Build Week

1. SQL injection

L’SQL injection (“Structured Query Language”) è una tecnica di hacking che, sfruttando alcuni errori nella programmazione di pagine HTML, consente di inserire ed eseguire codice non previsto all’interno di applicazioni web che interrogano un database.

Esso è un attacco potenzialmente pericoloso in quanto può essere effettuato soltanto avendo a disposizione un web browser qualsiasi e un pc.

Inizialmente, abbiamo messo le due macchine sulla stessa rete, cambiando i rispettivi indirizzi IP e verificando tramite il “ping” l’effettiva connessione tra le due.

Gli indirizzi IP delle rispettive macchine sono:

* IP Kali: 192.168.13.100
* IP Metasploitable: 192.168.13.150

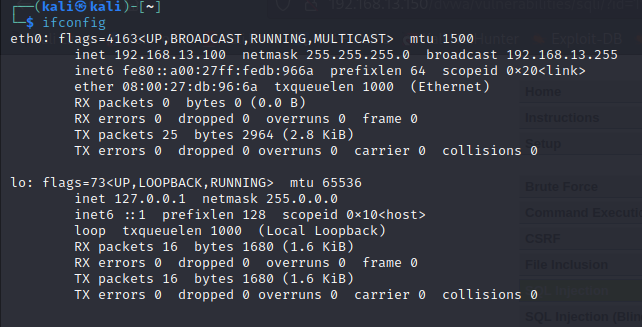


Immagine che contiene testo

Descrizione generata automaticamente

Una volta configurate le impostazioni di rete, ci siamo dedicati all’obiettivo prefissato per la giornata odierna.

Il nostro goal era quello di individuare le credenziali degli utenti registrati nel database della web application DVWA della macchina Metasploitable.

Per far ciò, ne abbiamo abbassato il livello di sicurezza (da HIGH a LOW) per poter più agevolmente recuperare quanto sopra descritto.

Immagine che contiene testo

Descrizione generata automaticamente

Ci siamo dunque spostati nella sezione “SQL injection”.

Immagine che contiene testo

Descrizione generata automaticamente

Qui abbiamo iniettato il codice che ci ha permesso di recuperare le credenziali delle quali necessitavamo.

Nella casella di testo “user ID” andremo ad inserire il comando utilizzato per stampare in output sulla pagina le varie informazioni, tra cui anche tutte le password cifrate di tutti gli utenti presenti all’interno del database della DVWA.

Il comando utilizzato è:

1' union select null, concat(user\_id,0x0a,first\_name,0x0a,last\_name, 0x0a, user,0x0a,password) from users #

Come si può evincere dallo screenshot di seguito, siamo riusciti a recuperare le credenziali, di cui username in chiaro e password crittografate nel formato hash MD5.

Immagine che contiene tavolo

Descrizione generata automaticamente

Il passo successivo è stato l’utilizzo del tool John the Ripper (un tool di password cracking per i sistemi Unix).

Le password cifrate riportate sopra sono state inserite innanzitutto all’interno di un file .txt, così da poter creare un dizionario, confrontato poi con la lista già predefinita in Kali “**rockyou.txt.gz”**.

In questo caso il file creato per contenere le password e gli username di DVWA si chiama “**hash.txt”**.

Immagine che contiene testo

Descrizione generata automaticamente

Di seguito vediamo il primo passaggio di ricerca della wordlist più adatta, in questo caso “**rockyou.txt.gz”**.

Aprendo il file, si ha evidenza di come al suo interno si trovi un file completamente scritto in hash.



I comandi riportati di seguito ci hanno permesso di caricare le password prima e di mostrarle a schermo in chiaro poi.

Immagine che contiene testo

Descrizione generata automaticamente

