PROGETTO SETTIMANALE

VULNERABILITY SCAN

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exporte...	RPC	1
CRITICAL	10.0		Unix Operat...	General	1
CRITICAL	10.0 *		VNC Server '...	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tom...	Web Servers	1
CRITICAL	9.8		SSL Version ...	Service detection	2
CRITICAL	9.8		Bind Shell B...	Backdoors	1
CRITICAL	...	...	SSL (M...	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badl...	General	1
HIGH	7.5		NFS Shares ...	RPC	1

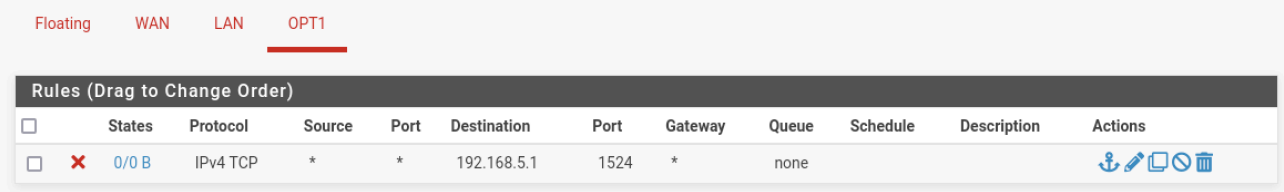
ALCUNE AZIONI DI RIMEDIO:

VNC Server ‘pasword’ Password
Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad effettuare l'accesso utilizzando l'autenticazione VNC e una password di 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.
Si può risolvere questa vulnerabilità cambiando la password del server VNC

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

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.
Nessus ha rilevato la presenza di una backdoor che permette di accedere alla Shell da remoto comunicando con la porta 1524.
Una volta scoperta questa vulnerabilità la prima cosa da fare è creare una regola nel firewall che blocca il traffico sulla porta 1524 e poi andare ad eliminare la backdoor.



Samba Badlock Vulnerability

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da una vulnerabilità nota come Badlock. Questa vulnerabilità riguarda i protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali Remote Procedure Call (RPC).
Per risolvere questa vulnerabilità è necessario installare o aggiornare Samba alla versione 4.2.11 o successive.