Mattia Chiriatti

Esercizio S5/L4

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.*

Analisi di alcuni errori critici nella Basic Network Analysis con Nessus

Errore Critico – Bind Shell Backdoor Detection

CVSS SCORE: 9.8

Questo potrebbe essere un problema molto serio per un qualsiasi computer collegato a una qualsiasi rete: l'errore evidenzia come ci sia una shell attiva e in ascolto su una porta remota senza alcuna autenticazione. Da questa porta, un possibile attaccante potrebbe penetrare facilmente nel sistema e inviare comandi diretti al sistema e al computer target.

Soluzione al problema

Anzitutto, bisogna verificare che l'host remoto non sia effettivamente compromesso. In caso l'host sia compromesso, bisognerà formattare il device e reinstallare il sistema nella sua interezza.

Errore Critico – SSL Version 2 and 3 Protocol Detection

CVSS SCORE: 9.8

L'errore riguarda più che altro la crittazione delle connessioni e il protocollo SSL. Il protocollo SSL è il protocollo che si occupa della comunicazione cryptata fra due host, con l'utilizzo di una chiave cryptata proprio per garantire la massima riservatezza delle comunicazioni. Nessus evidenzia come Metasploitable accetti connessioni crittate usando SSL 2.0 e SSL 3.0, che sono però influenzati da diversi flussi crittografici che possono diventare soggetto di attacchi man-in-the-middle o addirittura possono essere decrittate facilmente dal criminale informatico di turno.

Nonostante, però, siano dei protocolli di sicurezza e crittografia, lo stesso Nessus evidenzia come molti browser li ritengano ormai insicuri e superati a livello di sicurezza, in quanto permetterebbero a un possibile attaccante di effettuare facilmente un downgrade della connessione in essere. In più, tutte le versioni di SSL non rispettano più i requisiti di sicurezza stabiliti dal PCI SSC, il Payment Card Industry Security Standards Council.

Soluzione al problema

Disabilitare il protocollo SSL è un ottimo modo per risolvere l'errore, oppure un protocollo di livello di sicurezza più alto come il TLS 1.2 o più moderno.

Errore Critico – NFS Exported Share Information Disclosure

CVSS SCORE: 10

Questo errore critico fa riferimento al Network File System e ai file esportati dal server remoto da parte dell'host preso in esame con il network scan. Con il termine Disclosure, infatti, si intende che le informazioni non risultano protette; quindi un possibile attaccante potrebbe far leva su questo errore per modificare a proprio piacimento dei file presenti nell'host remoto.

Soluzione al problema

Configurare il NFS sull'host remoto in modo tale da consentire solo agli host autorizzati di poter utilizzare i dati condivisi.