不正アクセス検知

侵入検知技術の現状と将来

独立行政法人理化学研究所
渡辺　勝弘

不正アクセス検知の手法

- 不正アクセスの発生をどのように知るか
  - コンピュータのステータス情報、ログなど
  - ネットワーク機器のステータス情報、ログなど
  - ファイアーウォール
  - 侵入検知システム

侵入検知システム(IDS)とは、
不正アクセスを検知するための専用システム

侵入検知システム

- Intrusion Detection System (IDS)
  - 侵入検知(IntrusionDetection)とは、コンピュータおよびネットワークに対するセキュリティ侵害の検出、通知、検出情報の管理に関する一連のプロセスを指し、侵入検知システムは、侵入検知を行うことを目的として設計されたシステムのことである

*ネットワーク侵入検知　武田圭史/磯貝宏著
ソフトバンクパブリッシング

検知メカニズム

- 検知手法
  - 不正検知と異常検知
- 運用形態
  - ホストベースとネットワークベース

いまさらですが、おさらいしましょう

検知手法

- 不正検知(Misuse Detection)
  - ログやネットワークのデータに、あらかじめ登録してある不正アクセスのデータを照らし合わせることで、不正行為を検知する
- 異常検知(Anomaly Detection)
  - システムやユーザの振る舞いを監視し「通常では無い振る舞い」を検知する

運用形態

- ホスト型(HostBase)
  - コンピュータのログやシステム情報などを監視して、不正、異常行為を検知する
  - DragonHostSensor、RealsecureServerSensor
- ネットワーク型(NetworkBase)
  - ネットワーク上を流れるパケットを監視することで、不正、異常行為を検知する
  - DragonNetworkSensor、Snort、RealsecureNetworkSensor

検知メカニズム

- 現在では、シグネチャマッチングによる不正検知型のネットワーク侵入検知システムが主流
  - ネットワークを流れるパケットに含まれるデータパターンと、不正行為のデータパターン(シグネチャと呼ぶ)のマッチングを行うことで、不正行為、異常の検知を行う

もちろんホスト型の実装も存在する

シグネチャ型侵入検知

シグネチャ(ルール)の例：Snortの場合

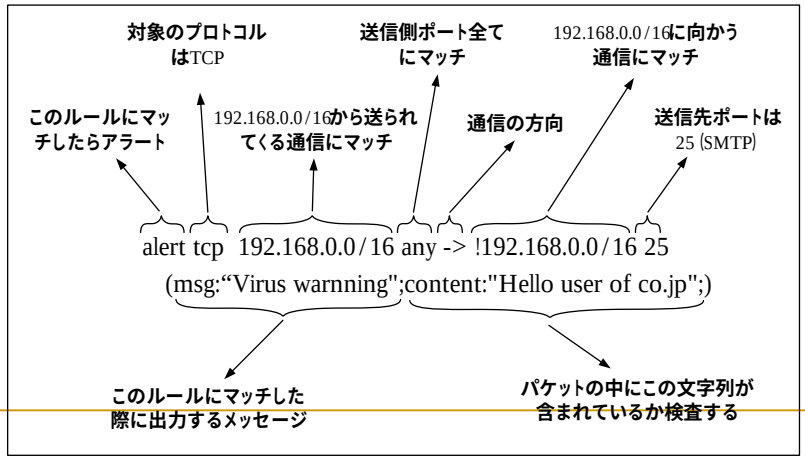
Bagle（ウィルスメール）を検知するルール

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any  (
msg:“Suspicious virus warnning v2 !!!”;
content:“Attached file";
content:"password";)

alert tcp $HOME_NET any -> $EXTERNAL_NET 25  (
msg:"Suspicious virus warnning v1 !!!";
content:"Hello user of Go.jp";)
```

検知メカニズム

シグネチャ(ルール)の例



ルールセット

```
# (C) Copyright 2001,2002, Martin Roesch, Brian Caswell, et al.
#    All rights reserved.
# $Id: icmp.rules,v 1.18 2002/08/18 20:28:43 cazz Exp $
#-----------
# ICMP RULES
#-----------
#
# Description:
# These rules are potentially bad ICMP traffic.  They include most of the
# ICMP scanning tools and other "BAD" ICMP traffic (Such as redirect host)
#
# Other ICMP rules are included in icmp-info.rules

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:“ICMP ISS Pinger”;  content:“|495353504e475251|”; itype:8;
depth:32; reference:arachnids,158; classtype:attempted-recon; sid:465; rev:1;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; content:
"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; itype: 8; icode: 0; depth: 32; reference:arachnids,311; classtype:attempted-
recon; sid:466; rev:1;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize: 20; itype: 8; icmp_id: 0;
icmp_seq: 0; content: "|0000000000000000000000000000000000000000|"; reference:arachnids,449; classtype:attempted-recon;
sid:467; rev:1;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize: 0; itype: 8; reference:arachnids,162;
classtype:attempted-recon; sid:469; rev:1;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; id: 666; dsize: 0; itype: 8; icmp_id: 666 ;
icmp_seq:0; reference:arachnids,450; classtype:attempted-recon; sid:471; rev:1;)
```

シグネチャ型の現状

- 未知の手法による不正アクセスには対処できない
- シグネチャはチューニングが必須
- 大量のアラートが発生してしまう
- 常にルール(シグネチャ)を更新しつづけなければならない
- ルールセットが肥大化してしまう

FalsePositiveとFalseNegative

シグネチャ型の現状

- False Positive
  - シグネチャにマッチした通信は、なんであろうとアラートを発生させる
- False Negative
  - 不正アクセスのパターンがシグネチャとして用意されていなければ検出しようがない

侵入検知システムは学習しないし
ネットワークを知らない

アノマリ型侵入検知

- プロトコルアノマリ
  - RFC等で規定されている正規の手順を踏まない通信を異常として検出する
- 行動ベース分析
  - システム、ユーザの振る舞いからプロファイルを作成し、通常でない振る舞いを異常として検知する
  - システム、ユーザの振る舞いに閾値を設定し、これを越える値を異常として検知する

アノマリ型の現状

- 実際に入手できて、運用することのできるアノマリ型侵入検知システムは、ネットワーク型のプロトコルアノマリ検知がほとんど
  - ネットワーク観測装置としては有益
  - 侵入検知システムとしては？？？？
  - もちろんFalsePositive、FalseNegativeの問題を持ちます

プロトコルアノマリ型侵入検知システムを動かしてみると、ネットワークのノイズが如何に多いか良く分かります

アノマリ型の現状

- アノマリ型侵入検知は実験的なシステムしかみかけない
- プロトコルアノマリなどの正しくない通信を監視するシステムとしては有益であるが、侵入検知システムではない

アノマリ検知は万能薬ではない
シグネチャ型の検知と組み合わせることで、その能力を発揮できる

侵入検知システムの問題点

- 信頼できないシステムである
  - FalsePositiveとFalseNegative
  - アラートの再分析が必要
- それひとつだけでは成り立たない
  - 検知するだけで防御はできない
- 高い導入、運用コスト
  - 導入に数百万円、運用に5〜70万円/月

検知できるもの

- 検知できる不正アクセス
  - ポートスキャン
  - Script Kiddies(ツール房)による幼稚な攻撃
  - 旧めのワーム、ウィルス

検知できる不正アクセスは、既知の攻撃ばかりで、大抵のばあい対策が済んでいる

知りたいこと

- 私たちが本当に知りたいのは
  - 身近に迫っている真の危機
  - システムの弱点を突いたワンポイント攻撃
  - 未知の危険なワーム、ウィルス等に感染したPC

ポートスキャンや影響を受けない不正アクセスは、月一のレポートででも報告してくれればいい

侵入検知に対する要望

もっと高い精度の侵入検知が
実現できないだろうか

不正アクセスを未然に防ぐことが
できないだろうか

侵入検知周辺の動向

- IDPS（不正侵入防御システム）
- Target Based IDS
- UTM (統合脅威管理)
- SIM (統合セキュリティ管理ツール)
- PFW(パーソナルファイアウォール)
- トラフィック分析

不正侵入防御システム

- IDPS (Intrusion Detection & Prevention System)
  - 現時点での主流
  - 侵入検知システムに、自動フィルタリング機能が付いたもの
  - 既存の侵入検知システムがベースなので、その効果は推して知るべし
  - ワーム拡散防止などに活用している例はあるらしい
  - 何を遮断するかが鍵

TargetBasedIDS

- 監視対象のコンピュータのプロファイルを元に、アラートの重み付けを行うことで、検知精度を向上させる
  - たとえば、Linux+Apacheでサーバを運用しているなら、Nimdaによる悪性イベントが検出されても、必要以上の注意は無用であるから、アラートの危険度を下げる。逆にWindows+IISでサーバを運用しているなら、危険度を上げて管理者に注意を促す
  - 侵入検知の方向性としては良いかもしれない

MBSD 伊藤氏による解説 Snort-JP
http://www.snort.gr.jp/docs/N+I2005SnortBOF.pdf

統合脅威管理システム

- UTM (Unified Threat Management)
  - セキュリティ機能を単一のプラットフォーム上で提供するゲートウェイ型アプライアンス
    - ファイアーウォール、IDS/IDPS、ウィルス/スパム対策、コンテンツフィルタリング(HTTP、SMTP)等
  - 複数のセキュリティアプライアンスを一つの箱に実装することで省スペース、省コストを図る
  - まだ、ひとつにまとめただけのように見える
  - 検知精度が向上するわけではない
  - UTMにより不正アクセス管理が効率化するのかは、まだ良く分からない

SIM(統合セキュリティ管理ツール)

- SIM (Security Information Manager)
  - UTMとは逆のアプローチ
  - セキュリティアプライアンス等、さまざまな機器のアラート、ログ等をまとめて分析することで、不正行為、異常状態などを検知しようとする
  - ふたぎさんのセッションで紹介

PFW(パーソナルファイアウォール)

- クライアントコンピュータの上で検知と遮断を行う
- クライアントにおける検知と防御は、今後一般的になるだろう
- アンチウィルス、OS、他のセキュリティアプライアンス、ネットワーク機器等との連携がされてない
- 集中管理、監視の仕組みを整備する必要がある

トラフィック分析

- さまざまな通信の振る舞いを監視することで不正行為や異常を検知する
- 既知のネットワーク監視手法をもう少し掘り下げて、セキュリティ監視に応用しよう
- これだけで不正行為を検知することはできない
- 異常発生の参考データ程度にしかならない
- 他の監視手法と組み合わせる必要がある

不正アクセス手法の現状

- 高い頻度のワーム発生
  - 重要なアプリケーションに脆弱性が発見されると、それを対象としたワームがすぐに発生する
- ワームとウィルスの結合
  - 従来のメールによるウィルス拡散手法に、アプリケーションの脆弱性を用いたネットワーク感染が加わる
- 高度化する不正プログラム
  - バックドアの提供、自動運転機能の装備など、高度な機能を実装した不正プログラムの存在

不正アクセス手法の現状

- 新たな手法による不正プログラムは常に出現しつづける
- 不正プログラムは、対策手法の進化よりも早く進化し、また驚くべき速度増殖してゆく

侵入検知システムにかぎらず、
セキュリティ機器全体にとって不利な状況

特に侵入検知・防止手法の将来に不安を感じる

検知が困難な例

- 最近なにかと話題のBOTNETですが、侵入検知システムで検出するのは困難です
  - 亜種の発生サイクルが短い
    - 1日数十の新しいBOTが発生している
  - 感染後に自身を別なプログラムと置き換えることができる
  - 難読化される制御チャネル

ボットの一例

とあるアンダーグラウンドサイトにポストされていた記事

HTTP Controlled DDoS Bot Description:

This bot is quite unqiue, I haven't seen it done anywhere. Basically it's a trojan which works from the internet, and not through a mIRC server. This program downloads all the required settings it needs through a HTTP server, note: all the settings are encrypted using my very own developed, secure 3-bit encryption.

BOTNETの検出

- 暗号化チャネルの解読は既存の侵入検知システムでは難しい
- BOTNETが更新されると、それに対応するシグネチャが必要

BOTNETの検出

- 最近のセキュリティ機器の中には、ネットワークフロー(通信の流れ)の異常を監視することで、ワームやBOTNETに対処しようとする物が存在します
- これらはスキャン、極端な自己増殖行為など、目立ちやすい異常な行動を監視しようとするもので、こっそりと活動するワームなどに対する効果は疑問

侵入検知システムの将来

- 既存のシグネチャ型侵入検知システムの技術は別な形態に変化する
  - 侵入検知システムは、ネットワーク監視装置として、その形態を変化させてゆくのではないか
  - プロトコルアノマリ検知のように、不正アクセスだけを対象とせず、ネットワーク通信で、注意しなければならない現象を検知するための装置
- アノマリ型侵入検知システムが意外な進化を見せるかもしれません
- PFWを中心として進化がみられるでしょう

ネットワーク監視装置としての侵入検知システム

- ネットワークの振る舞い
- バックグラウンドノイズ

この検知結果から
アノマリ検知ができないだろうか

これについては以降のセッションで

侵入検知システムの将来

- 今後は動向で紹介した新しい技術等がますます進化することでしょう
  - IDPS、ファイアウォール、ウィルスゲートキーパーが結合する
  - UTM(統合脅威管理システム)とSIM(統合セキュリティ管理ツール)が結合する

とりあえずまとめ

今後も不正アクセス検知、防御のための手法は進化しつづけます。特定のソリューションだけに不必要なコストをかけず、情報セキュリティ対策全体に対してバランス良くコストをかけましょう

参考資料

- ネットワーク侵入検知　武田圭史/磯貝宏著
  - ソフトバンクパブリッシング ISBN479731253X
- The mosy psychoid
  - http://www.psychoid.net/
- Snort The Open Source Intrusion Detection System
  - http://www.snort.org/
- Network Attack Visualization G. Conti; DEFCON 12; August 2004.
  - http://www.rumint.org/gregconti/publications/20040731-DEFCON-12-Conti.ppt
- MBSD 伊藤氏による解説 Snort-JP
  - http://www.snort.gr.jp/docs/N+I2005SnortBOF.pdf
- Target based IDS review and discussion in Information Security
  - http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_art540,00.html
- Pigeye　Snortで作るTargetBasedIDS 慶応大学SFC 水谷、白畑氏
  - http://sourceforge.net/projects/char-siu/
- 電気通信大学　小池 助教授によるセキュリティ情報の視覚化について
  - http://www.vogue.is.uec.ac.jp/~koike/security/CSM.pdf