Vulnerability Assessment Nessus

Abbiamo effetuato un Vulnerability Assessment indicando come target la macchina Metasploitable2 , analizzando tutte le porte con il “Basic network scan” come risultato otteniamo questo Report in allegato.



Ora andremo ad analizzare alcune vulnerabilitá ottenute:

* **Apache Tomcat AJP Connector Request Injection (Ghostcat):**

QQuesta vulnerabilità richiede l'accesso alla porta AJP ,AJP è un protocollo utilizzato per la comunicazione tra un server web (come Apache HTTP Server) e Tomcat, generalmente utilizzato per migliorare le prestazioni e fornire funzionalità aggiuntive. La vulnerabilità Ghostcat è una vulnerabilità di lettura/inclusione di file che consente a un aggressore di leggere file sul server Tomcat. Un aggressore può creare una richiesta AJP appositamente progettata e inviarla al connettore AJP di Tomcat. Se avrà successo, potrà accedere a file di configurazione, codice sorgente e potenzialmente altre informazioni sensibili sul server.

Soluzioni:

1. Aggiornare Tomcat: Il modo migliore per proteggersi da Ghostcat è aggiornare il server Tomcat a una versione che include una correzione per la vulnerabilità. La vulnerabilità è stata risolta nelle versioni 9.0.31, 8.5.51 e 7.0.100. **http://www.nessus.org/u?107f9bdc**
2. Disabilitare AJP: Se non state utilizzando attivamente il connettore AJP, potete disabilitarlo per eliminare la superficie di attacco.

* **Bind Shell Backdoor Detection:**

É una tecnica o un processo utilizzato per individuare backdoor o porte di accesso non autorizzate nei sistemi. Le backdoor vengono create dagli aggressori per ottenere un accesso non autorizzato a un sistema, consentendo loro di eseguire comandi. La "Bind Shell Backdoor Detection" è il processo di individuazione di tali backdoor implementate tramite il meccanismo di "bind shell". In sostanza, la rilevazione di backdoor attraverso una bind shell si concentra sul monitoraggio del traffico di rete, dei log di sistema e l'identificazione di connessioni o comportamenti sospetti.

Soluzioni:

1. Aggiornamenti e Patching**:** Mantieni il tuo sistema operativo, le applicazioni e i servizi costantemente aggiornati con le ultime patch di sicurezza.
2. Firewall**:** Configura un firewall per limitare le connessioni in entrata e in uscita sul tuo sistema. Le regole del firewall possono aiutare a controllare quali porte sono accessibili dall'esterno e quali non lo sono.

* **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness:**

Questa vulnerabilità si è verificata nelle versioni di Debian comprese tra la 3.1 e la 4.0. Durante questo periodo, un manutentore di Debian aveva apportato una modifica nell'algoritmo di generazione dei numeri casuali all'interno delle librerie OpenSSL, pensando di migliorarne la performance. Tuttavia, questa modifica ha avuto l'effetto contrario, rendendo le chiavi crittografiche deboli e prevedibili. Poiché SSH e SSL/TLS sono ampiamente utilizzati per comunicazioni sicure, avere chiavi crittografiche deboli costituisce un serio rischio per la sicurezza, in quanto potenzialmente consente a un aggressore di decifrare le comunicazioni cifrate o addirittura di impersonare un server remoto.

Soluzione:

1. Aggiornamento dei pacchetti: Assicurati che il sistema Debian sia aggiornato con gli ultimi aggiornamenti di sicurezza
2. Rigenerazione delle chiavi crittografiche: Se il sistema Debian è stato compromesso o se le chiavi crittografiche sono state generate durante il periodo in cui era presente la vulnerabilità, è importante rigenerare tutte le chiavi crittografiche.

**http://www.nessus.org/u?107f9bdc**