



## طرح Workshop یک روزه (Know Your Enemy)

### بررسی تهدیدات امنیتی در فضای سایبر و شناسایی آنها با استفاده از Honeypot

عنوان دوره	مدت دوره	آغاز دوره
Honeypot	۸ ساعت (۱ روز)	هماهنگ می گردد.

هدف این کارگاه آموزشی، آشنا کردن مخاطبان با مهمترین تهدیدات امنیتی موجود در فضای سایبر و استفاده از Honeypot جهت شناسایی و مقابله با این تهدیدات است. در این راستا ابتدا اصلی ترین تهدیدات موجود در اینترنت و همچنین تهدیدات در حال ظهور را معرفی شده و سپس به بررسی دقیق پدیده Botnet که یکی از مهمترین تهدیدات سایبری است، پرداخته خواهد شد. بعد از مرور روش های موجود برای کشف تهدیدات و حملات اینترنتی و همچنین ذکر ضعف آنها، تکنولوژی امنیتی Honeypot به طور کامل معرفی و بررسی می گردد. تکنولوژی Honeypot یکی از اصلی ترین ابزارهای محققان و سازمان های امنیتی جهت شناسایی تهدیدات جدید سایبری بوده که در این کارگاه به طور کامل بررسی و نحوه راه اندازی آن آموزش داده می شود. در انتها، یک سناریوی واقعی از حملات کشف شده و داده های جمع - آوری شده توسط Honeypot به طور عملی آنالیز خواهد شد.

مخاطبان: کارشناسان امنیت اطلاعات و شبکه، مدیران فناوری اطلاعات سازمان های دولتی، بانک ها و تمامی متخصصان و علاقه مندان امنیت اطلاعات.

#### محتوای دوره :

۱. معرفی تهدیدات موجود در فضای سایبری
  - حملات Drive-by download، بات نت ها (Botnets)، بدافزار ها و ...
۲. بررسی تهدیدهای سایبری نو ظهور و گرایشات جدید
۳. روشهای شناسایی تهدیدات و ضعف آنها
  - سیستم های تشخیص نفوذ، NSM، و ...
  - مروری بر روش های کشف و ردیابی بات نت
۴. هانی پات (Honeypot)
  - تعریف هانی پات و کاربردهای آن
  - معرفی و بررسی کامل انواع هانی پات
  - پیاده سازی Honeynet مجازی
۵. آنالیز سناریویی از داده های به دست آمده از هانی پات

#### مخاطبان دوره:

مدیران و کارشناسان فعال در حوزه فناوری اطلاعات

جهت کسب اطلاع بیشتر از سایر دوره های آموزشی به سایت ما [www.Cdigit.com](http://www.Cdigit.com) مراجعه نمایید.

#### مزایای دوره :

- ❖ اعطای دو مدرک فارسی و انگلیسی با مجوز رسمی از :
  - ✓ شورای عالی انفورماتیک
  - ✓ تاییدیه صلاحیت از شرکت ملی نفت ایران
  - ✓ سازمان مدیریت و برنامه ریزی کشور (نهاد ریاست جمهوری)
- ❖ بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه های ملی