实验三：MS08-067 的漏洞渗透攻击

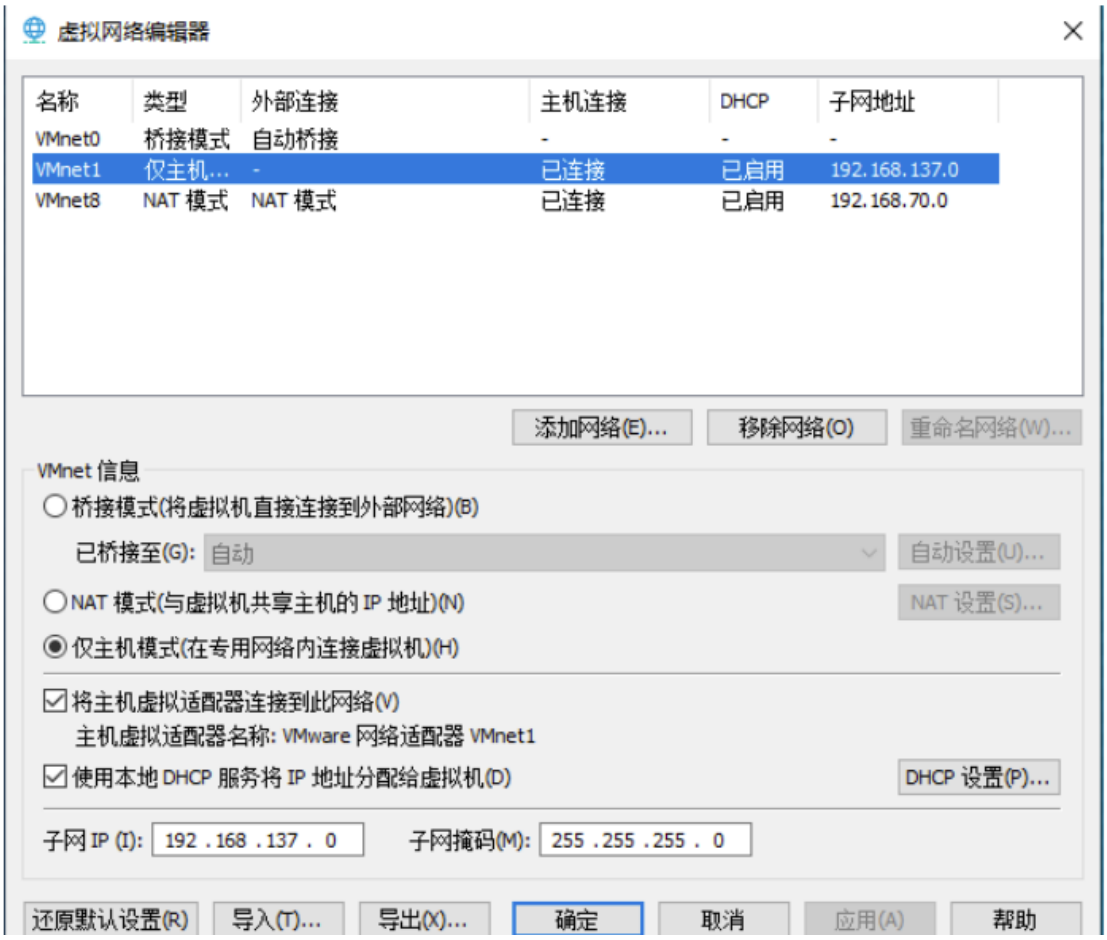
2152701-陈玟桦

一、 实验过程

本次实验通过 kali linux 中的 nmap、Metasploit 等渗透测试软件进行 MS08- 067 漏洞的扫描和攻击

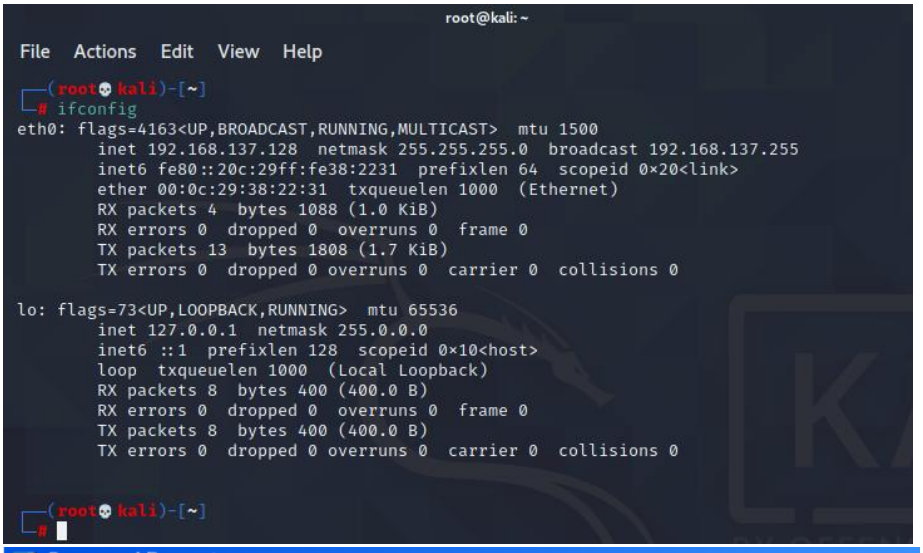
1.1 网络环境配置

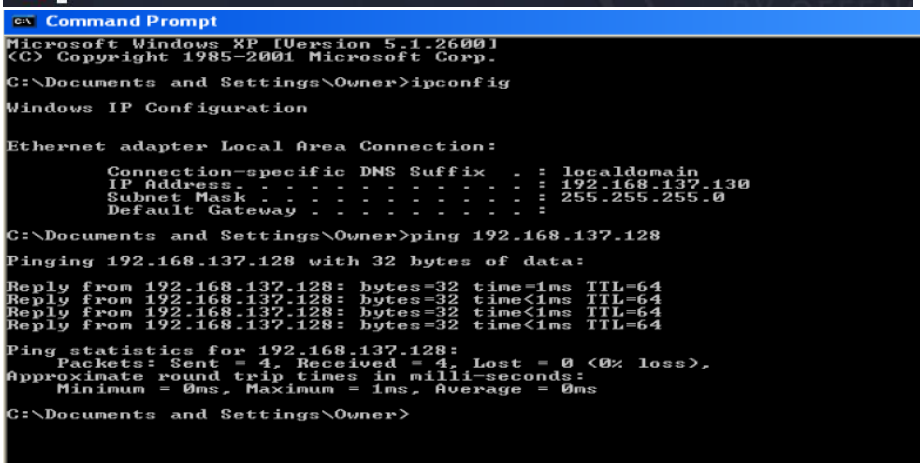
开启主机 win10 的 VMnet1 网卡，调整 VMware 的虚拟网络编辑器的子网 IP，并将 kali 和靶机英文版 Windows XP 的网络适配器均设置为仅主机模式。



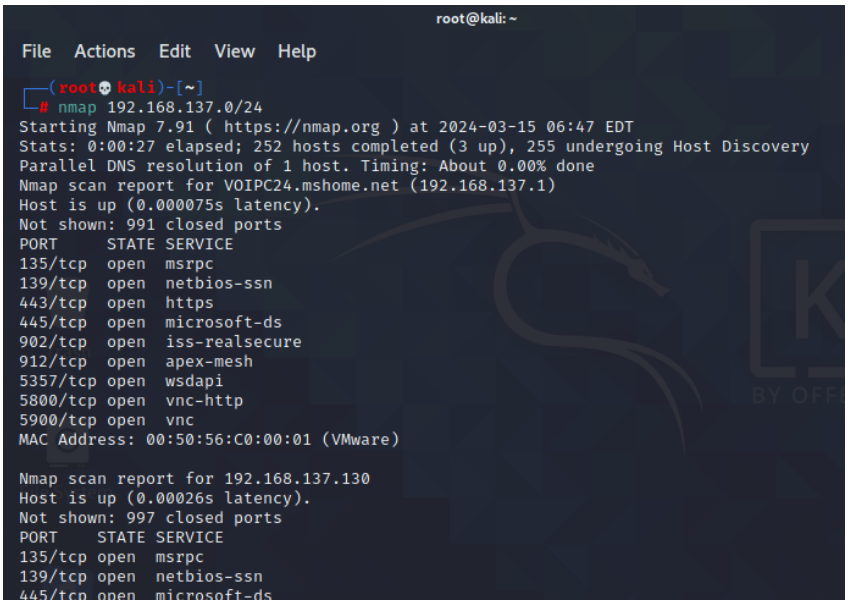
1.2 MS08-067 漏洞检测

分别在 kali 和 Windows XP 运行命令，查看攻击机和靶机的 IP





使用 nmap 检查攻击机和靶机所在网段是否有主机存活以及那些主机打开了 445 端口，445 端口开放是进行攻击的必要条件



192.168.137.1 以及 192.168.137.130 都打开了 445 端口，再用 nmap 的-o 命令查看一下目标主机操作系统的信息

```
┌──(root💀kali)-[~]
└─# nmap -sS -O 192.168.137.130
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-15 06:55 EDT
Nmap scan report for 192.168.137.130
Host is up (0.00043s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:B8:FC:72 (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 15.33 seconds
```

结论是 137.129 主机的操作系统是 Windows XP 2003 版本，这个版本的 MS08-067 漏洞未修复，进一步查看其具体信息：

```
File  Actions  Edit  View  Help

Host is up (0.00029s latency).
Not shown: 997 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
MAC Address: 00:0C:29:B8:FC:72 (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: -3h59m59s, deviation: 5h39m23s, median: -7h59m59s
|_nbstat: NetBIOS name: NET317-C7E3ADA8, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b8:fc:72 (VM
ware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: net317-c7e3ada8
|   NetBIOS computer name: NET317-C7E3ADA8\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-03-15T18:58:46+08:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

使用 nmap 的-A 命令可以获得 129 主机操作系统的具体类别，计算机名和创建时 期，开放端口等 使用 nmap 检查 129 主机是否真的存在 MS08-067 漏洞

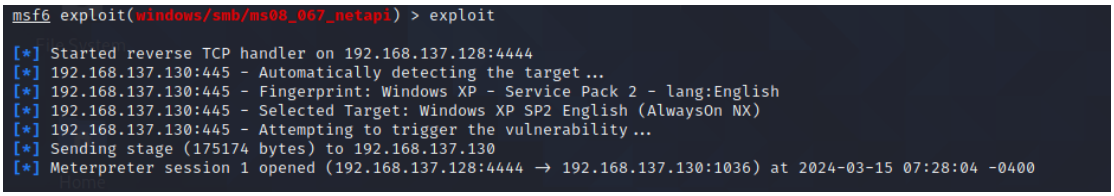
```
root@kali: ~
File  Actions  Edit  View  Help
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:DB:D5:D8 (VMware)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP
2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbit
rary
|           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
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 14.39 seconds

┌──(root💀kali)-[~]
└─#
```

返回的结果是该主机确实存在此漏洞，接下来可以进行进一步攻击

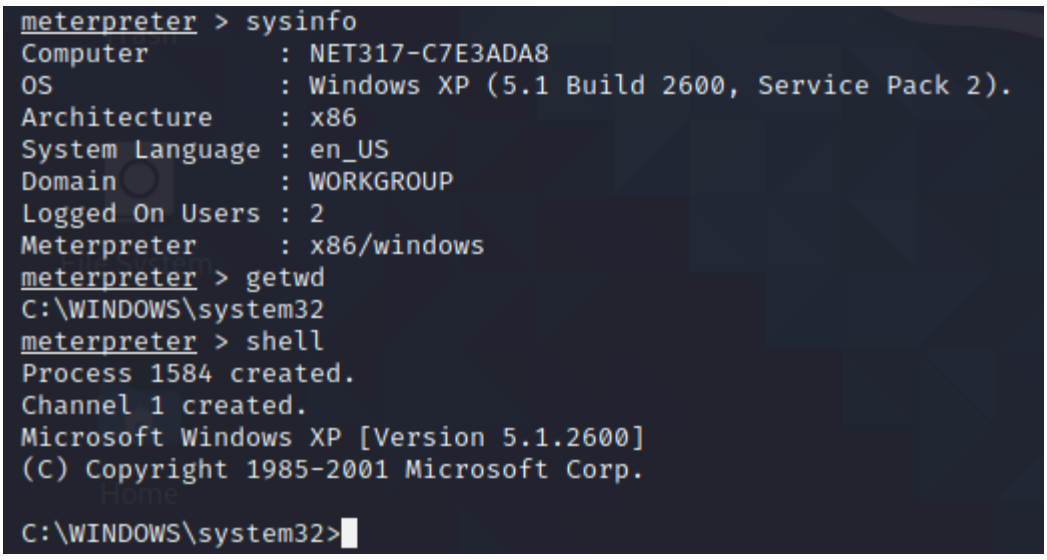
1.3 渗透测试

启动渗透软件 msf 终端

调整完参数，输入 exploit 开始渗透

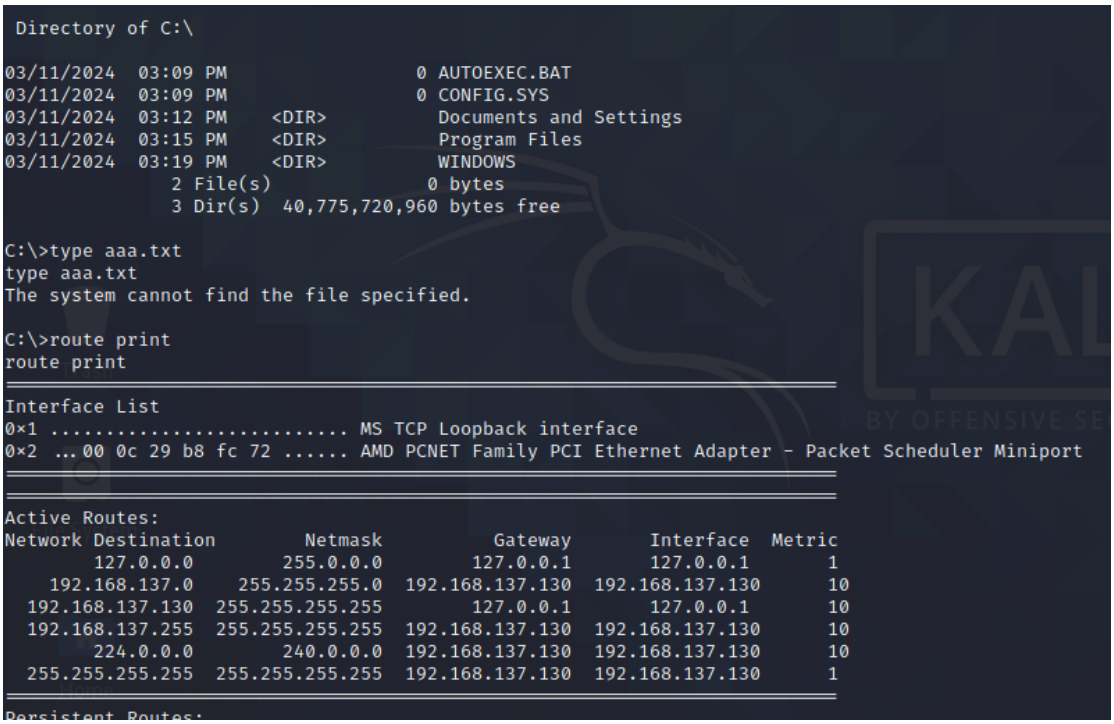


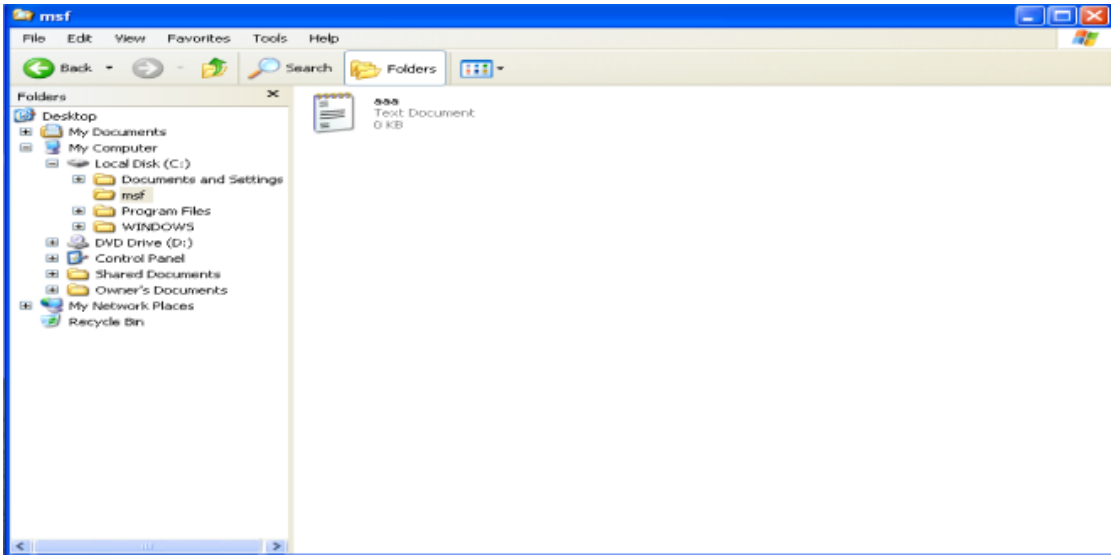
Meterpreter 能启用对目标的深度渗透，输入命令 sysinfo，得到靶机的操作系 统信息，getwd 查看当前目录，shell 启用靶机的命令行，这样就可以在攻击机 上像在本地一样操作靶机的命令行了

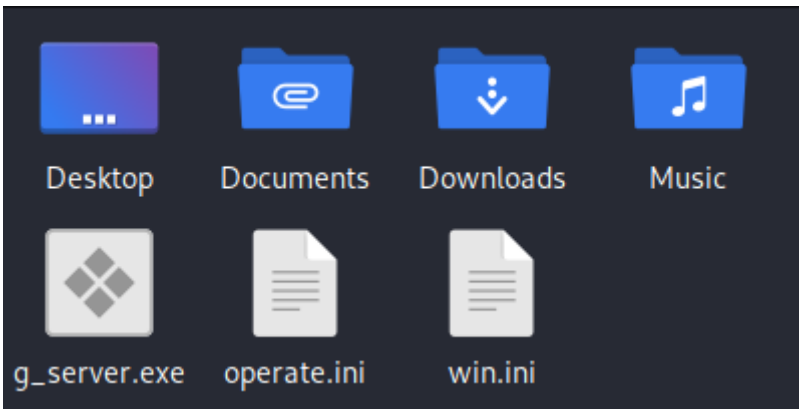


只要能操作靶机的命令行，就可以像在本地一样操作靶机文件，此处演示了在攻

击机上可以查询靶机文件，将靶机中的文件下载到攻击机内，也可以将攻击机中的文件上传到靶机。







二、心得体会

先要知道如何攻，才能知道如何守，要做好网络安全工程师，必须学会渗透软件的使用和渗透的逻辑，并多加实践。此外，系统的更新和维护是很重要的，要养成开启防火墙和及时更新系统的好习惯，加强安全意识