سر فصل های دوره

مهندسی معکوس نرم افزار مقدماتی

پل ورود شما به دنیای مهندسی معکوس نرم افزار

نگارش 1.0

برگزار کننده دوره های آموزش برنامه نویسی و امنیت نرم افزار | DORA

فصل اول : مقدمه

در این بخش به معرفی مهندسی معکوس نرم افزار می پردازیم.

- تعریف مهندسی معکوس نرم افزار
- کاربرد های مهندسی معکوس نرم افزار
- شاخه های مهندسی معکوس نرم افزار
- بررسی مشاغل و شرایط کاری مهندسی معکوس نرم افزار

بخش دوم : معماری کامپیوتر و مباحث پایه

در این بخش به معرفی ساختار کامپیوتر، سیستم عامل، فایل های باینری و مفاهیم پایه می پردازیم.

- آشنایی با Data Unit ها
- آشنایی با Data Type ها
- آشنایی با Unicode و ASCII
- آشنایی با مفهوم LSB و MSB
- آشنایی با اعداد Signed و Unsigned
- آشنایی با سیستم اعداد (مبناها) Decimal , Hex , Binary
- آموزش تبدیل سیستم اعداد (مبناها) به یکدیگر
- آشنایی با معماری سیستم عامل x86 , x64 و تفاوت آن ها
- آشنایی با Loader و فرایند لود شدن فایل ها و کتابخانه ها در سیستم عامل
- آشنایی با زبان های برنامه نویسی Native , Managed , Cross-Platform
- آشنایی با مفهوم برنامه نویسی High Level و Low Level
- آشنایی با زبان های برنامه نویسی Interpreted و Compiled
- آشنایی با Compiler, Linker و فرایند تبدیل کد ها به فایل های اجرایی
- آشنایی با مفهوم Code Optimization
- تفاوت فایل های باینری x86 , x64
- تفاوت های مد های کامپایل باینری Debug و Release
- آشنایی با انواع فایل ها در سیستم عامل های ویندوز، لینوکس، مک، اندروید و iOS
- آشنایی با ساختار فایل های PE
- آشنایی با ساختار و معماری دیباگر ها، دیس اسمبلر ها و دیکامپایلر ها

بخش سوم : زبان برنامه نویسی اسمبلی

آموزش مقدماتی زبان Assembly در محیط برنامه نویسی RadASM

- معرفی تاریخچه و اکو سیستم زبان برنامه نویسی Assembly
- چرا زبان برنامه نویسی Assembly
- نصب و پیکربندی RadASM
- Registers
- Flags
- Segments and Offset
- Instructions
- Opcode and Mnemonic
- Calling Conversion
- Prologue, Epilogue and Call Sequences
- Caller and Callee
- ISA, CISC and RISC
- Stack Concept
- Addressing Modes
- Endianness

بخش چهارم : زبان برنامه نویسی C++

آموزش مقدماتی زبان C++ در محیط برنامه نویسی Microsoft Visual Studio.

این بخش دارای تمرین (Home Work) است.

- معرفی تاریخچه و اکو سیستم زبان برنامه نویسی C++
- متغیر ها در زبان C++
- آموزش دستورات شرطی
- آموزش دستورات حلقه
- آموزش کنترل خطاها
- آموزش کلاس ها و فانکشن ها
- آموزش ساخت DLL
- آموزش استفاده از DLL ها در زبان های برنامه نویسی
- آموزش برنامه نویسی سیستمی با استفاده از API

بخش پنجم : ابزار ها در مهندسی معکوس نرم افزار

در این بخش به معرفی ابزار های استاتیک و داینامیک در مهندسی معکوس نرم افزار می پردازیم.

- معرفی روش های تحلیل داینامیک و استاتیک و بررسی تفاوت آن ها
- معرفی ابزار ها و دسته بندی های دیباگر، دیس اسمبلر، دیکامپایلر و ...

بخش ششم : تحلیل فایل های باینری (داینامیک)

در این بخش با استفاده از مثال های تمرینی به مهندسی معکوس فایل های باینری به صورت Single Process, Dual Process و Mixed Mode می پردازیم.

این بخش دارای تمرین (Home Work) است.

- مفاهیم تئوری
- آموزش نرم افزار x64dbg
- آموزش نرم افزار dnSpy
- معرفی اسکریپت ها و پلاگین های کاربردی

بخش هفتم : تحلیل فایل های باینری (استاتیک)

در این بخش با استفاده از مثال های تمرینی به مهندسی معکوس فایل های باینری به روش استاتیک می پردازیم.

این بخش دارای تمرین (Home Work) است.

- مفاهیم تئوری
- آموزش نرم افزار IDA Pro
- معرفی اسکریپت ها و پلاگین های کاربردی

بخش هشتم : شناخت مکانیسم های امنیتی جهت جلوگیری از دیباگ شدن برنامه ها

در این بخش با مکانیسم های امنیتی که جهت سخت شدن روند دیباگ برنامه ها استفاده می شوند آشنا خواهید شد و با توجه به سطح دوره، روش های مقابله با مکانیسم های امنیتی را فرا می گیرید.

- How to identify security mechanisms?
- What is the Packer and Protector and how they work?
- OEP protection
- IAT emulation and redirection
- Code obfuscation
- Code virtualization
- Code integrity
- Resource protection
- Encryption and decryption
- Hardcoding and hidden strings
- Anti-debug
- Anti-Virtual machines
- Anti DLL injection
- Anti hook
- Binary sign and certificate
- Stolen byte and stolen OEP
- Software and hardware breakpoint detection

بخش نهم : کاربرد های مهندسی معکوس نرم افزار در دنیای واقعی

در این بخش به صورت کاملا عملی با فرایند مهندسی معکوس در تحلیل فایل های باینری، تحلیل بدافزار و اکسپلویت نرم افزار آشنا خواهید شد.

- سناریو اول : جمع آوری اطلاعات اولیه بخش اول
- سناریو دوم : جمع آوری اطلاعات اولیه بخش دوم
- سناریو دوم : اضافه کردن سکشن به فایل و تغییر EP برنامه به روش دستی
- سناریو سوم : پیدا کردن مکان های Code Cave و اضافه کردن / تغییر کد برنامه به روش دستی
- سناریو چهارم : معرفی و پیاده سازی تکنیک Inline Patching
- سناریو پنجم : اضافه کردن / تغییر کد برنامه با استفاده از Import Table
- سناریو ششم : اضافه کردن / تغییر کد برنامه با استفاده از DLL Hijacking
- سناریو هفتم : اضافه کردن / تغییر کد برنامه با استفاده از DLL Injection
- سناریو هشتم : بررسی Stack Frame
- سناریو نهم : بررسی Stack Frame
- سناریو دهم : معرفی و کار با سایر دیباگر ها و دیس اسمبلر ها
- سناریو یازدهم : تحلیل بدافزار با استفاده از مهندسی معکوس
- سناریو دواردهم : اکسپلویت نرم افزار با استفاده از مهندسی معکوس

بخش دهم : جلسه پرسش و پاسخ

گواهینامه دوره :

ارزیابی و امتحان دوره به صورت تئوری و عملی پس از اتمام دوره، در یک جلسه آنلاین به صورت فرد به فرد برگزار خواهد شد. در انتها دانش آموختگانی که تمرین ها، تحقیق ها و آزمون را با موفقیت پشت سر بگذارند، گواهینامه dCBSRE دریافت می کنند.