WSLを用いて初学者が自分で構築できる不正アクセス解析のための安全で簡易な教育用攻撃・被攻撃環境の実装

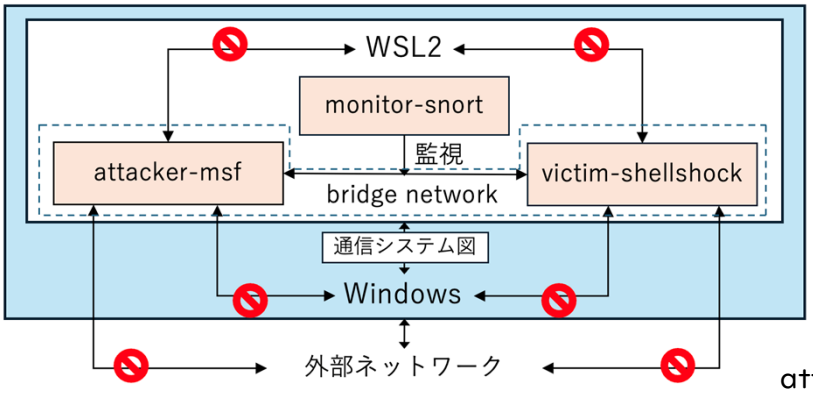
山﨑創 岡部寿男 (京都大学)

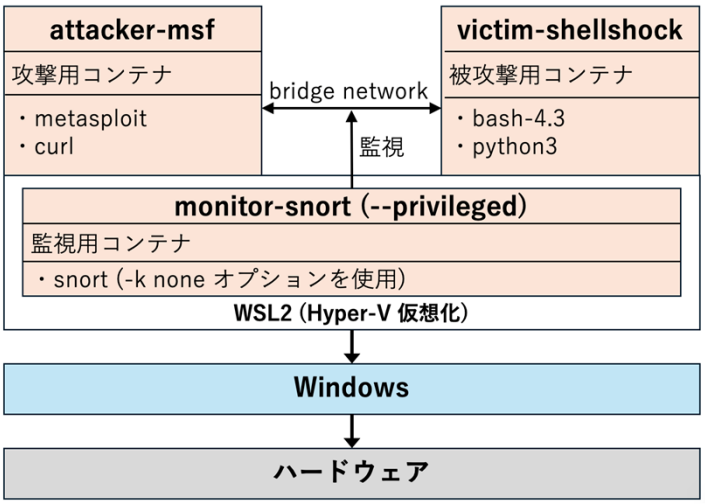
背景、目的

文科省補助事業enPiTの一つ、Basic SecCapのPBL演習: IDSを用いたshellshock検知演習
従来はVDI, VMを利用: 管理維持コストが大きい → WSLを用いて初学者用実験環境を構築

実験環境

Windows PCにWSL → WSLにDockerをインストール
2つのDockerコンテナ, 特権モードの監視用コンテナを利用





attacker-msf/victim-shellshock
・互い以外に通信できない
・bridgeを用いて接続

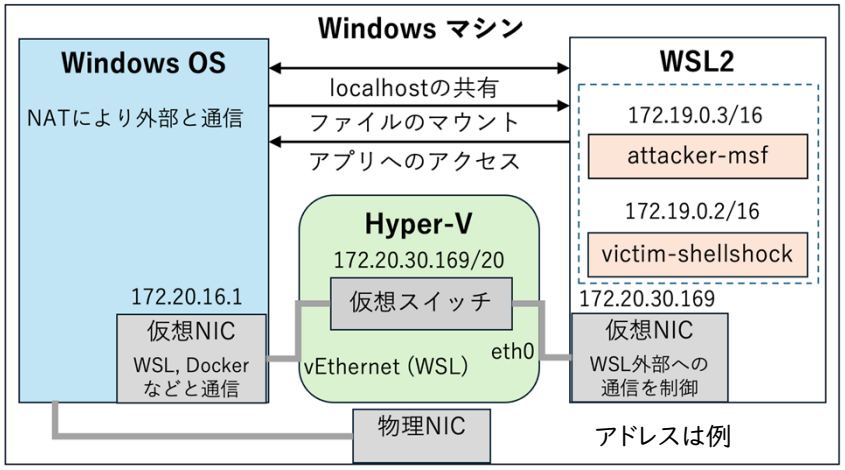
WSL, Dockerコンテナ

Windows-WSLの関係は通常のVMと大きく異なる

・WSL→外部インターネット の通信経路
仮想NIC(WSL) → 仮想スイッチ → 仮想NIC(Windows) → NAT処理(Windows) → 物理NIC

・コンテナの名前空間(namespace)
コンテナが独自ネットワークで動いているよう扱うために、各構造を他コンテナと隔離する

- PID名前空間
  プロセスIDを隔離
- Network名前空間
  IPアドレス、インターフェース、ルーティングテーブル等を隔離
- Mount名前空間
  マウントされたファイル構造を隔離
- UTS名前空間
  ホスト名、ドメイン名を隔離



通信システム図

構築手法

前提 WindowsにWSL, WSLにDockerがインストールされた状態

1. WindowsにDockerfileなどが含まれるattack/victim用tarファイル, snort用tarファイルをダウンロード
2. WSL内で任意のディレクトリにtarファイルを解凍
3. monitor-snortのDockerfile内、監視するブリッジ名を自分の環境に合わせて変更 例: br-ef92df9c4736
4. attack/victim, snortをそれぞれビルド、起動
5. attacker-msfからvictim-shellshockに攻撃→snortにアラートが表示される

詳細, ダウンロード: https://github.com/Syama03/IDS-Education

まとめ

・軽量で扱いやすいWSLを用いてsnort、metasploitを使用できる初学者用実験環境を構築した
・完全に隔離された環境であり、外部への攻撃危険性、外部からの攻撃危険性が低い
・metasploitを用いた実践的な検知実験、Dockerfileに追記して別のツールの使用等も可能
→ 学習者が自分で構築できる、安全かつ簡易な教育用IDS実験環境の構築手順を確立