Traccia

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, indicando come target solo le porte comuni.
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.
Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note.

Svolgimento

La scansione eseguita è di tipo "Basic Network Scan", porte selezionate "Common Ports".
Una volta eseguita la scansione, Nessus restituisce l'elenco di tutte le vulnerabilità trovate, con allegato anche una possibile soluzione ad ognuna.

Di seguito vedremo 3 delle vulnerabilità trovate.

Unix Operating System Unsupported Version Detection

Questa vulnerabilità è classificata come critica. Il sistema operativo installato sul target non è più supportato, quindi non riceve aggiornamenti sulla sicurezza.
Il consiglio è di aggiornarlo ad una versione supportata.

VNC Server 'password' Password

Questa vulnerabilità è classificata come critica. La password del servizio VNC (protocollo per il controllo remoto), è 'password'. Questa è una delle password più comuni, quindi facilmente individuabile con un attacco di tipo brute-force.
Il consiglio è di cambiare la password con una più sicura.

Samba Badlock Vulnerability

Questa vulnerabilità è classificata come alta. La versione di Samba (protocollo per la condivisione in rete di file system) installata sul target, è affetta dalla falla chiamata Badlock. Essa permette ad un attaccante, che intercetta il traffico di rete tra un client ed un server Samba, di effettuare delle richieste fingendo di essere il client stesso, potendo quindi vedere o modificare dei file.
Il consiglio è di aggiornare aggiornare la versione del protocollo.