CS0424IT — ESERCITAZIONE S5L4
NESSUS VULNERABILITY ASSESSMENT

Simone La Porta

GitHub

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

Avvio di Nessus

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

```
systemctl start nessusd.service
```

Questo comando avvia il servizio Nessusd, che 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.

Scansione

Come tipologia di scansione si è scelta la "Basic Network Scan", usando come target la macchina virtuale Metasploitable2. A seguito della scansione, il programma di vulnerability scanner Nessus ha prodotto un report sulle vulnerabilità trovate.

ANALISI DELLE VULNERABILITÀ

Le vulnerabilità nel report sono divise per livelli di criticità. Di seguito una tabella che riassume quelle più critiche:

ID Vulnerabilità	Sinossi	Soluzione
134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	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.
51988	Bind Shell Backdoor Detection	Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.
20007	SSL Version 2 and 3 Protocol Detection	Disabilitare SSL 2.0 e 3.0. Utilizzare TLS 1.2 o superiore con suite di cifratura approvate.
33850	Unix Operating System Unsupported Version Detection	Aggiornare a una versione del sistema operativo Unix attualmente supportata.
32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. Rigenerare tutte le chiavi SSH, SSL e OpenVPN.

Continua nella pagina successiva

Tabella 1 – continua dalla pagina precedente

ID Vulnerabilità	Sinossi	Soluzione
32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. Rigenerare tutte le chiavi SSH, SSL e OpenVPN.
11356	NFS Exported Share Information Disclosure	Configurare NFS in modo che solo gli host autorizzati possano montare le sue condivisioni remote.
61708	VNC Server 'password' Password	Proteggere il servizio VNC con una password forte.

DESCRIZIONE DETTAGLIATA DELLE SOLUZIONI

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Soluzione: Per risolvere questa vulnerabilità, è necessario aggiornare la configurazione AJP per richiedere l'autorizzazione. Inoltre, aggiornare il server Tomcat alle versioni 7.0.100, 8.5.51, 9.0.31 o versioni successive per assicurarsi che le patch di sicurezza siano applicate.

Bind Shell Backdoor Detection

Soluzione: In caso di compromissione dell'host remoto, è essenziale verificare l'integrità del sistema. Se viene confermato un accesso non autorizzato, si consiglia di reinstallare completamente il sistema operativo per rimuovere eventuali backdoor installate.

SSL Version 2 and 3 Protocol Detection

Soluzione: SSL 2.0 e 3.0 sono protocolli obsoleti con note debolezze crittografiche. La soluzione consiste nel disabilitare questi protocolli e configurare i servizi per utilizzare TLS 1.2 o versioni superiori. Assicurarsi che le suite di cifratura utilizzate siano approvate e sicure.

Unix Operating System Unsupported Version Detection

Soluzione: Utilizzare versioni del sistema operativo Unix che siano ancora supportate dal fornitore. Questo garantisce che vengano ricevute tutte le patch di sicurezza e aggiornamenti necessari per mantenere il sistema sicuro.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Soluzione: Tutto il materiale crittografico generato su sistemi affetti da questa debolezza deve essere considerato compromesso. Rigenerare tutte le chiavi SSH, SSL e OpenVPN utilizzando una versione aggiornata della libreria OpenSSL.

NFS Exported Share Information Disclosure

Soluzione: Configurare le condivisioni NFS in modo che solo gli host autorizzati possano montarle. Questo può essere fatto modificando il file `/etc/exports` e restringendo l'accesso alle condivisioni solo agli indirizzi IP specificati.

VNC Server 'password' Password

Soluzione: Cambiare la password di accesso al server VNC con una più complessa e sicura. Evitare l'utilizzo di password comuni o facilmente indovinabili.