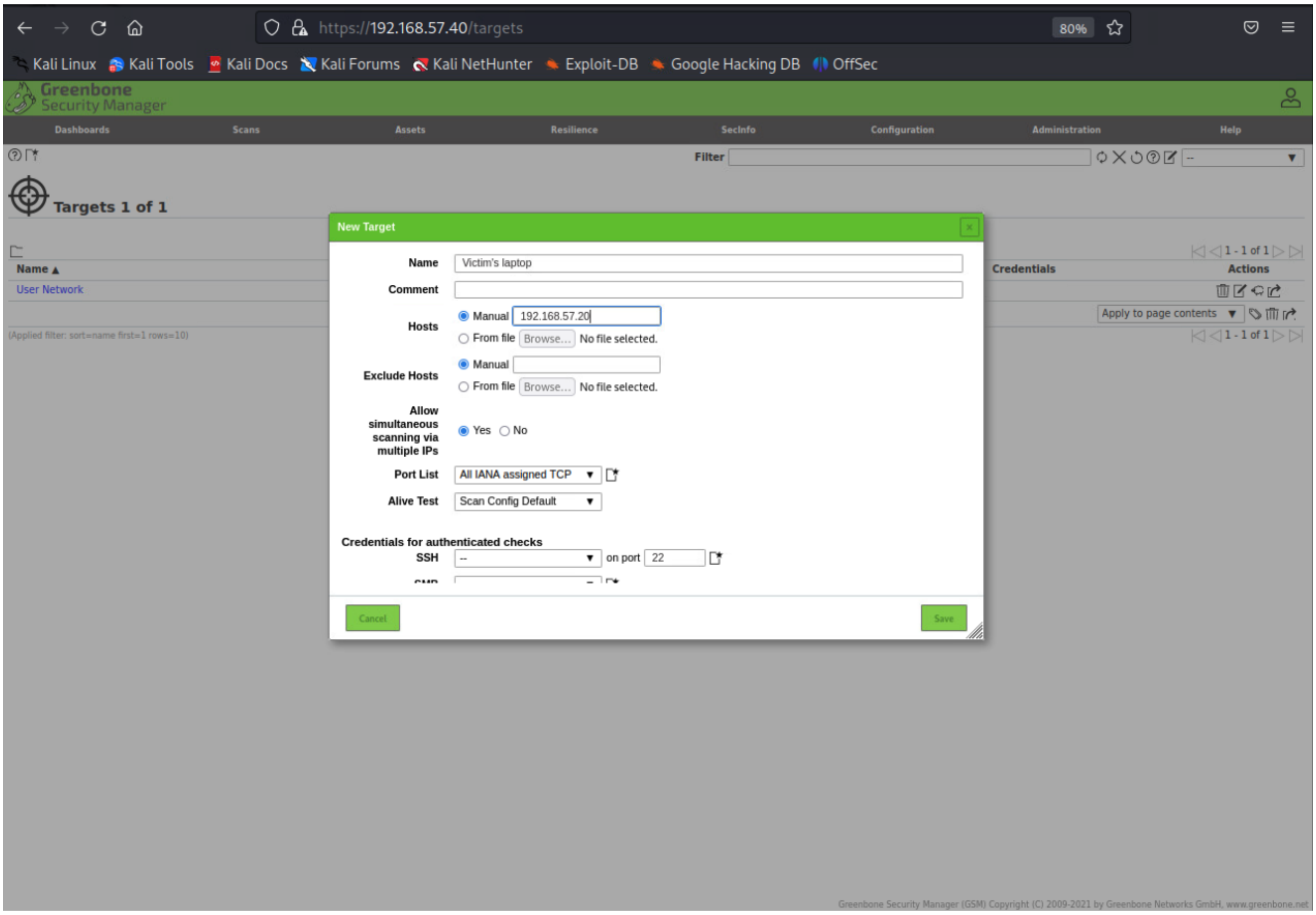
Greenbone scan for vulnerabilities

Setting up credentials:



https://192.168.57.40/targets

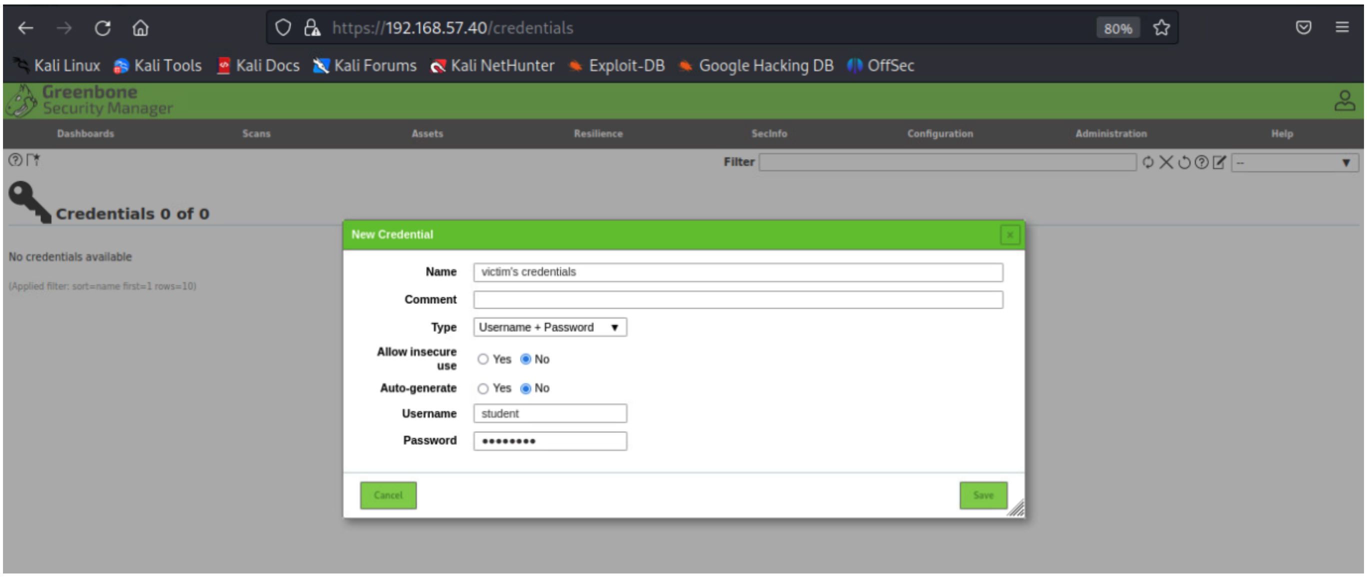
New Target

Name	Victim's laptop
Comment	
Hosts	● Manual 192.168.57.20 ○ From file Browse... No file selected.
Exclude Hosts	● Manual ○ From file Browse... No file selected.
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All IANA assigned TCP
Alive Test	Scan Config Default

Credentials for authenticated checks

SSH	-- on port 22

Cancel Save



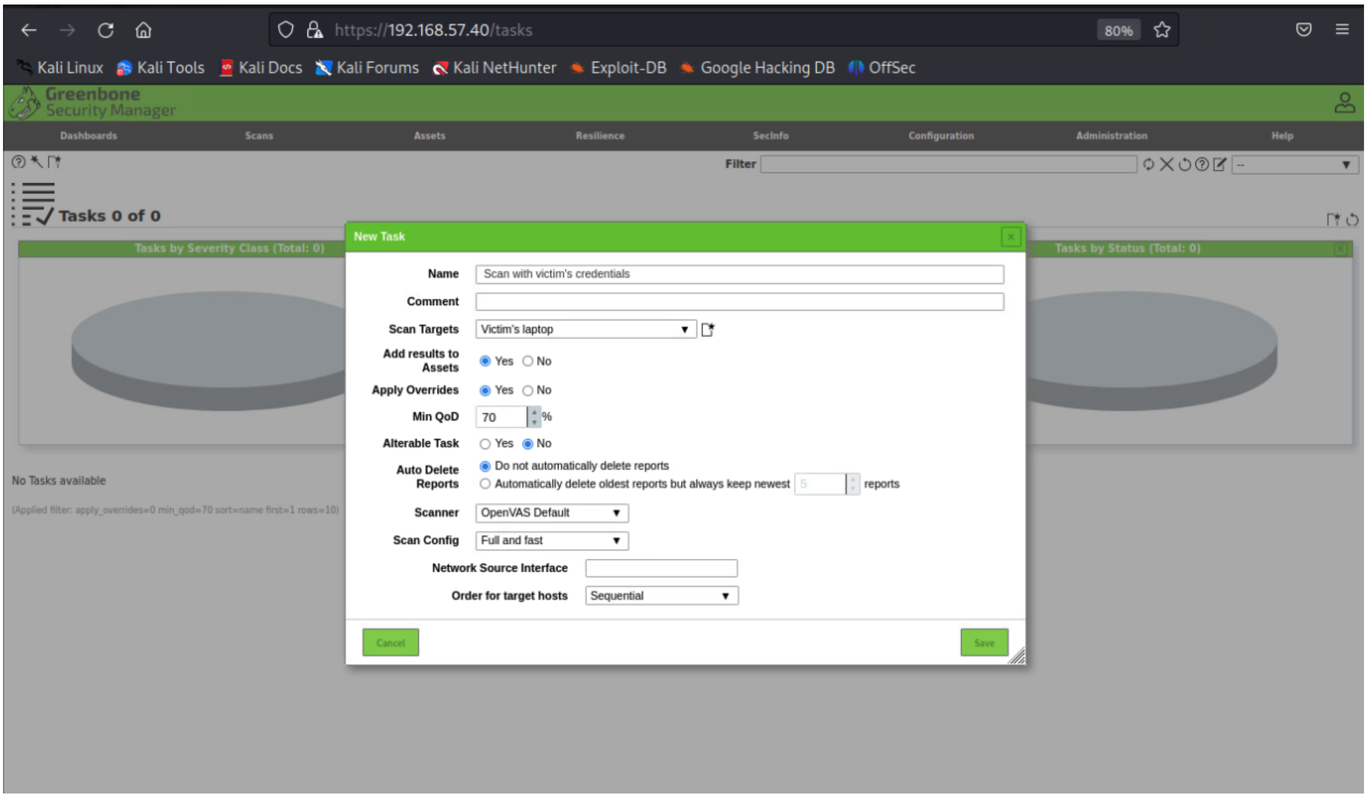
https://192.168.57.40/credentials

New Credential

Name	victim's credentials
Comment	
Type	Username + Password
Allow insecure use	○ Yes ● No
Auto-generate	○ Yes ● No
Username	student
Password	••••••••

Cancel Save

Creation of the task:



New Task

Name: Scan with victim's credentials

Comment:

Scan Targets: Victim's laptop

Add results to Assets: ● Yes ○ No

Apply Overrides: ● Yes ○ No

Min QoD: 70 %

Alterable Task: ○ Yes ● No

Auto Delete Reports: ● Do not automatically delete reports
○ Automatically delete oldest reports but always keep newest 5 reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

Resources:

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