Esercitazione Nessus

Ho utilizzato Nessus per effettuare una scansione sulle porte più comuni della macchina Metasploitable2.

1. Prima vulnerabilità trovata: (porta 445)
   Samba Badlock Vulnerability. Questa vulnerabilità viene classificata di tipo alto e riguarda il software Samba installato sulla metasploitable. Questa vulnerabilità può portare ad attacchi man-in-the-middle, dove un utente non autorizzato può impersonare un utente legittimo ed eseguire operazioni arbitrarie con i privilegi di quell'utente. La soluzione a questo tipo di problema è l'aggiornamento ad una versione di Samba che contiene una patch per Badlock.

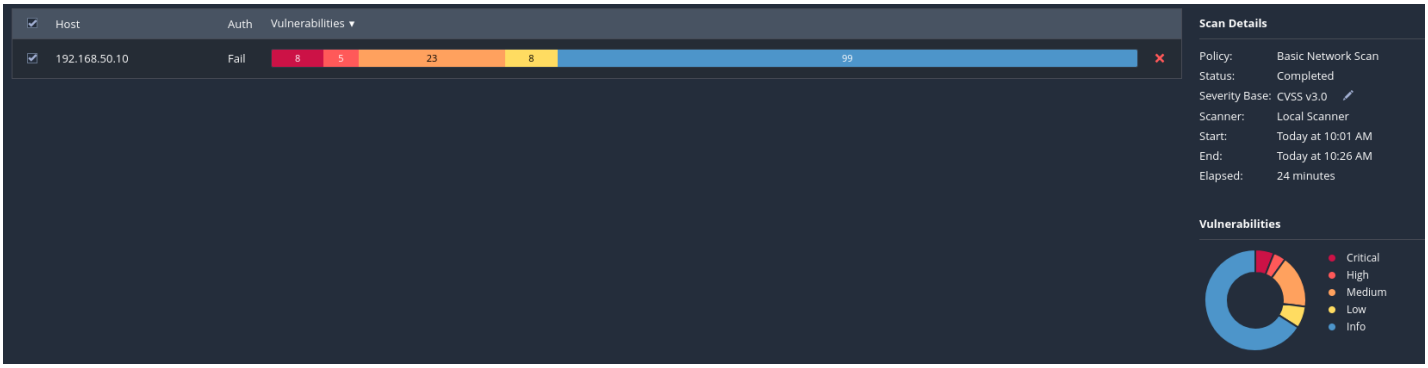
2. Seconda Vulnerabilità: (porta 22)
   Debian OpenSSH/OpenSSL Package Random Number Generator Weakness. Questa vulnerabilità è classificata di tipo critico. Si riferisce a una vulnerabilità che colpisce in particolare i sistemi Debian e Ubuntu che hanno uno specifico bug nella libreria OpenSSL che viene usata per generare le chiavi host SSH. Il problema risiede appunto al difetto del generatore casuale, il quale genera numeri che sembrano casuali ma sono in realtà prevedibili. Quindi un attaccante può facilmente entrare in possesso di questa chiave può impersonificare il server o decifrare le comunicazioni, può intercettare il traffico SSH crittografato e decrittografarlo. La soluzione è rigenerare tutte le chiavi SSH e aggiornare OpenSSL.

3. Terza vulnerabilità: (porta 80)
   Canonical Ubuntu Linux SEoL (8.04.x). Vulnerabilità di tipo critico. Questa si riferisce alla versione del sistema operativo che risulta essere non più aggiornata e quindi con molte lacune di sicurezza. La soluzione è aggiornare ad una versione più recente.

4. Quarta vulnerabilità: (porta 5900)
   VNC Server 'password' Password. Vulnerabilità di tipo critico. Questa vulnerabilità si riferisce ad un problema con il server VNC, responsabile del controllo remoto della macchina. Il problema riscontrato risiede in un problema con la forza della password la quale è impostata con 'password', quindi molto semplice da indovinare. La soluzione è rendere la password più forte

5. Quinta vulnerabilità: (porta 8009)
   Apache Tomcat A JP Connector Request Injection (Ghostcat). Vulnerabilità di tipo critico. Indica la presenza di un connettore AJP (Apache JServ Protocol) in ascolto sul server remoto e la sua vulnerabilità. Il problema risiede non nella presenza del connettore ma nella versione e configurazione di quest'ultimo. Un problema potrebbe essere che viene lasciato sulla porta di default, e sono esposti direttamente a internet mentre dovrebbero essere raggiungibili solamente dal server Apache http interno. Delle soluzioni potrebbero essere: aggiornare la versione di Apache Tomcat ad una versione stabile e ottimizzare la configurazione dell'AJP. Un'altra soluzione è quella di chiudere il servizio qualora non venga utilizzato.

Queste non sono le uniche vulnerabilità trovate, quindi per un maggiore controllo allego il file del report che nessus ha generato.


Host
Auth
Vulnerabilities ▾
192.168.50.10
Fail
8
5
23
8
99
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:01 AM
End: Today at 10:26 AM
Elapsed: 24 minutes
Vulnerabilities
Critical
High
Medium
Low
Info