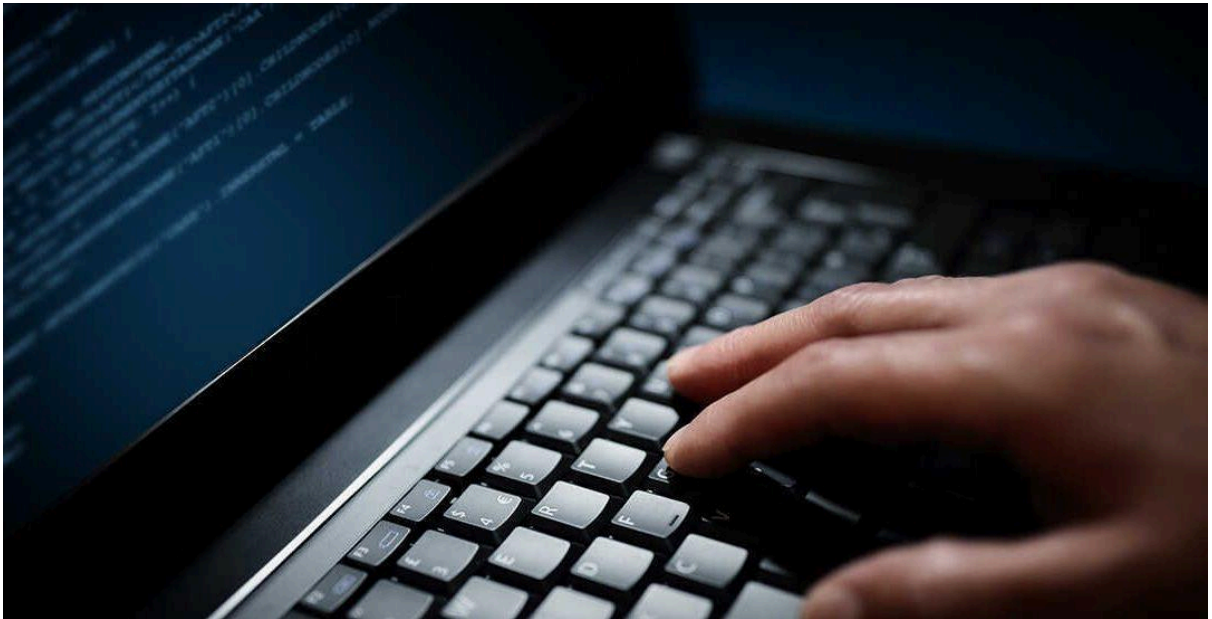


Auditoría del Sistema



AUTOR: Pedro Antonio Giménez Meroño

Índice

1. Objetivo de la práctica.....	3
2. Descripción de las herramientas.....	3
2.1 Lynis (Linux).....	3
2.2 CLARA (Windows).....	3
2.3 Nessus (Linux/Windows).....	3
3. Auditoría en Linux con Lynis.....	3
3.1 Proceso de instalación Lynis en Linux.....	3
3.2 Ejecución de los análisis.....	4
3.3 Resumen resultados de auditoría.....	4
4. Auditoría en Linux con Nessus.....	15
4.1 Proceso de instalación Nessus en Linux.....	15
4.2 Ejecución de los análisis.....	16
4.3 Resumen resultados de auditoría.....	19
5. Auditoría en Windows con Nessus.....	21
5.1 Proceso de instalación Nessus en Windows.....	21
5.2 Ejecución de los análisis.....	22
5.3 Resumen resultados de auditoría.....	24
6. Auditoría en Windows con CLARA.....	26
6.1 Proceso de instalación CLARA en Windows.....	26
6.2 Ejecución de los análisis.....	26
6.3 Resumen resultados de auditoría.....	28
7. Fuentes.....	29

1. Objetivo de la práctica

El objetivo de esta práctica es realizar una auditoría de seguridad de sistemas operativos Linux y Windows utilizando herramientas especializadas. Se trabajará con las herramientas **Lynis** para Linux, **CLARA** para Windows, y **Nessus** para un análisis de vulnerabilidades en ambos sistemas. A partir de los resultados obtenidos, los estudiantes deben identificar posibles problemas de seguridad y proponer soluciones.

2. Descripción de las herramientas

2.1 Lynis (Linux)

Lynis es una herramienta de auditoría enfocada en mantener la seguridad de los sistemas operativos basados en Linux, MacOS y en el entorno Unix. Su funcionamiento se basa en analizar exhaustivamente el estado en el que se encuentran sus sistemas, identificando posibles vulnerabilidades o problemas en el mismo.

2.2 CLARA (Windows)

Es una herramienta que desarrolló el *CCN-CERT* la cual permite analizar las características de seguridad de un sistema operativo, los criterios empleados por el programa se basan en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

2.3 Nessus (Linux/Windows)

Es un programa para auditorías de ciberseguridad, cuya función es escanear puertos, detectar puertos e identificar vulnerabilidades de distintos sistemas operativos. Nessus es un software especial que utiliza una extensa base de datos con vulnerabilidades para detectar fallas de seguridad en dispositivos.

3. Auditoría en Linux con Lynis

3.1 Proceso de instalación Lynis en Linux

Primero actualizaremos el sistema.

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo apt update  
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]  
Hit:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1.85  
8 kB]  
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [547 k  
B]  
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [300  
kB]  
Get:8 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [  
910 kB]  
Get:9 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [  
LibreOffice Writer  
Fetched 3.920 kB in 3s (1.556 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
259 packages can be upgraded. Run 'apt list --upgradable' to see them.  
pedro@pedro-VirtualBox:~$ sudo apt upgrade  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

Después desde los repositorios de ubuntu instalamos Lynis.

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo apt-get -y install lynis  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libwpe-1.0-1 libwpebackend-fdo-1.0-1  
Use 'sudo apt autoremove' to remove them.
```

3.2 Ejecución de los análisis

Para comenzar a utilizar Lynis y hacer una auditoría del sistema ejecutamos el siguiente comando. Este comando una vez finalizada nos dará un archivo .txt con los resultados de la auditoría el cual podemos encontrar en el directorio “/home/pedro/Desktop”.

```
pedro@pedro-VirtualBox: ~/Downloads  
pedro@pedro-VirtualBox:~/Downloads$ sudo lynis audit system > /home/pedro/Desktop/lynis_auditoria.txt  
pedro@pedro-VirtualBox:~/Downloads$
```

3.3 Resumen resultados de auditoría

Estos son los resultados del análisis en la máquina ubuntu:

```
[ Lynis 3.0.7 ]  
#####  
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.  
2007-2021, CISOfy - https://cisofy.com/lynis/
```

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

#####

[+] Initializing program

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

Program version: 3.0.7
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: pedro-VirtualBox

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: 12,743186 seconds
- libpam-tmpdir [Not Installed]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Software:
 - apt-listbugs [Not Installed]
 - apt-listchanges [Not Installed]
 - needrestart [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 34 running services
- Check enabled services at boot (systemctl) [ DONE ]
Result: found 50 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
- ModemManager.service: [ MEDIUM ]
- NetworkManager.service: [ EXPOSED ]
- accounts-daemon.service: [ MEDIUM ]
- acpid.service: [ UNSAFE ]
- alsa-state.service: [ UNSAFE ]
- anacron.service: [ UNSAFE ]
- appport.service: [ UNSAFE ]
- avahi-daemon.service: [ UNSAFE ]
- colord.service: [ EXPOSED ]
- cron.service: [ UNSAFE ]
- cups-browsed.service: [ UNSAFE ]
- cups.service: [ UNSAFE ]
- dbus.service: [ UNSAFE ]
- dmesg.service: [ UNSAFE ]
- emergency.service: [ UNSAFE ]
- fwupd.service: [ EXPOSED ]
- gdm.service: [ UNSAFE ]
- getty@tty1.service: [ UNSAFE ]
- irqbalance.service: [ MEDIUM ]
- kerneloops.service: [ UNSAFE ]
- lynis.service: [ UNSAFE ]
- nessusd.service: [ UNSAFE ]
- networkd-dispatcher.service: [ UNSAFE ]
- open-vm-tools.service: [ UNSAFE ]
- packagekit.service: [ UNSAFE ]
- plymouth-start.service: [ UNSAFE ]
- polkit.service: [ UNSAFE ]
- power-profiles-daemon.service: [ EXPOSED ]
- rc-local.service: [ UNSAFE ]
- rescue.service: [ UNSAFE ]
- rsyslog.service: [ UNSAFE ]
- rtkit-daemon.service: [ MEDIUM ]

- snapd.service: [ UNSAFE ]
- switcheroo-control.service: [ EXPOSED ]
- 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: [ PROTECTED ]
- systemd-logind.service: [ PROTECTED ]
- systemd-networkd.service: [ PROTECTED ]
- systemd-oomd.service: [ PROTECTED ]
- systemd-resolved.service: [ PROTECTED ]
- systemd-rfkill.service: [ UNSAFE ]
- systemd-timesyncd.service: [ PROTECTED ]
- systemd-udev.service: [ MEDIUM ]
- thermald.service: [ UNSAFE ]
- ubuntu-advantage.service: [ UNSAFE ]
- udisks2.service: [ UNSAFE ]
- unattended-upgrades.service: [ UNSAFE ]
- upower.service: [ PROTECTED ]
```

- user@1000.service: [UNSAFE]
- uidd.service: [PROTECTED]
- vgauth.service: [UNSAFE]
- whoopsie.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 [PROTECTED]
- 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 [OK]
- Checking 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]
- PAM password strength tools [OK]
- 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]
- 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) [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 8 shells (valid shells: 8).
- 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 [ PARTIALLY HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Total without nodev:9 noexec:20 nosuid:16 ro or noexec (W^X): 11 of total 38
- Disable kernel support of some filesystems
[+] 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) [ DISABLED ]
[+] NFS
-----
- Check running NFS daemon [ NOT FOUND ]
[+] Name services
-----
- Checking search domains [ FOUND ]
- Checking /etc/resolv.conf options [ FOUND ]
- 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 RPM package manager [ FOUND ]
- Querying RPM package manager
=====
Exception found!
Function/test: [PKGS-7328]
Message: No installed packages found with Zypper
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!

-
- Using Zypper to find vulnerable packages [NONE]
 - Searching dpkg package manager [FOUND]
 - Querying package manager
- [WARNING]: Test PKGS-7345 had a long execution: 11,085699 seconds
- Query unpurged packages [NONE]
 - Checking security repository in sources.list file [OK]
 - Checking APT package database [OK]
 - Checking upgradeable packages [SKIPPED]
 - Checking package audit tool [INSTALLED]

Found: zypper

Exception found!

Function/test: [PKGS-7410]

Message: Could not find any kernel packages via package manager. Maybe using a different kernel package?

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!

-
- Toolkit for automatic upgrades (unattended-upgrade) [FOUND]

[+] Networking

-
- Checking IPv6 configuration [ENABLED]
- Configuration method [AUTO]
- IPv6 only [NO]
- Checking configured nameservers
 - Testing nameservers
- Nameserver: 127.0.0.53 [OK]
- DNSSEC supported (systemd-resolved) [NO]
 - Getting listening ports (TCP/UDP) [DONE]
 - Checking promiscuous interfaces [OK]
 - Checking status DHCP client
 - 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 [WARNING]
 - Checking CUPS addresses/sockets [FOUND]
 - Checking lp daemon [NOT RUNNING]

[+] Software: e-mail and messaging

[+] Software: firewalls

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

[+] Software: webserver

```
- Checking Apache [ NOT FOUND ]
- Checking nginx [ NOT FOUND ]
[+] SSH Support
-----
- Checking running SSH daemon [ 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
- 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 ]
[+] Accounting
-----
- Checking accounting information [ NOT FOUND ]
- Checking sysstat accounting data [ NOT FOUND ]
```

- Checking auditd [NOT FOUND]

[+] Time and Synchronization

- NTP daemon found: systemd (timesyncd) [FOUND]

- Checking for a running NTP daemon or client [OK]

- Last time synchronization [1583s]

[+] Cryptography

- Checking for expired SSL certificates [0/151] [NONE]

[WARNING]: Test CRYPT-7902 had a long execution: 48,492076 seconds

- Kernel entropy is sufficient [YES]

- HW RNG & rngd [NO]

- SW prng [NO]

- MOR variable not found [WEAK]

[+] Virtualization

[+] Containers

[+] Security frameworks

- Checking presence AppArmor [FOUND]

- Checking AppArmor status [ENABLED]

Found 120 unconfined processes

- Checking presence SELinux [NOT FOUND]

- Checking presence TOMOYO Linux [NOT FOUND]

- Checking presence grsecurity [NOT FOUND]

- Checking for implemented MAC framework [OK]

[+] Software: file integrity

- Checking file integrity tools

- Checking presence integrity tool [NOT FOUND]

[+] Software: System tooling

- Checking automation tooling

- Automation tooling [NOT FOUND]

- Checking for IDS/IPS tooling [NONE]

[+] Software: Malware

- Malware software components [NOT FOUND]

[+] File Permissions

- Starting file permissions check

File: /boot/grub/grub.cfg [SUGGESTION]

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/passwd [OK]

File: /etc/passwd- [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
- dev.tty.ldisc_autoload (exp: 0) [DIFFERENT]
- fs.protected_fifos (exp: 2) [DIFFERENT]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFFERENT]
- kernel.core_uses_pid (exp: 1) [OK]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFFERENT]
- kernel.modules_disabled (exp: 1) [DIFFERENT]
- kernel.perf_event_paranoid (exp: 3) [DIFFERENT]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFFERENT]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFFERENT]
- kernel.yama_ptrace_scope (exp: 1 2 3) [OK]
- net.core.bpf_jit_harden (exp: 2) [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) [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) [NOT FOUND]
- Installed malware scanner [NOT FOUND]
- Non-native binary formats [FOUND]

[+] Custom tests

- Running custom tests... [NONE]

[+] Plugins (phase 2)

=====

-[Lynis 3.0.7 Results]-

Warnings (1):

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

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

Suggestions (40):

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available.

[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 apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
<https://cisofy.com/lynis/controls/DEB-0811/>
* 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 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/>
* Configure password hashing 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/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/>
* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
<https://cisofy.com/lynis/controls/USB-1000/>
* Check DNS configuration for the dns domain name [NAME-4028]
<https://cisofy.com/lynis/controls/NAME-4028/>
* Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]
<https://cisofy.com/lynis/controls/PKGS-7308/>
* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
<https://cisofy.com/lynis/controls/PKGS-7370/>
* Install package apt-show-versions for patch management purposes [PKGS-7394]
<https://cisofy.com/lynis/controls/PKGS-7394/>
* 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/>
* Access to CUPS configuration could be more strict. [PRNT-2307]
<https://cisofy.com/lynis/controls/PRNT-2307/>

* Check CUPS configuration if it really needs to listen on the network [PRNT-2308]
<https://cisofy.com/lynis/controls/PRNT-2308/>
* 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/>
- * Enable process accounting [ACCT-9622]
<https://cisofy.com/lynis/controls/ACCT-9622/>
- * Enable sysstat to collect accounting (no results) [ACCT-9626]
<https://cisofy.com/lynis/controls/ACCT-9626/>
- * Enable auditd to collect audit information [ACCT-9628]
<https://cisofy.com/lynis/controls/ACCT-9628/>
- * 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 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 : 65 [#####]
Tests performed : 250
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

=====

Exceptions found

Some exceptional events or information was found!

What to do:

You can help by providing your log file (/var/log/lynis.log).

Go to <https://cisofy.com/contact/> and send your file to the e-mail address listed

=====

Lynis 3.0.7

Auditing, system hardening, and compliance for UNIX-based systems

(Linux, macOS, BSD, and others)

2007-2021, CISOFy - <https://cisofy.com/lynis/>

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

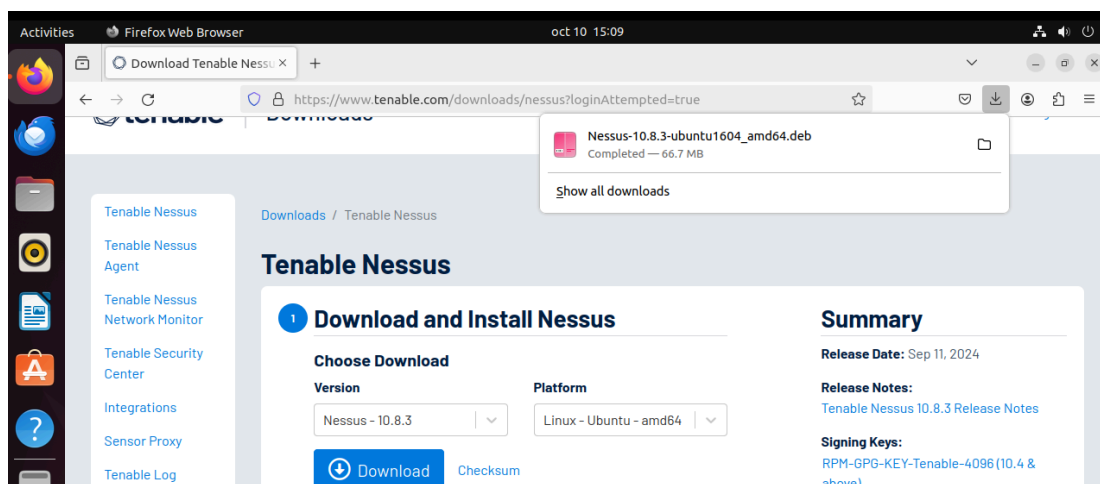
[TIP]: Enhance Lynis audits by adding your settings to custom.prfl (see /etc/lynis/default.prfl for all settings)

4. Auditoría en Linux con Nessus

4.1 Proceso de instalación Nessus en Linux

Descarga Nessus desde el siguiente enlace

<https://www.tenable.com/tenable-for-education/nessus-essentials> y escogemos la version para ubuntu 22.04.



Ahora antes de instalar actualizaremos el sistema.

```
pedro@pedro-VirtualBox: ~  
pedro@pedro-VirtualBox:~$ sudo apt update  
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Hit:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
257 packages can be upgraded. Run 'apt list --upgradable' to see them.  
pedro@pedro-VirtualBox:~$
```

Abrimos una terminal en la carpeta donde se ha descargado el programa y ejecutamos “sudo dpkg -i Nessus-*.deb” cuando finalice solo nos quedará inicializar el servicio, yo lo he hecho con “sudo systemctl start nessusd.service”.

```
pedro@pedro-VirtualBox: ~/Downloads
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://pedro-VirtualBox:8834/ to configure your scanner

pedro@pedro-VirtualBox:~/Downloads$ sudo systemctl start nessusd.service
pedro@pedro-VirtualBox:~/Downloads$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor prese
   Active: active (running) since Thu 2024-10-10 15:30:37 CEST; 14s ago
     Main PID: 10585 (nessus-service)
        Tasks: 14 (limit: 4608)
       Memory: 42.2M
          CPU: 14.393s
      CGroup: /system.slice/nessusd.service
              └─10585 /opt/nessus/sbin/nessus-service -q
                 └─10586 nessusd -q

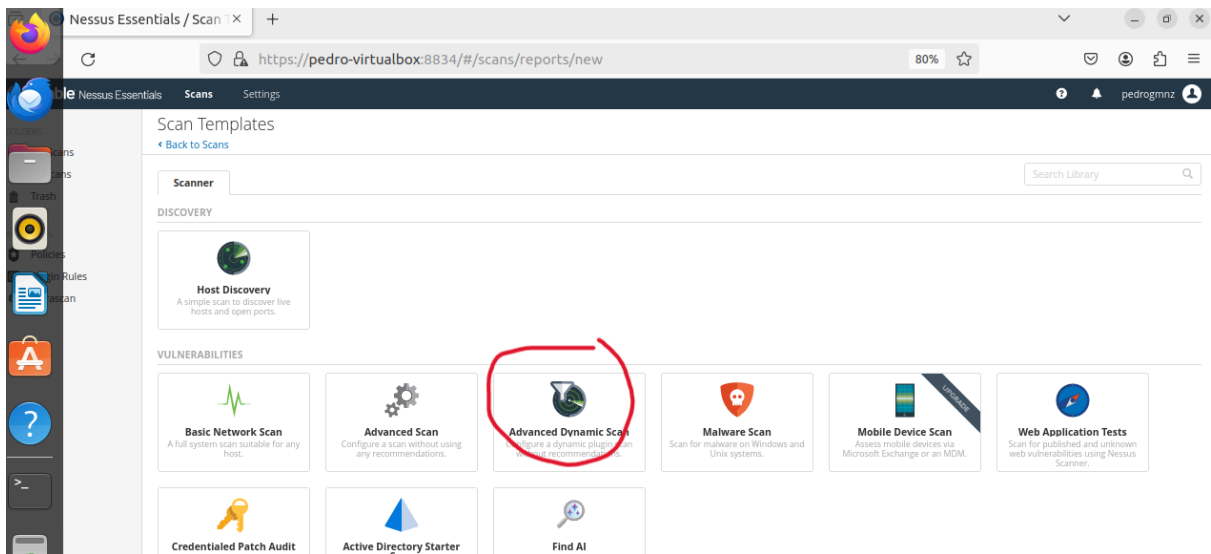
oct 10 15:30:37 pedro-VirtualBox systemd[1]: Started The Nessus Vulnerability S
oct 10 15:30:44 pedro-VirtualBox nessus-service[10586]: Cached 0 plugin libs in
oct 10 15:30:44 pedro-VirtualBox nessus-service[10586]: Cached 0 plugin libs in
lines 1-14/14 (END)
```

Para iniciar el programa nos vamos al navegador y escribimos localhost:8834 una vez aquí nos pedirá iniciar sesión con un correo y crear un usuario. Por último terminará una instalación de plugins que utiliza Nessus.

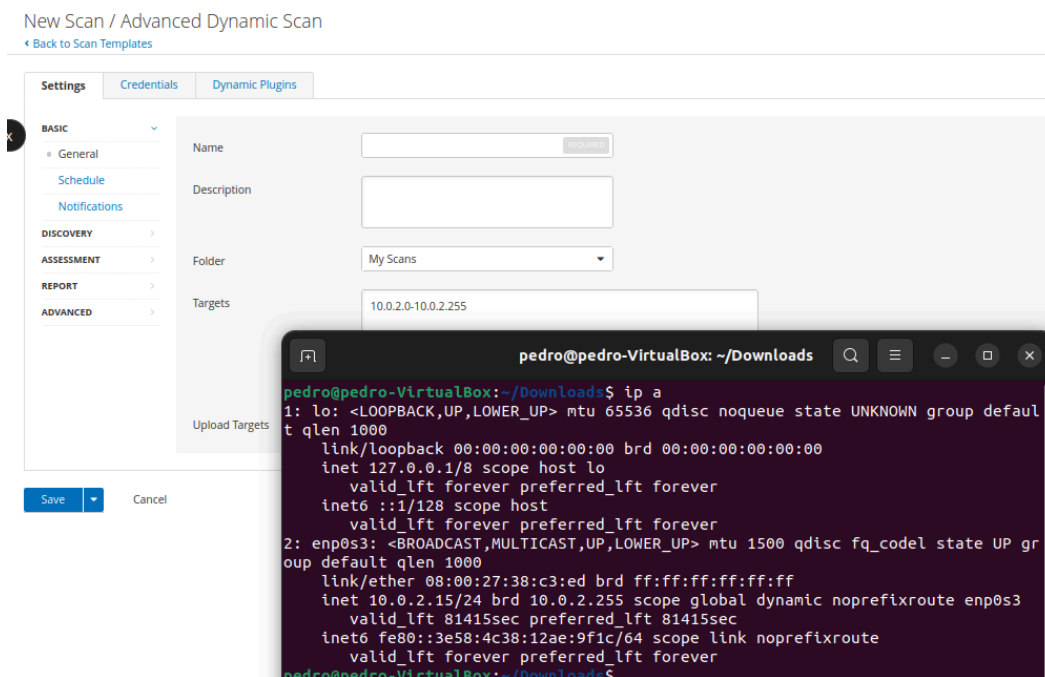


4.2 Ejecución de los análisis

Ya en el menú clicamos en “New Scan” y nos aparecerán varias aplicaciones a utilizar. Vamos a usar la de “Advanced Dynamic Scan”.



Al iniciar un nuevo escaneo con este programa tenemos que darle un nombre y elegir una dirección IP o rango. Yo he mirado la IP de mi máquina y he puesto el rango en el que está. Después iniciamos el análisis.



Una vez finaliza el proceso te da unos resultados de la auditoría de forma gráfica. Si hacemos clic en “Report” nos dará la opción de ver los resultados de forma más completa en formato CSV o HTML.

The screenshot displays the Tenable Nessus Essentials web interface. The top navigation bar includes 'Configure', 'Audit Trail', 'Launch', 'Report' (highlighted with a red circle), and 'Export'. The main content area shows a scan named 'pedro' with a table of hosts and their vulnerability counts. A 'Vulnerabilities' donut chart is also visible. A 'Generate Report' dialog box is open, allowing the user to select a report format (HTML or CSV) and a report template. The dialog also shows a 'Template Description' and 'Filters Applied'.

Host	Vulnerabilities
10.0.2.15	5
10.0.2.2	3
10.0.2.3	3
10.0.2.4	3

Scan Details

- Policy: Advanced Dynamic Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:58 PM
- End: Today at 6:59 PM
- Elapsed: a minute

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Generate Report

Report Format: ☒ HTML ☐ CSV

Select a Report Template:

- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations


Template Description: This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied: None

Generate Report Cancel Save as default

4.3 Resumen resultados de auditoría

Por temas de seguridad solo incluiré el archivo de los resultados de Vulnerabilidades por Host:

 Report generated by Tenable Nessus™

pedro

Thu, 10 Oct 2024 18:59:45 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.2
- 10.0.2.3
- 10.0.2.4
- 10.0.2.15

Vulnerabilities by Host [Collapse All](#) | [Expand All](#)

10.0.2.2

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

2

INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

10.0.2.3

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

2

INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Hide

10.0.2.4

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

2

INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available;
the v2.0 score is shown

Hide

10.0.2.15

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

2

INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)

* indicates the v3.0 score was not available;
the v2.0 score is shown

Hide

© 2024 Tenable™, Inc. All rights reserved.

20

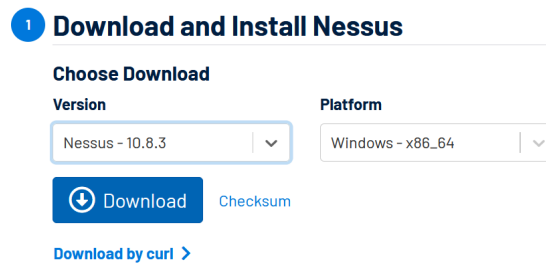
Pedro A. Giménez Meroño

5. Auditoría en Windows con Nessus

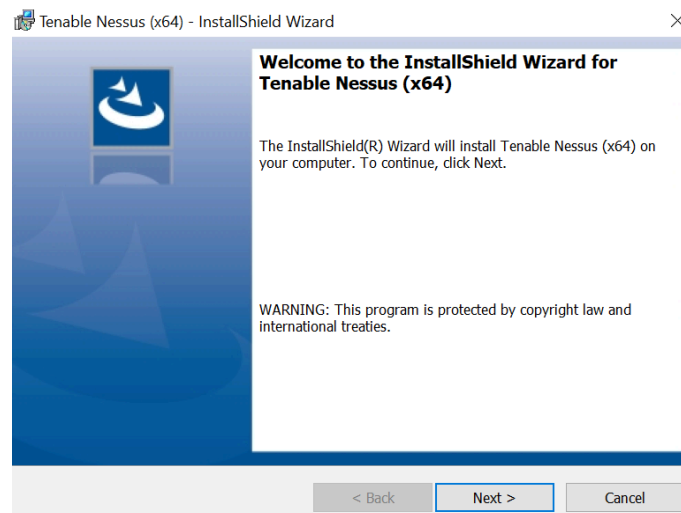
5.1 Proceso de instalación Nessus en Windows

Descarga Nessus desde el siguiente enlace

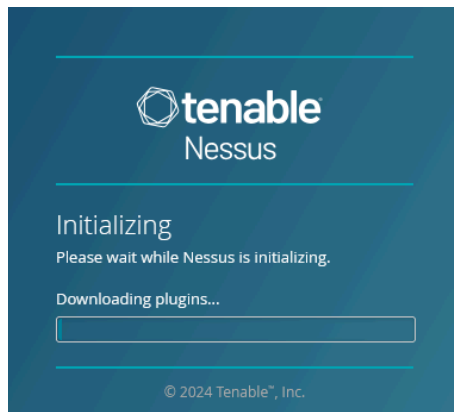
<https://www.tenable.com/tenable-for-education/nessus-essentials>



Una vez finalice la descarga ejecutamos el archivo obtenido y seguimos la instalación.



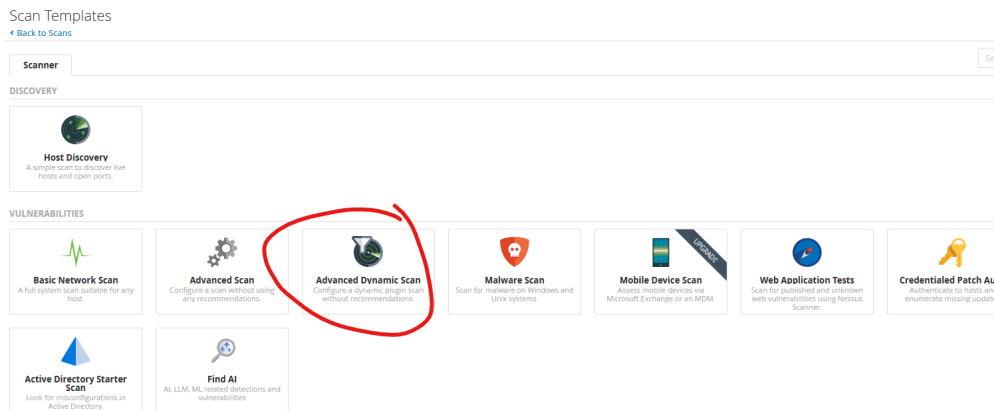
Cuando finaliza la instalación se abrirá el programa en localhost desde nuestro navegador. Y faltará crear un nombre de usuario para que termine de descargar el programa.





5.2 Ejecución de los análisis

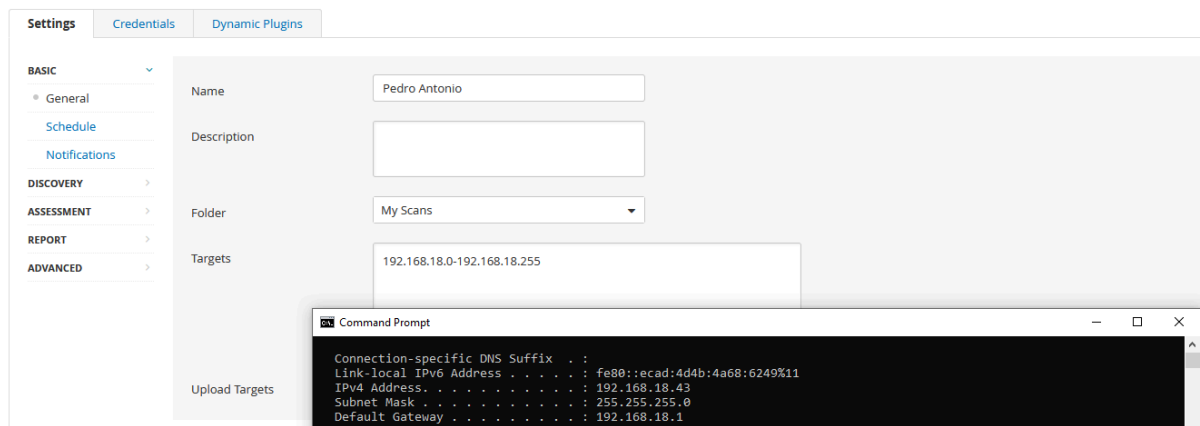
Si vamos a “New Scan” nos aparecerán varias aplicaciones a utilizar. Vamos a usar la de “Advanced Dynamic Scan”.



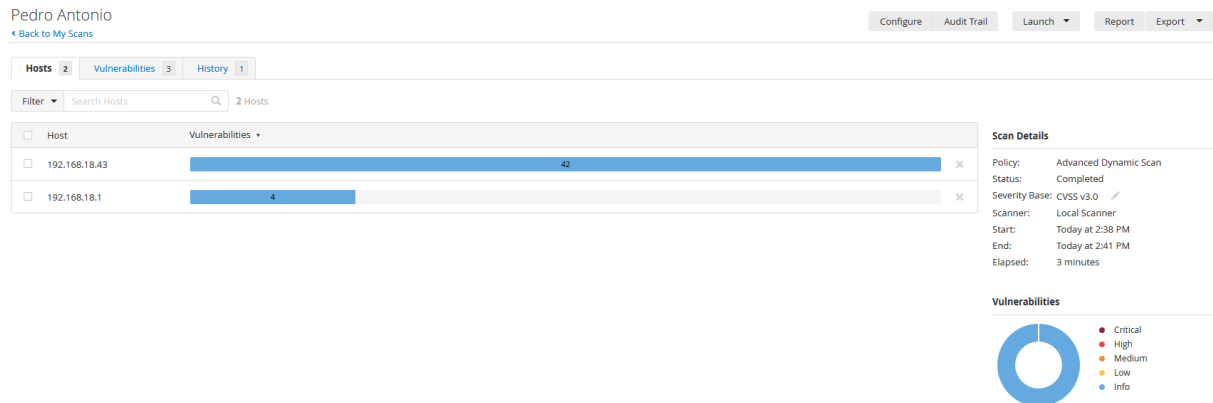
Al iniciar un nuevo escaneo con este programa tenemos que darle un nombre y elegir una dirección IP o rango. Yo he mirado la IP de mi máquina y he puesto el rango en el que está. Después iniciamos el análisis.

New Scan / Advanced Dynamic Scan

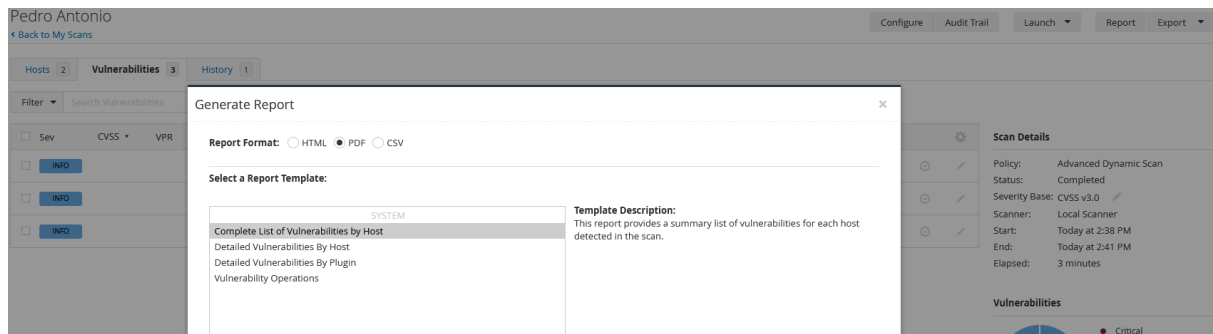
[Back to Scan Templates](#)



Una vez finaliza el proceso te da unos resultados de la auditoría de forma gráfica.



Clicando en “Report” podemos ver donde aparecen los resultados de la auditoría, con la opción donde podemos exportar todos los resultados en forma de pdf para verlos de forma más clara.



5.3 Resumen resultados de auditoría

Por temas de seguridad solo incluiré el archivo de los resultados de Vulnerabilidades por Host:



Pedro Antonio

Report generated by Tenable Nessus™

Thu, 10 Oct 2024 14:41:04 Romance Standard Time

Vulnerabilities by Host

192.168.18.43



Vulnerabilities

Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.18.1



Vulnerabilities

Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown

6. Auditoría en Windows con CLARA

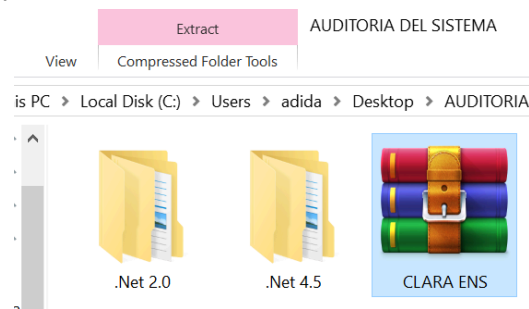
6.1 Proceso de instalación CLARA en Windows

Descarga CLARA desde el siguiente enlace:

<https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html>

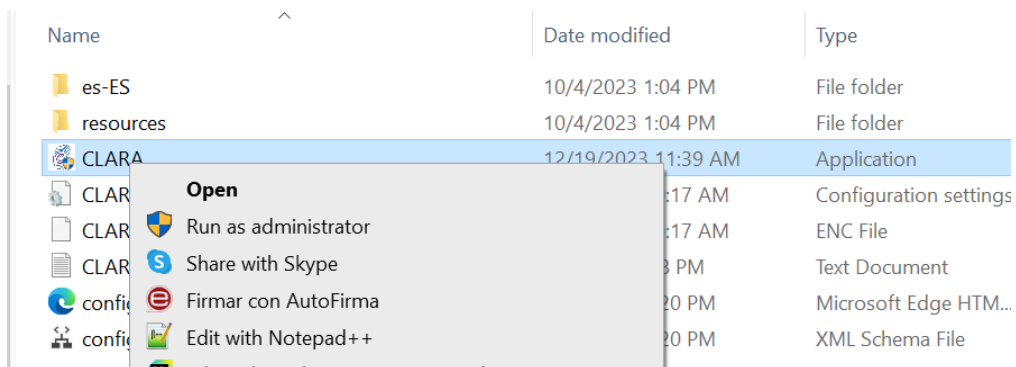


Descomprimos el archivo y nos saldrán dos carpetas que son el programa adaptado según versiones de framework de tu sistema yo en mi caso he utilizado el 4.5.

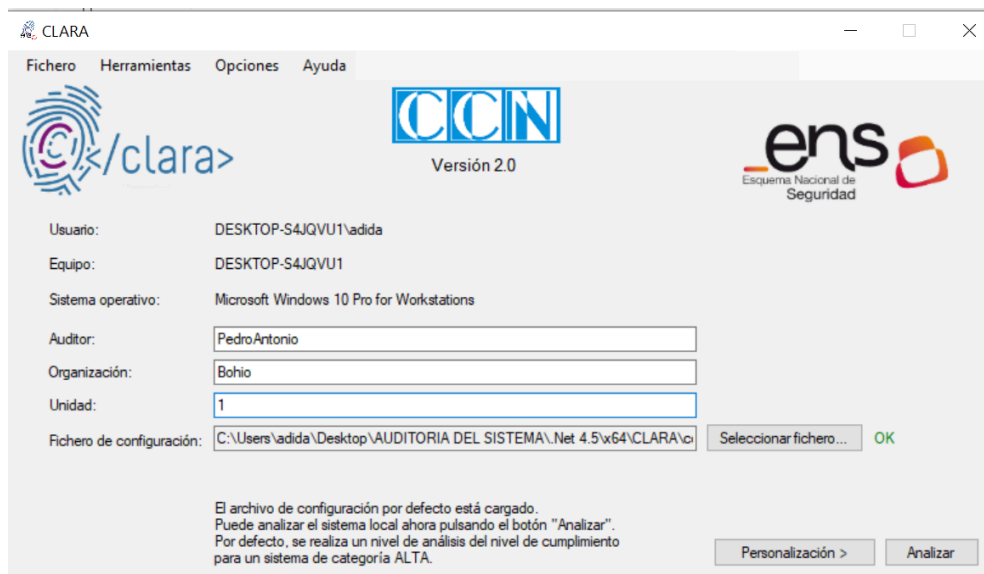


6.2 Ejecución de los análisis

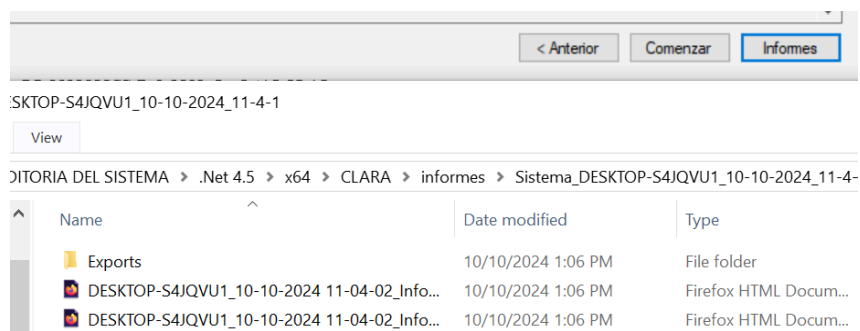
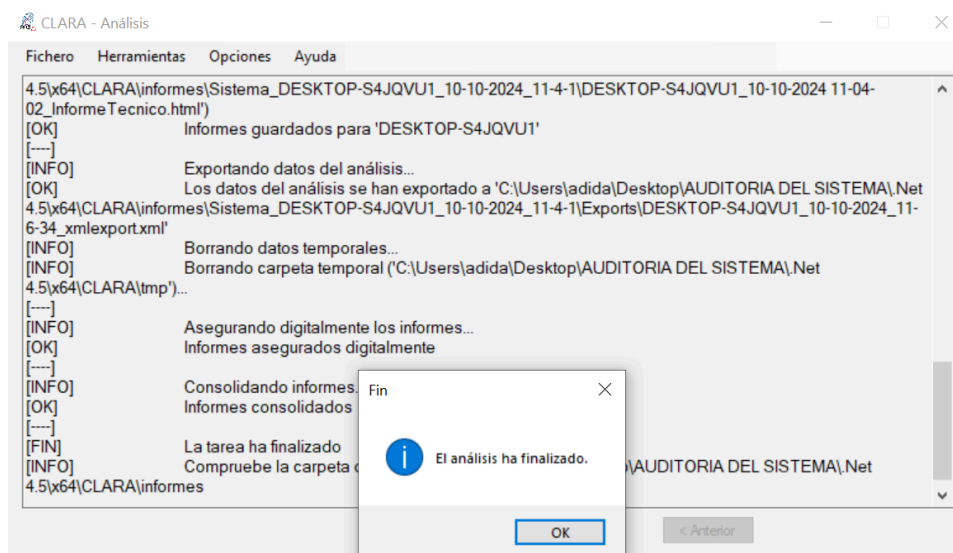
Una vez en la carpeta ejecutamos el ejecutable CLARA con permisos de admin.



Cuando se inicia el programa para poder comenzar con el análisis nos pedirá nombre de auditor, organización y unidad. Los ponemos y hacemos clic en “Analizar”.



Una vez finalizado nos aparecerá una ventana emergente, clicamos al OK y nos aparecerá la opción de ver el informe del análisis ya guardados en una carpeta del sistema.



6.3 Resumen resultados de auditoría

Por motivos de seguridad mostraré solo el resumen de los informes de la auditoría.

Centro Criptológico Nacional



Nombre del sistema: DESKTOP-S4JQVU1
Organización: Bohio
Unidad: 1
Categoría del sistema: ALTA

Auditado por PedroAntonio
Informes generados el día 10/10/2024 11:04:02 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99e5-1647218f2953-09504803-81c9-4de8-a235-3b5bdc3239e1-2f74

Mostrar todo

Resumen

Ocultar

Cumplimiento del sistema - 40,23%

40,23%

Sistema

Ocultar

Nombre del sistema

Sistema operativo

Rol del dominio

Dominio / Grupo de trabajo

Discos

Direcciones IP

DESKTOP-S4JQVU1

Microsoft Windows 10 Pro for Workstations (No hay Service Pack instalado / Internet Explorer: 11.3636.19041.0 / Windows Media Player: 12.0.19041.320)

Cliente independiente

WORKGROUP

C: (NTFS)

192.168.18.43

192.168.56.1

192.168.192.1

Resultados

Control ENS

OP.ACC.5 - Mecanismos de autenticación (0%)

OP.ACC.6 - Acceso local (0%)

OP.EXP.2 - Configuración de seguridad (0%)

OP.EXP.5 - Gestión de cambios (100%)

OP.EXP.6 - Protección frente a código dañino (33,33%)

MPEQ.2 - Bloqueo de puesto de trabajo (0%)

MPEQ.3 - Protección de equipos informáticos (100%) **

Estado del control

Cumplimiento del control *

0%

0%

0%

100%

33,33%

0%

100%

* Cumplimiento de las medidas técnicas del ENS en función del nivel analizado para este sistema.

** Esta prueba solo se realiza en el caso de que el sistema de cifrado Bitlocker se encuentre configurado en el sistema. En caso contrario, deberá evaluar de forma manual el sistema de cifrado del equipo.

Leyenda de estado del control

Leyenda de cumplimiento del control

Cumplimiento satisfactorio del control. No es necesario realizar ninguna acción.

Cumplimiento parcial del control. Es necesaria la revisión del informe técnico.

Incumplimiento del control. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.

Representación visual del porcentaje de elementos del sistema que cumplen satisfactoriamente con el control ENS evaluado.

Representación visual del porcentaje de elementos del sistema que cumplen parcialmente con el control ENS evaluado. Aún no tratándose de un incumplimiento, estos elementos no atienden de forma óptima a las exigencias del ENS. Se hace necesaria la revisión del informe técnico para la posible aplicación de medidas correctoras.

Representación visual del porcentaje de elementos del sistema que no cumplen con el control ENS evaluado.

%

Valor numérico indicativo del porcentaje total de cumplimiento del control ENS evaluado. Engloba tanto los elementos del sistema que cumplen satisfactoriamente con el control, como aquellos elementos que lo hacen parcialmente.

7. Fuentes

<https://keepcoding.io/blog/que-es-lynis/>

<https://soka.gitlab.io/blog/post/2021-07-05-auditorias-seguridad-con-clara/>

https://www.ccn-cert.cni.es/publico/herramientas/clara_ENS/Manual_de_uso_Clara_cumplimiento_ENS_v1.3.pdf

<https://keepcoding.io/blog/que-es-nessus/>

<https://docs.tenable.com/nessus/Content/GettingStarted.htm>