ESERCIZIO S5L4

Traccia: Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web. Gli obiettivi dell'esercizio sono:
● Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
● Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

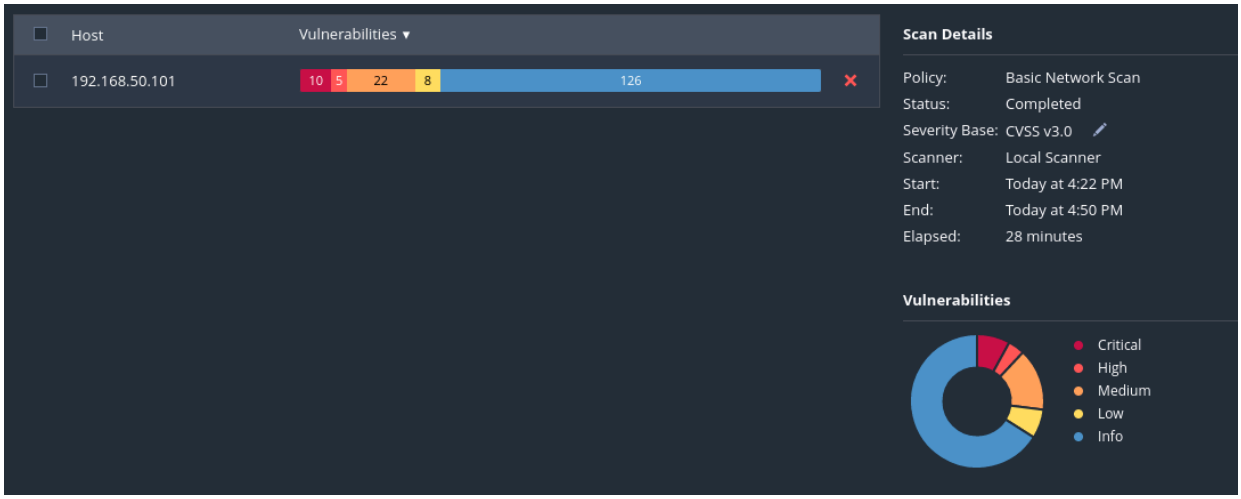
SVOLGIMENTO

Per poter utilizzare Nessus, da Kali si è dato il comando:

>*systemctl start nessusd.service*

con il quale si è avviato il servizio Nessusd. Il servizio sarà in ascolto sulla porta 8834 sul localhost. Successivamente si è effettuato l'accesso in Nessus con le credenziali per iniziare la configurazione dello scanner.
Come tipologia di scansione si è scelta la "Basic Network Scan", usando come target la macchina virtuale Metasploitable2.

A seguito della scansiona effettuata su Metasploitable, il programma di vulnerability scanner Nessus ha prodotto un report sulle vulnerabilità trovate. Il report completo è riportato in fondo alla pagina. L'immagine sottostante mostra la fine della scansione e un grafico dei risultati trovati.



Le vulnerabilità nel report sono divise per livelli di criticità. Di seguito descriviamo solo quelle più critiche.

VULNERABILITÀ: 134862 - Apache Tomcat A JP Connector Request Injection (Ghostcat)

Descrizione
È stata riscontrata una vulnerabilità nella lettura/inclusione di file in AJP connector. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione
Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versione successiva.

VULNERABILITÀ: 51988 - Bind Shell Backdoor Detection

Sinossi
L'host remoto potrebbe essere stato compromesso.

Descrizione
Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione
Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

VULNERABILITÀ: 20007 - SSL Version 2 and 3 Protocol Detection

Sinossi
Il servizio remoto cripta il traffico utilizzando un protocollo con debolezze note.

Descrizione
Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diverse falle crittografiche, tra cui:
- Uno schema di imbottitura insicuro con i cifrari CBC.
- Schemi di rinegoziazione e ripresa della sessione non sicuri.
Un aggressore può sfruttare queste falle per condurre attacchi man-in-the-middle o per decriptare le comunicazioni tra il servizio interessato e i client.
Sebbene SSL/TLS disponga di un metodo sicuro per scegliere la versione più alta del protocollo supportata (in modo che queste versioni vengano utilizzate solo se il client o il server non

supportano nulla di meglio), molti browser Web lo implementano in modo non sicuro, consentendo a un aggressore di declassare una connessione (come nel caso di POODLE). Pertanto, si raccomanda di disabilitare completamente questi protocolli.
Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. A partire dalla data di applicazione prevista da PCI DSS v3.1, qualsiasi versione di SSL non soddisfa la definizione di “crittografia forte” del PCI SSC.

Soluzione
Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.
Utilizzare invece TLS 1.2 (con suite di cifratura approvate) o superiore.

VULNERABILITÀ: 33850 - Unix Operating System Unsupported Version Detection

Sinossi
Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione
Secondo il numero di versione dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.
La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione
Aggiornare a una versione del sistema operativo Unix attualmente supportata.

VULNERABILITÀ: 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Sinossi
Le chiavi dell'host SSH remoto sono deboli.

Descrizione
La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un aggressore può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione
Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN deve essere rigenerato.

VULNERABILITÀ: 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness(SSL check)

Sinossi
Il certificato SSL remoto utilizza una chiave debole.

Descrizione
Il certificato x509 del server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della libreria OpenSSL.
Il problema è dovuto alla rimozione da parte di un packager Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o impostare un attacco man in the middle.

Soluzione
Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN deve essere rigenerato.

VULNERABILITÀ: 11356 - NFS Exported Share Information Disclosure

Sinossi
È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione
Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione
Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

VULNERABILITÀ: 61708 - VNC Server ‘password’ Password

Sinossi
Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

Descrizione
Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password “password”. Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Soluzione
Proteggere il servizio VNC con una password forte.

Di seguito è mostrato il report ottenuto da Nessus.

192.168.50.101

8	4	16	7	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 106

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	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*	-	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*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	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	5.9	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	31705	SSL Anonymous Cipher Suites Supported

MEDIUM	5.9	-	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	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
MEDIUM	4.0*	-	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	-	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	-	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	-	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	-	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)

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	-	35371	DNS Server hostname.bind Map Hostname Disclosure
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
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection

INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version

INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	11819	TFTP Daemon Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	19288	VNC Server Security Type Detection
INFO	N/A	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown