# 计算机网络渗透:基础和实践IMG_256

作者:直接影响

第一章

安装和配置kali

本文介绍kali2021-3版本的安装，apt国内源的配置并拍摄快照。（超详细！真保姆级教程）

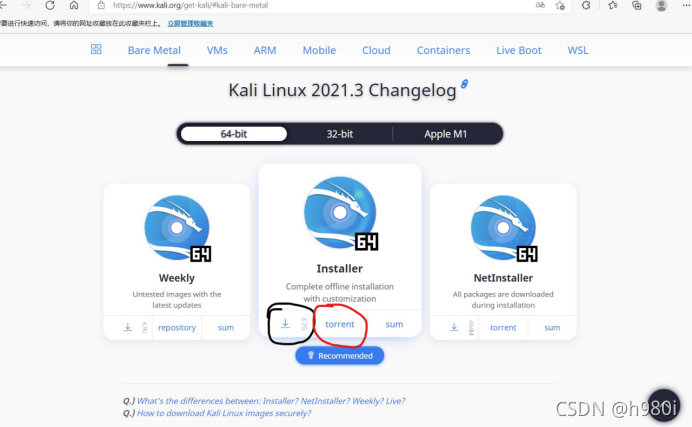
1.kali镜像的查找与下载

首先我们去kali.org官网下载kali的镜像

打开之后，点击下载

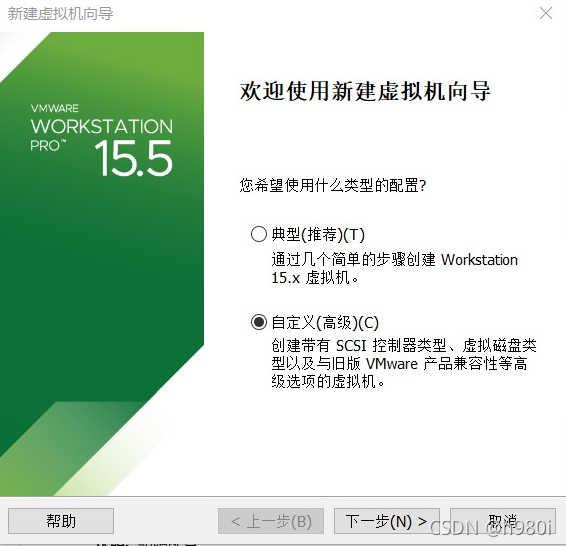


点击下载后，我们来到如下界面



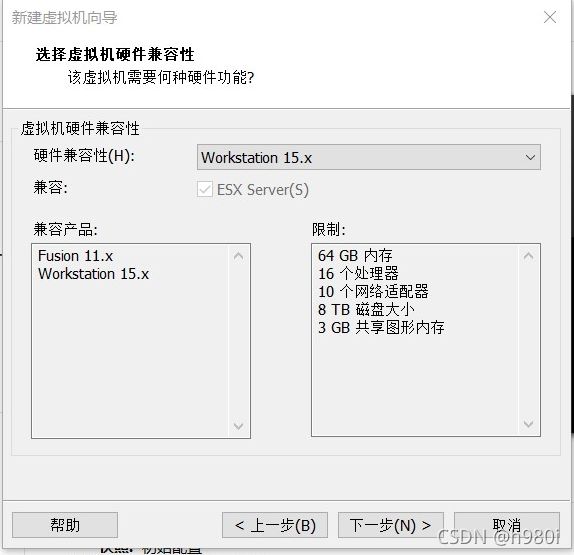
我们下载中间的64位即可，其中左面黑色圆圈里面的是下载本体，因为国外的网站速度很慢，所以我们直接下载右边红色圆圈中种子，种子下载好之后再去下载本体 ，都完成下载之后我们进行kali镜像的安装与配置。

2.kali镜像的安装与配置



启动虚拟机，创建一个新的虚拟机，选择自定义，并点击下一步

选择好自己对应虚拟机的兼容性，我这里是vm15，所以我选择vm15，并点击下一步



选择自己对应的kali版本，我这里是2021.3版本，点击下一步



选择Linux操作系统，因为kali是基于Debian版本的，我的操作系统是64位，所以我选择Debian10.\*64位，再点击下一步



在这里设置自己虚拟机的名称，然后选择自己安装位置（不建议C盘），

点击下一步

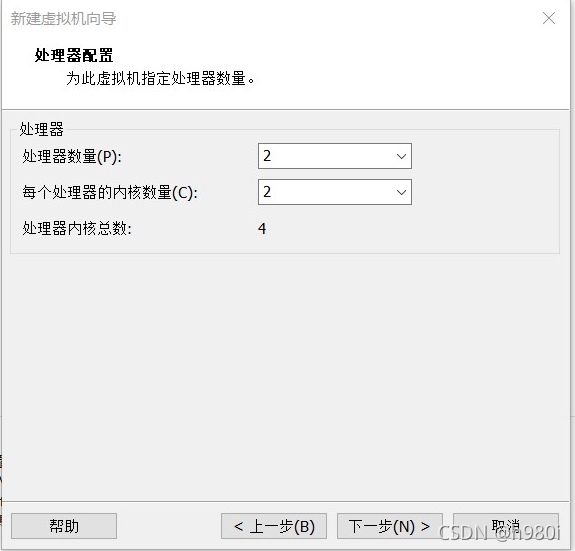


这里是让我们选择处理器数量，当然处理器越多虚拟机运行越流畅，（一般来说处理器数量不要超过自己电脑本身最大处理器的数量，如自己处理器有6个，你选择3个或者4个就行）因为我的电脑不太好，所以我选择2个处理器，2个内核数

\*（怎么查看自己的处理器？右键我的计算机，点击属性，点击设备管理器，点击处理器，即可看到处理器的数量



就像我的这处理器，只能说，懂得都懂吧）

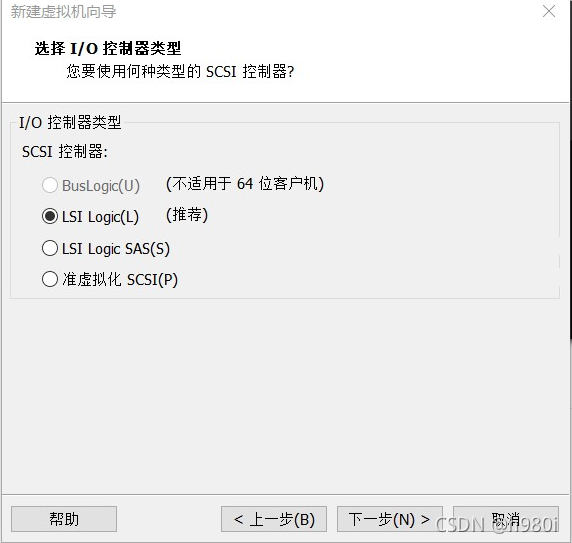


设置完处理器后我们来到下一步，设置内存，一般来说2g或者3g足够，土豪随意,点击下一步



如果是校园网用户网络模式选择nat模式，其余用户选择桥接模式，选择完后，点击下一步

这里选择它推荐的控制器点击下一步



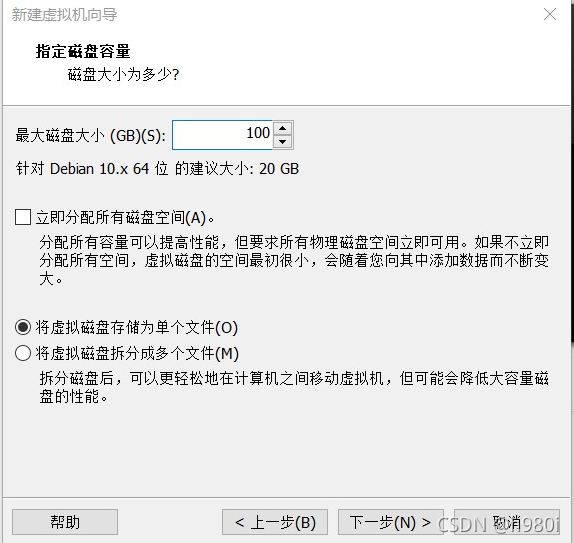
继续选择推荐，进行下一步

创建新虚拟磁盘，点击下一步



指定磁盘大小这里选择100g，或者更多，因为后续可能往虚拟机中加入更多文件可能造成虚拟机中空间不足，所以要加的大一些。并选择将其存储为单个文件，其实拆分成多个和单个区别不大，随意选择，我选择存储为单个。

\*（这里选择磁盘大小后不是立即就从主机里面拿出100g空间给了虚拟机，而是给虚拟机限定一个最大的磁盘空间，随着给虚拟机中添加的文件越来越多，虚拟机才会慢慢占用主机中的磁盘空间，所以多多益善）

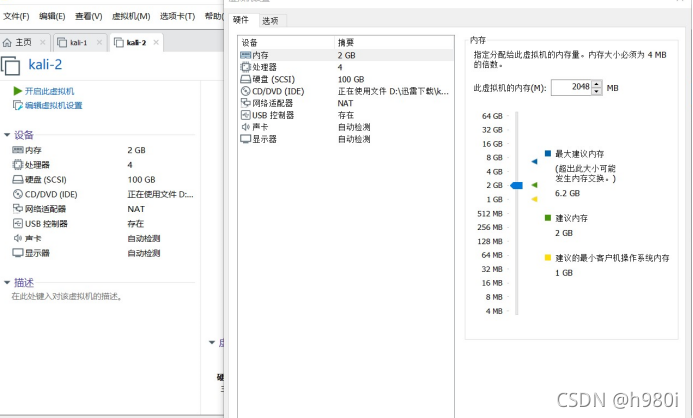


继续点击下一步，下一步，来到这个界面



我们点击自定义硬件，如果刚刚没有选择好内存的话，可以再次 进行重新选择，点击完成

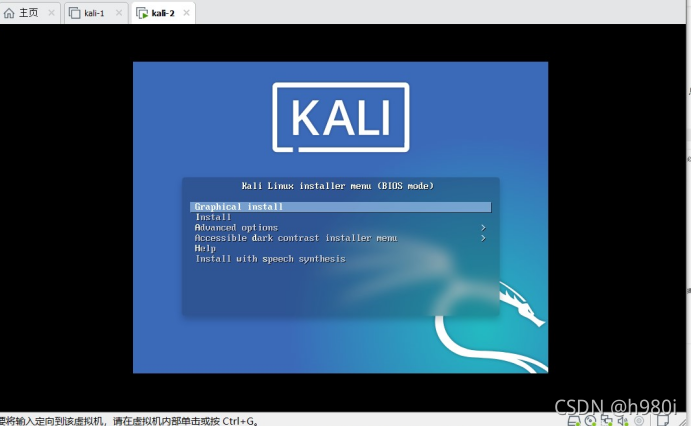
我们来到如下界面



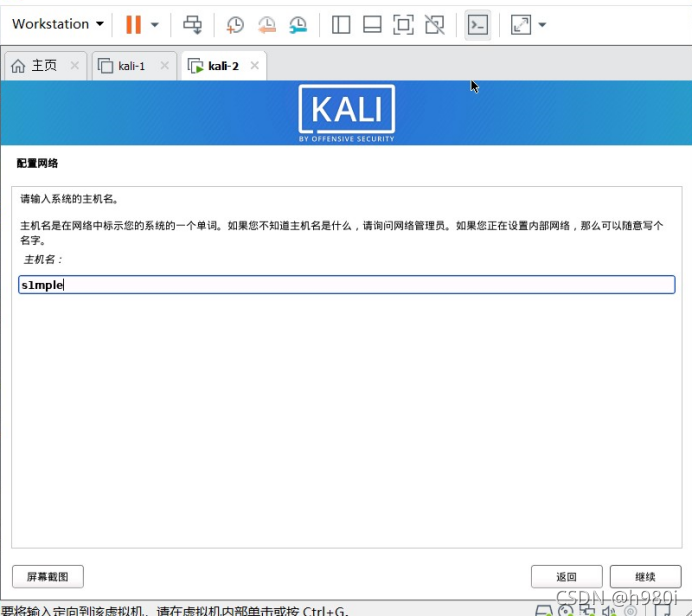
点击左侧编辑虚拟机设置也可打开自定义硬件进行相关设置

然后我们点击开启此虚拟机，进行安装

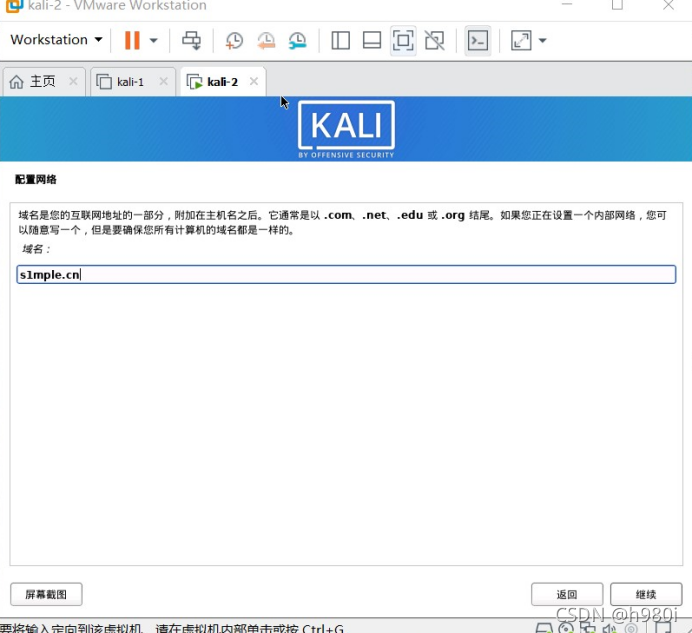
我们选择第一行图形化安装，将鼠标点进去，点击回车。点击Ctrl+Alt恢复出鼠标（每次当鼠标调不出来时我们都选择按下此按键，鼠标就会恢复）



英文好的选择英语版，我选择中文(简体)，点击继续Continue，选择中国（我相信很快就不会看到台湾这个选项了），点击继续，选择汉语，点击继续，显示正在安装介质，这里会很快，我们稍等，完成后这里显示主机名，我们起一个主机名，点击继续，

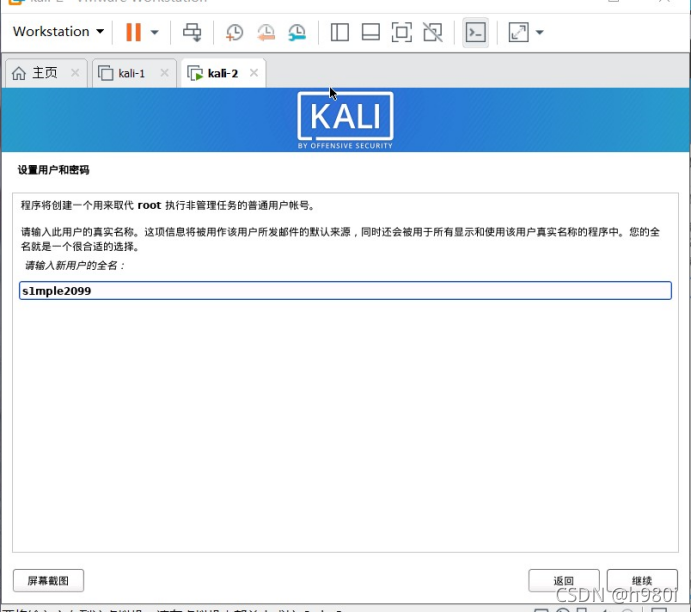


在刚才起的名字后加.cn 点击继续



点击后会显示正在配置一些文件，我们稍等，然后会让我们创建一个kali登陆时的用户名和密码，我们自行创建（这里的用户名和密码请各位记住）

选择第二行，点击继续，再次点击继续



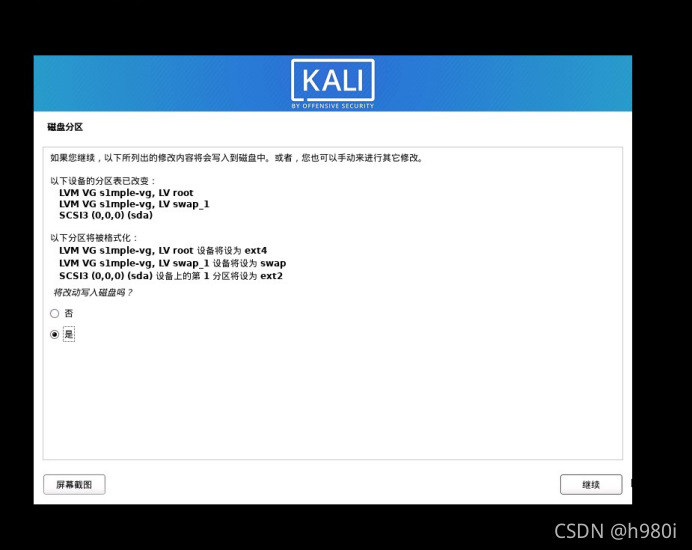
选择第一行，点击继续



选择是。点击继续，之后再次选择默认继续。

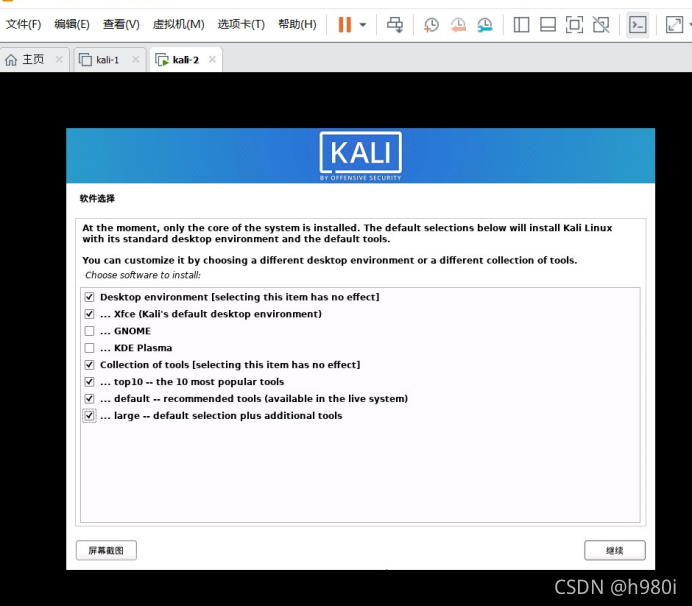


再次选择是，继续



可以看到正在安装基本系统，，这里也很快，我们稍等。

之后来到界面，按照我的选择进行勾选，其中Xface,GNOME和KDE这三个进行三选一，千万不要全选，我选择Xface,最后一行的large一定要选，否则会少安装很多工具，选择好后点击继续



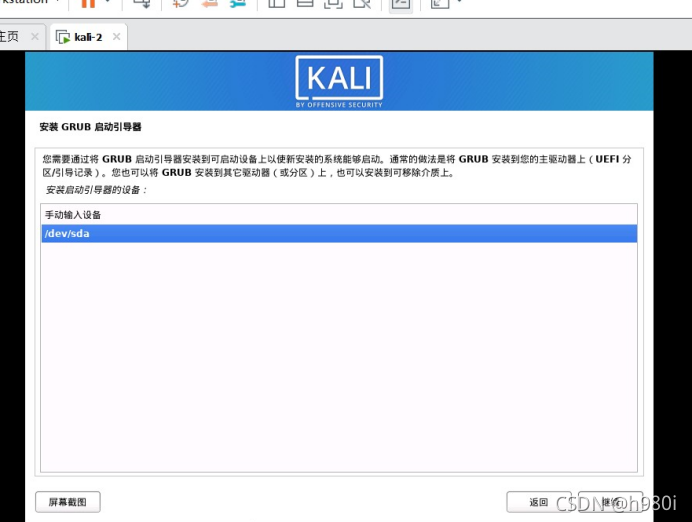
来到这个界面，此过程比较漫长，大家可以抽一根烟放松放

松，或者上个厕所，看看手机

经过漫长的等待，出现以下界面，选择是，点击继续

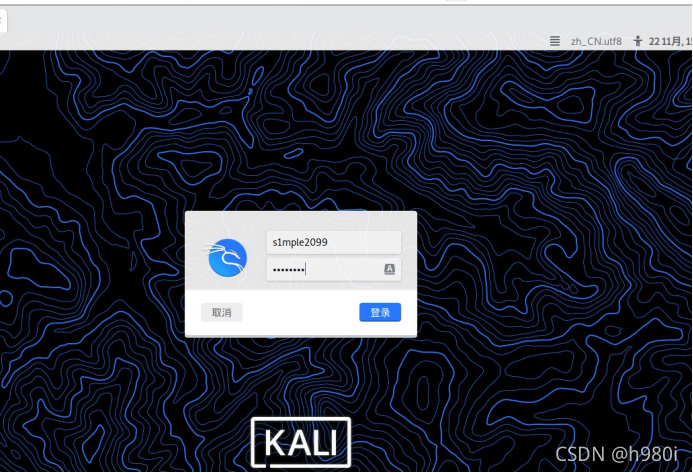


出现如下界面，选择/dev/sda点击继续，进行安装。

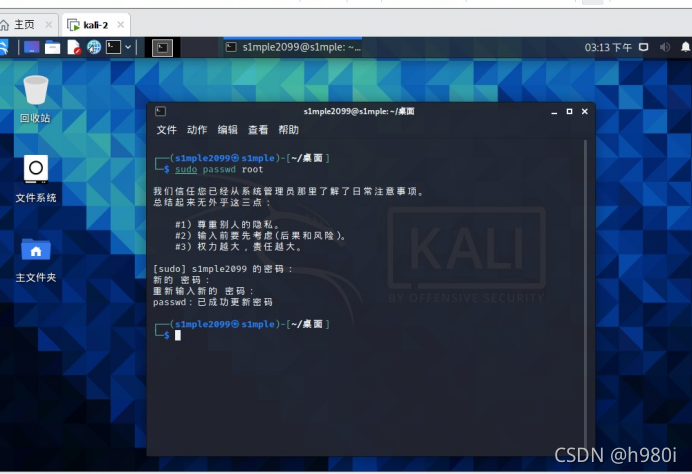


紧接着我们又会进入一个安装进程，这个稍微比较慢3~5分钟，我们静静等待。

安装完成后我们点击继续。可以看到系统进行重启，我们等待它重启。

然后我们进入到界面，输入自己在配置过程中的账号和密码，点击登录

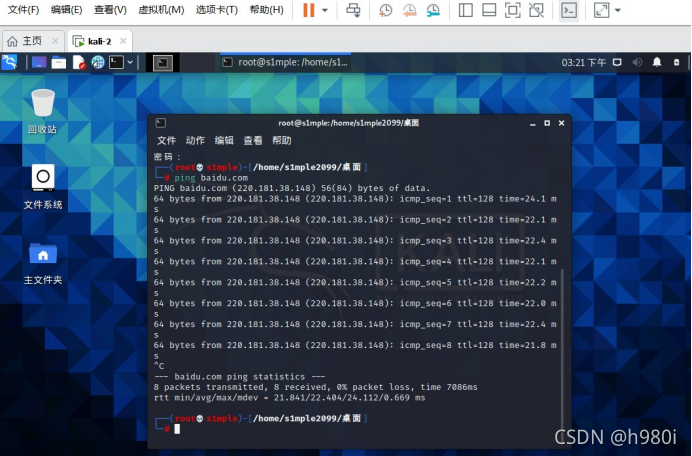
登陆进去之后，我们现在的身份是普通用户，所以我们要先激活root权限，以方便之后的操作（root权限比普通用户权限大）我们点击右键打开终端，或者点击屏幕左上方最右边的小黑框，打开终端，输入sudo passwd root



此时会让我们先输入普通用户的密码，即开机时输入的密码，输入完成后，会显示一条“新的密码”，此密码为root密码，我们进行设置，完成之后再次确认密码，完成root用户密码的设置。



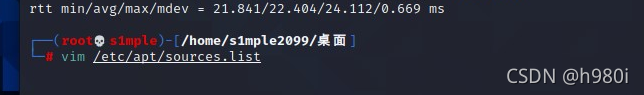
完成之后我们输入su root 再输入自己刚设置的root密码进入root模式



输入ping baidu.com如果能ping通就说明网络没有问题（如果一直在ping则Ctrl+c中断）

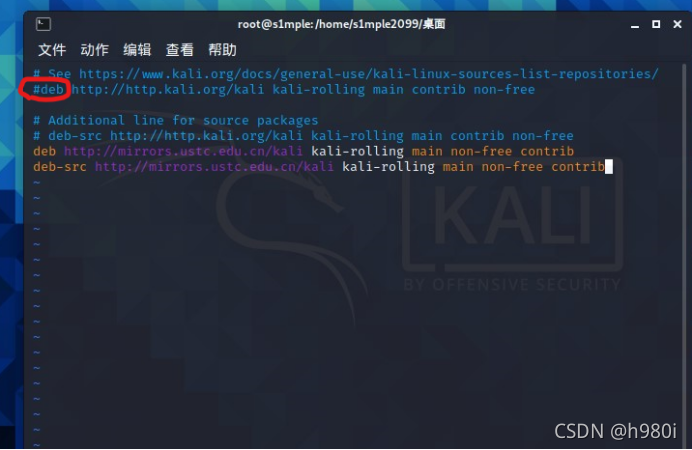
3.完成后我们配置apt国内源（我们这里用的是中科大的源）

输入vim /etc/apt/sources.list点击回车，进入编辑模式

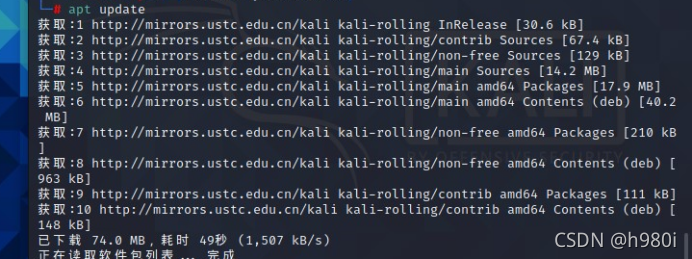


进入后键盘按i进入编辑模式，在第二行前加“#”

再在后面添加两行，如下，写完后，我们按Esc进入命令模式，然后我们再“shift+：”进入底层模式输入wq，点击回车



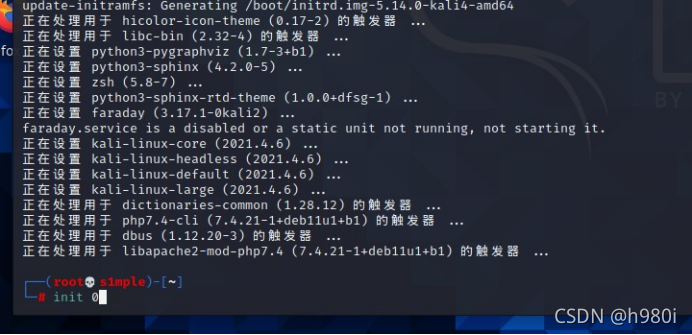
完成后，我们退回到root中的终端，输入apt update点击回车，可以看到，我们已经在使用中科大的源了



再次输入apt full-upgrade -y下载更新包



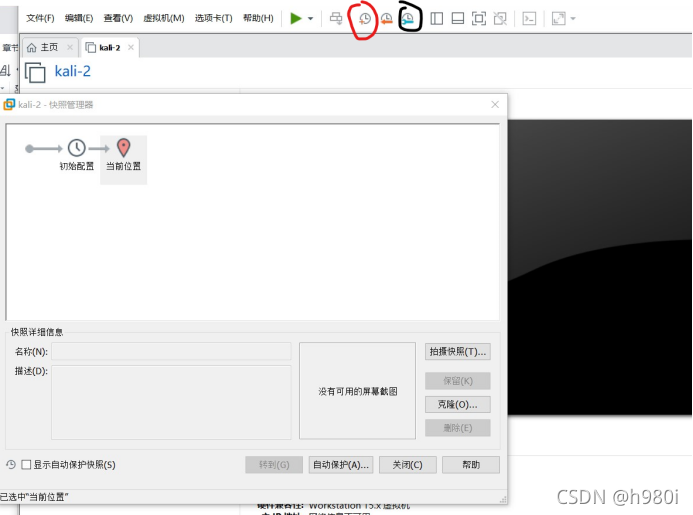
等待时间稍长，完成后选择yes,再次等待。完成后我们输入init 0关机



4.拍摄快照：

关机之后我们点击虚拟机最上方一行红色圆圈这里点击拍摄此虚拟机的快照

给自己快照命名就可看到拍摄的快照了，点击黑色圆圈可看到自己拍摄过的快照



1. 计算机网络安全常识

1、什么是防火墙？什么是堡垒主机？什么是DMZ？

防火墙是在两个网络之间强制实施访问控制策略的一个系统或一组系统。

堡垒主机是一种配置了安全防范措施的网络上的计算机，堡垒主机为网络之间的通信提供了一个阻塞点，也可以说，如果没有堡垒主机，网络间将不能互相访问。

DMZ成为非军事区或者停火区，是在内部网络和外部网络之间增加的一个子网。

2、网络安全的本质是什么？

网络安全从其本质上来讲是网络上的信息安全。

信息安全是对信息的保密性、完整性、和可用性的保护，包括物理安全、网络系统安全、数据安全、信息内容安全和信息基础设备安全等。

3、计算机网络安全所面临的威胁分为哪几类？从人的角度，威胁网络安全的因素有哪些？

答：计算机网络安全所面临的威胁主要可分为两大类：一是对网络中信息的威胁，二是对网络中设备的威胁。从人的因素考虑，影响网络安全的因素包括：

（1）人为的无意失误。

（2）人为的恶意攻击。一种是主动攻击，另一种是被动攻击。

（3）网络软件的漏洞和“后门”。

4、网络攻击和防御分别包括那些内容？

网络攻击：网络扫描、监听、入侵、后门、隐身；

网络防御：操作系统安全配置、加密技术、防火墙技术、入侵检测技术。

5、分析TCP／IP协议，说明各层可能受到的威胁及防御方法。

网络层：IP欺骗攻击，保护措施；防火墙过滤、打补丁；

传输层：应用层：邮件炸弹、病毒、木马等，防御方法：认证、病毒扫描、安全教育等。

6、请分析网络安全的层次体系

从层次体系上，可以将网络安全分成四个层次上的安全：物理安全、逻辑安全、操作系统安全和联网安全。

7、请分析信息安全的层次体系

信息安全从总体上可以分成5个层次：安全的密码算法，安全协议，网络安全，系统安全以及应用安全。

8、简述端口扫描技术的原理

端口扫描向目标主机的TCP／IP服务端口发送探测数据包，并记录目标主机的相应。通过分析相应来判断服务端口是打开还是关闭，就可以知道端口提供的服务或信息。端口扫描可以通过捕获本地主机或服务器的注入／流出IP数据包来监视本地主机运行情况。端口扫描只能对接受到的数据进行分析，帮助我们发现目标主机的某些内在的弱点，而不会提供进入一个系统的详细步骤。

9、缓冲区溢出攻击的原理是什么？

缓冲区溢出攻击是一种系统的攻击手段，通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。

缓冲区溢出攻击最常见的方法是通过使某个特殊的程序的缓冲区溢出转而执行一个shell，通过shell的权限可以执行高级的命令。如果这个特殊程序具有system权限，攻击成功者就能获得一个具有ｓｈｅｌｌ权限的shell，就可以对程序进行操控。

10、列举后门的三种程序，并阐述其原理和防御方法。

(1)远程开启TELNET服务。防御方法：注意对开启服务的监护；

（2）建立WEB和TELNET服务。防御方法：注意对开启服务的监控；

（3）让禁用的GUEST用户具有管理权限。防御方法：监护系统注册表。

11、简述一次成功的攻击，可分为哪几个步骤？

隐藏IP-踩点扫描-获得系统或管理员权限-种植后门-在网络中隐身。

12、简述SQL注入漏洞的原理

利用恶意SQL语句（WEB缺少对SQL语句的鉴别）实现对后台数据库的攻击行为。

13、分析漏洞扫描存在问题及如何解决

（1）系统配置规则库问题存在局限性

如果规则库设计的不准确，预报的准确度就无从谈起；

它是根据已知的是安全漏洞进行安排和策划的，而对网络系统的很多危险的威胁确实来自未知的漏洞，这样，如果规则库更新不及时，预报准确度也会相应降低；

完善建议：系统配置规则库应能不断地被扩充和修正，这样是对系统漏洞库的扩充和修正，这在目前开将仍需要专家的指导和参与才能实现。

（2）漏洞库信息要求

漏洞库信息是基于网络系统漏洞库的漏洞扫描的主要判断依据。如果漏洞库

完善建议：漏洞库信息不但应具备完整性和有效性，也应具备简易性的特点，这样即使是用户自己也易于对漏洞库进行添加配置，从而实现对漏洞库的及时更新。

14、按照防火墙对内外来往数据的处理方法可分为哪两大类？分别论述其技术特点。

按照防护墙对内外来往数据的处理方法，大致可以分为两大类：包过滤防火墙和应用代理防火墙。

包过滤防火墙又称为过滤路由器，它通过将包头信息和管理员设定的规则表比较，如果有一条规则不允许发送某个包，路由器将其丢弃。

在包过滤系统中，又包括依据地址进行过滤和依据服务进行过滤。

应用代理，也叫应用网关，它作用在应用层，其特点是完全“阻隔”了网络的通信流，通过对每个应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

代理服务器有一些特殊类型，主要表现为应用级和回路级代理、公共与专用代理服务器和智能代理服务器。

15、什么是应用代理？代理服务有哪些优点？

应用代理，也叫应用网关，它作用在应用层，其特点是完全“阻隔”了网络的通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

代理服务器有以下两个优点：

（1）代理服务允许用户“直接”访问互联网，采用代理服务，用户会分为他们是直接访问互联网。

（2）代理服务适合于进行日志记录，因为代理服务遵循优先协议，他们允许日志服务以一种特殊且有效的方式来进行。

第三章 网络安全具体讲解

第一章 网络安全概述与环境配置

1.狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全。广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。

2信息安全的基本要求

①机密性②完整性③可用性④不可否认性

3信息保障的核心思想是对系统或者数据的4个方面的要求：保护（protect），检测（detect），反应（react）和恢复（restore）。

利用4个单词首字母表示为PDRR，称之为PDRR保障体系。

4.从层次体系上，可以将网络安全分成4个层次的安全：物理安全，逻辑安全，操作系统安全和联网安全。

5.1999年10月经过国家质量监督局批准发布将计算机安全保护级别分为5个级别。

①用户自主保护级②系统审计保护级③安全标记保护级④结构化保护级⑤访问验证保护级

6.计算机安全级国际评价标

C1 C2 B1 B2 B3 A

D级是最低的安全级别，属于这个级别的操作系统有DOS和Windows98。

C2级别的常见操作系统有几种：UNIX系统；Novell 3.X或者更高版本；Windows NT,Windows 2000和Windows2003以上版本。

第二章 网络安全协议基础

1.OSI模型将通信会话需要的各种进程划分成7个相对独立的层次。

①物理层②数据链路层③网络层④传输层⑤会话层⑥表示层⑦应用层

2.TCP/IP协议族包括4个功能层：应用层、传输层、网络层和网络接口层。

3.IPv4的IP地址分成5类：A、B、C、D、E

4.TCP协议的头结构都是固定的。

①源端口:16位的源端口包含初始化通信的端口号。源端口和IP地址的作用是标识报文的返回地址。

②目的端口：16位的目的端口域定义传输的目的。这个端口指明报文接收计算机上的应用程序地址接口。

③序列号：TCP连线发送方向接收方的封包顺序号。

④确认序号：接收方回发的应答顺序号。

⑤头长度：表示TCP头的双四字节数，如果转化为字节个数需要乘以4.

⑥URG:是否使用紧急指针，0为使用，1为不使用。

⑦ACK:请求-应答状态。0为请求，1为应答。

⑧PSH：以最快的速度传输数据。

⑨RST：连线复位，首先断开连接，然后重建。

⑩SYN:同步连线序号，用来建立连线。

（11）FIN:结束连线。0为结束连线请求，1为表示结束连线。

（12）窗口大小：目的机使用16位的域告诉源主机，他想收到的每个TCP数据段大小。

（13）校验和：这个校验和与IP的校验和有所不同，它不仅对头数据进行校验还对封包内容校验。

（14）紧急指针:当URG为1时才有效。TCP的紧急方式是发送紧急数据的一种方式。

5.在下列情况中通常自动发送ICMP消息。

①IP数据报无法访问目标。

②IP路由器（网关）无法按当前的传输速率转发数据报。

③IP路由器将发送主机重定向为使用更好的到达目的的路。

6.常用的网络命令。

①判断主机是否联通的Ping命令

②查看IP地址配置情况的ipconfig指令

③查看网络连接状态的netstat指令

④进行网络操作的net指令

⑤进行定时器操作的at指令

第四章 网络扫描与网络监听

1.黑客攻击五部曲

①隐藏IP

②踩点扫描

③获得系统与管理员权限

④种植后门

⑤在网络中隐身

2.网络踩点

踩点就是通过各种途径对所要攻击的目标进行尽可能的了解。

常见的踩点方法包括：在域名及其注册机构的查询，公司性质的了解，对主页进行分析，邮件地址的收集和目标IP地址范围的查询。

踩点的目的就是探查对方的各方面情况，确定攻击的时机。摸清对方最薄弱的环节和守卫最松散的时刻，为下一步的入侵提供良好的策略。

3.网络扫描

网络扫描的原理是利用操作系统提供的connect（）系统调用，与每一个感兴趣的目标计算机的端口进行连接。如果端口处于工作状态，那么CONNECT（）就能成功。这个技术的一个最大优点是不需要任何权限，系统中的任何用户都有权利使用这个调用。

黑客攻击五部曲中第二步踩点扫描中的扫描，一般分成两种策略：一种是主动式策略，另一种是被动式策略。

被动策略是基于主机之上，对系统中不合适的设置、脆弱的口令及其他同安全规则抵触的对象进行检查。主动式策略是基于网络的，它通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。

4.网络监听器Sniffer(嗅探)的原理是

在局域网中与其他计算机进行数据交换时，数据包发往所有的连在一起的主机，也就是广播，在报头中包含目的机的正确地址。因此只有与数据包中目的地址一致的那台主机才会接受数据包，其他的机器都会将包丢弃。但是，当主机工作在监听模式下时，无论接受到的数据包中目的地址是什么，主机都将其接受下来。然后对数据包进行分析，就得到了局域网中通信的数据。一台计算机可以同一网段所有的数据包，不能监听不同网段的计算机传输的信息。

第五章 网络入侵

1.目前社会工程学攻击主要包括两种方式。

①打电话请求密码

②伪造E-msil

2.最常见的DOS攻击是计算机网络带宽攻击和连通性攻击。

3.比较著名的拒绝服务攻击包括：SYN风暴，Smurf攻击和利用处理程序错误进行攻击。

4.Smurf攻击是以最初发动这种攻击的程序名Smurf来命名。这种攻击方法结合使用了IP欺骗和带有广播地址的ICMP请求-响应方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务，属于间接、借力攻击方式。任何链接到互联网上的主机或者其他支持ICMP请求-响应的网络设备都可能成为这种攻击的目标。

5.利用处理程序错误进行攻击

①ping of death攻击

②Teardrop攻击

③Land攻击

第六章 网络后门与网络隐身

1.木马

木马是一种可以驻留在对方服务器系统中的一种程序，木马程序一般由两部分组成：服务器端程序和客户端程序。木马的功能是通过客户端可以操纵服务器，进而操纵对方的主机。

2.本质上，木马和后门都是提供网络后门的功能，但是木马的功能稍微强大一些，一般还有远程控制的功能，后门程序则功能比较单一，只是提供客户端能够登陆对方的主机。

第八章 操作系统安全基础

1.常用操作系统概述及特点

目前服务器常用的操作系统有4类：FreeBSD、UNIX、Linux和Windows NT/2000/2003 Server。

这些操作系统都是符合C2以上安全级别的操作系统，但是都存在不少漏洞，如果对这些漏洞不了解，不采取相应的安全措施，就会使操作系统安全暴露给入侵者。所有的应用都运行在操作系统上，稳固的操作系统是网络安全的基石。

2.安全操作系统和操作系统安全是不同的概念，如果操作系统的源代码内置了特定的安全策略，通常称之为安全操作系统，而操作系统安全则指的是一些设置等操作，使操作系统更加可靠。

3.Multics是开发安全操作系统最早期的尝试。1965年美国贝尔实验室和麻省理工学院的MAC课题组等一起联合开发一个称为Multics的新操作系统，

4.1969年B.W.Lampson通过形式化表示方法运用主体（Subject）、客体（Object）和访问矩阵（Access Matrix）的思想第一次对访问控制问题进行了抽象。主体是访问操作中的主动实体，客体是访问操作中被动实体，主体对客体进行访问。访问矩阵以主体为行索引、以客体为列索引，矩阵中的每个一元素表示一组访问方式，是若干访问方式的集合。矩阵中第i行第j列的元素Mij记录着第i个主体Si可以执行的对第J个客体Oj的访问方式，比如Mjj={read,Write}表示Si可以对Oj进行读和写操作。

5.主体与客体

操作系统中的每一个实体组件都必须是主体或者客体，或者既是主体又是客体。主体是一个主动的实体，它包括用户、用户组、进程等。系统中最基本的主体应该是用户（包括一般用户和系统管理员、系统安全员、系统审计员等特殊用户）。每个进入系统的用户必须是唯一标识的并经过鉴别确定为真实的。系统中所有事件要求，几乎全是由用户激发的。进程是系统中最活跃的实体，用户的所有事件要求都要通过进程的运行来处理。在这里，进程作为用户的客体，同时又是其访问对象的主体。

客体是一个被动的实体。在操作系统中，客体可以是按照一定格式存储在一定记录介质上的数据信息（通常以文件系统格式存储数据），也可以是操作系统中的进程。操作系统中的进程（包括用户进程和系统进程）一般有着双重身份。当一个进程运行时，它必定为某一用户服务—直接或间接地处理该用户的事件要求。于是，该进程成为该用户的客体，或为另一进城的客体（这时另一进城则是该用户的客体）。

6.安全策略和安全模型

安全策略和安全模型是计算机安全理论中容易相互混淆的两个概念。安全策略是指由关管理、保护和发布敏感信息的法律、规定的实施细则。

说一个操作系统是安全的，是指它满足某一给定的安全策略。安全策略由一套严密的规则组成，这些确定授权存取的规则是决定存取控制的基础。

安全模式则是对于安全策略所表达的安全需求的简单、抽象和无歧义的描述，它为安全策略和安全策略实现机制的关联提供了一种框架。安全模型描述了对某个安全策略需要用哪种机制来满足；而模型的实现则描述如何把特定的机制应用与系统中，从而实现某一特定安全策略所需的安全保护。

7.标识与鉴别

标识与鉴别涉及系统和用户。标识就是系统要标识用户的身份，并未每个用户取一个系统可以识别的内部名称----用户标识符。用户标识符必须是唯一的且不能伪造，将用户标识符和用户联系的过程成为鉴别，鉴别操作总是要求用户具有能够证明他的身份的特殊信息，并且这个信息任何其他用户都不能拥有他。

在操作系统中，鉴别一般是在用户登录时发生的，系统提示用户输入口令，然后判断用户输入的口令是否与系统中存在的用户的口令一致。较为安全的口令应该是不小于6个字符并同时含有数字和字母的口令，并且限定一个人口令的生存周期。另外生物技术是一种比较有前途的鉴别用户身份的方法，如利用指纹、视网膜等。

8.访问控制一般涉及两种形式

①自主访问控制DAC②强制访问控制MAC

9.安全配置方案初级篇主要介绍常规的操作系统安全配置，包括12条基本配置原则：物理安全、停止Guest账号、限制用户数量、创建多个管理员账号、管理员账号改名、陷阱账号、更改默认权限、设置安全密码、屏幕保护密码、使用NTFS分区、运行防毒软件和确保备份盘安全。

10.安全配置方案中级篇主要介绍操作系统的安全策略配置，包括10条基本配置原则：操作系统安全策略、关闭不必要的服务、关闭不必要的端口、开启审核策略、开启密码策略、开启账户策略、备份敏感文件、不显示上次登录名、禁止建立空连接和下载最新的补丁。

第九章 密码学与信息加密

1.密码学相关科学大致可以分为三个方面：密码学、密码编码学、密码分析学。

2.原则上来说对电子数据的攻击有两种形式

①被动攻击，即非法从传输信道上截取信息，或从存储载体上偷窃信息。

②主动进攻，即对传输或存储的数据进行恶意的删除、修改等。

3.除了提供机密性外，密码学需要提供三方面的功能：鉴别、完整性和抗抵赖性。

4.DES加密需要4个关键点：IP置换表和IP逆置换表，函数f，子秘钥K和S盒子的工作原理。

5.RSA算法的工作原理

RSA算法是一种基于大数不可能质因数分解假设的公钥体系。简单的说，就是找两个很大的质数，一个公开给世界，称之为“公钥”，另一个不告诉任何人，称之为“私钥”。

RSA体制可以简单描述如下：

①生成两个大素数p和q

②计算着两个素数的乘积n=p\*q

③计算小于n并且与n互质的整数的个数，即欧拉函数（n）=（p-1）(q-1)

④选择一个随机数e满足1<e<（n），并且e和（n）互质，即ged(e,(n))=1

⑤计算de=1 mod(n)

⑥保密d,p和q，公开n和e

利用RSA加密时，明文以分组的方式加密，即每一个分组的比特数应该小于log2n。加密明文x时，利用公钥（e,n）计算c=X mod n就可以得到相应的密文c。解密时，通过计算X=C mod n就可以恢复明文x。在RSA系统中，（e,n）构成加密秘钥，即公钥，（d,n）构成解密秘钥，即私钥。

选取的素数p和q要足够大，从而乘积n足够大，在事先不知道p和q的情况下分解n是计算上不可行的。常用的公钥加密算法包括：RSA密码体制、EIGamal密码体制和散列函数密码体制（MD4和MD5等）。

6.数字签名是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与自己受到的原始数据产生的哈希摘要对照，便可确信原始信息是否被篡改。这样就保证了信息来源的真实性和数据传输的完整性。

数字信封的功能类似于普通信封。普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密码技术保证了只有规定的接受人才能阅读信息的内容。数字信封中采用了单钥密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接受方的公钥加密对称密码，被公钥加密后的对称密码被称为数字信封。

第十章 防火墙与入侵检测

1.防火墙的局限性

①防火墙不能防范网络内部的攻击。比如：防火墙无法禁止变节者或内部间谍将敏感数据拷贝到软盘上。

②防护墙也不能防范那些伪装成超级用户或诈称新雇员的黑客们劝说没有防范心理的用户公开其口令，并授予其临时的网络访问权限。

③防火墙不能防止传送已感染病毒的软件或文件，不能期望防火墙对每一个文件进行扫描，查出潜在病毒。

2.防火墙的分类（防火墙的实现技术）

①分组过滤：作用在协议族的网络层和传输层，根据分组包头源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过，只有满足过滤逻辑的数据包才被转发到相应的目的地的出口端，其余的数据包则从数据流中丢弃。

②应用代理：也叫应用网关，它作用在应用层，其特点是完全“阻隔”网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。

③状态监测：直接对分组里的数据进行处理，并且结合前后分组的数据进行综合判断，然后决定是否允许该数据包通过。

3.常见的防火墙系统模型一般分为4类：筛选路由器模型、单宿主堡垒主机（屏蔽主机防火墙）模型、双宿主堡垒主机模型（屏蔽防火墙系统模型）和屏蔽子网模型。

4.入侵检测系统的概念

入侵检测系统指的是一种硬件或者软件系统，该系统对系统资源的非授权使用能够做出及时的判断、记录和报警。入侵者课分为两类：外部入侵者和内部入侵者。外部入侵着一般指来自局域网外的非法用户和访问受限制资源的内部用户；内部入侵者指假扮或其他有权访问敏感数据的内部用户或者是能够关闭系统审计的内部用户，内部入侵者不仅难以发现而且更具有危险性。

入侵检测是一种增强系统安全的有效方法，能检测出系统中违背系统安全性规则或者威胁到系统安全的活动。检测时，通过对系统中用户行为或系统行为的可疑程度进行评估，并根据评价结果；来鉴别系统中行为的正常性，从而帮助系统管理员进行安全管理或对系统所受到的攻击采取相应的对策。

5.入侵检测系统的类型和性能比较

根据入侵检测的信息来源不同，可以讲如前检测系统分为两类：基于主机的入侵检测系统和基于网络的入侵检测系统。

①基于主机的入侵检测系统：主要用于保护运行关键应用的服务器。他通过监视与分析主机的审计记录和日志文件来检测入侵。日志中包含发生在系统上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快的启动相应的应急想赢程序。

②基于网络的入侵检测系统：主要用于实时监控网络关键路径的信息，他监听网络上的所有分组来采集数据，分析可疑现象。

6.入侵检测的方法有3种分类依据：根据物理位置进行分类，根据建模方法进行分类和根据时间分析进行分类。

常用的方法有三种：静态配置分析、异常性检测方法和基于行为的检测方法。

7入侵检测的步骤3个：信息收集、数据分析和响应。

8.数据检测

数据检测是入侵检测系统的核心，他的效率高低直接决定了整个入侵检测系统的性能的高低。根据数据分析的不同方式可将入侵检测系统分为异常入侵检测和滥用入侵检测两类。

第十一章 IP安全和WEB安全

1.IPSec协议族包括两个安全协议：AH协议和ESP协议。

2.IPSec的实现方式有两种:传输模式和隧道模式，都可用于保护通信。

3.传输层安全性原理

在TCP传输层之上实现数据的安全传输是另一种安全解决方案，安全套接层SSL和TLS通常工作在TCP层之上，可以为更高层协议提供安全服务。