M3-W12D1 - Pratica (Vulnerability Assessment)

DATA

Cybersecurity Analyst

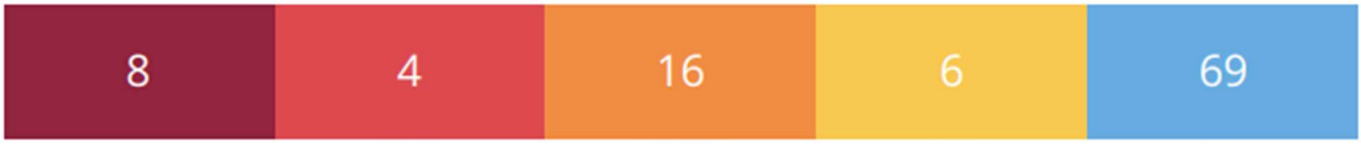
Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Traccia:

A partire dal report di ieri:
•Analisi/studio delle vulnerabilità (PDF) - servirà sia per exploit che remediation
•Report PDF per «dirigente»
• Inteso come riassunto che va presentato ai dirigenti per l'approvazione a livello finanziario ecc. Non contiene troppi dettagli tecnici ma soltanto l'indicazione della vulnerabilità e soprattutto i grafici con la pericolosità delle varie vulnerabilità riscontrate

Esecuzione:
Dopo l'analisi della macchina Metasploitable, qui sotto vengono esposte le principali criticità.

192.168.50.100



Vulnerabilities — Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Di queste criticità solo una è semplice da risolvere (51988), mentre le altre impiega del tempo per la soluzione non al quanto semplice.

Livello:	CVSS	Plugin	Note	Soluzione
Critico	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o esegui l'aggiornamento del server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.
Critico	9.8	51988	Bind Shell Backdoor Detection	Verifica se l'host remoto è stato compromesso e reinstalla il sistema se necessario
Critico	10	33850	Unix Operating System Unsupported Version Detection	Effettua l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.

Livello Alto, anche se non rientra tra la categoria critica è più sempre una vulnerabilità difficile da gestire, il tempo impiegato non è calcolabile.

Livello:	CVSS	Plugin	Note	Soluzione
Alto	8.6	136769	ISC BIND Service Downgrade / Reflected DoS	Esegui l'aggiornamento alla versione di ISC BIND indicata nell'avviso del produttore.

Livello Basso: In questo caso si disabilita la funzione, semplice.

Livello:	CVSS	Plugin	Note	Soluzione
Basso	3.7	70658	SSH Server CBC Mode Ciphers Enabled	Contatta il fornitore o consulta la documentazione del prodotto per disabilitare la crittografia a blocco (CBC mode) e abilitare la crittografia a contatore (CTR) o la crittografia di modalità di contatore di Galois (GCM).

Livello Info: Semplice da attuare, e non crea problemi di sicureza.

Livello:	CVSS	Plugin	Note	Soluzione
Info	N/D	10114	ICMP Timestamp Request Remote Date Disclosure	Filtra le richieste di timestamp ICMP (13) in uscita e le risposte ai timestamp ICMP (14).

Svolgimento per mettere in sicurezza:

Come si nota le più semplici che impiega poco tempo sono quella della fase 1, mentre le altre impiega più tempo e si passa alla fase 2.

Livello:	CVSS	Plugin	Note	Soluzione	Fase:
Critico	9.8	51988	Bind Shell Backdoor Detection	Verifica se l'host remoto è stato compromesso e reinstalla il sistema se necessario	1
Basso	3.7	70658	SSH Server CBC Mode Ciphers Enabled	Contatta il fornitore o consulta la documentazione del prodotto per disabilitare la crittografia a blocco (CBC mode) e abilitare la crittografia a contatore (CTR) o la crittografia di modalità di contatore di Galois (GCM).	1
Info	N/D	10114	ICMP Timestamp Request Remote Date Disclosure	Filtra le richieste di timestamp ICMP (13) in uscita e le risposte ai timestamp ICMP (14).	1
Critico	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Aggiorna la configurazione AJP per richiedere l'autorizzazione e/o esegui l'aggiornamento del server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.	2
Critico	10	33850	Unix Operating System Unsupported Version Detection	Effettua l'aggiornamento a una versione del sistema operativo Unix attualmente supportata.	2
Alto	8.6	136769	ISC BIND Service Downgrade / Reflected DoS	Esegui l'aggiornamento alla versione di ISC BIND indicata nell'avviso del produttore.	2

Cybersecurity Analyst 2023