网络安全技术　复习题

第一套样题

一、单项选择题（本题共 20 小题，每小题 2 分，共 40 分。请在给出的选项中，选出最符合题目要求的一项。）

1.没有网络安全就没有_____，就没有_____，广大人民群众利益也难以得到保障。

A、国家发展、社会进步　　B、国家安全、经济社会稳定运行

C、社会稳定运行、经济繁荣　　D、社会安全、国家稳定运行

2. 网络安全的基本属性有：可用性、完整性和_____。

A、多样性　　B、复杂性　　C、保密性　　D、不可否认性

3.《中华人民共和国网络安全法》正式施行的时间是_____。

A、2017 年 6 月 1 日　　B、2016 年 11 月 7 日

C、2017 年 1 月 1 日　　D、2016 年 12 月 1 日

4. 下列哪个不是网络攻击的主要目的：

A、获取目标的重要信息和数据　　B、对目标系统进行信息篡改和数据资料删除等

C、让目标无法正常提供服务　　D、造成人员伤亡

5. 以下哪个不是常见的网络攻击手段：

A、端口和漏洞扫描　　B、破坏供电系统造成服务器停电

C、网络窃听　　D、使用 MS17-010 漏洞获取服务器权限

6. 网络嗅探器 (Network Sniffer) 是一种常用的网络管理工具，也常常被攻击者利用来进行信息获取。以下哪个工具可以进行网络嗅探：

A、fscan　　B、hydra　　C、snort　　D、metasploit

7.以下哪个不是常见的恶意代码：

A、病毒　　B、木马　　C、蠕虫　　D、细菌

8.关于勒索软件，以下哪个说明是错误的：

A、勒索软件是一种恶意软件，传播范围广，危害大。

B、勒索软件通过加密受害者文件并试图通过威胁勒索获利。

C、解密高手可以破解勒索软件的密钥，从而恢复出被加密的文件

D、勒索软件通常要求使用数字货币支付赎金，这使得追踪和起诉犯罪者都十分困难

9.以下哪个不是计算机病毒的生命周期：

A、感染阶段　B、繁殖阶段　C、触发阶段　D、执行阶段

10.以下哪个不是防火墙的基本功能：

A、访问控制功能　　B、内容控制功能

C、日志功能　　D、防范钓鱼邮件功能

11.网络防御技术所包含的身份认证基本方法，不包括：

A、基于信息秘密的身份认证　　B、基于信任物体的身份认证

C、基于生物特征的身份认证　　D、基于数字签名的身份认证

12.根据 Endsley 模型，可以将态势感知划分为三个层级，不包括_____。

A、要素感知　　B、态势理解

C、安全审计　　D、态势预测

13.加密算法的功能是实现信息的_____。

A、不可否认性　　B、保密性　　C、完整性　　D、真实性

14.数字签名算法可实现信息的_____。

A、不可否认性　　B、保密性　　C、可用性　　D、真实性

15.在以下古典密码体制中，不属于置换密码的是（）：

A、移位密码　B、倒序密码　C、凯撒密码　D、转轮密码

16.以下哪种认证方式相对最安全？

A、口令认证技术　　B、人脸识别认证　　C、短信验证码认证　　D、人脸识别加短信验证码认证

17.以下哪个口令相对最为安全？

A、123456　　B、1qaz2wsx　　C、pAsswOrd　　D、p@ssword

18.某网站后台密码过于简单，被黑客破解登录了后台，并篡改了后台登录密码导致管理员无法登录，该网站遭受到了什么类型的攻击？

A. 非授权访问　　B.数据泄露　　C.网站仿冒　　D.拒绝服务

19.某单位员工收到一封仿冒的邮件，要求其立马通过邮件里的链接更新账号密码，该员工受到的是什么类型的电子邮件攻击？

A.附件病毒　　B.钓鱼邮件　　C.勒索病毒　　D.窃听攻击

20.以下哪个不属于物联网安全防护层次：

A、终端安全　B、通信网络安全　C、服务端安全　D、应用层安全

.

二、多项选择题（本题共10小题，每小题3分，共30分。请在下列每小题给出的选项中，选出符合题目要求的两个或两个以上选项。~~多选、漏选、错选均不得分。~~）

21.CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。常见的CTF竞赛模式有：

A、解题模式（Jeopardy）　　B、攻防模式（Attack-Defense）

C、渗透模式（Penatration）　　D、混合模式（Mix）

22.端口扫描工具能获取以下哪些信息：

A、端口开放信息　　B、端口提供的服务

C、主机的操作系统　　D、主机带宽信息

23.高级持续威胁（APT）的特征有：

A、它比传统攻击具有更高的定制程度和复杂程度，需要花费大量时间和资源来研究确定系统内部的漏洞

B、这类攻击持续监控目标，对目标保有长期的访问权

C、攻击目标通常是特定的重要目标，攻击方一旦得手，往往会给被攻击目标造成巨大的经济损失或政治影响，乃至于毁灭性打击

D、APT攻击可以被防病毒软件发现并查杀阻断

24.漏洞蠕虫破坏力强、传播速度快，它的传播过程一般可以分为（　）步骤。

A、扫描　B、攻击　C、复制　D、破坏

25.下列哪些步骤属于恶意代码的作用过程：

A、入侵系统　B、提升权限　C、实施隐藏　D、潜伏等待　E、执行破坏

26.按照访问控制方式不同，防火墙可以分为（）。

A、包过滤防火墙　　B、新一代防火墙
C、应用代理防火墙　　D、状态检测防火墙

27.使用 VPN 技术，可以建立安全通道，并能用 VPN 提供的安全服务，这些安全服务包括：
A、保密性服务　　B、可用性服务　　C、完整性服务　　D、认证服务

28.一般来说，认证机制由哪几个部分构成：
A、验证对象　　B、认证协议　　C、认证口令　　D、鉴别实体

29.电子邮件面临的主要安全威胁有哪些：
A、钓鱼邮件　B、勒索病毒　　C、拒绝服务　D、恶意链接

30.区块链技术主要有哪些特点：
A、去中心化　B、不可篡改　C、共识　D、匿名性

四、判断题(本题共 15 小题，每小题 2 分，共 30 分。以下叙述中，你认为正确的打“√”，错误的打“×”。)

31.我国网络安全领域的基础性法律《中华人民共和国网络安全法》正式施行，对保护个人信息、治理网络诈骗、保护关键信息基础设施、网络实名制等方面作出明确规定，成为我国网络空间法治化建设的重要里程碑。
（　　）

32.网络社会的形成与发展为现实社会中的违法犯罪分子提供了一个新的违法犯罪领域，但其社会危害性不及现实社会中的违法犯罪。
（　　）

33.MITRE 公司提出的网络攻击矩阵模型，它是一个站在防守者的视角来描述攻击中各阶段用到的技术的模型。
（　　）

34.口令是最常用的资源访问控制机制，也是最容易被突破的。
（　　）

35.受感染机器间是否能够协同工作是区分僵尸网络和其他恶意软件的重要特征。
（　　）

36.按照网络蠕虫的传播途径和攻击性，可以分为传统蠕虫、邮件蠕虫和漏洞蠕虫。其中漏洞蠕虫破坏力强、传播速度快。
（　　）

37.网络隔离技术总体上可以分为物理隔离及逻辑隔离两类方法。

（　　）

38.网络防御技术所包含的访问控制技术内容认证包括负载均衡、认证、控制策略实现等几部分。

（　　）

39.迪菲（Diffie）和赫尔曼（Hellman）提出的公钥密码系统是密码学历史上的一次革命。

（　　）

40.在 DES 加密过程中，S 盒对加密的强度没有影响。

（　　）

41.单点登录是指用户访问不同系统时，只需要进行一次身份认证，就可以根据这次认证身份访问授权资源

（　　）

42.认证是一个实体向另外一个实体证明其所声称的能力的过程。

（　　）

43.网站假冒是指攻击者通过网站域名欺骗、网站域名劫持、中间人等技术手段，诱骗网站用户访问以获取敏感信息或提供恶意服务。

（　　）

44.Web 应用防火墙是一种用于保护 Web 服务器和 Web 应用的网络安全机制。其技术原理是根据预先定义的过滤规则和安全防护规则，对所有访问 Web 服务器的 HTTP 请求和服务器响应，进行 HTTP 协议和内容过滤，进而对 Web 服务器和 Web 应用提供安全防护功能。

（　　）

45.移动应用安全和传统的 Web 安全面临的问题是一样的，可以完全借鉴，不需要专门为移动应用单独考虑安全问题。

（　　）

第一套样题

参考答案及评分标准

一、单项选择题（本题共×小题，每小题×分，共×分。请在给出的选项中，选出最符合题目要求的一项。）

BCADB　CDCAD　DCBAB　DCABD

二、多项选择题（本题共×小题，每小题×分，共×分。请在下列每小题给出的选项中，选出符合题目要求的两个或两个以上选项。多选、漏选、错选均不得分。）

21、ABD

22、ABC

23、ABC

24、ABC

25、ABCDE

26、ACD

27、ACD

28、ABD

29、ABD

30、ABC

四、判断题(本题共×小题，每小题×分，共×分。以下叙述中，你认为正确的打“√”，错误的打“×”。)

31．√　32．×　33．×　34．√　35．√

36．√　37．√　38．×　39．√　40．×

41．√　42．×　43．√　44．√　45．×

第二套样题

一、单项选择题（本题共 20 小题，每小题 2 分，共 40 分。请在给出的选项中，选出最符合题目要求的一项。）

1. 没有网络安全就没有_____，就没有_____，广大人民群众利益也难以得到保障。

A、国家安全、网络空间的合法权益　　B、国家安全、国家政治安全

C、社会稳定运行、国家繁荣发展　　D、国家安全、经济社会稳定运行

2. 网络安全的基本属性不包括：

A、可用性　　B、完整性　　C、保密性　　D、不可抵赖性

3. 《中华人民共和国网络安全法》正式施行的时间是：

A、2021 年 11 月 1 日　　B、2020 年 9 月 1 日

C、2017 年 1 月 1 日　　D、2018 年 12 月 1 日

4. 网络扫描是信息收集的重要手段。通过扫描可以发现存活主机、开放端口，进而发现其运行的服务、操作系统等信息。以下哪个工具不属于网络扫描工具：

A、nmap　　B、zmap

C、ipconfig　　D、masscan

5. SQL 注入是一种非常常见的数据库攻击手段，SQL 注入漏洞也是最普遍的漏洞之一。以下哪个工具是 SQL 注入常用的工具：

A、SQLMap　　B、PostgresSQL

C、SQLite　　D、wireshark

6. 以下哪个是常见的恶意代码类型：

A、PoC　B、木马　C、漏洞信息　D、IoC

7. 关于勒索软件，以下哪个说法是正确的：

A、勒索软件是一种威胁较低的恶意软件，传播范围和造成的危害都有限

B、勒索软件通过加密受害者的文件并试图通过威胁勒索获利

C、遭受勒索软件后支付赎金就可以收到密钥，从而恢复被加密的文件

D、勒索软件使用数字货币支付赎金，使得追踪和起诉犯罪者比较容易

8. 以下哪一种是防止系统不受恶意代码威胁的良好习惯：

A、学习安全知识、及时更新系统补丁，以及一个好的防毒程序

B、来历不明的 U 盘要先插到个人电脑上杀毒后使用

C、安全补丁攒到一定数量再一起安装，节省系统资源
D、系统的管理员密码保存到桌面上防止丢失

9. 以下哪个不是计算机病毒的类别：
A、朊病毒　　B、宏病毒　　C、文件型病毒　　D、电子邮件病毒

10. 以下哪项属于防火墙的基本功能：
A、多租户管理功能　　B、镜像备份功能
C、内网穿透功能　　D、访问控制功能

11. 网络防御技术所包含的身份认证基本方法，不包括：
A、基于信息秘密的身份认证　　B、基于信任物体的身份认证
C、基于生物特征的身份认证　　D、基于签名证书的身份认证

12. 根据 Endsley 模型，可以将态势感知划分为三个层级，不包括：
A、要素感知　　B、态势理解　　C、事件审计　　D、态势预测

13. 加密算法的功能是实现信息的：
A、不可否认性　　B、可控性　　C、保密性　　D、真实性

14. 数字签名算法可实现信息的：
A、不可否认性　　B、可控性　　C、保密性　　D、真实性

15. 在以下古典密码体制中，属于置换密码的是：
A、轮换密码　　B、逆序密码　　C、单表密码　　D、周期置换密码

16. 以下哪种加密算法相对最安全？
A、AES　　B、RSA
C、DES　　D、Blowfish

17. 以下哪个口令相对最为安全？
A、19990101　　B、78g@tw23.Y　　C、QWERTY　　D、password123

18. 以下哪种是常见的网站拒绝服务攻击技术？
A、HTTP Flood　　B、SQL 注入
C、目录扫描　　D、XSS 攻击

19. 某单位员工在非官方网站下载了一个软件工具的安装包，安装完成后发现

所有个人文件都被加密无法访问，并被提示向一个数字货币钱包地址转账后获取解密方式，该员工受到的是什么类型的攻击？

A、DDoS 攻击　　B、钓鱼攻击

C、勒索攻击　　D、窃听攻击

20. 物联网网络层分为：

A、核心网和接入网　　B、骨干网和核心网

C、核心网和边缘网　　D、骨干网和边缘网

二、多项选择题（本题共 10 小题，每小题 3 分，共 30 分。请在下列每小题给出的选项中，选出符合题目要求的两个或两个以上选项。漏选、错选和多选一个选项扣 1 分。）

21. CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。常见的 CTF 竞赛模式有：

A、解题模式（Jeopardy）　　B、攻防模式（Attack-Defense）

C、 混合模式（Mix）　　D、自由解题（Free style）

22. Metasploit 工具包括以下哪些功能：

A、漏洞探测　　B、漏洞开发

C、漏洞查询　　D、漏洞利用

23. 以下关于高级持续威胁（APT）的说法不正确的有：

A、APT 攻击由于出现频次低，因此威胁性较小

B、APT 攻击往往一次得手后，便不再对目标进行后续攻击

C、攻击目标通常是特定的重要目标，攻击方一旦得手，往往会给被攻击目标造成巨大的经济损失或政治影响，乃至于毁灭性打击

D、APT 攻击可以被专业的杀毒软件发现并查杀阻断

24. 以下属于挖矿木马的特征是：

A、CPU 或 GPU 的占用率持续 90%以上

B、系统频繁崩溃或重新启动

C、存在外连 IP 或可疑域名等异常网络活动

D、系统存在多个线程

25. 下列哪些步骤属于恶意代码的作用过程：

A、入侵系统　B、提升权限　C、实施隐藏　D、潜伏破坏

26. 按照形态的不同，防火墙可以分为：

A、软件防火墙　　B、硬件防火墙
C、专用防火墙　　D、混合防火墙

27. 以下属于零信任遵循的原则有：
A、不做任何假定 B、做最好的打算 C、随时检查一切 D、防范动态威胁

28. 以下关于认证机制说法正确的是：
A、根据认证依据所利用的时间长度分类，可分为一次性口令和持续认证
B、根据要求提供的认证凭据的类型分类，可分为单因素认证、双因素认证和多因素认证
C、按照鉴别双方角色及所依赖的外部条件分类，可分为单向认证、双向认证和多向认证
D、认证一般由标识和鉴别两部分组成

29. 以下哪些是政务网站安全防护的内容：
A、用户实名登记　　B、网页防篡改
C、网络/数据库审计　D、入侵防御和病毒防护

30. 区块链攻击者常用的一些攻击方法包括：
A、49%攻击 B、路由攻击 C、女巫攻击 D、钓鱼攻击

三、判断题(本题共 15 小题，每小题 2 分，共 30 分。以下叙述中，你认为正确的打“√”，错误的打“×”。)

31. 从广义来说，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。
（　　）

32. 网络安全最基本的 3 个属性是保密性、完整性、真实性。
（　　）

33. MITRE 公司提出的网络攻击矩阵模型，它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。
（　　）

34. 明文保存的用户口令容易被直接利用。很多系统对口令进行加密运算后再保存，加密运算通常采用单向哈希算法（Hash）。
（　　）

35. 受感染机器间是否能够协同工作是区分僵尸网络和其他恶意软件的重要特征。
（　　）

36. 文件类病毒一般会藏匿和感染硬盘的引导扇区。
（　　）

37. 网络隔离技术的主要目标是将有害的网络安全威胁隔离开，以保障数据信息无论在可信网络之内还是之外都可以安全交互。

（　　）

38. 访问控制技术指系统对用户身份及其所属的预先定义的策略，限制其使用数据资源能力的手段，通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

（　　）

39. 对称密码体制和非对称密码体制的最大区别就是发送方和接收方彼此拥有不同的公私钥。

（　　）

40. 目前，在数字签名中常用的非对称算法包括 RSA、DSA 和 AES 算法等

（　　）

41. 多因素认证技术使用多种鉴别信息进行组合，以提升认证的安全强度。根据认证机制所依赖的鉴别信息的多少，该认证通常被称为双因素认证或多因素认证。

（　　）

42. 认证是一个实体向另外一个实体证明其所声称的凭证的过程。

（　　）

43. 钓鱼邮件指恶意邮件冒充正常邮件骗取用户信任，从而非法获得密码、盗取敏感数据、诈骗资金等。

（　　）

44. 防火墙本质上就是一种能够限制网络访问的设备或软件，既可以是一个硬件的“盒子”，也可以是计算机和网络设备中的一个“软件”模块。

（　　）

45. 移动应用安全中的网络攻击都在设备层。

（　　）

第二套样题 参考答案及评分标准

一、单项选择题（本题共 20 小题，每小题 2 分，共 40 分。请在给出的选项中，选出最符合题目要求的一项。）

DDACA　BBAAD　DCACD　BBACA

二、多项选择题（本题 10 小题，每小题 3 分，共 30 分。请在下列每小题给出的选项中，选出符合题目要求的两个或两个以上选项。多选、漏选、错选均不得分。）

21、ABC

22、ACD

23、ABD

24、ABC

25、ABC

26、ABC

27、ACD

28、ABD

29、BCD

30、BCD

三、判断题(本题共 15 小题，每小题 2 分，共 30 分。以下叙述中，你认为正确的打“√”，错误的打“×”。)

31．√　32．×　33．√　34．√　35．√

36．×　37．×　38．√　39．√　40．×

41．√　42．×　43．√　44．√　45．×