

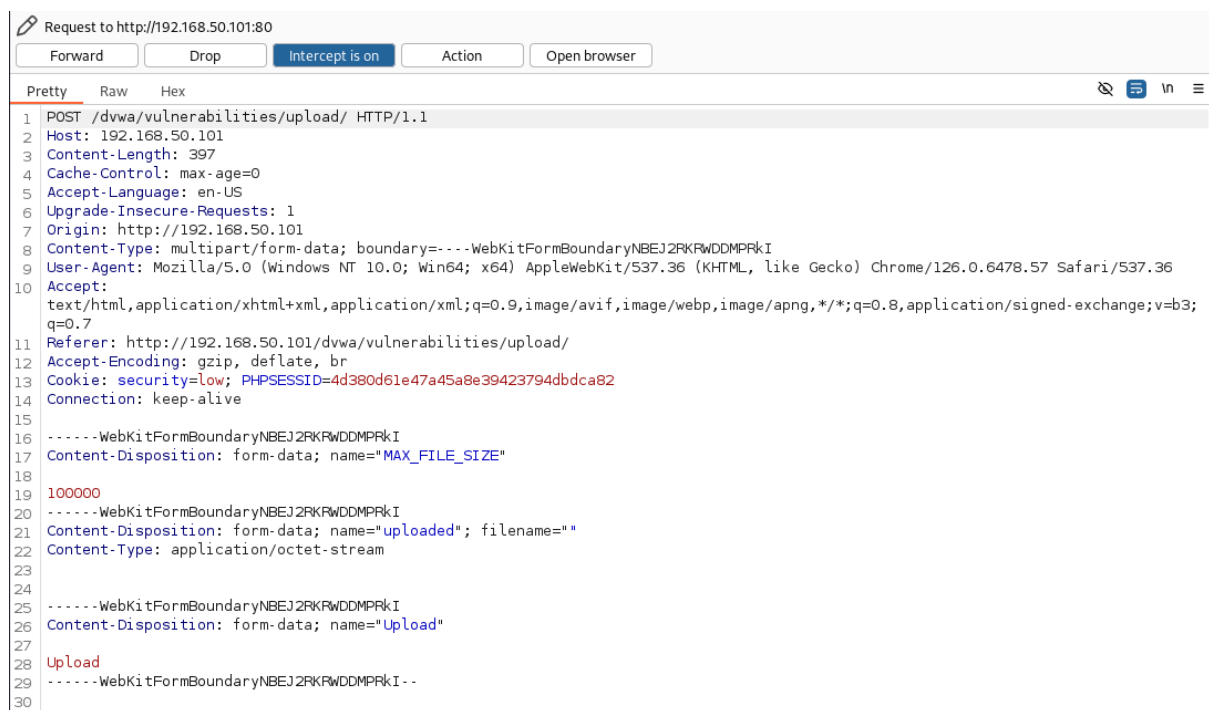
Upload shell.php su metasploitable

Verifico che le macchine si pinghino

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=10.0 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.000 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.000 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.000 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.000/2.500/10.000/4.330 ms
msfadmin@metasploitable:~$ _
```

Intercetto la richiesta POST quando vado a fare l'upload



```
Request to http://192.168.50.101:80
Forward Drop Intercept is on Action Open browser

Pretty Raw Hex
1 POST /dwva/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.50.101
8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryNBEJ2RKRWDDMPKkI
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 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
11 Referer: http://192.168.50.101/dwva/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=4d380d61e47a45a8e39423794dbdca82
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryNBEJ2RKRWDDMPKkI
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryNBEJ2RKRWDDMPKkI
21 Content-Disposition: form-data; name="uploaded"; filename="
22 Content-Type: application/octet-stream
23
24
25 -----WebKitFormBoundaryNBEJ2RKRWDDMPKkI
26 Content-Disposition: form-data; name="Upload"
27
28 Upload
29 -----WebKitFormBoundaryNBEJ2RKRWDDMPKkI--
30
```

Carico il mio codice per la shell.php

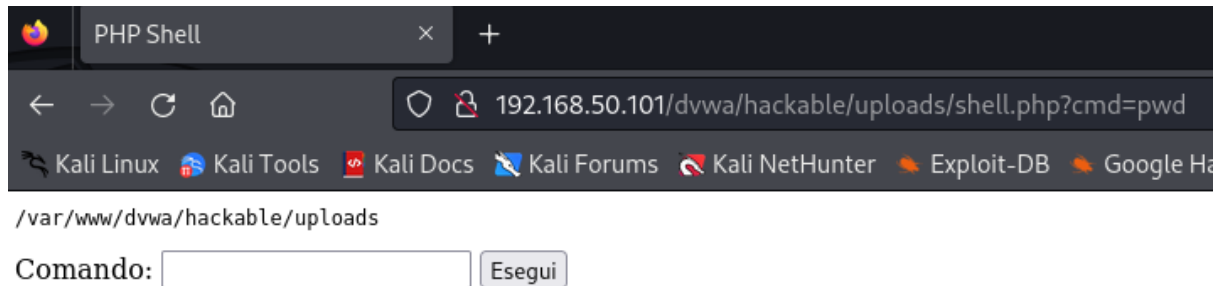
Vulnerability: File Upload

Choose an image to upload:

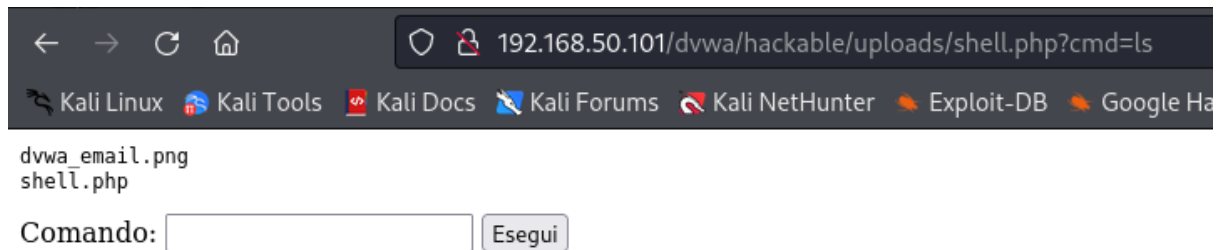
No file chosen

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

Mi connetto a quel path e immetto il comando “pwd”



Immetto il comando “ls”, posso sia scriverlo nell’ URL dopo il ?cmd che nel campo comando



ARP Spoofing

Durante l’attacco con arpspoof ho catturato il pacchetto HTTP con i campi di login tra Win7 e metasploitable utilizzando wireshark

No.	Time	Source	Destination	Protocol	Length	Info
50	302.665511746	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
51	339.994079103	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
52	339.994173648	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
53	341.995230029	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
54	341.995396311	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
55	343.997394441	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
56	343.997494329	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
57	346.002773295	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
58	346.002878536	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
59	346.119770745	192.168.50.102	192.168.50.101	HTTP	696	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
60	346.430080256	192.168.50.102	192.168.50.101	TCP	696	[TCP Retransmission] 49177 → 80 [PSH, ACK] Seq=1 Ack=1 Win=256 Le...
61	347.031561585	192.168.50.102	192.168.50.101	TCP	696	[TCP Retransmission] 49177 → 80 [PSH, ACK] Seq=1 Ack=1 Win=256 Le...
62	348.021290079	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
63	348.021389722	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6
64	348.236036933	192.168.50.102	192.168.50.101	TCP	592	[TCP Retransmission] 49177 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=536
65	349.438218008	192.168.50.102	192.168.50.101	TCP	592	[TCP Retransmission] 49177 → 80 [ACK] Seq=1 Ack=1 Win=256 Len=536
66	350.025055585	PCSSystemtec_1c:68:...		ARP	44	192.168.50.101 is at 08:00:27:1c:68:a6
67	350.025156566	PCSSystemtec_1c:68:...		ARP	44	192.168.50.102 is at 08:00:27:1c:68:a6

```
▶ Frame 59: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface 0
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.101
▶ Transmission Control Protocol, Src Port: 49177, Dst Port: 80,
▶ Hypertext Transfer Protocol
▶ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "username" = "admin"
  ▶ Form item: "password" = "password"
  ▶ Form item: "Login" = "Login"
```