

# Enterprise Network Security

## Task 1: Hardening Local VMs

### 1. OPNSense Router

Win11\_WS(TechSecure) [Running] - Oracle VirtualBox

FileMachineViewInputDevicesHelp

LAN | Rules | Firewall | OPNSense

192.168.1.1/firewall\_rules.php?f=lan

root@OPNsense.localdomain

OPNsense

LobbyReportingSystemInterfacessFirewallAliasesAutomationCategoriesGroupsNATRulesFloatingLANWANShaperSettingsLog FilesDiagnosticsVPNServicesPowerHelp

Firewall: Rules: LAN

Select categoryInspect

The changes have been applied successfully.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
Automatically generated rules								
	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	*	Allow DNS
	IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	*	Allow HTTP
	IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	*	Allow HTTPS
	IPv4 *	LAN net	*	*	*	*	*	Block all other LAN traffic
pass								in
pass (disabled)								out
								log
								log (disabled)
								reject
								reject (disabled)
								block
								block (disabled)
								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.								

OPNsense (c) 2014-2025 Deciso B.V.

21°C Clear

Search

8:45 PM 8/2/2025

## 2. Windows 11

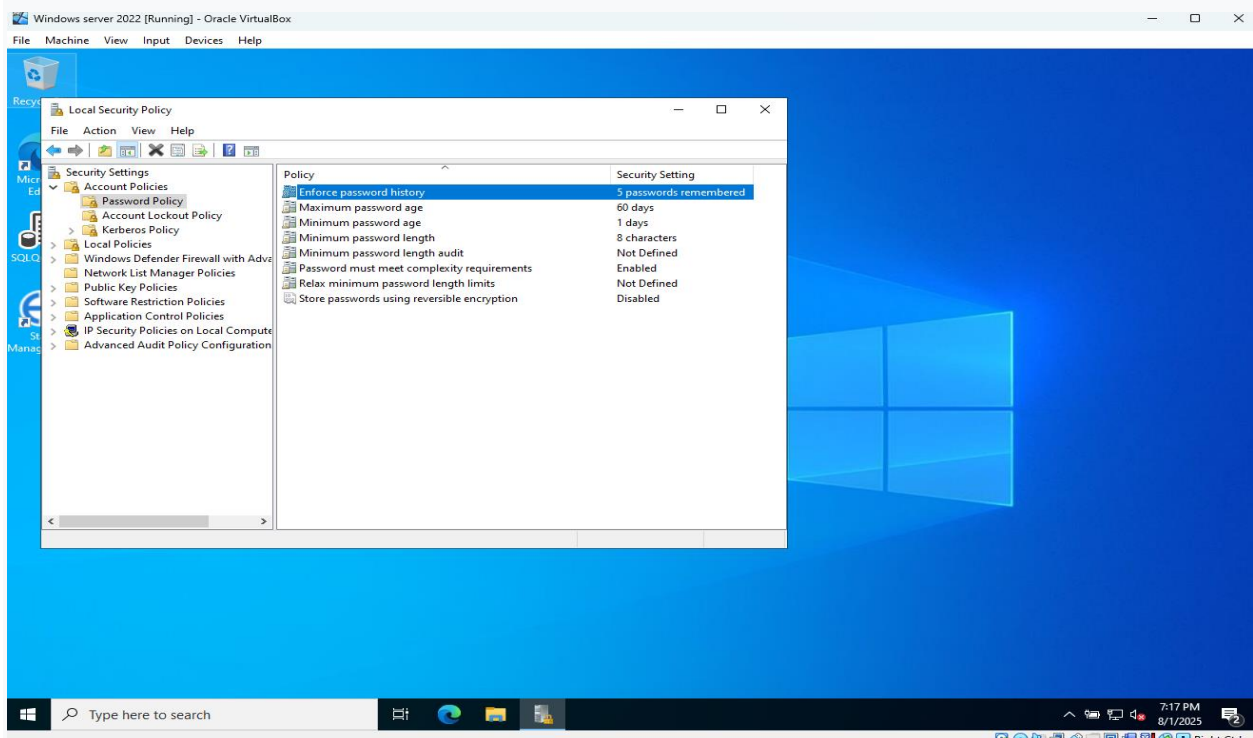
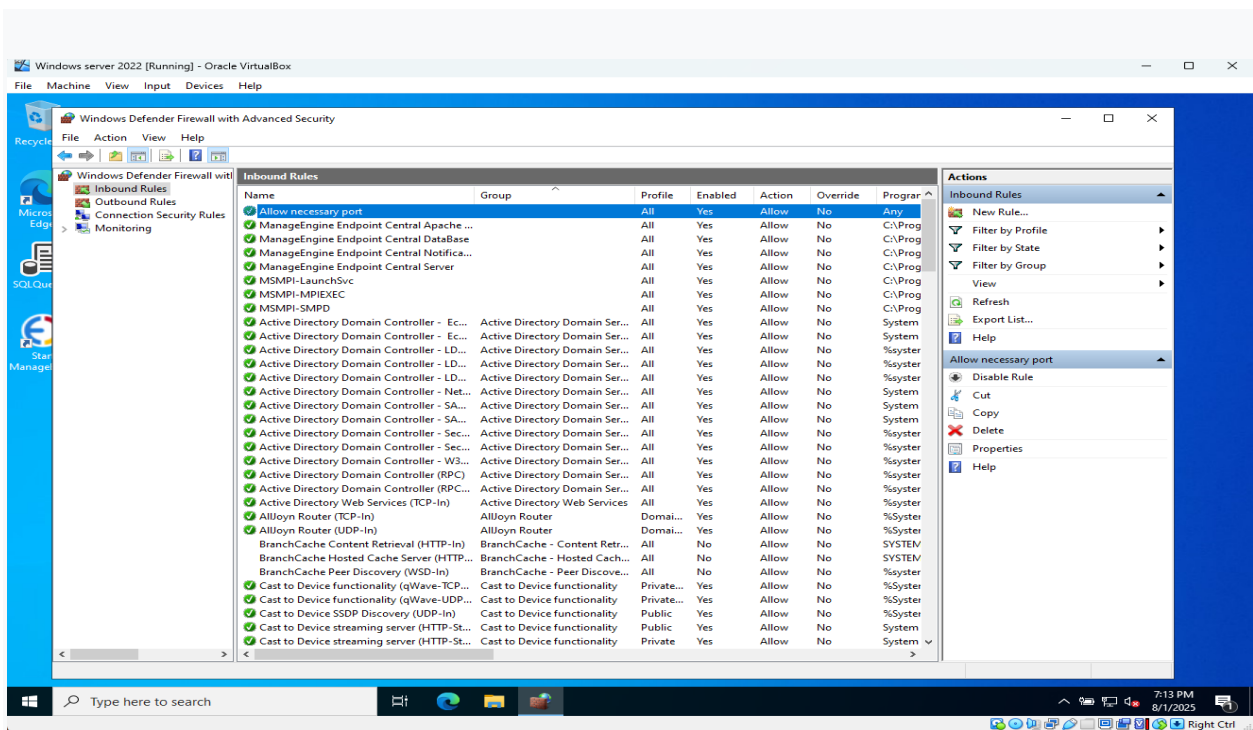
The screenshot displays a Windows 11 desktop environment. The taskbar at the bottom shows the Start button, a search bar, and several pinned applications. The desktop background is a scenic image of a lake and mountains. A window titled 'Win11\_WS(TechSecure) [Running] - Oracle VirtualBox' is open, showing the 'Local Group Policy Editor' application. The 'Local Group Policy Editor' window has a left-hand navigation pane with a tree view showing various policy categories. The main pane is divided into two sections: 'Turn off Windows Installer' and 'Windows Installer'. The 'Turn off Windows Installer' section is currently selected, showing a list of settings. The 'Windows Installer' section is also visible, showing a list of settings. The 'Turn off Windows Installer' section is currently selected, showing a list of settings. The 'Windows Installer' section is also visible, showing a list of settings.

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

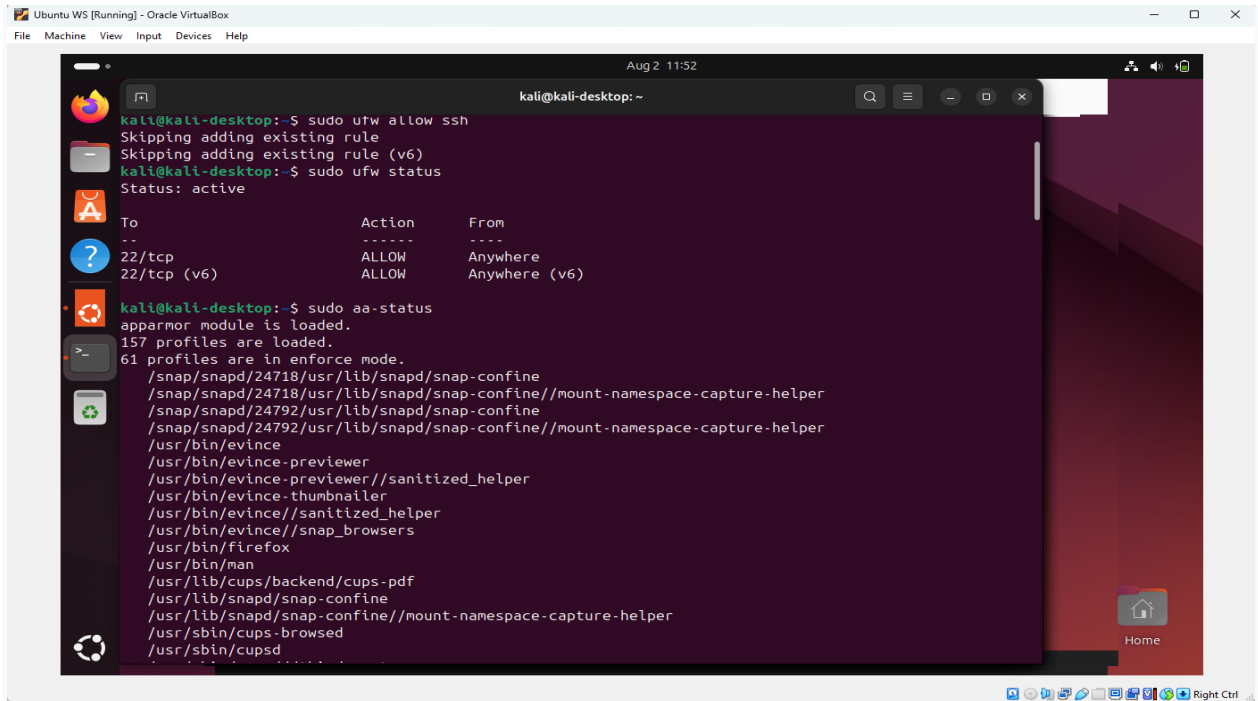
The 'Local Group Policy Editor' window also shows a list of settings under the 'Windows Installer' section. The 'Turn off Windows Installer' section is currently selected, showing a list of settings. The 'Windows Installer' section is also visible, showing a list of settings.

Subcategory	Audit Events
1. Audit Access Rights	Not Configured
2. Audit Account Lockout	Not Configured
3. Audit User / Device Claims	Not Configured
4. Audit Group Membership	Not Configured
5. Audit IPsec Extended Mode	Not Configured
6. Audit IPsec Main Mode	Not Configured
7. Audit IPsec Quick Mode	Not Configured
8. Audit Logoff	Not Configured
9. Audit Logon	Success and Failure
10. Audit Network Policy Server	Not Configured
11. Audit Other Logon/Logoff Events	Not Configured
12. Audit Special Logon	Not Configured

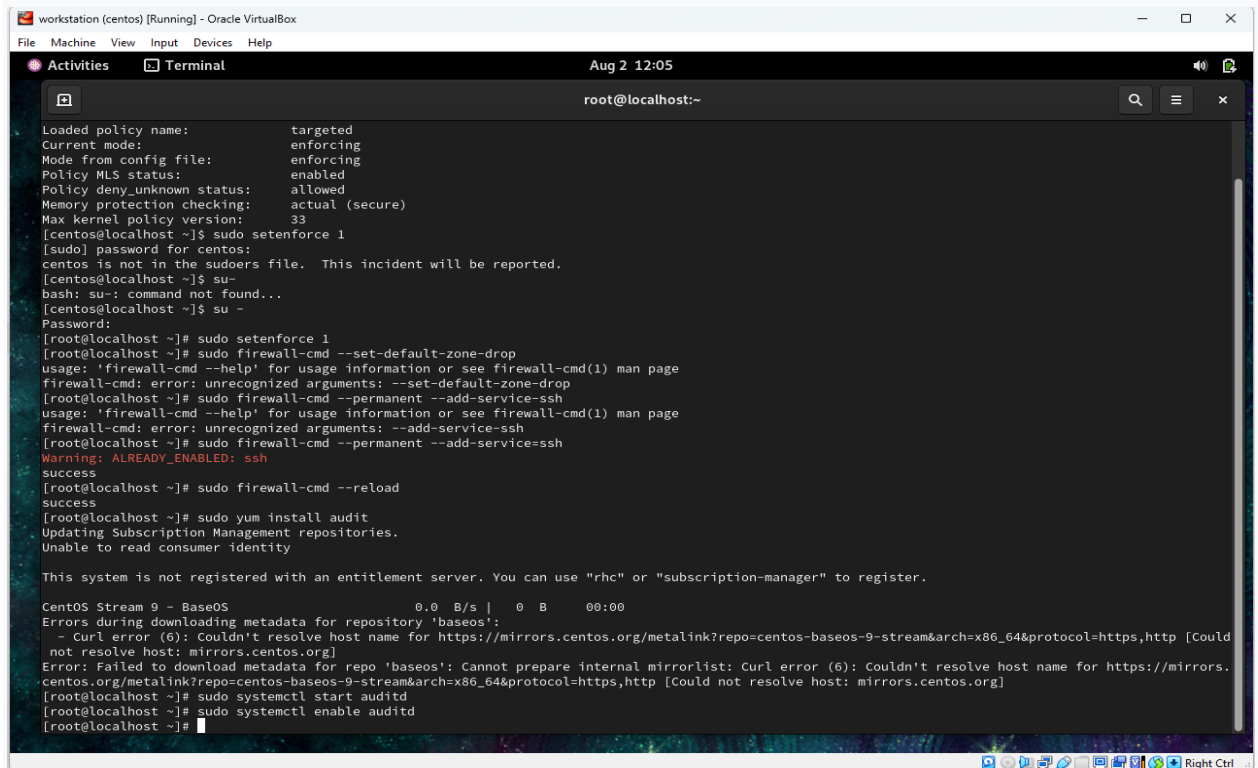
## 3. Windows Server 2022



## 4. Ubuntu



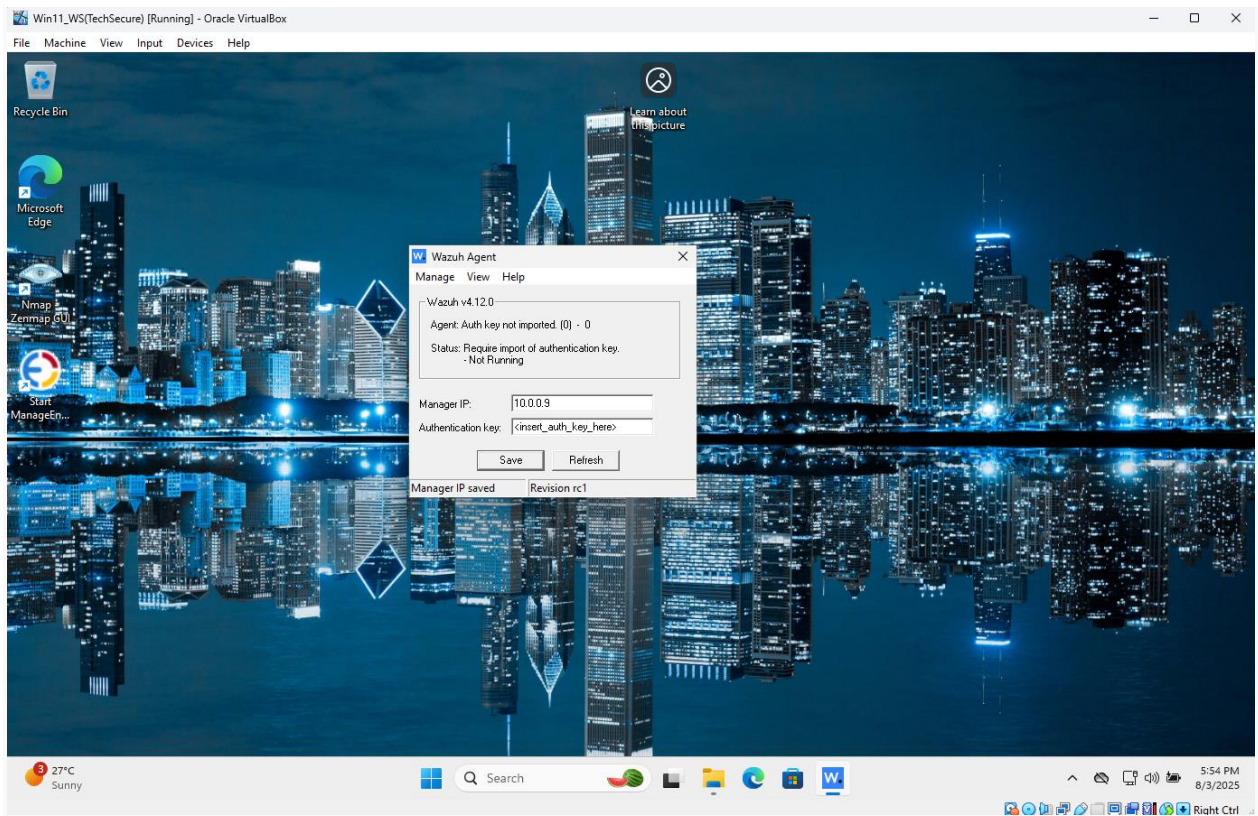
## 5. Centos



## 6. Kali







# Task 2: Hardening Cloud Instances

## 1. Azure

The screenshot shows the Microsoft Defender for Cloud Overview page. The left sidebar contains a navigation menu with categories like General, Cloud Security, and Management. The main content area displays several key metrics and sections:

- Security posture:** Shows 0 critical recommendations, 0 attack paths, and 0/0 overdue recommendations. It also displays an environment risk and secure score bar.
- Regulatory compliance:** Shows the Microsoft cloud security benchmark with 57 of 63 controls passed.
- Workload protections:** A section for managing workload protections.
- Inventory:** Shows 1 total resource.

On the right, there are additional sections for agentless code scanning, permissions management, and upgrading to the new Defender CSPM plan.

---

The screenshot shows the Access control (IAM) page for the user Mohammed Shahwar Ahmed. The left sidebar contains a navigation menu with categories like Overview, Billing, and Products + services. The main content area displays a table of access control results:

Name	Email	Role	Scope	Type
Mohammed Shahwar Ahmed	[REDACTED]	Owner	This scope	User

At the bottom, there is a pagination bar showing "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, and last 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. A green banner at the top indicates that the permissions boundary AdministratorAccess has been added.

**Summary**

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

Created: August 03, 2025, 01:07 (UTC-04:00)

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.

Policy name	Type	Attached via
<code>IAMUserChangePassword</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, PAM, Principal Access Boundary, Organizations, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federat..., Workforce Identity Federa..., Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit logs, Manage Resources, and Release Notes. The main content area displays the permissions for the 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"/>		[Redacted]	Viewer	
<input type="checkbox"/>		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

Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste 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[]=LYNIS|This release is more than 4 months old. Check the website or GitHub to see if there is an update a
available.|-|-|
binaries_count=1951
binaries_suid_count=/usr/bin/chfn /usr/bin/chsh /usr/bin/fusermount /usr/bin/fusermount3 /usr/bin/gpasswd /usr/bin/mo
unt /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_chkpw
d /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."	<b>Update Lynis:</b> Run: <code>sudo apt update &amp;&amp; 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.)	<b>Audit binaries:</b> 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.	<b>No immediate remediation needed</b> , but be aware of VM-specific risks. Disable unused virtual interfaces and guest tools if not required.

<b>OS Kernel Info</b>	Ubuntu 24.04.2 LTS running kernel 6.11.0-26-generic	Keep kernel and OS fully patched: Run: <code>sudo apt update &amp;&amp; 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
<b>Lynis</b>	<ul style="list-style-type: none"><li>- Outdated audit tool version</li><li>- SUID/SGID binaries found</li></ul>	<ul style="list-style-type: none"><li>- Updated Lynis</li><li>- Analyzed and removed risky binaries</li></ul>
<b>Wazuh</b>	<ul style="list-style-type: none"><li>- Some agents not reporting initially</li></ul>	<ul style="list-style-type: none"><li>- Reconfigured agent IP to point to Wazuh Manager</li><li>- Restarted Wazuh agent service</li></ul>
<b>Azure</b>	<ul style="list-style-type: none"><li>- No critical vulnerabilities found</li></ul>	<ul style="list-style-type: none"><li>- Verified recommendations are met</li><li>- Ensured MFA and secure IAM practices</li></ul>
<b>AWS</b>	<ul style="list-style-type: none"><li>- No critical findings via Amazon Inspector</li></ul>	<ul style="list-style-type: none"><li>- Reviewed IAM roles and enforced least privilege</li><li>- Enabled CloudTrail</li></ul>
<b>GCP</b>	<ul style="list-style-type: none"><li>- IAM had overly permissive roles</li></ul>	<ul style="list-style-type: none"><li>- Reassigned viewer roles</li><li>- Reviewed security findings in SCC</li></ul>

