LABORATORIO 13 GENNAIO 2024 L1-S6

ESERCIZIO DEL GIORNO:

Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shellin PHP:

1: Configurazione del laboratorio:

Configurate il vostro ambiente virtuale in modo che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux.

Assicuratevi che ci sia comunicazione bidirezionale tra le due macchine.

2: Esercizio Pratico:

Sfruttate la vulnerabilità di file upload presente sulla DVWA (Damn Vulnerable Web Application) per ottenere il controllo remoto della macchina bersaglio.

Caricate una semplice shell in PHP attraverso l'interfaccia di upload della DVWA.

Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

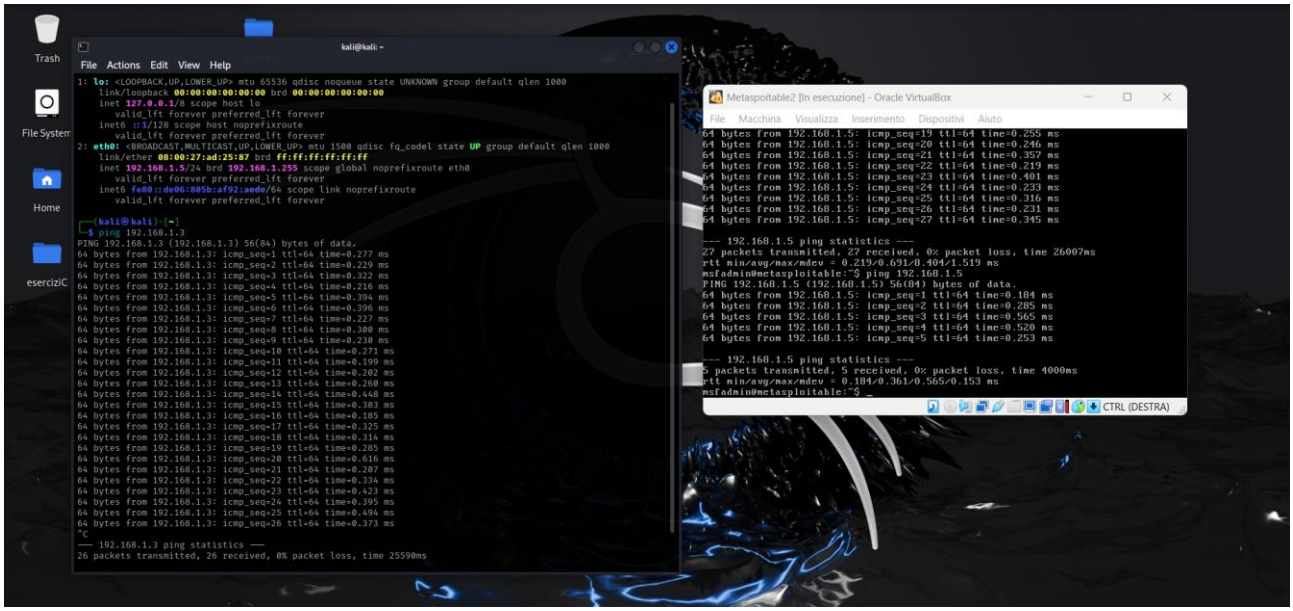
3: Monitoraggio con BurpSuite:

Intercettate e analizzate ogni richiesta HTTP/HTTPS verso la DVWA utilizzando BurpSuite.

Familiarizzate con gli strumenti e le tecniche utilizzate dagli Hacker Etici per monitorare e analizzare il traffico web.

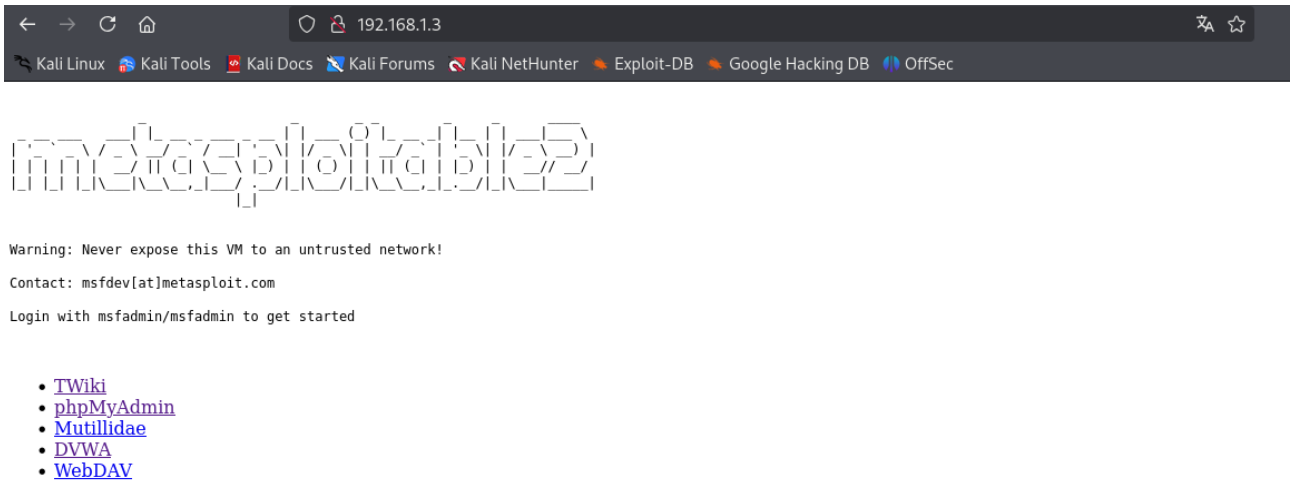
PREPARAZIONE DELL' AMBIENTE:

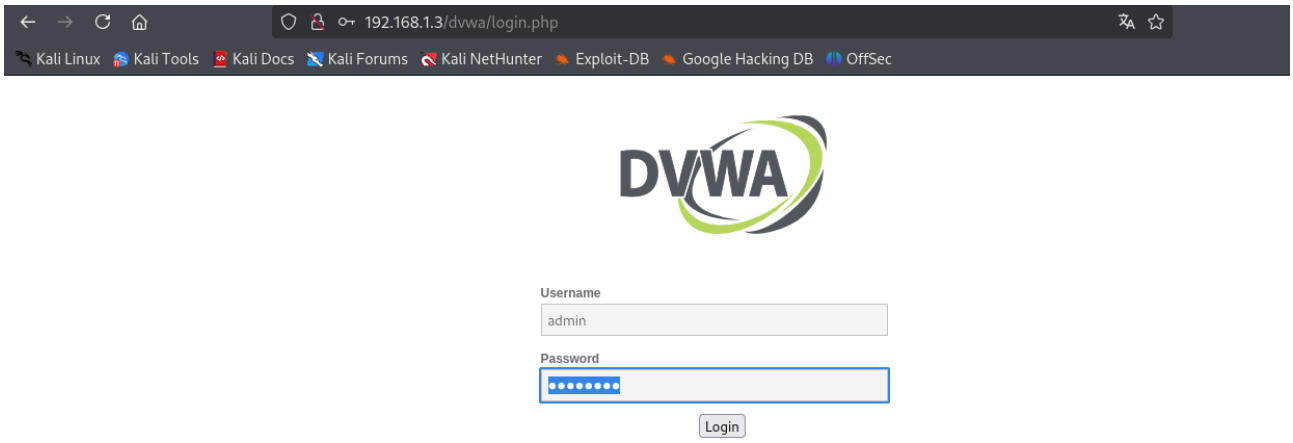
Assicuriamoci di configurare le macchine virtuali Kali e Metaspoitable e che queste abbiano la comunicazione l' una con l' altra.



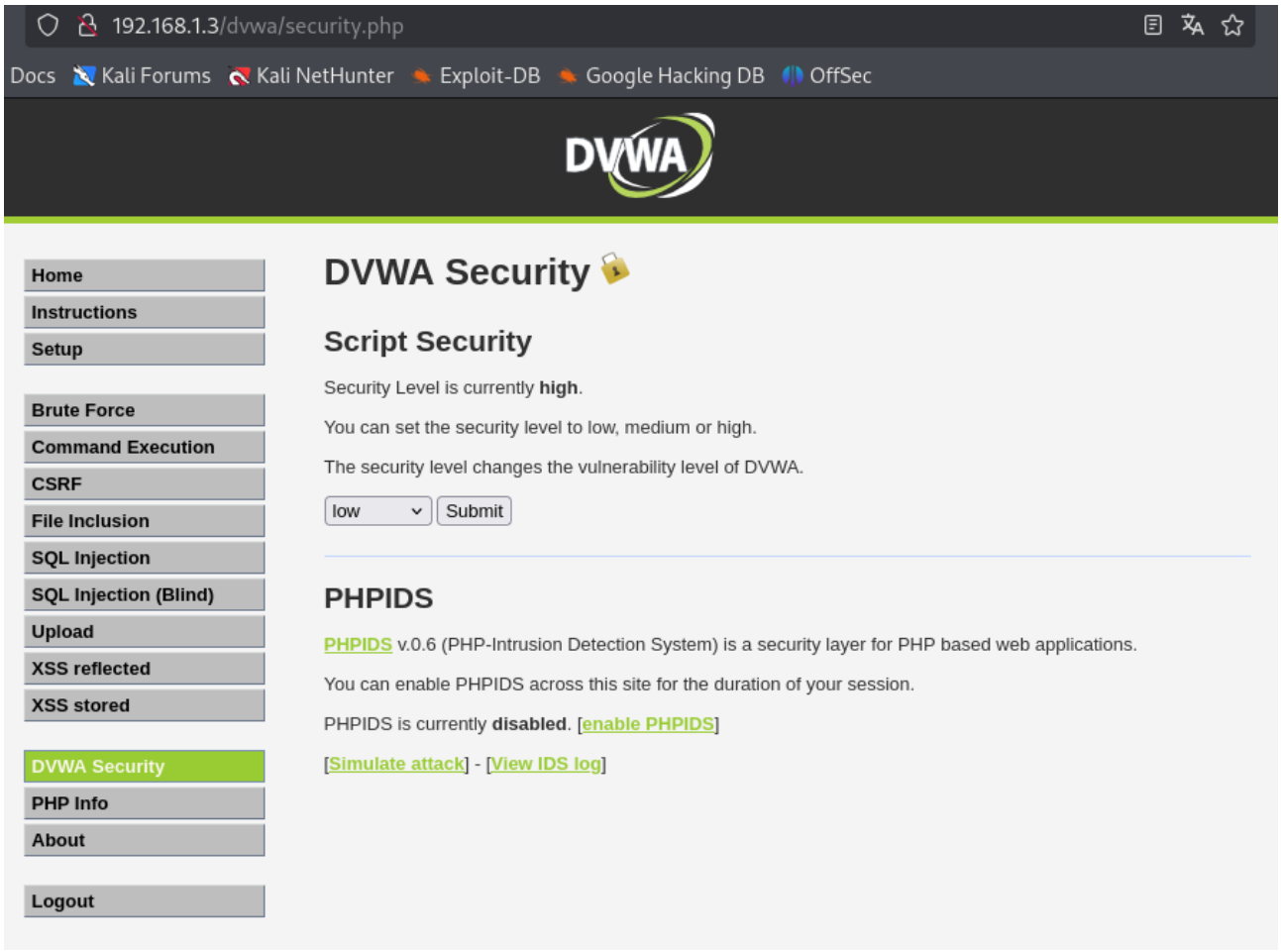
CARICAMENTO DELLA SHELL PHP:

Accediamo alla DVWA sulla macchina Metasploitable tramite il browser della macchina Kali Linux.



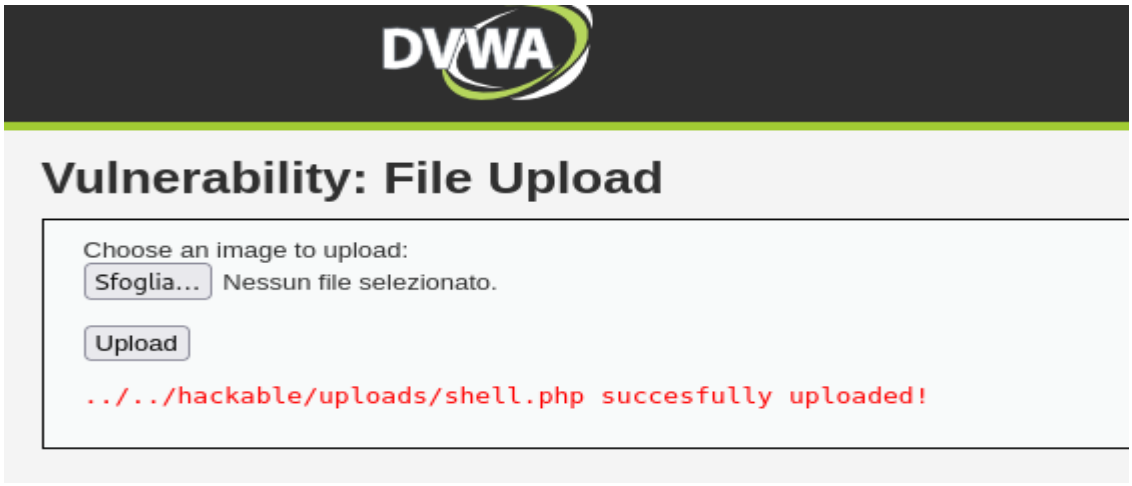


Impostiamo il livello di sicurezza più basso possibile e salviamo la scelta.



Navighiamo alla sezione Upload quindi creiamo un semplice file shell.php e lo carichiamo attraverso il modulo di upload.

Verifichiamo quindi che sia caricato correttamente.



Apriamo burpsuite e iniziamo ad intercettare il traffico.