MWS Cup 2012 課題1
「インシデントレスポンス」の解き方のヒント

2012 年 9 月 14 日（金）
MWS Cup 2012 企画担当

シナリオ

- あなたは某社でフォレンジックによるインシデントレスポンスを行うエンジニア。ある日、顧客から「弊社の機密情報がなぜか漏洩している。原因を調べてほしい」との依頼を受ける。あなたが独自に調査したところ、本来機密情報である文書ファイル（ファイルサーバ上で管理していたファイル）の一部がインターネット上に漏洩していることを確認。この顧客のネットワークを詳細に調査することになった。あなたは手始めに、機密情報の入っていたファイルサーバのアクセスログを調べたところ、本来アクセスを許可されていないユーザの所有する端末から、このユーザが知るはずのない別のアカウントを使って当該ファイルへのアクセスが成功しているログが発見されたため、このユーザの所有する端末をまず調査することになった。
- この顧客は専任のネットワーク管理者がおらず、開発を行う社員が管理者を兼ねていたため、厳格な管理がされていなかった。ファイヤウォールは存在していたもののログはとられておらず、ネットワーク機器のログから調査を行うことは不可能だったため、あなたは調査手法として、フォレンジックによる端末の詳細調査を提案した。その際、端末は既に電源オフの状態だったため、揮発性情報の取得を行わず、ハードディスクイメージを証拠として保全して持ち帰り、調査を開始することにした。

サーバ構成

ドメインコントローラ（DC）	Windows Server 2008 R2 SP1
ファイル共有サーバ	Windows Server 2003 R2 SP2
mail server	Linux, postfix
web server	Windows Server 2003 R2 SP2, IIS
Client A（今回配布する HDD イメージ）	Windows 7 SP1
Client B（ドメイン管理者利用 PC）	Windows XP SP3
Client C	Windows Vista SP2

ツール、解き方について

- 出題者は利用を想定しているフォレンジック分析環境（SANS SIFT Forensic Workstation）が、以下の環境下で動作することを確認しています。
  - Ubuntu 12.04, VMware Workstation 8
  - Windows7 SP1, VMware Workstation 8
  - Windows7 SP1, VMware Player 4.0
- 一部 Windows マシンでの分析作業もあります。Windows 7 、もしくは Windows 2008 R2 もご用意ください。
  - 分析時は二次感染を防ぐために VM などを利用し、隔離されたネットワークでご利用ください。

解き方のヒント

- ツールの指定はありません。フォレンジックの経験、知識のある方は注意点に反しない限りにおいて、ご自身の好きなツールを利用ください。
- フォレンジック未経験の方は、以降で挙げるツールや情報を参考に、解析を行ってみてください。フォレンジックはファイルシステムのファイルやディレクトリなどのタイムスタンプからタ

イムラインを作ることで、その端末でいつ、どのような操作が行われたかを把握するのが基本です。タイムライン作成は SANS SIFT Forensic Workstation に付属している log2timeline-sift を用いて行ってみてください。作業手順等も次ページの URL に記載されています。その他紹介しているツールは、適宜必要に応じて使用してみてください。

例題

- フォレンジックに慣れるための例題として、以下のようなものがありますので、これらを参考に、事前に体験してみるのもいいのではないかと思います。
  - http://www.cfreds.nist.gov/Hacking_Case.html
  - http://www.forensickb.com/2008/01/forensic-practical.html
  - http://www.forensickb.com/2008/01/forensic-practical-2.html
  - http://www.honeynet.org/challenges
- また、ご自身で意図的にマルウェアに感染させたり、脆弱性を使って任意のコード実行などを行った HDD イメージを VM 上で作り出してみて、どのような結果が得られるかなどを検証してみるのもいいと思います。

ツール、情報（フォレンジック分析）

- フォレンジック分析用 OS
  - SANS SIFT Forensic Workstation
    http://computer-forensics.sans.org/community/downloads
- タイムライン作成
  - log2timeline-sift
    blogs.sans.org/computer-forensics/files/2012/06/
    SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf
    http://computer-forensics.sans.org/blog/2011/12/16/
    digital-forensics-sifting-cheating-timelines-with-log2timeline
    http://computer-forensics.sans.org/blog/2011/12/07/
    digital-forensic-sifting-super-timeline-analysis-and-creation
    http://computer-forensics.sans.org/blog/2011/11/30/
    log2timeline-plugin-creation
  - log2timeline
    http://code.google.com/p/log2timeline/
  - log2timeline-sift で、タイムライン生成時に $fn（$filename）タイムスタンプも生成するための変更箇所
    http://list-archives.org/2012/07/10/dfir-lists-sans-org/
    log2timeline-vs-log2timeline-sift/f/4359338113
- ファイルシステム解析
  - Digital Forensic Framework
    http://www.digital-forensic.org/
  - TSK
    http://www.sleuthkit.org/
- プログラムの実行履歴解析
  - Prefetch Parser
    http://computer-forensics.sans.org/blog/2010/02/12/prefetch-parser-v1-4/

    - ShimCacheParser
      https://github.com/mandiant/ShimCacheParser
- ボリュームシャドーコピー解析
    - vssadmin, mklink
      http://www.forensicswiki.org/wiki/Mount_shadow_volumes_on_disk_images
      http://computer-forensics.sans.org/blog/2008/10/10/shadow-forensics/
    - VSC Toolset
      http://dfstream.blogspot.jp/p/vsc-toolset.html
    - TSK
      http://windowsir.blogspot.jp/2011/01/accessing-volume-shadow-copies.html
      http://computer-forensics.sans.org/blog/2011/09/16/
      shadow-timelines-and-other-shadowvolumecopy-digital-
      forensicstechniques-with-the-sleuthkit-on-windows
- レジストリ解析
    - Registry Decoder
      http://www.digitalforensicssolutions.com/registrydecoder/
    - KaniReg
      http://www.ji2.co.jp/forensics/tools/index.html
- IE キャッシュ、閲覧履歴解析
    - IECacheView
      http://www.nirsoft.net/utils/ie_cache_viewer.html
    - IEHistoryView
      http://www.nirsoft.net/utils/iehv.html
    - Web historian
      http://www.mandiant.com/resources/download/web-historian
- 自動で実行される実行ファイルの列挙
    - Autoruns
      http://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx
- Windows 上で raw（dd）イメージをマウント（autoruns などの実行の際に必要）
    - FTK Imager
      http://accessdata.com/support/product-downloads
    - OSFMount
      http://www.osforensics.com/tools/mount-disk-images.html
- イベントログ解析
    - イベントビューア
    - Event Log Explorer
      http://www.eventlogxp.com/
- HDD イメージ変換
    - qemu-img
      https://access.redhat.com/knowledge/docs/ja-JP/
      Red_Hat_Enterprise_Linux/5/html/Virtualization/
      sect-Virtualization-Tips_and_tricks-Using_qemu_img.html

- FTK Imager
  http://accessdata.com/support/product-downloads
- vhdtool
  http://archive.msdn.microsoft.com/vhdtool

ツール、情報（コード解析（動的解析））

- ファイル入出力、プロセスの動作解析
  - process monitor
    http://technet.microsoft.com/ja-jp/sysinternals/bb896645.aspx
  - process explorer
    http://technet.microsoft.com/ja-jp/sysinternals/bb896653.aspx
  - process hacker
    http://processhacker.sourceforge.net/
  - captureBAT
    http://www.honeynet.org/node/315
  - API Monitor
    http://www.rohitab.com/apimonitor
- レジストリ、ファイルシステム差分取得
  - regshot
    http://sourceforge.net/projects/regshot/
- パケット解析
  - Wireshark
    http://www.wireshark.org/
- エミュレーションサーバ
  - InetSim
    http://www.inetsim.org/
  - FakeNet
    http://practicalmalwareanalysis.com/fakenet/

ツール、情報（コード解析（静的解析））

- コード解析（EXE(PE)、shellcode）
  - CFF Explorer
    http://www.ntcore.com/exsuite.php
  - IDA Pro 5.0 Free
    http://www.hex-rays.com/products/ida/support/download_freeware.shtml
  - OllyDbg
    http://www.ollydbg.de/
  - Immunity Debugger
    http://debugger.immunityinc.com/
  - libemu
    http://libemu.carnivore.it/
  - Malzilla
    http://malzilla.sourceforge.net/

- バイナリエディタ
  - FileInsight
    http://www.mcafee.com/us/downloads/free-tools/fileinsight.aspx
- Javascript 解析
  - jsunpack-n
    https://code.google.com/p/jsunpack-n/
  - Revelo
    http://www.kahusecurity.com/2012/revelo-javascript-deobfuscator/
  - Malzilla
    http://malzilla.sourceforge.net/
- PDF 解析
  - http://computer-forensics.sans.org/blog/2011/05/04/
    extract-flash-from-malicious-pdf-files/
  - PDF Stream Dumper
    http://sandsprite.com/blogs/index.php?uid=7&pid=57
    http://blog.zeltser.com/post/3235995383/
    pdf-stream-dumper-malicious-file-analysis
    http://www.kahusecurity.com/2011/pdf-analysis-using-pdfstreamdumper/
  - peepdf
    http://eternal-todo.com/tools/peepdf-pdf-analysis-tool
- MS Office ドキュメント解析
  - OfficeMalScanner
    http://www.reconstructer.org/code.html
  - offvis
    http://www.microsoft.com/en-us/download/details.aspx?id=2096
- Flash 解析
  - SWFTOOLS
    http://www.swftools.org/
    http://securitylabs.websense.com/content/Blogs/3165.aspx
  - SWFREtools
    https://github.com/sporst/SWFREtools/
    http://www.google.co.jp/search?q=malicious+swf+analysis
    &ie=utf-8&oe=utf-8&hl=ja&client=ubuntu&channel=fs
  - SWFInvestigator
    http://labs.adobe.com/technologies/swfinvestigator/
  - PDF Stream Dumper
- JAVA 解析
  - jad
    http://www.varaneckas.com/jad/
  - Jd
    http://java.decompiler.free.fr/?q=jdgui