VULNERABILITA TROVATE:

Critical: NFS Exported Share Information Disclosure

NFS (Network File System) ed SMB (Server Message Block) sono **protocolli o regole di archiviazione di accesso ai file per una condivisione efficiente dei file su una rete**.

### 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.

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

### Solution:

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

Soluzione
Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

### Output

- The following NFS shares could be mounted:
- È possibile montare le seguenti condivisioni NFS
-

```
+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
```

## Linee guida generali per la protezione del file system di rete

Esistono diverse linee guida che possono aiutarti a proteggere il Network File System (NFS).
•Assicurarsi che siano installate le patch software più recenti. Le patch che risolvono i problemi di sicurezza dovrebbero essere considerate particolarmente importanti. Tutto il software in una determinata infrastruttura dovrebbe essere mantenuto. Ad esempio, installare le patch in un sistema operativo ma non riuscire a installare le patch su un server Web potrebbe fornire a un aggressore un modo per collegare il tuo ambiente che avrebbe potuto essere evitato se anche il server Web fosse stato aggiornato.
•Configurare il server NFS per esportare i file system in modo esplicito per gli utenti che dovrebbero avervi accesso. La maggior parte delle implementazioni di NFS ti consentirà di specificare quali client NFS dovrebbero avere accesso a un dato file system. Ciò mitigherà i tentativi da parte di utenti non autorizzati di accedere ai file system. In particolare, non configurare un server NFS per esportare un file system su se stesso.
•I file system esportati dovrebbero essere nelle loro partizioni. Un aggressore potrebbe causare il degrado del sistema scrivendo su un file system esportato fino a quando non è pieno. Ciò potrebbe rendere il file system non disponibile per altre applicazioni o utenti che ne hanno bisogno.

•Non consentire ai client NFS di accedere al file system con credenziali utente root o credenziali utente sconosciute. La maggior parte delle implementazioni di NFS può essere configurata per mappare le richieste da un utente privilegiato o sconosciuto a un utente non privilegiato. Ciò eviterà scenari in cui un aggressore tenta di accedere ai file ed eseguire operazioni sui file come utente privilegiato.

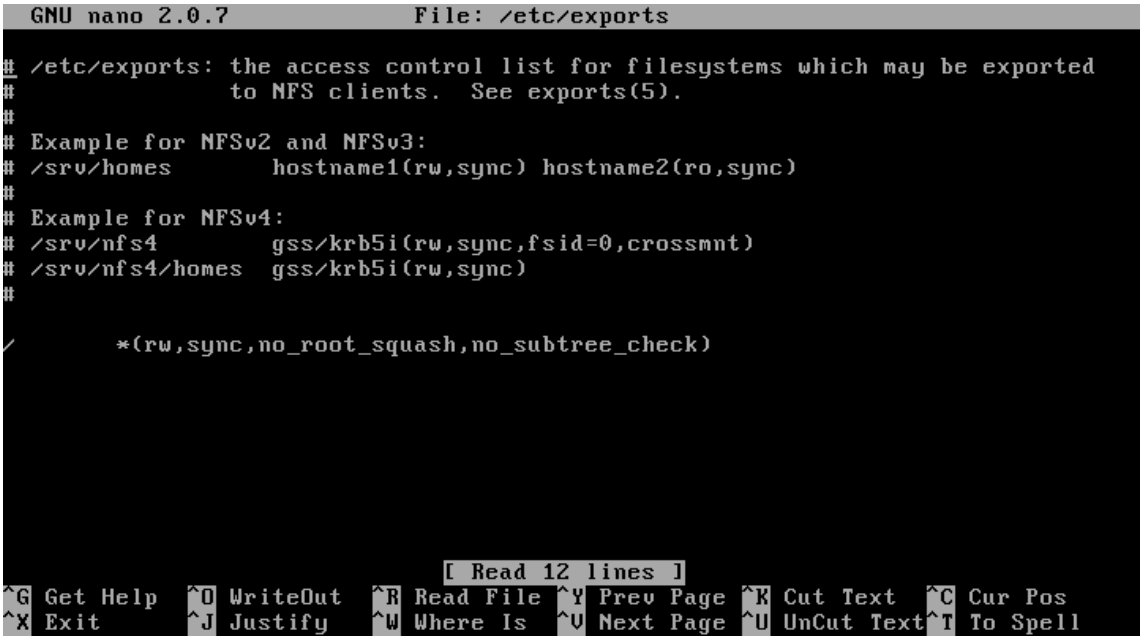
Non consentire ai client NFS di eseguire programmi suid e sgid sui file system esportati. Ciò impedirà ai client NFS di eseguire codice dannoso con privilegi. Se l'aggressore è in grado di rendere l'eseguibile di proprietà di un proprietario o gruppo privilegiato, si possono causare danni significativi al server NFS
-Ciò può essere fatto specificando l' opzione di comando **mknfsmnt -y**

Usa Secure NFS. Secure NFS usa la crittografia DES per autenticare gli host coinvolti nelle transazioni RPC. RPC è un protocollo usato da NFS per comunicare le richieste tra gli host. Secure NFS mitigherà i tentativi di un aggressore di falsificare le richieste RPC crittografando il timestamp nelle richieste RPC. Un ricevitore che decifra correttamente il timestamp e conferma che è corretto serve come conferma che la richiesta RPC proviene da un host attendibile.

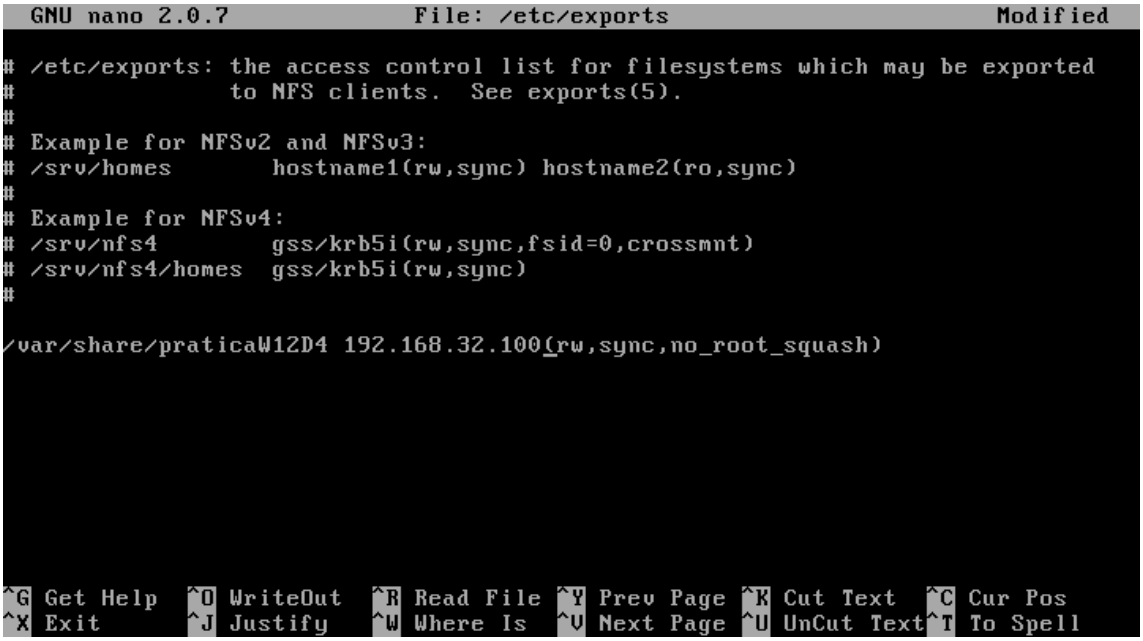
Se NFS non è necessario, disattivarlo. Ciò ridurrà il numero di possibili vettori di attacco disponibili per un intruso.

NFS supporta anche l'uso del tipo di crittografia AES con autenticazione Kerberos 5 oltre a Triple DES e Single DES.

## Configurazione di defauld




## Configurazione sucessiva



## General guidelines for securing Network File System

There are several guidelines that help you secure the Network File System (NFS).

- Ensure that the latest software patches are installed. Patches that address security issues should be considered especially important. All software in a given infrastructure should be maintained. For example, installing patches in an operating system but failing to install patches on a Web server may provide an attacker with a way to attach your environment that could have been avoided if the Web server been updated as well.
- Configure the NFS server to export file systems with the least amount of privileges necessary. If users only need to read from a file system, they should not be able to write to the file system. This can mitigate an attempt to overwrite important data, modify configuration files, or write malicious executable code to an exported file system. Specify privileges using SMIT or by directly editing the /etc/exports file.

  •Configure the NFS server to export file systems explicitly for the users who should have access to it. Most implementations of NFS will allow you to specify which NFS clients should have access to a given file system. This will mitigate attempts by unauthorized users to access file systems. In particular, do not configure an NFS server to export a file system to itself.

  •Exported file systems should be in their own partitions. An attacker could cause system degradation by writing to an exported file system until it is full. This may make the file system unavailable to other applications or users that needed it.

  •Do not allow NFS clients to access the file system with root user credentials or unknown user credentials. Most implementations of NFS can be configured to map requests from a privileged or unknown user to an unprivileged user. This will avert scenarios where an attacker tries to access files and perform file operations as a privileged user.

  •Do not allow NFS clients to run suid and sgid programs on exported file systems. This will prevent NFS clients from executing malicious code with privileges. If the attacker is able to make the executable owned by a privileged owner or group, significant harm can be done to the NFS server. This can be done by specifying the mknfsmnt -y command option.

  •Use Secure NFS. Secure NFS uses DES encryption to authenticate hosts involved in RPC transactions. RPC is a protocol used by NFS to communicate requests between hosts. Secure NFS will mitigates attempts by an attacker to spoof RPC requests by encrypting the time stamp in the RPC requests. A receiver successfully decrypting the time stamp and confirm that it is correct serves as confirmation that the RPC request came from a trusted host.

  •If NFS is not needed, turn it off. This will reduce the number of possible attack vectors available to an intruder.
-

Nella scanzione 2 nessus non a trovato questa vulnerabilita.