howstuffworks
comotudofunciona

Como funciona a cabeça de um hacker

por Daniel Koch

Introdução

Há mesmo genialidade nas invasões a computadores e servidores ou podemos classificá-las como mera atitude de estelionatários? Com a popularização da Internet, muito se tem ouvido falar sobre os hackers e seus feitos: invasões a sites e corporações, desvio de dinheiro pela Internet, roubo de dados confidenciais, destruição de bancos de dados.

O que não se sabe, e o que a mídia convencional não explica, é como funciona a cabeça de um indivíduo classificado como "hacker". **Seriam nerds delinquentes revoltados com o mundo? Gênios da computação que não sabem o que fazer com seu conhecimento?**

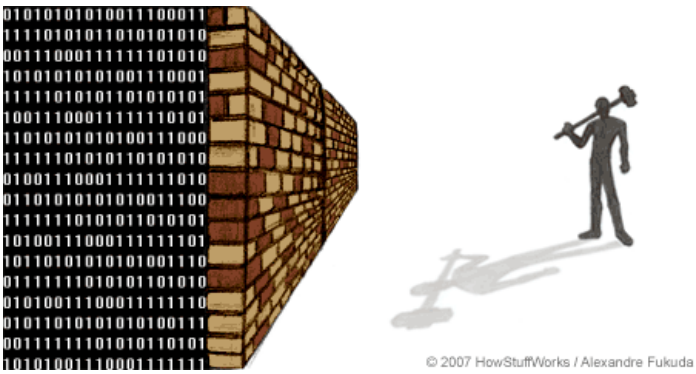
Krzysztof Zmij/iStockphoto

Neste artigo, vamos abordar o comportamento dos diversos tipos de hacker, desde os responsáveis por alertar sobre vulnerabilidades em uma grande companhia, até aqueles que utilizam a vulnerabilidade para obter fama e popularidade.

Não só isso. Mostraremos **como nascem os hackers**, o que cada tipo de hacker faz e o que os motiva.

Tipos de hackers e suas características

O termo hacker surgiu em meados dos anos 60 e originou-se da palavra ***phreak*** (acrônimo de phone hacker), que eram os hackers que estudavam o sistema de telefonia e com isso conseguiam fazer ligações de graça. Naquela época os sistemas de informática (assim como os de telefonia) eram restritos a poucos: apenas tinham acesso a eles os envolvidos com computação nos grandes CPDs (Centros de Processamento de Dados) de universidades e empresas.



Movidos pela curiosidade de saber como tudo aquilo funcionava, alguns grupos de estudantes quebravam os cadeados dos CPDs usando um machado. Hack significa cortar, golpear em inglês, daí o termo ter sido adotado para designar aqueles que quebram a segurança para aprender sobre algo que pessoas comuns não têm acesso.

De posse da informação desejada, cada um resolveu fazer o que bem entendia com isso, e hoje podemos classifica-los como:

White Hats (hackers éticos): Seguem a mesma linha de pensamento original do hacking. Gostam apenas de saber e conhecer mais das coisas, principalmente as fechadas ao público. Para essas pessoas, aprender é a diversão mais importante do mundo. Elas gastam boa parte de seu tempo estudando o funcionamento do que as cerca, como telefonia, internet e protocolos de rede e programação de computadores.

No mundo da segurança de sofware, os hackers éticos são os responsáveis por "informar" as grandes empresas de vulnerabilidades existentes em seus produtos. Fora do mundo da segurança, essas pessoas são responsáveis por desenvolver software livre, como o sistema operacional GNU/Linux.

O hacker ético defende o conhecimento em prol de todos, portanto não o utiliza para prejudicar outras pessoas ou companhias, a menos que considere que uma empresa faz mau uso do poder. A quebra da segurança do iPhone, que bloqueia o seu funcionamento com outras operadoras de telefonia, foi um notável ato de um White Hat.

Black Hats (hackers mal-intencionados): Assim como os White Hats, os Black Hats também são movidos pela curiosidade. O que os distingue é o que cada um faz com a informação e o conhecimento.

O Black Hat vê poder na informação e no que ele sabe fazer. São aqueles hackers que descobrem uma vulnerabilidade em um produto comercial ou livre e não contam para ninguém até que eles próprios criem meios de obter dados sigilosos de outras pessoas e empresas explorando a vulnerabilidade recém-descoberta.

Essa espécie de hacker é responsável por gerar a terceira espécie, os *script kiddies*. Eles surgem quando cai na rede uma ferramenta ou técnica de invasão criado por um grupo de Black Hats.

Script Kiddies: São os responsáveis pelas invasões em massa e por fazer barulho na mídia quando invadem sites importantes e alteram sua página inicial colocando frases de protesto ou quando tiram serviços do ar.

Recebem esse nome por não saber o que estão fazendo. Eles simplesmente buscam ferramentas prontas, os chamados *exploits*, que exploram uma determinada vulnerabilidade, e então buscam servidores e serviços vulneráveis. Não sabem como o exploit funciona, já que ele que foi denvolvido por um Black Hat, que provavelmente estudou o assunto.

Grande parte dos Black Hats já atuou como Script Kid no início de sua jornada no mundo do hacking.

Crackers: São de outra natureza. Ao contrário dos hackers convencionais, que estudam protocolos de rede, telefonia e sistemas operacionais, e dos kiddies, que buscam obter fama por causar transtornos a websites e serviços, os crackers se distinguem de todo o resto por se focarem em como funcionam os programas de computador.

São os responsáveis pela criação dos cracks, ferramentas que quebram a ativação de um software comercial, permitindo que qualquer pessoa tenha uma versão pirata do software em seu computador.

Esses hackers são responsáveis pelo prejuízo das empresas de software, e também por desenvolver vírus e outras pragas como *spywares* e *trojans*. O termo cracker também é usado incorretamente para designar os Black Hats, o que é ofensivo tanto para o Black Hat como para o Cracker.

Na próxima página saiba o que motiva um hacker.

O que motiva o hacker

Os hackers são motivados por diversos fatores. O conhecimento e a informação em coisas fechadas ao público é o principal deles. Mas é o que cada um pode fazer com isso que motiva os diferentes tipos de hackers.

Um hacker nasce quando ele descobre algo que ninguém ou poucas pessoas sabem e com isso consegue obter vantagens, sejam elas popularidade e respeito das outras pessoas, sejam elas poder e dinheiro.

Os White Hats são motivados pelo conhecimento e pela liberdade de informação e pelo quanto isso pode ser útil para:

- outros hackers iniciantes,
- grupos de projetos de software livre,
- empresas de softwares e serviços comerciais e
- as pessoas comuns.

Para esses hackers, ter a liberdade de saber como as coisas funcionam é o principal motivo de fazer o que fazem. Uma frase muito comum no mundo hacker define a conduta geral de um White Hat: *"Hack to learn, not learn to hack"* (em tradução livre, "Invadir para aprender, e não aprender para invadir").

Os Black Hats, por sua vez, são motivados pelo subproduto do conhecimento e da informação que adquirem estudando sobre o funcionamento das coisas. Conhecer bem os protocolos de rede que rodeiam a Internet significa que podem tirar serviços importantes do ar apenas brincando com as falhas que descobrem.

E isso tudo tem um preço, que pode ser pago com popularidade e respeito por tirar um serviço grande do ar, ou até o valor financeiro incluído na informação confidencial a que somente eles tiveram acesso. Se os black hats tiverem acesso aos dados de compra e venda de um site de e-commerce, por exemplo, eles podem obter dados pessoais e números de cartão de crédito dos clientes. Ou então chantagear os donos da empresa se, durante a invasão, descobrir algo irregular. As possibilidades de se fazer dinheiro com esse tipo de informação são inúmeras.

Para esses hackers, a conquista pela informação secreta significa poder, e poder é o seu principal motivador. **Hackers assim são chamados de elite, ou l33t ou 1337**, por esconder do público as técnicas e as vulnerabilidades que descobrem.

Já **os Script Kiddies são motivados unicamente pela fama**. Para esse grupo de hacker pouco importa como as coisas funcionam ou qual é a informação confidencial que existe nas máquinas que invadem. Para os kiddies, saber como as coisas funcionam faz parte do processo de invadir, e a invasão é feita para a conquista da popularidade.

Crackers são motivados pelo jogo que existe entre os desenvolvedores de software comercial e eles próprios. Eles se empenham em entender como um software é rodado pelo sistema operacional e pelo computador, e com isso conseguem burlar muitos softwares que só rodam por 30 dias e que exigem um número de série para habilitar as demais funcionalidades.

Para os crackers, **a motivação é conquistada no conhecimento das técnicas, na popularidade e no respeito que conseguem** quando criam um crack ou *keygen* (acrônimo de key generator, programa que gera chaves de números de série).

Mas como eles atacam. Saiba na próxima página

Como os hackers atacam

Será que apenas os script kiddies têm culpa por invadir os sistemas e causar transtornos com usuários de computador? Qual é a parcela de culpa que cada um têm quando algum incidente ocorre?

White Hats descobrem a vulnerabilidade, informam aos responsáveis e liberam a informação para o público.

Os **White Hats, ou hackers éticos,** não são diretamente responsáveis pelos incidentes que acontecem. Esses hackers **passam a maior parte do tempo estudando e aprendendo** sobre protocolos de redes, sistemas operacionais, telefonia e tudo o que for possível e impossível saber, desenvolvendo assim suas técnicas de invasão.

Quando descobrem alguma vulnerabilidade em algum projeto de código aberto, além de avisarem o time de desenvolvimento do projeto, costumam contribuir com patches, os remendos que garantem a segurança do software.

Invadem sistemas apenas para provar que existe uma vulnerabilidade e que ela é real, ou então para testar suas técnicas e impressionar as pessoas, deixando os dados do alvo intactos. Quando causam danos diretos, fazem isso como forma de protesto contra alguma companhia que esteja fazendo coisas anti-éticas, claro que dentro do conceito do que é ético para o hacker.

Os White hats costumam escrever tutoriais, explicando suas técnicas e expondo para o mundo o que conhecem e aprenderam. Esses tutoriais são publicados em e-zines, que são revistas eletrônicas distribuídas na internet e em BBS, normalmente em formato de texto puro.

Black Hats descobrem a vulnerabilidade, invadem sistemas importantes, roubam informações e só então informam aos responsáveis, liberando a informação para o público.

Os Black Hats se apoderam das vulnerabilidades que descobrem e as utilizam para conseguir informações secretas, acessando computadores de empresas e pessoas específicas.

É raro um ataque de Black Hat aparecer na mídia comum. São muito discretos, costumam entrar e sair dos sistemas sem fazer barulho e sem deixar rastros. Quando uma técnica cai na rede, junto com exploits e outras ferramentas, é porque os Black Hats já tiraram dela tudo o que conseguiram e ela já não serve mais para eles.

Normalmente eles próprios publicam a vulnerabilidade e suas ferramentas, assim o respeito e a popularidade do grupo também cresce. Mas esse não é o foco dos Black Hats.

Script Kiddies se informam das vulnerabilidades, buscam ferramentas e então invadem os sistemas, ficando desta forma conhecidos pelos

Os **kiddies atuam como hienas esperando os leões** terminarem a refeição para comerem o resto. Ficam esperando os Black Hats ou até os White Hats disponibilizarem técnicas ou ferramentas para invadir os sistemas.
Quando conseguem, invadem a maior parte de sites e serviços

forma conhecidos pelos ataques em massa.

que conseguirem, sem saber o que estão fazendo. Se consideram hackers e impõem medo na maioria dos administradores de redes e gerentes de TI incompetentes.

Também são culpados por tirar sites e serviços do ar utilizando técnicas de negação de serviço (DoS, Denial of Service), com o auxílio de ferramentas desenvolvidas por Black Hats. Não costumam se preocupar em apagar pegadas, por isso são frequentemente capturados pelas autoridades.

Crackers estudam a arquitetura interna do computador, criam cracks e keygens para quebrar a ativação de um programa comercial.

Já **os crackers se empenham em estudar como os programas funcionam no computador**. Estudam linguagens de programação de baixo nível como Assembly e passam boa parte do tempo monitorando programas de computador, para entender como ele funciona.

Quando não desenvolvem vírus, trojans ou spywares, criam algoritmos que geram seriais para softwares comerciais como Adobe Photoshop, Microsoft Windows, Winzip e etc. Esses algoritmos são chamados keygens. Muitas vezes criam programas que alteram o comportamento de outro programa, desativando a função que pede por uma chave de ativação. Com isso conseguem burlar o sistema antipirataria dos softwares comerciais. Essas ferramentas são os famosos cracks.

Na próxima página você vai saber quais são os três pilares em que se apóiam os hackers.

A ciência do hacking

Remus Eserblom/iStockphoto

Pela complexidade, o que todos os hackers fazem é parte de uma ciência ou de uma arte que pode ser aprendida e dissecada para o seu melhor entendimento.

O hacking, assim como o phreaking, consiste em entender o funcionamento dos sistemas de informação como um todo e então tirar vantagem dele. As habilidades básicas se apóiam em **quatro pilares**:

1- Sistemas operacionais

Windows, Mac OS X, Unix e GNU/Linux são alguns exemplos. Cada sistema operacional trabalha com o computador de uma forma e pode ou não expor a sua complexidade para o usuário.

O conhecimento sobre sistemas operacionais é o primeiro pilar do hacking.
Sistemas operacionais mais seguros como Linux e Unix são a primeira escola fundamental para um hacker começar o seu aprendizado. Aqui ele aprende sobre permissões de acesso, senhas, protocolos de rede e programação Esses sistemas operacionais são os preferidos pelos hackers e pelos iniciantes.

Sistemas operacionais para usuários finais, como o Windows e o Mac OS , são escolhidos para o estudo quando o hacker pretende atacar usuários comuns.

2 - Programação de computadores

Não é verdade que todos os programadores são hackers. A grande maioria não é. Kevin Mitnick, que ficou famoso na década de 90 ao atacar os sistemas de telefonia dos EUA e os servidos de um funcionário da Agência de Segurança Nacional daquele país, já havia dito: “Ótimos programadores são péssimos hackers”. Quando um hacker estuda programação, ele vai além.

Movido pela curiosidade, um hacker busca saber como o programa funciona no computador, como um sistema operacional trata um programa de computador e como os administradores, humanos, sabem da existência do programa. É aqui também que surgem os crackers e criadores de vírus.

Saber programar é muito útil para qualquer hacker. É com isso que eles desenvolvem ferramentas e exploits que podem automatizar seus ataques e permitir acesso posterior à máquina invadida, com o uso de backdoors.

3- Sistemas de Comunicação: Redes de Computadores, Internet e Telefonia

O terceiro pilar do hacking são os protocolos de comunicação. Na época do phreaking, antes da internet, os sistemas de telefonia eram o alvo de estudo. Atualmente os protocolos de internet e rede de computadores são os mais estudados.

Saber como um computador se comunica com o outro é essencial para tirar proveito de comunicações secretas ou até se aproveitar de falhas e então tirar serviços importantes do ar.

4- Relações humanas: engenharia social

Quando os sistemas são praticamente fechados e seguros, a exemplo dos sistemas bancários, a falha mais passível de ser explorada é a humana.

As pessoas que lidam com o sistema sabem muito sobre ele, e o hacker se passando por outra pessoa pode conseguir informações confidenciais para entrar no sistema.

Essa técnica de se passar por outra pessoa para conseguir informações é chamada de engenharia

social.

A engenharia social ficou muito famosa com hackers como Kevin Mitnick, que invadiu sistemas fechados se passando por funcionário das empresas, conseguindo com isso informações sobre o funcionamento dos sistemas que invadiu.

Nos tempos atuais, a engenharia social não é muito utilizada pelos hackers, uma vez que a maioria passa seu tempo nos computadores e com isso não tem muitos contatos sociais, falhando nas relações pessoais mais simples.

Nas próximas páginas você vai conhecer um pouco dos hackers que fizeram história e como é o jargão usado por eles.

Hackers que fizeram história

Kevin Mitnick (Condor)
O mais famoso dos hackers chegou a roubar 20 mil números de cartões crédito e passeava pelo sistema telefônico dos EUA com total desenvoltura. Foi o primeiro hacker a entrar para a lista dos dez criminosos mais procurados pelo FBI. Depois de quatro anos de prisão. Mitnick está agora em liberdade e tem uma empresa que presta consultoria em segurança de sistemas.

Tsutomu Shimomura
Tsutomu Shimomura é um cientista da computação e hacker notório. Teve grande influencia na captura de Kevin Mitnick, um dos maiores crackers de todos os tempos. Escreveu o livro "Contra-ataque", em que conta como ajudou a prender Mitnick.

Kevin Poulsen (Watchman)
Kevin Poulsen, o Watchman, amigo de Mitnick, era um simples especialista em telefonia de rara habilidade. Em 1990, ganhou um Porsche num concurso realizado por uma emissora de rádio da Califórnia. O prêmio era para o 102º ouvinte que telefonasse. Poulsen invadiu a central telefônica, interceptou as ligações e garantiu seu prêmio. Passou quatro anos na prisão e hoje é diretor do site Security Focus.

John Draper (Captain Crunch)
John Draper, o Captain Crunch, é considerado o inventor do phreaking. No início dos anos 80, ele usava um simples apito de plástico para produzir o tom de 2.600 Hz, capaz de enganar o sistema telefônico americano. Assim, fazia ligações de graça.

Johan Helsingius (Julf)
O filandês é responsável por um dos mais famosos servidores de e-mail anônimo. Foi preso após se recusar a fornecer dados de um acesso que publicou documentos secretos da Church of Scientology na Internet. Tinha para isso um 486 com HD de 200Mb, e nunca precisou usar seu próprio servidor.

Vladimir Levin (Rússia)
O russo Vladimir Levin é o ladrão digital mais notório da história. Ele liderou uma gangue russa que invadiu os computadores do Citibank e desviou US$ 10 milhões de contas de clientes. Levin foi preso na Inglaterra, quando tentava fugir do país. Ele dizia que um dos advogados alocados para defendê-lo era, na verdade, um agente do FBI.

Ehud Tenebaum (Analyser)
O israelense Ehud Tenebaum, o Analyser, foi preso em 1998, após ter participado de um bem-organizado ataque contra os computadores do Pentágono. Seus companheiros de conspiração eram dois jovens de Israel e mais dois da Califórnia.

Mike Calce (Mafiaboy)
Aos 15 anos, o canadense Mike Calce, o Mafiaboy, confessou ter orquestrado os ataques de indisponibilidade de serviço que derrubaram sites como Yahoo!, CNN e ZD Net em fevereiro de 2001. Ele foi sentenciado a 8 meses de prisão, por ter acarretado um prejuízo estimado em US$ 1,2 milhão. Ele é um exemplo de script kid. Alardeou tanto os seus feitos, que acabou sendo preso por isso.

O glossário do hacker

Dentro da comunidade hacker, a definição do termo hacker varia de socialmente muito positiva (indivíduos talentosos) a criminosa. De acordo com "*The New Hacker's Dictionary*", que traz as gírias, os jargões, o folclore, o estilo de falar e escrever, o modo de vestir, o tipo de educação e as características de personalidade dos hackers, o termo pode ser definido como:

1. Uma pessoa que gosta de explorar os detalhes de sistemas programáveis e esticar suas capacidades, em oposição à maioria dos usuários, que preferem aprender apenas o mínimo necessário.
2. Alguém que programa entusiasticamente (até de forma obsessiva) ou que gosta de programar em vez de apenas teorizar sobre programação.
3. Uma pessoa capaz de apreciar o valor do hacking. Uma pessoa que programa bem e rápido.
4. Um especialista em um programa específico, ou que trabalha com ou sobre esse programa.
5. Um especialista ou entusiasta de qualquer tipo. Ele pode ser um hacker em astronomia, por exemplo
6. Aquele que gosta do desafio intelectual de superar ou contornar limitações.
7. [desuso] Um intrometido malicioso que tenta descobrir informações sensíveis fuçando. Daí os termos "hacker de senha" e "hacker de rede". O correto termo para isto seria cracker.

Mas qualquer que seja a definição correta para hackers, o mundo da segurança de sistemas tem seu próprio jargão. Veja os mais comuns:

Os termos mais usados no mundo hacker e em segurança de sistemas

1337/l33t	Forma de escrever o alfabeto latino usando outros símbolos em lugar das letras, como números por exemplo. A própria palavra leet admite muitas variações, como l33t ou 1337. O uso do leet reflete uma subcultura relacionada ao mundo dos jogos de computador e internet, sendo muito usada para confundir os iniciantes e para firmar-se como parte de um grupo.
Assembly	Linguagem de programação básica equivalente à linguagem de máquina.
Backdoor	Ou Porta dos fundos, é um trecho de código mal-intencionado que cria uma ou mais falhas de segurança para dar acesso ao sistema operacional a pessoas não-autorizadas
BBS	Bulletin Board System, ou Sistema de Quadro de Avisos. Sistema no qual um ou mais computadores recebem chamadas de usuários e depois de uma checagem permitem que eles retirem ou depositem arquivos.
Black hat	Pessoa que usa seus conhecimentos com computadores e outras tecnologias de maneira maliciosa ou criminosa
CPD	Sigla para Centro de Processamento de Dados, o local onde são concentrados os computadores e sistemas (software) responsáveis pelo processamento de dados de uma empresa ou organização.
Cracker	É o termo usado para designar quem quebra um sistema de segurança, de forma ilegal ou sem ética.
Crack	(software) É a modificação de um software para remover métodos de proteção como prevenção de cópia e número de serial.
Debug	É um programa, ou componente de um programa, que auxilia o programador a encontrar erros de programação em seu código ou em programas desenvolvidos por terceiros
DoS	Denial-of-service ou Ataque de negação de serviço. Tentativa de tornar os recursos de um sistema indisponíveis para seus usuários. Alvos típicos são servidores web. Não se trata de uma invasão de sistema e sim da sua invalidação por sobrecarga.
Engenharia social	Método utilizado para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas
Exploit	Programa de computador com uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional ou de serviços.
E-zine	Electronic magazine, revista eletrônica distribuída na Internet
Keygen	Significa gerador de chaves, key generator em inglês. Um pequeno programa de computador que gera uma chave do CD ou um número da série/registro de um software ou algoritmo de criptografia.
Patch	Conserto de um programa que acrescenta ou modifica somente uma parte pequena de um software
Phreak	Acrônimo de Phone Hacker. É o hacker da telefonia
Script kid	Nome atribuído aos grupos de hackers inexperientes (geralmente das faixas etárias mais baixas) que desenvolvem atividades relacionadas com segurança da informação utilizando-se do trabalho intelectual dos verdadeiros especialistas técnicos. Esses hackers, não possuem conhecimento de programação, e não estão interessados em tecnologia, mas em ganhar fama ou outros tipos de lucros pessoais.
Sistemas operacionais	Programa (software) ou um conjunto de programas cuja função é servir de interface entre um computador e o usuário. É comum utilizar-se a abreviatura SO (em português) ou OS (do inglês "Operating System").

Software livre	Qualquer programa de computador que pode ser usado, copiado, estudado, modificado e redistribuído com algumas restrições.
Spyware	Tecnologia projetada para, secretamente, coletar informações sobre o usuário
Técnicas de invasão	Fórmula de obter acesso não-autorizado em servidores que explora vulnerabilidades e falhas de sistemas.
Trojan	Trojan ou Cavalo de Tróia é um programa que age como a lenda do cavalo de Tróia: ele vem escondido dentro de outro arquivo, entrando no computador, e liberando uma porta para um possível invasor
Vírus	Programa de computador destinado a causar danos
White hat	Hacker ético. Pessoa que é eticamente oposta ao abuso de sistemas de computadores

Para saber mais sobre o mundo hacker, consulte os links da próxima página.

Mais informações

Artigos relacionados

- Como os computadores-zumbis funcionam
- Os hackers poderiam acabar com a economia americana?
- Como funcionam os vírus de telefones celulares
- Como funciona o spyware

Sites interessantes

- Phrack.org (Inglês) - Phrack é uma ezine underground feita por hackers desde 17 de Novembro de 1985. Os artigos são relacionados a segurança, hacking, phreaking, anarquismo, criptografia, espionagem, programação, conspiração e outras notícias do mundo.
- Barata Elétrica - Barata elétrica é um fanzine eletrônico criado e editado por Derneval R. da Cunha em 1995, abordando temas como vida alternativa, hackers, phreaking e softwares.
- Como se tornar um Hacker (em inglês)
- Como se tornar um Hacker (em português) - Guia de Eric S. Raymond, notável hacker do software livre. Aborda tudo o que uma pessoa precisa saber para ser um hacker White Hat.
- Unsekurity Scene - Antigo grupo de hackers brasileiros que ganhou fama entre 2000 a 2002, por escrever e documentar suas técnicas e popularizar o hacking ético no Brasil. O site saiu do ar em 2003, porém seus textos ainda podem ser encontrados na internet no link acima.
- Guia do Iniciante, por Meleu (Português) - Meleu foi um dos hackers brasileiros envolvidos no extinto grupo Unsekurity Scene, seus textos ainda são acessíveis em seu site pessoal. Com o Guia do Inciante pode-se conhecer as habilidades básicas necessárias para se tornar um hacker. O texto foi publicado em 2002.
- Packet Storm (em inglês) - Site especializado na divulgação de exploits e papers sobre vulnerabilidades.
- Security Focus - Site especializado na divulgação de boletins de segurança e mantenedora da famosa lista de discussões Bugtraq, lista onde é trocada informações sobre as vulnerabilidades nos sistemas atuais.

Livros interessantes

- ***A Arte de Enganar***, Kevin D. Mitnick e William L. Simon, 2006, Makron Books, 284 páginas
- ***Diário Hacker: Confissões de Hackers Adolescentes***, Dan Verton, 2002, Berkeley Brasil, 288 páginas
- ***Hackers Expostos: Quarta Edição***, George Kurtz, 2003, Campus-BB, 832 páginas

Filmes relacionados

- ***Caçada Virtual*** (Takedown, EUA, 2000), de Joe Chapelle, com Amanda Peet, Skeet Urlich, Nicole Arnold, Tom Berenger e Cara Buono