

REPORT NESSUS

Durante il primo scan di Meta sono emerse 3 vulnerabilità critiche di cui:

- VNC Server 'password' Password
- NFS Exported Share information Disclosure
- rexecd Service Detection

Per risolvere la vulnerabilità VNC Server 'password' Password

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.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.1.101

Dobbiamo eseguire il comando su Meta:

```
root@metasploitable:~# sudo su
root@metasploitable:~# cd /
root@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

root@metasploitable:~# cd /root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# rm passwd
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  xstartup
metasploitable:0.pid  metasploitable:2.log
root@metasploitable:~/.vnc# _
```

facendo ciò andremo a togliere la password da root e potremo eseguire l'accesso solamente da msfadmin. (non più da remoto)

Per risolvere la vulnerabilità NFS Exported Share information Disclosure

CRITICAL 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.

Dobbiamo eseguire il comando su Meta:

`sudo nano /etc/exports`

```
GNU nano 2.0.7 File: /etc/exports

# /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)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

Successivamente modificare il root /

`*(rw,sync,no_root_squash,no_subtree_check)` in questo modo:

```
/*(noaccess,root_squash)
```

Prima

- Con `(rw,sync,no_root_squash,no_subtree_check)` un Host da remoto poteva avere sia lettura che scrittura e poteva prendere i privilegi

Risolvendo la vulnerabilità

- Con `(no access,root_squash)` all'Host gli neghiamo l'accesso e gli togliamo i privilegi.

Con questa configurazione vado a risolvere anche una vulnerabilità HIGH

HIGH NFS Shares World Readable

Description
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution
Place the appropriate restrictions on all NFS shares.

Per risolvere questa vulnerabilità

rexecd Service Detection
CRITICAL Nessus Plugin ID 10203

Synopsis
The rexecd service is running on the remote host.

Description
The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.
However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution
Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Dobbiamo entrare nel file di configurazione con il comando:
`sudo nano /etc/inetd.conf`

```
Metaexploitable
GNU nano 2.0.7 File: /etc/inetd.conf
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
shell               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

E modificarlo mettendo # prima di exec in questo modo:

```
#exec                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
```

Ciandri Leonardo