VunFisher remote scan setup

Prepare a Windows target, test access, then run a credentialed scan. Choose Route A or B, then follow the shared VunFisher steps. Examples use the successful CyberTech-Intel assessment.

Why this workflow exists

Vulnerability detection is only the beginning. VunFisher is designed to preserve the evidence chain from authorized target preparation and authentication through findings, ownership, remediation, retest, risk decisions and reporting. This guide helps you establish trustworthy credentialed coverage before interpreting a result. Missing or blocked checks must remain visible and must never be treated as proof that the target is secure.

Why VunFisher | Product and beta presentation | Submit beta feedback

Know which computer you are using

Role	Example	What you do there
SCANNER	KGIC-PC1 192.168.1.2	Runs VunFisher and starts scans
TARGET	CyberTech-Intel 192.168.1.195	The computer being checked
SCAN ACCOUNT	CyberTech-Intel\vunfisher_scan	An account on the TARGET, not the VunFisher website login

Replace example names and addresses. Find the name in Settings > System > About, and IPv4 in Settings > Network & internet > connected network > Properties. Record both computers.

Choose your route

Route	Use it when	Pages

A Windows menus plus one command	You prefer clicking through Windows settings	2-3, then 6-7
B PowerShell	You are comfortable copying short command blocks	4-5, then 6-7
IT prepared computers	IT has already configured WinRM, access and firewall rules	6-7
Help and optional setup	Troubleshooting, Remote Registry and cleanup	8-11

Before starting

The menus assume Windows 11 Pro. Windows 10/11 Enterprise or Education and Windows Server may need IT adaptations; Home may lack these consoles. Have an administrator available on both computers.

Keep both computers awake on a trusted LAN or approved VPN. Avoid guest Wi-Fi isolation. Remote Desktop and internet port forwarding are unnecessary. Let IT handle company-managed policy changes.

Full Windows inventory uses administrative checks. A standard account can authenticate but return partial evidence. Administrator membership grants full control of the target; use a dedicated, approved account and protect its password.

Route A prepare the target with Windows menus

A1 Choose the trusted network

Open Settings > Network & internet > Wi-Fi or Ethernet > the connected network. On your trusted lab LAN, select Private. Do not change a public network to Private just to make scanning work. Leave a company domain network under IT policy. Keep the target awake during the scan.

A2 Create the scan account

Right-click Start > Computer Management. Open Local Users and Groups > Users. Right-click Users > New User. Enter vunfisher_scan and a strong, unique password. Clear User must change password at next logon for this dedicated scan account, then click Create. Do not use a blank password or Windows Hello PIN. Follow your organization's password rotation policy. If the approved account already exists, reuse it; do not recreate or reset it unnecessarily.

A3 Give the account access for the full assessment

In Computer Management, open Local Users and Groups > Groups > Administrators. Click Add, type vunfisher_scan, click Check Names, then OK and Apply. Confirm the name refers to the TARGET computer. This grants full local administrator access. Do not remove this membership until the scan and verification are finished.

If IT only permits a standard scan account, ask IT to configure its remote endpoint permissions. Expect some checks to remain unavailable. Membership in Remote Management Users alone does not guarantee access to every PowerShell endpoint or administrative inventory check.

A4 Enable the Windows PowerShell endpoint

This is the one PowerShell command in Route A. On the TARGET, search Start for Windows PowerShell, right-click it and choose Run as administrator. Use Windows PowerShell 5.1, not PowerShell 7 or PowerShell ISE. Run: [1]

```
Enable-PSRemoting -Force
```

Expected: the command returns without a red error. It configures WinRM and Windows PowerShell session endpoints. Starting the WinRM service alone is not enough. Continue immediately to A5 to restrict the firewall scope.

If users must use no PowerShell at all, IT must provision the PowerShell endpoint and WinRM configuration in advance. Users can then complete the remaining menu steps and scan in VunFisher. This guide does not claim that changing a service startup setting fully configures remoting.

Route A finish the access settings

A5 Limit the target firewall to the scanner

On the TARGET, press Windows+R, type wf.msc, and press Enter. Select Inbound Rules. Find Windows Remote Management (HTTP-In), TCP 5985. Open each applicable enabled rule > Scope. Under Remote IP address, choose These IP addresses > Add > enter the SCANNER address, 192.168.1.2. Apply. On Advanced, use Private for this lab; leave Public unchecked. Check for other enabled rules allowing 5985 more broadly. On managed systems, ask IT to scope the policy instead of overriding it. Keep Windows Firewall enabled. [2]

A6 Allow the approved local administrator to use its full token

For this workgroup/local-account lab only: on the TARGET, open Registry Editor as administrator. Before changing anything, record whether the value below exists and its current data. Navigate to: [3]

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

This is one continuous registry path. In the right pane, find LocalAccountTokenFilterPolicy. If absent, create New > DWORD (32-bit) Value with that exact name, even on 64-bit Windows. Set its data to 1. If already 1, leave it unchanged.

This setting relaxes remote UAC restrictions for local administrator accounts across the target, not only the scan account. Use it only with approval and a restricted firewall. For domain-managed machines, prefer IT-approved domain credentials and policy; do not apply this workgroup change automatically.

A7 Configure the scanner without PowerShell

On the SCANNER, press Windows+R > services.msc. Open Windows Remote Management (WS-Management), set Startup type to Automatic, click Apply, then Start if stopped.

Press Windows+R > gpedit.msc. Go to Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client > Trusted Hosts. Record the current setting. Enable it and add the TARGET IP, 192.168.1.195. Preserve any existing approved entries, separated by commas. Do not enter an asterisk (*). [4]

Allow policy to apply; restart the scanner if needed after saving other work. If this policy is managed or the editor is unavailable, ask IT to set it, or use Route B step B5 instead. A TrustedHosts entry is an exception to server-identity verification, not proof of the target's identity. Check the target address carefully. Now continue to page 6.

Route B configure the target with PowerShell

Use this route instead of Route A. Copy one block at a time. Replace example values first. Do not copy the PS C:\...> prompt from screenshots. If a block returns an unexpected red error, stop and use page 8.

B1 Identify the target and trusted network

```
hostname
Get-NetIPConfiguration
Get-NetConnectionProfile
```

Confirm the name and IPv4 address. On a trusted lab network only, use the InterfaceIndex shown above in the next command. Replace 12 with the actual index; skip this command if already Private. Leave DomainAuthenticated networks unchanged.

```
Set-NetConnectionProfile -InterfaceIndex 12 -NetworkCategory Private
```

B2 Create or reuse the approved scan account

```
$scanUser = 'vunfisher_scan'
if (-not (Get-LocalUser -Name $scanUser -ErrorAction SilentlyContinue)) {
    $scanPassword = Read-Host 'New scan account password' -AsSecureString
    New-LocalUser -Name $scanUser -Password $scanPassword
    Remove-Variable scanPassword
}
Get-LocalUser -Name $scanUser | Select-Object Name,Enabled
```

Expected: Enabled is True. For an existing account, this block does not change its password or enable a disabled account. Ask its owner if it is disabled. Now grant approved administrator membership; “already a member” means it is already set. [5]

```
Add-LocalGroupMember -SID 'S-1-5-32-544' -Member $scanUser
```

B3 Enable remoting and restrict the built in firewall rule

```
Enable-PSRemoting -Force
$scannerIP = '192.168.1.2'
```

```
Get-NetFirewallRule -Name 'WINRM-HTTP-In-TCP*' |
    Set-NetFirewallRule -Enabled True -Profile Private -RemoteAddress $scannerIP
```

This lab block changes the built-in WinRM HTTP rules to Private and the scanner IP only. It can affect existing management access; have IT adapt it on shared or managed computers. In wf.msc, also check for other rules that allow port 5985 broadly. Continue to B4. [1,2]

TARGET for B4 | SCANNER for B5-B6

Route B finish the target and prepare the scanner

B4 Set the local account policy on the target

For an approved workgroup/local-admin setup, first record the old value below. A blank result means it is absent. Do not use this step automatically with domain credentials. The setting affects all local administrators on this target. [3]

```
$policyPath = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
Get-ItemPropertyValue -Path $policyPath -Name LocalAccountTokenFilterPolicy `
    -ErrorAction SilentlyContinue
New-ItemProperty -Path $policyPath -Name LocalAccountTokenFilterPolicy `
    -PropertyType DWord -Value 1 -Force
```

If the account was just added to Administrators, use a new credential test so Windows creates a new remote session. Do not run any cleanup commands yet.

B5 Trust the specific target on the scanner

Move to the SCANNER. Open Windows PowerShell 5.1 as administrator. The following starts the local WinRM service and adds only the TARGET to TrustedHosts while preserving existing entries. Do not use Enable-PSRemoting on the scanner just to send scans. Record existing service and TrustedHosts settings before changing them. [4]

```
Get-Service WinRM | Select-Object Name,Status,StartType
Set-Service WinRM -StartupType Automatic
Start-Service WinRM
$targetIP = '192.168.1.195'
$trustPath = 'WSMan:\localhost\Client\TrustedHosts'
$oldTrust = (Get-Item $trustPath).Value
$oldTrust
$entries = @($oldTrust -split ',' | ForEach-Object { $_.Trim() } |
    Where-Object { $_ })
if ($entries -notcontains $targetIP) {
    $newTrust = (@($entries) + $targetIP) -join ','
    Set-Item $trustPath -Value $newTrust -Force
}
Get-Item $trustPath
```

B6 Test the network from the scanner

```
Test-NetConnection 192.168.1.195 -Port 5985
```

Expected: TcpTestSucceeded : True. This confirms the port is reachable; it does not test the password. If False, check the target IP, sleep state, network profile, firewall scope and network isolation. Continue to page 6. [6]

Create the credential profile in VunFisher

1 Open the local application

Start the installed VunFisher application on the SCANNER. On that same computer, open http://127.0.0.1:8787 and sign in. Click Credentials. The address 127.0.0.1 means “this computer.” A hosted website is not automatically able to reach your private target network.

2 Create the profile

Under Step 1 Create Credential Profile, enter the values below and click Create Profile. If the matching profile already exists, select it rather than creating duplicates.

Field	Example value
Profile Name	CyberTech laptop
Type	Windows WinRM
Username	vunfisher_scan
Domain / Computer Name	CyberTech-Intel (the TARGET name)
Port	5985
SSH Private Key Path	Leave blank for Windows WinRM
Password Environment Variable	TXVF_LAPTOP_PASSWORD

The last field is a reference name, not the password. Use a different reference for accounts with different passwords. If an existing working profile uses TXVF_WINRM_PASSWORD, keep that reference unless intentionally creating a new profile. Enter the username and target computer name separately as shown.

3 Load the target account password

Under Step 2 Add Windows Password, select CyberTech laptop. Enter that account’s actual Windows password. Do not enter your VunFisher login password or a PIN. Click Load Session

Secret.

For a one-time session, leave Securely remember unchecked. If approved for repeat scans, select Securely remember with Windows DPAPI before loading. A session-only secret may need reloading after VunFisher restarts. Store and rotate account passwords under your organization’s policy; never paste them into email, training slides or screenshots.

4 Test the credential

Under Step 3 Test Connection, enter 192.168.1.195, choose CyberTech laptop, check the authorization box if you own or are authorized to assess this target, and click Test Credential.

Continue only when the result shows Authentication SUCCESS, the intended target identity, and Privilege ADMINISTRATOR for the full assessment. Preflight checks access; it is not a vulnerability scan.

Run the scan and confirm success

1 Start a new assessment

Click New Scan. Choose Credentialed Windows Assessment. Enter only the authorized target, for example 192.168.1.195 or 192.168.1.195/32 where a scope field is used. Select the CyberTech laptop credential profile, complete the authorization confirmation and submit the scan. Button labels can vary by installed build.

To repeat a configured assessment, open its saved report and click Rerun Assessment. Check the target and credential first. Do not reuse the guide's example assessment number as if it existed on every installation.

2 Watch the monitor

Keep the target awake and retain account permissions. The tested collector allows three minutes per full Windows collection attempt; total scan time may be longer. A temporary progress pause does not prove a freeze.

3 Open the assessment and check all results

What to check	Expected for a complete successful collection
Scan status	COMPLETED
Progress	100% after completion
Connectivity	REACHABLE
Authentication	SUCCESS
Identity	TARGET\scan-account
Privilege	ADMINISTRATOR
Evidence	SUCCESS
Inventory	Windows details and collected inventory are visible

PARTIAL means some checks did not complete. It is not the same as a full assessment. Zero findings on an incomplete scan is not evidence that the target is secure. Even a successful scan covers only the checks supported by the selected template.

Example from the completed training session

Assessment 49 succeeded with administrator access: 32 applications, 6 hotfixes and 9 findings (3 high, 4 medium, 2 low). Your results will vary.

4 Save the report

Open Scans > Scan History > the local date > the report. Export JSON or CSV if needed. Save the report and review findings with the owner before making changes.

Troubleshoot in this order

Result or symptom	Next action
TCP 5985 unreachable	Confirm target IP, power and Private network. Check the target's WinRM service, listener and firewall remote scope. Check guest Wi-Fi/VPN isolation.
Authentication failed	Confirm TARGET computer name, account name and actual password. Reload the secret for the selected profile. Check account enabled/locked/expired state.
SUCCESS but STANDARD	On the TARGET, verify approved Administrators membership. For this workgroup setup, check the local token policy. Start a fresh credential test.
SUCCESS but PARTIAL	Read the unavailable-check list. Verify administrator privilege. Missing features, provider errors and policy restrictions can also cause partial results.
Collection exceeded timeout	Check the target's responsiveness and Windows providers. Use the current support-approved build. Do not repeatedly reset the password.
Secret unavailable after restart	Reload the password in Step 2, or use approved DPAPI persistence. A ready secret does not prove it matches the target.
Member was not found in group	If you ran Remove-LocalGroupMember, you may have removed scan access already. Re-add only when administrator access is still required for the exercise.
Application still shows old behavior	Confirm the running installation and its folder. Finish active scans, restart the correct instance, refresh the browser, then verify the version and behavior.

Optional direct login check

On the SCANNER, run this in Windows PowerShell. Enter the password in the credential prompt, not in the command. Expected output: the target account name. This checks remote login only. [4]

```
$cred = Get-Credential -UserName 'CyberTech-Intel\vunfisher_scan' `
    -Message 'Target scan account password'
$test = @{
    ComputerName = '192.168.1.195'
    Port = 5985
    Authentication = 'Negotiate'
    Credential = $cred
    ScriptBlock = { whoami }
}
Invoke-Command @test
Remove-Variable cred
```

For support, provide the assessment number, target, timestamp, privilege and diagnostic text. Do not provide the password or credential-secret files.

Only for a tool or exercise that explicitly requires Remote Registry

Remote Registry is a separate optional path

VunFisher's tested Windows WinRM collector reads registry values inside its remote PowerShell session. It does not require the Windows Remote Registry service. Do not enable Remote Registry to fix a WinRM password, privilege or timeout error.

If a different approved tool requires Remote Registry

1. On the TARGET, open Services from Start or run services.msc. Record the Remote Registry service's original startup type and status. With IT approval, set it to Manual, click Apply, then Start. If policy disables it, have IT approve the change rather than overriding policy.

2. Ask IT to permit the required Remote Registry transport from the SCANNER only. The Windows protocol commonly uses the winreg named pipe over SMB. For that transport, TCP 445 is needed; other RPC requirements depend on the tool. Do not enable every File and Printer Sharing rule or open ports to the internet. Keep only the approved firewall profile and source IP scope. [7]

3. Use an approved target account with the required registry read permissions. Local administrator remote token restrictions may also apply. Do not grant Everyone access or change registry ownership as a general workaround.

4. On the SCANNER, open Registry Editor using the approved identity. Select File > Connect Network Registry, enter the TARGET computer name, then connect. Read only the test key approved by IT. If your current Windows identity is not accepted, use your tool's credential option or have IT establish the correct authenticated session; Registry Editor does not provide the same credential profile form as VunFisher.

5. Confirm the intended remote computer appears and the approved key is readable. Do not edit values during a read-only exercise. After the exercise, disconnect and restore only the service and firewall changes made for it.

Equivalent service commands for an approved exercise

Run on the TARGET in administrator Windows PowerShell. These commands only configure the service; they do not grant registry rights, configure the firewall or prove connectivity.

```
Get-Service RemoteRegistry | Select-Object Name,Status,StartType
Set-Service RemoteRegistry -StartupType Manual
```

```
Start-Service RemoteRegistry
```

Use this optional path only when the selected scanner explicitly supports and requires Remote Registry. The VunFisher profile in this guide remains Windows WinRM on port 5985.

After the scan restore temporary access

Complete and save the scan first. For recurring production scans, IT decides which approved access should remain. Do not undo settings that were already required by other tools or administrators.

1 Remove temporary administrator membership on the target

Only if you added this membership for the exercise: open Computer Management > Local Users and Groups > Groups > Administrators, select vunfisher_scan and remove it. This removes membership, not the account. The PowerShell equivalent is:

```
Remove-LocalGroupMember -SID 'S-1-5-32-544' -Member 'vunfisher_scan'
```

Run the removal once. “Member was not found” means the account is not currently in that group. Removing membership makes later full scans fail or become partial; reapprove access before a future assessment.

2 Restore the recorded target settings

If you changed LocalAccountTokenFilterPolicy only for this exercise, use Registry Editor to restore its recorded original value. If it was absent, remove only the value you created. Do not delete the System key. If it was already 1 for an approved purpose, do not change it blindly.

Restore the previous firewall rule scope and profile, or disable only a rule created exclusively for this exercise. Ask IT before stopping WinRM, removing listeners or disabling PowerShell endpoints: other management tools may rely on them. Do not assume Disable-PSRemoting reverses every service, listener and firewall change.

3 Restore the scanner settings

If the target was newly added to TrustedHosts only for the exercise, remove just that entry through the same method you used. Retain all pre-existing approved entries. If managed by Group Policy, have IT update that policy. Restore the scanner’s original WinRM service setting only if it is no longer needed.

In VunFisher, clear the runtime or remembered secret for the exercise profile when it is no longer needed. Disable the dedicated credential profile or target account if required by your

organization. Do not delete shared accounts or profiles.

Instructor completion check

The trainee can identify SCANNER versus TARGET; explain WinRM versus Remote Registry; test the intended account; recognize SUCCESS versus PARTIAL; locate the saved report; and restore temporary access only after the scan is complete.

Reference notes for instructors

The procedures combine Microsoft's documented Windows configuration with the VunFisher workflow observed in this training session. The successful acceptance example is assessment 49 supplied by the user. The guide's alternative setup routes have been reviewed for syntax and consistency, but have not each been run on a newly installed Windows machine.

This is a workgroup IPv4 lab procedure using Windows PowerShell 5.1 and WinRM HTTP 5985 with Negotiate. It does not instruct users to enable Basic authentication, unencrypted WinRM traffic, CredSSP, public-network access or internet forwarding. Organizations should prefer their approved domain/Kerberos or certificate-based management design. Adding a TrustedHosts entry does not authenticate the target server. [4,8]

1 Enable PSRemoting

2 Set NetFirewallRule

3 User Account Control and remote restrictions

4 PowerShell remote troubleshooting

5 New LocalUser

6 Test NetConnection

7 Remote Registry protocol server transport

8 Security considerations for WinRM remoting

Windows labels and available features vary by edition and organization policy. An unavailable cmdlet, absent feature or blocked provider should be recorded as unavailable evidence, not interpreted as a secure setting or a bad password.