SecHack365

仕組みが理解しやすいシンプルなハニーポット Stepot

開発駆動コース 川合ゼミ　豊田 昂輝

制作背景

ハニーポットとは、あえて脆弱性のあるコンピュータであると見せかけてサイバー攻撃を観測するシステムのことである。ハニーポットの多くは、ブラックボックス化していて**仕組みが分かりづらい**。さらに、サーバ運用経験のない人はハニーポット運用にどのようなリスクがあるのかを把握することは難しい。

これらを解決するために、シンプルで仕組みの理解しやすいハニーポットの開発に取り組んだ。

Stepot

Stepotを使用すると、セキュリティについて学習することができてユーザがStep upすることができる。
さらに、Stepotはまだまだ開発途中であり、Step upの余地があるためこの名前に決めた。

想定するユーザ

- ハニーポット(サーバ)をまだ運用したことがない人
- サイバー攻撃を実際に見てみたい人

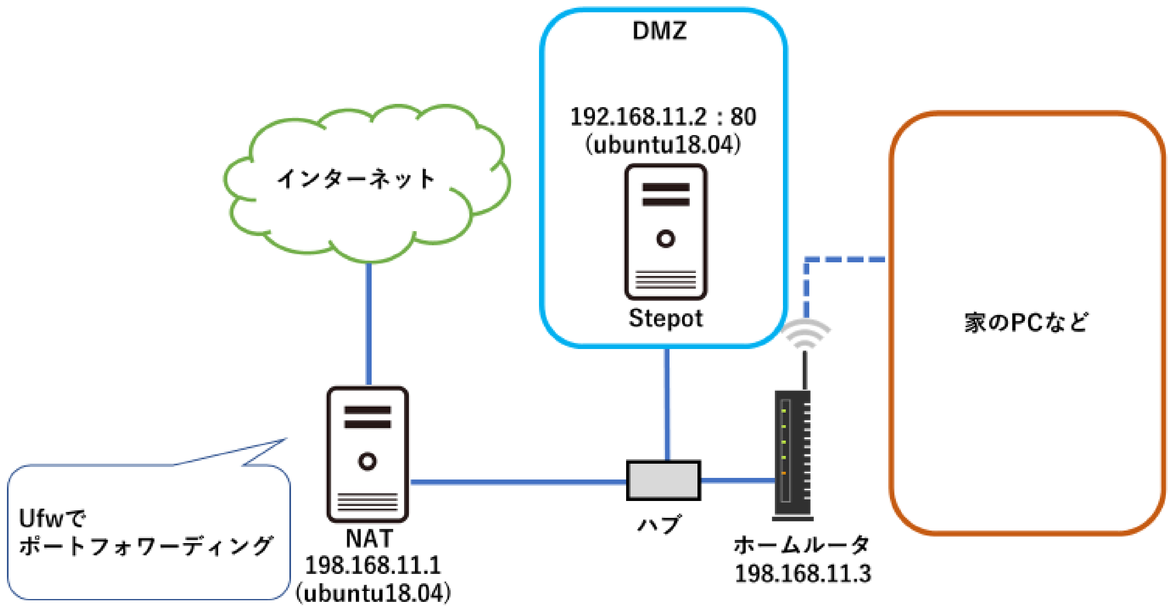
特徴

- シンプルに実装
  - webサーバ型の低対話型ハニーポット
  - ログをファイルに出力
- できるだけ短いコードで実装
  - 53行程度で実装
  - Python3のHTTP.serverモジュールを使用
    - SimpleHTTPRequestHandler
    - BaseHTTPRequestHandler　など

設置方法

自宅に設置する場合、このような構成で設置する

- Stepotの設置場所が隔離されているため、踏み台にされてしまったとしても自宅のPCなどに影響はない
- ネットワークのルーティングなどの設定も学べる



運用結果

Stepotを実際に自宅に設置して3日間運用した結果

- Tomcatの脆弱性を狙った攻撃 → **17件**
- 家庭用ルータの脆弱性を狙った攻撃 → **6件**
- フレームワークの脆弱性を狙った攻撃 → **5件**
- 任意のコードを実行させようとしていた攻撃 → **3件**

→ たった3日間の運用でも
これだけの攻撃を観測することができた！

↓

- インターネットに接続している機器のセキュリティ管理意識の向上につながった
- 観測することのできた攻撃への対策を調べて学ぶきっかけができた

今後の展望

- 攻撃者の行った攻撃が成功しているかのように見せかけられるようにする
- 学習用コンテンツとして自分の行った開発の流れをwebサイトを作成し、まとめる
- 安全性をさらに高めるようなシステムにする
- ルータの脆弱性を狙った攻撃が気になったため、ルータ型ハニーポットへの移行を目指す

NICT 国立研究開発法人 情報通信研究機構