题一（ 1）：选择题

1. 软件的供应商或是制造商可以在他们自己的产品中或是客户的计算机系统上安装一个 “后门” 程序。（ ）是这种情况面临的最主要风险。
A、软件中止和黑客入侵 B 、远程维护和黑客入侵 C 、软件中止和远程监控 D 、远程监控和远程 维护

2. 对于需要进行双层防火墙进行防护的系统，为避免因同品牌或同种类防火墙弱点被利用导致双 重防护措施全部失效的风险，需要实现 （ ） 。
A、单层防火墙防护 B 、双重异构防火墙防护 C 、单层异构防火墙防护 D 、双重防火墙防护

3. 一般的防火墙不能实现以下哪项功能 （ ） 。 A、隔离公司网络和不可信的网络 B 、访问控制 C 、隔离内网 D 、防止病毒和特洛伊木马

4. 下面不属于恶意软件的是 （ ） 。
A、病毒 B 、扫描软件 C 、木马 D 、蠕虫

5. 依据信息系统安全保障模型，以下哪个不是安全保证对象 （ ） 。
A、机密性 B 、人员 C 、过程 D 、管理

6. 加密、认证实施中首要解决的问题是（ ）。
A、信息的包装与用户授权 B 、信息的包装与用户的分级 C 、信息的分级与用户分类 D 、信息的 分布与用户的分级

7. 状态检测技术能在 （ ） 实现所有需要的防火墙能力。
A、网络层 B 、应用层 C 、传输层 D 、数据层

8. HTTPS 是一种安全的 HTTP 协议，它使用 （ ） 来保证信息安全，使用 （ ） 来发送和 接收报文。
A、SSH、UDP 的 443 端口 B 、SSH、TCP 的 443 端口 C、SSL、UDP 的 443 端口 D 、SSH、TCP 的 443 端口

9. 身份认证和访问管理的相关控制措施防护要点不包括（ ）。 A、最小化授权原则 B 、定期备份恢复 C 、重要资源访问审计 D 、统一身份认证

10. DES 算法属于加密技术中的（ ）。
A、对称加密 B 、以上都是 C 、不可逆加密 D 、不对称加密

11. 三重 DES 是一种加强了的 DES 加密算法，它的有效密钥长度是 DES 算法的（ ）倍。 A、2 B 、5 C、4 D 、3

资料

12. （ ）类型的攻击，攻击者在远程计算机使用一个自复制产生流量的程序。
A、字典攻击 B 、病毒攻击 C 、非法服务器攻击 D 、劫持攻击

13. 利用 TCP 连接三次握手弱点进行攻击的方式是（ ）。
A、SYN Flood B 、以上都是 C 、会话劫持 D 、嗅探

14. “公开密钥密码体制”的含义是（ ）。
A、将所有密钥公开 B 、两个密钥相同 C 、将公开密钥公开， 私有密钥保密 D 、将私有密钥公开， 公开密钥保密

15. 以下对计算机病毒的描述错误的是 （ ） 。 A、计算机病毒是在计算机程序中插入的破坏计算机功能或者毁坏数据的代码 B 、能够产生有害的
或恶意的动作 C 、具有自动产生和自身拷贝的能力 D 、可以作为独立的可执行程序执行

16. 防火墙的路由模式配置中 DNAT 策略里的转换后的地址一般为 （ ） 。
A、防火墙外网口地址 B 、服务器的 IP 地址 C 、防火墙 DMZ 口地址 D 、防火墙内网地址

17. MD5 算法的 HASH 值长度为（ ）。
A、160bit B 、 256bit C 、128bit D 、64bit

18. 代理服务器所具备的特点是（ ）。
A、通过代理服务器访问网络， 对用户层面来说是透明的 B 、代理服务器会降低用户访问网络的速 度 C 、代理服务器能够支技所有的网络协议 D 、代理服务器能够弥补协议本身存在的缺陷

19. HTTPS 是一种安全的 HTTP 协议，它使用（ ）来保证信息安全。
A、 IPSec B 、SSH C、SET D、 SSL

20. 防火墙中地址翻译的主要作用是 （ ） 。
A、提供代理服务 B 、防止病毒入侵 C 、进行入侵检测 D 、隐藏内部网络地址

21. 以下哪个类型攻击属于拒绝服务攻击 （ ） 。
A、 SQL 注入 B 、网络钓鱼 C 、网页木马 D 、PINGOFDEATH

22. 以下 （ ） 标准是信息安全管理国际标准。
A、ISO9000-2000 B 、ISO15408 C 、ISO17799 D 、SSF-CMM

23. PKI 能够执行的功能是（ ）。
A、确认计算机的物理地址 B 、访问控制 C 、确认用户具有的安全生特权 D 、鉴别计算机消息的 始发者

24. 基于密码技术的（ ）是防止数据传输泄密的主要防护手段 资料

A、连接控制 B 、保护控制 C 、传输控制 D 、访问控制

25. 信息安全风险管理应该（ ）。
A、将所有信息安全风险都消除 B 、以上说法都不对 C 、基于可接受的成本采取相应的方法和措 施 D 、在风险评估之前实施

26. 在 Windows 操作系统中，用于备份 EFS 证书的工具是（ ）。
A、 mmc B、cipher C 、secedit D 、gpedit

27. PKI 的全称是（ ）。
A、Private Key Intrusion B 、Public Key Infrastructure C 、Private Key Infrastructure D 、 Public Key Intrusion

28. 对于 TCP SYN 扫描，如果发送一个 SYN 包后，对方返回（ ）表明端口处于开放状态。 A、ACK B、RST/ACK C、 SYN/RST D、SYN/ACK

29. 管理信息大区中的内外网间使用的是 （ ） 隔离装置。
A、正向隔离装置 B 、防火墙 C 、逻辑强隔离装置 D 、反向隔离装置

30. 根据 SG186 要求，重要文件完整性检查必须部署的域是 （ ） 。
A、二级系统域 B 、桌面终端域 C 、外网应用系统域 D 、三级系统域

31. 在什么情况下，防火墙会不起作用 （ ） 。
A、内部网用户通过防火墙访问 Internet B 、外部用户通过防火墙访问 WEB 服务器 C 、外部用户 向内部用户发 E-mail D 、内部网用户通过 Modem 拨号访问 internet

32. 目前安全认证系统主要采用基于（ ） 的数字证书来实现。
A、PKI B 、IDS C 、VPN D、KMI

33. 根据下面对“灰鸽子”的描述，请判断“灰鸽子”属于什么类恶意软件。 （ ）
（1）“灰鸽子”是一款可以远程控制的软件。
（2）“灰鸽子” 通过截获进程的 API 调用隐藏自己的文件、相关的注册表项， 甚至是进 程中的模 块名。
（3）“灰鸽子” 采用远程线程注入 IE 进程的方式来进行网络传输， 用以逃避主机防火墙 的拦截。 A、病毒 B 、流氓软件 C 、木马 D 、蠕虫

34. 木马程序通常不具备下列哪种特性 （ ） 。
A、能够自主传播自己 B 、盗取机密信息 C 、让系统完全被控制 D 、高度隐藏运行

35. DSA 指的是（ ）。
A、数字签名算法 B 、数字鉴别算法 C 、数字签名协议 D 、数字系统算法 资料

36. 木马程序通常不具备（ ）特性。
A、能够自主传播自己 B 、盗取机密信息 C 、让系统完全被控制 D 、高度隐藏运行

37. OSI 七层模型中 （ ） 层可以提供抗抵赖性。
A、数据链路层 B 、应用层 C 、表示层 D 、传输层

38. 下列哪一项不是防火墙所具有的一般特性 （ ） 。
A、所有的从内部到外部或从外部到内部的通信流量都必须通过防火墙B 、系统本身具有高可靠性，
防火墙本身是不可穿透的 C 、可以对由内部到外部的数据进行加密 D 、只有经过安全策略允许的 通信流量，才能通过防火墙

39. 间谍软件是 （ ） 。
A、一种能在没有任何用户动作的情况下自动传染计算机病毒变形B 、一种通过把代码在不被察觉
的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、 破坏被感染电脑数据的程序 C 、能够从主机传输到客户端计算机上并执行的代码 D 、放在你的计 算机中能秘密收集信息，并把信息传给广告商或其他相关人的程序

40. 不属于 DoS 攻击的是（ ）。
A、 Smurt 攻击 B 、TFN 攻击 C 、Ping of Death D 、 Ping of Death

41. 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（ ）。
A、中间人攻击 B 、重放攻击 C 、强力攻击 D 、口令猜测器和字典攻击

42. 评估者可根据自身情况选择相应的风险计算方法计算风险值，风险计算方法包括（ ） 。
A、矩阵法或相乘法 B 、系数法或函数法 C 、相加法加矩阵法 D 、相加法或相乘法

43. 用于实现身份鉴别的安全机制是（ ）。
A、加密机制和数字签名机制 B 、访问控制机制和路由控制机制 C 、数字签名机制和路由控制机 制 D 、加密机制和访问控制机制

44. 加密技术不能实现（ ）。
A、数据信息的完整性 B 、数据信息的保密性 C 、机密文件加密 D 、基于密码技术的身分认证

45. 属于 SNMP、Telnet 和 FTP 共性的安全问题的是（）。
A、主要的服务守护进程存在严重的系统漏洞 B 、都可以匿名连接 C 、在建立连接过程中，缺少 认证手段 D 、明文传输特性

46. Linux 操作系统用户需要检查从网上下载的文件是否被改动，可以用的安全工具是（ ） A、 RSA B、md5sum C、DES D、AES

资料

47. 对信息安全管理威胁最大的是 （ ） 。
A、外部恶意攻击 B 、病毒对网络的影响 C 、内部恶意攻击 D 、病毒对 PC 的影响

48. 下面哪个既提供完整性服务又提供机密性服务 （ ） 。
A、数字签名 B 、访问控制 C 、密码校验值 D 、加密

49. IPSec VPN 安全技术没有用到（ ）。
A、隧道技术 B 、身份认证技术 C 、入侵检测技术 D 、加密技术

50. 下面哪一种攻击方式最常用于破解口令 （ ） 。
A、哄骗 （spoofing） B 、WinNuk C 、拒绝服务（ Dos） D 、字典攻击（ dictionaryattack

51. 非对称算法是公开的，保密的只是（ ）。
A、数据 B 、口令 C 、密码 D 、密钥

52. 能最有效防止源 IP 地址欺骗攻击的技术是（ ）。
A、策略路由（ PBR） B 、IP 源路由 C 、访问控制列表 D 、单播反向路径转发（ uRPF）

53. 下面 （ ） 用于电子邮件的鉴别和机密性。
A、数字签名 B 、MD4 C、 PGP D、 IPSEC-AH

54. （ ）是用于电子邮件的鉴别和机密性。
A、数字签名 B 、MD4 C、 PGP D、 IPSEC-AH

55. “会话侦听和劫持技术”是属于（ ）技术。
A、密码分析还原 B 、 DOS 攻击 C 、应用漏洞分析与渗透 D 、协议漏洞渗透

56. 下列不属于信息安全的技术是 （ ） 。
A、防火墙 B 、防病毒 C 、认证 D 、加密狗

57. （ ）不包含在 AAA（ AAA 的描述）中。
A、 Authentication （认证） B 、Accounting （计费） C 、Authorization （授权） D （接入）

58. SYN FLOOD 攻击是通过（ ）协议完成的。
A、UDP B、AppleTalk C 、IPX/SPX D 、TCP

59. 某公司的 Windows 网络准备采用严格的验证方式， 基本的要求是支持双向身份认证， 议该公司采用（ ）认证方式。 应该建

A、 NTLM B、LanManager C 、Kerberos D 、NTLMv2

资料

60. SYN 风暴属于（ ）。
A、拒绝服务攻击 B 、社会工程学攻击 C 、操作系统漏 D 、缓冲区溢出攻击
洞攻击

61. ISO 9000 标准系列着重于以下哪一个方面 （ ） 。 A、产品 B 、生产厂家 C 、
原材料 D 、加工处理过程

62. 一个可以对任意长度的报文进行加密和解密的加密算法称为（ ） A、链路加密
B 、流加密 C 、端对端加密 D 、批量加密

63. 数字证书是在（ ）国际标准中定义的
A、 X.400 B 、X.509 CX、12 D 、 X.25
64. 数字签名是使用（ ）。
A、自己的私钥签名 B 、对方的公钥签名 C 、对方的私钥签名 D 、自己的公钥签名

65. 802.1X 是基于（ ）的一项安全技术。
A、 IP 地址 B 、物理地址 C 、应用类型 D 、物理端口

66. 网络层攻击中属于 IP 欺骗攻击的包括（ ）
A、 TFN B、DOS C、SYN-Flood D 、Smurf

67. 防止他人入侵电子邮箱的措施中，不正确的是（ ）。
A、不用生日做密码 B 、自己做服务器 C 、不要使用纯数字 D 、不要使用小于 5 位
的密码

68. 数据保密性安全服务的基础是（ ）。
A、数据完整性机制 B 、加密机制 C 、访问控制机制 D 、数字签名机制
69. Arp 欺骗可以对局域网用户产生（ ）威胁。
A、挂马 B 、以上均是 C 、中间人攻击 D 、局域网网络中断

70. （ ）是局域网中常见的被动威胁。
A、拒绝服务攻击 B 、消息服务的修改 C 、嗅探 D 、IP 欺骗

71. 统一认证系统提供（ ）方式的认证。
A、用户名/密码 B 、以上方式都提供 C、令牌 D 、X.509 数字证书

72. 为了控制目标主机，木马一般都包括（ ）。
A、一个客户端 B 、一个客户端和两个服务器端 C 、一个客户端和一个服务器端 D 、
一个服务器 端

73. 拒绝服务攻击损害了信息系统的（ ）性能。
A、完整性 B 、可靠性 C 、保密性 D 、可用性 资料

74. 以下哪个针对访问控制的安全措施是最容易使用和管理的 （ ） 。
A、密码 B 、加密数据文件 C 、硬件加密 D 、加密标志

75. 下面哪个漏洞属于应用系统安全漏洞 （ ） 。
A、Windows2000 中文版输入法漏洞 B 、Web 服务器 asp 脚本漏洞 C 、SQLServer 存在的 SA 空口 令漏洞 D 、Windows2000 的 Unicode 编码漏洞

76. 如果将风险管理分为风险评估和风险减缓，那么以下哪个不属于风险减缓的内容（ ） 。 A、计算风险 B 、接受残余风险 C 、实现安全措施 D 、选择合适的安全措施

77. 下述攻击手段中不属于 DOS 攻击的是 （ ） 。
A、 Smurt 攻击 B 、CGi 溢出攻击 C 、Teardrop 攻击 D 、Land 攻击

78. （ ）技术不能保护终端的安全。
A、防止非法外联 B 、漏洞扫描 C 、补丁管理 D 、防病毒

79. 下列 ISO27000 协议族中， （ ） 是关于信息安全管理体系实施指南。
A、27001 B 、27004 C 、 27003 D 、27002

80. Windows 有三种类型的事件日志，分别是 （ ） 。
A、系统日志、应用程序日志、安全日志 B 、系统日志、应用程序日志、事件日志 C 、安全日志、 应用程序日志、事件日志 D 、系统日志、应用程序日志、 DNS 日志

题一（ 2）：判断题：
1. 入侵检测系统可以弥补企业安全防御系统中的安全缺陷和漏洞。 （ ）
2. 宏属于恶意代码。（ ）
3. 信息数据备份包括全盘备份、增量备份、关键项目备份。 （ ）
4. 在 Windows 操作系统安全模式下，木马程序不能启动。 （ ）
5. 防火墙作为实现网络边界隔离的设备，其部署应以安全域划分以及系统边界整合为前提，综合 考虑边界风险的程度来设定。 （ ）
6. 使用 IE 浏览器浏览网页时，出于安全方面的考虑，需要禁止执行 Java Script ，可以在
IE 中禁用 cookie 。（ ）
7. 最新的研究和统计表明，安全攻击主要源自因特网。 （ ）
8. OSI 七层模型中，应用层可以提供抗抵赖性。 （ ）
9. 国家电网公司管理信息大区中的信息内外网间使用的是正向隔离装置（ ）
10. 宏病毒感染不了 EXE 文件。（ ）

题一（ 3）：简答题：
1. 什么是 DNS 劫持以及如何防范？
DNS 劫持意思是通过某些手段取得某域名的解析记录控制权，进而修改此域名的解析结

对该域名的访问由原 IP 地址转入到修改后的指定 IP ，其结果就是对特定的网址不能访问或访问 的是假网址，从而实现窃取资料或者破坏原有正常服务的目的。
通常在三种情况下会遇到 DNS 劫持的问题：
（ 1）用户计算机感染病毒，病毒在操作系统中的 HOSTS 文件中添加了虚假的 DNS 解析 记录。 Windows 中 HOSTS 文件的优先级高于 DNS 服务器，操作系统在访问某个域名时， 会 先检测 HOSTS 文件，然后再查询 DNS 服务器。
（2）用户试图访问的网站被恶意攻击。 这种情况下， 用户可能访问到的是一个欺骗性网 站，也有 可能被定向到其他网站。
（3）用户在浏览器中输入了错误的域名，导致 DNS 查询不存在的记录。以前遇到这种情 况时， 浏览器通常会返回一个错误提示。 而最近，这种情况下用户会看到 ISP 设置的域名纠 错系统提示。 如何防范 DNS 劫持：
（1）使用安全可靠的 DNS 服务器管理自己的域名，并且注意跟进 DNS 的相关漏洞信 息，更新最新补丁，加固服务器。
（2）保护自己的重要机密信息安全，避免域名管理权限被窃取。
（3）提高服务器安全级别，更新系统及第三方软件漏洞，避免遭受攻击。

2. 简述入侵检测系统和入侵防御系统的区别。
功能区别： IDS 主要是对入侵事件进行检测和告警，可以和其他设备联动实施阻断，但本身 没有 阻断功能；与 IDS 不同的是， IPS 除对安全事件能够进行检测和告警外，还能实施阻断。
部署方式： IDS 一般采用旁路部署， 对网络流量不会产生任何影响； 而 IPS 一般采用串联的方式 部署，可能存在单点故障。

3. 什么是 DDOS 攻击及怎么抵抗 DDOS 攻击？
DDOS 是 英文 Distributed Denial of Service 的缩写，意即“分布式拒绝服务” ，那么什么 又是 拒绝服务（ Denial of Service ）呢？可以这么理解，凡是能导致合法用户不能够访问正常 网络服 务的行为都算是拒绝服务攻击。也就是说拒绝服务攻击的目的非常明确，就是要阻止 合法用户对 正常网络资源的访问， 从而达成攻击者不可告人的目的。 虽然同样是拒绝服务攻 击，但是 DDOS 和 DOS 还 是有所不同， DDOS 的 攻击策略侧重于通过很多 “僵尸主机”（被攻击者入侵过或可间接利用 的主机）向受害主机发送大量看似合法的网络包， 从而造成网络阻塞或服务器资源耗尽而导致拒绝 服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会 犹如洪水般涌向受害主机，从而把合法 用户的网络包淹没，导致合法用户无法正常访问服务 器的网络资源，因此，拒绝服务攻击又被称 之为“洪水式攻击”，常见的 DDOS 攻击手段有 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 、 TCPF lood 、 ConnectionsFlood 、 Script Flood 、 Proxy Flood 等，而 DOS 则侧重于通过对主机 特定漏洞的利用攻击导致网络栈失效、系统崩 溃、主机死机而无法提供正常的网络服务功能，从 而造成拒绝服务，常见的 DOS 攻击手段有 TearDrop 、Land、Jolt 、IGMP Nuker、Boink 、Smurf、 Bonk、OOB 等 。 DDOS 和 DOS 这两种 拒绝服务攻击而言，危害较大的主要是

DDOS 攻击，原因是 很难防范，至于 DOS 攻击，通 过给主机服务器打补丁或安装防火墙软件就可以很好地防范。
对付 DDOS 是一个系统工程， 想仅仅依靠某种系统或产品防住 DDOS 是不现实的， 可以 肯定的是， 完全杜绝 DDOS 目前是不可能的，但通过适当的措施抵御 90%的 DDOS 攻击是可 以做到的，基于 攻击和防御都有成本开销的缘故，若通过适当的办法增强了抵御 DDOS 的能 力，也就意味着加大
了攻击者的攻击成本，那么绝大多数攻击者将无法继续下去而放弃，也 就相当于成功的抵御了

DDOS 攻 击。以下几点是防御 DDOS 攻击几点：
（1）采用高性能的网络设备。
（2）尽量避免 NAT 的使用。
（3）充足的网络带宽保证。
（4）升级主机服务器硬件。
（5）把网站做成静态页面。
（6）增强操作系统的 TCP/IP 栈。
（7）安装专业抗 DDOS 设备。

题一（ 4）：仿真题：
1. 配置加强 Linux 服务器系统安全性 一台按默认配置安装好的 Linux 服务器系统，通过哪些系统命令配置加强这台服务器的安全性？

答题要点：
1、用防火墙关闭不需要的任何端口，别人 PING 不到服务器，威胁自然减少了一大半。
2、更改 SSH 端口，最好改为 10000 以上，别人扫描到端口的几率也会下降，创建一个普通登录 用户，用户名： username,密码： username，并取消直接 root 登录。
3、删除 ftp 账号。
4、更改下列文件权限，使任何人没有更改账户权限：
1 ） /etc/passwd
2）/etc/shadow
3 ） /etc/group
4 ） /etc/gshadow

答案要点：
（1）用防火墙关闭不需要的任何端口， 别人 PING 不到服务器， 威胁自然减少了一大半 防止别人 ping 的方法：
1）命令提示符下打。
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
2）用防火墙禁止（或丢弃） icmp 包。
iptables -A INPUT -p icmp -j DROP
（2）更改 SSH 端口，最好改为 10000 以上，别人扫描到端口的几率也会下降。

vi /etc/ssh/ssh_config
将 PORT 改为 1000 以上端口。 同时，创建一个普通登录用户， 并取消直接 root 登录。 useradd 'username' passwd 'username'
vi /etc/ssh/sshd_config
在最后添加如下一句：
PermitRootLogin no ＃取消 root 直接远程登录
（3）删除 ftp 账号：
userdel ftp
（4）更改下列文件权限，使任何人没有更改账户权限：
资料

2. Linux 服务器实现 NAT 功能
如何使用一台双网卡的 Linux 服务器实现 NAT 功能？
已知外网网卡已配置， 外网 IP 为：210.77.176.66 ，内网网卡已配置 IP 为 :192.168.1.121 、IP 段： 192.168.1.2-192.168.1.254
1、配置内核数据包相关功能
2、配置防火墙设置数据包相关功能

打开内核数据包转发功能
echo "1" >/proc/sys/net/ipv4/ip_forward
2、防火墙设置数据包转发伪装
iptables -t nat -A POSTROUTIN-Gs 192.168.1.1/252 -o eth1 -j SNAT? to-source 210. 77. 176. 66

题二(1)：选择题

chattr +i /etc/passwd chattr +i /etc/shadow chattr +i /etc/group chattr +i /etc/gshadow

1. 在什么情况下，防火墙会不起作用（ ）。
A、 B 、 C 、 D 、

2. 防火墙的透明模式配置中在网桥上配置的 IP 主要用于( )。
A、管理 B 、双机热备 C 、NAT 转换 D 、保证连通性

3. 字典攻击是黑客利用自动执行的程序猜测用户名和密码，审计这类攻击通常需要借助（ ）。
A、全面的日志记录和强壮的加密 B 、强化的验证方法和入侵监测系统 C 、强化的验证方法和强

壮的加密 D 、全面的日志记录和入侵监测系统

4. 分布式拒绝服务攻击的简称是( )。 A、 SDOS B、LAND C、DDOS D、DROS

5. 一个数据包过滤系统被设计成只允许你要求服务的数据包进入， 而过滤掉不必要的服 于( )基本原则。 (分值： 0.5) 务。这属
A、最小特权 B 、防御多样化 C 、失效保护状态 D 、阻塞点

6. 下列不属于常用的 VPN 技术的是 ( )
A、IPSE B 、PPPOE C、L2TP D、SSL

7. 用户收到了一封可疑的电子邮件，要求用户提供银行账户及密码，这可能属于( ) A、溢出攻击 B 、DDOS 攻击 C 、后门攻击 D 、钓鱼攻击 攻击手段

8. 在许多组织机构中，产生总体安全性问题的主要原因是 ( ) 。 A、缺少安全性管理 B 、缺少技术控制机制 C 、缺少风险分析 D 、缺少故障管理

9. 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 往 B 称为( )。 (分值： 0.5) 息重新发
A、 B 、 C 、 D 、

10. Kerberos 提供的最重要的安全服务是 ( ) 。
A、鉴别 B 、可用性 C 、完整性 D 、机密性

11. 为了降低风险，不建议使用的 Internet 服务是 ( ) 。
A、 Web 服务 B 、 FTP 服务 C 、内部访问 Internet D 、外部访问内部系统

12. 路由器访问控制列表提供了对路由器端口的一种基本安全访问技术，也可以认为是一 ( )。 种内部
A、防火墙技术 B 、备份技术 C 、加密技术 D 、入侵检测技术

14. 状态检测技术能在 ( ) 实现所有需要的防火墙能力。
A、网络层 B 、应用层 C 、传输层 D 、数据层

15. 木马程序通常不具备下列哪种特性 ( ) 。
A、能够主动传播自己 B 、盗取机密信息 C 、让系统完全被控制 D 、高度隐藏运行

16. 安全等级是国家信息安全监督管理部门对计算机信息系统 ( ) 的确认 A、规模 B 、网络结构 C 、安全保护能力 D 、重要性

资料

17. SYN 风暴属于( )。
A、拒绝服务攻击 B 、社会工程学攻击 C 、操作系统漏洞攻击 D 、缓冲区溢出攻击

18. 入侵检测系统在进行信号分析时， 一般通过三种常用的技术手段， 以下 （ ） 不属于通常的三种 技术手段。
A、模式匹配 B 、密文分析 C 、完整性分析 D 、统计分析

19. 渗透性测试属于 （ ） 所采用的方法。
A、资产识别 B 、安全措施识别 C 、威胁识别 D 、脆弱性识别

20. SQL 杀手蠕虫病毒发作的特征是 （ ） 。
A、大量消耗带宽 B 、攻击手机网络 C 、破坏 PC 游戏程序 D 、攻击个人 PC 终端

21. 建立在通用操作系统上的防火墙 （ ） 。
A、对用户的技术要求高 B 、费用昂贵 C 、防火墙厂商具有操作系统的源代码，并可实现安全内 核 D 、安全性和速度大为提高

22. 下面 （ ） 通信协议不是加密传输的。
A、 SFTP B、HTTPS C、SSH D、TFTP

23. 在需要保护的信息资产中 （ ） 是最重要的。
A、环境 B 、软件 C 、数据 D 、硬件

24. 不属于 DoS 攻击的是( )。
A、 Smurf 攻击 B 、TFN C、Ping of Death D 、Ping of Death

26. ( )是磁介质上信息擦除的最彻底形式。
A、格式化 B 、文件粉碎 C 、删除 D 、消磁

27. 对于信息安全风险评估的形式，下列说法正确的是 （ ） 。
A、分为差量评估和检查评估两种形式 B 、应以检查评估为主，自评估和检查评估相互结合、 互相 补充 C 、应以自评估为主，自评估和检查评估相互结合、互相补充 D 、分为自评估和基准评估两 种形式

28. ( )不是防火墙的工作模式。
A、路由模式 B 、混合模式 C 、超级模式 D 、透明模式

29. 一个数据仓库中发生了安全性破坏。 ( )有助于安全调查的进行。
A、访问路径 B 、数据分类 C 、数据定义 D 、时间戳

30. SYN FLOOD 攻击是通过( )协议完成的 资料

A、UDP B、AppleTalk C 、IPX/SPX D 、TCP

31. 信息安全管理体系中的 BCP 指的是什么（）。
A、灾难恢复计划 B 、系统安全性评估 C 、业务连续性计划 D 、系统扩容计划

32. 输入控制的目的是确保( )。
A、对数据文件访问的授权 B 、完全性、准确性以及输入的有效性 C 、完全性、准确性以及更新 的有效性 D 、对程序文件访问的授权

33. 实施 SYN Flood ，攻击者需向攻击目标发送( )TCP 包 A、 SYN B、FIN C 、ACK D、SYNACK

34. 防火墙的主要性能指标不包括（）。
A、吞吐量 B 、新建连接数 C 、延时 D 、误报率

35. 以下哪个方法不能用于实现检测入侵攻击（）。
A、神经网络 B 、化学方法 C 、统计方法 D 、专家系统

36. 下列攻击方式中，既属于身份冒领，也属于 IP 欺骗的是( )。
A、 SQL 注入 B 、溢出攻击 C 、会话动持 D 、SYN flood

37. 信息安全管理体系第一层的文件主要是（）。
A、实施记录 B 、方针和总体政策 C 、实施表格 D 、工作程序

39. 从目前的情况看， 对所有的计算机系统来说， 以下（） 威胁是最为严重的， 可能造成巨大的损 害。
A、没有充分训练或粗心的用户 B 、心怀不满的雇员 C 、Hackers 和 Crackers D 、分包商和承包 商

40. 默认情况下， Window 2000 域之间的信任关系有什么特点（）。
A、只能单向，可以传递 B 、可以双向，不可传递 C 、可以双向，可以传递 D 、只能单向，不可 传递

41. 渗透性测试属于( )所采用的方法。
A、资产识别 B 、安全措施识别 C 、威胁识别 D 、脆弱性识别

42. NIDS 部署在交换环境下，需要对交换机进行( )配置 A、端口映射 B 、混杂模式 C 、隐蔽模式 D 、端口镜像

43. 在 Linux 系统中， telnet 服务认证是（）。
A、单向认证 B 、第三方认证 C 、双向认证 D 、智能卡认证

44. 采用三层交换机 VLAN 隔离安全域，通过防火墙模块或( )进行安全域的隔离。
A、虚拟防火墙 B 、接口 C 、数字证书 D 、访问控制列表

45. Apache 服务器对目录的默认访问控制是( )。
A、”Deny”from”all ” B、 ”Allow ” from ” all ” C、 Order Deny, Allow
D、 Order Deny,”all ”

46.( )威胁不可以通过包过滤防火墙设置予以缓解或解决。 A、针对特定协议和端口的蠕虫攻击 B 、针对电脑的扫描 C 、针对特定网络服务的拒绝服务攻击 D、针对网页 ASP 脚本的数据库注入攻击

48. SSL 指的是 ( ) 。
A、加密认证协议 B 、安全通道协议 C 、授权认证协议 D 、安全套接层协议

49. 从风险分析的观点来看，计算机系统的最主要弱点是 ( ) 。
A、内部计算机处理 B 、外部计算机处理 C 、通讯和网络 D 、系统输入输出

51. 以下 ( ) 不属于恶意代码。
A、病毒 B 、特洛伊木马 C 、宏 D 、蠕虫

52. 从风险管理的角度，以下哪种方法不可取 ( ) 。
A、接受风险 B 、拖延风险 C 、转移风险 D 、分散风险

53. 使用入侵检测技术的核心问题是( )的建立以及后期的维护和更新。
A、异常模型 B 、审计日志 C 、网络攻击特征库 D 、规则集处理引擎

54. 安全域的具体实现可采用的方式为 ( ) 。
A、物理防火墙隔离 B 、以上都是 C 、 Vlan 隔离等形式 D 、虚拟防火墙隔离

55. 密码处理依靠使用密钥， 密钥是密码系统里的最重要因素， 以下哪一个密钥算法在加密数据与 解密时使用相同的密钥 ( ) 。
A、 RSA B、DSA C、DES D、DH

57. 在防火墙上不能截获( )密码/ 口令。
A、 html 网页表单 B 、ftp C 、telnet D 、 ssh

58. 对信息系统而言，说法正确的是 ( ) 。
A、存在风险一定不安全 B 、一次彻底的风险评估， 将对信息系统的安全状况做出准确的判断 C 、 只要风险控制在可接受的范围内，就可以达到系统稳定运行的目的
D 、未发生安全事件，信息系 统就被认为安全
资料

59. 从安全属性对各种网络攻击进行分类，截获攻击是针对（ ）的攻击，阻断攻击是针对（ ） 的攻击。
A、机密性，完整性 B 、真实性、完整性 C 、完整性、可用性 D 、机密性、可用性

60. 包过滤型防火墙的特点 （ ） 。
A、处理包的速度要比代理服务器慢 B 、检测速度快 C 、包过滤可以访问包中所有信息 D 、能阻 止多种类型的 IP 欺骗

61. 入侵检测系统在进行信号分析时，一般通过三种常用的技术手段， （ ）不属于通常的三种 技术手段。
A、模式匹配 B 、密文分析 C 、完整性分析 D 、统计分析

62. 在信息系统安全中，风险由以下 （ ） 因素共同构成的。
A、攻击和脆弱性 B 、威胁和破坏 C 、威胁和脆弱性 D 、威胁和攻击

63. 在网络中，若有人非法使用 Sniffer 软件查看分析网络数据， （ ）协议应用的数 据不会受 到攻击。
A、 telnet B 、http C 、 ssh D 、ftp

64. 下列哪一个说法是正确的 （ ） 。
A、风险越大，越不需要保护 B 、越是中等风险，越需要保护 C 、风险越大，越需要保护 D 、风 险越小，越需要保护

65. 一般来说，网络安全中人是薄弱的一环， 也是最难管理的一环，作为安全管理人员， （ ） 能够 提升人员安全意识。 （ 分值： 0.5）
A、教员工认识网络设备 B 、做好安全策略 C 、设置双重异构防火墙 D 、定期组织企业内部的全 员信息安全意识强化培训

66. 包过滤在本地端接收数据包时，一般不保留上下文，只根据（ ）做决定。
A、以前数据包的内容 B 、目前数据包的内容 C 、以前数据包的数据信息 D 、目前数据包的数据 信息

68. 入侵检测技术起源于（ ）技术。
A、网络管理 B 、数据库 C 、防火墙 D 、安全审计

69. 作为组织具有价值的信息或资源， （ ） 是安全策略保护的对象。
A、系统 B 、资产 C 、财产 D 、信息

70. 审计追踪日志中，一般不会包括（ ）信息。
A、授权用户列表 B 、被获取的数据 C 、进行尝试的终端 D 、事件或交易尝试的类型
资料

72. 渗透性测试属于（ ）所采用的方法。
A、资产识别 B 、安全措施识别 C 、威胁识别 D 、脆弱性识别

73.（)类型的攻击，攻击者在远程计算机使用一个自复制产生流量的程序。
A、字典攻击 B 、病毒攻击 C 、非法服务器攻击 D 、劫持攻击

74. 以下对安全风险的描述最准确的是（）。
A、安全风险是指一种特定脆弱性利用一种或一组威胁造成组织的资产损失或损害的可能性 B 、安全风险是指资产的脆弱性被威胁利用的情形 C 、安全风险是指一种特定的威胁利用一种或一组脆 弱性造成组织的资产损失或损害的可能性 D 、安全风险是指一种特定的威胁利用一种或一组脆弱 性造成组织的资产损失事件

75. 以下 （ ） 威胁不可以通过防火墙设置予以缓解或解决。
A、针对特定协议和端口的蠕虫攻击 B 、针对电脑的扫描 C 、针对特定网络服务的拒绝服务攻击 D、针对网页 ASP 脚本的数据库注入攻击

76. 假设网络 202.110.8.0 是一个危险的网络，那么就可以用( )禁止内部主机和该网络进 行通信。
A、源地址过滤 B 、根据防火墙具体配置，设置源地址或目的地址过滤 C 、源端口过滤 D 、目的 地址过滤

77. 防火墙的路由模式配置中 DNAT 策略里的转换后的地址一般为 （ ） 。
A、防火墙外网口地址 B 、服务器的 IP 地址 C 、防火墙 DMZ 口地址 D 、防火墙内网口地址

78. 在安全评估过程中，采取( )手段，可以模拟黑客入侵过程，检测系统安全脆弱性。
A、脆弱性评估 B 、手工检查 C 、渗透性测试 D 、风险分析测试

79. UNIX 和 Windows NT 操作系统是符合( )级别的安全标准。
A、A 级 B 、D 级 C 、C 级 D 、B 级

80. 防火墙的透明模式配置中在网桥上配置的 ip 主要用于 （ ） 。
A、管理 B 、双机热备 C 、NAT 转换 D 、保证连通性

题二(2)：判断题：
1. 入侵检测系统 IDS 通过对计算机网络或计算机系统中的若干关键点的信息收集和信息分析，从 中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，并实时做出安全响应。 ( )
2. 国家电网公司管理信息大区中的信息内外网间使用的是正向隔离装置。 ( )
3. 如果某个网络告知有威胁来自我方网络。在这种情况下，我们在验证对方身份后，将管理权限 给予对方，同时自己对本方网络进行调查监控，做好相互配合。 ( )
4. 病毒是一段可执行代码， 可以将自己负载在一个宿主程序中。 病毒感染可执行文件或脚本程序，

从不感染数据文件和文档。（ ）
5. 安全的口令，长度不得小于 6 位字符串，要求是字母和数字或特殊字符的混合，用户 名和口 令禁止相同。（ ）
6. 加密技术不仅可以保证信息的机密性，而且可以保证信息的完整性，还能够实现通信用户间的 身份认证和不可否认性。（ ）
7. 任何一种协议都是建立在双方的基础上的，信息流也是双向的，所以在考虑允许内部用户访问 Internet 时，必须允许数据包不但可以出站而且可以入站。（ ）
8. 允许内部主机以 Telnet 方式访问 Internet 上的任何主机，包过滤防火墙策略配置中内部访问 外部的策略的源端口为 23。（ ）
9. 宏属于恶意代码。（ ）
10. 在 Windows 操作系统安全模式下，木马程序不能启动。（ ）
11. 入侵检测系统可以弥补企业安全防御系统中的安全缺陷和漏洞。（ ）

题二(3)：简答题：
1. 入侵检测系统主要分为哪两类，它们各自的特点是什么？ 基于主机的入侵检测系统和基于网络的入侵检测系统。
(1) 基于主机的入侵检测系统。 用于保护单台主机不受网络攻击行为的侵害， 需要安装在被保护 的主机上。 直接与操作系统相关，控制文件系统以及重要系统文件，确保操作系统不会被随意删 除。 按检测对象不同，分为两种：
1)网络链接检测。 网络链接检测是对试图进入主机的数据流进行检测， 分析确定是否有入侵 行为，避免或减少这些数据流进入主机系统后造成损害。 作用：有效地检测出是否存在攻击探测 行为。 管理员：设置好访问控制列表，审核。
2)主机文件检测。 主机型入侵检测系统往往以系统日志、应用程序日志等作为数据源，当然 也可以通过其他手段(如监督系统调用)从所在的主机收集信息进行分析。
(2) 基于网络的入侵检测系统。
1)网络链接检测。
网络链接检测是对试图进入主机的数据流进行检测， 分析确定是否有入侵行为， 避免或 减少这些数据流进入主机系统后造成损害。 作用：有效地检测出是否存在攻击探测行为。 管理员： 设置好访问控制列表，审核。
2)主机文件检测。 主机型入侵检测系统往往以系统日志、应用程序日志等作为数据源， 当 然也可以通过其他手段(如监督系统调用)从所在的主机收集信息进行分析。
3. 桌面计算机病毒和木马主要有哪些传播途径？ 计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或毁坏数据， 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，具有自我繁殖、大量传播和破坏系统 的特点。计算机 病毒主要通过文件系统、电子邮件、网页、即时通信软件和点对点软件、操 作系统漏洞、 U 盘、 移动硬盘等进行传播。
木马程序是指潜伏在电脑中， 受外部用户控制以窃取本机信息或控制权的程序。 它是具有欺骗性的 恶意程序，是一种基于远程控制的黑客工具，具有隐蔽性、非授权性