W12D1 – Scansione di Metasploitable con Nessus

Report tecnico. Esercizio obbligatorio

Ho eseguito un vulnerability assessment della macchina Metasploitable 2, con IP 192.168.50.101, scegliendo un basic network scan. Questo report analizza le principali vulnerabilità trovate, partendo da quelle critiche, propone delle soluzioni e va a completare il report in formato PDF creato automaticamente da Nessus alla fine della scansione. La prima vulnerabilità critica trovata è Bind Shell Backdoor Detection: significa che una shell è in ascolto sulla porta 1524 senza che sia richiesta alcuna autorizzazione e questo vuol dire che un attaccante può collegarsi da remoto e far eseguire dei comandi, magari malevoli. Per sfruttare questa vulnerabilità, è possibile collegarsi tramite netcat alla porta 1524 e controllare se è possibile eseguire dei comandi da remoto. Qualora questa vulnerabilità venisse effettivamente trovata, è necessario controllare se il sistema è manomesso, magari controllando i file di log, ed eventualmente reinstallarlo. Un'altra vulnerabilità critica trovata è Debian OpenSSH/OpenSSL Package Random Number Generator Weakness, che indica la presenza di SSH host keys remote generate su un sistema Debian o Ubuntu che ha un bug nella generazione dei numeri random nella libreria OpenSSL. Il bug è provocato da un pacchetto Debian che rimuove tutte le forme di entropia nella generazione delle chiavi e permette ad un attaccante di trovare le parti private delle chiavi remote e decriptare eventuali elementi criptati. Per questo, è necessario considerare che tutti i materiali criptati generati con SSH, SSL e OpenVPN non sono sicuri e vanno rigenerate le chiavi, soprattutto le parti private, con un sistema non vulnerabile. Un'altra vulnerabilità critica trovata è Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check), che implica l'utilizzo di una chiave debole da parte del certificato remoto SSL. Il certificato remoto x509 sul server remoto SSL è stato generato su un sistema Debian o Ubuntu con un bug nella generazione di numeri random nella libreria OpenSSL. Anche questo è dovuto alla presenza di un pacchetto Debian che rimuove ogni forma di entropia in OpenSSL e per questo è necessario rigenerare le chiavi, soprattutto quelle private, per proteggere i materiali protetti da chiavi SSH, SSL e OpenVPN che possono essere facilmente decriptati. Un'altra vulnerabilità critica trovata con Nessus è NFS Exported Share Information Disclosure. Questo vuol dire che è possibile accedere agli share NFS, e un attaccante può recuperarne le informazioni rintracciando uno share NFS esportato dal server remoto dell'host, riuscendo così a leggere o modificare dei file dell'host. È necessario configurare NFS affinché solo gli utenti autorizzati sull'host possano avere accesso agli NFS esportati, magari bloccando l'accesso ad NFS dall'esterno. L'ultima vulnerabilità di livello critico trovata è la password del server VNC, che è semplicemente "password". Il servizio VNC si trova sulla porta 5900 e in questo caso uno dei server VNC ha una password molto debole, per cui è stato possibile effettuare il login solamente con la password "password". A questo punto si rende necessario impostare una password più sicura. Un'altra vulnerabilità critica riscontrata è Apache Tomcat AJP Connector Request Injection; questo significa che un connettore AJP vulnerabile è in ascolto sul server remoto, e questo consente ad un attaccante di collegarsi al server remoto,

di avere accesso a file ed applicazioni web da remoto, di inviare del codice malevolo JavaServer Pages (JSP) e di far eseguire questo codice da remoto. La porta coinvolta è la porta 8009 AJP13. Per risolvere questa vulnerabilità, bisogna aggiornare la configurazione AJP per richiedere delle autorizzazioni ed aggiornare Tomcat ad una versione supportata, come le versioni 7.0.100, 8.5.51, 9.0.31 ed altre ultime versioni. Infine, un'altra vulnerabilità critica riscontrata è SSL Version 2 and 3 Protocol Detection, per cui il server remoto accetta del traffico di dati criptato con SSL 2.0 e 3.0, nonostante queste versioni del protocollo SSL abbiano dei problemi di sicurezza. Un attaccante può decriptare il traffico in transito tra client e server o lanciare attacchi man in the middle e per questo è consigliabile disabilitare completamente i protocolli SSL 2.0 e 3.0, perché un browser potrebbe usarli lo stesso se un attaccante riesce ad effettuare un downgrade del protocollo di cifratura utilizzato. È necessario anche assicurarsi di utilizzare la versione TLS 1.2 o superiore. La porta interessata da questa vulnerabilità è la porta 443 di Https.

Report per dirigenti. Esercizio facoltativo.

Il test di vulnerability assessment eseguito ha rilevato alcuni aspetti critici che richiedono un intervento per mettere in sicurezza la rete aziendale. Abbiamo a che fare con alcune vulnerabilità che rappresentano un pericolo critico per la sicurezza, che richiedono delle azioni risolutive non particolarmente complesse ma assolutamente necessarie per la sicurezza informatica aziendale. Esaminando le vulnerabilità critiche, la prima riscontrata è Bind Shell Backdoor Detection: a causa di questa vulnerabilità, un attaccante si può collegare alla macchina e far eseguire del codice spesso malevolo. È una vulnerabilità molto pericolosa e va corretta, controllando i log per accertarsi che non ci siano manomissioni ed eventualmente reinstallando il sistema. Un'altra vulnerabilità critica da correggere è Debian OpenSSH/OpenSSL Package Random Number Generator Weakness, collegata a Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check). Queste due problematiche non rendono sicuri i file protetti dalla crittografia, perché le chiavi crittografiche, specialmente quelle private, che sono state generate con SSH, SSL e OpenVPN potrebbero essere rintracciate e non garantiscono la sicurezza della comunicazione. Un attaccante potrebbe riuscire a trovare queste chiavi e a decifrare tutti i contenuti sensibili che dovrebbero essere protetti dalla crittografia, rendendo necessaria la generazione di nuove chiavi per garantire la riservatezza dei documenti. Un altro aspetto critico per la sicurezza è il fatto che gli share NFS sono accessibili ad un attaccante, il quale può accedere e modificare file aziendali e serve dunque assicurarsi che l'accesso ad utenti esterni sia limitato o non consentito. È ben nota anche l'importanza di usare delle password sicure e complesse, ma il server VNC ha impostato come password proprio la parola "password", il che rende estremamente facile il login da parte di un malintenzionato. Vi sono altre due vulnerabilità critiche da correggere, ovvero Apache Tomcat AJP Connector Request Injection e SSL Version 2 and 3 Protocol Detection. La prima si riferisce alla presenza di un connettore AJP vulnerabile, che consente ad un attaccante di collegarsi da remoto, accedere a file, inviare del codice malevolo e farlo eseguire. Per rimediare, è necessario aggiornare la

configurazione AJP e Tomcat. La seconda vulnerabilità, invece, riguarda un'importante falla nella sicurezza perché il server accetta connessioni criptate con i protocolli SSL 2.0 e 3.0 che non sono sicuri e non garantiscono la creazione di un canale di comunicazione che assicuri la riservatezza delle comunicazioni tra client e server. La soluzione è semplice, bisogna disabilitare l'utilizzo di SSL 2.0 e 3.0 ed utilizzare una versione del protocollo TLS pari a 1.2 o superiore. Queste vulnerabilità sono veramente pericolose e segnalate come critiche, perché permettono ad un attaccante di danneggiare facilmente l'azienda ottenendo file ed inviando del codice malevolo. Vi sono anche altri problemi da correggere, ma questi sono quelli che richiedono un'azione immediata e una copertura finanziaria adeguata per mettere in sicurezza l'azienda.