Guia do Hacker Brasileiro

by Wyllow
o0o→´-.-`←o0o

Prefácio

Esse livro se destina àquelas pessoas que gostam de informática e de aprender cada vez mais. Não importa se ao usuário comum ou o técnico, todos se identificarão muito com a obra. Os assuntos serão apresentados de maneira objetiva e universal. Mostrada em uma linguagem clara mas direta, é como um livro de história. Explica, como, onde e por quê a segurança na informática hoje é um problema tão grande. Ela está em nossa vida quando retiramos dinheiro do caixa eletrônico, fazemos compras pela Internet e até quando tiramos algum documento. Viver sem a Internet hoje é indispensável. Conhecer melhor a rede e os seus perigos é imprescindível. O lado mais obscuro da computação atualmente é a segurança, pois é uma faca de dois gumes. Se você sabe como invadir um sistema, sabe como protegê-lo.

É como uma arma. Você sabe que se atirar irá matar alguém, mas entre saber e fazer existe uma grande diferença. Eu não posso me assegurar que você use o conhecimento contido aqui para se proteger, apenas aconselho-o a fazê-lo. Não existe um sistema operacional ideal para estudar junto a esse livro. O meu interesse é mostrar a segurança como um todo, estudando problemas comuns que englobam os sistemas e apenas pequenas diferenças. Na maioria dos exemplos utilizarei programas em Windows, pois são mais fáceis de se explicar para quem está começando. E todos esses programas possuem similares em outros sistemas. Não têm

enrolação como páginas e páginas de códigos fontes e informações inúteis: será uma deliciosa viagem de conhecimento real e verdadeiro, adquirido durante meus mais de 6 anos de aventura pela Net.

Meu nome é Marcos Flávio Araújo Assunção, moro em Lavras, MG e estou me mudando em fevereiro de 2002 para Poços de Caldas, MG. Tenho 20 anos e amo a Internet e computação em geral, sou pesquisador amador na àrea, não fiz e nem penso em fazer ciëncias da computação (vou fazer direito), pretendo melhorar esse "livro" a cada nova versão para que se torne um ótimo guia brasileiro sobre hackers. Meu e-mail é mflavio2k@yahoo.com.br e meu UIN no icq é 27672882. Dúvidas e sugestões, à vontade. Se quiser me ligar, meus telefones são: 35-38220176 (Lavras) ou 35-38612309 (Nepomuceno). Não tenho formação nem fiz cursos na àrea. Sou apenas um interessado em estar sempre aprendendo.

A maioria dos programas mencionados no livro podem ser conseguidos nos sites www.blackcode.com. e ftp.technotronic.com Para os outros é só usar sites de downloads como www.superdownloads.com.br .Ferramentas de busca também servem, tais como *Altavista* (www.altavista.com) ou *Google* (www.google.com). Tente também meu site (www.anti-trojans.cjb.net) . Se quiser tirar textos desse livro, indique meu nome na frente.

Introdução à segurança

1

Definições de segurança

Segurança em informática

Estamos seguros?

A fragilidade dos sistemas informatizados não é nenhuma novidade. A décadas, celebridades como *Robert Morris Jr*, *Capitão Crunch*, *Kevin Poulsen* e *Kevin Mitnick*, esses últimos dois mais recentes, fazem com que as pessoas se preocupem e tenham um medo maior do computador. Esse medo virou pânico em pleno século XXI. Piratas novamente existem, mas sua arma não é mais a espada, é o fax-modem. Graças à essa maravilha do mundo moderno, dados podem navegar por linhas telefônicas, cabos e satélites, diminuindo as distâncias entre os povos e iniciando a nova era digital. Ladrões assaltam bancos confortavelmente no Havaí enquanto desviam o dinheiro para a Suíça. A espionagem industrial é um dos problemas agravados. Ela sempre existiu, mas com a facilidade de acesso à Internet, qualquer pessoa pode conseguir dados confidenciais e vendê-los para concorrentes.

Diariamente, páginas e páginas são tiradas do ar por piratas digitais. Grupos de hackers e crackers brasileiros, como *Prime Suspectz e Inferno.br* (esse último já extinto), junto a outros centenas pelo mundo realizam façanhas extraordinárias, como invadir vários sites da Microsoft, a Nasa, FBI, Interpol e muitos outros. Os grupos brasileiros atualmente são os que mais invadem homepages em todo o mundo, fazendo com que a própria Nasa restrinja acesso ao Brasil em algumas de suas páginas. Mas nem todos são ruins. Existem grupos que se especializam em criar ferramentas e ajudar usuários comuns, como o *UHOL*. Toda essa fama já criou até um novo termo no mundo da segurança: o Backer. Ou seja, Brazilian Hacker (Hacker Brasileiro). Isso demonstra a fragilidade da situação. Respondendo à pergunta do tópico: estamos seguros? Com certeza que não.

Características de um sistema inseguro

A segurança de sistemas existe por um conjunto de fatores. Engana-se quem pensa que somente por utilizar uma plataforma Unix ao invés de Windows está seguro. Ou que é só colocar um anti-vírus e um firewall na sua empresa que está tudo bem. A proporção do problema é bem maior. Geralmente os sistemas mais vulneráveis da rede possuem dois pontos em comum:

Administrador

O ponto chave e essencial para qualquer sistema de computador é o administrador. Ele é responsável por fazer com que tudo corra perfeitamente. Checa os dados, administra usuários, controla servidores, checa logs, tudo todos os dias. Acontece que a grande maioria dos administradores hoje não se preocupa com a segurança como deve. Logo terá problemas com o seu sistema, não importa qual seja. É como se fosse mãe e filho. Se uma mãe alimenta seu filho, cuida dos seus deveres de casa, compra roupas novas, dá brinquedos mas não é capaz de comprar um seguro de vida, ou pior, zela tão pouco pela segurança dele que ao sair de casa deixa as portas ou janelas abertas. Essa não pode ser uma boa mãe.

Mesmo que uma rede utilize um sistema operacional que contenha muitas falhas, os bons administradores todo dia estarão checando por falhas descobertas e corrigindo-as. Já os outros provavelmente vão ficar em algum chat comendo sanduíches.

Sistemas operacionais

Como eu disse anteriormente, não há realmente um sistema que seja melhor que o outro. Existem vantagens e desvantagens de cada um. Tudo bem que alguns possuem erros muitos grandes, mas podem facilmente ser corrigidos. A intenção do sistema também importa. Não adianta ter uma rede e utilizar Windows 98 ou ME. Os recursos de segurança deles são muito escassos, pois foram feitos para o usuário comum e não para o ambiente empresarial. Não adianta também instalar o **Digital Unix**, **FreeBSD** ou **AIX** se o seu administrador só possui experiência em **Lantastic**. O sistema também vai depender do tipo de rede que você terá. Se você terá um servidor Web ou algum tipo de acesso externo, seria melhor utilizar o **Linux** ou o **Windows NT**. Se for uma rede interna somente, utilize **Novell Netware**, que ainda não fez a sua história quanto à Internet, mas ainda é insuperável nas redes locais.

A segurança ao longo da história

Anos atrás, os operadores de um computador ENIAC se depararam com uma coisa curiosa. Um inseto havia ficado preso dentro da máquina e estava atrapalhando o funcionamento da mesma. Daí surgiu o termo **bug** (inseto) que virou sinônimo de falha. Hoje quando se descobre um erro em algum programa, se diz: "*novo bug descoberto*". De lá pra cá, as coisas evoluíram muito, mas os bugs continuam a existir. Muitos deles são frutos da história do próprio programa ou sistema. O Windows por exemplo. O Windows NT foi construído a partir do zero, mas o Windows ME não. Desde o início da criação de sua primeira interface gráfica, a Microsoft vêm tendo problemas com erros graves em seu sistema operacional. Já o sistema Unix, foi criado pelos desenvolvedores da linguagem C, para ser um sistema versátil e poderoso. Para conhecer melhor sobre a história de cada sistema, leia a seção sistemas operacionais .

A Internet também têm seus problemas ligadas à história de sua origem. Desde que se chamava Arpanet e foi criada pelo exército americano para resistir à guerra fria, a rede evoluiu muito e foram criados novos serviços como **E-mail**, **World Wide Web**, **Gopher**, **Wais** e outros. Milhões de computadores se juntaram a ela e seus recursos são cada vez mais sofisticados. Mas alguns problemas bem antigos ainda prejudicam hoje. Uma falha na implementação do TCP/IP(conjunto de protocolos em que a Internet se baseia) por exemplo, possibilita que o ataque de **Spoof** aconteça.

Invasores digitais

Todos os dias surgem notícias sobre piratas digitais na televisão e na Internet. Um pirata invadiu o computador de um sistema de comércio eletrônico, roubou os números de cartão, comprou Viagra e mandou entregar na casa do Bill Gates. Outro conseguiu derrubar sites famosos como YAHOO, CNN, AMAZON e ZDNET. Mais recentemente um grupo estrangeiro conseguiu tirar mais de 650 sites do ar em um minuto. Para entender como se organiza a hierarquia virtual da Internet, vamos estudar seus principais integrantes:

Hackers

Na verdade, os hackers são os bons mocinhos. Para os fãs de Guerra nas Estrelas, pensem no hacker como o cavaleiro jedi bonzinho. Ele possui os mesmos poderes que o jedi do lado negro da força (cracker) mas os utiliza para proteção. É um curioso por natureza, uma pessoa que têm em aprender e se desenvolver um hobby, assim como ajudar os "menos prevalecidos". Um bom exemplo real foi quando o cracker *Kevin Mitnick* invadiu o computador do analista de sistemas *Shimomura*. Mitnick destruiu dados e roubou informações vitais. Shimomura é chamado de hacker pois usa sua inteligência para o bem, e possui muitos mais conhecimentos que seu inimigo digital. Assim facilmente montou um **honeypot** (armadilha que consiste em criar uma falsa rede para pegar o invasor) e pegou Kevin. Infelizmente a imprensa confundiu os termos e toda notícia referente a baderneiros digitais se refere à hacker.

Essa é a imagem do hacker que você deve ter.

Crackers

Esses sim são os maldosos. Com um alto grau de conhecimento e nenhum respeito, invadem sistemas e podem apenas deixar a sua "marca" ou destruí-los completamente.

Geralmente são hackers que querem se vingar de algum operador, adolescentes que querem ser aceitos por grupos de crackers (ou script kiddies) e saem apagando tudo que vêem ou

mestres da programação que são pagos por empresas para fazerem espionagem industrial. Hackers e crackers costumam entrar muito em conflito. Guerras entre grupos é comum, e isso pode ser visto em muitos fóruns de discussão e em grandes empresas, as quais contratam hackers para proteger seus sistemas.

O Darth Maul representa bem um cracker

Os hackers e crackers são eternos inimigos. Um não gosta do outro e sempre estão lutando por seus ideais. Usei a analogia do guerra nas estrelas pois expressam exatamente bem pessoas de poderes iguais mas de ideologias opostas. Nossos invasores digitais são assim: mocinhos e vilões brigando. E brigas feias.

Phreakers

Maníacos por telefonia. Essa é a maneira ideal de descrever os phreakers. Utilizam programas e equipamentos que fazem com que possam utilizar telefones gratuitamente. O primeiro phreaker foi o *Capitão Crunch*, que descobriu que um pequeno apito encontrado em