踏み台は･誰にも待ってる･落とし穴

2004/06/04@LC2004 Lightning Talk

宮本 久仁男
wakatono@todo.gr.jp
http://d.hatena.ne.jp/wakatono/

この資料のライセンス

- この作品は、クリエイティブ・コモンズの帰属 - 非営利 - 同一条件許諾ライセンスの下でライセンスされています。この使用許諾条件を見るには、http://creativecommons.org/licenses/by-nc-sa/2.0/jp/をチェックするか、クリエイティブ・コモンズに郵便にてお問い合わせください。住所は：559 Nathan Abbott Way, Stanford, California 94305, USA です。

注意

- ~~妄~~想像8割？

なぜにこんなこと？

- Debian Projectのサーバクラックがショック

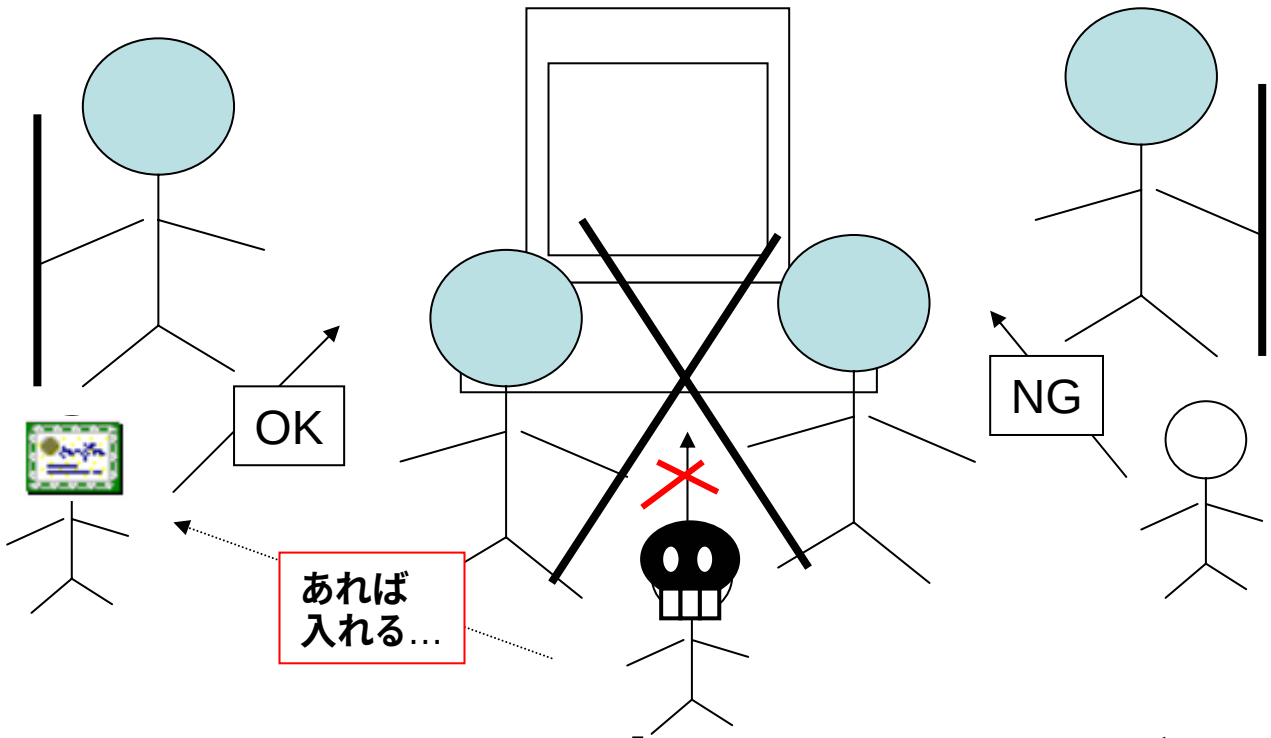
  “Some Debian Project machines have been compromised” はインパクト大きすぎ

- インシデントレスポンスはまさにお手本

  http://slashdot.jp/slash/03/12/01/2356223.shtml

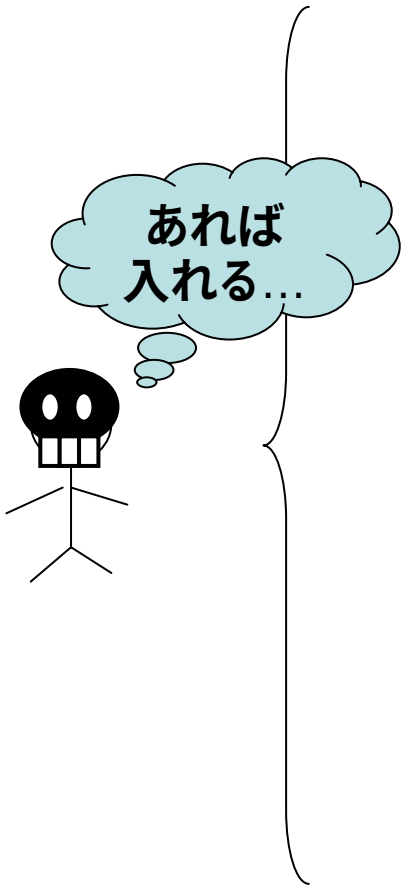
- 適切に管理されているはずのサーバ群の弱点は何か？にフォーカス

Cracker心理の妄想実験例



- **あるCrackerは、とある守りの堅いサーバを攻略することを考えました。何を狙いますか？**

あれば入れる…じゃ、どうすれば…

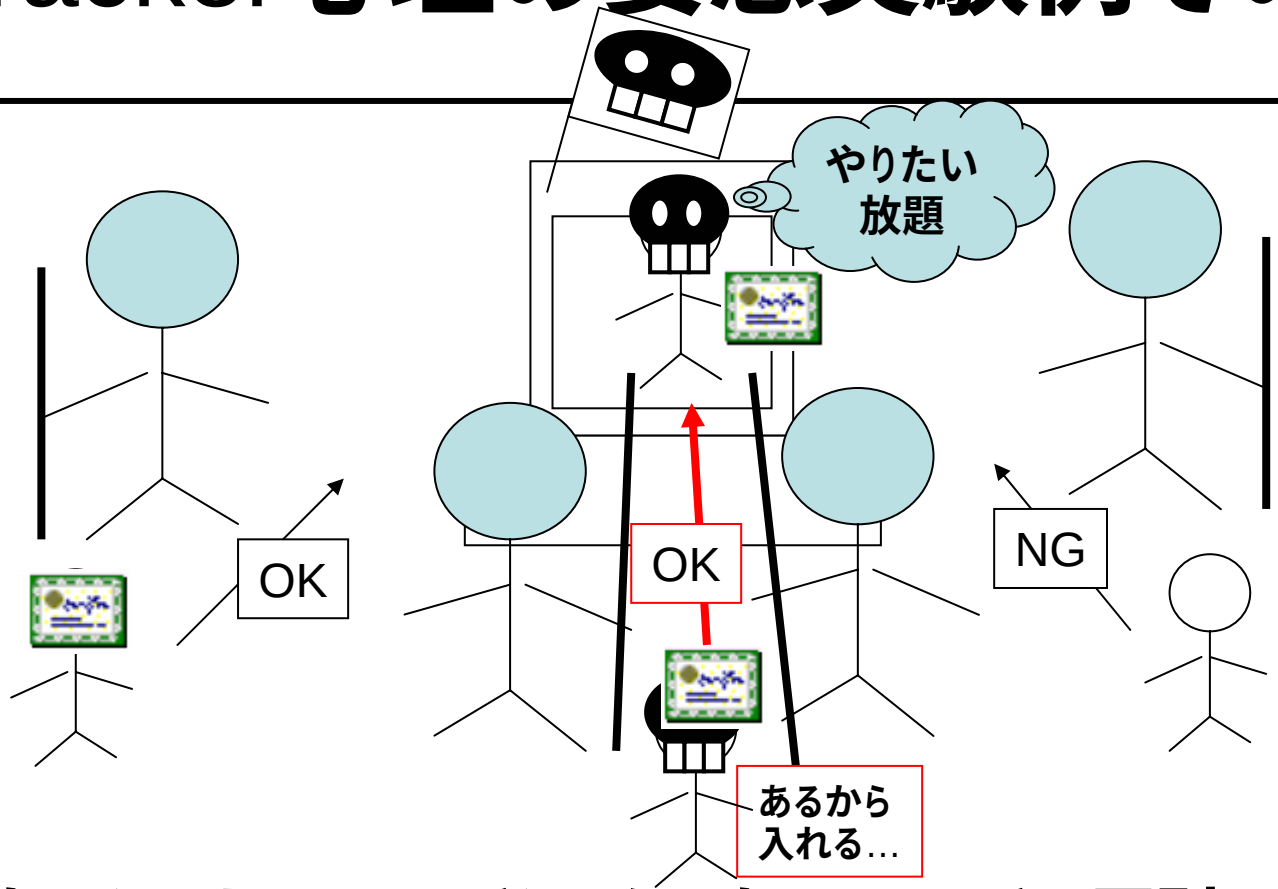


- まともに働いて資格を得る
- 証明書（もしくはそれに類したもの）を偽造する
- すでに持ってる人から拝借する

弱そうなマシンはないかな？

- Sniffing とかwiretapという言葉がアナウンスとかで使われていたが
  - 別に盗聴は通信回線上でなくとも可能
- 弱そうなマシンの例：
  - いかにも大学の共用マシンからアクセスしてる
  - いかにもメンテナンスされてなさそう
  - 「たまたま」使ったマシンにキーロガー/Rootkit
  - etc...

Cracker心理の妄想実験例その後



- **こうなると正しいユーザとそうでないユーザの区別はつかない**
  - 0dayによるExploitで特権を奪取できるようなCrackerに入られた時点でアウト(ここの手段は不明)

今回の件が教えてくれたこと

- サーバはもちろん、それを利用するユーザ環境にも気を使う必要がある
  - ユーザは自分のアカウントが踏み台にされる危険性を想定しよう
- メンテナンスされているかどうか怪しい環境から「そういうところ」に入るのは避けよう
  - キーロガーとかあるかもしれないし、それ以前に信用できない (ことを体感した)
- インシデントレスポンス内容のある程度のdisclose
  - 教訓になる
- ノートPCを持ち歩く人は盗難に注意しよう
  - 秘密鍵を抜かれる危険性とか

最後に

みんなもっと~~妄~~想像しようよ