Esercizio 08/11/2023

Nell'esercizio odierno ci viene richiesto di utilizzare Metasploit per exploitare php.

L'Exploit è la fase 3 del Pentesting ed è la fase più delicata di tutto il processo.
L'Exploit non è una sola azione ma la prima fase di una **serie di azioni** che va a testare, ad identificare le vulnerabilità di un sistema, è una sorta di metodo di sfondamento, va a creare cioè un varco (N.B. ciò significa che c'è una **vulnerabilità già esistente**). Alla fine di queste fasi, essendo comunque entrati e avendo, quindi, scoperto la vulnerabilità, il lavoro dell'Ethical Hacker (almeno per questo programma) finisce qui e si può passare direttamente alla fase 7, il report. Stesso discorso se la shell non viene creata dopo l'exploit perché vuol dire che se non entro io non entra neanche il BH.

La seconda fase è andare a trovare un **payload** (un file nocivo che mi permette di creare una shell) che ci permetterà di passare alla terza fase, la **shell**, che crea una connessione tra due dispositivi. Quest'ultima può essere di tipo **reverse o bind**, la differenza è che, una volta creato il payload ed è andato a buon fine, la prima creerà una connessione dal computer vittima al computer attaccante (quindi dall'interno verso l'esterno), mentre nella bind accade il contrario. Poiché è molto probabile che ci siano sistemi di sicurezza (firewall, IDS, IPS), è meglio utilizzare la reverse, la bind viene usata quando siamo già all'interno della rete, e non è detto che funzioni perché il dispositivo in questione potrebbe comunque essere coperto da un dispositivo di sicurezza come un firewall e quindi non funzionare ugualmente.

L'Exploit, a differenza del **Malware**, sfrutta la vulnerabilità del sistema e non richiede alcun tipo di permesso. Quello che utilizzeremo deve essere specifico per la versione di quel determinato programma, se devo ad esempio testare una vulnerabilità su Office devo ricercare la versione dell'Office in questione altrimenti non è detto che funzionerà. Non è detto perché se vado ad immettere una versione più datata è possibile che la vulnerabilità in questione sia già stata corretta dall'aggiornamento del programma.

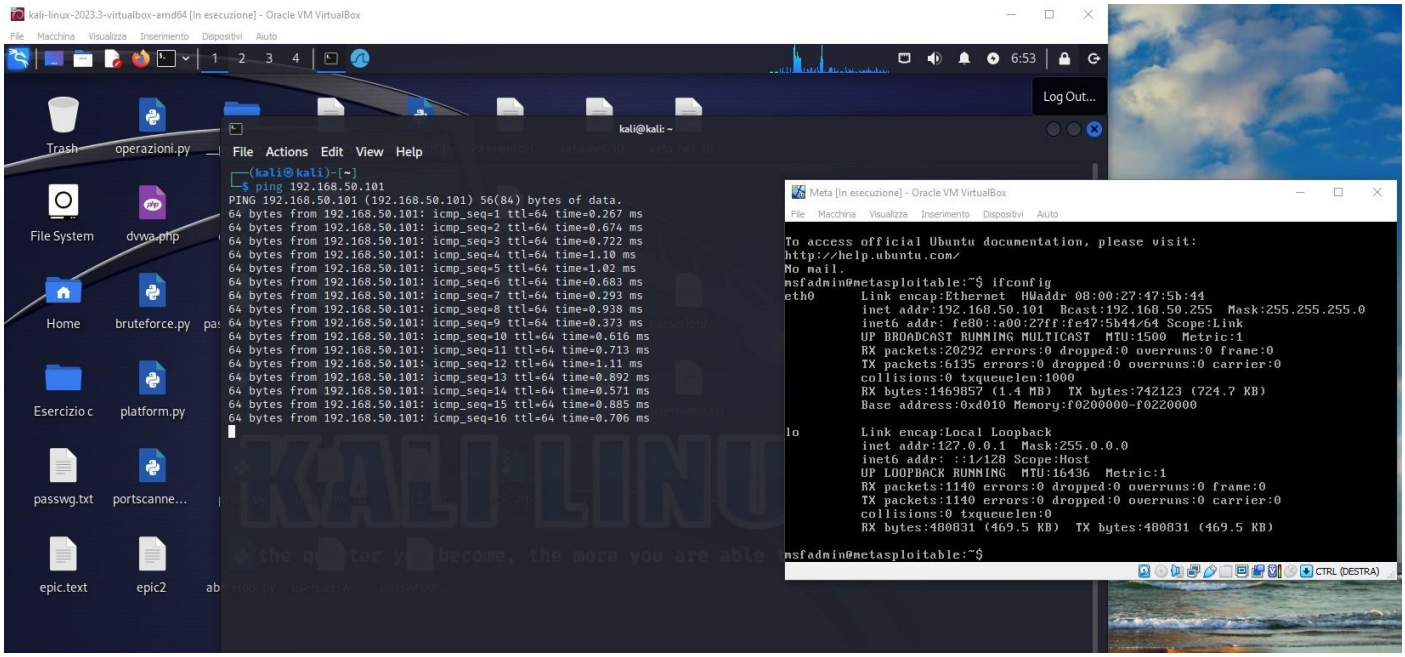
Per sapere se l'Exploit funziona avrò due strade, la prima a livello manuale (sconsigliata per via del tempo che impiegheremmo), la seconda a livello automatico e per fare questo si utilizzano programmi specifici come **Metasploit** che prova tutte le combinazioni in maniera automatica

Per arrivare a tutto questo si avvia Metasploit e si utilizzano una serie di comandi che ci porteranno all'ultima fase. E' molto importante sapere che perché l'exlpoit abbia effetto il programma che andiamo ad "exploitare" deve essere attivo, startato.

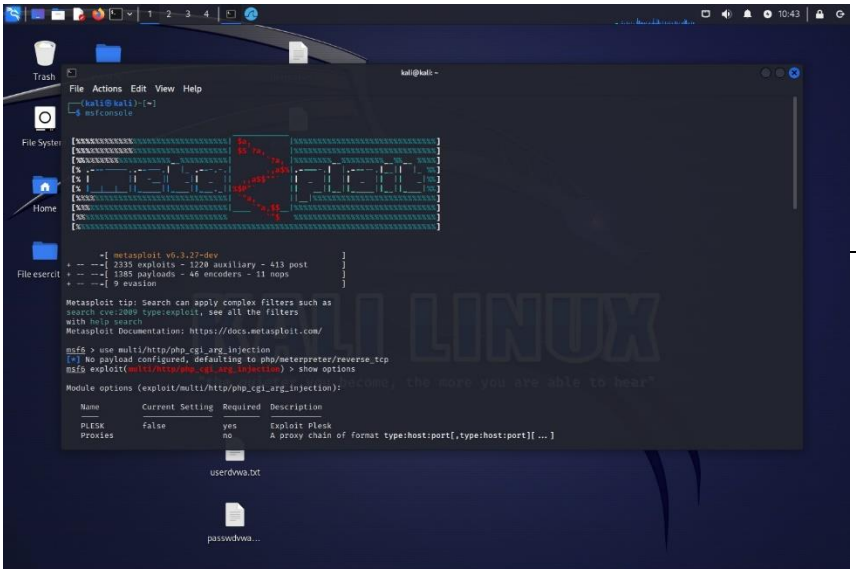
I moduli auxiliary, a differenza dei nomali che eseguono attacchi diretti e utilizzano un payload, sono moduli di supporto, forniscono cioè funzionalità ausiliarie che possono essere utilizzate in diverse fasi di pentesting. La differenza sostanziale sta proprio nel fatto che non usano (quasi mai) il payload

Di seguito la serie di comandi utilizzati per arrivare all'obiettivo:

Prima di tutto controllo che le macchine riescano a pingare

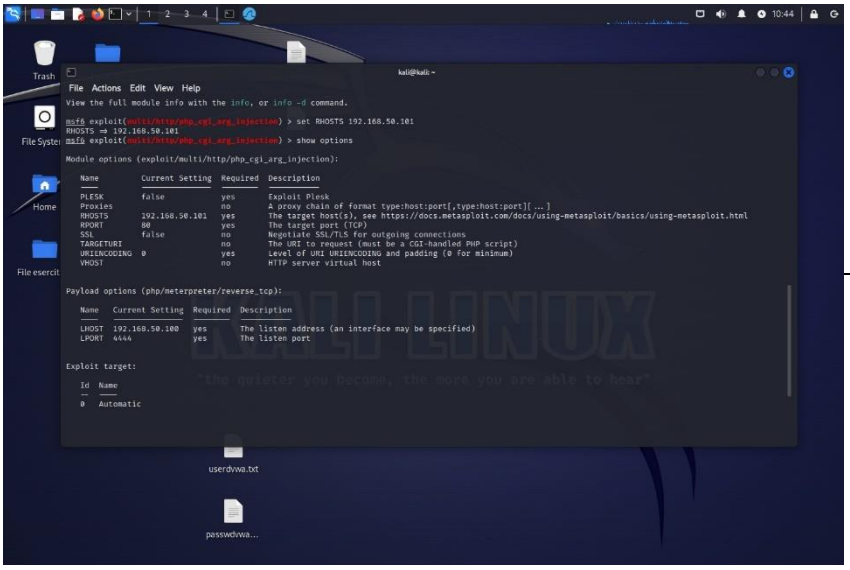


A questo punto, verificata la comunicazione tra le macchine, avvio metasploit su un nuovo terminale e entro in php



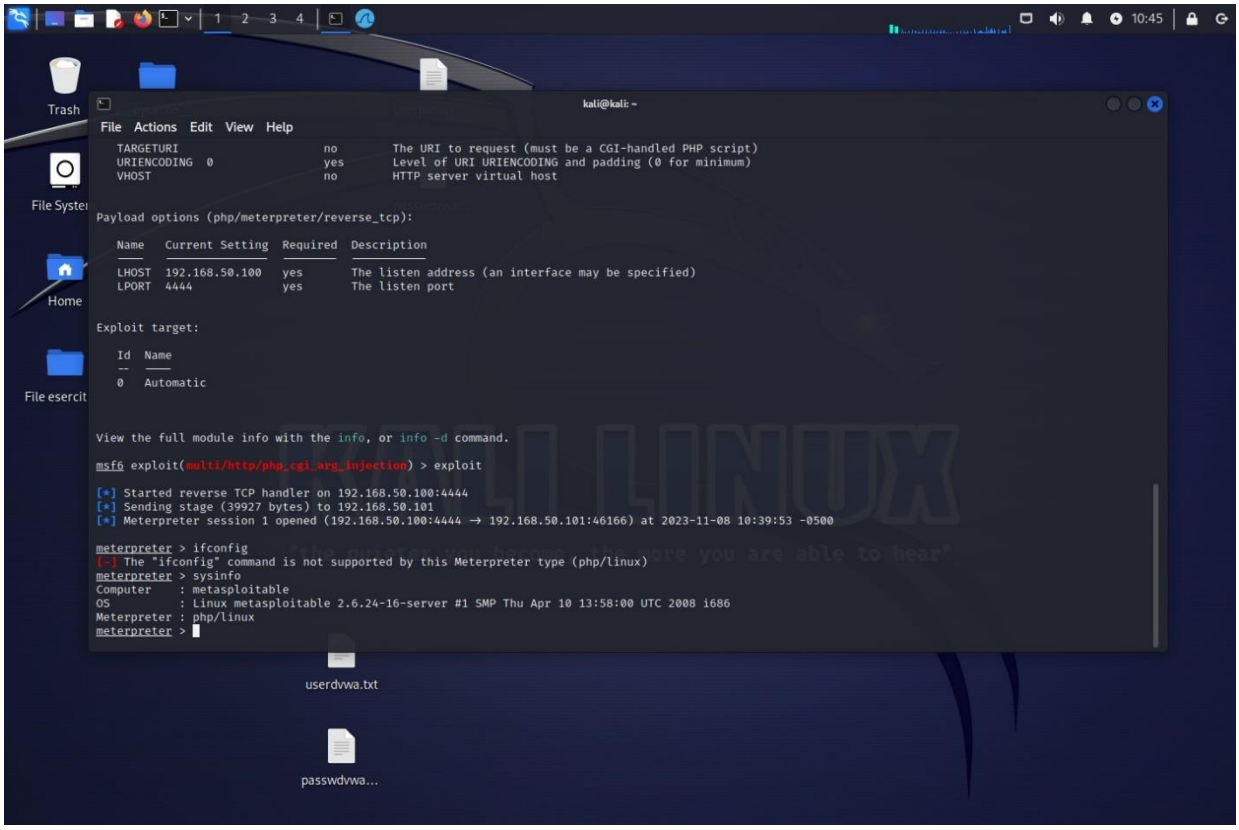
Avvio Metasploit e use

Quindi eseguo tutti i comandi per arrivare all'exploit:



Set RHOST e verifica

Infine lancio l’Exploit e verifico di poter effettivamente entrare nella macchina vittima



N.B. Nel comando show options è importante che tutti i “Required” contrassegnati con “yes” siano inseriti, quelli invece contrassegnati con “no” sono facoltativi.