Traccia: Effettuare una scansione completa sul target Metasploitable. Esercizio Traccia e requisiti Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

**NFS Exported Share Information Disclosure**

**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.

## Installare il Software del Server NFS

Per prima cosa, assicurati che il software del server NFS sia installato sull'host remoto. Questo può essere fatto utilizzando un gestore di pacchetti. Ecco i comandi per diverse distribuzioni Linux:

Debian/Ubuntu:

sudo apt update

sudo apt install nfs-kernel-server

Red Hat/CentOS:

sudo yum install nfs-utils

## Passaggio 2: Configurare la Directory da Esportare

Scegli o crea una directory che vuoi condividere. Ad esempio, condividiamo `/srv/nfs`.

Crea la directory (se non esiste)

sudo mkdir -p /srv/nfs

## Passaggio 3: Configurare le Esportazioni NFS

Modifica il file `/etc/exports` per specificare la directory da condividere e i client autorizzati.

Apri il file `/etc/exports` in un editor di testo:

sudo nano /etc/exports

Aggiungi una riga per la directory e specifica gli host autorizzati. Ad esempio

/srv/nfs 192.168.1.100(rw,sync,no_subtree_check) 192.168.1.101(ro,sync,no_subtree_check)

Questa riga significa:

- Condividi `/srv/nfs`
- Consenti l'accesso in lettura-scrittura all'host con IP `192.168.1.100`
- Consenti l'accesso in sola lettura all'host con IP `192.168.1.101`
- `sync`: Assicura che le modifiche siano scritte su disco prima di rispondere
- `no_subtree_check`: Disabilita il controllo dei sottoalberi per le prestazioni

### Passaggio 4: Applicare la Configurazione delle Esportazioni

Dopo aver modificato il file `/etc/exports`, applica le modifiche eseguendo:

sudo exportfs -ra

### Passaggio 5: Avviare e Abilitare il Server NFS

Avvia il server NFS e abilitalo per avviarsi all'avvio del sistema:

- **Debian/Ubuntu:**

sudo systemctl restart nfs-kernel-server

sudo systemctl enable nfs-kernel-server

**Red Hat/CentOS:**

sudo systemctl restart nfs

sudo systemctl enable nfs

### Passaggio 6: Configurare il Firewall

Assicurati che il firewall sia configurato per consentire il traffico NFS. Apri le porte necessarie (tipicamente 2049 per NFS):

Debian/Ubuntu (con UFW)

sudo ufw allow from 192.168.1.0/24 to any port nfs

Red Hat/CentOS (con firewalld):

sudo firewall-cmd --permanent --add-service=nfs

sudo firewall-cmd –reload

### Passaggio 7: Testare la Configurazione NFS

Dal client, prova a montare la condivisione NFS per assicurarti che solo gli host autorizzati possano montarla.

Sul client:

1. Installa il software client NFS:

Debian/Ubuntu:

sudo apt install nfs-common

Red Hat/CentOS:

sudo yum install nfs-utils

Crea un punto di montaggio e monta la condivisione NFS:

sudo mkdir -p /mnt/nfs

sudo mount -t nfs 192.168.1.1:/srv/nfs /mnt/nfs

2. Crea un punto di montaggio e monta la condivisione NFS:

sudo mkdir -p /mnt/nfs

sudo mount -t nfs 192.168.1.1:/srv/nfs /mnt/nfs

3. Verifica il montaggio

df -h /mnt/nfs

4. Per montare automaticamente all'avvio, aggiungi una voce a `/etc/fstab`:

192.168.1.1:/srv/nfs /mnt/nfs nfs defaults 0 0

## Riepilogo

Seguendo questi passaggi, avrai configurato un server NFS che limita l'accesso alle sue condivisioni solo agli host autorizzati, garantendo una configurazione NFS sicura ed efficiente.