SDNに基づく欺瞞防御システム

The research on deception defense using SDN

陳鑫・ネットワーク分科会・情報セキュリティ大学院大学

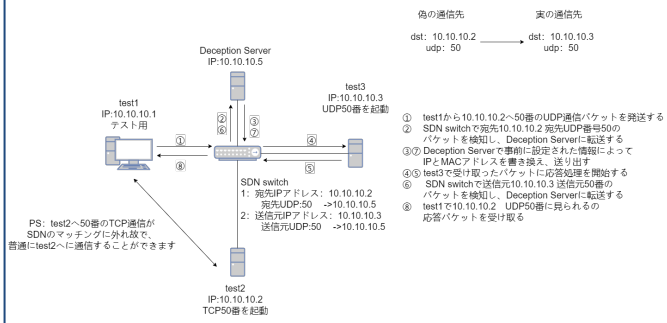
Abstract: With the development of internet technology, attack methods have become more diverse and sophisticated, and targeted attack incidents have increased in recent years. The hiding techniques have been innovated for avoid detection by IDS and IPS, etc. That making it difficult to prevent them completely. Therefore, the deception defensed was proposed which premise of being intruded. It believed that deception can be used to send wrong information to adversary to distort his decision making, causing the targets to shift form their true targets and spoiling the attack. In this part, the focus will be on the "System Network Connect Discovery" phase, which aims to create security policies. Using SDN and OpenFlow, with packet header fielder matching certain traffic is separated is separated from the initial route and its destination is forged. By rewriting the IP, it is conceivable to make the attacker make a wrong decision and hide the important hosts from the attacker's views.

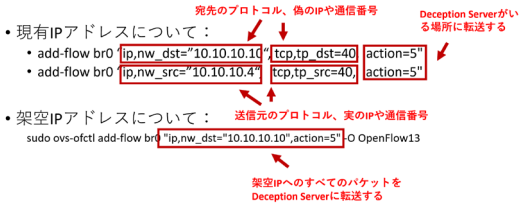
はじめに

サイバー攻撃の手段が巧妙化され、完全に防ぐことが困難になり、侵入されることを前提にした欺瞞防御が提案されていた。本研究は「ラテラルムーブメント」の偵察行動が主な段階に注目し、セキュリティ対策を築くことを狙う。SDNを用い、OpenFlowでパケットヘッダフィールダのマッチングを利用して、とある通信を元のルートから分離させ、その宛先を偽造する。IPの書き換えることで、攻撃者に誤った判断を下させ、重要のホストを攻撃者の視点から隠ぺいすることを考えられる。

提案手法

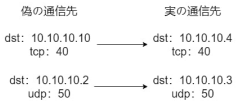
- 「ラテラルムーブメント」の偵察段階に注目し、セキュリティ対策を築くことを目指す。
- 攻撃者が得られる情報に一部を操作して、重要なホストを攻撃者の視点から隠蔽する
- OpenFlowでパケットのヘッダフィールダをマッチングし、特定ポート番号の通信を抽出し、Deception Serverに転送する。Deception Serverが受けたパケットのIPアドレスを事前に設定されたルールによって書き換える形で、重要のホストを攻撃者の視点から隠ぺいする。

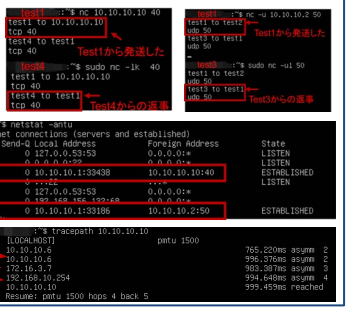




実験結果

- IPアドレスを書き換えながら、通信に影響を及ばない。
- 当該ホストにつながる通信を調べるとTCP40番が「10.10.10.10」へ、UDP50番が「10.10.10.2」にしか見られない。
- 架空IP「10.10.10.10」への「traceroute」請求した結果について、設定通り偽造される。





まとめと今後の課題

本研究は、標的型攻撃のラテラルムーブメントにおいて用いられる「netstat」などの偵察コマンドに対し、通信先情報の書き換えを用いて誤った通信情報を出すことを確認した。

- OpenFlowでIPの書き換えを実行する
- フローテーブルの設定にはSDNコントローラーに移行する