网络安全：  
被动攻击种类：截获、窃听、嗅探、监听、流量分析、抓包

被动攻击主要破坏了网络安全的保密性

主动攻击种类：中断、篡改、伪造

中断破坏了网络安全的可用性

篡改破坏了网络安全的完整性

伪造破坏了网络安全的认证性

网络安全的目标：保密性、完整性、可用性、认证性、不可抵赖性

网络安全模型：

**P2DR模型（PPDR）：**策略（Policy）、保护（Protection）、检测（Detection）和响应（Reaction）

**PDRR模型：**保护（Protection）、检测（Detection）、响应（Reaction）和恢复（Restore）

**P2DR2模型：**策略（Policy）、防护（Protection）、检测（Detection）、响应（Reaction）和恢复（Restore）

 **P2DR模型（PPDR）**

 **P2DR2模型（**将 P2DR2模型中的“安全策略”除掉就是PDRR模型**）**

网络攻击手段

阻塞类：DDOS（僵尸网络）、DOS（LAND、Smurf、泛洪、电子邮件炸弹、死亡ping）

控制类：口令猜测、木马攻击、缓冲区溢出

欺骗类：IP欺骗、ARP欺骗、DNS欺骗

Dos攻击防御手段：有效完善的设计、限制带宽、及时给系统安装补丁、运行少量的服务、只允许必要的通信、封锁敌意IP

DDos攻击的普遍特征：网络通信流量异常

口令猜测、破解方法：暴力破解、字典攻击、组合攻击、其他方式（社会工程学）

弱口令：少于8个字符的口令

MD5 可以将任意长度的原文生成一个128位（16字节）的哈希值

SHA-1可以将任意长度的原文生成一个160位（20字节）的哈希值

/etc/shadow：影子密码文件，包含了加密过的密码和密码失效时间，只有root用户才能获取

/etc/passwd：存储主用户组的文件

/etc/group：计算机上所有的组

/etc/gshadow：计算机上所有组的群组密码文件

ARP欺骗检测：

网络频繁掉线、莫名其妙慢下来，arp -a命令检查网关MAC地址是否和真实的网关MAC地址相同，使用网络嗅探软件发现局域网存在大量ARP包

ARP欺骗后果：

同网段其他用户无法正常上网

从交换式局域网的所有数据包中获取敏感信息

篡改重要信息，进而控制受害者会话

IP欺骗方式：

简单的IP地址更改、源路由攻击、TCP会话劫持

**简单的IP地址更改**：攻击者将IP地址更改为其他主机的IP（无法得到返回的数据流）

**源路由攻击**：在IP地址更改的基础上，发送端指定数据包必须经过的IP地址清单或者确切的IP地址，若数据包没有经过确切的路径，数据包将被丢弃并返回ICMP报文

**TCP会话劫持**：接管现存动态会话的过程，即攻击者可以替代原来的合法用户，同时监视并掌握会话内容，结合了嗅探和欺骗技术，一般伴随着Dos攻击，不依赖操作系统

会话劫持过程：发现目标 – 确认会话状态 – 猜测序列号 – 使客户主机下线（Dos）-- 接管会话

DNS欺骗：

当向本地DNS服务器查询域名时，如果服务器缓存中已有相应记录，就直接将这条记录返回给用户

DNS欺骗的关键是在DNS服务器的本地Cache中缓存一条伪造的解析记录

DNS欺骗的局限性：

攻击者不能替换缓存中已经存在的记录

DNS服务器存在缓存刷新时间问题

网络攻击的一般步骤：

搜集资料 — 弱点扫描/判断漏洞 — 刺探 — 获取权限 – 提权 – 攻击/获取信息 – 安装后门 – 进一步攻击 – 清除痕迹

刺探、踩点常用手段指令：

Whois查询：查询域名、IP地址

Nslookup： 查询域名信息和DNS服务器

Host/hostnew：把一个主机名解析到一个网际地址或把一个网际地址解析到一个主机名

Tracert：路由追踪

扫描的基本方法：

Ping

Nmap：-F：扫描目标主机端口

-O：识别目标主机的操作系统类型

-sV：探测目标主机开放的服务和版本信息

-PR：使用APR请求探测局域网内活跃的主机

-sn：发现指定子网中存活的主机

恶意代码：

恶意代码分类：计算机病毒、蠕虫、木马、僵尸网络

计算机病毒：是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码，典型的计算机病毒由引导模块、触发模块、传染模块和表现模块组成

按感染目标分类计算机病毒：文件型（感染可执行文件）、引导型（感染磁盘）、宏病毒（感染office）

按隐蔽方式分类计算机病毒：隐蔽型、加密型、多态病毒、变形病毒

蠕虫：蠕虫是一种可以独立运行，能主动寻找感染目标并且能够自动传播的恶意程序

蠕虫的传播依赖于特定的计算机漏洞，蠕虫由扫描模块、攻击模块、传输模块、负载模块组成

蠕虫和计算机病毒的区别：

计算病毒存在于文件中，蠕虫不在文件上

计算机病毒需要文件传播，蠕虫需要计算机网络传播

计算机病毒感染目标为文件、磁盘，蠕虫感染目标为分布在网络中的计算机

僵尸网络功能和蠕虫相似，最大的区别式僵尸网络具有远程控制的功能

Web攻击重点：SQL注入攻击、跨站脚本攻击

SQL注入攻击原理：利用Web应用对后台数据库查询语句的处理存在的安全漏洞，构造一段可以获取想要的数据的数据库查询代码

SQL注入攻击的原因：网站对用户提交的数据库查询语句和输入参数没有进行检查和过滤

SQL注入攻击过程：寻找漏洞 – 测试网站是否存在SQL注入漏洞 – 猜测数据库名称、表名、表信息 – 后续攻击

SQL注入攻击的防范：

使用预编译语句，绑定变量

对用户提交的数据和参数进行严格的过滤

采用存储过程来访问和操作数据

使用安全函数

迁移到ORM框架

避免Web应用使用root、dbowner等高权限账户

跨站脚本攻击（又称XSS）原理：

攻击者往Web页面里插入恶意脚本代码，当用户浏览该网页时，嵌入其中的代码被执行

跨站脚本攻击的原因：

Web服务器没有对用户输入进行有效性验证或验证强度不够，而又轻易地将它们返回给客户端

XSS分类：反射型XSS（将用户数据反射给浏览器，如恶意链接）

存储式XSS（攻击脚本永久存储在目标服务器的数据库或者文件中，如含有恶意js代码的博库文章）

DOM型XSS（利用客户端浏览器对请求的页面进行DOM渲染）

**XSS防御**

对用户，教育为主，比如不要点可疑链接，安装一些浏览器防范的插件，避免可疑的网站和破解版应用

对Web开发者：对所有用户提交的内容进行可靠的输入验证，保护所有敏感的功能，使用具有自动编码的框架，将敏感字符进行转义

XSS和SQL注入攻击的区别：XSS发生在Web网页和应用程序上，SQL注入攻击发生在Web服务器和数据库、磁盘上

Web攻击补充：

Cookie 劫持：Cookie中一般加密保存了用户的登录凭证；如果获取了用户的cookie，则可以不通过密码，就可以直接登录其账户

Cookie劫持的防御：启用Cookie的HttpOnly标识；或者将cookie与客户端IP绑定

缓冲区溢出：

向固定长度的缓冲区中写入超出其预定长度的内容，造成缓冲区数据溢出，从而覆盖缓冲区周围的内存空间

**原因**：各种操作系统和应用软件上存在的缓冲区溢出问题数不胜数，而其带来的影响不容小觑

**后果：**可以导致程序运行失败、系统崩溃以及重新启动等后果

**更严重的后果：**可以执行非授权指令，甚至取得系统特权，进而进行各种非法操作

程序在内存中的存放形式：程序运行时，计算机会在内存区域开辟一段连续的内存块，包括代码段、数据段和堆栈段三部分

**代码段**：文本段，存放程序的机器码和只读数据，一般只读，对该区进行写操作会导致段错误

**数据段（保存静态变量和全局变量）**

已初始化的数据段（保存已初始化的静态变量和全局变量）

.rdata（包含程序中全局可访问的只读数据）

未初始化的数据段（保存未初始化的静态变量和全局变量

**堆栈段**：  
函数栈（包含局部变量、栈帧状态、函数返回地址）

**ESP（栈指针寄存器，extended stack pointer）：**存放系统栈最上面栈帧的栈顶

**EBP（基址指针寄存器，extended base pointer）：**存放系统栈最上面栈帧的栈底

**EIP（指令寄存器，Extended Instruction Pointer）：**该指针永远指向下一条等待执行的指令地址

缓冲区溢出的基本类型：

栈溢出、堆溢出、BSS溢出、格式化串溢出、整数溢出

缓冲区溢出攻击过程：

在程序的地址空间里安排适当的代码（shellcode） ---- 通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行

缓冲区溢出的防御和防范：

及时给程序漏洞打补丁

关闭不需要的特权服务

编写安全的代码（检查输入数据的长度、使用安全的字符串处理函数、对函数参数进行边界检查）

网络安全的防御技术：

IDS、IPS、防火墙、漏洞扫描

防火墙的定义：防火墙是一种用来加强网络之间访问控制的特殊网络互连设备

防火墙核心思想：在不安全的网络环境中构造一个相对安全的子网环境

防火墙目的：在被保护的内网和不安全的非信任网络之间设立唯一的通道，便于监督和控制使用者的操作和数据信息的流入流出

防火墙的特征：保护脆弱的和有缺陷的网络服务、集中化安全管理、加强对网络系统的访问控制、加强隐私、对网络存取和访问进行监控审计

防火墙结构：

外网

|

|

内网-----------------防火墙------------------DMZ（非军事化区）

非军事化区包括FTP服务器、打印服务器、Email服务器、WWW服务器等

防火墙技术（防火墙类型）：

包过滤、应用代理（代理服务）、状态转换、NAT

包过滤技术优点：价格便宜便于安装和使用，网络性能和透明性好

包过滤技术缺点：安全性较低，数据包的源地址、目标地址和端口号都在头部，容易被窃听和假冒

代理服务技术优点：内部网络重要信息不易外泄，可以实施认证、数据加密等功能，安全性较高

代理服务技术缺点：不同的应用层协议必须有单独的代理，不能自动支持新的网络应用，安装使用较为不便需要一定的学习，网络性能差

状态检测防火墙是在动态包过滤的基础上增加了状态检测的机制形成的

优点：高安全性，高效性、应用范围广

缺点：在阻止DDos攻击、病毒传播和高级应用入侵方面力不从心

NAT本身并不是一种安全解决方案，不能提供类似防火墙、包过滤、隧道等技术的安全性，仅仅在包的最外层改变ＩＰ地址。一般会

将NAT集成在防火墙系统之中使用，提供访问控制和地址翻译的功能 。

防火墙的安全部署方案（防火墙体系结构）：

屏蔽路由器、双宿主机模式、屏蔽主机模式、屏蔽子网模式

屏蔽路由器（也称分组过滤路由器）



**将过滤器安装在路由器上或包过滤软件安装在PC机上的防火墙**

屏蔽路由器是目前使用最为广泛的防火墙，其原理很简单：

1、有选择地允许数据分组穿过防火墙，实现内部和外部主机之间的数据交换；

2、作用在网络层和传输层；

3、根据分组的源地址、目的地址、端口号、协议类型等标志确定是否允许数据包通过。满足过滤逻辑的数据包才被转发，否则丢弃。

**缺点**：

在单机上实现，是网络中的“单失效点”。

不支持有效的用户认证、不提供有用的日志，安全性低。

双宿主机



在被保护网络和Internet之间设置一个具有双网卡的堡垒主机，IP层的通信完全被阻止，两个网络之间的通信可以通过应用层数据共享或应用层代理服务来完成，通常采用代理服务的方法，堡垒主机上运行着防火墙软件，可以转发应用程序和提供服务等

**优缺点：**

堡垒主机的系统软件可用于身份认证和维护系统日志，有利于进行安全审计

该方式的防火墙仍是网络的“单失效点”。

隔离了一切内部网与Internet的直接连接，不适合于一些高灵活性要求的场合

屏蔽主机：



一个分组过滤路由器连接外部网络，同时一个运行网关软件的堡垒主机安装在内部网络。通常在路由器上设立过滤规则，使这个堡垒主机成为从外部唯一可直接到达的主机。

屏蔽子网



* 是最安全的防火墙系统，它在内部网络和外部网络之间建立一个被隔离的子网（非军事区，**DMZ**（Demilitarized Zone））
* 在很多实现中，两个分组过滤路由器放在子网的两端，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信
* 通常将堡垒主机、各种信息服务器等公用服务器放于DMZ中
* 堡垒主机通常是黑客集中攻击的目标，如果没有DMZ，入侵者控制堡垒主机后就可以监听整个内部网络的会话

概念：

**入侵(Intrusion)**不仅包括发起攻击的人取得超出范围的系统控制权，也包括收集漏洞信息，造成拒绝访问等对计算机造成危害的行为。

**入侵检测(Intrusion Detection)**即通过从网络系统中的若干关键节点收集并分析信息，监控网络中是否有违反安全策略的行为或者是否存在入侵行为。

**入侵检测系统IDS（Intrusion Detection System）**的概念：

IDS是执行入侵检测的软件或硬件系统

用于检测对网络的攻击

对攻击的积极响应

入侵检测系统的特点：实时性、可扩展性、适应性、安全性、有效性

**入侵检测系统分类**

根据检测方式分：误用检测系统、异常检测系统

根据输入数据来源分：基于主机的入侵检测系统、基于网络的入侵检测系统

根据检测方式分：协议分析、基于状态的检测

根据体系结构分：集中式、分布式

根据工作方式分：在线检测、离线检测

入侵检测信息收集的来源：系统或网络的日志文件、网络流量、系统目录和文件的异常变化、程序执行中的异常行为

**误用检测**

概念：也称为滥用检测，探测与具体特征(Signatures)相匹配的入侵行为，将收集到的信息与特征库匹配，即模式匹配。

优点：

基于已知的入侵行为

安装后立刻就能进行检测

缺点：

需要更新签名库（特征库）

有些攻击能绕过IDS

无法检测未知攻击

**异常检测**

概念：也称为模型检测，需要为用户习惯建立模型。模型为用户定义了行为特征，以及为用户执行正常任务定义了一个基线

优点：

检测以前未发布的攻击

缺点：

用户习惯改变时，必须更新用户模型

很难把特定的攻击与报警相关联

**IDS部署方式**

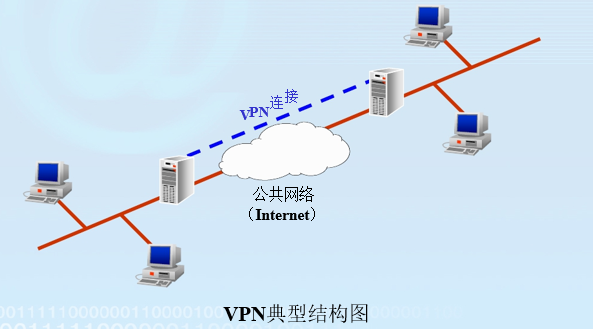
检测器部署位置：

放在边界防火墙之内

放在边界防火墙之外

放在主要的网络中枢

放在一些安全级别需求高的子网



VPN（虚拟专用网络，Virtual Private Network）是指将物

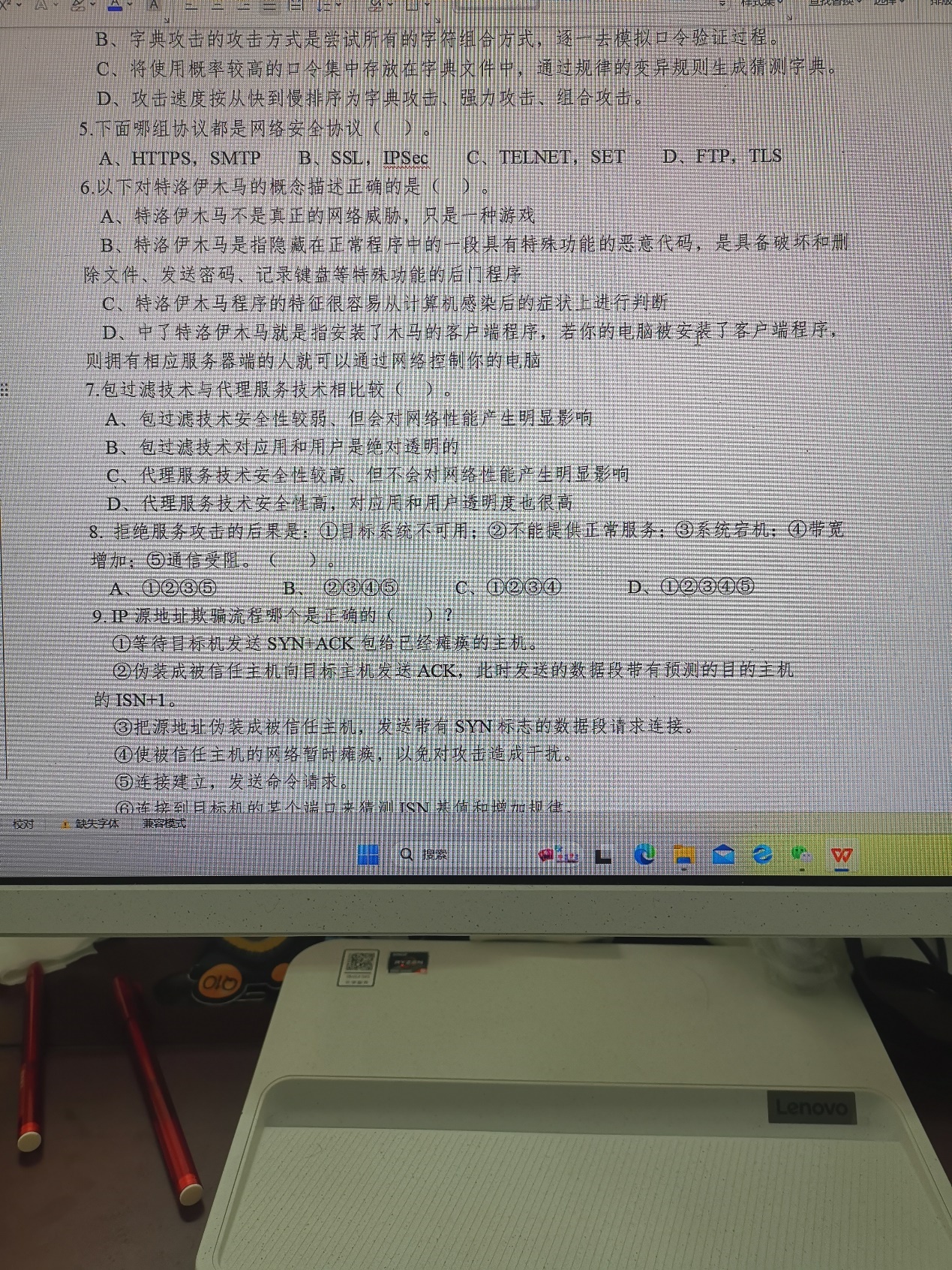
理上分布在不同地点的网络通过公用网络连接成逻辑上的虚

拟子网，并采用认证、访问控制、保密性、数据完整性等在

公用网络上构建专用网络的技术，使得数据通过安全的“加

密管道”在公用网络中传输。（公用网通常指Internet）

VPN关键技术：隧道技术、加解密技术、身份认证技术、密钥管理技术



回答和引申：

选择题5：

B 常见的网络安全协议：SSL IPSec HTTP

SMTP、FTP: 文件传输协议

选择题6：

B 木马是一段隐藏在计算机程序中的恶意代码，具有隐蔽性、欺骗性、自动运行自动恢复等特点

选择题7（防火墙）：

A 包过滤技术优点：价格便宜便于安装和使用，网络性能和透明性好

包过滤技术缺点：安全性较低，数据包的源地址、目标地址和端口号都在头部，容易被窃听和假冒

代理服务技术优点：内部网络重要信息不易外泄，可以实施认证、数据加密等功能，安全性较高

代理服务技术缺点：不同的应用层协议必须有单独的代理，不能自动支持新的网络应用，安装使用较为不便需要一定的学习，网络性能差

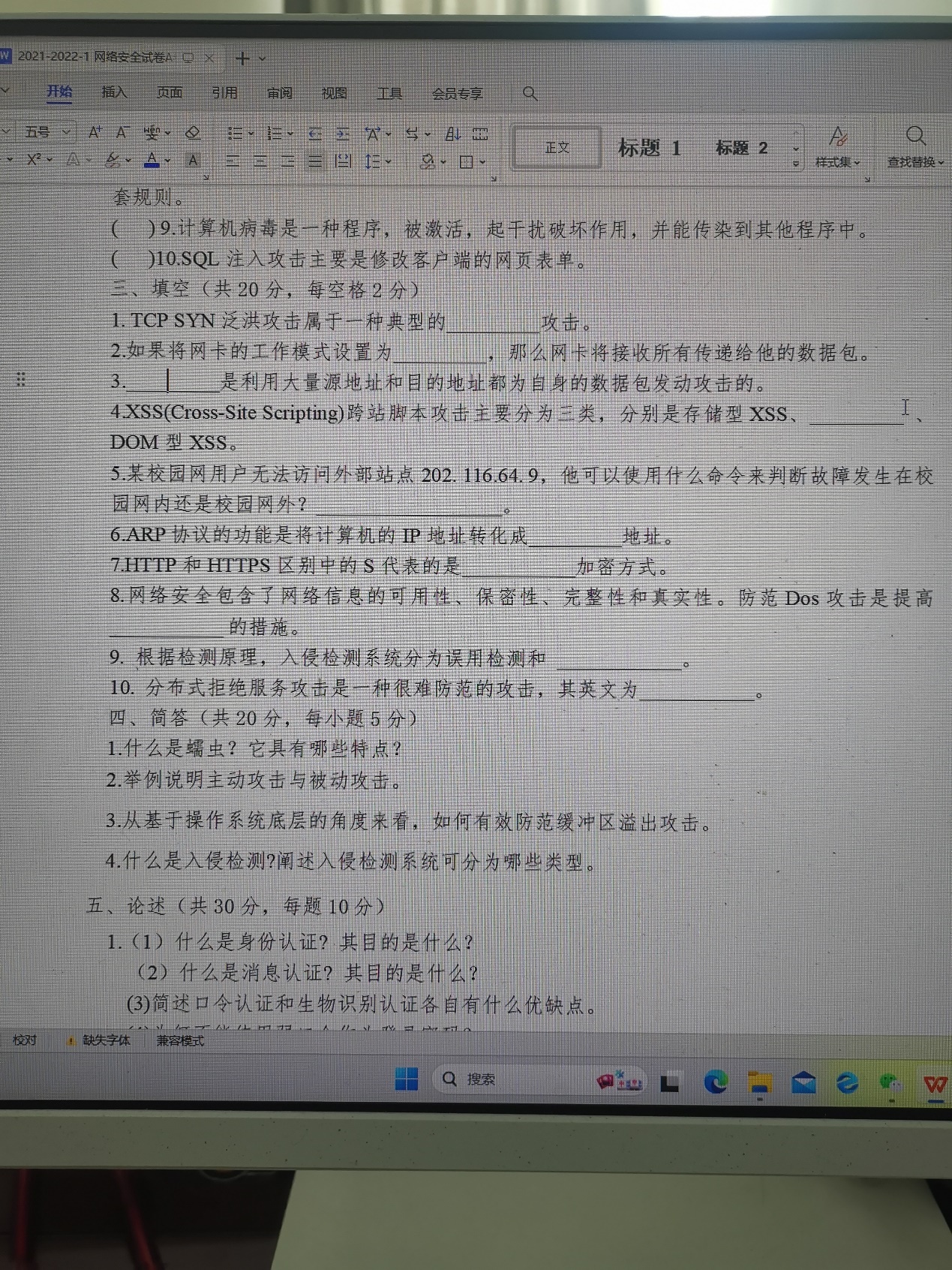
状态检测防火墙是在动态包过滤的基础上增加了状态检测的机制形成的

优点：高安全性，高效性、应用范围广

缺点：在阻止DDos攻击、病毒传播和高级应用入侵方面力不从心

选择题8：

D Dos：一种破坏性攻击，通常利用传输协议弱点、系统漏洞、服务漏洞对目标系统发起大规模进攻，用超出目标处理能力的海量数据包消耗可用**系统资源**、**带宽资源**等，或造成**程序缓冲区溢出**错误，致使其无法处理合法用户的请求，无法提供正常服务，最终致使网络服务瘫痪，甚至系统死机



判断题9：

错误

判断题10：

错误

填空题1：

阻塞类（Dos）

填空题2：

直接模式（单播模式） 网卡的工作模式分为广播模式（接收所有目的地址为广播地址的数据包）、多播传送（接收所有的多播传送帧，而不论它是不是组内成员）、直接模式（工作在直接模式下的网卡只接收目地址是自己 Mac 地址的帧）、混杂模式（接收所有流过网卡的帧）

填空题3：

Land攻击 UDP泛洪：用主机自动回复的服务（如使用UDP协议的chargen和echo）进行攻击

SYN泛洪：利用TCP协议缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽

Land攻击：向目标发送大量源地址和目标地址相同的包

Smurf攻击：将源地址设置为被攻击主机的地址，将目标地址设置为广播地址，不仅影响主机，还影响目标主机的整个网络

填空题4：

反射型XSS

填空题5：

Tracert

填空题6：

MAC

填空题7：

SSL

填空题8：

可用性

填空题9：

异常检测

填空题10：

DDos

简答题1：

蠕虫是一种可以独立运行，能主动寻找感染目标并且能够自动传播的恶意程序。

蠕虫的传播依赖于特定的计算机漏洞，蠕虫由扫描模块、攻击模块、传输模块、负载模块组成。蠕虫不利用文件寄生，不需要将自己复制到宿主程序。

简答题2：

上面有

简答题3：

及时给程序漏洞打补丁

关闭不需要的特权服务

编写安全的代码（检查输入数据的长度、使用安全的字符串处理函数、对函数参数进行边界检查）

简答题4：

上面有

论述题（认证的补充）

认证是用于证实某事是否真实或有效的过程，向对方证实身份的过程

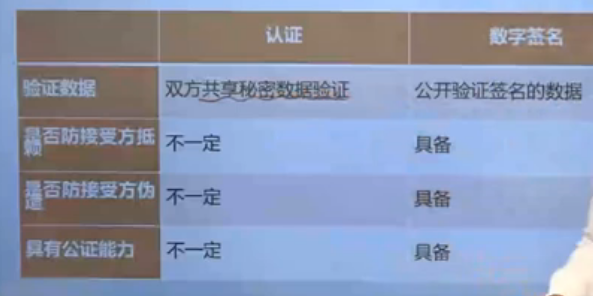
认证的原理是通过核对人或事的参数特征（口令、指纹、密钥）来验证目标的真实性和有效性

认证和加密的区别：

加密用于确保数据的保密性，认证用于确保发送者和接受者的真实性，保障保温的完整性

认证的组成部分：标识、鉴别

认证和数字签名的不同点：



单向认证：只有验证方对被验证方的验证，可分为基于共享密钥和基于挑战响应两种

消息认证的目的如下：

* 消息完整性认证，即验证信息在传送或存储过程中是否被篡改；
* 身份认证，即验证消息的收发者是否持有正确的身份认证符；
* 消息的序号和操作时间等的认证，其目的是防止消息重放或延迟等攻击；
* 确保信息的安全性；
* 信息的发送者是真正的而不是冒充的，即数据起源认证；
* 验证信息在传送过程中未被篡改、重放或延迟等。

身份认证也称为"身份验证"或"身份鉴别"，它是指在计算机及计算机网络系统中确认操作者身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

优点：口令算法足够复杂的情况下，黑客得到口令文件想要通过散列值计算出原始口令这种情况是不可能的，如果使用动态口令那安全性会进一步提升。

缺点：只使用单因素认证，完全依赖于口令，而用户只会设置容易记忆、容易被破解的口令，并不会按照开发人员设计的口令复杂度进行设置，这种情况就容易被离线字典攻击。

生物识别认证的优缺点：

优点：安全性高、便利性强、适用范围广

缺点：技术成本高、识别率有限、隐私问题