Lab 2.1 – Configuring Security Policies on a Virtual Machine

1. Lab Overview

1.1 Lab Description

In this lab, you'll practice **system hardening** by configuring security policies inside a virtual machine (VM). VMs provide a safe sandbox environment where you can apply real-world policies without risking your host system.

You'll learn how to:

- Create and manage user accounts with proper privileges.
- Enforce strong password policies.
- Restrict administrative rights.
- Enable system logging for monitoring and auditing.

By the end of this lab, you'll have a **hardened VM snapshot** — a secure baseline you can roll back to whenever needed.

1.2 Learning Objectives

After completing this lab, you will be able to:

- Explain the importance of system hardening in cybersecurity.
- Set up a virtual machine environment for testing security policies.
- Configure password policies on Windows and Linux.
- Restrict administrative privileges and apply the principle of least privilege.
- Enable and verify logging and auditing systems.
- Document and save a secure VM snapshot for reuse.

1.3 Prerequisites

To successfully complete this lab, you should have:

- A working computer with **at least 8GB RAM** and **20GB free disk space**.

- A virtualization tool installed (VirtualBox, VMware Workstation, or Hyper-V).
- A Windows (10/11) or Linux (Ubuntu Server recommended) installation ISO.
- Basic knowledge of command-line usage (Linux) and system administration.
- Administrative rights on your host system (to install/configure VMs).

1.4 Estimated Completion Time

Activity	**Estimated Time**
Setting up the VM (installation + user accounts)	90 minutes
Configuring password policies	60 minutes
Limiting administrative privileges	45 minutes
Enabling and verifying logging	45 minutes
Lab Challenge: Hardened VM snapshot + reflection	60 minutes
Total Estimated Time	**~5 hours**

Checkpoint
Before moving on, make sure you:

- Understand that this lab takes ~5 hours.
- Have a VM platform installed.
- Have chosen an OS (Windows or Linux) to practice with.

2. Getting Started

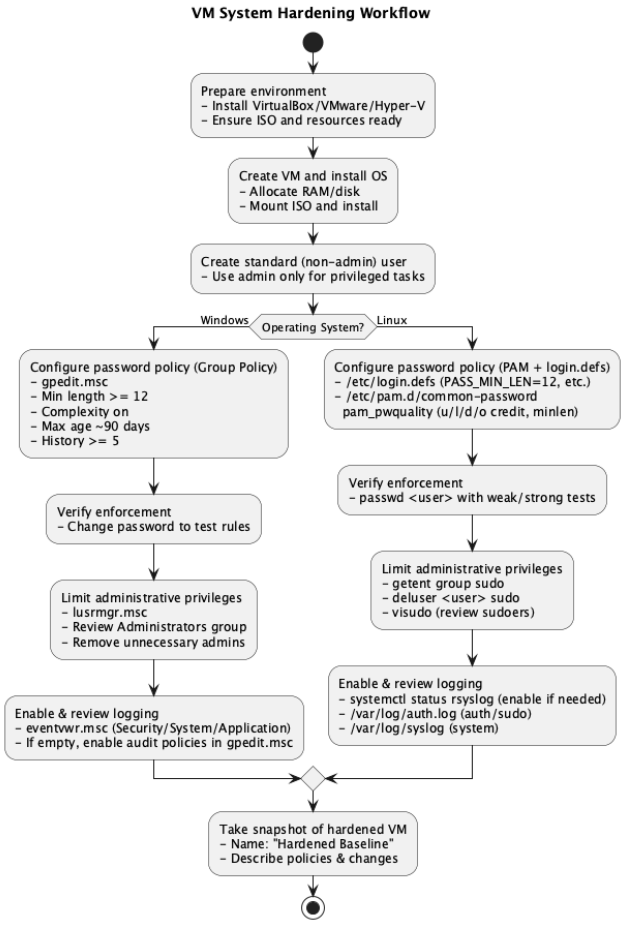
2.1 What is System Hardening?

System hardening is the process of securing a computer system by reducing its attack surface. This means eliminating unnecessary accounts, enforcing strict policies, and enabling monitoring features to catch suspicious behavior early.

Examples of hardening actions:

- Enforcing **strong passwords**
- Restricting **admin privileges**
- Enabling **logging and auditing**
- Removing or disabling unused services

Key Idea: The fewer "weak spots" a system has, the harder it is for an attacker to succeed.



2.2 Why Use Virtual Machines for Security Labs?

Virtual machines (VMs) provide a **safe sandbox** for practicing cybersecurity:

- **Isolation** – Your changes don't affect your host machine.
- **Reset capability** – You can roll back to a snapshot if something breaks.
- **Multiple OS support** – Practice hardening on both Windows and Linux.
- **Realism** – VMs behave like real systems, so the skills directly transfer to production environments.

2.3 Lab Setup Checklist

Before starting, make sure you have:

Virtualization software installed

- VirtualBox (free, cross-platform)
- VMware Workstation Player (free for personal use)
- Hyper-V (included with Windows Pro/Enterprise)

Operating system ISO

- Windows 10/11 (evaluation version is fine)
- Ubuntu Server (lightweight Linux option)

Host system requirements

- Minimum: 8 GB RAM and 20 GB free disk space
- Internet connection (for updates and downloads)

VM setup basics completed

- Created a new virtual machine
- Installed chosen OS
- Created at least **one standard (non-admin) user account**

Checkpoint
Before moving on:

- Do you have a working VM environment ready?
- Have you installed Windows or Linux inside the VM?
- Did you create a **standard user account** (not just admin/root)?

3. Setting Up Your Virtual Machine

3.1 Choosing a Virtualization Platform

You'll need virtualization software to run your VM. Popular choices:

- **VirtualBox** (free, cross-platform)
- **VMware Workstation Player** (free for personal use)
- **Hyper-V** (built into Windows Pro/Enterprise editions)

Tip: If unsure, choose **VirtualBox** — it's widely supported and easy to use.

3.2 Creating a New Virtual Machine

Follow your platform's "New VM" wizard. Typical steps include:

1. **Name and OS Selection**
    - Example: "Ubuntu Hardened VM" or "Windows Security Lab"
    - Select the operating system type and version
2. **Allocate Resources**
    - Memory: at least **2 GB for Linux**, **4 GB for Windows**
    - Disk: 20 GB minimum
3. **Attach Installation Media**
    - Mount the ISO file for Windows or Linux installation
4. **Install the Operating System**
    - Boot the VM and follow normal OS installation steps

3.3 Creating Standard User Accounts

Once your VM OS is installed:

- **On Windows**
    - Open **Settings → Accounts → Family & other users**
    - Add a new **standard user** account (non-admin)
    - Use the admin account only for privileged tasks
- **On Linux**
    - Add a new user with:
    - sudo adduser studentuser
    - Assign a password when prompted
    - Verify the account works by logging in

Principle of Least Privilege: Always use standard accounts for daily tasks. Admin/root access should only be used when necessary.

3.4 Recap: VM Setup Essentials

Step	Windows	Linux
Create VM	VirtualBox/VMware/Hyper-V wizard	VirtualBox/VMware/Hyper-V wizard
Install OS	Windows 10/11	Ubuntu Server/Desktop
Create Standard User	Settings → Accounts → Add user	`sudo adduser studentuser`
Verify Least Privilege	Login as standard user, not admin	Confirm sudo access restricted

Checkpoint
Before continuing:

- Is your VM installed and running?
- Do you have at least one **standard user account**?
- Can you log in without using the admin/root account?

4. Enforcing Password Policies

Passwords are often the first line of defense against intruders. Weak passwords make even a hardened system vulnerable. In this section, you'll enforce rules that require stronger, more secure passwords.

4.1 Windows: Using Group Policy Editor

1. **Open Group Policy Editor**
    - Press **Windows key + R**
    - Type:
    - gpedit.msc
    - Press **Enter**
2. **Navigate to Password Policy**
    - Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy
3. **Set Strong Rules**
    - Minimum password length: **12 characters**
    - Password must meet complexity requirements (uppercase, lowercase, number, symbol)
    - Maximum password age: **90 days**
    - Minimum password age: **1 day**
    - Enforce password history: **remember last 5 passwords**

Tip: After applying changes, log out and try creating a new password to test enforcement.

4.2 Linux: Configuring PAM and login.defs

Linux uses **PAM (Pluggable Authentication Modules)** for authentication rules.

A. Edit /etc/login.defs

1. Open the file in a text editor:
2. sudo nano /etc/login.defs
3. Adjust these values:
4. PASS_MAX_DAYS 90
5. PASS_MIN_DAYS 1
6. PASS_MIN_LEN 12
7. PASS_WARN_AGE 7
    - **PASS_MAX_DAYS** = force password change after 90 days
    - **PASS_MIN_LEN** = minimum password length

B. Edit PAM password policies

1. Open PAM password configuration:
2. sudo nano /etc/pam.d/common-password
3. Add or adjust the following line:
4. password requisite pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
    - minlen=12 → Minimum length 12
    - ucredit=-1 → At least one uppercase letter
    - lcredit=-1 → At least one lowercase letter
    - dcredit=-1 → At least one digit
    - ocredit=-1 → At least one special character

Test It: Try changing a password with passwd studentuser — weak passwords should be rejected.

4.3 Strong Password Guidelines

Even with enforced rules, remind users of good practices:

- Use **passphrases** instead of single words.
- Avoid dictionary words or predictable patterns.
- Never reuse passwords across accounts.
- Use a **password manager** for secure storage.

4.4 Recap Table: Password Policies by Platform

Policy	Windows (Group Policy)	Linux (PAM/login.defs)
Minimum Length	12 characters	PASS_MIN_LEN 12 / pam_pwquality minlen=12
Complexity	Require uppercase, lowercase, symbol	pam_pwquality with ucredit/lcredit/dcredit/ocredit
Maximum Age	90 days	PASS_MAX_DAYS 90
Password History	Remember last 5 passwords	Handled via PAM modules

Checkpoint

Before continuing:

- Did you configure password policies in Windows or Linux?
- Did you test enforcement by changing a password?
- Do you understand why password expiration and complexity matter?

5. Limiting Administrative Privileges

Not every user should have full control of a system. The **principle of least privilege** means giving users only the access they need to do their work. This reduces the risk of accidental misconfigurations or malicious actions.

5.1 Windows: Managing Local Users and Groups

1. **Open Local Users and Groups**
    - Press **Windows key + R**
    - Type:
    - lusrmgr.msc
    - Press **Enter**
2. **Review Administrator Group Members**
    - In the left panel, click **Groups**
    - Double-click **Administrators**
    - Review which accounts are listed
3. **Remove Unnecessary Admins**
    - Select any user that should not have admin rights
    - Click **Remove**
4. **Verify Standard Users**
    - Ensure your **daily-use account** is part of the **Users** group only

Tip: Always leave one emergency admin account enabled, but don't use it for daily work.

5.2Linux: Configuring sudoers File

1. **Check Current sudo Users**
   ```
   # This will list all users with sudo privileges
   getent group sudo
   ```
2. **Remove Unnecessary sudo Rights**
   ```
   #To remove a user from the sudo group:
   sudo deluser username sudo
   ```
3. **Edit sudoers File (if needed)**
   ```
   # Open with visudo (safer than editing directly)
   sudo visudo
   ```
4. Ensure only trusted accounts have ALL=(ALL:ALL) ALL privileges

Tip: Always keep one admin account — but use a **separate standard account** for daily work.

5.3 Best Practices for Privilege Management

Create separate **admin and standard accounts**.
Use **admin rights only when needed**.
Audit admin accounts regularly.
Disable or remove unused accounts.
Never share admin accounts among multiple users.

5.4 Recap: Admin Access Controls

Platform	Check Admin Rights	Restrict Admin Rights
Windows	lusrmgr.msc → Groups → Administrators	Remove unnecessary users from Admin group
Linux	getent group sudo	sudo deluser username sudo / visudo

Checkpoint
Before moving on:

- Did you review who has admin/sudo privileges?
- Did you remove unnecessary admin accounts?
- Do you now have at least one standard account for daily use?

6. Enabling Logging and Monitoring

Logs are your **early warning system**. They record system activity such as logins, errors, and security events, helping you detect attacks or policy violations.

In this section, you'll enable and verify logging on both **Windows** and **Linux**.

6.1 Windows: Event Viewer Setup

1. **Open Event Viewer**
    - Press **Windows key + R**
    - Type:
    - eventvwr.msc
    - Press **Enter**
2. **Review Security, System, and Application Logs**
    - In the left-hand menu, expand **Windows Logs**
    - Check:
        - **Security** (logon attempts, privilege use)
        - **System** (OS-level warnings/errors)
        - **Application** (program activity)
3. **Verify Security Logging is Active**
    - If Security logs are empty, auditing may not be enabled.
    - To enable auditing, open:
      gpedit.msc → Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies

Tip: Pay attention to repeated failed logon attempts — these may signal a brute-force attack.

6.2 Linux: Syslog and Auth.log

Linux systems typically use **rsyslog** or **syslog-ng** to manage logs.

1. **Check if rsyslog is running**
2. sudo systemctl status rsyslog
    - If inactive, start it:
      sudo systemctl start rsyslog
      sudo systemctl enable rsyslog
3. **View Authentication Logs**
    - Login attempts and sudo activity are logged here:
    - sudo less /var/log/auth.log
4. **View General System Logs**
    - System-wide events are stored here:
    - sudo less /var/log/syslog

Tip: Use grep to search logs, e.g.:

grep "Failed password" /var/log/auth.log

6.3 Why Logs Matter

- **Detection**: Failed logins or privilege escalation attempts stand out.
- **Forensics**: Logs provide evidence after an incident.
- **Compliance**: Many standards (ISO 27001, PCI DSS) require system logging.

6.4 Recap Table: Key Logs to Monitor

Platform	Logs to Check	Purpose
Windows	Security, System, Application	Monitor logins, errors, and program events
Linux	/var/log/auth.log	Authentication and sudo activity

Platform	Logs to Check	Purpose
Linux	/var/log/syslog	General system events

Checkpoint

Before moving on:

- Did you enable and verify logging on your VM?
- Can you locate **login attempts** in your logs?
- Do you understand why logs are crucial for attack detection?

7. Lab Challenge

Now it's time to put everything together. You'll enforce password policies, restrict admin privileges, enable logging, and save your hardened system as a reusable snapshot.

7.1 Harden Your VM

Apply the following changes inside your VM:

- Enforce strong **password policies** (length, complexity, expiration).
- Restrict **administrative privileges** so only trusted accounts have elevated rights.
- Enable and verify **logging and monitoring** (Event Viewer in Windows, auth.log and syslog in Linux).

7.2 Take a Snapshot of Your Hardened VM

Snapshots let you save the current state of your VM. If you make mistakes later, you can roll back to this hardened baseline.

Steps (VirtualBox example):

1. Shut down or pause your VM.
2. In VirtualBox, right-click your VM → **Take Snapshot**.
3. Name it: *Hardened Baseline*
4. Add a description (e.g., "Password policies, admin restrictions, and logging configured").

In VMware or Hyper-V, use the **Snapshot/Checkpoint** feature.

7.3 Reflection Questions

Write down your answers in your lab notebook or submit them if required:

1. What password rules did you configure, and how did you test them?

2. Which accounts have admin/sudo privileges after your changes?
3. What logs did you review, and what events did you see?
4. How would snapshots help you in real-world security administration?
5. What would be the **next hardening step** if this VM were going into production?

Challenge Complete!

You now have a **hardened VM snapshot** — a reusable secure baseline that you can roll back to anytime. This mirrors how IT professionals prepare “golden images” for enterprise deployment.

8. Wrap-Up and What's Next

8.1 Key Takeaways

In this lab, you successfully **hardened a virtual machine** by applying real-world security policies. Specifically, you:

Set up a secure VM environment using VirtualBox, VMware, or Hyper-V.
Enforced **strong password rules** to protect accounts.
Restricted **administrative privileges** to trusted users only.
Enabled and verified **system logging** for monitoring and early attack detection.
Created a **VM snapshot** — your hardened baseline for future labs.

8.2 Skills You've Gained

By completing this lab, you can now:

- Explain the principle of **least privilege** and apply it.
- Configure **password policies** on Windows and Linux.
- Manage **admin vs. standard accounts** effectively.
- Use **Event Viewer** (Windows) and /var/log (Linux) for security monitoring.
- Create and document **snapshots** to preserve hardened states.

These are core administrative skills that every cybersecurity professional must master.

8.3 Next Topic: Network Security Fundamentals

Now that your VM is hardened, the next challenge is to secure its **connections to the outside world**.

In the upcoming **Network Security Fundamentals module**, you'll explore:

- Basic network protocols and how attackers exploit them.
- Network-based defenses such as firewalls, IDS/IPS, and segmentation.
- Hands-on labs where you'll analyze traffic and secure communications.

Next Steps

- Save or submit your lab reflection answers.
- Keep your **Hardened VM snapshot** for use in future labs.
- Prepare for the **Network Security Fundamentals** module.

You've built a strong, secure foundation at the system level. Next, you'll learn how to protect that system when it communicates over a network.

9. Appendix

9.1 Key Linux Commands

Command	Purpose
sudo adduser username	Create a new standard user
sudo deluser username sudo	Remove a user from the sudo (admin) group
sudo nano /etc/login.defs	Edit password policy defaults
sudo nano /etc/pam.d/common-password	Configure PAM password complexity
sudo visudo	Safely edit sudoers file
sudo systemctl status rsyslog	Check if logging service is running
sudo less /var/log/auth.log	Review authentication logs
sudo less /var/log/syslog	Review general system logs
grep "Failed password" /var/log/auth.log	Search for failed login attempts in logs

9.2 Windows Quick Access Paths

Task	Path / Tool
Open Group Policy Editor	gpedit.msc → Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy
Manage Local Users and Groups	lusrmgr.msc → Groups → Administrators / Users
View Security Logs	eventvwr.msc → Windows Logs → Security
Enable Advanced Audit Policies	gpedit.msc → Security Settings → Advanced Audit Policy Configuration

9.3 Troubleshooting Tips

Problem	Possible Cause	Solution
Password policy not enforced (Windows)	Wrong policy scope / not applied yet	Run gpupdate /force to apply Group Policy
Weak passwords still accepted (Linux)	PAM module not configured correctly	Verify common-password includes pam_pwquality
Standard user can still use admin features	User left in Administrators or sudo group	Remove with lusrmgr.msc (Windows) / deluser (Linux)
Logs are empty (Windows)	Security auditing not enabled	Configure audit policies in Group Policy Editor
No auth.log on Linux	Logging service disabled	Start rsyslog: sudo systemctl enable --now rsyslog

9.4 Additional Resources

Documentation

- Microsoft Docs – Password Policy Settings: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- Ubuntu Security Documentation: https://ubuntu.com/security
- PAM Password Quality Module Guide: http://www.linux-pam.org/Linux-PAM-html/sag-pam_pwquality.html

Tools & Best Practices

- CIS Benchmarks (industry hardening standards): https://www.cisecurity.org/cis-benchmarks
- NIST Password Guidelines (SP 800-63): https://pages.nist.gov/800-63-3/sp800-63b.html