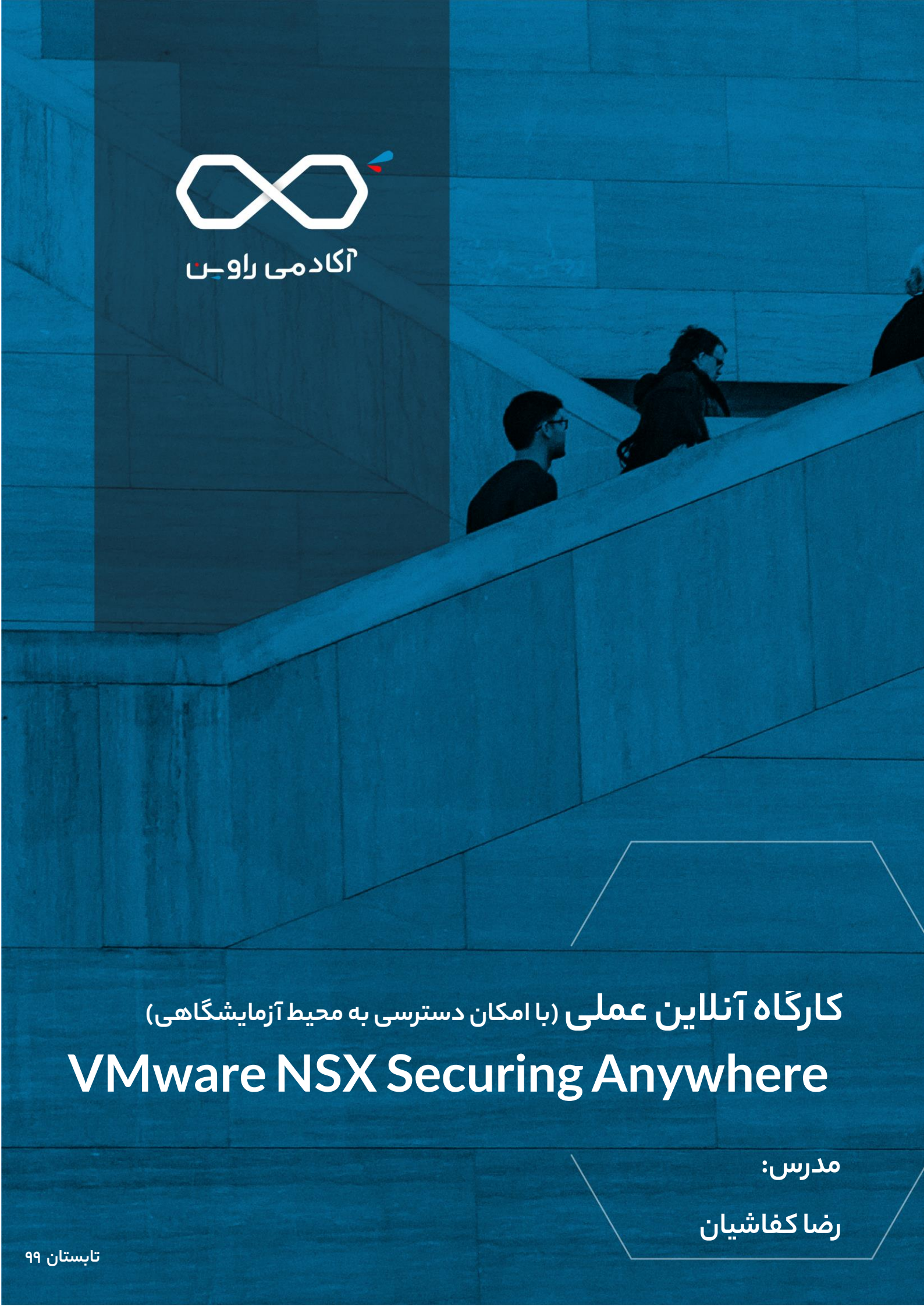

آکادمی راوین

کارگاه آنلاین عملی (با امکان دسترسی به محیط آزمایشگاهی)

VMware NSX Securing Anywhere

مدرس:

رضا کفاشیان

تابستان ۹۹

به‌نام خدا

درباره‌ی این دوره (آنلاین)

پلتفرم NSX یک راهکار مدیریت شبکه‌ی نرم‌افزار محور (SDN) است که توسط شرکت VMware ارایه شده و در واقع بخشی از مفهوم سطح بالاتر مرکز داده‌ی نرم‌افزار محور (SDDC) در زیرساخت‌های مجازی‌سازی این شرکت می‌باشد. پلتفرم NSX به شما قابلیت پیاده‌سازی و مدیریت زیرساخت رایانش ابری مبتنی بر فناوری مجازی‌سازی VMware را می‌دهد.

یکی از مهم‌ترین ویژگی‌های این پلتفرم، امکانات و قابلیت‌های متعدد موجود در آن در راستای طراحی و پیاده‌سازی زیرساخت‌های شبکه‌ی مجازی و ابری به صورت امن است. به عنوان مثال می‌توان به فایروال‌های لاجیکال، سوییچ، روتر، پورت و بسیاری از عناصر دیگر شبکه اشاره کرد. NSX همچنین قابلیت پیاده‌سازی، پیکربندی و امن‌سازی اپلیکیشن‌ها بین زیرساخت‌های ابری مختلف را نیز دارد.

یکی از پرکاربردترین راهکارهای NSX در زمینه‌ی امن‌سازی زیرساخت مجازی که در این دوره به آن می‌پردازیم مبحث NSX Firewall است که این قابلیت را به شما می‌دهد تا زیرساخت شبکه‌ی مجازی خود را بخش‌بندی کرده و امنیت بخش‌های مختلف را بدون هزینه‌های سخت‌افزاری و در عین حال بسیار موثرتر و مقیاس‌پذیرتر از راهکارهای امنیت سنتی، پیاده‌سازی و مدیریت کنید. در این دوره به معرفی، طراحی، پیاده‌سازی و پایش Micro-Segmentation پرداخته می‌شود.

مدت زمان دوره

مدت این کارگاه ۱۴ ساعت است که در طی دو روز (دو جلسه‌ی ۷ ساعته) به صورت آنلاین از ساعت ۱۱ تا ۱۸ برگزار می‌شود. شیوه‌ی تدریس به صورت عملی و در محیط آزمایشگاهی (برای استاد) خواهد بود. تاریخ برگزاری این دوره روزهای پنج‌شنبه و جمعه مورخ ۱۳ و ۱۴ شهریور ماه ۹۹ می‌باشد.

دسترسی به محیط آزمایشگاهی

در صورتی که نیاز به محیط آزمایشگاهی برای تمرین آموخته‌های خود داشته باشید، باید بلیط ویژه‌ی دوره (با امکان دسترسی به محیط آزمایشگاه اختصاصی از روز برگزاری به مدت یک ماه) را از ایوند خریداری کنید. در غیر این‌صورت به منظور صرفه‌جویی در هزینه می‌توانید بلیط حضور در دوره را تهیه کنید.

این دوره برای چه افرادی توصیه می‌شود؟

- کارشناسان امنیت شبکه
- کارشناسان زیرساخت‌های مجازی‌سازی VMware
- کارشناسان مرکز داده
- مشاورین و مدیران امنیت سایبری

برای شرکت در این دوره چه دانش‌هایی باید داشته باشم؟

- آشنایی با مفاهیم و اصول شبکه
- آشنایی با پروتکل‌های پرکاربرد TCP/IP
- آشنایی با مفاهیم و تعاریف حملات سایبری
- آشنایی با زیرساخت‌های مجازی‌سازی VMware
- حداقل یک سال تجربه‌ی کار در زمینه‌های مرتبط

برای ثبت‌نام در این دوره می‌توانید از اینجا اقدام کنید.

سهروردی شمالی، بین هویزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم
info@ravinacademy.com

آکادمی راوین

سرفصل‌های این دوره

Chapter 1: NSX Overview

1.1 Introduction to VMware NSX

1.2 NSX Architecture Components

1.3 Introduction to Security Solutions with NSX

Chapter 2: Micro-Segmentation Overview

2.1 Micro-segmentation Anywhere with VMware NSX

2.2 Acceptable Security in the Modern Data Center

2.3 Defining Micro-segmentation

2.4 Alignment with Emerging Cyber Security Standards

2.5 Micro-segmentation with NSX as a Security Platform

2.6 Securing Physical Workloads

Chapter 3: Physical Security in a Virtual World

3.1 Defining security requirements based on application deployment model or environment type

3.2 Understanding methods of protection in modern data centers

3.3 How NSX provides micro-segmentation for both physical and virtual workloads

3.4 How integration with ecosystem security and network controls functions

3.5 Deployment Examples

Chapter 4: Operationalizing Micro-segmentation

4.1 Micro-segmentation design patterns

4.2 Determining appropriate security groups and policies

4.3 Deploying micro-segmentation

4.4 Application lifecycle management with vRealize Automation and NSX

4.5 LAB: Deployment and Operating for micro-segmentation

Chapter 5: Micro-segmentation with Service Insertion

5.1 Defining Service Insertion

5.2 The Role of Service Insertion in Micro-segmentation

5.3 Network and Guest Introspection

5.4 NSX Service Insertion

Chapter 6: Context, Visibility and Containment

Chapter 7: Micro-segmentation Benchmark

7.1 Objectives of the NSX Micro-audit

7.2 Threat Simulation Methodology

7.3 Simulating Attacks

آکادمی راوین

درباره‌ی آکادمی راوین

شاید اغراق نباشد اگر بگوییم این روزها بزرگ‌ترین چالش پیش روی سازمان‌ها، شرکت‌ها و استارتاپ‌های فعال در صنعت فناوری اطلاعات، کمبود نیروی انسانی متخصص در کشور است. در حالی‌که 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، به‌گونه‌ای 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.

سهروردی شمالی، بین هویزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم
info@ravinacademy.com

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 هویزه و خرمشهر، کوچه‌ی نقدی، پلاک ۳۶، واحد سوم

۰۲۱-۸۸۵۰۲۴۴۲