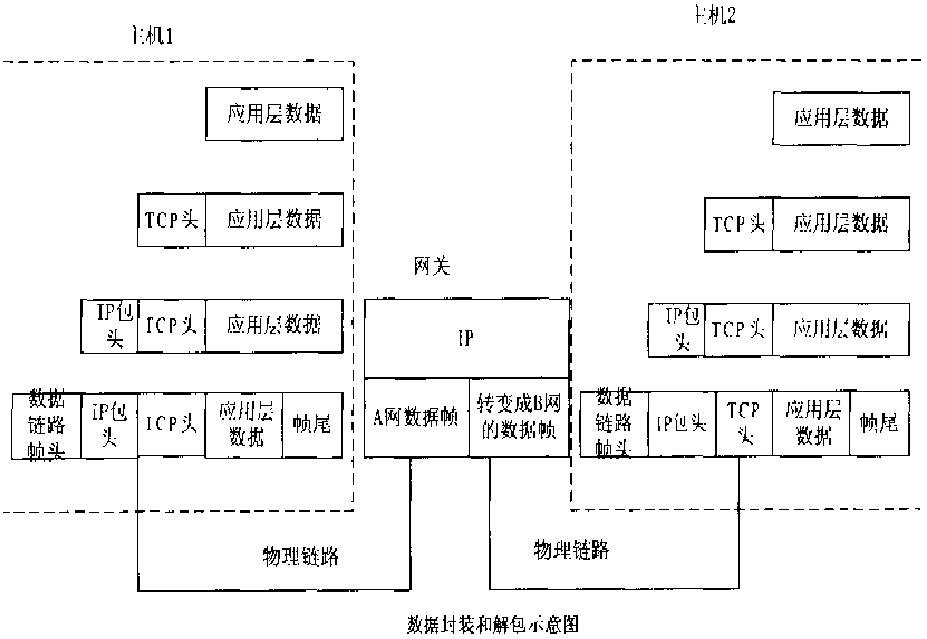
1. 画图并结合文字描述数据包在发送到网络之前，在协议栈中是如何封装的？为何说协议栈是符合“栈”这种数据结构的特征的？

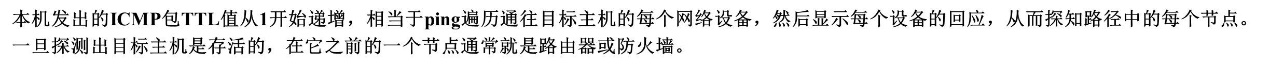


应用层的数据包沿着协议栈向下传递到传输层，作为传输层数据包的数据封装在传输层包头中；整个网络层数据包向下传递到网络层，作为网络层数据包的数据封装在网络层包头中；以此类推，直到封装成一个物理层的包。（2分）  
   在发送端先封装的内容，在接收端后解封。所以符合栈的“先进后出”特征。（2分）

1. 什么是主动攻击？什么是被动攻击？两者各有什么优缺点？

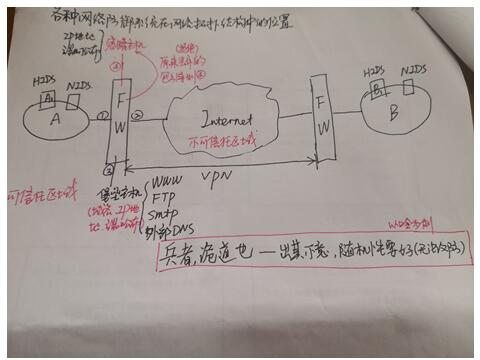
被动攻击是指攻击者监听正常通信双方之间的数据包，从而获取信息内容，或者进行信息量分析。  
被动攻击更容易实现、可以长时间攻击而不容易被发现，但是功能有限。  
主动攻击有中断数据流，伪造、篡改和重放数据包等几种攻击方式，会发送恶意数据包或者更改数据包信息。  
主动攻击的攻击力强大、可靠性高，但相对难以实现，且容易被发现。

1. 请分析Traceroute(Tracert)是哪一类网络安全工具？它的实现机理是什么？



1. 为保证局域网A上主机和局域网B上主机在互联网上通信的安全，需要使用防火墙、IDS、VPN、蜜罐等防御系统。试画出该两主机通信的拓扑图并在图中标出上述防御系统的位置，并分别阐述上述各个防御系统的功能以及放置于相应位置的原因。

拓扑图（4分）

  
1） 防火墙是边界安全设备，所以应该放于局域网和互联网之间，保证穿过两者之间通信的数据包的安全。（2分）  
2） 入侵检测系统大都放于局域网内，保证能够检测出穿过了防火墙的攻击数据包在局域网内的攻击行为，以及局域网主机间的相互攻击。（2分）  
3） 虚拟专用网是端-端的安全设备，配置在局域网网关处，在两网关之间建立安全隧道，用密码学技术保证隧道内传输的数据包的安全。（2分）  
注意VPN网关和防火墙放置的内外位置（哪个应该更接近Internet？），各种方案各有利弊，注意权衡  
VPN是对传输的数据包要加密的，但防火墙和入侵检测系统希望数据包全是明文的便于检测，同时使用这几者看似有一定的矛盾，怎么破？  
4）蜜罐是网络诱骗系统，一般放置在防火墙的DMZ区域，用来捕获网络入侵者的攻击行为。（2分）蜜罐和防火墙怎么配合使用

1. 使用动态包过滤的防火墙又叫什么类型的防火墙？以某种端口扫描类型为例说明该种防火墙相对静态包过滤防火墙的优越性。

[PowerPoint 演示文稿 (ustc.edu.cn)](http://cybersecurity.ustc.edu.cn/ns/ns05.pdf)

使用动态包过滤的防火墙又叫状态检测防火墙。（1分）如果Internet上的扫描者对防火墙内部进行扫描，他发送一个SYN+ACK包，对这样的数据包：

1）静态包过滤防火墙不能判断它是对内部用户向外发送请求进行应答的数据包，还只是外部扫描内部的一个单独数据包，为了保证通信的畅通，它会让这个数据包通过，也就是该扫描数据包能通过静态包过滤防火墙。（3分）

2）状态检测防火墙由于能记住在此数据包进入前内部用户是否发送过一个对该外部主机的一个TCP SYN连接请求，如果有这样的请求则允许该外部的SYN+ACK响应包进入，对于现在的这种扫描行为，因为事先内部主机没有相应请求，则不允许该SYN+ACK包进入。

因此状态检测防火墙比静态包过滤防火墙优越。（3分）

1. 防火墙对经过的数据包有哪四种不同的处理方式？并简单比较一下不同处理方式的安全性。

**①允许数据流通过；**

**②拒绝数据流通过：防火墙向发送者回复一条“该数据流已被拒绝”消息。**

**③将这些数据流丢弃：防火墙不给发送者任何提示信息——网络扫描所花费时间加长，发送者只能等待回应直至通信超时。**

④对不允许通过的数据包，将其引导到蜜罐中进行访问。

其中，对防火墙自身来说，丢弃数据包比拒绝数据包更安全；将防火墙引导到研究型蜜罐，有助于分析最新的攻击方式。

1. 补充：交换机和防火墙都是有一定安全功能的网络设备，如果对它们拒绝服务攻击成功的话，都是先牺牲各自的安全功能，而优先保证其通信功能。  
     
    交换机降级为集线器（Hub），防火墙降级为路由器。同层降级。

黑客的攻防思维和意识：  
一切皆有可能  
边界在于想象力（只有想不到，没有做不到）  
条条大路通罗马  
目标可能是陷阱（比如蜜罐），时刻警惕着

1. 什么是BPF、Libpcap、NPF、Winpcap？并简单阐述几者的关系。

WinPcap 是由伯克利分组捕获库派生而来的分组捕获库，它是在Windows 操作平台上来实现对底层包的截取过滤。WinPcap 为用户级的数据包提供了Windows 下的一个平台。

网络数据包过滤器（Netgroup Packet Filter，NPF）是Winpcap的核心部分，它是Winpcap完成困难工作的组件。它处理网络上传输的数据包，并且对用户级提供可捕获（capture）、发送（injection）和分析性能（analysis capabilities）。

WinPcap 是 BPF 模型和 Libpcap 函数库在 Windows 平台下网络数据包捕获和网络状态分析的一种体系结构。

***BPF：UNIX下的分组捕获过滤机制（驱动）；***

***Libpcap：UNIX下的分组捕获函数库；***

***NPF：Windows下的分组捕获过滤机制（驱动）；***

***Winpcap：Windows下的分组捕获函数库；（各1分）***

***BPF/ Libpcap分别从UNIX平台移植到windows平台相应得到NPF/ Winpcap。***

***分组捕获函数库是在分组捕获过滤机制的基础上构建的。（3分）***

1. 嗅探主机在接收不是发送给自己的数据包时，是如何绕过硬件过滤和IP地址过滤而将数据包捕获下来的？

Sniffer程序是一种利用以太网的特性把网络适配卡（NIC，一般为以太网卡）置为杂乱（promiscuous）模式状态的工具，一旦网卡设置为这种模式，它就能接收传输在网络上的每一个信息包。

普通的情况下，网卡只接收和自己的地址有关的信息包，即传输到本地主机的信息包。要使Sniffer能接收并处理这种方式的信息，系统需要支持 BPF，Linux下需要支持SOCKET-PACKET。但一般情况下，网络硬件和TCP/IP堆栈不支持接收或者发送与本地计算机无关的数据包，所以，为了绕过标准的TCP/IP堆栈，网卡就必须设置为混杂模式。一般情况下，要激活这种方式，内核必须支持这种伪设备BPFilter，而且需要root权限来运行这种程序，所以Sniffer需要root身份安装，如果只是以本地用户的身份进入了系统，那么不可能嗅探到root的密码，因为不能运行Sniffer。

***1）系统正常工作时网卡驱动程序会判断所接收到的数据包的目标MAC地址是否是本机，嗅探主机网卡设置成混杂模式后，将绕过硬件过滤，网卡驱动程序将不再检查数据包的目标MAC地址是否匹配，局域网上传输的所有数据被全部接收。（3分）***

***2）正常主机的网络层驱动程序还要对其目的IP地址进行判断：如果是本地IP，则上传给传输层处理，否则丢弃。嗅探主机安装了分组捕获过滤机制（BPF）后，将绕过IP地址过滤，将网卡驱动程序捕获到的所有数据包发送给操作系统进行处理。（4分）***

10.B主机对A主机和C主机进行ARP欺骗攻击时，A发给C的数据包能否到达B的网络接口？B能否直接接收这种数据包？为什么？  
***能够到达（2分）可以直接接收（2分）***

***因为ARP欺骗工具同时也带有嗅探功能，具有嗅探协议栈，可以接收目的IP地址不是本机的数据包（3分）***

***最后两问如果从该数据包的目的IP地址不是B，从而B不能直接接收的角度阐述也酌情给分。***

11.对于不是发送给自己的数据包，嗅探主机的协议栈是如何捕获的？  
   而普通主机的协议栈是如何接收发送给自己的数据包的呢？  
   请阐述上面两种情况下数据包的接收过程，以及是否对数据包进行回应。

对于不是发送给自己的数据包，嗅探主机的协议栈捕获过程如下：

1）嗅探主机网卡设置成混杂模式后，将绕过硬件过滤，网卡驱动程序将不再检查数据包的目标MAC地址是否匹配，局域网上传输的所有数据被全部接收。（2分）

2）嗅探主机安装了分组捕获过滤机制（BPF）后，将绕过IP地址过滤，将网卡驱动程序捕获到的所有数据包发送给操作系统进行处理。（2分）

但嗅探主机对捕获到的不是发送给自己的数据包并不进行任何回应。（2分）

普通主机的协议栈接收发送给自己的数据包的过程如下：

1）网卡驱动程序会判断所接收到的数据包的目标地址：不是本地主机，数据包将会被丢弃；是本地主机，数据包将被传到上层OS进一步处理。（2分）

2）网络层驱动程序还要对其目的地址进行判断：如果是本地IP，则上传给传输层处理，否则丢弃。（2分）

普通主机的协议栈是接收发送给自己的数据包后，当然要返回响应包进行回应。（2分）

12交换机上应该接入哪一种入侵检测系统？HIDS还是NIDS？从两者实现原理的不同加以分析。

1. HIDS（Host-based Intrusion Detection System，基于主机的入侵检测系统）

2. NIDS（Network Intrusion Detection System，网络入侵检测系统）



应该接入NIDS，因为交换机是内外网数据通信和局域网内主机通信的流量必经之处，从而可以方便实现NIDS的基本功能——抓包。

而HIDS是安装在局域网内重要主机或服务器上的，通过审计日志来检测是否有针对该机的入侵。

**嗅探检测技术1. 基于主机的检查2. 基于网络的检查**

13. 如何充分利用网卡混杂模式嗅探和ARP欺骗两种技术的优缺点，使之既能实现交换网络环境下的嗅探，又能较好地对捕获到的数据包进行分析和解码？请给出图示说明。

设想一个应用环境，比如学校的大型机房，就是一个交换式局域网，此时在其中的任一台主机上安装共享网络嗅探工具Wireshark，尽管它的嗅探功能非常强，但在交换网络中它也无能为力。这时它只能嗅探到从本机进出的数据包。而单独使用ARPspoof工具，虽然能嗅探到主机和主机（或网关）之间的数据流，但界面的不友好和弱的解码功能可能使得用户不方便得到、也可能得不到明文的用户帐号和口令。（6分）

在这种情况下，可以先用ARPspoof对目标主机和网关之间进行ARP欺骗，使它们的通信内容都从本地网卡通过。在进行了欺骗的同时打开Wireshark，这时再用Wireshark进行嗅探，用Wireshark强大的解码功能，就可以分析出大量的希望得到的敏感信息了。当然这种方案不但适用于交换网络环境中，也适用于共享网络环境中以及两者共存的更复杂环境中。（6分）

ARP协议。根据目的主机的ip，找到其mac地址。

14. 什么是网卡的隐秘模式？隐秘模式与混杂模式的区别是什么？管理员为何要将网卡设置成隐秘模式？NIDS的两块网卡是如何设置的？

15. 为了应对攻击者利用分片来穿越防火墙，防火墙在检测时进行数据包的重组（需要花费较长时间），仅当重组后的数据包符合通行规则时，数据包才可放行。攻击者如何利用防火墙这一处理机制对防火墙进行攻击呢？

16. IP欺骗攻击得以实现的两个基本前提是什么？为什么Windows系统中一般不能实现IP欺骗攻击？

17. 直接基于局域网的ARP欺骗，黑客能进行哪些攻击（至少两种）？如果黑客已能够对局域网主机（或网关）进行会话注射，试想一下，他下一步就会进行何种攻击？