EPICODE

ESERCIZIO W12D1

VULNERABILTY ASSESSMENT

Mungiovì Fabio

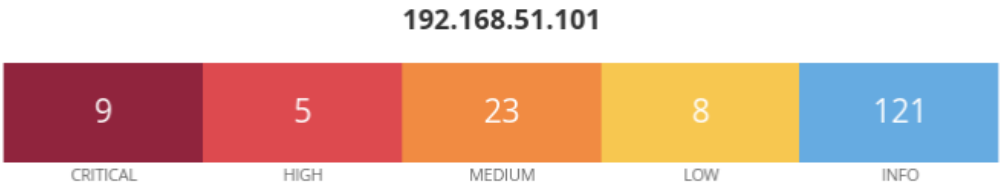
INDICE

1. Sommario

L'obbiettivo di questo Vulnerabilty Scan è analizzare e studiare le vulnerabiltà del sistema Metasploitable 2.
La scansione è stata efettuata tramite il tool Nessus.
Per ogni vulnerabiltà trovata sarà indicato anche le azioni da intraprendere per correggere e rimediare.

2. Risultati e impatto

I Risultati dello scan vengono suddivisi in baso al loro impatto e al tipo di richio a cui espongono.
Questi sono i risultati della scansione in oggetto.



Di seguito verranno analizzate nel dettaglio le vulnerabiltà CRITICAL e HIGH.

3. Analisi Vulnerabiltà

Vulnerabilità CRITICHE

Porta	Problema	Soluzione
8009 (AJP)	Esecuzione di codice remoto tramite Ghostcat	Aggiornare Tomcat e configurare l'AJP per richiedere l'autorizzazione
1524 (Backdoor)	Accesso a una shell remota senza autenticazione	Verificare la compromissione e reinstallare il sistema
- (Ubuntu 8.04)	Sistema operativo non supportato	Aggiornare a una versione supportata di Ubuntu
22, 25, 5432 (SSH/SSL)	Chiavi deboli a causa di un generatore di numeri casuali difettoso	Rigenerare tutte le chiavi crittografiche
25, 5432 (SSL)	Supporto per SSLv2 e SSLv3	Disabilitare SSLv2 e SSLv3, usare TLS 1.2 o superiore
5900 (VNC)	Password debole "password"	Impostare una password VNC forte
25 (SMTP)	Vulnerabilità DROWN	Disabilitare SSLv2 e usare cifrari più sicuri
445 (SMB)	Firma SMB non richiesta	Abilitare la firma SMB nel server
22 (SSH)	Algoritmi di crittografia deboli	Disabilitare algoritmi deboli come Arcfour

Vulnerabilità ALTE

Porta	Problema	Soluzione
80 (HTTP)	Metodi HTTP vulnerabili (TRACE/TRACK)	Disabilitare metodi HTTP non sicuri
139, 445 (SMB)	Supporto per SMBv1	Disabilitare SMBv1 e usare versioni più recenti
25, 5432 (SSL)	Cifrari SSL deboli	Aggiornare le configurazioni SSL per usare cifrari più sicuri
21 (FTP)	Banner disclosure, potenziale accesso non autorizzato	Limitare l'accesso FTP e aggiornare il software
23 (Telnet)	Comunicazione non cifrata	Disabilitare Telnet e usare SSH

4. Concluioni

Il rapporto evidenzia diverse vulnerabilità presenti sul sistema target, alcune delle quali molto gravi.

Sono presenti molte configurazioni insicure e utilizza software vecchio e non aggiornato.

Per risolvere questi problemi, è necessario aggiornare tutti i programmi, configurare correttamente i servizi e utilizzare password più sicure.

Questi interventi possono prevenire attacchi e proteggere il sistema.