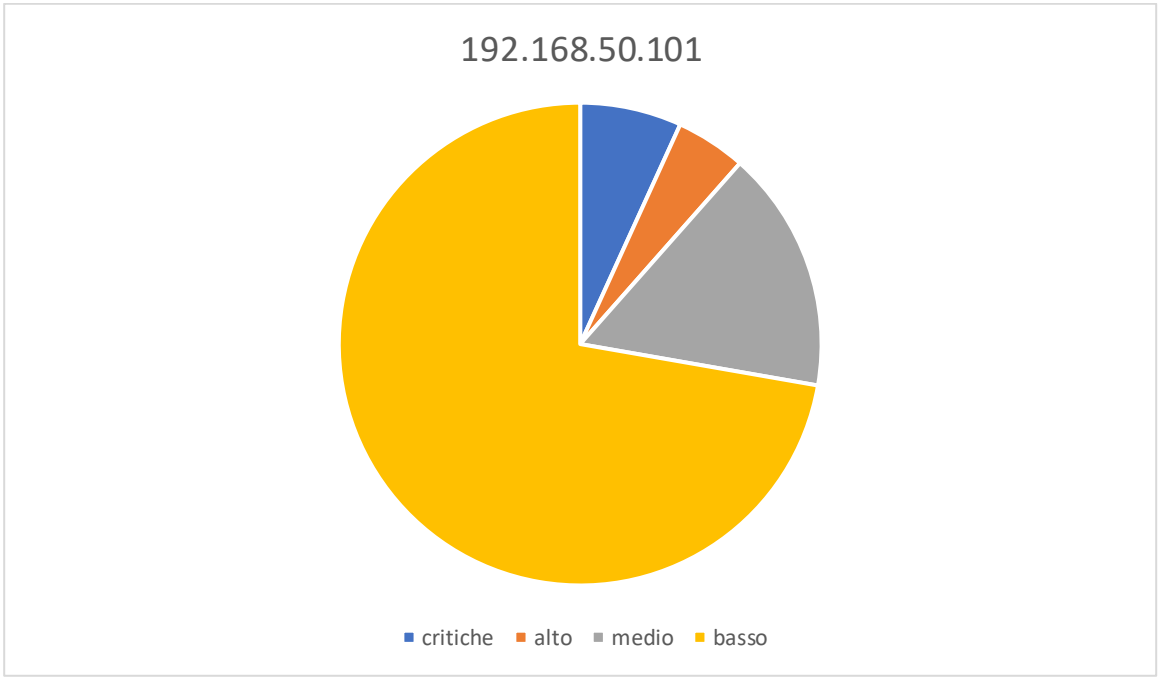
Report sulle Vulnerabilità – Metasploitable

La seguente analisi delle vulnerabilità è stata condotta sul sistema Metasploitable al fine di identificare le aree di rischio potenziale a fornire raccomandazioni per mitigare tali vulnerabilità.



Informazioni scansione

Inizio 26/08/2023 16:30:20

Fine 26/08/2023 16:34:15

Informazioni Host

Nome Host Metasploitable

IP 192.168.50.101

OS Linux Vulnerabilità vsFTPd versione 2.3.4. Backdoor

Descrizione

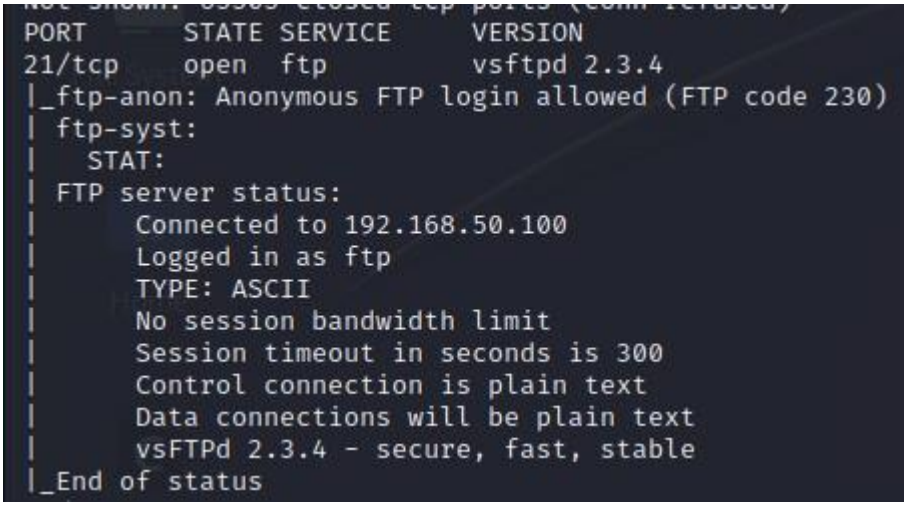
La vulnerabilità CVE-2011-2523 è una backdoor presente nella versione 2.3.4. del server FTP vsftpd. Questa backdoor consente

ad un attaccante remoto di ottenere l'accesso al sistema senza le credenziali corrette. La backdoor è stata inserita nel codice sorgente del software e consente all'attaccante di eseguire comandi arbitrari con privilegi elevati(root) sul sistema compromesso.

Soluzione

Disabilita l'accesso FTP anonimo o limita l'accesso solo a utenti autorizzati.

Aggiornare vsftpd all'ultima versione.



Fattore di rischio : Critico Vulnerabilità

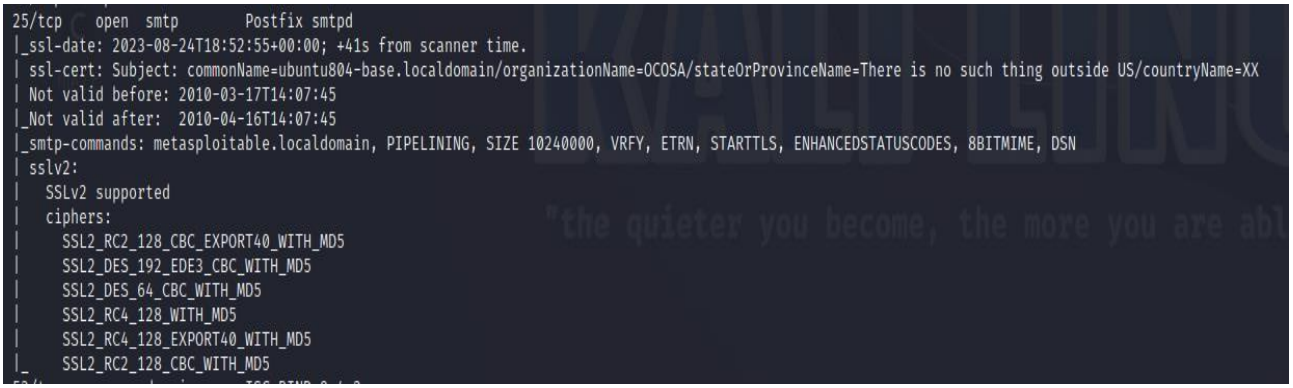
Porta 25 e 5432 ssl-dh-params

Descrizione

Questa vulnerabilità consente a un attaccante di ricevere dati in chiaro utilizzando un attacco padding-oracle.

Soluzione

Assicurarsi di disabilitare ssl e utilizzare tls



Fattore di rischio : Alto

Vulnerabilità

Porta 25 ssl-dh-params

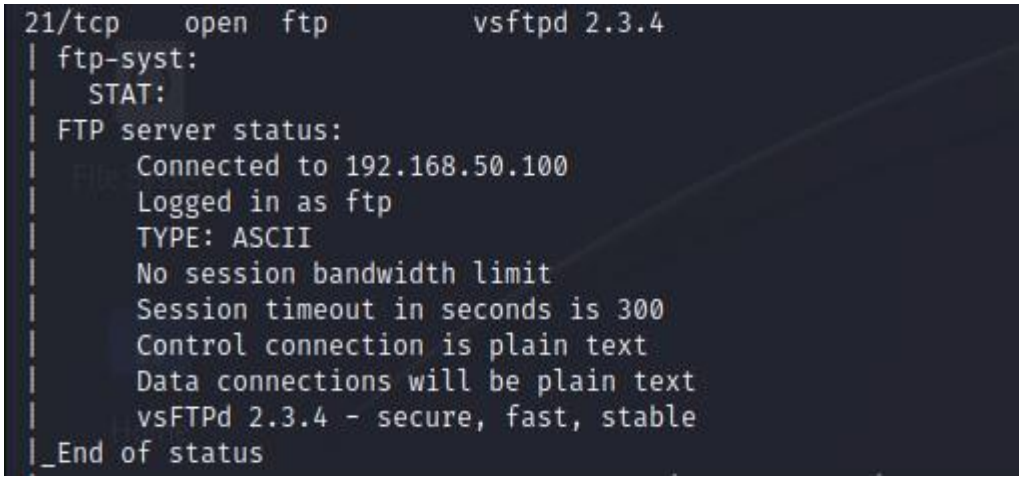
Descrizione

Questa vulnerabilità riguarda l'Exchange di chiavi DH e potrebbe permettere a un attaccante di compromettere la confidenzialità e l'integrità dei dati.

Soluzione

Si consiglia di rinforzare l'uso di DH

Risoluzione prima vulnerabilità:



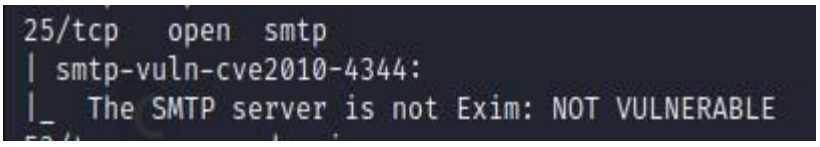
Spiegazione

Per mitigare questa vulnerabilità, è essenziale aggiornare il software vsftpd alla

versione più recente, che corregge questa vulnerabilità. Inoltre, è importante monitorare regolarmente i server FTP per rilevare eventuali attività sospette e adottare pratiche di sicurezza solide per proteggere i sistemi da intrusioni.

Inoltre è fondamentale tenere sempre aggiornati i software di sistema e le applicazioni per proteggere i sistemi da vulnerabilità conosciute e per garantire un ambiente di rete sicuro.

Seconda vulnerabilità :



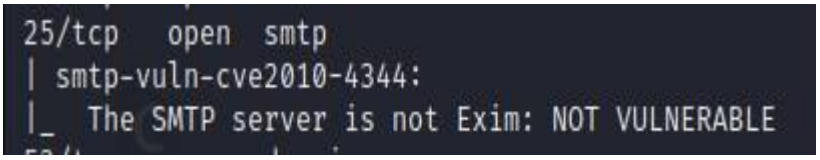
Soluzione

Disabilitare SSL :

Verifica la configurazione del tuo server e assicurati che tutti i protocolli SSL siano disabilitati. SSl è considerato insicuro a causa di numerose vulnerabilità e dovrebbe essere evitato. Assicurati che solo i protocolli TLS siano abilitati.

Abilitare TLS con Parametri sicuri utilizzi le versioni più recenti dei protocolli TLS.

Terza vulnerabilità



Soluzione

Rinforzare i parametri DH

Se il tuo server utilizza il protocollo DiffieHellman, assicurati che sia configurato con gruppi DH sufficientemente robusti. Evita l'uso di gruppi DH con lunghezza inferiore a 2048 bit.