Traccia:

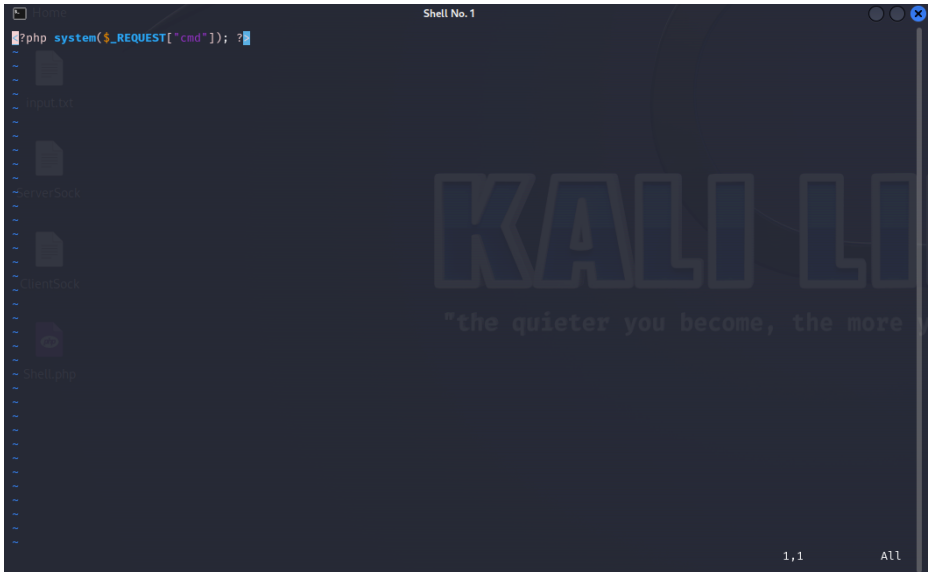
Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

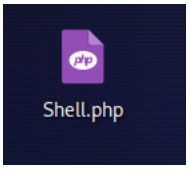
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

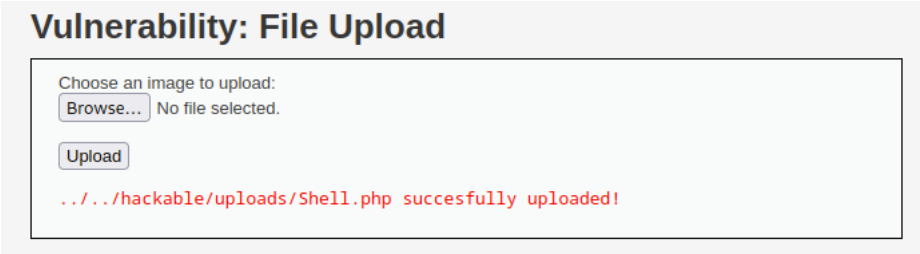
Svolgimento:

Partendo da un editor di testo che successivamente andremo a salvare con in .php creiamo la nostra shell di base che successivamente caricheremo sulla DVWA.

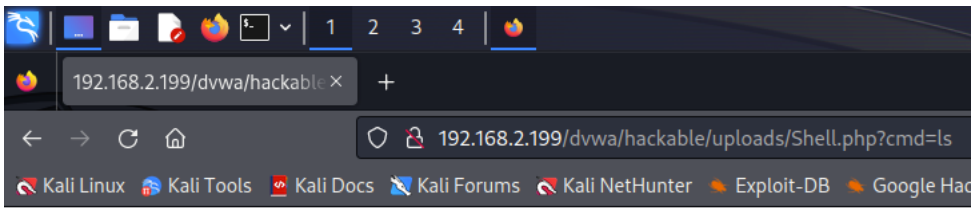




Dopo esserci collegati dal browser Kali ed aver settato il livello di sicurezza su low (altrimenti non funzionerebbe il caricamento in quanto viene eseguito il controllo del file) sfruttiamo la vulnerabilità che ci permette di caricare il nostro file invece di un immagine.



Infine sfruttiamo la shell e facciamo con l'esecuzione di un comdando "ls" passato come parametro dalla chiamata GET nell'url http://xyz.php?cmd=ls



Shell.php dvwa_email.png

Ci viene ritornato il contenuto della cartella.