ハニーポットによる不正ファイルの入手と分析

G984822019 吉村　直将

指導教員　教授　蓑原　隆
助手　田島　信行

1　はじめに

近年，サイバー攻撃の発生件数が年々増加してきており，その攻撃手法も多様化している．多様化した新しい攻撃に対処するためには攻撃手法の分析が必要である．攻撃手法の分析のために，攻撃者を誘き寄せ，不正アクセスを受けるハニーポットを用いて攻撃者の情報を収集する方法がある．例えばハニーポットを利用して，ログイン試行時に使われる ID やパスワード，ログイン後に攻撃者から送られるシェルコマンド等の情報を収集する方法が提案されている [1].

本研究では，より具体的な攻撃者の攻撃手法の情報を得るため, 攻撃者がログイン成功後に行う攻撃に着目し，ハニーポットを用いて，攻撃者から送信されるコマンドやそのコマンドから入手できるファイルの情報を収集し，解析するシステムを構築する．そして，攻撃の分析を行い，最新の攻撃内容について警告を発することを目的とする．

2　攻撃収集分析システム

攻撃者がダウンロードさせようとしてくる不正なソフトウェアの解析を実現する為のシステムの構成を図 1 に示す.

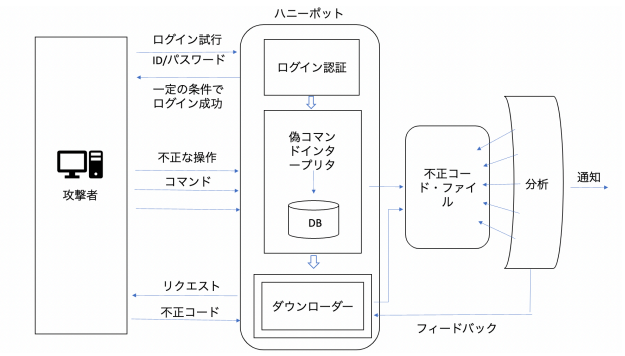

図 1　システムの構成

ハニーポットは, 攻撃者からの何度かのログイン試行を受け，一定の条件で，攻撃者にログイン成功したと思わせる．その後，攻撃者にコマンドインタープリタの様な返答を見せ，不正な操作のコマンドをデータベース DB に収集する．収集したコマンドから，攻撃者が不正なサイトからダウンロードさせようとする不正なファイルを安全に入手する．また，コマンドの中には、ハニーポット内に不正ファイルの作成を試みるものもあり、安全にファイルを作成し、収集を行う。収集した不正ファイルのコードから，どの様な不正ファイルかを分析し警告を発する．また，その情報からダウンローダーに生かせるものをフィードバックする．

本研究では，Dshield と呼ばれる分散型侵入検知システムをベースにしたハニーポットを実装する．これまで研究室では主に攻撃頻度の時系列解析のために Dshield ハニーポットを利用している [2].

図 1 のログイン認証部，コマンドインタープリタ部は，Dshield の cowrie に必要な機能を追加する形で実現する．また, コマンドからファイル又は，URL などを取集するダウンローダー部，不正ファイルの分析部は，新しくプログラムを作成する．

3　進捗状況

Raspberry Pi に Dshield をインストールし，パスワードや接続する無線 LAN の設定を行なった．Rassberry Pi のファイアウォールの設定から SSH を有効にする事で，外部からの接続を cowrie が対応するように設定した．また，研究室内のネットワークからの接続は攻撃と見さないように設定した.

攻撃者からコマンドを収集するために Dshield のプログラムを調査し，コマンドを収集できているのか確認した．調査の結果，Dshield は攻撃コマンドを取集し，/srv/cowrie/var/log/cowrie の場所に保存していることが分かった．また，ログイン試行に対応しているプログラムが/src/cowrie/core/の場所にある auth.py であることを突き止め，解読したところ，Dshield は外部からの攻撃者からのログイン試行を 1 回以上のランダム数行うと，ログイン可能とするように設定されていることが分かった.

実際にハニーポットを運用し 5/19 から 5/30 の期間中にコマンドを取集した．収集したコマンドの中には特定のパターンのコマンドが多く発見された．例えば組み込み Linux で複数のコマンドをまとめるために使われる busyBox が含まれていて, この期間中に多くの攻撃が組み込み Linux の機器を対象としていることが分かった．また, 収集したコマンド中には, 不正なファイルをダウンロードさせるためのコマンドや不正なファイルをハニーポット内に作成するコードが見られた.

4　今後の予定

9 月までにダウンローダー部を完成させ，不正ファイルを取得できるようにする．その後，収集したファイルの分析を行う部分を作成し，11 月までにシステムの運用評価を行う.

参考文献

[1] 中山楓, 鉄穎, 楊笛, 田宮和樹, 吉岡克成, 松本勉：“IoT 機器への telnet を用いたサイバー攻撃の分析”, 情報処理学会論文誌, **58**, 9, pp. 1399–1409 (2017).

[2] 西田圭介：“インターネット上のサイバー攻撃のハニーポットを用いた分析と可視化”, 拓殖大学工学部情報工学科卒業論文 (2022).