

2ª EDIÇÃO ACTUALIZADA
E COM NOVOS HACKS



50

HACKS

para o Windows XP

[Hugo Caramelo]

EXCLUSIVO >> Intrusão dupla, com *LiveCD* e *Keylogger*

Reservados todos os direitos por Centro Atlântico, Lda.

Qualquer reprodução, incluindo fotocópia, só pode ser feita com autorização expressa dos editores da obra.

50 HACKS PARA O WINDOWS XP

O ABC DO HACKER — 2ª edição

Colecção: Tecnologias

Autor: Hugo Caramelo

Direcção gráfica: António José Pedro

Revisão final: Centro Atlântico

Capa: António José Pedro

© Centro Atlântico, Lda., 2006

Av. Dr. Carlos Bacelar, 968 - Escr. 1-A - 4764-901 V. N. Famalicão

Rua da Misericórdia, 76 - 1200-273 Lisboa

Portugal

Tel. 808 20 22 21


geral@centroatlantico.pt

www.centroatlantico.pt

Impressão e acabamento: Inova

2ª edição: Fevereiro de 2006

ISBN: 989-615-020-6

 Depósito legal: /06

Marcas registadas: Todos os termos mencionados neste livro conhecidos como sendo marcas registadas de produtos e serviços foram apropriadamente capitalizados. A utilização de um termo neste livro não deve ser encarada como afectando a validade de alguma marca registada de produto ou serviço.

O Editor e o Autor não se responsabilizam por possíveis danos morais ou físicos causados pelas instruções contidas no livro nem por endereços Internet que não correspondam às *Home-Pages* pretendidas.

Apesar de terem sido tomadas todas as precauções, podem ter existido falhas humanas ou técnicas na apresentação das instruções técnicas, na transcrição da legislação ou nas suas referências. Por essas, ou por quaisquer outras falhas eventualmente existentes neste livro, quer o Editor quer o Autor, não assumem qualquer responsabilidade.

O Editor e o Autor não aconselham qualquer actividade que possa de algum modo ser ilegal. Em caso de dúvida o leitor deve consultar o seu advogado.

ÍNDICE

INTRODUÇÃO	7
Nota inicial	7
Porquê este livro?	7
Para quem é este livro?	8
Para quem não é este livro?	8
Como está organizado este livro?	8
Notação utilizada	9
Ícones utilizados	10
<i>Hackers</i> e <i>Crackers</i>	11
Requisitos prévios à aplicação dos <i>Hacks</i> deste livro	12
Como conseguir acesso ao computador da vítima?	13
HACKS PARA ACESSO A COMPUTADORES “PROTEGIDOS” COM PALAVRA-PASSE	15
1. <i>LiveCD</i> para intrusão no Windows XP	16
2. <i>Keylogger</i> para intrusão no Windows XP	24
HACKS NO ARRANQUE DO WINDOWS	29
3. Personalizar o ecrã de abertura (<i>Windows boot screen</i>)	30
4. Esconder o ecrã de abertura	38
5. Personalizar o ecrã de inicialização	40
6. Personalizar o ecrã de <i>logon</i>	44
HACKS NA INTERFACE	49
7. Esconder a Área de Notificação	50
8. Inserir uma mensagem anexa ao relógio	54
9. Esconder a lista de programas do menu Iniciar	58
10. Esconder um programa do painel Iniciar	62
11. Adicionar um <i>link</i> para Marte no painel Iniciar	66
12. Alterar os detalhes visíveis no Explorador do Windows	72
13. Limitar as imagens das contas de utilizadores	76

14. Remover todos os ícones do ambiente de trabalho	80
15. Mudar o nome da Reciclagem	84
16. Alterar o cursor	86
17. Alterar o som de erro do Windows	90
18. Apresentar um ambiente de trabalho congelado	94
19. Alterar o logo do fabricante do computador	100
20. Não 1, mas 4 ambientes de trabalho	104
21. <i>Relifting</i> completo à interface	108

HACKS NO FUNCIONAMENTO DO WINDOWS **119**

22. Um computador que se desliga sozinho!	120
23. Atalhos enganadores	122
24. Não deixar rastros no ecrã de <i>logon</i>	126
25. Impedir o acesso a programas	130
26. Revelar as <i>passwords</i> !	134

HACKS PARA OUTRO SOFTWARE **141**

27. Word: Alterar o modelo para criação de novos documentos	142
28. Word: Texto invisível	148
29. Excel: Assustar o utilizador com uma mensagem de “boas”-vindas	150
30. Excel: Esconder menus	154
31. Internet Explorer: Navegação em modo quiosque	158
32. Internet Explorer: <i>Home-Page</i> inalterável	160
33. Internet Explorer: Limitar o acesso à Web	164
34. Internet Explorer: Alterar o logo	168
35. Internet Explorer: Alterar a animação do logo	172
36. Internet Explorer: Alterar o fundo da barra de ferramentas	176
37. Internet Explorer: Alterar o texto na barra de título	182
38. Mozilla Firefox: Onde estão os meus menus?!	186
39. Mozilla Firefox: Limitar o acesso à Web	192
40. Outlook Express: Fruta e flores como fundo das mensagens	196
41. Outlook Express: <i>You've got mail</i> (em voz alta)	200
42. Outlook Express: Nova página de boas-vindas	204

HACKS EM REDES LOCAIS	209
43. Que <i>sites</i> consulta a Mariazinha durante o trabalho?	210
44. Quais são as <i>passwords</i> da Mariazinha?	218
HACKS NO HARDWARE	221
45. Uma impressora que trabalha sozinha!	222
46. Trocar os botões do rato	224
47. Modificar o funcionamento do teclado	226
48. Transformar o teclado numa máquina de escrever	230
49. Webcam transformada em <i>spycam</i>	234
50. Dividir a imagem do ecrã por 2 monitores	240
ANEXOS	243
ANEXO 1 - <i>Hackers, Crackers e Phreakers</i> , entre outras personagens!	245
ANEXO 2 - <i>Hackers</i> famosos (nem sempre pelos melhores motivos...)	253
ANEXO 3 - <i>Passwords</i> (palavras-passe)	259
ANEXO 4 - Engenharia Social	269
ANEXO 5 - <i>Malware</i>	271
ANEXO 6 - As 6 fases no arranque do Windows XP	285
ANEXO 7 - O Registry (Registo do Windows)	291
ANEXO 8 - Informação sobre o computador	305
ANEXO 9 - Navegar anonimamente pela Internet	321
ANEXO 10 - Os caminhos das mensagens de correio-electrónico	323
ANEXO 11 - <i>Sniffers</i>	335
ANEXO 12 - <i>Phishing</i> e <i>Pharming</i>	337
ANEXO 13 - As 9 dicas básicas para conectividade sem fios em segurança	341
ANEXO 14 - Localizar redes Wi-Fi com computador	345
ANEXO 15 - Localizar redes Wi-Fi sem computador	347
ANEXO 16 - Alguma legislação importante para <i>Hackers</i>	349

HACK 1

LIVECD PARA INTRUSÃO NO WINDOWS XP



30 MIN.



```

*****
* Win/NT Registry Edit Utility Floppy / chntpw
* (c) 1997 - 2004 Petter N Hagen - pnoordahl@eunet.no
* See file named "license" on floppy for licensing info and credits
*
* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP installation
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.
*
* It also has a registry editor, and there is now support for
* adding and deleting keys and values.
*
* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
*           Win2k Prof & Server to SP4. Cannot change AD.
*           XP Home & Prof: up to SP2
*           Win 2003 Server (all?): Seems to work
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
*****
DON'T PANIC!

```

Introdução >>

Digamos que se esqueceu de todas as palavras-passe para acesso a um seu computador onde deseja testar os *Hacks* deste livro. Qualquer especialista que consultar dir-lhe-á, sem levantar os olhos do ecrã: “Vais ter que reinstalar o Windows XP!”.

Ou, se não for tão nabo: “Podes utilizar um utilitário para descobrir e alterar essa *password* mas para tal precisas de entrar no sistema com uma conta com permissões de Administrador ou pelo menos ao nível da outra conta. Ou tentar repor uma cópia de segurança.”.

Mas, no nosso caso, nem temos cópias de segurança e como já vimos desconhecemos também qualquer palavra-passe de acesso ao sistema.

Bem, existem “felizmente” outras hipóteses, bem mais simples e rápidas (e ilegais, caso o computador não seja o seu!). É o que vamos ver neste *Hack* e no seguinte.

Para realizar este *Hack* vamos organizá-lo em 3 secções:

- I. Alteração dos parâmetros da BIOS;
- II. Criação de um LiveCD com Linux; e
- III. Utilização de um utilitário da distribuição Austrumi para anular a palavra-passe do Administrador do sistema.

bora lá!

Funcionamento >>

I. Alterar a sequência de *boot* na BIOS

Como deve saber, a BIOS (Basic Input/Output System) consiste num tipo de *firmware*, alojado na placa-mãe do computador, que contém o código relativo ao processador do sistema e inicia-se independentemente do sistema operativo a ser utilizado, controlando algumas das funções básicas do PC.

Dica >>

Se desejar obter mais informações sobre a BIOS do seu computador pode utilizar o utilitário gratuito BIOS Agent (<http://www.unicore.com/biosagent/index.cfm>).

I.01.

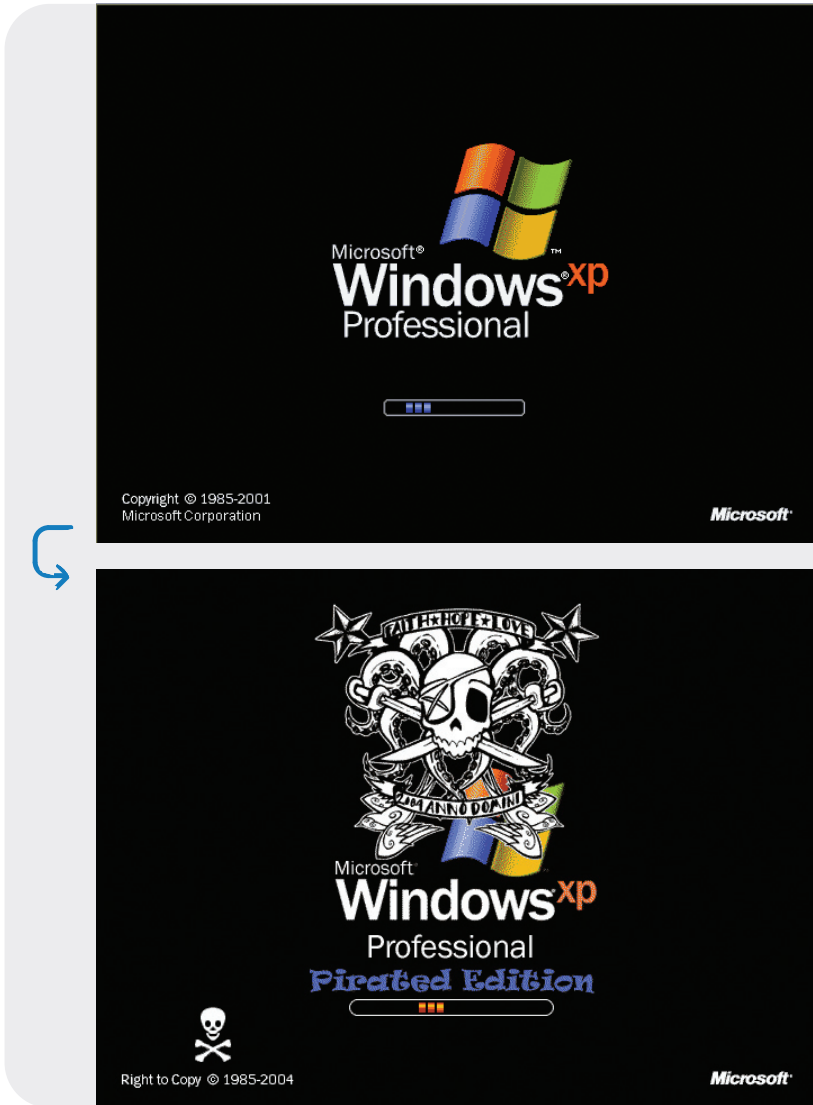
Para arrancar o seu sistema através de um CD, como iremos necessitar mais à frente, pode nem ter de alterar os parâmetros da BIOS, pois o mais normal é que a ordem de arranque (*boot sequence*) configurada seja a que desejamos: disquete, CD (ou vice-versa) e depois o disco duro. Mas se o seu sistema não estiver assim configurado, e apesar do processo variar ligeiramente de BIOS para BIOS, deve estar atento, no arranque do sistema, e procurar uma mensagem que diz `Press {key} for Setup`, em que

HACK 3

PERSONALIZAR O ECRÃ DE ABERTURA (WINDOWS BOOT SCREEN)



30 MIN.



HACK 43

QUE SITES CONSULTA A MARIAZINHA DURANTE O TRABALHO?



60 MIN.



LER ANEXO:



SNIFFERS

Neste Hack e no seguinte vamos utilizar um *sniffer* – como existe um anexo sobre este assunto propomos que o leia antes de continuar.



50 HACKS PARA O WINDOWS XP

Baseando-se a segurança de um computador na integridade, confidencialidade e disponibilidade dos seus dados, neste livro vemos como cada uma dessas premissas pode ser facilmente desfeita com a aplicação de técnicas diversas (*Hacks*) provocadas por intrusos (*Hackers* e *Crackers*).

Nesta obra, o autor convida os leitores a testarem a segurança dos seus sistemas informáticos, ou a dos computadores dos seus familiares ou colegas de trabalho, através da aplicação de 50 *Hacks* devidamente organizados em 7 capítulos, complementados por 16 anexos repletos de informação essencial.

50 Hacks para o Windows XP – O ABC do Hacker fornece ao leitor, à medida que vai executando os *Hacks* propostos no livro (e lendo, sempre que forem sendo necessários, os detalhados e também práticos Anexos), os conhecimentos necessários para proteger eficazmente o seu computador e respectiva rede local, proporcionando ainda noções sobre aspectos fundamentais do funcionamento do sistema operativo e das suas configurações de segurança.

Trocar e esconder atalhos, programas ou ecrãs, alterar o funcionamento do Windows ou de programas como o Internet Explorer, Mozilla Firefox, Excel, Word ou Outlook Express, aceder a dados confidenciais de terceiros – inclusive descobrindo as suas *passwords* – e negar o acesso a componentes e funcionalidades do sistema são algumas das operações reveladas neste livro, sempre com o propósito de ajudar o leitor a proteger-se de eventuais intrusões similares.

Esta 2ª edição apresenta, em exclusivo editorial, dois métodos distintos para acesso a computadores, com Windows XP SP2, dos quais se desconhecem as palavras-passe dos seus utilizadores. Essa intrusão dupla é apresentada em dois novos *Hacks*, com recurso a *LiveCD* e a *keyloggers*.

50 Hacks para o Windows XP – O ABC do Hacker é, por todos esses motivos, já considerado o mais importante livro português sobre segurança informática para sistemas com Microsoft Windows XP, motivo por que deve estar presente na estante de todos aqueles que se preocupam com a sua privacidade e com a segurança dos seus dados e informações.

ISBN 989-615-020-6



9 789896 150204