熊本大学公式 WEB システムセキュリティ監査支援

谷口勝紀，青木敏裕
電気情報技術系

1　はじめに

熊本大学公式 WEB システムは、データベースや認証、CMS などの機能毎に分割/最適化されて構築されており、仮想化されたサーバで 8 台、ホストサーバ 2 台、仮想化されていない WEB アクセス用サーバ 1 台の、合計 11 台のサーバ群で構築されている。　これらサーバは、非常に厳しいルールでアクセス制限の設定がされており、内部の極めて限られた端末からでしかアクセスされないよう制御されている。

本業務支援で行ったセキュリティ監査の範囲は、サーバシステムが持つセキュリティの脆弱性を検出する事にある。ここでいうセキュリティの脆弱性とは、OS やサービスプログラムが持つ脆弱性に止まらず、設定方法等の面からも含んでいる。

2　支援内容

ホストサーバ・GW サーバが仮に被害に遭った場合、その他のサーバ群へアクセス可能なルートができてしまう。

そこで、ホストサーバ・GW サーバが踏み台にされるという最悪の状況を想定し、これらのサーバから OpenVAS を用いて疑似攻撃を他のサーバへ行う事により、脆弱性の有無を確認する。　OpenVAS は 2014 年 4 月時点で、NVT フィードを用いて検証する脆弱性の数は 35,000 を超えている。

3　まとめ

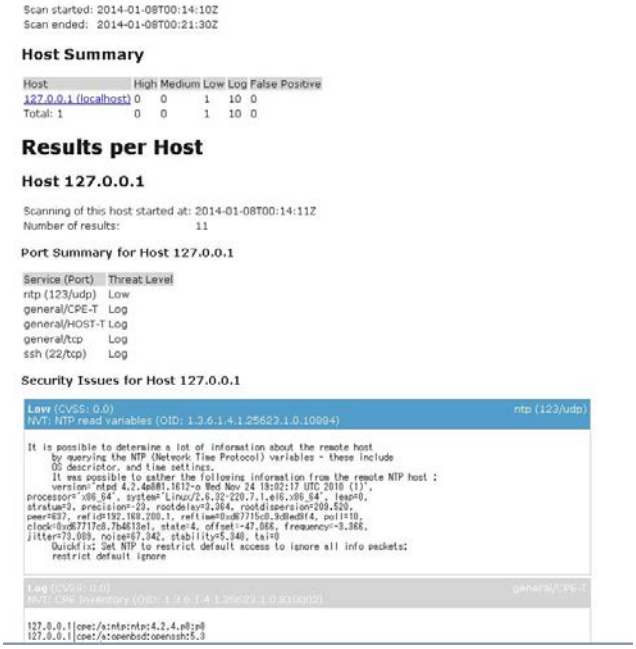
職員の繁忙期や WEB 利用が多い時期を避け、4 半期に一回程度のセキュリティ監査を行った。

稼動しているホストサーバ上で監査プログラムを実行しているが、システムで安定稼働している環境で、プログラムのアップデートが不可能になった為に、新たに監査システムサーバを構築して対応を行った。

実際に監査を行った期間は H25 年 5 月 14 日~16 日、H25 年 9 月 4 日~6 日、H25 年 1 月 8 日である

検出したアラートは CVE と呼ばれる脆弱性の種別を表したナンバーでレポートされるが、そのままでは意味をなさない。　脆弱性の内容を精査し、解析する事で対応するサービスを突き止め、より具体的な内容で報告書を作成する事で、脆弱性のアップデートが可能となる。

今回の支援では、OpenVAS の結果を精査した報告書の作成まで行い、対処法などを報告する事で脆弱性を埋める作業に貢献することが出来た。


Scan started: 2014-01-08T00:14:10Z
Scan ended: 2014-01-08T00:21:30Z

Host Summary

Host	High	Medium	Low	Log	False Positive
127.0.0.1 (localhost)	0	0	1	10	0
Total: 1	0	0	1	10	0

Results per Host

Host 127.0.0.1

Scanning of this host started at: 2014-01-08T00:14:11Z
Number of results: 11

Port Summary for Host 127.0.0.1

Service (Port)	Threat Level
ntp (123/udp)	Low
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log
ssh (22/tcp)	Log

Security Issues for Host 127.0.0.1

Low (CVSS: 0.0) — ntp (123/udp)
NVT: NTP read variables (OID: 1.3.6.1.4.1.25623.1.0.10884)

It is possible to determine a lot of information about the remote host
by querying the NTP (Network Time Protocol) variables - these include
OS descriptor, and time settings.
It was possible to gather the following information from the remote NTP host :
version="ntpd 4.2.4p8@1.1612-o Wed Nov 24 18:02:17 UTC 2010 (1)",
processor="x86_64", system="Linux/2.6.32-220.7.1.el6.x86_64", leap=0,
stratum=3, precision=-23, rootdelay=31.364, rootdispersion=209.820,
peer=4837, refid=192.168.200.1, reftime=0xd87715c8.9c8ed0f4, poll=10,
clock=0xd87717c8.7b4618e1, state=4, offset=-47.068, frequency=-3.366,
jitter=73.089, noise=67.342, stability=5.340, tai=0
Quickfix: Set NTP to restrict default access to ignore all info packets:
restrict default ignore

Log (CVSS: 0.0) — general/CPE-T
NVT: CPE Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

127.0.0.1|cpe:/a:ntp:ntp:4.2.4.p8:p8
127.0.0.1|cpe:/a:openbsd:openssh:5.3

参考 URL：

熊本大学：http://www.kumamoto-u.ac.jp/

OpenVAS: http://www.openvas.org/index.html