“sandnet”

tessy @ チームチドリ
www.t-dori.net

チーム チドリ
http://www.t-dori.net/

malwareの解析と問題

- あやしいファイルの解析……仮想環境
- 最近のmalware傾向……解析回避機能
  - 仮想環境（VMwareなど）を検知し動作停止
  - デバッガーを検知し動作停止
- 実機での動作確認が一番？
- ただし汚染された環境を直すのが面倒

TRUMAN

- LURHQ提供のmalware解析用仮想NW
- The Reusable Unknown Malware Analysis Net
  - http://www.lurhq.com/truman/
- Author(s): Joe Stewart
  - http://www.joestewart.org/

Shmoocon2006、Codecon2006などで発表されたらしいが資料が公開されていないので．．．．とりあえずいじってみる

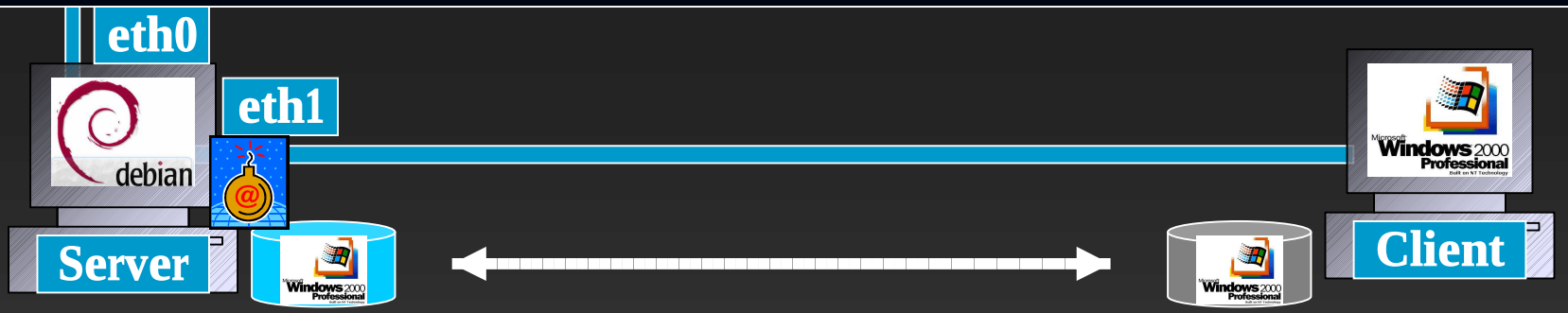
PXE Linuxを利用

- PXE (Pre-boot Execution Environment)
  - Intel提唱のネットワークブートの規格
  - PXE 対応NICとPXEサーバ (DHCP、TFTP)
- TRUMANは
  - malwareを実際のWindows上で実行。PXE Linuxを利用しWindows環境を保存、復元。クリーンイメージとの比較で解析を行うシステム

起動モード

- TRUMAN起動モード
  - 1 save & restore (Windows ディスクの保存、復元)
  - 2 normal boot　(Windows 起動)
  - 3 save only
  - 4 restore only
  - 5 maint

環境概要



・PXE Linux Server（DHCP,TFTP)

・仮想DNS, FTP, IRC, MySQL, SMB, SMTPサーバ
・通信データキャプチャ

・事前の取得データとの比較解析
・通信データの解析

・PXE Linux Client

・ディスクイメージの保存

・Serverからmalwareを取得し実行

・メモリダンプをして再起動(10分後)

・再度Linuxでディスクイメージ保存、復元

チーム チドリ

インストール

truman
- ├──etc　(サービス起動スクリプト、DHCP設定)
- ├──fauxservers　(仮想サーバ)
- ├──forensics　(解析用ファイル、解析済みファイル保存)
- ├──images　(Client環境のイメージ保存)
- ├──mnt　(取得イメージのマウントポイント)
- ├──tftpboot　(PXE Linuxイメージ)
- ├──usr　(cgiファイル、)
- │
- └──win32　(Client用 dd.、wget。起動バッチ)

Server
/直下にコピー
rcスクリプトを調整

Client
c:¥にコピー

その他：perl,apache,atftpd,dhcpd,xinetd,tcpdump,ngrep が必要

Windows環境ではSysinternalsのpsshutdown必要

解析

- 事前イメージと実行後イメージの比較
- mirkes.de – dumphive (registry dump)
  - http://www.mirkes.de/en/delphi/samples/dumphive.php
- SecCheck (Windows forensic tool)
  - http://www.mynetwatchman.com/tools/sc/

:

あとはお好みで

(個人的)ハマリポイント

- TFTPサーバが(inetdで)うまく動かなかった
- ファイルのダンプがうまく動かない
  - ddsave 45611/tcp
  - ddrestore 45612/tcp
- c:¥zero.txt ってなんだろ？(解析ファイルのsandnet.exeと比較している(詳細不明中)
- Linuxのディスク容量は多めに(Windowsのドライブ×2は最低)

:

おわり

チーム チドリ

http://www.t-dori.net/