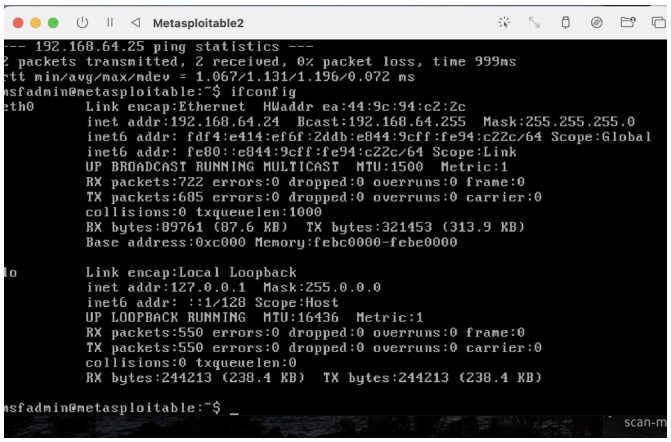
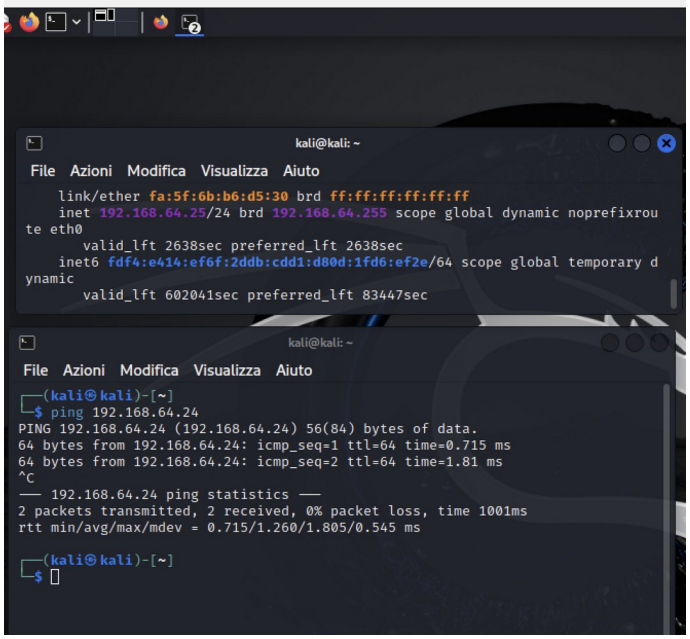
Nel **esercizio di oggi** ci è stato chiesto di **intercettare le richieste HTTP** tra **Metasploitable** e **Kali Linux**. Di seguito il procedimento:

Iniziamo verificando la connessione tra Metasploitable e Kali Linux tramite il comando ping, come mostrato nelle immagini seguenti.



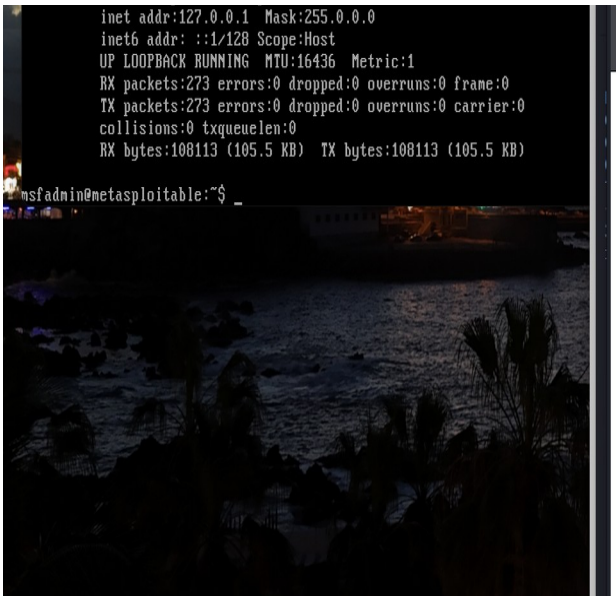



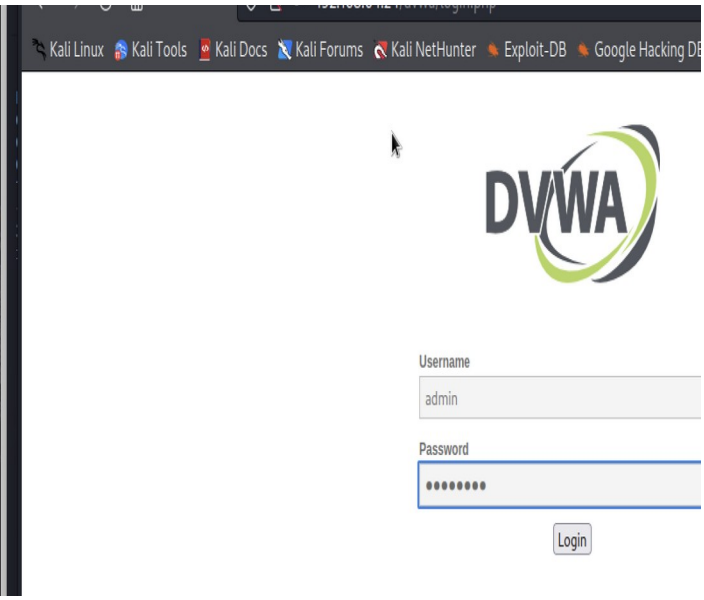

Una volta verificata la connessione tra le due macchine, procediamo da Kali Linux e accediamo alla

DVWA di Metasploitable ossia, indirizzo-ip/dvwa, utilizzando le credenziali:

•Username: admin

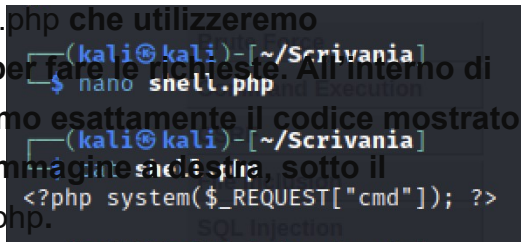
•Password: password




Una volta entrati, clicchiamo su DVWA SECURITY, e scegliamo LOW ed infine clicchiamo su SUBMIT

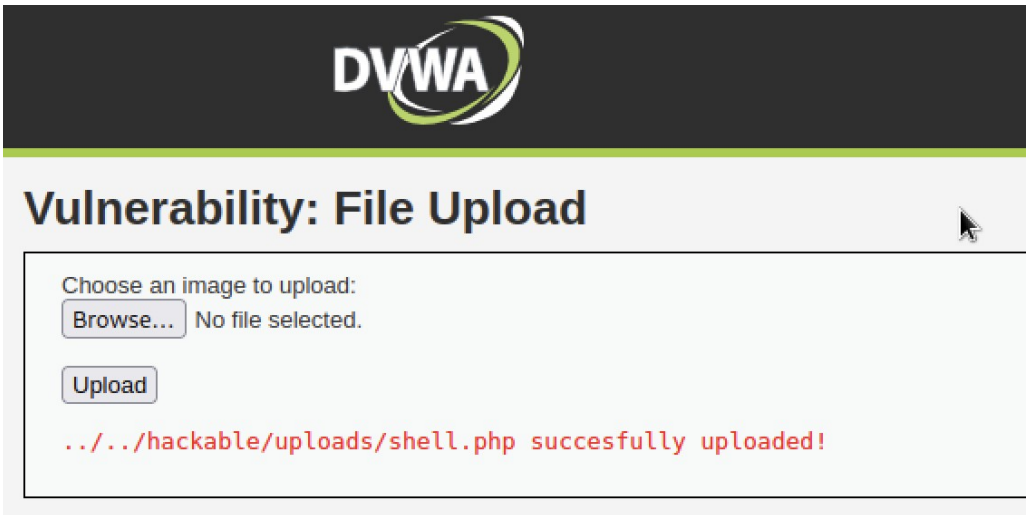
**Creiamo il file** shell.php **che utilizzeremo successivamente per fare le richieste. All'interno di questo file, inseriamo esattamente il codice mostrato nel terminale nell'immagine sotto, sotto il comando** cat shell.php**.**





**Ora, clicchiamo s**
**caricare il file**
**abbiamo creato**

**Se il caricamento è andato a buon f**
**vedremo la scritta in rosso, come mostrato nell'imm**



**Finito il caricamento, testiamo se effettivamente riceviamo le richieste di tipo HTTP. Per farlo, apriamo il motore di ricerca e modifichiamo le impostazioni del proxy in modalità manuale, inserendo** 127.0.0.1 **come indirizzo e** 8080 **come porta, così da attivare il proxy. Una volta configurato, inseriamo l'URL ottenuto precedentemente dalla DVWA. Come si può vedere nell'immagine successiva, tutto è andato a buon fine, poiché otteniamo informazioni dettagliate riguardo alla richiesta GET dell'URL digitato, lo stesso che abbiamo inserito nel motore di ricerca.**