S5L5

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Sev	CVSS	VPR	Name	Family	Count		
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		SSL Version 2 and 3 Protocol Detection	Service detection	2		

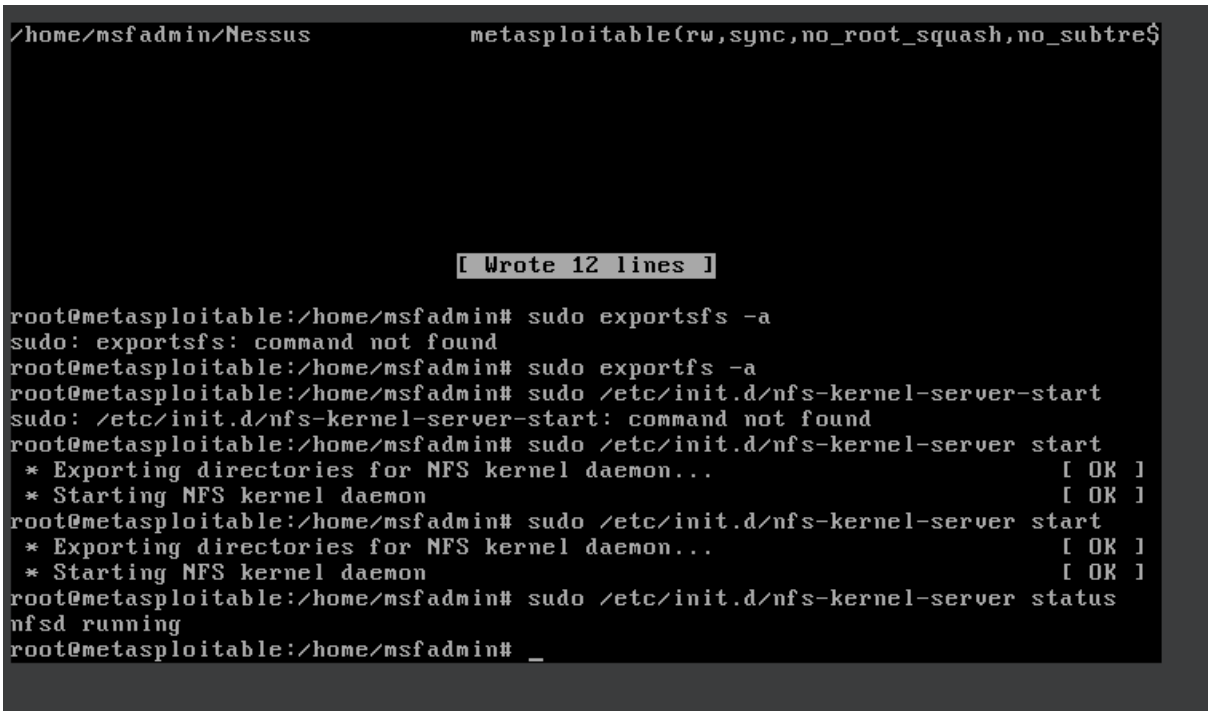
1)NFS Exported Share Information Disclosure
Questa è una vulnerabilità dove le informazioni condivise tramite NFS vengono diffuse in modo non autorizzato.Ciò accade quando la configurazione del sistema NFS non è protetta in modo adeguato.

Soluzione:
Limitare l'accesso NFS solo ad host o a reti autorizzate.

```
  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)
#

/home/msfadmin/Nessus           metasploitable(rw,sync,no_root_squash,no_subtre$

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ? _
 Y Yes
 N No            ^C Cancel
```

Dopo aver creato il file su meta lo andiamo a modificare

/home/msfadmin/Nessus è il percorso della directory che vogliamo condividere.



il comando sudo exportfs -a aggiorna la configurazione del NFS.
e con il comando sudo /etc/init.d/nfs-kernel-server start facciamo partire il servizio.

2)VNC Server ‘password’ Password:
Sono applicazioni software di accesso/controllo remoto utilizzate per l'amministrazione del proprio computer a distanza, potendo essere anche usate per controllare in remoto server che naturalmente non posseggono né monitor né tastiera.

Soluzione:
Strong password: impostare una password complessa e difficile da indovinare da almeno 8 caratteri comprendente caratteri alfanumerici, speciali e l’utilizzo di lettere maiuscole e minuscole.

```
root@metasploitable:/home/msfadmin# vncserver

New 'X' desktop is metasploitable:1

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:1.log

root@metasploitable:/home/msfadmin# vncpassword
bash: vncpassword: command not found
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

Tramite il comando vncserver avviamo il server e con il comando vncpasswd abbiamo la possibilità di cambiare la password.