How to securely isolate and execute Lynis from Kali Linux

Version 0.1, Last Updated: 11 Oct 2020

This site is dedicated to sharing information about the practice, ideas, concepts and patterns regarding computer security.

Table of Contents

1. Introduction

The motivation behind this paper is to explore using the tool Lynis that comes with Kali Linux.

What is this tool:

"Lynis is an open source security auditing tool. Its main goal is to audit and harden Unix and Linux based systems. It scans the system by performing many security control checks. Examples include searching for installed software and determine possible configuration flaws.

Many tests are part of common security guidelines and standards, with on top additional security tests. After the scan a report will be displayed with all discovered findings. To provide you with initial guidance, a link is shared to the related Lynis control." source: Kali Linux

"Since Lynis is flexible, it is used for several different purposes. Typical use cases for Lynis include: - Security auditing - Compliance testing (e.g. PCI, HIPAA, SOx) - Penetration testing - Vulnerability detection - System hardening " ***source***: Lynis

What does Lynus run on?

"Lynis runs on almost all UNIX-based systems and versions, including: - AIX - FreeBSD - HP-UX - Linux - macOS - NetBSD - NixOS - OpenBSD - Solaris - and others

It even runs on systems like the Raspberry Pi, IoT devices, and QNAP storage devices." ***source***: Lynis

"Lynis scanning is modular and opportunistic. This means it will only use and test the components that it can find, such as the available system tools and its libraries. The benefit is that no installation of other tools is needed, so you can keep your systems clean.

By using this scanning method, the tool can run with almost no dependencies. Also, the more components it discovers, the more extensive the audit will be. In other words: Lynis will always perform scans that are tailored to your system. No audit will be the same!" ***source***: Lynis

Audit Steps:

"This is what happens during a typical scan with Lynis:

- Initialization
- Perform basic checks, such as file ownership
- Determine operating system and tools
- Search for available software components
- Check latest Lynis version
- Run enabled plugins
- Run security tests per category
- Perform execution of your custom tests (optional)
- Report status of security scan

Besides the report and information displayed on screen, all technical details about the scan are stored in a log file (lynis.log). Findings like warnings and suggestions are stored in a separate report file (lynis-report.dat). " ***source***: Lynis

Supported Standards:

"Other tools typically use the same data files to perform tests. Lynis is not limited to a specific Linux distribution, therefore it uses the knowledge of 10+ years from a wide range of sources. It may help you to automate or test against security best practices from sources like: - CIS benchmarks - NIST - NSA - OpenSCAP data - Vendor guides and recommendations (e.g. Debian Gentoo, Red Hat) " ***source***: Lynis

After discovering all of these facts, I am really excited to get started with Lynis.

2. Requirements

2.1. Writing Conventions

If you see the following $ symbol on a command line to execute, what that means is that the command is executed as a regular user; meaning an account that does not have administrative privileges. Ignore the leading $ and execute the rest of the command.

```
$ command to execute as a regular user
```

If you see a command line lead with the # symbol, then that means that the command is executed as the root user. This implies you need to elevate to the root user before running the command, e.g. with: `sudo su - root`.

```
# command to execute as the root user
```

2.2. VirtualBox

Go to: https://www.virtualbox.org/wiki/Downloads and download VirtualBox.

The author is running on Ubuntu 18.04, so following to this URL: https://www.virtualbox.org/wiki/Linux_Downloads

For Ubuntu, double click on the .deb file, i.e. virtualbox-5.2_5.2.0-118431-Ubuntu-zesty_amd64.deb, and install VirtualBox on your local workstation.

2.2.1. Clean VirtualBox Networking

This section is here in case you already had virtualbox installed from before. The intent is to clean up the previous networking. If you do not need to do this, skip to Add VirtualBox Networking

Run these two commands from a Terminal:

```
$ VBoxManage list natnetworks
$ VBoxManage list dhcpservers
```

Output (example):

```
NetworkName:    192.168.139-NAT
IP:             192.168.139.1
Network:        192.168.139.0/24
IPv6 Enabled:   No
IPv6 Prefix:    fd17:625c:f037:2::/64
DHCP Enabled:   Yes
Enabled:        Yes
loopback mappings (ipv4)
        127.0.0.1=2


NetworkName:    192.168.139-NAT
Dhcpd IP:       192.168.139.3
LowerIPAddress: 192.168.139.101
UpperIPAddress: 192.168.139.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None

NetworkName:    HostInterfaceNetworking-vboxnet0
Dhcpd IP:       172.20.0.3
LowerIPAddress: 172.20.0.101
UpperIPAddress: 172.20.0.254
NetworkMask:    255.255.255.0
Enabled:        Yes
Global Configuration:
    minLeaseTime:     default
    defaultLeaseTime: default
    maxLeaseTime:     default
    Forced options:   None
    Suppressed opts.: None
        1/legacy: 255.255.255.0
Groups:               None
Individual Configs:   None
```

Now, delete ALL of the pre-installed VirtualBox networks (one at a time following the syntax below):

```
VBoxManage natnetwork remove --netname <NetworkName_from_above>
VBoxManage natnetwork remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

Now, delete ALL of the pre-installed DHCP services:

```
VBoxManage dhcpserver remove --netname <DHCP_Server_NetworkName_from_above>
VBoxManage dhcpserver remove --netname 192.168.139-NAT
```

Repeat as many times as necessary to delete all of them.

2.2.2. Add VirtualBox Networking

Now, add the new VirtualBox networks so the Kali Linux guides work.

```
VBoxManage natnetwork add \
    --netname 192.168.139-NAT \
    --network "192.168.139.0/24" \
    --enable --dhcp on

VBoxManage dhcpserver add \
    --netname 192.168.139-NAT \
    --ip 192.168.139.3 \
    --lowerip 192.168.139.101 \
    --upperip 192.168.139.254 \
    --netmask 255.255.255.0 \
    --enable

VBoxManage hostonlyif create

VBoxManage hostonlyif ipconfig vboxnet0 \
    --ip 172.20.0.1 \
    --netmask 255.255.255.0

VBoxManage dhcpserver add \
    --ifname vboxnet0 \
    --ip 172.20.0.3 \
    --lowerip 172.20.0.101 \
    --upperip 172.20.0.254 \
    --netmask 255.255.255.0

VBoxManage dhcpserver modify \
    --ifname vboxnet0 \
    --enable
```

VirtualBox install complete.

2.3. Vagrant

Go to: https://www.vagrantup.com/downloads.html, follow the appropriate link to your OS and 32 or 64 bit version representing your local workstation. Download.

For Ubuntu, double click on the .deb file, i.e. vagrant_2.0.1_x86_64.deb, and install Vagrant on your local system.

2.4. Kali Linux and Damn Vulnerable Web Application (DVWA)

The author highly recommends to create a directory structure that is easy to navigate and find your code. As an example, you could use something similar to:

```
${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Go ahead and make this structure with the following command (inside a Terminal):

```
$ mkdir -p ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

2.4.1. Vagrantfile

Inside of the kali-linux-vm directory, populate a new file with the exact name, “Vagrantfile”. Case matters, uppercase the “V”. This file will contain both virtual machines for Kali Linux as well as setting up the DVWA virtual machine.

Aggregating both virtual machines into one file has saved the author a lot of time. The coolness here is setting up the variables at the top of the Vagrantfile mimicing shell scripting inside of a virtual machine (passed in with provision: shell). I tested using: `apt-get update && apt-get upgrade -y`, but opted to take it out since it took over 45 minutes on my slower (old) hardware. See comment about downloading this file immediately preceding the code block.

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

$os_update = <<SCRIPT
apt-get update
SCRIPT

VAGRANTFILE_API_VERSION = "2"


Vagrant.configure(VAGRANTFILE_API_VERSION) do |config|
    config.vm.define "kali-linux-vagrant" do |conf|
        conf.vm.box = "kalilinux/rolling"

        # For Linux systems with the Wireless network, uncomment the line:
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)", auto_config: true

        conf.vm.hostname = "kali-linux-vagrant"
        conf.vm.provider "virtualbox" do |vb|
            vb.gui = true
            vb.memory = "4096"
            vb.cpus = "2"
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Debian_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
    end

    config.vm.define "dvwa-vagrant" do |conf|

        conf.vm.box = "ubuntu/xenial64"

        conf.vm.hostname = "dvwa-vagrant"

        # For Linux systems with the Wireless network, uncomment the line:
        conf.vm.network "public_network", bridge: "wlo1", auto_config: true

        # For macbook/OSx systems, uncomment the line and comment out the Linux Wireless network:
        #conf.vm.network "public_network", bridge: "en0: Wi-Fi (AirPort)", auto_config: true

        config.vm.network "forwarded_port", guest: 80, host: 8080, auto_correct: true
        config.vm.network "forwarded_port", guest: 3306, host: 3306, auto_correct: true

        conf.vm.provider "virtualbox" do |vb|
            vb.memory = "1024"
            vb.cpus = "2"
            vb.gui = false
            vb.customize ["modifyvm", :id, "--vram", "32"]
            vb.customize ["modifyvm", :id, "--accelerate3d", "off"]
            vb.customize ["modifyvm", :id, "--ostype", "Ubuntu_64"]
            vb.customize ["modifyvm", :id, "--boot1", "dvd"]
            vb.customize ["modifyvm", :id, "--boot2", "disk"]
            vb.customize ["modifyvm", :id, "--audio", "none"]
            vb.customize ["modifyvm", :id, "--clipboard", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--draganddrop", "hosttoguest"]
            vb.customize ["modifyvm", :id, "--paravirtprovider", "kvm"]
        end
        conf.vm.provision "shell", inline: $os_update
        conf.vm.provision :shell, path: "bootstrap.sh"
    end
end
```

Save and write this file.

You can also download from:

```
$ curl -o Vagrantfile  http://securityhardening.com/files/Vagrantfile_20200928.txt
```

2.4.2. bootstrap.sh

Inside of the kali-linux-vm directory, populate a new file with the exact name, `bootstrap.sh`. Case matters, all lowercase. See comment about downloading this file immediately preceding the code block. `bootstrap.sh` (include the shebang in your file: the first line with `#!/usr/bin/env bash`):

```
#!/usr/bin/env bash
PHP_FPM_PATH_INI='/etc/php/7.0/fpm/php.ini'
PHP_FPM_POOL_CONF='/etc/php/7.0/fpm/pool.d/www.conf'
MYSQL_ROOT_PW='Assword12345'
MYSQL_dvwa_user='dvwa'
MYSQL_dvwa_password='sunshine'
DVWA_admin_password='admin'
recaptcha_public_key='u8392ihj32kl8hujalkshuil32'
recaptcha_private_key='89ry8932873832lih32ilj32'


install_base() {
    add-apt-repository -y ppa:nginx/stable
    sudo apt-get update
    sudo apt-get dist-upgrade -y
    sudo apt-get install -y \
        nginx \
        mariadb-server \
        mariadb-client \
        php \
        php-common \
        php-cgi \
        php-fpm \
        php-gd \
        php-cli \
        php-pear \
        php-mcrypt \
        php-mysql \
        php-gd \
        git \
        vim
}

config_mysql(){
    mysqladmin -u root password "${MYSQL_ROOT_PW}"
## Config the mysql config file for root so it doesn't prompt for password.
## Also sets pw in plain text for easy access.
## Don't forget to change the password here!!

cat <<EOF > /root/.my.cnf
[client]
user="root"
password="${MYSQL_ROOT_PW}"
EOF
    mysql -BNe "drop database if exists dvwa;"
    mysql -BNe "CREATE DATABASE dvwa;"
    mysql -BNe "GRANT ALL ON *.* TO '"${MYSQL_dvwa_user}"'@'localhost' IDENTIFIED BY '"${MYSQL_dvwa_password}"';"

    systemctl enable mysql
    systemctl restart mysql
    sleep 2
}


config_php(){
    ## Config PHP FPM INI to disable some security settings:

    sed -i 's/^;cgi.fix_pathinfo.*$/cgi.fix_pathinfo = 0/g' ${PHP_FPM_PATH_INI}
    sed -i 's/allow_url_include = Off/allow_url_include = On/g' ${PHP_FPM_PATH_INI}
```

```
    sed -i 's/allow_url_fopen = Off/allow_url_fopen = On/g' ${PHP_FPM_PATH_INI}
    sed -i 's/safe_mode = On/safe_mode = Off/g' ${PHP_FPM_PATH_INI}
    echo "magic_quotes_gpc = Off" >> ${PHP_FPM_PATH_INI}
    sed -i 's/display_errors = Off/display_errors = On/g' ${PHP_FPM_PATH_INI}

    ## explicitly set pool options
    ## (these are defaults in ubuntu 16.04 so i'm commenting them out.
    ## If they are not defaults for you try uncommenting these)
    #sed -i 's/^;security.limit_extensions.*$/security.limit_extensions = \
    #.php .php3 .php4 .php5 .php7/g' /etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.owner.*$/listen.owner = www-data/g' /etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^listen.group.*$/listen.group = www-data/g' /etc/php/7.0/fpm/pool.d/www.conf
    #sed -i 's/^;listen.mode.*$/listen.mode = 0660/g' /etc/php/7.0/fpm/pool.d/www.conf


    systemctl restart php7.0-fpm
}


config_nginx(){

cat << 'EOF' > /etc/nginx/sites-enabled/default
server
{
    listen  80;
    root /var/www/html;
    index index.php index.html index.htm;
    #server_name localhost
    location "/"
    {
        index index.php index.html index.htm;
        #try_files $uri $uri/ =404;
    }

    location ~ \.php$
    {
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $request_filename;
    }
}
EOF

    systemctl restart nginx
}


install_dvwa(){

    if [[ ! -d "/var/www/html" ]];
    then
          mkdir -p /var/www;
          ln -s /usr/share/nginx/html /var/www/html;
          chown -R www-data. /var/www/html;
    fi

    cd /var/www/html
    rm -rf /var/www/html/.[!.]*
    rm -rf /var/www/html/*
    git clone https://github.com/ethicalhack3r/DVWA.git ./
    chown -R www-data. ./
    cp config/config.inc.php.dist config/config.inc.php

    ### chmod uploads and log file to be writable by nobody
    chmod 777 ./hackable/uploads/
    chmod 777 ./external/phpids/0.6/lib/IDS/tmp/phpids_log.txt

    ## change the values in the config to match our setup (these are what you need to update!
    sed -i '/db_user/ s/root/'${MYSQL_dvwa_user}'/' /var/www/html/config/config.inc.php
    sed -i '/db_password/ s/p@ssw0rd/'${MYSQL_dvwa_password}'/' /var/www/html/config/config.inc.php
    sed -i "/recaptcha_public_key/ s/''/'"${recaptcha_public_key}"'/" /var/www/html/config/config.inc.php
    sed -i "/recaptcha_private_key/ s/''/'"${recaptcha_private_key}"'/" /var/www/html/config/config.inc.php

}
```

```
update_mysql_user_pws(){
## The mysql passwords are set via /usr/share/nginx/html/dvwa/includes/DBMS/MySQL.php.
#  If you edit this every time they are reset it will reset to those.
#  Otherwise you can do a sql update statement to update them all (they are just md5's of the string.
#  The issue is the users table doesn't get created until you click that button T_T to init.

#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user = 'admin';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user = 'gordonb';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user = '1337';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user = 'pablo';"
#mysql -BNe "UPDATE dvwa.users SET password = md5('YOUR_MYSQL_PW_HERE') WHERE user = 'smithy';"

sed -i '/admin/ s/password/'${DVWA_admin_password}'/g'  /var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/gordonb/ s/abc123/'${DVWA_admin_password}'/g'  /var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/1337/ s/charley/'${DVWA_admin_password}'/g'  /var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/pablo/ s/letmein/'${DVWA_admin_password}'/g'  /var/www/html/dvwa/includes/DBMS/MySQL.php
sed -i '/smithy/ s/password/'${DVWA_admin_password}'/g'  /var/www/html/dvwa/includes/DBMS/MySQL.php
}


install_base
config_mysql
install_dvwa
update_mysql_user_pws
config_php
config_nginx
```

Save and write this file.

If you have issues with copying and pasting the above file because code blocks in PDFs always copy correctly [NOT!], you could use curl, i.e. Make sure the bootstrap.sh file ends up in the same directory as the Vagrantfile.

```
$ curl -o bootstrap.sh  http://securityhardening.com/files/bootstrap_sh_20200928.txt
```

From a Terminal, change directory to:

```
$ cd ${HOME}/Source_Code/Education/vagrant-machines/kali-linux-vm/
```

Then run (inside the directory kali-linux-vm):

```
$ vagrant up
```

This will download the appropriate images and start the virtual machines. Once running, through the VirtuaBox GUI, login as root. Password is “toor”, root backwards. Edit the following file: `/etc/ssh/sshd_config`

And change the line: `#PermitRootLogin prothibit-password` To: `PermitRootLogin yes` Meaning strip the comment out on the beginning of the line and alter `prohibit-password` to `yes`.

Then restart the ssh daemon:

```
# kill -HUP $(pgrep sshd)
```

Notice, you are on a Bridged adapter, this will open the instance to allow root to ssh in with the most unsecure password in the world. Only make this change (allowing root to login via SSH) if you require root SSH access. You can change the root user’s password, which is highly recommended.

For the DVWA instance, I would first run 'vagrant status' to capture the name that vagrant is using for the running instance.

```
# vagrant status
```

Choose

```
Current machine states:
kali-linux-vagrant running (virtualbox)
dvwa-vagrant running (virtualbox)
```

This environment represents multiple VMs. The VMs are all listed above with their current state. For more information about a specific VM, run `vagrant status NAME`.

From there, log into the DVWA instance with:

```
$ vagrant ssh dvwa-vagrant
```

And then get the current IP address.

```
$ ip a
```

Choose the second network adapter, it should look like:

```
ubuntu@dvwa:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:53:17:3c:de:80 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::53:17ff:fe3c:de80/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f0:77:2d brd ff:ff:ff:ff:ff:ff
    inet 172.20.156.76/24 brd 172.20.156.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef0:772d/64 scope link
        valid_lft forever preferred_lft forever
```

The test network used for this paper uses 172.20.156.0/24 as the network range [shown here in section 3]. Therefore, the adapter, enp0s8 is what he is looking for. The IP to use as a target is 172.20.156.76. Write down your value.

3. Lynis

On your Host system, running VirtualBox and Vagrant, open a teminal and run:

```
$ vagrant status
```

Then SSH into the Kali Linux namespace

```
$ vagrant ssh kali-linux-vagrant
```

Elevate to the root user (inside the Virtual Machine for Kali Linux)

```
$ sudo su -
```

Install lynis (inside the Virtual Machine for Kali Linux)

```
# apt-get install -y lynis
```

What options are available with lynus

```
################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                  : Perform local security scan
        audit system remote <host>    : Remote security scan
        audit dockerfile <file>       : Analyze Dockerfile

    show
        show                          : Show all commands
        show version                  : Show Lynis version
        show help                     : Show help

    update
        update info                   : Show update details


  Options:

    Alternative system audit modes
    --forensics                       : Perform forensics on a running or mounted system
    --pentest                         : Non-privileged, show points of interest for pentesting

    Layout options
    --no-colors                       : Don't use colors in output
    --quiet (-q)                      : No output
    --reverse-colors                  : Optimize color display for light backgrounds
    --reverse-colours                 : Optimize colour display for light backgrounds

    Misc options
    --debug                           : Debug logging to screen
    --no-log                          : Don't create a log file
    --profile <profile>               : Scan the system with the given profile file
    --view-manpage (--man)            : View man page
    --verbose                         : Show more details on screen
    --version (-V)                    : Display version number and quit
    --wait                            : Wait between a set of tests

    Enterprise options
    --plugindir <path>                : Define path of available plugins
    --upload                          : Upload data to central node

    More options available. Run '/usr/sbin/lynis show options', or use the man page.
```

Let's explore what is available

```
lynis show
```

Output:

```
    lynis show categories
    lynis show changelog
    lynis show commands
    lynis show dbdir
    lynis show details
    lynis show environment
    lynis show eol
    lynis show groups
    lynis show help
    lynis show hostids
    lynis show includedir
    lynis show language
    lynis show license
    lynis show logfile
    lynis show man
    lynis show options
    lynis show os
    lynis show pidfile
    lynis show plugindir
    lynis show profiles
    lynis show release
    lynis show releasedate
    lynis show report
    lynis show settings
    lynis show tests
    lynis show version
    lynis show workdir
```

That is a lot of stuff this tool can do. I recommend exploring each of those to understand the tool better for the reader.

To run the tool against the Kali Linux distribution, run this command:

```
# lynis audit system -Q
```

3.1. Lynis output on Kali Linux VM

Output:

```
################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------

================================================================

  Exception found!

  Function/test:  [OS Detection]
  Message:        Unknown OS found in /etc/os-release

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (/usr/sbin/lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!
```

```
================================================================

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

  ---------------------------------------------------
  Program version:           3.0.0
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  kali-rolling
  Kernel version:            5.9.0
  Hardware platform:         x86_64
  Hostname:                  kali-linux-vagrant
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                        [ FOUND ]
    - Checking /sbin...                                       [ FOUND ]
    - Checking /usr/bin...                                    [ FOUND ]
    - Checking /usr/sbin...                                   [ FOUND ]
    - Checking /usr/local/bin...                              [ FOUND ]
    - Checking /usr/local/sbin...                             [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):

  [WARNING]: Test DEB-0001 had a long execution: 11.806991 seconds

      - libpam-tmpdir                                         [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda1                               [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                            [ Not Installed ]
    - apt-listchanges                                         [ Installed and enabled for apt ]
    - needrestart                                             [ Not Installed ]
    - debsecan                                                [ Not Installed ]
    - debsums                                                 [ Not Installed ]
    - fail2ban                                                [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - 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 20 enabled services
```

```
  - Check startup files (permissions)                       [ OK ]
  - Running 'systemd-analyze security'
       - ModemManager.service:                              [ MEDIUM ]
       - NetworkManager.service:                            [ EXPOSED ]
       - accounts-daemon.service:                           [ UNSAFE ]
       - colord.service:                                    [ EXPOSED ]
       - cron.service:                                      [ UNSAFE ]
       - dbus.service:                                      [ UNSAFE ]
       - dm-event.service:                                  [ UNSAFE ]
       - emergency.service:                                 [ UNSAFE ]
       - gdm.service:                                       [ UNSAFE ]
       - getty@tty1.service:                                [ UNSAFE ]
       - haveged.service:                                   [ OK ]
       - lvm2-lvmpolld.service:                             [ UNSAFE ]
       - lynis.service:                                     [ UNSAFE ]
       - packagekit.service:                                [ UNSAFE ]
       - pcscd.service:                                     [ UNSAFE ]
       - plymouth-start.service:                            [ UNSAFE ]
       - polkit.service:                                    [ UNSAFE ]
       - rc-local.service:                                  [ UNSAFE ]
       - rescue.service:                                    [ UNSAFE ]
       - rpcbind.service:                                   [ UNSAFE ]
       - rsync.service:                                     [ EXPOSED ]
       - rsyslog.service:                                   [ UNSAFE ]
       - rtkit-daemon.service:                              [ MEDIUM ]
       - smartmontools.service:                             [ UNSAFE ]
       - ssh.service:                                       [ UNSAFE ]
       - stunnel4.service:                                  [ UNSAFE ]
       - systemd-ask-password-console.service:              [ UNSAFE ]
       - systemd-ask-password-plymouth.service:             [ UNSAFE ]
       - systemd-ask-password-wall.service:                 [ UNSAFE ]
       - systemd-fsckd.service:                             [ UNSAFE ]
       - systemd-initctl.service:                           [ UNSAFE ]
       - systemd-journald.service:                          [ OK ]
       - systemd-logind.service:                            [ OK ]
       - systemd-networkd.service:                          [ OK ]
       - systemd-rfkill.service:                            [ UNSAFE ]
       - systemd-udevd.service:                             [ EXPOSED ]
       - udisks2.service:                                   [ UNSAFE ]
       - upower.service:                                    [ OK ]
       - user@0.service:                                    [ UNSAFE ]
       - user@1000.service:                                 [ UNSAFE ]
       - uuidd.service:                                     [ OK ]
       - virtualbox-guest-utils.service:                    [ UNSAFE ]
       - wpa_supplicant.service:                            [ UNSAFE ]

[+] 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 62 active modules
  - Checking Linux kernel configuration file                [ FOUND ]
  - Checking default I/O kernel scheduler                   [ NOT FOUND ]
  - Checking for available kernel update                    [ OK ]
  - Checking core dumps configuration
    - configuration in systemd conf files                   [ DEFAULT ]
    - configuration in etc/profile                          [ DEFAULT ]
    - 'hard' configuration in security/limits.conf          [ DEFAULT ]
    - 'soft' configuration in security/limits.conf          [ DEFAULT ]
    - Checking setuid core dumps configuration              [ DISABLED ]
  - Check if reboot is needed                               [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                  [ FOUND ]
  - Searching for dead/zombie processes                     [ NOT FOUND ]
  - Searching for IO waiting processes                      [ NOT FOUND ]
  - Search prelink tooling                                  [ NOT FOUND ]

[+] 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 ]
  - Password hashing methods                                  [ SUGGESTION ]
  - Checking minimum group password hashing rounds            [ DISABLED ]
  - Checking maximum group password hashing rounds            [ DISABLED ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ NOT ENABLED ]
  - Sudoers file(s)                                           [ FOUND ]
    - Permissions for directory: /etc/sudoers.d               [ WARNING ]
    - Permissions for: /etc/sudoers                           [ OK ]
    - Permissions for: /etc/sudoers.d/README                  [ OK ]
    - Permissions for: /etc/sudoers.d/kali-grant-root         [ OK ]
    - Permissions for: /etc/sudoers.d/vagrant                 [ 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                              [ SUGGESTION ]
  - 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 ]
  - LDAP authentication support                               [ NOT ENABLED ]
  - Logging failed login attempts                             [ ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 11 shells (valid shells: 11).
    - 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)                             [ OK ]
  - 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 /                                        [ NON DEFAULT ]
  - Mount options of /dev                                     [ HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:5 noexec:6 nosuid:3 ro or noexec (W^X): 6 of total 33
  - Checking Locate database                                  [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: freevxfs hfs hfsplus jffs2 squashfs udf

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

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)           [ NOT DISABLED ]
```

```
[+] NFS
------------------------------------
  - Query rpc registered programs                             [ DONE ]
  - Query NFS versions                                        [ DONE ]
  - Query NFS protocols                                       [ DONE ]
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
------------------------------------
  - Searching DNS domain name                                 [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                         [ NONE ]
    - Presence of configured hostname in /etc/hosts           [ FOUND ]
    - Hostname mapped to localhost                            [ NOT FOUND ]
    - Localhost mapping to IP address                         [ 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 or directory  [ WARNING ]
  - Checking vulnerable packages (apt-get only)               [ DONE ]
  - 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: 172.20.156.1                              [ OK ]
    - Minimal of 2 responsive nameservers                     [ WARNING ]
    - DNSSEC supported (systemd-resolved)                     [ UNKNOWN ]
  - 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 ]
  - Uncommon network protocols                                [ 0 ]

[+] 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 (binary /usr/sbin/apache2)                [ FOUND ]
      Info: Configuration file found (/etc/apache2/apache2.conf)
      Info: No virtual hosts found
    * Loadable modules                                        [ FOUND (119) ]
        - Found 119 loadable modules
          mod_evasive: anti-DoS/brute force                   [ NOT FOUND ]
          mod_reqtimeout/mod_qos                              [ FOUND ]
          ModSecurity: web application firewall               [ NOT FOUND ]
  - Checking nginx                                            [ NOT FOUND ]

[+] SSH Support
```

```
------------------------------------
  - Checking running SSH daemon                               [ FOUND ]
    - Searching SSH configuration                             [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                      [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                     [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                     [ OK ]
    - OpenSSH option: Compression                             [ SUGGESTION ]
    - OpenSSH option: FingerprintHash                         [ OK ]
    - OpenSSH option: GatewayPorts                            [ OK ]
    - OpenSSH option: IgnoreRhosts                            [ OK ]
    - OpenSSH option: LoginGraceTime                          [ OK ]
    - OpenSSH option: LogLevel                                [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                            [ SUGGESTION ]
    - OpenSSH option: MaxSessions                             [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                         [ OK ]
    - OpenSSH option: PermitUserEnvironment                   [ OK ]
    - OpenSSH option: PermitTunnel                            [ OK ]
    - OpenSSH option: Port                                    [ SUGGESTION ]
    - OpenSSH option: PrintLastLog                            [ OK ]
    - OpenSSH option: StrictModes                             [ OK ]
    - OpenSSH option: TCPKeepAlive                            [ SUGGESTION ]
    - OpenSSH option: UseDNS                                  [ OK ]
    - OpenSSH option: X11Forwarding                           [ SUGGESTION ]
    - OpenSSH option: AllowAgentForwarding                    [ SUGGESTION ]
    - OpenSSH option: AllowUsers                              [ NOT FOUND ]
    - OpenSSH 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                                              [ FOUND ]
    - Checking PHP disabled functions                         [ FOUND ]
    - Checking expose_php option                              [ OFF ]
    - Checking enable_dl option                               [ OFF ]
    - Checking allow_url_fopen option                         [ ON ]
    - Checking allow_url_include option                       [ OFF ]
    - Checking listen option                                  [ OK ]

[+] 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 remote logging                                   [ NOT ENABLED ]
  - Checking log directories (static list)                    [ DONE ]
  - Checking open log files                                   [ DONE ]
  - Checking deleted files in use                             [ FILES FOUND ]

[+] 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 ]
  - Checking NIS client installation                            [ OK ]
  - Checking NIS server installation                            [ OK ]
  - Checking TFTP client installation                           [ OK ]
  - Checking TFTP server installation                           [ SUGGESTION ]

[+] 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 ]

[+] Accounting
------------------------------------
  - Checking accounting information                             [ NOT FOUND ]
  - Checking sysstat accounting data                            [ DISABLED ]
  - Checking auditd                                             [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/131]               [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 30.457526 seconds

Device sda5 not found
  - Found 0 encrypted and 1 unencrypted swap devices in use.    [ OK ]
  - Kernel entropy is sufficient                                [ YES ]
  - HW RNG & rngd                                               [ NO ]
  - SW prng                                                     [ YES ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                                  [ FOUND ]
    - Checking AppArmor status                                  [ DISABLED ]
  - Checking presence SELinux                                   [ NOT FOUND ]
  - Checking presence TOMOYO Linux                              [ NOT FOUND ]
  - Checking presence grsecurity                                [ NOT FOUND ]
  - Checking for implemented MAC framework                      [ NONE ]

[+] Software: file integrity
------------------------------------
  - Checking file integrity tools
  - dm-integrity (status)                                       [ DISABLED ]
  - dm-verity (status)                                          [ DISABLED ]
  - 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
    File: /boot/grub/grub.cfg                                   [ OK ]
    File: /etc/crontab                                          [ SUGGESTION ]
```

```
    File: /etc/group                                        [ OK ]
    File: /etc/group-                                       [ OK ]
    File: /etc/hosts.allow                                  [ OK ]
    File: /etc/hosts.deny                                   [ OK ]
    File: /etc/issue                                        [ OK ]
    File: /etc/issue.net                                    [ OK ]
    File: /etc/motd                                         [ OK ]
    File: /etc/passwd                                       [ OK ]
    File: /etc/passwd-                                      [ OK ]
    File: /etc/ssh/sshd_config                              [ SUGGESTION ]
    Directory: /etc/cron.d                                  [ SUGGESTION ]
    Directory: /etc/cron.daily                              [ SUGGESTION ]
    Directory: /etc/cron.hourly                             [ SUGGESTION ]
    Directory: /etc/cron.weekly                             [ SUGGESTION ]
    Directory: /etc/cron.monthly                            [ SUGGESTION ]

[+] Home directories
------------------------------------
  - Permissions of home directories                         [ WARNING ]
  - Ownership of home directories                           [ OK ]
  - 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)                             [ OK ]
    - kernel.core_uses_pid (exp: 1)                         [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                          [ OK ]
    - kernel.dmesg_restrict (exp: 1)                        [ OK ]
    - 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)                 [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)           [ DIFFERENT ]
    - 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)               [ DIFFERENT ]
    - 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)                  [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)       [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)    [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)           [ DIFFERENT ]
    - 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)                                 [ FOUND ]
    - Installed malware scanner                             [ NOT FOUND ]

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

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

================================================================================

  -[ Lynis 3.0.0 Results ]-

  Warnings (3):
  ----------------------------
  ! Can't find any security repository in /etc/apt/sources.list or sources.list.d directory [PKGS-7388]
```

```
      https://cisofy.com/lynis/controls/PKGS-7388/

  ! 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 (60):
  -----------------------------
  * This release is more than 4 months old. Consider upgrading [LYNIS]
      https://cisofy.com/lynis/controls/LYNIS/

  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
      https://cisofy.com/lynis/controls/DEB-0280/

  * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
      https://cisofy.com/lynis/controls/DEB-0810/

  * Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to
determine which daemons are using old versions of libraries and need restarting. [DEB-0831]
      https://cisofy.com/lynis/controls/DEB-0831/

  * Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
      https://cisofy.com/lynis/controls/DEB-0870/

  * Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
      https://cisofy.com/lynis/controls/DEB-0875/

  * Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
      https://cisofy.com/lynis/controls/DEB-0880/

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

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
      https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
      https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure minimum encryption algorithm rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * Configure maximum encryption algorithm rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

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

  * When possible set expire dates for all password protected accounts [AUTH-9282]
      https://cisofy.com/lynis/controls/AUTH-9282/

  * 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/

  * 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/
```

```
  * Consider disabling unused kernel modules [FILE-6430]
    - Details  : /etc/modprobe.d/blacklist.conf
    - Solution : Add 'install MODULENAME /bin/true' (without quotes)
      https://cisofy.com/lynis/controls/FILE-6430/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
      https://cisofy.com/lynis/controls/USB-1000/

  * Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
      https://cisofy.com/lynis/controls/STRG-1846/

  * Check DNS configuration for the dns domain name [NAME-4028]
      https://cisofy.com/lynis/controls/NAME-4028/

  * Purge old/removed packages (25 found) with aptitude purge or dpkg --purge command. This will cleanup old
configuration files, cron jobs and startup scripts. [PKGS-7346]
      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/

  * Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]
      https://cisofy.com/lynis/controls/NETW-2705/

  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'rds' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
      https://cisofy.com/lynis/controls/HTTP-6640/

  * Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
      https://cisofy.com/lynis/controls/HTTP-6643/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
```

```
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via PHP [PHP-2376]
      https://cisofy.com/lynis/controls/PHP-2376/

  * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
      https://cisofy.com/lynis/controls/LOGG-2154/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/

  * Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services
[INSE-8320]
      https://cisofy.com/lynis/controls/INSE-8320/

  * 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 (disabled) [ACCT-9626]
      https://cisofy.com/lynis/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/lynis/controls/ACCT-9628/

  * 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/

  * Consider restricting file permissions [FILE-7524]
    - Details  : See screen output or log file
    - Solution : Use chmod to change file permissions
      https://cisofy.com/lynis/controls/FILE-7524/

  * Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
      https://cisofy.com/lynis/controls/HOME-9304/

  * 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 compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/lynis/controls/HRDN-7222/

  * 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 : 60 [############        ]
  Tests performed : 263
  Plugins enabled : 1
```

```
  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  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 3.0.0

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

  2007-2020, 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)
```

That is a lot if Checks performed for host security.

3.2. Lynis Output on RHEL 7 VM

RHEL7

Out of curiosity, I fired this tool up on a RHEL 7 system. No hardening performed; base install of OS.

Output:

```
################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.2
  Operating system:          Linux
  Operating system name:     RHEL
  Operating system version:  7.7
  Kernel version:            3.10.0
  Hardware platform:         x86_64
  Hostname:                  rhel7
  ---------------------------------------------------
  Profiles:                  /root/Security/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
```

```
  Plugin directory:          ./plugins
  ------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ------------------------------------------------
  - Program update status...                                [ NO UPDATE ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 10.040343 seconds

..............]

[+] Boot and services
------------------------------------
  - Service Manager                                         [ systemd ]
  - Checking UEFI boot                                      [ DISABLED ]
  - Checking presence GRUB2                                 [ FOUND ]
    - Checking for password protection                      [ OK ]
  - Check running services (systemctl)                      [ DONE ]
        Result: found 45 running services
  - Check enabled services at boot (systemctl)              [ DONE ]
        Result: found 68 enabled services
  - Check startup files (permissions)                       [ OK ]

[+] Kernel
------------------------------------
  - Checking default runlevel                               [ 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 93 active modules
  - Checking Linux kernel configuration file                [ FOUND ]
  - Checking default I/O kernel scheduler                   [ FOUND ]
  - Checking core dumps configuration
    - configuration in systemd conf files                   [ DEFAULT ]
    - configuration in etc/profile                          [ DEFAULT ]
    - 'hard' configuration in security/limits.conf          [ DEFAULT ]
    - 'soft' configuration in security/limits.conf          [ DEFAULT ]
    - Checking setuid core dumps configuration              [ DISABLED ]
  - Check if reboot is needed                               [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                  [ FOUND ]
  - Searching for dead/zombie processes                     [ NOT FOUND ]
  - Searching for IO waiting processes                      [ NOT FOUND ]
  - Search prelink tooling                                  [ NOT FOUND ]

[+] 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 ]
  - Password hashing methods                                [ SUGGESTION ]
  - Checking minimum group password hashing rounds          [ DISABLED ]
  - Checking maximum group password hashing rounds          [ DISABLED ]
```

```
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ NOT ENABLED ]
  - Sudoers file(s)                                           [ FOUND ]
    - Permissions for directory: /etc/sudoers.d               [ OK ]
    - Permissions for: /etc/sudoers                           [ OK ]
  - PAM password strength tools                               [ OK ]
  - PAM configuration file (pam.conf)                         [ NOT FOUND ]
  - PAM configuration files (pam.d)                           [ FOUND ]
  - PAM modules                                               [ FOUND ]
  - LDAP module in PAM                                        [ NOT FOUND ]
  - Accounts without expire date                              [ SUGGESTION ]
  - Accounts without password                                 [ OK ]
  - Locked accounts                                           [ 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 and /etc/profile.d)                 [ SUGGESTION ]
    - umask (/etc/login.defs)                                 [ OK ]
    - umask (/etc/init.d/functions)                           [ SUGGESTION ]
  - LDAP authentication support                               [ NOT ENABLED ]
  - Logging failed login attempts                             [ DISABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 7 shells (valid shells: 7).
    - Session timeout settings/tools                          [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bashrc                   [ WEAK ]
    - Checking default umask in /etc/csh.cshrc                [ WEAK ]
    - Checking default umask in /etc/profile                  [ WEAK ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                              [ SUGGESTION ]
    - Checking /tmp mount point                               [ SUGGESTION ]
    - Checking /var mount point                               [ SUGGESTION ]
  - Checking LVM volume groups                                [ FOUND ]
    - Checking LVM volumes                                    [ FOUND ]
  - Query swap partitions (fstab)                             [ OK ]
  - Testing swap partitions                                   [ OK ]
  - Testing /proc mount (hidepid)                             [ SUGGESTION ]
  - Checking for old files in /tmp                            [ FOUND ]
  - Checking /tmp sticky bit                                  [ OK ]
  - Checking /var/tmp sticky bit                              [ OK ]
  - ACL support root file system                              [ ENABLED ]
  - Mount options of /                                        [ OK ]
  - Mount options of /boot                                    [ DEFAULT ]
  - Mount options of /dev                                     [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:14 noexec:18 nosuid:12 ro or noexec (W^X): 18 of total 35
  - Checking Locate database                                  [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: cramfs squashfs udf

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

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)           [ NOT DISABLED ]

[+] NFS
------------------------------------
  - Query rpc registered programs                             [ DONE ]
  - Query NFS versions                                        [ DONE ]
  - Query NFS protocols                                       [ DONE ]
```

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

[+] Name services
------------------------------------
  - Checking search domains                                 [ FOUND ]
  - Searching DNS domain name                               [ FOUND ]
      Domain name: example.com
  - Checking /etc/hosts
    - Duplicate entries in hosts file                       [ NONE ]
    - Presence of configured hostname in /etc/hosts         [ NOT FOUND ]
    - Hostname mapped to localhost                          [ NOT FOUND ]
    - Localhost mapping to IP address                       [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching RPM package manager                         [ FOUND ]
      - Querying RPM package manager

  [WARNING]: Test PKGS-7308 had a long execution: 15.091988 seconds

  - YUM package management consistency                      [ OK ]
  - Checking package database duplicates                    [ OK ]
  - Checking package database for problems                  [ OK ]

  [WARNING]: Test PKGS-7384 had a long execution: 22.884920 seconds

  - Checking missing security packages                      [ WARNING ]

  [WARNING]: Test PKGS-7386 had a long execution: 31.791617 seconds

  - Checking GPG checks (yum.conf)                          [ OK ]
  - Checking package audit tool                             [ INSTALLED ]
    Found: yum-security
  - Toolkit for automatic upgrades                          [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                             [ ENABLED ]
      Configuration method                                  [ AUTO ]
      IPv6 only                                             [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 172.20.156.1                            [ OK ]
    - Minimal of 2 responsive nameservers                   [ WARNING ]
  - Checking default gateway                                [ DONE ]
  - Getting listening ports (TCP/UDP)                       [ DONE ]
  - Checking promiscuous interfaces                         [ WARNING ]
  - Checking waiting connections                            [ OK ]
  - Checking status DHCP client                             [ RUNNING ]
  - Checking for ARP monitoring software                    [ NOT FOUND ]
  - Uncommon network protocols                              [ 0 ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                                    [ RUNNING ]
  - Checking CUPS configuration file                        [ OK ]
    - File permissions                                      [ OK ]
  - Checking CUPS addresses/sockets                         [ FOUND ]
  - Checking lp daemon                                      [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------
  - Postfix status                                          [ RUNNING ]
    - Postfix configuration                                 [ FOUND ]
      - Postfix banner                                      [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                         [ FOUND ]
    - Checking iptables policies of chains                  [ FOUND ]
      - Checking chain INPUT (table:
filter, policy ACCEPT)  [ ACCEPT ]
    - Checking for empty ruleset                            [ OK ]
    - Checking for unused rules                             [ FOUND ]
```

```
  - 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 ]
    - OpenSSH option: AllowTcpForwarding                        [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                       [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                       [ OK ]
    - OpenSSH option: Compression                               [ SUGGESTION ]
    - OpenSSH option: FingerprintHash                           [ OK ]
    - OpenSSH option: GatewayPorts                              [ OK ]
    - OpenSSH option: IgnoreRhosts                              [ OK ]
    - OpenSSH option: LoginGraceTime                            [ OK ]
    - OpenSSH option: LogLevel                                  [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                              [ SUGGESTION ]
    - OpenSSH option: MaxSessions                               [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                           [ SUGGESTION ]
    - OpenSSH option: PermitUserEnvironment                     [ OK ]
    - OpenSSH option: PermitTunnel                              [ OK ]
    - OpenSSH option: Port                                      [ SUGGESTION ]
    - OpenSSH option: PrintLastLog                              [ OK ]
    - OpenSSH option: StrictModes                               [ OK ]
    - OpenSSH option: TCPKeepAlive                              [ SUGGESTION ]
    - OpenSSH option: UseDNS                                    [ SUGGESTION ]
    - OpenSSH option: X11Forwarding                             [ SUGGESTION ]
    - OpenSSH option: AllowAgentForwarding                      [ SUGGESTION ]
    - OpenSSH option: UsePrivilegeSeparation                    [ OK ]
    - OpenSSH option: AllowUsers                                [ NOT FOUND ]
    - OpenSSH 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 remote logging                                     [ NOT ENABLED ]
  - Checking log directories (static list)                      [ DONE ]
  - Checking open log files                                     [ DONE ]
  - Checking deleted files in use                               [ FILES FOUND ]

[+] 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 ]
  - Checking NIS client installation                          [ OK ]
  - Checking NIS server installation                          [ OK ]
  - Checking TFTP client installation                         [ OK ]
  - Checking TFTP server installation                         [ OK ]

[+] 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                           [ OK ]
  - Checking sysstat accounting data                          [ ENABLED ]
  - Checking auditd                                           [ ENABLED ]
    - Checking audit rules                                    [ SUGGESTION ]
    - Checking audit configuration file                       [ OK ]
    - Checking auditd log file                                [ FOUND ]

[+] Time and Synchronization
------------------------------------
  - NTP daemon found: chronyd                                 [ FOUND ]
  - Checking for a running NTP daemon or client               [ OK ]

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/11]              [ NONE ]
  - Found 0 encrypted and 1 unencrypted swap devices in use.  [ OK ]
  - Kernel entropy is sufficient                              [ YES ]
  - HW RNG & rngd                                             [ NO ]
  - SW prng                                                   [ NO ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------
        - Docker info output (warnings)                       [ NONE ]

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                                [ NOT FOUND ]
  - Checking presence SELinux                                 [ FOUND ]
    - Checking SELinux status                                 [ ENABLED ]
      - Checking current mode and config file                 [ OK ]
        Current SELinux mode: enforcing
        Found 0 permissive SELinux object types
        Found 78 unconfined and 0 initrc_t processes
  - 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
    File: /boot/grub2/grub.cfg                                  [ SUGGESTION ]
    File: /etc/at.deny                                          [ SUGGESTION ]
    File: /etc/cron.deny                                        [ OK ]
    File: /etc/crontab                                          [ SUGGESTION ]
    File: /etc/group                                            [ OK ]
    File: /etc/group-                                           [ OK ]
    File: /etc/hosts.allow                                      [ OK ]
    File: /etc/hosts.deny                                       [ OK ]
    File: /etc/issue                                            [ OK ]
    File: /etc/issue.net                                        [ OK ]
    File: /etc/motd                                             [ OK ]
    File: /etc/passwd                                           [ OK ]
    File: /etc/passwd-                                          [ OK ]
    File: /etc/ssh/sshd_config                                  [ OK ]
    Directory: /etc/cron.d                                      [ SUGGESTION ]
    Directory: /etc/cron.daily                                  [ SUGGESTION ]
    Directory: /etc/cron.hourly                                 [ SUGGESTION ]
    Directory: /etc/cron.weekly                                 [ SUGGESTION ]
    Directory: /etc/cron.monthly                                [ SUGGESTION ]

[+] Home directories
------------------------------------
  - Permissions of home directories                             [ OK ]
  - Ownership of home directories                               [ OK ]
  - 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)                                 [ OK ]
    - kernel.core_uses_pid (exp: 1)                             [ OK ]
    - 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)                     [ DIFFERENT ]
    - 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)                     [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)                   [ DIFFERENT ]
    - 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)                 [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)           [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)        [ OK ]
    - net.ipv4.conf.default.log_martians (exp: 1)               [ DIFFERENT ]
    - 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)                                     [ FOUND ]
    - Installed malware scanner                                 [ NOT FOUND ]

[+] Custom tests
------------------------------------
```

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

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                     [ DONE ]

================================================================================

  -[ Lynis 3.0.2 Results ]-

  Warnings (4):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7386]
      https://cisofy.com/lynis/controls/PKGS-7386/

  ! Couldn't find 2 responsive nameservers [NETW-2705]
      https://cisofy.com/lynis/controls/NETW-2705/

  ! Found promiscuous interface [NETW-3015]
    - Details  : virbr0-nic
    - Solution : Determine if this mode is required or whitelist interface in profile
      https://cisofy.com/lynis/controls/NETW-3015/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  Suggestions (48):
  ----------------------------
  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
      https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure minimum encryption algorithm rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * Configure maximum encryption algorithm rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * When possible set expire dates for all password protected accounts [AUTH-9282]
      https://cisofy.com/lynis/controls/AUTH-9282/

  * 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/profile or /etc/profile.d/custom.sh could be more strict (e.g. 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/

  * Check 11 files in /tmp which are older than 90 days [FILE-6354]
      https://cisofy.com/lynis/controls/FILE-6354/

  * Consider disabling unused kernel modules [FILE-6430]
    - Details  : /etc/modprobe.d/blacklist.conf
    - Solution : Add 'install MODULENAME /bin/true' (without quotes)
      https://cisofy.com/lynis/controls/FILE-6430/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
      https://cisofy.com/lynis/controls/USB-1000/

  * Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
      https://cisofy.com/lynis/controls/STRG-1846/
```

```
  * Add the IP name and FQDN to /etc/hosts for proper name resolving [NAME-4404]
      https://cisofy.com/lynis/controls/NAME-4404/

  * Consider using a tool to automatically apply upgrades [PKGS-7420]
      https://cisofy.com/lynis/controls/PKGS-7420/

  * Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]
      https://cisofy.com/lynis/controls/NETW-2705/

  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'rds' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Check CUPS configuration if it really needs to listen on the network [PRNT-2308]
      https://cisofy.com/lynis/controls/PRNT-2308/

  * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e
or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
      https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to (FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : UseDNS (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
```

```
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
      https://cisofy.com/lynis/controls/LOGG-2154/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/

  * 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/

  * Audit daemon is enabled with an empty ruleset. Disable the daemon or define rules [ACCT-9630]
      https://cisofy.com/lynis/controls/ACCT-9630/

  * 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/

  * Consider restricting file permissions [FILE-7524]
    - Details  : See screen output or log file
    - Solution : Use chmod to change file permissions
      https://cisofy.com/lynis/controls/FILE-7524/

  * 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 compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/lynis/controls/HRDN-7222/

  * 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 : 55 [###########         ]
  Tests performed : 269
  Plugins enabled : 2

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  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 3.0.2
```

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

  2007-2020, 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 /root/Security/lynis/default.prf for all
settings)
```

3.3. Running Lynis on a Remote Server

For Remote Server

To run this on a remote system, make sure git is installed and then (as the root user):

```
cd /root/
mkdir Security
cd Security
git clone https://github.com/CISOfy/lynis
cd lynis
./lynis audit system -Q
```

4. Conclusion

Whoa!

After writing several other papers this year, this paper is making me very happy.

This awesome tool needs to be in my long term toolbelt.

In my job position, I use a licensed version of Nessus to scan servers for hardening and patch compliance. For an open source tool, this output and what is discovered is outstanding! I am able to immediately see the security posture of the system and recommend changes to my customers. I am highly impressed with this tool. The professional version of this tool looks to cost $3 / server / month. So for $36.00 per server / year, you get a solid understanding of the security level of that system. I see a value in this tool and highly recommend it.

5. Appendix

References

https://tools.kali.org/vulnerability-analysis/lynis

https://cisofy.com/lynis/