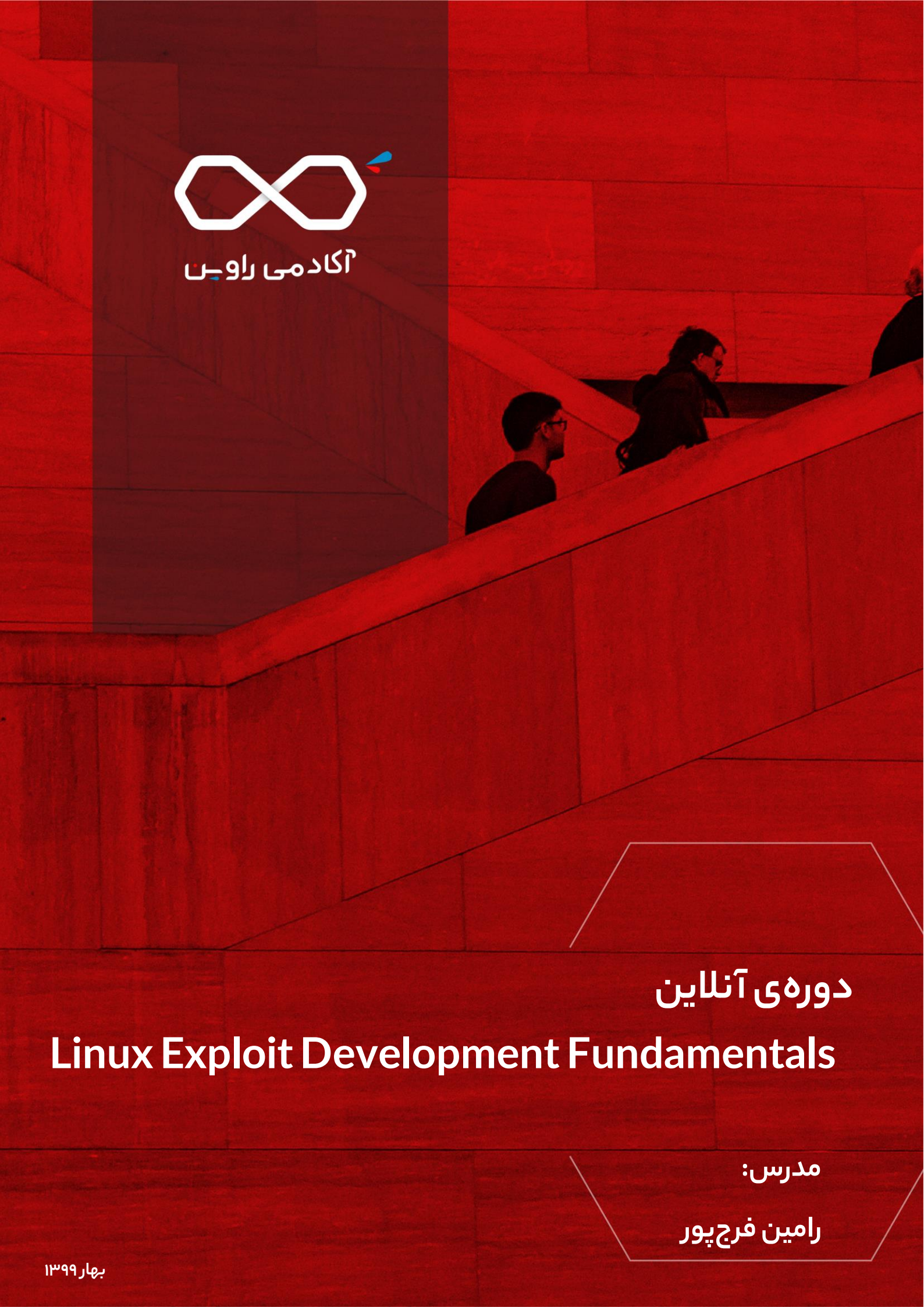

آکادمی راوین

دوره‌ی آنلاین

Linux Exploit Development Fundamentals

مدرس:

رامین فرج‌پور

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؟ از مهم‌ترین دلایل آن می‌توان به شناسایی آسیب‌پذیری‌های موجود قبل از افراد سودجو و خراب‌کار و همچنین دریافت جوایز تعیین شده توسط شرکت‌های ارایه دهنده‌ی این سامانه‌ها اشاره کرد. شما با گذراندن این دوره‌ی آموزشی، مبانی کشف آسیب‌پذیری در سیستم‌عامل لینوکس و توسعه‌ی Exploitبرای آن را فرا خواهید گرفت. از مهم‌ترین موضوعاتی که در این دوره تدریس می‌شود می‌توان به معماری سیستم‌عامل لینوکس، مبانی روش‌های Fuzzing، مهندسی معکوس، توسعه‌ی Shellcode و دور زدن راهکارهای محافظتی موجود در سیستم‌عامل لینوکس اشاره کرد.

مدت زمان دوره

مدت زمان این دوره ۲۱ ساعت است که به صورت کلاس‌های ۳ ساعته و در طی ۷ جلسه تدریس خواهد شد. جلسات این دوره در روزهای زوج و از ساعت ۱۸ تا ۲۱ برگزار می‌شود. شروع دوره از روز شنبه مورخ ۱۵ شهریور سال ۹۹ خواهد بود.

این دوره به چه افرادی توصیه می‌شود؟

- کارشناسان ارشد ارزیابی امنیت/تست نفوذ/تیم قرمز
- کارشناسان فعال در زمینه‌ی Bug Bounty
- برنامه‌نویسان علاقه‌مند به توسعه‌ی امن
- تحلیل‌گران و محققین امنیت سایبری
- کارشناسان مهندسی معکوس

برای شرکت در این دوره چه دانش‌هایی باید داشته باشم؟

- آشنایی با مفاهیم سیستم‌عامل Linux
- آشنایی با زبان برنامه‌نویسی Python در سطح متوسط
- آشنایی با زبان برنامه‌نویسی C یا C++ در سطح متوسط

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

آکادمی راوین

سرفصل‌های این دوره

Chapter 1: Intro

1.1 Linux Operation System Architecture

1.2 Why C/C++ Language is Important?

1.3 Who to integrate high language with C Lang?

1.4 What is System Call in Linux?

1.5 Explanation Type Vulnerability in C Lang

- 1.5.1 NULL Pointer Dereference
- 1.5.2 Use After Free
- 1.5.3 Double Free
- 1.5.4 Race Condition
- 1.5.5 Out Of Bound Read / Out Of Bound Write
- 1.5.6 Buffer Overflow
- 1.5.7 Heap Overflow
- 1.5.8 Memory Leak
- 1.5.9 Uninitialized Memory Access

Chapter 2: Fuzzing

2.1 What is Fuzzing?

2.2 Static Fuzzing

- 2.2.1 Familiar Unsafe C API in Linux
- 2.2.2 Clang Static Analyzer
- 2.2.3 Valgrind – Memcheck
- 2.2.4 Technique Code Review for Find Vulnerability

2.3 Dynamic Fuzzing

- 2.3.1 What is Address Sanitizer in the C Lang?
- 2.3.2 AFL Fuzzer

آکادمی راوین

7.3 Buffer Overflow Exploit – x64

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.

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