REVISTA HACKER BRASIL

> Ano 1 - N.00 - Dezembro de 2004
http://www.cursodehacker.com.br

DISTRIBUIÇÃO GRATUITA

\\Filosofansas\

Porque o hacker tem que ser mais inteligente que os outros.

\\Invasão de Natal\

Aproveite a ausência dos funcionários.

\\Hackeando Sem Ferramentas\

Ou você é hacker ou não é.

\\Windows x Linux\

Afinal, qual é o melhor sistema para hackear?

\\CISSPBR\ POR QUE TANTA INCOMPETÊNCIA ENTRE PROFISSIONAIS CERTIFICADOS?

O ano de 2004 está prestes a terminar e posso dizer que foi o ano em que o ***Curso de Hacker*** *teve a sua Prova de Fogo (TVE).*

Comemoramos o primeiro aniversário em junho e como presente, recebemos a maior onda de ataques e tentativas de censura que o ***Curso de Hacker*** *já teve desde que foi inaugurado.*

O simples fato de existir um 'curso de hacker', fez com que 'respeitáveis profissionais de TI' nos dirigisse todo o tipo de ofensa moral e pessoal.

Vindo dessa gente eu esperava ataques direcionados ao conteúdo do curso. Mas faltou competência ou decência para atacar o conteúdo. Os ataques foram pessoais; dirigidos a mim. Pessoas que nunca me viram na vida se comportando como se eu já as tivesse sodomizado em vidas passadas. E é nas mãos destas pessoas que as grandes empresas deixam seus servidores. Leia mais sobre a 'competência' dos profissionais de TI ainda nesta edição.

Os ataques não ficaram só na ofensa pessoal. Foi o mês que mais tentativas de invasão nosso site sofreu e eu não creio em coincidência. Não precisa dizer que nenhuma foi bem sucedida. Afinal, ou sou hacker ou não sou. Mas vindo de quem se diz 'ético' e 'abomina' invasões, o talo é um, o falo é outro.

*No meio da festa, eis que surge um divertido e-Mail da Fapesp (**http://Registro.br**), a responsável pelo registro de domínios no Brasil, sobre 'supostas irregularidades' na documentação enviada para registrar o domínio.*

(Re)Enviamos a documentação, que foi aceita sem problemas. E não poderia ser diferente, já que a irregularidade só existe na mente dos censores.

*Só que isto não bastou. Nem dez dias se passaram e nova notificação. Se em quinze dias não enviassemos (de novo?) a documentação, o domínio **www.cursodehacker.com.br** estaria fora do ar. Fizemos um novo envio e assim que acusaram o recebimento, liguei para o setor jurídico da Fapesp e exigi satisfações. Na verdade já estava pronto para ir a São Paulo tirar esta história a limpo. Nada melhor que olho no olho para resolver certas pendengas.*

Não foi preciso. O pessoal me pediu desculpas e alegou ser necessário tomar esta providencia toda vez que existe alguma denúncia. Infundada ou não.

Como vêem, tem muita gente interessada em manter em segredo as falhas de segurança. E é justamente o segredo em torno das falhas que causa a insegurança e mantém empresas certificadoras, prestadores de serviço e profissionais de TI, empregados e bem pagos. Estamos fazendo mais pela segurança na Internet que este pessoal que se esconde atrás de caríssimas certificações. Afinal, quem certifica as certificadoras?

Qualquer tentativa de nos calar é censura. Os hackers não criaram o problema de segurança. Os hackers alertam sobre as falhas. Quem tem obrigação de corrigi-las é quem as produz. Por isto incomodamos tanto.

Junte-se a nós e contibua para tornar a Internet mais segura, nem que para isso tenhamos que quebrar tudo.

HACKER1

EXPEDIENTE

Revista Hacker.BR

"A Revista do Curso de Hacker."

Dez2004 - Jan2005

DISTRIBUIÇÃO GRATUITA

A revista **Hacker.BR** *é mantida pelo* ***Curso de Hacker*** *do* ***Profº Marco Aurélio Thompson*** *e só está disponível no formato digital. A distribuição é gratuita, via download e a periodicidade é bimestral.*

Site oficial da revista **Hacker.BR***:*

http://www.cursodehacker.com.br

Editor:
Marco Aurélio Thompson
Diagramação:
Marco Aurélio Thompson
Revisão:
Marco Aurélio Thompson
Capa:
Marco Aurélio Thompson
Colaboradores desta edição:
Jonas Lopes
Leonardo Bueno

Contatos com a redação e envio de artigos para publicação:

atendimento@cursodehacker.com.br

\\Vá de Telnet

Telnet é um recurso da Internet que permite a conexão com outro computador. O seu micro passa a ser um terminal e você pode estar com um sistema operacional instalado e trabalhar em outro.
Como estamos falando de um recurso da Internet, isto siginifica que você poderá acessar computadores em qualquer lugar do mundo.
Antes mesmo da Internet ser liberada aos brasileiros, já era possível usar a Internet via Telnet, um serviço oferecido por alguns BBSs.
Quem nasceu no mundo das janelas, com certeza vai precisar de algum tempo para se acostumar a navegação por menus, linhas de comandos e a lentidão da conexão em alguns casos.
Se é tão arcaico assim, por que um hacker precisa aprender Telnet? Bem, primeiro por que um hacker precisa conhecer a base do funcionamento da Web. Isto inclui Telnet. E depois, por que apesar de ser arcaico, o Telnet é usado até hoje.
Você poderá ter acesso ao seu e-Mail, acessar bancos de dados, catálogos de bibliotecas, ferramentas de procura de informações, (des)configurar roteadores, fazer defacements, etc...

Eu quero...

Como esta coluna é para iniciantes, supomos que a maioria usa o Windows. Então siga o roteiro abaixo:

```
Iniciar -> Executar -> cmd -> OK
```

Na janela que vai aparecer, digite:

```
telnet
```

Vai aparecer o prompt:

```
Microsoft Telnet>
```

Estes são alguns comandos disponíveis:
c ou **close** para fechar a conexão atual sem sair do Telnet.
d ou **display** para exibir informações sobre a configuração.
o ou **open nome_ou_IP_do_servidor [port]** para se conectar a outro micro. A porta padrão é 23.
q ou **quit** para encerrar o Telnet.
set para definir opções. Digite **set ?** para detalhes.
sen para enviar seqüências de caracteres ao servidor.
st ou **status** para saber mais sobre a conexão atual.
u ou **unset** para anular definições de opções. Digite **unset ?** para detalhes.
?/h ou **help** para exibir as informações de ajuda.

O cliente de Telnet do Windows possui limitações que o tornam pouco atrativo para uso hacker. Quebra um galho quando só temos o Windows por perto ou como agora, para você dar os primeiros passos com Telnet. Eu particularmente recomendo o uso do PuTTy, cujo uso é ensinado no Curso de Hacker, no Livro Vermelho do Hacker Brasileiro e em uma das edições futuras da **Hacker.BR**.

Para acessar um micro via Telnet é só digitar:

```
telnet nome_do_computador
```

ou

```
telnet IP_do_computador
```

No exemplo acima não especificamos a porta, que vai ser a padrão, a 23. Para especificar a porta basta informá-la no final da linha de comando. Suponha que eu queira acessar por Telnet o IP **255.255.255.255** usando a porta **110**:

```
telnet 255.255.255.255 110
```

E se eu quiser acessar o servidor **www.vitima.com.br** pela porta **23**:

```
telnet www.vitima.com.br
```

Acessando o e-Mail via Telnet

Uma tarefa bem legal usando Telnet é o acesso a sua conta de e-Mail. E quem acessa por conexão discada e fica mordido quando o e-Mail tem um anexo e

demora a ser baixado, use Telnet para apagar os e-Mails indesejados, antes de baixá-los do servidor. Faça assim:

```
telnet pop3.bol.com.br 110
```

No exemplo acima eu usei o BOL, você deve usar o provedor da sua conta de e-Mal. Significa que estamos acessando a porta 110 do servidor de e-Mail. Se tudo estiver OK deverá aparecer a seguinte mensagem ou algo parecido:

```
+OK POP server ready
```

Agora entre com seu nome de usuário, digitando:

```
user nome_de_usuario
```

Aparecerá uma mensagem do tipo:

```
+OK Password required for
nome_de_usuario
```

Agora entre com a sua senha:

```
pass sua_senha
```

Supondo que exista 4 mensagens no servidor, vai aparecer algo assim:

```
+OK 4 messages
```

Para visualizar o tamanho de cada mensagem em bytes:

```
list
```

Em nosso exemplo este é o resultado:

```
+OK
1 11925
2 15049
3 15075
4 4572
.
```

Para ler a mensagem 3:

```
retr 3
```

Obs.: Se a mensagem tiver formatação HTML, as TAGs também serão exibidas.

Para apagar a mensagem de número 1:

```
dele 1
```

Aparecerá o seguinte aviso:

```
+OK message 1 deleted.
```

Usando o comando list novamente, vemos que a mensagem 1 não está mais disponível:

```
list

+OK
2 15049
3 15075
4 4572
.
```

Na verdade ela não foi realmente apagada. Só está marcada para ser apagada e isto só acontecerá se você encerrar a sessão com **q** ou **quit**.

Se você se arrependeu e quer recuperar a mensagem, é só usar o comando:

```
rset
```

Para saber quem enviou a mensagem 2, digite:

```
top 2 0
```

Neste artigo, espero ter aberto sua mente para as possibilidades que o Telnet oferece. Acessar a conta de e-Mail por Telnet é uma ponta do iceberg.

Próximos textos relacionados: manual do PuTTY, SSH, Telnet no Linux, e-Mail anônimo via Telnet, dissecando uma sessão de Telnet.

\\A (In)Competência dos Profissionais de TI

O tipo que mais se ofende quando o assunto é hacker, são os profissionais de TI. Em um primeiro momento não quis me preocupar em analisar o porquê desta conduta. No meu entender, os profisisonais de TI deveriam ser os primeiros a oferecer soluções para os problemas de segurança. Um site como o Infogarra por exemplo, cujo dublê de webmaster se vangloria de ser um 'profissional respeitável', não serve para nada mais que confirmar nossa teoria, título desta matéria.

Os profissionais de TI elitizados, aqueles que cuidam da segurança das maiores empresas nacionais, aqueles mesmos que gastam o equivalente a um carro popular para obter certificações, são os que deveriam ter a solução para os problemas da Internet. De quebra ficariam milionários com isso.

Só que na prática não é o que acontece. Os ataques pessoais dirigidos a mim pelo pessoal da lista CISSPBR e anteriormente o feito pelo Editor do site TIMaster, que acabou gerando um processo contra este indivíduo, demonstra o grau de ignorância, indecência e incompetência que premeia o meio de TI.

Após o episódio já comentado em nosso editorial, passei a aocmpanhar os posts da lista CISSPBR e também da Perícia Forense, que de alguma forma é conivente com os elementos da primeira. Preferia não tê-lo feito. No meio de perguntas pertinentes ao tema do grupo, vez ou outra surge umas baboseiras dignas de dó. O pior é que estes elementos assinam em baixo. Dão o nome da empresa em que trabalham ou o site que mantém. Um prato cheio para um hacker agir. E completam com uma sopa de letrinhas após seus nomes: CISSP, MSCO, FDP, como se só isto bastasse para ele ser o "Rei do Pedaço" (FOX). Não troco meu diploma da *Hard Life School* por nenhuma destas siglas exotéricas.

Mas convenhamos, depois de gastar os tubos para ser conhecido como CHISP ou coisa que o valha, o indivíduo tem mais é que defender a sua bandeira, a exemplo do que fazem os gays com aquela passeata gigante que meu primo e o Samuca não perdem uma.

Na coluna Filosofansas você vai entender que as pessoas criam seus mundos e os torna realidade a quantos acreditarem nele. Os loucos são assim. Vários filmes exploram este argumento. Um louco chega na cidade, revoluciona tudo e depois é execrado, quando o sabem louco. O profissional de TI chega na empresa com um monte de CISS debaixo do braço, geralmente indicado por outro CISS, e como o louco, enquanto todos acreditarem nele, será tratado como "O Palhaço" (Multishow).

Um hacker é a peça que faltava para dizer que o "Rei Está Nú" (Teatro da UfBA). Daí tanto medo. Daí tantos ataques emotivos a pessoa e não a obra, ao contéudo, ao resultado dos anos de pesquisa. E não precisa ir muito longe para entender o porquê do profissional de TI carecer de competência para manter os hackers fora das suas redes. O treinamento deste pessoal é voltado a elaboração de estratégias para restaurar um sistema em caso de incidente. Também inclui estratégias de defesa, todas conhecidas, o que as torna ineficazes contra os ataques bolados por uma mente hacker. Sabem lidar com o problema, sem a competência para resolvê-lo de forma definitiva.

Aos poucos as empresas estão percebendo que os TIs não dão conta do recado. Começa a surgir os cursos e certificações de Ética Hacker. Afinal, contra hackers só hackers. Um hacker está sempre a frente e vai desenvolver soluções para ataques que nem existem ainda. Um hacker é desonrado quando uma rede sob sua responsabilidade é invadida. Um profissional de TI, invariavelmente, esconde isto dos seus patrões. Não quer perder o contra cheque no final do mês. Já um hacker invadido, se levanta dez vezes mais forte. Enquanto os TIs passam a noite preocupados com a invasão de seus sites, os hackers passam a noite desenvolvendo novas técnicas de ataque e a respectiva estratégia de defesa. Quem você acha que ganha esta batalha? Não precisa responder, enquanto existir este número absurdo de invasões, já sabemos quem está na frente.

Por Dr. Jorge Picanças, CHISP, FDP, ABCD

\\Invasão Sem Ferramentas

O que difere um Hacker de um Aracker é a sua capacidade de realizar ações hacker sem o uso de programas de invasão. A maior prova do que estou dizendo você encontra na história do hackerismo, quando o Capitão Crunch burlou o sistema de telefonia americano com um apito de plástico.
O segredo é a mente hacker. A capacidade de encontrar falhas nos sistemas mais complexos e com milhares ou milhões de dólares envolvidos no projeto. Um Script Kiddie pode ou não chegar a ser hacker. Vai depender dele ter ou desenvolver a mente hacker.
Um hacker pode ser útil as empresas de diversas formas. E não é só na área de TI. Informe o problema e saia de perto. Hackers são especialistas em encontrar falhas. São as falhas que causam os problemas. Crie um plano de marketing e peça para um hacker analisar. Não se espante se tiver que mudar mais de 60% do projeto original. Explique a um hacker como funciona sua linha de produção e prepare-se para reduzir as etapas do processo e ter aumento de produção com redução de custos.
Você já viu um estereograma? São figuras com imagens em 3D escondidas. Só dá para ver bem de perto e se concentrando. Mas tem gente que não enxerga de jeito nenhum. Por mais que você dê dicas, descreva o que a pessoa deveria estar vendo. Nada. Não enxergam mesmo.
Isto ocorre também com os problemas de segurança. Estão lá. Fáceis de enxergar. Só que nem todos enxergam. Acredito ser esta a principal qualidade do hacker.
Um site como o **www.stockphotos.com.br** por exemplo, que vive de vender fotografias digitais, pode ser facilmente burlado:

Link protegido:
`http://www.stockphotos.com.br/dotnet/fotoprotegida.aspx?caminho=http://www.stockphotos.com.br/fotos/RF15/grandes/IS145-031.jpg`

Link desprotegido:
`http://www.stockphotos.com.br/fotos/RF15/grandes/IS145-031.jpg`

Quanto ganhou a empresa que fez este site? Assim eu também quero. E este aqui:

`http://www.consad.org.br/Login/Index.asp`

Experimente digitar **`Admin`** no campo login e **`' or '1`** como senha e veja o que acontece. Você ainda quer que eu acredite que não tem (pouca) incompetência no mundo da TI? Quer que eu acredite que os hackers é que são os caras maus? Um outro site facilmente invadido sem ferramentas é este:

Link protegido:
`http://www.seminarios.com.br/downsub.asp?download=nao`

Link desprotegido:
`http://www.seminarios.com.br/downsub.asp?download=sim`

Que brincadeira é essa? Dá a impressão que as falhas são deixadas de propósito. A empresa que fez o site ainda divulga seu nome na página principal do cliente. Que tal visitar cada site feito por ela para ver como está a segurança?
Já vimos que com Telnet temos acesso a outro sistema operacional. É possível rodar scripts e compilar programas Unix a partir de um Pentium 100, rodando Windows 95 e com conexão discada. Qual Kiddie consegue isto?Um hacker deve ser capaz de alcançar resultados com qualquer máquina, com qualquer sistema operacional e com qualquer conexão. Afinal, ou se é hacker ou não é.

Por I. Pay Day

Você está realmente seguro? Seus arquivos estão seguros em seu computador?

Segurança, eis a questão!

Todos acham que só acontece com os outros. Mas quando os arquivos começam a sumir e o computador foge ao controle, aí você se dá conta: fui invadido!!!

Qual foi a técnica desta invasão? Quem fez? Como fez? Quem é o inimigo? Qual é o motivo? Como ficou o computador após a invasão?

Isto pode ser evitado com procedimentos básicos de segurança. Nesta seção você vai conhecer estes procedimentos e saberá preparar seu computador para transformá-lo em uma fortaleza.

Como o hacker consegue invadir um computador? Vou explicar. Todo sistema tem falhas e é passivo de invasão. A culpa então é do Sistema Operacional? Não necessariamente. Quando digo sistema, falo de um todo que é formado por três camadas, que de fora para dentro protege seu computador e seus dados. São as seguintes: Firewall, Antivírus e Sistema Operacional (veja a figura 1).

A palavra que vai definir a qualidade da sua segurança é **atualização**. Todo o sistema tem que estar atualizado, pois os hackers aproveitam-se das falhas divulgadas em listas de discussão, fóruns e sites de segurança. Por isso é imprescindível que você mantenha todo o sistema (as três camadas) atualizado. Não basta colocar um sistema operacional novo e um antivírus da moda. Se faltar o firewall por exemplo, seu micro ainda estará vulnerável. Além disso você precisa manter tudo atualizado. Frequentar fóruns e listas de discussão também ajuda bastante. É lá que surgem as primeiras mensagens divulgando falhas de segurança. Se você souber primeiro que o hacker, ponto pra você.

Figura 1

Por Jonas Lopes

Firewall "Tradicional": software ou hardware que normalmente fica em dispositivo dedicado e que é posicionado entre duas ou mais redes. Estas podem ser, por exemplo, a rede interna (LAN) e a rede externa (normalmente a Internet).

Personal firewall: um software que normalmente filtra o trafego que sai ou entra de um único computador.

\\Ligação Gratuita no TP

No primeiro artigo sobre phreaking para a revista **Hacker.BR**, abordaremos uma técnica para fazer ligações de telefones públicos sem pagar, com o auxílio de um telefone celular.

Para isto será necessário um celular, configurado para "fazer aqueles barulhos peculiares a cada tecla digitada". Também será preciso, e esta é a grande dificuldade da técnica, a chave do orelhão.

Apenas os técnicos responsáveis pela manutenção às possuem. E mesmo que você consiga esta chave com alguém que a tenha, as fechaduras se diferenciam de região para região. Sugestões:

- Realizar um ataque de engenharia social aos técnicos que fazem a manutenção dos orelhões.
- Realizar um ataque de engenharia social a algum chaveiro.
- Fazer um curso de chaveiro (no **www.cursodephreaker.com.br** tem um).

Particularmente acho que a segunda opção seria a mais conveniente. É bem provável que um chaveiro de esquina, quase falido, aceite o trabalho se bem remunerado. E se você ensinar a técnica, a chave pode sair de graça. Aliás, caso você tenha que pagar por ela, não se preocupe, recuperará o dinheiro investido em pouco tempo. Várias pessoas pagariam muito bem por uma cópia dela.

Já com a chave do orelhão e o celular em mãos, podemos realizar a ligação. Primeiro abra o orelhão e localize um botão, geralmente preto, pequeno e quadrado. Provavelmente será o único botão que encontrará. Em seguida, mantenha este botão pressionado, retirando o telefone do gancho. Mas atenção, só pare de pressionar o botão depois que tirar o telefone do gancho. Em seguida, posicione o "local do celular onde você ouve" na frente do "local do telefone onde você fala". A intenção é que os barulhos que o celular emitir sejam captados pelo receptor de voz do telefone do orelhão. Cada número possui um tom característico e padronizado. Assim, o orelhão fará a ligação reconhecendo os números através de seus tons característicos. Finalmente, digite em seu celular o número a ser chamado. Deve-se digitar os números pausadamente, porém de maneira contínua. Não demore muito entre um número e outro, mas também não pressione muito rápido. Não é necessária a utilização de qualquer número a mais. Por exemplo, se você quer fazer uma ligação local, disque apenas o número do telefone. Se quiser realizar uma ligação interurbana, dique zero, a operadora, o DDD, e o número do telefone. E assim sucessivamente. Se tudo der certo, pronto! Você estará realizando uma chamada gratuita para onde quiser.

Aqui cabem alguns comentários. Primeiramente, isto é crime, e a empresa telefônica responsável pelo orelhão logo notará que estão utilizando seu aparelho de forma ilegal. Ouvi testemunhos que utilizaram esse método algumas vezes no orelhão dos seus respectivos bairros e não demorou muito para aumentar o movimento de PMs (policiais militares) nos locais. Há notícias também de uma menina que foi pega pela PM, que suspeitou que ela estivesse utilizando o método. Os PMs então pediram para que ela demonstrasse a eles como ela fazia as tais ligações gratuitas. Ela ingenuamente demonstrou o método, dando-lhes a oportunidade de prendê-la em flagrante. Portanto, recomendo que não utilizem sempre o mesmo orelhão, que não façam ligações longas e se for pego, negue tudo.

Faço também algumas observações:

- A chave costuma abrir quase todos os orelhões de uma determinada região. E digo isto em nível de Estado. Aliás, quanto mais gasta tiver a sua chave, mais orelhões ela abrirá. Você pode gastá-la usando uma lixa.

- Nem sempre as ligações dão certo. Alguns erros podem acontecer, por isso não desista na primeira tentativa. Com o tempo, você erra cada vez menos.

- Alguns orelhões são difíceis de serem abertos. Mas talvez alguns tapas, murros ou mesmo um "jeito certo" resolvem o caso.

- Aproveite a oportunidade para compreender melhor o funcionamento dos orelhões, ou mesmo para criar novas técnicas phreakers.

Bom é isso. Caso tenham alguma dúvida, contatem-me.

Por Leozaum

\\Windows ou Linux?

Afinal, qual é o sistema operacional dos hackers?

Em quase toda discussão sobre hacker costuma surgir a dúvida: qual sistema operacional o hacker utiliza? Mas, será que existe mesmo um sistema operacional dos hackers? Pura besteira. Ser hacker é pensar e agir como hacker. Isto independe do sistema operacional, da máquina e da conexão. Capitão Crunch inaugurou a era phreaker com um apito de plástico. Mitnick conseguiu a maior parte das informações que precisava usando a lábia. No filme *Prenda-me se For Capaz*, com Tom Hanks e Leonardo DiCaprio, vemos um hacker legítimo em ação, numa época sem micros pessoais para serem invadidos.

É claro que o Linux foi pensado desde o início para funcionar em rede. O Windows não. Se eu tiver opção, vou preferir qualquer versão do Linux, a melhor versão do Windows, devido as ferramentas de rede que já vem integradas ao SO.

Mas e se eu tiver que fazer uma ação hacker a partir de um micro com o Windows, como ocorre nos cybercafés? Vou ter que voltar pra casa e falar pra mamãe que não deu? É este o ponto em que quero chegar. Independente das diferenças entre o Windows e o Linux, o hacker deve ser capaz de agir. Conhecer bem tanto um SO quanto o outro ajuda. E se alguém disser que hackers só tem Linux em casa e abominam o Windows, decida tudo em uma partida em rede de Commmand & Conquer.

\\Invasão de Natal

Aproveite a ausência dos funcionários

A época de feriados prolongados, como é o caso das festas de fim-de-ano, é uma excelente ocasião para tirar da gaveta aquele plano de ataque aguardando execução. É que nesta época os fucionários estão mais suscetíveis aos ataques de engenharia social, devido ao espirito de Natal. E tem também a ausência dos funcionários do CPD, deixando o servidor a mercê dos hackers.

Um defacement por exemplo, só deverá ser descoberto no próximo dia útil. E até lá pode ter se passado quase uma semana. Se levarmos em conta que os defacements costumam durar de algumas horas a poucos dias, uma semana é um prazo e tanto.

Um black hat pode ir mais longe e aproveitar o efeito consumista causado pelo Natal. Algumas possibilidades incluem:

- trojans dissimulados de cartões de Natal virtuais
- ofertas fantasmas em sites de leilão virtual
- phishing scam aproveitando as inúmeras ofertas e promoções feitas pelas grandes lojas no fim do ano
- iscas em mídia física, enviadas pelo correio, simulando brindes de fim de ano, amostras grátis e outras malas diretas pertinentes a ocasião

A lista de ações hacker possíveis com as festas de fim de ano não tem fim. Um pouco de imaginação, uma mente hacker e nenhum pudor em enganar as pessoas é suficiente para um black hat ter seu próprio Natal Sem Fome.

\\Hackers x Kiddies

Uma das principais diferenças entre **HACKERS** e **KIDDIES** é a existência ou não de um método de ataque. Para os que desejam se tornar profissionais de segurança, a metodologia é condição *sine qua non*. Enquanto um **KIDDIE** usa tudo o que tem (ferramentas) contra alvos aleatórios ou escolhidos no calor de alguma discussão, o **HACKER ESTUDA** o **ALVO** e só então **ELABORA** o **PLANO DE ATAQUE.**

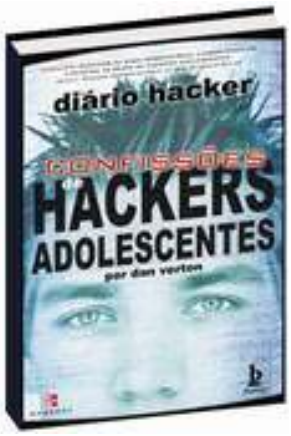
Na maioria das vezes o **KIDDIE** é mais rápido que um **HACKER** no **PROCESSO** de invasão. O problema de uma invasão assim, feita às pressas e sem **PLANEJAMENTO**, é a redução das chances de sucesso e o aumento das chances de ser rastreado.
É claro que há casos em que o **KIDDIE** vai levar mais tempo em uma invasão e talvez nem seja bem sucedido. Mas no geral o **KIDDIE** é mais rápido.

O índice de rastreabilidade de uma **AÇÃO** feita por **KIDDIE** é altíssimo. Fontes dentro da polícia especializada em crimes de informática, me confidenciaram que são tantos os **KIDDIES** fáceis de serem rastreados, que o maior trabalho destes policiais e decidir por quem enquadrar. Geralmente a decisão leva em conta **PEDOFILIA** e **ATAQUES AO SISTEMA FINANCEIRO**.

Antes de dar início a sua próxima invasão, faça as seguintes perguntas: Quem é o meu alvo? Qual é o objetivo desta ação hacker? Se você não tiver resposta a estas duas perguntas, é melhor desistir de ser hacker e feazer um curso de flores.

\\Seminários do Curso de Hacker

Os alunos do Curso de Hacker assíduos em nossa lista de discussão no Yahoo!, desde as últimas semanas de 2004 estão participando de seminários semanais, onde discutimos na teoria e na prática temas de interesse hacker. O seminário é uma forma excelente de aprofundar alguns assuntos, conhecer outros e até contribuir com informações úteis.
Todos os seminários estão sendo convertidos em vídeoaulas, e estas vídeoaulas estão sendo enviadas gratuitamente aos alunos VIP do Curso de Hacker.



Editora: *Berkeley* ***ISBN:*** *8572516263*

Ano: *2002* ***Páginas:*** *288*

O autor faz entrevistas com hackers adolescentes que continuam na ativa - invadindo sites e afins - e outros que 'aposentaram o mouse'. Entrevista também, agentes da FBI, oficiais de justiça e da lei, psicólogos, professores e pais de hackers, para explicar o que os motiva. Conta também, histórias da subcultura hacker. A tradução é muito ruim. Sugiro que você baixe a versão original em inglês para comparar os trechos em que o tradutor derrapou. **Onde achar?** FTP, eMule ou no CD Biblioteca Hacker #1.

Título: *Prenda-me Se For Capaz* ***Ano:*** *2003*

Baseado na história real de um dos maiores impostores dos Estados Unidos, "Catch Me If You Can" mostra toda a trajetória de Frank Abagnale Jr e como ele conseguiu juntar a fortuna de US$ 2,5 milhões falsificando cheques. Com um obstinado agente do FBI no seu encalço, ele terá que usar todos os seus artifícios para conseguir sair ileso. Este filme representa a arte da engenharia social.

Onde achar? Locadora mais próxima ou eMule.

Ano: *1998*
Genero: *Eletrônica (Euro House)*
Gravadora: *Paradoxx Music*

1.Intro
2.Amokk
3.Get up 2 da track (666 is back)
4.La vasca se mueve
5.Message (Backwards)
6.La tierra ya destruida
7.Alarma !
8.Paradoxx
9.Los ninos del demonio
10.Interlude
11.Diablo
12.El fuego
13.I'm your nitemare
14.666 Megamix
15.Message (Forwards)

Onde achar? FTP ou eMule. Busque também pelo DVD com o mesmo título.

Foi-se o tempo em que o hacker baixava o programa demo e depois crackeava. O melhor mesmo é baixar programas, eBooks, games e albúns full gratuitamente:

http://www.pootz.org
http://www.spanishare.com

\\O Que Você é Afinal?

O objetivo da seção filosofansas é fazer você pensar, em vez de só ter pensamentos, como ocorre com a maioria das pessoas. Vamos imaginar a seguinte situação. Você sofreu um acidente e acordou no hospital. O acidente foi grave e houve a necessidade de remover uma parte do seu corpo. O ano é 3010 e a tecnologia médica está bastante avançada. Para você ter uma idéia do avanço da medicina, a parte que removeram do seu corpo, foi o pecoço pra baixo. Sua cabeça é mantida viva em uma máquina e você consegue se comunicar normalmente com as pessoas a sua volta.

Este cenário já foi retratado no desenho Futurama (FOX) e não é tão hipotético, já que os casos de tetraplegia só deixam a cabeça funcionando, embora ainda ligada ao corpo. O ator Christopher Reeve por exemplo, mesmo com os movimento limitados quase a fala, antes de morrer escreveu um livro, criou uma fundação de pesquisas e atuou em um dos episódios de Smalville (SBT), além de ter feito palestras dentro e fora dos EUA.

Agora responda a seguinte pergunta: se você fosse reduzido a uma cabeça, você continuaria sendo você? Não vale dizer que seria apenas a cabeça. O que eu quero saber é em qual lugar do seu corpo você está. Na divisão do corpo com a cabeça, se os dois ficassem vivos, você estaria aonde? No corpo ou na cabeça?

Creio que sua resposta seja 'na cabeça'. Mas em que parte da cabeça? Se tirar a pele você continua sendo você? E se tirar os ossos? As orelhas? O nariz? A boca? Os dentes? No final só vai restar o cérebro. Se ele pudesse ser ligado a uma máquina para te devolver o sentido da visão, tato, olfato, audição e paladar e esta máquina ainda permitisse que você falasse, ainda seria você? O Stephen Hawking é um gênio da física e sua condição humana é quase isto que eu descrevi.

Está percebendo que você está no corpo, mas você nãoé o corpo? O cérebro já foi mapeado e os cientistas não encontraram nenhuma parte onde pudesse estar o SER.

E por falar no SER, o que somos afinal? Não quero a classificação científica nos reduzindo a seres de carbono. Por que um Stephen Halkings é aclamado mundialmente e outra pessoa em plena forma física nem tanto? O que nos torna diferentes diante das outras pessoas? É que SOMOS o que FAZEMOS. Se consideramos alguém médico, é porque este alguém exerce a medicina. Se consideramos alguém advogado, é porque este alguém exerce a advocacia. E para considerarmos alguém hacker, este alguém vai precisar nos mostrar que realiza ações hacker. E quanto mais difíceis ou divulgadas for estas ações hacker, mais hacker será considerado entre os hackers. Ou você acha mesmo que somos todos iguais?

\\Como Tudo Começou...

Se você gostaria de saber como eram as coisas a dez, vinte, trinta anos atrás, que tal deixar uma "velhinha" contar-lhe como as coisas eram ? Onde começar ? Dezessete anos atrás na Convenção Mundial de Ficção Científica em Boston ? Bem, naquela época, era a coisa mais próxima das convenções hackers de hoje.

1980. Ted Nelson e os caras do Xanadu: Roger Gregory, H. Keith Henson e K. Eric Drexler, pegando pesado para construir o Instituto Foresight. Eles sonham em criar o que hoje conhecemos como World Wide Web. Hoje, os hackers se vestem como vampiros nas convenções. Em 1980, eles usavam bonés de baseball pretos com asas prateadas e o slogan: "Xanadu: Wings of the Mind" (Xanadu, Asas da Mente). Na mesma convenção, encontramos uma turminha mais "underground" — drogando-se e fazendo uso das "blue boxes". A administração do hotel tem que interditar a piscina devido as orgias que estavam acontecendo ali.

Oh, mas isso dificilmente é o despertar dos hackers. Vamos voltar mais 17 anos atrás na mesma área de Boston, no início dos anos 60. Estudantes do MIT lutam pelo controle dos mainframes da escola. Eles usam programas em linguagem de máquina para deletar todos os programas e conseguir o controle da unidade central de processamento. Naquele tempo não existiam computadores pessoais.

Em **1965**, Ted Nelson, que viria a se tornar o líder do Xanadu na WorldCon de 1980, usa pela primeira vez a palavra "hipertexto" para descrever o que viria a se tornar a World Wide Web. Depois, ele espalha a idéia no seu livro "Literacy Online" (Literatura Online). A capa preta mostra um personagem tipo Super-Homem voando e o slogan "Você já pode e deve aprender a usar computadores".

Mas em 1965 o computador é temido por todos. Culpa de Orwell (George Orwell). Sim, no seu romance "1984", ele previa um futuro no qual a tecnologia acabaria com a liberdade humana. Poucos escutam Nelson. Poucos percebem a onda de anarquia da cultura hacker nascendo. Mas, a filha do guru do LSD Timothy Leary, Susan, começa a estudar programação.

Por volta de **1966**, Robert Morris, futuro cientista-chefe da NCSA, transformar aquela guerra de hackers no primeiro ambiente de "hacking seguro". Ele e dois amigos, criam um jogo chamado "Darwin". Depois, "Darwin" torna-se "Core War", um jogo de computador que até hoje é jogado por alguns hackers.

Vamos para **1968**. Sinta o aroma de gás lacrimogênio. Uau, olhe aquelas pedras quebrando as janelas do prédio de Ciências da Computação na Universidade de Illinois. Lá fora estão os protestos contra as guerras. Seu inimigo, eles acreditam, são os computadores da ARPA instalados no campus. Lá dentro estão os "nerds" cheios de cafeína e óxido nitroso. Dirigidos pelo jovem Roger Johnson, eles pegam quatro CDC 6400s e os ligam a terminais. Este fato torna-se a primeira realização do ciberespaço: Plato.

1969 torna-se o ano mais potencial para "hacking". Neste ano, a Agência de Pesquisa para Projetos Avançados (ARPA) do Departamento de Defesa, funda um segundo projeto para interligar quatro mainframes para que os pesquisadores possam compartilhar seus recursos. Este sistema não usa o terminal do sistema Plato. Seus terminais apenas mostram caracteres ASCII: letras e números. Chato, não ?

Mas esta ARPAnet é altamente "hackeável". Em um ano, seus usuários encontram um novo jeito de trocar

arquivos texto. Eles chamam esta invenção não-autorizada e não-planejada de “eMail”. ARPAnet desenvolve uma vida independente de seus criadores. É uma história que virá a se repetir mais tarde de vários modos. Ninguém consegue controlar o ciberespaço. Eles não conseguiram nem quando ele era apenas quatro computadores.

Ainda em 1969, John Goltz se associa a um empresário para fundar a Compuserve usando uma nova tecnologia de troca de pacotes que foi utilizada pela ARPAnet. Também em 1969, vemos um notável nascimento nos Laboratórios Bell (Bell Labs) — Ken Thompson cria um novo sistema operacional: Unix. Ele está para se tornar o padrão dourado do hacking e da Internet, o sistema operacional com o poder de fazer milagres.

Em **1971**, Abbie Hoffman e os Yippies fundam a primeira revista hacker/phreaker, YIPL/TAB (Youth International Party — Technical Assistance Program = Partido Jovem Internacional — Programa de Assistência Técnica). YIPL/TAP essencialmente inventa o phreaking — o esporte de brincar com os sistemas telefônicos de maneiras nunca pensadas pelos seus criadores. Eles são motivados pelo monopólio da compania telefônica Bell com suas taxas altissímas para ligações de longa distância, e um pesado imposto que Hoffman e muitos outros recusavam a pagar enquanto protestavam contra a Guerra do Vietnã. Que modo melhor de se pagar contas telefônicas do que não pagar conta nenhuma?

As “blue boxes” entram em cena. Seus osciladores automatizam o som que já possibilitaram pessoas como Captain Crunch (John Draper) a se tornarem piratas do megamonopólio da Bell. Repentinamente, os phreakers são capazes de conseguirem dinheiro com seus hobbies. Hans e Gribble vendem “blue boxes” no campus de Stanford.

Em junho de **1972**, a revista de extrema esquerda Ramparts, no artigo “Regulating the Phone Company In Your Home” (controlando a compania telefônica em sua casa) publica os esquemas para uma variante da “blue box” conhecida como “mute box”. Este artigo viola as leis do estado da Califórnia, que proibe a venda de “planos ou instruções para qualquer instrumento, aparato, ou dispositivo que possa ser usado para evitar cobranças de ligações telefônicas”. A polícia da Califórnia, ajudada por oficiais da Pacific Bell, apreendem cópias da revista das bancas. A pressão financeira causa sua falência.

Com a Guerra do Vietnã, o primeiro programa de simulação de voô da história entra na rede Plato. Gráficos, quase nunca vistos naquela época, são mostrados em terminais vetoriais sensíveis ao toque. Cyberpilotos de todos os lugares dos EUA tomam seus postos: Phatoms, MIGs, F-104s, X-15, Sopwith Camels. Pilotos virtuais decolam de aeroportos digitais e tentam derrubar uns aos outros e bombardear aeroportos. Enquanto pilotava um Phantom, vi uma mensagem na parte de baixo da tela — “Estou para te derrubar.”. É um MIG na minha cola. Mergulho e faço um loop para ver tentar ver meu algoz. A tela fica preta. Meu terminal mostra a mensagem ‘Você atingiu 37 Gs. Você mais parece uma pizza do que um ser humano”. Um dia a Enterprise aparece no nosso simulador, atira em todos e some no ciberespaço. Plato foi hackeado! Mesmo num jogo multiusuário de 1973, os jogadores tem que se preocupar em não serem “smurfados” ! (quando um hacker invade um jogo multiusuário na Internet e mata os outros jogadores como técnicas que não fazem parte do jogo — isso chama-se “smurfing”).

1975. Oh, ano abençoado! Sob um contrato com Força Aerea, na cidade de Albuquerque, Novo México, nasce o Altair. Altair - o primeiro microcomputador. Bill Gates escreve o sistema operacional. Sua mãe o persuade a mudar-se para Redmond, CA, onde ela conhece alguns empresários que gostariam de ver o sistema operacional. Lembra-se de Hans e Gribble? Eles afiliam-se ao clube “Home Brew Computer” e

escolhem processadores Motorola para fabricar o seu próprio computador. Começam a vender seus computadores, que batizaram de Apple, usando seus verdadeiros nomes - Steve Wozniak e Steve Jobs. Nasce uma nova "religião". Inicia-se a grande batalha Apple x Microsoft. Hackers norte-americanos surgem com "boxes" para terminais Tektronix.

Em **1978**, Ward Christenson e Randy Suess criam o primeiro BBS pessoal. Logo, ligados por nada além da rede telefônica de longa distância e por estas BBSs, os hackers criam um novo e privado ciberespaço. O "phreaking" torna-se mais importante do que nunca para conectar BBSs distantes. Também em 1978, as redes The Source e Compuserve começaram a buscar usuários domésticos. "Naked Lady" rodava "exuberante" na Compuserve. O primeiro cibercafé, Planet Earth (Planeta Terra), abre em Washington. As redes X.25 imperam.

Em **1980**, acontece então uma grande mutação na ARPAnet. Num salto gigantesco, ela muda do protocolo NCP (Network Control Protocol) para o TCP/IP (Transmission Control Protocol/Internet Protocol). Agora, a ARPAnet não é mais limitada a 256 computadores — pode ter mais de dez milhões de servidores! Assim, a Internet é concebida no ventre da ARPAnet do DoD. O esboço do que um dia uniria hackers do mundo todo, estava crescendo silenciosamente. Plato perece, para sempre, limitado aos seus 1024 terminais.

O famoso escritor de ficção científica Jerry Pournelle descobre a ARPAnet. Logo seus fãs estão loucos para entrar na ARPAnet. Os administradores da ARPAnet surpreendentemente não colocam empencílios para liberar contas, especialmente para pessoas no mundo acadêmico.

A ARPAnet é muito difícil de usar. Mas ao contrário de Plato, ela é realmente "hackeável" e agora tem o que precisa para crescer. Ao contrário das redes de BBS hacker, as pessoas não precisam gastar fortunas em ligações de longa distâncias para fazerem suas conexões. Tudo é local e gratuito.

No mesmo ano, 1980, o grupo "414 Gang" é perseguido. Fazer phreaking é mais arriscado do que nunca.

Os hackers dos anos 80 adoravam pegar peças. Joe College senta-se em frente do seu terminal DEC 10 da universidade e decide vasculhar na rede do campus. Lá está o Star Trek! Lá está o Adventure! Zork! Hummm, o que é este programa chamado Sex? Ele executa o programa. Uma mensagem aparece: "Atenção: brincar com sexo é arriscado. Tem certeza que quer jogar ? S/N". Quem pode resistir? Com "S", a tela se enche de caracteres ASCII e então aparece a mensagem: "Deletando todos os arquivos na sua conta.". Joe está chorando e xingando, descontrolado. Ele digita o comando para listar os seus arquivos. Nada ! Desesperado, ele corre até o administrador do sistema. Eles conectam-se novamente na sua conta mas os arquivos ainda estão lá. Tudo não passou de uma brincadeira.

Em **1983**, os hackers são quase todos inofensivos, pessoas que mantém-se afastadas daqueles que infrigem a lei. O "jargão" do MIT define um "hacker" simplesmente como "uma pessoa que gosta de aprender sobre sistemas de computador e como ampliar suas capacidades; uma pessoa que programa com entusiasmo e gosta de dedicar grande parte do seu tempo com computadores".

Em **1983**, o computador pessoal da IBM (IBM Personal Computer) entra no mercado impulsionado pelo sistema operacional de Bill Gates — o MS-DOS. Termina o império do sistema operacional. Nos próximos dois anos, praticamente todos os sistemas operacionais para microcomputadores estarão mortos, exceto o MS-DOS e os oferecidos pela Apple. Parte da fortuna do Vale do Silício vai para o esgoto. Morre

o Amiga. Os preços despencam e logo, todos os hackers tem seus próprios computadores.

Em **1994**, Emmanuel Goldstein lança a "2600: The Hacker Quarterly" e é formado o grupo hacker "Legion of Doom" (LoD). O Congresso aprova a Lei "Comprehensive Crime Control Act" dando poderes judiciários ao Serviço Secreto sobre fraudes com computadores. Fred Cohen, da Universidade Carnegie, Melon escreve sua tese de doutorado sobre um assunto totalmente novo chamado vírus de computador.

1984. Era para ser o ano, pensaram milhões de fãs de Orwell, em que o governo finalmente iria colocar suas mãos na mais alta tecnologia para se tornar o "Grande Irmão" (Big Brother). Ao invés disso, o escritor de ficção científica Willian Gibson, escrevendo o livro "Neuromancer" numa máquina de datilografar, cria o termo "ciberespaço".

Em 1984, surge a primeira BBS da polícia dos EUA. Desde 1985, Phrack tem fornecido informações sobre sistemas operacionais, tecnologias de rede e telefonia a comunidade hacker.

Os anos 80 foi a era do wardialers. Com exceção da ARPAnet e das redes X.25, a maioria dos computadores podia ser acessada apenas se descobertas suas linhas. Assim, um dos maiores tesouros para um hacker dos anos 80 era um número de telefone de algum computador misterioso.

Os computadores desta época rodavam dúzias de sistemas operacionais e usavam vários protocolos de comunicação. Os manuais destes sistemas muitas vezes eram secretos. A cena hacker trabalhava de acordo com o princípio de Mentor. A não ser que você encontrasse alguém que introduzisse no meio de um grupo hacker, que acumulava documentos pegos em depósitos de lixo ou mesmo roubados durante arrombamentos, você estaria muito longe de tudo. Kevin Poulsen fez seu nome através de vários arrombamentos na Pacific Bell.

Mesmo como estas barreiras, em 88 o hacking entra numa grande fase. De acordo com uma lista de grupos hacker compilada pelos editores da Phrack em 8 de agosto de 1998, os EUA tem centenas destes grupos.

O Serviço Secreto apreende fitas de vídeos da convenção SummerCon de 1988. Em 1988, Robert Tappan Morris, filho do cientista Robert Morris, escreve um exploit que será sempre lembrado como "Morris Worm". Ele usa uma combinação de Finger e Sendmail para invadir computadores, instalar-se e então enviar várias cópias para outros computadores. Morris, com pouca compreensão do poder desta replicação exponencial, lança-o na Internet. Logo, computadores vulneráveis são entupidos de cópias deste worm assim como os links de comunicação que estão ,enviando as cópias deste worm para outros computadores. A jovem Internet, que então tinha apenas alguns milhares de computadores, entra em colapso. Morris é preso, mas é solto logo depois.

1990 é o ano pivô para a Internet, tão importante como os anos 80 e a invenção do TCP/IP. Inspirado em Xanadu, Tim Berners-Lee, do Laboratório Europeu de Física Quântica (CERN), concebe uma nova maneira de implementar o hipertexto. Ele a batiza de World Wide Web. Em 1991, silenciosamente, ele a lança para o mundo. O ciberespaço nunca mais será o mesmo. Xanadu, Plato, assim como o CP/M, perecem.

1990 é também um ano de um grande número de perseguições a hackers e prisões. O Serviço Secreto Americano e a Polícia de Nova Iorque procuram por Phiber Optik, Acid Phreak e Scorpion em Nova

Iorque. Eles prendem Terminus, Prophet, Leftist e Urvile.

A Força Tarefa de Chicago prende Knight Lightning e procura Robert Izenberg, Mentor e Erik Bloodaxe. Procura Richard Andrew em seu trabalho e sua casa. O Serviço Secreto conduz buscas da "Operação Sundevil" em Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose e San Francisco. Uma famosa busca "sem-motivo" feita pela Força Tarefa de Chicago que ocorreu naquele ano foi a invasão da Steve Jackson Games.

Em junho de 1990 Mitch Kapor e John Perry Barlow reagem aos excessos de toda essa perseguição e fundam a Eletronic Frontier Foundation (EFF). Seus objetivos iniciais é proteger os hackers. Eles conseguem ajuda legal para a comunidade hacker.

Em **1993**, Marc Andreesson e Eric Bina do Centro Nacional de Aplicações para Supercomputadores (NCSA) lançam o Mosaic, o primeiro browser WWW gráfico. Finalmente, depois do fracasso do Plato vinte antes atrás, tinhamos gráficos decentes! Desta vez entretanto, os gráficos vieram para ficar. Logo, os browsers tornaram-se o caminho número um para os hackers pesquisarem e espalharem seus exploits. As BBSes, com seus segredos fortemente guardados, desaparecem da cena.

Em **1993**, a primeira DefCon (www.defcon.org) invade Las Vegas. A era da Conferências Hacker cresce com as conferências Beyond Hope, HoHocon e outras.

Em **1996**, Aleph One cria a lista de discussão Bugtraq e a torna a primeira lista pública sobre segurança de computadores "sem censura". Pela primeira vez na história, falhas de segurança que podem ser usadas para invadir computadores estão sendo discutidas abertamente e com códigos completos para "exploit". Os arquivos da Bugtraq são colocados na Web.

Em agosto de 1996 iniciei a lista Guides to (mostly) Harmless Hacking. Ela contém instruções bastante simples para ajudar os novatos a entender o que é hacking. Um grande número de hackers me procuram para ajudar no que se tornaria a Happy Hacker Digest.

1996 é também o ano em que a documentação sobre roteadores, sistemas operacionais, protocolo TCP/IP e muitos outros começam a proliferar na Web. A era dos ousados "ladrões" de manuais técnicos termina.

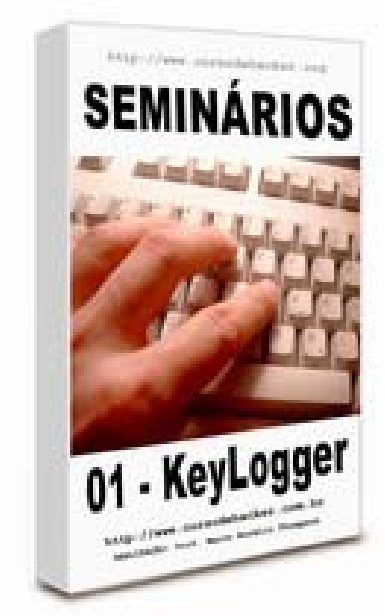
Nos idos de 1997, os leitores da Bugtraq começam a dissecar o Windows NT. Uma nova lista, NT Bugtraq, é lançada apenas para tratar o grande volume de falhas de segurança do NT que é discutida pelos leitores. Os auto-proclamados hackers Mudge e Weld do grupo L0pht, escrevem e lançam um "password cracker" para o WinNT que agita a Internet. Muitos dos que lidam com segurança devem agradecer o que Mudge e Weld estão fazendo pelo Windows NT.

Agradeço a boa vontade dos hackers que compartilharam seus conhecimentos na Web, e as listas como BugTraq, NT BugTraq e Happy Hacker. Devido a estas atitudes, os dias em que as pessoas tinham que implorar para entrar num grupo hacker para aprender os segredos da arte, finalmente estão acabando.

Qual será o próximo acontecimento do mundo hacker ? Você tem a resposta em suas mãos.

Por Carolyn P. Meinel

\\Keylogger (Dia 1)



Os alunos do Curso de Hacker participam semanalmente de seminários temáticos. Acompanhe dois dias do seminário sobre Keyloggers:

SEMINÁRIO VIRTUAL DO CURSO DE HACKER

MODERADOR: Prof. Marco Aurélio Thompson

KEYLOGGER: O Que é?

O keylogger é um programa do tipo 'espião' ou 'monitor'. Não se trata de um programa hacker ou que seja proibido. O uso inicial do keylogger (chamado de monitor) era para que pais monitorassem o uso do computador dos filhos. Também é um programa útil para usuários e empregadores que queiram saber o que as pessoas fizeram em sua ausência. No Curso de Hacker, algumas esposas anseiam por pegar algum furo do marido e vice-e-versa.

Apesar do monitor não ser inicialmente um programa hacker, bastou o primeiro kiddie botar as mãos nele para que passasse a fazer parte da lista de ferramentas do iniciante.

Keyloggers são essencialmente programas usados por Script Kiddies. Isto pela natureza e finalidade do programa. Um hacker, na verdadeira concepção da palavra, dedica seus estudos e ações em direção a micros servidores. Mas isto não quer dizer que um hacker não possa usar um keylogger como parte de um PLANO DE ATAQUE. Meu comentário diz respeito apenas a natureza deste programa. Não é um programa típico de ação hacker propriamente dita. Não se imagina um hacker invadindo micros de usuários, a não ser que isto o leve ao objetivo maior, que é o servidor.

Existem programas monitores com recursos variados. No decorrer deste seminário vamos conhecer alguns deles e você poderá optar pelo que lhe for mais conveniente.

O funcionamento básico de um keylogger é este: capturar toda a digitação e gravar em um arquivo de texto com extensão .txt ou .log.

A um keylogger podem-se acrescentar funções como:

- gravar os mais diversos tipos de atividade no micro, como abertura de janelas, execução de programas e coordenadas de movimentação do mouse.

- enviar o relatório da monitoria por e-Mail, para um FTP ou serviço de mensagem instantânea, sendo o mais comum o ICQ.

- capturar a imagem ao redor do mouse ao clicar. Um monitor deste tipo pode ser usado para burlar a segurança dos tecladinhos virtuais usados pelos bancos.

- se instalar a partir de outro programa, tornando o keylogger também um trojan (cavalo de tróia).

Pela lista de recursos acima, você pode perceber que existem keyloggers com funcinalidades e disponibilidade de recursos diferenciados.

KEYLOGGER: Como Usar?

O uso do keylogger mais simples é este:

- INSTALAR

- ANALISAR OS RELATÓRIOS DE TEMPOS EM TEMPOS

Já para um keylogger com mais recursos:

- INSTALAR (local)

- CONFIGURAR

- RECEBER E ANALISAR OS RELATÓRIOS DE TEMPOS EM TEMPOS

Para um keylogger instalado remotamente (keylogger com trojan):

- CONFIGURAR O SERVIDOR

- ENVIAR O SERVIDOR

- AGUARDAR QUE O USUÁRIO INSTALE O SERVIDOR

- RECEBER E ANALISAR OS RELATÓRIOS DE TEMPOS EM TEMPOS

Neste último exemplo as chances de êxito são bem menores. Poucas pessoas tem aberto anexos de e-Mail ultimamente. E se for um keylogger dos mais populares, provavelmente já consta na lista de programas maliciosos dos principais antivírus do mercado.

Este último tipo será analisado, bem como as formas de seduzir o usuário e enganar o antivírus, no seminário virtual que falarmos sobre trojans.

PRÁTICA

No link abaixo você poderá baixar e instalar seu primeiro keylogger. Neste primeiro dia não entrarei em detalhes sobre o uso deste primeiro keylogger. Amanhã, no segundo dia do seminário, responderei a todas as dúvidas que surgir neste primeiro contato e lhes apresentarei outro keylogger.

Até o fim deste seminário, após de ter experimentado vários keyloggers, você poderá decidir pelo que lhe for mais conveniente.

O link é este:

http://www.nilopolis.com.br/KeyLogger01.zip

Instale sem medo. Nada será danificado em seu micro e os seus dados não serão enviados pela Internet. Este primeiro keylogger é um dos mais simples. Ótimo para iniciar.

Eu fico por aqui. Amanhã a gente se fala. Ficou com alguma dúvida? É só enviar um e-Mail aqui mesmo para o grupo do Curso de Hacker. Não responderemos e-Mails enviados para outros endereços. E não esqueça de citar seu número de matrícula. Tenha um bom dia.

(a) Prof. Marco Aurélio Thompson

\\Keylogger (Dia 2)

SEMINÁRIO VIRTUAL DO CURSO DE HACKER

MODERADOR: Prof. Marco Aurélio Thompson

Este é o segundo dia do seminário sobre keyloggers. A esta altura já devemos saber no mínimo O QUE FAZ UM KEYLOGGER. Se ainda houver dúvida sobre isto, é melhor você tirar sua dúvida antes de prosseguir.

Nosso primeiro keylogger foi o mais simples possível. Pequeno. Sem grandes problemas com antivírus e firewall. Excelente para usar nas situações em que temos contato físico com a máquina, como por exemplo um cybercafé, curso, colégio, faculdade, escritório.

Ás vezes, existe dificuldade de configurar ou manter funcionando um keylogger com envio por e-Mail ou ICQ. Então é possível instalar um servidor FTP na máquina alvo (o antivírus não acusa e o firewall pode ser configurado, partindo do princípio que existe o acesso físico a máquina alvo). Com o FTP instalado, o keylogger é configurado para armazenar os logs (arquivos de texto com as informações capturadas ou imagens) na pasta do FTP. De outro micro, acessamos o FTP e lá estará o resultado do trabalho do keylogger.

É importante se acostumar com keyloggers simples, principalmente quem não conhece nenhum, para que possamos chegar a configurações mais avançadas, nos keyloggers que ainda aqui serão apresentados.

ANALISANDO O PRIMEIRO KEYLOGGER: HOME KEY LOGGER v1.70 FREEWARE

1. INSTALAÇÃO: A instalação é muito simples. O instalador é um arquivo único e o seu tamanho é ideal para ser transportado e instalado com rapidez.

2. CONFIGURAÇÃO: Após a instalação o programa executa e fica na bandeja do sistema, próximo ao relógio do Windows, na barra de tarefas. Clicando com o botão direito do mouse temos as opções:

- **View Log:** para visualizar o que já foi capturado no arquivo LOG

- **Autorun:** o keylogger incia junto com o Windows

- **Hide icon:** o ícone desaparece na bandeja. Para voltar a aparecer, tecle ao mesmo tempo CTRL+ALT+SHIFT+M

- **Clear log:** o arquivo de LOG é zerado para desocupar espaço

- **FAQ, About, etc...:** links para o Help, 'sobre' o programa perguntas comuns, etc...

- **Exit:** sai do programa

3. DETECÇÃO:

Não houve relatos sobre detecção deste programa por firewall (nem haveria o porque, já que este keylogger não se conecta com máquinas externas) e antivírus. Pode ocorrer de um anti spyware detectar este trojan, mas como é um programa que será instalado pelo hacker na máquina do usuário, é possível alterar a configuração do programa de proteção para ele não acusar o perigo.

Nada que preocupe já que este keylogger é instalado pelo próprio hacker na máquina do usuário.

Acessando a LISTA DE TAREFAS com a combinação de teclas CTRL+ALT+DEL, podemos visualizar na aba PROCESSOS, o keylogger, com o nome keylogger.exe. Usando um nome do sistema, o Windows não vai permitir o encerramento do processo. Poucos usuários tem por hábito analisar o que está sendo executado em sua máquina. E até administradores de rede constumam relaxar de vez em quando. E é aí que a coisa entra. Quando o administrador relaxa.

Basta alterar o nome do executável, de keylogger.exe para um outro nome, como por exemplo explorer.exe e será este o nome que vai aparecer na lista de tarefas do Windows. Agora vai ser preciso muita perspicácia, quase beirando a paranóia, para detectar este keylogger.

4. CONCLUSÃO

Se o hacker tiver acesso a máquina alvo regularmente, este keylogger será extremamente valioso. Simples. Pequeno. Ocultável. Gratuito. Se a idéia é um keylogger de preguiçoso :), daqueles que se manda por e-Mail e fica em casa aguardando os dados chegarem, então temos que seguir adiante e conhecer outros keyloggers.

O QUE SE ESPERA DE UM KEYLOGGER?

O keylogger ideal não existe. Está para ser feito e pode ser feito por você, com muito de estudo e dedicação. O keylogger ideal não é só keylogger, ele é um misto de servidor smtp, trojan, keylogger e screen logger (ou grabber). O problema de um keylogger deste tipo é ele fazer tanto sucesso que passaria a ser incluído na lista de programas perniciosos dos principais fabricantes de antivírus.

Enquanto o keylogger ideal não existe, voltemos a realidade e nos consideraremos momentâneamente satisfeitos com um keylogger que:

- possa ser instalador no computador local

- envie os dados coletados para nosso e-Mail ou ICQ

Tendo um keylogger com as características acima, e é este o nosso objetivo neste segundo dia, já será possível executar ações hacker respeitáveis.

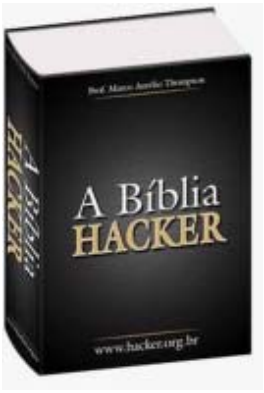
Após dominar o keylogger com as características acima, passemos para um keylogger que possa ser instalado a distância. Este tipo é um dos mais difíceis de obter sucesso, uma vez que pouca gente tem se arriscado a instalar programa desconhecido em suas máquinas. E a monitoria tem que ser constante. Quem garante que a vítima vai estar com o PC ligado ao mesmo tempo que você? Quem garante que o firewall não vai alertá-la do trojan? Não estamos lá pra ver. As chances de sucesso são mínimas quando o alvo é definido. Quando o alvo é indefinido (envio do trojan/keylogger em massa) ou quando combinamos o uso deste keylogger com outras técnicas, como phishing scam e engenharia social, as chances de sucesso aumentam.

Por fim, temos os keyloggers que capturam telas ou cliques do mouse. Neste caso, podemos usar até um programa de captura de tela, como o Snagit, que tem a opção de envio por e-Mail das telas capturadas (inclusive área em volta do mouse) a cada tantos segundos. Como nem tudo é perfeito, este programa não é instalado a distância.

Vamos ver até onde chegamos no seminário, usando soluções de terceiros. A partir daí, pegue a sua insatisfação e enfia-se num quarto para programar o melhor keylogger que o mundo já viu: o feito por você.

(a) Prof. Marco Aurélio Thompson

\\Aos ‘Cítricos’



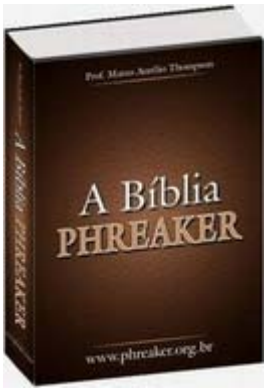
Este é o número zero da revista Hacker Brasil ou **HACKER.BR** para os íntimos. Esta revista é mantida pelo Curso de Hacker e a distribuição é gratuita, por download. Não existe uma versão impressa e não temos esta pretenção.

É comum em trabalhos deste tipo, surgir comentários variados. Desde elogios exagerados a críticas ferrenhas. Já sou vacinado contra isto e os leitores equilibrados podem ficar tranquilos que a revista não vai parar de ser editada por nada. Imaginem vocês que estou aqui concluindo o número zero e imaginando como estaremos por ocasião do lançamento do número cem, daqui a mais ou menos dois anos.

Se mantivermos a média de vinte páginas por edição, na edição de número cem totalizaremos duas mil páginas de opiniões brasileiras e contemporâneas sobre os temas ligados a segurança da informação. Mas como estou apostando que outros colaboradores virão, espero chegar a quarenta páginas por edição até o terceiro número da revista. Isto totalizará cerca de quatro mil páginas de material selecionadíssimo, feito por brasileiros, para brasileiros.

Eu não tenho bola de cristal, mas é certo encontrarmos pelo caminho os cítricos. É aquele pessoal que não faz ainda e se mete no que os outros fazem. Não estou falando dos críticos. Estes ajudam de alguma forma. Falo dos cítricos. Vocês acreditam que depois de escrever um livro que foi proibido pelas editoras (**O Livro Proibido do Curso de Hacker - ISBN 85-98941-01-8**), escrever uma **Bíblia Hacker** com 1.200 páginas e uma **Bíblia Phreaker** com 800 páginas, criar o primeiro **Curso de Phreaker** do mundo (**www.cursodephreaker.com.br**), ainda tem gente que acha que eu não entendo nada sobre o assunto? Estes são os cítricos. Medem os outros pelas suas medidas. Se não podem, ninguém mais pode.

Na lista CISSPBR por exemplo, as críticas ao meu trabalho eram do tipo; ‘ele é velho’, ‘ele é feio’, ‘ele é gordo’, ‘ele é bicha’. Peraí. Não sou nada disso e se fosse não influenciaria a minha criatividade. Cadê as críticas as técnicas? Ao conteúdo? Por que não apontam meus erros de português pelo menos? Não tenho revisor, não sou jornalista e meu português é do Ensino Médio. Deve ter erro aos montes para ser apontado. Cadê as críticas as idéias? Por que não apontam argumentos fracos, técnicas falhas, contradições? Sabem qual é a resposta? Ou não tem o que ser apontado ou não tiveram competência para tal. Façam suas apostas.



Um recurso muito comum usado pelo crítico de fim de semana é dizer que meu trabalho é copiado da Internet. Dá vontade de rir. Procurem por AVATAR, PLANO DE ATAQUE, ALVO, AÇÃO HACKER e constatarão que são termos cunhados por mim para facilitar o aprendizado no Curso de Hacker. E que já estão sendo copiados e adotados até por professores universitários.

Nós, através do Curso de Hacker e outros projetos relacionados, como os seminários virtuais e mais recentemente esta revista digital, estamos organizando as atividades hacker no Brasil. Todo este pessoal de TI junto não fez metade do que estamos fazendo. O Infomerda, que se acha o tal, se limita a divulgar problemas, em vez de discutir e propor soluções. O Machadinho é outro que segue pelo mesmo caminho. Estamos aqui para apressar as coisas. O hacker brasileiro, com fama de defacer, estelionatário e scammer, vai amadurecer e se tornar um profissional dos mais requisitadas pelas empresas ligadas a TI. Vem aí o Hacker Ético. Quem viver verá.

http://ww.cursodehacker.com.br

http://www.cursodephreaker.com.br