Destaque

Resenha: Guia do Hacker Brasileiro

25/11/2003 - 5:12 **Marcos Machado**

Guia do hacker: conceitos equivocados

Ser hacker é, primeiramente, ser polêmico. Antes mesmo de considerarmos toda a gama de significados do termo, dar este título a alguém abre a guarda dos mais catedráticos do ramo para questionamentos inflamados de representantes das mais diversas vertentes.

De um lado estarão os que cultivam certa paixão pela "filosofia de vida" do hacker, do especialista em informática e do grande construtor e disseminador de informações. Do outro lado estarão aqueles que desistiram da visão romântica (ou nunca a conheceram) e aceitaram o termo como designação de criminosos digitais.

O livro ***Guia do Hacker Brasileiro*** está presente nos dois lados. Seu objetivo é fornecer ao usuário de informática as ferramentas usadas por especialistas mas, ao mesmo tempo, insiste em mesclar seu conteúdo com guias destrutivos e criminosos.

Suas múltiplas personalidades prejudicam seu desenvolvimento. Os assuntos tratados possuem uma ordenação confusa e os textos perdem objetividade a cada parágrafo. Algumas definições são interrompidas para exemplificações que raramente ajudam a entender os conceitos.

Seus capítulos não seguem nenhuma ordem didaticamente coerente. Inicia contextualizando o leitor nas diversas divisões do underground virtual, como de praxe, seguindo-se pequenos trechos sobre serviços Internet, endereçamento e protocolos. Relata dezenas de ferramentas e técnicas, quase todas exaustivamente presentes em tutoriais básicos encontrados na Internet.

Por falar em Internet, este livro é uma revisão de um texto com o mesmo nome e do mesmo autor, que já circula há algum tempo por páginas, canais de bate-papo e fóruns relacionados à segurança e microinformática. Trata-se de uma coletânea de dicas sortidas e conceitos garimpados no senso comum dos profissionais ou meros interessados em segurança da informação, mas com uma dose bem original de inconsistências e incorreções.

Entre estes conceitos, você aprenderá, por exemplo, que o SMTP é um protocolo apenas para envio de e-mails, enquanto o POP serve para recebimento e responde na porta 113; que a diferença entre um trojan e uma backdoor é a dificuldade de instalação e que *buffer overflow* é o nome dado ao travamento do sistema por falhas de memória.

Aprenderá também que não existe roteamento de pacotes dentro de um provedor de acesso à Internet, que hieróglifo é um tipo de criptografia, que *race condition* é a execução de uma falha que pode lhe enviar para o *shell* de um sistema e que a briga judicial sobre a comercialização do PGP foi causada exclusivamente por uma quebra de patente da RSA.

Presente ainda no guia do hacker estão as informações de que firewall é um HD, que o objetivo do *shadow* em sistemas Unix é apenas esconder o arquivo de senhas fora do local padrão, que códigos-fontes em C não funcionam em sistemas Windows e que uma ótima proteção contra 50% dos vírus é manter a data do relógio do computador sempre fixa.

O objetivo do *buffer overflow*, segundo o autor, seria "adicionar trojans ou keyloggers" na lista de processos do servidor, sendo o uso mais famoso o telnet reverso. Ou ainda, um servidor FTP se presta a fornecer um acesso via shell para execução de comandos. Um invasor em um servidor Unix que não possui acesso root não representa perigo algum. A única função dos vírus é causar danos ao computador. Filtros de pacotes de roteadores não protegem máquinas internas contra spoofing.

É claro que, pelo que consta no livro, não importa se todas estas afirmações estão contundentemente erradas. As poucas informações tecnicamente corretas são genéricas demais para serem aproveitadas de alguma forma. Dados antigos também incomodam. A vulnerabilidade mais recente é de junho de 2001.

Parte do conteúdo é composta por screenshots de aplicativos, tabelas com listas de códigos ou relação de senhas *default* (quase todas desabilitadas nas novas versões dos sistemas), além de dezenas de páginas com código-fonte de aplicativos, como exploits. Quem teria coragem ou paciência de digitar duas páginas inteiras de *shell code* em hexadecimal?

Guias de comandos são simples traduções das telas de ajuda dos próprios comandos e a simplificação das explicações termina por podar assuntos que seriam de muito interesse para o estudioso de segurança. Por exemplo, os capítulos onde são abordadas as técnicas de *sniffing* sequer citam barramentos, enlaces físicos e menos ainda canais criptografados como VPN ou tunelamento de conexões.

O mesmo vale para as técnicas de varredura de vulnerabilidades. Sua introdução é correta, a importância da técnica para se manter um ambiente seguro é bem fundamentada (apesar de óbvia), mas suas páginas tratam apenas de scanner de portas. Fica subentendido que vulnerabilidades são encontradas apenas em servidores Web e FTP. Estes, apesar de críticos, são apenas parte do problema.

Na sessão avançada, o guia do hacker ensina — ou ao menos tenta ensinar — técnicas como o uso de compartilhamento através do IPC$ e *arp spoofing*, mas limita-se a executar comandos e aplicativos externos que, muito provavelmente, jamais teriam algum resultado positivo fora de um laboratório, principalmente por não explicar seu funcionamento, seus pré-requisitos e suas conseqüências. Uma atitude comumente manifestada por "script kiddies", felizmente sem muita utilidade.

De todo o livro podemos tirar uma única lição: se os "hackers brasileiros" realmente se guiassem por estas técnicas, atribuir-lhes o papel de criminosos os tornaria inócuos. Se hacker, em contrapartida, significasse o especialista em informática, os profissionais de

segurança do nosso país estariam em péssimos lençóis.

Guia do Hacker Brasileiro
Marcos Flávio de A. Assunção
Editora Visual Books - 189 pgs. - R$ 29,90 (Promoção)
Para comprar este livro, clique aqui.

Marcos Machado é analista de segurança com pós-graduação em redes de computadores e Internet e coordenador do fórum InfoSecurity Task Force.

RECOMENDE INFOGUERRA | ENVIE ESTA NOTÍCIA

Voltar

Destaque	MS aciona defensor do software livre no governo e comunidade reage
Noticias	Evento discute tendências de segurança da informação
Noticias	Supostos problemas com CPF são isca para scam
Noticias	Ataques derrubam grandes sites da Internet
Noticias	Pregão eletrônico com certificação roda em Linux e celulares
Noticias	Lançado no Brasil firewall de redes "inteligente"
Destaque	Criado primeiro vírus para celulares
Noticias	Cisco e Trend Micro anunciam parceria
Noticias	A verdade sobre o HAA continua
Noticias	Código explora bug grave do kernel do Linux

Pesquise no banco de dados Buscar

Boletim InfoGuerra Digite seu e-mail Cadastrar

Notícias | Artigos | News (in English) | Boatos | Dicas | Livros | Arquivo | Contato | Privacidade | Sobre o site | Iníc