CSPT0524

Esercitazione Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4

INFORMAZIONI DEL DOCUMENTO

1.	**Autore**	Giovanni D'Abrosca
2.	**Nome Documento**	Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4
3.	**Data Emissione**	10/02/2025

Traccia esercizio:

Esercizio Traccia e requisiti Effettuare una scansione completa sul target Metasploitable2.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche 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.

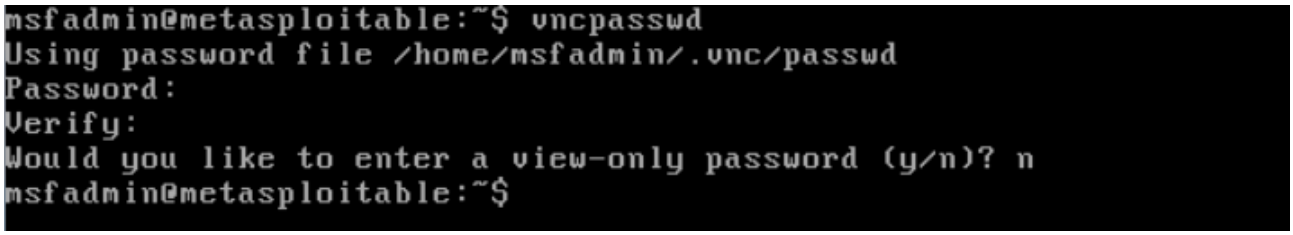
Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Screenshot e spiegazione dei passaggi della remediation

Per quanto riguarda la prima vulnerabilità identificata, essa riguardava l'utilizzo di una password di default o debole per il servizio VNC (Virtual Network Computing) su Metasploitable2. Questo problema permetteva agli attaccanti di ottenere facilmente accesso remoto non autorizzato al sistema.

Ho risolto questa vulnerabilità cambiando la password di VNC con una combinazione forte e complessa. Nello specifico, la nuova password è stata generata utilizzando una sequenza casuale di caratteri alfanumerici e simboli speciali, che includeva maiuscole, minuscole, numeri e caratteri speciali, garantendo così un elevato livello di sicurezza.

Di seguito lo screen del cambio password:



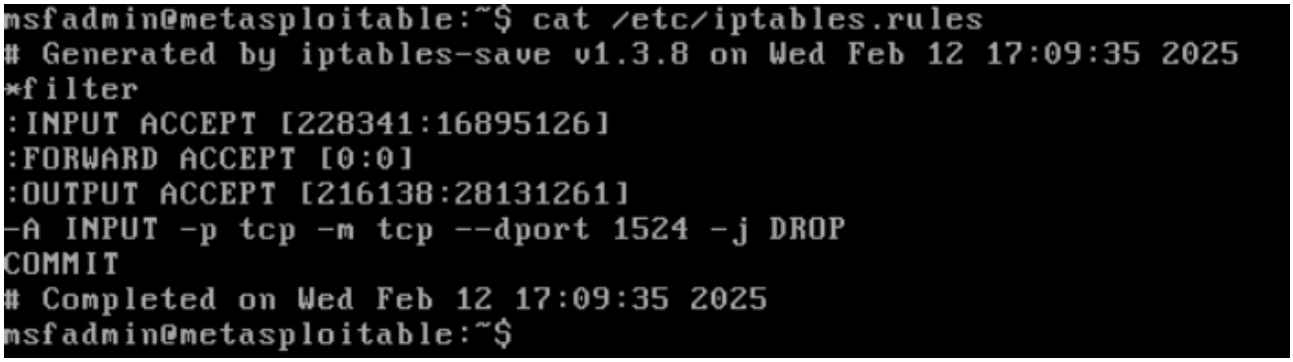
Per quanto riguarda la seconda vulnerabilità, ho deciso di chiudere la backdoor Bid shell utilizzando una regola firewall "iptables". La regola specifica implementata è stata:

sudo iptables -A INPUT -p tcp --dport 1524 -j DROP

Dopo aver creato questa regola firewall, ho proceduto a creare il file sotto la directory /etc/iptables.rules. Successivamente, ho modificato il file rc.local aggiungendo la seguente riga:

/sbin/iptables-restore < /etc/iptables.rules

Questa configurazione garantisce che, al riavvio del sistema Metasploitable2, la backdoor risulti filtrata, impedendo accessi non autorizzati tramite la porta TCP 1524.



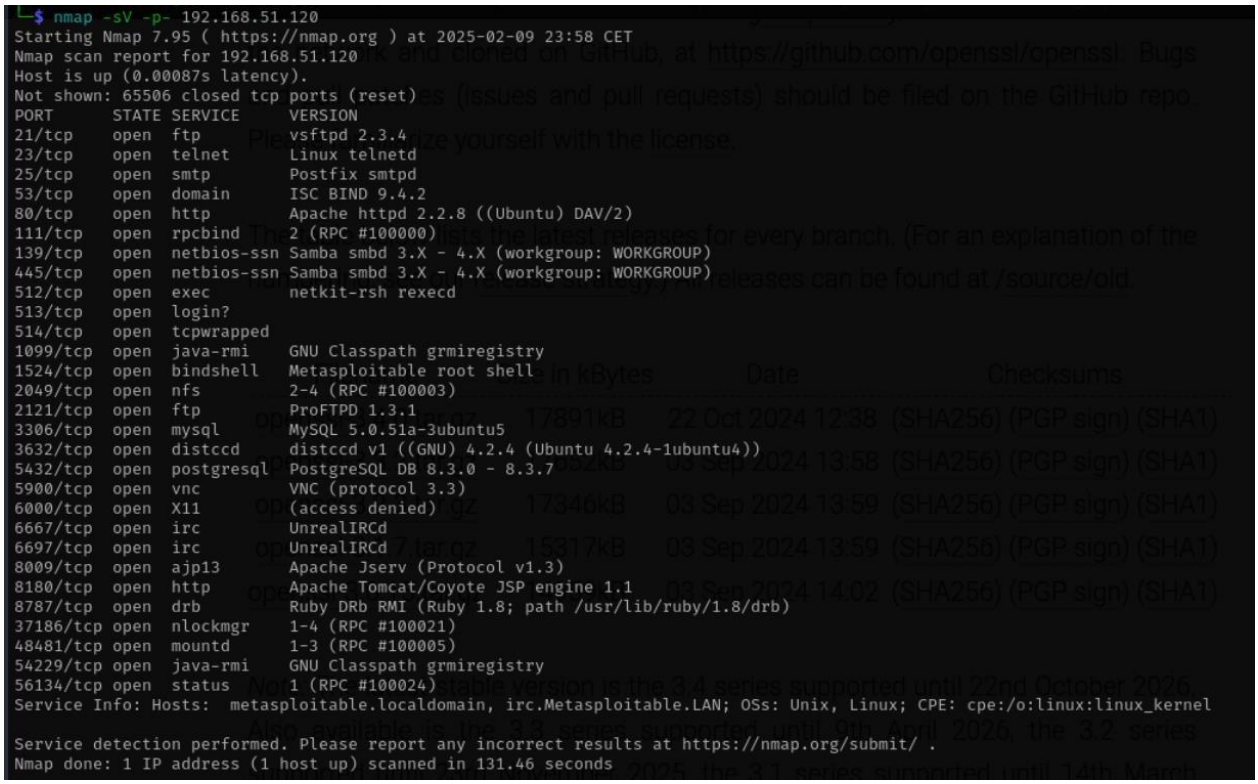
Per quanto riguarda la vulnerabilità del servizio OpenSSH che girava sulla porta 22 di Metasploitable2, la decisione di disinstallarlo è stata presa per eliminare completamente il rischio di attacchi legati a questo servizio. OpenSSH, pur essendo uno strumento fondamentale per la gestione remota sicura, se configurato in modo inadeguato o con versioni obsolete, può rappresentare una minaccia significativa.

Di seguito il comando della disinstallazione:

sudo apt-get remove --purge openssh-server

L'opzione `--purge` è stata utilizzata per assicurarsi che tutte le configurazioni e i file associati al pacchetto venissero completamente rimossi dal sistema. Questo garantisce che non rimangano residui che possano essere sfruttati da eventuali attaccanti.

Una volta completata la disinstallazione, è stato verificato che il servizio non fosse più presente e che la porta 22 non fosse più in ascolto. Di seguito lo screen:



L'assenza di output ha confermato che la porta 22 non era più utilizzata, eliminando così la vulnerabilità.