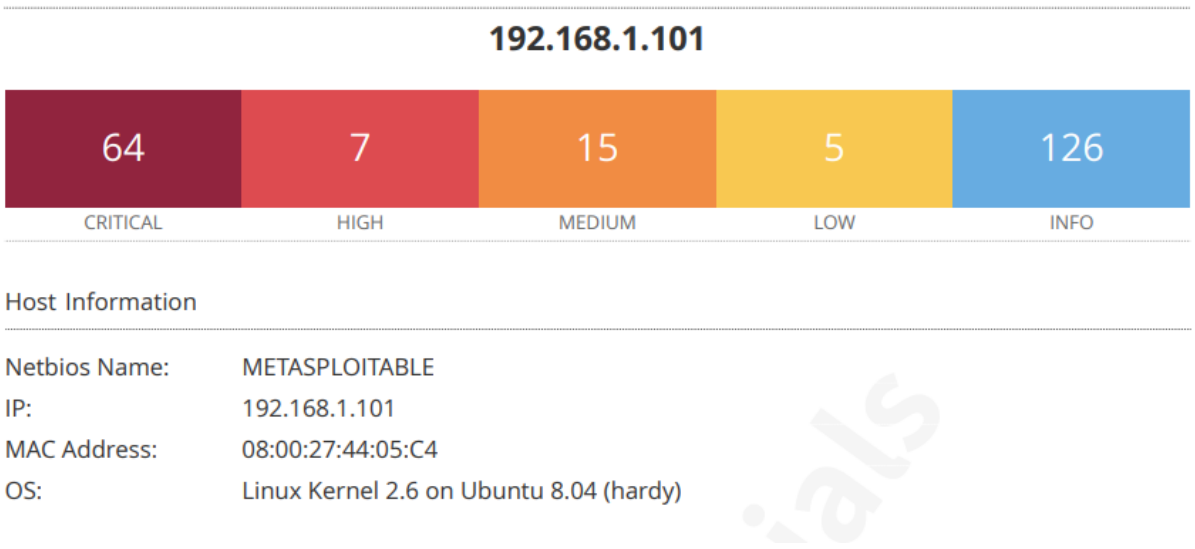
Report W12D1 – Scansione vulnerabilità Metasploitable (192.168.1.101) **Peppoli**

Per la scansione delle vulnerabilità di Metasploitable utilizzeremo Nessus, uno dei software più rinomati per la scansione e la valutazione della sicurezza informatica. È un potente strumento progettato per identificare vulnerabilità nei sistemi informatici, rilevare configurazioni non sicure e individuare potenziali minacce alla sicurezza. Nessus utilizza una vasta gamma di test e tecniche per esaminare reti, server, dispositivi e applicazioni alla ricerca di punti deboli che potrebbero essere sfruttati da attaccanti informatici. Il software fornisce report dettagliati e raccomandazioni per aiutare gli amministratori di sistema e i professionisti della sicurezza a mitigare i rischi e rafforzare la sicurezza delle infrastrutture IT.

Elenco delle vulnerabilità trovate:



Come si può notare abbiamo trovato:
Critiche: Queste sono le vulnerabilità più serie e potenzialmente dannose per un sistema. Possono consentire agli attaccanti di ottenere accesso completo al sistema o di eseguire codice dannoso senza autenticazione.

Alte: Le vulnerabilità considerate di gravità alta possono ancora costituire una minaccia significativa per la sicurezza dei sistemi. Possono consentire l'accesso non autorizzato o l'esecuzione di azioni dannose, anche se potrebbero richiedere condizioni specifiche per essere sfruttate.

Medie: Le vulnerabilità di gravità media rappresentano un rischio meno critico rispetto alle precedenti, ma possono comunque essere sfruttate dagli aggressori per compromettere la sicurezza dei sistemi.

Basse: Queste vulnerabilità sono considerate meno critiche e possono rappresentare un rischio limitato per la sicurezza. Tuttavia, è comunque consigliabile correggerle per mantenere un livello ottimale di sicurezza.

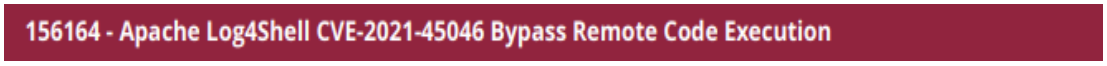
Informative (Info): Questo tipo di vulnerabilità fornisce informazioni aggiuntive sul sistema, come configurazioni non ottimali o informazioni sul software utilizzato. Anche se non rappresentano un rischio diretto per la sicurezza, possono essere utili per migliorare la configurazione e la gestione del sistema.

Nessus identifica queste vulnerabilità attraverso una serie di test e controlli che esaminano le configurazioni di sistema, le versioni del software, le patch applicate e altri fattori che potrebbero influenzare la sicurezza complessiva del sistema.

Valutiamo alcune vulnerabilità per tipo: FR = fattore di rischio

Vulnerabilità Critica

Riepilogo: È presente un connettore AJP vulnerabile in ascolto sull'host remoto. FR= Alto



Vulnerabilità Critica

Riepilogo: La versione di Apache Log4j utilizzata sul server remoto è interessata da una vulnerabilità legata all'esecuzione di codice in modalità remota. FR= Alto

Vulnerabilità Critica

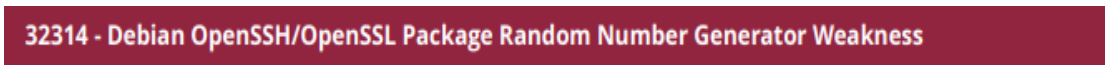
Riepilogo: La versione di Apache Log4j utilizzata sul server remoto è interessata da una vulnerabilità legata all'esecuzione di codice in modalità remota FR= Alto

Vulnerabilità Critica

Riepilogo: Sull' host remoto è installata una versione non supportata di Apache Tomcat FR= Alto

Vulnerabilità Critica

Riepilogo: L'host remoto potrebbe essere stato compromesso FR= Alto



Vulnerabilità Critica

Riepilogo: Le chiavi SSH dell'host remoto sono deboli FR= Alto

Vulnerabilità Alta

Riepilogo: Il servizio rlogin è in esecuzione sull' host remoto. FR= Alto

Vulnerabilità media

Riepilogo: Le funzioni di debug sono abilitate sul server Web remoto. FR= Medio

Vulnerabilità bassa

Riepilogo: Un server X11 è in ascolto sull'host remoto. FR= Basso

Vulnerabilità info

Riepilogo: Le patch di sicurezza sono sottoposte a backport. FR= Nessuno

Conclusioni:

1. **Sommario delle Azioni Raccomandate**: In considerazione delle numerose vulnerabilità identificate, si raccomanda di implementare un piano di azione suddiviso in fasi per risolvere le criticità più urgenti e ridurre il rischio complessivo per l'host. Questo include l'applicazione di patch, l'aggiornamento del software e la configurazione dei controlli di sicurezza.
2. **Benefici delle Azioni Raccomandate**: L'attuazione delle azioni proposte garantirà un notevole miglioramento della sicurezza dell'host, riducendo significativamente il rischio di compromissione e proteggendo i dati sensibili e critici. Ciò migliorerà la reputazione e la fiducia degli stakeholder nell'integrità del sistema.
3. **Rischio Residuo**: Nonostante gli sforzi per mitigare le vulnerabilità, è importante riconoscere che potrebbe persistere un rischio residuo. Tuttavia, con l'implementazione delle misure correttive, questo rischio sarà ridotto a un livello accettabile e gestibile.
4. **Pianificazione e Priorità**: Si propone di stabilire una roadmap dettagliata per l'attuazione delle azioni correttive, con un focus iniziale sulle 64 vulnerabilità critiche. Le fasi successive affronteranno le restanti vulnerabilità in base alla loro gravità e al livello di esposizione al rischio.
5. **Risorse Necessarie**: Sarà necessario un team dedicato di specialisti della sicurezza informatica per implementare con successo le soluzioni proposte. È richiesta anche un'allocazione finanziaria adeguata per l'acquisizione di strumenti e risorse supplementari necessarie per l'attuazione del piano.
6. **Coinvolgimento dell'Alta Direzione**: L'impegno e il sostegno dell'alta direzione sono essenziali per garantire il successo dell'iniziativa di sicurezza informatica. L'approvazione finanziaria e il supporto strategico dimostreranno l'importanza attribuita alla sicurezza dei dati e alla protezione dell'infrastruttura IT.
7. **Conclusioni e Riepilogo**: In conclusione, l'identificazione di numerose vulnerabilità richiede un'immediata azione correttiva per garantire la sicurezza e l'integrità dell'host. Il piano proposto mira a mitigare i rischi e a proteggere l'organizzazione da potenziali minacce informatiche.
8. **Ringraziamenti e Disponibilità**: Ringraziamo il dirigente per l'attenzione dedicata al report e ci mettiamo a disposizione per ulteriori discussioni o chiarimenti. Lavoreremo insieme per garantire un ambiente informatico sicuro e protetto per l'intera organizzazione.