

Finding: Insecure Permissions on /etc/sudoers.d (PERM-1005)

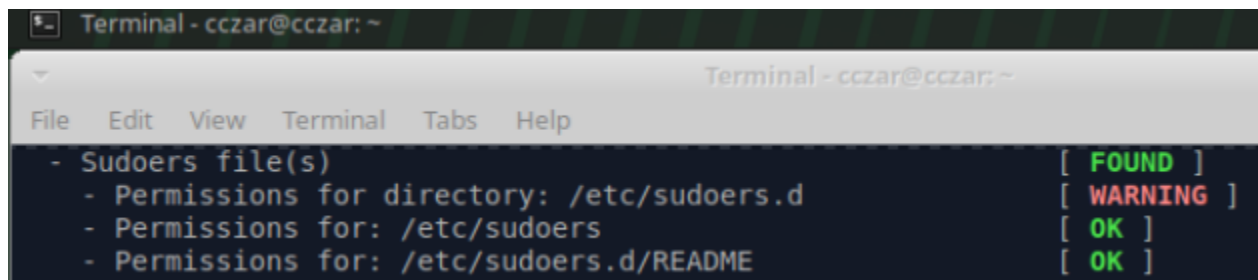
NIST Control Mapping: PR.AA-05 – Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

Risk: The [/etc/sudoers.d](#) directory has insecure permissions, which could allow unauthorized users to modify sudo configuration files, potentially leading to privilege escalation.

Severity: High

Remediation: Review and correct the permissions on the [/etc/sudoers.d](#) directory to ensure only authorized users can modify them.

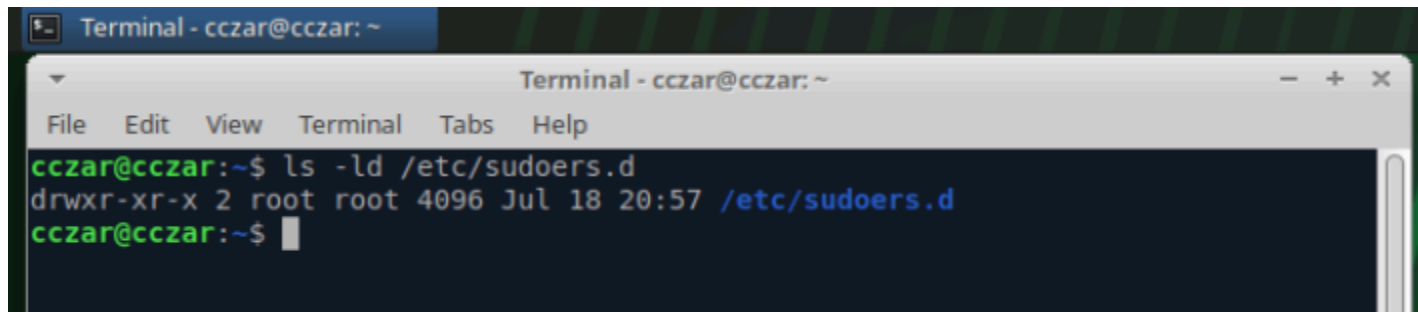
INITIAL LYNIS SCAN RESULT



```
Terminal - cczar@cczar: ~  
File Edit View Terminal Tabs Help  
- Sudoers file(s) [ FOUND ]  
- Permissions for directory: /etc/sudoers.d [ WARNING ]  
- Permissions for: /etc/sudoers [ OK ]  
- Permissions for: /etc/sudoers.d/README [ OK ]
```

REMEDIATION PROCESS

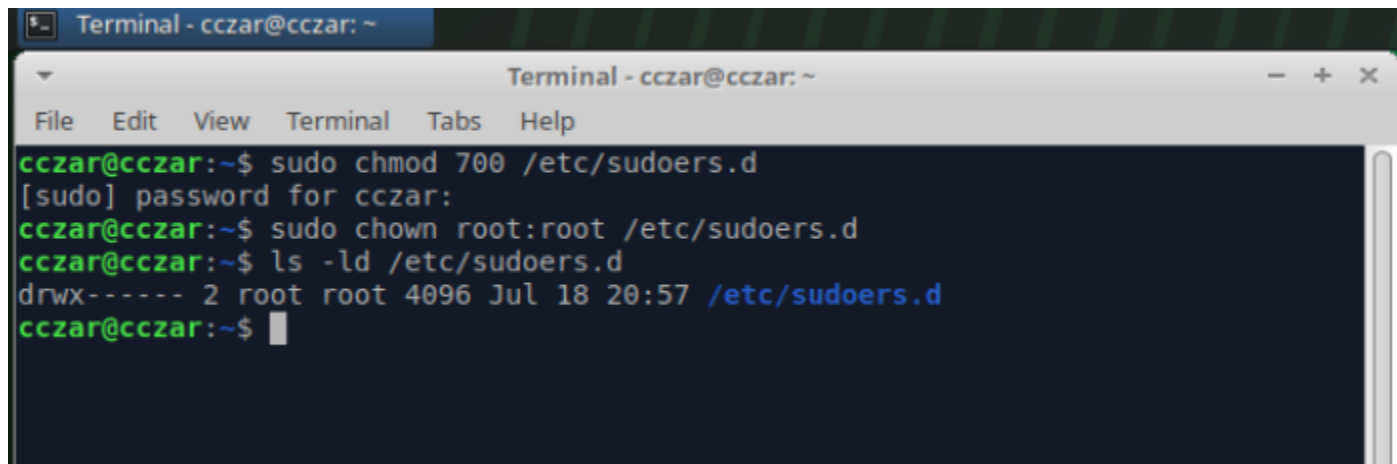
1. Reviewed current permissions, verifying that group and others have read/execute access to [/etc/sudoers.d](#) directory



```
Terminal - cczar@cczar: ~  
File Edit View Terminal Tabs Help  
cczar@cczar:~$ ls -ld /etc/sudoers.d  
drwxr-xr-x 2 root root 4096 Jul 18 20:57 /etc/sudoers.d  
cczar@cczar:~$
```

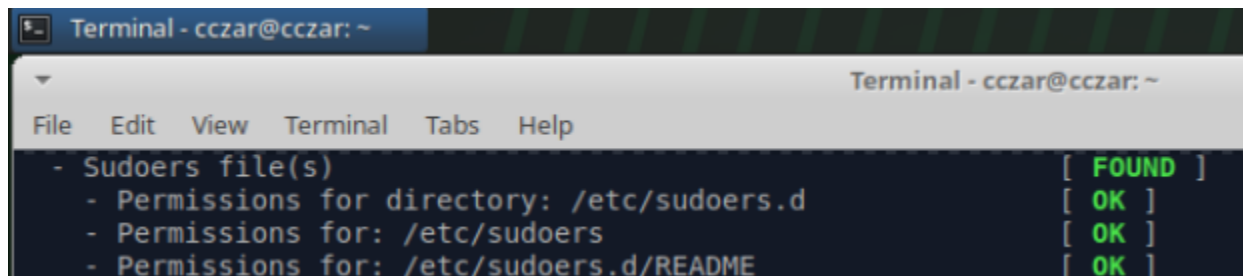
2. Restricted permissions to root-only, with group and others having no access, and verified permission change.

Note: Restricted the `/etc/sudoers.d` directory permissions so that only root can read, write, or execute. After updating permissions, `/etc/sudoers.d` is owned by root with access limited to root-only. Listing the directory confirms permissions set to `700`, ensuring that unauthorized users cannot modify sudo configuration files and mitigating the risk of privilege escalation.



```
Terminal - cczar@cczar: ~  
cczar@cczar:~$ sudo chmod 700 /etc/sudoers.d  
[sudo] password for cczar:  
cczar@cczar:~$ sudo chown root:root /etc/sudoers.d  
cczar@cczar:~$ ls -ld /etc/sudoers.d  
drwx----- 2 root root 4096 Jul 18 20:57 /etc/sudoers.d  
cczar@cczar:~$
```

LYNIS SCAN RESULT AFTER REMEDIATION



```
Terminal - cczar@cczar: ~  
- Sudoers file(s) [ FOUND ]  
- Permissions for directory: /etc/sudoers.d [ OK ]  
- Permissions for: /etc/sudoers [ OK ]  
- Permissions for: /etc/sudoers.d/README [ OK ]
```