به نام خدا

بررسی اجماالی برای ورود به مبحث مهندسی معکوس

مهندسی معکوس نرم افزار مقدماتی یا dCBSRE که مخفف DWORD Certified Basic Software Reverse Engineering می باشد، پل ورود به دنیای مهندسی معکوس نرم افزار است که شامل 9 بخش است که شامل موضوعات مقدماتی است و برای ورد به مباحث پیشرفته تر نیاز به زمان های بیشتر است .

1. بخش اول (2 ساعت آموزش)
   - تعریف مهندسی معکوس نرم افزار
   - کاربرد های مهندسی معکوس نرم افزار
   - شاخه های مهندسی معکوس نرم افزار
   - شرایط کاری مهندسی معکوس نرم افزار

2. بخش دوم (80 ساعت آموزش)

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

- . • آشنایی با Unit Data ها
- آشنایی با Type Data ها
- آشنایی با Unicodeو ASCI
- ا 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 x64 , x86 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 Cross-Platform , Managed
- آشنایی با مفهوم برنامه نویسی Level High و Low Level
- آشنایی با زبان های برنامه نویسی Interpreted و Compiled
- آشنایی با Linker ,Compiler و فرایند تبدیل کد ها به فایل های اجرایی
- آشنایی با مفهوم Optimization Code
- تفاوت فایل های باینری x64 , x86
- 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

3. بخش سوم (40 ساعت آموزش)

زبان برنامه نویسی اسمبلی آموزش مقدماتیزبان 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
  - Segments and Offset
  - Instructions
  - Opcode and Mnemonic
  - Prologue, Epilogue and Call Sequences
  - Caller and Callee
  - ISA, CISC and RISC
  - Stack Concept
  - Addressing Modes
  - Endianness

4. بخش چهارم (40 ساعت آموزش)

آموزش مقدماتی زبان C++ در محیط برنامه نویسی Visual
- 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

5. بخش پنجم : ابزار ها در مهندسی معکوس نرم افزار (10 ساعت آموزش)

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

6. بخش ششم تحلیل فایل های باینری به روش داینامیک (10 ساعت آموزش)

- مفاهیم تئوری

- آموزش نرم افزار dbg64x
- آموزش نرم افزار dnSpy
- معرفی اسکریپت ها و پالگین های کاربردی

7. بخش هفتم : تحلیل فایل های باینری استاتیک (10 ساعت آموزش)

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

8. بخش هشتم : شناخت مکانیسم های امنیتی جهت جلوگیری از دیباگ شدن برنامه ها (40 ساعت آموزش)

- How to identify security mechanisms?
- What is the Packer and Protector
- 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

9. بخش نهم : کاربرد های مهندسی معکوس نرم افزار (80 ساعت آموزش)

- سناریو اول : جمع آوری اطالعات اولیه بخش اول
- سناریو دوم : جمع آوری اطالعات اولیه بخش دوم
- سناریو دوم : اضافه کردن سکشن به فایل و تغییر EP برنامه به روش دستی
- سناریو سوم : پیدا کردن مکان هایCave Code و اضافه کردن/ تغییر کد برنامه به روش دستی
- سناریو چهارم : معرفی و پیاده سازی تکنیک Patching Inline
- سناریو پنجم : اضافه کردن / تغییر کد برنامه با استفاده از Table Import
- سناریو ششم : اضافه کردن/ تغییر کد برنامه با استفاده از Hijacking DLL
- سناریو هفتم : اضافه کردن / تغییر کد برنامه با استفاده از Injection DLL
- سناریو هشتم: بررسی Frame Stack
- سناریو نهم: بررسی Frame Stack
- 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