卒業論文に向けて(6)

学部4年生
島本 大輔
2005年1月17日

1

概要

- 卒論内容
- 進捗
- 異常検知部分について
- 予定

2

卒論内容

- Windows 版 IDS
  - System Service の記録で検出
    - System Service = UNIX 系の System Call
  - SYSENTER を使って Intercept
    - 問題発生

3

概要

- 卒論内容
- 進捗
- 異常検知部分について
- 予定

4

進捗

- Interceptionに問題発生
  - 多量のログがあふれてシステムが落ちる
- 異常検知するパターンをどうするか
  - 既存のウィルスの動作を調査中
  - Process ID を使うのか

5

概要

- 卒論内容
- 進捗
- 異常検知部分について
- 予定

6

異常検知部分について

- System Service のパターンから判断
  - 例
    - レジストリへの書き込みが頻繁
    - ファイルを検索している
    - 勝手にポートでlistenしている
    - 大量にパケットを送信している、など

7

ウィルスやワームの傾向

- ファイルを検索して、書き換える
  - よく行っている
  - 昔からのパターン
- ファイルを検索して、検索している
  - メールアドレスの検索のため

8

概要

- 卒論内容
- 進捗
- 異常検知部分について
- 予定

9

予定

- プログラムを仕上げる
  - 最低、単純な動作のウィルスでも検知するように
- 論文を書く

10