第7章 Windows攻防技术实践验收

* 用到的主机：

| **主机** | **IP** |
| --- | --- |
| kali（攻击机） | 192.168.200.4 |
| Win2KServer（靶机） | 192.168.200.124 |

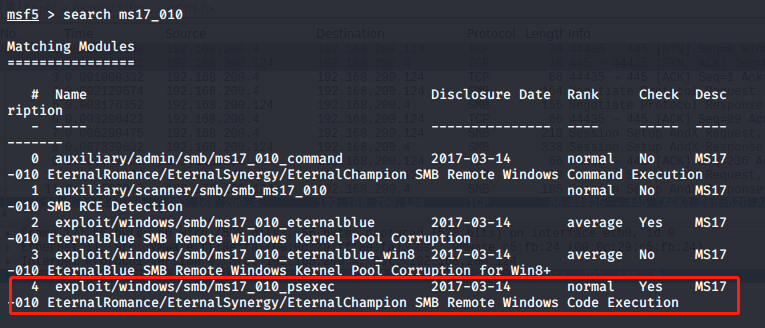
注：该攻击必须保证双方在同一网段，且可以ping通。

任务一：攻击方使用windows Attacker/BT4攻击机尝试对windows Metasploitable靶机上的漏洞进行远程渗透攻击，获取目标主机的访问权（要求漏洞必修是2015-2020年之间的漏洞）

实践过程：

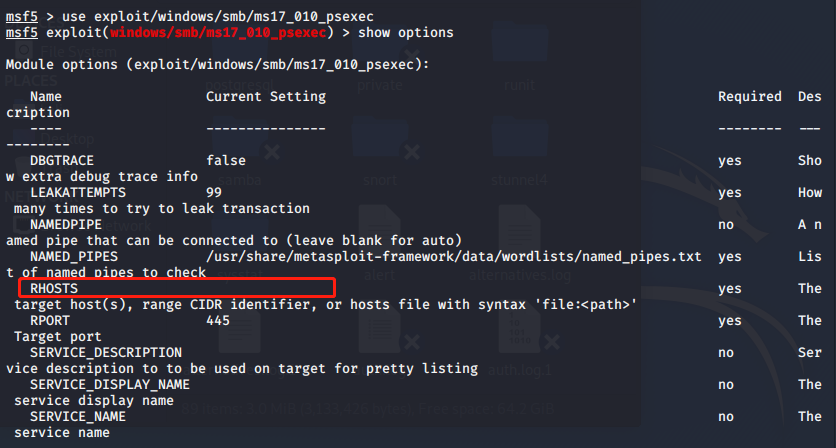
1. 搜索到17年的永恒之蓝漏洞，于是决定利用该漏洞进行攻击。首先在kali中输入msfconsole启动kali里面的msfconsole；
2. 选择渗透攻击模块

（1）输入search ms17\_010查看该漏洞的详细信息，如图：



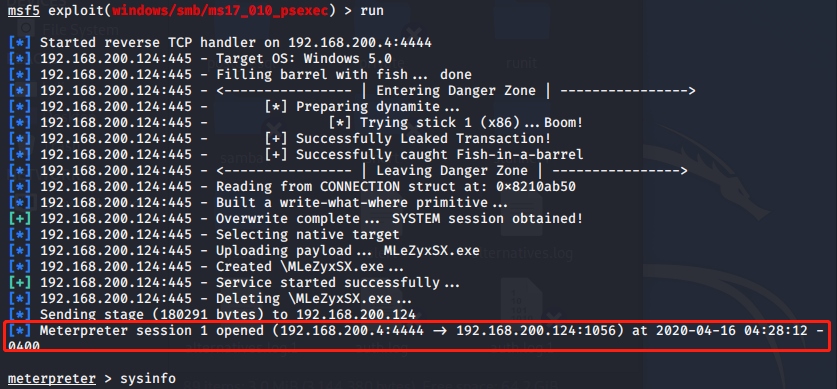
（2）这里我调用最后一个模块，因为它是最新的，尝试一下，执行命令use windows/smb/ms17\_010\_psexec。

1. 配置参数
2. 使用show options 查看需要设置的参数，如图，可见需要配置靶机IP：



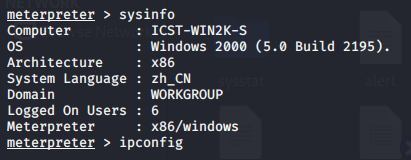
1. 输入set RHOST 192.168.200.124设置靶机为win2k，再show options确认配置成功。
2. 开始渗透攻击

执行命令run开始攻击，也可执行exploit。如图：



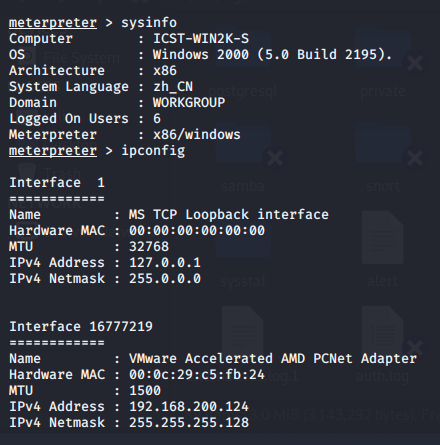
攻击成功。

1. 测试
2. 输入sysinfo 查看靶机系统信息，如图：



可以轻松获得靶机的计算机名称、操作系统、语言等信息。

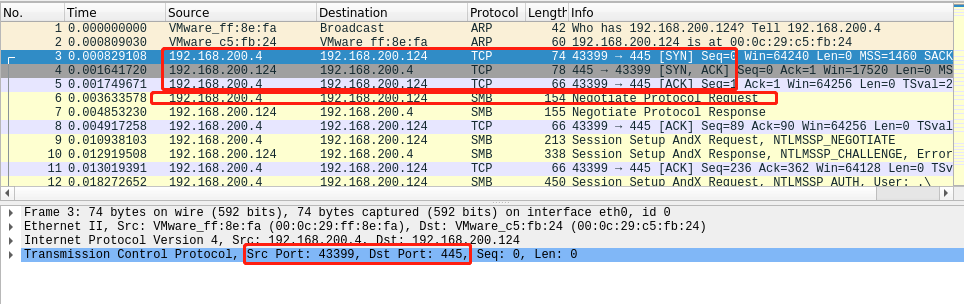
1. 输入ipconfig 查看靶机IP，验证攻击成功。如图：



任务二：防守方使用wireshark监听获得网络攻击的数据包，结合分析过程，获得攻击者IP地址、目的IP地址和端口、攻击发起时间、攻击利用漏洞、攻击使用的shellcode，以及本地执行的命令输入信息。

实践过程：

1. wireshark打开上面攻击抓到的数据包，大致扫描一下，发现大量SMB数据包，猜测是针对SMB服务发起的攻击。
2. 查看刚开始建立的TCP三次握手（攻击机先和靶机提出连接请求），也可通过SMP的请求包的源地址、目的地址等获得攻击者IP地址、目的IP地址和端口。如图：

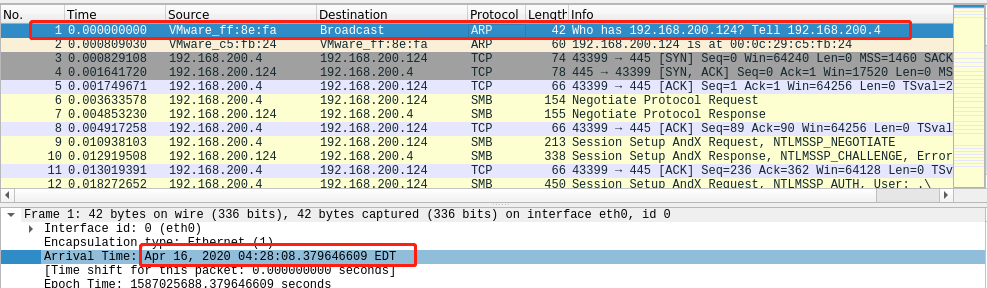


分析得到:

攻击者IP地址:192.168.200.4 攻击机端口：43399

靶机IP地址:192.168.200.4 靶机端口：445

1. 从第一个ARP解析MAC地址开始，表示试图建立连接发起攻击，所以攻击发起时间为美国东部夏令时间2020.4.16 04:28:08.380475717 EDT。如图：



1. 数据包中有大量SMB数据包，而资料查到MS17\_010就是针对该服务的漏洞，且靶机出现蓝屏，于是断定攻击者使用的漏洞是MS17\_010。
2. 追踪含[PSH],即有数据传输的数据流可查看本地执行的命令输入信息。如图3个tcp包为攻击机在本地执行命令的包，但是传输数据有点看不懂，可能是经过了某种加密吧。

