Attacchi low,medium,high

Obbiettivo chiesto:

Un obiettivo richiesto dal CISO era di provare un attacco con il codice nelle nostre macchine virtuali e di provare gli attacchi in security low,medium, high.

Codice in python per un attacco Brute Force :

(immagine codice)

Report sugli Attacchi di Forza Bruta alla DVWA:

Obiettivo dell'Attacco:

L'obiettivo principale dello script è eseguire tentativi di login automatizzati sulla DVWA attraverso una combinazione di username e password forniti in liste predefinite.
Ambienti di Attacco:

Home della DVWA:

Vengono eseguiti tentativi di login nella home della DVWA utilizzando richieste POST.
Se un tentativo di login ha successo, vengono visualizzate le credenziali valide.

Sezione Brute Force:

Viene tentato l'accesso alla sezione Brute Force utilizzando richieste GET con username e password inclusi nell'URL.
Le credenziali valide vengono visualizzate se l'attacco ha successo.

Strategia di Attacco:

Si utilizzano cicli for per iterare tra gli username e le password fornite.
Viene creata una sessione di richiesta (requests.Session()) per mantenere la coerenza tra le richieste.
Le risposte alle richieste di login vengono analizzate per determinare il successo o il fallimento del login.

Output e Visualizzazione:

L'output è colorato utilizzando la libreria colorama, facilitando la distinzione tra i tentativi di login falliti e quelli riusciti.

Attacchi fatti a security low, medium e high

spiegazione Attacchi:

Abbiamo condotto un test di sicurezza sull'ambiente a bassa sicurezza e abbiamo effettuato il login con tutte le password possibili attraverso l'implementazione di due cicli for. Durante questo processo, abbiamo creato sessioni e lanciato richieste POST per l'accesso. La nostra valutazione è stata basata sulla risposta ottenuta in caso di tentativo di login fallito, che ci ha permesso di determinare l'esito del login. Questo con gli attacchi in low.

Successivamente, abbiamo esteso la nostra analisi alla sezione di forza bruta della DVWA, dove abbiamo notato una variazione significativa nella logica del tentativo di login. In particolare, abbiamo osservato che, interagendo con la pagina di login di questa sezione, il metodo utilizzato non è stato POST, ma piuttosto GET.

Ambiente Low:

-In un contesto a sicurezza bassa, abbiamo riscontrato una maggiore vulnerabilità agli attacchi. Sfruttando cicli for per il login con tutte le password possibili, abbiamo constatato una scarsa resistenza alle tecniche di forza bruta.
-La mancanza di controlli avanzati ha reso gli attacchi più agevoli, senza la necessità di misure di protezione avanzate.
-L'assenza di un timer o di richieste di token utente semplifica gli attacchi, rendendo il sistema più suscettibile alle intrusioni.

Ambiente medium:

-Nel contesto a sicurezza media, abbiamo notato un miglioramento nelle difese rispetto a un ambiente a bassa sicurezza.
-Gli attacchi richiedono un maggior sforzo, poiché sono implementate alcune misure di sicurezza di base.
-Il timer potrebbe essere introdotto per rallentare gli attacchi di forza bruta, imponendo limiti temporali tra i tentativi di login.
-Mentre le contromisure sono più robuste, la mancanza di un user token potrebbe rappresentare ancora una potenziale vulnerabilità.

Questa differenza è importante in quanto implica che per accedere a questa sezione, i tentativi di login devono essere gestiti in modo diverso rispetto all'ambiente a bassa sicurezza. La consapevolezza di tale variazione ci ha guidato nella progettazione di strategie specifiche per affrontare le peculiarità di questa sezione e adottare approcci distinti per il login e l'analisi dei risultati.

Attacchi fatti a security low, medium e high

Ambiente high:

-In un ambiente a sicurezza elevata, abbiamo riscontrato una notevole resistenza agli attacchi.
Gli attacchi richiedono un alto grado di competenza, poiché sono implementati controlli avanzati e misure di sicurezza.
-L'introduzione di un timer con limiti rigorosi e la richiesta di un user token aggiungono ulteriore complessità agli attacchi di forza bruta.
-Le contromisure avanzate e la complessità dell'ambiente rendono gli attacchi più difficili da eseguire con successo.

Spiegazione di Token:

Un token è una stringa di caratteri utilizzata per rappresentare l'autenticazione di un utente o fornire accesso a risorse specifiche in un sistema.