

Greenbone scan for vulnerabilities

Setting up credentials:

The screenshot shows the 'New Target' dialog box in the Greenbone Security Manager. The target is named 'Victim's laptop' and the host IP is set to '192.168.57.20'. The 'Credentials' tab is open, showing a single credential entry for 'victim's credentials' with a 'Username + Password' type. The 'Save' button is visible at the bottom right of the dialog.

The screenshot shows the 'New Credential' dialog box in the Greenbone Security Manager. A new credential named 'victim's credentials' is being created. The 'Type' is set to 'Username + Password'. The 'Username' field contains 'student' and the 'Password' field contains '*****'. The 'Save' button is visible at the bottom right of the dialog.

Creation of the task:

The screenshot shows the Greenbone Security Manager web interface at <https://192.168.57.40/tasks>. The main dashboard displays 'Tasks 0 of 0' and 'No Tasks available'. A 'New Task' dialog box is open in the center, titled 'New Task'. The dialog contains the following fields:

- Name:** Scan with victim's credentials
- Comment:** (empty)
- Scan Targets:** Victim's laptop
- Add results to Assets:** Yes (radio button selected)
- Apply Overrides:** Yes (radio button selected)
- Min QoD:** 70 %
- Alterable Task:** No (radio button selected)
- Auto Delete Reports:** Do not automatically delete reports (radio button selected)
- Scanner:** OpenVAS Default
- Scan Config:** Full and fast
- Network Source Interface:** (empty)
- Order for target hosts:** Sequential

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Resources:

report by greebone: ../resources/greenbone-report-vulnerabilities.pdf