W12D4

Scansione iniziale

Informazioni generali

- Progetto: VA sulla macchina Metasploitable 2
- Ip target: 192.168.51.100
- Data: 18/05
- Autore del report: Fabio Falato

Sommario

Introduzione

Obiettivo del VA è una scansione sulla macchina VM Metasploitable 2 per identificarne le vulnerabilità, che poi verranno parzialmente risolte nella seconda fase del report .

Metodologia di scansione e strumenti

La scansione è stata condotta dalla macchina IP 192.168.50.100/24 in comunicazione con l'ip target attraverso un firewall Pfsense

```
┌──(kali㉿kali)-[~/Downloads]
└─$ traceroute 192.168.51.100
traceroute to 192.168.51.100 (192.168.51.100), 30 hops max, 60 byte packets
 1  pfSense.home.arpa (192.168.50.1)  0.338 ms  0.291 ms  0.277 ms
 2  192.168.51.100 (192.168.51.100)  0.894 ms  0.882 ms  0.909 ms
```

Strumenti

La scansione è avvenuta usando principalmente la funzione **Basic Network Scan** di Nessus Essential versione 10.8.4

Sono stati inoltrate usati strumenti quali:

- Nmap per ulteriore scansione più mirata prima e dopo mitigation
- Netstat per verificare dalla macchina target, per monitorare quali servizi sono in ascolto
- Traceroute/ping per l'identificazione del target e quanti Hop è distante
- Netcat principalmente per la fase verifica della vulnerabilità

Minacce rilevate

Di seguito un elenco delle vulnerabilità rilevate, faccio presente che la lista sottostante è solamente un estratto di tutte le minacce rilevate

Titolo	**Canonical Ubuntu Linux SEoL (8.04.x)**
Descrizione	Secondo la versione indicata, Canonical Ubuntu Linux è la 8.04.x. Di conseguenza, non è più supportata dal fornitore. La mancanza di supporto implica che non verranno rilasciate nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.
Gravità	Critica

Titolo	**VNC Server 'password' Password**
Descrizione	Il server VNC è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password **'password'**.
Gravità	Critica

Titolo	**Default Password 'service' for 'service' Account**
Descrizione	L'account **'service'** sull'host remoto utilizza la password predefinita **'service'.**
Gravità	Critica

Titolo	**Default Password (user) for 'user' Account**
Descrizione	L'account **'user'** sull'host remoto ha la password **'user'**
Gravità	Critica

Titolo	**Bind Shell Backdoor Detection**
Descrizione	Una back shell è in ascolto su una porta remota senza richiedere alcuna autenticazione.
Gravità	Critica

Titolo	**Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
Descrizione	Il certificato x509 del server SSL remoto è stato generato su un sistema Debian o Ubuntu affetto da un bug nel generatore di numeri casuali di OpenSSL. Questo difetto, causato dalla riduzione delle fonti di entropia, permette a un attaccante di ottenere facilmente la chiave privata e sfruttarla per decifrare la sessione o condurre attacchi man-in-the-middle.
Gravità	Critica

Titolo	**vsftpd Smiley Face Backdoor**
Descrizione	La versione di **vsftpd** sull'host remoto contiene una backdoor che accedendo con un nome utente che include **:)**, si attiva una shell in ascolto sulla porta TCP **6200**, che resta attiva finché un client non si disconnette.
Gravità	Alta

Titolo	**Samba Badlock Vulnerability**
Descrizione	La versione di Samba sull'host remoto è vulnerabile alla falla Badlock, che consente a un attaccante di intercettare le comunicazioni e ottenere accesso non autorizzato a dati sensibili o servizi critici tramite un abbassamento del livello di autenticazione
Gravità	Alta

Titolo	**NFS Shares World Readable**
Descrizione	Il server NFS remoto condivide una o più risorse senza limitare l'accesso, permettendo potenzialmente a chiunque di connettersi.
Gravità	Alta

Titolo	**Samba 3.0.0 'SamrChangePassword' RCE**
Descrizione	La versione di Samba sull'host remoto presenta una vulnerabilità che permette l'esecuzione di codice da remoto, sfruttabile da un attaccante autenticato tramite input non validati in specifiche chiamate RPC, specialmente con l'opzione 'username map script' attivata.
Gravità	Media

Titolo	**Web Server Generic XSS**
Descrizione	Il server web remoto non filtra correttamente le richieste contenenti JavaScript maligno, permettendo a un attaccante di eseguire codice arbitrario nel browser degli utenti sfruttando questa vulnerabilità.
Gravità	Media

Titolo	**Browsable Web Directories**
Descrizione	Diversi plugin di Nessus hanno rilevato che sul server web sono presenti directory accessibili e navigabili pubblicamente.
Gravità	Media

Titolo	**Backup Files Disclosure**
Descrizione	Aggiungendo suffissi come .old, .bak, ~ ai nomi di alcuni file sull'host remoto, è possibile accedere ai loro contenuti, rischiando la divulgazione di informazioni sensibili.
Gravità	Media

Titolo	**Web Application Potentially Vulnerable to Clickjacking**
Descrizione	Il server web remoto non imposta gli header di risposta **X-Frame-Options** né **Content-Security-Policy (frame-ancestors)**, esponendo il sito a possibili attacchi di click jacking. Questi attacchi permettono a un malintenzionato di indurre un utente a cliccare su elementi diversi da quelli percepiti, causando operazioni fraudolente o dannose. Gli header X-Frame-Options e CSP sono attualmente le misure più affidabili per prevenire questo tipo di attacchi, anche se non le uniche.
Gravità	Media

Conclusioni Finali

La sicurezza della macchina è decisamente insufficiente sono presenti numerose vulnerabilità che compromettono la sicurezza del sistema stesso. Purtroppo, come riportato in cima alla lista delle vulnerabilità trovate, la versione obsoleta del sistema operativo non viene più da tempo aggiornata dal vendor, questo di per se compromette la sicurezza della macchina e la espone a numerose CVE. Infine si notano svariate password impostate secondo standard di sicurezza molto bassi in alcuni casi lasciando la password standard del servizio o addirittura esposta in chiaro.