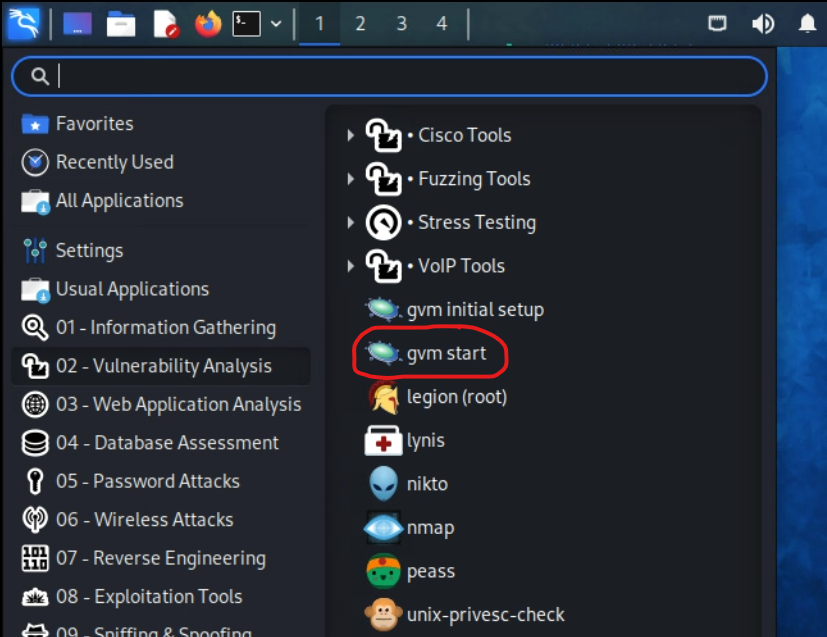
# CYBR430, Penetration Testing and Incident Response Module 5 Lab – Vulnerability Scanning

The lab for this week has two parts. In part one you will scan the HAL clients for vulnerabilities. In part two you will research those vulnerabilities and report on what you find.

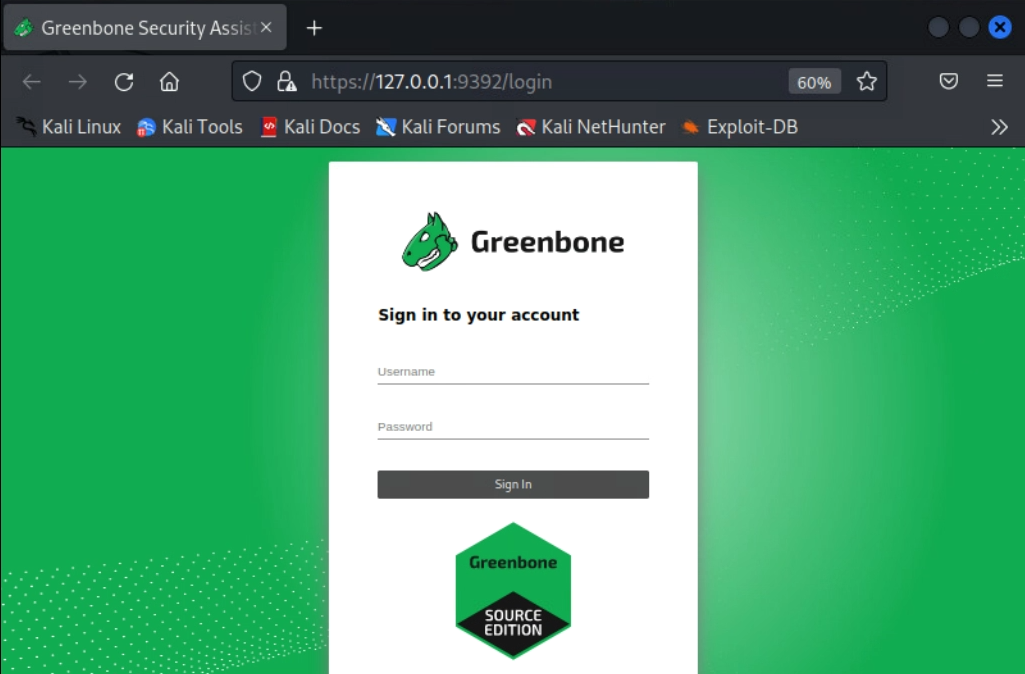
**Part 1: Scanning with GVM (25 points)**

To start gvm use the ‘Applications’ drop down menu. Go to the ‘Vulnerability Analysis’ section and click ‘gvm start.’ Your menu may clip the right side of the menu. Choose the second one as show below.

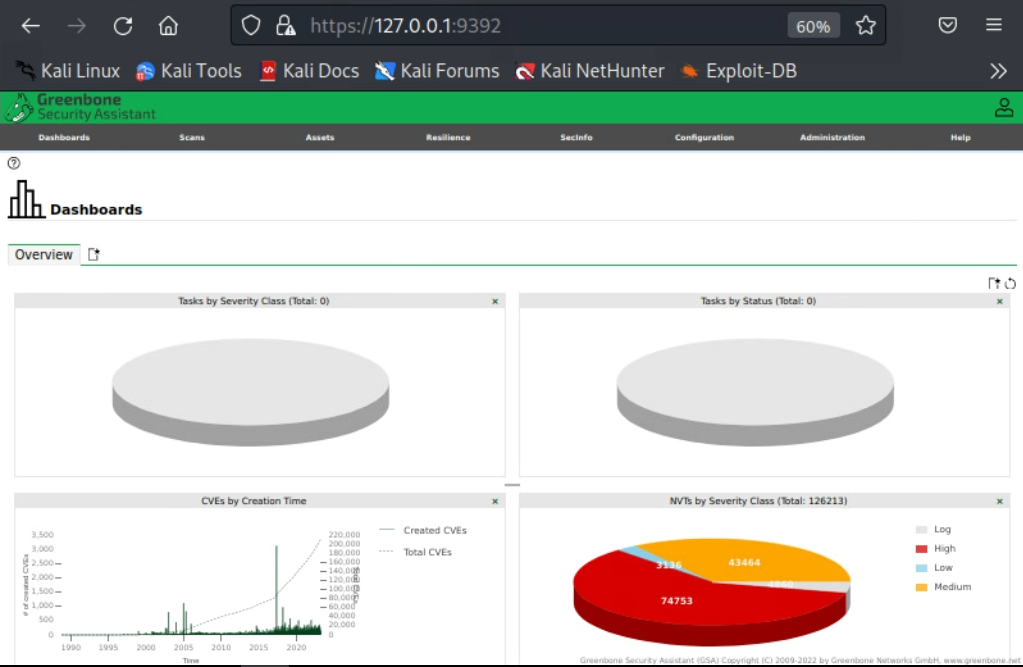


You system will launch a terminal window and state that it is ‘Please wait for GVM services to start.’ When you terminal returns to a command prompt you are ready to continue.

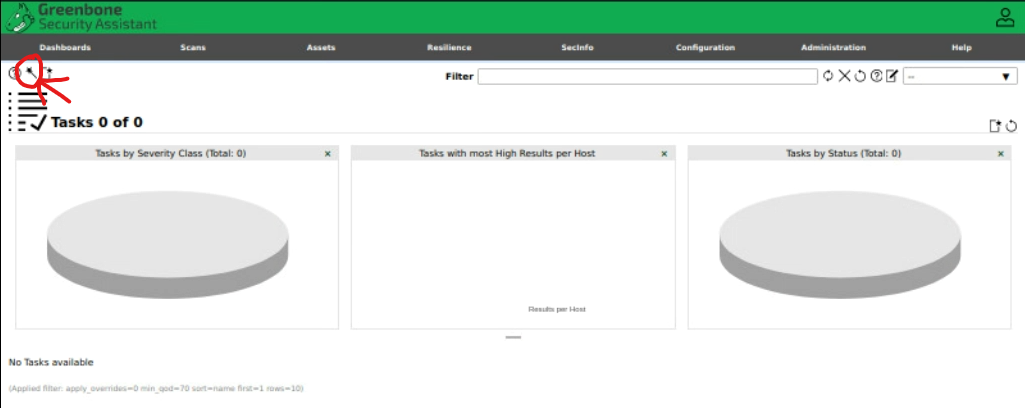
You will interact with the GVM scanner through your Firefox Browser. Start Firefox by clicking on the top tile on the left tile bar, right above the tile you use to start a terminal. Once Firefox launches go to **https://127.0.0.1:9392.** You will be greeted by the Greenbone Security Assistant login screen. Your username will be **admin** and your password is the same as your password for Kali **sighburrfourthree0**



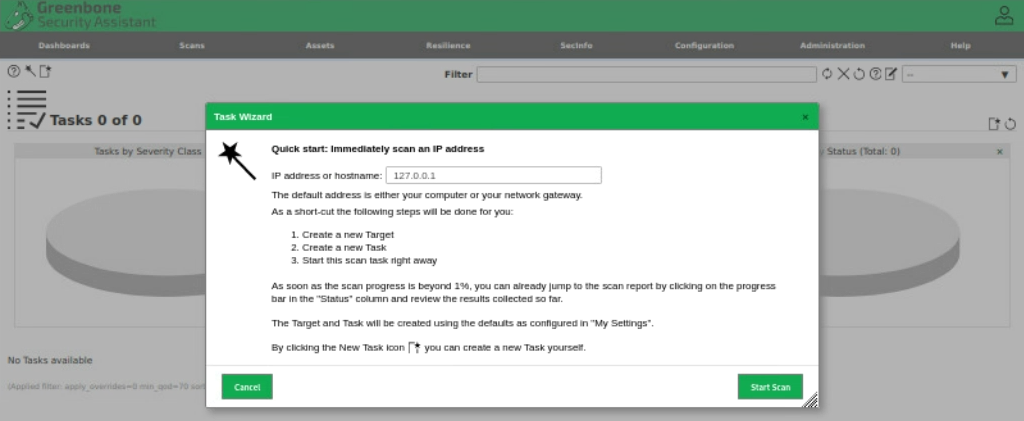
Once you have logged in you will be presented with the dashboard for GVM scans. At present you have no scans so you are viewing the number of CVEs contained in the GVM database.



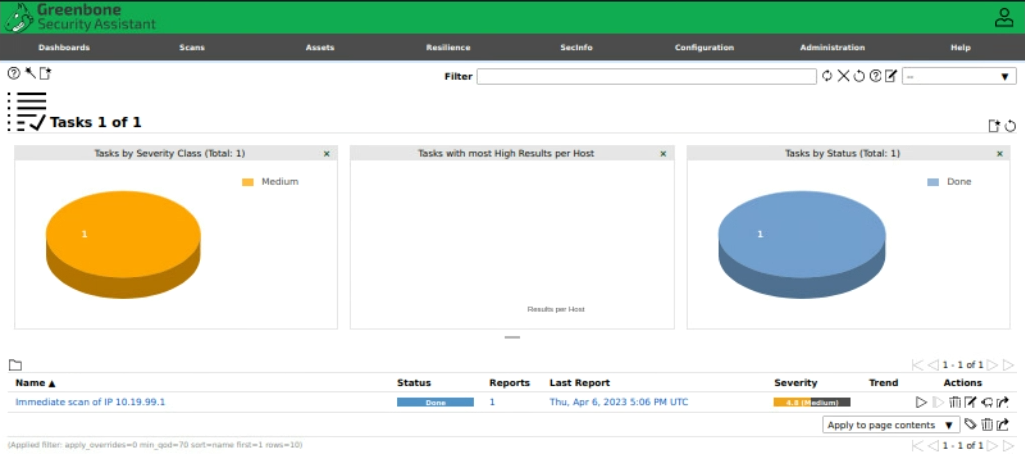
Look through the menus to see some of the capabilities of the Greenbone Security Assistant and the GVM scanner. The website for GVM is linked in your course readings for this week, it’s a great place to find documentation. When you are ready to start scanning use the ‘Scans’ menu and select ‘tasks.’ You will be presented with the scan task dashboard which is empty at present. Click the new scan wizard, indicated in the image below, to configure a scan.



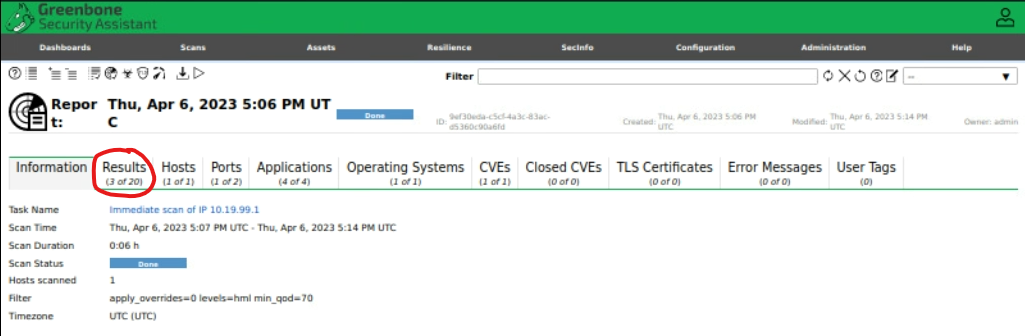
When the menu appears select the ‘task wizard’ menu choice. The second option, ‘Advanced Task Wizard’ allows you to change the type of scan, identify multiple IPs, schedule a scan in the future, and do credentialed scans. Credentialed scans will give more accurate results however as of yet you don’t have credentials for the target systems so you are limited to non-credentialed scans. Feel free to explore the Advanced Task Wizard and try out its features but for this lab all that is required is the basic ‘task wizard’ option.



Replace the highlighted IP address with the IP you wish to scan. As you are scanning the HAL network you have seen the network address is **10.19.99.** and the last tuple (the question marks in the above image) should be replaced with the host you are going to scan. You will want to conduct scans of all the systems on the HAL network. Remember these are the systems you found in your nmap scans that have IPs in the range 10.19.99.1-100. Above that range are student systems. For your first tries I recommend scanning one system at a time. You will be able to access all the reports even if the systems are scanned individually.



Once the scan task is complete you will be returned to the dashboard which at present isn’t very interesting as it is showing just your one scan task. If you had multiple tasks (also, remember a task could be a scan of multiple systems) the dashboard would show how many tasks were complete, scheduled, severity, etc. By clicking on the ‘Last Report’ name of the task (underlined in blue) at the center of the screen you will be taken to the details screen for that particular task.



From the detail screen click the results number as indicated in the image above. This is the number of findings in this particular task. The next screen will be the results dashboard along the top showing several results categorized by severity and CVSS number. Along the bottom will be a table with the vulnerabilities found. The columns provide the following information:

**Vulnerability:** The name of the vulnerability. Clicking on it will provide more information. This is where you will need to look for the information to complete Part 2 of the lab.

**Solution type (puzzle piece):** If a patch, work around, or mitigation exists it MAY be indicated here. There may be other mitigations or work arounds you can find.

**Severity:** How bad is it, scale of 1 – 10. This is the CVSS score.

**QoD:** Quality of Detection. The closer to 100 the less chance of a false positive.

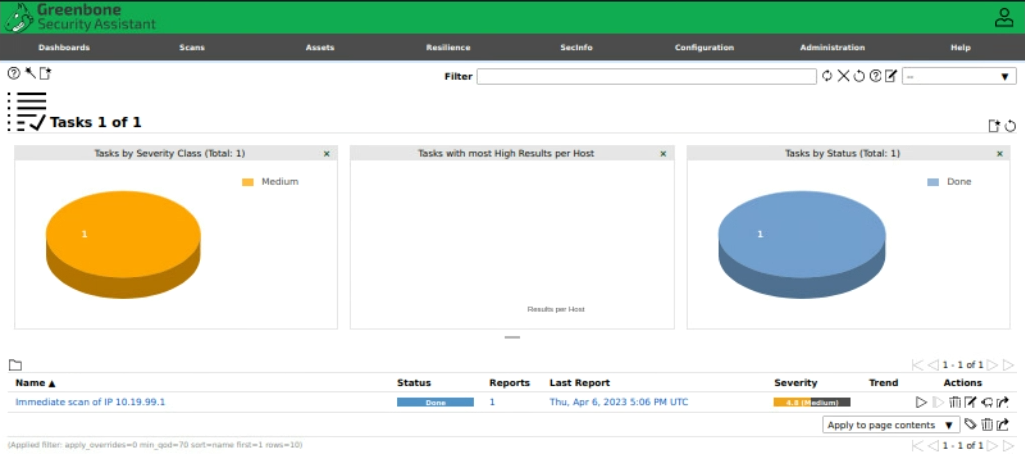
**Host:** Which host was the vulnerability found on. Remember a task can scan multiple hosts. Clicking on the host IP can provide some additional enumeration information.

**Location:** Where was the vulnerability detected on the host.

**Created:** When was the scan done.

**Complete scans on all the HAL assets. Once complete provide a screen shot of your task dashboard showing the completed scans. It’s the screen that looks like the below but should show all your scanning tasks complete.Graphical user interface, website

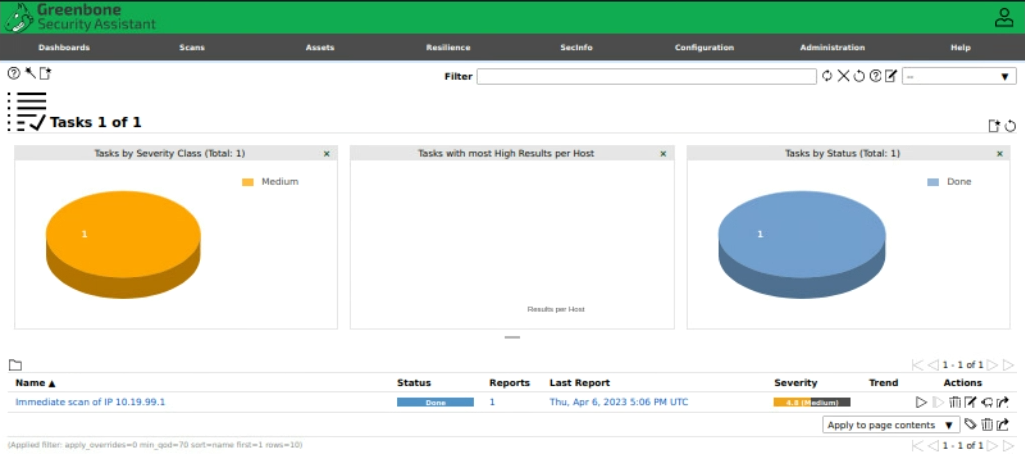
Description automatically generated**



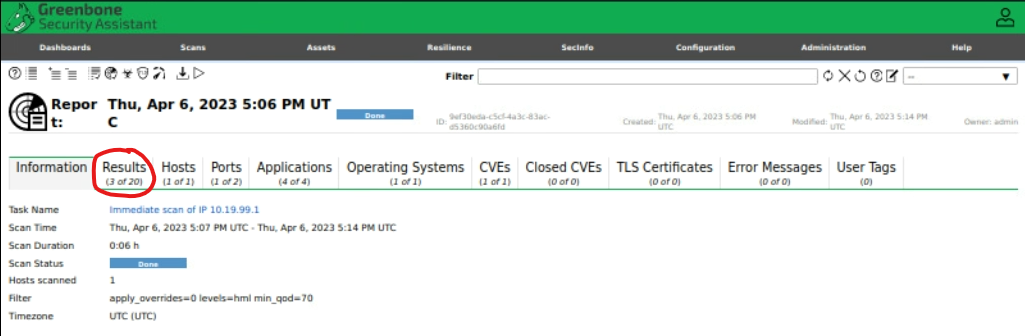
**Part 2: Vulnerability Research (25 points)**

For this part of your lab you will list the vulnerabilities you found across all hosts which are rated as medium or high (ignore the low), and research them through the Open VAS, CVE, and NVD databases.

As shown in part 1, your scan task dashboard will show at the bottom of the screen a list of all scan tasks. Below you will see one task, an immediate scan of 10.19.99.1.



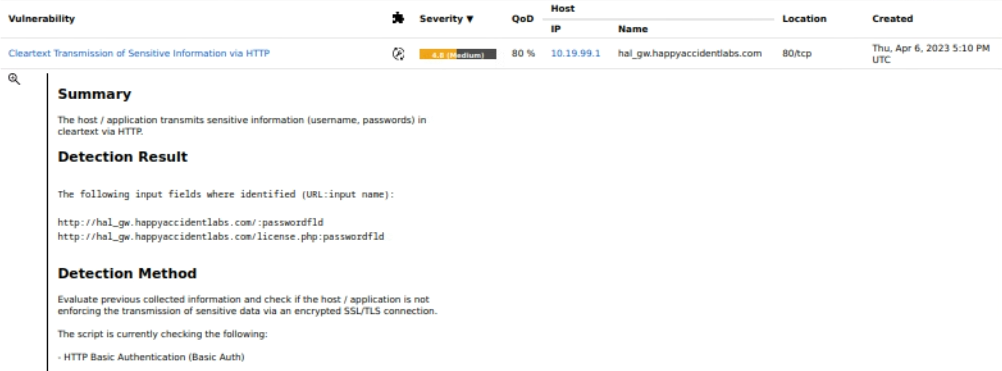
By clicking on the ‘Last Report’ of the scan task you will be brought to the scan summary page.



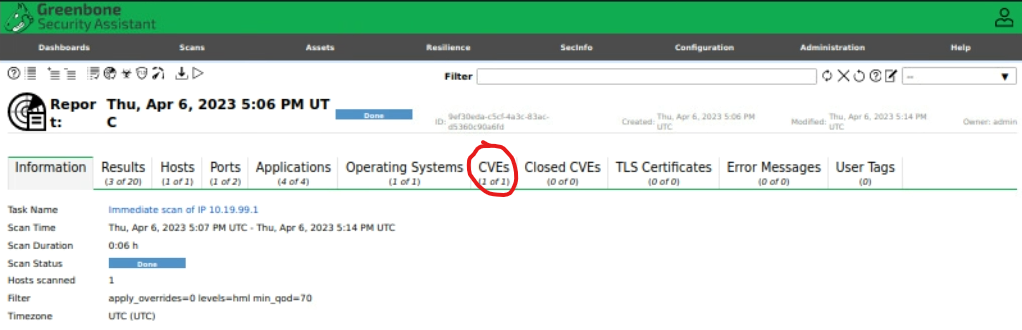
The number of results (findings) on this scan. Click that number to go to the summary page for findings in that scan. At the bottom of the screen is a list of the vulnerabilities found in that scan. Remember, depending on how you did the scan task your results could show multiple hosts.



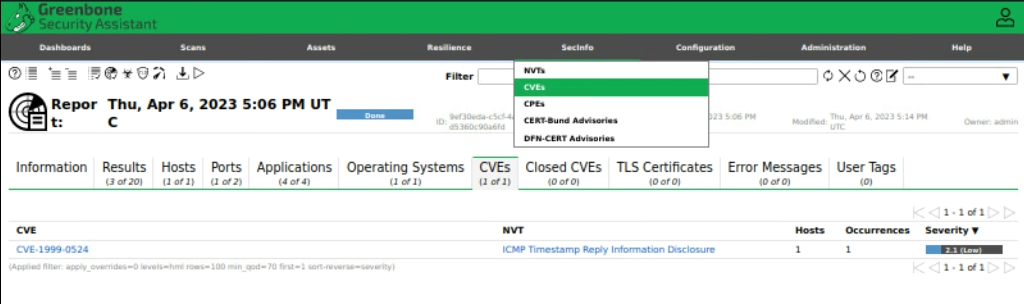
Clicking on a vulnerability in the list will take you to the summary page for that vulnerability. Across the top of the screen will be the title of the vulnerability, the severity (CVSS Score followed by a Low/Medium/High assessment) and other related information.



At the center of the screen under the references section is a link to information on the applicable CVE. The link itself is the CVE number. By clicking the CVE link you will be taken to the CVE summary page for that vulnerability.



Other options for finding information on the vulnerability are under the SecInfo menu at the top of the screen. This is information that GVM downloads from external information sources.

****

You can also go directly to the source and check the CVE (cve.mitre.org) and NVD (nvd.nist.gov) web sites. Searching by the CVE number will provide applicable information. You will need to access these websites from outside the toxic lab as the toxic lab does not have internet access.

**Using the information in GVM and the CVE and NVD databases research the vulnerabilities you have found**. **Complete the table below based on your research.**

| Host(s) IP | CVE or other Identifier | Severity | CVSS Score (if Available) | Vulnerability Name/Description |
| --- | --- | --- | --- | --- |
| 10.19.99.14 | CVE-1999-0519 | High | 7.8 | CVE-1999-0519 is a security vulnerability that affects the "rlogin" service on Unix-based operating systems. The vulnerability allows an attacker to gain unauthorized access to a system that is running the vulnerable service. |
|  |  |  |  |  |
|  |  |  |  |  |

**NOTE: The first line in the table is an example, information is fictitious. Delete it before submission**. Add lines to table as needed.