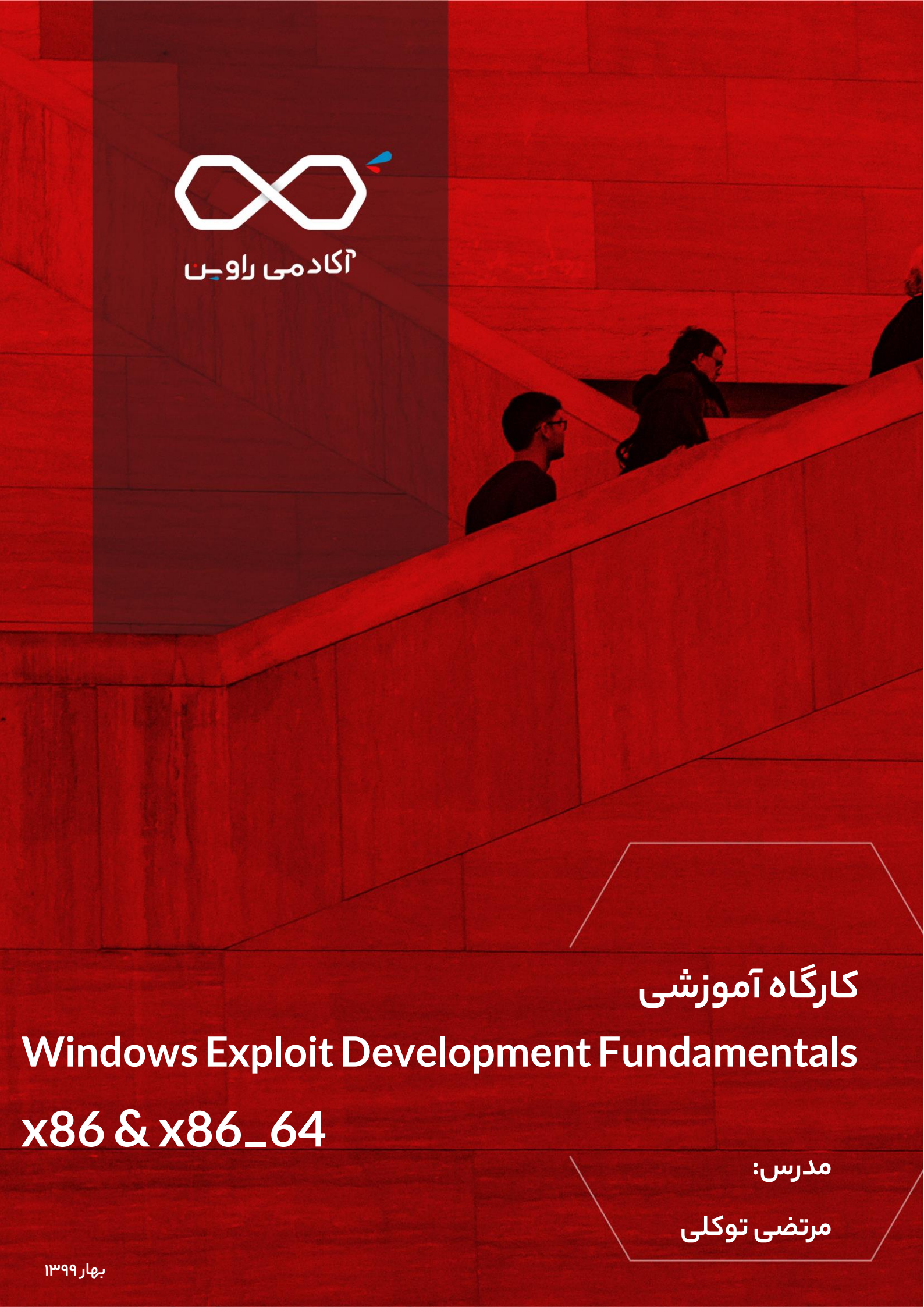

آکادمی راوین

کارگاه آموزشی

Windows Exploit Development Fundamentals

x86 & x86_64

مدرس:

مرتضی توکلی

بهار ۱۳۹۹

به‌نام خدا

درباره‌ی این دوره

اخبار مربوط به Exploit سیستم‌عامل‌ها و سرویس‌های پرکاربرد، همواره یکی از چالش برانگیزترین مباحث موجود در زمینه‌ی امنیت سایبری بوده است. چرا که مهاجمین ممکن است تنها با Exploit کردن موفق یک آسیب‌پذیری، بتوانند بخش قابل توجهی از تدابیر و لایه‌های امنیتی سازمان‌های قربانی را دور بزنند. Exploitها انواع مختلفی دارند و می‌توانند با اهداف متفاوتی مانند گرفتن دسترسی اولیه، گسترش دسترسی، خراب‌کاری و غیره توسعه داده شوند. اما کشف آسیب‌پذیری جدید در سیستم‌عامل‌ها و نوشتن Exploit برای آن‌ها نیاز به دانش و خلاقیت بالایی دارد و همین نکته سبب شده تا افراد محدودی در این زمینه به موفقیت‌های چشم‌گیری دست یابند.

اما با توجه به موارد ذکر شده، چرا هکرهای کلاه‌سفید باید این دانش را فرا بگیرند؟ دلایل متعددی می‌توان برای آن برشمرد که برخی از مهم‌ترین آن‌ها به شرح زیر است:

- شناسایی آسیب‌پذیری‌های موجود قبل از افراد سودجو و خراب‌کار
- شرکت در برنامه‌های Bug Bounty و کسب درآمد
- آشنایی با دانش Exploit در راستای افزایش آمادگی برای مقابله با این تهدیدات

در همین راستا آکادمی راوین برای علاقه‌مندان این حوزه، مسیر آموزش محقق امنیت ویندوز را ارایه کرده است که شامل سه دوره‌ی اکسپلویت‌نویسی پایه، پیشرفته و سطح هسته‌ی سیستم‌عامل می‌شود.

این دوره، به عنوان نقطه‌ی شروع مسیر اکسپلویت‌نویسی ویندوز محسوب شده و مخاطبان با حضور در این کارگاه، مباحثی مانند معماری پردازش‌گرها، دستورات و برنامه‌نویسی اسمبلی x86 و x86_64، کار با کامپایلر GCC و دیباگر GDB، مفاهیم Opcode، Buffer overflow و بسیاری از موارد دیگر را خواهند آموخت.

مدت زمان دوره

مدت زمان این دوره ۳۲ ساعت است که به صورت کارگاه ۴ روزه (و در هر روز ۸ ساعت) از ساعت ۱۰ صبح تا ۶ بعد از ظهر در روزهای ۲۳ و ۲۴ و ۳۰ و ۳۱ مرداد سال ۱۳۹۹ (پنج‌شنبه و جمعه) تدریس خواهد شد.

این دوره به چه افرادی توصیه می‌شود؟

- تحلیل‌گران و محققین امنیت سایبری
- کارشناسان ارشد ارزیابی امنیت/تست نفوذ/تیم قرمز
- کارشناسان فعال در زمینه‌ی Bug Bounty
- برنامه‌نویسان علاقه‌مند به توسعه‌ی امن
- کارشناسان لایه ۳ در SOC
- افراد علاقه‌مند به حضور در مسابقات CTF
- افراد علاقه‌مند به ورود به دنیای Exploit

برای شرکت در این دوره چه دانش‌هایی باید داشته باشم؟

- آشنایی با مفاهیم و ساختار سیستم‌عامل ویندوز
- آشنایی با محیط کاری سیستم‌عامل‌های مبتنی بر لینوکس
- آشنایی ابتدایی با اسمبلی ۳۲ و ۶۴ بیتی
- آشنایی با حملات سایبری در سطح سیستم عامل مانند گسترش دسترسی و غیره
- آشنایی با زبان برنامه‌نویسی C یا C++ در سطح متوسط
- آشنایی با مفاهیم کلی برنامه‌نویسی مانند متغیرها، حلقه‌های تکرار، توابع و غیره
- حداقل یک سال تجربه‌ی کاری در زمینه‌ی امنیت سایبری

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

Day 1:

1.1 Introduction to Road Map

1.2 Sample of Disassemble Hello World (Windows/Linux/Mac OS)

1.3 Fundamental Data Types

1.4 Radices (Decimal, Binary, Hexadecimal)

1.5 Negative Numbers

1.6 Architecture CISC vs RISC

1.7 Endianness

1.8 Registers

1.9 Caller/Callee

1.10 Stack Concept

1.11 Calling Conventions (cdecl/stdcall/fastcall)

1.12 General Stack Frame Operations

1.13 Addressing Forms

1.14 x86/x86_64 Instructions that Introduced over the Class

- 1.14.1 Nop
- 1.14.2 Push/Pop
- 1.14.3 Call/RET
- 1.14.4 MOV
- 1.14.5 LEA
- 1.14.6 ADD/SUB
- 1.14.7 MOVZX/MOVSX

Day 2:

2.1 Deep Examples about Day1 (More than 20 Examples)

آکادمی راوین

2.2 Control Flow

2.3 x86/x86_64 Instructions

2.3.1 JMP/JCC

2.3.2 CMP/TEST

2.3.3 AND/OR/XOR/NOT

2.3.4 INC/DEC

2.3.5 SHR/SHL/SAR/SAL

2.3.6 IMUL

2.3.7 DIV/IDIV

2.3.8 REP STOS/REP NOVES

2.3.9 LEAVE

2.4 Journey to the Center of memcpy and memmove

2.5 Introduction to Exploit Windows Kernel by Memory Overlay

2.6 Homework 1

Day 3:

3.1 Intel vs AT&T Syntax

3.2 GCC Basic Usage

3.3 Objdump

3.4 hexdump & xdd

3.5 GDB

3.6 Debug Examples with GDB

3.7 Inline Assembly

3.8 _emit and .byte

3.9 Interpreting the Instruction

3.10 x86/x86_64 Instructions

3.10.1 SAR

آکادمی راوین

3.11 Opcodes

3.12 Buffer Overflow Examples

3.13 Introduction to Obfuscation

3.14 Introduction to Packer

3.15 Effect of Compiler

Day 4: [Challenge day]

4.1 Q&A

4.2 Lab

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

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