1ZF-1

仮想マシンを活用した不正アクセス対策学習システム

福山　和生　　井口　信和
近畿大学理工学部情報学科

1.　序論

インターネットの普及に伴い，不正アクセスによる被害が多発している．対策方法の一つとしてファイアウォール(以下，FW)などの不正アクセス対策機器の導入が有効である．ところが警視庁による調査によると不正アクセス対策を実施し，システムの脆弱性を検証している組織は 4 分 1 以下となっている．[1)]その理由として，不正アクセス対策に必要な知識を有したエンジニアの不足や，外部委託するための予算がないといった問題が指摘されている．そのため，各組織は独自で不正アクセス対策の教育を実施しなければならない場合がある．しかし，エンジニアの教育に実環境を用いることは，現状のシステムに影響を及ぼすため危険である．

そこで，本研究では当研究室で開発してきた仮想マシンを活用した IP ネットワーク構築演習システム [2)]を基に，仮想的な FW を用いて不正アクセス対策の学習ができるシステム(以下，本システム)を開発した．本システムでは，仮想ネットワークを用いることで実環境に影響を与えず，安全に不正アクセス対策の学習ができる．これにより，各組織が独自にエンジニアの教育を実施できる．

2.　研究内容

本システムは，User Mode Linux を用いて作成した仮想マシンを,仮想的なネットワーク機器として動作させる．そして，ネットワーク機器同士を相互に接続することで，1 台の PC 上で実機を用いた場合と同様のネットワークの構築演習が可能となる．さらに，構築したネットワーク上で仮想的な FW を動作させることで，受信したパケットのフィルタリングやログの収集，フィルタリングのテストができる．以下に本システムの機能を示す．

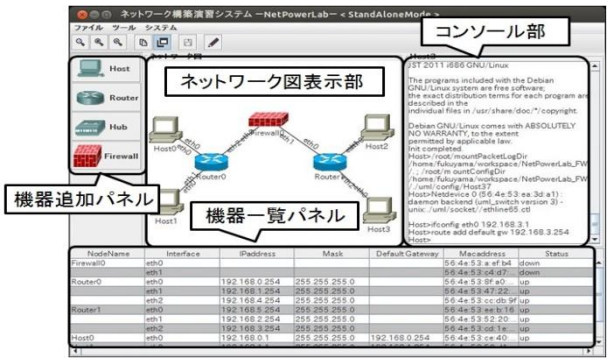


図 1：ネットワーク構築 GUI

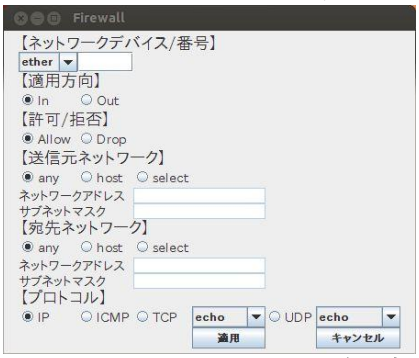


図 2：パケットフィルタリング設定 GUI

2.1　基本設定

学習者は，図 1 に示すネットワーク構築 GUI を用いて FW を含むネットワークを作成する．次に FW が他の機器と通信できるようにするため，各インターフェイスの IP アドレス，サブネットマスク，ルーティング方法を設定する．設定にはそれぞれ対応した GUI を用いる．また，ルーティング方法は，静的ルーティング，RIP，OSPF の 3 種類から選択する．

2.2　パケットフィルタリング機能

パケットフィルタリング機能では，FW にパケットのフィルタリング設定を実施する．フィルタリング方法には，静的フィルタリングと動的フィルタリングの 2 種類がある．

静的フィルタリングは，図 2 に示すパケットフィルタリング設定 GUI を用いてネットワークデバイス，パケットの通過する方向，送信元/宛先ネットワーク，プロトコルの情報を設定する．FW は，設定情報に基づいて，ネットワーク上のパケットをフィルタリングする．

Learning System for Countermeasure of Unauthorized Access utilizing Virtual Machine
Kazuki FUKUYAMA, Nobukazu IGUCHI
Department of Informatics, School of Science and Engineering Kinki University

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

動的フィルタリングは，フィルタリング条件としてネットワークを用いる．FW は外部ネットワークからのパケットを，内部ネットワークに対する応答以外フィルタリングする．例外として，静的フィルタリングと動的フィルタリングが同時に設定されている場合，静的フィルタリングの設定を優先して処理する．

また，設定したフィルタリング情報は図 3 に示すフィルタリング設定確認 GUI を用いて確認できる．

2.3 ログ収集機能

ログ収集機能では，FW が受信した全てのパケットのログを収集する．収集したログは図 4 に示すログ表示 GUI を用いて確認できる．このとき，パケットフィルタリング機能により破棄されたパケットは，赤色で強調して表示する．このログと設定情報を同時に確認することで，設定ごとのフィルタリング結果の変化を観察できる．

また，収集したログはパケットのヘッダ情報をプロトコルのフォーマットに合わせて表示できる．表示形式は簡易表示，詳細表示，16 進数表示の 3 種類がある．16 進数表示ではレイヤ別とフィールド別で色分け表示が可能である．

2.4 フィルタリングテスト機能

フィルタリングテスト機能では，図 5 に示すパケット生成 GUI を用いてパケットを自由に作成できる．パケットには，ネットワークデバイス，パケットの通過する方向，送信元/宛先ネットワーク，プロトコルの情報を設定する．また，作成するフレーム数や，送信間隔を指定できる．作成したパケットを FW に送信することでフィルタリングのテストを実施できる．



図 3：フィルタリング設定確認 GUI

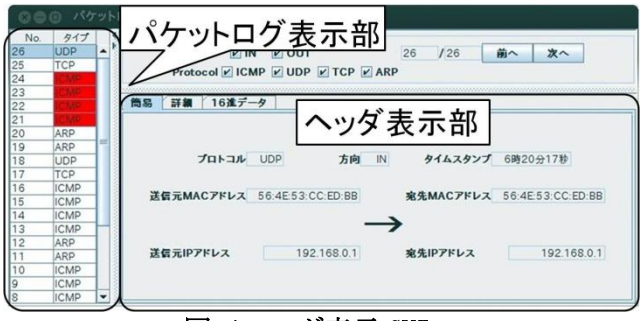


図 4：ログ表示 GUI



図 5：パケット生成 GUI

3. 結果考察

本システムの動作検証として，ネットワーク構築 GUI で FW を含むネットワークを構築した．パケットフィルタリング機能を検証するため，フィルタリングテスト機能を用いた．検証項目には，ネットワークデバイス，パケットの通過する方向，送信元/宛先ネットワーク，プロトコルの情報を使用した．これらの情報ごとに FW を通過するべきパケットと破棄されるパケットをそれぞれ複数作成し FW に送信した．パケットの到達性を確認した結果，全て正しく通信できていることが分かった．さらに，FW が受信したパケットのログを表示した際，フィルタリングにより破棄されたパケットが赤色で強調されていることを確認した．以上より，本システムは期待した動作をしていることが分かった．

4. 結論

本研究では，不正アクセス対策の学習ができるシステムを開発した．本システムは仮想ネットワーク上でパケットのフィルタリングやログの収集，フィルタリングのテストを実施することで不正アクセス対策の学習ができる．これを用いることで，組織が独自にエンジニアの教育を実施できる．

今後はパケットフィルタリング以外の不正アクセス対策を学習するために，プロキシサーバを利用した通信を可能とする，アプリケーションゲートウェイ型の FW の導入を予定している．これにより，パケットのヘッダ部だけでなく，データ部も含めたフィルタリングが可能になるため，より汎用性の高い不正アクセス対策学習が可能となる．さらに，本システムで設定した FW の情報を実際の FW に反映することで，容易に実環境に導入できるようにする．

参考文献

1) 平成 24 年度不正アクセス行為対策等の実態調査：http://www.npa.go.jp/cyber/research/index.html
2) 井口信和，“仮想ルータを活用したネットワーク構築演習支援システムの開発”，情報処理学会論文誌，Vol52, No3, pp.1412-1413, Mar.2011.

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.