- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。
- 題目：ネットワークセキュリティ HACKS
  ～ プロが使うテクニック＆ツール 100選 ～
- 著者：Andrew Lockhart
- 発行年月日：2005.7.14
- 出版社：オライリー・ジャパン

ネットワークセキュリティのためのテクニック＆ツール

名城大学理工学部
渡辺研究室
050427160　森崎明

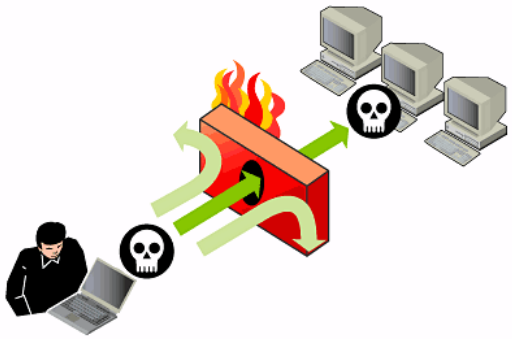
はじめに

- **ネットワークセキュリティとは**
  - コンピュータネットワーク上での安全確保のための防衛策
  - つまり、システム攻撃者からコンピュータを守り、不正アクセスの防止や情報漏洩の阻止、システムの安定性保持を行なうこと

- **セキュリティが甘いネットワークを不正アクセスから守るには、ファイアウォールの設置が効果的**

  （そのほかのセキュリティ対策として、アンチウイルスソフトウェアなどの導入などがありますが、ここでは触れません ）

- **しかし**
  - ユーザーが定めたルールに従って、不必要なアクセスを遮断する（必要なアクセスのみを許可する）のがファイアウォールの仕事であるために許可されたアクセスを利用した攻撃は防げない
  - よって、ファイアウォールは外敵の侵入を防ぐ最初の砦でしかない



適切なセキュリティ対策

- たった1台のセキュアでないシステムが、ネットワークに大きなトラブルを引き起こす原因になる
- そのシステムが攻撃者の制御下に置かれてしまうと、踏み台攻撃と呼ばれる、新たな標的を攻略するための起点として悪用されてしまう
- 簡単に陥落してしまうサービスが稼動している状況では、ファイアウォールは十分なセキュリティ対策といえない

- したがって、適切なセキュリティ対策をするためには
  - まず、各システムのセキュリティを可能な限り高めることが先決
  - 次いで、ネットワークの安定性やセキュリティの確保が重要

各システムのセキュリティを高める

Unix系OS（Linux,FreeBSD,OpenBSD）のシステムでセキュリティを高める方法①

- セキュアなマウントポイントの設定
  - マウントオプションを適切に設定してファイルのアクセス権を制限し、攻撃者が重要なファイルにアクセスするのを防ぐ
  - マウントオプションはファイルシステムへのアクセス方法を制御するためのオプションでコマンド mount –o　で指定する

セキュリティに有効なオプション

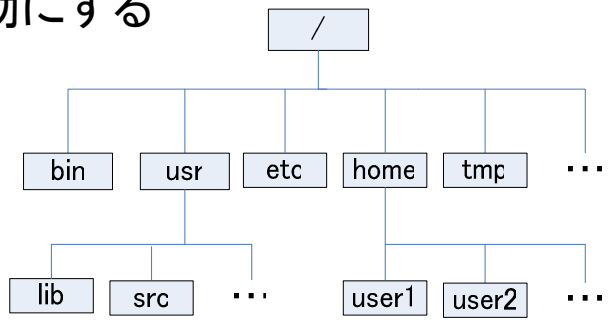
・nodevオプション・・・デバイスファイルを利用できないようにする

・noexecオプション・・・プログラムの実行を禁止にする

・nosuidオプション・・・SUIDビットの設定を無効にする

例）プライマリIDEハードディスクの3番目のパーティションを上記のオプションを指定して、/tmpにマウントするには、

#mount –o nodev,noexec,nosuid /dev/hda3 /tmp



ファイルシステムイメージ

Unix系OS（Linux,FreeBSD,OpenBSD）のシステムでセキュリティを高める方法②

- **ログの改ざん防止**
  - コンピュータが不正アクセスを受けた場合、コンピュータの中には攻撃者によって残されたさまざまな痕跡が存在する
  - そのため、侵入された証拠を記録しているログは必ず守る必要がある
  - その方法としてLinuxでは、拡張属性を割り当てることにより、ファイルやディレクトリにアクセス権を制限できる
  - ログファイルの保護に便利な属性として「追加のみ許可」がある
  - この属性が設定されているファイルにはデータを追記できるだけで削除することができません

例）Linuxでファイルに「追加のみ許可」属性を設定

```
# chattr + a /var/log/logfile
```

Unix系OS（Linux,FreeBSD,OpenBSD）のシステムでセキュリティを高める方法②

- しかし
  - root権限を奪った攻撃者であれば痕跡を消そうとして属性を変更しようとするかもしれない
  - これを防ぐためにはroot権限を制限することができるcapability機能を使用し、「追加のみ許可」属性の削除を許さないように設定する
  - capabilityの設定を変更するには、lcapユーティリティを使用する
    （入手：http://packetstormsecurity.org/linux/admin/lcap-0.0.3.tar.bz2）
    (インストール方法：　# tar xvfj lcap-0.0.3.tar.bz2 && cd lcap-0.0.3 && make)

例）「追加のみ許可」属性の変更禁止するには以下のようにしてlcapを実行

```
# ./lcap CAP_LINUX_IMMUTABLE
```

（一度lcapによって禁止されたcapabilityは、システムをリブートしないと元に戻すことができない）

Windowsのシステムでセキュリティを高める方法①

- **オープン状態のファイルとオープンしているプロセスのリスト取得**
  - タスクマネージャで見知らぬプロセスが動作しているとき、そのプロセスが何者であるかを突き止める
  - ツール Handleを使う

    （入手：http://download.sysinternals.com/Files/Handle.zip）

    （インストール方法： Handleをダウンロードして、圧縮ファイルを解凍して、どこか適切な場所へ置く）

  - このツールはプロセスのスレッド、イベント、セマフォなどの多くのリソースを表示できるだけでなく、使用しているレジストリキーも表示できる
  - handleコマンドを引数なしで実行すると、システム上で開かれているすべてのファイルハンドルのリストを表示

  例）インターネットエクスプローラが開いているファイルとプロセスだけを表示

  c:¥>handle –p iexplore

Handleを実際に実行した結果

```
C:¥>handle -p iexplore

Handle v3.3
Copyright (C) 1997-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

------------------------------------------------------------------------------
iexplore.exe pid: 4020 PC-0¥USER
  40: File  (RW-)   C:¥WINDOWS¥WinSxS¥x86_Microsoft.Windows.Common-Controls_659
5b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
  50: File  (RW-)   C:¥WINDOWS¥WinSxS¥x86_Microsoft.Windows.Common-Controls_659
5b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
  78: File  (RW-)   C:¥WINDOWS¥WinSxS¥x86_Microsoft.Windows.Common-Controls_659
            ・
            ・     (途中省略)
            ・
  98C: Section      ¥BaseNamedObjects¥WDMAUD_Callbacks
  9B4: File  (R--)   C:¥WINDOWS¥system32¥Macromed¥Flash¥Flash9e.ocx
  9FC: Section      ¥BaseNamedObjects¥MSIMGSIZECacheMap
  A44: File  (RW-)   C:¥Documents and Settings¥USER¥Local Settings¥History¥Histo
ry.IE5¥MSHist012008040720080408¥index.dat
  A48: Section      ¥BaseNamedObjects¥C:_Documents and Settings_USER_Local Sett
ings_History_History.IE5_MSHist012008040720080408_index.dat_81920

C:¥>
```

Windowsのシステムでセキュリティを高める方法②

- 一時ファイルフォルダの暗号化
  - たいていのWindowsアプリケーションは動作中にテンポラリファイル(一時ファイル)が作成される
  - プログラム終了時に常に消去されるわけではないため、他人に一時ファイルの内容を覗かれる可能性がある
  - そのため、テンポラリファイルを暗号化する
  - テンポラリファイル（Temp）の場所

    C:¥Documents and Settings¥＜ユーザー名＞¥Local Settings
  - Tempファイルのプロパティダイアログから[全般]→ [詳細設定]でフォルダの暗号化設定を変更することができる

ネットワークの安定性やセキュリティの確保

ネットワークの安定性やセキュリティの確保方法①

- **ARPスプーフィング（成りすまし）の検出**
  - ARPスプーフィングとは
    - ARPの仕組みにはネットワークセキュリティ的に大きな欠陥をもつ
    - ARPはARP要求とARP応答の対応を考慮した処理を行わないために、ARP要求に対応しないARP応答を受け入れてしまうことがある
    - 受け取ったコンピュータは正しい応答であるか判断できず、もし偽装されたARP応答なら偽のコンピュータと通信を開始してしまう
    - これをARPスプーフィングといい、ネットワークの監視（盗聴）などのさまざまな不正アクセスに繋がる

ネットワークの安定性やセキュリティの確保方法①

- **ARPスプーフィングの検出方法**
  - LinuxではツールArpwatchを使って検出
    - プロミスキャスモードでネットワークを一定期間モニタし、MACアドレスとIPアドレスのペアを記録
    - 記録されているMAC/IPアドレスペアの組み合わせが変わるなど異常な振舞いを検出すると、ログ(syslog)に出力

      （入手：ftp://ftp.ee.lbl.gov/arpwatch.tar.gz）
  - WindowsではツールPromiscan（フリー版）を使って検出
    - ローカルネットワークのPCをリモートから検査し、ARPに対する応答をもとに、パケットを不正に取得するプロミスキャスという状態になっているPCを見つけ出す

      （入手：http://www.securityfriday.com/jp/product_2.html）

ネットワークの安定性やセキュリティの確保方法①

- **プロミスキャスモードとは**
  - ネットワークカードの動作モードの一つで、ネットワークを流れるすべてのパケットを受信して読み込むモード
  - ネットワークカードは通常、宛先が自分になっているパケットのみを受信するよう設定されており、ケーブルから別の宛先のパケットが届いても読み込まずに破棄するようになっている
  - しかし、プロミスキャスモードに設定されたカードでは、宛先に関わらずすべてのパケットを受信し、同じネットワークセグメントを流れるすべてのデータを監視することができる

ネットワークの安定性やセキュリティの確保方法②

- **OSの特定防止**
  - OSの特定を防止する理由
    - OSの種類を知ることにより、コンピュータが持つであろう脆弱性や、有効な攻撃コードを容易に見つけ出すことができる
    - そのため、攻撃者はまず始めに標的のコンピュータがどのようなOSによって構成されているか知ろうとする
  - OSが特定される手法
    - OSのTCP/IPスタックの癖とある種のパケットに対するレスポンスから対象のOSの種類をかなりの精度で特定される
    - 有名なツールにNmapがある

（TCP/IPスタックとは、LANを使った通信を行うアプリケーションを作るとき必要とされる、TCP/IP通信のプロトコルに関するプログラムをまとめて1つのプログラム群としたもの）

ネットワークの安定性やセキュリティの確保方法②

- **OS特定の防止方法**
  - Nmapが送信するOS種別特定パケットを拒否するルールをファイアーウォールに追加することでそれらの試みを妨害することができる
    - OpenBSDのPF（Packet Filter）を利用した例

/etc/pf.conf のフィルタリング設定ファイルに以下のルールを記述

```
set block-policy return
block in log quick proto tcp flags FUP/WEUAPRSF
block in log quick proto tcp flags WEUAPRSF/WEUAPRSF
block in log quick proto tcp flags SRAFU/WEUAPRSF
block in log quick proto tcp flags /WEUAPRSF
block in log quick proto tcp flags SR/SR
block in log quick proto tcp flags SF/SF
```

ネットワークの安定性やセキュリティの確保方法③

- **Syslogサーバによるログの集中管理**
  - ログはどのようにコンピュータに侵入されたか、どのようにセキュリティホールを修正すればよいかといった被害範囲などを把握するために有益な情報を提供してくれる
  - そこで、専用のログサーバを構築し、すべてのログを集中的に管理し、攻撃者の手の届かないところに記録する

- Linuxでログサーバ（ホスト名：loghost）を構築するためには
  - syslogdというデーモンにリモートコンピュータからのログを受信するためのオプションを指定して起動する

例） # /user/sbin/syslogd -m 0 -r

ネットワークの安定性やセキュリティの確保方法③

- ログを送信するクライアント側での設定
  - クライアントがLinuxの場合
    - /etc/syslog.conf へ以下のようにして記述

      例） すべてのログをホスト名loghostに転送する

      .　　@loghost
  - クライアントがWindowsの場合
    - [管理ツール“]→ [ローカル セキュリティ ポリシー]で [ローカルセキュリティ設定] からすべての監査ポリシー有効にする
    - ツールNTsyslog を使ってsyslogサーバに転送する

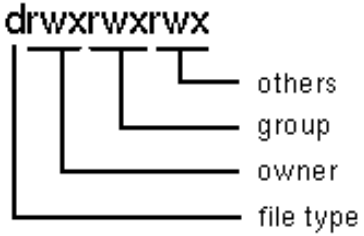
    （入手：http://www.hi-ho.ne.jp/denkas/library/ntsyslog-1.13-jp3p2-binary.lzh）

    （インストール方法：readme.txtを参照）

おわり

補足①

- **SUIDビットとは**
  - SUIDビットは主に root の所有するファイルに対して設定される
  - 即ちユーザ権限ではできない処理を root にお願いして代行して貰うのが SUID ビットである
  - UNIX 系OSでは、ユーザー自身、同じグループに属する利用者、その他の利用者に分け、ファイルのアクセス権（パーミッション）を設定することができ、以下の図で示されるブロックに分けられる



-　　：許可のない状態
r (readable)：読み取り権
w (writable)：書き込み権
x (executable)：実行権：実行できる。

  - ファイルの実行許可を表す x の代わりに s にするとSUID ビットを有効にできる

補足②

- デバイスファイル とは
  - デバイスファイルとは，ハード・ディスクなどの周辺装置（デバイス）を制御する際に用いられる特別なファイル
  - デバイスファイルはすべて，ディレクトリ　/dev　以下に配置される
  - 通常のファイルとは異なり，デバイス番号など，ごく少数のデータだけを保持し
  - プログラムからこれらのファイルに対してopen（）などのシステム・コールを用いてアクセスすると，カーネル内に組み込まれたデバイス・ドライバが呼び出され，ファイルの替わりにデバイスにアクセスする

補足③

- プライマリIDEとは
  - コンピュータにハードディスクなどの機器を接続する際の接続系統の一つ
  - IDE規格では、1台のコンピュータに2系統の接続経路ある
  - それぞれ「プライマリIDE」「セカンダリIDE」と呼ばれる
    - それぞれの経路について「マスター」と「スレーブ」の2台の機器を接続できる
    - OSの起動に使えるのはプライマリIDEのマスターに接続されているハードディスクのみという制限がある

補足④
ネットワーク攻撃の種類Ⅰ

- **ポートスキャン**
  - ターゲットとなるホスト上で通信可能状態にあるポートを探査すること
  - 稼動しているサービスなどからOSの種類やバージョンを特定すること

- **バッファオーバーフロー攻撃**
  - バッファに対して許容量を超えるデータを送りつけ、意図的にバッファをオーバーフローさせること
  - バッファオーバーフローを引き起こしたプログラムが持っているアクセス権の範囲で任意の動作を行なうことが可能となる

補足④
ネットワーク攻撃の種類Ⅱ

- **パケットスニッファリング**
  - ネットワークを流れるパケットを盗聴し、そこからIDやパスワードを拾い出すこと
  - パスワード以外にもメールの盗聴などが行われることもある

- **Dos攻撃**
  - 意図的に不正なパケットを送りつけることで、CPUやメモリなどのシステムリソースを過負荷状態・オーバーフロー状態にしたり、ネットワーク帯域をあふれさせたりすること
  - 最近ではサーバの処理が向上しているため単独で行っても麻痺させるには至らない
  - インターネット上に踏み台をつくり、予め仕掛けておいたエージャントプログラムを用いて一斉にターゲットホストに対して、Dos攻撃を仕掛ける
  - これをDDos攻撃という