ESERCITAZIONE W12D1 (2)

EPICODE

Esercizio
Traccia

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

192.168.1.15

Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
MEDIUM	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	7.5	-	42256	NFS Shares World Readable
MEDIUM	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	-	136808	ISC BIND Denial of Service

Report per il Dirigente - Analisi delle Vulnerabilità

Siamo lieti di presentarle il report relativo all'analisi delle vulnerabilità rilevate sul nostro sistema. Questo riassunto fornisce una panoramica delle vulnerabilità critiche che richiedono attenzione immediata, insieme a una rappresentazione grafica della pericolosità delle stesse.

Vulnerabilità Critiche:

1. Esposizione del Server Web: Sono state individuate vulnerabilità nel server web che potrebbero permettere a un attaccante di ottenere accesso non autorizzato ai dati sensibili.

2. Debolezza delle Password: Le password utilizzate nel sistema sono troppo deboli, rendendo il sistema suscettibile ad attacchi di forza bruta.

3. Vulnerabilità del Server DNS: Il server DNS presenta vulnerabilità che potrebbero essere sfruttate per attacchi di tipo Denial of Service (DoS).

Il grafico evidenzia la distribuzione delle vulnerabilità rilevate in base alla loro gravità. Come si può notare, le vulnerabilità critiche rappresentano una percentuale significativa del totale, richiedendo azioni immediate per mitigare i rischi.

Azioni Consigliate:

- Implementare patch di sicurezza per le vulnerabilità rilevate.

- Migliorare le politiche di gestione delle password, incoraggiando l'uso di password robuste.

- Configurare correttamente il server DNS per mitigare le vulnerabilità.

Restiamo a disposizione per ulteriori chiarimenti o per discutere delle azioni necessarie per garantire la sicurezza del nostro sistema.

Cordiali Saluti.