



TECH2400

Cyber Security

Workshop 9
Incident Response and
Management (Part 1)



COMMONWEALTH OF AUSTRALIA

Copyright Regulations 1969

WARNING

This material has been reproduced and communicated to you by or on behalf of Kaplan Business School pursuant to Part VB of the *Copyright Act 1968* (**the Act**).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.



Subject Learning Outcomes

LO1:	Explain the terminology associated with cyber security.
LO2:	Explain the vulnerabilities and threats pertaining to the IT infrastructure of organisations.
LO3:	Analyse risk mitigation strategies that address cyber security vulnerabilities and threats.
LO4:	Describe privacy, legal, ethical and security issues and solutions related to the IT infrastructure and use of technologies in organisations.



Weekly Schedule

Week	Topic
Week 1	Introduction and Cyber Security Foundations
Week 2	Cyber Threat Landscape
Week 3	Risk Management in Cyber Security
Week 4	Cryptography Basics and Network Fundamentals Review
Week 5	Network Security Fundamentals
Week 6	Study Success Week
Week 7	Access Control and Authentication
Week 8	Ethics and Legal Aspects of Cyber Security
Week 9	Incident Response and Management (Part 1)
Week 10	Incident Response and Management (Part 2)
Week 11	Introduction to Secure Software Development
Week 12	In-Class Assessment



Weekly Schedule

Week	Topic
Week 1	Introduction and Cyber Security Foundations
Week 2	Cyber Threat Landscape
Week 3	Risk Management in Cyber Security
Week 4	Cryptography Basics and Network Fundamentals Review
Week 5	Network Security Fundamentals
Week 6	Study Success Week
Week 7	Access Control and Authentication
Week 8	Ethics and Legal Aspects of Cyber Security
Week 9	Incident Response and Management (Part 1)
Week 10	Incident Response and Management (Part 2)
Week 11	Introduction to Secure Software Development
Week 12	In-Class Assessment

What to expect from this workshop

Incident Response Lifecycle

- Key phases: Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Lessons Learned

Hands-on Exercise: ELK Stack

- Using Elasticsearch, Logstash, and Kibana for incident detection & analysis



Incident Response

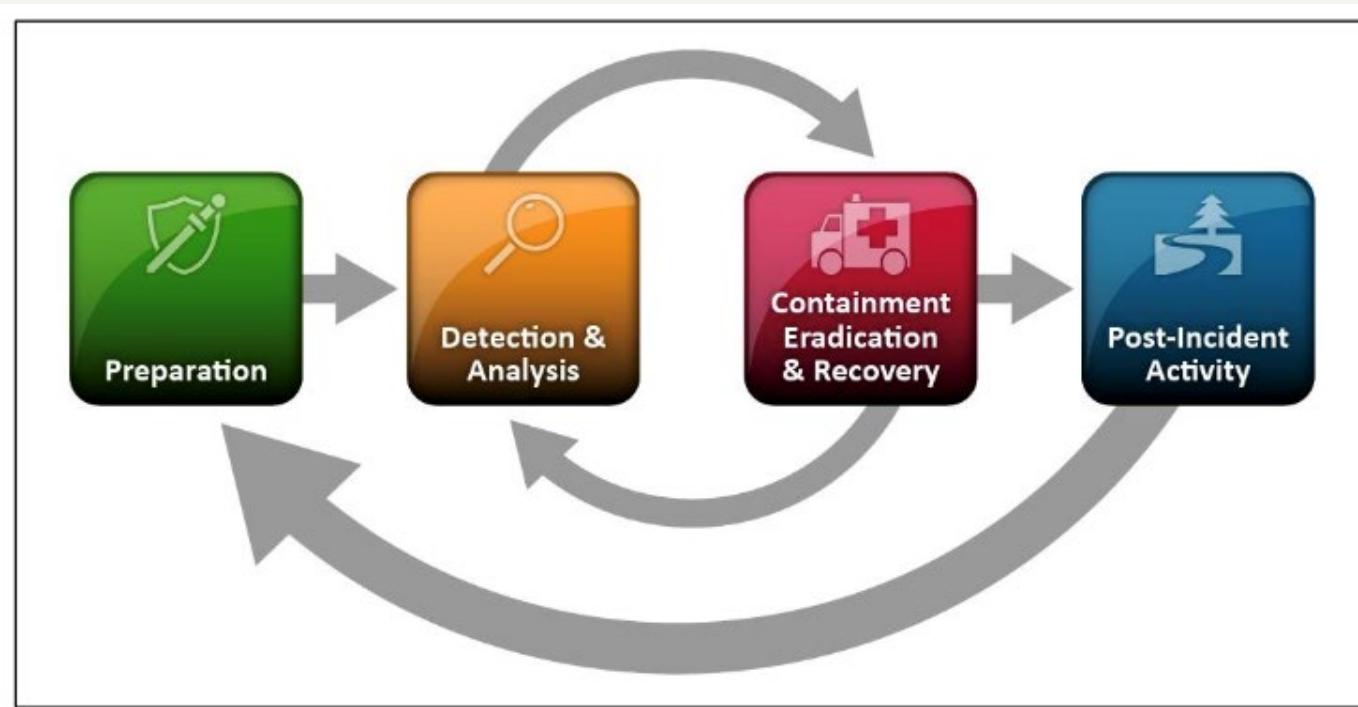
Incident response is the structured approach organisations take to handle and manage security incidents, cyber threats, or breaches to minimise damage and restore operations.

A strong incident response strategy helps:

- Reduce operational downtime
- Mitigate financial and reputational loss
- Ensure compliance with regulations

Incident Response Lifecycle

This model from the National Institute of Standards and Technology (NIST) is a widely adopted standard for incident response teams to systematically manage and mitigate cyber security incidents.



National Institute of Standards and Technology (NIST), 2012. *Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2)*. Gaithersburg, MD: U.S. Department of Commerce. Available at: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> [Accessed 27 Feb. 2025].



Incident Response Lifecycle

Sometimes referred to as PICERL framework or model

NIST	PICERL
Preparation	Preparation
Detection & Analysis	Identification
Containment, Eradication, & Recovery	Containment Eradication Recovery
Post-Incident Activity	Lessons Learned



Preparation

Goal: Establish readiness to respond to incidents.

Key Activities:

- Develop & maintain an Incident Response Plan (IRP)
- Define roles & responsibilities of the Incident Response Team (IRT)
- Implement security tools (SIEM, IDS/IPS, endpoint protection)
- Conduct risk assessments & threat modeling
- Perform incident response training & simulations (tabletop exercises, red/blue team drills)



Identification

Goal: Detect and confirm an incident.

Key Activities:

- Monitor security alerts and logs (SIEM, IDS/IPS)
- Analyse anomalies & correlate threat intelligence
- Classify incidents (low, medium, high severity)
- Gather evidence for investigation
- Activate the Incident Response Team (IRT)



Containment

Goal: Limit the impact and prevent further damage.

Key Activities:

- Short-term containment (isolating affected systems, blocking malicious activity)
- Long-term containment (applying patches, implementing network segmentation)
- Preserve forensic evidence for root cause analysis
- Coordinate with stakeholders (IT, legal, management)

Eradication

Goal: Remove the threat and restore integrity.

Key Activities:

- Identify & remove malware, vulnerabilities, and compromised accounts
- Patch affected systems and update security configurations
- Validate that no backdoors or persistent threats remain
- Conduct forensic analysis to understand attack vectors

Recovery

Goal: Restore normal operations securely.

Key Activities:

- Validate clean systems before reconnecting
- Monitor for any signs of reinfection or ongoing threats
- Restore data from backups (if necessary)
- Conduct post-recovery testing to ensure stability



Lessons Learned

Goal: Improve future response and strengthen security.

Key Activities:

- Conduct post-incident review (PIR)
- Document findings, root causes, and response effectiveness
- Update incident response plans & playbooks
- Implement additional security controls to prevent recurrence
- Provide training based on insights from the incident



Role of Software

Software systems enhance efficiency, accuracy, and speed in incident response.

Different tools support various phases of the incident response lifecycle (detection, analysis, containment, recovery, and reporting).

A well-integrated set of tools ensures proactive threat management and rapid response.



Examples of Software

Category	Examples	Purpose
Security Information & Event Management (SIEM)	ELK Stack , Splunk, Microsoft Sentinel	Centralised log collection, correlation, and alerting
Endpoint Detection & Response (EDR)	CrowdStrike, SentinelOne, Microsoft Defender	Detects and responds to endpoint threats
Threat Intelligence Platforms	MISP, Recorded Future, VirusTotal	Provides intelligence on emerging threats
Security Orchestration, Automation, & Response	Cortex XSOAR, IBM Resilient, Splunk SOAR	Automates incident response workflows
Forensic & Investigation Tools	Autopsy, Velociraptor, Wireshark	Helps analyse and reconstruct cyber incidents



Elasticsearch, Logstash, and Kibana (ELK)

ELK is an open-source log management and analytics solution used for security monitoring.

Component	Function	Benefit
Elasticsearch	Stores and indexes large volumes of log data for fast searching.	Enables quick log analysis and threat hunting.
Logstash	Collects, processes, and transforms log data from multiple sources.	Aggregates logs from firewalls, endpoints, and network devices.
Kibana	Provides dashboards and visualisations for data analysis.	Helps monitor threats, detect anomalies, and conduct forensic investigations.



Elasticsearch, Logstash, and Kibana (ELK)

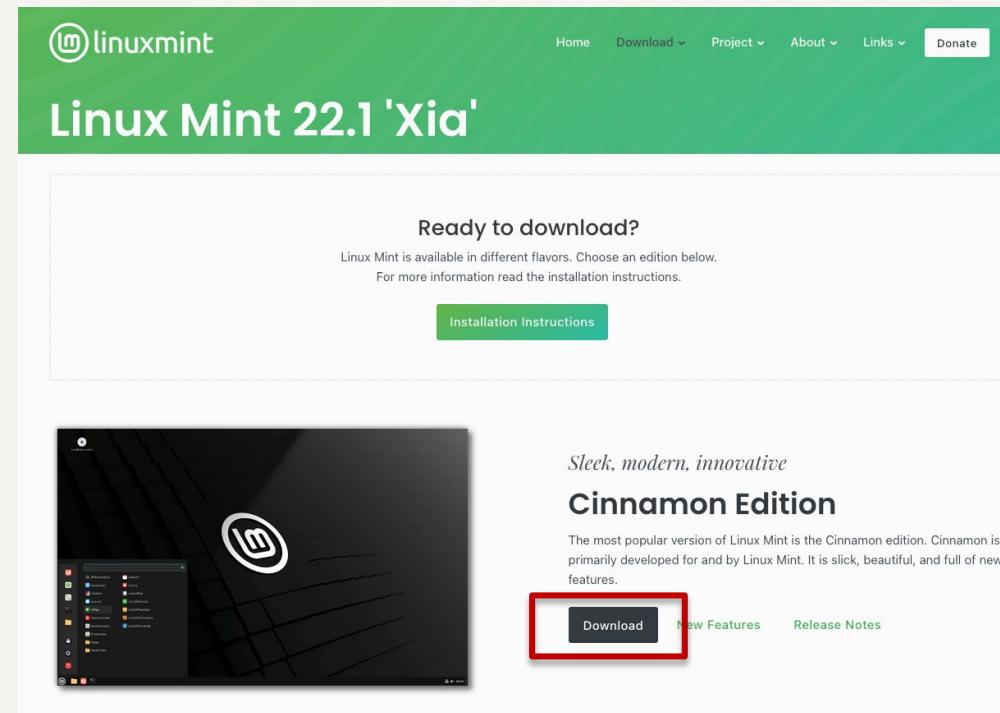
- Core component of many SIEM solutions due to its powerful log management and visualisation capabilities.
- When configured for security monitoring, ELK supports real-time threat detection, incident response, and compliance reporting.
- When integrated with Security Orchestration, Automation, and Response (SOAR) tools, ELK enables automated threat mitigation.
- ELK can function as a lightweight, open-source alternative to commercial SIEMs or as a supplementary tool for deeper log analysis.

Activity: Linux Mint Installation

Linux Mint provides a straightforward, native environment for ELK, ensuring better performance and easier setup.

Step 1: Download the Linux Mint ISO

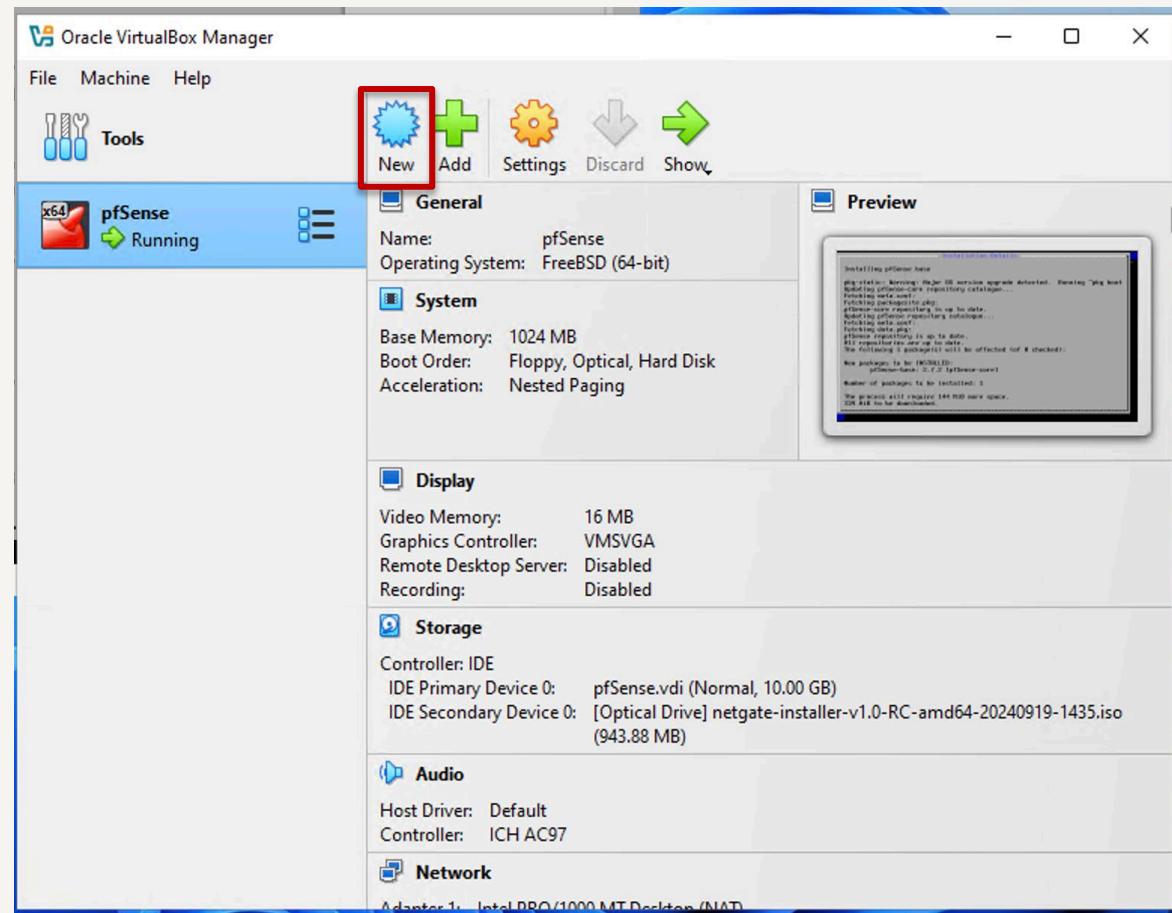
- Go to <https://www.linuxmint.com/download.php>
- Choose the Cinnamon edition
- Select a mirror near your location
- Download the ISO file



Activity: Linux Mint Installation

Step 2: Create a new virtual machine

- Launch VirtualBox
- Click on the New button to create a new VM

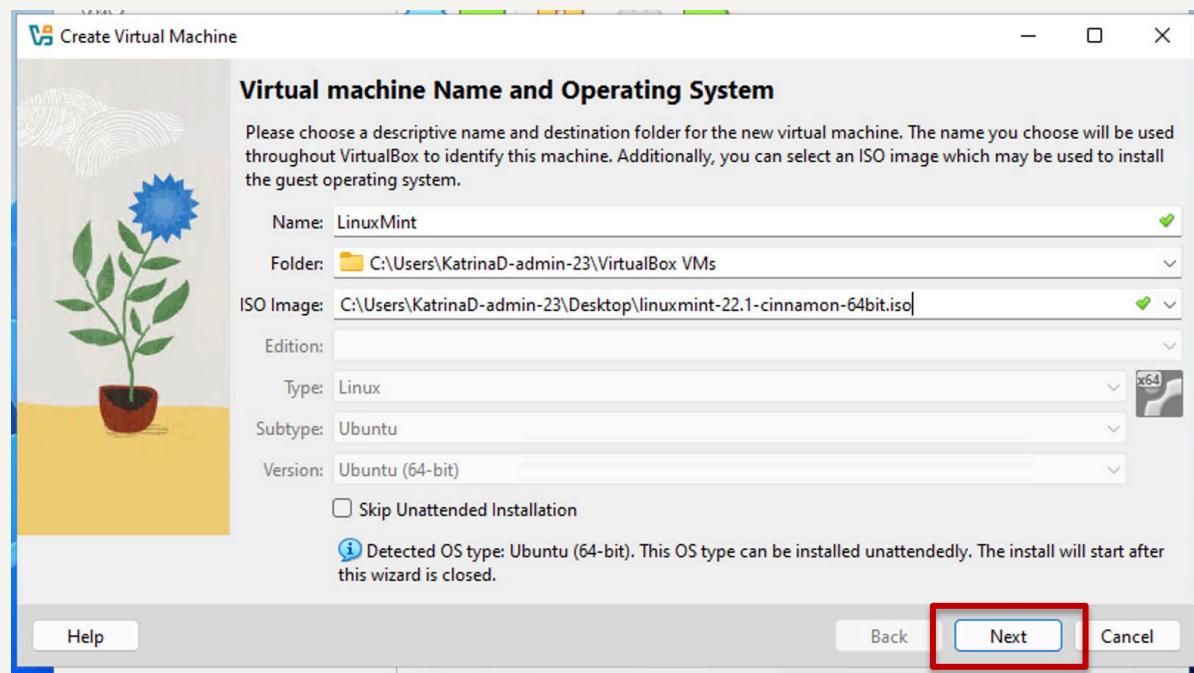


KAPLAN

Activity: Linux Mint Installation

Step 2: Create a new virtual machine

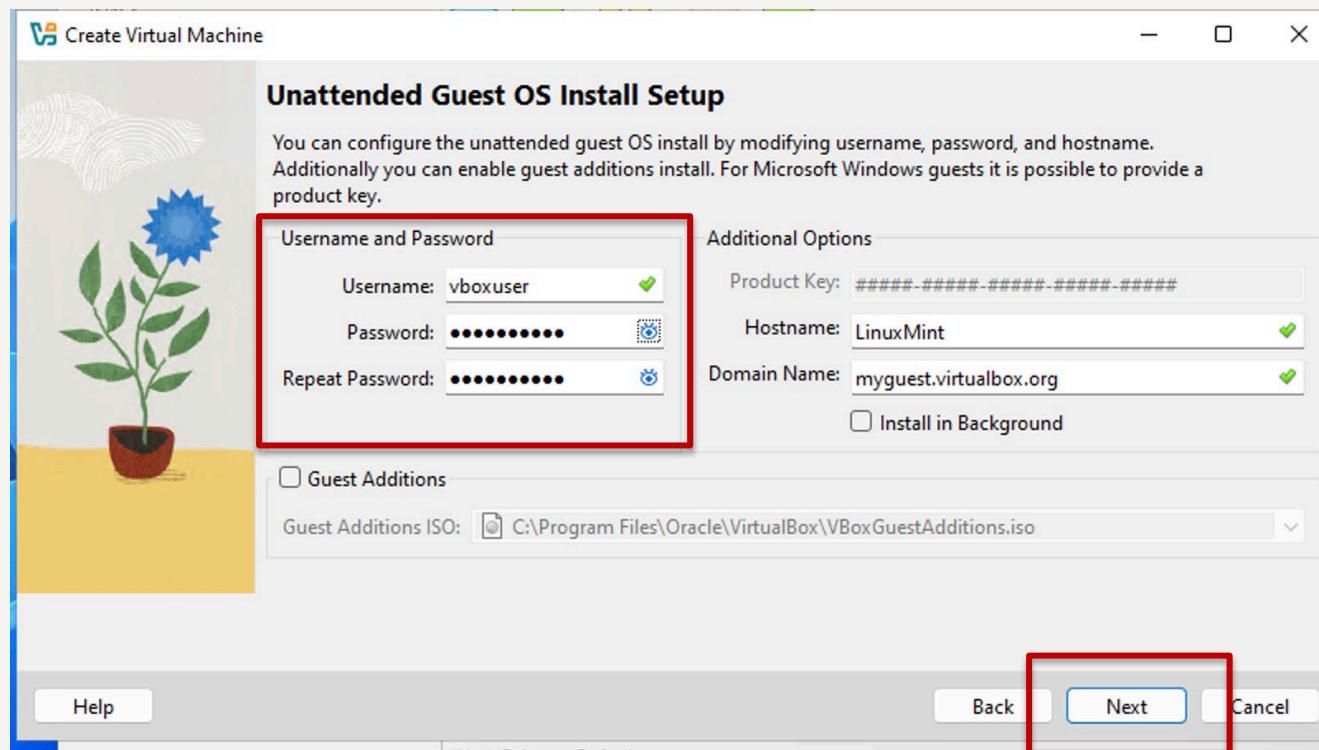
- Configure the VM
 - o Name: LinuxMint
 - o ISO Image: Select downloaded iso file
- Click Next



Activity: Linux Mint Installation

Step 2: Create a new virtual machine

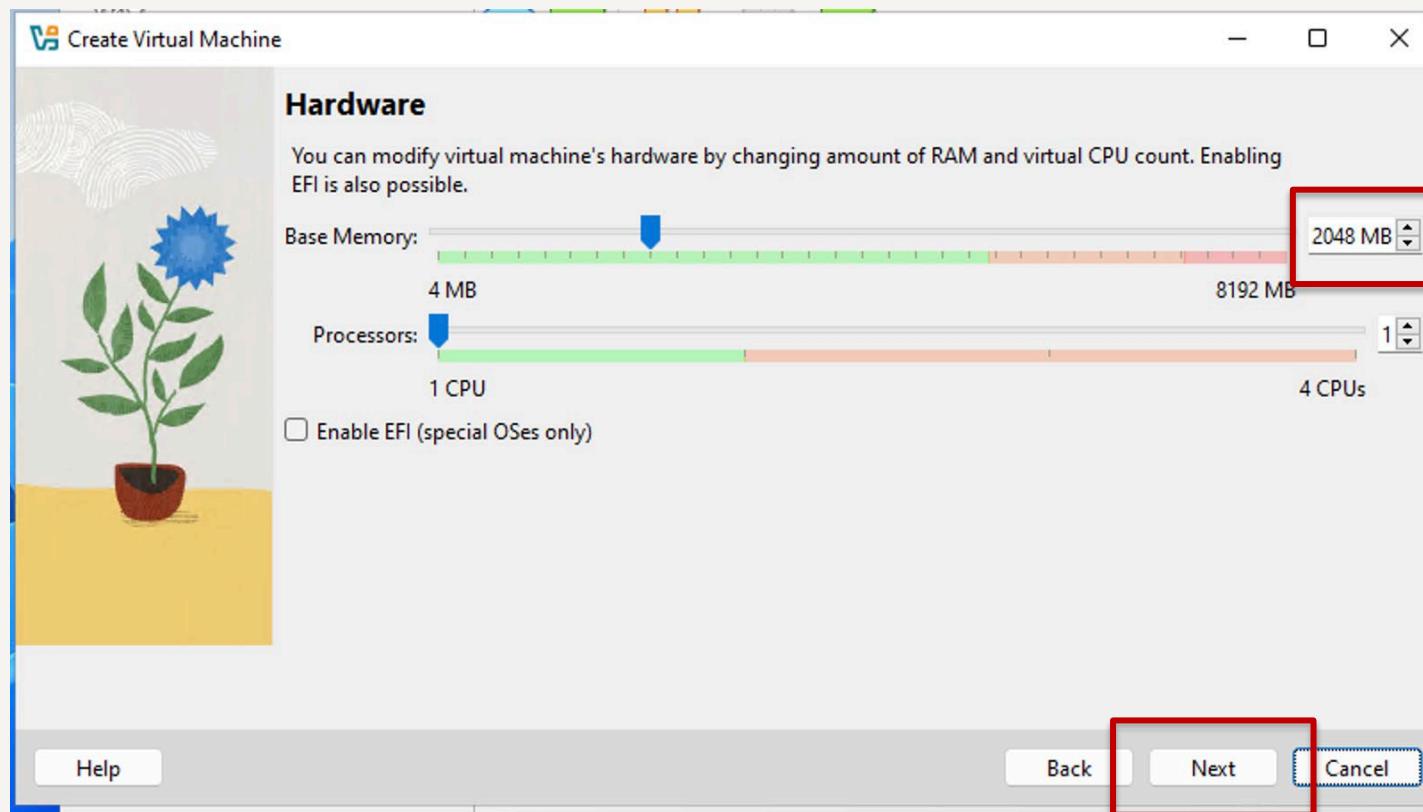
- Change default password
- Click Next



K Activity: Linux Mint Installation

Step 2: Create a new virtual machine

- Allocate at least 2048 MB (2GB) of RAM

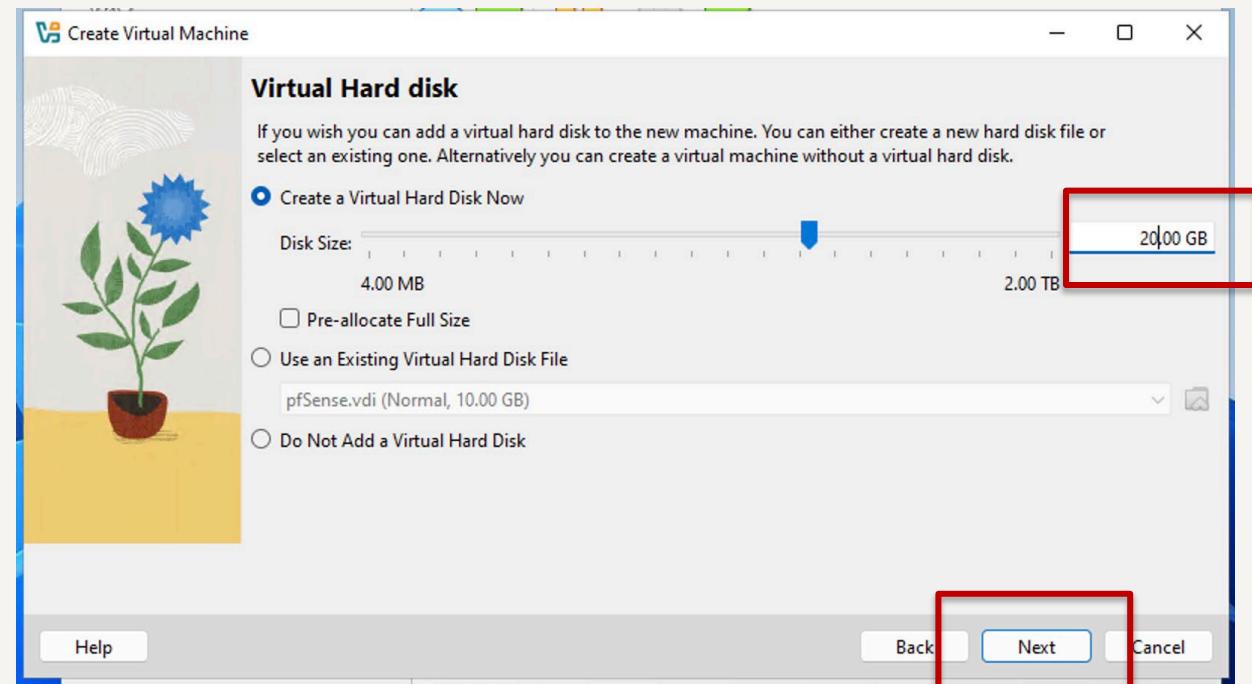


KAPLAN

Activity: Linux Mint Installation

Step 2: Create a new virtual machine

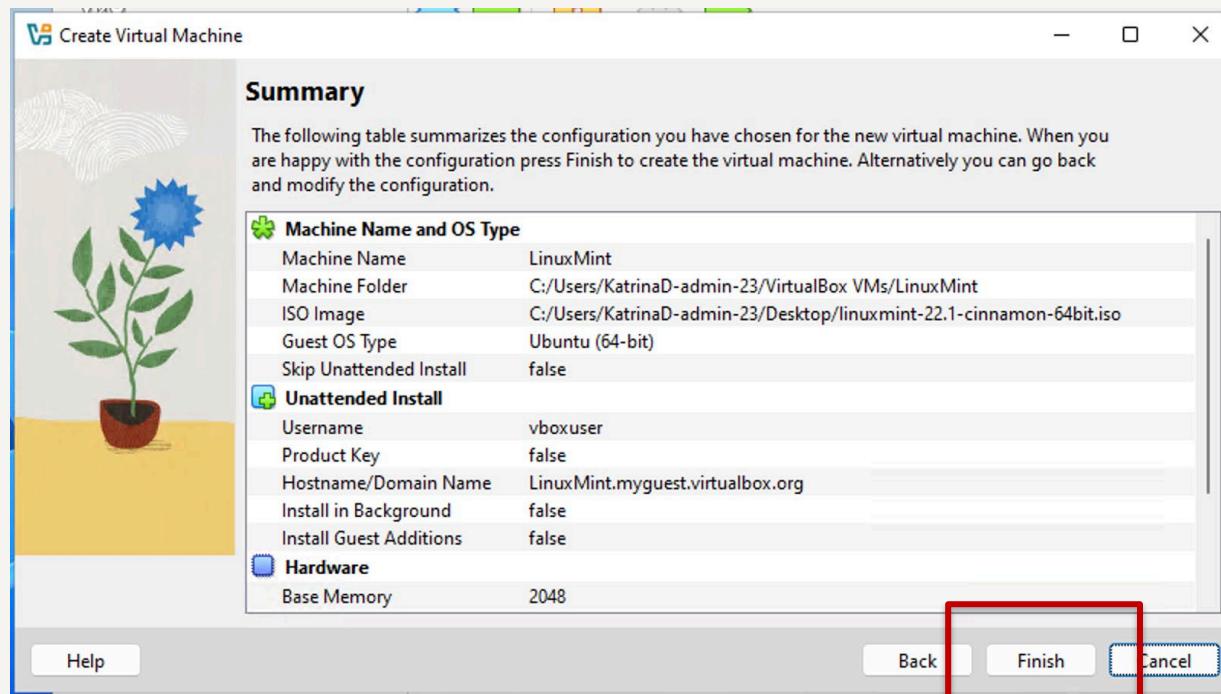
- Create a Virtual Hard Disk:
 - o Choose Create a Virtual Hard Disk Now
 - o Set the size of the virtual hard disk to 20GB or more
 - o Click Next



Activity: Linux Mint Installation

Step 2: Create a new virtual machine

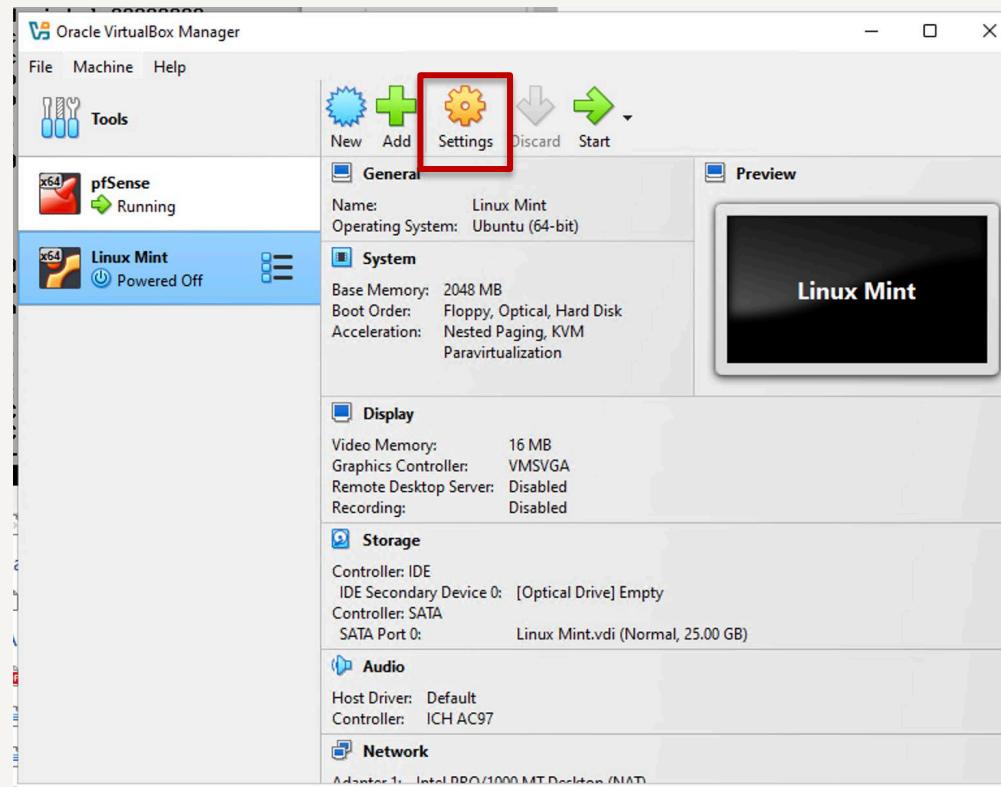
- Review the Summary
- Click Finish



Activity: Linux Mint Installation

Step 3: Mount the Linux Mint ISO to the Virtual Machine

- Select the Linux Mint VM in VirtualBox and click on Settings

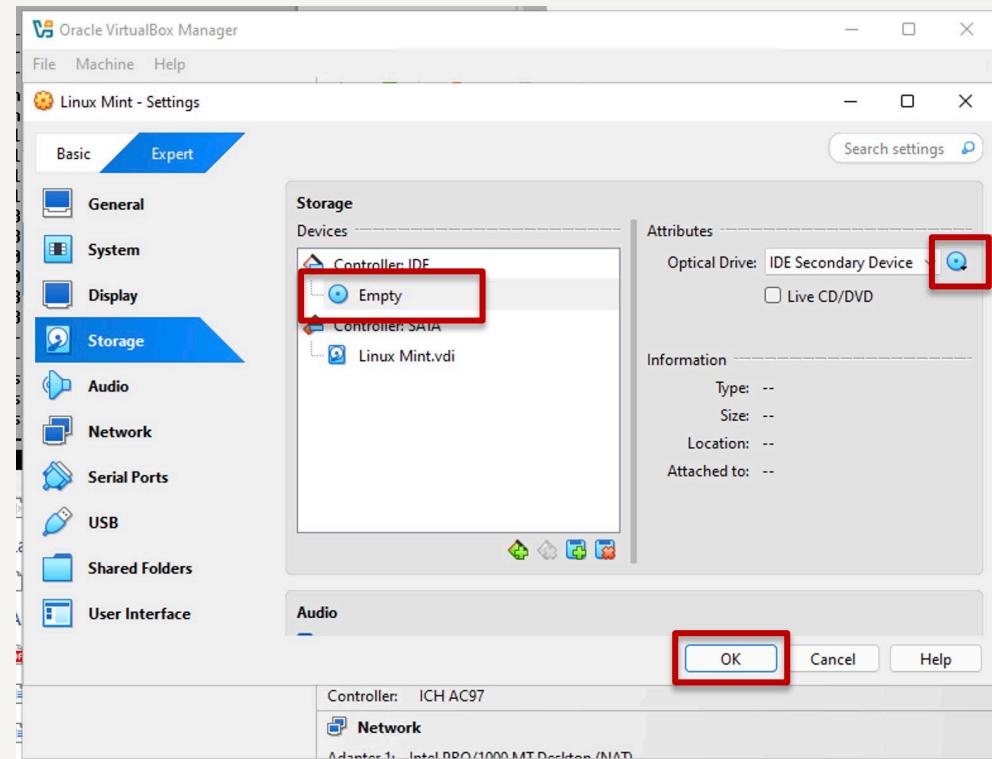


KAPLAN

Activity: Linux Mint Installation

Step 3: Mount the Linux Mint ISO to the Virtual Machine

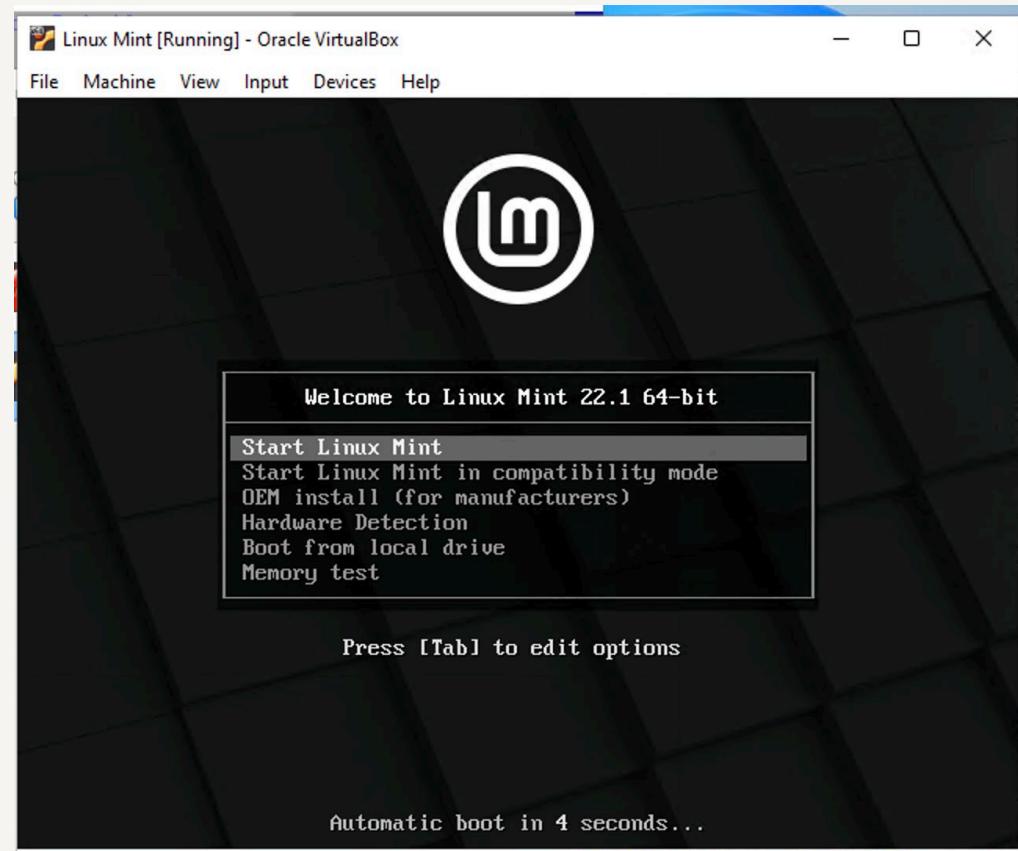
- Go to Storage:
 - o Under the "Controller: IDE section," click on the empty disk icon
 - o On the right side, click the disk icon next to "Optical Drive" and select Choose a disk file
 - o Browse to the location where you saved the Linux Mint ISO file and select it
- Click Open
- Click OK



Activity: Linux Mint Installation

Step 4: Start the Virtual Machine

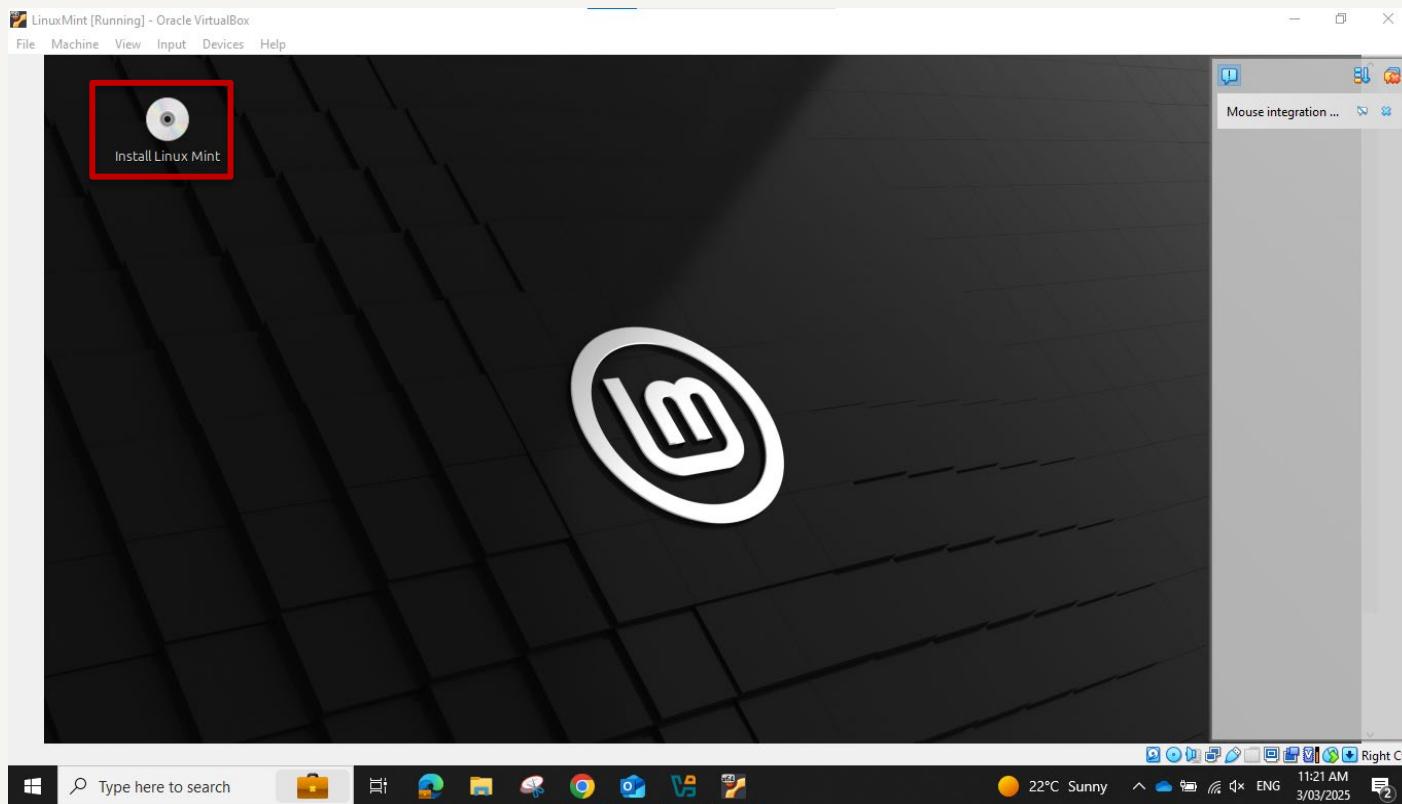
- Click Start in VirtualBox to boot from the Linux Mint ISO
- Wait for the Linux Mint welcome screen to appear
- Select Start Linux Mint and press Enter



K Activity: Linux Mint Installation

Step 5: Install Linux Mint

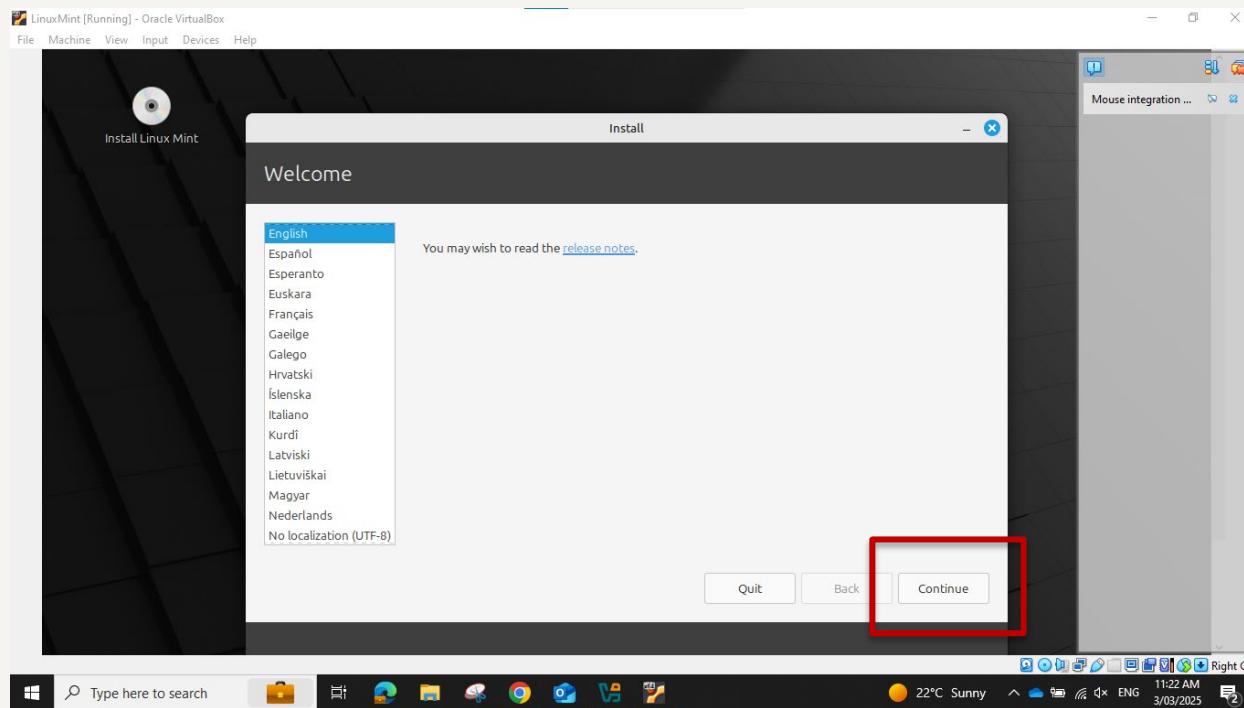
- Double-click on Install Linux Mint to launch



Activity: Linux Mint Installation

Step 5: Install Linux Mint

- Select English and click Continue

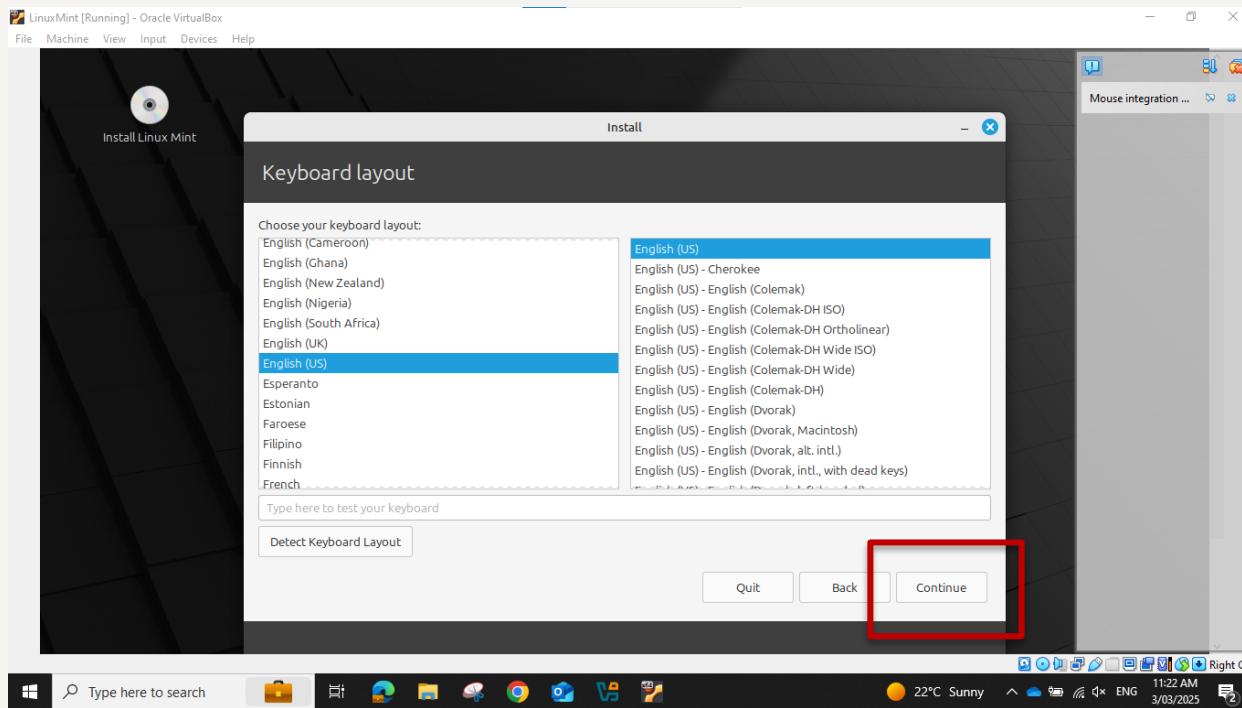


KAPLAN

Activity: Linux Mint Installation

Step 5: Install Linux Mint

- Choose your preferred keyboard layout and click Continue

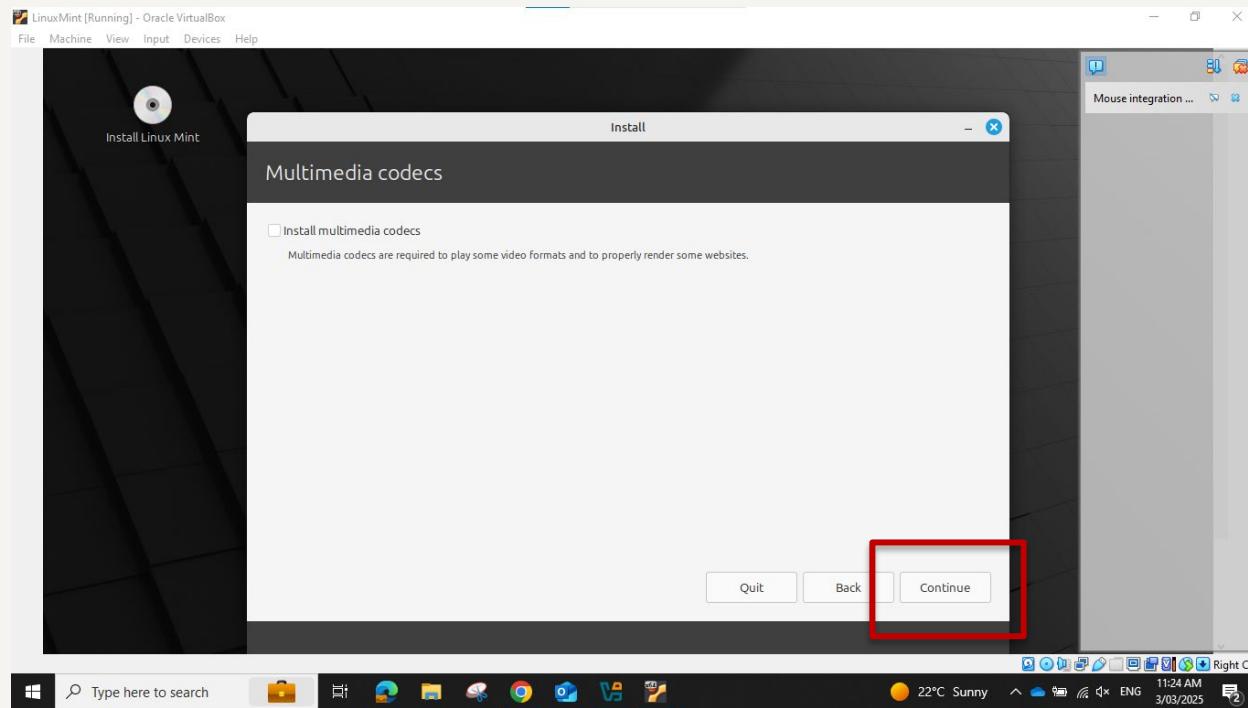


KAPLAN

Activity: Linux Mint Installation

Step 5: Install Linux Mint

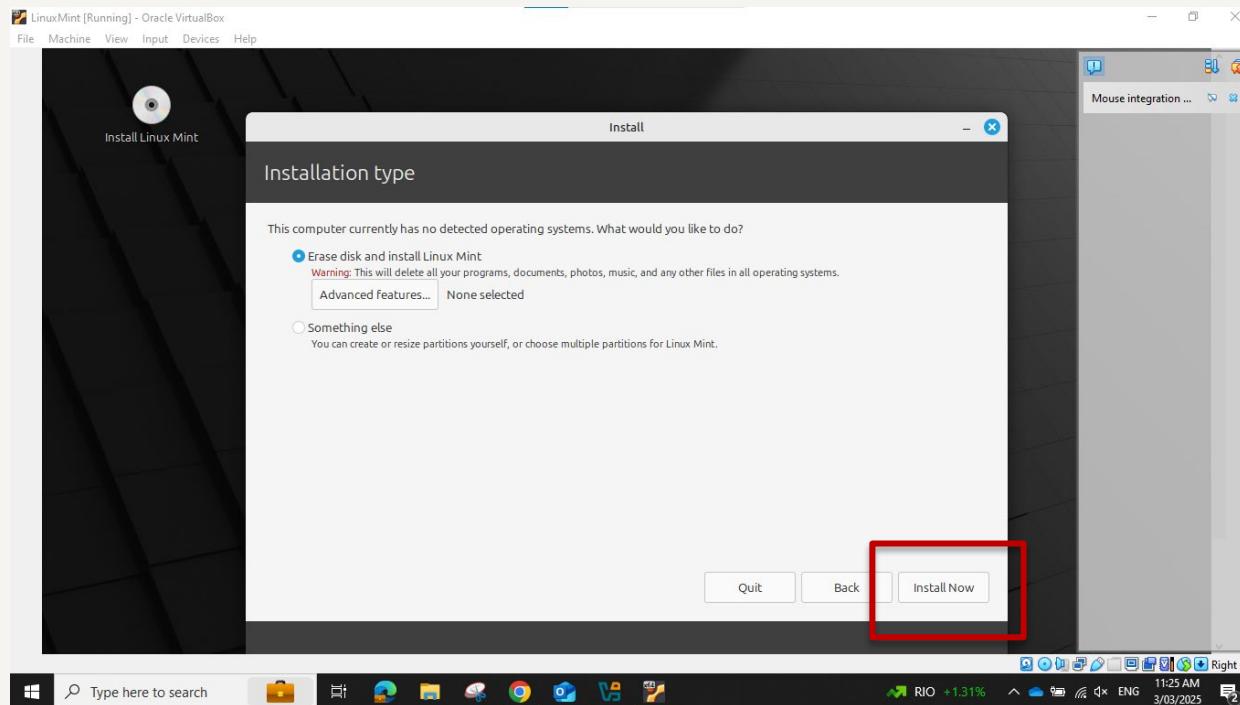
- No need to install Multimedia codecs. Click Continue



Activity: Linux Mint Installation

Step 5: Install Linux Mint

- Select Erase disk and install Linux Mint. Click Install now.

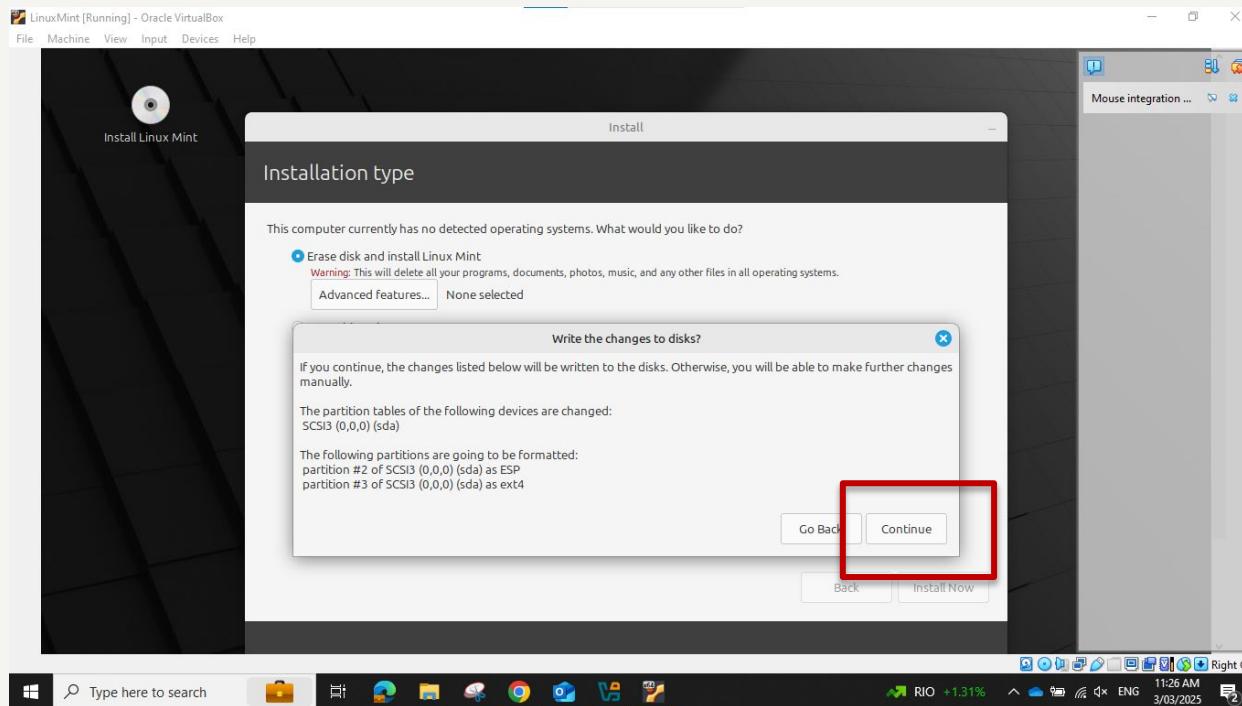


KAPLAN BUSINESS SCHOOL AUSTRALIA

Activity: Linux Mint Installation

Step 5: Install Linux Mint

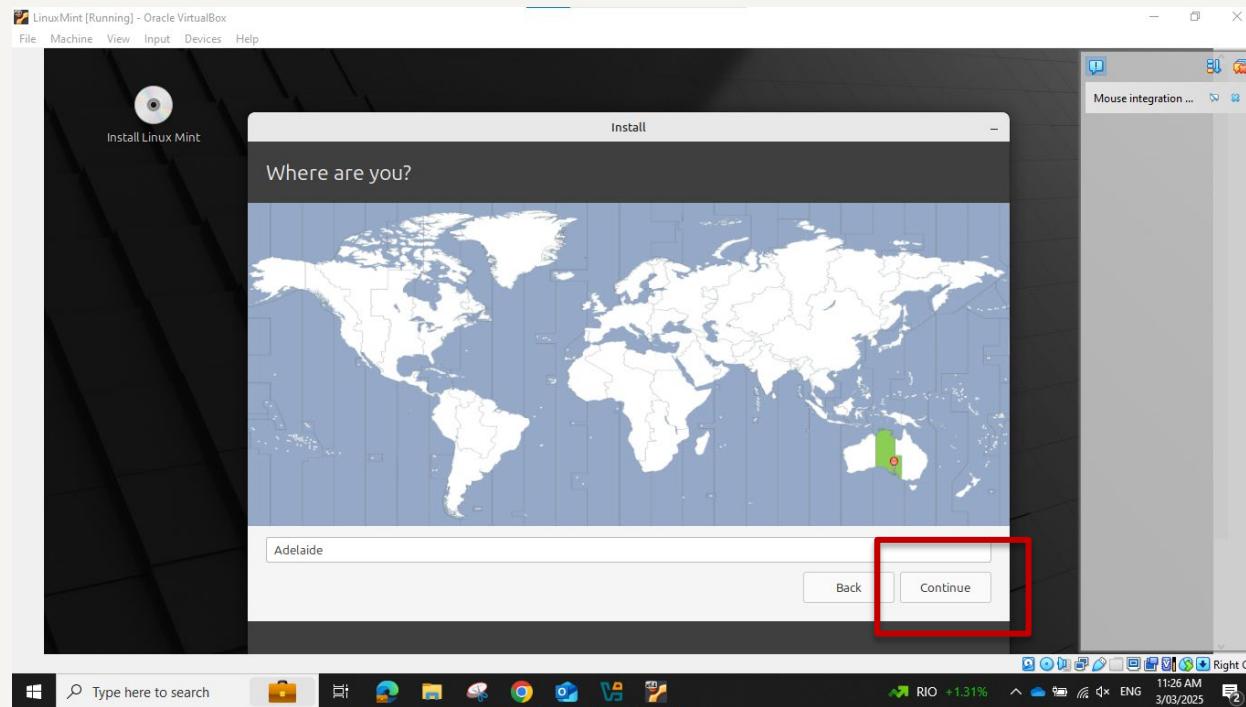
- You will get a warning message for the changes to the disk.
Confirm by clicking on Continue



Activity: Linux Mint Installation

Step 5: Install Linux Mint

- Select time zone and click Continue

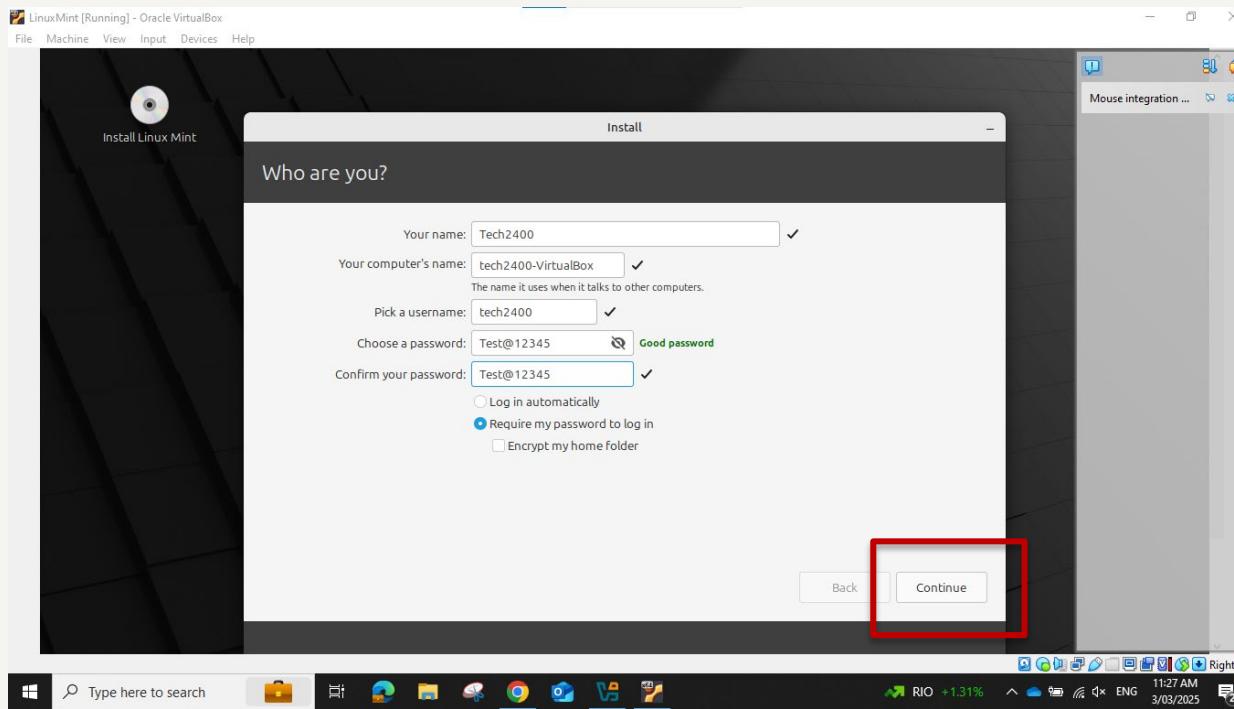


KAPLAN

Activity: Linux Mint Installation

Step 5: Install Linux Mint

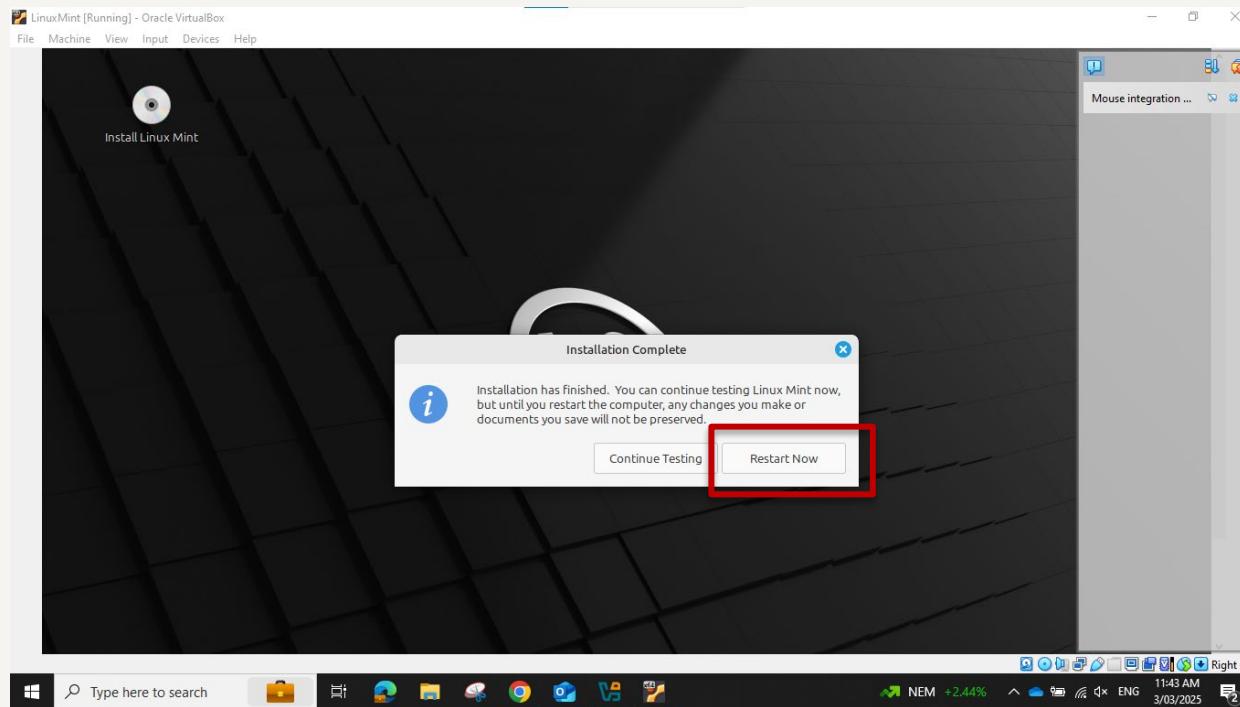
- Enter your name, computer name, username, and password.
- Click Continue.



Activity: Linux Mint Installation

Step 5: Install Linux Mint

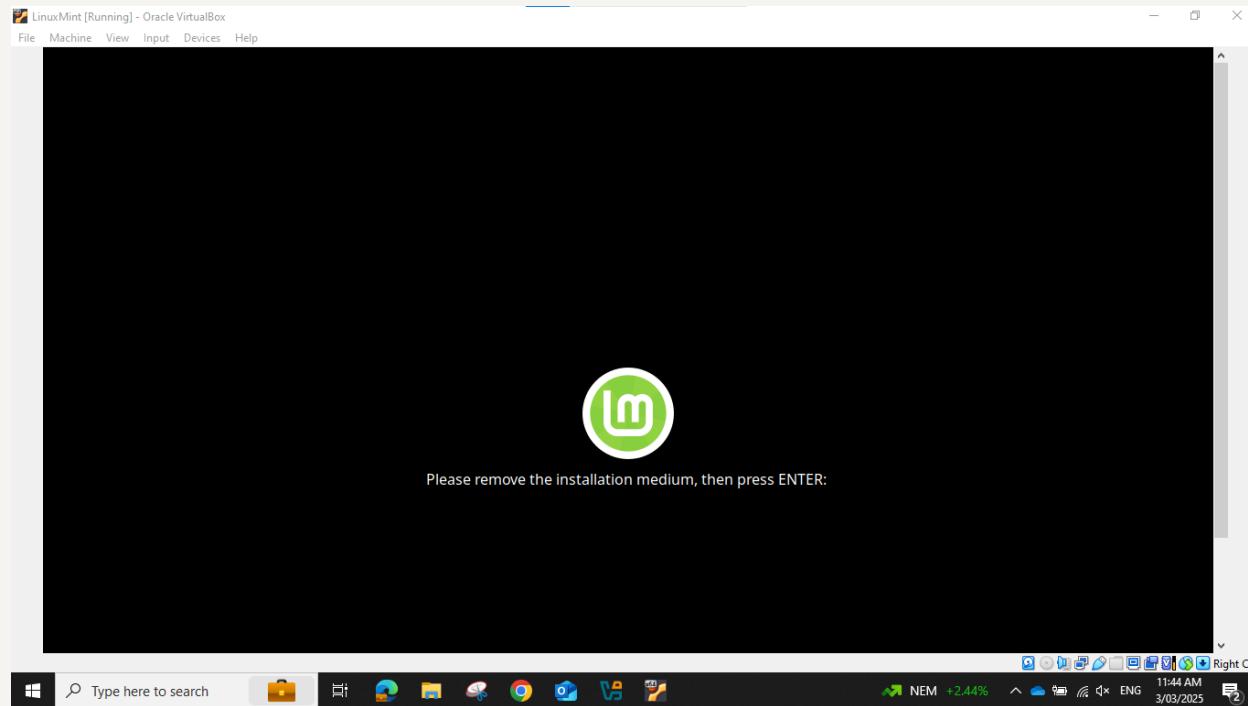
- The installation process will take a few minutes to complete. Once done, you'll be asked to reboot the system.



Activity: Linux Mint Installation

Step 6: Reboot and Log In

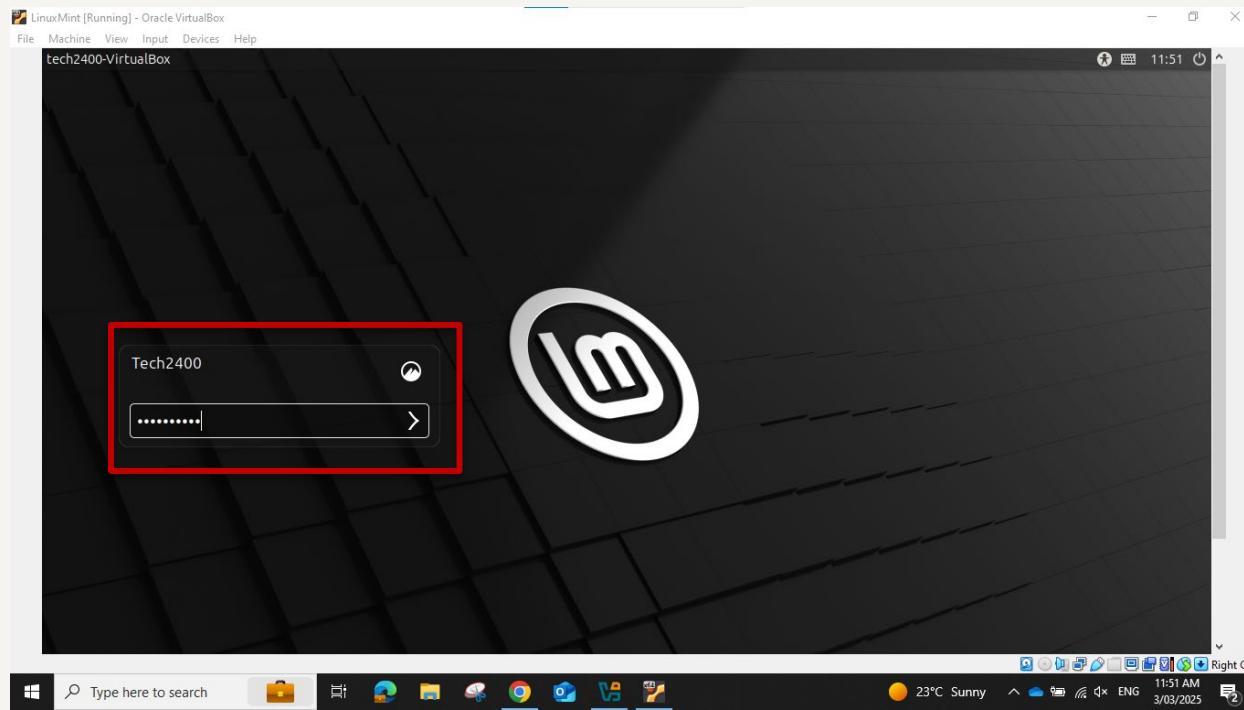
- Press Enter key when prompted to remove the installation media.



Activity: Linux Mint Installation

Step 6: Reboot and Log In

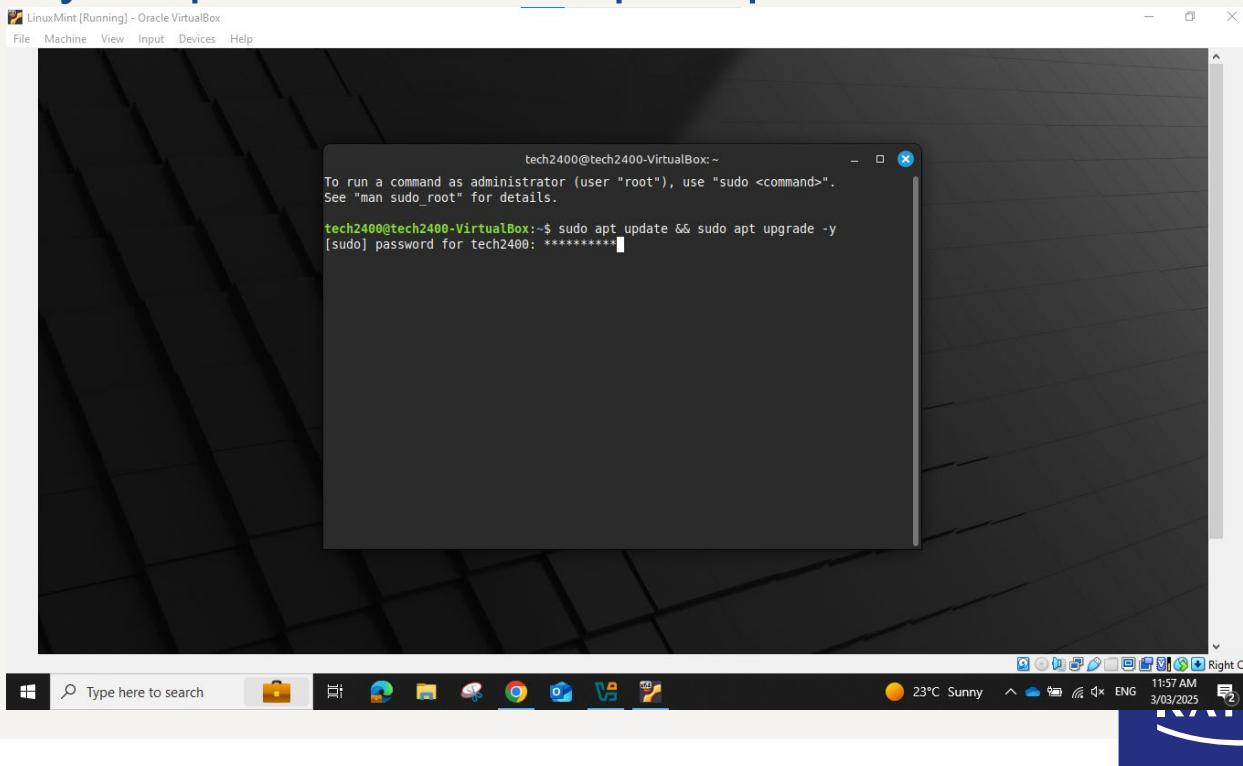
- After restarting, you should see the login screen.
- Enter your username and password to log in to Linux Mint



Activity: Linux Mint Installation

Step 7: Update the system

- After logging in, open a terminal and run the following command to update the system:
`sudo apt update && sudo apt upgrade -y`
- Enter your password when prompted



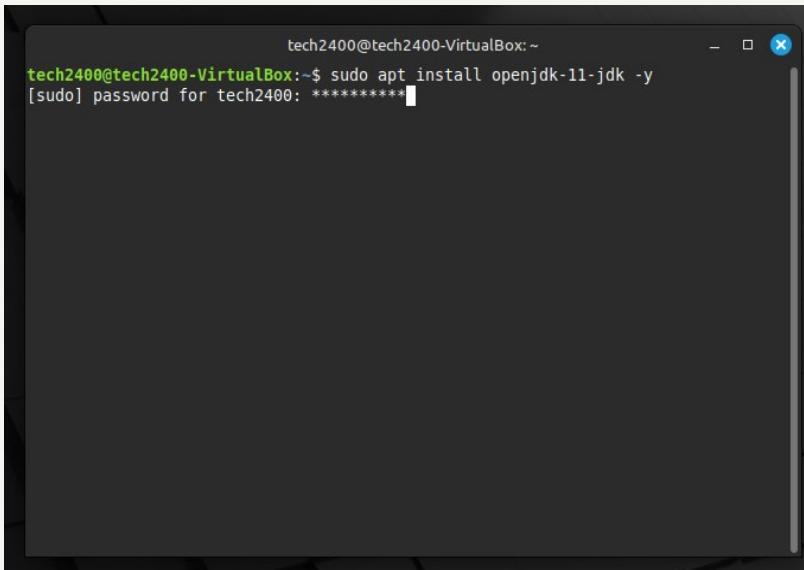
Activity: Install Java

Elasticsearch and Logstash both require Java.

OpenJDK 11 is an open-source implementation of Java SE.

Step 1: Install OpenJDK 11

- From your Terminal window
- Run `sudo apt install openjdk-11-jdk -y`
- Enter your password when prompted



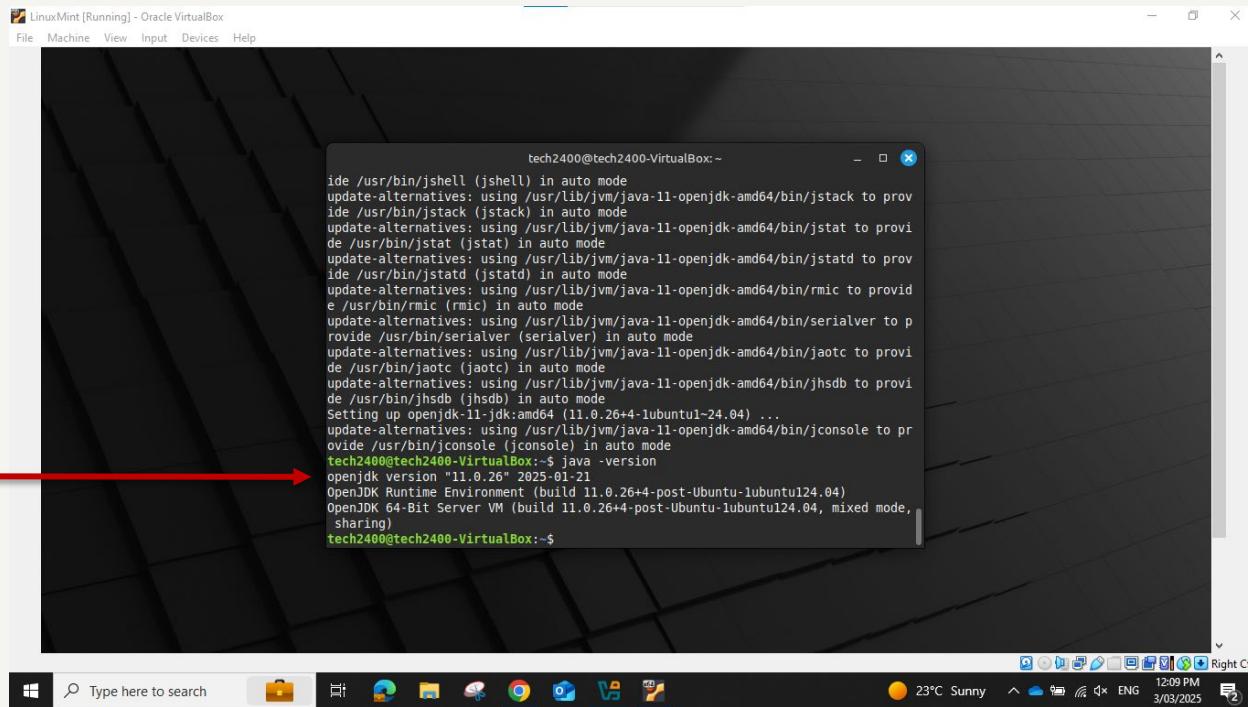
A screenshot of a terminal window titled "tech2400@tech2400-VirtualBox:~". The window contains the following text:
tech2400@tech2400-VirtualBox:~\$ sudo apt install openjdk-11-jdk -y
[sudo] password for tech2400: *****

KAPLAN

Activity: Install Java

Step 2: Verify Java installation

- Run `java -version`
- This should return the current OpenJDK version (11.x.x)



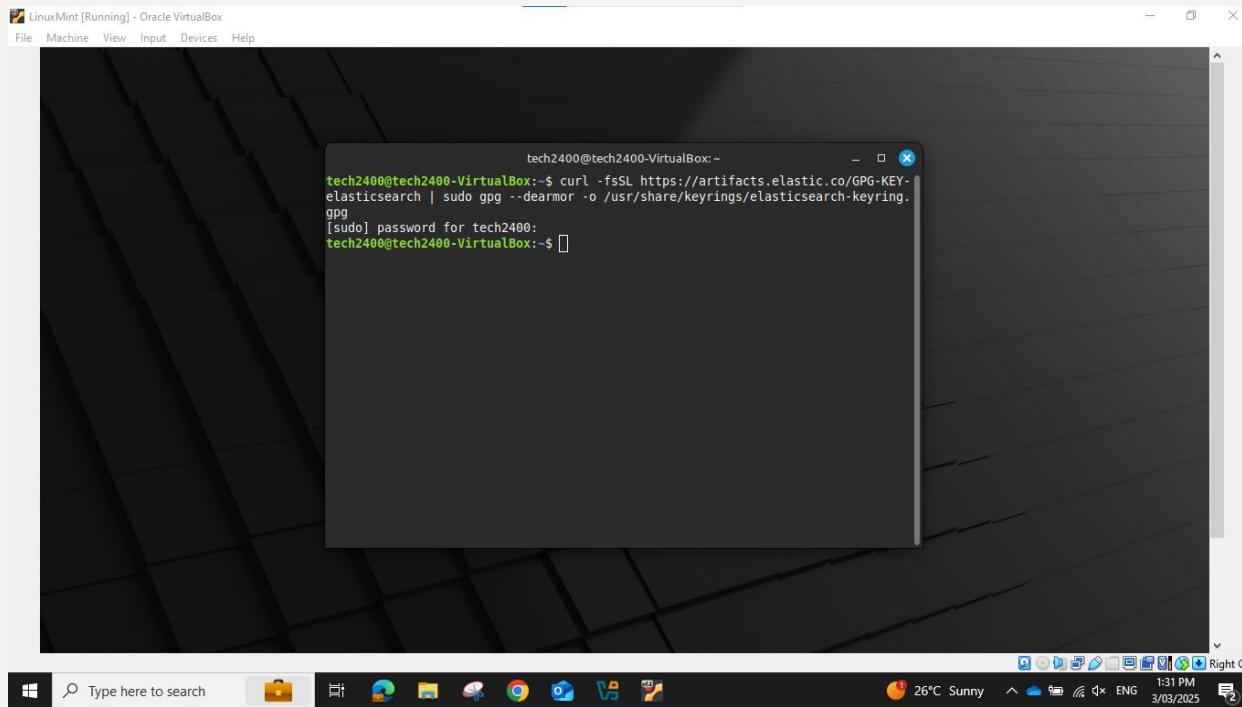
Indicates successful installation →

```
tech2400@tech2400-VirtualBox:~$ java -version
openjdk version "11.0.26" 2025-01-21
OpenJDK Runtime Environment (build 11.0.26+4-post-Ubuntu-1ubuntu124.04)
OpenJDK 64-Bit Server VM (build 11.0.26+4-post-Ubuntu-1ubuntu124.04, mixed mode, sharing)
```

Activity: Install Elasticsearch

Step 1: Add Elasticsearch GPG key

- Run `curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg`



A screenshot of a Linux Mint terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window shows a terminal session with the following command being run:

```
tech2400@tech2400-VirtualBox:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for tech2400:
tech2400@tech2400-VirtualBox:~$
```

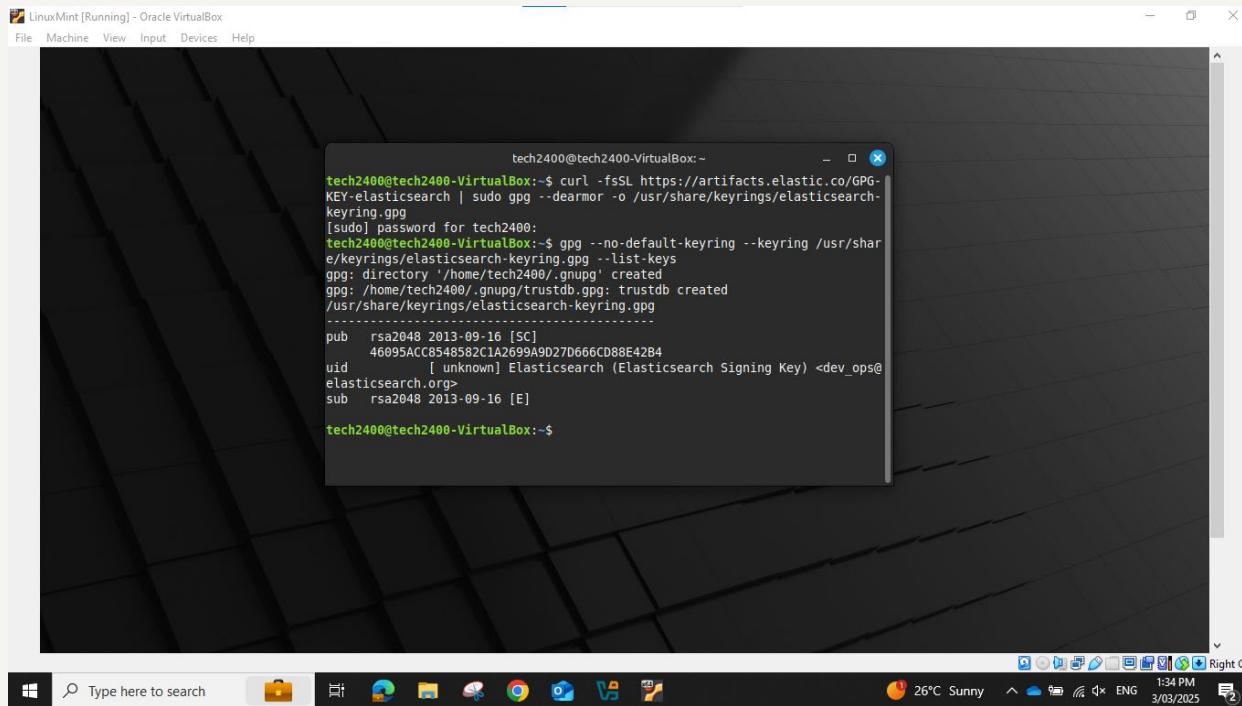
The terminal window is centered on a desktop background with a dark, geometric pattern. The desktop taskbar at the bottom shows various application icons, including a search bar, file explorer, and browser.

KAPLAN

Activity: Install Elasticsearch

Step 2: Verify that key was added successfully

- Run `gpg --no-default-keyring --keyring /usr/share/keyrings/elasticsearch-keyring.gpg --list-keys`



```
tech2400@tech2400-VirtualBox:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for tech2400:
tech2400@tech2400-VirtualBox:~$ gpg --no-default-keyring --keyring /usr/share/keyrings/elasticsearch-keyring.gpg --list-keys
gpg: directory '/home/tech2400/.gnupg' created
gpg: /home/tech2400/.gnupg/trustdb.gpg: trustdb created
/usr/share/keyrings/elasticsearch-keyring.gpg
-----
pub    rsa2048 2013-09-16 [SC]
      46095AC8548582CA2699A9027D666CD88E42B4
uid            [ unknown] Elasticsearch (Elasticsearch Signing Key) <dev_ops@elasticsearch.org>
sub    rsa2048 2013-09-16 [E]

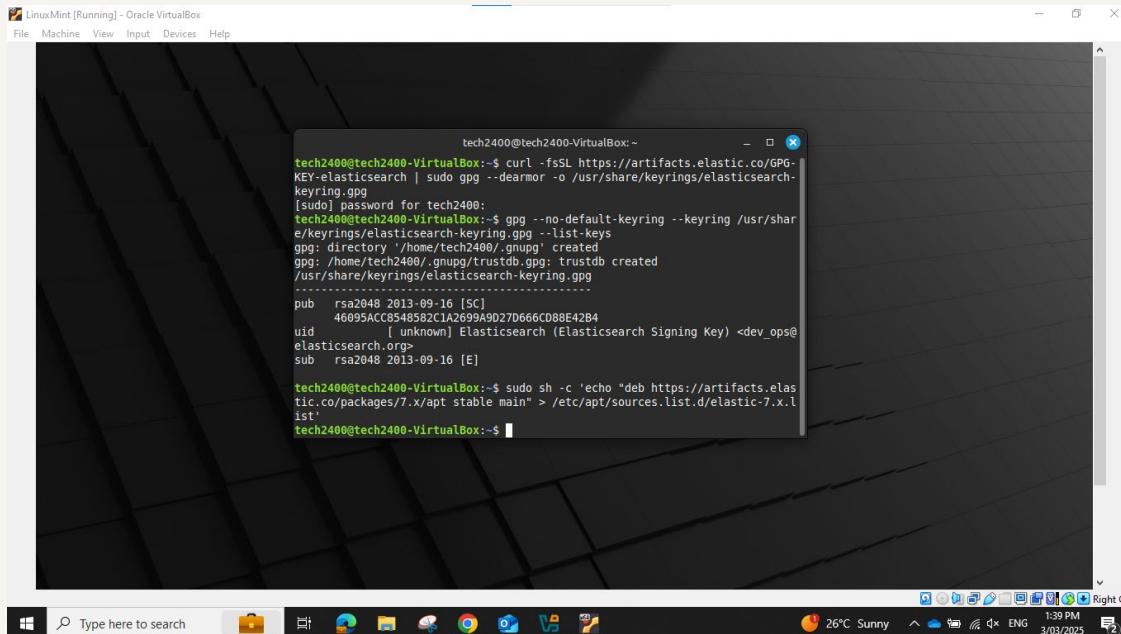
tech2400@tech2400-VirtualBox:~$
```

KAPLAN BUSINESS SCHOOL AUSTRALIA

Activity: Install Elasticsearch

Step 3: Add Elasticsearch APT repository to your system

- Run `echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list`



```
tech2400@tech2400-VirtualBox:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --armor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for tech2400:
tech2400@tech2400-VirtualBox:~$ gpg --no-default-keyring --keyring /usr/share/keyrings/elasticsearch-keyring.gpg --list-keys
gpg: directory '/home/tech2400/.gnupg' created
gpg: /home/tech2400/.gnupg/trustdb.gpg: trustdb created
/usr/share/keyrings/elasticsearch-keyring.gpg
-----
pub    rsa2048 2013-09-16 [SC]
        46095ACC8548582C1A2699A9D027D666CD88E42B4
uid            [ unknown] Elasticsearch (Elasticsearch Signing Key) <dev_ops@elasticsearch.org>
sub    rsa2048 2013-09-16 [E]

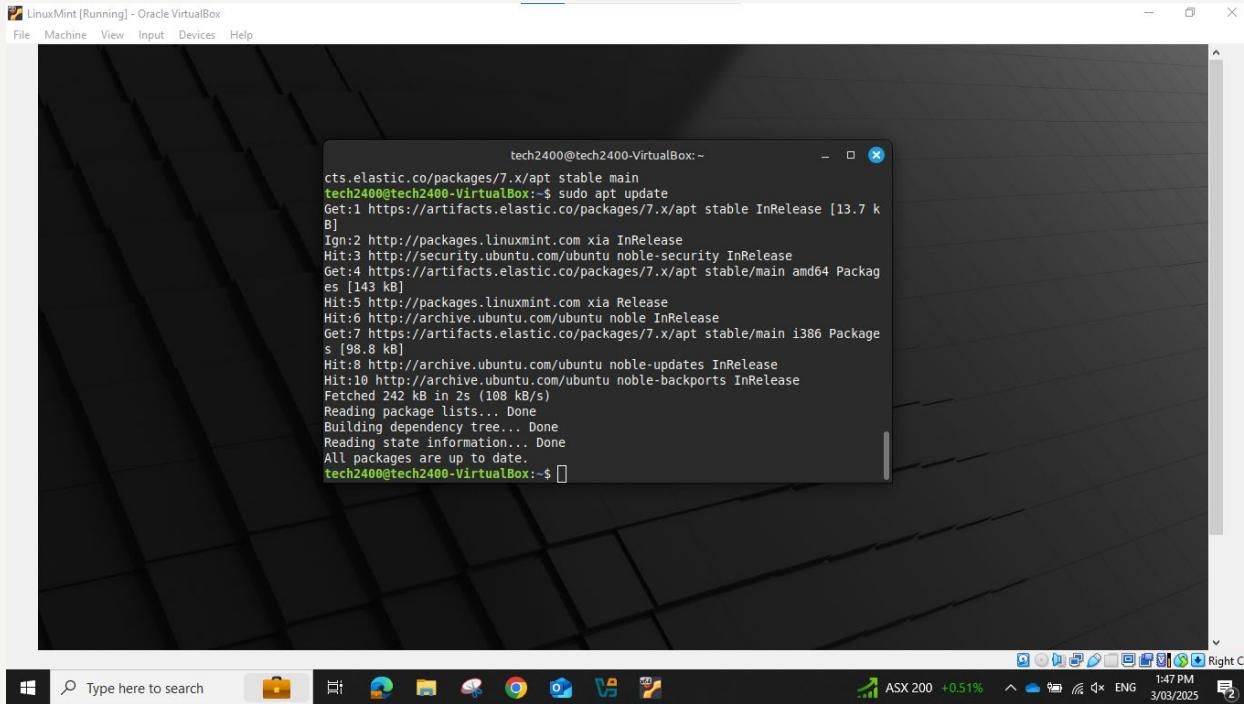
tech2400@tech2400-VirtualBox:~$ sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'
tech2400@tech2400-VirtualBox:~$
```

KAPLAN

Activity: Install Elasticsearch

Step 4: Update the APT package index

- Run `sudo apt update`



A screenshot of a Linux Mint desktop environment within Oracle VirtualBox. The desktop has a dark theme with a grid pattern. A terminal window is open in the center, showing the command `sudo apt update` being run and its output. The output shows various package sources being checked and updated.

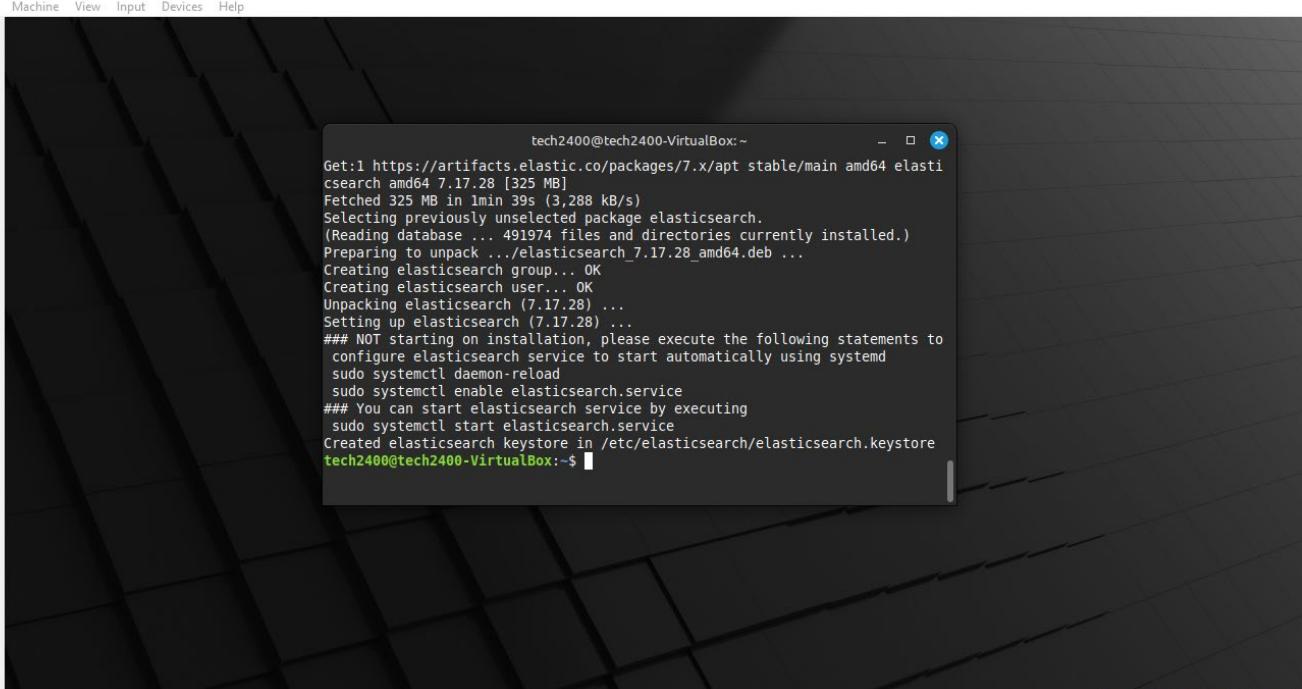
```
tech2400@tech2400-VirtualBox:~$ sudo apt update
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Ign:2 http://packages.linuxmint.com xia InRelease
Hit:3 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [143 kB]
Hit:5 http://packages.linuxmint.com xia Release
Hit:6 http://archive.ubuntu.com/ubuntu noble InRelease
Get:7 https://artifacts.elastic.co/packages/7.x/apt stable/main i386 Packages [98.8 kB]
Hit:8 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:10 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 242 kB in 2s (108 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
tech2400@tech2400-VirtualBox:~$
```

KAPLAN

Activity: Install Elasticsearch

Step 5: Install Elasticsearch

- Run `sudo apt install elasticsearch -y`



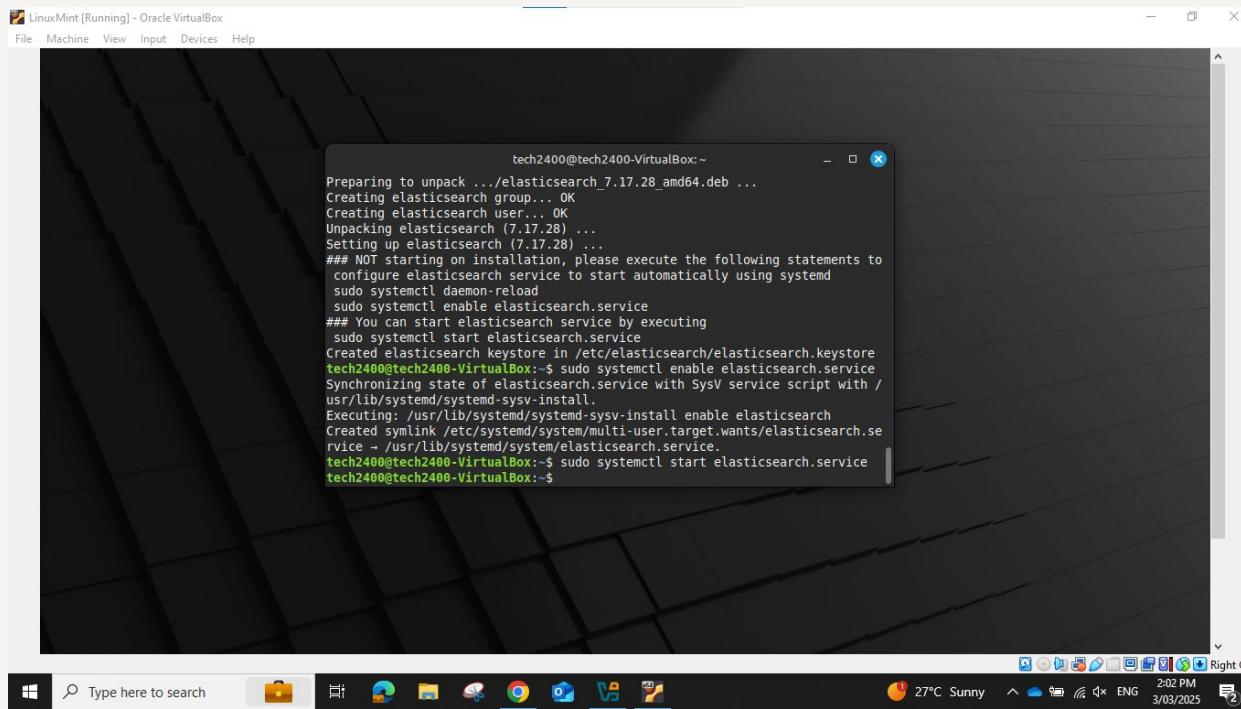
```
tech2400@tech2400-VirtualBox:~ Get:1 https://artifacts.elastic.co/packages/7.x/apt/stable/main amd64 elasti
csearch amd64 7.17.28 [325 MB]
Fetched 325 MB in 1min 39s (3,288 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 491974 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.28_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.28) ...
Setting up elasticsearch (7.17.28) ...
### NOT starting on installation, please execute the following statements to
configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
tech2400@tech2400-VirtualBox:~$
```

The screenshot shows a Linux Mint desktop environment with a terminal window open. The terminal window title is "LinuxMint [Running] - Oracle VirtualBox". The window contains the command-line output of running "sudo apt install elasticsearch -y". The output shows the download of the package, its extraction, and the creation of the elasticsearch user and group. It also provides instructions for configuring the service to start automatically using systemd. The desktop taskbar at the bottom includes icons for file explorer, browser, and other system tools, along with system status indicators like battery level and network.

Activity: Install Elasticsearch

Step 6: Enable and start Elasticsearch

- Run `sudo systemctl enable elasticsearch.service`
- Run `sudo systemctl start elasticsearch.service`



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VM VirtualBox". The terminal output is as follows:

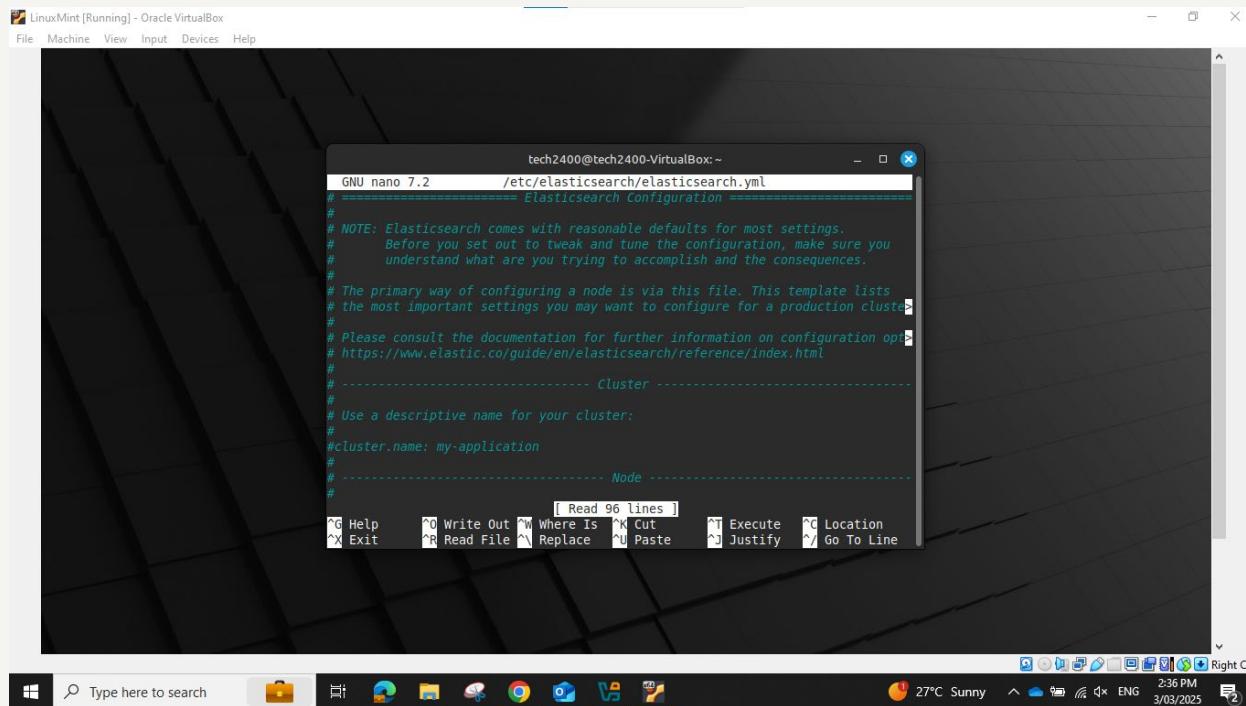
```
tech2400@tech2400-VirtualBox:~$ Preparing to unpack .../elasticsearch_7.17.28_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.28) ...
Setting up elasticsearch (7.17.28) ...
### NOT starting on installation, please execute the following statements to
configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
tech2400@tech2400-VirtualBox:~$ sudo systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
tech2400@tech2400-VirtualBox:~$ sudo systemctl start elasticsearch.service
tech2400@tech2400-VirtualBox:~$
```

The desktop environment includes a taskbar with icons for File Explorer, Task View, Start, and various application icons. The system tray shows the date (3/03/2025), time (2:02 PM), battery level (2%), and network status.

Activity: Configure Elasticsearch

Step 1: Open the Elasticsearch configuration file

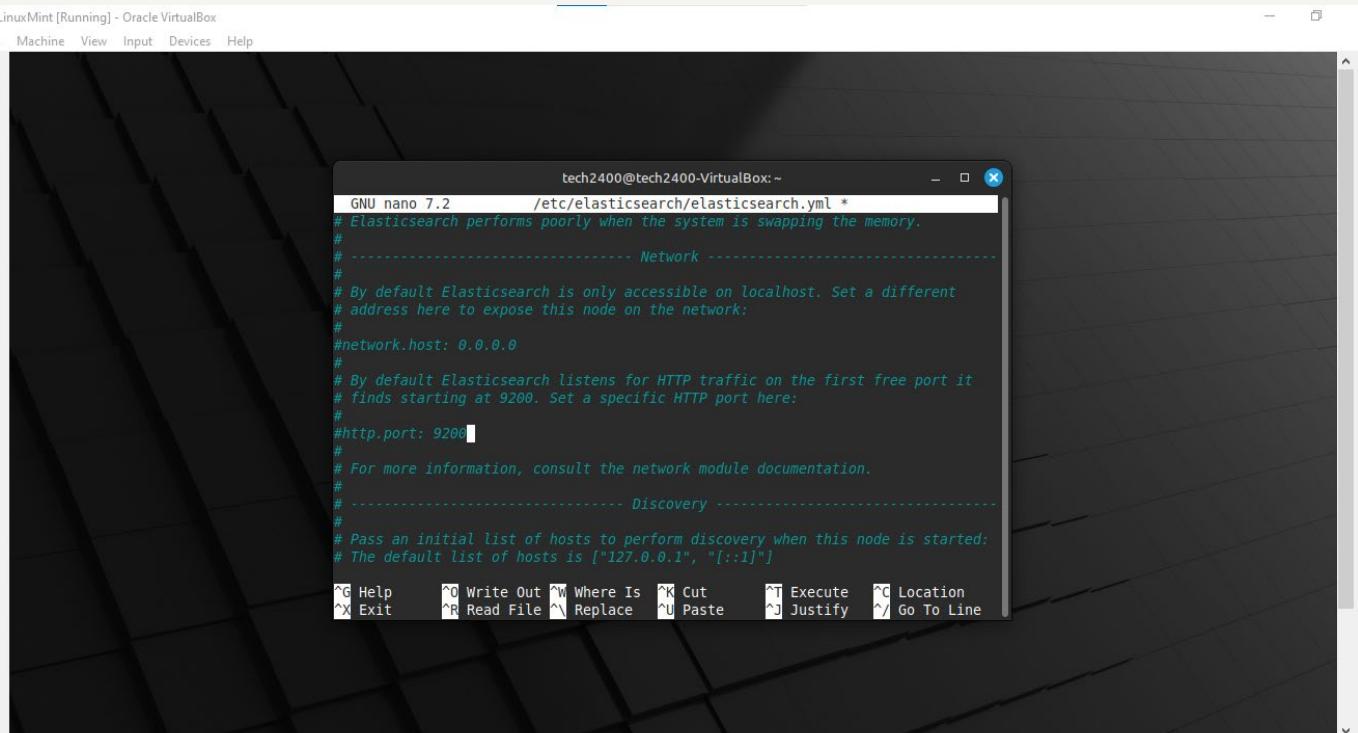
- Run `sudo nano /etc/elasticsearch/elasticsearch.yml`



Activity: Configure Elasticsearch

Step 2: Modify the configuration file

- Set the network.host line to 0.0.0.0 and http.port to 9200



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window title bar includes "File", "Machine", "View", "Input", "Devices", and "Help". The terminal window itself has a dark background and contains the following text:

```
tech2400@tech2400-VirtualBox:~$ nano /etc/elasticsearch/elasticsearch.yml
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
```

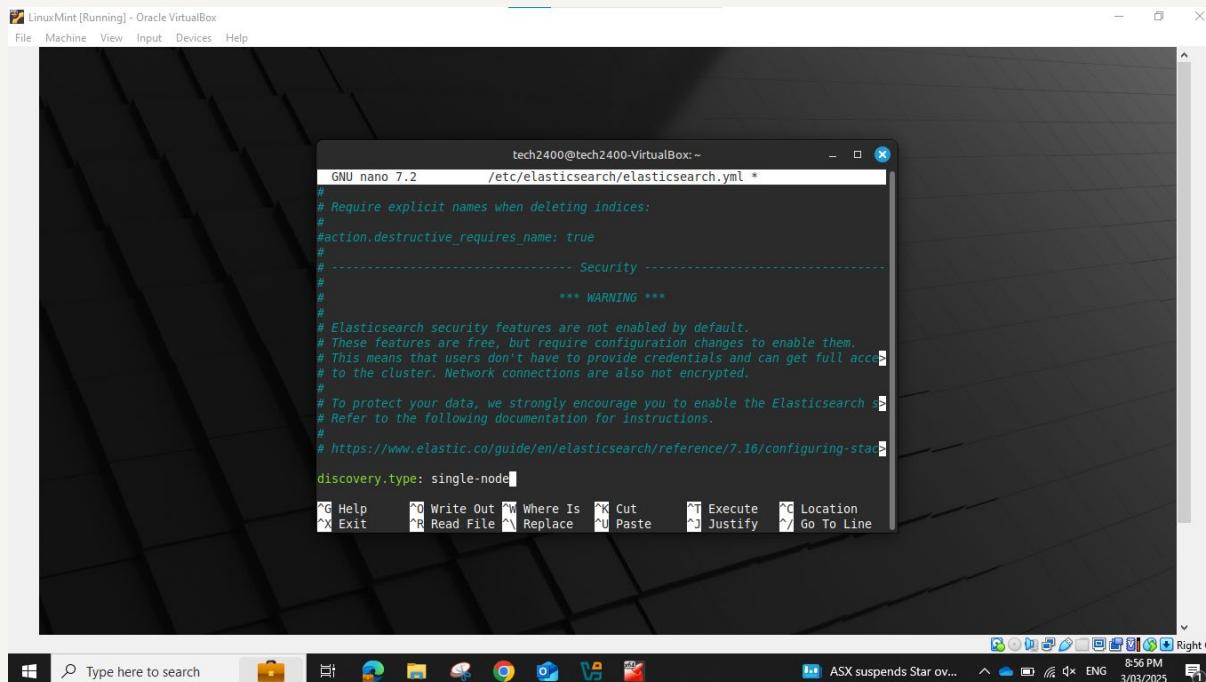
At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts for file operations like Help, Write Out, Cut, Paste, and Exit.

The desktop taskbar at the bottom of the screen includes icons for File Explorer, Task View, Control Panel, File History, Task Scheduler, Task Manager, and Mail. The system tray shows the date and time as 3/03/2025, 8:50 PM, and the weather as 19°C Partly cloudy. It also displays battery status, signal strength, and language settings.

Activity: Configure Elasticsearch

Step 2: Modify the configuration file

- Add an additional line under Discovery towards the bottom of the file: **discovery.type: single-node**
- Save (Ctrl+O), Enter to accept file name, and Close (Ctrl+X)



```
tech2400@tech2400-VirtualBox: ~
GNU nano 7.2          /etc/elasticsearch/elasticsearch.yml *
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
# ----- Security -----
#
# *** WARNING ***
#
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch security features.
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack.html
discovery.type: single-node

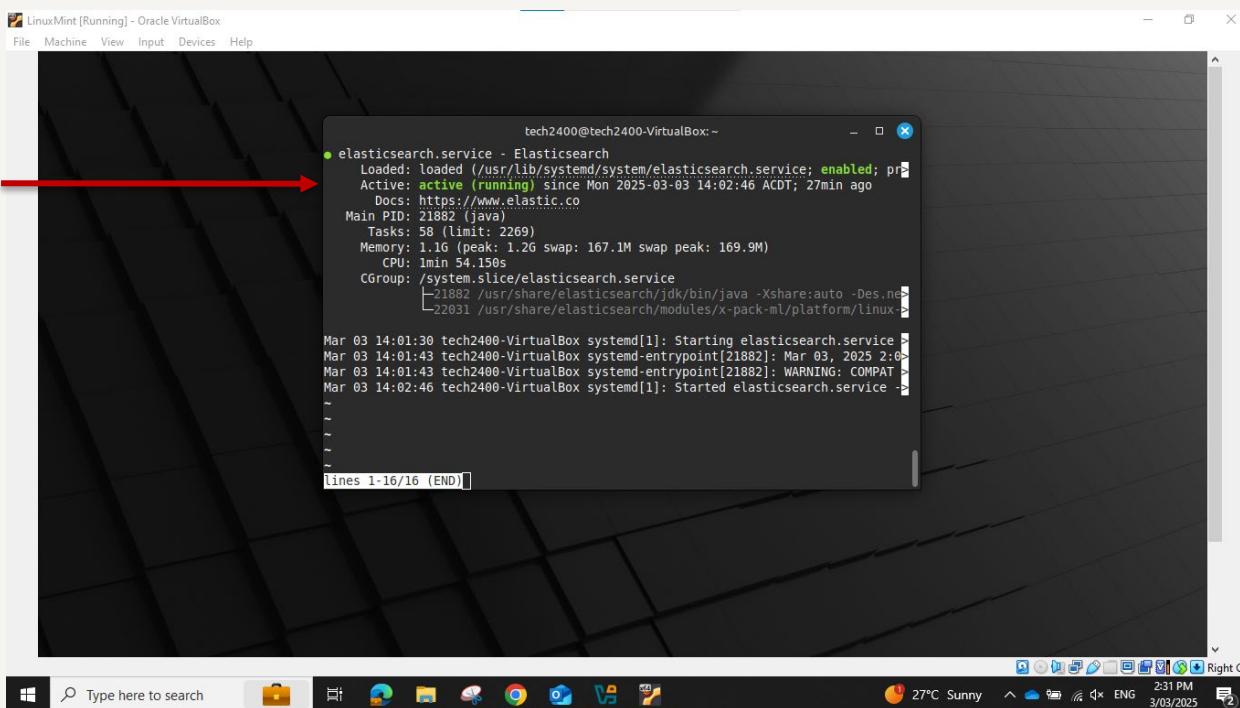
^G Help   ^O Write Out  ^W Where Is  ^X Cut      ^T Execute  ^C Location
^X Exit   ^R Read File  ^U Replace  ^P Paste     ^J Justify  ^L Go To Line
```

Activity: Configure Elasticsearch

Step 3: Verify that Elasticsearch is running

- Run `sudo systemctl status elasticsearch`
- The command should return a response saying it has been active (running) since [date and time]

Indicates
Elasticsearch
is running



```
tech2400@tech2400-VirtualBox:~
```

```
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pre
   Active: active (running) since Mon 2025-03-03 14:02:46 ACDT; 27min ago
     Docs: https://www.elastic.co
 Main PID: 21882 (java)
    Tasks: 58 (limit: 2269)
   Memory: 1.1G (peak: 1.2G)
      CPU: 1min 54.150s
     CGroup: /system.slice/elasticsearch.service
             ├─21882 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.n
             └─22031 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux

Mar 03 14:01:30 tech2400-VirtualBox systemd[1]: Starting elasticsearch.service...
Mar 03 14:01:43 tech2400-VirtualBox systemd-entropy[21882]: Mar 03, 2025 2:0
Mar 03 14:01:43 tech2400-VirtualBox systemd-entropy[21882]: WARNING: COMPAT >
Mar 03 14:02:46 tech2400-VirtualBox systemd[1]: Started elasticsearch.service >
```

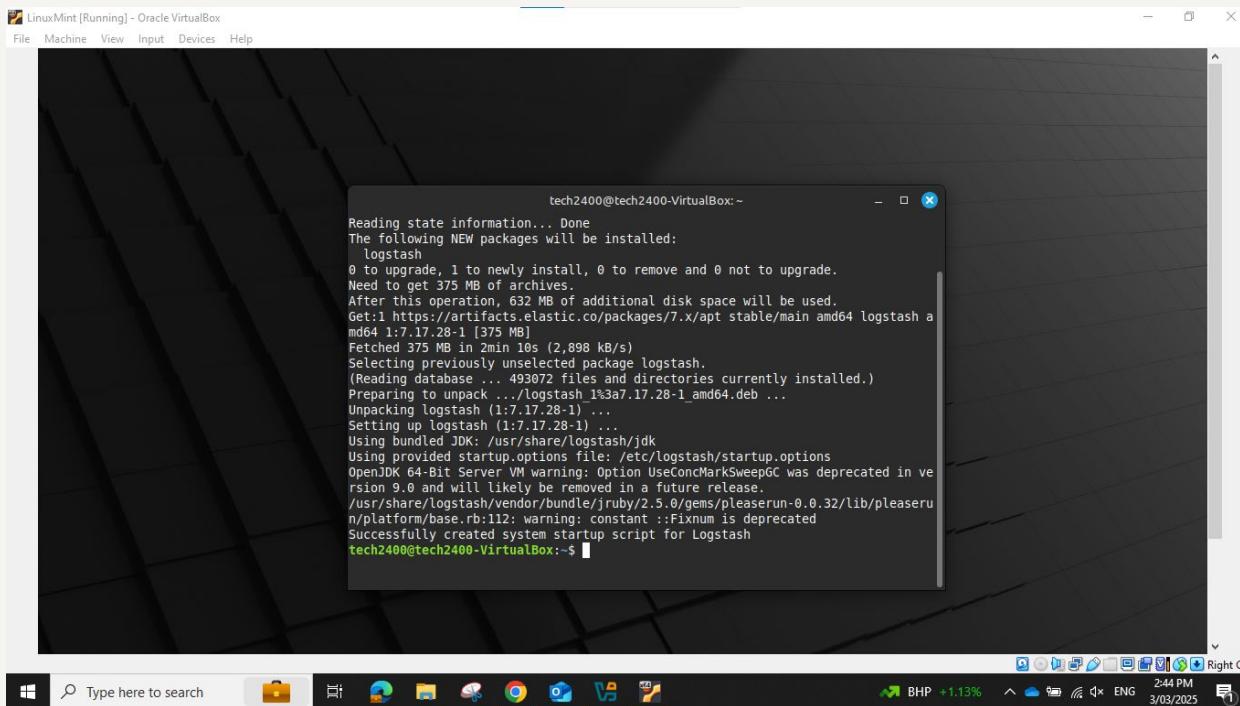
(lines 1-16/16 (END))

KAPLAN

Activity: Install Logstash

Step 1: Install Logstash

- Run `sudo apt install logstash -y`



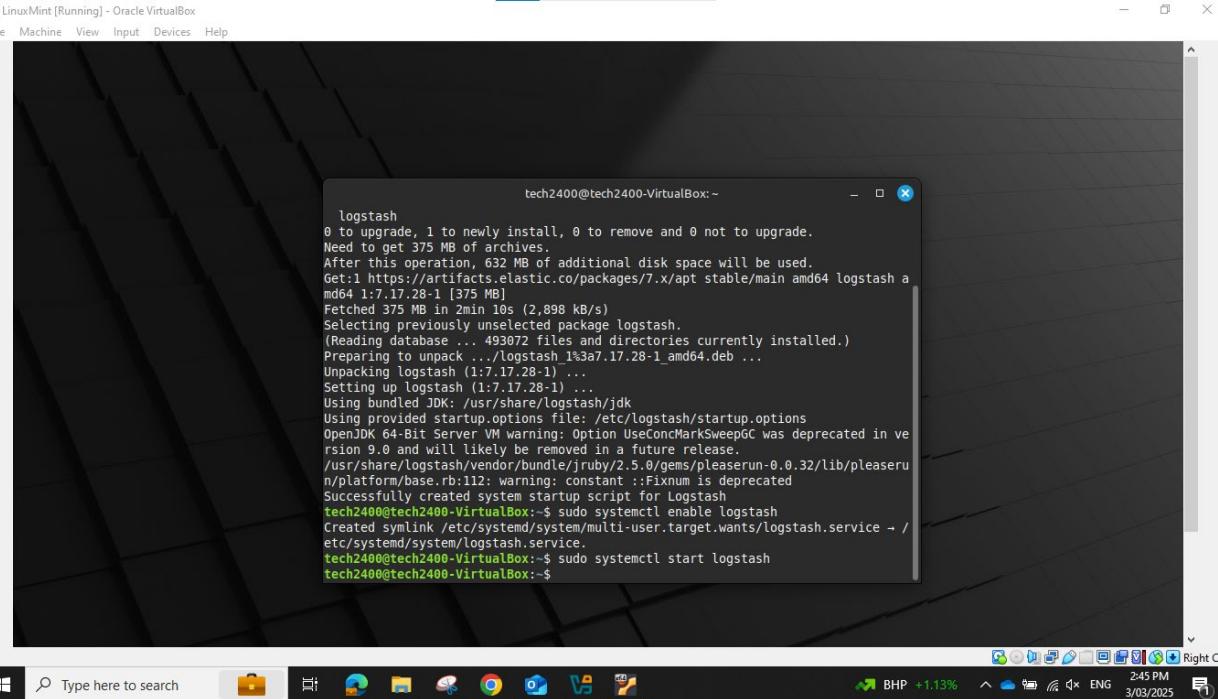
```
tech2400@tech2400-VirtualBox:~$ sudo apt install logstash -y
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 to upgrade, 1 to newly install, 0 to remove and 0 not to upgrade.
Need to get 375 MB of additional disk space will be used.
After this operation, 632 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash a
md64 1:7.17.28-1 [375 MB]
Fetched 375 MB in 2min 10s (2,898 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 493072 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.28-1_amd64.deb ...
Unpacking logstash (1:7.17.28-1) ...
Setting up logstash (1:7.17.28-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in ve
rsion 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaseru
n/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
tech2400@tech2400-VirtualBox:~$
```

KAPLAN

Activity: Install Logstash

Step 2: Enable and start Logstash

- Run `sudo systemctl enable logstash`
- Run `sudo systemctl start logstash`



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The terminal output is as follows:

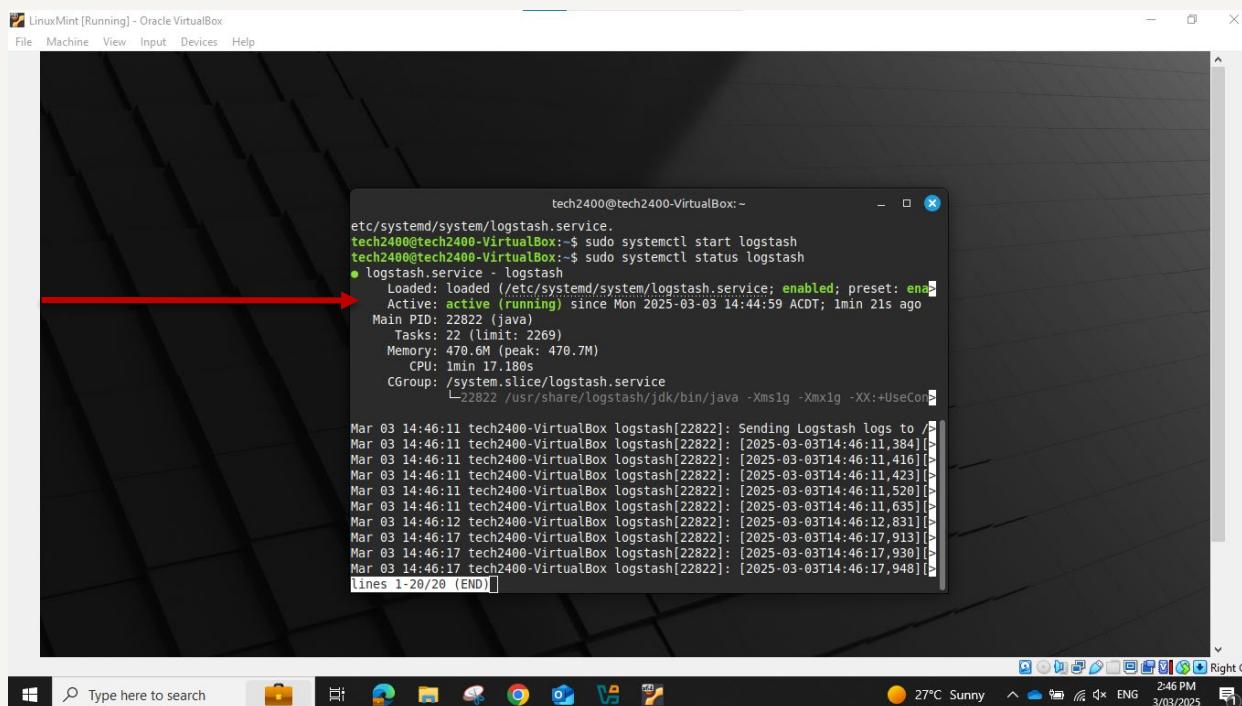
```
tech2400@tech2400-VirtualBox:~$ logstash
0 to upgrade, 1 to newly install, 0 to remove and 0 not to upgrade.
Need to get 375 MB of archives.
After this operation, 632 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash a
md64 1:7.17.28-1 [375 MB]
Fetched 375 MB in 2min 10s (2,898 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 493072 files and directories currently installed.)
Preparing to unpack .../logstash_1:347.17.28-1_amd64.deb ...
Unpacking logstash (1:7.17.28-1) ...
Setting up logstash (1:7.17.28-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in ve
rsion 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaseru
n/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
tech2400@tech2400-VirtualBox:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /
etc/systemd/system/logstash.service.
tech2400@tech2400-VirtualBox:~$ sudo systemctl start logstash
tech2400@tech2400-VirtualBox:~$
```

Activity: Install Logstash

Step 3: Verify that Logstash is running

- Run `sudo systemctl status logstash`
 - If Logstash is running, the command will return a response saying it has been active (running) since [date and time]

Indicates Logstash is running

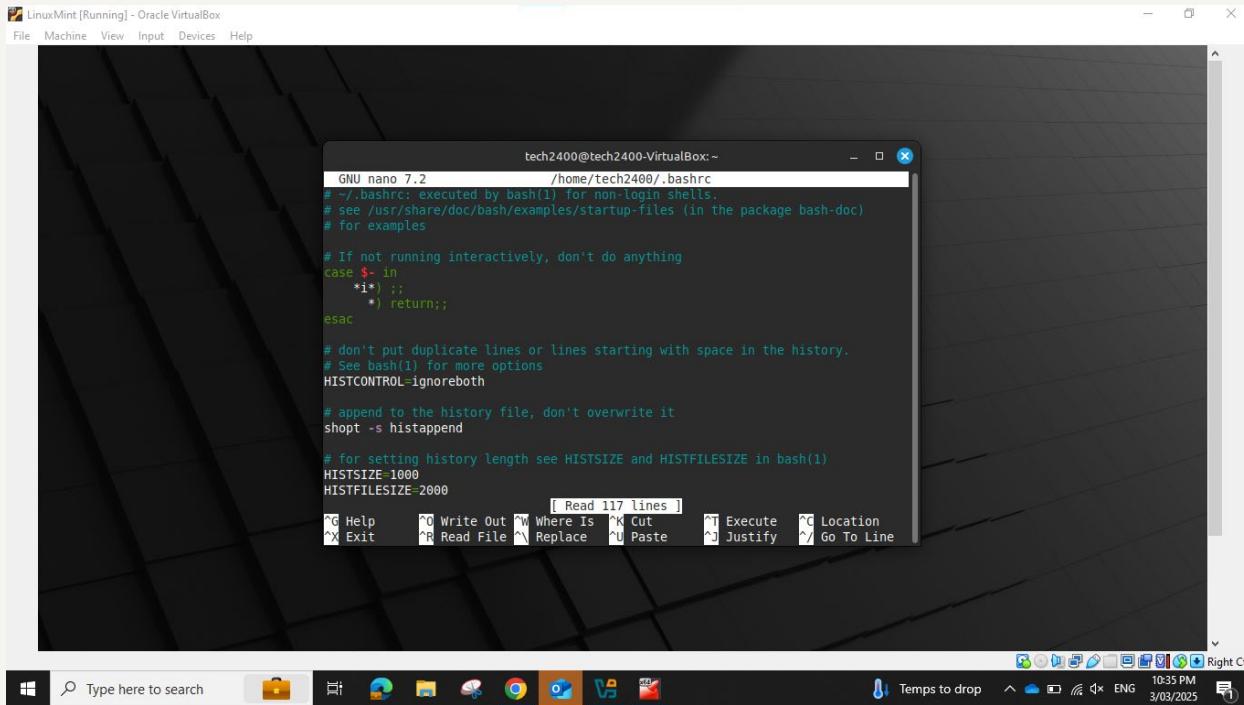


KAPLAN

Activity: Install Logstash

Step 4: Add Logstash to your \$PATH

- Run `nano ~/.bashrc` to open your shell configuration file

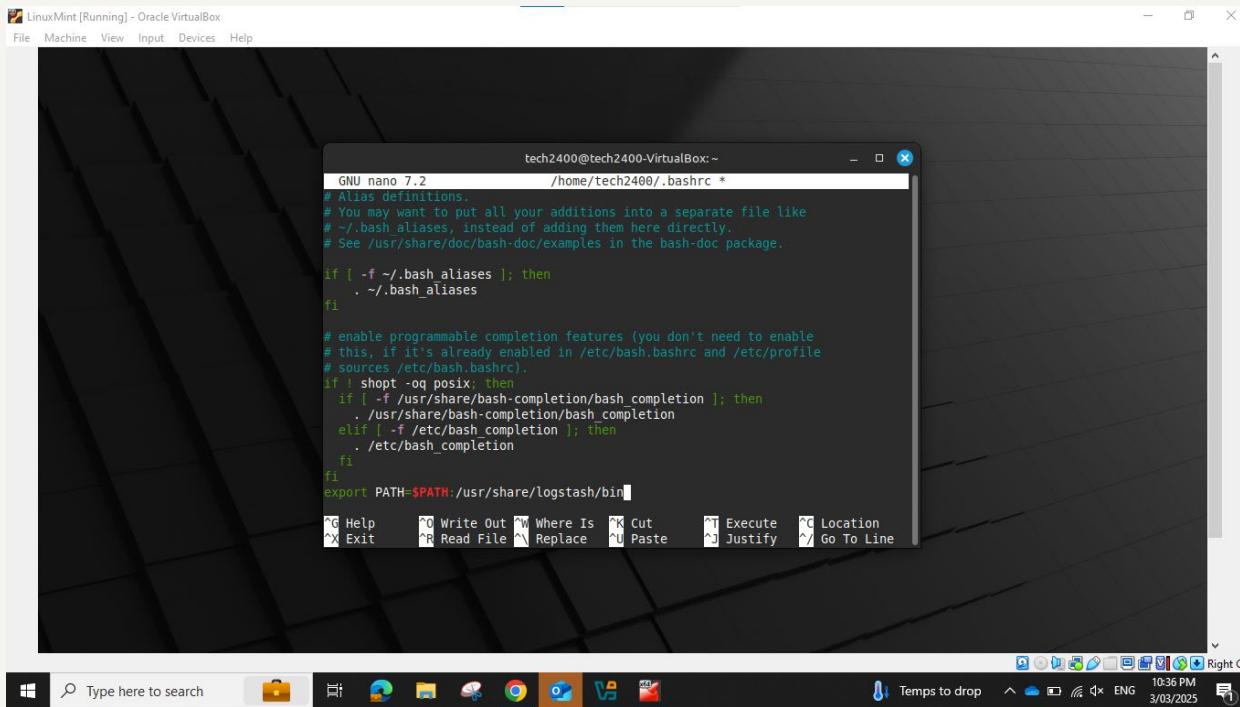


KAPLAN

Activity: Install Logstash

Step 4: Add Logstash to your \$PATH

- Navigate to the end of the file and add the following line:
export PATH=\$PATH:/usr/share/logstash/bin
- Save (Ctrl+O) > Enter > Close (Ctrl+X)



```
tech2400@tech2400-VirtualBox:~$ nano .bashrc
GNU nano 7.2          /home/tech2400/.bashrc *
# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
. ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
if [ -f /usr/share/bash-completion/bash_completion ]; then
. /usr/share/bash-completion/bash_completion
elif [ -f /etc/bash_completion ]; then
. /etc/bash_completion
fi
fi
export PATH=$PATH:/usr/share/logstash/bin
```

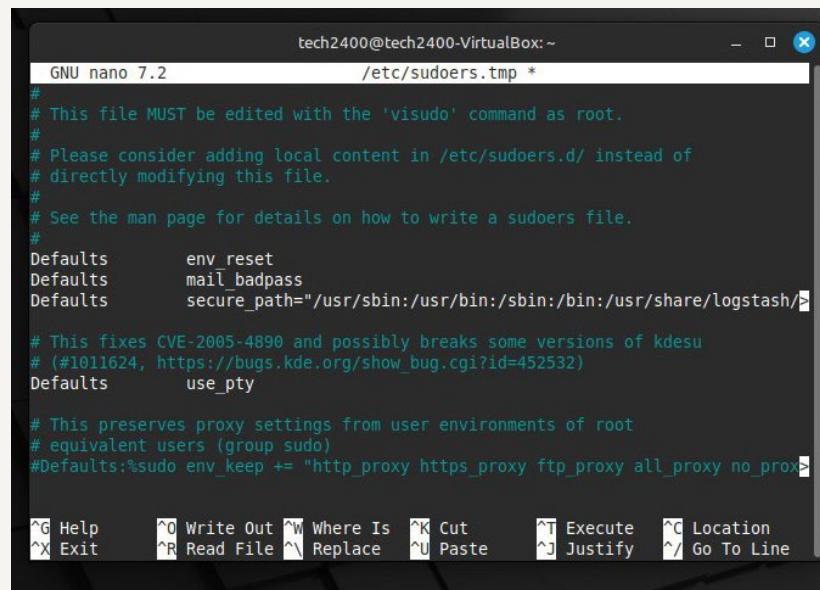
Activity: Install Logstash

Step 4: Add Logstash to your \$PATH

- Open `sudo visudo` to configure sudo to preserve \$PATH
- Navigate to Defaults `secure_path`
- Add the path to Logstash

Defaults

```
secure_path="/usr/sbin:/usr/bin:/sbin:/bin:/usr/share/logstash/
bin"
```



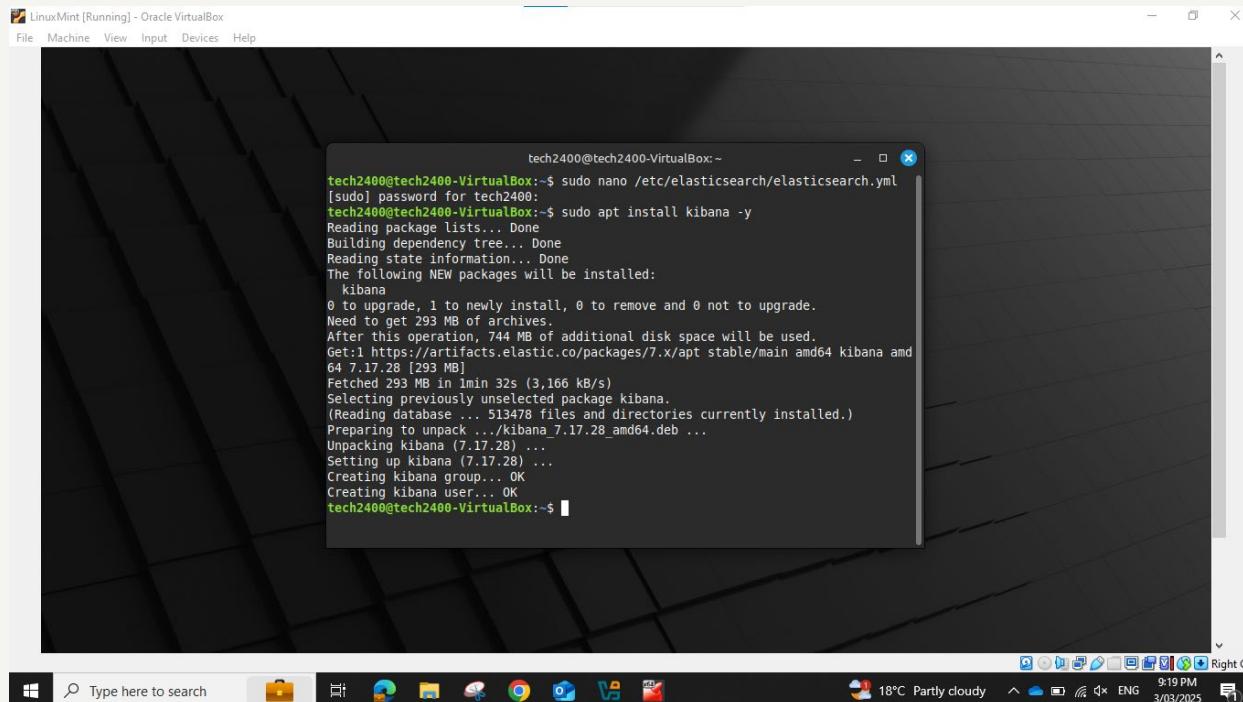
```
tech2400@tech2400-VirtualBox: ~
GNU nano 7.2          /etc/sudoers.tmp *
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/sbin:/usr/bin:/sbin:/bin:/usr/share/logstash/
bin"
#
# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults      use_pty
#
# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"
#
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute   ^C Location
^X Exit     ^R Read File  ^L Replace   ^U Paste    ^J Justify   ^/ Go To Line
```

KAPLAN

Activity: Install Kibana

Step 1: Install Kibana

- Run `sudo apt install kibana -y`



The screenshot shows a Linux Mint desktop environment with a terminal window open. The terminal window title is "LinuxMint [Running] - Oracle VirtualBox". The terminal content shows the command being run:

```
tech2400@tech2400-VirtualBox:~$ sudo apt install kibana -y
[sudo] password for tech2400:
tech2400@tech2400-VirtualBox:~$ Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 to upgrade, 1 to newly install, 0 to remove and 0 not to upgrade.
Need to get 293 MB of archives.
After this operation, 744 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.28 [293 MB]
Fetched 293 MB in 1min 32s (3,166 KB/s)
Selecting previously unselected package kibana.
(Reading database ... 513478 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.28_amd64.deb ...
Unpacking kibana (7.17.28) ...
Setting up kibana (7.17.28) ...
Creating kibana group... OK
Creating kibana user... OK
tech2400@tech2400-VirtualBox:~$
```

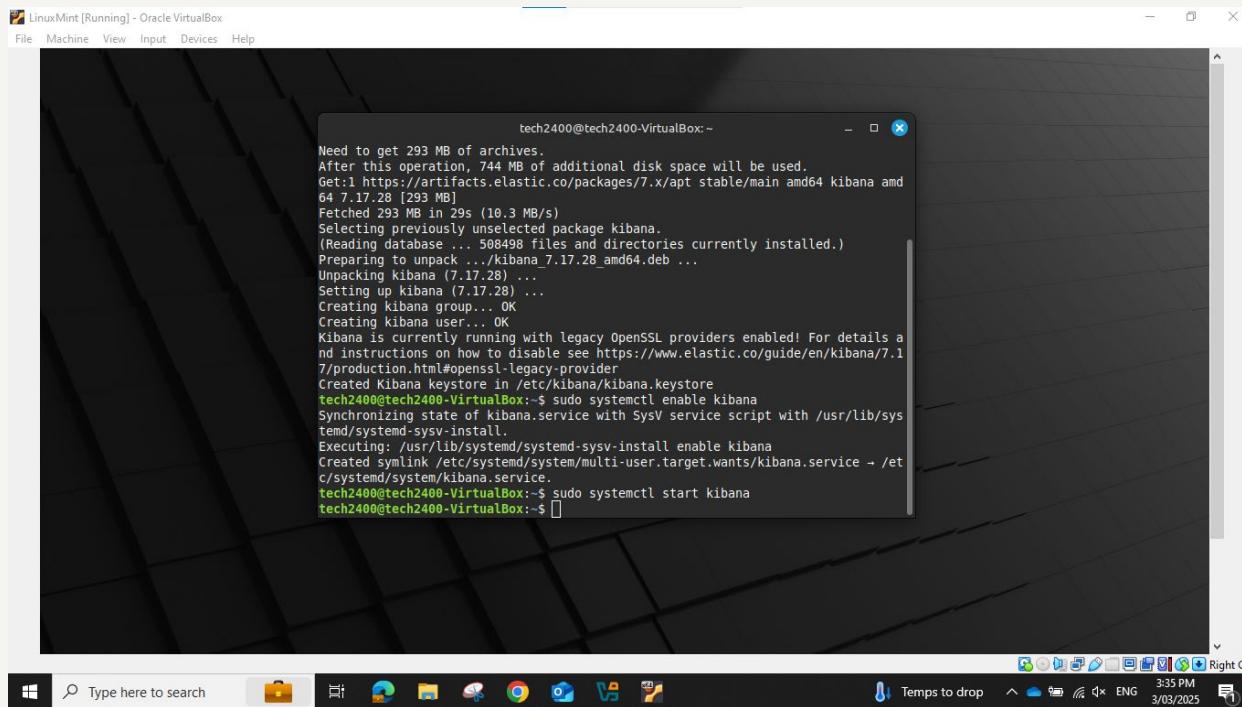
The desktop interface includes a taskbar with icons for various applications like File Explorer, Edge, and Visual Studio Code. The system tray shows the date and time as 3/03/2025, 9:19 PM, with a battery level of 18°C Partly cloudy.

KAPLAN

Activity: Install Kibana

Step 2: Enable and start Kibana

- Run `sudo systemctl enable kibana`
- Run `sudo systemctl start kibana`



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle.VirtualBox". The terminal displays the following command-line session:

```
tech2400@tech2400-VirtualBox:~$ sudo apt update  
Need to get 293 MB of archives.  
After this operation, 744 MB of additional disk space will be used.  
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.28 [293 MB]  
Fetched 293 MB in 29s (10.3 MB/s)  
Selecting previously unselected package kibana.  
(Reading database ... 508498 files and directories currently installed.)  
Preparing to unpack .../kibana_7.17.28_amd64.deb ...  
Unpacking kibana (7.17.28) ...  
Setting up kibana (7.17.28) ...  
Creating Kibana group... OK  
Creating Kibana user... OK  
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/7.1/production.html#openssl-legacy-provider  
Created Kibana keystore in /etc/kibana/kibana.keystore  
tech2400@tech2400-VirtualBox:~$ sudo systemctl enable kibana  
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemctl-sysv-install.  
Executing: /usr/lib/systemd/systemctl-sysv-install enable kibana  
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.  
tech2400@tech2400-VirtualBox:~$ sudo systemctl start kibana  
tech2400@tech2400-VirtualBox:~$
```

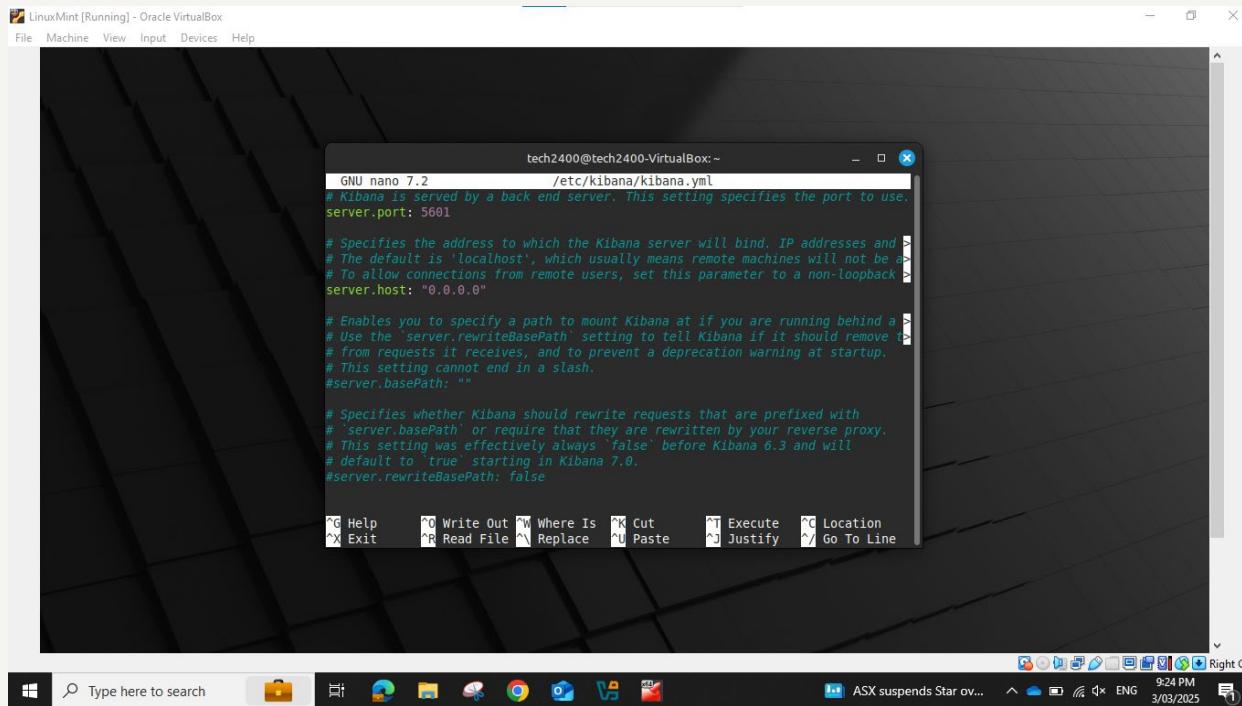
The terminal window is part of a desktop environment with a dark theme. The taskbar at the bottom shows various application icons, and the system tray indicates the date and time as "3/03/2025 3:35 PM".

KAPLAN

Activity: Install Kibana

Step 3: Edit the Kibana configuration file

- Run `sudo nano /etc/kibana/kibana.yml`

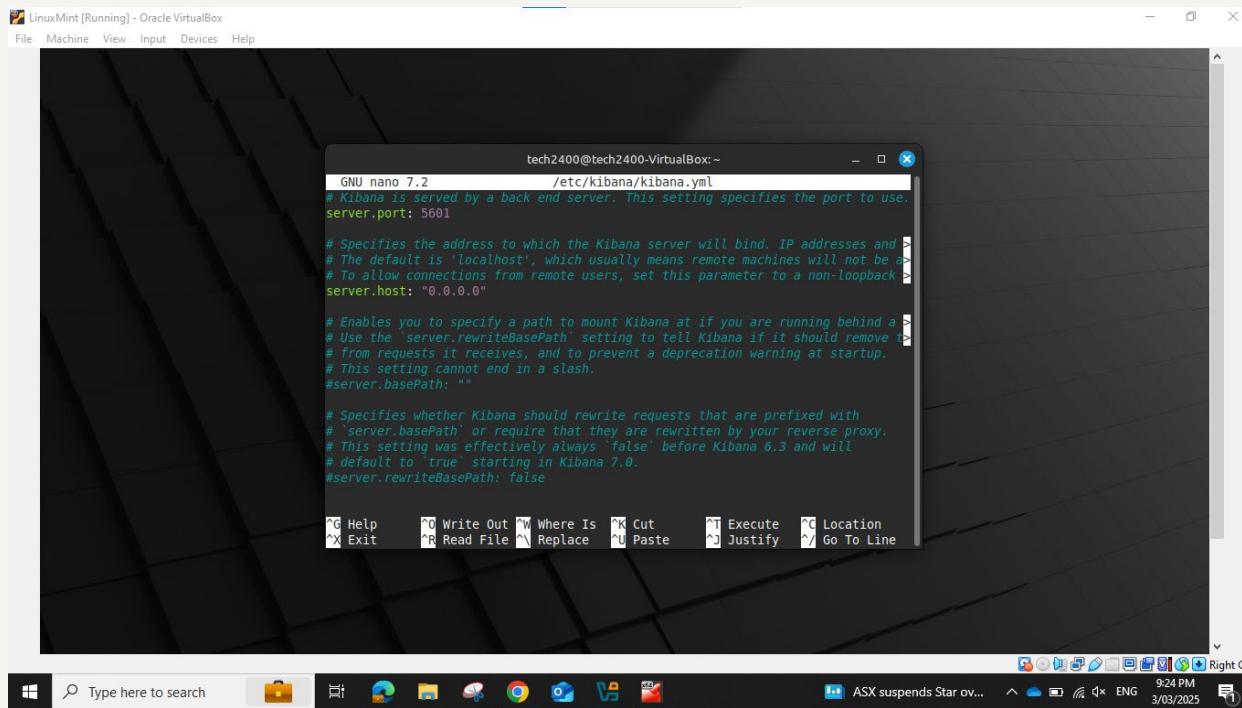


KAPLAN

Activity: Install Kibana

Step 3: Edit the Kibana configuration file

- Uncomment server.host
- Set the IP to 0.0.0.0 to listen on all interfaces
- Uncomment server.port (leave 5601)



The screenshot shows a Linux Mint desktop environment within Oracle VirtualBox. A terminal window titled 'tech2400@tech2400-VirtualBox: ~' displays the contents of the /etc/kibana/kibana.yml file. The file contains configuration settings for Kibana, specifically regarding its port and host. The terminal interface includes a menu bar with File, Machine, View, Input, Devices, Help, and a toolbar with various keyboard shortcuts.

```
tech2400@tech2400-VirtualBox: ~
GNU nano 7.2          /etc/kibana/kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and
# The default is 'localhost', which usually means remote machines will not be able to access it.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a reverse proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the prefix
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#serverbasePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# 'serverbasePath' or require that they are rewritten by your reverse proxy.
# This setting was effectively always 'false' before Kibana 6.3 and will
# default to 'true' starting in Kibana 7.0.
#server.rewritebasePath: false

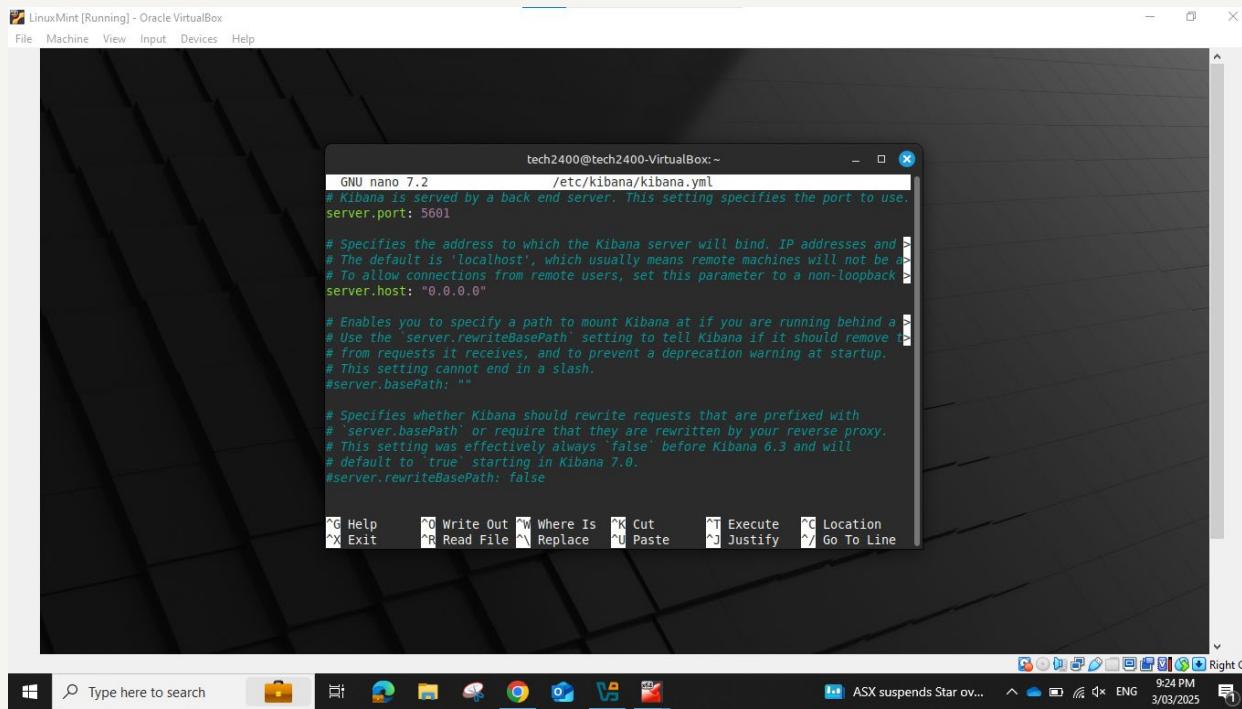
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^L Go To Line
```

KAPLAN

Activity: Install Kibana

Step 3: Edit the Kibana configuration file

- Save (Ctrl+O)
- Press Enter key to accept file name
- Close (Ctrl+X)



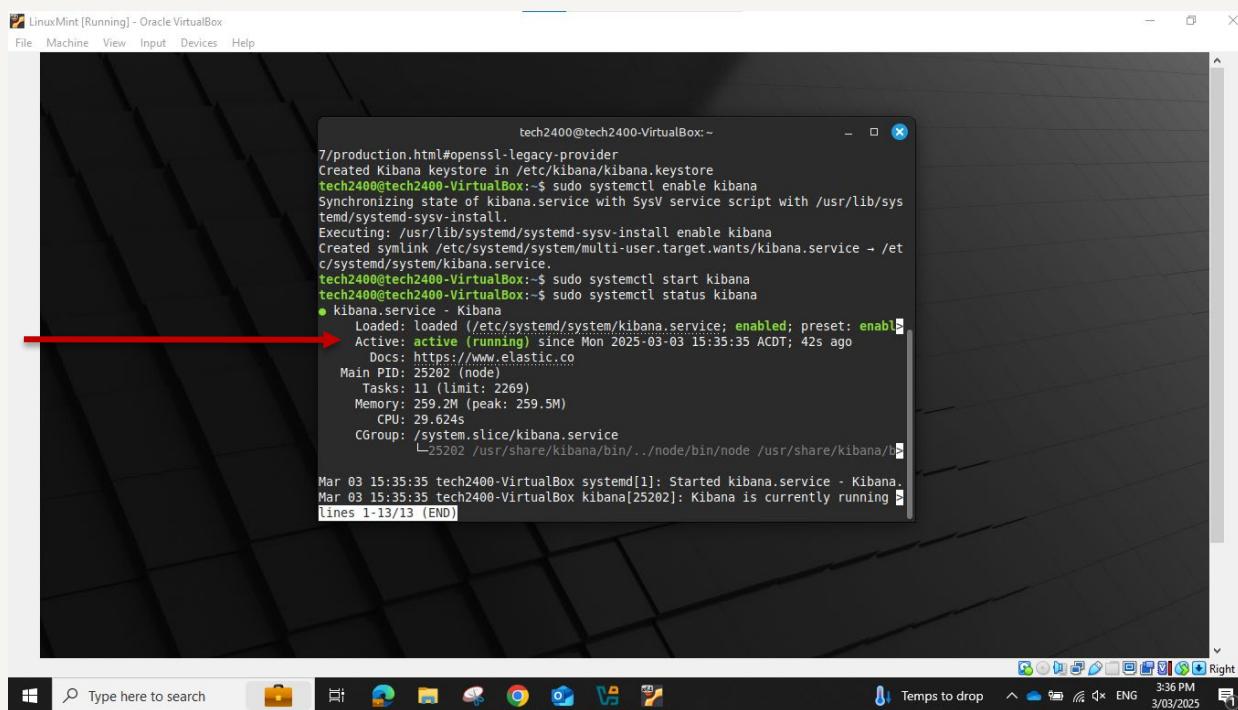
KAPLAN

Activity: Install Kibana

Step 4: Verify that Kibana is running

- Run `sudo systemctl status kibana`
- If Kibana is running, the command will return a response saying it has been active (running) since [date and time]

Indicates
Kibana is
running



```
7/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
tech2400@tech2400-VirtualBox:~$ sudo systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
tech2400@tech2400-VirtualBox:~$ sudo systemctl start kibana
tech2400@tech2400-VirtualBox:~$ sudo systemctl status kibana
● kibana.service - Kibana
    Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: enabled)
    Active: active (running) since Mon 2025-03-03 15:35:35 ACDT; 42s ago
      Docs: https://www.elastic.co
          Main PID: 25202 (node)
             Tasks: 11 (limit: 2269)
            Memory: 259.2M (peak: 259.5M)
              CPU: 29.624s
            CGroup: /system.slice/kibana.service
                    └─25202 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/b

Mar 03 15:35:35 tech2400-VirtualBox systemd[1]: Started Kibana.service - Kibana.
Mar 03 15:35:35 tech2400-VirtualBox kibana[25202]: Kibana is currently running
[lines 1-13/13 (END)]
```

Activity:

Generate SSH Logs for Analysis

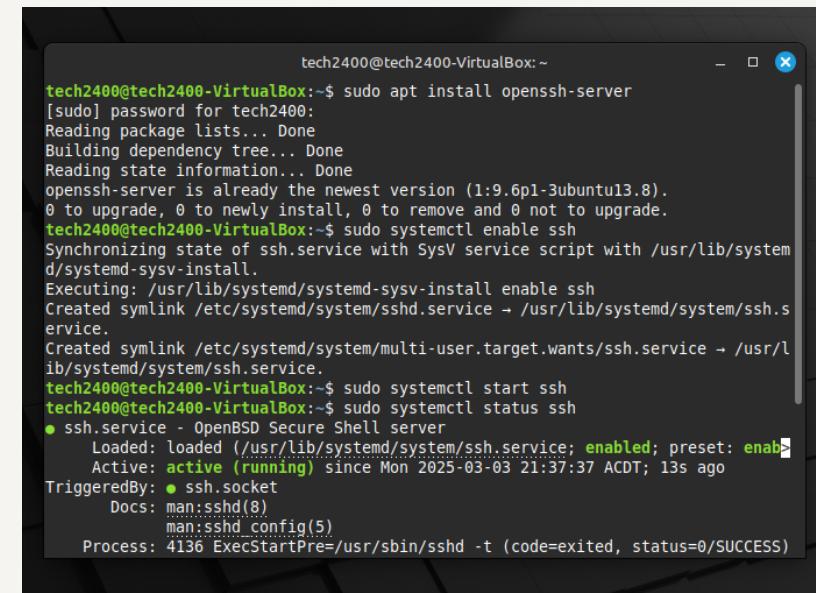
Goal: To simulate a security scenario where unauthorised users attempt to gain access to a system

Step 1: Ensure that SSH is enabled

- 1) Open Terminal on Linux Mint
- 2) Run `sudo systemctl status ssh` to ensure SSH is enabled.

If not:

```
sudo apt install openssh-server  
sudo systemctl start ssh  
sudo systemctl enable ssh
```



A screenshot of a terminal window titled "tech2400@tech2400-VirtualBox:~". The window shows the following command-line session:

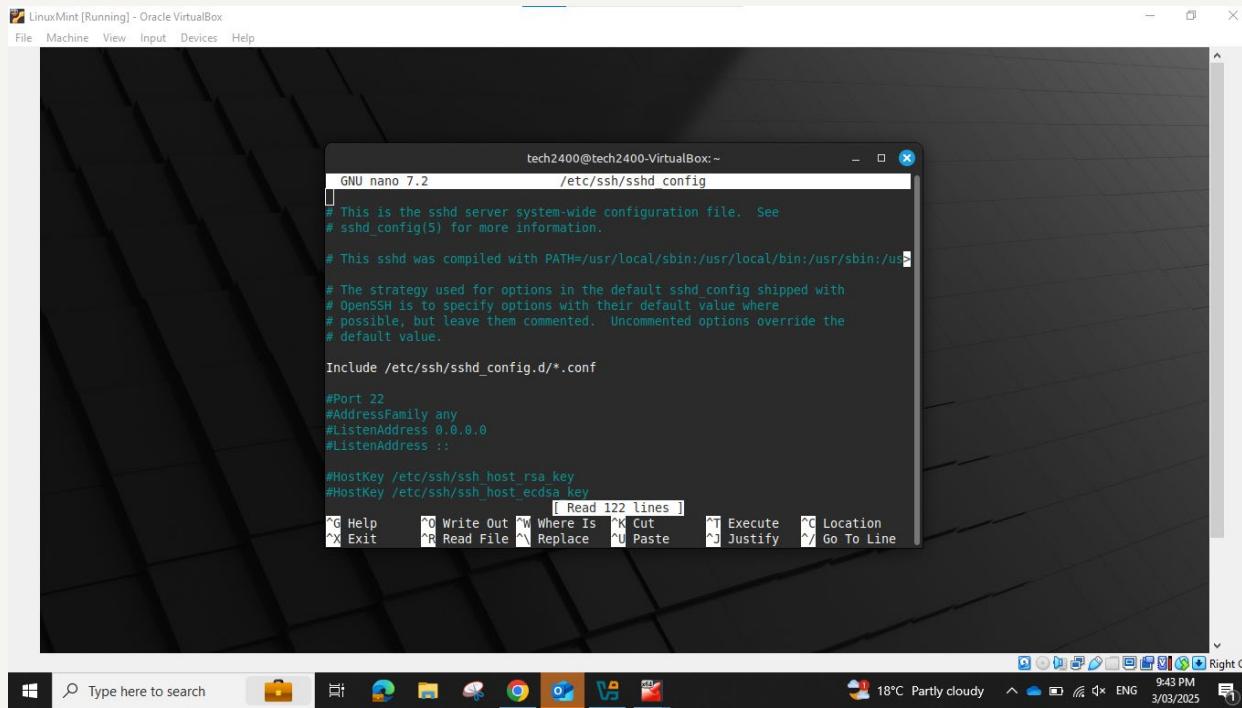
```
tech2400@tech2400-VirtualBox:~$ sudo apt install openssh-server
[sudo] password for tech2400:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:9.6p1-3ubuntu13.8).
0 to upgrade, 0 to newly install, 0 to remove and 0 not to upgrade.
tech2400@tech2400-VirtualBox:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/sshd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.
tech2400@tech2400-VirtualBox:~$ sudo systemctl start ssh
tech2400@tech2400-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
    Active: active (running) since Mon 2025-03-03 21:37:37 ACDT; 13s ago
      TriggeredBy: ● ssh.socket
        Docs: man:sshd(8)
               man:sshd_config(5)
    Process: 4136 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
```

Activity: Generate SSH Logs for Analysis

Step 2: Configure SSH to log unsuccessful login attempts

- Edit the SSH configuration file

```
sudo nano /etc/ssh/sshd_config
```



Activity:

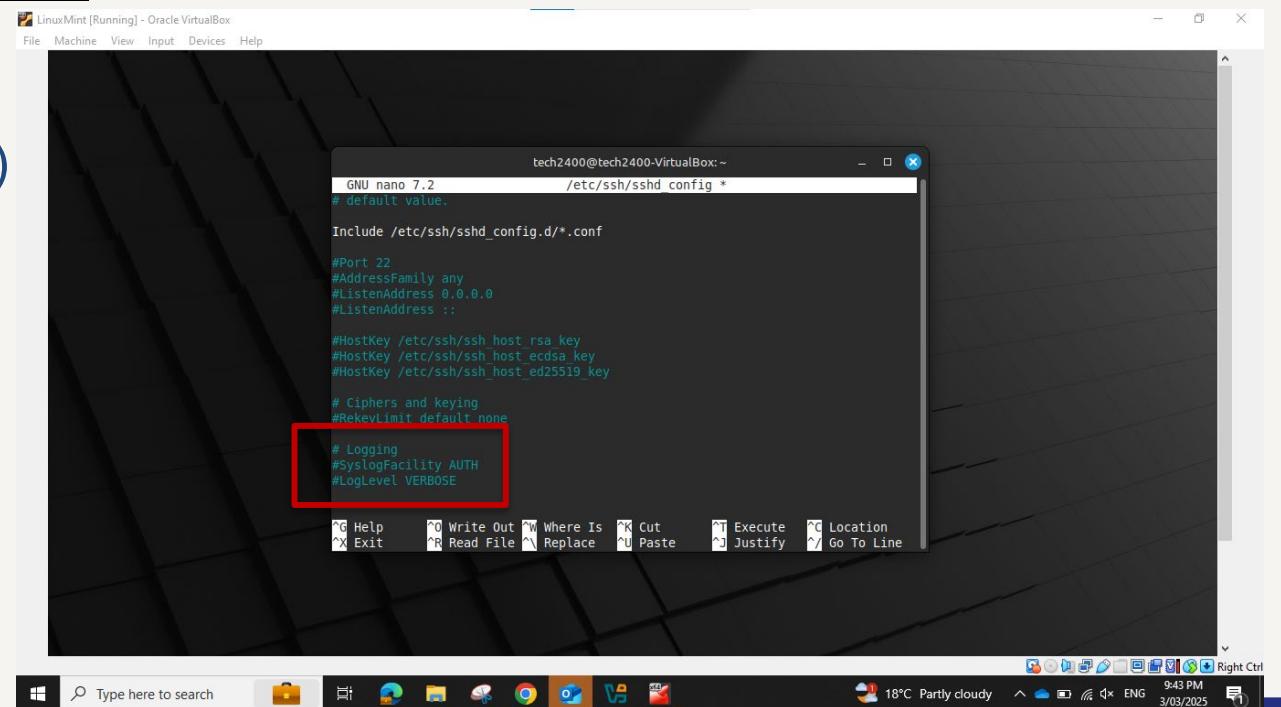
Generate SSH Logs for Analysis

Step 2: Configure SSH to log unsuccessful login attempts

- Ensure the following logging parameters are set to ensure detailed logging of SSH activity, including failed login attempts

LogLevel VERBOSE

- Save (Ctrl+O)
- Enter
- Close (Ctrl+X)



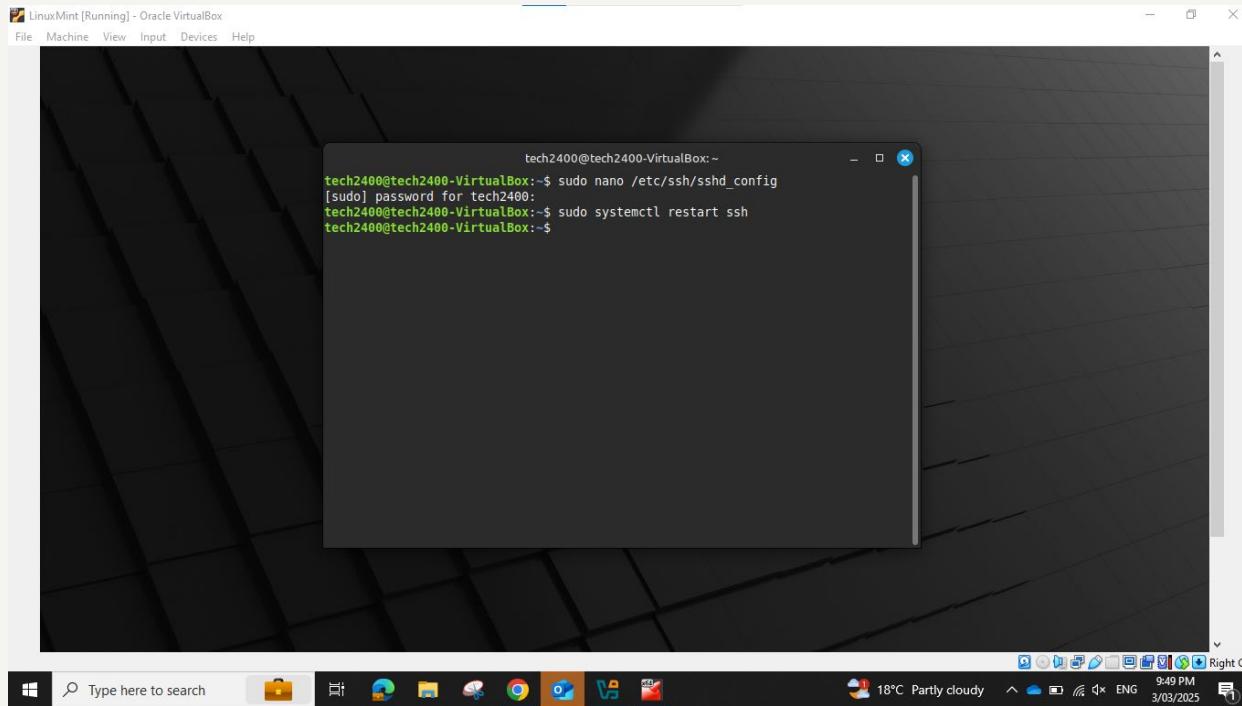
```
tech2400@tech2400-VirtualBox: ~ /etc/ssh/sshd config *  
# default value.  
  
Include /etc/ssh/sshd_config.d/*.conf  
  
#Port 22  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#syslogFacility AUTH  
#LogLevel VERBOSE
```

Activity:

Generate SSH Logs for Analysis

Step 2: Configure SSH to log unsuccessful login attempts

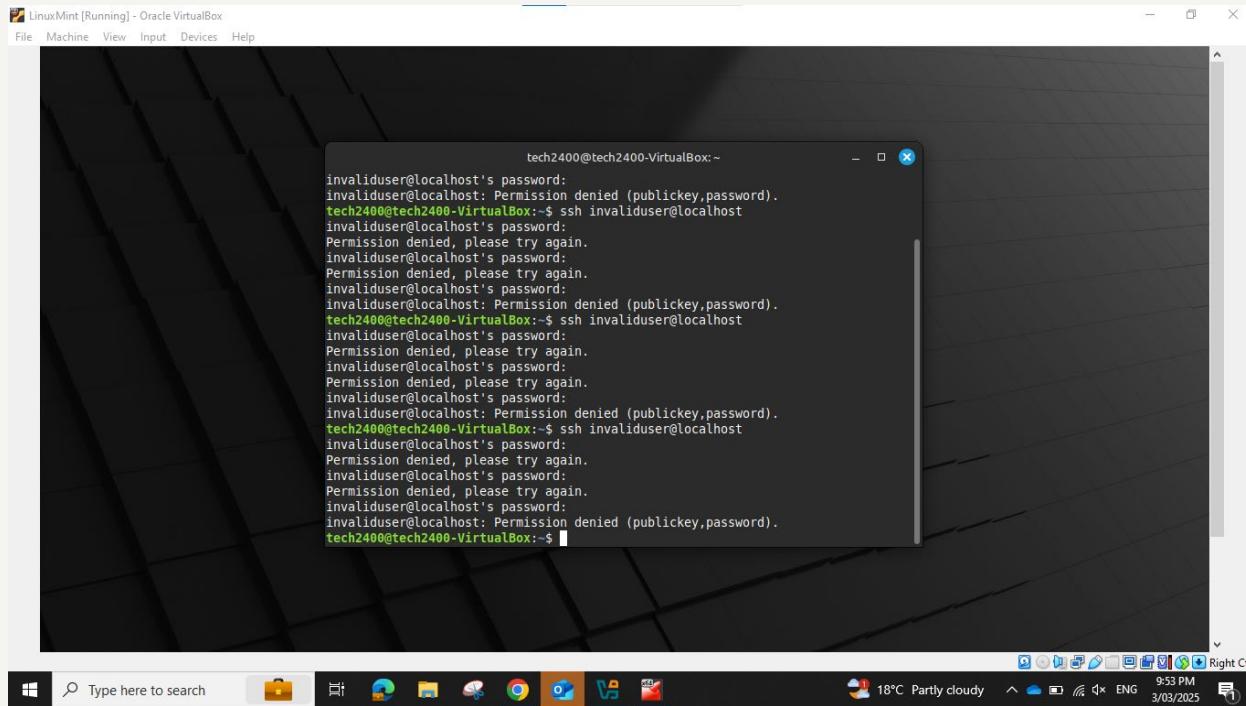
- Restart SSH for the changes to take effect
- **sudo systemctl restart ssh**



Activity: Generate SSH Logs for Analysis

Step 3: Simulate unauthorised login attempts

- Use the ssh command with invalid credentials several times
- **ssh invaliduser@localhost**



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window contains a series of failed SSH login attempts from the user "invaliduser" to the host "localhost". The log entries are as follows:

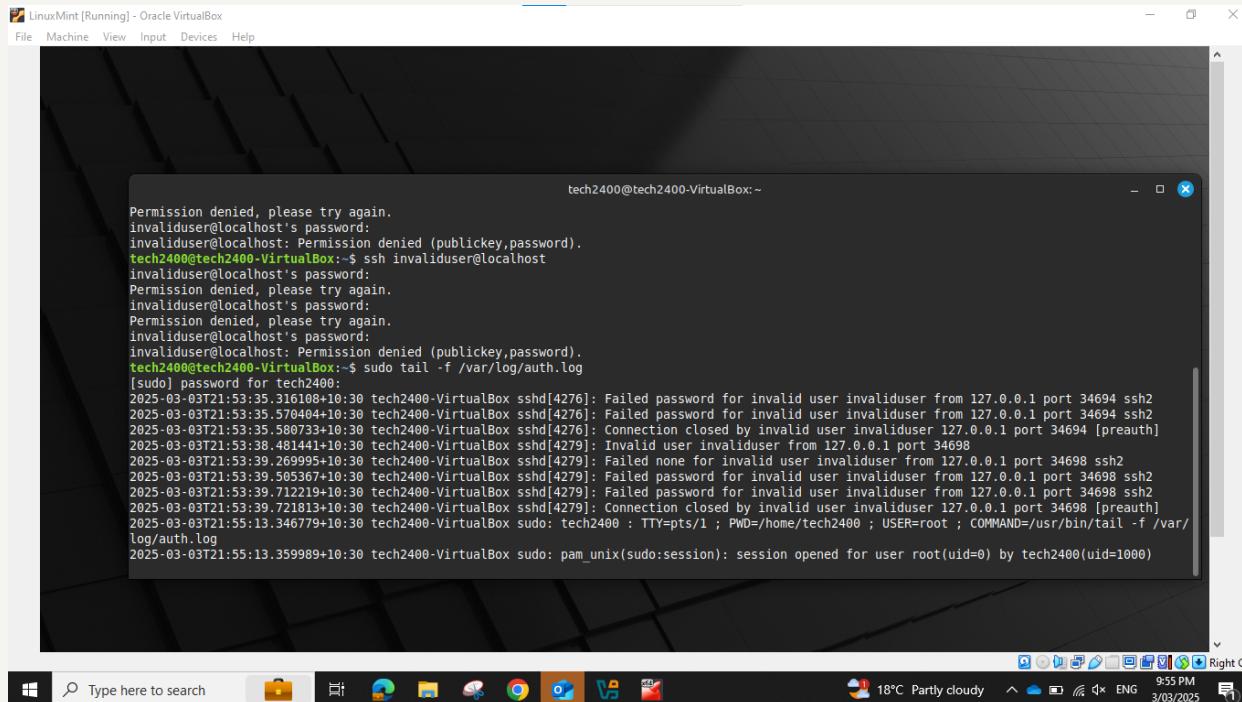
```
tech2400@tech2400-VirtualBox:~$ ssh invaliduser@localhost
invaliduser@localhost's password:
invaliduser@localhost: Permission denied (publickey,password).
tech2400@tech2400-VirtualBox:~$ ssh invaliduser@localhost
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
invaliduser@localhost: Permission denied (publickey,password).
tech2400@tech2400-VirtualBox:~$ ssh invaliduser@localhost
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
invaliduser@localhost: Permission denied (publickey,password).
tech2400@tech2400-VirtualBox:~$ ssh invaliduser@localhost
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
Permission denied, please try again.
invaliduser@localhost's password:
invaliduser@localhost: Permission denied (publickey,password).
tech2400@tech2400-VirtualBox:~$
```

Activity:

Generate SSH Logs for Analysis

Step 3: Simulate unauthorised login attempts

- View the generated logs: `sudo tail -f /var/log/auth.log`



A screenshot of a Windows desktop environment showing a terminal window. The terminal window title is "LinuxMint [Running] - Oracle VirtualBox". The command entered was `sudo tail -f /var/log/auth.log`. The output shows multiple failed login attempts from an invalid user:

```
Permission denied, please try again.  
invaliduser@localhost's password:  
invaliduser@localhost: Permission denied (publickey,password).  
tech2400@tech2400-VirtualBox:~$ ssh invaliduser@localhost  
invaliduser@localhost's password:  
Permission denied, please try again.  
invaliduser@localhost's password:  
Permission denied, please try again.  
invaliduser@localhost's password:  
invaliduser@localhost: Permission denied (publickey,password).  
tech2400@tech2400-VirtualBox:~$ sudo tail -f /var/log/auth.log  
[sudo] password for tech2400:  
2025-03-03T21:53:35.316108+10:30 tech2400-VirtualBox sshd[4276]: Failed password for invalid user invaliduser from 127.0.0.1 port 34694 ssh2  
2025-03-03T21:53:35.570404+10:30 tech2400-VirtualBox sshd[4276]: Failed password for invalid user invaliduser from 127.0.0.1 port 34694 ssh2  
2025-03-03T21:53:35.580733+10:30 tech2400-VirtualBox sshd[4276]: Connection closed by invalid user invaliduser 127.0.0.1 port 34694 [preauth]  
2025-03-03T21:53:38.481441+10:30 tech2400-VirtualBox sshd[4279]: Invalid user invaliduser from 127.0.0.1 port 34698  
2025-03-03T21:53:39.269995+10:30 tech2400-VirtualBox sshd[4279]: Failed none for invalid user invaliduser from 127.0.0.1 port 34698 ssh2  
2025-03-03T21:53:39.505367+10:30 tech2400-VirtualBox sshd[4279]: Failed password for invalid user invaliduser from 127.0.0.1 port 34698 ssh2  
2025-03-03T21:53:39.712219+10:30 tech2400-VirtualBox sshd[4279]: Failed password for invalid user invaliduser from 127.0.0.1 port 34698 ssh2  
2025-03-03T21:53:39.721813+10:30 tech2400-VirtualBox sshd[4279]: Connection closed by invalid user invaliduser 127.0.0.1 port 34698 [preauth]  
2025-03-03T21:55:13.346779+10:30 tech2400-VirtualBox sudo: tech2400 : TTY=pts/1 ; PWD=/home/tech2400 ; USER=root ; COMMAND=/usr/bin/tail -f /var/  
log/auth.log  
2025-03-03T21:55:13.359989+10:30 tech2400-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by tech2400(uid=1000)
```

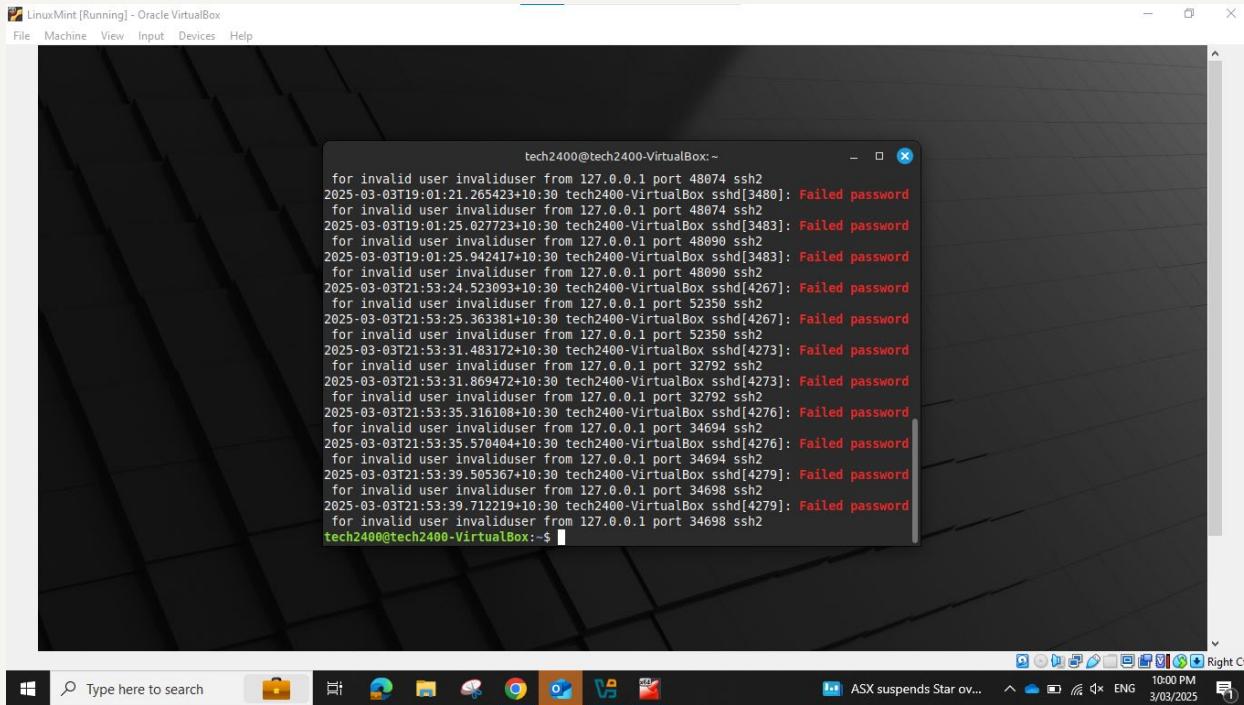
The taskbar at the bottom of the screen shows various icons for applications like File Explorer, Edge, and FileZilla. The system tray indicates the date as 3/03/2025, the time as 9:55 PM, the temperature as 18°C, and the weather as Partly cloudy.

Activity:

Generate SSH Logs for Analysis

Step 3: Simulate unauthorised login attempts

- Search logs for failed login attempts



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window displays a series of failed SSH login attempts from an invalid user "invaliduser" to port 48074. The log entries are as follows:

```
tech2400@tech2400-VirtualBox:~  
for invalid user invaliduser from 127.0.0.1 port 48074 ssh2  
2025-03-03T19:01:21.265423+10:30 tech2400-VirtualBox sshd[3480]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 48074 ssh2  
2025-03-03T19:01:25.027723+10:30 tech2400-VirtualBox sshd[3483]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 48090 ssh2  
2025-03-03T19:01:25.942417+10:30 tech2400-VirtualBox sshd[3483]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 48090 ssh2  
2025-03-03T21:53:24.523093+10:30 tech2400-VirtualBox sshd[4267]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 52350 ssh2  
2025-03-03T21:53:25.363381+10:30 tech2400-VirtualBox sshd[4267]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 52350 ssh2  
2025-03-03T21:53:31.483172+10:30 tech2400-VirtualBox sshd[4273]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 32792 ssh2  
2025-03-03T21:53:31.869472+10:30 tech2400-VirtualBox sshd[4273]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 32792 ssh2  
2025-03-03T21:53:35.316108+10:30 tech2400-VirtualBox sshd[4276]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 34694 ssh2  
2025-03-03T21:53:35.570404+10:30 tech2400-VirtualBox sshd[4276]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 34694 ssh2  
2025-03-03T21:53:39.505367+10:30 tech2400-VirtualBox sshd[4279]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 34698 ssh2  
2025-03-03T21:53:39.712219+10:30 tech2400-VirtualBox sshd[4279]: Failed password  
for invalid user invaliduser from 127.0.0.1 port 34698 ssh2  
tech2400@tech2400-VirtualBox:~$
```

Activity: Ingesting Logs into ELK

Goal: To process and store logs in Elasticsearch for analysis

Note: Logstash is the data processing pipeline that will pull in logs, process them, and forward them to Elasticsearch

Step 1: Create a Logstash configuration file

- Run `sudo nano /etc/logstash/conf.d/ssh_logs.conf`

Activity: Ingesting Logs into ELK

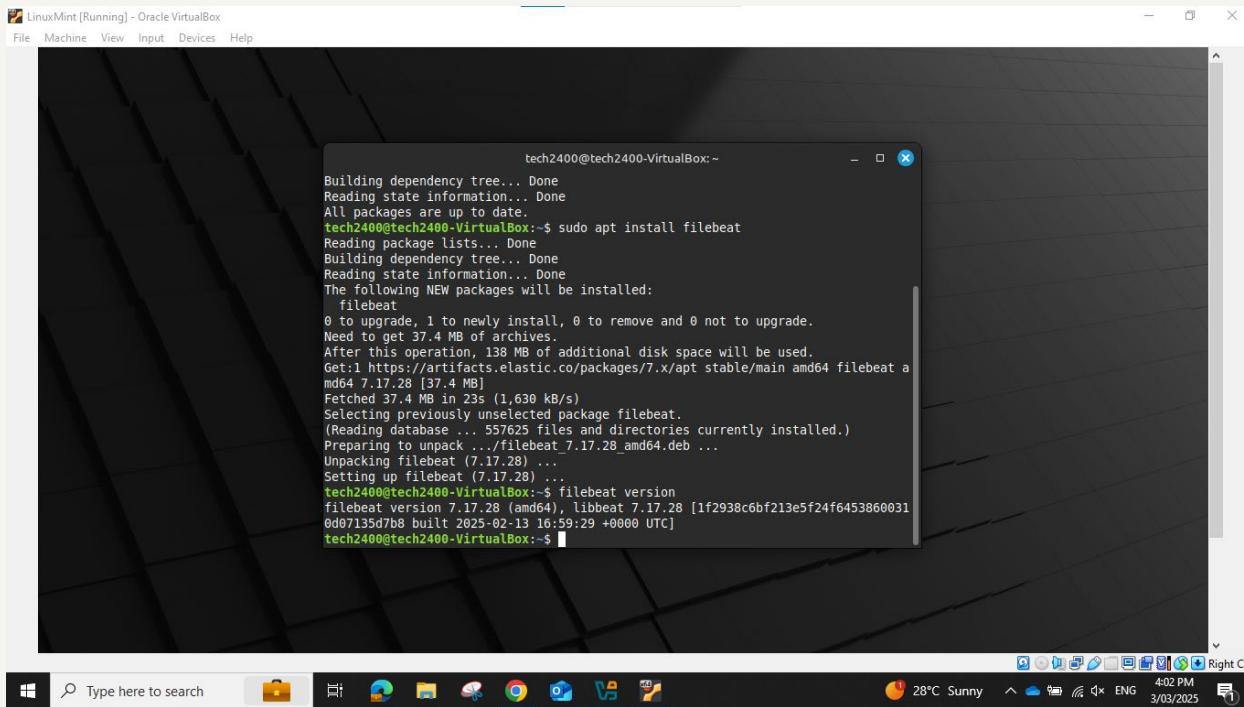
Step 1: Create a Logstash configuration file

- `sudo nano /etc/logstash/conf.d/ssh_logs.conf`

Activity: Ingesting Logs into ELK

Step 2: Verify Filebeat installation

- Run filebeat version



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window contains the following text:

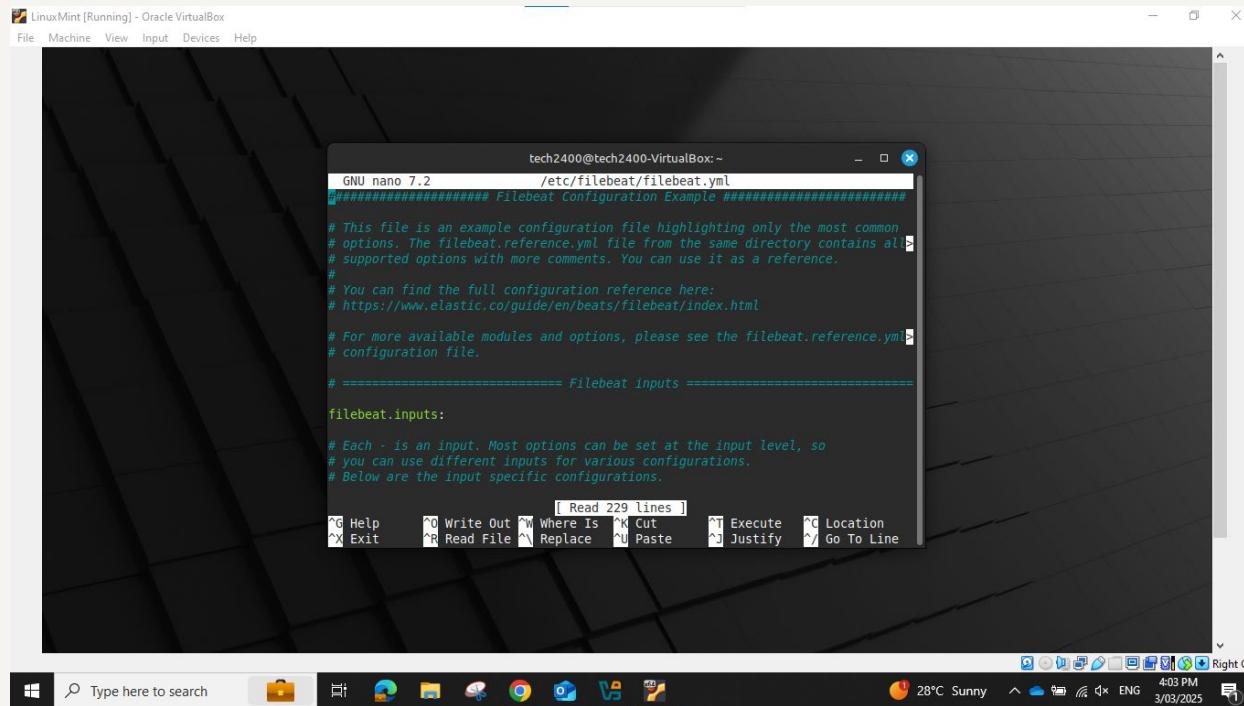
```
tech2400@tech2400-VirtualBox: ~
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
tech2400@tech2400-VirtualBox: $ sudo apt install filebeat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 to upgrade, 1 to newly install, 0 to remove and 0 not to upgrade.
Need to get 37.4 MB of archives.
After this operation, 138 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 filebeat all 7.17.28 [37.4 MB]
Fetched 37.4 MB in 23s (1,630 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 557625 files and directories currently installed.)
Preparing to unpack .../filebeat_7.17.28_amd64.deb ...
Unpacking filebeat (7.17.28) ...
Setting up filebeat (7.17.28) ...
tech2400@tech2400-VirtualBox: $ filebeat version
filebeat version 7.17.28 (amd64), libbeat 7.17.28 [1f2938c6bf213e5f24f6453860031
0007135d7b8 built 2025-02-13 16:59:29 +0000 UTC]
tech2400@tech2400-VirtualBox: $
```

The terminal window is positioned over a dark-themed desktop background. At the bottom of the screen, there is a taskbar with various icons and a system tray showing the date and time.

Activity: Ingesting Logs into ELK

Step 3: Configure Filebeat

- Open Filebeat configuration file by running
- `sudo nano /etc/filebeat/filebeat.yml`



The screenshot shows a Linux Mint desktop environment with a terminal window open. The terminal title is "tech2400@tech2400-VirtualBox: ~" and the command is "GNU nano 7.2 /etc/filebeat/filebeat.yml". The window displays the "Filebeat Configuration Example" file, which includes comments about the configuration file and sections for "Filebeat inputs" and "Filebeat outputs". The desktop background is dark, and the taskbar at the bottom shows various application icons and system status.

```
tech2400@tech2400-VirtualBox: ~
GNU nano 7.2      /etc/filebeat/filebeat.yml
#####
# Filebeat Configuration Example #####
#
# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html
#
# For more available modules and options, please see the filebeat.reference.yml
# configuration file.
#
# ===== Filebeat inputs =====
filebeat.inputs:
#
# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

[ Read 229 lines ]
^O Help      ^O Write Out  ^W Where Is  ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File  ^Y Replace   ^U Paste     ^J Justify    ^G Go To Line
```

Activity: Ingesting Logs into ELK

Step 3: Configure Filebeat

- Navigate through the file to add the following configuration:

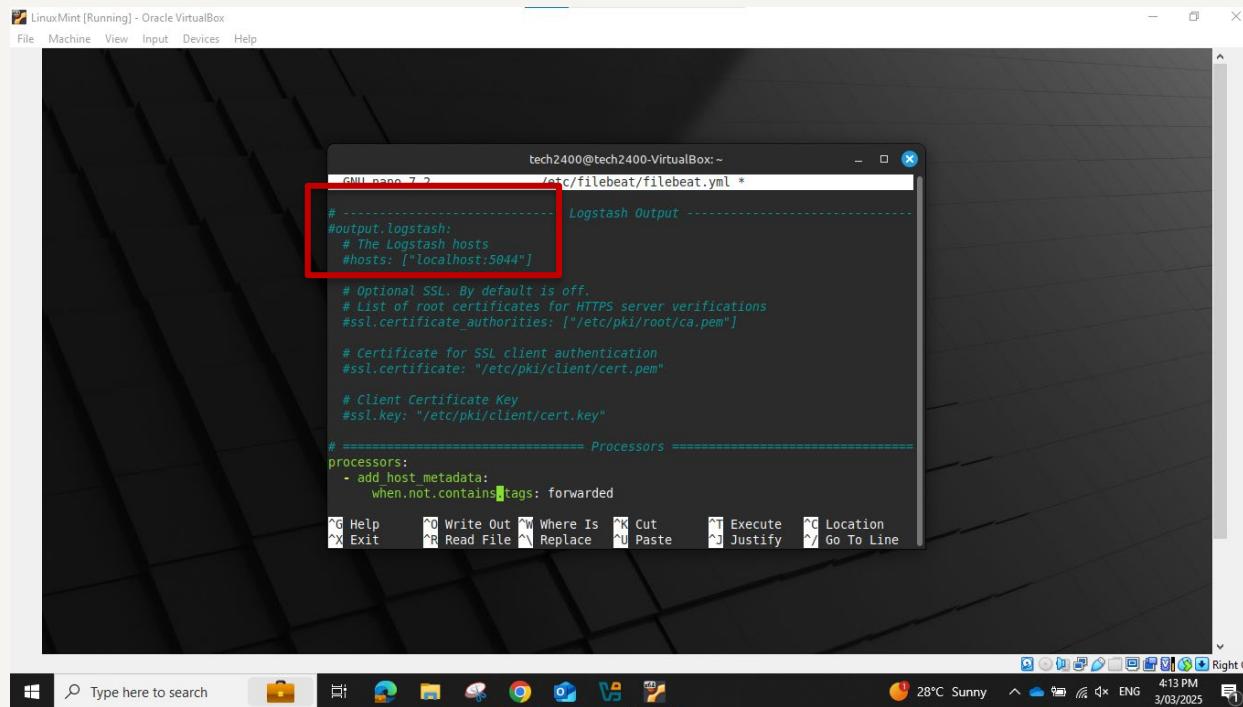
```
filebeat.inputs:
  - type: log
    paths:
      - /var/log/auth.log
```

```
GNU nano 7.2          /etc/filebeat/filebeat.yml *
# Below are the input specific configurations.
# filestream is an input for collecting log messages from files.
- type: log
  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id
  # Change to true to enable this input configuration.
  enabled: false
  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/auth.log
    #- c:\programdata\elasticsearch\logs\*
  # Exclude lines. A list of regular expressions to match. It drops the lines t#
  # matching any regular expression from the list.
  #exclude_lines: ['^DBG']
```

Activity: Ingesting Logs into ELK

Step 3: Configure Filebeat

- Look for output.logstash and make sure that hosts: ["localhost:5044"]



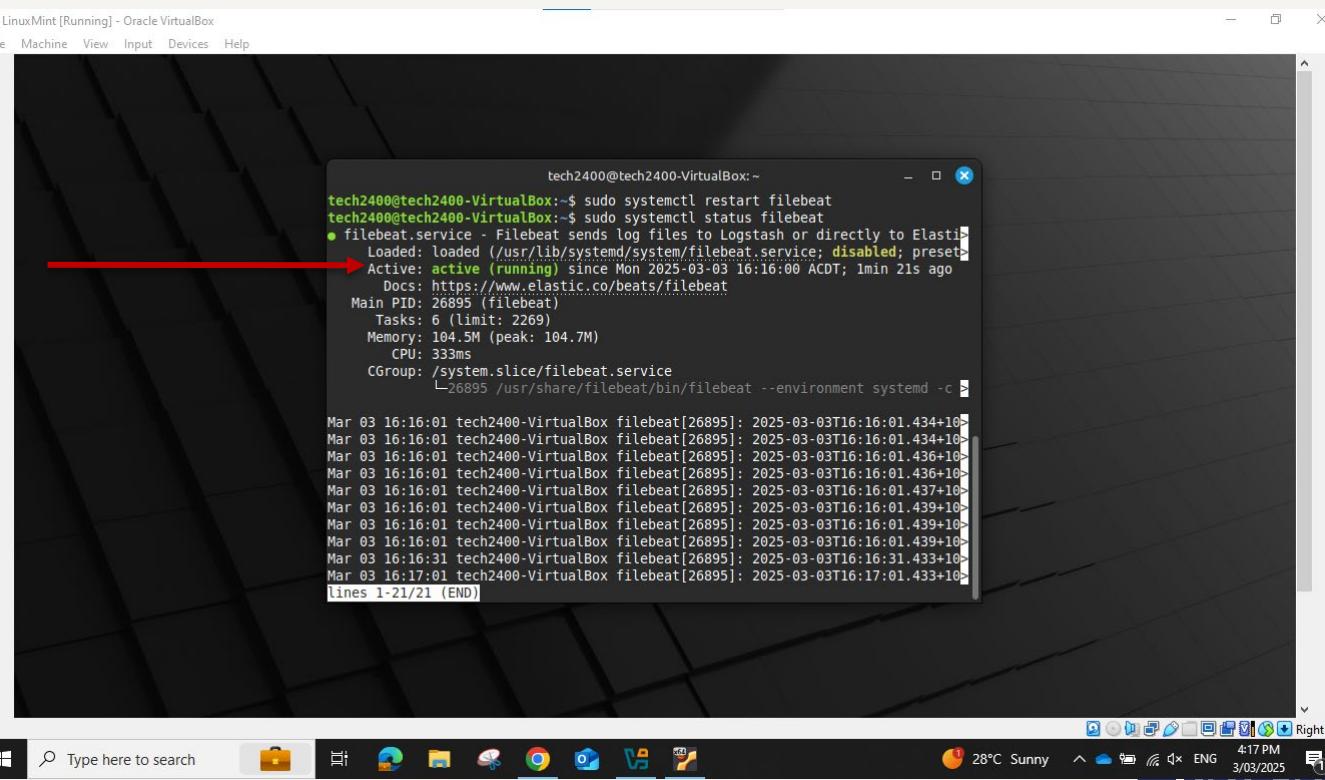
```
tech2400@tech2400-VirtualBox: ~ /etc/filebeat/filebeat.yml *  
GNU nano 7.2  
  
# -----  
#output.logstash:  
#  # The Logstash hosts  
#hosts: ["localhost:5044"]  
  
# -----  
# Optional SSL. By default is off.  
# List of root certificates for HTTPS server verifications  
#ssl.certificateAuthorities: ["/etc/pki/root/ca.pem"]  
  
# Certificate for SSL client authentication  
#ssl.certificate: "/etc/pki/client/cert.pem"  
  
# Client Certificate Key  
#ssl.key: "/etc/pki/client/cert.key"  
  
# ====== Processors ======  
processors:  
- add_host_metadata:  
  when.not.contains(tags: forwarded)  
  
^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location  
^X Exit      ^R Read File  ^L Replace   ^U Paste    ^J Justify  ^Y Go To Line  
Type here to search  28°C Sunny  4:13 PM  3/03/2025 Right Ctrl
```

Activity: Ingesting Logs into ELK

Step 3: Configure Filebeat

- Save the file (Ctrl+O) and exit (Ctrl+X)
- Restart Filebeat: **sudo systemctl restart filebeat**
- Verify status: **sudo systemctl restart filebeat**

Indicates
Filebeat
is running



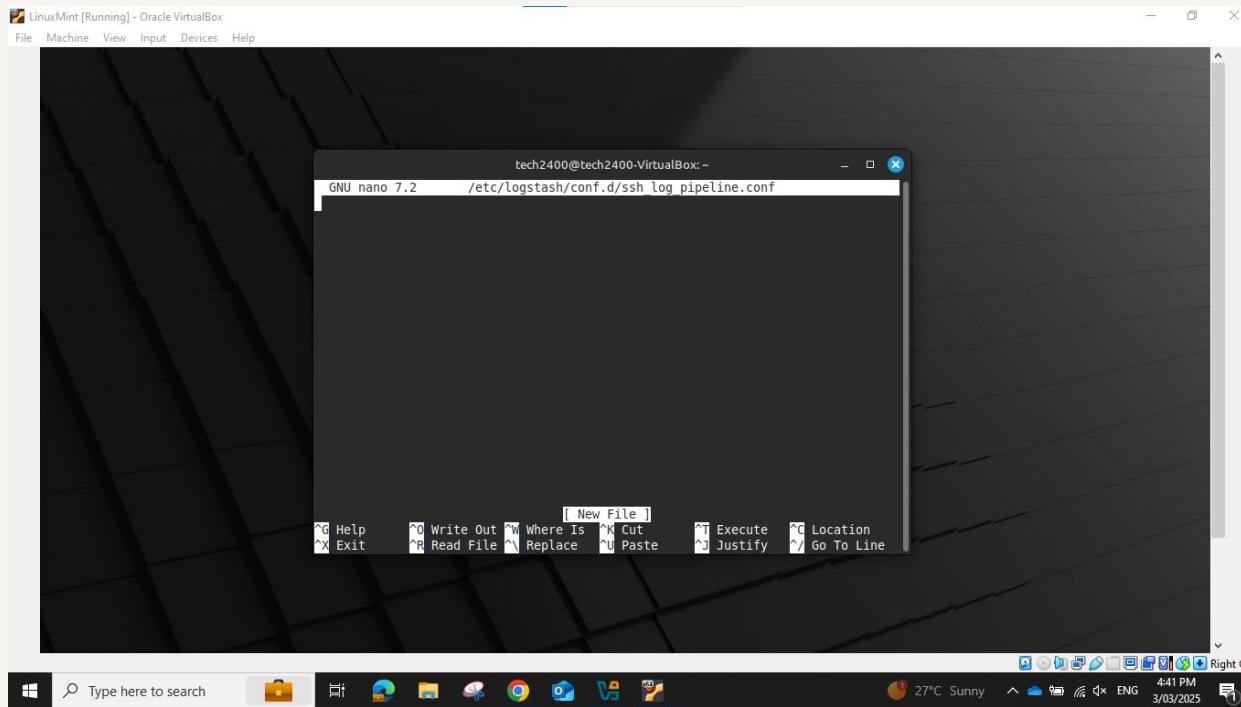
```
tech2400@tech2400-VirtualBox:~$ sudo systemctl restart filebeat
tech2400@tech2400-VirtualBox:~$ sudo systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; disabled; preset:)
   Active: active (running) since Mon 2025-03-03 16:16:00 ADT; 1min 21s ago
     Docs: https://www.elastic.co/beans/filebeat
          >Main PID: 26895 (filebeat)
              Tasks: 6 (limit: 2269)
             Memory: 104.5M (peak: 104.7M)
                CPU: 333ms
              CGroup: /system.slice/filebeat.service
                      └─26895 /usr/share/filebeat/bin/filebeat --environment systemd -c >

Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.434+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.434+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.436+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.436+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.436+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.437+1000
Mar 03 16:16:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:01.439+1000
Mar 03 16:16:31 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:16:31.433+1000
Mar 03 16:17:01 tech2400-VirtualBox filebeat[26895]: 2025-03-03T16:17:01.433+1000
lines 1-21/21 (END)
```

Activity: Ingesting Logs into ELK

Step 4: Configure Logstash to parse SSH logs

- Edit the Logstash pipeline configuration:
- `sudo nano /etc/logstash/conf.d/ssh_log_pipeline.conf`



Activity: Ingesting Logs into ELK

Step 4: Configure Logstash to parse SSH logs

- Copy the input, filter, and output configuration from the screenshot
- Or, use generative AI to generate the configuration
- Copy and then paste (Ctrl+Shift+V) the configuration to enable SSH log collection.
- Save (Ctrl+O)
- Enter to accept file name
- Close (Ctrl+X)

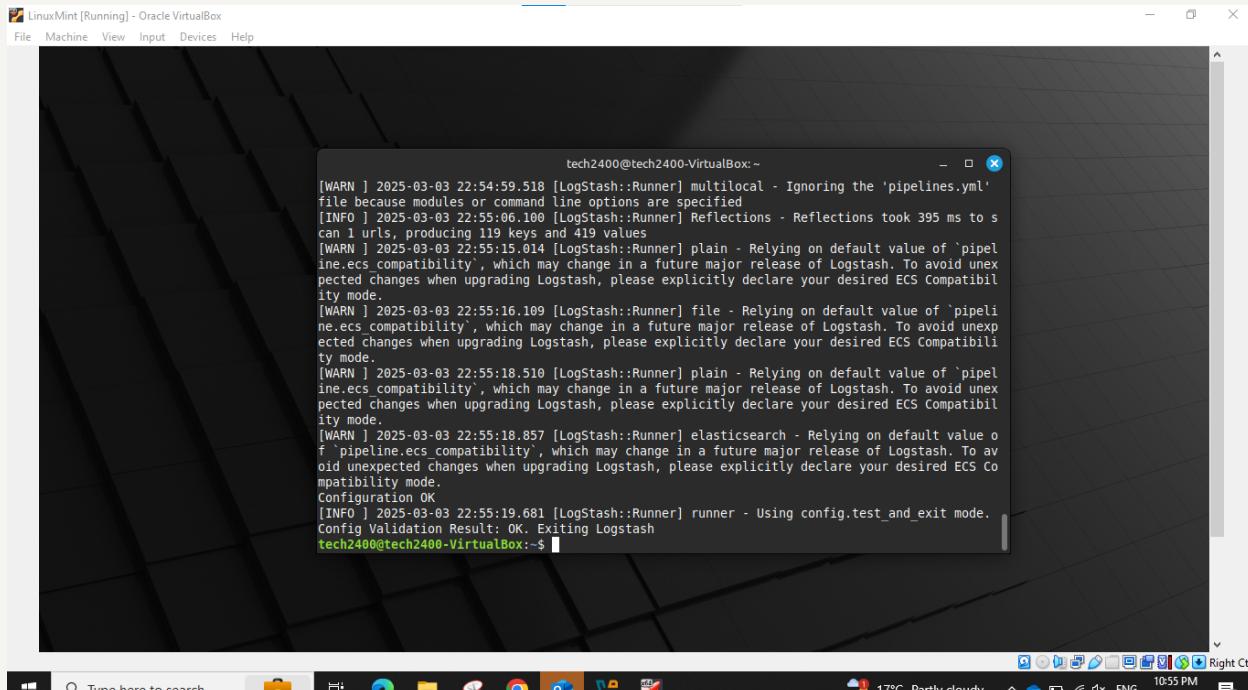
```
1  input {
2    file {
3      path => "/var/log/auth.log" # Path to the SSH log file
4      start_position => "beginning"
5      since_db_path => "/dev/null" # This ensures it reads the
6                                # file from the start every time
7    }
8
9    filter {
10      # Optional: Parse logs (you can use grok for more complex
11      # parsing)
12      grok {
13        match => { "message" => "%{SYSLOGTIMESTAMP:timestamp}
14                                %{HOSTNAME:hostname} %{DATA:program} [%{NUMBER:pid}]:
15                                %{GREEDYDATA:message}" }
16
17      # Optional: Add a date filter for parsing the timestamp
18      # properly
19      date {
20        match => ["timestamp", "MMM dd HH:mm:ss", "ISO8601"]
21
22      # Optional: You can use mutate to clean or modify fields as
23      # needed
24      mutate {
25        add_field => { "log_type" => "ssh" }
26      }
27
28      output {
29        elasticsearch {
30          hosts => ["http://localhost:9200"] # Elasticsearch URL
31          index => "ssh_logs-%{+YYYY.MM.dd}" # Index name pattern
32          with_date
33          user => "elastic" # Elasticsearch username (if required)
34          password => "changeme" # Elasticsearch password (if
35                                # required)
36        }
37      }
38
39      stdout {
40        codec => rubydebug # To print to the console for debugging
41      }
42    }
43  }
```

Activity: Ingesting Logs into ELK

Step 4: Configure Logstash to parse SSH logs

- Test the Logstash configuration

```
sudo logstash -f /etc/logstash/conf.d/ssh_logs.conf --  
config.test_and_exit
```



The screenshot shows a terminal window titled "LinuxMint [Running] - Oracle VirtualBox". The window contains the following Logstash configuration test output:

```
tech2400@tech2400-VirtualBox:~  
[WARN ] 2025-03-03 22:54:59.518 [Logstash::Runner] multilocal - Ignoring the 'pipelines.yml' file because modules or command line options are specified  
[INFO ] 2025-03-03 22:55:06.100 [Logstash::Runner] Reflections - Reflections took 395 ms to scan 1 urls, producing 119 keys and 419 values  
[WARN ] 2025-03-03 22:55:15.014 [Logstash::Runner] plain - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.  
[WARN ] 2025-03-03 22:55:16.109 [Logstash::Runner] file - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.  
[WARN ] 2025-03-03 22:55:18.510 [Logstash::Runner] plain - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.  
[WARN ] 2025-03-03 22:55:18.857 [Logstash::Runner] elasticsearch - Relying on default value of 'pipeline.ecs_compatibility', which may change in a future major release of Logstash. To avoid unexpected changes when upgrading Logstash, please explicitly declare your desired ECS Compatibility mode.  
Configuration OK  
[INFO ] 2025-03-03 22:55:19.681 [Logstash::Runner] runner - Using config.test_and_exit mode.  
Config Validation Result: OK. Exiting Logstash  
tech2400@tech2400-VirtualBox:~$
```



Activity: Exploring the Logs in Kibana

Goal: To search and analyse logs related to failed SSH login attempts.

- Open Kibana (<http://localhost:5601>) in a browser
- Navigate to Discover

The screenshot shows the Kibana interface. At the top, there is a dark header with the 'elastic' logo, a search bar containing 'Search Elastic', and some user icons. Below the header is a navigation sidebar with several sections: 'Home', 'Analytics' (which is currently selected and has a red box around its 'Discover' item), 'Observability', 'Security', and 'Analytics'. The 'Discover' item under 'Analytics' is highlighted with a red box. To the right of the sidebar, there are four main cards: 'Observability' (yellow background, icon of a bar chart), 'Security' (pink background, icon of a shield), and 'Analytics' (blue background, icon of a bar chart). Each card has a brief description below it. At the bottom of the sidebar, there are two more sections: 'Enterprise Search' and 'App Search'.



Activity: Exploring the Logs in Kibana

- Click on Create index pattern

The screenshot shows the Elasticsearch Stack Management interface. The top navigation bar includes the elastic logo, a search bar labeled 'Search Elastic', and icons for refresh, settings, and user profile. Below the navigation, the breadcrumb trail shows 'Stack Management > Index patterns'. A sidebar on the left lists management categories: Ingest, Data, and Alerts and Insights, each with sub-options like Pipelines, Index Management, and Rules and Connectors. The main content area has a heading 'To visualize and explore data in Kibana' and a sub-section titled 'Management'. It features a large callout box with the text 'You have data in Elasticsearch. Now, create an index pattern.' It explains that Kibana requires an index pattern to identify data streams, indices, and index aliases. A blue button labeled '+ Create index pattern' is prominent. To the right of the text is a graphic of a blue cloud-like shape with a yellow square and a green plus sign. At the bottom of the callout box is a link 'Want to learn more? Read documentation'. A close button is at the bottom left of the callout.

Activity: Exploring the Logs in Kibana

- Under Name, enter: ssh_logs*
- In the Timestamp field, select: @timestamp
- Click Create index pattern

The screenshot shows the Elastic Stack Management interface with the 'Index patterns' tab selected. On the left, there's a sidebar with 'Management', 'Ingest', 'Data', 'Alerts and Insights', and 'Kibana' sections. The main area is titled 'Create index pattern' with fields for 'Name' (ssh_logs*) and 'Timestamp field' (@timestamp). A note says 'Use an asterisk (*) to match multiple characters. Spaces and the characters , , ?, " , <, >, | are not allowed.' To the right, a message says 'Your index pattern matches 1 source.' followed by 'ssh_logs-2025.03.03' and an 'Index' button. A 'Rows per page: 10' dropdown is also visible.

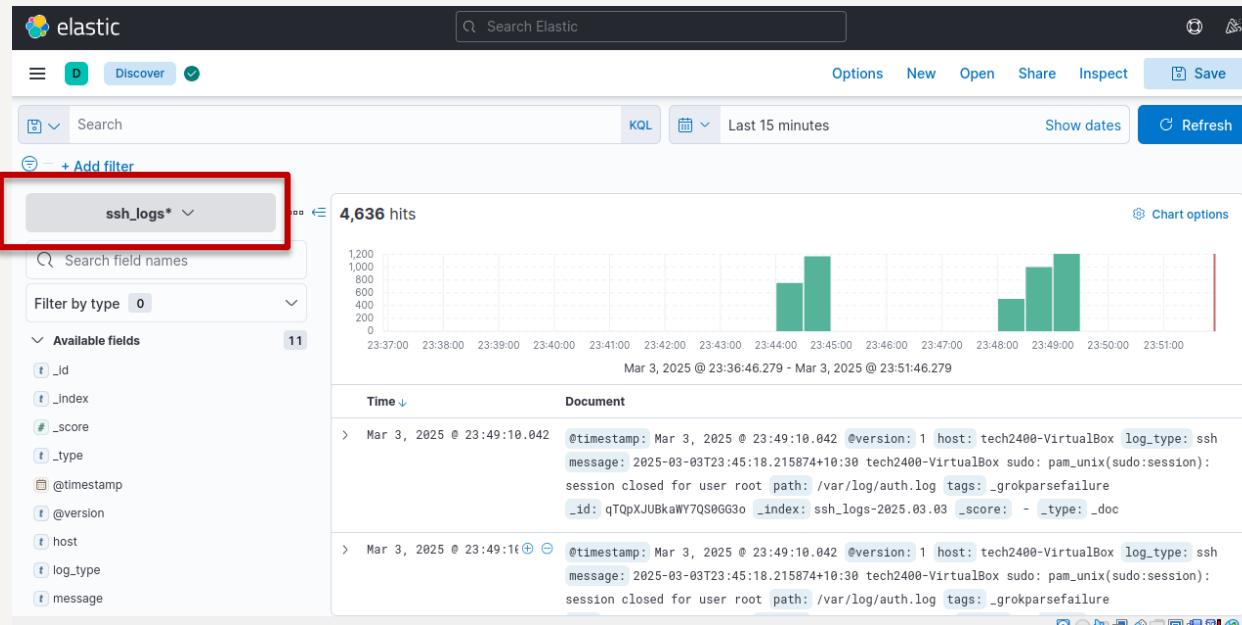
Activity: Exploring the Logs in Kibana

- Under Name, enter: ssh_logs*
- In the Timestamp field, select: @timestamp
- Click Create index pattern

The screenshot shows the Elastic Stack Management interface with the 'Index patterns' tab selected. On the left, there's a sidebar with 'Management', 'Ingest', 'Data', 'Alerts and Insights', and 'Kibana' sections. The main area is titled 'Create index pattern' with fields for 'Name' (ssh_logs*) and 'Timestamp field' (@timestamp). A note says 'Use an asterisk (*) to match multiple characters. Spaces and the characters , , ?, ", <, >, | are not allowed.' To the right, a message says 'Your index pattern matches 1 source.' followed by 'ssh_logs-2025.03.03' and an 'Index' button. A 'Rows per page: 10' dropdown is also visible.

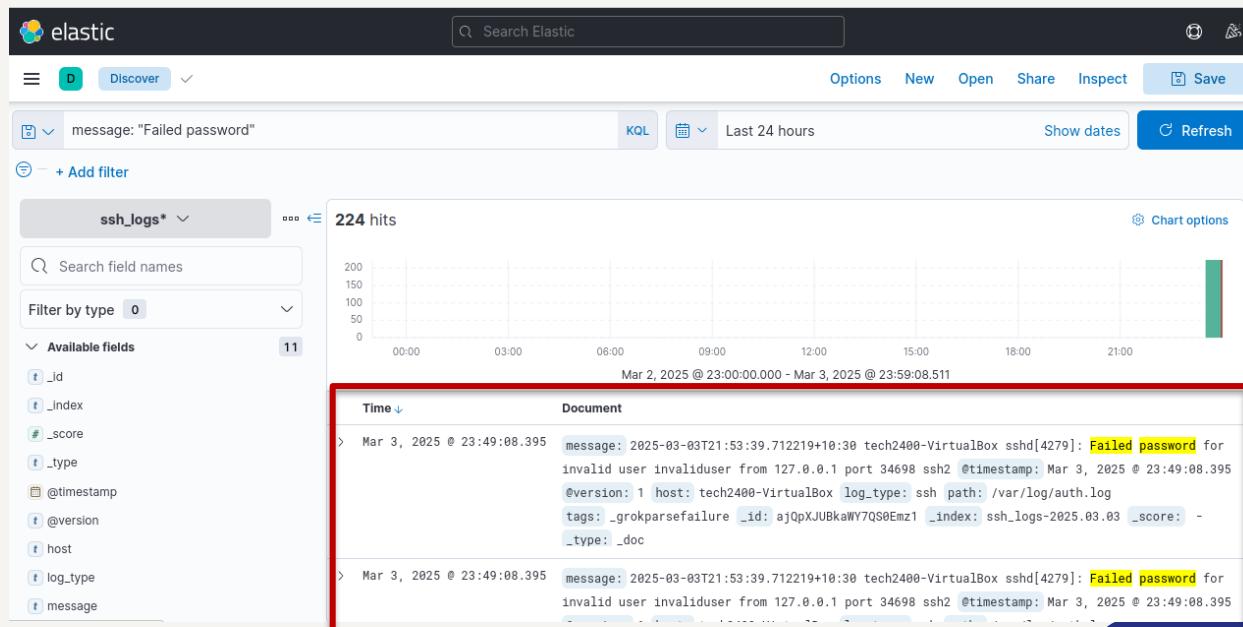
Activity: Exploring the Logs in Kibana

- Navigate back to Discover
- Make sure "ssh_logs-*" is selected from the dropdown



Activity: Exploring the Logs in Kibana

- Broaden the time range (e.g., Last 24 hours)
- Search for failed SSH attempts using
message: "Failed password"
- Check on the logs to identify patterns such as frequent failed attempts from the same IP.

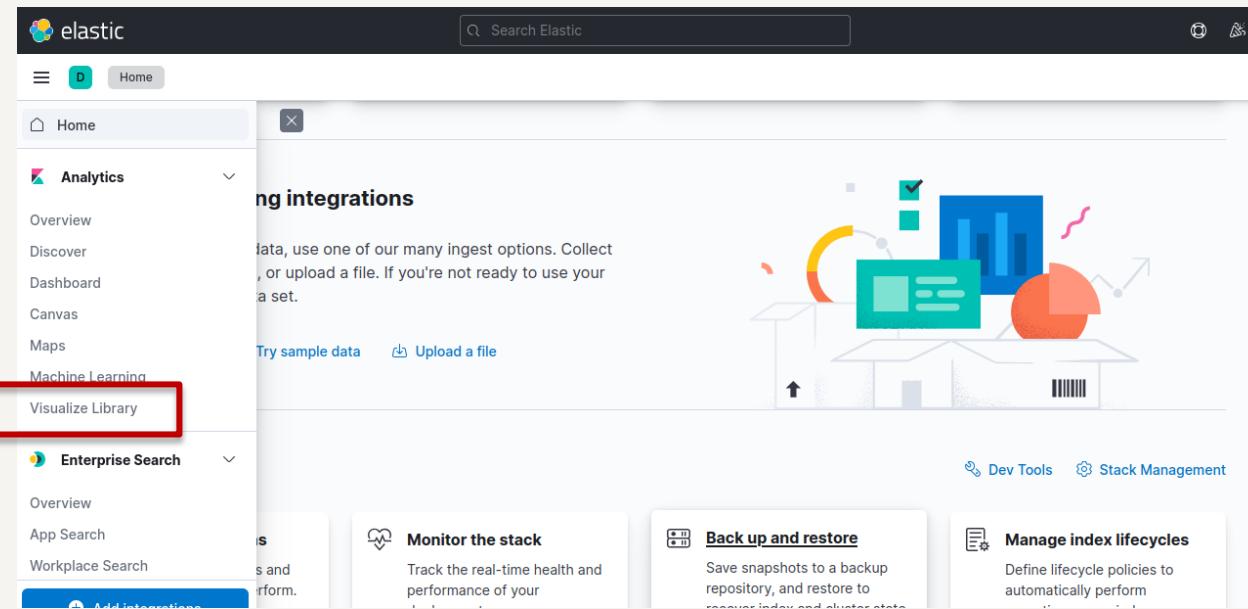


Activity:

Creating a Visualisation in Kibana

Goal: To visually analyse failed login attempts and detect brute force patterns.

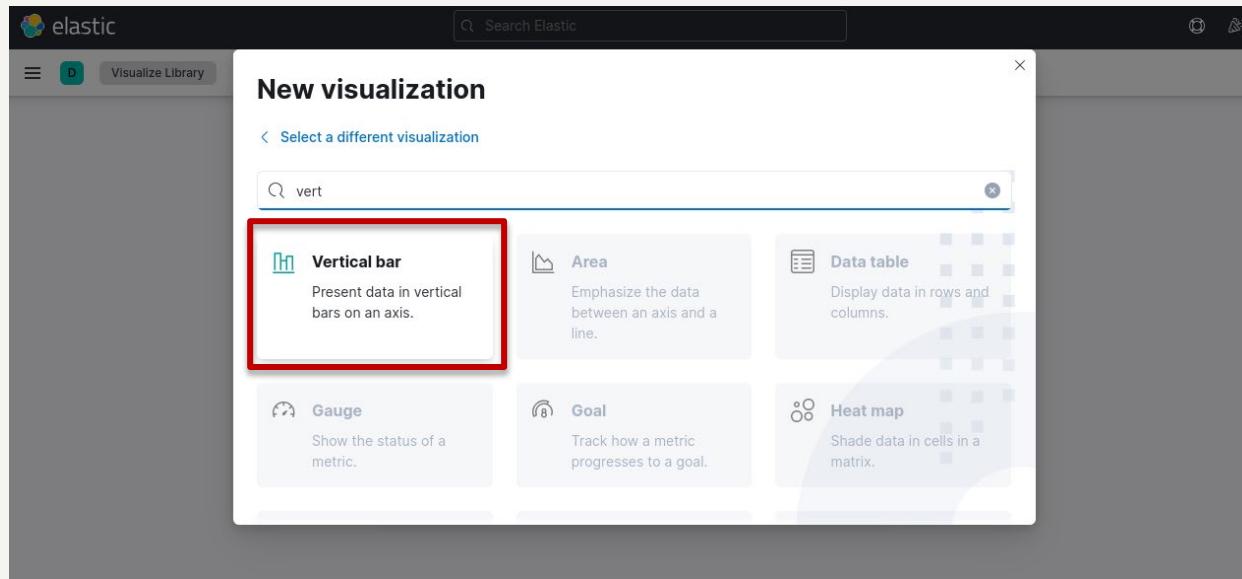
- Navigate to Visualize Library



Activity:

Creating a Visualisation in Kibana

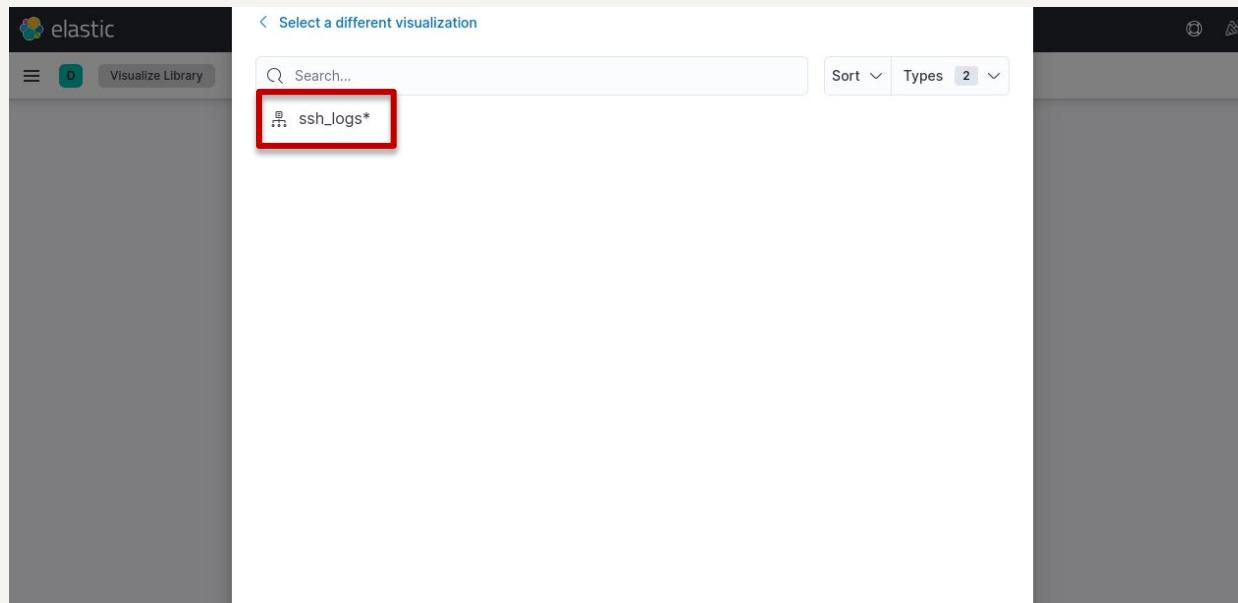
- Click Create new visualization > Aggregation based
- Filter: Vertical Bar



Activity:

Creating a Visualisation in Kibana

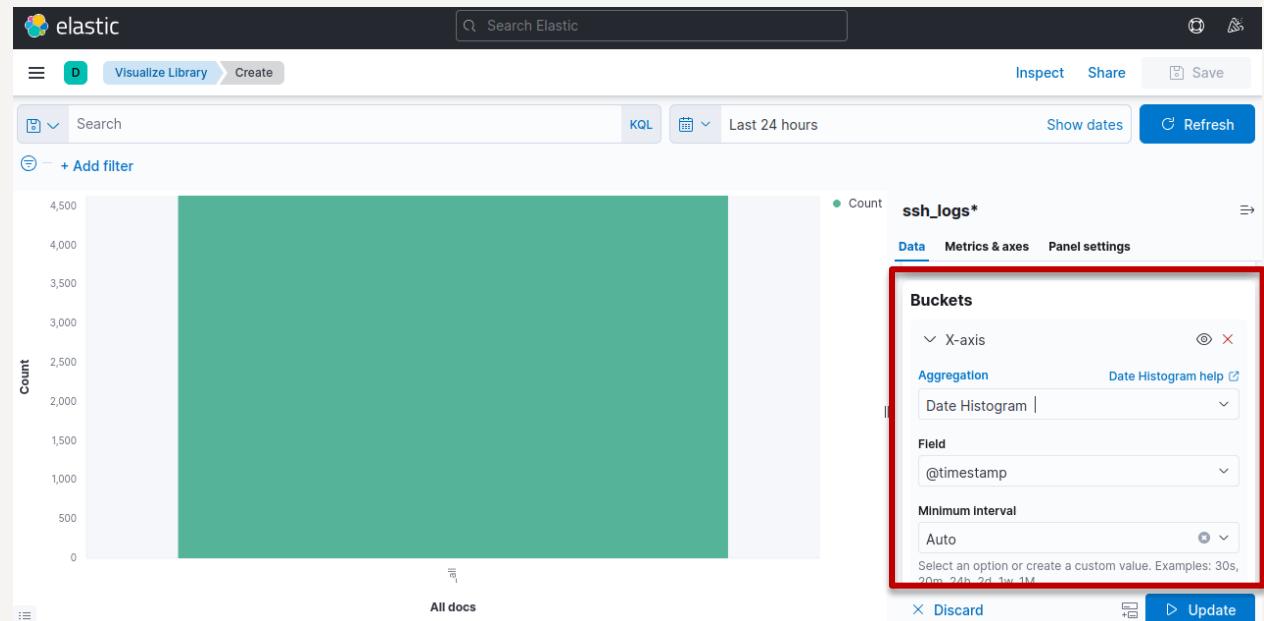
- Select ssh_logs* as the data source



Activity: Creating a Visualisation in Kibana

- Under Buckets, click Add
- Select X-axis
- Under Aggregation, select Date Histogram
- Set Field to @timestamp and Minimum interval to Auto
- Click Update

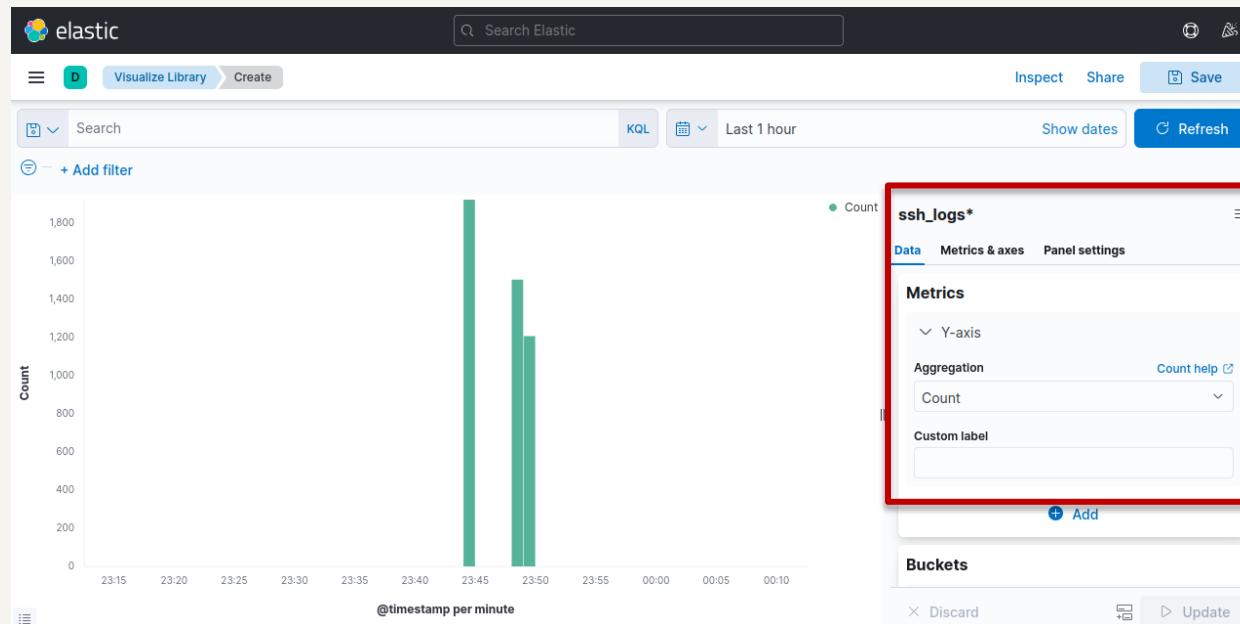
Note: By default,
Y-Axis is already
set to count



Activity: Creating a Visualisation in Kibana

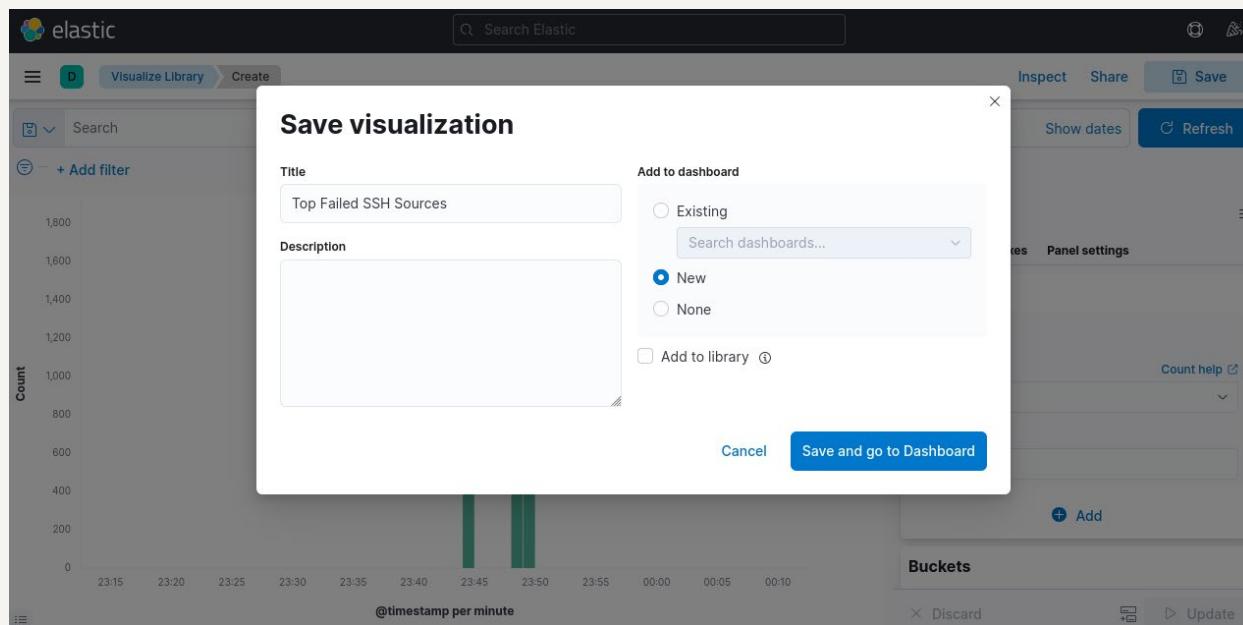
- The bar chart has been updated

Note: By default, Y-Axis is already set to count, which counts the number of logs



Activity: Creating a Visualisation in Kibana

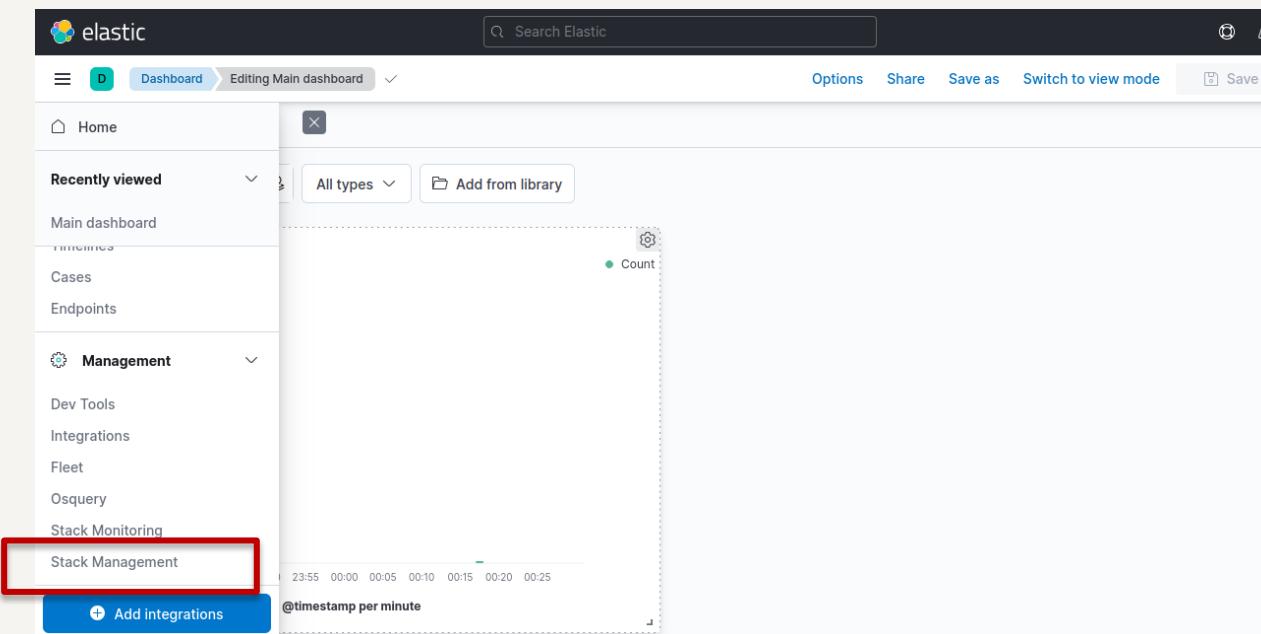
- Click on the Save button at the top right corner
- Save the visualisation and select the dashboard to which it will be saved (in this case, select New)



Activity: Setting up an Alert

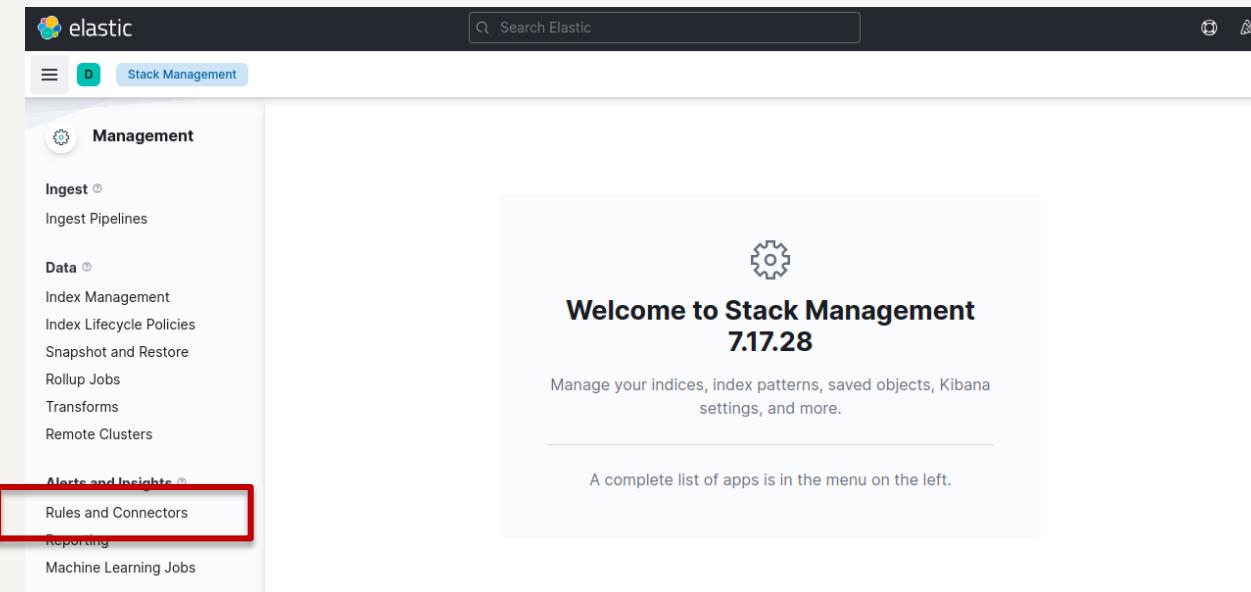
Goal: To get notified when a potential brute-force attack occurs.

- In Kibana, go to Stack Management



Activity: Setting up an Alert

- Navigate to Rules and Connectors



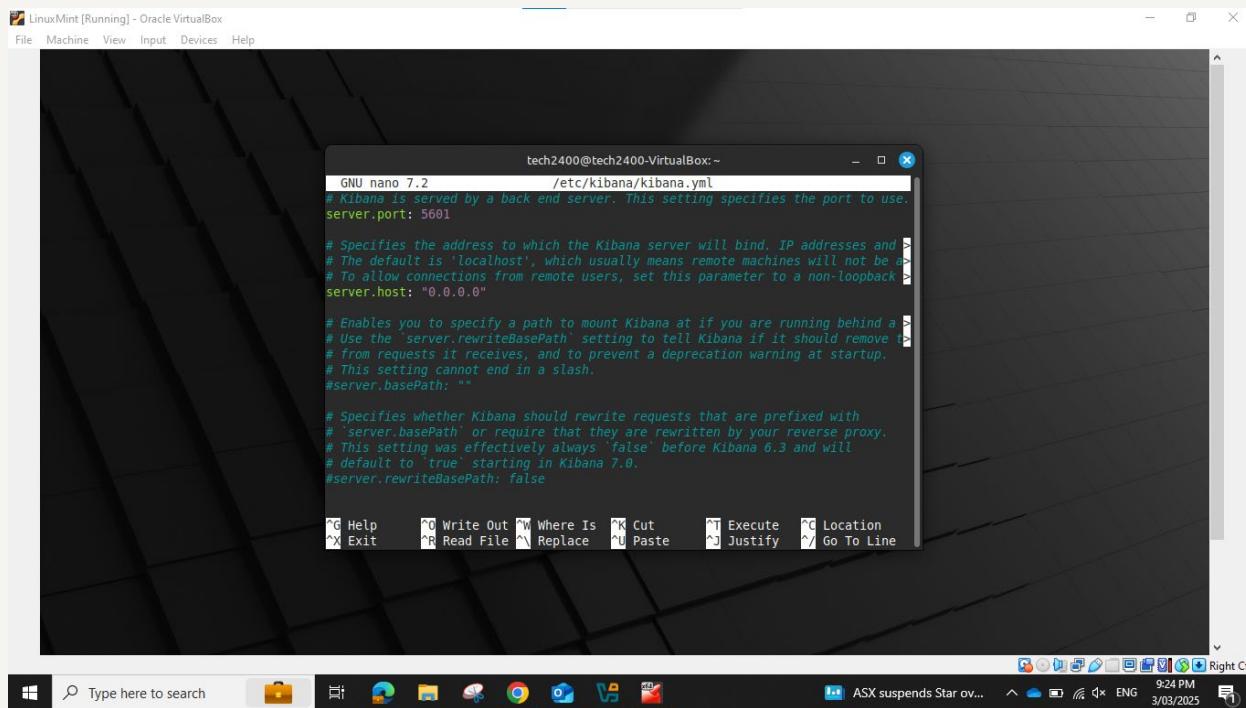
Activity: Setting up an Alert

- Additional setup will be required because Kibana needs to securely handle sensitive information when triggering alerts

The screenshot shows the Elastic Stack Management interface. The top navigation bar includes the elastic logo, a search bar labeled "Search Elastic", and icons for refresh, settings, and help. Below the navigation is a breadcrumb trail: "Management > Stack Management > Rules". On the left, a sidebar menu lists "Management", "Ingest", "Data", and "Alerts and Insights". Under "Alerts and Insights", "Rules and Connectors" is selected and highlighted in blue. The main content area is titled "Rules and Connectors" and contains the sub-instruction "Detect conditions using rules, and take actions using connectors." Below this are two tabs: "Rules" (selected) and "Connectors". A prominent red rectangular box highlights a callout message: "((o)) Additional setup required You must configure an encryption key to use Alerting. [Learn more.](#)"

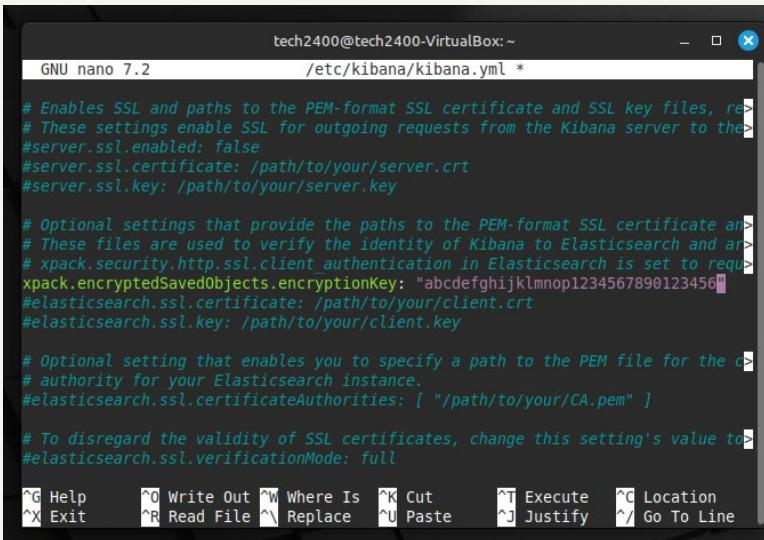
Activity: Setting up an Alert

- Close your browser and open a Terminal
- Run `sudo nano /etc/kibana/kibana.yml`



Activity: Setting up an Alert

- Add the Encryption Key setting (anywhere in the file):
**Xpack.encryptedSavedObjects.encryptionKey:
"your_encryption_key"**
- Save (Ctrl+O), Enter to accept filename, Close (Ctrl+X)



```
tech2400@tech2400-VirtualBox: ~
GNU nano 7.2          /etc/kibana/kibana.yml *

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, re>
# These settings enable SSL for outgoing requests from the Kibana server to the>
#server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate an>
# These files are used to verify the identity of Kibana to Elasticsearch and ar>
# xpack.security.http.ssl.client_authentication in Elasticsearch is set to requ>
xpack.encryptedSavedObjects.encryptionKey: "abcdefghijklmnopqrstuvwxyz1234567890123456"
#elasticsearch.ssl.certificate: /path/to/your/client.crt
#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the c>
# authority for your Elasticsearch instance.
#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]

# To disregard the validity of SSL certificates, change this setting's value to>
#elasticsearch.ssl.verificationMode: full

^K Help   ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit   ^R Read File  ^L Replace   ^U Paste    ^J Justify  ^/ Go To Line
```

Note: A strong random string of at least 32 characters is recommended.

- Restart Kibana: **sudo systemctl restart kibana**

Activity: Setting up an Alert

- Open Kibana on a browser (<http://localhost:5601>)
- Navigate back to Stack Management > Rules and Connectors
- Click on Create Rule

The screenshot shows the Elastic Stack Management interface. The top navigation bar includes the elastic logo, a search bar, and links for Stack Management and Rules. On the left, a sidebar titled 'Management' lists Ingest (Ingest Pipelines), Data (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters), and Alerts and Insights (Rules and Connectors, Reporting, Machine Learning Jobs). The main content area is titled 'Rules and Connectors' and contains the sub-titles 'Rules' and 'Connectors'. It features a large button labeled '(o) Create your first rule' with a sub-instruction: 'Receive an alert through email, Slack, or another connector when a condition is met.' A red box highlights the 'Create rule' button.

Activity: Setting up an Alert

Configure your rule:

- Name: SSH Brute Force Detection
- Check every: 1 minute
- Notify: Only on status change

Create rule

Name	Tags (optional)
SSH Brute Force Detection	
Check every <small>?</small>	Notify <small>?</small>
1	minute
	Only on status change

Activity: Setting up an Alert

Configure your rule:

- Rule type: Index threshold

INDEX ssh_logs*
WHEN count()
OVER all documents

IS ABOVE 50

- Click Save

Create rule

Index threshold X

Alert when an aggregated query meets the threshold. [Documentation](#) ↗

Select an index

INDEX ssh_logs*

WHEN count()

OVER all documents

Define the condition

IS ABOVE 50

Cancel ✓ Save

Activity: Setting up an Alert

- Access your rule through Stack Management > Rules and Connectors

The screenshot shows the Elastic Stack Management interface with the following details:

- Header:** elastic, Search Elastic, Documentation.
- Breadcrumbs:** Stack Management > Rules.
- Left Sidebar (Management):**
 - Ingest: Ingest Pipelines
 - Data: Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters
 - Alerts and Insights: Rules and Connectors
 - Reporting, Machine Learning Jobs
- Central Content:**

Rules and Connectors

Detect conditions using rules, and take actions using connectors.

Rules tab is selected.

Buttons: Create rule, Search, Type 0, Action type 0, Status 0, Refresh.

Statistics: Showing: 1 of 1 rules. Active: 0, Error: 0, Ok: 1, Pending: 0, Unknown: 0.

Ena...	Name ↑	Last run	Inter...	Duration	Status
<input type="checkbox"/>	<input checked="" type="checkbox"/> SSH Brute Force Detection Index threshold	Mar 4, 2025 01:47:08am a few seconds ago	1 min	00:00:00.118	Ok

Rows per page: 10.



Next Week

Week 10: Incident Response & Management (Part 2)

- Advanced Incident Response
- Basic Forensic Analysis Concepts
- Post-Incident Response & Lessons Learned
- Introduction to Snort on pfSense