链滴

自考计算机网络安全 第一章

作者：cxmnb

原文链接：https://ld246.com/article/1586503037298

来源网站：链滴

自考计算机网络安全 第一章(根据考点总结)

一、识记部分

1、计算机网络系统面临的典型安全威胁

主要有窃听,重传,伪造,篡改,非授权访问,拒绝服务攻击(也称为DDOS攻击),行为否认(不承认消息),旁路制,电磁/射频截获,人员疏忽.

2、计算机网络不安全主要因素有哪些

偶发因素:比如电源故障及软件开发过程中留下的漏洞或逻辑错误等。自然灾害:自然灾害对计算机系造成的威胁。人为因素:人为对计算网络的破坏也称为人对计算机网络的攻击。(官方定义好绕口)也分几个方面:1被动攻击。2主动攻击。3领近攻击4内部人员攻击(比如删库跑路)5分发攻击

3、计算机网络的安全定义

计算机网络安全是指利用管理控制和技术措施,保证在一个网络环境里,信息数据的机密性、完整性及使用性受到保护

4、计算机网络安全的目标

1保密性 2 完整性 3可用性 4不可否认性 5可控性

保密性是保证信息不被非授权用户访问

完整性是保证信息在传输过程中不被修改,破坏

可用性是指资源在需要被使用时可使用

不可否认性是保证信息行为人不能否认其信息行为

可控性是指对信息传播和内容具有控制力

5、PPDR模型

PPDR模型是一种常用的网络安全模型,主要由四个部分组成安全策略(Policy),防护(ProtecUon),检测(Dtection),响应(Response)。

安全策略(Policy):是整个网络安全的依据.

防护(ProtecUon):通常是采用一些传统的静态安全技术及方法来实现的,主要有防火墙,加密和认证等法.

检测(Detection):检测是动态响应和加强防护的依据.

响应(Response):响应是解决安全问题的最有效方法.

PPDR模型数学公式表达:(P31页)

公式1:Pt>Dt>Rt

公式2:Et=Dt+Rt,如果Pt=0

6、网络安全的主要技术

1物理安全措施 2数据传输安全技术 3内外网隔离技术 4入侵检测技术 5访问控制技术 6审计技术 7全性检测技术 8防病毒技术 9备份技术 10 终端安全技术

二、领会

1、OSI安全体系结构

1安全服务,也称为安全防护措施。OSI安全体系中定义了五大类安全服务:鉴别服务,访问控制服务,数据密性服务,数据完整性服务,抗抵赖服务。

2安全机制。其基本的安全机制有八种:加密机制,数字签名机制,访问控制机制,数据完整性机制,鉴别交机制,通信业务流填充机制,路由控制和公证机制。

2、网络安全管理的主要内容

1先进的技术 2 严格的管理 3威严的法律

3、网络安全威胁的发展趋势

1与Internet更加紧密地结合,利用一切可以利用的方式进行传播

2所有病毒都具有混合型特征,集文件传染,蠕虫,木马和黑客程序与一身,破坏性大大增加.

3扩散极快,而且更加注重欺骗性

4利用系统漏洞将成为病毒最有的传播方式

5 无线网的发展,使远程网络攻击的可能性加大

6各种境外情报,谍报人员将越来越多地通过信息网络渠道收集情报和窃取资料

7各种病毒、蠕虫和后门技术越来越智能化,并出现整合趋势,形成混合性威胁

8各种攻击技术的隐秘性增强,常规防范手段难以识别

9分布式计算机技术用于攻击的趋势增强,威胁高强度密码的安全性

10 一些政府部门的超级计算机资源将成为攻击者利用的跳板

11 网络管理安全问题日益突出

4网络安全技术发展趋势

网络安全的发展是多维的、全方位的,主要有:1物理隔离 2逻辑隔离 3防御来自网络的攻击 4防御网络的病毒 5身份认证 6 加密通信和虚拟专用网 7入侵检测和主动防卫 8网管、审计和取证