

Week 12 - Enterprise Network Security

Task 1: Hardening Local VMs

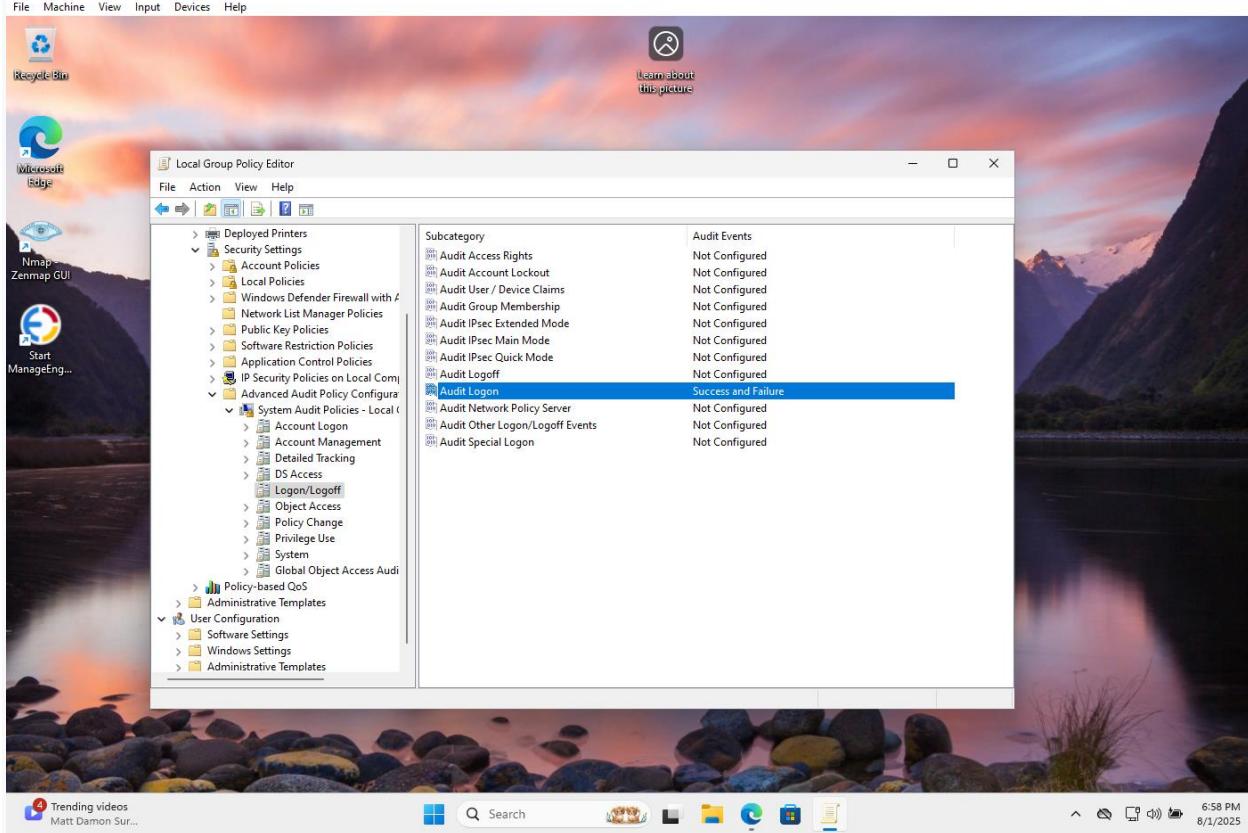
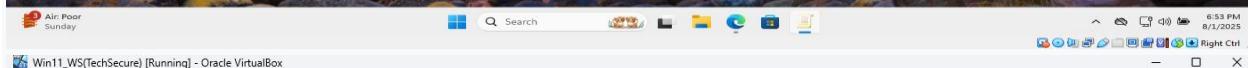
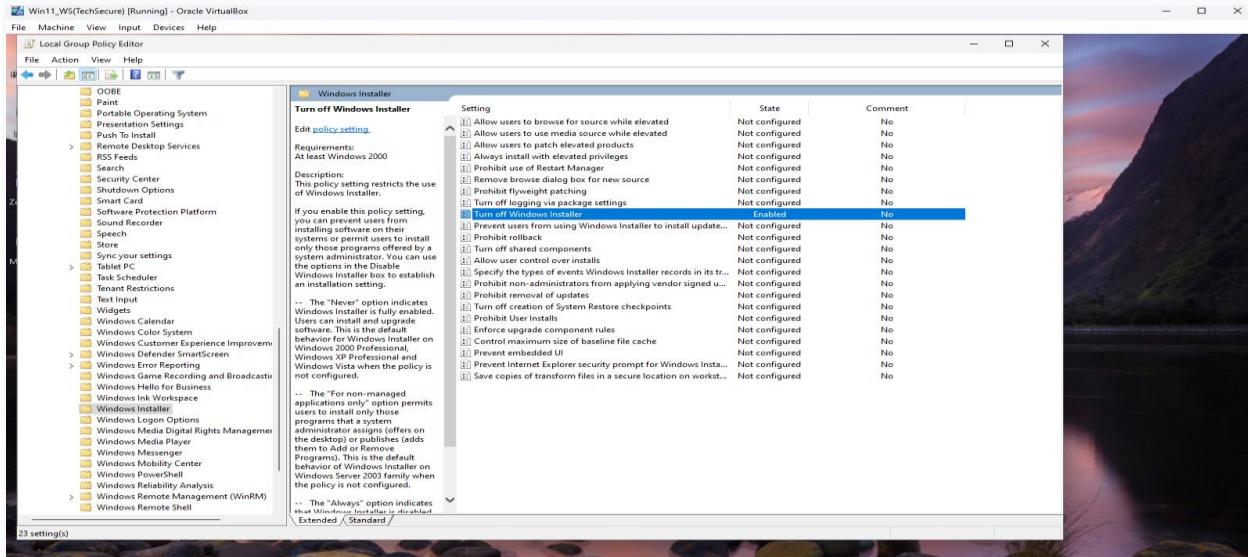
1. OPNSense Router

The screenshot shows the OPNSense web interface for managing firewall rules. The left sidebar is collapsed, showing the main navigation menu. The central panel displays the 'Firewall: Rules: LAN' configuration. A message at the top states 'The changes have been applied successfully.' Below this, a table lists four rules:

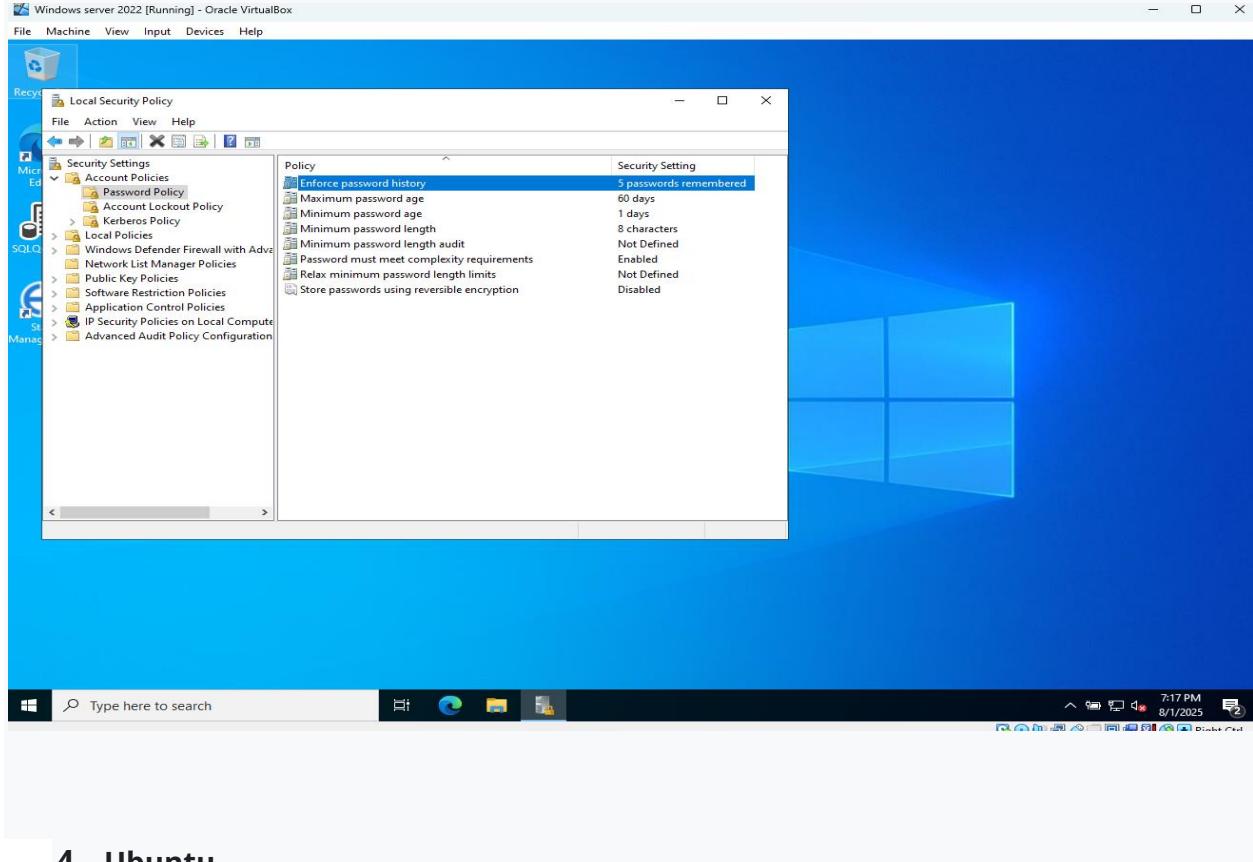
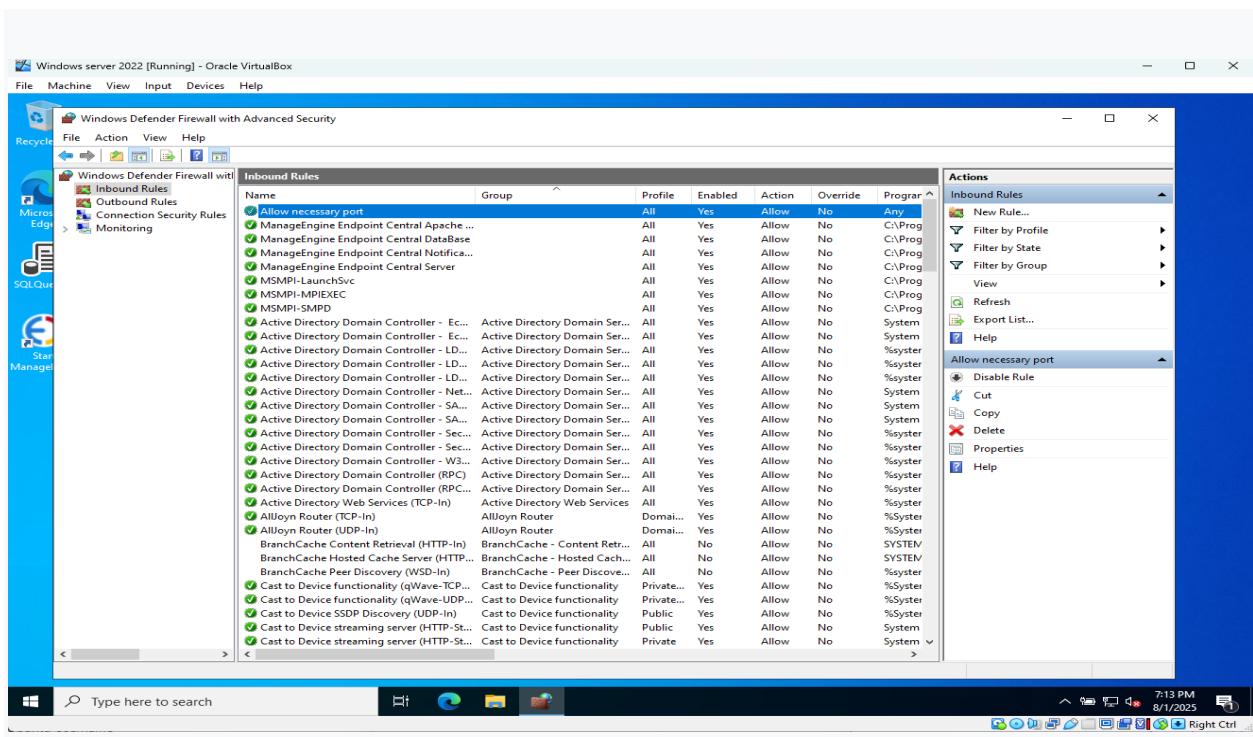
	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
1	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	*	Allow DNS
2	IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	*	Allow HTTP
3	IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	*	Allow HTTPS
4	IPv4 *	LAN net	*	*	*	*	*	Block all other LAN traffic

Below the table, there are icons for 'pass', 'block', 'reject', 'log', and 'first match/last match'. A note at the bottom explains 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.'

2. Windows 11



3. Windows Server 2022



4. Ubuntu

```
kali㉿kali-debian:~$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
kali㉿kali-debian:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

kali㉿kali-debian:~$ sudo aa-status
apparmor module is loaded.
157 profiles are loaded.
61 profiles are in enforce mode.
/snap/snapd/24718/usr/lib/snapd/snap-confine
/snap/snapd/24718/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/snap/snapd/24792/usr/lib/snapd/snap-confine
/snap/snapd/24792/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/bin/evince
/usr/bin/evince-previewer
/usr/bin/evince-previewer//sanitized_helper
/usr/bin/evince-thumbnailer
/usr/bin/evince//sanitized_helper
/usr/bin/evince//snap_browsers
/usr/bin/firefox
/usr/bin/man
/usr/lib/cups/backend/cups-pdf
/usr/lib/snapd/snap-confine
/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/sbin/cups-browsed
/usr/sbin/cupsd
```

5. Centos

```
root@localhost:~$ Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 33
[centos@localhost ~]$ sudo setenforce 1
[sudo] password for centos:
centos is not in the sudoers file. This incident will be reported.
[centos@localhost ~]$ su-
bash: su-: command not found...
[centos@localhost ~]$ su -
Password:
[root@localhost ~]# sudo setenforce 1
[root@localhost ~]# sudo firewall-cmd --set-default-zone-drop
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --set-default-zone-drop
[root@localhost ~]# sudo firewall-cmd --permanent --add-service=ssh
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --add-service=ssh
[root@localhost ~]# sudo firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
[root@localhost ~]# sudo firewall-cmd --reload
success
[root@localhost ~]# sudo yum install audit
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use "rhc" or "subscription-manager" to register.

CentOS Stream 9 - BaseOS          0.0 B/s |  0 B    00:00
Errors during downloading metadata for repository 'baseos':
 - Curl error (6): Couldn't resolve host name for https://mirrors.centos.org/metalink?repo=centos-baseos-9-stream&arch=x86_64&protocol=https,http [Could not resolve host: mirrors.centos.org]
Error: Failed to download metadata for repo 'baseos': Cannot prepare internal mirrorlist: curl error (6): Couldn't resolve host name for https://mirrors.centos.org/metalink?repo=centos-baseos-9-stream&arch=x86_64&protocol=https,http [Could not resolve host: mirrors.centos.org]
[root@localhost ~]# sudo systemctl start auditd
[root@localhost ~]# sudo systemctl enable auditd
[root@localhost ~]#
```

6. Kali

Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Applications

Trash

File System

Home

root@kali: ~

```
(root@kali)-[~]
# sudo systemctl start postgresql
(root@kali)-[~]
# msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

          dB8B8Bb dB8BP dB8B8BP dB8B8Bb
          dB' dB' dB' dB8P     dB8P dB8P
dB'dB'dB' dB8P     dB8P dB8P dB8P
dB'dB'dB' dB8P     dB8P dB8P dB8B8Bb
          dB8B8BP dB8P dB8B8BP dB8P dB8P dB8B8Bb

          dB8B8BP dB8B8Bb dB8P dB8B8BP dB8P dB8P dB8B8Bb
          dB' dB' dB' .BP   dB' .BP dB' .BP dB8P
dB' dB' dB' dB8P     dB8P dB8P dB8P dB8P
dB' dB' dB' dB8B8P   dB8P dB8B8P dB8B8P dB8P

          o
          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/>

File Machine View Input Devices Help

Right Ctrl .;

7. Wazuh

Wazuh v4.12.0 OVA [Running] - Oracle VirtualBox

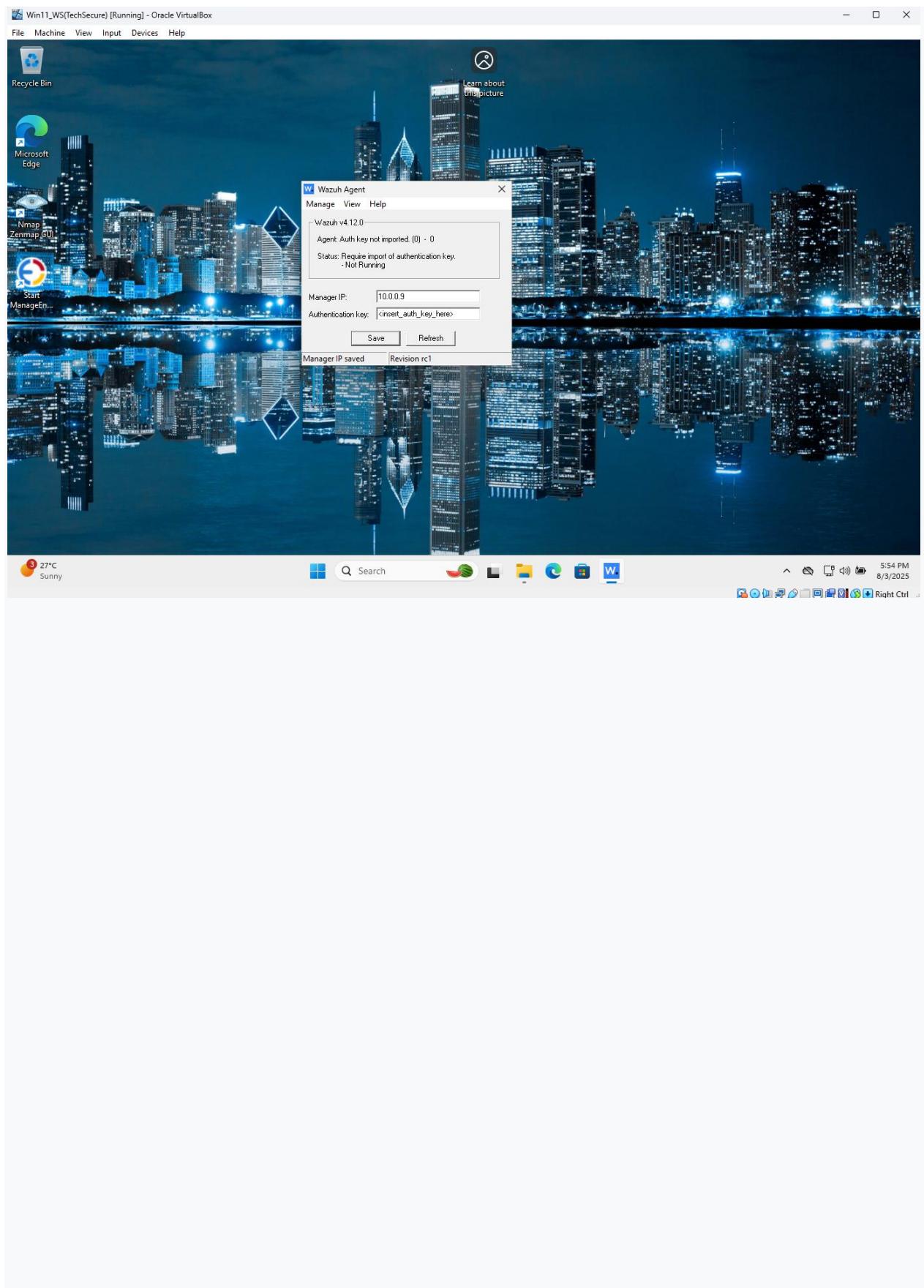
File Machine View Input Devices Help

```
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 19.306s
CGroup: /system.slice/wazuh-manager.service
└─2657 /var/ossec/framework/python/bin/python3 /var/ossec/api/script...
  ├─2658 /var/ossec/framework/python/bin/python3 /var/ossec/api/script...
  ├─2659 /var/ossec/framework/python/bin/python3 /var/ossec/api/script...
  ├─2662 /var/ossec/framework/python/bin/python3 /var/ossec/api/script...
  ├─2665 /var/ossec/framework/python/bin/python3 /var/ossec/api/script...
  ├─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)
```

File Machine View Input Devices Help

Right Ctrl .;



Task 2: Hardening Cloud Instances

1. Azure

The screenshot shows the Microsoft Defender for Cloud Overview page. Key metrics displayed include:

- 1 Azure subscriptions
- 1 Assessed resources
- 0 Attack paths
- 0 Security alerts
- 0 Critical recommendations
- 0 Attack paths
- 0 Overdue recommendations
- 0/0 Environment risk and secure score
- 0% Total secure score (Azure - AWS - GCP -)
- 57 of 63 controls passed (Regulatory compliance)
- No additional standards are currently monitored.
- Open security policies to manage additional compliance standards.
- Explore your security posture >
- Workload protections (Icon: server)
- Inventory (Icon: database)
- Total Resources: 1

On the right side, there are promotional cards for Agentless code scanning (Public Preview update) and Utilize the Permissions Management capability in Defender CSPM.

The screenshot shows the Microsoft Access control (IAM) page for user "Mohammed Shahwar Ahmed". The table displays the following information:

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

Helpful links and notes on the page include:

- Add or remove identities by pressing Ctrl+Shift+F
- Page 1 of 1
- < Previous | Next >
- Help me understand this table
- 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

2. AWS

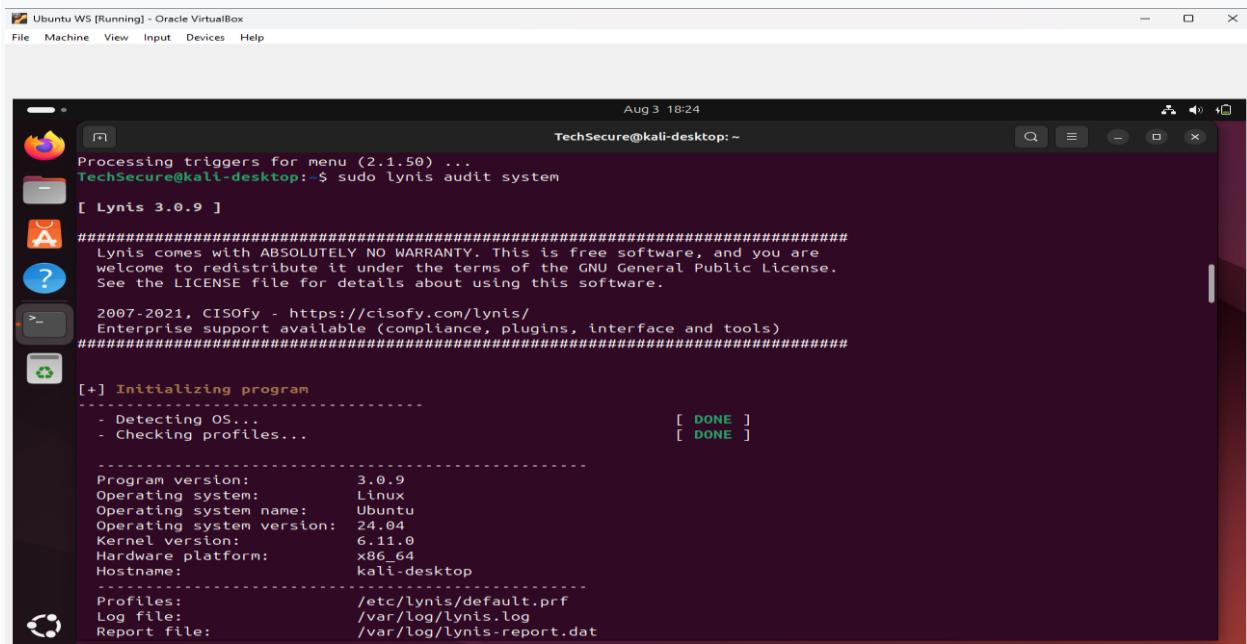
The screenshot shows the AWS IAM User details page for a user named MohammedShahwarAhmed. The top navigation bar includes links for IAM, Users, and MohammedShahwarAhmed. A green notification bar at the top right states "Permissions boundary AdministratorAccess added." Below the header, there's a "Summary" section with user information: ARN (arn:aws:iam::212067447266:user/MohammedShahwarAhmed), Created (August 03, 2025, 01:07 (UTC-04:00)), and Last console sign-in (Never). The "Console access" status is "Enabled without MFA". To the right, there's a link to "Create access key". The main content area has tabs for Permissions, Groups, Tags, Security credentials, and Last Accessed. Under the Permissions tab, there's a table showing one policy named "IAMUserChangePassword" attached directly. A "Permissions boundary (set)" section is also present. At the bottom, there's a "Generate policy based on CloudTrail events" button.

3. GCP

The screenshot shows the Google Cloud IAM Admin interface for a project titled "My First Project". The left sidebar lists various IAM-related services like PAM, Principal Access Boundary, Organizations, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federation, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit logs, Manage Resources, and Release Notes. The main content area is titled "IAM" and shows "Permissions for project 'My First Project'". It lists two principals: "ahmedshahwar786@gmail.com" with the role "Viewer" and "shahwar.fazal@gmail.com" with the role "Owner". There are buttons for "Grant access" and "Remove access". A "Policy updated" message is displayed at the bottom. On the right side, there's a sidebar titled "Recommended for you" with links to "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", and "Test role changes with Policy simulator".

Task 3: Security Auditing and Reporting

1. Local VMs

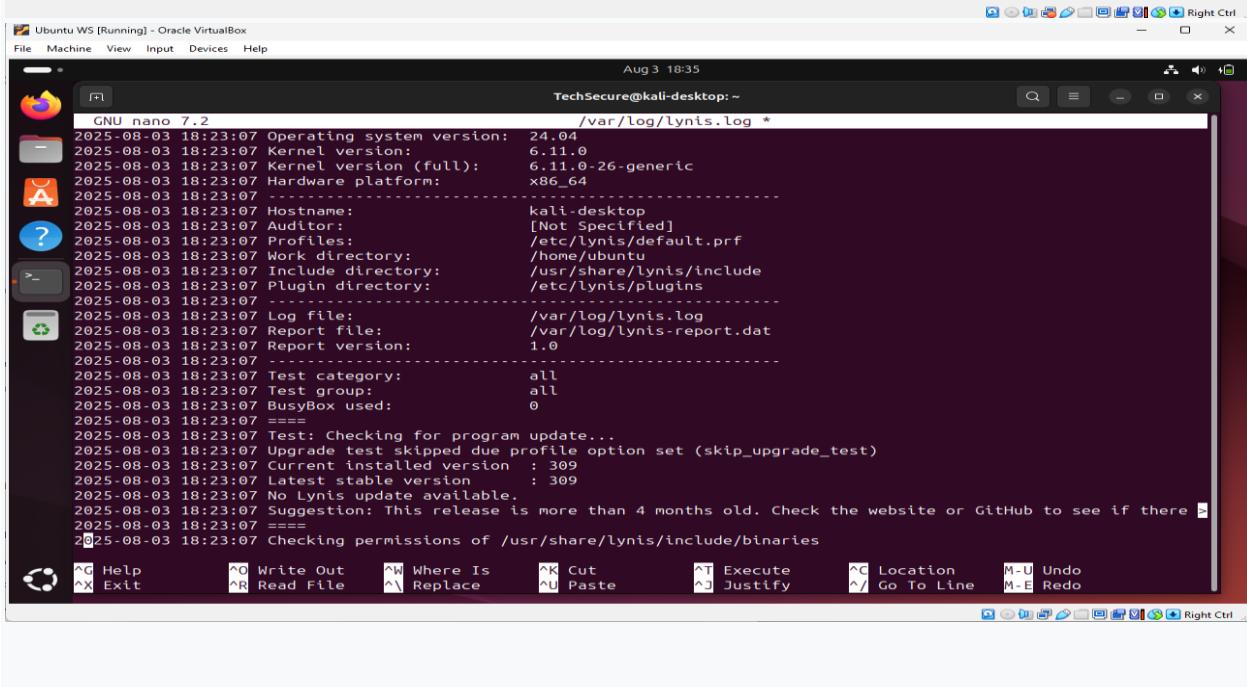


```
Ubuntu WS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 3 18:24
TechSecure@kali-desktop:~$ sudo lynis audit system
[ Lynis 3.0.9 ]
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

2007-2021, CISOfy - https://ciscofy.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
Aug 3 18:35
TechSecure@kali-desktop:~$ /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 is a newer version.
2025-08-03 18:23:07 ====
2025-08-03 18:23:07 Checking permissions of /usr/share/lynis/include/binaries
```

```

[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 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/unmount /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: 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