Linuxにおける脅威とその応用

宮本 久仁男 a.k.a. wakatono
wakatono@todo.gr.jp

この資料のライセンス

Linuxにおける脅威

- これまでに、カーネル／ユーザランド問わず数多くの脅威が発見されている
  - バッファオーバフロー
  - 境界チェックミス
- どうしようどうしよう…
- 具体的にはどんな脅威があるか分類を

まずは脅威を洗い出してみる

1. 第三者によるデータ閲覧の危険性
   - ディレクトリトラバーサル
   - 情報漏えい
2. 管理者権限奪取の危険性
   - マシンのっとり
3. DoS（サービス妨害）の危険性
   - マシン停止、速度低下
4. その他不具合発生の危険性
   - メールの不正中継、etc…

確かに脅威だが…

- リスクは可能な限り小さくするとして…
  リスクヘッジの結果として

- 小さくした（局所化した）リスクについては、リスクテイクしていく
  存在は認識しつつ、使われる可能性を小さくしていくことで、そのリスク（脅威）から受けられる恩恵というのはないか？

- とりあえず、2つについて検討してみる

応用その1

- 第三者によるデータ閲覧の危険性
  - →裏を返すと「こっそり」データを見ることができる、ということ
- 管理者が見てる、と悟らせずに（別のプロセスに偽装させるなり、監視プロセスを隠蔽するなりして）通信データを閲覧することが可能
  - Rootkit系のツールを使ってもいーかも
  - もちろん、管理者であるからして、システム管理のためにのみその情報を使うべし。

応用その2

- 管理者権限奪取の危険性
  - 放置しておくと危険。
  - ただ、リモートからの奪取以外は、ローカルユーザの管理さえなんとかなればOK
- リモートからの奪取はどうする？
  - アドレス指定でしばりかけとけ
  - イントラネットからのみOK、とか同一サブネットからのみOK、とか
- とりあえず、バグをついた権限昇格ツールは緊急suなどに
  - あくまで管理の範囲内で使うことが重要
- バックドアツールは緊急リモートメンテツールなどに
  - これも管理の範囲内で使うことが重要

神出鬼没のクラッカーだ!!

- 我々の武器は二つある。

- 不正閲覧
- 管理者権限取得

- そして、妨害だ！

応用3

- DoS（サービス妨害）の危険性
  - 想定しない不具合発生時の緊急停止ツールとしてorz
- ネットワーク上でDoSをかけられると、急激にネットワーク全体の負荷が上がることも
  - 制御できれば負荷試験ツールにもorz
- 特定条件におけるDoSが発生するについて、発生条件が違うものをサービス用のサーバに仕込んでおく
  - サーバごとにきめ細かい管理が可能

結論

- バグも使いよう
- バグは使用法を守って、適切にお使い下さい

…って、本気にしないでくださいねorz

- 当該システムの管理組織とちゃんと交渉しないと、訴えられたり捕まったりします…
- 教材として、バグ（脅威）をFIXさせるのはありかも
  - DJBセキュリティ道場の門下生の話
    http://slashdot.jp/article.pl?sid=04/12/17/087208