Image Security

Score: 85/100 (Passed)

Platform: Windows 11 Image (Aeacus Scoring Engine)

Category: Forensics

You can view the original challenge here: Advent of CTF 2025 - Image Security.

I. Forensics (Digital Forensics Investigation)

Question 1: Decrypt the intercepted message

- **Ciphertext:** `Xyebl V czkhijj klue go l qmueji'w tal? Tsmm ijy dshe yogcdg ssu qerr tpkhmjfki`
- **Methodology:**
  1. Based on the hint "very old cipher" and the text structure, I identified this as a **Vigenère Cipher**.
  2. Utilized **CyberChef** (or dcode.fr) for analysis. You can view the full decoding recipe here: CyberChef Solution.
  3. Key identified: `FREQANALYSIS` (Hinting at Frequency Analysis).
  4. Decoded the text, revealing a quote from Shakespeare's Sonnet 18.
- **Answer:** `Shall I compare thee to a summer's day? Thou art more lovely and more temperate`

Question 2: Startup Script Identification

- **Methodology:**
  1. Inspected **Task Manager** → **Startup Apps** tab.
  2. Identified a suspicious executable named `jokehaha.exe` enabled at startup.
  3. Verified the execution path via the **Details** tab (enabled Command Line column).
- **Answer:** `jokehaha.exe`

Question 3: Reverse Engineering Encrypt Tool

- **Artifact:** `encrypt.exe` found on the Desktop.
- **Analysis:**

  1. **Identification:** Identified the file as a **PyInstaller** packed executable using `Detect It Easy (DiE)` and string analysis.
  2. **Extraction:** Used `pyinstxtractor.py` to extract the contents and retrieved the bytecode file `encrypt.pyc`.
  3. **Decompilation:** Used `pycdc.exe` **(Decompyle++)** to decompile the `.pyc` file back to the original Python source code.

  Decompiled Code Result:

```python
# Source Generated with Decompyle++
# File: encrypt.pyc (Python 3.11)
import base64

def e(t):
    p = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]
    k = 165
    b = []
    for i, c in enumerate(t):
        a = ord(c)
        m = p[i % len(p)]
        x = a * m ^ k  # Encryption Logic
        b.append(x.to_bytes(2, 'big'))
    return base64.b64encode(b''.join(b)).decode('utf-8')
```

  4. **Decryption Logic:**
     - Encryption Algorithm: `x = (ASCII * Prime) XOR Key`.
     - Decryption Algorithm (Inverse): `ASCII = (Encoded_Value XOR Key) / Prime`.
     - I wrote a Python script to reverse the process and retrieve the flag.

```python
import base64

# Encrypted string from the challenge
```

```
encoded_str = "AEUBzgKoA6cEVAVBBtQIoQkRC9QNaw9kE8QQ0xIuFvkZMBy7GsobGRwhHnk="

# Constants extracted from decompiled code
p = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]
k = 165

# Step 1: Decode Base64 to bytes
data_bytes = base64.b64decode(encoded_str)

ans = ""

# Step 2: Iterate through every 2 bytes (Big Endian format)
for i in range(0, len(data_bytes), 2):
    chunk = data_bytes[i:i+2]

    # Convert bytes to integer
    x = int.from_bytes(chunk, 'big')

    # Calculate index to find the corresponding prime number
    char_index = i // 2
    m = p[char_index % len(p)]

    # Inverse logic:
    # Original: x = (a * m) ^ k
    # Reverse:  a = (x ^ k) // m
    val_after_xor = x ^ k
    ascii_val = val_after_xor // m

    ans += chr(ascii_val)

print("Decoded message:", ans)
```

- **Answer:** `pyinstallermybeloveddd`

II. User & Group Management

Objective: Ensure only authorized users (per README) have system access, remove unauthorized accounts, and enforce the Principle of Least Privilege.

Remediation Steps:

1. Remove Unauthorized User

- **Finding:** Identified user `Grinch`, who was not listed in the "Authorized Users" or "Administrators" section of the README.
- **Action:**
  - Executed command via CMD (Admin):

```
net user Grinch /delete
```

  - *(Alternative: `lusrmgr.msc` → Users → Right-click `Grinch` → Delete).*

2. Disable Built-in Administrator

- **Rationale:** The default `Administrator` account has a well-known SID and is a primary target for brute-force attacks. The `Santa` and `Elf` accounts are designated for administration.
- **Action:**
  - Executed command via CMD (Admin):

```
net user Administrator /active:no
```

  - Verified that the account is disabled.

3. Password Management

Based on the *Authorized Administrators* and *Authorized Users* list in the README:

- **A. Restore Administrator Passwords (Santa & Elves):**
  - **Rationale:** The README warned that authorized passwords might have been changed. Resetting them ensures authorized access control.
  - **Action:** Reset passwords for `Santa`, `Elf1`, `Elf2`, `Elf3`, and `Elf4` to the specific values provided in the README.

```
net user Santa "Chr157m45C4r0l5!"
net user Elf1 "M3rryChr157m45"
net user Elf2 "W0rk1ngH4rd."
net user Elf3 "Santa1"
net user Elf4 "1ts_71M333!"
```

- **B. Enforce Strong Passwords for Standard Users:**
  - **Rationale:** Standard users (`Buddy`, `Kevin`, `Frosty`) had weak or unknown passwords.
  - **Action:** Set new, complex passwords (Length > 10, utilizing uppercase, lowercase, numbers, and special characters).

```
net user Buddy "P@ssw0rd123!"
net user Kevin "P@ssw0rd123!"
net user Frosty "P@ssw0rd123!"
```

  - *(Note: `P@ssw0rd123!` is used here as an example of a compliant, complex password).*

4. Audit Administrators Group

- **Rationale:** Enforce Least Privilege. Standard users must not have administrative rights.
- **Action:**
  - Navigated to `lusrmgr.msc` → **Groups** → **Administrators**.
  - **Removed:** `Administrator`, `Guest`, and any standard users (e.g., `Kevin`, `Buddy`) found in the group.
  - **Retained:** Only `Santa`, `Elf1`, `Elf2`, `Elf3`, and `Elf4`.

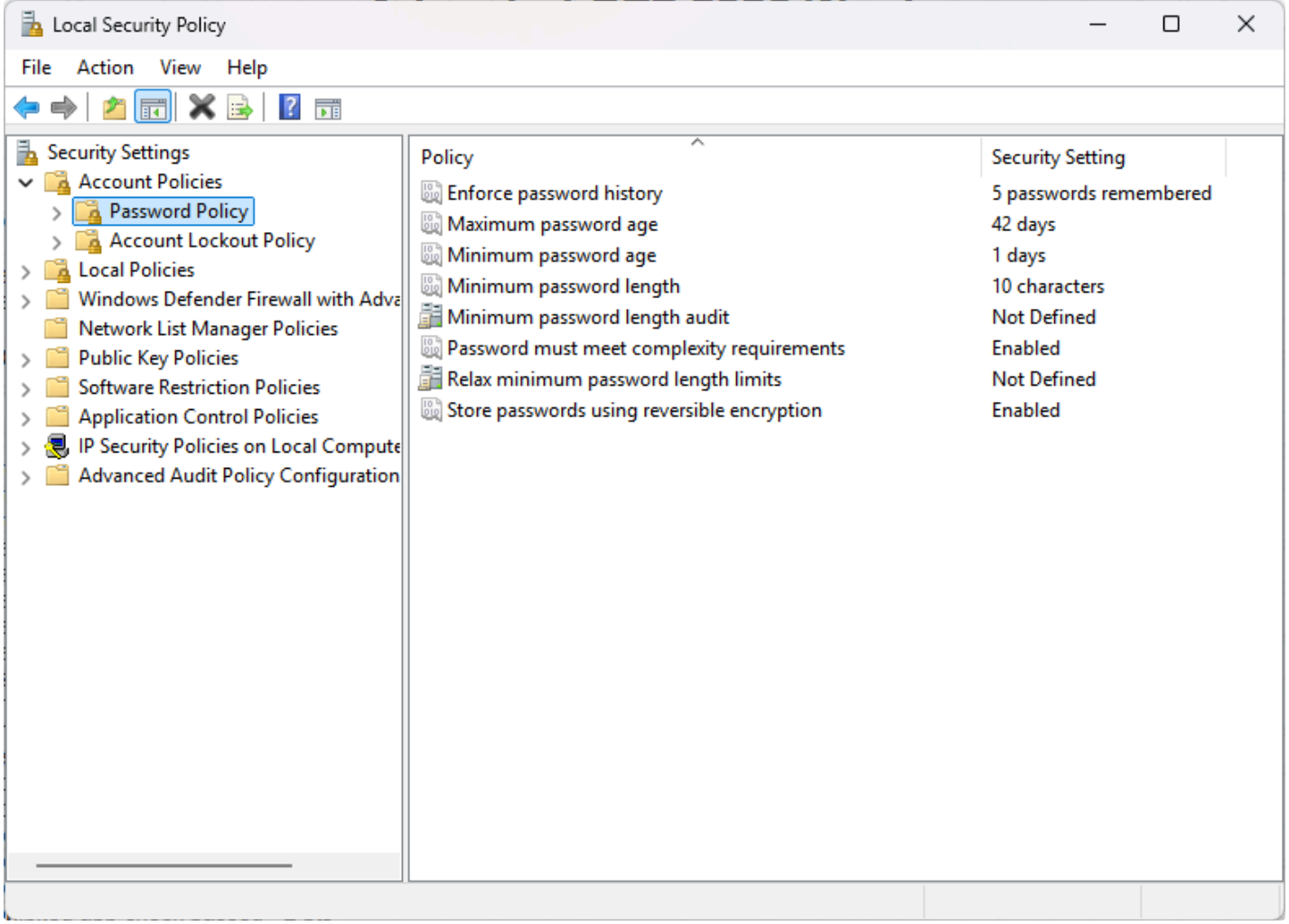
III. Password & Account Lockout Policy

Objective: Enforce strict password requirements and automated lockout mechanisms to mitigate brute-force and dictionary attacks.

Tool: `secpol.msc` (Local Security Policy) → **Account Policies**.

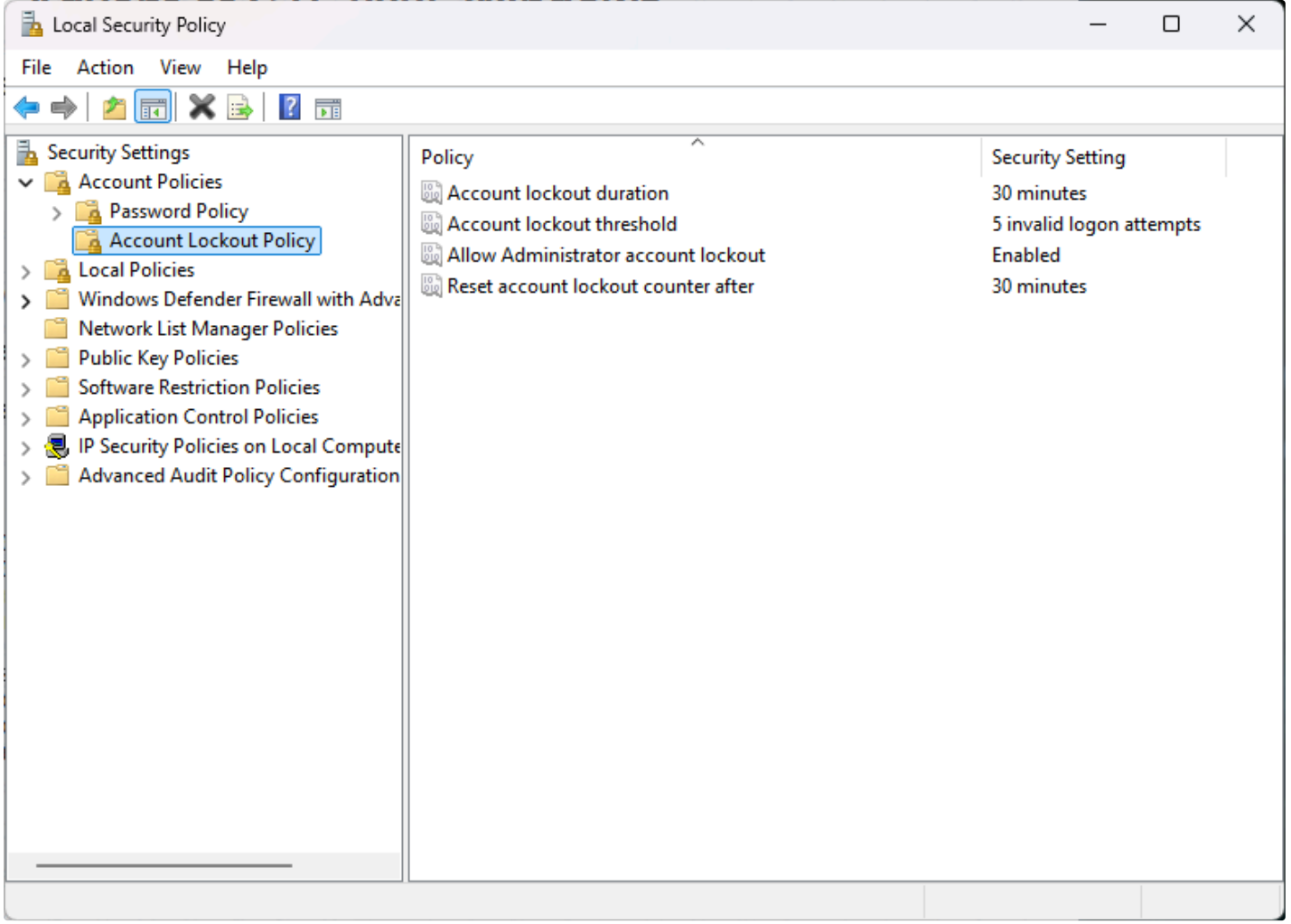
1. Password Policy

- **Maximum password age:** Set to **42** or **90** days.
  - *Rationale:* Ensures periodic password rotation; limits the window of opportunity for compromised credentials.
- **Minimum password age:** Set to **1** day.
  - *Rationale:* Prevents users from cycling through passwords immediately to reuse old ones.
- **Minimum password length:** Set to **10 - 12** characters.
  - *Rationale:* Increases the complexity for password cracking tools exponentially.
- **Enforce password history:** Set to **5** passwords remembered.
  - *Rationale:* Prevents password reuse.
- **Password must meet complexity requirements: Enabled**.
  - *Rationale:* Mandates the use of complex character combinations (Uppercase, Lowercase, Numbers, Symbols).



2. Account Lockout Policy

- **Account lockout threshold:** Set to **5** invalid logon attempts.
  - *Rationale:* Locks the account after 5 failures, stopping automated brute-force attacks effectively.
- **Account lockout duration:** Set to **30** minutes.
  - *Rationale:* Forces attackers to wait, significantly slowing down the attack.
- **Reset account lockout counter after:** Set to **30** minutes.
  - *Rationale:* The counter resets after 30 minutes if no further failed attempts occur.



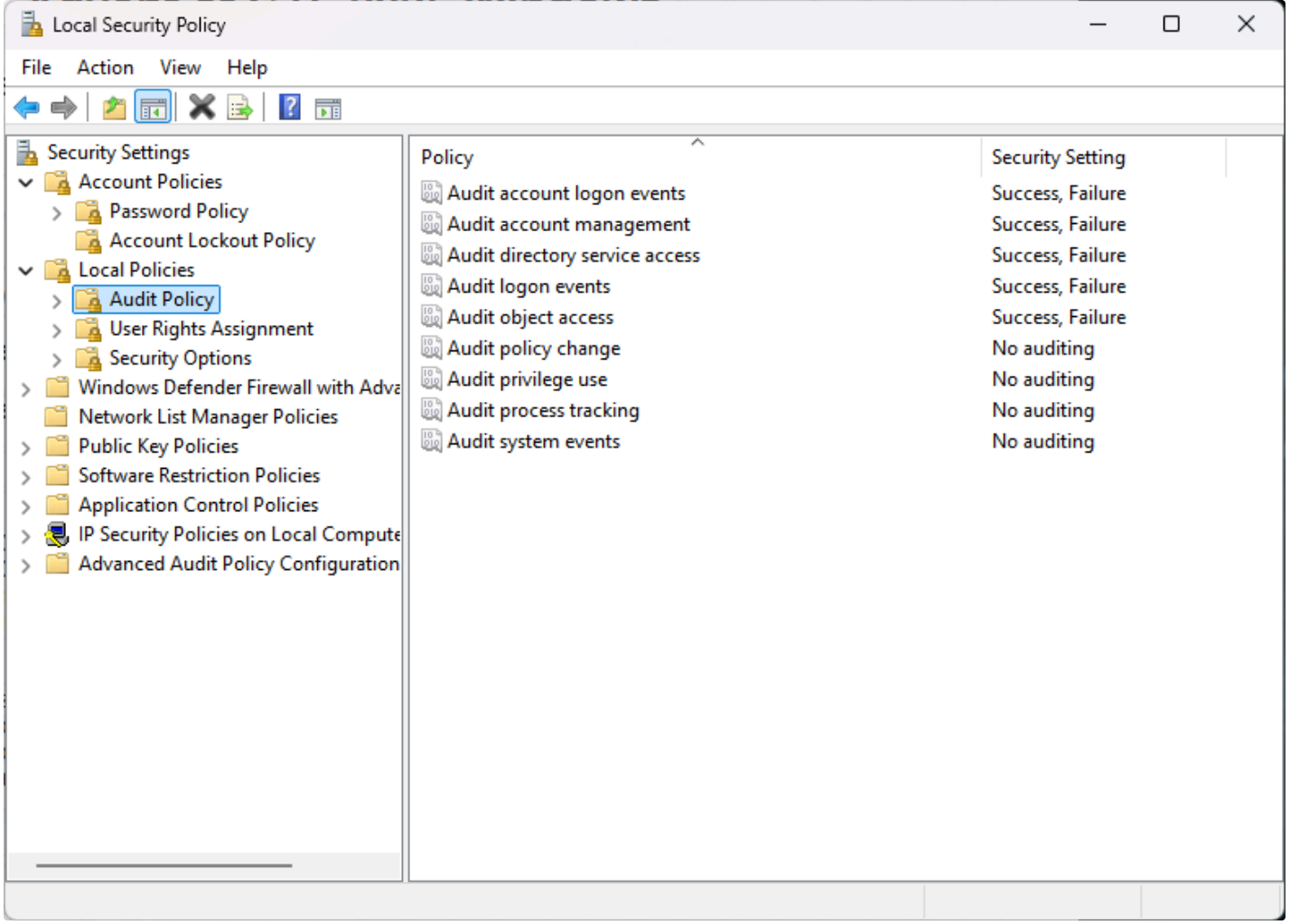
IV. Audit Policy

Objective: Enable logging for critical system events (logons, policy changes, account management) to facilitate security monitoring and incident response (Digital Forensics).

Tool: `secpol.msc` → **Local Policies** → **Audit Policy**.

Detailed Configuration:

- **Audit account logon events:**
  - *Configuration:* **Success, Failure**.
  - *Rationale:* Logs each time a user account is authenticated by this computer (crucial for detecting **Brute-force attacks**).
- **Audit account management:**
  - *Configuration:* **Success, Failure**.
  - *Rationale:* Logs user creation, deletion, password changes, or group membership modifications (detects unauthorized account manipulation).
- **Audit logon events:**
  - *Configuration:* **Success, Failure**.
  - *Rationale:* Logs when a user logs on or logs off the system directly.
- **Audit policy change:**
  - *Configuration:* **Success, Failure**.
  - *Rationale:* Alerts if security policies are intentionally modified (e.g., disabling Audit logging or weakening Password Policy).
- **Audit object access:**
  - *Configuration:* **Success, Failure**.
  - *Rationale:* Tracks access to critical files, folders, or registry keys (requires SACL configuration on specific objects).



V. Local Policies & Security Options

Objective: Harden system security settings to prevent Man-in-the-Middle (MitM) attacks, credential dumping, and information disclosure.

Tool: `secpol.msc` → **Local Policies** → **Security Options**.

1. Hardening Network Communications - SMB Signing

- **Configuration:**
  - `Microsoft network client: Digitally sign communications (always)` → **Enabled**.
  - `Microsoft network server: Digitally sign communications (always)` → **Enabled**.
- **Technical Explanation:**
  - Enforces packet signing for all SMB traffic.
  - Prevents **SMB Relay** and **Man-in-the-Middle** attacks.

2. Hardening Logon Process - Hide Last User Information

- **Configuration:**
  - `Interactive logon: Don't display last signed-in` → **Enabled**.
- **Technical Explanation:**
  - Prevents Windows from displaying the username of the last logged-in user.
  - Attackers with physical access must guess both the **Username** and **Password**.

3. Hardening Credential Protection - Disable Credential Caching

- **Configuration:**
  - `Network access: Do not allow storage of passwords and credentials for network authentication` → **Enabled**.
- **Technical Explanation:**
  - Prevents the OS from caching network credentials.
  - Mitigates credential dumping attacks (e.g., via tools like Mimikatz).

VI. Service Auditing

Objective: Reduce the Attack Surface by disabling unnecessary, risky, or legacy services.

Remediation Steps:

1. Disable Microsoft FTP Service (Critical)

- **Finding:** Service `ftpsvc` was Running.
- **Risk:** FTP uses clear-text transmission, exposing credentials and data.
- **Action:**
  - **Method 1 (GUI):** `services.msc` → Microsoft FTP Service → Stop → Startup Type: **Disabled**.
  - **Method 2 (PowerShell Admin):**

```
Stop-Service "ftpsvc" -Force
Set-Service "ftpsvc" -StartupType Disabled
```

2. Disable Print Spooler

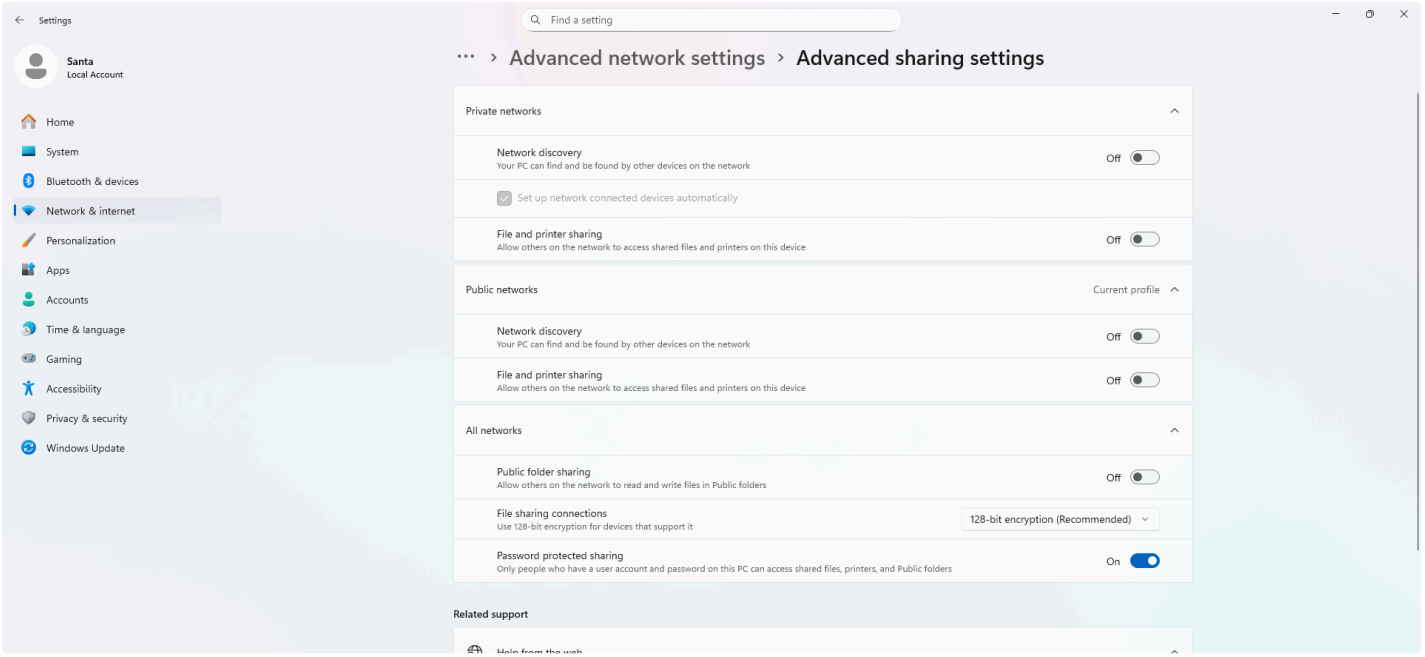
- **Finding:** Service `Spooler` was Running.
- **Risk:** The Print Spooler is vulnerable to exploits (e.g., PrintNightmare) and is unnecessary on a non-print server.
- **Action:** Stopped and set Startup Type to **Disabled**.

3. Verify Other Risky Services

- **Action:** Verified the following services were disabled:
  - **SSDP Discovery (`SSDPSRV`):** Disabled (UPnP risk).
  - **Remote Registry (`RemoteRegistry`):** Disabled (Remote modification risk).
  - **Telnet (`TlntSvr`):** Not installed.

4. Disable File and Printer Sharing

- **Finding:** The `LanmanServer` service was running, allowing SMB file sharing.
- **Action:**
  - **GUI:** Disabled "File and printer sharing" in *Advanced sharing settings*.



  - **Service Level:** Navigated to `services.msc`, stopped and **Disabled** the **Server** (`LanmanServer`) service to completely prevent the machine from acting as a file server.

VII. Software Audit

1. Unwanted Software Removal

- **Action:** Identified and uninstalled prohibited applications found on the system.
  - **Removed: Wireshark** (Network protocol analyzer - Classified as a "hacking tool").
  - **Removed: Discord** (Non-business communication application).

2. Software Updates

- **Requirement:** The README explicitly stated that critical applications must be kept up to date.
- **Action:** Checked current versions and updated **Notepad++** and **7-Zip** to the latest stable releases to patch known vulnerabilities and ensure software integrity.

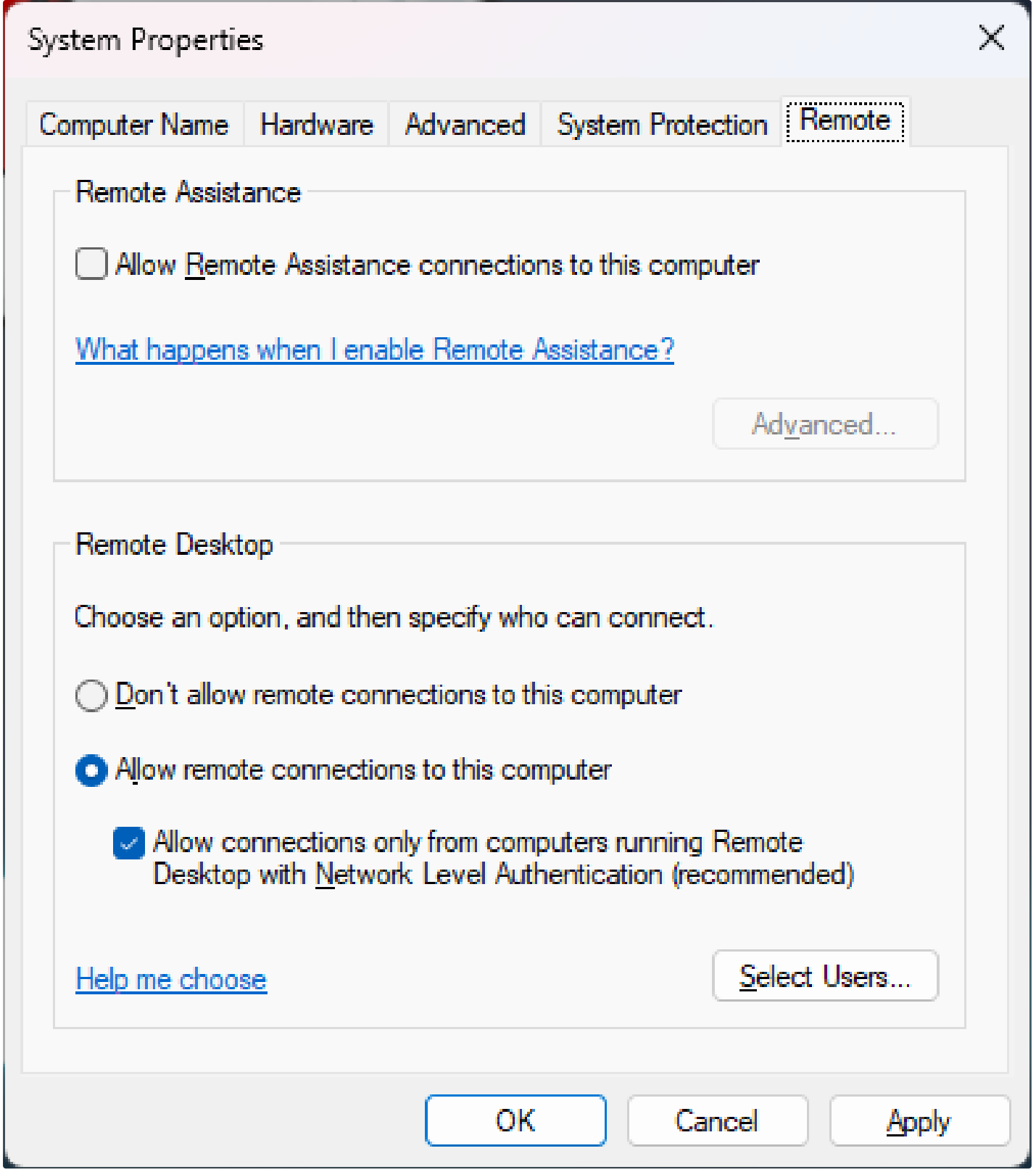
VIII. Application Security & Hardening

1. Remote Desktop (RDP) and Remote Assistance Configuration

Objective: Enable the RDP service (Critical Service) to ensure availability, but enforce the highest security standard (NLA) and disable the Remote Assistance feature to reduce the attack surface.

Remediation Steps:

1. **Open Remote Configuration:**
   - Press `Windows + R` to open the Run dialog.
   - Type command: `sysdm.cpl` and press **Enter**.
   - In the *System Properties* window that appears, select the **Remote** tab.
2. **Disable Remote Assistance:**
   - In the *Remote Assistance* section (top), **UNCHECK** the box: **"Allow Remote Assistance connections to this computer"**.
   - *Rationale:* This feature is often exploited by attackers to gain control or for Social Engineering attacks, so it should be disabled if not in use.
3. **Enable and Configure Remote Desktop (RDP):**
   - In the *Remote Desktop* section (bottom):
   - Select the radio button: **"Allow remote connections to this computer"** (To enable the service).
   - **IMPORTANT:** Check the box immediately below: **"Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)"**.
   - *Rationale:* **NLA (Network Level Authentication)** mandates user authentication before the RDP session is established, helping to prevent Man-in-the-Middle attacks and reducing server load.



2. Windows Features

- Disabled **SMB 1.0/CIFS** (Legacy protocol vulnerability).
- Disabled **Telnet Client**, **TFTP Client**.
- Disabled **Media Features** (Windows Media Player).

3. Defensive Countermeasures

- Enabled **Windows Defender Real-time Protection**.
- Enabled **SmartScreen** (Reputation-based protection) and **PUA** (Potentially Unwanted Apps) blocking.

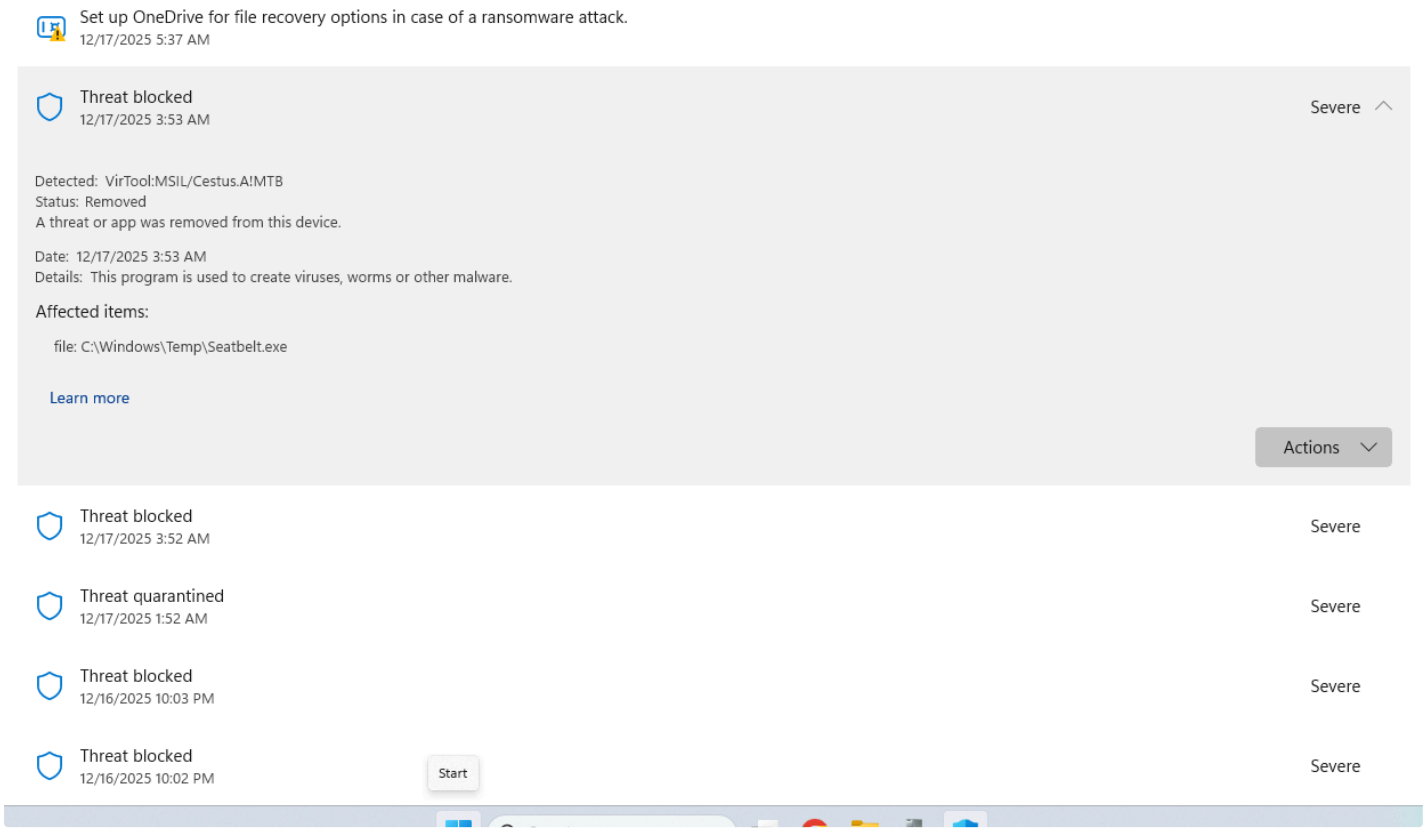
4. Remediating Malicious Antivirus Exclusions

- **Finding:** Malicious exclusions were configured in Windows Defender (excluding `.exe` extensions and the `C:\` drive).
- **Risk:** This allowed malware to bypass AV scans.
- **Action:** Removed all malicious exclusions. Retained only the exclusion for the Scoring Engine (`C:\aeacus`).

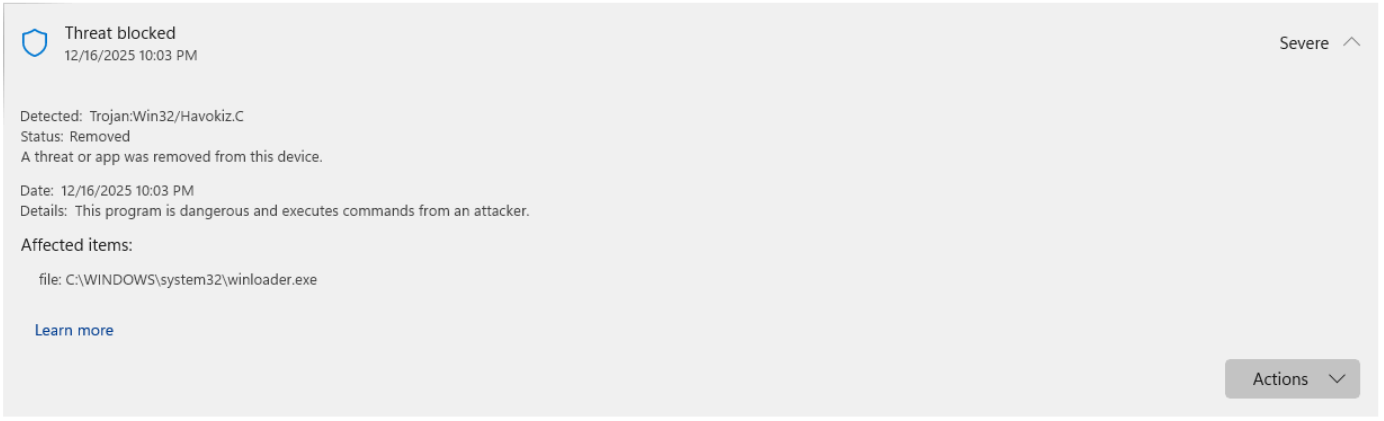
IX. Malware Removal & Prohibited Files

1. Malware Eradication

- **Startup Malware:** Removed `jokehaha.exe` and `fake-flag-child.ps1` from startup items.
- **Hidden Malware:**
  - Identified and removed malicious files via Virus & Threat Protection Scan.
  - Identified and removed `Seatbelt.exe` (Reconnaissance tool) in `C:\Windows\Temp`.

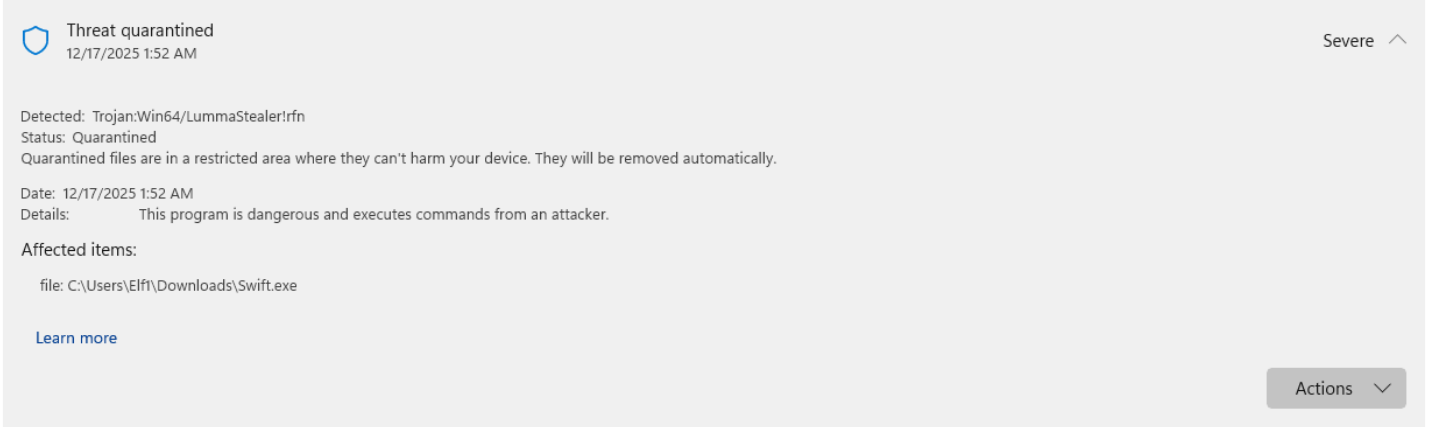


  - Purged all contents of `C:\Windows\Temp`.
  - Identified and removed `winloader.exe` (Backdoor) in `C:\Windows\System32`.

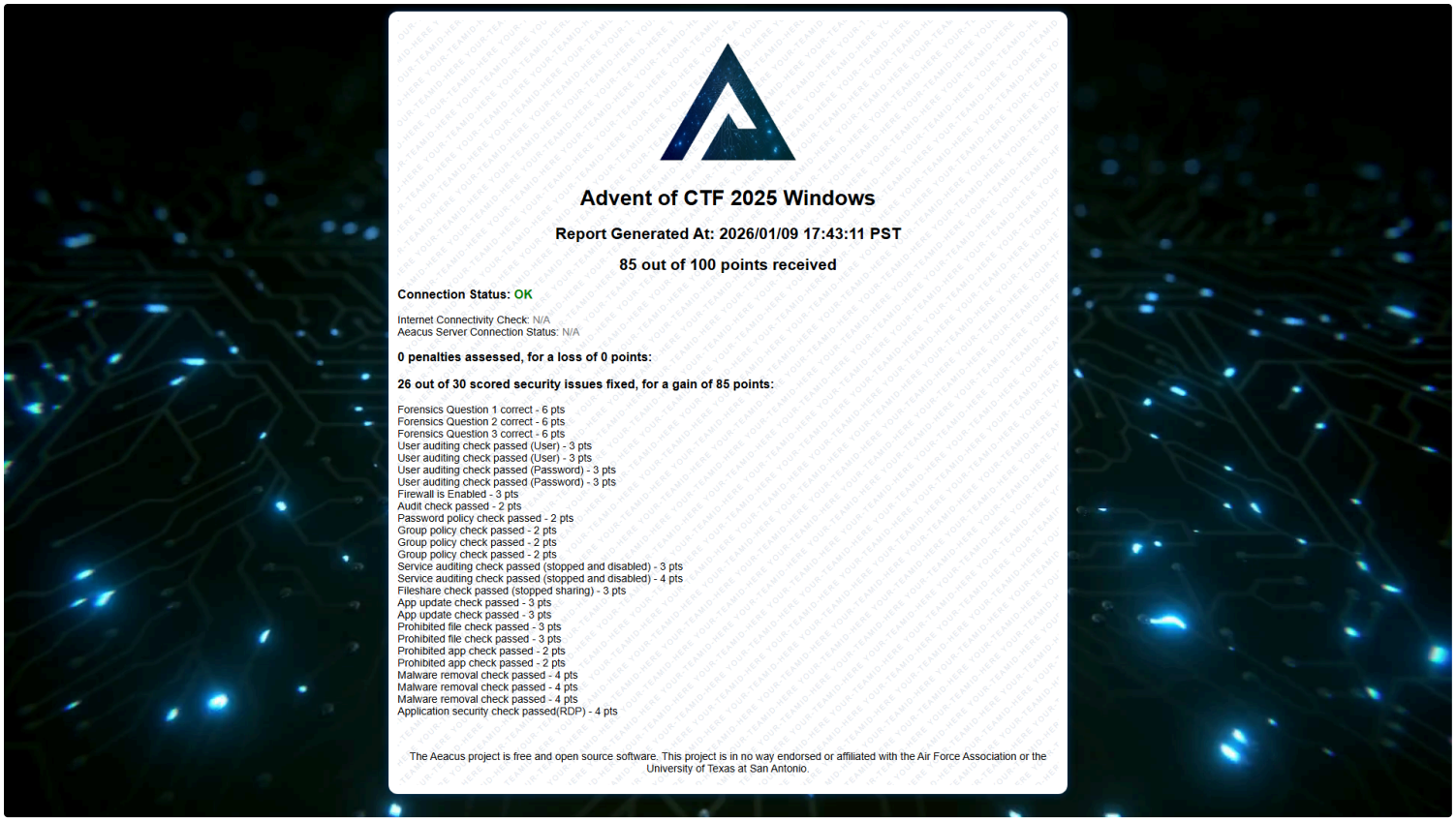


2. Prohibited File Removal

- Located and removed unauthorized archives (`.zip`) containing hacking tools and games in the `Downloads` folders of users `Elf1` and `Elf2`.



Result:



Advent of CTF 2025 Windows

Report Generated At: 2026/01/09 17:43:11 PST

85 out of 100 points received

Connection Status: OK

Internet Connectivity Check: N/A
Aeacus Server Connection Status: N/A

0 penalties assessed, for a loss of 0 points:

26 out of 30 scored security issues fixed, for a gain of 85 points:

Forensics Question 1 correct - 6 pts
Forensics Question 2 correct - 6 pts
Forensics Question 3 correct - 6 pts
User auditing check passed (User) - 3 pts
User auditing check passed (User) - 3 pts
User auditing check passed (Password) - 3 pts
User auditing check passed (Password) - 3 pts
Firewall is Enabled - 3 pts
Audit check passed - 2 pts
Password policy check passed - 2 pts
Group policy check passed - 2 pts
Group policy check passed - 2 pts
Group policy check passed - 2 pts
Service auditing check passed (stopped and disabled) - 3 pts
Service auditing check passed (stopped and disabled) - 4 pts
Fileshare check passed (stopped sharing) - 3 pts
App update check passed - 3 pts
App update check passed - 3 pts
Prohibited file check passed - 3 pts
Prohibited file check passed - 3 pts
Prohibited app check passed - 2 pts
Prohibited app check passed - 2 pts
Malware removal check passed - 4 pts
Malware removal check passed - 4 pts
Malware removal check passed - 4 pts
Application security check passed(RDP) - 4 pts

Flag: