1.将网卡设置在_____模式下，就可以捕获流经网卡的数据包。

混杂（杂错）

2.通过修改 MAC 地址的方法发起的攻击叫做_____。

MAC 地址欺骗

3.从技术上划分，入侵检测系统有两种模型 _____和_____。

异常检测　　滥用检测

4.木马程序一般由两部分组成，分别是_____和_____。

控制端　　被控制端

5.IPSec 在 Internet 的_____层提供安全服务，为_____提供了安全保障。

网络层　　私有信息通过公众网络

6.查看本机 IP 地址的命令是_____，查看本机开放端口的命令是_____，查看远程主机连通性的命令是_____。

ipconfig　　netstat　　ping

7.P2DR 模型是一种常用的网络安全模型，包括四个主要部分 _____、_____、_____和_____。

安全策略　　防护　　检测　　响应

8.一个完善的 DDoS 攻击体系包括_____、_____、_____和_____。

攻击者　　主控端　　代理端　　被攻击者

9.无线网络中的 AP 是指_____。

无线接入点

10.网络的基本功能有_____、_____和_____。

资源共享　　通信　　远程控制

11.导致网络安全威胁的原因不外乎以下三个_____、_____和_____。

系统的开放性　　系统的复杂性　　人的因素

12. 802.11 协议是_____组织的标准，在 802.11 协议中定义了两种类型的设备，分别是_____和_____。

IEEE　　无线终端　　无线接入点

13.计算机蠕虫包括三个模块 _____、_____和_____。

扫描模块　　感染模块　　执行功能模块

14.802.11 协议的 MAC 层采用的介质访问控制方法是_____。

CSMA/CA

15.IPsec 有两种工作模式，分别是_____和_____。

传输模式　隧道模式

16.NAT 有三种类型 _____、_____和_____。

静态 NAT　NAT 池　端口 NAT（PAT）

17.IPSec 定义的两种通信保护机制分别是_____机制和_____机制。

AH　ESP

18.木马传播的方式主要有两种 _____和_____。

E-mail　软件下载

19.垃圾邮件从内容上主要分为_____和_____。

广告邮件　宣传邮件

20.以太网环境有_____和_____两种基本类型。

共享以太网　交换以太网

21._____和_____可用于嗅探交换机上的通信。

ARP 欺骗　MAC 泛滥

22.应用层常见的攻击模式有_____、_____和_____。

带宽攻击　缺陷攻击　控制目标主机

23.IPSec 工作在_____层，SSL 工作在_____层，MPLS 工作在_____层。

网络层　传输层　应用层

24.无线局域网的结构有_____、_____和_____三种模式。

Infrastructure 模式　Ad Hoc 模式　混和模式

25. 802.11 协议中定义了两种类型的设备，分别是_____和_____。

无线终端　接入点

26.以太网络的介质访问控制方法是_____，无线局域网 802.11 协议的介质访问控制方法是_____。

CSMA/CD　CSMA/CA

27.无线局域网有_____、_____和_____安全需求。

数据机密性　数据完整性　访问控制

28.入侵检测系统按照检测的数据来源可以分为_____和_____两种。

HIDS　NIDS

29.入侵检测系统根据工作方式可分为_____和_____。

离线检测　在线检测

30.异常检测技术的误警率比滥用检测_____，漏警率比滥用检测_____。

高　低

31.防火墙与 IPS 联动的方式有_____和_____。

通过开放接口实现联动　通过紧密集成实现联动

32.IPS 根据部署方式可以分为 3 类，分别是_____、_____和_____。

NIPS　HIPS　AIPS

33.拒绝服务攻击具有_____、_____、_____等特点。

易于实现　难于防范　难于追查

34.拒绝服务攻击的危害主要体现在_____、_____、_____。

破坏网络或系统的可用性　经济损失　信誉损失

35.DDoS 攻击的过程是_____、_____、_____。

搜集目标信息　占领傀儡机　实际攻击

36.DDoS 的攻击防御中，最关键的技术是如何分辨_____和_____。

合法业务流量　恶意业务流量