

# OpenVAS - GVM Exercise

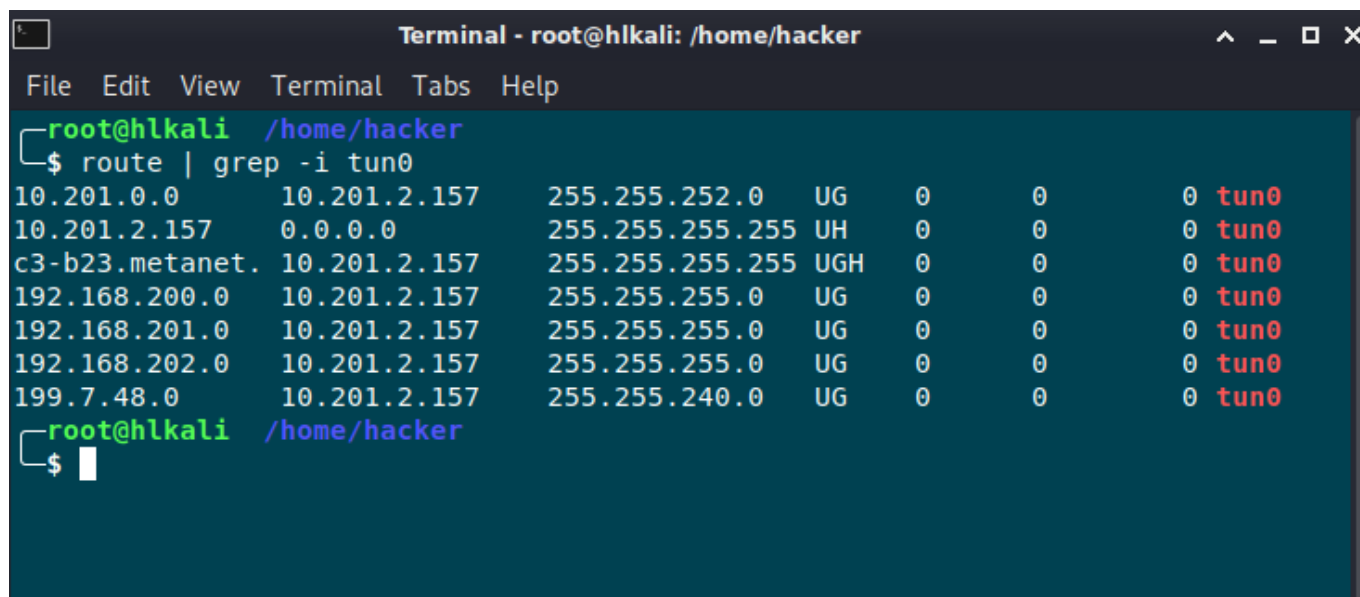
---

## 1. Introduction and task description

In 2005, the developers of the vulnerability scanner Nessus decided to discontinue the work under Open Source licenses and switch to a proprietary business model. The open source tool was called OpenVAS. In late 2008, the company Greenbone Networks GmbH, based in Osnabrück, Germany was founded to push forward OpenVAS. The year 2017 marked the beginning of a new era: Greenbone became visible as the driving force behind OpenVAS, reducing the brand confusion. This included several activities, the most essential one the renaming of the "OpenVAS framework" to "Greenbone Vulnerability Management" (GVM), of which the OpenVAS Scanner is one of many modules.

After setting up the Hackinglab VPN Connection, please perform a vulnerability scan with OpenVAS against the following networks:

```
192.168.200.0/24
192.168.202.0/24
```



```
Terminal - root@hkali: /home/hacker
File Edit View Terminal Tabs Help
root@hkali /home/hacker
└─$ route | grep -i tun0
10.201.0.0      10.201.2.157    255.255.252.0  UG    0        0        0 tun0
10.201.2.157   0.0.0.0         255.255.255.255 UH    0        0        0 tun0
c3-b23.metanet. 10.201.2.157    255.255.255.255 UGH   0        0        0 tun0
192.168.200.0  10.201.2.157    255.255.255.0  UG    0        0        0 tun0
192.168.201.0  10.201.2.157    255.255.255.0  UG    0        0        0 tun0
192.168.202.0  10.201.2.157    255.255.255.0  UG    0        0        0 tun0
199.7.48.0     10.201.2.157    255.255.240.0  UG    0        0        0 tun0
root@hkali /home/hacker
└─$
```

May you want to start with some single ip addresses (otherwise it take a very long time)

Please submit a ZIP file containing your own pdf report and html scan results

1. Describe this task
2. Describe your methodology
3. Describe your lesson learned
4. Attach the vulnerability report from your scan (html)

## 2. Answer and solution

1. See description above
2. This is the active part of reconnaissance. Using OpenVAS, an opensource vulnerability scanner for gathering useful information about the targets networks and any possible exploits and vulnerabilities.
3. This exercise gave me really headache, because the setup was very time consuming and there was a problem with updating the signatures. Finally I got it to work, but decided to scan a single host instead of the whole ip range. I got the signature update (`greenbone-nvt-sync`) only to work, by starting the docker setup without the `nvt-sync` container.

```
Terminal - root@hlkali: /home/hacker
File Edit View Terminal Tabs Help
root@hlkali /home/hacker
$ docker-compose -f docker-compose.yml -f cert-sync.yml -f scap-sync.yml up
```

`docker -execute -it c5fd91baa386 bash`

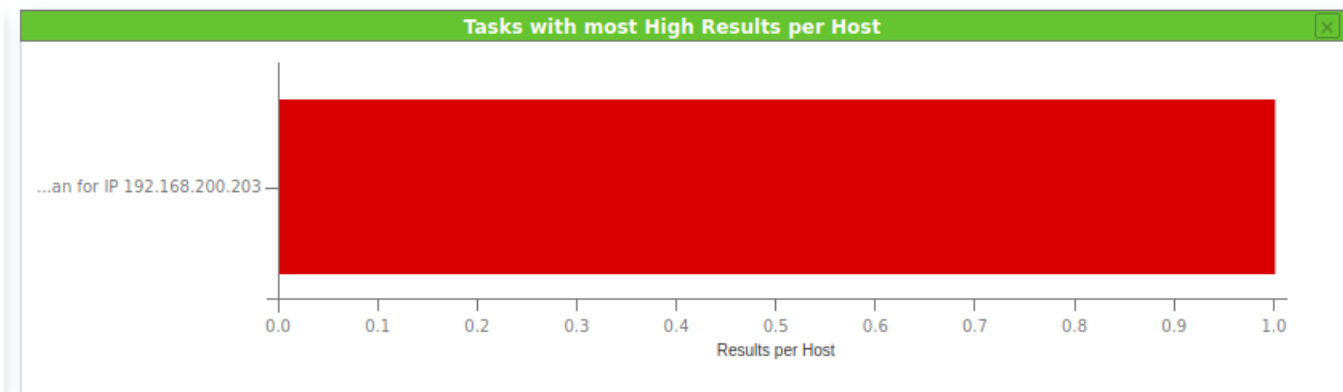
```
Application Options:
-V, --version                Display version information
-c, --config-file=<filename> Configuration file
-s, --cfg-specs              Print configuration settings
-y, --sysconfdir             Print system configuration directory (set at compile time)
-u, --update-vt-info        Updates VT info into redis store from VT files
--scan-start=<string>      ID of scan to start. ID and related data must be stored into redis before.
--scan-stop=<string>      ID of scan to stop

root@c5fd91baa386:/# greenbone-nvt-sync
```

After setting up the update command `greenbone-nvt-sync` and `openvas-u` the VTS list got loaded!

```
gvm-containers_scap-sync_1 exited with code 0
gsad gmp:MESSAGE:2020-11-02 22h16.05 utc:1: Authentication success for 'admin' from 172.20.0.1
lib nvticache:MESSAGE:2020-11-02 22h16.35 utc:324: Updated NVT cache from version 0 to 202011021456
2020-11-02 22:16:35,805 OSPD - openvas: INFO: (osspd openvas.daemon) Loading vts in memory.
event task:MESSAGE:2020-11-02 22h16.38 UTC:673: Status of task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has changed to Requested
event task:MESSAGE:2020-11-02 22h16.38 UTC:673: Task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has been requested to start by admin
md manage:WARNING:2020-11-02 22h16.48 UTC:675: OSP start scan 79577fbf-1032-4e74-b8a2-d61e033fe244: VTS list is empty
event task:MESSAGE:2020-11-02 22h16.48 UTC:675: Status of task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has changed to Done
2020-11-02 22:17:14,263 OSPD - openvas: INFO: (osspd openvas.daemon) Finish loading up vts.
md manage: INFO:2020-11-02 22h17.25 utc:738: OSP service has newer VT status (version 202011021456) than in database (version 0, 0 VTs). Starting up
date ...
event task:MESSAGE:2020-11-02 22h20.23 UTC:860: Status of task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has changed to Requested
event task:MESSAGE:2020-11-02 22h20.23 UTC:860: Task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has been requested to start by admin
md manage:WARNING:2020-11-02 22h20.33 UTC:862: OSP start_scan b440d3ca-3737-49b2-a7e7-48db278ec952: VTS list is empty
event task:MESSAGE:2020-11-02 22h20.33 UTC:862: Status of task Scan 192.168.200.0/24 (b7bc81e4-b5e9-4a8c-bf81-81c7fa21a68b) has changed to Done
md manage: INFO:2020-11-02 22h25.12 utc:738: Updating VTS in database ... 63135 new VTs, 0 changed VTs
md manage: INFO:2020-11-02 22h25.22 utc:738: Updating VTS in database ... done (63135 VTs).
```

4. See my attached result



Status	Reports	Last Report
Stopped at 54 %	2	Mon, Nov 2, 2020 6:55 PM UTC
Done	1	Tue, Nov 3, 2020 9:57 PM UTC

There was no option to export a html report. A pdf export gave me a 0byte document. Maybe there's a dependency missing?

<https://gist.github.com/rain1024/98dd5e2c6c8c28f9ea9d>