M3 D7

ES 1

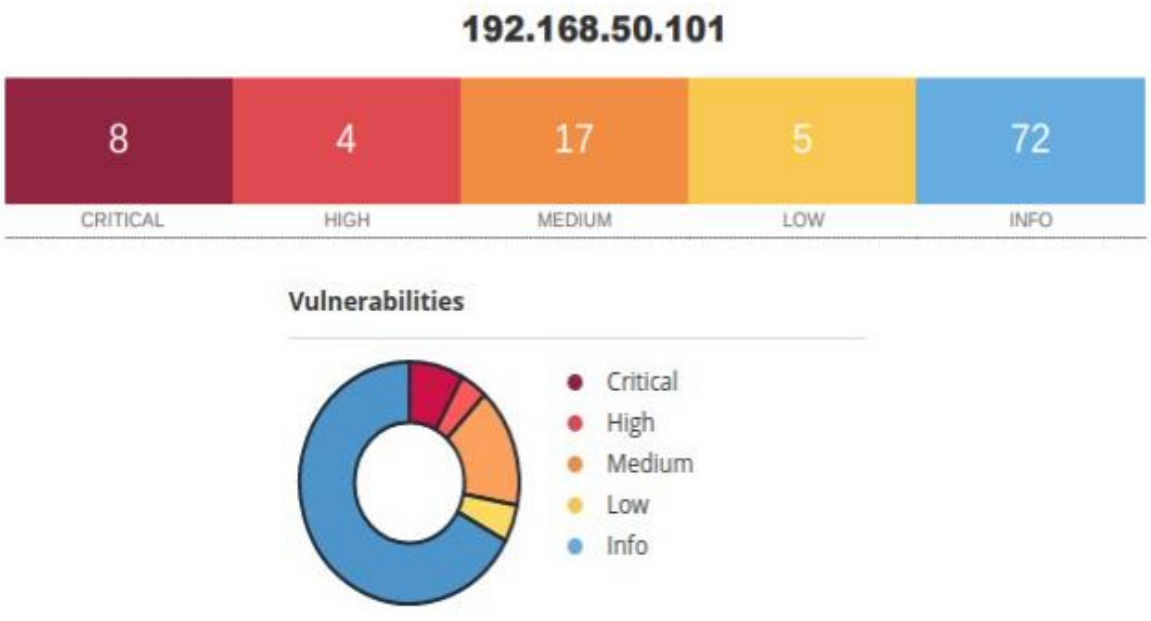
GIORNO 2 – VULNEARBILITY ASSESSMENT

Si tratta di un REPORT TECNICO sulle vulnerabilità della macchina Metasploitable.

Il report tecnico è un report quasi completo che evidenzia sia le porte (aperte) sia le vulnerabilità, assegnando loro una criticità: dal rosso scuro (gravi) all' azzurro (innocue).

Sono presenti anche le risoluzioni e remediation actions consigliate (come intervenire e risolvere il problema della vulnerabilità) o al più rendere il sistema meno debole e più difficilmente attaccabile da malintenzionati.

La scansione Nessus è fatta partire dal comando da terminale su Kali (avvio programma) e su https://kali:8834 per analizzare l' indirizzo IP di Metasploitable.



Analizziamo le più gravi (rosso scuro) fino ad arrivare a semplicemente elencare le meno pericolose (gialle e azzurre).

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

La 134862 indica un connettore AJP vulnerabile in ascolto sull'host remoto. Potrebbe essere sfruttata sia per leggere i file dell'applicazione web che per caricare codice remoto dannoso. Si propone l'aggiornamento della configurazione AJP e del server Tomcat.

La 51988 indica la presenza di una backdoor nel sistema in ascolto su porta remota.
Si consiglia il controllo del sistema per identificare eventuali compromissioni e, se necessario, reinstallarlo.

La 20007 indica che il servizio di criptazione del traffico presenta delle debolezze. Il servizio utilizza crittografia SSL 2.0 conosciuta per essere affetta da svariati difetti. Si consiglia di abbandonare tale servizio per passare al più sicuro TSL.

La 33850 indica che il sistema operativo in uso non è più supportato.
Si consiglia l'aggiornamento ad una versione Unix aggiornata.

La 32321 indica che il certificato remoto SSL utilizza una chiave di cifratura debole, sarebbe perciò possibile decifrare la sessione remota. Si vada quindi a considerare tutto il materiale crittografato come non affidabile e si rigenerino le chiavi.

La 11356 indica che è possibile accedere da remoto alle directory NFS del server dando la possibilità ad un eventuale attaccante di leggere e scrivere sull'host remoto. Si vada a configurare il tutto in modo che solo gli host autorizzati possano effetturare tali operazioni.

La 61708 indica che la password di un servizio VNC è debole, quindi facilmente sfruttabile. Generare una nuova password solida per risolvere il problema.

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

La 136769 indica che il server è esposto a vulnerabilità DoS e quindi a rischio di degrado servizi. Si vada ad aggiornare la ISC BIND all'ultima versione disponibile.

La 42256 indica che il server remoto esporta cartelle visibili a tutti. Si vada dunque ad impostare una restrizione adeguata.

La 42873 indica che il servizio remoto supporta una crittografia SSL vulnerabile, mettendo il sistema a rischio di un attacco di tipo "man in the middle". Si consiglia di riconfigurare il servizio di crittografia.

La 90509 indica un server SMB interessato da vulnerabilità "badlock". Anche in questo caso, il sistema è a rischio di un attacco di tipo "man in the middle". Imperativo aggiornare la versione SMB all'ultima versione disponibile.

MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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
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	5.9	5.1	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported

Le vulnerabilità 26928, 31705 e 81606 indicano un servizio di crittografia SSL debole. Si consiglia di riconfigurare tali servizi.

136808 e 139915 indicano che il server è esposto a vulnerabilità DoS e quindi a rischio di degrado servizi. Si vada ad aggiornare la ISC BIND all'ultima versione disponibile.

15901, 45411, 51192 e 57582 indicano una serie di falle nei certificati dei servizi SSL. Problemi quali la scadenza, certificazioni autofirmate, date errate e firme non valide. Si vada a generare un nuovo certificato SSL per sostituire quello attuale.

La vulnerabilità 65821 indica il supporto della cifratura RC4, un cifrario noto per la sua imperfezione. Si vada a riconfigurare l'applicazione interessata e si utilizzi una cifratura TLS.

78479 e 89058 ci indicano che è possibile ottenere informazioni dall'host remoto, una debolezza ben nota del protocollo SSLv3. Si consiglia di disabilitare il protocollo.

La vulnerabilità 104743 indica che il servizio remoto crittografa il traffico utilizzando una versione obsoleta di TLS. L'aggiornamento è in questo caso essenziale in quanto non è più garantito il corretto funzionamento degli endpoint.

La vulnerabilità 12085 indica che il server web remoto contiene file predefiniti. Questi file andrebbero rimossi per evitare l'accesso alle informazioni di installazione. Si consiglia di rimuoverli.

La vulnerabilità 42263 indica che il server Telnet trasmette traffico in chiaro. Disabilitare il servizio e passare a SSH.

La vulnerabilità 57608 indica che il server remoto SMB non richiede la firma. Si consiglia di imporre la richiesta di firma dei messaggi nella configurazione dell'host.

MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection

INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Queste ultime non destano grande preoccupazione.