L-008

統合脆弱性検査システムの提案

Proposal of integrated vulnerability inspection system

山口　聖大†　　佐藤 直†
Masahiro Yamaguchi　Naoshi Sato

１．まえがき

近年，多くのソフトウェアを活用した大規模情報システムが構築されることが多くなり，その構成は複雑化している．また，扱う情報の重要性も増したことにより，システムに対するセキュリティ強度の確保は必須のものとなってきている．

一方，ソフトウェアにはバグが存在し，それがシステムの脆弱性となる．攻撃者にこれらの脆弱性を攻撃される前に発見するには，構築したシステムに対して，定期的に脆弱性検査を実施していくことが重要である．

通常，検査には専用の脆弱性検査ツールが使用される．手動での検査では手間と時間が掛かるため，自動化が可能な部分はできる限り検査ツールを使用し，効率的に脆弱性検査を行うことは重要なことである．

しかし，これらの検査ツールを使った脆弱性検査には下記のような問題がある．(図 1 参照)

- １つの検査項目に対して，数多くの検査ツールが存在し，検査者はその中から有効なツールを選択しなければならない[1].
- 検査ツール毎の使用方法(入力値・オプション等)を修得しなければならない.
- 特定の OS 上でしか動作しない検査ツールがあり，端末(画面)を切り替えて操作することが煩雑である.

そこで，上記の問題点を解決するために，多くの脆弱性検査ツールを共通のインターフェースから使用可能にする統合脆弱性検査システム(図 2 参照)の構築を本研究の目的とする．本稿ではこの統合脆弱性検査システムの構成法を検討し，課題について考察した.

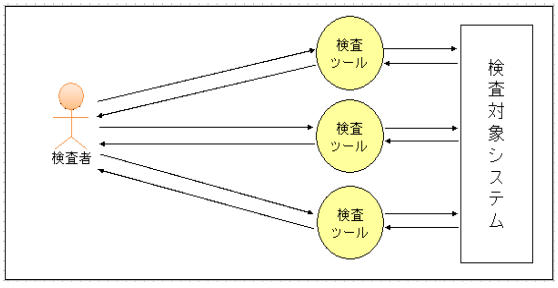

図 1. 従来の検査ツール使用方法

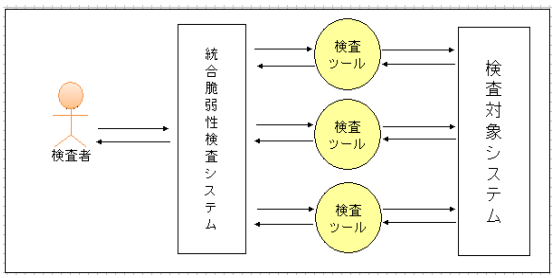

図 2. 提案システムを介した検査ツール使用方法

†情報セキュリティ大学院大学，Institute of Information Security

２．既存の脆弱性検査の問題点

２．１ 脆弱性検査の定義

一般的に脆弱性検査というと，ソースのレビューやユーザの運用等広い範囲で定義される場合があるが，ここではネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか，実際に攻撃者が用いる攻撃手法を試しながら安全性の検証を行うことを指す．また，脆弱性の洗い出しは行うが，その対策は対象外とする.

２．２ 検査ツールとは

脆弱性の検査ツールは有償・無償の物を含めて，１つの検査項目に対して複数の検査ツールが存在する．これらの検査ツールは BackTrack[2]や Whoppix[3]のような脆弱性検査用の Linux ディストリビューションを活用することで導入までの手間を省くことができる．また，検査ツールは異なる OS(Windows・Linux 等)に対してそれぞれ提供されている場合もあれば，特定の OS にのみ提供されている場合もある.

表 1. 検査ツールの例[4]

検査項目	ツール名
ポートスキャナ	nmap
CGI スキャナ	Nikto
セキュリティスキャナ	Nessus

２．３ 問題点

検査ツールを使用した脆弱性検査には以下の問題がある.

（１）検査ツールを選択する手間

脆弱性検査の実施者は，数百以上のツールの中から自分が実施したい検査項目に適切なツールを１つ又は複数選択することが必要となる．また，新たに検査ツールが開発された場合は，これまで使用していたツールとどちらが優れているかを判断する必要がある.

（２）検査ツールの使用法把握

検査者は多くの検査ツールの使用法を把握する必要がある．また，新たな検査ツールが開発された場合は，そのツールの使用法も習得しなければならない.

（３）動作 OS が異なる検査ツールの使用

検査ツールは特定の OS 上でのみ動作するものが存在するため，そのツールを使用して検査を実施する場合は，操作する端末を切替える必要がある．また，OS の使用法自体も合わせて修得する必要がある.

３． 統合脆弱性検査システム

３．１ 想定する利用者

＜システム利用者＞
- 脆弱性検査を実施する．
- 脆弱性検査に関する一定以上の知識を有する．
- 統合脆弱性検査システムの知識を有しない．
- システム管理者が定めた検査項目に従い検査を実施する．

＜システム管理者＞
- 統合脆弱性検査システムの管理を行う．
- 検査項目に対してどの検査ツールを用いるか，又どのオプションで使用するか等を決定する．
- 脆弱性検査だけでなく，統合脆弱性検査システムに関する知識も有する．

＜アダプタ開発者＞
- 統合脆弱性検査システムから検査ツールを実行する際に使用するプラグイン方式の検査ツールアダプタを開発し提供する．

３．２ システム構成要素

＜検査端末＞
- システム利用者が脆弱性検査時に操作する端末．
- 検査サーバに脆弱性検査内容を指示し，その結果を画面上に表示する．

＜検査サーバ＞
- 脆弱性検査ツールがインストールされているサーバ．
- 検査端末からの指示を元に対象サーバに脆弱性検査を実施し，その結果を検査端末に転送する．

＜対象サーバ＞
- 脆弱性検査の対象となるサーバ．

３．３ システム構成

本提案システムの構成を図 3 に示す．本提案システムは複数の OS 上で動作する検査ツールを使用するため，検査端末と検査サーバは別に用意した．検査端末で操作するアプリケーションはユーザの操作性を考慮して，クライアントサーバ型とした．クライアント-サーバ間は分散処理技術として広く普及している SOAP で実装した．検査サーバが検査端末からコマンド情報を受け付けるためのサーバソフトは Tomcat とした．開発言語は検査サーバ側のアプリケーションは多くの OS 上で動作する様に Java で，検査端末側のアプリケーションはユーザの操作性と開発効率を考慮して VB で実装した．また，統合脆弱性検査システムから直接検査ツールを使用して行うではなく，プラグイン方式で導入可能な，検査ツールアダプタを介して検査ツールを実行する仕組みとした．こうすることで統合脆弱性検査システムが検査ツールの細かい入出力値を把握する必要がない．この構成により，使用する検査ツールが増えた場合でもシステム改修の必要性が無くなるため，システムの拡張性が向上する．

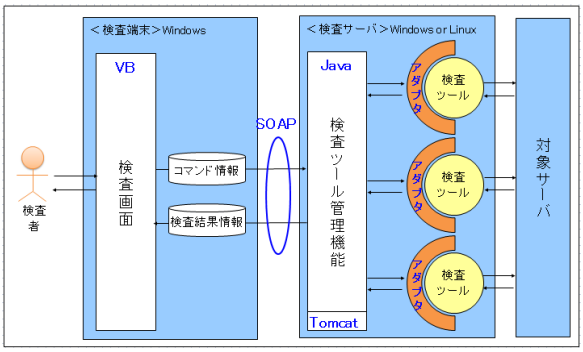

図 3. 統合脆弱性検査システムの構成

３．４ 検査ツール実行の流れ

（１）システム管理者がコマンド情報をシステムに登録する．必要に応じて検査サーバに検査ツール・検査ツールアダプタをインストールする．

（２）システム利用者が操作端末から対象サーバに対して，実施したい検査項目(ポートスキャン・Web 検査等)を選択する．

（３）システム利用者が選択した検査項目を元に検査端末から検査サーバに対して，コマンド情報を送信する．

（４）検査サーバはコマンド情報を解析し，その情報を元に検査ツールを実行する．

（５）検査サーバは検査ツールが出力した情報を元に検査結果情報を作成し，検査端末に送信する．

（６）検査端末は検査サーバから受信した検査結果情報を元に操作画面に検査結果を出力する．

４． 考察

今回構築した統合脆弱性検査システムでは，システム利用者が検査端末の検査画面から実施した検査項目を選ぶ操作だけで，異なる OS 上に存在する複数の検査ツールを同一のインターフェースから実行することができた．これにより，「検査ツールを選択する手間」，「検査ツールの使用法把握」，「動作 OS が異なる検査ツールの使用」といった検査ツール使用における問題点を解決できた．

しかし，本提案システムを構築・検証する中で，操作性と検査ツールの自由度の両立が課題として挙がった．システム利用者にツールの細かい操作(入力値・オプション)を意識させないことで操作は簡単になるが，オプション等で細かい調整を行いたい場合への対応も必要となることが分かった．上記を含めたユーザインタフェースは提案システムを効率良く利用する上で重要な要素であるため，今後更に検討を進めていく．

＜参考文献＞

[1]技術評論社，“ネットワークセキュリティ Expert7 ペネトレーションテスト手法”pp.12-17(2008)

[2]「Backtrack」<http://www.backtrack-linux.org/>（2011/07/3 アクセス）

[3]「Whoppix」< http://www.whoppix.net/>（2011/07/3 アクセス）

[4] 古川泰弘，吉成大知，“ペネトレーションテスト入門” pp.231-243，ソフトバンククリエイティブ(2006)