## **Install Nessus Essentials on Windows**

### Steps:

Go to Nessus Downloads

Select **Windows 64-bit**, download the .exe installer

Run the installer as Administrator

After installation, Nessus will start and open in your browser:  
https://localhost:8834

Select **"Nessus Essentials"** and **register for a free activation code**

Enter the activation code and let it download plugins (~15 mins)

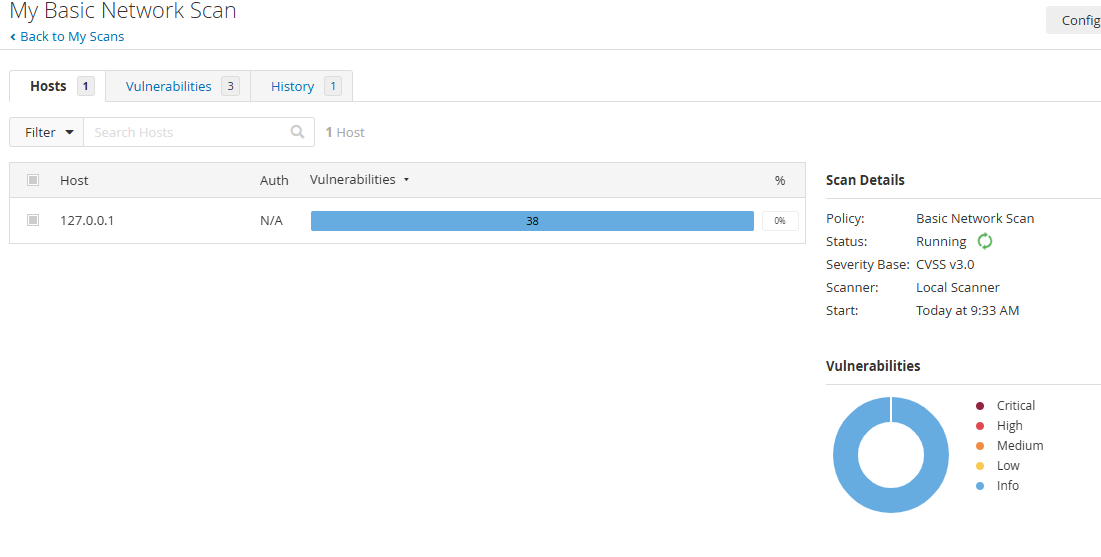
## **Start a Full System Vulnerability Scan**

From the Nessus dashboard → **New Scan** → **Basic Network Scan**

Target: 127.0.0.1 (localhost)

Name: "Local Windows Scan"

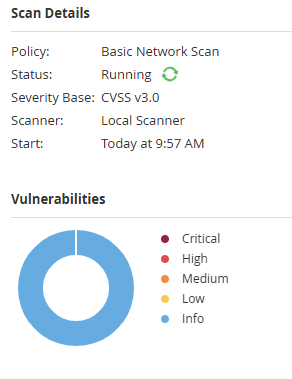
Save and **Launch Scan**



This may take **30–60 minutes** depending on your system.

You’ll see vulnerabilities ranked by severity:

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



## **Common Windows Vulnerabilities & Fixes**

### **SMBv1 Enabled (CVE-2017-0144 – WannaCry)**

**Fix:**

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

### **Unpatched Windows (Missing Cumulative Updates)**

**Fix:**

Go to **Settings → Windows Update**

Install all security and quality updates

### **Weak RDP Configuration**

Disable RDP if not needed:  
System Properties → Remote → Uncheck "Allow remote connections"

If used, enable NLA (Network Level Auth) only:

Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'UserAuthentication' -Value 1

### **Outdated Software (Java, Flash, WinRAR, etc.)**

Uninstall unused legacy software

Use PatchMyPC to auto-update apps

### **Missing Local Firewall Rules**

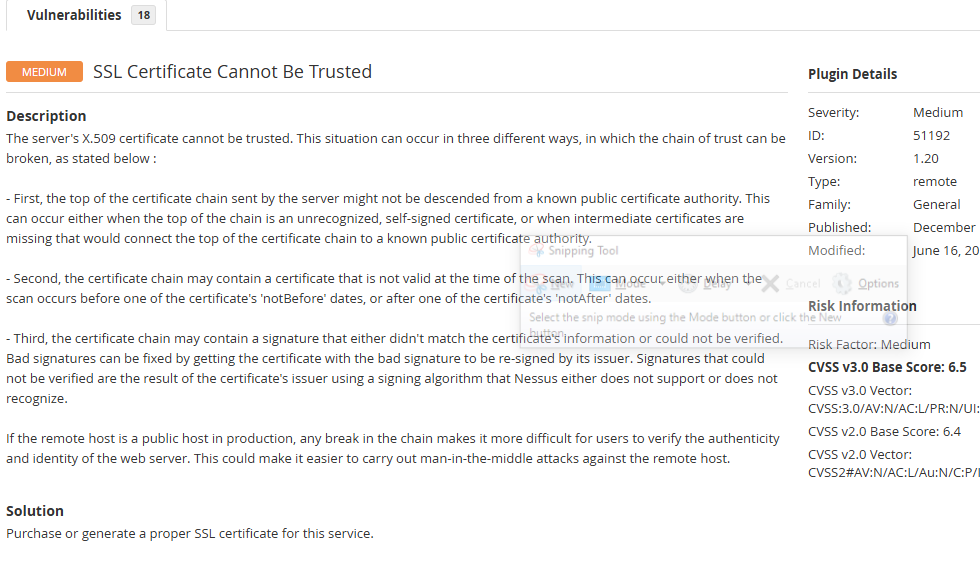
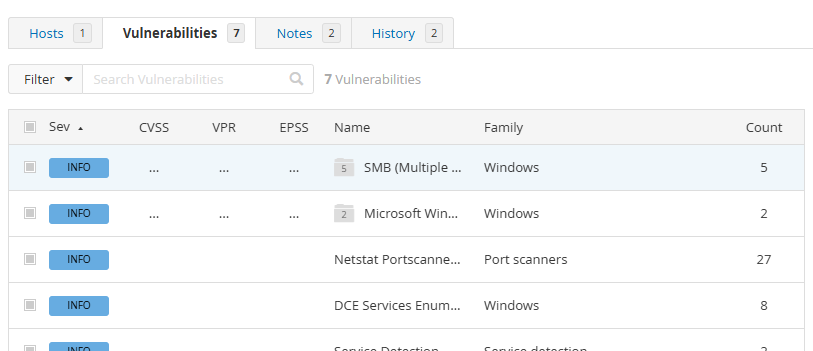
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

Take screenshots of:

Critical/High vulnerability list

CVE details page

Suggested fix page



## **Final Recommendations**

Use **Windows Defender** or a trusted antivirus

Keep **Windows Update enabled**

Regularly run **Nessus** (weekly or monthly scans)

Review **Windows Event Logs** for unusual activity