1、 （）就是入侵检测系统，它通过抓取网络上的所有报文，分析处理后，报告异常和重要的数据模式和行为模式，使网络安全管理员清楚地了解网络上发生的事件，并能够采取行动阻止可能的破坏。

A. IAS

B. IDS

C. IPS

D. IBS

答案：B

2、 在设备权限配置能力内，根据用户的业务需要，配置其所需的（）权限。

A. 最全

B. 最小

C. 最合适

D. 最大

答案：B

3、 机房应建立完善的系统和设备维护责任制度，机房内的各项现网设备应有专人负责管理，未经（）许可，他人不得随意进行操作？

A. 维护人员 维护人员

B. 机房主管人员

C. 监控人员

D. 厂商人员

答案：B

4、 如果存储的重要数据介质是光盘，则应该先（ ）再焚毁

A. 覆写

B. 捣碎

C.化学腐蚀

D.消磁

答案：B

5、 下列基于 ICMP 的扫描请求，不遵循查询/回应方式的是

A.address-mask

B.time-stamp

C.destination unreachable

D.echo

答案：C

6、 NTP 协议使用的端口为？

A.UDP 123

B.TCP 123

C.TCP 321

D.UDP321

答案：A

7、 下列说法不正确的是：（）

A.网络安全防御系统是个动态的系统，攻防技术都在不断发展。安防系统必须同时发展与更新。

B.建立 100% 安全的网络

C.系统的安全防护人员必须密切追踪最新出现的不安全因素和最新的安防理念，以便对现有的安防系统及时提出改进意见

D.安防工作是循序渐进、不断完善的过程

E.安防工作永远是风险、性能、成本之间的折衷。

答案：B

8、 目前网络垃圾短信过滤最主要的技术是基于垃圾短信的（）特征进行过

滤。

A.发送频率

B.主叫号码

C.关键字

D.目的号码

答案：C

9、 设备应支持对不同用户授予（）权限

A.相近

B.相同

C.不同

D.相似

答案：C

10、 什么命令关闭路由器的direct broadcast?

A.no broadcast

B.no ip direct-broadcast

C.no ip broadcast

D.ip prodcast disable

答案：B

11、 通信网的基本结构形式有五种，以下正确的说法是

A.网型、星型、线型、复合型、环型；

B.网型、星型、复合型、环型、总线型；

C.网型、星型、树型、环型、总线型；

D.网型、环型、线型、复合型、树型。

答案：B

12、 由于网络安全风险产生故障时应该采取（）原则。

A.先抢修故障，再抢通业务

B.先查找原因，再抢修故障

C.先抢通业务，再抢修故障

D.先抢修故障，再查找原因

答案：C

13、 下列哪些是防火墙的重要行为

A.准许

B.问候访问者

C.限制

D.日志记录

答案：C

14、 客户信息包括客户基本资料、客户身份鉴权信息、客户通信信息、（ ）等四大类。

A.客户通信内容

B.客户缴费记录

C.客户身份信息

D.客户通话记录

答案：A

15、 平台方式二主要利用数字 KVM ，进行基于图形、文本的维护记录，同时，可通过（）方式对系统进行管理。

A.带外

B.带内

C.SSH

D.telnet

答案：A

16、 安全事件准备阶段的工作内容主要有（）

A.对信息系统进行初始化的快照

B.备份应用程序

C.对应急事件进行抑制

D.对于业务恢复

答案：A

17、 风险评估的三个要素（）？

A.组织，技术和信息

B.硬件，软件和人

C.政策，结构和技术

D.资产，威胁和脆弱性

答案：D

18、彩信中心需要对 MM1 接口的上行彩信的大小进行限制,对于 3G 彩信，一般建议限制不大于（）

A.1M

B.2M

C.300K

D.50K

答案：C

19、 （）是指恶意人员绕过管理员的限制，上传任意类型的文件或者在禁

止写入的目录中写入文件。

A.非法转载

B.非法上传

C.非法下载

D.非法注入

答案：B

20、 windows 下的 nbtsta命令

A.可以查看进程列表

B.可以查看当前用户

C.可以查看当前的网络连接

D.可以用来查询涉及到 NetBIOS 信息的网络机器

答案：D

21、 衡量数字通信系统传输质量的指标是

A.话音清晰度

B.噪声功率

C.信噪比

D.误码率

答案：D

22、 设置安全域互访的原则为：（）

A.高保护等级访问低保护等级的安全域时只允许读，低保护等级访问高保护等级的安全域时只允许写。

B.高保护等级访问低保护等级的安全域时只允许写，低保护等级访问高保护

等级的安全域时只允许读。

C.高保护等级访问低保护等级的安全域时不允许写，低保护等级访问高保护等级的安全域时不允许读。

答案：B

23、 一般情况下，弱口令检查的快捷检查步骤是_____

A.选择设备，立即进行一次快速的检查

B.直接进行一次快速的检查

C.选择设备，弱口令字典类型，立即进行一次快速的检查

D.选择弱口令字典类型，立即进行一次快速的检查

答案：C

24、 在安全维护作业计划中，检查各防火墙访问控制策略的执行周期是_____

A.季度

B.半月

C.周

D.月

答案：C

25、 专用移动存储介质不再使用时，必须有专用介质管理员进行（）次以上数据填充和格式化后方可报废或进行物理销毁。

A.2

B.1

C.3

D.4

答案：A

26、 SNMP 只提供 3 种基本操作是

A.增操作、删操作、日志报告

B.获取信息、设置参数值和事件报告

C.Read: 读操作、Write:写操作、Trap 陷阱操作

D.Read: 读操作、Write:写操作、日志报告

答案：B

27、 系统漏洞类安全事件是指由于（）引起的安全事件

A.恶意用户利用发送虚假电子邮件、建立虚假服务网站、发送虚假网络消息

等方法

B.恶意用户利用挤占带宽、消耗系统资源等攻击方法

C.恶意用户利用以太网监听、键盘记录等方法获取未授权的信息或资料

D.恶意用户通过提交特殊的参数从而达到获取数据库中存储的数据、得到数

据库用户的权限

E.恶意用户利用系统的安全漏洞对系统进行未授权的访问或破坏

答案：E

28、在 UTM 校验未知数据流时，其 CPU 负荷达到 85% 以上，说明了什么？

A.正常现象

B.警示现象

C.错误现象

D.危机现象

答案：D

29、 题目：技术评估的一般流程？

A.手工检查-确定目标-远程扫描-报告分析-收集报告。

B.确定目标-手工检查-远程扫描-报告分析-收集报告；

C.确定目标-远程扫描-手工检查-报告分析-收集报告；

D.远程扫描-确定目标-手工检查-收集报告-报告分析；

答案：C

30、 重大故障处理完毕后，中国移动各省级公司网络维护部门应在（）日内通过工单以附件形式向集团公司网络部提交专题书面报告。

A.4

B.3

C.1

D.2

答案：D

31、 企业实施补丁加载方案的动机是？

A.追赶 IT 潮流

B.适应企业信息化的建设

C.将风险降至最低

D.保障企业数据安全

答案：C

32、 在网络安全中，中断指攻击者破坏网络系统的资源，使之变成无效的或无用的。这是对

A.保密性的攻击

B.完整性的攻击

C.可用性的攻击

D.真实性的攻击

答案：C

33、 IDS 系统的两大职责：实时监测和（）

A.应用审计

B.安全审计

C.账号审计

D.用户审计

答案：B

34、 一般安全事件应在（）内解决

A.8 小时

B.2 小时

C.无限期

D.4 小时

答案：A

35、 系统需提供 退出”功能，允许用户（）当前的会话。

A.自动终止

B.随时终止

C.强制终止

D.暂时终止

答案：C

36、 在安全维护作业计划中，检查应用系统端口、服务情况的执行周期是

_____

A.半月

B.周

C.月

D.季度

答案：B

37、 在 Windows 2000 操作系统下，以下工具不能用于查看系统开放端口和进程关联性的工具或命令是?

A.fport

B.tcpview

C.tcpvcon

D.netstat

答案：D

38、 对于非常重要的敏感数据因使用（ ）算法加密。

A.MD5

B.AES

C.HASH

答案：B

39、 代维公司办理的机房出入证有效期最长不可超过（）。其代维人员若因 故离职，代维公司必须将有关证件（代维资格证、机房出入证等）交还发证部门，并每月通报代维人员变动情况。

A.一个月

B.一周

C.三个月

D.一年

答案：C

40、 系统要防止将用户输入未经检查就用于构造数据库查询，防范（）攻

击。

A.查询注入

B.应用注入

C.WEB　注入

D.SQL　注入

答案：D

41、 持有（）的人员方可安装相应的电气设备和电气线路。测试电气设 备的电源是否正常应使用相应的测量工具，禁止用手触及电气设备的带电部分和使用短路的方法进行试验。

A.弱电资格证

B.电气资格证

C.网络安全证

D.上岗证

答案：B

42、 相关部门的安全分工中，通信线路的防中断属于哪个部门负责

A.网络部

B.研究院

C.业务支撑系统部

D.综合部

答案：A

43、 网络欺骗类安全事件是指由于（）所引起的安全事件。

A.恶意用户利用系统的安全漏洞对系统进行未授权的访问或破坏

B.恶意用户通过提交特殊的参数从而达到获取数据库中存储的数据、得到数据库用户的权限

C.恶意用户利用发送虚假电子邮件、建立虚假服务网站、发送虚假网络消息等方法

D.恶意用户利用以太网监听、键盘记录等方法获取未授权的信息或资料

E.恶意用户利用挤占带宽、消耗系统资源等攻击方法

答案：C

44、 专用介质使用者向专用介质管理员提出申请使用专用移动存储介质，专用介质管理员根据（）审核其是否具有使用授权。

A.《专用移动存储介质使用授权表》

B.《专用移动存储介质操作授权表》

C.《专用移动存储介质使用申请表》

D.《专用移动存储介质使用表》

答案：A

45、 用于查看/var/log/wtmp日志的命令是

A.lastmp

B.last

C.lastwtmp

D.lastlog

答案：D

46、 系统要防止将用户输入未经检查就直接输出到用户浏览器，防范（）攻击。

A.跨站脚本

B.web 脚本

C.手工脚本

D.插件脚本

答案：A

47、 用户访问企业生产系统时出现用户名或密码错误，该信息会被记录在生产系统中以下哪个变量中？

A.系统日志

B.应用日志

C.安全日志

D.IE日志

答案：A

48、 题目：下面关于VISTA 提供的计算机安全措施那个是错误的？

A.无需安装其他杀毒软件，仅依靠Windows Defender 可以查杀所有病毒。

B.
对恶意软件抵抗能力更强的计算机，受病毒、间谍软件、蠕虫和其他潜在不需要的软件的影响较少。

C.更加安全的联机体验

D.更清楚地了解 PC 中存在的漏洞，并获得更好的指导来帮助还原更安全的配置。

答案：A

49、 美国国防部与国家标准局将计算机系统的安全性划分为不同的安全等级。Solaris属于（）等级

A.C2

B.C4

C.C1

D.C3

答案：A

50、 为了达到防止非法手机盗打电话的目的，GSM 系统在 A 接口引入了签权技术。目前在中国移动的网络上实际运用时，对鉴权的要求为：（ ）

A.各种位置更新时进行鉴权

B.业务接入时进行鉴权

C.主叫进行鉴权

D.被叫进行鉴权

答案：A

51、 按照业务横向将支撑系统划分，可分为以下安全域：（）

A.互联接口区、核心生产区、日常维护管理区（维护终端）、第三方接入区（漫游区）、DMZ 区

B.集团网管系统安全子域、省公司网管系统安全子域、地市分公司的网管系统安全子域

C.业务支撑系统安全域、网管系统安全域、企业信息化系统安全域

答案：C

52、 以下属于安全管控平台策略管理模块可以管理的为

A.访问控制策略

B.密码策略

C.防火墙策略

D.信息加密策略

答案：B

53、 题目：以下哪项技术不属于预防病毒技术的范畴？

A.校验文件

B.系统监控与读写控制;

C.引导区保护;

D.加密可执行程序;

答案：D

54、在安全维护作业计划中，入侵检测系统健康性检查的执行周期是_____

A.月

B.半月

C.周

D.天

答案：D

55、 安全管理工作必须贯彻“（）”的方针？

A.谁使用、谁负责

B.群防群治

C.一把手问责

D.安全第一、预防为主、综合治理

答案：D

56、 网络窃听类安全事件是指由于()所引起的安全事件。

A.恶意用户利用系统的安全漏洞对系统进行未授权的访问或破坏

B.恶意用户利用发送虚假电子邮件、建立虚假服务网站、发送虚假网络消息