本資料について

本資料は下記著書を基にして作成されたものです。

著書の内容は保障できないため、正確な知識を求める方は原本を参考にしてください。

著者	ステフィン・ノースカット
	マーク・クーパー
	マット・フィルノウ
	カレン・フレデリック【著】
	武田圭史【監修】
著書名	ネットワーク侵入解析ガイド
出版社	ピアソン・エディケーション
	出版日2001年12月10日

輪講発表

名城大学　理工学部　情報科学科
渡邊研究室
01J078　播磨宏和

ネットワーク侵入解析ガイド

侵入検知のためのトラフィック解析法

Intrusion Signatures and Analysis

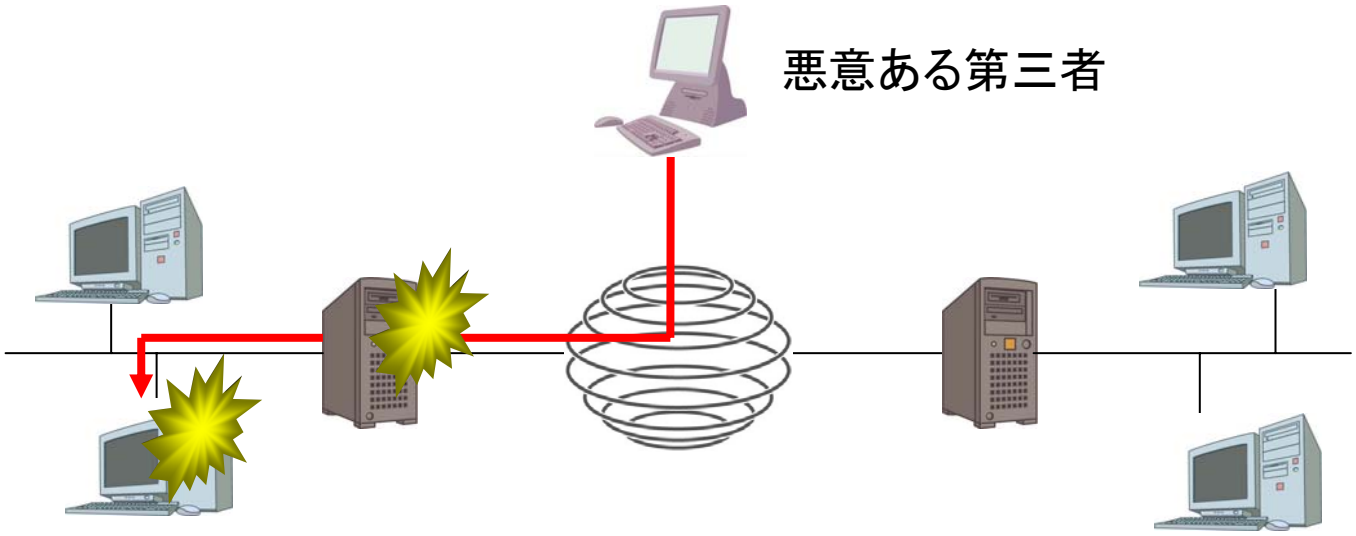
Northcutt Cooper Fearnow Frederick

初めに

コンピュータ同士がネットワークで繋がっていれば悪意ある第三者に侵入される可能性がある

強度なセキュリティを築いていても侵入されないシステムは100%存在しない

侵入の兆候や足跡をログによって見つけることで、攻撃者に対するシステムの破壊やファイルの改ざんを防ぐことができる



ログファイルの解析

- 侵入検知システム（IDS）
- ファイアウォール
- OS等

が生成するログの解析方法について紹介

ログ解析の目標は以下のとおり

- ログファイルを正しく解釈する
- データソースを識別する
- 情報の重要度を評価する

解析方法の流れと概要

1. ログファイル
2. ルールの確認
3. 詐称の有無
4. 攻撃の調査と判別
5. 攻撃の分析
6. 相関分析
7. 標的の調査
8. 重大度
9. 防御策の提案

1.ログファイル

ログファイルは、ある行為（ルール）に基づいて記録される
ただし、記録された内容が全て正確かどうか確かめる必要がある

- フォールスポジティブ（false positive）
  指定した行為ではない行為を不正と検出（誤検出）
- フォールスネガティブ(false negative)
  指定した行為が発生しているにもかかわらず、不正として検出

2.ルールの確認

- ルールは装置ごとに異なる
  - 独特のクセ、加工された情報など
- それぞれの装置を理解する必要がある
- ルールは毎日のように自動的に更新されるものも存在
- 装置の処理能力低下はフォールスポジティブ、フォールスネガティブの発生を招く

3. 詐称の有無

- ログ結果の送信元アドレスは詐称されている場合が多い
- DoS攻撃においては大半が詐称されている
- アドレスが偽造されている場合、一般に偵察行為としては役に立たない

ログの送信元トレース結果の
調査として分けられる3つのカテゴリ

- 偽造されている場合・・・・・サービス妨害（DoS）攻撃
- 偽造されていない場合・・・・・スリーウェイハンドシェイクの完了
- 第三者の可能性がある場合・・・・・サードパーティ効果（デバイスの影響）

4.攻撃の調査と判別

- それぞれの攻撃には特徴がある
- 特徴の情報を公開しているサイトで学ぶことが重要

5.攻撃の分析

- これは刺激なのか、それとも反応なのか
  - SYNフラグが設定されたTCPパケットは刺激
  - SYN-ACKが設定されたTCPパケットは反応
- どのサービスが標的にされたのか
- これは悪意のないものか、エクスプロイトか、DoSか、それとも偵察か

6.相関分析

- 相関分析
- ログファイルを収集し、グラフを作成、相関性を求める
  - 未知の攻撃を発見する
  - 攻撃の規模を把握するのに役立つ
  - フォールスポジティブ、フォールスネガティブを減らす

7.標的の調査

- 攻撃者に直接狙われているのか、標的の一部として狙われているのか調査する
- 特定のホストを標的にした場合はエクスプロイトをついた攻撃が多い
- ネットワーク全体に対する攻撃は、エクスプロイトをついた攻撃ほど重要ではない
- 相手がIPアドレスをうち間違えてもログは生成される可能性がある

8.重大度

- 重大度の計算方法、理解ができるようにする
- 攻撃の重大度を決定する問題の大きさを理解することが重要

例えば

重大度=（重要度+致命度）-（システムの対策+ネットワークの対策）

9.防御策の提案

- 重大度を持つことが確認されたログには、何らかの対応が必要
  - 標的を絞った攻撃が続く可能性がある

最も深刻なインターネットセキュリティの脅威

- Berkeley Internet Name Domain(BIND)
- Common Gateway Interface(CGI)
- リモートプロシージャコール（RPC）
- Microsoft Internet Information Server(IIS)
- Sendmail
- Sadmind,mountd
- ネットワーク経由のファイル共有
- 弱いパスワードが設定されたアカウント
- Internet Message Access Protocol(IMAP),Post Office Protocol(POP)
- Simple Network Management Protocol(SNMP)

おわり