**1. 下列哪种病毒能对计算机硬件产生破坏？（） 参考答案：（C）**

**窗体顶端**

**A. 维金   
B. CODE RED   
C. CIH   
D. 熊猫烧香**

**2. 以下哪些方法对防范SQL注入攻击无效？（） 参考答案：（C）**

**窗体顶端**

**A. 采用参数化查询方式，进行开发   
B. 对数据库系统的管理权限进行严格的控制   
C. 通过网络防火墙严格限制Internet用户对web服务器的访问   
D. 对web用户输入的数据进行严格的过滤**

**3. 在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（ ） 参考答案：（C）**

**窗体顶端**

**A. 产生日志的数量   
B. 较低的价格   
C. 攻击减少的速度   
D. 假阳性的减少量**

**4. 以下哪些软件是用于加密的软件？（ ） 参考答案：（D）**

**窗体顶端**

**A. DES   
B. SHA   
C. EFS   
D. PGP**

**5. 关于PPP协议下列说法正确的是：（ ） 参考答案：（B）**

**窗体顶端**

**A. PPP协议是物理层协议   
B. PPP协议支持的物理层可以是同步电路或异步电路   
C. PPP协议是在HDLC协议的基础上发展起来的   
D. PPP主要由两类协议组成：链路控制协议族（LCP）和网络安全方面的验证协议族（PAP和CHAP）**

**6. 无论是哪一种Web 服务器，都会受到HTTP 协议本身安全问题的困扰，这样的信息系统安全漏洞属于：（ ） 参考答案：（A）**

**窗体顶端**

**A. 运行型漏洞   
B. 开发型漏洞   
C. 设计型漏洞   
D. 以上都不是**

**7. Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle 9i 支持5 种命名方法，请选择错误的选项。（ ） 参考答案：（B）**

**窗体顶端**

**A. 本地命名和目录命名   
B. DNS和内部命名   
C. 主机命名和外部命名   
D. Oracle 名称（Oracle Names）**

**8. 以下哪一项不是流氓软件的特征？（ ） 参考答案：（A）**

**窗体顶端**

**A. 通常会显示下流的言论   
B. 通常添加驱动保护使用户难以卸载   
C. 通常会启动无用的程序浪费计算机的资源   
D. 通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装**

**窗体底端**

**9. 网上营业厅中间件如果启用了SSL，应采用不低于（）版本的SSL，采用经国家密码管理局认可的密码算法 ） 参考答案：（A）**

**窗体顶端**

**A. 3.0   
B. 2.5   
C. 2.0   
D. 3.1**

**窗体底端**

**10. 造成缓冲区溢出漏洞的原因有（ ）。 参考答案：（A,B,D）**

**窗体顶端**

**A. 某些开发人员没有安全意识   
B. 某些高级语言没有缓冲区边界检查   
C. 用户输入数据太长，超出系统负荷   
D. 软件测试不够严格**

**11. 统一威胁管理系统（UTM）描述正确的是（ ） 参考答案：（A,B,D）**

**窗体顶端**

**A. 部署UTM可以有效降低成本   
B. 部署UTM可以降低信息安全工作强度   
C. 部署UTM可以降低安全设备集成带来的风险   
D. 部署UTM可能降低网络性能和稳定性**

**窗体底端**

**12. 以下关于宏病毒说法不正确的是（ ）。 参考答案：（A,C,D）**

**窗体顶端**

**A. 宏病毒主要感染可执行文件　   
B. 宏病毒仅向办公自动化程序编制的文档进行传染   
C. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区　　   
D. CIH病毒属于宏病毒**

**窗体底端**

**13. 使用sudo工具可以对Unix/Linux系统中用户可运行的命令进行控制以增加安全性，它的特性包括（ ）。参考答案：（A,B,C,D）**

**窗体顶端**

**A. 需要授权许可   
B. 可以为系统管理员提供配置文件   
C. 能够限制指定用户在指定主机上运行某些命令   
D. 可以提供日志记录**

**窗体底端**

**14. 下列木马程序可能采用的激活方式有（ ）。 参考答案：（A,C）**

**窗体顶端**

**A. 修改注册表中的HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion下以“run”开头的键值   
B. 将木马程序复制在用户的桌面上   
C. 注册为系统服务   
D. 感染系统中所有的exe和html文件**

**窗体底端**

**15. 关于网络入侵检测系统，以下描述正确的是（） 参考答案：（B,C,D）**

**窗体顶端**

**A. 能够适用于加密环境   
B. 不会增加系统开销   
C. 对带宽的要求较高   
D. 其部署不影响现有网络架构**

**窗体底端**

**16. 无法用于对Windows系统口令进行暴力破解的工具有（ ） 参考答案：（A,D）**

**窗体顶端**

**A. NMAP   
B. Nessus   
C. X-Scan   
D. AppScan**

**窗体底端**

**17. 下面支持WPA加密方式的无线局域网标准有（ ）。 参考答案：（B,D）**

**窗体顶端**

**A. 802.11b   
B. 802.11i   
C. 802.11a   
D. 802.11n**

**窗体底端**

**18. 以下关于DOS攻击的描述，说法正确的有（ ） 参考答案：（B,C）**

**窗体顶端**

**A. 以窃取目标系统上的机密信息为目的   
B. 不需要侵入对方系统内部   
C. 导致目标系统无法处理正常用户的请求   
D. 如果目标系统没有漏洞，远程攻击就不可能成功**

**窗体底端**

**19. 选出可以被暴力破解的协议（ ） 参考答案：（A,B,C）**

**窗体顶端**

**A. POP3   
B. SNMP   
C. FTP   
D. TFTP**

**窗体底端**

**20. 关于HTTp协议说法不正确的是（） 参考答案：（B）**

**窗体顶端**

**A. http协议是明文传输的   
B. http协议是可靠的有状态的协议   
C. http协议主要有请求和响应两种类型   
D. http协议，在web应用中，可以有get、post、delete等多种请求方法，但是最常用是get和post**

**1. 下面哪一种说法是不正确的？（） 参考答案：（B）**

**窗体顶端**

**A. 虚拟专用网是利用公众网资源为客户构成专用网的一种业务。   
B. 使用VPN后就不需要再使用防火墙和入侵检测系统，它可以提供完善的安全保障。   
C. VPN可以看作是企业网在Internet上的延伸，通过Internet中一个私用的通道来创建一个安全的私有连接，VPN通过这个安全通道将远程用户，公司分支机构，公司业务合作伙伴等公司的企业网连接起来，构成一个扩展的公司企业网。   
D. VPN技术的关键主要体现在两个方面：相关的隧道协议和数据安全协议。**

**窗体底端**

**2. IP报文头的最前端是下列哪一个选项？（） 参考答案：（D）**

**窗体顶端**

**A. 报文头长度   
B. 标识   
C. 目的地址   
D. 版本**

**窗体底端**

**3. 网络渗透中第一步要做的是什么工作？（） 参考答案：（B）**

**窗体顶端**

**A. 加载木马   
B. 信息收集   
C. 隐藏自己   
D. 溢出**

**窗体底端**

**4. 下列不属于特征代码法检测病毒的优点的是（） 参考答案：（D）**

**窗体顶端**

**A. 检测准确快速   
B. 可识别病毒的名称   
C. 误报警率低   
D. 可检测隐蔽型病毒**

**窗体底端**

**5. 下列哪一项不存在于IDS的应用规则中？（） 参考答案：（C）**

**窗体顶端**

**A. 源IP地址   
B. 目的IP地址   
C. 日志条目   
D. 目的端口**

**窗体底端**

**6. 关于防火墙和VPN的使用，下面哪一种说法不对？（） 参考答案：（D）**

**窗体顶端**

**A. 配置VPN网关防火墙的一种方法是把它们并行放置，两者独立。   
B. 配置VPN网关防火墙的一种方法是把它们串行放置，防火墙在广域网一侧，VPN在局域网一侧。   
C. 配置VPN网关防火墙的一种方法是把它们串行放置，防火墙在局域网一侧，VPN在广域网一侧。   
D. 配置VPN网关防火墙的一种方法是把它们并行放置，两者要互相依赖。**

**窗体底端**

**7. 不同厂商的IDS系统之间需要通信，这种通信格式是（）。 参考答案：（A）**

**窗体顶端**

**A. IDMEF   
B. IETF   
C. IEEE   
D. IEGF**

**窗体底端**

**8. 特洛伊木马攻击的威胁类型属于()。 参考答案：（B）**

**窗体顶端**

**A. 授权侵犯威胁   
B. 植入威胁   
C. 溢出威胁   
D. 旁路控制威胁**

**窗体底端**

**9. （）系统是一种自动检测远程或本地主机安全性弱点的程序。 参考答案：（C）**

**窗体顶端**

**A. 入侵检测   
B. 防火墙   
C. 漏洞扫描   
D. 入侵防护**

**窗体底端**

**10. 在Windows以及Unix/Linux操作系统上，用来进行域名查询的命令工具是下列哪一项？（） 参考答案：（D）**

**窗体顶端**

**A. ping   
B. tracert/traceroute   
C. ipconfig/ifconfig   
D. nslookup**

**窗体底端**

**11. 冷备份的优点不包括（）。 参考答案：（C）**

**窗体顶端**

**A. 是非常快速的一种备份方法   
B. 容易归档   
C. 节省磁盘空间   
D. 恢复时间比热备份快**

**窗体底端**

**12. 利用（）可以防止共享文件可能造成的破坏，但会使系统开销很大。 参考答案：（A）**

**窗体顶端**

**A. 存取控制表   
B. 隐蔽文件目录   
C. 定义不同用户对文件的使用权   
D. 用户对树形目录中目录和文件规定权限**

**窗体底端**

**13. 在SQLServer2008中，某数据库中有教师表(教师号,姓名,职称)，其中教师号的数据类型是整型，其他均为字符类型。若教师表中当前没有数据，用户执行下列语Ⅰ.BEGINTRANSACTIONT1;Ⅱ.INSERTINTO教师表VALUES(1000,“张三”,“助教”);Ⅲ.INSERTINTO教师表VALUES(1001,“王二”,“助教”);Ⅳ.COMMITT1;Ⅴ.BEGINTRANSACTIONT2;Ⅵ.INSERTINTO教师表VALUES(1002,“王三”,“讲师”);Ⅶ.INSERTINTO教师表VALUES(1003,“李四”,“讲师”);Ⅷ.COMMITT2;在Ⅶ执行的时候数据库所在的服务器突然掉电，当数据库系统重新启动后，教师表中包含的数据条数为（）。 参考答案：（C）**

**窗体顶端**

**A. 4条   
B. 3条   
C. 2条   
D. 0条**

**窗体底端**

**14. 下列哪个参数用于释放本机已经获得的IP地址？（） 参考答案：（B）**

**窗体顶端**

**A. ipconfig/all   
B. ipconfig/release   
C. ipconfig/renew   
D. ipconfig/flushdns**

**窗体底端**

**15. 以下不属于注册表根键的是（）。 参考答案：（A）**

**窗体顶端**

**A. SYSTEM   
B. HKEY\_LOCAL\_MACHINE   
C. KEY\_DYN\_DATA   
D. HKEY\_CLASSES\_ROOT**

**窗体底端**

**16. 以下哪一项属于Web服务器上的漏洞（）。 参考答案：（C）**

**窗体顶端**

**A. 客户在服务器上可以得到要访问的文件等数据   
B. 远程用户可以向服务器发送信息   
C. 某些人可以进入到主机系统，对系统文件进行操作   
D. 对从网上下载的Web服务器谨慎使用**

**窗体底端**

**17. IP地址欺骗是（）。 参考答案：（C）**

**窗体顶端**

**A. 编写一段程序进行欺骗   
B. 设置一个路由器来代替一台机器   
C. 伪造某台主机的IP地址的技术   
D. E-mail欺骗**

**窗体底端**

**18. http服务使用的端口为（）。 参考答案：（A）**

**窗体顶端**

**A. 80   
B. 21   
C. 23   
D. 53**

**窗体底端**

**19. 一般而言，Internet防火墙是建立在一个网络的（）。 参考答案：（C）**

**窗体顶端**

**A. 内部子网之间传送信息的中枢   
B. 每个子网的内部   
C. 内部网络与外部网络的交叉点   
D. 部分内部网络与外部网络的结合处**

**窗体底端**

**20. 同时具有安全性和高效性的防火墙技术是（）。 参考答案：（C）**

**窗体顶端**

**A. 包过滤防火墙   
B. 代理服务器   
C. 状态检测防火墙   
D. 内容过滤防火墙**

**窗体底端**

**21. 下列加密算法中不是国产加密算法的是（）。 参考答案：（D）**

**窗体顶端**

**A. SM4算法   
B. ZUC算法   
C. SSF33算法   
D. RSA算法**

**窗体底端**

**22. HTTPS的安全基础是（）。 参考答案：（A）**

**窗体顶端**

**A. SSL   
B. VPN   
C. ACL   
D. DES**

**窗体底端**

**23. 为了保证数据库应用系统正常运行，数据库管理员在日常工作中需要对数据库进行维护。下列一般不属于数据库管理员日常维护工作的是()。 参考答案：（C,D）**

**窗体顶端**

**A. 数据内容的一致性维护   
B. 数据库备份与恢复   
C. 数据库安全性维护   
D. 销售公司的防火墙产品**

**窗体底端**

**24. 数据信息是否被篡改由（）技术来判断。 参考答案：（A）**

**窗体顶端**

**A. 数据完整性控制   
B. 身份识别   
C. 访问控制   
D. 入侵检测**

**窗体底端**

**25. 下列可被用来进行无线接入点（AP）通信加密的有（）。 参考答案：（B）**

**窗体顶端**

**A. MD5   
B. WEP   
C. SSL   
D. HASH**

**窗体底端**

**26. 下列不属于msconfig功能的是（）。 参考答案：（B）**

**窗体顶端**

**A. 管理系统启动项   
B. 查看本机IP地址   
C. 管理系统服务   
D. 查看BOOT.ini、win.ini、system.ini等**

**窗体底端**

**27. 在Web服务器上安装的基于主机的IDS，检测以下（）攻击最有效。 参考答案：（A）**

**窗体顶端**

**A. 非法登陆   
B. IIS开启FTP服务   
C. 分布式拒绝服务攻击   
D. 对防火墙的连续端口扫描**

**窗体底端**

**28. 一个栈的输入序列为12345，则以34开头的栈的输出序列的是（）。 参考答案：（B）**

**窗体顶端**

**A. 34125   
B. 34215   
C. 34152   
D. 34512**

**窗体底端**

**29. 采用Windows验证方式登录时，只要用户通过了Windows用户账户验证，就可以（）到SQLServer数据库服务器。 参考答案：（A）**

**窗体顶端**

**A. 连接   
B. 集成   
C. 控制   
D. 转换**

**窗体底端**

**30. 下面（）是流行的加壳鉴别工具。 参考答案：（C）**

**窗体顶端**

**A. superscan   
B. peid   
C. upxshell   
D. Armadillo**

**窗体底端**

**31. 增加主机抵抗DoS攻击能力的方法之一是（）。 参考答案：（A）**

**窗体顶端**

**A. 缩短SYNTimeout时间   
B. 调整TCP窗口大小   
C. 增加SYNTimeout时间   
D. 不进行IP-MAC绑定**

**窗体底端**

**32. 较新版本的unix系统日志文件通常是存放在（）。 参考答案：（B）**

**窗体顶端**

**A. /var/log   
B. /var/adm   
C. /etc/   
D. /var/run**

**窗体底端**

**33. 用一个特别打造的SYN数据包，它的原地址和目标地址都被设置成某一个服务器地址。这样将导致接收服务器向他自己的地址发送SYN-ACK信息，结果这个地址又发回ACK信息并创建一个空连接，被攻击的服务器每接收到一个这样的连接就将其保存，直到超时，这种拒绝服务攻击是下列中的（）。 参考答案：（D）**

**窗体顶端**

**A. SYNFlooding攻击   
B. Teardrop攻击   
C. UDPStorm攻击   
D. Land攻击**

**窗体底端**

**34. 属于被动攻击的恶意网络行为是（）。 参考答案：（B）**

**窗体顶端**

**A. 缓冲区溢出   
B. 网络监听   
C. 端口扫描   
D. IP欺骗**

**窗体底端**

**35. 保障信息安全最基本、最核心的技术是（）。 参考答案：（A）**

**窗体顶端**

**A. 信息加密技术   
B. 信息确认技术   
C. 网络控制技术   
D. 反病毒技术**

**窗体底端**

**36. 向有限的空间输入超长的字符串是哪一种攻击手段（）。 参考答案：（A）**

**窗体顶端**

**A. 缓冲区溢出   
B. 网络监听   
C. 拒绝服务   
D. IP欺骗**

**窗体底端**

**37. 在浏览器查看网页时出现403错误可能的原因是（）。 参考答案：（C）**

**窗体顶端**

**A. 页面源代码错误   
B. 与数据库连接错误   
C. 权限不足   
D. 文件不存在**

**窗体底端**

**38. 用Nmap扫描时，只想知道都有哪些主机正在运行的时候使用（）参数。 参考答案：（B）**

**窗体顶端**

**A. —sA   
B. —sP   
C. —sS   
D. —sU**

**窗体底端**

**39. 常见的网络攻击活动隐藏不包括（）。 参考答案：（A）**

**窗体顶端**

**A. 网络通信隐藏   
B. 目录文件隐藏   
C. 进程活动隐藏   
D. 网络连接隐藏**

**窗体底端**

**40. cookie的HttpOnly属性的作用（）。 参考答案：（C）**

**窗体顶端**

**A. 防止SQL注入   
B. 防止目录浏览   
C. 防止XSS攻击   
D. 防止跨域攻击**

**窗体底端**

**41. 下面哪些是LINUX操作系统的特点（）。 参考答案：（A,B,C,D）**

**窗体顶端**

**A. Linux支持多任务   
B. Linux支持多用户会话   
C. Linux可以提供分层文件系统   
D. Linux可以提供广泛的网络功能，支持大多数互联网通信协议和服务**

**窗体底端**

**42. 一个不易破解的口令至少满足（）。 参考答案：（B,D）**

**窗体顶端**

**A. 口令为123456   
B. 口令长度至少有6个字符长   
C. 用一些个人信息如生日等方便记忆   
D. 口令中取一些非字母的特殊字符**

**窗体底端**

**43. 拥有CAP-AUDIT特权可以（）。 参考答案：（A,C）**

**窗体顶端**

**A. 操作安全审计机制   
B. 超越自主存取控制读检查   
C. 写各种审计记录   
D. 安装或卸下一个文件系统**

**窗体底端**

**44. 以下模块是属于Unix/Linux安全模块的是（）。 参考答案：（A,B,C,D）**

**窗体顶端**

**A. SELinux   
B. DTELinux   
C. Openwall   
D. LIDS**

**窗体底端**

**45. BLP模型的安全策略包括（）。 参考答案：（C,D）**

**窗体顶端**

**A. 完整性保护   
B. 密码保护   
C. 强制访问控制   
D. 自主访问控制**

**窗体底端**

**46. 以下属于防火墙组成部分的是（）。 参考答案：（A,C,D）**

**窗体顶端**

**A. 包过滤   
B. 数据加密   
C. 应用网关   
D. 服务访问政策**

**窗体底端**

**47. 以下算法不属于非对称算法的是（）。 参考答案：（A,C）**

**窗体顶端**

**A. DES   
B. RSA   
C. IDEA   
D. Elgamal**

**窗体底端**

**48. 下列选项那些是壳对程序代码的保护方法（）。 参考答案：（A,C,D）**

**窗体顶端**

**A. 加密   
B. 指令加花   
C. 反跟踪代码   
D. 限制启动次数**

**窗体底端**

**49. 下面那个工具具有ARP嗅探功能（）。 参考答案：（B,C,D）**

**窗体顶端**

**A. hydra   
B. cain   
C. ettercap   
D. dsniff**

**窗体底端**

**50. 下列哪种方法能够用来防御CSRF漏洞（）。 参考答案：（A,B,C）**

**窗体顶端**

**A. 判断referer   
B. 使用验证码   
C. 使用一次性随机签名   
D. 使用$\_REQUEST获取客户端数据**

**窗体底端**

**51. 在LINUX系统中，Linux超级管理员用户root的宿主目录位于（ ）。 参考答案：（B）**

**窗体顶端**

**A. /boot   
B. /root   
C. /home/root   
D. /workspace**

**窗体底端**

**52. 在LINUX系统的引导过程中，（ ）脚本用于指定系统默认的运行级别。 参考答案：（B）**

**窗体顶端**

**A. init   
B. inittab   
C. rc.sysinit   
D. rc.local**

**窗体底端**

**53. 在Linux系统中，root用户通过crontab设置了”30 6 \* \* 1-5 /opt/mytar.sh”的计划任务条目，则mytar.sh脚本将会在（）被执行。（选择一项） 参考答案：（B）**

**窗体顶端**

**A. 每周一至周五晚上的18：30分 b   
B. 每周一至周五早上的06：30分   
C. 每个月初1～5日早上06：30分   
D. 1～6月份每天晚上的18：30分**

**窗体底端**

**54. 在Linux服务器中，查看用户vanzk密码记录的操作及输出如下所示： [root@localhost ~]#grep vanzk /etc/shadow vanzk:!!$1$fKuFV9X8$VxFk0Ergj4uzP9UZGnleb.:15771:0:99999:7::: 则据此可判断用户vanzk的帐号（）。 参考答案：（C）**

**窗体顶端**

**A. 每次设置新密码后，有效期为7天，过期后必须重设   
B. 其uid为0，具有与root用户一样的权限   
C. 因密码被锁定而无法登陆   
D. d) 使用的密码长度超过8位，安全性较高**

**窗体底端**

**55. 在LINUX服务器中，若要查询YUM仓库内wireshark软件包的详细描述信息，可以执行（）操作。 参考答案：（C）**

**窗体顶端**

**A. yum list|grep wireshark   
B. yum list wireshark   
C. yum info wireshark   
D. yum search wireshark**

**窗体底端**

**56. 针对系统内部的对象，Windows有两种访问控制形式。这两中访问控制形式是（） 参考答案：（B）**

**窗体顶端**

**A. 自主访问控制和强制访问控制   
B. 自主访问控制和特权访问控制   
C. 强制访问控制和特权访问控制   
D. 强制访问控制和管理员访问控制**

**窗体底端**

**57. 下列选项中，不属于注册表中的六个根键的是（） 参考答案：（D）**

**窗体顶端**

**A. HKEY\_CURRENT\_USER   
B. HKEY\_USERS   
C. HKEY\_LOCAL\_MACHINE   
D. HKEY\_PROGRAMMING\_DATA**

**窗体底端**

**58. 为了避免用户应用程序访问或修改关键的操作系统数据，Windows使用了两种处理器访问模式，这两种模式为（） 参考答案：（C）**

**窗体顶端**

**A. 修复模式和用户模式   
B. 进程模式和内核模式   
C. 内核模式和用户模式   
D. 线程模式和网络模式**

**窗体底端**

**59. 下列关于windows进程构成元素的说法错误的是（） 参考答案：（A）**

**窗体顶端**

**A. 一个公有的虚拟空间地址，这是指该进程使用的虚拟内存地址。   
B. 至少一个执行线程。   
C. 一个被称为进程ID的唯一标识符。   
D. 一个被称为访问令牌的安全环境。**

**窗体底端**

**60. 下列对象中，没有暴露给Windows API的执行体对象的是（） 参考答案：（D）**

**窗体顶端**

**A. 进程   
B. 内存区   
C. 文件   
D. 驱动**

**窗体底端**

**61. 在一下网络威胁中，哪项不属于信息泄露（） 参考答案：（C）**

**窗体顶端**

**A. 数据窃听   
B. 流量分析   
C. 拒绝服务攻击   
D. 偷窃用户帐号**

**窗体底端**

**62. 关于动态网络地址（NAT），不正确的做法是（） 参考答案：（B）**

**窗体顶端**

**A. 将很多内部地址映射到单个地址   
B. 外部网络地址和内部地址一一对应的映射   
C. 可有64000个同时的动态NAT连接   
D. 每个连接使用一个端口**

**窗体底端**

**63. 不属于黑客被动攻击的是（） 参考答案：（A）**

**窗体顶端**

**A. 缓冲区溢出   
B. 运行恶意软件   
C. 浏览恶意网页代码   
D. 打开病毒附件**

**窗体底端**

**64. 攻击者截获并记录了从A到B的数据，然后又从早些时候所捕获的数据中提取信息重新发往B。这种攻击方式称（） 参考答案：（D）**

**窗体顶端**

**A. 中间人攻击   
B. 强力攻击   
C. 字典攻击   
D. 回放攻击**

**窗体底端**

**65. 直接处于可信网络和不可信网络之间的主机是（） 参考答案：（D）**

**窗体顶端**

**A. FTP服务器   
B. 扼流点   
C. 网关   
D. 堡垒主机**

**窗体底端**

**66. 有一台过滤路由器与外部网络相连，在通过一个可提供安全保护的主机（堡垒主机）与内部网络相连，这是（）体系的防火墙 参考答案：（B）**

**窗体顶端**

**A. 包过滤防火墙   
B. 主机过滤防火墙   
C. 代理服务器防火墙   
D. 子网过滤防火墙**

**窗体底端**

**67. 端口扫描是一种（）型网络攻击 参考答案：（C）**

**窗体顶端**

**A. DoS   
B. 利用   
C. 信息收集   
D. 虚假信息**

**窗体底端**

**68. RSA算法建立的理论基础是（） 参考答案：（C）**

**窗体顶端**

**A. DES   
B. 替代相组合   
C. 大数分解和素数检测   
D. 哈希函数**

**窗体底端**

**69. 下列对跨站脚本攻击（XSS）的解释最准确的一项是：（ ） 参考答案：（B）**

**窗体顶端**

**A. 引诱用户点击虚假网络链接的一种攻击方法   
B. 将恶意代码嵌入到用户浏览的web网页中，从而达到恶意的目的   
C. 构造精妙的关系数据库的结构化查询语言对数据库进行非法的访问   
D. 一种很强大的木马攻击手段**

**窗体底端**

**70. 已知某个链接存在SQL注入漏洞，网址是http://www.xxx.com.cn/product.asp?id=20，以下哪个URL访问之后，页面不会报错（ ）。 参考答案：（C）**

**窗体顶端**

**A. http://www.xxx.com.cn/product\_more.asp?id=20’   
B. http://www.xxx.com.cn/product\_more.asp?id=20 and 1=2   
C. http://www.xxx.com.cn/product\_more.asp?id=20 and 1=1   
D. http://www.xxx.com.cn/product\_more.asp?id=20 and 99\*9<100**

**窗体底端**

**71. 下列关于web应用说法不正确的是（ ） 参考答案：（D）**

**窗体顶端**

**A. http请求中，cookie可以用来保持http会话状态   
B. web的认证信息可以考虑通过cookie来携带   
C. 通过SSL安全套阶层协议，可以实现http的安全传输   
D. web的认证，通过cookie和session都可以实现，但是cookie安全性更好**

**窗体底端**

**72. 关于SQL注入说法正确的是（ ） 参考答案：（D）**

**窗体顶端**

**A. SQL注入攻击是攻击者直接对web数据库的攻击   
B. SQL注入攻击除了可以让攻击者绕过认证之外，不会再有其他危害   
C. SQL注入漏洞，可以通过加固服务器来实现   
D. SQL注入攻击，可以造成整个数据库全部泄露**

**窗体底端**

**73. 针对SQL注入和XSS跨站的说法中，哪些说法是不正确的（ ） 参考答案：（A）**

**窗体顶端**

**A. SQL注入的SQL命令在用户浏览器中执行，而XSS跨站的脚本在Web后台数据库中执行。   
B. XSS和SQL注入攻击中的攻击指令都是由黑客通过用户输入域注入，只不过XSS注入的是HTML代码(以后称脚本)，而SQL注入注入的是SQL命令   
C. XSS和SQL注入攻击都利用了Web服务器没有对用户输入数据进行严格的检查和有效过滤的缺陷。   
D. XSS攻击盗取Web终端用户的敏感数据，甚至控制用户终端操作，SQL注入攻击盗取Web后台数据库中的敏感数据，甚至控制整个数据库服务器。**

**窗体底端**

**74. 下面不属于木马伪装手段的是（ ）。 参考答案：（C）**

**窗体顶端**

**A. 捆绑文件   
B. 隐蔽运行   
C. 自我复制   
D. 修改图标**

**窗体底端**

**75. 关于网络入侵防御系统，以下描述不正确的是（ ） 参考答案：（A）**

**窗体顶端**

**A. 能够实时过滤阻断攻击源   
B. 阻断的是攻击包   
C. 部署在网络关键点上   
D. 以透明模式串联于网络中**

**窗体底端**

**76. 某黑客组织通过拷贝中国银行官方网站的登陆页面，然后发送欺骗性电子邮件，诱使用户访问此页面以窃取用户的账户信息，这种攻击方式属于（ ） 参考答案：（B）**

**窗体顶端**

**A. SQL注入   
B. 钓鱼攻击   
C. 网页挂马   
D. 域名劫持**

**窗体底端**

**77. Linux2.6版的内核中集成了（ ），使Linux的安全性大幅度提高。 参考答案：（A）**

**窗体顶端**

**A. SELinux   
B. Netfilter   
C. Iptables   
D. TCPWrappers**

**窗体底端**

**78. 下列哪个平台经常被用来进行无线网络的破解( ) 参考答案：（B）**

**窗体顶端**

**A. Windows7   
B. BT5   
C. android   
D. iOS**

**窗体底端**

**79. 暴力破解Unix系统账户的工具是( ) 参考答案：（C）**

**窗体顶端**

**A. LC5   
B. X-Scan   
C. John   
D. AppScan**

**窗体底端**

**80. 以下哪种攻击方式，可以称为CC攻击（ ） 参考答案：（B）**

**窗体顶端**

**A. synflood   
B. http flood   
C. smurf   
D. TearDrop**

**窗体底端**

**81. 下列哪种病毒能对计算机硬件产生破坏？（） 参考答案：（C）**

**窗体顶端**

**A. 维金   
B. CODE RED   
C. CIH   
D. 熊猫烧香**

**窗体底端**

**82. 以下哪些方法对防范SQL注入攻击无效？（） 参考答案：（C）**

**窗体顶端**

**A. 采用参数化查询方式，进行开发   
B. 对数据库系统的管理权限进行严格的控制   
C. 通过网络防火墙严格限制Internet用户对web服务器的访问   
D. 对web用户输入的数据进行严格的过滤**

**窗体底端**

**83. 在安全策略的重要组成部分中，与IDS相比，IPS的主要优势在哪里？（ ） 参考答案：（C）**

**窗体顶端**

**A. 产生日志的数量   
B. 较低的价格   
C. 攻击减少的速度   
D. 假阳性的减少量**

**窗体底端**

**84. 以下哪些软件是用于加密的软件？（ ） 参考答案：（D）**

**窗体顶端**

**A. DES   
B. SHA   
C. EFS   
D. PGP**

**窗体底端**

**85. 关于PPP协议下列说法正确的是：（ ） 参考答案：（B）**

**窗体顶端**

**A. PPP协议是物理层协议   
B. PPP协议支持的物理层可以是同步电路或异步电路   
C. PPP协议是在HDLC协议的基础上发展起来的   
D. PPP主要由两类协议组成：链路控制协议族（LCP）和网络安全方面的验证协议族（PAP和CHAP）**

**窗体底端**

**86. 无论是哪一种Web 服务器，都会受到HTTP 协议本身安全问题的困扰，这样的信息系统安全漏洞属于：（ ） 参考答案：（A）**

**窗体顶端**

**A. 运行型漏洞   
B. 开发型漏洞   
C. 设计型漏洞   
D. 以上都不是**

**窗体底端**

**87. Oracle当连接远程数据库或其它服务时，可以指定网络服务名，Oracle 9i 支持5 种命名方法，请选择错误的选项。（ ） 参考答案：（B）**

**窗体顶端**

**A. 本地命名和目录命名   
B. DNS和内部命名   
C. 主机命名和外部命名   
D. Oracle 名称（Oracle Names）**

**窗体底端**

**88. 以下哪一项不是流氓软件的特征？（ ） 参考答案：（A）**

**窗体顶端**

**A. 通常会显示下流的言论   
B. 通常添加驱动保护使用户难以卸载   
C. 通常会启动无用的程序浪费计算机的资源   
D. 通常通过诱骗或和其他软件捆绑在用户不知情的情况下安装**

**窗体底端**

**89. 网上营业厅中间件如果启用了SSL，应采用不低于（）版本的SSL，采用经国家密码管理局认可的密码算法 ） 参考答案：（A）**

**窗体顶端**

**A. 3.0   
B. 2.5   
C. 2.0   
D. 3.1**

**窗体底端**

**90. 造成缓冲区溢出漏洞的原因有（ ）。 参考答案：（A,B,D）**

**窗体顶端**

**A. 某些开发人员没有安全意识   
B. 某些高级语言没有缓冲区边界检查   
C. 用户输入数据太长，超出系统负荷   
D. 软件测试不够严格**

**窗体底端**

**91. 统一威胁管理系统（UTM）描述正确的是（ ） 参考答案：（A,B,D）**

**窗体顶端**

**A. 部署UTM可以有效降低成本   
B. 部署UTM可以降低信息安全工作强度   
C. 部署UTM可以降低安全设备集成带来的风险   
D. 部署UTM可能降低网络性能和稳定性**

**窗体底端**

**92. 以下关于宏病毒说法不正确的是（ ）。 参考答案：（A,C,D）**

**窗体顶端**

**A. 宏病毒主要感染可执行文件　   
B. 宏病毒仅向办公自动化程序编制的文档进行传染   
C. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区　　   
D. CIH病毒属于宏病毒**

**窗体底端**

**93. 使用sudo工具可以对Unix/Linux系统中用户可运行的命令进行控制以增加安全性，它的特性包括（ ）。 参考答案：（A,B,C,D）**

**窗体顶端**

**A. 需要授权许可   
B. 可以为系统管理员提供配置文件   
C. 能够限制指定用户在指定主机上运行某些命令   
D. 可以提供日志记录**

**窗体底端**

**94. 下列木马程序可能采用的激活方式有（ ）。 参考答案：（A,C）**

**窗体顶端**

**A. 修改注册表中的HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion下以“run”开头的键值   
B. 将木马程序复制在用户的桌面上   
C. 注册为系统服务   
D. 感染系统中所有的exe和html文件**

**窗体底端**

**95. 关于网络入侵检测系统，以下描述正确的是（） 参考答案：（B,C,D）**

**窗体顶端**

**A. 能够适用于加密环境   
B. 不会增加系统开销   
C. 对带宽的要求较高   
D. 其部署不影响现有网络架构**

**窗体底端**

**96. 无法用于对Windows系统口令进行暴力破解的工具有（ ） 参考答案：（A,D）**

**窗体顶端**

**A. NMAP   
B. Nessus   
C. X-Scan   
D. AppScan**

**窗体底端**

**97. 下面支持WPA加密方式的无线局域网标准有（ ）。 参考答案：（B,D）**

**窗体顶端**

**A. 802.11b   
B. 802.11i   
C. 802.11a   
D. 802.11n**

**窗体底端**

**98. 以下关于DOS攻击的描述，说法正确的有（ ） 参考答案：（B,C）**

**窗体顶端**

**A. 以窃取目标系统上的机密信息为目的   
B. 不需要侵入对方系统内部   
C. 导致目标系统无法处理正常用户的请求   
D. 如果目标系统没有漏洞，远程攻击就不可能成功**

**窗体底端**

**99. 选出可以被暴力破解的协议（ ） 参考答案：（A,B,C）**

**窗体顶端**

**A. POP3   
B. SNMP   
C. FTP   
D. TFTP**

**窗体底端**

**100. 关于HTTp协议说法不正确的是（） 参考答案：（B）**

**窗体顶端**

**A. http协议是明文传输的   
B. http协议是可靠的有状态的协议   
C. http协议主要有请求和响应两种类型   
D. http协议，在web应用中，可以有get、post、delete等多种请求方法，但是最常用是get和post**

**1. 下面是Unix系统内文件welcome.txt的属性，如果想要用户user对该文件具有写权限，可以采取的方法有多种，哪一项是不正确的（ ）。-rw-r--r-- 1 welcome welcome 30 Sep 27 18:50 welcome.txt 参考答案：（C）**

**窗体顶端**

**A. df   
B. sd   
C. sdd   
D. fsd**

**窗体底端**

**2. Windows系统管理员如果想允许一个普通用户能够使用远程桌面连接登录到计算机，则应当（ ）。 参考答案：（C）**

**窗体顶端**

**A. 将他加入Administrators组   
B. 启用安全选项“网络访问：可匿名访问的终端服务”   
C. 将他加入Remote Desktop Users组   
D. 启用安全选项“网络访问：可远程访问的终端服务”**

**窗体底端**

**3. 对于NTFS权限继承的描述，（ ）是不正确的。 参考答案：（D）**

**窗体顶端**

**A. 所有的新建文件夹都继承上级的权限   
B. 子文件夹可以取消继承的权限   
C. 父文件夹可以强制子文件夹继承它的权限   
D. 子文件夹可以强制父文件夹继承它的权限**

**窗体底端**

**4. 一个共享文件夹的共享权限为完全控制，NTFS权限为读取，当用户从网络访问此文件夹时有效权限是（ ）。 参考答案：（B）**

**窗体顶端**

**A. 完全控制   
B. 读取   
C. 更改   
D. 拒绝访问**

**窗体底端**

**5. 下 面关于Linux文件系统中的文件的访问对象，哪一项是不存在的（ ）。 参考答案：（B）**

**窗体顶端**

**A. 文件拥有者   
B. 文件管理者   
C. 文件所属组   
D. 其他人**

**窗体底端**

**6. 在Unix/Linux系统中，文件类型为“b”，说明这是一个（ ）。 参考答案：（C）**

**窗体顶端**

**A. 二进制可执行文件   
B. 硬链接文件   
C. 块设备文件   
D. 进程文件**

**窗体底端**

**7. 以下关于DOS攻击的描述，哪些说法是不正确的？( ) 参考答案：（B）**

**窗体顶端**

**A. 不需要侵入受攻击的系统   
B. 以窃取目标系统上的机密信息为目的   
C. 导致目标系统无法处理正常用户的请求   
D. 如果目标系统没有漏洞，远程攻击仍可能成功**

**窗体底端**

**8. 关于设置提高提高无线AP安全性的措施中，下列哪一项不是不合理或无效的（）。 参考答案：（C）**

**窗体顶端**

**A. 关闭SSID广播   
B. 关闭DHCP服务   
C. 关闭AP的无线功能   
D. 开启WPA加密并设置复杂密码**

**窗体底端**

**9. 下列哪一项不是造成缓冲区溢出漏洞的原因（ ）。 参考答案：（C）**

**窗体顶端**

**A. 某些开发人员没有安全意识   
B. 某些高级语言没有缓冲区边界检查   
C. 用户输入数据太长，超出系统负荷   
D. 软件测试不够严格**

**窗体底端**

**10. 下列关于缓冲区溢出攻击，描述正确的是（ ）。 参考答案：（D）**

**窗体顶端**

**A. 缓冲区溢出，只存在于系统层漏洞   
B. 缓冲区溢出，一般只存在于应用层漏洞   
C. 只是TCP/IP协议栈的漏洞   
D. 既存在于系统层漏洞也存在于应用层漏洞**

**窗体底端**

**11. 关于HTTp协议说法正确的有哪些（） 参考答案：（A,C,D）**

**窗体顶端**

**A. http协议是明文传输的   
B. http协议是可靠的有状态的协议   
C. http协议主要有请求和响应两种类型   
D. http协议，在web应用中，可以有get、post、delete等多种请求方法，但是最常用是get和post**

**窗体底端**

**12. 下列关于web应用说法不正确的是（） 参考答案：（D）**

**窗体顶端**

**A. http请求中，cookie可以用来保持http会话状态   
B. web的认证信息可以考虑通过cookie来携带   
C. 通过SSL安全套阶层协议，可以实现http的安全传输   
D. web的认证，通过cookie和session都可以实现，但是cookie安全性更好**

**窗体底端**

**13. 关于SQL注入说法正确的是（） 参考答案：（D）**

**窗体顶端**

**A. SQL注入攻击是攻击者直接对web数据库的攻击   
B. SQL注入攻击除了可以让攻击者绕过认证之外，不会再有其他危害   
C. SQL注入漏洞，可以通过加固服务器来实现   
D. SQL注入攻击，可以造成整个数据库全部泄露**

**窗体底端**

**14. 针对SQL注入和XSS跨站的说法中，哪些说法是不正确的（ ） 参考答案：（A）**

**窗体顶端**

**A. SQL注入的SQL命令在用户浏览器中执行，而XSS跨站的脚本在Web后台数据库中执行。   
B. XSS和SQL注入攻击中的攻击指令都是由黑客通过用户输入域注入，只不过XSS注入的是HTML代码(以后称脚本)，而SQL注入注入的是SQL命令   
C. XSS和SQL注入攻击都利用了Web服务器没有对用户输入数据进行严格的检查和有效过滤的缺陷。   
D. XSS攻击盗取Web终端用户的敏感数据，甚至控制用户终端操作，SQL注入攻击盗取Web后台数据库中的敏感数据，甚至控制整个数据库服务器。**

**窗体底端**

**15. 为了防御XSS跨站脚本攻击，我们可以采用多种安全措施，但（ ）是不可取的 参考答案：（C）**

**窗体顶端**

**A. 编写安全的代码：对用户数据进行严格检查过滤   
B. 可能情况下避免提交HTML代码   
C. 阻止用户向Web页面提交数据   
D. 即使必须允许提交特定HTML标签时，也必须对该标签的各属性进行仔细检查，避免引入javascript**

**窗体底端**

**16. 关于HTTP协议，以下哪些字段内容是包含在http响应头（response headers）中（） 参考答案：（B,C）**

**窗体顶端**

**A. accept：   
B. Server:   
C. Cookie:   
D. Refere :**

**窗体底端**

**17. 有很多办法可以帮助我们抵御针对网站的SQL注入，其中不可取的方法是（ ） 参考答案：（A）**

**窗体顶端**

**A. 删除网页中的SQL调用代码，用纯静态页面   
B. 关闭DB中不必要的扩展存储过程   
C. 编写安全的代码：尽量不用动态SQL；对用户数据进行严格检查过滤   
D. 关闭Web服务器中的详细错误提示**

**窗体底端**

**18. 发现感染计算机病毒后，有很多方法可以帮助用户减小损失，以下哪一项不是优先采取的处理方式（） 参考答案：（B）**

**窗体顶端**

**A. 断开网络   
B. 格式化系统   
C. 使用杀毒软件检测、清除   
D. 可以通过PE系统启动，查找可以隐藏文件，并清除**

**窗体底端**

**19. 下面不属于木马伪装手段的是（） 参考答案：（C）**

**窗体顶端**

**A. 捆绑文件   
B. 隐蔽运行   
C. 自我复制   
D. 修改图标**

**窗体底端**

**20. 下列木马程序可能采用的激活方式是（） 参考答案：（A）**

**窗体顶端**

**A. 修改注册表中的HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion下以“run”开头的键值   
B. 将木马程序复制在用户的桌面上   
C. 将自身隐藏于系统启动分区   
D. 感染系统中所有的exe和html文件**

**窗体底端**

**21. 为了防御网络监听，最有效也最常用的方法是（ ） 参考答案：（D）**

**窗体顶端**

**A. 采用物理传输（非网络）   
B. 使用专线传输   
C. 用光纤传输数据   
D. 对传输数据进行加密**

**窗体底端**

**22. Windows2003，本地域名劫持（DNS欺骗）修改的是哪个系统文件（ ） 参考答案：（C）**

**窗体顶端**

**A. 、C:\Windows\System32\drivers\etc\lmhosts   
B. C:\Windows\System32\ etc\lmhosts   
C. C:\Windows\System32\drivers\etc\hosts   
D. C:\Windows\System32\etc\hosts**

**窗体底端**

**23. 某黑客组织通过拷贝中国银行官方网站的登陆页面，然后发送欺骗性电子邮件，诱使用户访问此页面以窃取用户的账户信息，这种攻击方式属于（ ） 参考答案：（B）**

**窗体顶端**

**A. SQL注入   
B. 钓鱼攻击   
C. 网页挂马   
D. 域名劫持**

**窗体底端**

**24. 关于网络入侵防御系统（IPS），以下描述不正确的是（） 参考答案：（A）**

**窗体顶端**

**A. 入侵防御系统，主要是识别网络、传输层的攻击特征。   
B. 能够实时阻断攻击包   
C. 通常部署在网关位置   
D. 通常以透明模式串联于网络中**

**窗体底端**

**25. 关于网络入侵检测系统（IDS），以下描述不正确的是（） 参考答案：（A）**

**窗体顶端**

**A. 能够适用于加密环境   
B. 不会增加系统开销   
C. 对带宽的要求较高   
D. 其部署不影响现有网络架构**

**窗体底端**

**26. 攻击者截获并记录了从A到B的数据，然后又从早些时候所截获的数据中提取出信息重新发往B称为（） 参考答案：（B）**

**窗体顶端**

**A. 中间人攻击   
B. 回放攻击   
C. 强力攻击   
D. 口令猜测器和字典攻击**

**窗体底端**

**27. 下列哪个平台经常被用来进行无线网络的破解( ) 参考答案：（B）**

**窗体顶端**

**A. Windows7   
B. BT5   
C. android   
D. iOS**

**窗体底端**

**28. 以下哪种攻击方式，可以称为CC攻击（ ） 参考答案：（B）**

**窗体顶端**

**A. synflood   
B. http flood   
C. smurf   
D. TearDrop**

**窗体底端**

**29. 下面不属于嗅探类工具的是( ) 参考答案：（D）**

**窗体顶端**

**A. SnifferPro   
B. WireShark   
C. Cain   
D. X-Way**

**窗体底端**

**30. 以下关于数据库安全的说法错误的是？（ ） 参考答案：（D）**

**窗体顶端**

**A. 数据库系统的安全性很大程度上依赖于DBMS的安全机制   
B. 许多数据库系统在操作系统下以文件形式进行管理，因此利用操作系统漏洞可以窃取数据库文件   
C. 数据库的安全需要在网络系统、操作系统和数据库管理系统三个方面进行保护   
D. 为了防止数据库中的信息被盗取，在操作系统层次对文件进行加密是唯一从根本上解决问题的手段**

**窗体底端**

**31. 以下哪个软件，常用于加密邮件使用，并集成了对称和非对称加密算法的（） 参考答案：（D）**

**窗体顶端**

**A. DES   
B. Openssl   
C. EFS   
D. PGP**

**窗体底端**

**32. 为了检测 Windows系统是否有木马入侵，可以先通过（）命令来查看当前的活动连接端口（） 参考答案：（B）**

**窗体顶端**

**A. ipconfig   
B. netstat -an   
C. tracert -d   
D. netstat -rn**

**窗体底端**

**33. Oracle的数据库监听器（LISTENER）的默认通讯端口是？（ ） 参考答案：（D）**

**窗体顶端**

**A. TCP 1433   
B. TCP 1025   
C. TCP 1251   
D. TCP 1521**

**窗体底端**

**34. HTTP, FTP, SMTP 建立在OSI模型的那一层？（ ） 参考答案：（C）**

**窗体顶端**

**A. 2 层– 数据链路层   
B. 3层 – 网络层   
C. 7 层– 应用层   
D. 4层– 传输层**

**窗体底端**

**35. 下列关于IIS的安全配置，哪些是不正确的？（） 参考答案：（A）**

**窗体顶端**

**A. 禁用所有Web 服务扩展   
B. 重命名 IUSR 账户   
C. 将网站内容移动到非系统驱动器   
D. 创建应用程序池**

**窗体底端**

**36. 下列措施中不能增强DNS安全的是（ ） 参考答案：（A）**

**窗体顶端**

**A. 更改DNS的端口号   
B. 设置区域复制权限及允许IP   
C. 使用最新的BIND工具   
D. 不要让HINFO记录被外界看到**

**窗体底端**

**37. 下列哪一项是arp协议的基本功能？（ ） 参考答案：（D）**

**窗体顶端**

**A. 将信息传递给网络层   
B. 对局域网内的其他机器广播路由地址   
C. 过滤信息，将信息传递个数据链路层   
D. 通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的进行**

**窗体底端**

**38. 在进行Sniffer监听时，系统将本地网络接口卡设置成何种侦听模式？（） 参考答案：（D）**

**窗体顶端**

**A. unicast单播模式   
B. Promiscuous混杂模式   
C. Multicast（组播模式）   
D. Broadcast（广播模式）**

**窗体底端**

**39. SQL Server的登录账户信息保存在哪个数据库中？（ ） 参考答案：（B）**

**窗体顶端**

**A. model   
B. master   
C. msdb   
D. tempdb**

**窗体底端**

**40. 以下哪些方法，可以有效防御CSRF带来的威胁（） 参考答案：（A,B,C,D）**

**窗体顶端**

**A. 使用图片验证码。   
B. 要求所有POST请求都包含一个伪随机值   
C. 只允许GET请求检索数据，但是不允许它修改服务器上的任何数据   
D. 使用多重验证，例如手机验证码**

**窗体底端**

**41. 以下哪些是web常见中间件（） 参考答案：（A,C,D）**

**窗体顶端**

**A. Tomcat   
B. Informix   
C. Weblogic   
D. Webshpere**

**窗体底端**

**42. 无线网络中常见的三种攻击方式包括（） 参考答案：（A,C,D）**

**窗体顶端**

**A. 中间人攻击   
B. 漏洞扫描攻击   
C. 会话劫持攻击   
D. 拒绝服务攻击**

**窗体底端**

**43. 无法用于对Windows系统口令进行暴力破解的工具是（ ） 参考答案：（A,D）**

**窗体顶端**

**A. NMAP   
B. Nessus   
C. X-Scan   
D. AppScan**

**窗体底端**

**44. Unix系统中某个文件的模式位为drwxr-xr-x，说明（ ） 参考答案：（A,B）**

**窗体顶端**

**A. 任何人都可以执行这个文件   
B. 文件的权限为755   
C. 这是一个普通文件   
D. 该文件只有超级用户root可写**

**窗体底端**

**45. 防范网页挂马攻击，作为第三方的普通浏览者，以下哪种办法可以有效？（） 参考答案：（A,D）**

**窗体顶端**

**A. 及时给系统和软件打最新补丁   
B. 不浏览任何网页   
C. 安装防火墙   
D. 安装查杀病毒和木马的软件**

**窗体底端**

**46. 以下关于宏病毒说法不正确的是（ ） 参考答案：（A,C,D）**

**窗体顶端**

**A. 宏病毒主要感染可执行文件　   
B. 宏病毒仅向办公自动化程序编制的文档进行传染   
C. 宏病毒主要感染软盘、硬盘的引导扇区或主引导扇区   
D. CIH病毒属于宏病毒**

**窗体底端**

**47. 常见的拒绝服务攻击手段有: ( ) 参考答案：（A,B,C,D）**

**窗体顶端**

**A. UDP Flood   
B. ICMP Flood   
C. SYN Flood   
D. IGMP Flood**

**窗体底端**

**48. Serv-U软件因自身缺陷曾多次被黑客用来进行提权攻击，针对提权的防御办法有（ ） 参考答案：（A,B,C,D）**

**窗体顶端**

**A. 禁用anonymous帐户   
B. 修改Serv-U默认管理员信息和端口号   
C. 修改默认安装路径，并限制安全目录的访问权限   
D. 限制用户权限，删除所有用户的执行权限**

**窗体底端**

**49. 以下哪些攻击方式，可以导致拒绝服务（） 参考答案：（A,C,D）**

**窗体顶端**

**A. Ping of Death   
B. ARP攻击   
C. Land攻击   
D. 畸形报文攻击**

**窗体底端**

**50. Unix系统中使用下面的find命令，可以实现的功能是（ ）。find / -type f \( -perm -4000 -o -perm –2000 \ ) -exec ls -lg {} \; 参考答案：（B）**

**窗体顶端**

**A. 所有SUID文件   
B. 所有SUID或者SGID文件   
C. 所有SGID文件   
D. 所有SUID以及SGID文件**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**

**窗体底端**