Vulnerability Assessment Meta2.

Abbiamo effettuato 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 e a risolvere 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. Per farlo in Metasploitable2 basta entrare nella configurazione di Tomcat5.5 (Nel nostro caso abbiamo questa versione) usando **cd** e modificare il file **server.xml**

**<Connector protocol="AJP/1.3" port="8009" redirectPort="8443" />** commentando questa riga

* **VNC Server 'password' Password:**

Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password", che un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

**Soluzione:**

1. Aggiornamento password: Proteggi il servizio VNC con una password complessa usando almeno 8 caratteri di cui uno speciale, in questo modo renderai l’accesso piú sicuro. Su Meta2 i comandi sono:

**vncpasswd** e si puó cambiare password

**vncserver -kill :1** per chiudere il programma

**vncserver** per avviare nuovamente il server

* **SSL Medium Strength Cipher Suites Supported (SWEET32)**

SSL Medium Strength Cipher Suites Supported (SWEET32) è una vulnerabilità o debolezza della sicurezza che riguarda le suite crittografiche utilizzate nei protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS). Non si tratta di una funzionalità o di uno standard, ma piuttosto di un problema di sicurezza

**Soluzione:**

1. Accedi a Metasploitable2 e individua il file di configurazione di Apache: Di solito, il file di configurazione principale di Apache su molte distribuzioni di Linux è situato in “/etc/apache2” In Metasploitable 2, potrebbe essere in una posizione leggermente diversa quindi cercare il file di configurazione di Apache nella directory corretta.
2. Modifica il file di configurazione: Apri il file di configurazione di Apache con un editor di testo (nano). Cerca la sezione che riguarda la configurazione SSL/TLS. Questa sezione dovrebbe contenere dettagli su quale suite di cifratura è abilitata.
3. Disabilita le suite di cifratura deboli: Cerca le righe che abilitano le suite di cifratura deboli come 3DES e Blowfish. Le suite di cifratura sono elencate in una sezione come "SSLCipherSuite". Modificare questa sezione per includere solo suite di cifratura forti e sicure, come AES (Advanced Encryption Standard) con chiavi di lunghezza adeguata. Ad esempio:

**SSLCipherSuite HIGH:!aNULL:!MD5**

Questo comando disabiliterà suite di cifratura deboli e algoritmi di hash insicuri come MD5.

1. Riavvia Apache: Dopo aver apportato queste modifiche, salva il file di configurazione e riavvia il server Apache con il seguente comando:

**sudo service apache2 restart**

* **Conclusioni:**

Per ovviare alle molteplici vulnerabilitá elencate nel report la soluzione migliore e quella di installare un Firewall all’interno di **Metasploitable2** in questo caso scegliamo **iptables**

Di seguito i vari comandi per installarlo e le regole che ho applicato in merito:

**sudo iptables -L** Controllare se è gia installato

**sudo apt-get install iptables** Installazione del programma

**sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT** Consente il traffico sulla porta 22 (SSH).

**sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT** Consente il traffico sulla porta 80 (HTTP).

**sudo iptables -A INPUT -j DROP** Blocca tutto il resto.

**sudo mkdir /etc/iptables** Crea la directory

**sudo iptables-save > /etc/iptables/rules.v4** Salva le nuove regole nella directory

****