Dificuldades Reais na Migração para Software Livre

Rodrigo Rubira Branco

rodrigo@kernelhacking.com
rbranco@mdsystems.com.br

Md Systems Networking

Agenda

- Objetivos
- O que é segurança
- Vida Real
- Segurança em Camadas
- Problemas Atuais
- Estamos perdidos?

Md Systems Networking

OBJETIVOS

- Apresentar na prática conceitos fundamentais em segurança;
- Demonstrar de maneira convincente através de exemplos reais, possíveis melhorias em sistemas operacionais que poderiam proporcionar um ambiente mais seguro;
- Fortalecer a comunidade de segurança, passando conhecimentos amplamente utilizados pelos invasores de sistemas;
- Exemplificar o uso real de um sistema operacional open-source com novos recursos de segurança, fazendo-se uso do alto know-how de suas estruturas e funcionamento;
- Provar que itens comerciais podem ser integradas com soluções open-source para prover uma solução completa aos clientes;
- Demonstrar que software Open Source para Desktops pode ser uma realidade, se tomados os devidos cuidados através de EXEMPLOS PRÁTICOS.

Md Systems Networking

C I D A L

C onfidencialidade

I ntegridade

D isponibilidade

A utenticidade

L egalidade

LEMBRAR-SE SEMPRE DISTO NO DECORRER DA PALESTRA!

Vida Real

Trabalhamos em um mundo real de sistemas mal configurados:

- Bugs de Software
- Empregados Insatisfeitos
- Administradores de Sistemas Sobrecarregados
- Acomodação de necessidades empresariais
- Falta de educação em segurança
- B2B,B2C,B2E,C2C,X2X?
- Tempo disponível para desenvolvimento
- Linguagens de 3 e 4 gerações
- Usuários LEIGOS!!!

Camadas

- Softwares sempre terão falhas;
- Falhas inerentes ao sistema operacional, se não previstas pelo software causam problemas (vide race condition do /tmp);
- Fortificações possíveis no sistema operacional, poderiam tornar as aplicações "livres de falhas" (vide Win2003, OpenBSD e patchs para o kernel do Linux);
- Segurança dos dados NÃO pode depender das estacoes!

Quando pensar em Segurança pense em uma CEBOLA.

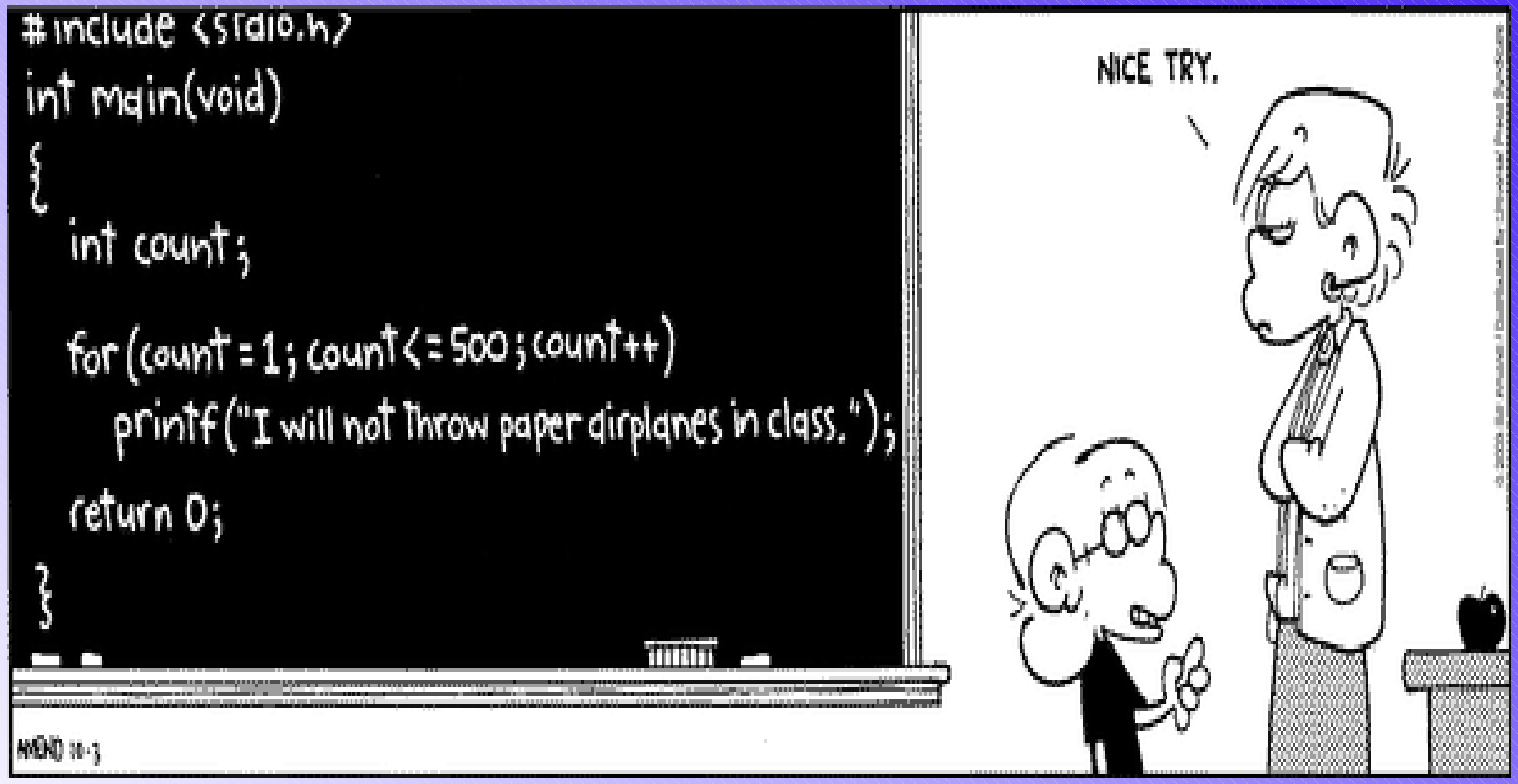
Md Systems Networking

Problemas Atuais

- Segurança dos dados NÃO pode depender das estaçõ̃es!
- Incompatibilidade de Softwares
- Software Legado

Md Systems Networking

“O” Problema – Linux Users



ROOT – Para que tanto poder

- Os problemas dos sistemas operacionais começam porque o administrador possui total controle sobre os mesmos, podendo desde modificar suas estruturas, até destruir totalmente o sistema

- Diversos patchs existem para modificação deste comportamento em sistemas Linux, tais como: GRSecurity, RBAC, LIDS e outros

- Kurumin entre outras distros permitem usuários com poderes de ROOT

Autenticação Centralizada

- Ambientes Linux provêm normalmente autenticação central através de NIS:
  - Multiplas bases de autenticação
  - Dificuldades em se manter “roaming profile”
    - /home do sistema exportado via NFS!
      - segurança de acesso baseado em IP??
        - novos equipamentos podem não ser colocados na rede, mas o acesso via comprometimento local de estação aparenta-se muito fácil (segurança dependente da ESTAÇÃO)

Controle de Acesso Centralizado

- Como efetuar o controle do acesso de determinado usuário em um sistema de forma centralizada, utilizando-se ambiente Linux?

    * Leia-se controle de acesso central, trazer diretivas e permissões de um servidor e não apenas autenticar o usuário e na estação determinar o que ele pode/não fazer

- Como instalar softwares automaticamente para múltiplos usuários, similarmente como pode-se fazer através do uso de COM/DCOM em ambientes Microsoft?

Existem problemas com Virus/Worms/Spywares?

A captura de senhas pode se dar no modo usuário através do hook de bibliotecas ou diretamente em modo kernel, capturando-se as informações digitadas no teclado.

Se o sistema for comprometido por aplicativos executados localmente pelos usuários, problemas com malwares poderão ocorrer.

Proteção de Aplicativos (*)

- Através da checagem de integridade de binários antes de sua execução, consegue-se garantir que executáveis que venham a ser modificados não possam ser executados

Proteção de Arquivos Essenciais

- O sistema operacional possui atributos estendidos poucas vezes utilizados, tais como immutable (chattr +i arquivo)

- Tais atributos infelizmente podem ser removidos pelo usuario root a qualquer momento

- Através de modificações na estrutura do SO, pode-se forcar que tais arquivos sejam realmente imutáveis.

Proteção de Arquivos Essenciais (*)

- Backdoor em módulos de kernel
- Interceptação de processos em memória
- Checagem da integridade interna do kernel
- Arquivos realmente imutáveis (exemplo real)

Estamos perdidos? (*)

- O segredo do sucesso está em dizer a verdade ao cliente, não vender falsas promessas
- Problemas e desvantagens existem e podem ser superados, no entanto não sem grande esforço e envolvimento no projeto
- Muitos dos problemas precisam de faze de maturação para aparecerem e serem solucionados, se o cliente não entender isto desde o princípio, a migração tornar-se-á dolorosa

Md Systems Networking

Agradecimentos

- Eventos, Workshops, Seminários, Palestras, RoadShows, Conversas
- Comunicação
- Elo mais fraco da segurança da informação

FIM! Será mesmo?

DÚVIDAS ?

Rodrigo Rubira Branco

rodrigo@kernelhacking.com
bsdaemon@bsdaemon.org