DC3
Cyber Training Academy

OPENVAS QUICK TIPS

WHAT IS IT?

OpenVAS is a framework consisting of several services and tools offering a vulnerability scanning and vulnerability-management solution

WHAT CAN IT DO?

Scan networks for vulnerabilities and display a report ranking vulnerabilities by level of concern and criticality

ACCESSING THE WEB INTERFACE

1. Open your browser
2. Enter *https://localhost:9392*
3. Enter your credentials
4. Click the **Login** button

Note: If you receive an error stating the page is unable to be displayed, your server is not started. You will need to open a terminal and type: `openvas-start`

CONFIGURING A SCAN

1. At the **Greenbone Security Assistant Main Dashboard**, left click on the **Scans** tab > **Tasks** function
2. At the **Tasks Summary** page, mouse over the purple wizard icon above the left side of the charts > select **Task Wizard** to start a new scan
3. Enter a host or IP address
4. Click the **Start Scan** button

For more info, visit: https://docs.greenbone.net/ GSM-Manual/gos-4/en/i_want_to.html

ADDING TARGETS

1. Mouse over the **Configuration** tab > left click the **Targets** function from the drop-down menu
2. At the **Targets Management** page, left click on the **New Target** icon
3. In the **New Target** window:
   - **a.** Enter the desired name of the target in the **Name** field
   - **b.** Input any desired description or comment about the target in the **Comment** field
   - **c.** Setup your target in the **Hosts** section (either manually or from a file)
   - **d.** Exclude specific hosts from the target as needed in the **Exclude Hosts** field
   - **e.** Select an existing port list from the **Port List** drop-down menu
   - **f.** Specify how Nessus checks if a target is reachable using the **Alive Test** drop-down menu
   - **g.** Set up credentials is the **Credentials for authenticated checks section** by selecting the ⭐ icon next to each type of credential: SSH, SMB, ESXi, SNMP
   - **h.** Click the **Create** button

The new target will now appear in the **Target Management** page.

ADDING CREDENTIALS

1. Mouse over the **Configuration** tab > left click the **Credentials** function from the drop-down menu

2. Click the ★ icon in the upper left corner
3. In the **New Credential** window:
    a. Type the desired name for the credentials in the **Name** field
    b. Input any desired description or comment about the credentials in the **Comment** field
    c. Select the credential type from the **Type** drop-down menu
    d. Indicate "yes" or "no" for the **Allow insecure use** field
    e. Indicate "yes" or "no" for the **Auto-generate** field; if "yes" the tool will create a random password
    f. Enter the login name used to authenticate the target system in the **Username** field
    g. If not auto-generated, enter the password to authenticate the target system in the **Password** field
    h. Click the **Create** button

CONFIGURING NETWORK VULNERABILITY TESTS

If you'd like to test for specific vulnerabilities, you can configure which Network Vulnerability Tests (NVTs) are executed.

To view all scan configurations, mouse over the **Configuration** tab > left click the **Scan Configs** function from the drop-down menu.

To create a new configuration once on the **Scan Configs** page, click the ★ icon in the upper left corner.

To import a scan configuration once on the **Scans Configs** page, click on the ⬆ icon.

REVIEWING SCAN RESULTS

To view all scan results, mouse over the **Scans** tab > left click the **Reports** function from the drop-down menu.

To download scan reports once on the **Reports** page, select the desired report format from the drop-down menu in the upper left corner > click the ⬇ icon.