CYBERSECURITY

SCANNING: VULNERABILITY & OPENVAS

OPENVAS

We're using KALI as our attack-OS.

OpenVAS is a scanning tool in which you define machines to scan and run tasks on them. This runs automatically, so it's an ideal tool to regularly check your infrastructure.

Warning: Scanning takes some time 😊

INSTALL OPENVAS:

- Check if this is needed!!!! Recent versions of Kali have GVM included (Greenbone Vulnerability Management) = the new name of OpenVas. The packet to install if needed is "gvm".
- Use the apt-get commands to install ~~"openvas"~~ or "gvm".
- Then run the setup: ~~"openvas-setup"~~. With "gvm" this is "gvm-setup"
    - o Note: make sure you run all commands as root!
    - o Gvm-setup takes a long time!
- Important: Note the admin password, something like:

    45cf0ab5-4bb0-4171-987c-441a8d4dba11

- After the installation you should be able to connect to the website on the localhost and port 9392.
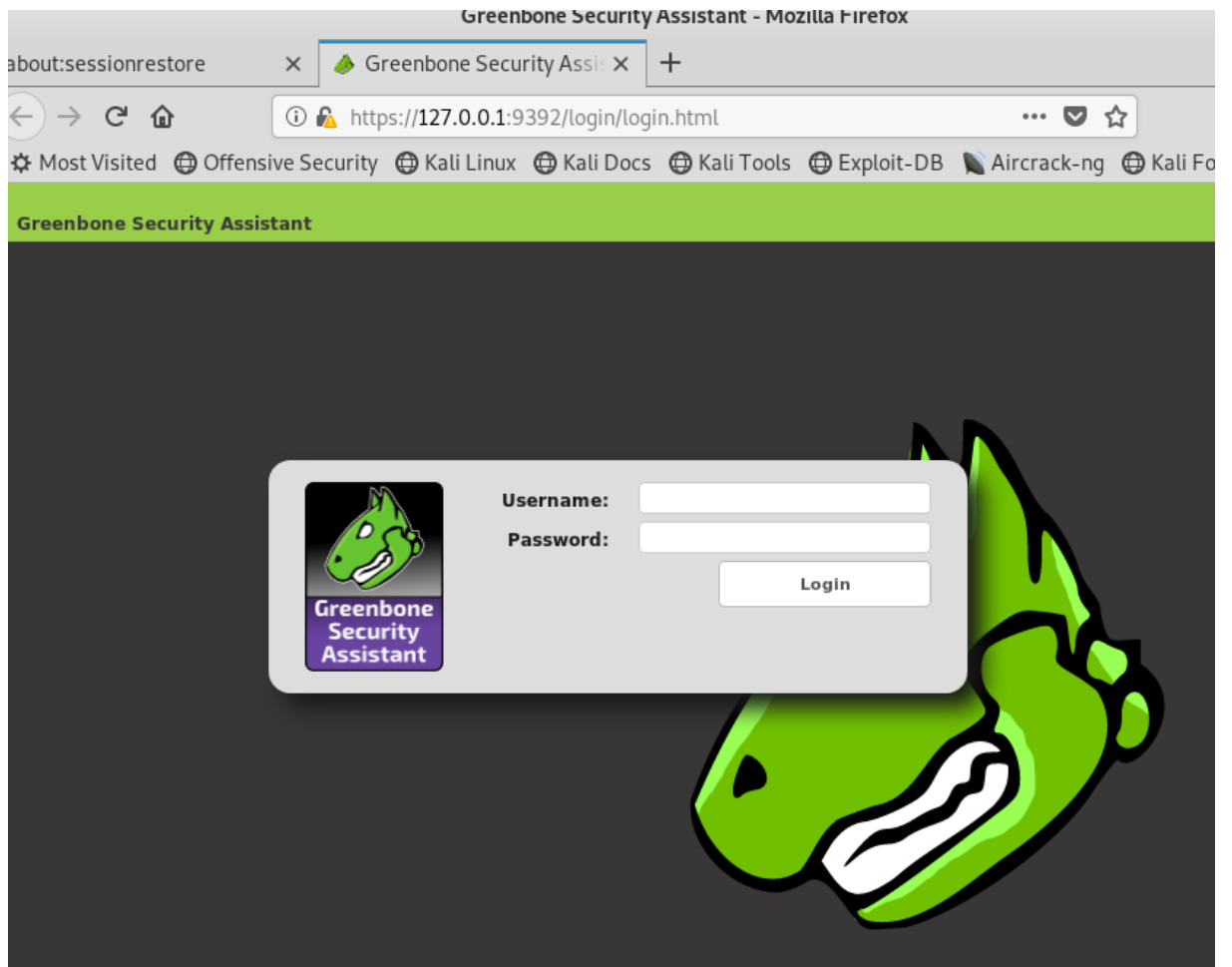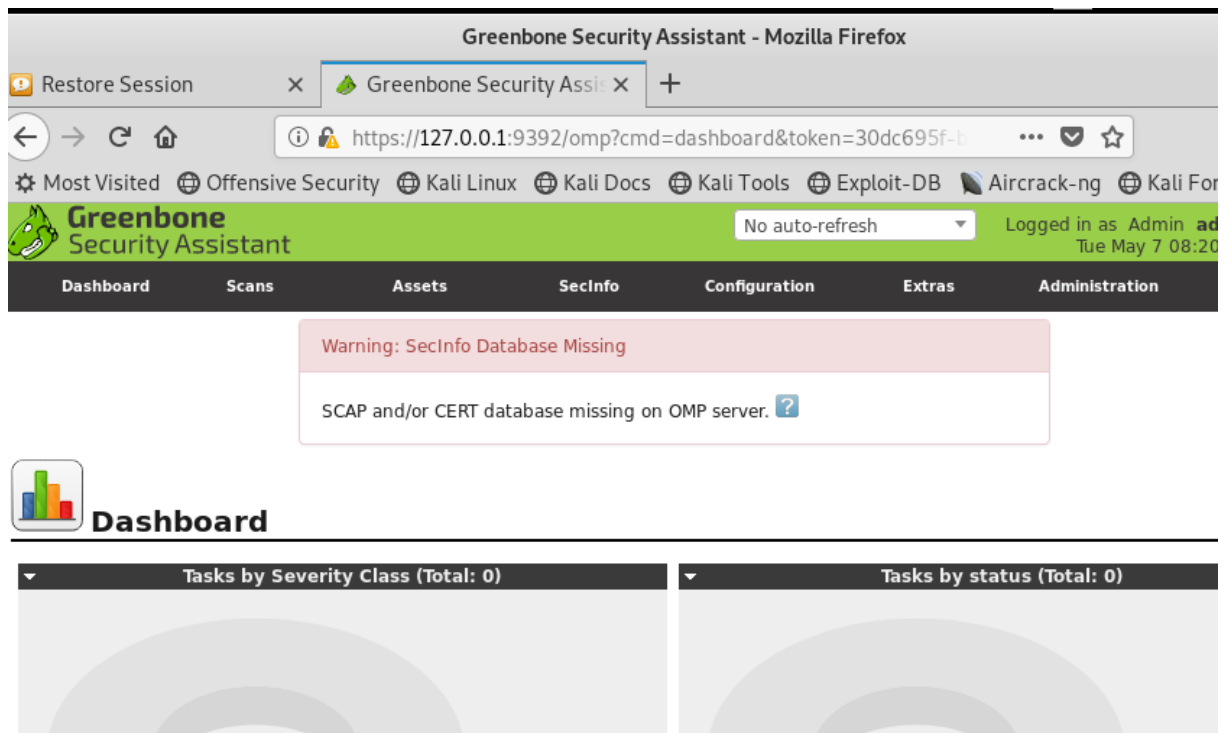
-
- You can check that the gvm tools have been added to your KALI vulnerability checking tools…
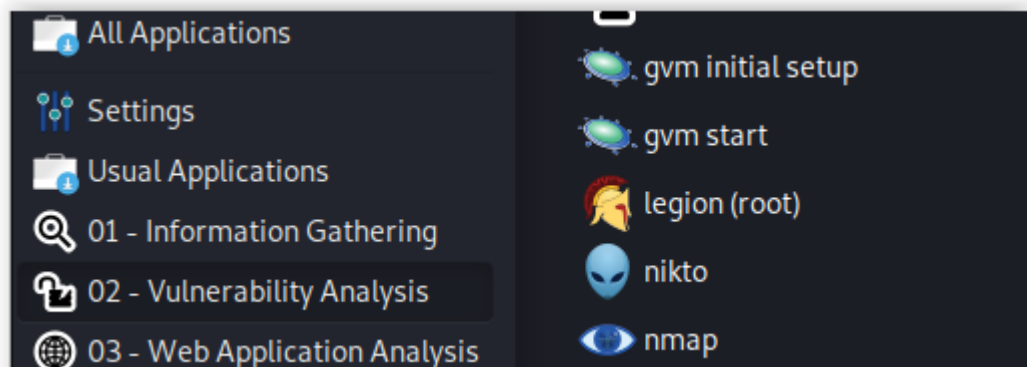
-
- If you need to restart: the startscript needs to be ran…

PERFORM ANALYSIS

- Login to the website with "admin" and the pw you got during the install. You get a dashboard:

-
- Add a new target: Configuration → Targets. Click "Star" icon
    - Put the server you want to scan. (scanme.nmap.org could be a choice)
    - Are you limited to just one server?
- Create a scanning task: Scans → Task. Click the "Star" icon
- Put the target to the target you just created
    - We will leave the "full and fast" type of scan
    - Click Play: Task will get the "Requested" status. We now have to wait for the scan to be executed. You can check progress by clicking the task. Manual refresh is needed.
    - When the task shows "done" the scan is finished. And you can check the report. What do you see?

CHECK REPORT

- In the UI, go to the Reports Section
- You will see the found vulnerabilities classified by severity.
- Analyse these….
    - Were vulnerabilities found?
    - Which severity?
    - What further study is needed?
- Note: The report can be exported in different formats to be used for your clients

OPENVAS EXTRA

Use it to scan the machine of your fellow students, or try at home…

ANSWERS