

ESERCIZIO W12D4

La seconda parte del progetto di fine modulo verte sul risolvimento da 2 fino 4 vulnerabilità trovate con il Vulnerability scanner Nessus. Una volta conclusa la scansione, e esportato un report iniziale, non ci resta apportare modifiche.

Prima vulnerabilità

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

Secondo lo scanner, il servizio NFS espone gran parte delle directory, rendendole di fatto montabili su sistemi client esterni. Non dovrebbero essere accessibili da tutti, ma solo dall'utenza autorizzata. Per correggere questa vulnerabilità andiamo a cambiare la configurazione del servizio NFS direttamente da dentro Metasploitable. Andremo a creare una cartella privata con mkdir e la renderemo visibile solo da localhost.

```
[ Read 12 lines ]
nsfadmin@metasploitable:/etc$ cd ..
nsfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  root  sys  var
boot   etc    initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom  home  lib     mnt        proc       srv   usr
nsfadmin@metasploitable:/$ sudo mkdir privateshare
nsfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  proc  srv  usr
boot   etc    initrd.img  media      opt        root  sys  var
cdrom  home  lib     mnt        privateshare  sbin  tmp  vmlinuz
nsfadmin@metasploitable:/$ sudo chmod 777 privateshare
nsfadmin@metasploitable:/$
```

Creazione cartella privateshare

Una volta fatto, accediamo al file di testo localizzato in /etc/exports. Usiamo sudo nano per aprire il foglio e specifichiamo la cartella privateshare come usufruibile solo da Metasploitable.

```
# /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)
#
/private share localhost(rw,sync,no_root_squash,no_subtree_check)
```

Configurazione Exports

Salviamo le nuove impostazioni e riavviamo Metasploitable2. Più tardi useremo un'altra volta il Vulnerability Scanner, ma ci accertiamo lo stesso della scongiurata vulnerabilità, andando ad effettuare un tentativo di montaggio sulla macchina attaccante. Creiamo una cartella mount per la condivisione, dentro la directory temp.

```
(kali@kali)-[~]
$ sudo mkdir /tmp/mount
(kali@kali)-[~]
$ cd /tmp/
(kali@kali)-[/tmp]
$ ls
mount
ssh-WFCqLZccCy54
systemd-private-08049c2fcef4095801f31b2af9553b8-colord.service-MpxpTu
systemd-private-08049c2fcef4095801f31b2af9553b8-ha
systemd-private-08049c2fcef4095801f31b2af9553b8-Mo
systemd-private-08049c2fcef4095801f31b2af9553b8-po
(kali@kali)-[/tmp]
$ sudo mount -t nfs 192.168.50.100:/privateshare /tmp/mount -nocheck
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /usr/lib/systemd/system/rpc-statd.service.
mount.nfs: access denied by server while mounting 192.168.50.100:/privateshare
(kali@kali)-[/tmp]
$
```

Creazione cartella e tentativo di montaggio

`sudo mount -t nfs 192.168.50.100:/privateshare /tmp/mount -nolock` è la sintassi che ci consentirà di tentare un montaggio di rete:

- `mount` viene utilizzato per montare un file system
- `-t nfs` indica il tipo di file system da montare, in questo `nfs`
- `192.168.50.100:/privateshare` specifica l'indirizzo IP del server NFS e la directory condivisa da montare.
- `/tmp/mount` specifica il punto di mount locale in cui verrà montata la cartella condivisa.
- `-nolock` specifica che il mount deve essere effettuato senza il lock manager NFS.

Da come si evince dallo screenshot, non è stato possibile completare il montaggio di rete perché il server ha vietato l'accesso alla macchina attaccante.