Nessus Scanner

Adding an Asset

1. Click-on "Assets" and then "+ Add" (top-right)
2. Click-on "Static IP List"
3. Provide the following details and click-on "Submit"
    - Name: `Assets - Windows Servers`
    - IP Addresses: `192.168.3.10,192.168.3.11`

Adding Credentials

1. Click-on "Scans > Credentials"
2. Click-on "Add a Credential" or "+ Add" (top-right)
3. Select "Password"
4. Provide the following details and click-on "Submit"
    - Name: `Credentials - Windows Servers & Clients`
    - Username: `nessus`
    - Password: `YourPassword123!`

Adding an Audit File

Audit Files are the baselines you want to measure a machine against. Ensure to download SCAP content and upload it to SecurityCenter.

1. Click-on "Scans > Audit Files"
2. Click-on "Add an Audit File" or "+ Add" (top-right)
3. Select "Advanced"
4. Browse for and select the relevant SCAP benchmark. It should be zipped and include a single XML file. Once uploaded, SecurityCenter should ask you to confirm details similar to what is listed below.
   - Audit file: `U_MS_Windows_2012_and_2012_R2_DC_VR19_STIG_SCAP_1-2_Benchmark.zip`
   - Data Stream Name: `scap_mil.disa.stig_datastream...`
   - Benchmark Type: `SCAP Windows`
   - Benchmark Name: `ccdf_mil.disa.stig_benchmark_Windows_2012_DC_STIG`
   - Profile: `xccdf_mil.disa.stig_profile_MAC-1...`
5. Provide the following details and click-on "Submit"
    - Name: `Audit File - Windows Server 2012 R2 STIG SCAP Benchmark`

Creating a Policy

Policies represent what kind of scan you want to run. For example, you may want to perform a simple "host discovery" scan or audit your machines for compliance.

1. Click-on "Scans > Policies"
2. Click-on "Add a Policy" or "+ Add" (top-right)
3. Select which kind of scan you want to run (ex: `SCAP and OVAL Auditing`)
4. Provide the following details and click-on "Submit"
    - Name: `Policy - Windows Server 2012 R2 STIG SCAP Benchmark`
    - Compliance: `Audit File - Windows Server 2012 R2 STIG SCAP Benchmark`

Creating an Active Scan

1. Click-on "Scans > Active Scans"
2. Click-on "Add an Active Scan" or "+ Add" (top-right)
3. Provide the following details and click-on "Submit"
    - Name: `Scan - Windows Server 2012 R2 STIG SCAP Benchmark`
    - Policy: `Policy - Windows Server 2012 R2 STIG SCAP Benchmark`
    - Schedule - Frequency: `Weekly`
    - Import Repository: `Repository - HQ`
    - Max scan duration (hours): `3`
    - Target Type: `Assets`
        - Assets: `Assets - Windows Servers`
    - Credentials: `Credentials - Windows Servers & Clients`

Scheduling a Scan

1. Click-on "Scans > Active Scans"
2. Click-on the play-button next to the Active Scan you previously created
3. Click-on "Scans > Scan Results" and wait for your scan to complete

Exporting Scan Results

1. Click-on "Scans > Scan Results"
2. Click-on the gear next to the scan you previously ran
3. Click-on "Download SCAP XML"
4. Extract the downloaded .xml file (ex: `1-2_windows-0-xccdf-res.xml`)

Reviewing DISA STIG and SCAP Benchmark Compliance

Before getting started, download the DISA STIG Viewer, your SCAP benchmarks, and most recent scan results to a machine separate from your Nessus scanner.

1. Open the DISA STIG Viewer
2. Click-on "File > Import STIG" and then, browse and select the relevant SCAP benchmark
3. Click-on the checkbox to the left of the STIG
4. Click-on "Checklist > Create Checklist - Check Marked STIG(s)"
5. Click-on "Import > XCCDF Results File" and then, browse and select the .xml file you exported from Nessus earlier (ex: `1-2_windows-0-xccdf-res.xml`)
6. Develop and execute a strategy for resolving "Open" vulnerabilities. This can be done by (1) implementing the fixes described within each rule (look for the "Fix Text" section) and (2) changing the "Status" of each when they have been addressed. Finally, when you believe you've made progress towards becoming more compliant, run another scan.

References

- Download DISA SCAP Benchmarks
- Download DISA STIG Files
- Download DISA STIG Viewer
- Download LGPO