Nessus Scanner

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: `Windows-Admin-for-Nessus`
    - Username: `miles.dyson`
    - Password: `ComeWithMeIfYouWantToLive1984`

Adding an Audit File

Audit Files are the baselines you want to measure a machine against.

1. Click-on "Scans > Audit Files"
2. Click-on "Add an Audit File" or "+ Add" (top-right)
3. Select "Windows"
4. Select the baseline to relevant the machine (ex: `DISA Windows Server 2012...`)
5. Provide the following details and click-on "Submit"
    - Name: `Baseline: Server 2012 R2 (v2)`
    - Logon Window Caption: `Notice and Consent Banner`
    - Logon Window Text: `You are accessing a Cyberdyne Systems (CS) machine...`
    - NTP Server: `ntp1.sky.net`

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 known-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: Audit via SCAP Definitions`
    - Compliance: `Baseline: Server 2012 R2 (v2)`

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: `Weekly Baseline Compliance Audit`
    - Policy: `Policy: Audit via SCAP Definitions`
    - Schedule - Frequency: `Weekly`
    - Import Repository: `Repository-California`
    - Max scan duration (hours): `3`
    - Target Type: `IP / DNS Name`
        - IPs / DNS Names: `192.168.1.0/24`
    - Credentials: `Windows-Admin-for-Nessus`

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

Reviewing DISA STIG and SCAP Benchmark Compliance

1. Download SCAP benchmarks and the DISA STIG Viewer
2. Run a `SCAP and OVAL Auditing` scan
3. Do the following using the DISG STIG Viewer:
    - Import the SCAP benchmark
    - Create a checklist
    - Import the XCCDF file (the scan results exported as an .xml file)

References

- Download DISA STIGs and SCAP Benchmarks
- Download DISA STIG Viewer
- Download LGPO