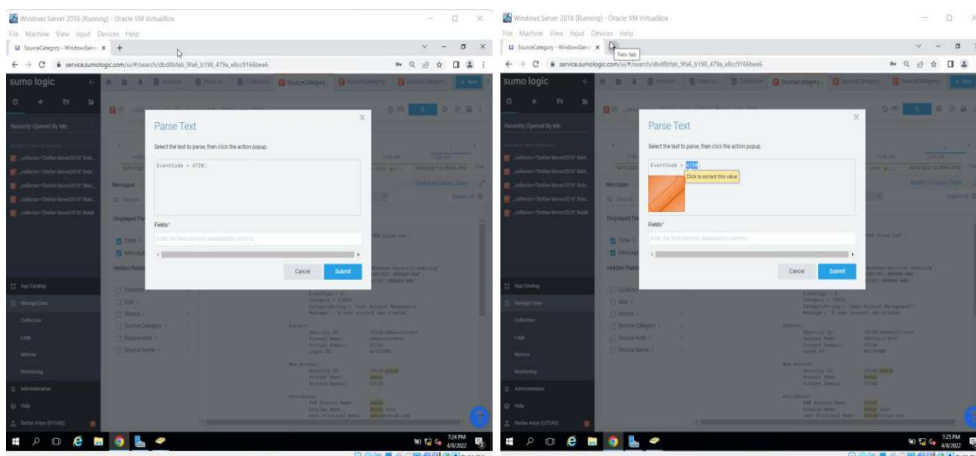


## 8.6 Parse the Event Code

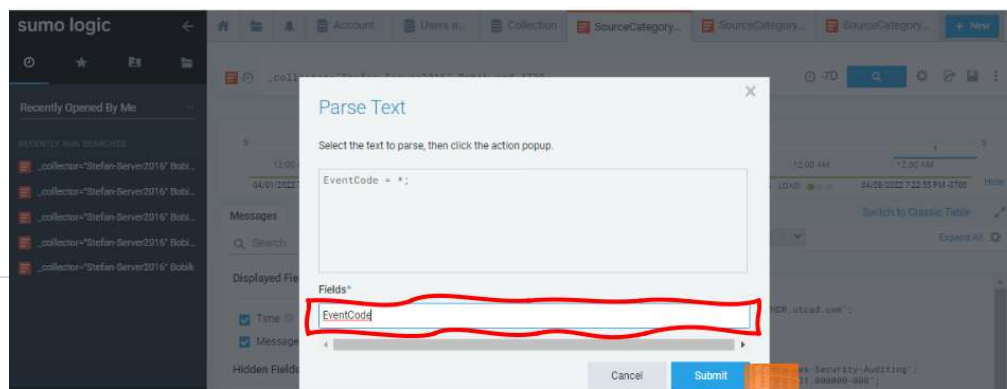
We are going to parse a field such as Event Code. Select the field and value and right click. Click “Parse selected text”.



Double click the value and select “Click to extract this value” it’ll change the value to star.



Give that field a name. We are going to use “Event Code”. Click Submit. Start the query again.



You'll see a new field "EventCode" and at the same time we can add "Msg"

| # | Receipt Time                    | Time                            | Message                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---|---------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 11/04/2022 5:14:09.231 PM -0400 | 11/04/2022 8:14:02.000 PM -0400 | instance of Win32_NTLogEvent<br>{<br>Computer = "winServer2016.CLASS.COM";<br>EventCode = 7036;<br>EventIdentifier = 1073748860;<br>LogFile = "System";<br>RecordNumber = 4814;<br>SourceName = "Service Control Manager";<br>TimeGenerated = "20221105091402.000000-000";<br>TimeWritten = "20221105091402.000000-000";<br>Type = "Information";<br>EventType = 3;<br>Category = 0;<br>CategoryString = "None";<br>...<br>Host:winServer2016.CLASS.COM Name:System Cate |
| 2 | 11/04/2022 5:13:58.948 PM -0400 | 11/04/2022 8:13:52.000 PM -0400 | instance of Win32_NTLogEvent<br>{<br>Computer = "winServer2016.CLASS.COM";<br>EventCode = 6891;<br>...                                                                                                                                                                                                                                                                                                                                                                   |

## 8.7 Creating Alert for Windows Event

We'll create search a security-enabled global group was created. We'll create the same search script for Event ID7036. After that click Save As.

**Save Item**

Name \*  
event- KeerthanaServer2016 7036

Description

Query \*  
\_collector="KeerthanaServer2016"

Time range  
11/04/2022 5:00:36 PM to 11/...

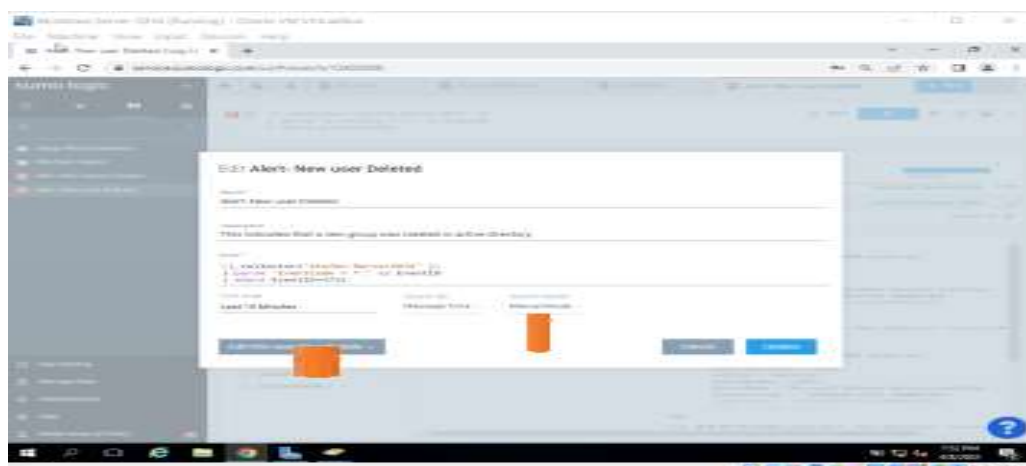
Search By  
Receipt Time

Search Mode  
Auto Parse Mode

Location to save to  
All Folders

[Schedule this search >](#) [Cancel](#) [Save](#)

We'll create an email alert to be send whenever a user is deleted. We'll create the same search script for Event ID7036. After that click Save As. Assign a Name and Description to this alert. Change Time range to 15 minutes. We'll save this to Personal folder. Click on "Schedule this search >".



Select "All time" from drop down box. This is lab so we can select this option. Otherwise, this is slow down the whole process. Change Time range for scheduled search to "Last 5 minutes". Change "Alert condition" to Greater than or equal to  $\geq$  and Number of results to "1". Alert Type should be Email and put your email address in Recipients. Click "Update". In 15 minutes if the user has been deleted, we will receive a corresponding email with an alert.

Sumo Logic <service@sumologic.com>

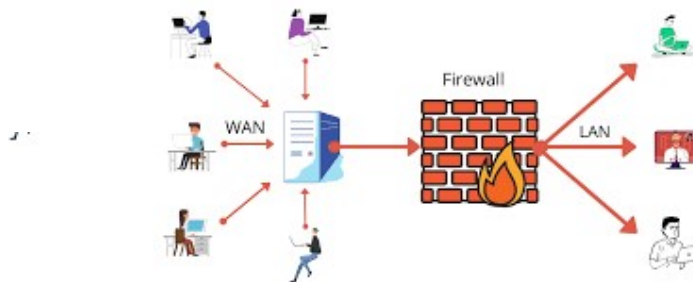
to me ▼

|                        |                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------|
| Saved Search           | <a href="#">Alert005 - User Account Deleted</a>                                                           |
| Search String          | (_collector="KeerthanaServer2016" 4726)<br>  parse "EventCode = *;" as EventCode   where EventCode = 4726 |
| Time Range             | 10/20/2022 12:00:00 PM EDT to 10/20/2022 12:15:00 PM EDT                                                  |
| Run Frequency          | Every 15 minutes                                                                                          |
| Notification Threshold | Every time a search is complete                                                                           |
| Run At                 | 10/20/2022 12:22:48 PM EDT                                                                                |
| Scheduled By           | Keerthana Tirumalaraju < <a href="mailto:keerthana.vizag@gmail.com">keerthana.vizag@gmail.com</a> >       |

## 9. Firewalls

### 9.1 What is firewall?

A Firewall is a network security device that monitors, and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.



Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications, or ports while allowing relevant and necessary data through.

#### Advantages of Firewall

- A Firewall prevents hackers and remote access.
- It protects data.
- It ensures better privacy and security.
- It protects from Trojans.
- A network-based Firewall, like a router, can offer protection to multiple systems, while an OS-based Firewall can protect individual systems.

#### Disadvantages of Firewall

- **Cost:** Installation of a Firewall can be costly depending on the sophistication required.
- **Performance:** This is affected as each packet has to be verified for authenticity before it is allowed into the network.
- **Virus and Malware:** There are a few limitations in a Firewall like its inability to prevent virus and malware attacks for which separate applications would be required, at the individual system level.
- A network-level Firewall might bring in a false sense of security in employees and make them slacken on securing individual systems. Companies need to make all employees understand the concept of a Firewall and the importance of a Firewall for information security and their responsibility.
- Firewall maintenance and up-gradation require extra manpower and resources.

## 9.2 Installing pfSense on VirtualBox

pfSense is a free and open-source operating system for routers and firewalls. pfSense can be installed on most commodity hardware, including old computers and embedded systems. pfSense is typically configured and operated through a user-friendly web interface, making administration easy even for users with limited networking knowledge. Generally, one never needs to use terminal or edit config files to configure the router. Even software updates can be run from the web UI.

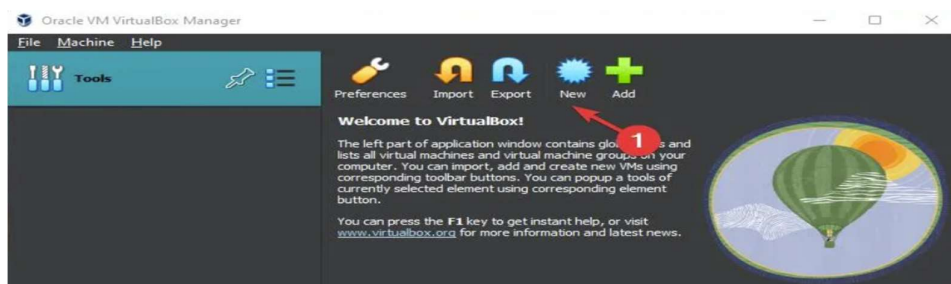


We'll use pfSense as our firewall in this lab. Go to <https://www.pfsense.org/download/> to download pfSense. Click on Architecture dropdown box and select "AMD64 (64-bit)". Click on Installer dropdown box and select "CD Image (ISO) Installer". Leave default value for "Mirror" and click download button.



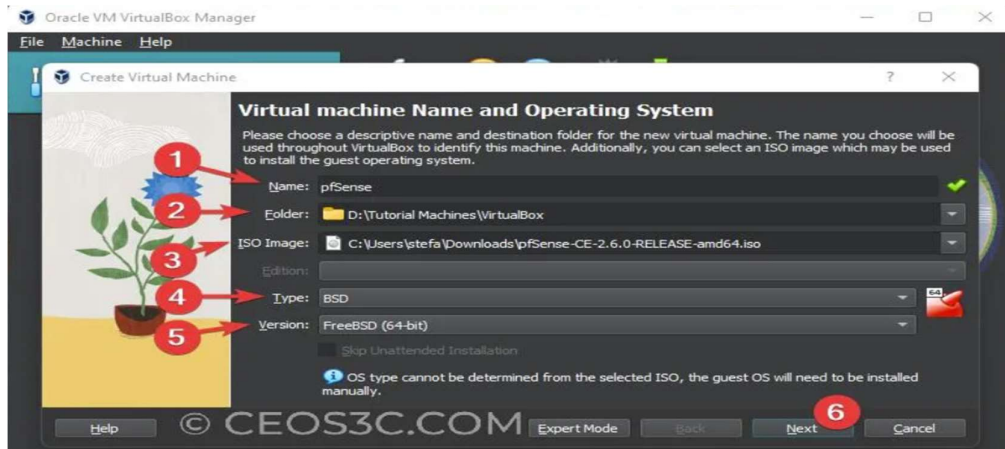
First off, **download** the pfSense ISO image file. Once downloaded, make sure you have 7-Zip installed. Head to your **Downloads** folder and **right-click** the **pfSense-amd64.iso.gz** file. Now choose **7-Zip** (if you are on Windows 11, you must select **Show More Options** first!) and select **Extract Here**.

**Start up VirtualBox and click on New.**



1. Choose a **name** for your VM (pfSense is good!).
2. Choose a **location** on your physical hard disk where you want to store the VM.

3. Select the **unzipped pfSense.amd64.iso** file from your **Downloads** folder.
4. As **Type**, choose **BSD** (pfSense's underlying Linux kernel).
5. As **Version**, choose **FreeBSD (64-bit)**.
6. Click on **Next** to continue.



The hardware settings are your personal preference. Just make sure to adhere to pfSense's [minimum hardware requirements](#). You should assign at least **1024 MB of memory** and **1 CPU**. We will assign a little bit more:



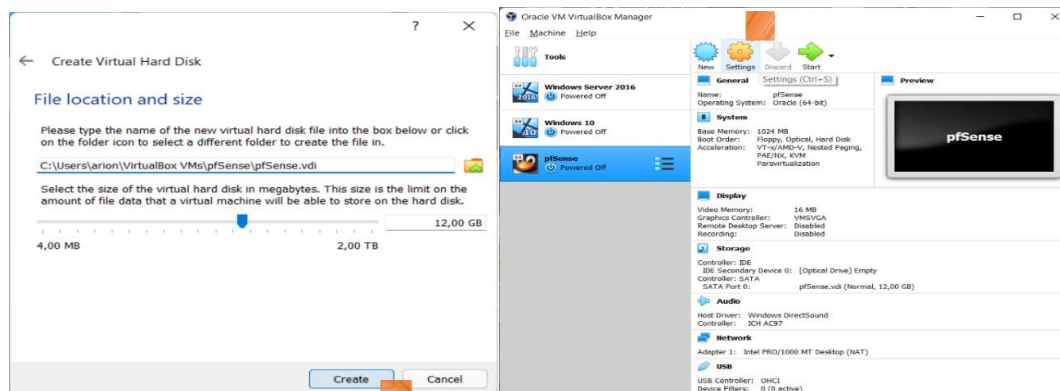
Next, we need to set up the Virtual Hard Disk. **10 GB** is sufficient for pfSense. If you plan to install a lot of packages, choose more:



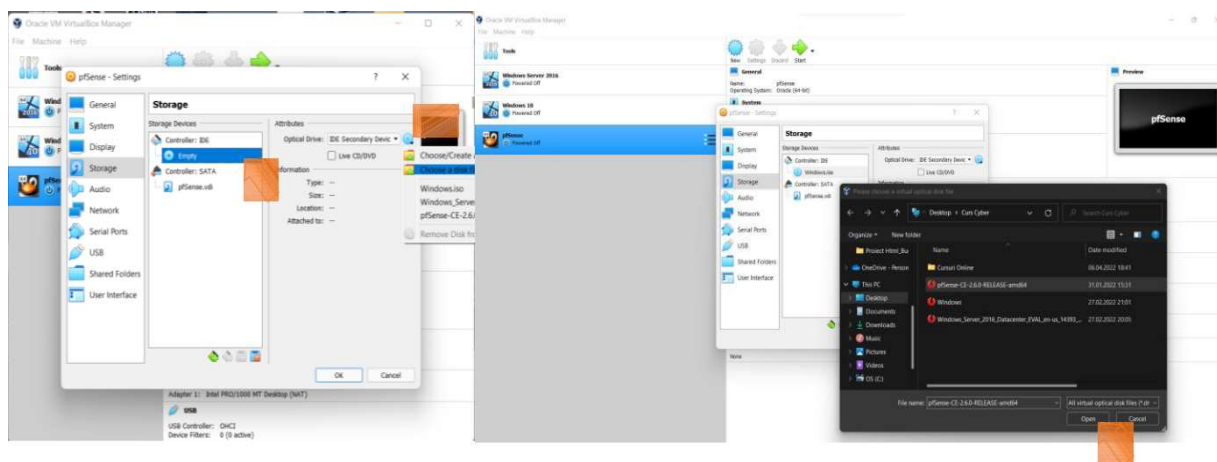
In the final screen, make sure everything is according to your preferences and click on **Finish**



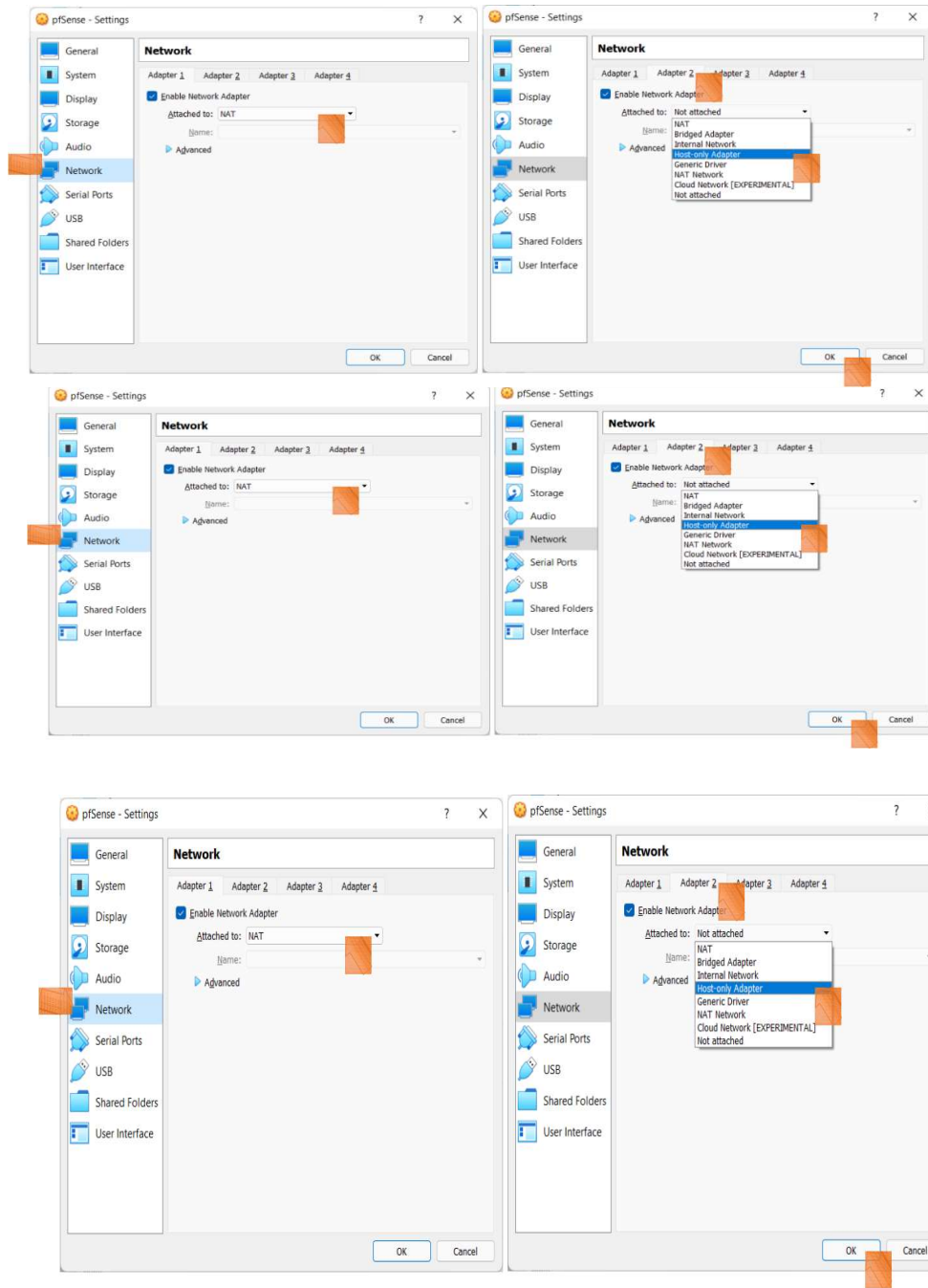
Leave default value for File location and size. You can change to different folder. Click “Create”. Select pfSense from left panel and click “Settings”



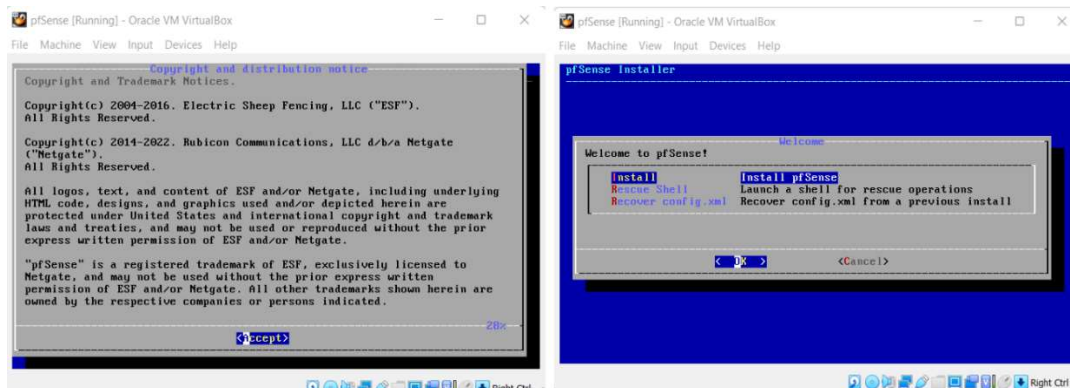
Select Storage then select “Empty” under Controller: IDE. Click on “CD” on right corner. Select “Chose a disk file”. Select pfSense ISO file which we have extracted earlier.



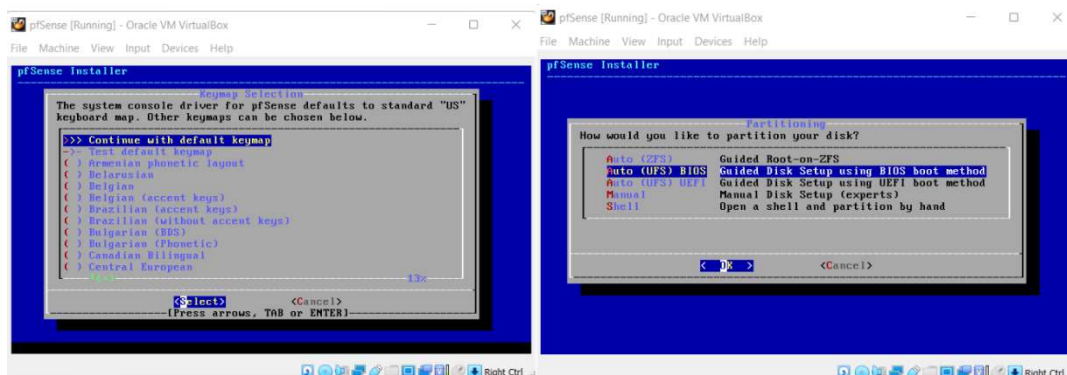
Select "Network" from left panel. Under Adapter 1, select NAT from drop down box. Click on "Adapter 2". Select "Enable Network Adapter". Click on "Host-only Adapter" from drop down. Click "OK".



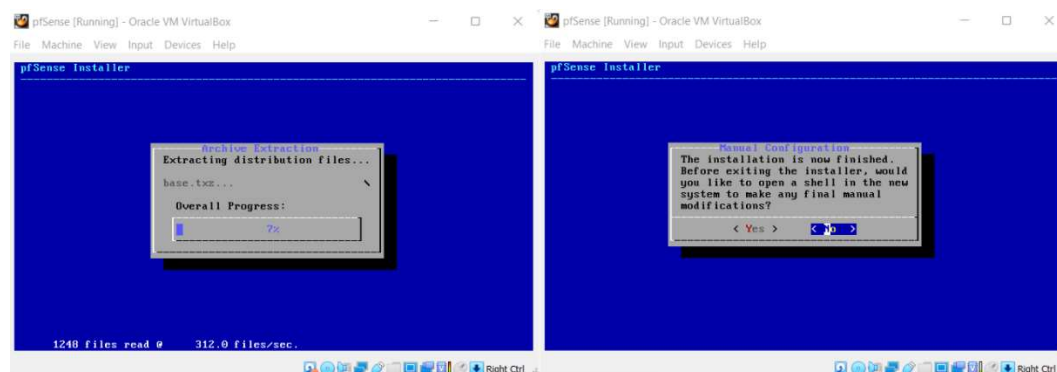
Click “Start” from VirtualBox main screen. It'll start the pfSense VM. Press enters “Accept” on first screen. Using arrow keys, select “Install pfSense” and press enter.



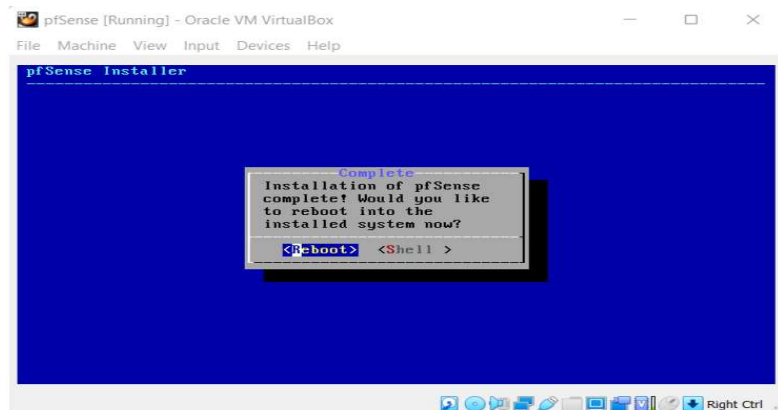
Press “Enter” on next screen. Using arrow keys, select “Auto (UFS) BIOS” and press enter.



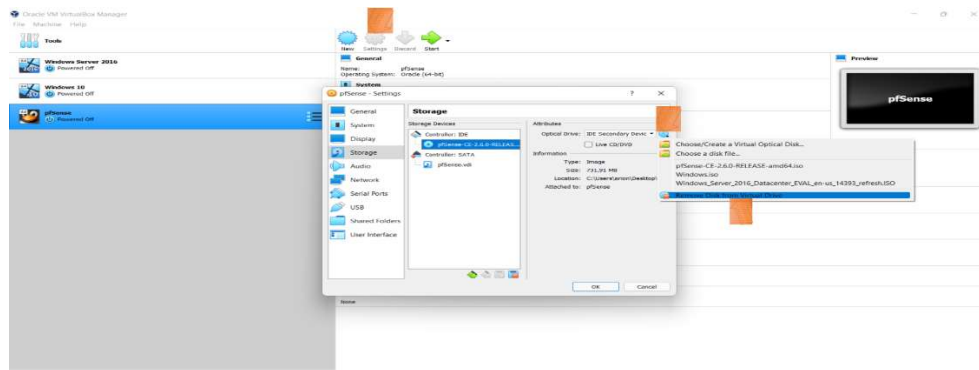
It'll start the installation Press “No” on next screen and exiting the installer.



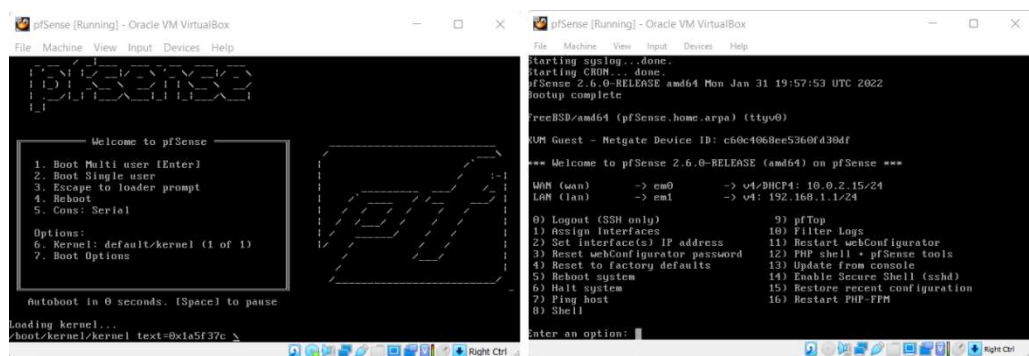
Press "Reboot" on next screen and restart system.



Next, we need to remove the disk from the virtual optical drive to run the Linux operating system.

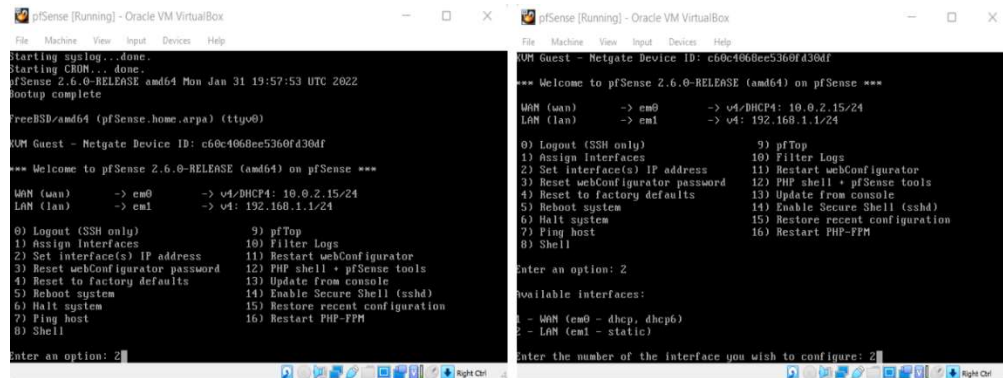


Runs the Linux operating system and the pfSense application. Once done it'll be on following Menu



Enter 2 to assign IP.

Again enter 2 to change LAN IP.



```
Starting syslog...done.
Starting CRON...done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

KVM Guest - Netgate Device ID: c60c4068ee5360fd30df

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0    -> v4/DHCP4: 10.0.2.15/24
LAN (lan)    -> em1    -> v4: 192.168.1.1/24

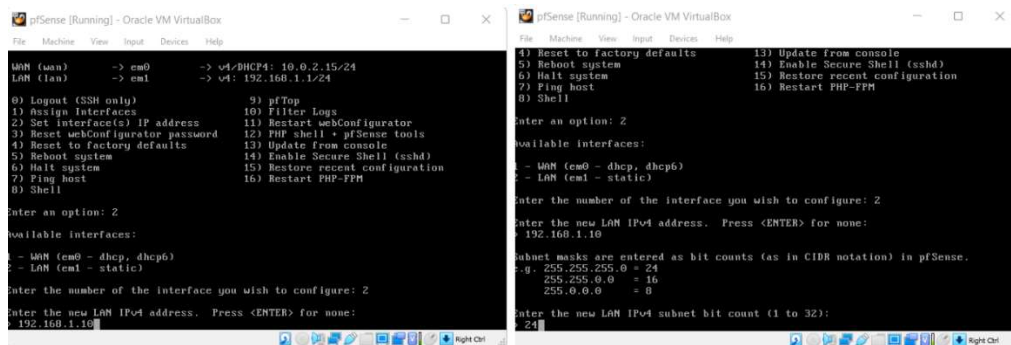
0) Logout (SSH only)      9) pfTop
1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system          14) Enable Secure Shell (ssh)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
0 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
```

We used 192.168.1.10, you can use any private IP.

Enter 24 for subnet:



```
0) Logout (SSH only)      9) pfTop
1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system          14) Enable Secure Shell (ssh)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
0 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

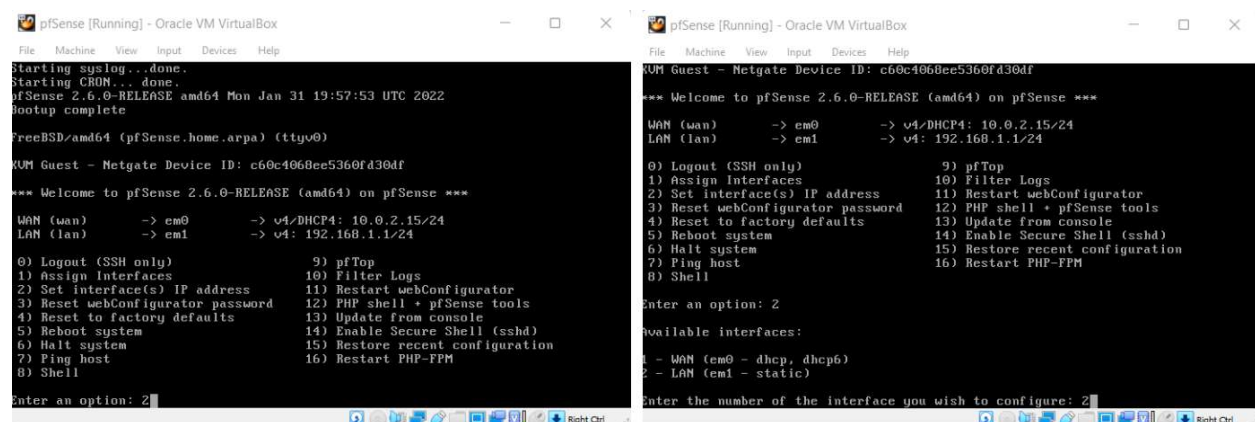
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
192.168.1.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
24
```

Press enters twice to select default value.



```
Starting syslog...done.
Starting CRON...done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

KVM Guest - Netgate Device ID: c60c4068ee5360fd30df

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0    -> v4/DHCP4: 10.0.2.15/24
LAN (lan)    -> em1    -> v4: 192.168.1.1/24

0) Logout (SSH only)      9) pfTop
1) Assign Interfaces      10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system          14) Enable Secure Shell (ssh)
6) Halt system            15) Restore recent configuration
7) Ping host              16) Restart PHP-FPM
8) Shell

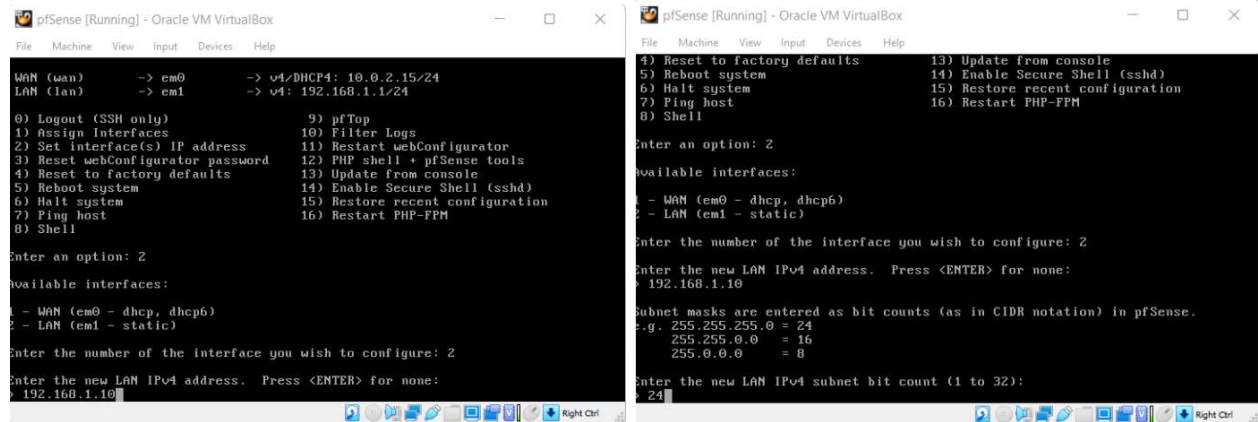
Enter an option: 2

Available interfaces:
0 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

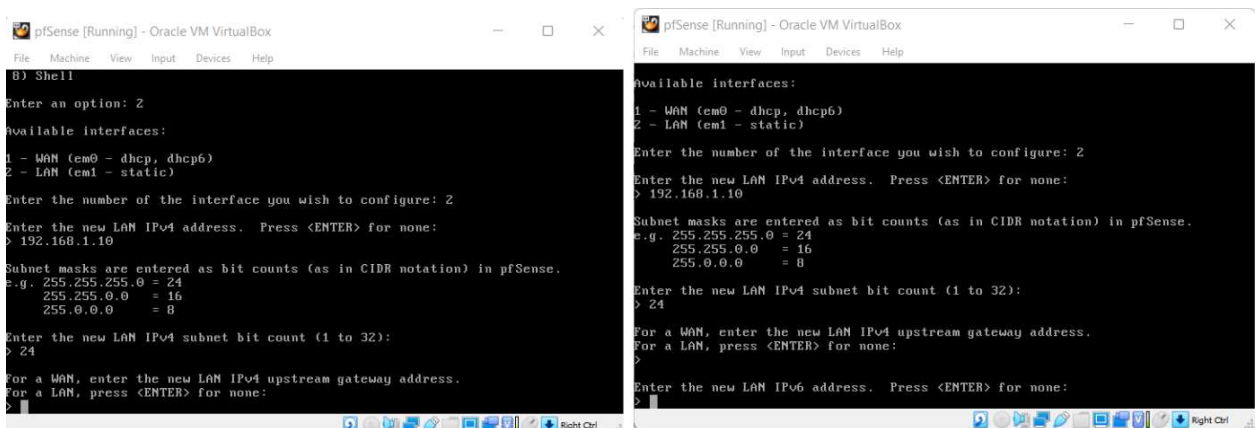
Enter the number of the interface you wish to configure: 2
```

We used 192.168.1.10, you can use any private IP.

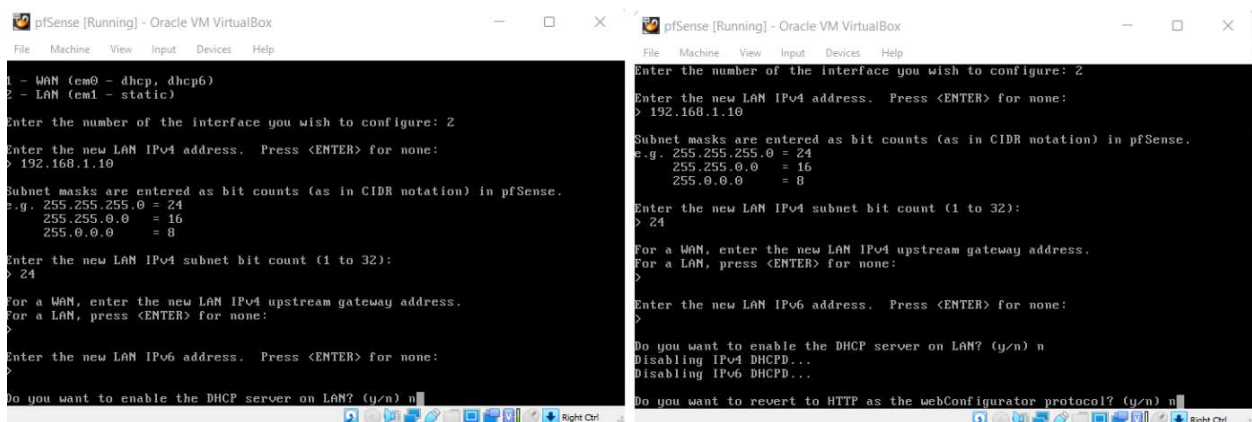
Enter 24 for subnet:



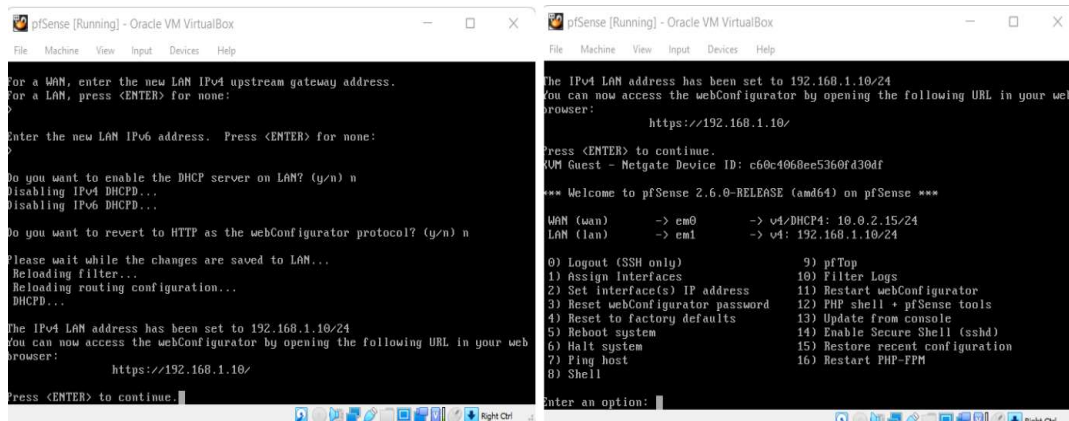
Press enters twice to select default value.



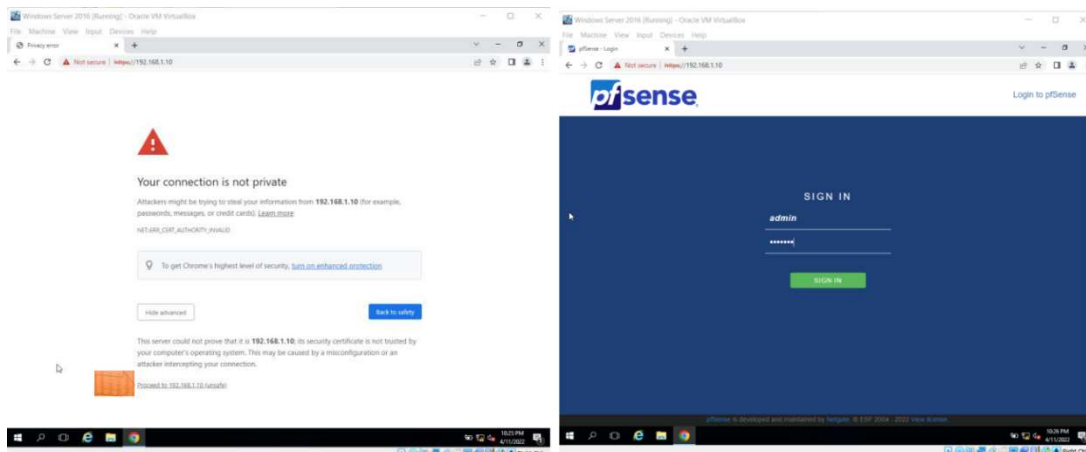
Then press "n" for DHCP option. Then press "n" for HTTP option.



Press enters to continue.

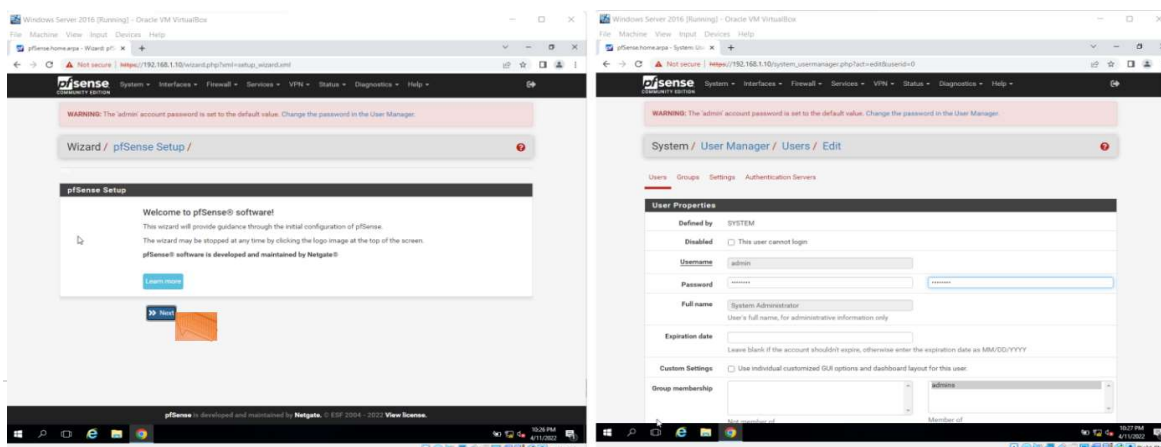


Open browser on Server or Windows 10 and put 192.168.1.10 (or pfSense IP which you have assigned.) Allow unsafe access to this page press “Proceed to 192.168.1.10 (unsafe)”. Enter “admin” as username and “pfSense” as password. (Default value)



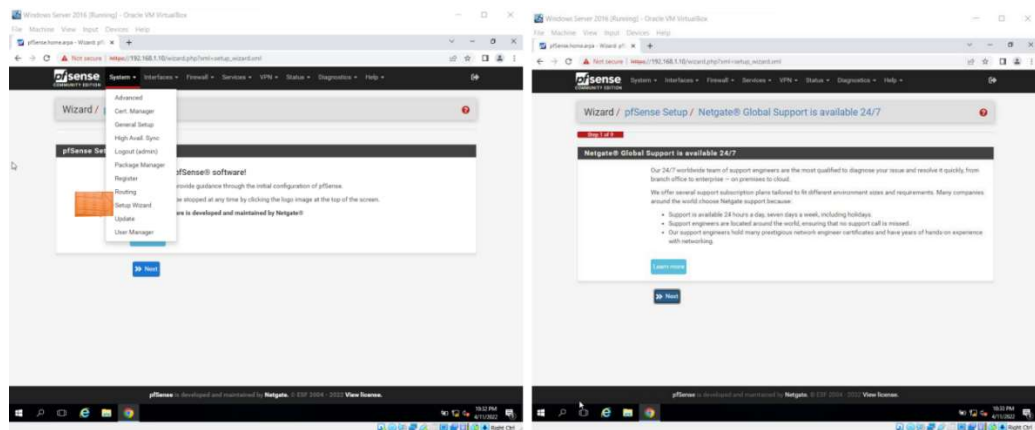
It'll take you to home screen. It shows warning to change default admin password.

Select Systems ----> User Manager. Under it select Users. Change Password and press save.

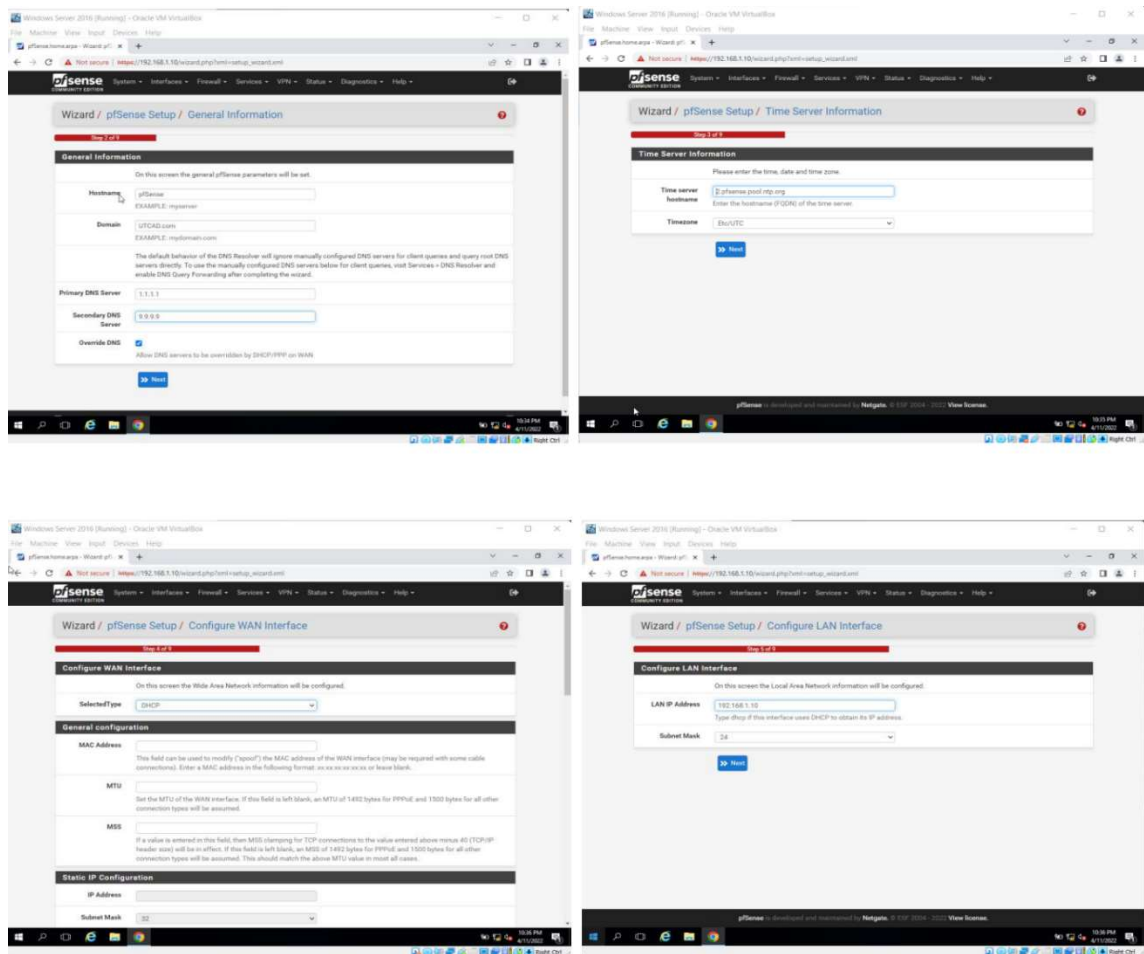


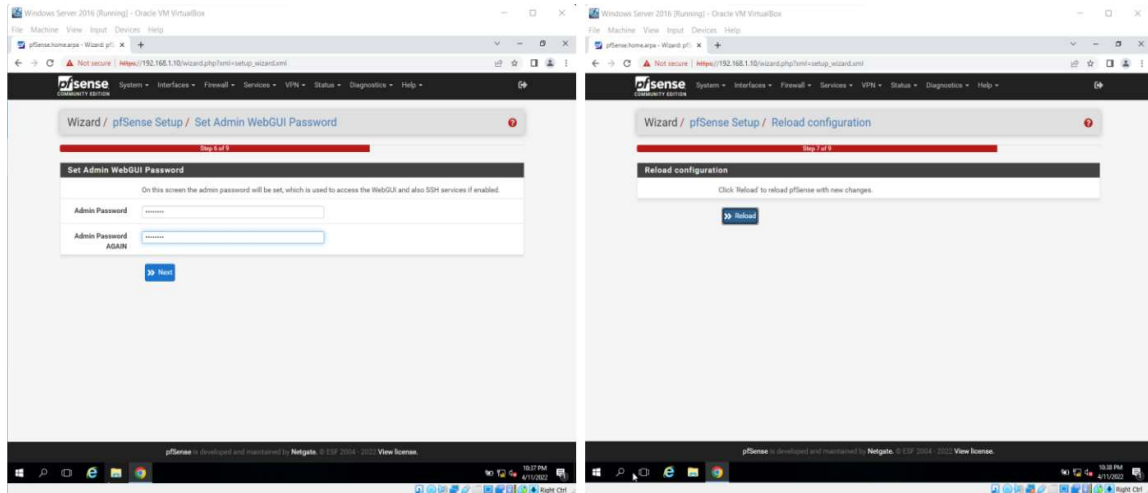
<https://t.me/learningnets>

Next in the setup wizard we do the basic configurations for the firewall

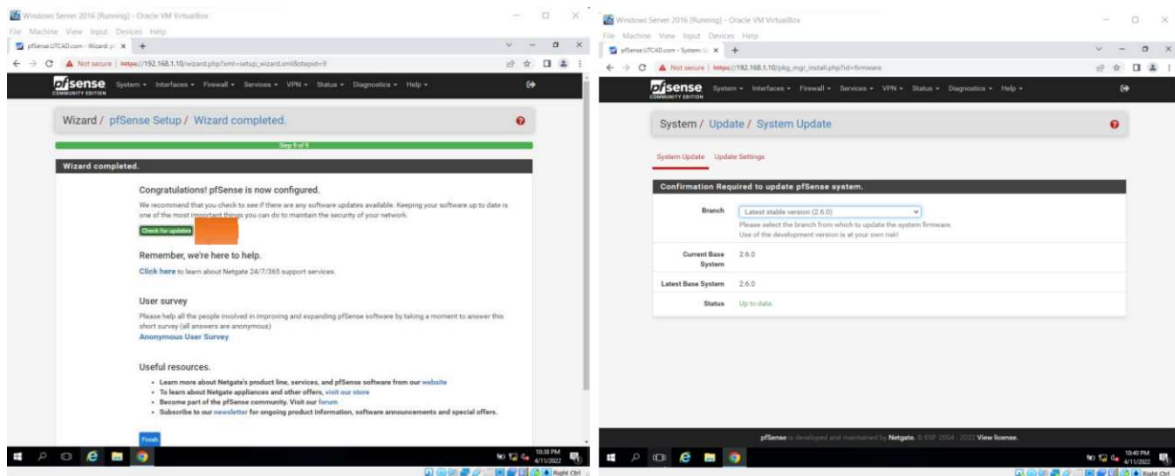


Fill in the fields in the general information and click next

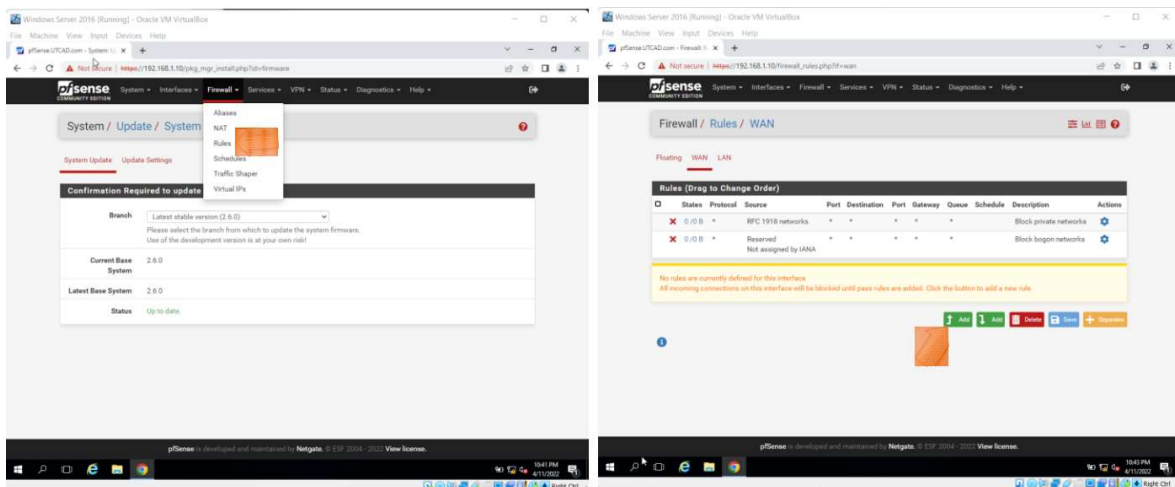




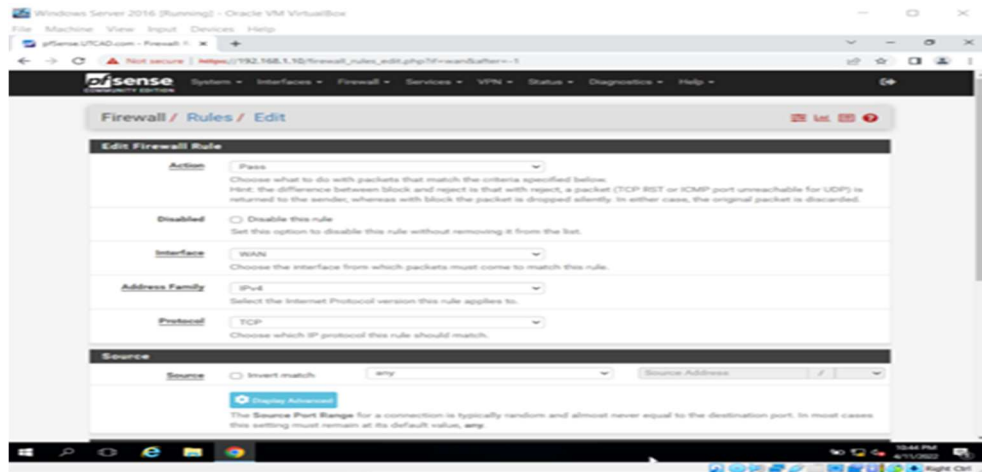
We complete all the configurations and then check the latest updates of the pfSense application



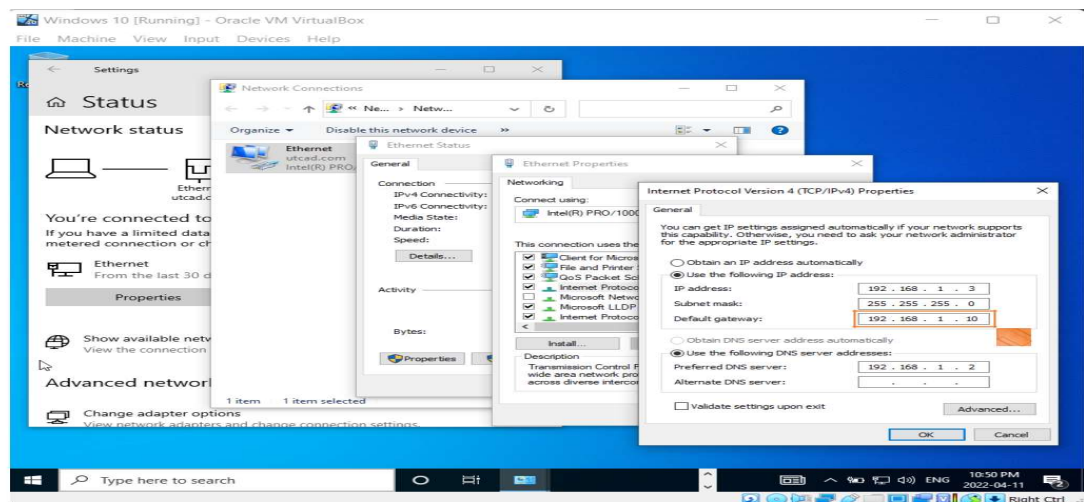
Now let's create the rule. Click "Firewall" and select "Rules" from drop down.



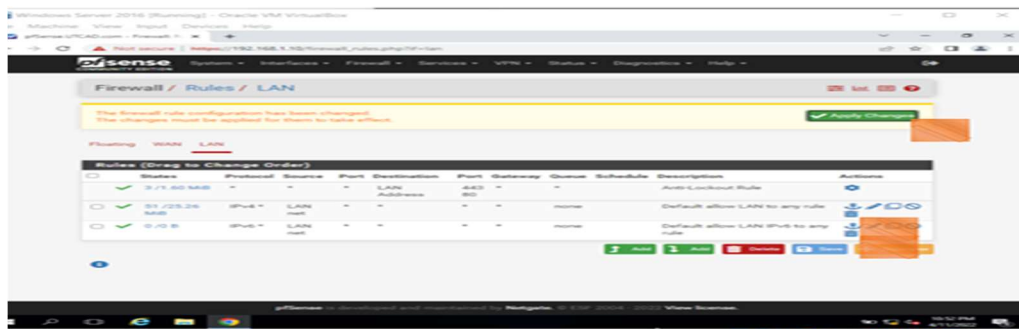
There'll be three options, Floating, WAN, LAN. Click on WAN and then then click "Add" button with arrow pointing upwards. We create a new rule for the wan and save. We open the client and check if we have internet access. It is noticed that we do not have access to the internet. Something is wrong...



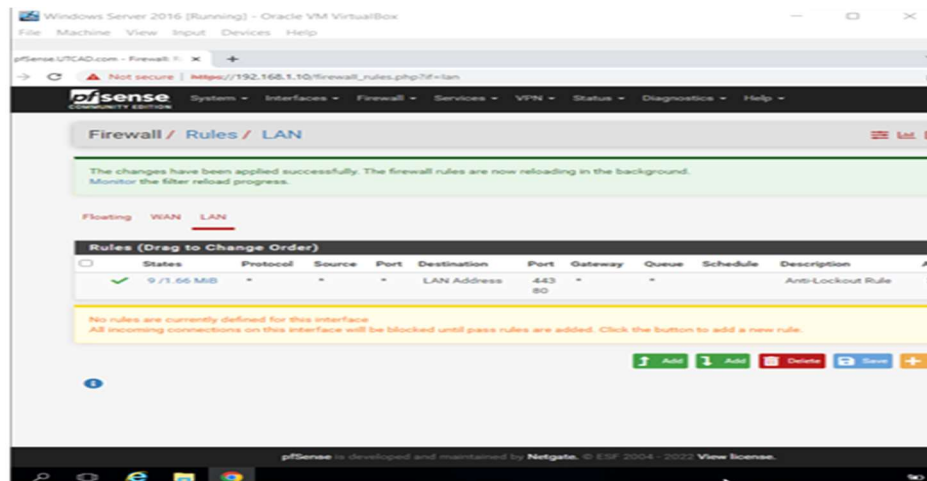
destination outside the current network. So, the IP address of the firewall must be set in the default gateway in the client's network settings



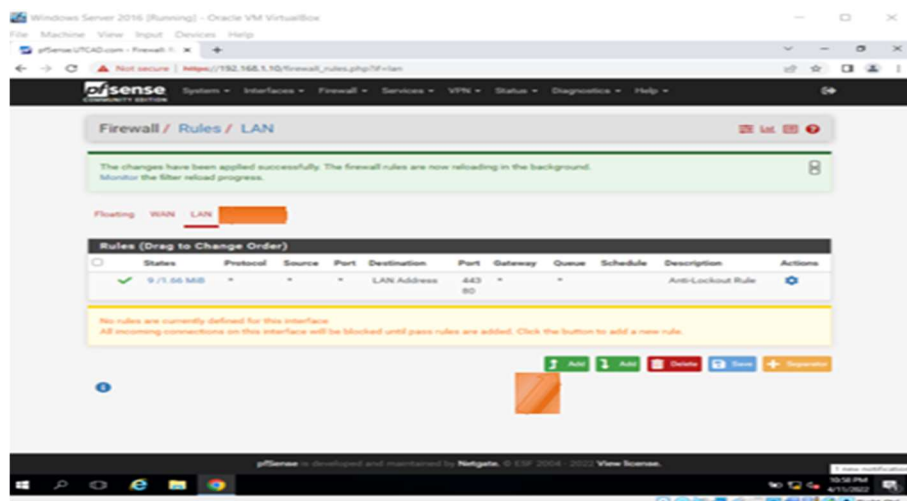
After checking the browser again, we delete the default rules from the LAN section.



After deleting the rules, we usually no longer have access to the internet. because these rules allow full internet access.

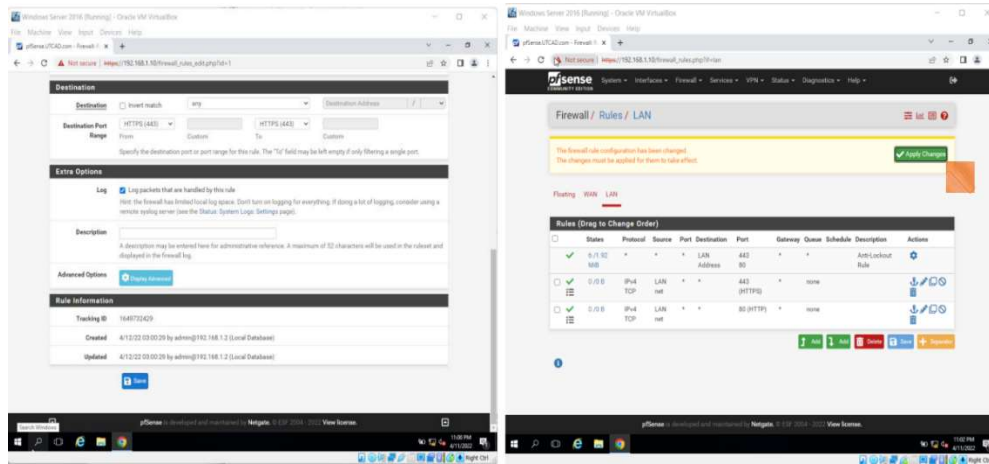


Firewall rules are the one of the fundamentals of networking. They are a set of rules that a firewall will follow when data flows through the firewall. The firewall can reject, block, or accept data according to the rules. To add an firewall rule, go to the interface that you want to add the firewall rule to, and select the Add button. The left Add button will create the firewall rule to the top of the firewall list and the right Add button will create the firewall rule to the bottom of the list.



The Action field have the options Pass, Block, or Reject. Pass allows traffic to pass through the firewall interface. The Interface field will show all the possible interface that the firewall rule can be placed on. The Address Family may be IPv4 or IPv6 or IPv4+IPv6. Currently, most network out there are still on IPv4, so this will be more applicable in most cases. You can always default to IPv4+IPv6 to cover both IPv4 and IPv6 traffic.

The Protocol is what kind of protocol the traffic you want to Pass/Block/Reject is. Typically, the most used options will be TCP or UDP.

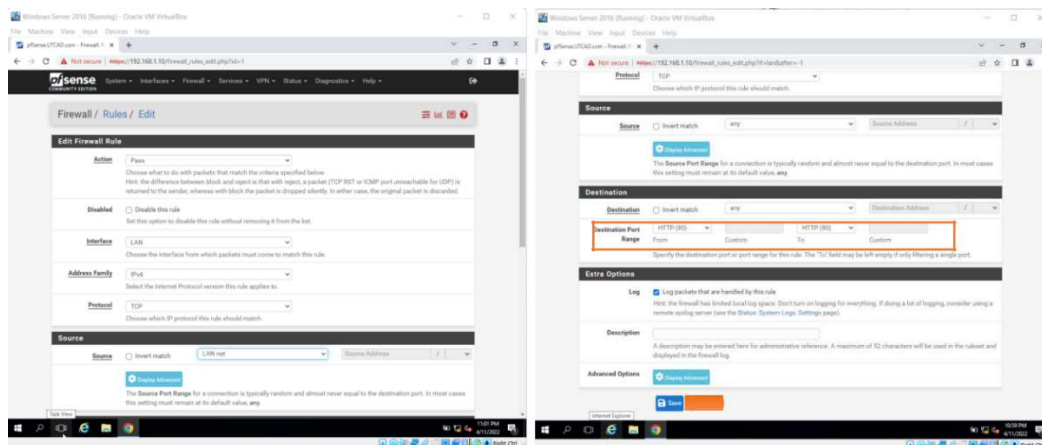


The Source section is where the traffic is coming from.

The Destination section is where the traffic is heading toward to.

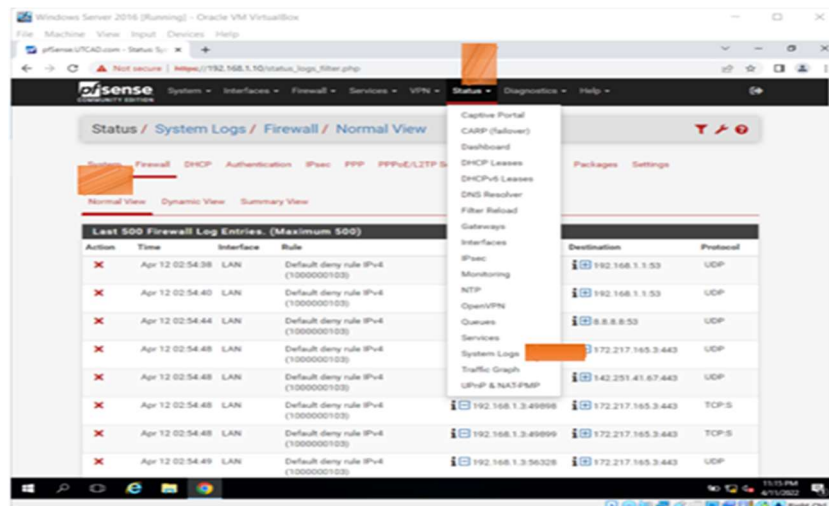
Firewall rules ordering are very important in pfSense. pfSense follows the first-match behavior when determining which firewall rule to follow and enforce. It will process rules from top to bottom and stop processing more rules once the first matching rule is found.

We add the typical rules for accessing web pages. These rules are for HTTP and HTTPS protocols.

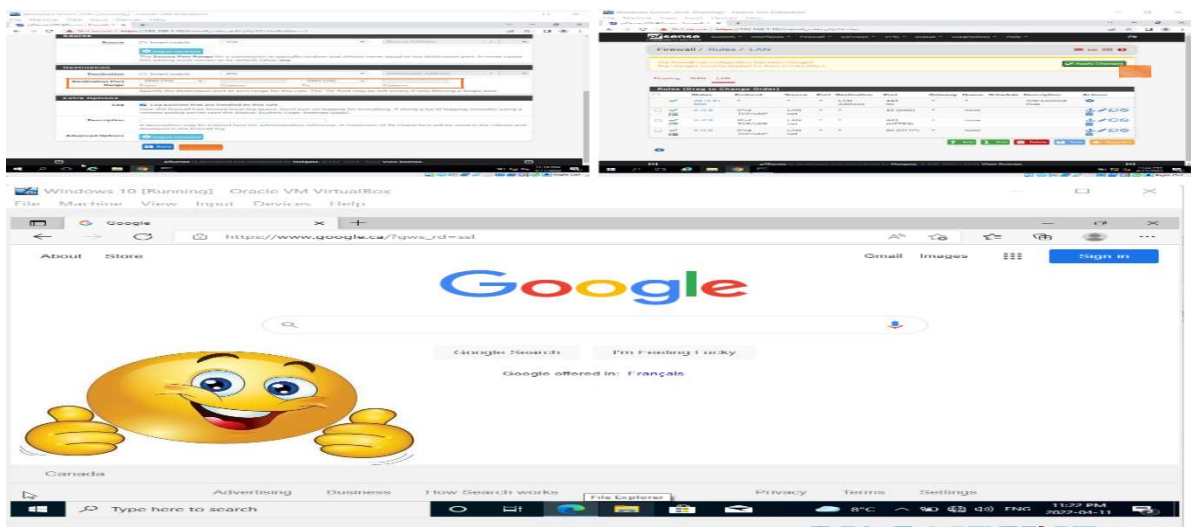
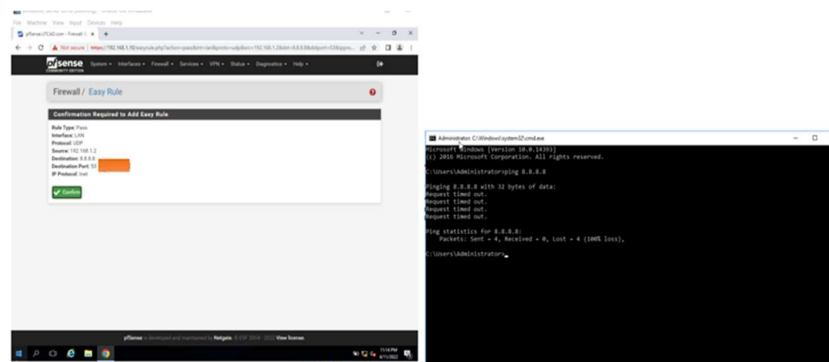


Click on “Save” and “Apply Changes”

We don't have internet access anyway ... We check the logs to identify the problem



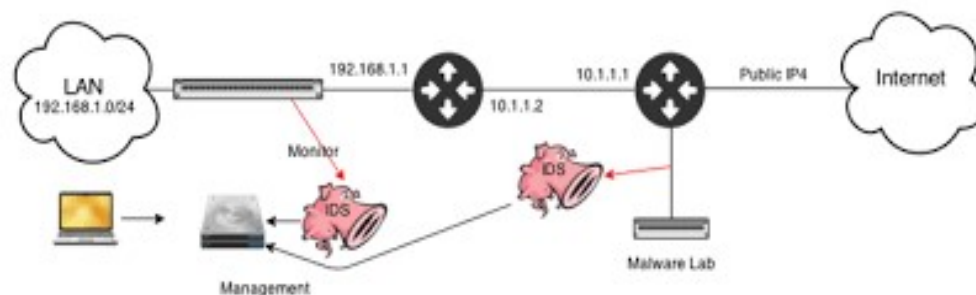
Note that we have the problem at the destination port 53. DNS port is the port number assigned to the domain name system. DNS uses UDP port 53 and TCP port 53. DNS query uses UDP port 53. It's lightweight and faster than TCP. This can reduce performance overhead on DNS servers. DNS zone transfers rely on TCP port 53 because TCP is more reliable.



## 9.3 Installing Snort Package

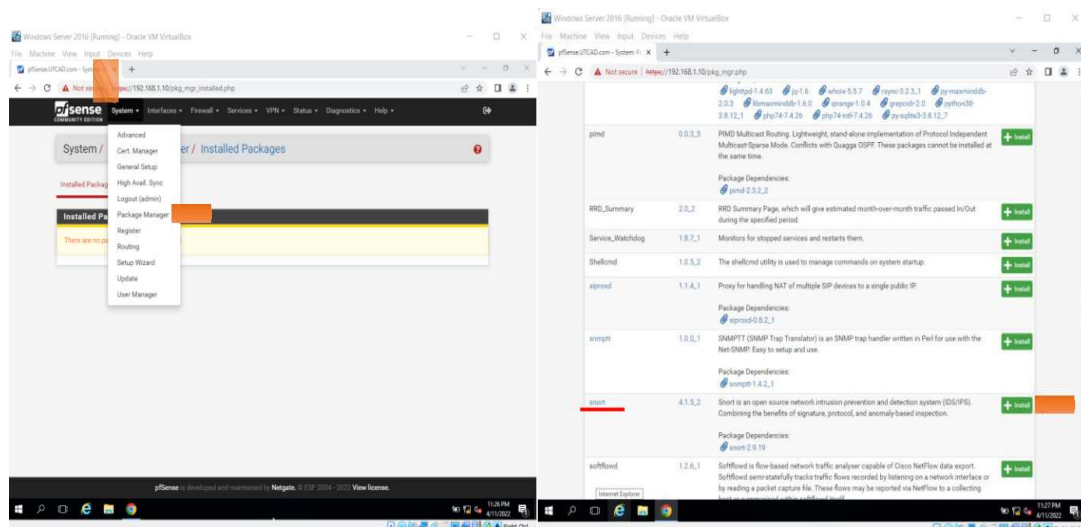
Snort is the foremost Open-Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

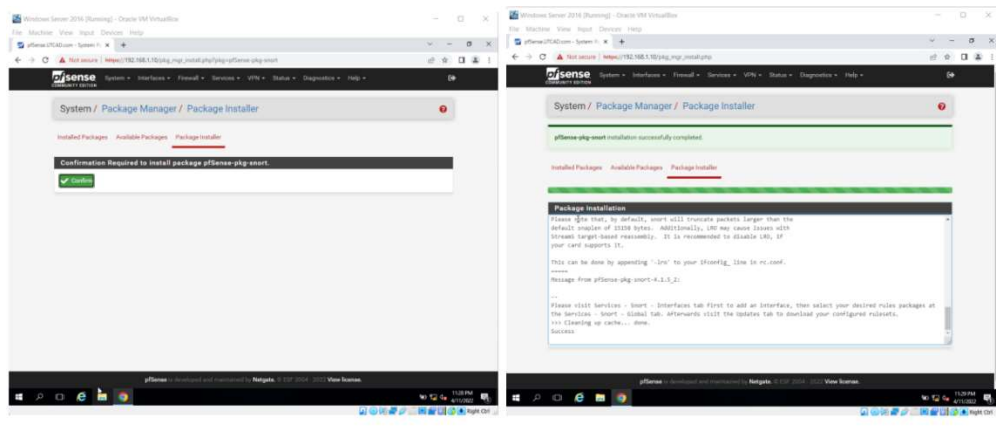


Select System ----> Package Manager. Under Package Manager select Available Packages:

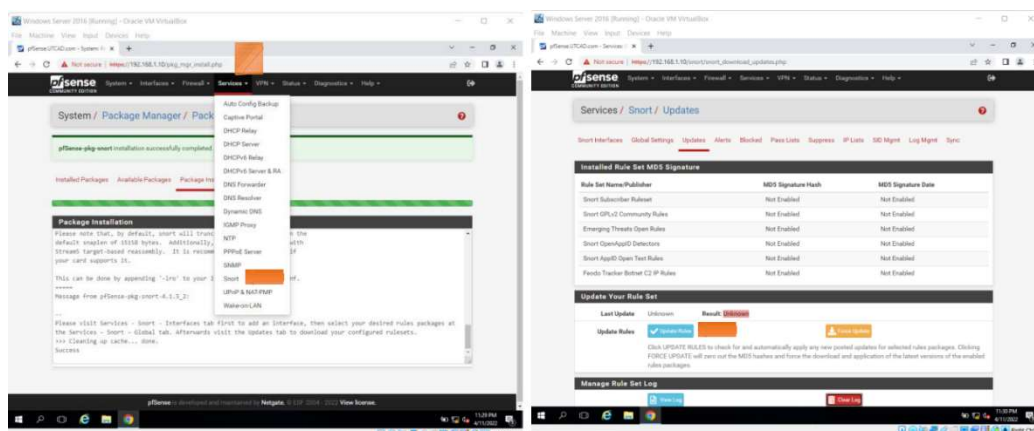
You can search for “snort” in search term or can scroll down to select snort. Press Install.



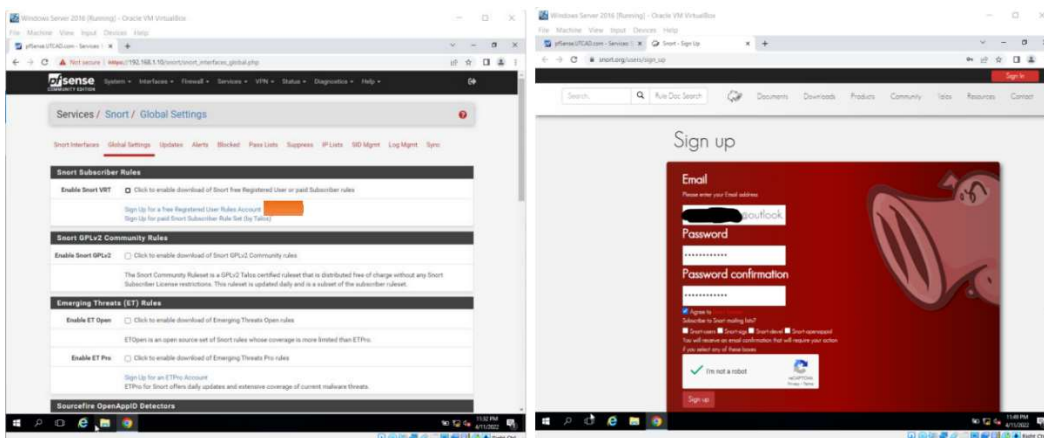
It'll ask for confirmation. Press Confirm. Once completed it'll show the completion message.



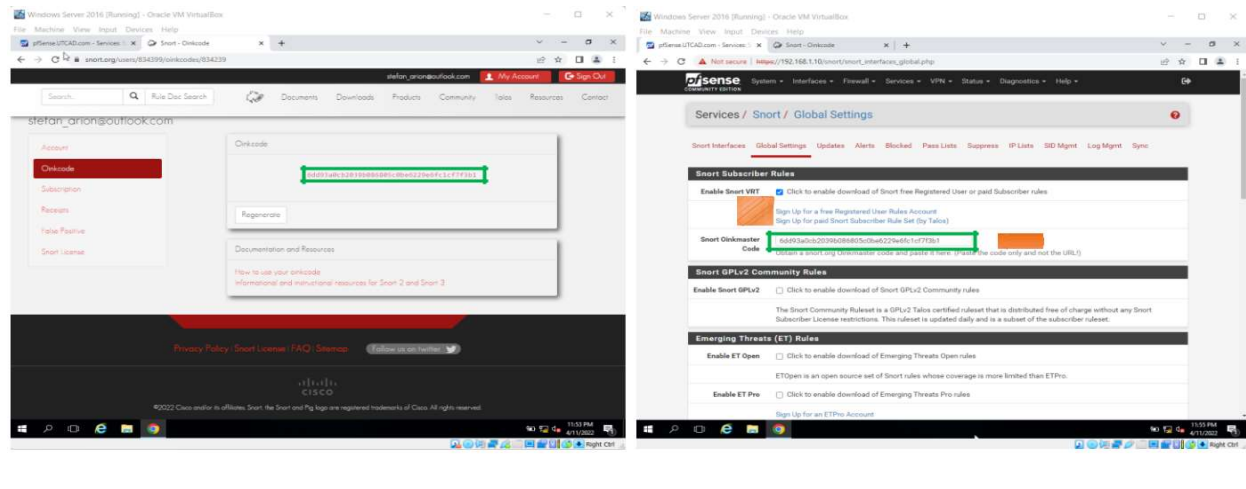
Go to Services ----> Snort  
Snort screen will appear.



Next, we register a new Snort account and get a key for new free protection rules.

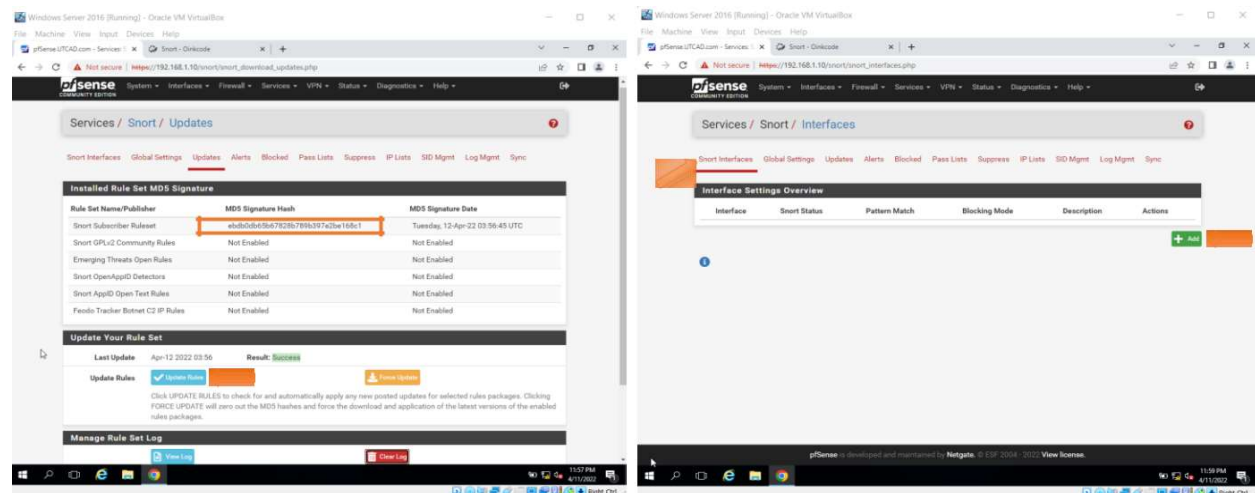


Copy the obtained key and apply the new settings

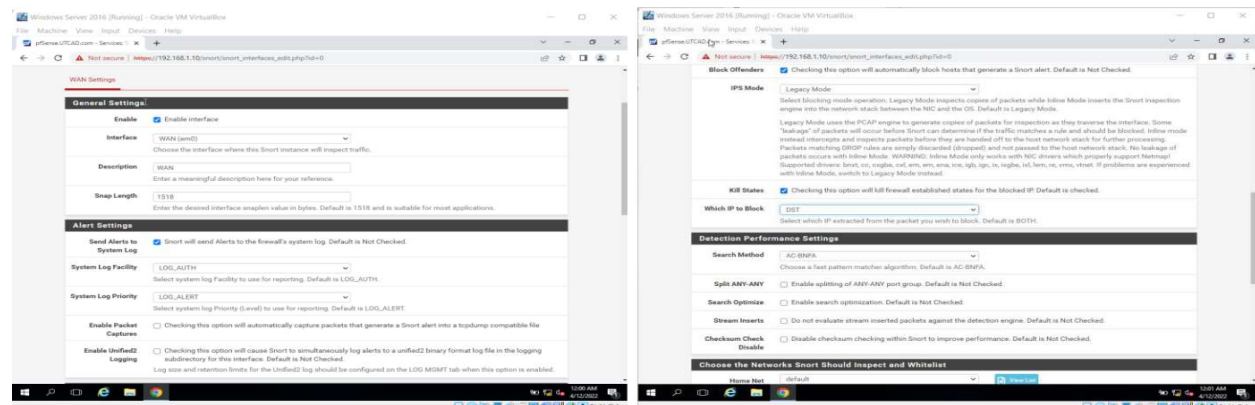


We update to the latest rules.

We are adding a new interface for proper operation

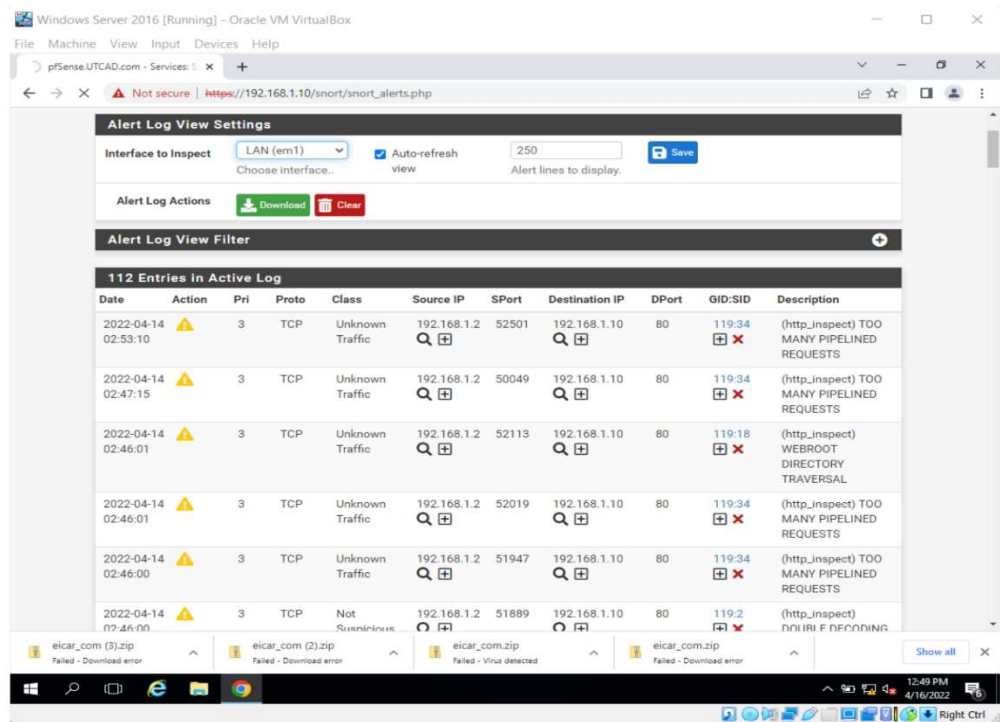
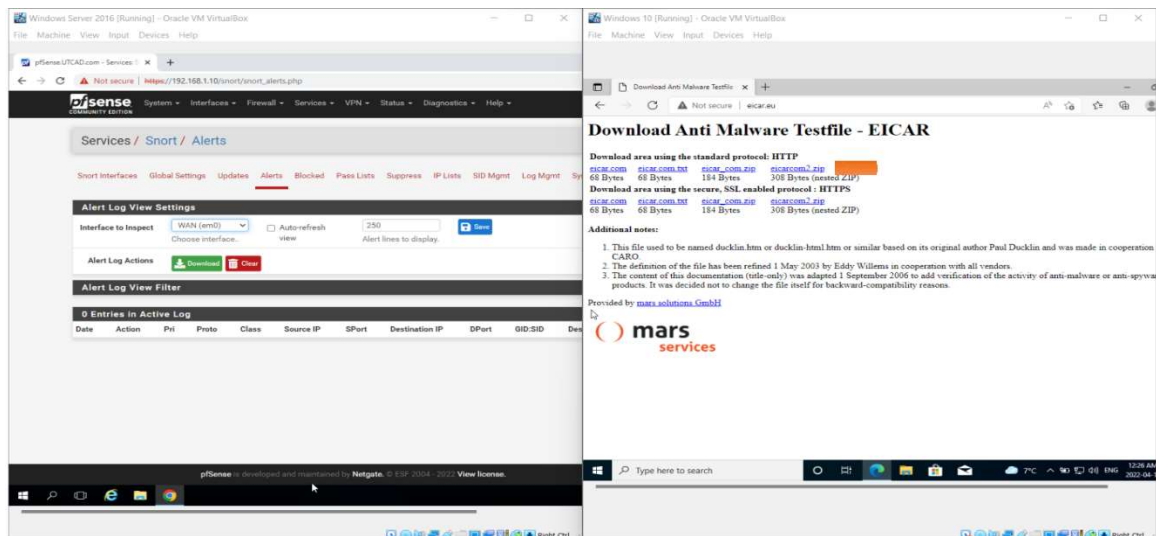


Configure the WAN interface according to the following instructions



We test the installed rules. For safe tests we use an EICAR test virus.

The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO), to test the response of computer antivirus (AV) programs. Instead of using real malware, which could cause real damage, this test file allows people to test anti-virus software without having to use a real computer virus.



## 10. Endpoint Security

Endpoint security is the process of protecting devices like desktops, laptops, mobile phones, and tablets from malicious threats and cyberattacks. [Endpoint security software](#) enables businesses to protect devices that employees use for work purposes either on a network or in the cloud from cyber threats.

The modern business landscape is seeing an increasing volume of cybersecurity threats from increasingly sophisticated cyber criminals. Hackers launch a cyberattack [every 39 seconds](#), with a daily total of 2,244 attacks. Endpoints are one of the most common targets, given the sheer number of them in use to connect to networks. According to [Strategy Analytics insight](#), there were already 22 billion connected devices in 2018, which is predicted to rise to 38.6 billion devices by 2025 and 50 billion devices by 2030. As a result, [Verizon's threat report](#) found that up to 30% of data breaches involved [malware](#) being installed on endpoints.

Every endpoint that connects to the corporate network is a vulnerability, providing a potential entry point for cyber criminals. Therefore, every device an employee uses to connect to any business system or resource carries the risk of becoming the chosen route for hacking into an organization. These devices can be exploited by malware that could leak or steal sensitive data from the business.

In the face of this, it is imperative for businesses to deploy solutions that can analyze, detect, then block and contain cyber attacks as they happen. Organizations also need to collaborate with one another and utilize technologies that provide their IT and security teams with visibility into advanced threats, enabling them to quickly detect security risks for swift remediation of potential issues.



## Why Is Endpoint Security Important?

Endpoint security technology plays a vital role in protecting organizations from the increasingly dangerous threat landscape. Some of the key benefits of an endpoint security approach include:

1. **Protecting all endpoints:** As employees now connect via not only a growing number of endpoints but also different types of devices, it is vital for organizations to ensure they do so securely. They also need to ensure that the data on those devices is secure and cannot be lost or stolen.
2. **Securing remote working:** The rise in device usage is linked to new ways of getting work done, such as [bring your own device \(BYOD\)](#) and remote working policies. These policies enable employees to be as effective as possible wherever they are and on any device. However, they also make it more difficult to ensure users are working securely, thus creating vulnerabilities for hackers to exploit. Protecting the device with an endpoint security platform is crucial.
3. **Sophisticated threat protection:** Hackers are deploying more sophisticated attack methods that see them come up with new ways of gaining access to corporate networks, stealing data, and manipulating employees into giving up sensitive information. Endpoint protection is critical to securing the modern enterprise and preventing cyber criminals from gaining access to their networks.
4. **Protecting identity:** As employees connect to business systems via various devices and from different networks and locations, the traditional process of protecting the business perimeter is no longer viable. Endpoint security ensures that the business puts security on employees' devices, enabling them to work safely regardless of how and where they connect to corporate data and resources.

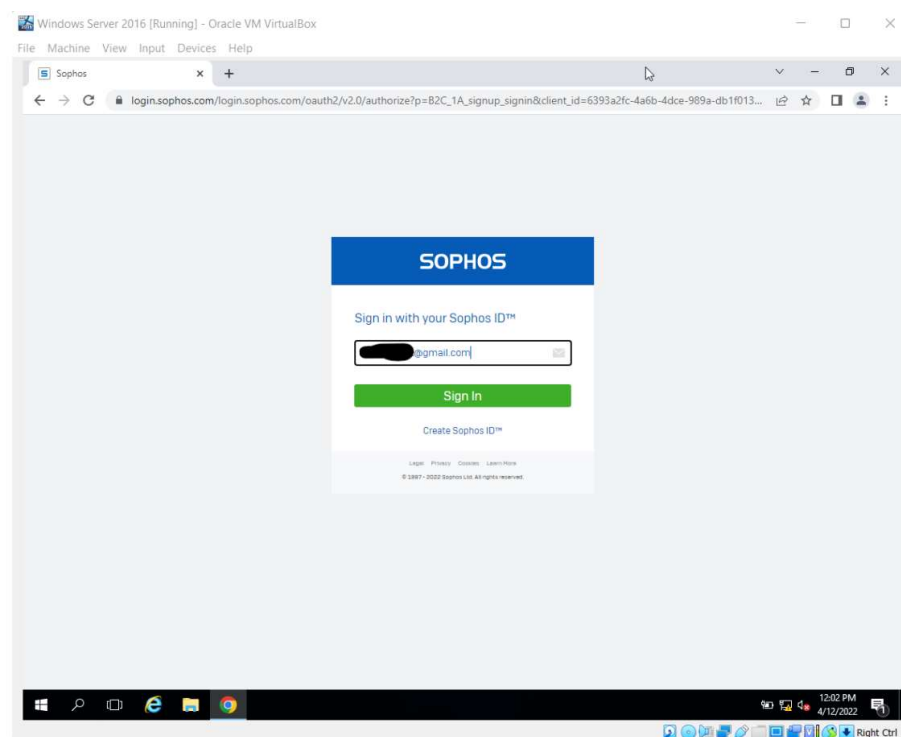
## 10.1 SOPHOS installation

**Sophos Endpoint Protection** —an on-premises solution that offers anti-malware, application control, DLP, IPS, and MDM features.

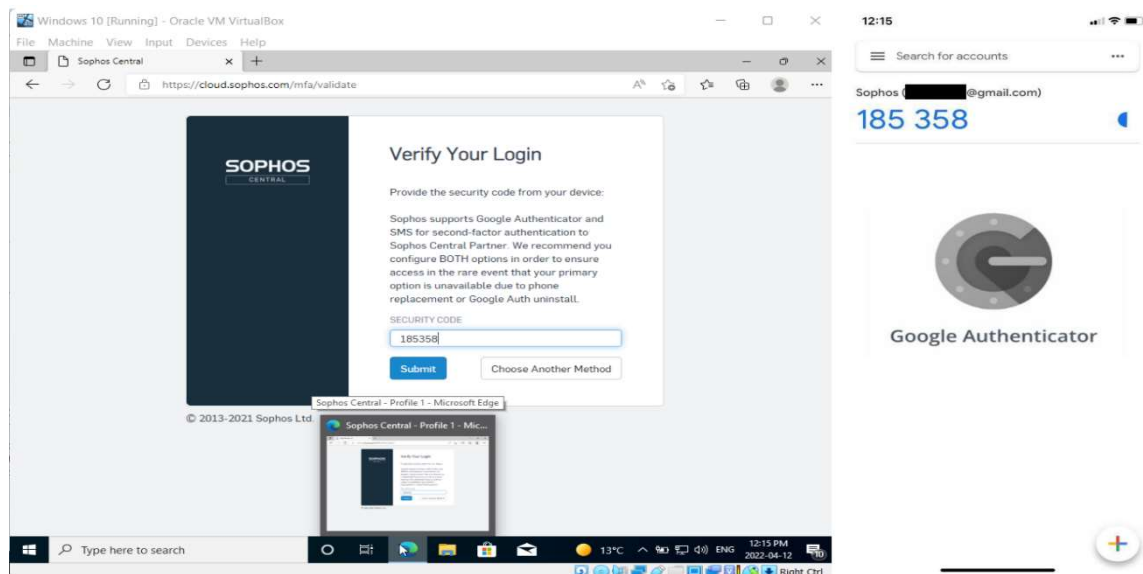
**Sophos Intercept X Endpoint** —a cloud-based solution that builds on top of the Sophos Endpoint Protection features and offers additional capabilities. Notable features include deep learning analysis, advanced ransomware protection, EDR, XDR, and MTR.



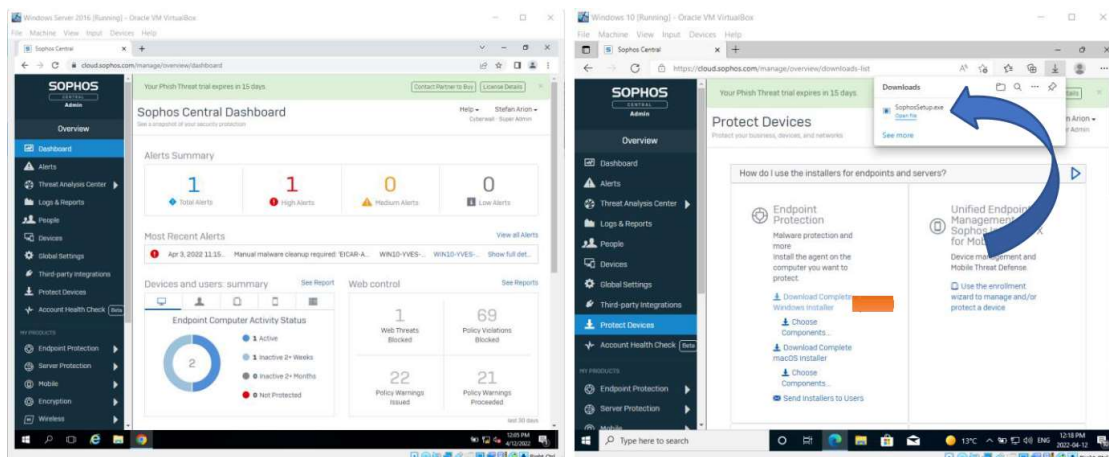
Open browser on Windows 10 virtual PC. Type <https://cloud.sophos.com/> once login screen appears, put in the registered email address and password.



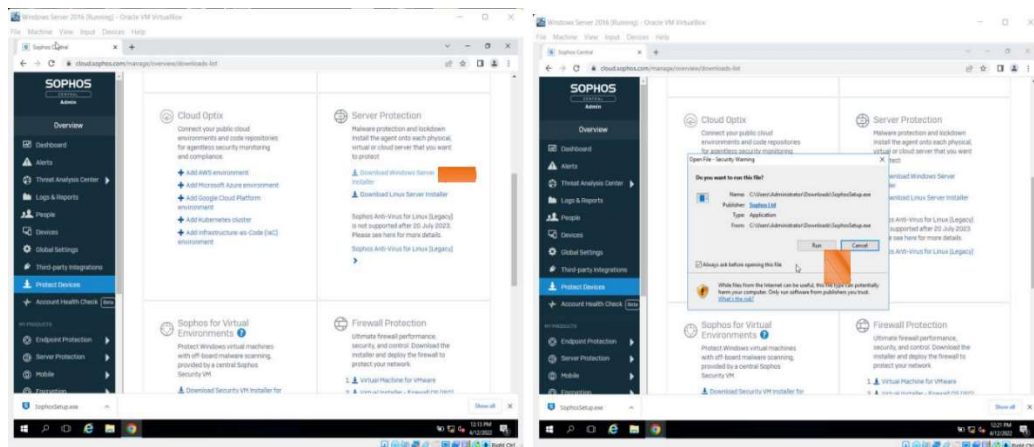
We enter the security key obtained through the Google Authenticator application installed on the smartphone.



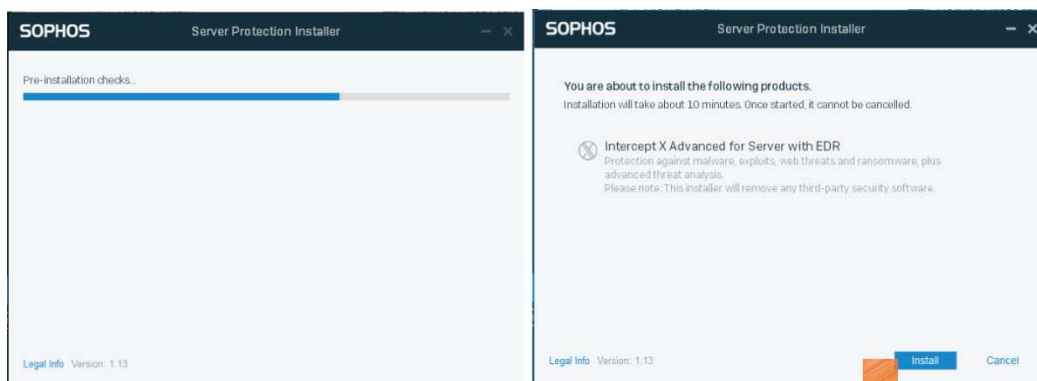
Select “Protected Devices” from menu on left. We’ll download “Endpoint Protection”. You install “Server Protection” too. Click on “Download Complete Windows Installer” under Endpoint Protection.



It'll start downloading the client on local machine. Once completed, go to the directory where client is downloaded and double click "SophosSetup.exe". Click "Run" on first screen.

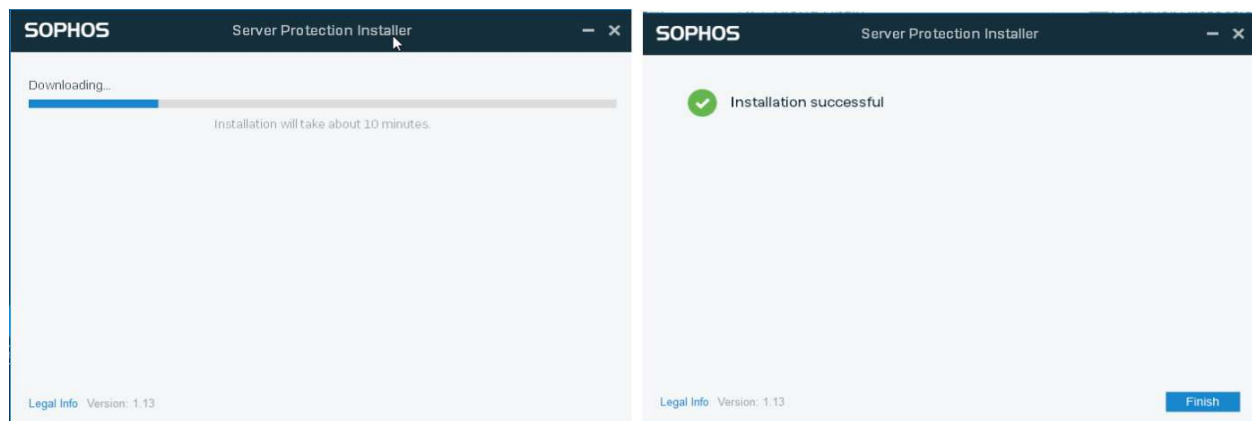


Click "Install"



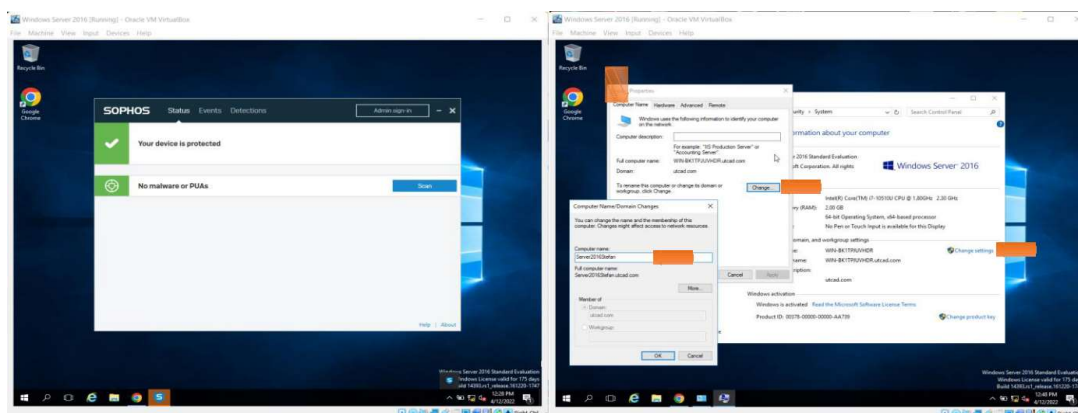
It'll take a while because it'll download and update

Once completed, click "Finish"

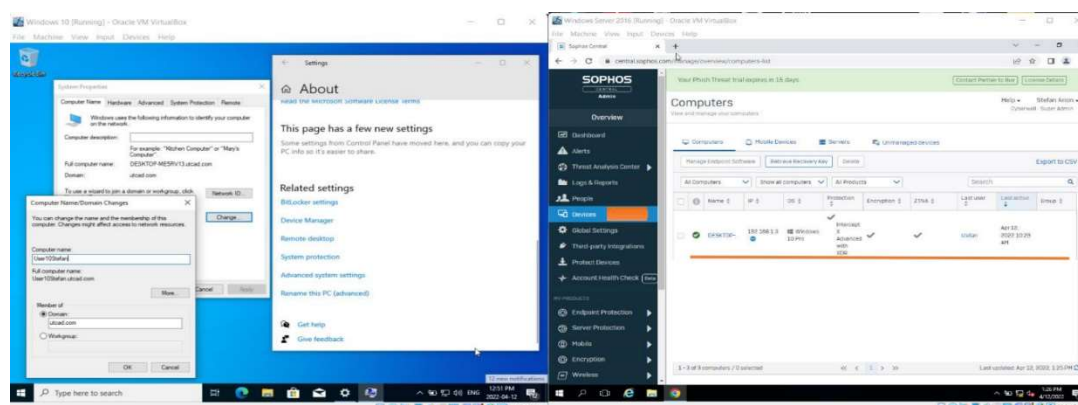


After the application is installed, run the application, and see if the program is active and functional for our server to be easily identified in the device list, the computer name must be changed.

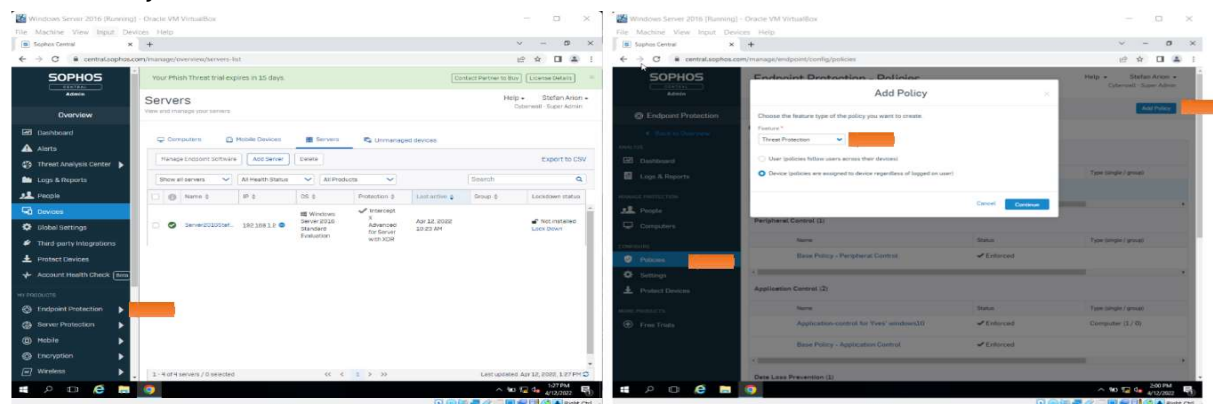
Access system properties and change settings. We change the name of the computer for Windows Server.



After PC reboots, open browser and go to <https://cloud.sophos.com/>. After login, click “Devices” from menu on left. In these lists in the Computers and Servers section we can see the registered active devices.



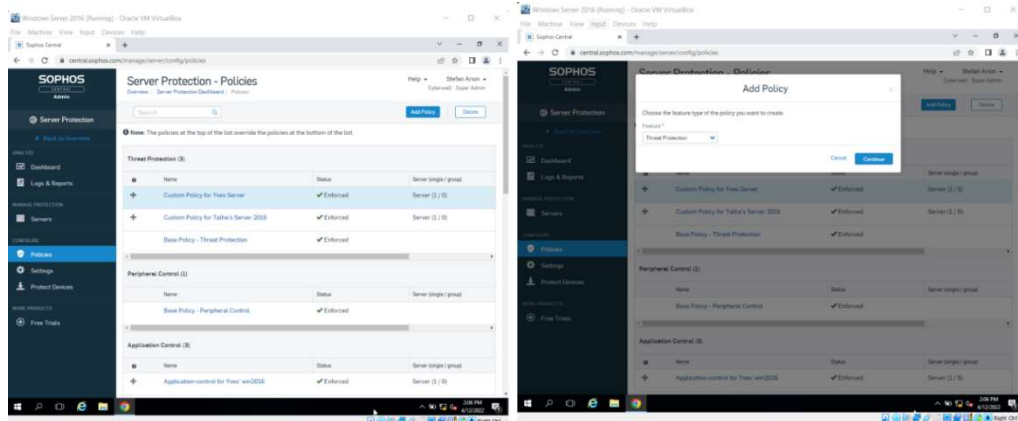
After login, click “Endpoint Protection” from menu on left. Click “Policies”. After click “Add Policy”



To create or edit a Threat Protection policy:

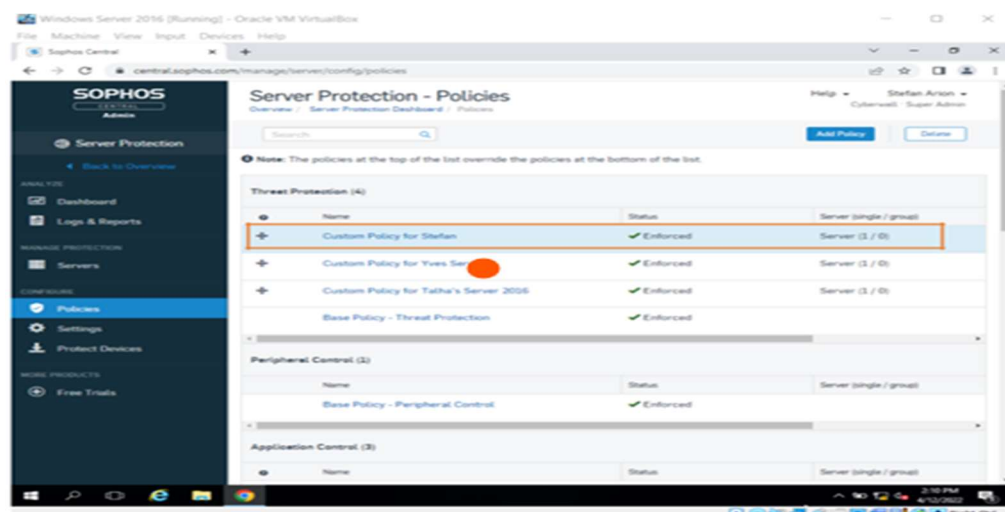
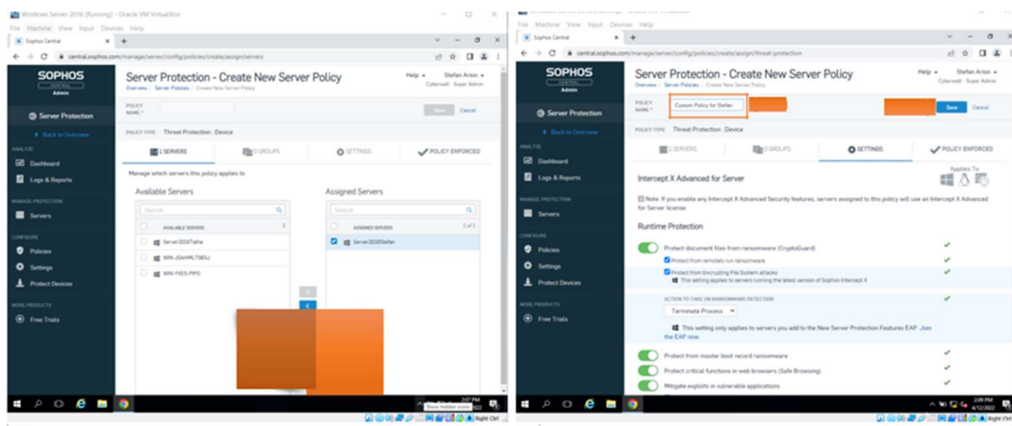
Open Sophos Central and go to Server Protection > Policies.

Click on a Threat Protection policy or click Add Policy to create a new one.



On the Servers tab, select the Security VMs you want to apply the policy to.

On the Settings tab, enter the settings you want

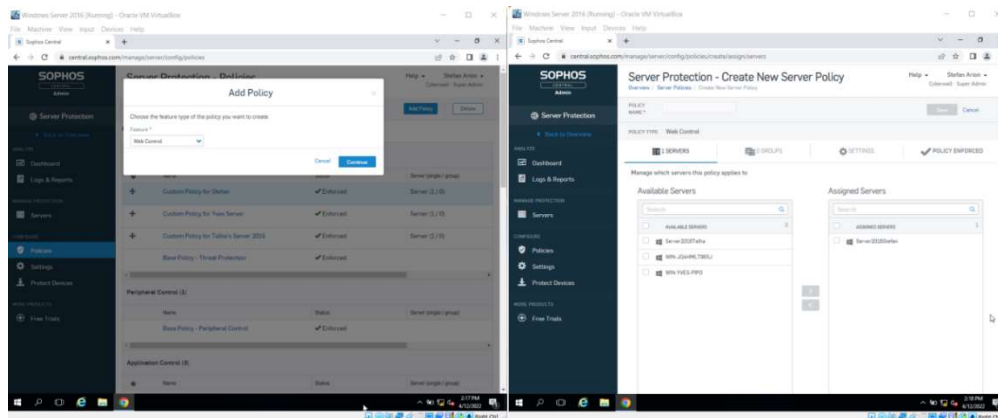


Go to Server Protection > Policies to apply web control.

To set up a policy, do as follows:

Create a Web Control policy. See Create or Edit a Policy.

Open the policy's Settings tab and configure it as described below. Make sure the policy is turned on. For more information on how we assess threats see Sophos Web Security and Control Test Site. Additional security options



Select Additional security options to configure access to advertisements, uncategorized sites, and risky downloads.

Block risky downloads: This option blocks risky file types but allows advertisements and uncategorized files.

None: This option allows risky file types, advertisements, and uncategorized files.

Let me specify: This allows you to set advertisements and uncategorized file types to Allow or Block.

It also allows you to set Risky File Types to:

Recommended: This gives you the settings shown in the table of file types below.

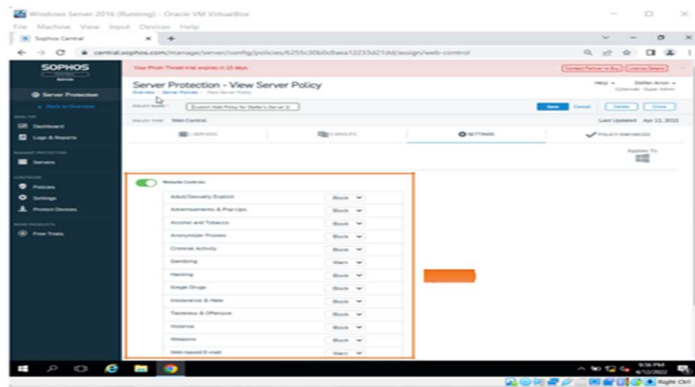
Allow: Allows all risky file types.

Warn: Warns the user that a file may be risky before they can download it.

Block: Blocks all risky file types.

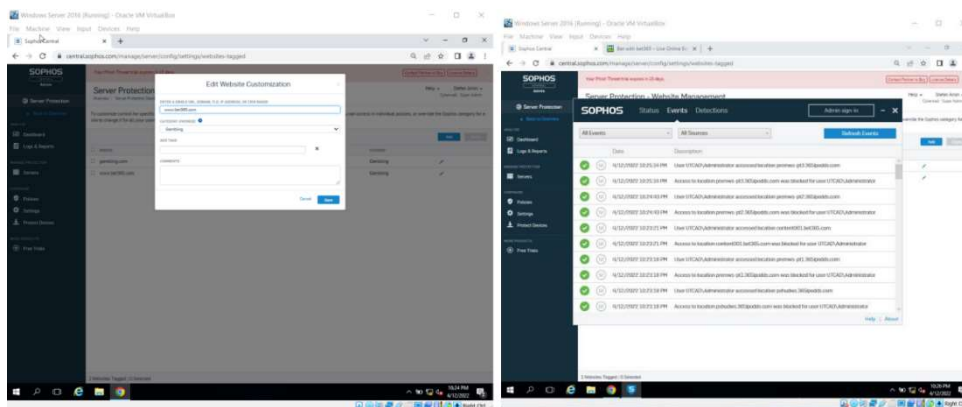
Let me specify: This allows you to set several individual file types to Allow, Warn, or Block. We apply the settings. Click "Save"

We access a site that contains a security risk, and we notice its blocking.



You can manually set up sites that are at risk and are not noticed by the Sophos system.

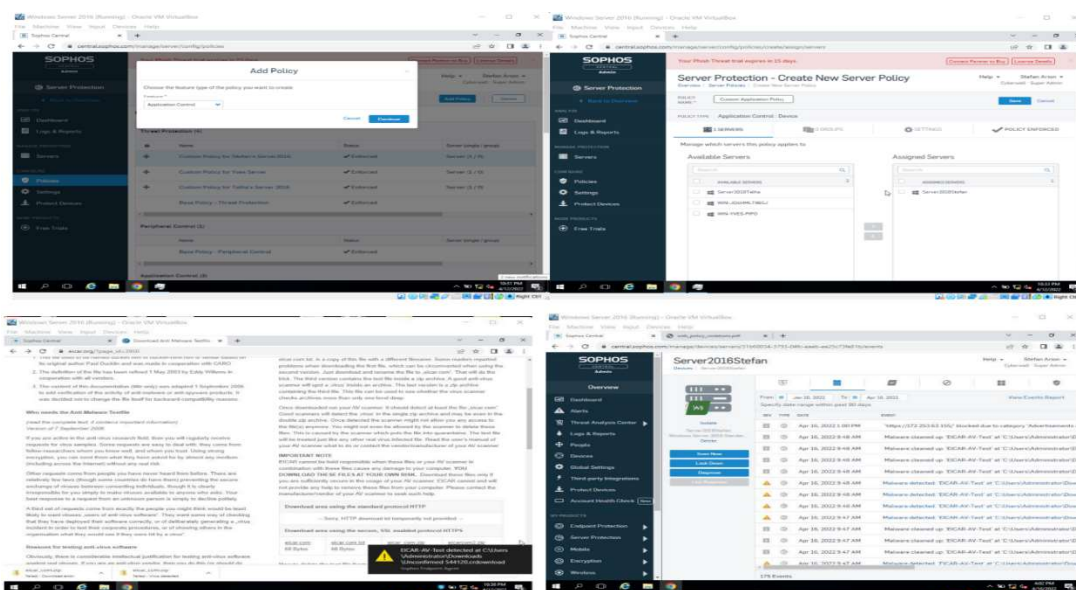
You can check logs from Sophos client. Open Sophos client and click “Events”.



Go to Server Protection > Policies to control applications.

To set up a policy, do as follows: Create an Application Control policy. See Create or Edit a Policy.

Open the policy's Settings tab and configure the policy as described below. Make sure the policy is turned on.



The screenshot displays the Sophos Central dashboard interface. The left sidebar contains navigation options: Overview, Dashboard (selected), Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Third-party Integrations, and Protect Devices. The main content area shows an Alerts Summary with 1 Total Alerts, 1 High Alerts, 0 Medium Alerts, and 0 Low Alerts. Below this, the 'Most Recent Alerts' section lists an alert from April 3, 2022, at 11:15, regarding a manual malware cleanup required. The 'Devices and users: summary' section includes a donut chart for 'Endpoint Computer Activity Status' showing 3 total devices (2 Active, 1 Inactive 2+ Weeks, 0 Inactive 2+ Months, 0 Not Protected). The 'Web control' section shows 1 Web Threats Blocked, 93 Policy Violations Blocked, 52 Policy Warnings Issued, and 50 Policy Warnings Proceeded over the last 30 days. At the bottom, a table lists various domains and their associated server names and actions.

| Domain            | Count 1 | Count 2 | Server Name          | Action   |
|-------------------|---------|---------|----------------------|----------|
| images4us.com     | 3       | 3       | Server2016Talha (1)  |          |
| 888casino.com     | 2       | 2       | Server2016Stefan (2) | Gambling |
| 888sport.ca       | 1       | 1       | Server2016Talha (1)  | Gambling |
| partycasino.ca    | 1       | 1       | Server2016Stefan (1) | Gambling |
| gamblingonline.co | 1       | 1       | Server2016Stefan (1) | Gambling |
|                   |         |         | Server2016Stefan (4) | Gambling |

## 11. Incident Response

### What is Incident Response?

- Incident response is a term used to describe **the process** by which an organization **handles** a data breach or cyberattack.
- The goal is to quickly identify an attack, effectively manage and contain the incident and remediate the root cause to reduce the risk of future incidents.
- Typically, incident response is conducted by an organization's computer incident response team (CIRT), also known as a cyber incident response team which is comprised of security and general IT Operation staff, along with members of the legal, human resources, public relations and Senior Management.
- Stratejm's Cyber Intelligence Center (CIC) is an extension of the customers IT Security Team, responsible for certain incident response function.



### What is a Security Operations Center (SOC)

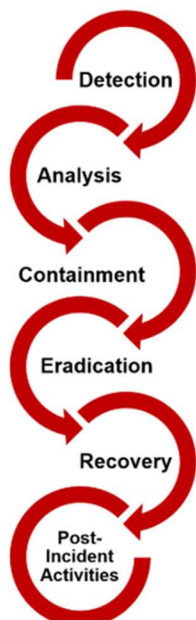
A security operations center (SOC) – is an in-house or outsourced **team of IT security professionals** that **monitors** an organization's **entire IT infrastructure**, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.

A **SOC maintains the organization's cybersecurity technologies**, and continuously **analyze event data** to find ways to improve the organization's security posture.

The key benefit of operating or outsourcing a SOC is that it **unifies the monitoring and management** of security tools and response capabilities for faster threat detection and cost-effective approach to security threats.



## Phases of Incident Response



**Detection** – Events are analyzed in order to determine whether an indicator of compromise or an indicator of an attack is observed.



**Analysis** – Collect data from tools and systems for further analysis of the IOCs and IOAs to identify the impacted, scope of the attack and containment efforts.



**Containment** – Isolate systems and contain the breach so it doesn't spread and cause further damage to your business.



**Eradication** – Eliminate the root cause of the breach. This means all malware should be securely removed, systems should be hardened and patched, and updates should be applied.



**Recovery** – Restoring and returning affected systems and devices back into your business environment for normal operations to resume.



**Post-Incident Activities** – Incident Response Team members and discuss what you've learned from the data breach.



## Preparing for the inevitable

- Despite on-going investments in **people, process** and **technology**, organizations still get breached.
- An incident response plan serves as the **blueprint** that **enables staff** to **detect, respond** to, and **recover** from security incidents.
- An organization's incident response capabilities are **not complete without planning and practicing** on how to respond to security incidents.
- The cyber incident response team must achieve their tasks and **work together** to accomplish the organization's mission of a successful response.
- The purpose of the tabletop exercise is to **validate your response capabilities** and to **identify strengths and weaknesses** before an actual incident occurs.
- **Together we make it Safer**



## Organizational Approach to Incident Response

Cyber incident response is an organized approach (plan) to address and manage the aftermath of a cyber security breach or attack (also known as an incident) against the organization. This plan is in place to ensure incidents have immediate action taken by the organization for each phase of the incident management process:

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

The incident response team are divided into three sections:

- Management
- Communications
- Technical

The **Technical Team** receives information about the incident, attempts to contain the threat, eradicate the malicious indicator, recover the systems and escalate to the management team if necessary.

When the **Management Team** is engaged, they will execute a formal meeting. Here, they will assess the impact the incident has on the organization and whether communication needs to be distributed.

When engaged, the **Communications Team** will distribute official communication to various stakeholders via e-mail, press releases and other statements from those in the Management Team.

These steps are to be repeated as necessary, as the Technical Team works to resolve the incident or uncover more details surrounding the incident.

## /02 Tabletop Exercise

Incident preparedness activity



# Objective

**Minimize impacts** that **cyber incidents** inflict on the organization (reliability, reputational, financial, legal, etc)

**Train** and **develop** capabilities to **respond** to cyber incidents

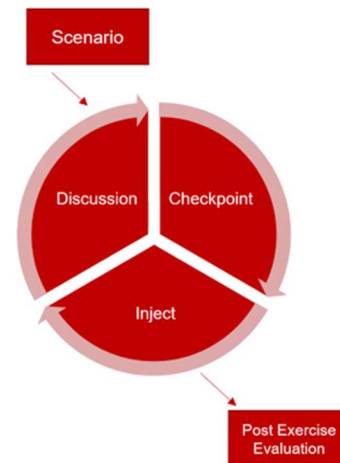
**Work together** to understand, prepare and respond to active cyber attack.

To **demonstrate** how today's **threat landscape** can cause **rapid escalation of crisis** and necessitates **swift repose**.

Identify **improvement** opportunities in incident response

The tabletop exercise is a practical way to make sure everyone on your team knows their roles and knows how certain attacks should be handled.

The tabletop exercise gets everyone on the same page through hands-on experience.



## Key Considerations (Facilitator Questions)

Have we considered Lateral movement of malware?

Do we have a dedicated decision maker?

Have we notified senior management of potential breach?

Is there evidence that data was exfiltrated?

How can we identify if other systems are vulnerable?

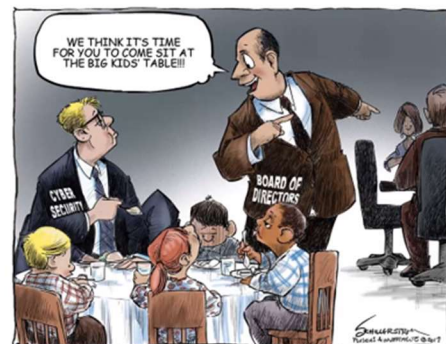
What can be done to mitigate and remediate the vulnerability?

Was there any critical data on the System? What are the recovery options?

Who is responsible of rebuilding and/or restoring the system?

Would you reach out to Cyber Insurance?

Would you invoke Incident Response retainer with third party?



# Key Considerations (Facilitator Questions)

Who owns the original ticket? What initial actions are taken?

What is the Severity/Priority of this event?

Is this incident escalated to IT Security?

If this were to occur Outside Business hours who will be contacted?

What is our Containment Strategy?

What are the technical investigatory considerations? Forensics?  
Evidence Preservation?

Who is directing your investigation and what groups from the  
organization are now involved?

How can we eradicate the threat?

Are there indicators of a crime being committed?



## 12. Importance of Vulnerability scan

A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a [cyberattack](#) can run malicious code, install [malware](#), and even steal [sensitive data](#).

Vulnerabilities can be exploited by a variety of methods, including [SQL injection](#), buffer overflows, [cross-site scripting \(XSS\)](#), and open-source exploit kits that look for known vulnerabilities and [security weaknesses in web applications](#).

Many vulnerabilities impact popular software, placing the many customers using the software at a heightened risk of a [data breach](#), or [supply chain attack](#). Such zero-day exploits are registered by MITRE as a [Common Vulnerability Exposure](#) (CVE).



### Vulnerability Examples

There are several different types of vulnerabilities, determined by which infrastructure they're found on. Vulnerabilities can be classified into six broad categories:

#### 1. Hardware

Any susceptibility to humidity, dust, soiling, natural disaster, poor [encryption](#), or firmware vulnerability.

#### 2. Software

Insufficient testing, lack of audit trail, design flaws, memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection), privilege-confusion bugs

(clickjacking, cross-site request forgery, FTP bounce attack), race conditions (symlink races, time-of-check-to-time-of-use bugs), side channel attacks, timing attacks and user interface failures (blaming the victim, race conditions, warning fatigue).

### 3. Network

Unprotected communication lines, [man-in-the-middle attacks](#), insecure network architecture, lack of authentication, default authentication, or other poor network security.

### 4. Personnel

Poor recruiting policy, lack of security awareness and training, poor adherence to security training, poor password management, or downloading malware via email attachments.

### 5. Physical site

Area subject to natural disaster, unreliable power source, or no key card access.

### 6. Organizational

Improper internal controls, lack of audit, continuity plan, security, or [incident response plan](#).

## 12.1 NESSUS Installation

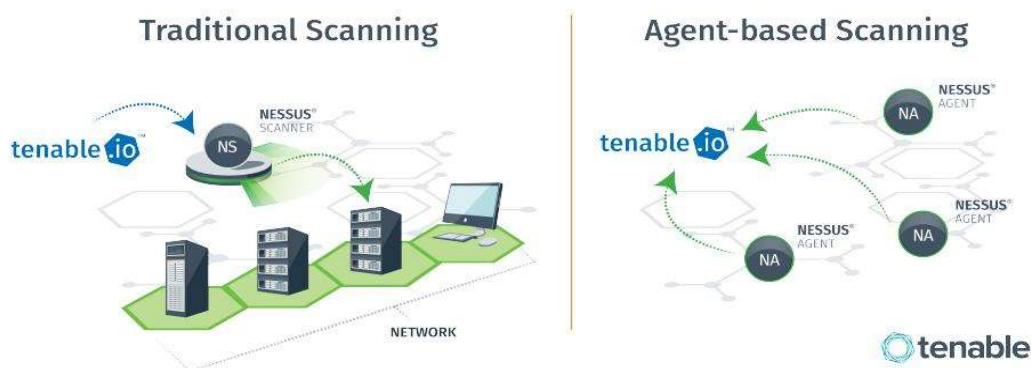
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. (NASDAQ: TENB) Examples of vulnerabilities and exposures Nessus can scan for include:

- Vulnerabilities that could allow unauthorized control or access to sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denial-of-service vulnerabilities

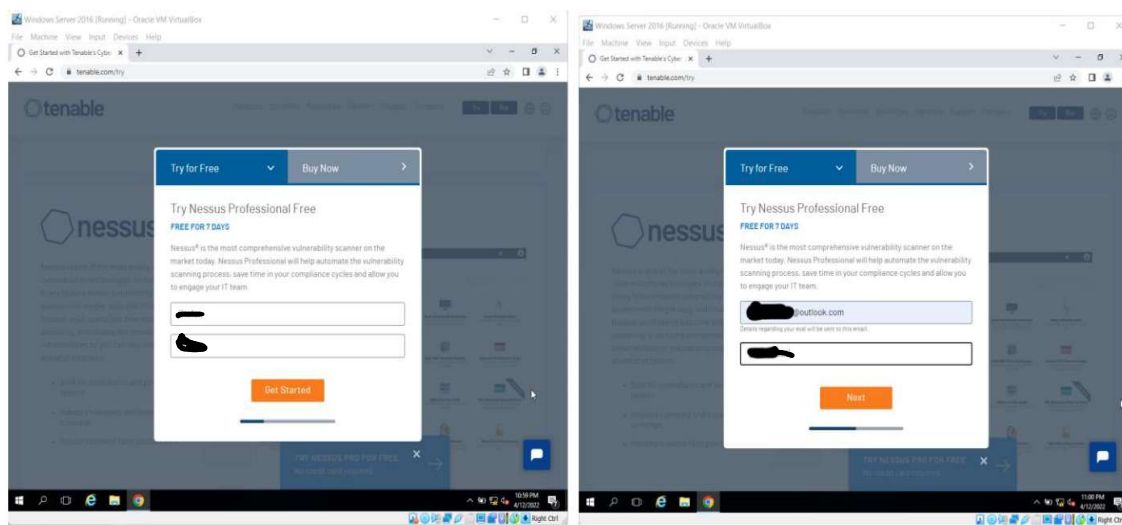
Nessus scans cover a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure.

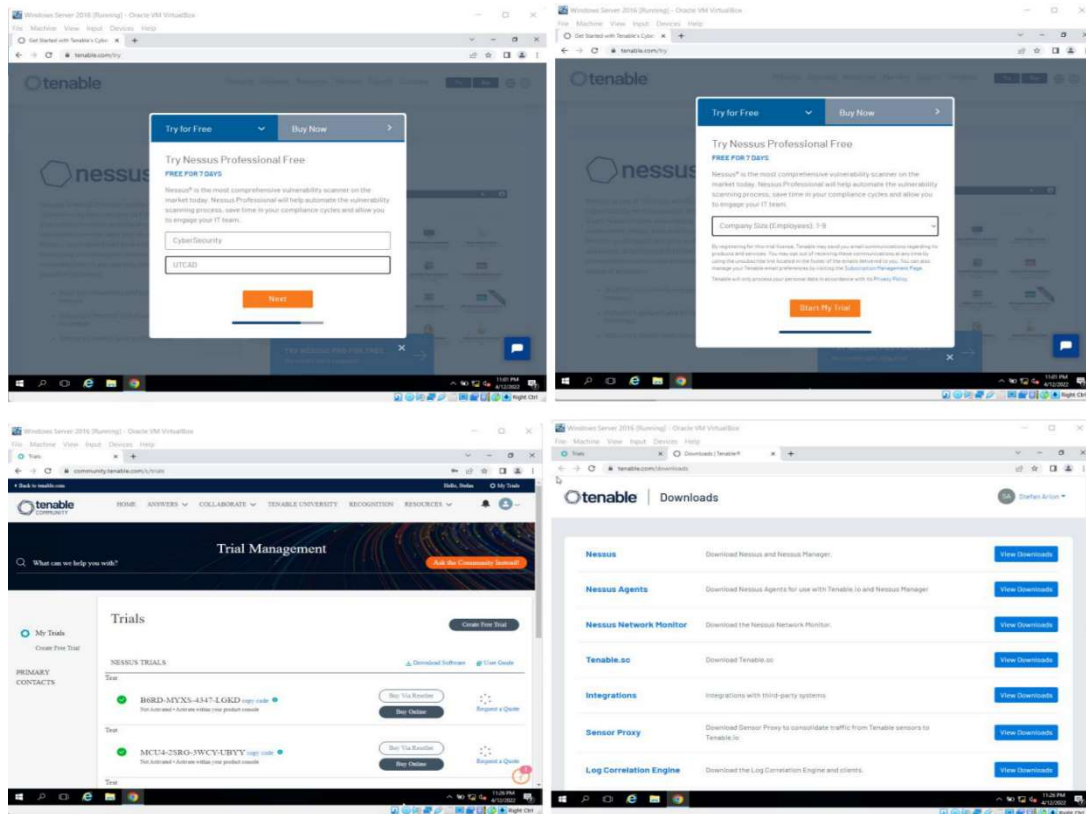
The results of the scan can be reported in various formats, such as plain text, XML, HTML and LaTeX. The results can also be saved in a knowledge base for debugging. On UNIX, scanning can be automated using a command-line client. There exist many different commercial, free, and open-source tools for both UNIX and Windows to manage individual or distributed Nessus scanners.

Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system. Nessus can also support configuration and compliance audits, SCADA audits, and PCI compliance.

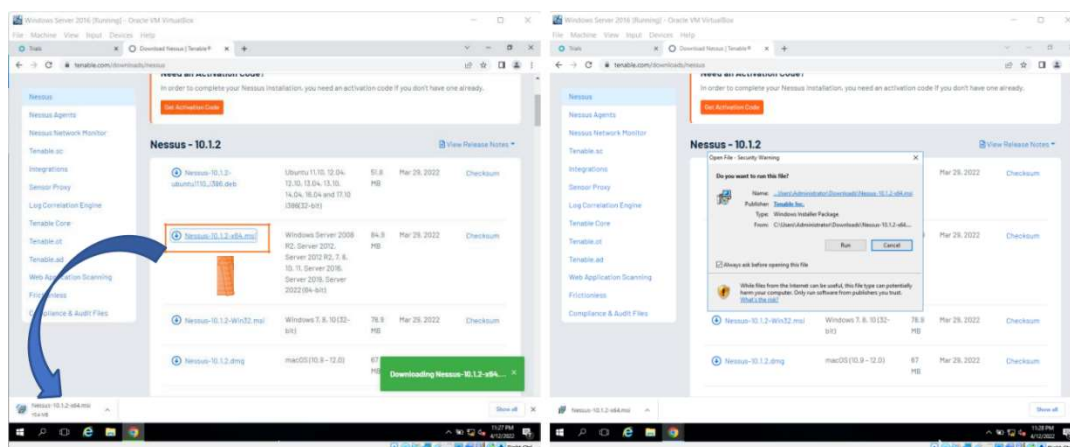


We access the Tenable.com site and register to be able to use the application, as a demo free version. We follow the following steps to register and obtain the access key to the application.

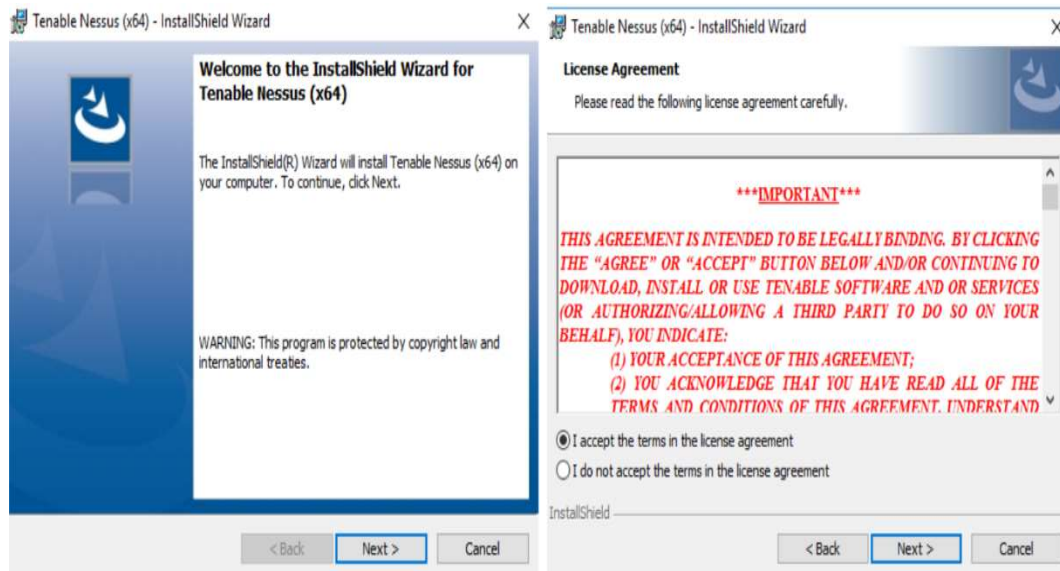




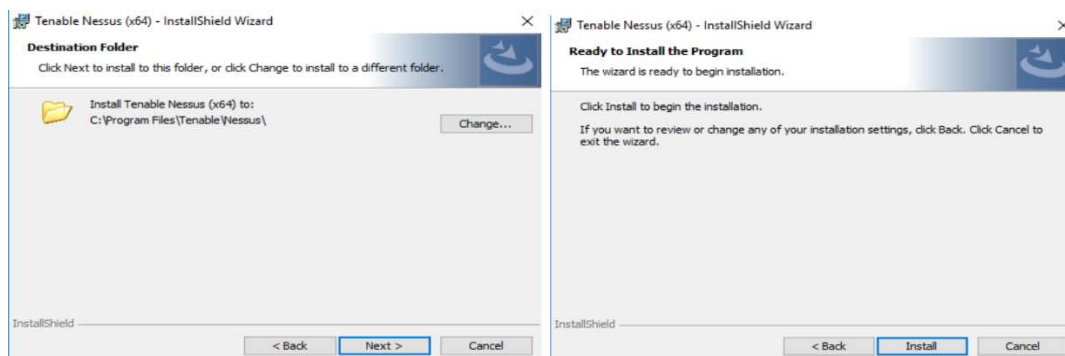
Go to <https://www.tenable.com/downloads/nessus> Search for the file ending with x64.msi and click it. It'll start downloading the file.



Once it's done downloading the file, double click on file name at bottom left corner. It'll start the installation. Click next. Read the License agreement and select "I accept the terms in the license agreement". Click Next.

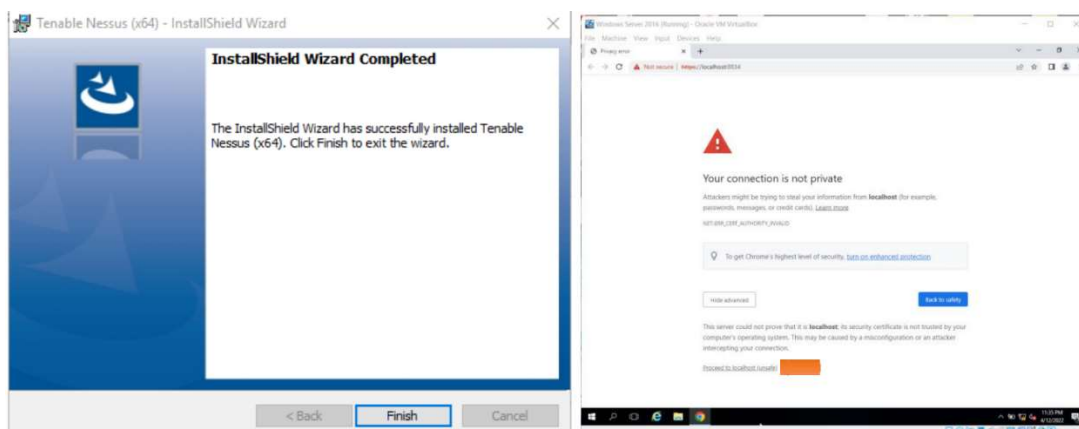


Next, it'll ask for the destination folder to install Nessus. If you like to change the destination, click Change or continue with default path. Click Next. Click "Install" on next screen.



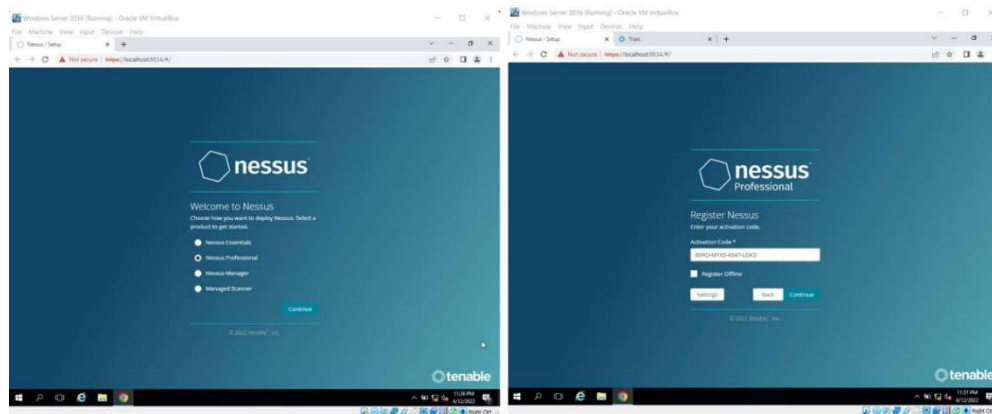
Once completed, click Finish

It'll automatically open a page in default browser. If not, go to localhost:8834. It'll give a certification error. Click "Advance" and then click "Proceed to localhost (unsafe)"



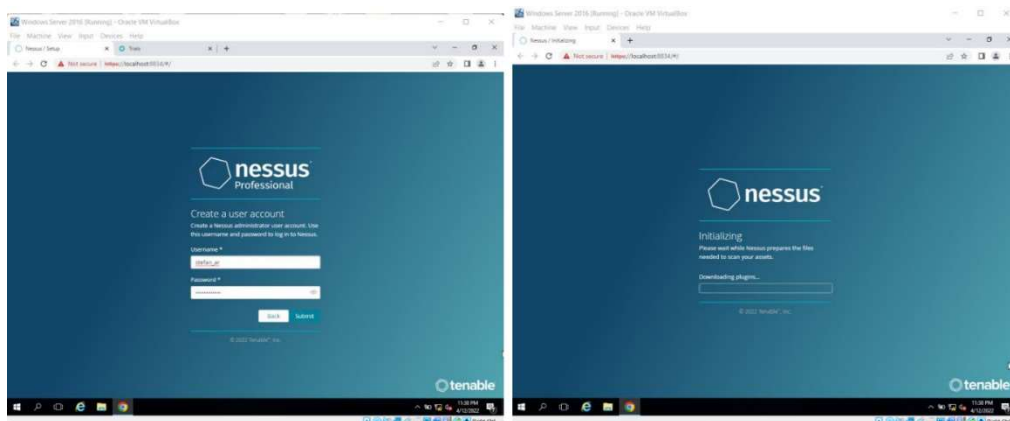
Select Nessus Professional and click Continue.

Type your activation code



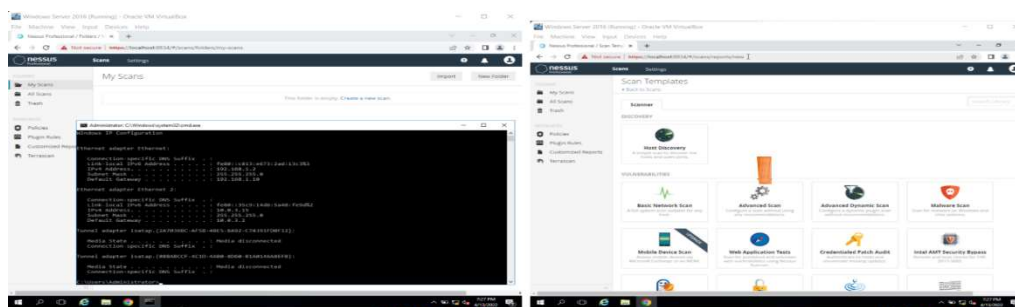
Type your username and password.

It'll start downloading the plugins. Once it's done downloading, it'll start compiling plugins.

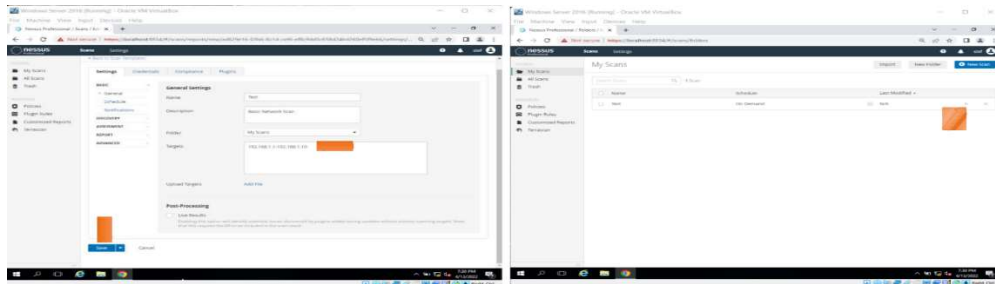


Once completed, it'll take you to the login screen. Enter Username and Password which was created earlier.

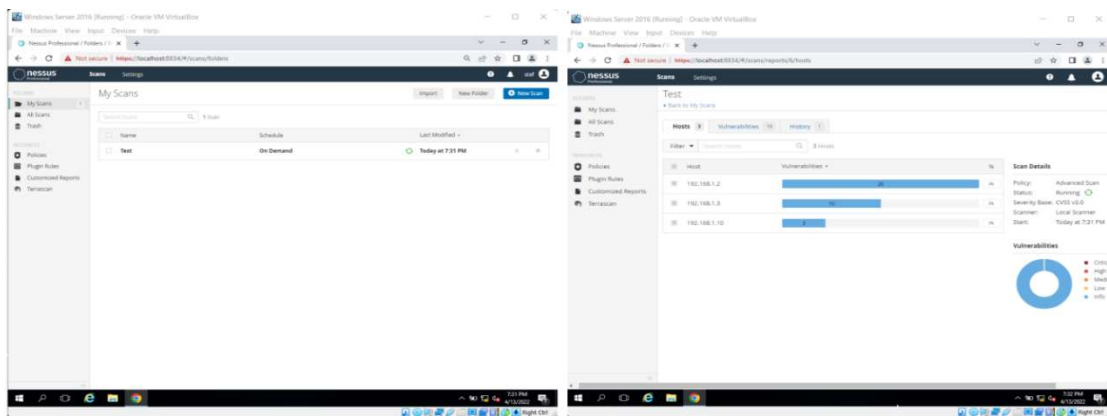
We remember used ip, accessing the IPCONFIG command line. After logging in, it'll show you a welcome screen. Open New Scan and choose Advanced Scan.



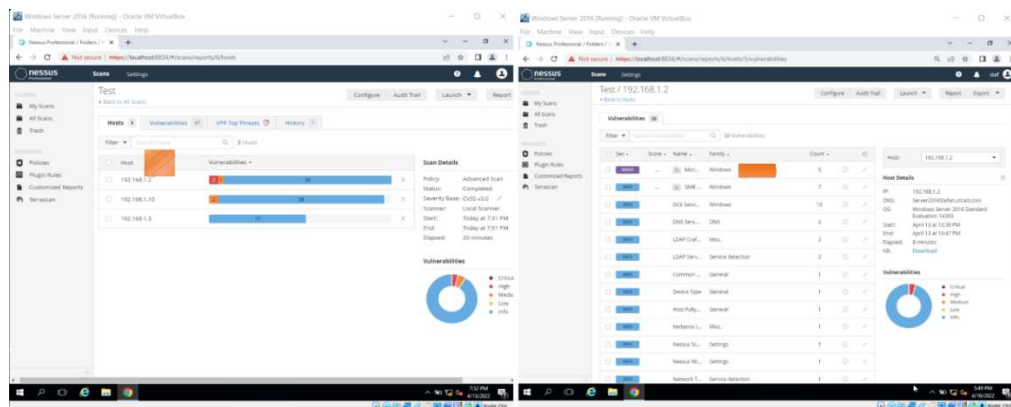
Put in IP address of targeted PC/Server and press submit. You can scan using xxx.xxx.xxx.xxx format and range. (192.168.1.0-192.168.1.10) Click “Save”



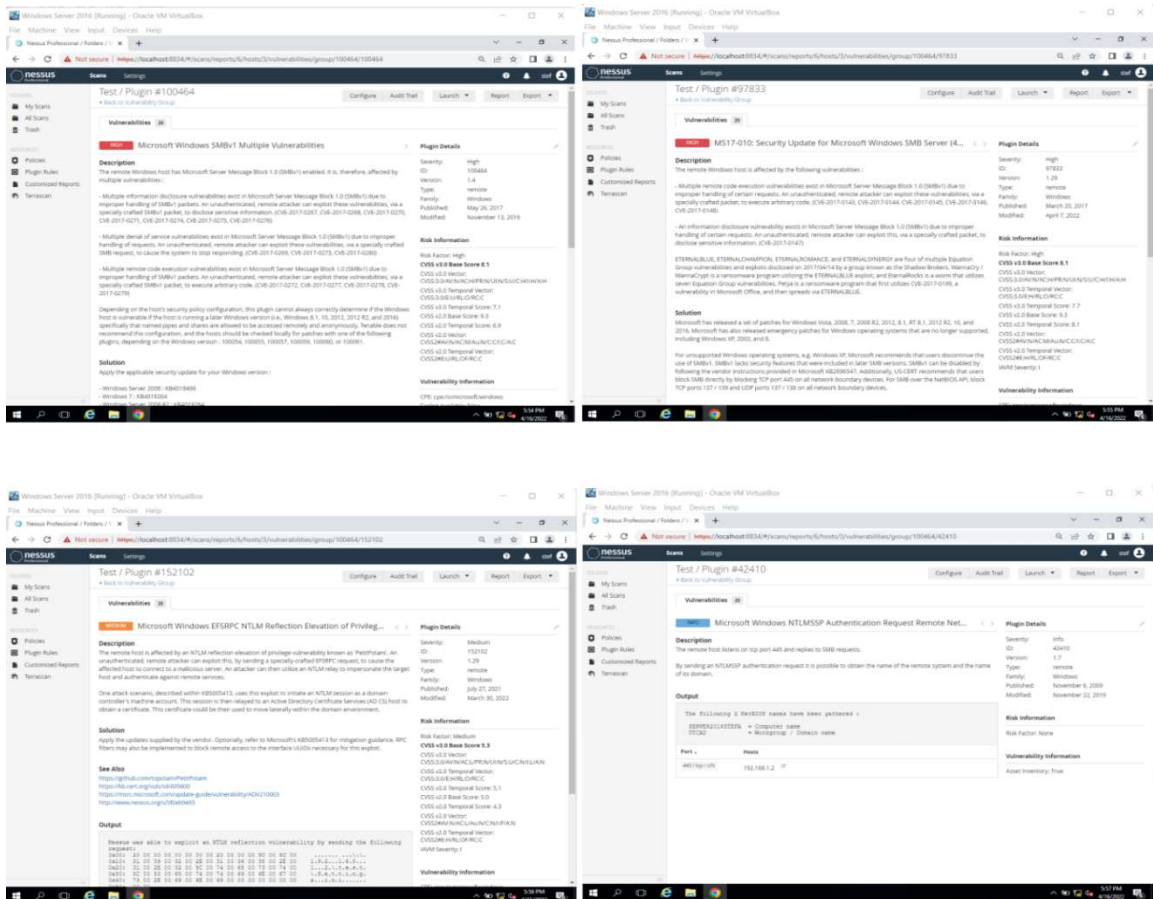
Go to My Scans to see the scanning progress. Click “run” Click on “My Basic Network Scan”. It’ll show the status on right hand side of the screen.



It’ll show all the vulnerabilities of that host. Click each one to see the details.



It’ll show you the description, solutions, and plugin details.



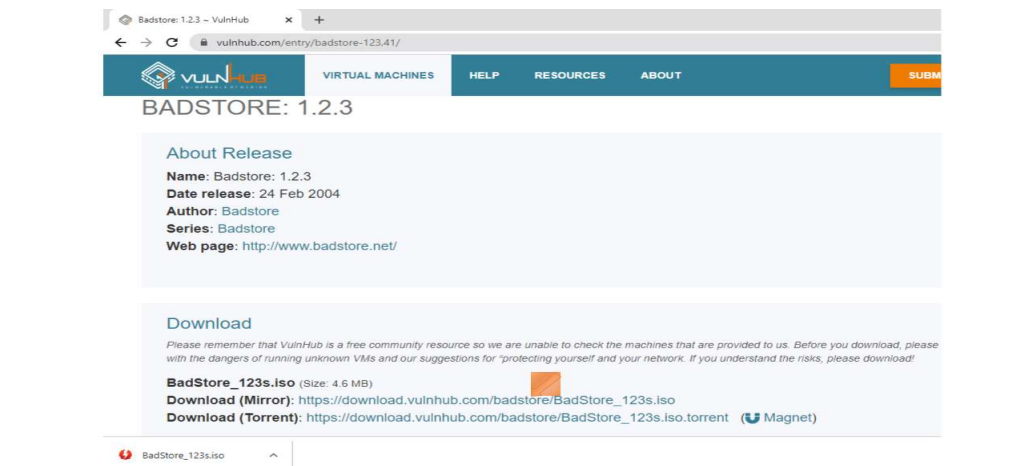
## 12.2 Deploying a dummy web server (BadStore)

We'll deploy Bad Store as dummy web server.

BadStore.net is an insecure application used for demonstration, security training, and testing purposes.

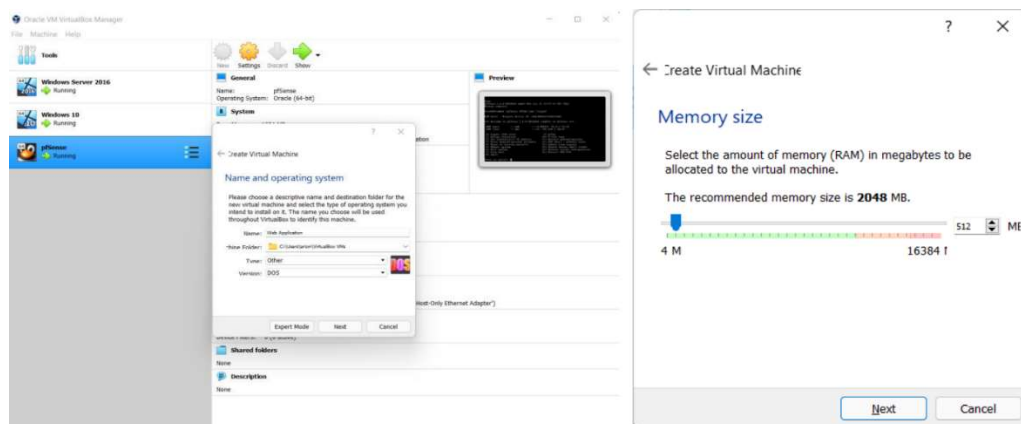
BadStore.net has been developed to illustrate the common vulnerabilities present in many applications exposed to intranets, extranets, and the Internet.

Go to <https://www.vulnhub.com/entry/badstore-123,41/>. Download Bad Store ISO file.



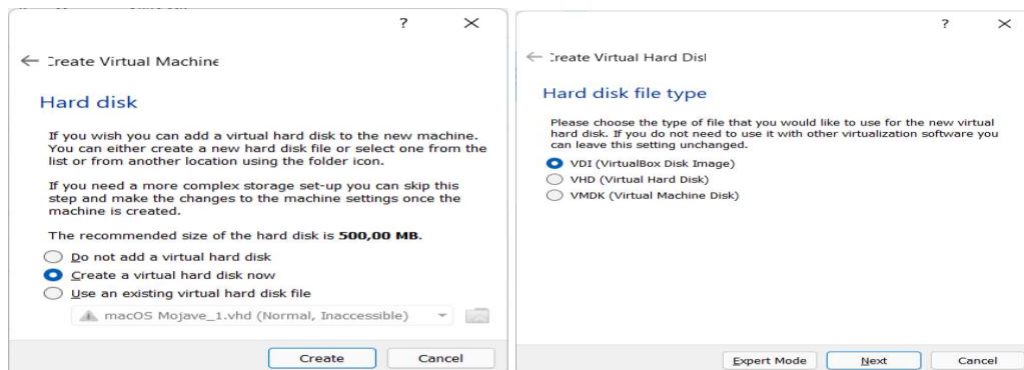
Start VirtualBox from start menu. Click on “New”

Type in name “Web Application” and select folder. It'll automatically assign Type and Version. Click “Next” Set memory size i.e. 512 MB.

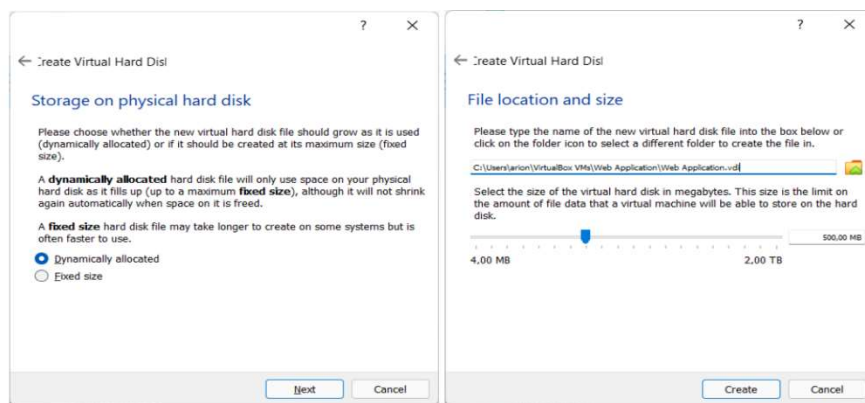


Select “Create a virtual hard disk now” and click “Create”.

Leave default value for next 2 screens and click “Next” on each option.



Leave default value for File location and size. You can change to different folder. Click “Create”.

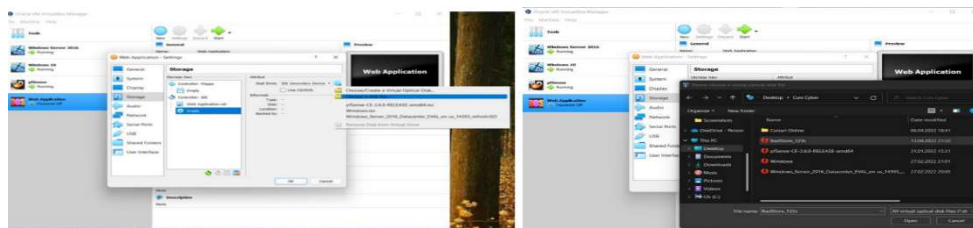


Select Web Application from left panel and click “Settings”

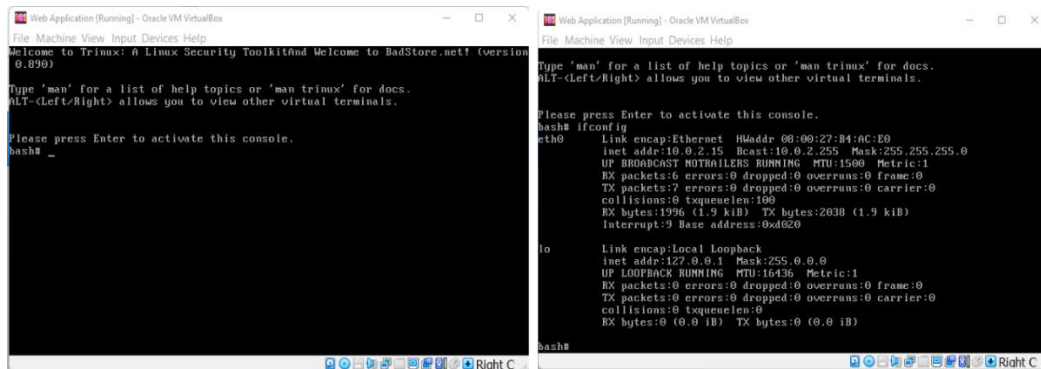
Select Storage then select “Empty” under Controller: IDE.

Click on “CD” on right corner. Select “Chose a disk file”.

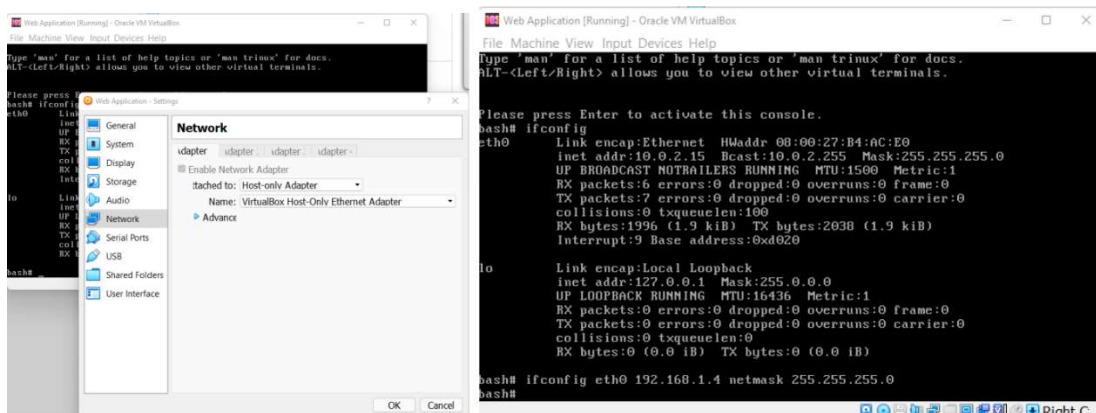
Select Bad Store ISO file which we have extracted earlier.



Press "Enter"

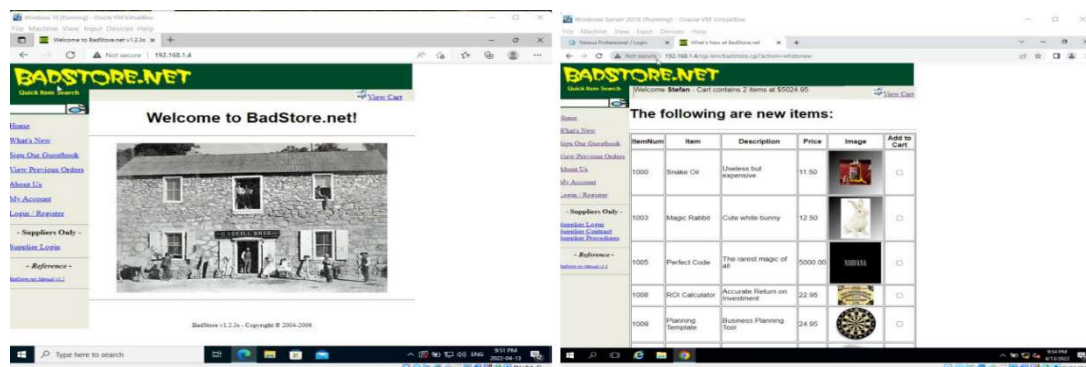


We change the type of interface. Select "Network" from left panel. Under Adapter 1, select NAT from drop down box. Then apply the ifconfig command and set the local ip and subnet mask

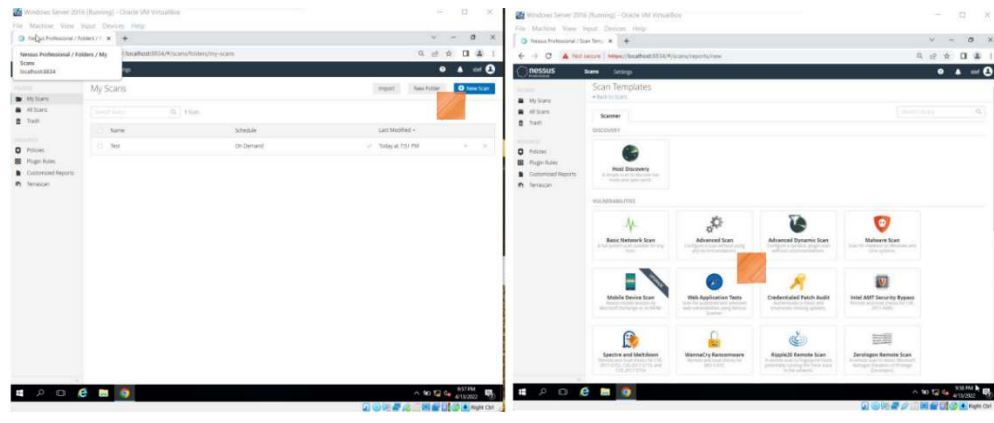


In the command line from the server and from the client we access the ping command to the web application at the address 192.168.1.4. and vice versa from the web application to the server and client we check the access

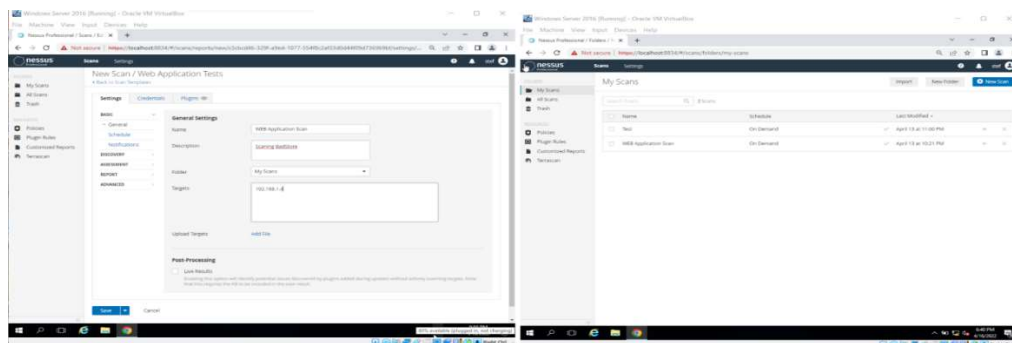
In Windows Server we open a browser and access the Bad store page at 192.168.1.4 We are viewing the full functionality of this page.



Access Nessus application. Open New Scan and choose Web application Tests.

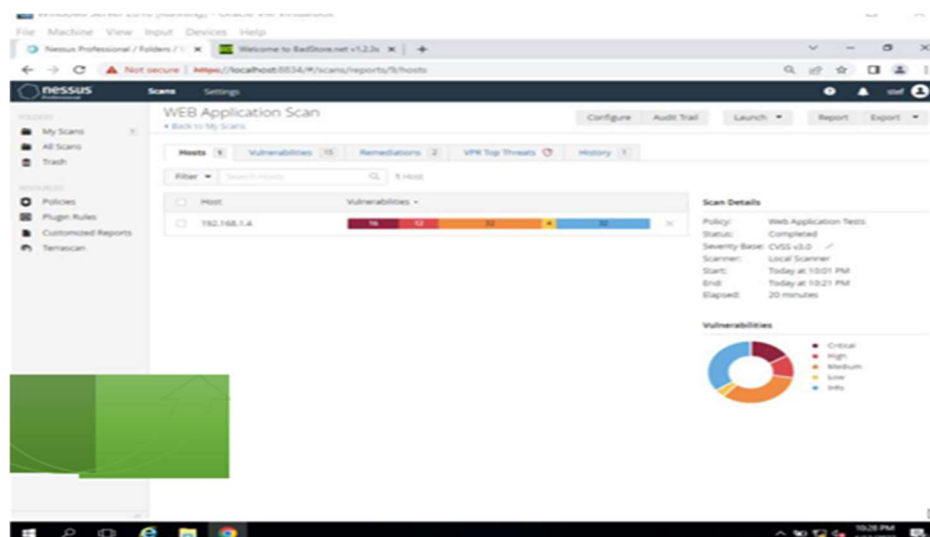


Put in IP address of targeted Web Application and press Save. Then run the scan process.



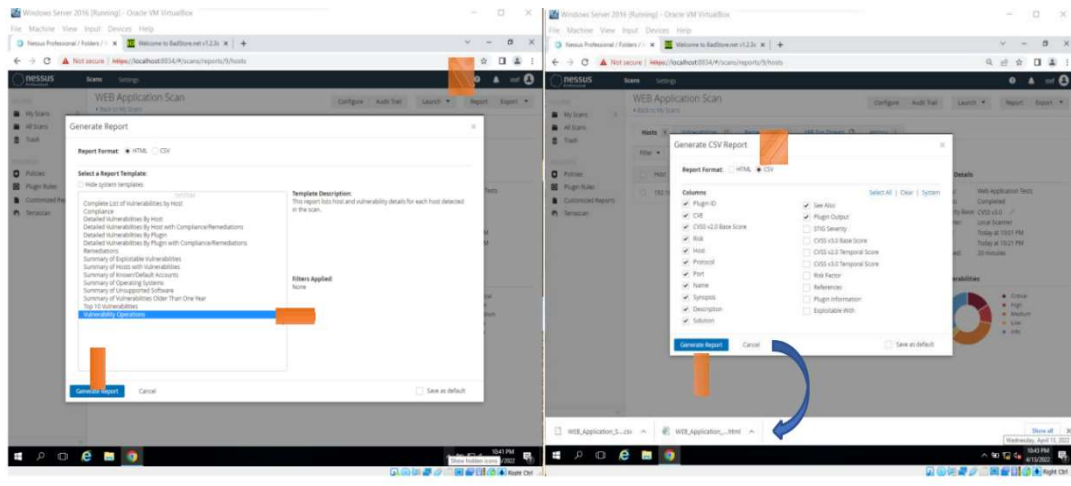
Once done, it'll show Status "Completed". Under Host you'll see the scanned hosts and their vulnerabilities.

Click on host IP address.

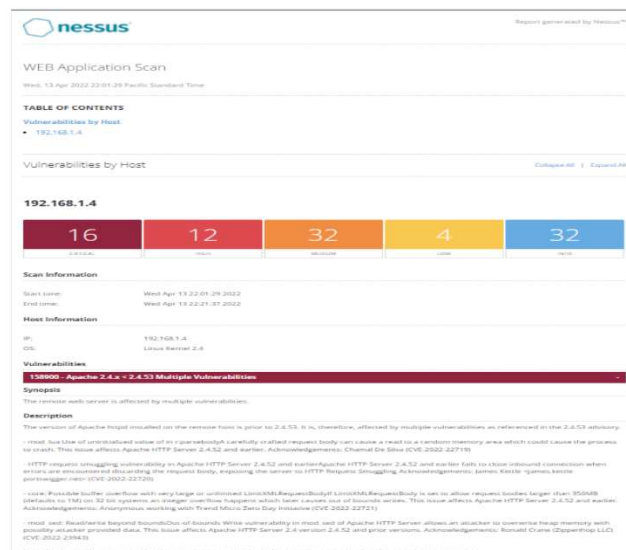


In the next step we export the report in one of the HTML or CSV formats which is opened with the help of Microsoft Excel.

These report files can be saved and sent for detailed study of site vulnerabilities.



In the following screenshots we see the generated reports.



Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that can not be seen from the network. Examples of the sorts of checks that a credentialed scan can do include checks to see if the system is running insecure versions of Adobe Acrobat or Java or if there are poor security permissions governing a service. Information Security Office (ISO) runs Nessus scanners that can run these credentialed scans; however, without accounts on the local machines, we are unable to use this functionality. ISO will create accounts on one of the Nessus scanners for departmental security administrators to do their own credentialed scans.

## Configure a Domain Account for Authenticated Scanning

To create a domain account for remote host-based auditing of a Windows server, the server must first be a supported version of Windows and be part of a domain.

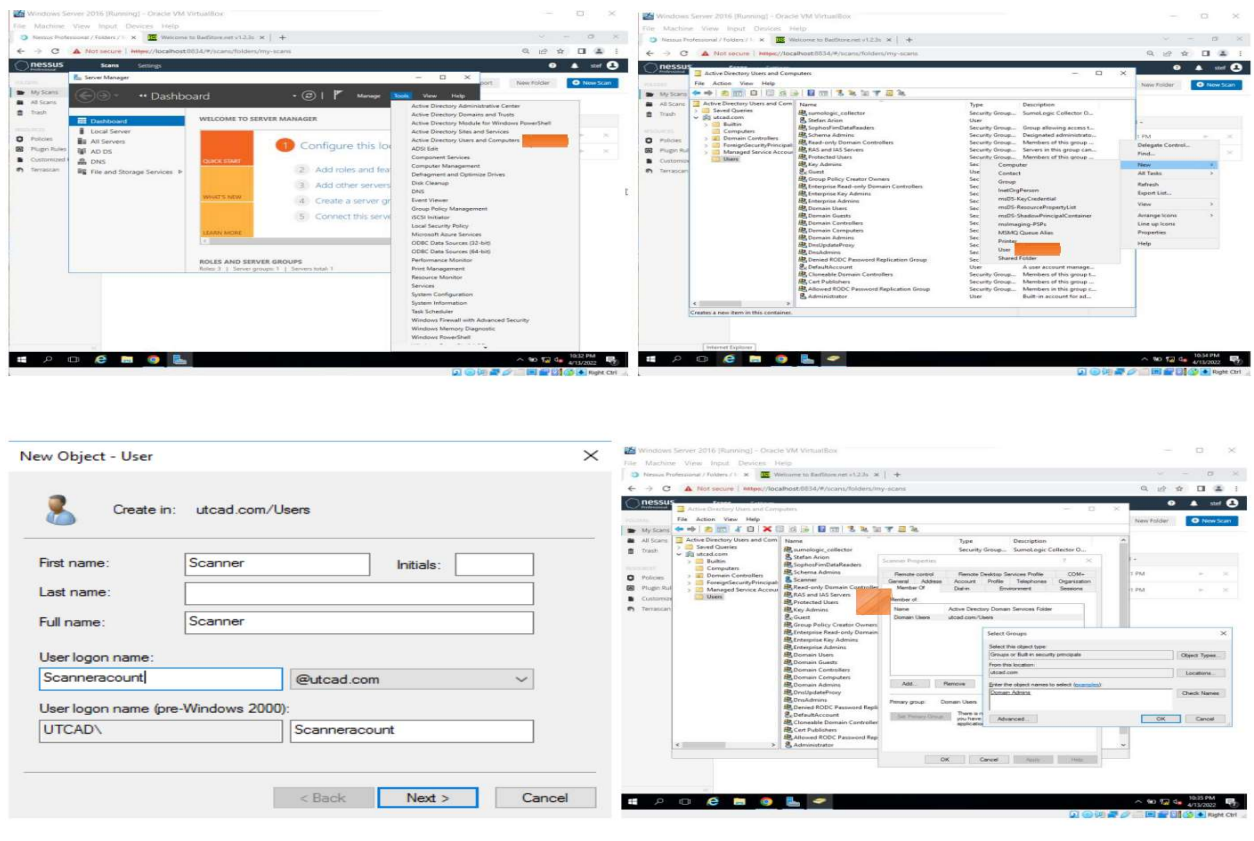
Create a Security Group called Nessus Local Access

Log in to a Domain Controller and open **Active Directory Users and Computers**.

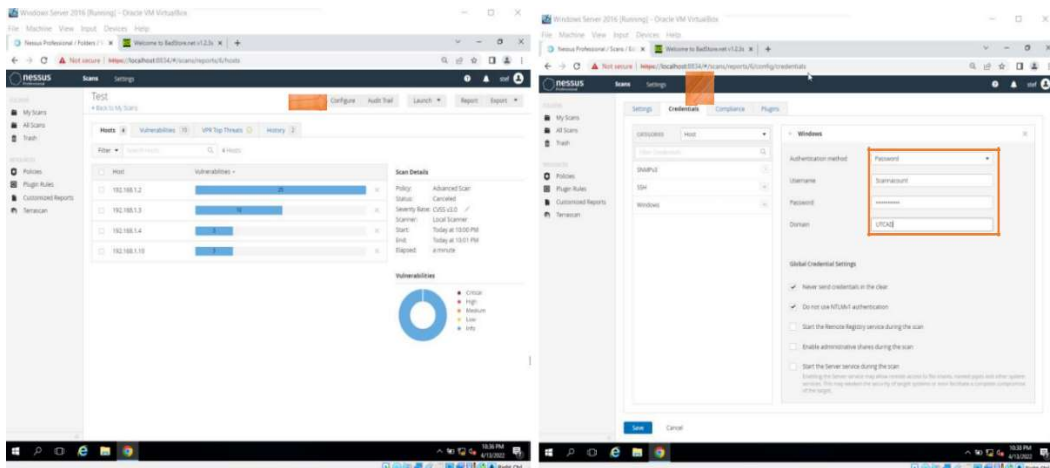
To create a security group, select **Action > New > User**.

Name the User **Scanner**. Set **Member Of** to add **Select Groups** and type **Domain Admins**.

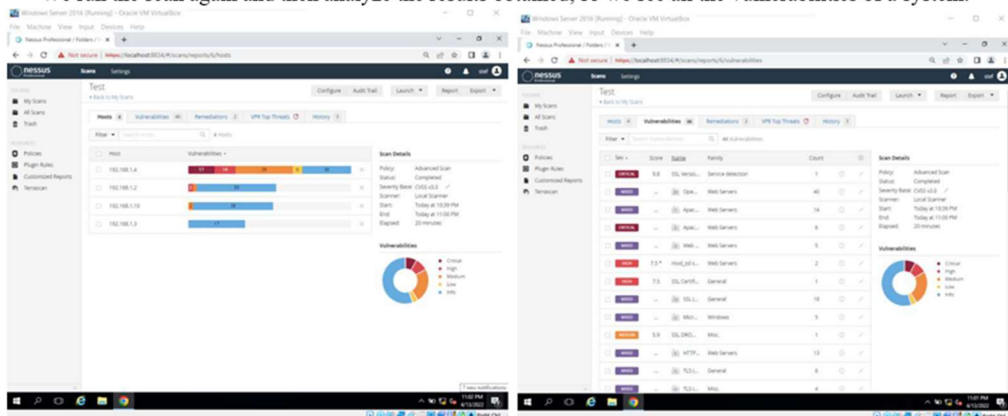
Add the account you will use to perform Nessus Windows Authenticated Scans to the Nessus Local Access group.



In the Nessus application, go to the server address, 192.168.1.2, and click Configure Initialize the credentials in the required fields and click Save



We run the scan again and then analyze the results obtained, so we see all the vulnerabilities of a system.



## 13 CIS Critical Security Controls

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.



Download CIS Controls v8

### **CIS Control 1 - Inventory and Control of Enterprise Assets**

Actively manage all enterprise hard assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately account for, monitor, and protect assets within the enterprise.

### **CIS Control 2 - Inventory and Control of Software Assets**

Actively manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

### **CIS Control 3 - Data Protection**

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

### **CIS Control 4 - Secure Configuration of Enterprise Assets and Software**

Establish and maintain the secure configuration of enterprise hard assets and software.

## **CIS Control 5 - Account Management**

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts and service accounts, to enterprise assets and software.

## **CIS Control 6 - Access Control Management**

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

## **CIS Control 7 - Continuous Vulnerability Management**

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure in order to remediate and minimize the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

## **CIS Control 8 - Audit Log Management**

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

## **CIS Control 9 - Email and Web Browser Protections**

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

## **CIS Control 10 - Malware Defenses**

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

## **CIS Control 11 - Data Recovery**

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

## **CIS Control 12 - Network Infrastructure Management**

Establish, implement, and actively manage (e.g., track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

## **CIS Control 13 - Network Monitoring and Defense**

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

## **CIS Control 14 - Security Awareness and Skills Training**

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

## **CIS Control 15 - Service Provider Management**

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

## **CIS Control 16 - Application Software Security**

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

## **CIS Control 17 - Incident Response Management**

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, communications) to prepare, detect, and quickly respond to an attack.

## **CIS Control 18 - Penetration Testing**

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (e.g., people, processes, technology), and simulating the objectives and actions of an attacker.

## 14. Cyber Security Questions & Answers

### 1. Explain risk, vulnerability, and threat?

*TIP: A good way to start this answer is by explaining vulnerability, threat, and then risk. Back this up with an easy-to-understand example.* Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when the vulnerability is exploited by the threat e.g., Default username and password for a server – An attacker can easily crack into this server and compromise it

### 2. What is the difference between Asymmetric and Symmetric encryption, and which one is better?

*TIP: Keep the answer simple as this is a vast topic.* Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption. Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel. Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using a symmetric process.

### 3. What is an IPS and how does it differ from IDS?

IDS is an intrusion detection system whereas an IPS is an intrusion prevention system. IDS will just detect the intrusion and will leave the rest to the administrator for further action whereas an IPS will detect the intrusion and will take further action to prevent the intrusion. Another difference is the positioning of the devices in the network. Although they work on the same basic concept the placement is different.

### 4. What is XSS, and how will you mitigate it?

Cross site scripting is a JavaScript vulnerability in web applications. The easiest way to explain this is a case when a user enters a script in the client-side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client-side. Countermeasures of XSS are input validation, implementing a CSP (Content security policy), etc.

### 5. What is the difference between encryption and hashing?

Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.

Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

### 6. Are you a coder/developer or know any coding languages?

*TIP: You are not expected to be a PRO; understanding of the language will do the job.*

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to

automate tasks, exploit development etc. A little knowledge of the three can be of great advantage – both in the interview and on the floor.

**7. What is CSRF?**

Cross-Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples, and countermeasures.

**8. What is a Security Misconfiguration?**

Security misconfiguration is a vulnerability when a device/application/network is configured in a way that can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

**9. What is a Black hat, white hat, and grey hat hacker?** Black hat hackers are those who hack without authority. White hat hackers are authorized to perform a hacking attempt under a signed NDA. Grey hat hackers are white hat hackers who sometimes perform unauthorized activities.

**10. What is a firewall?** A firewall is a device that allows/blocks traffic as per the defined set of rules. These are placed on the boundary of trusted and untrusted networks.

**11. How do you keep yourself updated with the information security news?**

Be sure to check and follow a few security forums so that you get regular updates on what is happening in the market and about the latest trends and incidents.

**12. The world has recently been hit by ..... Attack/virus etc. What have you done to protect your organization as a security professional?**

Different organizations work in different ways, and the ways to handle an incident are different for all. Some take this seriously and some do not. The answer to this should be the process to handle an incident. Align this with the one you had and go on... just don't exaggerate.

**13. CIA triangle?**

Confidentiality: Keeping the information secret.

Integrity: Keeping the information unaltered.

Availability: Information is always available to the authorized parties.

**14. HIDS vs NIDS which one is better and why?**

HIDS is a host intrusion detection system and NIDS is a network intrusion detection system. Both the systems work on similar lines. It's just that the placement is different. HIDS is placed on each host whereas NIDS is placed in the network. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes the processing power of the host as well.

**15. What is port scanning?**

Port scanning is the process of sending messages to gather information about the network, system, etc. by analyzing the response received.

**16. What is the difference between VA and PT?**

Vulnerability Assessment is an approach used to find flaws in an application/network whereas Penetration testing is the practice of finding exploitable vulnerabilities like a real attacker will do. VA is like travelling on the surface whereas PT is digging it for gold.

**17. What are the objects that should be included in a good penetration testing report?**

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category-wise split into high, medium, and low. Also include detailed observation along with replication steps, and screenshots of proof of concept along the remediation.

**18. What is compliance?**

Abiding by a set of standards set by a government/Independent party/organization. E.g. An industry that stores, processes or transmits payment-related information needs to have complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organization complying with its own policies.

**19. Tell us about your Personal achievements or certifications?**

Keep this simple and relevant, getting a SOC CERTIFICATION BY SIEM XPERT can be one personal achievement. Explain how it started and what kept you motivated. How do you feel now and what are your next steps.

**20. Various response codes from a web application?**

1xx – Informational responses

2xx – Success

3xx – Redirection

4xx – Client-side error

5xx – Server-side error

**21. When do you use tracert/traceroute?**

In case you can't ping the destination, tracert will help to identify where the connection stops or gets broken, whether it is the firewall, ISP, router, etc.

**22. DDoS and its mitigation?**

DDoS stands for distributed denial of service. When a network/server/application is flooded with many requests that it is not designed to handle making the server unavailable to legitimate requests. The requests can come from different not related sources hence it is a distributed denial-of-service attack. It can be mitigated by analyzing and filtering the traffic in the scrubbing centres. The scrubbing centres are

centralized data cleansing stations wherein the traffic to a website is analyzed and the malicious traffic is removed.

**23. What is a WAF and what are its types?**

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

**24. Explain the objects of Basic web architecture?**

A basic web architecture should contain a front-ending server, a web application server, and a database server.

**25. How do you handle Antivirus alerts?**

Check the policy for the AV and then the alert. If the alert is for a legitimate file, then it can be whitelisted and if this is a malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virus total, malwares.com, etc. AV needs to be fine-tuned so that the alerts can be reduced.

**26. What is a false positive and false negative in the case of IDS?**

When the device generated an alert for an intrusion that has not happened: this is a false positive and if the device has not generated any alert and the intrusion has happened, this is the case of a false negative.

**27. Which one is more acceptable?**

False positives are more acceptable. False negatives will lead to intrusions happening without getting noticed.

**28. Software testing vs. penetration testing?**

Software testing just focuses on the functionality of the software and not the security aspect. Penetration testing will help identify and address security vulnerabilities.

**29. What are your thoughts about the blue team and the red team?**

A red team is an attacker, and a blue team is a defender. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

**30. What is your preferred – Bug bounty or security testing?**

Both are fine, just support your answer like Bug Bounty is decentralized, can identify rare bugs, large pool of testers etc.

**31. Tell us about your Professional achievements/major projects?**

This can be anything like setting up your own team and processes or a security practice you have implemented. Even if the achievement is not from a security domain just express it well.

### **32. 2 quick points on Web server hardening?**

Web server hardening is the filtering of unnecessary services running on various ports and the removal of default test scripts from the servers. Although web server hardening is a lot more than this and usually organizations have a customized checklist for hardening the servers. Any server getting created must be hardened and hardening must be re-confirmed on a yearly basis. Even the hardening checklist must be reviewed on a yearly basis for new add-ons.

### **33. What is data leakage? How will you detect and prevent it?**

Data leak is when data gets out of the organization in an unauthorized way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorized upload of data to public portals, removable drives, photographs, etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to the internal network, restriction on printing confidential data, etc.

### **34. What are the different levels of data classification and why are they required?**

Data needs to be segregated into various categories so that its severity can be defined, without this segregation a piece of information can be critical for one but not so critical for others. There can be various levels of data classification depending on organization to organization, in broader terms data can be classified into:

Top secret – Its leakage can cause drastic effect to the organization, e.g., trade secrets etc.

Confidential – Internal to the company e.g., policy and processes.

Public – Publicly available, like newsletters etc.

### **35. In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?**

Users are usually not provided with admin access to reduce the risk, but in certain cases, the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only a limited time post senior management approval and a valid business justification.

### **36. What are your views on the usage of social media in the office?**

Social media is acceptable, just ensure content filtering is enabled and uploading features are restricted. Read-only mode is acceptable till the time it does not interfere with work.

### **37. What are the various ways by which the employees are made aware of information security policies and procedures?**

There can be various ways in which this can be done:

Employees should undergo mandatory information security training post joining the organisation. This should also be done on yearly basis, and this can be either a classroom session followed by a quiz or online training.

Sending out notifications on regular basis in the form of slides, one-pagers, etc. to ensure that the employees are kept aware.

**38. In a situation where both Open-source software and licensed software are available to get the job done. What should be preferred and why?**

For an enterprise, it is better to go for the licensed version of the software as most of the software have an agreement clause that the software should be used for individual usage and not for commercial purpose. Plus, the licensed version is updated and easy to track in an organization. It also helps the clients develop confidence in the organization's software and practices.

**39. When should a security policy be revised?**

There is no fixed time for reviewing the security policy, but all this should be done at least once a year. Any changes made should be documented in the revision history of the document and versioning. In case there are any major changes the changes need to be notified to the users as well.

**40. What all should be included in a CEO level report from a security standpoint?**

A CEO level report should have not more than 2 pages:

A summarized picture of the state of the security structure of the organization.

Quantified risk and ALE (Annual Loss Expectancy) results along with countermeasures.

**41. How do you report risks?**

Risk can be reported but it needs to be assessed first. Risk assessment can be done in 2 ways: Quantitative analysis and qualitative analysis. This approach will cater to both technical and business guys. The business guy can see a probable loss in numbers whereas the technical guys will see the impact and frequency. Depending on the audience, the risk can be assessed and reported.

**42. What is an incident and how do you manage it?**

Any event which leads to compromise of the security of an organization is an incident.

The incident process goes like this:

Identification of the Incident

Logging it (Details) Investigation and root cause analysis (RCA)

Escalation or keeping the senior management/party's informer mediation steps Closure report.

**43. Is social media secure?**

Not sure if the data is secure or not but users can take steps from their end to ensure safety.

Connect with trusted people

Do not post/upload confidential information

Never use the same username password for all accounts

#### 44. Chain of custody?

For legal cases the data/device (evidence) needs to be integrated, hence any access needs to be documented – who, what when, and why. Compromise in this process can cause legal issues for the parties involved.

