网络运营工程师 (CA) 课程 1.0 版
课程大纲

上次更新日期：2021 年 05 月 18 日

简介

快速检测网络安全漏洞并有效应对安全事件是当今组织面临着的严峻挑战。安全运营中心 (SOC) 团队不仅要时刻关注安全系统，还要持续检测并及时应对网络安全漏洞和威胁，保护组织安全。网络运营工程师课程讲授在安全运营中心担任工程师级网络安全分析师所需掌握的知识和技能。

目标受众

网络运营工程师课程专为希望学习入门级安全分析师职业技能的思科网络技术学院® 学生而设计，对象包括在高等教育机构就读技术学位课程的学生，以及希望从事安全运营中心 (SOC) 工作的 IT 专业人员。在本课程中，学生将学习使用常见开源工具检测、分析和上报基本网络安全威胁所需的基础知识。

前提条件

参加网络运营工程师课程的学生应掌握下列技能和知识：

- PC 和互联网操作技能
- Windows 和 Linux 系统的基本概念
- 对计算机网络具有基本的了解（“CCNA 网络简介”级别）
- 了解二进制和十六进制
- 熟悉 Cisco Packet Tracer

对应的认证

本课程与思科认证网络运营工程师级 (CBROPS) 认证直接挂钩。考生需要通过 200-201 CBROPS 考试才能获得思科认证网络运营工程师级认证。CBROPS 考试将考察考生在安全概念、安全监控、基于主机的分析、网络入侵分析以及安全策略和程序方面的知识和技能。

课程说明

本课程独具特色，可帮助学生理解以下概念：

- 本课程由二十八 (28) 个模块组成。每个模块包含多个主题。
- 课程模块注重培养批判性思维、问题解决能力、协作能力和技能的实际运用。
- 每个模块都会通过某种形式提供练习和测验机会，例如实验或 Packet Tracer 练习。这些模块级练习可提供反馈，指出学生对课程要求掌握技能的掌握程度。学生可以利用这些测验，确保自己在参加评分测验或评分考试之前充分掌握了所学知识。
- 在一些主题下，可能会通过“检查您的理解情况”交互式测验或其他方式（例如实验或 Packet Tracer）评估学生的学习情况。这些主题级别的测验旨在帮助学生了解他们是否很好地掌握了相关主题的内容，或者是否需要

先回顾已学内容再继续学习。学生可以利用这些测验，确保自己在参加评分测验或评分考试之前充分掌握了所学知识。“检查您的理解情况”测验不会影响学生的整体成绩。

- 互动练习、视频和测验等丰富的多媒体内容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。
- 通过虚拟环境模拟真实的网络安全威胁场景，让学生有机会实际监控、分析和解决安全问题。
- 动手实验可帮助学生培养批判性思维和解决复杂问题的技能。
- 创新的考试提供即时反馈，有助于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 IT 教育课程，同时也强调应用技能和动手经验。
- Cisco Packet Tracer 练习可在 Packet Tracer 7.3.0 或更高版本中使用。

课程目标

*网络运营工程师 1.0 版*课程涵盖在安全运营中心 (SOC) 工作的工程师级网络安全分析师成功处理任务、工作和职责所需的知识和技能。

完成*网络运营工程师 1.0 版*课程后，学生将能够执行以下任务：

- 安装虚拟机，以创建一个安全的环境，用于实施和分析网络安全威胁事件。
- 解释网络安全运营分析师在企业中的职责。
- 阐述支持网络安全分析所需的 Windows 操作系统功能和特性。
- 阐述 Linux 操作系统的功能和特性。
- 分析网络协议和服务的运行。
- 阐述网络基础设施的运行。
- 对各种类型的网络攻击进行分类。
- 使用网络监控工具来识别针对网络协议和服务的攻击。
- 阐述如何预防计算机网络、主机和数据被恶意访问。
- 阐述加密对网络安全监控的影响。
- 阐述如何调查终端漏洞和攻击。
- 评估网络安全警报。
- 分析网络入侵数据，发现遭受攻击的主机。
- 运用事件响应模型管理网络安全事件。

实验设备要求

除学生的实验 PC 之外，本课程不需要使用任何物理设备。课程使用多个虚拟机 (VM) 提供实验机会。

基础设备捆绑包：

- PC - 最低系统要求
  - CPU：Intel Pentium 4，2.53 GHz 或同等配置，支持虚拟化
  - 操作系统（例如 Microsoft Windows、Linux 和 Mac 操作系统）
  - 64 位处理器
  - 内存：8 GB

© 2021 思科和/或其附属公司。版权所有。思科机密

- 存储：40 GB 可用磁盘空间
- 显示器分辨率：1024 x 768
- 支持 Unicode 编码的语言字体（如果界面语言不是英语）
- 最新显卡驱动程序和操作系统更新版本

- 实验 PC 和学生 PC 需要连接互联网

学生 PC 软件：

- Oracle VM VirtualBox Manager（6.1 或更高版本）
- 网络运营工作站虚拟机
  - 可在课程中下载
  - 需要 1 GB RAM 和 20 GB 磁盘空间
- Security Onion 虚拟机
  - 可在课程中下载
  - 需要 4 GB RAM（最低）或 8GB RAM（强烈建议）和 20 GB 磁盘空间

网络运营工程师课程大纲

下面列出了本课程当前涵盖的一系列模块及相关能力。每个模块都是一个综合学习单元，由内容、练习和作业考试组成，目标是让学生掌握一组特定的能力。模块的大小取决于掌握相应能力所需的知识和技能的深度。某些模块属于基础模块，模块中的内容有助于学习 CBROPS 认证考试中涵盖的概念，但不在考试范围内。

表 1。 网络运营工程师课程 1.0 版课程大纲

模块/主题	目的/目标
模块 1. 网络面临的危险	**阐述网络和数据受到攻击的原因。**
1.0 简介	课程和第一个模块的简介。
1.1 实战案例	概述网络安全事件的特征。
1.2 威胁发起者	阐述特定安全事件背后威胁发起者的动机。
1.3 威胁的影响	阐述网络安全攻击的潜在影响。
1.4 网络面临的危险总结	模块的简要总结和章节测验。
模块 2. 打击网络犯罪的斗士	**阐述如何为从事网络安全运营工作做准备。**
2.0 简介	模块简介。
2.1 现代安全运营中心	阐述安全运营中心的使命。
2.2 成为守护者	阐述可用于为从事网络安全运营工作做准备的资源。
2.3 打击网络犯罪的斗士总结	模块的简要总结和章节测验。
模块 3. Windows 操作系统	**阐述 Windows 操作系统的安全功能。**

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
3.0 简介	模块简介。
3.1 Windows 发展简史	阐述 Windows 操作系统的历史。
3.2 Windows 架构和操作	阐述 Windows 的架构及其操作。
3.3 Windows 配置和监控	阐述如何配置和监控 Windows。
3.4 Windows 安全	阐述如何保持 Windows 的安全。
3.5 Windows 操作系统总结	模块的简要总结和章节测验。
模块 4. Linux 概述	**实施 Linux 基本安全功能。**
4.0 简介	模块简介。
4.1 Linux 基础知识	阐述为什么 Linux 技能对于网络安全监控和调查至关重要。
4.2 使用 Linux Shell	使用 Linux Shell 处理文本文件。
4.3 Linux 服务器和客户端	阐述客户端-服务器网络的工作方式。
4.4 基本服务器管理	阐述 Linux 管理员如何查找和处理安全日志文件。
4.5 Linux 文件系统	管理 Linux 文件系统和权限。
4.6 使用 Linux GUI	介绍 Linux GUI 的基本组件。
4.7 使用 Linux 主机	使用工具检测 Linux 主机上的恶意软件。
4.8 Linux 基础总结	模块的简要总结和章节测验。
模块 5. 网络协议	**阐述协议如何实现网络操作。**
5.0 简介	模块简介。
5.1 网络通信过程	阐述数据网络通信的基本工作原理。
5.2 通信协议	阐述协议如何实现网络操作。
5.3 数据封装	说明数据封装如何实现跨网络数据传输。
5.4 网络协议总结	模块的简要总结和章节测验。
模块 6. 以太网和互联网协议 (IP)	**阐述以太网和 IP 协议如何支持网络通信。**
6.0 简介	模块简介。
6.1 以太网	阐述以太网如何支持网络通信。
6.2 IPv4	阐述 IPv4 协议如何支持网络通信。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
6.3 IP 寻址基础知识	阐述 IP 地址如何实现网络通信。
6.4 IPv4 地址的类型	阐述用于实现网络通信的 IPv4 地址类型。
6.5 默认网关	阐述默认网关如何实现网络通信。
6.6 IPv6 前缀长度	阐述 IPv6 协议如何支持网络通信。
6.7 以太网和 IP 协议总结	模块的简要总结和章节测验。
模块 7. 网络安全原理	**验证连接。**
7.0 简介	模块简介。
7.1 ICMP	说明如何使用 ICMP 测试网络连接。
7.2 Ping 和 Traceroute 实用程序	使用 Windows 工具、ping 和 traceroute 验证网络连接。
7.3 验证连接总结	模块的简要总结和章节测验。
模块 8. 地址解析协议	**分析网络中的地址解析协议 PDU。**
8.0 简介	模块简介。
8.1 MAC 和 IP	比较 MAC 地址和 IP 地址的不同作用。
8.2 ARP	通过检查以太网帧来分析 ARP。
8.3 ARP 问题	阐述 ARP 请求如何影响网络和主机性能。
8.4 地址解析协议总结	模块的简要总结和章节测验。
模块 9. 传输层	**阐述传输层协议如何支持网络功能。**
9.0 简介	模块简介。
9.1 传输层特性	阐述传输层协议如何支持网络通信。
9.2 建立传输层会话	阐述传输层如何建立通信会话。
9.3 传输层可靠性	阐述传输层如何建立可靠的通信。
9.4 传输层总结	模块的简要总结和章节测验。
模块 10. 网络服务	**阐述网络服务如何支持网络功能。**
10.0 简介	模块简介。
10.1 DHCP	阐述 DHCP 服务如何支持网络功能。
10.2 DNS	阐述 DNS 服务如何支持网络功能。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
10.3 NAT	阐述 NAT 服务如何支持网络功能。
10.4 文件传输和共享服务	阐述文件传输服务如何支持网络功能。
10.5 邮件	阐述邮件服务如何支持网络功能。
10.6 HTTP	阐述 HTTP 服务如何支持网络功能。
10.7 网络服务总结	模块的简要总结和章节测验。
模块 11. 网络通信设备	**阐述网络设备如何支持有线和无线网络通信。**
11.0 简介	模块简介。
11.1 网络设备	阐述网络设备如何支持网络通信。
11.2 无线通信	阐述无线设备如何支持网络通信。
11.3 网络通信设备总结	模块的简要总结和章节测验。
模块 12. 网络安全基础设施	**阐述如何使用网络设备和服务增强网络安全。**
12.0 简介	模块简介。
12.1 网络拓扑	阐述网络设计如何影响通过网络的流量。
12.2 安全设备	阐述如何使用特殊设备增强网络安全。
12.3 安全服务	阐述网络服务如何增强网络安全。
12.4 网络安全基础设施总结	模块的简要总结。
模块 13. 攻击者及攻击工具	**阐述网络如何受到攻击。**
13.0 简介	模块简介。
13.1 谁在攻击我们的网络？	阐述网络威胁的变化形势。
13.2 威胁发起者工具	介绍威胁发起者使用的各种攻击工具。
13.3 攻击者及攻击工具总结	模块的简要总结和章节测验。
模块 14. 常见威胁和攻击	**阐述各种类型的威胁和攻击。**
14.0 简介	模块简介。
14.1 恶意软件	描述各类恶意软件。
14.2 常见网络攻击 - 侦查、访问和社交工程	阐述侦查、访问和社交工程攻击。
14.3 网络攻击 - 拒绝服务、缓冲区溢出和规避	阐述拒绝服务、缓冲区溢出和规避攻击。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
14.4 常见威胁和攻击总结	模块的简要总结和章节测验。
模块 15. 观察网络操作	**阐述网络流量监控。**
15.0 简介	模块简介。
15.1 网络监控简介	阐述网络监控的重要性。
15.2 网络监控工具简介	阐述如何执行网络监控。
15.3 网络监控和网络监控工具总结	模块的简要总结和章节测验。
模块 16. 底层攻击	**阐述 TCP/IP 漏洞如何导致网络攻击。**
16.0 简介	模块简介。
16.1 IP PDU 详细信息	阐述 IPv4 和 IPv6 报头结构。
16.2 IP 漏洞	阐述 IP 漏洞如何导致网络攻击。
16.3 TCP 和 UDP 漏洞	阐述 TCP 和 UDP 漏洞如何导致网络攻击。
16.4 底层攻击总结	模块的简要总结和章节测验。
模块17. 上层攻击	**阐述常见网络应用和服务易受攻击的原因。**
17.0 简介	模块简介。
17.1 IP 服务	阐述 IP 服务漏洞。
17.2 企业服务	阐述网络应用漏洞如何导致网络攻击。
17.3 上层攻击总结	模块的简要总结和章节测验。
模块 18. 了解防御	**阐述网络安全防御方法。**
18.0 简介	模块简介。
18.1 纵深防御	阐述如何使用深度防御策略来保护网络。
18.2 安全策略、法规和标准	阐述安全策略、法规和标准。
18.3 了解防御总结	模块的简要总结和章节测验。
模块 19. 访问控制	**阐述访问控制方法如何保护网络。**
19.0 简介	模块简介。
19.1 访问控制概念	阐述访问控制机制如何保护网络数据。
19.2 AAA 的使用与操作	阐述如何使用 AAA 控制网络访问。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
19.3 访问控制总结	模块的简要总结和章节测验。
模块 20. 威胁情报	**使用各种来源的情报识别最新安全威胁。**
20.0 简介	模块简介。
20.1 信息来源	介绍用于传达新型网络安全威胁的各种信息来源。
20.2 威胁情报服务	介绍各种威胁情报服务。
20.3 威胁情报总结	模块的简要总结和章节测验。
模块 21. 加密	**阐述公钥基础设施如何支持实现网络安全。**
21.0 简介	模块简介。
21.1 完整性和真实性	阐述加密在确保数据完整性和真实性方面的作用。
21.2 保密性	介绍加密方法如何提高数据保密性。
21.3 公钥加密	介绍公钥加密。
21.4 机构和 PKI 信任系统	介绍公钥基础设施的工作原理。
21.5 加密的应用和影响	介绍对加密的使用如何影响网络安全运营。
21.6 加密总结	模块的简要总结。
模块 22. 终端保护	**介绍恶意软件分析网站如何生成恶意软件分析报告。**
22.0 简介	模块简介。
22.1 恶意软件防护	介绍用于缓解恶意软件的方法。
22.2 基于主机的入侵防御	介绍基于主机的 IPS/IDS 日志条目。
22.3 应用程序安全	介绍如何使用沙盒分析恶意软件。
22.4 终端保护总结	模块的简要总结和章节测验。
模块 23. 终端漏洞评估	**介绍如何评估和管理终端漏洞。**
23.0 简介	模块简介。
23.1 网络和服务器分析	介绍网络和服务器分析功能的价值。
23.2 通用安全漏洞评分系统 (CVSS)	介绍如何使用 CVSS 报告来描述安全漏洞。
23.3 安全设备管理	介绍如何使用安全设备管理技术来保护数据和资产。
23.4 信息安全管理系统	介绍如何使用信息安全管理系统来保护资产。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
23.5 终端漏洞评估总结	模块的简要总结和章节测验。
模块 24. 技术和协议	**介绍安全技术如何影响安全监控。**
24.0 简介	模块简介。
24.1 监控常用协议	介绍常见网络协议在安全监控环境中的行为。
24.2 安全技术	介绍安全技术如何影响监控常见网络协议的能力。
24.3 技术和协议总结	模块的简要总结和章节测验。
模块 25. 网络安全数据	**介绍安全监控中使用的网络安全数据类型。**
25.0 简介	模块简介。
25.1 安全数据的类型	介绍在安全监控中使用的数据类型。
25.2 终端设备日志	介绍终端设备日志文件的元素。
25.3 网络日志	介绍网络设备日志文件的元素。
25.4 网络安全数据总结	模块的简要总结和章节测验。
模块 26. 评估警报	**介绍评估警报的过程。**
26.0 简介	模块简介。
26.1 警报来源	认识警报的结构。
26.2 警报评估概述	介绍如何进行警报分类。
26.3 评估警报总结	模块的简要总结和章节测验。
模块 27. 使用网络安全数据	**分析数据以确定警报的来源。**
27.0 简介	模块简介。
27.1 通用数据平台	介绍如何准备数据以用于网络安全监控 (NSM) 系统。
27.2 调查网络数据	使用 Security Onion 工具来调查网络安全事件。
27.3 加强网络安全分析师的工作	介绍用于改善工作流程管理的网络监控工具。
27.4 使用网络安全数据总结	模块的简要总结和章节测验。
模块 28. 数字调查分析与事件分析和响应	**介绍网络运营工程师如何应对网络安全事件。**
28.0 简介	模块简介。
28.1 证据处理和攻击归因	介绍数字调查分析流程的作用。

© 2021 思科和/或其附属公司。版权所有。思科机密

模块/主题	目的/目标
28.2 网络杀伤链	认识网络杀伤链中的各个环节。
28.3 入侵分析钻石模型	使用钻石模型对入侵事件进行分类。
28.4 事件响应	将 NIST 800-61r2 事件处理程序应用于特定事件场景。
28.5 数字调查分析与事件分析和响应总结	模块的简要总结。
28.6 备战认证考试，开启职业生涯！	认证考试备考资料、折扣券和其他职业资源。

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2021 思科和/或其附属公司。版权所有。思科机密