2025年河南省中等职业教育竞赛活动网络信息安全赛项

第一部分网络信息安全理论测试题库

一、单选题

1. 基于域名的虚拟主机所不具有的优点是(　　)。

A. 不需要更多的 IP 地址　　B. 复杂简单　　C. 无须特殊的软硬件支持　　D. 多数现代的浏览器支持这种虚拟主机的实现方法

参考答案：C

2. Linux 文件名的长度不得超过个字符(　　)。

A. 64　　B. 128　　C. 255.0　　D. 512

参考答案：C

3. 通常 Linux 支持的网卡类型不包括:(　　)。

A. 令牌网卡　　B. 以太网卡　　C. PCMCIA　　D. PS/2

参考答案：D

4. Linux 的根分区系统类型是 ( )

A. FAT16　　B. FAT32　　C. ext4　　D. NTFS

参考答案：C

5. 内核不包括的子系统是(　　)。

A. 进程调度系统　　B. 内存管理系统　　C. 虚拟文件系统　　D. 硬件管理系统

参考答案：D

6. 为了允许 vsftpd 读取用户主目录中的文件，需要设置以下哪个 SELinux 布尔值？

A. ftpd_full_access　　B. vsftpd_enable_access　　C. chroot_local_user　　D. allow_writeable_chroot

参考答案：A

7. SELinux 中的 MLS 策略指的是什么？

A. 标签访问控制策略　　B. 宽松访问控制策略　　C. 多级安全性策略　　D. 强制访问控制策略

参考答案：C

8. iptables 是 Linux 操作系统上用于配置和管理什么的工具？

A. 硬盘分区　　B. 用户权限　　C. 网络连接　　D. 防火墙规则

参考答案：D

9. 负载均衡的作用是什么？

A. 减少系统的延迟　　B. 增加用户的带宽　　C. 提高系统的可用性和可靠性　　D. 增加系统的带宽

参考答案：C

10. 下列哪个是常见的邮件传输代理（MTA）软件？

A. Dovecot　　B. Telnet　　C. OpenSSL　　D. Postfix

参考答案：D

11. linux 临时目录一般存在下面那个文件夹中

A. /dev　　B. /tmp　　C. /proc　　D. /data

参考答案：B

12. 在Linux系统上配置DNSSEC时，使用的常用软件是什么？

A. Nginx　　B. Tomcat　　C. BIND　　D. Apache

参考答案：C

13. 在使用openssl生成自签名证书时，以下哪个命令可以生成证书签名请求文件？

A. openssl x509　　B. openssl ca　　C. openssl genrsa　　D. openssl req

参考答案：D

14. 应急流程中，定位攻击者的目的是什么？

A. 找到攻击线索　　B. 定位攻击者的位置　　C. 缩小应急响应的范围　　D. 加快应急响应的速度

参考答案：B

15. 邮件服务器中的邮件传输代理（MTA）主要负责什么？

A. 处理邮件的传输和路由　　B. 提供邮件访问和管理功能　　C. 进行用户认证和权限控制　　D. 接收和存储邮件

参考答案：A

16. DNSSEC的数字签名是使用哪种算法生成的？

A. MD5　　B. SHA　　C. AES　　D. RSA

参考答案：D

17. 应急流程中，确定攻击时间的目的是什么？

A. 找到攻击线索　　B. 定位攻击者的位置　　C. 缩小应急响应的范围　　D. 加快应急响应的速度

参考答案：C

18. 以下哪个命令用于查看文件或目录的 ACL 权限？

A. getfacl　　B. setfacl　　C. chmod　　D. chown

参考答案：A

19. 在 DHCP 故障转移配置中，mclt 表示：

A. 最大未应答更新次数　　B. 最大负载均衡时间间隔　　C. 最大客户端租约到期时间　　D. 最大响应延迟时间

参考答案：C

20. 如何启动 Nginx 服务？

A. systemctl restart nginx　　B. systemctl stop nginx　　C. systemctl reload nginx　　D. systemctl start nginx

参考答案：D

21. 在 CentOS Linux 7 上安装 Apache 服务的命令是？

A. yum -y install apache　　B. apt-get install apache　　C. apt-get -y install apache　　D. yum install apache

参考答案：A

22. Linux 中，每个文件都有一个所有者和一个所在组。以下哪个命令可以查看文件的所有者和所在组？

A. chown　　B. chmod　　C. ps -ef　　D. ls -l

参考答案：D

23. 在使用 openssl 生成自签名证书时，以下哪个命令可以生成私钥文件？

A. openssl x509　　B. openssl ca　　C. openssl genrsa　　D. openssl req

参考答案：C

24. 在创建本地用户帐户时，默认情况下，Samba 使用哪个后端来存储数据库？

A. mysql　　B. postgresql　　C. tdbsam　　D. ldap

参考答案：D

25. 以下哪种安全措施可以保护数据库中的敏感数据？

A. 启用审计功能和日志记录。　　B. 多因素认证和强密码策略。　　C. 定期备份数据库。　　D. 及时更新数据库软件和补丁。

参考答案：B

26. CMS 的一些任意代码执行漏洞是什么造成的？( )

A. 开发人员对客户端进来的数据没有严格防范　　B. 允许用户进行搜索　　C. 允许用户上传文件　　D. 允许客户端的数据保存到服务器

参考答案：A

27. 下面哪个不是数据库主机系统加固的基本原则之一？

A. 安全审计和监控　　B. 最小权限原则　　C. 强密码策略　　D. 开放所有端口

参考答案：D

28. 下面哪个不是SQL Server 的内置模式?

A. sys　　B. guest　　C. schema　　D. dbo

参考答案：C

29. SQL Server 附带的 SQL 语言实现是什么?

A. PL/SQL　　B. MySQL　　C. ANSI SQL　　D. T-SQL

参考答案：D

30. 当 Tomcat 运行在主机上，且启用了 HTTP PUT 请求方法（例如，将 readonly 初始化参数由默认值设置为 false），攻击者将可通过精心构造的攻击请求向服务器上传包含任意代码的 JSP 文件。之后，JSP 文件中的代码将能被服务器执行。这就造成了（ ）

A. SQL 注入漏洞　　B. CSRF 漏洞　　C. XSS 漏洞　　D. 远程代码执行漏洞

参考答案：D

31. 经典MVC 模式中，M 是指（ ），V 是指用户界面，C 则是控制器。

A. 数据模型　　B. 菜单　　C. 业务模型　　D. 过滤器

参考答案：C

32. sqlmap 要想注入一个需要登录的网站时，需要加上什么参数?（ ）

A. --file-read　　B. --dbs　　C. --id　　D. --cookie

参考答案：D

33. Web 应用程序建立在（）协议基础上。

A. IP　　B. FTP　　C. HTTP　　D. TCP

参考答案：C

34. （ ）可以做到不损失任何图像质量，但同时也最容易被攻击。

A. MISC　　B. CTF　　C. LSB　　D. 元数据修改的方法

参考答案：D

35. 以下哪个工具可以用于数据库渗透测试中的弱口令检测？

A. Hydra　　B. Nessus　　C. SQLMap　　D. Nmap

参考答案：A

36. 以下哪项不是数据库基本安全措施中的一部分？

A. 数据库连接安全　　B. 访问控制　　C. 双因素身份验证　　D. 审计日志

参考答案：D

37. 一般来说，我们认为 CSRF 是一种（）攻击

A. 双向　　B. 跨域获取数据　　C. 参数　　D. 单方向

参考答案：D

38. sqlmap 要想列出所有数据库，需要加上什么参数？（）

A. --file-read　　B. --dbs　　C. --id　　D. --cookie

参考答案：B

39. 当我们在一个 PHP 写的网站的 URL 地址的 test 参数中注入../../etc/passwd\0 时，其中../../是返回上层目录，我们把这种方式称为（ ）

A. 命令注入　　B. Path Traversal　　C. 字符串截断　　D. 敏感信息读取

参考答案：B

40. 数据库快照是指在某个特定时间点上的数据库的

A. 数据恢复　　B. 数据分析　　C. 数据副本　　D. 数据备份

参考答案：C

41. 会话固定攻击是基于（ ）的一种漏洞。

A. XSS　　B. Cookie　　C. 登录前和登录后的 Session ID 不变　　D. CSRF

参考答案：C

42. MySQL 的查询日志（General Query Log）用于记录什么内容？

A. 事务的回滚和崩溃恢复　　B. 错误消息和警告信息　　C. 所有查询语句，包括 SELECT、INSERT、UPDATE、DELETE 等　　D. 慢查询的执行时间

参考答案：C

43. 哪个图形化工具是由 Microsoft 专门为管理 SQL Server 数据库开发的？

A. SQL Server Management Studio (SSMS)　B. pgAdmin　C. MySQL Workbench　D. phpMyAdmin

参考答案：A

44. 晓熙经过3年中职的学习，已经掌握了基本的信息安全技术。她心里很痒痒，非常想找些Web网站练习一下。于是她用GoogleHack技术在网上搜到了一些安全性能不强的网站，用Bp爆破了密码登录了进去，看到了很多敏感信息。请问晓熙的行为触犯了什么法律？（ ）。

A. 中华人民共和国数据安全法　B. 国家安全法　C. 中华人民共和国网络安全法　D. 计算机管理条例

参考答案：C

45. CVE-2018-1058漏洞的利用条件是什么？

A. 需要攻击者能够远程访问数据库服务器　B. 需要特定的操作系统环境才能利用该漏洞　C. 需要攻击者具有足够的权限才能利用该漏洞　D. 任何用户都可以利用该漏洞

参考答案：C

46. （ ）是一种常被用做图片隐写的算法（在CTF中经常见到她的身影）

A. JPG　B. PNP　C. LSB　D. JSP

参考答案：C

47. MySQL中常用的日期和时间类型是哪些？

A. INT　B. FLOAT　C. DATE　D. STRING

参考答案：C

48. 以下哪种 SQL 注入类型是利用"UNION"运算符来进行攻击的？

A. 基于时间的 SQL 注入　　B. 基于错误的 SQL 注入　　C. 基于联合的 SQL 注入　　D. SQL 盲注

参考答案：C

49. 数据库安全的一个重要组成部分是推理控制，它的目的是什么？

A. 防止未经授权的访问数据库　　B. 加密数据库中的敏感数据　　C. 阻止用户从不太敏感的数据中得出有关敏感信息的结论　　D. 控制数据库的数据流

参考答案：C

50. 以下哪种情况属于数据库安全事件中的数据泄露？

A. 数据库中的数据被意外删除。　　B. 数据库中的数据被篡改或修改。　　C. 数据库中的敏感数据被未授权访问。　　D. 数据库系统无法正常提供服务。

参考答案：C

51. 以下哪种情况可能导致 SQL 注入攻击？

A. 使用预编译语句来执行 SQL 查询　　B. 将用户输入直接拼接到 SQL 查询语句中　　C. 对用户输入进行充分验证和过滤　　D. 使用参数化查询来防止 SQL 注入

参考答案：B

52. 2017 年 9 月 5 日，Apache Struts 发布最新安全公告，Apache Struts2 的 REST 插件存在远程代码执行的高危漏洞，漏洞编号为 CVE-2017-9805（S2-052）。原因是启用 Struts REST 插件并使用 XStream

组件对 XML 进行反序列操作时（），可被攻击者进行远程代码执行攻击(RCE)

A. 未使用 jsonlib 方法　　B. 未对数据输出进行过滤　　C. 可以任意构建可执行代码　　D. 未对数据内容进行有效验证

参考答案：D

53. 想要查找 URL 中包含 nankai 的搜索指令的是（）

A. inurl：nankai　　B. ip：nankai　　C. intitle：nankai　　D. site：nankai

参考答案：A

54. HTTP 协议在网络协议族里属于（）协议

A. 传输层　　B. 链路层　　C. 网络层　　D. 应用层

参考答案：D

55. PostgreSQL 可以用作以下哪种类型的数据库存储?

A. 关系型数据库　　B. NoSQL 数据库　　C. 图数据库　　D. 所有答案都是正确的

参考答案：A

56. 在 MySQL 中删除数据使用的是什么语句?

A. UPDATE　　B. DELETE　　C. INSERT INTO　　D. SELECT

参考答案：B

57. SELECT 语句主要用于从数据库检索数据并将检索结果返回给应用程序或用户。下列 SQL 语句将返回 tbUsers 表中的所有数据：

A. SELECT * FROM tblUsers WHERE username=’admin’ AND password = ‘letmein’ B. SELECT * INTO hackerTable FROM tblUsers C. SELECT * FROM tblUsers D. SELECT username FROM tblUsers

参考答案：C

58. 已知服务器的代码为

```

function render (input) {

  return '<textarea>' + input + '</textarea>'

}

```

其中 input 参数是用户可以输入值的地方，请问用户输入下面哪条语句可以触发 xss。

A. "><script>alert(1)</script> B. <script>alert`1`</script> C. </textarea><script>alert(1)</script> D. <script>alert(1)</script>

参考答案：C

59. PHP 的配置文件是在( ) 中？

A. /etc/hosts B. /var/www/html C. /etc/php.ini D. /etc/httpd/conf.d/php.conf

参考答案：C

60. PostgreSQL 可以与下列哪种编程语言进行兼容和支持?

A. JavaScript　　B. C/C++　　C. Ruby　　D. 所有答案都是正确的

参考答案：D

61. 下列哪个是由 MySQL 开发的图形化数据库管理工具?

A. Navicat　　B. DBeaver　　C. MySQL Workbench　　D. phpMyAdmin

参考答案：C

62. SQL Server 中的透明数据加密 (TDE) 数据库的备份文件使用哪个密钥进行加密?

A. 证书私钥　　B. 对称密钥　　C. 密码　　D. 数据库主密钥 (DMK)

参考答案：B

63. 域组件的标识符是(　　)。

A. CN　　B. OU　　C. DC　　D. LADP

参考答案：C

64. 如果我们要在一台电脑上安装活动目录服务，应该选择以下哪一种文件系统(　　)。

A. FAT16　　B. FAT32　　C. NTFS　　D. UD

参考答案：C

65. 下面哪个方案是由于受 HTTP 协议头信息长度的限制,仅能存储小部分的用户信息(　　)。

A. 基于 Cookie 的 Session 共享　　B. 基于数据库的 Session 共享
C. 基于 Memcache 的 Session 共享　　D. 基于 Web 的 Session 共享

参考答案：A

66. 下面密码符合复杂性要求的是：(　　)。

A. admin　　B. Wang.123@　　C. !@#$%^　　D. 134587

参考答案：B

67. 为保证某 GPO 在域层次上使用,而又不被下层所覆盖。应使用以下那个选项?(　　)

A. 阻断策略继承　　B. 禁止　　C. 拒绝　　D. 禁止覆盖

参考答案：D

68. 组策略对象优先级决定了当多个 GPO 应用到同一对象时，哪个 GPO 的设置将被应用。下面哪个选项描述了组策略对象优先级的作用？

A. 它是组策略的基本单元，包含安全设置和配置。　　B. 它用于将 GPO 链接到特定的域、组织单位或站点。　　C. 它决定了哪个 GPO 的设置将被应用，根据优先级覆盖较低优先级的 GPO。　　D. 它决定了 GPO 的应用顺序，并覆盖先前应用的设置。

参考答案：C

69. DNSSEC 的设计方式是什么？

A. 强制要求所有应用程序使用 DNSSEC　　B. 不允许非 DNSSEC 应用程序访问 DNS 解析器　　C. 提供加密通信来保护应用程序和解析器之间的安全性　　D. 完全隐藏对不支持 DNSSEC 的应用程序的影响

参考答案：D

70. 下列哪个记录类型用于将主机名解析为 IP 地址？

A. CNAME 记录　　B. MX 记录　　C. PTR 记录　　D. A 记录

参考答案：D

71. Windows Server 中，哪个组策略可以控制密码的复杂性要求？

A. 账户锁定策略　　B. 密码策略　　C. 访问控制策略　　D. 安全审计策略

参考答案：B

72. 配置共享文件夹的配额需要使用哪个角色服务？

A. 文件服务器资源管理器　　B. 配额管理器　　C. 网络文件服务器　　D. 共享文件夹管理器

参考答案：A

73. 虚拟目录可以用于什么目的？

A. 映射 URL 路径到物理文件夹　　B. 托管动态内容　　C. 共享文件夹　　D. 访问外部资源

参考答案：A

74. 下面哪个选项是自签名证书的局限性之一？

A. 在公共环境中可能引发警告　　B. 可以节省成本　　C. 经过严格的验证和审核过程　　D. 提供强大的安全性

参考答案：A

75. 配置 Web 站点双向认证可以防止哪种攻击方式？

A. 中间人攻击　　B. DDOS 攻击　　C. XSS 攻击　　D. SQL 注入攻击

参考答案：A

76. 在配置 VPN 服务器时，选择的证书类型是什么？

A. 根证书　　B. 中级证书　　C. 用户证书　　D. 服务器证书

参考答案：D

77. IPSec 通过创建什么来管理加密和认证的参数？

A. 安全通道　　B. 安全连接　　C. 安全关联　　D. 安全策略

参考答案：C

78. 表单身份验证适用于什么类型的应用程序？

A. 移动应用程序　　B. 桌面应用程序　　C. Web 应用程序　　D. Windows 应用程序

参考答案：C

79. 当某个账户的登录成功时，会生成哪种类型的审核项？

A. 成功审核项　　B. 失败审核项　　C. 注销审核项　　D. 事件查看器

参考答案：A

80. 以下哪个选项不是防火墙的工作原理？

A. 规则管理　　B. 数据加密　　C. 数据包过滤　　D. 策略设置

参考答案：B

81. FTP 服务器的安全传输可以使用哪种协议来加密数据？

A. SMTP　　B. SSH　　C. SSL/TLS　　D. HTTP

参考答案：C

82. SSL 协议用于保护网络通信的安全，它能够对传输的数据进行什么操作？

A. 解密　　B. 签名　　C. 压缩　　D. 加密

参考答案：D

83. 在 NTFS 权限中，"读取和执行"权限的具体含义是什么？

A. 允许用户读取文件和执行可执行文件　　B. 允许用户读取文件和执行脚本文件　　C. 允许用户读取文件和执行系统命令　　D. 允许用户读取文件和执行任意操作

参考答案：A

84. 数字证书是一种包含了实体的公钥、身份信息和数字签名的电子文件，它是由（）颁发的。

A. 证书颁发机构　　B. 密钥颁发机构　　C. 证书服务　　D. 密钥服务

参考答案：A

85. 哪个选项禁用匿名管道访问，以减少潜在的风险？

A. 禁用 Guest 账户　　B. 禁用匿名管道访问　　C. 禁用本地系统将计算机标识用于 NTLM　　D. 不允许存储网络身份验证密码和凭据

参考答案：B

86. 账户锁定策略中，哪个选项指定了账户在多少次失败登录尝试后被锁定？

A. 密码最小长度　　B. 密码最大寿命　　C. 密码历史　　D. 锁定阈值

参考答案：D

87. 在防火墙 WEB 认证配置过程中，创建角色的目的是什么？

A. 创建角色映射规则，将用户组与角色相对应　　B. 便于管理人员的组织架构　　C. 将角色映射到 AAA 服务器　　D. 允许不同角色通过不同服务

参考答案：D

88. 下列哪个选项描述了 HTTP 响应报文的状态行？

A. 状态行包含了 HTTP 方法、URL 和协议版本。　　B. 状态行包含了客户端支持的 MIME 类型。　　C. 状态行包含了客户端的 IP 地址和端口号。　　D. 状态行包含了服务器的响应状态码和原因短语。

参考答案：D

89. 在 DCBC-netlog 中，文件类型条目之间的优先顺序是在哪个页面定义的？

A. 系统对象>文件类型　　B. 文件传输过滤>HTTP 上传　　C. 文件传输过滤>FTP 下载　　D. 应用控制策略

参考答案：A

90. 以下哪种方法可以有效防止文件包含攻击？

A. 使用最新版本的浏览器　　B. 避免在网站上发布任何内容　　C. 对用户输入进行适当的过滤和转义　　D. 定期更改用户密码

参考答案：C

91. 接收邮件过滤功能主要用于什么？

A. 防止用户访问特定网站　　B. 对接收的邮件进行检查和过滤　　C. 防止用户进行在线聊天　　D. 防止用户下载文件

参考答案：B

92. RIP 协议的更新时间间隔是多少？

A. 10 秒钟　　B. 20 秒钟　　C. 30 秒钟　　D. 40 秒钟

参考答案：C

93. OSPF 路由协议中，哪种区域是必须存在的？

A. 传输区域　　B. 边界区域　　C. 备份区域　　D. 核心区域

参考答案：D

94. 上网行为的流量管理技术中，哪项是不正确的？

A. 无法根据应用、服务、URL、服务类型、IP 地址(组)、用户(组)、服务(组)、时间进行流量控制　　B. 支持保障带宽和最大带宽　　C. 支持优先级，确保高优先级的应用能够优先获得带宽　　D. 使用通道带宽，实现层次化的流量管理

参考答案：A

95. 防病毒网关通常部署在（　）位置。

A. 网络出口　　B. 网络入口　　C. 网络边界　　D. 网络核心

参考答案：A

96. 在配置防盗链规则条目时，以下哪项是可选设置的？

A. 允许 Referer 为空　　B. 启用　　C. 保护 URL　　D. 检测方式

参考答案：A

97. 在源 NAT 中，如果转换前后的地址存在一种固定的映射关系，这种类型的源 NAT 叫做（ ）。

A. 静态 NAT　　B. 动态 NAT　　C. NAPT　　D. NAT Server

参考答案：A

98. 下列哪个选项描述了 HTTP 请求报文的请求行?

A. 请求行包含了 HTTP 方法、URL 和协议版本。　　B. 请求行包含了客户端支持的 MIME 类型。　　C. 请求行包含了客户端的 IP 地址和端口号。　　D. 请求行包含了服务器的响应状态码和原因短语。

参考答案：A

99. 防火墙的资源对象地址簿可以用于哪些方面的控制?

A. 控制应用程序访问　　B. 控制 URL 访问　　C. 所有上述控制　　D. 控制网络访问

参考答案：C

100. 在防火墙策略匹配原理中，以下哪个是最常用的匹配条件?

A. 目标端口号　　B. 源 IP 地址　　C. 目标 IP 地址　　D. 源端口号

参考答案：B

101. OSPF 路由协议中，哪种路由器负责连接不同的区域?

A. 自制路由器　　B. AS 边界路由器　　C. 区域边界路由器　　D. 备份设计路由器

参考答案：C

102. 防火墙的时间表主要用于控制哪些方面的访问?

A. 控制应用程序访问时间　　B. 控制用户访问时间　　C. 所有上述访问时间控制　　D. 控制网络访问时间

参考答案：D

103. 透明模式中，防火墙是什么状态？

A. 可见的　　B. 不可见的　　C. 部分可见的　　D. 不确定

参考答案：B

104. 常规盗链和分布式盗链的主要区别是什么？

A. 常规盗链和分布式盗链没有区别　　B. 分布式盗链只需要在自己的页面嵌入别人的链接　　C. 常规盗链只需要在自己的页面嵌入别人的链接　　D. 分布式盗链一般不针对某一个网站，互联网上任何一台机器都可能成为盗链的对象

参考答案：D

105. OSPF 路由协议中，哪种算法用于计算最短路径树？

A. Floyd 算法　　B. Prim 算法　　C. Bellman-Ford 算法　　D. Dijkstra 算法

参考答案：D

106. 在 python 中，打开文件的模式，要选择二进制，是以下哪一个选项（）

A. r　　B. a　　C. b　　D. x

参考答案：C

107. 发送一个 UDP 数据包，此数据包封装到三层，希望只接受 1 个应答数据包，我们应该使用的发送函数是

A. send()　　B. sendp()　　C. sr()　　D. sr1()

参考答案：D

108. 函数调用时所提供的参数可以是

A. 变量　　B. 函数　　C. 以上都可以　　D. 常量

参考答案：C

109. 在 Python 程序中执行了 import test as i ,若模块有函数 func()，在程序应该如何引用()。

A. test.func()　　B. i.func()　　C. 程序名.func()　　D. func()

参考答案：B

110. scapy 的 sniff 函数中，要监听网络中的 ARP 流量，下列 sniffer 写法正确的是（ ）

A. sniff(filter= protocol=arp)　　B. sniff(filter='arp')　　C. sniff(filter='tcp arp')　　D. sniff(filter='ether')

参考答案：B

111. 在网络路径中，有一台路由器接口断了，不能到达目的网络，此时它会向源发送 ICMP 协议，此时的类型与代码是()

A. 3， 3　　B. 3， 4　　C. 3， 1　　D. 3， 0

参考答案：D

112. 在 ARP 数据包中，有协议类型字段，它值通常 0x800，这是代表（）协议

A. IP　　B. ARP　　C. IGMP　　D. ICMP

参考答案：A

113. TCP 的半开连接扫描，是发送带有(　)标志位的 TCP 数据包

A. ACK　　B. FIN　　C. RST　　D. SYN

参考答案：D

114. 下面运算符优先级最低的是（）。

A. ==　　B. and　　C. +　　D. *=

参考答案：B

115. 下列那一种不是常见的 TCP 扫描技术（）

A. TCP FIN 扫描　　B. TCP connect()扫描　　C. TCP SYN 扫描　　D. IP 段扫描

参考答案：D

116. 若 aList=[1,2],则执行 aList.insert(-1,5)后，aList 的值是()。

A. [5,2,1]　　B. [1,5,2]　　C. [5,1,2]　　D. [1,2,5]

参考答案：B

117. 平时网络管理员需要经常查看主机的端口，以确认是否有非授权的网络程序在向外提供数据，下列说法正确的是：（）

A. 服务器上多开一个端口，少开一个端口是没有关系，只要网络服务正常即可　　B. 经常用命令或软件查看本地所开放的端口，看是否有

可疑端口　　C. 如果开放端口中有你不熟悉的，只要不是重要进程，可以不用去干涉它。　　D. 如果发现不正常的端口开放，我们只能关闭占用这个端口服务进程，没有其他办法

参考答案：B

118. 执行以下两条语句后，lst 的结果是（ ）

lst = [3, 2, 1]

lst.append (lst)

A. [3, 2, 1, lst]　　B. 抛出异常　　C. [3, 2, 1, ...,其中"."”表示无穷递归　　D. [3, 2, 1, [3, 2, 1]c

参考答案：C

119. 在 scapy 的 sniff 函数中，过滤 DNS 数据流量，下列写法正确的是（ ）

A. udp dst port 5353　　B. udp port 53　　C. dst port 53　　D. udp dst port 53

参考答案：D

120. 在 STP 的工作原理，交换机角色有

A. 接入交换与汇聚交换　　B. 根桥与非根桥　　C. 三层交换与二层交换　　D. 核心交换与汇聚交换

参考答案：B

121. 下面运算符优先级最高的是（ ）

A. ==　　B. and　　C. +　　D. *=

参考答案：C

122. 在DHCP的Discover包中，Ether层的目标MAC地址是（）

A. 随机的　　B. 01:02:03:04:05:06　　C. ff:ff:ff:ff:ff:ff　　D. 00:00:00:00:00:00

参考答案：C

123. 使用scapy构造DNS查询请求消息，其要求是一个标准查询，期望递归，假设dns=DNS(),如何设置对象dns的标志位，下列正确的是（）

A. dns.qr=0

dns.opcode=1

dns.rd=1　　B. dns.qr=0

dns.opcode=0

dns.rd=1　　C. dns.qr=1

dns.opcode=1

dns.rd=0　　D. dns.qr=1
dns.opcode=0
dns.rd=1

参考答案：B

124. 使用 ping 命令发送的数据包是遵守 ICMP 协议的，它的类型和代码分别是()

A. 3，3　　B. 13，0　　C. 0，0　　D. 8，0

参考答案：D

125. 下列那个端口用户私有端口（

A. 6666　　B. 49672　　C. 45672　　D. 22222

参考答案：B

126. "有下面一段程序

```
word ='山羊上山山碰山羊角'
sum =0
for letter in word:
    if letter == '山':
      sum +=1
print (sum)
```

这个程序运行的结果是（）

"

A. 3　　B. 1　　C. 2　　D. 4

参考答案：D

127. 对 subprocess.run()中的 args 参数，下面选项那一个是正确的（）

A. ['ls','-l']　　B. ('ls','-L')　　C. {'ls':'-l'}　　D. 'ls -l'

参考答案：D

128. DNS 客户端发出一个查询请求数据包，服务端收到后，回复一个响应数据包，客户端通过那一个字段来区分这次的查询与响应请求。（）

A. 查询请求中的问题内容　　B. 响应数据包中的 FLAGS　　C. 响应数据包的中的资源记录　　D. 查询请求中的事务 ID

参考答案：D

129. python3.7 在安装时，需要勾选

A. Add Python 3.7 to PATH　　B. Install launcher for all users　　C. Install Now　　D. Customize installation

参考答案：A

130. IP 数据包的头部最长可以是（）字节

A. 40　　B. 60　　C. 32　　D. 20

参考答案：B

131. 欲将两数中较小的数返回,应定义的匿名函数为（）

A. mymin=lambda x,y: x if x<y else y　　B. mymin=lambda x,y: if x<y x else y　　C. mymin-lambda x,y: if x<y:x else:y　　D. mymin=lambda x,y: x if x>=y else y

参考答案：A

132. 在根端口选中，首先比较的条件是（）

A. 以上都不是　　B. 端口 ID　　C. 桥 ID　　D. 链路的 COST 值

参考答案：D

133. Debian 的修改了安装源配置文件，应使用（）命令进行更新。

A. apt-get upgrade　　B. apt-cache search　　C. apt update　　D. apt list

参考答案：C

134. 当使用函数发送一个封装到三层的 UDP 数据包，对方主机并没有打开这个 UDP 端口，此时应该通过判断接收到的数的那层的协议来确认 UDP 端口状态

A. 以太网层协议　　B. 三层 ICMP 协议　　C. 三层 IP 协议　　D. 不确定

参考答案：B

135. DHCP 协议中的 Discover 消息是

A. 二层的目标 MAC 是“ff:ff:ff:ff:ff:ff”　　B. 二层的目标 MAC 是 DHCP 服务器　　C. 三层的目标 IP 是 DHCP 服务器的 IP　　D. 不确定二，三层的情况

参考答案：A

136. 如果客户机向 DHCP 服务器租用了 IP，租期为 4 天，那么在第 2 天时，客户机会向 DHCP 服务器发送（）数据包。

A. DHCPDiscover　　B. DHCPOffer　　C. DHCPAck　　D. DHCPRequest

参考答案：D

137. 若要创建 SOCKET 的 TCP 客户端，使用的的 SOCKET 的类型是（）

A. sock_stream　　B. socket.SOCK_DGRAM　　C. socket.SOCK_STREAM　　D. sock_dgram

参考答案：C

138. IP 报文中,固定长度部分为多少字节?

A. 10　　B. 20　　C. 30　　D. 40

参考答案：B

139. 硬件地址是固化在(　　)中的,比如 MAC 地址,用于同一链路上设备相互通信。

A. PIC　　B. NIC　　C. POWER　　D. FAN

参考答案：B

140. 网络管理希望能够有效利用 192.168.176.0/25 网段的 IP 地址现公司市场部门有 20 个主机,则最好分配下面哪个地址段给市场部(　　)?

A. 192.168.176.0/25　　B. 192.168.176.160/27　　C. 192.168.176.48/29　　D. 192.168.176.96/27

参考答案：D

141. 下列关于网桥的说法中，不正确的是（ ）。

A. 网桥工作在数据链路层　　B. 网桥可以有效地防止广播风暴　　C. 网桥可以连接数据链路层协议不同的局域网　　D. 网桥因处理接收到的数据而增加了网络延时

参考答案：B

142. 端口聚合带来的优势中不包括的是(　　)。

A. 提高链路带宽　　B. 实现流量负荷分担　　C. 提高网络的可靠性　　D. 便于复制数据进行分析

参考答案：D

143. Rstp 是从 stp 发展过来的,Rstp 把网络收敛的时间缩短到 1 秒,为此快速生成树协议定义了 2 种新增加的端口角色是(　　)。

A. 指定端口、根端口　　B. 替代端口、备份端口　　C. 转发端口、阻塞端口　　D. 阻塞端口、备份端口

参考答案：B

144. 以下关于无线局域网硬件设备特征的描述中,(　　)是错误的。

A. 无线网卡是无线局域网中最基本的硬件　　B. 无线接入点 AP 的基本功能是集合无线或者有线终端,其作用类似于有线局域网中的集线器和交换机　　C. 无线接入点可以增加更多功能,不需要无线网桥、无线路由器和无线网关　　D. 无线路由器和无线网关是具有路由功能的 AP,一般情况下它具有 NAT 功

参考答案：C

145. TCP 协议使用三次握手来建立连接。TCP 协议规定,在对发送端 SYN 确认信息中,同时捎带(　　)以减少通信的量。

A. 上一个已接收的报文编号　　B. 下一个希望接受的报文编号　　C. 对发送进程的链接请求 SYN　　D. 对发送进程的请求确认 ACK

参考答案：C

146. 哪个 vSphere 组件可用于为每台虚拟机创建实时卷影实例,以便在虚拟机出现故障时可由卷影实例取代虚拟机?

A. HighAvailability　B. FaultTolerance　C. DataProtection　D. DistributedResourcesScheduler

参考答案：B

147. 大部分 HPC 系统都使用了并行的概念,HPC 硬件可以分为 3 类Ⅲ下面那个不属于(　　)。

A. 对称多处理器ⅢSMP　B. 多核单处理器　C. 向量处理器　D. 集群

参考答案：B

148. 下面哪个是 LVS-MASTER 的用处(　　)。

A. 提供负载均衡　B. 提供 Web 服务　C. 集群的 VIP 地址　D. 共享存储

参考答案：A

149. 下列哪个不是实现虚拟服务器的 3 种方法之一(　　)。

A. 通过 NAT 实现虚拟服务器　B. 通过 IP 隧道实现虚拟服务器　C. 通过 VPN 实现虚拟服务器　D. 通过直接路由实现虚拟服务器

参考答案：C

150. 当 vSphere 管理员使用锁定模式的时候,已经登录到 ESXishell 的用户是什么状态?(　　)

A. 用户依然保持登录状态,可以运行命令,除了解除锁定模式的命令。

B. 用户依然保持登录状态,可以运行命令,包含解除锁定模式的命令。

C. 用户立即从 ESXiShell 注销。　D. 用户在 vSphere 管理员指定的时间之后注销。

参考答案：A

二、多选题

151. ssh 产生私钥和公钥的加密算法有哪些?

A. 3dsa　B. sha　C. rsa　D. dsa

参考答案：CD

152. 当使用 firewalld 实现端口转发时，需要配置的参数包括：

A. 目的地址　B. 目的端口　C. 源地址　D. 源端口

参考答案：ABD

153. 关于 linux 以下表明哪些就是恰当的?

A. linux 就是一个多任务的操作系统　B. linux 就是一个开放源码的操作系统　C. linux 就是一个类 unix 的操作系统.　D. linux 就是一个多用户的操作系统

参考答案：ABCD

154. 在 Linux 应急响应中，可以通过哪些方式加强系统的安全防护?

A. 加强入侵检测　B. 使用强密码策略　C. 更新系统补丁　D. 加强访问控制

参考答案：ABCD

155. 邮件服务器的防火墙规则中，以下哪些端口是常见的邮件服务器端口？

A. TCP/110　　B. TCP/25　　C. TCP/143　　D. TCP/80

参考答案：ABC

156. 在 Linux 系统中创建一个新的用户后，通常要为新增加的用户设置登录的密码，用户的口令涉及到两个文件：shadow 和 passwd，下面对这两个文件描述正确的是？

A. 只有 root 用户才能查看 shadow 文件的内容　　B. shadow 和 passwd 这两个文件均位于 /etc 目录下　　C. shadow 中存放的口令为密文形式，而 passwd 则是以明文的形式存放口令　　D. 任意一个用户均可以对 shadow 和 passwd 这两个文件进行操作

参考答案：AB

157. Postfix 和 Dovecot 的作用是什么？

A. 提供邮件访问和管理功能　　B. 实现用户认证和权限控制　　C. 进行反垃圾邮件过滤　　D. 处理邮件的传输和路由

参考答案：ABD

158. 以下哪些操作系统可以提供 iSCSI 目标功能？

A. Linux　　B. FreeBSD　　C. Windows Server　　D. macOS

参考答案：AC

159. DHCP 故障转移中，以下哪些步骤是确保主服务器和备用服务器之间网络连通性和防火墙设置的正确配置？

A. 配置主服务器和备用服务器的网络接口，设置正确的 IP 地址、子网掩码和默认网关。　　B. 开放主服务器和备用服务器的防火墙，允许 DHCP 协议相关的端口通过。　　C. 配置路由器或交换机，确保主服务器和备用服务器之间的互通。　　D. 确保主服务器和备用服务器连接到同一个局域网或子网。

参考答案：ABCD

160. Kerberos 可以实现以下哪些功能？

A. 数据库访问控制　　B. 电子邮件加密　　C. 单点登录（SSO）　　D. 安全的远程访问

参考答案：ACD

161. DHCP 安全性中的攻击类型包括以下哪些？

A. 未经授权的客户端获取资源的访问权限　　B. 来自恶意 DNS 服务器的资源耗尽攻击　　C. 未经授权的 DHCP 客户端向服务器发送虚假请求　　D. 未经授权的 DHCP 服务器提供虚假信息

参考答案：AD

162. 在本地的文件系统中下列哪些 linux 路径结构是无效的?

A. \usr/linux/memo　　B. //usr\linux/memo　　C. \usr\linux\memo　　D. /usr/linux/memo

参考答案：ABC

163. 以下哪些方法可以用于防止 SQL 注入攻击？

A. 使用强密码保护数据库访问　　B. 使用参数化查询　　C. 对用户输入进行充分验证和过滤　　D. 将敏感数据加密存储

参考答案：BC

164. WWW 服务需要一些关键的因素，其中（）解决了超文本内容编写的问题，（）解决了超文本传输的问题，（）解决了超文本阅读的问题，（）解决了内容定位的问题。

A. HTTP（Hypertext Transfer Protocal）　B. 浏览器（Browser）
C. HTML（Hypertext Markup Language）　D. URL（Uniform Resource Locators）

参考答案：ABCD

165. 还原数据库的备份快照的步骤包括以下哪些？

A. 启动数据库服务　B. 备份快照文件夹　C. 停止数据库服务　D. 复制快照文件夹

参考答案：ACD

166. MySQL 中，以下哪些语句可以用于条件查询？

A. SELECT　B. UPDATE　C. DELETE　D. INSERT INTO

参考答案：ABCD

167. 数据库镜像可以提高哪些方面的性能？

A. 数据传输性能　B. 数据读取性能　C. 数据写入性能　D. 数据存储性能

参考答案：BC

168. 警报监控能够帮助管理员及时采取防御措施，比如阻止被攻击者利用的 IP 地址或用户帐户。或将应用程序从网络中断开。警报监控的反常事件一般包括以下几种（）。

A. 包含已知攻击字符串的请求　　B. 请求中普通用户无法查看的数据被修改　　C. 应用反常，如收到由单独一个 IP 地址或用户发出的大量请求，表明应用程序正受到自定义攻击　　D. 交易反常，如单独一个银行账户所转入或转出的资金数量出现异常

参考答案：ABCD

169. HTTP.sys 是一个运行于 Windows 内核模式下的驱动程序，能够让任何应用程序通过它提供的接口利用 HTTP 进行通信。如编号为 CVE-2015-1635（MS15-034 ）的这个远程代码执行漏洞，攻击者只需要发送恶意的 http 请求数据包，就可能远程读取 IIS 服务器的内存数据，或使服务器系统蓝屏崩溃。这个漏洞能影响哪些版本？（ ）

A. IIS8.0　　B. IIS7.0　　C. IIS6.0　　D. IIS5.0

参考答案：AB

170. SQL Server 的用户管理可以分为以下哪几个分层实体？

A. 文件和文件组　　B. 服务器　　C. 数据库　　D. 安全对象

参考答案：BCD

171. 哪些 PHP 代表的后端网站技术可以让 Web 访问数据库。

A. JavaScript　　B. HTML　　C. ASP　　D. JSP

参考答案：CD

172. 文件包含是 PHP 的一种常见用法，主要由以下几个函数完成（ ）

当使用这 4 个函数包含一个新文件时，该文件将作为 PHP 代码执行，PHP 内核并不会在意该被包含的是什么类型。所以如果被包含的是 txt 文件、图片文件、远程 URL，也都将其作为 PHP 代码执行。如以下代

码：

```
<?php

Include($_GET[test]);

?>
```

用户可以控制 test 参数，传一个 txt 文档，txt 文档有 PHP 代码，就会执行。

A. include()　B. require()　C. include_once()　D. require_once()

参考答案：ABCD

173. Tomcat 是（ ）

A. Web 容器　B. web 中间件　C. 应用程序　D. 网站框架

参考答案：AB

174. Weblogic 的漏洞很多，主要有以下几种（ ）

A. 文件上传漏洞　B. 反序列化漏洞　C. CSRF　D. 文件包含

参考答案：AB

175. 以下哪些是数据库渗透测试中的常见目标？

A. 发现目标数据库中的漏洞和弱点　B. 提高目标数据库的可用性
C. 破坏目标数据库的数据完整性　D. 获取目标数据库中的敏感信息

参考答案：AD

176. 在 MySQL 中，删除用户时需要指定的是：

A. 登录主机/IP　　B. 用户密码　　C. 用户权限　　D. 用户名

参考答案：AD

177. 以下哪些措施可以用于防止暴力破解攻击和提高 MySQL 的安全性？

A. 启用 SSL/TLS 加密连接　　B. 定期备份和恢复数据库　　C. 使用强密码策略　　D. 限制远程访问

参考答案：ABCD

178. Struts2 曾被爆出过许多安全漏洞，业内对其命名也从 S2-001 命名到了 S2-061,也就是说前前后后一共产生了 61 个安全漏洞，其中的两个大类是（）。

A. DDOS 漏洞　　B. RCE 漏洞　　C. XML 漏洞　　D. 文件上传漏洞

参考答案：AB

179. XSS 漏洞一般分为哪几种类型？（　）

A. DOM 型 XSS　　B. 注入型 XSS　　C. 反射型 XSS　　D. 存储型 XSS

参考答案：ACD

180. SqImap 支持以下哪几种不同的注入模式？

A. 联合查询注入，可以使用 union 的情况下的注入　　B. 堆查询注入，可以同时执行多条语句的注入　　C. 基于布尔的盲注，即可以根据返回页面判断条件真假的注入　　D. 基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中

参考答案：ABCD

181. 当 Tomcat 运行在主机上，且启用了 HTTP （）请求方法（例如，将 readonly 初始化参数由默认值设置为 false），攻击者将可通过精心构造的攻击请求向服务器上传包含任意代码的 JSP 文件。之后，JSP 文件中的代码将能被服务器执行。这就造成了远程代码执行漏洞。通过该方法上传 JSP 文件时，我们看到这个应该是由（）来处理的，但是其并没有处理该请求的方法，所以会返回 404。

A. Servlet　　B. JspServlet　　C. PUT　　D. POST

参考答案：CD

182. Apache 解析漏洞的特点有以下几种（）

A. 罕见后缀，不仅 php，就连 phtml、pht、php3、php4 和 php5 都是 Apache 认可的 php 程序的文件后缀　　B. .htaccess 可以进行解析类型的修改　　C. 一般的 Apache 默认可以解析任何类型的文件　　D. 多后缀名

参考答案：ABD

183. 数据库镜像的作用是什么？

A. 提供数据压缩存储　　B. 提高数据库的可用性　　C. 提高数据库的性能　　D. 提供数据冗余备份

参考答案：BD

184. mysqldump 命令可以用于以下哪些操作？

A. 恢复 MySQL 数据库的逻辑备份　　B. 创建 MySQL 数据库的物理备份
C. 恢复 MySQL 数据库的物理备份　　D. 创建 MySQL 数据库的逻辑备份

参考答案：AD

185. 在数据库集群中，以下哪些机制可以实现数据的冗余和高可用性？

A. 负载均衡　　B. 数据复制　　C. 分片　　D. 故障切换

参考答案：BD

186. 如何配置 MySQL 的慢查询日志？

A. 将 slow_query_log 设置为 0　　B. 将 slow_query_log 设置为 1　　C. 设置 slow_query_log_file 为慢查询日志文件的路径和文件名　　D. 将 long_query_time 设置为慢查询的执行时间阈值

参考答案：BCD

187. 在基于证书的双向认证中，以下哪些内容是需要验证的？

A. 证书的私钥　　B. 证书的有效期　　C. 证书的有效性　　D. 证书的颁发机构

参考答案：ABC

188. IPSec 可以在哪两种模式下工作？

A. 加密模式　　B. 验证模式　　C. 隧道模式　　D. 传输模式

参考答案：CD

189. 配置辅助 DNS 服务器的步骤包括以下哪些操作？

A. 在主 DNS 服务器上添加辅助 DNS 主机　　B. 在辅助 DNS 服务器上添加辅助区域　　C. 在主 DNS 服务器上添加转发区域　　D. 在辅助 DNS 服务器上编辑区域传送

参考答案：AB

190. 共享文件夹的作用是什么？

A. 限制对文件夹内容的访问权限　　B. 方便文件的备份和恢复　　C. 在拥有你的帐户的所有计算机上共享文件夹内容　　D. 提供多个用户同时编辑文件的能力

参考答案：CD

191. iSCSI 的主要优势包括哪些？

A. 高带宽和低延迟　　B. 跨平台兼容性　　C. 数据安全性和身份验证　　D. 灵活性和可扩展性

参考答案：BCD

192. 基于域的限制策略的作用是什么？

A. 保护系统的安全性　　B. 保护敏感数据和资源　　C. 管理用户账户和计算机的访问权限　　D. 提高系统性能

参考答案：ABC

193. RAID 6 的特点是什么？

A. 包括分布在阵列中的驱动器上的第二个奇偶校验方案　　B. 可以继续运行，即使两个磁盘同时发生故障　　C. 写入性能通常比 RAID 5 慢　　D. 使用跨磁盘条带化和错误检查和纠正信息

参考答案：ABCD

194. 审核账户管理可以包括以下哪些事件类型？

A. 创建、更改或删除用户帐户或组。　　B. 用户帐户已重命名、禁用或启用。　　C. 设置或更改密码。　　D. 记录用户的登录和注销操作。

参考答案：ABC

195. DNSSEC 是在哪个层次上保护 DNS 查询的完整性？

A. 应用程序和 DNS 服务器之间　　B. 递归名称服务器和授权名称服务器之间　　C. DNS 服务器和互联网之间　　D. DNS 解析器和应用程序之间

参考答案：AB

196. 以下关于表单身份验证的描述，哪些是正确的？

A. 可以自定义登录页面和验证逻辑　　B. 表单身份验证是一种不安全的身份验证方式　　C. 表单身份验证适用于 Web 应用程序　　D. 用户需要通过登录页面输入凭据进行身份验证

参考答案：ACD

197. Windows 防火墙的作用是什么？

A. 防止未经授权的访问和入侵　　B. 提供实时的网络安全保护　　C. 监控和控制网络流量　　D. 保护计算机免受恶意网络活动的影响

参考答案：ABCD

198. 密码策略可以限制和控制以下哪些内容？

A. 密码的最小长度　　B. 密码的最大寿命　　C. 密码的复杂性要求　　D. 用户的登录时间限制

参考答案：ABC

199. 静态路由的缺点是（ ）。

A. 不适用于需要快速适应网络变化的网络　　B. 不适用于需要自动发现邻居路由器的网络　　C. 不适用于大型网络　　D. 不适用于复杂网络

参考答案：ACD

200. 下列哪些情况可能会触发验证码？

A. 访问频率过高　　B. 行为异常　　C. 登录　　D. 注册

参考答案：ABCD

201. RIP 协议的应用场景有哪些？

A. RIP 协议适用于小型网络。　　B. RIP 协议适用于大型网络。　　C. RIP 协议适用于复杂网络。　　D. RIP 协议适用于简单网络。

参考答案：AD

202. 在隧道模式下，ESP 协议的封装方式说法不正确是？

A. ESP 头被插入到原始 IP 头与新添加的 IP 头之间。　　B. ESP 头被插入到原始 IP 头与传输层协议头之间。　　C. ESP 头被插入到原始 IP 数据包有效载荷之前。　　D. ESP 头被插入到原始 IP 数据包有效载荷之后。

参考答案：BCD

203. 在哪些模式下，防火墙能够提供安全控制功能？

A. 透明模式　　B. 路由模式　　C. 混合模式　　D. 以上都不是

参考答案：ABC

204. SSL VPN 网关可以支持哪些协议？

A. ICMP 协议　　B. TCP/IP 协议都支持　　C. TCP 协议　　D. UDP 协议

参考答案：ACD

205. 下列哪些是网络游戏的弊处？

A. 影响学业　　B. 上瘾问题　　C. 社会问题　　D. 浪费钱财

参考答案：ABCD

206. WAF 采用了哪些技术来提高系统的处理效率、系统稳定性和安全性？

A. HTTPS 加密信息防护支持　　B. 多维细粒度防护引擎　　C. 及时权威的攻击特征库　　D. 强大灵活的策略模板

参考答案：ABCD

207. 在防火墙规则中，以下哪些规则是典型的允许流量的规则？

A. 允许所有源地址的 HTTP 流量访问目标地址的 80 端口　　B. 允许特定 IP 地址的 FTP 流量访问目标地址的 21 端口　　C. 允许所有源地址的 SSH 流量访问目标地址的 22 端口　　D. 允许特定 IP 地址的 ICMP 流量通过防火墙

参考答案：AB

208. DCNWAF 的串行模式和旁路模式有什么区别？

A. 串行模式下，WAF 故障会影响业务连通性。　　B. 旁路模式下，WAF 故障不会影响业务连通性。　　C. 串行模式下，所有流量都经过 WAF 处理。　　D. 旁路模式下，只有部分流量经过 WAF 处理。

参考答案：ABC

209. 在传输模式下，ESP 协议的封装方式说法不正确的是?

A. ESP 头被插入到 IP 头与传输层协议头之间。　　B. ESP 头被插入到 IP 头与 IP 数据包有效载荷之间。　　C. ESP 头被插入到 IP 数据包有效载荷之前。　　D. ESP 头被插入到 IP 数据包有效载荷之后。

参考答案：BCD

210. WEB 认证支持哪些浏览器和平台?

A. Google Chrome　　B. Mozilla Firefox　　C. Windows 10　　D. Android

参考答案：ABCD

211. ARP 泛洪攻击，可以有以下（）场景

A. 通过不断发送伪造 ARP 广播数据，使得网线一直工作，发热后，导致数据通信中断　　B. 通过不断发送伪造的 ARP 广播数据报使得交换机拼于处理广播数据报耗尽网络带宽。　　C. 令局域网内部的主机或网关找不到正确的通信对象，使得正常通信被阻断　　D. 用虚假的地址信息占满主机的 ARP 高速缓存空间，造成主机无法创建缓存表项，无法正常通信。

参考答案：BCD

212. 下列哪些函数可以发送 ARP 的数据包（）

A. srp　　B. send　　C. sendp　　D. sr

参考答案：AC

213. 若有函数 def abc(d,e=2,*t,**dict),程序下列那一传参是可以的()

A. abc(1,3,x=2,y=2)　　B. abc(1,(1,2),x=1)　　C. abc(1,2,3,4,5,6)　　D. abc（1，2，3，x=2,y=2）

参考答案：ABCD

214. 现在有一段使用 Socket 模块编写的程序，实现 TCP 扫描。将按顺序将挖空的地方补全

s_port = socket.socket(socket.AF_INET, socket.{F1}) #建立 socket 对象

result = s_port.connect_ex({F2}) #建立连接

if {F3}:

 print("This port %d is open!" % port)

else:

 {F4}

s_port.close()

F1,F2,F3 可能提代码是：()

A. print("This port %d is open!" % port)　　B. SOCK_STREAM　　C. (dst_ip, port)　　D. not result

参考答案：BCD

215. 下列那些是 TCP 的标志位

A. FIN　　B. RST　　C. SYN　　D. ACK

参考答案：ABCD

216. 如果局域网内存在 DHCP 攻击，会有（）现象

A. 客户机可能分配不到 IP 地址　　B. 客户机可能无法正常通信。
C. 客户机的数据可能被监听　　D. 没有什么关系，还是可以使用 IP 地址。

参考答案：ABC

217. RIP 协议的更新原则是

A. 对于本路由表中已有的路由项，当该路由项的下一跳是该邻居路由器时，不论度量值将增大或是减少，都更新该路由项　　B. 路由表中的每一路由项都对应了一个老化定时器，当路由项在 180 秒内没有任何更新时，定时器超时，该路由项的度量值变为不可达　　C. 当该路由项的下一跳不是该邻居路由器时，如果度量值将减少，则更新该路由项　　D. 对于本路由表中不存在的路由项，如果度量值小于 16，则在路由表中增加该路由项

参考答案：ABCD

218. 802.1Q Tag 主要分为两个部分：（　）

A. TPID　　B. TCI　　C. VID　　D. PRI

参考答案：AB

219. 在字符串格式化中,格式字符串中可以使用代表要输出的数据。

A. %d　　B. %s　　C. %n　　D. %f

参考答案：ABD

220. 下列那些方法是FTP对象初始化时调用一次即可，无需重复调用（ ）

A. FTP.storbinary( )　　B. FTP.login( )　　C. FTP.cwd(pathname)　　D. FTP.retrbinary( )

参考答案：AB

221. 信息收集获得信息的方法可以分成（　）

A. 间接扫描　　B. 被动扫描　　C. 直接扫描　　D. 主动扫描

参考答案：BC

222. 使用Socket模块编写扫描程序，以下哪些说法是正确（ ）

A. 使用Socket模块可以实现TCP扫描，也可以实现UDP扫描　　B. Socket模块可以通过connect()是不是执行成功来判断端口是不是开放
C. Socket模块，connect()和connect_ex（ ）都可以实现UDP端口扫描
D. Socket模块，connect()和connect_ex（ ）都可以实现TCP端口扫描

参考答案：ABD

223. 一个RIPV2协议的数据，发送请求报文，应该各层那一些参数

A. IP（dst="224.0.0.9"）　　B. UDP(sport=520,dport=520)　　C. RIP（cmd=1,version=2）　　D. RIPEntry()

参考答案：ABC

224. Socket函数中有一个参数是Family,下列那些是Family参数的选择（ ）

A. socket.AF_RAW　　B. socket.AF_UNIX　　C. socket.AF_INET　　D. socket.AF_INET6

参考答案：BCD

225. 函数传送的参数方式，可以有（ ）

A. 参数赋值和参数默认值传递　　B. 元组类型变长参数传递　　C. 字典类型变长参数传递　　D. 参数按位置一次传递

参考答案：ABCD

226. 在二层网络环境中，出现环路的问题也是比较严重的，常见的有（ ）

A. 交换机反复死机　　B. 广播风暴　　C. MAC 地址表翻滚　　D. 同一数据帧重复拷贝

参考答案：ABCD

227. Debian 的安装源，是使用那些命令进行安装软件

A. apt　　B. apt-cache　　C. aptitude　　D. apt-get

参考答案：ACD

228. DHCP 具有以下功能（ ）？

A. 保证任何 IP 地址在同一时刻只能由一台 DHCP 客户机所使用　　B. DHCP 应当可以给用户分配永久固定的 IP 地址。　　C. DHCP 应当可以同用其他方法获得 IP 地址的主机共存（如手工配置 IP 地址的主机）　　D. DHCP 服务器应当向现有的 BOOTP 客户端提供服务

参考答案：ABCD

229. 下列关于 python socket 操作叙述正确的是

A. 服务端使用 listen()开始 TCP 监听　　B. 使用 recvfrom()接收 TCP 数据　　C. 使用 getsockname()获取连接套接字的远程地址　　D. 使用 connect()初始化 TCP 服务器连接

参考答案：AD

230. 下面（）是非法的变量名

A. ID'　　B. my-name　　C. complex　　D. _address

参考答案：AD

三、判断题

231. (　　)Linux 的 3 组权限位的顺序是“属主-属组-其他”,每组中位的次序是“执行-写-读”

A. 正确　　B. 错误

参考答案：B

232. (　　)一个域名的每个组成部分不能超过 63 个字符,完整的域名全长不能超过 256 个字符

A. 正确　　B. 错误

参考答案：B

233. （）linux 没有扩展分区

A. 正确　　B. 错误

参考答案：B

234. (　　)符号链接只可以包含绝对路径,不可以包含相对路径。

A. 正确　　B. 错误

参考答案：B

235. (　　)MBR(masterBootRecorder)的硬盘分区表的大小为 512 字节。

A. 正确　　B. 错误

参考答案：B

236. (　　)Linux 文件系统的文件都按其作用分门别类的放在相关的目录中,对于外部设备,一般将其放在/bin 目录中

A. 正确　　B. 错误

参考答案：B

237. ( ) 磁盘定额的 hard 限制只有在设置了缓冲期限时才会运

A. 正确　　B. 错误

参考答案：B

238. WEB 服务器 apache 默认连接的接听端口号为 808

A. 正确　　B. 错误

参考答案：B

239. 虚拟用户是在 Samba 服务中创建的一种用户账号，与操作系统的用户账号无关。这种说法是否正确?

A. 正确　　B. 错误

参考答案：A

240. SQL Server 中的架构可以在不同的数据库中重复使用。

A. 正确　　B. 错误

参考答案：A

241. 数据库数据文件转移是指将数据库中的数据文件从一个存储设备转移到另一个存储设备的操作过程。这个说法是否正确?

A. 正确　　B. 错误

参考答案：A

242. SQL Server 中的模式所有权可以从一个用户转移到另一个用户。

A. 正确　　B. 错误

参考答案：A

243. (　　)你是一台 WindowsServer2008 计算机的系统管理员，你可以使用本地用户和组工具来管理该计算机中的组账号

A. 正确　　B. 错误

参考答案：A

244. (　　)控制面板--添加硬件:用于添加或删除计算机上的程序。上

A. 正确　　B. 错误

参考答案：B

245. (　　)GPO(组策略对象)不能链接到 ActiveDirectory 域对

A. 正确　　B. 错误

参考答案：B

246. (　　)Administrators 帐户默认情况下是禁用的。

A. 正确　　B. 错误

参考答案：B

247. (　　)父域的名字是 ACME.COM，子域的名字是 DAFFY，那么子域的 DNS 全名是 DAFFY.ACME.COM

A. 正确　　B. 错误

参考答案：A

248. 在运行框中输入“gpedit.exe”，确定后可以打开组策略编

A. 正确　　B. 错误

参考答案：B

249. (　　)在网络负载平衡群集的准备条件中，群集中的每台计算机有 2 块网卡是必须的

A. 正确　　B. 错误

参考答案：B

250. 禁用本地系统将计算机标识用于 NTLM 可以增加系统的安全性，避免本地系统滥用计算机账户的凭据进行身份验证。这个说法是否正确？

A. 正确　　B. 错误

参考答案：A

251. Windows Server Backup 是 Windows 提供的一项备份和恢复功能，可将整个磁盘卷的备份副本复制到另一个本地磁盘中。这个说法是

A. 正确　　B. 错误

参考答案：A

252. Windows 系统中的 guest 用户默认是启用状态吗？

A. 正确　　B. 错误

参考答案：B

253. WAF 无法防止跨站脚本（XSS）攻击。

A. 正确　　B. 错误

参考答案：B

254. 在基于用户的流控策略中，序号越小的规则优先级越高。

A. 正确　　B. 错误

参考答案：A

255. 上网行为的流量管理技术只能对带宽进行限制，无法根据应用、服务、用户进行带宽限制。

A. 正确　　B. 错误

参考答案：B

256. OSPF 路由协议支持多个区域，每个区域都有一个区域边界路由器。

A. 正确　　B. 错误

参考答案：A

257. WAF 通过分析 HTTP 流量来检测和阻止恶意流量。

A. 正确　　B. 错误

参考答案：A

258. SSL VPN 允许远程接入用户安全地访问企业内部网络资源。

A. 正确　　B. 错误

参考答案：A

259. DDoS 攻击是通过大规模互联网流量淹没目标服务器或其周边基础设施，以破坏目标服务器、服务或网络正常流量的恶意行为。

A. 正确　　B. 错误

参考答案：A

260. IKE 是 IPSEC 的一个子协议。

A. 正确　　B. 错误

参考答案：B

261. 动态路由协议的优点是可以减少人工干预，提高网络的可靠性和可扩展性。

A. 正确　　B. 错误

参考答案：A

262. 使用 WEB 网站扫描工具可以发现网站存在的漏洞、恶意代码等问题，但无法获取网站的 URL 结构和页面内容。

A. 正确　　B. 错误

参考答案：B

263. NAT 技术是为了解决 IPv4 地址短缺而开发的技术。

A. 正确　　B. 错误

参考答案：A

264. URL 是 URI 的一种。

A. 正确　　B. 错误

参考答案：A

265. 在企业中，IM、P2P、流媒体、网络游戏和股票软件等应用的管控是非常必要的。

A. 正确　　B. 错误

参考答案：A

266. 在 DCBC-netlog 中，所有的文件类型条目是按照顺序从后往前匹配。

A. 正确　　B. 错误

参考答案：B

267. 通过使用 SSH，不可以把所有传输的数据进行加密。

A. 正确　　B. 错误

参考答案：B

268. 要通过互联网进行通信，至少需要一对套接字，一个运行于客户机端，另一个运行于服务器端。

A. 正确　　B. 错误

参考答案：A

269. SFD 来表示一帧的开始，后面紧跟着传输的就是以太网的数据。

A. 正确　　B. 错误

参考答案：B

270. 被动扫描主要指的是在目标无法察觉的情况下进行的信息收集

A. 正确　　B. 错误

参考答案：A

271. 通常使服务器连续运行的办法是小心地设计一个无限循环。

A. 正确　　B. 错误

参考答案：A

272. VLAN 的链路类型有 ACCESS 链路和 TRUNK 链路

A. 正确　　B. 错误

参考答案：A

273. 在 FTP 的使用当中，下载"（Download）就是将文件从自己的计算机中拷贝至远程主机上。

A. 正确　　B. 错误

参考答案：B

274. 包的作用是包含多个模块，但包的本质依然是模块，因此包也可用于包含包。

A. 正确　　B. 错误

参考答案：A

275. 当DHCP客户机第一次登录网络的时候，它会通过UDP 67端口向网络上发出一个DHCPDISCOVER数据包

A. 正确　　B. 错误

参考答案：A

276. 在scapy中产生ip层的是IP类（）

A. 正确　　B. 错误

参考答案：A

277. 平时使用的ping命令，就是使用icmp协议，它构造的icmp类型字段为0，代码字段为8

A. 正确　　B. 错误

参考答案：B

278. .com，.mil,.cn这些是都是一级域名

A. 正确　　B. 错误

参考答案：A

279. Socket本身并不是协议，而是一个调用接口（API），这种说法是错的

A. 正确　　B. 错误

参考答案：B

280. 在Python中，若要将数据保存在文本文件中，需要复制输出的内容，在粘贴到一个文件里即可。

A. 正确　　B. 错误

参考答案：B

281. ARP 协议工作在 OSI 模块第一层。（

A. 正确　　B. 错误

参考答案：B

282. scapy 模块是用 TCP 类来构造 TCP 层

A. 正确　　B. 错误

参考答案：A

283. Pip 是对 easy_install 的取代，提供了和 easy_install 相同的查找包的功能，因此可以使用 easy_install 安装的包也同样可以使用 pip 进行安装

A. 正确　　B. 错误

参考答案：A

284. 国内没有 Debian 系统镜像站点，所以安装 Linux 的软件包，只能通过国外站点

A. 正确　　B. 错误

参考答案：B

285. VLAN 是 12 位的，所以用户可以取值的 VLANID 是在 0-4096

A. 正确　　B. 错误

参考答案：B

286. Python 使用/作为转义符的开始符号。

A. 正确　　B. 错误

参考答案：B

287. (　　)数据在传输过程中,出现差错最主要原因是随机错。

A. 正确　　B. 错误

参考答案：B

288. (　　)交换机都使用 IP 地址进行交换的。

A. 正确　　B. 错误

参考答案：B

289. (　　)通过 ADSL 访问 Internet,在用户端通过分离器和 ADSLModem 连接 PC 机,在 ISP 端通过 DSLAM 设备连接因特网

A. 正确　　B. 错误

参考答案：A

290. (　　)IP 协议首部的源地址和目的地址字段存放的是源主机和目的主机的物理地址地址

A. 正确　　B. 错误

参考答案：B

291. (　　)为了进行差错控制,必须对传送的数据帧进行校验。在局域网中广泛使用的校验方法是循环冗余校验

A. 正确　　B. 错误

参考答案：A

292. (　　)TCP 只支持流量控制,不支持拥塞控制。

A. 正确　　B. 错误

参考答案：B

293. (　　)假设用户请求由某些文本和两幅图片组成的 WEB 页面,对于这个页面,客户机将发送一个请求报文及接收三个响应报文

A. 正确　　B. 错误

参考答案：B

294. (　　)ISO 划分网络层次的基本原则是:不同的结点都有相同的层次;不同结点的相同层次可以有不同的功能

A. 正确　　B. 错误

参考答案：B

295. (　　)MPLS 支持各种网络层协议,带有 MPLS 标记的分组必须封装在 PPP 帧中传送

A. 正确　　B. 错误

参考答案：B

296. RAID　　10 需要四个以上磁盘才能组成该类型的磁盘阵列。

A. 正确　　B. 错误

参考答案：B

297. 存储虚拟化是将存储网络中的各个分散且异构的存储设备按照一定的策略，映射成一个统一的连续编址的逻辑存储空间，称为虚拟存储池

A. 正确　　B. 错误

参考答案：A

298. 块存储服务（cinder）为实例提供块存储。存储的分配和消耗是由块存储驱动器，或者多后端配置的驱动器决定的。如 NTFS、NFS、Cep

A. 正确　　B. 错误

参考答案：B

299. 负载均衡是计算机网络的功能之一，是指工作被均匀的分配给网络上的各台计算机系

A. 正确　　B. 错误

参考答案：A

300. 云平台中可以直接删除原有卷。

A. 正确　　B. 错误

参考答案：B