第5章 网络安全

5.1 单选题

1. 任何通过合法的方式使服务器不能提供正常服务的攻击手段就是(　　)。

A. 扫描攻击　　B. 嗅探器攻击

C. 电子欺骗攻击　　D. 拒绝服务攻击

2. 按攻击结果分类,可以将拒绝服务攻击分为(　　)。

A. 网络带宽攻击和连通性攻击

B. 利用软件缺陷和利用协议漏洞

C. 单机版拒绝服务攻击和分布式拒绝服务攻击

D. 扫描和欺骗

3. 在拒绝服务攻击中,Winnuke 攻击、Teardrop 攻击和 Land 攻击属于(　　)。

A. 网络带宽攻击　　B. 利用软件缺陷攻击

C. 利用协议漏洞攻击　　D. 连通性攻击

4. TCP syn 洪泛攻击的原理是利用了(　　)。

A. TCP 数据传输中的窗口技术　　B. TCP 面向流的工作机制

C. TCP 三次握手过程　　D. TCP 连接终止时的 FIN 报文

5. 死亡之 ping 属于(　　)。

A. 拒绝服务攻击　　B. 冒充攻击　　C. 重放攻击　　D. 篡改攻击

6. ICMP 洪泛攻击利用了(　　)。

A. ping 命令的功能　　B. ARP 命令的功能

C. tracert 命令的功能　　D. route 命令的功能

7. 攻击者冒充攻击目标向本网络的广播地址发送 ICMP Echo 请求包,使得网内所有机器对此请求产生响应,大量响应包涌向目标机,从而使得目标机无法正常处理服务。这种攻击方法称为(　　)。

A. Teardrop 攻击　　B. Smurf 攻击　　C. LAND 攻击　　D. 死亡之 ping

8. 在分布式拒绝服务攻击中,通过非法入侵并被控制,但并不向被攻击者直接发起攻击的计算机称为(　　)。

A. 攻击傀儡机　　B. 攻击者　　C. 控制傀儡机　　D. 被攻击主机

9. 对利用软件缺陷进行的网络攻击，最有效的防范方法是(　　)。

A. 及时更新补丁程序　　B. 安装防病毒软件

C. 安装防火墙　　D. 安装漏洞扫描软件

10. 黑客利用IP地址进行攻击的方法有(　　)。

A. 发送病毒　　B. 解密　　C. 窃取口令　　D. IP欺骗

11. 通过伪造源IP地址等于目标IP地址、源端口等于目标端口的TCP SYN数据包从而使得被攻击机瘫痪的攻击方式被称为(　　)。

A. Teardrop攻击　　B. Land攻击

C. Synflood攻击　　D. Smurf攻击

12. 在屏蔽子网结构中，路由器的作用是(　　)。

A. 作为外网访问内网的唯一出入口

B. 作为包过滤防火墙

C. 作为应用代理防火墙

D. 使各网段整合，方便数据交流

13. 将属于同一连接的所有包作为一个整体的数据流看待，这种防火墙属于(　　)。

A. 简单包过滤型防火墙　　B. 应用代理型防火墙

C. 状态检测包过滤型防火墙　　D. 混合型防火墙

14. 当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时，该服务器一般要置于防火墙的(　　)。

A. DMZ区　　B. 内部　　C. 外部　　D. 都可以

15. 以下不是防火墙功能的是(　　)。

A. 记录通过防火墙的信息内容和活动　　B. 过滤出口网络的数据包

C. 封堵某些禁止的访问行为　　D. 保护存储数据的安全

16. 防火墙中地址转换的主要作用是(　　)。

A. 隐藏内部网络地址　　B. 提供代理服务

C. 进行入侵检测　　D. 防止病毒入侵

17. 以下关于传统防火墙，不正确的描述是(　　)。

A. 静态技术，不能防范新的威胁和攻击

B. 既可防内，也可防外

C. 工作效率较低，易成为网络瓶颈

D. 容易出现单点故障

18. 在混合型防火墙系统组成中，下列选项(　　)不被包括在内。

A. 包过滤型防火墙　　B. 堡垒主机

C. 内网服务器　　D. 应用代理型防火墙

19. 以下功能不可能集成在防火墙上的是(　　)。

A. 防御内部病毒传播　　B. 网络地址转换

C. 内外网分离　　D. 规则过滤

20. 以下不属于入侵检测技术功能的是(　　)。

A. 检查系统配置和漏洞　　B. 地址转换

C. 识别已知攻击行为　　D. 发现未知攻击行为

21. 关于特征检测技术，下列说法正确的是(　　)。

A. 能检测未知攻击　　B. 误报率高

C. 收集非正常行为来建立特征库　　D. 实现难度大

22. Snort 是一个使用(　　)实例。

A. 特征检测的 NIDS　　B. 异常检测的 NIDS

C. 特征检测的 DIDS　　D. 异常检测的 DIDS

23. Snort 中不会对流量产生行为的规则选项是(　　)。

A. Post-detection 类　　B. 基本信息类

C. Payload 类　　D. Non-payload 类

24. 下列不属于分布式拒绝服务攻击防范措施的是(　　)。

A. 使用具有 syn cookie 的 TCP 连接处理程序

B. 安装防火墙，禁止访问不该访问的端口，过滤不正常的畸形数据包

C. 安装入侵检测系统，检测拒绝服务攻击行为

D. 安装先进杀毒软件，抵御攻击行为

25. 下面关于我们使用的网络是否安全，正确的表述是(　　)。

A. 没有绝对安全的网络，要时刻谨慎操作

B. 安装了防火墙，网络是安全的

C. 安装了防火墙和杀毒软件，网络是安全的

D. 设置了复杂的密码，网络是安全的

26. 下列哪一种方式是入侵检测系统通常采用的？(　　)

A. 基于网络的入侵检测　　B. 基于 IP 的入侵检测

C. 基于服务的入侵检测　　D. 基于域名的入侵检测

27. 下列(　　)不属于入侵检测系统的功能。

A. 监视网络上的通信数据流　　B. 建立通信信道

C. 捕获可疑的网络活动　　D. 提供安全审计报告

28. 以下属于数据链路层的隧道协议的是(　　)。

A. PPTP　　B. IPSec　　C. Socks5　　D. SSL

29. 如图 5-1 所示，在 GRE 隧道协议中，包头所含的信息为(　　)。

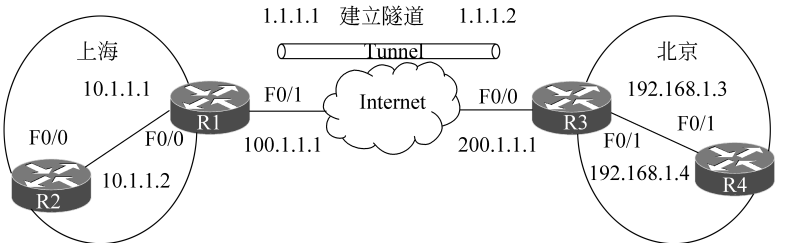

图 5-1　GRE 隧道协议

A. 源 10.1.1.2；目的 10.1.1.1　　B. 源 100.1.1.1；目的 200.1.1.1

C. 源 1.1.1.1；目的 1.1.1.2　　D. 源 192.168.1.3；目的 192.168.1.4

30. 以下不能用作 VPN 服务器的是(　　)。

A. 防火墙　　B. 路由器

C. 安装 VPN 的计算机或设备　　D. 专用网关中的 VPN 模块

31. 在以下隧道协议中,属于三层隧道协议的是(　　)。

A. L2F　　B. IPSec　　C. PPTP　　D. L2TP

32. 以下有关 VPN 技术的描述,不正确的是(　　)。

A. 易于扩展　　B. 使用费用低廉

C. 为数据传输提供机密性和完整性　　D. 未改变原有的网络边界

33. 以下关于 VPN 技术,说法正确的是(　　)。

A. VPN 是指用户自己租用线路,和公共网络物理上完全隔离、安全的线路

B. VPN 是指用户通过公用网络建立的临时、安全的连接

C. VPN 不能做到信息认证和身份认证

D. VPN 只提供身份认证,不能提供数据加密功能

5.2　多选题

1. 端口扫描的作用有(　　)。

A. 发现开放的服务　　B. 发现网络拓扑结构

C. 发现操作系统类型　　D. 发现主机是否在线

2. 常见的电子欺骗攻击方式有(　　)。

A. IP 地址欺骗　　B. DNS 欺骗　　C. ARP 欺骗　　D. 社工欺骗

3. 分布式拒绝服务(DDoS)攻击网络的组成有(　　)。

A. 一台或多台攻击主机　　B. 一些控制傀儡机

C. 大量的攻击傀儡机　　D. 被攻击主机

4. 防火墙的优点有(　　)。

A. 防止非授权用户进入内网　　B. 缓解地址空间短缺

C. 限制安全问题扩散　　D. 方便审计

5. 关于堡垒主机的说法,正确的是(　　)。

A. 使用两块网卡连接不同网络　　B. 配有网关服务

C. 仅存在于内网中　　D. 充当应用代理防火墙的作用

6. 基于事件产生器数据来源,可以将入侵检测系统分为(　　)。

A. 基于主机的入侵检测系统　　B. 基于网络的入侵检测系统

C. 分布式入侵检测系统　　D. 主动响应入侵检测系统

7. 以下属于 HIDS 分类的有(　　)。

A. 系统调用分析器　　B. 日志分析器

C. 文件完整性检查器　　D. 基于特征的检测器

8. 根据保护的目的,NIDS 可以被部署在(　　)。

A. 外网　　B. 移动设备　　C. 内网　　D. 防火墙内部

9. 异常入侵检测技术建立活动简档时可以考虑使用(　　)。

A. CPU 利用率　　B. 文件访问次数

C. 接收的数据包内容　　D. 网络连接次数

10. 关于蜜罐的特点，说法正确的是(　　)。

A. 内置入侵检测系统　　B. 尽可能模拟实际系统环境

C. 记录恶意活动　　D. 部署或模拟存在漏洞的服务

11. VPN 保护了以下哪些安全属性？(　　)

A. 完整性　　B. 不可否认性　　C. 机密性　　D. 可用性

12. VPN 可以允许(　　)访问内网。

A. 外部人员　　B. 公司在外出差的员工

C. 可信的合作伙伴　　D. 分支机构

13. VPN 实现过程中采用了(　　)。

A. 隧道技术　　B. 密钥管理技术

C. 加解密技术　　D. 消息及身份认证技术

14. VPN 的密钥管理技术提供了(　　)等保护功能。

A. 保证密钥交换安全　　B. 参与方身份验证

C. 阻止钓鱼攻击　　D. 防止拒绝服务攻击

5.3 判断题

1. 使用合法渠道收集信息不属于黑客的攻击手段。(　　)

2. 黑客技术方式进行攻击指的是通过专门设计的攻击工具或利用计算机系统的薄弱点进行攻击。(　　)

3. 发起大规模的分布式拒绝服务攻击通常要控制大量的中间网络或系统。(　　)

4. 防火墙一般采取的安全策略是“重可用性，轻安全性”。(　　)

5. 防火墙提供访问控制，只有允许的数据才能通过，而路由器只有被拒绝的数据才会禁止。(　　)

6. 防火墙既能防范外部攻击也能防范内部攻击。(　　)

7. 应用代理型防火墙工作在 TCP/IP 的应用层。(　　)

8. 设计防火墙时要将最特殊的规则放在最后面。(　　)

9. 防火墙的规则要简单实用。(　　)

10. 包过滤防火墙一般工作在 OSI 参考模型的网络层与传输层，主要对 IP 分组和 TCP/UDP 端口进行检测和过滤操作。(　　)

11. 采用防火墙的网络一定是安全的。(　　)

12. 硬件配置相同的情况下，应用代理防火墙对网络运行性能的影响要比包过滤防火墙小。(　　)

13. 入侵检测技术比防火墙要高级，故只需要使用入侵检测技术就好。(　　)

14. NIDS 主要保护网络的运行，可以不设置 IP 地址。(　　)

15. NIDS 和目标系统对于数据包的理解不一致，易受注入和逃避入侵的欺骗。(　　)

16. 异常检测技术的误报率较高，且实现难度大，正常模式的知识库难以建立，但不需要对每种入侵行为进行定义，可以检测未知的攻击。(　　)

17. 特征检测技术收集正常行为特征，当操作偏离特征时则认为行为是入侵。(　　)

18. NIDS 一定会取代 HIDS。（　　）

19. 在 IDS 中，特征检测不能检测到已经有过的攻击方式，但能够检测到从未出现过的攻击。（　　）

20. VPN 通过通信协议、身份验证和数据加密三方面技术保证了通信的安全性。（　　）

21. VPN 的灵活性很强，支持任意类型的数据流和传播媒介。（　　）

22. 为了保证消息的完整性以及身份认证，主要采用 RSA 或 ECC 等算法。（　　）

23. QoS 技术根据用户的不同要求支持不同级别的服务质量，使网络资源得到最大化利用。（　　）

24. 隧道技术中的运载协议也称隧道协议，与乘客协议相接。（　　）

25. VPN 由客户端、VPN 服务器、VPN 隧道协议和传输通道组成。（　　）

26. 自愿隧道技术和强制隧道技术的区别在于自愿隧道技术中多个客户的数据信息会通过一条隧道进行传递，而强制隧道技术中每个客户拥有一条独立的隧道。（　　）

27. 强制隧道技术中只有最后一个隧道用户断开连接后才终止整条隧道。（　　）

28. VPN 的主要特点是通过加密使信息能安全地通过 Internet 传递。（　　）

5.4　填空题

1.（　　）指的是利用漏洞谋取非法的个人、经济或政治利益的攻击者。

2.（　　）通过连接所有已知的 TCP/IP 端口和服务，测试目标节点，并记录目标的回答，从而可以收集到关于目标主机的有用信息。

3. 通过耗尽 CPU、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为被称为（　　）。

4. 按攻击方式分类，拒绝服务攻击可分为（　　）和（　　）。

5.（　　）攻击出现在 IP 层，运用了缓冲区溢出漏洞中的符号溢出漏洞。

6.（　　）是设置在不同网络或网络安全域之间的网络访问控制设备。

7. 按照技术原理，防火墙可分为（　　）、应用代理、状态检测包过滤和混合型防火墙。

8.（　　）防火墙工作在 TCP/IP 的网络层和传输层，检查单个数据包的包头字段信息，根据安全策略规则进行包头过滤。

9.（　　）是一种及时发现入侵、成功阻止黑客入侵、并在事后对入侵进行分析，查明系统漏洞并及时修补的动态网络安全技术。

10. 进行入侵检测的软硬件的组合被称为（　　），简称 IDS。

11. 入侵检测系统通常包括（　　）、（　　）、（　　）和（　　）四个模块。

12. 从主机中获取审计数据，准确知道目标系统发生的事件，主要目的是保护主机的检测系统被称为（　　）。

13. 基于网络的入侵检测系统被放置在交换机的（　　），以便能看到所有进出的数据包。

14. 分布式入侵检测系统可以对来自（　　）和（　　）的数据流进行分析，使用一个（　　）模块进行综合检测。

15. 异常检测技术常采用（　　）、（　　）和（　　）等方法进行检测。

16. Snort 规则由(　　)和(　　)组成。

17. 由人工构建的用于吸引、诱骗攻击者进行攻击从而获悉攻击活动的隔离环境被称为(　　)。

18. (　　)指构建在公用网络基础设施之上的虚拟专用网络。虚拟指用户无须建立各自专用的(　　)。专用网络指只有(　　)的用户才可使用。

19. VPN 使用(　　)服务质量技术为企业和用户提供不同等级的服务质量保证以及良好的稳定性。

20. VPN 中使用的(　　)能保证数据分组传输的透明性。

21. VPN 使用的加解密技术一般使用(　　)算法的(　　)工作模式来运行。

22. 隧道技术由(　　)协议、(　　)协议和(　　)协议组成。

参考答案

5.1　单选题

1～5.　D A B C A　6～10.　A B C A D　11～15. B B C A D
16～20. A B C A B　21～25. C A B D A　26～30. A B A C C
31～33. A D B

5.2　多选题

1. A C　2. A B C　3. A B C　4. A B C D　5. A B D
6. A B C　7. A B C D　8. A C D　9. A B D　10. B C D
11. A C　12. B C D　13. A B C D　14. A B D

5.3　判断题

1～5.　F T T F T　6～10.　F T F T T　11～15. F F F T T
16～20. T F F F T　21～25. T F T F T　26～28. F T T

5.4　填空题

1.(黑客)　2.(扫描攻击)
3.(拒绝服务)　4.(利用软件缺陷)(利用协议漏洞)
5.(Teardrop)　6.(防火墙)
7.(包过滤)　8.(简单包过滤型)
9.(入侵检测)　10.(入侵检测系统)
11.(事件产生器)(事件分析器)(事件数据库)(响应单元)
12.(基于主机的入侵检测系统)　13.(端口镜像口)
14.(网络)(主机)(中心管理员)　15.(统计方法)(预测模式)(神经网络)
16.(规则头)(规则选项)　17.(蜜罐)
18.(VPN)(物理线路)(经过授权)　19.(QoS)
20.(隧道技术)　21.(DES)(CBC)
22.(运载)(封装)(乘客)