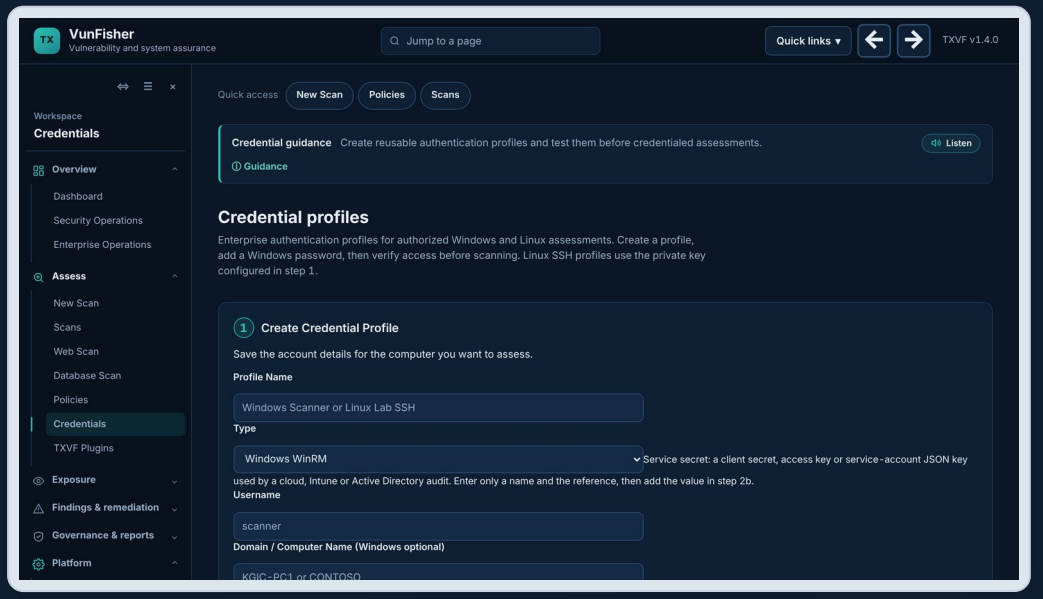
VunFisher credentialed scanning

Prepare Windows and Linux targets with or without the Target Setup Assistant, and run your first credentialed scan



Before the training

1

VunFisher installed and active

Platform > License shows ACTIVE (request and install deck)

2

Two computers on the same network

The scanner (runs VunFisher) and a target: a lab VM or a second PC

3

Administrator rights on the target

To turn on remote management and create a scan account

4

Written authorization

Only scan computers you own or your instructor has approved

Two ways to prepare a Windows target: the Target Setup Assistant (Part 1, easiest) or by hand (Part 2, also covers Linux).

Part 1: Prepare a Windows target with the assistant

Target Setup Assistant 0.3.0, run on the computer you will scan

Scanner and target: who does what

Scanner computer
Runs VunFisher
Holds the scan account password

Windows Remote Management, port 5985



Target computer
Runs the Target Setup Assistant
Allows only the scanner to connect

The assistant never asks for, shows or stores a password. You type the scan account password only in VunFisher on the scanner.

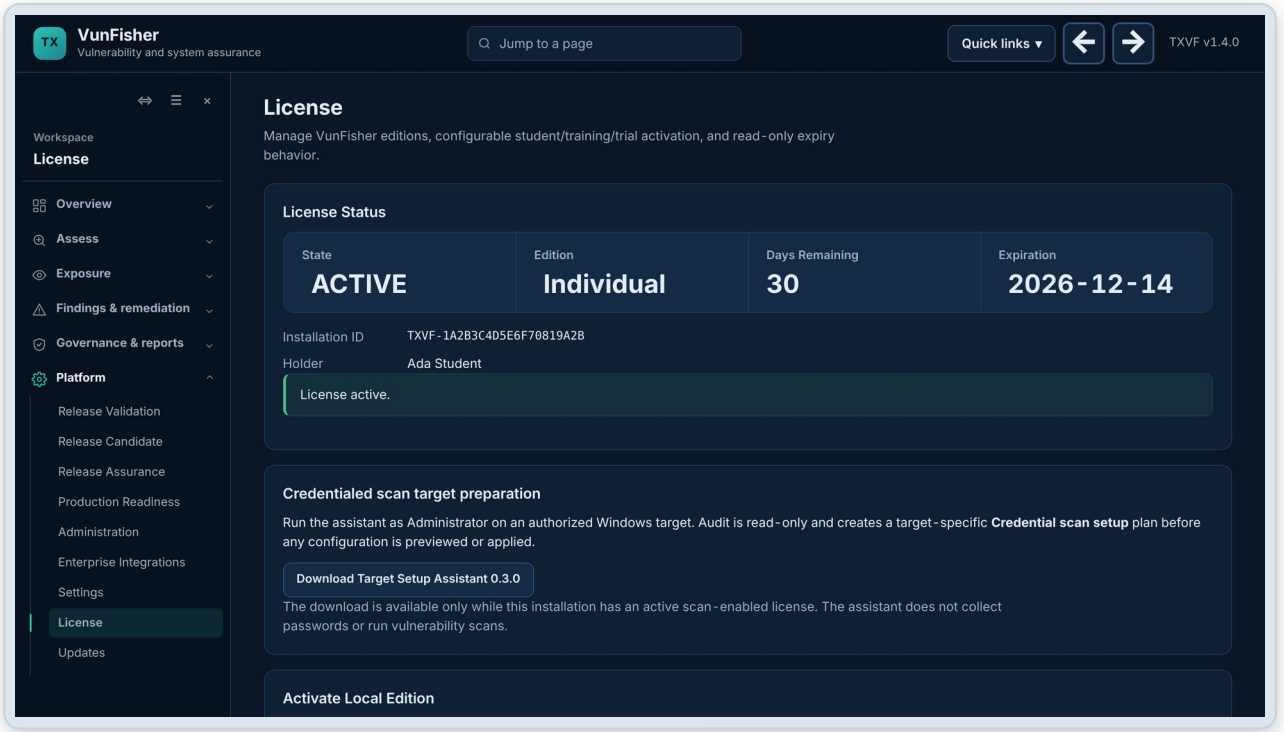
Get and start the Target Setup Assistant

1. **Download it**
   VunFisher > Platform > License > Download Target Setup Assistant 0.3.0

2. **Copy the ZIP to the target computer**
   USB drive or shared folder

3. **Extract All on the target**
   Then double-click Start-Assistant.cmd

4. **Approve the Windows prompt**
   The assistant needs administrator rights on the target



The assistant walks you through five steps

1	**Check this computer**	Reads network type, remote management and firewall. Changes nothing. Fix any STOP line first.
2	**Scanner and account**	Scanner IPv4 address (run ipconfig on the scanner) and the scan account, e.g. PC-NAME\vfscan.
3	**Preview the changes**	Shows exactly what will change. Nothing has changed yet.
4	**Apply the changes**	After you approve. A checkpoint folder is saved; keep its path for Undo.
5	**Connect VunFisher**	Shows the exact credential settings to enter on the scanner.

On the scanner: create and test the credential

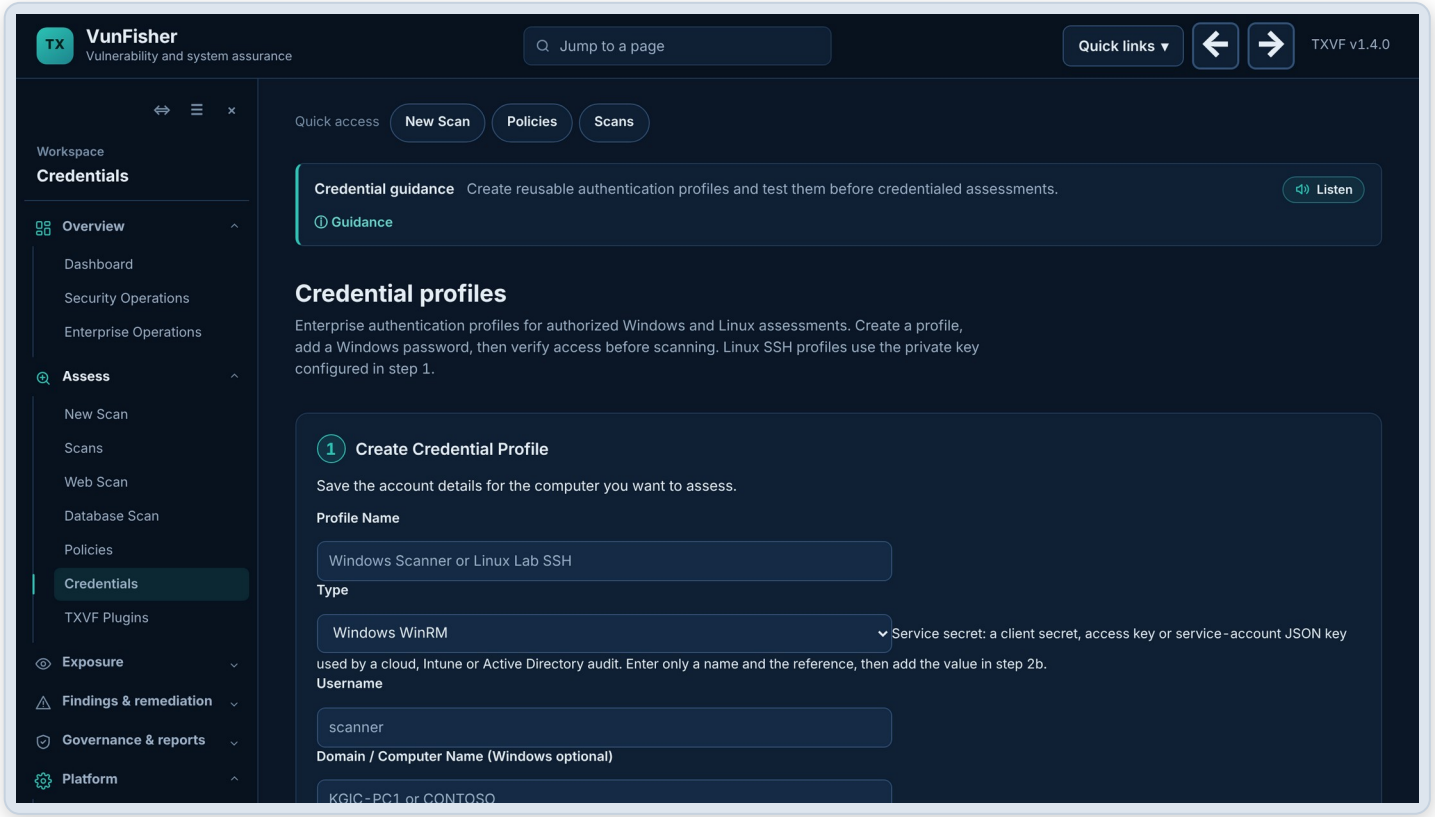
1. **Open Credentials**
   Left menu: ASSESS > Credentials

2. **1 Create Credential Profile**
   Windows WinRM, user, computer name, 5985, reference TXVF_LAB_PASSWORD

3. **2 Add Windows Password**
   Pick the profile and type the password

4. **3 Test Connection**
   Target address + profile > Test Credential; every stage should pass

5. **Then scan**
   New Scan > Credentialed Windows Assessment > select the profile



Part 2: Prepare targets by hand

Prepare Windows and Linux targets by hand, the way scanner guides such as Nessus describe it

What a credentialed scan needs

	Nessus (for comparison)	VunFisher
Windows connection	SMB (445) and WMI; Remote Registry and admin shares	Windows Remote Management (WinRM), TCP 5985, PowerShell remoting with Negotiate sign-in
Windows account	Administrator-level account	Administrator-level account (local or domain)
Local accounts	Remote UAC setting (LocalAccountTokenFilterPolicy)	Same setting, only for local accounts, and only when needed
Linux	SSH with a password or key; often sudo	SSH with a key; no sudo needed (reads the installed package list)
Where the password goes	Scan policy credentials	Credentials page on the scanner; never on the target

VunFisher does not need Remote Registry, admin shares or SMB for credentialed Windows checks: leave those as they are.

Windows target, by hand (1 of 2)

On the target: open Windows PowerShell as administrator

```
# 1. A scan account (Windows asks for the new password; type it there only)
net user vfscan * /add
net localgroup Administrators vfscan /add

# 2. The network must be Private (or Domain), not Public
Get-NetConnectionProfile
Set-NetConnectionProfile -InterfaceAlias "Ethernet" -NetworkCategory Private

# 3. Turn on Windows Remote Management (WinRM, port 5985)
Enable-PSRemoting -Force
```

Domain computers: skip step 1 and use a domain scan account in a group that is a member of the local Administrators group.

Windows target, by hand (2 of 2)

Still on the target, as administrator

```
# 4. Let only the scanner reach WinRM
Set-NetFirewallRule -Name WINRM-HTTP-In-TCP -RemoteAddress 192.168.56.10
Disable-NetFirewallRule -Name WINRM-HTTP-In-TCP-PUBLIC

# 5. Local accounts only (workgroup lab): allow remote admin rights
New-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System `
  -Name LocalAccountTokenFilterPolicy -Value 1 -PropertyType DWord -Force

# 6. Check that WinRM answers
Test-WSMan localhost
```

Step 5 lowers a Windows protection for local accounts. Use it only on lab computers, and remove it after the course (Undo slide).

On the scanner: trust the target and test

On the computer running VunFisher: Windows PowerShell as administrator

```
# 1. Is port 5985 reachable?
Test-NetConnection 192.168.56.20 -Port 5985

# 2. Workgroup or IP address targets only: trust this one target
Start-Service WinRM
Set-Item WSMan:\localhost\Client\TrustedHosts -Value '192.168.56.20' -Concatenate -Force

# 3. Sign in once by hand (a password prompt opens)
Invoke-Command -ComputerName 192.168.56.20 -Credential LAB-PC1\vfscan -ScriptBlock { whoami }
```

If step 3 prints lab-pc1\vfscan, VunFisher will be able to sign in too. Domain targets addressed by name do not need TrustedHosts.

In VunFisher: the Windows credential

1

ASSESS > Credentials > 1 Create Credential Profile

Type Windows WinRM; Username vfscan; Domain / Computer Name LAB-PC1; Port 5985; Secret reference TXVF_LAB_PASSWORD

2

2 Add Windows Password

Select the profile, type the password. Tick DPAPI remember only on your own computer.

3

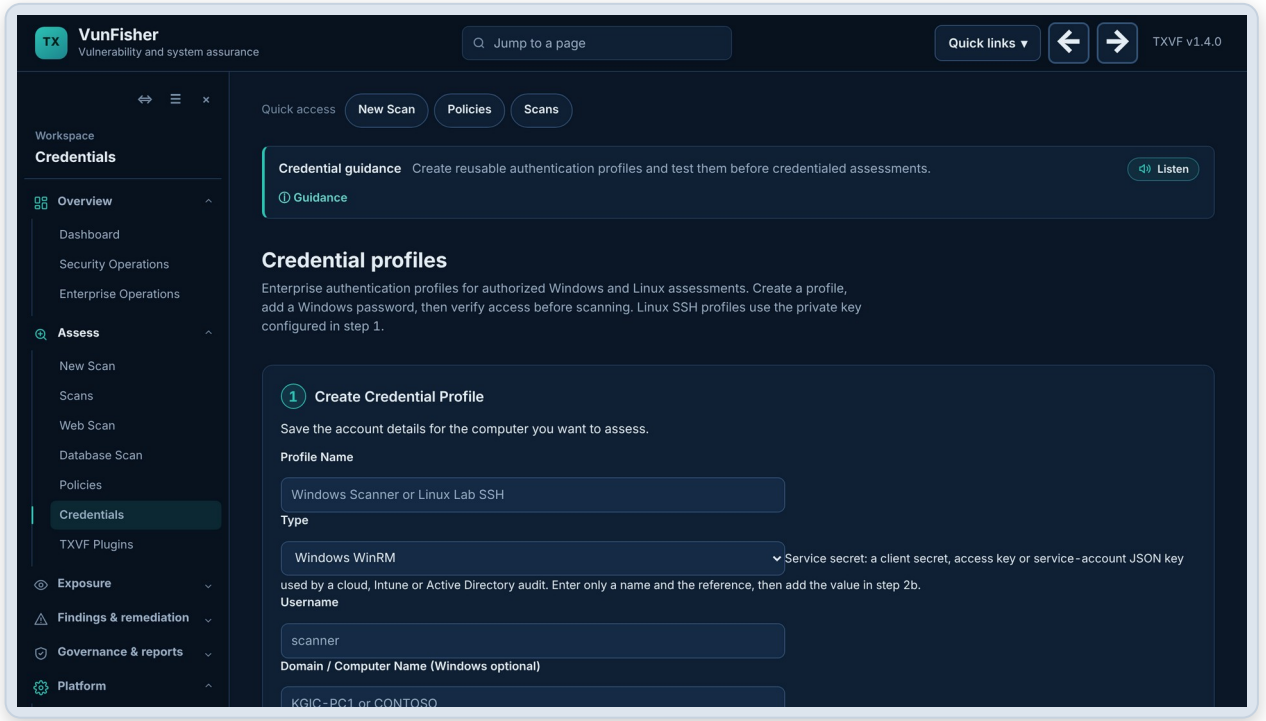
3 Test Connection

Target 192.168.56.20, the profile, the authorization box > Test Credential

4

New Scan

Credentialed Windows Assessment or Credentialed Patch Audit > select the profile



Linux target over SSH

On the scanner (Windows PowerShell)

```
# A key for VunFisher
$k = "$env:USERPROFILE\.ssh\vunfisher_ed25519"
ssh-keygen -t ed25519 -f $k
# Show the public key to copy
Get-Content "$k.pub"
# Test after the target is ready
ssh -i $k vfscan@192.168.56.30 id
```

On the Linux target (Ubuntu, Debian or Alpine)

```
sudo useradd -m -s /bin/bash vfscan
sudo install -d -m 700 -o vfscan -g vfscan /home/vfscan/.ssh
# paste the .pub line into this file:
sudo nano /home/vfscan/.ssh/authorized_keys
sudo chown vfscan:vfscan /home/vfscan/.ssh/authorized_keys
sudo chmod 600 /home/vfscan/.ssh/authorized_keys
sudo ufw allow from 192.168.56.10 to any port 22 proto tcp
```

1. **VunFisher > Credentials > 1 Create Credential Profile**
   Type Linux SSH; Username vfscan; Port 22; SSH Private Key Path C:\Users\you\.ssh\vunfisher_ed25519

2. **Test Connection, then New Scan**
   Credentialed Linux Assessment > select the profile. No sudo and no password are needed.

Many computers: domain and Intune

1. **Create a scan group**
   Add the approved domain scan account; test on one OU with one or two computers first

2. **Add the group to local Administrators**
   Group Policy Preferences > Local Users and Groups (add, do not replace the list)

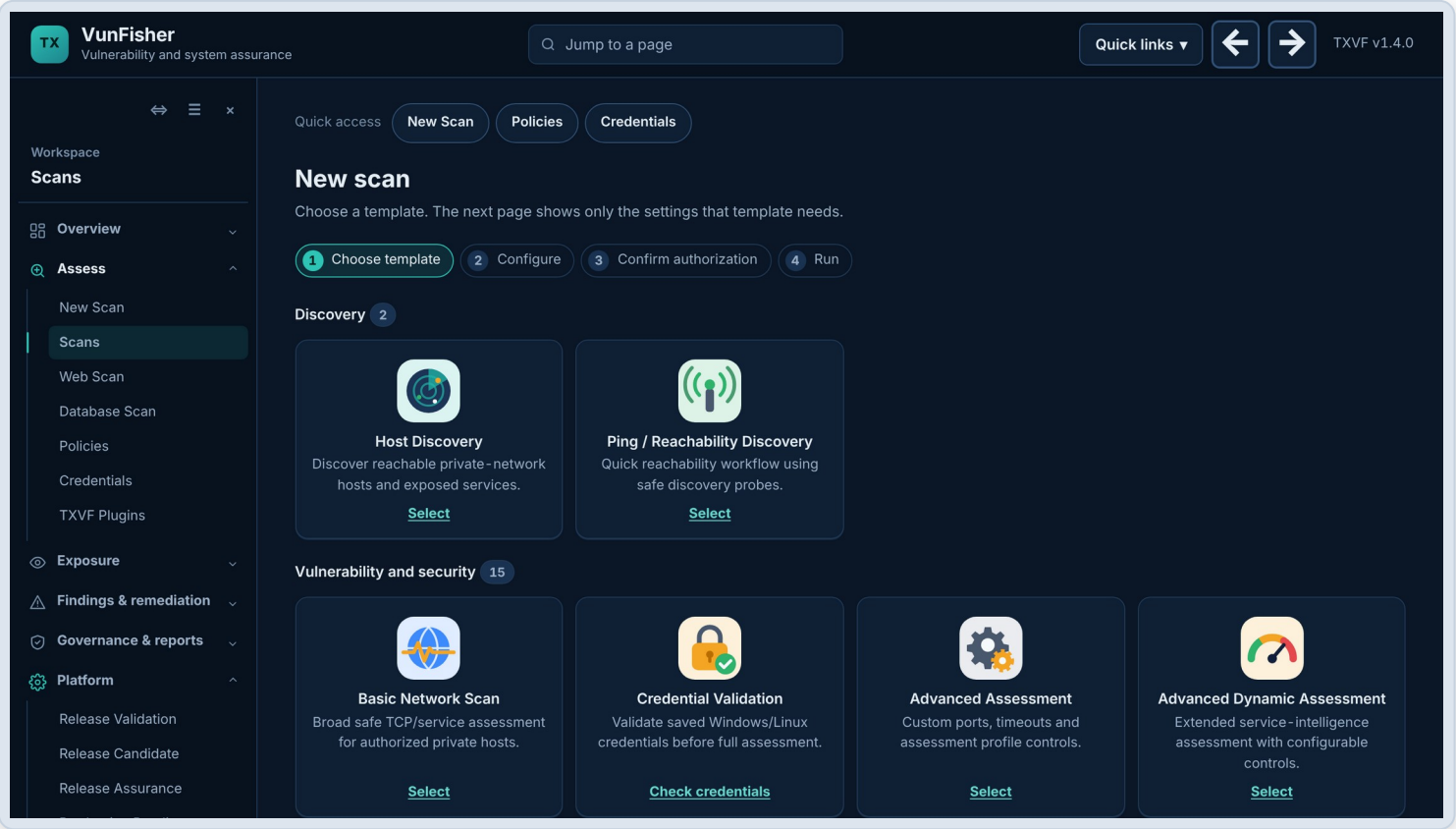
3. **Turn on WinRM by policy**
   Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management

4. **Firewall rule for TCP 5985**
   Domain and Private profiles; remote addresses = approved scanners only

5. **Check and widen slowly**
   gpresult /r on a target, Test Connection in VunFisher, then more OUs. Intune: the same settings in Settings Catalog profiles

Domain accounts do not need the LocalAccountTokenFilterPolicy setting. Do not add domain controllers until IT has reviewed them.

Run your first scan



New Scan

- Choose Credentialed Windows Assessment (or Credentialed Linux Assessment)
- Enter the authorized target address and select the credential profile
- Confirm authorization and run
- Open Findings when it completes; Explain with AI gives a plain-English summary of a finding

Undo after the course

Windows target (administrator PowerShell)

```
Disable-PSRemoting -Force
Disable-NetFirewallRule -Name WINRM-HTTP-In-TCP
Stop-Service WinRM
Set-Service WinRM -StartupType Manual
Remove-ItemProperty -Path `
 HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System `
 -Name LocalAccountTokenFilterPolicy
net user vfscan /delete
```

Scanner and Linux target

```
# Scanner: empty TrustedHosts again
Set-Item WSMan:\localhost\Client\TrustedHosts `
  -Value '' -Force
# VunFisher: Credentials > Clear secret,
# then Disable the profile
# Linux target:
sudo userdel -r vfscan
sudo ufw delete allow from 192.168.56.10 \
  to any port 22 proto tcp
```

If TrustedHosts listed other computers before the course, remove only the lab entries instead of emptying it. Delete the vunfisher_ed25519 key files on the scanner too.

Quick fixes

Test Credential: connectivity fails

Firewall rule or scanner address. Run Test-NetConnection target -Port 5985 on the scanner.

Test Credential: sign-in fails

Check the account name (COMPUTER\user), the password in step 2 and TrustedHosts for IP targets.

Signed in but not administrator

Add the account to local Administrators; local accounts also need LocalAccountTokenFilterPolicy.

Assistant shows STOP

Public network, Windows Home or a policy-managed computer: fix it or prepare the target by hand.

Linux: permission denied

Check authorized_keys permissions (600) and the key path in the profile.

Scan shows coverage gaps

A check could not collect evidence. Read the reason; it is not a clean result.

Links you will need

VunFisher

VunFisher website: https://txvf.tinkextra.com/overview/

Downloads (app, hash, SBOM): https://txvf.tinkextra.com/overview/downloads.html

Student license request: https://txvf.tinkextra.com/quote?for=student

Every published build: https://txvf.tinkextra.com/overview/roadmap.html#release-history

Your local app (after install): http://127.0.0.1:8787/credentials

Microsoft

Enable-PSRemoting (PowerShell 5.1): https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-5.1

Remote troubleshooting, TrustedHosts: https://learn.microsoft.com/powershell/module/microsoft.powershell.core/about/about_remote_troubleshooting

WinRM security: https://learn.microsoft.com/en-us/powershell/scripting/security/remoting/winrm-security

New-NetFirewallRule: https://learn.microsoft.com/powershell/module/netsecurity/new-netfirewallrule

UAC remote restrictions (local accounts): https://support.microsoft.com/help/951016

OpenSSH keys on Windows: https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_keymanagement

Nessus, for comparison

Credentialed checks on Windows: https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm

SSH credentials: https://docs.tenable.com/nessus/Content/SSH.htm

You are ready to scan

Target prepared · credential tested · first scan run · undo the lab changes when the course ends