PURPOSE

Vulnerability scanner for guest systems hosted in UniFR
6CPU/16GB/32GBSSD
Default IP: 192.168.1.42/24 (kali.fortier-family.com)
OS: Kali Linux
Open ports: SSH/HTTPS

INSTALL

Iso 2021.2 from https://www.kali.org/get-kali/#kali-bare-metal
Full US install (XFCE + large collection)

One account at install (sudoers): warnaud 🤣

POST-INSTALL

network

```
nmtui
```

to put back the DNS which were not set...

```
apt update
apt upgrade
systemctl enable ssh
```

SSH

root key-only

```
vi /etc/ssh/sshd_config
```

```
PermitRootLogin prohibit-password
```

```
systemctl restart ssh
```

from some IP

IPv6/rsyslog/ntp

IPv6

```
sysctl -w net.ipv6.conf.all.disable_ipv6=1 && sysctl -w
net.ipv6.conf.default.disable_ipv6=1 && sysctl -w
net.ipv6.conf.lo.disable_ipv6=1
```

```
vi /etc/ssh/sshd_config
```

```
AddressFamily inet
```

```
systemctl restart ssh
```

Rsyslog

```
vi /etc/rsyslog.conf
```

```
# 2020-01-15 renvoi vers (r)syslog.unifr.ch
#            la nouvelle machine est  vx-ditsyslog.unifr.ch 134.21.201.50
#            l'alias syslog.unifr.ch existe
#            utiliser l'adresse IP permet de s'affranchir d'une panne de DNS
#            le choix est laissé au sysadmin.
*.*     @@IPsyslog-server
```

NTP

```
timedatectl set-timezone Europe/Zurich
apt install ntp ntpdate
vi /etc/ntp.conf
```

```
#pool 0.debian.pool.ntp.org iburst
#pool 1.debian.pool.ntp.org iburst
#pool 2.debian.pool.ntp.org iburst
#pool 3.debian.pool.ntp.org iburst
server ntp.fortier-family.com iburst
```

```
systemctl enable --now ntp
ntpq -p
```

OpenVAS

Check

Verify haveged is running

```
ps aux | grep -i have
```

Install/setup

```
apt install gvm
gvm-setup
```

First update takes ages...

 Don't forget to get the password for the admin account 

Update

```
gvm-feed-update
```

MANUAL WAY

- Update NVT Feed

```
sudo runuser -u _gvm -- greenbone-nvt-sync
```

- Update SCAP Feed

```
sudo runuser -u _gvm -- greenbone-feed-sync --type SCAP
```

- Update CERT Feed

```
sudo runuser -u _gvm -- greenbone-feed-sync --type CERT
```

- Update gvmd DATA Feed

```
sudo runuser -u _gvm -- greenbone-feed-sync --type GVMD_DATA
```

crontab

```
0 12 * * * for optimize in vaccum analyse cleanup-report-formats cleanup-
```

```
result-nvts cleanup-config-prefs cleanup-result-severities update-report-
cache; do /usr/sbin/gvmd --optimize=$optimize; done
0 13 * * * sudo -u _gvm greenbone-scapdata-sync >/var/log/gvm-feed-update-
SCAP.log
0 15 * * * sudo -u _gvm greenbone-feed-sync --type GVMD_DATA 2>/var/log/gvm-
feed-update-GVMD.log
0 17 * * * sudo -u _gvm greenbone-certdata-sync >/var/log/gvm-feed-update-
CERT.log
0 19 * * * sudo -u _gvm greenbone-nvt-sync >/var/log/gvm-feed-update-
sync.log
```

PDF Problem

Since September https://forum.greenbone.net/t/kali-linux-cannot-create-pdf-reports/13014/4 :

```
vi /var/lib/gvm/gvmd/report_formats/a67ec44b-a708-445d-
a6a8-29f76a6a9647/c402cc3e-b531-11e1-9163-406186ea4fc5/latex.xsl
```

```
% \usepackage[utf8x]{inputenc}
```

Service

```
systemctl enable --now gvmd ospd-openvas
systemctl enable greenbone-security-assistant
systemctl status gvmd ospd-openvas greenbone-security-assistant

gvm-check-setup
```


greenbone-security-assistant doesn't need to be up

Reset password

```
su - _gvm -s /bin/sh -c "gvmd --user=admin --new-password mypasswd; history
-c"
history -c
```

Xrdp

```
apt install xrdp
```

```
systemctl enable --now xrdp
```

Fixing "xrdp Authentication is requiredto create a color managed device"

Doesn't work:

```
echo "polkit.addRule(function(action, subject) {
 if ((action.id == "org.freedesktop.color-manager.create-device" ||
 action.id == "org.freedesktop.color-manager.create-profile" ||
 action.id == "org.freedesktop.color-manager.delete-device" ||
 action.id == "org.freedesktop.color-manager.delete-profile" ||
 action.id == "org.freedesktop.color-manager.modify-device" ||
 action.id == "org.freedesktop.color-manager.modify-profile") &&
 subject.isInGroup("{users}")) {
 return polkit.Result.YES;
 }
 });" >  /etc/polkit-1/localauthority.conf.d/02-allow-color.d.conf

echo "[Allow Colord all Users] Identity=unix-user:*
Action=org.freedesktop.color-manager.create-device;org.freedesktop.color-
manager.create-profile;org.freedesktop.color-manager.delete-
device;org.freedesktop.color-manager.delete-profile;org.freedesktop.color-
manager.modify-device;org.freedesktop.color-manager.modify-profile;
ResultAny=no
ResultInactive=no
ResultActive=yes" > /etc/polkit-1/localauthority/50-local.d/45-allow-
colord.pkla
```

```
cp /usr/share/polkit-1/actions/org.freedesktop.color.policy
/usr/share/polkit-1/actions/org.freedesktop.color.policy.org
rm /usr/share/polkit-1/actions/org.freedesktop.color.policy
```

Working solution

```
vi /usr/share/polkit-1/actions/org.freedesktop.color.policy
```

switch all values to yes

```
      <allow_any>yes</allow_any>
      <allow_inactive>yes</allow_inactive>
      <allow_active>yes</allow_active>
```

And then:

```
vi /etc/polkit-1/localauthority.conf.d/02-allow-color.d.conf
```

```
polkit.addRule(function(action, subject) {
 if ((action.id == "org.freedesktop.color-manager.create-device" ||
 action.id == "org.freedesktop.color-manager.create-profile" ||
 action.id == "org.freedesktop.color-manager.delete-device" ||
 action.id == "org.freedesktop.color-manager.delete-profile" ||
 action.id == "org.freedesktop.color-manager.modify-device" ||
 action.id == "org.freedesktop.color-manager.modify-profile") &&
 subject.isInGroup("{users}")) {
 return polkit.Result.YES;
 }
 });
```

Debug

In case of problem...

```
 gvm-check-setup
systemctl status gvmd ospd-openvas greenbone-security-assistant
multitail /var/log/gvm/gsad.log /var/log/gvm/gvmd.log
/var/log/gvm/openvas.log /var/log/gvm/ospd-openvas.log
```

Upgrade

Postgresql 13 to 14

```
apt update
apt install postgresql-14 postgresql-server-dev-14
diff /etc/postgresql/13/main/postgresql.conf
/etc/postgresql/14/main/postgresql.conf
diff /etc/postgresql/13/main/pg_hba.conf /etc/postgresql/14/main/pg_hba.conf
systemctl stop postgresql
su - postgres
```

as user postgres

```
/usr/lib/postgresql/14/bin/pg_upgrade \
  --old-datadir=/var/lib/postgresql/13/main \
  --new-datadir=/var/lib/postgresql/14/main \
  --old-bindir=/usr/lib/postgresql/13/bin \
  --new-bindir=/usr/lib/postgresql/14/bin \
```

```
  --old-options '-c config_file=/etc/postgresql/13/main/postgresql.conf' \
  --new-options '-c config_file=/etc/postgresql/14/main/postgresql.conf' \
  --check
```

if there is an error like “There seems to be a postmaster servicing the new cluster. Please shutdown that postmaster and try again.” re-run **systemctl stop postgresql**

Then migrate data:

```
/usr/lib/postgresql/14/bin/pg_upgrade \
  --old-datadir=/var/lib/postgresql/13/main \
  --new-datadir=/var/lib/postgresql/14/main \
  --old-bindir=/usr/lib/postgresql/13/bin \
  --new-bindir=/usr/lib/postgresql/14/bin \
  --old-options '-c config_file=/etc/postgresql/13/main/postgresql.conf' \
  --new-options '-c config_file=/etc/postgresql/14/main/postgresql.conf'

exit
```

then as root, swap the ports and relaunch service

```
vi /etc/postgresql/14/main/postgresql.conf
# ...and change "port = 5433" to "port = 5432"

vi /etc/postgresql/13/main/postgresql.conf
# ...and change "port = 5432" to "port = 5433"


systemctl disable postgresql@13-main.service
systemctl start postgresql
```

Postgresql 14 to 15

```
apt update
apt install postgresql-15 postgresql-server-dev-15
diff /etc/postgresql/14/main/postgresql.conf
/etc/postgresql/15/main/postgresql.conf
diff /etc/postgresql/14/main/pg_hba.conf /etc/postgresql/15/main/pg_hba.conf
systemctl stop postgresql
su - postgres
```

as user postgres

```
/usr/lib/postgresql/15/bin/pg_upgrade \
  --old-datadir=/var/lib/postgresql/14/main \
  --new-datadir=/var/lib/postgresql/15/main \
  --old-bindir=/usr/lib/postgresql/14/bin \
  --new-bindir=/usr/lib/postgresql/15/bin \
  --old-options '-c config_file=/etc/postgresql/14/main/postgresql.conf' \
```

```
  --new-options '-c config_file=/etc/postgresql/15/main/postgresql.conf' \
  --check
```

if there is an error like “There seems to be a postmaster servicing the new cluster. Please shutdown that postmaster and try again.” re-run **systemctl stop postgresql**

Then migrate data:

```
/usr/lib/postgresql/15/bin/pg_upgrade \
  --old-datadir=/var/lib/postgresql/14/main \
  --new-datadir=/var/lib/postgresql/15/main \
  --old-bindir=/usr/lib/postgresql/14/bin \
  --new-bindir=/usr/lib/postgresql/15/bin \
  --old-options '-c config_file=/etc/postgresql/14/main/postgresql.conf' \
  --new-options '-c config_file=/etc/postgresql/15/main/postgresql.conf'

exit
```

then as root, swap the ports and relaunch service

```
vi /etc/postgresql/15/main/postgresql.conf
# ...and change "port = 5433" to "port = 5432"

vi /etc/postgresql/14/main/postgresql.conf
# ...and change "port = 5432" to "port = 5433"


systemctl disable postgresql@14-main.service
systemctl start postgresql
```

Postgresql 15 to 16

Reference:
https://medium.com/@gembit.soultan/how-to-upgrade-postgresql-15-to-postgresql-16-using-pg-upgradeclusters-in-ubuntu-22-04-c9f279c5d3ab

```
 pg_lsclusters
```

```
Ver Cluster Port Status Owner    Data directory              Log file
15  main    5432 online postgres /var/lib/postgresql/15/main
/var/log/postgresql/postgresql-15-main.log
16  main    5433 online postgres /var/lib/postgresql/16/main
/var/log/postgresql/postgresql-16-main.log
```

```
pg_dropcluster 16 main --stop
pg_lsclusters
```

```
Ver Cluster Port Status Owner    Data directory              Log file
15  main    5432 online postgres /var/lib/postgresql/15/main
```

```
/var/log/postgresql/postgresql-15-main.log
```

```
pg_upgradecluster 15 main
```

```
...
Success. Please check that the upgraded cluster works. If it does,
you can remove the old cluster with
    pg_dropcluster 15 main

Ver Cluster Port Status Owner    Data directory              Log file
15  main    5433 down   postgres /var/lib/postgresql/15/main
/var/log/postgresql/postgresql-15-main.log
Ver Cluster Port Status Owner    Data directory              Log file
16  main    5432 online postgres /var/lib/postgresql/16/main
/var/log/postgresql/postgresql-16-main.log
```

```
pg_dropcluster 15 main
apt purge postgresql-15 postgresql-client-15
```

Postgresql 16 to 17

```
 pg_lsclusters
```

```
Ver Cluster Port Status Owner    Data directory              Log file
16  main    5432 online postgres /var/lib/postgresql/16/main
/var/log/postgresql/postgresql-16-main.log
17  main    5433 online postgres /var/lib/postgresql/17/main
/var/log/postgresql/postgresql-17-main.log
```

```
pg_dropcluster 17 main --stop
pg_lsclusters
```

```
Ver Cluster Port Status Owner    Data directory              Log file
16  main    5432 online postgres /var/lib/postgresql/16/main
/var/log/postgresql/postgresql-16-main.log
```

```
pg_upgradecluster 16 main
```

```
....
Stopping target cluster...
Stopping old cluster...
Disabling automatic startup of old cluster...
Starting upgraded cluster on port 5432...
Running finish phase upgrade hook scripts ...
vacuumdb: processing database "gvmd": Generating minimal optimizer
statistics (1 target)
vacuumdb: processing database "postgres": Generating minimal optimizer
statistics (1 target)
```

```
vacuumdb: processing database "template1": Generating minimal optimizer
statistics (1 target)
vacuumdb: processing database "gvmd": Generating medium optimizer statistics
(10 targets)
vacuumdb: processing database "postgres": Generating medium optimizer
statistics (10 targets)
vacuumdb: processing database "template1": Generating medium optimizer
statistics (10 targets)
vacuumdb: processing database "gvmd": Generating default (full) optimizer
statistics
vacuumdb: processing database "postgres": Generating default (full)
optimizer statistics
vacuumdb: processing database "template1": Generating default (full)
optimizer statistics

Success. Please check that the upgraded cluster works. If it does,
you can remove the old cluster with
    pg_dropcluster 16 main

Ver Cluster Port Status Owner    Data directory              Log file
16  main    5433 down   postgres /var/lib/postgresql/16/main
/var/log/postgresql/postgresql-16-main.log
Ver Cluster Port Status Owner    Data directory              Log file
17  main    5432 online postgres /var/lib/postgresql/17/main
/var/log/postgresql/postgresql-17-main.log
```

```
pg_dropcluster 16 main
apt purge postgresql-16 postgresql-client-16
```

Logrotate

There was an issue with /etc/logrotate.d/ files:

```
systemctl --failed
  UNIT              LOAD   ACTIVE SUB    DESCRIPTION
● logrotate.service loaded failed failed Rotate log files

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
1 loaded units listed.

systemctl status logrotate
× logrotate.service - Rotate log files
     Loaded: loaded (/lib/systemd/system/logrotate.service; static)
     Active: failed (Result: exit-code) since Wed 2022-06-01 06:54:28 CEST;
2s ago
TriggeredBy: ● logrotate.timer
```

```
       Docs: man:logrotate(8)
             man:logrotate.conf(5)
    Process: 96050 ExecStart=/usr/sbin/logrotate /etc/logrotate.conf
(code=exited, status=1/FAILURE)
   Main PID: 96050 (code=exited, status=1/FAILURE)
        CPU: 24ms

Jun 01 06:54:28 svx-vs1 systemd[1]: Starting Rotate log files...
Jun 01 06:54:28 svx-vs1 logrotate[96050]: error: gsad:1 duplicate log entry
for /var/log/gvm/gsad.log
Jun 01 06:54:28 svx-vs1 logrotate[96050]: error: found error in file gsad,
skipping
Jun 01 06:54:28 svx-vs1 systemd[1]: logrotate.service: Main process exited,
code=exited, status=1/FAILURE
Jun 01 06:54:28 svx-vs1 systemd[1]: logrotate.service: Failed with result
'exit-code'.
Jun 01 06:54:28 svx-vs1 systemd[1]: Failed to start Rotate log files.
```

Indeed:

```
grep "/var/log/gvm/gsad.log" /etc/logrotate.d/*
/etc/logrotate.d/greenbone-security-assistant:/var/log/gvm/gsad.log {
/etc/logrotate.d/greenbone-security-assistant:    openvaslogs=`ls
/var/log/gvm/gsad.log.*`
/etc/logrotate.d/gsad:/var/log/gvm/gsad.log {
/etc/logrotate.d/gsad:    openvaslogs=`ls /var/log/gvm/gsad.log.*`
```

let's “fix” it

```
mv /etc/logrotate.d/greenbone-security-assistant .
systemctl restart logrotate
```

postgreSQL

:! using psql works, the .conf crashes the gvmd service... 
Using PGTune added the following lines at the end of **/etc/postgresql/14/main/postgresql.conf**:

```
 su - postgres
psql
```

```
ALTER SYSTEM SET
 max_connections = '20';
ALTER SYSTEM SET
 shared_buffers = '4GB';
ALTER SYSTEM SET
 effective_cache_size = '12GB';
ALTER SYSTEM SET
```

```
 maintenance_work_mem = '1GB';
ALTER SYSTEM SET
 checkpoint_completion_target = '0.9';
ALTER SYSTEM SET
 wal_buffers = '16MB';
ALTER SYSTEM SET
 default_statistics_target = '100';
ALTER SYSTEM SET
 random_page_cost = '1.1';
ALTER SYSTEM SET
 effective_io_concurrency = '200';
ALTER SYSTEM SET
 work_mem = '52428kB';
ALTER SYSTEM SET
 min_wal_size = '1GB';
ALTER SYSTEM SET
 max_wal_size = '4GB';
ALTER SYSTEM SET
 max_worker_processes = '16';
ALTER SYSTEM SET
 max_parallel_workers_per_gather = '4';
ALTER SYSTEM SET
 max_parallel_workers = '16';
ALTER SYSTEM SET
 max_parallel_maintenance_workers = '4';
```

Optimisation

From : https://community.greenbone.net/t/optimizing-postgresql-for-gvmd/6713/17

```
/usr/sbin/gvmd --optimize=vacuum
/usr/sbin/gvmd --optimize=analyze
/usr/sbin/gvmd --optimize=cleanup-report-formats
/usr/sbin/gvmd --optimize=cleanup-result-nvts
/usr/sbin/gvmd --optimize=cleanup-config-prefs
/usr/sbin/gvmd --optimize=cleanup-result-severities
/usr/sbin/gvmd --optimize=update-report-cache
```

in the crontab:

```
 for optimize in vaccum analyse cleanup-report-formats cleanup-result-nvts
cleanup-config-prefs cleanup-result-severities update-report-cache; do
/usr/sbin/gvmd --optimize=$optimize; done
```

Checks after update

- scan
- pdf generation

Journal

- PDF 0 Byte → edit var/lib/gvm/gvmd/report_formats/a67ec44b-a708-445d-a6a8-29f76a6a9647/c402cc3e-b531-11e1-9163-406186ea4fc5/latex.xsl (comment \usepackage[utf8x]{inputenc})
- Redis server out of memory ⇔ task stopped (add more ram (32GB) + 64GB swap)

```
echo 1 > /proc/sys/vm/overcommit_memory
```

```
fallocate -l 64G /mnt/64GB.swap
dd if=/dev/zero of=/mnt/64GB.swap bs=1024 count=67108864
echo "vm.swappiness=10" > /etc/sysctl.conf
chmod 0600 /mnt/64GB.swap
mkswap /mnt/64GB.swap
swapon /mnt/64GB.swap

echo "/mnt/64GB.swap  none  swap  sw 0  0" >>/etc/fstab
```

Services update

```
apt update && apt dist-upgrade -y
gvm-stop
su - _gvm -s /bin/sh -c "gvmd --migrate"
vi /lib/systemd/system/greenbone-security-assistant.service # check port
systemctl daemon-reload && systemctl restart gvmd.service gsad.service
greenbone-security-assistant.service
```

Running on different port

```
 vi /lib/systemd/system/gsad.service
```

```
[Unit]
Description=Greenbone Security Assistant daemon (gsad)
Documentation=man:gsad(8) https://www.greenbone.net
After=network.target gvmd.service
Wants=gvmd.service
```

```
[Service]
Type=exec
User=_gvm
Group=_gvm
RuntimeDirectory=gsad
RuntimeDirectoryMode=2775
PIDFile=/run/gsad/gsad.pid
ExecStart=/usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
Restart=always
TimeoutStopSec=10

[Install]
WantedBy=multi-user.target
Alias=greenbone-security-assistant.service
```

Change

```
 ExecStart=/usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
```

to

```
 ExecStart=/usr/sbin/gsad --foreground --listen 0.0.0.0 --port 443
```

Email size

If you get the message “Note: This report exceeds the maximum length of XXXXX characters…” in your mail report:

```
vi /lib/systemd/system/gvmd.service
```

```
...
ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-
group=_gvm --max-email-attachment-size=-1 --max-email-include-size=-1
...
```

```
systemctl daemon-reload
systemctl restart gvmd
systemctl status gvmd
```

```
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/lib/systemd/system/gvmd.service; enabled; preset:
disabled)
     Active: active (running) since Wed 2023-11-15 09:29:51 CET; 7s ago
       Docs: man:gvmd(8)
    Process: 278417 ExecStart=/usr/sbin/gvmd --osp-vt-
update=/run/ospd/ospd.sock --listen-group=_gvm --max-email-attachment-
size=8000000 --max-email-include-size=8000000 --max-email-message-
```

```
size=8000000 (code=exited, status=0/SUCCESS)
   Main PID: 278420 (gvmd)
      Tasks: 1 (limit: 9312)
     Memory: 184.2M
        CPU: 1.742s
     CGroup: /system.slice/gvmd.service
             └─278420 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm --max-email-attachment-size=8000000 --max-email-include-size=8000000 --max-email-message-size=8000000

Nov 15 09:29:48 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Nov 15 09:29:48 kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Nov 15 09:29:51 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
```

Better:

```
ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm --max-email-attachment-size=-1 --max-email-include-size=-1
```

References

- https://stafwag.github.io/blog/blog/2021/02/28/howto-install-opevas-on-kali/ [OUTDATED]
- https://emre.rocks/blog/2021/05/15/how-to-install-openvas-in-kali-linux/
- https://linuxhint.com/install-openvas-kali-linux/
- https://www.securitynewspaper.com/2020/12/19/how-to-configure-run-and-automate-openvas-free-vulnerability-scanner/
- https://www.hackingtutorials.org/scanning-tutorials/vulnerability-scanning-openvas-9-0-part-2/
- https://rafaelhart.com/2019/10/installing-xrdp-on-kali-linux/ | https://c-nergy.be/blog/?p=12073
- https://www.youtube.com/watch?v=_eLI8XuXf4I
- https://consulting-insights.de/2021-03/fix-for-kali-linux-xrdp-authentication-is-required-to-create-a-color-managed-device
- https://www.kostolansky.sk/posts/upgrading-to-postgresql-14/
- https://kifarunix.com/install-gvm-21-04-on-debian-11-debian-10/
- https://bugs.kali.org/view.php?id=7617#c15926
- https://forum.greenbone.net/t/kali-linux-cannot-create-pdf-reports/13014/4
- https://forum.greenbone.net/t/i-need-help-i-cant-see-the-reports-be-sent-out-because-of-maximum-length/14483/2
- https://www.geeksforgeeks.org/installing-openvas-on-kali-linux/