Analisi delle vulnerabilità

Richiede un aggiornamento di apache

CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

Questo messaggio sta a significare che il materiale non è in sicurezza (criptografia).

CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

In Questo caso lo scan ci dice che la versione di sistema non è aggiornata. La soluzione sarebbe Aggiornare periodicamente la versione.

CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection

Il programma ci mette in chiaro la password, la soluzione sarebbe quella di utilizzare una password più efficace.

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

In questo caso manca il certificato SSL. La soluzione sarebbe quello di acquistarlo e impostarlo.

MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

Qui ci dice che i file di backup non sono sicuri e potrebbero essere stati compromessi, la soluzione ideale sarebbe quella di proteggerli con le massime protezioni disponibili con una password efficace.

MEDIUM	5.0*	-	11411	Backup Files Disclosure