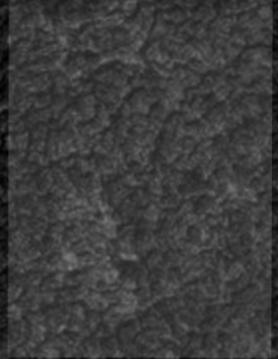




Marco Aurélio Thompson



A Bíblia HACKER



www.abibliahacker.com

Marco Aurélio Thompson

A Bíblia Hacker

Volume 1

2^a edição

Copyright © 2017 ABSI

Copyright © 2017 da Editora do Autor

Thompson, Marco Aurélio

A Bíblia Hacker – Volume 1 / Marco Aurélio Thompson 2. ed. – Rio de Janeiro:
Editora do Autor, 2017.

ISBN: 978-85-98941-41-7

1. Computadores - Segurança 2. Hackers de computadores 3. Internet (Rede de computadores) 4. Redes de computadores - Medidas de segurança I. Título

Índices para catálogo sistemático:

1. Internet: Invasões: Medidas de Segurança: Ciência da computação 005.8
2. Invasões: Internet: Medidas de Segurança: Ciência da computação 005.8

Todos os direitos reservados. Proibida a reprodução total ou parcial, por qualquer meio ou processo, sem autorização expressa do autor. A violação dos direitos autorais é punível como crime com pena de prisão e multa, conjuntamente com busca e apreensão e indenizações diversas (cf. Art. 184 e parágrafos do Código Penal, alterações da Lei 10.695/2003 e Lei 6.910/98, Lei dos Direitos Autorais).

O autor e o editor acreditam que as informações aqui apresentadas estão corretas e podem ser utilizadas para qualquer fim legal. Entretanto, não existe qualquer garantia, explícita ou implícita, de que o uso de tais informações conduzirá sempre ao resultado desejado. Os nomes de sites e empresas porventura mencionados foram utilizados apenas para ilustrar os exemplos, não tendo vínculo nenhum com o livro, não garantindo sua existência nem divulgação. Eventuais erratas estarão disponíveis no site www.abibliahacker.com. O autor também se coloca à disposição dos leitores para dirimir dúvidas e discutir ou aprofundar os assuntos aqui tratados, por qualquer meio de comunicação disponível.

Editora do Autor

A Bíblia Hacker

Marco Aurélio Thompson

www.editoradoautor.com

www.abibliahacker.com

MarcoAurelio.Net

O que é a Bíblia Hacker?

A **Bíblia Hacker** é o maior livro hacker do mundo. O tamanho A4 (21 x 29,7cm) é o tamanho de uma folha de papel de impressora. A primeira versão foi lançada em 2005 com 1.200 páginas e a versão 2017 tem mais de 1.600 páginas distribuídas em 12 volumes e abrange todo o universo hacker.

É também um livro pensando para a acessibilidade. A fonte tamanho grande garante a leitura confortável também para aqueles com baixa visão. O papel é o *couché*, o mesmo usado nas enciclopédias.

Ilustrações são centenas. A maioria das telas capturadas dos programas, demonstrando passo a passo como usar cada técnica e cada ferramenta.

A primeira edição de **A Bíblia Hacker** surgiu em 2005 e naquela época as pessoas associavam o conhecimento hacker a crimes de informática demonstrando grande ignorância sobre o assunto. Também não existia as facilidades de impressão de hoje, em que várias empresas oferecem o serviço de impressão sob demanda (*on demand*) e estão mais propensas a publicar livros *hacker*.

Em 2005 as editoras não publicavam livros hacker. A não ser aqueles considerados *inofensivos*. A opção que tínhamos era encomendar por conta própria uma tiragem mínima de 500 exemplares ao custo aproximado de 80 mil reais. Era um investimento alto e de risco, pois não sabíamos quanto tempo levaria para vender os 500 exemplares ou recuperar o investimento. E, como esse tipo de literatura se desatualiza rápido, optamos pela produção artesanal, em menor escala.

Assim o fizemos. As 600 folhas — 1.200 páginas — eram impressas frente e verso em impressora laser, depois encadernadas manualmente por um artesão.

Inicialmente o prazo de entrega acertado com o profissional era de três dias. Com o aumento das vendas subiu para uma semana. Com um mês de vendas, devido à grande procura, o prazo de entrega já estava em três meses. Esse prazo não dependia de nós. Dependia do artesão. Porém, a ansiedade das pessoas e um pouco de desconfiança começaram a causar constrangimentos, com pessoas postando na Internet que pagaram e não receberam, mesmo tendo concordado em aguardar o prazo longo da entrega ou alegando não saberem disso.

O mais desagradável era ver que após receberem **A Bíblia**, não voltavam ao site ou fórum para dizer que já havia recebido. Ainda pior eram aqueles que sequer compraram **A Bíblia** e postavam ofensas e alegações de não terem recebido. Alguns desses mentirosos foram processados por conta disso.

Para evitar toda essa aporrinhação decidimos suspender as vendas da **Bíblia Hacker** 2005. E só relançar quando tivéssemos certeza de que não haveria atraso nas entregas devido a aumento de demanda.

O tempo passou, lançamos diversos outros livros e cursos em videoaulas, nosso trabalho tornou-se cada vez mais conhecido e respeitado, a ponto de firmarmos convênio com as Forças Armadas, Ministério Público, Polícia Federal e Polícia Civil, até que em 2016 achamos que seria um bom momento para retornar ao projeto **A Bíblia Hacker**.

Só não daria para usar o material de 2005 pois quase tudo mudou. Até eu, que naquela época cursava Pedagogia e hoje tenho a Pedagogia e mais oito, entre graduações, Pós e MBA, em andamento ou concluídos, incluindo um bacharelado em Sistemas de Informação e um MBA em Gestão de TI.

A Bíblia Hacker versão 2017 foi escrita do zero. Começamos a (re)pensar o projeto em 2016 e fizemos a redação dos artigos a partir de março de 2017, com o lançamento do Volume 1 em abril desse mesmo ano.

A ideia era começar a redação em janeiro de 2017, mas nosso compromisso com a editora Érica-Saraiva para escrever o livro Windows Server 2016 – Fundamentos, só nos deixou com tempo para **A Bíblia Hacker** depois de março. E assim foi.

Comparando com **A Bíblia Hacker** 2005, na versão 2017 a única coisa que aproveitamos foi o título. O que você tem em mãos é nada menos que **o maior livro hacker do mundo**, distribuído em 12 volumes e totalizando mais de 1.600 páginas.

Aproveite!

Sobre o autor (Quem é esse cara?)

Carioca, professor, escritor¹ com licenciatura em Letras, pedagogo, psicopedagogo especialista em superdotação e heutagogia, jornalista², empresário, bacharel em Sistemas de Informação, MBA em Gestão de TI, poli graduando em Matemática e Administração de Empresas, estudante de Direito, hacker ético profissional, poeta, contista, cronista, roteirista, videomaker, voluntário em grandes eventos, consultor pelo Sebrae, atual presidente da Associação Brasileira de Segurança da Informação (ABSI), dirigente da Sociedade Brasileira de Educação para o Trabalho (SBET), diretor do Centro de Educação para o Trabalho (CET) e da Escola de Hackers.



Esse é Marco Aurélio Thompson em poucas palavras.

¹ Autor de 84 livros com previsão de chegar a 100 livros publicados até janeiro de 2018. Páginas no Skoob: <http://www.skoob.com.br/autor/livros/12924> e <http://www.skoob.com.br/autor/livros/17525>.

² Registro profissional como jornalista: 0005356/BA.

Hacker³

(Ing. /réquer/)

s2g.

1. Inf. 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.]

[Cf. cracker.]

Fonte: <http://www.aulete.com.br/hacker>

³ A pronúncia /ráker/ ou /réker/ são corretas. O dicionário online Caldas Aulete e muitos outros registra /réker/ e nós preferimos essa. Você usa a pronúncia que quiser.

SUMÁRIO

- Como Ser Hacker – Parte 1, 9
- Como enfrentar a Matrix, 18
- Você já roubou um carro?, 19
- O que se ganha sendo hacker?, 26
- As videoaulas da Bíblia Hacker, 28
- Criando um laboratório de testes, 29
- Escolhendo o software de virtualização, 35
- Criando a máquina virtual para instalar o Windows, 45
 - O primeiro boot na máquina virtual, 51
- O segredo dos hackers: portas, IPs e vulnerabilidades, 53
 - O que passa pelas portas?, 56
 - O aperto de mão em três vias, 59
 - Como proteger as portas?, 63
 - IPs e vulnerabilidades, 64
 - Varredura de portas, 65
 - Praticando a varredura de portas, 67
 - Descoberta de host e serviço, 70
 - Opções de varredura, 71
 - Enumeração do Windows, 73
 - Port Scan Avançado, 74
 - Tabela de uso das portas TCP/UDP, 77

Varredura online, 77
Como os hackers agem, 79
Aprenda a ser hacker com cases, 80
A Casa do Hacker: A Escuta – Parte 1, 81
 O falso botão de download, 86
 Jargon File, 87
 Glider, 87
 Escrita Leet, 89
 Owned, 92
 Lammer, 93
 As cores dos chapéus, 95
A importância do inglês para os hackers, 97
 Hackeando tudo, 109
Fazendo download do ISSUU, 111
 Hacks com PDF, 113
O que inicia com o Windows?, 117
 Memes, 121
 Invasão de e-mail, 129
 Scam, 141
 Spam, 143
 Spoofing, 144
 Estrutura do URL, 148
Invasão de e-mail por Telnet, 149
 A página de erro 404, 150

Casemod, 151

Você precisa aprender a escrever código, 155

Entendendo a programação de computadores, 158

 Exploits, 167

 Anatomia do exploit, 168

 Usando exploits, 171

 Exploit no filme Matrix Reloaded, 173

 O Linux e os hackers, 175

Por que o Linux Kali é a melhor opção para os hackers?, 175

 Criando a sua própria distribuição Linux, 182

Preparando o VirtualBox para o Linux Kali, 194

 Tux, 199

 Projeto Wikilivros, 200

Como ter acesso as videoaulas da Bíblia Hacker?, 202



Como Ser Hacker – Parte 1

Após todos esses anos ensinando as pessoas a ser hacker, se há uma coisa que descobri é que a maioria, principalmente os mais jovens, sempre querem partir para os “finalmente”, evitando tanto quanto possível “perder tempo” com qualquer coisa que não esteja relacionada à prática da invasão.

O problema desta abordagem 100% *hands on* (mãos na massa) é que ela não forma hackers ou qualquer outro tipo de profissional. Até fica a impressão de aprendizado porque o sujeito olha o tutorial ou videoaula, repete o que vê e às vezes funciona. O problema é que funcionando ou não, quem só consegue fazer invasão usando tutorial não tem conhecimento para entender o que acontece na invasão.

Ou se houver alguma variação na técnica como, por exemplo, a ferramenta demonstrada na videoaula era a versão 3 e a mais atual é a versão 4. O fato de a ferramenta não ser exatamente igual acaba com a alegria de quem acredita que é possível ser hacker só com tutoriais e videoaulas.

Nos Estados Unidos até deram um nome para quem só é hacker assim: Script kiddie. Um nome depreciativo para quem acha que sabe *hackear*, mas que só consegue *hackear* usando fórmulas prontas.

A Bíblia Hacker não é um livro para Script kiddie. **A Bíblia Hacker** é para quem quer se tornar hacker de verdade. Um hacker que domina a tecnologia, sabe o que faz e é capaz de desenvolver as próprias técnicas de invasão. Não vamos formar dependentes de tutorias destes que se acha na Internet.

Para alcançar este objetivo – de tornar você um hacker completo – precisamos apresentar a você junto com a prática, assuntos considerados “teóricos” e “chatos”. Mas são assuntos que se você não conhecer, não será capaz de ser hacker.

Se **A Bíblia** fosse um livro apenas demonstrando tutoriais práticos sem discutir a teoria envolvida o nome seria **A Bíblia do Script Kiddie**, não **A Bíblia Hacker**. E não seria eu a escrevê-la, pois quero sentir orgulho do meu trabalho, não vergonha.

Este primeiro capítulo é um bom exemplo do que estou dizendo. Ele faz parte da seção fundação (*foundation*), ou seja, das bases necessárias para alguém ser hacker. Mas é um capítulo para ler e refletir. Não trataremos de técnicas, nem de invasões, nem de ferramentas aqui. Estes são assuntos para os capítulos mais adiante.

O problema é que se você não entender o que estamos discutindo agora, vai chegar aos capítulos sobre técnicas, estratégias e ferramentas totalmente sem rumo. A melhor imagem que tenho de alguém com este comportamento é um zumbi caminhando sem rumo e dizendo “cérebro, cérebro”. É só trocar cérebro por “ferramentas prontas” ou “tutoriais” que o zumbi se torna um Script Kiddie.

Se você realmente quer tornar-se um hacker tão bom ou até melhor do que eu comece por aqui, entendendo o que é e como ser hacker. Após a leitura me diz se mudou alguma coisa na sua forma de pensar sobre hacker.

O que é ser hacker

A grosso modo ser hacker é invadir computadores. Todos - até as pessoas leigas - concordam com isto. Acontece que as coisas não são tão simples assim. Primeiro que a palavra hacker é de origem inglesa e diz que hacker é quem faz hacks. Da mesma forma que fotógrafo é quem tira fotografia, motorista é quem dirige, skatista é quem anda de skate, e assim por diante.

Então para entender hacker precisamos saber o que é hack. E hack é o mesmo que atalho, macete, gambiarra. O hacker é o cara dos atalhos, dos macetes e das gambiarras.

Se você chegar nos Estados Unidos e disser que é hacker, se não estiver em um ambiente de TI (Tecnologia da Informação) é capaz de pensarem que você é o cara dos macetes, não um hacker de computador.

Mas como estamos no Brasil a palavra hacker ficou totalmente vinculada à informática e invasores de computadores. O que se faz nestes casos é ajustar o discurso. Se eu estou falando com americanos fora de um contexto de TI e quero dizer que sou hacker, talvez precise dizer:

I'm a computer hacker.

Traduzindo:

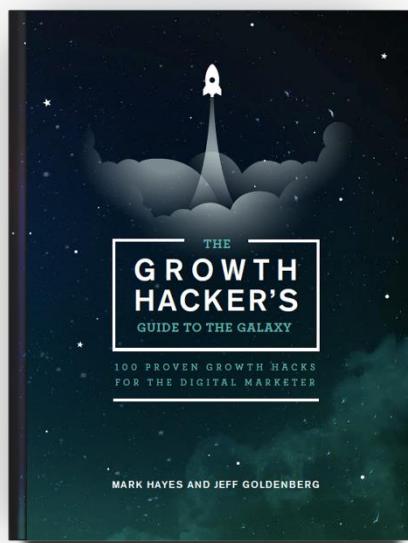
Eu sou hacker de computador.

E para os brasileiros que já se limitaram a entender hacker como invasor, o melhor é dizer:

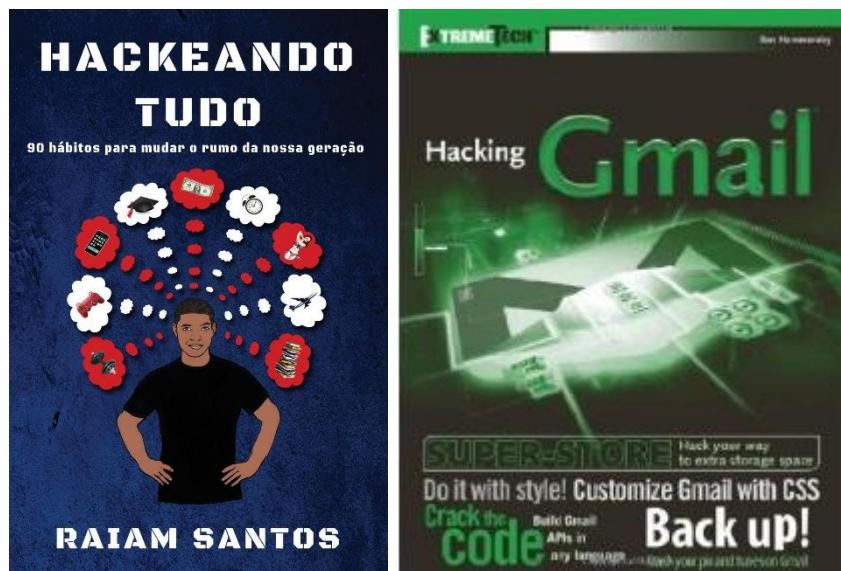
Eu sou hacker ético.

Ou hacker ético profissional. Porque dizer só hacker pode fazer com que pensem que você é hacker invasor criminoso. Melhor não arriscar. A propósito, tenho quase certeza de que antes desta explicação, se eu te perguntasse o que é ser hacker, ou você teria dificuldade para responder ou limitaria sua resposta a dizer que hackers são invasores de computadores. Lembre-se que esta resposta é limitada e só está correta no Brasil.

Observe que interessante:



O título é **The Growth Hacker's – Guide to The Galaxy**. Parece ser um livro hacker, certo? E estes: **Hackeando Tudo** ou **Hacking Gmail** (Hackeando o Gmail). O que lhe parece?



O que eles têm em comum é que todos são livros hacker, mas nenhum é sobre invasão de computadores.

Growth Hacker é uma profissão nova e diz respeito a administrar a empresa fugindo da administração convencional, ou seja, experimentando atalhos e estratégias que a administração formal nem emprega e nem admite. Mas como os tempos são outros e ninguém pode dizer com certeza onde vamos parar, as empresas inteligentes passaram a contar com um hacker no marketing, vendas ou na administração. Mas não é o hacker de informática. É o hacker com o sentido original da palavra: o cara dos macetes. O cara que vai descobrir atalhos para ajudar a empresa a superar a concorrência.

O Hackeando Tudo é um livro com dicas (macetes) de produtividade. Nada a ver com invasão de computadores também. O que mais parece sobre invasão, que é o Hackeando o Gmail (**Hacking Gmail**), nada tem a ver com invasão também. São dicas para usar melhor o Gmail. Só isso.

Além dos livros o Youtube está cheio de canais hacker, como por exemplo o **More Photoshop Hacks** (https://youtu.be/XWc4Ou_cXR0) que nada mais é que um canal com (mais) dicas e macetes para o Photoshop:



Como ser hacker

Agora que você já entendeu que hacker é o cara dos macetes e que só no Brasil temos esta visão limitada de hacker, que hacker é apenas um invasor de computadores, vamos descobrir como ser hacker e vamos fazer isto te ensinando dois hacks que você pode começar a usar a partir de hoje. Lembre-se que hacker é quem faz hacks. O hack que você cria ou o hack que ensinaram a você. Vamos começar com dois hacks poderosos:

Hack #001

Se você tiver alguma coisa para fazer no caixa do banco entre na agência faltando apenas 20 minutos para fechar. Neste horário uma mágica acontece e os caixas incorporam o The Flash. Você levará menos tempo no banco se chegar lá por volta do meio dia por exemplo. E as chances de ser assaltado no golpe conhecido como *saidinha bancária* são menores. De acordo com as Secretarias de Segurança Pública este tipo de assalto ocorre com mais frequência na parte da manhã ou início da tarde.

Hack #002

Para obter aquelas batatas fritas crocantes iguais as servidas nas redes de fast food como o McDonald's, o macete é ver se consegue a batata apropriada para fritar. Ela é vendida com o nome batata rosada (tem a casca rosada) ou batata Asterix. Mesmo que você não consiga esta batata especial para fritar, experimente fritar duas vezes. Primeiro você frita até a batata começar a ficar transparente. Depois você frita de novo e ela vai ficar sequinha e crocante, igual à do McDonald's.

Você deve estar se perguntando o que isso tem a ver com invasão de computadores, não é mesmo? Não tem nada a ver com computadores, mas tem tudo a ver com hacker. É claro que **A Bíblia Hacker** só vai tratar de hacks relacionados a sistemas informatizados, mas eu precisava mostrar a você que é possível ser hacker além dos computadores. E na verdade é isto que eu gostaria de ver acontecer com você. Será um grande desperdício se você só usar hacks com informática. Torne-se um hacker por completo, sendo hacker em todas as dimensões da sua vida.

Hackeie tudo. Seu tempo. Sua saúde. Seus relacionamentos familiares, amorosos e sexuais. Seus estudos. Seu emprego. Sua grana ou falta dela. Hackeie tudo, incluindo computadores, é claro.

Mas como ser hacker? Vou te dizer como. Para você ser hacker você precisa reeducar seu modo de pensar. Só assim você consegue fazer seus próprios hacks. Não importa se você vai ser hacker só de computadores ou se vai hackear tudo em sua vida. Tudo começa com um novo modo de pensar.

Para você entender como isso funciona vamos falar rapidamente sobre *status quo*. É uma expressão em latim que significa "o estado das coisas". A Sociedade para se manter organizada precisa desse *status quo*. Talvez você não tenha parado para pensar sobre o assunto, mas quando sai para trabalhar e põe o lixo para fora é o *status quo* que vai fazer o lixo "sumir" e o transporte público aparecer no ponto de embarque, tudo dentro de uma previsibilidade necessária ao funcionamento da Sociedade. Isto é o *status quo*. Precisamos dessas coisas funcionando para nos sentir seguros e com a sensação de que a Sociedade está funcionando e organizada.

Um outro exemplo é quando você vai até a padaria e sabe que haverá um pão quentinho à sua espera. Parece ótimo o *status quo*, não é verdade? O problema é que existem muitas coisas erradas que fazem parte do *status quo* e justamente por ser o *status quo*, aquilo que nos dá uma sensação de ordem

e segurança, nós deixamos do jeito que está mesmo quando nos causa dor, perturbação, aborrecimento ou prejuízo.

Aproveitando o momento turbulento que passa o Brasil, com várias acusações contra a cúpula que dirige o país, em princípio tudo parece muito distante da nossa realidade. Os acusados de corrupção são o presidente e os ex-presidentes, ministros, senadores, deputados federais e estaduais, governadores, empresários, gente com as quais provavelmente nunca vamos esbarrar por aí.

Mas pertinho de você, não importa a cidade em que você more, tem um bando de espertalhões se aproveitando do *status quo* e ninguém fala e nem faz nada. São os prefeitos e vereadores, com salários absurdos, aposentadoria precoce e uma carga horária de trabalho obscena, algo como trabalhar 30 dias em um ano.

Por que aceitamos isso? Porque isso já faz parte do *status quo*. Já está estabelecido, aceito como “normal” e ninguém questiona. Lembra o conto **A Roupa Nova do Imperador** de autoria do dinamarquês Hans Christian Andersen, inicialmente publicado em 1837. No conto alguns espertalhões convencem o povo de que o rei estava usando uma roupa invisível, quando na verdade estava nu. Quem questionou o *status quo* e abriu os olhos do povo foram as crianças.



Este é um dos maiores segredos para alguém que quer ser hacker. Entender que vivemos submissos ao *status quo* e se quisermos fazer hacks, precisamos subverter o *status quo*. Você pode se referir ao *status quo* como Matrix se quiser. Dá no mesmo. É uma situação mantida por conveniência, em que

todos concordam com aquela situação, mesmo que a situação seja extremamente prejudicial a nós.

Se você mora em área de risco, em local dominado por traficantes e bandidos, saiba que tudo começou com a bandidagem subvertendo o *status quo*. Todo bairro começa como um lugar tranquilo e de gente de bem. Até aparecer o primeiro traficante ou assaltante. As pessoas por medo não fazem nada. Fingem que não estão vendo. Então chega mais um traficante. E mais outro. Quando se dão conta o bairro está dominado, ou seja, tem novo *status quo*.

Se a comunidade tivesse se envolvido quando apareceu o primeiro traficante, ele não teria se criado e não haveria um bando deles por aí. O *status quo* da segurança pública no Brasil hoje é definido como dominado pelo tráfico.

O poder do *status quo* é tão grande que as pessoas acham normal o transporte público superlotado, ficar constantemente doente, trabalhar o mês todo e ficar sem dinheiro antes do próximo salário, pagar juros de mais de 400% ao ano no cartão de crédito. São exemplos de coisas absurdas que são aceitas como normais pela maioria da população. Minha vida mudou quando eu parei de aceitar coisa ruim como normal em minha vida.

Veja este exemplo de como o hacker poderia usar o *status quo* a seu favor. Nas Olimpíadas Rio 2016 um dos centros esportivos ficava num bairro chamado Deodoro. Quem entrasse pelo lado esquerdo se deparava com uma barraca do Exército Brasileiro onde passava por uma minuciosa revista e lá dentro por mais outra. Quem entrasse pelo lado direito só passava por uma única revista. Da rua dava para ver que um lado tinha a revista minuciosa e no outro não. Muita gente ia pelo lado esquerdo. E você? O que faria? Ser revistado duas vezes ou apenas uma? Eu acho que você prefere nenhuma, mas como tem que ser revistado é melhor ser uma do que duas, concorda? Como hackear isso? Você já deve ter matado a charada: entrar pelo lado direito, que só tem uma revista.

Eu sei que você está ansioso para começar a invadir computadores, mexer no Metasploit, usar o Kali ou Backtrack. Mas por favor não ignore esta parte. Se você não assimilar isto vai se comportar como um idiota carregando uma espingarda. Entenda o que é e como ser hacker antes de começar a ser um. Não se preocupe que a maior parte da **Bíblia Hacker** tem práticas de uso de ferramentas e técnicas de invasão, mas antes de chegar lá você precisa ser preparado.

Por enquanto espero que você ainda lembre que hacker é o cara do macete, que esperamos que você seja hacker por completo, capaz de hackear todas as áreas da sua vida, e que para ser hacker você precisa subverter o *status quo*.

Quando uma empresa ou fabricante cria um sistema de segurança, eles acreditam que realmente o sistema é seguro. Este é o *status quo*, o esperado. Até chegar alguém que não respeita o *status quo* e quebra tudo. Ou invade se preferir este termo.

Durante toda a minha vida ouvi dizer que era difícil passar em vestibular, conseguir boas notas no Enem (Exame Nacional do Ensino Médio), que era difícil cursar a faculdade. Este é o *status quo* que me venderam. Quando eu passei a hackeá-lo tornei-me capaz de cursar de duas a quatro faculdades ao mesmo tempo. Este é apenas um dos benefícios quando se subverte o *status quo*. Ser hacker é confrontar o *status quo*, é vencer a Matrix.

Como enfrentar a Matrix

Quem procura nossos cursos e livros está em busca de informações que o tornem capaz de invadir sites, contas de redes sociais e e-mail. Esperamos que a intenção com este conhecimento seja para trabalhar como profissional de segurança da informação, como hacker ético profissional ou como forma de se proteger. Mas não somos ingênuos a ponto de acreditar que entre os leitores não haverá aquele que está em busca de vingança, é um revoltado

querendo destruir tudo o que encontrar pela frente ou quer tirar algum proveito financeiro do conhecimento hacker, invadindo contas bancárias, desviando dinheiro dos outros e coisas do tipo. E não podemos esquecer aqueles que procuram o conhecimento hacker para investigar a vida do(a) namorado(a), amante, esposa(o), parceiro sexual, etc.

Eu não estou aqui para julgar ninguém e quem descambiar para o lado do crime que seja feliz. Da minha parte basta eu dizer que a intenção do livro é para uso lícito. Quem fizer uso ilícito arque com as consequências. Não é problema meu. Tanto quanto não é problema de um instrutor de tiro ou professor de artes marciais se o aluno fizer o curso para atirar ou dar um golpe mortal em alguém. Azar da vítima e a polícia que faça a sua parte.

Por outro lado, é justamente esta motivação que vai torna-lo(a) um hacker ou não. Se você não tiver uma motivação forte o suficiente você não seguirá adiante. Se você quer entrar no Facebook da sua ex para ver com quem ela anda se **estrepando**, use esta motivação para impulsionar seu aprendizado.

Quem sabe durante o processo você perceba que não vale a pena e passe a direcionar seu conhecimento para causas mais nobres? Mesmo que não mude de ideia e queira mesmo detonar o Facebook da(o) ex, sem uma motivação forte nunca vi ninguém ser hacker.

Encontre sua motivação. Este é mais um dos ingredientes que você precisa para se tornar hacker. E vamos precisar dele para enfrentar a Matriz, junto com o conhecimento dos fundamentos tecnológicos que a mantém.

Você já roubou um carro?

Espero que não. Mas você já viu como os ladrões de carro trabalham? Eles costumam chegar pela lateral, enfiar um arame estrategicamente entortado por alguma brecha no vidro e quando estão dentro do veículo dão a partida sem precisar da chave. Como isto é possível?

Isto é possível quando a pessoa conhece muito bem o funcionamento da segurança do veículo e como se dá a partida. Você sabe dar a partida no seu carro sem ter a chave? Acredito que não. Então podemos supor que estes ladrões de carro tem um conhecimento específico que não é todo mundo que tem. Eu não sei dar partida em um carro sem ter a chave, mas sei invadir um computador com a mesma facilidade do ladrão de automóveis.

Entendeu a moral da história? Vou explicar. Existe um conhecimento que podemos denominar como conhecimento leigo, onde a pessoa só consegue usar a coisa do jeito normal, do jeito que o fabricante previu.

Você provavelmente tem o conhecimento leigo de carros. Sabe o básico que é abrir e fechar, ligar e desligar, conduzi-lo no trânsito. E talvez também tenha o conhecimento leigo de computador: ligar e desligar, instalar programas, usar o Word, Excel, PowerPoint, navegar na Internet.

Mas da mesma forma que o ladrão de carros tem um conhecimento que permite levar o seu carro, tendo ou não a chave, existe este conhecimento de informática que permite obter coisas do seu computador. É um conhecimento que o leigo não tem e que não aparece nem nos cursos de informática.

Seria então o conhecimento profissional? Na verdade, não. Em contraponto ao conhecimento leigo sobre carros teríamos o mecânico. Não é todo mecânico que consegue abrir a porta do carro com a mesma facilidade do ladrão de carros. Da mesma forma um profissional de informática, que pode ser um técnico ou até mesmo um engenheiro ou alguém formado em Ciências da Computação, não é capaz de invadir um computador se não tiver conhecimento para fazer isso. Este conhecimento subversor é o que chamamos de conhecimento hacker. O que ocorre é que, além do conhecimento leigo que só permite o uso, e o conhecimento profissional ou avançado, que permite o uso avançado ou fazer reparos, consertos e manutenção, existe um conhecimento específico e voltado para a quebra da

segurança que é o que nós chamamos de conhecimento hacker. O conhecimento que você precisa para subverter o *status quo*. O conhecimento que vai derrubar a Matrix.



Se você observar na figura acima o conhecimento hacker é um conhecimento bem distinto que pode até ser menor do que o conhecimento do profissional.

Isto ocorre porque o profissional precisa entender de vários assuntos, nem sempre relacionados a informática ou computadores. Quando cursei Sistemas de Informação na Unifacs¹ fui obrigado a estudar 45 disciplinas durante 4 anos, distribuídas entre:

- **PROGRAMAÇÃO:** Algoritmos e Programação, Engenharia de Software I e II, Estrutura de Dados I e II, Linguagem e Técnicas de Programação I, II e III, Linguagens Formais e Compiladores, Desenvolvimento de Aplicações para Web, Interface Homem-Computador e Banco de Dados I e II.
- **DISCIPLINAS DIVERSAS:** Antropologia e Cultura, Meio Ambiente, Desenvolvimento Humano e Social, Comunicação Profissional, Desafios Contemporâneos, Metodologia Científica, Metodologia de Pesquisa e Empreendedorismo.

¹ <http://www.unifacs.br/graduacao-bacharelado/sistemas-de-informacao/>

- **SISTEMAS:** Análise e Modelagem de Sistemas de Informação, Arquitetura e Organização de Computadores, Sistemas Operacionais, Sistemas de Informação, Sistemas de Informação Aplicados, Gerência de Projetos, Governança de TI e Introdução à Computação.
- **MATEMÁTICA:** Calculo I e II, Fundamentos de Matemática Discreta, Fundamentos de Matemática para Computação, Matemática Aplicada e Probabilidade e Estatística.
- **REDES:** Redes de Computadores I e II e Sistemas Distribuídos.

Além de um TCC (Trabalho de Conclusão de Curso) em que tratei da IoT (Internet das Coisas), um estágio supervisionado de 300 horas e apenas 60 horas na disciplina Auditoria e Segurança de Sistemas de Informação.

Repare que eu tive uma carga horária bem distribuída entre sistemas, matemática, programação e redes. Tive umas disciplinas obrigatórias, mas não relacionadas a informática e apenas 60 horas divididas entre Auditoria e Segurança de Sistemas de Informação.

Este é o conhecimento profissional, mas está longe de ser um conhecimento hacker. Por favor não culpe a Unifacs por isso. O objetivo da graduação em Sistemas de Informação não é formar hackers. Se você comparar a grade curricular de qualquer faculdade vai ser mais ou menos a mesma coisa: REDES, PROGRAMAÇÃO, MATEMÁTICA, SISTEMAS, algumas disciplinas obrigatórias e só um pouquinho de segurança da informação, quando houver.

E não pense que verá ataques e invasões. Na faculdade você trata mais de conceitos, não tem aulas direcionadas a ataques ou como se proteger deles.

É por isso que um adolescente que vai mal da escola, um Zé Ninguém que não tem onde cair morto, quando consegue acesso ao conhecimento hacker é capaz de complicar a vida do profissional de segurança.

Sempre me perguntam qual faculdade devem cursar para se tornar hackers. A resposta é que nenhuma faculdade será capaz de torna-lo(a) hacker. A única vantagem da formação universitária é abrir as portas para o mercado de trabalho, dar maior credibilidade a você como hacker ético e fornecer um conhecimento além do conhecimento leigo, algo que será muito útil.

Para ser hacker você vai precisar do conhecimento hacker e o conhecimento hacker não está nas faculdades. Está espalhado pela Internet, organizado em alguns cursos e livros que tem por aí e também aqui na **Bíblia Hacker**.

Nem a Pós Graduação do SENAC em Segurança da Informação – que pretendo cursar em 2018 – nem o MBA em Gestão da Segurança da Informação pela FMU que já estou cursando, incluem disciplinas relacionadas ao uso de ferramentas hacker. É tudo muito filosófico e acadêmico, que na verdade é o *status quo* do ensino universitário em qualquer lugar do mundo, inclusive Harvard (que já foi invadida algumas vezes).

É claro que não dá para ser hacker sem ter também o conhecimento leigo. O que não precisa, embora ajude, a ter também o conhecimento profissional.

Você já usou um iMac? O iMac é o computador da Apple que usa o sistema operacional macOS baseado no kernel (núcleo) do Linux. O iMac é um computador caro para os padrões do brasileiro. Um fato interessante é que alguém que nunca viu o iMac talvez tenha dificuldade até para liga-lo.



Agora vamos supor que você queira hackear um iMac. Não dá para fazê-lo só com o conhecimento hacker. No mínimo você vai precisar também do conhecimento leigo, compreende? Então podemos dizer que o conhecimento hacker é no mínimo o conhecimento leigo + o conhecimento hacker, podendo ou não incluir o conhecimento profissional.

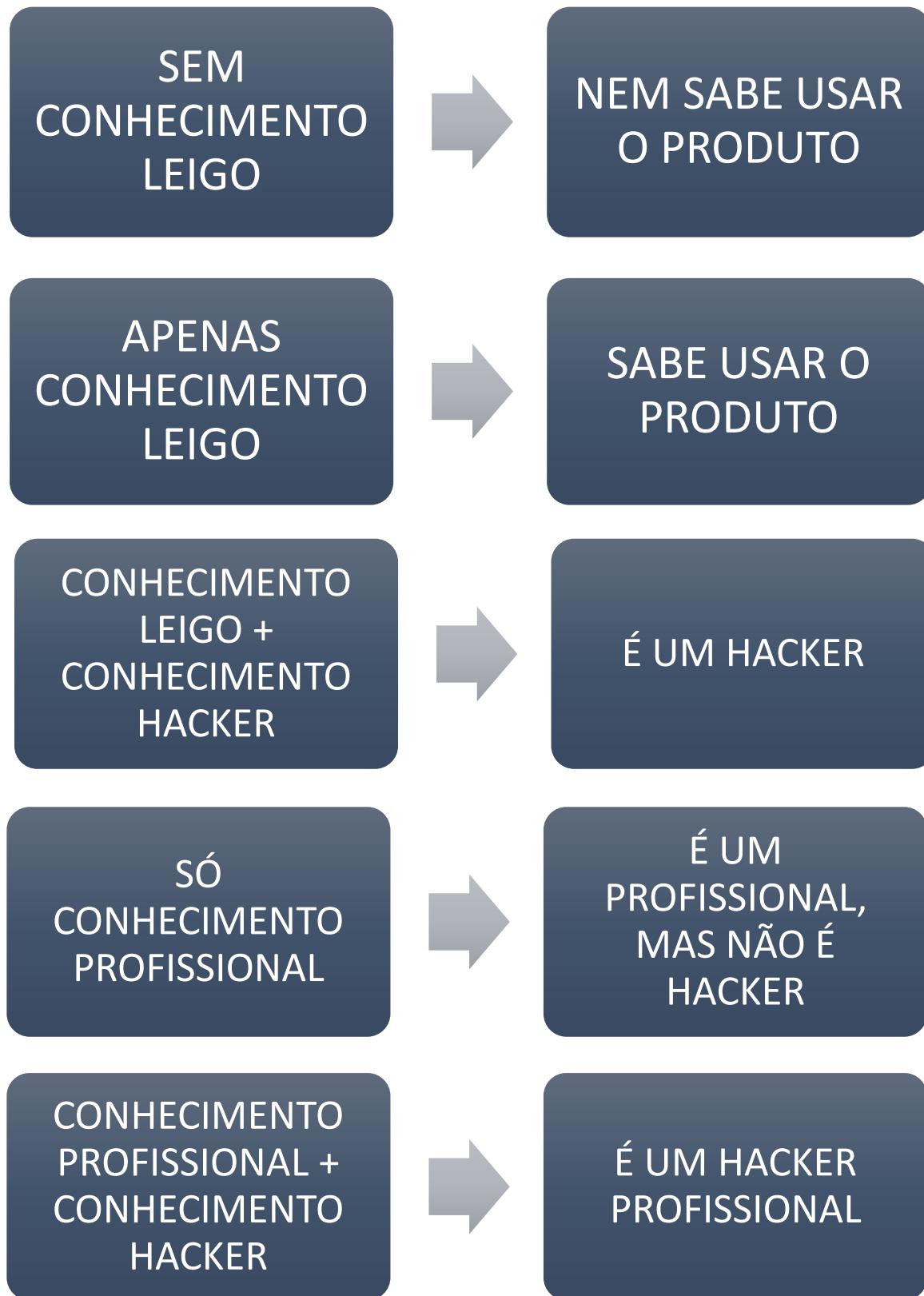


Sabe porque isto é uma boa notícia? É uma boa notícia porque mesmo se você for leigo você vai poder ser hacker. O conhecimento hacker, como foi possível perceber, não é um conhecimento maior que o conhecimento profissional. É um conhecimento à parte e específico.

Um profissional que saiba fazer a manutenção de um celular talvez não consiga cloná-lo. Mas alguém leigo, que só sabe usar o celular no dia a dia mais obtenha o conhecimento hacker, será capaz de clonar o celular. O profissional também será capaz de clonar, se tiver o conhecimento hacker.

Às vezes me perguntam se é preciso ser programador para ser hacker. Ajuda ser programador, mas não precisa ser programador, até porque programador só é hacker se tiver também o conhecimento hacker.

Podemos resumir tudo da seguinte forma:



O que se ganha sendo hacker?

Sendo hacker você ganha duas coisas muito valiosas: poder e dinheiro. Poder no sentido de fazer coisas que a pessoa comum não faz. Eu por exemplo trabalho a hora que quero, raramente entro em filas, faço várias faculdades ao mesmo tempo, moro na cidade em que escolhi para morar – sou do Rio de Janeiro e moro em Salvador (Bahia). E ganho dinheiro fazendo o que gosto, ajudando as pessoas a sair do que se popularizou a chamar de Matrix, mas que na verdade é o velho e conhecido *status quo* do qual já falamos.

Sendo hacker você vai aumentar as chances de ter o que você ainda não tem na sua vida. Como já foi dito ser hacker não se limita a invadir computadores, embora seja este o foco da **Bíblia Hacker**.

Mas como você vai precisar mudar seu modo de pensar para se tornar hacker, esta mudança vai refletir em todos os aspectos da sua vida. Não se limite a ser hacker para invadir computadores. Isto é um grande desperdício. Use o conhecimento hacker também para ajuda-lo(a) a emagrecer, se isto for seu problema, arrumar um emprego, entrar para a faculdade, quantas quiser, ter um(a) namorado(a), viajar. Tudo o que você acha que não pode fazer você vai descobrir que pode usar o conhecimento hacker e obter.

Olhe ao seu redor e verá quanta gente idiota, com pouco estudo, feia pelos padrões de beleza atuais, mas que estão conquistando seus sonhos, subvertendo o *status quo*, mesmo que nem saibam que isto existe.

Quais são as chances de um jovem com pouco estudo e aparência de gosto duvidoso, conseguir um salário de cinco ou mais mil reais por mês? O Youtube está cheio deles enquanto engenheiros estão por aí procurando emprego e aceitando salários de até 3 mil reais.

Ser hacker é isso. É encontrar um desafio determinado pelo *status quo*, como por exemplo o que diz que sem estudo você não consegue emprego e conseguir ganhar mais do que um engenheiro fazendo o que gosta no Youtube.

Este é apenas um exemplo. Conforme for lendo os artigos da **Bíblia Hacker** você vai ser apresentado a muitas ideias e tecnologias que vão demorar a chegar no Brasil. E com nossa ajuda vai acabar descobrindo novas formas de usar seu conhecimento hacker, além da simples invasão de computadores.

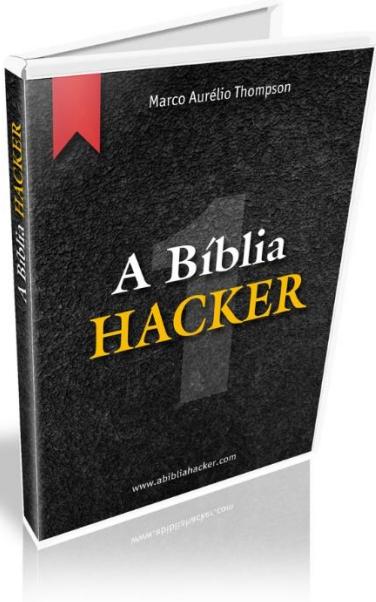
Eu tenho certeza de que te disseram que para se dar bem na vida você precisa concluir o Ensino Médio, o antigo 2º Grau, e depois fazer o ENEM para conseguir uma vaga na faculdade ou tentar uma vaga no SISU.

Se você aceita a minha opinião sincera eu preciso dizer que esta fórmula é mentira. Ela não funciona mais tem uns vinte anos. Funcionou quando quase não havia profissional formado em curso superior. Agora você encontra faculdade em qualquer esquina e sem querer desmerecer qualquer profissão, até dona de casa e empregada doméstica hoje faz faculdade.

Quando você terminar a faculdade e ver que não consegue um emprego vão te dizer que precisa fazer uma Pós. E lá vai você de novo acreditando na mentira, cursando mais um ou dois anos para descobrir que mais uma vez não será fácil conseguir emprego, apesar da Pós.

Se você gosta de estudar faça como eu. Estude por prazer. Eu só comecei a fazer faculdade depois de estar com minha situação financeira estabelecida. Você não precisa da faculdade para ser quem você quer ser. O que você precisa é do conhecimento hacker, que vai ensinar como invadir computadores, mas vai ensinar também como fazer da sua vida uma vida melhor. Voltaremos a este assunto no **Volume 2** da **Bíblia Hacker**. Agora prepare-se porque sua nova vida como hacker começa agora.

Videoaulas da Bíblia Hacker



A Bíblia Hacker Varredura de portas

Identificando a interface do scanner

 A screenshot of the SuperScan 4 software interface. The window title is 'SuperScan 4 - Found 0 hosts'. The interface includes tabs for 'Scan', 'Host and Service Discovery', 'Scan Options', 'Tools', and 'Windows Enumeration', with 'Scan' selected. There are input fields for 'Start IP', 'End IP', and 'Exclude IP'. A main table area shows network results with three red numbered callouts: '1' points to the 'Start IP' field, '2' points to the 'End IP' field, and '3' points to the table header. At the bottom, there's a 'Ready' status message and a 'View HTML Results' button. To the right of the interface is a small cartoon character wearing a hooded cloak.

www.abibliahacker.com

Prof. Marco Aurelio Thompson

Nós acreditamos que muito do sucesso dos nossos cursos de formação hacker se deve às videoaulas. Uma grande prova disso é que você encontra na Internet videoaulas que foram gravadas em 2003 ou 2005 e que ainda estão ajudando pessoas a se tornar hacker.

Apesar de **A Bíblia** não ser um curso com videoaulas achamos conveniente disponibilizar videoaulas gratuitas para complementar os capítulos. Algumas destas videoaulas você vai encontrar no site **www.abibliahacker.com** e estão disponíveis a todos gratuitamente. Outras videoaulas só vão estar disponíveis para quem comprovar ter adquirido **A Bíblia Hacker** em alguma das lojas autorizadas como o Clube de Autores (www.clubedeautores.com.br) ou na Amazon Brasil (www.amazon.com.br). Informe-se sobre as videoaulas da **Bíblia Hacker** em nosso site, via WhatsApp ou no Facebook:

- **WhatsApp**
- **Página no Facebook**

(71) 9-9130-5874
www.fb.com/abibliahacker



Criando um laboratório de testes

Para ser hacker ou profissional de segurança você vai precisar praticar. Não existe outro caminho. Leia quantos livros quiser. Assista quantas videoaulas quiser. Se não praticar não vai conseguir ser hacker.

Hacker tem mais a ver com fazer do que saber. Você vai se deparar com inúmeros casos em que profissionais de segurança muito bem preparados são vítimas de invasores não tão bem preparados assim.

A prática hacker não deve ser feita em seu computador de uso diário, muito menos no computador da empresa. Tenho relatos de leitores e alunos que decidiram praticar na rede da empresa onde trabalham e por pouco não foram mandados embora por causa disso.

Mexer com material hacker é perigoso. É claro que nada vai explodir ou pegar fogo, mas o risco é de perder informações importantes ou ter as próprias contas invadidas durante algum exercício prático.

Também tenho relatos de leitores e alunos que foram invadidos após começarem a estudar sobre hacking. Só precisei fazer uma pergunta para descobrir que ele (ou ela) decidiu fazer as práticas no computador de uso, ignorando meu aviso. Parecido com o tal do *se beber não dirija*, quando o motorista só acredita na seriedade do aviso após se envolver em acidentes e perder ou tirar vidas.

Se o problema é não praticar no computador de uso e nem no computador da empresa, como fazer? A solução ideal é ter um segundo e até um terceiro computador só para praticar. Um computador fazendo o papel de invasor e um outro de vítima.

Esta solução ideal se mostra inadequada porque além do custo de ter mais dois computadores temos também a questão do espaço. Alguns leitores e alunos relataram que ressuscitaram um computador velho só para praticar. Outros adquiriram computadores mais antigos, tipo o Pentium IV, pagando menos de duzentos reais pelo equipamento.

E você que talvez não queira ou não possa comprar outro computador? Ou que não tem espaço para mais um micro e precisa praticar se quiser ser hacker? Para estes casos a solução ideal é o uso de máquinas virtuais para criar laboratórios de teste. A máquina virtual é um programa de computador capaz de virtualizar um ou mais computador isolando um do outro.

E o melhor é que não vai lhe custar nada, caso o seu computador tenha o mínimo de recursos, tais como:

- Processador acima de 1GHz, o ideal é ter acima de 2GHz.
- No mínimo 2 GB de memória RAM, o ideal é ter 4GB ou mais.
- Pelo menos 40GB de espaço livre no disco rígido, o ideal é ter 100GB.
- A placa de vídeo preferencialmente deve ser do tipo *off-board*, que é quando a placa de vídeo é independente da placa mãe. Mesmo que seu computador tenha a placa de vídeo *on-board* dá para usar.

Se for um notebook é preciso verificar se ele atende aos requisitos mínimos. Os modelos mais baratos de notebook têm pouca memória RAM, processador lento, pouco espaço livre no disco rígido e a placa de vídeo é compartilhada. Netbook? Nem pensar. No máximo para rodar algumas ferramentas e programas.

O laboratório de testes consiste em no mínimo dois computadores. Um como invasor e outro como cobaia. Este invasor pode muito bem ter instalado o Windows XP, se você estiver começando e não conhece o Linux. Sugerimos que você crie também um segundo invasor rodando Linux, como o Kali (sucessor do Backtrack) ou outro Linux qualquer.

Assim você pode aprender com mais facilidade usando o Windows com o qual está mais familiarizado, enquanto aprende a usar o Linux para invasão, que é o sistema operacional que oferece mais recursos e ferramentas hacker.

Você talvez se pergunte porque sugerimos o Windows XP já que atualmente a versão mais recente do Windows é o Windows 10. O que você precisa ter em mente é o seguinte. Um bom invasor consegue resultados com qualquer versão do Windows. Nossa sugestão para usar o Windows XP é que ele ocupa pouco espaço e a maioria das ferramentas hacker foram feitas para ele.

Não pense que os programadores hacker saem convertendo suas ferramentas para a versão mais recente do Windows assim que sabem do lançamento. Na verdade, os hackers que usam Windows até preferem o Windows XP porque é um Windows que quase não interfere no funcionamento das ferramentas de segurança.

O novíssimo Windows 10 S, voltado para estudantes, não permite sequer usar o Google como sistema de buscas e nem instalar o navegador Firefox, um navegador repleto de recursos para hackers. Só pensa em usar o Windows mais recente como máquina do invasor quem não está o suficientemente informado de como as coisas realmente funcionam.

Além das duas máquinas virtuais para fazer o papel de invasor – uma com Windows e outra com Linux – sugerimos a criação de pelo menos duas máquinas para o papel de alvo, vítima ou cobaia. Uma cobaia terá instalado o Windows para desktop, podendo ser qualquer um entre o Windows XP e o Windows 10.

A outra cobaia terá instalado um Windows para servidores, podendo ser qualquer um entre o Windows Server 2003 ao novíssimo Windows Server 2016, sobre o qual escrevi um livro lançado pela editora Érica-Saraiva. A propósito, este nosso livro sobre o Windows Server 2016 é o primeiro no mundo em língua portuguesa.

Ajude-me a escolher

Com tantas opções de sistemas operacionais é comum o leitor ou estudante ficar em dúvida sobre qual Sistema Operacional (SO) instalar na máquina **Invasor** e qual SO instalar na máquina **Cobaia**, a que fará o papel de vítima.

Nós já sugerimos um invasor rodando o Windows XP e outro rodando o Linux Kali, que é o sucessor do Backtrack, o Linux hacker. Se você não se sentir

confortável com o Windows XP ou achar que é um SO ultrapassado, instale outro como o Windows 8 ou o Windows 10 por exemplo. A escolha é sua, apenas fazemos sugestões.

Quanto às cobaias, ter uma rodando o Windows 10 e outra rodando o Windows Server 2003 nos parece a configuração ideal para quem está começando. Você talvez pense que o Windows Server 2003 é um SO muito antigo e ultrapassado. O fato é que o Windows Server 2003 ainda é bastante usado, mas você pode criar cobaias com outros servidores como o Windows Server 2008, 2012 e até o novíssimo Windows Server 2016. Ou caso tenha em mente atacar servidores Linux, pense em uma cobaia rodando algum tipo de Linux Server como o Debian, Red Hat ou SuSE por exemplo.

Ainda está em dúvida? Instale:

- INVASOR_01 – Windows XP ou Windows 7
- INVASOR_02 – Linux Kali
- VITIMA_01 – Windows 7 ou Windows 10
- VITIMA_02 – Windows Server 2003

Máquina Virtual: Visão Geral

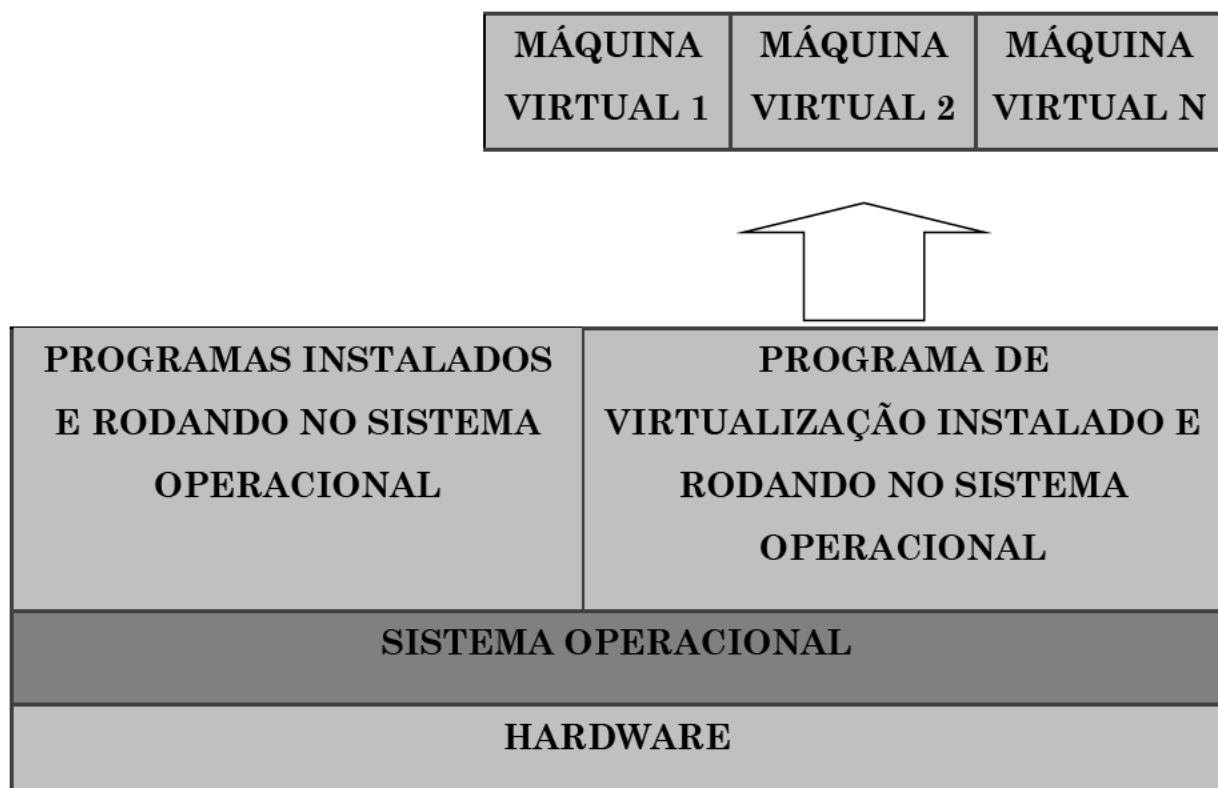
Máquina virtual é um programa de computador que reproduz em memória o hardware de um computador real. Se você parar para pensar vai perceber que todos os recursos necessários ao funcionamento do computador executam em memória. Inclusive o sistema operacional e os drivers de dispositivos, necessários para o sistema operacional reconhecer o hardware.

De uns tempos para cá os preços do disco rígido e da memória do tipo RAM reduziram drasticamente. As pessoas têm acesso a baixo custo, a muito espaço em disco, processadores muito melhores, de núcleo duplo ou quádruplo, e a muita memória RAM.

Não demorou para a supercapacidade dos PCs popularizarem os programas de virtualização. Programas que reproduzem em memória, o hardware necessário para um computador funcionar. É como se você tivesse um computador dentro do outro. Um só não, quantos o processador, a memória RAM e o espaço livre no disco rígido da máquina real permitirem.

Para as empresas a virtualização também ajudou a reduzir o espaço necessário para armazenamento de vários servidores. No lugar de dez ou vinte CPUs para a mesma quantidade de servidores é possível ter apenas duas ou quatro CPUs para os mesmos vinte servidores.

O diagrama abaixo demonstra o funcionamento da máquina virtual. Ela é instalada como um aplicativo comum dentro do sistema operacional e consegue gerenciar várias máquinas virtuais com sistemas operacionais independentes, limitado apenas pela capacidade da máquina real: processamento, espaço livre no disco rígido e quantidade de memória RAM.



Escolhendo o software de virtualização: Oracle VM Virtual Box

O Oracle VM VirtualBox é um software de virtualização desenvolvido pela Oracle. Ele permite a instalação e utilização de um sistema operacional dentro de outro, compartilhando fisicamente o mesmo hardware.

O VirtualBox está disponível gratuitamente como software de código aberto sob os termos da GNU General Public License (GPL). Atualmente, o VirtualBox roda em Windows, Linux, Macintosh e OpenSolaris e suporta um grande número de sistemas operacionais convidados, incluindo, mas não limitado ao Windows (NT 4.0, 2000, XP, Vista, 7, 8, 8.1, 10, Server 2003, Server 2008, Server 2012, Server 2016), MS-DOS, Linux, Solaris e OpenBSD.

Criando um laboratório virtual usando o VirtualBox

É preciso lembrar que cada máquina virtual compartilha recursos da máquina real. Vamos supor que você tenha um computador com o Windows 10 instalado, 4 GB de memória RAM e 400 GB de espaço livre no disco rígido.

Ao criar duas máquinas virtuais, cada uma configurada para 1 GB de memória RAM e 100 GB de disco rígido virtual, vai deixar a máquina real com apenas 2 GB de memória RAM e 200 GB de espaço livre no disco rígido.

Por outro lado, a(s) máquina(s) virtual(is) só consome(m) recursos enquanto ativa(s) e os discos rígidos virtuais podem ter um tamanho estabelecido, mas só ocupam o espaço que realmente estiver em uso.

Desta forma podemos ter N máquinas virtuais criadas desde que o total da soma de recursos da máquina real e da(s) virtual(is) (em uso) não ultrapasse a capacidade do hardware da máquina real.

O ideal para o laboratório é um processador recente com 4 a 8 GB de RAM e mais de 100GB de espaço livre no disco rígido. Esta configuração será suficiente para trabalhar com duas máquinas virtuais ativas sem comprometer a performance da máquina real.

Para o que pretendemos, que é criar um laboratório simples para a prática hacker, o VirtualBox mostrou-se uma opção bastante viável: por ser gratuito (licença GPL), por rodar até no Windows 7 e por hospedar o Windows Server 2016.

O primeiro passo é fazer o download do VirtualBox, em:

- <https://www.virtualbox.org/wiki/Downloads>

No mesmo link também faça o download do arquivo VirtualBox Extension Pack para incluir melhorias no VirtualBox após instalado, incluindo suporte ao USB 3.0.

Enquanto aguarda o download sugerimos a leitura da licença de uso, principalmente a parte que diz que a gratuidade do VirtualBox se limita ao uso pessoal ou para avaliação:

- http://www.virtualbox.org/wiki/VirtualBox_PUEL

O documento está em inglês, mas é possível traduzi-lo usando a ferramenta de tradução do Google ou alguma outra de sua preferência.

Se você por acaso já possui o VirtualBox instalado, verifique se a versão dá suporte à instalação do Windows Server 2016. Apenas as versões mais recentes dão suporte à instalação do Windows server 2016 e ao Windows 10, que vamos precisar para algumas demonstrações.

O próximo passo é fazer a instalação do VirtualBox, um procedimento simples que consistem basicamente em clicar em **Avançar** até o final da instalação. A interface do instalador está em inglês, mas não se preocupe que vamos ajudá-lo passo-a-passo:

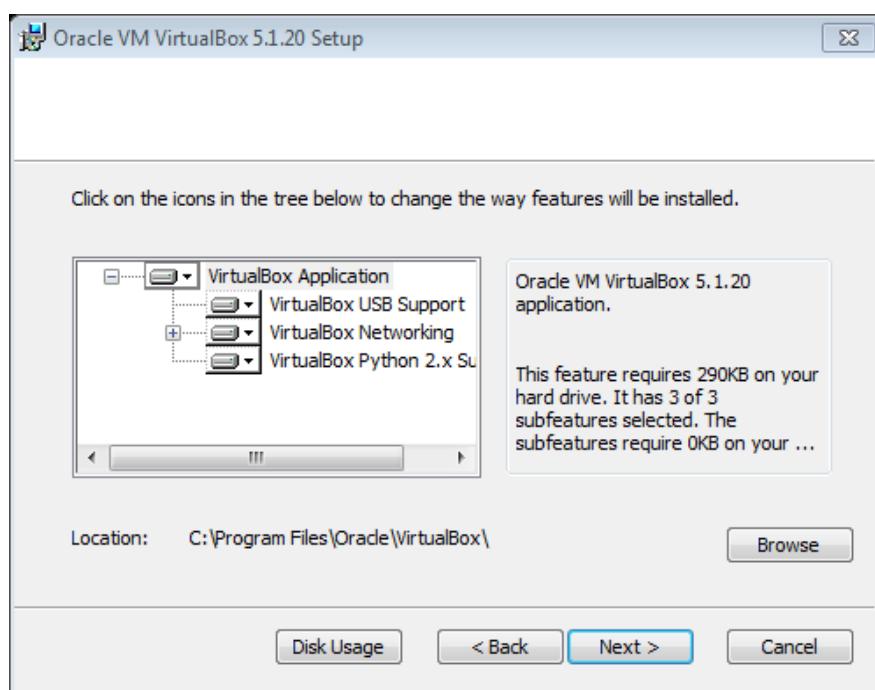
Tela inicial de Boas-vindas Do instalador. Basta clicar em **Next** (Próximo) para prosseguir.

Tela de Boas-vindas do VirtualBox.



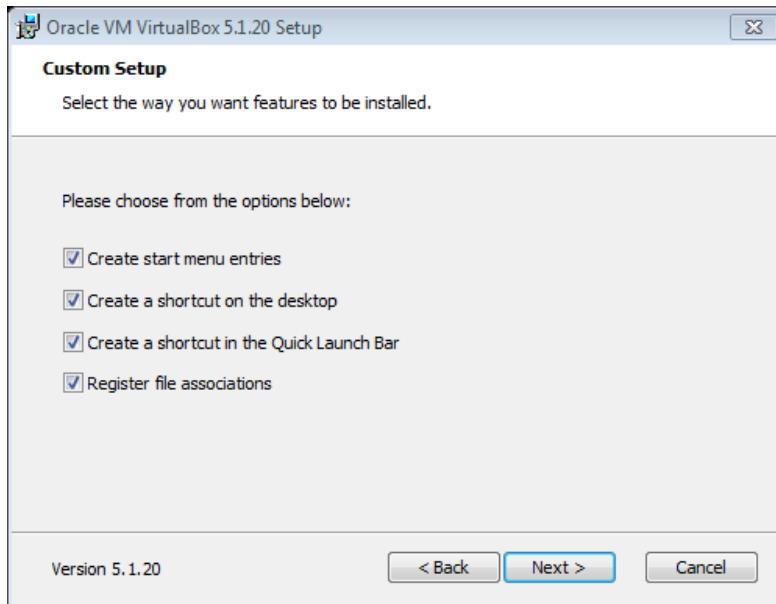
Na próxima tela você pode selecionar o local da instalação do VirtualBox clicando em **Browse**, ou apenas deixe como está e clique em **Next**:

Tela para selecionar outro caminho para a instalação, se quiser.



O instalador criará atalhos no sistema:

Informação sobre a criação de atalhos após a instalação.



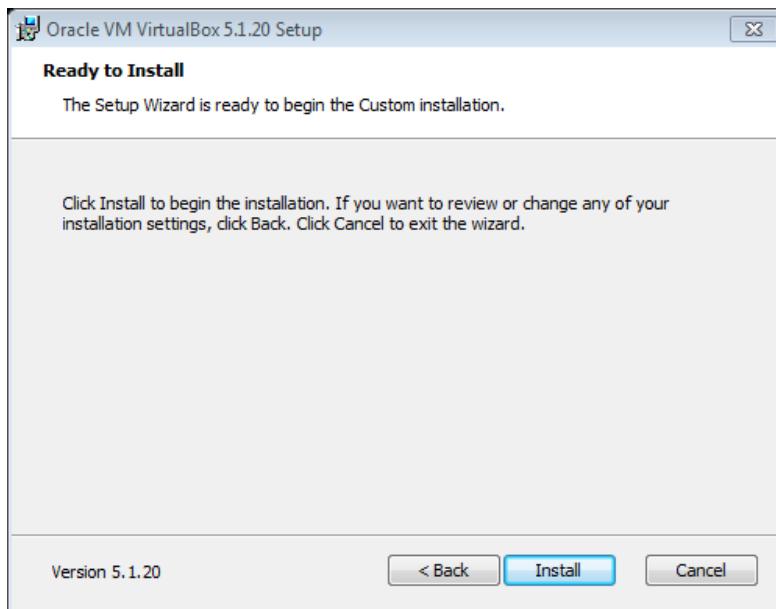
A próxima tela é uma tela de advertência. Como serão instalados drivers para a interface de rede virtual, as conexões de rede serão desligadas temporariamente. Se você estiver fazendo algum download recomendamos aguardar a conclusão, pois pode ocorrer perda momentânea da conexão.

Tela advertindo sobre perda da conexão com a Internet, se prosseguir.



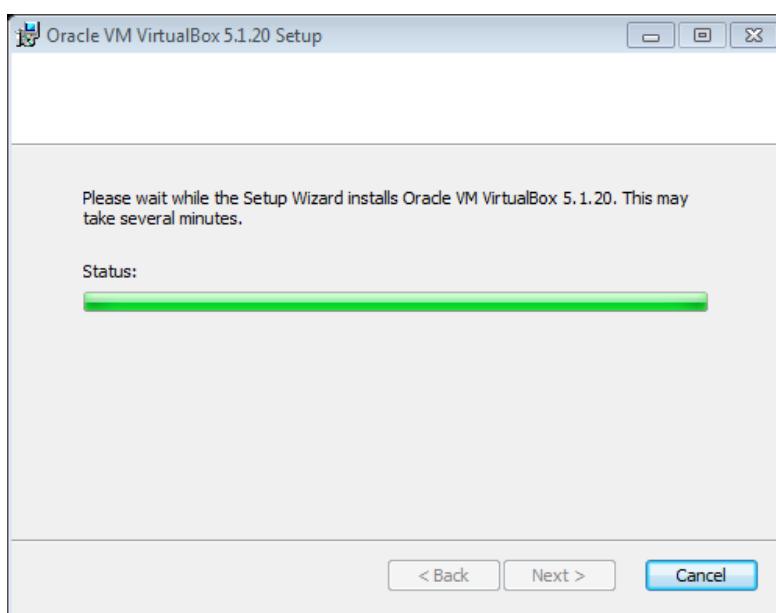
Após as seleções iniciais o instalador está pronto para começar. Clique em **Install** para prosseguir.

Tela que dará início a instalação.



Após clicar em **Install** a instalação tem início com a cópia de arquivos para o disco rígido e as devidas configurações iniciais, de acordo com as seleções realizadas nas telas anteriores:

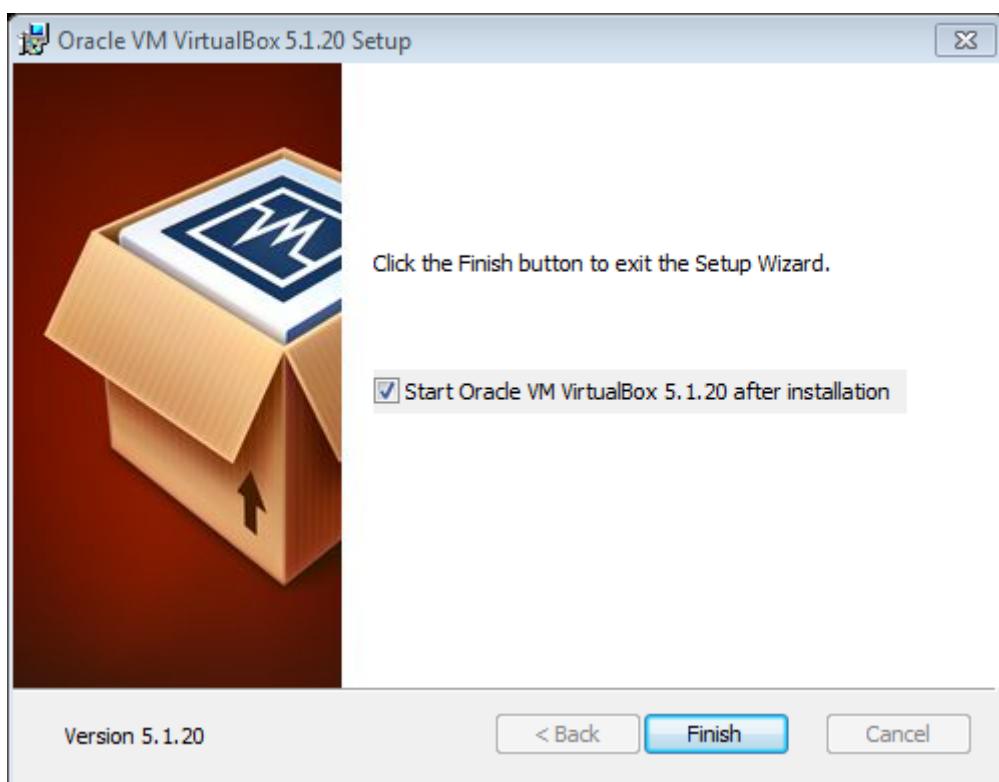
Tela informando o andamento do processo de instalação.



Em poucos minutos a instalação chegará ao fim e ao clicar em **Finish** o Oracle VM VirtualBox será iniciado.

É importante você saber que a instalação do VirtualBox apenas cria as condições para a instalação de outros sistemas operacionais. A instalação destes outros sistemas operacionais deverá ser feita por você, usando o DVD ou a imagem (ISO) do arquivo de instalação de cada SO desejado.

Tela informando o final da instalação.

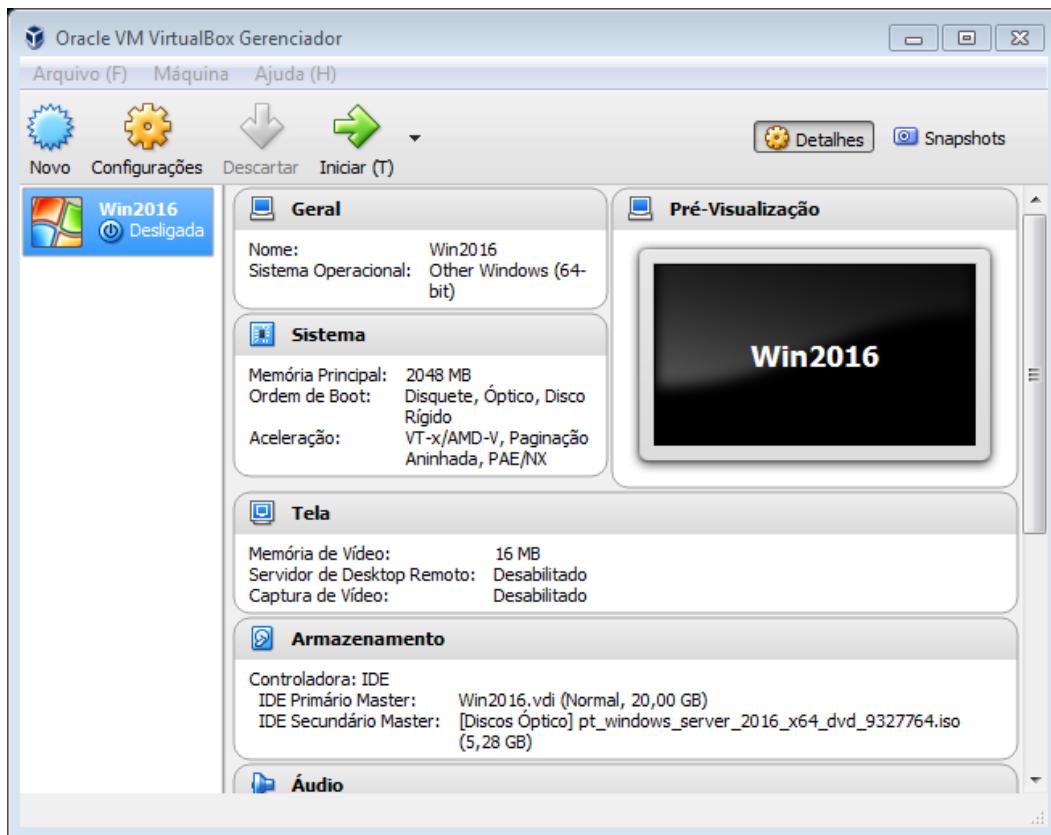


Conforme antecipamos mesmo que as telas do instalador estejam em inglês, ao executar o VirtualBox o programa reconhece o idioma do sistema operacional e a interface do usuário deverá estar em português, como aparece na próxima figura.

Caso não ocorra a tradução automática para o português, altere o idioma acessando o menu:

Arquivo (File) -> Preferências (Preferences) -> Idioma (Language)

Tela inicial do Oracle VM VirtualBox exibindo o Windows Server 2016 que foi instalado previamente:



Entendendo o Oracle VM VirtualBox

Observe na figura acima que já estamos com uma máquina virtual criada.

Observe que a barra de menus do Virtual Box tem somente três opções:

- **Arquivo**, que também pode ser acessado pela combinação de teclas **ALT + F**.
- **Máquina**, que também pode ser acessado pela combinação de teclas **ALT + M**.
- **Ajuda**, que também pode ser acessado pela combinação de teclas **ALT + H**.

Em **Arquivo** temos as seguintes opções:

- **Preferências** - em preferências é possível definir a localização da pasta padrão para os discos e máquinas virtuais, a frequência de verificação de atualizações para o VirtualBox, a seleção do idioma e gerenciar a interface de rede. É possível ter mais de uma interface de rede virtual. Inicialmente deixe tudo do jeito que está.
- **Importar Appliance/Exportar Appliance** - Appliance são máquinas virtuais prontas que podem ser importadas e exportadas. Não usaremos este recurso.
- **Gerenciador de Mídias Virtuais** - serve para você criar discos virtuais, trabalhar com imagens de disco do tipo ISO e também para criar drives de disquete virtuais. Sua máquina virtual pode ter mais de um disco virtual e isto será útil para a prática do uso de discos em RAID. O disco virtual já é criado no processo de criação da máquina virtual, então esta opção só é útil quando queremos manusear discos virtuais adicionais ou para gerenciá-los.
- **Gerenciador de Operações de Rede** – caso existam operações de rede ativas poderão ser gerenciadas aqui.
- **Verificar por atualizações** – verifica se a versão instalada do VirtualBox é a mais recente. O programa já faz isto por padrão.
- **Redefinir todos os avisos**.
- **Sair**.

Em **Máquina** temos as seguintes opções:

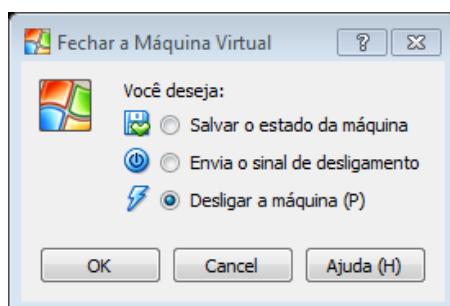
- **Novo** – abre o assistente de criação de máquinas virtuais. Deve ser executado uma vez para cada máquina virtual a ser criada. Em nosso laboratório vamos executá-lo no mínimo duas vezes, uma para o **Invasor** e outro para a **Cobaia**.
- **Acrescentar** - permite acrescentar máquinas virtuais anteriormente criadas ou clonadas.

- **Configurações** - esta opção aparece após ser criada pelo menos uma máquina virtual. Permite fazer o ajuste fino da configuração padrão obtida com o assistente. Isto inclui:
 - Ajustar a interação entre a máquina virtual (hóspede) e a real (hospedeira)
 - Definir o número de processadores. Para o Windows Server 2016 recomendamos dois processadores virtuais.
 - Alterar a sequência de boot. Para instalar o Windows Server 2016 a partir de um leitor de DVD a sequência de boot precisa incluir o leitor de DVD no início.
 - Definir quanta memória vai ser disponibilizada para a placa de vídeo virtual e se haverá aceleração 2D e 3D.
 - Configuração da administração remota.
 - Configuração das opções de armazenamento e do áudio.
 - A configuração da rede é um ponto importante, pois permite trabalhar em diferentes modos: não conectado, NAT, modo bridge, etc. Também permite configurar mais de uma placa de rede, recurso muito útil em nosso laboratório.
 - Habilitar e desabilitar portas seriais e USB
- **Clonar** – permite criar uma cópia exata de qualquer máquina virtual disponível. É uma função útil para você praticar com o Windows Server 2016 porque você pode criar uma instalação inicial, fazer a clonagem e recuperar esta instalação limpa sempre que quiser usando a opção **Aumentar**.
- **Remover** – remove a máquina virtual selecionada. Você pode optar entre apenas remover da lista de máquinas virtuais ou remover também os arquivos da máquina virtual.
- **Grupo** – permite criar grupos para suas máquinas virtuais. Você pode criar um grupo intitulado Museu Virtual do Windows e criar

uma máquina virtual para cada versão do Windows. Pode criar um grupo com o nome BibliaHacker para as máquinas virtuais que irá usar com este livro. Um grupo Linux só para máquinas virtuais Linux e assim por diante. É uma forma de organizar melhor o ambiente quando temos muitas máquinas virtuais criadas.

- **Iniciar** - tem o mesmo efeito de ligar do computador real. Lembre-se que o fato de termos criado uma máquina virtual para o Windows Server 2016 não significa que ele já está instalado.
- **Pausar** - a máquina virtual em uso pode ser pausada e retomada a qualquer momento. Isto quer dizer que você não precisa encerrar o sistema operacional instalado na máquina virtual. Pode pausá-lo e voltar ao ponto em que parou, como se fosse uma ação de congelar e descongelar. Este procedimento é útil quando você está fazendo alguma coisa no sistema virtual, precisa interromper o que está fazendo e só vai retornar muito mais tarde ou nos dias seguintes. É só congelar a máquina virtual e retomar de onde parou.
- **Reinicializar**
- **Fechar** – oferece as opções **Salvar o estado da máquina** (congelar), **Enviar o sinal de desligamento** (caso não tenha encerrado o sistema operacional) e **Desligar a máquina** (tem o mesmo efeito de desconectar o computador da tomada). Só use a opção **Desligar a máquina** em caso de travamento ou se já tiver encerrado o sistema operacional normalmente.

Opções do Fechar a Máquina Virtual.



- **Descartar o Estado Salvo**
- **Exibir Log...** - exibe informações sobre mudanças, mensagens e tudo o mais que interessa saber para acompanhar o funcionamento e uso da máquina virtual.
- **Atualizar** - atualiza o sistema, incluindo eventuais novas configurações.
- **Exibir no Explorer** – exibe os arquivos da máquina virtual no Windows Explorer.
- **Criar atalho na Área de Trabalho**
- **Organizar** – útil quando temos muitas máquinas virtuais criadas e precisamos ordená-las. Para poucas máquinas virtuais criadas esta função praticamente não tem uso.

A opção **Ajuda** dispensa comentários, mas é bom você saber que a ajuda é dada em inglês, independentemente de a interface do programa estar em português ou outro idioma.

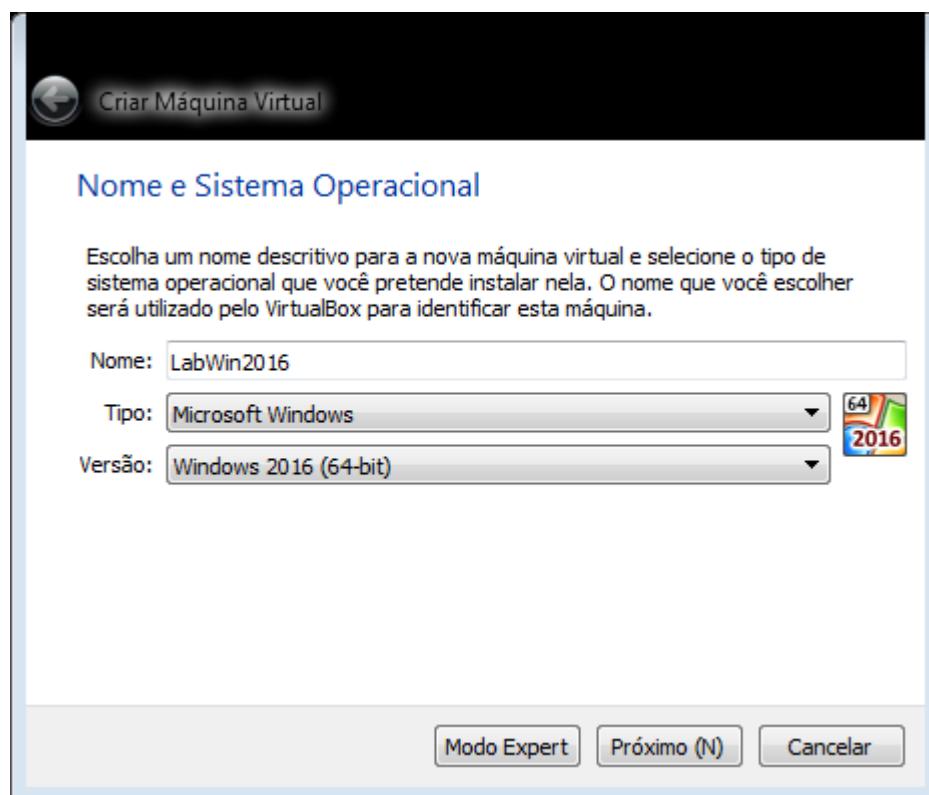
Criando a máquina virtual para instalar o Windows

O primeiro passo é entrar na opção **Máquina** da barra de menus e clicar em **Novo**. Você também pode clicar direto sobre o botão **Novo** ou usar a combinação de teclas **Ctrl + N**, opte pelo que for mais prático. Como você já deve saber as opções dos programas Windows costumam aceitar diferentes formas de acesso e o fato de a interface estar em português vai facilitar bastante.

Na figura abaixo vemos as possibilidades de sistemas que podem ser instalados, entre eles o Windows Server 2016 que deve ser a nossa opção. Para prosseguir é preciso dar um nome a máquina virtual. Em nosso exemplo usamos o nome LabWin2016.

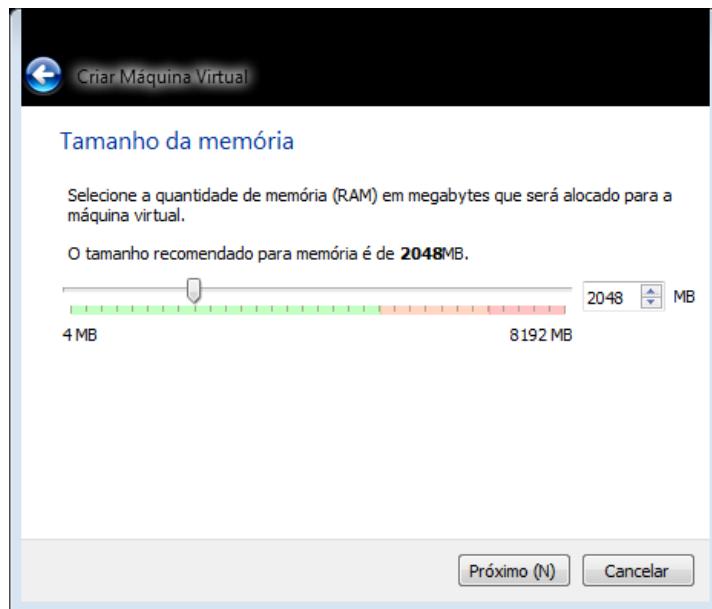
Escolha o sistema operacional a ser instalado e não esqueça de dar um nome para a máquina virtual. Se entre os sistemas operacionais suportados não aparecer o Windows 10 e nem o Windows Server 2016, provavelmente a versão do VirtualBox instalada é antiga. Basta atualizá-la ou usar a opção genérica: **Other Windows (64-bit)**.

Selecionando um modelo de sistema operacional para ser instalado.



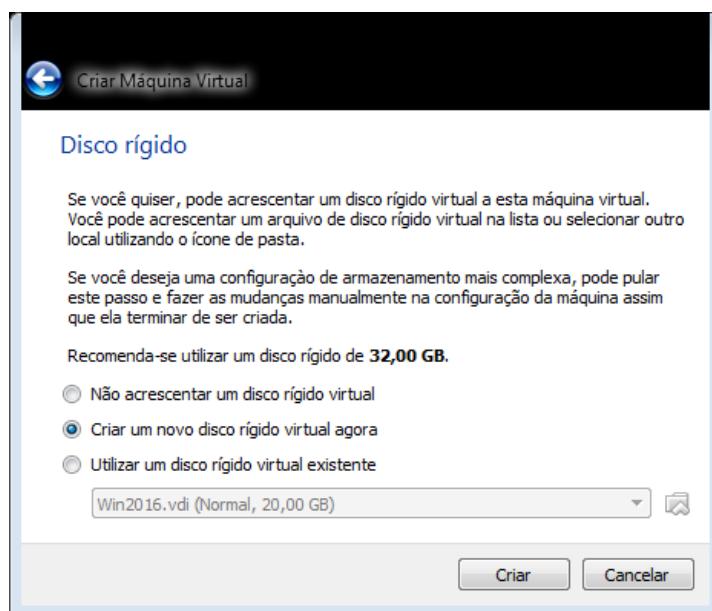
O próximo passo é definir quanto de memória RAM você pretende destinar ao uso pela máquina virtual. Esta RAM virtual depende de quanta memória RAM existe na máquina real. Recomendamos 2 GB de RAM para a máquina virtual que vai receber a instalação do Windows Server 2016. Para dispor de 2 GB de RAM você precisa ter no mínimo 4 GB de RAM na máquina real.

Selecionando a memória para o Windows Server 2016: mínimo 2GB.



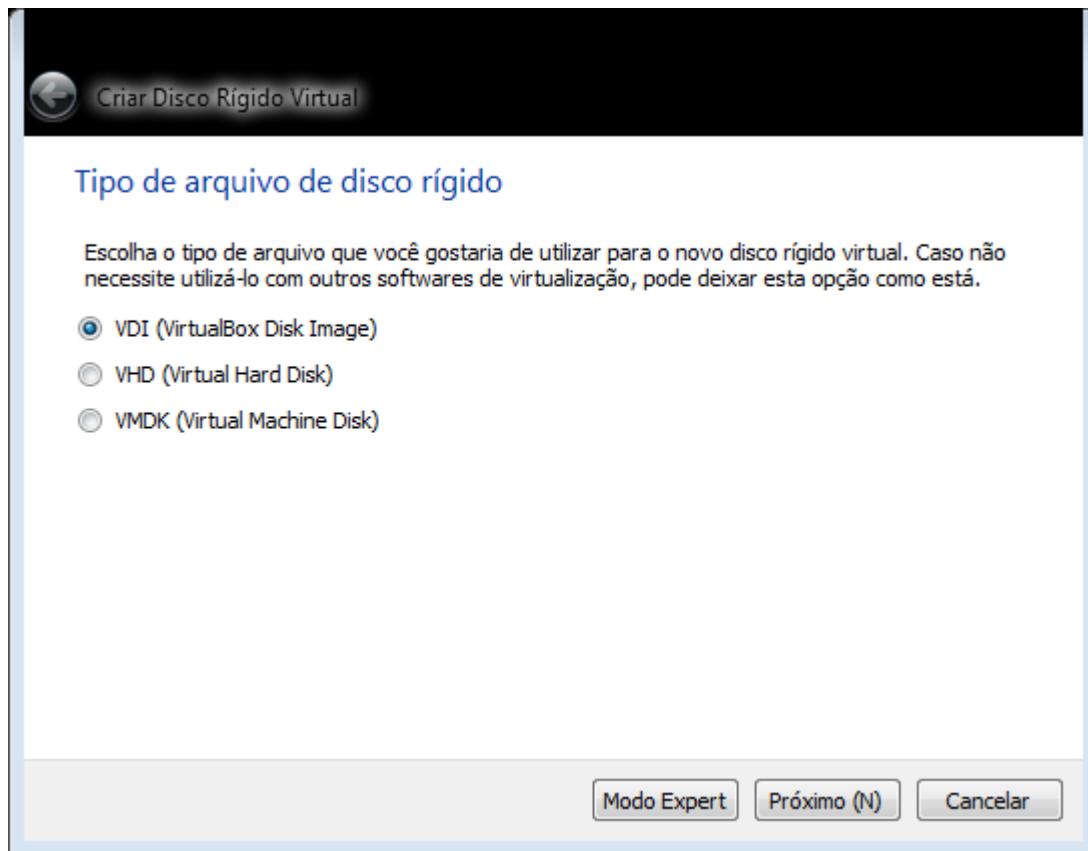
O próximo passo é criar o disco rígido virtual, que tanto pode ser criado antecipadamente usando o gerenciador de discos a partir do menu **Arquivo**, como pode ser criado junto com a criação da máquina virtual, que é a opção usada neste exemplo. O espaço para o disco rígido virtual precisa existir na forma de espaço livre no disco da máquina real. Para este exemplo estamos criando um disco virtual de 40GB, apesar da sugestão ser de 32GB.

Opções para o disco rígido virtual.



As opções de disco virtual incluem os sistemas mais utilizados para que você possa, inclusive, criar discos virtuais compatíveis com outros programas de virtualização.

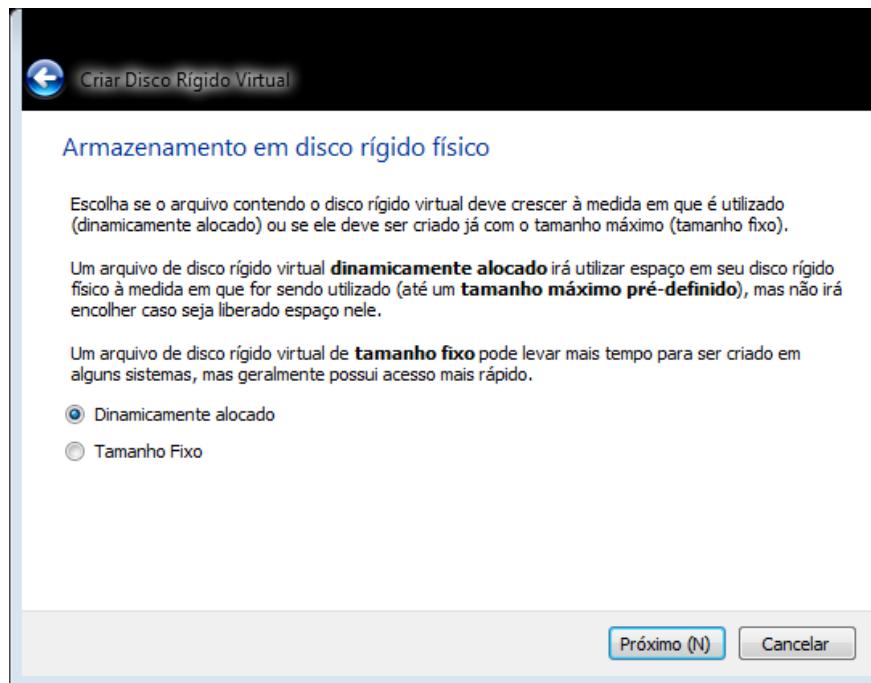
Opções para o tipo de arquivo de disco rígido virtual.



Na opção **Dinamicamente alocado** o disco rígido virtual só ocupará o espaço realmente necessário, não o tamanho total com que foi criado. Na medida em que for sendo preenchido com arquivos e dados, o arquivo do disco virtual aumentará de tamanho até o limite estipulado.

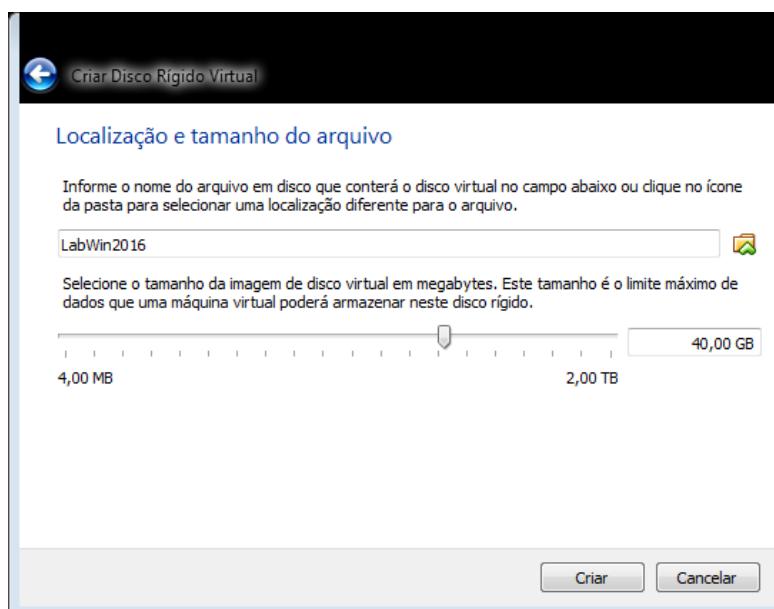
Na opção **Tamanho fixo** será criado um arquivo com o tamanho total do disco virtual que é de 40GB em nosso exemplo.

Decida entre criar o disco virtual ocupando desde já o tamanho previsto ou deixar que o arquivo cresça conforme o uso.



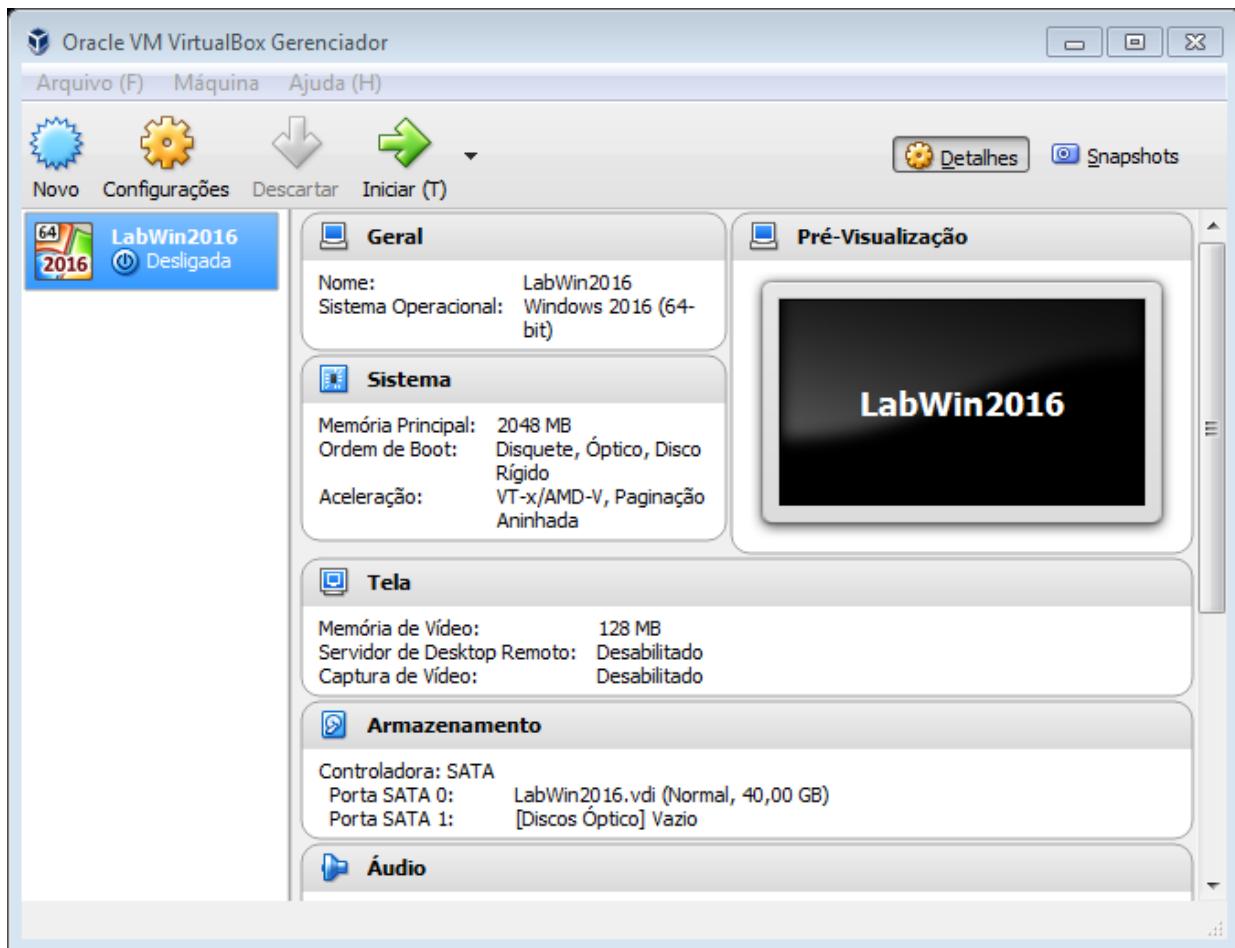
Aqui determinamos o tamanho máximo para o disco rígido virtual, modificamos a pasta de armazenamento se isto nos interessar e também podemos alterar o nome do disco virtual que, por padrão, é o mesmo nome dado à máquina virtual.

Definindo a localização e o tamanho do arquivo de disco virtual.



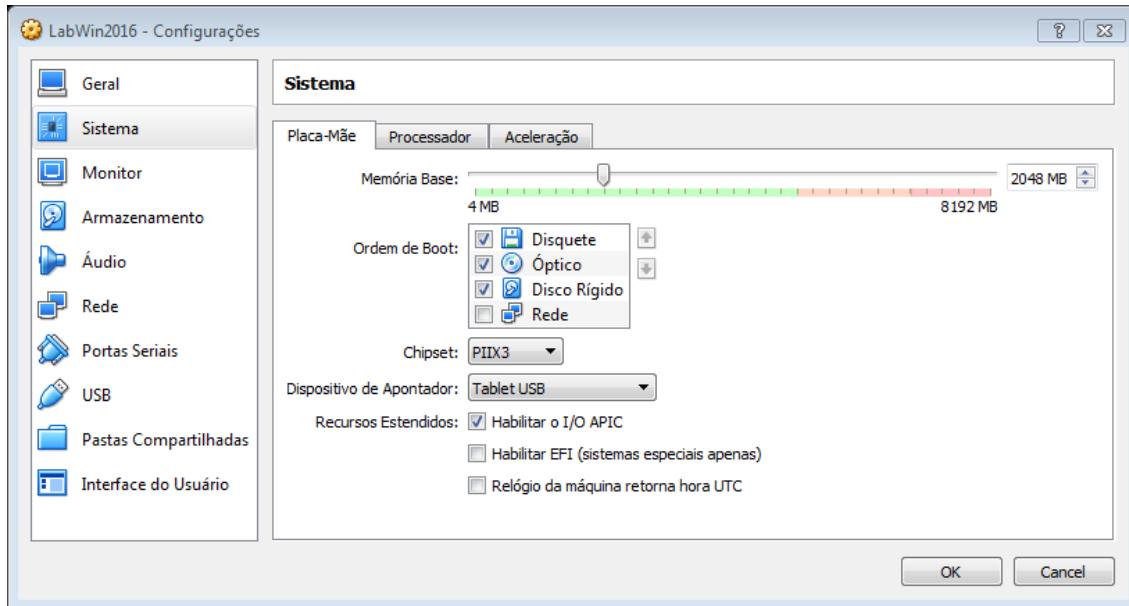
A máquina virtual criada passa a ser exibida na lista de máquinas virtuais, na coluna da esquerda do VirtualBox.

À esquerda a lista de máquinas já virtuais criadas.



Clicando no botão **Configurações** você pode fazer ajustes na máquina virtual como por exemplo, aumentar a memória RAM virtual, habilitar um segundo adaptador de rede, desabilitar o driver de disquete que é obsoleto e desnecessário, associar um segundo disco rígido virtual, que deve ser antecipadamente criado na opção **Arquivo -> Gerenciador de Mídias Virtuais**.

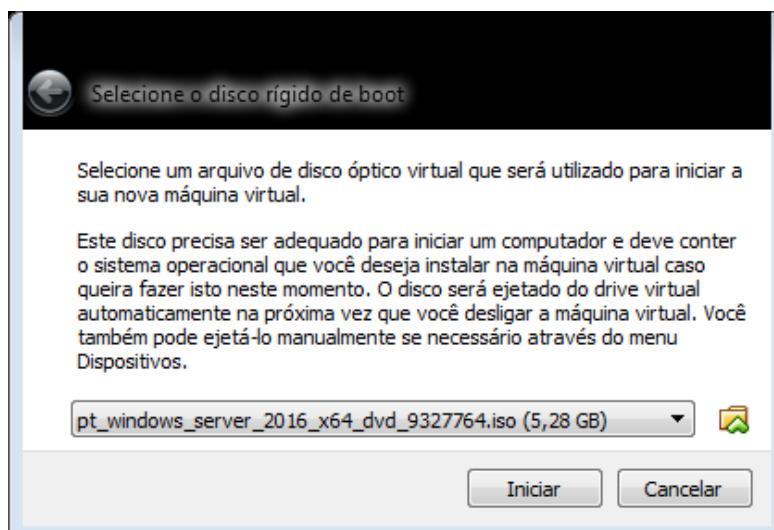
Em **Configurações** podemos modificar ou acrescentar hardware virtual.



O primeiro boot na máquina virtual

O primeiro boot corresponde a ligar um computador novo e isto é feito clicando em **Iniciar**. Para ajudá-lo ainda mais o VirtualBox detecta o primeiro uso e inicia mais um assistente para guiá-lo neste processo:

Inicialmente informe a letra da unidade de disco real que vai usar para instalar o Windows Server 2016. Você pode inserir o DVD com o Windows Server 2016 ou indicar a pasta onde salvou a imagem do tipo ISO baixada do site da Microsoft, que é a opção que aparece na figura abaixo.



Neste exemplo usamos o Windows Server 2016 instalado a partir de uma imagem de disco (ISO) baixada do site da Microsoft:

Para instalar outros sistemas operacionais é só você clicar na pasta amarela e localizar a imagem de disco (ISO) ou a unidade de disco com o DVD de instalação, seja do Windows ou Linux, o que preferir. Ainda neste Volume da Bíblia Hacker vamos demonstrar a instalação e uso do Linux Kali, o Linux hacker. Sobre a instalação e uso dos servidores Windows daremos mais informações em outros Volumes e capítulos da Bíblia Hacker.

Para cada SO instalado como Invasor ou Cobaia a operação de instalação do SO deverá ser repetida. E como já me perguntaram algumas vezes, apesar de parecer óbvio, não custa responder. O VirtualBox você instala uma vez só. Dentro do VirtualBox é que você instala um por um, cada sistema operacional. A partir do DVD ou imagem de disco. Se quiser ter duas máquinas Invasor e duas máquinas Cobaia, terá de fazer quatro instalações de sistemas operacionais, duas de cada.

Só não esqueça que a soma dos recursos das máquinas ativas e da máquina real não pode superar os recursos totais da máquina real. Temos uma videoaula demonstrando isto. Informe-se sobre como obtê-la entrando em contato conosco.





O segredo dos hackers: Portas, IPs e Vulnerabilidades

Se eu tivesse alguns minutos de vida e alguém me perguntasse como últimas palavras se eu poderia sintetizar o conhecimento hacker, eu diria que tudo se resume a portas, IPs e vulnerabilidades.

Isto quer dizer que qualquer um pode se tornar hacker se souber identificar e trabalhar com portas, IPs e vulnerabilidades.

O IP nos dá um endereço, a porta nos diz por onde entrar e a vulnerabilidade nos diz o ponto fraco que pode ser explorado.

Fazendo uma analogia com a invasão de uma casa, o IP equivale ao nome da rua, número, bairro, cidade ou coordenada do GPS. O IP nos diz onde está o computador a ser invadido.

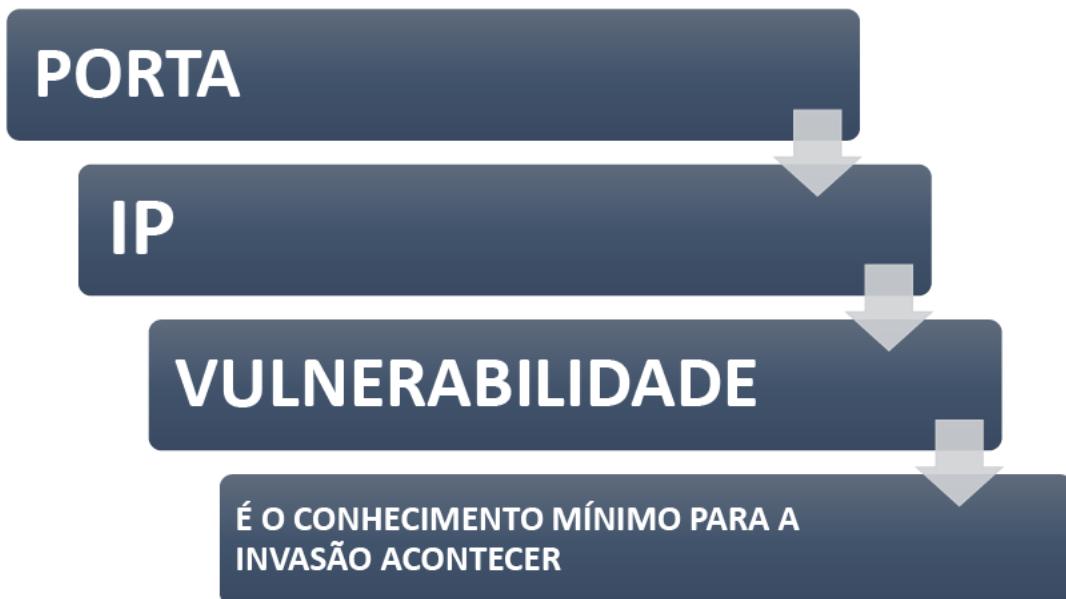
A porta tanto pode ser a porta da frente, a de trás, como também pode ser a janela, o basculante, o buraco do ar condicionado, a claraboia, até uma parede frágil, como por exemplo, o tijolo sem revestimento, paredes de

madeira ou o Dry-wall¹, tão popular nos Estados Unidos e até coberturas de telha. A porta é um local de passagem. Pode estar aberto ou ser uma passagem forçada. Esta analogia se aplica a um prédio ou computador e é importante que você compreenda, porque o computador pode ter portas abertas, mas às vezes você é quem vai abrir as portas para a invasão.

E finalmente chegamos a vulnerabilidade, que pode ser entendida como ponto fraco. Se existe um alarme na porta da frente a mais vulnerável é a porta de trás. Se a porta da frente usa fechadura do tipo tetra, muito mais difícil de abrir usando michas², a vulnerabilidade está na janela ou na porta de trás, que geralmente usa fechaduras mais fracas.

A propósito, qualquer porta que só tenha fechadura ou cadeado é vulnerável. Qualquer chaveiro - ou invasor com o mesmo conhecimento – abre.

A fechadura das portas no computador é o firewall, mas nem sempre é o suficiente, como podemos comprovar através dos inúmeros casos de invasão noticiados a cada dia.



¹ Paredes construídas com gesso acartonado impermeável.

² A chave micha nada mais é que uma chave comum onde todos os cortes estão em seu máximo e assim permitem abrir várias fechaduras e cadeados, como se fosse uma chave mestra.

Começando neste e prosseguindo por mais alguns capítulos nos próximos volumes da **Bíblia Hacker**, vamos apresentar de forma fácil de entender e com muita prática, tudo o que você precisa saber sobre portas, IPs e vulnerabilidades: o segredo dos hackers.

Pense na porta como se fosse a porta da sua casa. Qual a serventia? É por onde entra e sai tudo o que puder entrar e sair, incluindo os moradores, parentes e visitantes, mas também a polícia - quando for o caso - e eventualmente algum animal ou bandido.

Nas empresas e repartições públicas a forma usada para controlar o acesso é usando um segurança, porteiro, catracas. No computador quem faz isto é o firewall. O antivírus serve para verificar se alguém está entrando com alguma coisa perigosa, como armamento ou explosivo. Um papel que seria da máquina de raios X ou do detector de metais.

Se as portas da casa ficarem escancaradas há chance de entrar algum invasor. E existem bairros em que a segurança precisa ser maior do que a de outros, como usar grades e fechaduras reforçadas por exemplo. Uma casa em condomínio fechado ou apartamento tem a vantagem de contar com a segurança do perímetro. O invasor precisa passar por uma primeira barreira antes de chegar até você. Infelizmente isto não tem impedido furtos, roubos e invasões em condomínios e prédios.

Pessoas famosas com recursos financeiros, como o comediante Renato Aragão³ e o – na época – casal de apresentadores do Jornal da Globo, William Bonner e Fátima Bernardes⁴, tiveram suas luxuosas e protegidas residências invadidas por assaltantes. Ninguém está seguro.

A mesma coisa vai ocorrer com as portas dos computadores. Se forem deixadas escancaradas serão invadidas. Tem bairros, ou melhor, redes que

³ <http://g1.globo.com/rio-de-janeiro/noticia/2011/10/casa-de-renato-aragao-no-rio-e-invadida-diz-pm.html>

⁴ <http://www1.folha.uol.com.br/folha/cotidiano/ult95u104989.shtml>

são menos seguras e vão exigir mais segurança. Tem computadores que estão protegidos por redes com servidores que funcionam como uma primeira barreira de segurança, mas ainda assim correm riscos. E tem os computadores e redes que pensamos estar muito bem protegidos até vir um invasor e provar que não.

De forma fácil para você entender vamos explicar portas em cinco blocos:

1. O que passa pelas portas?
2. Como as portas são acessadas?
3. Quais portas existem?
4. Como são identificadas?
5. Como proteger as portas?

O que passa pelas portas?

Tudo o que chega até as portas do computador são sinais elétricos. Estes sinais foram gerados em algum lugar e transmitidos até chegar ao computador no destino.

A Internet é a maior rodovia de informações já criada. No início, antes da popularização do nome Internet, as pessoas usavam o nome superestrada da informação, como no livro de 1995 **Superestrada da Informação: descubra como as novas fronteiras eletrônicas irão revolucionar sua vida⁵.**

O que entra e sai pelas portas do computador na maioria das vezes vai passar pela Internet, pela super estrada da informação. O que você precisa saber no

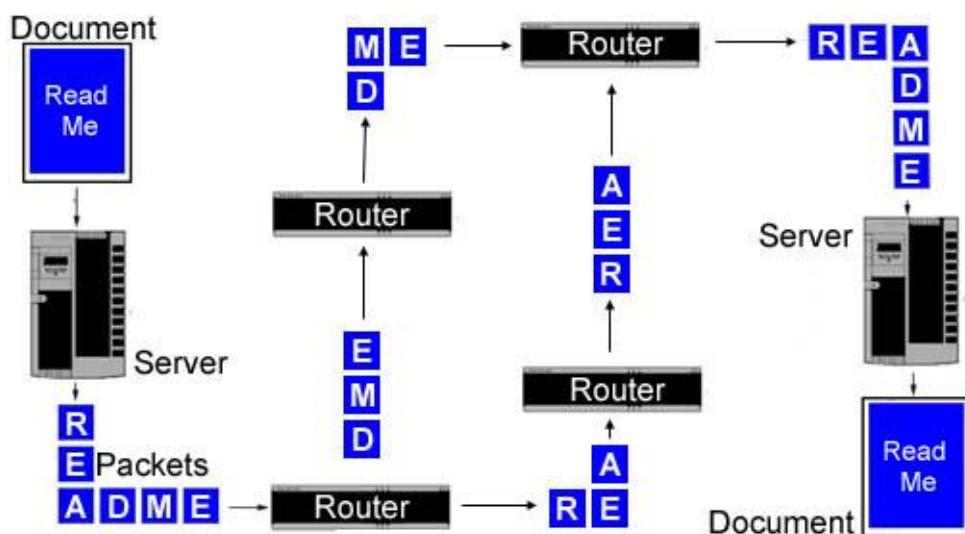
⁵

https://books.google.com.br/books/about/Desvendando_a_superestrada_da_informa%C3%A7.html?id=PFdqkQEACAAJ&redir_esc=y

momento é que a informação é dividida em pacotes. Se pudéssemos ver o tráfego veríamos incontáveis pacotes nessa super rodovia de várias faixas.

Vamos supor que você queira enviar uma mensagem com a palavra hacker para um computador do outro lado do mundo, no caso de quem mora no Brasil, é a China.

Esta mensagem é dividida em pacotes e estes pacotes são enviados do computador para um servidor e do servidor para a super estrada - a Internet, até chegar ao servidor que cuida dos e-mails do destinatário, o responsável por fazer a entrega.



Na figura anterior a mensagem enviada continha a palavra READ ME, LEIA-ME em português. Repare que o primeiro servidor (Server) dividiu a mensagem em pacotes, representados pelas letras isoladas R E A D M E.

Estes pacotes foram enviados fora de ordem e passaram por diversos inspetores de rota (roteadores) responsáveis por fazer os pacotes chegarem ao endereço de destino correto (o IP do destinatário).

No destino um outro servidor foi responsável por organizar os pacotes na sequência correta e reconstruir a mensagem.

Você não precisa ter um servidor em casa para enviar um e-mail, mas precisa ter uma conta cadastrada em um servidor de e-mail. É este servidor de e-mail que vai ser responsável tanto por dividir a mensagem em pacotes (o servidor de e-mail de quem envia) como reconstruir os pacotes no destino (o servidor de e-mail de quem recebe).

Assista no Youtube ao vídeo Warriors of the Net (Guerreiros da Internet):

- <https://youtu.be/e6SU42eP7e4>

Nele você visualiza os pacotes sendo transportados e roteados, incluindo alguns pacotes indesejados barrados pelo firewall. Não se preocupe se você não compreender todos os termos técnicos. O importante é consolidar seu conhecimento sobre pacotes e como eles trafegam desde a rede ou computador local até o destino final, onde quer que seja.

Falaremos um pouco mais sobre pacotes em breve, no volume da **Bíblia Hacker** que tratarmos do IP.

Nós hacker usamos um programa especialmente criado para raptar e capturar os pacotes durante o tráfego. São programas conhecidos como farejadores de pacotes ou sniffers e tem por objetivo tentar descobrir senhas e outras informações importantes que estejam trafegando.

Para tentar proteger nossos dados algumas conexões tentam esconder o conteúdo dos pacotes, criptografando-os. Mas nem sempre isto ocorre e senhas como a do e-Mail e das redes sociais, são facilmente capturadas, principalmente quando estamos usando redes sem fio ou computadores de uso promiscuo, como os das Lan Houses e laboratórios de informática.

Como as portas são acessadas?

Vimos que o que chega nas portas são os pacotes, mas como as portas são acessadas? Se você seguiu nossa orientação e assistiu ao vídeo Guerreiros da Internet, viu que os roteadores são os principais organizadores do tráfego, direcionando os pacotes até chegarem ao destino.

Isto nos faz concluir que as portas são acessadas a partir de uma requisição. Se você envia uma mensagem você está requerendo do servidor local o serviço de envio para determinado destinatário. Se você acessa uma página na Internet, está requerendo ao servidor remoto que envie para seu computador o conteúdo do site. A página Web.

Não há como estabelecer a comunicação sem que exista no mínimo o emissor de um lado e o receptor do outro. Por este motivo é impossível invadir um computador desligado. Toda empresa quando suspeita de estar sob ataque ou invasão determina que seus funcionários desliguem todas as máquinas, como ocorreu em maio de 2017 quando tivemos o maior ataque hacker já registrado em toda a história moderna.

As portas são acessadas através de uma conexão. Esta conexão também é conhecida como requisição, dependendo do serviço utilizado. Quando você acessa uma página na Internet você está fazendo uma requisição. A requisição da página. Se ela não existir você recebe algum tipo de mensagem de erro, tornando-se importante para o hacker conhecer estas mensagens.

O aperto de mão em três vias

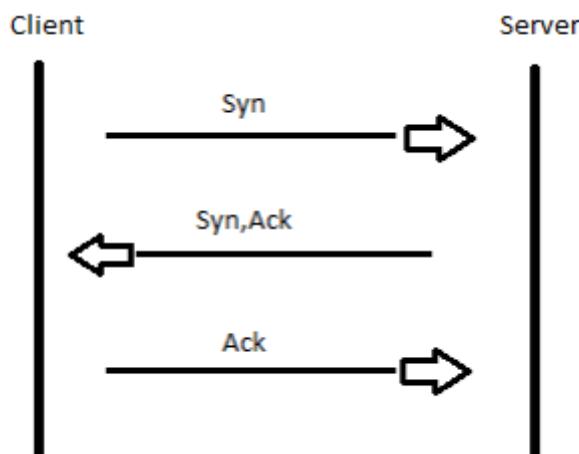
Todos que estudam sobre redes de computadores, incluindo os hackers, precisam conhecer o **TCP 3-Way Handshake**, que se traduzido quer dizer **aperto de mão em três vias**.

Este nome explica como ocorrem as conexões no TCP e se você precisar fazer alguma prova ou exame de certificação, a dica é memorizar a sequência:

SYN -> SYN-ACK -> ACK

- SYN vem de **SYN**chronize ou sincronizar em português.
- ACK vem de **ACK**nowledgemet ou reconhecimento em português.

Esta imagem descreve o processo do Three-Way Handshake:



1. O cliente envia um pacote com a flag SYN ativa;
2. O servidor responde com um pacote com as flags SYN + ACK;
3. O cliente reponde com um pacote ACK.

Uma forma um pouco mais “técnica” seria:

1. Cliente: Servidor, estou enviando a mensagem 100 (Número de sequência do cliente). Dá para sincronizar (SYN)?
2. Servidor: Claro, sincroniza a mensagem 200 (Número de sequência do servidor) que estou enviando (SYN). Prossiga com a mensagem 101 (ACK).
3. Cliente: OK, estou enviando a mensagem 101. Prossiga com a mensagem 201 (ACK).

O cliente e o servidor, possuem números de sequência distintos, por este motivo faz-se necessária a sincronização em ambos os sentidos.

Feita a sincronização, começa a troca de pacotes com base em números de sequência, que tem o objetivo de enumerar os pacotes de cada um.

É possível ver tudo isto acontecendo usando um software de análise de pacotes, como o Wireshark por exemplo. Mas seria apenas para fins de aprofundamento no assunto, não ver o Three-way Handshake acontecendo não o impede de funcionar e nem você de ser hacker.

Quais portas existem?

A IANA (Internet Assigned Numbers Authority, em português Autoridade para Atribuição de Números da Internet) é a organização mundial que supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autônomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.

Se não houvesse um órgão regulador cada empresa poderia decidir qual porta usar para acessar páginas na Internet e isto poderia causar conflitos e confusões.

Quando você acessa um site como www.abibliahacker.com por exemplo, está usando a porta 80 que é a porta padrão para este tipo de acesso. Se cada fabricante ou site usasse o número de porta que quisesse, ao acessar um site você precisaria definir também a porta, digitando:

www.abibliahacker.com:80

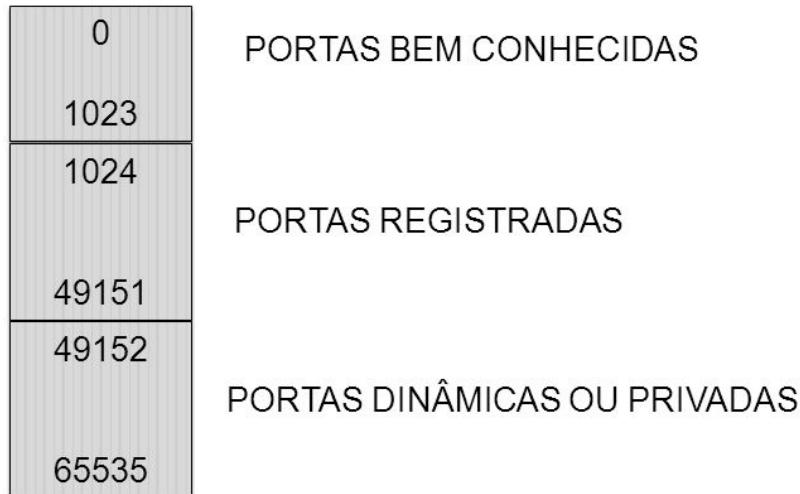
Isto causaria um problema, porque se o serviço de e-Mail usasse a porta 80 haveria um conflito de portas. Por este motivo as portas dos serviços mais populares e importante foram previamente definidas.

Como as portas são identificadas?

Existem 65.536 portas numeradas de 0 a 65.535, mas nem todas as portas estão disponíveis para uso. A IANA divide as portas em três blocos, sendo de 0 a 1.023 as portas bem conhecidas, de 1.024 a 49.151 as portas registradas e de 49.152 a 65.535 as portas dinâmicas ou privadas.

Portas TCP e UDP

- Números inteiros de 16 bits padronizadas pela IANA (Internet Assigned Number Authority)



Quando você estiver fazendo a varredura das portas de um computador ou servidor, na maioria das vezes será o suficiente fazer a varredura até a porta 1.023, deixando a varredura para as portas altas para casos específicos.

Como proteger as portas?

As portas podem ser monitoradas usando programas de monitoramento de portas, podendo ser o que vem junto com a maioria dos sistemas operacionais.

Uma outra forma de proteger as portas é configurando no firewall o acesso de uma das seguintes formas:

- Deixando a porta aberta (open)
- Filtrando a porta (filtered)
- Deixando a porta fechada (closed)

Este controle pode ser feito por porta ou por software. A porta 80 por exemplo, costuma ficar aberta porque é a porta de comunicação com as páginas da Internet. Se você bloquear esta porta na rede da empresa ninguém vai conseguir acessar a Internet.

A mesma porta 80 pode ser filtrada, impedindo, por exemplo, o acesso aos sites das redes sociais, jogos online, pornográficos ou qualquer outro que interfira na produtividade da empresa ou possa trazer riscos.

Se você frequenta o laboratório de informática de alguma faculdade já deve ter percebido que não consegue abrir alguns sites. Este é um bom exemplo da porta 80 filtrada.

Mais adiante em outro volume da **Bíblia Hacker** você vai aprender como burlar esta segurança e vai poder acessar qualquer site, mesmo que a rede esteja com a porta filtrada ou bloqueada.

A porta também pode ser completamente bloqueada, não permitindo qualquer tipo de acesso. O bloqueio pode ser feito sobre um software específico, não sobre portas. Este bloqueio de software é muito usado para impedir que o fabricante consiga bloquear programas crackeados. Veremos

isTo na prática em outro momento, quando tratarmos do firewall. Por enquanto você precisa compreender bem como funcionam as portas.

Uma outra informação importante é que este bloqueio ou filtragem pode ser aplicado apenas na entrada, apenas na saída ou na entrada e na saída, ou seja, bloqueio total.

Como vimos o gerenciamento das portas da rede ou do computador é feito pelo firewall. O firewall pode ser um programa de computador, pode ser aquele que vem no Windows e pode ser um equipamento chamado firewall, geralmente usado só por grandes empresas.

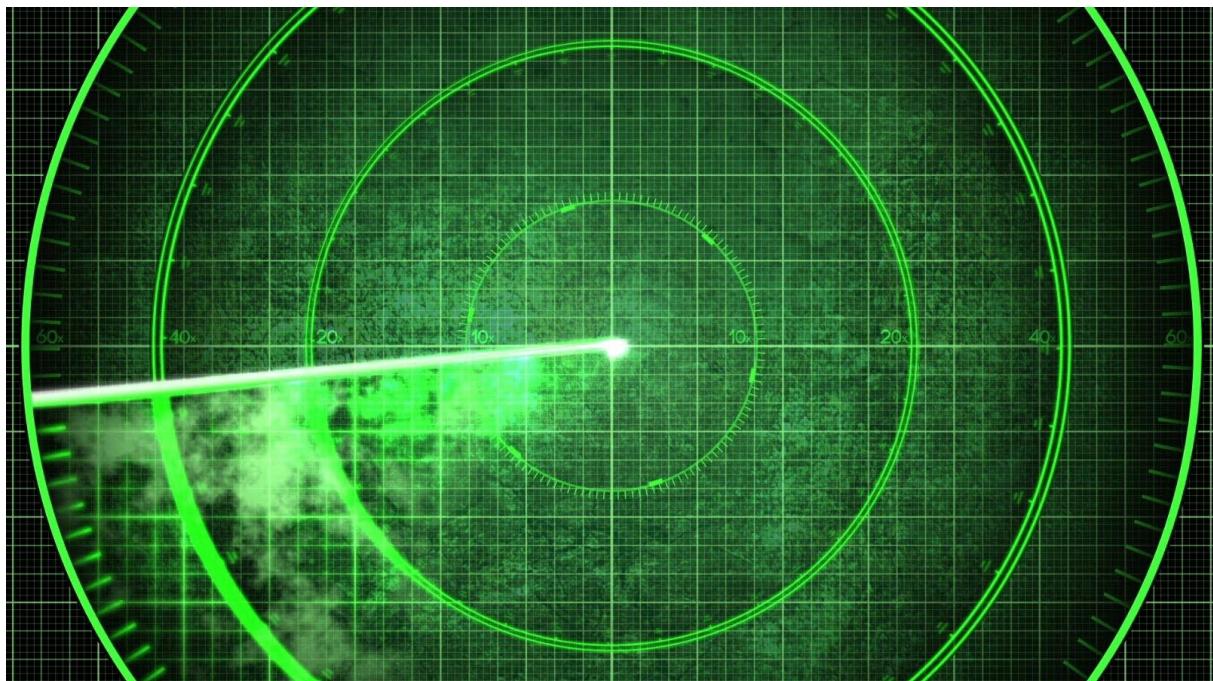
Firewall de spam e vírus.



IPs e Vulnerabilidades

Sobre IPs e vulnerabilidades trataremos mais tarde. Por enquanto aprenda tudo o que puder sobre portas, neste e nos próximos volumes da **Bíblia Hacker**.





Varredura de Portas

Aproveitando seu recém adquirido conhecimento sobre as portas das redes e dos PCs chegou a hora da parte prática, a primeira de muitas que você vai ter na **Bíblia Hacker**.

Você conseguirá ser hacker se dominar técnicas e ferramentas separadamente até que consiga juntá-las para realizar ataques e invasões.

Por nossa experiência todos que tentaram entender a invasão de uma só vez, sem passar pela experiência e prática das técnicas e ferramentas separadamente, não tiveram êxito. São os eternos buscadores que fazem um curso após o outro e nunca conseguem alcançar os resultados almejados.

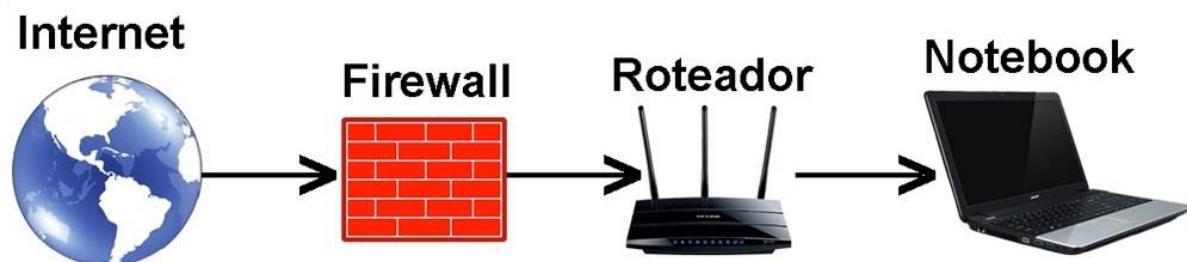
A propósito, sempre que falarmos em invasões estaremos nos referindo as invasões do tipo autorizado, aquela que a gente faz em nosso próprio computador para testar a segurança ou a pedido de alguma empresa¹ e ainda ganhamos dinheiro com isso.

¹ Teste de invasão autorizado ou Pentest (Penetration Testing).

Como já foi dito você precisa saber quais portas estão disponíveis, seja em uma rede local, computador pessoal, servidor de redes, IoT², ou dispositivo móvel como tablet, wearable³ ou smartphone.

Podemos usar o próprio sistema operacional para inspecionar as portas, mas o melhor é usar um software especializado, com mais recursos e mais informações.

As portas podem ficar inacessíveis dependendo de onde você tente fazer o acesso. Por exemplo, se você faz a varredura nas portas do seu próprio computador encontrará uma visibilidade maior do que alguém que tente fazer a varredura de fora, usando a Internet ou a conexão de rede sem fio (WiFi). Isto ocorre porque o dispositivo de acesso à Internet funciona como uma barreira, conforme pode ser visto na figura abaixo:



Se você está na Internet tentando acessar o Notebook vai ter que passar pelo firewall e pelo roteador. Às vezes até mais de um firewall, pois é comum o modem, o roteador, o firewall e até o switch fazerem parte do mesmo dispositivo eletrônico. Então você tem o firewall do modem-router e mais o firewall do Windows.

Olhando a figura acima vemos três pontos de acesso:

1. A partir da Internet.
2. Acesso a partir do roteador, usando a rede WiFi por exemplo.
3. Acesso direto ao computador.

² Internet das Coisas.

³ Dispositivos vestíveis como pulseiras fitness por exemplo.

Esta informação é importante porque dependendo de onde você esteja, se em 1, 2 ou 3, a quantidade de portas e vulnerabilidades que vai enxergar pode ser diferente.

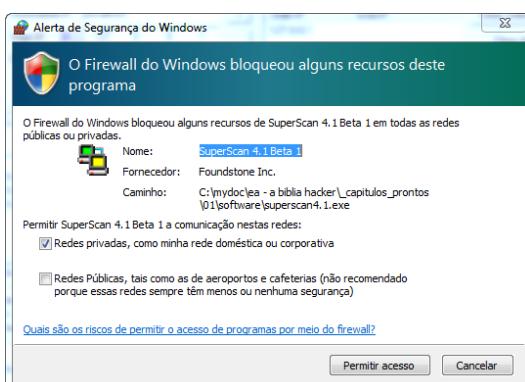
Praticando a varredura de portas

Agora que você já sabe que existem 65.536 portas numeradas de 0 a 65.535, que dependendo do ponto de acesso você terá mais ou menos acesso as portas do alvo e que na maioria das vezes só nos interessa as portas de 0 a 1.023, podemos começar.

Primeiro faça download dos seguintes programas:

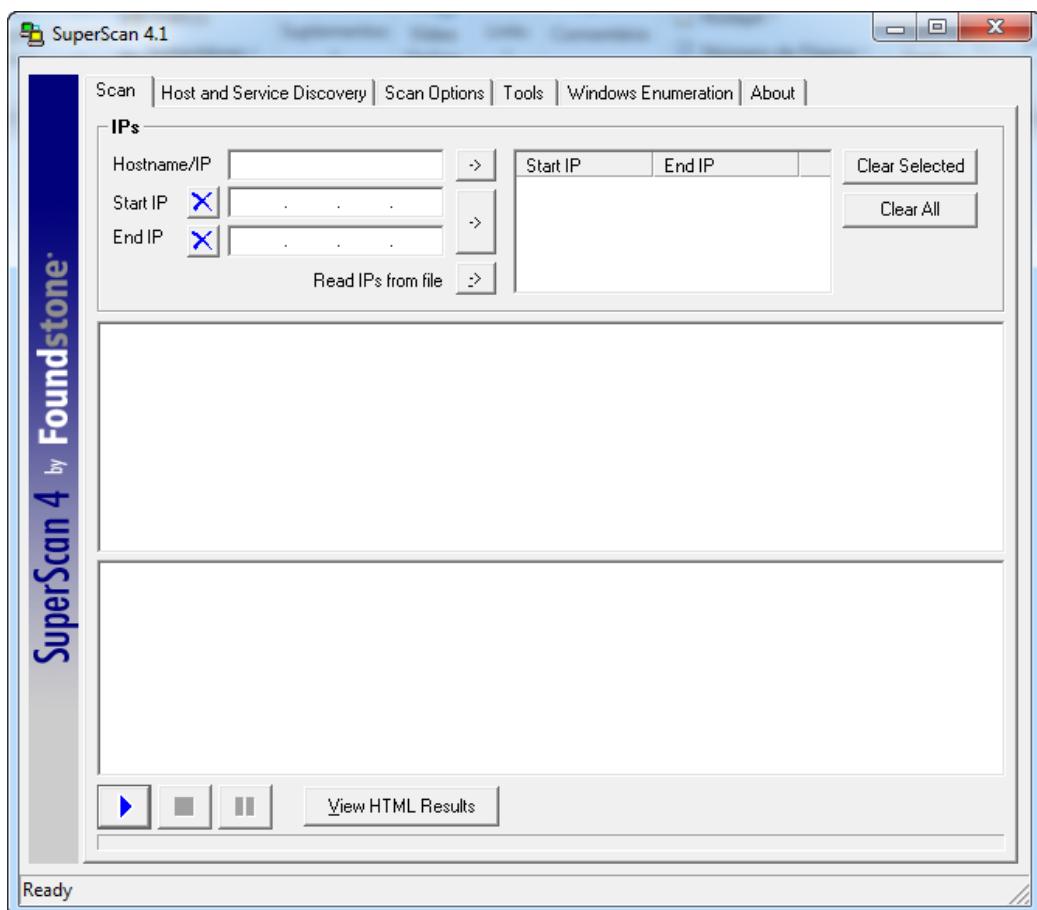
- **SuperScan v4.1**
 - <https://www.mcafee.com/br/downloads/free-tools/superscan.aspx#>
- **NMap**
 - <https://nmap.org/download.html>
- **Advanced Port Scan**
 - <http://www.advanced-port-scanner.com/br/>

O NMap será visto em outro volume, pois merece um capítulo à parte. Vamos começar pelo SuperScan. Este programa não precisa ser instalado, mas você precisará executá-lo como administrador. Para fazer isto basta clicar com o botão direito do mouse sobre o arquivo e selecionar a opção **Executar como administrador**. Vai aparecer a tela abaixo e você precisa **Permitir acesso**:



Feito isto chegamos a tela principal do SuperScan. Vamos conhecê-la. Repare que o SuperScan não tem barra de menus. Ele está organizado pelas seguintes abas:

- Scan (Varredura)
- Host and Service Discovery (Descoberta de host e serviço)
- Scan Options (Opções de varredura)
- Tools (Ferramentas)
- Windows Enumeration (Enumeração do Windows)
- About (Sobre)



Scan (Varredura)

A aba Scan do SuperScan é a principal e provavelmente a única que será utilizada se tudo o que você deseja é fazer uma varredura de portas bem simples.

A aba Scan é dividida em quatro painéis. Dois na parte de cima lado a lado e um sobre o outro na parte de baixo. O principal recurso desta aba é o painel IPs. Em Hostname/IP tanto você pode digitar um IP como por exemplo 192.168.1.1 como pode digitar o nome do host, como por exemplo www.abibliahacker.com.

Após digitar o IP ou o nome do host ou do domínio clique sobre a seta -> para adicionar este IP no painel do lado direito. Para começar a varredura clique sobre o botão ► que se encontra na parte de baixo da tela.

Faça o teste em seu próprio computador e também no seu modem-router, se houver. O IP do computador local é o 127.0.0.1, mas você também pode usar o nome localhost. O IP do modem router geralmente é o 192.168.1.1, mas você precisa consultar esta informação olhando na caixa do aparelho.

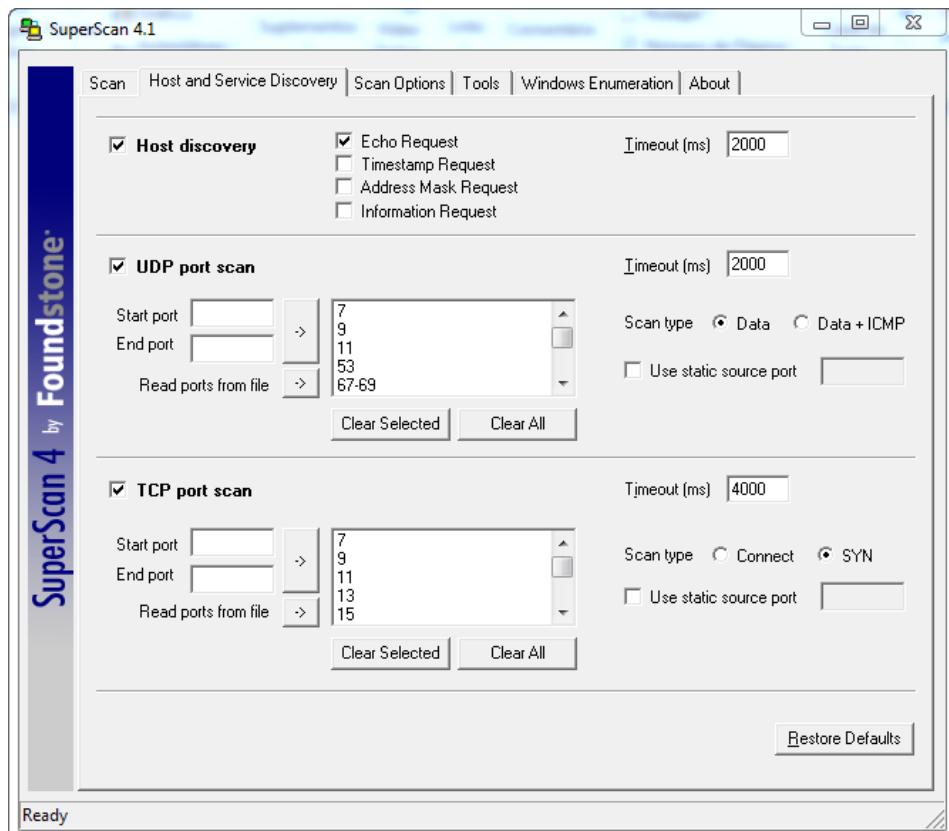
Temos uma videoaula demonstrando o SuperScan em funcionamento. Você poderá assisti-la gratuitamente acessando nossa Fanpage www.fb.com/abibliahacker. Apenas lembrando que o acesso ao grupo é restrito aos clientes que adquiriram a **Bíblia Hacker** legalmente. O acesso as videoaulas não é repassado a terceiros.

Se você realizou o exercício proposto com o SuperScan talvez não receba nenhuma porta como resultado da varredura. Isto ocorre porque se você não fizer nada nas configurações do SuperScan ele fará todas as varreduras usando a configuração padrão, de fábrica. E esta configuração de fábrica nem sempre consegue descobrir portas escondidas atrás de firewalls.



Host and Service Discovery (Descoberta de host e serviço)

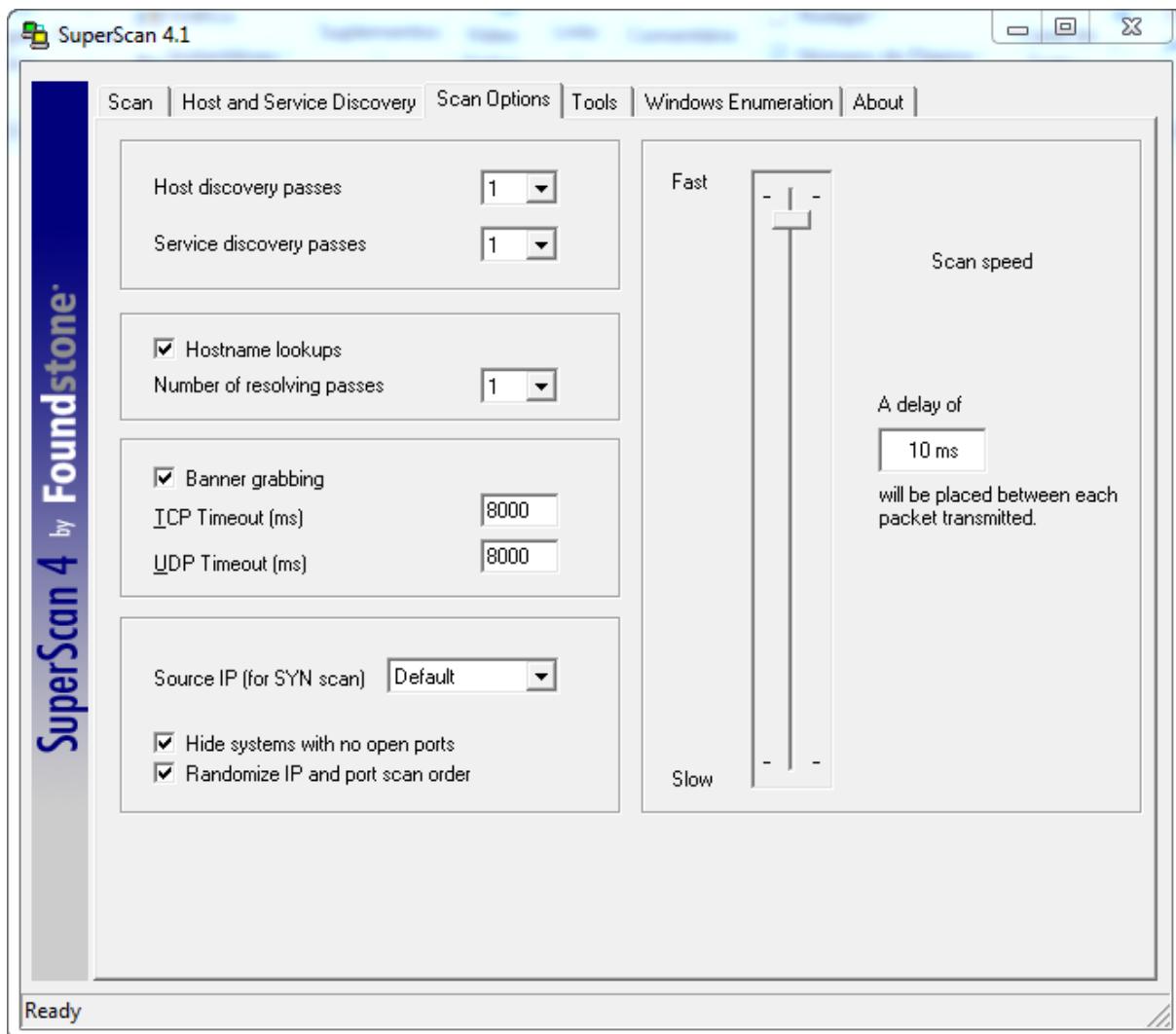
Na aba **Descoberta de host e serviço** encontramos as primeiras opções de personalização da nossa varredura.



Scan Options (Opções de varredura)

Na aba **Opções de varredura** podemos definir alguns parâmetros sendo o principal o **Scan Speed** (Velocidade da Varredura). Por padrão a varredura será feita em modo rápido (Fast). O problema do modo rápido é que às vezes não dá tempo de o host estabelecer a comunicação, conforme vimos na explicação sobre o aperto de mãos em três vias.

Se após fazer a varredura nenhuma porta apareceu para você, experimente acessar a aba **Scan Options** e reduzir o tempo de espera da varredura, trazendo o cursor de Fast para Slow. Posicione-o no centro por exemplo.



Tools (Ferramentas)

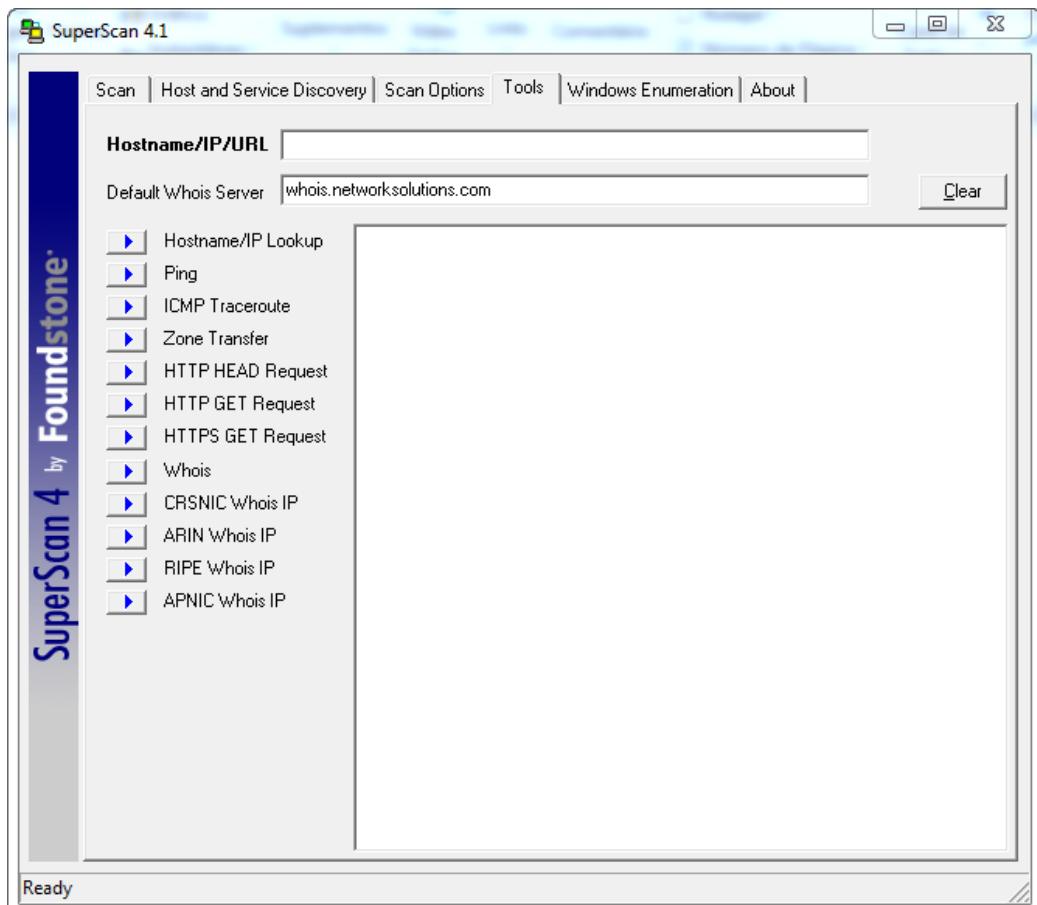
Na aba **Ferramentas** encontramos ferramentas úteis para investigação e varredura remota. No campo Hostname/IP/URL você pode digitar o nome de um computador na rede, o IP ou o endereço de um site na Internet, a URL.

Depois é só escolher a ferramenta desejada, como por exemplo:

- Hostname/IP Lookup – exibe o nome do domínio se você informar um IP ou o IP se você informar o nome de domínio.

- Ping – verifica se o host está ativo, mas como é um ping configurado minimamente, pode ser que o host esteja ativo e o ping diga que não por causa do firewall.

Todas estas opções estão demonstradas na videoaula sobre o SuperScan. Não deixe de assisti-la visitando nossa Fanpage no Facebook.

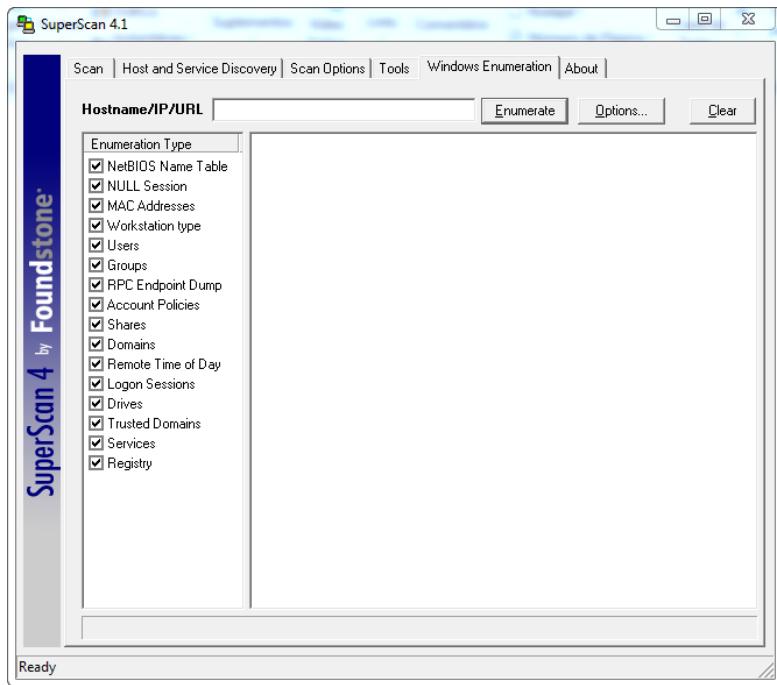


Windows Enumeration (Enumeração do Windows)

A aba Enumeração do Windows reúne um conjunto de ferramentas para uso no computador local. Da mesma forma, você pode informar o nome do host, IP ou URL e após clicar em **Enumerate** é só aguardar alguns minutos para a enumeração ser realizada.

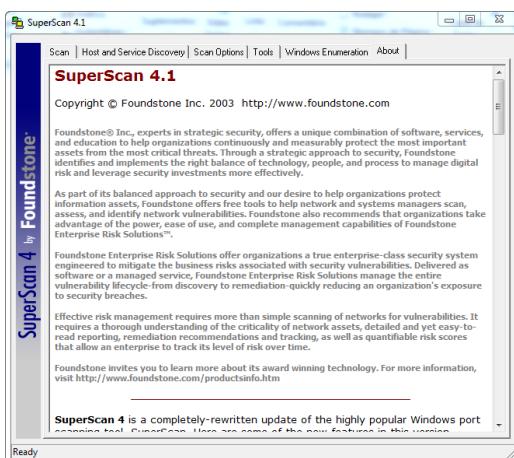
Este recurso é útil quando usado em um computador desconhecido, para sabermos diversas informações importantes que poderão ser usadas em uma invasão, inclusive de redes sem fio.

Para obter os melhores resultados das ferramentas de enumeração do SuperScan, acesse **Options...** e marque a opção de fazer a varredura usando as credenciais de **Administrador**.



About (Sobre)

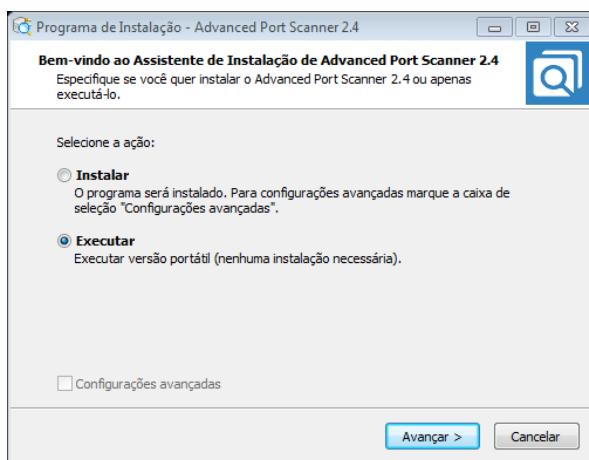
Esta aba apenas traz informações sobre o fabricante e o programa. Talvez cause estranhamento saber que o SuperScan foi criado em 2003. Não se preocupe com isso, em 2003 foi criada a primeira versão. A versão 4.1 é a mais recente e nem está mais com a Foundstone, passou para a McAfee que é quem agora responde pelo produto.



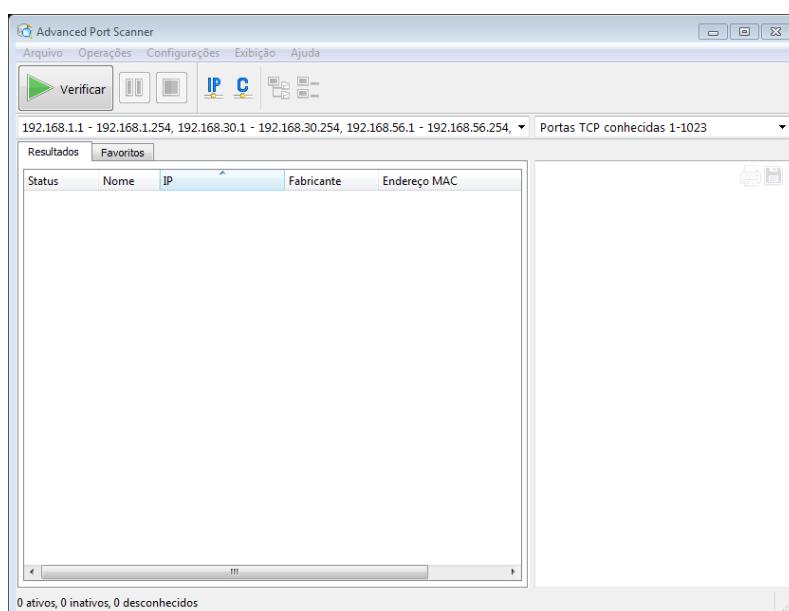
Advanced Port Scan

O **Advanced Port Scan**, que pode ser baixado do site <http://www.advanced-port-scanner.com/br/> como já indicamos, tem a vantagem de estar em português.

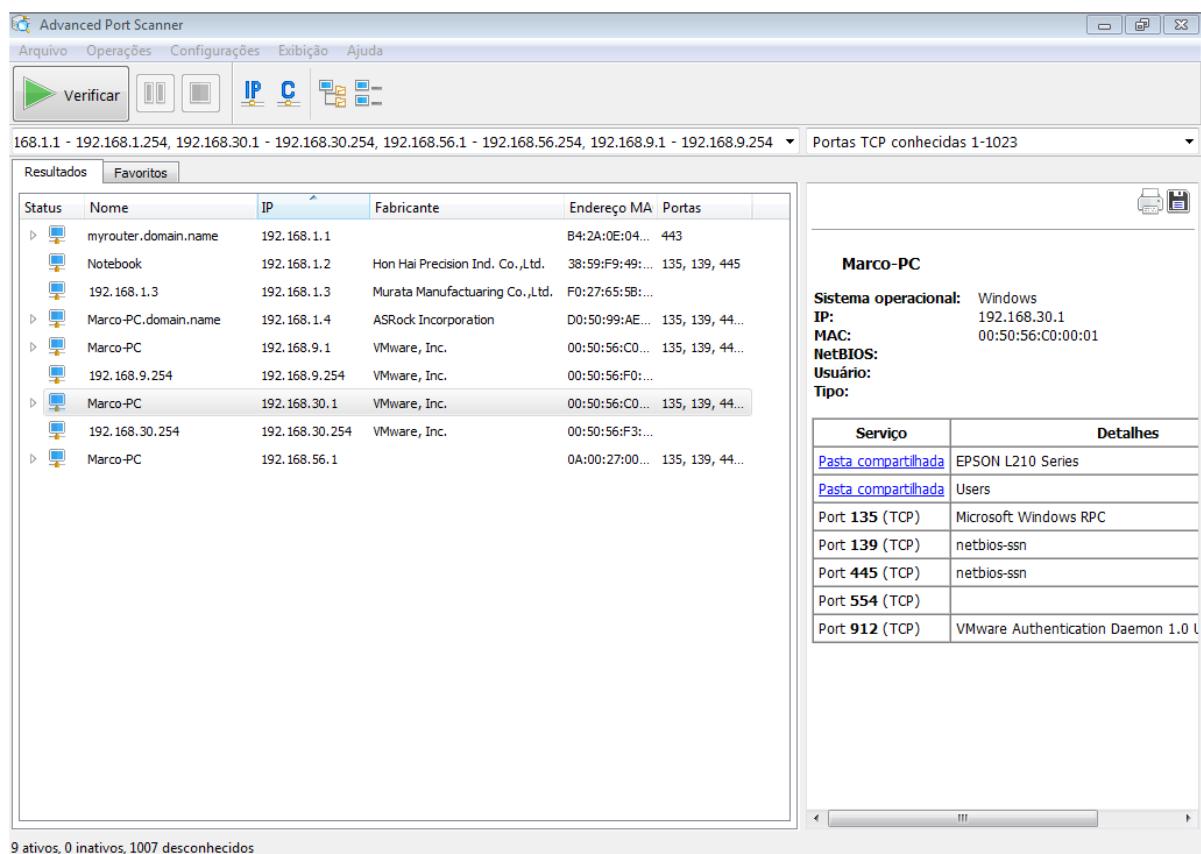
Ao executá-lo você terá a opção de instalar ou executar sem instalar. Sempre que possível e estiver disponível, a melhor opção é sempre executar sem instalar o que é conhecido como programa portátil ou portable.



Após a instalação observe que ele usa uma interface mais simples, com um campo para definir o IP ou hostname da varredura e uma grande área para exibição dos resultados. Ao clicar no botão verde (►) **Verificar**, a varredura começa.



De cara você já vai perceber grandes diferenças entre o SuperScan e o Advanced Port Scan. A primeira é que o programa identifica todos os computadores ativos e já se configura para a varredura. Na prática tudo o que você precisa fazer é abrir o programa e clicar no botão verde (►) **Verificar** para dar início a varredura. O resultado é o melhor possível, com identificação dos hosts, portas, serviços, compartilhamentos, sistemas operacionais. O SuperScan também é capaz disto, mas não com esta facilidade. É preciso fazer vários ajustes na configuração. No Advanced Port Scan esta operação é feita no modo automático.



Em nossas videoaulas também demonstramos o uso do Advanced Port Scan, mas como você deve ter percebido, usá-lo é bem simples. Basta executar até sem instalar e depois clicar no botão que dará início a varredura. Para que este relatório seja realmente útil a você, é preciso que saiba a utilidade das principais portas.

Tabela de uso das portas TCP/UDP

A lista oficial é publicada pela IANA em:

goo.gl/7ziFqn

Você também pode consultar a lista de portas na Wikipédia:

https://pt.wikipedia.org/wiki/Lista_de_portas_de_protocolos

Vale a pena estudar e memorizar pelo menos estas portas, que são as mais usadas:

Serviço	Porta
http	80
ftp	20 e 21
telnet	23
dhcp	67
dns	53
snmp	161 e 162
nfs	2049
smb	137, 138, 139 e 445
smtp	25
pop3	110

Varredura online

Às vezes o que precisamos é fazer a varredura em nossa própria rede, site ou computador, mas de fora para dentro. Usando um IP externo. Se fizermos usando o nosso próprio computador os resultados não são tão realistas quanto quando fazemos a varredura externa, de fora para dentro.

Também pode acontecer de você tentar executar o programa de varredura e o administrador da rede ter configurado o sistema para não deixar executar nenhum programa. Isto é o que todo administrador de redes deveria fazer.

Para estes casos podemos contar com os sites que fazem a varredura externa. Você tanto pode inserir no site o endereço de algum site que queira pesquisar, como também pode inserir o IP do seu próprio computador e ver se ele está com alguma porta aberta. Serve também para celular.

Comece obtendo o seu IP externo em um destes sites:

- <https://whatismyip.com.br/>
- <https://www.iplocation.net/find-ip-address>
- <http://whatismyipaddress.com/>
- <http://www.whatsmyip.org/>

Após obter o IP externo, o IP que aparece para os outros que estão fora da rede, use o IP descoberto em um ou mais dos sites que fazem varredura de portas:

- <http://www.ipfingerprints.com/portscan.php>
- <http://www.yougetsignal.com/tools/open-ports/>
- <http://www.t1shopper.com/tools/port-scan/>
- <http://www.whatsmyip.org/port-scanner/>

Alguns destes sites já identificam o IP externo, não sendo necessário informá-lo como orientamos inicialmente. Outro ponto importante a considerar é que o IP externo, o IP que aparece na Internet, não é o do seu computador. É o IP do modem-router e todo modem-router tem um firewall embutido. O resultado esperado é que a maioria das portas esteja filtrada ou fechada. O importante deste exercício é comparar o resultado dos programas de varredura locais executados internamente com os resultados dos sites com ferramentas de varredura executadas de fora para dentro.

Como os hackers agem

Agora que você sabe tudo o que precisa saber sobre portas e varredura de portas, vamos entender como este conhecimento é usado pelos hackers.

Como já foi dito, para ser um hacker você precisa conhecer porta, IP e vulnerabilidade. Outra coisa que você precisa saber e vou dizer agora é que a estratégia para invadir celulares, servidores e computadores de usuário é completamente diferente uma da outra.

Veja os exemplos:

- **Invasão de celular**
 - Depende do conhecimento do sistema operacional Android ou iOS, a invasão pode ser feita por Apps ou clonagem, permite ataques a identidade baseado em serviços Web (AIBW), a varredura de portas ou vulnerabilidades não serve para muita coisa.
- **Invasão de servidores**
 - Por terem o IP fixo a invasão pode ser planejada a longo prazo, permite a clonagem do SO para definir estratégia antes do ataque, as empresas estão dispostas a pagar aos profissionais de segurança que consigam mantê-los longe dos invasores mal-intencionados, técnicas como engenharia social, trojan e scam não funcionam, porque não vai ter ninguém no servidor para interagir com os malwares.
- **Invasão de computadores de usuários**
 - O IP é dinâmico, precisa ser marcado para não o perdermos de vista, é ideal para usarmos as técnicas clássicas, como homem no meio, trojan, scam, spam, engenharia social, etc.

Esta questão de porta não é muito relevante na invasão de usuários ou de smartphones. É mais importante para a invasão de servidores. Porque quando você escaneia o IP de um usuário que esteja usando um PC, notebook ou smartphone, geralmente estará escaneando o modem-router. O IP que vai aparecer não é o do computador, é o do roteador da Internet.

Então se a intenção for invadir um computador de usuário ou smartphone, a identificação das portas até pode ser feita, mas não ajudará tanto quanto o que queremos é invadir um site, servidor ou rede da empresa (para fins de segurança).

Como então o invasor poderá usar programas de varredura de portas para invasão? Para uma destas finalidades:

- Se estiver escaneando alguma rede local, como a da empresa ou a Internet compartilhada ou a rede sem fio do vizinho, poderá descobrir pastas compartilhadas e outras informações sobre o alvo.
- Se estiver escaneando sites e servidores, a lista de portas disponíveis será fundamental para conseguir a invasão.



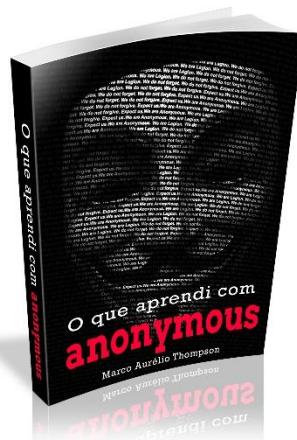
Aprenda a ser Hacker com Cases

Uma das grandes dificuldades que o hacker iniciante tem é a falta de referência sobre o que é ser hacker. Não é segredo que eu participo de grandes eventos como a Copa do Mundo FIFA, Olimpíadas Rio 2016, Rock in Rio, Carnaval do Rio e de Salvador, entre outros. O que percebi é que nessas épocas recebo ofensas e reclamações de desconhecidos, dizendo que “participar de eventos não é *papel* de hacker”. Basta aparecer a primeira foto no evento para *haters* e *trolls* chegarem juntos.

É triste ter contato com a ignorância das pessoas em relação aos hackers. O hacker é uma pessoa comum. Sou eu. É você. Do jeito que nós somos. A referência que as pessoas têm de hackers é que aparece no cinema, na imprensa, na televisão.

Na maioria das vezes o que aparece não existe. Os melhores exemplos são aquelas interfaces futurísticas que não existem no mundo real. Ou as invasões ocorrendo em questão de minutos e até de segundos. Cinema é assim. É para entreter. Não é documentário e muito menos videoaula.

Para ajudar você a entender melhor como os hackers agem decidimos lançar em 2018 uma série de livros demonstrando as técnicas dos maiores hackers e como obter os mesmos resultados que aparecem nas séries e filmes.





Episódio de hoje: A Escuta (1)

O clima na empresa era tenso. O ano começou com boatos de corte de pessoal. Boatos que logo se mostraram verdadeiros. Tirando o filho do dono, ninguém estava seguro. Até um dos diretores, que gostava de falar que a empresa não funcionaria sem ele, foi o primeiro a levar um pé na bunda. A partir daí é que começou o desespero geral. Ninguém estava seguro naquela empresa.

Eu que gosto de planejar o orçamento comecei o ano sem comprar nada. Sem aproveitar nenhuma daquelas liquidações de início do ano. Resisti a todas as tentações de consumo.

Não me pareceu sensato ficar sem reservas ou fazer dívidas, estando sujeito a ser mandado embora a qualquer momento. Cada dia parecia ser o último. Mas não era. E isto só piorava as coisas. Porque quando você é demitido, é ruim, mas pelo menos teve um desfecho. Já sabe que está desempregado e pode procurar outro emprego.

Mas quando fica esta situação de manda embora ou não manda, ficamos em uma espécie de limbo. Sem saber se estamos dentro ou fora da empresa. O futuro é indefinido.

As demissões ocorriam geralmente no final da tarde de sexta-feira. O funcionário era chamado até a sala do chefe. Lá era avisado da demissão e que teria dez minutos para esvaziar as gavetas. Já saía acompanhado por dois seguranças e sequer podia se despedir dos colegas.

Para não nos prejudicarmos, fingíamos que nada de anormal estava acontecendo. Não nos incomodávamos com as lágrimas, principalmente das mulheres. Saíam de lá como almas penadas. Sem que qualquer um de nós desse qualquer apoio ou atenção.

Os demitidos tonavam-se invisíveis. E nós, aliviados por não ter chegado a nossa vez.

A explicação que dávamos a nós mesmos é que se o chefe visse alguém de conversinha com o(a) demitido(a), ele poderia ser o próximo.

_Eu sou hacker!, pensei.

Não podia admitir passar por uma situação dessas. Já estava ficando paranoico. Em uma sexta-feira me chamaram até a sala do chefe e quase me mijei. E não era nada demais. Era só para eu ver o novo logotipo que deveria entrar no site da empresa.

Pedir demissão estava fora de questão. Não queria perder meus direitos trabalhistas. Se já é ruim ser demitido, é ainda pior pedir demissão.

Como eu poderia saber se chegara a minha vez?

A única forma que encontrei para fazer isto foi plantando uma escuta. No telefone não dava. O sujeito usava uma linha de telefone fixo sem fio. Parece um celular, mas é um telefone fixo. Só que em vez de fio usa ondas

de rádio. Era um telefone sem fio fornecido pela companhia telefônica, diferente destes que compramos nas lojas.

Se fosse um telefone fixo convencional eu colocaria a escuta no fio do telefone ou na caixa de inspeção. Mas sem fio não dava.

Por ser responsável pela manutenção da rede e dos computadores, eu tinha acesso ao computador do chefe. Um PC de mesa usado quase que exclusivamente para navegar na Internet e conferir o site da empresa.

O sujeito era um analfabeto digital. Exigir dele mais do que navegar na Internet e entrar no site da empresa era pedir demais. Sua condição de chefe de nós todos só se justificava por sua incompetência para ser empregado.

Como disse, plantar a escuta nos fios do telefone não dava. A solução era plantar a escuta no PC. Mas não havia microfone. Só caixa de som. E haviam outros técnicos na empresa. Todos com medo de serem mandados embora. Se descobrissem o que eu pretendia fazer não teriam qualquer problema em me denunciar para livrar o deles.

Eu precisava plantar uma escuta no PC, que fosse invisível até para um experiente profissional de informática. E foi o que eu fiz.

Primeiro bloqueei o endereço MAC da placa de rede no firewall. Com isto o computador ficou sem acesso à Internet. Eu pensei que seria chamado para resolver o problema. Me considerava o melhor dos três. Mas não foi bem assim. Chamaram um puxa-saco metido a resolver tudo.

De nada adiantou. Sem suspeitar do bloqueio do endereço MAC, o sujeito passou a tarde toda sem conseguir fazer o computador acessar a Internet. Foi então que me chamaram.

Assim que entrei na sala já deu para notar a cara feia do Frederico (nome fictício), torcendo para que eu também quebrasse a cara. E por falar

em cara, dava para sentir a respiração do sujeito em cima do meu ombro, tentando não perder nenhum detalhe do que eu faria.

_Isto eu já fiz. Isto eu também já tentei.

Na verdade, eu só estava ganhando tempo. Não podia resolver em dois minutos para não dar bandeira. Então fiquei digitando comandos de rede, olhando configurações. E o sujeito igual a um papagaio repetindo:

_Isto eu já fiz também.

Passados uns dez minutos desliguei o PC, abri o gabinete, removi a placa de rede, saí da sala e voltei com outra. Frederico abriu a boca na hora:

_Eu já testei a placa de rede.

_Vá a merda Frederico., é o que deu vontade de falar. Mas não era nem o momento, nem o local.

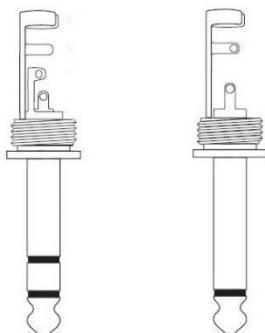
Trocada a placa de rede a Internet voltou. Claro que voltou. Outra placa de rede, outro endereço MAC. Este o firewall não barrava. Mas só eu sabia do detalhe. E no processo de abrir e fechar o gabinete, propositalmente danifiquei o conector da caixa de som.

Avisei que o conector estava quebrado e me comprometi a fazer o conserto. Como envovia ferro de soldar, faria isto na sala de manutenção que era também o refeitório dos técnicos e onde pegávamos as funcionárias da limpeza de vez em quando.

Ao chegar na sala de manutenção, coloquei a caixa de som na bancada, peguei um microfone velho e instalei este microfone dentro da caixa de som. Não dava para puxar um fio para o microfone, então fiz o seguinte.

Quando a caixa de som é estéreo, o conector, um plugue do tipo P2, possui três seções. Uma seção é o terra ou comum. Uma seção é para a caixa da direita e a outra seção é para a caixa da esquerda.

Plugues estéreo e mono usados em caixas de som e microfones de PC.



Dentro da caixa de som liguei um alto falante ao outro. Assim haveria som nas duas caixas, mas não seria mais estéreo. O fio que sobrou eu liguei no microfone. E como não poderia ligar o plugue da caixa de som no microfone sem perder o som, instalei mais um plugue, só para o microfone. Se alguém perguntasse eu diria que o plugue estéreo deu defeito e eu coloquei dois plugues mono.

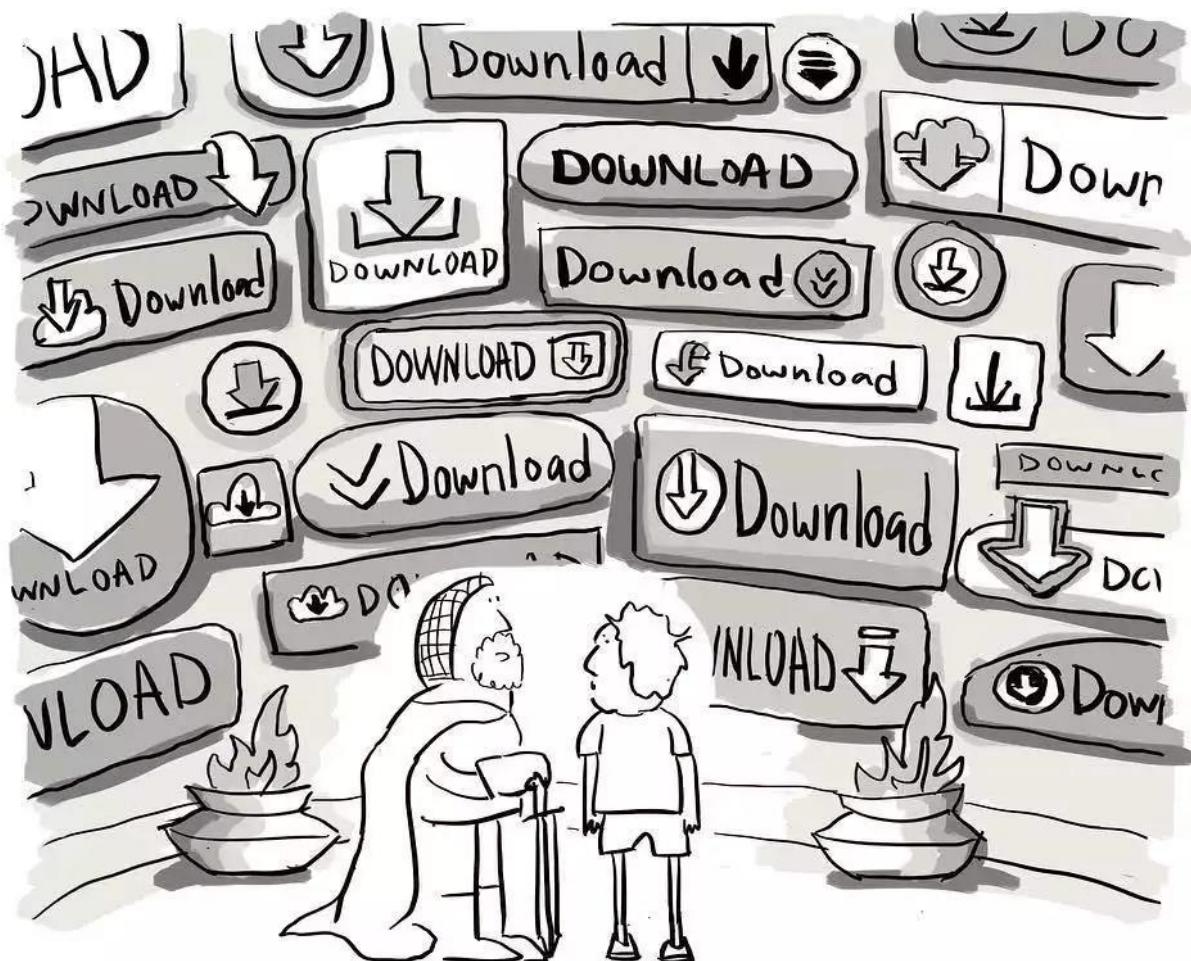
Um técnico em eletrônica não engoliria essa, mas ali só eu entendia de eletrônica. Os demais só conheciam o básico.

A primeira parte do plano estava concluída. Conseguí plantar um microfone oculto dentro da caixa de som e liga-lo ao PC pelo mesmo cabo.

Agora eu só precisava encontrar um jeito de gravar o áudio do ambiente e enviar para mim depois. Você não vai acreditar em como consegui resolver isto.

(continua)





O Falso Botão de Download

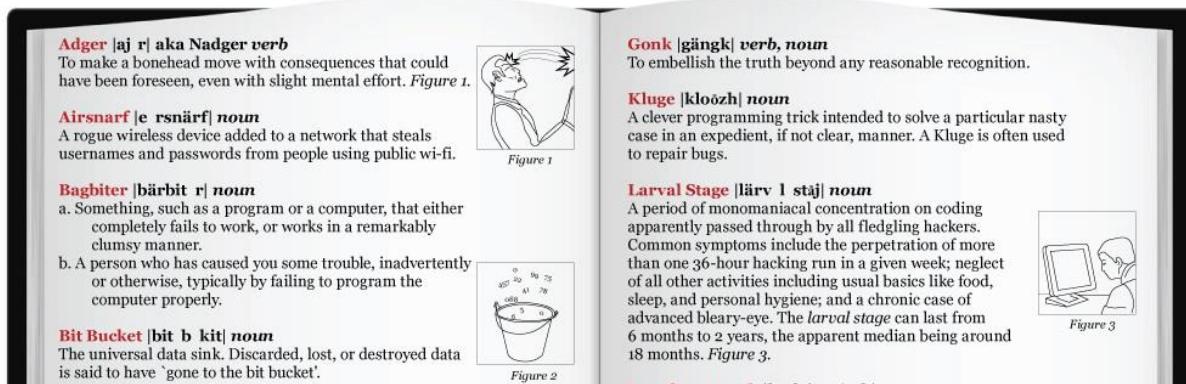
Os golpistas da Internet estão sempre inventando novas formas de conseguir instalar vírus, malwares ou desviar o tráfego para outros sites, geralmente sites com conteúdo pornográfico ou jogos, pois ganham dinheiro com isto.

Funciona assim:

1. Você pesquisa na Internet e acha um site com o programa, música, e-book, filme ou série que você está procurando.
2. Você clica no link para download e aparece uma página com vários botões de download. Sem saber qual escolher você clica no que lhe parece ser o mais correto. Agora é rezar para ter clicado no lugar certo.

Proteja-se contra este golpe assistindo nossa videoaula sobre o assunto.

The HACKER'S DICTIONARY

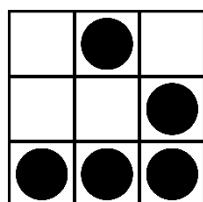


Jargon File

Jargão (jargon em inglês) é o vocabulário específico de uma área de conhecimento. A Comunidade Hacker tem o seu próprio jargão. Vamos conhecer alguns para você não ficar perdido(a) quando estiver conversando com ou sobre hackers.

Glider

O glider é o símbolo dos hackers. Eric S. Raymond¹ propôs o glider como um emblema para representar a subcultura hacker, mas não podemos dizer que a ideia pegou, pois o glider não é universalmente aceito como símbolo hacker.



¹ Eric Steven Raymond (4 de Dezembro de 1957 em Boston, Massachusetts), conhecido também como ESR, é um hacker e escritor americano. Depois da publicação em 1997 do seu livro *A Catedral e o Bazar*, Raymond foi por alguns anos frequentemente citado como um porta-voz extraoficial para o movimento open source. É ele quem mantém o Jargon File, mais conhecido como *The Hacker's Dictionary* (O Dicionário dos Hackers).

Mesmo não sendo aceito universalmente a verdade é que o glider aparece o suficiente para justificar conhecê-lo. Agora vamos entender o que o glider. A pronúncia é *glaider* e quer dizer planador em português. Você até deve conhecer esportes como o paraglider.

Na década de 1940 os matemáticos procuravam uma forma de criar um algoritmo que pudesse representar a vida. Em 1970 o matemático britânico John Horton Conway conseguiu criar um jogo com estas características, tornando-se o exemplo mais conhecido de autômato celular.

O jogo foi criado de modo a reproduzir, através de regras simples, as alterações e mudanças em grupos de seres vivos com aplicações em diversas áreas da Ciência.

As regras são simples:

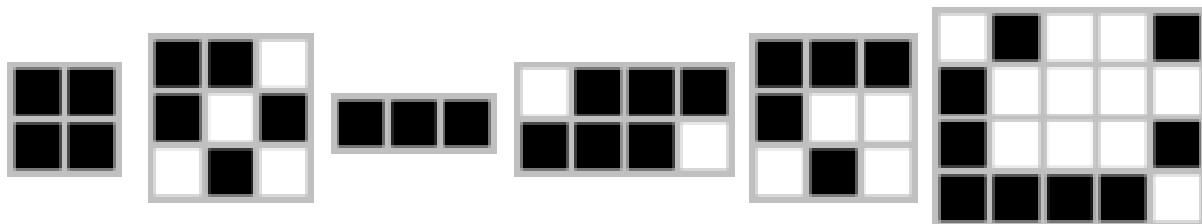
- Qualquer célula viva com menos de dois vizinhos vivos morre de solidão.
- Qualquer célula viva com mais de três vizinhos vivos morre de superpopulação.
- Qualquer célula morta com exatamente três vizinhos vivos se torna uma célula viva.
- Qualquer célula viva com dois ou três vizinhos vivos continua no mesmo estado para a próxima geração.

É importante entender que todos os nascimentos e mortes ocorrem simultaneamente. Juntos eles constituem uma geração ou, como podemos chamá-los, um "instante" na história da vida completa da configuração inicial.

Estas regras transformadas em algoritmo e depois em programa de computador, tornaram possível criar simulações dos mais diferentes tipos e para os mais diferentes propósitos.

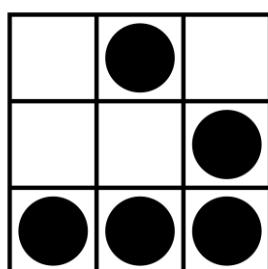
Este "jogo" é na realidade um jogo sem jogador, o que quer dizer que sua evolução é determinada pelo seu estado inicial, não necessitando de nenhuma entrada de jogadores humanos. Ele é jogado em um conjunto de células quadradas que seguem ao infinito em todas as direções. Cada célula tem oito "vizinhos", que são as células adjacentes, incluindo as diagonais. Cada célula pode estar em dois estados: "viva" ou "morta". Também são usados os termos "ligado" e "desligado". O estado do tabuleiro evolui e se modifica em pequenas passagens de tempo. Os estados de todas as células em um instante são considerados para calcular o estado de todas as células no instante seguinte. Todas as células são atualizadas simultaneamente. As transições dependem apenas do número de vizinhos vivos.

Agora o fim do mistério. Os exemplos mais simples destas classes são mostrados abaixo, com as células vivas em preto e as células mortas em branco. O glider é uma das possibilidades do Jogo da Vida e foi ele o adotado pelo Raymond. Nas figuras abaixo temos tabuleiros com células vivas e mortas.



Bloco **Bote** **Blinker** **Sapo** **Glider** **LWSS**

O glider é, portanto, um dos possíveis estados das células no Jogo da Vida.



Escrita Leet

Leet é um tipo de escrita cifrada. Consiste em trocar determinadas letras por outras. A escrita leet não a torna impossível de ler e na maioria das vezes nem é preciso ter uma chave para decifrar a grafia.

A palavra hacker por exemplo, pode ser escrita em leet como h@cker ou h4ck3r. A escrita leet foi usada na novela Geração Brasil da Rede Globo, exibida em 2014:



O fato é que a escrita leet não é exclusividade da comunidade hacker, mas ficou muito associada a tecnologia da informação. Por este motivo quase sempre veremos a escrita leet associada a hackers.

Em se tratando de “escrita hacker” a escrita leet (lê-se lit) existe com diferentes graus de dificuldade. Isto ocorre porque não existe só uma letra ou número associado ao alfabeto. Então o escriba pode escolher os símbolos mais complicados, em vez de usar os mais simples, como 4 para substituir a letra A e o 3 para substituir a letra E.

Observe a tabela e veja que podemos escrever a palavra hacker das formas mais complicadas, como essas conversões da palavra hacker:

h4ck3r

h4x0r

h4 (| {3r

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	8	()	3	=	6	-	!	_	X	1	/ \ /	\	0	*	0 _	2	5	7	_	\ / \ /	8	j	2
@	3	<	[]	£	=	9	#	1	_ /	< 7	\ /	/ \ /	o	o	0,	2	\$	+	(_)	\ /	v v	><	^ /	≥	
/-\	6	¢	ð	&	}	&	- [X	_	em	// \ //	oh	o	(,)	/ 2	z	- -	Y3W	\ // /	' / /	X	` (~ / _	
/\	13	{)	€	ph	(_ +	[-]	eye	z	{	£	v	[\]	[]	>	<	I2	\$	1	M	\ \	\ \ \ '	} {	- /	8
^	3	©	I >	[-	(=	C -) - (3y3	< /	3	_	IYI	< \ >	H	"	cue	^ es	'] t'	μ	\ ^	ecks	' /	3		
aye	B	sea	>	a	f	gee	(-)	ai	_)	_	IYI	{ \ }	R	?	9	~	+	[_]	(n)	x	Ψ	7 -			
ð	13	see	0			jee	: - :	i	j	IJ	[V]	//	9	¶	iz	\ /	\ /	\ /	\ X /	*	φ	7 -			
ci						(\ ,	}{			^		nn	[] \ []	7	2					\ \ \ \ /	(λ			
λ						c l		c j	- {	aych	// \ // / \ \ \] \ [q	z						\ \ \ \ / \ \ \ \ /	ex	ü			
z											(V)	~	b	`						\ \ : _ /					
											(\ \ /)		¶	12						J I [
											/ \ \ /		®	Я						UU					
											/ /		D	.	-					III					
											. \ \ \ /									¶					
											/ \ \ \ /									W					
											^														

Na prática só usa a escrita leet os pré-adolescentes e adolescentes em seu primeiro contato com o mundo hacker. Não é o tipo de comunicação que pega bem para um adulto e muito menos para um profissional de segurança.

Um uso interessante é na área de design em tecnologia, para logotipo, assinatura de e-mail, títulos de artigos, mas sempre com o leet menos complicado, como por exemplo escrever hacker como **h4ck3r**. Na camiseta abaixo por exemplo, está escrito LEET HACKER (1337 h4X0r):



Como você pode perceber são apenas palavras, mas trazem toda uma história e fazem parte da cultura hacker. Se alguém se diz hacker e não conhece a cultura hacker, é comparado a um médico que nunca ouviu falar do Juramento de Hipócrates² ou limitou-se a dizer “juro” sem a preocupação de saber das origens.

Estes são alguns sites em que você poderá usar para codificar e decodificar a escrita leet. Como existem muitas opções para cada letra, nem sempre o decodificador consegue compreender a mensagem codificada por outro:

www.robertecker.com/hp/research/leet-converter.php

www.1337.me/

<http://genr8rs.com/Generator/Fun/LeetSpeakGenerator>

Estes sites podem lhe ser úteis se você encontrar exploits ou textos em arquivos de crack usando a escrita leet e precisar traduzi-los.

Owned

Outra palavrinha que você precisa conhecer é a **owned**. Owned é o passado do verbo em inglês own, que significa possuir alguma coisa e por isso transmite o sentido de propriedade. Owned também possui diversos outros significados, como fazer alguém de bobo ou tolo, fazer algo embaraçoso ou envergonhar uma pessoa.

No contexto dos videogames, a palavra owned é usada quando um jogador vence o outro de forma extraordinária. Assim, dizer que alguém foi ou está owned, significa que a pessoa foi derrotada ou humilhada e que o vencedor é muito superior em suas habilidades. Praticamente humilhou o adversário.

² O Juramento de Hipócrates é um juramento solene efetuado pelos médicos, tradicionalmente por ocasião de sua formatura, no qual juram praticar a medicina honestamente.

Owned é também um termo utilizado por hackers que desfiguram sites de pessoas e empresas. Assim que o hacker invade um site ele faz questão de deixar claro sua superioridade sobre o administrador do site, escrevendo o termo **owned** na página inicial. Na imagem a seguir vemos uma pichação no site do MIT (Massachusetts Institute of Technology):



O hacker tirou onda porque era de se esperar que o MIT estivesse melhor protegido. A dúvida é se o invasor é realmente bom ou se o MIT é que não é lá tudo o que dizem.

O importante é que agora você já sabe que quando ver um site desfigurado com a palavra owned, o invasor está se exibindo, humilhando o administrador do sistema.

Lammer

O termo lammer - às vezes grafado também como lamer – tem origem na palavra lame, que quer dizer coxo, incapaz, inepto. Pode ser considerado sinônimo de Script Kiddie e no Brasil é usado de forma pejorativa, seja para ofender alguém, ou para se referir a alguém que entra em um grupo e faz perguntas idiotas, do tipo:

“Se eu invadir um banco online vou ser preso?”

Também é considerado lammer aquele que entra em um grupo hacker em que a maioria dos seus membros encontra-se em estágio avançado e faz perguntas muito básicas, por ingenuidade. Acabam vítimas de ataques realizados por membros do próprio grupo, que às vezes se mostram prestativos, enviam arquivos dizendo que são ferramentas de ataque, quando na verdade são verdadeiros cavalos de Tróia, prontos para invadir o computador do ingênuo estudante.

Eu participo de vários grupos hacker, incluindo alguns na Deep Web. É claro que lá não vou aparecer como Professor Thompson, pois atrairia atenção desnecessária, não acreditariam que sou eu e se acreditassem, me desafiariam o tempo todo. Posso dizer que seria muito lammer da minha parte entrar em um grupo hacker, qualquer que seja ele, dizendo quem sou e o que faço para viver.

Lammer é:

- O idiota
- O ingênuo
- O iniciante em um grupo de pessoas melhor preparadas
- O sem noção
- O considerado burro, que não aprende, seja por preguiça de estudar ou por que não tem a capacidade mental para entender o assunto



As cores dos chapéus

Você também vai ver por aí a definição de hacker pela cor do chapéu:

- **White Hat:** Hacker chapéu branco.
- **Gray Hat:** Hacker chapéu cinza.
- **Black Hat:** Hacker chapéu preto.

No dia a dia estes termos não são usados. Eles existem, aparecem em vários materiais hacker, tem imagens deles, mas não se usa estes termos. Porém como existem e fazem parte da cultura hacker você precisa conhecê-los.

O chapéu usado como símbolo geralmente é do modelo fedora (tem até um Linux com este nome e o chapéu é vermelho). O chapéu fedora se popularizou no filme Indiana Jones.



Vamos aos significados. Supostamente o hacker chapéu branco, o White hat, é o hacker do bem, o hacker ético. Supostamente o hacker chapéu preto, o black hat, é o hacker do mal.

Não existe um consenso quanto ao hacker chapéu cinza, o Gray Hat. Uns aceitam que é um ex-Black Hat. Outros – e eu concordo com eles – acreditam que a melhor definição para Gray Hat é o hacker que trabalha para os dois lados.

Na série – que eu recomendo muito – Mr. Robot, o hacker protagonista é um bom exemplo de Gray Hat. Ele trabalha como profissional de segurança da informação, o que o enquadraria como White Hat. Mas ele também executa ações hacker ilegais. Uma melhor representação do Gray Hat é impossível.

Como já disse, apesar de não usarmos estes termos no Brasil eles fazem parte da cultura hacker e vão aparecer em diversos materiais. Black Hat por exemplo é o nome de uma convenção de segurança da informação internacionalmente reconhecida:



Existem outros termos como newbie (novato), guru, larva, carder, etc. Nós achamos estas classificações uma grande bobagem. Seja porque não fazem sentido, seja porque a definição hacker já é ampla o suficiente para designar todo tipo de invasor. A imprensa usa o termo cracker para designar o Black Hat e usa também o termo Pirata da Internet. Nós acreditamos que todos são hackers, classificados em iniciantes, amadores e profissionais. É uma classificação que dá para mensurar. Quanto a ser do bem ou do mal, somos todos pessoas boas, capazes das piores maldades.





A importância do inglês para o hacker

Se você realmente quer levar a sério seu projeto de ser hacker ou de ser profissional de informática ou de segurança da informação, sinto muito mais você vai ter que aprender inglês.

O motivo é bem simples. O Brasil carece de pesquisadores e escritores técnicos e tudo o que diz respeito à informática e tecnologia da informação surge primeiro em inglês.

Se você ficar esperando eu e meia dúzia de escritores e blogueiros técnicos escrevermos ou traduzirmos o que surge em inglês, vai perder muito tempo. O melhor é você fazer como nós fazemos, ficamos sabendo das coisas assim que elas surgem (em inglês). Veja este exemplo.

No Brasil o primeiro autor a escrever sobre o Windows Server em português sou eu. Existem centenas de especialistas em Windows Server, mas ou não querem ou não sabem como transformar o conhecimento em livro.

Escrevi sobre o Windows 2000 Server, Windows Server 2003, Windows Server 2008 e 2008 R2, Windows server 2012 e 2012 R2 e recentemente sobre o Windows Server 2016. Desde o Windows Server 2008 leva dois anos para surgir um segundo livro em português sobre a mesma versão do Windows Server no livro que lancei.

Com o conhecimento hacker é pior ainda. No momento sou o maior autor hacker em língua portuguesa. E não é porque quero, é porque quase não temos escritores hacker.

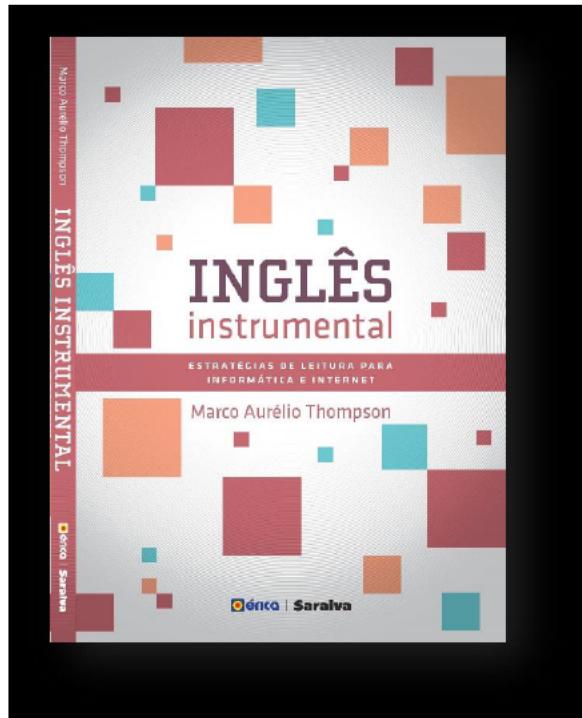
Algumas editoras nacionais lançam livros sobre hacking e segurança da informação. Mas se você reparar são livros traduzidos. São livros com dois a quatro anos desde que foram lançados no exterior no idioma original. Uma das edições do livro Hackers Expostos (Hacking Exposed) por exemplo, levou dez anos para ser traduzido para o português.

Como o livro surge depois da tecnologia, então acrescente mais um a dois anos em cada livro e estamos falando de uma defasagem de três a cinco anos entre o que tem no livro traduzido e o que ainda funciona.

Se hoje consigo ser o primeiro a escrever sobre o Windows Server em língua portuguesa e sou profundo conhecedor das mais diversas técnicas hacker, pode ter certeza de que foi graças a saber ler em inglês. O que me permite conhecer os assuntos assim que surgem, sem depender da boa vontade de alguém para traduzir e publicar, ou postar em blog em português.

Talvez você já tenha tentado aprender inglês e não foi bem-sucedido(a). O que eu posso fazer para te tranquilizar é dizer que tudo o que você precisa é aprender a ler em inglês. É muito mais fácil ler em inglês do que educar o ouvido para entender a fala ou tomar coragem para desenvolver a pronúncia.

Aprender a ler em inglês é uma questão de aquisição de vocabulário. Selecionei um trecho do livro de minha autoria **Inglês Instrumental: Estratégias de Leitura para Informática e Internet**. Acredito que possa ajuda-lo(a) a compreender a importância do inglês para leitura, não só para hackers, mas para todos que queiram estar na vanguarda das suas profissões.



Como se escreve “aquecendo os motores” em inglês?

Se você consultar um dicionário de inglês e traduzir palavra por palavra vai pensar que aquecendo os motores se traduz para o inglês como **warming the engines**. Não há porque pensar diferente, pois:

warm = aquecer

warming = aquecendo, aquecimento

the = os

engines = motores

Infelizmente esta tradução não está correta. O que há de errado? O erro é que não é assim que se fala ou escreve em inglês. Aquecendo os motores é traduzido para o inglês como **warming up the engines**. O que você deve estar se perguntando é de onde surgiu este **up** (para cima)? Assim não ficaria “aquecendo para cima os motores”? Por que é assim e não do jeito que nos parece mais correto?

A primeira lição que você precisa aprender para não ter dificuldade com o inglês é que inglês é inglês e português é português. Isto quer dizer que são línguas diferentes e não podem ser simplesmente comparadas palavra por palavra ou pelas mesmas regras gramaticais. Tentar aprender inglês partindo de uma ideia equivocada de ler traduzindo palavra por palavra tornará o aprendizado um pouco mais difícil.

Na frase que estamos usando como exemplo, **warming up** é uma construção grammatical conhecida como *phrasal verb*, ela dá novo significado às palavras que isoladas, têm significado diferente. Apenas aceite o fato de a frase do exemplo “aquecendo” ser warming up. Não há mais o que pensar sobre isto, é aceitar a diferença e pronto. Inglês é inglês. Português é português. Para aprender inglês devemos pensar em inglês, e isto inclui aceitar a língua como ela é, mesmo estranhando a formação de frases em outro idioma.

Crianças de até 7 anos aprendem idiomas com mais facilidade do que as maiores, os jovens e adultos. Isto ocorre porque o cérebro delas funciona como esponja. O senso crítico pouco desenvolvido reduz questionamentos desnecessários, muitos dos quais não precisam de explicações.

É diferente de explicar a um jovem ou adulto que uma palavra em português equivale, neste exemplo, a duas em inglês. No lugar de apenas aceitar que, neste contexto, “aquecendo” é *warming up*, o senso crítico questiona, atrasa e às vezes até bloqueia o aprendizado.

Para este início de conversa precisamos que você perceba esta diferença entre os idiomas. Que a tradução nem sempre é aos pares e que você precisa aceitar a língua inglesa como ela é, sem perder tempo tentando torná-la o português que você já conhece. Chegamos a um acordo? Então vamos prosseguir.

Aprender inglês é fácil ou difícil?

O que é fácil? O que é difícil? Aprender inglês é fácil ou é difícil? E aprender os ideogramas chineses ou o alfabeto cirílico russo? O inglês tem a vantagem de ser nosso conhecido desde a infância. Mais de duzentas palavras em inglês são de identificação imediata como *hot-dog*, *banana*, *love*, *brother*, etc. Isto é bem diferente dos ideogramas usados como palavras em outras línguas:



Tivemos a oportunidade de conversar com pessoas que aprenderam ou tentaram aprender inglês. O que descobrimos é bastante curioso. Muitos dos que disseram achar o inglês difícil sequer tentaram aprender. Convenceram-se que era difícil e sequer tentaram. Será este o seu caso? Falta de confiança no próprio potencial para o aprendizado?

Alguns chegaram a frequentar renomados cursos de idiomas, mas por apenas algumas semanas. Outros compraram livros e não passaram do primeiro capítulo, sequer tocaram nos exercícios. Coleções de idiomas em VHS, K-7, CD-ROM, DVD, ficaram com a maior parte da mídia ainda intacta, na embalagem.

Com a Internet, pensamos que as dificuldades para aprender outro idioma desapareceriam. Não foi bem o que ocorreu, e as dificuldades dos estudantes da década de 1990, quando começamos a lecionar idiomas, são praticamente as mesmas de hoje. Isto preocupa porque em 1990 não havia as facilidades da Internet.

O que está acontecendo? Por que um número expressivo de pessoas tenta aprender inglês e não consegue? É de fato tão difícil assim?

Não temos todas as respostas, cada caso é um caso. Mas a experiência de lecionar inglês em comunidades carentes, para jovens com dificuldade de se expressar na própria língua, comparada à experiência das aulas particulares para empresários e executivos, nos deu algumas pistas desta suposta dificuldade.

Aprender inglês deveria ser tão fácil quanto foi aprender a língua materna. E como aprendemos a língua materna? Certamente não foi na escola, pois as crianças emitem sons com poucas semanas de vida e por volta dos doze meses já conseguem alguma comunicação oral. E ninguém frequenta a escola com meses de idade. No máximo uma creche.

Não é a escola que nos ensina a língua materna. Ela é adquirida em casa, no convívio social ou familiar, com as pessoas estimulando, incentivando e dando o necessário feedback. Dia após dia, todos os dias desde o nascimento, o ser humano busca esta comunicação com os outros ao redor. Com a prática vem a perfeição e se hoje você é um jovem ou adulto articulado, tudo começou com o *gú-gú dá-dá* de anos atrás.

O papel da escola foi introduzir os sinais linguísticos e as regras para a comunicação escrita, complementando a comunicação oral. Começamos rabiscando, depois desenhando letras, formando sílabas, palavras, usando a pontuação corretamente. Até os dias de hoje, quando muitos de vocês já têm que lidar com as regras da Associação Brasileira de Normas Técnicas (ABNT) para a formatação de trabalhos acadêmicos.

Você achou fácil ou difícil aprender a língua materna? Talvez não consiga responder, porque foi um processo natural do seu desenvolvimento e é assim em qualquer parte do mundo: em Portugal, Angola, nos Estados Unidos, na China, na Rússia, na Alemanha, na Argentina ou em outro país. Ninguém considera difícil a língua materna, por mais difícil que pareça aos olhos dos outros. Por que não é assim quando aprendemos outro idioma?

Não é assim por vários motivos:

- **Interferência da língua materna:** a partir dos sete anos começamos a criar hábitos e barreiras que podem tornar-se obstáculos ao novo idioma.
- **Ausência de feedback:** nem todo estudante tem ao seu redor pessoas com as quais possa interagir no novo idioma. A falta de feedback desestimula e pode contribuir para hábitos de leitura equivocados. Este feedback é tão influente que muitos continuam trocando o R por L mesmo depois de adultos, a exemplo de porta e porca, pronunciado como polta e polca em algumas regiões do país.

- **Ausência de motivo:** o senso comum nos diz que precisamos aprender inglês, mas nem sempre os motivos são claros. Alguém com viagem marcada para o exterior vai se desenvolver mais em uma semana do que um estudante de cursinho em alguns meses. Ter um motivo forte para querer aprender outro idioma é fundamental.
- **Conflito de personalidade:** todos nós somos pessoas diferentes com personalidades diferentes. Esta particularidade precisa ser considerada em qualquer programa de aprendizado de idiomas. Quando falamos em aprender outros idiomas, estamos nos referindo a aprender a ouvir, falar, ler, escrever e conversar, compreender e ser compreendido. Por outro lado precisamos considerar que nem todos gostam de ler, escrever ou conversar. Geralmente existe uma predominância de uma habilidade sobre a outra. Alguém que não leia muito em português lerá menos ainda em inglês. Alguém introvertido, que converse pouco em português, conversará menos ainda em inglês. Alguém que não goste de escrever ou de falar, escreverá ou falará menos ainda em inglês. É importante alinhar com o inglês as habilidades que possua na língua materna: ouvir, falar, cantar, ler, escrever ou conversar. Precisamos identificar no que você se sobressai e usar esta força como facilitador da sua aprendizagem.

Segundo a Wolfram Research, através do serviço Wolfram Alpha, existe no mundo mais pessoas falando inglês (760 milhões) do que os nativos deste idioma (335 milhões). E no Brasil? Será que 100% da população fala português? Nada disso, apenas 89% dos brasileiros falam português. Outro fato curioso é que o inglês não é o idioma oficial dos Estados Unidos: é falado por apenas 67% da população. Ao aprender inglês, você estará apto a se comunicar com 760 milhões de pessoas ao redor do mundo, mas com apenas 67% dos americanos. O que acha disso? Experimente comparar inglês e

português digitando as palavras English-Portuguese no serviço online, acessível em:

www.wolframalpha.com

Em quanto tempo alguém aprende inglês?

Em quanto tempo você aprendeu a língua materna? Se pensar um pouco, não importa a idade que tenha, está aprendendo até hoje. Se já soubéssemos tudo sobre a língua portuguesa, as notas no Exame Nacional do Ensino Médio (Enem) e nos concursos públicos seriam sempre as melhores e não é bem isto o que acontece.

O que você acha do texto a seguir?

Projetar uma matriz acumuladora de números em BCD. Deve ter uma saída de carry para o próximo dígito. Utilizar uma EPROM 2764. (GARCIA; MARTINI, 2006)¹

É um exercício sobre memórias copiado de um livro de eletrônica digital, mas se você nunca estudou eletrônica digital, o mais provável é que não compreenda o texto, mesmo estando em português, sua língua materna. Também não entenderia um texto jurídico, de Engenharia, da área médica, da Biologia, a não ser que fosse da referida área.

Sempre existirá a necessidade de adaptação quando nos deparamos com termos técnicos, jargões, expressões populares, expressões com duplo sentido, gírias e tudo o mais que for estranho ao nosso repertório.

¹ Garcia, Paulo Alves; Martini, José Sidnei Colombo. ELETRÔNICA DIGITAL - TEORIA E LABORATÓRIO, 1a ed., São Paulo, Editora Érica, 2006.

Qual será então o tempo necessário para aprender inglês? Podemos estudar o idioma durante toda a vida e ainda assim haverá algo a ser aprendido. Mas não se preocupe. Da mesma forma que ocorre com o nosso idioma, só precisamos estudá-lo até não ser mais necessário o estudo. É quando o que sabemos é o suficiente para o que precisamos. Basta a manutenção.

O grande segredo é este. Você vai estudar inglês até ser suficiente para as suas necessidades. Nossos pais, em algum momento, deixaram de estudar português, mas até hoje aprendem palavras novas e conseguem identificá-las nos textos e conversas.

O que podemos fazer para ver se estamos com algum progresso é estabelecer metas realistas e mensuráveis, como até o final do ano conseguir ler textos adequados ao nosso universo com 70% de compreensão e sem o uso de tradutores.

Leia o artigo O Futuro das Línguas Inglesas, disponível em:

www.filologia.org.br/viicnlf/anais/caderno08

É de autoria do Rafael Lanzetti, um brasileiro que domina nada menos que 11 idiomas. Qual será o segredo dele?

English for Specific Purposes (ESP)

O livro trata do inglês instrumental, também conhecido como inglês técnico ou inglês para propósitos específicos, ou ainda ESP (English for Specific Purposes), no Brasil desde a década de 1970.

Alguns professores, escritores, pesquisadores e linguistas consideram inglês instrumental aquele que trata exclusivamente de uma das quatro habilidades necessárias ao domínio de outro idioma: ler, escrever, ouvir e compreender e falar e ser compreendido. Sob este ponto de vista temos o

inglês instrumental para leitura, para escrita, para conversar ou para desenvolver a compreensão auditiva.

Outros consideram o inglês instrumental essencialmente focado na leitura de textos, não havendo ensino de pronúncia, exercícios com diálogos ou compreensão auditiva.

O que nós percebemos é que o inglês instrumental dos cursos é focado em conversação e o inglês instrumental dos livros tem foco em leitura. Em ambos, o inglês instrumental procura contemplar alguma área ou atividade específica, como inglês instrumental para turismo, inglês instrumental para secretárias, inglês instrumental para taxistas etc.

O livro trata do inglês instrumental para informática com foco em leitura. Tem por finalidade ajudar você a compreender textos em inglês com o máximo de compreensão. A proposta é alcançar este objetivo em um curto espaço de tempo e, para fazer isto você precisa se comprometer a ler muitos textos, principalmente aqueles relacionados com a sua área de interesse. Em nosso caso, livros e textos sobre *hacking* e *information security*.

E quem não gosta de ler?

Seria bom se todos gostassem de ler e lessem muito. O fato é que existem pessoas de todas as idades que não gostam de ler. Alguns alegam não ter paciência, outros têm problemas de visão que os deixam com os olhos cansados ou irritados assim que começam a ler. Será este o seu caso? Consulte um especialista. Quem sabe não está aí o problema com a leitura?

Supondo não ser um problema de visão, mas apenas aversão a leitura, é importante você entender que nem sempre fazemos só as coisas que gostamos. Engarrafamento, transporte público superlotado, filas, trabalhar de segunda a sábado, são exemplos de atividades que desagradam, mas com

as quais muitos de nós precisamos lidar para atingir objetivos maiores ou apenas pagar as contas.

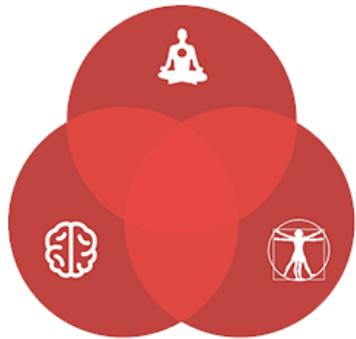
Quem não gosta de ler precisa entender que não tem que gostar de ler. Tem é que ler. Se gostar de ler, ótimo. Se não gostar de ler, leia do mesmo jeito. Quem é ou pretende trabalhar com informática precisa conseguir ler em inglês, até mais do que em outras profissões.

Você já ouviu falar de Internet das Coisas ou IoT (Internet of Things)? A IoT está sendo considerada uma revolução maior do que a própria Internet. Trata-se de conectar à Internet todo tipo de coisa, como objetos, construções, veículos, animais e até pessoas. Estima-se que em 2020 exista 38,5 bilhões de objetos conectados à Internet². Sabe quantos livros escritos em inglês tratam da Internet das Coisas? No momento da nossa pesquisa listamos 348 títulos no site www.amazon.com. Sabe quantos títulos em português existiam sobre a IoT em agosto de 2015? Nenhum.

Não se trata de gostar de ler. Trata-se de sair na frente. Reduzir a concorrência em uma vaga de emprego. De saber o que está acontecendo no mundo da tecnologia da informação e de se preparar para manter a empregabilidade. A IoT é apenas uma destas tecnologias que estão prestes a se propagar em larga escala. Não espere surgir livros sobre a IoT em língua portuguesa, porque quando isto acontecer o Brasil já estará importando a tecnologia. Uma tecnologia que você pode aprender, usar para desenvolver aplicativos (Apps) e ganhar dinheiro com isso começando agora. E este é só um exemplo do que a leitura pode fazer por você.



² <http://exame.abril.com.br/ciencia/mundo-tera-38-5-bilhoes-de-objetos-conectados-em-2020/>



HACK LIFE

integre corpo, mente e alma

Hackeando Tudo

Quando passei a entender exatamente quem os hackers são e o que fazem, percebi que já fazia hacks há algum tempo. Comecei hackeando telefones na década de 1980. Mas ninguém falava ou sabia o que era hacker e na verdade eu era um phreaker (hacker de telefone). Depois, com a chegada dos computadores em minha vida de adolescente é que me tornei um hacker, sem saber que era nisso que eu me tornava.

Acontece que no Brasil de poucos leitores e pouca gente estudada, hacker é o que aparece na imprensa de massa. Ou seja, hacker é sinônimo de invasor de computador. Não é que seja mentira, mas o hacker não é só isso.

Faz mais ou menos uns cinco anos que eu passei a estudar no exterior. Não é isso que você está pensando. Eu não saí do Brasil para estudar fora. Eu passei a usar a Internet para estudar no exterior. Você deve saber que as faculdades americanas ministram cursos pela Internet ou apenas disponibilizam o material das aulas. Entendi que se quisesse ser um cara bom eu precisaria estudar onde o conhecimento hacker surge primeiro: nos Estados Unidos da América (EUA).

A grande surpresa é que de uns dois anos para cá, em grupos de estudo que nada tem a ver com informática ou ciência da computação, começou a aparecer mensagens sobre Growth Hacking e Hack Life.

Hack Life eu já conhecia. Quando pesquisei sobre Growth Hacking descobri que é usado para se referir a ações inusitadas na área administrativa.

Explicando de outro jeito. O mundo está virando de cabeça para baixo. E não tem nada a ver com o fim do mundo bíblico. É a trajetória previsibilíssima da humanidade rumo a entropia.

Este cenário caótico-apocalíptico em que vivemos não encontra respostas nas indagações comuns nem nas teorias administrativas tradicionais, algumas com mais de cem anos desde que foram criadas.

O Growth Hacking nada mais é que uma abordagem “fora dos padrões” ou “fora da caixa” para alavancar startups ou reorganizar empresas com dificuldade para crescer no mercado.

Este é apenas um dos conceitos usando palavras com *hacker*, *hack* e *hacking* nos países de língua inglesa. No Brasil praticamente ficamos limitados a hacker como sinônimo de invasor de computador e queremos combate-los.

E Hack Life? O que é? Hack Life diz respeito a você hackear sua própria vida. Entenda – como já dissemos no início – o *hack* como macete, gambiarra, jeitinho, dica, atalho. Não confunda com o *jeitinho brasileiro* – sinônimo de trapaça – com o jeitinho como sinônimo de *hack*.

O que eu gostaria de propor a você – de novo – é que você não se limite a ser hacker de computador. Hackeie tudo. Encontre o atalho (o *hack*) para alcançar os objetivos que você se propôs e não está alcançado.

Procure por hacks para a casa, para o carro, para fazer limpeza, lidar com os pets, com as crianças, para a cozinha. Cultivando a mente hacker e fazendo hacks de todo tipo, seus hacks de computador também serão melhores e mais fáceis, pois você terá desenvolvido a mente hacker (*hacker mind*).



Fazendo Download do ISSUU

O site ISSUU (www.issuu.com) para quem não conhece, funciona como se fosse uma mistura de livraria e banca de revistas. Lá você encontra livros e revistas completos ou amostras. É no ISSUU que hospedamos amostras dos nossos livros pela Editora do Autor (www.editoradoautor.com) e também alguns livros completos, como os do projeto Wikilivros (www.wikilivros.org).

O problema é que alguns dos materiais disponibilizados no ISSUU não têm a opção para fazer download. Repare na imagem que abre este capítulo e verá que o botão download está desabilitado (está cinza em vez de branco).

Já funcionou, hoje não funciona mais, maximizar a janela de leitura, acessar compartilhar e lá encontrariam um botão de download oculto. Se você encontrar tutoriais ensinando desse jeito é passado. Não funciona mais.

O que você pode fazer para baixar o material de seu interesse que está no ISSUU é copiar o link do livro ou revista no ISSUU e colar no endereço:

<http://vebuka.com/>

O passo a passo é este:

1. Copie o link do material desejado no ISSUU
2. Cole no site <http://vebuka.com/>
3. Clique no botão **Download**
4. Aguarde terminar a conversão
5. Se a opção **Salvar como PDF** ou **Imprimir como PDF** não aparecer automaticamente, experimente usar o botão direito do mouse e **Salvar como...** (em PDF, é claro)

Assim você consegue salvar em PDF todos os materiais de seu interesse que estiverem no ISSUU, incluindo os nossos livros completos ou amostras.

Uma outra forma de se fazer isto, é instalando o programa JDownloader:

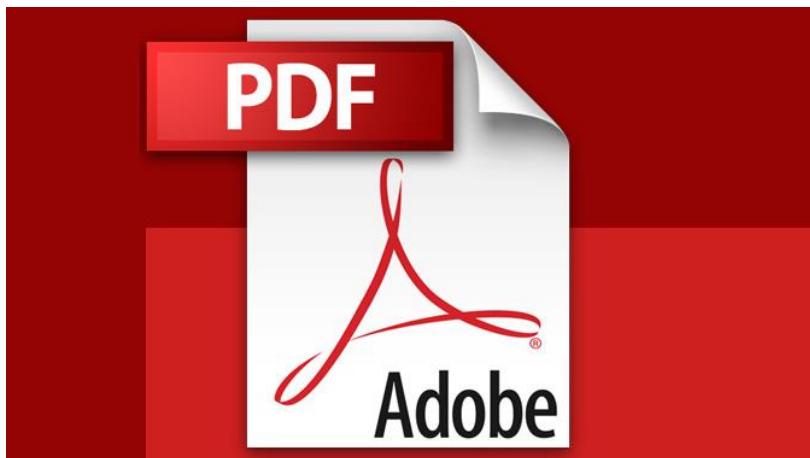
<http://jdownloader.org/download/index>

Este programa é um gerenciador de downloads e se ele estiver ativo e você copiar o link do ISSUU ele captura automaticamente o link e faz download do livro ou revista. Mas aqui tem um detalhe. O arquivo será salvo no formato JPG/JPEG, página por página. Veja neste mesmo volume da **Bíblia Hacker** como converter arquivos de imagem em PDF sem precisar ter programas instalados no computador.

Fizemos uma videoaula demonstrando este passo a passo. Ela está disponível em nosso grupo fechado, exclusivo para os clientes que adquirirem legalmente **A Bíblia Hacker**. Informe-se em:

www.fb.com/abibliahacker





Hacks com PDF

De acordo com a Adobe™ o PDF (Portable Document Format) ou Formato de Documento Portátil em português, é um formato de arquivo, desenvolvido pela própria Adobe Systems em 1993 para representar documentos de maneira independente do aplicativo, do hardware e do sistema operacional usados para criá-los.

Um arquivo PDF pode descrever documentos que contenham texto, gráficos e imagens num formato independente de dispositivo e resolução.

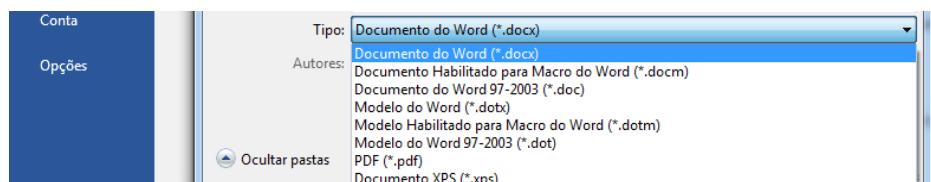
O PDF é um padrão aberto, e qualquer pessoa pode escrever aplicativos que leiam ou escrevam neste padrão. Há aplicativos gratuitos para Microsoft Windows, Apple Macintosh e Linux, alguns deles distribuídos pela própria Adobe. Também encontramos diversos aplicativos sob licenças livres.

Na prática os arquivos do tipo PDF estão em todos os lugares e você certamente deve ter de dezenas a milhares deles armazenados em seu computador. O TCC (Trabalho de Conclusão de Curso) por exemplo, na maioria das faculdades passou a ser entregue apenas em PDF. Sem a necessidade de ter uma versão impressa.

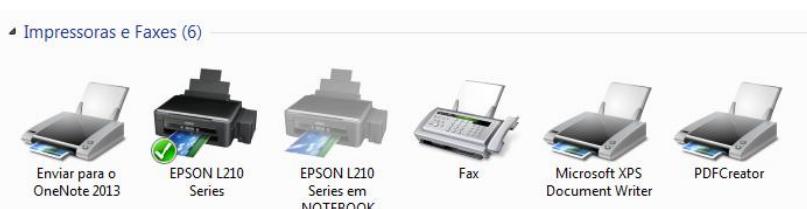
O que vamos ensinar agora são alguns truques (hacks) úteis para quem precisa criar e manipular arquivos em PDF:

1. Gerar arquivo PDF

Para gerar arquivos PDF você tem duas escolhas. A melhor e a mais simples é quando o programa gera o PDF como parte de seus recursos. As versões mais recentes do Word por exemplo, em **Salvar como...** tem a opção de salvar em PDF.



Usuários das versões mais antigas do Word ou de algum processador de textos que não tenha saída em PDF, vão precisar instalar uma **impressora PDF**. Nada mais é que um programa de computador que vai aparecer na lista de impressoras como **PDF Creator** ou outro nome parecido.



Recomendo o programa **PDF Creator**. É gratuito, não tem anúncios, é leve e você vai poder gerar arquivos PDF de qualquer coisa que possa imprimir: arquivos do Word, Excel, Powerpoint, Photoshop, etc.

<http://www.pdfforge.org/pdfcreator/download>

Lembre-se. Sempre que o programa tiver a opção de salvar ou exportar em PDF daremos preferência a salvar pelo programa em vez de usar uma impressora de PDF. A qualidade é melhor.

2. Ler arquivo PDF

Para ler arquivos no formato PDF o mais usado até pouco tempo é o programa da Adobe, o Adobe PDF Reader.

A propósito, a Adobe tem um programa que lê PDF e outro que gera PDF. Este que gera PDF é pago. O problema do leitor de PDF da Adobe é que ele é muito pesado e consome muita memória. Sugerimos um leitor de PDF mais leve, gratuito e sem propagandas como o Foxit Reader:

<https://www.foxitsoftware.com/pt-br/>

3. Desbloquear arquivos PDF

Não é tão comum como era há alguns anos encontrarmos arquivos PDF bloqueados. Ou seja, arquivos PDF com senha. Mas caso isto ocorra existem programas e sites que prometem revelar ou remover a senha dos arquivos PDF como por exemplo o:

<https://www.pdfcrack.com/pt/>

Basta subir (fazer upload) do arquivo PDF e o site removerá o bloqueio devolvendo um PDF desbloqueado, na maioria das vezes. Em nossos testes funcionou, mas como existem diversos geradores de PDF, pode ser que o programa gerador do PDF que você quer desbloquear seja incompatível com a tecnologia do site que vai desbloquear. Se não funcionar com o seu PDF, experimente também:

<https://smallpdf.com/unlock-pdf>

<http://www.ensode.net/pdf-crack.jsf>

<https://www.lifewire.com/free-pdf-password-remover-tools-2626181>

DICA: Gere você mesmo um PDF e coloque uma senha simples, como 1234. Assim você pode testar o site e ver se ele desbloqueia mesmo.

4. Proteger o PDF

Como já disse atualmente não é muito comum proteger (bloquear) arquivos PDF com senha. Mas caso você precise fazer isto é só verificar na hora de **Salvar em PDF** ou **Imprimir em PDF**, em **Opções** ou **Configurações** - depende de qual programa você está usando. Lá você encontrará a opção de criptografar e colocar senha no arquivo.

5. Converter para PDF

Pode ocorrer de você precisar converter arquivos para PDF como, por exemplo, a imagem de um diploma ou certificado para enviar como atividade complementar e às vezes não tem o programa que faça isso.

A solução é bem simples, basta acessar um dos sites que indicamos abaixo para converter praticamente qualquer arquivo em PDF, até mesmo usando o celular:

<https://www.convert-jpg-to-pdf.net/>

<http://www.convertfiles.com>

<https://www.pdftoword.com/pt/>

DICA: Às vezes quando temos um arquivo PDF bloqueado conseguimos desbloquear o arquivo fazendo a conversão do PDF para outro formato.

6. Unir vários arquivos PDF (merge)

Na faculdade pode ocorrer de você precisar entregar vários documentos em um único arquivo PDF. Eu e meus colegas passamos por isto quando precisamos entregar vários certificados de atividades extracurriculares ou vários relatórios de estágio reunidos em um único arquivo PDF. O site a seguir resolve o problema:

<https://www.pdfmerge.com/>

7. Converter PDF em imagem

Também pode ocorrer o contrário. Você tem um arquivo em PDF e precisar converte-lo em imagem. Falsários costumam fazer isto para adulterar documentos em PDF, como diplomas, boletos, etc. Eles convertem em imagem e adulteram a imagem no Photoshop. Depois convertem de novo em PDF. Só espero que não seja sua intenção, mas caso precise converter PDF em imagem acesse:

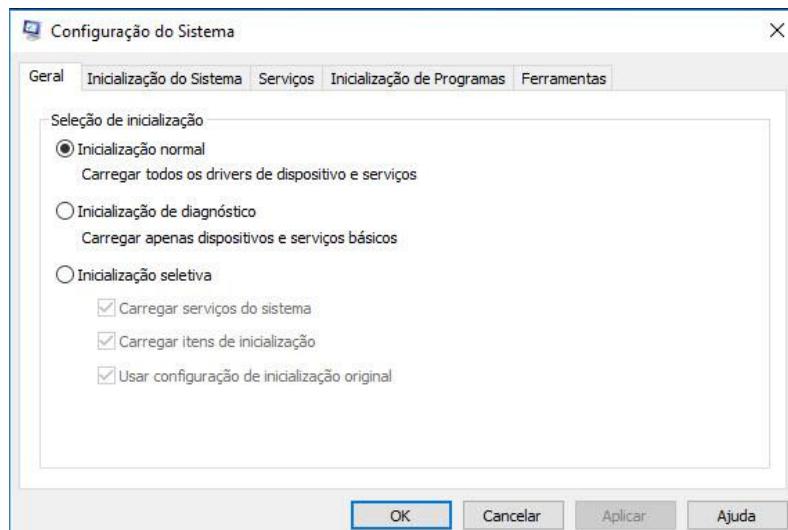
<https://pdf2jpg.net/>



O que inicia junto com o Windows?

Quando você liga o computador rodando o Windows (Linux ou Mac também), vários programas iniciam juntos sem que você perceba. Particularmente no Windows a possibilidade de alguns destes programas serem indesejáveis é muito grande. Tanto o usuário preocupado com a segurança do próprio computador, quanto o hacker e o profissional de segurança, todos precisam ter conhecimento e controle sobre o que inicia junto com o Windows.

Mas como saber quais programas estão iniciando junto com o Windows? No Windows 7, 8 ou 10 acesse **Pesquisar**, digite **msconfig** e pressione **ENTER**. Vai aparecer para a janela **Configuração do sistema**:



Observe as abas com as opções:

- **Geral**
- **Inicialização do Sistema**
- **Serviços**
- **Inicialização de programas**
- **Ferramentas**

Você consegue descobrir se existe algum arquivo malicioso roubando dados ou consumido a largura de banda da sua conexão com a Internet. Por aqui também dá para descobrir porque o computador está lento, travando e podemos até resolver estes problemas. Vamos ver como.

Em **Geral** temos opções de boot (reiniciar) normal, modo de segurança e a inicialização seletiva, que permite selecionar o que vai ser executado ou não. Em **Inicialização do Sistema** você consegue acelerar a inicialização do Windows fazendo alguns ajustes.

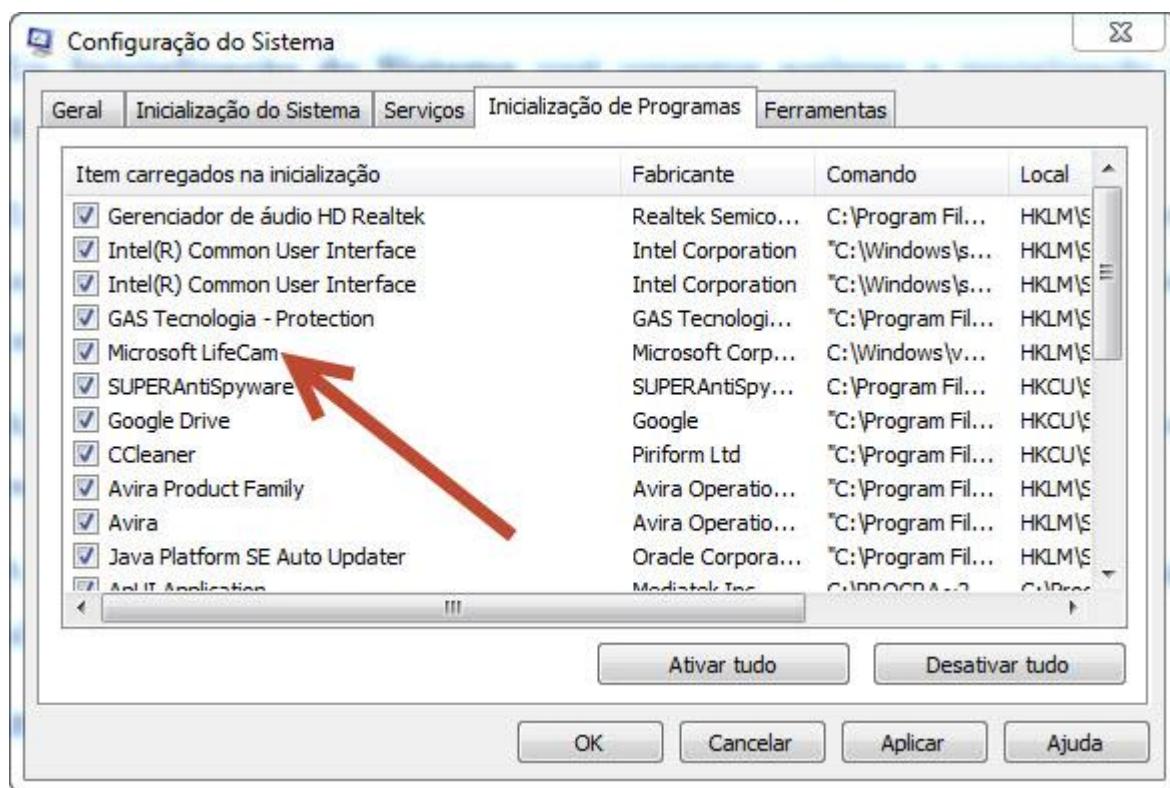
Em **Serviços** você encontra a lista de serviços (programas) que podem estar na condição de **Parado** ou **Em Execução**. Use algum tempo analisando cada um dos serviços para ver se encontra algo que não deveria estar ali.

Alguns nomes de serviços são autoexplicativos. Os que você não conhecer recomendo uma pesquisa no seu mecanismo de buscas preferido.

A aba **Inicialização de Programas** é a que mais vai nos interessar porque ali estarão os programas que iniciam junto com o Windows. É extremamente importante que você verifique programa por programa, compreendendo cada um deles e desmarcando todos aqueles que julgar desnecessários para iniciar junto com o Windows.

Na figura a seguir a Webcam da Microsoft (Microsoft LifeCam) não estava mais instalada no computador. Mesmo assim continuava a ser carregada,

ocupando espaço na memória RAM e contribuindo para a lentidão do sistema como um todo:



Na mesma imagem vemos o CCleaner que é um programa de limpeza do sistema que não precisa iniciar junto com o Windows. O CCleaner pode ser executado semanalmente, sem precisar ser inicializado junto com o Windows.

Em Inicialização de Programas você vai encontrar:

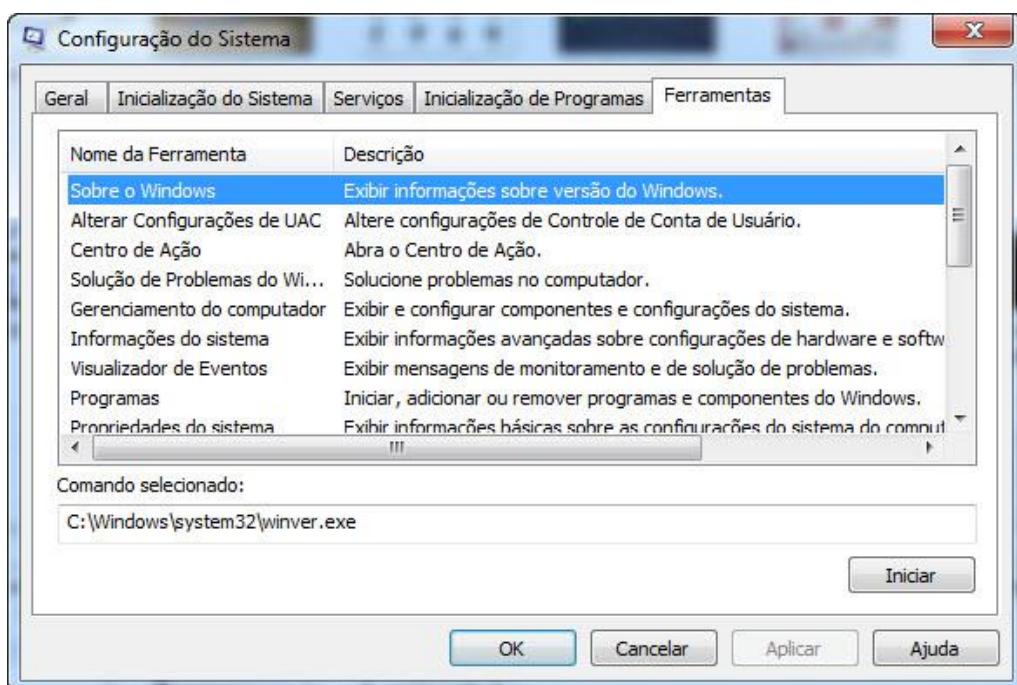
- Softwares de segurança, como antivírus, firewall de outros fornecedores além da Microsoft, antispyware, etc.
- Drivers e gerenciadores quando existem, tanto de áudio quanto de vídeo.
- Java.
- Programas que fazem a atualização automática de outros programas (Auto Updater).
- Software de segurança de alguns bancos (Ex.: GAS Tecnology).

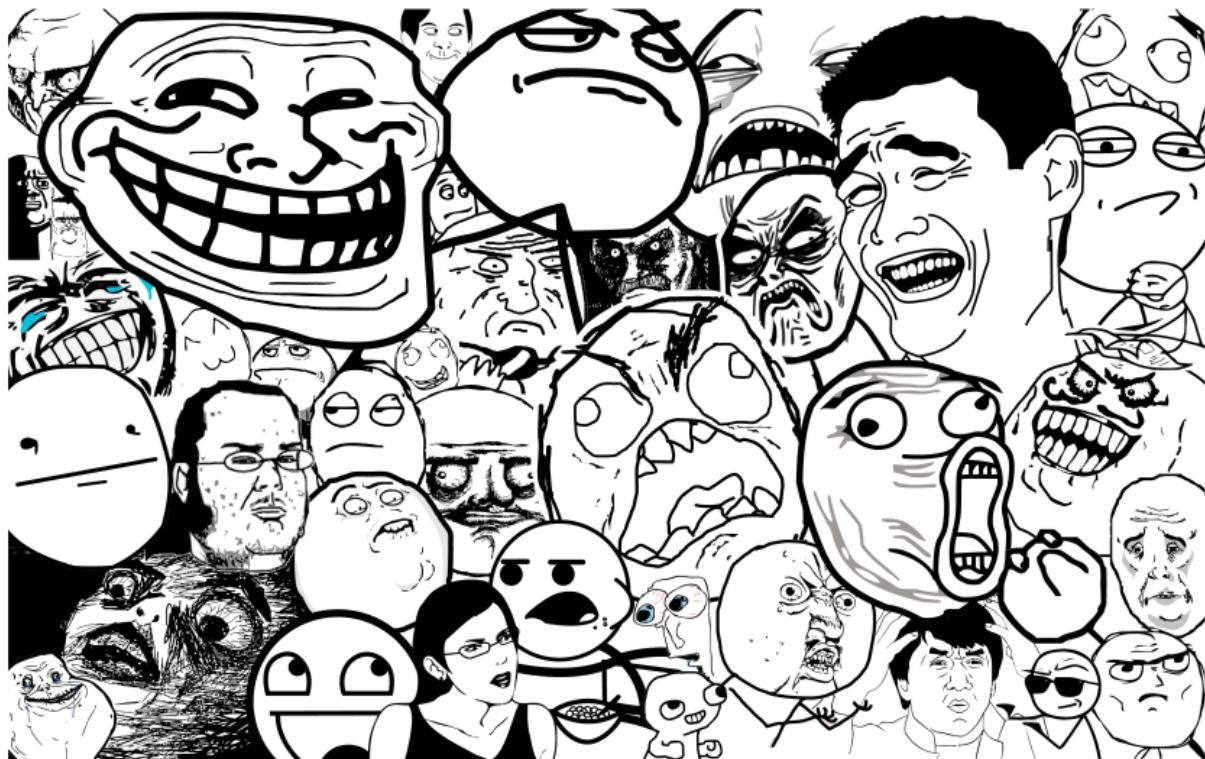
- Softwares gerenciadores de download.
- Softwares de captura de tela.
- Softwares desconhecidos.
- Softwares suspeitos (Ex.: keylogger, trojan, etc.)

Aqui não existe atalho. Tem que ver um por um, usar o bom senso, desabilitar tudo o que não for necessário e pesquisar pelo nome o que encontrar e não saber se deve manter ou desmarcar.

Exemplo: vamos supor que você tenha instalado um software de captura de tela como o Snagit da TecSmith. A instalação padrão inclui fazer o Snagit iniciar automaticamente junto com o Windows. Mas se você só vai fazer captura de telas de vez em quando, não há porque deixar o Snagit inicializando com o Windows, ocupando espaço na memória e consumindo parte do processamento.

Finalmente chegamos a **Ferramentas**. É uma janela com atalhos para diversas ferramentas úteis no dia a dia do técnico, do hacker ou do profissional de segurança que faz manutenção no Windows. Basta selecionar a ferramenta desejada e em seguida clicar em **Iniciar**.





Memes

Meme¹ é algo que se tornou um fenômeno na Internet. Geralmente são fotos, desenhos, canções ou vídeos que se popularizam de forma muito rápida e praticamente se tornam celebridades na rede mundial de computadores.

Hackers precisam saber o que é meme (e como cria-los) por dois motivos:

- Não dá para acreditar que alguém seja hacker e não saiba o que é meme.
- Memes são usados para disseminar vírus, cavalos de Tróia, arquivos maliciosos e também encontram uso na engenharia social.

¹ Meme é um termo criado em 1976 por Richard Dawkins no seu bestseller O Gene Egoísta e é para a memória o análogo do gene na genética, a sua unidade mínima. É considerado como uma unidade de informação que se multiplica de cérebro em cérebro ou entre locais onde a informação é armazenada (como livros). No que diz respeito à sua funcionalidade, o meme é considerado uma unidade de evolução cultural que pode de alguma forma autopropagar-se. Os memes podem ser ideias ou partes de ideias, línguas, sons, desenhos, capacidades, valores estéticos e morais, ou qualquer outra coisa que possa ser aprendida facilmente e transmitida como unidade autônoma. O estudo dos modelos evolutivos da transferência de informação é conhecido como memética.

Tipos de memes:

- Fotos, geralmente com mensagens e rage faces.
- Vídeos e GIF animado: gafes, trolagens, pegadinhas, receitas culinárias, hacks de todo tipo, saúde, comerciais de TV, pessoas construindo coisas, obras, pessoas demonstrando perícia, nostalgias.
- Motivacional e Desmotivacional
- Citações, provérbios e versículos bíblicos.
- Músicas.
- Notícias (geralmente falsas ou manipuladas).
- Gafes de artistas, políticos, celebridades, também de pessoas comuns, como a menina que escorregou em uma poça d'água antes de entrar no restaurante e foi parar até no programa Fantástico da Rede Globo.
- Rage faces na forma de cartum ou história em quadrinho (banda desenhada).

Basicamente, meme é um conceito que se espalha rapidamente na internet e um dos principais memes da internet são as **rage faces**, que demonstram várias expressões faciais comumente adotadas pelas pessoas. Você já deve ter visto alguns destes por aí:



Com traços simples, os memes de carinhas são usados para expressar uma série de sentimentos (da raiva à frustração), além de serem protagonistas de (muitas) piadas na internet. A carinha que aparece no centro, na imagem acima, foi a primeira de que se tem registro. Você pode fazer um passeio pelos memes de diferentes épocas no Museu Virtual de Memes, em:

www.museudememes.com.br

Alguns foram feitos a partir de fotos reais, como este do Yao Ming²:



Agora que você já sabe ou refreshou a memória sobre o que é meme, chegou a hora de cria-los. E já foi tempo em que era necessário saber Photoshop para criar memes. Agora você pode fazer isto online. Mas antes faça um teste para saber se você conhece o significado das diversas expressões rage faces.

Já pensou na confusão se a expressão não tiver relação com o que você quis dizer?

<https://tecnologia.uol.com.br/quiz/2014/05/23/qual-e-o-meme-veja-se-voce-sabe-os-nomes-dessas-carinhas.htm>

URL encurtada: <http://goo.gl/1gbpmy>

Agora prepare-se para fazer seus próprios memes. Uma das grandes habilidades esperadas de um hacker é a capacidade de persuasão, de convencer as pessoas a clicar em links, botões, curtir postagens. Sem esta habilidade os ataques em massa como o de negação de serviço (DoS e DDoS) ou propagação massiva de código malicioso (PMCM) tornam-se impossíveis.

Vamos começar pelo pôster desmotivacional (que também pode ser usado como motivacional).

² Chinês, ex-jogador de basquetebol que atuava na NBA. Com 2,29 m de altura foi um dos jogadores mais altos da história da NBA.

O site é este:

<https://imgflip.com/memegenerator>

Para criar o meme basta inserir alguma imagem ou usar uma das disponíveis. Depois é só escolher um texto para a parte de cima (TOP TEXT) outro para a parte de baixo (BOTTOM TEXT) e clicar em **Generate Meme**:



O próprio site, após a criação do meme, exibe botões para você compartilhar sua criação nas redes sociais. Memes também podem ser criados no smartphone. Procure na loja de aplicativos usando as palavras MEME MAKER ou MAME GENERATOR ou MEME CREATOR ou ainda MAME WIZARD. Vai encontrar vários programas, todos fáceis de usar.

Outro site parecido com o anterior e que em nossa opinião produz um resultado final ainda mais atraente é este:

<http://www.imagechef.com/meme-maker>

Choose a popular meme template or upload your own photos to generate funny memes. You can easily share your creation with friends on social networks.

VOCÊ ESTÁ ENTENDENDO

O QUE É SER HACKER?

Warning: All uploads and work will be lost when you leave unless you sign in! [Registre-se](#) | [Fazer o Login](#)

FOTOS

WHAT IF I TOLD YOU

+ Camera Carregar nova foto

Tirar um Snapshot

Salvar

COMPARTILHAR

f Facebook

t Twitter

r Reddit

e E-mail

Obter imagem

Antes que você pense que conhecer meme é um desperdício de tempo, eu preciso te dizer que existem vagas de emprego para quem consegue criar bons memes.

A maioria destas vagas (no Brasil) está em São Paulo. Nada impede de você candidatar-se mesmo morando em outra região do Brasil. Os memes podem ser criados a partir da sua casa, quarto ou até mesmo de uma Lan House ou aparelho celular. Primeiro torne-se conhecido por criar bons memes, aqueles que ganham muitos likes. Depois apresente-se para o mercado. As agências de marketing digital (que não param de crescer) precisam de você.

Mais alguns sites que permitem criar memes com qualidade e facilidade:

<http://www.memes.com/generator>

<https://makeameme.org/>

<https://www.memecreator.org/create>



WHY U NO MEME GENERATOR



Upload Your Own Meme Template

Popular Memes Add Image Search

8th Grader

Actual Advice Mallard

adasi

Asdf

Asian Father

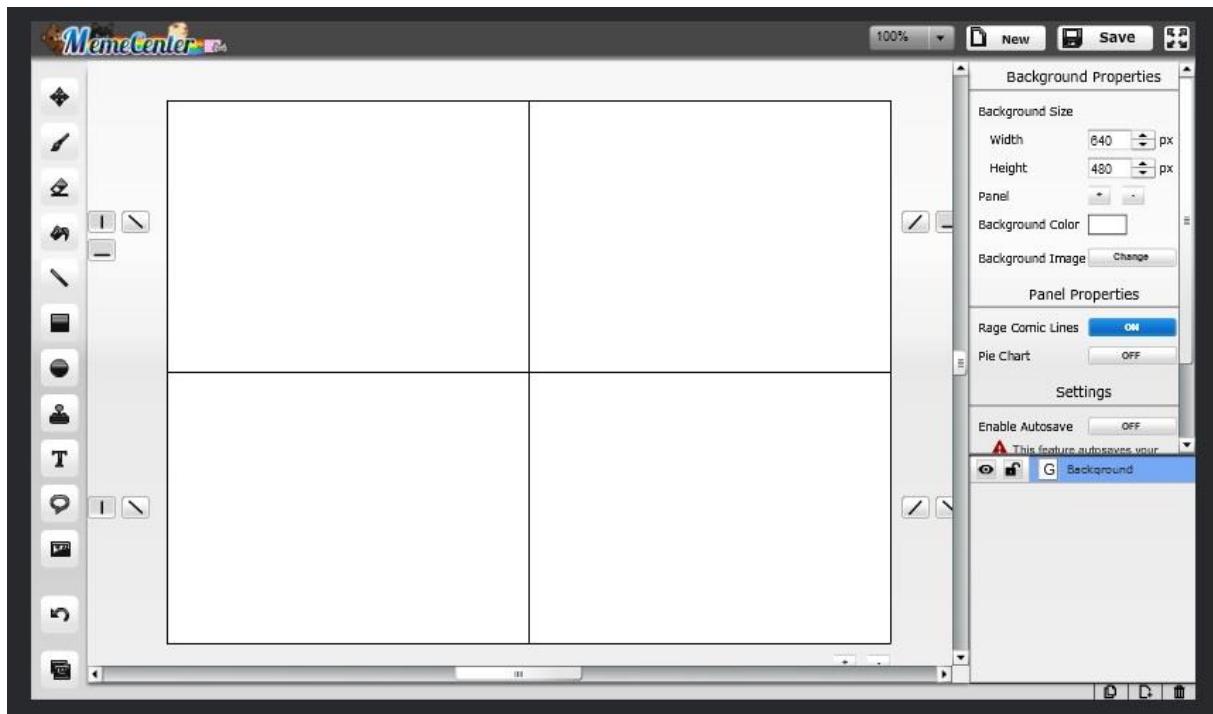
Awkward Moment Seal

Memes na forma de charges e histórias em quadrinho

Memes do tipo pôster talvez exijam mais criatividade do que os memes na forma de histórias em quadrinho e cartuns. Os sites que sugerimos até aqui são específicos para o meme no formato imagem ou pôster. A próxima sugestão é de um site que cria memes dos seguintes tipos:

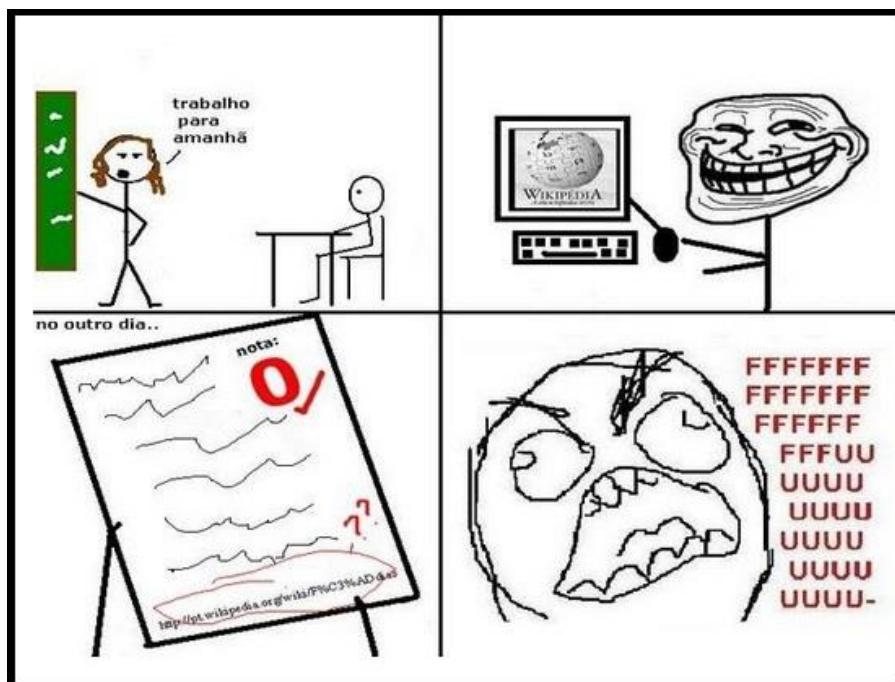
- Página branca para você começar do zero
- Imagem com texto
- Pôster com tarja preta em volta
- Rage Comic (história em quadrinho com rage faces)
- Gráficos

<https://www.memecenter.com/memebuilder>



Perceba que ele é bem completo e talvez você leve um pouco mais de tempo para criar seus memes. A vantagem é que por ser mais trabalhoso, as chances de alguém usá-lo são menores. As pessoas costumam preferir os geradores de meme que dão menos trabalho.

São quatro quadros para você criar uma história completa, veja o exemplo:



A estratégia segue um formato mais ou menos previsível que pode pegar emprestado a narrativa da Jornada do Herói³:

1. O primeiro quadro oferece um desafio, problema, proposta, obstáculo ou questionamento.
2. O herói tenta resolver o desafio, problema, proposta, obstáculo ou questionamento.
3. Aparece um contratempo, imprevisto, reviravolta.
4. O herói aparece bem-sucedido ou humilhado e fracassado, que é o mais comum nos memes.

Baseado nestas orientações podemos roteirizar um meme assim:

NOTÍCIA DE FERIADO PROLONGADO.	FACE 1: VOU SAIR MAIS CEDO PARA NÃO PEGAR TRÂNSITO NA ESTRADA.
IMAGEM DA CIDADE TODA PENSANDO ALTO: VOU SAIR MAIS CEDO PARA NÃO PEGAR TRÂNSITO NA ESTRADA.	FACE 2 (QUE SAIU ATRASADO, EM VEZ DE MAIS CEDO E ENCONTRA A ESTRADA DESERTA): UÉ? CADÊ TODO MUNDO?

No projeto acima o herói se vê diante de um obstáculo: as estradas estarão lotadas de automóveis devido ao feriado prolongado, segundo a notícia.

Nosso carinha pensa que a solução é sair mais cedo para fugir do trânsito. O problema é que a cidade toda tem a mesma ideia e todos acabam no engarrafamento, mesmo saindo mais cedo. É o contratempo.

A redenção aparece no final quando um segundo carinha, que não saiu mais cedo, acaba encontrando as entradas vazias com o trânsito bom.

Agora pratique, pois é assim que se faz meme de historinha.

³ O monomito (às vezes chamado de "Jornada do Herói") é um conceito de jornada cíclica presente em mitos, de acordo com o antropólogo Joseph Campbell. Como conceito de narratologia, o termo aparece pela primeira vez em 1949, no livro de Campbell *The Hero with a Thousand Faces* ("O Herói de Mil Faces").



Invasão de e-mail

Apesar de nós termos um curso específico de invasão de e-mail (procure no site www.amazon.com.br por **Curso de Recuperação de Contas de e-mail**) decidimos incluir na **Bíblia Hacker** orientações mais aprofundadas sobre o assunto.

Porque no curso formado por livro impresso mais videoaulas, fomos direto a prática, com a teoria mínima necessária. Dá para fazer muita coisa, mas você conseguirá recuperar/invadir contas que não dependam de ataques ao servidor.

Se a intenção for aprender invadir contas de e-mail diretamente no servidor você vai precisar de um entendimento da teoria maior do que o que damos no Curso de Recuperação de Contas de e-mail.

E quando falamos de recuperação de contas de e-mail estamos falando também da invasão de redes sociais, uma vez que o acesso a elas é feito por e-mail, como nome de usuário, e senha.

Vamos conhecer um pouco da teoria relacionada a invasão de e-mail e depois veremos algumas formas de invadir e-mail, começando por como fazer isto usando telnet. A propósito, o conteúdo da **Bíblia Hacker** sobre invasão de

e-mail será voltado a invasão de e-mail em servidores. O **Curso de Recuperação de Contas de e-mail** (vendido separadamente) é direcionado ao usuário leigo, com foco na recuperação de e-mail a partir de computadores de usuários.



Origem e Funcionamento do Correio Eletrônico

Talvez você se surpreenda ao saber que o correio eletrônico foi criado antes da Web e independentemente da Internet. Abordaremos alguns conceitos fundamentais que você precisa conhecer ou rever antes de chegar aos servidores de e-mail.

Breve história da Internet

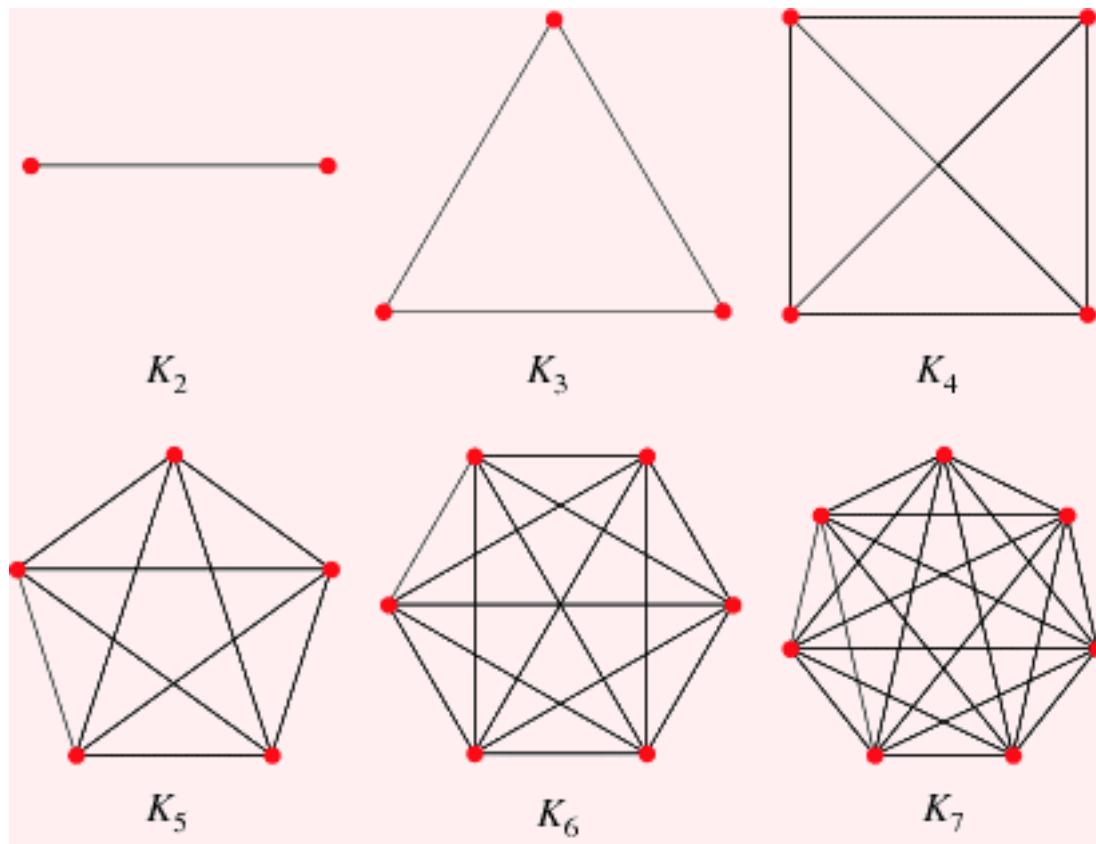
Após a Segunda Guerra Mundial (1939-1945) a extinta União Soviética e os Estados Unidos da América emergiram como superpotências mundiais, porém antagônicas.

Devido ao poderio nuclear destas grandes nações, se houvesse uma terceira Grande Guerra, o planeta poderia ser destruído um certo número de vezes. Apesar de ninguém querer isto, se preparavam para o pior.

Este período de grande tensão mundial ficou conhecido como Guerra Fria (1945-1991). Estimulou o desenvolvimento de tecnologias de defesa, incluindo um sistema de comunicações imune a ataques nucleares.

Na ilustração abaixo vemos grafos, o modelo que deu origem à Internet:

Em um grafo completo todo vértice é adjacente a todos os outros vértices



Use o dedo para tapar qualquer um dos círculos, chamados de nós ou vértices, e vai perceber que enquanto houver pelo menos dois vértices a comunicação se estabelece.

A ARPANET foi a principal rede de comutação de pacotes que posteriormente deu origem à Internet. Em 1971 havia quinze hosts conectados à ARPANET. A título de comparação, o número de sites web atualmente ultrapassa o bilhão. Se você pensar que em 1991 só havia um site no mundo, em 1992 eram 10 sites em todo o mundo, em 1993 eram 130

sites e apenas 22 anos depois, em 2015, o número de sites ultrapassa o bilhão, o que devemos esperar da Web nos próximos dez anos?

Com um bilhão de sites e crescendo, é difícil imaginar algo que ainda não tenham feito na Web. Se você tiver curiosidade em saber quantos sites existem no mundo no momento em que estiver lendo isto, acesse este contador on-line:

<http://www.internetlivestats.com/total-number-of-websites/>

Com o fim da Guerra Fria o governo americano começou a ser pressionado para liberar a Internet ao uso civil. Este processo ocorreu principalmente na década de 1980, sendo concluído a partir da década de 1990. O nome Internet começou a ser usado no início dos anos 1970 e acabou se tornando sinônimo desta grande rede. No Brasil a Internet comercial teve início em 1995.

Breve história do e-mail

A tecnologia que deu origem ao e-mail surgiu na década de 1970 quando, em 1971, o engenheiro e programador estadunidense Ray Tomlinson, enviou a primeira mensagem de correio eletrônico de que se tem notícia. O conteúdo exato da mensagem é desconhecido. Nas inúmeras entrevistas disponíveis na Internet o autor acredita ter sido QWERTYUIOP, que está mais para um exercício de digitação do que para uma mensagem.

A primeira versão do programa de correio eletrônico era um aplicativo simples, nomeado SNDMSG, letras retiradas da frase em inglês **SeND MeSsaGe**, ou Enviar Mensagem, em português.

Esta primeira versão era muito limitada, pois só permitia enviar mensagens para alguém conectado ao mesmo computador. É algo tão estranho quanto falar pelo celular com alguém sentado ao seu lado.

O SNDMSG foi aperfeiçoado e incluiu um protocolo de comunicação mais sofisticado, permitindo o envio e recebimento de mensagens pela ARPANET.

O símbolo @ (lê-se arroba) foi adotado para identificar a origem da mensagem. O símbolo arroba é o mesmo que *at* em inglês. Traduzido para o português, *at* é a preposição **em**.

Quando lemos um endereço de e-mail queremos dizer:

[nome do usuário] [**em**] [local]

Tomando como exemplo o e-mail **professor@marcoaurelio.net**, temos:

Nome do usuário	em	Local, ou seja, o nome de domínio atribuído ao servidor de e-mail
professor	@	marcoaurelio.net

O nome de usuário pode se repetir, mas não no mesmo servidor. Se assim fosse, como o servidor de e-mail saberia separar as mensagens de cada usuário? Você já passou pela experiência de criar uma conta de e-mail escolhendo um nome de usuário e este nome de usuário não estar disponível? A partir do que você acabou de aprender sobre a origem do e-mail, consegue entender o porquê de alguns nomes de usuário não estarem disponíveis?

Breve história da Word Wide Web (WWW)

Não devemos confundir a WWW ou Web com a Internet. A Internet é uma rede de comutação de pacotes que interliga outras redes ao redor do mundo. A Internet funciona como uma grande rodovia por onde passam dados e informações e, por conta desta analogia, por um bom tempo as pessoas se referiam a Internet como a superestrada da informação.

Se a Internet é uma rodovia a Web está mais para posto de conveniência, onde você para quando encontra os serviços que está procurando.

O nome Web é uma simplificação de World Wide Web, também conhecida pela sigla WWW, ou Teia Mundial. Quando você acessa um site na Internet está acessando a Web usando a Internet. O principal conteúdo da Web é o site que, como vimos, já ultrapassa o bilhão.

O recurso que popularizou o uso da Web foi o hipertexto, o vínculo de uma página a outra. Toda vez que você clicar em um link de uma página Web, está usando o hipertexto ou hipermídia, pois nem todo link remete a texto.

Certamente a Internet não teria se desenvolvido no ritmo que se desenvolveu se não fosse a Web. E a Web também não seria tão atraente se os links não existissem. Faça o teste. Acesse qualquer site e tente descobrir como seria a mesma página Web se ela não tivesse links para te tirar dali.

A Web foi desenvolvida entre as décadas de 1980 e 1990 pelo físico Tim Berners-Lee no CERN, Organização Europeia para a Investigação Nuclear com sede na Suíça.

Um computador NeXTcube da Apple (veja figura) foi usado por Tim Berners-Lee como primeiro servidor Web e também para escrever o primeiro navegador, o WorldWideWeb.



No final de 1990 ele já havia construído todas as ferramentas necessárias para um sistema: o navegador, o servidor e as primeiras páginas Web. O dia 6 de agosto de 1991 marca a estreia da Web como um serviço publicado na Internet e se você voltar e ler nossa contagem de web sites no tópico sobre a história da Internet, vai perceber que o único Web site existente na Web em 1991 era sobre o projeto WWW.

The screenshot shows the first version of the World Wide Web homepage. It features a dark background with white text and several blue hyperlinks. The title "World Wide Web" is at the top. Below it is a paragraph of text, followed by a list of links under various categories: "What's out there?", "Help", "Software Products", "Technical", "Bibliography", "People", "History", "How can I help?", and "Getting code". Each category has a brief description and a link to more information.

World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), November's [W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)
Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)
on the browser you are using

[Software Products](#)
A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#))

[Technical](#)
Details of protocols, formats, program internals etc

[Bibliography](#)
Paper documentation on W3 and references.

[People](#)
A list of some people involved in the project.

[History](#)
A summary of the history of the project.

[How can I help?](#)
If you would like to support the web..

[Getting code](#)
Getting the code by [anonymous FTP](#), etc.

Ele continua online em:

<http://info.cern.ch/hypertext/WWW/TheProject.html>

Conceitos importantes

Veremos agora alguns conceitos importantes que vão ajudar você a entender o funcionamento e administração dos servidores de e-mail, o primeiro passo para quem pretende depois, invadi-los.

Autenticação

Autenticação é o ato de verificar se é autêntico. No contexto dos servidores de e-mail é quando você fornece as credenciais que o identificam no sistema em que está cadastrado. Geralmente estas credenciais são o nome de usuário

e a senha de acesso, mas pode incluir algo mais como por exemplo, a biometria, certificado digital, etc.

Cliente de e-mail

Cliente de e-mail é o nome genérico para todo software de correio eletrônico, responsável pelo envio e recebimento de e-mail. Quando o cliente de e-mail é uma página Web, o nome é Webmail.

Alguns clientes de e-mail populares:

- Apple Mail no Mac OS
- Eudora
- Gmail
- Hotmail
- Incredimail
- Kmail no Linux
- Mozilla Thunderbird
- Opera
- Outlook
- Pegasus
- Yahoo!

Estrutura da mensagem

As primeiras mensagens de e-mail eram simples e limitadas a um pequeno texto, similar ao SMS (Short Message Service). A tecnologia evoluiu e, apesar da aparente simplicidade, as mensagens de e-mail atuais são repletas de recursos, como veremos a seguir. Usaremos o nome em inglês porque é como vai aparecer nas opções de configuração dos servidores de e-mail e nas linguagens de programação:

- **From** (De): este campo contém o endereço eletrônico do remetente. Geralmente é preenchido automaticamente pelo cliente de e-mail. Equivale ao nome de usuário cadastrado no servidor de e-mail.
- **To** (Para): este campo contém o endereço eletrônico do destinatário da mensagem.
- **CC** (Carbon Copy ou em tradução livre, Com Cópia): este campo contém um ou mais endereços de destinatário. Para mais de um destinatário os endereços são separados por vírgula.
- **BCC** (Blind Carbon Copy ou em tradução livre, Com Cópia Oculta): este campo também contém um ou mais endereços de destinatário separados por vírgula. A diferença em relação ao CC é que o destinatário não visualizará o e-mail de quem está recebendo cópia da mensagem.
- **Subject** (Assunto): este campo contém uma breve descrição do conteúdo da mensagem.
- **Attachment** (Anexo): é um recurso que permite incluir arquivos com a mensagem. Por questões de segurança arquivos com extensão exe, com, vbs, entre outras, são bloqueados no servidor.
- **Body** (Corpo): é o texto da mensagem.

Além destes identificadores existem outros menos comuns, como;

- **Priority** (Prioridade): define a prioridade da mensagem.
- **Encoding** (Codificação): determina o tipo de codificação da mensagem, uma codificação errada exibe caracteres estranhos no lugar dos acentos).
- **BodyAsHtml** (Mensagem em HTML): indica que o texto da mensagem deve ser interpretado como HTML.
- **UseSSL** (Criptografado): indica que o remetente usa um certificado digital e a mensagem é criptografada.

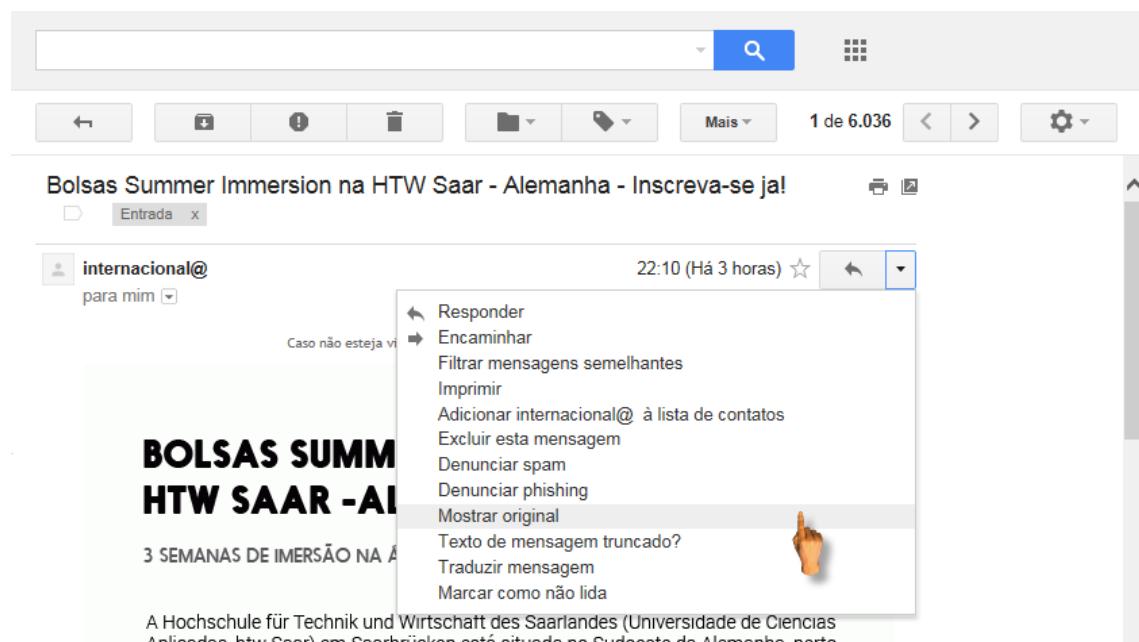
E-mail Header

Header quer dizer cabeçalho e e-mail header é o cabeçalho do e-mail. Uma seção com informações importantes sobre o servidor do remetente e a rede que deu suporte ao envio.

Quando existem dúvidas sobre a origem e autenticidade de uma mensagem de e-mail, o que devemos fazer é analisar o cabeçalho em busca de evidências que comprovem a autenticidade e origem da mensagem.

O cabeçalho do e-mail é oculto por padrão e cada cliente de e-mail possui uma forma própria para exibi-lo. No GMail você exibe o cabeçalho do e-mail acessando a opção **Mostrar original** na mensagem que estiver visualizando:

Opção do GMail para exibir o e-mail Header



Hoax

Hoax é uma palavra da língua inglesa que quer dizer boato. O hoax se tornou fonte de preocupação nas empresas porque interfere na produtividade. Também por gerar tráfego desnecessário nos servidores.

Outro perigo representado pelo hoax é a possibilidade de a mensagem também conter vírus. Os hoaxes mais comuns noticiam a morte de famosos, acidentes com grande repercussão ou acontecimento inusitado que desperte a curiosidade das pessoas. O perigo está na busca por mais informações, o que pode levar o usuário a clicar sobre links de acesso a site ou a programas maliciosos. Com a popularização do WhatsApp e dos memes, outra fonte de propagação de notícias falsas são os grupos nos aplicativos de mensagens.

Nome de domínio

Nome de domínio é o nome registrado no servidor DNS. É ele que permite localizar um web site pelo nome em vez de usar o endereçamento IP. O servidor de e-mail sempre estará vinculado a um nome de domínio e isto quer dizer que antes de instalar um servidor de e-mail, o servidor de DNS precisa estar funcionando.

Portas

As portas podem ser portas físicas, como a porta da impressora, a porta do mouse, a porta USB. Como também podem ser portas lógicas, como LPT1, LPT2, COM1, COM2, USB1, etc. As portas que temos interesse são as do tipo TCP e UDP, que vão de 0 a 65.535. Já falamos de portas neste volume da **Bíblia Hacker**.

Vamos ampliar nossa discussão especificando as portas usadas pelos servidores e contas de e-mail. Apesar do grande número de portas disponíveis, as portas associadas aos serviços de e-mail são as que aparecem na tabela a seguir:

USO PADRÃO	SEGURANÇA	AUTENTICAÇÃO	PORTA
SMTP Server (envio de mensagens)	Sem criptografia	AUTH	25 (ou 587)
	Criptografada (TLS)	StartTLS	587
	Criptografada (SSL)	SSL	465
POP3 Server (recebimento de mensagens)	Sem criptografia	AUTH	110
	Criptografada (SSL)	SSL	995

Protocolos

Protocolo em informática é uma convenção que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais. Os protocolos definem as regras para a comunicação entre sistemas. São adotados e aceitos pela indústria, o que permite a um estudante chinês, do outro lado do mundo em relação ao Brasil, aprender sobre servidores de e-mail da mesma forma que você.

Sem o acordo e aceitação global dos protocolos o servidor de e-mail chinês poderia ser incompatível com o servidor de e-mail de outros países. Limitando as comunicações e inviabilizando a Internet como a conhecemos.

Em se tratando de comunicação por correio eletrônico, os principais protocolos são:

- **SMTP** (Simple Mail Transfer Protocol) ou, em português, Protocolo de Transferência de Correio Simples. É o protocolo padrão para envio de e-mail através da Internet.
- **POP** (Post Office Protocol) ou, em português, Protocolo dos Correios. É o protocolo utilizado para acesso remoto a uma caixa de correio eletrônico, permitindo que todas as mensagens contidas na caixa de correio eletrônico possam ser transferidas sequencialmente para um computador local, quando o usuário poderá ler as mensagens recebidas, apaga-las, responde-las, salva-las, etc. Também conhecido como POP3.
- **IMAP** (Internet Message Access Protocol) ou, em português, Protocolo de Acesso a Mensagem da Internet. Um protocolo de gerenciamento de correio eletrônico com mais recursos que o POP3, oferecido pela maioria dos provedores aos seus clientes.

RFC

RFC é a sigla para Request for Comments ou, em português, Requisição para Comentários. Trata-se de um documento que descreve os padrões de cada protocolo da Internet antes mesmo de o protocolo tornar-se oficial. Alguns exemplos de RFC relacionados a e-mail:

- RFC 2821 - SMTP
- RFC 1939 - POP3
- RFC 3501 - IMAP

Existe RFC para praticamente tudo que existe na Web e na Internet. Para pesquisar e ler RFCs acesse:

<http://www.rfc-editor.org/>.

Scam

Scam é uma palavra de origem inglesa que em português quer dizer embuste. O scam é outra fonte de preocupação nas empresas, porque sobrecarrega o servidor e pode causar constrangimento e prejuízo financeiro.

A mensagem de e-mail identificada como scam deve ser descartada antes mesmo de chegar à caixa de mensagens do usuário. Mas nem sempre o sistema de proteção do servidor de e-mail consegue isto e o usuário acaba exposto às mensagens fraudulentas, podendo cair em algum tipo de golpe.

Em 2013 uma famosa atriz brasileira foi vítima de e-mail fraudulento. Alguém se passou pelo provedor e acabou convencendo a atriz a fornecer a senha de acesso. Uma vez com a senha o invasor descobriu fotos íntimas da atriz, que acabaram na Internet. A repercussão deste caso foi tão grande, que o nome da atriz se tornou sinônimo da Lei que trata dos crimes de informática no Brasil.

Scam é isto. Um e-mail com mensagem falsa geralmente usado para aplicar golpes nas pessoas. Uma das preocupações com a segurança dos servidores de e-mail inclui o que fazer para evitar que este tipo de mensagem chegue na caixa de mensagens do usuário.

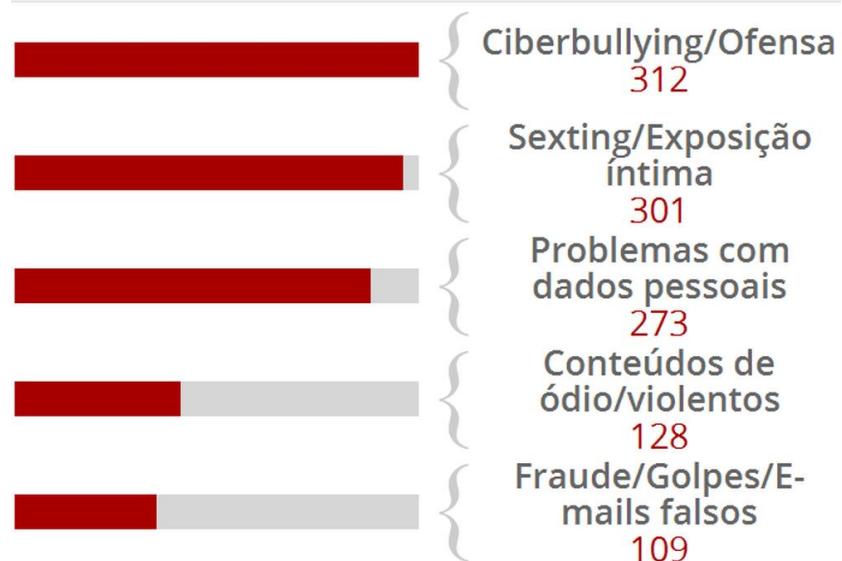
Os golpistas enviam mensagens para milhares de conhecidos na esperança de que alguns caiam no golpe. E geralmente é exatamente assim que acontece.

De acordo com a ONG o scam (fraude/golpes/e-mails falsos) ocupa o quinto maior número de reclamações sobre crimes na Internet¹:

¹ <http://g1.globo.com/tecnologia/noticia/cai-o-n-de-vitimas-de-nudes-vazadas-na-internet-do-brasil-em-2016-diz-ong.ghtml>

Top 5 de violações virtuais no Brasil

Veja o número de caso das principais violações na internet registradas em 2016



Spam

Spam é o nome de um apresuntado bastante popular nos Estados Unidos. Em informática é a palavra usada para definir o recebimento ou envio de mensagens indesejadas.



O primeiro spam de que se tem notícia ocorreu em 1994, quando dois advogados enviaram um e-mail para vários grupos de discussão da Usenet,

uma rede criada em 1979, divulgando uma loteria para receber o Green Card (visto de permanência nos Estados Unidos).

Se não existissem regras para coibir esta prática o volume de mensagens indesejadas no mundo seria o suficiente para paralisar a Internet ou no mínimo, deixá-la lenta.

Você deve dar atenção especial aos servidores de e-mail, porque caso estejam desprotegidos, podem ser usados por spammers de qualquer parte do mundo para enviar milhões de mensagens indesejadas sem que você perceba. Quando os órgãos reguladores da Internet identificam um IP como vetor de spam incluem este IP em uma lista negra de spam (Spam Black List).

Quando o endereço IP ou nome de domínio de um servidor é incluído em listas negras de spam, as mensagens deste servidor são bloqueadas e os usuários não conseguem mais usar o e-mail da empresa.

Quando você precisar verificar se um endereço IP ou nome de domínio consta em alguma lista negra de spam, visite: <http://mxtoolbox.com/blacklists.aspx>.

Segundo a Composite Blocking List (<http://cbl.abuseat.org/country.html>) o Brasil é um dos países que mais envia mensagens indesejadas no mundo. Nem sempre são cidadãos brasileiros que enviam estas mensagens. Pessoas mal-intencionadas de qualquer lugar do mundo, se aproveitam de servidores Web e de e-mail vulneráveis e os utilizam para enviar spam.

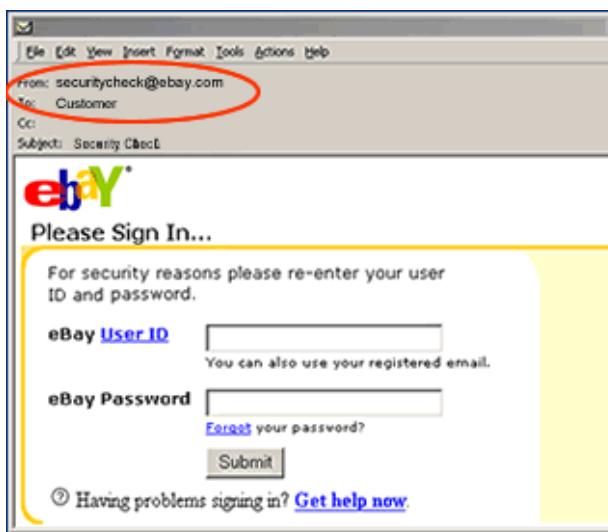
Como forma de reduzir esta prática que é considerada delito em alguns países, os provedores passaram a bloquear a porta 25 associada ao protocolo SMTP. Apesar de tecnicamente esta porta ainda poder ser usada, na prática a mensagem pode ser bloqueada antes mesmo de chegar ao servidor do destino.

Geralmente o spam é feito junto com o scam. Ou seja, o invasor envia milhares de mensagens de e-mail (spam) e o conteúdo destas mensagens é o golpe (scam).

Spoofing

Spoofing é mascaramento, melhor traduzido como falsificação. Spoofing relacionado a e-mail quer dizer que alguém falsificou o nome do remetente. Geralmente o spam, o scam e o spoofing estão juntos, pois a pessoa mal-intencionada falsifica o remetente (spoofing), cria uma mensagem fraudulenta (scam) e a envia para o maior número de pessoas mesmo sem ter o consentimento (spam).

Na imagem abaixo vemos um e-mail fraudulento (scam) com o remetente fraudado (spoofing) tentando convencer (scam) o usuário a informar o nome de usuário e a senha de acesso da conta no e-Bay.



O invasor envia mensagens de e-mail em grande quantidade (spam) porque sempre alguém cai no golpe. Eu posso não cair, você pode não cair, mas ao enviar mensagem para 100 mil e-mails por exemplo, se apenas 0,1% por cento cair no golpe já estamos falando em 100 pessoas invadidas em um

único dia. Como o índice de sucesso de um spam com peça (texto) bem construída é de 5%, as chances reais de sucesso são de 5 mil contas invadidas para cada 100 mil contas de e-mail que receberem a mensagem do golpista.

Você pode testar o e-mail spoofing (envio de e-mail falso) agora mesmo em qualquer um dos sites abaixo:

<https://emkei.cz/>

<http://www.sendanonymousemail.net/>

<http://www.5ymail.com/>

<https://anonymousemail.me/>

<http://deadfake.com/Send.aspx>

Nos sites acima você pode forjar qualquer remetente. Imagine um invasor que está a par de uma transação bancária a ser feita pela secretaria da empresa. O invasor envia mensagens de e-mail para a secretaria, se passando pelo chefe e informando a própria conta bancária (ou a de um laranja) para receber a grana.

Este golpe foi notícia em 2016 envolvendo o WhatsApp. Invasores em parceria com funcionários das companhias telefônicas conseguiam clonar o WhatsApp das pessoas e a partir disso aplicaram diversos golpes.

O pior é que a Justiça na maioria das vezes não consegue recuperar o dinheiro perdido. Parecido com um assaltante que se for preso depois, quando já tiver gasto o dinheiro, não tem como você receber o dinheiro de volta.



URL

O URL (Uniform Resource Locator - Localizador Padrão de Recursos) é o formato de atribuição universal para designar um recurso na Internet. É uma cadeia de caracteres ASCII imprimíveis com cinco partes:

1. **O nome do protocolo:** a linguagem utilizada para se comunicar na rede. O protocolo mais usado é o protocolo HTTP (HyperText Transfer Protocol), que permite passar as páginas Web para o formato HTML. Contudo, muitos outros são possíveis (FTP, News, Mailto, Gopher, etc.).
2. **Identificador e senha:** permite especificar os parâmetros de acesso a um servidor protegido. Esta opção é desaconselhada porque a senha é visível no URL.
3. **Nome do servidor:** se refere ao nome de domínio do computador que aloja o recurso pedido. Saiba que é possível utilizar o endereço IP do servidor, o que torna o URL XSR menos legível.
4. **Quantidade de portas:** trata-se de um número associado a um serviço permitindo ao servidor saber qual o tipo de recurso solicitado. A porta associada por padrão ao protocolo é a porta número 80. Sendo assim, quando o serviço Web do servidor for associado ao número da porta 80, sua inscrição se torna facultativa.
5. **Caminho para acessar o recurso:** esta última parte permite ao servidor conhecer o lugar onde o recurso está situado, ou seja, o diretório e o nome do arquivo solicitado.

Os seguintes protocolos podem, por exemplo, ser utilizados através do URL:

- **HTTP** - para a consulta de páginas Web.
- **FTP** - para a consulta de sites FTP.
- **Telnet** - para a conexão a um terminal remoto.
- **Mailto** - para o envio de um e-mail.

Estrutura do URL

O hacker precisa aprender a identificar as estruturas dos URLs mais complexos. O leigo identifica a estrutura mais simples. O profissional de TI e hacker precisam ir além e conseguir decifrar estruturas URL que às vezes se tornam bastante longas e complexas.

Na tabela abaixo demonstramos as cinco partes que formam o URL. Você poderá usá-la como ponto de partida para treinar a identificação de outras URLs, principalmente as que forem relacionadas a formulários e serviços online de e-mail (Webmail):

PROTÓCOLO	SENHA (se houver)	NOME DO SERVIDOR	PORTE (80 é padrão)	CAMINHO
http://	usuario:senha@	abibliahacker.com	:80	/download

Caracteres com codificação especial

Ao analisar URLs em busca de vulnerabilidades, você vai perceber que alguns usam códigos no lugar de caracteres. O espaço em branco por exemplo, é representado pelo código %20 que poderá aparecer no URL da seguinte forma:

www.abibliahacker.com/A%20Biblia%20Hacker.pdf

No lugar de:

www.abibliahacker.com/A Biblia Hacker.pdf

Recomendo a leitura e estudo da RFC que trata do assunto, porque a manipulação do URL é uma das fortes habilidades hacker:

<http://www.ietf.org/rfc/rfc1738.txt>

Na tabela abaixo você encontra os principais caracteres que vão aparecer em alguns URLs ou nos arquivos de log dos programas de escuta de portas:

CARACTERE	CODIFICAÇÃO URL
Tabulação	%09
Espaço	%20
"	%22
#	%23
%	%25
&	%26
(%28
)	%29
+	%2B
,	%2C
.	%2E
/	%2F
:	%3A

;	%3B
<	%3C
=	%3D
>	%3E
?	%3F
@	%40
[%5B
	%5C
]	%5D
^	%5E
'	%60
{	%7B
	%7C
}	%7D
~	%7E

Invasão de e-Mail por Telnet

O telnet é uma ferramenta de acesso remoto que permite estabelecer comunicação entre um computador e um servidor. Uma vez estabelecida esta comunicação é possível enviar comandos ao servidor e alguns destes comandos diz respeito ao e-mail. Ou seja, é possível acessar contas de e-mail usando Telnet. Mas para não sobrecarregarmos este volume 1 com muitas páginas sobre invasão de e-mail, daremos prosseguimento a este assunto no próximo Volume da **Bíblia Hacker**.





A Página de Erro 404

O protocolo HTTP prevê o uso de mensagens para comunicar ao usuário o resultado das suas requisições. Se não houvesse o feedback do HTTP poderíamos ficar perdidos ou perder tempo tentando acessar recursos inexistentes, bloqueados ou indisponíveis. Um destes códigos de erro é o 404. Exibido sempre que um recurso não é encontrado servidor, geralmente páginas Web. O erro 404 se tornou *cult* e fez surgir o hábito da página de erro 404 personalizada.

Nos capítulos sobre HTTP e servidores Windows e Linux você vai aprender um pouco mais sobre o erro 404 e personalização das páginas de erro 404.

Além de fazer parte da cultura hacker o invasor pode personalizar a página de erro 404 do servidor para fazer publicidade do servidor invadido. Toda vez que alguém tentar acessar uma página e a página não for encontrada, aparecerá a mensagem do invasor.





600v.deviantart.com

Casemod

Casemod é uma palavra da língua inglesa formada pela junção da palavra *case* (caixa, gabinete) e *mod* (abreviatura de *modification*, modificação em português).

Casemod é a modificação do gabinete do computador, mas pode ser usado também para se referir ao gabinete (comprado) modificado.

No começo da microinformática quando surgiram os primeiros computadores pessoais, os PCs, praticamente todo gabinete era bege com o formato retangular do tipo torre. Aquele que todo mundo conhece.



Entre os fabricantes foi Steve Jobs da Apple que rompeu com este padrão colocando no mercado gabinetes não convencionais, usando cores e diferentes formas.



Em algum momento os usuários de PC sentiram a necessidade de inovar e tornaram suas máquinas personalizadas. Assim surgiu a cultura da modificação dos gabinetes, o casemod.

Muitas pessoas, particularmente entusiastas em hardware, usam o casemod para ilustrar o poder do computador (mostrando o hardware interno) e também para fins estéticos, de decoração. Gabinetes também são modificados para melhorar a performance do computador como por exemplo, melhorar a ventilação ou fazer caber mais hardware do que caberia em um gabinete normal. Não custou muito para algumas empresas pensarem em como atender a estes modificadores de gabinete.

O resultado é que se tornou mais fácil encontrar todo tipo de acessório para quem quiser deixar seu gabinete com aparência estilizada. Há também os gabinetes modificados vendidos prontos, mas estes não são tão valorizados pelos entusiastas porque é algo que qualquer um pode comprar. Não é feito pelo usuário.

Se você pensar que ao ser hacker você adota uma cultura com algumas décadas de existência, precisa trazer para a sua vida os elementos que representam a cultura hacker.

Todos deveriam ter em casa um cantinho especial. Alguns conseguem ter um canto na casa, mesmo quando já estão casados e com filhos. Outros vão perdendo espaço até serem “donos” no máximo, de uma cadeira ou poltrona velha que ninguém mais quer sentar. Há também aqueles que tem seu cantinho, mas não se preocupam em fazer dele algo especial.

Um hacker completo não vai perder a oportunidade de trazer para sua vida alguns elementos da cultura hacker. Um destes símbolos é o casemod, o gabinete modificado.

Imagine-se chegando na casa de um hacker e ao se deparar com o computador que ele usa, nota que não tem nada de especial ali. É igual ao computador de qualquer pessoa que mal sabe mover um mouse.

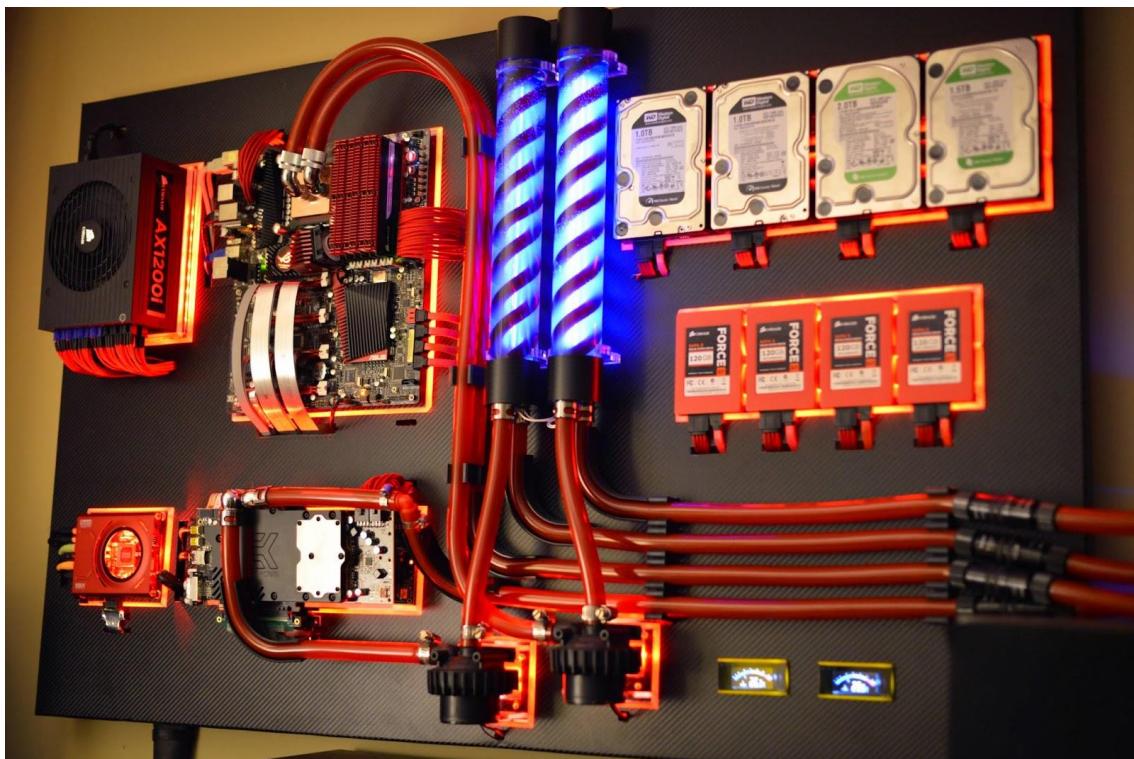
Isto é muito diferente de ter um gabinete modificado. Preferencialmente um modificado pelo usuário. Não estes comprados na loja e que qualquer um poder ter igual.

Aventure-se em uma das edições da Campus Party¹ e poderá ver modificações incríveis feitas em gabinetes. Outra coisa que você vai perceber é que os donos das melhores modificações conquistam de imediato o respeito dos seus pares. Todos entusiastas da tecnologia e prováveis adeptos da modificação de gabinetes.

Da mesma forma você, se pretende ser respeitado como hacker, precisa aparecer socialmente com alguns dos símbolos da nossa cultura, o casemod é um deles, talvez um dos mais importantes pelo impacto que causa.

¹ <http://brasil.campus-party.org/>

Você pode começar aos poucos. Fazer pinturas sugestivas com spray comum. Destes vendidos em lojas de material de construção. Pode também usar o computador fora do gabinete, preso a parede como vemos nesta ilustração:



Você não precisa começar com um gabinete modificado destes que faz as pessoas se deslumbrarem e é de cair o queixo. Pode começar com algo mais simples. Inclusive colando decalques sugestivos, que podem ser impressos na impressora comum usando papel fotográfico adesivo. Use a Internet para buscar inspiração. Mas por favor não me decepcione usando um computador cujo gabinete parece ter sido feito para a minha avó.

Após este empurrãozinho, o que você pretende fazer para modificar a aparência do seu gabinete?





Você Precisa Aprender a Escrever Código

Já dissemos algumas vezes neste primeiro volume que nós criamos **A Bíblia Hacker**, não **A Bíblia do Script Kiddie**. Isto quer dizer que existirão algumas partes que para alguns poderá ser considerada “chata”. Aprender a escrever código é uma delas. Se você gosta ou tem interesse nisto, ótimo. Se você não gosta de programação, lamento. Se quiser ser hacker vai ter que escrever código. Se fizer isto gostando melhor ainda.

A boa notícia é que vamos explicar sobre como escrever código de uma maneira bem fácil de você entender. E tem alguns benefícios. Quem sabe você não inclui mais esta profissão em seu currículo. A de programador de computadores?

Vamos começar respondendo a principal pergunta do dia:

_Por que o hacker tem que saber escrever código?

Se for um hacker de outra área realmente não precisa. Mas se for um hacker de computador, destes que invadem redes, smartphones e computadores, não tem como escapar. Precisa aprender código.

A lógica é simples. Os computadores funcionam a base de código. Tudo o que seu computador faz, desde escrever no Word, jogar qualquer jogo, enviar mensagem por e-Mail, navegar na Internet, qualquer que seja a atividade desenvolvida pelo computador, alguém escreveu um código para ele fazer.

O mesmo vale para os smartphones. Celulares que na verdade são computadores de bolso que fazem ligações telefônicas. O que menos importa em um telefone celular hoje em dia é se ele faz ligações telefônicas.

Aprender a criar código tem outras vantagens. Todo mundo pode criar código. Do garotinho de 8 anos ao senhor de 80 anos. Você já deve ter visto por aí, principalmente na TV, sobre crianças que criaram programas e jogos de computador. Faz com que eles pareçam gênios, não é verdade? O que talvez você não saiba é que tudo o que estas crianças fizeram foi juntar blocos lógicos, imagens prontas, combinar com as telas de fundo que já vem no programa e escolher um dos scripts pré-instalados.

Não há nenhuma genialidade nisto. O que há, e merece crédito, é o interesse da criança por criar jogos de computador. Isto foge ao padrão de só querer jogar, não criar.

Se até criança está programando, por que não você que já deve ser adulto ou no mínimo adolescente? A propósito, não temos notícias do pessoal da melhor idade programando. É um desperdício. Além de ajuda-los a retardar doenças típicas do cérebro, como Parkinson, Alzheimer e senilidade, esse pessoal poderia estar criando Apps de sucesso entre os idosos. Eles saberiam melhor do que ninguém sobre as necessidades dessa turma.

Se você ainda acha que aprender a programar está em seus últimos planos, pense no que falou o ex-presidente americano Obama:

“Não apenas compre um videogame, faça um. Não apenas faça download do último aplicativo, ajude a desenvolvê-lo. Não apenas jogue no seu celular, programe-o!”

Ouça você mesmo a fala do Obama em <https://youtu.be/6XvmhE1J9PY>. No vídeo o ex-presidente fala que apoia o ensino de programação nas escolas pois, além de ser importante para o futuro de todos, é importante para o futuro do país.

É isso mesmo. Um país sem programadores é um país atrasado, perdido no tempo. Nós reclamamos dos atrasos do Brasil em várias áreas. Mas um país é formado por seu povo e se o atraso existe, ele existe em nós também.

Se você tem filhos e permite um conselho obrigue-os a aprender matemática, português, inglês, empreendedorismo, finanças pessoais e programação. Todas as outras disciplinas são subordinadas a estas. Vá por mim.

Voltando a programação vamos esclarecer o seguinte. Os jogos que estas supostas crianças prodígio conseguiram criar são criados em programas que criam programas. São programas de uso muito simples e permitem criar jogos com roteiros pré-estabelecidos. Quer fazer seu filho de seis anos virar uma celebridade? Ajude-o a criar um jogo que procura pelo mosquito da dengue. Poste nas redes sociais. Entre em contato com o jornal e a TV local. As pessoas vão mesmo acreditar que seu filho é um gênio.

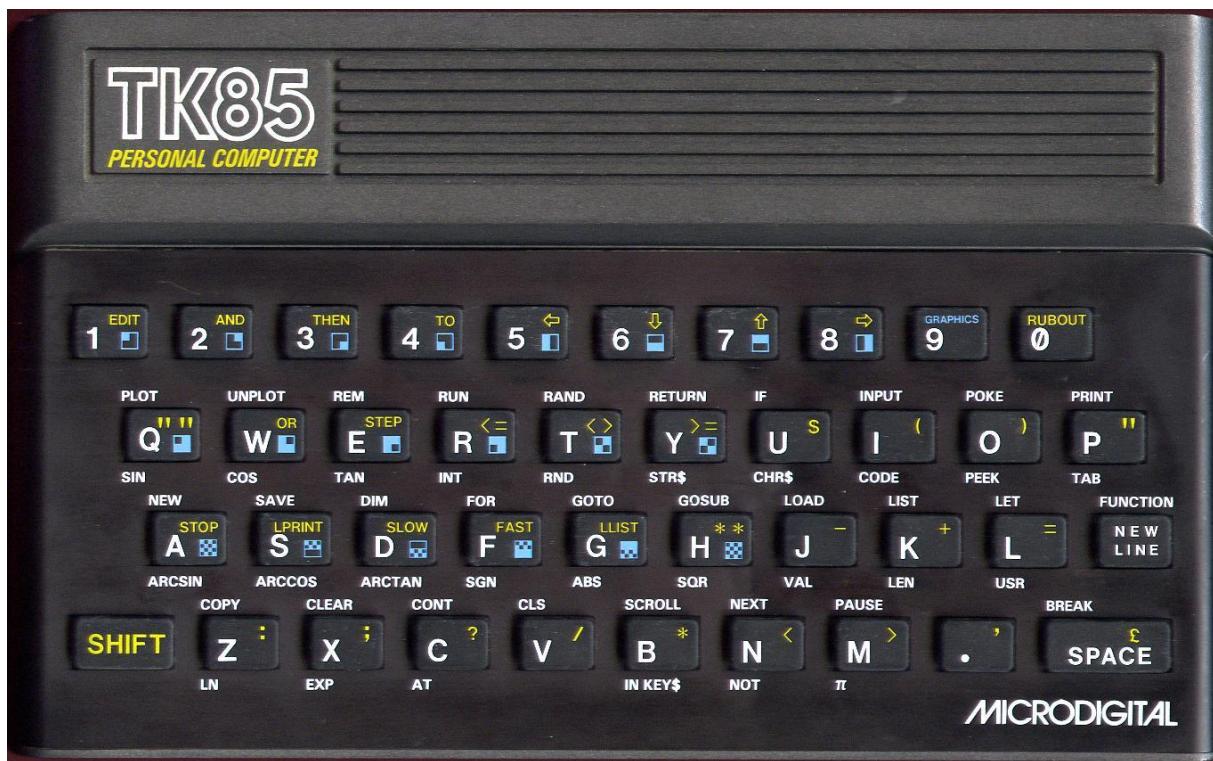
Espero que tenha percebido o sarcasmo. Na verdade, o que estou querendo dizer é que programar nos dias de hoje está muito mais fácil do que há alguns anos. Estou dizendo isto para ajudar você a perder o medo da programação e tentar convencê-lo(a) da importância da programação para você que é ou pretende ser hacker. A programação vai contribuir para a saúde do seu

cérebro e também ajuda a pôr algum dinheiro no bolso. Está convencido(a)? Então vamos lá.

Como aprendi a programar

Comprei meu primeiro computador – um modelo TK-85 da Microdigital – ainda era adolescente. Naquela época só os caras estranhos se interessavam por isso. Hoje vocês adoram os nerds, mas no meu tempo eu era chamado é de estranho e esquisito. Por gostar de eletrônica e computador.

Meu computador era uma caixa plástica com teclas de borracha. Cada tecla poderia ter entre duas e quatro e até cinco funções diferentes. Para baratear o preço o computador não era entregue nem com monitor, nem com unidade de armazenamento. O monitor era a TV, igual se fazia – e ainda fazem – com os videogames. E a unidade de armazenamento era a fita K7. A mesma usada para gravar músicas, porém se você não comprasse uma fita de boa qualidade como a BASF, ou não gravava ou gravava e não lia depois.



O que interessa nessa história sobre meu início como programador é que não havia muitos programas prontos. O que havia eram revistas com listagens que você precisava digitar, salvar na fita K7 e carregar no micro toda vez que quisesse jogar ou usar o programa. Só dava para usar um programa de cada vez.

Acontece que muitas vezes as listagens dessas revistas vinham com erro de digitação, erro de impressão e até erro lógico, causado pelo programador. Então você passava a tarde toda (ou a noite toda) digitando linhas e mais linhas de código e quando ia rodar o programa, o programa não funcionava. Que ódio, viu? É claro que as revistas publicavam correções, mas isso poderia levar dois a três meses, que é o tempo médio da revista receber as reclamações dos leitores, fazer a correção e publicar a correção na edição seguinte.

A maioria de nós dessa época não queríamos ficar aguardando a correção da revista. Queríamos ver a coisa funcionando ali, na hora. E assim fomos obrigados a entender o código. Aprender programação. Por pura necessidade de fazer o programa dos outros funcionar.

Uma das minhas revistas preferidas era a Micro Sistemas. Ela voltou online no endereço:

<http://revistamicrosistemas.com.br>

Muitos programadores de jogos atuais aprenderam a programar nas páginas da Micro Sistemas e com a coleção INPUT que você vê como era na próxima página.





Após aprender programação na marra, para não ficar refém de erros nos programas das revistas de informática, daí a criar meus próprios programas foi um passo.

Na época eu era técnico em Eletrônica, Rádio e TV formado pela Escola Técnica Electra (www.escolaelectra.com.br/ielectra/). Isto fez com que naturalmente eu criasse programas para eletrônica, como calculadora de valor de resistores e capacitores em série e paralelo, calculadora de bobinas de RF, identificadores de códigos de cores, etc. A propósito, foi por causa destes programas que eu me tornei escritor prestes a comemorar o lançamento do meu centésimo livro, previsto para 2018.

Aconteceu assim. Além das revistas com listagens de programas e jogos, as editoras começaram a lançar livros sobre o assunto. O livro muitas vezes era

melhor do que a revista, porque os programas listados nos livros dificilmente davam problema e vinham completos.

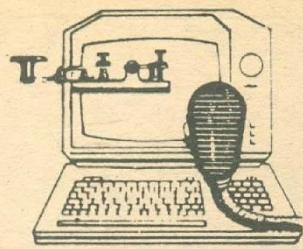
Conforme os programas foram ficando mais complexos e as listagens maiores, as revistas passaram a publicar os códigos em duas ou três edições. Então você levava uns três meses para finalmente poder rodar aquele programa ou jogo que te interessou.

Então comprei o livro Os Melhores Jogos para o TK85. Foi uma decepção. Tão grande que escrevi para a revista manifestando meu descontentamento. O interessante é que me responderam convidando para escrever um livro melhor para eles.

Gostei da ideia, mas como não era programador de jogos, sempre fui melhor programador de aplicativos – programas que resolvem problemas do dia a dia – decidi juntar meus programas sobre eletrônica e oferecer para a editora da revista Antenna-Eletrônica Popular, a Antenna Edições Técnicas (www.anep.com.br/).

O problema é que o TK85 já estava ultrapassado e eu não tinha dinheiro para algo mais avançado como o MSX ou o recém lançado PC XT. Sobre o PC XT nós brasileiros não podíamos ter a versão importada. Só a versão nacional que era uma porcaria fabricada no Brasil e custava 5 mil reais em valores atuais. Pesquise sobre Reserva de Mercado se quiser saber mais a respeito.

Meu dinheiro não dava nem para o MSX de 2 mil reais, imagine o PC XT? O TK85 estava ultrapassado e quase saindo do mercado. A sorte foi o dono da editora, o Sr. Gilberto Afonso Penna - PY1AFA, já falecido, ter ido com a minha cara e me convidado para lançar os programas na forma de artigos mensais. Na página seguinte você vê um destes artigos escritos por mim quando era adolescente.



O COMPUTADOR NO RADIOAMADORISMO

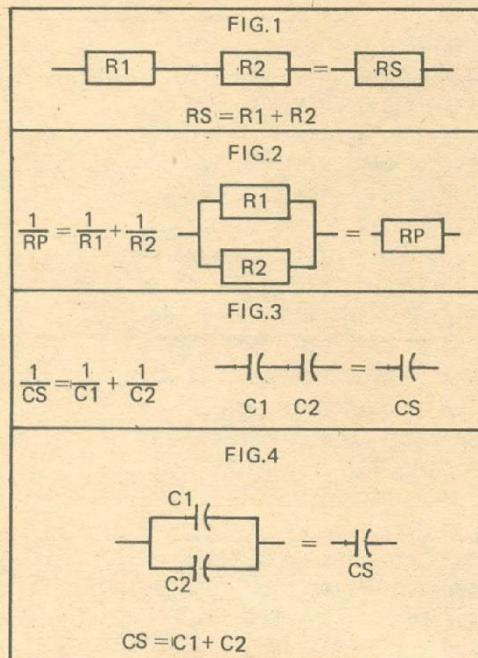
PROGRAMAS PARA O "SHACK" E A OFICINA

Nº3 - ASSOCIAÇÃO SÉRIE/PARALELO DE RESISTORES

M.A. Thompson

Após ter digitado o programa, grave-o com GO-TO 440.. O micro solicitará o nome do componente para cálculo: RESISTOR OU CAPACITOR. Pressione "R" ou "C" conforme o caso. A seguir, entre com o número de componentes envolvidos, o tipo de associação (S ou P) e os valores (em ohms ou microfarads).

Abaixo vão as fórmulas e diagramas utilizados no programa (que é para a linha Sinclair e compatíveis):



```

1 REM THOMPSON C 1988 V 1.0
2 P.O. BOX: 79.963
3 26.501 - NILÓPOLIS - RJ
4 GOSUB 380
5 GOSUB 410
6 PRINT,,,,"> CALCULO PARA RESISTOR O
U CAPACITOR ?"

```

```

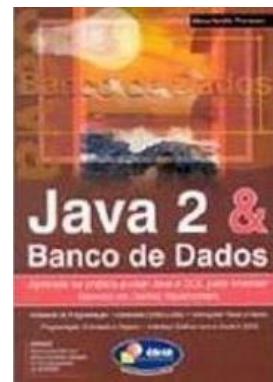
40 LET R$=INKEY$
50 IF R$="R" THEN LET C$="RESISTOR"
60 IF R$="C" THEN LET C$="CAPACITOR"
70 IF R$<>"R" AND R$<>"C" THEN GOTO 40
80 PRINT TAB 1;"=";C$;"ES
90 PRINT,,,> QUAL O NUMERO DE?;C$;"ES
?
100 INPUT N
110 DIM C(N)
120 PRINT TAB 1;"=";N
130 PRINT,,,> CALCULO EM SERIE OU PARALELO ?
140 LET R$=INKEY$
150 IF R$<>"S" AND R$<>"P" THEN GOTO 1
40
160 PRINT TAB 1;"=";R$
170 PRINT AT 14,1;"=????"
180 FOR A=1 TO N
190 PRINT AT 13,0;"> QUAL O VALOR DO "
" ;A;" ";C$;" ?"
200 INPUT C(A)
210 NEXT A
220 FOR B=1 TO N
230 LET RI=RI+(1/C(B))
240 LET RS=RS+C(B)
250 NEXT B
260 LET RP=1/RI
270 IF C$(TO 1)="R" THEN PRINT,,,,"> A
RESISTENCIA";
280 IF C$(TO 1)="C" THEN PRINT,,,,"> A
CAPACITANCIA";
290 PRINT "RESULTANTE E";"
```

(*Continuação da série iniciada à página 304 do Vol. 97- n.º 4 - Ref. 1110/1989.

AN-EP - VOL. 98 Nº 1
(Ref. 1112/1989)

E assim foi feito e apesar de o livro de programação não ter surgido nessa época, aquele desejo me acompanhou por vários anos até eu publicar o livro **Java 2 & Banco de Dados** pela Editora Érica em 2002.

Este breve resumo da minha trajetória como programador não estaria completo sem uma lista dos benefícios que obtive:



- Aumento da capacidade intelectual.
- Virei escritor de livros técnicos nacionalmente conhecido.
- Pude obter o registro profissional como jornalista por ter publicado artigos técnicos em revistas e jornais.
- Como hacker-programador pude criar minhas próprias ferramentas hacker, ler e modificar exploits e dar aulas de programação hacker.
- Ganhei dinheiro como professor em cursos de programação.

Gostei muito desses resultados, mas poderiam ser ainda melhores se naquela época alguém tivesse me alertado sobre as vantagens de ser programador. Como estou fazendo hoje com você.

Veja algumas pessoas da minha época ou de um pouco antes ou de um pouco depois, que se deram muito melhor do que eu após aprenderem programação:

- Bill Gates, fundador da Microsoft™
- Mark Zuckerberg, fundador do Facebook™
- Jack Dorsey, Evan Williams, Biz Stone e Noah Glass, fundadores do Twitter™
- Linus Torvalds, criador do Linux
- Garrett Camp e Travis Kalanick, fundadores do Uber™
- Larry Page e Sergey Brin, fundadores da Google™

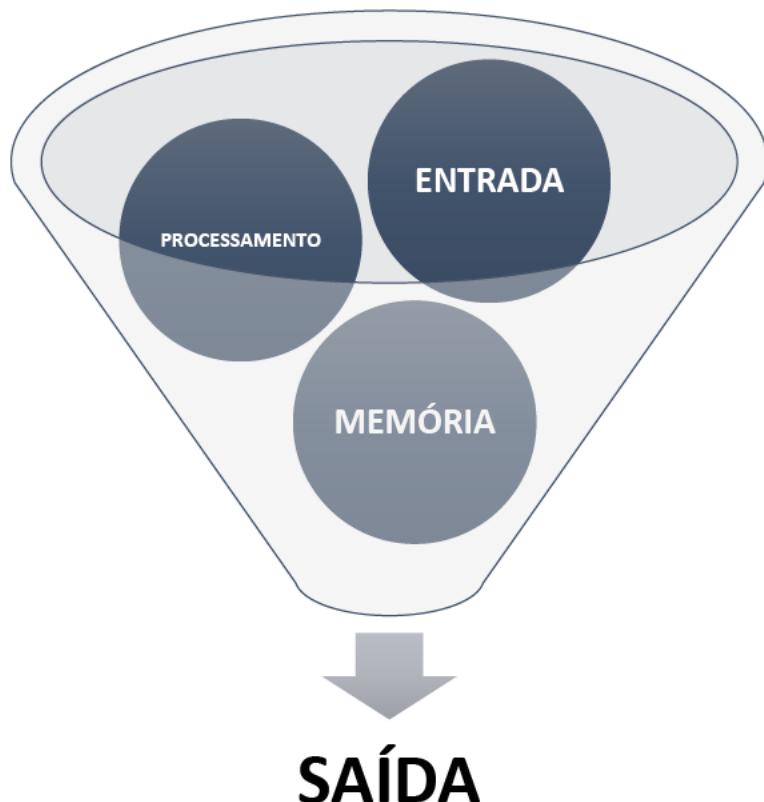
Sabe qual é a boa notícia? O mundo não acabou em 2012 como disse a profecia Maya. Isto quer dizer que ainda vamos ter muitos anos pela frente. Agora cabe a você decidir se vai passa-los programando ou sendo programado.

A dica quente que é se ligar na IoT (Internet das Coisas). A IoT funciona com um dispositivo que pode ser um sensor ou beacon e um App para celular.

O Brasil ainda não acordou para o potencial da IoT e para este potencial ser explorado é preciso entender de programação. E se tudo o que você quer é ser hacker, aprender programação não é opção, é conhecimento obrigatório.

Entendendo a programação de computadores

Podemos compreender facilmente a essência da programação olhando o seguinte diagrama:



Eu gosto de criar programas de trás para frente: primeiro defino o que o programa vai fazer. Depois vejo quais entradas são necessárias. Faço um mapa da memória que vou precisar. E finalmente trabalho na parte do processamento, que é a parte do código que vai permitir ir de A (entrada) até B (saída ou resultado almejado).

Vamos supor que você queira criar um programa para quebrar senhas de e-mail. Começando pela saída o programa deverá exibir algo como:

A SENHA DESTE E-MAIL É: XXXXXX

A frase “**A senha deste e-mail é**” em programação é chamada de string (cadeia de caracteres). O local onde vai aparecer a senha, onde está **XXXXXX**, é ocupado por uma variável. A variável precisa ter um nome como por exemplo **SENHA_DESCOBERTA**. O nome é variável porque para cada e-mail teremos um valor de senha diferente.

Para a entrada deste programa podemos ter algo como:

INFORME O E-MAIL PARA OBTER A SENHA?

A frase “**Informe o e-mail para obter a senha**” é outra string. Também vamos precisar de um local para armazenar o e-mail a ser digitado. Usaremos outra variável que pode ter o nome: **SENHA_A_REVELAR**.

Geralmente não usamos nomes de variáveis tão compridos. Poderia ser algo como **EMAIL_IN** e **PASS_OUT**. Estou usando nomes fáceis e compridos nos exemplos para ficar mais fácil de entender.

O programa já tem entrada, saída e definição dos nomes para as variáveis. A parte que é mais dependente do intelecto e capacidade técnica é o processamento, também chamado de algoritmo.

Nas universidades muitos colegas são reprovados nas aulas de programação. Não porque têm dificuldade com a linguagem. Na maioria das vezes a dificuldade é com o algoritmo.

É pior ainda quando o professor mistura aula de programação com aula de algoritmo. O estudante às vezes não aprendeu programação e já tem que lidar com algoritmos nem sempre simples, como o de Dijkstra¹ por exemplo.

Como você vai aprender programação com A Bíblia Hacker

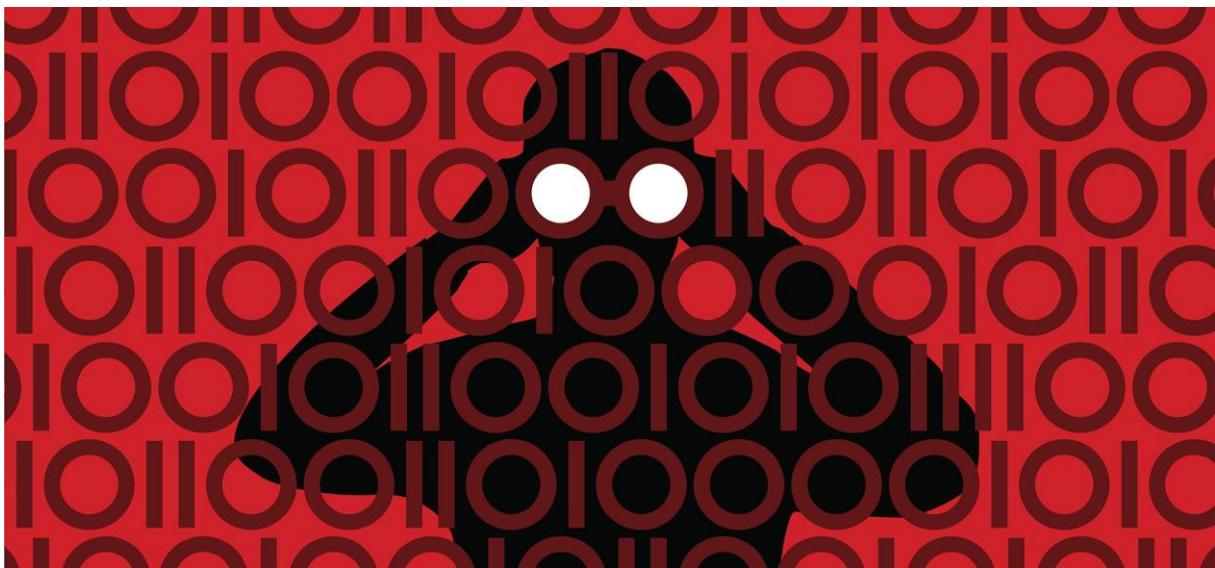
Nosso objetivo hoje foi despertar seu interesse e falar sobre a importância de você aprender programação. Seja para ser hacker, seja para melhorar sua empregabilidade, seja para ter mais ofertas de emprego e renda, seja para manter seu cérebro saudável, seja para ser o mais novo brasileiro a ficar milionário como programador, seja para evitar as doenças da velhice que afetam o cérebro, seja para criar programas que o(a) auxiliem no seu dia a dia ou em sua profissão, seja para tornar-se mais inteligente ou para ser um hacker realmente capacitado.

Voltaremos ao assunto no próximo Volume ensinando como você poderá criar vários programas, em diferentes linguagens de programação, incluindo programas para o smartphone com o Android.

Não é exatamente um curso de programação, mas se você seguir a orientação de todos os volumes da Bíblia Hacker você conseguirá programar. Isso eu te garanto. Há! E não se esqueça. Temos também as videoaulas.



¹ https://pt.wikipedia.org/wiki/Algoritmo_de_Dijkstra



Exploits

Exploit é uma palavra de origem inglesa que funciona no texto como verbo ou pronome. Exploit na função verbo é o verbo **explorar**. Por esta lógica deveríamos chamar de **exploiter** o programa que explora vulnerabilidades em sistemas.

Mas exploit também é substantivo e em segurança da informação exploit é o nome dado aos códigos que exploram vulnerabilidades ou criam brechas em sistemas informatizados.

O nome da técnica hacker que usa exploits é **exploitation** ou **exploiting** e se você já buscou informações sobre exploiting em livros e na Internet, já deu para perceber que existe informação desencontrada ou incompleta, que acaba confundindo mais do que explicando.

Nosso primeiro objetivo com este treinamento é eliminar qualquer dúvida sobre a natureza dos exploits. Em seguida veremos onde obtê-los e encerraremos com dicas de como usá-los na prática hacker ou em testes de invasão para fins de segurança.

Só vai ficar faltando ensinar como você poderá criar seus próprios exploits, mas sendo o exploit um programa de computador, apenas programadores

são capazes de criá-los. Deixaremos esta parte para os capítulos que tratam de programação.

A primeira definição de exploit você já teve. É um código capaz de explorar vulnerabilidades ou subverter sistemas informatizados. Subverter sistemas é causar falhas onde não havia nada de errado. Os exploits têm estas duas funções:

- Causar falhas e
- Explorar vulnerabilidades.

E podem ser divididos em:

- Exploits locais
- Exploits remotos
- Exploits para aplicações web
- Exploits para negação de serviço (DoS)
- Exploits de shellcode

Cada qual tem uma estrutura de código própria. Alguns são compilados, outros não. Todos seguem os princípios que vamos apresentar neste material.

Anatomia do Exploit

Vamos supor que um invasor queira remover a senha da CMOS de um computador antigo sem precisar abrir a tampa do gabinete. A CMOS é um chip de memória que armazena o sistema BIOS e um programa utilitário chamado Setup. Para evitar o acesso indevido a CMOS é possível colocar uma senha de acesso. Este será o obstáculo que o invasor deseja remover, a senha de acesso ao Setup.

Isto pode ser feito manualmente, abrindo uma janela de Prompt de Comando no Windows e digitando:

```
debug  
o 70 ff  
o 71 17  
q
```

NOTA: Este procedimento é ilustrativo, não funciona nas BIOS atuais e os endereços ff e 17 podem ser outros dependendo da BIOS.

A explicação do que é o exploit vem agora. O invasor, para não ter que ficar digitando linha por linha toda vez que precisar remover a senha de alguma CMOS, geralmente prefere automatizar o processo. Esta automatização pode ser feita em várias linguagens de programação, incluindo o Batch Files do Windows, que é antigo mas funciona até hoje, inclusive no Windows 10. Exploit nada mais é do que isto: a automatização de um procedimento que inicialmente foi feito de forma manual por quem o criou.

Veja como você mesmo pode criar um exploit em apenas alguns minutos:

- 1) Abra o bloco de notas e digite **md hacker**.
- 2) Salve na Área de Trabalho com o nome **exploit.bat**.

- 3) Baixe um conversor de arquivo BAT em executável (EXE) de um destes sites:

<https://bat2exe.codeplex.com/>

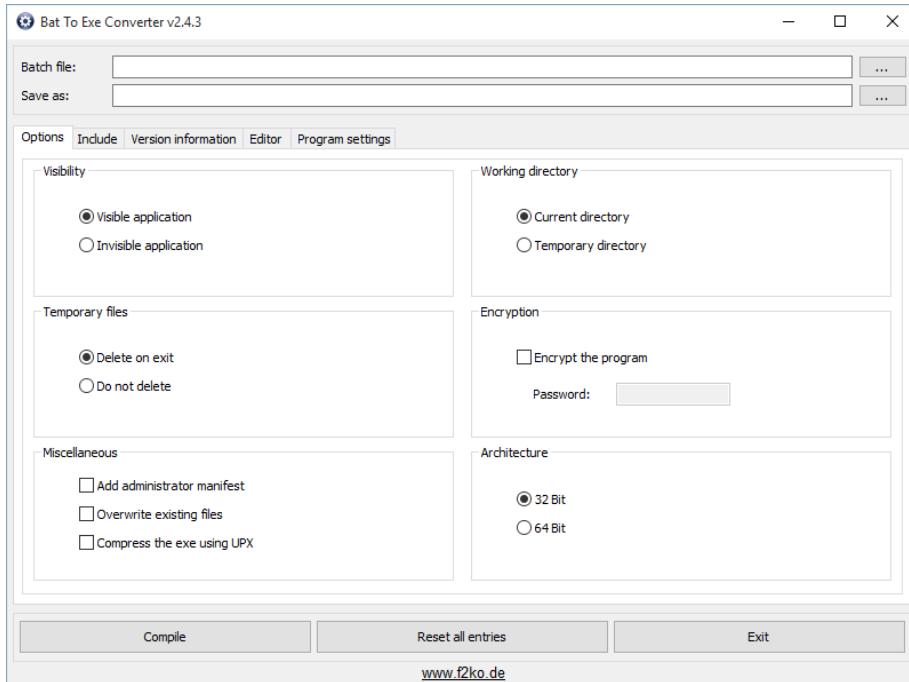
<http://www.f2ko.de/en/b2e.php>

<http://bat2exe.net/>

<https://sourceforge.net/projects/bat-to-exe/>

<http://www.bat-to-exe.com/>

<http://www.scriptcode.com/battoexe/>



- 4) Pronto. Você acaba de criar um exploit com a função de criar uma pasta com o nome hacker na Área de Trabalho. Confira após executar o arquivo de lote (BAT) ou o executável (EXE).

É um exploit inútil, só serve para criar a pasta na Área de Trabalho. Mas serviu para mostrar o que de fato são os exploits e como eles são criados. Neste caso usamos o Batch Files do Windows, mas poderia ser em linguagem C, C++, C#, Java, Assembly, JavaScript, Perl, Python, PHP, Windows PowerShell, Microsoft Windows Scripting Host, Bash, etc.

Perceba que o mesmo procedimento que ensinamos, de criar um script e transformá-lo em executável, pode resultar em códigos muito poderosos. Estes são exploits que precisam rodar localmente. Alguém precisa clicar neles. Em outros capítulos mostraremos como fazer os exploits parecem arquivos úteis e inofensivos.

Conheça outras informações importantes sobre exploits:

- 1) O exploit só se aplica a uma situação específica. Nosso primeiro exploit removeria a senha da CMOS e o segundo exploit criou uma

- pasta na Área de Trabalho. O que precisamos que você entenda é isto, que cada exploit só serve para a finalidade a qual foi criado.
- 2) O exploit é criado para automatizar algum procedimento manual. Tudo o que o exploit faz é possível de ser feito manualmente, porém em várias etapas e estas etapas só quem conhece é quem programou o exploit. É possível fazer a engenharia reversa do exploit para saber que etapas são estas, mas não é tarefa simples se o exploit estiver compilado e/ou criptografado.
 - 3) O exploit pode ser codificado em qualquer linguagem de programação, desde que a linguagem consiga fazer o que se espera do exploit. A preferência por C/C++ e Assembly é a capacidade que estas linguagens têm de subverter o sistema. O uso de Perl e PHP aproveita a capacidade destas linguagens de interagir com os protocolos do TCP/IP. Para linguagens de script no Windows temos os arquivos de lote, Windows PowerShell e Windows Scripting Host, além do ASP, JavaScript, etc.

Usando exploits

Quem não é programador só poderá fazer uma coisa com exploits: usá-los. E como se usa um exploit? Devido à natureza do exploit, de servir a um único propósito, a forma de usar um exploit não é padronizada. Para cada exploit precisamos descobrir como ele é usado.

Isto ocorre porque o exploit é um programa simples, destinado a alvo certo, sem interface gráfica nem menus de opções. Geralmente é um arquivo que você executa e o estrago está feito. Quando admitem interação é por linha de comando.

[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#)

Offensive Security's Exploit Database Archive

37284

Exploits
Archived

The Exploit Database – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).



O que podemos fazer para ajudar você a dominar os exploits é classifica-los de acordo com a forma de uso. Assim temos:

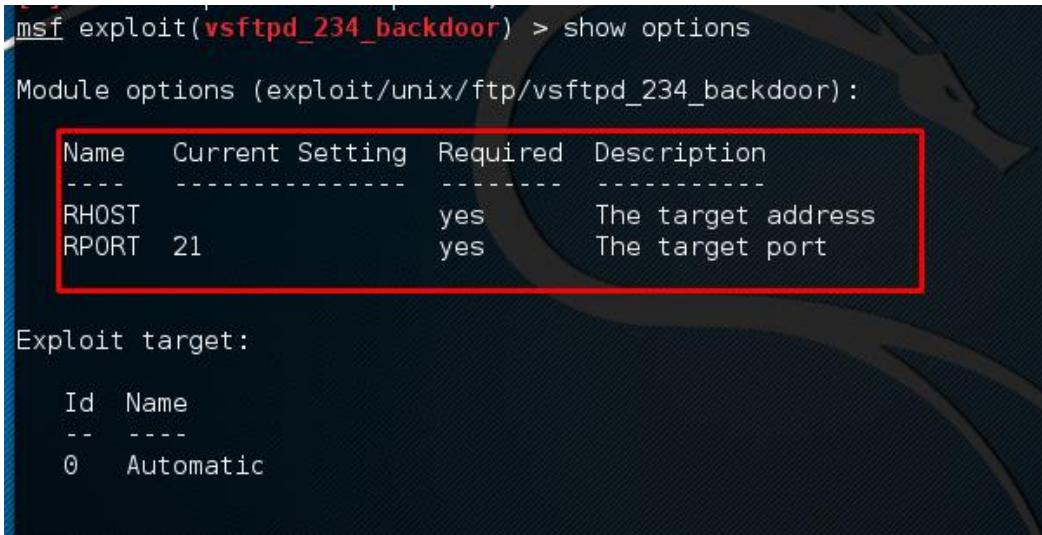
- Exploits de execução direta
- Exploits interativos
- Exploits com argumentos ou exploits parametrizados

Os exploits de execução direta são àqueles que você executa e eles cumprem seu papel. Não é preciso mais nada. Nossa exemplo didático do exploit que remove a senha de acesso a CMOS e o que cria a pasta hacker na Área de Trabalho, são exemplos de exploits de execução direta.

Se você é o tipo de pessoa que baixa programas para depois cracheá-los, já deve ter usado patchs, pequenos programas que servem para remover a restrição dos softwares comerciais. Estes patchs também são exploits de execução direta.

O segundo grupo é menos comum. São os exploits interativos. Você executa o exploit e precisa programá-lo através de menus com opções ou respondendo perguntas em prompt de comando. O menu ou as perguntas no prompt

podem se referir ao sistema operacional, ao número de tentativas, as opções de funcionamento do exploit. Não espere nunca interface gráfica em exploits, é tudo por linha de comando.



msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	21	yes	The target port

Exploit target:

Id	Name
--	--
0	Automatic

O exploit interativo não é muito comum, exceto por projetos que reúnem exploits em uma mesma interface, como é o caso do The Metasploit Project, sobre o qual falaremos nos capítulos sobre o Kali Linux.

O terceiro grupo é mais comum e é formado pelos exploits com argumentos, também conhecidos como exploits parametrizados. Os parâmetros são valores que precisam ser passados ao exploit na mesma linha de comando. O parâmetro mais comum passado ao exploit é o IP ou nome de domínio do alvo e a porta a ser exploitada. Veja o exemplo:

exploitABCD www.alvo.com:123

Exploit no filme Matrix Reloaded

No filme Matrix Reloaded (2003) a personagem Trinity (Carrie-Anne Moss) roda um exploit para ter acesso privilegiado (root) a Matrix. Observe a figura abaixo e veja se consegue descobrir o nome do exploit que ela executou.

```
tcp      nmap      host<2-nc      [mobile]
1 Starting nmap 0. 2.54BETA25
1 Insufficient responses for TCP sequencing (3), OS detection may be less
3 accurate
3 Interesting ports on 10.2.2.2:
3 (The 1539 ports scanned but not shown below are in state: closed)
4 Port      State    Service
4 22/tcp    open     ssh
1
1 No exact OS matches for host
8
8 Nmap run completed -- 1 IP address (1 host up) scanned
8 # sshnuke 10.2.2.2 -rootpw="Z10N0101"
4 Connecting to 10.2.2.2:ssh ... successful.
0 Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "Z10N0101".
e System open: Access Level <9>
P # ssh 10.2.2.2 -l root
root@10.2.2.2's password:
7 _PER_CONTROL > disable qgrid nodes 21 - 48
```

Tente descobrir também que tipo de exploit foi usado. Se é um exploit de execução direta, se é parametrizado ou interativo. É importante que você faça este exercício e se encontrar dificuldade não deixe de nos procurar.

Aqui encerramos esta primeira parte descrevendo o que são os exploits, os pequenos programas usados para criar falhas ou explorar vulnerabilidades em sistemas informatizados.

Também demonstramos que os exploits são criados por programadores ao transformarem procedimentos manuais em procedimentos automatizados. Daremos prosseguimento ao assunto no próximo volume da Bíblia Hacker.





O Linux e os Hackers

Se eu te disser que após a leitura deste capítulo você será capaz de instalar em máquina virtual a mais famosa distribuição Linux para hackers já criada? Não só instalar como também já sair usando? Você acredita?

Não precisa acreditar. É só continuar lendo e depois assistir as videoaulas que preparamos sobre o assunto. Apenas lembrando que estas videoaulas são gratuitas e estarão disponíveis em nossa página do Facebook apenas para os compradores da **Bíblia Hacker**.

Por que Linux é a melhor opção para hackers?

Antes de responder vamos analisar o seguinte. O Linux é um sistema operacional (SO), certo? SO é o programa que faz o computador funcionar. É o programa antes do programa. Se você quer instalar um processador de textos ou game, antes precisa ter no computador – ou no celular – um SO instalado e funcionando. Os SOs mais usados atualmente são:

- Windows, da Microsoft
- macOS e iOS, da Apple
- Linux, de diversos distribuidores
- Android, da Google

Voltando à pergunta título, por que Linux é o SO indicado para os hackers, vamos ver primeiro porque os outros não são os mais indicados para os hackers, começando pelos sistemas operacionais da Apple.

O macOS e o iOS são sistemas operacionais que só rodam em hardware específico. O macOS nos computadores Mac e o iOS no iPhone. O problema é que no Brasil tanto o Mac como o iPhone são caros para os nossos padrões, então não se vê muitos deles por aí.

Além disto são sistemas fechados, que não atraem o interesse do pessoal que cria programas e ferramentas hacker. Ou seja, a quantidade de programas e ferramentas hacker criadas para o macOS e para o iOS é pequena.

Imagine você hacker. Não creio que sua primeira opção de computador para hackear seja um Mac ou iPhone. Você não vai pagar caríssimo por um computador da Apple para correr o risco de corromper o sistema operacional e depois não conseguir reinstalar.

E caso a intenção seja invadir (para fins de segurança) um computador da Apple, seja o Mac ou iPhone, você não precisa ter um Mac para fazer isto. O computador que invade não precisa ter o mesmo SO do computador invadido.

Lembra da atriz Carolina Dieckmann? Aquela que teve as fotos íntimas vazadas na Internet em 2012 e deu nome à Nova Lei de Crimes de Informática¹? O computador dela era um Mac e o do invasor era um PC rodando Windows.

Sobre usar o Mac ou iPhone como máquina de invasão, não interessa porque:

- São caros.
- Quase não têm ferramentas hacker escritas para eles.
- Pouca gente usa Mac ou iPhone em comparação a outros SO.

¹ http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Além do que, se o alvo tiver um Mac ou iPhone ele pode ser invadido de um computador rodando Windows ou Linux. Então descartamos os SOs da Apple para uso na máquina de onde vai partir a invasão.

E quanto ao Android da Google? O Android é o SO mais usado em dispositivos móveis, como tablets e smartphones. Existem muitas ferramentas hacker escritas para o Android e você poderá usá-las diretamente do seu smartphone. Veremos muitas destas ferramentas aqui na **Bíblia Hacker**.

Porém existem ferramentas importantes que não funcionam no Android. Então podemos contar com o Android sempre que for possível, mas vamos precisar de um PC rodando Windows ou Linux para a maioria dos ataques e invasões.

E já que falamos no Windows, o Windows é um bom sistema operacional para usar em invasões? É sim. Pelos seguintes motivos:

- Você encontra o Windows instalado em todo lugar, nas casas e escritórios.
- Você pode usar o Windows da Lan House.
- Instala até em computador muito antigo, como o Pentium III que tem 18 anos desde que foi lançado em 1999.
- Você consegue facilmente o DVD ou a imagem (ISO) para fazer a instalação. Seja nos sites piratas ou com o vendedor da esquina.
- É fácil de usar. Todo mundo que usa computador sabe um pouco de Windows.
- Tem milhares de ferramentas hacker escritas para o Windows. Muitas distribuídas com o código fonte, que você pode modificar.
- Por ser o SO mais usados pelas pessoas nos computadores desktop, o Windows é também o maior alvo de ataques e invasões. Você pode usar

o conhecimento hacker para tentar invadir (e proteger) seu próprio micro.

Com tantas vantagens assim o Windows deve ser o melhor sistema operacional para hackers, não é mesmo?

Na verdade, não. Principalmente as versões mais recentes, como o Windows 10 S que é uma versão do Windows cheia de limitações e provavelmente vai aparecer nos computadores de algumas escolas e faculdades.

A Microsoft não quer ver as pessoas usando o Windows para hackear, então algumas portas que são importantes para as ferramentas hacker acabam fechadas por padrão. Se você não desabilitar o firewall, a ferramenta hacker não funciona. E em muitos casos o antivírus ou o Windows Defender impedem o funcionamento da ferramenta.

Eu mesmo recomendo a quem quiser usar o Windows para hackear escolher entre o Windows XP ou o Windows 7. O Windows 8, 8.1 e o Windows 10 não são boas alternativas.

A propósito, você vai ver nas videoaulas eu usando o Windows 10. Mas isto é para calar os *boca de latrina*. Para que não digam que as videoaulas são antigas só porque usam uma versão do Windows que não seja o 10. Tenho aulas de 2003 pirateadas e circulando no Youtube e na Internet que usam o Windows XP. Se você segue o que está demonstrado lá, vai ver que muita coisa ainda funciona.

Para quem está começando o Linux pode não ser a melhor opção. O ideal é aprender a hackear no Windows e depois que conseguir fazer alguns hacks, começa a usar Linux.

Se você já faz hacks no Windows, chegou a hora de dar o próximo passo e aprender a hackear usando o Linux. As vantagens são:

- O Linux desde que foi criado já previa o uso em redes e na Internet. A Microsoft, inicialmente – acredite se quiser – não apostou na Internet. Então o Windows foi adaptado para funcionar na Internet, não se integra tão bem quanto o Linux. Podemos dizer que os protocolos de comunicação do Linux conseguem estabelecer conexões muito melhores e estáveis do que quando usamos o Windows.
- Os programas criados para o Linux na maioria das vezes são distribuídos junto com o código fonte. Isto quer dizer que você pode modificar os programas e até redistribui-los se quiser.
- O Linux é conhecido por possuir edições personalizadas. Tem Linux para músicos, Linux para os entusiastas da eletrônica, Linux só com jogos e tem também Linux para hackers, testes de invasão, perícia forense. Isto quer dizer que com um único download você consegue um sistema operacional repleto de ferramentas hacker, prontas para uso.
- O Linux roda facilmente a partir de um CD, DVD ou pen drive, sem precisar instalar. O Linux roda até dentro do Windows, seja em máquina virtual ou não.
- Também instala em computadores antigos.

Os pontos fracos do Linux para hackers é que:

- Se você não conhece o Linux, primeiro precisa aprender Linux para depois aprender a usar as ferramentas hacker. No Windows você pode ir direto para as ferramentas hacker.
- É bastante comum a ferramenta não funcionar por causa de algum problema de incompatibilidade, dependência de pacotes ou configuração.
- Como o Linux permite ter controle sobre tudo, às vezes algo simples você só consegue fazer funcionar se entender a tecnologia envolvida. No Windows quase tudo é automático ou com assistentes (Wizards).

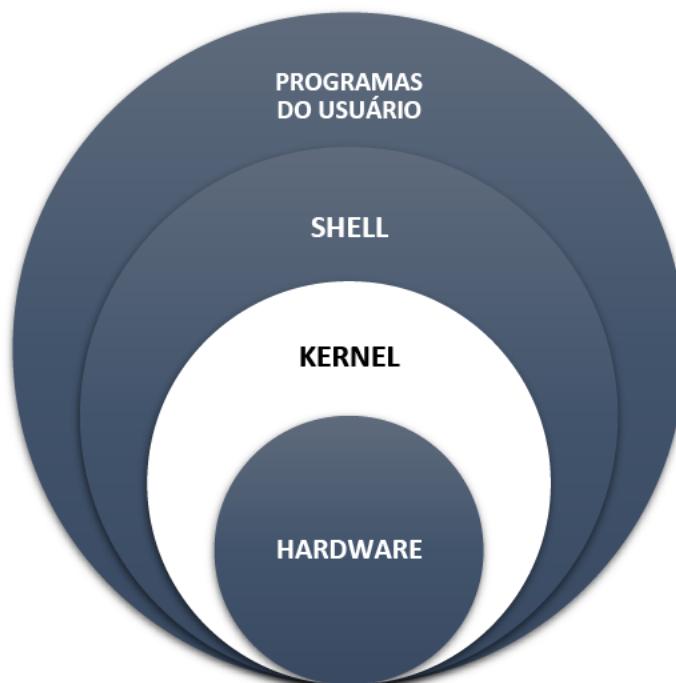
- O Linux usa muito as linhas de comando, algo estranho para quem a vida toda só clicou em botões, menus e em janelas do Windows.
- Às vezes ocorre de um hardware não funcionar por falta do driver de dispositivo. Isto não afeta muito o hacker, mas pode complicar a vida do usuário que optar pelo Linux e não consegue fazer a impressora ou scanner funcionar com todos os recursos.

Se você quiser guardar apenas os dois motivos que tornam o Linux ideal para hackers, anote:

- **A qualidade da comunicação em rede** – incluindo a Internet – e
- **A quantidade – e qualidade - das ferramentas hacker** disponíveis.

Por que usar o Linux Kali?

Como antecipei, não existe um único Linux. Na verdade, tem um pequeno núcleo que é o que chamamos de Linux Kernel ou apenas kernel (núcleo do Linux) e tem também o Linux mais os programas pré-instalados que é o que nós chamamos de distribuição Linux.



O kernel recebe um número conforme vai ganhando atualizações. A mais recente versão do núcleo do Linux é a 4.9 e você pode acompanhar as atualizações no site oficial, em www.kernel.org.

A história da criação do Linux é curiosa, porque os caras liderados pelo Richard Stallman trabalhavam nos programas (aplicações) e no shell. A parte mais importante, a parte que vai dar suporte para todas as outras funcionarem, não estava saindo. Estava amarrada, como se diz no Brasil.

Foi quando o Linus Torvalds lançou o kernel e aí foi possível oferecer para a comunidade um sistema operacional completo: kernel + shell + aplicações.

O shell é o interpretador de comandos. Vamos falar sobre ele em breve.

As versões do Linux são chamadas de distribuição ou popularmente de **distro**. Qualquer pessoa ou empresa pode criar a própria distribuição. Criar uma distribuição é juntar no mesmo pacote:

- Kernel
- Drivers
- Shell
- Interface gráfica
- Aplicações (programas)

Diferentemente do Windows que você instala o sistema operacional e depois precisa instalar outros programas um por um, as distribuições Linux costumam vir com os programas instalados. Algumas empresas criaram distribuições muito boas e passaram a ser referência quando se trata de Linux:

- Red Hat
- Debian
- Slackware

A partir destas três distribuições foram criadas a maioria das outras, como por exemplo a SuSE que se baseou na Slackware, a Fedora que se baseou na Red Hat, a Ubuntu que se baseou na Debian.

A distribuição Backtrack se baseou na Ubuntu. Já a distribuição Kali Linux se baseou na Debian. Podemos dizer que o Linux Backtrack é um Ubuntu modificado e que o Linux Kali é um Debian modificado.



Até você pode fazer um Linux personalizado, colocar um nome e distribuir como seu. O que acha de fazer isto em menos de dez minutos? É só seguir nosso tutorial:

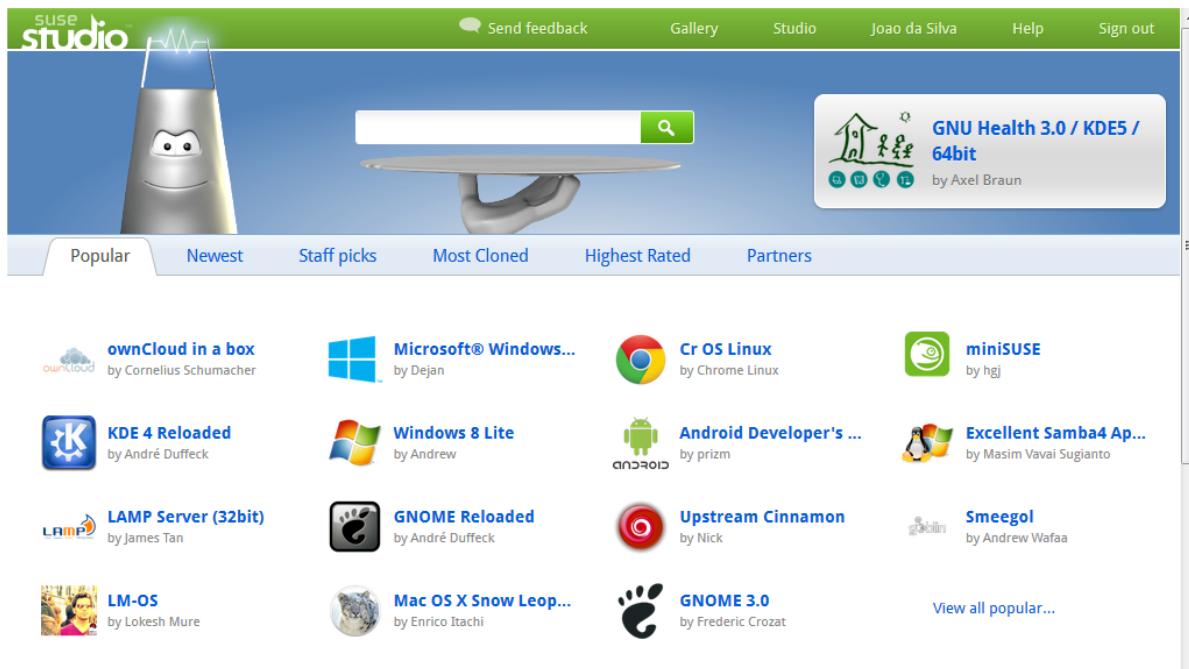
1. Acesse o site que vai automatizar o processo:

<https://susestudio.com/>

2. Você terá a opção de criar uma conta ou acessar como uma conta existente, como a do Facebook ou a do Google por exemplo.
3. Após criar a conta ou fazer login você será direcionado a página de criação da distribuição personalizada. A primeira escolha que você deverá fazer diz respeito a versão (openSUSE ou SUSE Linux Enterprise), a interface gráfica (KDE ou GNOME) e no final da página escolher um nome para o arquivo. A opção Server cria uma distribuição sem interface gráfica, cujo acesso e administração serão feitos exclusivamente em modo shell (linha de comandos).
Para facilitar vou ajuda-lo(a) a escolher: em **openSUSE Leap** selecione a opção **KDE 4 desktop**, depois vá até o final da página e mude o nome do arquivo. Feito isto é só clicar no botão **Create appliance**:

The screenshot shows the SUSE Studio interface. At the top, there's a green header bar with the SUSE studio logo, a 'Send feedback' button, 'Gallery', 'Home', 'Joao da Silva', 'Help', and 'Sign out'. Below the header, the main area has a title 'Choose a base template'. It displays two sections: 'openSUSE Leap 42.1' and 'SUSE Linux Enterprise 11 SP3'. Under 'openSUSE Leap 42.1', the 'Just enough OS (JeOS)' option is selected, highlighted with a yellow box. Other options shown are 'Server' (text-only base) and 'GNOME desktop' (openSUSE Leap 42.1 GNOME). Under 'SUSE Linux Enterprise 11 SP3', the 'Just enough OS (JeOS)' and 'KDE 4 desktop' options are listed. Below these sections, a note says '... or clone one of the 12,103 appliances shared in [SUSE Gallery](#)'. The next section, 'Select your architecture', shows a single option '64-bit' selected. The final section, 'Name your appliance', contains a text input field with 'Bíblia Hacker's openSUSE Leap 42.1, GNOME desktop' and a note 'This can be changed later', followed by a green 'Create appliance' button.

Você também pode começar sua distribuição personalizada clonando uma das 12.103 distribuições criadas e disponibilizadas na **SUSE Gallery**:



<https://susestudio.com/browse>

4. Feito isto você vai parar em outra tela, onde deverá fazer todos os ajustes necessários para criar sua distribuição. Observe nas abas as opções:

 - **Start** – que é a tela que está aparecendo na figura abaixo, onde só dá para mudar o nome da Appliance.

The screenshot shows the SUSE Studio Start tab interface. At the top, there's a navigation bar with links for 'Send feedback', 'Gallery', 'Home', 'Joao da Silva', 'Help', and 'Sign out'. Below the navigation bar, there's a section for 'Software information' showing '0 patterns selected', '36 packages selected', and '756 total packages'. The main content area features a yellow speech bubble with the text 'Welcome to SUSE Studio! Configure your appliance using the tabs above.' and 'When you're finally done making everything the way you want, visit the Build tab to generate your appliance.' Below this, there's a note 'But first, give your appliance a name! It will be used in the boot screen, and in several other places.' To the right, there's a large cartoon character of a robot holding a wrench. At the bottom, there's a field for 'Appliance name:' containing 'Biblia Hacker's openSUSE Leap 42.1, GNOME'.

- **Software** – que é onde você pode selecionar quais programas sua distribuição personalizada vai ter. Já começa com 36 de um total de 756 pacotes. Se algum pacote (programa) não estiver na lista dos 756, ele poderá ser incluído manualmente na aba **Files**.

Software sources

openSUSE Leap 42.1 OSS, openSUSE Leap 42.1 Updates

Add repositories... Upload RPMs...

Selected software

Packages: branding-openSUSE, e2fsprogs, gpxboot-branding-openSUSE, glibc, glibc-locale, gnome-power-manager, gnome-terminal, gnote, grub2, grub2-branding-openSUSE, gsettings-backend-dconf, gtk3-branding-openSUSE, gvfs-backends, iutils, kernel-default, less, libgnomesu, patterns-openSUSE-base, patterns-openSUSE-gnome, patterns-openSUSE-gnome_utilities, patterns-openSUSE-minimal_base, plymouth, sax3, SuSEfirewall2, syslog-ng, timezone, vim, x11-tools, xorg-x11, xorg-x11-driver-input, xorg-x11-driver-video, xorg-x11-fonts, yast2-control-center-gnome, yast2-firstboot, yast2-x11, zypper

- **Configuration** – esta aba é a que realmente personaliza a distribuição. Aqui você define idioma, layout do teclado, fuso horário, senha do administrador (root), comportamento ao iniciar (Startup), imagem da área de trabalho, configuração de rede, etc.

Default locale

Language: English (US)
Keyboard Layout: English (US)

Default time zone

Region: Global
Time Zone: UTC

Network

Do not configure network
Configure network during first boot
Use NetworkManager to configure the network at run-time

Firewall

Enable firewall
Open SSH port (22)
Open HTTP ports (80, 443)

- **Files** – nesta opção você pode incluir pacotes de programas que não estejam entre as opções disponíveis na aba **Software**.

The screenshot shows the SUSE Studio interface with the 'Files' tab selected. On the left, there's a sidebar with software information: 0 patterns selected, 36 packages selected, and 756 total packages. The main area is titled 'Overlay files' and contains instructions about what happens when files are added. Below this is a table with columns: Name, Directory, Extract, Size, Owner/Group, and Permissions. At the bottom of the table are buttons for 'Select all / Select none', 'Disable', 'Enable', 'Move / Rename', 'Edit details', and 'Remove'. There are also buttons for 'Upload file...' and 'Add from the Web (URL)...'.

- **Build** – aqui você define o tipo de mídia que vai criar. Se vai ser um Live DVD, se vai ser a imagem (ISO) para gravar um DVD, se vai ser um arquivo para abrir em máquina virtual (VMWare ou VirtualBox). A opção marcada por padrão é para usar em pen drive ou instalar no HD. Repare que na parte de cima, logo abaixo do nome do arquivo, tem uma previsão do tamanho que está.

The screenshot shows the SUSE Studio interface with the 'Build' tab selected. On the left, there's a sidebar with software information: 0 patterns selected, 36 packages selected, and 756 total packages. The main area has a 'Version' input field set to '0.0.1'. Below it, a 'Default format:' dropdown is set to 'USB Stick / Hard Disk Image'. To the right is a 'Build' button with a gear icon. Underneath are several checkboxes for additional formats: 'Live CD / DVD (.iso)', 'Preload ISO (.iso)', 'VMware Workstation / VirtualBox (.vmdk)', 'OVF Virtual Machine / ESXi (.ovf)', 'Xen guest (.img)', and 'SUSE Cloud / OpenStack / KVM (.qcow2)'. At the bottom is a link 'Read more about formats...'

- **Share** – é onde você poderá compartilhar sua distribuição personalizada do SUSE Linux na SUSE Gallery.

The screenshot shows the SUSE Studio interface. At the top, there's a green header bar with the SUSE Studio logo, a feedback button, and user account links for "Home", "Joao da Silva", "Help", and "Sign out". Below the header, a banner displays the title "Bíblia Hacker's openSUSE Leap 42.1, GNOME desktop" along with system details: "64-bit x86, based on openSUSE Leap 42.1", "400 MB download, 1.5 GB uncompressed", and package counts ("0 patterns selected", "36 packages selected", "756 total packages"). The main content area is titled "Appliance summary" and contains fields for "Description" (with a rich text editor), "Website", and "Tags", each with an associated input field. A "Save summary" button is located at the bottom right of this section. On the left side, a sidebar titled "Software information" provides a summary of the selected packages.

Isso é tudo o que você precisa para criar em menos de dez minutos, uma distribuição personalizada do Linux baseada na distribuição SUSE Linux. E se restou alguma dúvida sobre este processo, assista nossa videoaula² demonstrando como criamos uma distribuição Linux para a **Bíblia Hacker**.

Não deixe de pesquisar na SUSE Gallery as distribuições personalizadas para forensic, hacking e pentesting:

The screenshot shows the SUSE Gallery interface. At the top, there's a green header bar with the SUSE Studio logo, a search bar, and user account links for "Studio", "Joao da Silva", "Help", and "Sign out". A "Create new appliance..." button is located in the top right. Below the header, a search bar and a "Create new appliance..." button are visible. The main content area features a card for "Cherri Linux", which has a 5-star rating. It includes details such as "Published by Joshua Pritsker", "Based on openSUSE Leap 42.1 64-bit x86", and a description: "Cherri Linux is an operating system that is focused on penetration testing and ethical hacking and is based off openSUSE.". It also lists "Version 2.0.4" and "Updated about a year ago", a "Clone appliance..." link, and a "Testdrive" section with a preview image. Below this, a "Download" section shows statistics: "Downloaded 76 times" and "Cloned 63 times", with options for "Physical", "Virtual", and "Cloud" formats. A "Tags" section at the bottom lists "hacking, pentesting, linux, cherry".

² Disponível em www.fb.com/abibliahacker apenas para os compradores do livro.

Criar uma distribuição personalizada do Linux há alguns anos era algo impossível para um leigo ou iniciante. Agora é muito fácil fazer isto com resultados excepcionais.

O pessoal que criou o Backtrack e depois o Linux Kali fez algo parecido com o passo a passo que você acabou de ver. Só que uma distribuição como a Backtrack ou Kali não dá para fazer usando estes serviços de personalização automáticos. O nível de personalização do Backtrack ou do Kali só é possível criando a distribuição a partir do zero. E foi isso que os caras fizeram.

Distribuição Linux Kali

A distribuição Linux Kali é uma distribuição baseada no Debian, como já dissemos, considerado o sucessor do Linux BackTrack. É voltada principalmente para auditoria e segurança de computadores em geral, motivo pelo qual tornou-se uma distribuição Linux bastante querida também pelos hackers. É desenvolvida e mantida pela Offensive Security Ltd. desde 2016. É uma distribuição *rolling-release*³.

O Linux Kali dispõe de muitos softwares pré-instalados como, o Nmap (port scanner), Wireshark (um sniffer), John the Ripper (crackeador de password) e Aircrack-ng (software para testes de segurança em redes sem fios).

O sistema pode ser utilizado a partir de um Live CD ou de um pen drive, além de poder ser instalado como sistema operacional principal. É distribuído em imagens ISO que podem ser baixadas do site oficial:

www.kali.org

³ Em software, rolling release é um termo empregado para se referir a um sistema de software que se encontra em constante desenvolvimento, que é o oposto do modelo onde versões são liberadas em determinados períodos de tempo. O sistema de rolling release é comumente utilizado em distribuições de sistemas operacionais que passam por atualizações constantes ao invés de lançamentos periódicos.

O grande mérito do Kali é vir com centenas de ferramentas úteis para teste de invasão, perícia forense computacional e também para ações hacker. Obviamente não é o tipo de Linux que se instale em um computador para uso doméstico ou diário. É um Linux feito por e para hackers e profissionais de segurança.

Este grande número de ferramentas acaba confundindo a cabeça de quem se aventura a fazer o download do Kali por conta própria e sair usando. Para dominar o Kali primeiro você precisa entender de Linux.

No decorrer dos doze volumes da Bíblia Hacker daremos todas as informações necessárias para você poder usar tanto o Linux como o Linux Kali.

Para começar vamos fazer com que em menos de dez minutos você já consiga usar o Kali como parte de uma ação hacker. Está pronto? Então siga o nosso tutorial passo a passo:

1. Faça o download da imagem de instalação do Linux Kali em:

www.kali.org/downloads

ou

<http://cdimage.kali.org/kali-weekly/>

2. Repare que existem muitas opções de Kali, algumas para processadores de 32 bits outras para processadores de 64 bits. Se você não souber se o seu processador é de 32 ou de 64 bits, vá até **Pesquisar** de qualquer versão do Windows e digite **Informações do sistema**. Ao pressionar ENTER vai abrir a janela com o mesmo nome e em **Tipo do sistema** estará informando se é 32 ou 64 bits.
3. Uma vez decidido se vai fazer o download da versão de 32 ou de 64 bits, você precisa tomar mais duas decisões: se vai querer a versão

Light ou completa? Eu recomendo a versão completa cujo arquivo tem aproximadamente 2,7GB. A versão Light não chega a 1GB e pode acontecer de demonstrarmos um recurso na **Bíblia** ou nas videoaulas que a versão Light não tem.

A outra decisão que você precisa tomar diz respeito a interface gráfica.

As opções são:

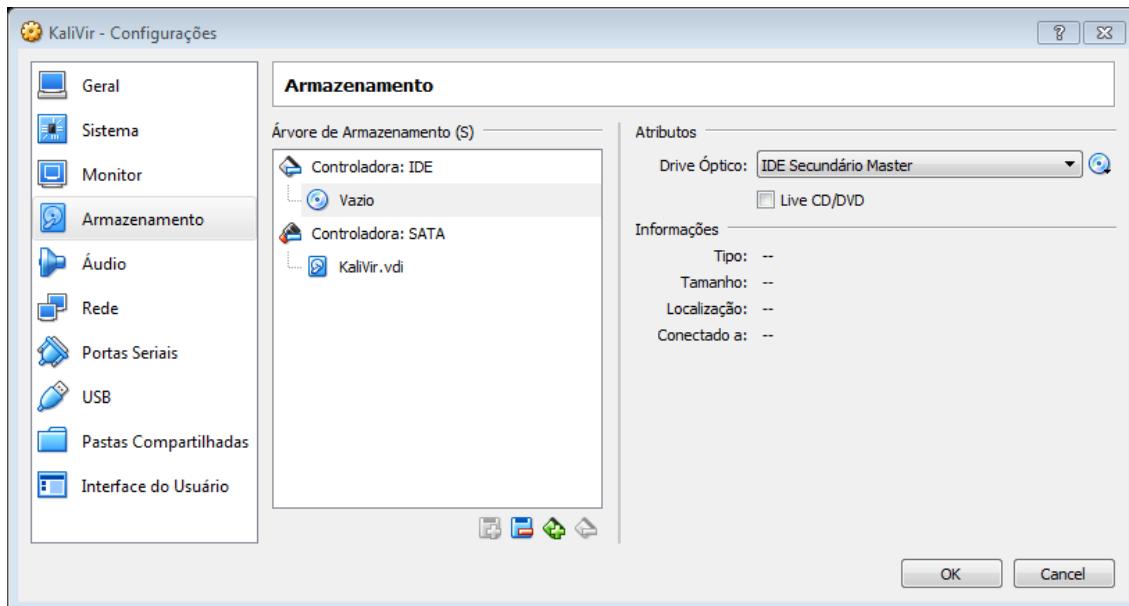
- E17 (Enlightenment 0.17)
- MATE Desktop Environment (continuação do GNOME 2)
- XFCE (parecida com o GNOME 2)
- LXDE (Lightweight X11 Desktop Environment) (indicada para computadores antigos ou com poucos recursos)
- KDE (K Desktop Environment)

Nós vamos ficar com a KDE por ser a mais tradicional e a que você encontra fácil em praticamente qualquer distribuição Linux. Assim, quando usar outro Linux que não seja o Kali, não vai estranhar tanto.

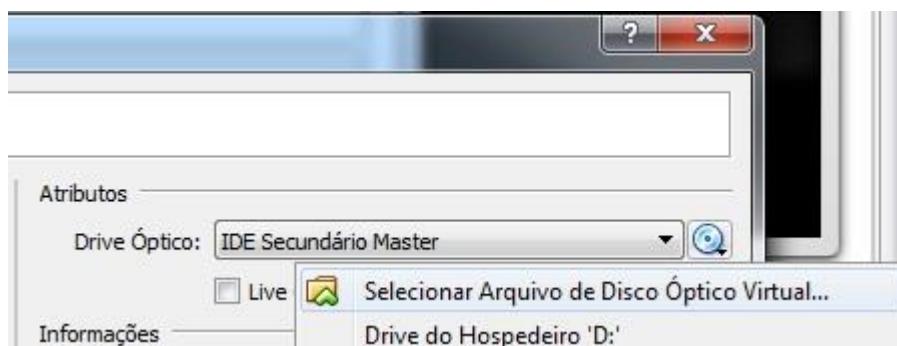
4. Após fazer o download abra o arquivo de imagem (ISO) do Kali no VirtualBox. Você já leu sobre o VirtualBox neste volume da Bíblia Hacker e deve ter assistido nossas videoaulas, então não terá dificuldade para fazer isto, pois basta clicar sobre o nome da máquina virtual (KaliVir, em nosso exemplo) e depois em **Configurações**:



5. Em **Configurações** selecione **Armazenamento**. Na janela **Árvore de Armazenamento** clique sobre o ícone do **DVD Vazio**.



6. Em seguida do lado direito, clique sobre o ícone do DVD e depois em **Selecionar Arquivo de Disco Óptico Virtual...**. Você deverá localizar o arquivo de imagem (ISO) do Linux Kali para que ele seja usado pela máquina virtual **KaliVir**.



7. Após carregar o arquivo de imagem (ISO) clique em **Iniciar**. Isto tem o efeito de ligar um computador real:



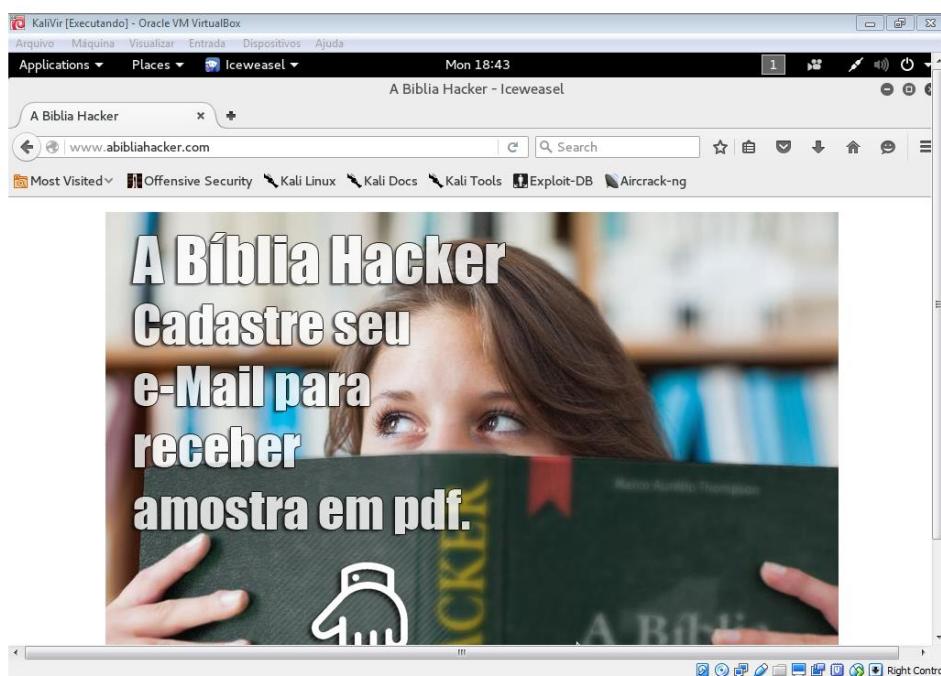
8. Esta é a tela inicial do Linux Kali. Podemos usar a opção **Graphical install**, opção que inclui a interface gráfica com o usuário. Mas como queremos apenas demonstrar o funcionamento vamos ficar com a primeira opção que já estará marcada (Live). Se você nunca viu o Linux sendo ligado não se preocupe com o texto que vai aparecer rolando na tela. Faz parte da inicialização (boot) do Linux.



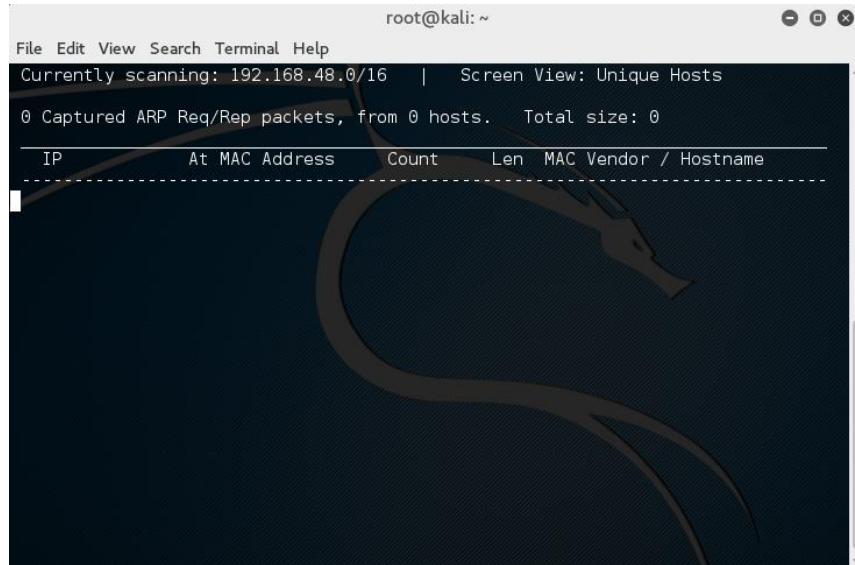
- **Live** - roda direto do DVD ou da imagem (ISO) na máquina virtual, sem precisar instalar.
 - **Live USB** – roda direto do pen drive.
9. Se tudo ocorrer como o esperado você verá a seguinte tela:



10. Normalmente a rede e a Internet compartilhada já devem estar funcionando. Faça um teste acessando uma página qualquer na Internet. O navegador instalado no Kali é o **IceWeasel**. Para acessá-lo vá até a parte superior esquerda do Kali. Clique sobre **Applications**. Siga até o final da lista onde está escrito **Usual applications** e procure por **Internet**. Depois por **IceWeasel**. Se tudo estiver funcionando você poderá usar o IceWeasel para navegar na Internet:



11. Vamos usar a primeira (de muitas) ferramentas hacker do Linux Kali. Em **Applications** você encontra quatorze categorias de ferramentas totalizando mais de 300 ferramentas dos mais variados tipos. Como neste volume da **Bíblia Hacker** nós estamos trabalhando com scanner de portas, é ele que vamos ver. Os scanners de portas estão no primeiro grupo de ferramentas do Linux Kali, em **01 – Information Gathering** (Coleta de Informações). Procure por **netdiscover** e quando a janela do terminal abrir, apenas digite **netdiscover** seguido de **ENTER**.



12. Todo isto está demonstrado nas videoaulas que disponibilizamos em nosso grupo fechado do Facebook.

Você acaba de

- Baixar
- Instalar
- Testar a conexão com a rede e com a Internet
- Usar uma ferramenta de varredura de portas

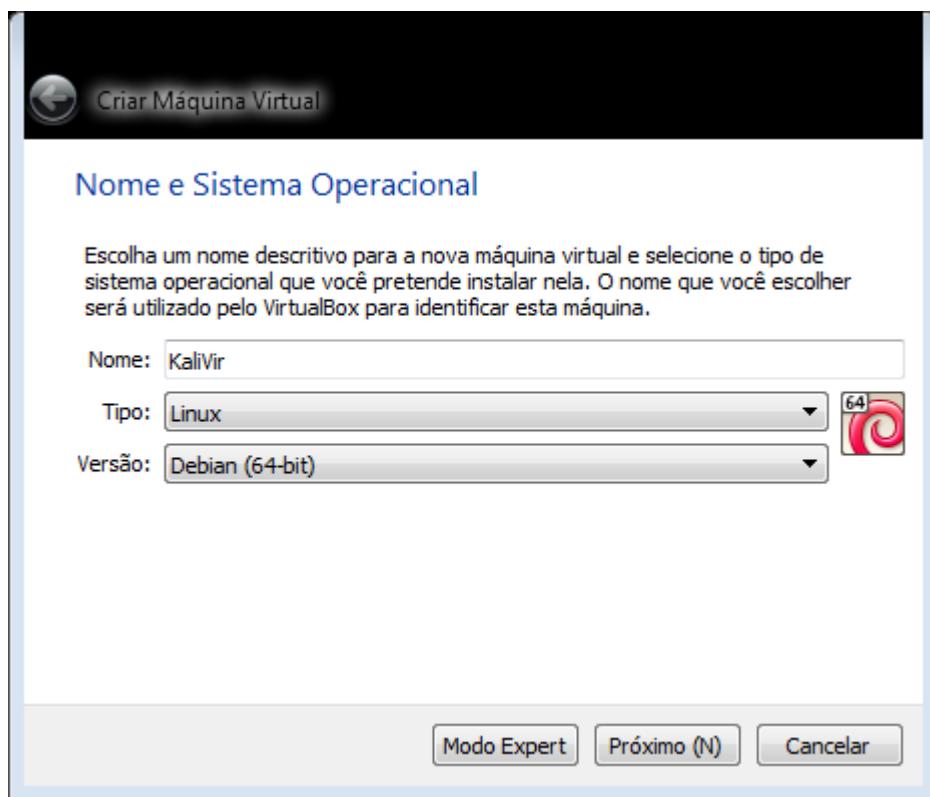
Tudo no Linux Kali. Daremos prosseguimento a este assunto no próximo e em todos os volumes da **Bíblia Hacker**. A cada volume você se tornará mais hábil no uso do Linux Kali, podendo usar este conhecimento em outras distribuições Linux. Até na sua própria distribuição se quiser.

Preparando o VirtualBox para o Linux Kali

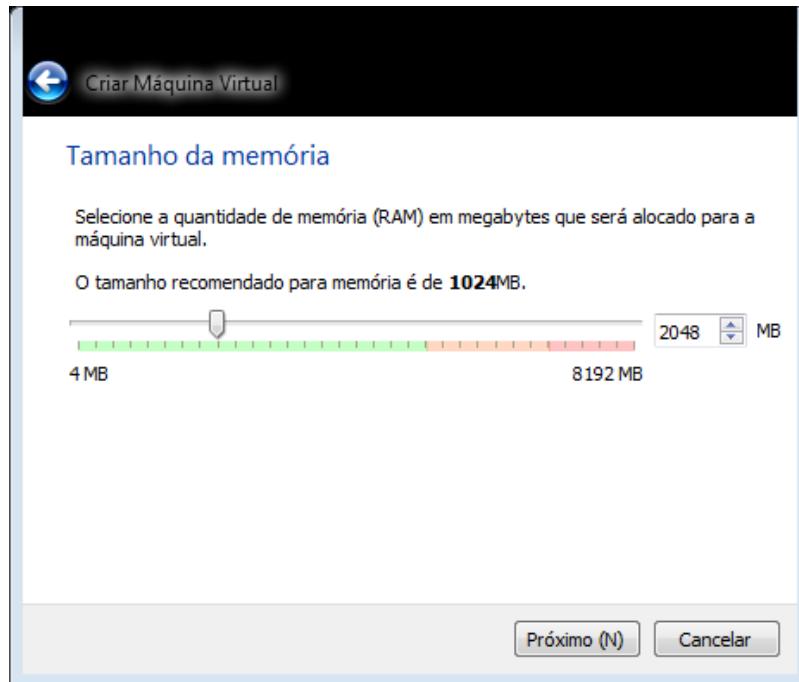
Apesar de neste volume da **Bíblia Hacker** já termos demonstrado como criar máquinas virtuais, por via das dúvidas vamos demonstrar passo a passo como criar a máquina virtual para receber o Linux Kali.

Estamos partindo da suposição de que você já baixou o arquivo de imagem (ISO) do Linux Kali e que o VirtualBox já está instalado em seu computador. Estamos usando o VirtualBox versão 5.1.22 que era a versão mais recente disponível quando escrevemos este capítulo. Este detalhe pode fazer a diferença na hora de seguir o passo a passo, pois de uma versão para outra algo pode mudar. A título de comparação, só recentemente o VirtualBox passou a apresentar o Windows Server 2016 na lista de sistemas operacionais pré-configurados. Dito isto é só seguir nosso passo a passo:

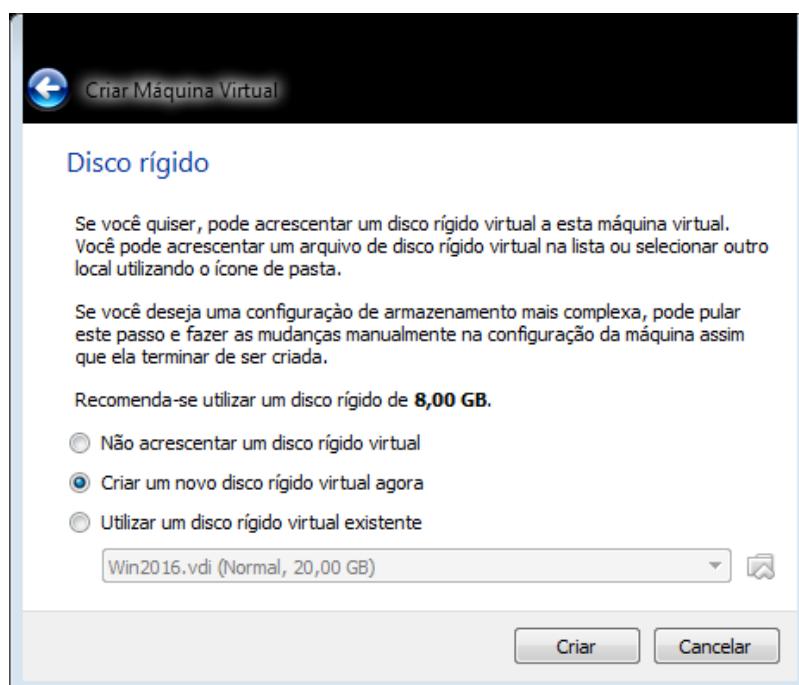
1. Com o VirtualBox aberto clique em **Novo** para criar uma nova máquina virtual. Nesta opção você deverá definir um nome para a máquina virtual, selecionar a plataforma e definir o sistema operacional de referência. Para o Linux Kali usaremos o nome **KaliVir**, a plataforma **Linux e Debian (64 bits)** como distribuição de referência. Como não tem a opção Kali usaremos a distribuição que lhe deu origem.



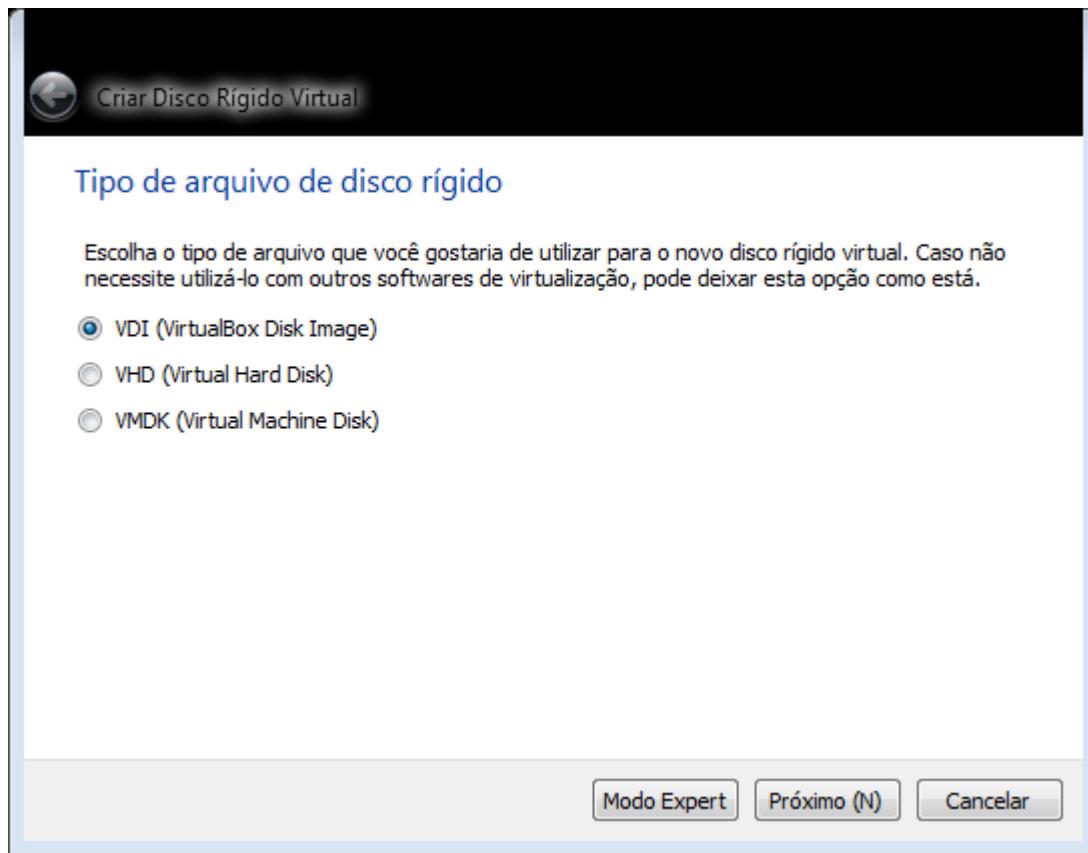
2. O próximo passo é definir quanta memória RAM vamos destinar ao Linux Kali. Dá para trabalhar com o Kali a partir de 512MB mas o ideal é ter 1GB de RAM virtual. Como no exemplo estou com 8GB de RAM vou dedicar 2GB (2.048MB) para o Kali.



3. Precisamos criar um disco virtual agora. É só deixar como está e clicar em **Próximo:**



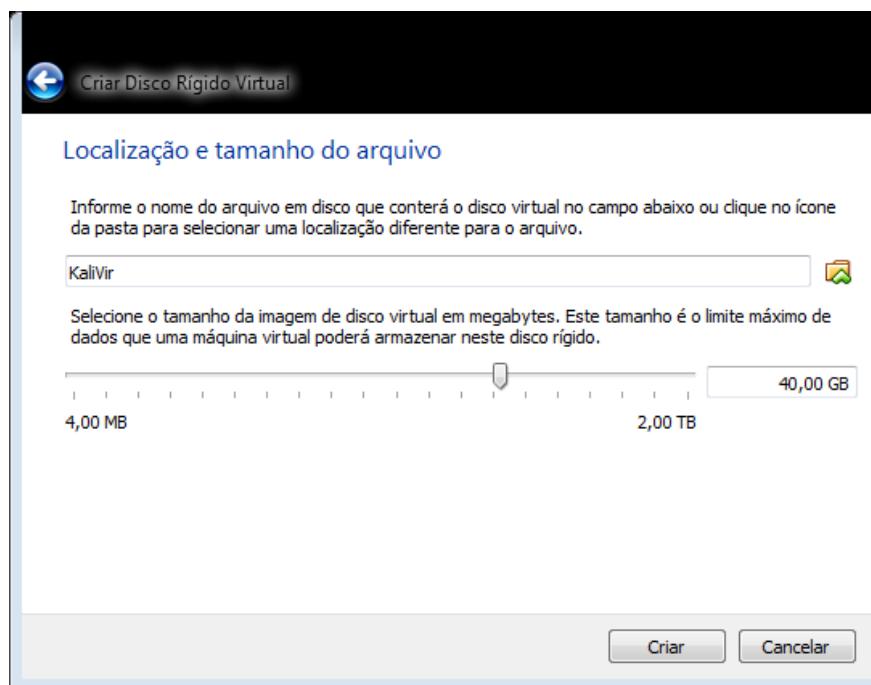
4. O VirtualBox oferece três formatos de disco virtual. Como não pretendemos compartilhar nosso disco virtual com outros programas de virtualização, como o VMWare ou Virtual PC, ficaremos com o VDI que é o formato nativo do VirtualBox:



- VDI é o formato nativo do VirtualBox
 - VMDK é o formato original da VMWare e também é aceito pelo VirtualBox
 - VHD é o formato nativo do Microsoft Virtual PC e também é aceito pelo VirtualBox
5. Já vimos sobre isso. Optamos pelo disco **Dinamicamente alocado** que é o que cresce conforme for recebendo arquivos. Se usarmos o **Tamanho fixo** vamos ter um arquivo de HD virtual enorme ocupando espaço no disco rígido sem necessidade.



- O tamanho máximo do disco rígido virtual pode ser de até 2TB. Vamos criar um disco virtual de 40GB que é o suficiente. Certifique-se de ter estes 40GB de espaço livre no seu disco rígido. Se não tiver espaço livre no disco rígido crie o disco para o Kali virtual com pelo menos 10GB:



Se você quiser alterar a localização do disco virtual clique sobre a pastinha amarela que aparece do lado direito.

7. Isto é tudo o que você precisa fazer para preparar o VirtualBox para receber o Kali Linux.

Nos próximos volumes da **Bíblia Hacker** vamos demonstrar cada uma das quatorze categorias de ferramentas do Kali Linux. Sempre explicando porque e quando usar, com exemplos de uso. Também veremos como usar a mesma ferramenta em qualquer Linux, para que você não fique preso(a) ou limitado(a) ao Linux Kali.

Tux

O Tux é o pinguim símbolo do Linux. Dizem por aí que a escolha de um pinguim como símbolo é por que um pinguim mordeu o Linus Torvalds quando ele visitava um zoológico. Será que é isso mesmo? Você vai descobrir a verdade quando fizermos a resenha do livro **Just for Fun** (Só por Prazer), onde o Linus Torvalds desvenda a escolha do pinguim como mascote do Linux.



Marco Aurélio Thompson

ÔLIVRO DO HACKER 2018

300 PÁGINAS DE TUTORIAIS

* Windows Server 2016 * Kali Linux * Android *



Nossos Contatos

IMPORTANTE: Estamos abandonando o e-mail como canal de comunicação. O motivo é que muitas das mensagens enviadas por nós ou para nós, não chegam. Provedores e sistemas antivírus e AntiSpam têm bloqueado mensagens que incluem a palavra *hacker*. Para evitar que a sua mensagem não chegue e você pense que nós não respondemos e também para evitar que respondamos, mas nossa mensagem não chegue até você, por favor entre em contato conosco por qualquer um dos canais abaixo, exceto por e-mail:

- **WhatsApp**
 - +55 (71) 9-9130-5874
- **Facebook**
 - www.fb.com/abibliahacker
 - www.fb.com/marcoaureliothompson
- **LinkedIn**
 - www.linkedin.com/in/marcoaureliothompson/
- **Site**
 - www.abibliahacker.com
- **Plataforma Lattes**
 - <http://lattes.cnpq.br/0072812690655821>

Nossos Livros no Skoob

Para saber quais livros já temos lançado acesse o Skoob em:

www.skoob.com.br/autor/livros/12924

skoob

Busque por título, autor, editora, ISBN...

Explorar

Entrar

Marco Aurélio Thompson

Seguir

Biografia

Livros publicados

57

Vídeos

1

Seguimentos

1

Leitores

252

Editar

Livros Publicados

57 encontrados | exibindo 1 a 57



Somos a maior rede social do Brasil 100% focada em leitores. Funcionamos como uma estante virtual onde você pode colocar os livros que já leu, como aqueles que ainda deseja ler. Compartilhe suas opiniões com seus amigos... [Leia mais](#).

[FAQ](#)
[Quem Somos](#)
[Blog](#)
[Cadastro de livros](#)
[Cadastro de autores](#)
[Downloads](#)
[Fale Conosco](#)



Baixe nosso app



Projeto Wikilivros

Sem sombra de dúvidas a Wikipédia tem se tornado uma das maiores fontes de informação classificada de que sem tem notícia. Mas por ser uma plataforma colaborativa, não podemos confiar plenamente nas informações disponíveis na Wikipédia.

Por outro lado, a Wikipédia pode ser o ponto de partida para pesquisas que depois serão aprofundadas. Seus milhares de artigos cobrem praticamente qualquer assunto e quase sempre incluem links e referências para consulta.

Pensando em uma forma de organizar os artigos da Wikipédia nós criamos o projeto Wikilivros, com livros criados a partir dos artigos da Wikipédia. O mérito do projeto é organizar os assuntos na forma de um livro, incluindo apresentação, introdução e comentários. Com isso esperamos facilitar o trabalho do estudante, universitário ou pesquisador, uma vez que se dependesse de ler artigo por artigo talvez não conseguissem reunir toda a informação sobre o assunto que está disponível na Wikipédia.

Existem ocasiões que não se sabe o que está procurando e ao encontrar os artigos reunidos na forma de um livro, vai poupar tempo e trabalho de pesquisa. É como se você já encontrasse a pesquisa adiantada, só precisando prosseguir a partir daí.

Para ajudá-lo(a) ainda mais incluímos exemplos de citações e referências que você pode usar no seu TCC e outros trabalhos acadêmicos. Geralmente os professores pedem para evitar referenciar a Wikipédia, mas como se trata de referenciar um livro, esta observação não se aplica.

Os Wikilivros são de distribuição gratuita e podem ser lidos em nossa página no ISSUU:

www.issuu.com/editoradoautor

Para saber quais Wikilivros já foram criados acesse:

www.wikilivros.org

Seja avisado dos próximos lançamento seguindo nossa página no Facebook:

www.fb.com/WikilivrosBr

E se você quiser adquirir e receber em casa pelo correio a versão impressa do seu Wikilivro preferido e assim ajudar a manter o projeto, procure por Wikilivros no Clube de Autores:

www.cludedeaautores.com.br



Marco Aurélio Thompson

GRÁTIS

O que é A Bíblia HACKER?

www.abibliahacker.com

Marco Aurélio Thompson

A Bíblia HACKER

www.abibliahacker.com



2018

