STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 10/18/2025
  STIG Finding: WN11-CC-000280
- **SRG:** SRG-OS-000373-GPOS-00156
  Severity: medium
  Vulnerability ID: V-253404 **CCI:** CCI-004895

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-CC-000280 "Remote Desktop Services must always prompt a client for passwords upon connection.."

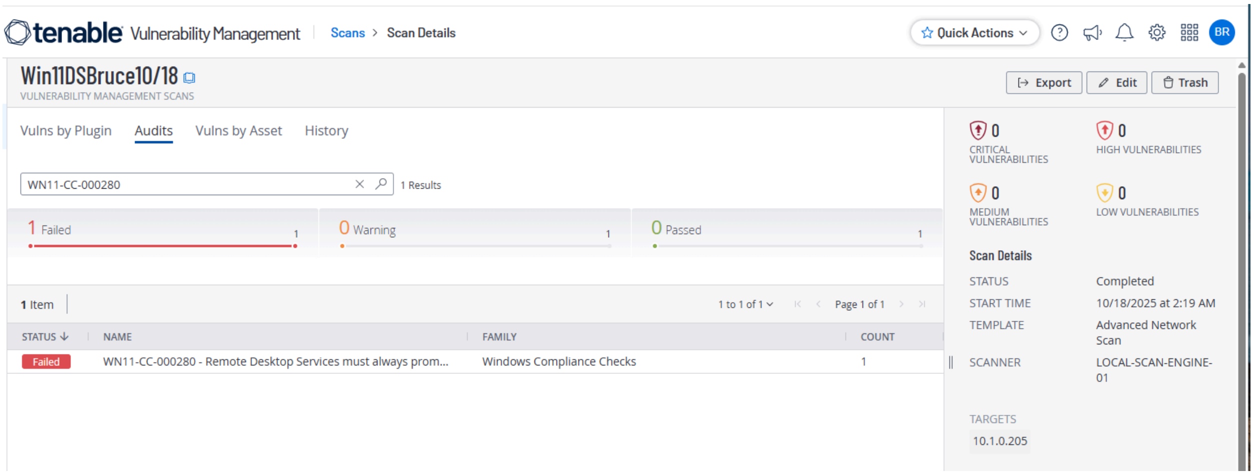
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000280
- Status: **Failed** (non-compliant)

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

https://stigaview.com/products/win11/v2r1/WN11-CC-000280/

Initial scan result:



Win11DSBruce10/18
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000280 — 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-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	10/18/2025 at 2:19 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.205

3. Manual Remediation Steps

Run “gpedit.msc”

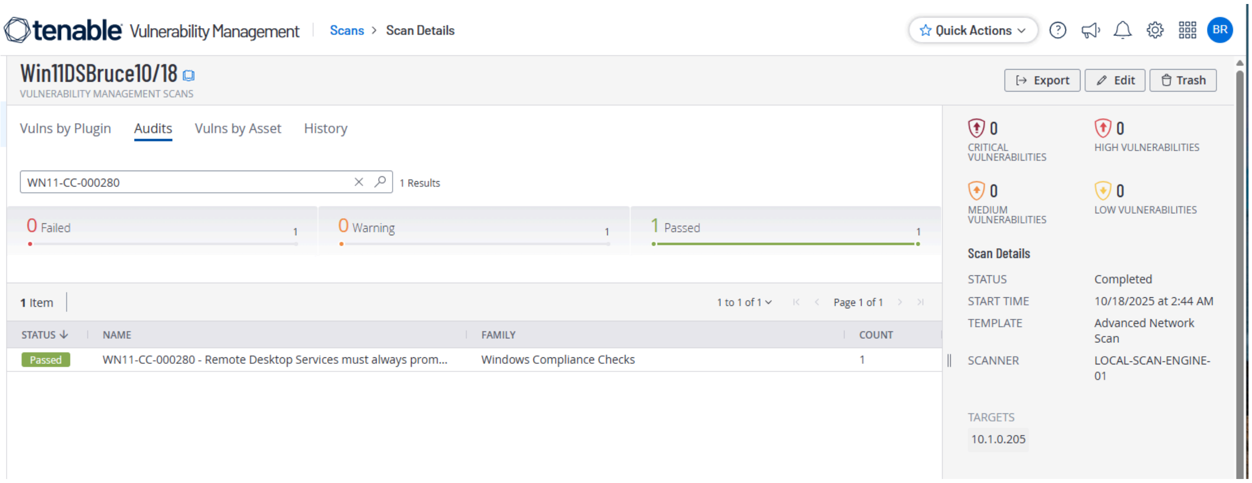
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security >> "Always prompt for password upon connection" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000280
- Status: **Passed**

Evidence:



Win11DSBruce10/18

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000280 — 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-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	10/18/2025 at 2:44 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.205

---

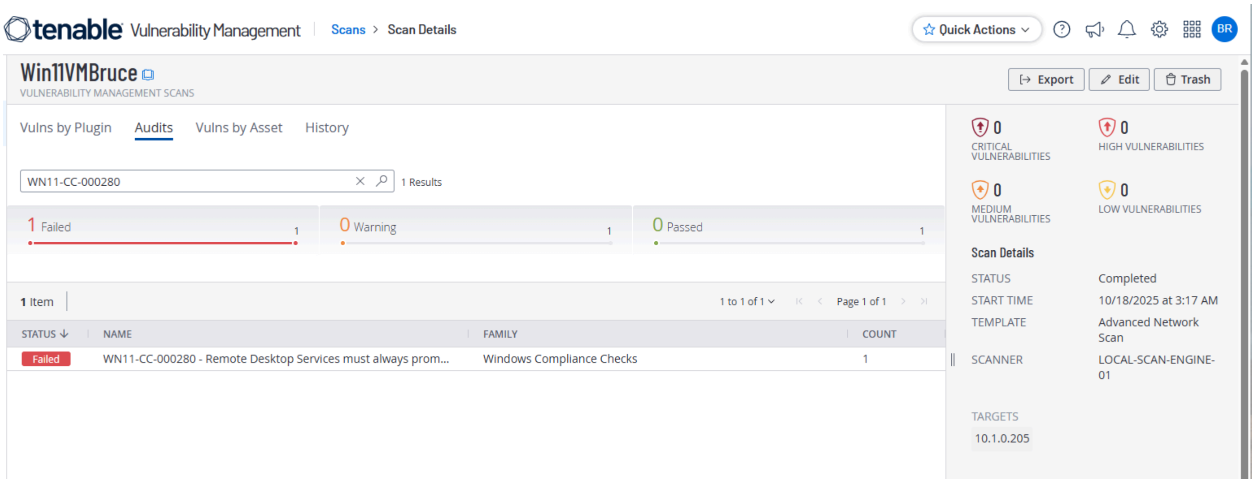
4. Reintroduction of Finding (Manually Undo Test)

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: “Not Configured.”
- Ran `“gpupdate /force”` and rescanned.

Status: **Failed**, Non-Compliant

Evidence:



Win11VMBruce

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000280 — 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-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	10/18/2025 at 3:17 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.205

5. Remediation with PowerShell Script

Utilizing PowerShell ISE.

Save as Remediate-WN11-CC-000280.ps1 (or the name of choice) and run as Administrator:

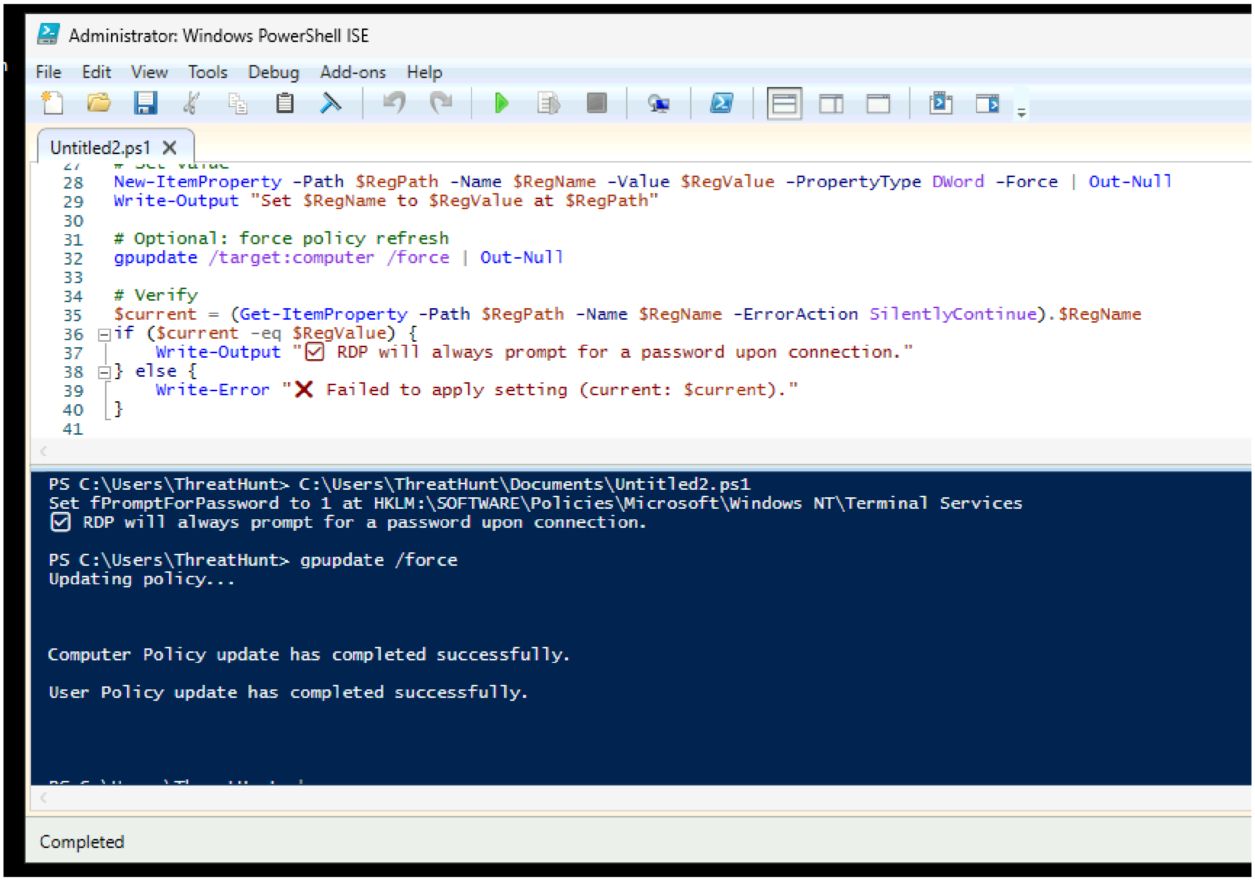
```
<#
.SYNOPSIS
  Remediates STIG WN11-CC-000280:
  Forces RDP to always prompt for a password upon connection.

.NOTES
  Run as Administrator. A gpupdate/reboot may be required for scanners to reflect the change.
#>

# Require admin
if (-not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()
    ).IsInRole([Security.Principal.WindowsBuiltinRole] "Administrator")) {
    Write-Error "Run this script as Administrator."
    exit 1
}

$RegPath  = "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"
$RegName  = "fPromptForPassword"
$RegValue = 1
```

```powershell
# Ensure path exists
if (-not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
    Write-Output "Created registry path: $RegPath"
}

# Set value
New-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -PropertyType DWord -Force | Out-Null
Write-Output "Set $RegName to $RegValue at $RegPath"

# Optional: force policy refresh
gpupdate /target:computer /force | Out-Null

# Verify
$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction SilentlyContinue).$RegName
if ($current -eq $RegValue) {
    Write-Output "✅ RDP will always prompt for a password upon connection."
} else {
    Write-Error "❌ Failed to apply setting (current: $current)."
}
```

Notes for Tenable/Nessus

- This control is computer-scope (HKLM under Policies), which Tenable expects.
- After running, do a `gpupdate /force` (script does this) and, if needed, reboot before rescanning.

Saved and ran on Virtual Machine following directions:



Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled2.ps1

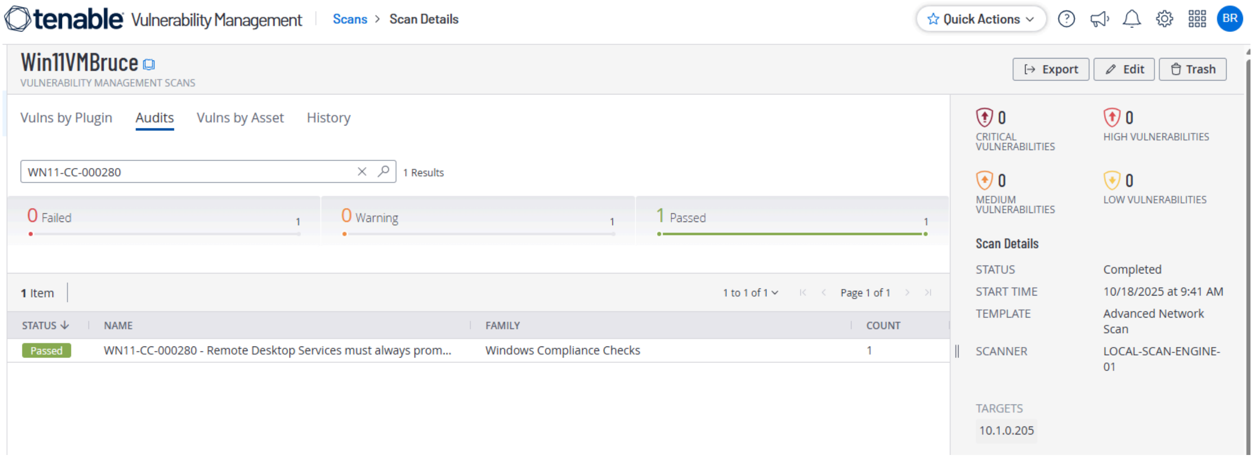
```powershell
# Set value
New-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -PropertyType DWord -Force | Out-Null
Write-Output "Set $RegName to $RegValue at $RegPath"

# Optional: force policy refresh
gpupdate /target:computer /force | Out-Null

# Verify
$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction SilentlyContinue).$RegName
if ($current -eq $RegValue) {
    Write-Output "☑ RDP will always prompt for a password upon connection."
} else {
    Write-Error "✗ Failed to apply setting (current: $current)."
}

```

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Documents\Untitled2.ps1
Set fPromptForPassword to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
☑ RDP will always prompt for a password upon connection.

PS C:\Users\ThreatHunt> gpupdate /force
Updating policy...



Computer Policy update has completed successfully.

User Policy update has completed successfully.




PS C:\Users\ThreatHunt>
```

Ran “`gpupdate /force`” and rescanned.

Status:**Passed**

Evidence:



WN11-CC-000280 — 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-CC-000280 - Remote Desktop Services must always prom...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES — 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES — 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	10/18/2025 at 9:41 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.205

6. Conclusion

The finding **WN11-CC-000280** 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 PowerShell automation.