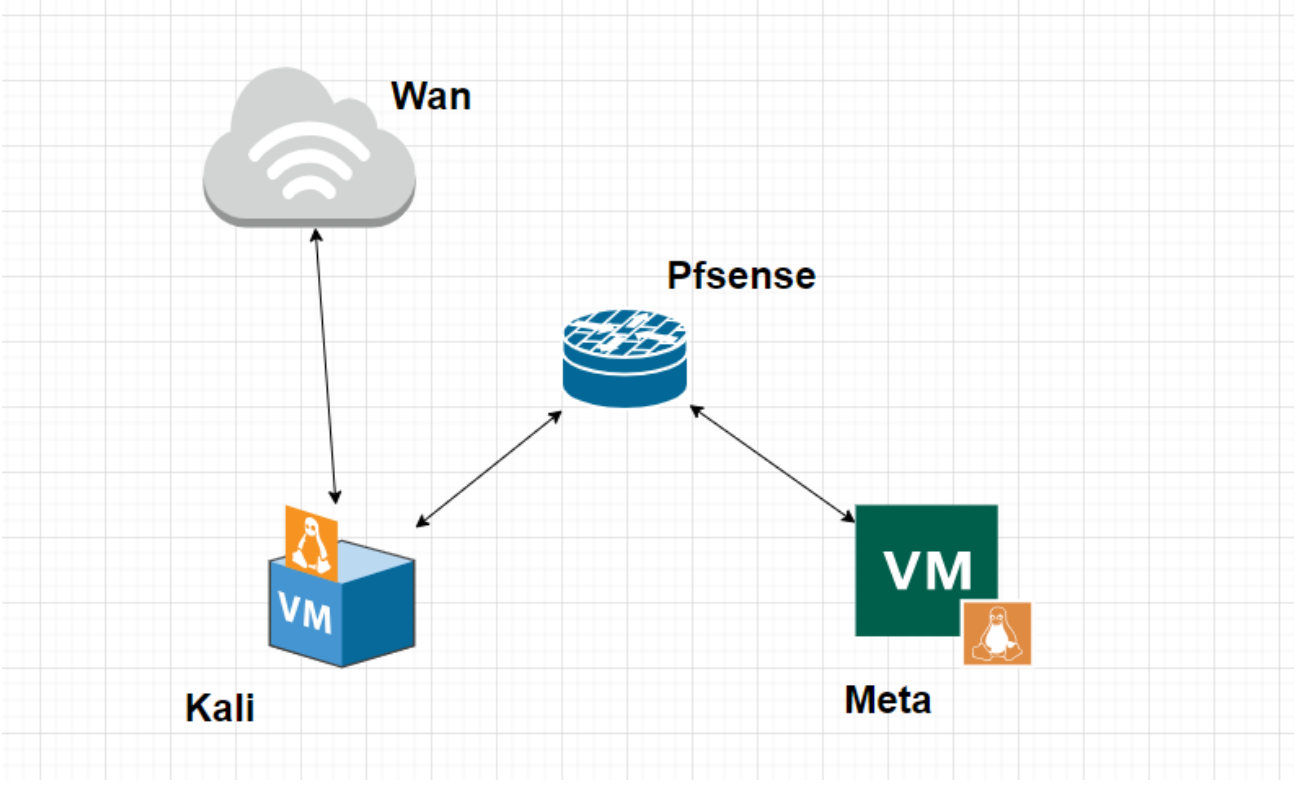
Exploit Dvwa

Richieste esercizio

Sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. Monitorando tutti gli step con BurpSuite.

Il laboratorio virtuale

- Una VM kali linux
- Una Vm metasploitable2
- Un firewall pfsense



Programmi utilizzati:

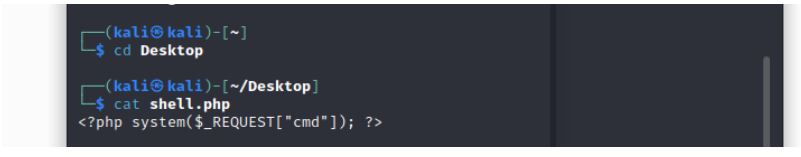
BURPSUITE

- Burpsuite=Le funzionalità di Burp Suite includono la capacità di intercettare e analizzare il traffico web, l'iniezione di dati malevoli o "payload" per rilevare vulnerabilità e una scansione automatica che individua e segnala problemi di sicurezza

Fasi dell'exploit

Fase 1

- **Scrittura della shell in php**



In questo caso ne prediamo una molto semplice:

Fase 2

- **Accesso su dvwa**

Prima ci accertiamo che le due machine comunichino (un semplice "ping ip_meta" da kali andrà benissimo), poi avviamo dalla Home di Kali avviamo Burpsuite, scegliamo l'opzione proxy, mettiamo le intercetazoni su on e avviamo il browser.

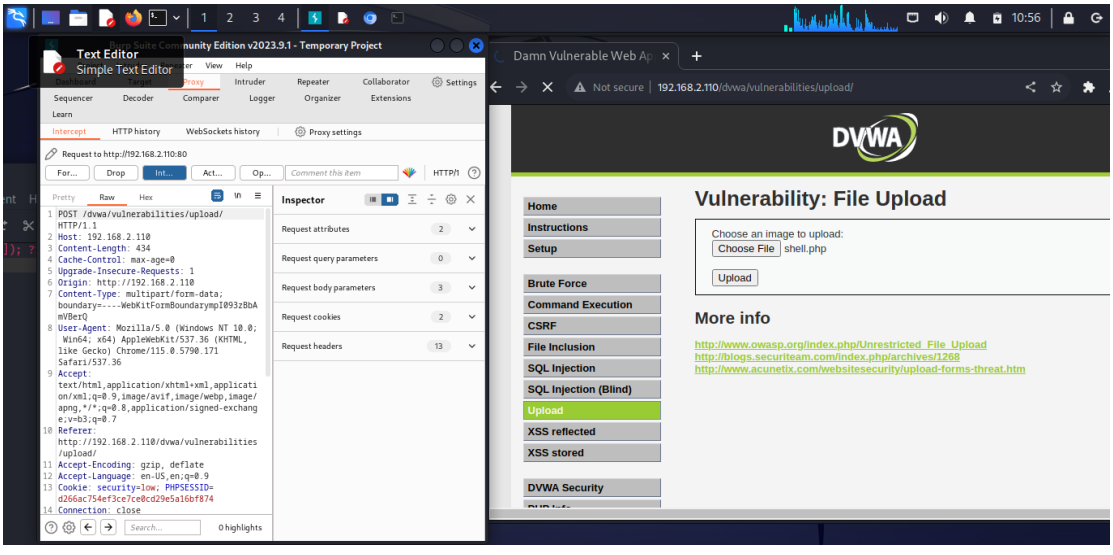
Il browser predefinito è chromium, ma va bene qualsiasi altro, scriviamo nella barra di ricerca l'ip di metasploitable2,ci porta alla pagina server di metasploitable, noi scegliamo l'opzione DVWA e fra le impostazioni di DVWA mettiamo la sicurezza al minimo (fattore molto importante).

Fase 3

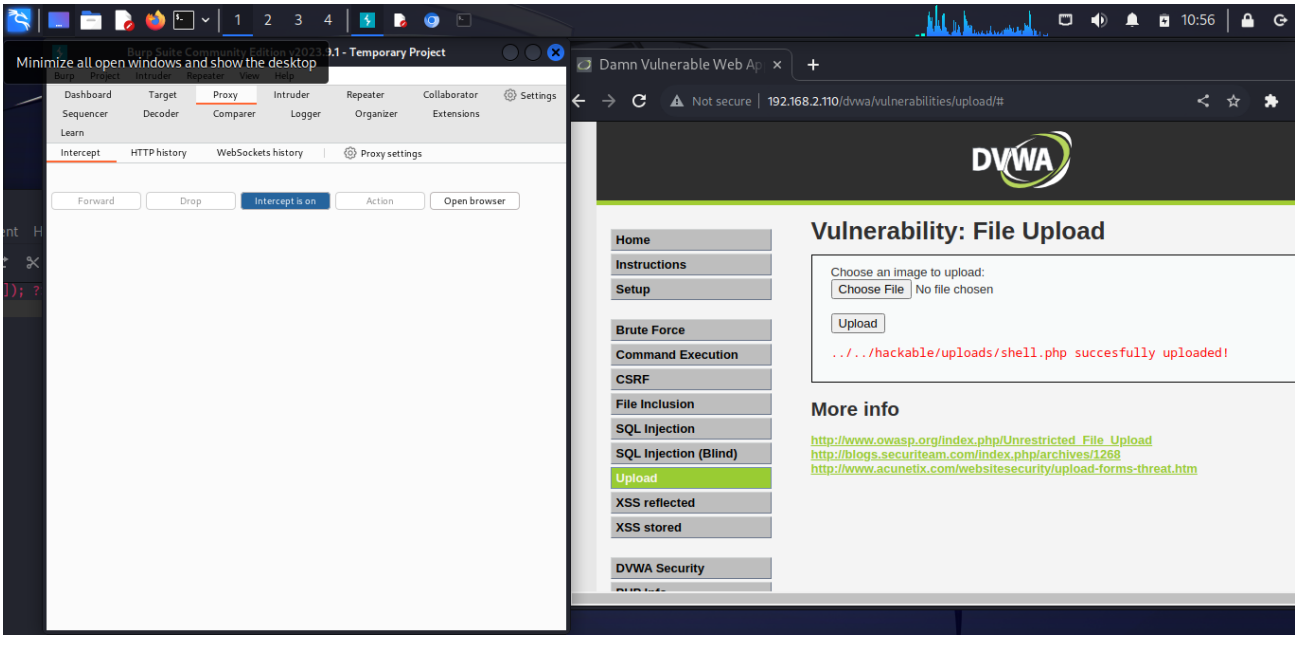
- **Upload della shell**

Nella sezione Upload di dwva carichiamo la shell che abbiamo scritto in precedenza e guardiamo da burpusuite cosa otteniamo, dovremmo ottenere una

comunicazione in POST.



E successivamente una modifica dell'interfaccia HTML di DVWA con la comparsa di alcune opzioni da inserire in GET

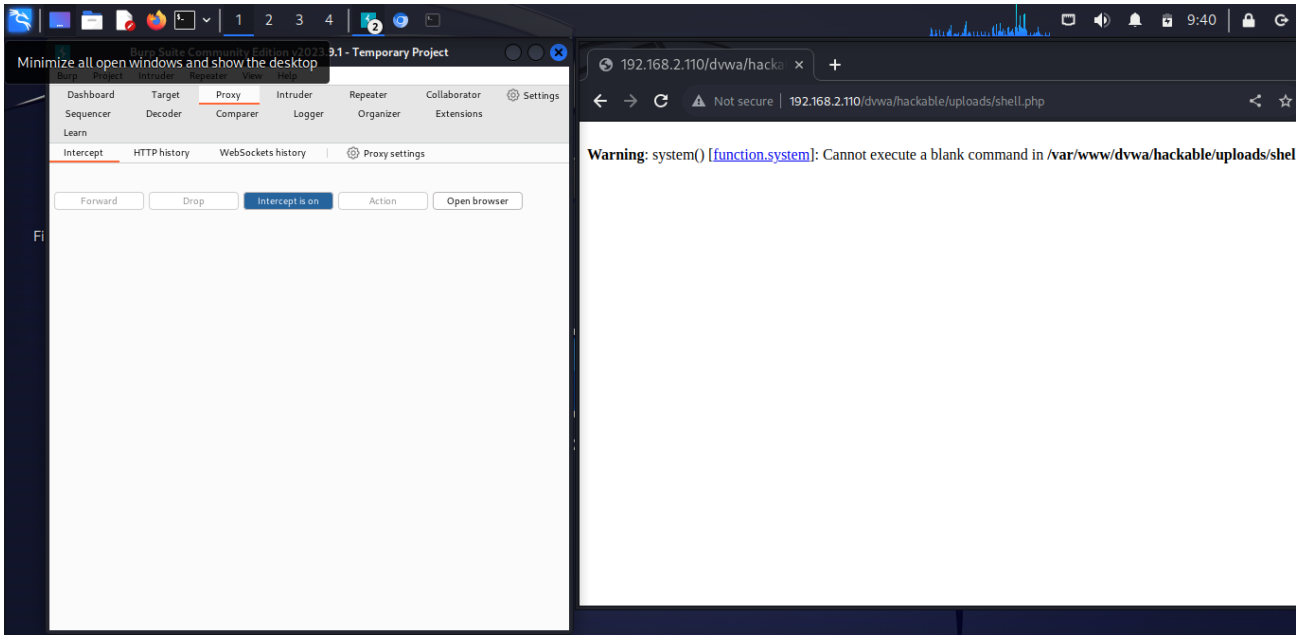


Fase 4

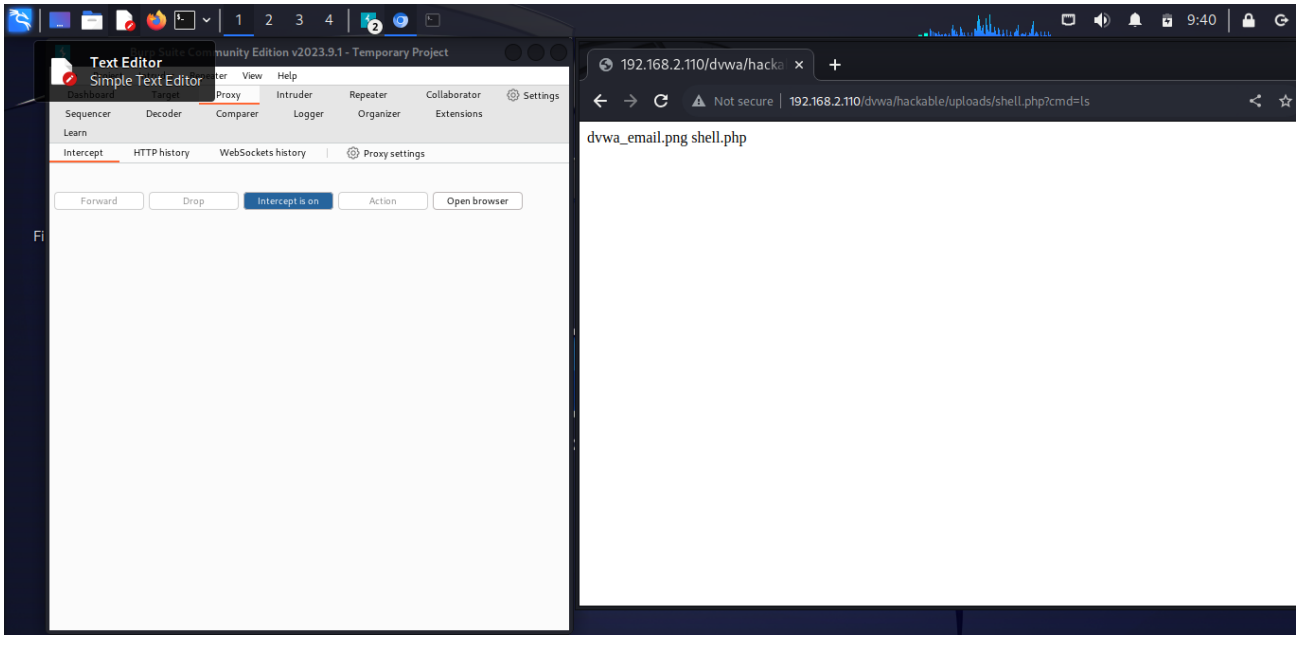
- **Completamento dell'exploit**

Copiamo la riga nell'url, lasciano l'indirizzo ip e la scritta dwva, e lanciamo la ricerca

la ricerca darà errore:



l'errore è dovuto all'assenza di un comando, noi cometteremo "cmd=ls" un comando utilizzato in sistemi Unix e Unix-like per elencare i file e le directory nella directory corrente.



E otteniamo questo come responso

Conlusioni

Siamo riusciti con facilitare a compire l'exploit su DVWA ma perchè è una webApp progettata apposta per essere facilmente penetrabile (Basti pensare che se la sicurezza non è su low questo procedimenti deve subire delle modifiche e diventa meno immediato), però è una buona patrica per impare a usare script entrare bene nella logica della

comunicazione dei dati fra utente e server, quanto siano importanti le comunicazioni con i metodi HTTP/ HTTPS e come siano differenti tra loro questi metodi.