
Open Vulnerability Assessment System (OpenVAS)

The OpenVAS is a wrapper for a collection of security tools and services that, when combined, produces a powerful vulnerability management platform. It has been developed on the basis of a client-server architecture, where the client requests a specific set of network vulnerability tests against its target from the server. Its modular and robust design allows us to run the security tests in parallel; it is available for a number of operating systems (Linux/Win32). Let us take a look at the core components and functions of OpenVAS:

- **OpenVAS scanner**: This effectively manages the execution of **Network Vulnerability Tests** (**NVT**). The new test plugins can be updated on a daily basis via NVT Feeds (http://www.openvas.org/nvt-feeds.html).
- **OpenVAS Client**: This is a traditional form of desktop and CLI-based tools. Its main function is to control the scan execution via **OpenVAS Transfer Protocol** (**OTP**), which acts as a front-line communication protocol for OpenVAS scanner.
- **OpenVAS Manager**: This provides us with a central service to scan the vulnerability. A manager is solely responsible for storing the configuration and scan results centrally. Additionally, it offers us an XML-based **OpenVAS Management Protocol** (**OMP**) to perform various functions; for instance, scheduled scans, report generation, scan results filtering, and aggregation activity.
- **Greenbone Security Assistant**: This is a web service that runs on the top of OMP. This OMP-based client offers us a web interface through which the users can configure, manage, and administer the scanning process. A desktop version of this, called **GSA Desktop** , is also available; it provides us with the same functionality. On the other hand, OpenVAS CLI provides us with a command-line interface for OMP-based communication.
- **OpenVAS Administrator**: This is responsible for handling the user administration and feed management.

Tools used by OpenVAS

OpenVAS uses the following set of tools:

Security tool	Description
Amap	An application protocol detection tool
Ike-scan	IPsec VPN scanning, fingerprinting, and testing
Ldapsearch	Extracts information from LDAP dictionaries
Nikto	Web server assessment tool
Nmap	Port scanner
Ovaldi	Open vulnerability and assessment language interpreter
pnscan	Port scanner
Portbunny	Port scanner
Seccubus	Automates the regular OpenVAS scans
SLAD	Security Local Auditing Daemon tools include John-the-Ripper, Chkrootkit, ClamAV, Snort, Logwatch, Tripwire, Lsof, Tiger, TrapWatch, and LM-sensors
Snmpwalk	SNMP data extractor
Strobe	Port scanner

Security tool	Description
w3af	Web application attack and audit framework

In order to set up OpenVAS, following are the necessary steps that have to be followed:

1. Navigate to **Kali Linux** | **Vulnerability Analysis** | **OpenVAS** | **Openvas check setup** and follow the instructions to ensure that your OpenVAS installation is complete. Using the default settings for the certificate and other items is recommended until you understand the tools completely. After following the instructions for each `FIX` step, you will need to re-run the **openvas check setup** option until it states that you have successfully configured the program. You can run this command directly from the command-line window as well. The following screenshot displays this step:

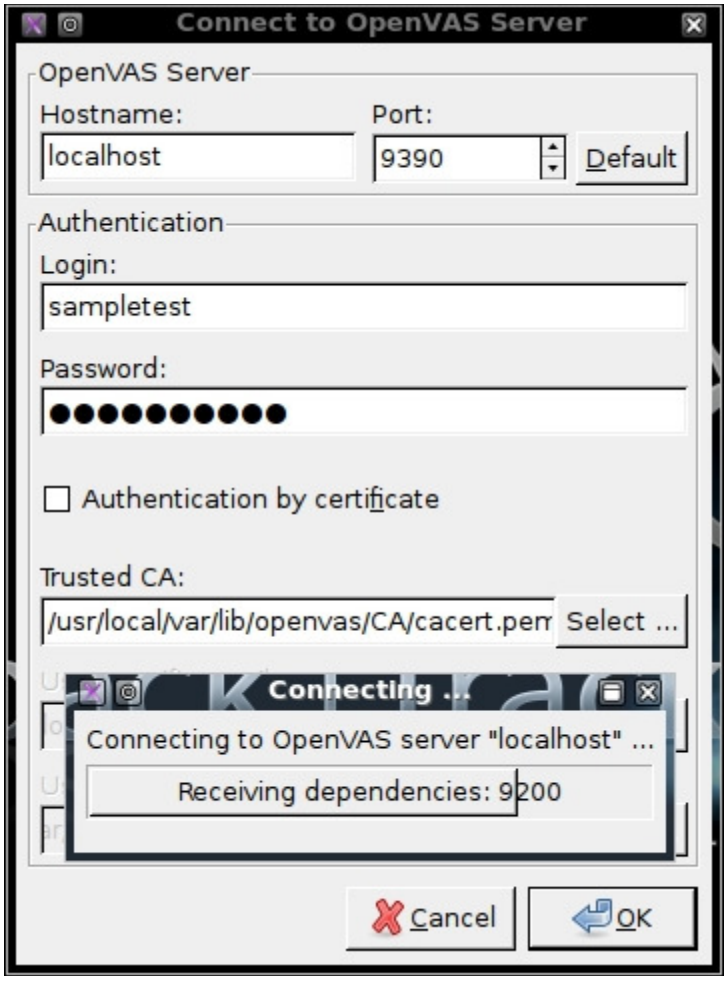
```
openvas-check-setup 2.2.3
  Test completeness and readiness of OpenVAS-6
  (add '--v4', '--v5' or '--v7'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the proble
m.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 3.4.0.
        ERROR: No CA certificate file of OpenVAS Scanner found.
        FIX: Run 'openvas-mkcert'.

 ERROR: Your OpenVAS-6 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the
 problem.

root@kali:~#
```

2. Navigate to **Kali Linux** | **Vulnerability Assessment** | **OpenVAS** | **OpenVas Adduser** in order to create a user account under which the vulnerability scanning will be performed. Press *Enter* when you are asked for the **Authentication (pass/cert)** value. At the end, you will be prompted to create rules for the newly created user. If you don't have any rules to define, simply press *Ctrl* + *D* to exit, or learn to write the rules by firing up a new Konsole (terminal program) window and typing the following command:

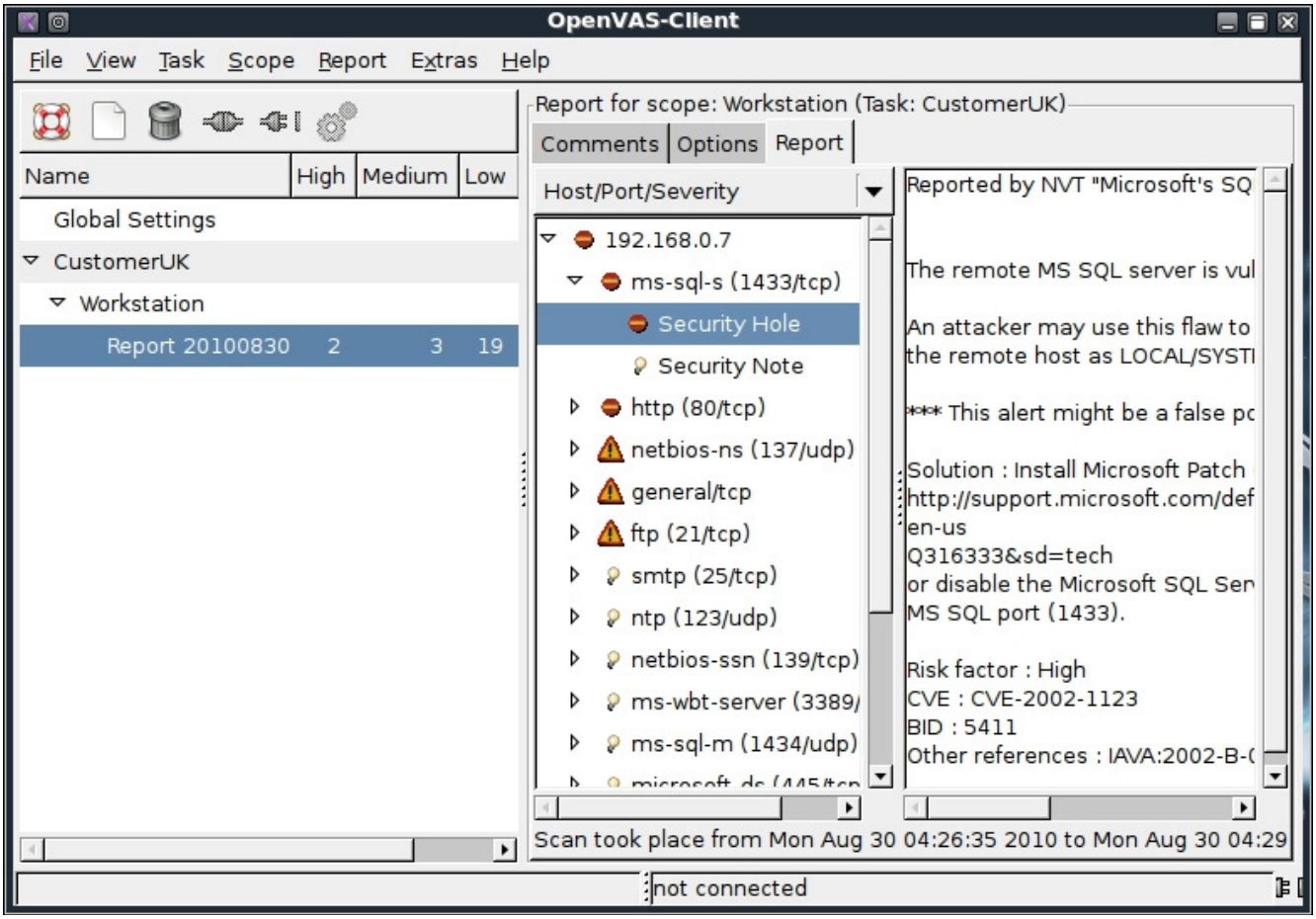
```
# man openvas-adduser
```

3. If you have an Internet connection, and want to update your OpenVAS plugins with the latest NVT feeds, then navigate to **Kali Linux** | **Vulnerability Assessment** | **OpenVAS** | **OpenVas NVT Sync**.
4. Now, start the OpenVAS server service before the client can communicate with it. Navigate to **Kali Linux** | **Vulnerability Assessment** | **OpenVAS** | **OpenVas Server** and wait until the process loading is completed.
5. Finally, we are ready to start our OpenVAS client. Navigate to **Kali Linux** | **Vulnerability Assessment** | **OpenVAS** | **OpenVas Client**. Once the client window appears, navigate to **File** | **Connect** and use the exact account parameters that you defined in step 1 and step 2.

Now your client is successfully connected to OpenVAS server, as shown in the following screenshot:



It is time to define the target parameters (one or multiple hosts), select the appropriate plugins, provide the required credentials, and define any necessary access rules (as mentioned in step 2). Once these global settings have been set, navigate to **File** | **Scan Assistant** and specify the details for all the four major steps (**Task**, **Scope**, **Targets**, and **Execute**) in order to execute the selected tests against your target. You will be prompted to specify the login credentials and the assessment will commence afterwards. This process will take some time to complete the assessment based on your chosen criteria. The following screenshot shows us the report of the assessment that was performed:



You can see that we have successfully finished our assessment and the report is presented under the given task name, `CustomerUK`, in the preceding example. In the top menu, navigate to **Report** | **Export**; there, you can select the appropriate format of your report (**NBE**, **XML**, **HTML**, **LaTeX**, **TXT**, **PDF**). OpenVAS is a powerful vulnerability assessment software that allows you to assess your target against all critical security problems and provide a comprehensive report with the risk measurement, vulnerability detail, solution, and references to online resources.