**OpenVAS:-**

**introduction:-**

**History;-** Greenbone Vulnerability Manager began under the name of OpenVAS, and before that the name GNessUs, as a [fork](https://en.wikipedia.org/wiki/Fork_(software_development)) of the previously [open source](https://en.wikipedia.org/wiki/Open-source_software) [Nessus](https://en.wikipedia.org/wiki/Nessus_(software)) scanning tool, after its developers [Tenable Network Security](https://en.wikipedia.org/wiki/Tenable,_Inc.) changed it to a proprietary ([closed source](https://en.wikipedia.org/wiki/Closed_source)) license in October 2005. OpenVAS was originally proposed by [pentesters](https://en.wikipedia.org/wiki/Penetration_test) at SecuritySpace, discussed with [pentesters](https://en.wikipedia.org/wiki/Penetration_test) at Portcullis Computer Securityand then announcedby Tim Brown on [Slashdot](https://en.wikipedia.org/wiki/Slashdot).

OpenVAS is the scanner component of Greenbone Vulnerability Manager, a software framework of several services and tools offering vulnerability scanning and vulnerability management. All Greenbone Vulnerability Manager products are free software, and most components are licensed under the GNU General Public License.

[**Developer(s)**](https://www.google.com/search?bih=657&biw=1366&hl=en&q=openvas+developers&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQ6BMoAHoECHMQAg)**:**Greenbone Networks GmbH

[**License**](https://www.google.com/search?bih=657&biw=1366&hl=en&q=openvas+license&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQ6BMoAHoECHQQAg)**:**[GPL](https://www.google.com/search?bih=657&biw=1366&hl=en&q=GPL&stick=H4sIAAAAAAAAAONgVuLQz9U3MDZPzl3Eyuwe4AMAS5QyrxIAAAA&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQmxMoAXoECHQQAw)

[**Stable release**](https://www.google.com/search?bih=657&biw=1366&hl=en&q=openvas+stable+release&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQ6BMoAHoECFsQAg)**:**21.4.4 / 22 February 2022; 3 months ago

[**Written in**](https://www.google.com/search?bih=657&biw=1366&hl=en&q=openvas+written+in&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQ6BMoAHoECFwQAg)**:**[C](https://www.google.com/search?bih=657&biw=1366&hl=en&q=C&stick=H4sIAAAAAAAAAONgVuLQz9U3MCwxS1rEyugMAAqDqO4QAAAA&sa=X&ved=2ahUKEwi-wvTLycL4AhV0ZWwGHREzC5QQmxMoAXoECFwQAw)

**Technical related information:*-***

**Technical** details of the scan configuration. A number of high performance servers are hosting **OpenVAS**/GVM 21.4. The NVT's or vulnerability database is updated A number of high performance servers are hosting **OpenVAS/GVM 21.4**. The NVT's or vulnerability database is updated multiple times a week or as required, using the **open source signature feed** (community feed). For Enterprise Software Vulnerability testing and **internal network scanning** we recommend looking at the [Greenbone Security Manager range of appliances](https://www.greenbone.net/en/product-comparison/). Combine an Internal appliance with our external facing suite of tools for full coverage of across all your network attack surface.OpenVAS / GVM is configured to run using configurations based off the "Full and Fast Scan" profile. Hosts are found to be alive after testing for an ICMP response or if this fails a test against common TCP ports. If no open ports are found and ICMP is blocked the target will be seen as not responding and a full scan will not be performed. Vulnerability Testing from behind a **firewall or intrusion prevention device** is generally unreliable - timeouts, slow scanning (rate limiting) and differences in the results can sometime observed. We balance the need for testing as many targets as possible with the performance requirements of Internet based scanning.

* **Pros;-**
* OpenVAS is a free open-source vulnerability assessment tool that is maintained by Greenbone Networks.
* Common vulnerabilities and exposure (CVE) coverage of around 26,000.
* Popular and useful among SME's.
* Built to be an all-in-one scanner.
* The scan engine of OpenVAS is updated on a regular basis.

**Cons:=**

* Covers fewer CVEs as compared to Nessus.
* Less operating system supportability.
* Does not offer policy management.

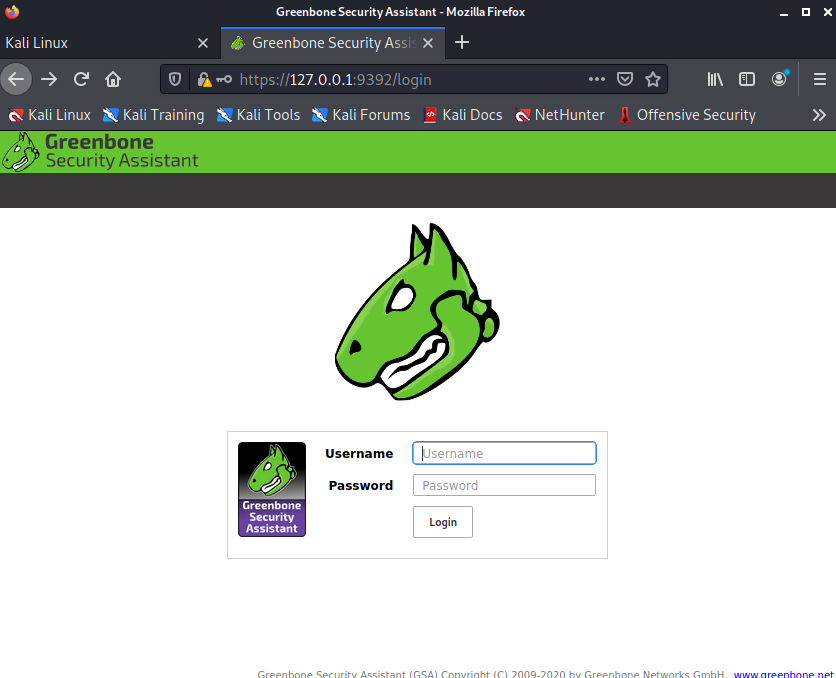
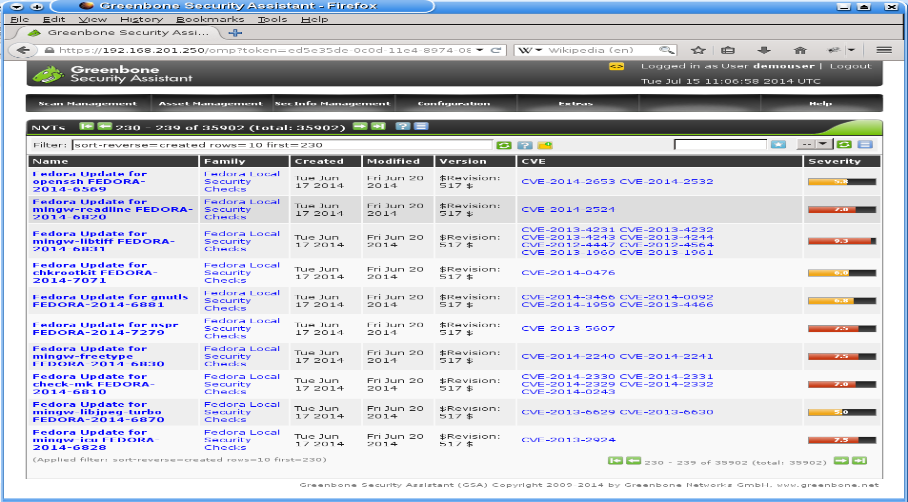
**Application;-**

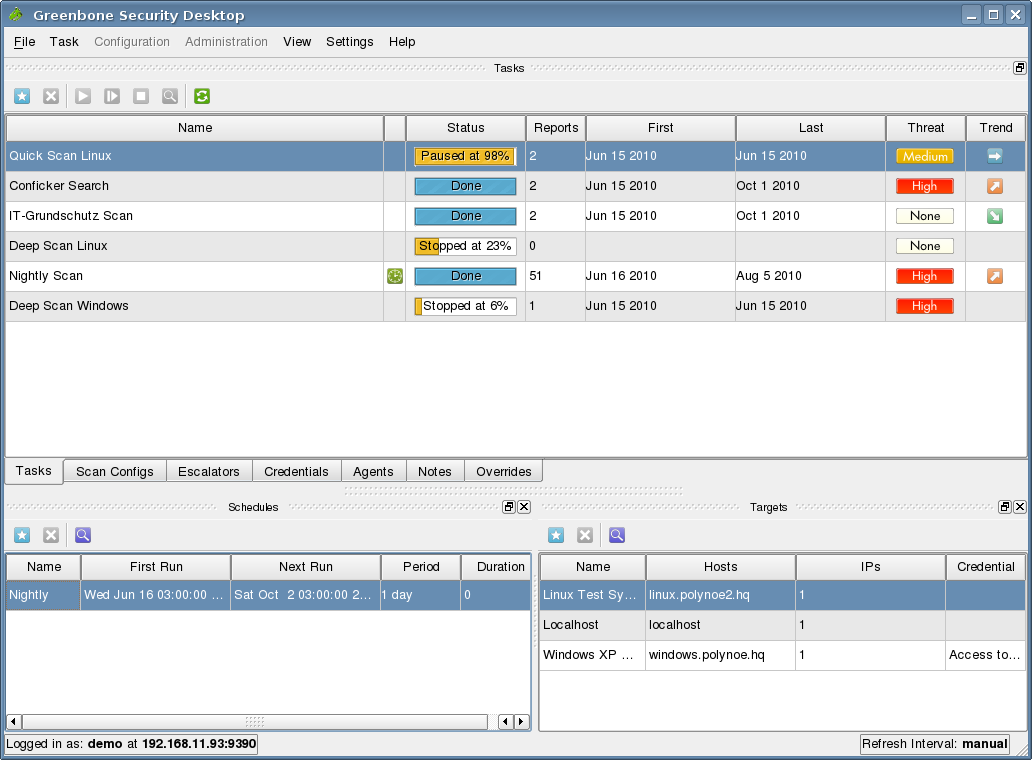
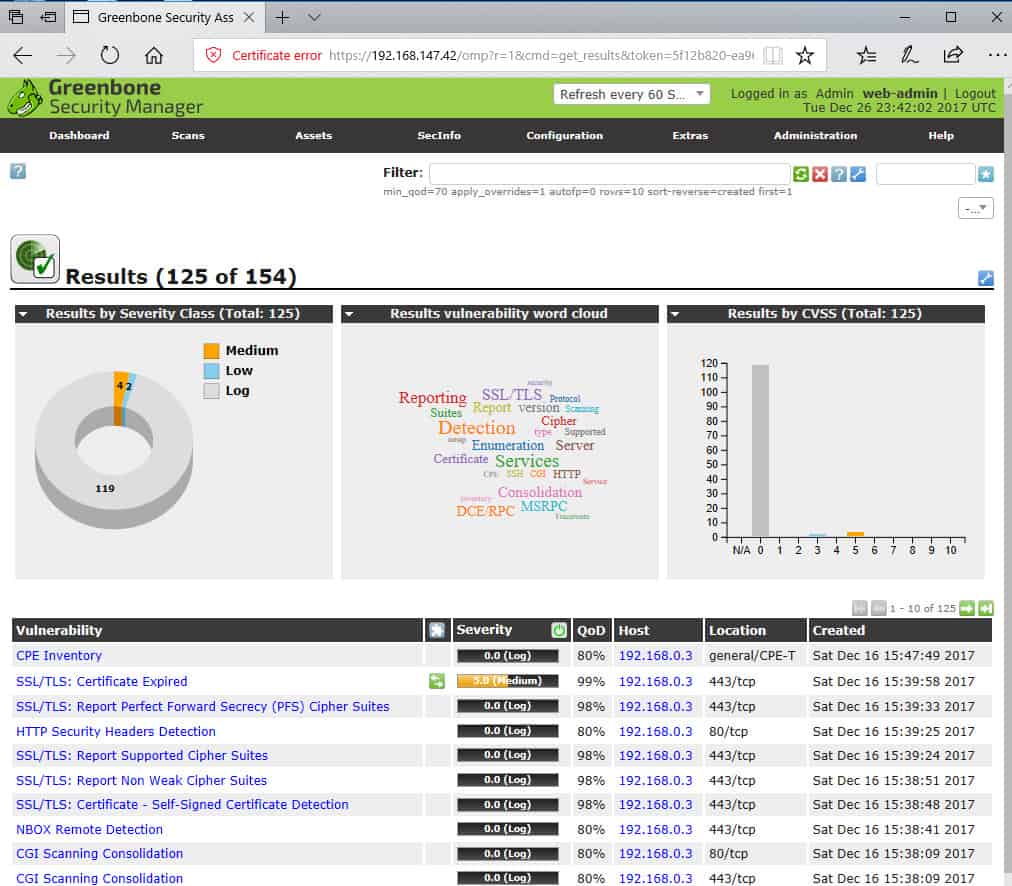
* Application Security Services.
* Data Security Services.
* Email Security Services.
* Endpoint Security Services.
* Incident Response Services.
* IoT Security Services.
* IT Compliance Services.
* Network Security Services.

**Features;-**

* Find security vulnerabilities in any Internet facing system.
* Detailed reporting for risk assessment and re-mediation.
* Vulnerability Alerts on detected change in scheduled report.
* Custom scan options; Network/Server, Web, WordPress and Joomla Scans.

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

 Login page **Open Source Vulnerability Scanner and manager**



ogin page **Open Source Vulnerability Scanner and manager**

