

# 目录

任务一 实施网络安全加固.....	1
1.0 网络安全加固目的.....	1
1.1 网络数据包过滤.....	1
1.1.1 实验环境.....	1
1.1.2 实验步骤.....	1
1.1.3 访问控制.....	1
1.1.4 流量监控.....	1
任务二 实施主机安全加固.....	2
2.0 主机安全加固目的.....	2
2.1 补丁升级与病毒查杀.....	2
2.1.1 漏洞扫描.....	2
2.1.2 系统补丁升级.....	2
2.1.3 杀毒软件的配置与使用.....	2
任务三 实施应用安全加固.....	3
3.0 应用安全加固目的.....	3
3.1 实现安全的远程登录.....	3
3.1.1 网络环境.....	3
3.1.2 远程登录安全性加固与测评.....	3
3.1.3 客户端远程登录 IP 限制加固与测评.....	3
任务四 实施数据安全加固.....	3
4.0 数据安全加固目的.....	3
4.1 数据库备份与恢复.....	3
4.1.1 网络环境.....	3
4.1.2 MySQL 数据库备份与恢复.....	3
4.1.3 SQL 2000 数据库备份与恢复.....	4

## 任务一 实施网络安全加固

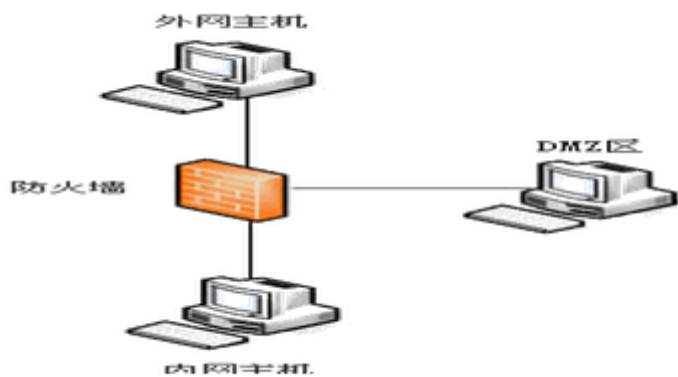
### 1.0 网络安全加固目的

网络安全是企业稳定运行的保障, 通过对企业网络安全进行加固, 可以保护和控制本地网络信息的访问、读写等操作, 避免出现病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁, 可以有效地制止和防御网络黑客的攻击, 避免机要信息的泄露。

### 1.1 网络数据包过滤

#### 1.1.1 实验环境

本参考操作对UTM设备的数据包过滤功能进行设置, 其中包括数据包内容的过滤, 防火墙规则设置, 网络数据流量的监控等。管理员通过配置UTM设备, 通过监测控制网络数据包来加固网络。功能验证过程中需要三台主机配合完成, 分别为一台外网主机、一台内网主机和一台DMZ区主机。






#### 1.1.2实验步骤

1. 启用数据包过滤
2. 功能测试

#### 1.1.3访问控制

1. 网络访问控制
2. 防火墙DNAT规则设置

### 1.1.4 流量监控

1. 选择导航栏中“服务”页下“Traffic Monitoring”，单击“Enable Traffic Monitoring”按钮，开启流量监控。
2. 单击 [administration interface](#) 链接，进入流量监控管理页面。
3. 查看 UTM 设备流量。流量监控的首页显示整个网络的流量状态表。通过查看 Traffic Report for 'br0' 表中的 Traffic 栏中的 Total 值，查看当前网络中的总流量。单击该表右下角的  图标按钮，查看网络流量的历史记录。记录中包含多种协议的网络流量日志。通过选择页面中左上方的下拉列表，查看特定范围的历史记录。单击协议图表右侧的  按钮，可查看该协议的历史记录。

4. IP访问日志。单击导航栏中的“IP”|“Summary”|“Traffic”，可以查看网络中特定IP主机的流量。方便发现网络中主机的流量异常现象。



## 任务二 实施主机安全加固

### 2.0 主机安全加固目的

主机安全是包括服务器、终端/工作站等在内的计算机设备以及在操作系统/数据库系统层面的安全。主机内通常会存放较多重要的文件和数据，往往成为黑客的主要目标，从实际运作来看，主机本身一旦遭遇攻击、病毒破坏或黑客获得了对主机的访问权，就会造成严重的损失和影响。因此需要对主机进行加固，以预防直接从网络内部发动的攻击。

#### 2.1 补丁升级与病毒查杀

##### 2.1.1漏洞扫描

1. QQ医生的安装
2. 打开QQ医生进行修复漏洞扫描，发现系统存在漏洞如下图所示。



### 2.1.2系统补丁升级

1. 系统客户端配置
2. 补丁下载与安装
3. 补丁升级验证

### 2.1.3杀毒软件的配置与使用

1. 获取实验工具
2. 杀毒软件安装与设置

病毒查杀验证

### 任务三 实施应用安全加固

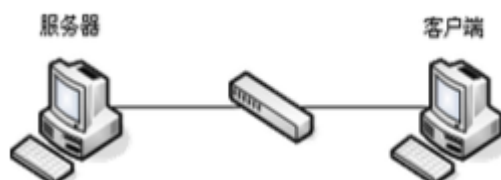
#### 3.0. 应用安全加固目的

应用安全，顾名思义就是保障应用程序使用过程和结果的安全。简言之，就是针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃，通过其他安全工具或策略来消除隐患。应用安全加固是对网络应用的安全保障，对整个系统的安全策略至关重要。

#### 3.1 实现安全的远程登录

##### 3.1.1网络环境

本参考操作需要可以相互通信的2台主机配合完成，分别扮演服务器和客户端(即工作站)两种角色。



##### 1.2 远程登录安全性加固与测评

1. 获取实验工具
2. 安装协议分析软件
3. 安装SSHTServer工具
4. 远程登录安全性分析

3.1.3客户端远程登录IP限制加固与测评

1. 实现SSH远程访问限制

任务四 实施数据安全加固

4.0. 数据安全加固目的

数据安全有对立的两方面的含义:一是数据本身的安全,主要是指采用现代密码算法对数据进行主动保护,如数据保密、数据完整性、双向强身份认证等,二是数据防护的安全,主要是采用现代信息存储手段对数据进行主动防护,如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全,数据安全是一种主动的包含措施,数据本身的安全必须基于可靠的加密算法与安全体系,所以要想保证数据的本身与防护安全,必须对数据安全进行加固。

4.1 数据库备份与恢复

4.1.1 网络环境

一台主机

4.1.2 MySQL数据库备份与恢复

1. 获取实验工具

2. 安装Navicat工具

3. 使用图形工具(Navicat for MySQL)对数据库discuz进行定时备份

4. 删除discuz中的cdb\_access表,模拟数据库遭到破坏 选中root用户下数据库discuz中的cdb\_access表,在右侧的工具栏上单击“删除表”按钮,在弹出的提示框中单击“确定”,完成表cdb\_access的删除。 查看数据库discuz中是否还存在cdb\_access表。

5. 使用图形工具(Navicat for MySQL)对数据库discuz进行恢复

4.1.3 SQL 2000数据库备份与恢复

1. 依次单击“开始”|“程序”|“Microsoft SQL Server”|“服务管理器”,单击“开始/继续”前的按钮,启动数据库服务。2. 将数据库msdb定时备份到D:\backup下

(1) 依次单击“开始”|“程序”|“Microsoft SQL Server”|“企业管理器”,展开左侧目录树,如图所示。

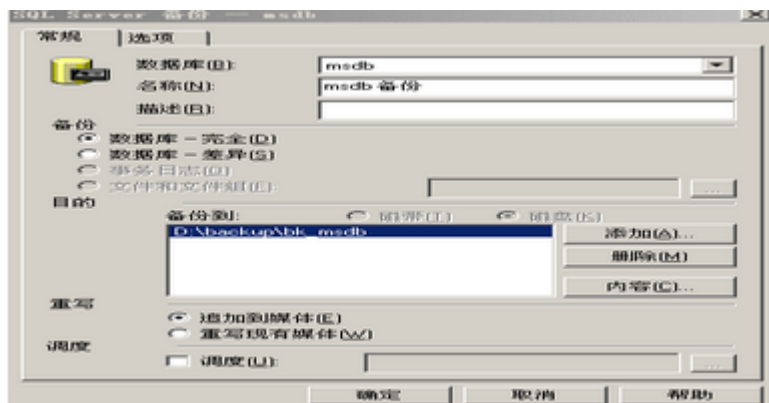


在“管理”目录下,右键单击“SQL Server代理”,选择“启动”。

(3) 在数据库目录下,右键单击“msdb”数据库,选择“所有任务”|“备份数据库”,在弹出窗口中进行如下设置:

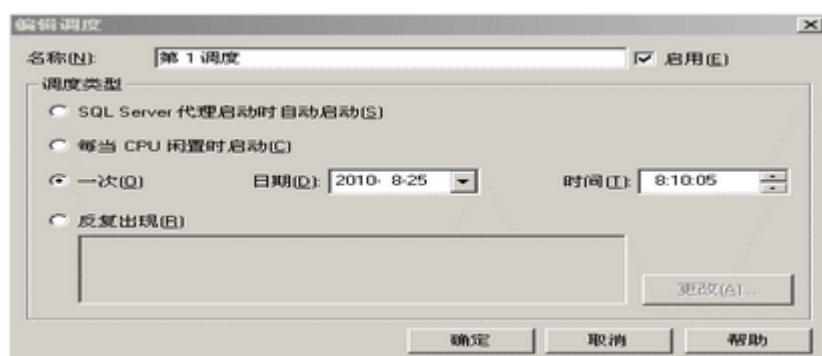
① 设置备份文件名称和存放目录 【注】“备份到:”下面框中如果已有路径,需要先把路径删除,且每次设置备份路径时,都需把之前已存在路径删除。

单击“添加”,在弹出“选择备份目的”对话框中单击右端“.”按钮,输入文件名,如bk\_msdb,选择存放路径为D:\backup(需要自建文件夹),连续单击两个“确定”,回到“SQL Server 备份-msdb”对话框,如图所示:



## ② 定时备份设置

选中“调度”，单击右端“...”按钮，在弹出的“编辑调度”对话框中选择调度类型，可根据实际需要进行选择，这里选择“一次”，如图所示。



4) 在“管理”\“SQL Server代理”目录下，查看“作业”中内容，可看到上一步设置的定时备份任务(如没有，可刷新后再查看)。



5. 选中“调度”，单击右端“...”按钮，在弹出的“编辑调度”对话框中选择调度类型，可根据实际需要进行选择，这里选择“一次”，如图所示。

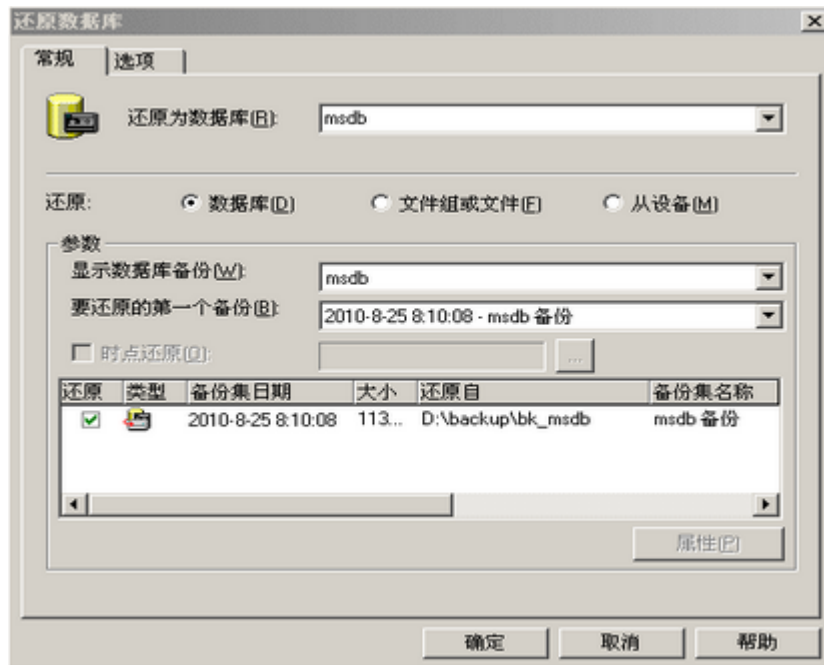
(4) 在“管理”\“SQL Server代理”目录下，查看“作业”中内容，可看到上一步设置的定时备份任务(如没有，可刷新后再查看)。

(5) 定时备份完成后，查看D:\backup目录下，会生成bk\_msdb文件。

3. 删除msdb中的log\_shipping\_databases表，模拟数据库遭到破坏 选中数据库msdb中的log\_shipping\_databases表，将其删除，查看数据库msdb中是否还存在log\_shipping\_databases表。4. 对数据库msdb进行恢复

(1) 在“管理”目录下，右键单击“SQL Server代理”，选择“停止”。

- (2) 在数据库目录下, 右键单击“msdb”数据库, 选择“所有任务”|“还原数据库”。 (3) 在弹出窗口中, 进行如下设置: ① 还原为数据库: msdb; ② 还原: 选择“数据库”;
- ③ 显示数据库备份: msdb;
- ④ 要还原的第一个备份: 在后面的下拉菜单中会给出所有的msdb备份, 选择需要还原的文件即可, 这里选择步骤2/(5)生成的备份, 点击“确定”即可。



查看数据库msdb中是否存在log\_shipping\_databases表(如没有, 可刷新后再查看)。