見えざる脅威、ゼロデイ攻撃に備える

TOMOYO Linuxによるセキュリティ強化について

2008年９月11日

株式会社NTTデータ
技術開発本部
原田季栄
haradats@nttdata.co.jp

出発点（前提）

- これからご紹介するお話の出発点です
  - **ソフトウェアには脆弱性が伴い、それを解消することはできません**
  - **不正アクセス、クラッキングはなくなりません**
- これらは否定したくても否定できません

「権限」とユーザモデル

- オペレーティングシステムには「権限」という考え方があります
- 何故「権限」が必要なのでしょう？
  - 「誰でも何でもできる」では、セキュリティ以前に秩序が保てません＝たとえばWindows 95, 98, Me
  - かといって「誰も何もできない」のでは話になりません＝たとえば電源を落としたコンピュータ
  - そこで「（必要な）権限を持っていれば実行できる」ようにしようというわけです

具体的には

- Windows XP
  - Administratorユーザは、「全権」を与えられています
    - 何でもインストールできますし、Windows XPが起動しなくなるようなこともできてしまいます（セキュリティを強化されたWindows Vistaでは少々窮屈になりました）
- Linux/UNIX
  - rootとしてログインしたユーザは「全権」を持ちます
  - プロセスに権限を持たせる仕組みが存在します

問題の所在

- 望ましい状態
  - 権限が過不足なく適切に与えられている

- 望まない状態
  - 必要な権限が与えられていない
  - 権限を過剰に与えてしまう

- **「権限をいかに適切に与えるか」が解決すべき問題です**

ゼロデイ攻撃

- Windows XPでAdministratorの権限を奪われたり、Linux/UNIXでrootの権限を奪われてしまうとどうしようもありません
  - 例はWindows Updateに死ぬほどあります（Linuxにもあります）
  - 「攻撃者によりこの脆弱性が悪用され、**影響を受けるコンピュータが完全に制御される可能性**があります。」（リモートでコードが実行される(890047) (MS05-008)）
- そうした脆弱性（セキュリティ上の欠陥）を埋めるためにアップデートやパッチを当てるわけですが、当然ながら攻撃する側はそうした対処を待っていてくれません
- あなたのシステムは「**対処を適用する前の攻撃**」にさらされています

被害を受けたらどうなる？

- 実はそれ以前に「被害を受けたかどうか」を知ることが困難です
  - 「ログがあるのに？」
  - 攻撃がログに残る保証はありませんし、残ったとしてもそのログが信用できるかわかりません（**管理者だったらログだって変更できます**）
  - 「ファイルの改ざん検知ツールをいれているから大丈夫」
  - 改ざん検知ツールがやっていることは、「一定時間ごとの特定されたファイル内容の比較」で全てのファイルをリアルタイムに監視しているわけではありません。また、**管理者であれば、設定内容の変更も結果の「改ざん」もツールの停止もできてしまいます**

(続) 被害を受けたらどうなる？

- 攻撃者によります（やりたいことは何でもできます)
- あなたなら？
- 私なら・・・（しませんが)
  - HPを「攻撃成功(^-^)v」のように改ざんしたりはしないと思います
  - 乗っ取ったことをわからないようにした上で、やりたかったことをやるでしょう（継続的に）

被害に遭ったとき

- あなたを助けるのは、すぐれたシステム管理者です
  - システムのログ、ツール、そして直感（冗談ではありません）により被害の可能性に気づき、それを可能な範囲で確認してから、
    - **「いつからかはっきりわかりませんが、どうもサーバがクラックされているかもしれません」**と報告してくれるでしょう（あなたがこの言葉を聞くことがなければ良いのですが）
- 「自分には起こりえない」と考えるのは、残念ながら間違いです
- 起こりえることは起こるのです

このあとどうなる？

- 予想ですが
  - 何があったか、いつから始まったかを可能な限り調べる（推測する）
  - わかった範囲で告知を行い、ユーザ、関係者に連絡する
  - バックアップからシステムを回復する（どこから始めるか、どのバックアップを使うかが難しい）

復元できたとして

- こう思うのではないでしょうか
  - 「みんな本当によくやってくれて、なんとか短期間にほぼ復元することができたけれど、また同じように被害を受けることはないんだろうか？」
- もちろんあります（残念ながら）
  - 前回攻撃された脆弱性には対処が完了していても、既知の脆弱性について可能な限り迅速に対処したとしても、未知の脆弱性には手をうちようがありません

被害に対するありがちな対応

- 「二度とこんなことが起こらないように、うちもセキュリティを強化した製品を導入しよう。費用はいくらかかってもいいから、とにかく一番高機能で強力なやつだ。休日返上で最優先で作業しろ！」
- 気持ちはわかりますが、極端かつ無茶です。ろくなことになりません

どうして「ろくなことにならない」？

- 冷静に考えれば当たり前のことが、「非常事態」で見えなくなります
  - 「強力」＝設定する量が多い分、時間もかかります。当然高額です
  - 「強力」＝難しくて設定内容を理解できません→「おまかせ」するしかなくなります（あとから自分でコントロールするのは困難です）
  - 「強力」＝内容が細かいため（何とか設定できたとしても）トラブルが頻発し支障が生じます→結局簡単な設定に戻すことになります

被害に遭う前に

- 知っておくべきことがあります
  - これまで説明してきた問題は新しく発見されたものではなく、議論・研究されてきたものです
  - 対策が考案され、利用できます
  - 昔は特殊で効果な専用システムしかありませんでしたが、今やオープンソースでも利用できるようになりました。使わないのは損です

対策

- 基本的な考え方
  - **「権限」を分割する**
    - 全権とそれ以外しかなければ、処理をする度に全権を渡すことになります（消しゴムの購入のために社印を渡してそれが悪用されたら？）
  - **「権限」の審査を徹底する**
    - 管理者であろうがなかろうが例外扱いしない
    - 事前に定めた「条件」に基づき審査する

「セキュアOS」とは

- 管理人をも「制限」できるOSのことです
- 技術的には
  - 「強制アクセス制御」(Mandatory Access Control)を実装したOSです
- 標準機能/オプションの違いはあっても主要なOSではだいたい利用できるようになりました
  - LinuxであればSELinux, Smack, AppArmor, TOMOYO Linux

セキュアOS導入の利点

- ポリシー（良い悪いの定義）が適切に行われていれば
  - 万一不正アクセスを受けた場合でも**被害を限定（局所化）することができます**
    - ポリシー違反の監視により**不正アクセスの検知が可能**となります（本来的には検知だけでなく守るべきですが）
    - **管理者の誤操作による被害や内部関係者による情報漏洩の可能性を軽減できます**（管理者であろうが内部関係者であろうがポリシーで許可されていない操作は失敗します）
- 「必要としない」人は本当はいないはずです

どれを使う？(Linux)

- **SELinux（米National Security Agencyが開発）**
  - Linux標準機能に含まれており、Red Hat EL, Fedoraでは有効状態で出荷されています。強力ですがその分難易度も高くなっています（管理GUIが開発されるなど、着実に改善されています）
- **Smack（Casey Schauflerが個人で開発）**
  - 2008年4月、SELinuxに続きLinux標準機能に追加されました
- **AppArmor（Immunix社が開発したものをNovellが買収）**
  - Linux標準には含まれていませんが、Ubuntu, openSUSE, Mandrivaに搭載されています

TOMOYO Linux

- 「使いこなせて安全なLinux」を目指してNTTデータが開発しました。Turbolinux 11 Server, Turbolinux Client 2008, Mandriva 2008.1に搭載されています

- 「**ポリシーを範囲に含む有償サポート**」が提供されています（Turbolinux 11 Server, TOMOYO LinuxともOSSなので利用するだけなら無料です）

- 2008年３月からNPO日本ネットワークセキュリティ協会サーバで稼働しています（2006年にも商用システム導入事例を発表しています）

- Linux標準機能にするための活動を展開中です

まとめ

- ゼロデイ攻撃の脅威は常に存在しています
- セキュリティを強化されていない標準のOSが攻撃されると被害は検知しにくく、歯止めもありません
- 「ゼロデイ攻撃」という見えない脅威に備えるためには、セキュリティを強化したOSが有効です
- セキュリティ強化OSは「クラッキングを防ぐ」ものではなく、「権限を適切に与える」ための手段です
- 適切に活用することにより情報漏洩の防止、管理者の誤操作の防止も可能です

demo

- Turbolinux 11 Server, Turbolinux Client 2008はTOMOYO Linuxを搭載済みなので、カーネルを差し替えることなく簡単な手順でTOMOYO Linuxを利用することができます
- これからTurbolinux Client 2008を用いて、以下の実演を行います
  - ツールを導入してTOMOYO Linuxを有効にします
  - いくつかのコマンドを実行し、それに必要な権限をTOMOYO Linuxに学習させます
  - 学習した内容に基づき、それ以外の操作を禁止するようにします

是非ご利用ください

- まずは試してみてください（オープンソースなのですから）
  - http://www.turbolinux.co.jp/
  - http://d.hatena.ne.jp/keyword/TOMOYO%20Linux
- 役に立つと思ったなら是非使ってみてください
- ビジネス用途なら是非サポートプランの利用もご検討ください
- ご相談は内容を問わずどうぞお気軽に