L-024

Dockerによる仮想ネットワーク環境における侵入挙動観測に関する研究

Research on observation of intrusion behavior in virtual network environment by using Docker

ファン スォン ホアン‡　　中村 康弘‡

Hoang Xuan Pham　　Yasuhiro Nakamura

1.はじめに

近年、ソフトウェアの脆弱性やマルウェアを用いて標的のシステムへ侵入するサイバー攻撃は大きな社会問題となっており、その攻撃手法は巧妙化・多様化している。マルウェアが組織のネットワークへ不正侵入した後に、水平展開という組織内部ネットワークに感染を拡散させていくことが行われる。システムへの侵入を防ぐことが最も重要なセキュリティ対策であるが、もし侵入された場合には、侵入後の攻撃者の挙動がいかなるものであるのかについて、情報を収集しておくことが重要である。攻撃者に気付かれないように侵入後の挙動を観測するために、実ネットワークと類似した仮想ネットワーク環境を用いる研究があるが、構成したネットワーク環境は固定であり、全ての水平展開手法を観測できるとは限らない。

そこで、外部ネットワークの攻撃者からの接続要求を観測した結果に基づいてネットワーク構成を動的に変更することを目的として、Dockerを用いて仮想ネットワーク環境を構築し、侵入してきた攻撃者の侵入後の挙動を観測するシステムを提案する。

2.Docker

DockerとはDocker社によって開発されたコンテナ型の仮想環境を作成、実行、そして管理できるオープンソースソフトウエアである。DockerはLinuxコンテナ技術をベースとして完全仮想化のサービスを提供するのではなく、コンテナ型仮想化を実現するので、よくVirtualBoxとかVMwareなどの仮想マシンと比較される（図１）。

仮想マシンの技術と異なり、ゲストOSのインストールをことが必要とせず、Dockerのコンテナ型仮想化における複数のコンテナはホストサーバのカーネルを共有して利用しているため、プロセスやユーザなどをサーバごとに隔離することで、あたかも別のマシンがOS上に動いているかのように動かすことが可能となる。そのため、Dockerはアプリケーションをコンテナにパッケージングして、サーバの高速な起動、停止などが可能である。

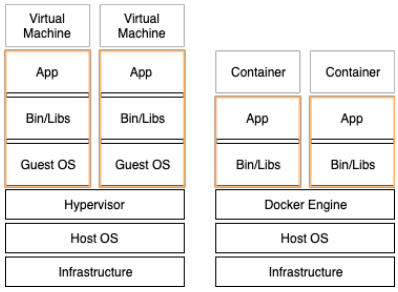

図１　Dockerとバーチャルマシンの構成

†防衛大学校　理工学研究科　サイバーセキュリティ工学

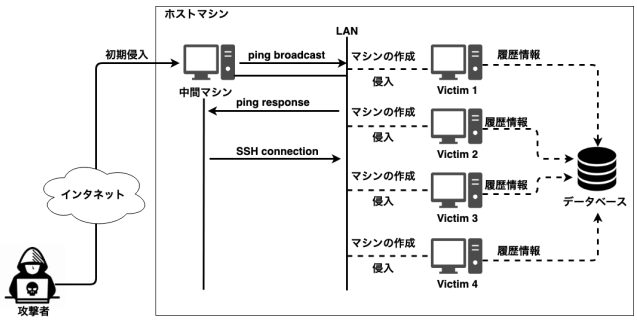

図２　提案手法の概要

3.侵入挙動観測の既存研究

攻撃者の侵入挙動を観測するためのいくつかの既存手法が提案されている。文献[1]では、攻撃者の行動を監視及び調査するためにDockerコンテナ上で複数のハニーポットセンサーを配置し、それを用いて侵入してきた攻撃者からの行動を収集する。収集した全てのキャップチャデータをELK Stackで保存、分析、可視化する手法を提案している。しかし、提案システムでは各ハニーポット（マシン）が相互に侵入不可ため、侵入後の挙動が得られない。

また、文献[2]では、標的型攻撃の攻撃者を実ネットワークに類似した仮想ネットワーク環境に誘い込み、長期にわたって手動攻撃の挙動を観測している。このシステムではWindowsクライアントマシン上でマルウェアを実行しているため、初期のLinuxマシンを攻撃対象としたマルウェアの挙動が観測されていない。

そして、文献[3]では、Linux上で動作するマルウェアをプライベートネットワークとパブリックネットワーク内で安全に解析可能な動的手法を提案している。実際にマルウェア 検体が行なった通信挙動のみを観測したが、解析環境内で内部挙動を観測しない。

本研究ではLinuxマシンを狙ったマルウェアの侵入挙動について仮想ネットワークを動的に構築することで侵入後の挙動を観測する手法を提案する。

4.提案手法

攻撃者が組織内のあるマシンに侵入した後、同じネットワーク内に接続する機器を調査するためにマシンのログを見ることやブロードキャストアドレス宛にpingコマンドを投げることなどがよく利用される。

本研究では、後者に着目して、動的に仮想ネットワークを構築し、侵入後の挙動を観測する手法を提案する（図２）。提案手法の各ステップを以下に示す。

（１）仮想内部ネットワーク環境（LAN）を構築する。

（２）外部と内部ネットワークとのアクセスできる脆弱性がある中間マシンを作成する。

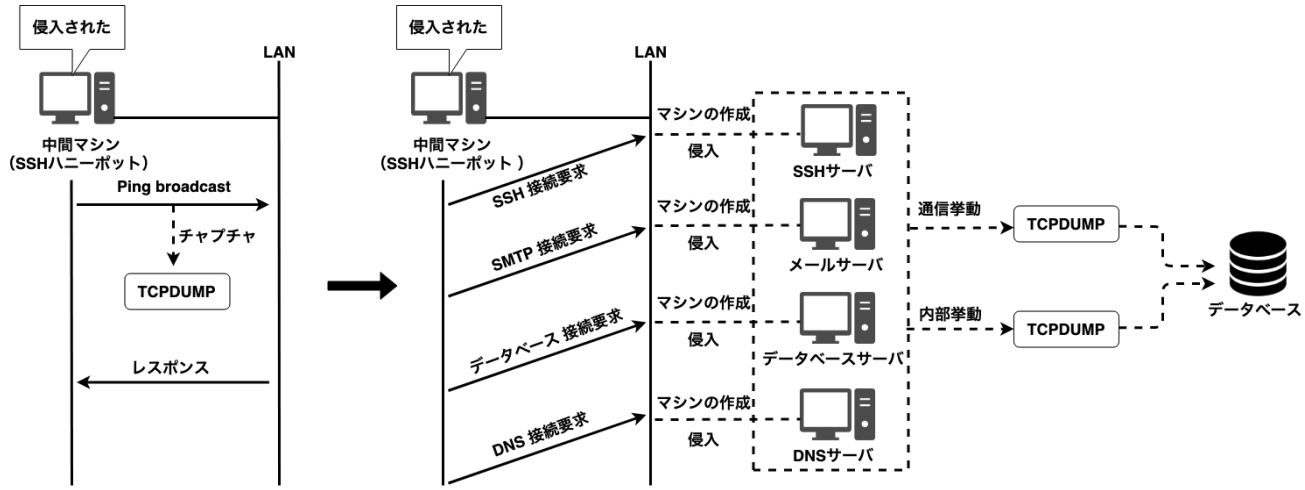

図３　侵入挙動観測の実装

（３）外部ネットワークからの攻撃者に侵入された中間マシン経由で仮想LAN内のブロードキャストアドレスへ通信に対して自動的に応答するよう設定する。

（４）攻撃者からの接続要求IPアドレスを合わせて内部ネットワークに接続する仮想マシンを迅速かつ自動的に用意し、アクセスさせる。

（５）構築した内部ネットワーク内の全ての仮想マシン上で発生した通信挙動と内部挙動を観測する。

5.侵入挙動観測の実装

本研究では具体的な侵入挙動観測の実装を図３に示す。

（１）一台のホストマシン上にDockerを用いて内部間通信のみの仮想ネットワークを構築する。

（２）外部ネットワークの攻撃者を仮想内部ネットワーク内に侵入させるために、SSHハニーポット（Cowrieハニーポット）コンテナで中間マシンを構成する。

（３）ホストマシンでは中間マシン上で攻撃者から発生したブロードキャストアドレスへの通信をtcpdumpでキャプチャし、接続要求に自動応答する。

（４）攻撃者からの接続IPアドレスを要求する瞬間にそのIPアドレスを合わせてDockerのコンテナで内部のネットワーク内のマシン（コンテナ）を作成・起動する。

（５）tcpdumpツールを用いて内部ネットワークインターフェースの通信をキャプチャし、内部のコンテナ（マシン）にはsyslogによるプロセスの挙動をホストマシンにログファイルとして転送して保存する。

中間マシンにログインしてきた攻撃者が入力したコマンド（内部挙動）及び通信データを記録する。

6.まとめ

Dockerを用いて仮想ネットワーク環境を動的に構築し、侵入後の攻撃者の挙動を観測する手法を提案した。初期侵入されたマシン（中間マシン）の内部挙動と通信挙動を確認できる。また、関連研究との比較結果を表１に示す。この結果により、本研究の提案手法の有効性が明らかにした。今後、観測結果の分析と予防措置について検討する必要がある。そして、無限侵入の問題に対しての対策も検討したい。

表１　関連研究との比較結果

	侵入観測	水平展開	ネットワーク動的構築
ハニーポット (Andronikosら)	O	X	X
Stardust (津田ら)	O	O	X
マルウェア動的解析 (田辺ら)	O	O	X
提案手法	O	O	O

参考文献

[1] Andronikos Kyriakou, Nicolas Sklavos, “Container-Based Honeypot Deployment for the Analysis of Malicious Activity”, Global Information Infrastructure and Networking Symposium (GIIS’18), 2018.

[2] 津田 侑, 遠峰 隆史, 金谷 延幸, 牧田 大佑, 丑丸 逸人, 神宮 真人, 高野 祐輝, 安田 真悟, 三浦 良介, 太田 悟史, 宮地 利幸, 神薗 雅紀, 衛藤 将史, 井上 大介, 中尾 康二, “サイバー攻撃誘引基盤 STARDUST”, コンピュータセキュリティシンポジウム2017 (CSS2017) 論文集, Vol.2017, No.2, pp.472-479, 2017.

[3] 田辺 瑠偉, 筒見 拓也, 小出 駿, 牧田 大佑, 吉岡 克成, 松本 勉, “Linux上で動作するマルウェアを安全に観測可能なマルウェア動的解析手法の提案”, コンピュータセキュリティシンポジウム 2014 (CSS2014) 論文集, Vol.2014, No.2, pp.1007-1014, 2014.