**INFORMATION SECURITY**



**Session 2023 - 2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Mam Faiza Iqbal

**Course:**

Information Security

Department of Computer Science

**University of Engineering and Technology**

**Lahore Pakistan**

Contents

[**Implementing Security Policies and Compliance Standards** 3](#_Toc191661606)

[**1.** **Lab Task 1:** 3](#_Toc191661607)

[**2.** **Lab Task 2:** 3](#_Toc191661608)

[**a.** **Enforcing Policies on Windows:** 3](#_Toc191661609)

[**b.** **Enforcing Policies on Linux** 6](#_Toc191661610)

[**c.** **Compliance Verification:** 8](#_Toc191661611)

[**d.** **Incident Simulation and Login Attempts** 10](#_Toc191661612)

# **Implementing Security Policies and Compliance Standards**

# **Lab Task 1:**

Policy is already described in previous lab which can be accessed through following link

[Security Policy Task](https://docs.google.com/document/d/1hOyNgXLzw2eNtc231haUUV1SWTXwZG_W/edit?usp=sharing&ouid=101030228409717981607&rtpof=true&sd=true)

# **Lab Task 2:**

# **Enforcing Policies on Windows:**

**Configuring Password Policy:**

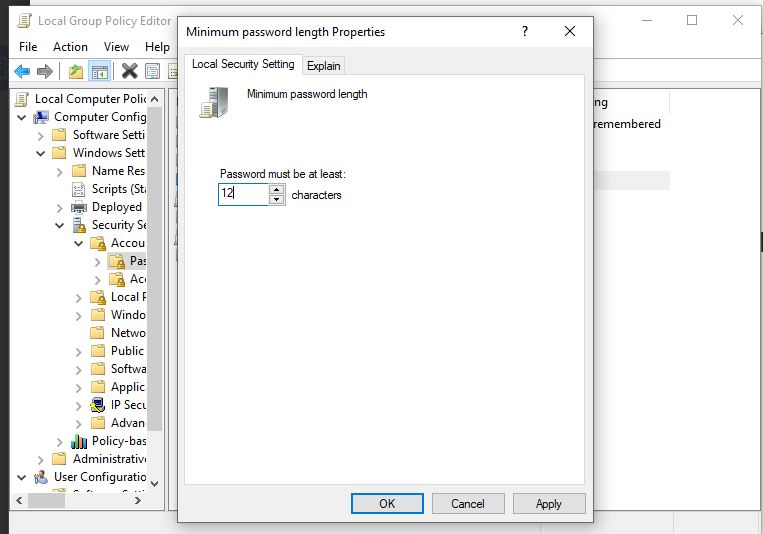
****

Fig1: Set password to minimum length of 12

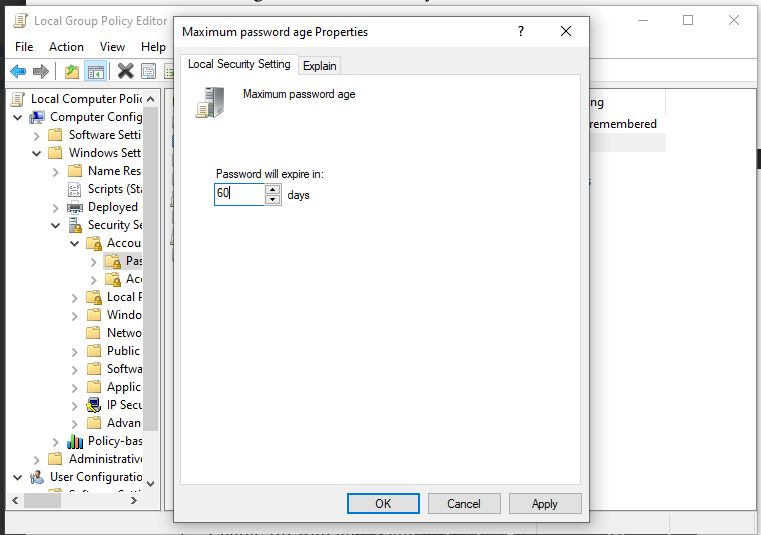


Fig:2 Enabling Password Expiration

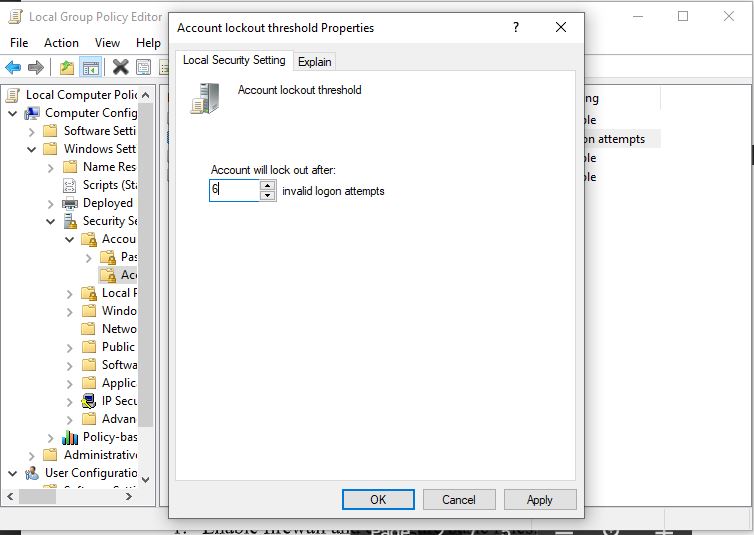


Fig3: Account lockout

**Configuring Internet Policies:**

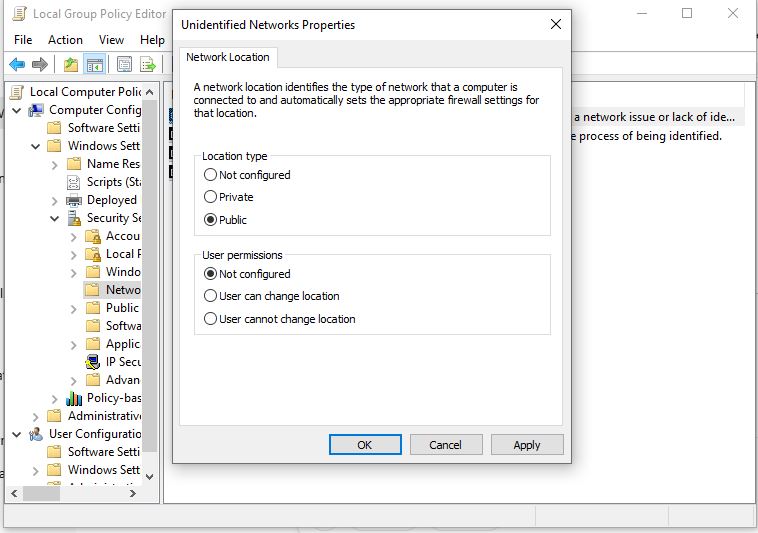
****

Fig4: Blocks Access

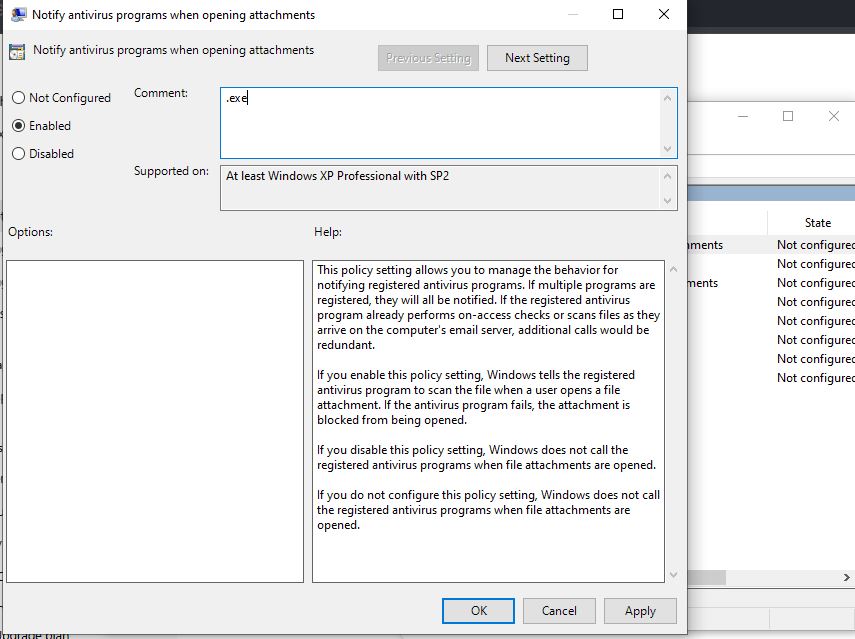


Fig5: Restrict Executable Downloads

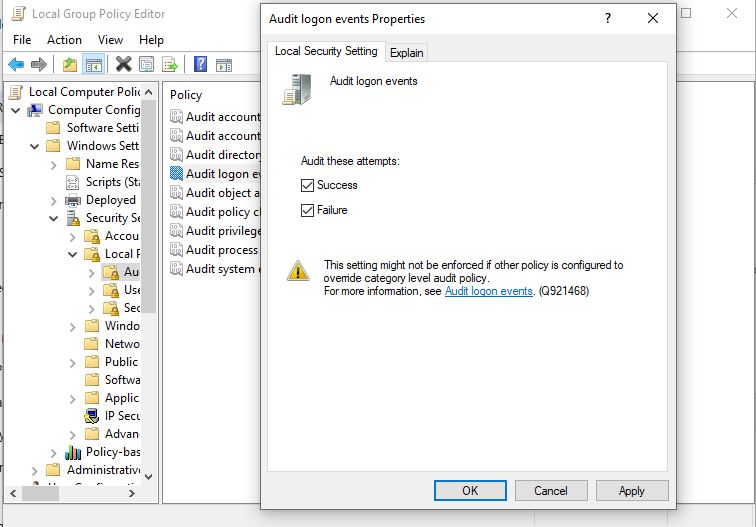


Fig6: Audit for unauthorized access

# **Enforcing Policies on Linux**

**Enable Firewalls and configuring Basic Rules:**

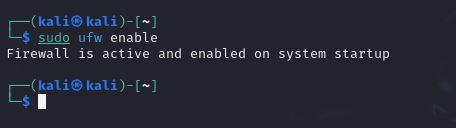
****

Fig7: Enabling FireWall

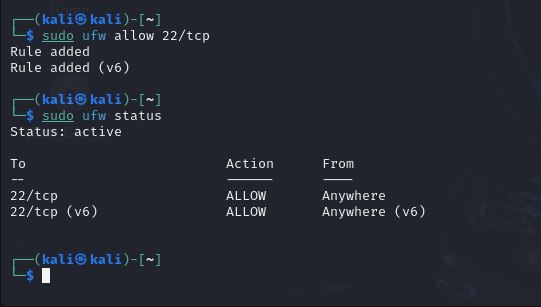


Fig8: Allowing TCP

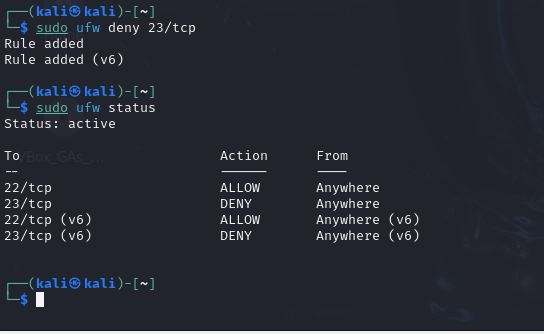
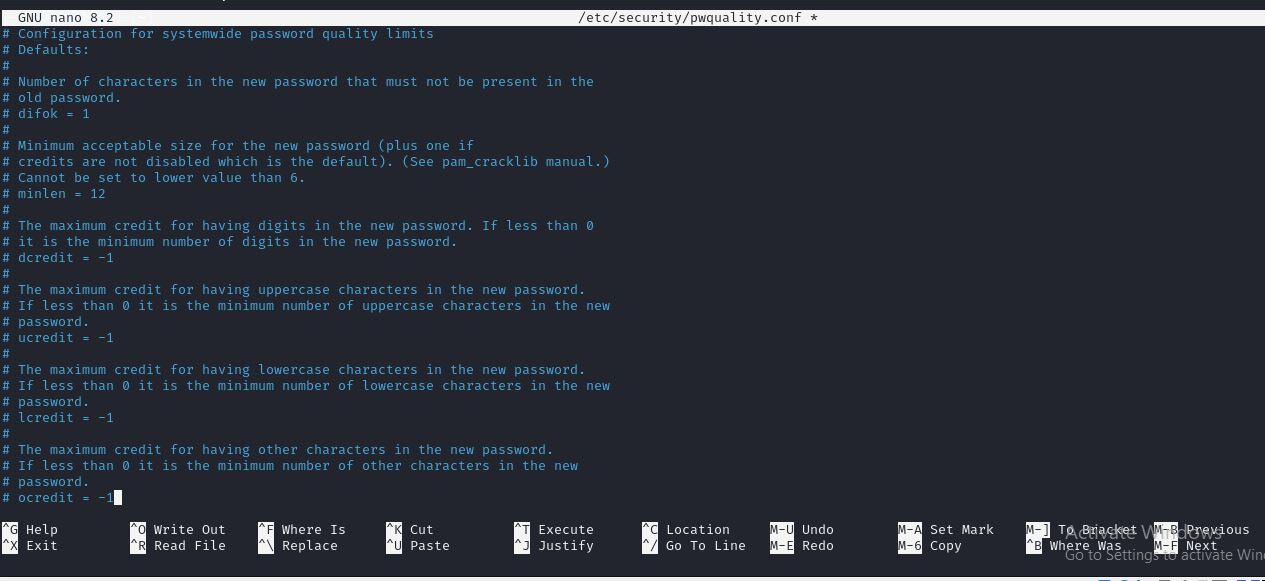


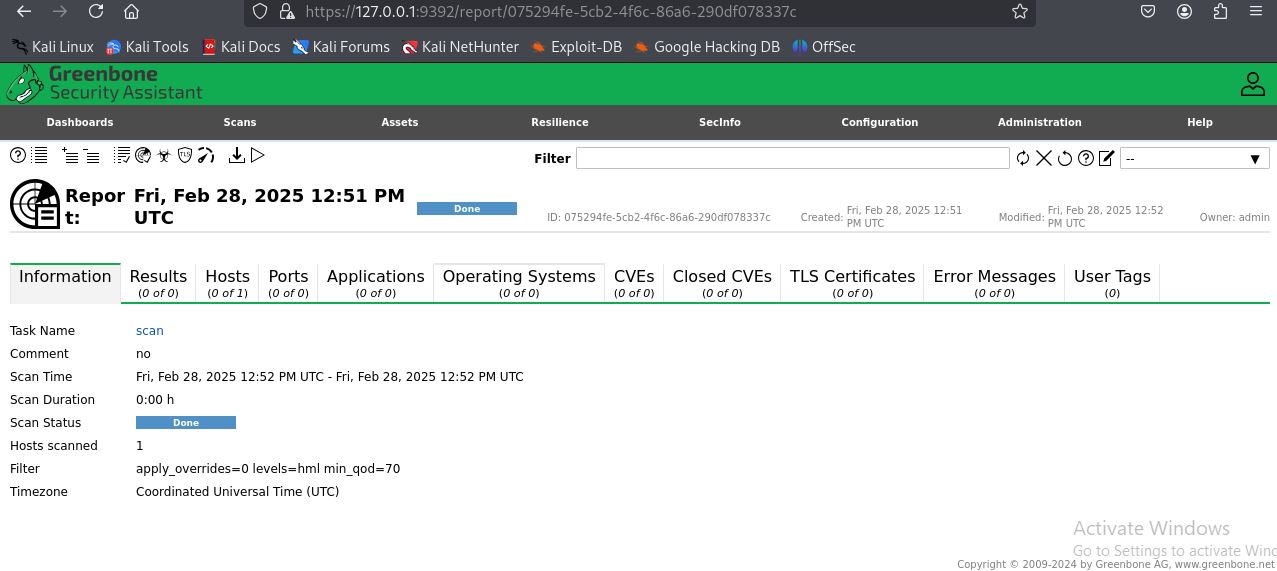
Fig9: Denying TCP

**Configuring Password Policies:**

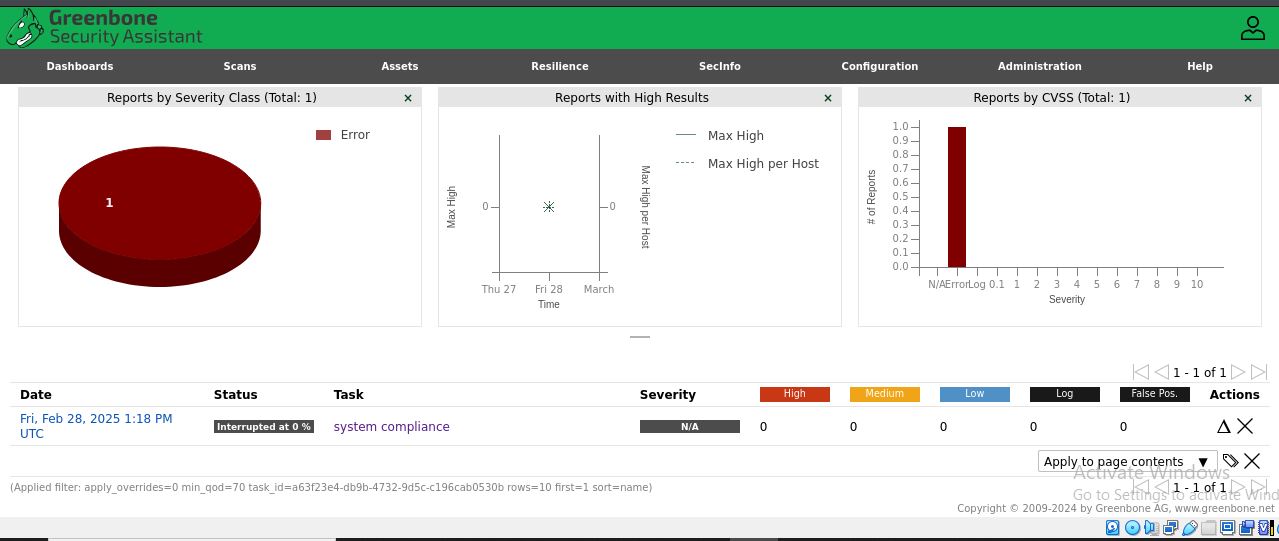
****

**Fig10: Setting up Password Policies**

# **Compliance Verification:**



**Fig 11: Verification scan using OpenVAS**

****

**Fig 12: Generating Reports**

**Comparison with ISO and NIST**

**A. ISO 27001 Compliance Check**

| **ISO 27001 Control** | **Findings from Scan** | **Issue** |
| --- | --- | --- |
| A.9.1.2 - User Access Management | Weak passwords found | High risk of unauthorized access |
| A.12.1.1 - Malware Protection | No antivirus detected | System vulnerable to malware |
| A.14.2.2 - Secure Development | Open ports detected | Possible security risk |

**B. NIST 800-53 Compliance Check**

| **NIST 800-53 Control** | **Findings from Scan** | **Issue** |
| --- | --- | --- |
| AC-2 - Account Management | Unused accounts active | Potential insider threats |
| SI-2 - Flaw Remediation | Unpatched software found | Exploitable vulnerabilities |
| SC-7 - Boundary Protection | Open SSH/FTP ports | Attack surface too large |

**Findings and Recommendations:**

According to the generated report four categories of Risks was Identified:

 High & Critical vulnerabilities

 Misconfigurations

 Outdated software

 Weak authentication settings

It can be resolved using :

**A. Secure Authentication**

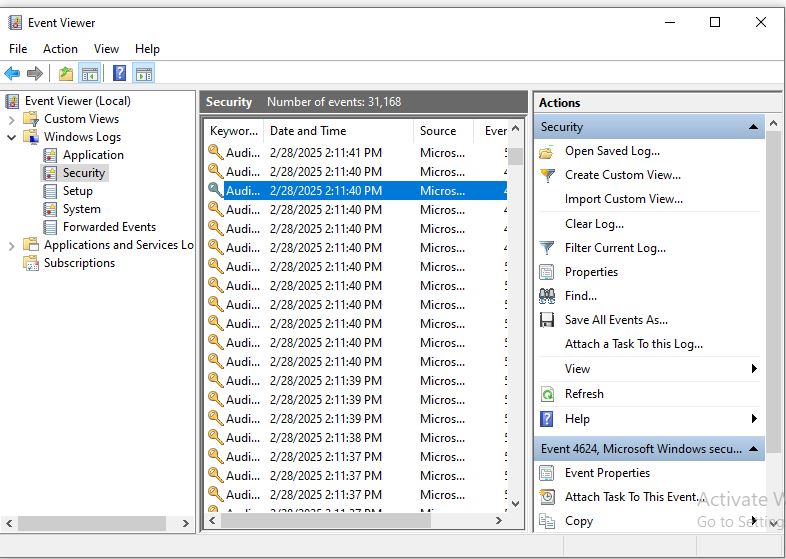
* Enforce **multi-factor authentication (MFA)**.
* Disable unused accounts and enforce **password rotation**.

**B. Patch & Update**

* Update all software and apply **security patches** regularly.
* Use **automatic updates** where possible.

# **Incident Simulation and Login Attempts**

**Windows:**

****

**Fig11: Event Viewer**

**Linux**