

## Remediation meta



## Scan meta

---

Report generated by Nessus™

Thu, 24 Nov 2022 09:12:45 EST

---

## 51988 - Bind Shell Backdoor Detection:

Per la risoluzione di questa minaccia si può procedere in questo modo: andiamo sulla shell di meta e avremmo bisogno dei privilegi di root (SUDO), andiamo a digitare il comando **iptables** questo comando corrisponde al firewall dei sistemi operativi LINUX, per andare a bloccare il traffico verso la porta 1524 il comando è il seguente: **iptables -I INPUT -p tcp --dport 1524 -j DROP**.

Ho eseguito poi il comando: **iptables -L** per controllare che la regola sia stata inserita correttamente.

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  anywhere              anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin# _
```

## 11356 - NFS Exported Share Information Disclosure:

Per ovviare a questo problema dobbiamo andare sulla shell di meta avere i privilegi root(SUDO) la procedura è la seguente. Accedere al file di configurazione del NFS con il comando nano /etc/exports e come si può vedere nell'ultima riga c'è \* che permette la comunicazione, per permettere la comunicazione dobbiamo sostituire \* con l'hostname delle macchine autorizzate.

Ho inserito l'IP di meta così da non permettere la comunicazione con altri client.

```
GNU nano 2.0.7      File: /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
192.168.90.101(rw,sync,no_root_squash,no_subtree_check)

[ Wrote 12 lines ]
root@metasploitable:/home/msfadmin#
```

**61708 - VNC Server 'password' Password:** Per risolvere questa criticità la soluzione è la seguente: andare nella shell di meta eseguire il comando **vncpasswd** e inserire una password più complessa

```
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)?
```