部分観測マルコフ決定過程に基づいたニューラルエージェントを使用したペネトレーションテスト手法の提案

Proposal of a penetration testing method using neural agents based on partially observable Markov decision process

米田智紀・ネットワーク研究会・情報セキュリティ大学院大学

先行研究調査:
- 既存の強化学習ペンテスタはMDPが中心
- ハッキングにおいて常に状態が観測できるとは限らない → POMDPが有効
- ニューラルエージェントを基にした、テキストベースダンジョン攻略 → ペンテストに有効

目標:
POMDPを基にしたニューラルエージェントを使用して、コマンド実行時の結果から自然言語処理によって解釈し、状態を推定しながら、次の最適な攻撃コマンドを選択するシステムを提案すること

提案手法:
Metasploitのmfsconsole上でニューラルエージェントを作用させ、nmap等で事前処理された攻撃コマンドを実行し、対象システムのシェルやプロンプトの取得を行う

今後の研究:
- 提案システム内に敵対的模倣学習を加え、コマンドの生成を行う。
- 部分観測情報の増加（OS情報、CVE情報等）
- 前処理の部分（スキャン等）も攻撃コマンドの一部として学習させる能力の追加

今後の方針:

2,3	4,5	6,7	8,9	9,10	11,12	1,2	3
システム改修	実験	輪講発表 応用・実験	Summer	CSS、 中間発表	修論準備	修論発表 SCIS	情報処理学会(全国)