INSec#10 ネットワークの防御

攻撃の検知と防御

要素技術

ファイアウォール

導入と設置

機能

- 侵入検知システム(IDS：Intrusion Detection System)
  - ネットワーク型：NIDS
    - トラフィック監視
    - 技術：パターンマッチング
    - 対象：通信
    - 例：空港の監視カメラ
  - ホスト型：HIDS
    - 運用違反、異常反応…運用監視
    - 技術：パターンマッチング
    - 対象：システム・OSのログ
    - 例：空港の入国管理
  - シグネチャ：既知の攻撃パターン情報
- 侵入防御システム(IPS：Intrusion Prevention System)
  - ネットワーク型：NIPS
    - 監視対象ネットワークへの通信遮断
  - ホスト型：HIPS
    - 監視対象ホストへの通信遮断
- NIDS/NIPS
  - 1.侵入検知
  - 2.アノマリ通信検知
    - 正常な通信とは考えにくい通信の検知
  - 3.不正通信へのレスポンス
    - 管理コンソールへの通知機能
    - TCPパケット → セッションの切断機能
    - FWやルータと連動 → 通信遮断
    - NIPS：不正なパターン文字列検知 → 通信遮断
- HIDS/HIPS
  - 1.ユーザ操作検知
  - 2.ファイル改ざん検知
  - 3.ハニートラップ
  - 4.不正操作へのレスポンス
- ハニーポット
  - 仮想的に脆弱なシステムを公開しておくこと
  - 1.攻撃統計調査
  - 2.攻撃者行動調査
  - 3.悪意のあるプログラムの収集
- ファイル改ざんのチェック
  - Tripwire：チェックを行いたいファイルやディレクトリの状態をデータベースとして保存し、システムの現在の状態をデータベースと照らし合わせ、変化がないかを比較するツール
  - ➜ http://www.tripwire.org/

導入と設置

- NIDS/NIPS
  - インターネットとの境界
    - FWの外側設置
      - パフォーマンス
        - Gbit対応？
      - ネットワーク環境
        - 携帯対応…ショートパケットの処理
    - FWの内側設置
      - FWの発信元IPアドレス変換禁止
      - Proxyサーバ内側設置
        - 内部ネットからの脅威検知
  - DMZの監視
    - DMZ内サービス
      - トラフィック量
      - パケットサイズ
    - DMZ内サーバのハートビート(heartbeat)有無
      - 正常稼動を外部に知らせ信号
  - イントラネットの監視
    - ウイルス
    - ワーム
    - …
- 構成
  - 1.プロミスキャス・モード(promiscuous mode)
    - すべてのパケットを受信
    - プロミスキャス=無差別の
  - 2.ステルスモード(stealth mode)
    - NICにIPアドレスを定義しない
  - 3.リピータハブの利用
    - データを電気的に中継するだけ
    - コリジョン発生の可能性
  - 4.スイッチングハブの利用
    - MACアドレスにより特定ポートのみ通信可能
    - SPAN(Switched Port Analyzer)：ポートミラーリングにより多くのセグメント監視
  - 5.IDSタップの利用
    - 双方向の全二重トラフィック解析
  - 6.IDSバランサーの利用
    - 通信を複数のIDSに分散、またその逆も可

検知

- パターンマッチング
  - パケット(ヘッダ＋ペイロード)のペイロード内の文字列検知
  - ASCII文字+16進表記
- アノマリ検知
  - プロトコルアノマリ検知
    - セッションのハイジャック
    - 発信元の偽造通信
    - DoS攻撃(Exploitによる)
  - トラフィックアノマリ検知
    - しきい値の設定による検知
      - コネクション数
      - SYNパケット
      - FINパケット
      - RSTパケット
    - 自動学習機能による検知
  - アプリケーションアノマリ検知
    - 通常では考えられない通信や挙動を検知
    - バッファオーバーフローによる攻撃等
- その他の検知
  - ステートフルシグネチャ検知
    - 通信の一部分対象
  - バックドア検知
    - トロイの木馬、DDoS攻撃プログラム
- HIDS
  - 利用目的：運用管理、変化の確認、観察、侵入検知
  - OSが出力するログ
    - シグネチャ化 → 不正な操作を検知
  - システムログ
    - UNIX：messagesファイル監視
  - OS特有の出力ログ
    - Solaris：Basic Security Module(BSM)
  - イベントログ
    - WindowsOS：システム、セキュリティ、アプリケーション
  - NIDSとの組合せが有効
- ハイブリッド型IDS
  - HIDSをベースに、NIDSの機能を併せ持ったIDS
  - ホストの状態を監視＋パケット監視

IDS・IPSの運用

侵入検知システムの課題