一、单选题（每题 2 分，共 20 分）

1、 以下攻击方式中属于被动攻击的是（ ）。

A. 搭线窃听 B. 拒绝服务 C. 消息重放 D. 身份假冒

2、 以下对安全服务分层部署描述错误的是（ ）。

A. 可基于用户制定安全策略和措施；B. 可不依赖于操作系统提供安全服务；C. 对数据实际含义有充分理解，便于采取针对性的保护；D. 实现的效率高，兼容性好。

3、 在 TCP 连接中，ACK 序列号用于确认收到数据包的数据长度，SYN 序列号表示对方已接收的数据包的数据长度，假定客户端向服务器端发出的数据包中 ACK=1，SYN=1，数据包中数据长度为 725，服务器正常接收客户端的数据并回复，在回复数据包中 ACK 序列号的值为（ ）。

A. 725 B. 726 C. 1 D. 2

4、 通过构造目的地址和源地址均为目标主机地址的特殊 TCP SYN 攻击包，导致目标主机建立空连接的攻击被称为（ ）。

A. IP 欺骗攻击 B. SYN 泛洪攻击 C. Land 攻击 D. 序列号猜测攻击

5、 状态检测防火墙工作在 OSI 网络模型的（ ）。

A. 链路层 B. 传输层 C. 会话层 D. 应用层

6、 在强制访问控制模型中，为保障信息的机密性应采用的访问控制策略是（ ）。

A. 向上读，向上写 B. 向上读，向下写 C. 向下读，向下写 D. 向下读，向上写

7、 采用包过滤防火墙很难屏蔽的端口扫描方式是（ ）。

A. TCP Connect 扫描 B. TCP SYN 扫描 C. TCP FIN 扫描 D. ICMP 错误报文扫描

8、 以下不属于入侵检测系统功能的是（ ）。

A. 监测并分析用户和系统的行为活动；B. 核查系统配置和漏洞；C. 评估系统关键资源和数据文件的完整性；D. 执行访问控制策略，限制用户的网络访问。

9、 攻击者通过缓冲区溢出植入并执行 Shellcode 必须修改的寄存器是（ ）。

A. EBP B. ESS C. ESP D. EIP

10、 通过链接的方式将自身隐藏在宿主文件中的恶意代码是（ ）。

A. 文件型病毒 B. 木马 C. 蠕虫 D. 流氓软件

二、填空题（每空 1 分，共 20 分）

1、 在信息安全保障技术框架（IATF）中，将攻击类型分为主动攻击、被动攻击、_____、_____、_____五种类型。

2、 常见的网络地址转换（NAT）实现方式包括：_____、_____、和_____。

3、 虚拟子网（VLAN）按照不同的划分方式，可以分为_____、_____、_____、_____和_____。

4、 常见的访问控制模型包括：_____、_____、_____。

5、 网络扫描按照采用的**技术和目的**不同可以分为_____、和_____。

6、 入侵检测依据**检测方法**的不同可以分为_____和_____。

7、 广义的计算机病毒可以分为_____和_____。

三、判断题（每题 1 分，共 10 分）

1、 系统的可靠性是 ISO7498 中定义的五种基本安全服务之一。（ ）
2、 在网络层可以实现进程到进程的安全通信。（ ）
3、 子网屏蔽防火墙需要由两个包过滤路由器和一个堡垒主机构成。（ ）
4、 物理隔离的情况下内外网不能够进行数据交换。（ ）
5、 ACL 是以主体为中心建立的访问控制列表。（ ）
6、 基本 RBAC 参考模型中体现了责任分离的安全原则。（ ）
7、 通过主机扫描可以发现远程主机上开放的服务。（ ）
8、 基于异常的入侵检测可以准确检测已有的入侵行为。（ ）
9、 利用系统漏洞进行自动传播是蠕虫程序的典型特征。（ ）
10、 目前使用最为广泛病毒检测技术为启发式扫描检测。（ ）

四、 简答题（每小题 5 分，共 20 分）

1、 在信息安全体系中，什么是安全服务？什么是安全机制？如何理解安全服务和安全机制之间的关系？（5 分）

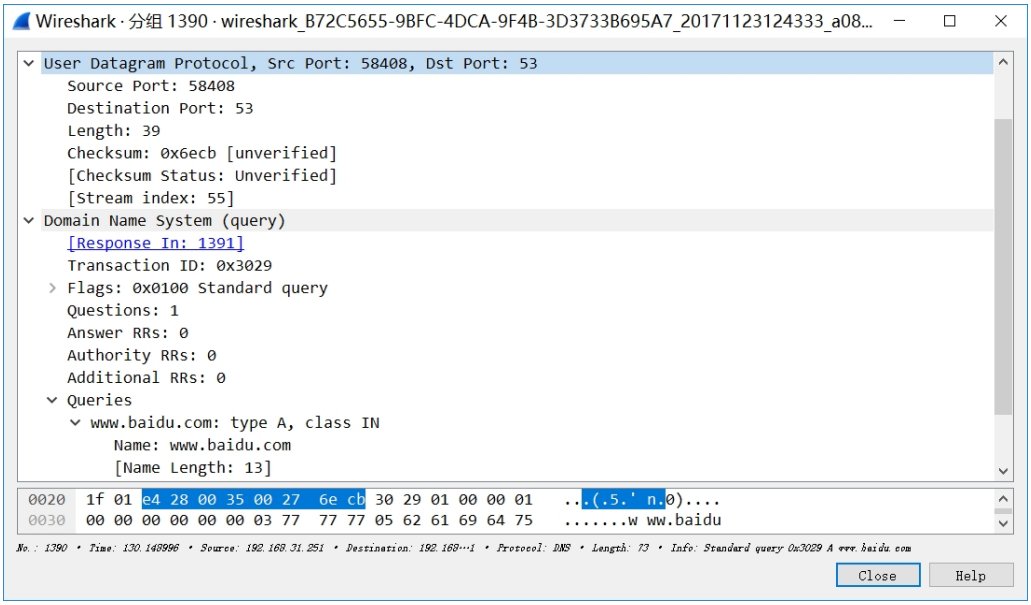
2、 需要实现对用户网络访问行为的控制应使用什么类型的防火墙技术？简述该技术的特点（优缺点）。（5 分）

3、 假定用户 Alice 和用户 Bob 通过离线方式已经安全协商好用于双方身份认证的共享密钥 K_{ab}，请设计一个简单的身份认证协议，要求协议可抵抗重放攻击并同时完成用于临时通信的会话密钥 Ks 的协商，写出协议过程并进行简要说明。（5 分

4、 计算机病毒程序通常包含哪几个功能模块？模块的基本功能是什么？（5 分）

五、分析题（每小题 15 分，共 30 分）

1. 在局域网中捕获到一个以太网帧，此帧的全部数据如下图所示，请对照相关协议的数据结构图，回答以下问题：



A. 此数据帧中采用的传输层协议类型是什么？封装的应用层协议类型是什么？该数据帧的用途和目的是什么？（6 分）

B. 收到该数据帧的主机会进行何种响应，收到响应的主机会进行什么样的处理？（3 分）

C. 利用该协议攻击者可以实施何种攻击，请简述攻击过程。（6 分）

2. 阅读以下用于口令验证的代码，并回答代码后的问题。（15 分）

```
#include <stdio.h>
```

```
#include "string.h"
#define PASSWORD "1234567"
int verify(char *password){
        int auth;
        char buff[8];
        auth = strcmp(password, PASSWORD);
        strcpy(buff, password);
        return auth;
}
int main(void){
      int flag = 0;
      char pass[1024];
      while(1){
                printf("enter the password:\t");
                scanf("%s", pass);
                flag = verify(pass);
                if(flag)
                      printf("password incorrect!\n");
                else{
                      printf("congratulation!\n");
                      break;
                      }
              }
   }
```

（1） 说明在 main( )中调用 verify( )时栈是如何工作的？（6 分）

（2） 试分析：

1）如果输入的字符串为“qqqqqqqq”验证是否会通过？请简要说明理由。（6 分）

2） 怎样修改才能够保证程序是安全的？请简要说明理由。（3 分）