

Week 12 - Enterprise Network Security

Task 1: Hardening Local VMs

1. OPNSense Router

The screenshot shows the OPNSense web interface running in a browser. The page title is "Firewall: Rules: LAN". A message at the top states "The changes have been applied successfully." Below this is a table of firewall rules. The table has columns for Protocol, Source, Port, Destination, Port, Gateway, Schedule, and Description. There are four rules listed: "Allow DNS", "Allow HTTP", "Allow HTTPS", and "Block all other LAN traffic". The "Block all other LAN traffic" rule is highlighted in red. Below the table, there are sections for "Active/Inactive Schedule (click to view/edit)", "Alias (click to view/edit)", and a note about rule evaluation: "LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default."

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
<i>Automatically generated rules</i>								
<input type="checkbox"/>	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	*	Allow DNS
<input type="checkbox"/>	IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	*	Allow HTTP
<input type="checkbox"/>	IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	*	Allow HTTPS
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	*	Block all other LAN traffic

pass (disabled) block (disabled) reject (disabled) log (disabled) in out first match last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

2. Windows 11

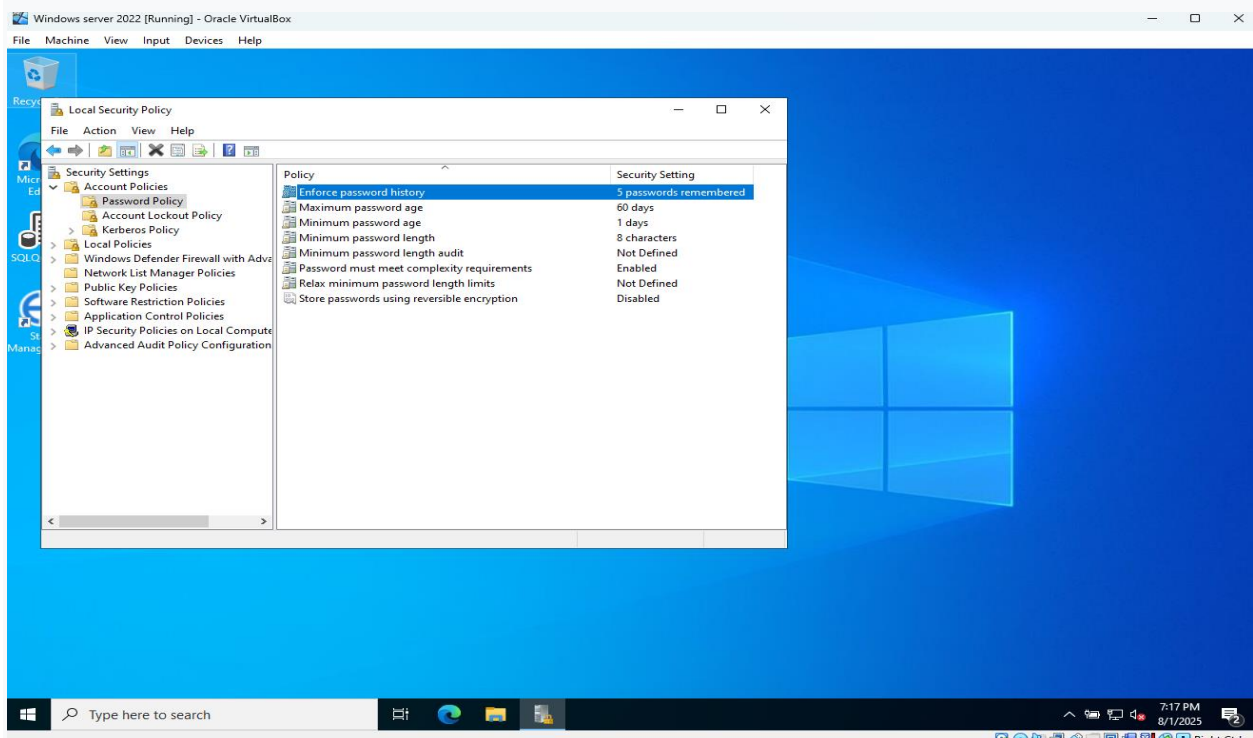
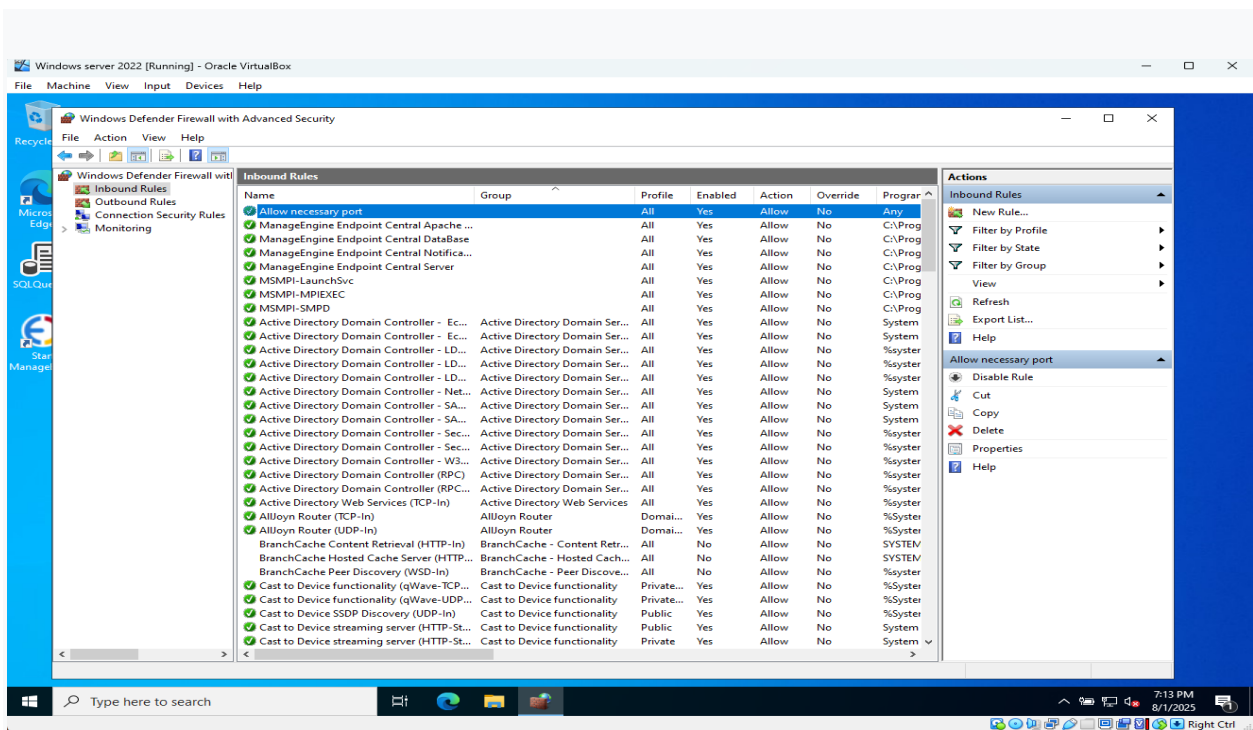
The screenshot shows the Windows 11 desktop environment with the Local Group Policy Editor open. The left pane displays the tree structure, and the right pane shows the 'Windows Installer' settings. The 'Turn off Windows Installer' policy is highlighted, showing its state as 'Enabled'.

Setting	State	Comment
Allow users to browse for source while elevated	Not configured	No
Allow users to use media source while elevated	Not configured	No
Allow users to patch elevated products	Not configured	No
Always install with elevated privileges	Not configured	No
Prohibit use of Restart Manager	Not configured	No
Remove browse dialog box for new source	Not configured	No
Prohibit flyweight patching	Not configured	No
Turn off logging via package settings	Not configured	No
Turn off Windows Installer	Enabled	No
Prevent users from using Windows Installer to install update...	Not configured	No
Prohibit rollback	Not configured	No
Turn off shared components	Not configured	No
Allow user control over installs	Not configured	No
Specify the types of events Windows Installer records in its tr...	Not configured	No
Prohibit non-administrators from applying vendor signed u...	Not configured	No
Prohibit removal of updates	Not configured	No
Turn off creation of System Restore checkpoints	Not configured	No
Prohibit User installs	Not configured	No
Enforce upgrade component rules	Not configured	No
Control maximum size of baseline file cache	Not configured	No
Prevent embedded UI	Not configured	No
Prevent Internet Explorer security prompt for Windows insta...	Not configured	No
Save copies of transform files in a secure location on work...	Not configured	No

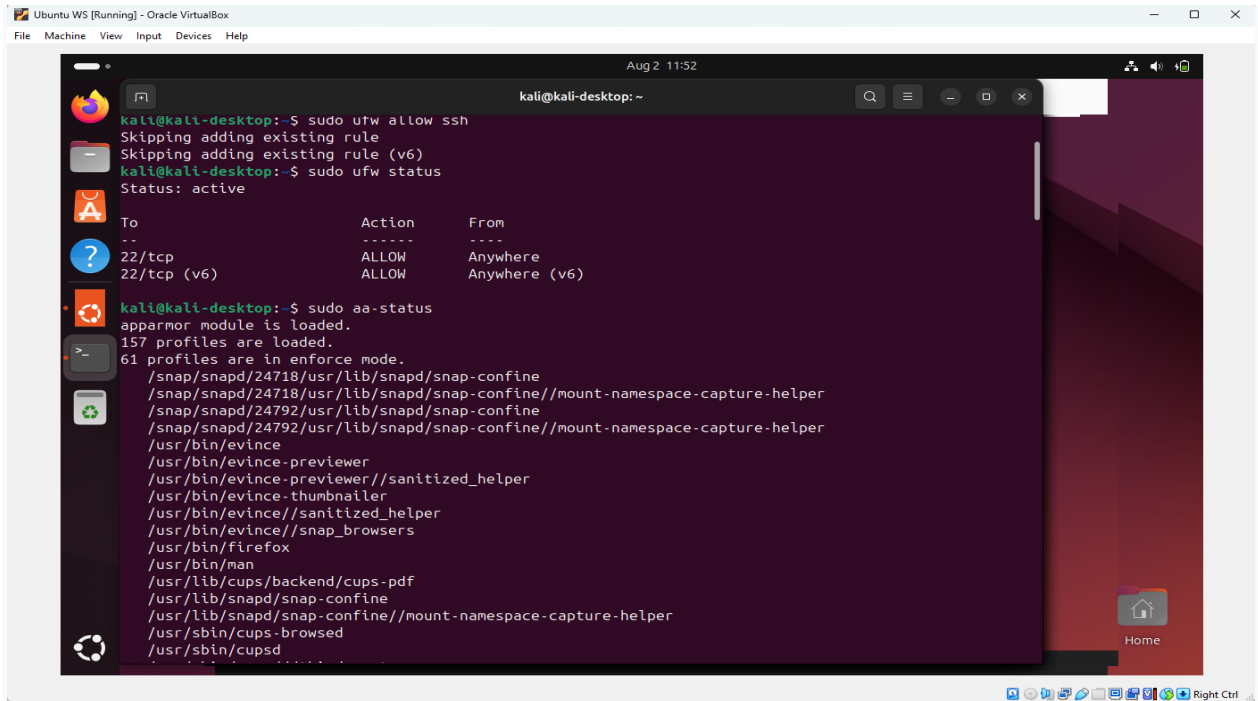
The screenshot also shows the Windows 11 desktop environment with the Local Group Policy Editor open. The left pane displays the tree structure, and the right pane shows the 'Audit Logon' settings. The 'Audit Logon' policy is highlighted, showing its state as 'Success and Failure'.

Subcategory	Audit Events
Audit Access Rights	Not Configured
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

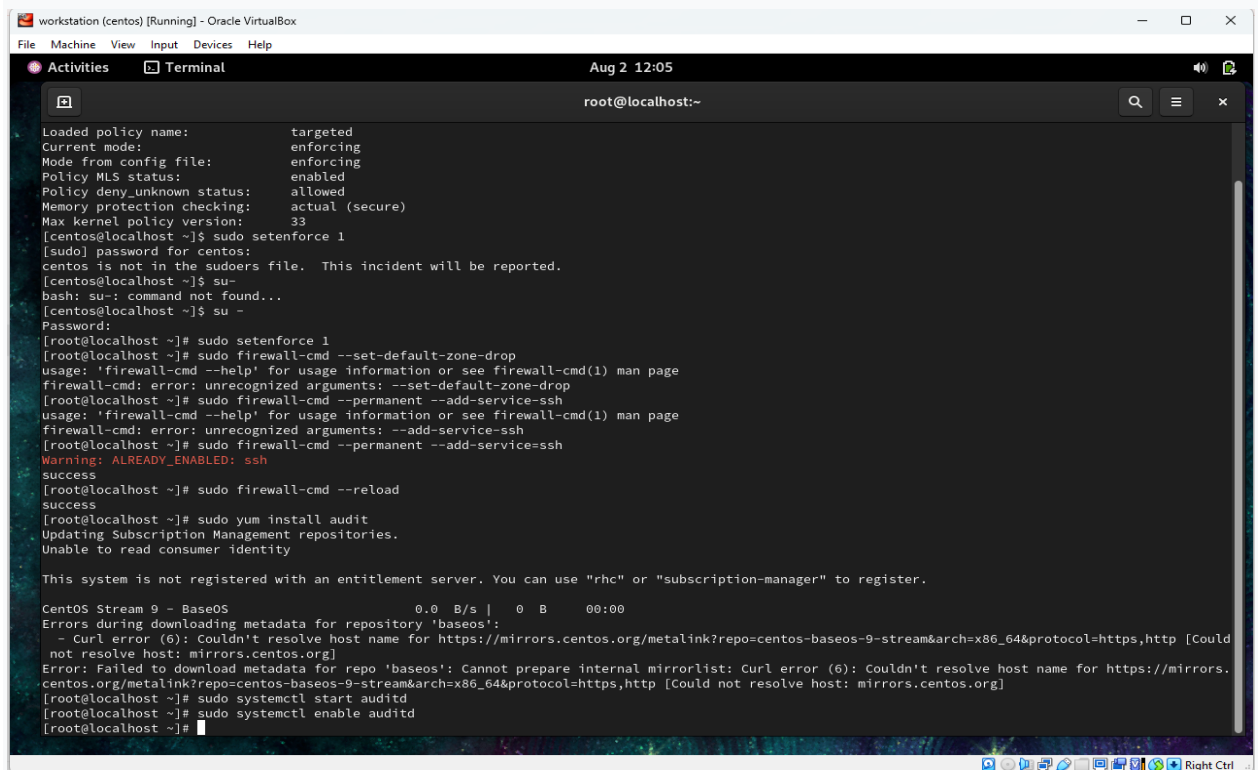
3. Windows Server 2022



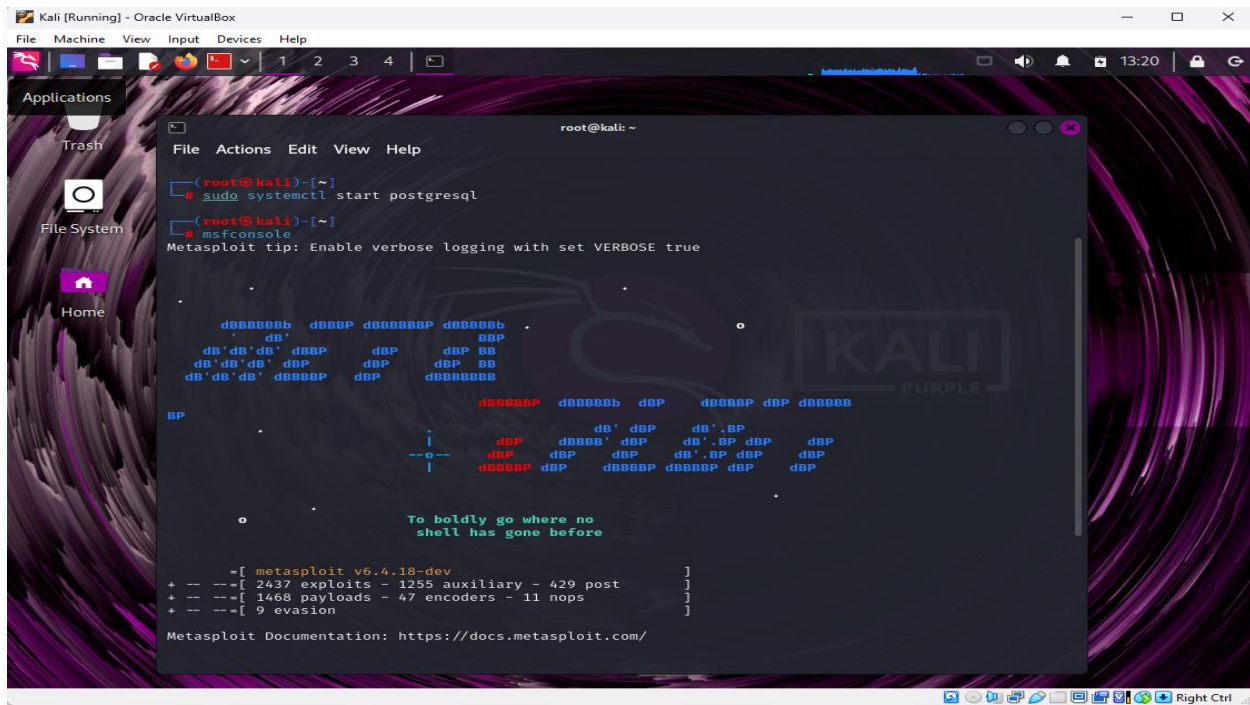
4. Ubuntu



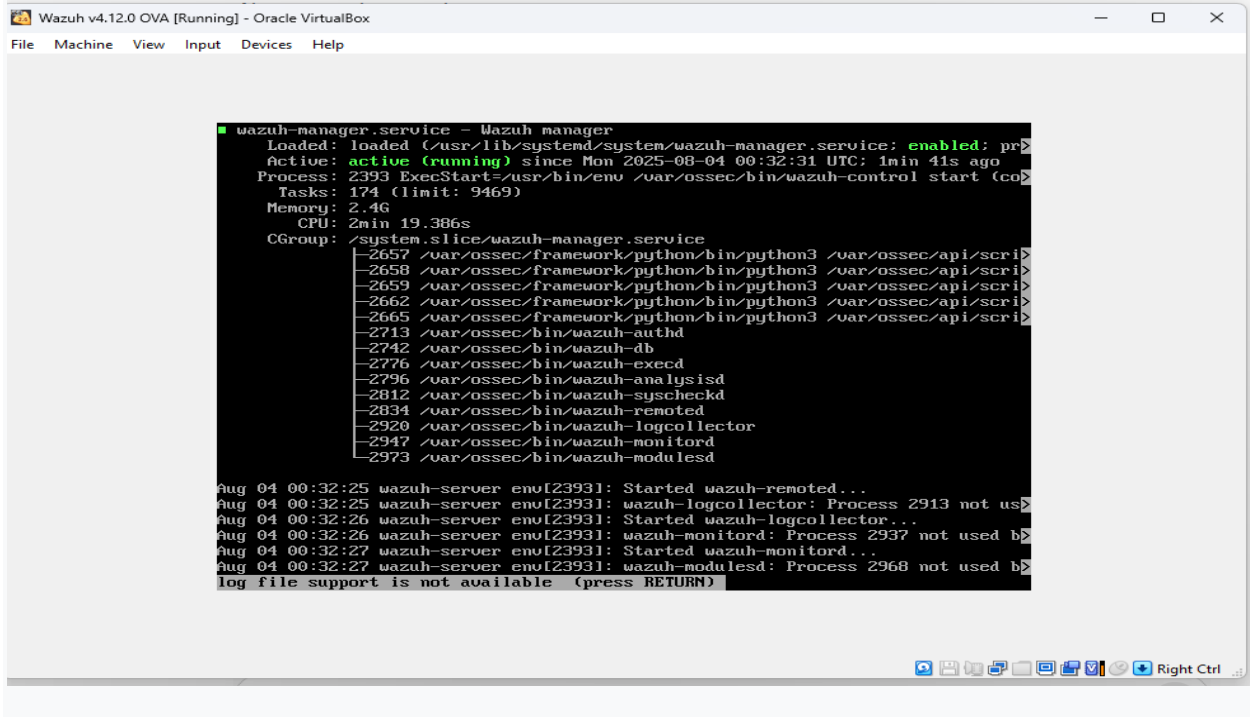
5. Centos

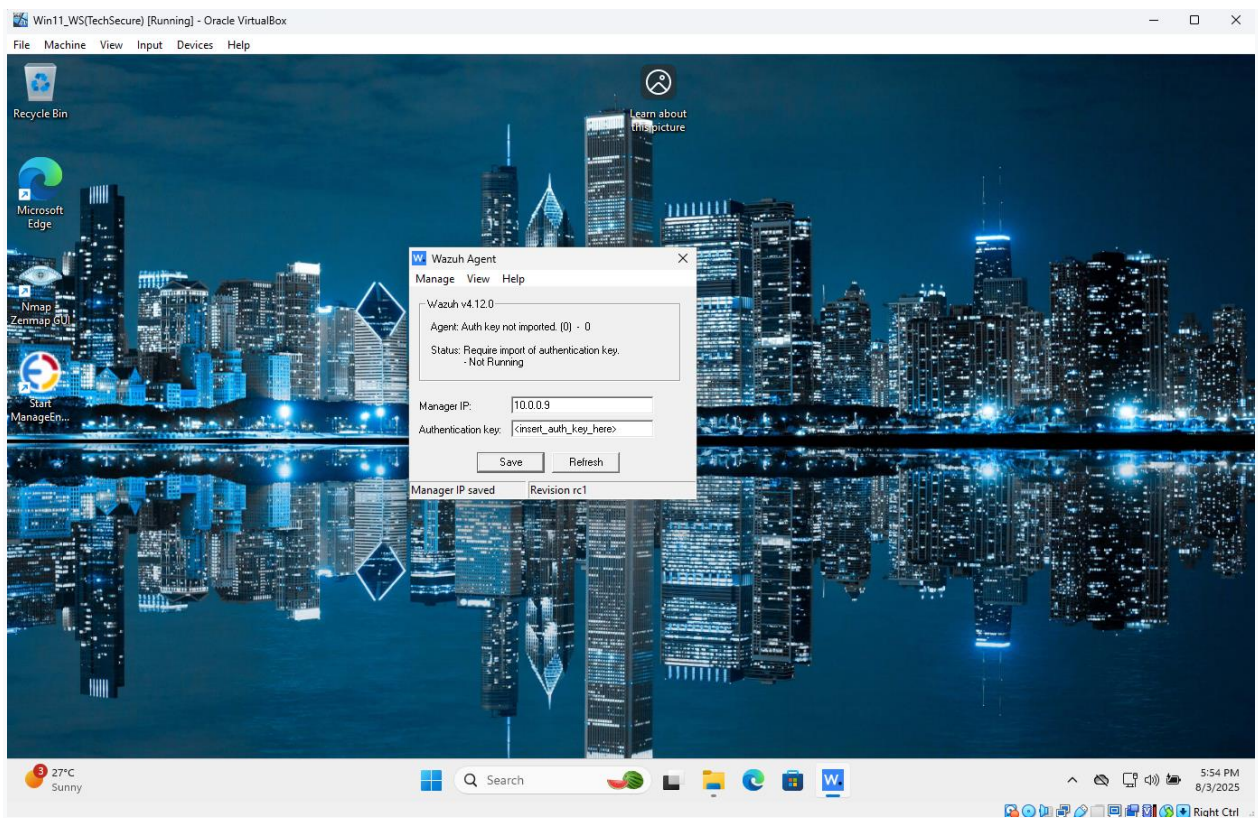


6. Kali



7. Wazuh





Task 2: Hardening Cloud Instances

1. Azure

The image displays two screenshots of the Microsoft Azure portal. The top screenshot shows the 'Microsoft Defender for Cloud | Overview' page. The bottom screenshot shows the 'Access control (IAM)' page for the user 'Mohammed Shahwar Ahmed'.

Microsoft Defender for Cloud | Overview

Showing subscription 'Azure subscription 1'

Search resources, services, and docs (G+7)

Home > Microsoft Defender for Cloud | Overview

Subscriptions: 1, Assessed resources: 1, Attack paths: --, Security alerts: --

Security posture

Critical recommendations: 0, Attack paths: 0, Overdue recommendations: 0/0

Environment risk and secure score

All recommendations by risk (6)

Critical 0, High 0, Medium 0, Low 0, Not evaluated 6

Total secure score: 0%

Azure, AWS, GCP

Regulatory compliance

Microsoft cloud security benchmark

57 of 63 controls passed

Lowest compliance standards by controls passed

No additional standards are currently monitored.

Open security policies to manage additional compliance standards

Agentless code scanning: Public Preview update

Identify security issues in code and IaC in **Azure DevOps** and **GitHub** - without pipeline changes. Scan all orgs or specific repos and choose which scanners run. Free during preview.

Utilize the Permissions Management capability in Defender CSPM

CIEM empowers security admins to identify overprovisioned, unused and super identities to facilitate the implementation and enforcement of least privilege across multi-cloud environments. Explore the **CIEM dashboard**, to get granular, contextual visibility into all identities, configurations, access policies, and permissions across your multi-cloud estate all at one place.

Upgrade to new Defender CSPM plan

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM

Workload protections

Inventory

Total Resources: 1

Access control (IAM)

Home > Mohammed Shahwar Ahmed

Billing account

Search by name or email

Role: All, Scope: All, Type: All

Showing 1 of 1 results

Name	Email	Role	Scope	Type
Mohammed Shahwar Ahmed	A00332346@mycambrian.ca	Owner	This scope	User

Page 1 of 1

2. AWS

The screenshot shows the AWS IAM console for user MohammedShahwarAhmed. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, IAM Identity Center, and AWS Organizations. The main content area displays the user's summary, including their ARN, console access status (Enabled without MFA), and last console sign-in. Below the summary, there are tabs for Permissions, Groups, Tags, Security credentials, and Last Accessed. The Permissions tab is active, showing a list of permissions policies (1) and a permissions boundary. A green banner at the top indicates that the permissions boundary AdministratorAccess has been added.

Summary

ARN: `arn:aws:iam::212067447266:user/MohammedShahwarAhmed`

Console access: Enabled without MFA

Last console sign-in: Never

Access key 1: Create access key

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name	Type	Attached via
<code>iam:UserChangePassword</code>	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

The screenshot shows the Google Cloud IAM console for project "My First Project". The left sidebar contains navigation links for IAM & Admin, IAM, PAM, Principal Access Boundary, Organizations, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federat..., Workforce Identity Federat..., Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit logs, Manage Resources, and Release Notes. The main content area displays the permissions for project "My First Project", including a table of principals and their roles. A "Policy updated" notification is visible at the bottom.

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
<input type="checkbox"/>	ahmedshahwar786@gmail.com		Viewer	
<input type="checkbox"/>	shahwar.fazal@gmail.com	shahwar ahmed	Owner	

Policy updated

Task 3: Security Auditing and Reporting

1. Local VMs

```
Ubuntu WS [Running] - Oracle VirtualBox
File Machine View Input Devices Help

TechSecure@kali-desktop: ~
Aug 3 18:24

Processing triggers for menu (2.1.50) ...
TechSecure@kali-desktop:~$ sudo lynis audit system

[ Lynis 3.0.9 ]

#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
-----

Program version:      3.0.9
Operating system:     Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version:       6.11.0
Hardware platform:    x86_64
Hostname:             kali-desktop
-----
Profiles:             /etc/lynis/default.prf
Log file:             /var/log/lynis.log
Report file:          /var/log/lynis-report.dat
```

```
Ubuntu WS [Running] - Oracle VirtualBox
File Machine View Input Devices Help

TechSecure@kali-desktop: ~
Aug 3 18:35

GNU nano 7.2 /var/log/lynis.log *
2025-08-03 18:23:07 Operating system version: 24.04
2025-08-03 18:23:07 Kernel version: 6.11.0
2025-08-03 18:23:07 Kernel version (full): 6.11.0-26-generic
2025-08-03 18:23:07 Hardware platform: x86_64
2025-08-03 18:23:07 -----
2025-08-03 18:23:07 Hostname: kali-desktop
2025-08-03 18:23:07 Auditor: [Not Specified]
2025-08-03 18:23:07 Profiles: /etc/lynis/default.prf
2025-08-03 18:23:07 Work directory: /home/ubuntu
2025-08-03 18:23:07 Include directory: /usr/share/lynis/include
2025-08-03 18:23:07 Plugin directory: /etc/lynis/plugins
2025-08-03 18:23:07 -----
2025-08-03 18:23:07 Log file: /var/log/lynis.log
2025-08-03 18:23:07 Report file: /var/log/lynis-report.dat
2025-08-03 18:23:07 Report version: 1.0
2025-08-03 18:23:07 -----
2025-08-03 18:23:07 Test category: all
2025-08-03 18:23:07 Test group: all
2025-08-03 18:23:07 BusyBox used: 0
2025-08-03 18:23:07 ====
2025-08-03 18:23:07 Test: Checking for program update...
2025-08-03 18:23:07 Upgrade test skipped due profile option set (skip_upgrade_test)
2025-08-03 18:23:07 Current installed version : 309
2025-08-03 18:23:07 Latest stable version : 309
2025-08-03 18:23:07 No Lynis update available.
2025-08-03 18:23:07 Suggestion: This release is more than 4 months old. Check the website or GitHub to see if there
2025-08-03 18:23:07 ====
2025-08-03 18:23:07 Checking permissions of /usr/share/lynis/include/binaries

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location ^M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^/_ Go To Line ^M-E Redo
```

```
Ubuntu WS [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Aug 3 18:40
TechSecure@kali-desktop: ~

[1]+  Stopped                  sudo less /var/log/lynis.log
TechSecure@kali-desktop:~$ sudo cat /var/log/lynis-report.dat

# Lynis Report
report_version_major=1
report_version_minor=0
report_datetime_start=2025-08-03 18:23:06
auditor=[Not Specified]
lynis_version=3.0.9
os=Linux
os_name=Ubuntu
os_fullname=Ubuntu 24.04.2 LTS
os_version=24.04
linux_version=Ubuntu
os_kernel_version=6.11.0
os_kernel_version_full=6.11.0-26-generic
hostname=kali-desktop
test_category=all
test_group=all
plugin_directory=/etc/lynis/plugins
lynis_update_available=0
suggestion[0]=LYNIS|This release is more than 4 months old. Check the website or GitHub to see if there is an update available.|-|-|
binaries_count=1951
binaries_suid_count=/usr/bin/chfn /usr/bin/chsh /usr/bin/fusermount /usr/bin/fusermount3 /usr/bin/gpasswd /usr/bin/mount /usr/bin/newgrp /usr/bin/passwd /usr/bin/pkexec /usr/bin/sg /usr/bin/su /usr/bin/sudo /usr/bin/sudoedit /usr/bin/umount /usr/sbin/pppd
binaries_sgid_count=/usr/bin/chage /usr/bin/crontab /usr/bin/expiry /usr/bin/ssh-agent /usr/sbin/pam_extrausers_chkpwd /usr/sbin/unix_chkpwd
binary_paths=/snap/bin,/usr/bin,/usr/sbin,/usr/local/bin,/usr/local/sbin
vm=1
vmtype=virtualbox
container=0
```

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: <code>sudo apt update && sudo apt upgrade lynis</code>
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: <code>find / -perm /6000 -type f -exec ls -l {} +</code> 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: <code>sudo apt update && sudo apt full-upgrade</code> Also enable unattended upgrades if not already: <code>sudo apt install unattended-upgrades.</code>
-----------------------	---	---

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	<ul style="list-style-type: none">- Outdated audit tool version- SUID/SGID binaries found	<ul style="list-style-type: none">- Updated Lynis- Analyzed and removed risky binaries
Wazuh	<ul style="list-style-type: none">- Some agents not reporting initially	<ul style="list-style-type: none">- Reconfigured agent IP to point to Wazuh Manager- Restarted Wazuh agent service
Azure	<ul style="list-style-type: none">- No critical vulnerabilities found	<ul style="list-style-type: none">- Verified recommendations are met- Ensured MFA and secure IAM practices
AWS	<ul style="list-style-type: none">- No critical findings via Amazon Inspector	<ul style="list-style-type: none">- Reviewed IAM roles and enforced least privilege- Enabled CloudTrail
GCP	<ul style="list-style-type: none">- IAM had overly permissive roles	<ul style="list-style-type: none">- Reassigned viewer roles- Reviewed security findings in SCC

