



دوره ها



جهانے فکر کنیم؛
جهانے بیاموزیم



درآمد بر آکادمی راوین

با توجه به چالش‌های دانشی موجود در صنعت امنیت سایبری کشور از یک سو و کمبود نیروی متخصص آماده به کار از سوی دیگر، «آکادمی راوین» در راستای هرچه کوچک‌تر کردن شکاف تخصصی موجود بین افراد جویای کار و نیاز شرکت‌های فعال در صنعت فناوری اطلاعات کشور تاسیس شد. آکادمی راوین فعالیت خود را از سال ۹۸ به صورت تخصصی در زمینه‌ی آموزش و تحقیقات امنیت سایبری با هدف شکستن ساختارهای سنتی امنیت در ایران و ایجاد حرکت به سوی دانش و فناوری‌های لبه‌ی دنیا، آغاز کرد.

آکادمی راوین در زمینه‌ی ارائه‌ی دوره‌های تخصصی امنیت سایبری در ایران، پیشرو بوده و تمام دوره‌های آموزشی آن توسط برترین **متخصصان داخلی و خارجی** همگام با دانش روز دنیا طراحی و تدریس می‌شود. در واقع تولید محتوای این دوره‌های آموزشی اختصاصی، به طور کامل توسط اساتید آکادمی، براساس متدهای روز و هم سطح دوره‌های ارائه شده در موسسه‌های بزرگ **بین‌المللی** انجام شده است.

یکی از ویژگی‌های تیم آکادمی راوین که آن را از سایر موسسه‌های فعال متمایز می‌کند، وجود تخصص‌های متنوع و ناب در این تیم است که از بین آن‌ها می‌توان به تخصص‌های فازینگ و کشف آسیب پذیری، اکسپلویت نویسی در لایه‌های مختلف ویندوز و لینوکس، هک وب و موبایل، تیم قرمز، تحلیل بدافزار، مهندسی معکوس، شکار تهدیدات سایبری و بسیاری از موارد دیگر اشاره کرد.

این دوره‌ها در سه مسیر قرمز، آبی و بنفش، متناسب با نیازهای شغلی کشور و مبتنی بر جایگاه‌های تخصصی این مشاغل در کشورهای توسعه‌یافته و پیشرو طراحی و ارائه می‌شود.

مسیر آبی، شامل دوره‌های آموزشی «امنیت دفاعی» بوده و هدف آن، امن‌سازی زیرساخت‌ها و نرم‌افزارهای سازمان‌ها به‌منظور پیش‌گیری از نفوذ یا شناسایی و ردیابی نفوذگران است. همچنین، این دوره‌ها شامل تحلیل روش‌ها و بدافزارهای مورد استفاده‌ی مهاجمان نیز می‌شود.

در مقابل آن، **مسیر قرمز** است که شامل دوره‌های آموزشی «امنیت تهاجمی» می‌شود و هدف آن، ارزیابی امنیتی زیرساخت‌های شبکه، نرم‌افزارهای وب، موبایل و غیره است. به عبارت دیگر، متخصصان این حوزه با شبیه‌سازی رفتار نفوذگران، نقاط ضعف و آسیب‌پذیری‌های امنیتی موجود را قبل از آن‌ها شناسایی می‌کنند.

مسیر بنفش، ترکیبی از آموزش‌های «امنیت دفاعی» و «امنیت تهاجمی» است. به عبارت دیگر، مخاطبان در این دوره‌ها، با انواع تکنیک‌ها و تاکتیک‌های مربوط به حملات سایبری آشنا شده و سپس راهکارهای مقابله، شناسایی و پاسخ به این تهدیدات را نیز فرا خواهند گرفت.

در ادامه، فهرست دوره‌های آکادمی راوین به صورت خلاصه ارائه شده است. در صورت نیاز به دریافت شناسنامه‌ی هر دوره، با آکادمی در تماس باشید. لازم به ذکر است، علاوه بر دوره‌های شرح داده شده، آکادمی راوین آمادگی دارد تا دوره یا مسیر آموزشی مورد نیاز سازمان شما را به صورت اختصاصی طراحی و ارائه کند.

RED



۳۲ ساعت

Windows Internals For Red Teaming

این دوره، به آموزش اجزای اصلی سیستم عامل ویندوز، معماری و شیوهی ارتباط آنها با یکدیگر و روش های بهره برداری از این قابلیت ها می پردازد. به عبارت دیگر، با حضور در این دوره، با معماری ویندوز آشنا می شوید و مباحثی، مانند مدیریت حافظه، پروسس های ویندوز، I/O، Thread، معماری امنیت ویندوز و بسیاری از موارد دیگر را خواهید آموخت.



۴۰ ساعت

Penetration Testing Zero To Hero

با گذراندن این دوره، شما طیف گسترده ای از دانش های مورد نیاز برای تبدیل شدن به یک هکر کلاه سفید، شامل مبانی امنیت سایبری، مبانی امنیت انواع سیستم عامل ها، مبانی هک شبکه های کامپیوتری، مبانی هک وب، ارزیابی آسیب پذیری و تهدیدات سایبری و در نهایت فرایند کامل تست نفوذ و ارائه ی گزارش از نتایج ارزیابی را خواهید آموخت.



۳۰ ساعت

Android Penetration Testing Professional

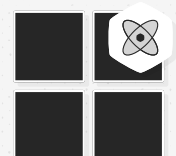
با گذراندن این دوره، با انواع حملات بر روی اپلیکیشن های اندرویدی آشنا شده و در انتهای دوره می توانید یک اپلیکیشن اندرویدی را از دیدگاه امنیت تهاجمی ارزیابی و تحلیل کنید. با استفاده از دانش کسب شده در این دوره، می توانید از وقوع بسیاری از حملات مبتنی بر اندروید پیش گیری کرده و تهدیدات مربوطه را پیش از وقوع شناسایی کنید.



۱۲ ساعت

Offensive System/Kernel Development For Windows

با حضور در این دوره به مواردی، مانند ساختار سیستم عامل ویندوز، Kernel Objects API، فرایندهای ویندوز، thread در ویندوز، کار با حافظه، DLL ها، رجیستری، درایورها، کار با کرنل و بسیاری از مباحث دیگر مسلط می شوید.



۳۰ ساعت

JavaScript Security

با حضور در این دوره، به مباحث مختلفی، مانند ساختار کلی زبان JavaScript، ساختار مرورگرهای وب، باگ‌های سمت کاربر و سایر موارد تسلط پیدا خواهید کرد.



۸ ساعت

AV/EDR Bypass

در این بوت‌کمپ ضمن آشنایی با شیوه‌ی عملکرد و معماری آنتی‌ویروس‌ها و EDRها، برخی روش‌های دور زدن (Bypass) این محصولات را خواهید آموخت. به‌طور دقیق‌تر شما با گذراندن این بوت‌کمپ، مبانی معماری آنتی‌ویروس و EDR و شیوه‌ی عملکرد آنها، دور زدن این محصولات در مراحل مختلف Red Teaming به شکل کاربردی، روش‌های دور زدن راهکار AMSI در سیستم‌عامل ویندوز و در نهایت مباحثی، مانند Credential Dumping و کاربرد آنها برای توسعه ابزارهای مختلف را خواهید آموخت.



۳۰ ساعت

Web3 & Smart Contract Programming

با گذراندن این دوره، شما با مبانی بلاک‌چین و الگوریتم‌های رمزنگاری آن آشنا می‌شوید و برنامه‌نویسی و توسعه‌ی قراردادهای هوشمند را خواهید آموخت. به‌این‌ترتیب آماده‌ی ادامه‌ی مسیر یادگیری امنیت سایبری در Web3 خواهید شد.



۴۰ ساعت

Active Directory Attacks

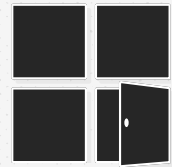
با گذراندن این دوره، شما علاوه‌بر مرور مفاهیم مرتبط با ساختار ویندوز و Active Directory، انواع حملات سایبری مبتنی‌بر Active Directory در زمینه‌های مختلف را مانند جمع‌آوری اطلاعات، گسترش دسترسی، دور زدن راهکارهای پیشرفته‌ی شناسایی، پایدارسازی دسترسی و بسیاری از موارد دیگر خواهید آموخت.



۱۸ ساعت

Windows Persistence Techniques

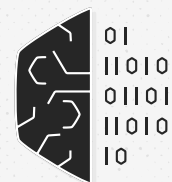
در این دوره، روش‌های مختلف پایداریسازی دسترسی در زیرساخت‌های مبتنی بر سیستم‌عامل ویندوز، که در حملات تیم‌های APT مختلف از آن‌ها استفاده می‌شود، به صورت عملی و سناریو محور بررسی خواهد شد. شما در این دوره، با انواع روش‌های پایداریسازی دسترسی، شامل روش‌هایی که با سطح دسترسی پایین قابل اجرا هستند، روش‌هایی که اجرای آن‌ها به سطح دسترسی Admin نیاز دارد و در نهایت، انواع روش‌های پایداریسازی دسترسی در Domain Controller سازمان، آشنا خواهید شد.



۱۹ ساعت

Web Logic Attacks

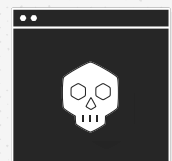
با حضور در دوره‌ی Web Logic Attacks ضمن آشنایی با این نوع از آسیب‌پذیری‌ها، دانش‌های کاربردی از حملات منطقی، مانند مفاهیم آسیب‌پذیری‌های منطقی، منطق‌های کسب‌وکاری، نقاط ضعف منطقی در کنترل دسترسی، نقاط ضعف منطقی در احراز هویت و بسیاری موارد دیگر را به صورت عملی خواهید آموخت.



۲۸ ساعت

Introduction To Web Hacking

این دوره در سطح پایه و برای افراد علاقه‌مند به امنیت سایبری که تجربه‌ی کمی داشته‌اند و قصد ورود به مسیر آموزش تست نفوذ وب (یا شکار باگ) را دارند، طراحی شده است. شما با گذراندن این دوره مباحث گسترده‌ای، مانند ساختار و فرایند تست نفوذ، پروتکل‌های مهم و شیوه‌ی ارتباط اجزای وب، ساختار سامانه‌های تحت وب، مبانی احراز هویت و کنترل دسترسی، شیوه‌ی کار Browserها، مفاهیم پایگاه داده، مفاهیم سرویس‌ها و میکروسرویس‌های تحت وب، مفاهیم زیرساخت‌های ابری و CDN، کار با پرکاربردترین ابزارهای تست نفوذ، مبانی شناسایی و جمع‌آوری اطلاعات از هدف و بهره‌برداری از آسیب‌پذیری‌های موجود را به صورت کاربردی و در سطح پایه خواهید آموخت.



BLUE



۲۴ ساعت

ICS Cybersecurity Fundamental

این دوره‌ی آموزشی، با تمرکز بر سامانه‌های کنترل صنعتی موجود در زیرساخت‌های حیاتی، ضمن بیان چالش‌های امنیتی آن‌ها، روند حملات و رخداد‌های امنیتی مرتبط را تحلیل و بررسی می‌کند و راهبردها و راهکارهای مقاوم‌سازی و کاهش خطرهای امنیتی در این زیرساخت‌ها را آموزش می‌دهد.



۲۴ ساعت

Cisco Ise Device Administration And NAC

در این دوره، شما ساختار سامانه‌ی CISCO ISE، دستورهای و پیکربندی آن، مدیریت تجهیزات و استفاده از آن، پیکربندی Radius، TACACS، Dot1x، انواع کنترل دسترسی، پایش دسترسی‌ها و بسیاری از موارد دیگر را به صورت عملی خواهید آموخت.



۱۹ ساعت

Windows Log Analysis

این دوره‌ی آموزشی، بر روی فهم بهتر آن‌چه در ویندوز در حال وقوع است، به وسیله‌ی Log‌هایی که در سطوح مختلف ویندوز وجود دارد، متمرکز است. دانشجویان بعد از گذراندن این دوره، دید جامعی نسبت به مآزول‌های مختلف Logging پیدا کرده و با شیوه‌ی کنار هم چیدن آن‌ها، به منظور تحلیل‌های موثر آشنا می‌شوند.

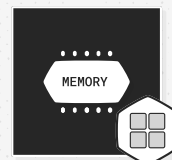


۴۲ ساعت

Professional Windows Memory Analysis

این دوره، با هدف بررسی حافظه‌ی سیستم‌عامل ویندوز و پروسه‌های آن، به صورت Live و به کمک Dump، به صورتی طراحی شده است که موارد زیر را پوشش داده و می‌تواند برای برنامه‌نویسان و متخصصان امنیت، بسیار کاربردی باشد:

- آشنایی با ساختارهای Internal ویندوز و شیوه‌ی عملکرد آن‌ها
- بررسی موارد مشکوک در ویندوز و استفاده از آن برای Malware Hunting
- دلیل بروز استثنا در برنامه‌ها و پیدا کردن Bug
- بررسی دلیل Hang و Crash در پروسه‌ها و سیستم‌عامل



۱۲۰ ساعت

SOC Tier 1 Operations Zero To Hero

این دوره ی جامع با هدف آموزش دانش مورد نیاز برای تبدیل شدن به کارشناس لایه ی یک در مراکز عملیات امنیت، با چهار ماژول اصلی به شرح زیر ارائه شده است:

- عملیات امنیت و مانیتورینگ
- تحلیل ترافیک
- مبانی کار با Splunk
- تحلیل SIEM و تیم آبی



۴۲ ساعت

SOC Management

این دوره، با توجه به نیاز موجود در سازمان های کشور جهت پیاده سازی و مدیریت بهینه ی مراکز عملیات امنیت، طراحی و ارائه شده است. مخاطبان، با گذراندن این دوره مباحث مختلف مربوط به مدیریت SOC، از جمله طراحی و برنامه ریزی عملیات SOC، بخش های مختلف معماری SOC، فرایندهای شناسایی، شکار و پاسخ به تهدیدات سایبری، راهکارها و فرایندهای خودکارسازی وظایف و بسیاری از موارد دیگر را به صورت نظری و عملی خواهند آموخت.



۳۹ ساعت

Network Security Professional

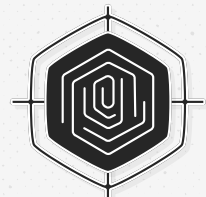
مسیر آموزشی کوتاه «امنیت شبکه» که شامل دو دوره ی «Network & Protocols Fundamentals» و «Network Security Professional» است در آکادمی راوین طراحی و ارائه شده است. در دوره ی اول (Network & Protocols Fundamentals) شما تمام مفاهیم و دانش پایه ی مورد نیاز برای ورود به دنیای امنیت شبکه را می آموزید. با گذراندن این دوره، انواع تهدیدات سایبری و روش های مقابله با این تهدیدات در لایه های مختلف شبکه را به صورت عملی خواهید آموخت.



۴۰ ساعت

Threat Hunting & Incident Response

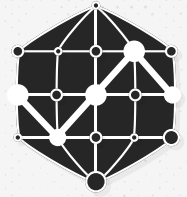
در طی این دوره، شما با انواع تکنیک ها، تاکتیک ها و به طور کلی روش کار مهاجمان سایبری پیشرفته و تیم های APT آشنا شده و روش های شکار این تهدیدات، تحلیل تکنیک ها و پاسخ به آنها را به صورت عملی خواهید آموخت. به عبارت دیگر، شما دانش مربوط به روش عملکرد و شکار انواع روش های مورد استفاده ی تیم های APT (مانند بدافزارهای Fileless، روش های پیشرفته ی گسترش و پایداری دسترسی، حملات باج افزار و بسیاری موارد مشابه دیگر) را مبتنی بر چارچوب MITRE ATT&CK و همچنین شیوه ی پاسخ به این حملات را کسب خواهید کرد.



۵ ساعت

Network Traffic Analysis

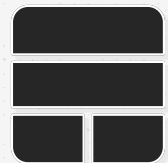
این دوره، در کنار معرفی و استفاده از ابزارهای مختلف، بر روی آموزش مفاهیم اصولی پروتکل‌های پرکاربرد و ساختار بسته‌های آن‌ها تمرکز دارد. با حضور در این دوره، اصول تحلیل ترافیک شبکه، پروتکل‌های پرکاربرد TCP/IP و ساختار بسته‌های هریک، استخراج اطلاعات از این بسته‌ها، تحلیل اطلاعات با ابزارهایی مانند Wireshark، TCPDump، Splunk و بسیاری از موارد دیگر را خواهید آموخت.



۲۰ ساعت

Build ELK As A SIEM

در این دوره، به آموزش پیکربندی ELK با هدف آماده‌سازی آن به عنوان یک SIEM پیشرفته پرداخته می‌شود. به عبارت دیگر در طی دوره، این پلتفرم برای استفاده‌های امنیتی اعم از جمع‌آوری و تحلیل لاگ، Analytics، Enrichment، Correlation، Dashboard و غیره پیکربندی خواهد شد.



۸ ساعت

WebShell Hunting

در این کارگاه، شناسایی انواع وب‌شل‌های شناخته‌شده و شناخته‌نشده با استفاده از روش‌های متنوع به مخاطبان آموزش داده می‌شود. همچنین ابزارها، رول‌های شناسایی و اسکریپت‌های مختلفی برای این منظور در بخش‌های مختلف ارائه می‌شود.



۲۸ ساعت

Threat Hunting Using Sysmon

با حضور در این کارگاه، ضمن آشنایی با ساختار Sysmon، مواردی مانند پیکربندی Sysmon، ساختار و گام‌های شناسایی تهدیدات سایبری، مفاهیم شکار تهدیدات سایبری، ساختار Event IDهای ویندوز، شناسایی حملات سایبری و بسیاری از موارد دیگر را به صورت عملی خواهید آموخت. همچنین، چندین سناریوی حملات سایبری در دنیای واقعی و شیوه‌ی شکار آن‌ها را تحلیل خواهیم کرد.



۳۰ ساعت

Android Reverse Engineering

این دوره، به بررسی ابزارها، رویکردها و روش‌های مهندسی معکوس اپلیکیشن‌های اندرویدی، در کنار شیوه‌ی تعامل برنامه‌ها با سیستم‌عامل و بخش‌های مختلف اندروید می‌پردازد. شما پس از گذراندن این دوره، قادر خواهید بود ساختمان و شیوه‌ی کار یک اپلیکیشن اندرویدی را طی فرایند مهندسی معکوس کشف کنید.



۶۰ ساعت

Digital Forensic Zero To Hero

این دوره، به‌گونه‌ای طراحی شده است تا شما را با طیف گسترده‌ای از تکنیک‌ها و روش‌های Forensic آشنا کند. در واقع با گذراندن این دوره، شما خواهید توانست ردپای مهاجمان را در زیرساخت شبکه، سامانه‌های ویندوزی و سامانه‌های لینوکسی، ردیابی و تحلیل کنید. همچنین، کار با فایل سیستم‌های مختلف، بازیابی اطلاعات دیسک‌ها، بررسی داده‌های موجود در RAM، تحلیل وقایع و در نهایت تهیه‌ی گزارش از مدارک به دست آمده را نیز خواهید آموخت.



۳۰ ساعت

VMware NSX Securing Anywhere

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.



۲۴ ساعت

Cyber Security Strategy Development

این دوره، دانش مورد نیاز برای تدوین اهداف و استراتژی امنیت سازمان را مطابق با استانداردهای جهانی، به مخاطبان آموزش خواهد داد. از مهم‌ترین سرفصل‌های این دوره می‌توان به آشنایی با مفاهیم کسب‌وکار، شناسایی اولویت‌های کسب‌وکار، شناخت ساختار و توزیع قدرت در سازمان، مفاهیم استراتژی، تدوین استراتژی امنیت سایبری و همسوسازی آن با اولویت‌های کسب‌وکار سازمان اشاره کرد.



PURPLE





Purple Team

این دوره ی جامع، به گونه ای طراحی شده است که شما با گذراندن آن، انواع تیم های امنیتی، ساختار تهدیدات APT و تکنیک های پیشرفته ی اخذ دسترسی اولیه، جمع آوری اطلاعات، گسترش دسترسی، پایداری سازی دسترسی، حملات اکتیو دایرکتوری، Lateral Movement و دور زدن راهکارهای امنیتی را به همراه روش های شناسایی و مقابله با این تهدیدات و ابزارهای دفاعی مدرن را به همراه بررسی سناریوهای APT عملی، خواهید آموخت.

INTER NATIONAL



دوره‌ها و بین‌المللی

آکادمی راوین آمادگی دارد تا علاوه بر عناوین آموزشی خود، انواع دوره‌های امنیت سایبری ارائه شده توسط موسسه‌های معتبر بین‌المللی را نیز به صورت اختصاصی برای سازمان‌ها برگزار کند. این دوره‌ها، امکان برگزاری به صورت حضوری (در محل کارفرما یا آکادمی) و آنلاین را خواهند داشت.



CompTIA®

SANS



(ISC)²®

EC-Council



آکادمی راورین



info@ravinacademy.com