به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

مروری بر همبسته‌سازی هشدارهای امنیتی و بررسی این قابلیت‌ها در سامانه OSSIM

Correlation of Security Alerts and Evaluate the Capabilities of OSSIM

مهدیه صفرزاده

زمان: شنبه ۱۳ اردیبهشت ماه ۱۳۹۳ ساعت ۳ بعد از ظهر

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن ۴۰۴

در این ارائه یک رویکرد ترکیبی به مسئله همبسته‌سازی هشدار داریم. و این راه‌حل را با در نظر گرفتن تحقیقات آکادمیک و ابزارهای فنی توسعه داده شده در این زمینه مورد بررسی قرار می‌دهیم. یکی از ابزارهایی که در این زمینه توسعه داده شده است OSSIM ابزاری برای مدیریت هشدارهای اطلاعات امنیتی می‌باشد. در ادامه به معرفی این ابزار پرداخته و در مقایسه‌ای بین عملکرد این ابزار و فرآیند همبسته‌سازی هشدار در دنیای آکادمیک، فرآیند همبسته-سازی هشدار OSSIM را تشریح می‌کنیم. تا انتهای این ارائه راجع به موارد زیر صحبت می‌شود:

- معرفی OSSIM و بیان قابلیت‌های آن
- سپس مروری بر فرآیند همبسته‌سازی هشدار و کارهای صورت گرفته در زمینه آکادمیک
- تشریح فرآیند همبسته‌سازی هشدار در OSSIM در مقایسه‌ای بین تحقیقات صورت گرفته در زمینه آکادمیک و قابلیت های همبسته‌سازی هشدار در ابزار OSSIM
- اجرای یک نمونه همبسته‌سازی هشدار در OSSIM
- نتیجه‌گیری
- بیان نقاط ضعف و قوت OSSIM و کارهای آینده

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.

مشخصات سخنران:

مهدیه صفرزاده

m.safarzadeh_cn@yahoo.com

سوابق تحصیلی:

- کارشناسی علوم کامپیوتر از دانشگاه تبریز
- کارشناسی ارشد از دانشگاه صنعتی مالک اشتر (در حال تحصیل)

سوابق شغلی:

- مسول شبکه شرکت ویستابست
- پیاده‌سازی کلاس آموزش مجازی در موسسه ویستا
- پیاده‌سازی شبکه شهرداری منطقه ۱۵

مقالات:

- ارائه روشی برای ارزیابی نرخ مثبت نادرست در سیستم‌های جلوگیری از نفوذ، کنفرانس سیتادیم، اسفند ۹۲، مجموعه مقالات کنفرانس