



آکادمی راون



دوره‌ی آنلاین

Linux Exploit Development Fundamentals

مدرس:

رامین فرچپور

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 کلاه سفید 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 Exploit برای 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 می شود؟

- کارشناسان ارشد ارزیابی امنیت / تست نفوذ / تیم قرمز
- کارشناسان فعال در زمینه ی Bug Bounty
- برنامه نویسان علاقه مند به توسعه ی امن
- تحلیل گران و محققین امنیت سایبری
- کارشناسان مهندسی معکوس

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

- آشنایی با مفاهیم سیستم عامل Linux
- آشنایی با زبان برنامه نویسی Python در سطح متوسط
- آشنایی با زبان برنامه نویسی C یا C++ در سطح متوسط

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 راورین

2.3.3 LibFuzzer

2.3.4 Domato

2.3.5 Honggfuzz

Chapter 3: Security Protection

3.1 PIE

3.2 PIC

3.3 NX Bit (MS:DEP)

3.4 RELRO

3.5 Canaries

3.6 ASLR

Chapter 4: Assembly Language in Linux – x64

4.1 Assembly Language Code Structure

4.2 Data Types

4.3 Develop Hello World Program

4.4 Stack in Assembly

4.5 Data Manipulation

4.6 Data Swapping

4.7 Load Effective Address

4.8 Arithmetic Operations

4.9 Loops

4.10 Controlling the Flow

4.11 Operations

Chapter 5: Reverse Engineering – x64

5.1 Introduction to the ELF Format

5.1.1 ELF Header



آکادمی رابین

5.1.2 Section Header

5.1.3 Program Header

5.1.4 ELF Injection

5.2 Install Python Exploit Assistance (PEDA)

5.3 Customizing Disassembly with Capstone

5.4 GDB Debugger

5.5 PWNGDB (SCWUAPTX)

5.6 PWNTTOOLS

5.7 GEF

5.8 GDB Commands

5.9 Reverse Hello World Program

5.10 Reverse Function Call

5.11 Crack Password with GDB

Chapter 6: Writing Shellcode – x64

6.1 What is Shellcode?

6.2 Bad Characters

6.3 The Relative Address Technique

6.4 The JMP–CALL Technique

6.5 The Stack Technique

6.6 The execve Syscall

6.7 TCP Bind Shell

6.8 Reverse TCP Shell

6.9 Generating Shellcode Using Metasploit

Chapter 7: Buffer Overflow Attacks x64

7.1 Stack Overflow on Linux

7.2 Inject Shellcode



7.3 Buffer Overflow Exploit – x64

7.3.1 What is ROP?

7.3.1.1 ROP Bypass Technique

7.3.2 Bypassing on NX Using *ret2libc* Technique

7.3.3 Bypassing ASLR Using *ret2libc* Techniques

7.3.4 Chain-*ret2libc* Technique

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



آکادمی راوین

 <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 