مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

دوره متوسط تحلیل بدافزار

تحلیل بدافزار

مدت(ساعت): ۴۰

اهداف دوره :

با یادگیری روش های تحلیل و مفاهیم کاربردی حوزه تحلیل در دوره مقدماتی، در این دوره با یادگیری تکنیک های خاص بدافزار، مهارت بیشتری در شناسایی رفتار بدافزار و خنثی کردن اثرات تخریبی در سیستم کسب می شود، همچنین کارآموز با تحلیل فایلهای ۶۴ بیتی و سرویس ها نیز آشنا می شود.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

پیش نیاز دوره :

- پیش‌نیاز این دوره گذراندن دوره مقدماتی تحلیل بدافزار می‌باشد.

محتوای دوره :

۱. معماری X86
۱.۱. دستورالعمل(Instruction)
۱.۲. عملگر(Opcodes) و Endianness
۱.۳. حافظه اصلی(Main Memory)
۱.۴. عملوند(Operand)
۱.۵. رجیستر
۱.۶. پشته (Stack)
۱.۷. بررسی شرطی
۱.۸. شاخه(Branch)
۱.۹. معرفی چند دستور دستورات اسمبلی
۱.۱۰. متد Main() در زبان C
۱.۱۱. اسمبلی دات نت (IL)
۱. تحلیل کد بدافزار
۱.۱. تحلیل کد بصورت ایستا
۱.۱.۱. تحلیل بدافزار در یک Disassembler نظیر IDA
۱.۱.۲. دیکامپایل کردن کد
۱.۱.۲.۱ Reflector
۱.۱.۲.۲ VBDecompiler

Course Outline :

۱.۱.۲.۳ AutoIT Decompiler
۱.۱.۲.۴ Python Decompiler
۱.۱.۲.۵ Delphi Decompiler
۱.۲. تحلیل کد بصورت پویا(تحلیل رفتاری بدافزار در حال اجرا)
۱.۲.۱. تحلیل فایل های exe در دیباگر OllyDBG
۱.۲.۲. دیباگ کردن کد در IDA
۱.۲.۳. بررسی روند تحلیل DLL
۱.۲.۴. تحلیل Exportها
۲. تکنیک‌های بدافزاری
۲.۱. تکنیک های مخفی کردن
۲.۲. تکنیک های بقا
۲.۲.۱. از طریق رجیستری
۲.۲.۲. از طریق سیستم فایل
۲.۳. تکنیک های تخریب
۲.۴. تکنیک های هوک کردن سطح کاربر
۲.۴.۱. هوک inline
۲.۴.۲. هوک IAT
۲.۴.۳ ابزارهای مفید جهت شناسایی تکنیک

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس: ۸۸۰۶۵۲۲۲

محتوای دوره :	Course Outline :
۲.۵. تکنیک های انتشار بدافزارها	۳.۴. پک شدن بدافزار
۲.۵.۱. انتشار از طریق فلش	۴. تحلیل عملکرد شبکه
۲.۵.۲. انتشار از طریق شبکه	۴.۱. مفاهیم اولیه شبکه
۲.۶. تکنیک های تزریق	۴.۲. آشنایی با پروتکل‌های مشهور
۲.۶.۱. تزریق DLL	۴.۲.۱. پروتکل HTTP
۲.۶.۲. تزریق کد بصورت مستقیم	۴.۲.۲. پروتکل SSL
۲.۶.۳. جایگزینی پردازه	۴.۲.۳. پروتکل SMB
۲.۶.۴. تزریق هوک	۴.۲.۴. پروتکل SOCKS
۲.۶.۵. ابزارهای مفید جهت شناسایی تکنیک	۴.۲.۵. پروتکل RDP
۲.۶.۵.۱ PC Hunter	۴.۳. Wireshark
۲.۶.۵.۲ Gmer	۴.۴. NetCat
۲.۷. تکنیک های انتشار بدافزارها	۴.۵. Snort
۳. روش های ضدتحلیل(Anti Reverse)	۴.۶. Suricata
۳.۱. AntiDebug	۵. تحلیل سرویس ها
۳.۲. Anti VM	۶. تحلیل فایل های ۶۴ بیتی
۳.۳. Anti Disassembly	

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲