کارگاه آموزشی

تحلیل امنیتی ترافیک شبکه

دکتر علی فانیان - مهندس سیدعلی سنائی

مرکز تخصصی آپا دانشگاه صنعتی اصفهان

چکیده: هدف از این کارگاه، آموزش نحوه تحلیل امنیتی ترافیک شبکه با استفاده از ابزارهایی مانند Wireshark است. در این کارگاه، ابتدا کاربران با مفاهیم کلی تشخیص نفوذ، وظایف تحلیل‌گر امنیتی شبکه و نحوه‌ی جمع‌آوری ترافیک مورد نظر آشنا خواهند شد. در ادامه، پس از آموزش نحوه کار با ابزار Wireshark، تکنیک‌ها و اصول تحلیل ترافیک توسط ابزار فوق ارائه خواهد شد.

سرفصل کارگاه:

- معرفی ابزارها و روش‌های جمع‌آوری ترافیک
  - بررسی روش‌های مختلف شنود ترافیک
  - معرفی ابزارهای تحلیل ترافیک
- آشنایی با ابزار تحلیل ترافیک Wireshark
  - معرفی بخش‌های مختلف نرم‌افزار
  - معرفی نحوه تعریف انواع فیلترها
  - معرفی نحوه انتخاب یک ترافیک خاص
- اصول تحلیل امنیتی ترافیک شبکه
  - آشنایی با مفاهیم پایه‌ی مدل مرجع TCP/IP
  - تاثیر تجهیزات شبکه بر نحوه‌ی تحلیل ترافیک
  - بررسی الگوهای رفتاری در پروتکل‌های لایه‌های مختلف TCP/IP
    - تحلیل الگوهای عادی / ناهنجار ترافیک مرتبط با پروتکل‌های لایه‌ی لینک داده
    - تحلیل الگوهای عادی / ناهنجار ترافیک مرتبط با پروتکل‌های لایه‌ی شبکه
    - تحلیل الگوهای عادی / ناهنجار ترافیک مرتبط با پروتکل‌های لایه‌ی انتقال
    - تحلیل الگوهای عادی / ناهنجار ترافیک مرتبط با پروتکل‌های متداول لایه‌ی کاربرد (http, ftp , . . .)

مدت زمان کارگاه: ۴ ساعت