Cos’è e come funziona Nessus

Nmap è uno **scanner di vulnerabilità**, in grado anche di testare le vulnerabilità.

Se nmap viene utilizzato per ottenere dei dati oggettivi sulla rete, nessus (così come tutti gli scanner di vulnerabilità) ci dà dei **dati soggettivi**.

Per dati soggettivi si intendono delle informazioni che dipendono dal caso specifico. Ad esempio, ci dà una **valutazione del rischio** che va da 1 a 10.

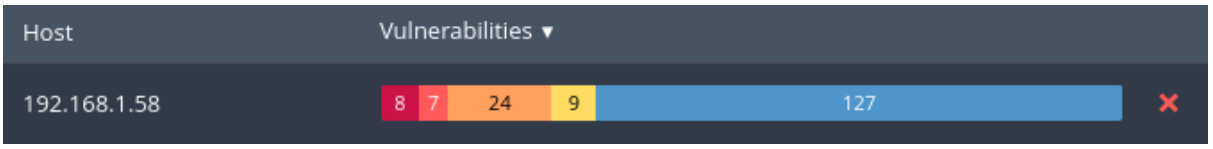
Non solo: ci darà anche un **consiglio** su come risolvere le vulnerabilità. Il consiglio è basato su una tabella (un database).

Bisogna fare attenzione però, perché il database potrebbe non essere aggiornato, oppure potrebbe essere corrotto.

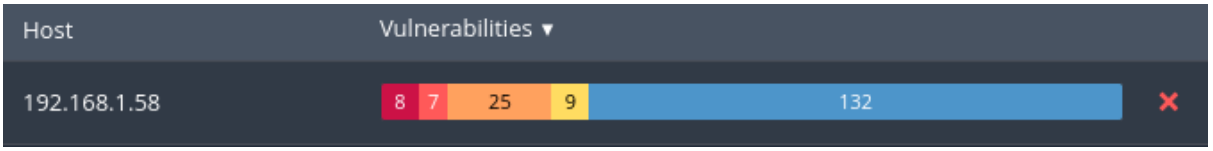
Esercizio

Nell’esercizio di oggi andiamo a scansionare le vulnerabilità di **Metasploitable**.

Target: Metasploitable
Porte: Solo le porte comuni
Scansione base:



Scansione avanzata:



Scansione delle vulnerabilità di Metasploitable

Sev ▾	CVSS	VPR	EPSS	Family	Count
CRITICAL	10.0 *			Gain a shell remotely	1
CRITICAL	9.8	9.0	0.9728	Web Servers	1
CRITICAL	9.8			Service detection	2
CRITICAL	9.8			Backdoors	1
CRITICAL	...	...	...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	General	1
HIGH	7.5 *	5.9	0.015	Service detection	1
HIGH	7.5 *	5.9	0.015	Service detection	1
HIGH	7.5			RPC	1
MIXED	...	...	...	General	28
MIXED	...	...	...	DNS	5
MEDIUM	6.5			Service detection	2

Analisi delle vulnerabilità

Prendiamo in analisi le prime 5 vulnerabilità presenti in tabella, contrassegnate come critiche e con una valutazione del rischio massima (o quasi).

• Il server VNC* in esecuzione sull'host remoto è protetto con una password debole.

Nessus è riuscito a effettuare l'accesso utilizzando la password "password". Un attaccante remoto potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.

*Il server VNC offre un servizio di controllo remoto (simile a TeamViewer).

Soluzione:

Cambiare la password del server VNC con una password robusta.

• È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP*.

Un attaccante potrebbe sfruttarla per leggere file di applicazioni web da un server vulnerabile.

Nei casi in cui il server vulnerabile consenta il caricamento di file, un attaccante potrebbe caricare codice malevolo.

*AJP inoltra le richieste HTTP dal server web ad un server Tomcat (o simili), permettendo lo scambio di dati tra la parte statica della pagina web e la parte dinamica (come ad esempio app in javascript).

Soluzione:

Cambia i permessi nella configurazione dell'AJP in modo che solo chi è autorizzato possa accedervi.

• Il servizio remoto accetta connessioni criptate utilizzando SSL 2.0 e/o SSL 3.0.

Queste versioni di SSL presentano diverse vulnerabilità crittografiche.

Un attaccante può sfruttare queste vulnerabilità per condurre attacchi man-in-the-middle o decrittografare le comunicazioni tra il server e i client.

Soluzione:

Utilizza TLS anziché SSL. Disabilita SSL.

• Una shell è in ascolto su una porta remota senza richiedere alcuna autenticazione.

Un attaccante potrebbe usarla collegandosi alla porta remota ed eseguire comandi in modo diretto.

Soluzione:

Verifica se l'host remoto è stato compromesso e reinstalla il sistema se necessario.

• Il certificato x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu con un difetto nel generatore di numeri casuali della sua libreria OpenSSL.

Soluzione:

Il materiale crittografico generato sull'host remoto risulta indovinabile. Tutte le chiavi SSH, SSL e OpenVPN vanno rigenerate.