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**