7ZC-07

仮想環境における L2 ネットワークの脆弱性分析と DHCP スプーフィング緩和手法の提案

瀬川　大悟 †,　中村　康弘 ‡
防衛大学校理工学研究科情報数理専攻 †, 防衛大学校情報工学科 ‡

1　はじめに

マルチテナント型クラウドサービスでは，複数のユーザが一つのリソースを分割して利用するため，悪意のあるユーザやマルウェア感染した仮想マシンから攻撃を受けるセキュリティ上のリスクが指摘されている．クラウドサービスプロバイダがクラウド環境構築のために利用するハイパーバイザの仮想スイッチや，オープンソースの仮想スイッチは，物理スイッチを模倣して実装しているが，仮想環境内の通信の効率性を優先するため，物理スイッチが備えているようなセキュリティ機能が実装されているとは限らない．

本研究では，物理ネットワーク上で指摘され，改善されてきた脆弱性のうち，仮想環境において対策されているもの，有効なものを明らかにするため，仮想環境の実装に対して既知の L2 層（Layer2 層，データリンク層）プロトコルの脆弱性攻撃（以下，L2 攻撃）による検証を行う．検証の結果，有効であると判明した DHCP スプーフィングを検知，遮断する緩和手法を提案する．

2　関連研究

コンピュータネットワークプロトコルレイヤにおける，L2 層の脆弱性とその緩和手法についてはこれまでに数多くの研究が行われてきた．物理環境では，主にネットワーク機器メーカが開発する L2 スイッチのセキュリティ機能により攻撃に耐性がある．一方，仮想環境については，文献 [1] において，仮想化ハイパーバイザや Open vSwitch で構築した仮想環境に対して，MAC フラッディングや DHCP スプーフィングといった攻撃が，仮想環境においても有効であるかどうかの検証が行われた．しかしながら，上記の研究は攻撃に対する仮想環境や仮想スイッチの脆弱性の評価に止まり，攻撃に対する緩和手法については言及されていない．また，主要な仮想化ハイパーバイザの一つである VMware vSphere の製品ドキュメント [2] では，攻撃に対する標準スイッチと仮想ネットワークの保護について言及しているが，一部の攻撃に限定されるとともに耐性のない攻撃に関する記載はない．

3　仮想環境の実装に対する L2 攻撃の検証

主要な L2 攻撃と仮想環境における攻撃の可否を表 1 に示す．

文献 [2] で耐性が不明となっている DHCP スプーフィングが，文献 [1] と同様に現在においても攻撃可能であるかどうか確認するため検証を行う（図 1）．

DHCP クライアント（攻撃対象）は IP アドレスを要求するため，DHCP Discover を LAN 内にブロードキャストする．正規の DHCP サーバよりも先に攻撃者の DHCP サーバが応答した場合，DHCP Option により LAN 内に存在しないアドレスがデフォルトゲートウェイに，DNS は攻撃者の仮想マシンに設定されたりすることで，攻撃対象は正常な通信を行えなくなる．DHCP プロトコルは攻撃を考慮して設計されておらず，受信したパケットの真正性を判断することなくキャッシュされるため攻撃が可能となる．

表 1: 主要な L2 攻撃と仮想環境における攻撃の可否

攻撃手法	仮想環境（VMware ESXi）	
	文献 [1]	文献 [2]
MAC アドレススプーフィング	-	攻撃可 緩和策：MAC アドレス変更拒否， 偽装転送拒否
スパニングツリー攻撃	-	攻撃不可 STP をサポートしていない
VLAN ホッピング （802.1q 及び ISL タギング攻撃）	-	攻撃不可 動的トランキングを実行しない
MAC フラッディング （CAM テーブルオーバーフロー）	攻撃不可	攻撃不可 観測可能なトラフィックから MAC アドレスを取得しない
DHCP スプーフィング	攻撃可	記載なし

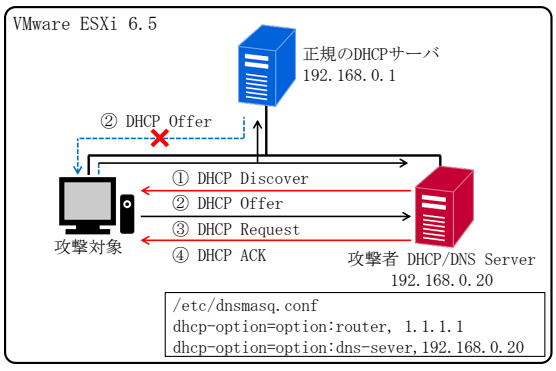

図 1: DHCP スプーフィング

Vulnerability Analysis of L2 Network in Virtual Environments and Proposed DHCP Spoofing Mitigation Method,
†Daigo Segawa, Master Course Mathematics and Computer Science, Graduate School of Science and Engineering, National Defense Academy of Japan,
‡Yasuhiro Nakamura, Department of Computer Science, National Defense Academy of Japan

4 提案手法

検証の結果，仮想環境において有効である DHCP スプーフィングを，仮想化ハイパーバイザと仮想スイッチの機能を利用し，それを補完する形で DHCP スプーフィングを検知し，攻撃者の仮想マシンをネットワークから自動遮断する緩和手法を提案する．

4.1 提案手法の手順

提案手法の手順を以下に示す．

1. 監視対象の仮想マシン情報の取得
   監視対象のポートグループに存在する各仮想マシンを一意に識別する VMID，MAC アドレス，ネットワークアダプタの Device ID を取得し，それぞれの値をデータベースに保存する．また，監視対象の LAN を流れる DHCP パケットを捕捉し，正規の DHCP サーバの MAC アドレスをハッシュテーブルに保持する．
2. 不正な DHCP パケットの検知
   新たにキャプチャしたパケットの送信元 MAC アドレスと，ハッシュテーブルに保持している MAC アドレスが一致しない場合は，不正なパケットと判断する．
3. 不正な DHCP パケットの送信元の遮断
   送信元 MAC アドレスをもとにデータベースから取得した VMID と Device ID を引数として vSphere CLI コマンドを実行し，不正なパケットの送信元仮想マシンが監視対象の LAN に接続しているネットワークアダプタを Disable にする．

4.2 提案手法の実装

提案手法の実装の概要を図 2 に示す．

各仮想マシンの OS は Ubuntu20.04LTS，Linux Kernel は ver5.15 を使用している．ポートグループ 1 には不正な DHCP パケットを検知する監視用の仮想マシンを設置し，標準スイッチとポートグループ 1 のセキュリティポリシの「無差別モード」を「承諾」に設定する．VLAN ID を「4095」にすることで，VGT（Virtual Guest Tagging）モードに設定され，VLAN タグの付け外しは仮想スイッチではなく仮想マシン上で実行されるため，同じ標準スイッチに接続されている他のポートグループのパケットを捕捉できる．監視対象の LAN をポートグループ 2 とする．また，標準スイッチに VMKernel NIC を追加し，構成した管理用 LAN と同じ VMID をポートグループ 3 に設定することで，リモートから vSphere CLI コマンドを実行し監視対象の仮想マシンを操作する．なお，標準スイッチとポートグループのセキュリティポリシの設定により，MAC アドレスの変更ができないことを前提とする．

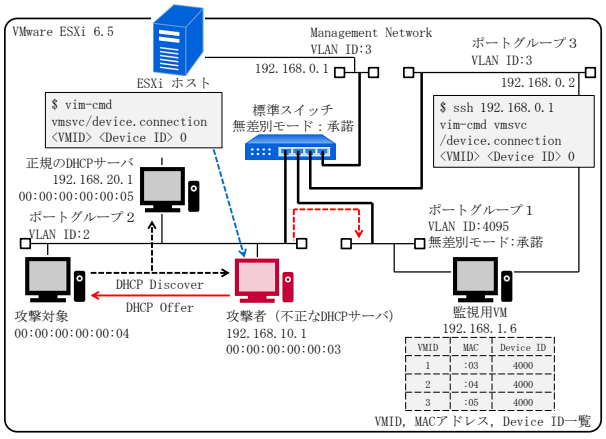

図 2: 提案手法の実装の概要

4.3 検証実験

提案手法により，不正な DHCP パケットを検知し送信元の仮想マシンを遮断することで，DHCP スプーフィングを緩和できるか確認するため検証実験を行った．

正規の DHCP サーバの MAC アドレスをハッシュテーブルに保持した監視用の仮想マシンが攻撃者の DHCP Offer を受信した際，攻撃者の仮想マシンを遮断するのを確認した．

5 まとめ

仮想環境において攻撃可能であると判明した DHCP スプーフィングの緩和策として，仮想化ハイパーバイザと仮想スイッチの機能を利用し，それを補完する形で攻撃を検知，遮断する緩和手法を提案した．実験の結果，提案手法の実装で攻撃を検知，遮断できることを確認した．

しかしながら，本手法は，不正な DHCP Offer を確認した後，攻撃者の仮想マシンを遮断するが，遮断が完了するまでに攻撃者が DHCP ACK を送信した場合，攻撃対象は攻撃者から IP アドレスを割り当てられ，不正なデフォルトゲートウェイや DNS サーバと接続させられてしまう．攻撃者が DHCP ACK を送信する前に攻撃者のネットワークアダプタを切断するための改良が必要であると考える．

参考文献

[1] Ronny L. Bull, Jeanna N. Matthews: *Critical analysis of layer 2 network security in virtualised environments*, International Journal of Communication Networks and Distributed Systems, Vol.17, No.3, pp.315-333, Inderscience Publishers, 2016.

[2] VMware: *VMware vSphere Product Documentation*, `https://docs.vmware.com/en/VMware-vSphere/index.html`,（2022 年 12 月 21 日閲覧）