Progetto S5/L5

Svolgimento:

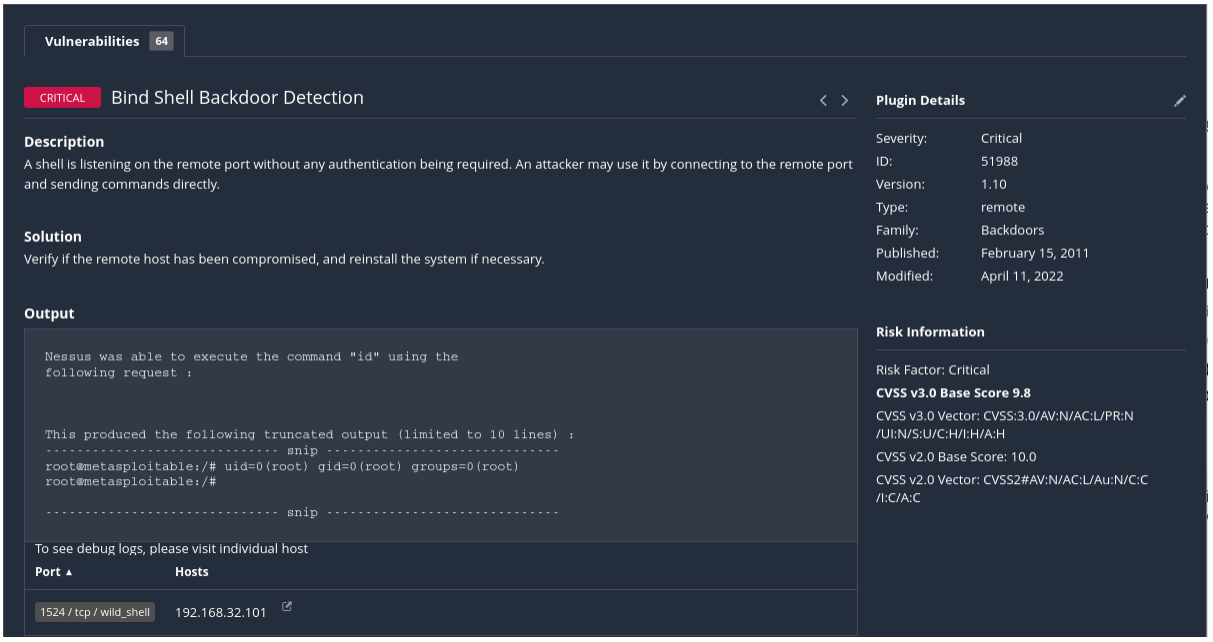
-Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (ScansioneInizio.pdf).
-Screenshot e spiegazione dei passaggi della remediation (RemediationMeta.pdf)
-Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità
-(il grafico che mostra tutte le vulnerabilità) ScansioneFine.pdf.
-Nota: i report possono essere lasciati in inglese.

Prendendo in considerazione 4 vulnerabilità del metasploitable :

- **Bind Shell Backdoor Detection (critico)**
- **VNC Server 'password' Password (critico)**
- **NFS Exported Share Information Disclosure (critico)**
- **Samba Badlock Vulnerability (alto)**

Caso 1)

Bind Shell Backdoor Detection : Una shell è in ascolto sulla porta (1524) remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.



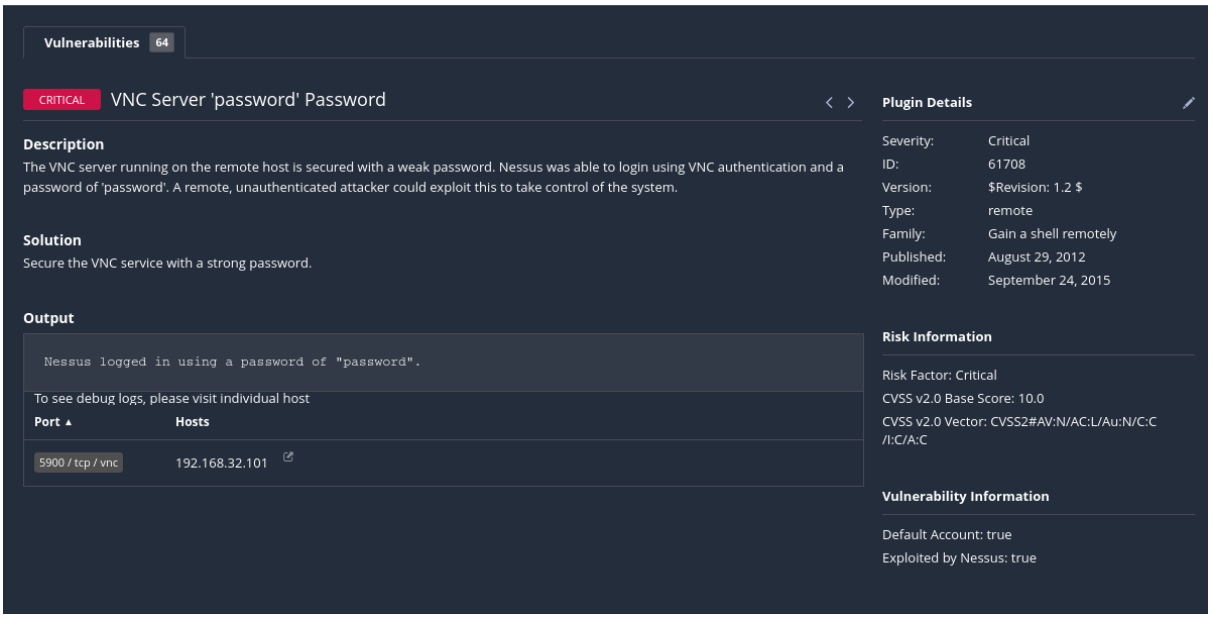
Per risolvere questo problema ho aggiunto una regola nel firewall che nega l’accesso alla porta 1524

```
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ ufw deny 1524
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere

msfadmin@metasploitable:~$
```

utilizzando :
-**sudo ufw enable** (per entrare nel firewall)
-**sudo ufw deny 1524** (per aggiungere la regola)
-**sudo ufw status** (per visualizzare la regola che ho aggiunto)

Caso 2)

VNC Server 'password' Password : Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.



Per risolvere questo problema basta un cambio di password al Server VNC

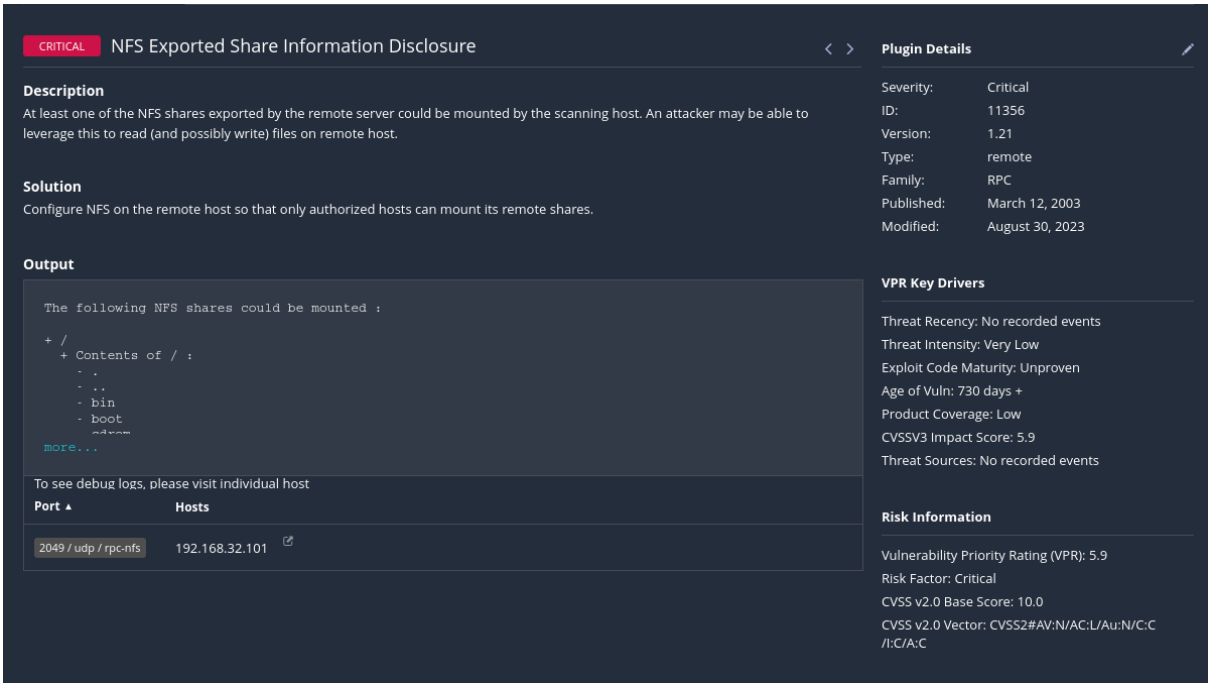
```
root@metasploitable:/# ls
bin    dev    initrd      lost+found  nohup.out  root  sys  var
boot   etc    initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home   lib         mnt         proc       srv   usr
root@metasploitable:/# cd root
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc# _
```

Si cerca il la cartella **.vnc** , con il comando **ls -a** riuscite a visualizzare anche file nascosti , la cartella l'ho trovata nella directory root .

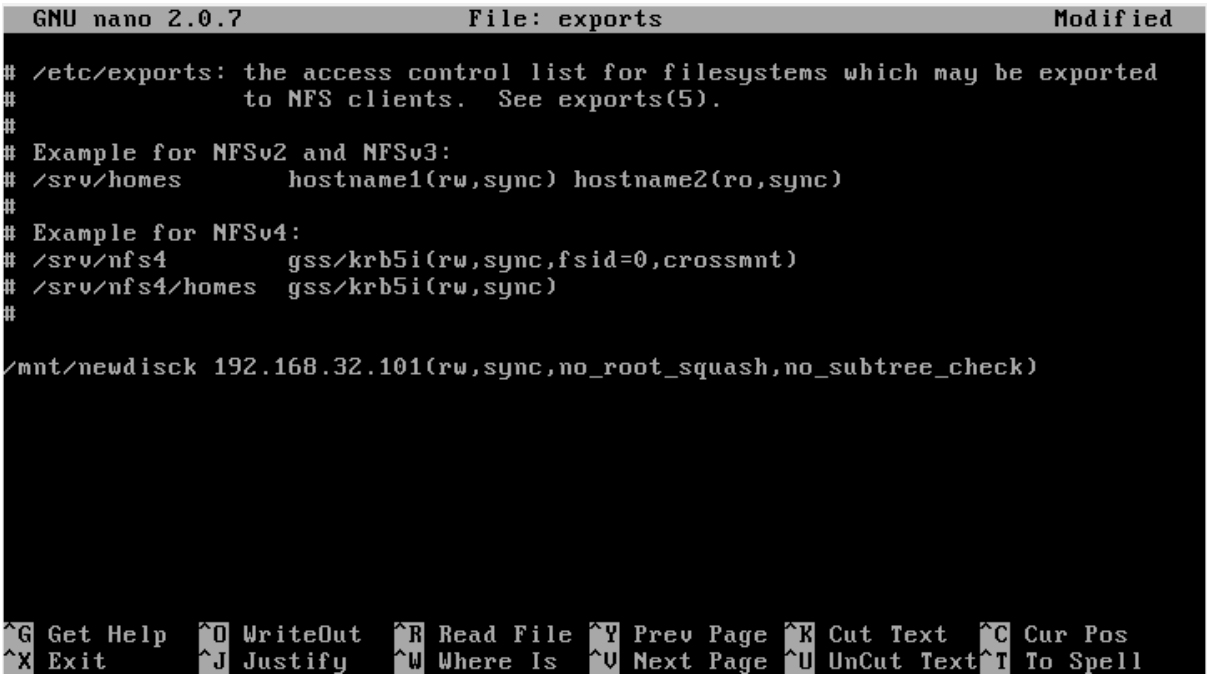
Una volta entrati nella cartella .vnc con il comando cd **.vnc** digitate il codice "vncpasswd" (per cambiare la password) inserite la password da cambiare (questo caso ho utilizzato 123456 come password)

Caso 3)

NFS Exported Share Information Disclosure : 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 (ed eventualmente scrivere) file su host remoti.



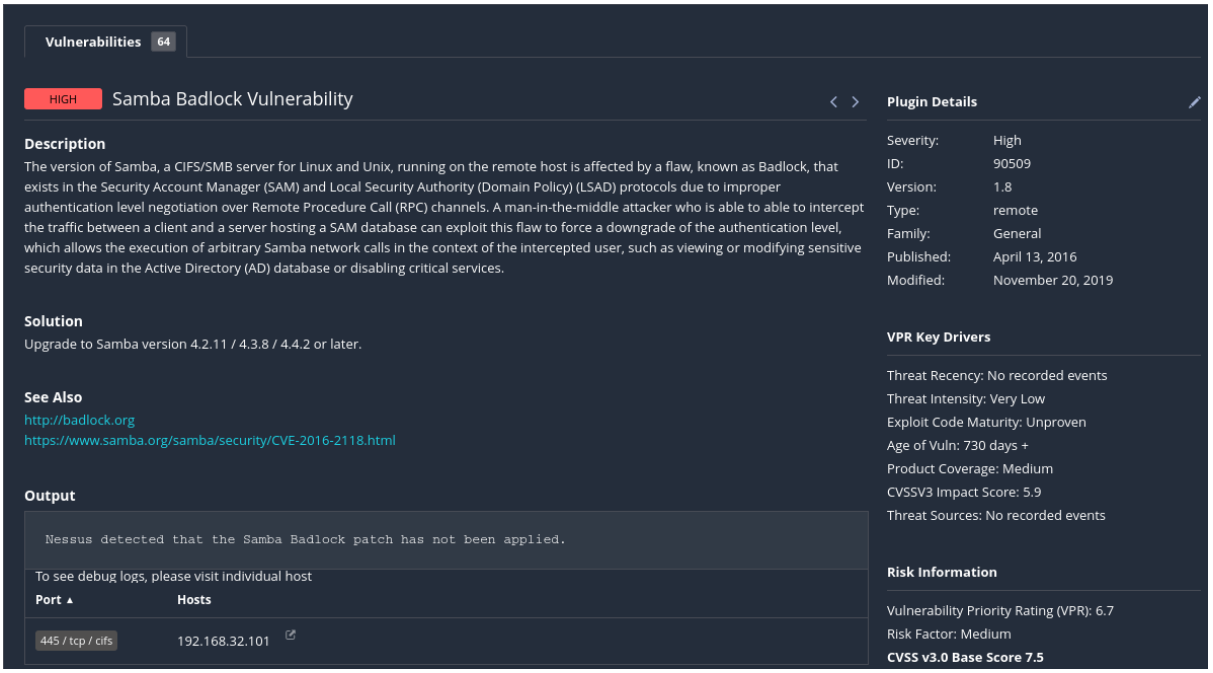
Per risolvere questo problema serve aggiungere un regola al file exports entrando con il comando -sudo nano /etc/exports



una volta entrati si aggiunge ip della macchina di metasploitable (192.168.32.101) salvate e uscite facendo “**ctrl + x**” poi digitando “**y**”.

Caso 3)

Samba Badlock Vulnerability : La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

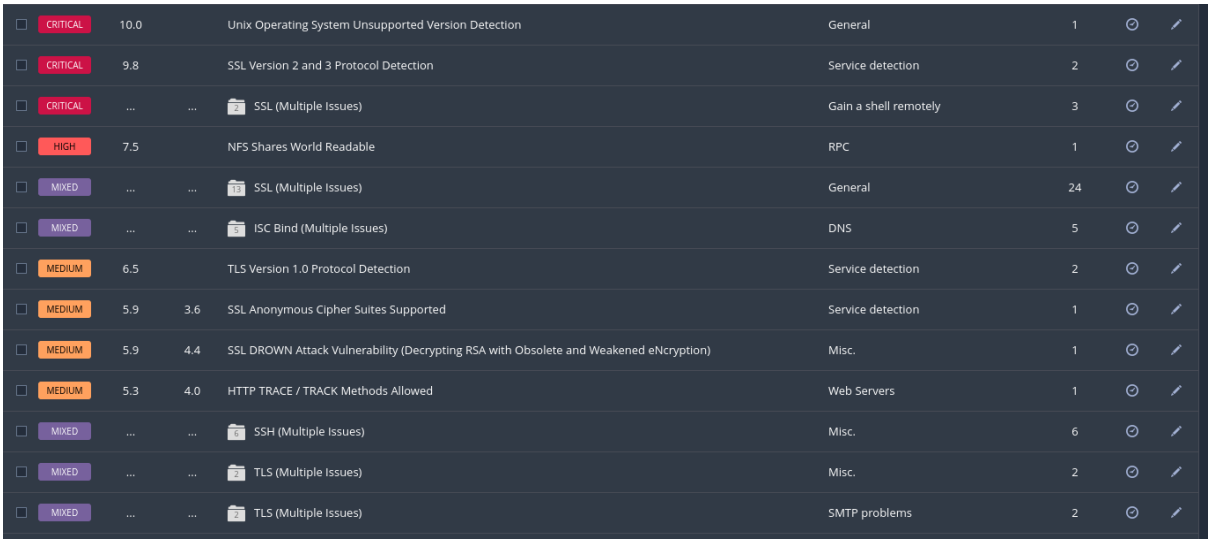


Ci sono due metodi per risolvere questo problema :
1) mettere la macchina online e aggiornarlo
2) chiudere le porte e quindi chiudere il servizio

Ho utilizzato il secondo metodo per non far connettere la macchina online

```
root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere
445:tcp                    DENY    Anywhere
445:udp                    DENY    Anywhere
139:tcp                    DENY    Anywhere
139:udp                    DENY    Anywhere
```

Ho aggiunto due regole al firewall - **ufw deny 445** e - **ufw deny 139** per chiudere le porte del servizio Samba



CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		
HIGH	7.5		NFS Shares World Readable	RPC	1		
MIXED	...	...	SSL (Multiple Issues)	General	24		
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5		
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2		
MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1		
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1		
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1		
MIXED	...	...	SSH (Multiple Issues)	Misc.	6		
MIXED	...	...	TLS (Multiple Issues)	Misc.	2		
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2		

Dopo lo scan finale si può notare che gli 4 punti vulnerabili lo abbiamo risolto .