【BugKu-CTF论坛writeup(杂项)】这么多数据包

原创

Kingyo12 于 2018-03-05 18:18:26 发布
分类专栏： BugKu-CTF论坛writeup(杂项)

这么多数据包找找吧，先找到getshell的流

下载下来是一个 

，里面有个pcap包。

wireshark打开可以发现真的有好多好多好多数据包。根据提示找getshell的流。（说实在的我对攻击主机这一块不是很了解，但是大体可以看出来数据包一开始是在扫描端口，后面的就不太清楚了）。以下是在朋友的指导下追踪到的TCP流（然而还是不是很懂，这里就不乱讲了以免误导了大家），找到之后可以发现在流里有一段BASE64编码。

Wireshark · 追踪 TCP 流 (tcp.stream eq 1735) · CTF

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B03C-791A

 Directory of C:\

04/14/2016  08:50 PM                 0 AUTOEXEC.BAT
04/14/2016  08:50 PM                 0 CONFIG.SYS

04/14/2016  08:52 PM    <DIR>          Documents and Settings
03/12/2012  10:24 PM            61,454 nc.exe
04/14/2016  08:54 PM    <DIR>          Program Files
04/14/2016  09:22 PM                36 s4cr4t.txt
04/14/2016  08:59 PM    <DIR>          WINDOWS
               4 File(s)         61,490 bytes
               3 Dir(s)  17,719,083,008 bytes free

C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"
```


在线解码可以得到CCTF{do_you_like_sniffer}