Name: Abdurrahman Qureshi

Roll No: 242466

Assignment No: 1

Date Of Performance: 01/09/2025

Aim: Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities (use NMAP on Kali Linux)

NESSUS:

Nessus:

- **Nessus** is a popular **vulnerability assessment tool** by Tenable.
- It scans systems, servers, and networks for **vulnerabilities, misconfigurations, and compliance issues**.

Key Features:

- Large **plugin database** (150k+ vulnerabilities).
- **Credentialed & non-credentialed scans**.
- Supports **compliance checks** (PCI, HIPAA, CIS).
- Generates detailed **reports with severity levels**.

Scan Types:

- Host discovery
- Port & service scanning
- Vulnerability detection (CVEs, misconfigs)
- Web app checks (SQLi, XSS, etc.)

Severity Levels:

- **Critical** – Full system compromise possible
- **High** – Major risks (privilege escalation)

- **Medium/Low** – Exploits with conditions or minor issues
- **Info** – Useful details

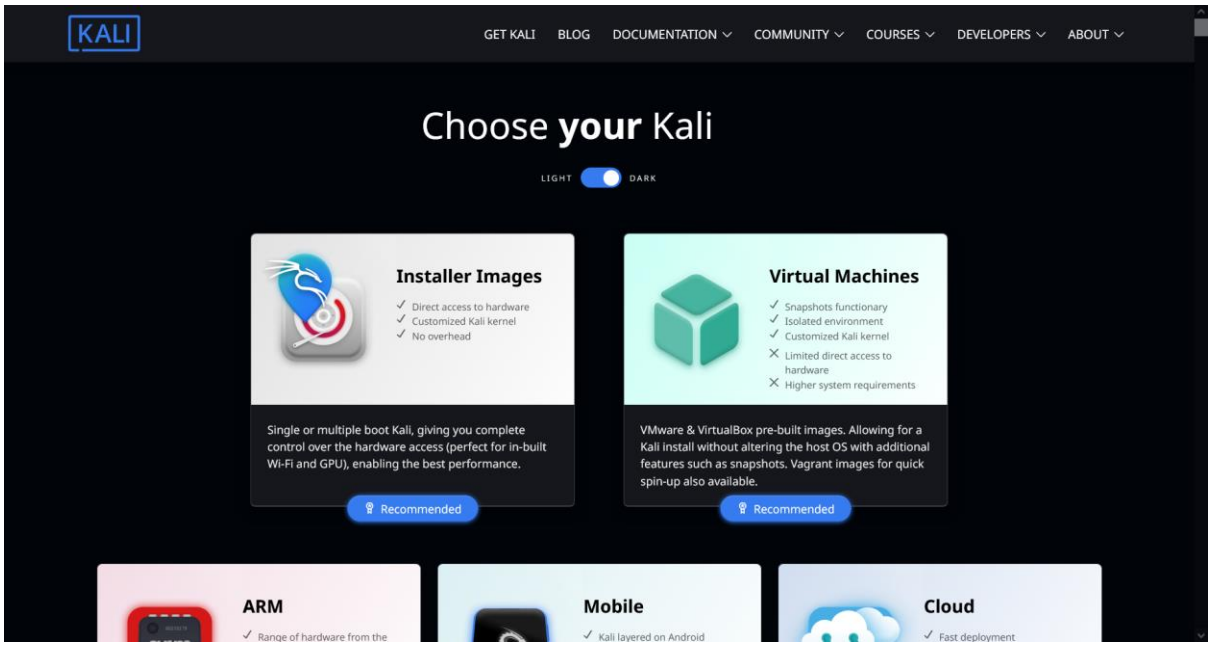
Pros:

- Easy GUI, frequent updates
- Detects vulnerabilities & misconfigs
- Professional reports

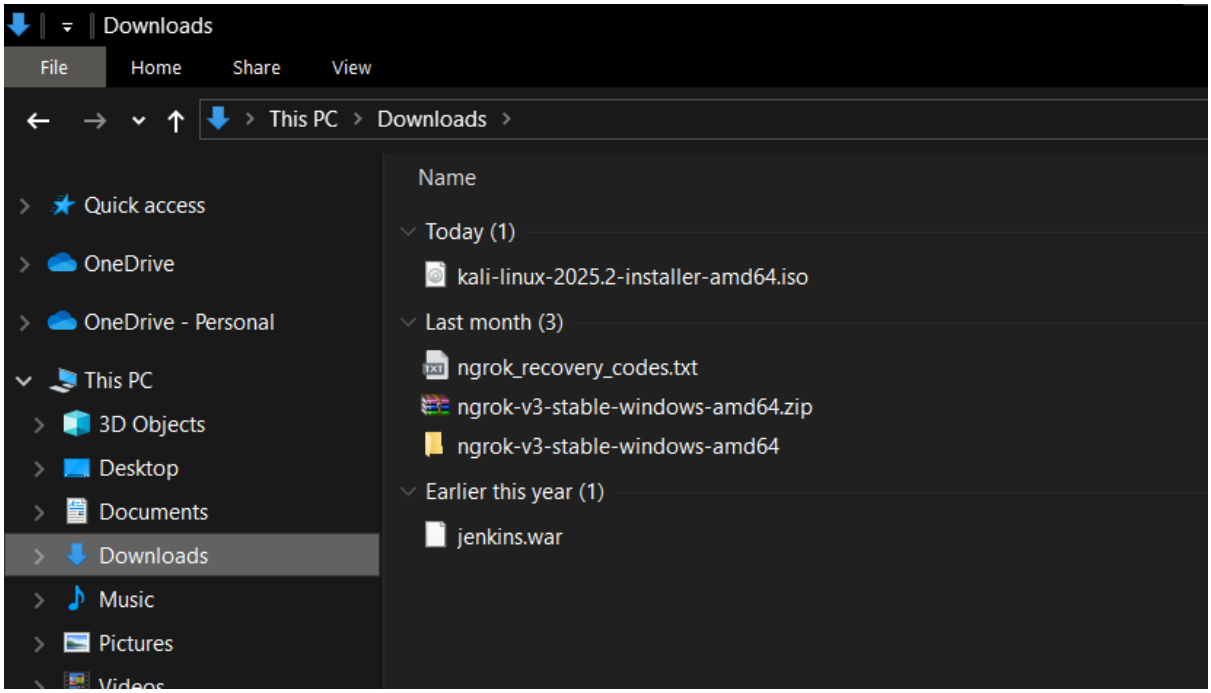
Cons:

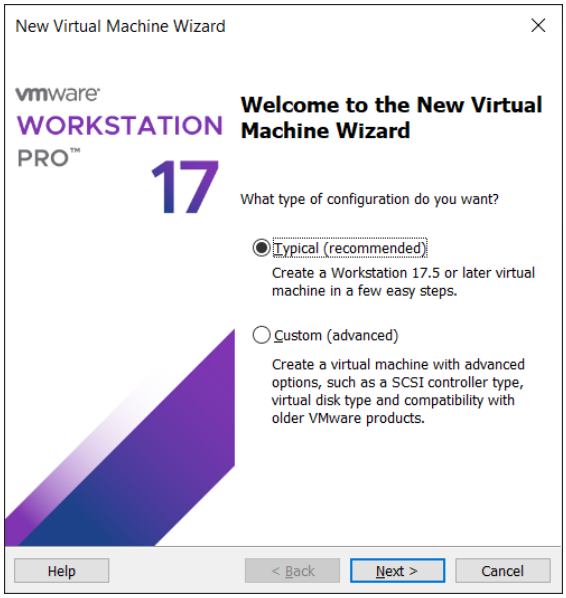
- Paid license for full version
- Possible false positives
- Heavy scans may slow systems

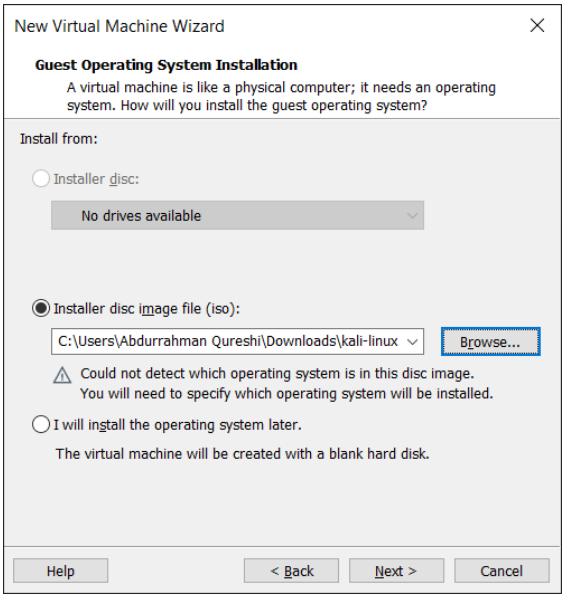
Vulnerability Scan via Nessus:

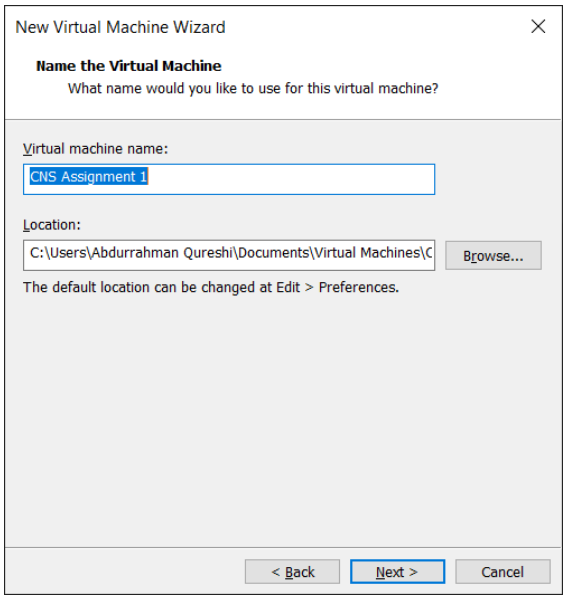


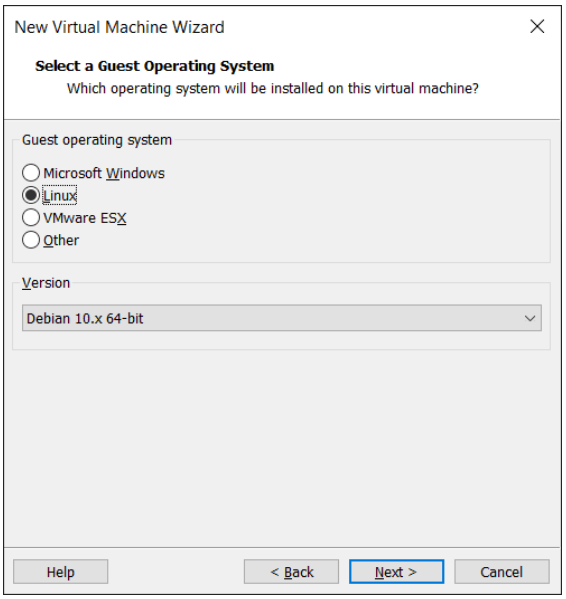

Installer
Pre-built VMs
ARM
Mobile
Cloud
Containers
Live
WSL
Kali Linux 2025.2 Changelog
x86_64
Apple Silicon (ARM64)
Recommended
Installer
Complete offline installation with customization
torrent
sum
Weekly
NetInstaller
Everything

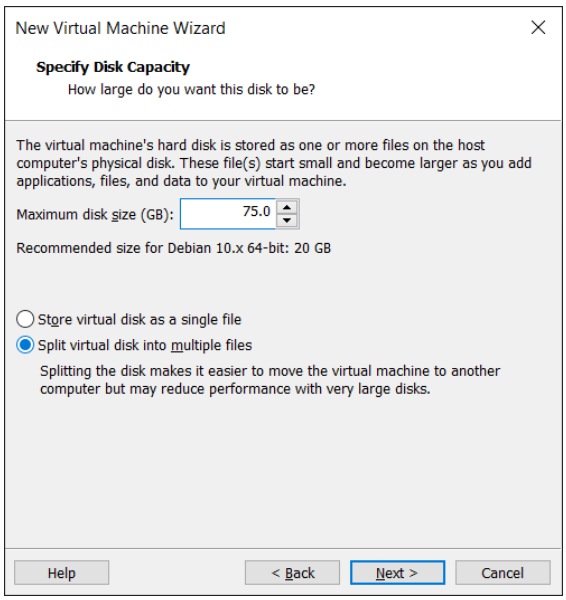

Downloads
File
Home
Share
View
This PC
Downloads
Quick access
OneDrive
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Name
Today (1)
kali-linux-2025.2-installer-amd64.iso
Last month (3)
ngrok_recovery_codes.txt
ngrok-v3-stable-windows-amd64.zip
ngrok-v3-stable-windows-amd64
Earlier this year (1)
jenkins.war

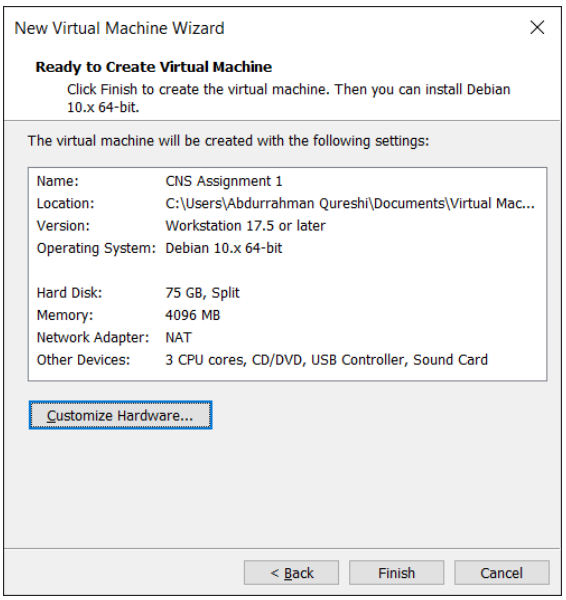

New Virtual Machine Wizard
vmware
WORKSTATION
PRO™
17
Welcome to the New Virtual Machine Wizard
What type of configuration do you want?
Typical (recommended)
Create a Workstation 17.5 or later virtual machine in a few easy steps.
Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Help
< Back
Next >
Cancel

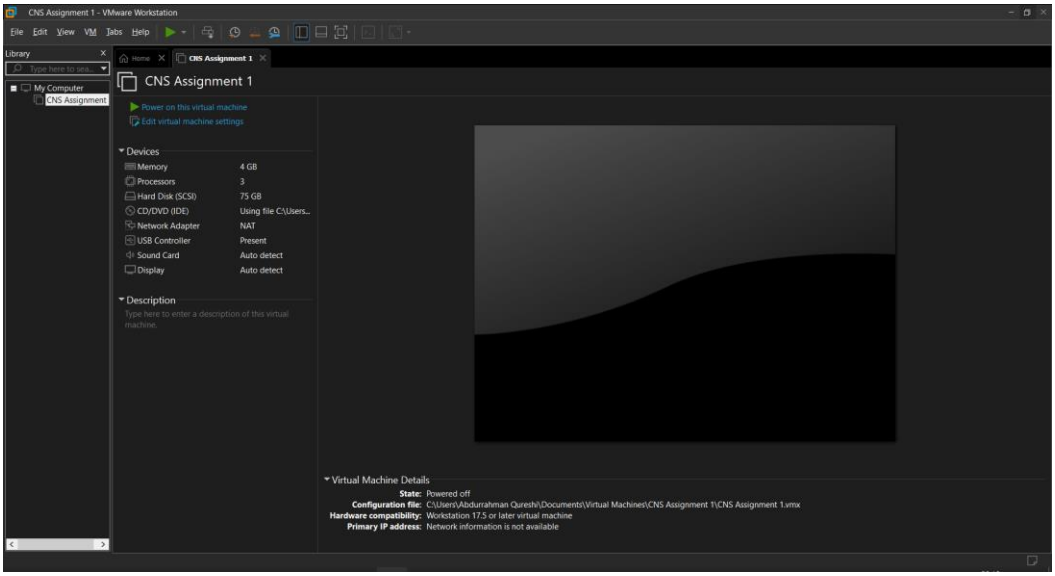

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
C:\Users\Abdurrahman Qureshi\Downloads\kali-linux
Browse...
Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

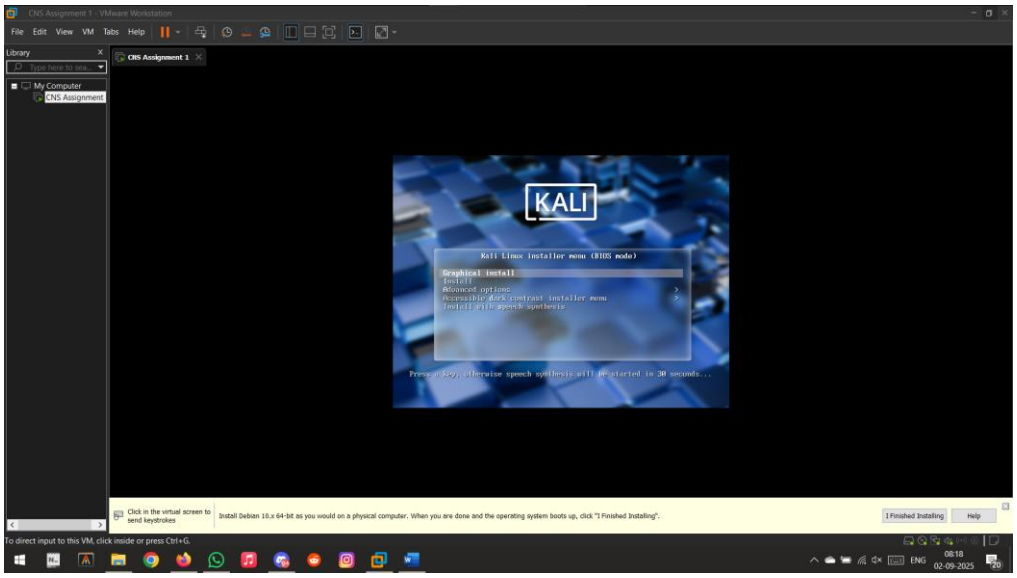

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
CNS Assignment 1
Location:
C:\Users\Abdurrahman Qureshi\Documents\Virtual Machines\C
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

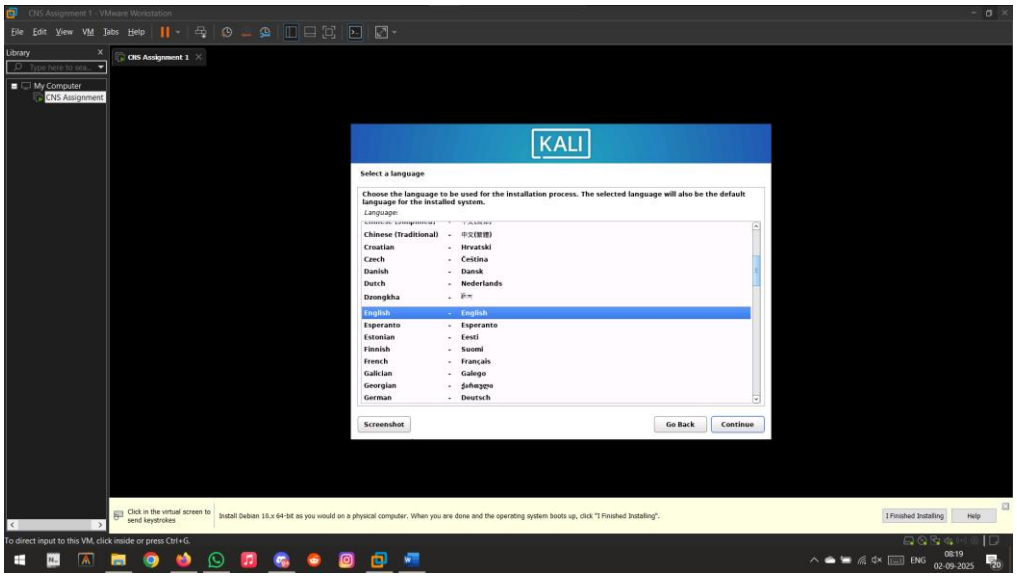

New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
VMware ESX
Other
Version
Debian 10.x 64-bit
Help
< Back
Next >
Cancel

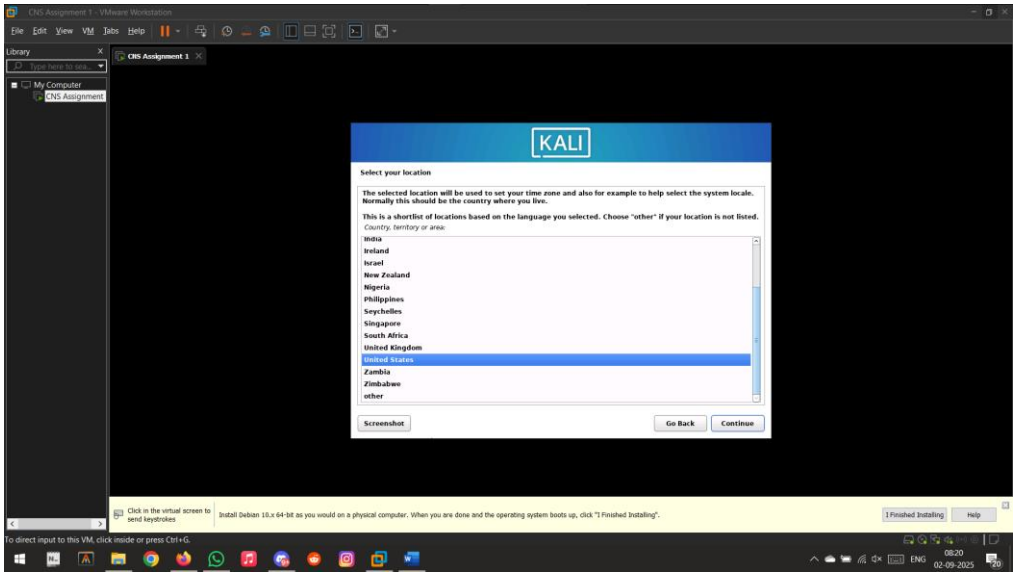

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
75.0
Recommended size for Debian 10.x 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

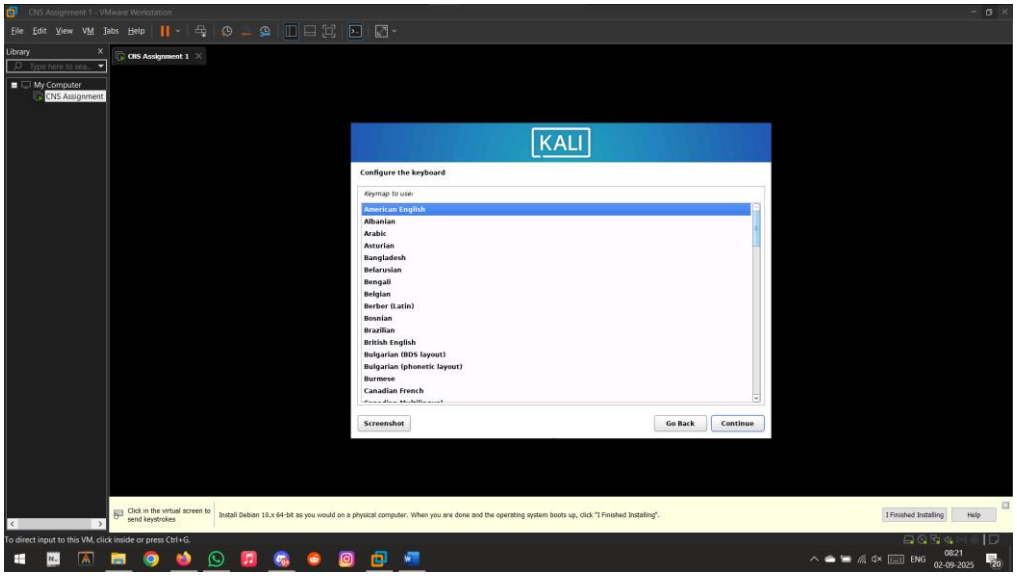

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Debian 10.x 64-bit.
The virtual machine will be created with the following settings:
Name: CNS Assignment 1
Location: C:\Users\Abdurrahman Qureshi\Documents\Virtual Mac...
Version: Workstation 17.5 or later
Operating System: Debian 10.x 64-bit
Hard Disk: 75 GB, Split
Memory: 4096 MB
Network Adapter: NAT
Other Devices: 3 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
< Back
Finish
Cancel

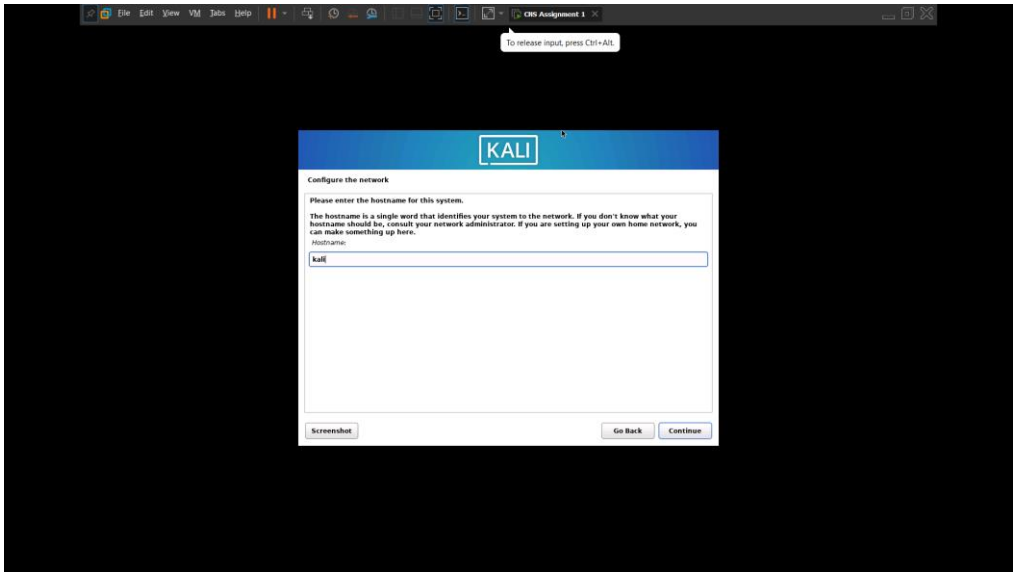

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 4 GB
Processors 3
Hard Disk (SCSI) 75 GB
CD/DVD (IDE) Using file C:\Users...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\Abdurrahman Qureshi\Documents\Virtual Machines\CNS Assignment 1\CNS Assignment 1.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

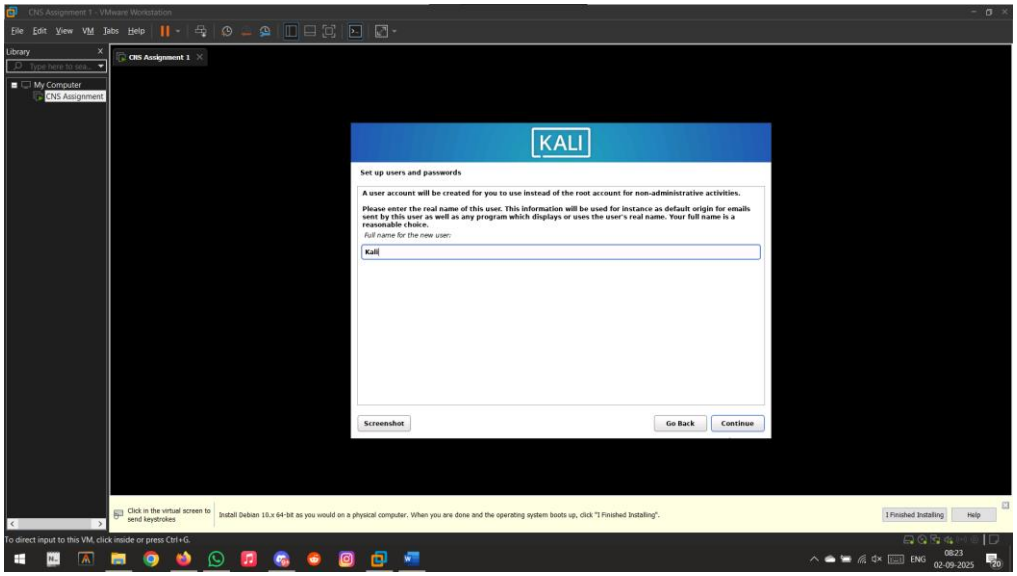

KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Install with speech synthesis
Press a key, otherwise speech synthesis will be started in 30 seconds...
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
08:18
02-09-2025

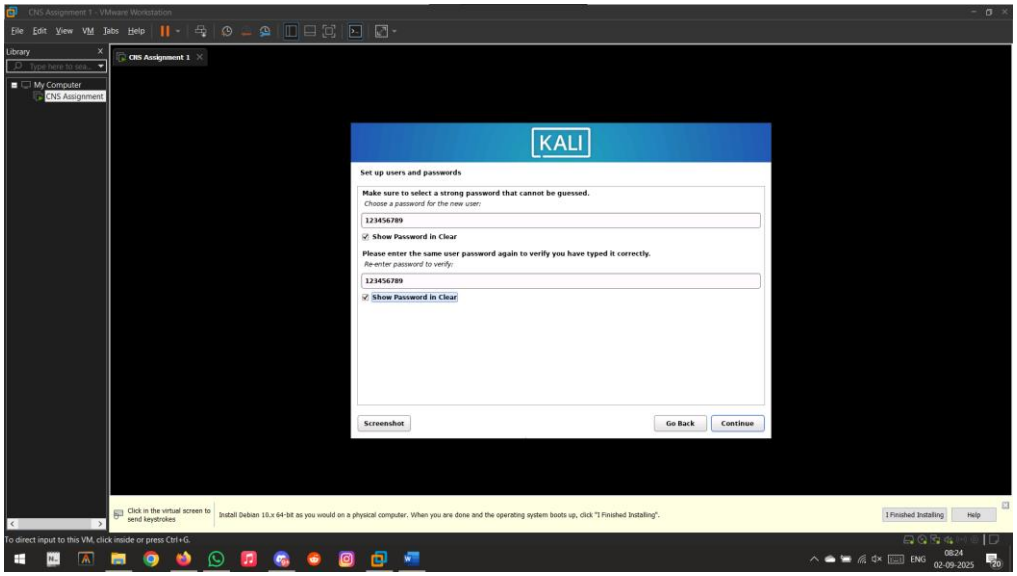

KALI
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང་ཁ
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
08:19
02-09-2025

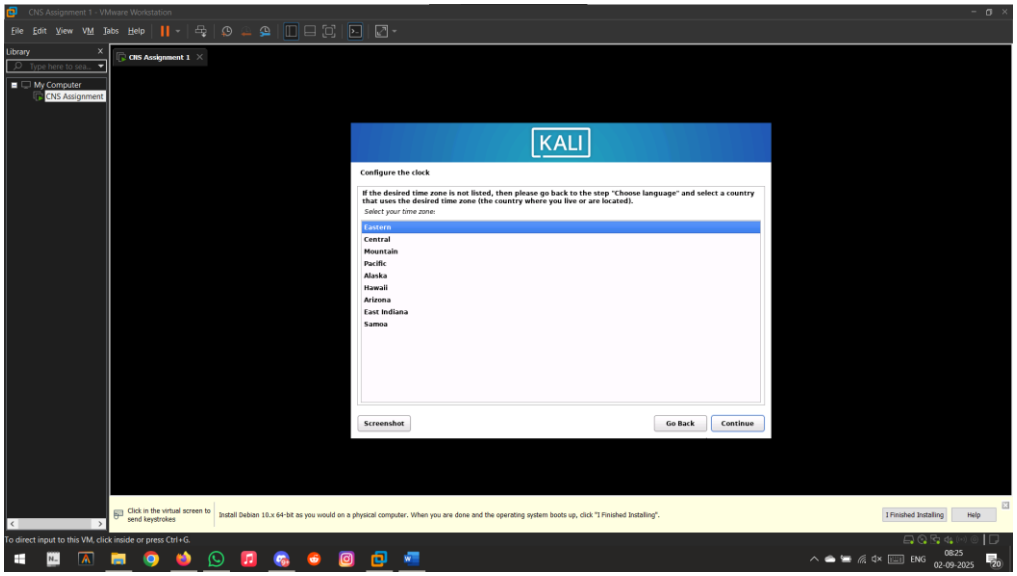

KALI
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue

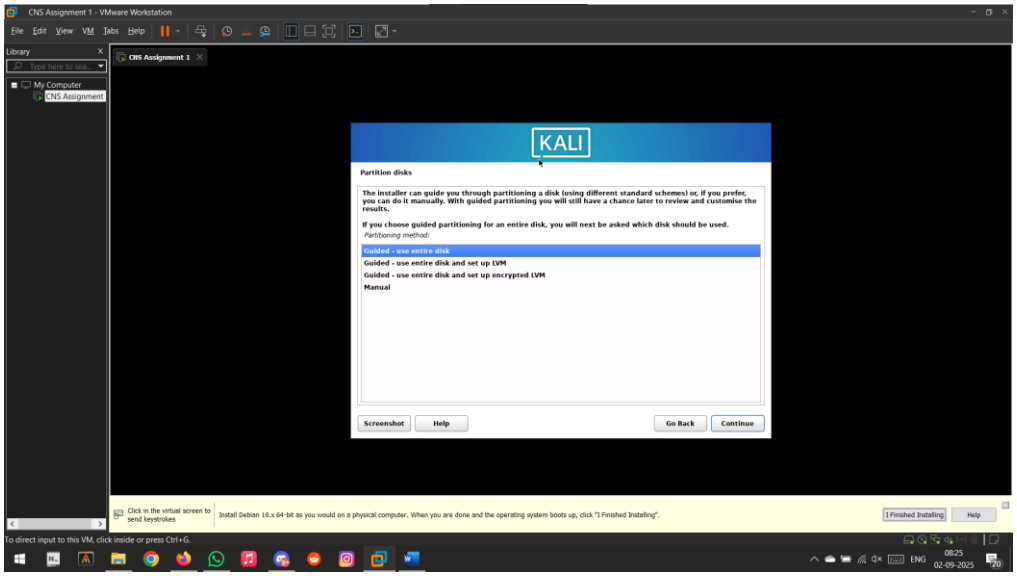

KALI
Configure the keyboard
Keymap to use:
American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Berber (Latin)
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Screenshot
Go Back
Continue

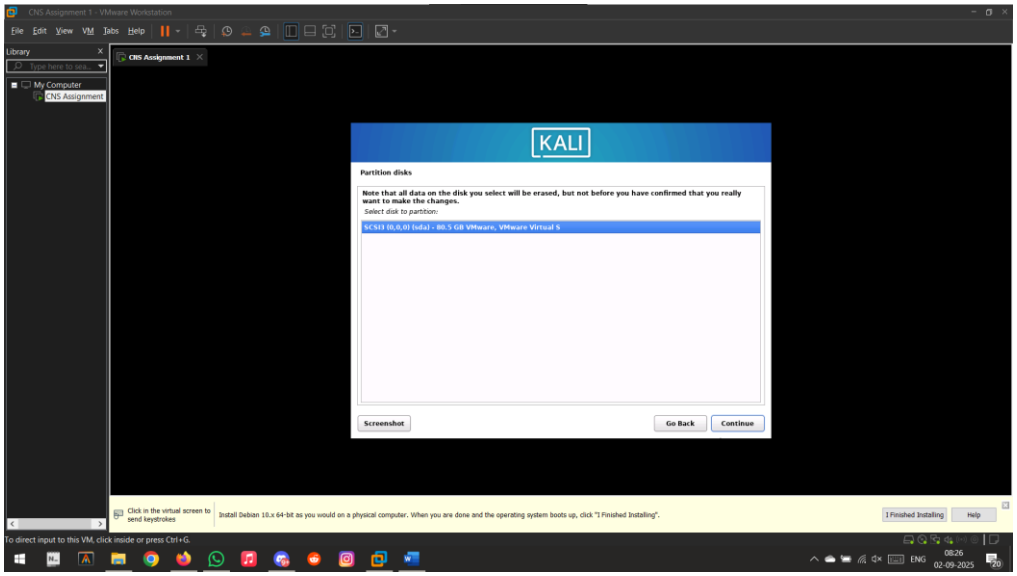

To release input, press Ctrl+Alt.
KALI
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
kali
Screenshot
Go Back
Continue

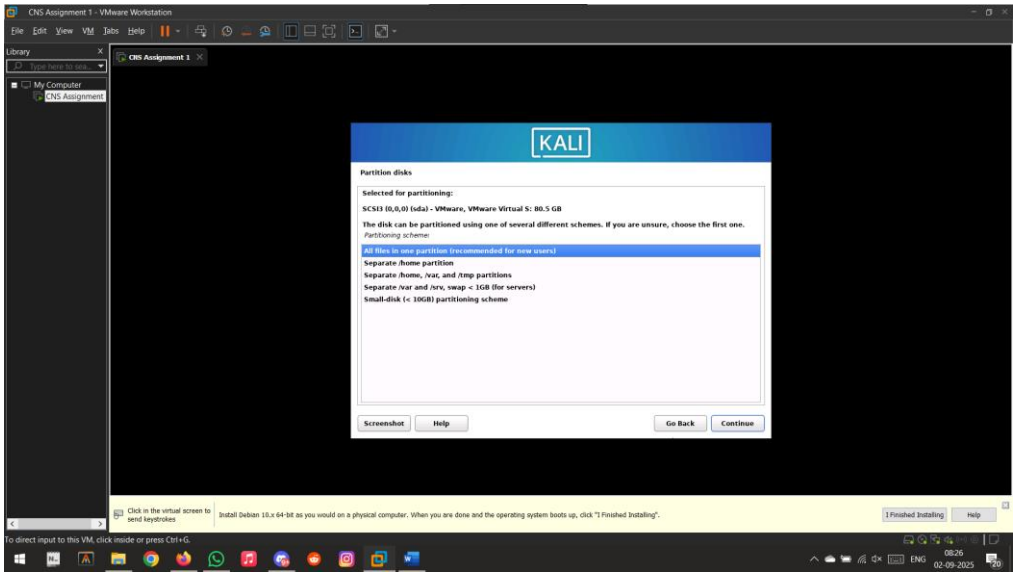

KALI
Set up users and passwords
A user account will be created for you to use instead of the root account for non-administrative activities.
Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.
Full name for the new user:
Kali
Screenshot
Go Back
Continue

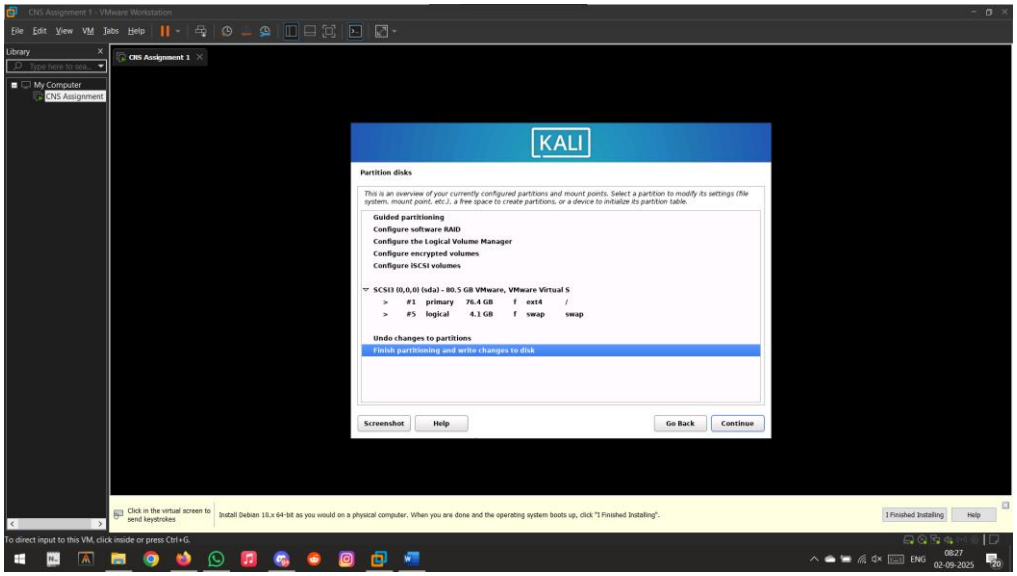

KALI
Set up users and passwords
Make sure to select a strong password that cannot be guessed.
Choose a password for the new user:
123456789
Show Password in Clear
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
123456789
Show Password in Clear
Screenshot
Go Back
Continue

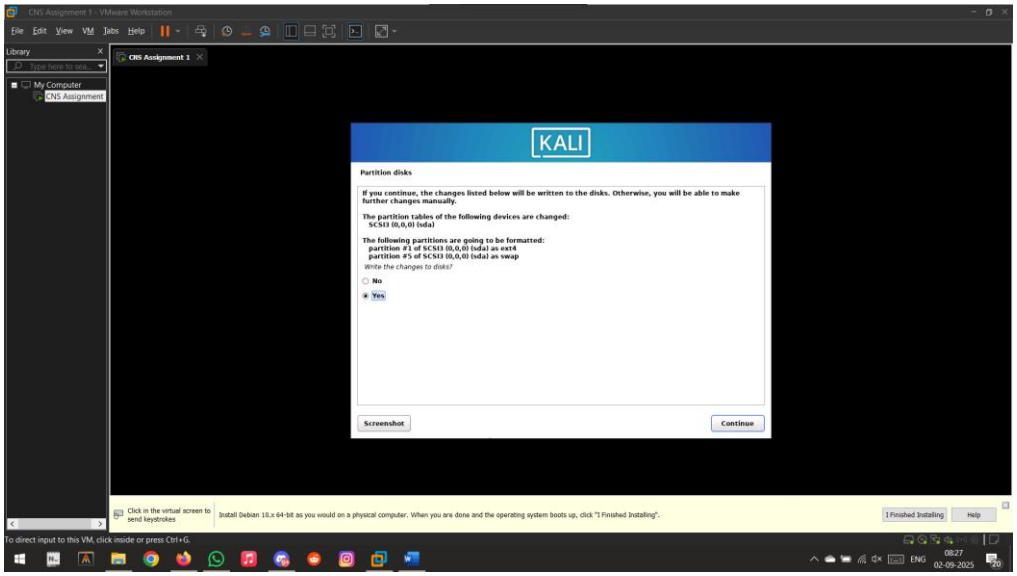

KALI
Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
Screenshot
Go Back
Continue

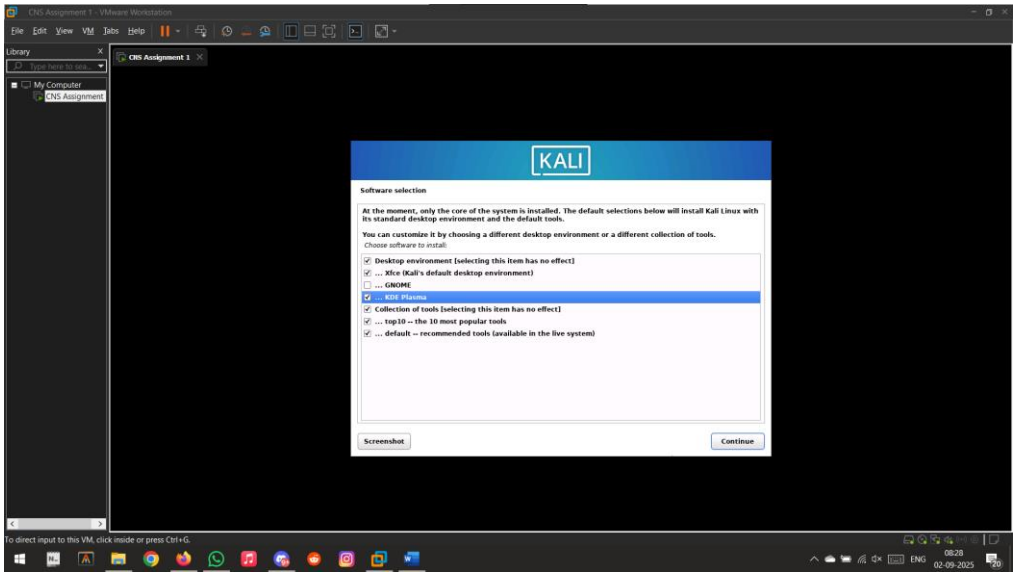

CNS Assignment 1 - VMware Workstation
KALI
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Help
Go Back
Continue
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
08:25
02-09-2025

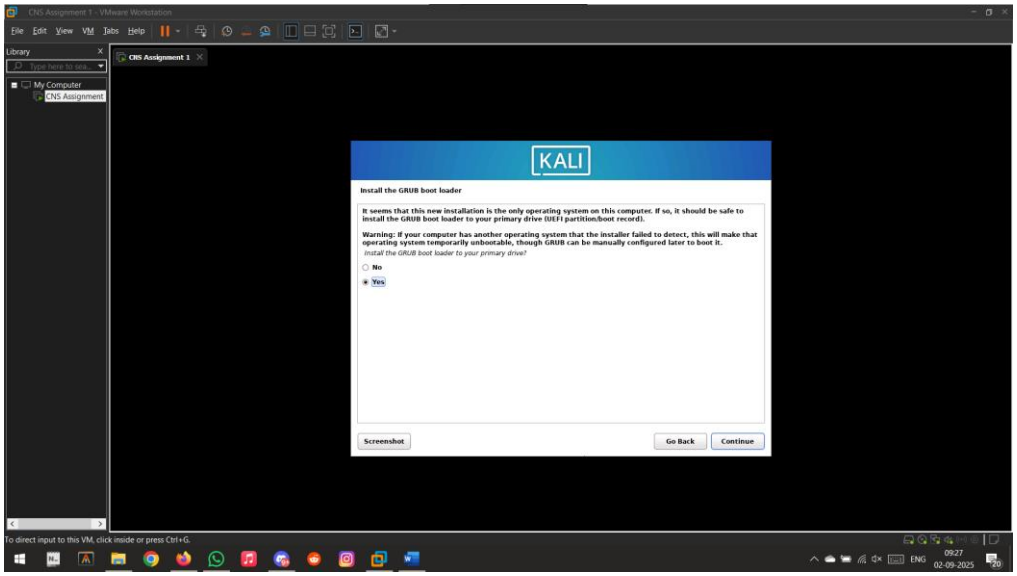

CNS Assignment 1 - VMware Workstation
KALI
Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI3 (0,0,0) (sda) - 80.5 GB VMware, VMware Virtual S
Screenshot
Go Back
Continue
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
08:26
02-09-2025

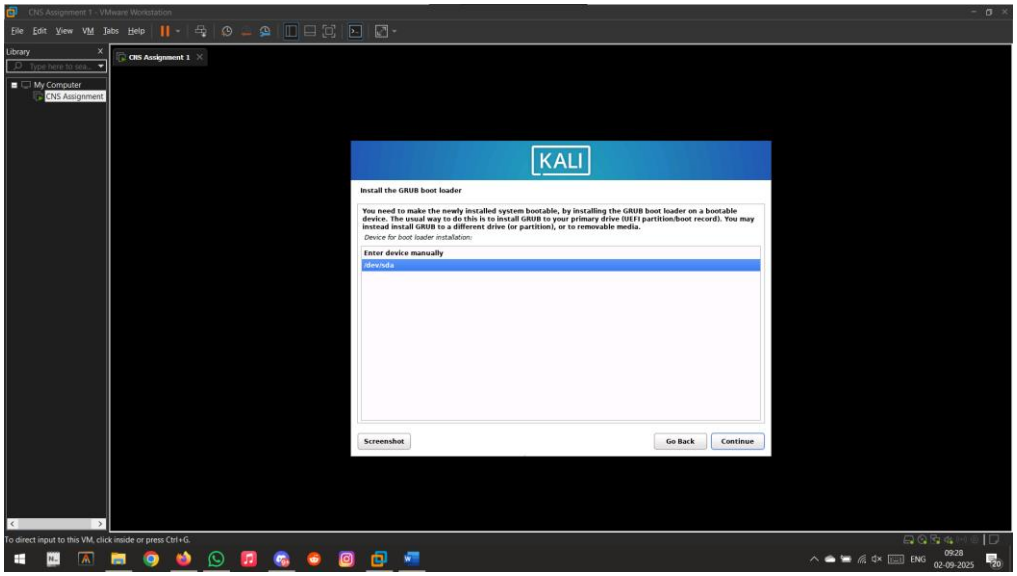

CNS Assignment 1 - VMware Workstation
KALI
Partition disks
Selected for partitioning:
SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 80.5 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
Separate /var and /srv, swap < 1GB (for servers)
Small-disk (< 10GB) partitioning scheme
Screenshot
Help
Go Back
Continue
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
08:26
02-09-2025

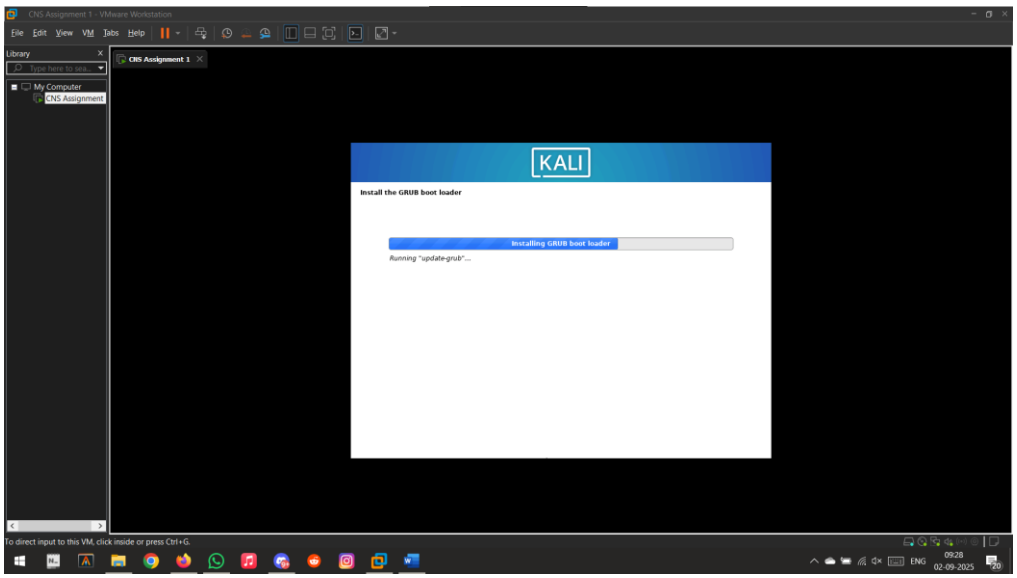

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI3 (0,0,0) (sda) - 80.5 GB VMware, VMware Virtual S
#1 primary 76.4 GB f ext4 /
#5 logical 4.1 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue
Click in the virtual screen to send keystrokes
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
ENG
08:27
02-09-2025

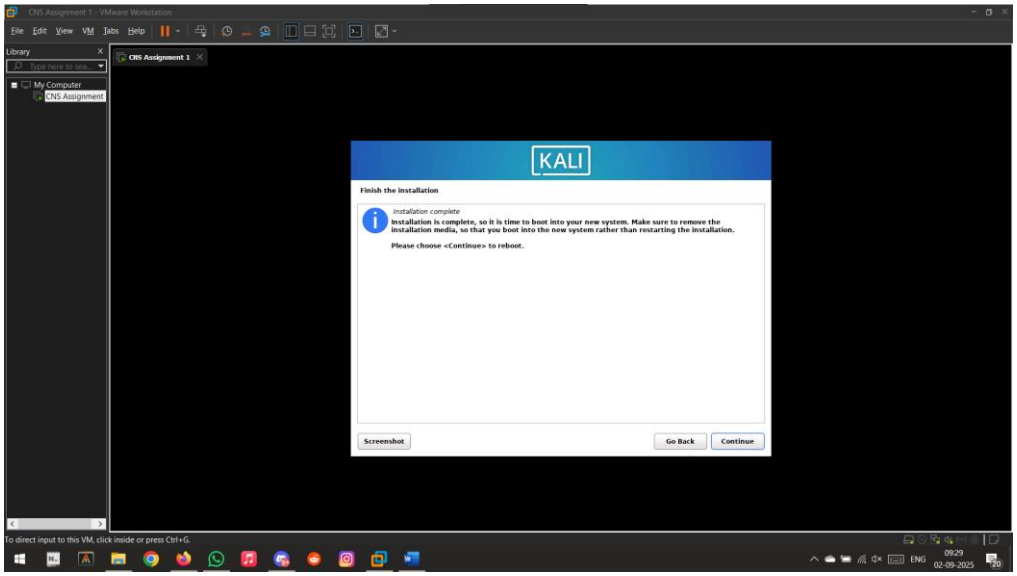

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue
Click in the virtual screen to send keystrokes
Install Debian 10.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.
ENG
08:27
02-09-2025

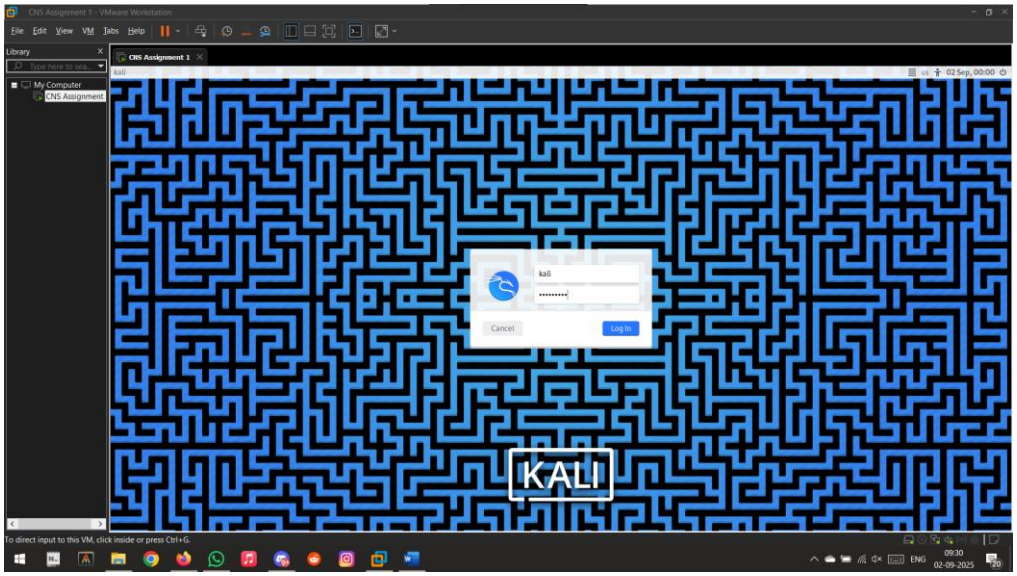

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Software selection
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)
Screenshot
Continue
To direct input to this VM, click inside or press Ctrl+G.
ENG
08:28
02-09-2025

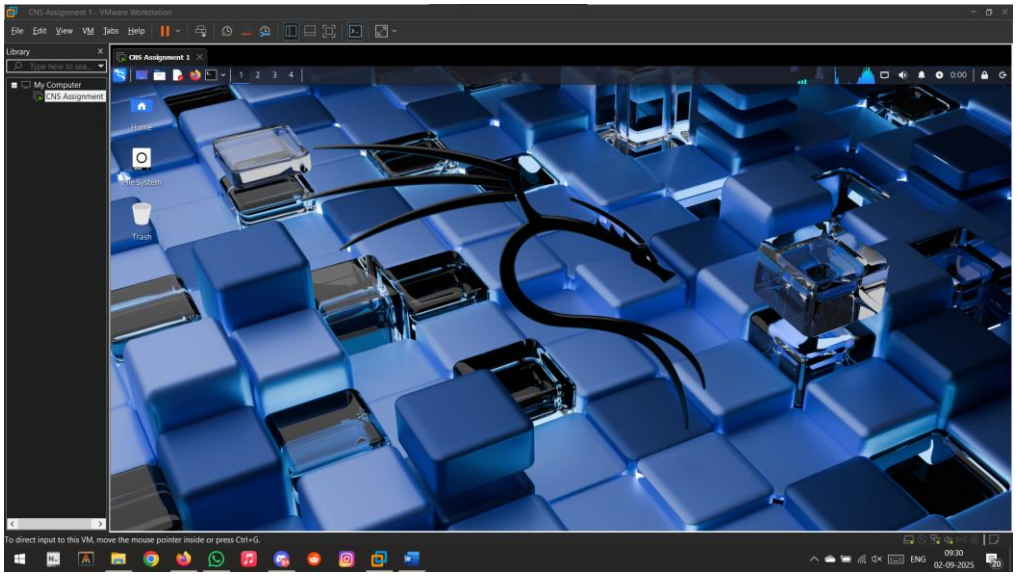

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
No
Yes
Screenshot
Go Back
Continue
To direct input to this VM, click inside or press Ctrl+G.
ENG
09:27
02-09-2025

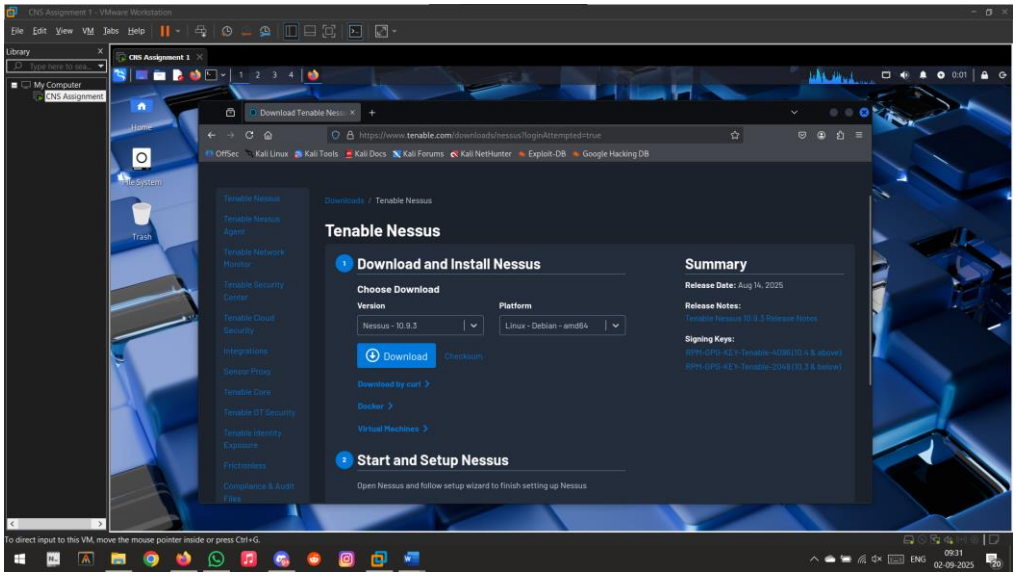

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
/dev/sda
Screenshot
Go Back
Continue
To direct input to this VM, click inside or press Ctrl+G.
ENG
09:28
02-09-2025

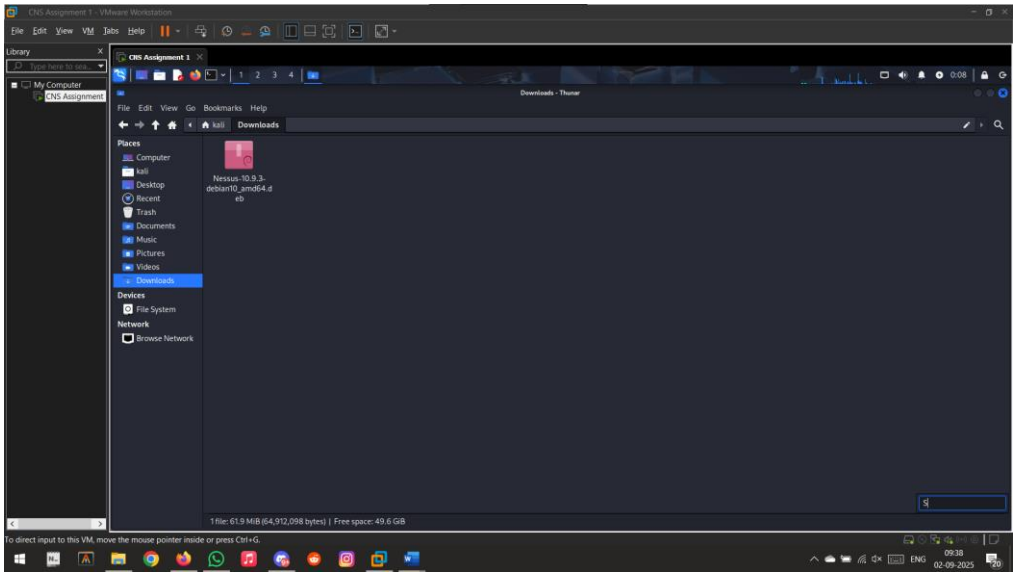

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Install the GRUB boot loader
Installing GRUB boot loader
Running "update-grub"...
To direct input to this VM, click inside or press Ctrl+G.
ENG
09:28
02-09-2025

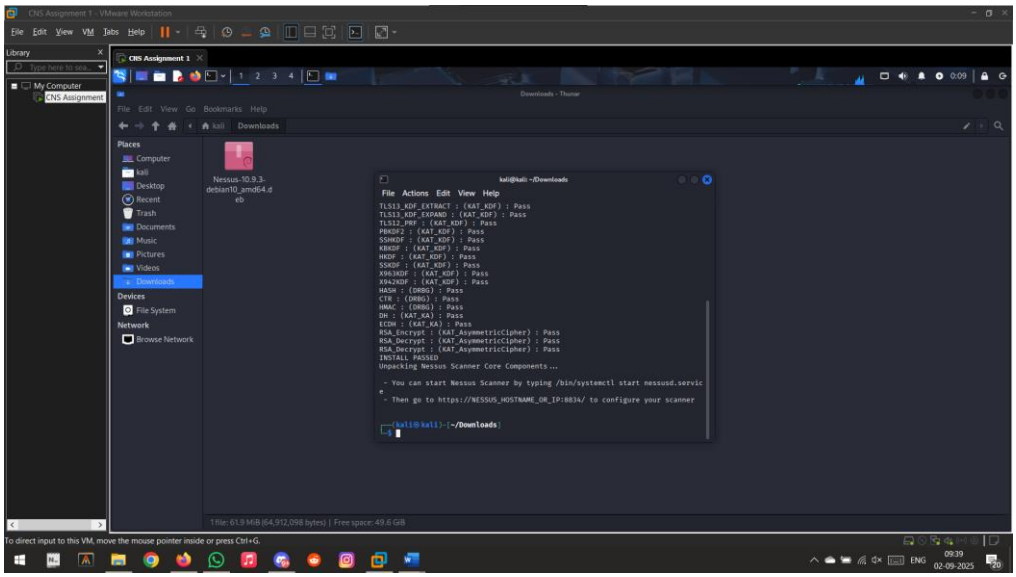

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
KALI
Finish the installation
Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Please choose <Continue> to reboot.
Screenshot
Go Back
Continue
To direct input to this VM, click inside or press Ctrl+G.
09:29
02-09-2025

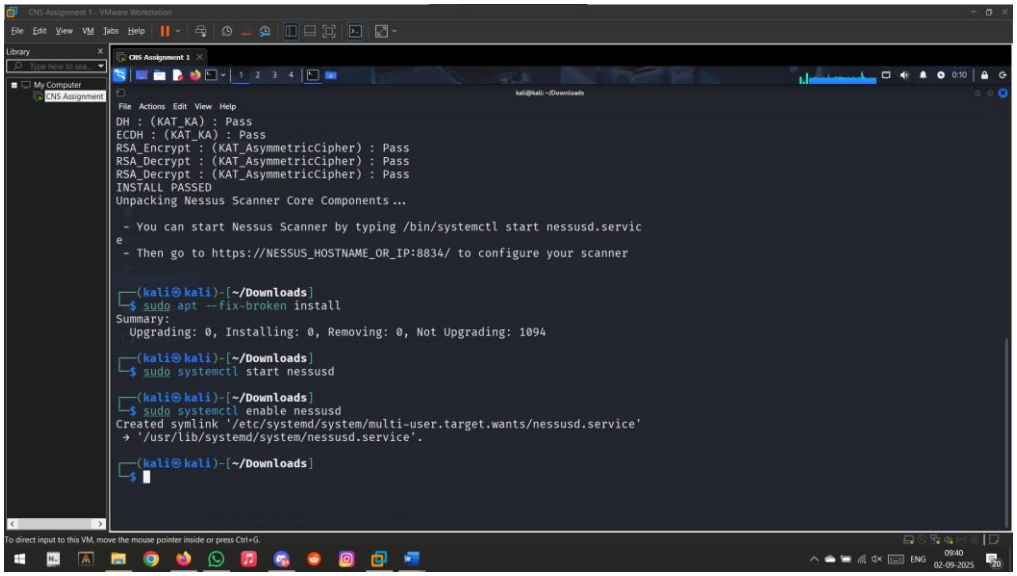

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
kali
02 Sep, 00:00
kali
Cancel
Log In
KALI
To direct input to this VM, click inside or press Ctrl+G.
09:30
02-09-2025

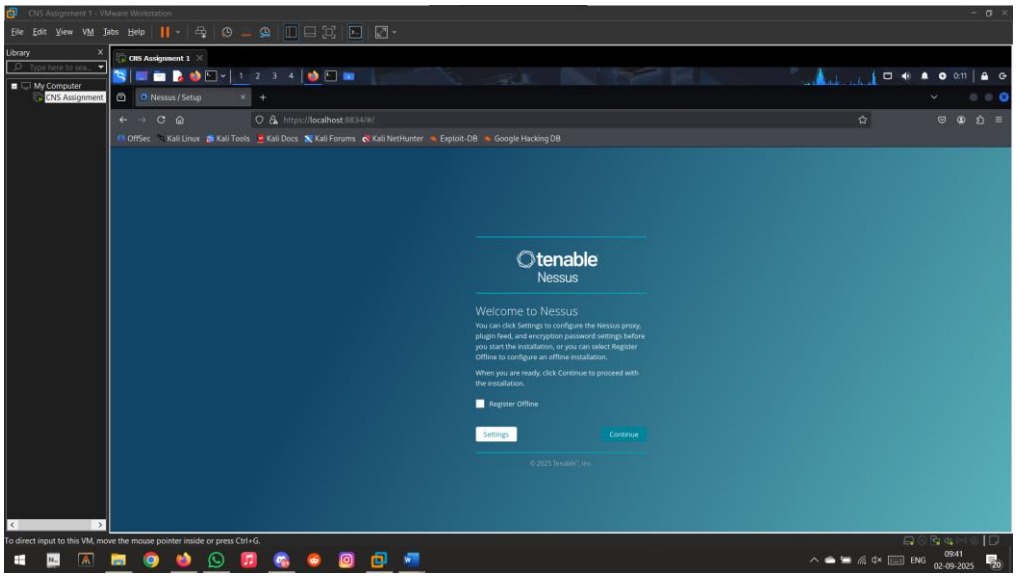

CNS Assignment 1 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CNS Assignment
CNS Assignment 1
Home
File System
Trash
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
09:30
02-09-2025

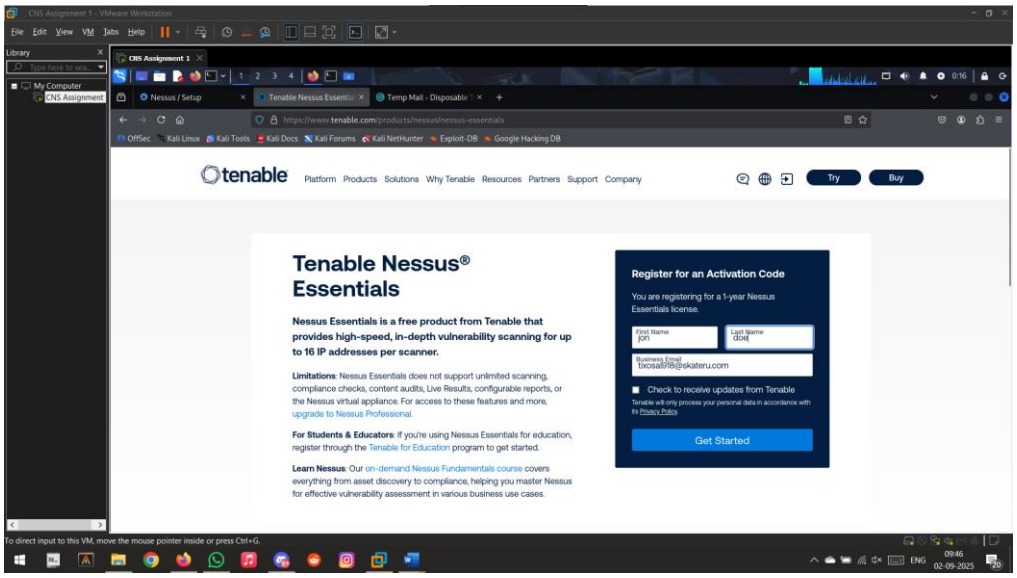

Tenable Nessus
Download and Install Nessus
Choose Download
Version
Nessus - 10.9.3
Platform
Linux - Debian - amd64
Download
Summary
Release Date: Aug 14, 2025
Release Notes:
Signing Keys:
Start and Setup Nessus
Open Nessus and follow setup wizard to finish setting up Nessus

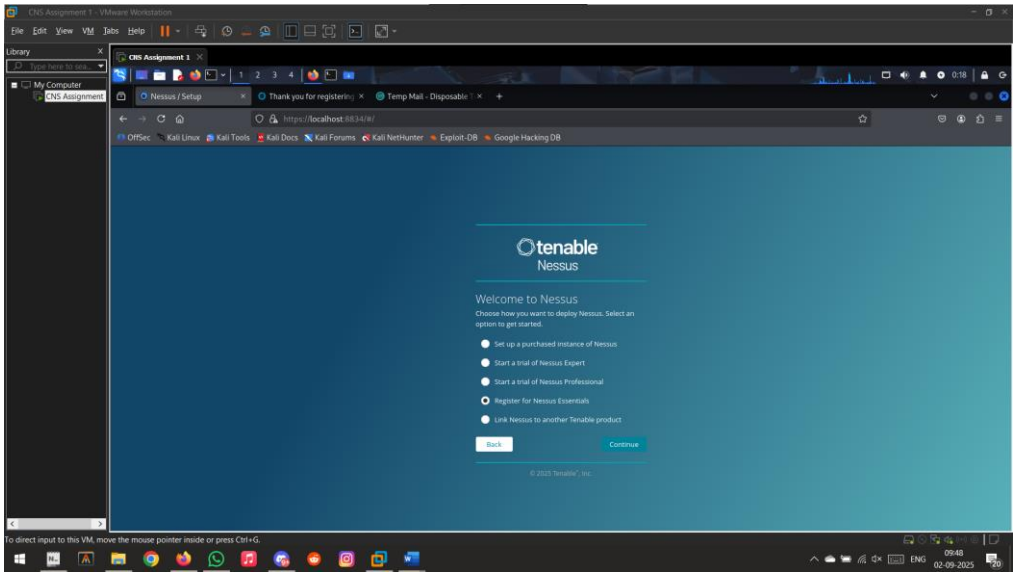

Downloads - Thunar
Nessus-10.9.3-debian10_amd64.deb
1 file: 61.9 MiB (64,912,098 bytes) | Free space: 49.6 GB

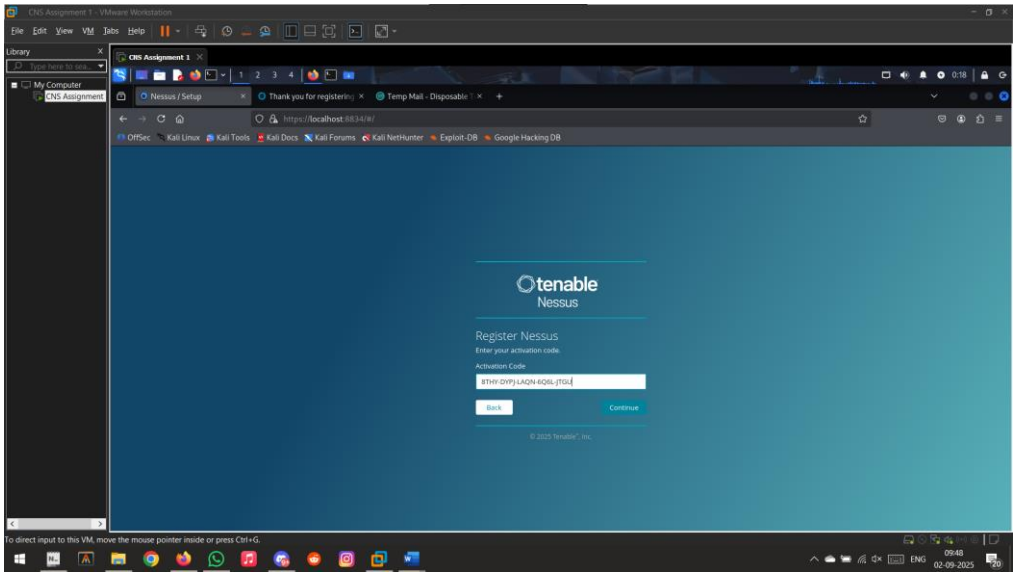

Downloads - Thunar
Nessus-10.9.3-debian10_amd64.deb
kali@kali: ~/Downloads
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner
1 file: 61.9 MiB (64,912,098 bytes) | Free space: 49.6 GB

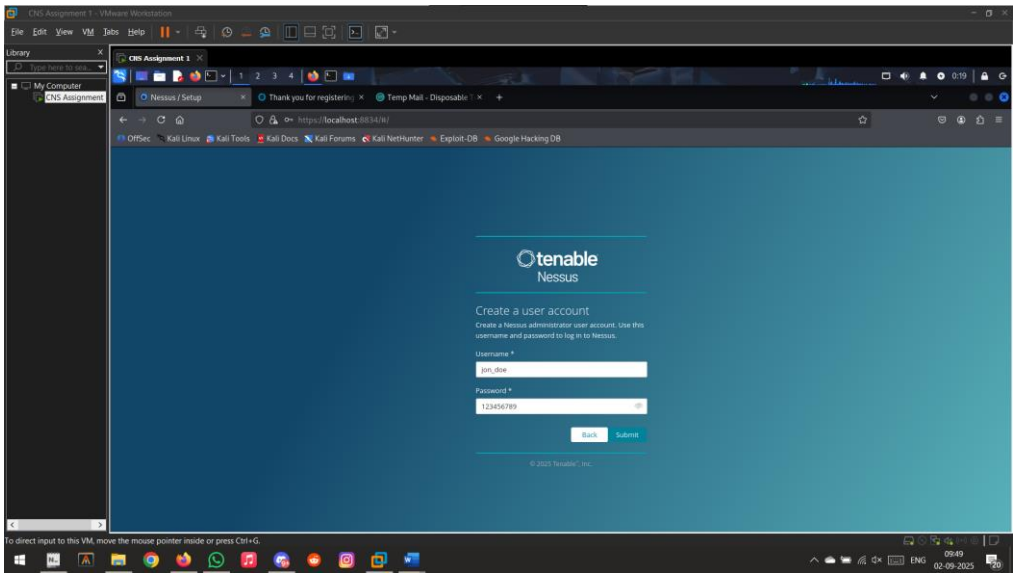

DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner
(kali㉿kali)-[~/Downloads]
$ sudo apt --fix-broken install
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1094
(kali㉿kali)-[~/Downloads]
$ sudo systemctl start nessusd
(kali㉿kali)-[~/Downloads]
$ sudo systemctl enable nessusd
Created symlink '/etc/systemd/system/multi-user.target.wants/nessusd.service'
→ '/usr/lib/systemd/system/nessusd.service'.
(kali㉿kali)-[~/Downloads]
$

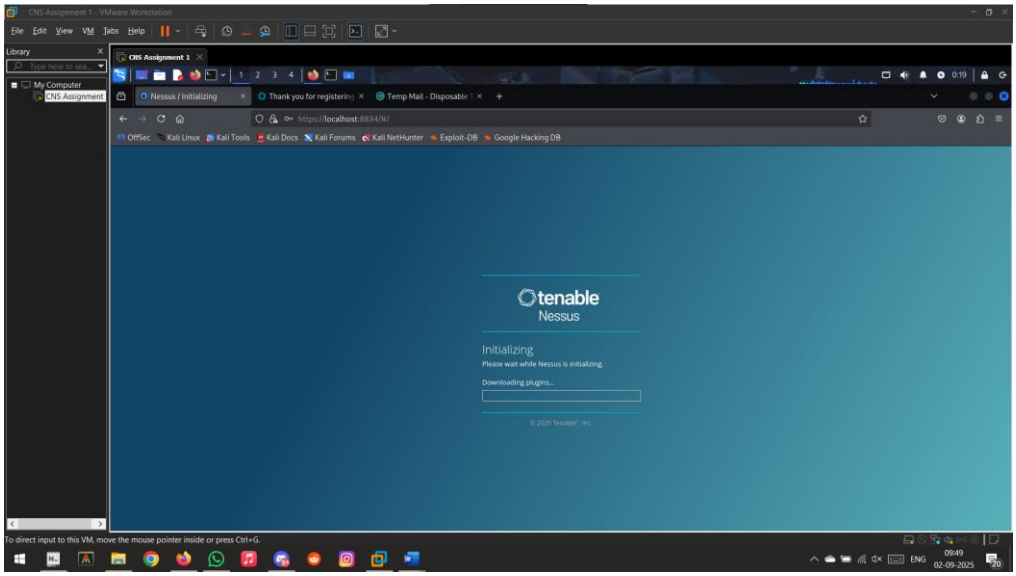

tenable
Nessus
Welcome to Nessus
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.
When you are ready, click Continue to proceed with the installation.
Register Offline
Settings
Continue

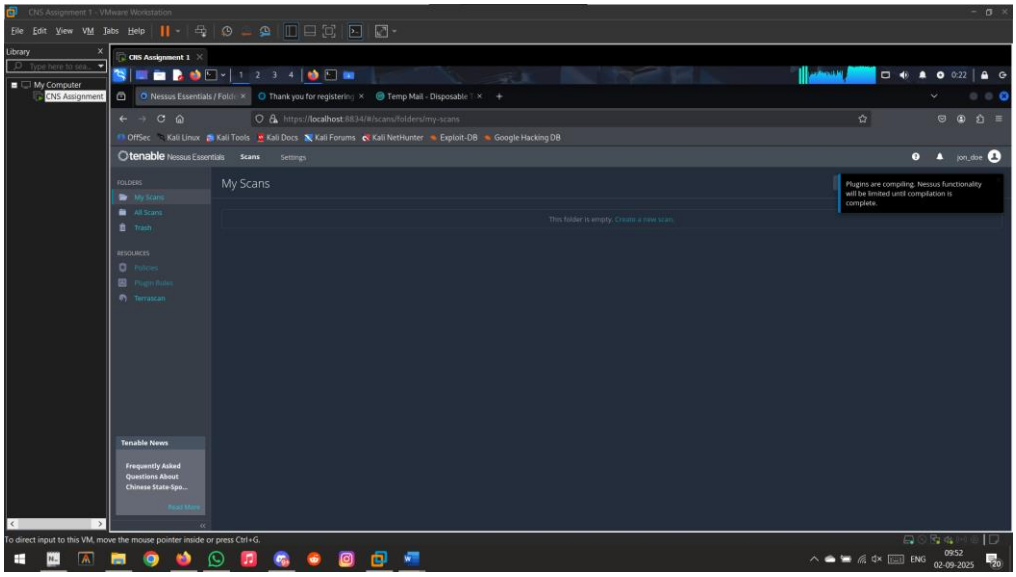

tenable
Platform Products Solutions Why Tenable Resources Partners Support Company
Try
Buy
Tenable Nessus® Essentials
Nessus Essentials is a free product from Tenable that provides high-speed, in-depth vulnerability scanning for up to 16 IP addresses per scanner.
Limitations: Nessus Essentials does not support unlimited scanning, compliance checks, content audits, Live Results, configurable reports, or the Nessus virtual appliance. For access to these features and more, upgrade to Nessus Professional.
For Students & Educators: If you're using Nessus Essentials for education, register through the Tenable for Education program to get started.
Learn Nessus: Our on-demand Nessus Fundamentals course covers everything from asset discovery to compliance, helping you master Nessus for effective vulnerability assessment in various business use cases.
Register for an Activation Code
You are registering for a 1-year Nessus Essentials license.
First Name
jon
Last Name
doe
Business Email
tkosaa6f6@skateru.com
Check to receive updates from Tenable
Tenable will only process your personal data in accordance with its Privacy Policy
Get Started

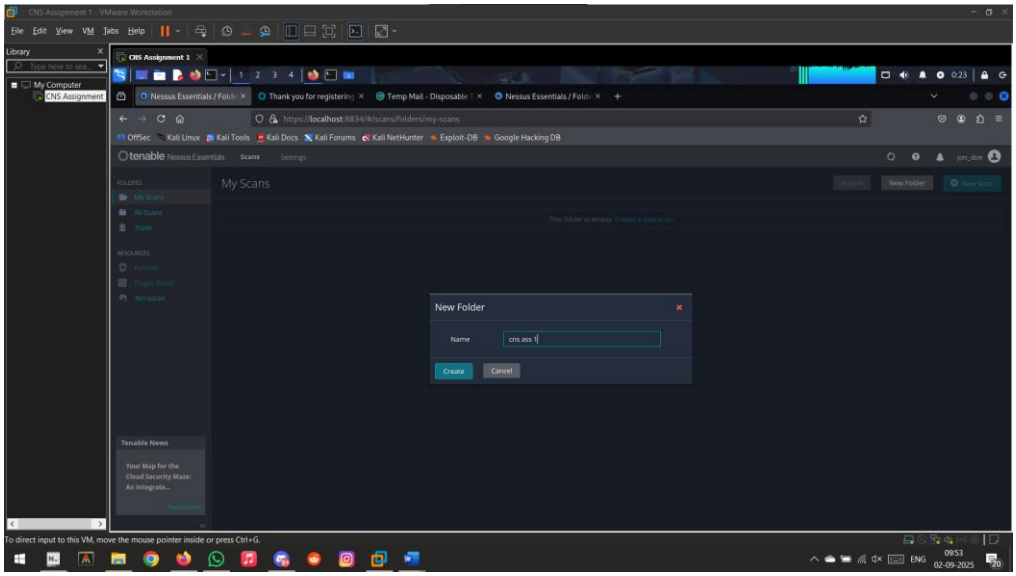

tenable
Nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
Link Nessus to another Tenable product
Back
Continue

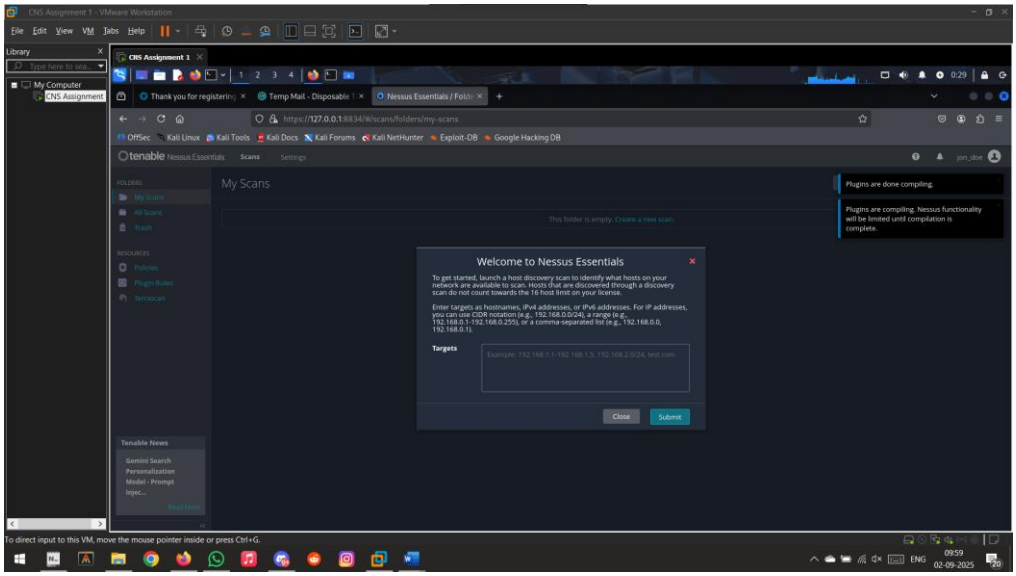

tenable
Nessus
Register Nessus
Enter your activation code.
Activation Code
Back
Continue

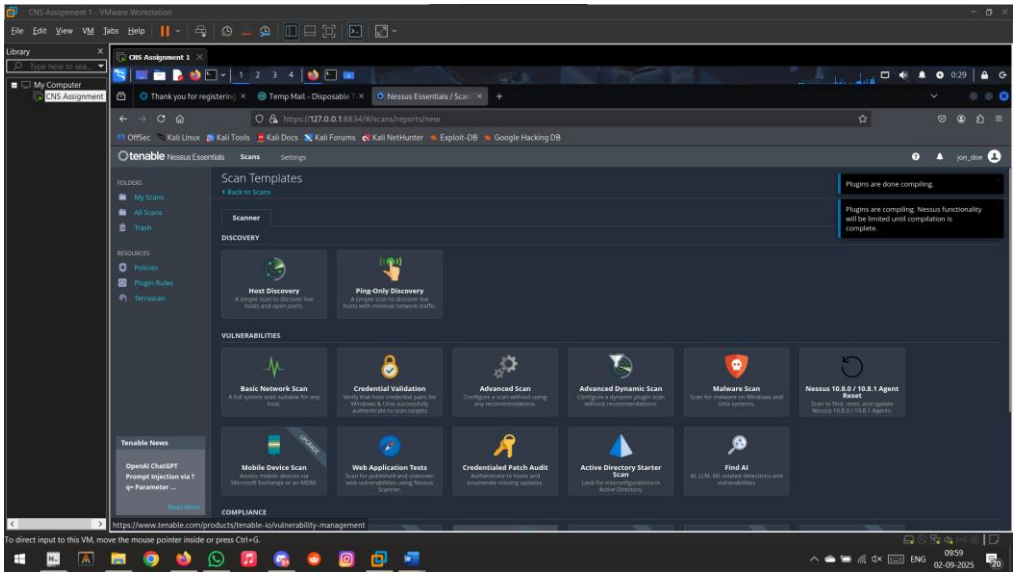

tenable
Nessus
Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
jon_doe
Password *
123456789
Back
Submit

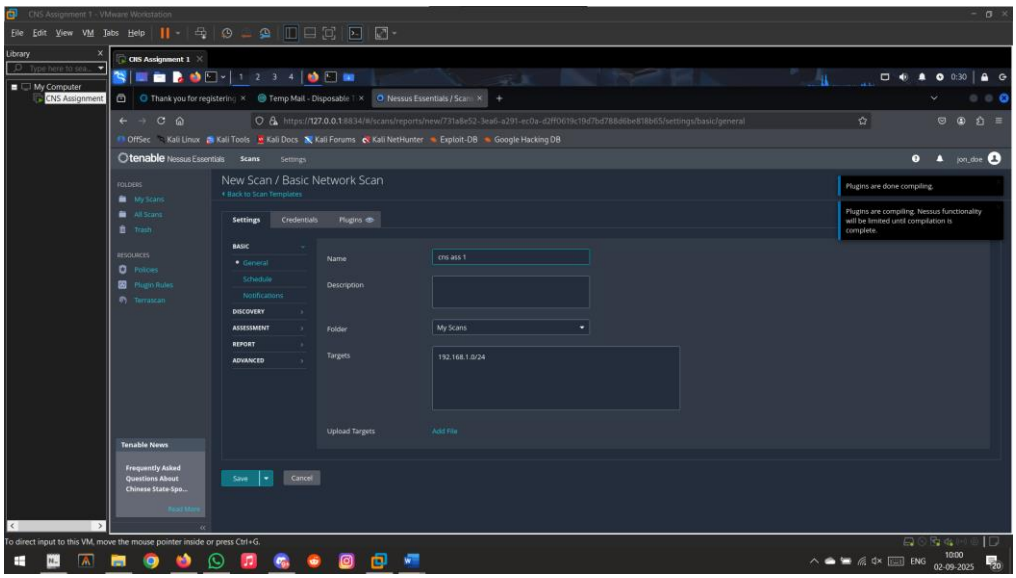

tenable
Nessus
Initializing
Please wait while Nessus is initializing.
Downloading plugins...

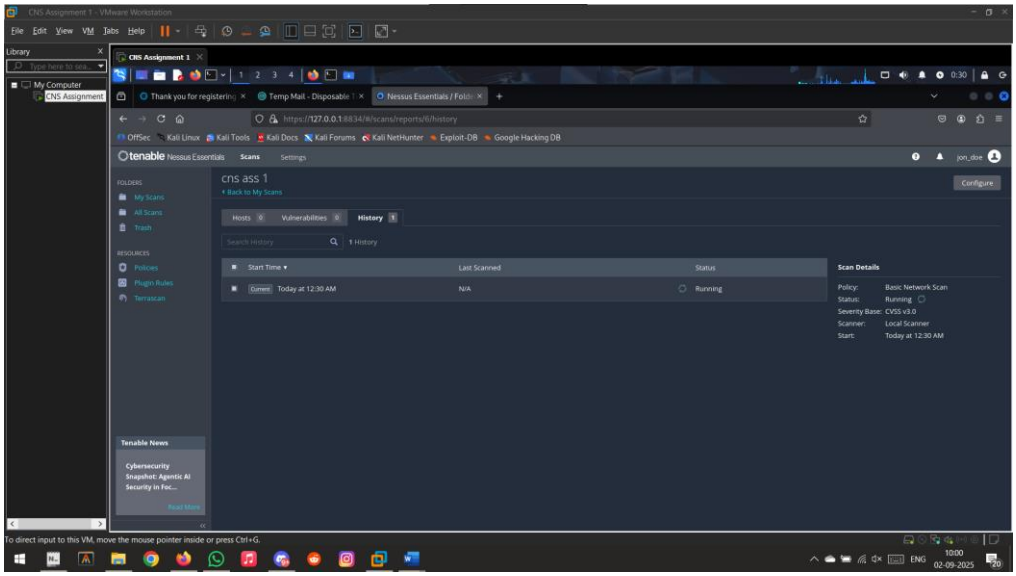

My Scans
Plugins are compiling. Nessus functionality will be limited until compilation is complete.

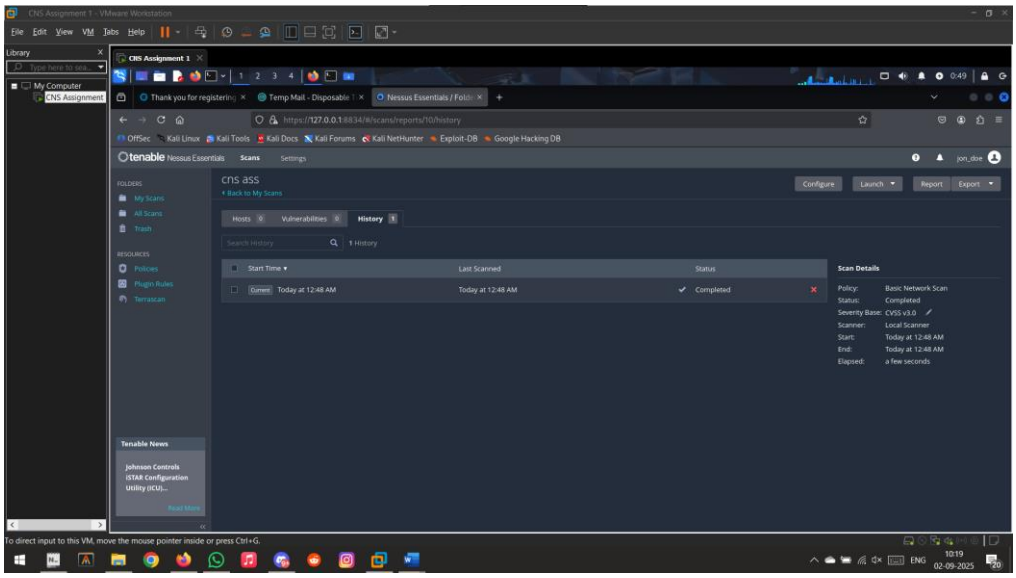

My Scans
New Folder
Name
cns ass 1
Create
Cancel

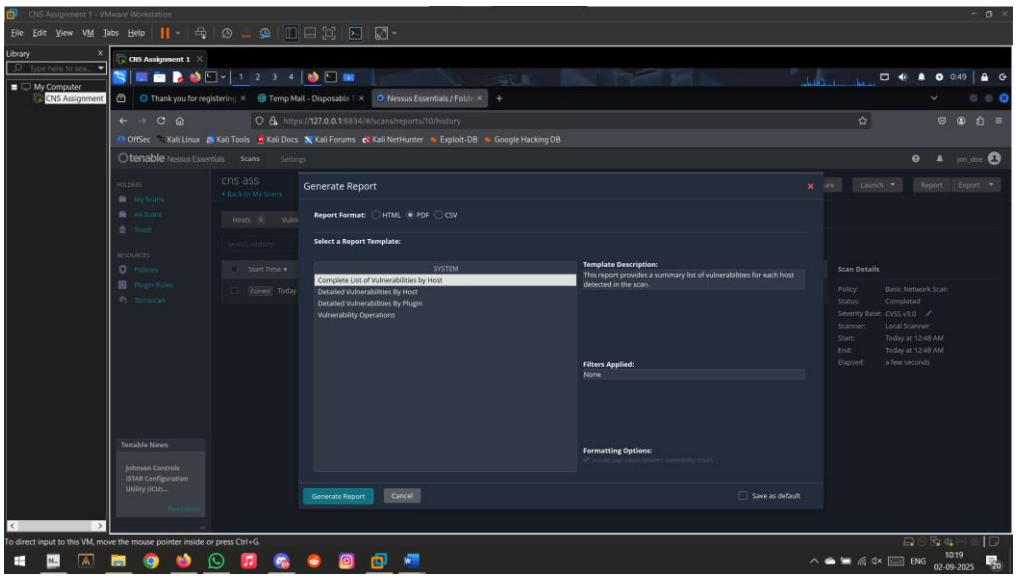

CNS Assignment 1 - VMware Workstation
My Scans
Welcome to Nessus Essentials
Close
Submit
Plugins are done compiling.

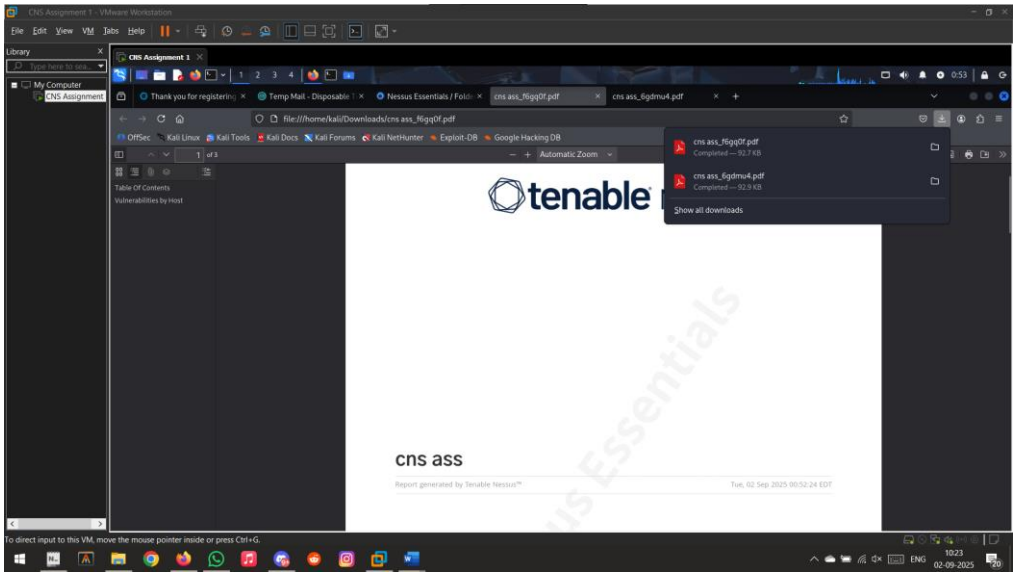

CNS Assignment 1 - VMware Workstation
Scan Templates
DISCOVERY
Host Discovery
Ping-Only Discovery
VULNERABILITIES
Basic Network Scan
Credential Validation
Advanced Scan
Advanced Dynamic Scan
Malware Scan
Mobile Device Scan
Web Application Tests
Credentialed Patch Audit
Active Directory Starter Scan
Find AI
COMPLIANCE
Plugins are done compiling.


CNS Assignment 1 - VMware Workstation
New Scan / Basic Network Scan
Settings
Credentials
Plugins
Name
cns ass 1
Description
Folder
My Scans
Targets
192.168.1.0/24
Upload Targets
Add File
Save
Cancel
Plugins are done compiling.


CNS Assignment 1 - VMware Workstation
cns ass 1
Configure
Hosts
Vulnerabilities
History
Start Time
Last Scanned
Status
Today at 12:30 AM
N/A
Running
Scan Details
Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:30 AM
Tenable News
Cybersecurity Snapshot: Agentic AI Security in Foc...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


CNS Assignment 1 - VMware Workstation
cns ass
Configure
Launch
Report
Export
Hosts
Vulnerabilities
History
Start Time
Last Scanned
Status
Today at 12:48 AM
Today at 12:48 AM
Completed
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:48 AM
End: Today at 12:48 AM
Elapsed: a few seconds
Tenable News
Johnson Controls iSTAR Configuration Utility (ICU)...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


CNS Assignment 1 - VMware Workstation
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Generate Report
Cancel
Save as default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


cns ass
Report generated by Tenable Nessus™
Tue, 02 Sep 2025 00:52:24 EDT
cns ass_f6gq0f.pdf
cns ass_6gdmu4.pdf
Show all downloads

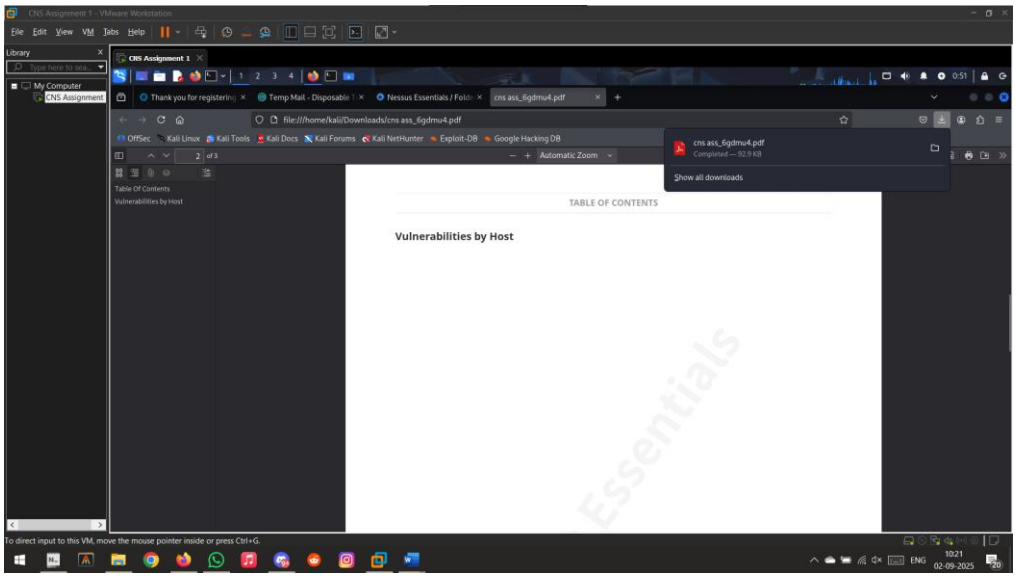
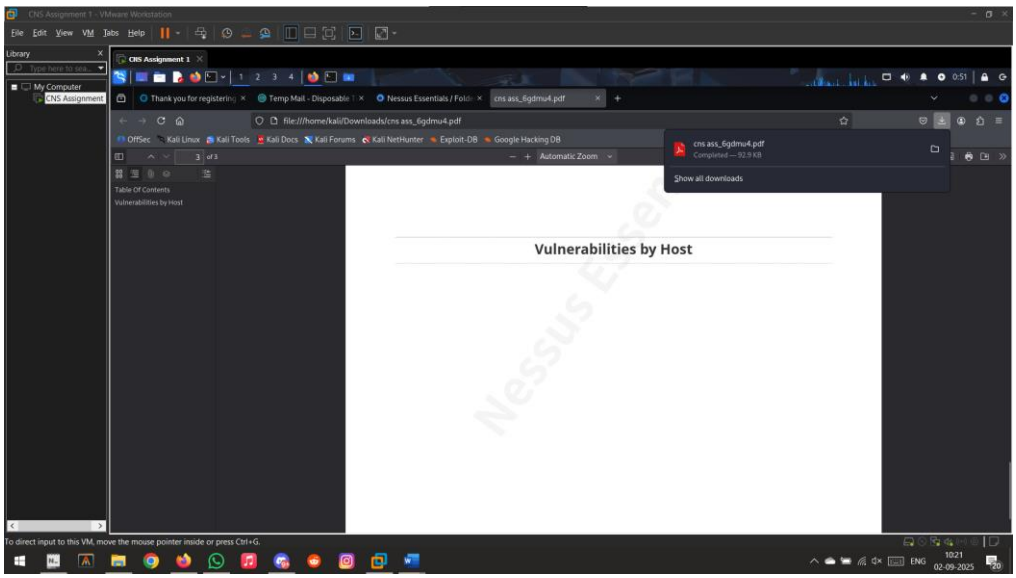


TABLE OF CONTENTS
Vulnerabilities by Host
cns ass_6gdmu4.pdf
Show all downloads


Vulnerabilities by Host
cns ass_6gdmu4.pdf
Show all downloads

Nmap:

Basic Ping Device Sweep: nmap -sn 192.168.1.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.165.255

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 00:59 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
```

Service & Version Detection: nmap -sv 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 01:01 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00033s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Aggressive Scan (OS + services + scripts): nmap -A 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 01:02 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds
```

Vulnerability Script Scan: nmap –script vuln 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.1.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 01:03 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00047s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 15.35 seconds
```

Top 20 fastest ports (stealthy recon):

nmap --top-ports 20 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ nmap --top-ports 20 192.168.1.105

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 01:05 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00052s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```