Microsoft
Technology
Associate

MICROSOFT 技术关联

学员研究指南

考试 98-367
安全性基础

Microsoft

准备 MTA 认证

MICROSOFT 技术关联 (MTA)
学员研究指南

98-367 安全性基础

作者

Michael Teske（Windows Server 管理与安全）。Michael 在东北威斯康星技术学院从事网络专家计划的教学工作已达 10 年，同时他还拥有 15 年的工程师从业经验。他对于教学和技术都十分热衷，并乐于帮助人们发现工作中的乐趣。Mike 认为学习技术的过程应当是快乐的，但同时他也意识到网络领域的发展日新月异，即使对于最聪明的学生也充满挑战性。Mike 还担任着东北威斯康星几家小型企业的独立顾问，他非常喜欢将现实世界中的真实经历带到日常的课堂教学中。在校内，人们称 Michael 为“微软的那个家伙”。Michael 的目标是在未来的很多年里继续以同样的热情教授网络技术，并帮助他的学生领略到他在这个神奇的行业和事业中所发现的乐趣与激情。Mike 是 MTA 考试复习工具包系列中 Windows Server 考试复习工具包的作者。

Patricia Phillips（主要作者和项目经理）。Patricia 在威斯康星州的简斯维尔教授计算机科学 20 年。她曾在 Microsoft 的国家 K-12 教师顾问委员会任职，并在适用于技术教师的 Microsoft MainFunction 网站从事过两年编辑工作。在过去五年中，她以与 K-12 课程开发和试点方案（包括 Expression Studio Web 设计和 XNA 游戏开发）相关的各种角色与 Microsoft 合作。担任作者和编辑时，Patricia 编写了有关多个主题（包括计算机科学、Web 设计和计算思维）的多篇文章和一本学员练习册。她目前是计算机科学教师联合会新闻稿（语音）的编辑。

目录

简介

MTA 验证了构建块技术概念，并帮助学员通过激动人心且卓有成效的方式追求令人兴奋并且回报丰厚的信息技术 (IT) 职业！作为 Microsoft 技术认证系列的第一步，这一新的入门级认证为学员提供了信心、信誉以及卓尔不群的优势。

了解可以选择的 IT 职业不需要投入很多时间和资源 MTA 考试可以验证您的核心技术知识，这些知识正是今天全世界的企业都需要的。无论您希望成为一名网络管理员，还是软件工程师、Web 开发人员，或者是数据库分析师，MTA 都能帮助您进入正确的门槛。

准备完成 在今天的就业市场中，对 IT 的少量投资即可维持很长一段时间。获得 MTA 认证有助于您为准备开展中级技术研究和获得 Microsoft 认证技术专家 (MCTS) 认证奠定坚实的基础。它还可以帮助您在高校录取方面获得竞争优势，并可帮助您启动 IT 职业规划！

武装自己 作为成为 MCTS 的第一步，MTA 将表明您在技术上的努力，同时您还可以加入拥有五百多万名 Microsoft 认证专家的社区。只要通过 MTA 认证，您就可以向他们学习，并向他们展示 您的能力！

本 MTA 学员研究指南可作为帮助学员准备 MTA 认证考试的学习工具。本指南针对考试中涉及的每项主要主题向学员提出了现实情况下可能会发生的问题。虽然成功完成本研究指南中的练习不能确保您通过 MTA 考试，但这是检验您是否已为参加考试做好准备以及建立考试时的自信心的最佳方式。

祝您在准备开始自己在技术领域的成功职业生涯方面一切顺利！

Victoria Pohto

Victoria Pohto
MTA 产品营销经理

职业规划

大多数基于 Microsoft 技术构建的 IT 解决方案或基础结构均要求下列一个或所有产品，它们通常称为“Microsoft Stack”。

- Microsoft Windows® Server® 作为数据中心或开发平台
- Microsoft SQL Server® 作为数据和商业智能 (BI) 平台
- Microsoft Visual Studio® 作为应用程序生命周期管理工具套件

作为 Microsoft 技术认证的起点，MTA 为有抱负的技术人员提供了继续深造和在技术领域成功实现职业发展所必需的基础知识。

通过准备和通过 MTA 认证，将帮助您了解多种职业道路，而不必在特定职业道路上投入很多时间和资金。在寻找适合您的道路时，Microsoft 学习产品和认证可以指导和帮助您准备更长期的职业规划。

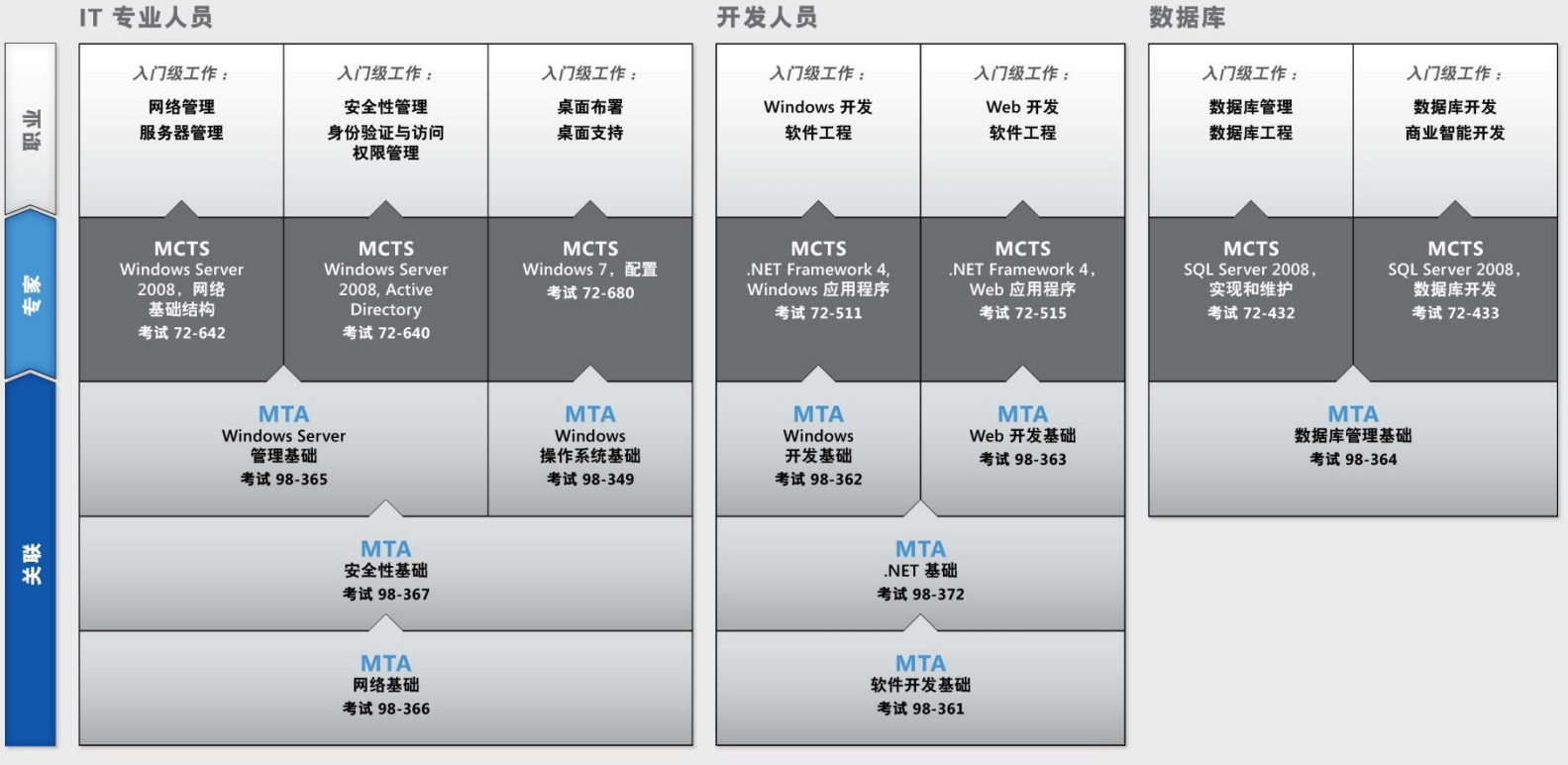
如果您已明确自己要在技术领域开展职业生涯，那么我们建议您采用 MTA 准备与认证作为您的切入点。获得 MTA 认证表明您已经牢牢掌握了基础 IT 概念方面的工作知识，这对于成功开展中级学习以及取得 Microsoft 认证技术专家 (MCTS) 等认证至关重要。此外，Microsoft 认证可以展示个人的自我投入情况和以行业认可的凭证将其知识和技能带到下一级别的信心。

MTA 不是雇主判断您“可以就业”的“职业证明”，但它是面向这个职业目标的第一步，并且可以帮助您在实习或大学入学时脱颖而出。当您准备第一个着重技术的职业时，请确保您有 MCTS 证书 – 验证 Microsoft 产品和技术技能的中级证明。

下一页中的 MTA 认证途径向您介绍了 MTA 考试，在着手参加 Microsoft 的某个中级技术认证（如 MCTS）之前，建议您参加该考试。

Microsoft 技术关联认证途径

MTA 是 Microsoft® 技术认证系列中的第一步。对于 MCTS 考试，MTA 是建议拥有但并非必备的前提条件。每通过一次考试获得一项认证。
《学员研究指南》可供免费下载，网址是：www.certiport.com/mta。



有关完整的 Microsoft 认证方案，请访问 **http://www.microsoft.com/learning/certification（英语）**

探索职业角色

选择职业发展道路是我们人生中的一项重大决策，虽然困难重重，但我们并不孤单！Microsoft 建立了一个职业站点，以帮助学员了解从事 IT 职业的各种选择和可能性。此站点还将您与各种学习资源和学员技术迷社区联系起来，为您准备开始技术职业生涯提供了巨大帮助。

要了解 Microsoft 技术下的职业情况，请访问 *www.microsoft.com/learning/career/en/us/career-org-charts.aspx（英语）*。

数据库管理员

作为数据库管理员，您需负责跨多种平台和环境的重要数据库。在快节奏的环境中，您是一名重要的团队成员。您需要构建能够满足企业需求与安全要求的具有高扩展性的复杂数据库。您不仅是数据库优化、维护和故障排除方面的专家，而且还是设计存档、数据分布以及高可用性解决方案方面的专家。

服务器管理员

作为服务器管理员，您负责实施和管理您的组织中最重要的一些技术，即服务器。您采用广泛的监视和分析工具来管理网络和调试系统，使其能够达到最佳性能。您是 Active Directory® 专家，并且您深入了解网络协议，以及文件和目录安全。

客户支持技术人员

可以考虑通过成为一名客户支持技术人员来开始您的 IT 职业生涯。您无需具备任何正式工作经验，但企业可能会要求您了解如何在具有台式计算机、便携式计算机和打印机的家用网络环境中对操作系统进行安装、管理和故障排除。作为客户支持技术人员，您还需要处理网络、病毒、恶意软件和硬件支持问题。您通常会在中小型公司或组织中发现此职位。

探索职业角色

Web 开发人员

作为 Web 开发人员，您是使用为 Web 注入活力的动态编程工具和语言方面的专家。您可以独立工作，或者作为团队成员为内部和公共站点构建和集成交互式网站、应用程序和服务。您的任务是使它们能够正常运行，即开发 Web 应用程序并在各种浏览器上进行测试，并根据需要对其进行增强和修改，以确保用户获得最佳体验。作为 Web 开发人员，您可能还需要设计网站结构、设计数据驱动的应用程序，以及寻找高效的客户端-服务器解决方案。您必须对软件开发生命周期有深入的了解，并且能够就项目状态、问题以及解决方案进行沟通。

Windows 开发人员

作为 Windows 客户端开发人员，您需要了解如何优化 Windows 代码和跟踪 Bug。但您还需要了解如何使用 Microsoft Visual Studio® 和 Microsoft .NET 框架来设计、开发、测试和部署可以在企业服务器和台式计算机上运行的基于 Windows 的应用程序。您的主要能力包括了解多个 Windows 应用程序模型和 n 层应用程序，以及如何使用面向对象的编程、算法、数据结构和多线程技术。Windows 开发人员对软件工程规则、软件生命周期以及安全性准则具有深入认识。

适用于新开发人员的其他在线资源：

http://msdn.microsoft.com/beginner

http://msdn.microsoft.com/rampup

创新杯

Imagine Cup 是全球重要的学员技术竞赛，在这里，来自全世界的学员可以学习新技能、交到新朋友和改变世界。竞赛包括软件设计、嵌入式开发、游戏设计、数字媒体和 Windows Phone 7。最聪明的头脑利用技术的强大能力， 去解决世界上最困难的问题。

china.imaginecup.com（英语）

认证的价值

技术在我们生活中的各个方面均扮演着重要的角色。自 Microsoft 开始向人们提供其产品和技术认证的 20 多年来，数百万人获得了相关知识、专业技能和证书，从而在可以想象到的每一个商业和社会部门中提高其职业能力、优化业务解决方案并开展创新。当前，信息技术 (IT) 招聘经理通常会使用专业证书（如 Microsoft 认证）来确定 具备所需 IT 技术的候选人。认证成为在众多简历中轻松区分出合格候选人的方法。

根据美国劳工部劳工统计局 (BLS) 的研究报告，IT 专业人员的就业前景非常乐观！BLS 指出，对于计算机支持专家、系统工程师、数据库管理员以及计算机软件工程师岗位，“一直到 2014 年，其增长率均超过所有工作岗位的平均水平”。

从这份研究报告得出的一个重要信息是，无论国家/地区、行业或工作职责，信息和通信技术 (ICT) 技能都是就业市场的入场券。很明显，信息技术是值得投入时间、资源和教育的领域，而技术认证则是教育过程的一个关键部分，作为学习经历的结果，它可以检验学员对产品和技术的掌握水平。

Microsoft IT 认证可以为全球 IT 专业人员、开发人员和信息工作者成功执行关键 IT 功能的能力提供客观的验证尺度。Microsoft 认证代表着丰富、广泛的知识、职业角色和责任。此外，通过获得特定认证，可以客观地证明候选人成功履行重要 IT 职能的能力。Microsoft 认证倍受全球行业专业人员推崇，一直是帮助您实现长期职业目标的最有效方式。

MTA 98-367

安全性基础

1

了解安全层

本章内容

了解核心安全原则

情景：Blue Yonder 航空公司在过去 18 个月里业务发展迅速，最近他们进行了一次安全审核以确保技术系统的安全性，从中确定了若干需要改进的方面。公司 CIO 请求 Blue Yonder 航空公司的安全顾问 Toni Poe 为一线员工提供一些重要安全培训。其目标是向员工传授社会工程学方面的知识以及某些基本安全原则，以此将潜在的安全威胁风险降至最低水平。

Toni 评估了每位员工与计算机访问和外围访问相关的安全权限。Toni 注意到某些员工具有访问 Blue Yonder 航空公司 Intranet 网站的提升权限。他还了解到在其培训中重点讲解“机密性、完整性和可用性”三角概念是非常重要的。

1. **Toni 准备实施最小权限原则。这对员工会有何影响呢？**
   - **a.** 员工将保持其当前对所有资源的访问权限
   - **b.** 员工将获得资源的最小权限集
   - **c.** 员工将不得不以管理员身份登录以访问其资源
2. **下面哪个是与安全培训有关的提供可用性的示例？**
   - **a.** 确保开启所有工作站
   - **b.** 确保所有员工具有完美的出勤率
   - **c.** 防范分布式拒绝服务攻击
3. **下面哪个是社会工程学的示例？**
   - **a.** 假扮他人呼叫某位员工以获取可提供敏感信息访问权限的信息
   - **b.** 在组织内开发安全威胁的社会意识
   - **c.** 构建社交网站

提示

社会工程与社交网络无关。黑客的最终目标是通过利用安全事务中人的因素尽可能获取更多信息。

答案

1. 实施最小权限原则意味着：
   b. 员工将获得资源的最小权限集
2. 与安全培训有关的提供可用性意味着：
   c. 防范分布式拒绝服务攻击
3. 社会工程学的示例是：
   a. 假扮他人呼叫某位员工以获取可提供敏感信息访问权限的信息

重要细节

- **CIA（机密性、完整性和可用性）三角**这一概念是指确保防止未经授权披露信息、错误修改信息和未经授权保留信息或资源。
- **最小权限原则**要求只对系统中的每个主体授予执行授权任务所需的最有限的权限集（或最低许可）。
- **社会工程**是指可能在有意或无意间帮助攻击者获取用户密码或其他敏感信息的访问权的任何类型的行为。

快捷帮助

- **http://technet.microsoft.com/en-us/library/cc875841.aspx**（英语）

了解物理安全性

情景：Erin Hagens 刚刚晋升为 Woodgrove 银行的安全主管。这一职务对于客户资金和信息的安全担负着巨大责任，当然还有银行的信誉。该职务要求她要密切跟进一长串要求以保护 Woodgrove 银行的安全。一家银行业监管机构通知 Erin 要对其银行进行安全审核以确保其符合行业规定和标准。Erin 清楚这一请求并且必须尽职尽责提供监管者在检查潜在安全漏洞时所需的任何信息。她最大的担忧是银行系统的物理安全性。

1. **Erin 可以怎样做以确保银行台式计算机的物理安全性？**
   - **a.** 通过使用组策略禁止使用软盘驱动器或 USB 驱动器
   - **b.** 在每个机柜区域设置一个警卫
   - **c.** 为每个台式计算机采取某种锁定机制，使其无法被搬走
2. **Erin 担心人们会通过身份验证访问数据中心的服务器。她可以怎样防止普通用户登录这些系统？**
   - **a.** 确保将服务器锁起来
   - **b.** 拆除所有服务器的键盘
   - **c.** 创建一个适用于服务器的组策略，针对所有非管理员用户“拒绝本地登录”
3. **Erin 可以怎样防止在银行中使用击键记录器？**
   - **a.** 确保将终端锁定并定期检查系统上的端口
   - **b.** 没有办法 – Erin 无法控制其计算机中都会插入什么
   - **c.** 将所有计算机换成触摸屏显示器

提示

对于银行来说，将所有系统都换成触摸屏可能缺乏财务上的可行性或实际的可能性。

答案

1. 为确保台式计算机的物理安全性，Erin 可以：
   a. **通过使用组策略禁止使用软盘驱动器或 USB 驱动器。**多数计算机确实具有某种将锁定装置与桌面相连接的机制，但禁用 USB 和软盘驱动器可禁防更大的威胁。
2. 要防止普通用户登录系统，Erin 可以：
   c. **创建一个适用于服务器的组策略，针对所有非管理员用户“拒绝本地登录”。**一个更大的问题是数据中心的人们可以实际接触服务器。但是，普通用户应无法以本地方式登录。
3. 要防止在银行中使用击键记录器，Erin 必须：
   a. **确保将终端锁定并定期检查系统上的端口**

重要细节

- **按键记录**（通常称为**击键记录**）是指记录在键盘上输入的键（一般在用户不知情的情况下）的过程。
- **访问控制**是指根据用户标识及其在各种预定义安全组中的成员资格将其访问权限限定为特定信息项或特定控制功能的机制。

快捷帮助

- **http://technet.microsoft.com/en-us/library/bb457125.aspx**（英语）
- **http://www.microsoft.com/smallbusiness/security.aspx**（英语）

了解 Internet 安全性

情景：Terry Adams 是 Tailspin Toys 公司的桌面管理员。为紧跟最新的 Internet 技术，Tailspin Toys 决定将其浏览器升级到 Internet Explorer (IE) 8。Terry 希望确保能够利用浏览器中内置的许多安全功能，同时还能保持公司 Intranet 中的功能。Terry 还希望将其用户培养成为优秀的“Internet 市民”并进行安全的网上冲浪。他清楚 Internet 安全方面的第一道防线就是掌握相关知识与技能的用户。

1. **Terry 希望以如下方式配置 IE 8 中的 Internet 区域功能，即用户可以轻松访问本地 Intranet 上的内容，同时仍然保持较高的安全级别。他应当怎么做呢？**
   - **a.** 创建一个外围网络，确保 Intranet 站点位于其中，并将每个部门中单一一台 PC 指定为 Intranet 浏览 PC (IBPC)
   - **b.** 转到“Internet 选项”，选择“安全”，并将其 Intranet 站点添加到“本地 Intranet 站点”列表中
   - **c.** 每周打印 Intranet 站点的内容并通过内部邮件系统进行分发
2. **Terry 可以告诉其员工通过寻找什么来确保自己位于安全的网站上？**
   - **a.** 浏览器右下角的挂锁和地址栏中的 **https://**
   - **b.** 网站上的联系信息
   - **c.** 他们无法浏览安全网站，因为您不能信任任何站点
3. **受限站点区域中设置的安全级别是什么？**
   - **a.** 低；站点受到限制，因此无需担心
   - **b.** 高；禁用大多数功能，具有最大的安全保护，可防范有害内容
   - **c.** 中；过严和过宽之间的很好的平衡

提示

受限站点区域中的默认级别设置为“高”。

答案

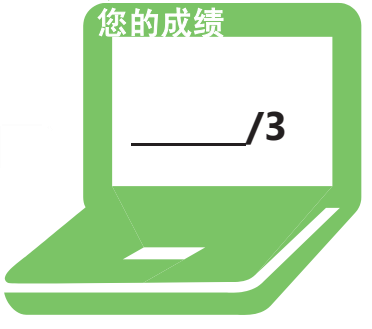
1. 要在 IE 8 中配置 Internet 区域功能并使用户能够轻松浏览本地 Intranet，Terry 应当：
   b. 转到“Internet 选项”，选择“安全”，并将其 Intranet 站点添加到“本地 Intranet 站点”列表中。
2. 为确保员工位于安全的网站上，他们应当寻找：
   a. 浏览器右下角的挂锁和地址栏中的 https://。这并不能保证站点是安全的。但这是一个起点。
3. 受限站点区域中的安全级别是：
   b. 高；禁用大多数功能，具有最大的安全保护，可防范有害内容。

重要细节

- **Internet 区域**包含不在您的计算机或本地 Intranet 上或尚未分配给其他区域的网站。默认安全级别为“中”。
- **安全站点**是指能够提供安全交易的网站，它能保证未经身份验证的用户不能访问信用卡号和其他个人信息。

快捷帮助

- **http://support.microsoft.com/kb/174360**



了解无线安全性

情景：Pilar Ackerman 是 Fourth Coffee 的系统管理员，该公司是一家广受欢迎且盈利颇丰的咖啡厅全国连锁机构。咖啡厅领域的竞争异常激烈！为保持竞争优势，Fourth Coffee 计划在其全部 200 家咖啡厅中为其客户增添开放式高速无线访问，并为其员工提供安全的无线网络。Pilar 面临着多项安全问题，并且必须确保其业务通信的安全。除此之外，他还要承担使这一新功能成为一项取胜战略的压力。

1. **为确保对业务相关通信进行加密，Pilar 可以实施的最安全的协议是什么？**
   - **a.** 有线对等保密 (WEP)
   - **b.** WiFi 安全访问 (WPA) 2
   - **c.** 可扩展的身份验证协议 (EAP)
2. **除了加密业务无线通信以外，Pilar 还可以怎样添加另一个安全级别？**
   - **a.** 实施访问点隔离并隐藏服务集标识符 (SSID)
   - **b.** 在客户到来时关闭业务访问点
   - **c.** 启用 MAC 筛选
3. **Pilar 希望员工在与他联系之前能够独立排除各自的无线连接故障。他可以指导员工采取怎样的基本故障排除步骤？**
   - **a.** 重新启动计算机
   - **b.** 关闭然后开启无线访问点
   - **c.** 右键单击系统托盘中的网络图标并选择“问题故障排除”

提示

关闭然后开启访问点会断开其他用户的网络连接。

答案

1. 为确保对业务相关通信进行加密，Pilar 可以实施的最安全的协议是：
   b. **WiFi 安全访问 (WPA) 2**。EAP 是处理身份验证的安全功能，而 WPA 比 WEP 更安全。
2. Pilar 可以通过以下方式添加另一个安全级别：
   a. **实施访问点隔离并隐藏服务集标识符 (SSID)**。MAC 筛选也是一种选择；但是，MAC 地址可能是“假的”或“欺骗性的”。隐藏 SSID 是一项可以实施的简单安全措施。
3. Pilar 可以指导员工按以下方式进行故障排除：
   c. **右键单击系统托盘中的网络图标并选择“问题故障排除”**

重要细节

- **服务集标识符 (SSID)** 是由 32 个字符构成的唯一标识符，附加在通过 WLAN 发送的数据包的标头中，当移动设备尝试连接到无线 LAN 上的通信站时作为密码使用。
- **Wi-Fi 安全访问 (WPA)** 是旨在提高 WEP 安全功能的 Wi-Fi 标准。
- **有线对等保密 (WEP)** 是作为 802.11 标准一部分的加密算法系统，由电气和电子工程师协会开发，用来作为保护无线 LAN 免遭随意性窃听的安全措施。

快捷帮助

- **http://technet.microsoft.com/en-us/magazine/2005.11.securitywatch.aspx**（英语）
- **http://windows.microsoft.com/zh-cn/windows-vista/What-are-the-different-wireless-network-security-methods**
- **http://www.windowsnetworking.com/articles_tutorials/Securing-Wireless-Network-Traffic-Part1.html**（英语）

2

了解操作系统安全性

本章内容

- 2.1A 了解用户身份验证
- 2.1B 了解用户身份验证
- 2.2 了解权限
- 2.3 了解密码策略
- 2.4 了解审核策略
- 2.5A 了解加密
- 2.5B 了解加密
- 2.6 了解恶意软件

了解用户身份验证

情景：Jim Hance 是 Coho Winery 的安全管理员。在过去的几个月里，各种安全威胁层出不穷，管理问题越来越多。他们无法承受系统受到危害的后果；他们的客户希望能有一个可靠且安全的网站。Jim 正在检查 Coho Winery 的安全策略，

以确定公司需要在哪里增强安全策略，或者至少更新现有策略和安全措施。他的第一项任务是确定公司在用户身份验证方面的强度。

1. **Jim 知道较强的密码是安全计划中的一个重要因素。那么一个强密码都包含哪些特征呢？**
   - **a.** 包含 7 个以上字符；不含用户名、真实名称或公司名称
   - **b.** 包含嵌入在公司名称中的顺序数字
   - **c.** 包含用户的姓氏和电子邮件地址
2. **可以使用哪种协议保护网络上的工作站和计算机身份验证的安全？**
   - **a.** TCP/IP
   - **b.** Kerberos
   - **c.** 轻量目录访问协议
3. **Jim 可以采取哪种战略来减少用户访问特定资源时所必须进行的身份验证次数？**
   - **a.** 双重身份验证
   - **b.** 数字证书
   - **c.** 单一登录 (SSO)

提示

减少用户必须进行身份验证的次数可以降低其凭据被捕获的可能性。

答案

1. 强密码：
   a. **包含 7 个以上字符；不含用户名、真实名称或公司名称**
2. 要保护网络上的工作站和计算机身份验证的安全，Jim 可以使用：
   b. **Kerberos**
3. 要减少用户访问特定资源时所必须进行的身份验证次数，Jim 可以实施：
   c. **单一登录 (SSO)**

重要细节

- **身份验证**是获取用户的身份凭据（如名称和密码）并根据某个颁发机构对这些凭据进行验证的过程。
- **Kerberos** 对尝试登录网络的用户的标识进行身份验证并通过密钥加密措施加密其通信。
- **轻量目录访问协议 (LDAP)** 是设计为在 TCP/IP 堆栈上工作以提取来自层次结构目录（如 X.500）的信息的网络协议。
- **远程身份验证拨入用户服务 (RADIUS)** 是一种 Internet 协议，其中一个身份验证服务器会将授权和身份验证信息提供给用户试图链接的网络服务器。

快捷帮助

- **http://www.microsoft.com/windowsserver2008/en/us/ad-main.asp**（英语）
- **http://web.mit.edu/Kerberos/#what_is**（英语）
- **http://technet.microsoft.com/en-us/library/bb463152.aspx**（英语）

了解用户身份验证

情景：Graphic Design Institute (GDI) 拥有超过 30,000 名学生。学生个人信息（包括财务数据、地址、家庭联系方式、特殊健康需求和成绩等）的安全是网络管理团队的首要任务。然而，在过去的几个月里，学生数据曾多次受到威胁。个人数据出现在社交网站上，这令网络团队倍感难堪。GDI 官员要求网络管理员 Todd Rowe 为学生采取更强的身份验证措施，并杜绝 IT 员工凭借提升的权限进行登录的现象。Todd 具有多种选择，但他意识到对于咨询台员工，过程需要相对简单。

1. **Todd 希望实施双重身份验证。他可以使用什么呢？**
   - **a.** 智能卡和用户密码
   - **b.** 两个密码
   - **c.** 两个用户 ID 及两个密码
2. **GDI 员工可以采用哪种服务取代使用提升的权限登录？**
   - **a.** 远程桌面
   - **b.** 辅助登录-身份
   - **c.** 域用户管理器
3. **使用生物特征识别的缺点是什么？**
   - **a.** 用户必须有手
   - **b.** 对于很多组织来说成本过高
   - **c.** 视网膜扫描可以伪造

提示

生物特征识别极为安全；但是，支持生物特征的设备成本过于高昂。

答案

1. 要实施双重身份验证，Todd 可以使用：
   a. **智能卡和用户密码**
2. 不使用提升的权限登录，员工可以采用：
   b. **辅助登录-身份**
3. 使用生物特征识别的缺点是：
   b. **对于很多组织来说成本过高**

重要细节

- **证书**是在 Internet 和 Intranet 上验证用户身份的电子凭据。
- **公钥基础结构 (PKI)** 是使用密钥对进行加密的一种不对称方案：公钥用于加密数据，对应的私钥用于解密数据。
- “运行为”命令允许用户以不同于当前登录所提供权限的权限运行特定工具和程序。
- 更改密码的步骤：
  - 按 <Ctrl><Alt><Del> 并选择“更改密码”
- 使用“辅助登录”或“运行为”的步骤...
  - 右键单击应用程序图标并选择“以管理员身份运行”

快捷帮助

- **http://technet.microsoft.com/zh-cn/library/cc782756(WS.10).aspx**
- **http://technet.microsoft.com/zh-cn/library/cc756862(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc261673(office.12).aspx**（英语）

了解权限

情景：Fabrikam, Inc. 最近进行了一项基本重组和各种公司变革。Shawn Richardson 是 Fabrikam 的网络管理员，受命按照新的组织情况安排公司的服务器。第一步，Shawn 完成了公司的 Microsoft® Windows Server® 2008 R2 文件服务器的安全审核，并确定需要根据公司重组情况修订文件夹和共享安全性。Shawn 必须将其计划呈报给管理层并指导其团队成员完成该项目。

1. **Shawn 注意到文件系统中的某些共享没有安全保护。创建共享时默认的权限设置是什么？**
   - **a.** 每个人都具有读取权限
   - **b.** 管理员具有完全控制权限
   - **c.** 每个人都具有完全控制权限
2. **为什么 Shawn 应当在域中强制实施用户帐户控制 (UAC)？**
   - **a.** 这样他便可以控制用户帐户
   - **b.** 有助于防止对域中的计算机进行未经授权的更改
   - **c.** 允许用户使用管理员密码进行身份验证以执行管理任务
3. **在重新分配权限时，利用哪种功能（Active Directory 对象也可使用此功能）才能不必为每个父文件夹和子文件夹分配权限，从而简化 Shawn 的工作？**
   - **a.** 批处理文件
   - **b.** 继承
   - **c.** 员工

提示

继承允许将权限或特权从父对象传播至子对象。可以阻止或删除此功能。

答案

1. 创建共享时，默认权限为：
   a. 每个人都具有读取权限
2. Shawn 应当在域中强制实施用户帐户控制 (UAC)，因为：
   b. 有助于防止对域中的计算机进行未经授权的更改
3. 在重新分配权限时，利用以下功能可简化 Shawn 的工作：
   b. 继承

重要细节

- **权限**包括“完全控制”、“修改”、“读取和执行”、“列出文件夹目录”、“读取”以及“写入”；权限可以应用于文件夹对象和文件对象。权限还可应用于 Active Directory 对象。
- **继承这一概念是指将权限从父对象传播至某个对象。**继承可出现在文件系统权限和 Active Directory 权限中。它不适用于共享权限。
- **新技术文件系统 (NTFS)、FAT 和 FAT32。**NTFS 与 FAT 文件系统之间的主要区别在于为文件系统应用安全性的能力。您可以在 NTFS 上授予或拒绝各种权限。NTFS 还支持加密数据的功能。
- **共享权限和 NTFS 权限**根据资源的访问方式来应用。共享权限在通过网络访问资源时才会生效，而 NTFS 权限将始终有效。当共享权限和 NTFS 权限应用于同一资源时，将采用最具限定性的权限。

快捷帮助

- **http://technet.microsoft.com/zh-cn/library/cc730772.aspx**
- **http://technet.microsoft.com/zh-cn/library/cc771375.aspx**
- **http://technet.microsoft.com/zh-cn/library/cc770906(WS.10).aspx**

了解密码策略

情景：Jay Hamlin 受命为 Wingtip Toys 实施强密码策略，这是一项艰巨任务。他清楚公司需要最短长度的复杂密码，但在使员工了解整个 Wingtip Toys 公司的安全如何依赖于这些耦合要求以及他计划采取的其他一些措施时遇到了困难。他还必须确定在锁定用户帐户之前用户可以尝试登录的次数，用户必须更改密码的频率，以及用户可以重复使用所喜欢的密码的频率。

他的密码复杂性策略计划包括以下密码条件：

- 不能包含用户的登录名
- 至少包含 6 个字符或更多
- 必须包含以下四个字符中的三个：大写字母、小写字母、数字和特殊字符

1. **如果 Jay 将密码要求的难度设置得过高，他将面临怎样的困境？**
   - **a.** 复杂密码难猜且难记
   - **b.** Jay 在工作中将不再有朋友
   - **c.** 用户不会使用密码
2. **密码最长使用期限策略是指什么？**
   - **a.** 确定用户必须达到多大年龄才能创建密码
   - **b.** 是指之后必须更改密码的持续使用时间
   - **c.** 是指密码必须使用多长时间之后才允许用户更改密码
3. **将“强制密码历史”的值设置为 10 将发生什么？**
   - **a.** 用户在验证其密码时可以尝试 10 次
   - **b.** 密码必须至少使用 10 天，然后才能更改密码
   - **c.** 系统会记住最后的 10 个密码并且不允许用户重复使用前 10 个密码中的任何密码

提示

密码历史记录可防止用户重复使用其密码。

答案

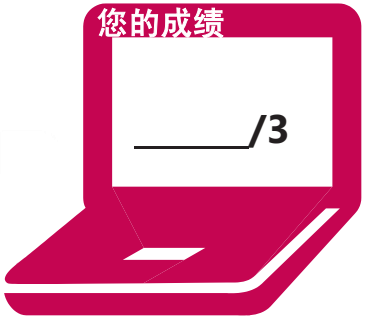
1. 难度过高的密码要求会使 Jay 面临以下困境：
   a. **复杂密码难猜且难记**
2. 密码最长使用期限：
   b. **是指之后必须更改密码的持续使用时间**
3. 将“强制密码历史”的值设置为 10 时：
   c. **系统会记住最后的 10 个密码并且不允许用户重复使用前 10 个密码中的任何密码**

重要细节

- **帐户锁定**是 Windows 中的一项安全功能，根据安全策略锁定设置，当在指定时间内失败的登录尝试达到一定次数时，将锁定用户帐户。
- **密码攻击**是计算机或网络上的一种攻击，是指密码被盗并被破解或被密码字典程序披露。
- **密码探查**是黑客采用的一种技术，通过截获数据包并在其中搜索密码来捕获密码。
- Microsoft Windows Server 2008 允许使用细化的密码策略，即允许在 Active Directory® 中为整个组织指定更灵活的密码策略。

快捷帮助

- **http://technet.microsoft.com/zh-cn/library/cc784090(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc875814.asp**（英语）



了解审核策略

情景：Margie's Travel 的网络必须非常安全。其中的文件包含客户信息，其中包括信用卡号、生日、地址以及护照的复印件。如果系统被黑客攻入，就真有可能会发生身份盗用事件。显然，这种风险是 Margie's Travel 所不能接受的。

Arlene Huff 是 Margie's Travel 的系统管理员。公司要求她跟踪谁试图登录系统以及试图登录的时间。他们还要求她创建一个系统以跟踪何时以及由谁打开了机密文件。Arlene 很高兴地接受了这项任务，这对她来说并不是一个难题。

1. **Arlene 希望在有人以管理员身份登录系统失败时进行记录，但为什么她在他们成功登录时也要记录呢？**
   - **a.** 确定是否有人以及何时使用提升的权限成功进行了身份验证
   - **b.** 确保他们成功登录而没有任何问题
   - **c.** 监控计算机上的驱动器空间
2. **当启用审核时，在何处写入文件审核事件？**
   - **a.** 审核事件日志
   - **b.** pfirewall.log
   - **c.** 安全事件日志
3. **适当保护审核日志的安全为什么很重要？**
   - **a.** 这样潜在的黑客便无法删除事件日志以掩盖其踪迹
   - **b.** 这并不重要，没有人会查看审核日志
   - **c.** 这样只有获得授权的人员才能查看日志文件

提示

技艺高超的计算机黑客会在完成信息的获取后修改审核日志，使其看起来从未有黑客光临过。

答案

1. Arlene 希望在有人成功登录系统以及登录失败时进行日志记录，目的是：
   a. **确定是否有人以及何时使用提升的权限成功进行了身份验证。**如果有人失败了四次，然后在第五次取得成功，则可能表明是黑客活动。
2. 启用的文件审核事件写入到：
   c. **安全事件日志**
3. 适当保护审核日志的安全很重要
   a. **这样潜在的黑客便无法删除事件日志以掩盖其踪迹**

重要细节

- **审核**是操作系统用来检测和记录安全相关事件（如试图创建、访问或删除文件和目录等对象）的过程。
- **审核策略**是确定要报告给网络管理员的安全事件的策略。
- **安全日志**可由防火墙或其他安全设备生成，其中会列出可能影响安全性的事件，例如访问尝试或命令，以及所涉及的用户的名称。

快捷帮助

- **http://technet.microsoft.com/zh-cn/library/dd408940(WS.10).aspx**
- **http://technet.microsoft.com/zh-cn/library/dd349800(WS.10).aspx**

了解加密

情景：Adventure Works 最近扩充了其移动销售员工队伍。管理团队最近意识到数百台便携式计算机同时分布在数百个未加安全防护的位置所带来的特殊安全问题。

David Johnson 是负责 Adventure Works 移动销售员工队伍的网络管理员。最近他受到来自管理团队的事关敏感数据的重压，如果其中的任何便携式计算机被盗或放置不当，这些敏感数据就可能会落入竞争对手的手里。他们必须找到一种解决方案，能够确保移动站上的数据的机密性，它们运行的都是 Windows® 7 Enterprise— 他们需要尽快获得这一解决方案！

1. **David 可以启用哪种功能来确保数据的安全？**
   - **a.** 加密文件系统 (EFS)
   - **b.** 密码保护屏幕保护程序
   - **c.** BitLocker
2. **必须配置哪一项以确保可以回收 Bitlocker® 存储？**
   - **a.** 销售人员的个人标识和登录凭据
   - **b.** BitLocker 以使用数据恢复代理
   - **c.** 秘密检索代理
3. **在决定使用 BitLocker 时，David 必须认真考虑哪些事项？**
   - **a.** 销售员工的责任心和自律性
   - **b.** 硬件的部署，因为 BitLocker 需要一个系统保留分区
   - **c.** 这很简单，没有什么重要的考虑事项

提示

Bitlocker 要求在标准安装过程中创建一个系统保留分区。

答案

1. 为确保数据的安全，David 必须启用：
   c. BitLocker
2. 为确保在 Bitlocker 保护的存储移动到另一台计算机时能够回收所保护的数据，管理员必须创建并适当存储：
   b. BitLocker 以使用数据恢复代理
3. 使用 BitLocker 时，管理员必须考虑：
   b. 硬件的部署，因为 BitLocker 需要一个系统保留分区

重要细节

- **BitLocker (ToGo)** 驱动器加密是 Windows Server 2008 R2 和某些版本的 Windows 7 中提供的一种数据保护功能。
- **加密文件系统 (EFS)** 是一项 Windows 功能，允许您将信息以加密格式存储在硬盘上。
- **加密**是将数据编码以防止未经授权的访问的过程，尤其是在传输过程中。

快捷帮助

- **http://technet.microsoft.com/en-us/windows/dd408739.aspx**（英语）
- **http://technet.microsoft.com/zh-cn/library/cc732774.aspx**
- **http://technet.microsoft.com/zh-cn/library/ee706523(WS.10).aspx**
- **http://technet.microsoft.com/zh-cn/library/ee706518(WS.10).aspx**

了解加密

情景：Southridge Video 的所有者对于她与海岸上下各分支机构经理的密切关系深感自豪。每周的沟通是维系关系和掌握业务进展情况与所面临困难的关键。

所有者和经理们希望将其周一的电话早间会议取代为公司总部与各分支机构之间的安全的周一视频早间会议。他们要求 WAN 管理员 Jeff Wang 创建一个经济高效的解决方案。该解决方案必须能够在远程分支机构之间工作，而在分支机构间建立专用连接会过于昂贵。因此，最佳解决方案是利用每个分支机构的 Internet 连接。

1. **怎样才能在非安全网络上创建安全连接？**
   - **a.** 虚拟专用网络 (VPN)
   - **b.** 在其路由和远程访问服务器上配置回调功能
   - **c.** 使用社交网站召开会议
2. **Jeff 需要在点对点隧道协议 (PPTP) 与第 2 层隧道协议 (L2TP) 之间做出取舍。哪种协议更安全？**
   - **a.** PPTP
   - **b.** L2TP
   - **c.** 都不安全，它们都会以明文传递信息
3. **什么是公用证书？**
   - **a.** 为表彰卓越的业务安全策略而颁发的一种奖励
   - **b.** 一种两部分加密中不与其他各方共享的那部分
   - **c.** 一种数字签名的声明，通常用于身份验证以及开放网络上的信息

提示

私钥证书是两部分加密中驻留在发起计算机上且不共享的那部分。

答案

1. 可以通过以下方式在非安全的网络上创建安全连接：
   a. **虚拟专用网络 (VPN)**
2. 更安全的协议是：
   b. **L2TP**。PPTP 使用 MPPE 实现安全性，其安全性不如 L2TP，后者使用 IPsec 作为其加密方法。
3. 公用证书是：
   c. **一种数字签名的声明，通常用于身份验证以及开放网络上的信息**

重要细节

- **第 2 层隧道协议与 Internet 协议安全 (L2TP/IPSec)** 是使用 IPsec 进行加密的 PPTP 与第 2 层转发 (L2F) 的组合。
- 用户将**私钥**保密并使用它加密数字签名和解密收到的邮件。
- 用户向公众发布**公钥**，公众可以使用它加密要发送给用户的消息以及解密用户的数字签名。
- **虚拟专用网络 (VPN)** 是穿越公用网络（如 Internet）的受保护隧道，其中使用加密技术以防止数据被未经授权的用户截获和了解。

快捷帮助

- **http://technet.microsoft.com/en-us/library/cc700805.aspx**（英语）

了解恶意软件

情景：Consolidated Messenger 为很多领域的商家处理客户反馈。每天他们都会收到来自满意或不满意客户的数千封电子邮件，并将其分发至其客户公司的相应个人。

Mary Kay Anderson 是 Consolidated Messenger 的系统管理员。该公司的网络上曾出现过几次病毒，似乎是通过电子邮件传播的。他们要求 Mary Kay 主持一个“午餐学习会”，为 Consolidated Messenger 员工讲解一些有关恶意软件和电子邮件的知识。Mary Kay 还受命寻找一种可以更好地保护系统的解决方案。

1. **当员工收到来自客户或同事的包含嵌入的超链接的可疑电子邮件时应怎样做？**
   - **a.** 删除电子邮件，然后与 Mary Kay 以及该客户或同事联系
   - **b.** 立即单击超链接，看看会发生什么，以便对威胁做出评估
   - **c.** 将电子邮件转发给其他同事，警告他们该电子邮件不合法
2. **Mary Kay 可以怎样防止可疑电子邮件进入其网络？**
   - **a.** 安装 Microsoft® Forefront® 和 Threat Management Gateway 并将其配置为阻止恶意电子邮件
   - **b.** 禁用 Internet 电子邮件
   - **c.** 警告同事如果他们再转发任何电子邮件就将其开除
3. **Mary Kay 可以下载哪种工具来删除恶意软件？**
   - **a.** 远程服务器管理工具 (RSAT)
   - **b.** Microsoft Windows Malicious Software Removal Tool
   - **c.** 任何网上宣传的安全软件工具 — 它们都是一样的

提示

恶意软件删除工具包含在 Windows 更新中。

答案

1. 当员工收到包含嵌入的超链接的可疑电子邮件时，他们应当：
   a. **删除电子邮件，然后与 Mary Kay 以及该客户或同事联系。**绝不要转发包含可疑内容的电子邮件。如果电子邮件带有附件或链接，请与发件人联系并确认对方是否发送了该邮件。
2. 要防止可疑电子邮件进入网络，Mary Kay 可以：
   a. **安装 Microsoft Forefront 和 Threat Management Gateway 并将其配置为阻止任何恶意电子邮件。**Exchange Server 具有若干垃圾邮件筛选工具。Forefront 和 TMG 是附加安全措施，可以更好地保护系统。
3. 要删除恶意软件，Mary Kay 可以下载：
   b. **Microsoft Windows Malicious Software Removal Tool**

重要细节

- **Bot** 是可在网络上执行某种任务的程序，尤其是重复性或耗时的任务。
- **Rootkit** 是黑客可用来获取未经授权的远程计算机访问权限并启动附加攻击的软件程序的集合。
- **间谍软件**有时也称为 spybot 或跟踪软件。间谍软件使用其他形式的欺骗性软件和程序在计算机上执行特定活动，而无需获取用户的适当许可。
- **特洛伊木马**是一种看似有用或无害的程序，实际上包含隐藏代码，意图操控或损害运行该木马的系统。
- **蠕虫**使用自我传播的恶意代码，可以自动通过网络连接将自身从一台计算机分发到另一台计算机。

快捷帮助

- **http://www.microsoft.com/downloads/details.aspx?FamilyId=F24A8CE3-63A4-45A1-97B6-3FEF52F63ABB&displaylang=en**（英语）
- **http://support.microsoft.com/kb/889741**

3

了解网络安全性

本章内容

- 3.1 了解专用防火墙
- 3.2 了解网络访问保护 (NAP)
- 3.3A 了解网络隔离
- 3.3B 了解网络隔离
- 3.4 了解协议安全

了解专用防火墙

情景：Matt Berg 已经获得了多个 Microsoft 证书，现在他是一名独立安全顾问，自己给自己当老板。Trey Research 聘请他提供服务，执行其网络的安全评估。Trey Research 具有多台暴露于 Internet 的服务器，他们担心自己的内部网络可能容易受到攻击。他们有一个外围防火墙，但他们不清楚这是否足够。Matt 的工作就是对状况进行评估并给出 Trey Research 可以如何保护其数据的建议。

1. **对于暴露于 Internet 的服务器，Matt 应为 Trey Research 提供什么建议？**
   - **a.** 创建一个外围网络，将这些服务器与内部网络隔离开
   - **b.** 外包关联的服务
   - **c.** 无需采取任何措施 — 服务器放在内部网络中就很好
2. **单个外围防火墙对于 Trey Research 是否足够？**
   - **a.** 是 – 单个防火墙在任何环境中都可提供足够的保护
   - **b.** 否 – Trey Research 的担心是有道理的。他们应当采用多种安全工具，为其组织提供“深入防范”，并启用工作站软件防火墙和防病毒软件
   - **c.** 否 – 他们还应创建一个 DMZ
3. **有状态数据包检验和无状态数据包检验哪个可提供更好的安全性？**
   - **a.** 无状态数据包检验，因为它更高效且可停止更多数据包
   - **b.** 两者都不行 – 它们不会提供任何类型的安全保护
   - **c.** 有状态数据包检验，因为它会在数据包通过连接传递时检验数据包

提示

无状态数据包检验是一种速度更快的安全类型，需要的内存较少，但并非完全可靠。

答案

1. Matt 应当建议 Trey Research：
   a. **创建一个外围网络，将这些服务器与内部网络隔离开。**暴露于 Internet 的服务器和设备不应驻留在内部网络上。应当将它们划分或隔离到网络的一个受保护的部分中。
2. 单个外围防火墙对于 Trey Research 是否足够？
   b. **否 – Trey Research 的担心是有道理的。他们应当采用多种安全工具，为其组织提供“深入防范”，并启用工作站软件防火墙和防病毒软件。**没有任何一种解决方案能够完全保护网络的安全；不过，提供多层安全保护可以降低公司的风险。
3. 更好的数据包检验选择是：
   c. **有状态数据包检验，因为它会在数据包通过连接传递时检验数据包**

重要细节

- **防火墙**是用于保护组织网络免受来自其他网络（例如 Internet）的外部威胁（例如黑客）的安全系统。
- **数据包筛选**是根据 IP 地址控制网络访问的过程。防火墙通常会集成筛选器，用于允许或拒绝用户进入或离开局域网 (LAN) 的功能。
- **代理服务器**是管理 Internet 与局域网之间的往来通信并可提供其他功能（例如文档缓存和访问控制）的安全工具。

快捷帮助

- **http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx**（英语）
- **http://technet.microsoft.com/zh-cn/library/cc700828.aspx**
- **http://technet.microsoft.com/en-us/library/cc700820.aspx**（英语）

了解网络访问保护 (NAP)

情景：Adventure Works 是美国最大的高端运动器材供应商之一。二十五位 Adventure Works 销售顾问在国内到处旅行，向零售商推销运动器材。他们每周五携带自己的便携式计算机返回公司总部参加会议和培训。

Allie Bellew 是 Adventure Works 的网络管理员，她希望采取一种方法，以确保移动设备在周五的会议中访问公司网络时处于良好的“健康”安全状态。

1. **Allie 可以采取哪种控制或策略来确保“健康”的安全性？**
   a. 网络访问保护，它将验证每个移动设备的完整性
   b. 每次销售顾问登录时进行病毒扫描
   c. 在连接到网络之前重新建立每台便携式计算机的映像
2. **除了防范感染便携式计算机的病毒外，NAP 还可以做些什么？**
   a. 防止丢失数据
   b. 没有别的了 — 病毒扫描已经很完美
   c. 通过检查设备是否具有最近的软件更新或配置更改验证其完整性
3. **对于与 NAP 不兼容的计算机，Allie 可以采取什么办法？**
   a. 升级不兼容的计算机
   b. 在 NAP 中为不兼容的设备定义例外
   c. 禁止这些设备使用网络

提示

对于“任务所需”的系统可以定义例外，直到可以对其进行升级。

答案

1. Allie 可以采取：
   a. **网络访问保护，它将验证每个移动设备的完整性**
2. 除了防范感染便携式计算机的病毒外，NAP 还可以：
   c. **通过检查设备是否具有最近的软件更新或配置更改验证其完整性。**尚未收到更新的系统可能会与受到恶意软件感染的系统一样容易出现问题。
3. 对于与 NAP 不兼容的计算机，Allie 应当：
   b. **在 NAP 中为不兼容的设备定义例外**

重要细节

- **网络访问保护 (NAP)** 是一个新的平台和解决方案，可基于客户端计算机的标识并遵循公司治理策略控制对网络资源的访问。
- **NAP 强制点**是使用 NAP 或可以与 NAP 结合使用以要求评估 NAP 客户端的健康状况并提供受限网络访问或通信的计算机或网络访问设备。

快捷帮助

- **http://technet.microsoft.com/en-us/network/cc984252.aspx**（英语）
- **http://technet.microsoft.com/en-us/network/bb545879.aspx**（英语）
- **http://www.microsoft.com/windowsserver2008/en/us/nap-faq.aspx**（英语）

了解网络隔离

情景：Coho Winery 从事葡萄酒酿造业务已有三代。他们仍在使用相同的葡萄园和相同的酒窖生产高品质的葡萄酒。甚至他们的多数业务组织也在几十年里保持如故。现在是时候采用与其数据保留基础结构有关的新技术对 Coho 的企业方面进行更新了。

Karen Berg 受命评估 Coho Winery 的网络基础结构并根据其下列特定需求提供相应建议：

- 多数员工需要 Internet 访问。
- 葡萄酒厂内的计算机被隔离，并且不需要 Internet 访问。
- “在家工作”的员工应具有使用 IP 安全的虚拟专用网络访问。

1. **Karen 可以怎样防止葡萄酒厂的计算机能够访问 Internet？**
   - **a.** 创建一个不允许 Internet 访问、而是中继到主网络的 VLAN
   - **b.** 手动配置每台计算机，使其没有网关
   - **c.** 从计算机中删除 Internet Explorer
2. **Karen 必须采取哪项技术以允许办公室员工访问 Internet 且不会将其暴露于 Internet？**
   - **a.** 设置一台具有公共 IP 地址的 Walk-Up 计算机，以便它可以访问 Internet
   - **b.** 为每个办公室用户提供一个拨号调制解调器以建立 Internet 连接
   - **c.** 设置一个路由器以执行网络地址转换，从而允许多个专用地址加入到公用网络中
3. **哪个 Microsoft Windows Server 2008 R2 功能可以同时完成 Internet 访问和 VPN 解决方案？**
   - **a.** DHCP
   - **b.** 远程桌面服务
   - **c.** 路由和远程访问服务

提示

多数服务器操作系统都具有某种形式的路由技术。最低要求包括具有多个网络接口卡 (NIC)。

答案

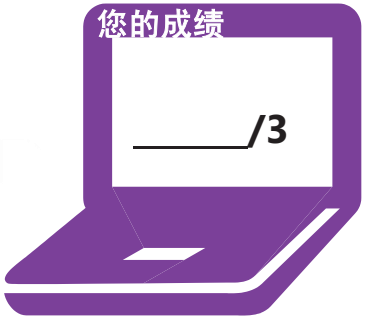
1. 为防止葡萄酒厂的计算机能够访问 Internet，Karen 可以：
   a. **创建一个不允许 Internet 访问、而是中继到主网络的 VLAN**
2. 要允许办公室员工访问 Internet 且不会将其暴露于 Internet，Karen 可以：
   c. **设置一个路由器以执行网络地址转换，从而允许多个专用地址加入到公用网络中。**多数零售无线路由器可执行网络地址转换或端口地址转换，从而使家庭网络设备（Xbox、便携式计算机等）能够访问 Internet。
3. Microsoft Windows Server 2008 R2 可以通过以下功能同时完成 Internet 访问和 VPN 解决方案：
   c. **路由和远程访问服务 (RRAS)。**RRAS 可以同时充当 VPN 和 Internet 网关。可以使用多种安全协议（包括 IP 安全 (IPsec)）为 VPN 访问提供安全保护。

重要细节

- **网络地址转换 (NAT)** 是在 Intranet 或其他专用网络内使用的 IP 地址与 Internet IP 地址之间的转换过程。
- **路由**是将网络之间的数据包从源转发到目标的过程。
- **虚拟 LAN (VLAN)** 是一组具有共同要求的主机，其通信方式就好像它们都连接到相同的广播域，而不管其物理位置如何。

快捷帮助

- **http://technet.microsoft.com/en-us/network/bb531150.aspx**（英语）
- **http://technet.microsoft.com/en-us/network/bb545655.aspx**（英语）
- **http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7E973087-3D2D-4CAC-ABDF-CC7BDE298847&displaylang=en**（英语）
- **http://en.wikipedia.org/wiki/Virtual_LAN**（英语）



了解网络隔离

情景：Arlene Huff 是 Margie's Travel 的系统管理员，最近几周她为保护公司和客户数据的安全而非常忙碌。网络上出现了可疑活动，幸亏 Arlene 跟踪网络用户的措施保护了系统。但保护机密数据的安全仍是一项充满挑战性的长期任务。

公司的所有者 Margie 希望其远程旅行代理能够访问公司网络，这样他们便可以查收电子邮件并发布当日预定的约会。Margie 决定允许旅行代理使用其家庭计算机，但必须确保信息安全。客户信息的安全是其首要任务。

1. **适合 Margie's Travel 的最佳常规解决方案是什么？**
   - **a.** 设置一台 VPN 服务器以允许旅行代理远程访问
   - **b.** 设置一个调制解调器库并让旅行代理为其家庭计算机购买调制解调器，以便可以向办公室拨号
   - **c.** 没有 Margie 想要的那种解决方案
2. **让旅行代理使用其家庭计算机进行 VPN 访问的潜在风险是什么？**
   - **a.** 没有风险 – VPN 可处理一切并加密数据
   - **b.** 旅行代理可能会忘记断开连接，从而使 VPN 连接保持打开状态并禁止他人进行连接
   - **c.** 仅靠 VPN 无法防范家庭计算机上的潜在病毒和恶意软件感染网络
3. **Arlene 担心攻击者会渗透到 VPN 中。她可以怎样设置以“引诱”攻击者，从而更好地了解对手的方法？**
   - **a.** 外围网络之外的一个蜜罐，它是一个伪造的程序，可模拟 VPN 或服务
   - **b.** 一个声称“这里什么都没有”的诱惑性网站
   - **c.** 一个永远不会应答的假 VPN

提示

蜜罐遍布于 Internet 上，用于发现攻击者可能用来侵害系统的方法。

答案

1. 适合 Margie’s Travel 的最佳常规解决方案是：
   a. **设置一台 VPN 服务器以允许旅行代理远程访问。**她可以配置 VPN 以使用多种加密方法。
2. 让旅行代理使用其家庭计算机进行 VPN 访问的风险是：
   c. **仅靠 VPN 无法防范家庭计算机上的潜在病毒和恶意软件感染网络。**Arlene 可以使用“直接访问”，这是 Windows 7 和 Windows Server 2008 R2 中的新功能，有助于缓解潜在风险。
3. 要“引诱”攻击者以更好地了解其方法，Arlene 可以创建：
   a. **外围网络之外的一个蜜罐，它是一个伪造的程序，可模拟 VPN 或服务**

重要细节

- **外围网络**（也称为 DMZ，非军事区和屏蔽子网）是一个物理或逻辑网络，其中包含组织的外部服务并将其公开给更大的非信任网络，通常是 Internet。
- **Internet 协议安全 (IPsec)** 是一个 Internet 协议安全标准，该标准提供一个常规的基于策略的 IP 层安全机制，该机制非常适合提供逐个主机式的身份验证。IPsec 策略定义为具有控制入站数据流的安全规则和设置。
- **虚拟专用网络 (VPN)** 公用网络（如 Internet）上的节点使用加密技术相互通信，以此防止未经授权的用户截获和了解其消息，就像这些节点是通过专用线路连接的一样。

快捷帮助

- **http://technet.microsoft.com/en-us/network/dd420463.aspx**（英语）

了解协议安全

情景：自从 Graphic Design Institute 的网络管理员 Todd Rowe 采取强化安全措施保护学生数据以来，所报告的泄露事件次数已降低至零！行政管理部门对此很高兴，但 Todd 知道防止数据遭受攻击是一场持久战。

Todd 的朋友 Neil Black 是专用数据存储攻击方法方面的专家。Todd 请求 Neil 为行政管理部门和办公室员工就网络安全、协议安全措施、攻击方法和防范手段做一次演示报告。Todd 深知，掌握相关知识的员工是防范和截获攻击这一整个战略中的重要组成部分。

1. **哪种类型的攻击可通过使用 IP 地址或物理地址将一台计算机配置为看似是受信任网络上的另一台计算机？**
   - **a.** 身份欺骗
   - **b.** 计算机伪造
   - **c.** 应用程序层攻击
2. **哪种安全协议可帮助防止未经授权修改、破坏或访问数据？**
   - **a.** DNSSEC
   - **b.** IP 安全 (IPsec)
   - **c.** NetBIOS
3. **哪种类型的攻击会危害网络或计算机，使系统表现为无法使用？**
   - **a.** 中间人攻击
   - **b.** 密码攻击
   - **c.** 拒绝服务 (DOS) 攻击

提示

有多种形式的分布式拒绝服务 (DOS) 攻击，它们可妨碍计算机、服务器或应用程序的正常运行。

答案

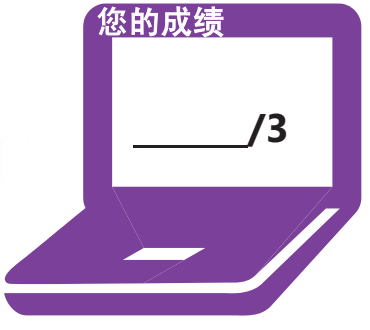
1. 可将一台计算机配置为看似是受信任网络上的另一台计算机的攻击是：
   a. **身份欺骗**
2. 可帮助防止未经授权修改、破坏或访问数据的安全协议是：
   b. **IP 安全 (IPsec)**。Ipsec 不仅可用于 VPN 安全，还可用于局域网通信。80% 的安全攻击来自组织内部。如果认为位于外围防火墙之内的数据是安全的，那么这一假定会很危险。
3. 会危害网络或计算机，使系统表现为无法使用的攻击是：
   c. **拒绝服务 (DOS) 攻击**

重要细节

- **探查**是指监控网络通信以获取数据（如明文密码或配置信息）的行为。
- **身份欺骗（IP 地址欺骗）**是指攻击者未经授权使用网络、计算机或网络组件的 IP 地址。
- **Internet 协议安全 (IPsec)** 支持网络级别的数据完整性、数据机密性、数据源身份验证和重播保护。由于 IPsec 集成在 Internet 层（第 3 层）中，因而它可以为 TCP/IP 套件中的几乎所有协议提供安全保护。
- **域名系统 (DNS)** 是包含名称与其他信息（如 IP 地址）之间的映射的一个分层分布式数据库。DNS 允许用户通过将友好可读的名称（如 *www.microsoft.com* ）转换为计算机可连接到的 IP 地址找到网络上的资源。

快捷帮助

- **http://technet.microsoft.com/en-us/library/cc959354.aspx**（英语）
- **http://technet.microsoft.com/en-us/library/ee649205(WS.10).aspx**（英语）



4

了解安全软件

本章内容

- 4.1 了解客户端保护
- 4.2 了解电子邮件保护
- 4.3 了解服务器保护

了解客户端保护

情景：Jeff Hay 是 Tailspin Toys 公司的网络管理员。在玩具销售淡季，Tailspin 技术员工仍然忙于维护和升级各种系统，准备应对繁忙的假日销售高峰。

Jeff 希望在此时间对所有计算机进行维护并更新软件。他担心公司员工会安装来自 Internet 的软件。Jeff 意识到使用享有盛誉的防病毒软件也只能做那么多。其公司网络由 Windows XP、Windows 7 和 Windows Server 2008 R2 混合组成。

1. **Jeff 可以怎样做以确保计算机具有最新的安全更新？**
   - **a.** 采用 Windows 软件更新服务控制所使用的操作系统和任何 Microsoft 产品的所有 Microsoft 更新
   - **b.** 每周一早些上班并在每台计算机上运行“Windows 更新”
   - **c.** 向公司员工发送电子邮件，指导他们在午休时间执行“Windows 更新”
2. **Jeff 可以怎样防止公司员工从 Internet 上下载并安装软件？**
   - **a.** 在所有 Windows 7 计算机上启用“用户帐户控制”并配置软件限制策略
   - **b.** 向所有用户发送附有“Internet 使用政策”的措辞强硬的电子邮件
   - **c.** 禁止所有用户访问 Internet
3. **Jeff 应使用哪种方法标识软件限制策略中的 Internet软件？**
   - **a.** 哈希规则
   - **b.** 路径规则
   - **c.** 区域规则

提示

哈希规则会基于可执行文件创建一个哈希校验和。路径规则会限制位于特定路径中的软件。

答案

1. 要确保计算机具有最新的安全更新，Jeff 可以：
   a. **采用 Windows 软件更新服务控制所使用的操作系统和任何 Microsoft 产品的所有 Microsoft 更新**
2. 要防止公司员工从 Internet 上下载并安装软件，Jeff 可以：
   a. **在所有 Windows 7 计算机上启用“用户帐户控制”并配置软件限制策略**
3. 要标识软件限制策略中的 Internet 软件，Jeff 可以使用：
   c. **区域规则**

重要细节

- **防病毒软件**是一种计算机程序，可扫描计算机内存和大容量存储以识别、隔离和清除病毒，还可在计算机接收传入文件时对其进行病毒检查。
- **用户帐户控制 (UAC)** 有助于防止恶意程序（恶意软件）损害计算机，并可帮助组织进行更完善的桌面管理部署。使用 UAC，应用程序和任务将始终在非管理员帐户的安全上下文中运行，除非管理员专门授权对系统进行管理员级别的访问。

快捷帮助

- **http://www.microsoft.com/security_essentials/market.aspx**（英语）
- **http://technet.microsoft.com/en-us/library/bb457141.aspx**（英语）
- **http://technet.microsoft.com/en-us/library/bb456987.aspx**（英语）
- **http://windows.microsoft.com/zh-cn/windows7/what-is-user-account-control**

了解电子邮件保护

情景：最近 Coho Winery 遇到一系列垃圾邮件问题；有些员工甚至由于仿冒欺诈邮件而遭遇身份被盗用。John Kane 是 Coho Winery 的系统管理员，解决这些问题的任务就直接落在了他的头上。经过一番研究之后，他想出了一些解决方案。John 希望通过采取各种安全措施解决这些问题，其中最重要的是提供一些迫切需要的与使用电子邮件的最佳实践有关的公司培训。

1. **John 可以怎样做以帮助减少到达其 Microsoft Exchange Server 的垃圾邮件数量？**
   - **a.** 至少在 SMTP 虚拟服务器上启用反向 DNS 查找
   - **b.** 禁用 Internet 电子邮件
   - **c.** 更改域名
2. **当 Coho 用户收到来自他们所知道的公司的电子邮件并且其中要求单击链接以“验证其帐户信息”时，他们应当怎样做？**
   - **a.** 删除该电子邮件
   - **b.** 将其转发给公司其他人员并警告大家不要单击链接
   - **c.** 单击链接，因为他们根据公司名称“知道”这是一封合法电子邮件
3. **除了启用反向 DNS 查找之外，John 还可以怎样保护其 Exchange Server 的安全？**
   - **a.** 启用自动发现
   - **b.** 添加发送方策略框架 (SPF)
   - **c.** 更新防病毒软件

提示

电子邮件服务器上的防病毒软件不会防范垃圾邮件。

答案

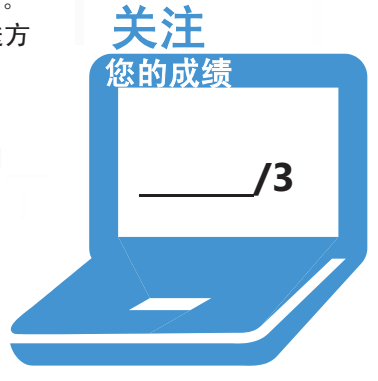
1. 要帮助减少到达其 Microsoft Exchange Server 的垃圾邮件数量，John 可以：
   a. **至少在 SMTP 虚拟服务器上启用反向 DNS 查找。**将系统配置为进行反向 DNS 查找可使用 PTR 记录交叉检查域名，该记录是与该域名相关联的 IP 地址。如果 IP 地址与域名的关联记录不匹配，则不会传递它。
2. 当用户收到来自他们所知道的公司的电子邮件并且其中要求“验证其帐户信息”时，他们应当：
   a. **删除该电子邮件。**如今，公司不会通过电子邮件请求帐户信息。用户在收到这类电子邮件时应小心。他们还可以致电公司，警告他们注意防范该邮件。
3. 除了启用反向 DNS 查找之外，John 还可以：
   b. **添加发送方策略框架 (SPF)。**SPF 允许管理员配置服务器以明确谁可以从其域中发送电子邮件。

重要细节

- **垃圾邮件**是收件人与之没有个人或业务关系的某人未经请求发送的无用的电子邮件。
- **仿冒和网址嫁接**是用来欺骗计算机用户披露个人或财务信息的技术。
- **SPF 记录**是 SMTP 协议的扩展，可通过验证对于发件人的域，SMTP 接收头中的 IP 地址是否获准发送电子邮件来防止垃圾邮件发送者伪造电子邮件中的“发件人”字段。
- **欺骗**是指假冒电子邮件发送方、IP 连接或域，使得电子邮件似乎是源自实际发送方以外的其他发送方。

快捷帮助

- **http://technet.microsoft.com/en-us/exchange/dd251269.aspx**（英语）
- **http://www.microsoft.com/athome/security/email/phishing/video1.mspx**（英语）
- **http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.mspx**（英语）



了解服务器保护

情景：几年前，Humongous Insurance (HI) 重新组织了其业务和技术基础结构。Alfons Parovsky 最近受聘成为 HI 的服务器管理员。有关安全更新的记录十分粗糙，他不希望在自己作为管理员期间发生任何重大安全过失。为确保一切都符合标准，Alfons 决定立即对数据中心执行一次安全评估。他希望确保服务器符合所有必要的安全要求并且能够定期更新。Alfons 还希望确保 HI 的远程位置没有任何暴露于网络的情况。

1. **Alfons 可以使用哪种工具评估 HI 服务器是否存在与操作系统和所安装的软件相关的任何薄弱之处？**
   - **a.** Microsoft Baseline Security Analyzer
   - **b.** 事件查看器
   - **c.** 资源监视器
2. **Alfons 可以启用哪种服务以确保服务器收到所有必要软件更新？**
   - **a.** Windows 备份服务
   - **b.** 路由和远程访问服务
   - **c.** Windows 软件更新服务
3. **Alfons 可以怎样做以确保域在远程位置的安全？**
   - **a.** 在远程站点中安装一个只读域控制器
   - **b.** 删除远程站点中的任何服务器并让员工使用电子邮件传送文件
   - **c.** 在远程站点使用细化的密码实施更强的密码策略

提示

强密码不会减少域控制器的暴露情况。

答案

1. 要评估与操作系统和所安装的软件相关的薄弱之处，Alfons 可以使用：
   a. **Microsoft Baseline Security Analyzer。**MBSA 是一款易于使用的工具，可提供即时反馈和资源以标识服务器和工作站上的潜在薄弱之处。它将分析操作系统以及任何安装的 Microsoft 软件。
2. 要确保服务器收到所有必要软件更新，Alfons 可以启用：
   c. **Windows 软件更新服务。**Alfons 可以为其服务器创建一个单独的组，这样便可以有选择地管理何时安装哪些更新。
3. 要确保域在远程位置的安全，他可以：
   a. **在远程站点中安装一个只读域控制器 (RODC)。**只读域控制器 (RODC) 是 Windows Server 2008 操作系统中的一种新型域控制器。使用 RODC，组织可以轻松在无法保证物理安全性的位置部署域控制器。

重要细节

- **DNS 动态更新**允许 DNS 客户端计算机在 DNS 服务器中注册并在发生更改时动态更新其资源记录。
- **Microsoft Baseline Security Analyzer (MBSA)** 是一款为 IT 专业人士设计的工具，旨在按照 Microsoft 的安全建议帮助中小企业确定其安全状况并提供具体修正指导。
- **Windows Server Update Services (WSUS)** 允许信息技术管理员向运行 Windows 操作系统的计算机部署最新的 Microsoft 产品更新。

快捷帮助

- **http://technet.microsoft.com/zh-cn/security/cc184923.aspx**
- **http://technet.microsoft.com/zh-cn/security/cc185712.aspx**
- **http://technet.microsoft.com/zh-cn/library/cc755058(WS.10).aspx**