0x01 背景介绍

金融行业的攻防演练早已过了简单扫描通过1/Nday漏洞可以直接突破边界的时期，社工和供应链攻击成了攻击常态。

本文介绍某一次演练项目，通过供应链+社工的组合攻击，绕过安全设备防护，打穿目标的案例。

0x02 突破路径

1、伪造登录页钓鱼获取账号密码

2、登录系统后台文件上传getshell（云服务器）

3、登录页水坑攻击获取办公pc权限（dns上线cs）

4、对抗绕过安全厂商ac设备防护，转http上线cs

5、内网横向打下域控

0x03 突破详情

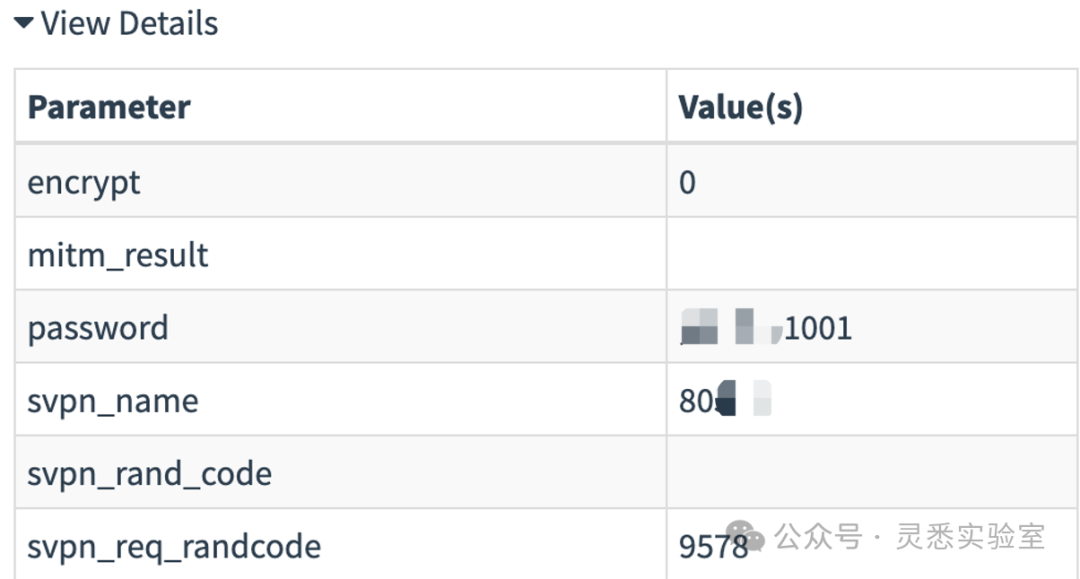
经过简单的扫描踩点，发现该单位暴露面小，且系统都为自主研发，没有发现边界突破的入口点。并且边界存在waf防护，没有0day漏洞的情况下举步维艰。

针对收集到的web资产逐一分析，发现带有该单位logo的电子学习平台，但是资产在云上，不属于客户it资产。在没有找到其他登录口的情况下，只能以此为突破口进行尝试。

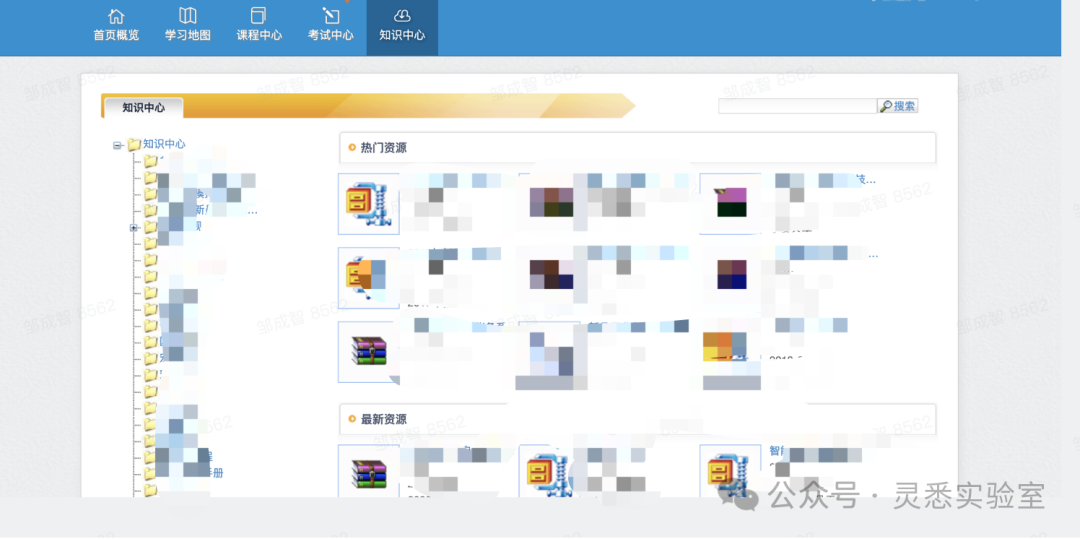
制作钓鱼页面，使用EmailAll收集目标邮箱，并批量发送100封钓鱼邮件。



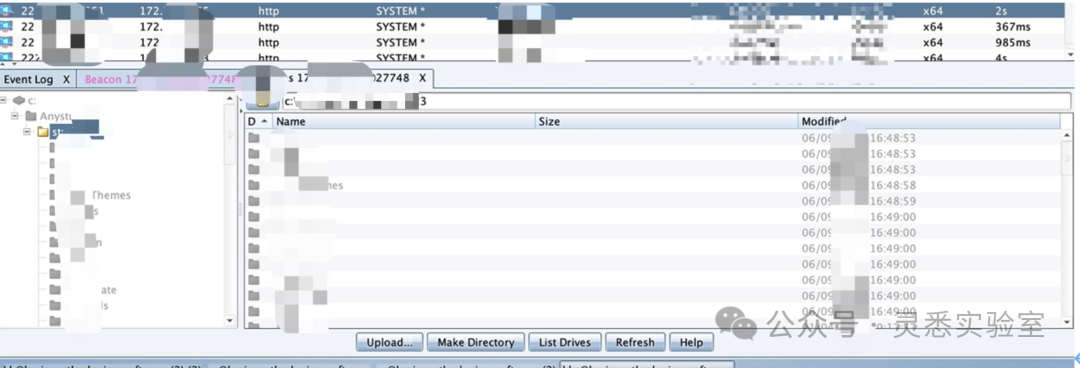
经过了一晚上的等待，运气不错，终于等到了一人提交



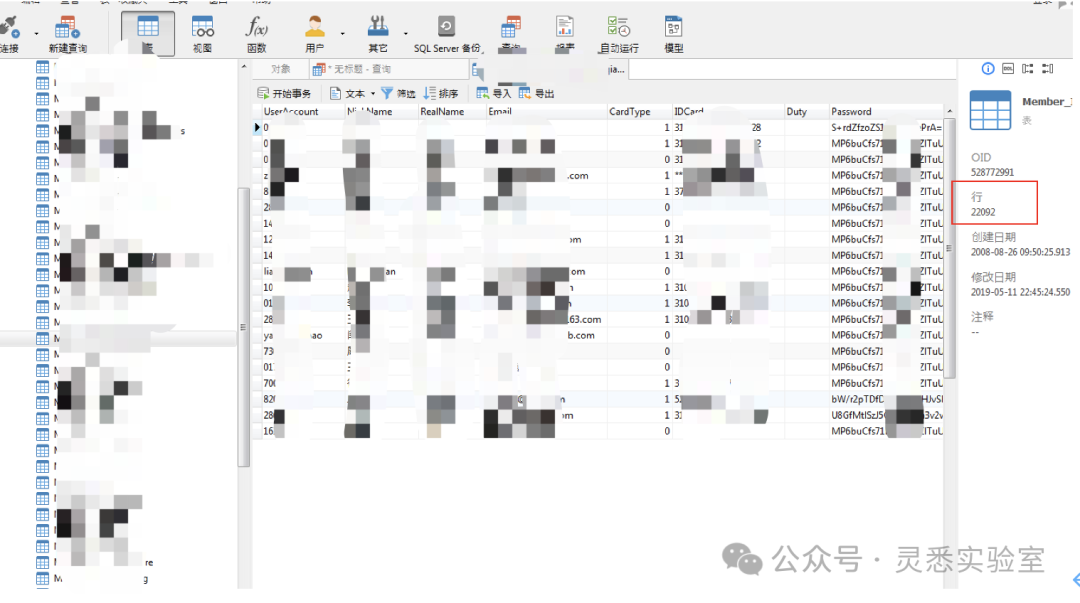
成功登录



文件上传漏洞getshell，并通过cs上线。由于是一台云服务器，与实际内网不通，所以想着只能刷一些数据分。



找到数据库配置文件，发现超2w+条该单位员工信息



基于上述信息可以得到该平台为第三方供应商提供的在线电子学习平台，所有员工会定期登录平台进行学习。加上我们基本获取了该单位所有员工的信息，可以进一步进行精准打击。

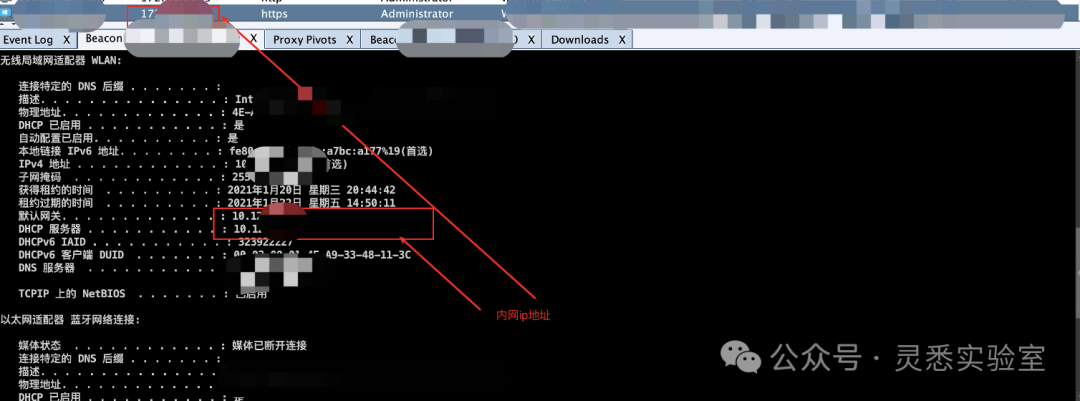
所以下一步的思路：登录页面水坑攻击打个人办公pc进办公网！！

和裁判报备通过，水坑攻击走起！制作flash水坑，嵌入到网页。



将运维人员邮箱筛选出来进行鱼叉攻击，发送邮件告知其需要登录学习网站修改密码。如果点了“立即升级”并运行，电脑就立即上线。这里遇到一个问题，很多金融单位会限制办公电脑上网，但是一般只会限制http，而很容易把dns给忽略，所以走cs dns上线可以尽量多的上线目标。

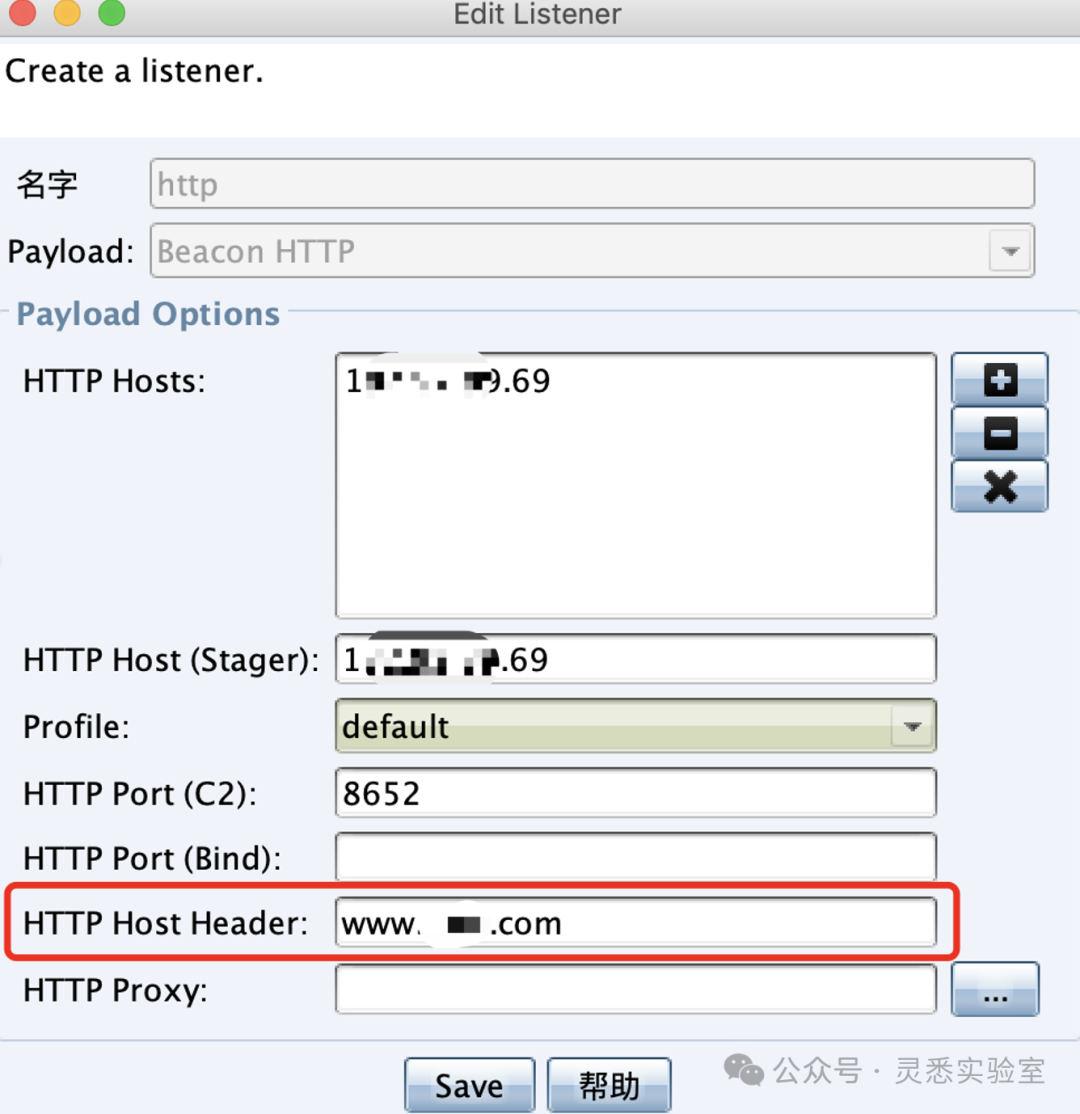
很快，上线了一台pc，成功进入办公网



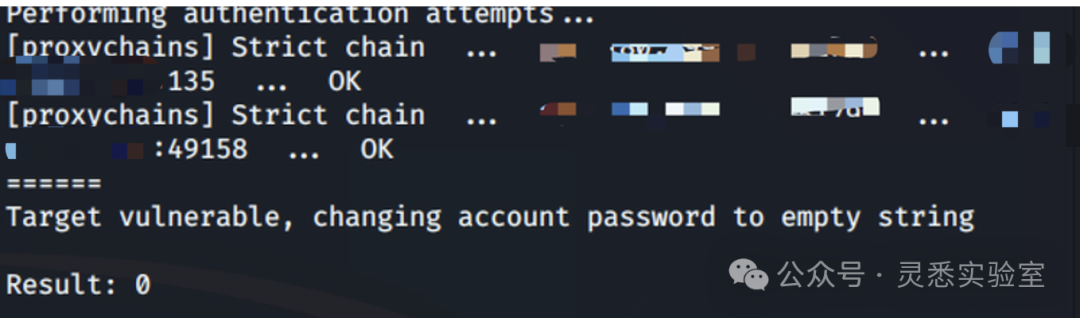
如果试过dns协议进行cs操作，延迟是非常之高的，正常的执行一条命令可能要等待1分钟，内网横向在这样的时间成本下基本冲不动。尝试上线http listener，但是失败了。。。

简单的信息收集后，发现使用了某安全厂商的ac上网设备，pc终端输入账号密码通过ac认证后可以访问互联网，而限制用户能否访问目标网站，一般都是通过配置http host头白名单来实现。

试了下公司官网，http可以正常访问，所以cs listener中配置host为公司官网域名，成功http上线。



接下来就是愉快的内网横向，扫到域控，与裁判报备后，使用CVE-2020-1472获取域控权限。



至此结束。

0x04 复盘总结

1、员工安全意识薄弱

2、供应商系统未定期进行安全测试

3、内网系统普遍防护薄弱，未加固

4、安全设备未更新至最新，导致被绕过