Report Exploit File Upload

Obiettivo: simulare un attacco alla DVWA sfruttando la vulnerabilità nel modulo File Upload, al fine di ottenere l'accesso remoto tramite Reverse Shell.

Step 1: Configurazione delle reti e dei servizi.

Per questa simulazione, sono state utilizzate due macchine virtuali, Kali Linux come attaccante e Kali con DVWA come target.
Le ho configurate in modalità Host-only per garantire la comunicazione diretta tra di loro senza avere connessione ad internet. Ho verificato che il DHCP stesse fornendo un IP valido (ho utilizzato il DHCP per semplicità) e successivamente ho testato la connessione con il ping, con risultato positivo.
Ho dovuto configurare Apache2, PHP e MariaDB (non avevo tenuto lo snapshot dall'ultima volta, lezione imparata) affinchè si potesse accedere alla pagina della DVWA.

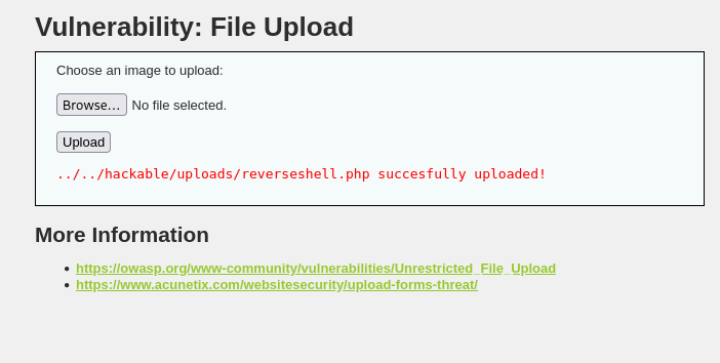
Step 2: Creazione della Reverse Shell in php.

Ho generato una Reverse Shell PHP con l'aiuto dell'AI inserendo il mio IP di Kali (La macchina attaccante) e la porta in ascolto. In questo caso come IP ho messo 192.168.56.103 e come porta 4444.

Step 3: Upload del file via DVWA

Sempre dalla Kali principale, dopo aver attivato i servizi configurati in precedenza, sono entrato nella pagina della DVWA tramite l'ip target, digitando quindi: http://192.168.56.102/dvwa/

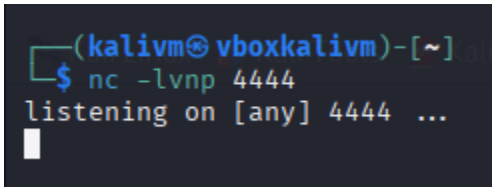
E successivamente, dopo aver impostato il livello di Sicurezza su Low, ho caricato la Reverse Shell.



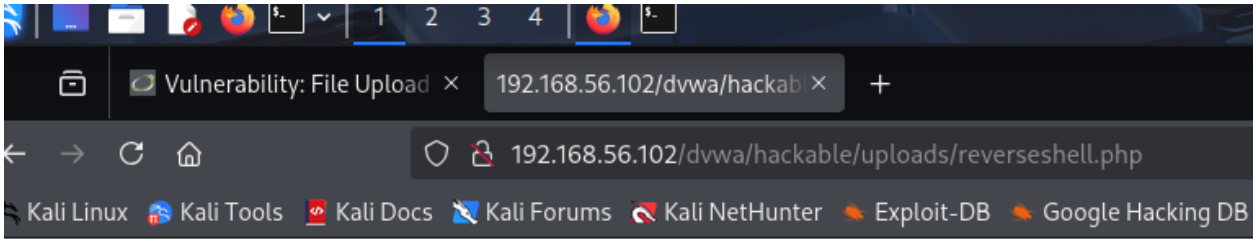
Fase 4: Netcat

Subito dopo aver caricato il file nella DVWA, ho aperto Netcat per iniziare l'ascolto sulla porta 4444, così che andando nella pagina della Reverse Shell, potessi ottenere l'accesso remoto della macchina target.

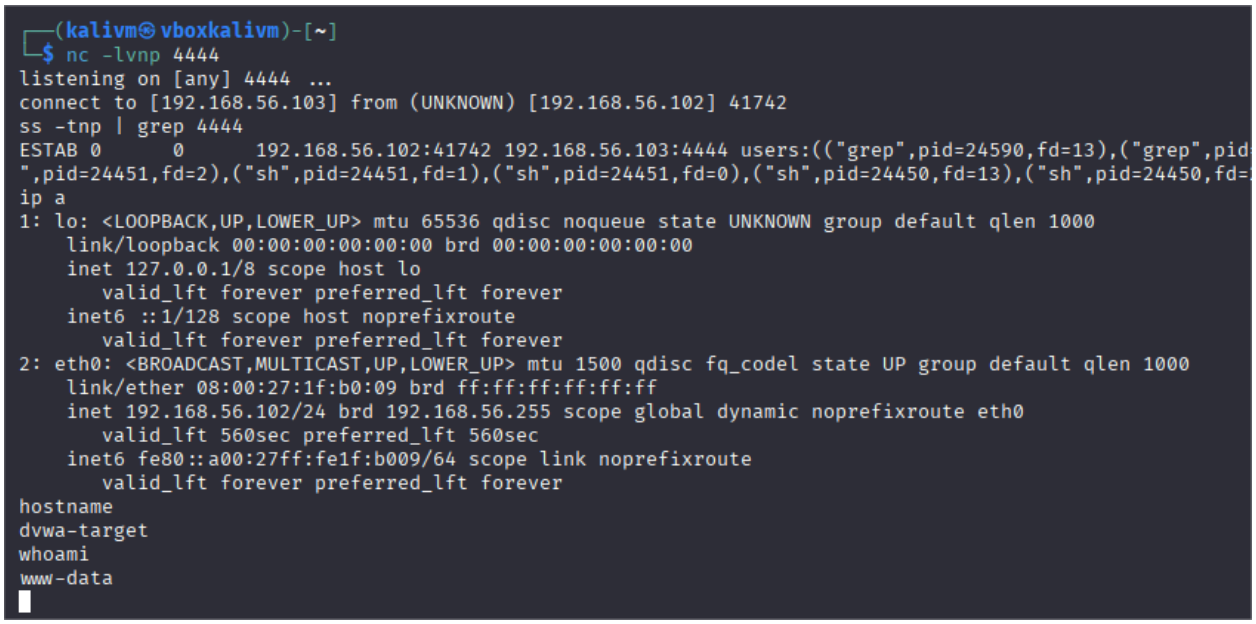
Ho quindi utilizzato il comando nc -lvnp 4444 per iniziare l'ascolto:



Subito dopo, sono andato nella pagina della Reverse Shell caricata in precedenza:



Questo procedimento, ci ha permesso di ottenere l'accesso remoto alla DVWA, potendo agire direttamente a livello del sistema. Ho utilizzato comandi come whoami, hostname e ip a per ottenere informazioni relative all'utente e comandi come ls e cd per spostarmi a livello delle directory.



Fase 5: Analisi e Intercettazione con Burp Suite

Ho configurato Firefox utilizzando il Proxy manuale verso l'ip di localhost 127.0.0.1, con la porta 8080, quindi ho aggiunto la stessa impostazione anche su Burp Suite e ho intercettato le richieste HTTP/HTTPS.

Durante le visite alla pagina sono emerse principalmente richieste GET:

Time	Type	Direction	Method	URL
00:00:48 6 mag 2025	HTTP	→ Request	GET	http://192.168.56.102/dvwa/hackable/uploads/reverseshell.php
00:01:29 6 mag 2025	HTTP	→ Request	GET	http://192.168.56.102/dvwa/hackable/uploads/reverseshell.php/cmd=ls

Nel dettaglio:

Request

Pretty Raw Hex

```
1  GET /dvwa/hackable/uploads/reverseshell.php/cmd=ls HTTP/1.1
2  Host: 192.168.56.102
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: keep-alive
8  Cookie: PHPSESSID=8b252a6a930d07e076d2d06fda85ab5b; security=low
9  Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
```

Conclusioni:

L'esercizio ha dimostrato come una cattiva gestione del caricamento file possa portare a una compromissione a livello anche di un accesso remoto. L'utilizzo combinato di Netcat e Burp Suite ha permesso di testare e documentare il comportamento della web app in ogni fase.