レイヤ2スイッチを用いた不正パケット遮断システムの研究

05G458 串間 竜治 （最所研究室）

本研究では、コンピュータウィルスや情報流出などの対策として、レイヤ 2 スイッチを用いた不正パケットを遮断システムを提案する。このシステムは、不正パケットを送信したホストの IP アドレスから、MAC アドレス、ホストの接続されているレイヤ 2 スイッチ、ポート番号を調べ、レイヤ 2 スイッチの設定変更を自動的に行うものである。

1 はじめに

現在、パソコンやインターネットの普及に伴い、コンピュータウィルスに感染し、知らない間に攻撃してしまう事や、悪意のある人の不正行為、個人情報流出なども急増している。このような問題に対してレイヤ 2 スイッチ (以降 L2 スイッチ) を用いて不正パケットを遮断するシステムを提案する。このシステムは、侵入検知システムを用いて不正パケットを検知し、対象のホストが接続されている L2 スイッチをつきとめ、その L2 スイッチの設定を変更し通信を遮断するといった一連の動作を自動的に行うものである。なお、ユーザインタフェース部を共同研究者の長野氏 [1] が研究している 。

2 システムの概要

本システムの構成を図 1 に示す。本システムは、(1)PC1 が不正パケットを送信する。(2) 侵入検知システム (IDS) が不正パケットを検知し、同時に PC の IP アドレスが取得する。(3) この情報をここで開発するツールが受け取る。(4) 不正パケットの情報を受けた管理ツールは、DHCP データベースもしくはルータの ARP テーブルを参照し、IP アドレスから MAC アドレスを取得する。(5)MAC アドレスが判明したら、次は SNMP [2] で各 L2 スイッチのフォワーディングデータベースを参照し、ホストがどの L2 スイッチのどのポートに接続されているかを特定する。(6) そして、L2 スイッチの MAC アドレスフィルタリング設定を変更し、通信を遮断するものである。

2.1 本システムで対象となる L2 スイッチ

本システムで用いることができる L2 スイッチが満たさなければならない条件は以下である。

1. SNMP などを用いてフォワーディングデータベース (FDB) を参照できる。
2. 指定した MAC アドレスの通信を遮断できる。もしくは、指定した MAC アドレスの通信のみ許可できる。

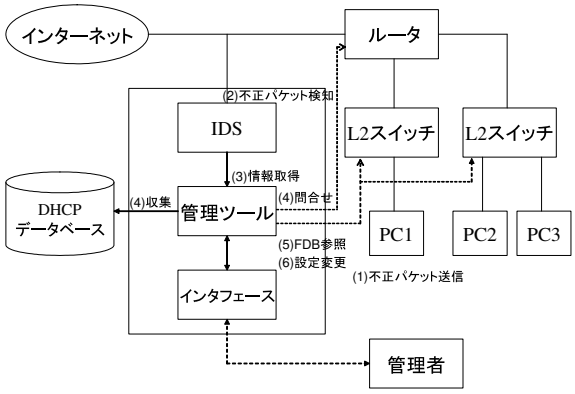

図 1: システム図

3. SNMP または Telnet を用いて FDB の設定が変更できる。

なお、本研究では Allied Telesis 社の CentreCOM GS908M [3] を使用している。

3 設計

3.1 機能

本システムに必要な機能を以下の 3 つに分割する。

- 情報の取得
  通信の遮断などの動作を行うには、IP アドレスから MAC アドレスに変換し、MAC アドレスをもとにホストが接続されているスイッチを特定し、スイッチのどのポートに接続されているか特定するという手順を踏む必要がある。この一連の動作を「情報の取得」と定義する。PHP から SNMP を実行し、それぞれのステップで取得した情報を分析し、結果として MAC アドレス、スイッチ、スイッチのポートの 3 つの項目を得る。
  この機能は、通信の遮断を行う際に必要となる 3 つの情報を取得し表示し、要求があれば「通信の遮断」へ情報を渡すものである。
- 通信の遮断
  MAC アドレスをもとに L2 スイッチの設定を

変更することで、不正パケットを送信したホストの通信を遮断する。SNMP と Telnet のどちらのインタフェースであっても設定変更できるようにする。

- 遮断の解除
  通信の遮断を行ったホストの接続を回復させる。

3.2 シナリオファイル

本研究では、レイヤ 2 スイッチとして CentreCOM GS908M を使用しているが、ネットワークの規模が大きくなると複数種類のレイヤ 2 スイッチが使われる場合がある。そこで、複数種類のレイヤ 2 スイッチに対応するためにシナリオファイルを用意する。シナリオファイルとは、スイッチ毎に本システムで必要な SNMP や、Telnet のコマンドをシナリオファイルとして記述しておき、あらかじめ用意しておいたスイッチリストからスイッチの種類を取得し、スイッチの種類に合ったシナリオファイルから必要なコマンドを自動的に選択するものである。

4 実装

本システムは PHP で記述しており、SNMP および Telnet を PHP から実行する必要がある。

PHP で SNMP を実行するために、バッククォート演算子を使用する。バッククォート演算子は、PHP スクリプトがアップロードされているサーバ上のコマンドを実行し、そのコマンドが標準出力に出力した文字列を得るものである。

PHP から Telnet を行うためには、Telnet の対話的入力に対応させなければならないので、双方向パイプを用いることにした。PHP にはそのための関数として proc_open() が用意されているのでこれを使用する。

proc_open() を利用すれば、PHP と Telnet で双方向にやり取りできるが、Telnet からの出力が完全に終わる前に出力を読み込んでしまうと、出力結果を完全に得られない事や、Telnet へ入力したコマンドの処理が終わらないうちに次のコマンドを入力してしまう事が起こり得る。

そこで、あらかじめ Telnet から出力される最後の文字列 (待機文字列) をシナリオファイルに記述しておき、その文字列が出力されるまで Telnet からの出力を読み込み続けることにする。これにより最小の待ち時間で出力結果を得ることができる。

4.1 情報の取得

まず、IP アドレスから MAC アドレスへ変換する。ここでは DHCP データベースに見立てたデータベースから MAC アドレスを取得する。次に SNMP を用いて L2 スイッチの FDB の内容を問い合わせる。そのために、L2 スイッチと IP アドレスを対応させたデータベースをあらかじめ用意しておき、このデータベースをもとに問い合わせる。この動作を目的の MAC アドレスが含まれる L2 スイッチが見つかるまで繰り返す。

ホストの接続されている L2 スイッチが判明したら、次はスイッチのどのポートに接続されているかを特定する。これも同様に SNMP を用いてスイッチに問い合わせる。

4.2 通信の遮断

通信の遮断は、情報の取得で得られた、MAC アドレス、スイッチ、ポートの 3 つの情報をもとに、L2 スイッチの MAC アドレスフィルタリング機能の設定を変更することで実現する。

ここでは、本研究で使用している CentreCOM GS908M の通信の遮断について考える。この L2 スイッチは、指定した MAC アドレスの通信のみ許可することができる。該当の L2 スイッチのポートのポートセキュリティを有効化し、フォワーディングデータベースから MAC アドレスを削除することで通信の遮断が行える。設定は Telnet を用いて行う。

また、通信の遮断を行った後、スイッチに問い合わせてもどの MAC アドレスの通信を遮断したのかわからないため、通信の遮断を行う際に、遮断データベースに情報を保存しておく。

4.3 遮断の解除

遮断の解除は、通信の遮断の際に登録したデータベースの内容をもとに、L2 スイッチの MAC アドレスフィルタリングの設定変更を行う。CentreCOM GS908M の場合、ここも Telnet を用いる必要がある。遮断を解除した後は、遮断データベースから遮断情報を削除する。

5 まとめ

本研究では、L2 スイッチを用いた不正パケット遮断システムについて設計、開発を行った。本システムに IP アドレスを入力することで、情報の取得、通信の遮断、遮断の解除の処理をそれぞれ自動的に行うことができる。今後の課題として、IDS からのアラートに対応することが挙げられる。

参考文献

[1] 長野一樹, “不正パケット遮断システムのユーザインタフェースに関する研究”, 香川大学大学院 工学研究科 修士論文, 2007.

[2] 緒方亮・鈴木暢・矢野ミチル, “マスタリング TCP/IP SNMP 編”, オーム社, 2005.

[3] “ CentreCOM GS908M”, http://www.allied-telesis.co.jp/products/list/switch/gs900m/catalog.html