学外公開ホストの脆弱性解消に関する取組み

打矢 隆弘 [1)], 梶岡 慎輔 [1)], 松井 俊浩 [1)], 齋藤 彰一 [1)], 内匠 逸 [1)], 松尾 啓志 [1)]

1) 名古屋工業大学 情報基盤センター

t-uchiya@nitech.ac.jp

Approach of removing vulnerabilities of in-campus public servers

Takahiro Uchiya [1)], Shinsuke Kajioka [1)], Toshihiro Matsui [1)],
Shoichi Saito [1)], Takumi Ichi [1)], Hiroshi Matsuo [1)]

1) Information Technology Center, Nagoya Institute of Technology

概要

大学がインターネットに公開している各種サーバ群のセキュリティ対策の一環として、サーバの脆弱性を調査することは非常に有効である。名古屋工業大学では、学内すべての“学外公開ホスト”を対象として、2016 年 5 月に脆弱性検知スキャナ Nessus を用いて脆弱性調査を実施した。調査の結果、29 台のホストから脆弱性を検出し、2 カ月以内にすべての脆弱性を解消する対策を実施した。本稿では、脆弱性調査に至った経緯と、本学の脆弱性調査スキーム、及び、発見された脆弱性の種類と有効な対策を報告する。

1 はじめに

大学がインターネットに公開している各種サーバ群のセキュリティ対策の一環として、サーバの脆弱性を調査することは非常に有効である。名古屋工業大学では、新たに脆弱性調査スキームを導入し、学内すべての「学外公開ホスト」を対象として、2016 年 5 月に脆弱性検知スキャナ Nessus を用いて脆弱性調査を実施した。調査の結果、学外公開ホスト 148 台のうち 29 台のホストから脆弱性を検出し、2 カ月以内にすべての脆弱性を解消する対策を実施した。本稿では、脆弱性調査に至った経緯と、本学の脆弱性調査スキーム、及び、発見された脆弱性の種類と有効な対策を報告する。

2 名古屋工業大学のホスト管理ポリシ

2.1 管理ポリシ 1:学外から学内への通信不可

本学では、学内で利用される端末に対してグローバル IP を付与する。グローバル IP の付与された端末は学外から攻撃を受ける可能性があるため、セキュリティ対策が必須である。

この対策として、本学では学外から学内の全てのホストに対する通信の可否を UTM(統合脅威管理装置)において管理している。UTM のファイアウォールポリシにおいて、

学外→学内　全通信　不可

とし、学外からのサイバー攻撃を防御している。

2.2 管理ポリシ 2:学外から“学外公開ホスト”への通信可

学内で利用される端末には、研究活動の周知を目的として学外に公開したい Web サーバや、共同研究先からのアクセスを可能とする SSH サーバ等が存在する。これらの端末への通信を可とするため、学外向け端末を“学外公開ホスト”と定義し、学外公開ホストの利用の際はサブネット管理者が基盤センターへ申請を行う形式を採用した。UTM へは、申請ベースで下記のポリシが追加される。

学外→学外公開ホスト　利用ポート　通信可

申請者は図 1 の申請書にホスト情報を記入し、電子ワークフローを用いて申請する。

学外公開ホストは、「サーバ」クラスと「カスタム」クラスの 2 種類が存在する。

「サーバ」クラスでは、サーバの利用用途に応じてウェブ用／メール用／SSH 用が選択できる。

「カスタム」クラスでは、学外に公開を希望するサービスのサービス名とポート番号を記入し、基盤センターと協議の上、学外公開の可否を決定する。

2016 年 5 月時点で、学外公開ホストは 66 人の利用者がおり、148 台利用されていた。内訳は、Web 用途 96、メール用途 9、SSH 用途 17、カスタム用途 26 である。各ホストの管理者は、定期的にホストのセキュリティ対策を実施する。

申請ID

MAINS学外公開ホストの登録情報変更申請書

申請日 平成 28年 9月 26日

申請者 → 情報基盤センター長 → 情報基盤センター担当者

1．申請に際しての留意事項

Webサーバーやsshサーバーなどを学外に公開する場合は**最々のホスト毎に本申請が必要**です。下記事項を理解された上でご申請ください。

- 本学の**グローバルIPアドレス（133.68.x.x）が割り当てられたホストのみが申請の対象**となります（MAINSデータベースで**事前にホストを名台で登録**しておく必要があります）。
- 一般的なWebサイトの学外公開については、情報基盤センター提供の**Webサイトホスティングサービス**が大変便利です（その場合、**本申請は不要**です）。是非ご利用ください。
- 学外から学内ホストへのリモートアクセス（SSHやRDPなど）は**VPNを経由することが前提**です。従ってリモートアクセス用ホストの学外公開は**最小限、かつ必要不可欠な場合のみ**としてください。また、SSHサーバーを学外公開する場合は、よく知られたアカウント（rootやmysqlなど）に**安易なパスワードを付けない**ようにしてください。
- MAINSの運用と干渉するような特殊なサービスの公開は、ご希望に添えない場合があります。

2．申請者

氏名	打矢　隆弘	所属	しくみ領域	内線	7139
職名	准教授	E-mail	egz71773@ict.nitech.ac.jp		

3．MAINSデータベース登録情報

管理責任者		端末種別	○ 計算機 ○ その他（ネットワーク機器）
ホスト名		サブネット名	
機種名		IPアドレス	
OS		CNAME	
備考			

4．希望変更内容

以下よりご希望の項目を選択してください。

変更内容	学外公開サービス（ポート）
○「サーバー」用（複数選択可）	☐ウェブ用 HTTP（TCP：80）・HTTPS（TCP：443） ☐メール用 POP3（TCP：995）・IMAPS（TCP：993）・SMTPS（TCP：465／587［STARTTLS］） ☐SSH用 SSH（TCP：22） 外部からのクラッキングの大部分はSSHを使っています。MAINSへの外部からの接続はVPN（すべてのOSで標準でサポートされています）の利用を強くお勧めします。どうしてもSSHの利用を希望する場合は、 (1)強いパスワードの利用 (2)共通鍵SSHの利用 をお願いします。
○「カスタム」クラスに変更（情報基盤センターと別途協議を希望）	学外に公開を希望するサービスの名とポート種別・番号の一覧を以下にご記入ください。 ※記入例：telnet（TCP：23）
○「標準」状態に戻す	なし

5．利用規約

- 申請者は、変更申請ホストの運用管理等全般について責任を負うこと。

上記利用規約に同意する場合は「申請」ボタンを、同意できない場合は「キャンセル」ボタンをクリックしてください。

申請　キャンセル

図 1：学外公開ホストの利用申請書

2.3 ホスト管理の課題

学外公開ホストの管理はホスト管理者に一任されている。学内全てのホスト管理者が随時適切なセキュリティ対策を実施している場合、既知の脆弱性は解消済となるため、適切な運用となり得る。

しかし、OS／ソフトウェアの更新やセキュリティパッチの適用などのセキュリティ対策は作業コストが発生するため、即座に対策作業が実施されない状況も発生しうる。また、セキュリティに関する専門知識を有していない管理者にとって、ホストが脆弱性を有しているかの判定を行うことや、脆弱性を解消するためにどのセキュリティ対策を採用するかを決定することは難しい。

上記の課題を解決するため、本稿では“脆弱性検知スキャナ”を利用した、定期的な脆弱性チェック手法を提案する。

3 脆弱性検知スキャナ Nessus

3.1 概要

脆弱性検知スキャナとして、Tenable Network Security 社が提供する Nessus Vulnerability Scanner (Nessus Professional)有償版[1]を利用した。利用者は Web ブラウザを用いて操作を行う。

3.2 スキャン項目

Nessus では、ネットワークを介した基本スキャン、Web アプリーケーションの脆弱性スキャン、ハートブリード検出、ホスト検出／ポートスキャンなど複数の脆弱性チェックが可能であるが、今回はネットワークを介した基本スキャンに相当する“Basic Network Scan”の項目を指定し、脆弱性スキャンを実施した。

3.3 機能

Nessus は、“検出”と“対策の提示”の 2 つの機能を有している。

“検出”では、指定したホストに対してセキュリティに関する既知の脆弱性を調査し、脆弱性を検出する。検出した脆弱性はレポートとして Nessus 利用者に提供される。レポートには脆弱性の内容と、脆弱性のレベル(Critical, High, Medium, Low, Info)、脆弱性を解消するための対策が提示される。今回は、脆弱性のレベル(Critical, High)の 2 つを緊急に対応すべき重要な脆弱性と定義し、これらのレベルの脆弱性を解消することとした。

“対策の提示”では、OS のバージョンアップや、ソフトウェアの最新バージョンへのアップデートなど、その脆弱性を解消するために適切な対策方法が具体的に示される。これを学外公開ホストの管理者に提供することで、脆弱性解消につながる最良の対策を実施することが可能となる。

4 脆弱性解消スキームの導入

4.1 概要

学外に公開しているホスト群のセキュリティの向上を目的として、脆弱性検知スキャナを用いた脆弱性解消スキームを導入する（図２）。
センター担当者の端末に脆弱性スキャナをインストールし、当該端末からネットワークを介し学外公開ホストの脆弱性調査を実施する。重要な脆弱性を発見した場合にホスト管理者に脆弱性の内容と対応策を提示し、管理者が対応を実施する。

4.2 処理の流れ

図２を用いて、処理の流れを説明する。

1.脆弱性調査

脆弱性検知スキャナを用いて学外公開ホストの脆弱性を調査する。Nessus では、同時に全台の学外公開ホストの脆弱性調査が可能である。

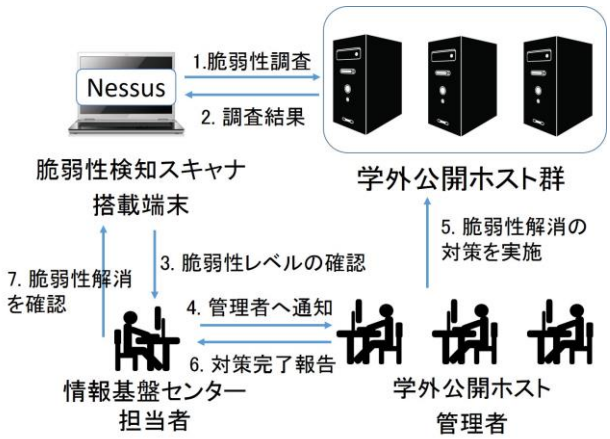

図２：脆弱性解消スキーム

2.調査結果の表示

Web 画面に脆弱性調査の結果が表示される。

ホストごとに、脆弱性のレベル(Critical, High, Medium, Low, Info)別の脆弱性の数が表示される。

3.脆弱性レベルの確認

センター担当者は、Web 画面を用いて、各ホストに重要な脆弱性(Critical, High)が存在しているかどうか確認する。

Nessus が提供する脆弱性のレポートの内容も確認する。

4.脆弱性発見の通知

脆弱性が検出された旨を学外公開ホスト管理者に通知する。報告レポートを送付し、一定期限までに脆弱性解消の対応を行うよう依頼する。

5.脆弱性解消処理の実施

学外公開ホスト管理者は自身の管理しているホストの脆弱性を解消するための対策を速やかに行う。

6.対策完了報告の通知

管理者は、管理ホストの脆弱性を解消する対策を実施したことを担当者に通知する。

7.脆弱性解消を確認

センター担当者は、管理者からの対策完了報告に基づき、脆弱性が解消されたかどうかを脆弱性検知スキャナを用いて確認する。

5 第１回脆弱性調査の実施

5.1 概要

前述の脆弱性解消スキームを適用して、2016 年 5 月に第 1 回脆弱性調査を実施した。学外公開ホストの管理者には脆弱性調査の趣旨と実施時期を事前に伝えた。

5.2 脆弱性の有無

148 台の学外公開ホストの脆弱性を調査した結果、29 台のホストから脆弱性が検出された。

5.3 脆弱性レベル

検出された脆弱性の脆弱性レベル別の件数を以下に示す。

Critical：33 件、High：75 件

5.4 脆弱性が発見されたホストの対応

脆弱性が検出されたホストの管理者は、脆弱性報告レポートを利用して対策を行う。即座の対策が難しい場合は、ホストの学外公開を停止することになる。今回は 29 台のホストのうち、24 台が対策・継続利用を希望し、5 台が公開停止を希望した。

5.5 脆弱性の分析

脆弱性レベル：Critical の 33 件について、脆弱性の種類と件数を表 1 に示す。

表１：脆弱性の種類

種類	脆弱性名	件数
PHP 脆弱性	PHP Multiple Vulnerabilities	12
Linux OS サポート切れ	Unsupported Unix Operating System	9
OpenSSL 脆弱性	OpenSSL Multiple Vulnerabilities	3
PHP サポート切れ	PHP Unsupported Version Detection	2
Apache 脆弱性	Apache Multiple Vulnerabilities	2
SSH 脆弱性	SunSSH CBC Plaintext Disclosure	2
telnetd 脆弱性	FreeBSD 'telnetd' Daemon Remote Buffer Overflow	1
OpenSSL サポート切れ	OpenSSL Unsupported	1
rexecd 利用	rexecd Service Detection	1

サポート終了となった OS やソフトウェアの利用が検出されていることがわかる。また、古いバージョンのソフトウェアの利用も検出されている。SSH, telnetd などソフトウェア個別の脆弱性についても検出されている。本学では特に Linux OS 関

連のセキュリティアップデートが不十分なホストが複数存在していることが明らかになった。

5.6 脆弱性解消に有効な対策

脆弱性検知スキャナが出力するレポートには脆弱性名、脆弱性の説明、適切な対策方法が含まれている。ここでは、脆弱性レベル：Critical として検出された 9 種類の脆弱性について、それぞれの適切な対策方法を下記に示す。学外公開ホスト管理者はこの対策方法を参考にして、脆弱性を解消するための対策を施すことができた。

PHP 脆弱性　(PHP Multiple Vulnerabilities)

・対策方法

Upgrade to PHP version 5.6.17 or later.

Linux OS サポート切れ (Unsupported Unix Operating System)

・対策方法

Upgrade to a more recent version that is currently supported.

OpenSSL 脆弱性 (OpenSSL Multiple Vulnerabilities)

・対策方法

Upgrade to OpenSSL version 1.0.1o or later.

PHP サポート切れ (PHP Unsupported Version Detection)

・対策方法

Upgrade to a version of PHP that is currently supported.

Apache 脆弱性 (Apache Multiple Vulnerabilities)

・対策方法

Upgrade to Apache version 2.2.15 or later.

SSH 脆弱性 (SunSSH CBC Plaintext Disclosure)

・対策方法

Upgrade to SunSSH 1.1.1 / 1.3 or later.

telnetd 脆弱性 (FreeBSD 'telnetd' Daemon Remote Buffer Overflow)

・対策方法

Upgrade to the version specified in the vendor's advisory.

OpenSSL サポート切れ (OpenSSL Unsupported)

・対策方法

Upgrade to a version of OpenSSL that is currently supported.

rexecd 利用 (rexecd Service Detection)

・対策方法

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

6 議論

大学における学外公開ホストの脆弱性解消につながる重要なポイントについて議論する。

・脆弱性検知スキャナ Nessus の採用

今回利用した Nessus はセキュリティ分野における検知スキャナとして認知度が高く、信頼性に対する評価も高い製品である。Web ブラウザを用いた操作も容易で、複数端末の同時調査も可能であったため、100 台を超える学外公開ホストの脆弱性調査に適していた。また、脆弱性の検知も適切であり、調査結果のレポートも有効であることから、スキャナとして非常に有効であると考える。

・脆弱性レベルの活用

第 1 回の脆弱性調査では、脆弱性レベルをホストの危険度とみなし、Critical, High を対象として脆弱性解消の対策を実施した。定期的な脆弱性調査の際には、レベル Medium, Low についても考慮する必要がある。Nessus のレポート内容を確認した上で、重要な脆弱性については対策を実施することが望ましい。

・脆弱性定期調査の方式

Nessus にはスキャンのスケジューリング機能が備わっている。同機能を利用して、月に一度などの定期スキャンを実施することが望ましい。

・脆弱性解消までの期間短縮

脆弱性解消に OS のインストールを伴う作業が必要な場合、即座の作業時間が確保できず解消まで時間がかかる場合があった。ホスト管理者に円滑に対策作業をしてもらうことが極めて重要である。

7 おわりに

本学で新たに導入した脆弱性調査スキームに基づき、「学外公開ホスト」を対象として、脆弱性検知スキャナ Nessus を用いた脆弱性調査を実施した。調査の結果、学外公開ホスト 148 台のうち 29 台のホストから脆弱性を検出した。ホスト管理者は、Nessus の脆弱性調査レポートを活用してすべての脆弱性を解消する対策を実施できた。

今後は脆弱性の定期調査によりさらなるセキュリティの強化を進めていく。

参考文献

[1] Nessus Vulnerability Scanner | Tenable Network Security
https://www.tenable.com/products/nessus-vulnerability-scanner