バッファオーバーフローアタックの実際と対策

～Firewallを通り越える攻撃ツール実演デモ～

Nissho Techno System Corporation
徳植 寛
toku@nissho-ele.co.jp

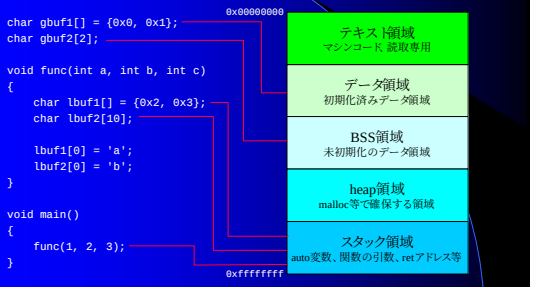
コンピュータウィルス

- マクロウィルス
- ワーム
- トロイの木馬

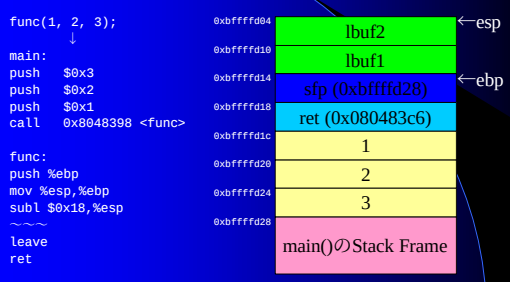
実行しなければただのデータ！

悪さをするプログラムをどうやってターゲットのコンピュータに実行させるかが肝

プログラムのメモリ配置



スタックの中身



スタック破壊サンプル

- リターンアドレスをauto変数の所に書き換えられたら?
- auto変数に/bin/shを実行するマシンコードがコピーされてたら?
- super user権限で実行するプログラムだったら?
- でも、telnet出来ないマシンにそんな事出来るの!?

クラッキング実演

- クラックするにはアセンブラの知識も必要だけど
- ウィルスといっしょで誰でもクラック出来るツールが出回るし
- FireWallが有っても防げないなんてどうすれば良いの?

バッファオーバーフロー対策

- パッチの適用
  当てたら当てたで色々有るけど
- 不要なサービスの禁止
  メモリの節約にもなるし
- Firewallの設置
  入ってくるのだけじゃなく出るのもね
- IDSの導入
  取り敢えずsnortとか

参考

- クラシック: 趣味と実益のスタック破壊
  http://linux.ascii24.com/linux/linuxcom/2000/06/13/465216-000.html
- アセンブラ入門講座
  http://paran0ia.virtualave.net/documents/asm.html
- gdb-4.18日本語texinfo from gnujdoc
  http://www.swlab.csce.kyushu-u.ac.jp/man/gdb-4.18/gdb-ja_toc.html
- Snortの導入
  http://jem.serveftp.com/

最後に

クラッキングはいけないと思います!
By まほろ