睢宁县2022年网络安全知识技能大赛

单位名称	_____
计算机号	_____
手机号码	_____

1.网络防御技术，是指为了确保网络系统的抗攻击能力，保证信息的机密性、完整性、可用性、可靠性和不可否认性而采取的一系列安全技术，下列哪项技术用于对计算机或用户的身份进行鉴别与认证 [单选题]*

A、防火墙技术

B、访问控制技术

C、加密技术

D、身份认证技术(正确答案)

2.下列选项哪个不是Activit启动的方法 [单选题]*

A、startActivity

B、goToActivity(正确答案)

C、startActivityForResult

D、startActivityFromChild

3. FINS协议通用开放端口是 [单选题]*

A、2405

B、20000

C、2404

D、9600(正确答案)

4. VPN通常用于建立（ ）之间的安全通道 [单选题]*

A、总部与分支机构、与客户伙伴、与移动办公用户(正确答案)

B、客户与客户、与合作伙伴、与远程用户

C、总部与分支机构、与外部网站、与移动办公用户

D、不确定

5.下列哪个攻击不在网络层？ [单选题]*

A、IP欺骗

B、内网嗅探

C、Smurf攻击

D、SQL 注入(正确答案)

6.未来防御网络监听，最常用的是 [单选题]*

A、采用物理传输（非网络）

B、信息加密(正确答案)

C、无线网

D、使用专线传输

7. TLS安全协议中不包含以下哪种技术？ [单选题]*

A、认证

B、秘密分享(正确答案)

C、加密

D、密钥交换

8.风险评估的三个要素是 [单选题]*

A、政策、结构、技术

B、组织、技术、信息

C、硬件、软件、人

D、资产、威胁、脆弱性(正确答案)

9.下列关于固件的说法错误的是 [单选题]*

A、在电子系统和计算机系统中，固件一般指持久化的内存、代码和数据的结合体

B、固件是一种密码模块的可执行代码，它存储于硬件并在密码边界内，在执行期间能动态地写或修改(正确答案)

C、存储固件的硬件可以包括但不限于PROM 、EEPROM 、FLASH 、固态存储器、硬盘驱动等

D、固件的数据和代码一般是在密码产品出厂之前就写入硬件中的，而当写入固件的代码中存在恶意代码时，硬件固件攻击也将发生

10.根据网络安全法的相关规定，以下说法错误的是 [单选题]*

A、国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

B、国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

C、国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

D、国家推进网络安全社会化服务体系建设，只能由国家机构开展网络安全认证、检测和风险评估等安全服务。(正确答案)

11.入侵检测系统强大的功能可为被保护网络提供有力的网络安全保障，请问以下哪一项不属于入侵检测系统的功能 [单选题]*

A、捕捉可疑的网络活动

B、监视网络上的通信数据流

C、提供安全审计报告

D、过滤非法的数据包(正确答案)

12.以下不属于社会工程学技术的是 [单选题]*

A、个人冒充

B、直接索取

C、钓鱼技术

D、木马攻击(正确答案)

13.常用的主机漏洞扫描软件是 [单选题]*

A、nessus(正确答案)

B、awvs

C、appscan

D、office

14.下面哪一个工具可以用来破解 windows 系统用户口令 [单选题]*

A、Cain(正确答案)

B、Rootkit

C、Icesword

D、Trinoo

15.什么样的攻击将恶意代码嵌入到文档或电子表格中。 [单选题]*

A、逻辑炸弹

B、Rootkit

C、特洛伊木马

D、宏病毒(正确答案)

16.英国著名哲学家弗兰西斯·培根曾指出：“知识的力量不仅取决于自身价值的大小，更取决于它是否被传播以及被传播的深度和广度。”这是信息的（） [单选题]*

A、共享性

B、可转换性

C、时效性

D、可传递性(正确答案)

17.（）可以把文件恢复过程简单化 [单选题]*

A、差分备份(正确答案)

B、全备份

C、余量备份

D、增量备份

18.证书校验过程中必须检查 [单选题]*

A、有效期、CA

B、有效期、域名

C、有效期、公钥、域名

D、有效期、颁发者、域名(正确答案)

19.入侵检测系统可以分为（）和基于网络数据包分析两种基本方式 [单选题]*

A、基于主机分析(正确答案)

B、基于操作系统分析

C、基于数据库分析

D、基于用户分析

20.服务商发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，应当（）。 单选题]*

A、继续传输

B、停止传输(正确答案)

C、删除日志

D、删除浏览记录

21.以下应用于工控网络边界的安全产品有 单选题]*

A、工控主机卫士

B、工控防火墙系统(正确答案)

C、工控漏洞挖掘系统

D、工控基线配置核查系统

22. Linux下常见的反调试方法是 单选题]*

A、检测 c 盘大小

B、检测子进程调用

C、检测 ptrace(正确答案)

D、检测权限

23.当用户输入的数据被当作是查询语句的一部分执行时，会产生哪种漏洞 单选题]*

A、SQL 注入(正确答案)

B、信息泄露

C、跨站脚本攻击

D、DDOS

24.以下哪一项是 DOS 攻击的一个实例？ 单选题]*

A、SQL 注入

B、IP 地址欺骗

C、Smurf 攻击(正确答案)

D、字典破解

25.网络攻击方式多种多样，从单一方式向多方位、多手段、多方法结合化发展。（）是指攻击者在非授权的情况下，对用户的信息进行修改，如修改电子交易的金额。 单选题]*

A、信息泄漏攻击

B、完整性破坏攻击(正确答案)

C、拒绝服务攻击

D、非法使用攻击

26.计算机安全的核心元素是（）。 单选题]*

A、访问控制(正确答案)

B、隐私保护

C、资源清理

D、防御攻击

27.（）是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序 单选题]*

A、计算机病毒

B、蠕虫(正确答案)

C、特洛伊木马

D、僵尸网络

28.基于源的过滤技术通过内容的来源进行过滤，以下属于基于源的过滤技术的有（） 单选题]*

A、IP包过滤(正确答案)

B、内容分级审查

C、关键字过滤

D、启发式内容过滤

29.在短时间内向网络中的某台服务器发送大量的无效链接请求，导致合法用户暂时无法访问服务器的攻击行为是破坏了（） 单选题]*

A、保密性

B、完整性

C、可用性(正确答案)

D、可控性

30.以下属于非对称加密技术的是_____。 单选题]*

A、RSA (正确答案)

B、DES

C、AES

D、古典密码

31. 2018年《工业互联网安全框架》中指出（ ）是确保落实工业互联网信息安全管理，支撑工业互联网系统与服务持续运行的保障。 [单选题]*

A、应用安全

B、数据安全

C、检测感知

D、处置恢复(正确答案)

32.以下不属于网络安全五大要素的是？ [单选题]*

A、机密性

B、完整性

C、完备性(正确答案)

D、可控性

33.下面哪一种攻击方式最常用于破解口令？ [单选题]*

A、哄骗（spoofing）

B、字典攻击（dictionary attack）(正确答案)

C、拒绝服务（DoS）

D、WinNuk

34.计算机病毒一般由三部分组成，以下哪个不属于三个组成部分？ [单选题]*

A、引导模块

B、传输模块(正确答案)

C、传染模块

D、干扰或破坏模块

35.以下属于网络端口扫描技术的是？ [单选题]*

A、源码扫描

B、半连接扫描(正确答案)

C、插件扫描

D、特征匹配扫描

36.下列哪个部署不属于僵尸网络的组成部分？ [单选题]*

A、ISP(正确答案)

B、命令控制中心

C、僵尸程序

D、僵尸计算机

37.在电子取证初查过程中收集、提取的电子数据，以及下列哪类数据，可以作为证据使用 [单选题]*

A、通过移动设备提取的电子数据

B、通过智能家居提取的电子数据

C、通过网络在线提取的电子数据(正确答案)

D、通过服务器提取的电子数据

38. 2017年（）病毒利用永恒之蓝漏洞进行传播，波及了150多个国家和30多万用户 [单选题]*

A、熊猫烧香

B、WannaCry(正确答案)

C、2345联盟

D、Petya

39.安全员在渗透某具备mysql数据库的网站时，发现只有一个80端口开放，下列原因不可能的是？ [单选题]*

A、更改了数据库端口，没有扫出来

B、站库分离

C、3306端口不对外开放

D、数据库内没有数据(正确答案)

40.黑客搭线窃听属于哪一类风险？ [单选题]*

A、信息存储安全

B、信息传输安全(正确答案)

C、信息访问安全

D、以上都不正确

41. Linux中以下哪条命令可以显示出最近执行过的命令？ [单选题]*

A、history(正确答案)

B、log

C、date

D、cmd

42.前渗透测试流程一般分为信息收集、（）、漏洞利用、报告。 [单选题]*

A、漏洞扫描

B、漏洞分析(正确答案)

C、DDOS　攻击

D、查询数据库

43.某公司网站被黑客入侵，网站程序被删。已知服务器为 Windows 系统,管理员登录服务器查看情况,发现系统中多了几个可疑账户。经过初步分析，可以确定这些账户为黑客创建，通过分析以下哪个日志可以确定黑客是否使用这些账户登录过系统？ [单选题]*

A、对 Web 日志进行排查

B、通过事件查看器对系统事件进行排查

C、通过事件查看器对安全事件进行排查(正确答案)

D、通过事件查看器对应用程序事件进行排查

44.按照《互联网电子公告服务管理规定》，任何人不得在互联网上的电子布告牌（BBS ）、电子白板、电子论坛、（　）、留言板等电子公告服务系统中发布淫秽、色情、赌博、暴力、恐怖等违法有害信息。 [单选题]*

A、电子邮件

B、网站

C、网络聊天室(正确答案)

D、个人文件

45.有关《中华人民共和国数据安全法》的说法错误的是？ [单选题]*

A、国家支持数据开发利用和数据安全技术研究。

B、数据安全法就是要求数据各自保存，不交流(正确答案)

C、国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数