Febbraio 2024

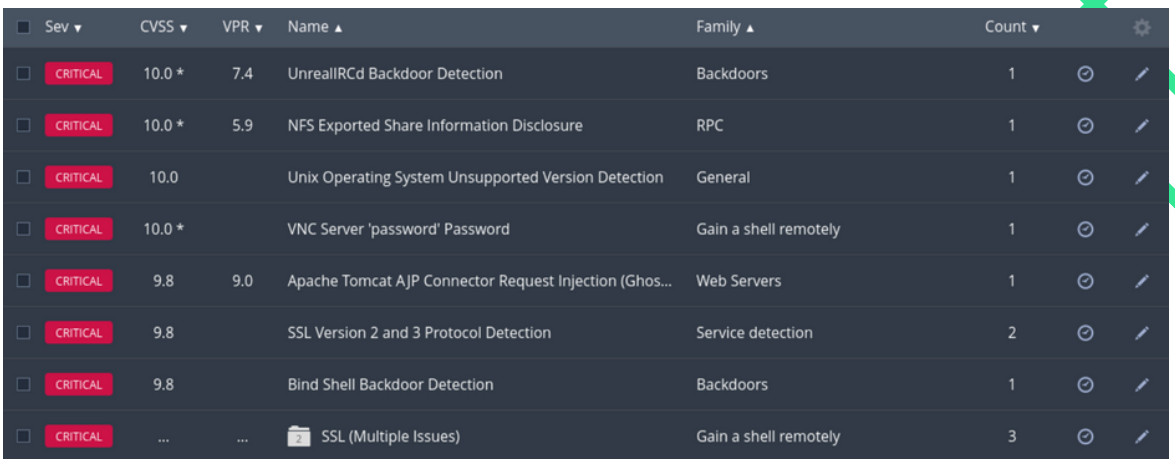
CYBER SECURITY SPECIALIST

S5L5

Jacopo Trovato

Vulnerability assessment

Tramite il software di Nessus è stata eseguita una scansione sul server di Metasploitable al fine di rilevare delle vulnerabilità e risolverle al meglio. Verranno presi in esempio solo 2 tra le vulnerabilità critiche trovate.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghos...	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3

Prima vulnerabilità

NFS Exported Share Information Disclosure:

- Significato:

Questa vulnerabilità indica che è possibile accedere alle condivisioni NFS sull'host remoto, questo potrebbe portare un attaccante a scrivere file sull'host remoto.

- Soluzione:

Per risolvere questa vulnerabilità bisogna far sì che solo gli host autorizzati posso leggere e scrivere file, per far questo è necessario configurare NFS sull'host remoto.

Andare su Metasploitable e eseguire il comando
“sudo nano /etc/exports” e dove si trova ‘*’ bisogna sostituirlo con
l’indirizzo IP associato a Meta.

```
  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)



                        [ Smooth scrolling enabled ]
^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
```

```
  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)
#

/_      192.168.49.101(rw,sync,no_root_squash,no_subtree_check)



^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
```

Seconda vulnerabilità

VNC Server ‘password’ Password

- Significato:

Questa vulnerabilità ci va ad indicare che la password è molto debole e probabilmente è PASSWORD, questo rende estremamente facile entrare.

- Soluzione

Per risolvere bisogna cambiare la password e inserire una più sicura.
Su metasploitable usare il comando “sudo su” per ottenere i privilegi da amministratore e con il comando “vnctpasswd” che ti permette di modificare la password predefinita. effettuare un reboot di Meta per salvare le modifiche.