Esercizio S7L3

L’esercizio ci chiedeva di creare una sessione sul servizio php tramite un exploit ma prima diamo una definizione di exploit:

1) Per Exploit s’intende un codice malevolo che va a sfruttare le vulnerabilità del codice o del software.Non ha bisogno dell’interazione dell’uomo dato che la vulnerabilità è già presente nel codice

Procedure:

- Si avvia Metasploit;
- Si cerca il servizio da fare l’exploit, controlliamo le opzioni necessarie per vedere se abbiamo inserito tutti i parametri necessari;
- In questo caso l’unico parametro richiesto che mancava era l’RHOSTS quindi si va a settare per l’RHOSTS l’indirizzo IP della vittima cioè Metasploitable;
- si rifà il controllo dei parametri necessari;
- Poi è possibile effettuare l’exploit.