به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

معرفی سامانه بومی تله عسل

Introduction of a Customized HoneyPot System

مهدی توکلی

زمان: شنبه ۱۹ اردیبهشت ماه ۱۳۹۴ ساعت ۹:۱۵

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

در سال‌های اخیر شاهد تجهیز سیستم‌های‌عامل مدرن به ابزارهای قدرتمند پایش و نیز کنترل پردازه‌ها و منابع سیستم بوده‌ایم. از سویی در بسیاری از کاربردهای امنیتی بنیان سامانه‌ها و ابزارهای مرتبط بر همین دو رویکرد نهاده می‌شود. برای نمونه در سامانه‌های تله‌عسل که با هدف شناسایی آسیب‌پذیری‌ها و چگونگی عمل‌کرد نفوذگر در بهره‌برداری این آسیب‌پذیری‌ها راه‌اندازی می‌گردد، پایه‌ی مهم و اصلی پایش رفتار و تعاملات ماشین قربانی خواهد بود. از سویی در هنگام راه‌اندازی سامانه بایستی نوع و سطح دسترسی نفوذگربه منابع، در عین پیشگیری از تخریب سامانه امکان تکمیل فرآیند نفوذ از سوی وی را فراهم سازد.

در این ارائه به معرفی یک سامانه‌ی تله‌عسل تولید شده در مرکز آپا شریف می‌پردازیم. اجزای پایه‌ای این سامانه از ویژگی‌های موجود در سیستم‌عامل لینوکس تشکیل می‌گردد. به عنوان بخشی از این ابزارها می‌توان به مجموعه‌ی Audit در سیستم‌عامل لینوکس اشاره نمود. این زیر سامانه هسته‌ی سیستم‌عامل را برای جمع‌آوری اطلاعات حسابرسی پردازه‌ها و منابع سیستم مجهز می‌سازد. ویژگی دیگر، گروه‌های کنترلی تعبیه‌شده در لینوکس است که امکان کنترل دسترسی نفوذگر به منابع گوناگون سیستم‌عامل را فراهم می‌سازد

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.