2021 年大学生网络安全知识竞赛题库及答案（共 60 题）

1 如何修改 Web server（IIS、Apache）的 banner 字段（A)

修改存放 banner 文件

利用 server mask 此类的插件

以上均可

2 以下对 IDS（入侵检测系统）的异常检测技术的描述中，不正确的是（C）

基于异常检测的入侵检测系统在检测时，将系统检测到的行为与预定义的正常行为比较，得出是否有被攻击的迹象

由于正常行为模型相对固定，所以异常检测模式对网络环境的适应性不强，误报的情况比较多

异常检测模式的核心是维护一个入侵模式库

异常检测模式则无法准确判别出攻击的手法，但它可以判别更广泛、甚至未发觉的攻击

3 在做恶意代码分析时，通常使用什么工具监测恶意代码的注册表操作（A）

Regmon

Filemon

Autoruns

Ollydug

4Windows 2000 所支持的认证方式包括下列哪些（D）

NTLM

Kerberos

LanManager

以上均是

5 在对 Windows 系统进行安全配置时，“LAN Manager 身份验证级别”应选用的设置为：(A)

仅发送 NTLMV2 响应

发送 LM & NTLM 响应

仅发送 NTLM 响应

仅发送 LM 响应

6 使用 Windows2000 的组策略,可以限制用户对系统的操作权限,该实例是何种功能的应用？（B）

访问控制列表

执行控制列表

身份验证

数据加密

7、SQL Server 默认的通讯端口为（ ），为提高安全性建议将其修改为其他端口（C）

TCP1434

TCP 1521

TCP 1433

TCP 1522

8 信息安全风险应该是以下哪些因素的函数？（A）

A.信息资产的价值、面临的威胁以及自身存在的脆弱性等

B.病毒、黑客、漏洞等

C.保密信息如国家秘密、商业秘密等

D.网络、系统、应用的复杂程度

9 哪项不属于网络 DOS 攻击（A）

Session table flood

SYN flood

ICMP flood

UDP flood

10 下面哪项不是数字证书中的内容.（D）

A. 证书发布人的姓名

B. 发行证书的实体

C. 实体的公开密钥

D. 上面所有的都是数字证书的组成部分

11 冰河软件是哪国产的什么软件?(D)

A 国外产的远程桌面程序

B 国内产的远程桌面程序

C 国外产的远程控制木马程序

D 国内产的远程控制木马程序

12 什么是 ids(A)

A 入侵检测系统

B 入侵防御系统

C 网络审计系统

D 主机扫描系统

13 若需要修改 TOMCAT 的监听地址，应修改哪个配置文件?(B)

A tomcat.xml

B server.xml

C web.xml

D tomcat-users.xml

14 在 MPLS L3 VPN 当中通过 LDP 协议来分发标签，LDP 分发的是(A)标签?

A 公网标签

B 私网标签

C 公网和私网标签

D LDP 分发除公网和私网以外的标签

15 关于防火墙的描述不正确的是(C)

A 作为不同网段之间的逻辑隔离设备，防火墙将内部可信区域与外部危险区域有效隔离

B 防火墙将网络的安全 策略制定和信息流动集中管理控制

C 防火墙规则是一种细颗粒的检查，能对大多数协议的细节做到完全解析

D 防火墙为网络边界提供保护，是抵御入侵的有效手段之一

16 以下哪个工具通常是系统自带任务管理器的替代（D）

A Regmon

B Filemon

C Autoruns

D Process explorer

17 下列恶意代码传播最快的是(B)

A 木马

B 蠕虫

C ROOTKIT

D 病毒

18 蠕虫和病毒的最大区别是(C)

A 自我复制

B 主动传播

C 是否需要人机交互

D 多感染途径

19Arp 欺骗可以对局域网用户产生何类威胁(D)

A 挂马

BDNS 毒化

C 中间人攻击

D 以上均是

20Linux 内核主要由五个子系统组成:进程调度，内存管理，进程间通信和(A/C)

A 虚拟文件系统， 网络接口

B 文件系统，设备接口

C 虚拟文件系统， 网络接口

D 文件系统， 设备接口

21 默认情况下，Window 2000 域之间的信任关系有什么特点(B)

A 只能单向，可以传递

B 只能单向，不可传递

C 可以双向，可以传递

D 可以双向，不可传递

22 下列文件中可以防止 Solaris 下 root 用于远程登陆的是（B）

A　/etc/securetty

B　/etc/default/login

C　/etc/securetty

D . /etc/security/user

23 通过 SSH 的使用，无法规避的风险是（A）

AIP 假冒

B 数据传输工程中操纵数据

C 利用源/目的主机漏洞，并最终对其实现控制

24 下面哪一 种攻击方式最常用于破解口令(B)

A 哄骗(spoofing)

B 字典攻击 (dictionary attack)

C 拒绝服务(DoS)

D WinNuke

25 关于 Win2K 的日志，下列说法正确的是(D)

A 默认的 http 日志存放在%systemroot%/system32/logfiles/w3svc1 下

B 默认的 ftp 日志存放在%systemroot%/system32/logfiles/w3svc2

C　Win2K 默认有 系统日志和安全日志两种

D Win2K 默认开启安全日志

26 防火墙可分为两种基本类型是（D）正确：包过滤和应用代理

A、分组过滤型和复合型

B、　复合型和应用代理型

C、　分组过滤型和应用代理型

D、以上都不对

27 以下不属分布式防火墙的产品的有（B）

A、 网络防火墙

B、软件防火墙

C、 主机防火墙

D、 中心防火墙

28 当进行分析校验的时候你通常会在什么情况下发现一个被木马感染了的文件(B)

A. 在可执行文件的末尾有扩展名为.TRJ 的文件

B. 文件的尺寸变大或者变小,或者时间戳错误

C. 文件被删除

D.文件已经具备了一个.SRC 扩展名

29 以下关于 Smurf 攻击的描述，那句话是错误的?(A)

A 它是一种拒绝服务形式的攻击

B 它依靠大量有安全漏洞的网络作为放大器

C 它使用 ICMP 的包进行攻击

D 攻击者 最终的目标是在目标计算机上获得一个帐号

30 Solaris 操作系统下，下面哪个命令可以修改/n2kuser/.profile 文件的属性为所有用户可读、可写、可执行?(D)

A chmod 744 /n2kuser/.profile

B chmod 755 /n2kuser/.profile

C chmod 766 /n2kuser/.profile

D chmod 777 /n2kuser/.profile

31 下面哪个是为广 域网(WWW).上计算机之间传送加密信息而设计的标准通信协议(B)

A. SSL

B. HTTPS

C.HTTP

D. TSL