EPICODE

Esercizio S6 – L2

TRACCIA

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.  
Lo scopo dell’esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.  
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

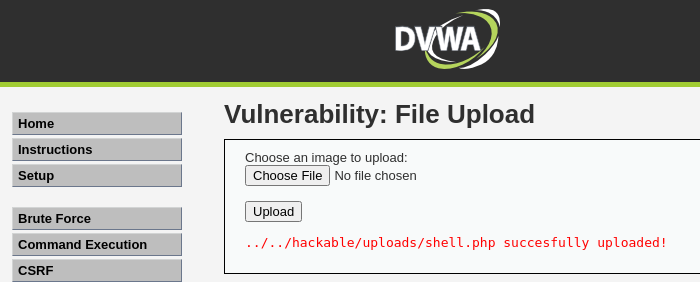
SOLUZIONE

Per iniziare si è accertata la connessione tra Kali Linux e Metasploitable. Successivamente si è creato un codice php e lo si è salvato sul Desktop.

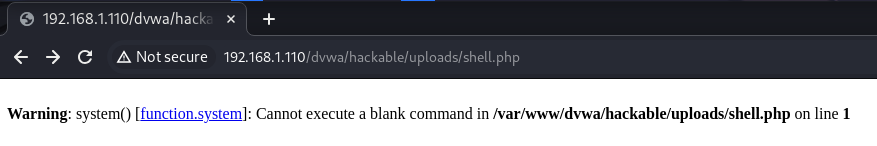
Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

Si è poi aperto il web browser da Burbsuite. Si è entrati nella DVWA, si è impostato su low la difficoltà, e in seguito si è caricato il file .php nella pagina “upload” di DVWA.  
A valle dell’upload si è ricevuta la conferma del caricamento sul path “…/.../hackable/uploads/shell.php”.



Inserendo “http://192.168.1.110/dvwa/hackable/uploads/shell.php” nell’URL si riceve un messaggio di errore perché la shell si aspetta un parametro cmd nella GET con un comando da eseguire.

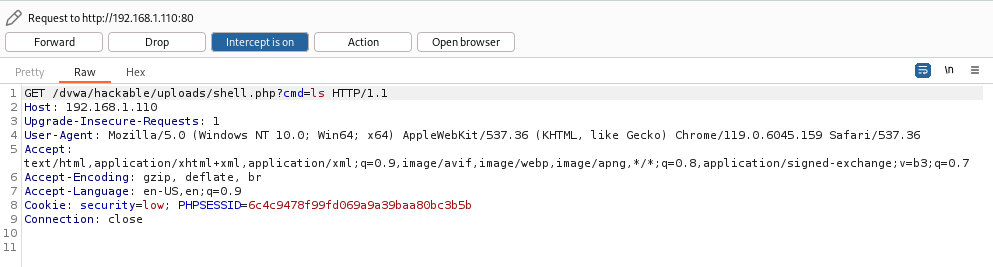


Così si aggiunge “?cmd=ls” per far eseguire il comando “ls” via GET.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Nell’immagine sotto è possibile vedere la richiesta GET su Burpsuite.



Modificando la richiesta su Burpsuite è possibile far eseguire comandi differenti. Nell’immagine sotto un esempio con il comando “pwd”.



Il comando “pwd” permette di vedere il percorso effettuato.

