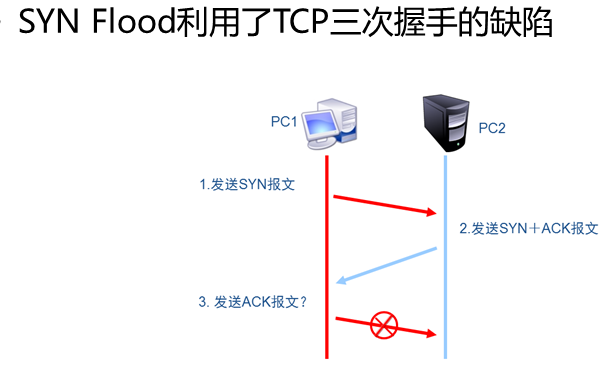
**DOS攻击（占用CPU、内存资源）**

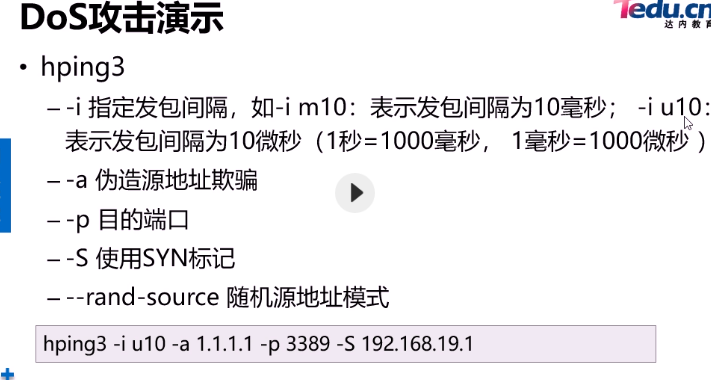
概述：DOS（拒绝服务）全称为denial of service，指的是无论通过哪种方式，最终导致目标系统崩溃、失去响应，从而无法正常提供服务或资源访问的情况

常见的是洪水方式，如SYN Flood 、PING flood（死亡之ping）

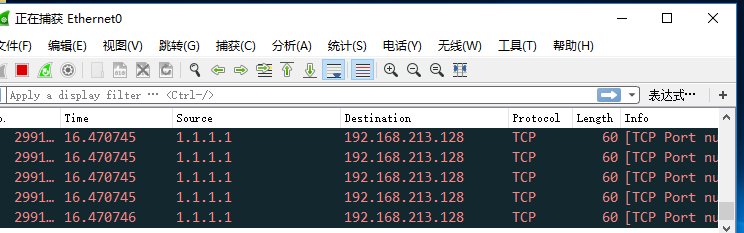
Ping flood通过向目标发送大量大数据包，导致对方网络堵塞、带宽耗尽，从而无法提供正常服务。Ping xxxx –l 65500



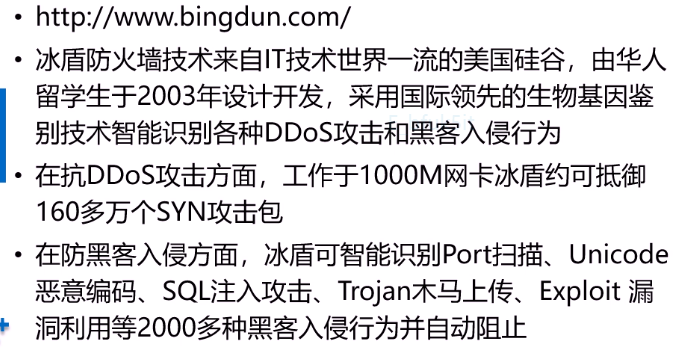
假设一个用户向服务器发送了SYN报文后突然死机或者掉线，那么服务器在发出SYN+ACK应答报文后是无法接受到客户端的ACK报文的，这种情况下服务器端一般会重试，发送确认信息，大概等（0.5-2分钟）后丢弃未完成连接。如果黑客大量模拟这种情况，发送大量伪造源IP地址的SYN，服务器每收到一个SYN就要给这个连接分配内存，如果短时间内接受到的SYN太多，这段连接的内存（半连接队列）就会占满，这样正常用户发送的SYN请求连接也会被服务器丢弃。







冰盾防火墙防范DOS攻击



**DDOS攻击**

概述：威力更大的DOS攻击，寄分布式拒绝服务，这种方式的攻击方不再是一台主机，数量上呈现规模化，可能是分布在不同网络、不同位置的成千上万的主机（通常称为僵尸网络）被发起者所控制

DDOS攻击的发起或防御，都有较大的难度。



**漏洞利用**

概述：

使用专门的漏洞攻击程序，利用操作系统、应用软件中的漏洞，可攻击或入侵系统

Kali中的metasploit framework(攻击框架)

漏洞攻击：

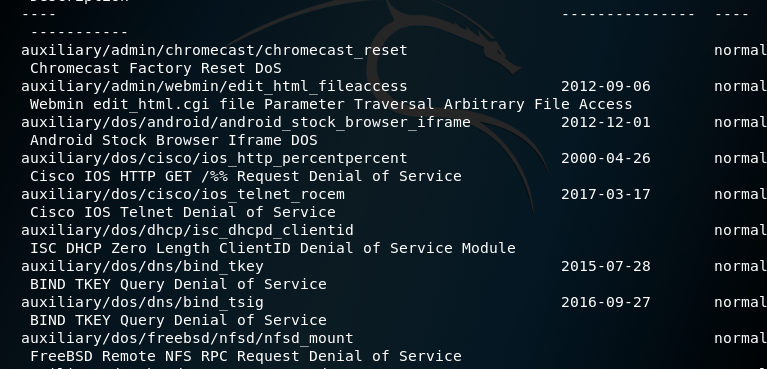
启动：msfconsole



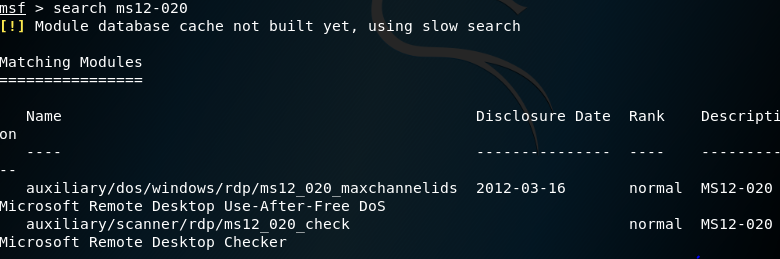


扫描漏洞：search dos





扫描指定漏洞：search ms12-020



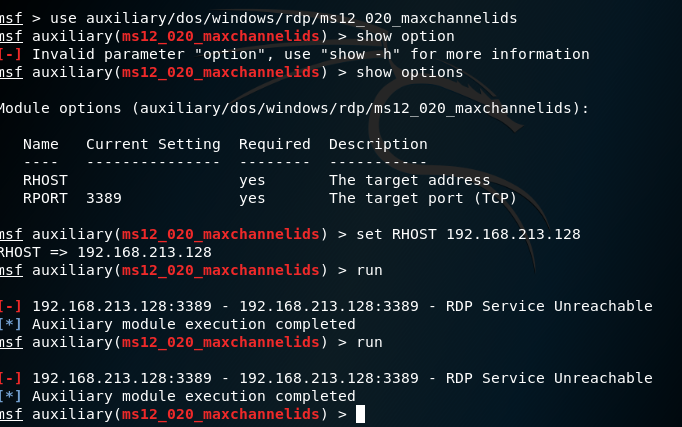
使用和运行

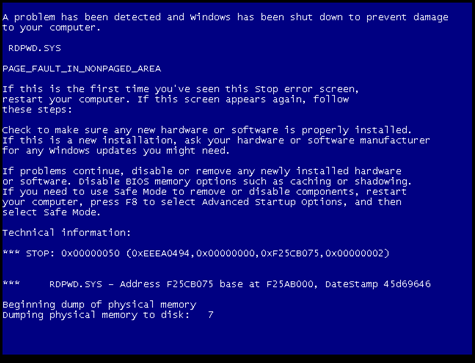
Use

Show optins

Set rhost IP地址

run





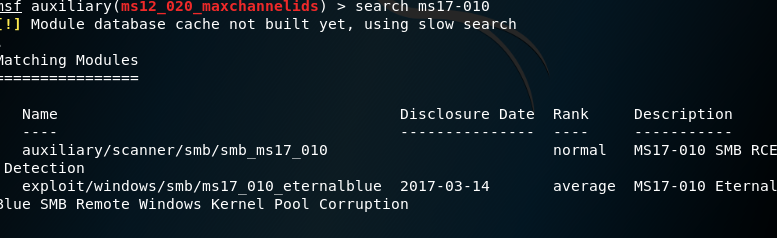
Systeminfo windows查看补丁状况



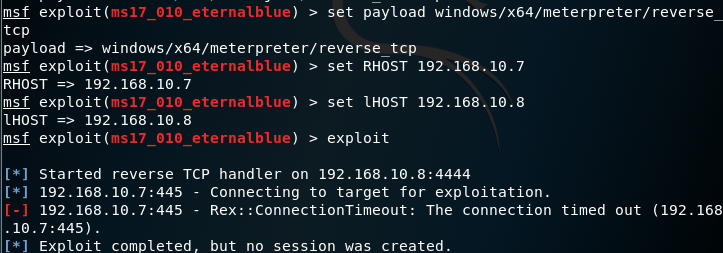
MS17-010漏洞入侵

利用meterpreter渗透工具

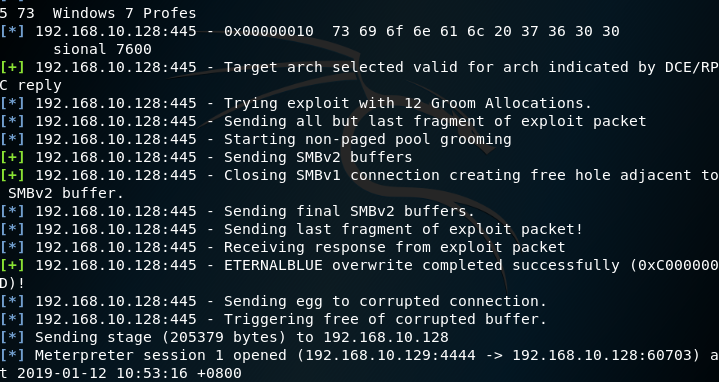
在kali上启动msfconsole,search ms17-010

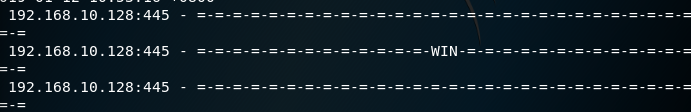


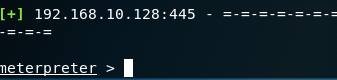
配置参数



利用exploit



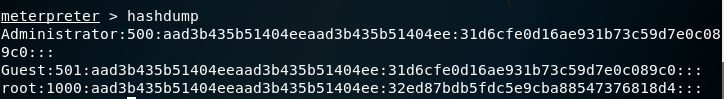


进入渗透工具视图



破解密码

Hashdump模块可以从SAM数据库中导出本地用户账号，run hashdump或hashdump也可以



认证算法：哈希HASH

-MD5和SHA算法

校验文件

-网站下载的文件

MD5（信息摘要算法）：创建了一个128位（16字节）的签名，很多协议都使用该算法做验证，MD5执行速度较快，但其安全性相对SHA稍微差点

SHA（安全散列算法）：已成为美国标准，它可以产生160位的签名（20字节的长度），为了更加安全，现在已经开发了SHA-256和SHA-512等。

屏幕截图screenshot

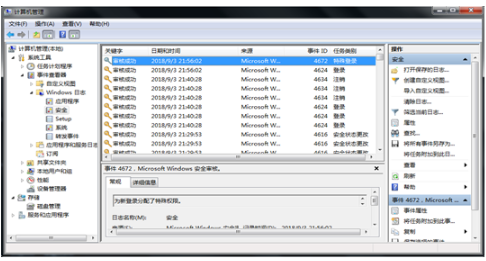


远程登陆





清除日志clearev



**漏洞扫描**

安装kali更新源





更新软件包索引

Apt-get update

更新系统

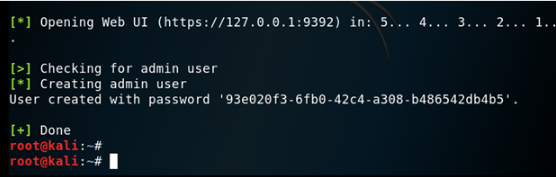
Apt-get dist-upgrade

下载openvas

Apt-get install openvas

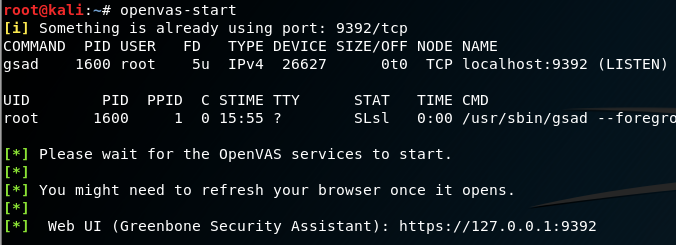
安装openvas

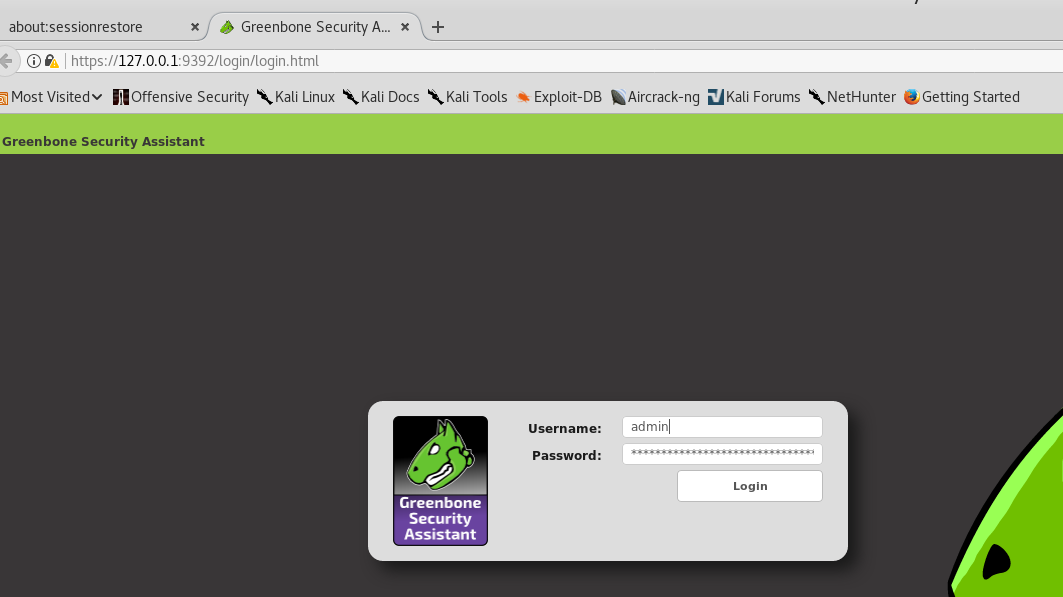
Openvas-setup

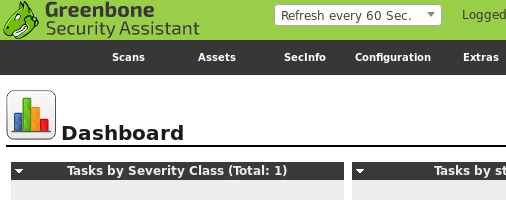


启动openvas

Openvas-start







Scans->tasks

