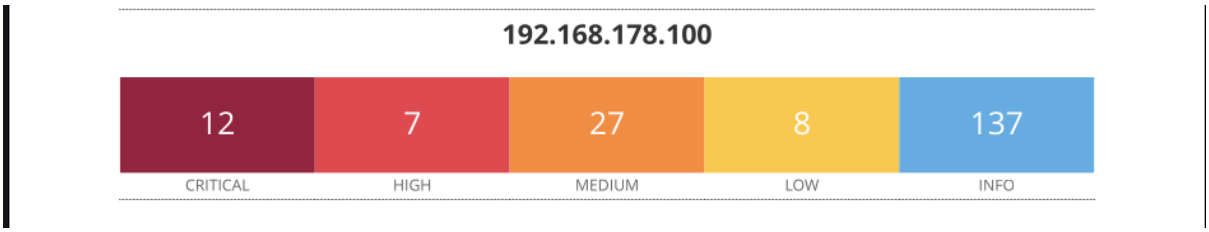
Vulnerability Assessment - Metasploitable

Lo scopo di questo report è analizzare le vulnerabilità presenti sulle common ports nella macchina Metasploitable, per poi agire di conseguenza per eliminarle.

Procedimento

Procediamo alla scansione delle common ports tramite Nessus. Abbiamo il seguente riscontro delle vulnerabilità trovate, il quale indica i livelli di gravità: Critico, Alto, Medio, Basso e Informazione (ovvero nessuna vulnerabilità) basandosi sul sistema CVSS, il quale assegna un voto da 1 a 10 in base al livello di gravità della vulnerabilità, dove 10 è il livello più alto.



Andiamo ora ad analizzare le singole vulnerabilità, partendo dalle più gravi.

Vulnerabilità riscontrate

1) Il Server VNC ha come password la parola “password” - Voto CVSS: 10

Come scritto nella descrizione, la password è troppo debole e scontata, facilmente trovabile sia con che senza un BruteForce.

Remediation: *aggiornare la password. Usare lettere maiuscole e minuscole, numeri e caratteri speciali, evitando parole troppo scontate.*

2) Il Server VRC contiene una backdoor – Voto CVSS: 10

Questo server è una versione del software UnrealIRC che contiene una backdoor, che permette di eseguire codice malevolo sulla macchina Metasploitable.

Remediation: Scaricare nuovamente il software e usare i checksum MD5 e SHA1 per verificarne l’affidabilità prima di reinstallarlo.

3) La versione del sistema operativo *Unix* non è più supportata

Come da descrizione, la versione di Unix installata è datata: il che indica che non riceverà più supporto dagli sviluppatori riguardo alle patch di sicurezza, che andrebbero ad agire su eventuali falle del sistema.

Remediation: aggiornare il sistema operativo Unix a una versione più recente e supportata, in modo da poter applicare le patch a eventuali falle di sicurezza.

4) **Il servizio remoto sulla porta TCP 5432 applica delle cifrature (SSL 2.0 e SSL 3.0) che hanno delle debolezze note – Voto CVSS: 9.8**

Il traffico di rete a questo remote service applica delle cifrature alle quali possono essere facilmente intercettati i dati trasmessi.

Remediation: applicare il protocollo TLS a questo servizio (Transport Layer Security) per trasmettere i dati con una cifratura più affidabile.

5) **Il servizio SMTP sulla porta TCP 25 applica delle cifrature (SSL 2.0 e SSL 3.0) che hanno delle debolezze note – Voto CVSS: 9.8**

Il traffico di rete a questo servizio applica delle cifrature alle quali possono essere facilmente intercettati i dati trasmessi.

Remediation: applicare il protocollo TLS a questo servizio (Transport Layer Security) per trasmettere i dati con una cifratura più affidabile.

6) Backdoor sulla Shell in ascolto sulla TCP 1524 - Voto CVSS: 9.8

La shell sulla porta TCP 1524 è in ascolto senza nessuna autenticazione, il che renderebbe molto facile per un attaccante l'installazione di una backdoor, permettendo di eseguire comandi sulla shell della vittima da remoto. Tramite questi comandi si potrebbero eseguire azioni come utente root, o addirittura distruggere il sistema operativo cancellando file di sistema.

Remediation: Verificare se la macchina è stata compromessa ed eventualmente reinstallarla.