

# スキヤナ調査

2002.11

# はじめに

スキャナ製品は様々なものがあるが、これらを機能により次のように分類した。

1. ネットワーク型
2. ホスト型
3. パスワードクラック
4. ポートスキャン
5. ウィルススキャン
6. その他

# 1. ネットワーク型

調査対象以外のホストにインストールする。

開発元独自の脆弱性データベースに基づき、ルータやファイアウォールなどのネットワーク機器やWebサーバ、メールサーバ、その他ネットワーク全体に対して、ネットワーク越しにスキャンを実施し脆弱性の有無を調査する。

脆弱性データベースは、各ハードウェアやソフトウェアについて既知の脆弱性を網羅したものである。新たな脆弱性は日々報告されているため、データベースは常に最新の状態に更新することが重要である。それとともに、未知の脆弱性については検知できず、脆弱性の調査には限界があることも留意しなくてはならない。

多くはレポート機能を有し、html形式の出力ができる。  
専用のハードウェアを用いるもの(アプライアンス型)もある。  
擬似的にDoS攻撃を行い、耐性を調査するものもある。

## 2. ホスト型

調査対象のホストにインストールする。

開発元独自の脆弱性データベースに基づき、ローカルマシン内部からスキャンを実施し脆弱性の有無を調査する。これにより設定ファイルなど詳細部分の検査が可能となる。

脆弱性データベースはネットワーク型と一部共通であるが、それに加え、ファイルのパーミッションや所有権、OSのコンフィグレーションなど、ポリシーに関する検査項目も含んでいる。また、バックドアの有無、侵入者の痕跡なども含んでいる。

脆弱性データベースは、各ハードウェアやソフトウェアについて既知の脆弱性を網羅したものである。新たな脆弱性は日々報告されているため、データベースは常に最新の状態に更新することが重要である。それとともに、未知の脆弱性については検知できず、脆弱性の調査には限界があることも留意しなくてはならない。

多くはレポート機能を有し、html形式の出力ができる。

### 3. パスワードクラック

パスワードクラックは、パスワードの脆弱性を調査するツールである。パスワードを次から次に試行し、推測されやすいものを使用していないかを調査する。

パスワードの試行方法により、総当り型、辞書型、ハイブリッド型がある。総当り型は、正しいパスワードが判明するまで、あらゆる文字を組み合わせたパスワードを生成し、試行する。

辞書型は、あらかじめ用意した辞書にある単語をパスワードに用いる。

ハイブリッド型は、まず辞書型でパスワードを生成し、パスワードが判明しない場合に総当り型を実行する。

また、オフラインで行う方法とオンラインで行う方法がある。

オフラインで行う場合、ローカルのパスワードファイル(/etc/passwd、/etc/shadowなど)に対してパスワードを試行する。

オンラインで行う方法に対しては、認証失敗回数制限などの設定により、防御が可能な場合もある。

## 4 . ポートスキャン

T C PやU D Pポートの空き状況を調査する。

ツールのインストール先に関わらず、任意のネットワークに対して、あるいは特定のマシンに対して調査が可能。

また、ネットワーク上のホストのIPアドレスやOSの種類などを把握することもできる。

## 5 . ウィルススキャン

ゲートウェイ型とホスト型に分かれる。

ゲートウェイ型は調査対象ネットワークのゲートウェイ(メールサーバやプロキシサーバ)にインストールし、通過するファイルにウィルスが潜んでいないか調査する。

ホスト型は調査対象ホストにインストールし、ローカルマシンにウィルスが潜んでいないかを調査する。一般的なアンチウィルスソフトは、ホスト型である。

開発元独自のウィルス情報データベース(パターンファイル)に基づき調査を行い、パターンファイルと適合した場合を感染と判断する。

ウィルス情報データベースは、既に報告されたウィルス情報を網羅したものである。新種のウィルスが日々発見されているため、常にデータベースを更新し最新の状態に保つことが重要である。それとともに、未知のウィルスについては検知できず、ウィルスの検知に限界があることも留意しなくてはならない。

## 6. その他

次の機能を持ったツールがある。

- ◆ 無線LAN …… アクセスポイントを検出し、暗号化や認証などの脆弱性を調査
- ◆ インターフェイススキャン …… プロミスキャスモードのホストを検出
- ◆ オープンポートスキャン …… オープンポートと使用しているファイルなどを調査
- ◆ ファイルアクセス権の調査 …… ファイル属性の脆弱性を調査
- ◆ OSスキャナー …… リモートホストのOSを特定
- ◆ FTPサーバスキャン …… ネットワーク内のFTPサーバを探索
- ◆ SMTPリレースキャン …… SMTPサーバを探し、不正中継が可能か調査
- ◆ アクセスリストスキャン …… ルータなどを対象にし、アクセスリスト設定状況を調査
- ◆ CGIスキャン …… CGIのセキュリティホールを調査
- ◆ リプライパケットチェック …… ファイアウォールの動作確認
- ◆ スパイウェア駆除 …… ローカルディスクのスパイウェアを発見し、駆除
- ◆ 共有ファイルスキャン …… 共有ファイルを検出
- ◆ ソースコードスキャン …… Cのソースからセキュリティホールを調査