doi:10.1631/FITEE.1800532

题目：NIG-AP：一种自动化渗透测试新方法

概要：渗透测试在发现网络脆弱性与评估网络安全状态方面发挥着重要作用。但是，渗透测试过程只能由安全专家进行，造成了大量时间、人力开销。自动化渗透测试为解决该问题提供了思路，其中最为关键的是攻击规划。不少学者对攻击路径发现进行了大量深入研究，但是大都基于完备的网络拓扑信息，这与实际渗透测试情况不符。为了从攻击者视角发现网络中存在的所有攻击路径，提出一种基于网络信息增益的攻击规划算法（NIG-AP），该算法将渗透测试过程形式化为马尔科夫决策过程，并利用网络信息构建回报函数，并指导代理从入侵者角度发现隐藏的攻击路径，选择最佳响应操作。实验结果表明本文提出的算法能够有效提高攻击路径发现效率。

关键词：渗透测试；强化学习；经典规划；部分观测的马尔科夫决策过程