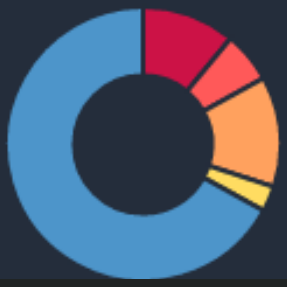
SCANSIONE NESSUS

SU METASPLOITABLE

Host Details

IP:	192.168.50.101
MAC:	08:00:27:CF:71:97
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 2:21 PM
End:	Today at 2:52 PM
Elapsed:	32 minutes
KB:	Download

Vulnerabilities



Nessus ci offre una panoramica chiara dello stato della sicurezza, Vediamo la sua capacità di rilevare una vasta gamma di vulnerabilità,

Vulnerabilities

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	31705	SSL Anonymous Cipher Suites Supported
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	10407	X Server Detection

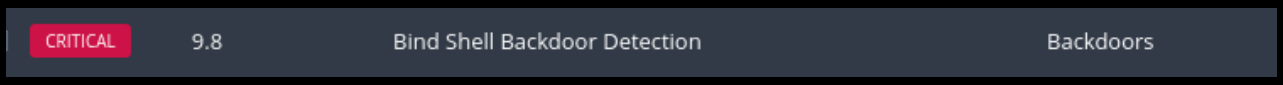
Obiettivi

La vulnerabilità "Apache Tomcat AJP Connector Request Injection" riguarda il protocollo AJP utilizzato per la comunicazione tra un server web Apache Tomcat e un server frontend come Apache HTTP Server. Gli attaccanti possono sfruttare questa vulnerabilità manipolando le richieste AJP per eseguire azioni non autorizzate sul server Tomcat o comprometterne la sicurezza.

Per mitigare questo rischio, è consigliabile:

1. Aggiornare Apache Tomcat alla versione più recente.
2. Configurare correttamente il server Tomcat.
3. Implementare filtri per l'input delle richieste AJP per sanificare e validare i dati in ingresso.
4. Monitorare e registrare le attività sospette.
5. Utilizzare firewall per limitare l'accesso al server Tomcat.
6. Applicare tempestivamente le patch di sicurezza rilasciate dagli sviluppatori di Apache Tomcat.

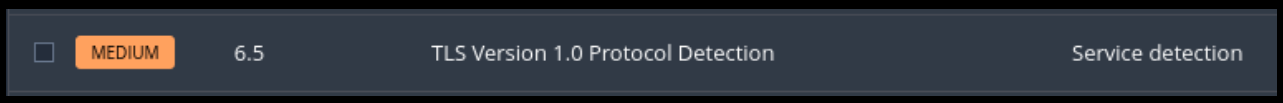
Obiettivi



Una backdoor è una vulnerabilità o un meccanismo nascosto che consente l'accesso non autorizzato al sistema, bypassando le normali procedure di sicurezza.
Per risolvere questa vulnerabilità:

1. Verificare dell'autenticità: Verificare se la segnalazione della backdoor è confermata e se effettivamente rappresenta una minaccia per il sistema.
2. Aggiornamento del software: Assicurarsi di utilizzare la versione più recente e aggiornata di Band Shell, poiché gli sviluppatori spesso rilasciano correzioni per le vulnerabilità.
3. Analisi approfondita: Condurre un'analisi dettagliata del sistema per individuare eventuali segni di compromissione o attività sospette correlate alla backdoor di Band Shell.
4. Disabilitazione o rimozione: Se confermata l'esistenza della backdoor, prendi provvedimenti per disabilitarla o rimuoverla dal sistema.
5. Monitoraggio continuo: Implementare un sistema di monitoraggio costante per rilevare eventuali tentativi di sfruttare la backdoor e per reagire prontamente.
6. Rafforzamento della sicurezza: Rivedere e potenziare le misure di sicurezza complessive del sistema, inclusi l'accesso utente, le autorizzazioni di sistema e le politiche di sicurezza.

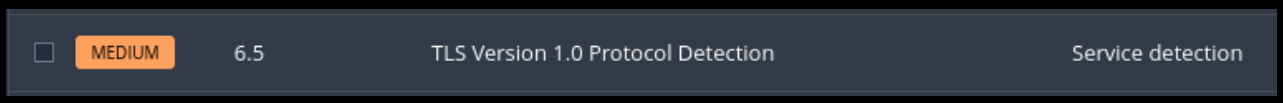
Obiettivi



La rilevazione del protocollo TLS versione 1.0 indica che il sistema supporta una versione obsoleta e meno sicura del protocollo di crittografia TLS (Transport Layer Security). Poiché TLS 1.0 è vulnerabile a diverse vulnerabilità di sicurezza note, è consigliabile disabilitarlo o aggiornare a versioni più recenti e sicure come TLS 1.2 o TLS 1.3.
Per risolvere questa criticità:

- **Aggiornamento del software**: Assicurarsi che il software del server supporti le versioni più recenti e sicure di TLS.

Obiettivi



La rilevazione del protocollo TLS versione 1.0 indica che il sistema supporta una versione obsoleta e meno sicura del protocollo di crittografia TLS (Transport Layer Security). Poiché TLS 1.0 è vulnerabile a diverse vulnerabilità di sicurezza note, è consigliabile disabilitarlo o aggiornare a versioni più recenti e sicure come TLS 1.2 o TLS 1.3.
Per risolvere questa criticità:

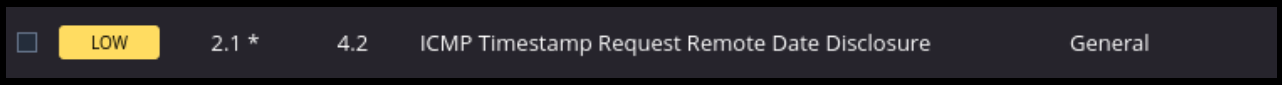
- **Aggiornamento del software**: Assicurarsi che il software del server supporti le versioni più recenti e sicure di TLS.

Obiettivi

La "Server Detection" indica che il server web fornisce informazioni dettagliate sulla sua identità e configurazione durante l'handshake iniziale. Questo può includere il nome e la versione del software del server, il sistema operativo e altre informazioni che potrebbero essere utilizzate da un potenziale aggressore per individuare vulnerabilità specifiche o condurre attacchi mirati.
Per mitigare questo rischio:

1. Nascondere le informazioni di identificazione del server: Configura il server per nascondere o minimizzare le informazioni fornite durante l'handshake iniziale. Questo può essere fatto attraverso la configurazione del server web per limitare le informazioni divulgate o utilizzando moduli o patch aggiuntivi progettati per mascherare o modificare le risposte del server.
2. Aggiornare il software.

Obiettivi



1. La rilevazione di "ICMP Timestamp Request Remote Date Disclosure" indica che il server sta rispondendo alle richieste ICMP Timestamp. Questo tipo di risposta può essere sfruttato da un aggressore per ottenere informazioni sulla data e l'ora del server remoto, che potrebbero essere utilizzate per scopi malevoli come il fingerprinting del sistema o il coordinamento di attacchi mirati.
2. **Disabilitare le risposte ICMP Timestamp**: Configurare il server per non rispondere alle richieste ICMP Timestamp. Questo può essere fatto attraverso la configurazione del firewall o del sistema operativo per filtrare o bloccare le richieste ICMP Timestamp in entrata.
3. **Limitare l'esposizione delle informazioni**: Verificare e limitare le informazioni sensibili che il server divulga pubblicamente. Ridurre al minimo le informazioni sulla data e sull'ora disponibili tramite altri mezzi di comunicazione.
4. **Aggiornare e configurare il firewall**: Assicurarsi che il firewall sia configurato correttamente per filtrare o bloccare le richieste ICMP Timestamp in ingresso, se necessario.