HyperDemo
HyperDemo1
生体情報システム・開発・セキュリティ
2017年11月21日(火) 16:45 〜 18:00 K会場（Hyper Demo） (3F イベントホールB・C・D・E)

[2-K-1-HD1-5] Open Source Softwareとフリーウェアを活用した部門システム向けセキュリティ設計の一提案

辻岡 和孝, 中川 肇 （富山大学附属病院医療情報部）

【背景】
　部門システムを導入する場合、電子カルテシステムの LANと同一セグメントに設置される場合があり、システム間のアクセス制御の対処は弱点と考えられる。今回、 Open Source Software（以下、 OSS）である Zabbixと、フリーウェアであるソフトイーサ社のパケット警察を利用し、正規部門端末以外からの部門サーバへのアクセスを検知する仕組みを構築した。導入時に、プログラミング知識は必要としない。
【方法】
　部門システム毎に Zabbixを導入し、正規端末の MACアドレスを登録しておく。部門システムサーバにはパケット警察と Zabbixエージェントをインストールする。サーバ上ではパケット警察で常時 TCPの通信ログ出力を行い、 Zabbixエージェントがログを常時監視し、部門システムで使用するサービスポートに TCPのコネクション要求が発生した際に、 Zabbixサーバに該当ログ情報の転送を行う。 Zabbixサーバはログ内に格納されている接続元 MACアドレスと、登録済みの正規端末の MACアドレスとの突合処理を行い、一致しない場合、トリガーを発生させ、部門システムサーバに Zabbixエージェントを介してアラート通知を行う。
【考察】
　本システムの特徴は、 TCPコネクション確立時に、最初の SYNパケットがサーバに到達した時点で接続元 MACアドレスを特定できる点である。このためステルススキャンなどフロー制御を伴わない通信においても確実にログを記録し、 SYNフラッド攻撃にも対応が可能である。アラート時にサーバ側でスクリプトの実行が可能であるため、他社の遮断システムとの連携も可能となり拡張性に優れる点もメリットである。また、 OSSとフリーウェアの組み合わせで実装しているため、安価に部門システムのセキュリティを高めることが期待できる。

Open Source Software とフリーウェアを活用した部門システム向けセキュリティ設計の一提案

辻岡 和孝[*1]、鍋島 一斗[*1]、中川 肇[*1]

*1 富山大学附属病院医療情報部

One proposal of security for department system with OSS and Freeware.

Tsujioka Kazutaka[*1], Kazuto Nabeshima[*1], Nakagawa Hajime[*1]
*1 Division of Medical Informatics ,Toyama Univasity Hospital

There is, generally, security vulnerability if the systems would be arranged on the same segment of the LAN. With the OSS (Open Source Software) and the freeware, we built the system to detect the injustice access from irregular clients with no administration of MAC address to the server, and to execute the script file in the server. The advantage of this system is summarized that no programming skills are required, and little cost is paid.

Keywords: Open Source Software, Freeware, Security, MAC address, Irregular access

1. 背　景

部門システムを導入する場合、電子カルテシステムの LAN と同一セグメントに設置される場合があり、システム間のアクセス制御の対処は弱点と考えられる。

今回、Open Source Software(以下、OSS)である Zabbix SIA 社の「Zabbix3.2(以下、Zabbix)」と、フリーウェアであるソフトイーサ社の「パケット警察」を利用し、部門システムクライアント端末以外からの部門システムサーバへのアクセスを検知する仕組みの構築を試みた。導入済みの部門システム構成になるべく変更を加えないことを目標とした。

2. 方　法

当研究室に実際の部門システムの構成と類似した環境を実験環境として用意した。

部門システムサーバとして Windows XP SP3 上で稼動する当院で導入されている「テルモ社メディセーフデータビジョン Ver4.2(以下、データビジョン)」を採用した。部門システム正規クライアント端末として、Windows7 上にデータビジョンクライアントをインストールした。部門システムサーバ上では、データベースエンジンとしてマイクロソフト社 SQL サーバ 2005 が稼動しており、データビジョンクライアントからは、データビジョンアプリケーションより TCP ポートの 6000 番を通じて、部門システムサーバと通信を行う(図 1)。

図 1:部門アプリケーションは TCP6000 番を利用する.

次に、Zabbix サーバを追加導入し、部門システムサーバへの接続を許可された正規端末の MAC アドレスを登録しておく。部門システムサーバにはパケット警察と Zabbix エージェントをインストールする [1,2]。Zabbix サーバは別途用意した CentOS7 上に構築し、部門システムサーバの Zabbix エージェントと通信を行う(図 2)。

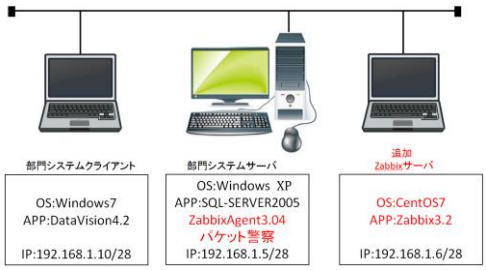

図 2:Zabbix サーバを追加し、部門システムクライアントの MAC アドレスを登録する. また、部門システムサーバにパケット警察と、Zabbix エージェントをインストールする.

部門システムサーバ上ではパケット警察で常時 TCP の通信ログ出力を行い、Zabbix エージェントがログを常時監視し、部門システムで使用するサービスポートに SYN 要求が発生した際に、Zabbix サーバに該当ログの転送を行う(図 3)。

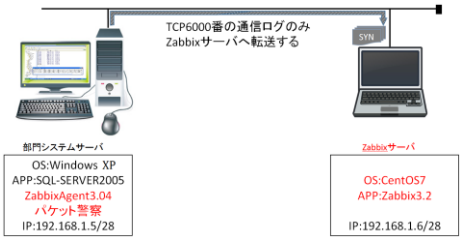

図 3:Zabbix エージェントが、パケット警察の通信ログを転送する.

Zabbix サーバはログ内に格納されている接続元 MAC アドレスと、登録済み正規端末の MAC アドレスとの突合処理を行い、一致しない場合、トリガーを発生させ、部門システムサーバに Zabbix エージェントを介してスクリプトを実行させる(図 4)。

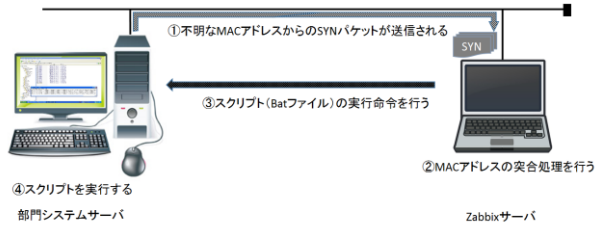

図 4:登録済み MAC アドレスと突合処理を行い、一致しない場合は部門システムサーバへスクリプト実行命令を行う.

3. 結　果

部門システムサーバと同一セグメント上で稼動する Kali-Linux 端末より、脆弱性診断ソフトである nmap7.01 を用いて、部門システムサーバに対してステルススキャン [3]を実施したところ(図 5)、Zabbix サーバ上でアクセスを検知することができた(図 6)。また、アクセスをトリガーにして、部門システムサーバ内にあるスクリプトファイルの実行をすることができた(図 7)。

図 5:Kali-Linux 端末よりステルススキャンを実施する.

図 6:Zabbix サーバがアクセスを検知し、部門システムサーバへスクリプトの実行を指示する.

図 7:部門システムサーバ上のスクリプトが実行された.

4. 考　察

本設計の特徴は、TCP プロトコルにおけるスリーウェイハンドシェイクにおいて、最初の SYN パケットがサーバに到達した時点で接続元 MAC アドレスを特定できる点である。MAC アドレスはエッジスイッチで、どのポートからのアクセスかの把握は可能である。市販の遮断システムの中には MAC アドレスを指定することで該当ポートを閉じる製品も販売されてきているので、アラート発生時にスクリプトの実行を、これらの機能と連動することで、スマートな遮断システムの構築が期待できる。

また、近年普及が進んでいる、仮想マシン環境においては、仮想マシンの MAC アドレスを任意に設定することが可能である。このため、MAC アドレスと IP アドレスを正常端末に偽装することで、条件をすり抜けてアクセスすることが可能であるが、IP が競合した場合には Windows の機能でシステムエラーとなるため、クライアント端末を常時起動しているような環境においては、効果があるセキュリティ手法と思われた。

ステルススキャンは通常、サーバアプリケーションのログ機構ではログに記録されない。IDS などを導入することで、検知することは可能であるが、別途スイッチへのミラーポートの設定等が必要になり、実現のハードルは高くなる。フリーウェアのパケット警察と OSS の組み合わせで、安価に部門システムのセキュリティ向上が望める点はメリットと考える。

昨今、仮想ネットワーク技術により、仮想マシン単位の個別ファイアウォールが実現できるようになっているが、実現にはコスト面や運用面でのハードルが高いことは否めない。本設計は低価格、運用面でのハードルが低い点でメリットがあり、特に物理環境においては現実的なセキュリティ設計と思われた。

注意点として、医療機器に組み込まれている OS の場合は厚生労働省「医療機器プログラムに関する通知」[4]の内容を鑑み、フリーウェアのアドオンが可能かを慎重に確認する必要がある。

5. まとめ

本設計により、病院情報システムと同一セグメントに配置する部門システムサーバにおいて、正規の部門システムクライアント以外からのアクセスを検知することができた。またアクセスをトリガーとしたスクリプトの実行ができた。

OSS とフリーウェアの組み合わせにより、低価格で運用負荷が少ないセキュリティ向上の設計をすることができた。

既に導入済みの部門システムがある場合、特に物理環境において、現実的な選択肢となりえた。

参考文献

1) 寺島広大. 改訂版 Zabbix 統合監視実践入門.技術評論社, 第 2 版, 14-34.
2) ソフトイーサ(株)ホームページ.パケット警察 for Windows.ソフトイーサ(株), 2017, [http://www2.softether.jp/jp/packetpolice (cited 2017-Aug-16)].
3) Gordon Lyon. ポートスキャンのテクニック.nmap.org, 2017,[https://nmap.org/man/jp/man-port-scanning-techniques.html(cited 2017-Aug-16)].
4) 厚生労働省大臣官房参事官. 医療機器プログラムの取扱いについて(薬食機発 1121 第 33 号). 厚生労働省, 2016,[http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000073073.html(cited 2017-Aug-31)]]