

## Vulnerability management

Per l'indirizzo ip 192.168.50.101 (ip della macchina metasploitable) è stato realizzato dalla nostra macchina Kali uno scan semplice della sua rete utilizzando come strumento Nessus.

Le vulnerabilità in totale sono:

Critical 8

High 4

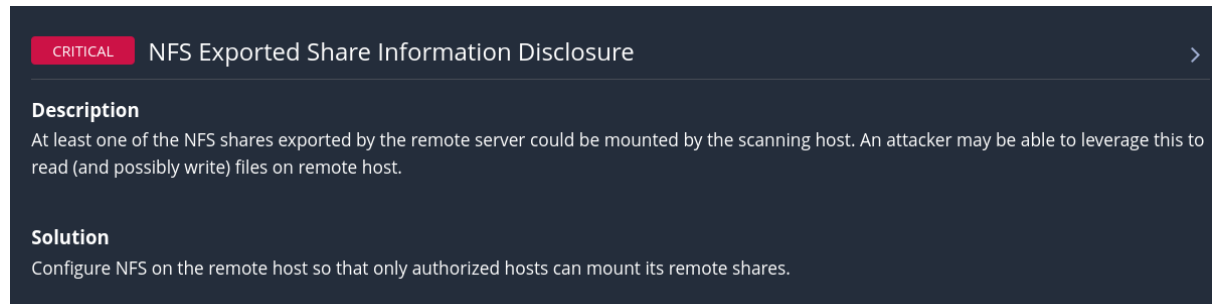
Medium 16

Low 7

Info 72

### Spiegazioni di 3 vulnerabilità critiche

Port: 2049 / udp / rpc-nfs



The screenshot shows a vulnerability entry in a dark-themed interface. At the top, a red box with the word 'CRITICAL' is followed by the title 'NFS Exported Share Information Disclosure'. Below this, the 'Description' section states: '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.' The 'Solution' section follows, stating: 'Configure NFS on the remote host so that only authorized hosts can mount its remote shares.'

Network File System (NFS) è un protocollo di file system distribuito per l'archiviazione condivisa. Il protocollo di archiviazione condivisa NFS definisce il modo in cui i file vengono archiviati e recuperati dai dispositivi di archiviazione attraverso le reti. È uno dei numerosi standard di file system distribuiti NAS (Network-Attached Storage).

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

No port

**CRITICAL** Unix Operating System Unsupported Version Detection < >

**Description**

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version of the Unix operating system that is currently supported.

Il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

Come soluzione si dovrà eseguire l'aggiornamento del sistema operativo Unix alla versione attualmente supportata

Port: 1524 / tcp / wild\_shell

**CRITICAL** Bind Shell Backdoor Detection < >

**Description**

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution**

Verify if the remote host has been compromised, and reinstall the system if necessary.

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

## Spiegazioni di 1 vulnerabilità High

Port: 445 / tcp / cifs

HIGH

Samba Badlock Vulnerability

< >

**Description**

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

**Solution**

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Il protocollo Server Message Block (SMB) è un protocollo di comunicazione client-server utilizzato per l'accesso condiviso a file, directory, stampanti, porte seriali e altre risorse su una rete.

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

Come soluzione si dovrà aggiornare alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.