Gabriele Di giampietro **Data 25/11/2022**

Obbiettivo: Effettuare una VA sulla macchina virtuale Metasploitable, analizzare e attuare delle remediation action su un minimo di 2 ad un massimo di 4 vulnerabilità trovate di livello Critical.

VA Scan finale

Dopo aver effettuato le rimediation action, le vulnerabilità trovate e analizzate come richiesto nella scansione iniziale sono state risolte. Otteniamo infatti una scansione finale ridimensionata che come possiamo vedere dal report di nessus le vulnerabilità sono diminuite e soprattutto non ci sono più quelle richieste da risolvere (11356 - NFS Exported Share Information Disclosure; 61708 - VNC Server 'password' Password; 51988 – Bind Shell Backdoor Detection).

Metasploitable

Report generated by Nessus™ 25/11/2022

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	3	17	5	71

Scan Information

Start time: Nov 25 14:00 2022

End time: Nov 25 14:30 2022

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:D9:D6:ED

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

Total: 101

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
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)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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