

جزئیات برگزاری کارگاه‌های آموزشی هشتمین کنفرانس بین‌المللی انجمن رمز ایران  
<http://iscisc2011.um.ac.ir>

۱. کد کارگاه : W03

۲. عنوان: شناسایی تهدیدات جدید در فضای سایبری با استفاده از Honeypot

۳. چکیده: هدف این کارگاه آموزشی، آشنا کردن مخاطبین با تهدیدات اصلی موجود در فضای سایبری و استفاده از Honeypot جهت شناسایی و مقابله با این تهدیدات است. در این راستا ابتدا اصلی ترین تهدیدات موجود در اینترنت و همچنین تهدیدات در حال ظهور را معرفی کرده و سپس به بررسی دقیق پدیده Botnet که یکی از مهمترین تهدیدات سایبری است می پردازیم. بعد از مرور روش های موجود برای کشف تهدیدات و حملات اینترنتی و همچنین ذکر ضعف آنها، تکنولوژی امنیتی Honeypot را به طور کامل معرفی و بررسی خواهیم کرد. تکنولوژی Honeypot یکی از اصلی ترین ابزارهای محققان و سازمان های امنیتی جهت شناسایی تهدیدات جدید سایبری بوده که در این کارگاه به طور کامل بررسی و نحوه راه اندازی آن آموزش داده می شود. در انتها، یک سناریوی واقعی از حملات کشف شده و داده های جمع آوری شده توسط Honeypot را به طور عملی آنالیز می کنیم.

۴. ارائه دهنده:

نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	عنوان شغلی	وابستگی	رایانامه
عادل کریمی	کارشناسی (دانشجوی کارشناسی ارشد)	مهندسی فناوری اطلاعات - گرایش شبکه های کامپیوتری	کارشناس امنیت شبکه	دانشگاه صنعتی امیرکبیر، عضو رسمی Honeynet Project	adel.net@gmail.com

۵. زندگی نامه ارائه دهنده: آقای کریمی دانشجوی مقطع کارشناسی ارشد مهندسی فناوری اطلاعات گرایش شبکه های کامپیوتری می باشد و همچنین مدارک CCNP و LPIC را نیز اخذ کرده اند. ایشان تاکنون در رابطه با موضوع کارگاه، سمینار و مقاله هایی را ارائه و منتشر نموده اند.

۶. مخاطبان کارگاه:

○ کارشناسان امنیت اطلاعات، مدیران شبکه، مدیران فناوری اطلاعات و تمامی متخصصان و علاقه مندان امنیت اطلاعات

۷. سرفصل:

- معرفی تهدیدات موجود در فضای سایبری
  - حملات Drive-by download، بات نت ها (Botnets)، بدافزار ها و ...
- بررسی تهدیدهای سایبری نو ظهور و گرایشات جدید

- روش‌های شناسایی تهدیدات و ضعف آنها
  - سیستم‌های تشخیص نفوذ، NSM، و ...
  - روش‌های کشف و ردیابی بات‌نت
- هانی پات (Honeypot)
  - تعریف هانی پات و کاربردهای آن
  - معرفی و بررسی کامل انواع هانی پات
  - پیاده‌سازی Honeynet مجازی
- آنالیز سناریویی از داده‌های به دست آمده از هانی پات

۸. زمان برگزاری: نیم‌روز - سه‌شنبه ۲۲ شهریور ۱۳۹۰ - ساعت ۸ الی ۱۲

۹. پیش‌نیاز: ندارد

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