Cybersecurity Essentials 1.0 课程范围和学习次序

上次更新日期 13 三月 2017

目标受众

Cybersecurity Essentials 1.0 课程面向有兴趣在网络安全领域进行更高级学习的学生。此预备课程提供对网络安全领域的概述。该课程探讨网络犯罪分子的特点及其使用的战术，然后探讨网络安全专业人员用于打击网络犯罪的技术、产品和程序。该课程适合于许多教育级别和机构类型的学生，包括初中、高中、大学、学院、技校和社区组织。

必备条件

为了掌握适当的技能，学生应熟悉预备课程中介绍的内容和技能：

- Introduction to Cybersecurity 2.0

目标认证

本课程无目标认证

课程描述

本课程有许多功能，可帮助学生理解这些概念：

- 丰富的多媒体内容，包括基于 Flash 的互动练习、视频、游戏和测验，支持各种不同的学习方式并帮助激励学习兴趣和巩固知识
- 动手实验和 Packet Tracer 基于模拟的学习活动可以帮助学生发展批判性思维和复杂问题的解决技巧。
- 创新的评估提供即时反馈，支持评估知识和技能掌握程度
- 技术概念采用适合所有层次学生的语言进行解释，嵌入的互动练习避免了书面内容堆砌，有助于加强理解。
- 本课程鼓励学生参加其他的 IT 教育课程，同时也强调应用技能和实际动手经验

思科 Packet Tracer 练习旨在与 Packet Tracer 6.3 或更高版本配合使用。

课程目标

Cybersecurity Essentials 1.0 涵盖网络世界所有安全领域的基础知识和基本技能 - 保护企业时使用的信息安全、系统安全、网络安全、移动安全、物理安全、道德标准和法律、相关技术、防御和缓解技术。

完成 *Cybersecurity Essentials 1.0* 课程后，学生将能够执行以下任务：

- 描述网络安全领域中犯罪分子和英雄的特征。
- 描述与数据状态和网络安全对策相关的机密性、完整性和可用性原则。
- 描述网络犯罪分子使用的战术、技术和程序。
- 描述如何使用技术、产品和程序来保护机密性。
- 描述如何使用技术、产品和程序来确保完整性。
- 描述如何使用技术、产品和程序来实现高可用性。
- 解释网络安全专业人员如何使用技术、过程和程序来保护网络的所有组件。
- 解释与网络安全相关的法律的目的。

最低系统要求

为了让学生获得最佳的学习体验，我们建议班级可容纳 12 至 15 名学生且每个学生一台实验 PC。最多两个学生共享一台实验 PC 进行动手实验。有些实验练习要求将学生实验 PC 连接到本地网络。

实验 PC 硬件要求

- 至少具有 2 GB RAM 和 8 GB 可用磁盘空间的计算机
- 高速互联网接入，用于下载 Oracle VirtualBox 和虚拟机映像文件。

课程概述

Cybersecurity Essentials 1.0 可帮助学生：

- 了解网络安全世界中的参与者以及网络犯罪分子和网络安全专家的动机。
- 学习识别安全攻击、症状、过程和对策。
- 学习各种安全领域的基础知识。
- 建立安全管理、控制、保护和缓解技术方面的技能。
- 学习安全法律、道德标准，以及如何制定安全策略。
- 了解不同网络安全专业人员的角色和职业选择。

课程大纲

表 1. Cybersecurity Essentials 1.0 课程大纲

章/节	目的/目标
第 1 章. 网络安全：魔法师、英雄和犯罪分子的世界	**描述网络安全领域中犯罪分子和英雄的特征。**
1.1 网络安全世界	说明构成网络安全世界的常见特征
1.2 网络犯罪分子与网络英雄	区分网络犯罪分子与英雄的特征。
1.3 网络王国面临的威胁	比较网络安全威胁如何影响个人、企业和组织。
1.4 网络安全的黑暗势力	介绍导致网络犯罪蔓延和增长的因素。
1.5 打造更多英雄	介绍致力于扩大网络安全人才队伍的组织和所做的工作。
第 2 章. Cybersecurity Sorcery Cube	**描述与数据状态和网络安全对策相关的机密性、完整性和可用性原则。**
2.1 Cybersecurity Sorcery Cube	说明 McCumber Cube 的三个维度。
2.2 CIA 三要素	说明保密性、完整性和可用性原则。
2.3 数据状态	区分数据的三种状态。
2.4 网络安全对策	比较网络安全对策的类型。
2.5 IT 安全管理框架	说明 ISO 网络安全模型
第 3 章. 网络安全威胁、漏洞和攻击	**描述网络犯罪分子使用的战术、技术和程序。**
3.1 恶意软件和恶意代码	区分恶意软件和恶意代码的类型。
3.2 欺诈	比较社交工程中使用的不同方法。
3.3 攻击	比较不同类型的网络攻击。
第 4 章. 保护秘密的技术	**描述如何使用技术、产品和程序来保护机密性。**
4.1 加密	解释加密技术如何保护机密性。
4.2 访问控制	介绍访问控制技术如何保护机密性。
4.3 混淆数据	介绍混淆数据的概念。

第 5 章. 确保完整性的技术	**描述如何使用技术、产品和程序来确保完整性。**
5.1 数据完整性控制的类型	介绍用于确保完整性的流程。
5.2 数字签名	解释数字签名的目的。
5.3 证书	解释数字证书的目的。
5.4 数据库完整性的实施	解释实施数据库完整性的必要性。
第 6 章. 五个九 (99.999%) 的领域	**描述如何使用技术、产品和程序来实现高可用性。**
6.1 高可用性	介绍高可用性的概念。
6.2 提升可用性的措施	介绍如何采用高可用性措施提升可用性。
6.3 事件响应	介绍事件响应计划如何提升高可用性。
6.4 灾难恢复	介绍灾难恢复计划如何在实施高可用性方面发挥重要作用。
第 7 章. 加强网络王国防御	**解释网络安全专业人员如何使用技术、过程和程序来保护网络的所有组件。**
7.1 保护系统和设备	介绍流程和程序如何保护系统。
7.2 服务器加固	介绍如何保护网络上的服务器。
7.3 网络加固	介绍如何实施安全措施以保护网络设备。
7.4 物理和环境安全	介绍如何实施物理安全措施以保护网络设备。
第 8 章. 加入网络英雄的行列	**解释与网络安全相关的法律的目的。**
8.1 网络安全领域	描述如何在 CIA（保密性、完整性和可用性）三要素范围内使用网络安全领域。
8.2 了解成员的宣誓词	解释道德标准如何提供指导。
8.3 后续步骤	介绍如何采取下一步以成为网络安全专业人员

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。