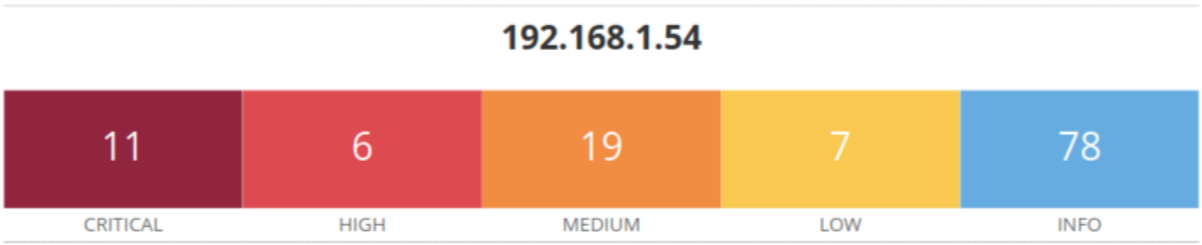
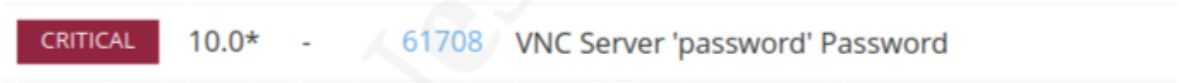
Effettuo un Vulnerability Assessment con Nessus sulla macchina Metasploitable (indirizzo ip 192.168.1.54):



Analizzo 2 vulnerabilità a rischio elevato e 1 a rischio medio:

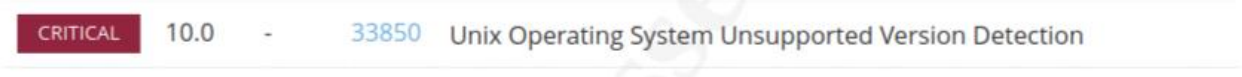
- ***Vulnerabilità rischio elevato***



Il server VNC (è un software che consente di condividere e controllare il desktop di un computer da un'altra posizione tramite una connessione di rete) che opera su Metasploitable è attualmente vulnerabile a causa dell'utilizzo di una password debole. In particolare, Nessus è riuscito ad accedere con successo utilizzando l'autenticazione VNC e inserendo una password estremamente semplice, ossia 'password'. Questa situazione apre la porta a un possibile attacco da parte di un malintenzionato remoto e non autenticato, il quale potrebbe sfruttare questa vulnerabilità per ottenere il controllo completo del sistema.

Per mitigare questo rischio, è necessario proteggere il servizio VNC attraverso l'implementazione di una password robusta e sicura. Una password forte dovrebbe essere composta da una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali, garantendo così una maggiore resistenza agli attacchi di forza bruta e migliorando complessivamente la sicurezza del sistema.

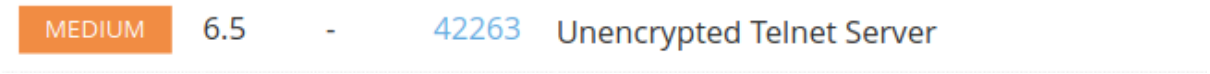
- ***Vulnerabilità rischio elevato***



Il sistema operativo Unix su Metasploitable ha raggiunto una fase in cui il supporto non è più disponibile. Questo significa che il fornitore non rilascerà ulteriori patch di sicurezza per questa versione. Questa situazione potrebbe renderlo vulnerabile a potenziali minacce di sicurezza, poiché non beneficerà di correzioni e miglioramenti di sicurezza più recenti.

La soluzione consigliata è quella di effettuare un aggiornamento a una versione del sistema operativo Unix attualmente supportata. Questo garantirà che il tuo sistema sia allineato con le più recenti misure di sicurezza e riceva tempestivamente gli aggiornamenti necessari per proteggerti da potenziali vulnerabilità.

- ***Vulnerabilità rischio medio***



Metasploitable utilizza un server Telnet su un canale non crittografato. Il problema è che le informazioni di accesso, come username e password, insieme ai comandi, viaggiano in modo non sicuro. Questo significa che un potenziale attaccante remoto, posizionato tra la connessione tra il tuo computer e il server, potrebbe intercettare queste informazioni in chiaro. In pratica, c'è il rischio che un malintenzionato possa ascoltare una sessione Telnet e ottenere accesso non autorizzato alle credenziali o ad altre informazioni sensibili. Inoltre, c'è anche la possibilità di modificare il traffico tra il client e il server.

La soluzione consigliata è passare a SSH (Secure Shell) anziché continuare con Telnet. SSH offre un canale crittografato che protegge le credenziali dagli sguardi indiscreti e fornisce un ambiente più sicuro per le comunicazioni tra il computer e il server remoto (in questo caso Metasploitable).