martedì 1 ottobre 2024 20:11

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 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.

Consegna:
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna

Apriamo la machina PfSense per fare da ponte tra le macchine Linux e Meta in modo che comunichino tra di loro anche se appartengono a reti diverse e verifichiamone poi la connessione a internet. Fatto ciò, la prima cosa da fare è aprire burpsuite e cliccare su intercept in modo che sia su ON e aprire il broswer di burpsuite per intercettare le nostre richieste. Una volta inserito l'IP di Meta sul browser di ricerca cliccare su DVWA, impostare le credenziali per entrare.

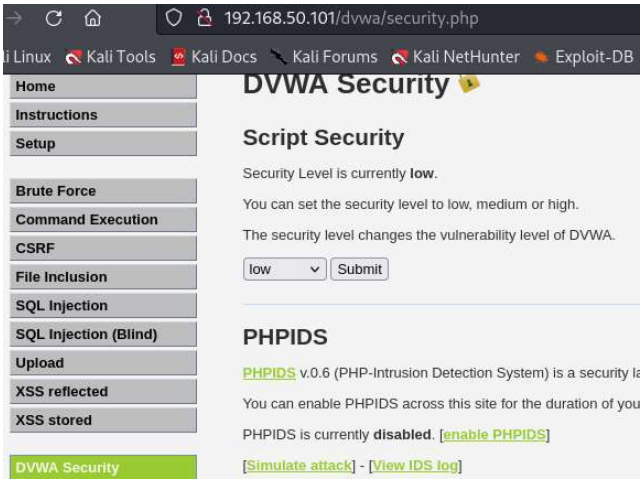
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

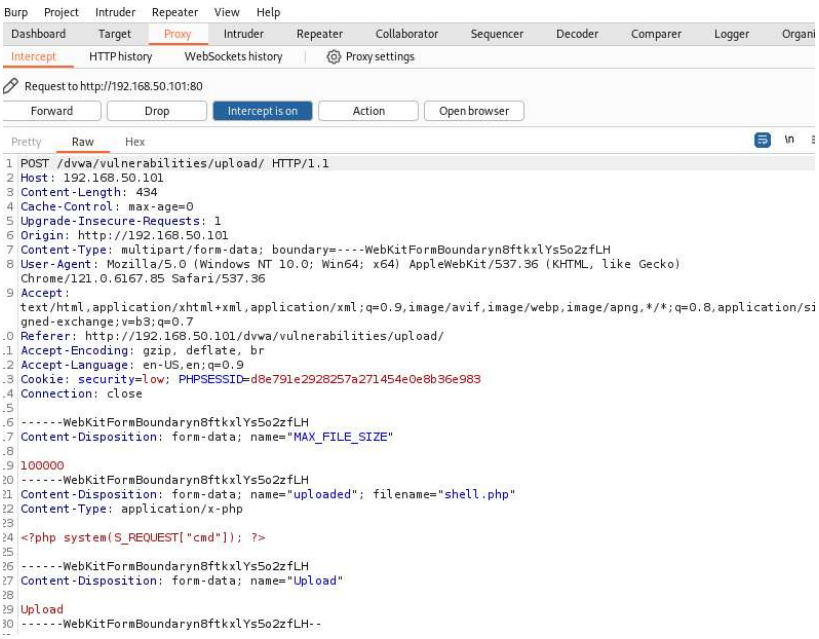
Una volta entrati impostare la sicurezza su low e salvare



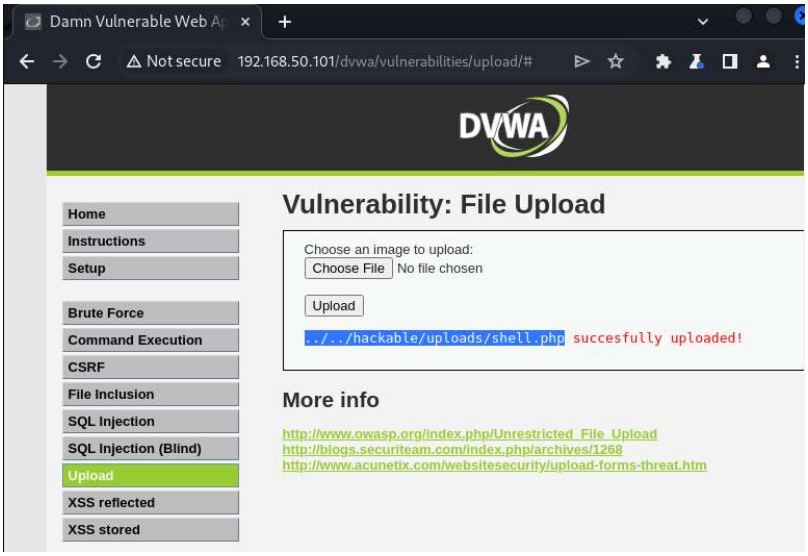
Creare un file shell.php con nano con all'interno un codice PHP che crea una web shell che consente di eseguire comandi di sistema sul server.

Spostiamo ora su Upload e carichiamo la nostra shell

Come possiamo vedere dall'immagine qui sotto burpsuite ha intercettato la nostra richiesta e ci mostra l'header del pacchetto (riga 1-14) con il tipo di richiesta (POST), l'Host, la lunghezza e informazioni varie come cookie ed il file caricato (riga 24)



Se torniamo sul nostro browser ci accorgeremo di aver ricevuto un messaggio in rosso che ci conferma che la nostra shell è stata caricata al path **../../hackable/uploads/shell.php**



Connettendoci al path, riceveremo un errore perché la nostra shell si aspetta un parametro cmd nella get con un comando da eseguire.

Aggiungiamo quindi il parametro cmd=ls nella GET e vedremo che l'applicazione ci ha restituito la lista dei file. Ciò significa che la nostra richiesta «ls» è stata eseguita dalla shell.