Report vulnerabilità metasploitable

Sommario

Introduzione

- **Obiettivo del tes**t: L'obiettivo principale dell'attività è identificare le vulnerabilità presenti sulla macchina target tramite strumenti di scansione, e successivamente implementare azioni di rimedio, per mitigarne o eliminarne l'impatto.
- **Scopo:**
    - Dimostrare la capacità di rilevare e comprendere le vulnerabilità critiche attraverso strumenti di scansione adeguati.
    - Valutare l'efficacia delle azioni di rimedio adottate, mostrando come esse riducano o eliminino l'esposizione a rischi concreti.

Sintesi dei risultati

La scansione ha rivelato che la macchina Metasploitable presenta numerose vulnerabilità critiche, molte delle quali possono essere sfruttate per ottenere accesso non autorizzato o eseguire codice maligno. È fondamentale procedere con l'implementazione di misure di sicurezza adeguate, come l'aggiornamento dei servizi, la modifica delle credenziali di default e la configurazione di firewall, per mitigare questi rischi.

Target Metasploitable

Metasploitable è una macchina virtuale volontariamente vulnerabile, creata per essere un bersaglio da attaccare durante test di sicurezza informatica. Serve principalmente a praticare tecniche di hacking etico e penetration testing in un ambiente sicuro, senza rischiare danni reali.

Quick summary

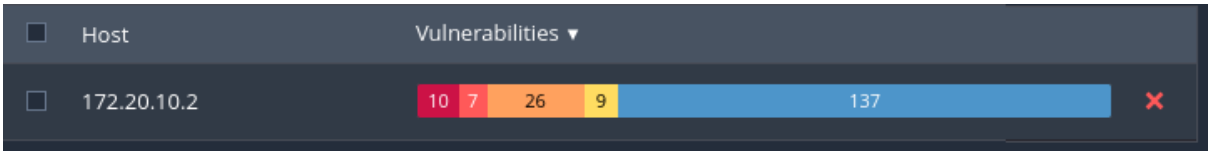
Lo stato generale del sistema target analizzato evidenzia la presenza di una superficie d'attacco piuttosto ampia, esposta a numerosi rischi di tipo Remote Code Execution, Default Credentials e Servizi Non Sicuri, tipici di ambienti di test volutamente vulnerabili.

L'analisi ha evidenziato come diversi servizi attivi presentino vulnerabilità note e sfruttabili con relativa facilità, alcune delle quali già documentate in exploit pubblici e ampiamente automatizzabili. In particolare, la presenza di backdoor, applicazioni web vulnerabili e accessi con credenziali deboli rappresenta una minaccia concreta in scenari reali.

Tra le criticità evidenziate, merita attenzione anche l'esposizione di porte e servizi sensibili non protetti da meccanismi di controllo d'accesso, oltre a configurazioni predefinite non modificate, che rappresentano un rischio soprattutto in caso di riutilizzo in contesti produttivi.

Possiamo dunque riassumere i risultati in:

- **Totale delle vulnerabilità identificate:**
  - **Critiche: 11**
  - **Alte: 7**
  - **Medie: 27**
  - **Basse: 9**
- **Stato complessivo della macchina: Critico.**



Dettaglio dei risultati:

Di seguito viene documentata ogni vulnerabilità critica trovata sulla macchina metasploitable, con una breve descrizione e potenziale impatto delle falle

Titolo	UnrealiRCd Backdoor detention	Gravita	Critica 10.0

Descrizione:
Il server IRC remoto è una versione di Unrealircd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato

Titolo	Canonical Ubuntu Linux SEol	Gravita	Critica 10.0

Descrizione:
Secondo la versione, Canonical Ubuntu Linux è la 8.04.x. Pertanto, non è più supportato dal suo fornitore o provider.
La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Titolo	VNC Server 'password' password	Gravità	Critica 10.0

Descrizione:
Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password". Un

aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.

Titolo	Debian OpenSSH/OpenSSL Package Random Number Generator weakness	Gravità	Critica 10.0

Descrizione:
Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Il problema è dovuto alla rimozione da parte di un pacchettizzatore Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.

Titolo	Apache Tomcat AJP Connector Request Injection	Gravità	Critica 9.8

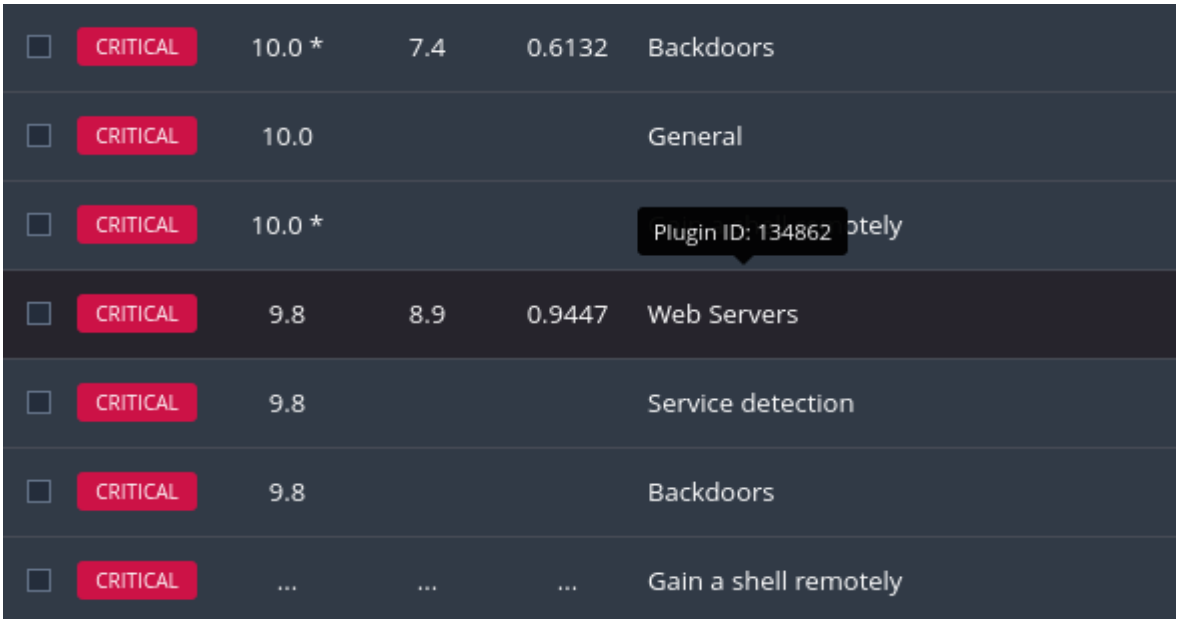
Descrizione:
È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un aggressore remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un aggressore potrebbe caricare codice JavaServer Pages (JSP) dannoso in diversi tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Titolo	Bind Shell Backdoor Detection	Gravità	Critica 9.8

Descrizione:
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un aggressore potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Titolo	SSL Version 2 and 3 Protocol Detection	Gravità	Critica 9.8

Descrizione:
Il servizio remoto crittografa il traffico utilizzando un protocollo con debolezze note.
Un aggressore può sfruttare queste falle per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio interessato e il client



Conclusione

L'attività di scansione e analisi condotta sulla macchina Metasploitable ha permesso di individuare diverse vulnerabilità critiche, molte delle quali largamente documentate e facilmente sfruttabili da attori malevoli. In particolare, la presenza di servizi non aggiornati, backdoor note, configurazioni insicure e credenziali deboli evidenzia un elevato livello di esposizione e rischio per il sistema analizzato.