# **Progetto W12D4**

## **Introduzione**

Questo report illustra le attività svolte nell’ambito di una scansione di sicurezza sul target Metasploitable, con particolare attenzione all’identificazione e al trattamento di vulnerabilità critiche. L’obiettivo principale consiste nell’individuare da due a quattro vulnerabilità di rilievo, applicare le relative azioni di rimedio e verificare l’efficacia degli interventi attraverso una nuova scansione e il confronto dei risultati ottenuti.

## **Obiettivi e metodologia**

Il lavoro si colloca nell’ambito del vulnerability assessment, una delle fasi centrali del Penetration Test, svolto in un ambiente simulato per riprodurre un’analisi di sicurezza.

La scansione è stata effettuata tramite il tool Nessus, installato su una macchina Kali Linux (192.168.50.100), indirizzando l’analisi verso Metasploitable2 (192.168.50.101), un sistema volutamente vulnerabile e utilizzato a scopo didattico.

## **Fasi operative**

* Identificazione delle vulnerabilità: La prima attività ha riguardato la scansione automatizzata tramite Nessus, seguita da una verifica manuale per escludere eventuali “falsi positivi”.
* Analisi dei risultati: In questa fase sono stati esaminati gli esiti della scansione e le raccomandazioni suggerite per la risoluzione delle criticità rilevate.
* Applicazione delle misure correttive: Sono state implementate le azioni di rimedio sulle vulnerabilità confermate.
* Verifica dell’efficacia: Infine, è stata rieseguita la scansione sul target per accertare che le misure adottate abbiano effettivamente risolto i problemi individuati, confrontando i nuovi risultati con quelli precedenti.

**Identificazione delle vulnerabilità**

La scansione viene effettuata utilizzando il tool Nessus. In questa fase, si procede con la configurazione delle macchine sulla rete interna e si avvia la scansione mirata sul target Metasploitable, così da raccogliere dati sulle vulnerabilità presenti.

Immagine che contiene testo, schermata, software, Software multimediale

Il contenuto generato dall'IA potrebbe non essere corretto.

Figura 1

Come illustrato dalla figura 1, lo strumento Nessus restituisce un elenco dettagliato delle vulnerabilità individuate sul sistema Metasploitable.

***Analisi dei risultati:***

Immagine che contiene testo, schermata, software, Software multimediale

Il contenuto generato dall'IA potrebbe non essere corretto.

Figura 2

La schermata di riepilogo (Figura 2) generata da Nessus fornisce una panoramica chiara e dettagliata delle vulnerabilità rilevate durante la scansione. Questa vista consente di comprendere rapidamente la situazione di sicurezza del sistema target attraverso diversi elementi chiave.

*Elementi presenti nella schermata*

* È presente un elenco di vulnerabilità, per l’esattezza, ordinate secondo il livello di gravità, suddivise nelle categorie Critical, High, Medium, Low e Info. Questa classificazione aiuta a focalizzare l’attenzione sulle problematiche più urgenti e a pianificare in modo efficace le attività di remediation.
* Sono riportate informazioni dettagliate per ciascuna vulnerabilità, tra cui il nome, la gravità attribuita, il tipo di rischio, la famiglia di appartenenza e il numero di host coinvolti. Questi dettagli sono fondamentali per valutare l’impatto potenziale e per indirizzare le attività di mitigazione.
* La visualizzazione include un grafico a torta che rappresenta la distribuzione delle vulnerabilità in base al livello di rischio. Questo strumento grafico agevola una rapida comprensione della situazione complessiva.
* Sono inoltre disponibili filtri e opzioni per l’esportazione dei dati, utili sia per affinare l’analisi che per documentare in modo strutturato i risultati ottenuti durante la scansione.

### *Criteri di valutazione del punteggio delle vulnerabilità*

Il punteggio attribuito alle vulnerabilità si basa su tre gruppi di metriche, che permettono una valutazione completa e contestualizzata dei rischi:

1. **Base** : queste metriche considerano le caratteristiche intrinseche della vulnerabilità, come la facilità di sfruttamento e l’impatto su confidenzialità, integrità e disponibilità dei dati.
2. **Temporal** : riguardano fattori che possono variare nel tempo, ad esempio la disponibilità di exploit noti o la presenza di patch correttive.
3. **Environmental** : valutano l’impatto specifico che la vulnerabilità può avere nel contesto dell’organizzazione, consentendo di adattare la priorità degli interventi alle reali esigenze operative.
4. Canonical Ubuntu Linux SEoL (8.04.x) (10)
5. VNC Server 'password' Password (10)
6. Apache Tomcat AJP Connector Request Injection (Ghostcat) (9.8)
7. SSL Version 2 and 3 Protocol Detection (9.8)
8. Bind Shell Backdoor Detection (9.8)
9. 2 SSL (Multiple Issues)

***Applicazione delle misure correttive:***

***VNC Server 'password' Password***

***Gravità: Critica***

***ID: 61708***

Vulnerabilità VNC Server: Password Debole

È stato rilevato che un server VNC in esecuzione sull'host remoto utilizza una password molto debole per la protezione dell'accesso. Durante la scansione, Nessus è riuscito ad autenticarsi con il servizio VNC utilizzando la password predefinita 'password'. Questo evidenzia una grave carenza nella sicurezza, poiché un attaccante remoto, non autenticato, potrebbe facilmente sfruttare questa vulnerabilità per ottenere il controllo del sistema.

### Soluzione

Per mitigare il rischio, è necessario mettere in sicurezza il servizio VNC configurando una password robusta che non sia facilmente intuibile o vulnerabile ad attacchi di forza bruta.

Immagine che contiene testo, schermata, software, Icona del computer

Il contenuto generato dall'IA potrebbe non essere corretto.

***SSL v2/v3 Protocol Detection***

***Soluzione: disabilitare SSLv2/SSLv3 nel file di configurazione e riavviare il servizio***

Il servizio remoto utilizza protocolli SSL 2.0 e/o SSL 3.0, noti per vulnerabilità crittografiche come padding insicuro, rinegoziazione e ripresa delle sessioni deboli. Questi problemi espongono a rischi di attacchi man-in-the-middle e decriptazione delle comunicazioni. Molti browser gestiscono male il downgrade del protocollo, aggravando il rischio (es. attacco POODLE). È consigliato disattivare completamente questi protocolli, non più considerati sicuri dal NIST e PCI DSS.

***Immagine che contiene testo, schermata, software, Software multimediale

Il contenuto generato dall'IA potrebbe non essere corretto.***