

Name: Ehsan Rasheed

Reg. No: BCS223075

## OPENVAS Download and Installation:

```
(kali@kali)-[~]
└─$ sudo apt install openvas
[sudo] password for kali:
Note, selecting 'gvm' instead of 'openvas'
Upgrading:
  python3-gpg

Installing:
  gvm

Installing dependencies:
  greenbone-security-assistant  gsad  gvm-tools  libmicrohttpd12t64

Summary:
  Upgrading: 1, Installing: 5, Removing: 0, Not Upgrading: 221
  Download size: 4,095 kB
  Space needed: 14.3 MB / 53.2 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 greenbone-security-assistant all 23.3.0~precompiled-0kali1 [3,230 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmicrohttpd12t64 amd64 1.0.1-2 [155 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 gsad amd64 24.0.0-1 [133 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 gvm all 24.11.1 [11.8 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 gvm-tools all 24.8.0-1 [158 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 python3-gpg amd64 1.24.2-1+b1 [408 kB]
Fetched 4,095 kB in 9s (440 kB/s)
Selecting previously unselected package greenbone-security-assistant.
(Reading database ... 425637 files and directories currently installed.)
Preparing to unpack .../0-greenbone-security-assistant_23.3.0~precompiled-0kali1_all.deb ...
Unpacking greenbone-security-assistant (23.3.0~precompiled-0kali1) ...
Selecting previously unselected package libmicrohttpd12t64:amd64.
Preparing to unpack .../1-libmicrohttpd12t64_1.0.1-2_amd64.deb ...


└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
   Active: active (running) since Sun 2025-03-23 15:13:17 EDT; 15ms ago
   Invocation: 7159be25a9484424a201387444fb3208
   Docs: man:gsad(8)
         https://www.greenbone.net
   Main PID: 149568 (gsad)
   Tasks: 1 (limit: 6497)
   Memory: 1.3M (peak: 2M)
   CPU: 20ms
   CGroup: /system.slice/gsad.service
           └─149568 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392 admin

Mar 23 15:13:17 KALI systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Mar 23 15:13:17 KALI systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvm.service - Greenbone Vulnerability Manager daemon (gvm)
   Loaded: loaded (/usr/lib/systemd/system/gvm.service; disabled; preset: disabled)
   Active: active (running) since Sun 2025-03-23 15:13:12 EDT; 5s ago
   Invocation: 1e244f5999a244aabe84b8d2b989caa0
   Docs: man:gvm(8)
```

## Scanning CUST IP(162.159.132.42)




**Quick start: Immediately scan an IP address**  
IP address or hostname:   
The default address is either your computer or your network gateway.  
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Cancel

Start Scan

Backbone

Search

Configuration

Administration

Help

ubhan-ahmed@KALI: ~

Filter

51#53

Host High Results per Host

2.168.212.251

du.pk: SERVFAIL

Results per Host

Tasks by Status (Total: 1)

Done

1

Status	Reports	Last Report	Severity	Trend	Actions
Done	1	Sun, Mar 23, 2025 5:05 PM UTC	2.4 (Low)		<div>Apply to page contents</div>

## Scanner

Name **OpenVAS Default**  
Type **OpenVAS Scanner**  
Scan Config **Full and fast**  
Order for target hosts  
Maximum concurrently executed NVTs per host **4**  
Maximum concurrently scanned hosts **20**

## Assets

Add to Assets **Yes**  
Apply Overrides **Yes**  
Min QoD **70 %**

## Scan

Duration of last Scan **an hour**  
Auto delete Reports **Do not automatically delete reports**

## Results:

Report: Sun, Mar 23, 2025 5:05 PM UTC Done ID: 607d156f2796-48a9-8c72-3e5941410508 Created: Sun, Mar 23, 2025 5:05 PM UTC Modified: Sun, Mar 23, 2025 6:29 PM UTC Owner: admin

Information Results (1 of 57) Hosts (1 of 1) Ports (0 of 5) Applications (2 of 2) Operating Systems (1 of 1) CVEs (0 of 0) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (2 of 2) User Tags (0)

Vulnerability **Severity** **QoD** **Host IP** **Name** **Location** **Created**

TCP Timestamps Information Disclosure **2.6 (Low)** 80 % 162.159.135.42 kinsta.cloud general/tcp Sun, Mar 23, 2025 5:46 PM UTC

(Applied filter: apply\_overrides=0 levels=html rows=100 min\_qod=70 first=1 sort=reverse=severity)

```
subhan-ahmed@KALI: ~  
File Actions Edit View Help  
Address: 192.168.212.251#53  
Non-authoritative answer:  
Name: www.vu.edu.pk  
Address: 111.60.183.36  
;; Got SERVFAIL reply from 192.168.212.251  
** server can't find www.vu.edu.pk: SERVFAIL
```

Results 55 of 57

Results by Severity Class (Total: 55)

Results by CVSS (Total: 55)

**Severity** **QoD** **Host IP** **Name** **Location** **Created**

TCP Timestamps Information Disclosure **2.6 (Low)** 80 % 162.159.135.42 kinsta.cloud general/tcp Sun, Mar 23, 2025 5:46 PM UTC

Services **0.0 (Log)** 80 % 162.159.135.42 kinsta.cloud 80/tcp Sun, Mar 23, 2025 5:23 PM UTC

SSL/TLS: Version Detection **0.0 (Log)** 80 % 162.159.135.42 kinsta.cloud 443/tcp Sun, Mar 23, 2025 5:23 PM UTC

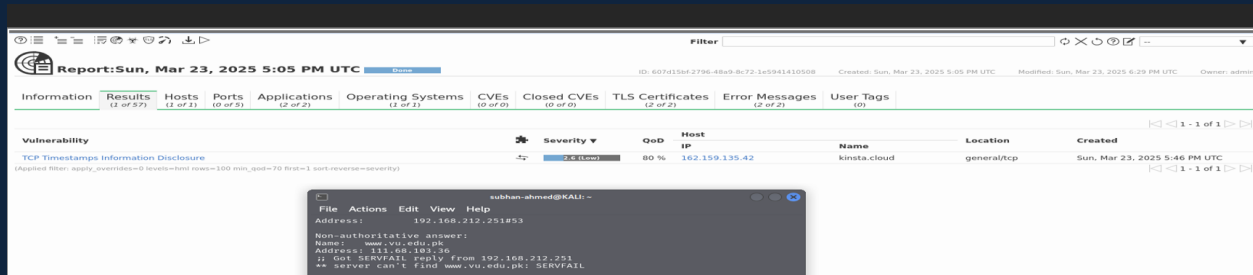
Services **0.0 (Log)** 80 % 162.159.135.42 kinsta.cloud 2087/tcp Sun, Mar 23, 2025 5:23 PM UTC

Services **0.0 (Log)** 80 % 162.159.135.42 kinsta.cloud 443/tcp Sun, Mar 23, 2025 5:23 PM UTC

Services **0.0 (Log)** 80 % 162.159.135.42 kinsta.cloud 8080/tcp Sun, Mar 23, 2025 5:23 PM UTC

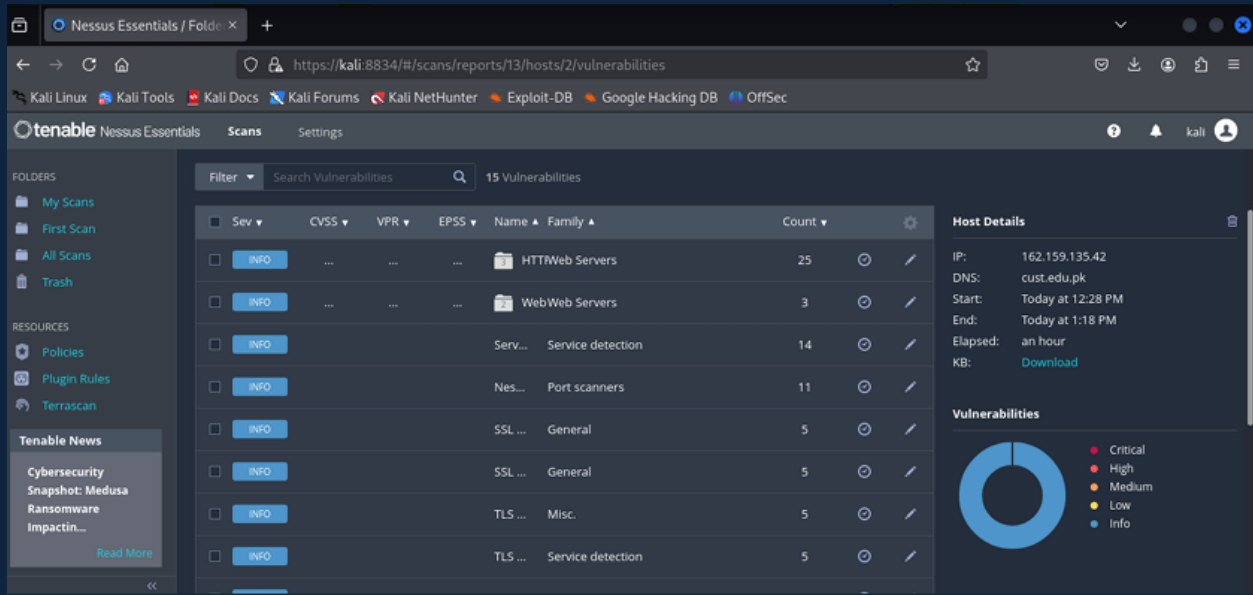
Copyright © 2006-2025 OpenVAS Project

## Comparison of both, OPENVAS and Nessus:



The screenshot shows the OpenVAS web interface. At the top, it displays the report title "Report: Sun, Mar 23, 2025 5:05 PM UTC" and a "Done" button. Below this is a navigation bar with tabs for Information, Results (12 of 27), Hosts (11 of 21), Ports (0 of 2), Applications (12 of 2), Operating Systems (11 of 1), CVEs (0 of 2), Closed CVEs (0 of 2), TLS Certificates (2 of 2), Error Messages (2 of 2), and User Tags (0). The main content area shows a table of vulnerabilities. The table has columns for Severity, QoD, Host IP, Name, Location, and Created. The first row shows a vulnerability with a severity of "Info", a QoD of "80 %", a host IP of "162.159.135.42", a name of "kinsta.cloud", and a location of "general/tcp". Below the table, there is a terminal window showing a command prompt with the following output:

```
subhan-ahmed@KALI: ~  
File Actions Edit View Help  
Address: 192.168.212.251#53  
Non-authoritative answer:  
Name: www.vu.edu.pk  
Address: 111.68.103.56  
! Got SERVFAIL reply from 192.168.212.251  
* server can't find www.vu.edu.pk: SERVFAIL
```



The screenshot shows the Nessus Essentials web interface. The browser address bar displays "https://kali-8834/#/scans/reports/13/hosts/2/vulnerabilities". The interface includes a sidebar with navigation options: FOLDERS (My Scans, First Scan, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Cybersecurity Snapshot: Medusa Ransomware Impactin...). The main content area shows a table of vulnerabilities. The table has columns for Sev, CVSS, VPR, EPSS, Name, Family, and Count. The first row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "HTTPWeb Servers", a family of "HTTPWeb Servers", and a count of "25". The second row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "WebWeb Servers", a family of "WebWeb Servers", and a count of "3". The third row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "Serv...", a family of "Service detection", and a count of "14". The fourth row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "Nes...", a family of "Port scanners", and a count of "11". The fifth row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "SSL ...", a family of "General", and a count of "5". The sixth row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "SSL ...", a family of "General", and a count of "5". The seventh row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "TLS ...", a family of "Misc.", and a count of "5". The eighth row shows a vulnerability with a severity of "Info", a CVSS of "...", a VPR of "...", an EPSS of "...", a name of "TLS ...", a family of "Service detection", and a count of "5". On the right side of the interface, there is a "Host Details" section showing the IP address "162.159.135.42", the DNS name "cust.edu.pk", the start time "Today at 12:28 PM", the end time "Today at 1:18 PM", the elapsed time "an hour", and a "Download" button. Below the host details, there is a "Vulnerabilities" section showing a donut chart with a legend for severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue).