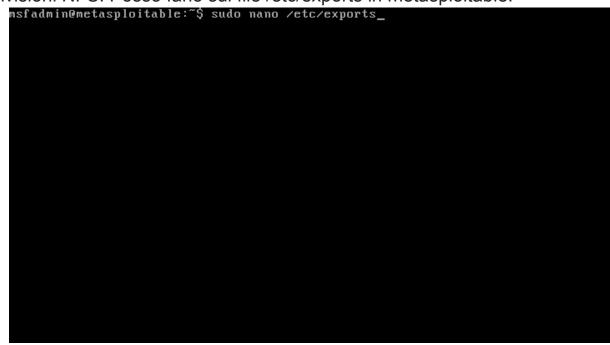
Remediation

Vulnerability: NFS Exported Share Information Disclosure **Soluzione:**

Come possiamo quindi prevenire gli attacchi a questa vulnerabilità?

Innanzitutto, posso limitare l'accesso. Posso specificare indirizzi IP o subnet specifici a cui è consentito accedere alle condivisioni NFS. Posso farlo sul file /etc/exports in metasploitable.



Quindi posso digitare gli indirizzi IP o le subnet che desidero nell'editor di testo.

Posso configurare le regole del firewall come un altro metodo. Posso impostare le regole del firewall per consentire solo il traffico NFS necessario. Ad esempio, posso usare *ufw* .

```
msfadmin@metasploitable:~$ sudo ufw allow from 192.168.50.120 to any port 2049
Rules updated
msfadmin@metasploitable:~$ _
```

Vulnerability: Bind Shell Backdoor Detection

Ho tentato di chiudere questa porta usando il comando fuser.

```
display unused files too
    -a
    -c
              mounted FS
    -\mathbf{f}
              silently ignored (for POSIX compatibility)
              ask before killing (ignored without -k)
    – i
              kill processes accessing the named file
    -\mathbf{k}
    -1
              list available signal names
              show all processes using the named filesystems
    -m
    -n SPACE search in this name space (file, udp, or tcp)
              silent operation
    -5
    -SIGNAL
              send this signal instead of SIGKILL
              display user IDs
    -\mathbf{u}
              verbose output
    -u
    −U
              display version information
              search IPv4 sockets only
    -4
              search IPv6 sockets only
    -6
              reset options
 udp/tcp names: [local_port][,[rmt_host][,[rmt_port]]]
nsfadmin@metasploitable:~$ sudo fuser -k -n tcp 1524
[sudo] password for msfadmin:
1524/tcp:
                       4509
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

- -k = uccide il processo
- -n = id processo