Analisi report scansione con Nessus

Il file allegato è il report di una scansione verso la macchina Metasploitable in laboratorio virtuale.

Come possiamo vedere la scansione ha riscontrato 9 vulnerabilità critiche, 4 alte, 17 mede, 6 basse e 76 segnate come info ovvero che non sono vulnerabilità già gestite.

Ora andrò ad analizzare le prime 4 vulnerabilità critiche.

1.Apache Tomcat A JP Connector Request Injection (Ghostcat)

AJP è un protocollo che consente ad Apache Tomcat di comunicare con un server web, un utente malintenzionato non autenticato potrebbe collegarsi da remoto e sfruttare questa vulnerabilità per entrare nel server web ed avere accesso a file contenuti nello stesso.

Come soluzione posso consigliare di aggiornale la configurazione A JP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successiva.

Questi sono link che potrebbe aiutare nell'approfondire questa vulnerabilità:
http://www.nessus.org/u?8ebe6246

http://www.nessus.org/u?4e287adb

http://www.nessus.org/u?cbc3d54e

2. Bind Shell Backdoor Detection

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarla per collegandosi alla porta remota e prendere il controllo della macchina.

Alcune soluzioni potrebbero essere: controllare se la macchina è già stata infettata, ovvero che questa backdoor sia già stata utilizzata da un malintenzionato, in questo caso si consiglia di reistallare il sistema perchè potrebbe aver creato altre backdoor.

Una volta reinstallato il sistema operativo assicurarsi di mettere un'autenticazione sulla porta o chiuderla se non necessaria.

3. SSL Version 2 and 3 Protocol Detection

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono colpite da diverse vulnerabilità crittografiche.

Uno schema di riempimento non sicuro con cifrari CBC.

Schemi non sicuri di rinegoziazione e ripresa della sessione.

Un attaccante può sfruttare queste vulnerabilità per effettuare attacchi di tipo man-in-the-middle o per decrittare le comunicazioni tra il servizio interessato e i client. Pertanto, si consiglia di disabilitare completamente questi protocolli.

Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

Ecco alcuni approfondimenti:

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

4.Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Il server DNS remoto non utilizza porte casuali durante le query ai server DNS di terze parti. Un attaccante remoto non autenticato può sfruttare questa situazione per alterare il server DNS remoto, consentendo all'attaccante di deviare il traffico legittimo verso siti arbitrari. Così facendo l'attaccante può reindirizzare la vittima su dei siti creati da lui magari con dei virus o malware.

Si consiglia di contattare il fornitore di serve DNS per far patchare questa vulnerabilità.

Per maggiori informazioni:

https://www.cnet.com/news/massive-coordinated-dns-patch-released/

https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/