Windowsシステムの調査訓練座学

訓練概要

- 目的
  - 侵入されたシステムのログやコマンド実行結果から、侵入の痕跡を調査できること
- 種別
  - 調査・解析
- 前提知識
  - Windowsコマンド、Linuxコマンド
- 習得技術
  - ログ分析技術
- 対象
  - 防護隊員

調査前に用意するもの

- Sysinternals Suite
  - Microsoft社製のトラブルシューティングユーティリティ
  - 外部記録媒体に保存し、調査対象マシン上で実行
- 調査解析用プラットフォーム
  - SIFT Workstation、DEFT Linux など
  - 調査対象マシンで取得したログデータを解析するための環境

注意：インシデント発生マシンに与える影響を極力抑える

- ツールは外部記録媒体から実行する
- 生成されるファイルは外部記録媒体に保存する

Windowsシステムにおける情報取得

1. コマンド実行結果の取得（揮発性の高い情報を優先的に取得する）
   - OS標準コマンド
   - Sysinternalsコマンド
2. メモリの保全（インシデント発生時からシャットダウンをしていない場合）
   - FTK Imager など
3. HDDの保全
   - FTK Imager、dcfldd など
4. イベントログの取得
   - wevtutil、psloglist など

Windows コマンド

WindowsシステムのOS標準コマンド

- OS標準コマンドとは
  - OSに付属しているコマンド
  - コマンドプロンプトから実行可能
  - GUIによる情報取得操作よりも処理が軽いため高速
  - Microsoft Technet コマンドラインリファレンス
    - <http://technet.microsoft.com/ja-JP/library/cc754340.aspx>

種別	例
ファイル情報	dir, tree など
システム情報	systeminfo, hostname など
サービス情報	sc, schtasks など
プロセス情報	tasklist など
ネットワーク情報	ipconfig, netstast など
レジストリ情報	reg など

ファイル情報取得コマンド

取得できる情報	コマンド
作成日時	dir C:¥ /S /OD /TC
更新日時	dir C:¥ /S /OD /TW
アクセス日時	dir C:¥ /S /OD /TA
フォルダ構造をツリー形式で表示	tree C:¥ /F /A
隠し属性ファイル	dir C:¥ /S /A:H /T:A
最近オープンしたファイル	dir %AppData%¥Microsoft¥windows¥Recent
プリフェッチ	dir %SystemRoot%¥prefetch

システム情報取得コマンド

取得できる情報	コマンド
システム情報	systeminfo
ホスト名	hostname
ドメイン情報	net config rdr
ユーザアカウント	net user
グループ	net localgroup
グループ（ドメイン）	net group
アカウント設定	net accounts
アカウント設定（ドメイン）	net accounts /domain
監査ポリシー設定	auditpol /get /category:*

サービス情報取得コマンド

取得できる情報	コマンド
インストールされたサービス	sc queryex
起動中のサービス	net start
スケジュールされたジョブ一覧	at
スケジュールされたタスク一覧	schtasks /Query /FO LIST /V

プロセス情報取得コマンド

取得できる情報	コマンド
プロセス	tasklist /v
プロセスに対応したサービス	tasklist /svc

ネットワーク情報取得コマンド

取得できる情報	コマンド
ネットワークインターフェース設定	ipconfig /all
DNS キャッシュ	ipconfig /displaydns
ARP キャッシュ	arp -a
ルーティング	route print, netstat -rn
コネクションおよびリッスンポート（名前解決あり）	netstat -a
コネクションおよびリッスンポート（名前解決なし）	netstat -an
コネクションおよびリッスンポート（名前解決なし、関連するPID）	netstat -ano
コネクションおよびリッスンポート（名前解決なし、関連する実行ファイル）	netstat -anb
NetBIOS名	nbtstat -n
NetBIOSキャッシュ	nbtstat -c
NetBIOSセッション	nbtstat -s
共有リソースへの接続一覧	net use
ドメイン内のコンピュータリスト	net view
セッション一覧	net session
共有リソース一覧	net share
サーバで開いてるファイル一覧	net file

レジストリ情報取得コマンド

取得できる情報	コマンド
システム開始時に自動起動されるプログラム	reg query HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run /S
システム開始時に自動起動されるプログラム（1回のみ）	reg query HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnce /S
「名前を指定して実行」の履歴	reg query HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥RunMRU /S

Sysinternalsコマンド

- Sysinternalsとは
  - Windows のプロセスやファイル アクセスの状態を把握するための様々なツール
  - Windows標準のタスク マネージャーでは調べられない、より詳細な情報を取得可能
  - Microsoft社より無償で提供されている
- Sysinternals Suiteとは
  - Sysinternalsのトラブルシューティング用ツール集
  - <http://technet.microsoft.com/ja-jp/sysinternals/bb842062>

Sysinternalsコマンド

取得できる情報	コマンド
システム情報	psinfo -d -s -h
サービス	psservice
ログイン中のユーザ	psloggedon
イベントログのダンプ（システム）	psloglist -s system
イベントログのダンプ（アプリケーション）	psloglist -s application
イベントログのダンプ（セキュリティ）	psloglist -s security
NTFS ボリューム	ntfsinfo C
リモートからアクセスしているファイルやフォルダ	psfile
自動的に起動するよう構成されているプログラム	autoruns
実行中のプロセス	pslist
実行中のプロセスが読み込んでいるモジュール	listdlls
プロセスで開かれているハンドル	handle -a

イベントログ調査

イベントログ

- イベントとは
  - Windowsにおいて、ユーザーに通知するかログに記録する必要のある、システムまたはプログラム上の重要な問題のこと
- Windowsでは主に3つのログに記録される
  （予め指定した監視イベントのみが記録される）
- イベントログの保存場所
  - %Systemroot%¥System32¥Config（Windows 2000/XP/2003）
  - %Systemroot%¥System32¥winevt¥Logs（Windows Vista/2008/7）

ログ	記録されるイベント	イベントの例
アプリケーションログ	プログラムによって記録されたイベント	データベースプログラムのファイルエラー
セキュリティログ	ログオン、ログオフイベント リソース使用関連のイベント	ユーザのログオン ファイルの生成、削除
システムログ	システムコンポーネントによって記録されたイベント	起動中のドライバ読み込みエラー

イベントログの見方

- イベントのヘッダには下表の情報が付加される

項目	概要
日付	イベントが発生した日付
時間	イベントが発生した時刻
ユーザ	イベント発生時にログオンしていたユーザのユーザ名
コンピュータ	イベントが発生したコンピュータ名
イベントID	イベントの種類を示すイベント番号
ソース	イベントのソース プログラム名、システムコンポーネント名、または大きなプログラムの個々のコンポーネント名を指す
種類	イベントの種類 エラー、警告、情報、成功の監査、失敗の監査のいずれか
カテゴリ	イベントソースによるイベントの分類

イベントの種類

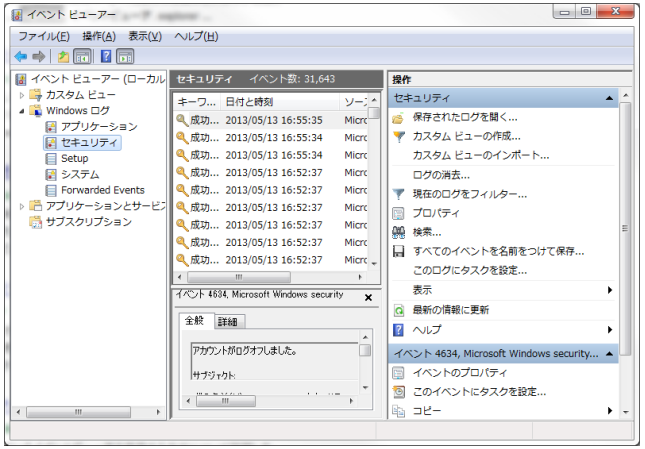
- ログに記録されるイベントの説明はイベントの種類によって異なる

ログのイベントの分類

イベントの種類	概要
情報	アプリケーション、ドライバ、サービスなどのタスクの成功した操作を記述するイベント
警告	必ずしも重大でないが、将来問題になる可能性のあるイベント
エラー	クリティカルタスクの失敗など重大な問題を記述するイベント
成功の監査	監査対象のセキュリティイベントが成功したことを示すイベント
失敗の監査	監査対象のセキュリティイベントが成功しなかったことを示すイベント

イベントビューア

- OSに付属しているGUIツール
- evtx, evt形式のログを参照・保存可能
- csv形式でも保存可能だが、集計や検索には不向き
- 処理が重く、参照に時間がかかる
- 起動方法
  - コントロールパネル -> 管理ツール -> イベントビューアー
  - 「ファイル名を指定して実行」->「eventvwr」を入力して実行



wevtutil

- OSに付属しているCUIツール
- evtx, evt形式のログを参照・保存可能
- csv形式でも保存可能だが、フォーマットが特殊なため集計や検索には不向き

- コマンド例
  - helpの表示

    ```
    > wevtutil /?
    ```

  - セキュリティログをsecurity.evtxに保存する

    ```
    > wevtutil epl security security.evtx
    ```

psloglist

- Sysinternalsのツール
- 集計や検索に適したCSV形式でログを保存可能

- コマンド例
  - helpの表示

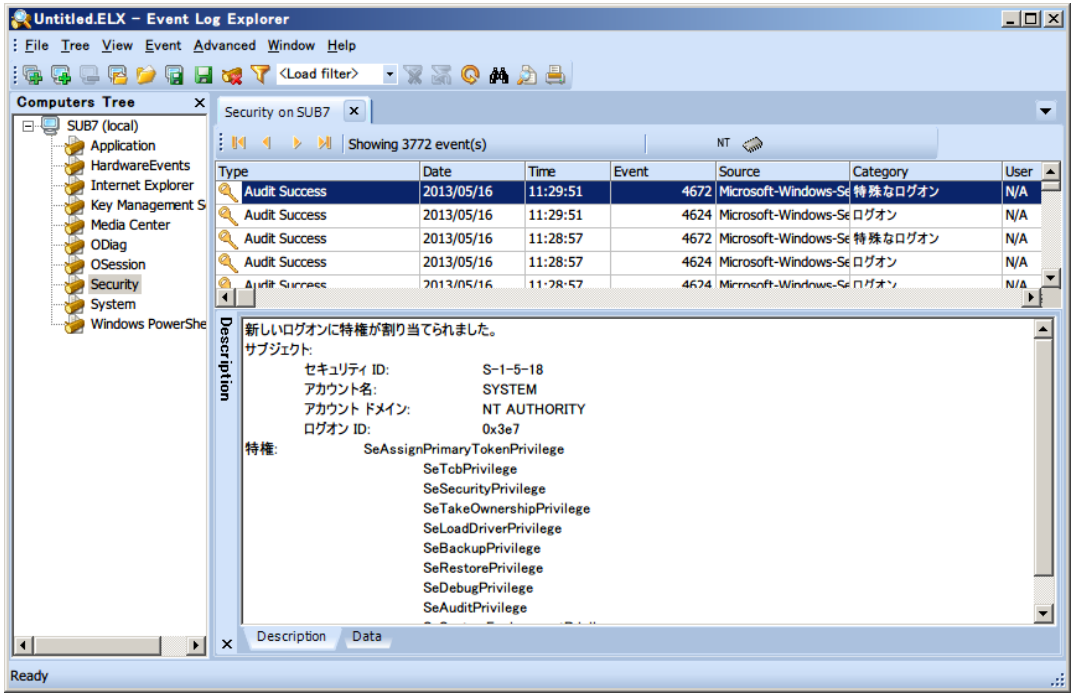
    ```
    psloglist –h
    ```

  - セキュリティログをsecurity.csvに保存する

    ```
    psloglist –s security > security.csv
    ```

Event Log Explorer

- イベントログ参照ツール
- イベントビューアよりも動作が軽い
- 保存したログファイル（EVTX）を参照することも可能



イベントログの調査手順例

- 手順例①
  1. イベントログをevtx形式で保存（wevtutil）

```
> wevtutil epl application application.evtx
> wevtutil epl security security.evtx
> wevtutil epl system system.evtx
```

  2. evtx形式のファイルからイベントを検索
     （Log Parser、Event Log Explorer など）

- 手順例②
  1. イベントログをcsv形式で保存（psloglist）

```
> psloglist –s application > application.csv
> psloglist –s security > security.csv
> psloglist –s system > system.csv
```

  2. csvファイルからイベントを検索（Excel、シェル等）

注目すべきイベントログ

大項目	小項目	イベントID (2000/XP)	イベントID (Vista/2008/7)
ログオン	成功	528, 540	4624, 4636
	失敗	529-537, 539	4625-4633, 4635
ログオフ	成功	538, 551	4634, 4647
アカウント	作成	624	4720
	有効	626	4722
	変更	642	4738
	無効	629	4725
	削除	630	4726
パスワード変更	自身で変更	628	4724
	他のユーザが変更	627	4723
サービス	開始	7035, 7036	7035, 7036
	停止	7035, 7036	7035, 7036
オブジェクトアクセス	失敗	560, 567	4656, 4663

The Sleuth Kit (TSK)

The Sleuth Kit (TSK)

- The Sleuth Kit とは
  - オープンソースのフォレンジックソフトウェア
  - ファイルシステム解析用のプログラムセット
  - ファイルシステムのレイヤに対応したコマンド構成
- 主な機能
  - ファイルシステムの内部情報の調査
  - キーワード検索
  - ファイル復元
  - ファイル識別
  - ハッシュデータベース検索
  - タイムライン解析

NTFS ファイルシステムの概要（1）

- クラスタ
  - NTFS が読み書きする最小単位
- MFT(Master File Table) によってファイルやディレクトリを管理
  - MFT のレコードサイズは 1kb ～ 4kb
  - MFT の最初の 16レコードは予約されている
  - MFT のレコードヘッダは FILE, BAAD で始まる
- MFT は複数の属性を持つ
  - STANDARD_INFORMATION
  - FILE_NAME, DATA

NTFS ファイルシステムの概要（2）

- Alternate Data Stream (ADS) 機能
  - type malware.exe > example.txt:malware.exe
  - start “example.txt:malware.exe”
- レコードデータタイプ
  - レコード内にデータを持つものをレジデント(Resident)
  - レコード外のクラスタにデータをもつものを非レジデント(Non-Resident)
- タイムスタンプ情報
  - STANDARD_INFORMATION、FILE_NAME
  - Vista 以降はパフォーマンスのために、アクセス時刻を更新しない（OSの設定）

TSK - プログラム（1）

レイヤ	プログラム名
メディア マネージメント	mmstat, mmls, mmcat
ファイルシステム	fsstat
ファイルネーム	fls, ffind
メタデータ	ils, istat, icat, ifind
データ	blkcat, blkls, blkcalc, blkstat

TSK - プログラム（2）

- 自動化ツール

用途	プログラム名
ファイルの抽出	tsk_recover
タイムラインの作成	tsk_gettimes
ディレクトリ階層の比較	tsk_comparedir
メタデータ情報を SQLite データベースに格納	tsk_loaddb

TSK - プログラム（3）

- ユーティリティ

用途	プログラム名
文字列検索	srch_strings
バイナリシグネチャ検索	sigfind
ファイル識別	sorter
ハッシュデータベース	hfind
タイムライン作成	mactime

タイムライン分析

タイムライン分析

- ファイルのタイムスタンプ（MAC Time）を時系列に整理し、侵入者が行った痕跡を調査分析
- ファイル・タイムスタンプの種類（MACB）
  - M　　：File Modified（最終修正時刻）
  - A　　：Accessed（最終アクセス時刻）
  - C　　：Inode Changed（最終inode変更時刻）
  - B　　：File Birth（ファイル作成時刻）
- 注意事項
  - タイムスタンプは最終の時刻
  - 改ざんされている可能性もある
- ログなどの他の情報と合わせて総合的に分析

タイムスタンプの変化（NTFS）

MACB	File Modified	Accessed	MFT Modified	Created
作成	○	○	○	○
更新	○	―	○	―
読み込み・実行	―	○	○	―
コピー	―	○	○	○
移動（ボリューム内）	―	―	○	―
移動（ボリューム外）	―	○	○	―
削除	―	―	―	―

- STANDARD_INFORMATION 属性のタイムスタンプ
- OS設定 やアプリケーション動作やキャッシュの有無等によって変わる

タイムスタンプの変化（EXT2/3）

MACB	File Modified	Accessed	i-node Modified	File Birth
作成	○	○	○	―
更新	○	―	○	―
実行	―	○	―	―
パーミッション等の変更	―	―	○	―
コピー	○	○	○	―
移動	―	―	○	―

- EXT2/3にB Timeはない
- ファイルシステムの種類によって異なる
- アプリケーション動作やキャッシュの有無等によって変わる

The Sleuth Kit による タイムラインの作成

- fls
  - ディスクイメージからファイル、ディレクトリ名を表示する
- mactime
  - ファイルアクティビティのタイムラインをASCIIで作成する
- タイムライン作成手順
  1. body ファイルの作成
     fls –m mountpoint –rp image-file > bodyfile
  2. body ファイルをタイムラインに変換
     mactime –y –m –d –b bodyfile > timeline-file
  3. タイムラインをエクセルなどで開いて調査

タイムラインの例

日時	サイズ	MACB	パーミッション	UID	GID	inode番号	ファイル名
Sun Dec 10 2006 06:10:45	87500	.a..	r/rrw-r--r--	10000	10000	16418	/home/admin/.bash/lang/english.lng
	4096	m.c.	d/drwxr-xr-x	10000	10000	384932	/home/admin/.bash
	4096	m.c.	d/drwxr-xr-x	10000	10000	384934	/home/admin/.bash/log
	444848	.a..	r/rrwxr-xr-x	10000	10000	385156	/home/admin/.bash/ntpd
	76	.a..	r/rrw-r--r--	10000	10000	385167	/home/admin/.bash/psybnc.conf
	204	mac.	r/rrw-------	10000	10000	385171	/home/admin/.bash/log/psybnc.log
	6	mac.	r/rrw-------	10000	10000	385172	/home/admin/.bash/psybnc.pid
Sun Dec 10 2006 06:25:34	22936	.ac.	r/rrwxr-xr-x	10000	10000	161906	/home/admin/adv/kswap.help

log2timeline

- 様々なファイルが持っているタイムスタンプをパースして、時系列に出力するツール
- 使用例

  log2timeline –f format –w output-file –r mountpoint
- 下記の入力フォーマットに対応している
  - Apacheログ
  - Squidログ
  - ブラウザ閲覧履歴
  - イベントログ
  - 削除ファイル　　など

  log2timeline –f list # フォーマット一覧を表示する

Volatility によるメモリ解析

メモリ解析手法

- 文字列検索
  - メモリ内の読み取り可能な文字列を抽出
- List Traversal
  - OSが行う手順でメモリ内の構造体から情報を抽出
- Pattern Search
  - 構造体の特徴（シグネチャ）を元に、メモリ内の構造体を探し出して情報を抽出
  - OSが管理していない情報も抽出可能

Volatility

- Volatility とは
  - オープンソースのメモリフォレンジックプラットホーム
  - プラグインを追加することで機能追加が可能
  - List Traversal，Pattern Search の解析手法に対応
- 使用方法

  # vol.py --profile=profile –f image-file plugin

  # vol.py –h　オプションなどのヘルプを表示

  # vol.py --info プロファイルやプラグインの一覧などを表示
- 使用例

  # vol.py --profile=Win2008SP2x86 -f winsvr2008.001 psscan

Volatility プラグイン（1）

List Traversal	Pattern Search	概要
pslist	psscan	実行プロセス
connections (xp,2003)	connscan (xp,2003)	ネットワーク接続
sockets(xp,2003)	sockscan (xp,2003)	オープンソケット
―	netscan (vista,2008,7)	ネットワーク接続、オープンソケット
―	filescan	オープンファイル
modules	modscan	モジュール

SIFT2.12 の Volatility Framework 2.1_alpha に収録されているプラグイン

Volatility プラグイン（2）

プラグイン	概要
dlllist	ロードしている DLL ファイル
hivelist	メモリ上のハイブのアドレスを表示
printkey	指定したレジストリキーを表示
procexedump	実行ファイルのダンプ
psxview	pslist, psscan の結果を比較することで隠されたプロセスを検出
vadinfo, vaddump	メモリにマップされたファイルやデータの情報を表示、ダンプ
malfind	コードインジェクション等の検出
apihooks	APIフックの検出

SIFT2.12 の Volatility Framework 2.1_alpha に収録されているプラグイン

ネットワーク調査

通信ログの解析

- 通信ログ調査ツール
  - WireShark、tshark、ngrep など
- ngrepコマンド例

  ngrep -I dump.pcap strings

  # 「strings」文字列を含むパケットを検索

  ngrep -I dump.pcap port 80

  # 80番ポートのパケットを検索