5.4 信息安全与网络安全

主要考点

1、常见的网络攻击技术
2、安全的分类
3、防火墙技术
4、入侵检测与防御
5、认证
6、报文摘要
7、数字签名和数字证书

常见的网络攻击技术

（1）篡改消息：是指一个合法消息的某些部分被修改、删除、延迟、重新排序等。如修改传输消息中的数据，将“允许甲执行操作”改为“允许乙执行操作”。

（2）伪造（伪装、假冒）：是指某个实体假扮成其他实体，从而以欺骗的方式获取一些合法用户的权利和特权。

（3）重放：是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

（4）拒绝服务(DOS)：是指攻击者不断地对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

（5）窃听（截取）：是指攻击者在未经用户同意和认可的情况下获得了信息或相关的数据。

常见的网络攻击技术

（6）流量分析（通信量分析）：是指攻击者虽然从截获的消息中无法得到消息的真实内容，但攻击者还是能通过观察这些数据报的模式，分析确定出通信双方的位置、通信的次数及消息的长度，获知相关的敏感信息。

（7）字典攻击：一种破解用户密码或密钥的一种攻击方式。事先将所有可能的密码口令形成一个列表（字典），在破解密码或密钥时，逐一将字典中的密码口令（或组合）尝试进行匹配。

（8）社会工程学攻击：是指通过与他人进行合法的交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式。这通常被认为是一种欺诈他人以收集信息、行骗和入侵计算机系统的行为。

（9）SQL注入攻击：把SQL命令插入Web表单的输入域或页面的请求查找字符串，欺骗服务器执行恶意的SQL命令。在某些表单中，用户输入的内容直接用来构造（或者影响）动态SQL命令，或作为存储过程的输入参数，这类表单特别容易受到SQL注入式攻击。

紫依

常见的网络攻击技术

（10）会话劫持：是指攻击者在初始授权之后建立一个连接，在会话劫持以后，攻击者具有合法用户的特权权限。例如，一个合法用户登录一台主机，当工作完成后，没有切断主机。然后，攻击者乘机接管，因为主机并不知道合法用户的连接已经断开，于是，攻击者能够使用合法用户的所有权限。典型的实例是“TCP会话劫持”。

（11）漏洞扫描：是一种自动检测远程或本地主机安全漏洞的软件，通过漏洞扫描器可以自动发现系统的安全漏洞。

（12）缓冲区溢出：攻击者利用缓冲区溢出漏洞，将特意构造的攻击代码植入有缓冲区漏洞的程序之中，改变漏洞程序的执行过程，就可以得到被攻击主机的控制权。

主动攻击与被动攻击

1、主动攻击：

- 主动攻击会导致某些数据流被篡改或者产生虚假的数据流。如：篡改消息、伪造消息、重放和拒绝服务。

2、被动攻击

- 与主动攻击不同的是，被动攻击中攻击者并不对数据信息做任何修改，也不产生虚假的数据流。如窃听、流量分析等攻击方式。

安全的分类

1、物理安全：物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故及人为操作失误及各种计算机犯罪行为导致的破坏。主要是场地安全与机房安全。

2、网络安全：与网络相关的安全。

3、系统安全：主要指操作系统的安全。

4、应用安全：与应用系统相关的安全。

防火墙技术

- 防火墙阻挡对网络的非法访问和不安全数据的传递，使得本地系统和网络免于受到许多网络安全威胁。防火墙主要用于逻辑隔离外部网络与受保护的内部网络。
- 防火墙技术经历了包过滤、应用代理网关和状态检测技术三个发展阶段。

1、包过滤防火墙：

- 它处于网络层和数据链路层，一般有一个包检查块（包过滤器），通过该检查模块，对每一个传入和传出网络的IP包打开进行检查，例如源地址、目的地址、协议和端口等，对于不符合包过滤规则的包进行记录，发出报警并丢弃该包。

优点：（1）过滤型的防火墙通常直接转发报文，它对用户完全透明，速度较快。

（2）包过滤通常被包含在路由器数据包中，所以不需要额外的系统来处理。

缺点：（1）它可以控制站点与网络之间的相互访问，但不能控制传输数据的内容，因为内容是应用层数据。

（2）访问控制粒度太粗糙，不能防范黑客攻击，不能处理新的安全威胁。

防火墙技术

2、应用代理网关防火墙

- 能彻底隔断内网与外网的直接通信，内网用户对外网的访问变成了防火墙对外网的访问，然后再由防火墙转发给内网用户。
- 所有通信都必须经应用层代理软件转发，访问者任何时候都不能与服务器建立直接的TCP连接，应用层的协议会话过程必须符合代理的安全策略要求。
- 优点：可以检查应用层、传输层和网络层的协议特征，对数据包的检测能力比较强。
- 缺点：难以配置，处理速度非常慢。

防火墙技术

3、状态检测技术防火墙

- 它结合了代理防火墙的安全性和包过滤防火墙的高速等优点，在不损失安全性的基础上，提高了代理防火墙的性能。
- 状态监测不仅仅根据规则表来检查每一个进出的包，更考虑了数据包是否符合会话所处的状态，因此提供了完整的对传输层的控制能力，同时也改进了流量处理速度。
- 因为它采用了一系列优化技术，使防火墙性能大幅度提升，能应用在各类网络环境中，尤其是在一些规则复杂的大型网络上。

入侵检测与防御

- 入侵检测与防御技术主要有两种：

1、入侵检测系统(IDS)：注重的是网络安全状况的监管，通过监视网络或系统资源，寻找违反安全策略的行为或遭到入侵攻击的迹象，并发出报警。因此绝大多数IDS系统都是被动的。

2、入侵防御系统(IPS)：是在入侵检测系统的基础上发展起来的，不仅能够检测到网络中的攻击行为，同时可以主动地对攻击行为发出响应，对入侵活动和攻击性网络流量进行拦截，避免造成损失。

1、12年第68题

网络的可用性是指（　）。

A.网络通信能力的大小　　B.用户用于网络维修的时间

C.网络的可靠性　　D.用户可利用网络时间的百分比

2、14年第8题

防火墙的工作层次是决定防火墙效率及安全的主要因素，以下叙述中，正确的是（　）。

A.防火墙工作层次越低，工作效率越高，安全性越高

B.防火墙工作层次越低，工作效率越低，安全性越低

C.防火墙工作层次越高，工作效率越高，安全性越低

D.防火墙工作层次越高，工作效率越低，安全性越高

3、14年第9题

以下关于包过滤防火墙和代理服务防火墙的叙述中，正确的是（　）。

A.包过滤成本技术实现成本较高，所以安全性能高

B.包过滤技术对应用和用户是透明的

C.代理服务技术安全性较高，可以提高网络整体性能

D.代理服务技术只能配置成用户认证后才建立连接

4、15年第8、9题

安全需求可划分为物理线路安全、网络安全、系统安全和应用安全。下面的安全需求中属于系统安全的是（　），属于应用安全的是（　）。

A.机房安全　　B.入侵检测　　C.漏洞补丁管理　　D.数据库安全

A.机房安全　　B.入侵检测　　C.漏洞补丁管理　　D.数据库安全

5、16年第8题

传输经过SSL加密的网页所采用的协议是（　）。

A.HTTP　　B.HTTPS　　C.S-HTTP　　D.HTTP-S

紫依

6、17年第7题

HTTPS 使用（ ）协议对报文进行封装。

A. SSH B. SSL C. SHA-1 D. SET

7、18年第14题

在网络安全管理中，加强内防内控可采取的策略有（ ）

①控制终端接入数量

②终端访问授权，防止合法终端越权访问

③加强终端的安全检查与策略管理

④加强员工上网行为管理与违规审计

A. ②③ B. ②④ C. ①②③④ D. ②③④

8、18年第15题

攻击者通过发送一个目的主机已经接收过的报文来达到攻击目的，这种攻击方式属于（ ）攻击。

A. 重放 B. 拒绝服务 C. 数据截获 D.数据流分析

9、19年第11题

下列攻击行为中，（ ）属于被动攻击行为。

A. 伪造 B. 窃听 C. DDOS攻击 D. 篡改消息

10、19年第12题

（ ）防火墙是内部网和外部网的隔离点，它可对应用层的通信数据流进行监控和过滤。

A. 包过滤 B. 应用级网关 C. 数据库 D. WEB

11、19年第13题

（ ）并不能减少和防范计算机病毒。

A. 安装、升级杀毒软件 B. 下载安装系统补丁 C. 定期备份数据文件 D. 避免U盘交叉使用

紫依

12、20年第13题

以下关于拒绝服务攻击的叙述中，不正确的是（　）。

A. 拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务

B. 拒绝服务攻击是通过不断向计算机发起请求来实现的

C. 拒绝服务攻击会造成用户密码的泄露

D. DDos是一种拒绝服务攻击形式

13、20年第14题

下列不属于社会工程学攻击的是（　）。

A. 攻击者编造一个故事使受害者信服，从而透露秘密消息

B. 攻击者伪造一条来自银行或其他金融机构的需要“验证”登录的消息

C. 攻击者通过搭线窃取了从网络节点A发送到网络节点B的消息

D. 通过电话以知名人士的名义去推销诈骗

14、20年第15题

Linux系统中，文件的权限表示为“-rw-rw-rw-”，下列说法正确的是（　）。

A. 文件所有者拥有读、写和执行权限

B. 文件所在组用户拥有读、写和执行权限

C. 其他组用户拥有读和写权限

D. 其他组用户拥有读和执行权限

紫依

15、21年第12题

攻击者使网络中的服务器充斥着大量需要回复的信息，消耗带宽，导致系统停止正常服务或者响应很慢，这种攻击类型属于（ ）。

A. 盲注入攻击　　B. TCP会话劫持　　C. DDoS攻击　　D. ARP欺骗攻击

16、21年第13题

以下关于蜜罐的叙述中，不正确的是（ ）。

A. 蜜罐对攻击者更有吸引力
B. 对蜜罐的任何连接都被确定为入侵
C. 蜜罐计算机中有吸引力的文件使入侵者逗留并留下证据
D. 蜜罐能够主动发现攻击者

17、21年第14题

不属于SQL注入防范措施的是（ ）。

A. 使用预编译语句，绑定变量　　B. 对用户提交的数据进行严格过滤
C. 使用安全函数　　D. 使用动态SQL语句

18、21年第15题

防止重放攻击最有效的方法是（ ）。

A. 对用户密码进行加密存储　　B. 使用一次一密的加密方式
C. 强制用户经常修改用户密码　　D. 强制用户设置复杂度高的密码

19、21年第31题

防火墙的主要功能不包括（ ）。

A. 包过滤　　B.访问控制　　C. 加密认证　　D.应用层网关

20、21年第32题

下列协议中，属于安全远程登录协议的是（ ）。

A. TLS　　B. TCP　　C. SSH　　D. TFTP

紫依

【22年第12题】（ ）不属于基于生物特征的认证技术。

A.指纹识别　　B.人脸识别　　C. 口令　　D.手写签名

【22年第15题】以下恶意代码中，不需要宿主程序的是（ ）

A.病毒　　B. 蠕虫　　C. 木马　　D. 宏

【22年第32题】某信息系统不断受到SQL注入攻击，应部署（ ）进行安全防护，实时阻断攻击行为。

A. 防火墙　　B. WEB防火墙　　C. 入侵检测系统　　D. 堡垒机

紫依