

Epicode

Esercizio Remediation Metasploitable

Traccia:

Effettuare una scansione completa sul target Metasploitable. Scegliere da un minimo di 2 fino a un massimo di 4 **vulnerabilità critiche** e provate ad implementare delle azioni di rimedio. Per dimostrare l'efficacia delle azioni di rimedio si esegua nuovamente la scansione sul target e si confrontino con i risultati ottenuti in precedenza. Qui di seguito le vulnerabilità scelte da risolvere:

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

NFS Exported Share Information Disclosure

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Soluzione

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

```
/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)
```

Per risolvere la Vulnerabilità abbiamo cancellato l'ultima riga con riga con i permessi root: (rw, sync, no_root_squash, no_subtree_check).

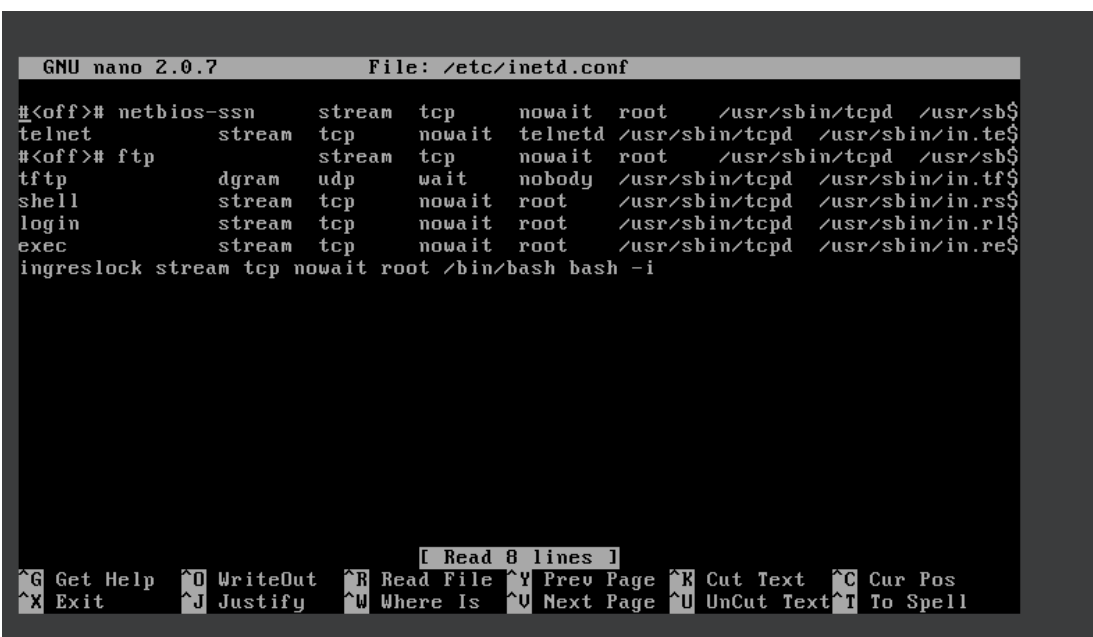
Bind Shell Backdoor Detection

Descrizione

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 comandi direttamente.

Soluzione

Entrando nella configurazione con comando **sudo nano etc/inetd.conf** da Meta cancelliamo l'ultima riga con l'ingresso al root di sistema da backdoor.



```
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

[ Read 8 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   ^V Next Page  ^U UnCut Text ^T To Spell
```

Ingresso Backdoor tolto.

```
GNU nano 2.0.7      File: /etc/inetd.conf
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.td$
telnet               stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.tel$
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ft$
tftp                dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tft$
shell               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh$
login              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlog$
exec               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex$
```

VNC server "password" Password

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione

Proteggiamo il servizio VNC server modificando la password: "password" con una password molto più difficile.

La password immessa è : Pa!pA!22 .Procediamo col comando **vncpasswd** che ci permette come vediamo sotto di reimpostare la password su file : **.vnc/passwd**.

```
msfadmin@metasploitable:~$ vncpasswd
-bash: vncpasswd: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$ _
```

Controlliamo ora con comando: **sudo nano .vnc/passwd** il cambio di password , come vedremo la password è protetta da crittografia ma è cambiata.

```
GNU nano 2.0.7 File: .unc/passwd
H♦o^G^Pz_♦H♦o^G^Pz_♦

[ Read 1 line ]
^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
```

Unix Operating System Unsupported Version Detection

Descrizione

In base al numero di versione auto-riportato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione

Si consiglia per tanto di reinstallare totalmente la macchina Metasploitable alla versione successiva perché non si rilasciano più aggiornamenti su di essa e il sistema rimarrebbe vulnerabile.

Rexecd service Detection

Dopo varie scansioni con Nessus il sistema non ha rilevato la vulnerabilità.

Conclusioni

Dopo aver trovato con Nessus le vulnerabilità al sistema Metasploitable con dei metodi di configurazioni sono state tolte le 4 vulnerabilità scelte in traccia rendendo il sistema più sicuro , ora possiamo passare alla scansione finale.