



Universidad
del Caribe

2000

CANCUN, QUINTANA ROO, MÉXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

UNIVERSIDAD DEL CARIBE

HARDENING DE UN CENTOS7

INGENIERÍA EN DATOS E INTELIGENCIA
ORGANIZACIONAL

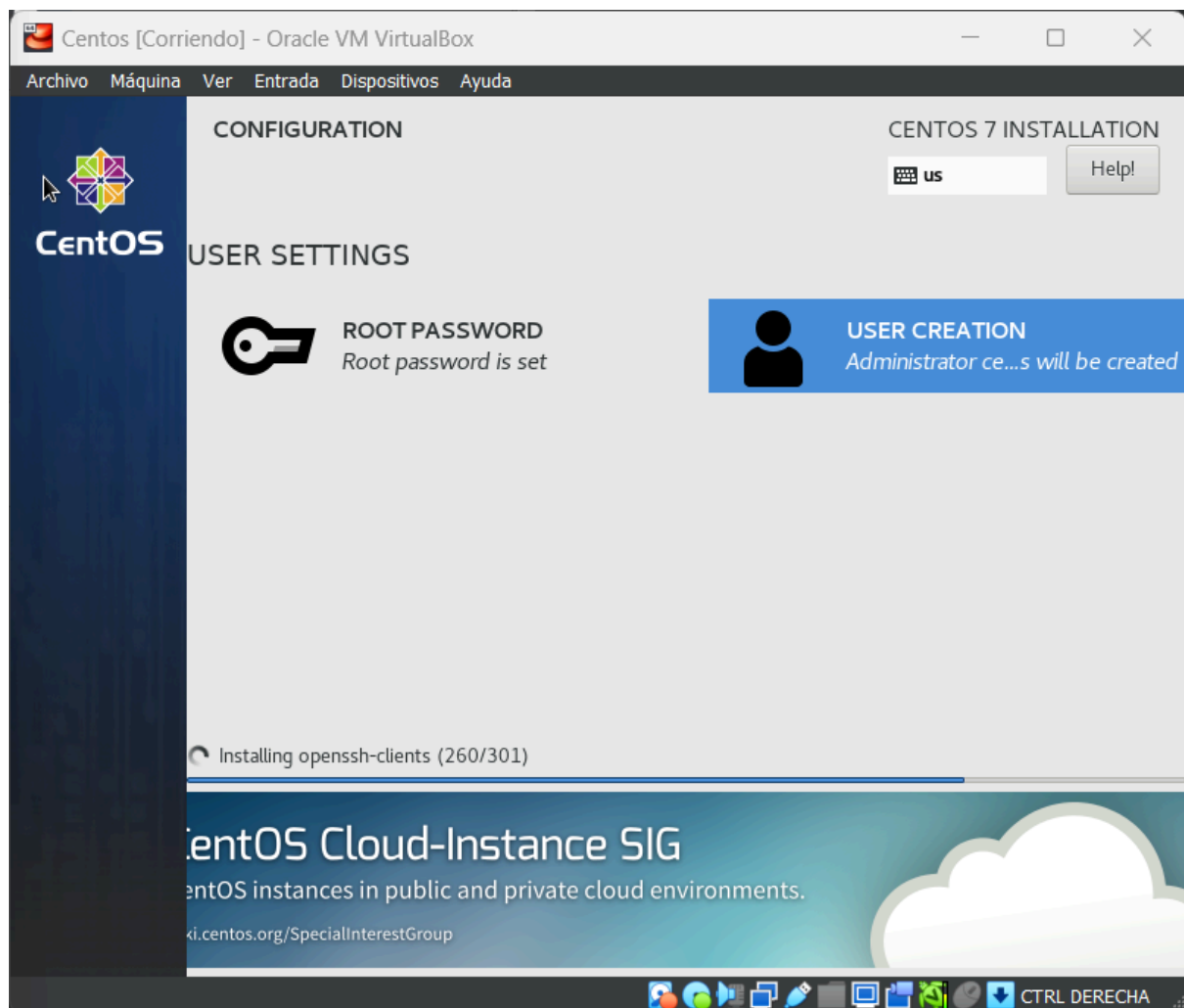
30 DE ABRIL DEL 2024

LESSTER MAC WILLIAMS ROMERO


En esta práctica, nos enfocaremos en fortalecer la seguridad de un sistema CentOS 7 mediante el proceso de hardening, utilizando un agente de Wazuh para validar la configuración de seguridad. Siguiendo una guía paso a paso, instalaremos el agente de Wazuh en una máquina virtual CentOS 7 en VirtualBox y aplicaremos el script de hardening proporcionada.

Script obtenido del repositorio de Tuxttter: <https://github.com/tuxttter/hardening>

Prevía instalación y configuración del CentOS7. Se configuró la red para que tuviera conexión y estuviera conectada a la red de mi computadora, para realizar la práctica.



Observamos cómo ha avanzado el porcentaje del hardening.


SCA: Lastest scans 

CIS CentOS Linux 7 Benchmark v3.0.0 cis_centos7_linux

| Policy | End scan | Passed | Failed | Not applica... | Score |
|-------------------------------------|-----------------------------|--------|--------|----------------|-------|
| CIS CentOS Linux 7 Benchmark v3.0.0 | Apr 30, 2024 @ 19:37:12.000 | 76 | 107 | 13 | 41% |

< 1 >

Posteriormente a las demás configuraciones podemos observar nuevamente cómo el porcentaje incrementó.

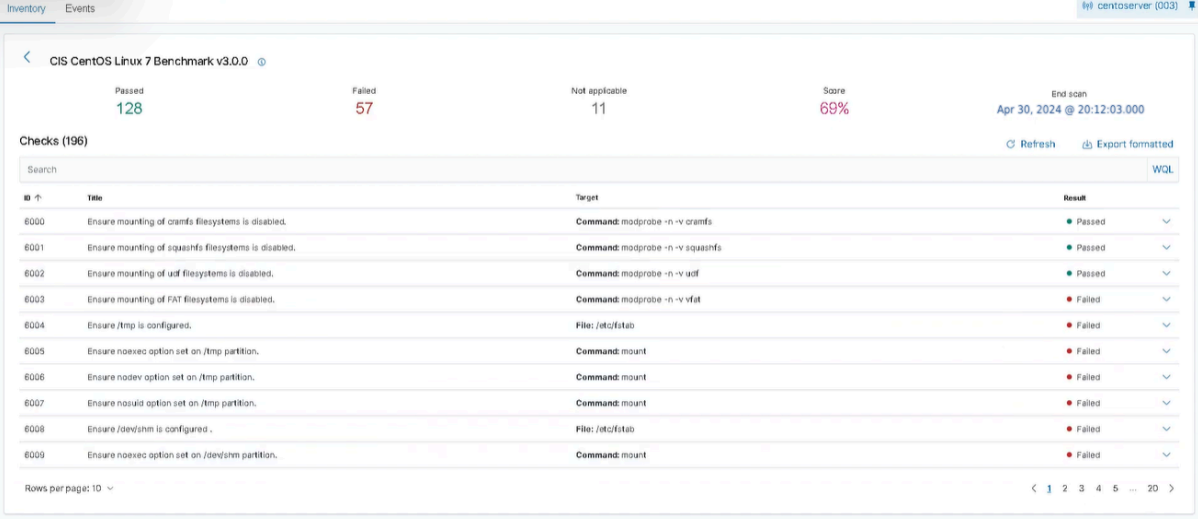
SCA: Lastest scans 

CIS CentOS Linux 7 Benchmark v3.0.0 cis_centos7_linux

| Policy | End scan | Passed | Failed | Not applica... | Score |
|-------------------------------------|-----------------------------|--------|--------|----------------|-------|
| CIS CentOS Linux 7 Benchmark v3.0.0 | Apr 30, 2024 @ 20:11:09.000 | 128 | 57 | 11 | 69% |

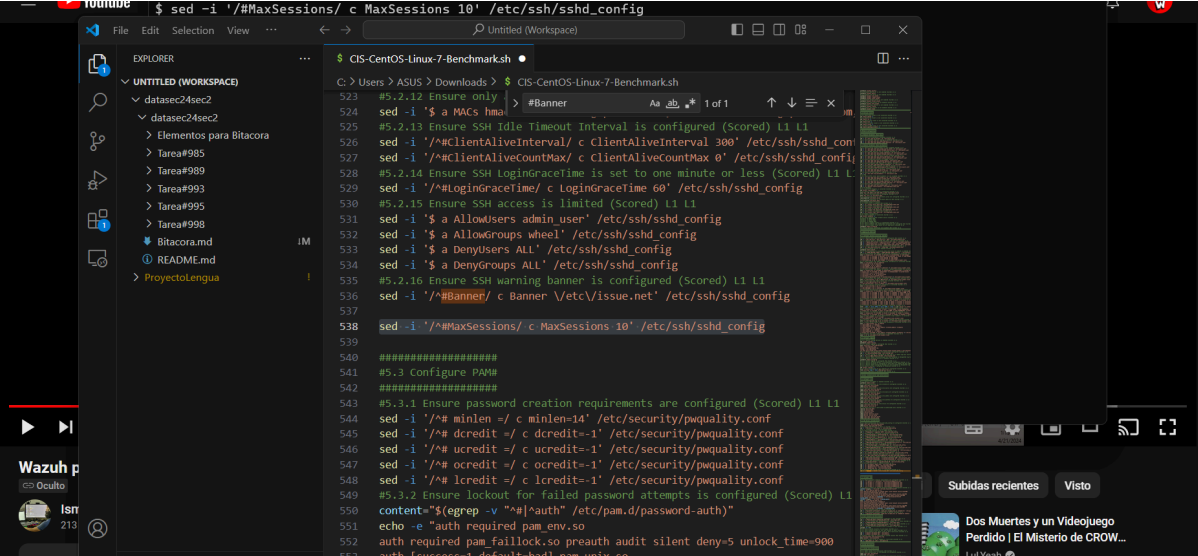
< 1 >

Si se clickea en él podemos ver todos los comandos, los que pudieron funcionar bien, los fallidos y a los que no se aplicó. observamos el nuevo score.



| ID | Title | Target | Result |
|------|--|----------------------------------|--------|
| 6000 | Ensure mounting of cramfs filesystems is disabled. | Command: modprobe -n -v cramfs | Passed |
| 6001 | Ensure mounting of squashfs filesystems is disabled. | Command: modprobe -n -v squashfs | Passed |
| 6002 | Ensure mounting of udf filesystems is disabled. | Command: modprobe -n -v udf | Passed |
| 6003 | Ensure mounting of FAT filesystems is disabled. | Command: modprobe -n -v vfat | Failed |
| 6004 | Ensure /tmp is configured. | File: /etc/fstab | Failed |
| 6005 | Ensure noexec option set on /tmp partition. | Command: mount | Failed |
| 6006 | Ensure noexec option set on /tmp partition. | Command: mount | Failed |
| 6007 | Ensure noexec option set on /tmp partition. | Command: mount | Failed |
| 6008 | Ensure /dev/shm is configured. | File: /etc/fstab | Failed |
| 6009 | Ensure noexec option set on /dev/shm partition. | Command: mount | Failed |

Llegamos hasta el punto que vemos a continuación.



```
$ sed -i '/^#MaxSessions/ c MaxSessions 10' /etc/ssh/sshd_config
```

```
CIS-CentOS-Linux-7-Benchmark.sh
523 #5.2.12 Ensure only
524 sed -i '$ a MACs hma
525 #5.2.13 Ensure SSH Idle Timeout Interval is configured (Scored) L1 L1
526 sed -i '/^#ClientAliveInterval/ c ClientAliveInterval 300' /etc/ssh/sshd_conf
527 sed -i '/^#ClientAliveCountMax/ c ClientAliveCountMax 0' /etc/ssh/sshd_conf
528 #5.2.14 Ensure SSH LoginGraceTime is set to one minute or less (Scored) L1 L
529 sed -i '/^#LoginGraceTime/ c LoginGraceTime 60' /etc/ssh/sshd_config
530 #5.2.15 Ensure SSH access is limited (Scored) L1 L1
531 sed -i '$ a AllowUsers admin user' /etc/ssh/sshd_config
532 sed -i '$ a AllowGroups wheel' /etc/ssh/sshd_config
533 sed -i '$ a DenyUsers ALL' /etc/ssh/sshd_config
534 sed -i '$ a DenyGroups ALL' /etc/ssh/sshd_config
535 #5.2.16 Ensure SSH warning banner is configured (Scored) L1 L1
536 sed -i '/^#Banner/ c Banner "/etc/issue.net"' /etc/ssh/sshd_config
537
538 sed -i '/^#MaxSessions/ c MaxSessions 10' /etc/ssh/sshd_config
539
540 #####
541 #5.3 Configure PAM#
542 #####
543 #5.3.1 Ensure password creation requirements are configured (Scored) L1 L1
544 sed -i '/^# minlen =/ c minlen=14' /etc/security/pwquality.conf
545 sed -i '/^# dcredit =/ c dcredit=1' /etc/security/pwquality.conf
546 sed -i '/^# ucredit =/ c ucredit=1' /etc/security/pwquality.conf
547 sed -i '/^# ocredit =/ c ocredit=1' /etc/security/pwquality.conf
548 sed -i '/^# lcredit =/ c lcredit=1' /etc/security/pwquality.conf
549 #5.3.2 Ensure lockout for failed password attempts is configured (Scored) L1
550 content="$(egrep -v "^#|^auth" /etc/pam.d/password-auth)"
551 echo -e "auth required pam_env.so
552 auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
553 auth [success=1 default=bad] pam_unix.so"
```