Progetto S5/L5 Alessio Forli Secure Sentinels 28/06/2024

Effettuare una scansione completa sul target Metaspoitable (192.168.5.101)
Tramite Nessus:

-Discovery- Scan Type: Port Scan (all ports)
-Assessment- Scan for all web vulnerability (quick)

Scegliere da un minimo di 2 fino ad un massimo di 4 vulnerabilità CRITICHE/HIGH e provare ad implementare delle azioni di rimedio.

-CRITICAL- NFS Exported Share Information Disclosure
-CRITICAL- VNC Server 'password' Password
-CRITICAL- Bind Shell Backdoor Detection

NFS Exported Share Information Disclosure:

Questo problema ci mostra che le condivisioni NFS potrebbero essere accessibili ad un possibile malintenzionato.

Soluzione:

Tramite PFSense limiteremo gli accessi alle condivisioni NFS permettendo l'accesso solo alle macchine autorizzate. A seguito di un port scan abbiamo identificato la porta TCP 2049 come porta predefinita per la condivisione NFS così da avere una regola di firewall specifica per bloccare quelle determinate richieste.

VNC Server 'password' Password:

Questo problema ci mostra che il server VNC ha una password debole che avvantaggerebbe un attacco di un possibile malintenzionato.

Soluzione:

Direttamente dalla macchina target, in questo caso Metaspoitable, riconfiguriamo la password VNC utilizzando il comando "vncpasswd" e scegliendone una più complessa successivamente in seguito ad un riavvio (sudo service vncserver restart) la configurazione sarà ultimata.

Bind Shell Backdoor Detection:

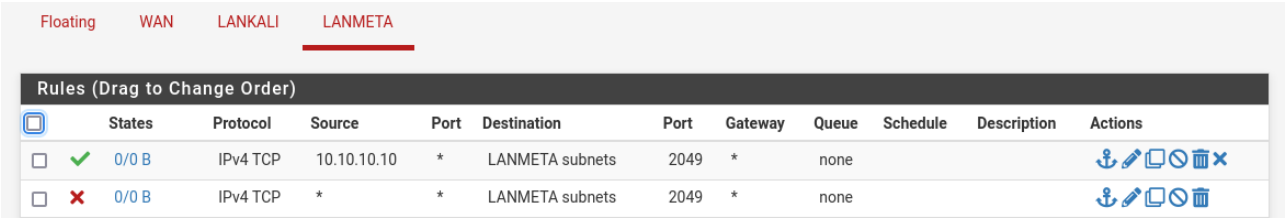
Questo problema ci mostra la presenza di una potenziale backdoor di tipo Bind Shell consentendo ad un possibile malintenzionato di accedere al nostro sistema da remoto. Nessus ci indica anche il numero della porta.

Soluzione:

Direttamente dalla macchina target, in questo caso Metaspoitable, identifichiamo il Process ID del servizio attivo sulla porta in questione tramite il comando "lsof", e lo terminiamo con "kill".

Sev	CVSS	VPR	Name
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure
CRITICAL	10.0		Unix Operating System Unsupported Version Detection
CRITICAL	10.0 *		VNC Server 'password' Password
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8		Bind Shell Backdoor Detection

Per la risoluzione della prima vulnerabilità abbiamo configurato il firewall ipotizzando che solo un determinato indirizzo IP potesse usufruire delle condivisioni NFS.
Come esempio ipotizziamo che solo un'unica macchina con indirizzo IP 10.10.10.10 debba accedere al servizio, configuriamo le regole di firewall come indicato dalla prossima immagine:



Così che se la macchina autorizzata cercasse di accedere a quel servizio (che si trova sulla porta 2049) riesca ad accedere, mentre alle altre macchine che cercherebbero di accedervi verrebbe negata la richiesta.

Per quanto riguarda la terza vulnerabilità scelta, ovvero quella della backdoor, volendo risolverla senza l'uso del firewall abbiamo adottare un rimedio non permanente, terminando il processo della backdoor, tuttavia si riattiverà con un riavvio del sistema, quindi utilizzerei questa soluzione solo se la macchina target fosse un server che non deve spegnersi. Ho evitato di eliminare permanentemente la directory contenente la backdoor (con il comando sudo rm /percorso dove si trova la backdoor/) solo perché era un esercizio e non sapevo se fosse utile mantenere quel file.