بسمه تعالی

جزئیات برگزاری کارگاه‌های آموزشی هشتمین کنفرانس بین‌المللی انجمن رمز ایران

http://iscisc2011.um.ac.ir

۱. **کد کارگاه : W11**

۲. **عنوان: تحلیل بدافزارها**

۳. **چکیده:** امروزه انواع مختلفی از بدافزارها از قبیل ویروس‌ها، کرم‌های اینترنتی، اسب‌های تروی، بات‌نت‌ها، روت‌کیت‌ها و جاسوس‌افزارها وجود دارد که با اهداف گوناگون شامل تخریب، جمع‌آوری اطلاعات، جاسوسی صنعتی و دسترسی غیرمجاز به منابع یک سیستم کامپیوتری تولید می‌شوند. بنابراین تحلیل بدافزارها از اهمیت زیادی برای افراد و سازمان‌های مختلف برخوردار است. عمدتا از دو رویکرد تحلیل ایستا و تحلیل پویا برای این منظور استفاده می‌شود. در تحلیل ایستا، هدف بررسی رفتار کلی یک بدافزار بدون نیاز به اجرای آن است. در صورتی که در تحلیل پویا، بدافزار در یک محیط شبه‌واقعی اجرا شده و نحوه تعامل آن با سیستم میزبان مورد بررسی قرار می‌گیرد. بات‌نت‌ها به عنوان یکی از خطرناک‌ترین انواع بدافزارها شناخته می‌شوند. چرخه حیات هر بات‌نت شامل سه مرحله انتشار، فرمان و کنترل، و حمله است. در مرحله انتشار، مهاجم با آلوده‌سازی تعداد زیادی از میزبان‌های آسیب‌پذیر، آن میزبان‌ها را به بات تبدیل کرده و شبکه‌ای از بات‌ها را برای خود ایجاد می‌کند. در مرحله فرمان و کنترل، با ارسال فرامین بات‌ها را از راه دور هدایت کرده و در مرحله حمله، انواع مختلفی از حملات را به صورت هماهنگ و با قدرت تخریبی بسیار بالا بر روی قربانی سازماندهی می‌کند.

۴. **ارائه‌دهندگان:**

نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	عنوان شغلی	وابستگی	رایانامه
مهدی آبادی	دکتری	مهندسی کامپیوتر	عضو هیات علمی	دانشگاه تربیت مدرس	mahdi.abadi@gmail.com
سینا رستگار	کارشناسی	مهندسی کامپیوتر		دانشگاه فردوسی مشهد	
موسی یحیی‌زاده	کارشناسی ارشد	مهندسی کامپیوتر	دانشجو	دانشگاه تربیت مدرس	
شهاب‌الدین نمازی‌خواه	کاردانی	مهندسی کامپیوتر	عضو تیم عملیات	آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد	

۵. **زندگی‌نامه ارائه‌دهندگان:** آقای آبادی عضو هیات علمی دانشگاه تربیت مدرس و دانش‌آموخته دکتری مهندس کامپیوتر گرایش نرم‌افزار از دانشگاه تربیت مدرس می‌باشند. زمینه تخصصی ایشان امنیت اطلاعات است و پروژه‌های مختلفی را تاکنون در این زمینه انجام داده‌اند. دکتر آبادی مدیر عملیات آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد نیز می‌باشند.

آقای یحیی‌زاده دانشجوی کارشناسی‌ارشد مهندسی کامپیوتر دانشگاه تربیت مدرس می‌باشند که فعالیت‌هایی در حوزه افتا انجام می‌دهند.

آقای نمازی‌خواه نیز از اعضای تیم عملیات آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد می‌باشند.

۶. **مخاطبان کارگاه:**
   - کارشناسان و مدیران شبکه و امنیت اطلاعات

۷. **سرفصل:**
- معرفی انواع بدافزارها
  - ویروس‌ها، کرم‌های اینترنتی، اسب‌های تروی، بات‌نت‌ها، روت‌کیت‌ها، جاسوس‌افزارها
- بات‌نت‌ها
  - چرخه حیات بات‌نت‌ها
  - مکانیزم فرمان و کنترل
  - انواع بات‌نت‌ها (بات‌نت‌های متمرکز، غیرمتمرکز و ترکیبی)
  - مثال‌هایی از بات‌نت‌ها (AgoBot، SDBot، PhatBot، Storm و Waledac)
  - بات‌نت‌های نسل آینده
  - نمایش عملی بات‌های RBot و HTTPBot
- تحلیل پویای بدافزارها
  - مراحل ایجاد آزمایشگاه تحلیل بدافزارها
  - تحلیل پویا در محیط ویندوز (نظارت بر پردازه‌ها، فایل‌ها، اتصالات شبکه، رجیستری و غیره)
  - تحلیل پویا در محیط لینوکس (نظارت بر پردازه‌ها، فایل‌ها، اتصالات شبکه و غیره)
- مهندسی معکوس و تحلیل ایستای بدافزارها
  - اصول مهندسی معکوس
  - تکنیک‌های مبهم‌سازی و رفع ابهام
  - روبرداری از حافظه
  - قالب فایل‌های PE
  - مهندسی معکوس یک بدافزار
- تحلیل کرم اینترنتی استاکس‌نت

۸. **زمان برگزاری:** **تمام‌روز – سه‌شنبه ۲۲ شهریور ۱۳۹۰ – ساعت ۸ الی ۱۸**

۹. **پیش‌نیاز:** آشنایی با زبان اسمبلی و اصول سیستم‌های عامل

برای اطلاع از نحوه ثبت‌نام در این کارگاه به وب‌گاه http://iscisc2011.um.ac.ir مراجعه نمائید.