STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 09/03/2025
  STIG Finding: STIG ID: WN11-AC-000010
- **SRG:** SRG-OS-000021-GPOS-00005
  Severity: Medium
  Vulnerability ID: V-253298 **CCI:** CCI-000044

---

1. Introduction

This report documents the process of identifying, remediating, and verifying the fix for a Windows 11 STIG compliance finding. The selected finding was: STIG ID: WN11-AC-000010 “The number of allowed bad logon attempts must be configured to three or less.”

---

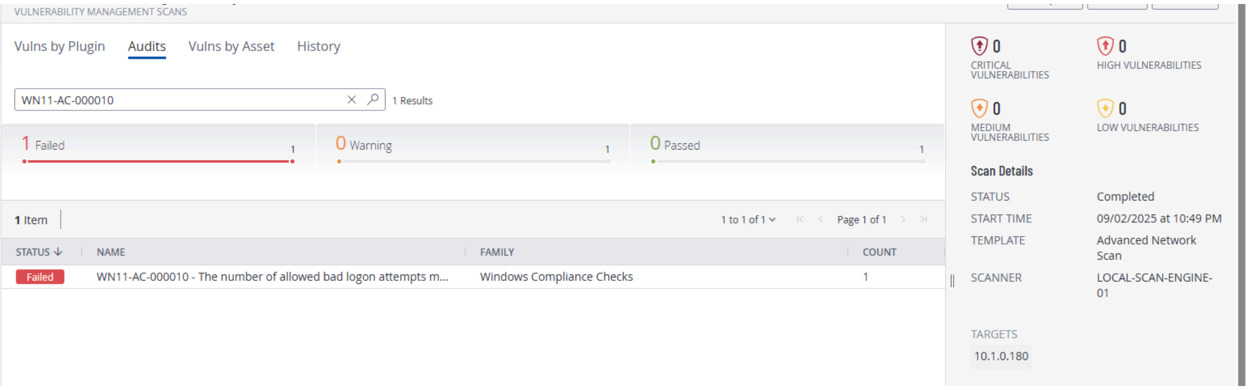
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AC-000010
- Status: **Fail** (non-compliant)

📎 **Evidence:** First identified the STIG:

https://stigaview.com/products/win11/v2r1/WN11-AC-000010/

Along with initial scan results:



WN11-AC-000010 1 Results

1 Failed 1
0 Warning 1
0 Passed 1

1 Item 1 to 1 of 1 Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Failed	WN11-AC-000010 - The number of allowed bad logon attempts m...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/02/2025 at 10:49 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.180

3. Manual Remediation Steps

Run "gpedit.msc".

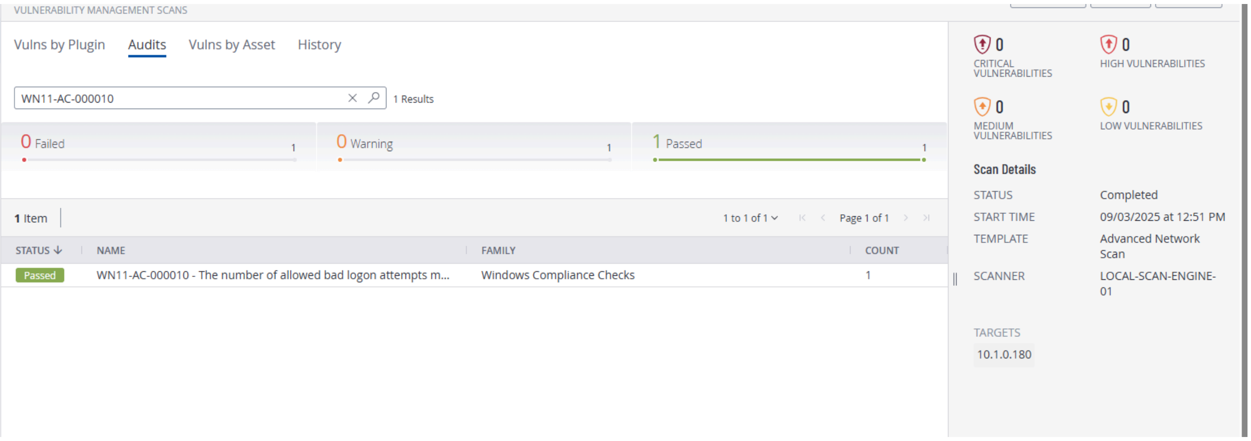
Navigate to Local Computer Policy >> Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy.

Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout threshold" to "3" or less invalid logon attempts (excluding "0" which is unacceptable)

Scan again.

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AC-000010
- Status: Passed

Evidence:



VULNERABILITY MANAGEMENT SCANS

WN11-AC-000010 — 1 Results

0 Failed 1 | 0 Warning 1 | 1 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-AC-000010 - The number of allowed bad logon attempts m...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/03/2025 at 12:51 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.180

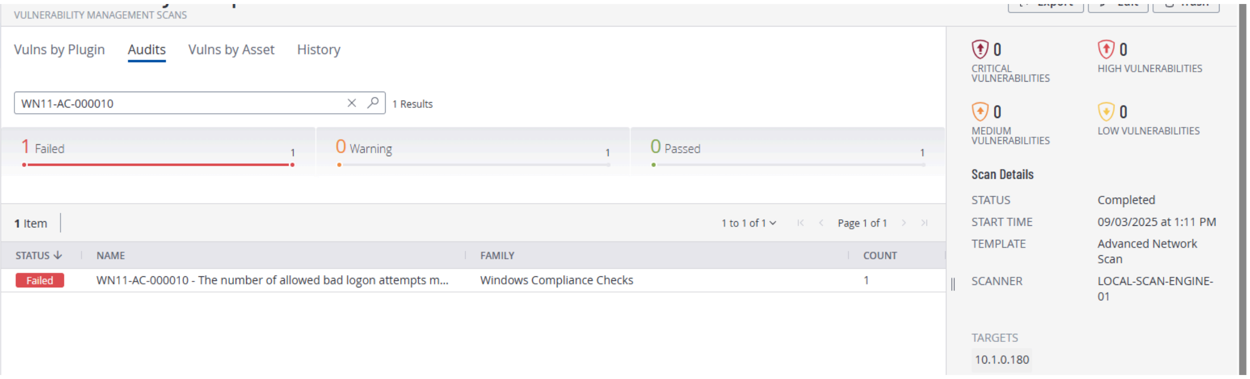
4. Reintroduction of Finding (Manually Undo Test)

To demonstrate full control of the setting, the fix was undone:

- Disabled the setting. Open **Group Policy Management** (`gpedit.msc`) and followed the instructions for remediation from before and set it to the original setting: 10.
- Ran `gpupdate /force` and rescanned.

Status: Failed, Non-Compliant

Evidence:



VULNERABILITY MANAGEMENT SCANS

WN11-AC-000010 — 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Failed	WN11-AC-000010 - The number of allowed bad logon attempts m...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/03/2025 at 1:11 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.180

5. Remediation with PowerShell Script

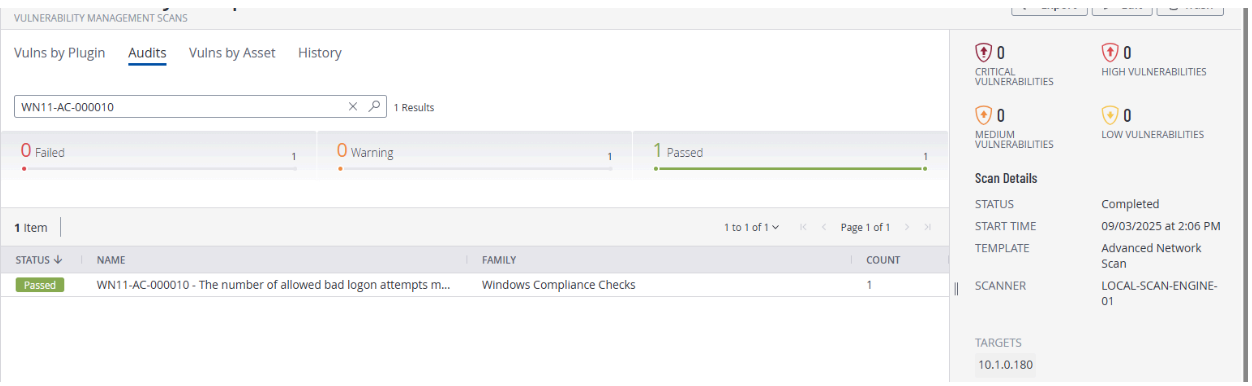
Ran the PowerShell script utilizing Windows PowerShell ISE:

```
# Paths
$infPath = "$env:TEMP\lockout.inf"
$dbPath = "$env:TEMP\lockout.sdb"

# Full security template
@"
[Unicode]
Unicode=yes
[Version]
signature="\$CHICAGO\$"
Revision=1
[System Access]
LockoutBadCount = 3
ResetLockoutCount = 30
LockoutDuration = 15
"@ | Out-File -FilePath $infPath -Encoding ASCII

# Apply security template to a fresh db
secedit /configure /db $dbPath /cfg $infPath /areas SECURITYPOLICY /overwrite

# Force Group Policy refresh
gpupdate /force

# Verify
secedit /export /cfg "$env:TEMP\verify.inf" /areas SECURITYPOLICY
Select-String -Path "$env:TEMP\verify.inf" -Pattern "LockoutBadCount"
```

Then restart.

Status: Passed

Evidence:



WN11-AC-000010 1 Results

0 Failed 1 | 0 Warning 1 | 1 Passed 1

1 Item 1 to 1 of 1 Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-AC-000010 - The number of allowed bad logon attempts m...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/03/2025 at 2:06 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.180

6. Conclusion

The finding **WN11-AC-000010** was successfully:

- Detected in an initial Tenable STIG Audit scan,
- Remediated manually,
- Verified through a second scan,
- Undone and confirmed as vulnerable again,
- Finally re-applied through PowerShell automation, and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance both manually and through automation