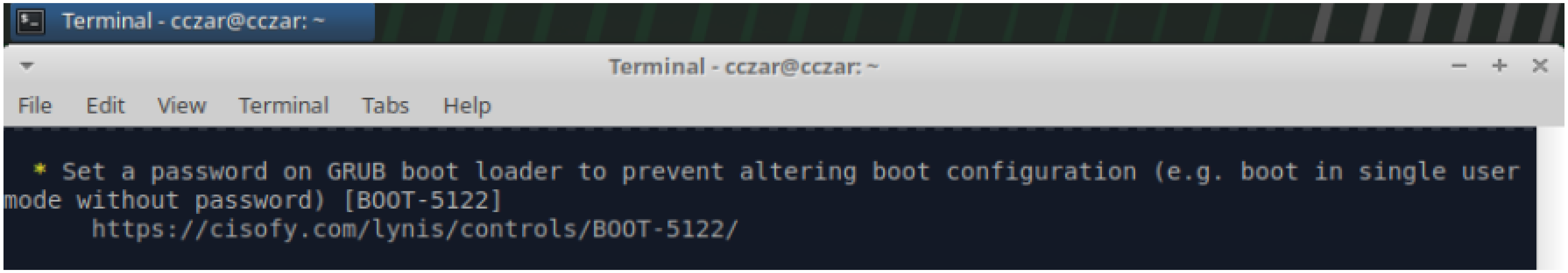
Finding: GRUB Bootloader Unprotected (BOOT-1003)

NIST Control Mapping: PR.PS-01: Configuration management practices are established and applied
Risk: Without a GRUB boot password, an attacker with physical access could modify boot parameters to bypass authentication controls, disable security mechanisms, or gain root access.
Severity: High
Remediation: Configure a GRUB boot password to ensure that only authorized administrators can modify boot parameters.

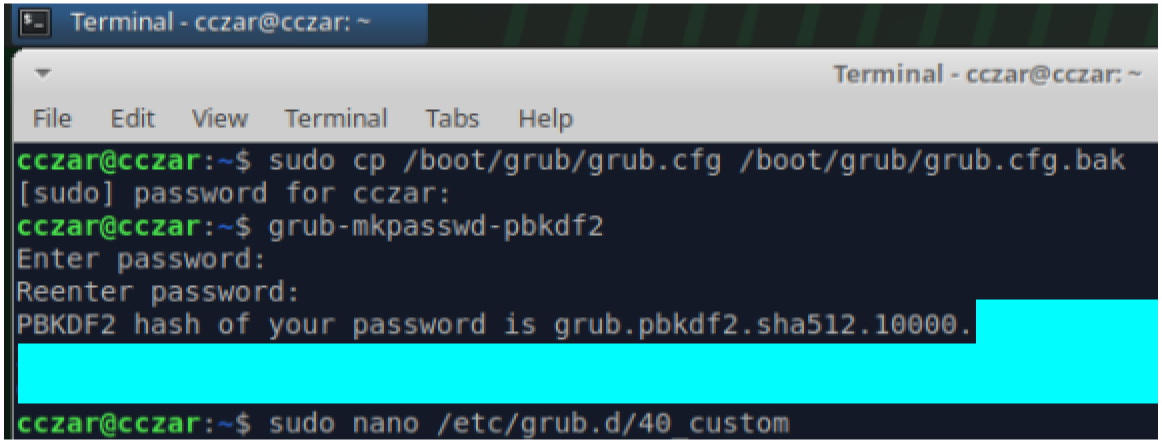
INITIAL LYNIS SCAN RESULT



```
  * 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/
```

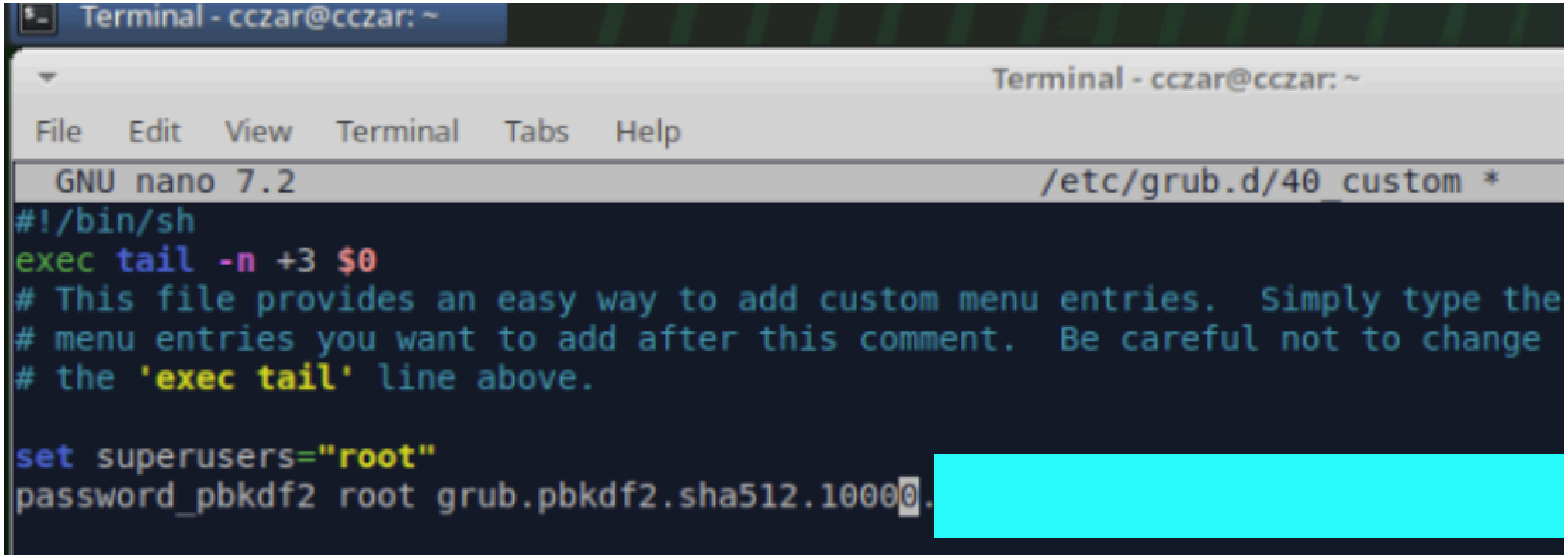
REMEDIATION PROCESS

1. Generated a GRUB Password Hash (hash is hidden for security purposes)



```
cczar@cczar:~$ sudo cp /boot/grub/grub.cfg /boot/grub/grub.cfg.bak
[sudo] password for cczar:
cczar@cczar:~$ grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.[redacted]
cczar@cczar:~$ sudo nano /etc/grub.d/40_custom
```

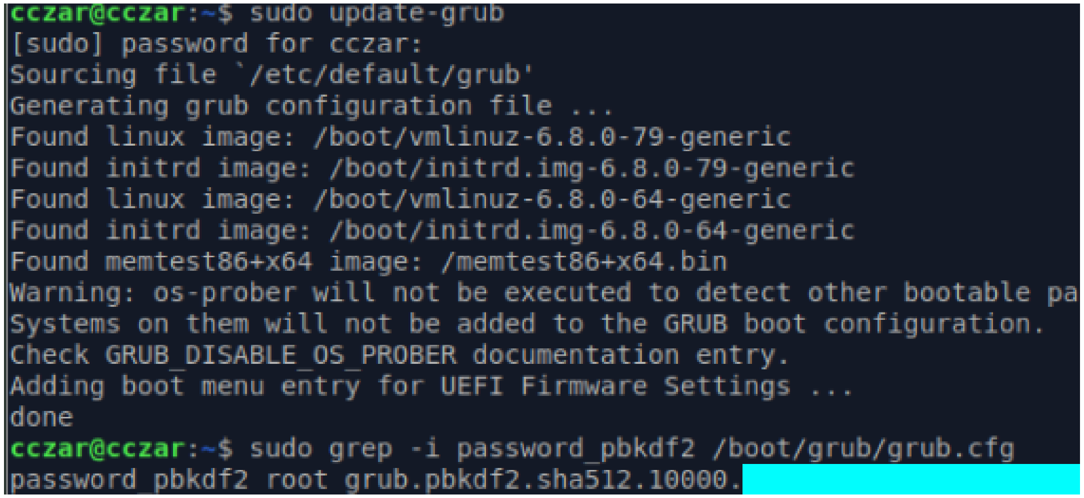
2. Configured GRUB



```
 GNU nano 7.2                                          /etc/grub.d/40_custom *
#!/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.

set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.[redacted]
```

3. Rebuilt the GRUB configuration to incorporate the changes from 40_custom, ran the update command, and verified password line was applied



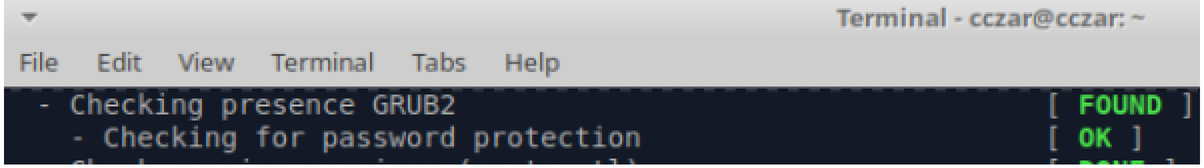
```
cczar@cczar:~$ sudo update-grub
[sudo] password for cczar:
Sourcing file `/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-79-generic
Found initrd image: /boot/initrd.img-6.8.0-79-generic
Found linux image: /boot/vmlinuz-6.8.0-64-generic
Found initrd image: /boot/initrd.img-6.8.0-64-generic
Found memtest86+x64 image: /memtest86+x64.bin
Warning: os-prober will not be executed to detect other bootable pa
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
cczar@cczar:~$ sudo grep -i password_pbkdf2 /boot/grub/grub.cfg
password_pbkdf2 root grub.pbkdf2.sha512.10000.[redacted]
```

4. Tested GRUB configuration

- After reboot, at the GRUB menu, pressing “e” to edit boot entry prompted for the password configured in /etc/grub.d/40_custom. Entering the correct password allowed the system to boot normally, confirming that GRUB hardening is in effect.

Note: To further secure the system against unauthorized physical access, it is recommended to restrict root login on virtual and physical consoles (TTYs).

LYNIS SCAN RESULT AFTER REMEDIATION



```
  - Checking presence GRUB2                                    [ FOUND ]
    - Checking for password protection                         [ OK ]
```