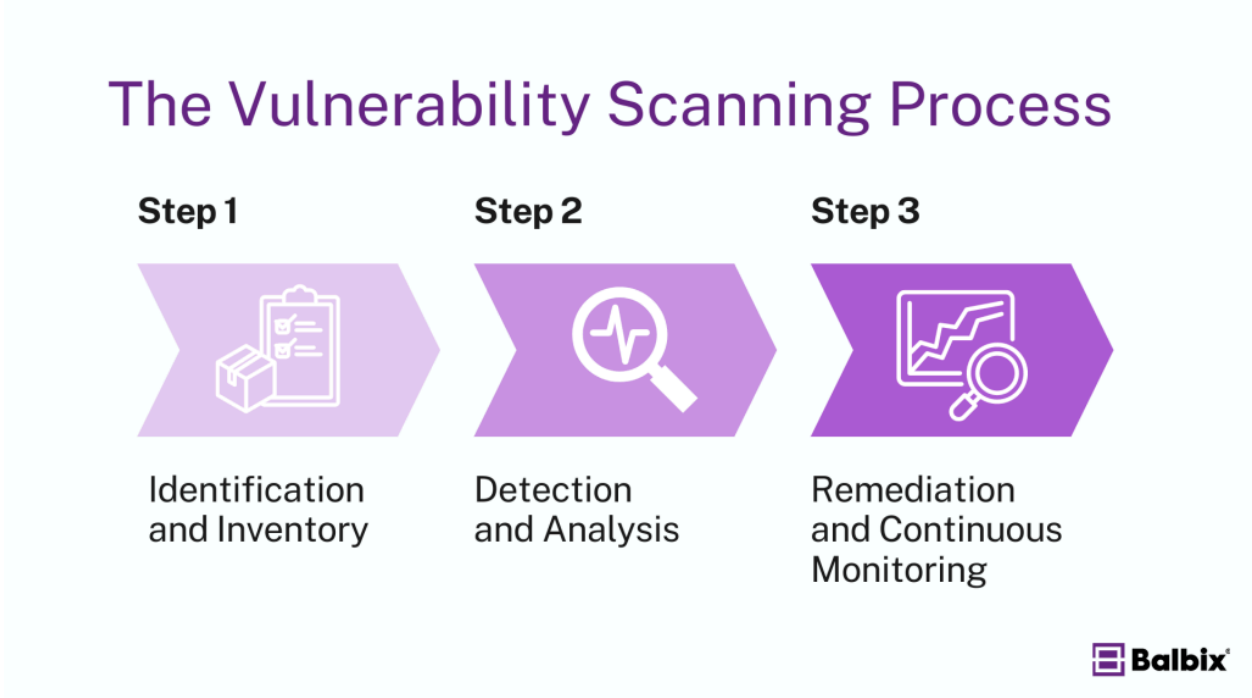
Azure Vulnerability Lab Scanner

This project showcases practical cloud security operations by implementing a complete vulnerability management process in Microsoft Azure, including asset deployment, threat discovery, credentialed scanning, vulnerability remediation, and post-fix verification using OpenVAS.

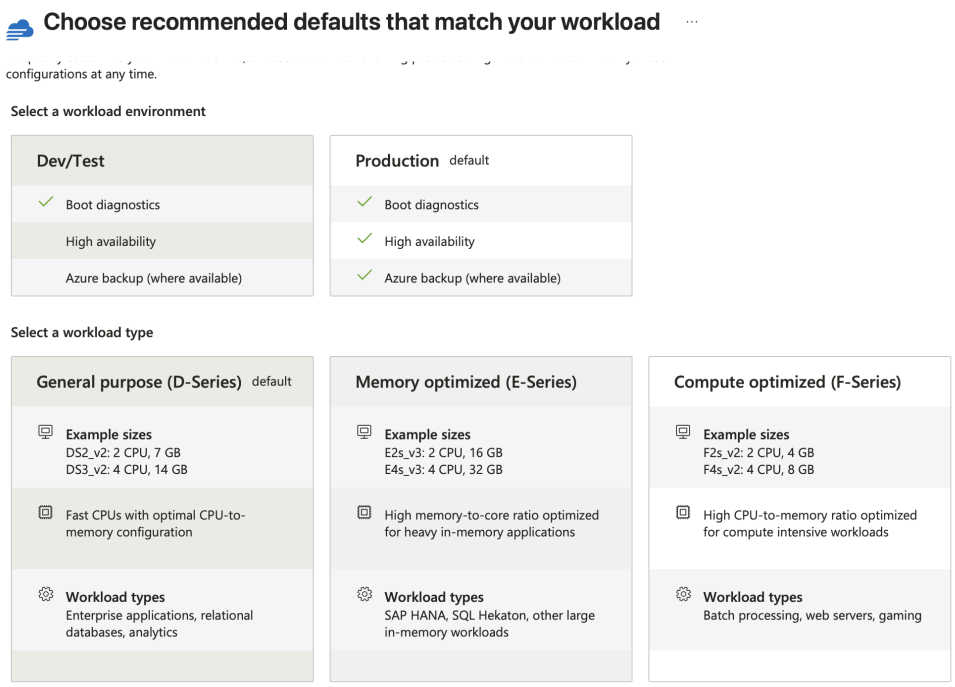
Prerequisites

- Computer with Internet access
- Azure Account (Free Subscription may be possible)
    - Create your Free Azure Account here
    - Log in to your Azure Account here



Step 1: Prepare Vulnerability Management Scanner

1. Go to Azure Portal.
2. Navigate to the Marketplace and search for "OpenVAS secured and supported by HOSSTED."
3. Choose "Start with a pre-set configuration" and select the weakest configuration.

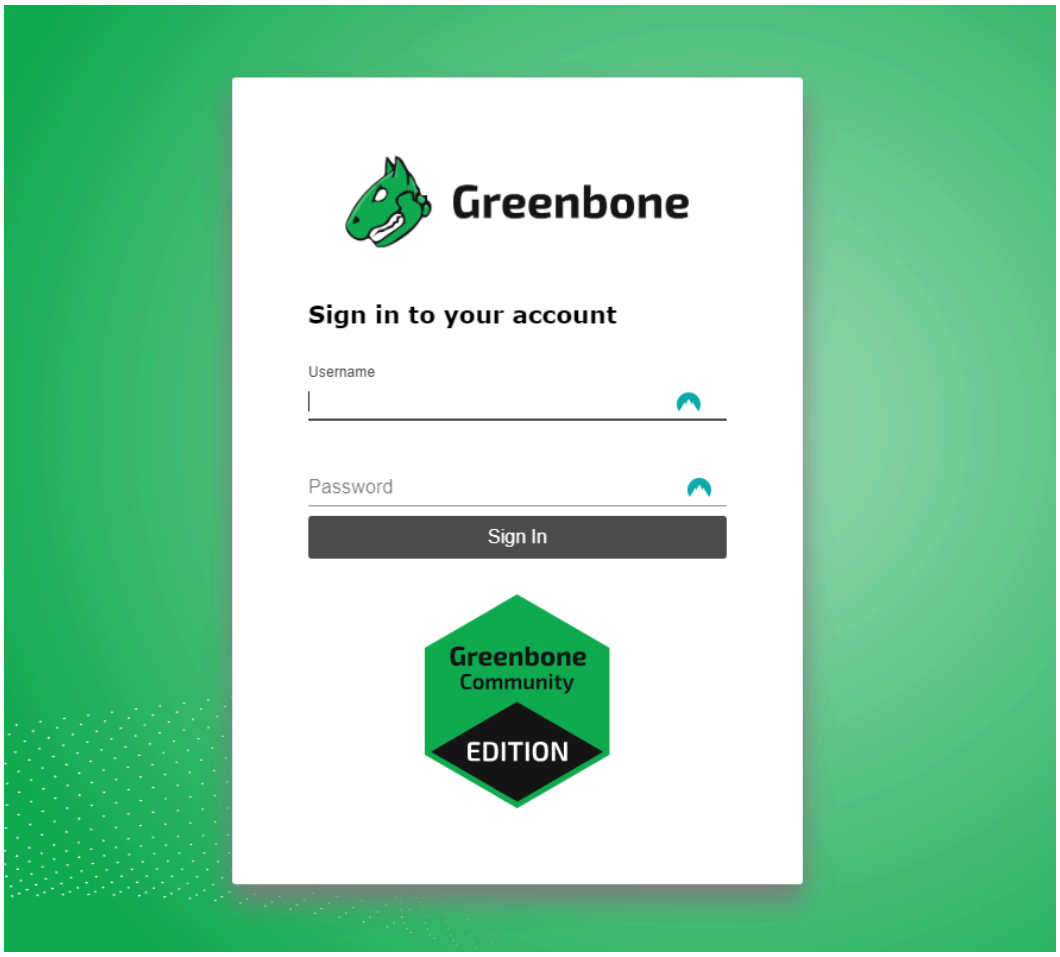


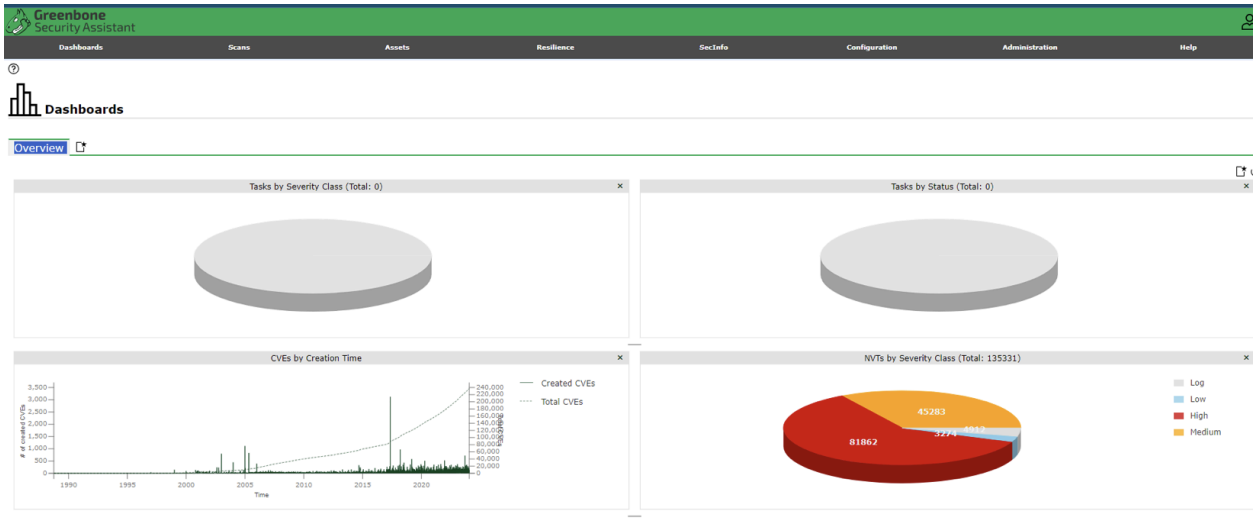
4. Continue to create the VM:
    - Resource Group: Vulnerability-Management
    - VM Name: OpenVAS (Note the region and Vnet - consider East US 2)
    - Security: Standard
    - Authentication: Username → azureuser / Password → Cyberlab1234!
    - Monitoring: Disable Boot Diagnostic (not needed)
    - Management: Disable auto-deploy
5. Create the VM.
6. Once created, SSH into it using PowerShell (Windows) or Terminal (MacOS) with the credentials you created.

```
sudo ssh username@ip
```

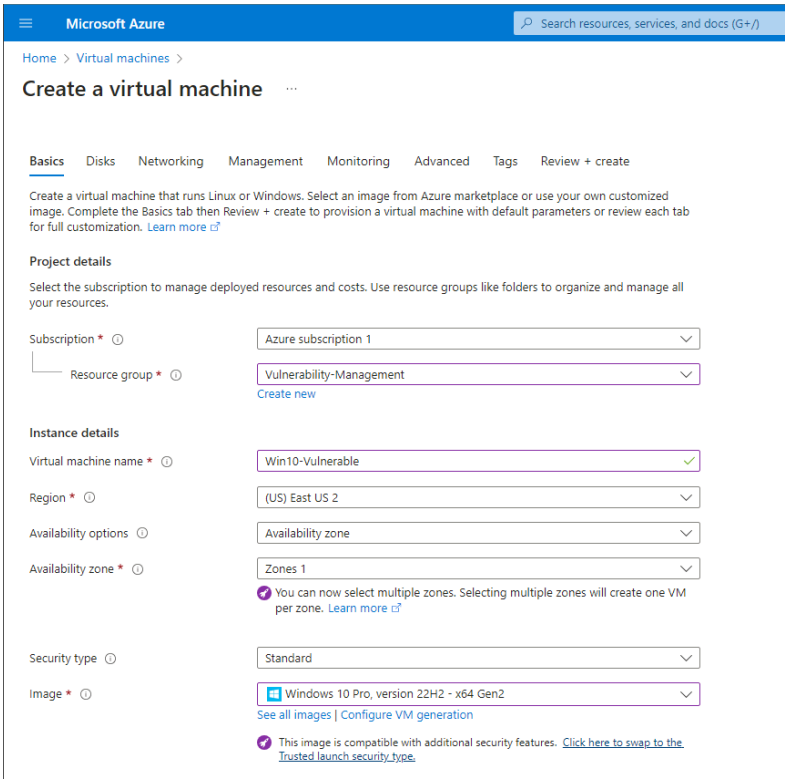
7. Wait for the deployment to complete, and it should display the web app URL and default username and password.

8. Copy the URL and log in to the web app. If it doesn't work, try using admin/admin.


Greenbone
Sign in to your account
Username
Password
Sign In
Greenbone
Community
EDITION


Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Dashboards
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
Created CVEs
Total CVEs
NVTs by Severity Class (Total: 135331)
45283
81862
Log
Low
High
Medium

Step 2: Create Client VM and Make it Vulnerable



1. Go to Azure Portal.
2. Search for Virtual Machines and create a new Virtual Machine.
3. Configure the VM:
    - Resource Group: Vulnerability-Management
    - VM Name: Win10-Vulnerable
    - Region: Same as the OpenVAS VM (East US 2)
    - Virtual Network: Same as OpenVAS
    - Image: Windows 10 Pro
    - Size: Any size with 2 vCPUs
    - Username: azureuser / Password: Cyberlab1234!
    - Networking: Same Vnet as OpenVAS
4. Create the VM.
5. Once created, ensure you can RDP into it with the credentials.

- MacOS needs an RDP app to access

6. the VM vulnerable by:

- Disabling the Windows Firewall (Allows Vulnerability Scanner to Scan the VM without dropping traffic)
    - Start > wf.msc > Firewall Properties
        - Domain Profile > Off
        - Private Profile > Off
        - Public Profile > Off
- Installing old software on Win10-Vulnerable VM! :

https://drive.google.com/drive/u/2/folders/1n83ilCjZWZulbDdYnUe9wQPK2buY47_U

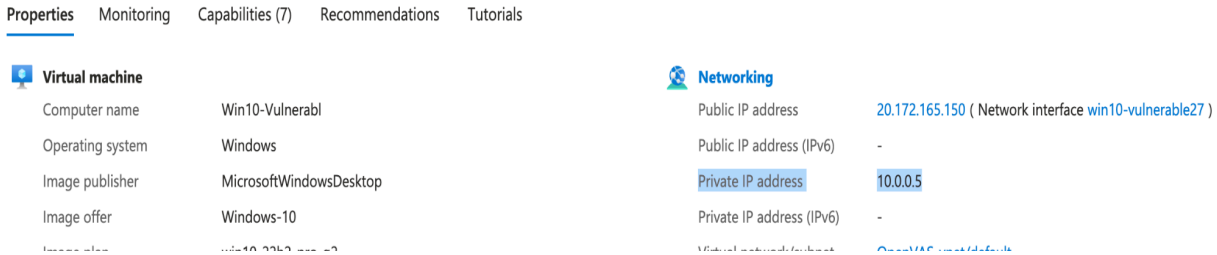
- Old Version of Firefox: Firefox Setup 97.0b5
- Old Version of VLC Player: vlc-1.1.7-win32

- Old Version of Adobe Reader: 10.0_AdbeRdr1000_en_US_1_

7. Restart the VM.

Step 3: Configure and Run Unauthenticated Scan with OpenVAS

1. Log in to OpenVAS.
2. Navigate to Assets → Hosts → New Host.
3. Add the Client VM PRIVATE IP Address. -Found in Azure: VM > Win10-Vulnerable Properties > Private IP



1. Create a new Target from the Host, naming it "Azure Vulnerable VMs."
2. Take note of the credentials; SMB credentials will be added later.
3. Create a new Task:
    - Name & Comment: "Scan - Azure Vulnerable VMs"
    - Scan Targets: "Azure Vulnerable VMs"
4. Save the Task.
5. Start the "Scan - Azure Vulnerable VMs" Task.
6. Take note of the scan status.
7. After the scan finishes, click the date under "Last Report" to view the results.
8. Examine the "Results" tab. Note that some vulnerabilities may not appear due to the unauthenticated scan.

Results

- The scan did not find the vulnerable installed apps since it was not an authenticated scan

Report:Sun, Sep 3, 2023 3:00 AM UTC Done

ID: ea4b79a

Information | Results (3 of 32) | Hosts (1 of 1) | Ports (2 of 4) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (7 of 7) | TLS Certificates (1 of 1) | Error Messages (1 of 1) | User Tags (0)

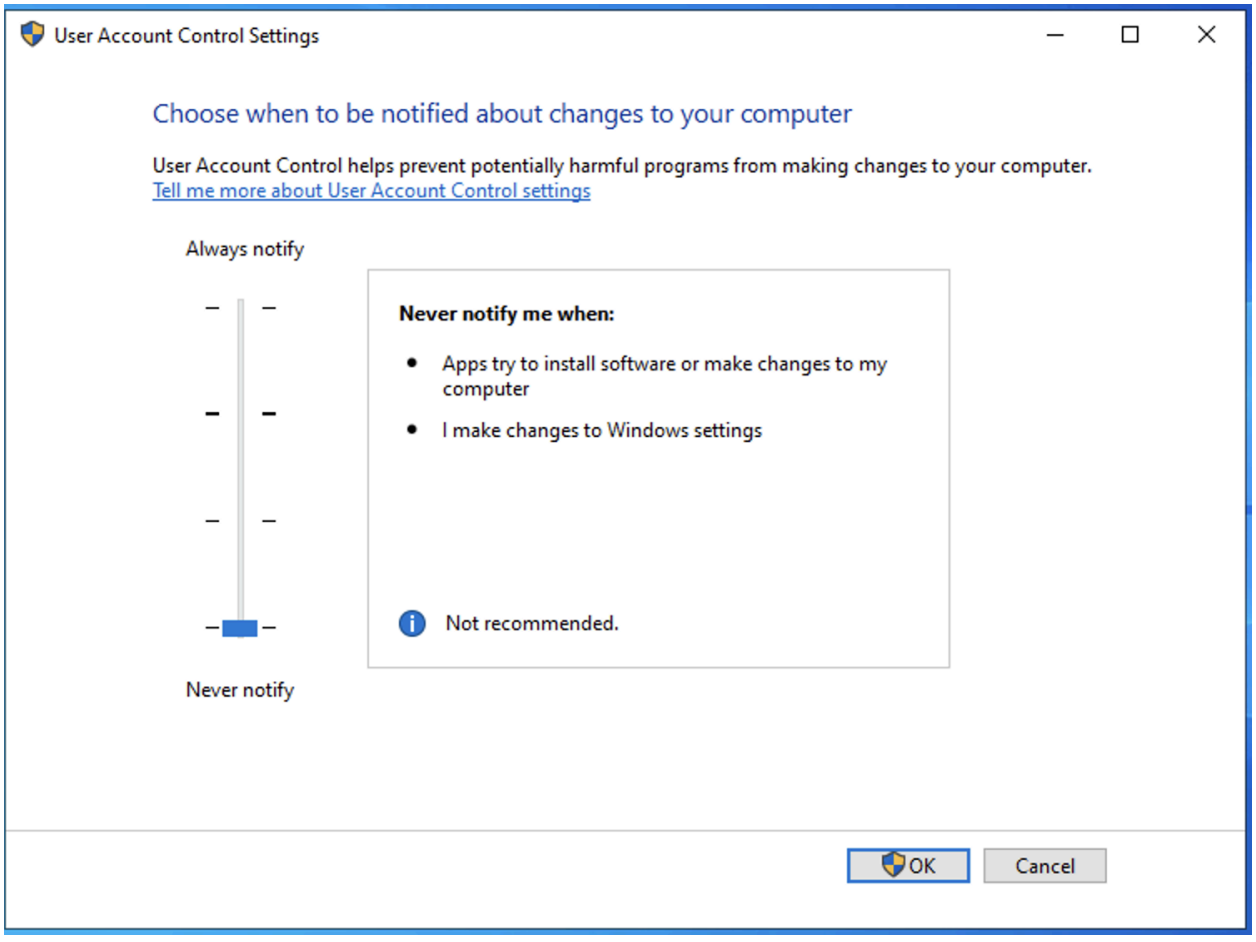
Vulnerability	Severity ▼	QoD	Host	
			IP	Name
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.0.0.5	win10-v
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.0.0.5	win10-v
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	10.0.0.5	win10-v

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Step 4: Configure Authenticated Scans (Within VM)

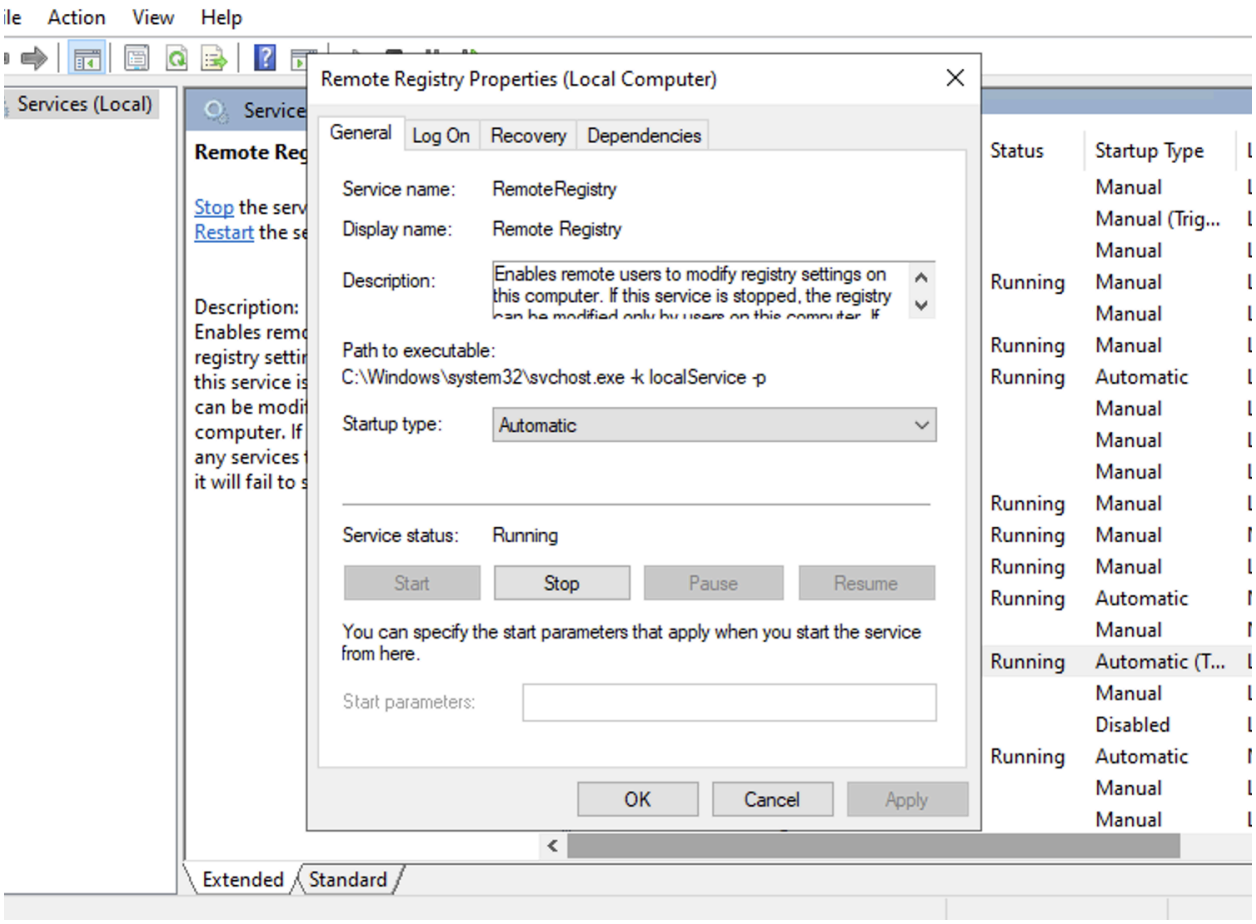
On the vulnerable Windows VM, perform the following configurations:

- Disable Windows Firewall
- Disable User Account Control
    - Start > "user account control" > set to "never notify" -



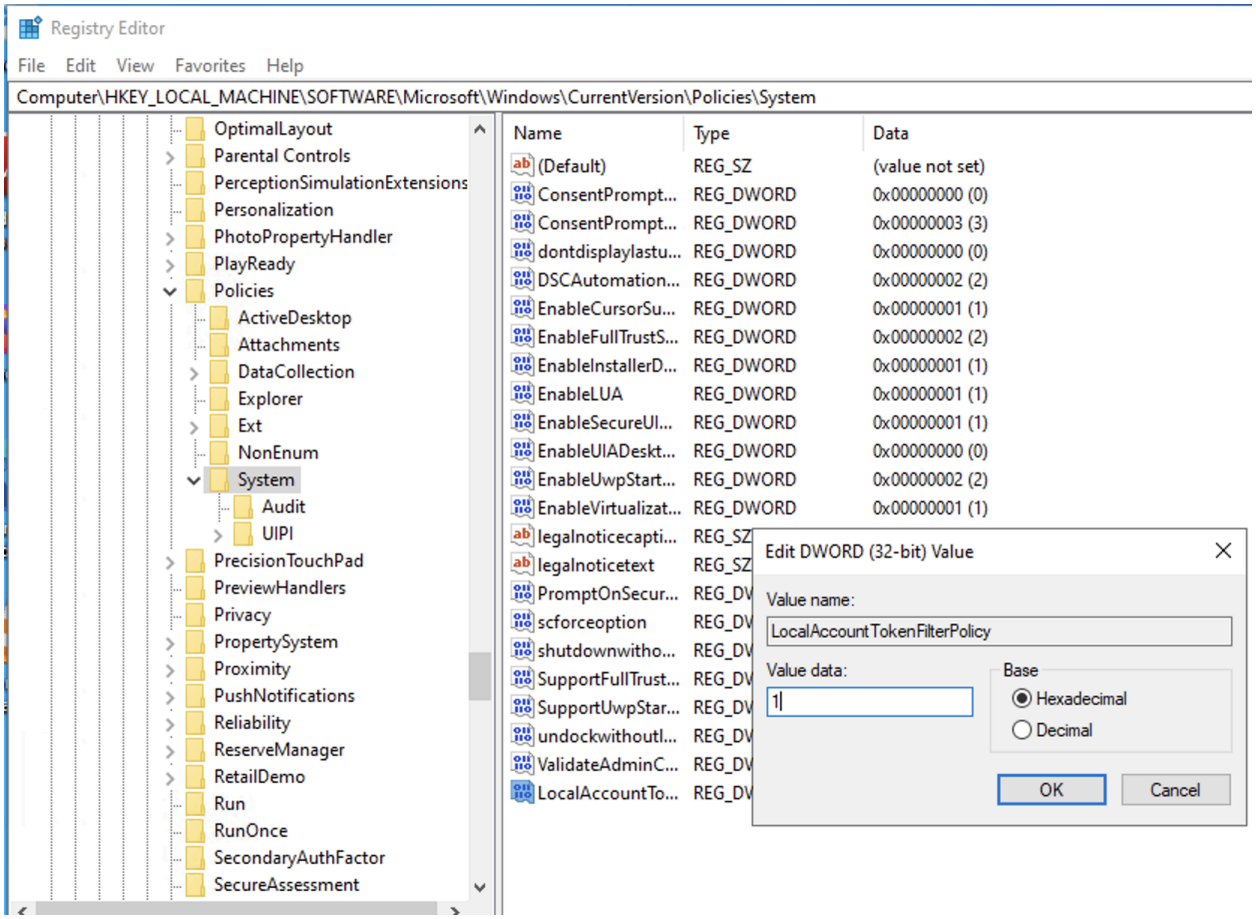
Enable Remote Registry

- Start > services.msc
- Search for: Remote Registry > Properties > Startup type: Automatic > Apply > Start -



Set Registry Key (LocalAccountTokenFilterPolicy: 1)

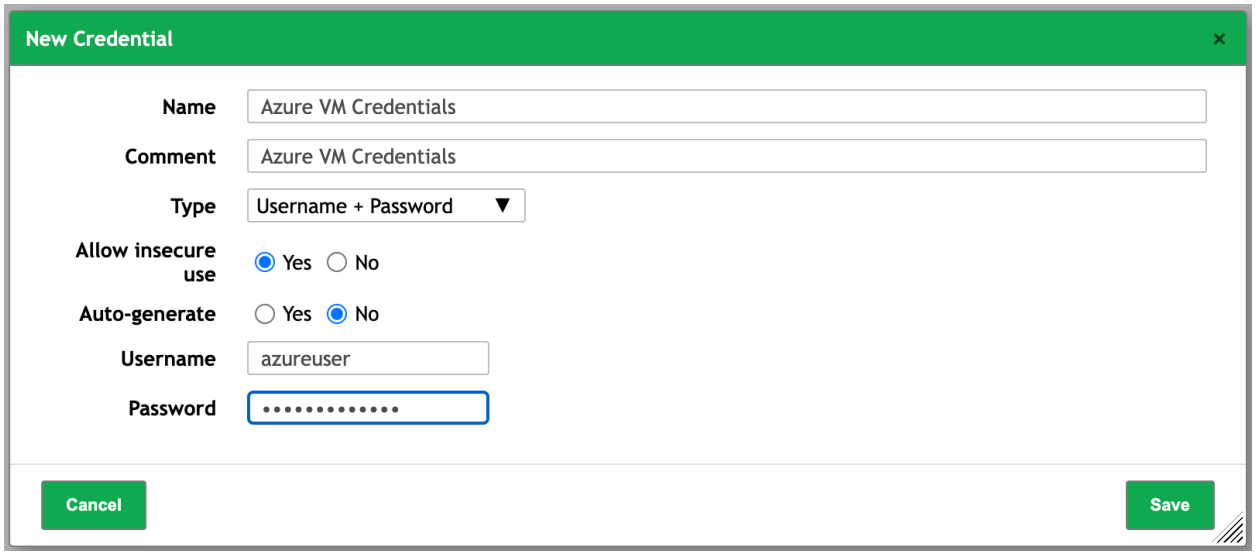
- Start > regedit > HKEY_LOCAL_MACHINE > Open SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Create a new DWORD (32-bit) value with the following properties:
    - Name: LocalAccountTokenFilterPolicy
    - Value: 1 -



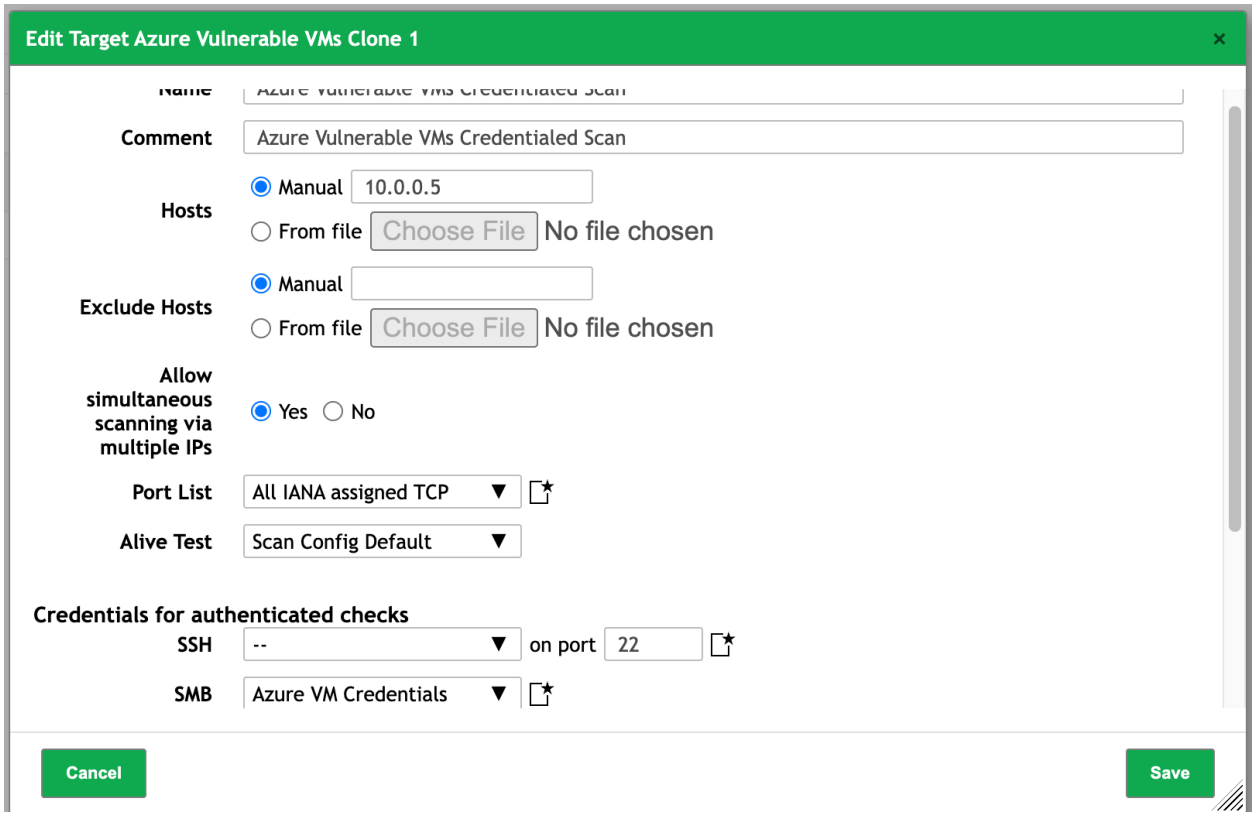
- Restart VM

Configure Authenticated Scans (OpenVAS)

1. In OpenVAS, go to Configuration → Credentials → New Credential.
2. Name / Comment: "Azure VM Credentials."
3. Allow Insecure Use: Yes
4. Username: azureuser
5. Password: Cyberlab1234!



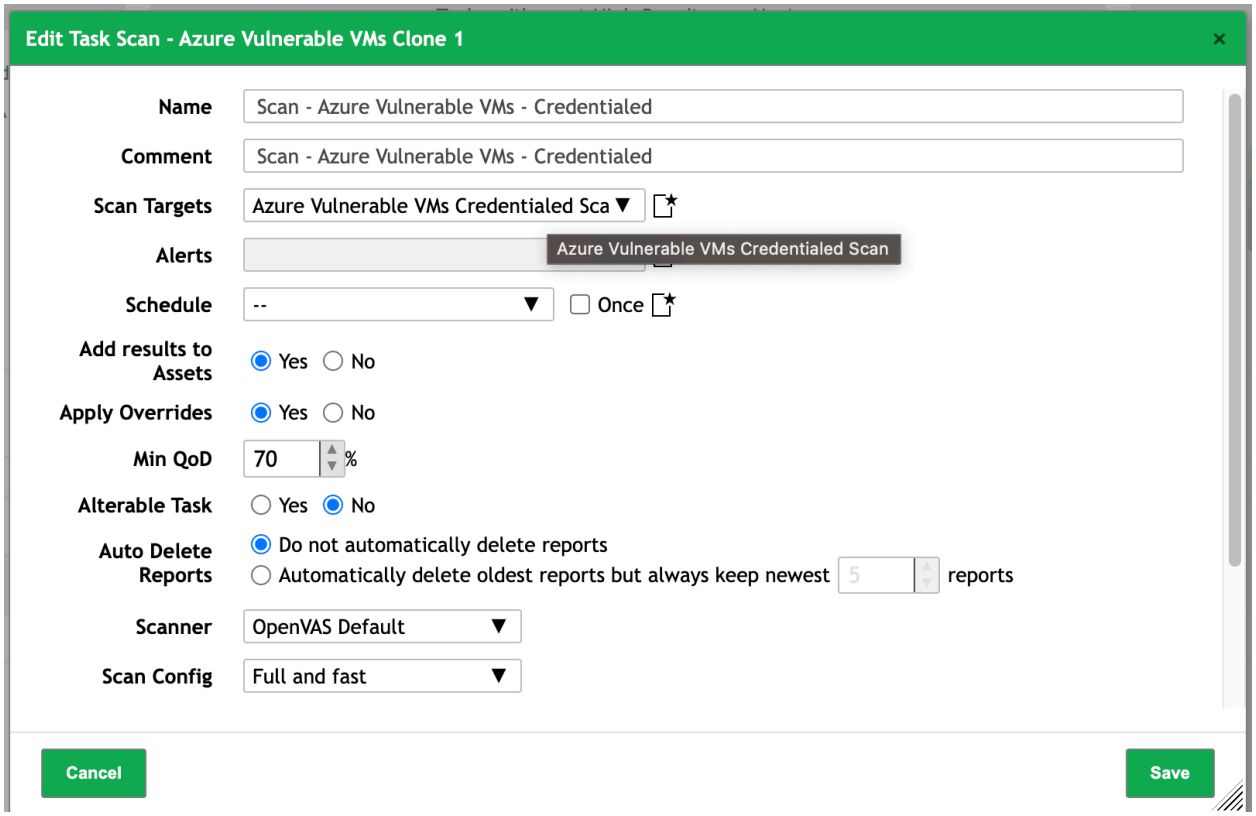
6. Save.
7. Go to Configuration → Targets → Clone the Target previously created.
8. Name / Comment: "Azure Vulnerable VMs - Credentialed Scan."
9. Ensure the Private IP is still accurate.
10. Credentials → SMB → Select the "Azure VM Credentials" created earlier.



11. Save.

Step 5: Execute Authenticated Scan against Vulnerable Windows VM

1. In OpenVAS, go to Scans → Tasks.
2. Clone the "Scan - Azure Vulnerable VMs" Task and edit it:
    - Name / Comment: "Scan - Azure Vulnerable VMs - Credentialed."
    - Targets: Azure Vulnerable VMs - Credentialed Scan



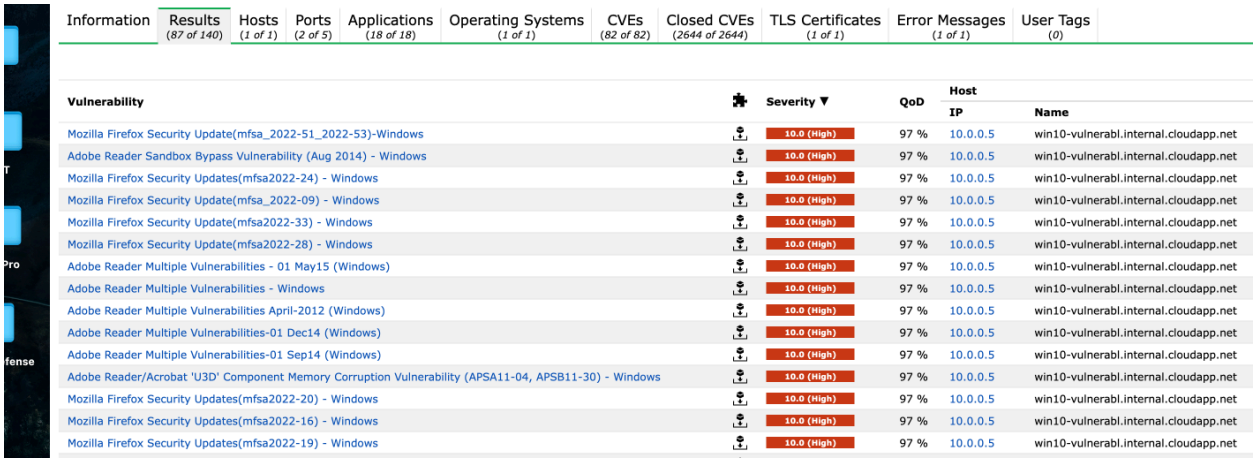
3. Save.

4. Launch the new Credentialed Scan and wait for it to finish (this may take longer).

5. After the credentialed scan finishes, check SMB Login under "Results."

6. Inspect individual vulnerabilities, including critical findings related to outdated software.

7. Remove the filter (upper right).

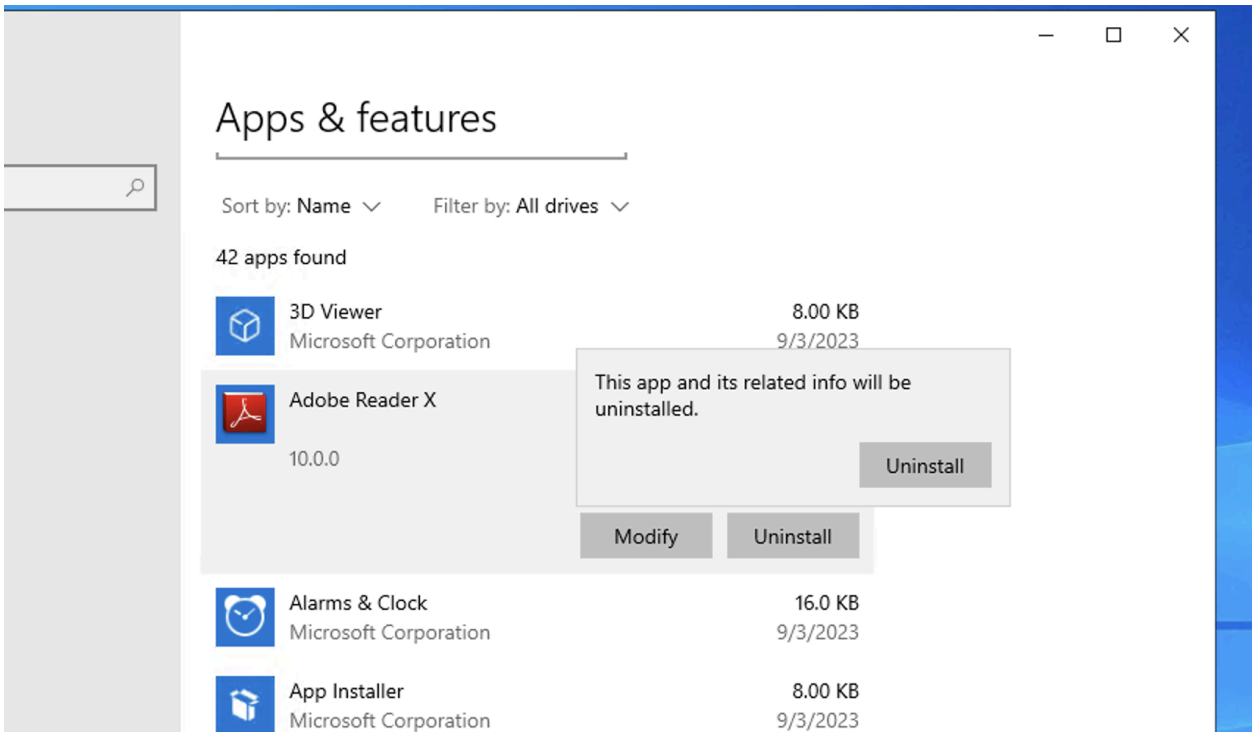


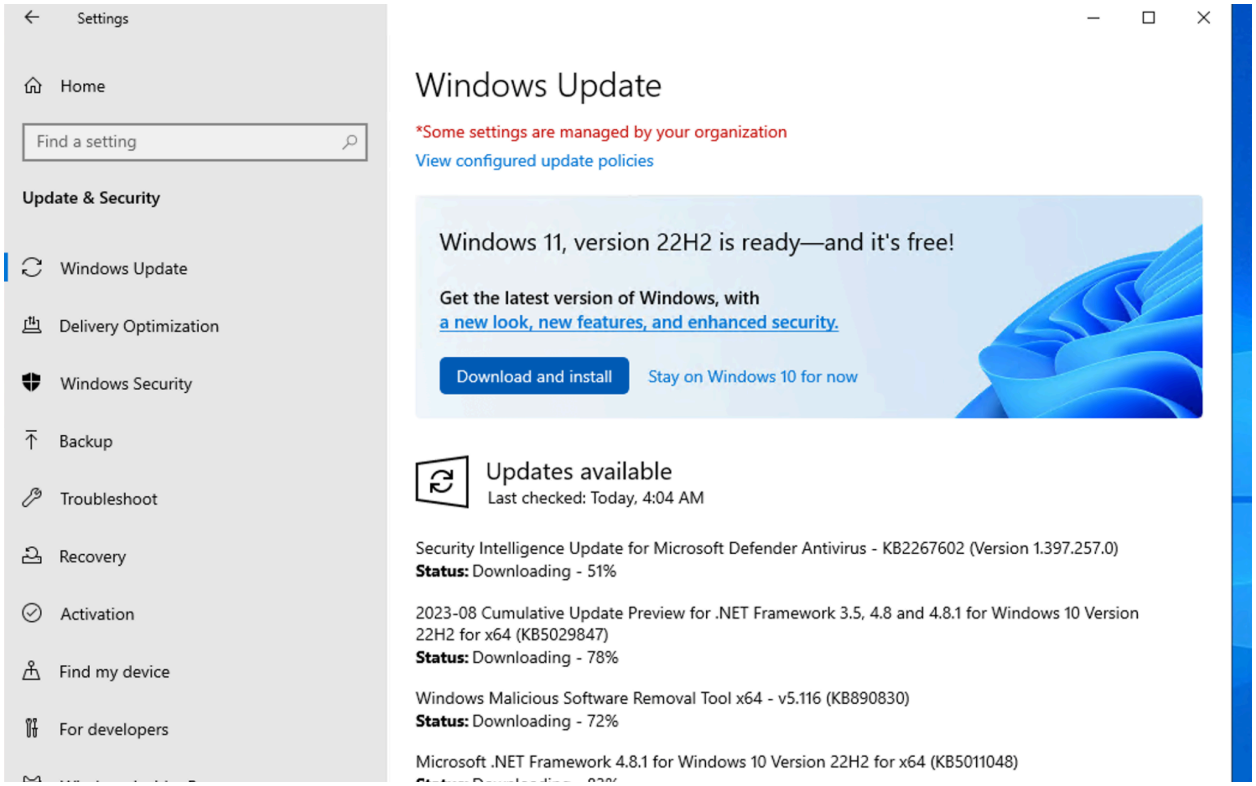
Information | Results (87 of 140) | Hosts (1 of 1) | Ports (2 of 5) | Applications (18 of 18) | Operating Systems (1 of 1) | CVEs (82 of 82) | Closed CVEs (2644 of 2644) | TLS Certificates (1 of 1) | Error Messages (1 of 1) | User Tags (0)

Vulnerability	Severity ▼	QoD	Host IP	Host Name
Mozilla Firefox Security Update(mfsa_2022-51_2022-53)-Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Sandbox Bypass Vulnerability (Aug 2014) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Updates(mfsa2022-24) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Update(mfsa_2022-09) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Update(mfsa2022-33) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Update(mfsa2022-28) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Multiple Vulnerabilities - 01 May15 (Windows)	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Multiple Vulnerabilities - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Multiple Vulnerabilities April-2012 (Windows)	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Multiple Vulnerabilities-01 Dec14 (Windows)	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader Multiple Vulnerabilities-01 Sep14 (Windows)	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Adobe Reader/Acrobat 'U3D' Component Memory Corruption Vulnerability (APSA11-04, APSB11-30) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Updates(mfsa2022-20) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Updates(mfsa2022-16) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net
Mozilla Firefox Security Updates(mfsa2022-19) - Windows	10.0 (High)	97 %	10.0.0.5	win10-vulnerabl.internal.cloudapp.net

Step 6: Remediate Vulnerabilities

1. Log back into your Win10-Vulnerable VM.
2. Uninstall Adobe Reader, VLC Player, and Firefox.
3. Update Windows

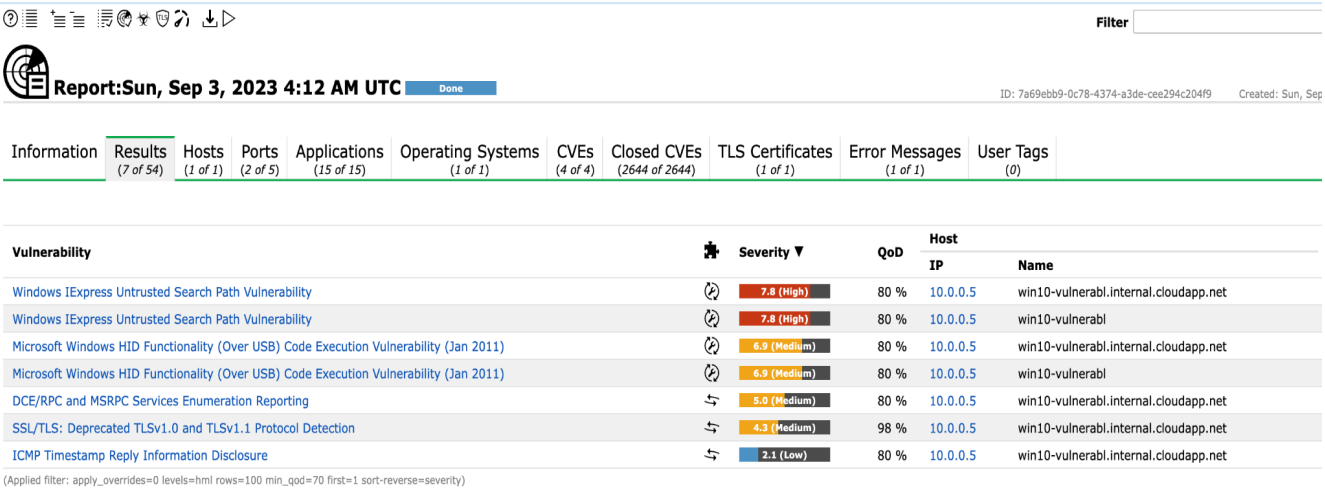




4. Restart VM

Step 7: Verify Remediations

1. Re-initiate the "Scan - Azure Vulnerable VMs - Credentialed" scan and observe the results.



Summary:

I built a cloud-based security lab in **Microsoft Azure** to demonstrate the complete **vulnerability management lifecycle**. The project involved deploying **OpenVAS**, performing both **unauthenticated and authenticated vulnerability scans against** a purposely vulnerable Windows VM, analyzing critical findings, executing **remediation actions**, and validating fixes through **re-scanning**. This lab showcases hands-on experience with **cloud security operations, risk assessment, remediation, and vulnerability verification**.