2023年上海市高等学校信息技术水平考试试卷

四级 网络与信息安全（模拟卷）

（本试卷考试时间 150 分钟）

一、单选题（ 本大题 30 道小题 ，每小题 1 分，共 30 分），从下面题目给出的A、B、C、D四个可供选择的答案中选择一个正确答案。

1.某用户使用百度搜索引擎搜索到某大学招聘网站的后台访问链接，点击访问该链接，发现可直接进入后台，并可进行一系列后台管理操作。该招聘网站存在的漏洞属于（ ）。

A.密码泄露漏洞

B.水平授权漏洞

C.垂直越权漏洞

D.未授权访问漏洞

2.暴力破解即使用暴力穷举的方式进行大量地猜解，以下关于暴力破解正确的说法是？

A.只有在网页登录的入口才可使用暴力破解，其它如telnet、ssh等登录入口处不能使用是暴力破解的

B.猜解密码只可使用字典破解方式

C.猜解网站登录密码只需使用暴力破解方式即可，无需使用手动猜解方式

D.采用短信验证和验证码安全机制相结合的方式是很好的防御暴力破解的方法

3.查询已经安装的某个RPM软件包的信息，应该使用下面哪个rpm命令？

A.rpm -qf

B.rpm -ql

C.rpm -qa

D.rpm -qi

4.在Linxu系统中配置防火墙，使其转发除ICMP协议以外所有流量的命令是（ ）。

A.iptables -A INPUT -p icmp -j REJECT

B.iptables -A INPUT -p ! icmp -j REJECT

C.iptables -A FORWARD -p icmp -j ACCEPT

D.iptables -A FORWARD -p ! icmp -j ACCEPT

5.在企业内网与外网之间，用来检查网络请求是否合法，保护网络资源不被非法使用的技术是（ ）。

A.防病毒技术

B.差错控制技术

C.流量控制技术

D.防火墙技术

6.当防火墙位于内部网络和外部网络之间时，需要将防火墙与内部网络、外部网络以及DMZ三个区域相连的接口分别配置成不同网段的IP地址，重新规划原有的网络拓扑，这样的部署模式是（）。

A.透明模式

B.混合模式
C.交换模式
D.路由模式

7.以下防火墙的哪个功能在使用时不需要在安全策略中引用？
A.URL 过滤
B.防病毒 AV
C.IPS
D.域名解析

8.关于使用上网行为管理设备，对用户身份认证时使用“IP 身份识别”或“Web 本地认证”，以下描述正确的是（ ）。
A.Web 本地认证不适应于静态 IP 环境
B.IP 本地认证适应于动态 IP 环境
C.IP 身份识别不适应于静态 IP 环境
D.Web 本地认证适应于动态 IP 环境

9.基于传统的“五元组”来制定策略的方式在当今的网络环境中往往不再有效，关于造成这一现象的原因，以下说法错误的是（ ）。
A.越来越多的应用通过 SSL 或 SSH 对流量进行加密，通过端口无法识别到真实的应用
B.大量非法应用通过常用协议的端口（如 HTTP 协议的 80 端口）进行隐藏
C.随着应用的爆发式增长，非标准端口的使用率越来越多
D.越来越多新的互联网应用已不再基于 TCP/IP 架构

10.关于 SSL VPN 的本地密码认证，以下说法不正确的是？
A.密码可以设置过期策略，过期时强制修改密码
B.用户设置密码时需满足指定密码强度
C.用户可以自行修改密码
D.用户不可以自行修改密码

11.在企业内网访问控制要求较高的场景下，该企业的 SSL VPN 设备，启用了 “专线”功能，当用户接入 SSL VPN 后，类似接入了一条“专线”，那么关于 SSL VPN 的“专线”功能，说法正确的是？
A.启用 SSL 专线功能后，用户可以访问所有内网资源
B.通过 SSL 专线功能，移动用户只能访问 TCP 资源
C.通过 SSL 专线功能，在移动用户和总部之间建立一条专有的线路，以加快访问速度
D.启用 SSL 专线功能后，移动用户接入 SSL VPN 后将无法访问 Internet

12.如果目标主机禁止 ping 扫描，此时用 Nmap 扫描应当使用的参数是( )。
A.-sS
B.-sP
C.-p
D.-Pn

13.下列不属于 Metasploit 的模块的是（ ）。
A.post
B.payload
C.auxiliary
D.msf6

14.下列不属于 Burpsuite 默认模块的是（ ）。
A.Proxy
B.Intruder
C.Logger
D.BurpJS

15.MSSQL 数据库的默认端口是( )。
A.8080
B.3306
C.3389
D.1433

16.以下哪个函数不属于 MYSQL?
A.version()
B.database()
C.@@datadir
D.@@version

17.Oracle 数据库的连接符为( )。
A.单引号'
B.加号+
C.空格
D.双竖线||

18.Sqlmap 反弹 shell 的命令是?
A.--os-cmd
B.--os-shell
C.--sql-shell
D.--os-pwn

19.《中华人民共和国个人信息保护法》指出，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，（ ）。
A.包括加密处理后的信息
B.不包括加密处理后的信息
C.包括匿名化处理的信息
D.不包括匿名化处理后的信息

20.若 Alice 采用公钥密码加密给 Bob 发送的消息，则 Bob 应该选用( )对信息进行解

密。
A. Bob 的公钥
B. Alice 的公钥
C. Alice 的私钥
D. Bob 的私钥

21. 以下不属于数字签名特性的是( )。
A. 不可伪造性
B. 完整性
C. 不可篡改性
D. 保密性

22. 传输层的 UDP 协议提供的是（ ）。
A. 有连接的可靠服务
B. 有连接的不可靠服务
C. 无连接的可靠服务
D. 无连接的不可靠服务

23. 对于 IP 地址为 202.101.208.17/24 的主机来说，其网络号为（ ）。
A. 255.255.0.0
B. 255.255.255.0
C. 202.101.0.0
D. 202.101.208.0

24. L2TP 隧道在两端的 VPN 服务器之间采用（ ）来验证对方的身份。
A. SSL
B. 数字证书
C. Kerberos
D. 口令握手协议 CHAP

25. 某公司与外部供应商、客户及其他利益相关群体需要进行专用网络连接，则应使用（ ）。
A. 其他都不是
B. Access VPN
C. Intranet VPN
D. Extranet VPN

26. 如下图所示，在IPSec架构中，该数据包属于传输模式下的（）协议封装。

IP Header	ESP Header	TCP Header	data

A.其他都不是
B.AH
C.AH-ESP
D.ESP

27.文件上传漏洞能够使用户越过上传限制向服务器上传可执行的动态脚本文件，以下哪项措施对预防文件上传漏洞没有帮助？
A.使用白名单校验文件后缀
B.使用黑名单校验文件后缀
C.限制上传文件的权限
D.限制上传文件的大小

28.IIS5.X-IIS6.X 解析漏洞中，服务器默认不解析( )号后面的内容，因此能将非 asp 后缀的文件解析成 asp 文件。
A.横杠 -
B.点 .
C.逗号 ,
D.分号 ;

29.Apache 默认一个文件可以有多个以点.分割的后缀，在存在解析漏洞的 apache 版本中，如上传 test.php.owf.rar.docx 文件，则访问上传文件时最终将解析为（ ）。
A.test.docx
B.test.owf
C.test.rar
D.test.php

30.在没有图形验证码限制或一次图形验证码可以多次重复使用的 web 应用中，可以破解此 web 应用的用户帐号和密码的做法有（ ）。
A.使用密码字典对已知用户帐号进行暴力破解
B.用一个通用密码对不同用户帐号（用户名字典）进行暴力破解
C.使用用户名字典和密码字典组合进行暴力破解
D.使用工具软件对特定的图形验证码进行暴力破解

二、多选题（ 本大题 10 道小题 ，每小题 2 分，共 20 分），从下面题目给出的 A、B、C、D 四个可供选择的答案中选择所有正确答案。

1.在没有图形验证码限制或一次图形验证码可以多次重复使用的 web 应用中，可以破解此 web 应用的用户帐号和密码的做法有（ ）。
A.使用密码字典对已知用户帐号进行暴力破解
B.用一个通用密码对不同用户帐号（用户名字典）进行暴力破解
C.使用用户名字典和密码字典组合进行暴力破解
D.使用工具软件对特定的图形验证码进行暴力破解

2.部署在互联网外部边界的防火墙不能防止以下哪些攻击行为？
A.内部网络用户的攻击
B.通过 U 盘传送已感染病毒的软件和文件
C.来自外部非授权用户的非法访问
D.内部员工的违规操作

3.某客户希望使用上网行为管理设备保障视频会议带宽，在此场景下说法正确的是？
A.如果客户的视频会议系统使用私有协议，上网行为管理设备无法识别此私有协议，则无法满足客户需求
B.可以通过自定义协议方式，添加客户的视频会议系统协议，完成自定义协议的带宽保障
C.可以将内部的视频会议服务器当作内网用户，针对该用户做所有应用的带宽保障
D.可以通过上网行为管理设备的应用协议库，针对网络会议协议做带宽保障

4.SSL VPN 设备可以校验用户的硬件特征码，防止非法登录，关于硬件特征码，说法正确的是？
A.一个终端设备只有一个硬件特征码
B.多个用户可以对应一个硬件特征码
C.一个用户可以对应多个硬件特征码
D.硬件特征码根据时间变化会自动改变

5.下列哪些工具可以进行漏洞扫描？
A.Nmap
B.Sqlmap
C.Nessus
D.Metesploit

6.下列哪些属于防御 sql 注入的正确措施？
A.数据有效性校验
B.使用存储过程
C.不回显错误信息
D.后缀校验

7.《中华人民共和国网络安全法》是为( ) 而制定。
A.保障网络安全
B.维护网络空间主权和国家安全、社会公共利益
C.保护公民、法人和其他组织的合法权益
D.促进经济社会信息化健康发展

8.经典密码学包括( )。
A.密码编码学
B.密码分析学
C.网络攻防
D.量子密码

9.某公司员工小王在出差过程中，需要远程接入公司内网的财务系统，管理员为了防止未授权访问，可以使用下列哪些身份验证手段？
A.TOKEN 卡
B.数字证书
C.802.1x
D.RADIUS

10.文件上传漏洞的危害主要有以下哪些方面？
A.上传 webshell 脚本，获取服务器权限
B.上传错误后暴露文件绝对路径地址
C.错误的文件不能被服务器识别，界面给出拒绝上传的提示
D.上传的文件解析错误，直接显示上传文件源码

三、操作题

实操题请在文件"C:\KS\网信安答题纸.docx"中作答！

实操题一的代码在"C:\素材\网信安代码.rar"文件中！

实操题一

在 2022 年的“俄乌战争”中，网络安全的攻击作为战略化武器多次出现群众的视野中，如 DDOS 攻击、针对关键信息基础设施的 APT 攻击、针对政府官员的隐私泄漏等。在复杂的国际形势和网络环境中，网络空间作为第五大空间，其安全性在国家安全以及经济民生中的的重要性不言而喻。2017 年至今，我国陆续颁发了网络安全法、数据安全法、个人信息保护法、关键信息基础设备保护条例等多项法律法规，形成了一套初步完善的网络空间安全治理的顶层框架。

同时，我国也在不断加强关键信息基础设施的信息安全防护建设的力度，并多次下文对信息安全等级保护建设进行指导。保障在复杂安全形势下建立一个立体的、基于全局的、科学的、完善的网络安全体系。

在当下的众多安全事件中，WEB 系统安全往往是网络安全研究的重点对象。著名的 OWASP TOP 10 列出了 WEB 系统面临十大安全风险，如未授权访问、管理员配置问题、输入验证问题、逻辑漏洞等。

现在某企业管理员接到反馈，该企业的 WEB 网站出现异常，疑似被黑客入侵。请你帮助管理员，解决下面的一些问题并作答。

请帮助管理员解决以下问题:

一、该网络管理员已表明他们系统使用了 php+mysql 的环境，怀疑系统中被植入了一句话木马，但是又不知道哪个文件是一句话木马文件。请你帮忙写一个 PHP 的一句话木马代码，便于管理员分析查找。(5 分)

二、请写出在 WEB 系统中找到一句话木马的常规操作思路。(5 分)

三、黑客是如何将一句话木马植入 WEB 系统中的？请列举三种常见的方式。(5 分)

四、该网站管理员使用代码审计工具，对网站源代码进行扫描，发现某页面有漏洞。该页面的代码如下，请帮助管理员找出该代码中一个明显的漏洞，并简要描述该漏洞的成因。

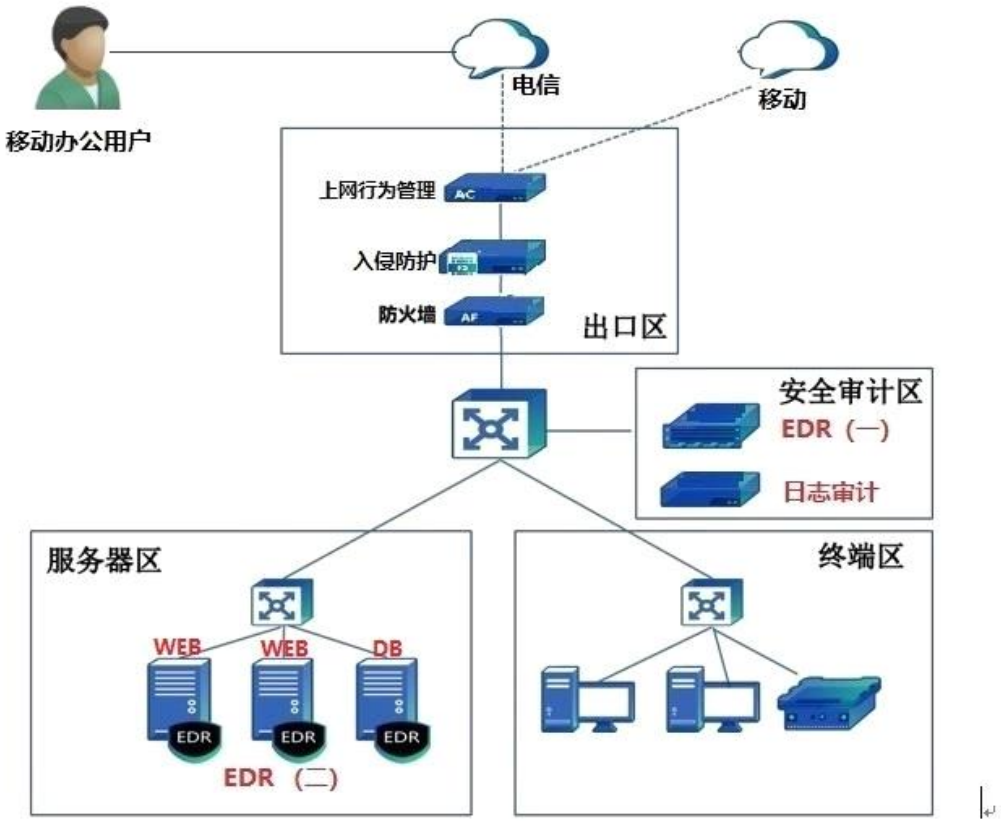
```php
/**
 * 获取文章详情
 * @param  $id
 */
function getArticleInfo($id=0){
    global $db;
    if($id==0){
        if(empty($_GET['id'])){
            return false;
        }else{
            $id = $_GET['id'];
        }
    }
    return $db->getOneRow("select * from cms_article where id=".$id);
}
```

五、你通过对网站的访问日志分析，发现网站后台管理员密码发生了泄露。 请你列举出在渗透测试过程中，获取网站后台管理员权限的一些思路。(5 分)

实操题二

随着 5G 技术的高速发展、网络带宽的显著增长、物联网新技术以及大数据技术的应用，远程办公及移动化事务处理已逐渐普及。在新的办公模式和交互模式中，企业的网络安全有了新需求与新挑战。当今网络环境中的实体算力与通信端的个体差异性远超过去，导致了网络信息安全管理难度提升，集防御（P）、检测（D）、响应（R）于一体的 PDR 闭环安全模型已经得到了广泛应用。

在此基础上，如何设计企业网络安全拓扑，使其安全能力显著提升，为企业构建以技术、管理和运营三大安全体系为目标的可运营网络安全体系架构，从而让企业具备安全可视、持续检测、协同防御的能力，值得让安全从业者思考。以某医疗企业构建的小型网络拓扑为例（下图），回答以下问题。



一、 终端检测响应平台（EDR）是的一套终端安全解决方案，方案由轻量级的客户端安全软件和服务端的管理平台软件共同组成。请从图中判断 EDR（一）和 EDR（二）哪个是服务端，哪个是客户端？（2 分）为什么？（3 分）

二、 该拓扑图中有什么设备部署问题？（2 分）你有什么好的建议？（3 分）

三、 一条完整的日志包含哪些要素？（2 分）日志审计设备应当提供哪些功能？（3 分）

四、 如果移动办公用户有安全访问内网的需求，则需要部署什么设备？（3 分）如果要加强用户使用该设备的身份验证管理，我们可以在该设备上使用什么验证技术？（2 分）

五、 假设攻击者入侵 WEB 服务器后，通过 WEB 服务器获取了同一网段的数据库（DB）服务器权限，请问攻击者获取该权限的方式有哪些？（3 分）要如何避免类似的风险？（2 分）