検出・検知
―IDS、マルウェア対策―

上原哲太郎
UEHARA Tetsutaro

攻撃の検出の重要性

- 公開しているサービスなどへの攻撃
  - 通常の利用か，悪意あるアクセスかを判別する必要性
    - セキュリティホール
    - DDoS攻撃
- メールやWebを介してやってくるマルウェア

攻撃の検知と防御

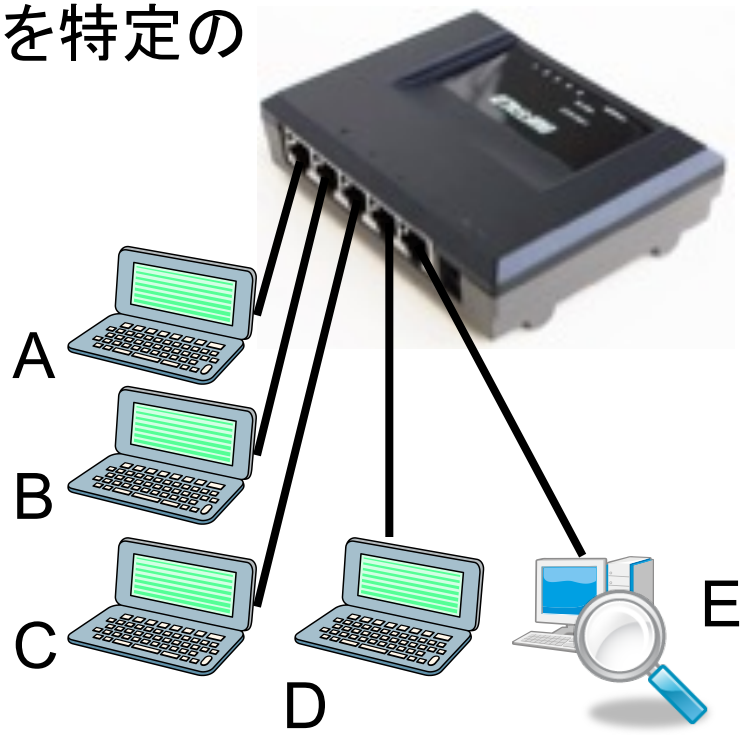
- これまでも述べてきたように，インターネットの世界にも様々な脅威があり，重要な情報を守るには「監視」が必要不可欠．
  - コンピュータへの侵入
  - 詐欺行為
  - サービス妨害行為

- Firewallで「防止」もできるが，
  「監視」をすることでさらなる安全を手に入れる
  - IDS: Intrusion Detection System（侵入検知システム）
  - IPS: Intrusion Prevention System
  - それぞれネットワーク型とホスト型がある
    - NIDS/NIPS，HIDS/HIPS

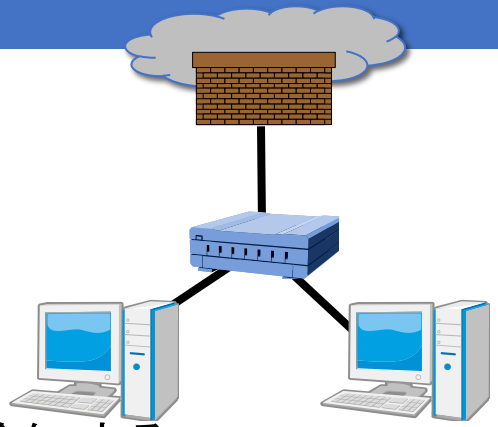
簡単な方法

- 流れているパケットを監視するツール
  - tcpdump, wireshark などのツールやアナライザ

- IPアドレス，プロトコル，ポート番号などがわかる
- ポートミラーリング（パケットのコピーを特定のポートに送る方法）とあわせて使う



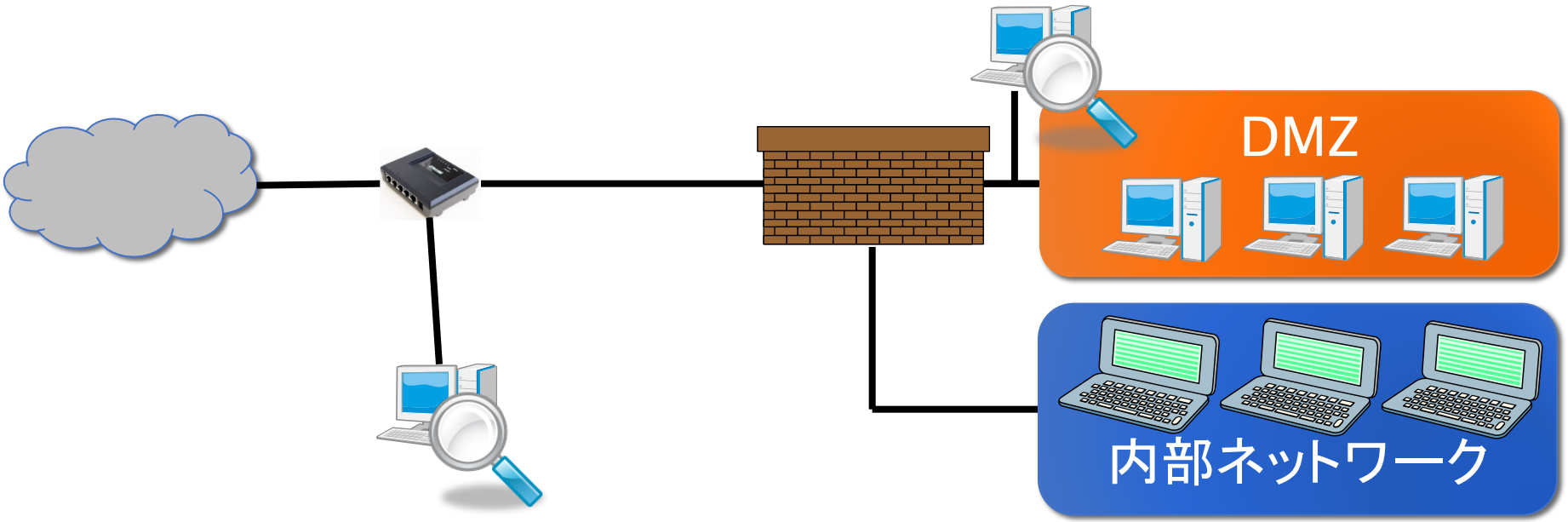
NIDS/NIPS



- 侵入検知機能
  - 不正と思われる通信を検知する
  - 悪性サイトやわいせつなサイトへの通信，P2Pソフトの通信など，組織内のセキュリティポリシに関わる通信も検知する
- Anomaly通信検知機能
  - 正常とは考えにくい通信を検知する
    - RFCに準拠しているか，使用帯域はどうか，どのアプリの通信か
    - 0-day攻撃など侵入検知でひっかからないものを対象とできる
- 不正通信へのレスポンス機能
  - 上記2つを検出したときの動作
  - 管理ソフトウェアや管理者への通知
  - 当該の通信を強制終了させる(TCPのRST，Firewall連携)

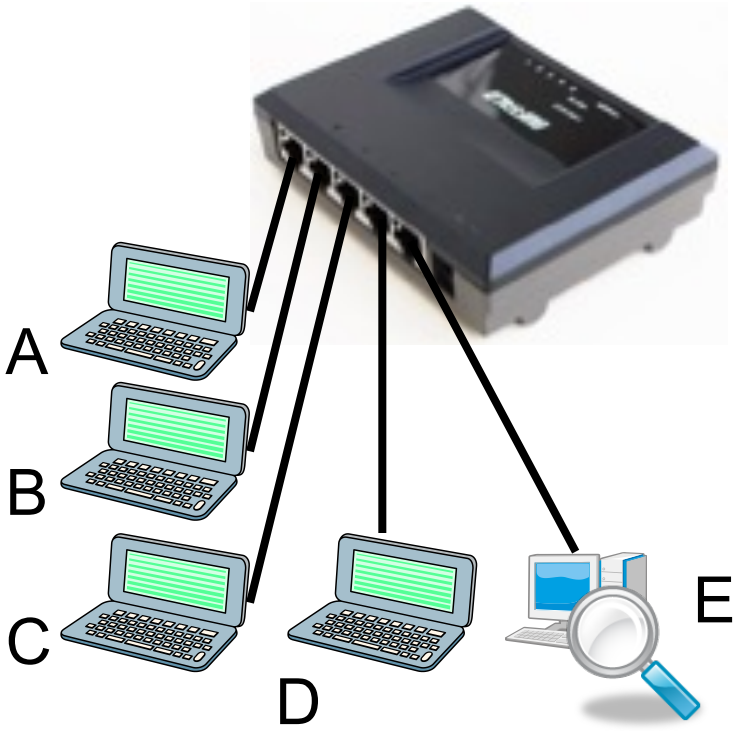
NIDSの設置

- 目的に応じて設置箇所を検討
  - FWの外側に設置
    - 自分のシステムに向かう攻撃全てを分析
    - FWで防がれる攻撃も監視（大量のトラフィックを監視）
  - FWの内側に設置
    - FWを通過した攻撃を防御



NIDSの接続におけるいくつかのポイント

- promiscuous(無差別)モード
  - NICが自分宛以外のパケットも拾うようになる
- ステルスモード(NICにIP addressを振らない)
  - NIDS自体が攻撃されたり，存在を検知されにくくなる
- 接続するネットワーク機器の選択
  - shared hub(repeater hub)
  - switching hub
  - mirroring 機能付き intelligent hub
  - タップ



不正な通信の検知手法（パターンマッチング）

- 攻撃に使われる文字列・バイナリパターン（シグネチャと呼ぶ）と，トラフィックを比較
- 最も基本的で確実な方法だが，既知の物のみ検出可

```
alert tcp any any -> 192.168.1.0/24 21 (content: "user root"; \
    msg: "FTP root login";)
```

```
alert tcp ![192.168.1.0/24,10.1.1.0/24] any -> \
    [192.168.1.0/24,10.1.1.0/24] 111 (content: "|00 01 86 a5|"; \
    msg: "external mountd access";)
```

- せっかくなので文字列探索アルゴリズムを見てみよう
  - クヌース・モリス・プラット法 Knuth-Morris-Pratt Algorithm KMP
  - ボイヤー・ムーア法 Boyer-Moore Algorithm BM
  - ラビン・カープ法 Rabin-Karp，エイホ・コラシック法 Aho-Corasick

不正な通信の検知手法（anomaly検知）

- プロトコルアノマリ検知
  - RFC違反の通信を検出
- トラフィックアノマリ検知
  - 事前に設定された値よりもトラフィックが多い
    - コネクション数，SYN/FIN/RST，UDP，ICMPなどに分類することも
  - 普段の傾向を自動的に学習して，その値との差で異常を検出
- アプリケーションアノマリ検知
  - あるプロトコルにおいて異常なデータが送られることを検知
    - SSH/Telnetではないのにシステムコマンドがタイプされている
    - HTTPで異様に長いHTTP requestが流れている

Snort

Snort

- OpenSource
- Always improving
- Lightweight
- Detection:
  - Stealth scans, OS fingerprinting, buffer overflows, back doors, CGI exploits, etc.
- Modes
  - Sniffer
  - NIDS
  - Packet Logging

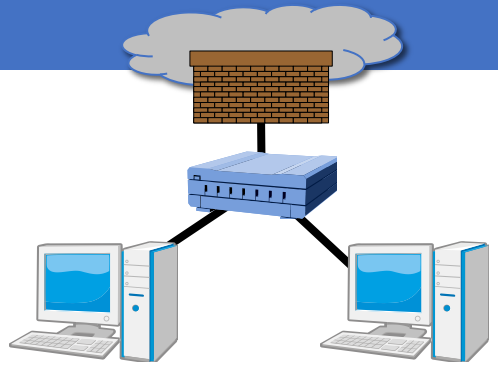
IDSの例: snort

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 192.168.24.100 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
11/15-20:59:34.027914

[**] [1:100000122:1] COMMUNITY WEB-MISC mod_jrun overflow attempt [**]
[Classification: Web Application Attack] [Priority: 1]
11/15-18:12:07.960246 218.223.42.116:8254 -> 192.168.24.100:80
TCP TTL:115 TOS:0x0 ID:65100 IpLen:20 DgmLen:1500 DF
A* Seq: 0x7F3A1067 Ack: 0xA6EBB188 Win: 0xFA2C TcpLen: 20

[**] [1:3197:2] NETBIOS DCERPC ISystemActivator path overflow attempt little endian [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
11/15-19:35:37.086844 192.168.21.1:2345 -> 192.168.24.100:135
TCP TTL:128 TOS:0x0 ID:21361 IpLen:20 DgmLen:936 DF
AP Seq: 0xC1E25945 Ack: 0x8940F1D7 Win: 0x4318 TcpLen: 20

HIDS/HIPS



- ユーザ操作検知機能
  - 不正なログイン・ログアウト，特権ユーザへの昇格を検知
    - 時間外のログイン，本来特権ユーザになれないユーザの昇格
- ファイル改ざん検知機能
  - 指定したディレクトリやファイルの変更・削除を検知
    - /etc以下，C:\windows\system32以下の監視
- ハニートラップ機能
  - 意図的にオープンされた未使用通信ポートへの通信を検出
    - L3, L7的な接続要求の有無，L7的な行動の監視
    - 場合によっては監視をしている旨のメッセージを返す
- 不正操作へのレスポンス機能
  - 不正検知時の管理コンソールへの通知
  - 不正実行されているプロセス等の強制終了

HIDSの検知方法

- 主にはログを使う
  - syslogやevent log

kterm

```
frigg:~ : cat /etc/syslog.conf
*.err                           /dev/console
*.notice                        /var/log/messages
#
console.*                       /var/log/console.log
#
auth,authpriv.*                 /var/log/auth.log
security.*                      /var/log/security
mail.*                          /var/log/maillog
lpr.*                           /var/log/lpd-errs
cron.*                          /var/log/cron
daemon.*                        /var/log/daemon
kern.*                          /var/log/kernel
#
*.warn                          root
*.emerg                         *
```

kterm

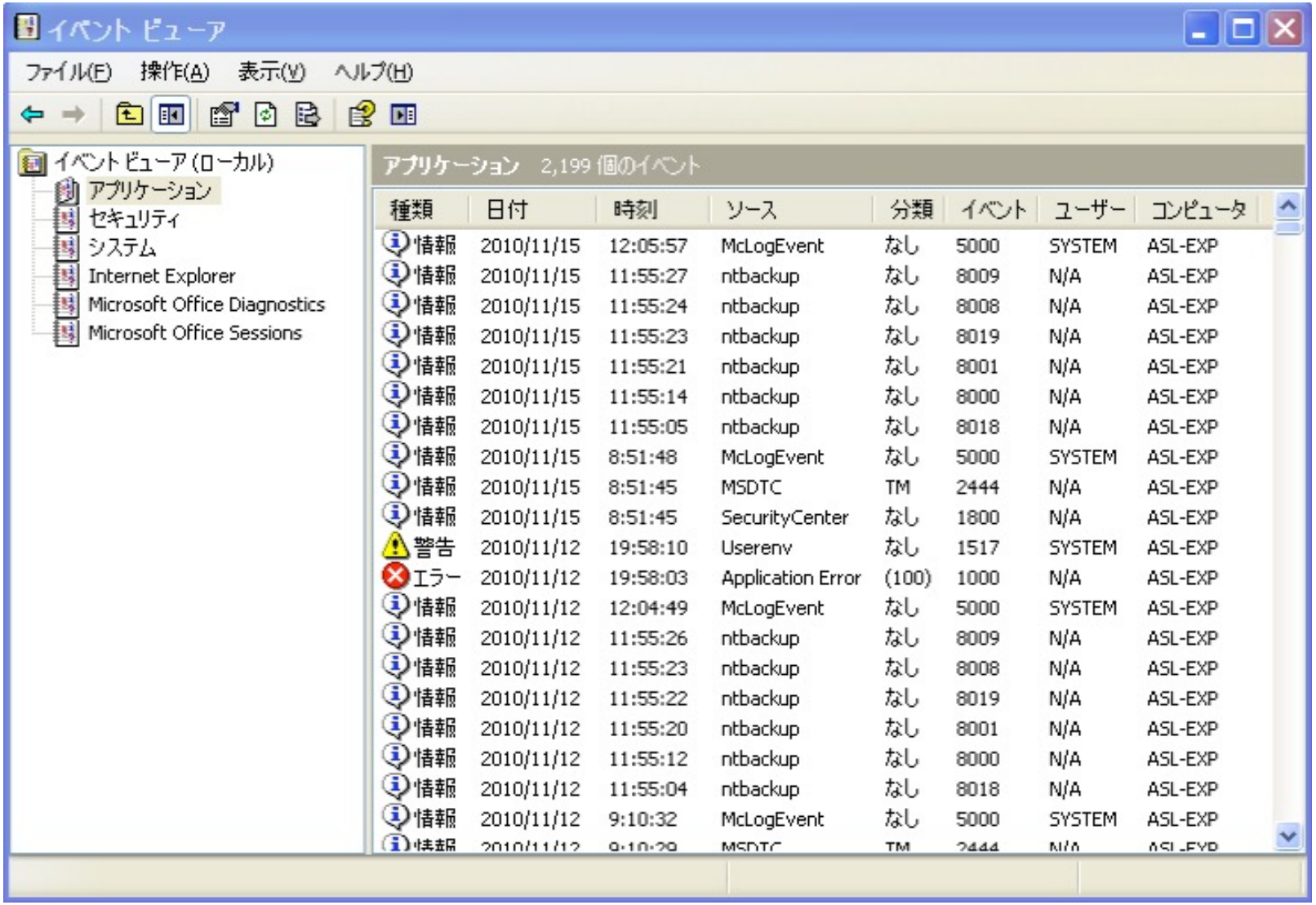
```
frigg:~ : ps axw|grep syslogd
  583  ??  Ss     0:05.17 /usr/sbin/syslogd -l /var/run/log -l /var/named/var/ru
```

```
Nov 12 15:20:50 frigg sshd[51679]: warning: /etc/hosts.allow, line 18: host name
/address mismatch: 123.30.183.120 != static.vdc.vn
Nov 12 15:20:50 frigg sshd[51679]: refused connect from 123.30.183.120 (123.30.1
83.120)
Nov 13 09:19:57 frigg sshd[68647]: refused connect from 112.217.12.162 (112.217.
12.162)
Nov 13 10:00:45 frigg sshd[69282]: refused connect from 111.10.1.58 (111.10.1.58
)
Nov 13 16:19:55 frigg sshd[74487]: refused connect from 211.151.67.73 (211.151.6
7.73)
Nov 13 23:01:32 frigg sshd[80131]: refused connect from 221.226.17.14 (221.226.1
7.14)
```

syslog

- facility
  - LOG_AUTH, LOG_AUTHPRIV, LOG_SECURITY
  - LOG_KERN, LOG_DAEMON, LOG_MAIL, LOG_FTP, …
  - LOG_CONSOLE
  - LOG_USER, LOG_LOCAL0〜LOG_LOCAL7
- priority
  - LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, LOG_DEBUG
- プログラムは
  - openlog(), syslog(), closelog() などを使って出力
  - syslogdが受信し(udp/514), syslog.confに従いファイルへ

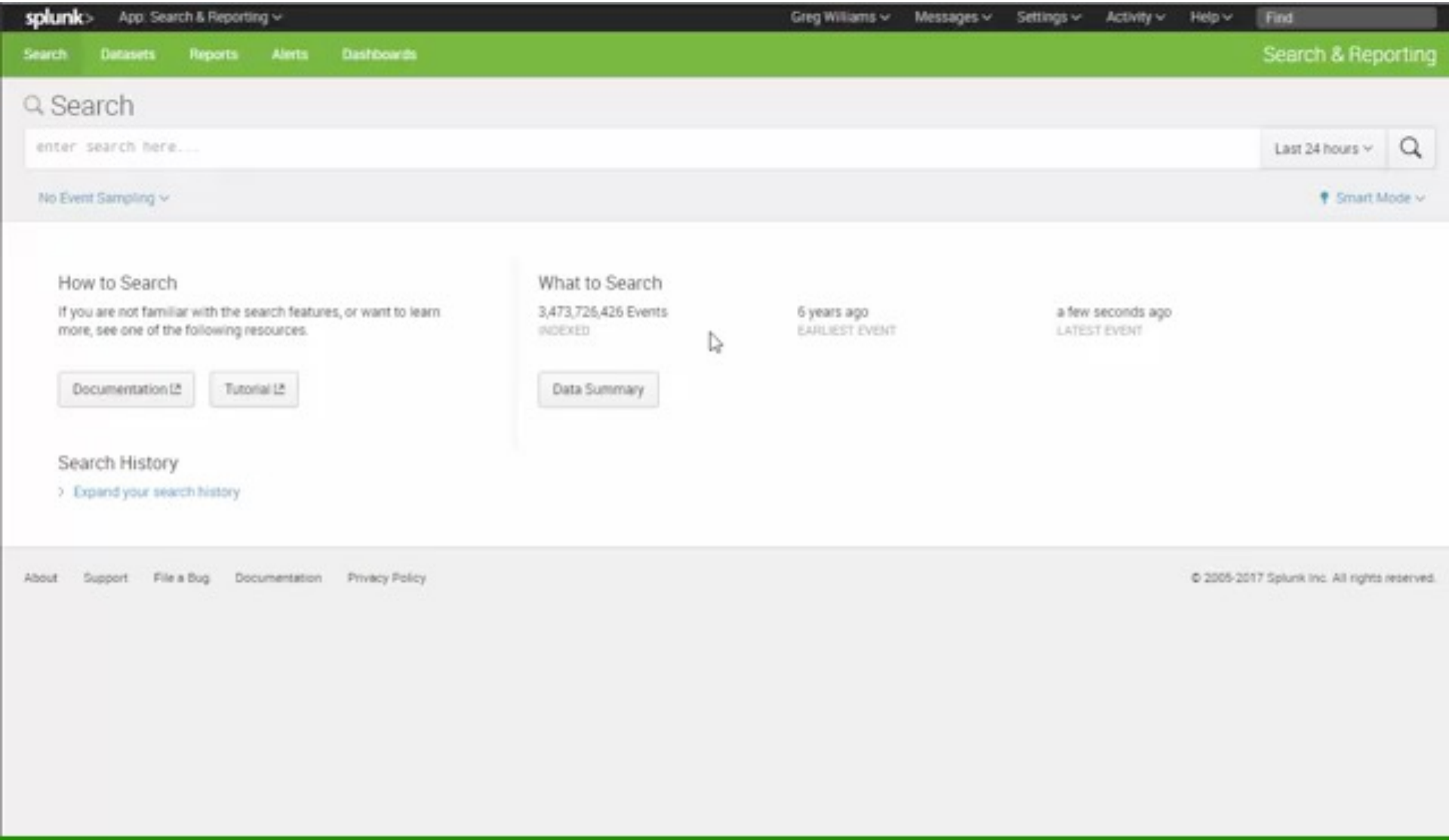
WindowsでのSyslog的なもの: Event Viewer イベントビューア



OSSEC

- Key Features
- File Integrity checking
  ファイル改ざん検出
- Log Monitoring
  ログ監視
- Rootkit detection
  ルートキット検出
- Active response
  動的遮断

Splunk


splunk>
App: Search & Reporting
Greg Williams
Messages
Settings
Activity
Help
Find
Search
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Search
enter search here...
Last 24 hours
No Event Sampling
Smart Mode
How to Search
If you are not familiar with the search features, or want to learn more, see one of the following resources.
Documentation
Tutorial
What to Search
3,473,726,426 Events
INDEXED
6 years ago
EARLIEST EVENT
a few seconds ago
LATEST EVENT
Data Summary
Search History
Expand your search history
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2017 Splunk Inc. All rights reserved.

わざと攻撃を誘い込むハニーポット Honeypot

- 仮想的に「脆弱なシステム」を公開しておき，
  そこへアクセスしてくる攻撃者を監視・観測するシステム
  - IDS/IPSに必要な機能ではないのだけど
- 攻撃統計調査
  - 単純に，接続を試みてきた数を調査
  - 具体的に，攻撃手法を特定するような調査
- 攻撃者行動調査
  - どのような手法で攻撃をするのか，どのような役割のホストを狙うのか，
    どのようなデータを狙うのか
  - ネットワーク全体を監視するハニーネットを構築することも
- 悪意あるプログラムの収集
  - 攻撃時・侵入後に使用されたプログラムを収集

ハニーポットの種類

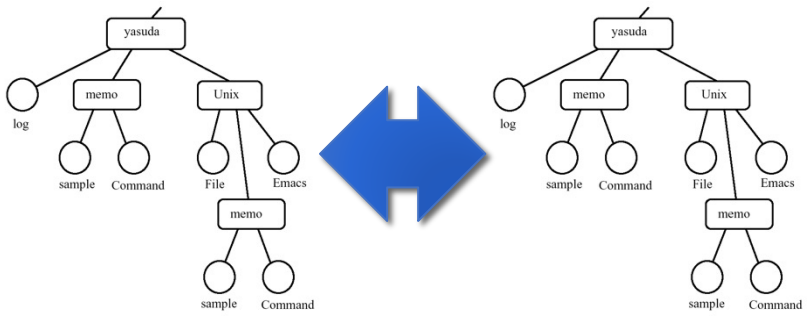
- Low-interaction honeypot (低対話型)
  - 特定のOSやアプリケーションをエミュレーションした観測環境
    - 目的によっては脆弱性を再現することも
  - 当然エミュレーションの範囲が限られるので，
    得られる情報も限られる
  - Nepenthes, mwcollect, dionaea, spector, honeyd, …
- High-interaction honeypot (高対話型)
  - 実際のOSやアプリケーションを用いた観測環境
  - 実物であるため，予想しなかった行動も観測できる
    - ただし，観測の方法は限られる
  - 攻撃によって本当にダメージを受けるリスクもある．
    細心の注意が必要

他のファイルの改ざん検出法

- HIDSなどではリアルタイムの検出を行う
- 事後も含めてやるとすれば・・・

- Tripwire
  - ディレクトリやファイルのハッシュ値を事前に記録
  - 検査時に再度ハッシュ値を求め，事前のものと比較
  - Open Source Tripwireなんてのもある

- rsync　の -c -n (Linuxのファイル比較)
  - 2つのディレクトリツリーを比較



マルウェア対策 Anti-Malware
ウイルス対策 Anti-Virus

- コンピュータのファイル読み書きや通信を監視、マルウェア(Malware / Virus)固有のパターンpatternを発見したら中止させる
  - マルウェアは新種がどんどん出てくるのでパターンを定義するファイルが重要
    - よってサポートを受け続ける必要がある
    - 最近は新種の登場にアンチウィルス会社は十分追随できていない＝マルウェア対策が入っていても感染の危険はなくならない
    - 特にbotnetの検出は困難になりつつある
- クライアントで行うものとサーバで行うものがある
  - 通常は併用する
- 最近はフィッシングPhishing検出機能なども持っている

「パターン認識」の限界

- ウィルス対策ソフトやスパイウェア対策ソフト、IDS（侵入検知システム）などの多くは基本的に「パターンファイル」を用いて侵入を検出
  - パターンファイルは、いずれかの組織やハニーポットへの侵入結果から、そこで利用されたマルウェアそのものまたは通信の特徴を抽出して作成
    - 脆弱性が明らかな場合には、脆弱性そのものを狙うプログラムの特徴を利用できる場合もある
  - つまり「どこにも侵入したことがない」マルウェアは原理的に捕らえることが困難
    - 特に既知の脆弱性を利用していない場合は絶望的

マルウェア数の爆発と被害深刻化

- 近年マルウェアの発生数が爆発的に増加
  - マルウェアのなかでもランサムウェアが増えてきた
- もはや「パターンファイル」では維持できない？
  - 大規模感染が確認されない限りパターンファイルに取り入れられない状態
  - マルウェアの変化があまりに早すぎて追いつけない
  - 標的型も増えている　OfficeだけでなくPDFも・・・
- ブラックリストの時代は終わった？
  次はホワイトリスト？
  AIによる予測？

最近の動向を知るには？

例えばセキュリティ会社 F-Secureが出しているレポート

- F-Secure State of Cyber Security

まとめ・何故「監視」が重要なのか

- いわゆるウイルス対策ソフトウェア（Anti-Virus Software)はあまり効果的ではなくなってしまった
  - 攻撃者の能力が上がっている
  - 攻撃者が「成功するまで繰り返す」ようになっている
- なので組織を守るためには…
  - Computer単体でマルウェア（Malware）を検出するのでは不十分
    なのでネットワーク（Network）でも検出するなど
    さまざまな手法で何度も「検知」「検出」をする必要がある
    （日本語では多層防御　英語ではDefense-in-depth　中国語は？）
  - それでも攻撃されてしまった場合には、
    「監視」と「記録」を徹底しておき
    高い能力を持った人(Forensic analyst, Investigator)が
    侵入の早期にそれを発見して対処することが求められている

個人の意識はとても大切

- 犯罪に使える（金になる）と判って以来
  みなさんのパソコンは狙われている
- 「PCには大したものは入ってないから大丈夫」は
  みんなの迷惑
  - Botnetみたいな話もある
  - パスワード・メールアドレスだけでも「お金になる」
- まずは絶対マルウェア対策(Anti-virus)を入れる・最新に
- WindowsUpdateは絶対にする
  - Adobe等のSoftwareのアップデートも「必ず」する
- 怪しいサイトに行かない
  怪しいソフト（特にP2Pファイル交換）は使わない