Nessusによる脆弱性スキャンの実施と運用について

情報政策課　技術専門職員　金森　浩治

１．はじめに

富山大学では2014年からNessusによる脆弱性検査を実施している。本稿ではその実施と運用について述べる。

2. Nessusとは

Nessusとは，ネットワーク経由でターゲットホストの脆弱性，設定，マルウエアプロセスを含む様々な情報を収集しシステムの脆弱性をスキャンするソフトウェアである。Windows, Linux, Macなど様々なプラットフォームに対応しており，スキャンできる対象も様々なOS､ネットワーク機器、仮想環境プラットフォーム、データベースWebアプリケーション、クラウドサービス，モバイルデバイスなど幅広く対応している。[1]

なおNessusではXSSやSQLインジェクションといったアプリケーション層に起因する脆弱性を検出することはできない。

3. 運用について

Nessusによる脆弱性スキャンは2014年度から年一回ペースで計3回行っている。脆弱性対応まで含めた運用は以下の通りである。

1. Nessusによる脆弱性スキャンの実施
2. 検査結果の解析および分析
3. 検査結果通知書の作成
4. 各機器管理者への通知および回収

3.1　Nessusによる脆弱性スキャンの実施

脆弱性スキャンはファイヤーウォール内から学内LAN全てのIPアドレスを対象に行っている。

実施初年度は，主にサーバーをターゲットとするため土日に脆弱性スキャンを行っていたが，2年目からはクライアントもターゲットとするため平日に行うようにした。そのため2年目から検査実施中に「Symantecのアンチウィルスソフトが不正アクセスを検知した」といった問い合わせがくるようになっている。

3.2　スキャン結果の解析および分析

脆弱性スキャン結果は約 10 万レコードにおよぶ。この結果すべてを機器管理者に通知した場合，問い合わせが殺到し混乱することが想定される。そのため機器管理者に通知する脆弱性の選定作業を毎年行っている。

選定作業を行うにあたって 10 万レコードにおよぶデータを分析する必要がある。このデータを効率よく解析および分析するため，RDB(MySQL)に取り込み，脆弱性の内容と危険度，台数，機器管理者人数を集計し，機器管理者に通知する脆弱性内容を選定している。

過去 3 回で通知した脆弱性の内容は，大まかに分けて，「OSおよびミドルウェアの旧バージョン使用に起因する脆弱性」，「共有フォルダーの不適切なアクセス設定」，「デフォルトパスワードの使用」，といったものである。なお，「OSおよびミドルウェアの旧バージョン使用に起因する脆弱性」が通知数の大半を占めている。

3.3　検査結果通知書の作成

機器管理者へ脆弱性スキャン結果を通知するために機器管理者ごとに「検査結果通知書」というものを作成している。(図 1 参照)

作成するにあたり使用しているツールは OSS の ETL「Pentaho Kettle」と，OSS の帳票作成ツール”「Pentaho Report」である。

Nessus からのスキャン結果の原文をそのまま記載しているが，対策方法のみ日本語訳をつけている。

なお CVE(共通脆弱性識別子)については 2016 年度より記載している。機器管理者がメーカーにNASの脆弱性対応方法を伺ったところCVEを求

められた、という経緯があったためである。

3.4　各機器管理者への通知および回収

検査結果通知書と脆弱性対応報告書，脆弱性対応報告書記入例を同封し学内便で送付，脆弱性対応報告書を機器管理者が記入し学内便で返送してもらっている。紙媒体で通知を行う理由は，情報が漏洩したときのリスクを考慮したためである。

脆弱性対応報告書の内容が見当違いであれば、対応者にその旨を連絡し，再度提出していただいている。

なお機器管理者からの問い合わせは電話のみにしている。対象端末の種類，OS，バージョン，管理状況，使用状況，管理者の技術レベル等を把握し，その状況に応じたアドバイスが求められるためである。

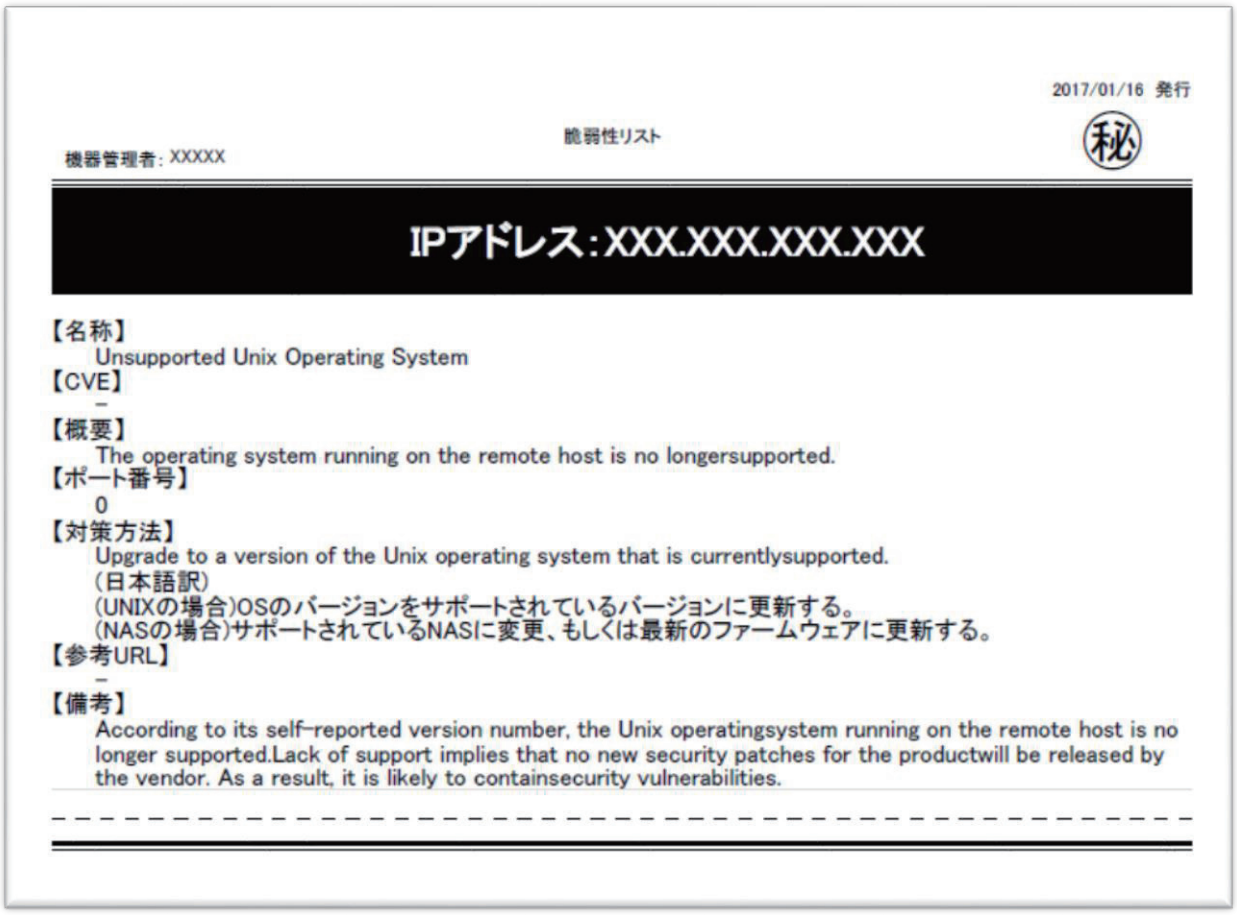
4. 最後に

Nessus で脆弱性検査を行うことは有用であるが、検査できるのは大学全体の脆弱性のごく一部である。

Nessus の脆弱性検査でカバーできない部分をいかに対応していくのかが今後重要となると思われる。

参考文献

[1] 脆弱性スキャナー Nessus 利用ガイド初級編（ http://www.slideshare.net/RyuichiTomita/nessus-start-guidejprev1 ）



2017/01/16 発行

脆弱性リスト

秘

機器管理者：XXXXX

IPアドレス：XXX.XXX.XXX.XXX

【名称】
Unsupported Unix Operating System
【CVE】
-
【概要】
The operating system running on the remote host is no longersupported.
【ポート番号】
0
【対策方法】
Upgrade to a version of the Unix operating system that is currentlysupported.
(日本語訳)
(UNIXの場合)OSのバージョンをサポートされているバージョンに更新する。
(NASの場合)サポートされているNASに変更、もしくは最新のファームウェアに更新する。
【参考URL】
-
【備考】
According to its self-reported version number, the Unix operatingsystem running on the remote host is no longer supported.Lack of support implies that no new security patches for the productwill be released by the vendor. As a result, it is likely to containsecurity vulnerabilities.

図 1　　検査結果通知書