REPORT SICUREZZA

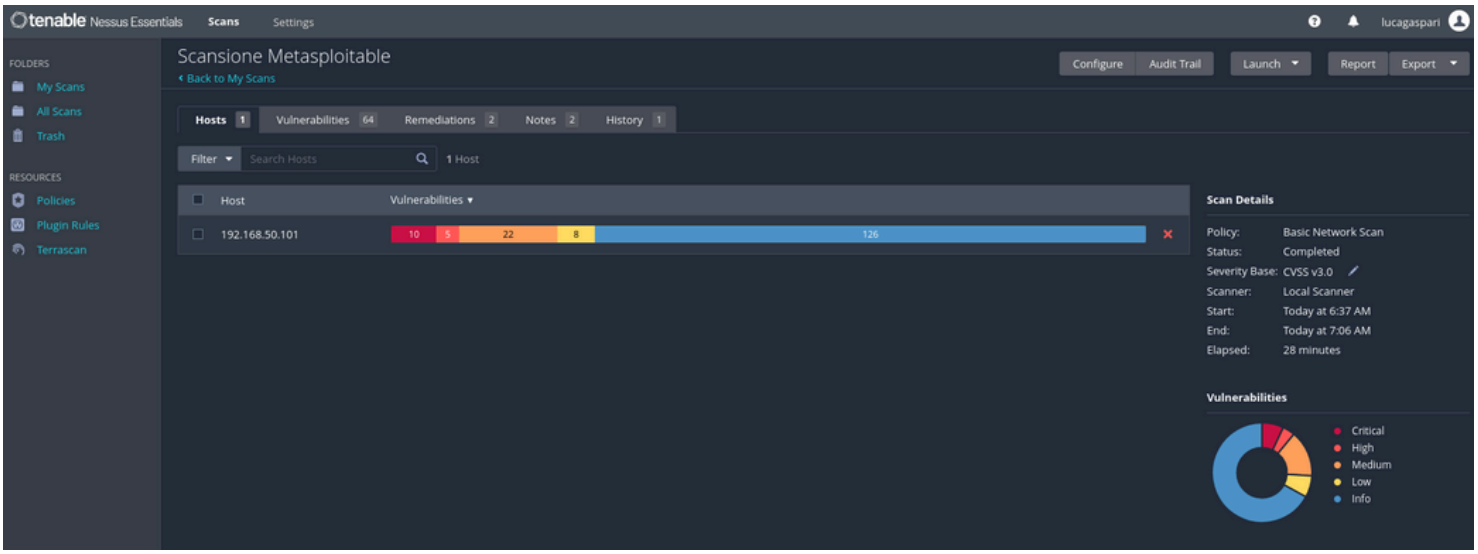
METASPLOITABLE

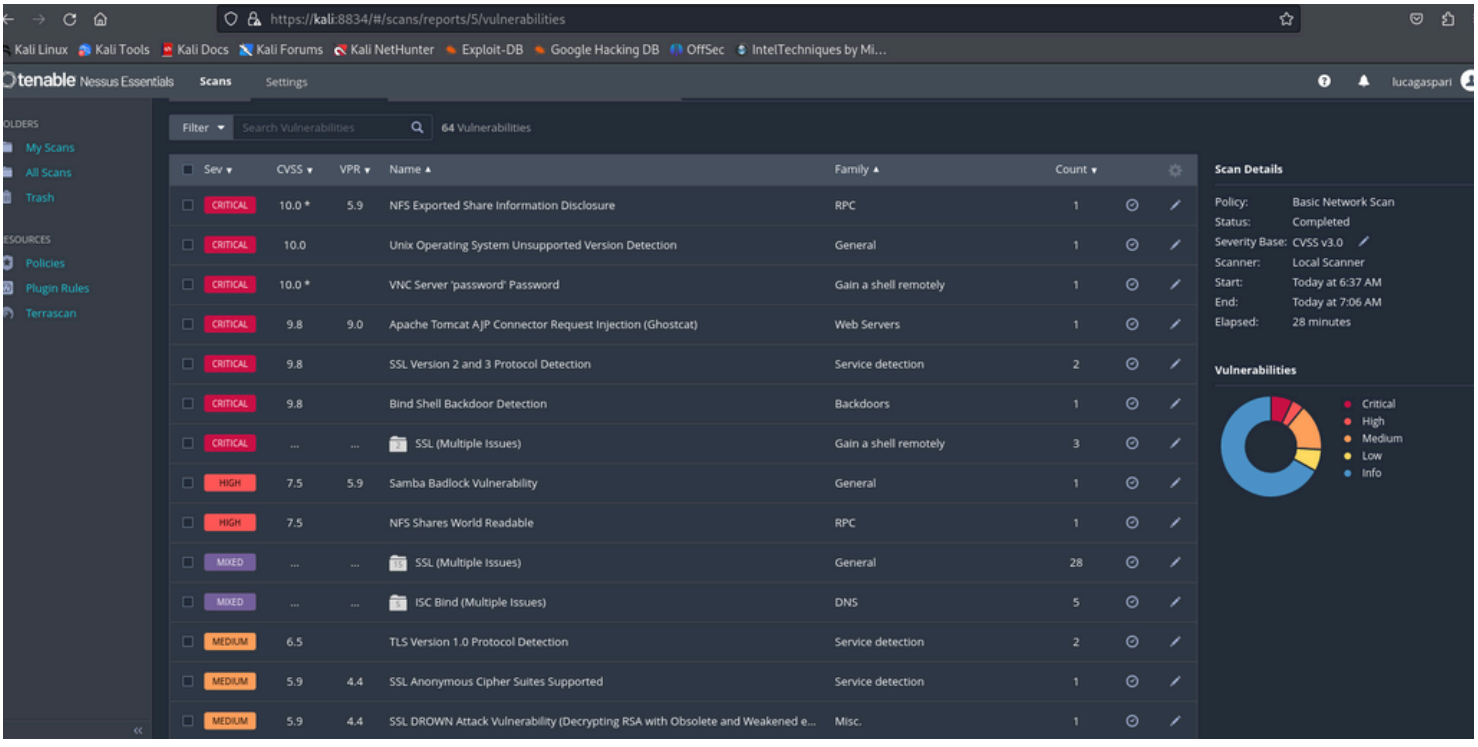
SOMMARIO

Il presente report dettaglia i risultati di una scansione di sicurezza effettuata utilizzando Nessus, che ha identificato diverse vulnerabilità critiche e di alta gravità all'interno di Metasploitable. Queste vulnerabilità, se non mitigate, potrebbero potenzialmente permettere accessi non autorizzati, perdite di dati, e altri rischi per la sicurezza dell'organizzazione.

Dettagli della Scansione

- Strumento di Scansione: Nessus
- Tipo di Scansione: Basic Network Scan
- Durata: 28 minuti
- Data: 9/5/2024





Vulnerabilità Critiche

VNC Server 'password' Password (CVSS 10.0)

- **Descrizione**: Questa vulnerabilità è stata identificata in un server VNC che utilizza una password di default o debole, questo può permettere ad un attaccante di accedere facilmente al sistema remoto e di eseguire azioni con i privilegi dell'utente che ha avviato il servizio VNC, potenzialmente ottenendo il controllo completo del sistema.
- **Raccomandazione**: Cambiare immediatamente la password in una più forte e complessa, considerare l'implementazione di autenticazione a due fattori e limitare l'accesso al server VNC attraverso una rete sicura o VPN.

Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVSS 9.8)

- **Descrizione**: La vulnerabilità Ghostcat permette agli attaccanti di leggere o includere file sul server Apache Tomcat attraverso il connettore AJP. Gli attaccanti possono sfruttarla per visualizzare file di configurazione sensibili, codice sorgente dell'applicazione o addirittura iniettare file eseguibili, portando a una compromissione del server.
- **Raccomandazione**: Aggiornare Apache Tomcat alla versione che non è affetta da questa vulnerabilità o disabilitare il connettore AJP se non è necessario per le operazioni del server.

SSL Version 2 and 3 Protocol Detection (CVSS 9.8)

- **Descrizione**: Questa vulnerabilità indica che i protocolli SSL versione 2 e 3 sono abilitati, questi protocolli sono considerati obsoleti e vulnerabili a numerosi attacchi, come il famoso POODLE. L'uso di questi protocolli può mettere a rischio la sicurezza delle comunicazioni criptate.
- **Raccomandazione**: Disabilitare SSLv2 e SSLv3 sui server interessati e abilitare TLS 1.2 o superiore.

Bind Shell Backdoor Detection (CVSS 9.8)

- **Descrizione**: La rilevazione di una bind shell backdoor suggerisce che il sistema è stato compromesso per permettere agli attaccanti di connettersi in remoto e eseguire comandi arbitrari. Questo tipo di backdoor può essere usato per mantenere l'accesso persistente a un sistema compromesso anche dopo che le vulnerabilità originali sono state mitigate.

Vulnerabilità di Alta Gravità

Samba Badlock Vulnerability (CVSS 7.5)

- **Descrizione**: Questa vulnerabilità, conosciuta come "Badlock", colpisce i server Samba, è una debolezza di sicurezza che può essere sfruttata per causare negazioni di servizio (DoS). Questo può permettere agli attaccanti di intercettare o modificare le sessioni di autenticazione e dati sensibili.
- **Raccomandazione**: È essenziale applicare le patch di sicurezza fornite dal team di Samba per correggere questa vulnerabilità. Inoltre, monitorare il traffico di rete per rilevare attività sospette e limitare l'accesso ai servizi Samba ai soli client fidati.

NFS Shares World Readable (CVSS 7.5)

- **Descrizione**: È stata rilevata una configurazione in cui le condivisioni NFS sono leggibili globalmente, il che espone i file a chiunque nella rete. Questo può portare a una non autorizzata divulgazione di informazioni sensibili.
- **Raccomandazione**: Modificare le impostazioni di NFS per limitare l'accesso alle condivisioni solo agli utenti e ai gruppi che necessitano di accesso. Implementare controlli di accesso più stringenti e considerare l'uso di tecniche di cifratura per proteggere i dati sensibili.

Le vulnerabilità elencate rappresentano rischi significativi che devono essere affrontati prontamente per mantenere l'integrità e la sicurezza della rete e dei dati

Vulnerabilità di Livello Medio

TLS Version 1.0 Protocol Detection (CVSS 6.5)

- **Descrizione**: La presenza del protocollo TLS 1.0 nel sistema indica l'uso di una tecnologia di crittografia considerata obsoleta e vulnerabile. Nonostante TLS 1.0 non sia suscettibile come SSLv2 e SSLv3, è comunque esposto a vari attacchi crittografici che potrebbero compromettere la sicurezza dei dati trasmessi.
- **Raccomandazioni**: Aggiornare i sistemi per supportare versioni più recenti di TLS, preferibilmente TLS 1.2 o TLS 1.3, che offrono miglioramenti significativi in termini di sicurezza e privacy. Disabilitare TLS 1.0 nelle configurazioni dei server e dei client.

SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) (CVSS 5.9)

- **Descrizione**: Questa vulnerabilità permette agli attaccanti di decriptare le comunicazioni protette da SSLv2 utilizzando tecniche di attacco side-channel. L'attacco DROWN sfrutta i server che hanno ancora abilitato SSLv2 per decriptare connessioni protette da crittografia più moderna, compromettendo la sicurezza delle sessioni TLS.
- **Raccomandazioni**: Disabilitare completamente SSLv2 su tutti i dispositivi nella rete, è consigliabile verificare che nessun certificato venga condiviso tra servizi che utilizzano SSL/TLS per ridurre ulteriormente il rischio di attacchi.

Vulnerabilità di Livello Basso

SSL Anonymous Cipher Suites Supported (CVSS 4.4)

- **Descrizione**: Il server supporta l'uso di suite di cifratura anonime in SSL/TLS, che non autenticano la sessione e lasciano le connessioni vulnerabili a attacchi man-in-the-middle. Questo tipo di suite di cifratura non fornisce l'identità crittografica delle parti nella comunicazione, aumentando il rischio di intercettazioni non autorizzate.
- **Raccomandazioni**: Configurare i server per non accettare suite di cifratura anonime durante la negoziazione di sessioni SSL/TLS. Utilizzare solo suite di cifratura che forniscono autenticazione e integrità sia del client che del server.

SSL DROWN Attack Vulnerability (CVSS 4.4)

- **Descrizione:** Questa è un'altra occorrenza dell'attacco DROWN indicata con un punteggio CVSS diverso, possibilmente riflettendo una configurazione diversa o un impatto meno critico in un altro contesto della rete. Nonostante sia classificata come minaccia di livello basso, richiede attenzione.
- **Raccomandazioni:** Le stesse raccomandazioni per la vulnerabilità di livello medio si applicano anche qui. Disabilitare SSLv2 e assicurarsi di non usare certificati condivisi tra servizi che utilizzano differenti versioni di SSL/TLS.