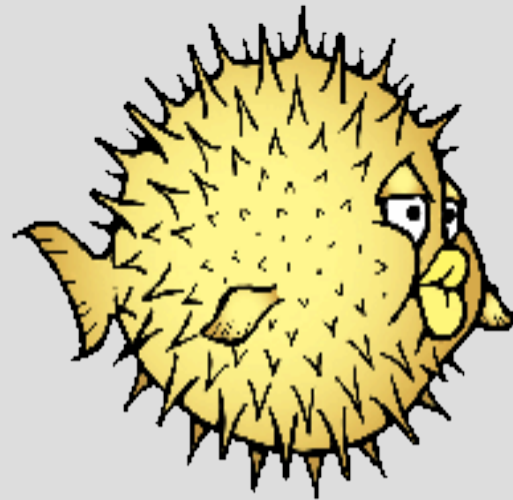


SEGURANÇA COM OPENBSD / Congresso de Tecnologia FATEC-SP 2006

**AS2MWPC - Qualificação e Assessoria em
Tecnologia de Informação
Pedro Moura**

Segurança com OpenBSD



OpenBSD

O mascote do OpenBSD é o Puffy, um peixe baiacu.

Visão Geral

Segurança não é um produto, é um processo.

(Bruce Schneier)

Alerta!!!!

NO - FLAMES!!!!

OBJETIVOS

Os propósitos desta apresentação são:

- a) Elucidar pontos chaves que fortalecem a segurança do sistema operacional OpenBSD.
- b) Divulgar o referido OS para os profissionais de TI, de forma a oferecer mais uma excelente opção, livre e gratuita.

PS: Continuo gostando muito de GNU/Linux.

O QUE É OPENBSD?

- “O projeto OpenBSD produz um LIVRE, sistema operacional Unix-like multiplataforma baseado no 4.4BSD. Nossos esforços enfatizam portabilidade, padronização, exatidão, segurança proativa e criptografia integrada”.

O QUE É OPENBSD?

- “OpenBSD suporta emulação binária de programas oriundos dos sistemas SVR4 (Solaris), FreeBSD, Linux, BSD/OS, SunOs e HP-UX”.

O QUE É OPENBSD?

- Utiliza licença BSD

HISTÓRICO

- O primeiro release do sistema operacional (2.0), foi disponibilizado em outubro de 1996. São planejadas novas versões a cada seis meses.
- A próxima versão (4.0) é aguardada para 1º de novembro (a versão atual é a 3.9).

Histórico

- **Tendo apenas uma vulnerabilidade remota, na sua instalação padrão, durante mais de 10 anos.**

Objetivos do Projeto OpenBSD

- Ser o NÚMERO UM em segurança (se já não o somos).

Objetivos do Projeto OpenBSD

- Divulgação completa de falhas.

Metodologia de trabalho

- Divulgação completa de falhas.

Metodologia de trabalho

- Processo de Auditoria

A solução para diminuir as chances de bugger overflow é o processo de auditoria constante e pró-ativo.

Metodologia de trabalho

- Processo de Auditoria

O time de auditoria busca antecipar-se na resolução de problemas simples, mas que com o passar do tempo foi constatado que os mesmos (em outros sistemas) se tornaram vulnerabilidades.

Metodologia de trabalho

- **Processo de Auditoria**

O buffer overflow é por vezes ocasionado por falta de atenção dos programadores, e até por linguagens de programação e compiladores que não realizam a verificação do tamanho dos buffers. Um estouro do buffer pode ser explorado por um malware (exploit) para ter acesso ao sistema.

Metodologia de trabalho

- Técnicas preventivas

O projeto têm implementado algumas técnicas próprias para melhorar a segurança do sistema, tais como:

Metodologia de trabalho

- Técnicas preventivas

`strncpy()` and `strncat()`

(substituindo as `strcpy()` e `strcat()`)

São funções que implicam em códigos mais seguros pois conseguem

Metodologia de trabalho

- Técnicas preventivas

Mecanismo W xor X

Forçar que as páginas na memória poderão ter permissão de execução o escrita, nunca as duas, aumentando a proteção contra buffer overflow, pois não será possível escrever o código em uma área alocada e memória em que possa ser executado.

Metodologia de trabalho

- Técnicas preventivas

Em outros sistemas esta funcionalidade é conhecida como Pax.

Metodologia de trabalho

- Técnicas preventivas

Privilege separation

Certos daemons (serviços) como o httpd necessitam de privilégios extras. A separação por privilégios é uma forma, separar os processos que precisam de privilégios extras dos que não o requerem. Isto é realizado através de uma relação pai/filho entre processos.

Metodologia de trabalho

- Técnicas preventivas
- **Privilege revocation**
Também baseada em uso mínimo de privilégios, revogando-se os direitos sempre que possível.

Metodologia de trabalho

- Técnicas preventivas

Chroot jailing

Possibilita mudar a raiz do sistema para o contexto de um serviço, funcionando como uma contenção.

Metodologia de trabalho

- **Técnicas preventivas**

Geração de números aleatórios mais incrementada.

Diminuindo os problemas do determinismo.

Metodologia de trabalho

- **Técnicas preventivas**

Stack-Mashing Protector – ProPolice

Trata-se de uma extensão do compilador c do projeto gnu (gcc).

Um programa em C, será protegido pela inserção automática de código de proteção durante o processo de compilação.

Metodologia de trabalho

- **Técnicas preventivas**

Stack-Mashing Protector – ProPolice

Trata-se de uma extensão do compilador c do projeto gnu (gcc).

Um programa em C, será protegido pela inserção automática de código de proteção durante o processo de compilação.

Metodologia de trabalho

“Seguro por padrão”

Todos os serviços não essenciais são desabilitados.

Metodologia de trabalho

- **Criptografia**

- O projeto é baseado no Canadá, logo não sofre restrições (como nos EUA) com relação a criptografia.
- É possível criptografar páginas de memória swap, evitando o acesso a conteúdo sensível na memória.

Metodologia de trabalho

- **Carregamento de módulos**
 - **O kernel do OpenBSD é monolítico assim como no Linux.**
 - **Ele também permite o carregamento de módulos dinamicamente, contudo para isto o sistema dever alternar para modo monousuário e posteriormente retorna ao modo multiusuário (discorrer sobre esta vantagem).**

Metodologia de trabalho

- **Um erro em algum manual é considerado um Bug**

Quem o desenvolve?

- **É mantido por um time de desenvolvimento espalhado por muitos países e o projeto é coordenado por Theo de Raadt, seu criador.**

Quem usa OpenBSD?

- **NASA**
- **Adobe System**
- **Microsoft adotando a Address Space Layout Randomization (ASLR)
(randomização de bibliotecas e pilhas)**
- **Cisco**
- **Appalachian Web Solutions**

Quem usa OpenBSD?

- <http://www.openbsd.org/users.html>
- <http://www.openbsd.org/testimonials.html>
- Conselho Regional de Enfermagem (São Paulo) <http://corensp.org.br>

Quem usa OpenBSD?

- **99,99% Dos administradores Linux utilizam o Openssh.**
- **Trata-se de uma implementação livre do protocolo ssh, (secure shell) para acesso remoto seguro.**

Conclusões

- **Em função do sucesso deste projeto Theo de Raadt ganhou o prêmio de Software Livre da FSF (Free Software Foundation) em 2004 (competiu na ocasião com o Andrew Triggell - criador do samba.**

Conclusões

- **OpenBSD é uma alternativa muito interessante. Para o profissional de TI que já conhece GNU/LINUX é importante investir em dominá-lo também.**

Marketing

- Curso:
 - Segurança com OpenBSD
 - Instalação
 - Implementação de Firewall
 - Implementação de VPN
 - ETC...
- Início: 26/02/2007 à 07/03/2007
- De segunda à sexta
- Das 18:45 às 22:45

Marketing

- Temos também cursos sobre Linux
- Consultoria em Linux e em OpenBSD

Contatos: pedro@wpc.com.br

treinamento@wpc.com.br

site: wpc.com.br

fone: (11) 3228-3709