|  |
| --- |
| 形考任务四 |
| 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。单选题 |
| 【答案】国家安全、经济社会稳定运行 |
| 2.《中华人民共和国网络安全法》正式施行的时间是？单选题 |
| 【答案】2017年6月1日 |
| 3.网络安全的基本属性有：可用性、完整性和\_\_\_\_\_\_\_\_\_。单选题 |
| 【答案】保密性 |
| 4.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：多选题 |
| 【答案】解题模式（Jeopardy） |
| 【答案】攻防模式（Attack-Defense） |
| 【答案】混合模式（Mix） |
| 5.可以通过以下哪种方式来获取网络安全情报与科技信息（　　）多选题 |
| 【答案】网络安全会议 |
| 【答案】网络安全期刊 |
| 【答案】网络安全网站 |
| 【答案】CTF比赛 |
| 6.2019年5月13日，《信息安全技术网络安全等级保护基本要求》（简称等保2.0）正式发布，并已于2019年12月1日起正式实行。“等保2.0”保护对象包括：多选题 |
| 【答案】基础信息网络（广电网、电信网等） |
| 【答案】信息系统（采用传统技术的系统） |
| 【答案】云计算平台、以及大数据平台 |
| 【答案】移动互联、物联网和工业控制系统等 |
| 7.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。判断题 |
| 【答案】正确 |
| 8.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。（　　）判断题 |
| 【答案】错误 |
| 9.下列哪个不是网络攻击的主要目的：单选题 |
| 【答案】造成人员伤亡 |
| 10.以下哪个不是常见的网络攻击手段：单选题 |
| 【答案】破坏供电系统造成服务器停电 |
| 11.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：单选题 |
| 【答案】snort |
| 12.随着攻防技术对抗的不断演进，一些漏洞扫描工具在检测目标系统的脆弱点时，还会进行攻击的概念验证（POC），从而确认此脆弱点是否可以被利用。以下哪个工具有攻击概念验证的功能：单选题 |
| 【答案】fscan |
| 13.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哈希加密运算后再保存。对这种加密后口令，以下哪个说法是正确的：单选题 |
| 【答案】加密储存的口令可以被“撞库”攻击 |
| 14.端口扫描工具能获取以下哪些信息：多选题 |
| 【答案】端口开放信息 |
| 【答案】端口提供的服务 |
| 【答案】主机的操作系统 |
| 15.软件漏洞利用是攻击者利用软件应用程序中的缺陷进行攻击的方法，常见被利用的软件漏洞有：多选题 |
| 【答案】缓冲区溢出漏洞 |
| 【答案】业务逻辑错误 |
| 【答案】数据验证问题 |
| 【答案】身份认证和授权错误 |
| 【答案】文件处理问题 |
| 16.高级持续威胁（APT）的特征有：多选题 |
| 【答案】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 |
| 【答案】这类攻击持续监控目标，对目标保有长期的访问权 |
| 【答案】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 |
| 17.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。（　　）判断题 |
| 【答案】错误 |
| 18.常见的口令破解方式有口令组合、社会工程学、机器学习破解、撞库等。（　　）判断题 |
| 【答案】错误 |
| 形考任务五 |
| 1.病毒为什么会将自己附着在主机可执行程序中？单选题 |
| 【答案】因为病毒不能独立执行 |
| 2.以下哪一种是防止系统不受恶意代码威胁的最简单最完美的方法？单选题 |
| 【答案】没有这样通用的完美的保护系统的方法 |
| 3.防病毒产品可以实施在网络的哪三个层次中？单选题 |
| 【答案】网关、服务器、桌面 |
| 4.以下关于恶意代码的说法，哪个是错误的：单选题 |
| 【答案】恶意代码无法独立运行，需要与捆绑在正常软件上才能运行。 |
| 5.以下哪个不是漏洞数据库：单选题 |
| 【答案】CVE |
| 6.以下哪个不是常见的恶意代码：单选题 |
| 【答案】细菌 |
| 7.关于勒索软件，以下哪个说明是错误的：单选题 |
| 【答案】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 |
| 8.以下哪个不是计算机病毒的生命周期：单选题 |
| 【答案】感染阶段 |
| 9.以下哪个不是计算机病毒的类别：单选题 |
| 【答案】电子病毒 |
| 10.以下哪个不是预防计算机病毒的方法：单选题 |
| 【答案】不使用容易被猜到弱口令 |
| 11.恶意软件主要采用以下哪些传播途径进行传播：多选题 |
| 【答案】软件捆绑 |
| 【答案】利用漏洞 |
| 【答案】移动介质 |
| 【答案】远程下载 |
| 【答案】社会工程学 |
| 12.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。多选题 |
| 【答案】扫描 |
| 【答案】攻击 |
| 【答案】复制 |
| 13.下列哪些步骤属于恶意代码的作用过程：多选题 |
| 【答案】入侵系统 |
| 【答案】提升权限 |
| 【答案】实施隐藏 |
| 【答案】潜伏等待 |
| 【答案】执行破坏 |
| 14.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。判断题 |
| 【答案】正确 |
| 15.以下哪个不是防火墙的基本功能：单选题 |
| 【答案】防范钓鱼邮件功能 |
| 16.网络防御技术所包含的身份认证基本方法，不包括（　　）。单选题 |
| 【答案】基于数字签名的身份认证 |
| 17.根据Endsley模型，可以将态势感知划分为三个层级，不包括（　　）。单选题 |
| 【答案】安全审计 |
| 18.网络防御技术所包含的访问控制技术内容，不包括（　　）。单选题 |
| 【答案】负载均衡 |
| 19.按照访问控制方式不同，防火墙可以分为（　　）。多选题 |
| 【答案】包过滤防火墙 |
| 【答案】应用代理防火墙 |
| 【答案】状态检测防火墙 |
| 20.入侵检测技术系统分为：多选题 |
| 【答案】基于主机的入侵检测系统 |
| 【答案】基于网络的入侵检测系统 |
| 【答案】分布式入侵检测系统 |
| 21.防火墙的典型部署模式包括（　　）。多选题 |
| 【答案】屏蔽主机模式 |
| 【答案】双宿/多宿主机模式 |
| 【答案】屏蔽子网模式 |
| 22.逻辑隔离的主要技术包括（　　）。多选题 |
| 【答案】虚拟局域网 |
| 【答案】虚拟路由及转发 |
| 【答案】多协议标签转换 |
| 【答案】虚拟交换机 |
| 23.入侵防御系统主要包括以下几个部分（　　）。多选题 |
| 【答案】应用数据重组 |
| 【答案】协议识别和协议解析 |
| 【答案】特征匹配 |
| 【答案】响应处理 |
| 24.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。 （　　）判断题 |
| 【答案】正确 |
| 25.加密算法的功能是实现信息的（　　）：单选题 |
| 【答案】保密性 |
| 26.数字签名算法可实现信息的（　　）：单选题 |
| 【答案】不可否认性 |
| 27.在以下古典密码体制中，不属于置换密码的是（　　）：单选题 |
| 【答案】倒序密码 |
| 28.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：多选题 |
| 【答案】保密性服务 |
| 【答案】完整性服务 |
| 【答案】认证服务 |
| 29.零信任遵循的原则有：多选题 |
| 【答案】不做任何假定 |
| 【答案】不相信任何人 |
| 【答案】随时检查一切 |
| 【答案】防范动态威胁 |
| 【答案】做最坏打算 |
| 30.PKI系统包含以下哪些部分：多选题 |
| 【答案】权威认证机构CA |
| 【答案】证书库 |
| 【答案】密钥备份及恢复系统 |
| 【答案】证书废止处理系统 |
| 【答案】PKI应用接口系统 |
| 31.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。判断题 |
| 【答案】正确 |
| 32.在DES加密过程中，S盒对加密的强度没有影响。判断题 |
| 【答案】错误 |
| 形考任务六 |
| 1.人脸识别采用了哪个认证技术：单选题 |
| 【答案】基于生物特征 |
| 2.以下哪种认证方式相对最安全？单选题 |
| 【答案】人脸识别加短信验证码认证 |
| 3.以下哪个口令相对最为安全？单选题 |
| 【答案】pAsswOrd |
| 4.按照对验证对象要求提供的认证凭据的类型数量，认证可以分成：多选题 |
| 【答案】单因素认证 |
| 【答案】双因素认证 |
| 【答案】多因素认证 |
| 5.一般来说，认证机制由哪几个部分构成：多选题 |
| 【答案】验证对象 |
| 【答案】认证协议 |
| 【答案】鉴别实体 |
| 6.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？单选题 |
| 【答案】非授权访问 |
| 7.以下哪种是常见的网站拒绝服务攻击技术？单选题 |
| 【答案】HTTP Flood |
| 8.某单位员工收到一封仿冒邮件，要求其立马通过邮件里的链接更新账号密码，该员工受到了电子邮件什么类型的攻击？单选题 |
| 【答案】钓鱼邮件 |
| 9.网站面临的主要安全威胁有哪些：多选题 |
| 【答案】非授权访问 |
| 【答案】数据泄露 |
| 【答案】拒绝服务 |
| 【答案】网站后台管理安全威胁 |
| 10.以下哪些是政务网站安全防护的内容：多选题 |
| 【答案】网页防篡改 |
| 【答案】入侵防御和病毒防护 |
| 【答案】网络/数据库审计 |
| 11.电子邮件面临的主要安全威胁有哪些：多选题 |
| 【答案】钓鱼邮件 |
| 【答案】勒索病毒 |
| 【答案】恶意链接 |
| 12.以下关于云计算安全的说法，哪个是错误的：单选题 |
| 【答案】云计算的用户资源相互会干扰，需要让不同用户使用的资源在物理环境中分开 |
| 13.某单位员工收到了一封电子邮件，发件人显示为网络管理员，邮件内容里提示其帐户过期，要求他重置密码，并给出了一个重置密码的链接。该员工点开链接发现网站要求他输入当前使用的用户名和密码。该员工经过观察，发现网站页面内容显示有问题，URL的地址栏并不是熟悉的域名。请问该员工遇到攻击手段的类型是：单选题 |
| 【答案】社会工程攻击 |
| 14.以下哪个不属于物联网安全防护层次：单选题 |
| 【答案】应用层安全 |
| 15.目前漏洞挖掘分析技术有多种，主要包括多选题 |
| 【答案】手工测试技术 |
| 【答案】模糊测试技术 |
| 【答案】二进制比对技术 |
| 【答案】静态分析技术 |
| 【答案】动态分析技术 |
| 16.区块链技术主要有哪些特点：多选题 |
| 【答案】去中心化 |
| 【答案】不可篡改 |
| 【答案】共识 |
| 17.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。判断题 |
| 【答案】错误 |
| 18.安全大数据分析要以建立科学合理的分析模型作为前提。一般认为安全大数据的分析模型包括但不仅限于：规则模型、关联模型、统计模型、异常检测模型等。判断题 |
| 【答案】正确 |
| 19.威胁情报的目的是利用公开的资源、数据、情报等，发现安全威胁并指导企业行动以改善安全状况，可以帮助企业和组织快速了解到敌对方对自己的威胁信息，从而帮助提前威胁防范、攻击检测与响应、事后攻击溯源等能力。判断题 |
| 【答案】正确 |
| 形考任务七 |
| 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。单选题 |
| 【答案】国家安全、经济社会稳定运行 |
| 2.网络安全的基本属性有：可用性、完整性和\_\_\_\_\_。单选题 |
| 【答案】保密性 |
| 3.《中华人民共和国网络安全法》正式施行的时间是\_\_\_\_\_\_\_\_。单选题 |
| 【答案】2017年6月1日 |
| 4.下列哪个不是网络攻击的主要目的：单选题 |
| 【答案】造成人员伤亡 |
| 5.以下哪个不是常见的网络攻击手段：单选题 |
| 【答案】破坏供电系统造成服务器停电 |
| 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：单选题 |
| 【答案】snort |
| 7.以下哪个不是常见的恶意代码：单选题 |
| 【答案】细菌 |
| 8.关于勒索软件，以下哪个说明是错误的：单选题 |
| 【答案】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。 |
| 9.以下哪个不是计算机病毒的生命周期：单选题 |
| 【答案】感染阶段 |
| 10.以下哪个不是防火墙的基本功能：单选题 |
| 【答案】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：单选题 |
| 【答案】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\_\_\_\_\_\_。单选题 |
| 【答案】安全审计 |
| 13.加密算法的功能是实现信息的\_\_\_\_\_\_\_。单选题 |
| 【答案】保密性 |
| 14.数字签名算法可实现信息的\_\_\_\_\_\_\_。单选题 |
| 【答案】不可否认性 |
| 15.在以下古典密码体制中，不属于置换密码的是（　　）：单选题 |
| 【答案】倒序密码 |
| 16.以下哪种认证方式相对最安全？单选题 |
| 【答案】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？单选题 |
| 【答案】pAsswOrd |
| 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？单选题 |
| 【答案】非授权访问 |
| 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？单选题 |
| 【答案】钓鱼邮件 |
| 20.以下哪个不属于物联网安全防护层次：单选题 |
| 【答案】应用层安全 |
| 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：多选题 |
| 【答案】解题模式（Jeopardy） |
| 【答案】攻防模式（Attack-Defense） |
| 【答案】混合模式（Mix） |
| 22.端口扫描工具能获取以下哪些信息：多选题 |
| 【答案】端口开放信息 |
| 【答案】端口提供的服务 |
| 【答案】主机的操作系统 |
| 23.高级持续威胁（APT）的特征有：多选题 |
| 【答案】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 |
| 【答案】这类攻击持续监控目标，对目标保有长期的访问权 |
| 【答案】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 |
| 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。多选题 |
| 【答案】扫描 |
| 【答案】攻击 |
| 【答案】复制 |
| 25.下列哪些步骤属于恶意代码的作用过程：多选题 |
| 【答案】入侵系统 |
| 【答案】提升权限 |
| 【答案】实施隐藏 |
| 【答案】潜伏等待 |
| 【答案】执行破坏 |
| 26.按照访问控制方式不同，防火墙可以分为（　　）。多选题 |
| 【答案】包过滤防火墙 |
| 【答案】应用代理防火墙 |
| 【答案】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：多选题 |
| 【答案】保密性服务 |
| 【答案】完整性服务 |
| 【答案】认证服务 |
| 28.一般来说，认证机制由哪几个部分构成：多选题 |
| 【答案】验证对象 |
| 【答案】认证协议 |
| 【答案】鉴别实体 |
| 29.电子邮件面临的主要安全威胁有哪些：多选题 |
| 【答案】钓鱼邮件 |
| 【答案】勒索病毒 |
| 【答案】恶意链接 |
| 30.区块链技术主要有哪些特点：多选题 |
| 【答案】去中心化 |
| 【答案】不可篡改 |
| 【答案】共识 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】错误 |
| 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。（　　）判断题 |
| 【答案】错误 |
| 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。(　　)判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 36.按照网络蠕虫的传播途径和攻击牲，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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】错误 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 40.在DES加密过程中，S盒对加密的强度没有影响。（　　）判断题 |
| 【答案】错误 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】错误 |
| 43.网站仿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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】正确 |
| 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。（　　）判断题 |
| 【答案】错误 |