O MUNDO HACKER

AULA 01

Por Luiz Alvarenga

Sumário

O HACKER

Introdução

Então, quem são os hackers? O termo está sendo usado corretamente?

Se você não é o tipo de pessoa que se sente assim naturalmente, precisará se tornar um para se tornar um hacker. Caso contrário, você descobrirá que sua energia de hackers é minada por distrações como sexo, dinheiro e aprovação social.

(Você também deve desenvolver um tipo de fé em sua própria capacidade de aprendizado - uma crença de que, embora você não saiba tudo o que precisa para resolver um problema, se você resolver apenas um pedaço dele e aprender com isso, você ' aprenderei o suficiente para resolver a próxima peça - e assim por diante, até que você termine.)

A definição de hacker pode variar dependendo de quem você pergunta, mas na maioria dos casos envolvendo cobertura da mídia, eles estão realmente falando de "crackers".

Então agora precisamos perguntar: os termos "hacker" e "cracker" são diferentes? E se sim, quais são as metodologias que os separam?

Para realmente entender suas semelhanças e diferenças, primeiro precisamos aprender o que são hackers e crackers.

O que é um hacker?

Se nos voltarmos para a definição formal no Glossário de Usuários da Internet, sob a RFC 1392 , um hacker é uma pessoa que se deleita em ter uma compreensão íntima do funcionamento interno de um sistema, computadores e redes de computadores em particular.

O termo é frequentemente mal utilizado em um contexto pejorativo, onde 'cracker' seria o termo correto.

Cérebros criativos são um recurso valioso e limitado. Eles não devem ser desperdiçados em reinventar a roda quando há tantos problemas fascinantes esperando por lá.

Os hackers são naturalmente anti-autoritários. Qualquer pessoa que possa lhe dar ordens pode impedi-lo de resolver qualquer problema pelo qual você esteja fascinado - e, dada a maneira como as mentes autoritárias funcionam, geralmente encontrará algumas razões terrivelmente estúpidas para fazê-lo. Portanto, a atitude autoritária deve ser combatida onde quer que você a encontre, para não sufocar você e outros hackers.

A atitude do hacker é vital, mas as habilidades são ainda mais vitais. Atitude não substitui competência, e há um certo conjunto básico de habilidades que você precisa ter antes que qualquer hacker sonhe em chamá-lo de um.

Em termos mais simples, um hacker é alguém que usa suas habilidades e conhecimentos para encontrar vulnerabilidades em sistemas de computador e ajuda a melhorar e corrigir essas vulnerabilidades. Para se comportar como um hacker, você precisa acreditar que o tempo de reflexão de outros hackers é precioso - tanto que é quase um dever moral compartilhar informações, resolver problemas e distribuir as soluções apenas para que outros hackers possam resolver *novos* problemas. problemas em vez de ter que reiterar perpetuamente os antigos.

O conhecimento que os Hackers possuem sobre programação, várias linguagens de computador, código e segurança geral do computador é avançado e usado para fins moralmente bons. Eles são normalmente profissionais de segurança que podem ser contratados pelas organizações para tentar invadir seus sistemas, auditar o DNS e suas redes, para que possam identificar quaisquer falhas que possam ter. Eles costumam ser empregados como parte da equipe vermelha e da equipe azul.

Quando os hackers encontram uma vulnerabilidade ou ameaça, eles documentam o processo e notificam a organização que os contratou, ou o fornecedor do software que construiu o sistema, para que a vulnerabilidade possa ser corrigida antes de ser explorada por atores mal-intencionados.

Muitas vezes vemos o termo chapéu branco (White Hat) , ou hacker ético, vinculado a esses mocinhos que usam suas habilidades para fins de defesa.

Motivação do hacker

Hackers são aqueles que constroem e criam. Eles aprendem e descobrem diferentes sistemas, redes de computadores e geralmente têm experiência anterior em programação, o que apenas aumenta seu amplo conhecimento. Eles constroem ambientes seguros.

O ditado " conheça seu atacante " nunca é mais verdadeiro do que quando se fala de hackers e de seu trabalho; eles usam as mesmas ferramentas, software e até técnicas que os crackers. Os hackers sabem o que os invasores procuram quando planejam um ataque, para que possam se proteger proativamente contra eles. Eles constroem software e ferramentas que podem até ser os mesmos que os crackers usam, mas usam-nos para melhorar a segurança, não para quebrá-la.

A abordagem adotada pelos hackers também é semelhante à usada pelos crackers; eles entram em sistemas e redes para encontrar brechas na segurança, mas a motivação por trás de suas ações é puramente não maliciosa e ética. Eles trabalham com permissão da empresa que possui o sistema que estão tentando quebrar e que é sempre informado sobre os resultados finais. Por causa dos hackers, as vulnerabilidades podem ser corrigidas e as ameaças evitadas. As práticas dos hackers não envolvem nada ilegal e não danificam os dados com os quais eles entram em contato; eles utilizam suas habilidades para um benefício positivo.

O que é um cracker?

Vamos agora pular para a definição formal de cracker: “Um cracker é um indivíduo que tenta acessar sistemas de computador sem autorização. Esses indivíduos geralmente são maliciosos, em oposição aos hackers, e têm muitos meios à sua disposição para invadir um sistema. ”

Os crackers também são chamados de "chapéus pretos". Eles procuram backdoors em programas e sistemas, exploram esses backdoors e roubam informações privadas para uso malicioso.

Enquanto os hackers trabalham para ajudar organizações e indivíduos a proteger seus sistemas e redes, os crackers têm um objetivo diferente em mente. Quando quebram a segurança de uma rede, o fazem ilegalmente sem a permissão do proprietário e o fazem para ganho pessoal. As habilidades e conhecimentos que eles possuem são usados expressamente para violar a segurança com intenção maliciosa. Seu objetivo pode ser roubar informações de cartão de crédito, obter dados privados que podem ser aproveitados para atividades ilegais, obter dados privados e vendê-los ou simplesmente destruir os dados.

Os crackers são os culpados que se envolvem em crimes cibernéticos; eles lançam campanhas de phishing nos funcionários da empresa e criam dispositivos que variam de roteadores e laptops a impressoras e aparelhos de fax para entrar na rede de uma organização. Frequentemente atacam as empresas quando estão mais vulneráveis, como durante fusões e aquisições, ou atacam os fornecedores da cadeia de suprimentos de uma organização, pois costumam ser o elo mais fraco.

Todos os vetores de ataque para crackers têm o mesmo resultado final: obter dados ilegalmente. Os dados podem ser comprometidos, mas nem sempre - pois os crackers podem ter motivações diferentes por trás de suas atividades ilegais.

O que motiva os biscoitos?

Os hackers criam, os crackers quebram e destroem. Os crackers geralmente são motivados por ganhos financeiros: estamos bastante familiarizados com ataques de ransomware, nos quais um cracker invade um sistema através de emails de phishing e anexos maliciosos, depois bloqueia o acesso a um computador ou dados e ameaça a vítima por expor seus dados privados, resgate não é pago. Alguns crackers também roubam informações de cartão de crédito ou qualquer outra informação privada que possam usar para acessar as contas bancárias das vítimas e roubar dinheiro delas.

É claro que existem outras motivações que levam os crackers a se envolverem em atividades ilegais. Há casos em que os crackers violaram uma rede apenas para se exibir e ganhar publicidade. Com grande parte da mídia cobrindo violações, não é surpresa que muitos desejem usar isso para se tornarem "famosos", especialmente porque alguns tipos de crimes cibernéticos não exigem um alto nível de habilidade. Também podemos encontrar crackers que desejam quebrar o software por engenharia reversa, para explorar suas fraquezas. E também há quem faça isso apenas por diversão.

Enquanto os hackers trabalham para ajudar organizações e indivíduos a proteger seus sistemas e redes, os crackers têm um objetivo diferente em mente.

Sim, existem crackers por aí que quebram um sistema apenas para mostrar suas habilidades, sem uma única intenção de adulterar ou prejudicar dados.

Diferenças entre hackers e crackers

Até agora, muitas diferenças entre hackers e crackers podem parecer óbvias, mas vamos revisar suas principais diferenças:

Diferença ética Hacker vs Cracker

Hackers são os mocinhos, chapéus brancos que invadem redes para descobrir brechas e restaurar a segurança de redes corrompidas para criar um sistema seguro. Eles nunca fazem isso ilegalmente e sempre informam sua organização contratada ou indivíduo sobre suas ações. Eles são uma ótima arma na caça e captura de biscoitos. Crackers, no entanto, entrarão no mesmo sistema para ganhos pessoais, financeiros ou qualquer outro tipo de ganho sem o conhecimento ou permissão dos proprietários do sistema, com o objetivo de se envolver em atividades ilegais.

Diferença de habilidade

Os hackers possuem a capacidade de criar programas e ferramentas de software; eles são hábeis em vários códigos e idiomas e têm conhecimento avançado de vários idiomas selecionados. Os crackers, por outro lado, não precisam possuir um profundo poço de conhecimento, exceto aquele sobre como realmente quebrar um sistema, e normalmente não os vemos com habilidade suficiente para criar seus próprios programas. Mesmo com tão poucos crackers qualificados o suficiente para criar ferramentas e software para ajudá-los a explorar as fraquezas que descobrem, nunca devemos ignorar sua ameaça.

Crackers Black Hat

Nada é preto e cinza na TI quando se trata de hackers e crackers. É aí que os chapéus cinzas entram em jogo.

A maneira mais fácil de descrever os chapéus cinza é que eles são indivíduos que agem ilegalmente com o objetivo de melhorar a segurança do sistema ou rede em que invadiram. Eles não terão a permissão da organização ou do fornecedor de software antes de procurar vulnerabilidades e podem até se reportar para solicitar renumeração, sua taxa pela descoberta de uma vulnerabilidade. Eles costumam explorar uma vulnerabilidade descoberta com o objetivo de aumentar a conscientização.

Mesmo com a mídia pintando todos os hackers como inerentemente ruins e anexando conotações negativas a eles, precisamos lembrar que nem tudo é como a mídia vê e que nem todos os hackers e crackers são iguais. O mundo seria um lugar muito mais assustador com muito mais crimes cibernéticos se os hackers não estivessem descobrindo ativamente vulnerabilidades e parando as ameaças que os crackers representam. E se não tivéssemos chapéus cinza, teríamos que dizer que o mundo é completamente apresentado em preto e branco, o que sabemos que não é verdade.

O que precisa para ser um Hacker?

O passo mais importante que qualquer iniciante pode dar para adquirir habilidades hackers é obter uma cópia do Linux ou um dos BSD-Unixes, instale-o em uma máquina pessoal e execute-o.

Sim, existem outros sistemas operacionais no mundo além do Unix. Mas eles são distribuídos em binário - você não pode ler o código e não pode modificá-lo. Tentar aprender a hackear em uma máquina Microsoft Windows ou em qualquer outro sistema de código fechado é como tentar aprender a dançar enquanto usava um corpo.

No Mac OS X, é possível, mas apenas parte do sistema é de código aberto - é provável que você atinja muitas paredes e tenha cuidado para não desenvolver o mau hábito de depender do código de propriedade da Apple. Se você se concentrar no Unix sob o capô, poderá aprender algumas coisas úteis.

Unix é o sistema operacional da Internet. Embora você possa aprender a usar a Internet sem conhecer o Unix, não pode ser um hacker da Internet sem entender o Unix. Por esse motivo, hoje a cultura hacker é fortemente centrada no Unix. (Isso nem sempre foi verdade, e alguns hackers antigos ainda não estão satisfeitos com isso, mas a simbiose entre o Unix e a Internet se tornou forte o suficiente para que nem o músculo da Microsoft pareça capaz de prejudicá-lo seriamente).

Então, abra um Unix - eu gosto do Linux, mas existem outras maneiras (e sim, você *pode* executar o Linux e o Microsoft Windows na mesma máquina). Aprenda. Executá-lo. Mexa com isso. Fale com a Internet com ele. Leia o código. Modifique o código. Você obterá melhores ferramentas de programação (incluindo C, LISP, Python e Perl) do que qualquer sistema operacional da Microsoft pode sonhar em hospedar, você se divertirá e absorverá mais conhecimento do que imagina estar aprendendo até você olha para trás como um hacker mestre.

Aprenda a programar.

Essa, é claro, é a habilidade fundamental de hackers. Se você não conhece nenhuma linguagem de computador, recomendo começar com Python. É bem desenhado, bem documentado e relativamente gentil para iniciantes. Apesar de ser uma boa primeira língua, não é apenas um brinquedo: ele é muito poderoso;

Se você entrar em programação séria, precisará aprender C, a linguagem principal do Unix. C ++ está intimamente relacionado a C; se você conhece um, aprender o outro não será difícil. Entretanto, nenhum dos idiomas é bom para tentar aprender como o primeiro. E, na verdade, quanto mais você evitar a programação em C, mais produtivo será.

C é muito eficiente e poupa muito os recursos da sua máquina. Infelizmente, C obtém essa eficiência exigindo que você faça muito gerenciamento de baixo nível de recursos (como memória) manualmente.
Para ser um hacker de verdade, você precisa chegar ao ponto em que pode aprender um novo idioma em dias, relacionando o que está no manual com o que você já conhece. Isso significa que você deve aprender vários idiomas muito diferentes.
Encontrar um bom código para leitura costumava ser difícil, porque havia poucos programas grandes disponíveis na fonte para os hackers novatos lerem e mexerem. Isso mudou drasticamente; software de código aberto, ferramentas de programação e sistemas operacionais (todos criados por hackers) estão agora amplamente disponíveis.

A Web é a única grande exceção, o enorme brinquedo hacker brilhante que até os *políticos* admitem ter mudado o mundo. Por esse motivo, sozinho (e muitos outros bons), você precisa aprender a trabalhar na Web.

Debug open-source software

Eles também servem quem suporta e depura software de código aberto. Nesse mundo imperfeito, inevitavelmente passaremos a maior parte do tempo de desenvolvimento de software na fase de depuração. É por isso que qualquer autor de código aberto que esteja pensando lhe dirá que bons testadores beta (que sabem descrever claramente os sintomas, localizam bem os problemas, podem tolerar bugs em uma versão rápida e estão dispostos a aplicar algumas rotinas simples de diagnóstico) vale o seu peso em rubis. Mesmo um deles pode fazer a diferença entre uma fase de depuração que é um pesadelo prolongado e exaustivo e uma que é apenas um incômodo salutar.

Se você é iniciante, tente encontrar um programa em desenvolvimento no qual esteja interessado e seja um bom testador beta. Há uma progressão natural: ajudar os programas de teste, ajudar a depurá-los e ajudar a modificá-los. Você aprenderá muito dessa maneira e gerará um bom karma com pessoas que o ajudarão mais tarde.

Publique informações úteis

Outra coisa boa é coletar e filtrar informações úteis e interessantes em páginas da web ou documentos como listas de perguntas frequentes (FAQ) e disponibilizá-las em geral.

Os mantenedores das principais perguntas frequentes técnicas têm quase tanto respeito quanto os autores de código aberto.

A cultura hacker (e o desenvolvimento de engenharia da Internet, nesse caso) é administrada por voluntários. Há muito trabalho necessário, mas sem glamour, para continuar - administrando listas de discussão, moderando grupos de notícias, mantendo grandes sites de arquivos de software, desenvolvendo RFCs e outros padrões técnicos.

As pessoas que fazem esse tipo de coisa são muito respeitadas, porque todo mundo sabe que esses trabalhos são imensos e não tão divertidos quanto brincar com código. Fazê-los mostra dedicação.

Mercado de Trabalho Hacker

Havia **313.735** vagas para especialistas em segurança cibernética até agosto de 2018. Esse número continuará a crescer, como veremos um pouco mais adiante. As estatísticas de segurança cibernética garantem que este será um dos empregos com melhor pagamento no futuro próximo.

Você está aprendendo coisas? Bom, essas estatísticas são impressionantes. Todos esses números parecem impressionantes, não é? Há mais por vir, mas vamos fazer uma pausa por um segundo para ver o mundo através dos olhos dos hackers.

Por exemplo - se você vir uma nova tecnologia, a primeira pergunta lógica que você poderá fazer é - "O que ela faz?"

Hackers vê-lo de forma diferente, embora - a sua pergunta é “O que eu posso **fazer** ele faz?”

Essas estatísticas sobre hackers podem não nos ajudar a entender como um hacker pensa, mas podemos tirar algumas conclusões definitivas sobre sua natureza.

Primeiro, deixe-me explicar a diferença entre um **hacker de chapéu preto** , um **hacker de chapéu branco** e **um hacker de chapéu cinza** .

Os hackers de chapéu preto são hackers com intenção criminosa.

Os hackers de chapéu branco são contratados para testar a segurança de um sistema. Eles têm permissão para fazê-lo.

Os hackers de chapéu cinza não têm motivos criminais, mas depois que começam a explorar um sistema, podem violar algumas leis.

Estatísticas Hackers

- Há um **ataque de** hackers a **cada 39 segundos** .
- Os hackers russos são os mais rápidos.
- **300.000 novos malwares** são criados todos os dias.
- **A autenticação e criptografia multifatoriais** são os maiores obstáculos dos hackers.
- Você pode **se tornar um cidadão americano por US $ 6.000** .
- O custo médio das violações de dados será de **cerca de 150 milhões em 2020.**
- O orçamento de segurança cibernética nos EUA é de US **$ 14,98 bilhões** .

Existem quase 314 mil vagas de emprego para especialistas em segurança cibernética somente nos EUA a partir de outubro de 2018. A Cybersecurity Ventures espera que o cibercrime mais do que triplique o número de vagas de emprego nos próximos cinco anos.

Agora vamos fazer uma pausa nas estatísticas de hackers por um tempo.

Veja, hackers são como você e eu de certa forma. Eles são curiosos sobre o mundo e eles mesmos. Alguns deles descrevem o hack como uma adrenalina. Todas as pessoas têm o que querem - alguma dança, outras escalam montanhas e assim por diante. Os hackers exploram vulnerabilidades. Venha para pensar sobre isso - é como um quebra-cabeça. Coloque todas as peças certas juntas, e pronto.

Agora vamos imaginar uma situação. Você está em um hotel. Há uma televisão no seu quarto. O que você vê? "A TV", a maioria de vocês diria. O que um hacker vê? Uma porta de entrada para a rede do hotel. É semelhante a qualquer outro alvo.