کارگاه آموزشی

# تشریح چگونگی تولید ابزار بهره‌برداری(Exploit) از آسیب‌پذیری دستگاه‌های میکروتیک و ارائه نتایج رصد شبکه ملی اطلاعات کشور در حوزه این آسیب‌پذیری

**مهندس وحید مغیث – مهندس علیرضا مسجل – مهندس محمدمصطفی یالپانیان**

مرکز تخصصی آپا دانشگاه بوعلی سینا همدان

**چکیده:** هدف از اجرای این کارگاه توضیح و نمایش روند پیشرفت و تولید ابزار بهره‌برداری از آسیب‌پذیری دستگاه میکروتیک بوده که با استفاده از ابزارهای مختلف، بصورت زنده مراحل انجام شده در آزمایشگاه ، قدم به قدم اجرا و شرح داده می‌شود. آسیب پذیری سیستم‌عامل این دستگاه از نوع سرریز عدد صحیح می‌باشد که با استفاده از روش‌های روز مقابله با مکانیزم‌های امنیتی، امکان اخذ دسترسی از دستگاه ممکن می‌شود. در این کارگاه با استفاده از ابزارهایی مانند IdaPro، R2 و GDB به بررسی و نحوه عملکرد سیستم‌عامل RouterOS بر روی دستگاه میکروتیک پرداخته می‌شود. سپس برخی از روش‌های امنیتی اعمال شده برروی این سیستم‌عامل، مانند ASLR و NX bit توضیح داده شده و چگونگی مقابله با آن‌ها نیز مورد بررسی قرار می‌گیرد. سپس با استفاده از ابزارهای ROPGadget، Pwntools و Peda آسیب‌پذیری مورد نظر، تحلیل و مورد استفاده قرار گرفته می‌شود. در نهایت چگونگی امن‌سازی و مقابله با حملات در برابر این آسیب‌پذیری شرح داده می‌شود.

**سرفصل کارگاه:**

- بررسی روش‌های امنیتی مقابله با حملات سرریز بافر
- تحلیل روش‌های دورزدن مکانیزم‌های امنیتی
- بررسی کد ماشین سیستم‌عامل میکروتیک
- تولید اسکریپت جهت اخذ دسترسی از سیستم‌عامل برای معماری‌های MIPS، PPC، x86

**مدت زمان کارگاه:** ۴ ساعت

**زمان برگزاری:** پنج‌شنبه ۱۷ اسفند ۱۳۹۶ – ساعت ۱۸-۱۴