**模块二**

[**第一部分**](true) **网络安全事件响应**

[任务1：Unix服务器应急响应](true)**（70分）**

A集团的Debian服务器被黑客入侵，该服务器的Web应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

[本任务素材清单：Unix服务器虚拟机](true)

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务1：Unix服务器虚拟机** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交攻击者的IP地址 |  |
| 2 | 请提交攻击者使用的操作系统 |  |
| 3 | 请提交攻击者进入网站后台的密码 |  |
| 4 | 请提交攻击者首次攻击成功的时间，格式：DD/MM/YY:hh:mm:ss |  |
| 5 | 请提交攻击者上传的恶意文件名（含路径） |  |
| 6 | 请提交攻击者写入的恶意后门文件的连接密码 |  |
| 7 | 请提交攻击者创建的用户账户名称 |  |
| 8 | 请提交恶意进程的名称 |  |

[任务1：Unix服务器应急响应](true)**（70分）**

A集团的Debian服务器被黑客入侵，该服务器的Web应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

[本任务素材清单：Unix服务器虚拟机](true)

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务1：Unix服务器虚拟机** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交攻击者的IP地址 |  |
| 2 | 请提交攻击者使用的操作系统 |  |
| 3 | 请提交攻击者进入网站后台的密码 |  |
| 4 | 请提交攻击者首次攻击成功的时间，格式：DD/MM/YY:hh:mm:ss |  |
| 5 | 请提交攻击者上传的恶意文件名（含路径） |  |
| 6 | 请提交攻击者写入的恶意后门文件的连接密码 |  |
| 7 | 请提交攻击者创建的用户账户名称 |  |
| 8 | 请提交恶意进程的名称 |  |
| 9 | 请提交恶意进程对外连接的IP地址 |  |

[任务](true)1：Linux服务器应急响应（70分）

A集团的Linux服务器被黑客入侵，该服务器的Web应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

[本任务素材清单：](true)Linux服务器虚拟机

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务1：Linux服务器应急响应** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交攻击者的IP地址 |  |
| 2 | 请提交攻击者使用的操作系统 |  |
| 3 | 请提交攻击者进入网站后台的密码 |  |
| 4 | 请提交攻击者首次攻击成功的时间，格式：DD/MM/YY:hh:mm:ss |  |
| 5 | 请提交攻击者上传的恶意文件名（含路径） |  |
| 6 | 请提交攻击者写入的恶意后门文件的连接密码 |  |
| 7 | 请提交攻击者创建的用户账户名称 |  |
| 8 | 请提交恶意进程的名称 |  |

[任务](true)1：Windows服务器应急响应（70分）

A集团的Windows服务器被黑客入侵，该服务器的Web应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，发现系统中的漏洞，并对发现的漏洞进行修复。

[本任务素材清单：Windows](true)服务器虚拟机。

受攻击的Server服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

注意：Server服务器的基本配置参见附录，若题目中未明确规定，请使用默认配置。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| [**任务**](true)**1：Windows server服务器应急响应** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交攻击者攻击成功的第一时间，格式：YY:MM:DD hh:mm:ss |  |
| 2 | 请提交攻击者的浏览器版本 |  |
| 3 | 请提交攻击者目录扫描所使用的工具名称 |  |
| 4 | 找到攻击者写入的恶意后门文件，提交文件名（完整路径） |  |
| 5 | 找到攻击者隐藏在正常web应用代码中的恶意代码，提交该文件名（完整路径） |  |
| 6 | 请提交内存中可疑进程的PID |  |
| 7 | 请提交攻击者执行过几次修改文件访问权限的命令 |  |
| 8 | 请指出可疑进程采用的自动启动的方式 |  |

[第二部分](true) **数字取证调查（150分）**

[任务](true)**2 ：基于windows的内存取证（40分）**

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析A集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

[本任务素材清单：存储镜像、内存镜像。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务2：基于windows的内存取证** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交内存中恶意进程的名称 |  |
| 2 | 请提交恶意进程写入的文件名称（不含路径） |  |
| 3 | 请提交admin账户的登录密码 |  |
| 4 | 请提交攻击者创建的账户名称 |  |
| 5 | 请提交在桌面某文件中隐藏的flag信息，格式：flag{...} |  |

[任务](true)2 ：基于Linux的内存取证（40分）

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析A集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

[本任务素材清单：存储镜像、内存镜像。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务2：基于Linux的内存取证** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交用户目录下压缩包的解压密码 |  |
| 2 | 请提交root账户的登录密码 |  |
| 3 | 请指出攻击者通过什么命令实现提权操作 |  |
| 4 | 请指出内存中恶意进程的PID |  |
| 5 | 请指出恶意进程加密文件的文件类型 |  |

[任务2：基于MacOS的内存取证](true)（40分）

A集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析A集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

[本任务素材清单：存储镜像、内存镜像。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务2：基于MacOS的内存取证** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交用户目录下压缩包的解压密码 |  |
| 2 | 请提交root账户的登录密码 |  |
| 3 | 请指出攻击者通过什么命令实现提权操作 |  |
| 4 | 请指出内存中恶意进程的PID |  |
| 5 | 请指出恶意进程加密文件的文件类型 |  |

[任务](true)**3：通信数据分析取证（USB）（50分）**

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

[本任务素材清单：捕获的通信数据文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务3：通信数据分析取证（USB）** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交攻击者一共上传了几个文件 |  |
| 2 | 请提交攻击者上传的木马文件的MD5值 |  |
| 3 | 请写出攻击者运行木马文件的命令（含参数） |  |
| 4 | 攻击者获取主机权限之后，进行了回连操作，请提交回连的IP地址 |  |

[任务3：通信数据分析取证(工控)](true)（50分）

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

[本任务素材清单：捕获的通信数据文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务3：通信数据分析取证(工控)** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交攻击者通过什么协议发起的攻击 |  |
| 2 | 请提交攻击者第一次攻击成功的时间 |  |
| 3 | 请提交攻击者在目标主机上上传的文件名 |  |
| 4 | 请解密出上传的文件内容 |  |

[任务](true)**3：通信数据分析取证（TPC/IP）（50分）**

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑通信数据。请您根据捕捉到的通信数据，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

[本任务素材清单：捕获的通信数据文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务3：通信数据分析取证（TPC/IP）** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请指出攻击者使用什么协议传输了敏感信息 |  |
| 2 | 请提交两个攻击者用于收信息的二级域名 |  |
| 3 | 请提交攻击者传输的敏感信息key1，格式：key1{xxx} |  |
| 4 | 请提交攻击者获取的flag，格式：flag{xxx} |  |

[任务](true)3：通信数据分析取证（USB）（50分）

A集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，分解出隐藏的恶意程序，并分析恶意程序的行为。

[本任务素材清单：捕获的通信数据文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务3：通信数据分析取证（USB）** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请提交攻击者一共上传了几个文件 |  |
| 2 | 请提交攻击者上传的木马文件的MD5值 |  |
| 3 | 请写出攻击者运行木马文件的命令（含参数） |  |
| 4 | 攻击者获取主机权限之后，进行了回连操作，请提交回连的IP地址 |  |

[任务4：基于Windows计算机单机取证](true)**（60分）**

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”“evidence 2”……“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

[本任务素材清单：取证镜像文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务4：基于Windows计算机单机取证** | | |
| **证据编号** | **在取证镜像中的文件名** | **镜像中原文件Hash码（MD5，不区分大小写）** |
| evidence 1 |  |  |
| evidence 2 |  |  |
| evidence 3 |  |  |
| evidence 4 |  |  |
| evidence 5 |  |  |
| evidence 6 |  |  |
| evidence 7 |  |  |
| evidence 8 |  |  |
| evidence 9 |  |  |
| evidence 10 |  |  |

[任务](true)**4： 基于Linux计算机单机取证（60分）**

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

[本任务素材清单：取证镜像文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务4：基于Linux计算机单机取证** | | |
| 证据编号 | 在取证镜像中的文件名 | 镜像中原文件Hash码（MD5，不区分大小写） |
| evidence 1 |  |  |
| evidence 2 |  |  |
| evidence 3 |  |  |
| evidence 4 |  |  |
| evidence 5 |  |  |
| evidence 6 |  |  |
| evidence 7 |  |  |
| evidence 8 |  |  |
| evidence 9 |  |  |
| evidence 10 |  |  |

[任务](true)4： 基于MacOS计算机单机取证（60分）

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”、“evidence 2”、……、“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

[本任务素材清单：取证镜像文件。](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务4：基于MacOS计算机单机取证** | | |
| 证据编号 | 在取证镜像中的文件名 | 镜像中原文件Hash码（MD5，不区分大小写） |
| evidence 1 |  |  |
| evidence 2 |  |  |
| evidence 3 |  |  |
| evidence 4 |  |  |
| evidence 5 |  |  |
| evidence 6 |  |  |
| evidence 7 |  |  |
| evidence 8 |  |  |
| evidence 9 |  |  |
| evidence 10 |  |  |

[第三部分](true) **应用程序安全**

[任务5：Linux恶意程序分析](true)**（50分）**

A集团发现其发布的应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

[本任务素材清单：Linux恶意程序](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务5：Linux恶意程序分析** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交恶意程序回传数据的url地址 |  |
| 2 | 请指出恶意程序会加密哪些类型的文件 |  |
| 3 | 请指出恶意程序加密文件的算法 |  |
| 4 | 请指出恶意程序创建的子进程名称 |  |

[任务](true)**5：Windows恶意程序分析（50分）**

A集团发现其发布的应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

[本任务素材清单：](true)**Windows恶意程序**

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务5：Windows恶意程序分析** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请指出恶意程序的壳名称 |  |
| 2 | 请提交恶意程序反向连接的IP地址 |  |
| 3 | 请提交恶意程序用于解密数据的函数名称 |  |
| 4 | 请提交恶意程序反弹shell的命令（含参数） |  |

[任务](true)5：Android恶意程序分析（50分）

A集团发现其发布的Android移动应用程序文件遭到非法篡改，您的团队需要协助A集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

[本任务素材清单：](true)Android的apk文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务5：Android恶意程序分析** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交恶意应用回传数据的url地址 | 提交正确flag值得分 |
| 2 | 请提交恶意应用保存数据文件名称（含路径） | 提交正确flag值得分 |
| 3 | 请提交恶意应用解密数据的密钥 | 提交正确flag值得分 |
| 4 | 请描述恶意应用的行为 | 提交正确flag值得分 |

[任务6：JAVA语言代码审计](true)**（30分）**

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的一部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

[本任务素材清单：Java源文件](true)

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务6：JAVA语言代码审计** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请指出存在安全漏洞的代码行 |  |
| 2 | 请指出可能利用该漏洞的威胁名称 |  |
| 3 | 请修改该代码行使其变得安全 |  |

[任务](true)6：PHP代码审计（30分）

A集团发现其发布的web应用程序中被黑客种植了webshell，文件遭到非法篡改，您的团队需要协助A集团对该恶意脚本程序样本进行分析、对其攻击/破坏的行为进行调查取证。

[本任务素材清单：](true)PHP文件。

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务6：PHP代码审计** | | |
| **序号** | **任务内容** | **答案** |
| 1 | 请提交存在安全漏洞的代码行 |  |
| 2 | 请指出安全漏洞的名称 |  |
| 3 | 请修改该代码行使其变得安全 |  |

[任务](true)6：C语言代码审计（30分）

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的一部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

[本任务素材清单：](true)C源文件

请按要求完成该部分的工作任务。

|  |  |  |
| --- | --- | --- |
| **任务6：C语言代码审计** | | |
| 序号 | 任务内容 | 答案 |
| 1 | 请指出存在安全漏洞的代码行 |  |
| 2 | 请指出可能利用该漏洞的威胁名称 |  |
| 3 | 请提出加固修改建议 |  |

**模块三**

[项目和任务描述](true)

在A集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取flag值。网络环境参考样例请查看附录A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

[•](true) 数据库攻击

• 枚举攻击

• 权限提升攻击

• 基于操作系统的攻击

• 逆向分析

• 密码学分析

• 隐写分析

所有设备和服务器的IP地址请查看现场提供的设备列表。

[特别提醒](true)

通过找到正确的flag值来获取得分，flag统一格式如下所示：

flag{<flag值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏感信息并利用工具把它找出来。

注：部分flag可能非统一格式，若存在此情况将会在题目描述中明确指出flag格式，请注意审题。

[工作任务](true)

[一、      
商城购物系统](true)**（45分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务一** | 请对商城购物系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| **任务二** | 请对商城购物系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |
| **任务三** | 请对商城购物系统进行黑盒测试，利用漏洞找到flag3，并将flag3提交。flag3格式flag3{<flag值>} |  |  |

**二、      
企业云盘系统（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务四** | 请对企业云盘系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| **任务五** | 请对企业云盘系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |

**三、      
FTP服务器（165分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务六** | 请获取FTP服务器上task6目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务七** | 请获取FTP服务器上task7目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务八** | 请获取FTP服务器上task8目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务九** | 请获取FTP服务器上task9目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十** | 请获取FTP服务器上task10目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十一** | 请获取FTP服务器上task11目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十二** | 请获取FTP服务器上task12目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| **任务十三** | 请获取FTP服务器上task13目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**四、      
存储服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务十四** | 存储服务器10000端口存在漏洞，获取FTP服务器上task14目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**五、      
大数据服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| **任务十五** | 大数据服务器10001端口存在漏洞，获取FTP服务器上task15目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

[一、         
门户](true)**网站（45分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务一 | 请对门户网站进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| 任务二 | 请对门户网站进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |
| 任务三 | 请对门户网站进行黑盒测试，利用漏洞找到flag3，并将flag3提交。flag3格式flag3{<flag值>} |  |  |

**一、人力资源管理系统（45分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务一 | 请对人力资源管理系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| 任务二 | 请对人力资源管理系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |
| 任务三 | 请对人力资源管理系统进行黑盒测试，利用漏洞找到flag3，并将flag3提交。flag3格式flag3{<flag值>} |  |  |

**二、         
办公系统（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务四 | 请对办公系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| 任务五 | 请对办公系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |

**二、     
邮件系统（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务四 | 请对邮件系统进行黑盒测试，利用漏洞找到flag1，并将flag1提交。flag1格式flag1{<flag值>} |  |  |
| 任务五 | 请对邮件系统进行黑盒测试，利用漏洞找到flag2，并将flag2提交。flag2格式flag2{<flag值>} |  |  |

**三、         
FTP服务器（165分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务六 | 请获取FTP服务器上task6目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务七 | 请获取FTP服务器上task7目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务八 | 请获取FTP服务器上task8目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务九 | 请获取FTP服务器上task9目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十 | 请获取FTP服务器上task10目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十一 | 请获取FTP服务器上task11目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十二 | 请获取FTP服务器上task12目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十三 | 请获取FTP服务器上task13目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**三、     
FTP服务器（165分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务六 | 请获取FTP服务器上task6目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务七 | 请获取FTP服务器上task7目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务八 | 请获取FTP服务器上task8目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务九 | 请获取FTP服务器上task9目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十 | 请获取FTP服务器上task10目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十一 | 请获取FTP服务器上task11目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十二 | 请获取FTP服务器上task12目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务十三 | 请获取FTP服务器上task13目录下的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**四、         
应用系统服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务十四 | 应用系统服务器10000端口存在漏洞，获取FTP服务器上task14目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**二、         
认证服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务十四 | 认证服务器10000端口存在漏洞，获取FTP服务器上task14目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

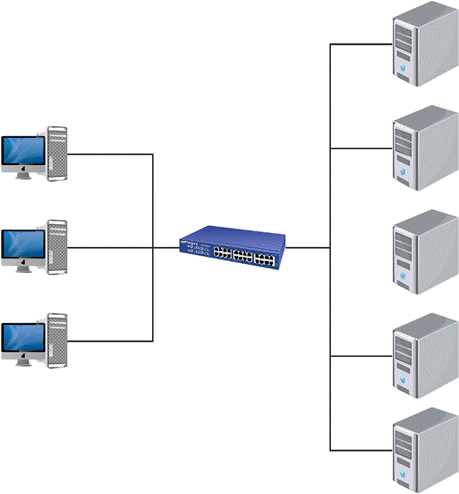
**五、         
测试系统服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务十五 | 应用系统服务器10001端口存在漏洞，获取FTP服务器上task15目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

**二、         
运维服务器（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 任务编号 | 任务描述 | 答案 | 分值 |
| 任务十五 | 运维服务器10001端口存在漏洞，获取FTP服务器上task15目录下的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

[附录](true)A



**六、         
理论技能与职业素养（100分）**

**“信息安全管理与评估”测试题（样题）**

【注意事项】

1.理论测试前请仔细阅读测试系统使用说明文档，按提供的账号和密码登录测试系统进行测试，账号只限1人登录。

2.该部分答题时长包含在第三阶段比赛时长内，请在临近竞赛结束前提交。

3.参赛团队可根据自身情况，可选择1-3名参赛选手进行作答，团队内部可以交流，但不得影响其他参赛队。

**一、 单选题 （每题2分，共35题，共70分）**

1、《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过，现予公布，自（  ）起施行。

A、2020年9月1日

B、2021年9月1日

C、2020年1月1日

D、2021年1月1日

2、下列(   )方式属于对学生进行信息道德与信息安全教育。

A、用计算机播放影片

B、用计算机为某活动搜索素材

C、用计算机处理班级照片

D、播放计算机犯罪新闻专题片

3、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（  ）。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

4、下面程序的运行结果是: ＃i nclude&amp;lt;stdio.h&amp;gt; {int k=0; char c='A'; do {switch(c++) {case 'A':k++;break; case 'B':k--; case'C':k+=2;break; case 'D':k=k%2;continue。

A、 k=0

B、 k=2

C、 k=3

D、 k=4

5、大学遭遇到DDOS攻击，那么根据网络安全应急预案，启动应急响应方案时，可以将应急预案定为哪个等级？（   ）

A、 3级

B、 4级

C、 2级

D、 1级

6、以下不属入侵检测中要收集的信息的是（   ）。

A、 系统和网络日志文件

B、 目录和文件的内容

C、 程序执行中不期望的行为

D、 物理形式的入侵信息

7、外部数据包过滤路由器只能阻止一种类型的IP欺骗，即（ ），而不能阻止DNS欺骗？

A、 内部主机伪装成外部主机的IP

B、 内部主机伪装成内部主机的IP

C、 外部主机伪装成外部主机的IP

D、 外部主机伪装成内部主机的IP

8、部署全网状或部分网状 IPSEC VPN时为减小配置工作量可以使用哪种技术。（   ）

A、 L2tp+IPSEC

B、 DVPN

C、 IPSEC over GRE

D、 动态路由协议

9、在一下古典密码体制中，属于置换密码的是？（   ）

A、 移位密码

B、 倒叙密码

C、 仿射密码

D、 PlayFair 密码

10、数据库管理员应该定期对数据库进行重组，以保证数据库性能。下列有关数据库重组工作的说法，错误的是（  ）。

A、 重组工作中可能会对数据库数据的磁盘分区方法和存储空间进行调整

B、 重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式

C、 重组工作一般在数据库运行一段时间后进行，不应频繁进行数据库重组

D、 重组工作中应尤其注意频繁修改数据的表，因为这些表很容易出现存储碎片，导致效率下降

11、Skipjack是一个密钥长度为(     )位。

A、 56

B、 64

C、 80

D、 128

12、m-序列本身是适宜的伪随机序列产生器，但只有在（    ）下，破译者才不能破解这个伪随机序列。

A、 唯密文攻击

B、 已知明文攻击

C、 选择明文攻击

D、 选择密文攻击

13、小李在使用nmap对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是什么？（   ）

A、 文件服务器

B、 邮件服务器

C、 WEB服务器

D、 DNS服务器

14、下面不是 Oracle 数据库支持的备份形式的是（  ）。

A、 冷备份

B、 温备份

C、 热备份

D、 逻辑备份

15、以下关于TCP和UDP协议的描述中，正确的是？（   ）

A、 TCP是端到端的协议，UDP是点到点的协议

B、 TCP是点到点的协议，UDP是端到端的协议

C、 TCP和UDP都是端到端的协议

D、 TCP和UDP都是点到点的协议

16、下面不是计算机网络面临的主要威胁的是?（   ）

A、 恶意程序威胁

B、 计算机软件面临威胁

C、 计算机网络实体面临威胁

D、 计算机网络系统面临威胁

17、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（   ）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

18、关于并行数据库，下列说法错误的是（   ）。

A、 层次结构可以分为两层，顶层是无共享结构，底层是共享内存或共享磁盘结构

B、 无共享结构通过最小化共享资源来降低资源竞争，因此具有很高的可扩展性，适合于OLTP应用

C、 并行数据库系统经常通过负载均衡的方法来提高数据库系统的业务吞吐率

D、 并行数据库系统的主要目的是实现场地自治和数据全局透明共享

19、Str='heiheihei' print str[3:]将输出？（   ）

A、 hei

B、 heihei

C、 eih

D、 ihe

20、包过滤型防火墙工作在?（   ）

A、 会话层

B、 应用层

C、 网络层

D、 数据链路层

21、下面是个人防火墙的优点的是?（   ）

A、 运行时占用资源

B、 对公共网络只有一个物理接口

C、 只能保护单机，不能保护网络系统

D、 增加保护级别

22、关于IP提供的服务，下列哪种说法是正确的？（   ）

A、 IP提供不可靠的数据投递服务，因此数据包投递不能受到保障

B、 IP提供不可靠的数据投递服务，因此它可以随意丢弃报文

C、 IP提供可靠的数据投递服务，因此数据报投递可以受到保障

D、 IP提供可靠的数据投递服务，因此它不能随意丢弃报文

23、print type(2.0)将输出？（   ）

A、 <type 'long'>

B、 <type 'str'>

C、 <type 'int'>

D、 <type 'float'>

24、Open函数中w 参数的作用是？（   ）

A、 读文件内容

B、 写文件内容

C、 删除文件内容

D、 复制文件内容

25、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（   ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

26、在RHEL5服务器中，查看用户vanzk密码记录的操作及输出如下所示: [root@pc05~]#grep vanzk /etc/shadowvanzk:!!$1$fKuFV9X8$VxFk0Ergj4uzP9UZGnleb.:15771:0:99999:7::: 则据此可判断用户vanzk的账号（ ）。

A、 每次设置新的密码后，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录

D、 使用的密码长度超过8位，安全性较高

27、Shell编程条件判断中，文件权限判断说法错误的是？

A、 -r 判断该文件是否存在，并且该文件是否拥有读写权限

B、 -w 判断该文件是否存在，并且该文件是否拥有写权限

C、 -x 判断该文件是否存在，并且该文件是否拥有执行权限

D、 -u 判断该文件是否存在，并且该文件是否拥有SUID权限

28、IPSec包括报文验证头协议AH 协议号（）和封装安全载荷协议ESP协议号（ )。

A、 51 50

B、 50 51

C、 47 48

D、 48 47

29、VIM光标操作说法中错误的是？（   ）

A、 h光标向左移动一位

B、 2j 光标向下移动两行

C、 w 跳到下一个单词的词尾

D、 G 跳到文档的最后一行

30、Linux软件管理rpm命令，说法不正确的是？（   ）

A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示2%

C、 -q PACKAGE\_NAME：查询指定的包是否已经安装

D、 -e 升级安装包

31、部署IPSEC VPN 时，配置什么安全算法可以提供更可靠的数据验证（).

A、 DES

B、 3DES

C、 SHA

D、 128位的MD5

32、指数积分法（Index Calculus）针对下面那种密码算法的分析方法？

A、 背包密码体制

B、 RSA

C、 ElGamal

D、 ECC

33、Linux的基本命令ls，其选项-l 代表的是？

A、 显示详细信息

B、 查看目录属性

C、 人性化显示文件大小

D、 显示文件索引号

34、VIM命令中，用于撤销的命令是？

A、 a

B、 x

C、 p

D、 u

35、你想发送到达目标网络需要经过那些路由器，你应该使用什么命令？

A、 Ping

B、 Nslookup

C、 Traceroute

D、 Ipconfig

**二、 多选题 （每题3分，共10题，共30分）**

1、数据库系统可能的潜在安全风险包括（）。

A、 操作系统安全风险，包括软件的缺陷、未进行软件安全漏洞修补工作、脆弱的服务和选择不安全的默认配置

B、 数据库系统中可用的但并未正确使用的安全选项、危险的默认设置、给用户不适当的权限、对系统配置的未经授权的改动等

C、 不及时更改登录密码或密码太过简单，存在对重要数据的非法访问以及窃取数据库内容或恶意破坏等

D、 数据库系统的内部风险，如内部用户的恶意操作等

2、SQL Server 中的预定义服务器角色有（）。

A、 Sysadmin

B、 Serveradmm

C、 Setupadmin

D、 Securityadmin

3、想使用python输出im happy下面哪些写法是正确的？

A、 print (im happy)

B、 print 'im happy'

C、 echo 'im happy'

D、 print '''im happy'''

4、以下属于多表代换的密码是？

A、 Playfair

B、 Polybius

C、 Vigenere

D、 Hill密码

5、下列关于SQL Server 2008身份验证模式的说法，正确的是（）。

A、 在"Windows身份验证模式"下，不允许sa登录到SQL Server服务器

B、 在"Windows身份验证模式"下，所有Windows用户都自动具有登录到SQL Server服务器的权限

C、 不管是哪种身份验证模式，Windows中的Administrator无需授权就可登录到SQL Server服务器

D、 安装好 SQL Server之后，可以根据需要随时更改身份验证模式

6、数据库访问控制的粒度可能有（）。

A、 数据库级

B、 表级

C、 记录级 ( 行级 )

D、 属性级

7、操作系统安全主要包括（）等方面 。

A、 账户密码安全和文件共享安全

B、 文件权限管理和用户权限管理

C、 日志审计和远程访问权限管理

D、 文件夹选项和安全选项

8、IPSec可以提供哪些安全服务（)

A、 数据机密性

B、 数据完整性

C、 数据来源认证

D、 防重放攻击

9、关于类的说法，下面哪些是错误的？

A、 私有方法和私有变量只能在类的内部使用

B、 一个类只能创建一个实例

C、 两个不同的类中的方法不能重名

D、 创建类的实例时，传入的变量类型要和类中定义的一致

10、IKE的主要功能包括()

A、 建立IPSec安全联盟

B、 防御重放攻击

C、 数据源验证

D、 自动协商交换密钥

[一、       理论技能与职业素养（100分）](true)

**一、 单选题 （每题2分，共35题，共70分）**

1、《中华人民共和国个人信息保护法》是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定的法规，自（   ）起施行。

A、 2020年11月1日

B、 2021年11月1日

C、 2022年1月1日

D、 2021年1月1日

2、下列(  )方式不适合对学生进行信息道德与信息安全教育。

A、观看相关新闻

B、观看相关视频

C、信息技术课

D、一起玩游戏

3、有关数据库加密，下面说法不正确的是（   ）。

A、 索引字段不能加密

B、 关系运算的比较字段不能加密

C、 字符串字段不能加密

D、 表间的连接码字段不能加密

4、入侵检测的目的是（     ）。

A、 实现内外网隔离与访问控制

B、 提供实时的检测及采取相应的防护手段，阻止黑客的入侵

C、 记录用户使用计算机网络系统进行所有活动的过程

D、 预防、检测和消除病毒

5、\x32\x2E\x68\x74\x6D此加密是几进制加密？（    ）

A、 二进制

B、 八进制

C、 十进制

D、 十六进制

6、现代密码学中很多应用包含散列运算，而下面应用中不包含散列运算的是？（    ）

A、 消息机密性

B、 消息完整性

C、 消息认证码

D、 数字签名

7、目标计算机与网关通信失败，更会导致通信重定向的攻击形式是？（    ）

A、 病毒

B、 木马

C、 DOS

D、 ARP欺骗

8、设在RSA 的公钥密码体制中，公钥为（e,n）=（13，35），则私钥d=？（   ）

A、 11

B、 13

C、 15

D、 17

9、Shell变量命令，说法错误的是？（    ）

A、 变量名必须以字母或下划线开头，且只能由字母、数字和下划线组成

B、 变量名的长度不得超过100个字符

C、 变量名在有效的范围内必须是唯一

D、 在bash中，变量的默认类型都是字符串型

10、SQL的GRANT和REVOKE语句可以用来实现（   ）。

A、 自主存取控制

B、 强制存取控制

C、 数据库角色创建

D、 数据库审计

11、Str='heiheihei' print str[3:]将输出？（    ）

A、 hei

B、 heihei

C、 eih

D、 ihe

12、能修改系统引导扇区，在计算机系统启动时首先取得控制权的病毒属于（   ）。

A、 文件病毒

B、 引导型病毒

C、 混合型病毒

D、 恶意代码

13、下列哪个不是密码字典？（    ）

A、 弱口令字典

B、 社工字典

C、 彩虹表

D、 《康熙字典》

14、Skipjack是一个密钥长度为(     )位。

A、 56

B、 64

C、 80

D、 128

15、在RSA算法中，取P=3，q=11,e=3，则d等于多少？（   ）

A、 33

B、 20

C、 14

D、 7

16、已知字母A的ASCII码为十进制数65,且c2为字符型,则执行语句c2='A'+'6'-'3';后,c2中的值为？（   ）

A、 D

B、 68

C、 58

D、 24

17、Burp suite是用于攻击（    ）的集成平台。

A、 web应用程序

B、 客户机

C、 服务器

D、 浏览器

18、远程windows 口令破解的工具是？（    ）

A、 NtScan

B、 getpass

C、 Hydra

D、 Saminside

19、如果想在文件test.txt中追加内容，应该使用下列哪个选项？（    ）

A、 a=open('test.txt',"a")

B、 a=open('test.txt',"r")

C、 a=open('test.txt',"d")

D、 a=open('test.txt',"w")

20、在强制存取控制机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作（   ）。

A、 读取

B、 写入

C、 不可操作

D、 读取、写入

21、关于数据库应用系统的设计，下列说法正确的是（   ）。

A、 数据库应用系统设计需要考虑数据组织与存储、数据访问与处理、应用设计等几个方面

B、 数据库概念设计阶段，采用自上而下的E-R设计时，首先设计局部E-R图，然后合并各局部E-R图得到全局E-R图

C、 在数据库逻辑设计阶段，将关系模式转换为具体DBMS平台支持的关系表

D、 在数据库物理设计阶段，一般需要设计视图和关系模式的完整性约束

22、如果想在类中创建私有方法，下面哪个命名是正确的？（    ）

A、 \_add\_one

B、 add\_one

C、 \_\_add\_one

D、 add\_one\_\_

23、nmap的-SV是什么操作？（    ）

A、 TCP全连接扫描

B、 FIN扫描

C、 版本扫描

D、 全面扫描

24、扫描器之王NMAP中，全面扫描的命令是什么？（    ）

A、 -o

B、 -SV

C、 -sP

D、 -a

25、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（   ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

26、一个完整的密码体制，不包括以下（       ）要素。

A、 明文空间

B、 密文空间

C、 数字签名

D、 密钥空间

27、如果VPN网络需要运行动态路由协议并提供私网数据加密,通常采用什么技术手段实现（   ）。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

28、在现有的计算能力条件下，对于椭圆曲线密码算法(ECC)，被认为是安全的最小密钥长度 是？（    ）

A、 128位

B、 160位

C、 512位

D、 1024位

29、在(     )年，美国国家标准局NBS把IBM的Tuchman-Meyer方案确定数据加密标准，即  DES。

A、 1949

B、 1972

C、 1977

D、 2001

30、过滤所依据的信息来源不包括？（    ）

A、 IP包头

B、 TCP包头

C、 UDP包头

D、 IGMP包头

31、SEAL使用了四个（     ）位寄存器。

A、 24

B、 32

C、 48

D、 56

32、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（   ）。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

33、Linux中，使用哪一个命令删除非空文件夹？（    ）

A、 mv

B、 rm

C、 rmdir

D、 del

34、下面哪一项不是hash函数的等价提法？（    ）

A、 压缩信息函数

B、 哈希函数

C、 单向散列函数

D、 杂凑函数

35、差分分析是针对下面那种密码算法的分析方法？（    ）

A、 DES

B、 AES

C、 RC4

D、 MD5

一、 单选题 （每题2分，共35题，共70分）

1、外部数据包过滤路由器只能阻止一种类型的IP欺骗，即（        ） ，而不能阻止DNS欺骗？（        ）

A、 内部主机伪装成外部主机的IP

B、 内部主机伪装成内部主机的IP

C、 外部主机伪装成外部主机的IP

D、 外部主机伪装成内部主机的IP

2、Open函数中w 参数的作用是？（       ）

A、 读文件内容

B、 写文件内容

C、 删除文件内容

D、 复制文件内容

3、通过设置网络接口（网卡）的（        ） ，可以使其接受目的地址并不指向自己的网络数据包，从而达到网络嗅探攻击的目的？

A、 共享模式

B、 交换模式

C、 混杂模式

D、 随机模式

4、以下不属于入侵监测系统的是（        ） 。

A、 AAFID系统

B、 SNORT系统

C、 IETF系统

D、 NETEYE系统

5、通过TCP序号猜测，攻击者可以实施下列哪一种攻击？（        ）

A、 端口扫描攻击

B、 ARP欺骗攻击

C、 网络监听攻击

D、 TCP会话劫持攻击

6、下面不是数据库的基本安全机制的是（        ） 。

A、 用户认证

B、 用户授权

C、 审计功能

D、 电磁屏蔽

7、假设创建了名为f的实例，如何在f中调用类的add\_food函数？（       ）

A、 f(add\_food())

B、 f.[add\_food()]

C、 f.add\_food

D、 f.add\_food()

8、aspx 的网站配置文件一般存放在哪个文件里？（        ）

A、 conn.asp

B、 config.php

C、 web.config

D、 index.aspx

9、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（        ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

10、完成数据库应用系统的设计并进行实施后，数据库系统进入运行维护阶段。下列工作中不属于数据库运行维护工作的是（        ） 。

A、 恢复数据库数据以核查问题

B、 为了保证安全，定期修改数据库用户的密码

C、 更换数据库服务器以提高应用系统运行速度

D、 使用开发人员提供的SQL语句易始化数据库中的表

11、以下不属入侵检测中要收集的信息的是（        ） 。

A、 系统和网络日志文件

B、 目录和文件的内容

C、 程序执行中不期望的行为

D、 物理形式的入侵信息

12、POP3服务器使用的监听端口是？（        ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

13、目标计算机与网关通信失败，更会导致通信重定向的攻击形式是？（        ）

A、 病毒

B、 木马

C、 DOS

D、 ARP欺骗

14、\_\_\_\_\_\_\_\_的目的是发现目标系统中存在的安全隐患，分析所使用的安全机制是否能够保证系统的机密性、完整性和可用性。（        ）

A、 漏洞分析

B、 入侵检测

C、 安全评估

D、 端口扫描

15、以下哪一项描述不正确？（        ）

A、 ARP是地址解析协议

B、 TCP/IP传输层协议有TCP和UDP

C、 UDP协议提供的是可靠传输

D、 IP协议位于TCP/IP网际层

16、如果想在类中创建私有方法，下面哪个命名是正确的？（        ）

A、 \_add\_one

B、 add\_one

C、 \_\_add\_one

D、 add\_one\_\_

17、MD5的主循环有（       ） 轮。

A、 3

B、 4

C、 5

D、 8

18、根据网络安全应急处理流程，应急启动后，应该进行哪一步（        ） 。

A、 归类&定级

B、 应急处置

C、 信息通报

D、 后期处理

19、( )是一种架构在公用通信基础设施上的专用数据通信网络，利用 IPSec 等网络层安全协议和建立在 PKI 上的加密与签名技术来获得私有性。（        ）

A、 SET

B、 DDN

C、 VPN

D、 PKIX

20、假设系统中有n个用户，他们使用对称加密体制实现保密通信，那么系统中共需要管理（ n(n-1)/2）个密钥，每个用户需要保存（        ） 个密钥。

A、 n-1

B、 2n

C、 Cn2

D、 n！

21、什么是数据库安全的第一道保障（）。（        ）

A、 操作系统的安全

B、 数据库管理系统层次

C、 网络系统的安全

D、 数据库管理员

22、下列方法中不能用来进行DNS欺骗的是？（        ）

A、 缓存感染

B、 DNS信息劫持

C、 DNS重定向

D、 路由重定向

23、下列选项哪列不属于网络安全机制？（        ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

24、部署大中型 IPSEC VPN  时，从安全性和维护成本考虑，建议采取什么样的技术手段提供设备间的身份验证。（        ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

25、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（        ）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

26、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（        ） 。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

27、如果VPN网络需要运行动态路由协议并提供私网数据加密,通常采用什么技术手段实现（        ） 。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

28、过滤所依据的信息来源不包括？（        ）

A、 IP包头

B、 TCP包头

C、 UDP包头

D、 IGMP包头

29、bind9的日志默认保存在？（       ）

A、 /var/log/named.log

B、 /var/log/named/named.log

C、 /var/named/data/named.run

D、 /var/log/data/named.run

30、一个完整的密码体制，不包括以下（         ）要素。

A、 明文空间

B、 密文空间

C、 数字签名

D、 密钥空间

31、Linux系统中，添加用户的命令是？（        ）

A、 net user test /add

B、 user add test

C、 useradd test

D、 test useradd

32、以下关于正则表达式，说法错误的是？（        ）

A、 ‘root’表示匹配包含root字符串的内容

B、 ‘.’表示匹配任意字符

C、 [0-9]表示匹配数字

D、 ‘^root’表示取反

33、将用户user123修改为管理员权限命令是 （       ） 。

A、 net user localgroup administratorsuser123 /add

B、 net use localgroup administratorsuser123 /add

C、 net localgroup administrators user123/add

D、 net localgroup administrator user123/add

34、VIM模式切换的说法中，正确的是？（        ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

35、在常见的安全扫描工具中，以下（       ） 主要用来分析Web站点的漏洞，可以针对数千种常见的网页漏洞或安全风险进行检测。

A、 SuperScan

B、 Fluxay（流光）

C、 Wikto

D、 MBSA

**二、 多选题 （每题3分，共10题，共30分）**

1、SQL Server提供了DES、RC2、RC4和AES等加密算法，没有某种算法能适应所有要求，每种算法都有优劣势，但选择算法需要有如下共通之处（        ） 。

A、 强加密通常会比较弱的加密占用更多的CPU资源

B、 长密钥通常会比短密钥生成更强的加密

C、 如果加密大量数据，应使用对称密钥来加密数据，并使用非对称密钥来加密该对称密钥

D、 可以先对数据进行加密，然后再对其进行压缩

2、以下关于TCP和UDP协议的说法错误的是？（       ）

A、 没有区别，两者都是在网络上传输数据

B、 TCP是一个定向的可靠的传输层协议，而UDP是一个不可靠的传输层协议

C、 UDP是一个局域网协议，不能用于Interner传输，TCP则相反

D、 TCP协议占用带宽较UDP协议多

3、关于函数中变量的定义，哪些说法是正确的？（       ）

A、 即使函数外已经定义了这个变量，函数内部仍然可以定义

B、 如果一个函数已经定义了name变量，那么其他的函数就不能再定义

C、 函数可以直接引用函数外部定义过的变量

D、 函数内部只能定义一个变量

4、下面标准可用于评估数据库的安全级别的有（       ）

A、 TCSEC

B、 IFTSEC

C、 CC DBMS.PP

D、 GB17859-1999E.TD

5、安全的网络通信必须考虑以下哪些方面？（       ）

A、 加密算法

B、 用于加密算法的秘密信息

C、 秘密信息的分布和共享

D、 使用加密算法和秘密信息以获得安全服务所需的协议

6、RC4加密算法被广.泛应用，包括（        ）

A、 SSL/TLS

B、 WEP协议

C、 WPA协议

D、 数字签名

7、VIM的工作模式，包括哪些？（        ）

A、 命令模式

B、 输入模式

C、 高亮模式

D、 底行模式

8、在反杀伤链中，情报可以分为那几个层次？（       ）

A、 战斗

B、 战略

C、 战区

D、 战术

9、我国现行的信息安全法律体系框架分为（   ）三个层面。

A、信息安全相关的国家法律

B、信息安全相关的行政法规和部分规章

C、信息安全相关的地方法规/规章和行业规定

D、信息安全相关的个人职业素养

10、信息道德与信息安全问题一直存在的原因有（   ）。

A、信息系统防护水平不高

B、信息安全意识不强

C、信息安全法律法规不完善

D、网络行为道德规范尚未形成

**一、 单选题 （每题2分，共35题，共70分）**

1、下列不属于口令安全威胁的是？（        ）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

2、在学校或单位如果发现自己的计算机感染了病毒,应首先采取什么措施(  )。

A、断开网络

B、告知领导

C、杀毒

D、重启

答案：A

3、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（        ） 。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

4、下列哪个不属于密码破解的方式？（        ）

A、 密码学分析

B、 撞库

C、 暴力破解

D、 字典破解

5、下列不属于应用层安全协议的是哪一项？（        ）

A、 Secure shell

B、 超文本传输协议

C、 电子交易安全协议SET

D、 SSL协议

6、\x32\x2E\x68\x74\x6D此加密是几进制加密？（        ）

A、 二进制

B、 八进制

C、 十进制

D、 十六进制

7、下列关于SQL Server 2008中分离和附加数据库的说法，错误的是（        ）

A、 在分离数据库之前，必须先断开所有用户与该数据库的连接

B、 分离数据库只分离数据文件，不会分离日志文件

C、 附加数据库时文件存储位置可以与分离数据库时文件所处的存储位置不同

D、 进行分离数据库操作时不能停止SQL Server服务

8、C语言中的标识符只能由字母、数字和下划线三种字符组成,且第一个字符 ？（        ）

A、 必须为字母

B、 必须为下划线

C、 必须为字母或下划线

D、 可以是字母,数字和下划线中任一种字符

9、下面那个名称不可以作为自己定义的函数的合法名称？（        ）

A、 print

B、 len

C、 error

D、 Haha

10、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（        ）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

11、.IPSec包括报文验证头协议AH 协议号（）和封装安全载荷协议ESP协议号（        ） 。

A、 51 50

B、 50 51

C、 47 48

D、 48 47

12、SYN攻击属于DOS攻击的一种，它利用（）协议缺陷，通过发送大量的半连接请求，耗费CPU和内存资源？（        ）

A、 UDP

B、 ICMP

C、 TCP

D、 OSPF

13、POP3服务器使用的监听端口是？（        ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

14、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（        ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

15、下列工具中可以直接从内存中读取windows 密码的是？（        ）

A、 getpass

B、 QuarkssPwDump

C、 SAMINSIDE

D、 John

16、利用虚假IP地址进行ICMP报文传输的攻击方法称为？（        ）

A、 ICMP泛洪

B、 死亡之ping

C、 LAND攻击

D、 Smurf攻击

17、关于函数，下面哪个说法是错误的？（        ）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

18、在TCP/IP参考模型中，与OSI参考模型的网络层对应的是？（        ）

A、 主机-网络层

B、 传输层

C、 互联网层

D、 应用层

19、MD5的主循环有（       ） 轮。

A、 3

B、 4

C、 5

D、 8

20、Open函数中w 参数的作用是？（       ）

A、 读文件内容

B、 写文件内容

C、 删除文件内容

D、 复制文件内容

21、根据工信部明确的公共互联网网络安全突发事件应急预案文件，公共互联网网络突发事件等级最高可标示的颜色是什么？（        ）

A、 红色

B、 黄色

C、 蓝色

D、 橙色

22、下列选项哪列不属于网络安全机制？（        ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

23、以下选项中，不属于结构化程序设计方法的是哪个选项？（        ）

A、 可封装

B、 自顶向下

C、 逐步求精

D、 模块化

24、关于并行数据库，下列说法错误的是（        ） 。

A、 层次结构可以分为两层，顶层是无共享结构，底层是共享内存或共享磁盘结构

B、 无共享结构通过最小化共享资源来降低资源竞争，因此具有很高的可扩展性，适合于OLTP应用

C、 并行数据库系统经常通过负载均衡的方法来提高数据库系统的业务吞吐率

D、 并行数据库系统的主要目的是实现场地自治和数据全局透明共享

25、下面不是 Oracle 数据库支持的备份形式的是（        ） 。

A、 冷备份

B、 温备份

C、 热备份

D、 逻辑备份

26、Linux中，通过chmod修改权限设置，正确的是？（        ）

A、 chmod test.jpg +x

B、 chmod u+8 test.jpg

C、 chmod 777 test.jpg

D、 chmod 888 test.jpg

27、windows自带FTP服务器的日志文件后缀为？（        ）

A、 evt或.evtx

B、 log

C、 w3c

D、 txt

28、部署IPSEC VPN时，配置什么样的安全算法可以提供更可靠的数据加密（        ）。

A、 DES

B、 3DES

C、 SHA

D、 128位的MD5

29、如果明文为abc，经恺撒密码-加密后，密文bcd，则密钥为？（       ）

A、 1

B、 2

C、 3

D、 4

30、部署IPSEC VPN 网络时我们需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，其中每条加密ACL将消耗多少IPSEC SA资源（        ） 。

A、 1个

B、 2个

C、 3个

D、 4个

31、部署IPSEC VPN 网络时我们需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，其中每条加密ACL将消耗多少IPSEC SA资源（        ） 。

A、 1个

B、 2个

C、 3个

D、 4个

32、DES的秘钥长度是多少Bit?（       ）

A、 6

B、 56

C、 128

D、 32

33、VIM命令中，用于删除光标所在行的命令是？（        ）

A、 dd

B、 dw

C、 de

D、 db

34、Linux软件管理rpm命令，说法不正确的是？（        ）

A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示2%

C、 -q PACKAGE\_NAME：查询指定的包是否已经安装

D、 -e 升级安装包

35、RIP路由协议有RIP v1 和RIP v2两个版本，下面关于这两个版本的说法错误的是（        ） 。

A、 RIP v1和RIP v2都具有水平分割功能

B、 RIP v1 是有类路由协议，RIP v2是无类路由协议

C、 RIP v1 和 RIP v2 都是以跳数作为度量值

D、 RIP v1 规定跳数的最大值为15，16跳视为不可达；而RIP v2无此限制

**二、 多选题 （每题3分，共10题，共30分）**

1、Bash变量类型，包括以下哪些？（        ）

A、 用户自定义变量

B、 环境变量

C、 预定义变量

D、 高级变量

2、关于函数中变量的定义，哪些说法是正确的？（        ）

A、 即使函数外已经定义了这个变量，函数内部仍然可以定义

B、 如果一个函数已经定义了name变量，那么其他的函数就不能再定义

C、 函数可以直接引用函数外部定义过的变量

D、 函数内部只能定义一个变量

3、移动用户常用的VPN接入方式是（       ） 。

A、 L2TP

B、 IPSECHIKE野蛮模式

C、 GRE+IPSEC

D、 L2TP+IPSEC

4、RC4加密算法被广泛应用，包括（        ） 。

A、 SSL/TLS

B、 WEP协议

C、 WPA协议

D、 数字签名

5、关于类的说法下面哪些是正确的？（        ）

A、 我们把类中定义的函数称为方法

B、 可以不通过类直接调用类中的方法

C、 可以在方法前加上\_\_来声明这是一个私有方法

D、 类中必须定义\_\_init\_\_方法

6、安全的网络通信必须考虑以下哪些方面？（        ）

A、 加密算法

B、 用于加密算法的秘密信息

C、 秘密信息的分布和共享

D、 使用加密算法和秘密信息以获得安全服务所需的协议

7、以下Linux命令中，跟用户与用户组管理相关的命令有哪些？（        ）

A、 usermod

B、 mkdir

C、 groupdel

D、 useradd

8、VPN 组网中常用的站点到站点接入方式是（        ） 。

A、 L2TP

B、 IPSEC

C、 GRE+IPSEC

D、 .L2TP+IPSEC

9、信息道德包括（   ）。

A、网络信息道德

B、学术性信息道德

C、思想品德

D、社会公德

10、下列说法正确的是（  ）。

A、离岗离职人员也要遵守信息安全管理制度不能泄露岗位机密信息

B、滥发广告、随心所欲散发虚假信息和新闻、利用互联网传播淫秽物品牟利属于信息道德与信息安全失范行为

C、网络的开放性致使学生们比以往传统社会面临更多的道德冲突

D、《中华人民共和国计算机信息系统安全保护条例》中关于信息安全的定义是“保障计算机及其相关的和配套的设备、设施( 网络)的安全运行环境的安全，保障信息安全保障计算机功能的正常发挥以维护计算机系统的安全。

**一、 单选题 （每题2分，共35题，共70分）**

1、(   )是指在信息的采集、加工、存储、传播和利用的各个环节中，用来规范期间产生的各种社会关系的道德意识、道德规范和道德行为的总和。

A、信息规范

B、信息规则

C、信息道德

D、信息行为

2、以下能够大幅度提高信息安全的做法是( )。

A、不再网络条件下使用计算机

B、定期使用安全软件

C、尽量少用计算机

D、多用纸质工具工作

3、以下不属于入侵监测系统的是（       ） 。

A、 AAFID系统

B、 SNORT系统

C、 IETF系统

D、 NETEYE系统

4、当数据库系统出现故障时，可以通过数据库日志文件进行恢复。下列关于数据库日志文件的说法，错误的是（        ） 。

A、 数据库出现事务故障和系统故障时需使用日志文件进行恢复

B、 使用动态转储机制时，必须使用日志文件才能将数据库恢复到一致状态

C、 在OLTP系统中，数据文件的空间使用量比日志文件大得多，使用日志备份可以降低数据库的备份空间

D、 日志文件的格式主要有以记录为单位的日志文件和以数据块为单位的日志文件两种

5、下面不是 SQL Server 支持的身份认证方式的是（        ）。

A、 Windows NT 集成认证

B、 SQL Server 认证

C、 SQL Server混合认证

D、 生物认证

6、下面那个名称不可以作为自己定义的函数的合法名称？（        ）

A、 print

B、 len

C、 error

D、 Haha

7、SHA-1接受任何长度的输入消息，并产生长度为（        ） 比特的hash值。

A、 64

B、 160

C、 128

D、 512

8、下列选项中不是 Hydra工具中的-e参数的值是？（        ）

A、 o

B、 n

C、 s

D、 r

9、在Google Hacking 中，下面哪一个是搜索指定文件类型的语句？（        ）

A、 intext

B、 Intitle

C、 site

D、 filetype

10、以下选项中，对文件的描述错误的是哪个选项？（        ）

A、 文件中可以包含任何数据内容

B、 文本文件和二进制文件都是文件

C、 文本文件不能用二进制文件方式读入

D、 文件是一个存储在辅助存储器上的数据序列

11、以下关于TCP和UDP协议的描述中，正确的是？（        ）

A、 TCP是端到端的协议，UDP是点到点的协议

B、 TCP是点到点的协议，UDP是端到端的协议

C、 TCP和UDP都是端到端的协议

D、 TCP和UDP都是点到点的协议

12、攻击者在使用nmap对目标网络进行扫描时发现，某个主机开放了25和110端口，此主机最有可能是？（        ）

A、 文件服务器

B、 邮件服务器

C、 WEB服务器

D、 DNS服务器

13、在数据库系统中,死锁属于（        ） 。

A、 系统故障

B、 事务故障

C、 介质保障

D、 程序故障

14、在TCP/IP参考模型中，与OSI参考模型的网络层对应的是？（        ）

A、 主机-网络层

B、 传输层

C、 互联网层

D、 应用层

15、下面程序的运行结果是: ＃include&amp;lt;stdio.h&amp;gt; { int k=0; char c='A'; do {switch(c++){case 'A':k++;break; case 'B':k--; case 'C':k+=2;break; case 'D':k=k%2;continue。（        ）

A、 k=0

B、 k=2

C、 k=3

D、 k=4

16、如果想在类中创建私有方法，下面哪个命名是正确的？（        ）

A、 \_add\_one

B、 add\_one

C、 \_\_add\_one

D、 add\_one\_\_

17、如果想在文件test.txt中追加内容，应该使用下列哪个选项？（        ）

A、 a=open('test.txt',"a")

B、 a=open('test.txt',"r")

C、 a=open('test.txt',"d")

D、 a=open('test.txt',"w")

18、当下各大厂商均有相关的应急响应中心部门，奖励均根据漏洞等级来进行划分。根据相应的安全标准，下列哪项不符合该要求？（        ）

A、 警告

B、 中危

C、 低危

D、 超危

19、SYN攻击属于DOS攻击的一种，它利用（）协议缺陷，通过发送大量的半连接请求，耗费CPU和内存资源？（        ）

A、 UDP

B、 ICMP

C、 TCP

D、 OSPF

20、外部数据包过滤路由器只能阻止一种类型的IP欺骗，即（），而不能阻止DNS欺骗？（        ）

A、 内部主机伪装成外部主机的IP

B、 内部主机伪装成内部主机的IP

C、 外部主机伪装成外部主机的IP

D、 外部主机伪装成内部主机的IP

21、当发现原有的IDS不能检测到新的攻击类型时，你应该采取哪种措施？（        ）

A、 购买或更新特征库

B、 配置防火墙

C、 关闭IDS直到得到新的IDS应用程序

D、 定义一个新的规则来检测攻击

22、下列工具中可以直接从内存中读取windows 密码的是？（        ）

A、 getpass

B、 QuarkssPwDump

C、 SAMINSIDE

D、 John

23、下面不是计算机网络面临的主要威胁的是?（        ）

A、 恶意程序威胁

B、 计算机软件面临威胁

C、 计算机网络实体面临威胁

D、 计算机网络系统面临威胁

24、数据库管理员应该定期对数据库进行重组，以保证数据库性能。下列有关数据库重组工作的说法，错误的是（        ） 。

A、 重组工作中可能会对数据库数据的磁盘分区方法和存储空间进行调整

B、 重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式

C、 重组工作一般在数据库运行一段时间后进行，不应频繁进行数据库重组

D、 重组工作中应尤其注意频繁修改数据的表，因为这些表很容易出现存储碎片，导致效率下降

25、os.getcwd()函数的作用是？（        ）

A、 返回当前目录下的文件

B、 返回当前目录的路径

C、 返回上一层目录的路径

D、 返回当前目录下的文件夹列表

26、哪个关键词可以在python中进行处理错误操作？（        ）

A、 try

B、 catch

C、 finderror

D、 error

27、下面哪一项不是hash函数的主要应用？（        ）

A、 文件校验

B、 数字签名

C、 数据加密

D、 鉴权协议

28、Geffe发生器使用了（        ） 个LFSR。

A、 1

B、 2

C、 3

D、 4

29、ELK日志解决方案中，Elasticsearch的作用是？（        ）

A、 收集日志并分析

B、 保存日志并搜索日志

C、 收集日志并保存

D、 保存日志并展示日志

30、CVE-2016-8704（        ）

A、 CVE-2016-8704

B、 CVE-2016-8705

C、 CVE-2018-8174

D、 CVE-2016-8706

31、下面哪种密码算法抵抗频率分析攻击能力最强，而对已知明文攻击最弱？（        ）

A、 仿射密码

B、 维吉利亚

C、 轮转密码

D、 希尔密码

32、re.match函数中参数Flag的作用是？（        ）

A、 声明正则表达式的内容

B、 声明正则表达式的名称

C、 控制正则表达式的匹配方式

D、 声明要匹配的字符串

33、部署IPSEC VPN 网络时我们需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，其中每条加密ACL将消耗多少IPSECSA资源（)。（        ）

A、 1个

B、 2个

C、 3个

D、 4个

34、VIM退出命令中，能强制保存并退出的是？（        ）

A、 x

B、 wq

C、 q

D、 wq!

35、将用户user123修改为管理员权限命令是 （        ）。

A、 net user localgroup administrators user123 /add

B、 net use localgroup administrators user123 /add

C、 net localgroup administrators user123 /add

D、 net localgroup administrator user123 /add

**二、 多选题 （每题3分，共10题，共30分）**

1、安全业务指安全防护措施，包括（       ） 。

A、 保密业务

B、 认证业务

C、 完整性业务

D、 不可否认业务

2、下列哪些选项属于木马程序？（       ）

A、 X—Scan

B、 流光

C、 BO

D、 冰河

3、关于函数，下面哪些说法是错误的？（        ）

A、 函数必须返回一个结果

B、 函数不能调用自身

C、 函数命名只能以字母或数字开头

D、 在同一个文件中，不应定义重名的函数

4、下面哪些函数的执行结果将返回一个元组？（        ）

A、 os.stat

B、 os.path.split

C、 os.listdir

D、 os.getcwd

5、Python中哪些符号可以包含字符串数据？（        ）

A、 单引号

B、 双引号

C、 两个双引号

D、 三个双引号

6、数据库的完整性分为以下种类（       ） 。

A、 实体完整性

B、 域完整性

C、 参照完整性

D、 用户定义完整性

7、VIM的工作模式，包括哪些？（        ）

A、 命令模式

B、 输入模式

C、 高亮模式

D、 底行模式

8、上传文件夹权限管理方法包括 ？（       ）

A、 取消执行权限

B、 限制上传文件大小

C、 设置用户umask值

D、 在上传目录关闭php解析引擎

9、IPSec的安全联盟与IKE的安全联盟的区别是（        ）。

A、 IPSec的安全联盟是单向的

B、 IPSec的安全联盟是双向的

C、 IKE的安全联盟是单向的

D、 IKE的安全联盟是双向的

10、Bash环境变量中，常见的环境变量有？（        ）

A、 HOSTNAME

B、 PASS

C、 SHELL

D、 USER

**二、 多选题 （每题3分，共10题，共30分）**

1、分组密码的常见的四中运行模式中，如果其中一个密文分组有一个比特的错误，不会将该错误进行传播的模式是？（    ）

A、 ECB

B、 CBC

C、 CFB

D、 OFB

2、Apache服务器外围加固措施包括？（    ）

A、 部署WAF

B、 部署IPS

C、 部署IDS

D、 部署蜜罐系统

3、Bash编程中，常见的循环有？（    ）

A、 foreach

B、 while

C、 for

D、 until

4、netwox工具拥有以下哪些功能？（    ）

A、 嗅探

B、 SQL注入

C、 欺骗

D、 地址转换

5、如何在不改变原始网络拓扑和业务的前提下，消除或者避免ICMP重定向攻击？（    ）

A、 关掉ip redirects

B、 代理ARP

C、 使用访问控制表（ACL）

D、 不同掩码长度子网划分

6、移动用户常用的VPN接入方式是（   )。

A、 L2TP

B、 IPSECHIKE野蛮模式

C、 GRE+IPSEC

D、 L2TP+IPSEC

7、Linux的ls命令，下列说法正确的是？（    ）

A、 -d：选项是查看目录属性

B、 -l：选项是显示详细信息

C、 -h：选项是人性化显示文件大小

D、 -i：选项是显示文件索引号

8、以下Linux命令中，跟网络管理相关的命令有哪些？（    ）

A、 ifconfig

B、 df

C、 lsmod

D、 netstat

9、防火墙一般需要检测哪些扫描行为？（    ）

A、 Port-scan

B、 Icmp-scan

C、 Udp-scan

D、 Tcp-synflood

10、在RHEL5系统中，以下（   ）操作将在分区/dev/sdb7上创建EXT3文件系统。

A、 mkfs –t ext3 /dev/sdb7

B、 mkfs.ext3 /dev/sdb7

C、 fdisk –t ext3 /dev/sdb7

D、 format /dev/sdb7 –t ext3

一、 单选题 （每题2分，共35题，共70分）

1、脏数据是指（  ）。

A、 不健康的数据

B、 缺失的数据

C、 多余的数据

D、 被撤销的事务曾写入库中的数据

2、滥发各种广告和虚假信息传播计算机病毒等信息道德与信息安全失范行为是从以下（  ）角度出发来定义。

A、信息获取角度

B、信息处理角度

C、信息传播角度

D、以上都不是

3、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（        ） 。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

4、在数据库系统中,死锁属于（       ） 。

A、 系统故障

B、 事务故障

C、 介质保障

D、 程序故障

5、下列选项哪列不属于网络安全机制？（        ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

6、SQL中的ROLLBACK语句的主要作用是（        ） 。

A、 终止程序

B、 中断程序

C、 事务提交

D、 事务回退

7、在强制存取控制机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作（        ） 。

A、 读取

B、 写入

C、 不可操作

D、 读取、写入

8、端口扫描的原理是向目标主机的\_\_\_\_\_\_\_\_端口发送探测数据包，并记录目标主机的响应。（        ）

A、 FTP

B、 UDP

C、 TCP/IP

D、 WWW

9、计算复杂性是密码分析技术中分析计算量和研究破译密码的固有难度的基础，算法的运行时间为难解的是？（        ）

A、 O(1)

B、 O(n)

C、 O(n2)

D、 O(2^n)

10、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（        ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

11、如果想在文件test.txt中追加内容，应该使用下列哪个选项？（        ）

A、 a=open('test.txt',"a")

B、 a=open('test.txt',"r")

C、 a=open('test.txt',"d")

D、 a=open('test.txt',"w")

12、关于IP提供的服务，下列哪种说法是正确的？（        ）

A、 IP提供不可靠的数据投递服务，因此数据包投递不能受到保障

B、 IP提供不可靠的数据投递服务，因此它可以随意丢弃报文

C、 IP提供可靠的数据投递服务，因此数据报投递可以受到保障

D、 IP提供可靠的数据投递服务，因此它不能随意丢弃报文

13、下列哪一项攻击防火墙不能发现而入侵检测系统可以发现？（        ）

A、 拒绝服务攻击

B、 端口扫描

C、 蠕虫病毒攻击

D、 局域网内非法登陆

14、m-序列本身是适宜的伪随机序列产生器，但只有在（        ） 下，破译者才不能破解这个伪随机序列。

A、 唯密文攻击

B、 已知明文攻击

C、 选择明文攻击

D、 选择密文攻击

15、MD5 的压缩函数中， 512bit 的消息被分为 16 块输入到步函数，每一块输入（        ）次。

A、 3

B、 4

C、 5

D、 8

16、在RSA算法中，取P=3，q=11,e=3，则d等于多少？（        ）

A、 33

B、 20

C、 14

D、 7

17、包过滤型防火墙工作在?（       ）

A、 会话层

B、 应用层

C、 网络层

D、 数据链路层

18、关于TCP协议的描述中，错误的是？（        ）

A、 提供全双工服务

B、 采用重发机制实现流量控制

C、 采用三次握手确保连接建立

D、 采用自适应方法确定重发前等待时间

19、入侵检测的目的是（          ）

A、 实现内外网隔离与访问控制

B、 提供实时的检测及采取相应的防护手段，阻止黑客的入侵

C、 记录用户使用计算机网络系统进行所有活动的过程

D、 预防、检测和消除病毒

20、print 'aaa' &gt; 'Aaa'将返回？（        ）

A、 TRUE

B、 FALSE

C、 SyntaxError: invalid syntax

D、 1

21、已知各变量的类型说明如下: int k,AB; unsigned long w= 5; double x=1.42; 则以下不符合C语言语法的表达式是？（        ）

A、 x%(一3)

B、 w+=-2

C、 k=(a=2,b=3,a+b)

D、 a+= a一=(b=4)\*(a=3)

22、Str='heiheihei' print str[3:]将输出？（        ）

A、 hei

B、 heihei

C、 eih

D、 ihe

23、关于并行数据库，下列说法错误的是（        ） 。

A、 层次结构可以分为两层，顶层是无共享结构，底层是共享内存或共享磁盘结构

B、 无共享结构通过最小化共享资源来降低资源竞争，因此具有很高的可扩展性，适合于OLTP应用

C、 并行数据库系统经常通过负载均衡的方法来提高数据库系统的业务吞吐率

D、 并行数据库系统的主要目的是实现场地自治和数据全局透明共享

24、\x32\x2E\x68\x74\x6D此加密是几进制加密？（        ）

A、 二进制

B、 八进制

C、 十进制

D、 十六进制

25、假设系统中有n个用户，他们使用对称加密体制实现保密通信，那么系统中共需要管理（ n(n-1)/2）个密钥，每个用户需要保存（        ） 个密钥。

A、 n-1

B、 2n

C、 Cn2

D、 n！

26、Python中哪个占位符表示字符串数据？（        ）

A、 %s

B、 %S

C、 %d

D、 %b

27、Linux系统中，格式化分区通常使用那个命令？（        ）

A、 du

B、 fdisk

C、 netstat

D、 lsmod

28、禁止目录浏览，配置方法是？（        ）

A、 去掉根目录的Indexes属性

B、 改变服务端口号

C、 修改目录名称

D、 将目录设置为只读属性

29、能显示TCP和UDP连接信息的命令是？（        ）

A、 netstat -s

B、 netstat -e

C、 netstat -r

D、 netstat -a

30、以下关于VI的说法正确的是？（        ）

A、 VI和VIM没有任何关系

B、 使用VI打开一个文件后可以立即编辑文件内容

C、 VI编辑器一次只能编辑一个文件

D、 以上说法全是错误的

31、RIP路由协议有RIP v1 和RIPv2两个版本，下面关于这两个版本的说法错误的是（         ） 。

A、 RIP v1和RIP v2都具有水平分割功能

B、 RIP v1 是有类路由协议，RIP v2是无类路由协议

C、 RIP v1 和 RIP v2 都是以跳数作为度量值

D、 RIP v1 规定跳数的最大值为15，16跳视为不可达；而RIP v2无此限制

32、适合文件加密，而且有少量错误时不会造成同步失败，是软件加密的最好选择,这种分组密码的操作模式是指？（        ）

A、 电子密码本模式

B、 密码分组链接模式

C、 密码反馈模式

D、 输出反馈模式

33、生日攻击是针对下面哪种密码算法的分析方法？（         ）

A、 DES

B、 AES

C、 RC4

D、 MD5

34、VIM命令中，用于删除光标所在行的命令是？（        ）

A、 dd

B、 dw

C、 de

D、 db

35、按目前的计算能力，RC4算法的密钥长度至少应为（        ） 才能保证安全强度。

A、 任意位

B、 64位

C、 128位

D、 256位

 二、 多选题 （每题3分，共10题，共30分）

1、以下属于多表代换的密码是？（        ）

A、 Playfair

B、 Polybius

C、 Vigenere

D、 Hill密码

2、安全业务指安全防护措施，包括（        ） 。

A、 保密业务

B、 认证业务

C、 完整性业务

D、 不可否认业务

3、在SQL Server中数据库用户的权限分为以下几个级别（        ） 。

A、 服务器级别

B、 数据库级别

C、 数据库对象级别

D、 数据库对象字段权限

4、SQL Server 中的预定义服务器角色有（        ） 。

A、 Sysadmin

B、 Serveradmm

C、 Setupadmin

D、 Securityadmin

5、netwox工具拥有以下哪些功能？（        ）

A、 嗅探

B、 SQL注入

C、 欺骗

D、 地址转换

6、关于yum命令，说法正确的有哪些？（        ）

A、 -y 自动应答yes

B、 -e 静默执行

C、 -t 延迟安装

D、 -R[分钟] 设置等待时间

7、关于类的说法，下面哪些是错误的？（        ）

A、 私有方法和私有变量只能在类的内部使用

B、 一个类只能创建一个实例

C、 两个不同的类中的方法不能重名

D、 创建类的实例时，传入的变量类型要和类中定义的一致

8、以下Linux命令中，跟网络管理相关的命令有哪些？（        ）

A、 ifconfig

B、 df

C、 lsmod

D、 netstat

9、VPN 组网中常用的站点到站点接入方式是()。（        ）

A、 L2TP

B、 IPSEC

C、 GRE+IPSEC

D、 .L2TP+IPSEC

10、APTECH公司的管理员使用DPM 2007对Exchange Server 2007中的邮件进行备份还原，当通过ExchangeServer 2007中的恢复存储组进行还原时，下列选项中说法正确的是（        ） 。

A、 可以对单个用户的邮箱数据进行还原

B、 只能够对整个存储组的所有用户邮箱数据进行还原

C、 其他存储组的用户邮箱不可用

D、 需要停止Microsoft Exchange Information Store服务

一、 单选题 （每题2分，共35题，共70分）

[1](true)、《中华人民共和国个人信息保护法》是为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定的法规，自（   ）起施行。

A、 2020年11月1日

B、 2021年11月1日

C、 2022年1月1日

D、 2021年1月1日

2、能够保证信息系统的操作者或者信息的处理者不能否认其行为或处理结果，这可以防止参与某次操作或通信的乙方事后否认该事件曾发生过，这属于信息安全的(  )。

A、可用性

B、完整性

C、非否认性

D、机密性

3、下面那个名称不可以作为自己定义的函数的合法名称？（       ）

A、 print

B、 len

C、 error

D、 Haha

4、print 'aaa' &gt;'Aaa'将返回？（       ）

A、 TRUE

B、 FALSE

C、 SyntaxError: invalid syntax

D、 1

5、下列在2017 年6月1日开始施行的法律是？（       ）

A、 《网络安全法》

B、 《刑法修正案》

C、 《计算机信息系统安全保护条例》

D、 《互联网上网服务营业场所管理条例》

6、针对Windows系统主机，攻击者可以利用文件共享机制上的Netbios“空会话”连接漏洞，获取众多对其攻击有利的敏感信息，获取的信息中不包含下列哪一项信息？（       ）

A、 系统的用户和组信息

B、 系统的共享信息

C、 系统的版本信息

D、 系统的应用服务和软件信息

7、POP3服务器使用的监听端口是？（       ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

8、利用虚假IP地址进行ICMP报文传输的攻击方法称为？（       ）

A、 ICMP泛洪

B、 死亡之ping

C、 LAND攻击

D、 Smurf攻击

9、下列不属于口令安全威胁的是？（       ）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

10、下列工具中可以直接从内存中读取windows 密码的是？（       ）

A、 getpass

B、 QuarkssPwDump

C、 SAMINSIDE

D、 John

11、什么是数据库安全的第一道保障（）。（       ）

A、 操作系统的安全

B、 数据库管理系统层次

C、 网络系统的安全

D、 数据库管理员

12、aspx 的网站配置文件一般存放在哪个文件里？（       ）

A、 conn.asp

B、 config.php

C、 web.config

D、 index.aspx

13、SQL Server 2008支持多种数据库还原级别。下列有关其数据库恢复的说法，错误的是（       ） 。

A、 在进行数据库整体还原和恢复过程中，此数据库处于脱机状态

B、 SQL Server支持对数据库的一个数据文件进行还原，在还原过程中此文件处于脱机状态，数据库中的其他文件不受影响

C、 在还原数据库之前，如果数据库的日志没有损坏，为了减少数据丢失可以进行一次尾部日志备份

D、 在进行数据库还原的过程中可以将数据库移动到其他位置

14、下面（）不包含在 MySQL 数据库系统中。（       ）

A、 数据库管理系统，即DBMS

B、 密钥管理系统

C、 关系型数据库管理系统，即 RDBMS

D、 开放源码数据库

15、外部数据包过滤路由器只能阻止一种类型的IP欺骗，即（），而不能阻止DNS欺骗？（       ）

A、 内部主机伪装成外部主机的IP

B、 内部主机伪装成内部主机的IP

C、 外部主机伪装成外部主机的IP

D、 外部主机伪装成内部主机的IP

16、下列哪个不是密码字典？（       ）

A、 弱口令字典

B、 社工字典

C、 彩虹表

D、 《康熙字典》

17、完成数据库应用系统的设计并进行实施后，数据库系统进入运行维护阶段。下列工作中不属于数据库运行维护工作的是（       ） 。

A、 恢复数据库数据以核查问题

B、 为了保证安全，定期修改数据库用户的密码

C、 更换数据库服务器以提高应用系统运行速度

D、 使用开发人员提供的SQL语句易始化数据库中的表

18、黑客利用IP地址进行攻击的方法有？（       ）

A、 IP欺骗

B、 解密

C、 窃取口令

D、 发送病毒

19、一个C程序的执行是从哪里开始的？（       ）

A、 本程序的main函数开始，到main函数结束

B、 本程序文件的第一个函数开始，到本程序main函数结束

C、 本程序的main函数开始，到本程序文件的最后一个函数结束

D、 本程序文件的第一个函数开始，到本程序文件的最后一个函数结束

20、Str='heiheihei'print str[3:]将输出？（       ）

A、 hei

B、 heihei

C、 eih

D、 ihe

21、一个基于网络的IDS应用程序利用什么来检测攻击？（       ）

A、 正确配置的DNS

B、 特征库

C、 攻击描述

D、 信息包嗅探器

22、脏数据是指（）。（       ）

A、 不健康的数据

B、 缺失的数据

C、 多余的数据

D、 被撤销的事务曾写入库中的数据

23、数据库管理员应该定期对数据库进行重组，以保证数据库性能。下列有关数据库重组工作的说法，错误的是（       ）

A、 重组工作中可能会对数据库数据的磁盘分区方法和存储空间进行调整

B、 重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式

C、 重组工作一般在数据库运行一段时间后进行，不应频繁进行数据库重组

D、 重组工作中应尤其注意频繁修改数据的表，因为这些表很容易出现存储碎片，导致效率下降

24、下面不是 SQL Server 支持的身份认证方式的是（        ）。

A、 Windows NT 集成认证

B、 SQL Server 认证

C、 SQL Server混合认证

D、 生物认证

25、ELK中的各种beats主要作用是？（       ）

A、 作为前端过滤日志

B、 作为前端定义日志的格式

C、 作为前端收集不同类型日志

D、 作为前端将日志发送给kibana

26、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（       ） 。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

27、Shell编程条件判断中，整数比较说法错误的是？（       ）

A、 整数1 -eq 整数2，判断整数1是否和整数2相等

B、 整数1 -ge 整数2，判断整数1是否大于等于整数2

C、 整数1 -lt 整数2，判断整数1是否小于等于整数2

D、 整数1 -gt 整数2，判断整数1是否大于整数2

28、DES的秘钥长度是多少Bit?（       ）

A、 6

B、 56

C、 128

D、 32

29、Shell编程条件判断中，文件权限判断说法错误的是？（       ）

A、 -r 判断该文件是否存在，并且该文件是否拥有读写权限

B、 -w 判断该文件是否存在，并且该文件是否拥有写权限

C、 -x 判断该文件是否存在，并且该文件是否拥有执行权限

D、 -u 判断该文件是否存在，并且该文件是否拥有SUID权限

30、Linux命令的基本格式中，正确的是？（       ）

A、 命令[参数][选项]

B、 命令 [选项] [参数]

C、 [选项]命令[参数]

D、 [参数]命令[选项]

31、如果VPN网络需要运行动态路由协议并提供私网数据加密,通常采用什么技术手段实现（       ） 。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

32、VIM模式切换的说法中，正确的是？（       ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

33、以下关于VPN说法正确的是（ )（       ）

A、 VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

B、 VPN 指的是用户通过公用网络建立的临时的、安全的连接

C、 VPN不能做到信息验证和身份认证

D、 VPN只能提供身份认证、不能提供加密数据的功能

34、目前，使用最广泛的序列密码是？（       ）

A、 RC4

B、 A5

C、 SEAL

D、 PKZIP

35、2000年10月2日，NIST 正式宣布将（        ）候选算法作为高级加密标准（AES），该算法是由两位比利时密码学着提出的。

A、 MARS

B、 Rijndael

C、 Twofish

D、 Bluefish

二、 多选题 （每题3分，共10题，共30分）

1、netwox工具拥有以下哪些功能？（       ）

A、 嗅探

B、 SQL注入

C、 欺骗

D、 地址转换

2、Python中哪些符号可以包含字符串数据？（       ）

A、 单引号

B、 双引号

C、 两个双引号

D、 三个双引号

3、Apache服务器外围加固措施包括？（       ）

A、 部署WAF

B、 部署IPS

C、 部署IDS

D、 部署蜜罐系统

4、安全业务指安全防护措施，包括（       ） 。

A、 保密业务

B、 认证业务

C、 完整性业务

D、 不可否认业务

5、如果想写一个循环，遍历从1到100的所有数字，下面哪些语句是正确的？（       ）

A、 for i in range(1,101):print i

B、 i=0 while i<100: i=i+1 print i

C、 for i in range(0,101): print i

D、 for i in range(1,100): print i

6、对-rw-rw-r―权限描述，正确的说法是？（       ）

A、 所有者具有读写权限

B、 所属组具有读写权限

C、 其他人具有读写权限

D、 所有用户和组都没有执行权限

7、操作系统安全主要包括（ ）等方面 。（       ）

A、 账户密码安全和文件共享安全

B、 文件权限管理和用户权限管理

C、 日志审计和远程访问权限管理

D、 文件夹选项和安全选项

8、防火墙的主要技术有哪些？（       ）

A、 简单包过滤技术

B、 状态检测包过滤技术

C、 应用代理技术

D、 复合技术

9、VIM的工作模式，包括哪些？（       ）

A、 命令模式

B、 输入模式

C、 高亮模式

D、 底行模式

10、关于安全联盟SA，说法正确的是（       ） 。

A、 IKESA是单向的

B、 IPSEC SA 是双向的

C、 IKESA 是双向的

D、 IPSEC SA是单向的

**一、      
理论技能与职业素养（100分**

一、 单选题 （每题2分，共35题，共70分）

1、外部数据包过滤路由器只能阻止一种类型的IP欺骗，即（      ） ，而不能阻止DNS欺[1](true)、《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过，自（  ）起施行。

A、 2019年6月1日

B、 2018年6月1日

C、 2017年6月1日

D、 2016年6月1日

2、传播计算机病毒属于以下（   ）问题行为。

A、信息道德与信息安全失范行为

B、侵害他人财产

C、危害国家安全

D、传播有害文件

3、一个基于网络的IDS应用程序利用什么来检测攻击？（      ）

A、 正确配置的DNS

B、 特征库

C、 攻击描述

D、 信息包嗅探器

4、你检测到一次针对你的网络的攻击，你的服务器日志显示了攻击的源IP地址，但是你需要确定这个地址来自哪个域，你应该？（      ）

A、 Ping根服务器

B、 进行反向DNS查找

C、 检查你的DNS服务器的A记录

D、 请你的互联网服务供应商为你寻找需要的信息

5、扫描器之王NMAP中，全面扫描的命令是什么？（      ）

A、 -o

B、 -SV

C、 -sP

D、 -a

6、根据网络安全应急处理流程，应急启动后，应该进行哪一步（      ） 。

A、 归类&定级

B、 应急处置

C、 信息通报

D、 后期处理

7、能修改系统引导扇区，在计算机系统启动时首先取得控制权的病毒属于（      ） 。

A、 文件病毒

B、 引导型病毒

C、 混合型病毒

D、 恶意代码

8、你有一个共享文件夹，你将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有什么样的权限？（      ）

A、 读取

B、 写入

C、 修改

D、 完全控制

9、通过设置网络接口（网卡）的（），可以使其接受目的地址并不指向自己的网络数据包，从而达到网络嗅探攻击的目的？（      ）

A、 共享模式

B、 交换模式

C、 混杂模式

D、 随机模式

10、下面那个名称不可以作为自己定义的函数的合法名称？（      ）

A、 print

B、 len

C、 error

D、 Haha

11、下列有关数据库系统及相关内容的说法中，错误的是（      ） 。

A、 数据库系统是由计算机软硬件组成的复杂系统，其体系结构与系统硬件平台密切相关

B、 数据库管理系统提供了查询、插入、删除、更新等通用数据操作，但没有提供各种面向具体应用领域的业务处理

C、 数据库中的数据是按照一定的数据模型组织和存储的、可供多个用户共享的、具有最小冗余度的相关数据集合

D、 数据字典记录数据库系统运行时数据库操作情况的日志信息，通常由数据库管理员管理和维护

12、下列对计算机网络的攻击方式中，属于被动攻击的是？（      ）

A、 口令嗅探

B、 重放

C、 拒绝服务

D、 物理破坏

13、关于分布式数据库，下列说法正确的是（      ） 。

A、 分布式数据库的事务管理包括恢复控制和并发控制，恢复控制一般采用的策略是基于两阶段提交协议

B、 在分布式数据库查询中，导致数据传输通信代价大的主要原因是各个站点分片的连接和并操作

C、 分布式数据库中的分布透明性包括分片透明性、位置透明性、局部数据模型透明性，其中分片透明性是最高层次的透明性

D、 分布式数据库的目标是本地自治、非集中式管理、高可用性、位置独立性、数据分片独立性等

14、MD5算法以（       ）位分组来处理输入文本。

A、 64

B、 128

C、 256

D、 512

15、关于函数，下面哪个说法是错误的？（      ）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

16、根据我国网络安全应急响应的法律法规，网络安全事件可以分为7类，下列哪项不属于有害程序事件。（      ）

A、 蠕虫事件

B、 特洛伊事件

C、 信息泄露事件

D、 混合程序攻击事件

17、攻击者在使用nmap对目标网络进行扫描时发现，某个主机开放了25和110端口，此主机最有可能是？（      ）

A、 文件服务器

B、 邮件服务器

C、 WEB服务器

D、 DNS服务器

18、关于IP提供的服务，下列哪种说法是正确的？（      ）

A、 IP提供不可靠的数据投递服务，因此数据包投递不能受到保障

B、 IP提供不可靠的数据投递服务，因此它可以随意丢弃报文

C、 IP提供可靠的数据投递服务，因此数据报投递可以受到保障

D、 IP提供可靠的数据投递服务，因此它不能随意丢弃报文

19、ICMP泛洪利用了？（      ）

A、 ARP命令的功能

B、 traceroute命令的功能

C、 ping命令的功能

D、 route命令的功能

20、根据工信部明确的公共互联网网络安全突发事件应急预案文件，公共互联网网络突发事件等级最高可标示的颜色是什么？（      ）

A、 红色

B、 黄色

C、 蓝色

D、 橙色

21、黑客利用IP地址进行攻击的方法有？（      ）

A、 IP欺骗

B、 解密

C、 窃取口令

D、 发送病毒

22、在强制存取控制机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作（）。（      ）

A、 读取

B、 写入

C、 不可操作

D、 读取、写入

23、ARP欺骗的实质是？（      ）

A、 提供虚拟的MAC与IP地址的组合

B、 让其他计算机知道自己的存在

C、 窃取用户在网络中的传输的数据

D、 扰乱网络的正常运行

24、函数的\_\_doc\_\_属性表示？（      ）

A、 函数的名称

B、 函数中的说明

C、 函数中定义的变量

D、 函数的返回值

25、下列不属于口令安全威胁的是？（      ）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

26、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（      ） 。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

27、DES的秘钥长度是多少Bit?（      ）

A、 6

B、 56

C、 128

D、 32

28、MD5散列算法具有（      ） 位摘要值。

A、 56

B、 128

C、 160

D、 168

29、VIM模式切换的说法中，正确的是？（      ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

30、Shell编程条件判断中，说法错误的是？（      ）

A、 -b 判断文件是否存在，并且是否为块设备文件

B、 -c 判断文件是否存在，并且是否为字符设备文件

C、 -d 判断文件是否存在，并且是否为目录文件

D、 -e 判断文件是否存在，并且是否为普通文件

31、Linux软件管理rpm命令，说法不正确的是？（      ）

A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示2%

C、 -q PACKAGE\_NAME：查询指定的包是否已经安装

D、 -e 升级安装包

32、关于sed操作命令中，说法错误的是？（      ）

A、 a 命令在行的前面另起一行新增

B、 p 命令打印相关行，配合-n使用

C、 c 命令替换行

D、 d 命令删除行

33、部署大中型IPSEC VPN 时，从安全性和维护成本考虑，建议采取什么样的技术手段提供设备间的身份验证?（      ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

34、Jennings 发生器用了一个复合器来组合（     ）个LFSR。

A、 1

B、 2

C、 3

D、 4

35、vim命令中，用于查找并替换的命令，正确的是？（      ）

A、 xw

B、 1,$s/test/360/g

C、 cw

D、 p

二、 多选题 （共每题3分，共10题，共30分）

1、安全业务指安全防护措施，包括（       ）  。

A、 保密业务

B、 认证业务

C、 完整性业务

D、 不可否认业务

2、SQL Server提供了DES、RC2、RC4和AES等加密算法，没有某种算法能适应所有要求，每种算法都有优劣势，但选择算法需要有如下共通之处（       ）  。

A、 强加密通常会比较弱的加密占用更多的CPU资源

B、 长密钥通常会比短密钥生成更强的加密

C、 如果加密大量数据，应使用对称密钥来加密数据，并使用非对称密钥来加密该对称密钥

D、 可以先对数据进行加密，然后再对其进行压缩

3、Python中哪些符号可以包含字符串数据？（       ）

A、 单引号

B、 双引号

C、 两个双引号

D、 三个双引号

4、下面哪些选项是类的属性？（       ）

A、 \_\_doc\_\_

B、 \_\_init\_\_

C、 \_\_module\_\_

D、 \_\_class\_\_

5、下面那些方法可以检测恶意ICMP流量？（       ）

A、 检测同一来源ICMP数据包的数量

B、 注意那些ICMP数据包中payload大于64比特的数据包

C、 寻找那些响应数据包中payload跟请求数据包不一致的ICMP数据包

D、 检查ICMP数据包的协议标签

6、使用os.walk函数可以得到哪些内容？（       ）

A、 目录的路径

B、 子目录的列表

C、 非目录的文件列表

D、 目录中文件的大小

7、VPN设计中常用于提供用户识别功能的是（       ）  。

A、 RADIUS

B、 TOKEN卡

C、 数字证书

D、 8O2.1xAA.OOcIn.com

8、上传文件夹权限管理方法包括 ？（       ）

A、 取消执行权限

B、 限制上传文件大小

C、 设置用户umask值

D、 在上传目录关闭php解析引擎

9、在反杀伤链中，情报可以分为那几个层次？（       ）

A、 战斗

B、 战略

C、 战区

D、 战术

10、以下后缀中，属于Linux中常见压缩文件后缀的有？（       ）

A、 doc

B、 zip

C、 tar.gz

D、 ppt

**一、 单选题 （每题2分，共35题，共70分）**

1、为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行制定的条例。由中华人民共和国国务院于（  ）年2月18日发布实施《中华人民共和国计算机信息系统安全保护条例》，（  ）年1月8日修订。

A、 1994   2010

B、 1995   2011

C、 1994   2011

D、 1995   2010

2、随意下载、使用、传播他人软件或资料属于（ ）信息道德与信息安全失范行为。

A、黑客行为

B、侵犯他人隐私

C、侵犯知识产权

D、信息传播

3、部署大中型 IPSEC  VPN  时，从安全性和维护成本考虑，建议采取什么样的技术手段提供设备间的身份验证。（     ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

4、针对Windows系统主机，攻击者可以利用文件共享机制上的Netbios“空会话”连接漏洞，获取众多对其攻击有利的敏感信息，获取的信息中不包含下列哪一项信息？（     ）

A、 系统的用户和组信息

B、 系统的共享信息

C、 系统的版本信息

D、 系统的应用服务和软件信息

5、IP数据报分片后的重组通常发生在？（     ）

A、 源主机和数据报经过的路由器上

B、 源主机上

C、 数据报经过的路由器上

D、 目的主机上

6、下面不属于SYN FLOODING攻击的防范方法的是？（     ）

A、 缩短SYN Timeout（连接等待超时）时间

B、 利用防火墙技术

C、 TCP段加密

D、 根据源IP记录SYN连接

7、当数据库系统出现故障时，可以通过数据库日志文件进行恢复。下列关于数据库日志文件的说法，错误的是（     ）。

A、 数据库出现事务故障和系统故障时需使用日志文件进行恢复

B、 使用动态转储机制时，必须使用日志文件才能将数据库恢复到一致状态

C、 在OLTP系统中，数据文件的空间使用量比日志文件大得多，使用日志备份可以降低数据库的备份空间

D、 日志文件的格式主要有以记录为单位的日志文件和以数据块为单位的日志文件两种

8、SQL的GRANT和REVOKE语句可以用来实现（     ）。

A、 自主存取控制

B、 强制存取控制

C、 数据库角色创建

D、 数据库审计

9、下面对于数据库视图的描述正确的是（     ）。

A、 数据库视图也是物理存储的表

B、 可通过视图访问的数据不作为独特的对象存储，数据库内实际存储的是 SELECT语句

C、 数据库视图也可以使用 UPDATE 或 DELETE 语句生成

D、 对数据库视图只能查询数据，不能修改数据

10、有一种攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统显影减慢甚至瘫痪。它影响正常用户的使用，甚至使合法用户被排斥而不能得到服务。这种攻击叫做（     ）。

A、 可用性攻击

B、 拒绝性攻击

C、 保密性攻击

D、 真实性攻击

11、16模20的逆元是？（    ）

A、 3

B、 4

C、 5

D、 不存在

12、PKZIP 算法广泛应用于（      ）程序。

A、 文档数据加密

B、 数据传输加密

C、 数字签名

D、 文档数据压缩

13、下列选项哪列不属于网络安全机制？（     ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

14、一个C程序的执行是从哪里开始的？（     ）

A、 本程序的main函数开始，到main函数结束

B、 本程序文件的第一个函数开始，到本程序main函数结束

C、 本程序的main函数开始，到本程序文件的最后一个函数结束

D、 本程序文件的第一个函数开始，到本程序文件的最后一个函数结束

15、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（     ）。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

16、下列不属于口令安全威胁的是？（     ）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

17、在远程管理Linux服务器时，以下（     ）方式采用加密的数据传输。

A、 rsh

B、 telnet

C、 ssh

D、 rlogin

18、在C语言中（以16位PC机为例），5种基本数据类型的存储空间长度的排列顺序为?（    ）

A、 char<int<longint<=float<double

B、 char=int<longint<=float<double

C、 char<int<longint=float=double

D、 char=int=longint<=float<double

19、下列方法中不能用来进行DNS欺骗的是？（     ）

A、 缓存感染

B、 DNS信息劫持

C、 DNS重定向

D、 路由重定向

20、以下对DoS攻击的描述，正确的是？（     ）

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、 导致目标系统无法正常处理用户的请求

D、 若目标系统没有漏洞，远程攻击就不会成功

21、通过TCP序号猜测，攻击者可以实施下列哪一种攻击？（     ）

A、 端口扫描攻击

B、 ARP欺骗攻击

C、 网络监听攻击

D、 TCP会话劫持攻击

22、下面不是保护数据库安全涉及到的任务是（）。（     ）

A、 确保数据不能被未经过授权的用户执行存取操作

B、 防止未经过授权的人员删除和修改数据

C、 向数据库系统开发商索要源代码，做代码级检查

D、 监视对数据的访问和更改等使用情况

23、下面不是 Oracle 数据库提供的审计形式的是（     ）。

A、 备份审计

B、 语句审计

C、 特权审计

D、 模式对象设计

24、在一下古典密码体制中，属于置换密码的是？（     ）

A、 移位密码

B、 倒叙密码

C、 仿射密码

D、 PlayFair 密码

25、一个基于网络的IDS应用程序利用什么来检测攻击？（     ）

A、 正确配置的DNS

B、 特征库

C、 攻击描述

D、 信息包嗅探器

26、下列工具中可以对web表单进行暴力破解的是?（    ）

A、 Burp suite

B、 Nmap

C、 sqlmap

D、 Appscan

27、在(    )年，美国国家标准局NBS把IBM的Tuchman-Meyer方案确定数据加密标准，即  DES。（     ）

A、 1949

B、 1972

C、 1977

D、 2001

28、VIM模式切换的说法中，正确的是？（     ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

29、密码学的目的是?（     ）

A、 研究数据加密

B、 研究数据解密

C、 研究数据保密

D、 研究信息安全

30、能显示TCP和UDP连接信息的命令是？（     ）

A、 netstat -s

B、 netstat -e

C、 netstat -r

D、 netstat -a

31、重合指数法对下面哪种密码算法的破解最有效？（     ）

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

32、Python中哪个占位符表示字符串数据？（     ）

A、 %s

B、 %S

C、 %d

D、 %b

33、关于sed操作命令中，说法错误的是？（     ）

A、 a 命令在行的前面另起一行新增

B、 p 命令打印相关行，配合-n使用

C、 c 命令替换行

D、 d 命令删除行

34、RIP路由协议有RIP v1 和RIP v2两个版本，下面关于这两个版本的说法错误的是（     ）。

A、 RIP v1和RIP v2都具有水平分割功能

B、 RIP v1 是有类路由协议，RIP v2是无类路由协议

C、 RIP v1 和 RIP v2 都是以跳数作为度量值

D、 RIP v1 规定跳数的最大值为15，16跳视为不可达；而RIP v2无此限制

35、在RHEL5系统中，对Postfix邮件服务的配置主要通过修改（    ）文件来进行。

A、 Main.cf

B、 Smtpd.conf

C、 Postfix.cf

D、 Postfix.conf

**二、 多选题 （每题3分，共10题，共30分）**

1、Apache服务器外围加固措施包括？（       ）

A、 部署WAF

B、 部署IPS

C、 部署IDS

D、 部署蜜罐系统

2、数据库系统可能的潜在安全风险包括（       ）。

A、 操作系统安全风险，包括软件的缺陷、未进行软件安全漏洞修补工作、脆弱的服务和选择不安全的默认配置

B、 数据库系统中可用的但并未正确使用的安全选项、危险的默认设置、给用户不适当的权限、对系统配置的未经授权的改动等

C、 不及时更改登录密码或密码太过简单，存在对重要数据的非法访问以及窃取数据库内容或恶意破坏等

D、 数据库系统的内部风险，如内部用户的恶意操作等

3、关于函数，下面哪些说法是错误的？（       ）

A、 函数必须返回一个结果

B、 函数不能调用自身

C、 函数命名只能以字母或数字开头

D、 在同一个文件中，不应定义重名的函数

4、netwox工具拥有以下哪些功能？（       ）

A、 嗅探

B、 SQL注入

C、 欺骗

D、 地址转换

5、移动用户常用的VPN接入方式是（       ）。

A、 L2TP

B、 IPSECHIKE野蛮模式

C、 GRE+IPSEC

D、 L2TP+IPSEC

6、以下关于TCP和UDP协议的说法错误的是？（       ）

A、 没有区别，两者都是在网络上传输数据

B、 TCP是一个定向的可靠的传输层协议，而UDP是一个不可靠的传输层协议

C、 UDP是一个局域网协议，不能用于Interner传输，TCP则相反

D、 TCP协议占用带宽较UDP协议多

7、APTECH公司的管理员使用DPM 2007对Exchange Server 2007中的邮件进行备份还原，当通过Exchange Server 2007中的恢复存储组进行还原时，下列选项中说法正确的是（       ）。

A、 可以对单个用户的邮箱数据进行还原

B、 只能够对整个存储组的所有用户邮箱数据进行还原

C、 其他存储组的用户邮箱不可用

D、 需要停止Microsoft ExchangeInformation Store服务

8、Bash环境变量中，常见的环境变量有？（       ）

A、 HOSTNAME

B、 PASS

C、 SHELL

D、 USER

9、防火墙的主要技术有哪些？（       ）

A、 简单包过滤技术

B、 状态检测包过滤技术

C、 应用代理技术

D、 复合技术

10、关于IKE的描述正确的是（       ）

A、 IKE不是在网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥

B、 IKE是在网络上传送加密后的密钥，以保证密钥的安全性

C、 IKE采用完善前向安全特性PFS，一个密钥被破解，并不影响其他密钥的安全性

D、 IKE 采用DH算法计算出最终的共享密钥

**六、         
理论技能与职业素养（100分）**

【注意事项】

1.理论测试前请仔细阅读测试系统使用说明文档，按提供的账号和密码登录测试系统进行测试，账号只限1人登录。

2.该部分答题时长包含在第三阶段比赛时长内，请在临近竞赛结束前提交。

3.参赛团队可根据自身情况，可选择1-3名参赛选手进行作答，团队内部可以交流，但不得影响其他参赛队。

**一、 单选题 （每题2分，共35题，共70分）**

1、《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过，自（  ）起施行。

A、 2019年6月1日

B、 2018年6月1日

C、 2017年6月1日

D、 2016年6月1日

2、下列(   )行为属于信息道德与信息安全失范行为。

A、上网

B、朋友圈恶作剧

C、网络诈骗

D、网上购物

3、设在RSA 的公钥密码体制中，公钥为（e,n）=（13，35），则私钥d=？（   ）。

A、 11

B、 13

C、 15

D、 17

4、关于函数，下面哪个说法是错误的？（   ）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

5、以下哪一项描述不正确？（   ）

A、 ARP是地址解析协议

B、 TCP/IP传输层协议有TCP和UDP

C、 UDP协议提供的是可靠传输

D、 IP协议位于TCP/IP网际层

6、下列选项中不是 Hydra工具中的-e参数的值是？（   ）

A、 o

B、 n

C、 s

D、 r

7、网络监听（嗅探）的这种攻击形式破坏了下列哪一项内容？（   ）

A、 网络信息的抗抵赖性

B、 网络信息的保密性

C、 网络服务的可用性

D、 网络信息的完整性

8、下面程序的运行结果是: ＃i nclude&lt;stdio. h&gt; main() { int x,i; for(j-1;i&lt;=100;i++) {x=i;if(++x%2==0) if(++x%3==0) if(++x%7==0) printf("%d",x); } } 。（   ）

A、 26 68

B、 2870

C、 39 81

D、 42 84

9、IPSEC包括报文验证头协议AH协议号（）和封装安全载荷协议ESP协议号。（   ）

A、 51 50

B、 50 51

C、 47 48

D、 48 47

10、在远程管理Linux服务器时，以下(）方式采用加密的数据传输。（   ）

A、 rsh

B、 telnet

C、 ssh

D、 rlogin

11、在wireshark中下列表达式能捕获设置了PSH位的TCP数据包的是？（   ）

A、 tcp[13]&4==4

B、 tcp[13]&2==2

C、 tcp[13]&16==16

D、 tcp[13]&8==8

12、什么是数据库安全的第一道保障（  ）。

A、 操作系统的安全

B、 数据库管理系统层次

C、 网络系统的安全

D、 数据库管理员

13、以下不属于防火墙作用的是（   ）。

A、 过滤信息

B、 管理进程

C、 清除病毒

D、 审计监测

14、在数据库系统中,死锁属于（  ）。

A、 系统故障

B、 事务故障

C、 介质保障

D、 程序故障

15、哪个关键字可以在python中定义函数？（   ）

A、 dcf

B、 def

C、 class

D、 public

16、下面哪些选项可以让输出的字符串换行？（   ）

A、 print '''im Happy'''

B、 print 'im \nhappy'

C、 print 'im /nhappy'

D、 print ''im happy''

17、小李在使用nmap对目标网络进行扫描时发现，某一个主机开放了25和110端口，此主机最有可能是什么？（   ）

A、 文件服务器

B、 邮件服务器

C、 WEB服务器

D、 DNS服务器

18、手动脱压缩壳一般是用下列哪种方法？（   ）

A、 使用upx 脱壳

B、 使用winhex 工具脱壳

C、 使用fi扫描后，用unaspack脱壳

D、 确定加壳类型后，ollyice 调试脱壳

19、下面不是 Oracle 数据库提供的审计形式的是（  ）。

A、 备份审计

B、 语句审计

C、 特权审计

D、 模式对象设计

20、如果想在类中创建私有方法，下面哪个命名是正确的？（   ）

A、 \_add\_one

B、 add\_one

C、 \_\_add\_one

D、 add\_one\_\_

21、POP3服务器使用的监听端口是？（   ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

22、下列哪个工具可以进行web程序指纹识别？（   ）

A、 nmap

B、 openVAs

C、 御剑

D、 whatweb

23、在需求分析阶段规定好不同用户所允许访问的视图，这属于数据库应用系统的（  ）。

A、 功能需求分析

B、 性能需求分析

C、 存储需求分析

D、 安全需求分析

24、假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包，这时你可以使用以下哪一种类型的进攻手段？（   ）

A、 缓冲区溢出

B、 暴力攻击

C、 地址欺骗

D、 拒绝服务

25、下面那个名称不可以作为自己定义的函数的合法名称？（   ）

A、 print

B、 len

C、 error

D、 Haha

26、以下关于正则表达式，说法错误的是？（   ）

A、 ‘root’表示匹配包含root字符串的内容

B、 ‘.’表示匹配任意字符

C、 [0-9]表示匹配数字

D、 ‘^root’表示取反

27、哪个关键词可以在python中进行处理错误操作？（   ）

A、 try

B、 catch

C、 finderror

D、 error

28、VIM退出命令中，能强制保存并退出的是？（   ）

A、 x

B、 wq

C、 q

D、 wq!

29、下列不属于网络安全CIA需求属性的是哪一项？（   ）

A、 机密性

B、 可抵赖性

C、 完整性

D、 可用性

30、在一台Cisco路由器R1上进行了如下ACL配置: R1（config）#access-list 1permit any R1（config）#access-list 1 deny192.168.21.1 0.0.0.0 R1（config）#interface f0/0 R1（config）#ip access-group 1 in 以上设置可以实现在路由器R1的F0/0接口的（   ）功能。

A、 拒绝来自主机192.168.21.1的数据包

B、 只允许来自主机192.168.21.1的数据包

C、 允许所有报文通过

D、 拒绝所有报文转发

31、在RHEL5系统中，使用lvextend为逻辑卷扩容以后，还需要进行（   ）操作以便系统能够识别新的卷大小。

A、 Lvscan

B、 Partprobe

C、 Reboot

D、 resize2fs

32、Linux软件管理rpm命令，说法不正确的是？（    ）

A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示2%

C、 -q PACKAGE\_NAME：查询指定的包是否已经安装

D、 -e 升级安装包

33、SYN Flood属于？（    ）

A、 拒绝服务攻击

B、 缓存区溢出攻击

C、 操作系统漏洞攻击

D、 社会工程学攻击

34、差分分析是针对下面那种密码算法的分析方法？（    ）

A、 DES

B、 AES

C、 RC4

D、 MD5

35、按目前的计算能力，RC4算法的密钥长度至少应为（       ）才能保证安全强度。

A、 任意位

B、 64位

C、 128位

D、 256位

**二、 多选题 （共10题，30分）**

1、下面标准可用于评估数据库的安全级别的有（  ）。

A、 TCSEC

B、 IFTSEC

C、 CC DBMS.PP

D、 GB17859-1999E.TD

2、Bash编程中，常见的循环有？（    ）

A、 foreach

B、 while

C、 for

D、 until

3、关于yum命令，说法正确的有哪些？（    ）

A、 -y 自动应答yes

B、 -e 静默执行

C、 -t 延迟安装

D、 -R[分钟] 设置等待时间

4、源代码泄露可能让攻击者分析出哪些其它漏洞？（    ）

A、 SQL注入

B、 命令执行

C、 文件上传

D、 XSS

5、下列关于SQL Server 2008中guest用户的说法，正确的是（  ）。

A、 guest用户没有对应的登录账户名

B、 通过授权语句可以启用数据库中的guest用户

C、 所有数据库用户都继承该数据库中guest用户的权限

D、 任何SQL Server登录账户都可以访问启用了guest用户的数据库

6、隐藏Apache服务器信息的方法包括？（    ）

A、 隐藏HTTP头部信息

B、 禁止显示错误信息

C、 自定义错误页面，消除服务器的相关信息

D、 修改服务IP地址

7、在RHEL5系统中，以下（   ）操作将在分区/dev/sdb7上创建EXT3文件系统。

A、 mkfs –t ext3 /dev/sdb7

B、 mkfs.ext3 /dev/sdb7

C、 fdisk –t ext3 /dev/sdb7

D、 format /dev/sdb7 –t ext3

8、IKE的主要功能包括(   )

A、 建立IPSec安全联盟

B、 防御重放攻击

C、 数据源验证

D、 自动协商交换密钥

9、利用Metasploit进行缓冲区溢出渗透的基本步骤包括（   ）。

A、 选择利用的漏洞类型

B、 选择meterpreter或者shell 类型的payload

C、 设置渗透目标IP、本机IP地址和监听端口号

D、 选择合适的目标类型

10、以下Linux命令中，跟目录及文件基本操作相关的命令有哪些？（    ）

A、 cd

B、 touch

C、 rm

D、 userdel