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.

Produrre infine un report su 2 vulnerabilità critiche e 1 vulnerabilità media.

NFS Exported Share Information Disclosure -CRITIC-

Network file system (NFS) è un protocollo utilizzato solitamente per condividere files o directory da un sistema Linux/Unix su una rete.

La vulnerabilità NFS exported share information disclosure si ha quando le informazioni sulle condivisioni effettuate possono essere intercettate da host non autorizzati e potrebbero potenzialmente far leggere o scrivere file sul server remoto.

La soluzione per mitigare questo tipo di vulnerabilità è quella di installare la versione più recente di NFS (come ad esempio NFSv4) che garantiscano una sicurezza maggiore e implementare un firewall con delle regole che permettano l'accesso al server nfs solo ad ip attendibili.

SSL Version 2 and 3 Protocol Detection -CRITIC-

Il protocollo SSL è un protocollo crittografato utilizzato per scambiarsi informazioni in maniera sicura su una rete.

La vulnerabilità SSL Version 2 and 3 Protocol Detection sta ad indicare che nella scansione sono risultati in utilizzo dei protocolli ormai obsoleti a cause di alcune falle presenti in essi, come ad esempio schemi di rinegoziazione e ripresa delle sessioni non sicuri. Queste vulnerabilità potrebbero esser sfruttate da hacker per configurare un attacco Man in the Middle o un attacco Poodle.

La soluzione per risolvere questo tipo di vulnerabilità è quella di utilizzare il protocollo TLS (transport layer security) sempre nella sua versione più recente, ove possibile, al posto del protocollo SSL.

Unencrypted Telnet Server -MEDIUM-

Il protocollo telnet permette di trasferire informazioni tra host ma non crittografati.

La vulnerabilità Unencrypted Telnet Server ci avvisa che sul dispositivo analizzato si sta utilizzando il protocollo telnet server su un canale non crittografato. Questo rende le informazioni scambiate su di esso (esempio: logins, password, dati sensibili, etc.) facilmente intercettabili da un eventuale attacco hacker che potrebbe poi utilizzarle per scopi illegali.

La soluzione è quella di utilizzare al posto del protocollo telnet il protocollo SSH, in quanto quest'ultimo crea un canale crittografato su cui scambiare i vari pacchetti.