به نام خدا

جلسه سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه


# دفاع مبتنی بر هدف متحرک: معرفی و رویکردها

# Moving Target Defense: Introduction and Approaches

**هادی جعفریان**

**زمان: یک شنبه ۵ بهمن ماه ۱۳۹۳ ساعت ۴:۱۵ عصر**

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

شناسایی سامانه هدف، یکی از اقدامات اولیه و اصلی در بسیاری از حملات سایبری است. با این حال، غیرمتغیربودن تنظیمات شبکه و میزبانها این امکان را به مهاجمان میدهد تا بتوانند با شناسایی تدریجی و توزیع شده، سامانه‌های هدف را به شکل دقیق و کاملی شناسایی نموده و حملات آگاهانه‌ای را بر روی آنها انجام دهند.

دفاع مبتنی بر هدف متحرک، یک رویکرد دفاعی فعالانه مبتنی بر تغییر پویای تنظیمات شبکه و سامانه هاست. این تغییرات میبایست سریع، غیرقابل پیشبینی، و کمسربار بوده و در عین حال بر روی عملکرد و ماموریت سامانهها تاثیر منفی نداشته باشد. در این ارائه، دفاع مبتنی بر هدف متحرک معرفی گردیده و چندین تکنیک در این حوزه معرفی خواهد گردید. از جمله این تکنیکها، روش تغییر تصادفی IP است که با هدف شکست حملات در مرحله شناسایی انجام میپذیرد. چالش تحقیقاتی این تکنیک، تغییر سریع و غیرقابل پیشبینی IP سیستمها با در نظر گرفتن محدودیتهای امنیتی و عملکردی سازمانها، و همچنین ارزیابی کمی میزان اثربخشی این روش در برابر حملات مختلف از جمله انتشار کرم در شبکههاست.

تکنیک دیگر در این حوزه، تغییر تصادفی مسیرهای شبکه است، که با هدف شکست حملات منعدسترسی و سایر حملات شبکهای انجام میپذیرد. چالش تحقیقاتی این تکنیک، شناسایی پارامترهای متغیر با توجه به تواناییهای مهاجم و انتخاب مسیرهای حائز شرایط و همچنین ارزیابی میزان اثربخشی این روشها در برابر حملات شبکهای است. علاوه بر این دو تکنیک، تکنیکهای مبتنی بر MTD دیگری نیز به اختصار معرفی خواهند شد.

**شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.**