

Remediation

Tabella versione software e ip delle macchine

Macchina/software	Versione
Kali (192.168.32.100)	2023.2
Meta (192.168.50.101)	Linux Kernel 2.6
Pfsense	2.6.0
Nessus	10.5.2

In questa rete, Pfsense fa da router tra kali e meta, poste su due reti differenti e verrà utilizzato anche per la Remediation con qualche regola firewall.

Vulnerabilità n1

1356 - NFS Exported Share Information Disclosure

Una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.

Per risolvere questa vulnerabilità con il comando “sudo nano /etc/exports” accedo al file di configurazione dell'esportazioni NFS.

```
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)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

Vado a modificare l'unica riga attiva dove i client hanno permessi di scrittura e lettura. Col no_root_squash, consente all'utente root di mantenere i propri privilegi root sulla condivisione NFS.

Modifico la riga con no access, root_squash così da risolvere la vulnerabilità vietando l'accesso e evitando di far mantenere al client, i privilegi root sulla condivisione NFS.

```
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)
#
#
#*(noaccess,root_squash)

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

Vulnerabilità n2

42256 - NFS Shares World Readable

Il server NFS remoto sta esportando una o più condivisioni senza restrizioni di accesso (basate su hostname, IP o intervallo IP).

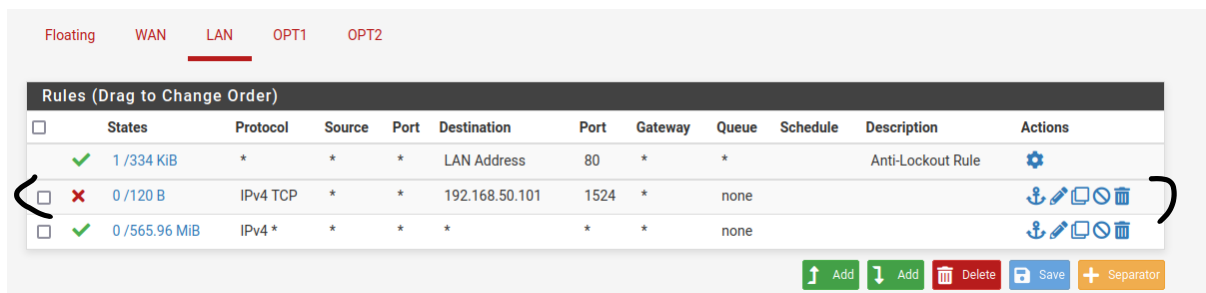
Con la modifica del file `/etc/exports/` fatto nella vulnerabilità 1, si risolve anche quest'altra, in quanto collegate tra di loro.

Vulnerabilità n3

51988 - Bind Shell Backdoor Detection

Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Per rimuovere questa vulnerabilità utilizzo il firewall Pfsense, per andare a bloccare la porta specifica della backdoor "1524". Effettuando un `nmap -p 1524` su meta, lo stato della porta infatti è passata da aperta a filtrata.



Vulnerabilità n4

61708 - VNC Server 'password' Password

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password "password". Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

Per risolvere questa vulnerabilità vado nella directory root ed entro in vnc. Dentro la cartella di vnc trovo il file password, e lo rimuovo così da mantenere l'accesso solo con l'utente msfadmin ed un attaccante da remoto non è in grado di prendere i privilegi root.

```
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cd /
msfadmin@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
msfadmin@metasploitable:/$ sudo su
[sudo] password for msfadmin:
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#
```

Vulnerabilità n5

Rexecd Service Detection

Da traccia, dovevo risolvere anche questa vulnerabilità, che Nessus non mi ha rilevato. Facendo ricerche sul web, ho capito che ciò non è stata rilevata per la versione dei dispositivi. Quindi ho visto ugualmente come poter risolvere questa vulnerabilità e col comando "sudo nano/etc/inetd.conf" si accede alla configurazione del servizio e basta andare a commentare la riga del servizio exec, che è appunto il servizio con la vulnerabilità.

```
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
```

