

# Harden Linux OS

## POSTER



## FIREWALL

```
cisco@ubuntu:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
cisco@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
cisco@ubuntu:~$ sudo apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.35ubuntu1)
cisco@ubuntu:~$ sudo ufw allow http
Rule added
Rule added (v6)
cisco@ubuntu:~$
```

## REGULAR AUDIT

```
#
#
# Weekly Lynis scan:
# 0 3 * * 0 /usr/bin/lynis audit system > /var/log/lynis-weekly.log
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
```

## ANTIVIRUS SOFTWARE

```
cisco@ubuntu:~$ sudo apt install chkrootkit rkhunter
[sudo] password for cisco:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required
--> libltdl7.1.2-1
Uninstalling libltdl7.1.2 (0.9.27-1)...
cisco@ubuntu:~$ sudo chkrootkit
ROOTDIR is '/'
Checking `amd'...
Checking `basename'...
Checking `biff'.cov ...
cisco@ubuntu:~$ sudo rkhunter
Usage: rkhunter {--check | --unlock | --update | --version |
                  --propupd [{filename | directory | package} |
                  --list [{tests | {lang | languages} | rootfiles}] |
                  --config-check | --version | --help} [options]
cisco@ubuntu:~$ sudo freshclam
[...]
cisco@ubuntu:~$ sudo clamscan -r /
[...]
```