



آکادمی راون



دورهی آنلاین

Network & Protocols Fundamentals In Cyber Security

مدرس:

احسان نیک‌آور

درباره‌ی این دوره

گاهی شوق به پیشرفت در افرادی که شروع به یادگیری یک تخصص می‌کنند سبب می‌شود تا زمان کمی را به یادگیری مفاهیم پایه‌ای آن رشته اختصاص داده و در نتیجه تصمیمات عجولانه‌ای برای ورود سریع‌تر به رده‌های بالاتر بگیرند. یکی از مهم‌ترین نکات در گام نخست ورود به هر رشته‌ی تخصصی، آشنایی با مسیر یادگیری و آموختن عمیق مفاهیم پایه‌ی مربوط به آن رشته است. شاید بتوان ادعا کرد یادگیری صحیح اصول پایه در رشته‌ی امنیت سایبری نسبت به بسیاری از رشته‌های تخصصی دیگر حتی از اهمیت بالاتری نیز برخوردار است زیرا بسیاری از آسیب‌پذیری‌ها و اشتباهات انسانی در امن‌سازی دارایی‌های سازمان یا حتی ارزیابی امنیت آن‌ها که در دنیای واقعی مشاهده می‌کنیم، ناشی از عدم آشنایی یا درک صحیح کارشناسان امنیتی از همین مفاهیم پایه است.

بنابراین فارغ از این‌که قصد ورود به مسیر قرمز (امنیت تهاجمی) یا مسیر آبی (امنیت دفاعی) را داشته باشید، ابتدا نیاز است تا مفاهیم پایه را به خوبی بیاموزید. حتی شاید بهتر باشد تصمیم‌گیری برای انتخاب تخصص را به بعد از گذراندن دوره‌های پایه موکول کنید.

این دوره برای افرادی طراحی شده که به عنوان نخستین تجربه‌ی خود در دنیای فناوری اطلاعات، قصد ورود به زمینه‌ی امنیت سایبری را دارند. برخی از مهم‌ترین موضوعاتی که با گذراندن این دوره خواهید آموخت به شرح زیر است:

- مفاهیم شبکه‌های کامپیوتری
- مدل‌های ارتباطی در شبکه‌های کامپیوتری
- انواع تجهیزات امنیتی و ارتباطی در شبکه‌های کامپیوتری
- پروتکل‌های پرکاربرد TCP/IP
- سویچینگ و مسیریابی در لایه‌های ۲ و ۳
- شبکه‌های بی‌سیم
- مفاهیم ابتدایی امنیت سایبری
- آشنایی با حملات سایبری مختلف

مدت زمان دوره

مدت این دوره ۳۳ ساعت است که طی ۱۱ جلسه ۳ ساعته و در روزهای زوج از ساعت ۱۷ تا ۲۰ برگزار خواهد شد. تاریخ شروع دوره از دوشنبه ۹۹/۰۵/۲۷ می باشد.

این دوره به چه افرادی توصیه می شود؟

- علاقه مندان ورود به صنعت امنیت سایبری
- دانشجویان رشته های فناوری اطلاعات و سایر رشته های مربوطه
- مهندسين نرم افزار علاقه مند به افزایش دانش خود در زمینه ی زیرساخت و پروتکل های پرکاربرد
- کارشناسان پشتیبانی شرکت های فعال در زمینه ی فناوری اطلاعات

برای شرکت در این دوره چه دانش هایی باید داشته باشم؟

با توجه به این که این دوره، نقطه ی شروع ورود به دنیای امنیت سایبری است، بنابراین افراد برای حضور در این دوره نیاز به دانش خاصی ندارند و آشنایی با مفاهیم ابتدایی و تجهیزات متداول در دنیای فناوری اطلاعات کافی است. برای ثبت نام در این دوره می توانید از [اینجا](#) اقدام کنید.

Chapter 1: Introduction to Networks

1.1 What is network?

- 1.1.1 Local Area Network (LAN)
- 1.1.2 Wide Area Network (WAN)
- 1.1.3 Internet
- 1.1.4 Peer to Peer Model
- 1.1.5 Client/Server Model

1.2 Physical Network Topologies

1.3 OSI Model

Chapter 2: Network Topologies and Connectors

2.1 Network Topologies Overview

2.2 Physical Media

2.3 Cable Types

2.4 Ethernet Basics

- 2.4.1 Collision Domain
- 2.4.2 Broadcast Domain
- 2.4.3 CSMA/CD
- 2.4.4 Wavelength
- 2.4.5 Half-Duplex and Full-Duplex Ethernet
- 2.4.6 Broadband/Baseband
- 2.4.7 Power over Ethernet (PoE)
- 2.4.8 Ethernet Addressing

Chapter 3: Network Devices

3.1 Network Interface Cards

3.2 Hub and Bridge

3.3 Switch

3.4 Router

3.5 Firewall

3.6 IDS/IPS

3.7 HIDS

3.8 EDR

3.9 WAF

3.10 SIEM

3.11 HSM

3.12 Load Balancer

3.13 Proxy Server

3.14 VoIP PBX

3.15 VoIP Gateway

3.16 Cache Server

3.17 Access Point

Chapter 4: Introduction to TCP/IP

4.1 TCP/IP Stack Overview

4.2 TCP/IP Protocols

4.3 TCP & UDP Header

Chapter 5: Introduction to IPv4

5.1 IPv4 Overview

5.2 Hierarchical IP Addressing Scheme

5.2.1 Network Addressing & IPv4 Classes

5.2.2 Private IPv4 Addresses

5.2.3 Public IPv4 Addresses

5.3 IPv4 Subnetting

5.3.1 Subnetting Basics

5.3.2 Subnet Masks

5.3.3 Subnetting Class C Addresses

5.3.4 Subnetting Class B Addresses

5.3.5 Subnetting Class A Addresses

5.4 IPv4 Header

5.5 Network Address Translation (NAT)

Chapter 6: IPv6

6.1 IPv6 Overview

6.2 The Benefits of Using IPv6

6.3 IPv6 Addressing

6.4 Shortened Expression

6.5 Address Types

6.6 Special Addresses

6.7 Stateless Autoconfiguration

Chapter 7: IP Routing Basics

7.1 IP Routing Overview

7.2 Static & Dynamic Routing

7.3 IP Routing Protocols

7.3.1 RIP

7.3.2 OSPF

7.3.3 EIGRP

7.3.4 BGP

7.4 High Availability

7.4.1 Virtual Router Redundancy Protocol

7.4.2 Hot Standby Router Protocol (HSRP)

7.5 Advanced IPv6

7.5.1 Router Advertisement

7.5.2 Neighbor Discovery

7.5.3 Tunneling

7.5.4 Dual Stack

7.6 IPv6 Routing Protocols

7.6.1 RIPng

7.6.2 EIGRPv6

7.6.3 OSPFv3

Chapter 8: Switching and Virtual LANs

8.1 Layer 2 Switching Overview

8.2 Spanning Tree Protocol (STP)

8.3 Virtual LAN (VLAN)

8.4 VLAN Trunking Protocol

8.5 Port Mirroring/Spanning

Chapter 9: Wireless Networks

9.1 Wireless Networks Overview

9.2 The 802.11 Standards

9.3 Wireless Network Components

9.4 Wireless Network Threats

Chapter 10: Authentication and Access Control

10.1 Introduction

10.2 Access Control Lists

10.3 Managing User Account and Password Security

10.4 User Authentication Methods

10.4.1 Kerberos

10.4.2 Authentication, Authorization and Accounting (AAA)

10.4.3 Network Access Control (NAC)

10.4.4 Challenge Handshake Authentication Protocol (CHAP)

10.4.5 MS-CHAP

10.4.6 Extensible Authentication Protocol (EAP)

10.5 LDAP

Chapter 11: Encryption

11.1 Encryption Basics

11.1.1 Goals of Encryption

11.1.2 What is an Encryption Algorithm?

11.2 Types of Encryption

11.2.1 Symmetric Encryption

11.2.2 Asymmetric Encryption

11.3 Hashing Functions Basics

11.3.1 Common Hashing Functions

11.3.2 Why and where do We Use Hashing?

11.4 PKI Fundamentals

11.4.1 Certificates

11.4.2 Certificate Authorities

11.5 SSL\TLS Overview

11.5.1 SSL Handshake

11.5.2 HTTPS

Chapter 12: Virtual Private Network (VPNs)

12.1 Virtual Private Networks Overview

12.2 Packet Encapsulation

12.3 Tunneling Overview

12.4 Tunneling Protocols

12.5 VPN Overview

12.6 VPN Protocols

Chapter 13: Introduction to TCP/IP Cyber Threats

13.1 Cyber Threats Overview

13.2 Application Layer Cyber Threats

13.3 Internet Layer Cyber Threats

13.4 Network Access Link Layer Cyber Threats

درباره‌ی آکادمی راوین

شاید اغراق نباشد اگر بگوییم این روزها بزرگ‌ترین چالش پیش روی سازمان‌ها، شرکت‌ها و استارت‌آپ‌های فعال در صنعت فناوری اطلاعات، کمبود نیروی انسانی متخصص در کشور است. در حالی که تعداد افراد جویای کار هر روز بیشتر می‌شود، کماکان اغلب شرکت‌ها در تامین نیروی متخصص مورد نیاز خود با مشکلات جدی مواجه هستند.

با توجه به چالش‌های موجود در کشور، تصمیم گرفتیم تا با تاسیس «آکادمی راوین» قدمی در راستای هرچه کوچک‌تر کردن شکاف تخصصی موجود بین افراد جویای کار و نیاز شرکت‌های فعال در صنعت فناوری اطلاعات کشور برداریم. بر همین اساس، تمام دوره‌های آموزشی این موسسه مبتنی بر مسیرهای شغلی (Career Path) و به صورت تخصصی در زمینه‌ی امنیت سایبری طراحی و تدوین شده است. همچنین «آکادمی راوین» دو مسیر اصلی را برای تمام دوره‌های خود در نظر گرفته، به گونه‌ای که هر دوره‌ی آموزشی در یکی از این دو مسیر قرار می‌گیرد:

۱. مسیر «امنیت دفاعی» که با رنگ آبی مشخص شده است. دوره‌های آموزشی این مسیر، با هدف امن‌سازی زیرساخت‌ها و نرم‌افزارهای سازمان‌ها به منظور پیش‌گیری از نفوذ یا شناسایی و ردیابی نفوذگران طراحی شده است. همچنین این دوره‌ها شامل تحلیل روش‌ها و بدافزارهای مورد استفاده مهاجمین نیز می‌شود.

۲. مسیر «امنیت تهاجمی» که با رنگ قرمز مشخص شده است. هدف از این دوره‌های آموزشی، ارزیابی امنیتی زیرساخت‌های شبکه، نرم‌افزارهای وب، موبایل و غیره می‌باشد. به عبارت دیگر متخصصان این حوزه با شبیه‌سازی رفتار نفوذگران، نقاط ضعف و آسیب‌پذیری‌های امنیتی موجود را قبل از آن‌ها شناسایی می‌کنند.

تمام دوره‌های این موسسه در هر دو مسیر «آبی» و «قرمز»، بر اساس آخرین دانش روز دنیا و هم سطح دوره‌های ارایه شده در موسسات بزرگ بین‌المللی طراحی شده است و توسط به‌نام‌ترین مدرسین ایرانی و غیر ایرانی تدریس می‌شود. آخرین دوره‌های ارایه شده در آکادمی راوین را می‌توانید در صفحه‌ی [دوره‌های آموزشی](#) در وبسایت این موسسه دنبال کنید.

با ما در ارتباط باشید



 <https://twitter.com/ravinacademy>

 <https://linkedin.com/company/ravin-academy/about>

 <https://t.me/ravinacademy>

 info@ravinacademy.com

سهروردی شمالی، بین هوپزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم 

۰۲۱-۸۸۵۰۲۴۴۲ 