

Trap製品調査

2002.12

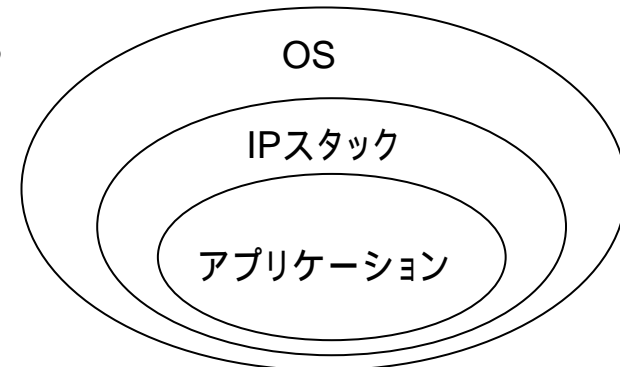
トラップシステムの分類

導入目的での分類

- ・不正侵入検出
 - ・不正侵入検出のトリガとする
 - ・IDSとしての役割
 - ・偽装ホスト、サービスへの接続は不正アクセスである可能性が高い
 - ・対抗措置の実行につなげる - アクセス拒否・PortScanなど
- ・システム防衛
 - ・不正侵入者の攻撃対象を偽装サーバへ誘導し実サーバを防御する
- ・不正侵入手法調査
 - ・不正侵入手法の調査手段とする
 - ・研究機関での用途
 - ・不正侵入の証跡としての用途

ソフトウェアアーキテクチャでの分類

- ・アプリケーション
 - 監視対象のコンピュータ上でサーバプロセスのみを偽装する
 - アプリケーション(Webサーバ等)、OS等のバナー情報や擬似ユーザインタラクティブ機能を提供する
 - TCPWrapper等のスーパーデーモンにより機能実現するものがある
- ・IPスタック
 - 監視対象のコンピュータ上で独自IPスタックを実装し、複数IPを偽装する
- ・OS
 - 監視対象のコンピュータ上でホストOSと同等または別OSを偽装する



機能実現可能範囲

トラップソフトウェアの偽装対象アーキテクチャによる分類

	アプリケーション	IPスタック	OS
長所	<ul style="list-style-type: none">・踏み台になりにくい	<ul style="list-style-type: none">・踏み台になりにくい・1ホストに複数のIPを偽装可能	<ul style="list-style-type: none">・1ホストに複数のホストを偽装可能・ホストに対する全ての攻撃情報を取得可能(不正侵入手法調査に適する)
短所	<ul style="list-style-type: none">・偽装アプリケーション上での情報しか取得できない	<ul style="list-style-type: none">・偽装アプリケーション上での情報しか取得できない	<ul style="list-style-type: none">・踏み台になりやすい

補足

- OSレベルのトラップシステムは次の3つに分けられる
 - 仮想マシンによるOSエミュレート
 - 仮想OSエミュレート
 - ファイルアクセス制限(OS機能)によるOSエミュレート
 - chroot、jailなど
- 保存ログによる分類
 - コマンドログ(アプリケーション上でのコマンド履歴)
 - ネットワークダンプ(パケットダンプ)
- 業界動向
 - ハニーポットとしては仮想マシンによるOSエミュレートを利用したシステム構成が多い。