

SYSTEM HARDENING REPORT

Windows 11 — Local Security Policy Implementation

Prepared By: Rabya Hassan

Course: Network Security

Platform: Windows 11

Role: System Security Administrator

Document Type: Portfolio Project — Educational

1. Executive Summary

This report documents the implementation of system hardening techniques on a Windows 11 endpoint using the Local Security Policy (secpol.msc) framework. The project simulates a real-world scenario in a university environment where repeated unauthorized login attempts were detected, requiring a structured security response.

Five security control domains are addressed: password policy enforcement, account lockout configuration, audit logging, user rights assignment, and security options. Each control is grounded in NIST SP 800-53 principles and Microsoft security baseline guidance.

2. Objectives

- Analyze and document the default security posture of a Windows 11 system
- Configure password policies aligned with NIST SP 800-63B guidelines
- Implement account lockout to defend against brute-force attacks
- Enable audit policies to ensure visibility into security events
- Apply User Rights Assignment to enforce the Principle of Least Privilege
- Harden Security Options to reduce information disclosure
- Validate all configurations through live testing and Event Viewer log analysis

3. Tools & Technologies

Tool	Purpose	Access Path
Windows 11	Target operating system	—
Local Security Policy	Policy configuration	secpol.msc
Event Viewer	Security log analysis	eventvwr.msc
Local Users and Groups	Account management	lusrmgr.msc

4. Theoretical Background

4.1 System Hardening

System hardening reduces the attack surface of a system by removing unnecessary services, enforcing strong authentication, and applying the Principle of Least Privilege. It follows a defense-in-depth approach where multiple overlapping controls compensate for the potential failure of any single layer.

4.2 Windows Local Security Policy

The Local Security Policy editor (secpol.msc) gives administrators granular control over security settings on standalone Windows machines. It covers account policies (passwords and lockout), local policies (audit settings, user rights, and security options), and is the standard tool for applying Microsoft security baselines without an Active Directory domain.

4.3 Brute-Force Attacks & Mitigations

A brute-force attack systematically tries password combinations until a match is found. Defenses include: enforcing minimum password length and complexity to increase entropy, enabling account lockout after a threshold of failed attempts, monitoring failed logon events (Event ID 4625), and renaming or disabling default accounts such as Administrator and Guest.

4.4 Principle of Least Privilege

Every user and process should have only the minimum rights needed to perform its function. In Windows, this is enforced through User Rights Assignment policies that control sensitive operations such as local logon, system shutdown, and network access.

4.5 Audit Logging

Audit policies configure the Windows Security Event Log to record security-relevant activity. These logs are the foundation of incident response and forensic investigation. Key event IDs: 4624 (successful logon), 4625 (failed logon), and 4740 (account lockout). Without auditing enabled, an attacker leaves no traceable record on the system.

5. Baseline Analysis

A baseline assessment of the default Windows 11 configuration was performed before applying any controls. The following weaknesses were identified:

- No minimum password length — single-character passwords were accepted
- Password complexity disabled — simple dictionary passwords were permitted
- No account lockout — unlimited login attempts allowed
- Audit policies disabled — no logging of logon events, privilege use, or policy changes
- Excessive user privileges — standard users could shut down the system
- Default Administrator and Guest account names unchanged
- Last logged-on username displayed on the login screen, leaking valid account names

6. Implementation of Security Controls

6.1 Password Policy

Password strength is the first line of defense against credential attacks. Minimum length enforcement is the most effective single control, as password entropy grows exponentially with length. Complexity rules further reduce the viable search space for dictionary and rule-based attacks. Reversible encryption must be disabled — it stores a recoverable form of the password that compromises the entire authentication model if the SAM database is accessed.

Configuration applied:

- Minimum Password Length: 10 characters
- Password Complexity: Enabled (uppercase, lowercase, digits, special characters)
- Store Passwords Using Reversible Encryption: Disabled

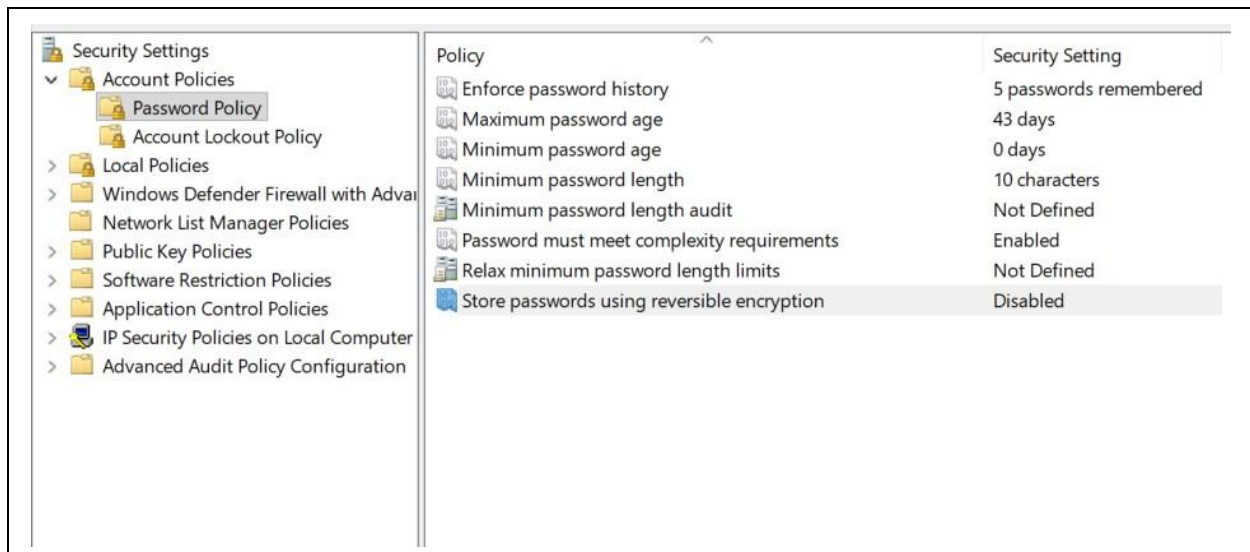


Figure 1: Password policy configured in Local Security Policy — minimum length of 10 characters, complexity enabled, and reversible encryption disabled.

6.2 Account Lockout Policy

Account lockout introduces an enforced delay after repeated failed authentication attempts, making exhaustive password guessing impractical. Three parameters govern the policy: lockout threshold (failures before lockout), lockout duration, and the observation window for resetting the failure counter.

Configuration applied:

- Account Lockout Threshold: 3 invalid login attempts
- Account Lockout Duration: 20 minutes
- Reset Account Lockout Counter After: 15 minutes

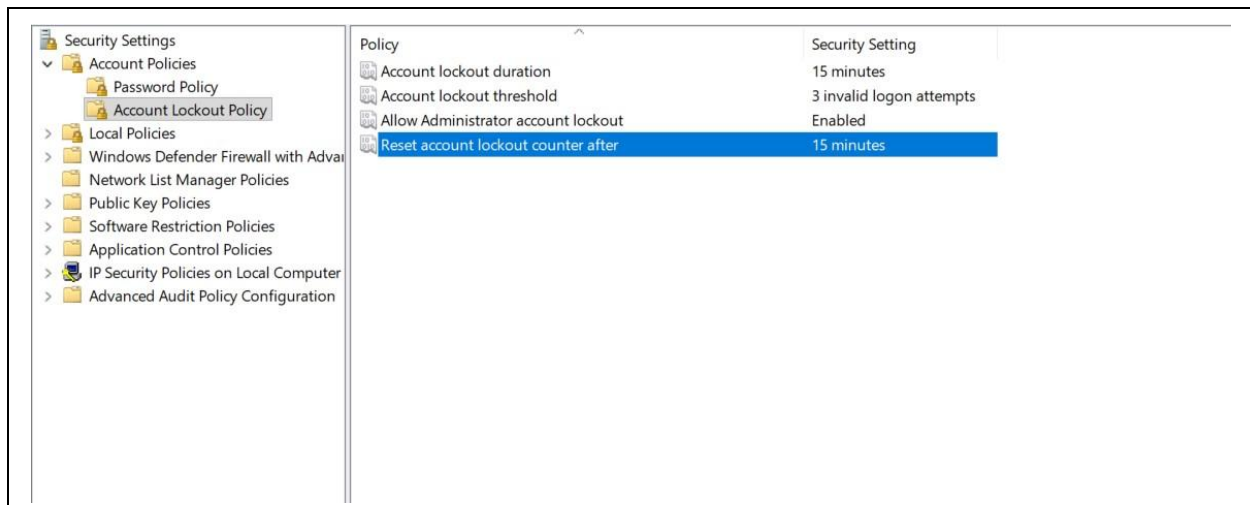


Figure 2: Account lockout policy — threshold of 3 consecutive failures triggers a 20-minute lockout, with the failure counter resetting after 15 minutes.

6.3 Audit Policies

Audit policies determine which security events are written to the Windows Security Event Log. Enabling them transforms a forensically blind system into one with a full event trail for incident detection and investigation. The following categories were enabled for both success and failure:

- Audit Logon Events — interactive and network logons and logoffs
- Audit Account Logon Events — authentication against the local account database
- Audit Policy Change — modifications to audit and trust policies
- Audit Privilege Use — use of sensitive privileges
- Audit Object Access — access to files, folders, and registry keys

Security Number of events: 30,564

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 298

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/3/2026 10:50:45 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:50:44 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:50:44 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:50:44 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:50:37 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:50:28 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:49:10 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:47:18 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:29 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:07 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:05 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:04 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:04 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/3/2026 10:41:04 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:41:00 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:39:41 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:37:36 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:34:02 AM	Microsoft Windows security au...	4624	Logon
Audit Success	3/3/2026 10:33:58 AM	Microsoft Windows security au...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject: Security ID: SYSTEM

Log Name: Security

Source: Microsoft Windows security ; Logged: 3/3/2026 10:50:45 AM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-PQNI6RP

Figure 3: Audit policy settings in Local Security Policy — logon events, account management, privilege use, and policy change auditing enabled for both success and failure.

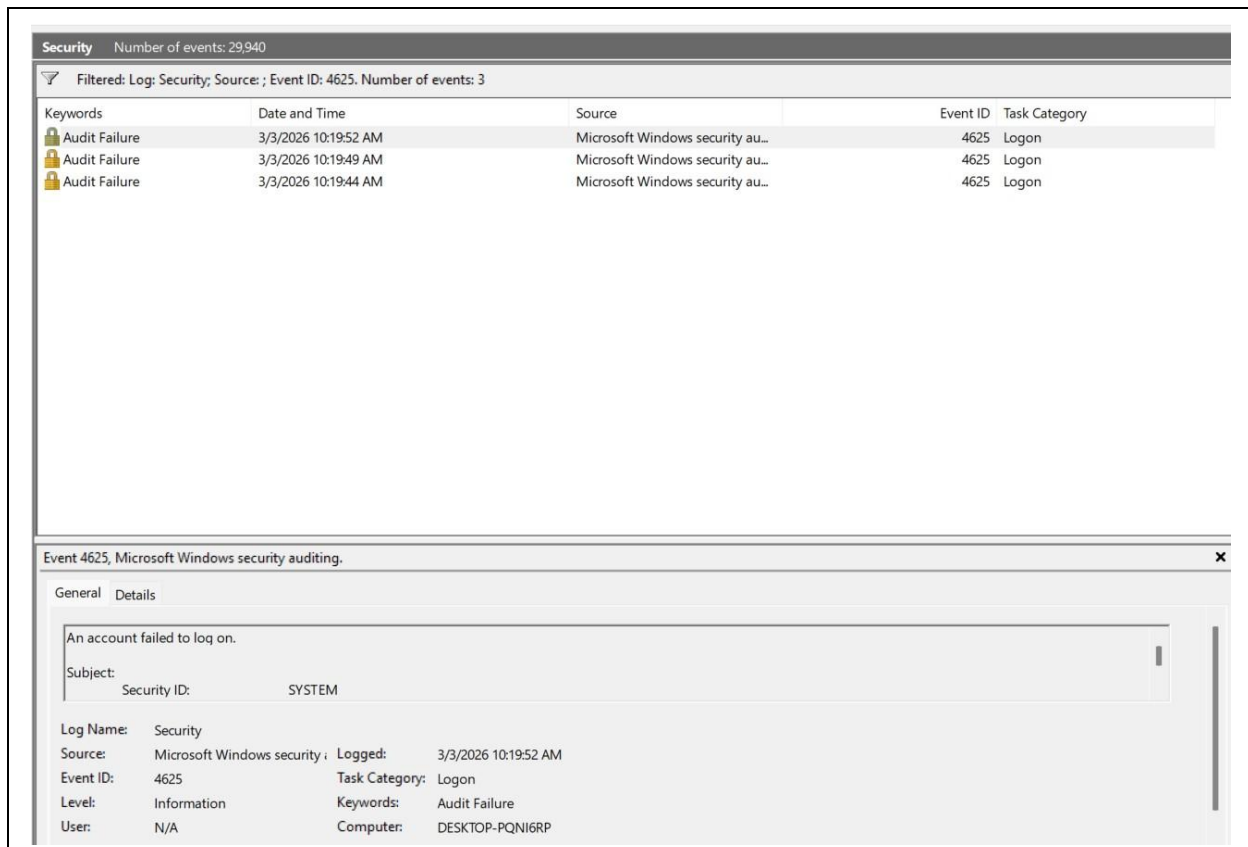


Figure 4: Windows Event Viewer Security Log showing Event ID 4625 (Failed Logon) — captures the timestamp, targeted account, and failure reason, confirming audit logging is active.

Note: A spike in Event ID 4625 entries against the same account over a short period is a high-confidence indicator of an automated brute-force attack in progress.

6.4 User Rights Assignment

User Rights Assignment controls which accounts can perform privileged system-level operations. Unlike file permissions, which restrict access to resources, these rights govern actions such as shutting down the system, logging on locally, or accessing the system over the network. Removing unnecessary rights limits the damage a compromised account can cause.

Configuration applied:

- Shut Down the System: Restricted to Administrators group only
- Deny Log On Locally: Applied to the Guest account
- Access This Computer from the Network: Restricted to authorized accounts

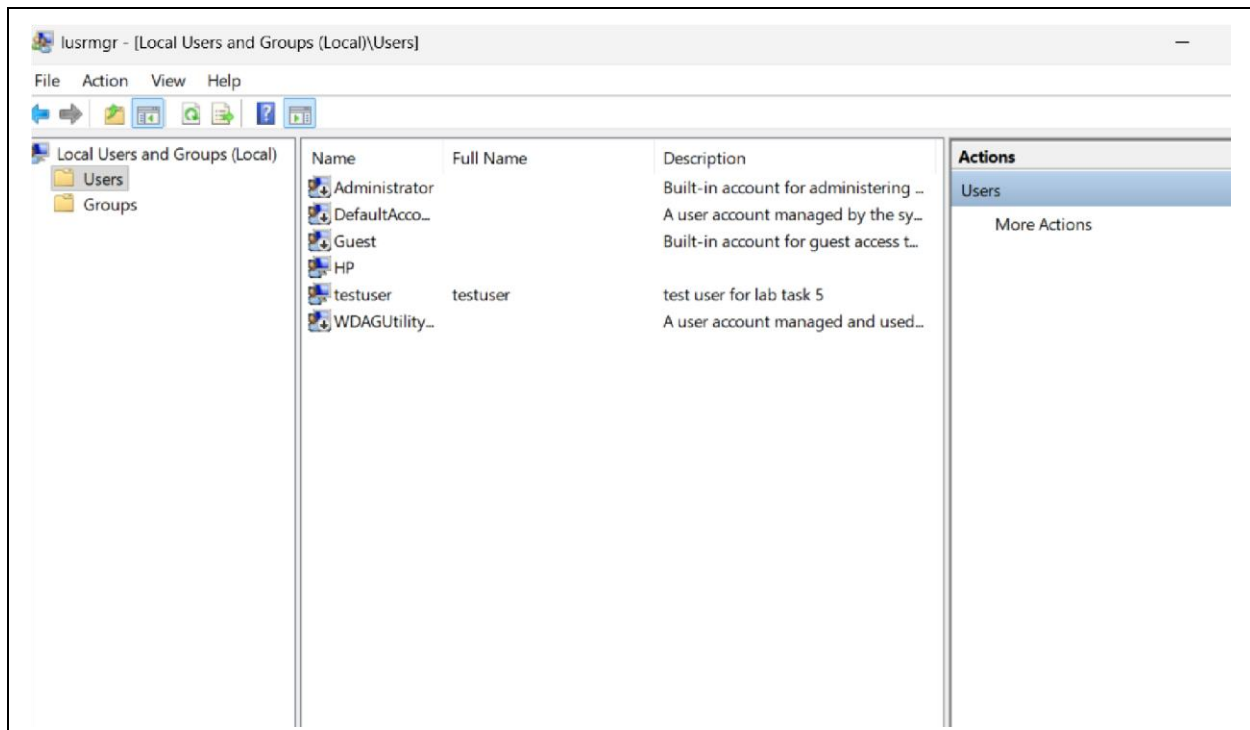


Figure 5: User Rights Assignment — shutdown privilege restricted to Administrators; local logon denied for the Guest account.

6.5 Security Options

Security Options address operational security settings beyond basic authentication. Hiding the last logged-on username prevents an attacker from enumerating valid account names directly from the login screen. Renaming default accounts removes predictable targets from the local namespace. SMB signing prevents man-in-the-middle relay attacks against network file sharing.

Configuration applied:

- Administrator account renamed to a non-default value
- Guest account renamed and disabled
- Interactive logon: Do not display last user name — Enabled
- Microsoft network server: Digitally sign communications (always) — Enabled

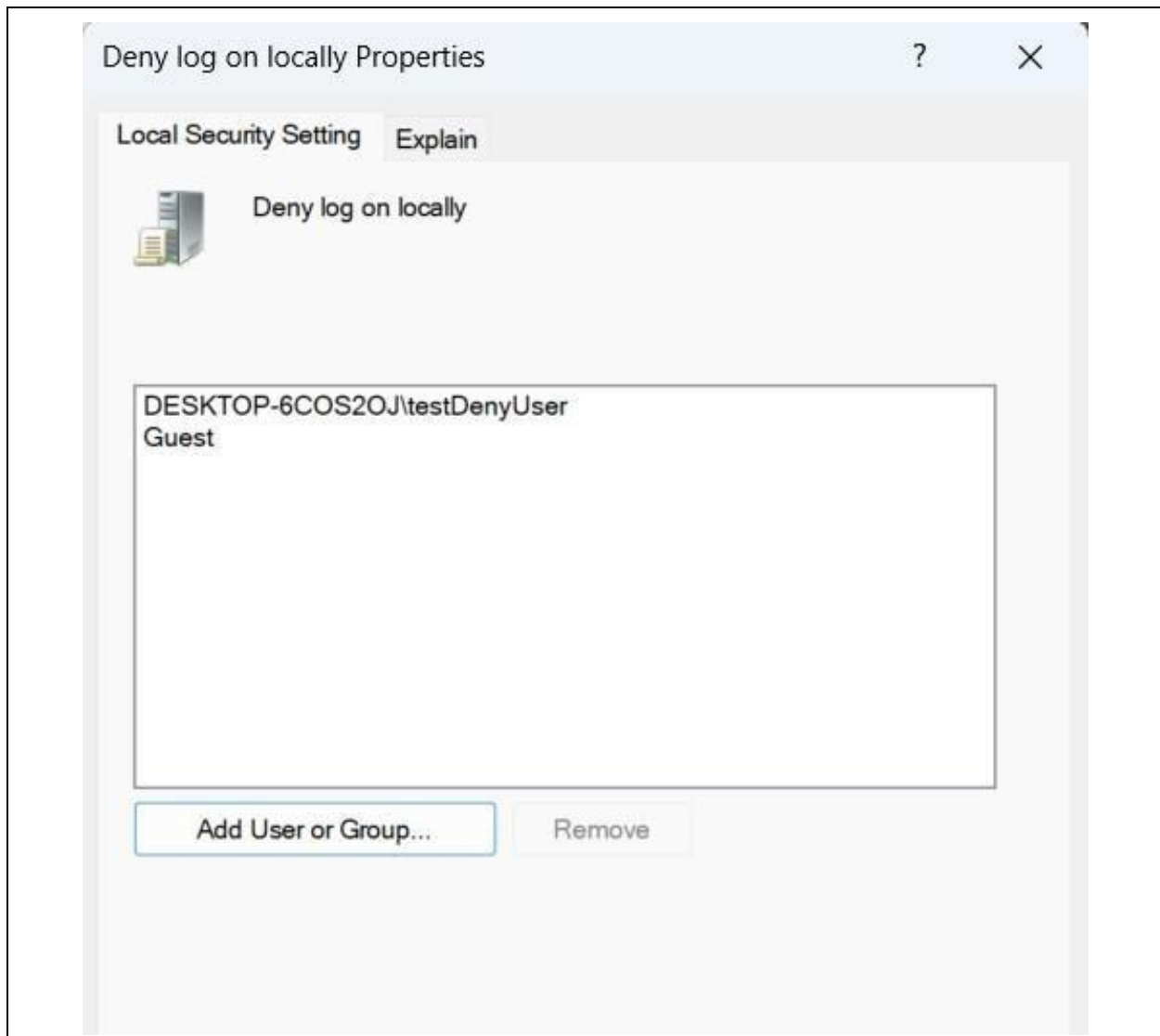


Figure 6: Security options — administrator and guest accounts renamed; 'Do not display last user name' enabled to prevent login screen account enumeration.

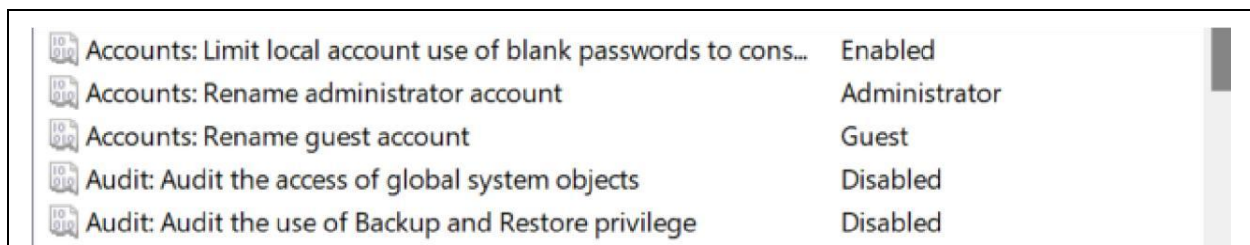


Figure 7: Event Viewer Security Log overview after audit policy activation — multiple recorded entries confirm that logging is operational across all configured categories.



Figure 8: Account lockout triggered after three consecutive failed login attempts — the locked status is visible in Local Users and Groups, confirming policy enforcement.

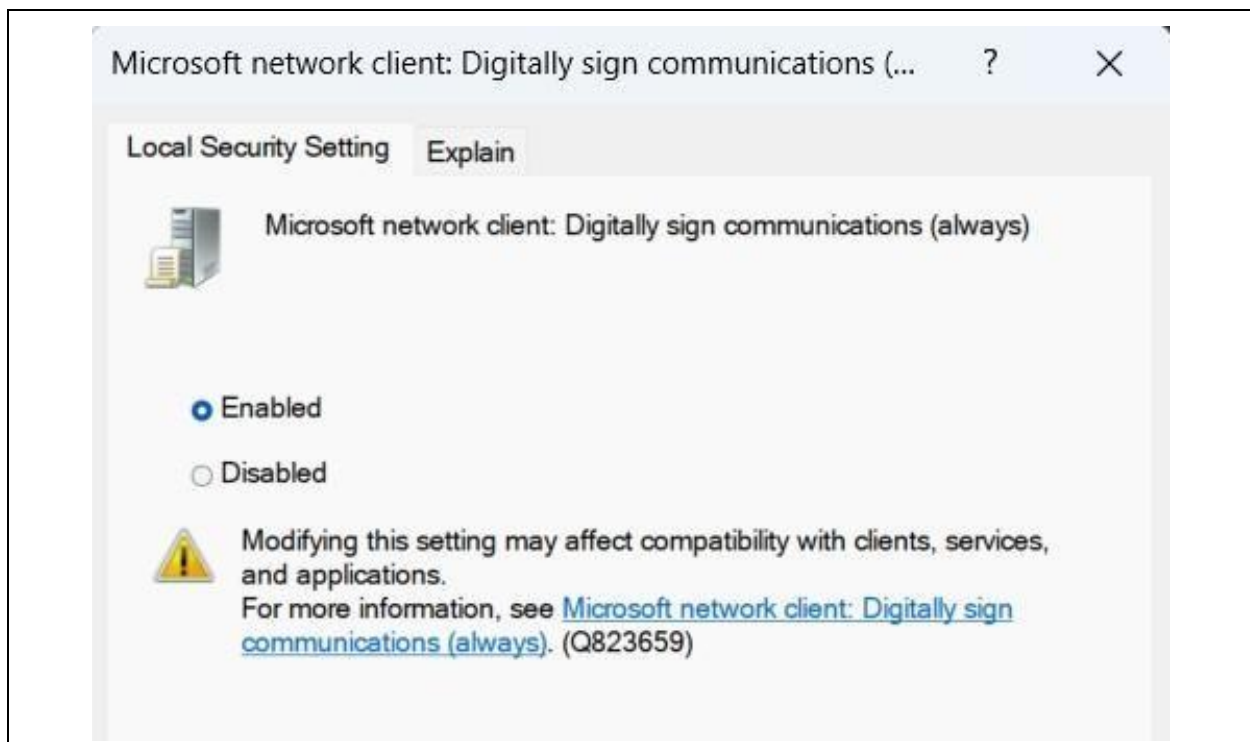


Figure 9: Event Viewer displaying Event ID 4740 (Account Lockout) alongside Event ID 4625 (Failed Logon) entries — validates the end-to-end enforcement of the lockout policy.

7. Testing & Validation

All security controls were functionally tested after configuration. Each test attempted to trigger the control and verified the expected outcome through live system response and Event Viewer log review.

Test	Method	Expected Outcome	Result
Password Complexity	Set a 3-character simple password	Policy rejects the password	Pass
Account Lockout	Enter wrong password 3 times	Account locked for 20 minutes	Pass
Audit — Failed Logon	Perform failed login; check logs	Event ID 4625 recorded	Pass
Audit — Account Lockout	Trigger lockout; check logs	Event ID 4740 recorded	Pass
User Rights — Shutdown	Attempt shutdown as standard user	Access denied	Pass
Username Concealment	Log out; observe login screen	Last username not displayed	Pass

8. Key Windows Security Event IDs

Event ID	Event	Significance
4624	Successful Logon	Baseline event; unexpected logons outside business hours may indicate compromise
4625	Failed Logon	Primary indicator of brute-force attempts; high frequency warrants immediate investigation
4740	Account Lockout	Confirms lockout policy activation; may also indicate a forgotten password or intentional DoS against the account
4672	Special Privileges Assigned	Logged when an account with administrative privileges logs on; monitor for unexpected entries

9. Environment-Based Security Design

Security policy settings must be calibrated to the risk profile and operational requirements of each environment. The same core controls are tuned differently across deployment contexts:

Environment	Security Level	Lockout Threshold	Key Focus
Banking / Financial	Very High	3 attempts / 30 min	Strict MFA, full audit trail, real-time alerting
University Lab	Medium	5 attempts / 15 min	Controlled access, audit logging, network segmentation
Home PC	Moderate	10 attempts / 5 min	Usability-balanced: Defender, BitLocker, auto-updates

10. Additional Hardening Recommendations

The controls in this project form a foundational hardening baseline. The following additional measures are recommended for a production environment:

- Enable Windows Defender Firewall with advanced inbound and outbound rules
- Deploy an endpoint detection and response (EDR) solution for behavioral threat detection
- Enable BitLocker Drive Encryption to protect data if physical access is gained
- Enforce timely Windows Update patching — apply security patches within 72 hours of release
- Disable unused services and Windows features (e.g., Remote Registry, LLMNR, Telnet)
- Enable PowerShell Script Block Logging to detect living-off-the-land attacks
- Implement AppLocker to restrict execution to approved applications only

11. Key Skills Demonstrated

Skill Area	Demonstrated Competency
Windows Hardening	Configured password, lockout, audit, user rights, and security option policies via secpol.msc
Policy Configuration	Applied security controls aligned with NIST SP 800-53 principles
Audit Log Analysis	Interpreted Windows Security Event IDs 4624, 4625, and 4740 in Event Viewer
Access Control	Enforced Principle of Least Privilege through User Rights Assignment
Threat Mitigation	Implemented controls addressing brute-force attacks and information disclosure

Security Documentation

Produced a structured technical report suitable for professional portfolio use

12. Lessons Learned

- Security policy configuration requires balancing security strength with usability — overly aggressive lockout thresholds can cause denial-of-service for legitimate users
- Default system configurations are rarely secure — every endpoint should be hardened against a documented baseline before deployment
- Event log analysis is a core blue team skill — correlating Event IDs to attack techniques is fundamental to threat detection
- The Local Security Policy covers standalone systems; Group Policy Objects (GPOs) in Active Directory enable the same controls at enterprise scale
- Defense-in-depth means no single control is sufficient — security emerges from multiple overlapping layers working together

13. Conclusion

This project successfully implemented a system hardening baseline on a Windows 11 endpoint covering all five core security control domains. All configurations were tested and validated against defined objectives, with results confirmed through Event Viewer log analysis.

The applied controls reduce the risk of credential-based attacks, establish a forensic audit trail for incident detection, and enforce the Principle of Least Privilege across user accounts. These techniques are directly applicable to enterprise environments including finance, education, and government, and represent core competencies for a System Security Administrator role.