

Finding: USB Storage Driver Enabled (USB-1001)

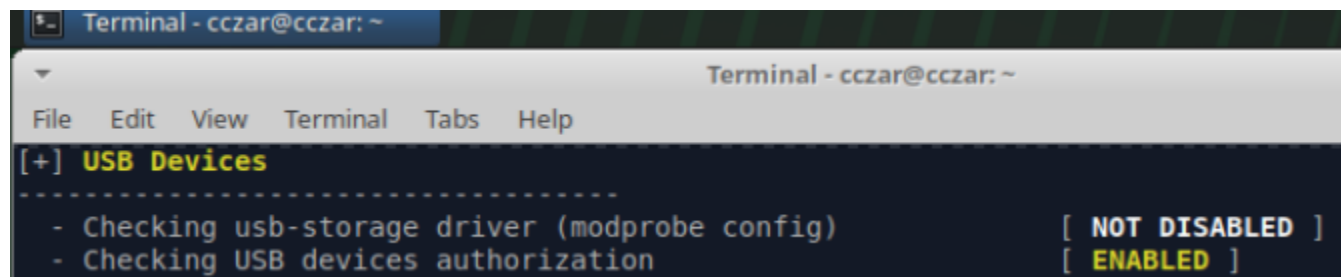
NIST Control Mapping: PR.DS-01 – The confidentiality, integrity, and availability of data-at-rest are protected

Risk: The USB storage driver is enabled, allowing unauthorized users to transfer sensitive data via USB devices.

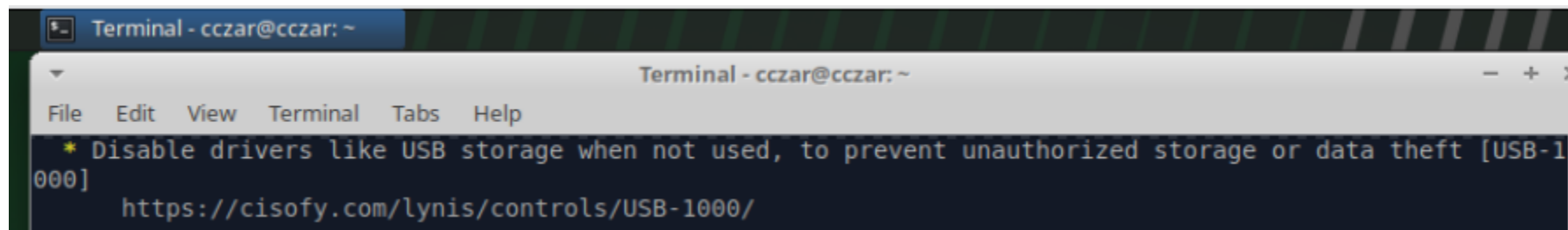
Severity: High

Remediation: Disable the USB storage driver to prevent data exfiltration via USB.

INITIAL LYNIS SCAN RESULT



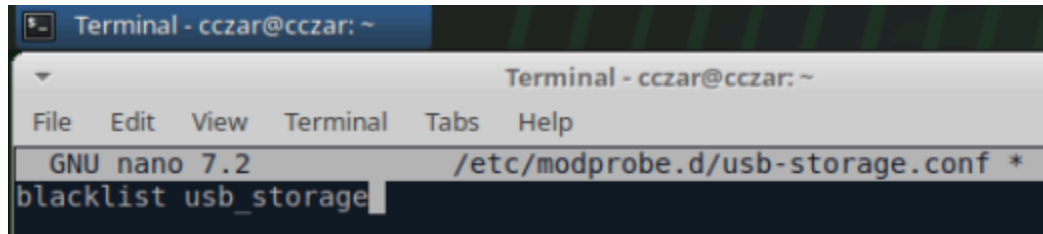
```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help
[+] USB Devices
-----
- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ ENABLED ]
```



```
Terminal - cczar@cczar: ~
File Edit View Terminal Tabs Help
* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
https://cisofy.com/lynis/controls/USB-1000/
```

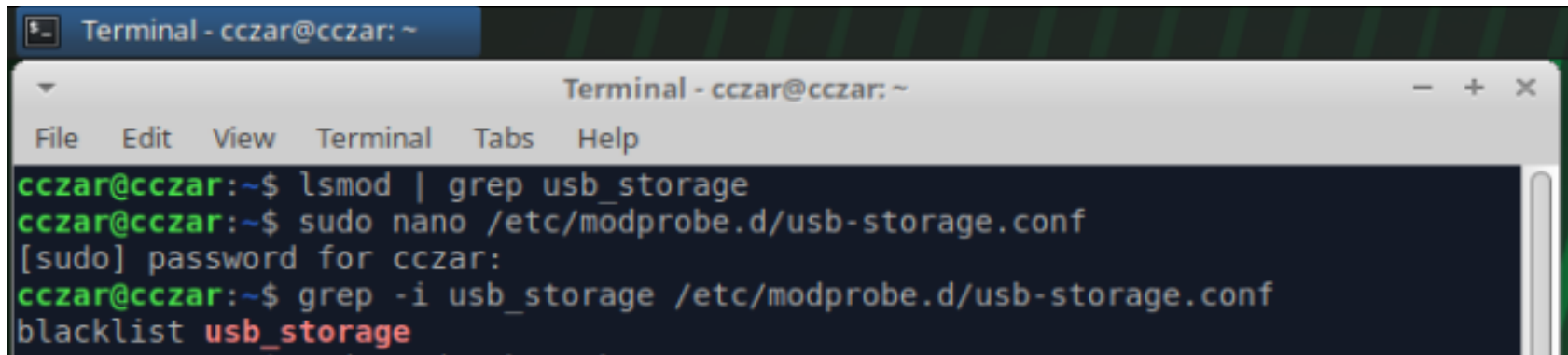
REMEDIATION PROCESS

1. Verified USB storage driver was unloaded and created blacklist file for modprobe to prevent USB storage driver from loading



```
Terminal - cczar@cczar: ~
GNU nano 7.2 /etc/modprobe.d/usb-storage.conf *
blacklist usb_storage
```

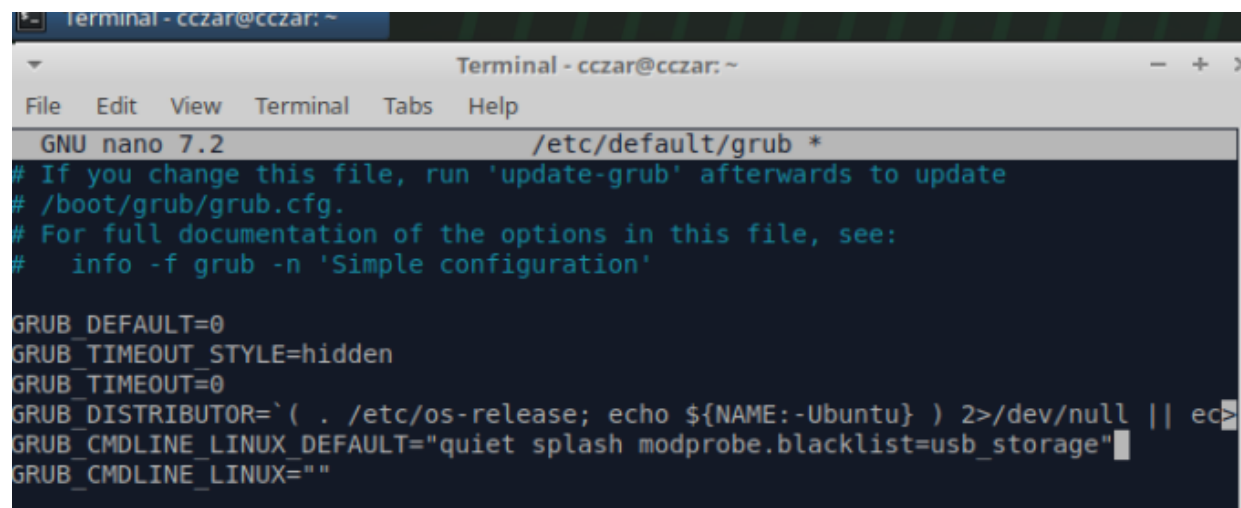
2. Confirmed blacklist status of USB storage driver



```
Terminal - cczar@cczar: ~
cczar@cczar:~$ lsmod | grep usb_storage
cczar@cczar:~$ sudo nano /etc/modprobe.d/usb-storage.conf
[sudo] password for cczar:
cczar@cczar:~$ grep -i usb_storage /etc/modprobe.d/usb-storage.conf
blacklist usb_storage
```

3. Disabled the USB module via kernel parameters

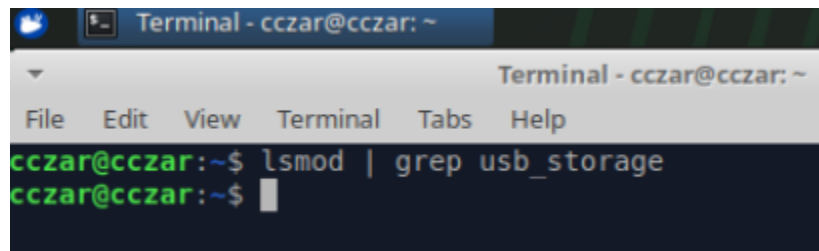
```
cczar@cczar:~$ grep -i usb_storage /etc/modprobe.d/usb-storage.conf
blacklist usb_storage
cczar@cczar:~$ sudo modprobe usb_storage
cczar@cczar:~$ lsmod | grep usb_storage
usb_storage                86016  0
cczar@cczar:~$ sudo nano /etc/default/grub
cczar@cczar:~$ lsmod | grep usb_storage
usb_storage                86016  0
cczar@cczar:~$ sudo update-grub
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 partitions.
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
```



```
Terminal - cczar@cczar: ~
GNU nano 7.2 /etc/default/grub *
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
# info -f grub -n 'Simple configuration'

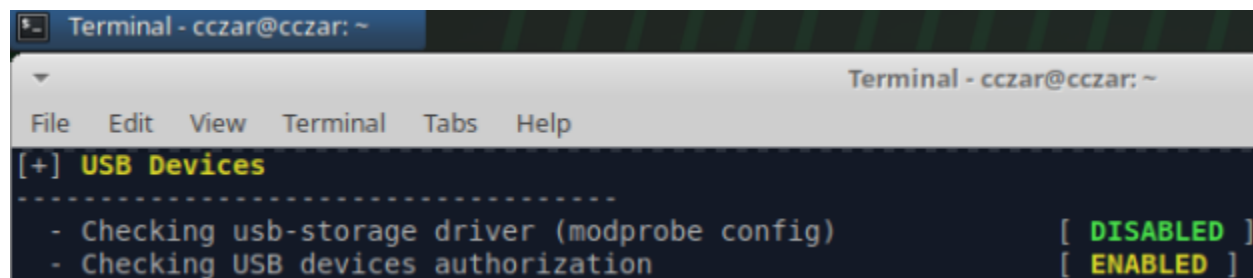
GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`(. /etc/os-release; echo ${NAME:-Ubuntu}) 2>/dev/null || ec>
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash modprobe.blacklist=usb_storage"
GRUB_CMDLINE_LINUX=""
```

4. After applying the USB storage module blacklist and updating the kernel parameters, a reboot shows `lsmod | grep usb_storage` does not return the module, confirming the module is no longer loaded at boot and the hardening is effective.



```
Terminal - cczar@cczar: ~  
File Edit View Terminal Tabs Help  
cczar@cczar:~$ lsmod | grep usb_storage  
cczar@cczar:~$
```

LYNIS SCAN RESULT AFTER REMEDIATION



```
Terminal - cczar@cczar: ~  
File Edit View Terminal Tabs Help  
[+] USB Devices  
-----  
- Checking usb-storage driver (modprobe config) [ DISABLED ]  
- Checking USB devices authorization [ ENABLED ]
```