بسمه تعالی

جزئیات برگزاری کارگاه‌های آموزشی هشتمین کنفرانس بین‌المللی انجمن رمز ایران

http://iscisc2011.um.ac.ir

۱. **کد کارگاه : W08**

۲. **عنوان: شبکه‌های بات: تاریخچه، تهدیدات، انواع، راه‌کارها**

۳. **چکیده:** سیر پیشرفت فناوری اطلاعات و ارتباطات موجب افزایش بهره‌وری و پیدایش انواع جدیدی از خدمات و در کنار آن افزایش پتانسیل سوءاستفاده از این بستر شده است. یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری شبکه بات می‌باشد. شبکه بات شبکه‌ای از کامپیوترهای آلوده و متصل به اینترنت است که برای حملات توزیع شده اینترنتی مانند ممانعت از سرویس، مورد استفاده قرار می‌گیرد. بدست آوردن ظرفیت منابع، حس کنجکاوی، کسب پول و جمع‌آوری اطلاعات، انگیزه‌هایی برای ایجاد شبکه‌های بات است. به عنوان مثال در سال ۲۰۰۹ سایت‌های مخصوص شبکه‌های اجتماعی همچون Livejournal، Twitter و Facebook مورد تهاجم حملات ممانعت از سرویس توزیع شده قرار گرفتند. یا حمله مشابه که در سال ۲۰۱۰ بر روی سازمان‌های بزرگی همچون PayPal.com،Visa.com و Mastercard.com صورت گرفت و باعث شد تا وب‌سایت‌های مخصوص این سازمان‌ها از ارائه سرویس باز بمانند. تعداد شبکه‌های بات روزانه در حال افزایش است. از طرف دیگر سازندگان چنین شبکه‌هایی از فناوری‌ها و تکنیک‌های جدید استفاده می‌کنند. باتوجه به اهمیت موضوع شبکه بات و حملات صورت گرفته توسط این شبکه‌ها، امروزه بیش از پیش تلاش برای کشف و مقابله با این شبکه‌ها صورت پذیرفته است. هدف از این کارگاه معرفی مفاهیم مرتبط با شبکه‌های بات و انواع مختلف آن‌ها، نحوه ایجاد و انتشار یک شبکه بات، مروری بر تهدیدات به وجود آمده توسط این شبکه‌ها و بررسی روش‌های کشف و مقابله با آن‌ها است.

۴. **ارائه‌دهندگان:**

نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	عنوان شغلی	وابستگی	رایانامه
محمدهاشم حقیقت	کارشناسی ارشد	مهندسی کامپیوتر	مدیر گروه پژوهش	مرکز آپای دانشگاه صنعتی شریف	haghighat@cert.sharif.edu
مریم حیدری	کارشناسی ارشد	مهندسی فناوری اطلاعات	کارشناس فنی	مرکز آپای دانشگاه صنعتی شریف	heidari@cert.sharif.edu

۵. **زندگی‌نامه ارائه‌دهندگان:** آقای حقیقت دانش‌آموخته مهندسی کامپیوتر گرایش نرم‌افزار دانشگاه صنعتی شریف هستند که موضوع پایان‌نامه ایشان نیز Formal Analysis of Security Properties of Homomorphic-Cryptography-Based E-voting Protocols Model Checking Approach بوده است. ایشان هم‌اکنون با مرکز آپای دانشگاه صنعتی شریف همکاری دارند.

خانم حیدری نیز در رشته مهندسی فناوری اطلاعات تحصیل کرده‌اند و با مدرک کارشناسی‌ارشد از دانشگاه صنعتی شریف دانش‌آموخته شده‌اند. زمینه‌های کاری ایشان امنیت شبکه‌های کامپیوتری و تحلیل ترافیک شبکه‌های کامپیوتری می‌باشد.

۶. مخاطبان کارگاه:

- کارشناسان شبکه و امنیت اطلاعات

۷. سرفصل:

۱- مقدمه‌ای بر شبکه‌های بات

۱-۱- تعریف شبکه بات

۱-۲- تهدیدات یک شبکه بات

۱-۳- گستردگی شبکه‌های بات

۱-۴- خلاصه و نتیجه‌گیری

۲- انواع شبکه‌های بات

۲-۱- مبتنی بر پروتکل IRC

۲-۲- مبتنی بر پروتکل HTTP

۲-۳- مبتنی بر شبکه‌های نقطه به نقطه

۲-۴- خلاصه و نتیجه‌گیری

۳- انواع روش‌های کشف و مقابله

۳-۱- تکنیک‌های کشف مبتنی بر امضا

۳-۲- تکنیک‌های کشف مبتنی بر رفتارهای غیرعادی

۳-۳- تکنیک‌های کشف مبتنی بر درخواست‌های DNS

۳-۴- تکنیک‌های کشف مبتنی بر تحلیل بدافزار

۳-۵- تکنیک‌های کشف مبتنی بر شبکه‌های بات نقطه به نقطه

۳-۶- خلاصه و نتیجه‌گیری

۸. زمان برگزاری: نیم‌روز – سه‌شنبه ۲۲ شهریور ۱۳۹۰ – ساعت ۱۴ الی ۱۸

۹. پیش‌نیاز: -

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