

INSec#10
ネットワークの防御

要素技術
ファイアウォール

- 機能
- 導入と設置
- 検知

攻撃の検知と防御

IDS・IPSの運用

ポリシーの作成とチューニング

- NIDS
 - 1.ネットワーク構成
 - 2.ネットワーク機器の設定情報(FWのACL等含む)
 - 3.実際に流れている通信
 - シグネチャの選定、アノマリ検知機能の調整、ポリシー作成
- HIDS
 - 監視対象：
 - 1.ファイルなどの改ざん
 - 2.不正ログイン
 - 3.不正操作
- ポリシーチューニング
 - 運用効率を高めるために
 - 検知内容のバランスを調整

シグネチャの作成

- 作成方針：
 - 1.脆弱性の内容に則したシグネチャ
 - 2.攻撃手法、攻撃プログラムに則したシグネチャ
- NIDS
 - 1.脆弱性情報に基づいて作成
 - 2.パケットをキャプチャしたデータから作成
 - 3.プログラムのソースコードから作成
- HIDS
 - OSに依存
 - 検知パラメータ
 - ファイルの書き込み
 - ファイルの削除
 - ディレクトリ操作
 - シスログと出力形式パターンの関係把握

ログの運用

- 保存ディスクの容量
- ローテーション
 - WindowsOS : atコマンド
 - UNIX : cron
- バックアップ方針
- ログの分析
 - インターネット境界セグメント
 - 攻撃通信
 - 外部から公開サーバへのメンテナンス情報
 - ワーム通信
 - DMZ
 - Webサーバへの攻撃通信
 - イントラネット
 - ワーム・ウイルス
 - 攻撃通信
 - PSP通信
 - VPNプロトコル
 - チャット

ログの分析方法

- 統計分析
- 相関分析
 - データマイニング：
 - 1.発信元IPアドレス・サービスポート
 - 2.発信先IPアドレス・サービスポート
 - 3.攻撃手法
 - 4.ネットワークアドレス セグメント単位
 - 5.センサー IDSセグメント単位
 - 6.時刻
- イベント分析
 - 攻撃先のホストを絞り込んでいるログ
 - 攻撃を検知したログ
 - ホストへの攻撃が成功したと考えられるログ
- セッション分析
 - トリガーパケットにより

誤検知

- 2つの誤検知：
 - 1.フォルスポジティブ(False Positive) 正常な通信にもかかわらず、不正な通信と判断されてしまった誤検知
 - 2.フォルスネガティブ(False Negative) 不正な通信にもかかわらず、不正な通信と判断されなかった誤検知

侵入検知システムの課題

パフォーマンス Gbpsの時代

- IDS検知妨害
 - snortへの攻撃 : stick, snot
- IPS回避技術
 - レイヤごとの回避
 - L1・2 ハードウェアレイヤ：
 - ネットワークレイヤ：
 - TTLへの細工
 - IPフラグメンテーション 最小フラグメントサイズ：8byte
 - TCPフラグメンテーション
 - L3・4
 - アプリケーションレイヤ：
 - HTTP, FTP, SMTP, DNS
 - DCE/RPC(Distributed Computing Environment / Remote Procedure Calls)
 - 複数のコンピュータ上のソフトウェアをあたかも1つのコンピュータ上で動作しているかのように動作させるRPCシステム
 - SMB(Server Message Block) WindowsOS : ファイル共有、プリンタ共有
 - L5・6・7
 - プロトコル実装上の問題 HTTP Request Smuggling Attack

誤検知 2つの誤検知に対する研究

- アノマリ型IDS
- ハニーポット技術を用いたISD

アプリケーション層の監視および防御

- ISD/IPSが苦手なアプリケーション層への攻撃
- WAF(web application firewall)導入
 - SQLインジェクション 個人情報漏えい
 - 脅威対策
 - クロスサイトスクリプティング 有害サイトへ誘導
 - バッファオーバーフロー 管理者権限盗用・サイト改ざん