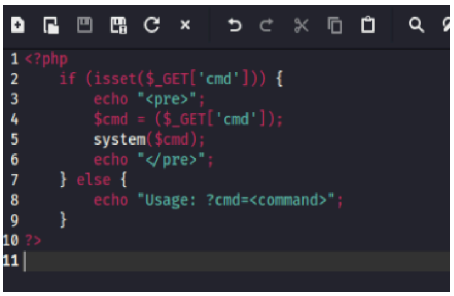
ARP-POISONING

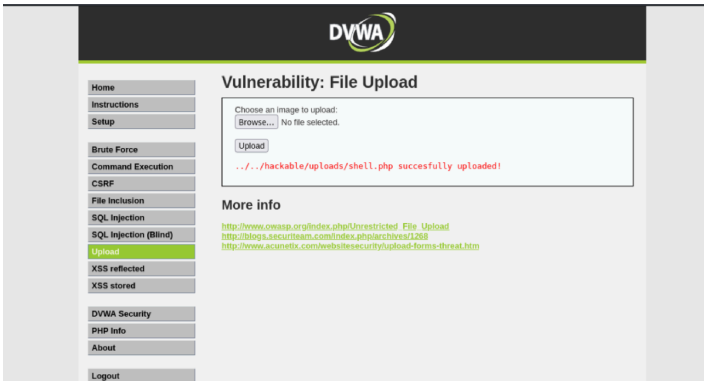
L’esercizio di oggi prevede di riuscire a controllare una macchina attraverso la vulnerabilità di porte aperte.

ecco i seguenti passaggi fatti:

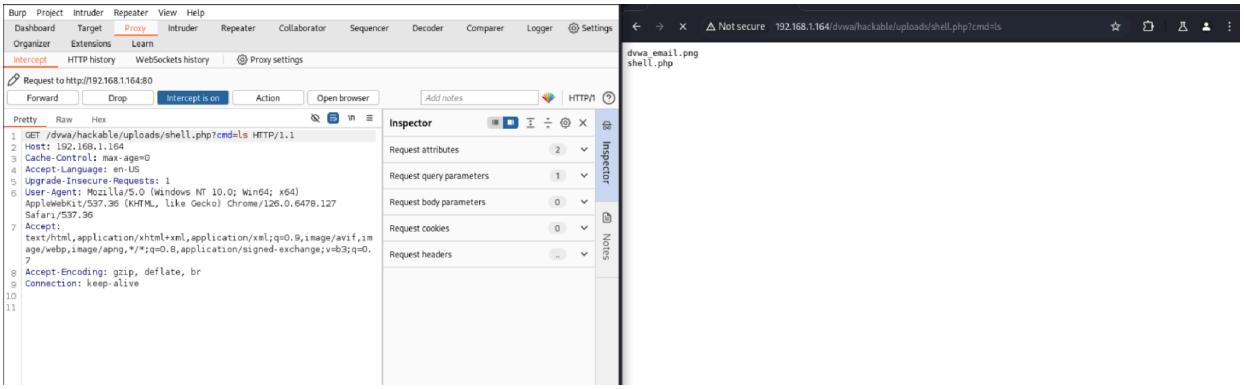
1 - Abbiamo usato un codice PHP che creasse di default alcuni file e ci permette di muoverci all’interno di Metasploitable:



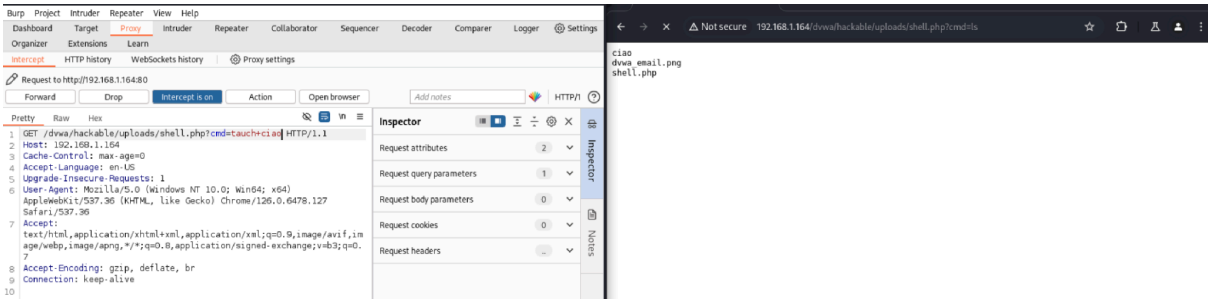
2 - siamo andati su DVWA e abbiamo impostato lo stato di sicurezza in low, e successivamente abbiamo uploadato il file PHP



3 - Abbiamo verificato che l’intercettazione tramite burpsuite stesse funzionando:



4 - Abbiamo aggiunto con il semplice comando da terminale “tauch+nomefile” un nuovo file, da qui abbiamo avuto la conferma di starci muovendo all’interno di metasploitable grazie a kali:



In questi procedimenti ci siamo messi a elaborare un attacco MITM (Man In The Middle) verso una rete appartenente alla stessa nostra rete, possiamo definire un attacco ARP POISONING questo test.

Il procedimento dei dati funziona che, A manda un pacchetto a B ma noi riusciamo a intercettare e addirittura a modificare in modo che arrivi con aggiunte, così che il file possa contenere link, immagini, file e altre variabili che potrebbero influenzare il pc.

Diego Petronaci