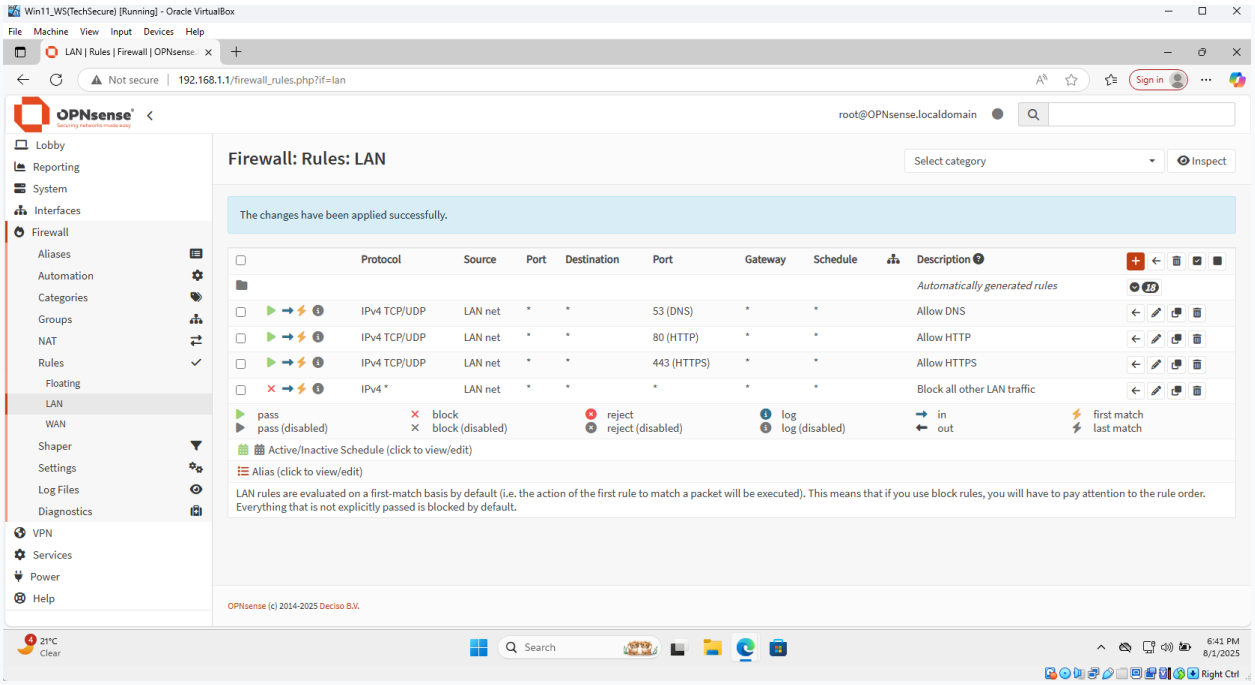
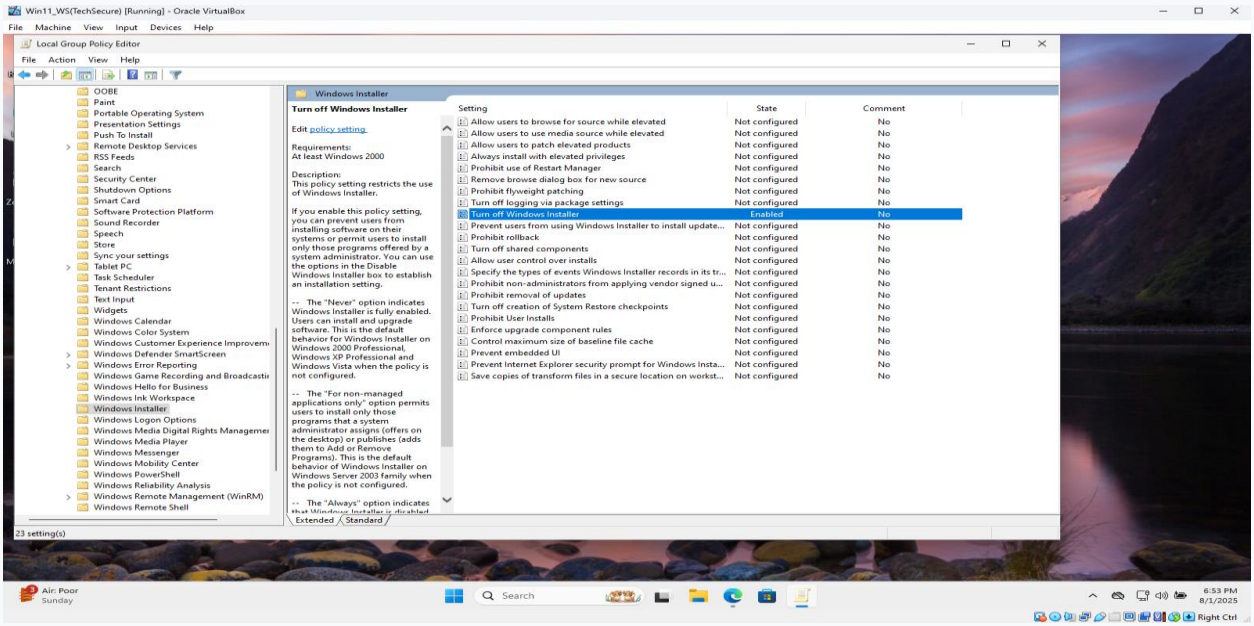
Week 12 - Enterprise Network Security

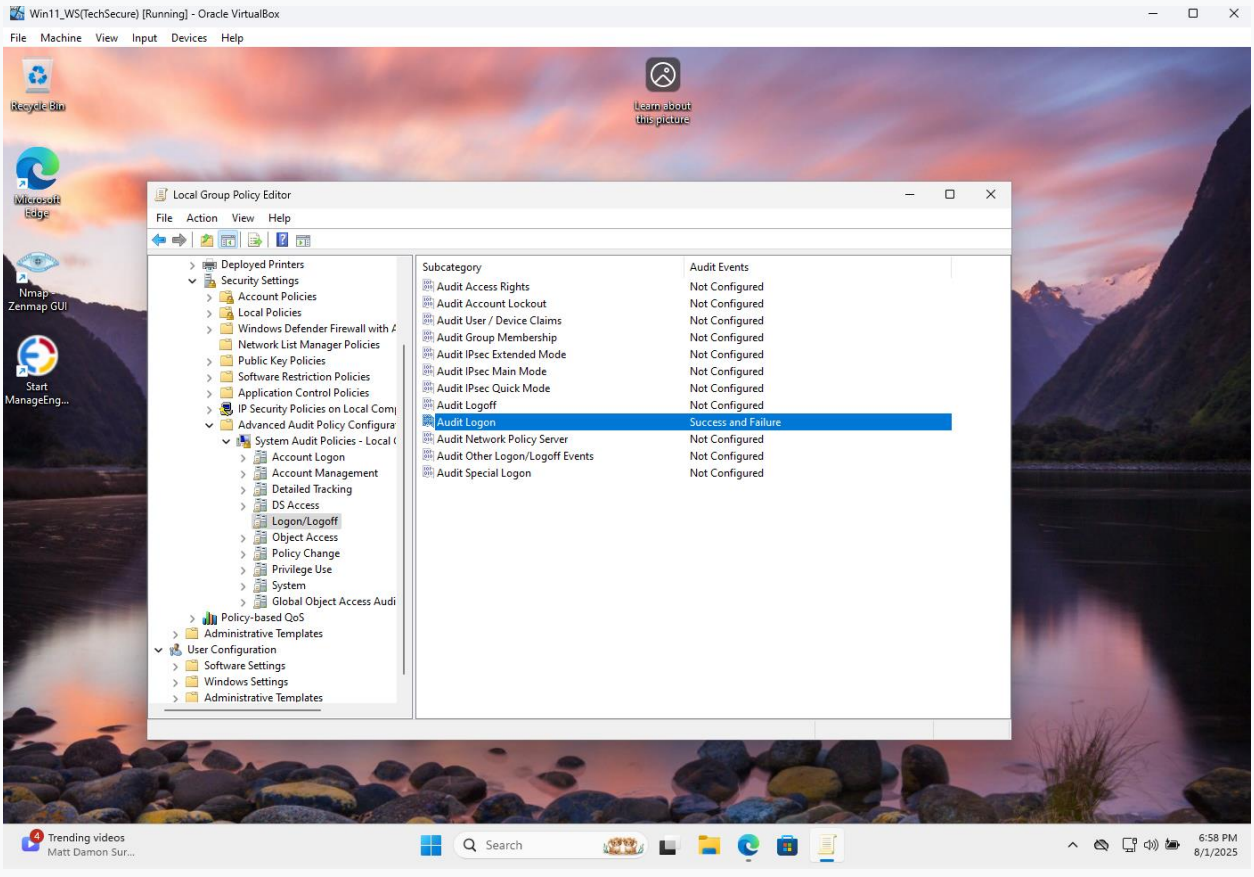
Task 1: Hardening Local VMs

1. OPNSense Router

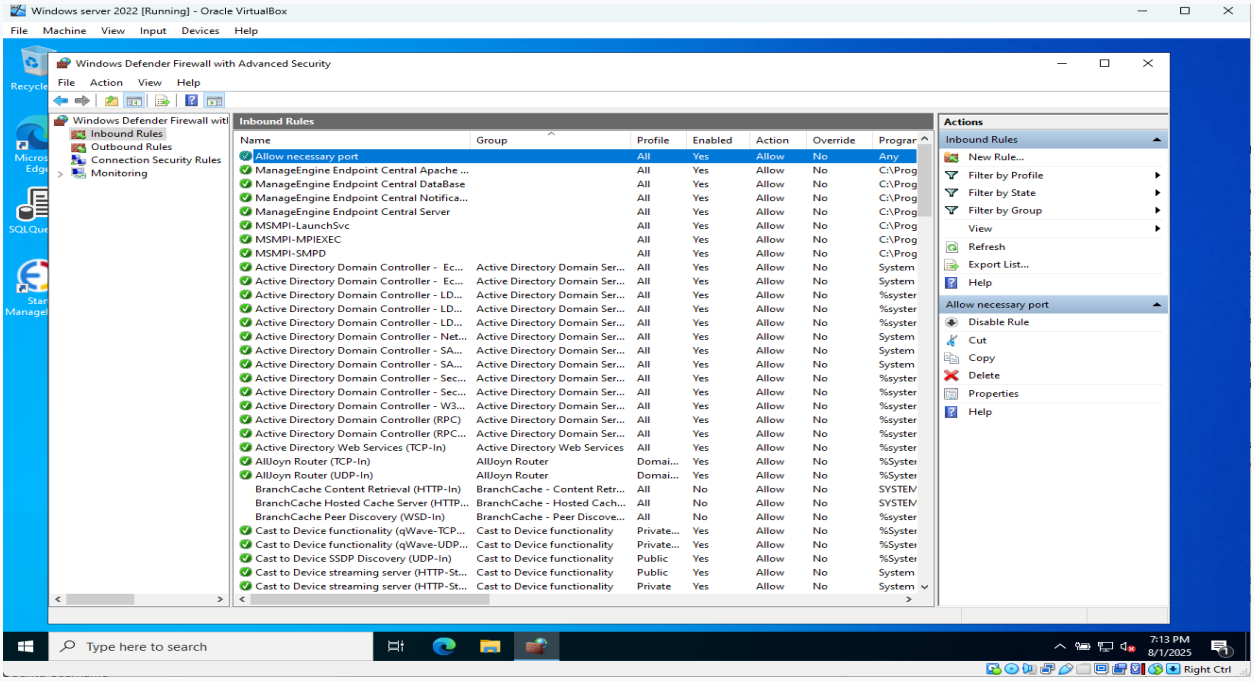


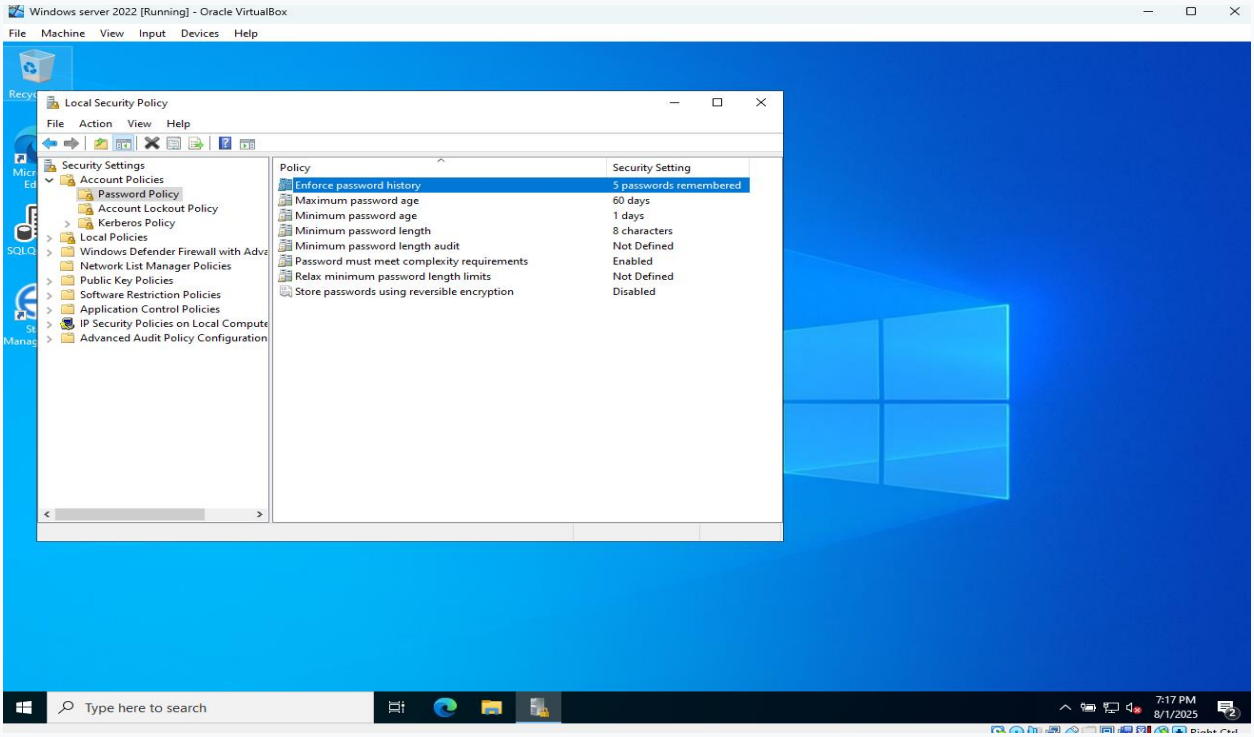
2. Windows 11



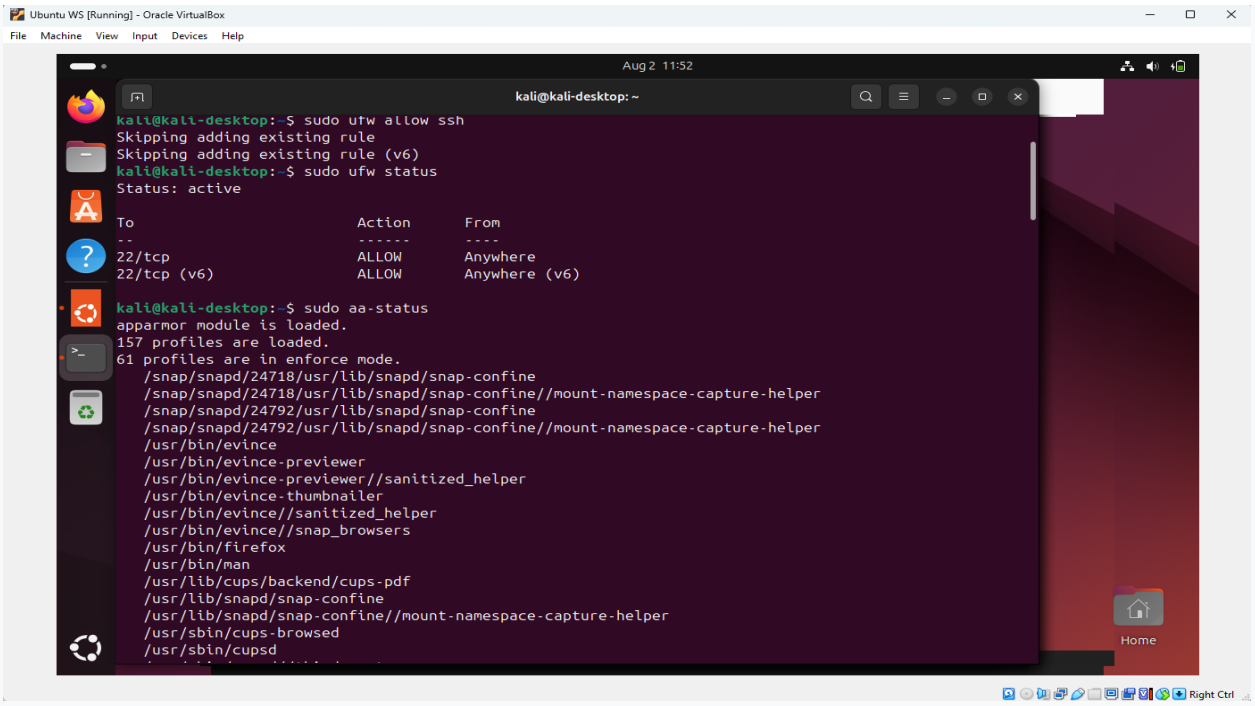


3. Windows Server 2022

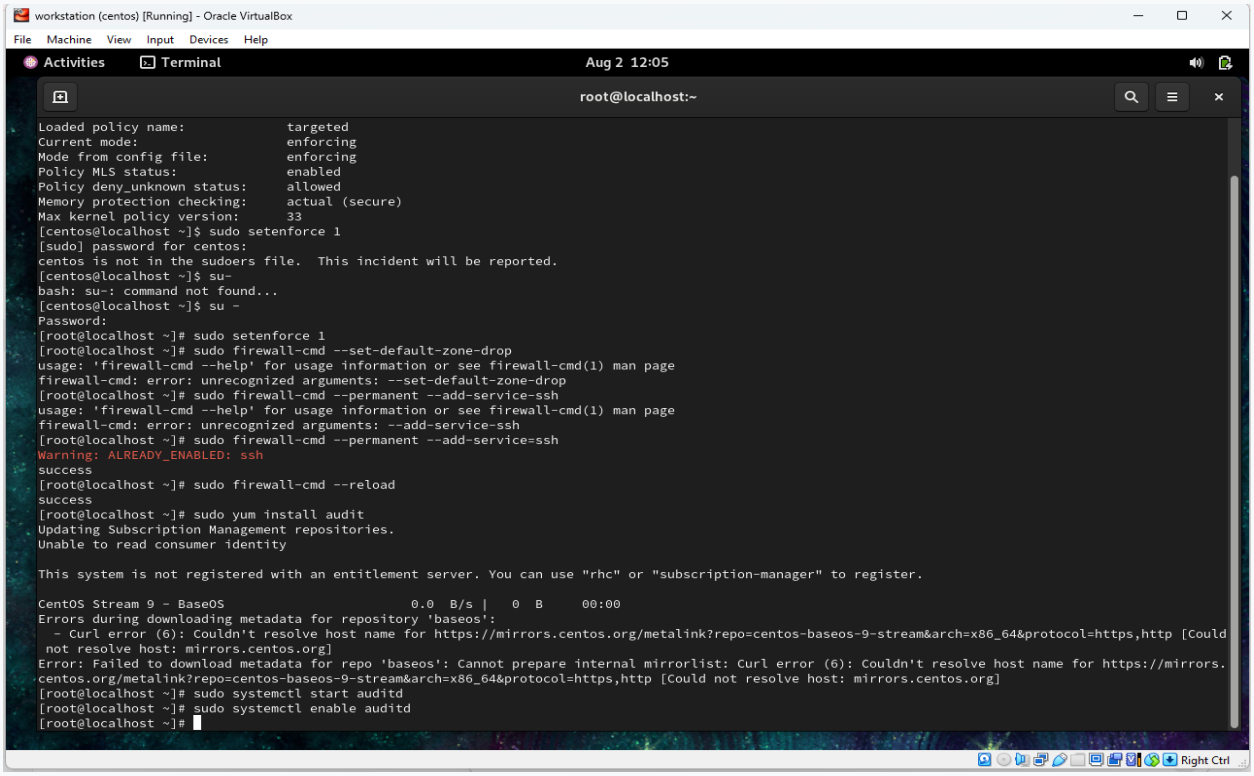

Windows server 2022 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action Override Program
Allow necessary port All Yes Allow No Any
ManageEngine Endpoint Central Apache ... All Yes Allow No C:\Prog
ManageEngine Endpoint Central DataBase All Yes Allow No C:\Prog
ManageEngine Endpoint Central Notifica... All Yes Allow No C:\Prog
ManageEngine Endpoint Central Server All Yes Allow No C:\Prog
MSMPI-LaunchSvc All Yes Allow No C:\Prog
MSMPI-MPIEXEC All Yes Allow No C:\Prog
MSMPI-SMPD All Yes Allow No C:\Prog
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes Allow No System
Active Directory Domain Controller - Ec... Active Directory Domain Ser... All Yes Allow No System
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller - LD... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller - Net... Active Directory Domain Ser... All Yes Allow No System
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes Allow No System
Active Directory Domain Controller - SA... Active Directory Domain Ser... All Yes Allow No System
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller - Sec... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller - W3... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller (RPC) Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Domain Controller (RPC... Active Directory Domain Ser... All Yes Allow No %syster
Active Directory Web Services (TCP-In) Active Directory Web Services All Yes Allow No %syster
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes Allow No %Syster
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes Allow No %Syster
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No Allow No SYSTEM
BranchCache Hosted Cache Server (HTTP... BranchCache - Hosted Cach... All No Allow No SYSTEM
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No Allow No %syster
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes Allow No %Syster
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes Allow No %Syster
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow No %Syster
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes Allow No System
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes Allow No System
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Allow necessary port
Disable Rule
Cut
Copy
Delete
Properties
Help
Type here to search
7:13 PM
8/1/2025
Right Ctrl


Windows server 2022 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy Security Setting
Enforce password history 5 passwords remembered
Maximum password age 60 days
Minimum password age 1 days
Minimum password length 8 characters
Minimum password length audit Not Defined
Password must meet complexity requirements Enabled
Relax minimum password length limits Not Defined
Store passwords using reversible encryption Disabled
Type here to search
7:17 PM
8/1/2025

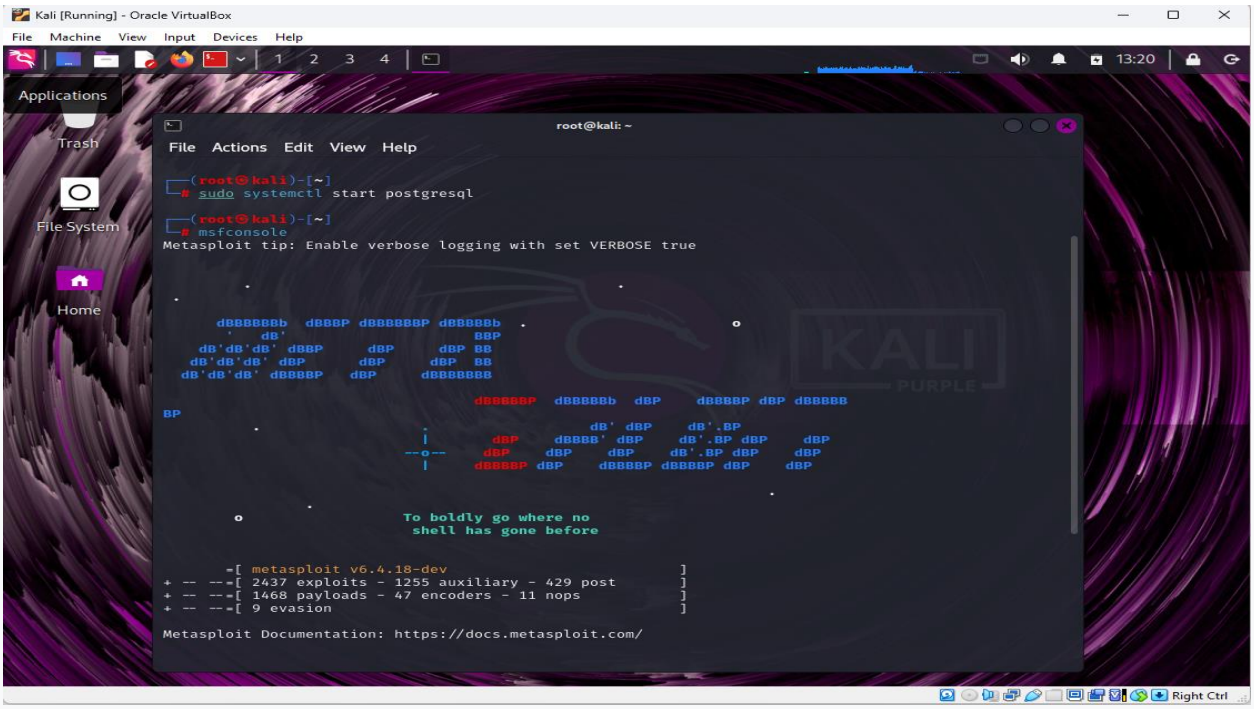
4. Ubuntu



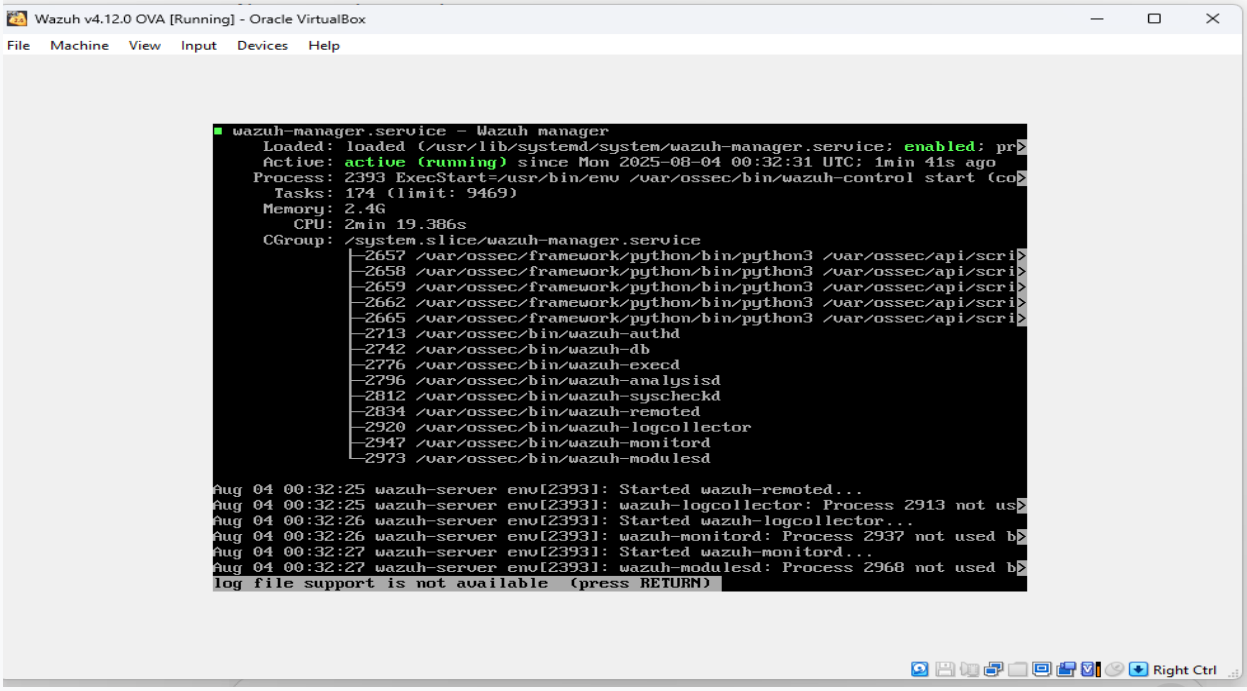
5. Centos

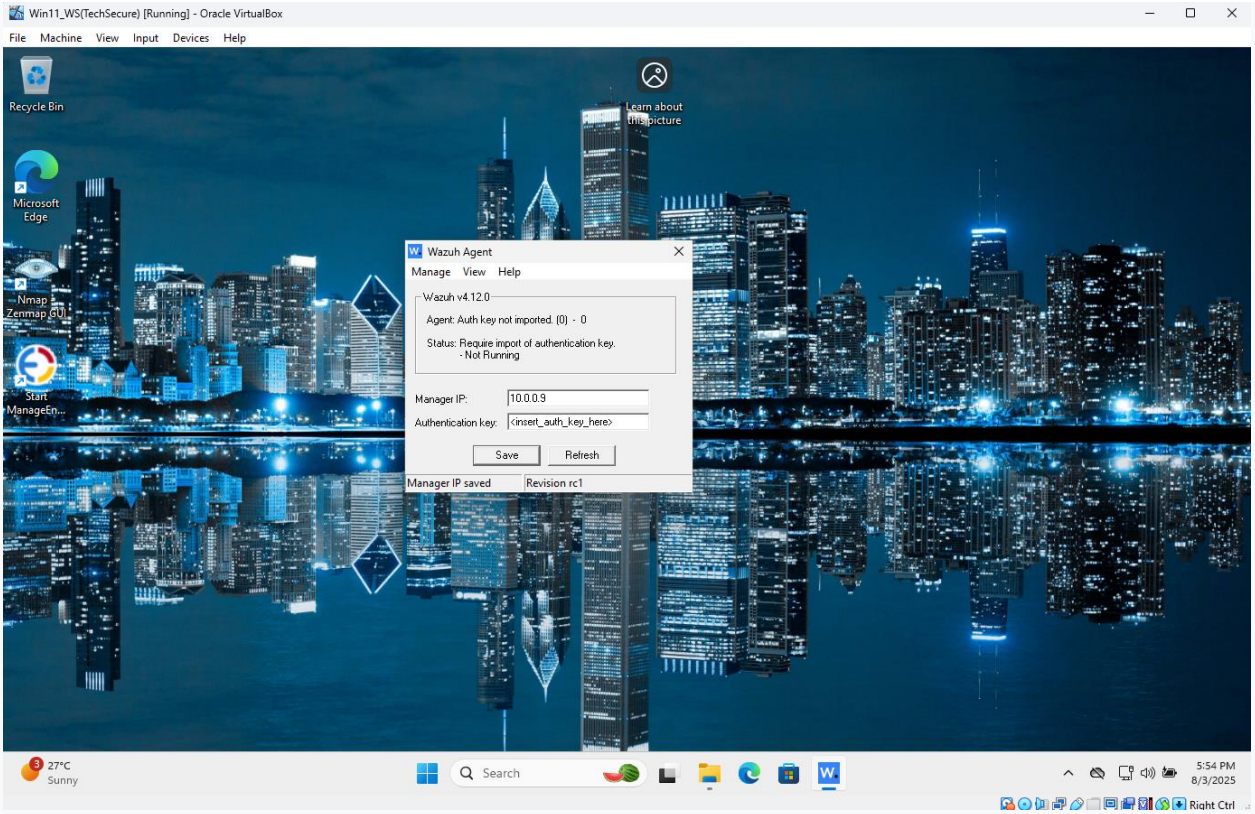


6. Kali


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications
Trash
File System
Home
root@kali: ~
File Actions Edit View Help
sudo systemctl start postgresql
msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true
To boldly go where no
shell has gone before
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
Right Ctrl

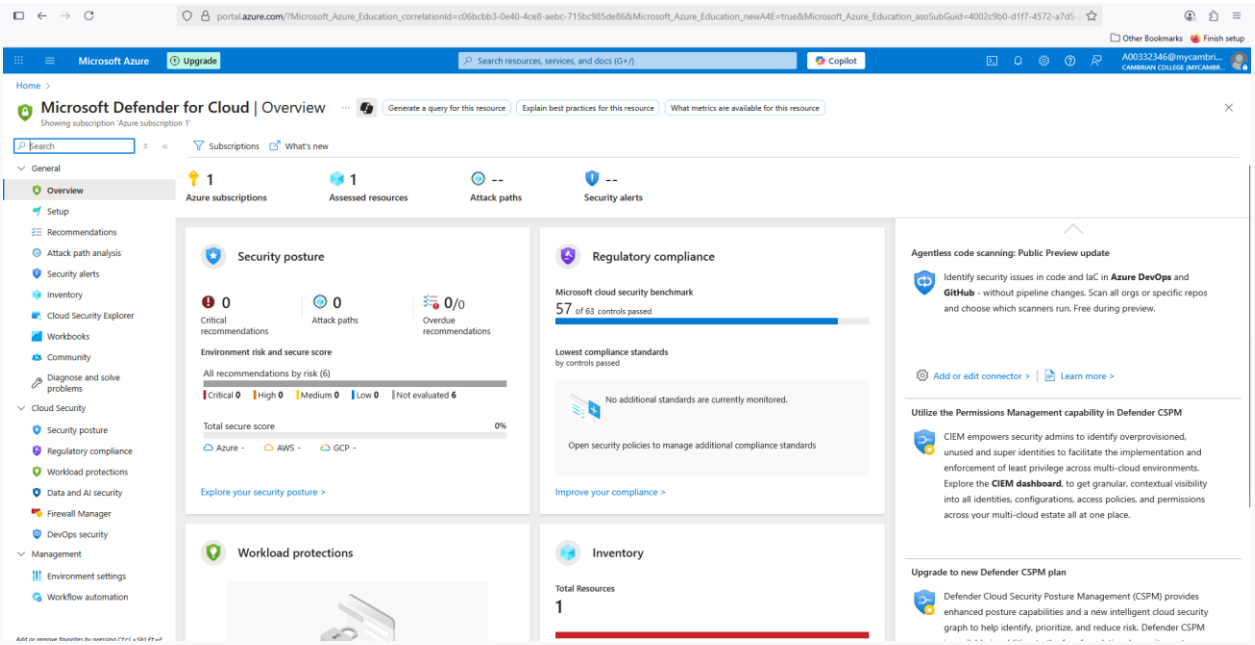
7. Wazuh

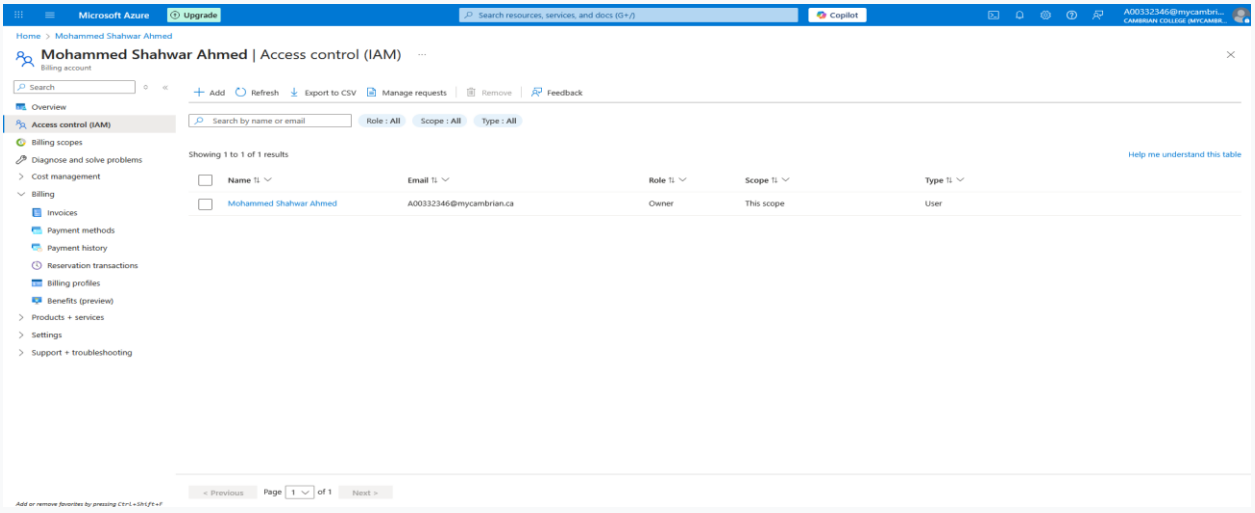

Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
wazuh-manager.service - Wazuh manager
Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; pr>
Active: active (running) since Mon 2025-08-04 00:32:31 UTC; 1min 41s ago
Process: 2393 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (co>
Tasks: 174 (limit: 9469)
Memory: 2.4G
CPU: 2min 19.386s
CGroup: /system.slice/wazuh-manager.service
├─2657 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri>
├─2658 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri>
├─2659 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri>
├─2662 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri>
├─2665 /var/ossec/framework/python/bin/python3 /var/ossec/api/scri>
├─2713 /var/ossec/bin/wazuh-authd
├─2742 /var/ossec/bin/wazuh-db
├─2776 /var/ossec/bin/wazuh-execd
├─2796 /var/ossec/bin/wazuh-analysisd
├─2812 /var/ossec/bin/wazuh-syscheckd
├─2834 /var/ossec/bin/wazuh-remoted
├─2920 /var/ossec/bin/wazuh-logcollector
├─2947 /var/ossec/bin/wazuh-monitord
└─2973 /var/ossec/bin/wazuh-modulesd
Aug 04 00:32:25 wazuh-server env[2393]: Started wazuh-remoted...
Aug 04 00:32:25 wazuh-server env[2393]: wazuh-logcollector: Process 2913 not us>
Aug 04 00:32:26 wazuh-server env[2393]: Started wazuh-logcollector...
Aug 04 00:32:26 wazuh-server env[2393]: wazuh-monitord: Process 2937 not used b>
Aug 04 00:32:27 wazuh-server env[2393]: Started wazuh-monitord...
Aug 04 00:32:27 wazuh-server env[2393]: wazuh-modulesd: Process 2968 not used b>
log file support is not available (press RETURN)
Right Ctrl


Win11_WS(TechSecure) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Learn about this picture
Microsoft Edge
Nmap - Zenmap GUI
Start ManageEn...
Wazuh Agent
Manage View Help
Wazuh v4.12.0
Agent: Auth key not imported. (0) - 0
Status: Require import of authentication key.
- Not Running
Manager IP: 10.0.0.9
Authentication key: <insert_auth_key_here>
Save
Refresh
Manager IP saved
Revision rc1
27°C
Sunny
Search
5:54 PM
8/3/2025
Right Ctrl

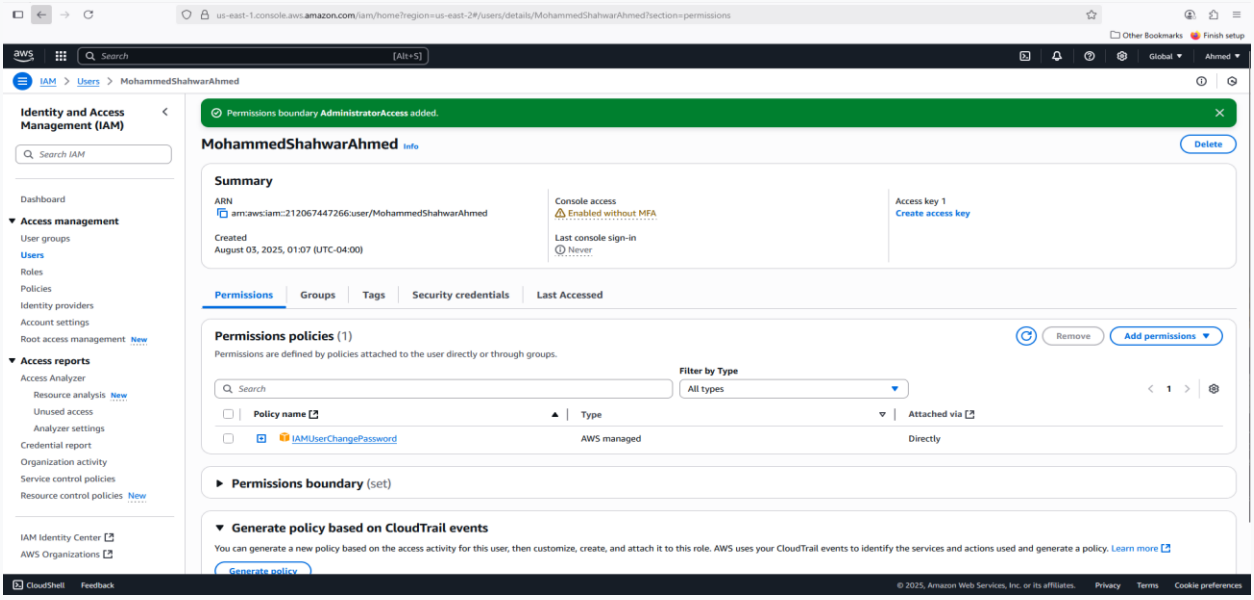
Task 2: Hardening Cloud Instances

1. Azure

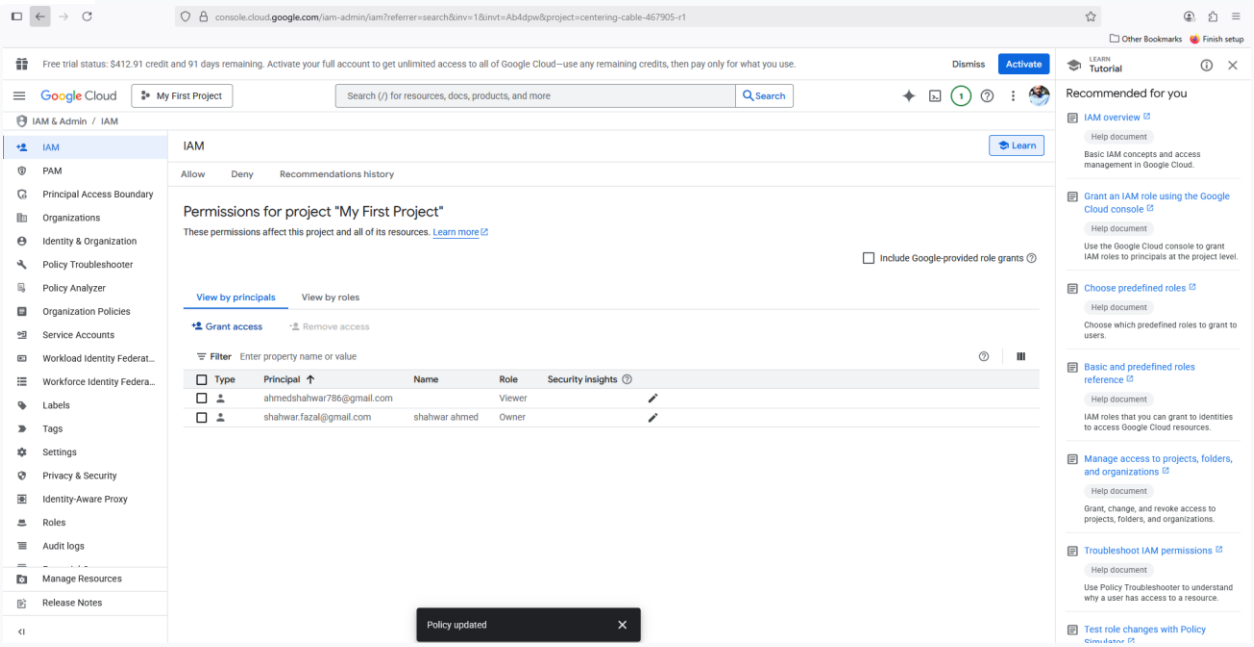




2. AWS

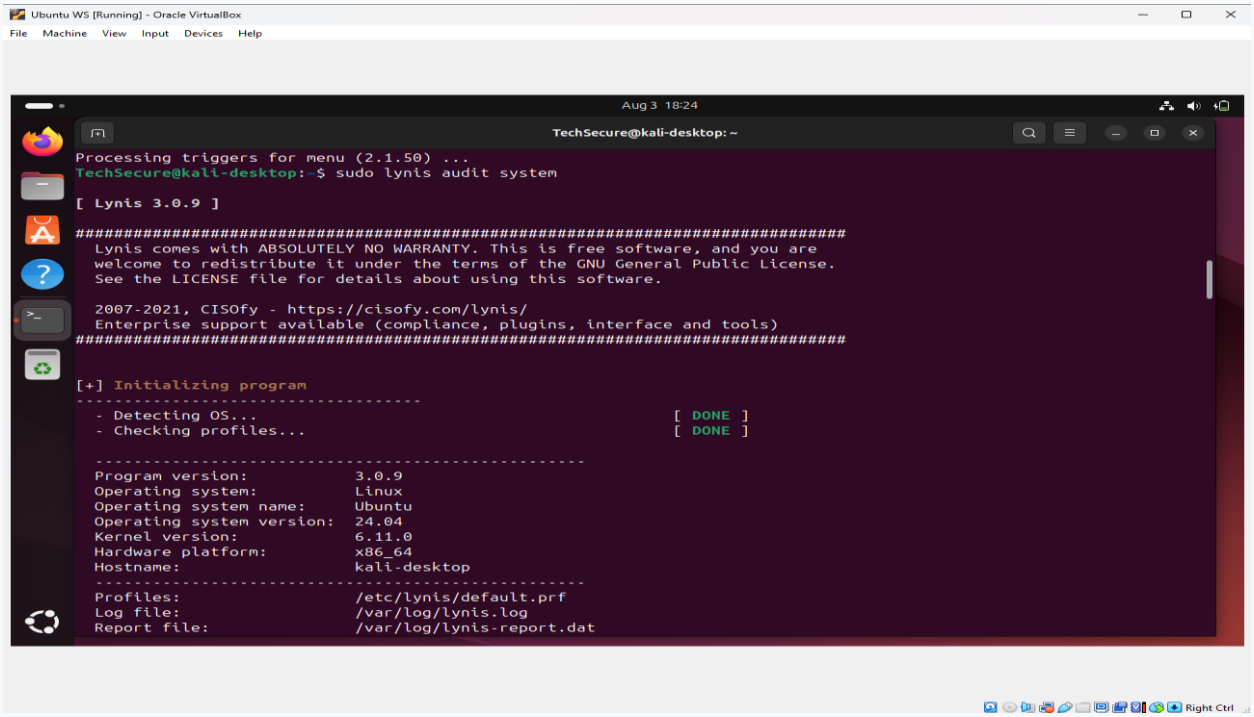

Permissions boundary AdministratorAccess added.
MohammedShahwarAhmed
Delete
Summary
ARN
arn:aws:iam::212067447266:user/MohammedShahwarAhmed
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2025, 01:07 (UTC-04:00)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached via
IAMUserChangePassword
AWS managed
Directly
Permissions boundary (set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy

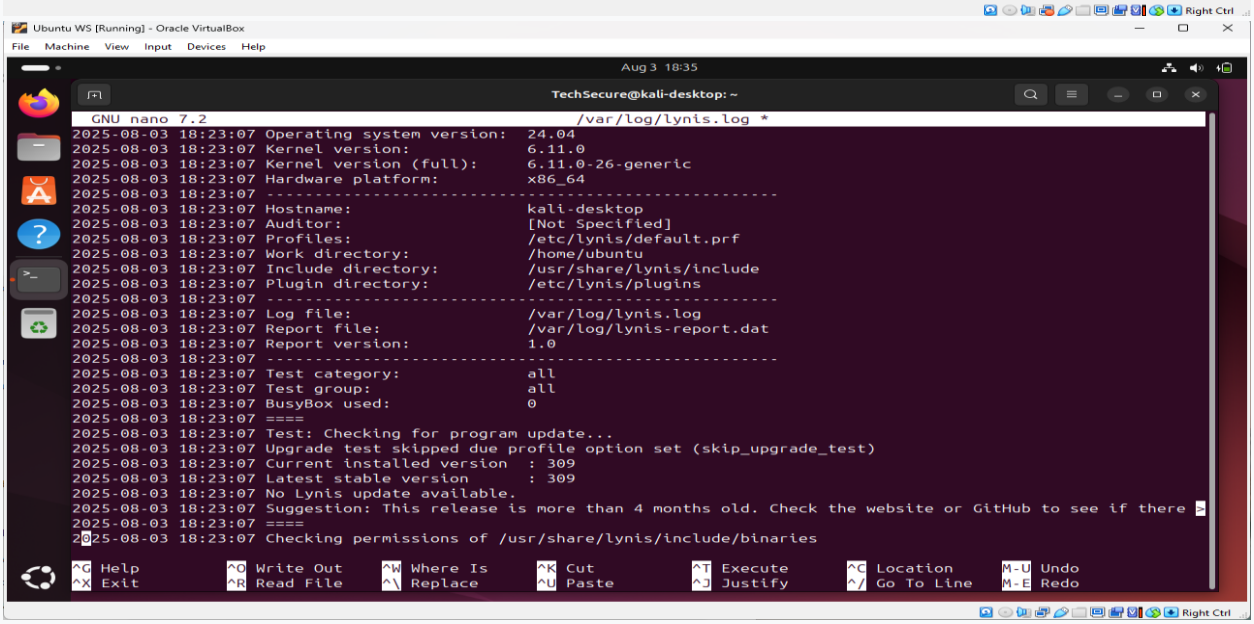
3. GCP

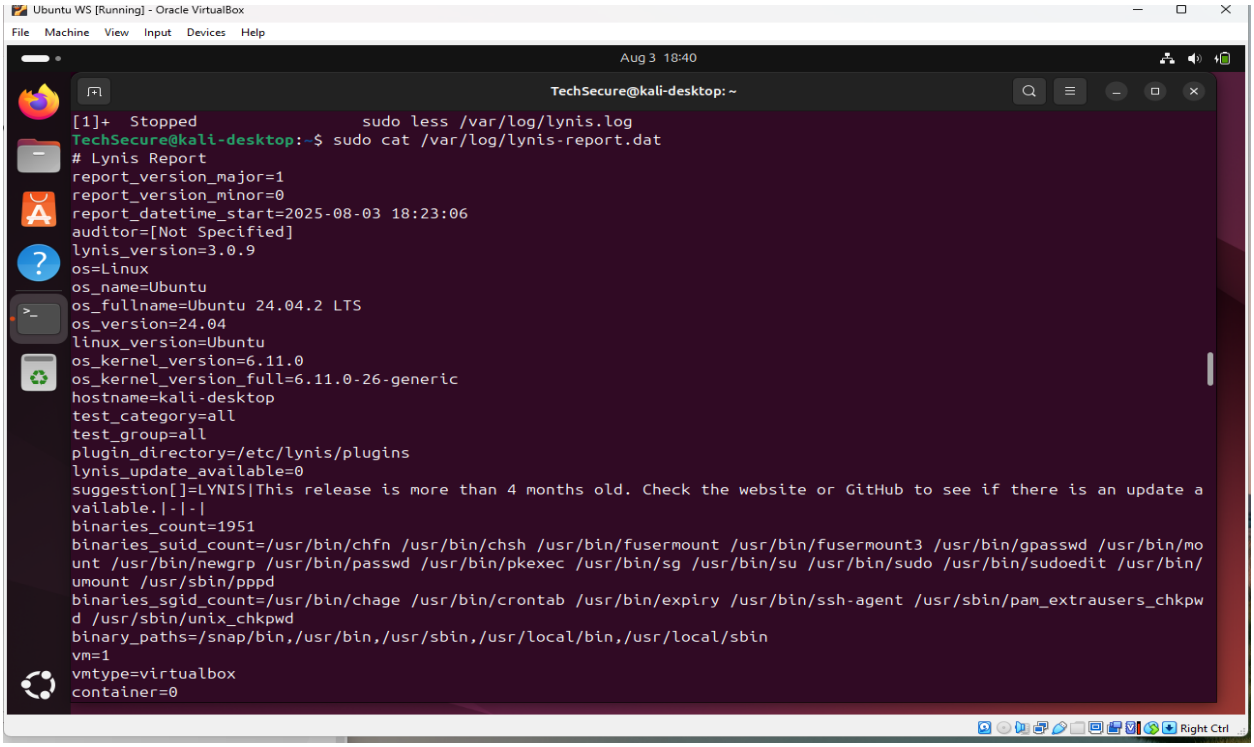

Free trial status: $412.91 credit and 91 days remaining. Activate your full account to get unlimited access to all of Google Cloud—use any remaining credits, then pay only for what you use.
Dismiss
Activate
Google Cloud
My First Project
Search (/) for resources, docs, products, and more
IAM & Admin / IAM
IAM
Learn
Allow
Deny
Recommendations history
Permissions for project "My First Project"
These permissions affect this project and all of its resources. Learn more
Include Google-provided role grants
View by principals
View by roles
Grant access
Remove access
Filter
Enter property name or value
Type
Principal
Name
Role
Security insights
ahmedshahwar786@gmail.com
Viewer
shahwar.fazal@gmail.com
shahwar ahmed
Owner
Policy updated
Recommended for you
IAM overview
Grant an IAM role using the Google Cloud console
Choose predefined roles
Basic and predefined roles reference
Manage access to projects, folders, and organizations
Troubleshoot IAM permissions

Task 3: Security Auditing and Reporting

1. Local VMs







Document findings and provide remediation steps.

Finding	Description	Remediation
Outdated Lynis version	`lynis_version=3.0.9`, and the suggestion states: "This release is more than 4 months old."	**Update Lynis:** Run: `sudo apt update && sudo apt upgrade lynis`
Multiple SUID/SGID binaries	High number of SUID (`/usr/bin/chsh`, `/usr/bin/passwd`, `/usr/bin/sudo`, etc.) and SGID binaries (`/usr/bin/crontab`, `/usr/bin/ssh-agent`, etc.)	**Audit binaries:** Run: `find / -perm /6000 -type f -exec ls -l {} +` Remove SUID/SGID bits where not needed.
Running in a VM (VirtualBox)	`vmtype=virtualbox` – Lynis notes that you're running in a virtualized environment.	**No immediate remediation needed**, but be aware of VM-specific risks. Disable unused virtual interfaces and guest tools if not required.

OS Kernel Info	Ubuntu 24.04.2 LTS running kernel `6.11.0-26-generic`	Keep kernel and OS fully patched: Run: `sudo apt update && sudo apt full-upgrade` Also enable unattended upgrades if not already: `sudo apt install unattended upgrades.`

2. Cloud Instances

Azure

Findings:

- Multi-Factor Authentication (MFA) was not enabled for all users.
- Network Security Groups (NSGs) had open inbound rules allowing traffic from any IP.

Remediations:

- Enabled MFA for all user accounts to prevent unauthorized access.
- Updated NSG rules to restrict access to known and trusted IP addresses only.

AWS

Findings:

- EC2 instances had outdated software and unpatched vulnerabilities.
- IAM users had overly broad permissions (e.g., full access to services).
- CloudTrail was not enabled for auditing activities.

Remediations:

- Performed updates on all EC2 instances using Amazon Inspector findings.

- Created custom IAM policies with least-privilege access (e.g., S3ReadOnly).
- Enabled CloudTrail to log all API activity for accountability.

GCP

Findings:

- Some IAM roles were too permissive (e.g., "Editor" role assigned unnecessarily).
- Virtual Machines had open firewall rules and exposed ports.
- Security Command Center (SCC) was not actively monitoring resources.

Remediations:

- Replaced over-permissive roles with specific ones like Viewer.
- Closed unused ports and removed external IPs from VMs.
- Activated Security Command Center to track risks and misconfigurations.

Summary Report

1. Installing and configuring endpoint protection tools.
2. Performing vulnerability scans using tools like Lynis and Amazon Inspector.
3. Monitoring systems using Wazuh Manager and Agents.
4. Implementing cloud security best practices using Azure Security Center, AWS IAM & CloudTrail, and GCP Security Command Center.
5. Documenting all findings and remediation steps.

Security Measures Implemented

On Local Virtual Machines (Opsense,Windows 11,Windows 2022 server,Kali, Ubuntu, CentOS, etc.)

- Installed Wazuh agents on all VMs to centralize monitoring with the Wazuh Manager.
- Performed Lynis security audits to assess system hardening levels.
- Identified and reviewed SUID/SGID binaries that may pose privilege escalation risks.
- Set SELinux to enforcing mode on CentOS and configured UFW.Firewalld as host firewalls.
- Ensured that password policies were strong .
- Enabled logon auditing and account lockout policies via secpol.msc on Windows VMs.

On Cloud Platforms

Azure

- Logged into the Azure portal and accessed Microsoft Defender for Cloud.
- Reviewed and confirmed implementation of high/medium level recommendations.
- Verified MFA was enabled.
- Created custom IAM roles with limited permissions to follow least privilege access.

AWS

- Accessed IAM console to create users with S3ReadOnly or limited access policies.
- Enabled AWS CloudTrail for auditing user activity and logging events.
- Removed billing and credit card information after the lab for safety.

GCP

- Logged into GCP Console, configured IAM roles, and assigned viewer/custom roles.
- Enabled Security Command Center to detect and review findings.
- Deleted GCP project and removed credit card details to avoid charges after completion.

Audit Findings and Remediation Steps

Platform	Findings	Remediation Steps
Lynis	- Outdated audit tool version - SUID/SGID binaries found	- Updated Lynis - Analyzed and removed risky binaries
Wazuh	- Some agents not reporting initially	- Reconfigured agent IP to point to Wazuh Manager - Restarted Wazuh agent service
Azure	- No critical vulnerabilities found	- Verified recommendations are met - Ensured MFA and secure IAM practices
AWS	- No critical findings via Amazon Inspector	- Reviewed IAM roles and enforced least privilege - Enabled CloudTrail
GCP	- IAM had overly permissive roles	- Reassigned viewer roles - Reviewed security findings in SCC