网络安全

Modified:: 2023-03-23 16:30

1. TCP传输的可靠性表现在哪些方面
   TCP是一种面向连接的传输协议，我认为TCP传输的可靠性主要表现在以下方面
   1. 确认和重传，接收方接收到发送方发送的数据后会发送确认信息，如果没有收到发送方发送的消息就不会发送确认信息，那么一段时间之后发送方就会重新传送信息
   2. 流量控制：TCP采用滑动窗口机制来进行流量控制，确保发送方的数据不会超过接收方能够处理的极限
   3. 拥塞控制：TCP采用拥塞控制机制来避免网络拥塞，确保网络可靠性
   4. 数据检验：TCP中有校验和来确保数据在传输的过程中没有被破坏或是被篡改
2. 防火墙是什么
   防火墙是一种网络安全设备，可以在计算机网络和互联网之间建立一道屏障，控制网络流量的进出，以确保网络不受未经授权的访问，攻击或是威胁。
   防火墙主要分为软件防火墙和硬件防火墙。软件防火墙是个运行在计算机的程序，可以监视和控制进出计算机的网络流量。硬件防火墙是一种独立设备，运行在网络的边界，保护整个网络。
   防火墙主要采用的技术和策略有：访问控制，NAT，VPN，威胁检测等。
3. 防火墙有哪些分类，有什么作用
   防火墙主要分为软件防火墙和硬件防火墙。软件防火墙是个运行在计算机的程序，可以监视和控制进出计算机的网络流量。硬件防火墙是一种独立设备，运行在网络的边界，保护整个网络。
4. 说一下你了解的网络安全方面的专有名词
   1. 防火墙：一种网络安全设备，可以在计算机网络和互联网之间建立一道屏障，控制网络流量的进出，以确保网络不受未经授权的访问，攻击或是威胁。
   2. 入侵检测系统（IDS）：是一种网络安全设备，用来检测和相应网络中的入侵行为。
   3. 入侵防御系统(IPS)：是一种网络安全设备，用来防止网络中的入侵行为，提供实时防御和响应能力
5. IDS是什么
   IDS是一种网络安全设备，用来检测和响应网络中的入侵行为。主要通过监测网络流量，系统日志和其他相关事件来检测是否存在异常行为。
   IDS可以分为两种类型，网络IDS和主机IDS，网络IDS在网络流量上运行，用来监测网络流量是否有异常。而主机IDS在主机运行，主要检测操作系统和应用程序的日志

6. IPS是什么
   IPS是一种网络安全设备，用来防止网络中的入侵行为，提供实时防御和响应能力。通常放置在网络边界，监测防止从外部网络进入内部网络的威胁。
   IPS可以分为两种类型，网络IPS和主机IPS
   IPS不仅可以检测威胁，也可以采用主动措施，防止威胁的扩散或对系统造成危害。
7. http和https有什么区别
   http和https都是作用在应用层的协议，用来在服务端和客户端提供数据传输服务，他们之间的主要区别在于安全性。
   http协议的数据在传输过程中不加密，因此很容易被窃取和修改，https协议则通过TLS协议对数据进行加密，保障了传输过程中的安全性。
   此外，因为https还要进行加密解密的操作，所以传输性能相比于http要稍弱一些
8. VPN你了解多少，他的端口号是什么
   VPN是虚拟专用网络，是一种通过公用网络建立安全连接的技术，主要用来实现远程访问，数据传输加密等，可以让用户远程访问公司或者学校的私有网络资源，同时保证数据传输的安全性和隐私性。
   VPN常见的协议有PPTP，L2TP等，PPTP的端口号是1723，L2TP的端口号是500
9. 什么是DOS攻击，怎么应对DOS攻击
   DOS攻击是一种恶意攻击行为，通常是发送大量的数据流或者是连接请求来占用目标服务器的带宽，计算资源和存储资源等，导致服务器没有办法处理其他合法的请求。
   要应对DOS攻击，可以采用下面的措施
   1. 配置防火墙，屏蔽未知来源的数据包
   2. 限制某些IP或端口的数据流量
   3. 加强服务器性能
10. 什么是SQL注入攻击，怎么应对
    SQL注入攻击指的就是输入恶意的SQL代码，绕过应用程序的认证和授权阶段，直接访问和控制数据库
    要应对SQL注入攻击，可以采用下面的措施
    1. 输入过滤，对用户的输入进行过滤盒检查
    2. 最小化权限，为数据库用户分配尽可能小的权限
11. 你主要用过哪些虚拟机
    我主要用过vmware，在上面运行ubuntu，我的毕设有一部分就是在虚拟机上做的。
12. 安全体系结构中定义的安全服务通常包括什么
    应该能提供以下安全服务
    1. 机密性：保证只有被授权的用户才能访问加密后的数据
    2. 完整性：保证数据不被篡改，损坏或删除
    3. 不可否认性：发送者发送的消息不能否认，接受者接收到消息也不能否认

13. 安全机制有哪些
    安全机制指的是计算机网络中采用的保护机制，主要的安全机制有
    1. 访问控制：根据实体的身份和有关信息来确认实体的访问权限
    2. 加密：包括对称加密和非对称加密
    3. 数字签名：对数据进行数字签名，来验证信息的完整性和身份认证
       此外还有
    4. 防火墙
    5. 入侵检测和预防系统
    6. 等
14. 从体系上看，Internet网络安全问题可以分为哪几个层次
    可以分为用户层，应用层，操作系统层，数据链路层和网络层
15. 采用TCP/IP的应用层服务有哪些
    主要有
    1. 邮件传输协议SMTP
    2. 文件传输协议FTP
    3. 超文本传输协议HTTP
    4. 域名系统DNS
16. 用户或者系统可以用哪几种方法证明其身份
    1. 实物认证：用实体所拥有的某个东西来认证
    2. 密码认证
    3. 生物特征认证：如指纹，声音，头像等
    4. 位置认证：根据实体所在的位置进行认证
17. 数字签名的功能和作用是什么
    数字签名主要有以下几点作用
    1. 防止信息篡改：发送者使用私钥对数据进行加密，接受者用公钥对数据进行解密，可以验证数据的完整性
    2. 确认发送者身份：因为每个人的私钥是只有他本人拥有的，所以他加密过的数据理论上也是只能由他本人加密的，这样就可以确认发送者的身份
    3. 实现不可否认性：因为只有发送者本人才能拥有私钥，加密数据，所以发送者不能否认曾经发送过的信息
18. 网络防病毒工具的防御能力应该体现在哪些地方
    1. 病毒检测能力
    2. 实时保护能力
    3. 病毒查杀能力
    4. 资源占用小
    5. 方便使用
19. 什么是PKI，由哪几个部分组成
    PKI是一种基于公钥密码学的安全体系结构，用来实现数字证书的管理和应用。

他的组成部分主要有：数字证书，公钥密码技术，公钥的安全策略等

20. 认证中心有什么功能，由哪几个部分组成
    认证中心的功能有证书发放，证书更新，证书撤销，证书验证。认证中心的核心功能就是发放和管理数字证书。
    认证中心的主要组成有：注册服务器，证书申请受理和审核机构，认证中心服务器
21. 基于PKI的电子商务交易系统实现过程有哪几步
    1. 首先客户浏览信息，初始化请求，客户端认证
    2. 然后验证客户身份，确认客户购买权限，返回应答请求，用户进入购买状态
    3. 完成购物，发送订单
    4. 服务器收到订单，请求获取安全时间戳，记录交易信息
    5. 想商家发送订单通知，确认交易成功
22. 什么是数据包过滤技术
    数据包过滤技术是网络安全中常用的一种安全机制，通过系统设置的过滤的逻辑，对数据包进行分析选择，确定数据包能否通过网络。
    数据包过滤技术通常由防火墙实现，有基于端口的过滤，基于IP地址的过滤，基于MAC地址的过滤等。
23. 什么是状态检测技术
    状态检测技术是一种网络安全技术，用来检测网络连接的状态，已确认网络连接是否是属于合法的或是恶意的。
24. 防火墙体系结构通常分为哪几类
    主要分为
    1. 屏蔽路由器
    2. 屏蔽主机网关
    3. 双宿主机网关
    4. 屏蔽子网
25. OSI 安全体系中的五类相关安全服务:
    1. 认证(鉴别)服务:提供通信中对等实体和数据来源的认证(鉴别)。
    2. 访问控制服务:用于防止未授权用户非法使用系统资源，包括用户身份认证和用户权限确认
    3. 数据保密性服务:为防止网络各系统之间交换的数据被截获或被非法存取而泄密，提供机密保护。同时， 对有可能通过观察信息流就能推导出信息的情况进行防范。
    4. 数据完整性服务:用于防止非法实体对交换的数据的修改、插入、删除以及在数交换过程中的数据丢 失。
    5. 抗否认性服务(也叫不可否认性服务):用于防止发送方在发送数据后否认发送，接收方在接收到数据后否认收到或伪造数据的行为。
26. 网络攻击的类型有哪些
    从安全属性来看主要有阻断攻击，截取攻击，篡改攻击，伪造攻击
    1. 阻断攻击：使系统的资产被破坏，无法提供用户使用

2. 截取攻击：使非授权者得到资产的访问
3. 篡改攻击：非授权者访问资产，并且还修改信息
4. 伪造攻击：非授权者在系统中插入伪造的信息
   从攻击方式来看主要有主动攻击和被动攻击
5. 被动攻击：传输报文信息的泄露和通信流量分析
6. 主动攻击：对数据流进行一些修改或者生成一些假的数据流

27. 网络信息的安全服务有哪些
    1. 机密性服务：提供信息的保密
    2. 完整性服务：提供信息的正确性
    3. 可用性服务：提供的信息是可用的
    4. 可审性服务：进行身份的认证
28. 安全评估准则有哪些
    1. TCSEC
    2. ITSEC
    3. CC
    4. 我国信息安全评估准则
29. 网络攻击的类型主要有哪些
    主要有阻断攻击，截取攻击，篡改攻击，伪造攻击
30. 风险评估工具有哪些
    1. 调查问卷
    2. 检查列表
    3. 人员访谈
    4. 漏洞扫描器
    5. 渗透测试
31. 网卡一般有哪几种工作模式
    一般有四种工作模式
    1. 广播模式
    2. 多播模式
    3. 直接模式
    4. 混杂模式
32. 什么是ARP协议
    ARP协议就是地址解析技术，是根据IP地址解析物理地址的一个TCP/IP协议。ARP协议的作用就是将网络层的IP地址转换成数据链路层的MAC地址，以便数据在网络中的传播。具体的协议内容是：
    当A主机向B主机发送消息时，先检查自己ARP缓存中有没有B主机的MAC地址，如果没有的话，广播一个ARP请求报文，然后B主机收到ARP请求报文之后，向A主机回复一个ARP应答报文，其中包含B主机的MAC地址，然后A主机就可以传送数据帧给B主机了。

33. 什么是ARP欺骗攻击
    ARP欺骗攻击就是比如在一个交换式网络环境中，有正常通信的A和B主机，有攻击的主机C，还有一个交换机S。C主机每隔一段时间就向A和B主机发送ARP应答包，告诉他们A的IP地址对应的MAC地址是C的，B的IP地址对应的MAC地址是C的。然后A和B主机就会在ARP缓存中保存这个信息，当A要发送数据给B的时候就会选择C的MAC地址发送
34. ARP攻击技术有哪些
    1. 发送发亮的虚假MAC地址数据报
    2. ARP欺骗攻击
    3. 修改本地MAC地址
35. 怎么样找到ARP攻击的病毒源
    有三种方法
    1. 对网络中任意一台主机进行捕包分析，如果发现有另一个主机一直在发送ARP请求包，那么这就是病毒源
    2. 找两台不能上网的主机，查看和他们通信的设备，如果都有某个主机的话，那这个主机就是病毒源
    3. 在已经中毒的主机上跟踪某个外网地址，第一跳的地址往往就是病毒主机的地址
36. 如何防御ARP攻击
    有下面几种方法
    1. 减少ARP缓存的更新间隔时间
    2. 建立静态的ARP表
    3. 禁止ARP
37. 有哪些典型的DoS攻击
    1. Land攻击
    2. SYN洪水
    3. Smurf攻击
    4. HTTP洪水
    5. CC攻击
38. 什么是SQL注入攻击
    SQL注入攻击就是将恶意的SQL命令注入到后台数据库的行为，SQL注入是网站存在最多也是最简单的漏洞，是一种常见的数据库攻击手段。攻击者可以通过SQL攻击获得敏感信息，篡改数据，甚至控制整个网站。
39. SQL注入攻击的流程有哪些
    1. 寻找注入点
    2. 信息采集
    3. 权限判断
    4. 攻击系统

40. 如何防范SQL注入攻击
    1. 对用户输入的数据进行过滤盒检查，过滤掉不合法的数据
    2. 使用参数化的SQL语句
    3. 限制数据库用户的权限
41. 什么是恶意代码
    恶意代码是一种有害的计算机代码或web脚本，目的是破坏计算机或网络资源的可用性、机密性和完整性。恶意代码包括病毒，蠕虫，木马等
42. 病毒和木马的区别
    1. 病毒主要是依附在电脑某个程序上，当运行这个程序时被激活运行，然后进行大量的复制。而木马大多数本身就是一个程序，只有当运行这个程序的时候木马才会运行
    2. 病毒的主要目的是破坏，而木马的主要目的是获取用户隐私
    3. 病毒具有一定的传染性，而传染性通常不是木马的主要目的
43. 病毒和蠕虫的区别
    1. 病毒主要是依附在电脑某个程序上，当运行这个程序时被激活运行，然后进行大量的复制。而蠕虫大多数本身就是一个程序
    2. 蠕虫主要目的是为了影响整体网络性能和系统性能，通常会通过网络从一台主机感染到其他的主机
44. 什么是DNS协议
    DNS协议是一种应用层协议，将用户提供的域名解析为响应的IP地址，使用端口号53
45. 什么是DNS攻击
    DNS攻击就是利用DNS协议中的弱点和漏洞进行攻击，攻击者通过欺骗DNS服务器或者污染DNS缓存来重定向用户流量，将用户重定向到恶意站点。
46. 什么是网络安全扫描
    是对计算机系统进行相关的安全检测，找出安全隐患和漏洞，有效避免非法入侵。
47. 什么是PGP
    PGP是一套用于信息加密，验证的应用程序，PGP将纯文本更改为代码，用来保护电子邮件，数据文件，驱动器和即时消息的隐私