Lynis, auditando sistemas

I.E.S. Gonzalo Nazareno

C.F.P.G.S. Administración de Sistemas Informáticos en Red

Carlos Rivero Martín

Fases

+ Inicio.

- Determinar el sistema operativo y si hay alguna actualización del mismo.
- Comprobación de la versión de Lynis.

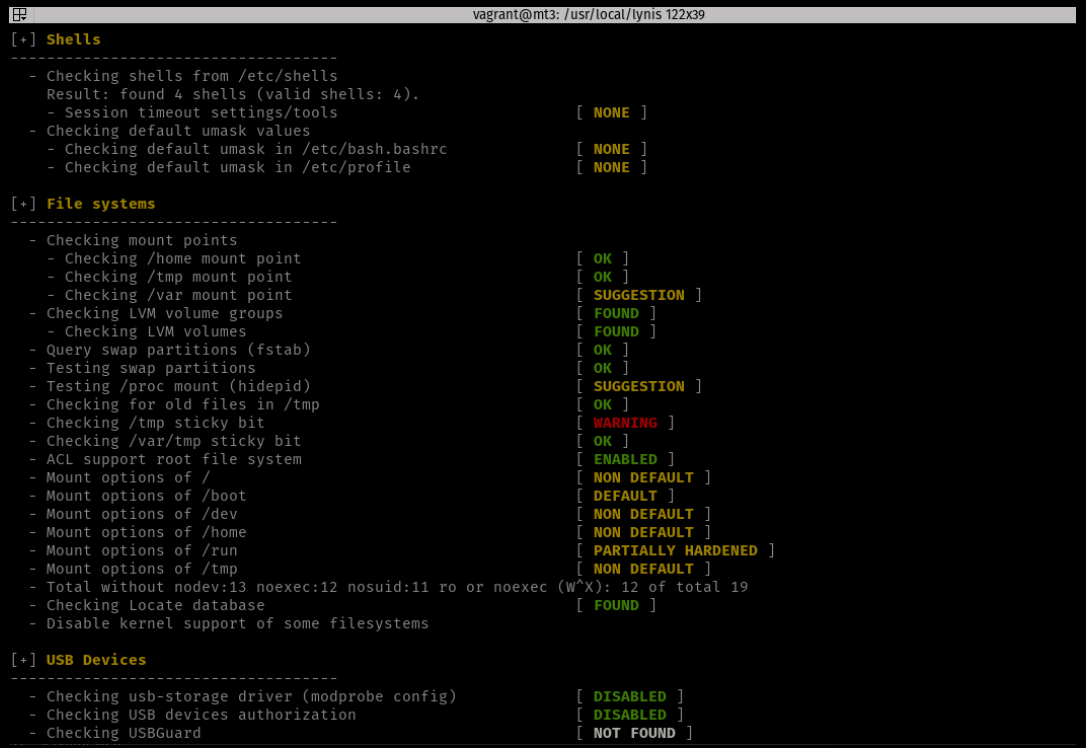
+ Fase 1 de los “plugins”.

+ Test de seguridad por grupos.

+ Fase 2 de los “plugins” y test personalizados.

+ Reporte de estado y resultados obtenidos.

Salida por pantalla



Resultados

```
-[ Lynis 1.3.9 Results ]-

Tests performed: 168

Warnings:
----------------------------
- Version of Lynis very outdated [test:NONE]
- Found possible unused iptables rules (3 4 6 7 8 9 10 11 12 13 14 15 1) [test:FIRE-4513]
```

```
Suggestions:
----------------------------
- update to the latest stable release.
- Run systemctl --full --type=service to see all services
- Run systemctl list-unit-files --type=service to see all services
- Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [test:AUTH-9262]
- Configure password aging limits to enforce password changing on a regular base [test:AUTH-9286]
- Default umask in /etc/login.defs could be more strict like 027 [test:AUTH-9328]
- Default umask in /etc/init.d/rc could be more strict like 027 [test:AUTH-9328]
- To decrease the impact of a full /home file system, place /home on a separated partition [test:FILE-6310]
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition [test:FILE-6310]
- Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [test:STRG-1840]
- Install package apt-show-versions for patch management purposes [test:PKGS-7394]
- Install a package audit tool to determine vulnerable packages [test:PKGS-7398]
- Check CUPS configuration if it really needs to run on several network addresses [test:PRNT-2308]
- Check iptables rules to see which rules are currently not used (iptables --list --numeric --verbose) [test:FIRE-4513]
- Install Apache mod_evasive to guard webserver against DoS/brute force attempts [test:HTTP-6640]
- Install Apache mod_qos to guard webserver against Slowloris attacks [test:HTTP-6641]
- Install Apache mod_spamhaus to guard webserver against spammers [test:HTTP-6642]
- Install Apache modsecurity to guard webserver against web application attacks [test:HTTP-6643]
- Check what deleted files are still in use and why. [test:LOGG-2190]
- Add a legal banner to /etc/issue, to warn unauthorized users [test:BANN-7126]
- Add legal banner to /etc/issue.net, to warn unauthorized users [test:BANN-7130]
- Enable auditd to collect audit information [test:ACCT-9628]
- Install a file integrity tool [test:FINT-4350]
- One or more sysctl values differ from the scan profile and could be tweaked [test:KRNL-6000]
- Harden the system by removing unneeded compilers. This can decrease the chance of customized trojans, backdoors and rootkits to be compiled an
d installed [test:HRDN-7220]
- Harden compilers and restrict access to world [test:HRDN-7222]
- Harden the system by installing one or malware scanners to perform periodic file system scans [test:HRDN-7230]
================================================================================
```

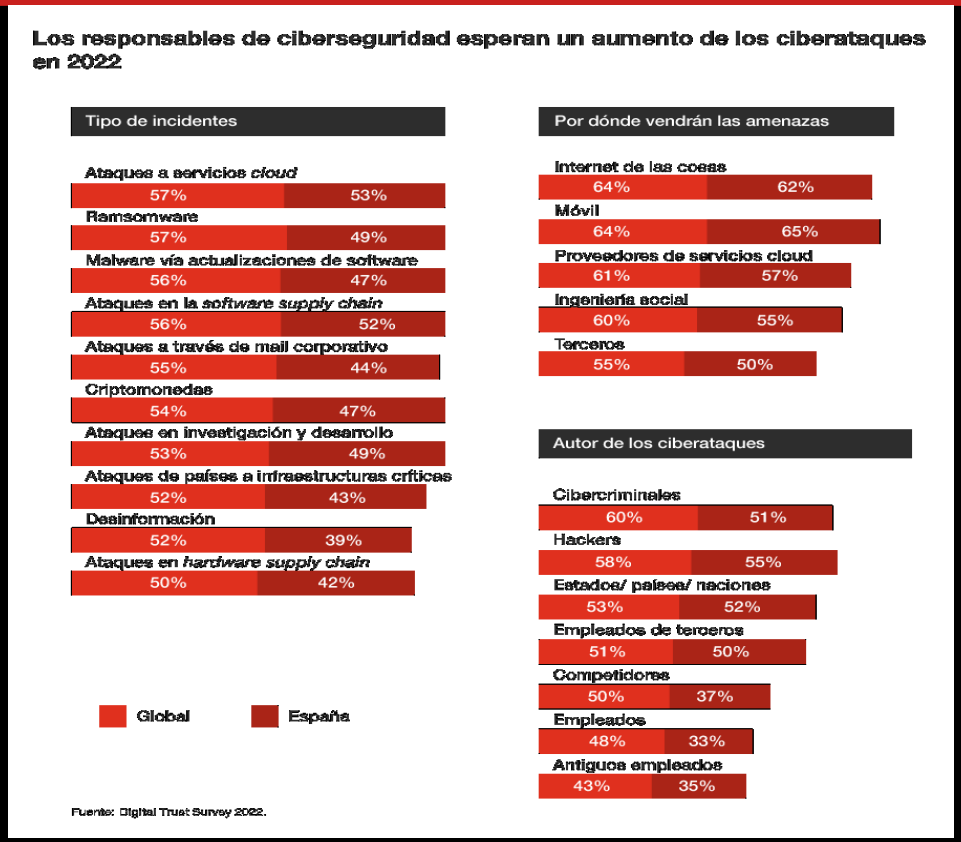
Reportes


vagrant@mt3: /usr/local/lynis 122x39
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/lynis/controls/HRDN-7222/
Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /home/vagrant/auditoria2.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 : 71 [##############]
Tests performed : 279
Plugins enabled : 2
Components:
- Firewall [V]
- Malware scanner [V]
Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]
Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
Files:
- Test and debug information : /home/vagrant/auditoria2.log
- Report data : /var/log/lynis-report.dat
Lynis 3.0.8

Ventajas y desventajas de Lynis

VENTAJAS	DESVENTAJAS
Facilidad de uso	Dificultad de interpretar resultados
Da mucha información del sistema	El uso avanzado requiere grandes conocimientos de “shell script”
Ofrece sugerencias	Necesita una gran planificación
Permite comprobaciones por grupos	Existencia de la versión para empresas

La importancia de la ciberseguridad



¡GRACIAS!

crivmar

@crivmar88