50 HACKS

para o Windows XP

[Hugo Caramelo]

CENTROATLANTICO.PT

50 HACKS PARA O WINDOWS XP
O ABC DO HACKER

Colecção: Tecnologias
Autor: Hugo Caramelo
Direcção gráfica: António José Pedro
Revisão final: Centro Atlântico
Capa: António José Pedro

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
1ª edição: Abril de 2005

ISBN: 989-615-008-7
Depósito legal: ...../05

ÍNDICE

INTRODUÇÃO

Nota inicial

Este livro destina-se a informar os leitores e não a instruir ou persuadir que cometam actos desagradáveis (de forma não ética) ou ilegais (criminosos).

LER ANEXO:

ALGUMA LEGISLAÇÃO IMPORTANTE PARA HACKERS

Este livro pode servir como apoio em testes de segurança informática, desde que obtidas as devidas autorizações pelos responsáveis dos sistemas ou pela administração da empresa respectiva. Aconselhamos que, em ambiente empresarial, obtenha sempre, por escrito, da administração da empresa/organização, autorização para os seus testes (neste caso, *Hacks*). Os *Hacks* assim realizados irão de certeza revelar vulnerabilidades de segurança e apontar soluções para a sua correcção.

O leitor pode, e deve, em primeiro lugar, aplicar os 50 *Hacks* no seu computador, evitando assim qualquer problema legal e, por outro lado, testando a segurança do mesmo.

O leitor assume todas as responsabilidades pela utilização da informação constante neste livro.

Porquê este livro?

A grande maioria dos utilizadores de sistemas operativos amigáveis como o Microsoft Windows XP não conhece muitas das suas funcionalidades, não está consciente dos riscos a que o seu sistema e dados estão sujeitos e não praticam hábitos seguros. Este livro pretende contribuir, positivamente, para corrigir essas atitudes, provocando a atitude de "casa roubada, trancas à porta".

Para quem é este livro?

Em poucas palavras: para os *Hackers* e para as vítimas, ou seja, para todos os que utilizam computadores com Microsoft Windows XP.

Considera-se neste livro um *Hacker* alguém que vai testar, com as devidas autorizações, a segurança do sistema e os conhecimentos técnicos de outrem, e como vítima qualquer utilizador de computadores que está sujeito às consequências naturais da falta de cuidados básicos na protecção do seu sistema e dados, independentemente de no seu passado ter sido ou não alvo de intrusões, vírus, ou outros problemas similares.

Para quem não é este livro?

Em poucas palavras: para os *Hackers* e para as vítimas que utilizam computadores com sistemas operativos que não pertencem à família de sistemas Microsoft Windows.

Existem diversos livros no mercado que aprofundam técnicas de *Hacking* para sistemas Unix, Linux ou mesmo DOS – sendo o mais conhecido o livro **Técnicas para Hackers – Soluções para Segurança** publicado em 2001 (1ª edição, e em 2002 a 2ª edição) pelo Centro Atlântico. O facto dos sistemas Unix e Linux terem menos de 10% da quota de mercado e do facto de um modo geral os seus utilizadores possuírem conhecimentos mais aprofundados de sistemas e tecnologias da informação e da comunicação, fez com que um manual com as características do presente livro se tornasse, nesta fase da massificação da Internet e do uso generalizado dos computadores em ambientes domésticos, académicos e profissionais, da maior importância e pertinência.

Como está organizado este livro?

Os 50 *Hacks* foram organizados em 6 capítulos, conforme estejam relacionados com o arranque do sistema, alterações à interface do Windows, ao funcionamento do Windows, a outras aplicações instaladas no sistema, à rede local ou ao hardware.

Procuraram-se descrever 50 *Hacks* simples e rápidos de serem realizados – apesar de terem grande impacto na integridade, confidencialidade e/ou disponibilidade do sistema –, com níveis de dificuldade para a necessária correcção (pelas vítimas) muito variáveis. Indica-se para tal, para cada *Hack*, o tempo médio para a sua realização. Teremos assim presente em cada *Hack* um relógio que varia entre 1 e 60 minutos indicando o tempo necessário para ser executado.

O tempo necessário para a vítima solucionar o problema causado pelo *Hack* variou muito nos nossos testes, dependendo da experiência, inteligência e... número de amigos da vítima. De 5 minutos a 5 meses, tudo poderá acontecer...

O capítulo de Anexos destina-se a tornar mais sólidos os conhecimentos dos leitores, garantindo uma aplicação correcta e consciente dos *Hacks* propostos. Para tal, e da primeira vez que um *Hack* requerer conhecimentos específicos tratados nesses Anexos, será efectuada uma chamada de atenção recomendando essa leitura antes da aplicação do *Hack*.

Notação utilizada

Para tornar a leitura mais rápida e eficaz foram adoptadas algumas normas de notação (comuns a outros livros do Centro Atlântico):

a) Linhas de código de programação (ou formatação) aparecem no tipo de letra Courier. Exemplo (*Hack* 36):

```
menu[label="Arquivo"], menu[label="Exibir"],
menu[label="Favoritos"], menu[label="Ajuda"] {

     display: none;

     }
```

b) Variáveis ou nomes de ficheiros ou de pastas aparecem a negrito, quando inseridas no meio do texto. Exemplo (*Hack* 36):

userChrome.css

c) Comandos que se activam mediante combinação de duas ou três teclas são indicados pela sua associação com um sinal de soma: Exemplo: CTRL+ALT+DEL ou ALT+F10.

d) Nomes de menus, comandos, opções ou nomes de teclas surgem em maiúsculas pequenas. Exemplos: ARQUIVO, OPÇÕES, CTRL.

e) Quando for necessário seleccionar um conjunto de menus e comandos sucessivos tal é indicado pelo sinal de maior (>). Exemplos: FERRAMENTAS > OPÇÕES ou FILE > PRINT.

f) Como o hardware e software referidos ao longo deste livro muito dificilmente poderão ser adquiridos (com alguma vantagem) em Portugal, os preços são sempre indicados em dólares americanos, através da sigla "US$".

Ícones utilizados

Cada *Hack* tem associado de 1 a 4 ícones, com os seguintes significados:

Indica o tempo necessário para reproduzir o *Hack* no computador da vítima. O tempo varia entre 1 e 60 minutos. Claro que em muitos casos o *Hack* deve já ter sido testado num outro computador para que seja possível, depois, no tempo indicado, ser implementado no computador da vítima. Por outro lado, alguns *Hacks* requerem software adicional ou ficheiros de apoio; nestes casos, pressupomos que quando se desloca para o computador da vítima já tem consigo quer o software quer todas as imagens ou sons necessários.

Este ícone é uma mera advertência que indica que para realizar o *Hack* precisará aceder ao Registry. Serve também para recordar que o anexo sobre o Registry deve ser lido antes de editar o Registo do Windows. E, já agora, recorda-o da necessidade de fazer uma cópia de segurança ao Registry antes de o editar.

Sempre que estiver presente na página de título de um *Hack* este ícone informa-o que deverá efectuar o *download* e instalar software adicional.

Neste caso (só acontece em três situações) deverá estar preparado com hardware especial para que possa aplicar o *Hack*.

Hackers e *Crackers*

Principalmente depois do 11 de Setembro de 2001, os governos (com especial destaque para o americano) e os média passaram a referir-se aos *Hackers* e suas actividades como que relacionadas com o ciberterrorismo. Nada mais errado!

Um *Hacker* (no contexto da informática) pode ser entendido como um interessado em tecnologias da informação e da comunicação e que se dedica a desvendá-las. O seu propósito é o de resolver problemas, desenvolver capacidades e exercitar a inteligência... mesmo que para tal utilize vítimas reais! Trata-se muitas vezes do designado Ethical Hacking (*white-hat hacking*, normalmente associado ao *Penetration testing*) que é tão útil quanto o trabalho (também considerado de *hacking*) relativo ao teste e avaliação de versões alfa ou beta de um determinado software.

Um *cracker* (ou *black-hat hacker*), por outro lado, usa esses mesmos conhecimentos mas de forma mal-intencionada ou mesmo criminosa, com a intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros – NÃO é disto que trata este livro.

De acordo com o código de ética dos *Hackers,* um *Hack* deve:

- Ser seguro;
- Não estragar nada;

LER ANEXO:

HACKERS, CRACKERS E PHREAKERS, ENTRE OUTRAS PERSONAGENS!

- Não magoar ninguém (nem fisicamente, nem emocionalmente);
- Ter piada (bem, pelo menos para alguns; daí também podermos designar alguns dos *Hacks*, os tais com piada assegurada, como *Pranks*); e
- Ser inteligente.

Neste livro tudo foi feito para não defraudar esse código.

Requisitos prévios à aplicação dos *Hacks* deste livro

1. Existem *requisitos legais, éticos e técnicos fundamentais* a satisfazer antes de aplicar os *Hacks* deste livro.

Legais:

a) Obter autorização, por escrito, do proprietário do computador a utilizar, ou responsável legal caso se trate de uma instituição.

b) Não causar prejuízo a outrem ou procurar obter um benefício ilegítimo, para si ou para terceiros.

Éticos:

a) Apenas realizar um *Hack* quando entender que percebeu o seu pleno funcionamento, a operação inversa respectiva (para voltar a colocar o sistema no seu estado inicial) e estar consciente de que uma pequena falha na aplicação do *Hack* pode tornar o computador inoperacional (ver requisitos técnicos a seguir).

Técnicos:

a) Providenciar uma cópia de segurança (*backup*) completa do sistema e idealmente um segundo *backup* apenas das pastas dos dados do utilizador;

b) Ter à mão o CD de instalação do Windows XP da máquina a ser *hackada*;

c) Ter acesso, ao nível de administrador, ao computador a ser *hackado*;

d) Ter o acesso à Internet activo nesse computador.

e) Ter consciência que nem o autor nem o editor nem outras pessoas e entidades envolvidas na concepção e edição deste livro estarão disponíveis para solucionar qualquer dúvida ou problema resultante da aplicação dos 50 *Hacks*.

Como conseguir acesso ao computador da vítima?

A primeira pergunta que o leitor poderá fazer quando iniciar a leitura deste livro é a seguinte: "Mas como é que obtenho acesso ao computador da minha vítima, pois não possuo qualquer *password* para tal?". Pois bem, para tal, poderá,

LER ANEXO:
ENGENHARIA SOCIAL

1. recorrer a uma qualquer técnica de Engenharia Social;

2. esperar por um momento de distracção e quando a sua vítima abandonar o sistema, para, por exemplo, ir ao WC ou tomar café, deixando as sessões abertas, criar um novo utilizador para mais tarde utilizar;

3. utilizar a *password* da vítima caso a conheça, ou através da respectiva disquete criada com a opção PREVENIR O ESQUECIMENTO DE PALAVRA-PASSE, em PAINEL DE CONTROLO > CONTAS DE UTILIZADORES;

4. utilizar software tipo *keylogger* ou *spyware* para registar o que é escrito no teclado ou para receber *snapshots* do ecrã do computador;

5. esperar que a vítima aceda à Internet, sem um *router*, e instalar uma *backdoor* no respectivo computador;

6. se mesmo assim não conseguir, resta-lhe esperar pela 3ª edição deste livro (bora lá a pedir aos amigos para comprarem todos um exemplar), onde irei mostrar como mesmo sem qualquer *password* e sem espiar a vítima ou os seus papéis se consegue entrar num computador com Windows XP.

Ah! e de duas formas distintas ;-)

Vamos lá. Mãos à obra!

HACK 19

"RELIFTING" COMPLETO À INTERFACE

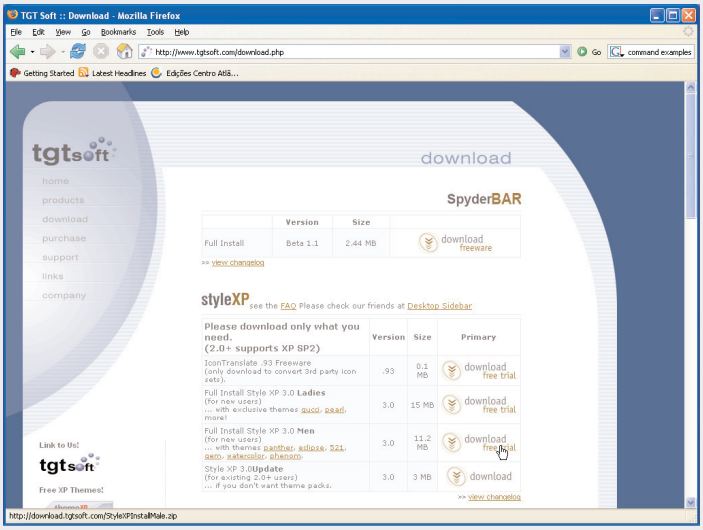
Introdução »

Se já viu o resultado do *relifting* na Cinha Jardim ou na Lili Caneças então deverá ter ficado com uma má impressão dessas técnicas pois nada conseguem fazer às mãos ou à pele do pescoço. No nosso caso, e com o apoio dos Temas, vamos mesmo tornar a pele completa de um computador umas dezenas de anos mais nova.

Os temas possibilitam guardar, de forma centralizada, a configuração visual e áudio de cada computador, o que inclui os valores para os tipos de letra, cores, estilos visuais, papéis de fundo, protecção de ecrã, cursores e sons utilizados.

Aquando da instalação, o Windows XP inclui dois temas: Windows XP e Windows Clássico (confira clicando com o botão direito do rato na área de trabalho e depois em PROPRIEDADES > TEMAS). Neste *Hack* vamos utilizar o software Style XP 3.0 da TGTSoft (poderia ser, por exemplo, e em alternativa, o Object Desktop da Stardock) e temas do *site* ThemeXP.

Funcionamento »

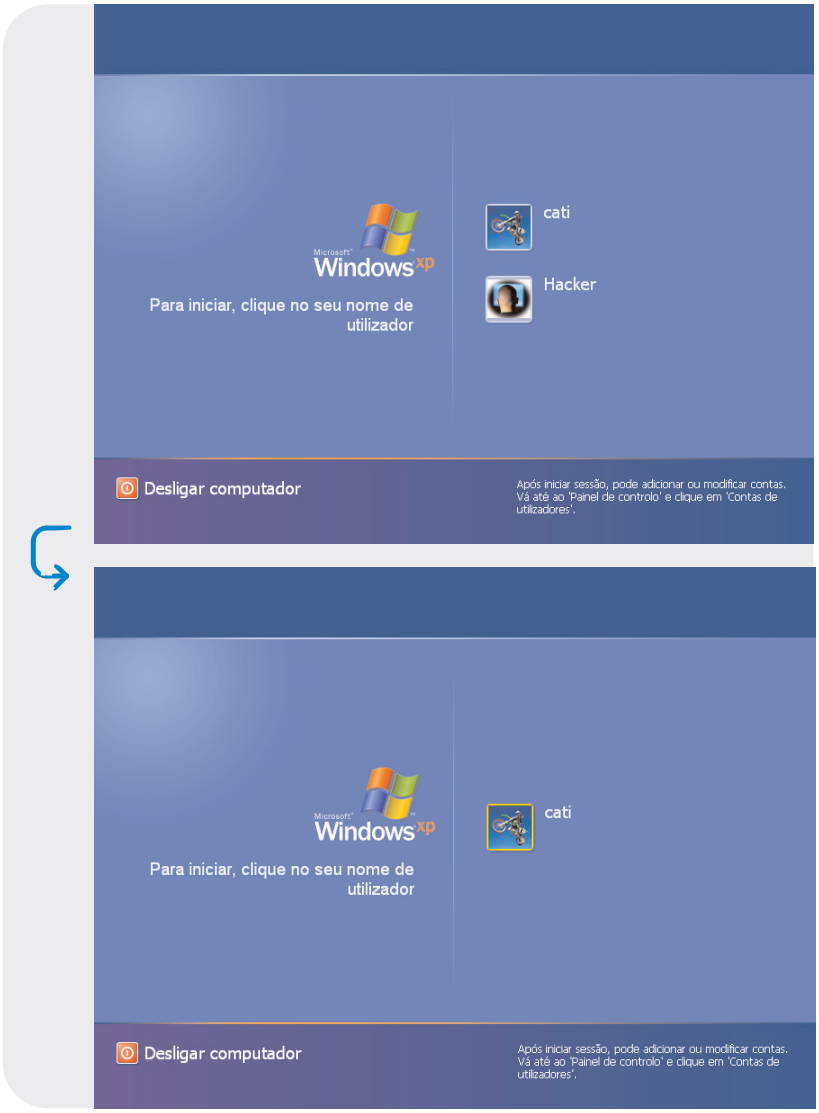


01.

Faça *download* (*http://www.tgtsoft.com/download.php*) instale e execute a aplicação StyleXP 3 para instalar os seus novos temas.

HACK 22

NÃO DEIXAR RASTOS NO ECRÃ DE LOGON



Introdução »

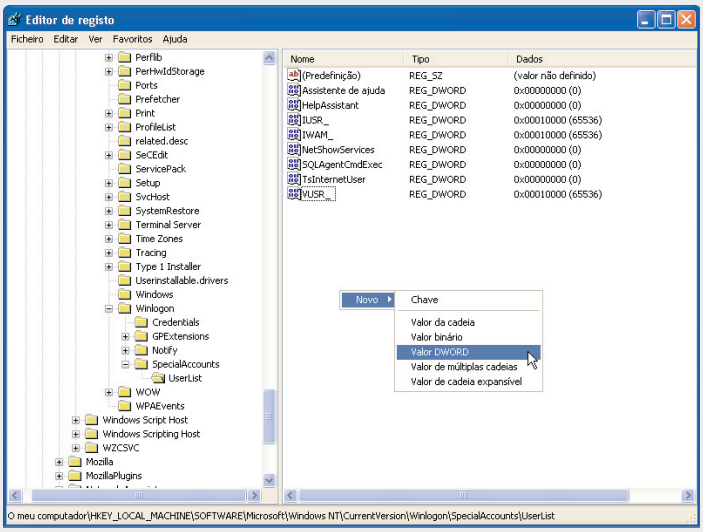
Como vai passar a frequentar com assiduidade o computador da(s) sua(s) vítima(s), a primeira coisa que o(a) poderá preocupar é o rasto que possa deixar. Começando pela forma de acesso, vamos supor que criou um utilizador (não vá a vítima descobrir como listar as entradas no sistema e verificar que existem registos em horários em que ela estava, por exemplo, a dormir ou a almoçar). Depois de criar o seu próprio utilizador no Windows, este passa a listá-lo no ecrã de *logon* juntamente com todos os utilizadores definidos. Temos então que esconder essa referência.

Funcionamento »

01.

Aceda ao Editor de Registo (INICIAR > EXECUTAR > REGEDIT) e localize e abra a chave `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList`

02.



Para adicionar um nome à lista, com o botão direito do rato faça NOVO > VALOR DWORD. Como nome da chave escreva o nome da conta.

HACK 41

QUE SITES CONSULTA A MARIAZINHA DURANTE O TRABALHO?

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.

Introdução »

O *sniffer* (para capturar os pacotes que atravessam a rede), ou Network Analyzer, que iremos utilizar, é o Ethereal (*open source* disponível para Windows, Unix e Linux). Para utilizar o Ethereal precisa também instalar o software WinPcap.

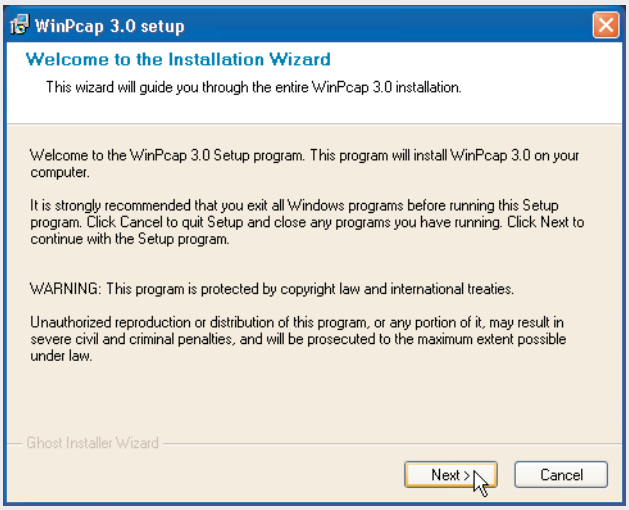
Neste primeiro *Hack* vamos descobrir que *sites* é que a nossa vítima anda a consultar na Web.

LER ANEXO:

NAVEGAR ANONIMAMENTE PELA INTERNET

Se não desejar que conheçam os *sites* por onde navega, deve ler o anexo sobre este assunto.

Funcionamento »



01.

Faça *download* (*http://winpcap.polito.it*) e instale a aplicação WinPcap.