

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

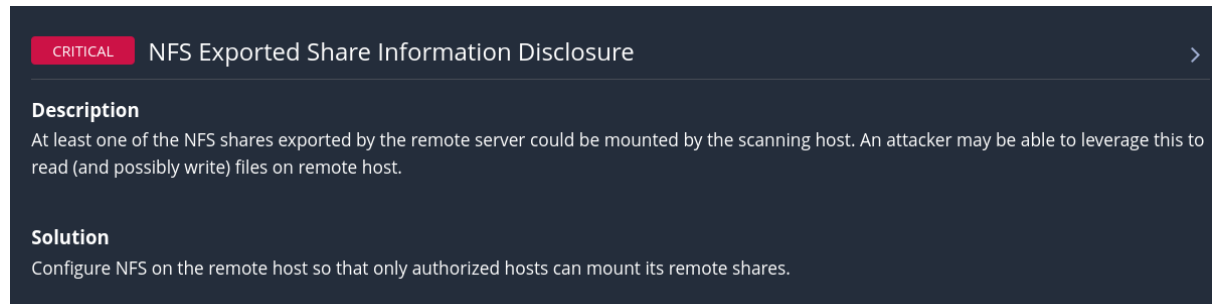
Medium 16

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.

Soluzione

Aggiungere solo gli indirizzi ip che possono avere accesso a questo server, prima era impostato 'ALL' ora è stato inserito un ip 192.168.50.100

```
GNU nano 2.0.7      File: /etc/exports      Modified
# /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)
#
192.168.50.100(rw,sync,no_root_squash,no_subtree_check)

[ Cancelled ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Port: 5900 / tcp / vnc

CRITICAL VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Soluzione

Implementiamo una password che non sia facile da indovinare per un bruteforce

```
msfadmin@metasploitable:/$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
```

Possiamo aggiungere un livello di sicurezza aggiungendo una regola per la gestione del traffico verso la porta in questione (5900).

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.

Soluzione

Cerchiamo i processi che tengono attiva la porta 1524 e la chiudiamo

```
root@metasploitable:/# sudo netstat -tuln | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
root@metasploitable:/# sudo netstat -tulnp | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN 12 0 4504/xin
etd
root@metasploitable:/# sudo kill 4504
root@metasploitable:/# sudo netstat -tulnp | grep :1524
root@metasploitable:/#
```

```
(kali㉿kali)-[~]
└─$ sudo nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

aggiungiamo una regola per rifiutare il traffico sulla porta 1524 per rafforzare la sicurezza.