Broadview®
www.broadview.com.cn

“十一五”国家重点图书出版规划项目
国家信息安全等级保护系列丛书

信息安全
等级测评师
培训教程
（初级）

公安部信息安全等级保护评估中心　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“十一五”国家重点图书出版规划项目
国家信息安全等级保护系列丛书

信息安全等级测评师培训教程

初级

公安部信息安全等级保护评估中心　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本教材结合我国信息安全等级保护制度编写，是长期从事信息安全等级测评人员结合等级测评工作实践的总结，根据信息安全等级测评师（初级）岗位特点、能力要求进行编写，用以指导等级测评人员开展信息安全等级测评工作。内容包括：网络安全测评，主机安全测评，应用安全测评，数据安全测评，物理安全测评，安全管理测评，工作测试等内容。

本书为信息安全等级测评师（初级）专用教材，也可作为信息安全测评人员、信息系统运行维护人员、信息系统安全设计、建设和集成人员、大专院校信息安全相关专业人员参考用书。

图书在版编目（CIP）数据

信息安全等级测评师培训教程：初级 / 公安部信息安全等级保护评估中心编著. —北京：电子工业出版社，2010.10
（安全技术大系. 国家信息安全等级保护系列丛书）
ISBN 978-7-121-11811-1

Ⅰ. ①信… Ⅱ. ①公… Ⅲ. ①信息系统－安全技术－技术培训－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2010）第 177999 号

策划编辑：毕 宁 bn@phei.com.cn
责任编辑：高洪霞
文字编辑：毕 宁
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×980 1/16 印张：24 字数：308 千字
印 次：2010 年 10 月第 1 次印刷
印 数：4000 册 定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

信息安全等级保护制度是国家信息安全保障工作的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。国务院法规和中央文件明确规定，要实行信息安全等级保护，重点保护基础信息安全网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度。

信息安全等级保护测评是等级测评是等级保护工作的重要环节，信息系统备案单位通过委托测评机构开展等级测评，可以查找系统安全隐患和薄弱环节，明确系统与相应等级标准要求的差距和不足，有针对性地进行安全建设整改。等级测评工作涉及的信息系统范围广、政策性强，需要建立专门的测评机构专业开展测评工作，需要培养一批专门从事等级测评工作的专业技术人员。

我们结合近些年的工作实践，在公安部网络安全保卫局的指导下，编写了这本教程，对开展信息安全等级测评工作的主要内容和方法进行了介绍，供读者参考、借鉴。本教材除了适用于等级测评师培训外，还适用于信息系统运营使用单位的运维、管理人员，有助于他们在信息系统运行维护和组织本单位系统自查过程中有针对性地开展相应工作。由于水平有限，书中难免有不足之处，敬请读者指正。

本书由公安部信息安全等级保护评估中心组织编写，在编写过程中得到国家网络与信息安全信息通报中心赵林副主任的大力支持和指导，在此表示由衷的感谢。参加编写的有朱建平、马力、李升、陈广勇、于东升、陈雪秀、黄洪、尚旭光、尹湘培、张振峰、黄顺京、江雷等。

读者可以登录中国信息安全等级保护网 www.djbh.net，了解最新情况。

目　录

CHAPTER 1

第 1 章　网络安全测评

信息系统在完成定级确定后，需要依据测评要求，开发现场测评的测评指导书，用于指导测评人员开展现场测评工作。对于信息系统物理安全、安全管理、应用安全和各类设备的安全检查都可以制作成检查表格，在表格中列出现场所要测评的项目、具体操作步骤和方法等，在本书的附录中列出了部分网络设备、主机、管理等方面的检查表格范例供测评人员参考。另外，对现场测评过程中可能用到的测试工具，本书也做了简要介绍。

本书主要以三级系统 S3A3G3 测评为例，以举例的形式介绍测评指导书中所涉及的一些检查步骤和方法，为测评人员开发各类安全检查表格提供一种思路。

网络设备的种类很多，本章主要介绍最常用到的路由器和交换机两类设备的配置和检查方法，并以思科和华为网络设备为例进行说明。

1.1　网络全局

1.1.1　结构安全

a）应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

【描述】

为了保证主要网络设备具备足够的数据处理能力，应定期检查网络设备系统资源占用情况，确保网络设备的业务处理能力具备冗余空间。

【检查方法】

访谈网络管理员，询问信息系统中边界设备和主要网络设备的处理性能能否满足目前业务高峰流量的需求，询问采用何种技术手段对主要网络设备运行状态进行监控。

b）应保证网络各个部分的带宽满足业务高峰期需要。

【描述】

为了保证业务服务的连续性，应保证网络各个部分的带宽满足业务高峰期需要。如果存在带宽无法满足业务高峰期需要的情况，则需要在主要网络设备上进行带宽配置，保证关键业务应用的带宽需求。

【检查方法】

访谈网络管理员，询问网络各个部分的带宽是否满足业务高峰期需要。例如，询问业务应用的高峰流量是多少？各个网络接入链路带宽是多少？是否有过网络带宽瓶颈事件发生？

如果各个网络接入链路带宽无法满足业务高峰期需要，则需要在主要网络设备上进行带宽配置，保证关键业务应用的带宽需求。据此需要核查关键网络设备的配置信息是否存在相关的带宽配置。

c）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。

【描述】

在网络路由配置中主要有静态路由和动态路由。静态路由是指由网络管理员手工配置的路由信息，当网络的拓扑结构或链路的状态发生变化时，网络管理员需要

手工修改路由表中相关的静态路由信息。动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由机制的运作依赖路由器的两个基本功能：对路由表的维护和路由器之间适时的路由信息交换。路由器之间的路由信息交换是基于路由协议实现的，如 OSPF 路由协议是一种典型的链路状态的路由协议，它通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。如果使用动态路由协议应配置使用路由协议认证功能，保证网络路由安全。

【检查方法】

核查边界设备和主要网络设备的配置信息，查看是否进行了路由控制建立安全的访问路径。

检查路由器的配置信息中是否存在路由协议认证。

在思科路由器中：

1）在特权模式下输入命令 show running-config 会输出该路由器相关配置信息。

2）检查配置信息中应当存在类似如下配置信息：

```
interface Serial0
 ip address 192.16.64.1 255.255.255.0
 ip ospf message-digest-key 1 md5 XXXXXX（认证码）

router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.16.64.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

在华为路由器中：

1）在特权模式下输入命令 display current-configuration 会输出该路由器相关配置信息。

2）检查配置信息中应当存在类似如下配置信息：

```
ospf 100
 import-route direct
 import-route static
 area 0.0.0.0

interface Vlan-interface100
ospf authentication-mode md5
```

d）应绘制与当前运行情况相符的网络拓扑结构图。

【描述】

为了便于网络管理和安全运维，应绘制与当前运行情况相符的网络拓扑结构图。当网络拓扑结构发生改变时，应及时更新网络拓扑结构图。

【检查方法】

访谈网络管理员和检查网络拓扑图，查看其与当前运行情况是否一致。

e）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

【描述】

根据组织实际情况、业务应用重要性和安全区域防护要求，应在主要网络设备上进行 VLAN 划分。VLAN 是一种通过将局域网内的设备逻辑而不是物理划分成不同子网从而实现虚拟工作组的新技术。不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信，如果不同 VLAN 要进行通信，则需要通过路由器或三层交换机等三层设备实现。

【检查方法】

访谈网络管理员，是否依据部门的工作职能、重要性和应用系统的级别划分了不同的 VLAN，并检查交换机的配置。

在思科交换机中：

1）在特权模式下输入命令 show vlan 会输出该交换机相关配置信息。

2）检查配置信息中应当存在类似如下配置信息：

```
display vlan static :
 Now, the following static VLAN exist(s):
  1(default), 100, 200, 1203-1204, 2101-2102, 2105-2107, 2109
  2111-2112, 2116-2119, 2148
int e0/2
vlan-membership static 2

int e0/3
vlan-membership static 3ip address 10.1.10.2 255.255.255.0
```

在华为交换机中：

1）在特权模式下输入命令 display vlan all 会输出该交换机相相关配置信息。

2）检查配置信息中应当存在类似如下配置信息：

```
display vlan static
 Now, the following static VLAN exist(s):
  1(default), 100, 200, 1203-1204, 2101-2102, 2105-2107, 2109
  2111-2112, 2116-2119, 2148
display vlan all
VLAN ID: 100
 VLAN Type: static
Description: VLAN 0100
 Name: VLAN 0100
 Tagged   Ports: none
 Untagged Ports:
 GigabitEthernet1/1/1

 VLAN ID: 200
 VLAN Type: static
Description: VLAN 0200
 Name: VLAN 0200
 Tagged   Ports: none
```

```
Untagged Ports:
GigabitEthernet1/1/2
```

f）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

【描述】

为了保证信息系统的安全，应避免将重要网段部署在网络边界处且直接连接外部信息系统，防止来自外部的网络攻击。同时在重要网段和其他网段之间采取可靠的技术隔离手段、配置安全策略进行访问控制。

【检查方法】

访谈网络管理员和检查网络拓扑结构，查看是否将重要网段部署在网络边界处，重要网段和其他网段之间是否采取可靠的技术隔离手段、配置安全策略进行访问控制。如安全区域边界处是否部署防火墙、网闸，或者边界网络设备是否配置并启用ACL。

g）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护重要主机。

【描述】

为了保证重要业务服务的连续性，应按照对业务服务的重要次序来指定带宽分配优先级别，从而保证在网络发生拥堵时优先保护重要主机。

【检查方法】

访谈网络管理员，依据实际应用系统状况是否进行了带宽优先级分配，并检查防火墙和路由器配置。

如果在网络边界处部署防火墙，检查防火墙是否存在策略带宽配置。

如果网络边界处未部署防火墙，检查边界网络设备是否存在相关配置信息。

1.1.2 边界完整性检查

a）应能够对非授权设备私自联到内部网络的行为进行检查，准确定位，并对其进行有效阻断。

【描述】

可以采用技术手段和管理措施对“非法接入”行为进行检查。技术手段包括网络接入控制、关闭网络设备未使用的端口、IP/MAC 地址绑定等。管理措施包括进入机房全程陪同、红外视频监控等。

【检查方法】

访谈网络管理员，询问采用何种技术手段或管理措施对非授权设备私自联到内部网络的行为进行检查、定位和阻断。如果采用技术手段则询问采用了何种技术手段，并在网络管理员的配合下验证其有效性。同时要询问相关的管理措施。

b）应能够对内部网络用户私自联到外部网络的行为进行检查，准确定位，并对其进行有效阻断。

【描述】

主要用来发现和管理用户非法建立通路连接非授权网络的行为，非法外联行为绕过了边界安全设备的统一管理，打破了网络边界的统一控制管理，使得内网面临的安全风险增大。可以依靠内网安全管理系统的非法外联监控功能或者非法外联软件实现，通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致信息泄密。

【检查方法】

访问网络管理员，询问采用了何种技术手段或管理措施对“非法外联”行为进行检查。如果采用技术手段，则询问采用了何种技术手段，并在网络管理员的配合下验证其有效性。