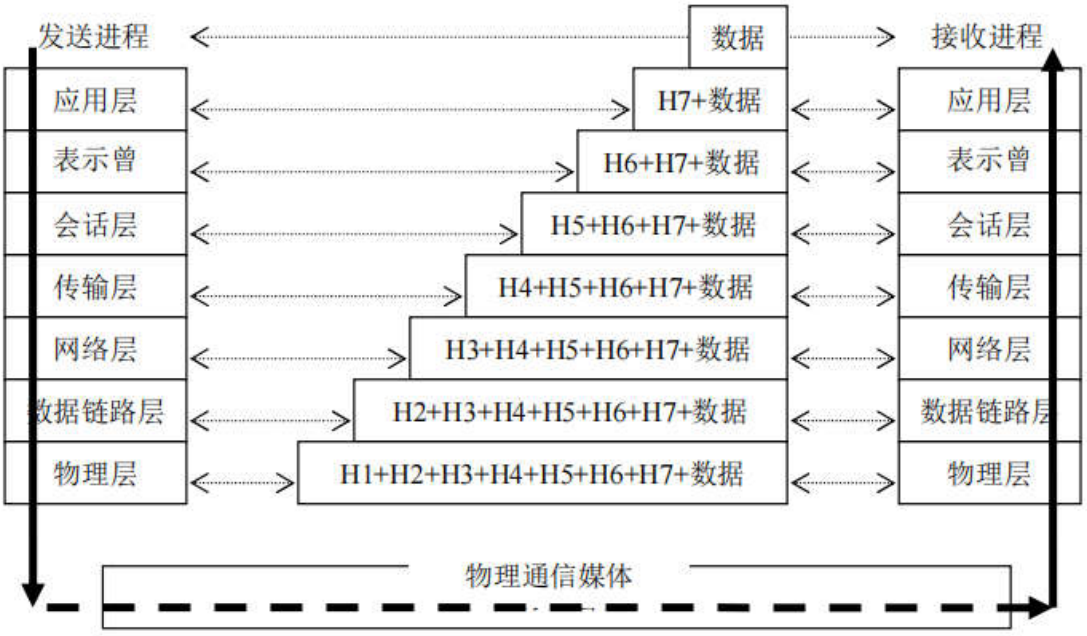
1、画图并结合文字描述数据包在发送到网络之前，在协议栈中是如何封装的？为何说协议栈是符合“栈”这种数据结构的特征的？

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；整个传输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）



2、什么是主动攻击？什么是被动攻击？两者各有什么优缺点？

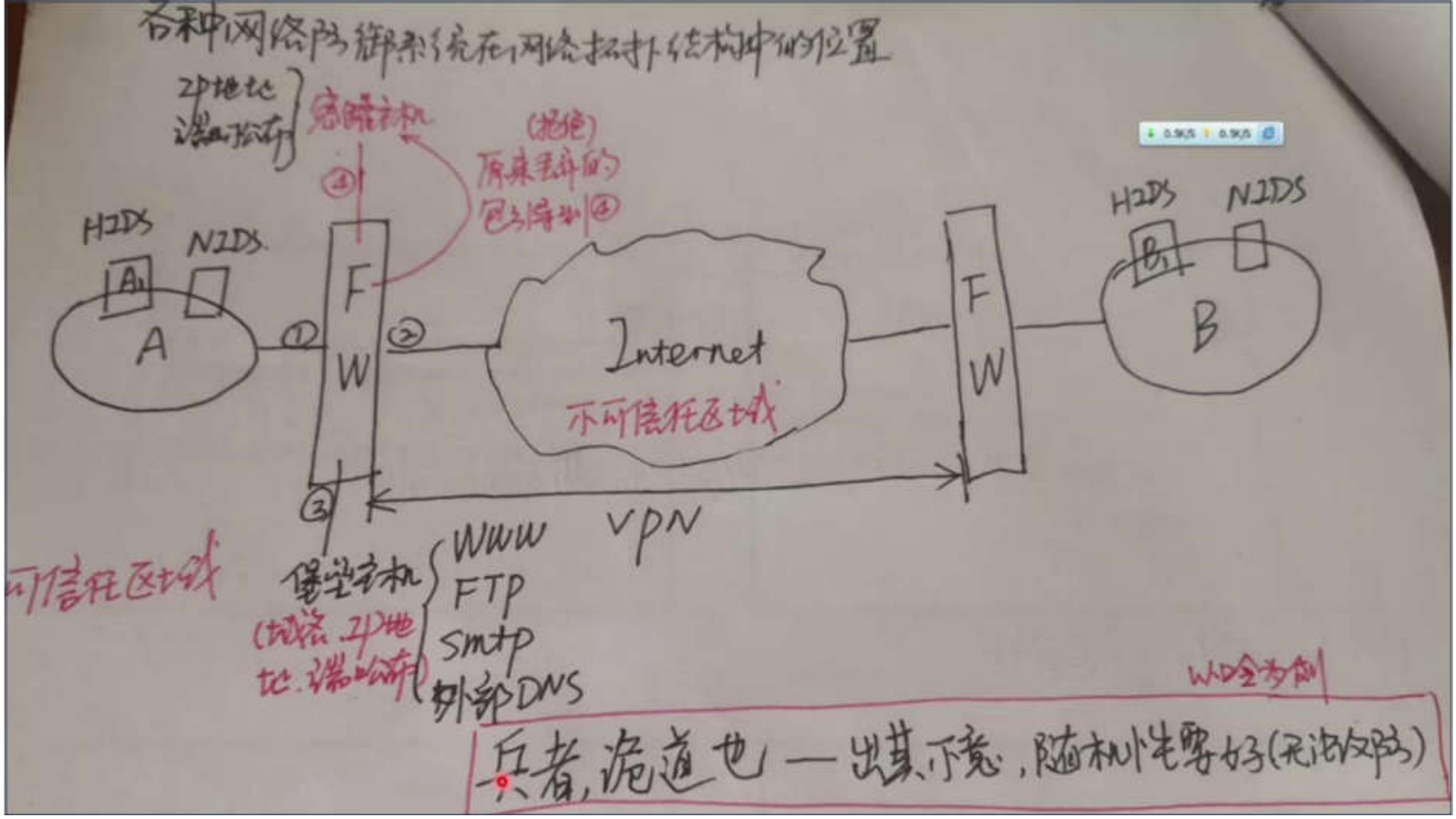
① 被动攻击是指攻击者监听正常通信双方之间的数据包，从而获取信息内容，或者进行信息量分析。被动攻击更容易实现、可以长时间攻击而不容易被发现，但是功能有限。

② 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。

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

Traceroute（Tracert）是使用命令行方式的踩点工具。本机发出的 ICMP 包 TTL 值从 1 开始递增，相当于 ping 遍历通往目标主机的每个网络设备，然后显示每个设备的回应，从而探知路径中的每个节点。一旦探测出目标主机是存活的，在它之前的一个节点通常就是路由器或防火墙。

4、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。



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）

④ 蜜罐是网络诱骗系统，一般放置在防火墙的 DMZ 区域，捕获网络入侵者的攻击行为。（2 分）

注意 VPN 网关和防火墙放置的内外位置（后者更接近 Internet）。VPN 是要对传输的数据包加密的，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。

5、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。

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：

① 静态包过滤防火墙不能判断它是内部用户向外发送请求进行应答的数据包，还是外部扫描内部的一个单独数据包。为了保证通信的畅通，它会直接让这个数据包通过。（3 分）

② 状态检测防火墙能记住在此数据包进入前，内部用户是否发送过对外部主机的一个 TCP SYN

连接请求。如果有，则允许外部的 SYN+ACK 响应包进入。如果没有，则不允许外部的 SYN+ACK 响应包进入。（3 分）

6、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 ③ 将这些数据流丢弃 ④ 将数据流引入蜜罐

系统安全性：④>③>②>①

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，防火墙降级为路由器。同层降级。这次期末考试有一题跟这个相关哦。

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

BPF：UNIX 下的分组捕获过滤机制。Libpcap：UNIX 下的分组捕获函数库；（1 分）

NPF：Windows 下的分组捕获过滤机制。Winpcap：Windows 下的分组捕获函数库；（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）

8、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？

① 正常情况，网卡驱动程序会对数据包的目标 MAC 地址进行判断。嗅探主机网卡设置成混杂模式后，将绕过硬件过滤，局域网上传输的所有数据被全部接收。（3 分）

② 正常情况，网络层驱动程序会对数据包目的 IP 地址进行判断。嗅探主机安装分组捕获过滤机制 BPF 后，将绕过 IP 地址过滤，将数据包传给操作系统处理。（4 分）

9、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。（2 分）能。（2 分）因为 ARP 欺骗工具带有嗅探功能，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）

10、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，局域网上传输的所有数据被全部接收。

② 嗅探主机安装分组捕获过滤机制 BPF 后，将绕过 IP 地址过滤，将数据包传给操作系统处理。嗅探主机不进行回应。（6 分）

对于发送给自己的数据包，普通主机的协议栈捕获过程如下：

① 网卡驱动程序对数据包的目标 MAC 判断：如果是本地 MAC，则上传给 OS 处理，否则丢弃。

② 网络层驱动程序对数据包目的 IP 判断：如果是本地 IP，则上传给传输层处理，否则丢弃。普通主机要进行回应。（6 分）

11、交换机应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。

应该接入 NIDS。

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 NIDS 的抓包。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。

12、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。

尽管 Wireshark 嗅探功能非常强，但在交换网络中也无能为力，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，但其界面的不友好和较弱的解码功能，使得用户不方便得到明文的用户帐号和口令。（6 分）这种情况下，可以先用 ARPspoof 对目标主机和网关之间进行欺骗，使它们的通信内容都从本地网卡通过。再用 Wireshark 进行嗅探，其强大的解码功能可以分析出大量的敏感信息。（6 分）

13、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？

网卡的隐秘模式就是网卡设置成混杂模式的同时，外界扫描不到对应的 IP 地址。（2 分）

管理员将网卡设置成隐秘模式是为了使得攻击者无法访问 NIDS 主机。（1 分）

一块设置隐秘模式进行网络监听。一块连接到独立网段，由管理员远程配置和管理。（4 分）

14、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），当重组后的数据包符合通行规则时才可放行。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？

攻击者短时间内向防火墙发送大量分片，耗尽防火墙处理器资源，导致防火墙被拒绝服务攻击。

15、IP 欺骗攻击得以实现的两个基本前提？为什么 Windows 中一般不能实现 IP 欺骗攻击？

一是目前的 TCP/IP 网络在路由数据包时，不对源 IP 地址进行判断，给伪造 IP 包创造了条件；

二是两台主机之间，存在着基于 rlogin 命令的信任，可以进行“会话劫持”。（5 分）

因为 Windows 系统中不存在基于 rlogin 命令的信任。（2 分）

16、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？

黑客能进行 DNS 欺骗、会话劫持等攻击。（4 分）

黑客在会话注射的基础上可以进行注入欺骗网页、网页挂马等攻击。（3 分）

17、网络攻击中黑客可以将数据包真实的源 IP 地址修改成“假”的地址，请问在实现中源 IP 地址的“假”具体有哪两种不同的含义？SYN 攻击使用的是其中的哪一种？

第一种“假”的含义是“假冒”：即假冒同一网段内另一台真实主机；（3 分）

第二种“假”的含义是“虚假”：即假冒源 IP 地址在该网段可路由但不可到达。（4 分）

SYN 攻击使用的是虚假 IP 地址。（1 分）

18、使用 SYN Proxy 进行防范，外网主机对服务器进行 SYN Flood 攻击能成功吗？但它有什么不足呢？这种防范方法中，防火墙是包过滤型防火墙还是应用层网关型的？

使用 SYN Proxy 进行防范，外网主机对服务器进行 SYN Flood 攻击很难成功。（2 分）

它的不足是防火墙自身可能被 SYN Flood 攻击成功。（2 分）

这种防范方法中，防火墙是应用层网关型的。（3 分）

19、对一个程序设置 SUID 位的含义是什么？为什么一般会寻找如下一个程序的漏洞进行缓冲区溢出攻击：具有 root 执行权限且设置了 SUID 位？

SUID 位赋予普通用户临时的权限提升，以保证用户可以在系统中完成某些特定的任务。（2 分）

如果某个设置 SUID 位的程序属主是 root，那无论谁执行它，都相当于用 root 在运行。（2 分）

这样，即使是只具有普通用户权限的黑客运行一个“具有 root 执行权限且设置了 SUID 位”的程序，并对其进行缓冲区溢出攻击成功，黑客就能直接获得 root 权限。（3 分）

20、被加载的应用程序在内存中的影像包括哪三个区域？各有什么作用？其中哪些区域容易受到缓冲区溢出攻击？这些区域在读写上有什么共同特点？

从内存低地址向高地址方向分别为：文本区、数据区、堆栈区。（2 分）

文本区：存储程序的执行代码以及只读数据。（1 分）

数据区：未初始化数据区存储静态分配的变量，已初始化数据区存储程序的初始化数据。（1 分）

堆栈区：堆区用于存储程序运行过程中动态分配的数据块（调用 malloc 或 calloc 函数），

栈区用于在函数调用中存储栈帧。（1 分）

未初始化数据区、堆区、栈区都是可以写的内存区域，容易受到缓冲区溢出攻击。（2 分）

21、C 语言与其他程序设计语言不同，它是如何标识字符串结束的？没有使用长度参数对字符串边界进行检测会引起哪两方面问题？其中哪种会造成缓冲区溢出攻击？

C 语言中字符串是以’\0’（NULL）结束的。（2 分）

1）如果读取数组以外内容，会使程序得出错误结果。（1.5 分）

2）如果是写入，可能破坏该进程内存的其它内容。（1.5 分）

其中后者会造成缓冲区溢出攻击。（2 分）