中等职业教育新课程改革丛书

网络安全与防御

◎ 贾艳光 胡志齐 主编

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

中等职业教育新课程改革丛书

网络安全与防御

主　编　贾艳光　胡志齐

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

内 容 简 介

当今社会是一个高度信息化的社会，信息的传播方式在不断的改进，由有线网络到无线网络，网络已成为人们生活的重要媒介。随着各类安全问题和安全事件暴露于公众视野，网络安全不再单单是重要组织和企业关注的热点，公司的管理人员、技术人员甚至普通员工都应该提高网络安全意识，确保公司网络的安全与稳定。

本书内容涉及网络设备的安全、网络信息的安全和网络软件的安全。内容包括计算机漏洞的监测与修复、病毒的防范、ISA 保护企业安全、UTM 的应用、内网用户的接入的管理、CA 证书服务器的部署与管理、IDS 系统的搭建等。

本书是为中等职业学校网络技术专业的学生编写的，同样适用于网络技术领域的入门者以及职业院校开设计算机网络技术等相关课程的专科学生。

图书在版编目（CIP）数据

网络安全与防御 / 贾艳光，胡志齐主编. —北京：电子工业出版社，2014.6
（中等职业教育新课程改革丛书）

ISBN 978-7-121-22707-3

Ⅰ. ①网… Ⅱ. ①贾… ②胡… Ⅲ. ①计算机网络—安全技术—中等专业学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2014）第 056281 号

策划编辑：肖博爱
责任编辑：郝黎明
印　　刷：北京京师印务有限公司
装　　订：北京京师印务有限公司
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：787×1 092　1/16　印张：10　字数：256 千字
版　　次：2014 年 6 月第 1 版
印　　次：2014 年 6 月第 1 次印刷
定　　价：21.00 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

本书编写立足于北京市中等职业学校计算机网络技术专业网络管理与维护方向的职业能力分析为指导，以《北京市中等职业学校计算机网络技术专业网络管理与维护方向课程标准》中的“网络安全攻击与防御课程标准”为大纲，以岗位项目任务引领，以工作任务为载体，强调理论与实践相结合，体系安排遵循学生的认知规律，注意深入浅出的讲解，把网络安全方面的最新发展成果纳入教材的同时，力争使教材具有趣味性和启发性。

在学习单元的设计上，注重学生学习能力的持续发展。从简单到复杂，从复习任务到新任务。在学习单元一中涉及的工作任务是按照本课程提出的网络安全与防御要求，分别以前期课程的内容（《系统维护》中的企业版杀毒软件部署、《网络安全配置与测试》中防火墙配置部分）作为知识准备和铺垫，进而开展本课程的内容。学习单元二以学习单元一作为铺垫，引入新的网络安全理念和防范技术，增加了任务难度，对网络安全日常巡检中发现的网络攻击行为进行防御、部署统一威胁管理系统保护网络安全等都是当前主流的网络安全技术。学习单元三重点锻炼学生对网络的整体安全防范意识。学习单元遵循“以点到线，以线到面，以面到空间”的认知规律展开，在实践中逐步学习网络安全与防御相关职业技术和方法能力。

学习单元的载体选择

学习单元	载体	载体选择的依据
小型企业网络安全防御	小型企业	小型桌面主机安全与服务器安全、集中杀毒需求、边界网络安全防御需求
中型企业网络安全防御	中型企业	中型企业对网络设备的日常巡检、巡检中发现的对网络设备的攻击进行防御，统一威胁管理系统在中型企业中的应用（防护垃圾邮件、病毒等）
大型企业网络安全防御	大型企业	大型企业中的接入控制和上网认证计费管理，使用入侵检测系统识别大型网络中的攻击行为

由于编者的学术水平有限，时间仓促，书中难免存在不足之处，敬请读者提出宝贵的意见和建议。

编　者

目录

学习单元一　小型企业网络安全防御 ····· 1
工作任务一　小型企业计算机的安全与防御 ····· 3
活动一　扫描计算机漏洞 ····· 3
活动二　扫描计算机系统漏洞 ····· 9
活动三　小型企业病毒防范 ····· 13
工作任务二　小型企业服务器的安全防御 ····· 17
活动一　利用 Apache 缓冲器溢出入侵 ····· 18
活动二　篡改网站首页 ····· 23
工作任务三　使用防火墙对企业网络进行安全防护 ····· 30
活动　使用 ISA 对企业网络进行防护 ····· 31
单元评价与反思 ····· 43
学习单元二　中型企业网络安全防御 ····· 45
工作任务　中型企业计算机的安全与防御 ····· 47
活动一　UTM 的基本配置 ····· 48
活动二　利用 UTM 进行网络病毒控制 ····· 84
单元评价与反思 ····· 94
学习单元三　大型企业网络安全防御 ····· 96
工作任务一　构建大型企业内网系统 ····· 98
活动一　通过 802.1x 认证　管理内网用户的接入 ····· 98
活动二　部署和管理 CA 证书服务器 ····· 119
工作任务二　入侵检测系统的安装与部署 ····· 129
活动一　明确用户需求 ····· 130
活动二　制定网络安全策略 ····· 130
活动三　配置安装 IDS 系统 ····· 130
单元评价与反思 ····· 152

学习单元一

小型企业网络安全防御

[单元学习目标]

知识目标

1. 了解病毒特征和传播方式。
2. 了解网络版杀毒软件的工作方式。
3. 掌握漏洞扫描软件的使用方法。
4. 了解 Apache 服务器的版本。
5. 掌握防火墙的部署和配置方法。
6. 掌握木马的概念。
7. 了解木马的工作原理。

能力目标

1. 能根据需求制定网络安全规范。
2. 能够使用灰鸽子木马远程控制主机。
3. 能够防御网站首页被篡改。
4. 能根据不同的网络环境配置防火墙。
5. 具备用网络杀毒工具发现网络中的病毒并进行防范能力。
6. 具备用漏洞扫描工具，完成网络安全状况扫描的能力。
7. 能够整理和分析防火墙安全日志。
8. 能借助第三方软件评估网络安全。
9. 能收集网络安全需求，有提出网络安全升级建议的能力。

情感态度价值观

1. 团队合作精神。
2. 认真细致的工作态度，逐步树立一切从用户安全需求出发的服务意识。
3. 具备组织协调、管理、沟通能力。

[单元学习内容]

在本单元中你将体验到小型企业办公的安全，小型企业中员工的计算机需要做的安全防范工作，这些工作包括防范病毒、木马，避免因系统漏洞使员工的计算机受到攻击。部署网络版杀毒软件提高员工计算机的安全防范能力，并对改进后的安全状况记录分析。分析网站服务器端的安全现状，防御网站首页被篡改，整理工作日志并对现有系统进行升级。分析小型企业出口安全现状，使用防火墙对企业内网进行保护，包括防火墙的安装与外网接入。根据网络需求，制定安全策略，配置完成防火墙实现内网保护（基础策略制定、搭建动态安全体系实现对应用层的数据过滤），并对防火墙上的安全日志进行审计分析。评估小型企业安全防御现状，提出网络安全防护升级建议。

[单元情景描述]

悠然旅行社在 2010 年 11 月注册并开始运营，目前网络环境如下：

40 台 PC，PC 的系统为 Windows XP。每台 PC 都只有 administrator 账户，密码为空；公司内部的文件服务器也只有 administrator 账户，兼职网管人员为了方便记忆，将密码设置为 123456，有一台面向公网的网站服务器。

1台24口普通100M交换机，机柜及配线架放置在开放的员工休息室，由于员工经常发现上网速度慢，所以经常自己到机柜更换交换机接口。

采用ADSL拨号上网，通过SOHO路由器共享上网，用户名和密码都是默认的admin；公司有时会有客户来访，为了给客户提供方便，无线网络并没有加密。

每台PC都安装了不同的杀毒软件，任何人员在任何时间都可以访问公司的服务器。

公司要求你作为网络安全管理员，对公司的网络运行保驾护航，抵御常见的黑客攻击。

[学习环境]

硬件环境

（1）网络要求：能够接入外网。

（2）网络设备：交换机、路由器、防火墙、服务器、神州数码安全沙盒实验平台。

软件环境

科来网络协议分析软件、木马软件、漏洞扫描软件、网络版杀毒软件、微软基线安全分析器（MBSA）。

工作任务一　小型企业计算机的安全与防御

【任务描述】

为了悠然旅行社企业办公的安全，企业中员工的计算机需要做安全防范工作，这些工作包括防范病毒、木马，避免因系统漏洞使员工的计算机受到攻击。部署网络版杀毒软件提高员工计算机的安全防范能力，并对改进后的安全状况记录分析。

【工作流程】

1．扫描计算机网络漏洞。

2．模拟木马入侵及防护。

3．扫描计算机系统漏洞。

4．部署网络版杀毒软件。

活动一　扫描计算机漏洞

【活动描述】

使用Nmap扫描网络状态。

【岗前培训】

一、关于漏洞

迅速发展的Internet给人们的生活、工作带来了巨大的方便，但同时也带来了一些

不容忽视的问题，网络信息的安全保密问题就是其中之一。安全保密问题中非常常见的就是计算机系统的漏洞。

打个比喻，计算机系统就像一座房子，这座房子是由各种软件和硬件构成的，漏洞就是房子破损的地方，而病毒就是危害房子中人们正常生活的老鼠、蟑螂等害虫。如果房子有破损，老鼠、蟑螂等害虫就会不断从外面进入房子侵扰，有些还会在房子里筑巢繁衍。同样，计算机系统有漏洞，或者说有缺陷，病毒也会趁虚而入，破坏计算机系统的正常工作。如果我们像修房子一样把计算机系统的漏洞堵住，就会在很大程度上减少病毒从外部对系统的攻击。

网络管理的一个基础工作就是维护个人计算机的可用性，减少由于漏洞和病毒构成的威胁。

二、扫描器简介

扫描器是一种自动检查远程或本地主机安全脆弱点的程序，通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配，提供的服务和它们的软件版本，这就能让我们间接地或直观地了解到远程主机所存在的安全问题。使用扫描器还可以采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查，目标可以是工作站、服务器、交换机、数据库应用等各种对象。然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告，为提高网络安全整体水平产生重要影响。

扫描器应该有 3 项功能：发现主机和网络；发现主机上运行的服务；通过测试服务。

三、扫描器功能

其基本功能有三个，一是探测一组主机是否在线；二是扫描主机端口，嗅探所提供的网络服务；三是可以推断主机所用的操作系统。Nmap 可用于扫描仅有两个节点的 LAN，直至 500 个节点以上的网络。Nmap 还允许用户定制扫描技巧。通常，一个简单的使用 ICMP 协议的 Ping 操作可以满足一般需求；也可以深入探测 UDP 或者 TCP 端口，直至主机所使用的操作系统；还可以将所有探测结果记录到各种格式的日志中，供进一步分析操作。

四、扫描参数

GUI 版的功能基本上和命令行版本一样，鉴于许多人更喜欢用命令行版本，本文后面的说明就以命令行版本为主。 下面是 Nmap 支持的 4 种最基本的扫描方式：

（1）TCP connect()端口扫描（-sT 参数）。

（2）TCP 同步（SYN）端口扫描（-sS 参数）。

（3）UDP 端口扫描（-sU 参数）。

（4）Ping 扫描（-sP 参数）。

如果要勾画一个网络的整体情况，Ping 扫描和 TCP SYN 扫描最为实用。Ping 扫描通过发送 ICMP （Internet Control Message Protocol，Internet 控制消息协议）回应请求数据包和 TCP 应答（Acknowledgement， ACK）数据包，确定主机的状态，非常适合于检测指定网段内正在运行的主机数量。

TCP SYN 扫描一下子不太好理解，但如果将它与 TCP connect（half connect）扫描比较，就很容易看出这种扫描方式的特点。在 TCP connect 扫描中，扫描器利用操作系

统本身的系统调用打开一个完整的 TCP 连接——也就是说，扫描器打开了两个主机之间的完整握手过程（SYN，SYN-ACK 和 ACK）。一次完整执行的握手过程表明远程主机端口是打开的。

TCP SYN 扫描创建的是半打开的连接，它与 TCP connect 扫描的不同之处在于，TCP SYN 扫描发送的是复位（RST）标记而不是结束 ACK 标记（SYN、SYN-ACK 或 RST）；如果远程主机正在监听且端口是打开的，远程主机用 SYN-ACK 应答，Nmap 发送一个 RST；如果远程主机的端口是关闭的，它的应答将是 RST，此时 Nmap 转入下一个端口。

Nmap 支持丰富、灵活的命令行参数。例如，如果要扫描 192.168.7.0 网络，可以用 192.168.7.x/24 或 192.168.7.0～255 的形式指定 IP 地址范围。指定端口范围使用-p 参数，如果不指定要扫描的端口，Nmap 默认扫描从 1 到 1024 再加上 nmap-services 列出的端口。如果要查看 Nmap 运行的详细过程，只要启用 verbose 模式，即加上-v 参数，或者加上-vv 参数获得更加详细的信息。例如，nmap -sS 192.168.7.1-255 -p 20，21，53-110，30000- -v 命令，表示执行一次 TCP SYN 扫描，启用 verbose 模式，要扫描的网络是 192.168.7，检测 20、21、53 到 110 及 30000 以上的端口（指定端口清单时中间不要插入空格）。再举一个例子，nmap -sS 192.168.7.1/24 -p 80 扫描 192.168.0 子网，查找在 80 端口监听的服务器（通常是 Web 服务器）。

有些网络设备，例如，路由器和网络打印机，可能禁用或过滤某些端口，禁止对该设备或跨越该设备的扫描。初步侦测网络情况时，-host_timeout 参数很有用，它表示超时时间，例如，nmap sS host_timeout 10000 192.168.0.1 命令规定超时时间是 10000ms。

网络设备上被过滤掉的端口一般会大大延长侦测时间，设置超时参数有时可以显著降低扫描网络所需时间。Nmap 会显示出哪些网络设备响应超时，这时你就可以对这些设备个别处理，保证大范围网络扫描的整体速度。当然，host_timeout 到底可以节省多少扫描时间，最终还是由网络上被过滤的端口数量决定。

【任务实战】

参照图 1-1-1 所示，部署环境。

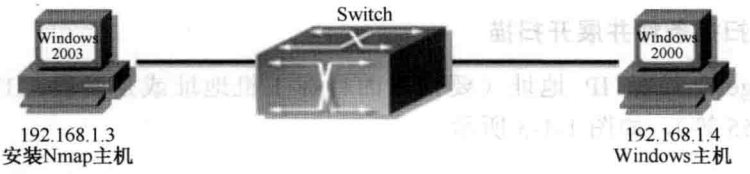

图 1-1-1

一、安装 Nmap

Nmap 要用到一个称为“Windows 包捕获库”的驱动程序 WinPcap——如果你经常从网上下载流媒体电影，可能已经熟悉这个驱动程序——某些流媒体电影的地址是加密的，侦测这些电影的真实地址就要用到 WinPcap。WinPcap 的作用是帮助调用程序（这里的 Nmap）捕获通过网卡传输的原始数据。WinPcap 支持 XP/2K/Me/9x 全系列操作系统，下载得到的是一个执行文件，双击安装，一路确认使用默认设置就可以了，安装好之后需要重新启动。

二、运行 Nmap

运行桌面的快捷方式 Nmap - Zenmap GUI，启动 Nmap，如图 1-1-2 所示。

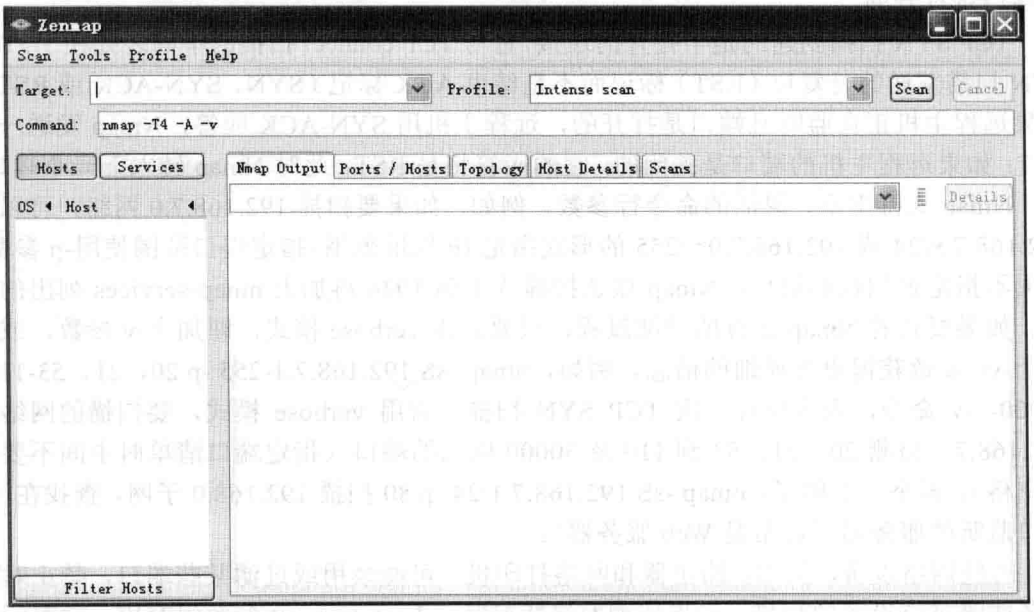

图 1-1-2

小贴士：

Nmap 是一款完全免费的软件，无须注册，需要 WinPcap 支持。

WinPcap（Windows Packet Capture）Windows 数据包捕获器，是 Windows 平台下一个免费的，公共的网络访问系统。WinPcap 是用于网络封包抓取的一套工具，适用于 32 位操作平台解析网络数据包，它包括了核心的包过滤、一个底层动态链接库和一个高层系统函数库。

三、设置扫描条件并展开扫描

设置 Target：目标 IP 地址（要扫描的目标主机地址或是网段，172.16.1.0/24，172.16.1.0～255 等），如图 1-1-3 所示。

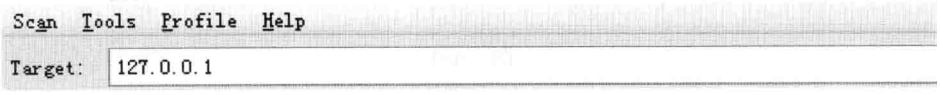

图 1-1-3

Profile：扫描的种类、UDP 或 TCP、快速扫描等，如图 1-1-4 所示。

图 1-1-4

Command：命令行，与 Nmap 的命令行版对应（想了解更多 Nmap 命令行版可以查阅 Nmap 操作手册），如图 1-1-5 所示。

Host：扫描出来的主机，如图 1-1-6 所示。

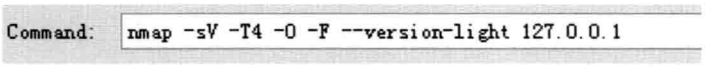

图 1-1-5

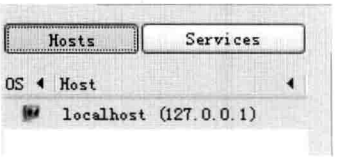

图 1-1-6

Service：列出周知的服务名称，包括对应的端口，如图 1-1-7 所示。

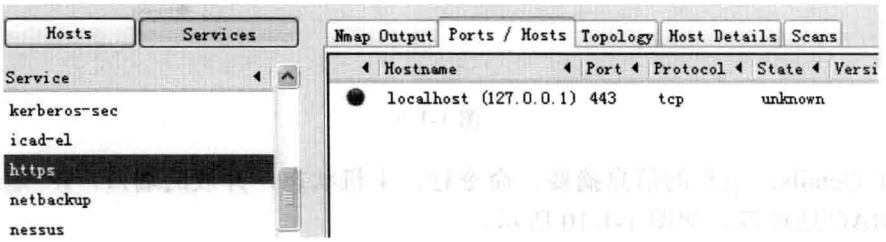

图 1-1-7

Nmap Output：Nmap 输出，包括开始时间、扫描的目标地址、周知端口号、状态和服务等，如图 1-1-8 所示。

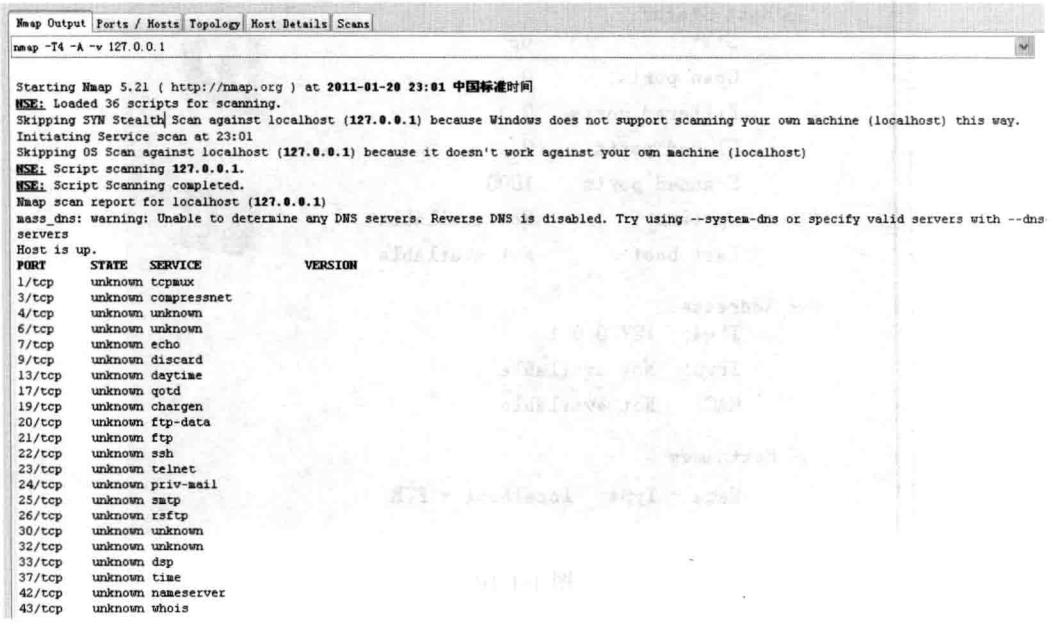

图 1-1-8

Port/Hosts：目标端口、协议、状态、服务及版本。

Topology：逻辑的拓扑结构描述，如图 1-1-9 所示。

图 1-1-9

Host Details：主机的信息摘要。命令行，主机状态，开放的端口，IP 地址，IPv6 地址和 MAC 地址等，如图 1-1-10 所示。

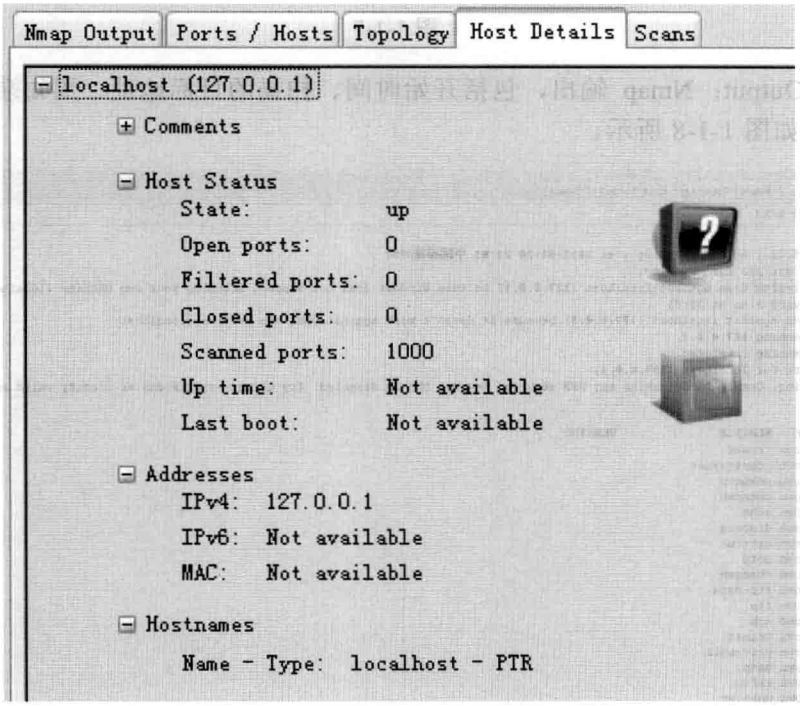

图 1-1-10

四、汇总扫描结果

将扫描结果汇总于表 1-1-1 中。

表 1-1-1　小型企业主机扫描结果表

扫描主机地址	
开放的端口号	
发现的问题	

活动二　扫描计算机系统漏洞

【活动描述】

本次任务的环境为 Windows XP，安装了一些普通的应用工具，并做过一些简单的加固，使用第三方工具 360 等修补了系统中的安全漏洞。

【岗前培训】

在 MBSA 主程序中有三大主要功能。

（1）扫描一个计算机：使用计算机名称或者 IP 地址来检测单台计算机，适用于检测本机或者网络中的单台计算机。

（2）扫描一批计算机：使用域名或者 IP 地址范围来检测多台计算机。

（3）查看已有的安全报告：查看已经检测过的安全报告。

【任务实战】

一、运行 MBSA

单击“开始”→“程序”→“Microsoft Baseline Security Analyzer 1.2”，打开 Microsoft Baseline Security Analyzer 1.2 程序主界面，如图 1-1-11 所示。

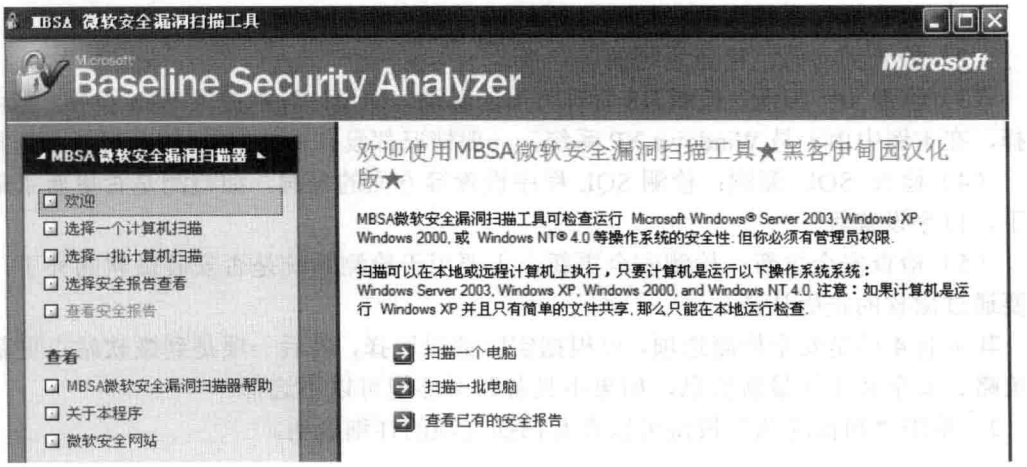

图 1-1-11

二、设置单机 MBSA 扫描选项

1. 选择“扫描一个计算机”选项，接着会出现一个扫描设置的窗口，如图 1-1-12 所示，如果仅仅是针对本机就不用设置“主机名”和“IP 地址”，MBSA 会自动获取本机的计算机名称，如果是要扫描网络中的计算机，则需要在“IP Address”中输入欲扫描的 IP 地址。在 MBSA 扫描选项中，默认会自动命名一个安全扫描报告名称为

%D%-%C% (%T%)，该名称按照“域名-计算机名称（扫描时间）”进行命名，用户也可以输入一个自定义的名称来保存扫描的安全报告。

如图 1-1-12 所示中的“选项”中有 5 个。

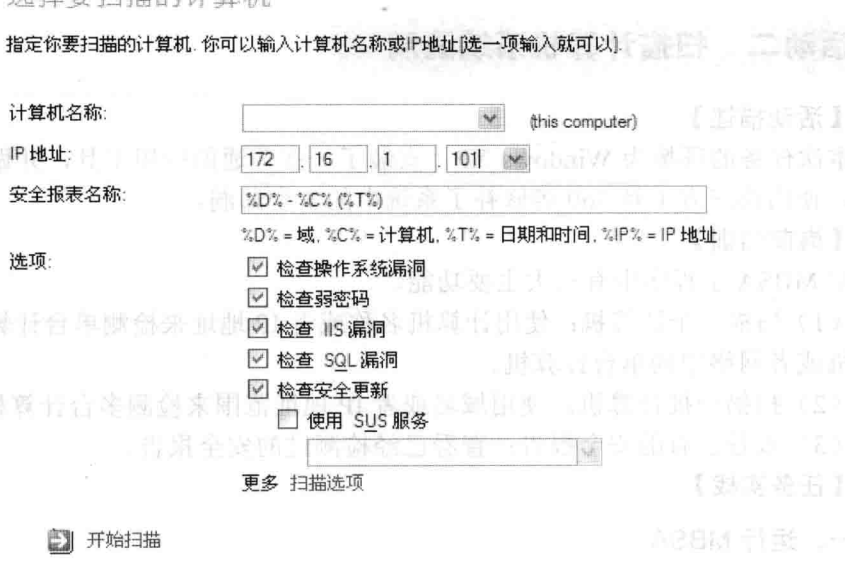

图 1-1-12

（1）检查操作系统漏洞：检测 Windows 管理方面的漏洞。

（2）检查弱密码：检查系统的弱口令。

（3）检查 IIS 漏洞：检测 IIS 管理方面的漏洞，如果计算机提供 Web 服务，则可以选择，在本例中由于是 Windows XP 系统，一般情况都没有安装 IIS，因此可以不选择。

（4）检查 SQL 漏洞：检测 SQL 程序设置等方面的漏洞，如检测是否更新了最新补丁，口令设置等。

（5）检查安全更新：检测安全更新，主要用于检测系统是否安装微软的补丁，不需要通过微软的正版认证。

其中前 4 项是安全检测选项，可根据实际情况选择，最后一项是到微软站点更新安全策略、安全补丁等最新信息，如果不具备联网环境可以不选择。

2．单击“扫描选项”按钮可以查看扫描选项的详细说明。

三、开始进行扫描

如果选择了“开始扫描”命令，程序会进行自动更新，如图 1-1-13 所示，在扫描时会等待一段时间，根据网络连接及更新量大小，有时候等待时间会比较长，直到下载更新信息完毕后才会自动进行安全扫描，在下载过程中有可能出现 CPU 占有率比较高的情况，这是正常的，MBSA 将更新下载到本地后需要对程序和策略进行更新，所有占有率会出现比较高的情况。

开始扫描，扫描结束后，程序会自动跳转扫描结果窗口。

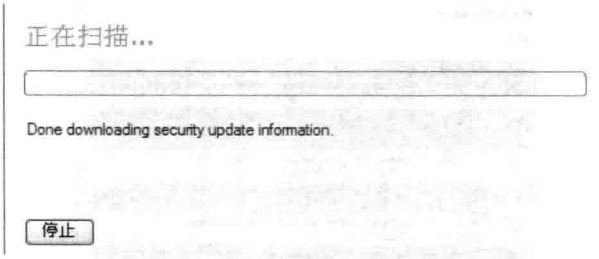

图 1-1-13

四、查看扫描结果

如图 1-1-14 所示，可以查看本次扫描的详细信息。在扫描报告中可以按照“按名称排序”，“按安全性评价排序（最差排第一）”和“按安全性评价排序（最好排第一）”3 种方式进行排序显示扫描结果。在扫描结果中主要有“安全更新扫描结果”、“操作系统扫描结果”、“Internet 信息服务 (IIS) 扫描结果、“SQL 服务扫描结果”和“桌面应用程序扫描结果”5 种。

图 1-1-14

五、分析扫描结果

如图 1-1-15 所示，扫描结果的详细信息如下。

（1）红色或黄色的叉号：表示该项目未能通过测试。

（2）雪花图标：表示该项目还可以进行优化，也可能是程序跳过了其中的某项测试。

（3）感叹号：表示尚有更详细的信息。

（4）绿色的对钩：这当然是最理想的，表示该项目已通过测试。

在那些未能通过测试的项目下面，一般都会提供“已扫描了什么”、“详细结果”和“如何去纠正”等选项，其中第一个将告诉我们分析器在该项目上主要进行了什么测试，而后两项告诉我们详细的结果，及如何做才能够通过这项测试。你只需选择“如何去纠正”选项，就可以按照系统提示去下载补丁程序以修补漏洞了。

图 1-1-15

六、发现的系统问题

本次扫描发现操作系统存在问题。

Automatic Update：Windows 的自动更新被关闭了，下面选择“如何去纠正”选项，出现如图 1-1-16 所示界面。

Automatic Updates Check

Issue

Automatic Updates can keep your computer up-to-date automatically with the latest updates from Microsoft by delivering them directly to your computer from the Windows Update site (or from a local Software Update Services (SUS) server if you are in a managed environment). MBSA will warn users if Automatic Updates is not enabled on the scanned machine, or if it is enabled but is not configured to automatically download and install updates. Automatic Updates is available on Windows® 2000 SP3 machines and higher.

Solution

Enable and configure Automatic Updates to automatically download and install the latest updates from Microsoft. For more information on Automatic Updates settings, please refer to the Knowledge Base article on scheduling Automatic Updates in Windows XP, Windows 2000, or Windows Server 2003 listed below under Additional Information.

Instructions

To configure Automatic Updates to automatically download and install updates on computers running Windows 2000 (SP3 or higher):

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Automatic Updates**.
3. Ensure the checkbox is checked to "Keep my computer up to date".
4. Select the setting to "Automatically download the updates, and install them on the schedule that I specify".

To configure Automatic Updates to automatically download and install updates on computers running Windows XP Home Edition, Windows XP Professional, or Windows Server 2003:

1. Click **Start** and then click **Control Panel**.
2. Double-click **System** and then select the **Automatic Updates** tab.
3. Ensure the checkbox is checked to "Keep my computer up to date".
4. Select the setting to "Automatically download the updates, and install them on the schedule that I specify".

图 1-1-16

其中，Issue：安全更新的作用，Solution：解决方案，Instructions：说明。（Windows 2000 SP3 的用户按照这个步骤来解决这个安全问题：“开始”→“设置”→“控制面板”→“自动更新”→“开启自动更新”；当系统是 Windows XP 或 Windows Server 2003 时使用：“开始”→“控制面板”→“系统”→“自动更新”→“开启自动更新”）。

七、记录系统扫描情况。

将刚刚进行的扫描和分析，汇总于表 1-1-2 中。