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

1.1　研究背景

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. 対策として, 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運用し, 攻撃者の情報を収集してきた. ハニーポットは, 攻撃を受け, 攻撃内容を記録する. その攻撃手法を分析することで, 攻撃への対策を強化することやデータ収集方法を改良することにつながる. 過去の研究では, 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し, 研究を行ってきた. [1] 本研究では、ログイン後に攻撃者から送られるコマンドに着目する. コマンドについて解析することは、攻撃者がログイン成功後にどうゆう意図を持ち, 何を目的をとして攻撃を行なってくるかの予測が立てらる. 又, コマンドから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情報を知り、調査できる為, より最新の攻撃に対して具体的なセキュリティ対策につながると思われる. 本研究でのハニーポットは,Dshield と呼ばれるハニーポットを用いる. DShield（Distributed Intrusion Detection System）は, グローバルなセキュリティコミュニティによって構築された分散型侵入検知システムである. 世界中のネットワーク上で発生するセキュリティイベントのデータを収集し, 分析することでセキュリティの脅威情報を提供する.Dshield は研究室で以前から運用していて, 主にログイン試行時の Id やパスワードを収集することを目的としたハニーポットとして利用していた.

1.2　目的

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為、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ることで, 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　研究方法

本研究の目的である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を図 2 に示す. ハニーポットはインターネットから攻撃受け, 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, ハニーポットは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 DB に収集する. 収集したコマンドから, 不正なサイトで攻撃者がダウンロードさせてくるソフトウェアのデータを集めるダウンロードーを構築する. 又, コマンドの中には, コマンドからハニーポット内に直接不正なファイルを作成しようとしてくるものもあり, そのコマンドのコードからどの様な不正ファイルかを分析し、警告を発し, 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していく.
研究計画として,

1. Dshield を運用できる環境を構築をする.
2. コマンドを収集するために、Dshield のプログラム内で、攻撃者からのコマンドに対してどのような動作をしているかを確認する.
3. 実際に Dshield を運用してみる.
4. 取集したコマンドの内容について調べる.
5. コマンドからファイル又は,URL などを取集するプログラムを作成する.
6. ファイルがどのようなものなのか調べる.
7. 安全に不正なファイルを一時的に保存するダウンローダーを作成する.

という手順で進めていき, 攻撃ファイルがどの様なものなのか把握し, どのような対策が有効的なのか等の警告を発することで, セキュリティの向上に貢献していく.

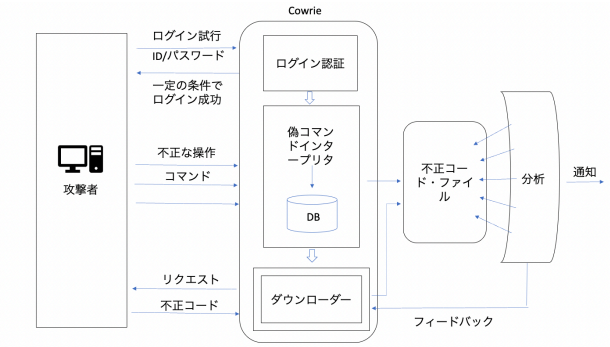

図 1　ファイル入手システム

3　今まで行ってきたこと

3.1　Dhield の運用できる環境の構築

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. 設定の更新には, 少しの時間が掛かっった. 又,RassberryPi の設定からインターフェースの SSH を有効にする事で, SSH を通って外部 PC から接続を可能にした. 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.

3.2　Dshield が行う攻撃者のログイン試行への対処方法

Dshield は研究室で以前から運用されていたが id やパスワードの収集を目的として使われていた. 本研究

では、コマンドを収集したいので, Dshield のプログラム内容からコマンドを収集できているのか, 又出来る様に設定していきたい．Dshield のプログラを調査した結果, Dshield は id/パスワード情報だけでなく, コマンドを取集していることが分かった．収集したコマンドは,/srv/cowrie/var/log/cowrie の場所に保存されていることが分かった．又,Dshield が行う攻撃者のログイン試行への対処方法は,/src/cowrie/core/の場所にある auth.py から分かった。Dshield は外部からの攻撃者（一つの決まった IP アドレス）からのログイン試行を１回以上のランダム数行うと, ログイン可能とし, そのログイン成功時に使用していたユーザー ID とパスワードがその IP アドレス限定でのログイン成功するものとなる．これは, ハニーポットと見破られないように考えられたシステムだと思われる．

3.3　収集したコマンド内容

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、特に多かったパターンのコマンドが存在していた．そのパターンのコマンド内には,bin/busyBox が含まれていて, busybox は組み込み Linux で一般的なファイルとして有名であり, この事から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．又, 収集したコマンド中には, 目的としていた不正なファイルをダウンロードさせる為のコマンドとして wget や crul 後に URL があるものや不正なファイルをハニーポット内で作成するコードを用いたコマンドが見られた．

4　今後やる事

今後やる事としては, 収集したコマンドからハニーポット内に直接不正なファイルを作成しようとしてくるコードに対して, 安全に考慮した上で, 自分でコードから少しずつファイルを作成してみて, どの様な不正ファイルか解析していく事と安全に URL から不正なファイルを一時的に保存できるダウンローダーを作成する事とする。

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).