ACAS Scanning

ACAS Scanning

NOTE
ACAS will be reachable by the URL https://acas.lan on a properly configured CVA/H 3.5.0 DIP, if this is not the case then it may be reached by IP address instead.

1. Using a web browser, navigate to https://acas.lan
2. Log into your account.

Create a host scan discovery

NOTE
This step may be skipped if there is a pre-existing host discovery scan to be used.

1. Navigate to **Scans -> Policies** and click on the **+Add** button
2. Select the **Host Discovery** template
3. In the **Setup** tab, enter a **Name** for the scan (optional to enter a description)
4. In the **Configuration** section under **Discovery**, choose either **Host Enumeration**, **OS Identification**, **Port Scan (common ports)**, **Port Scan (all ports)**, or **custom**. Click **Submit**.
5. Navigate to **Scans** > **Active Scans and**
6. Click **Submit** to save the scan policy

Create a vulnerability scan policy

NOTE
This step may be skipped if there is a pre-existing scan policy to be used.

1. Navigate to **Scan -> Policies** and click on the **+Add** button
2. Select the **Advanced Scan** type
3. In the **Setup** tab, enter a **Name** for the scan
4. In the **Plugins** tab
   a. Click **Disable All** to disable all default plugins
   b. **Enable** any desired plugins
   c. Click on **Show Enable** to verify enable plugins
5. (For Windows scans) In the **Authentication** tab within the **Windows** section, enable:
   - **Start the remote registry service during the scan**
   - **Enable administrative shares during the scan**
6. Click **Submit** to save the scan policy

Create a compliance scan policy

NOTE
This step may be skipped if there is a pre-existing scan policy to be used.

1. Navigate to **Scan -> Policies** and click on the **+Add** button
2. Select the **Policy Compliance Auditing scan** type
3. In the **Setup** tab, enter a **Name** for the scan
4. In the **Compliance** tab, ad relevant SCAP file(s) based on operating system:
   1) Click on **+Add Audit File**
   2) Open the drop-down options and choose the desired SCAP content
   3) Click on the check-mark to save and apply the audit file

5. (For Windows scans) In the **Authentication** tab within the **Windows** section, enable:
   - **Start the remote registry service during the scan**
   - **Enable administrative shares during the scan**
6. Click **Submit** to save the scan policy

Create an credentialed scan

NOTE
This step may be skipped if there is a pre-existing active scan to be used.

1. Navigate to **Scan -> Credentials** and click on the **+Add** button
2. Choose the authentication method for the credentials:

   Windows Password Method

   1) Select **Windows**
   2) Select **Password** as the authentication method
   3) Set a **Name** for the credentials
   4) Enter the password credentials:
      - **Username**
      - **Password**
      - **Domain** *(For domain joined hosts)*

   ***Nix SSH Method**

   1) Select **SSH**
   2) Select **Password** as the authentication method
   3) Set a **Name** for the credentials
   4) Enter the password credentials:
      - **Username**
      - **Password**
3. Click **Submit** to save the scan credentials

Create an active scan

NOTE
This step may be skipped if there is a pre-existing active scan to be used.

1. Navigate to **Scan -> Active Scans** and click on **Add an Active Scan**
2. In the **General** section, enter the following:
   - **Name:** (A name for the overall scan)
   - **Policy:** (Your desired **Scan Policy**)
   - **Schedule: On Demand**
3. In the **Settings** section, accept all defaults
4. In the **Targets** section, set the **Target Type** to **IP/DNS Name** and enter the scan targets by IP addresses, ranges, CIDR subnets, or hostnames
5. In the **Credentials** section:
   1) Click **Add Credential**
   2) Select the desired credential type
   3) Select the desired scan credentials
   4) Click the check-mark to save
6. Click **Submit** to save the active scan

Launch the active scan

1. Navigate to **Scan -> Active Scans** and click on the “play button” next to the desired scan
2. Navigate to **Scan -> Scan Results** to monitor scan progress and view results

Create an report

> **NOTE**
> This step may be skipped if there is a pre-existing active scan to be used.

1. Navigate to **Options** and click on **Send to Report**
2. Name to the report (Description is optional)
3. In the **Schedule** section under **Frequency** select **Now,** click **Submit**
4. Navigate to **Reporting -> Report Results**
5. Report will show along with Status