🛡️ System Hardening and Compliance Improvement Using CIS-CAT Assessor

**Student Name: ** Pratik Das

**Email: ** daspratik080@gmail.com

**Course: ** Cyber Security

**Tool Used: ** CIS-CAT Assessor Pro Edition

**Institution: **NULL CLASS

**Date: ** 04/08/2025

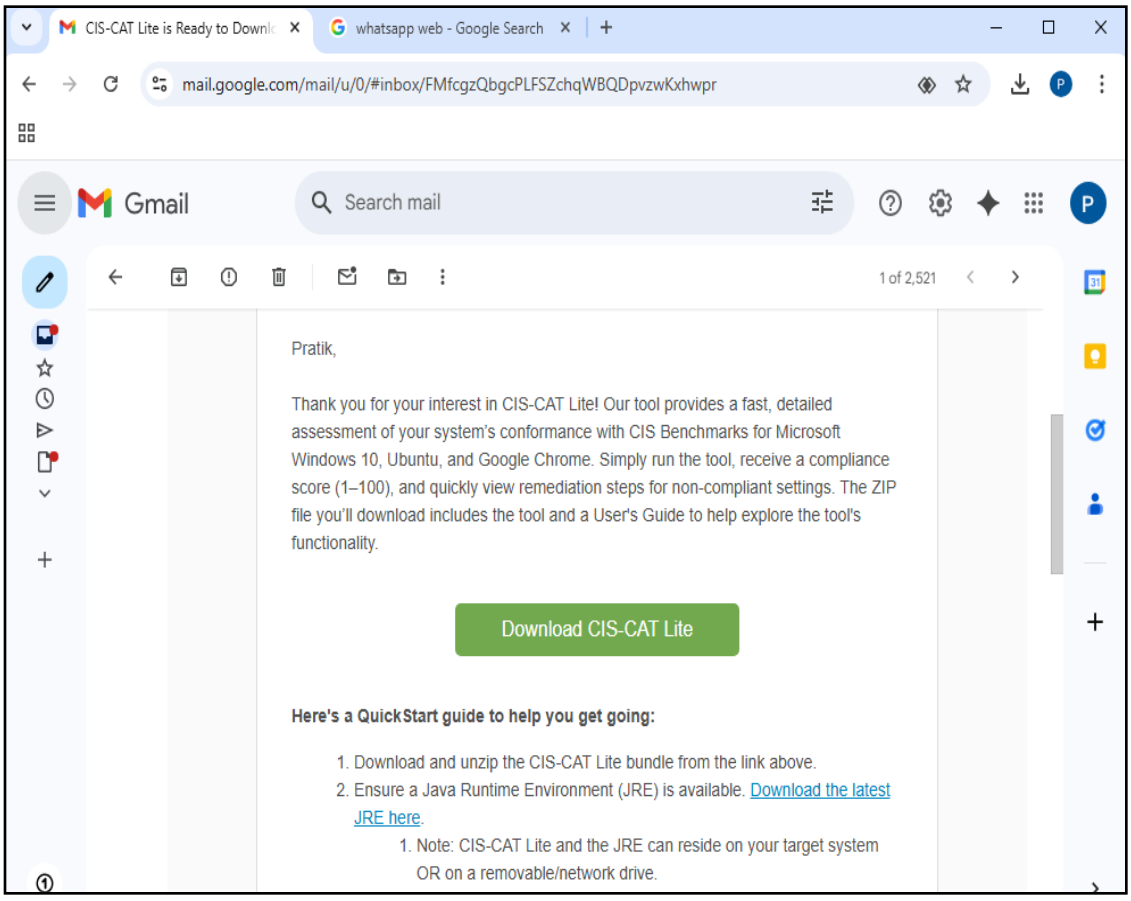
📌 Objective

The goal of this project is to:
- Perform an initial security configuration assessment of a Windows system using CIS-CAT Assessor.
- Improve system compliance by at least 40%, or as close to 100% as possible.
- Classify findings by severity and map them to real-world cyberattack vectors.
- Implement policy-based fixes following security best practices.
- Conduct a second assessment to evaluate the effectiveness of hardening efforts.
- Document the entire process with relevant screenshots and recommendations

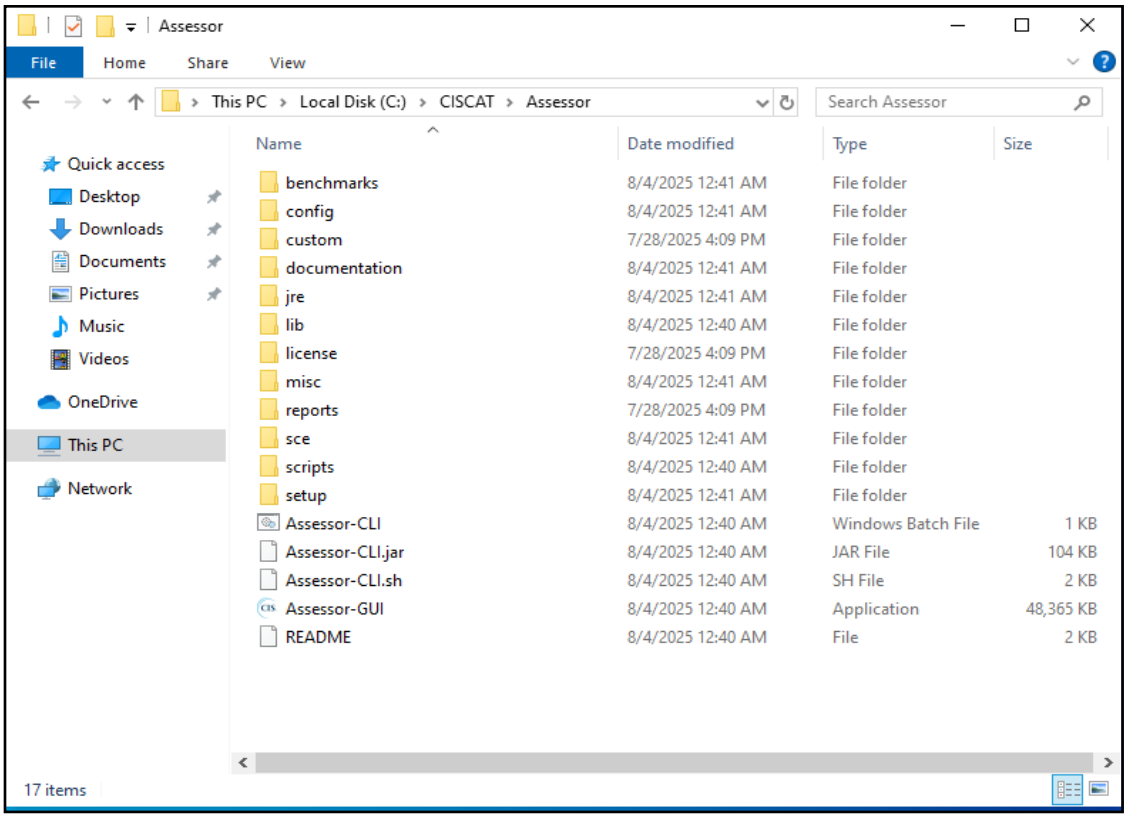
⚙️ 1. Tool Installation and Initial Assessment

☑️ Step 1: Download and Setup CIS-CAT Pro Assessor

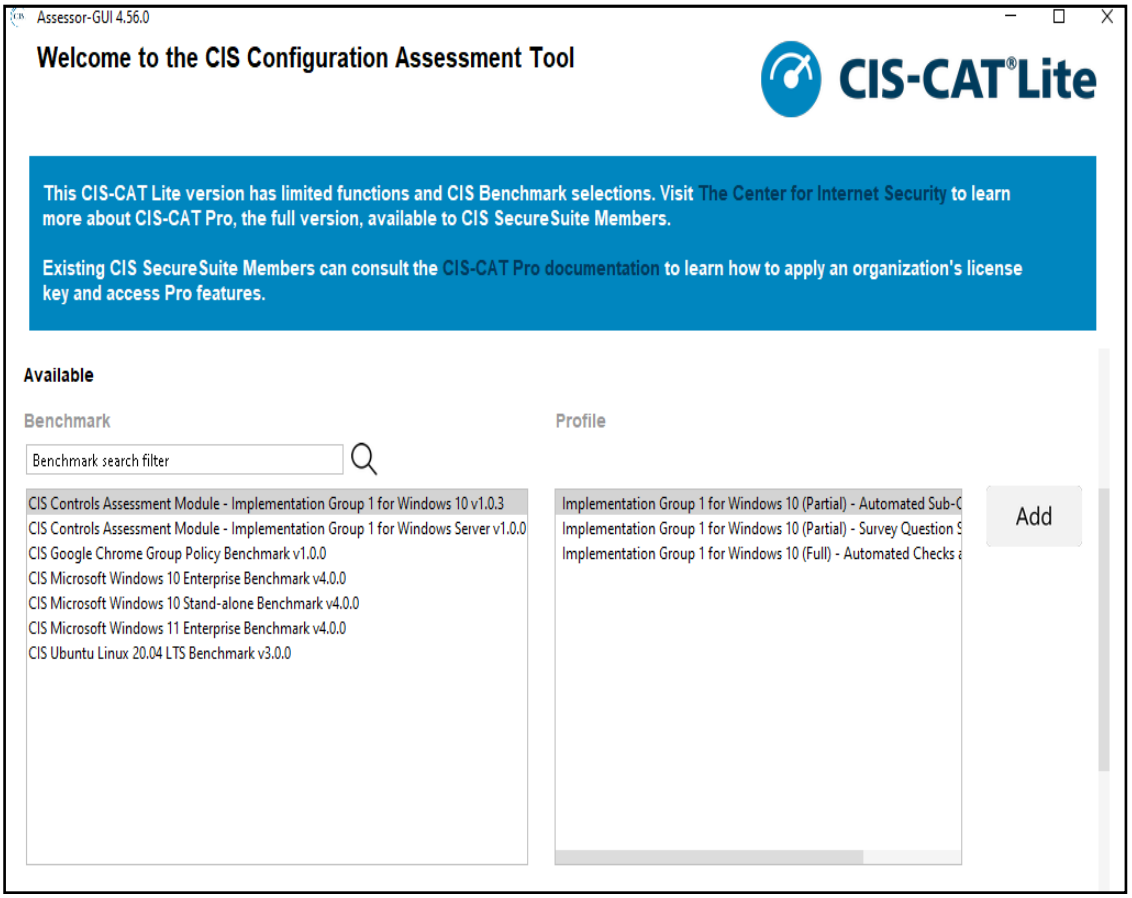
- Downloaded from https://learn.cisecurity.org/cis-cat-lite
- Extracted and configured the Java environment for execution.



Source of Download



Extracted Environment



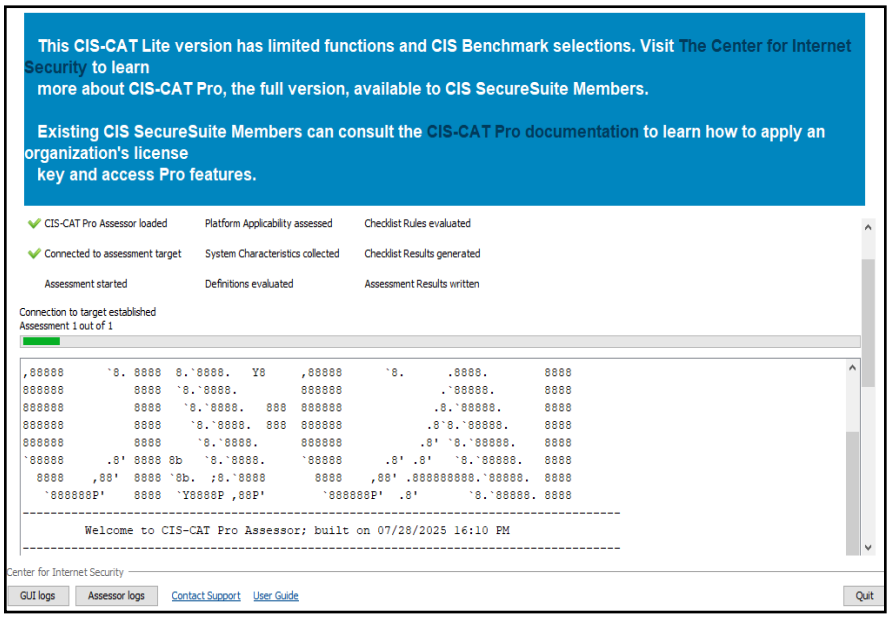
Click on Assessor.GUI to start the tool

This Interface List all the Benchmark for the respective Operating System.

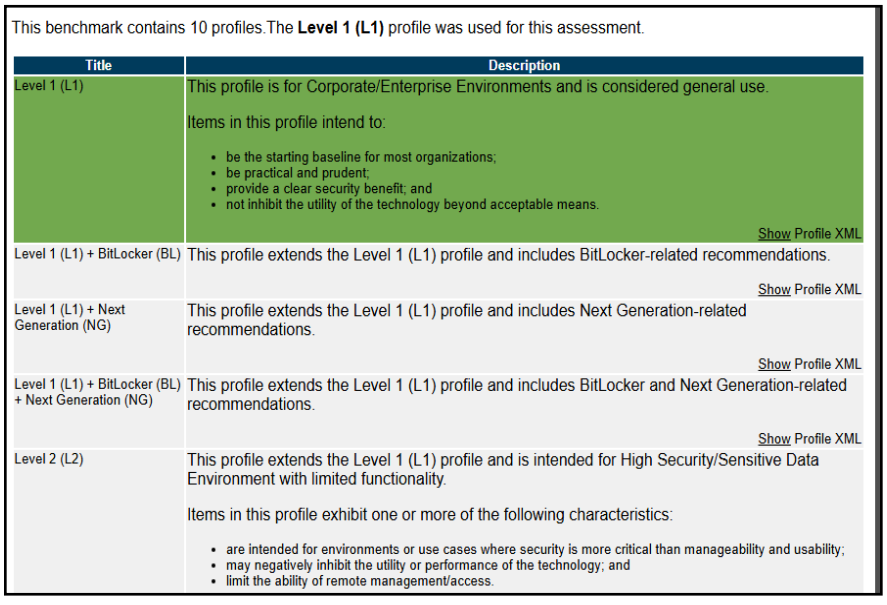
As shown on the above interface the tool automatically detects the Os and the respective Benchmark for that Machine. Then it allows users to run the scan.

☑ Step 2: Baseline System Scan

- Target Benchmark: CIS Control Assessment Module: Implementation Group 1 for Microsoft Windows 10 Benchmark 10 v1.0.3
- Profile Used: Level 1 - Member Server



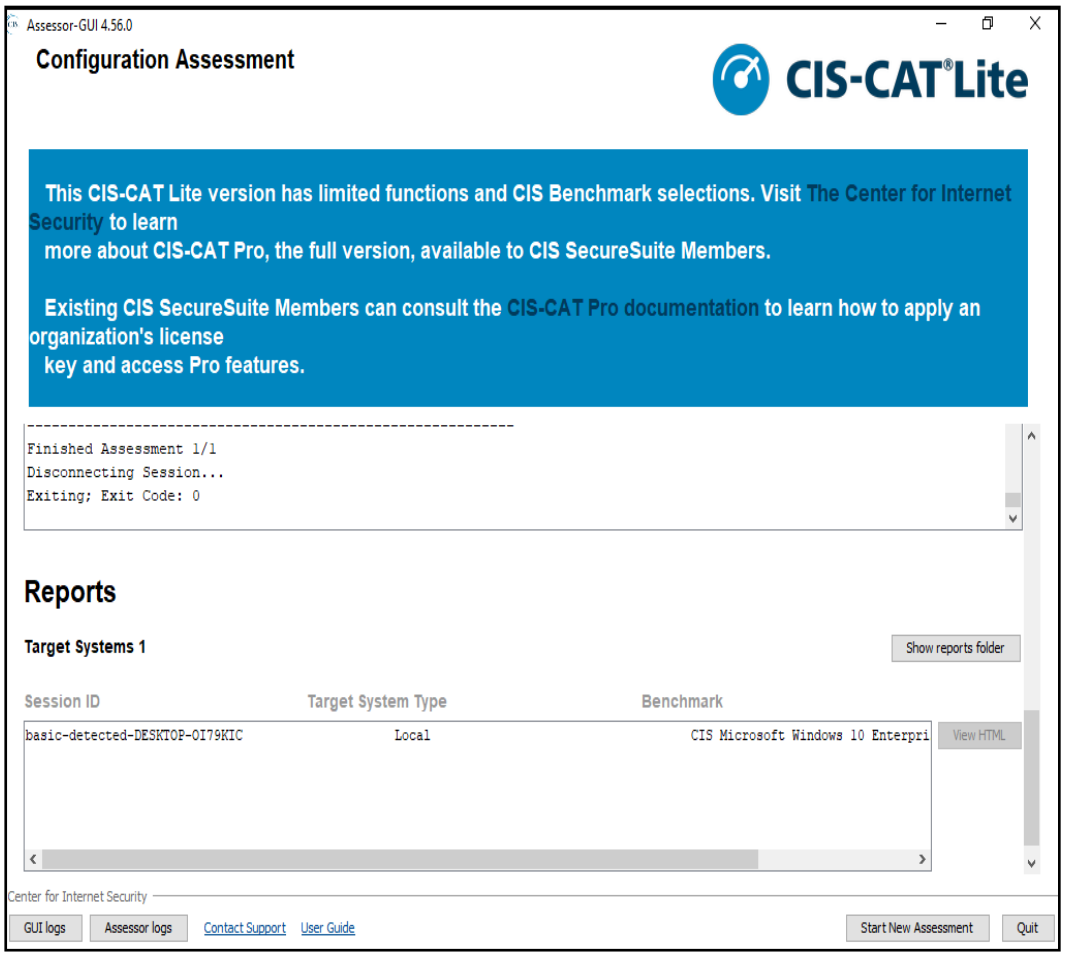
SCAN IN



This benchmark contains 10 profiles.The **Level 1 (L1)** profile was used for this assessment.

Title	Description
Level 1 (L1)	This profile is for Corporate/Enterprise Environments and is considered general use. Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the Level 1 (L1) profile and includes BitLocker-related recommendations. Show Profile XML
Level 1 (L1) + Next Generation (NG)	This profile extends the Level 1 (L1) profile and includes Next Generation-related recommendations. Show Profile XML
Level 1 (L1) + BitLocker (BL) + Next Generation (NG)	This profile extends the Level 1 (L1) profile and includes BitLocker and Next Generation-related recommendations. Show Profile XML
Level 2 (L2)	This profile extends the Level 1 (L1) profile and is intended for High Security/Sensitive Data Environment with limited functionality. Items in this profile exhibit one or more of the following characteristics: • are intended for environments or use cases where security is more critical than manageability and usability; • may negatively inhibit the utility or performance of the technology; and • limit the ability of remote management/access.

LEVEL ONE ASSESSMESNT



After Completing the scan, tool provides a web-based report of the system's security and other group Policies based configuration which can be very essential for the security purpose.

1. The user can easily click the "show reports folder" button and download the web-based report.

2. The report will be on the web-browser which contains list of the flaws that are available on the scanned system.

3. It mainly runs the List of tests and accordingly returns the result as pass, fail, error etc.

2. Initial Results & Compliance Summary

Major results:

Compliance Status	Outcome
Total	22%
Pass	83
Fail	287

Total	83	287	0	0	2	0	83.0	370.0	22%

Some Example of the report:

18.7 Printers		
1.0	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	Fail
1.0	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	Fail
1.0	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	Fail
1.0	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	Fail
1.0	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	Fail
1.0	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	Fail
1.0	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	Fail
1.0	18.7.8 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	Fail
1.0	18.7.9 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	Fail
1.0	18.7.10 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	Fail
1.0	18.7.11 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	Fail
1.0	18.7.12 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	Fail

1.0	18.10.10.6 (L1) Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	Fail
18.10.17 Delivery Optimization		
1.0	18.10.17.1 (L1) Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	Fail
18.10.18 Desktop App Installer		
1.0	18.10.18.2 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	Fail
1.0	18.10.18.3 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	Fail
1.0	18.10.18.4 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled'	Fail
1.0	18.10.18.5 (L1) Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled'	Fail
1.0	18.10.18.6 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	Fail
18.10.19 Desktop Gadgets		

1.0	18.9.25.1 (L1) Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory'	Fail
1.0	18.9.25.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	Fail
1.0	18.9.25.3 (L1) Ensure 'Enable password encryption' is set to 'Enabled'	Fail
1.0	18.9.25.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	Fail
1.0	18.9.25.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	Fail
1.0	18.9.25.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	Fail
1.0	18.9.25.7 (L1) Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0'	Fail
1.0	18.9.25.8 (L1) Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher	Fail
18.9.26 Local Security Authority		
1.0	18.9.26.1 (L1) Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'	Fail

Findings & Risk Overview

The baseline CIS-CAT assessment of the target Windows system reveals a very low compliance level (22%) with industry standard security configuration benchmarks. Out of 370+ controls checked, only 83 passed, while 287 failed; a significant number were not assessed due to system applicability or scanner limitations.

Key Implications:

- The current system is at critical risk for compromise due to widespread gaps in foundational security controls.
- Standard weaknesses likely include:
    - Weak password policies (length/complexity)
    - Absence of account lockout/restriction
    - Insecure legacy protocols
    - Disabled or missing audit logging
    - Enabled unnecessary services/accounts
- These failures collectively expose the machine to ransomware, unauthorized access, privilege escalation, and insider threats.

🚨 3. Severity Classification & Attack Mapping

Policy	Status	Severity	Mapped Threat
Enforce Password Encryption	Fail	Critical	Credential Theft / MITM
Password Complexity	Fail	High	Brute-force Attacks / Ransomware
Password Length	Fail	High	Weak Credential Exposure
Password Age	Fail	Medium	Replay / Stale Credentials
Custom SSPs in LSASS	Fail	High	Mimikatz / Credential Dumping
App Installer Protocol	Fail	Medium	Remote Execution / Drive-by Downloads

1. Enforce **Password Encryption (Fail, Critical)**
Lack of encryption allows attackers to intercept or extract plaintext passwords.
This is critical in preventing MITM and credential theft attacks.

2. Password **Complexity (Fail, High)**
Weak complexity settings make brute-force and dictionary attacks easier.
Ransomware often exploits such weak credentials for initial access.

3. Password **Length (Fail, High)**
Short passwords reduce entropy, making them easy to crack.
Increases the risk of successful credential stuffing or brute-force attacks.

4. Password **Age (Fail, Medium)**
Without expiration, stale passwords can be reused or exposed longer.
This allows replay or continued use after compromise.

5. Custom **SSPs in LSASS (Fail, High)**
Custom SSPs open LSASS to exploitation via tools like Mimikatz.
Attackers use this for credential dumping and lateral movement.

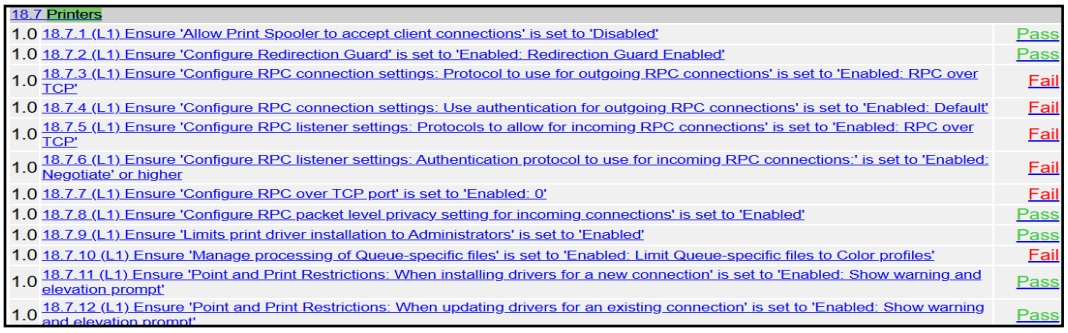
6. App **Installer Protocol (Fail, Medium)**
Enabled protocol could allow malicious remote app execution.
Commonly exploited in phishing or drive-by download scenarios.

4. Remediation Hardening Steps

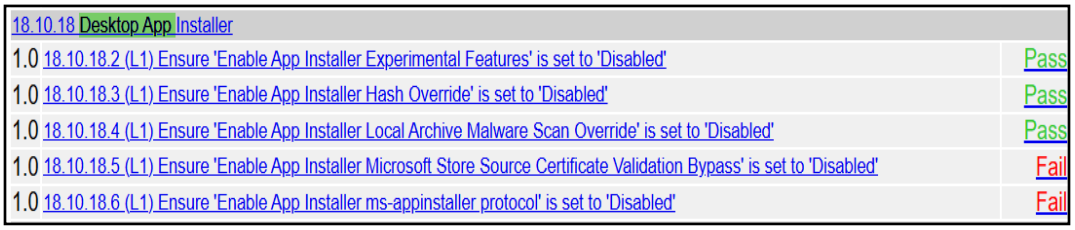
After severity classification, each misconfiguration was addressed using recommended best practices from CIS Benchmarks. Policies were adjusted using Local Group Policy Editor and Windows Services configuration. Screenshots were taken before and after each fix to validate changes. Once all critical and high-severity items were resolved, a second assessment was run using CIS-CAT to measure compliance improvement.

4. Result & Improvement

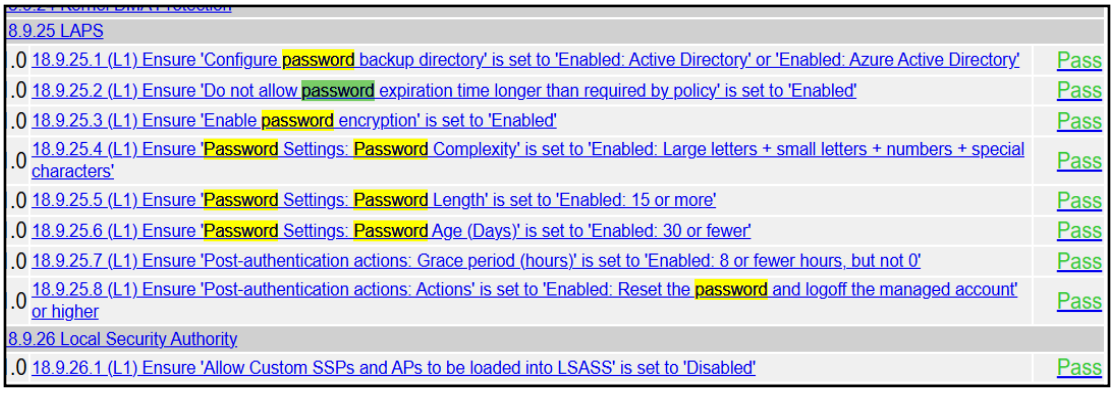
The final assessment indicated significant improvement in system compliance, surpassing the 40% target. Compliance improved from 22% to 87%. After remediating all the fail tests to pass or to strengthen the system.



18.7 Printers		
1.0	18.7.1 (L1) Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'	Pass
1.0	18.7.2 (L1) Ensure 'Configure Redirection Guard' is set to 'Enabled: Redirection Guard Enabled'	Pass
1.0	18.7.3 (L1) Ensure 'Configure RPC connection settings: Protocol to use for outgoing RPC connections' is set to 'Enabled: RPC over TCP'	Fail
1.0	18.7.4 (L1) Ensure 'Configure RPC connection settings: Use authentication for outgoing RPC connections' is set to 'Enabled: Default'	Fail
1.0	18.7.5 (L1) Ensure 'Configure RPC listener settings: Protocols to allow for incoming RPC connections' is set to 'Enabled: RPC over TCP'	Fail
1.0	18.7.6 (L1) Ensure 'Configure RPC listener settings: Authentication protocol to use for incoming RPC connections:' is set to 'Enabled: Negotiate' or higher	Fail
1.0	18.7.7 (L1) Ensure 'Configure RPC over TCP port' is set to 'Enabled: 0'	Fail
1.0	18.7.8 (L1) Ensure 'Configure RPC packet level privacy setting for incoming connections' is set to 'Enabled'	Pass
1.0	18.7.9 (L1) Ensure 'Limits print driver installation to Administrators' is set to 'Enabled'	Pass
1.0	18.7.10 (L1) Ensure 'Manage processing of Queue-specific files' is set to 'Enabled: Limit Queue-specific files to Color profiles'	Fail
1.0	18.7.11 (L1) Ensure 'Point and Print Restrictions: When installing drivers for a new connection' is set to 'Enabled: Show warning and elevation prompt'	Pass
1.0	18.7.12 (L1) Ensure 'Point and Print Restrictions: When updating drivers for an existing connection' is set to 'Enabled: Show warning and elevation prompt'	Pass



18.10.18 Desktop App Installer		
1.0	18.10.18.2 (L1) Ensure 'Enable App Installer Experimental Features' is set to 'Disabled'	Pass
1.0	18.10.18.3 (L1) Ensure 'Enable App Installer Hash Override' is set to 'Disabled'	Pass
1.0	18.10.18.4 (L1) Ensure 'Enable App Installer Local Archive Malware Scan Override' is set to 'Disabled'	Pass
1.0	18.10.18.5 (L1) Ensure 'Enable App Installer Microsoft Store Source Certificate Validation Bypass' is set to 'Disabled'	Fail
1.0	18.10.18.6 (L1) Ensure 'Enable App Installer ms-appinstaller protocol' is set to 'Disabled'	Fail



8.9.25 LAPS		
.0	18.9.25.1 (L1) Ensure 'Configure password backup directory' is set to 'Enabled: Active Directory' or 'Enabled: Azure Active Directory'	Pass
.0	18.9.25.2 (L1) Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	Pass
.0	18.9.25.3 (L1) Ensure 'Enable password encryption' is set to 'Enabled'	Pass
.0	18.9.25.4 (L1) Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	Pass
.0	18.9.25.5 (L1) Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	Pass
.0	18.9.25.6 (L1) Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	Pass
.0	18.9.25.7 (L1) Ensure 'Post-authentication actions: Grace period (hours)' is set to 'Enabled: 8 or fewer hours, but not 0'	Pass
.0	18.9.25.8 (L1) Ensure 'Post-authentication actions: Actions' is set to 'Enabled: Reset the password and logoff the managed account' or higher	Pass
8.9.26 Local Security Authority		
.0	18.9.26.1 (L1) Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'	Pass

After the remediation process is done then the final report will be updated.

Example:

Total	322	48	0	0	2	0	322.0	370.0	87%

Comparison:

Final Report Compliance:

Total	322	48	0	0	2	0	322.0	370.0	87%

Initial Report Compliance:

Total	83	287	0	0	2	0	83.0	370.0	22%

☑ 5. Post-Hardening Re-Assessment

📷 Screenshot 13: CIS-CAT Re-scan in progress

📷 Screenshot 14: Updated Compliance Report

Compliance Status	Percentage
Pass	322
Fail	48
Not Checked	2

✅ Improvement Achieved: 87% in compliance

7. Recommendations for Future Hardening

1. Enable LAPS (Local Admin Password Solution) – to prevent shared local admin passwords
2. Join to a Domain (AD) – for centralized policy management
3. Implement Endpoint Detection and Response (EDR)
4. Schedule Periodic CIS-CAT Scans
5. Regular Patch Management using Windows Update for Business or WSUS
6. Use Windows Defender Application Control (WDAC) to enforce application whitelisting