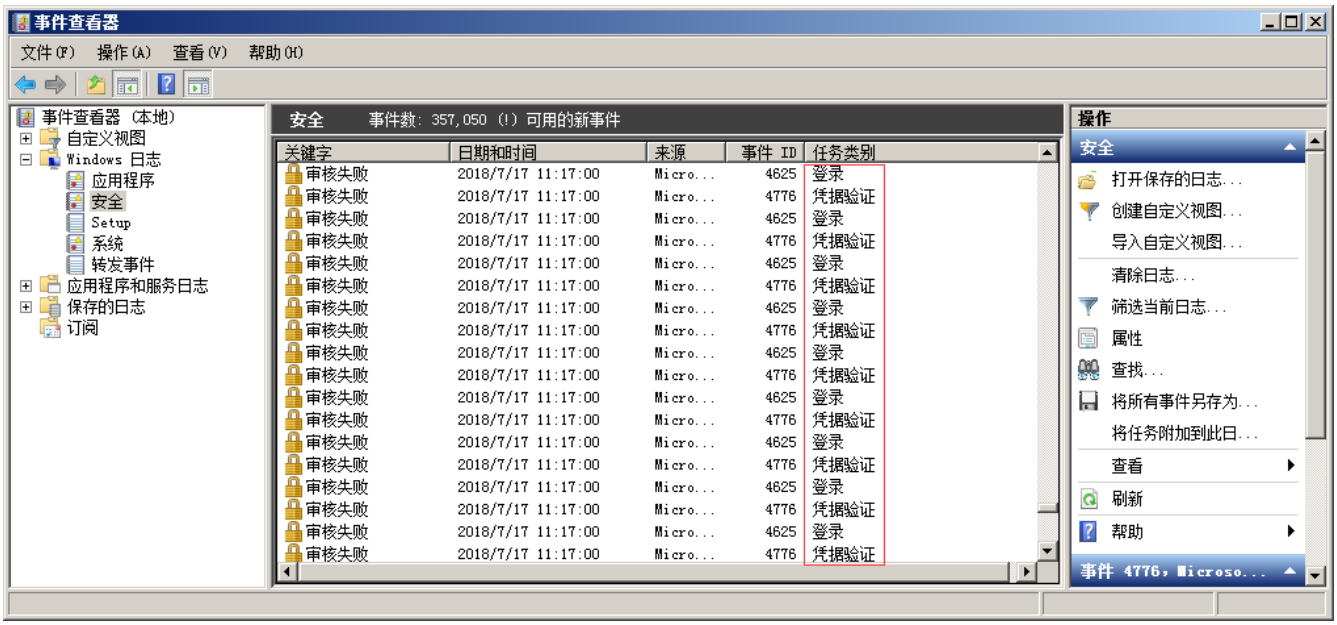
第1篇：FTP暴力破解

0x00 前言

FTP是一个文件传输协议，用户通过FTP可从客户机程序向远程主机上传或下载文件，常用于网站代码维护、日常源码备份等。如果攻击者通过FTP匿名访问或者弱口令获取FTP权限，可直接上传webshell，进一步渗透提权，直至控制整个网站服务器。

0x01 应急场景

从昨天开始，网站响应速度变得缓慢，网站服务器登录上去非常卡，重启服务器就能保证一段时间的正常访问，网站响应状态时而飞快时而缓慢，多数时间是缓慢的。针对网站服务器异常，系统日志和网站日志，是我们排查处理的重点。查看Window安全日志，发现大量的登录失败记录：

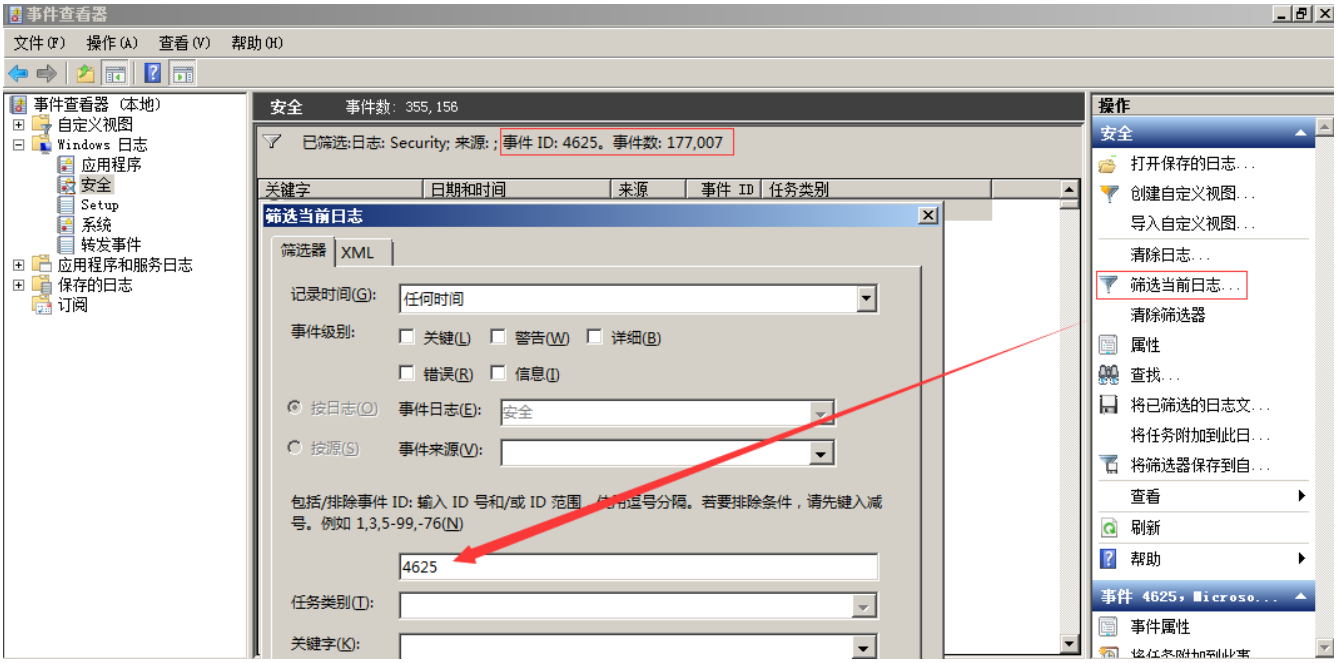


0x02 日志分析

安全日志分析：

安全日志记录着事件审计信息，包括用户验证（登录、远程访问等）和特定用户在认证后对系统做了什么。

打开安全日志，在右边点击筛选当前日志， 在事件ID填入4625，查询到事件ID4625，事件数177007，从这个数据可以看出，服务器正则遭受暴力破解：



进一步使用Log Parser对日志提取数据分析，发现攻击者使用了大量的用户名进行爆破，例如用户名：fxxx，共计进行了17826次口令尝试，攻击者基于“fxxx”这样一个域名信息，构造了一系列的用户名字典进行有针对性进行爆破，如下图：

```
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe  -i:EVT "SELECT  EXTRACT_TOK
EN(Message,13,' ')  as EventType,EXTRACT_TOKEN(Message,19,' ') as user,count(EXT
RACT_TOKEN(Message,19,' ')) as Times,EXTRACT_TOKEN(Message,38,' ') as Loginip FR
OM c:\Security.evtx  where EventID=4625 GROUP BY Message"
EventType user            Times Loginip
--------- --------------- ----- -------
8         f[illegible]    17826 -
8         f[illegible].gov.cn 2747  -
8         f[illegible]govcn 15362 -
8         www.f[illegible].gov.cn 9842  -
8         f[illegible]123 1350  -
8         f[illegible]888 1156  -
8         f[illegible]666 1156  -
8         f[illegible]123456 1155  -
8         f[illegible]-govcn 153   -
8         f[illegible]_govcn 152   -
Press a key...
EventType user                      Times Loginip
--------- ------------------------- ----- -------
8         govcn                     208   -
8         www-data                  2     -
8         admin@f[illegible].govcn  3022  -
8         f[illegible]@f[illegible].govcn 2592  -
8         administrator             893   -
8         f[illegible].govcn        1505  -
8         webmaster@f[illegible].govcn 3004  -
8         .f[illegible].govcn       1500  -
8         administrator@f[illegible].govcn 2566  -
8         administrators@f[illegible].govcn 2562  -
Press a key...
```

这里我们留意到登录类型为8，来了解一下登录类型8是什么意思呢？

登录类型8：网络明文（NetworkCleartext）

这种登录表明这是一个像类型3一样的网络登录，但是这种登录的密码在网络上是通过明文传输的，WindowsServer服务是不允许通过明文验证连接到共享文件夹或打印机的，据我所知只有当从一个使用Advapi的ASP脚本登录或者一个用户使用基本验证方式登录IIS才会是这种登录类型。“登录过程”栏都将列出Advapi。

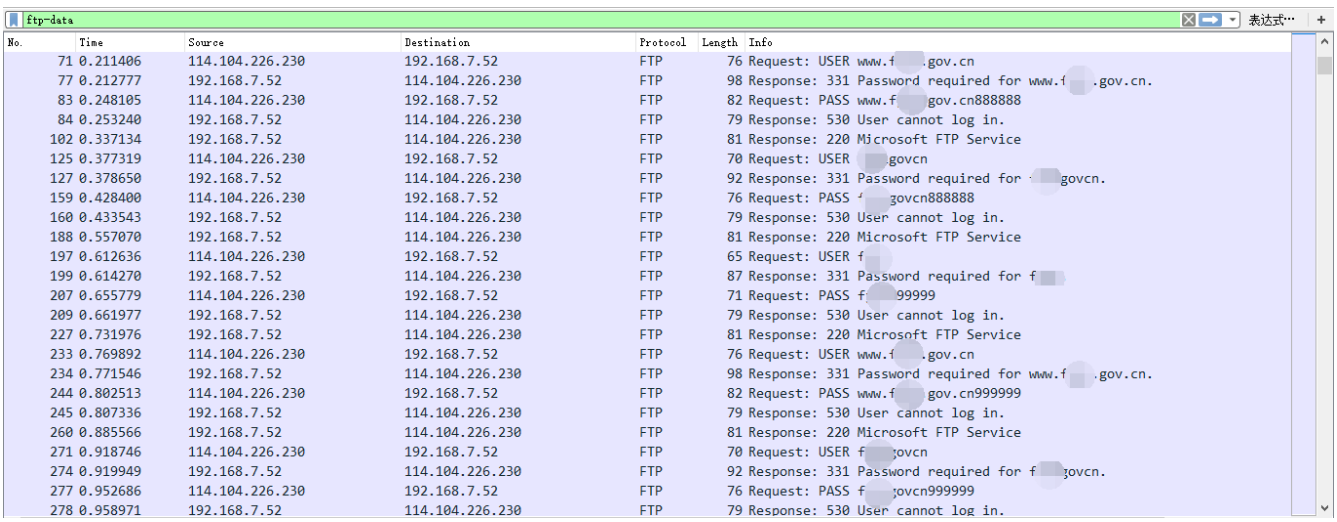
我们推测可能是FTP服务，通过查看端口服务及管理员访谈，确认服务器确实对公网开放了FTP服务。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       1068
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING       1640
  TCP    0.0.0.0:2383           0.0.0.0:0              LISTENING       1708
  TCP    0.0.0.0:2809           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1740
  TCP    0.0.0.0:8880           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9043           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9060           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9080           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9100           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9402           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9403           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:9443           0.0.0.0:0              LISTENING       2924
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       380
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       740
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       484
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       784
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       476
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       1816
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       1640
  TCP    127.0.0.1:9633         0.0.0.0:0              LISTENING       2924
  TCP    127.0.0.1:49163        127.0.0.1:49164        ESTABLISHED     2924
  TCP    127.0.0.1:49164        127.0.0.1:49163        ESTABLISHED     2924
  TCP    192.168.204.162:139    0.0.0.0:0              LISTENING       4
```

另外，日志并未记录暴力破解的IP地址，我们可以使用Wireshark对捕获到的流量进行分析，获取到正在进行爆破的IP：



ftp-data

No.	Time	Source	Destination	Protocol	Length	Info
71	0.211406	114.104.226.230	192.168.7.52	FTP	76	Request: USER www.f .gov.cn
77	0.212777	192.168.7.52	114.104.226.230	FTP	98	Response: 331 Password required for www.f .gov.cn.
83	0.248105	114.104.226.230	192.168.7.52	FTP	82	Request: PASS www.f gov.cn888888
84	0.253240	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
102	0.337134	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
125	0.377319	114.104.226.230	192.168.7.52	FTP	70	Request: USER govcn
127	0.378650	192.168.7.52	114.104.226.230	FTP	92	Response: 331 Password required for govcn.
159	0.428400	114.104.226.230	192.168.7.52	FTP	76	Request: PASS govcn888888
160	0.433543	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
188	0.557070	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
197	0.612636	114.104.226.230	192.168.7.52	FTP	65	Request: USER f
199	0.614270	192.168.7.52	114.104.226.230	FTP	87	Response: 331 Password required for f
207	0.655779	114.104.226.230	192.168.7.52	FTP	71	Request: PASS f 99999
209	0.661977	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
227	0.731976	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
233	0.769892	114.104.226.230	192.168.7.52	FTP	76	Request: USER www.f .gov.cn
234	0.771546	192.168.7.52	114.104.226.230	FTP	98	Response: 331 Password required for www.f .gov.cn.
244	0.802513	114.104.226.230	192.168.7.52	FTP	82	Request: PASS www.f gov.cn999999
245	0.807336	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.
260	0.885566	192.168.7.52	114.104.226.230	FTP	81	Response: 220 Microsoft FTP Service
271	0.918746	114.104.226.230	192.168.7.52	FTP	70	Request: USER f govcn
274	0.919949	192.168.7.52	114.104.226.230	FTP	92	Response: 331 Password required for f govcn.
277	0.952686	114.104.226.230	192.168.7.52	FTP	76	Request: PASS f govcn999999
278	0.958971	192.168.7.52	114.104.226.230	FTP	79	Response: 530 User cannot log in.

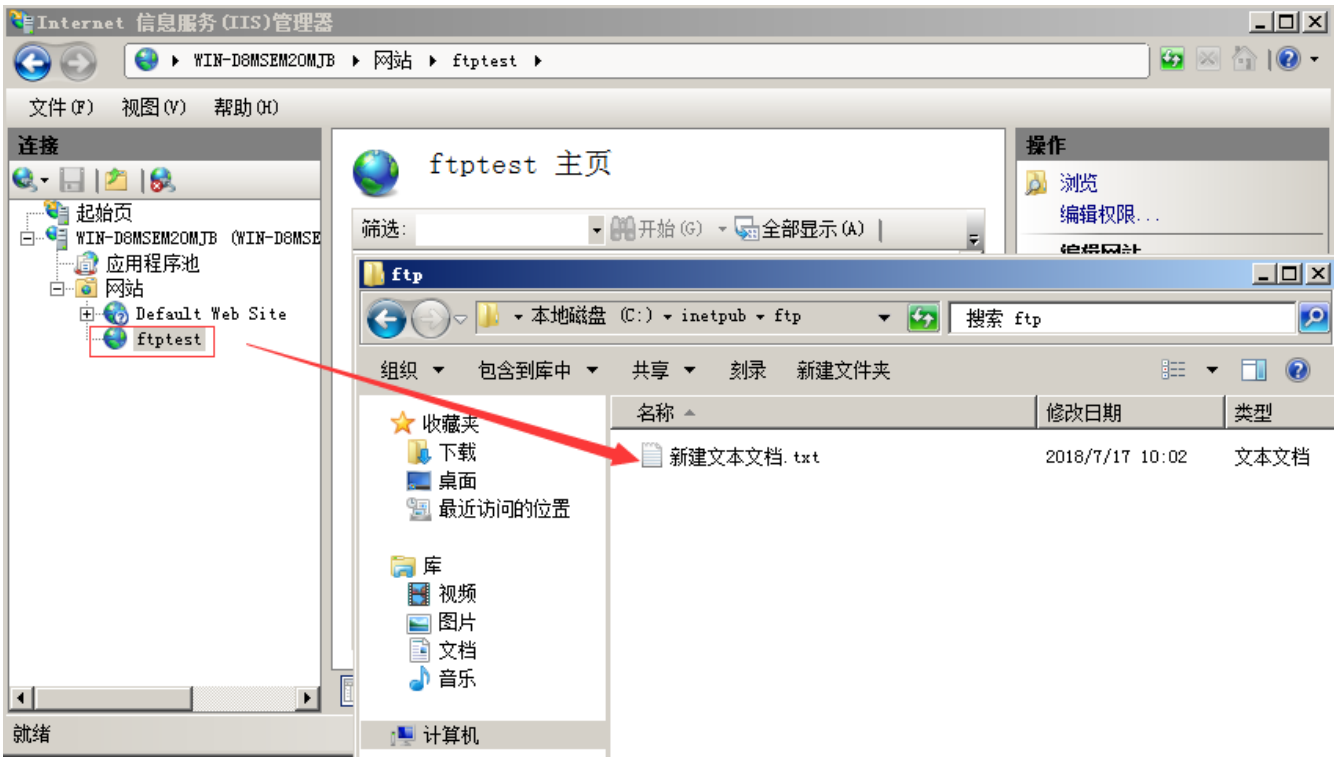
通过对近段时间的管理员登录日志进行分析，如下：

```
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe -i:EVT  "SELECT EXTRACT_TOKE
N(Message,13,' ') as EventType,TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,
5,'|') as Username,EXTRACT_TOKEN(Message,38,' ') as Loginip FROM c:\Security.evt
x where EventID=4624 and EXTRACT_TOKEN(Message,13,' ')='10'"
EventType LoginTime           Username Loginip
--------- ------------------- -------- -----------
10        2018-07-05 07:26:00 [redacted] admin 192.168.6.5
10        2018-07-05 07:34:40 [redacted] admin 192.168.6.5
10        2018-07-05 07:35:07 [redacted] admin 192.168.6.5
10        2018-07-05 07:48:52 [redacted] admin 192.168.6.5
10        2018-07-05 08:29:02 [redacted] admin 192.168.6.5
10        2018-07-05 08:35:21 [redacted] admin 192.168.6.5
10        2018-07-05 09:55:24 [redacted] admin 192.168.6.5
10        2018-07-05 10:53:36 [redacted] admin 192.168.6.5
10        2018-07-05 10:58:20 [redacted] admin 192.168.6.5
10        2018-07-05 15:07:45 [redacted] admin 192.168.6.5
Press a key...
EventType LoginTime           Username Loginip
--------- ------------------- -------- -----------
10        2018-07-05 15:18:33 [redacted] admin 192.168.6.5

Statistics:
-----------
Elements processed: 355852
Elements output:    11
Execution time:     29.14 seconds
```

管理员登录正常，并未发现异常登录时间和异常登录ip，这里的登录类型10，代表远程管理桌面登录。

另外，通过查看FTP站点，发现只有一个测试文件，与站点目录并不在同一个目录下面，进一步验证了FTP暴力破解并未成功。



应急处理措施：1、关闭外网FTP端口映射 2、删除本地服务器FTP测试

0x04 处理措施

FTP暴力破解依然十分普遍，如何保护服务器不受暴力破解攻击，总结了几种措施：

1、禁止使用FTP传输文件，若必须开放应限定管理IP地址并加强口令安全审计（口令长度不低于8位，由数字、大小写字母、特殊字符等至少两种以上组合构成）。
2、更改服务器FTP默认端口。
3、部署入侵检测设备，增强安全防护。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复"应急响应" 即可下载。