修士学位論文要約（令和 4 年 3 月）

SDN における Moving Target Defense を用いたネットワークスキャン対策手法に関する研究

千葉　翔也

指導教員：菅沼 拓夫

A Study on Network Scan Countermeasure Method Using Moving Target Defense in SDN

Shoya CHIBA

Supervisor: Takuo SUGANUMA

Measures against network scans are necessary to prevent damage caused by targeted attacks. Since attackers can bypass Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) with low-rate scans, Moving Target Defense has been proposed as a countermeasure for low-rate scans. In this paper, we propose a method to prevent low-rate scans that IPS cannot detect with Moving Target Defense (MTD) and prevent high-rate scans with IPS by using MTD that is transparent to IPS. In the evaluation, the number of successful scans was measured in a simulation environment, and it was confirmed that the proposed method was effective in protecting both low-rate scans and high-rate scans.

1.　序論

標的型攻撃では，侵害されたホストを通じて，IP アドレススキャンやポートスキャンなどのローカルネットワークへの偵察が行われる．これらの対策として，Intrusion Prevention System（IPS）や Intrusion Detection System（IDS）などの防御技術が用いられている．しかし，攻撃者は低レートスキャンでそれらを回避できる．そこで，Moving Target Defense（MTD）[1] が注目されている．ネットワークの MTD では，IP アドレスなどを頻繁に変更し偵察を妨害する．しかし，攻撃者は高レートスキャンを行い，アドレスの変更前に攻撃できる．Software Defined Network（SDN）による実装では，パケットヘッダの書き換えによりアドレス変更を実現する．このアドレス変更は，IPS などの既存の防御技術に悪影響を及ぼすことがあり，IPS と MTD を同時に利用するだけでは，様々なレートのスキャンを防ぐことは難しい．本研究では，IPS に透過的な MTD を SDN を用いて実装し，IPS と併用することで，ローカルネットワーク内のホストを高レート・低レートの両方のスキャンから防御する手法を提案する．

2.　関連研究

IPS は高レートのスキャンを容易に検知できる一方で，設定したレート未満の低レート スキャンの検知は難しい．また，そのような低レートスキャンも検知できるように IPS に設定する場合，通常の疎通確認等もスキャンとして誤検知してしまう恐れがある．

そこで，アドレスをランダム化する MTD が注目されている．ネットワークの MTD では，集中型のコントローラとスイッチで通信を柔軟に制御できる SDN の一実装である OpenFlow を用いた手法 [2] が提案されている．MTD は，時間をかけて行う低レートのスキャンに対して有効であるが，高レート のスキャンによりアドレス変更が適用されるまでの間にスキャンを完了し，攻撃を実行することは可能となってしまう．高レートスキャンを防ぐためには，高頻度のアドレス変更が考えられるが，通信品質やコントローラのパフォーマンス等に影響が出ることから，MTD のみで様々なレートのスキャンを防ぐことは難しい．そこで，防御できるスキャンや攻撃の戦略が異なる MTD と IPS を併用することでより高精度にスキャン・攻撃対策が可能となると考えられる．しかし，MTD はアドレス変更を伴うため，IPS のような既存の防御技術に悪影を及ぼすことが懸念される．

3.　提案

本研究では，MTD を IPS の動作に影響を与えないように IPS と併用し，それぞれ単体では防御が難 しいスキャンを同時に防御する手法を提案する．提案手法は，OpenFlow を利用して IPS に透過的となるようにアドレスを変更する．そのため，IPS は MTD の影響を受けずに，スキャン元ホストを継続的に 隔離し，低レートスキャンは MTD により妨害される．

提案手法の動作を図 2 に示す．OpenFlow スイッ

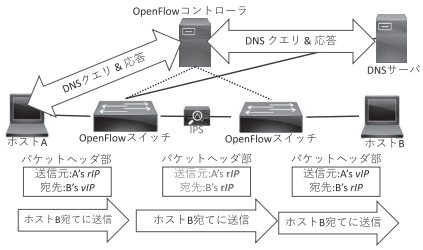

図 1: 提案手法の概要

チは，OpenFlow コントローラがインストールしたフロールールに基づきアドレス書き換えと転送を行う．このアドレス書き換え手法は OpenFlow スイッチ間を流れるパケットの宛先や送信元が時間変化する仮想のアドレス *vIP* ではなく各機器に設定された実際のアドレス *rIP* に基づく点で，既存手法と異なる．この機構によりスイッチ間に配置する IPS は，時間変化しない *rIP* に基づき通信を監視する．

4. 実験

本研究ではスキャン対策としての有効性を評価するため，ネットワーク内のスキャナが一定時間内にスキャンできた回数を測定した．実験には 30 ホスト，2IPS，3 スイッチからなるトポロジをシミュレーション環境で作成して利用した．この際，OpenFlow コントローラに設定するアドレス変更間隔 T を 120 秒とし，IPS は 120 秒間に 10 ホスト以上に対するスキャンを検知するように設定した．

まず，単一のアドレス変更間隔内に完了する短期的なスキャンを 120 秒間に渡って実行した．スキャンのレートは 1 から 254[ホスト/分] とし，スキャンできたホスト数を提案手法（IPS+MTD）と既存手法 [2] に基づく MTD（MTD）で比較した．

図 2 に，単一のアドレス変更間隔内にスキャンできた回数を示す．スキャンレートが 150[ホスト/分] 以下の場合，2 手法に大きな差は認められないが，既存手法ではスキャンレートが高くなるにつれて，提案手法よりも多くのホストをスキャンできると分かる．

次に，複数のアドレス変更間隔にまたがって行われる，長期的なスキャンにおいて，スキャナがホストをスキャンできた回数を測定した．このときスキャナは 1200 秒間にわたりスキャンを行い，スキャンレートは 4，64，128，254[ホスト/分] とし，1200 秒間にスキャンできた総回数を，IPS のみ，既存手法 [2]（RHM），RHM と IPS の併用（RHM+IPS），提案手法の場合で測定した．表 1 にスキャンできた回数の合計を示す．提案手法において，254[ホスト/分] の高レートでスキャンできた回数は，IPS のみの場合と同程度である．一方，既存手法を用いる場合，スキャンできた回数は IPS のみを利用した場合と提案

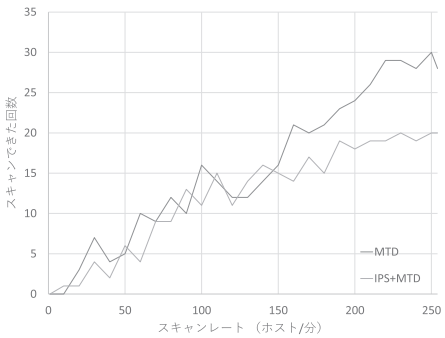

図 2: アドレス変更間隔内にスキャンできた回数

表 1: 1200 秒間にスキャンできた回数の合計

レート	IPS	RHM	RHM+IPS	提案
4	14	6	8	6
64	90	120	134	77
128	111	285	287	101
254	210	577	574	198

手法を利用した場合の 2 倍以上となっている．また，4[ホスト/分] の低レートスキャンにおいて，IPS のみを利用した場合と比べ他の 3 手法ではスキャン回数は半数程度となっている．このことから提案手法は MTD を適用しながら IPS への透過性を確保することにより，高レートスキャンの防御と低レートスキャンの防御を両立できていると考えられる．

5. 結論

本研究では，スイッチ間のパケットを時間変化しない *rIP* に基づいて転送する MTD 手法を提案した．MTD の IPS への透過性を確保することで，IPS と MTD の併用を実現し，高レート及び低レートスキャンの防御を可能とした．実験から，提案手法では IPS は MTD の影響を受けずにホストを遮断し，スキャンを抑制できることを示した．今後は，アプリケーションへの影響や遅延の評価が必要となる．

参考文献

1) U.S. NSTC, “Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program,” Federal Cybersecurity: Strategy and Implementation for Research and Development, pp. 69–99, 2011.
2) J. H. Jafarian et al, “OpenFlow random host mutation: Transparent moving target defense using software defined networking” Proceedings of the 1st ACM International Workshop on Hot Topics in SDN, pp. 127–132, 2012.