



50 HACKS

para o Windows XP

[Hugo Caramelo]

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

Colecção: Tecnologias

Autor: Hugo Caramelo

Direcção gráfica: António José Pedro

Revisão final: Centro Atlântico

Capa: António José Pedro

© Centro Atlântico, Lda., 2005

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

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.

I 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 e Crackers</i>	11
Requisitos prévios à aplicação dos <i>Hacks</i> deste livro	12
Como conseguir acesso ao computador da vítima?	13
 HACKS NO ARRANQUE DO WINDOWS	 15
1. Personalizar o ecrã de abertura (<i>Windows boot screen</i>)	16
2. Esconder o ecrã de abertura	24
3. Personalizar o ecrã de inicialização	26
4. Personalizar o ecrã de <i>logon</i>	30
 HACKS NA INTERFACE	 35
5. Esconder a Área de Notificação	36
6. Inserir uma mensagem anexa ao relógio	40
7. Esconder a lista de programas do menu Iniciar	44
8. Esconder um programa do painel Iniciar	48
9. Adicionar um <i>link</i> para Marte no painel Iniciar	52
10. Alterar os detalhes visíveis no Explorador do Windows	58
11. Aumentar as miniaturas!	62
12. Limitar as imagens das contas de utilizadores	66
13. Remover todos os ícones do ambiente de trabalho	70
14. Mudar o nome da Reciclagem	74
15. Alterar os ícones do ambiente de trabalho	76

16. Alterar o cursor	80
17. Alterar o som de erro do Windows	84
18. Apresentar um ambiente de trabalho congelado	88
19. <i>Relifting</i> completo à interface	94

HACKS NO FUNCIONAMENTO DO WINDOWS	105
--	------------

20. Um computador que se desliga sozinho!	106
21. Atalhos enganadores	108
22. Não deixar rastros no ecrã de <i>login</i>	112
23. Revelar as <i>passwords</i> !	116
24. Impedir o acesso a programas	122

HACKS PARA OUTRO SOFTWARE	127
----------------------------------	------------

25. Word: Alterar o modelo para criação de novos documentos	128
26. Word: Texto invisível	134
27. Excel: Assustar o utilizador com uma mensagem de “boas”-vindas	136
28. Excel: Esconder menus	140
29. Internet Explorer: Navegação em modo quiosque	144
30. Internet Explorer: <i>Home-Page</i> inalterável	146
31. Internet Explorer: Limitar o acesso à Web	150
32. Internet Explorer: Alterar o logo	154
33. Internet Explorer: Alterar a animação do logo	158
34. Internet Explorer: Alterar o fundo da barra de ferramentas	162
35. Internet Explorer: Alterar o texto na barra de título	168
36. Mozilla Firefox: Onde estão os meus menus?!	172
37. Mozilla Firefox: Limitar o acesso à Web	178
38. Outlook Express: Fruta e flores no fundo das mensagens de e-mail	182
39. Outlook Express: <i>You’ve got mail</i> (em voz alta)	186
40. Outlook Express: Nova página de boas-vindas	190

HACKS EM REDES LOCAIS	195
------------------------------	------------

41. Que <i>sites</i> consulta a Mariazinha durante o trabalho?	196
42. Quais são as <i>passwords</i> da Mariazinha?	204
43. <i>Spray</i> para maiores velocidades nas redes Wi-Fi	206

HACKS NO HARDWARE	209
44. Uma impressora que trabalha sozinha!	210
45. Trocar os botões do rato	212
46. Botão de pânico	214
47. Modificar o funcionamento do teclado	216
48. Transformar o teclado numa máquina de escrever	220
49. Webcam transformada em <i>spycam</i>	224
50. Dividir a imagem do ecrã por 2 monitores	230
 ANEXOS	 233
ANEXO 1 - <i>Hackers, Crackers e Phreakers</i> , entre outras personagens!	235
ANEXO 2 - <i>Hackers</i> famosos (nem sempre pelos melhores motivos...)	241
ANEXO 3 - <i>Passwords</i> (palavras-passe)	247
ANEXO 4 - Engenharia Social	253
ANEXO 5 - <i>Malware</i>	255
ANEXO 6 - As 6 fases no arranque do Windows XP	265
ANEXO 7 - O Registry (Registo do Windows)	271
ANEXO 8 - Informação sobre o computador	285
ANEXO 9 - Navegar anonimamente pela Internet	299
ANEXO 10 - Os caminhos das mensagens de correio-electrónico	301
ANEXO 11 - <i>Sniffers</i>	313
ANEXO 12 - As 7 dicas básicas para conectividade sem fios em segurança	315
ANEXO 13 - Localizar redes Wi-Fi com computador	319
ANEXO 14 - Localizar redes Wi-Fi sem computador	321
ANEXO 15 - Alguma legislação importante para <i>Hackers</i>	323

I 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).

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.

LER ANEXO:



**ALGUMA LEGISLAÇÃO
IMPORTANTE PARA
HACKERS**

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:

- Obter autorização, por escrito, do proprietário do computador a utilizar, ou responsável legal caso se trate de uma instituição.
- Não causar prejuízo a outrem ou procurar obter um benefício ilegítimo, para si ou para terceiros.

Éticos:

- 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:

- Providenciar uma cópia de segurança (*backup*) completa do sistema e idealmente um segundo *backup* apenas das pastas dos dados do utilizador;
- Ter à mão o CD de instalação do Windows XP da máquina a ser *hackada*;
- 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,

1. recorrer a uma qualquer técnica de Engenharia Social;
2. esperar por um momento de distração 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!

LER ANEXO:



ENGENHARIA
SOCIAL

HACK 19

“RELIFTING” COMPLETO À INTERFACE



30 MIN.



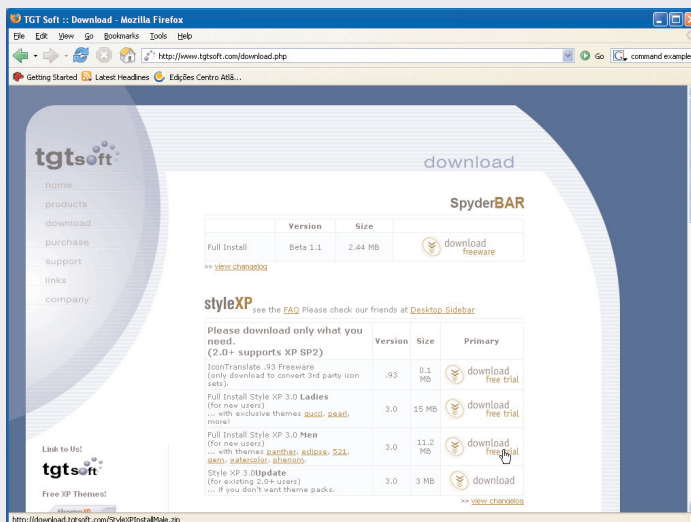
Introdução >>

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 da *site* ThemeXP.

Funcionamento >>



01.

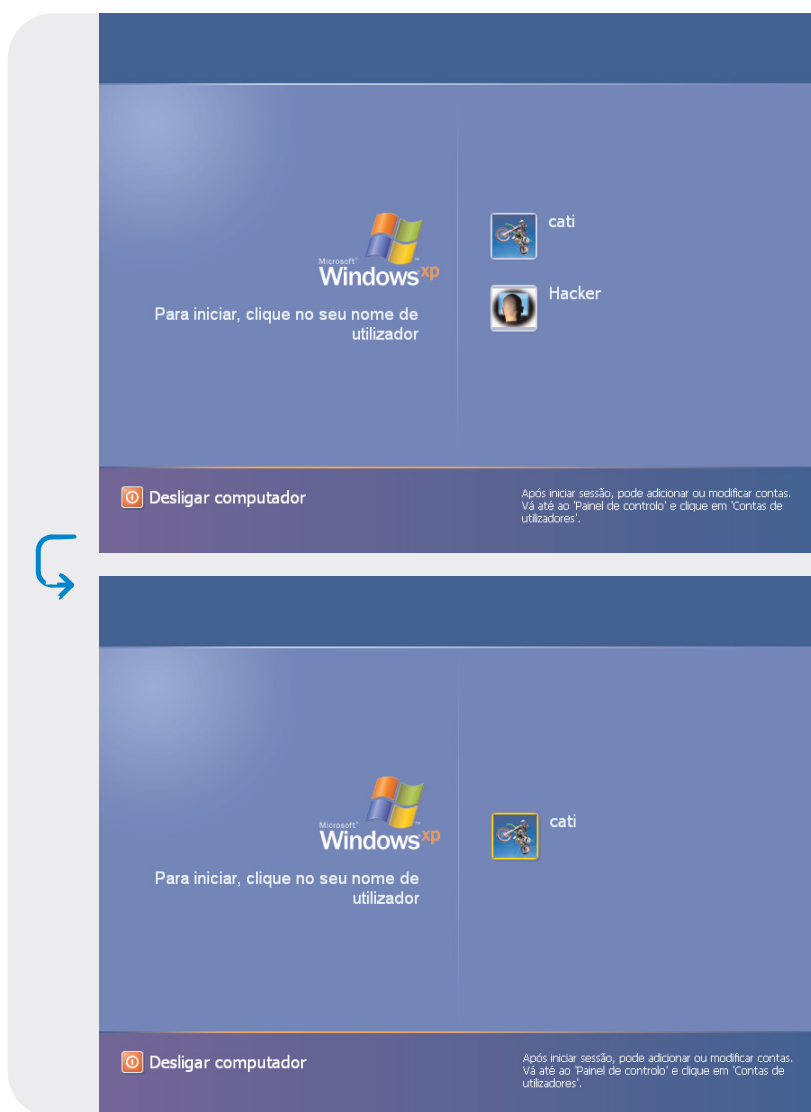
Faça download (<http://www.tgtsoft.com/download.php>) instale e execute a aplicação StyleXP 3 para instalar os seus novos temas.

HACK 22

NÃO DEIXAR RASTOS NO ECRÃ DE LOGON



2 MIN.



Introdução >>

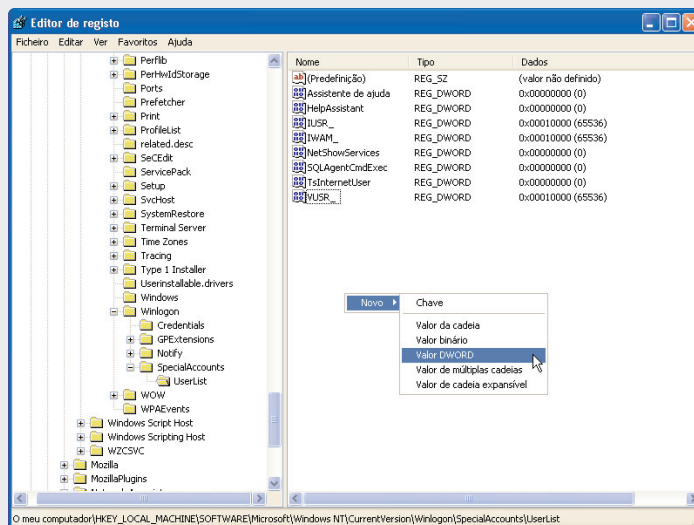
Como vai passar a frequentar com assiduidade o computador da(s) sua(s) vítima(s), a primeira coisa que o(a) poderá preocupar é o rasto que possa deixar. Começando pela forma de acesso, vamos supor que criou um utilizador (não vá a vítima descobrir como listar as entradas no sistema e verificar que existem 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?



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.

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.

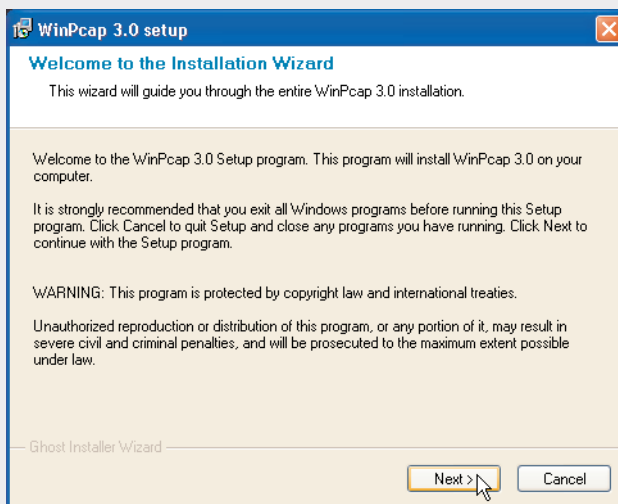
LER ANEXO:



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.