Obiettivo:

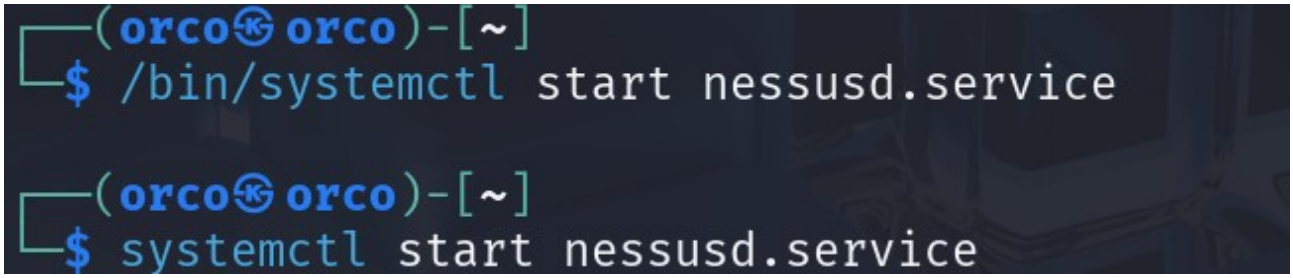
Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Analisi delle Vulnerabilità di Metasploitable

In questo esercizio testeremo le vulnerabilità della macchina Metasploitable con indirizzo IP 192.168.60.40. Come da istruzioni, ho utilizzato Nessus come vulnerability scanner e di seguito illustrerò le impostazioni adottate per la scansione.

Iniziamo

Avviamo il servizio tramite il comando mutuamente intercambiabile di seguito



Entrambi i comandi servono ad avviare il servizio Nessus che utilizzeremo per la scansione

L'attivazione di questo servizio è un prerequisito fondamentale per poter procedere con l'analisi.

Accesso all'Interfaccia Web di Nessus

Successivamente all'esecuzione del comando sopra citato, il servizio avvierà un web server sulla porta 8834. A questo punto dobbiamo accedere al server web tramite un qualunque browser con l'indirizzo "https://[NOME UTENTE]:8834/".

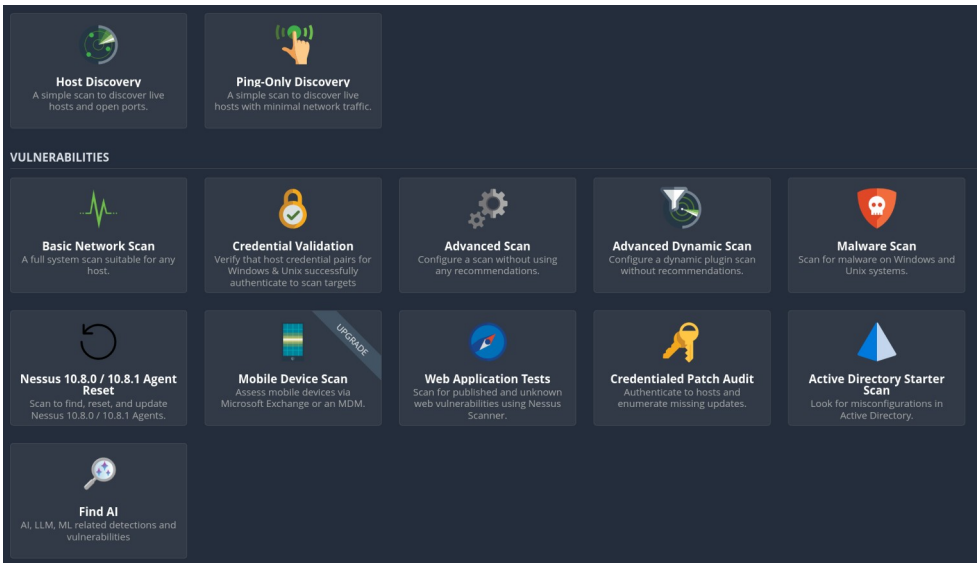
Sarà necessario autenticarsi con le proprie credenziali per accedere alla home del web server di Nessus. Una volta effettuato l'accesso, occorrerà cliccare sul pulsante "New Scan" per iniziare la configurazione di una nuova scansione

Comparirà una selezione di scansioni possibili, alcune gratuite e altre a pagamento. In questo esercizio ci concentreremo su due tipologie principali

"Basic Network Scan"

e

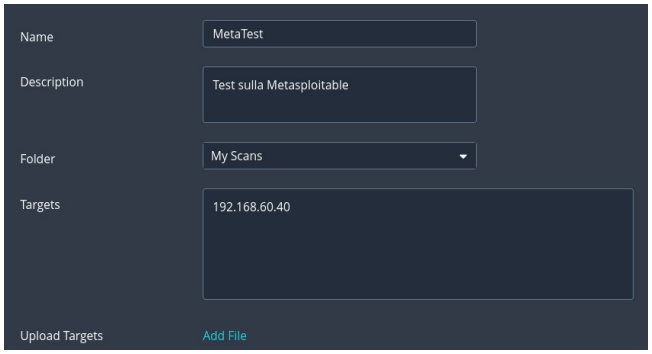
"Advanced Scan"



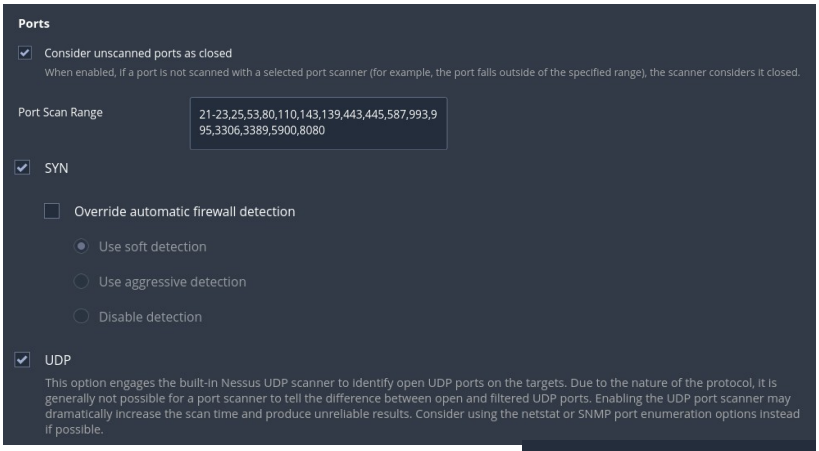
Configurazione della Basic Network Scan

Per cominciare, selezioniamo "Basic Network Scan". Verremo reindirizzati nella pagina di configurazione della scansione, dove dovremo indicare:

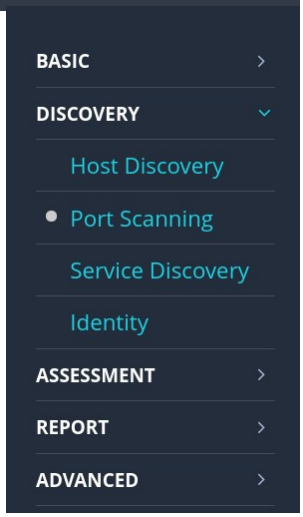
1. Il nome della scansione
2. Una descrizione (opzionale)
3. Il target della scansione



dopo aver indicato le informazioni essenziali



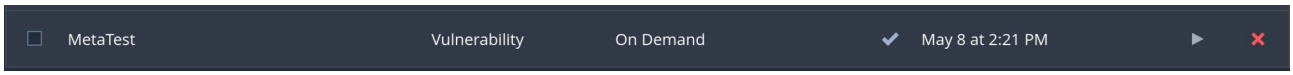
Clicchiamo su "Discovery/Port Scanning" per poter specificare, come da consegna, le porte da scansionare e abilitare la scansione dei protocolli sia TCP SYN che UDP.



Questa sezione è fondamentale per definire l'ampiezza della scansione, permettendoci di identificare quali servizi sono in ascolto sul sistema target

alla fine della configurazione clicco su salva (in basso a sinistra)

Tornando alla schermata principale, ora comparirà



Cliccando sul pulsante "play" potremo avviare la procedura di scansione. ^^

Al termine del processo, dopo qualche minuto, potremo esportare i risultati della scansione appena effettuata. Questa esportazione ci permetterà di conservare un report dettagliato che potrà essere utilizzato successivamente per risolvere i problemi identificati o per sfruttare le vulnerabilità rilevate, a seconda dello scopo della scansione.

A questi livelli, la configurazione della scansione avanzata è praticamente indifferente dalla scansione base in termini di setup. Tuttavia, al costo di tempo supplementare, fornirà informazioni più dettagliate e approfondite sulle vulnerabilità identificate.

Riferimenti ai file MetaTest_BS e MetaTest_AS nella cartella m2s5L3