



# INFORMATION ASSURANCE AND AUDITING

Mini project

## Server Audits

Linux Server audit using Lynis, wapiti, Openscap Tools | Windows Server audit using XIA  
configuration Tool

R.K.M Shamal Karunanayake  
IT17032070/CSNE weekend

## Table of Contents

<b>1. Introduction</b>	2
<b>2. Linux Server Audits</b>	2
2.1 Create a VM instance and installing Software (Apache web server)	2
2.2 Perform Server audit using Lynis tool	5
<b>2.2.1 Audit results</b>	6
<b>2.2.2 Checklist</b>	7
2.3 Perform WebServer audit using Wapiti tool	28
<b>2.3.1 Audit results</b>	29
2.4 Perform Server audit using OpenSCAP tool	30
<b>2.4.1 Audit results</b>	31
<b>3. Windows Server Audits</b>	32
3.1 Perform Server audit using XIA Configuration tool	32
<b>3.1.1 Audit results</b>	35
References	37

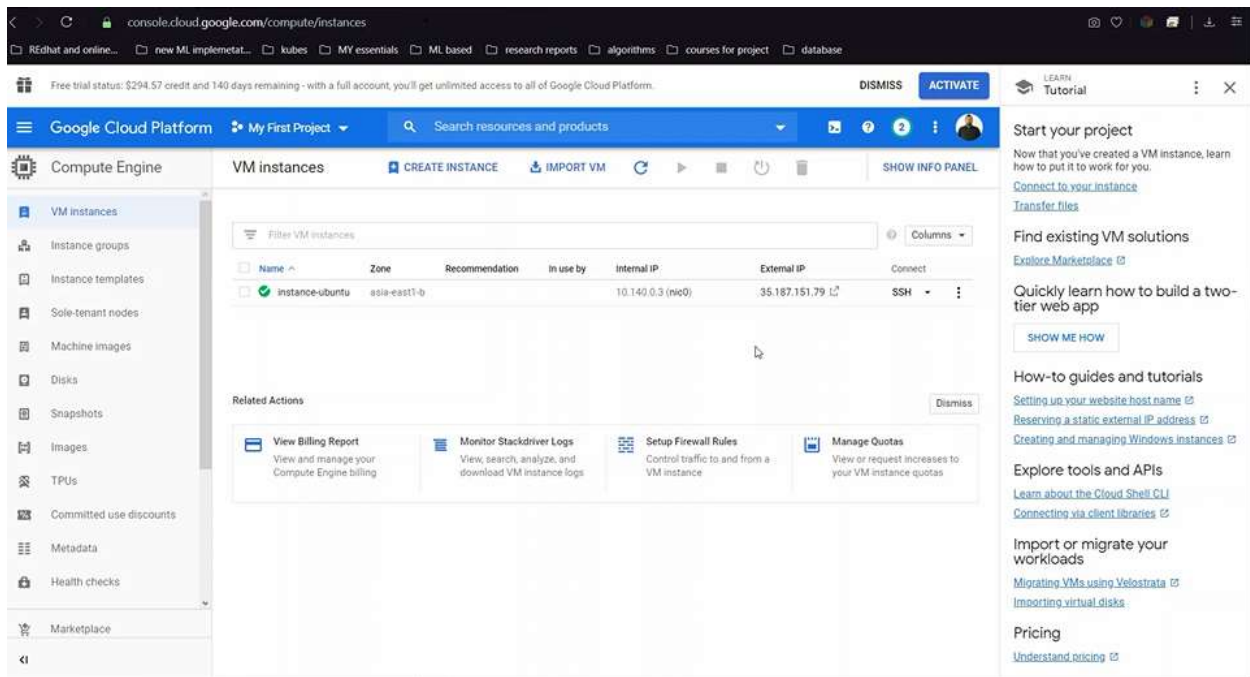
## 1. Introduction

An **audit** is an independent examination of financial information of any entity, whether profit oriented or not, irrespective of its size or legal form. When such an examination is conducted with a view to express an opinion thereon - <https://en.wikipedia.org/wiki/Audit>

Audits are important tools for organizations. A thoroughly conducted audit program can assure organizational stakeholders of the financial, operational and ethical well-being of an organization. It should confirm the effectiveness of current operations and on-going compliance with administrative or legal regulations. Or it can reveal the need for change or urgent action.

## 2. Linux Server Audits

### 2.1 Create a VM instance and installing Software (Apache web server)



### Install Apache

Apache is available within Ubuntu's default software repositories, so we will install it using conventional package management tools.

```
sudo apt-get update
```

```
sudo apt-get install apache2
```

## Adjust the Firewall

We can list the ufw application profiles by typing following command

```
sudo ufw app list
```

OUTPUT:

Available applications:

Apache

Apache Full

Apache Secure

OpenSSH

we will allow incoming traffic for the Apache Full profile by typing:

```
sudo ufw allow 'Apache Full'
```

## Check your Web Server

```
sudo systemctl status apache2
```

```
hostname -I
```

When you have your server's IP address or domain, enter it into your browser's address bar:

```
http://server_domain_or_IP
```

```
root@instance-ubuntu: ~ - Opera
ssh.cloud.google.com/projects/focus-union-253707/zones/asia-east1-b/instances/instance-ubuntu
shamalkarunamayake@instance-ubuntu:~$ sudo -s
root@instance-ubuntu:~#
root@instance-ubuntu:~# sudo apt-get update
Hit:1 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:3 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Get:4 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:5 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:6 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/multiverse amd64 Packages [144 kB]
Get:7 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/multiverse Translation-en [106 kB]
Get:8 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1,141 kB]
Get:9 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [797 kB]
Get:10 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [333 kB]
Get:11 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Packages [17.1 kB]
Get:12 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translation-en [8,632 B]
Get:13 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports/main amd64 Packages [7,280 B]
Get:14 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports/main Translation-en [4,456 B]
Get:15 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Packages [8,064 B]
Get:16 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports/universe Translation-en [4,328 B]
Get:17 http://archive.canonical.com/ubuntu xenial InRelease [11.5 kB]
Get:18 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Get:19 http://archive.canonical.com/ubuntu xenial/partner amd64 Packages [3,124 B]
Get:20 http://archive.canonical.com/ubuntu xenial/partner Translation-en [1,672 B]
Get:21 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [861 kB]
Get:22 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [323 kB]
Get:23 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [490 kB]
Get:24 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [200 kB]
Get:25 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [6,088 B]
Get:26 http://security.ubuntu.com/ubuntu xenial-security/multiverse Translation-en [2,888 B]
Fetched 16.7 MB in 3s (4,875 kB/s)
Reading package lists... Done
root@instance-ubuntu:~# sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
```

```
root@instance-ubuntu: ~ - Opera
ssh.cloud.google.com/projects/focus-union-253707/zones/asia-east1-b/instances/instance-ubuntu

root@instance-ubuntu:~# sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
root@instance-ubuntu:~# sudo ufw allow 'Apache Full'
ERROR: Need 'to' or 'from' clause
root@instance-ubuntu:~# sudo ufw allow 'Apache Full'
Rules updated
Rules updated (v6)
root@instance-ubuntu:~# systemctl status ap
apache2.service          apport.service           apt-daily-upgrade.service
apparmor.service         apt-daily.service        apt-daily-upgrade.timer
appport-forward.socket   apt-daily.timer
root@instance-ubuntu:~# systemctl status apache2
* apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Tue 2020-05-05 18:47:22 UTC; 1min 40s ago
     Docs: man:systemd-sysv-generator(8)
    CGroup: /system.slice/apache2.service
            └─3444 /usr/sbin/apache2 -k start
               3447 /usr/sbin/apache2 -k start
               3448 /usr/sbin/apache2 -k start

May 05 18:47:21 instance-ubuntu systemd[1]: Starting LSB: Apache2 web server...
May 05 18:47:21 instance-ubuntu apache2[3401]: * Starting Apache httpd web server apache2
May 05 18:47:22 instance-ubuntu apache2[3401]: *
May 05 18:47:22 instance-ubuntu systemd[1]: Started LSB: Apache2 web server.
root@instance-ubuntu:~# hostname -i
10.140.0.3
```


Compute Engine - My Inst...Apache2 Ubuntu Default

35.107.151.79

Not secure

35.107.151.79

Reddit and online...new ML implementat...kubesMy essentialsML basedresearch reportsalgorithmscourses for projectdatabase



## Apache2 Ubuntu Default Page

### It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the

## 2.2 Perform Server audit using Lynis tool

Install Lynis using the package manager.

```
dpkg -s apt-transport-https | grep -i status
```

Add the repository's key.

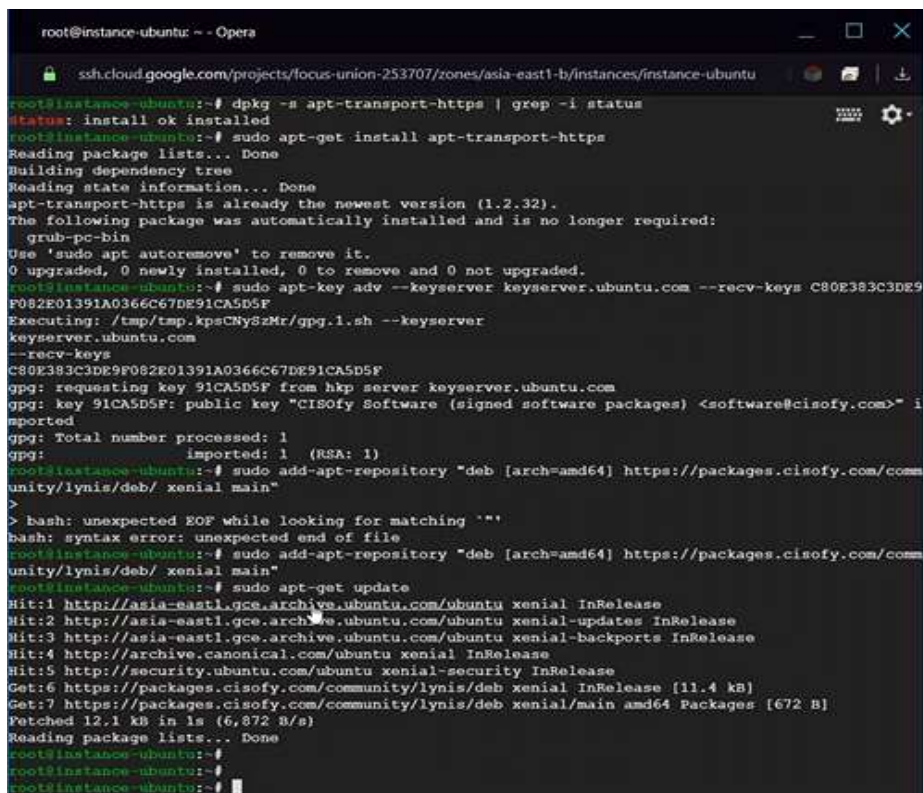
```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys  
C80E383C3DE9F082E01391A0366C67DE91CA5D5F
```

Then add the Lynis repository to the list of those available to the package manager.

```
sudo add-apt-repository "deb [arch=amd64] https://packages.cisofy.com/community/lynis/deb/  
xenial main"
```

To make the packages in the newly added repository available to the system, update the package database.

```
sudo apt-get update
```



```
root@instance-ubuntu: ~ - Opera
ssh.cloud.google.com/projects/focus-union-253707/zones/asia-east1-b/instances/instance-ubuntu

root@instance-ubuntu:~# dpkg -s apt-transport-https | grep -i status
Status: install ok installed
root@instance-ubuntu:~# sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
apt-transport-https is already the newest version (1.2.32).
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@instance-ubuntu:~# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys C80E383C3DE9
F082E01391A0366C67DE91CA5D5F
Executing: /tmp/tmp.kpsCNYsZMr/gpg.1.sh --keyserver
keyserver.ubuntu.com
--recv-keys
C80E383C3DE9F082E01391A0366C67DE91CA5D5F
gpg: requesting key 91CA5D5F from hkp server keyserver.ubuntu.com
gpg: key 91CA5D5F: public key "CISofy Software (signed software packages) <software@cisofy.com>" i
mported
gpg: Total number processed: 1
gpg:      imported: 1 (RSA: 1)
root@instance-ubuntu:~# sudo add-apt-repository "deb [arch=amd64] https://packages.cisofy.com/comm
unity/lynis/deb/ xenial main"
>
> bash: unexpected EOF while looking for matching `"'
bash: syntax error: unexpected end of file
root@instance-ubuntu:~# sudo add-apt-repository "deb [arch=amd64] https://packages.cisofy.com/comm
unity/lynis/deb/ xenial main"
root@instance-ubuntu:~# sudo apt-get update
Hit:1 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-backports InRelease
Hit:4 http://archive.canonical.com/ubuntu xenial InRelease
Hit:5 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:6 https://packages.cisofy.com/community/lynis/deb xenial InRelease [11.4 kB]
Get:7 https://packages.cisofy.com/community/lynis/deb xenial/main amd64 Packages [672 B]
Fetched 12.1 kB in 1s (6,872 B/s)
Reading package lists... Done
root@instance-ubuntu:~#
root@instance-ubuntu:~#
root@instance-ubuntu:~#
```

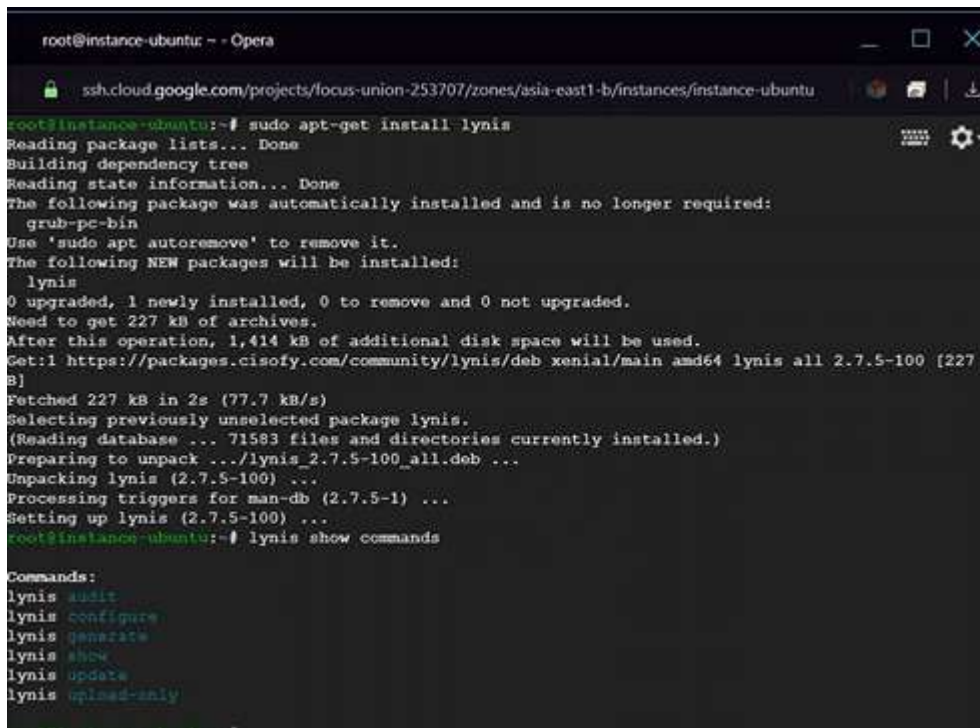


Finally, install Lynis.

```
sudo apt-get install lynis
```

To viewing a list of actions you can perform with Lynis. Execute the following command:

```
lynis show commands
```

A terminal window titled 'root@instance-ubuntu: ~ - Opera' showing the installation of Lynis. The user runs 'sudo apt-get install lynis'. The output shows that 'grub-pc-bin' is automatically installed and no longer required, and 'lynis' is the new package to be installed. The installation completes successfully. Then, the user runs 'lynis show commands', which lists the following commands: 'lynis audit', 'lynis configure', 'lynis generate', 'lynis show', 'lynis update', and 'lynis upload-only'.

```
root@instance-ubuntu:~# sudo apt-get install lynis
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  lynis
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 227 kB of archives.
After this operation, 1,414 kB of additional disk space will be used.
Get:1 https://packages.cisofy.com/community/lynis/deb xenial/main amd64 lynis all 2.7.5-100 [227 kB]
Fetched 227 kB in 2s (77.7 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 71583 files and directories currently installed.)
Preparing to unpack .../lynis_2.7.5-100_all.deb ...
Unpacking lynis (2.7.5-100) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up lynis (2.7.5-100) ...
root@instance-ubuntu:~# lynis show commands

Commands:
lynis audit
lynis configure
lynis generate
lynis show
lynis update
lynis upload-only
```

view the settings for the default profile:

```
lynis show settings
```

To run an audit of your system. You can run Lynis in privileged and non-privileged (pentest) mode.

```
sudo lynis audit system
```

## 2.2.1 Audit results

After each audit, test results, debug information, and suggestions for hardening the system are written to standard output terminal screen. report data is saved to `/var/log/lynis-report.dat`. Report data consists of general information of server and application . The log file is overwritten on each audit. The first significant part of a Lynis audit output is purely informational. It tells you

the result of every test, grouped by category. The information takes the form of keywords, like **NONE**, **WEAK**, **DONE**, **FOUND**, **NOT\_FOUND**, **OK**, and **WARNING**.

### 2.2.2 Checklist

#### [+] Initializing program

```
-----  
- Detecting OS...                [ DONE ]  
- Checking profiles...           [ DONE ]  
-----
```

```
Program version:      2.7.5  
Operating system:     Linux  
Operating system name: Ubuntu Linux  
Operating system version: 16.04  
Kernel version:       4.15.0  
Hardware platform:    x86_64  
Hostname:             instance-1  
-----
```

```
Profiles:            /etc/lynis/default.prf  
Log file:            /var/log/lynis.log  
Report file:         /var/log/lynis-report.dat  
Report version:      1.0  
Plugin directory:    /usr/share/lynis/plugins  
-----
```

```
Auditor:             [Not Specified]  
Language:            en  
Test category:       all  
Test group:          all  
-----
```

```
- Program update status...        [ NO UPDATE ]
```

```
=====
```

```
=====
```

```
Lynis update available
```

```
=====
```

```
=====
```

```
Current version is more than 4 months old  
Current version : 275   Latest version : 275
```



Please update to the latest version.

New releases include additional features, bug fixes, tests, and baselines.

Download the latest version:

Packages (DEB/RPM) - <https://packages.cisofy.com>

Website (TAR) - <https://cisofy.com/downloads/>

GitHub (source) - <https://github.com/CISOfy/lynis>

---

---

## [+] System Tools

---

- Scanning available tools...
- Checking system binaries...

## [+] Plugins (phase 1)

---

Note: plugins have more extensive tests and may take several minutes to complete

- Plugins enabled [ NONE ]

## [+] Boot and services

---

- Service Manager [ systemd ]
- Checking UEFI boot [ ENABLED ]
- Checking Secure Boot [ DISABLED ]
- Checking presence GRUB [ OK ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ NONE ]
- Check running services (systemctl) [ DONE ]
- Result: found 24 running services
- Check enabled services at boot (systemctl) [ DONE ]
- Result: found 40 enabled services
- Check startup files (permissions) [ OK ]

## [+] Kernel

---

- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE)
- CPU support: PAE and/or NoeXecute supported [ FOUND ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules [ DONE ]

Found 46 active modules

- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ FOUND ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration [ DISABLED ]
  - Checking setuid core dumps configuration [ PROTECTED ]
- Check if reboot is needed [ NO ]

### [+] Memory and Processes

---

- Checking /proc/meminfo [ FOUND ]
- Searching for dead/zombie processes [ OK ]
- Searching for IO waiting processes [ OK ]

### [+] Users, Groups and Authentication

---

- Administrator accounts [ OK ]
- Unique UIDs [ OK ]
- Consistency of group files (grpck) [ OK ]
- Unique group IDs [ OK ]
- Unique group names [ OK ]
- Password file consistency [ OK ]
- Query system users (non daemons) [ DONE ]
- NIS+ authentication support [ NOT ENABLED ]
- NIS authentication support [ NOT ENABLED ]
- sudoers file [ FOUND ]
  - Permissions for directory: /etc/sudoers.d [ OK ]
  - Permissions for: /etc/sudoers [ OK ]
  - Permissions for: /etc/sudoers.d/90-cloud-init-users [ OK ]
  - Permissions for: /etc/sudoers.d/README [ OK ]
  - Permissions for: /etc/sudoers.d/google\_sudoers [ OK ]
- PAM password strength tools [ SUGGESTION ]
- PAM configuration files (pam.conf) [ FOUND ]
- PAM configuration files (pam.d) [ FOUND ]
- PAM modules [ FOUND ]
- LDAP module in PAM [ NOT FOUND ]
- Accounts without expire date [ OK ]
- Accounts without password [ OK ]
- Checking user password aging (minimum) [ DISABLED ]
- User password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]

- Checking Linux single user mode authentication [ OK ]
- Determining default umask
  - umask (/etc/profile) [ NOT FOUND ]
  - umask (/etc/login.defs) [ SUGGESTION ]
  - umask (/etc/init.d/rc) [ SUGGESTION ]
- LDAP authentication support [ NOT ENABLED ]
- Logging failed login attempts [ ENABLED ]

#### [+] Shells

---

- Checking shells from /etc/shells  
Result: found 6 shells (valid shells: 6).
- Session timeout settings/tools [ NONE ]
- Checking default umask values
  - Checking default umask in /etc/bash.bashrc [ NONE ]
  - Checking default umask in /etc/profile [ NONE ]

#### [+] File systems

---

- Checking mount points
  - Checking /home mount point [ SUGGESTION ]
  - Checking /tmp mount point [ SUGGESTION ]
  - Checking /var mount point [ SUGGESTION ]
- Query swap partitions (fstab) [ NONE ]
- Testing swap partitions [ OK ]
- Testing /proc mount (hidepid) [ SUGGESTION ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- Checking /var/tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Mount options of / [ OK ]
- Checking Locate database [ FOUND ]
- Disable kernel support of some filesystems
  - Discovered kernel modules: udf

#### [+] USB Devices

---

- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ DISABLED ]
- Checking USBGuard [ NOT FOUND ]

#### [+] Storage

---

- Checking firewire ohci driver (modprobe config) [ DISABLED ]

## [+] NFS

-----  
- Check running NFS daemon [ NOT FOUND ]

## [+] Name services

-----  
- Checking search domains [ FOUND ]  
- Searching DNS domain name [ FOUND ]  
Domain name: us-central1-a.c.focus-union-253707.internal  
- Checking /etc/hosts  
- Checking /etc/hosts (duplicates) [ SUGGESTION ]  
- Checking /etc/hosts (hostname) [ OK ]  
- Checking /etc/hosts (localhost) [ OK ]  
- Checking /etc/hosts (localhost to IP) [ OK ]

## [+] Ports and packages

-----  
- Searching package managers  
- Searching dpkg package manager [ FOUND ]  
- Querying package manager  
- Query unpurged packages [ FOUND ]  
- Checking security repository in sources.list file [ OK ]  
- Checking APT package database [ OK ]  
- Checking vulnerable packages [ WARNING ]  
- Checking upgradeable packages [ SKIPPED ]  
- Checking package audit tool [ INSTALLED ]  
Found: apt-get  
- Toolkit for automatic upgrades (unattended-upgrade) [ FOUND ]

## [+] Networking

-----  
- Checking IPv6 configuration [ ENABLED ]  
Configuration method [ AUTO ]  
IPv6 only [ NO ]  
- Checking configured nameservers  
- Testing nameservers  
Nameserver: 169.254.169.254 [ OK ]  
- Minimal of 2 responsive nameservers [ WARNING ]  
- Checking default gateway [ DONE ]  
- Getting listening ports (TCP/UDP) [ DONE ]  
- Checking promiscuous interfaces [ OK ]

- Checking waiting connections [ OK ]
- Checking status DHCP client [ RUNNING ]
- Checking for ARP monitoring software [ NOT FOUND ]

#### [+] Printers and Spools

---

- Checking cups daemon [ NOT FOUND ]
- Checking lp daemon [ NOT RUNNING ]

#### [+] Software: e-mail and messaging

---

#### [+] Software: firewalls

---

- Checking iptables kernel module [ FOUND ]
- Checking iptables policies of chains [ FOUND ]
- Checking for empty ruleset [ WARNING ]
- Checking for unused rules [ OK ]
- Checking host based firewall [ ACTIVE ]

#### [+] Software: webserver

---

- Checking Apache [ NOT FOUND ]
- Checking nginx [ NOT FOUND ]

#### [+] SSH Support

---

- Checking running SSH daemon [ FOUND ]
- Searching SSH configuration [ FOUND ]
- SSH option: AllowTcpForwarding [ SUGGESTION ]
- SSH option: ClientAliveCountMax [ SUGGESTION ]
- SSH option: ClientAliveInterval [ OK ]
- SSH option: Compression [ SUGGESTION ]
- SSH option: FingerprintHash [ OK ]
- SSH option: GatewayPorts [ OK ]
- SSH option: IgnoreRhosts [ OK ]
- SSH option: LoginGraceTime [ OK ]
- SSH option: LogLevel [ SUGGESTION ]
- SSH option: MaxAuthTries [ SUGGESTION ]
- SSH option: MaxSessions [ SUGGESTION ]
- SSH option: PermitRootLogin [ OK ]
- SSH option: PermitUserEnvironment [ OK ]
- SSH option: PermitTunnel [ OK ]
- SSH option: Port [ SUGGESTION ]

- SSH option: PrintLastLog [ OK ]
- SSH option: StrictModes [ OK ]
- SSH option: TCPKeepAlive [ SUGGESTION ]
- SSH option: UseDNS [ OK ]
- SSH option: VerifyReverseMapping [ NOT FOUND ]
- SSH option: X11Forwarding [ SUGGESTION ]
- SSH option: AllowAgentForwarding [ SUGGESTION ]
- SSH option: Protocol [ OK ]
- SSH option: UsePrivilegeSeparation [ SUGGESTION ]
  - SSH option: AllowUsers [ NOT FOUND ]
- SSH option: AllowGroups [ NOT FOUND ]

#### [+] SNMP Support

---

- Checking running SNMP daemon [ NOT FOUND ]

#### [+] Databases

---

No database engines found

#### [+] LDAP Services

---

- Checking OpenLDAP instance [ NOT FOUND ]

#### [+] PHP

---

- Checking PHP [ NOT FOUND ]

#### [+] Squid Support

---

- Checking running Squid daemon [ NOT FOUND ]

#### [+] Logging and files

---

- Checking for a running log daemon [ OK ]
- Checking Syslog-NG status [ NOT FOUND ]
- Checking systemd journal status [ FOUND ]
- Checking Metalog status [ NOT FOUND ]
- Checking RSyslog status [ FOUND ]
- Checking RFC 3195 daemon status [ NOT FOUND ]
- Checking minilogd instances [ NOT FOUND ]
- Checking logrotate presence [ OK ]
- Checking log directories (static list) [ DONE ]
- Checking open log files [ DONE ]
- Checking deleted files in use [ DONE ]



## [+] Insecure services

---

- Installed inetd package [ NOT FOUND ]
- Installed xinetd package [ OK ]
  - xinetd status [ NOT ACTIVE ]
- Installed rsh client package [ OK ]
- Installed rsh server package [ OK ]
- Installed telnet client package [ OK ]
- Installed telnet server package [ NOT FOUND ]

## [+] Banners and identification

---

- /etc/issue [ FOUND ]
- /etc/issue contents [ WEAK ]
- /etc/issue.net [ FOUND ]
- /etc/issue.net contents [ WEAK ]

## [+] Scheduled tasks

---

- Checking crontab and cronjob files [ DONE ]
- Checking atd status [ RUNNING ]
- Checking at users [ DONE ]
- Checking at jobs [ NONE ]

## [+] Accounting

---

- Checking accounting information [ NOT FOUND ]
- Checking sysstat accounting data [ NOT FOUND ]
- Checking auditd [ NOT FOUND ]

## [+] Time and Synchronization

---

- NTP daemon found: ntpd [ FOUND ]
- Checking for a running NTP daemon or client [ OK ]
- Checking valid association ID's [ FOUND ]
- Checking high stratum ntp peers [ OK ]
- Checking unreliable ntp peers [ NONE ]
- Checking selected time source [ OK ]
- Checking time source candidates [ NONE ]
- Checking falsetickers [ OK ]
- Checking NTP version [ FOUND ]

## [+] Cryptography

---

- Checking for expired SSL certificates [0/1] [ NONE ]

#### [+] Virtualization

---

#### [+] Containers

---

#### [+] Security frameworks

---

- Checking presence AppArmor [ FOUND ]  
- Checking AppArmor status [ ENABLED ]  
- Checking presence SELinux [ NOT FOUND ]  
- Checking presence TOMOYO Linux [ NOT FOUND ]  
- Checking presence grsecurity [ NOT FOUND ]  
- Checking for implemented MAC framework [ OK ]

#### [+] Software: file integrity

---

- Checking file integrity tools  
- Checking presence integrity tool [ NOT FOUND ]

#### [+] Software: System tooling

---

- Checking automation tooling  
- Automation tooling [ NOT FOUND ]  
- Checking for IDS/IPS tooling [ NONE ]

#### [+] Software: Malware

---

#### [+] File Permissions

---

- Starting file permissions check  
/root/.ssh [ OK ]

#### [+] Home directories

---

- Checking shell history files [ OK ]

#### [+] Kernel Hardening

---

- Comparing sysctl key pairs with scan profile  
- fs.protected\_hardlinks (exp: 1) [ OK ]  
- fs.protected\_symlinks (exp: 1) [ OK ]  
- fs.suid\_dumpable (exp: 0) [ DIFFERENT ]  
- kernel.core\_uses\_pid (exp: 1) [ DIFFERENT ]  
- kernel.ctrl-alt-del (exp: 0) [ OK ]

- kernel.dmesg\_restrict (exp: 1) [ DIFFERENT ]
- kernel.kptr\_restrict (exp: 2) [ DIFFERENT ]
- kernel.randomize\_va\_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ DIFFERENT ]
- kernel.yama.ptrace\_scope (exp: 1 2 3) [ OK ]
- net.ipv4.conf.all.accept\_redirects (exp: 0) [ OK ]
- net.ipv4.conf.all.accept\_source\_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp\_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.log\_martians (exp: 1) [ OK ]
- net.ipv4.conf.all.mc\_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy\_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp\_filter (exp: 1) [ OK ]
- net.ipv4.conf.all.send\_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept\_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept\_source\_route (exp: 0) [ OK ]
- net.ipv4.conf.default.log\_martians (exp: 1) [ OK ]
- net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) [ OK ]
- net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1) [ OK ]
- net.ipv4.tcp\_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp\_timestamps (exp: 0 1) [ OK ]
- net.ipv6.conf.all.accept\_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.all.accept\_source\_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept\_redirects (exp: 0) [ DIFFERENT ]
- net.ipv6.conf.default.accept\_source\_route (exp: 0) [ OK ]

#### [+] Hardening

- 
- Installed compiler(s) [ NOT FOUND ]
  - Installed malware scanner [ NOT FOUND ]

#### [+] Custom Tests

- 
- Running custom tests... [ NONE ]

#### [+] Plugins (phase 2)

---



---

-[ Lynis 2.7.5 Results ]-

#### Warnings (3):

! Found one or more vulnerable packages. [PKGS-7392]

<https://cisofy.com/lynis/controls/PKGS-7392/>

! Couldn't find 2 responsive nameservers [NETW-2705]

<https://cisofy.com/lynis/controls/NETW-2705/>

! iptables module(s) loaded, but no rules active [FIRE-4512]

<https://cisofy.com/lynis/controls/FIRE-4512/>

### **Suggestions (39):**

-----  
\* This release is more than 4 months old. Consider upgrading [LYNIS]

<https://cisofy.com/lynis/controls/LYNIS/>

\* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

<https://cisofy.com/lynis/controls/BOOT-5122/>

\* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]

<https://cisofy.com/lynis/controls/AUTH-9262/>

\* Configure minimum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

\* Configure maximum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

\* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

<https://cisofy.com/lynis/controls/AUTH-9328/>

\* Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]

<https://cisofy.com/lynis/controls/AUTH-9328/>

\* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

\* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

\* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]

<https://cisofy.com/lynis/controls/STRG-1840/>

\* Remove duplicate lines in /etc/hosts [NAME-4402]

<https://cisofy.com/lynis/controls/NAME-4402/>

<https://cisofy.com/lynis/controls/PKGS-7346/>

\* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

<https://cisofy.com/lynis/controls/PKGS-7370/>

\* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]

<https://cisofy.com/lynis/controls/PKGS-7392/>

\* Install package apt-show-versions for patch management purposes [PKGS-7394]

<https://cisofy.com/lynis/controls/PKGS-7394/>

\* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]

<https://cisofy.com/lynis/controls/NETW-2705/>

\* Consider running ARP monitoring software (arpwatch, arpon) [NETW-3032]

<https://cisofy.com/lynis/controls/NETW-3032/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : AllowTcpForwarding (YES --> NO)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : ClientAliveCountMax (3 --> 2)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : Compression (YES --> NO)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : LogLevel (INFO --> VERBOSE)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxAuthTries (6 --> 3)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : MaxSessions (10 --> 2)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : Port (22 --> )

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : TCPKeepAlive (YES --> NO)

<https://cisofy.com/lynis/controls/SSH-7408/>

\* Consider hardening SSH configuration [SSH-7408]

- Details : X11Forwarding (YES --> NO)

<https://cisofy.com/lynis/controls/SSH-7408/>

- \* Consider hardening SSH configuration [SSH-7408]
  - Details : AllowAgentForwarding (YES --> NO)
   
<https://cisofy.com/lynis/controls/SSH-7408/>
- \* Consider hardening SSH configuration [SSH-7408]
  - Details : UsePrivilegeSeparation (YES --> SANDBOX)
   
<https://cisofy.com/lynis/controls/SSH-7408/>
- \* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
   
<https://cisofy.com/lynis/controls/BANN-7126/>
- \* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
   
<https://cisofy.com/lynis/controls/BANN-7130/>
- \* Enable process accounting [ACCT-9622]
   
<https://cisofy.com/lynis/controls/ACCT-9622/>
- \* Enable sysstat to collect accounting (no results) [ACCT-9626]
   
<https://cisofy.com/lynis/controls/ACCT-9626/>
- \* Enable auditd to collect audit information [ACCT-9628]
   
<https://cisofy.com/lynis/controls/ACCT-9628/>
- \* Check ntpq peers output for time source candidates [TIME-3128]
   
<https://cisofy.com/lynis/controls/TIME-3128/>
- \* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
   
<https://cisofy.com/lynis/controls/FINT-4350/>
- \* Determine if automation tools are present for system management [TOOL-5002]
   
<https://cisofy.com/lynis/controls/TOOL-5002/>
- \* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
  - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
   
<https://cisofy.com/lynis/controls/KRNL-6000/>
- \* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
  - Solution : Install a tool like rkhunter, chkrootkit, OSSEC
   
<https://cisofy.com/lynis/controls/HRDN-7230/>

### **Follow-up:**

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (<https://cisofy.com>)
- Use --upload to upload data to central system (Lynis Enterprise users)

---

Lynis security scan details:

Hardening index : 63 [##### ]



Tests performed : 229

Plugins enabled : 0

Components:

- Firewall [V]
- Malware scanner [X]

Lynis modules:

- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:

- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

---

---

Lynis 2.7.5

Auditing, system hardening, and compliance for UNIX-based systems  
(Linux, macOS, BSD, and others)

2007-2019, CISOfy - <https://cisofy.com/lynis/>

Enterprise support available (compliance, plugins, interface and tools)

---

---

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

\* Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanu

## [+] Boot and services

```
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ ENABLED ]
- Checking Secure Boot [ DISABLED ]
- Checking presence GRUB [ OK ]
- Checking presence GRUB2 [ FOUND ]
  - Checking for password protection [ NONE ]
- Check running services (systemctl) [ DONE ]
  Result: found 25 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 40 enabled services
- Check startup files (permissions) [ OK ]
```

## [+] Kernel

```
-----
- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE)
  CPU support: PAE and/or NoeXecute supported [ FOUND ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules [ DONE ]
  Found 56 active modules
- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ FOUND ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration [ DISABLED ]
  - Checking setuid core dumps configuration [ PROTECTED ]
- Check if reboot is needed [ NO ]
```

## [+] Memory and Processes

```
-----
- Checking /proc/meminfo [ FOUND ]
- Searching for dead/zombie processes [ OK ]
- Searching for IO waiting processes [ OK ]
```

## [+] Users, Groups and Authentication

```
-----
- Administrator accounts [ OK ]
- Unique UIDs [ OK ]
- Consistency of group files (grpck) [ OK ]
- Unique group IDs [ OK ]
- Unique group names [ OK ]
- Password file consistency [ OK ]
- Query system users (non daemons) [ DONE ]
- NIS+ authentication support [ NOT ENABLED ]
```

```

[+] Shells
-----
- Checking shells from /etc/shells
  Result: found 6 shells (valid shells: 6).
- Session timeout settings/tools [ NONE ]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [ NONE ]
- Checking default umask in /etc/profile [ NONE ]

[+] File systems
-----
- Checking mount points
  - Checking /home mount point [ SUGGESTION ]
  - Checking /tmp mount point [ SUGGESTION ]
  - Checking /var mount point [ SUGGESTION ]
- Query swap partitions (fstab) [ NONE ]
- Testing swap partitions [ OK ]
- Testing /proc mount (hidepid) [ SUGGESTION ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- Checking /var/tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Mount options of / [ OK ]
- Checking Locate database [ FOUND ]
- Disable kernel support of some filesystems
  - Discovered kernel modules: udf

[+] USB Devices
-----
- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ DISABLED ]
- Checking USBGuard [ NOT FOUND ]

[+] Storage
-----
- Checking firewire ohci driver (modprobe config) [ DISABLED ]

[+] NFS
-----
- Check running NFS daemon [ NOT FOUND ]

[+] Name services
-----
- Checking search domains [ FOUND ]
- Searching DNS domain name [ FOUND ]
  Domain name: asia-east1-b.c.focus-union-253707.internal
- Checking /etc/hosts
- Checking /etc/hosts (duplicates) [ SUGGESTION ]

```

## [+] Ports and packages

- Searching package managers
  - Searching dpkg package manager [ FOUND ]
  - Querying package manager
  - Query unpurged packages [ FOUND ]
- Checking security repository in sources.list file [ OK ]
- Checking APT package database [ OK ]
- Checking vulnerable packages [ OK ]
- Checking upgradeable packages [ SKIPPED ]
- Checking package audit tool [ INSTALLED ]
  - Found: apt-check
- Toolkit for automatic upgrades (unattended-upgrade) [ FOUND ]

## [+] Networking

- Checking IPv6 configuration [ ENABLED ]
  - Configuration method [ AUTO ]
  - IPv6 only [ NO ]
- Checking configured nameservers
  - Testing nameservers
    - Nameserver: 169.254.169.254 [ OK ]
  - Minimal of 2 responsive nameservers [ WARNING ]
- Checking default gateway [ DONE ]
- Getting listening ports (TCP/UDP) [ DONE ]
- Checking promiscuous interfaces [ OK ]
- Checking waiting connections [ OK ]
- Checking status DHCP client [ RUNNING ]
- Checking for ARP monitoring software [ NOT FOUND ]

## [+] Printers and Spools

- Checking cups daemon [ NOT FOUND ]
- Checking lp daemon [ NOT RUNNING ]

## [+] Software: e-mail and messaging

## [+] Software: firewalls

- Checking iptables kernel module [ FOUND ]
- Checking iptables policies of chains [ FOUND ]
- Checking for empty ruleset [ WARNING ]
- Checking for unused rules [ OK ]
- Checking host based firewall [ ACTIVE ]

### [+] **SSH Support**

```
-----
- Checking running SSH daemon [ FOUND ]
- Searching SSH configuration [ FOUND ]
- SSH option: AllowTcpForwarding [ SUGGESTION ]
- SSH option: ClientAliveCountMax [ SUGGESTION ]
- SSH option: ClientAliveInterval [ OK ]
- SSH option: Compression [ SUGGESTION ]
- SSH option: FingerprintHash [ OK ]
- SSH option: GatewayPorts [ OK ]
- SSH option: IgnoreRhosts [ OK ]
- SSH option: LoginGraceTime [ OK ]
- SSH option: LogLevel [ SUGGESTION ]
- SSH option: MaxAuthTries [ SUGGESTION ]
- SSH option: MaxSessions [ SUGGESTION ]
- SSH option: PermitRootLogin [ OK ]
- SSH option: PermitUserEnvironment [ OK ]
- SSH option: PermitTunnel [ OK ]
- SSH option: Port [ SUGGESTION ]
- SSH option: PrintLastLog [ OK ]
- SSH option: StrictModes [ OK ]
- SSH option: TCPKeepAlive [ SUGGESTION ]
- SSH option: UseDNS [ OK ]
- SSH option: VerifyReverseMapping [ NOT FOUND ]
- SSH option: X11Forwarding [ SUGGESTION ]
- SSH option: AllowAgentForwarding [ SUGGESTION ]
- SSH option: Protocol [ OK ]
- SSH option: UsePrivilegeSeparation [ SUGGESTION ]
- SSH option: AllowUsers [ NOT FOUND ]
- SSH option: AllowGroups [ NOT FOUND ]
```

### [+] **SNMP Support**

```
-----
- Checking running SNMP daemon [ NOT FOUND ]
```

### [+] **Databases**

```
-----
No database engines found
```

### [+] **LDAP Services**

```
-----
- Checking OpenLDAP instance [ NOT FOUND ]
```

### [+] **PHP**

```
-----
- Checking PHP [ NOT FOUND ]
```

## [+] Time and Synchronization

- NTP daemon found: ntpd [ FOUND ]
- NTP daemon found: systemd (timesyncd) [ FOUND ]
- Checking for a running NTP daemon or client [ OK ]
- Checking valid association ID's [ FOUND ]
- Checking high stratum ntp peers [ OK ]
- Checking unreliable ntp peers [ NONE ]
- Checking selected time source [ OK ]
- Checking time source candidates [ NONE ]
- Checking falsetickers [ OK ]
- Checking NTP version [ FOUND ]

## [+] Cryptography

- Checking for expired SSL certificates [0/2] [ NONE ]

## [+] Virtualization

## [+] Containers

## [+] Security frameworks

- Checking presence AppArmor [ FOUND ]
  - Checking AppArmor status [ ENABLED ]
- Checking presence SELinux [ NOT FOUND ]
- Checking presence TOMOYO Linux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ OK ]

## [+] Software: file integrity

- Checking file integrity tools
- Checking presence integrity tool [ NOT FOUND ]

## [+] Software: System tooling

- Checking automation tooling
- Automation tooling [ NOT FOUND ]



[+] **Home directories**

-----  
- Checking shell history files [ OK ]

[+] **Kernel Hardening**

-----  
- Comparing sysctl key pairs with scan profile  
- fs.protected\_hardlinks (exp: 1) [ OK ]  
- fs.protected\_symlinks (exp: 1) [ OK ]  
- fs.suid\_dumpable (exp: 0) [ DIFFERENT ]  
- kernel.core\_uses\_pid (exp: 1) [ DIFFERENT ]  
- kernel.ctrl-alt-del (exp: 0) [ OK ]  
- kernel.dmesg\_restrict (exp: 1) [ DIFFERENT ]  
- kernel.kptr\_restrict (exp: 2) [ DIFFERENT ]  
- kernel.randomize\_va\_space (exp: 2) [ OK ]  
- kernel.sysrq (exp: 0) [ DIFFERENT ]  
- kernel.yama.ptrace\_scope (exp: 1 2 3) [ OK ]  
- net.ipv4.conf.all.accept\_redirects (exp: 0) [ OK ]  
- net.ipv4.conf.all.accept\_source\_route (exp: 0) [ OK ]  
- net.ipv4.conf.all.bootp\_relay (exp: 0) [ OK ]  
- net.ipv4.conf.all.forwarding (exp: 0) [ OK ]  
- net.ipv4.conf.all.log\_martians (exp: 1) [ OK ]  
- net.ipv4.conf.all.mc\_forwarding (exp: 0) [ OK ]  
- net.ipv4.conf.all.proxy\_arp (exp: 0) [ OK ]  
- net.ipv4.conf.all.rp\_filter (exp: 1) [ OK ]  
- net.ipv4.conf.all.send\_redirects (exp: 0) [ OK ]  
- net.ipv4.conf.default.accept\_redirects (exp: 0) [ OK ]  
- net.ipv4.conf.default.accept\_source\_route (exp: 0) [ OK ]  
- net.ipv4.conf.default.log\_martians (exp: 1) [ OK ]  
- net.ipv4.icmp\_echo\_ignore\_broadcasts (exp: 1) [ OK ]  
- net.ipv4.icmp\_ignore\_bogus\_error\_responses (exp: 1) [ OK ]  
- net.ipv4.tcp\_syncookies (exp: 1) [ OK ]  
- net.ipv4.tcp\_timestamps (exp: 0 1) [ OK ]  
- net.ipv6.conf.all.accept\_redirects (exp: 0) [ DIFFERENT ]  
- net.ipv6.conf.all.accept\_source\_route (exp: 0) [ OK ]  
- net.ipv6.conf.default.accept\_redirects (exp: 0) [ DIFFERENT ]  
- net.ipv6.conf.default.accept\_source\_route (exp: 0) [ OK ]

[+] **Hardening**

-----  
- Installed compiler(s) [ NOT FOUND ]  
- Installed malware scanner [ NOT FOUND ]

[+] **Custom Tests**

-----  
- Running custom tests... [ NONE ]

```

-[ Lynis 2.7.5 Results ]-
.
Warnings (2):
-----
! Couldn't find 2 responsive nameservers [NETW-2705]
  https://cisofy.com/lynis/controls/NETW-2705/

! iptables module(s) loaded, but no rules active [FIRE-4512]
  https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (40):
-----
* This release is more than 4 months old. Consider upgrading [LYNIS]
  https://cisofy.com/lynis/controls/LYNIS/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  https://cisofy.com/lynis/controls/BOOT-5122/

* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
  https://cisofy.com/lynis/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/lynis/controls/AUTH-9286/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
  https://cisofy.com/lynis/controls/AUTH-9328/

* Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]
  https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
  https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
  https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
  https://cisofy.com/lynis/controls/FILE-6310/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
  https://cisofy.com/lynis/controls/STRG-1840/

```

#### Lynis security scan details:

```

Hardening index : 69 [##### ]
Tests performed : 236
Plugins enabled : 0

```

#### Components:

```

- Firewall           [V]
- Malware scanner    [X]

```

#### Lynis modules:

```

- Compliance status  [?]
- Security audit     [V]
- Vulnerability scan [V]

```

#### Files:

```

- Test and debug information : /var/log/lynis.log
- Report data                : /var/log/lynis-report.dat

```

#### Lynis 2.7.5

Auditing, system hardening, and compliance for UNIX-based systems  
(Linux, macOS, BSD, and others)

2007-2019, CISofy - <https://cisofy.com/lynis/>  
Enterprise support available (compliance, plugins, interface and tools)

## 2.3 Perform WebServer audit using Wapiti tool

Wapiti allows you to audit the security of your websites or web applications. It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data.

Using wapiti, we perform the audit for the installed apache webserver we have installed before.

Sudo apt-get install wapiti

```
root@instance-ubuntu:~# apt-get install wapiti
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  javascript-common libjs-jquery python-beautifulsoup
The following NEW packages will be installed:
  javascript-common libjs-jquery python-beautifulsoup wapiti
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 363 kB of archives.
After this operation, 1,744 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/main amd64 javascript-common all 11 [6,066 B]
Get:2 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/main amd64 libjs-jquery all 1.11.3+dfsg-4 [161 kB]
Get:3 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/universe amd64 python-beautifulsoup all 3.2.1-1 [34.6 kB]
Get:4 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial/universe amd64 wapiti all 2.3.0+dfsg-4 [161 kB]
Fetched 363 kB in 3s (121 kB/s)
Selecting previously unselected package javascript-common.
(Reading database ... 71699 files and directories currently installed.)
Preparing to unpack .../javascript-common_11_all.deb ...
Unpacking javascript-common (11) ...
Selecting previously unselected package libjs-jquery.
Preparing to unpack .../libjs-jquery_1.11.3+dfsg-4_all.deb ...
Unpacking libjs-jquery (1.11.3+dfsg-4) ...
Selecting previously unselected package python-beautifulsoup.
Preparing to unpack .../python-beautifulsoup_3.2.1-1_all.deb ...
Unpacking python-beautifulsoup (3.2.1-1) ...
Selecting previously unselected package wapiti.
Preparing to unpack .../wapiti_2.3.0+dfsg-4_all.deb ...
Unpacking wapiti (2.3.0+dfsg-4) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up javascript-common (11) ...
apache2_invoke: Enable configuration javascript-common
Setting up libjs-jquery (1.11.3+dfsg-4) ...
Setting up python-beautifulsoup (3.2.1-1) ...
Setting up wapiti (2.3.0+dfsg-4) ...
root@instance-ubuntu:~#
```

hostname -i

Start the following command using following command and locate the .html file in given folder

wapiti <http://10.140.0.3> -n 10 -b folder

```
root@instance-ubuntu:~# hostname -i
10.140.0.3
root@instance-ubuntu:~# wapiti http://10.140.0.3 -n 10 -b folder
Wapiti-2.3.0 (wapiti.sourceforge.net)

Note
-----
This scan has been saved in the file /home/zhamalkarunanayake/.wapiti/scans/10.140.0.3.xml
You can use it to perform attacks without scanning again the web site with the "-k" parameter
[*] Loading modules:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, m
od_permanentxss, mod_nikto

[+] Launching module exec

[+] Launching module file

[+] Launching module sql

[+] Launching module xss

[+] Launching module blindsql

[+] Launching module permanentxss

Report
-----
A report has been generated in the file /home/zhamalkarunanayake/.wapiti/generated_report
Open /home/zhamalkarunanayake/.wapiti/generated_report/index.html with a browser to see this repor
t.
root@instance-ubuntu:~#
```

## 2.3.1 Audit results

### Wapiti vulnerability report for http://10.140.0.3

**Date of the scan: Tue, 05 May 2020 19:00:51 +0000.**

**Scope of the web scanner : folder**

---

#### Summary

Category	Number of vulnerabilities found
Cross Site Scripting	0
Htaccess Bypass	0
Backup file	0
SQL Injection	0
Blind SQL Injection	0
File Handling	0
Potentially dangerous file	0
CRLF Injection	0
Commands execution	0
Resource consumption	0
Internal Server Error	0

## 2.4 Perform Server audit using OpenSCAP tool

install the OpenSCAP base (which is a command line-only tool).

```
sudo apt-get install libopenscap8 -y
```

Next download the Ubuntu-specific profile the OpenSCAP command will use for the audit. On the off-chance your Ubuntu machine doesn't include the wget command, install it with:

```
sudo apt-get install wget -y
```

Download the necessary OVAL definitions with the command:

```
wget https://people.canonical.com/~ubuntu-security/oval/com.ubuntu.xenial.cve.oval.xml
```

```
root@instance-ubuntu:~# sudo apt-get install libopenscap8 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package -y
root@instance-ubuntu:~# sudo apt-get install wget -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package -y
root@instance-ubuntu:~# wget https://people.canonical.com/~ubuntu-security/oval/com.ubuntu.xenial.cve.oval.xml
--2020-05-05 19:04:34-- https://people.canonical.com/~ubuntu-security/oval/com.ubuntu.xenial.cve.oval.xml
Resolving people.canonical.com (people.canonical.com)... 91.189.89.62
Connecting to people.canonical.com (people.canonical.com)[91.189.89.62]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2010778 (1.9M) [application/x-bzip2]
Saving to: 'com.ubuntu.xenial.cve.oval.xml'

com.ubuntu.xenial.cve.ov 100%[=====>] 1.92M 318KB/s in 8.4s

2020-05-05 19:04:44 (234 KB/s) - 'com.ubuntu.xenial.cve.oval.xml' saved [2010778/2010778]
```

Run the audit

Now that you have the profile in place, it's time to run the audit. issue the command:

```
oscap oval eval --results /tmp/oscap_results.xml --report /tmp/oscap_report.html
com.ubuntu.xenial.cve.oval.xml
```

The scan will output its results into two files, an .xml and .html file. We want to view the .html file. To do that, issue the command:

```
sudo cp /tmp/oscap_report.html /var/www/html/
```



```

root@instance-ubuntu:~# apt install libopenscap8
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  libopenscap8
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,329 kB of archives.
After this operation, 59.8 MB of additional disk space will be used.
Get:1 http://asia-east1.gce.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 libopenscap8 a
md64 1.2.8-1ubuntu0.2 [2,329 kB]
Fetched 2,329 kB in 0s (9,023 kB/s)
Selecting previously unselected package libopenscap8.
(Reading database ... 71842 files and directories currently installed.)
Preparing to unpack .../libopenscap8_1.2.8-1ubuntu0.2_amd64.deb ...
Unpacking libopenscap8 (1.2.8-1ubuntu0.2) ...
Processing triggers for libc-bin (2.23-0ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libopenscap8 (1.2.8-1ubuntu0.2) ...
Processing triggers for libc-bin (2.23-0ubuntu1) ...
root@instance-ubuntu:~#
root@instance-ubuntu:~# oscap oval eval --results /tmp/oscap_results.xml --report /tmp/oscap_report.html com.ubuntu.xenial.cve.oval.xml

```

## 2.4.1 Audit results

OVAL Results Generator Information					OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time	Schema Version	Product Name	Product Version	Date	Time
5.11.1	cpe:/a:open-scap:oscap	1.2.8	2020-05-05	19:06:24	5.11.1	Canonical CVE OVAL Generator	1.1	2020-05-05	19:03:33
#X	#✓	#Error	#Unknown	#Other	#Definitions	#Tests	#Objects	#States	#Variables
251	14937	0	0	1	15189 Total 10 1 0 0 15188	4976	1758	3278	923

System Information	
Host Name	instance-ubuntu
Operating System	Linux
Operating System Version	#65-Ubuntu SMP Thu Apr 9 05:37:44 UTC 2020
Architecture	x86_64
Interfaces	Interface Name: lo
	IP Address: 127.0.0.1
	MAC Address: 00:00:00:00:00:00
	Interface Name: ens4
	IP Address: 10.140.0.3
	MAC Address: 42:01:0A:8C:00:03
	Interface Name: lo
	IP Address: ::1
	MAC Address: 00:00:00:00:00:00
	Interface Name: ens4
	IP Address: fe80::4001:aff:fe8c:3
	MAC Address: 42:01:0A:8C:00:03

OVAL System Characteristics Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.11.1	cpe:/a:open-scap:oscap	1.1	2020-05-05	19:06:24

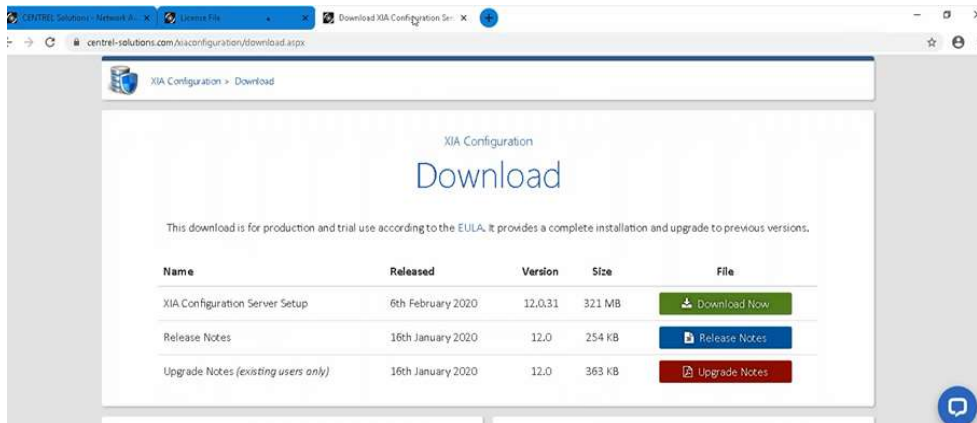
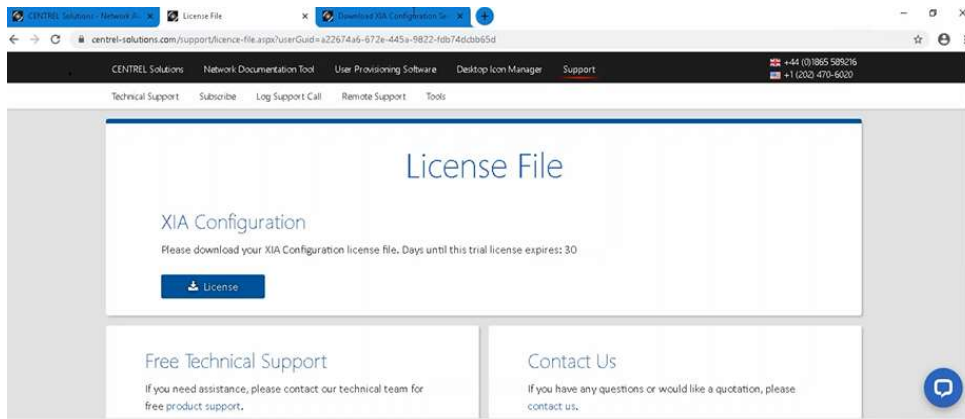
OVAL Definition Results				
<input checked="" type="checkbox"/> X	<input checked="" type="checkbox"/> ✓	<input checked="" type="checkbox"/> Error	<input checked="" type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Other
ID	Result	Class	Reference ID	Title
oval.com.ubuntu.xenial:def:202089910000000	true	vulnerability	[CVE-2020-8991]	CVE-2020-8991 on Ubuntu 16.04 LTS (xenial) - low.
oval.com.ubuntu.xenial:def:202086490000000	true	vulnerability	[CVE-2020-8649]	CVE-2020-8649 on Ubuntu 16.04 LTS (xenial) - medium.
oval.com.ubuntu.xenial:def:202086470000000	true	vulnerability	[CVE-2020-8647]	CVE-2020-8647 on Ubuntu 16.04 LTS (xenial) - medium.
oval.com.ubuntu.xenial:def:202086320000000	true	vulnerability	[CVE-2020-8632]	CVE-2020-8632 on Ubuntu 16.04 LTS (xenial) - low.
oval.com.ubuntu.xenial:def:202086310000000	true	vulnerability	[CVE-2020-8631]	CVE-2020-8631 on Ubuntu 16.04 LTS (xenial) - low.
oval.com.ubuntu.xenial:def:202080060000000	true	vulnerability	[CVE-2020-8006]	CVE-2020-8006 on Ubuntu 16.04 LTS (xenial) - medium.



### 3. Windows Server Audits

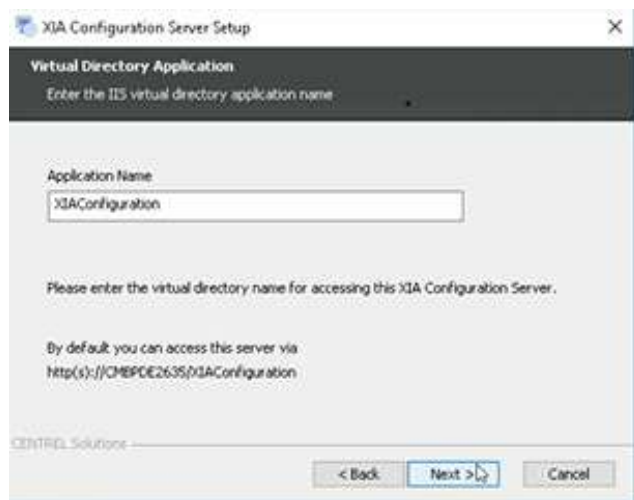
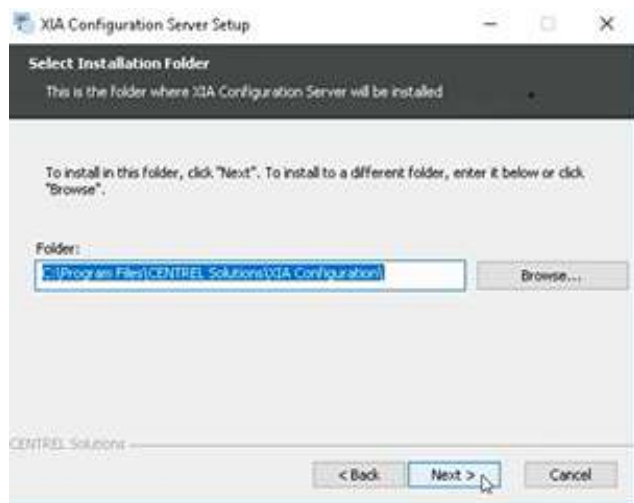
#### 3.1 Perform Server audit using XIA Configuration tool

Download the XIA configuration File by requesting license from the site they are provided

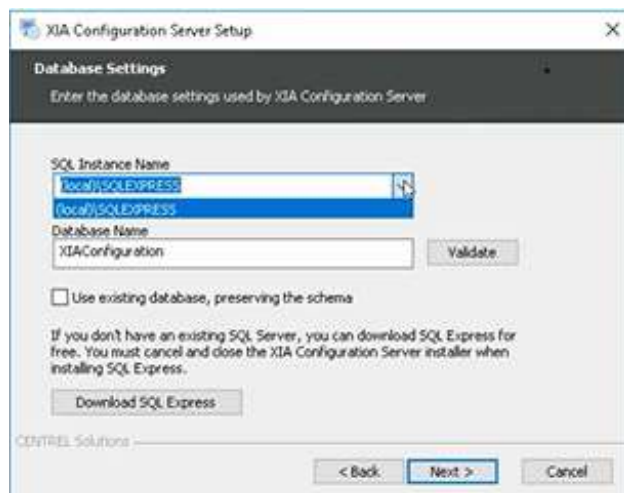


Run the .exe file

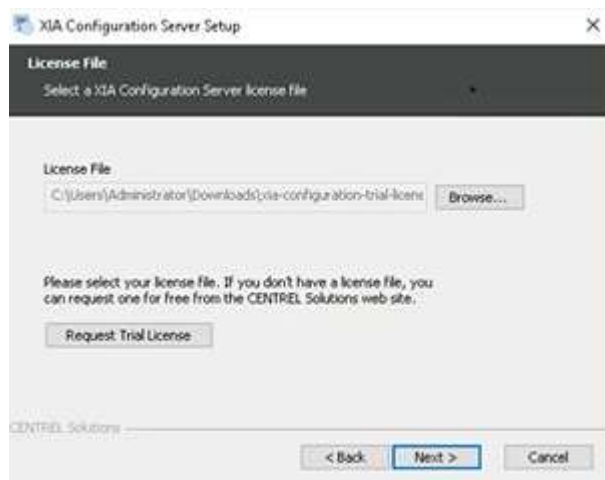




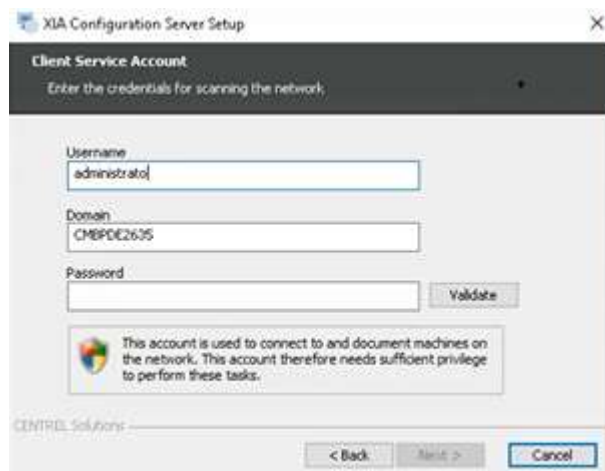
Continue with the screenshots provide the enter and sql instance for database settings.



Enter the license file provided and in the next step , provide server administrative username and password.



The screenshot shows the 'License File' step of the XIA Configuration Server Setup wizard. The title bar reads 'XIA Configuration Server Setup'. The main heading is 'License File' with the instruction 'Select a XIA Configuration Server license file'. Below this, there is a text box containing the file path 'C:\Users\Administrator\Downloads\xia-configuration-trial-license' and a 'Browse...' button. A note states: 'Please select your license file. If you don't have a license file, you can request one for free from the CENTREL Solutions web site.' Below the note is a 'Request Trial License' button. At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. The CENTREL Solutions logo is in the bottom left corner.



The screenshot shows the 'Client Service Account' step of the XIA Configuration Server Setup wizard. The title bar reads 'XIA Configuration Server Setup'. The main heading is 'Client Service Account' with the instruction 'Enter the credentials for scanning the network'. Below this, there are three input fields: 'Username' with the value 'administrator', 'Domain' with the value 'CHRPDC2635', and 'Password'. A 'Validate' button is to the right of the password field. A note with a Windows logo icon states: 'This account is used to connect to and document machines on the network. This account therefore needs sufficient privilege to perform these tasks.' At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'. The CENTREL Solutions logo is in the bottom left corner.



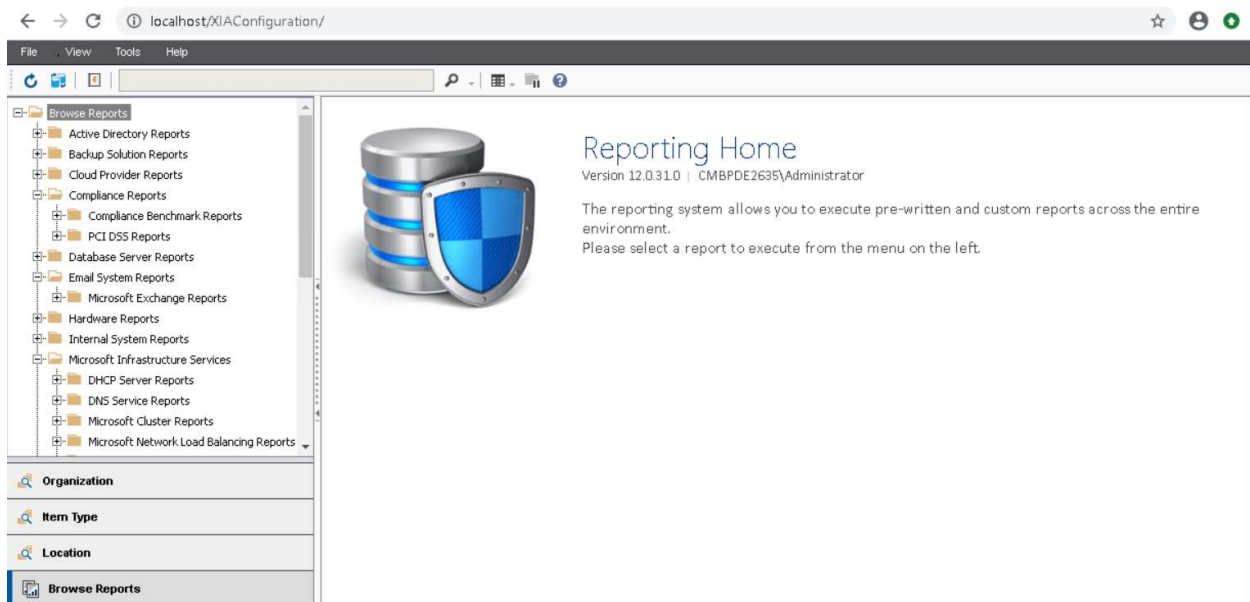
The screenshot shows the 'Installing XIA Configuration Server' step of the XIA Configuration Server Setup wizard. The title bar reads 'XIA Configuration Server Setup'. The main heading is 'Installing XIA Configuration Server'. Below this, a message states: 'Please wait while the Setup Wizard installs XIA Configuration Server. This may take several minutes.' Below the message, the status is shown as 'Status: Configuring Windows features.' with a green progress bar. At the bottom, there are navigation buttons: '< Back', 'Next', and 'Cancel'. The CENTREL Solutions logo is in the bottom left corner.



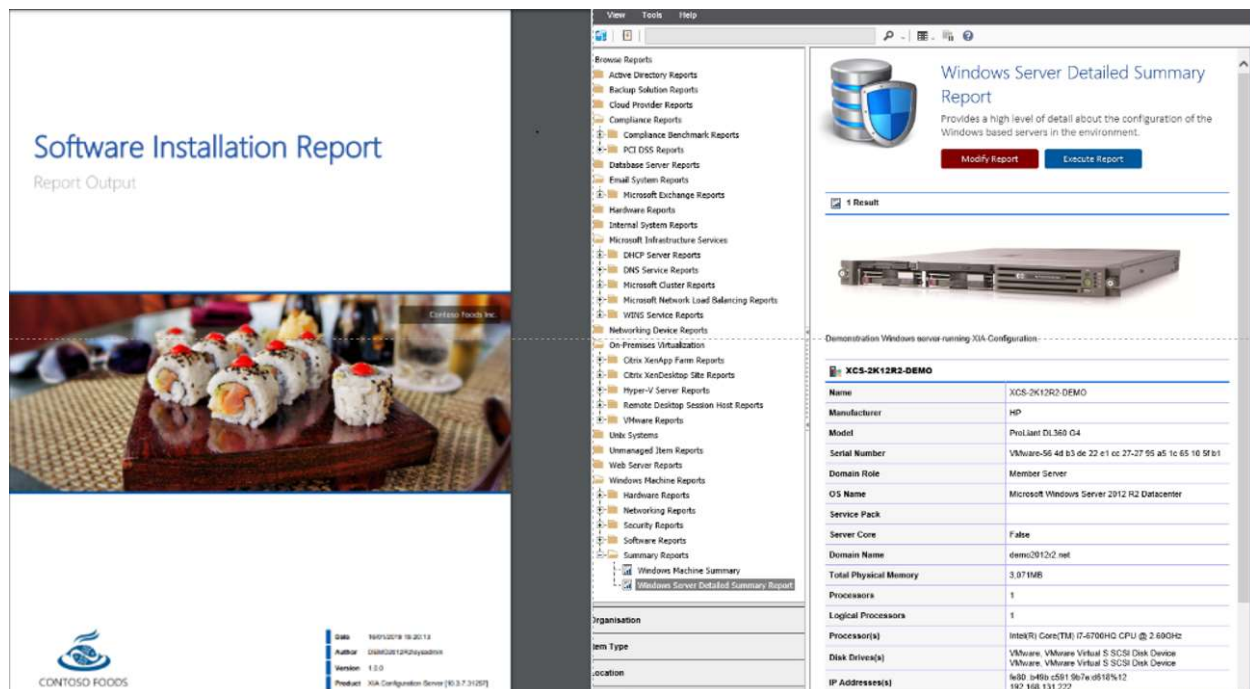
After finishing the installation view the server and execute essential or specific reports

### 3.1.1 Audit results

Here you can generate .csv and .pdf files along with online localhost.



[illegible]



## References

J. Wallen, "How to perform security audits on Ubuntu server with OpenSCAP," *TechRepublic*, 24-Jul-2019. [Online]. Available: <https://www.techrepublic.com/article/how-to-perform-security-audits-on-ubuntu-server-with-openscap/>. [Accessed: May-2020].

DigitalOcean, "How To Configure the Apache Web Server on an Ubuntu or Debian VPS," *DigitalOcean*, 18-Sep-2019. [Online]. Available: <https://www.digitalocean.com/community/tutorials/how-to-configure-the-apache-web-server-on-an-ubuntu-or-debian-vps>. [Accessed: May-2020].

DigitalOcean, "How to Perform Security Audits With Lynis on Ubuntu 16.04," *DigitalOcean*, 30-Mar-2020. [Online]. Available: <https://www.digitalocean.com/community/tutorials/how-to-perform-security-audits-with-lynis-on-ubuntu-16-04#step-1---installing-lynis-on-your-server>. [Accessed: May-2020].

"XIA Configuration - Network Documentation Tool - IT Audit Software," *CENTREL Solutions*. [Online]. Available: <https://www.centrel-solutions.com/xiaconfiguration/network-documentation-tool.aspx>. [Accessed: May-2020].