GUIA DE ESTUDOS PARA SE TORNAR UM HACKER

O que você vai encontrar nesse **guia?**

Aqui vou tentar compartilhar algumas dicas de estudos para aqueles que querem entrar para a área de cybersecurity, principalmente pentest/ethical hacking, que é o meu foco e obviamente o que eu tenho mais propriedade para falar, tudo aqui é baseado na minha experiência pessoal, coisas que eu estudei, uso para estudar e erros que eu cometi e quero que você evite para não perder tempo.

Seguindo o que vou passar aqui você vai chegar pelo menos no nível de resolver CTFs (capture the flag) e consequentemente ter alguma experiência para apresentar em entrevistas de emprego.
Lembre-se que não estou te oferecendo nenhuma fórmula mágica para aprender em 2 semanas, apenas estou tentando facilitar o seu caminho nessa jornada que é longa.

"O preguiçoso deseja e nada consegue, mas os desejos do diligente são amplamente satisfeitos." - Provérbios 13:4

Minha intenção não é montar um cronograma de estudos, mas tentarei manter uma ordem de prioridades das coisas, se você vai ver mais de uma coisa ao mesmo tempo, se vai tentar terminar um livro para então iniciar outro é uma escolha totalmente sua e também vai de você entender o que funciona melhor para você nessa questão, mas digo que não precisa se tornar um especialista em um assunto para partir para outro, é muito possível avançar antes disso, apenas não se esqueça de continuar buscando conhecimento sobre aquele assunto, o que irá te tornar um hacker de verdade é conhecer as coisas bem e no nível "mais baixo".

OBS: No final do arquivo tem um compilado de todos os materiais de estudo mencionados aqui e alguns extras.

Dica principal para todos:

Aprenda inglês caso ainda não saiba, é a principal língua da área, é muito mais fácil de se encontrar material para estudo, até mesmo quem não tem o inglês como língua materna acaba MUITAS VEZES produzindo em inglês, e sempre as coisas saem primeiro em inglês do que em português, por exemplo, divulgação de analise de novas vulnerabilidades.

Para quem é um completo iniciante na área de T.I de forma geral :

Caso você não tenha nenhuma experiência com programação, principalmente na parte de criar sites, comece estudando isso, vai te ajudar a entender o conceito por trás das vulnerabilidades que acontecem neste ambiente, não precisa estudar ao ponto de se tornar um desenvolvedor Senior, apenas ser capaz de criar um site básico onde tenha front-end e back-end, comunicação com um banco de dados (SQL e NoSQL) e um sistema de login, o famoso CRUD (Create, Read, Update & Delete).

Existem algumas pessoas que inclusive são da área e que dizem que um hacker não precisa saber programar, isso pode até funcionar para essa pessoa, mas na minha opinião e de várias outras pessoas que são muito influentes na área.

Não saber programar é muito mais um ponto negativo do que positivo, afinal você vai estar sempre dependendo de outras pessoas, vai depender que outros criem ferramentas, criem exploits e outras coisas.

Um exemplo disso para quem assistiu Mr Robot (se não assistiu recomendo muito, pelo entretenimento mesmo), provavelmente se lembra que em um episódio a tentativa de ataque deles acaba falhando por utilizar uma ferramenta muito conhecida por não terem muito tempo, e surge esse assunto de que se tivessem mais tempo teriam feito um código do zero e teria muito mais chance de funcionar, pois quando uma ferramenta se torna muito conhecida, os payloads gerados por ela passam a serem detectados facilmente por antiviris e outros tipos de proteção.

Qual linguagem você deve escolher?

Sinceramente não existe uma resposta correta para isso, a base de programação é basicamente a mesma em qualquer linguagem e quando falamos de hacking é certo que você vai ter que lidar com diferentes tecnologias o tempo todo, mas existem algumas que são mais comuns de se aparecer, como o PHP por exemplo, você também poderia focar em javascript tendo em vista que você pode usar no back-end (NodeJS) e obviamente vai precisar para o front-end e uma das vulnerabilidades mais comum em sites é o XSS que acontece justamente no javascript.

Passando da parte de aprender programação :

Imago que você já saiba fazer um site, mas pode ser que você ainda não saiba os detalhes de como isso funciona além da parte de programação, então busque aprender sobre HTTP/HTTPS, DNS, como funciona uma URL, Cookies, SSL, e todas as outras coisas que são utilizadas em um site, afinal cada parte pode ser uma janela para vulnerabilidades.

A Mozilla (*a empresa do navegador mozilla firefox*) tem um site "*developer.mozilla.org*" que conta com documentação de diversas coisas relacionadas a internet/sites, lá podemos encontrar sobre HTTP e cada parte de um site, alguns exemplos:

Cookies, CORS, Request Methods.

O site da Mozilla é uma ótima fonte de estudos para tudo relacionado a sites e também para programação em diversas linguagens.

Estudando as vulnerabilidades web:

Os dois melhores recursos para aprender sobre a parte de vulnerabilidade em ambiente WEB é o *OWASP* e o site *Portswigger Academy. O OWASP* vai ter mostrar a parte teórica das vulnerabilidades, já no *Portswigger* você encontra sobre a parte teórica e também prática, lá temos diversos "*laboratórios*" onde podemos treinar a exploração de muitos tipos de vulnerabilidades diferentes, caso você tenha dificuldade de resolver algo é muito tranquilo de achar alguém que já resolveu aquele desafio e compartilhou a resposta (*mais para frente eu falo como usar esse tipo de coisa para estudar*).

No site da Portswigger temos laboratórios para diversas vulnerabilidades possíveis em um ambiente web (talvez para todas) e para cada vulnerabilidade, vários desafios diferentes, você vai passar alguns dias se divertindo por lá.

Uma ferramenta muito utilizada para fazer testes em ambiente web é o burp suite, que por um acaso é desenvolvido pela portswigger. Você com certeza vai precisar utilizar essa ferramenta, uma outra alternativa é o OWASP Zap, mas creio que o burp seja mais utilizado, e particularmente acho mais agradável de se usar.

Estudando as vulnerabilidades na parte de infra (Sistemas operacionais e redes):

A parte de infra é com certeza mais extensa do que a parte de web, afinal temos Windows, Linux, Redes e até mesmo MacOS (esse é menos utilizado) para ver.

Se você tem o interesse em hacking você com certeza já ouviu falar em Kali linux e provavelmente já até tem ele instalado em uma VM (Máquina Virtual), se não tiver, comece por aí.

Caso você seja um usuário de MacOS, o ParrotOS é uma alternativa ao Kali que tem um pouco mais a cara do MacOS.

REALMENTE PRECISA DO KALI LINUX?

Não, mas é o mais popular e já vem com praticamente tudo que você irá precisar instalado, então economiza tempo.
E com a experiência você vai perceber que não importa tanto o sistema operacional que você está usando, mas sim se você sabe o que e como fazer.

E com isso obviamente você vai precisar aprender pelo menos o básico de Linux, alguns comandos, como se localizar nas pastas, onde fica alguns documentos (grande maioria, se não todas as configurações do Linux, são feitas em arquivos de texto).

Para essa parte dos estudos focaremos principalmente no site TryHackMe, que é um site de CTFs e tem centenas de “laboratórios” para estudo, procure por “Linux Fundamentals tryhackme”.

OBSERVAÇÃO :

Na TryHackMe os desafios são chamados de “rooms” e lá tem tanto “rooms” grátis quanto alguns que apenas quem tem assinatura do site consegue ter acesso, mas mesmo assim a quantidade de gratuitos é enorme, esses “rooms” possuem diferentes tipos de dificuldade (fácil, médio, difícil e insano) e também existe a categoria “walkthrough”, onde ele te dá o passo a passo do que precisa ser feito, o que obviamente é melhor para quem ainda está começando.

Além dos “*Linux essentials*” também é essencial fazer os que são relacionados a redes (network), algumas opções são, “*what is networking*”, “*introductory networking*”, e também é importante ver Windows, onde temos também os “Windows fundamentals”, na parte de Windows temos um assunto extra que é o “Active Directory” que é utilizado em empresas, e consequentemente você terá que lidar com isso.

Como foi o meu estudo nessa parte :

Eu comecei focando em Linux e redes, quando já estava me sentindo confortável comecei a focar na parte de Windows, não precisa seguir essa regra, veja como vai ser melhor para você, apenas tenha em mente que o Windows é sim muito importante de se aprender

e redes é com toda certeza algo indispensável, mas não significa que você precisa se tornar um especialista antes de partir para a próxima etapa.

Começando a ação na parte de infra:

Obviamente a melhor opção para começar é com os “*walkthtrough*” mencionados anteriormente, para que você entenda como funciona a dinâmica, para que você possa se familiarizar com algumas ferramentas e então começar a “*caminhar com suas próprias pernas*”.
Alguns “*rooms*” que acredito serem bons para te dar o contexto de ferramentas e dinâmica de um teste :

- *Intro to offensive security*
- *Nmap*
- *Vulnversity*
- *Metasploit*
- *Hydra*
- *Ice (focada em windows)*

Veja o compilado de recomendações no final do arquivo para mais opções.

A partir desse momento aqui pode ser que você enfrente algumas dificuldades mesmo com os “*rooms*” classificados como “walkthrough”, e não tem nenhum problema nisso, a grande maioria dos desafios da T*ryHackMe* é possível encontrar alguém que fez um tutorial deles ou um “*writeup*” (é a forma como chamamos um review de alguma vulnerabilidade ou resolução de um CTF, se acostume com esse nome que ele será bem presente na sua vida), mas é importante saber como utilizar esses writeup para estudar, não procure a solução e apenas cole lá na máquina para conseguir resolver, procure entender o que foi feito, como foi feito e por que foi feito, se algo for mencionado de diferente, como o nome de uma categoria de vulnerabilidade, procure mais matérias sobre essa vulnerabilidade, ou caso a pessoa tenha utilizado alguma ferramenta diferente, talvez valha a pena você pelo menos testar a ferramenta, treine seu cérebro para tratar os writeup dessa forma e não apenas como uma “cola” da época de escola.

Após finalizar alguns “walkthrough”, ter o conhecimento de algumas ferramentas, comece aumentar a dificuldade, apesar de eu ter falado sobre os writeup e que eles são de grande ajuda, é importante ter o cuidado de não ficar dependente deles, tente fazer o máximo que puder sem nenhuma ajuda e deixe para buscar a solução quando estiver mesmo sem mais nenhuma ideia.

Um outro site que segue o mesmo estilo do *TryHackMe* com CTFs é o *HackTheBox*, porém os desafios nele são mais complicados, um desafio que lá seria classificado como médio é equivalente a um desafio difícil na TryHackMe, então deixe o objetivo de estudar por lá no futuro, outra diferença é que eles não permitem fazer WriteUp das máquinas, apenas quando uma máquina é “aposentada”.

COMPILADO DE MATERIAIS PARA ESTUDO :

Para Web:

- MDN Web docs (developer.mozilla.org)
- OWASP Top 10
- Portswigger academy
- Portswigger blog
- root-me.org
- overthewire.org
- Bug bounty writeups
- TryHackMe OWASP Juice Shop
- TryHackMe sql injection lab
- Livro Web Hacking 101 (apenas em inglês)
- Livro The Web Applications Hacker’s Handbook (apenas em inglês)

Para Redes :

- TryHackMe What is networking
- TryHackMe Introductory Networking
- TryHackMe Intro to Lan
- TryHackMe Nmap
- Livro Tanembaum redes de computadores (devo dizer que esse livro não é um dos mais amigáveis, ele começa pela parte física da rede e chega até a mencionar parte de ondas magnéticas, ele é sim muito completo em detalhes, mas não uma leitura fácil para quem está iniciando)
- TCP IP for dummies
- TCP-IP illustrated Voulnme 1 (esse livro é muito mais amigável para iniciantes, mas acredito que só exista em inglês)
- Análise de tráfego TCP/IP com TCPDump – youtube canal Eriberto mota

Para sistemas operacionais :

- Livro Organização Estruturada de Computadores - Tannenbaum
- Livro Windows System Internals 7 edition
- Livro Como o linux funciona
- TryHackMe Linux fundamentals (1,2 e 3)
- TryHackMe Linux PrivEsc
- TryHackMe Linux Privilege Escalation
- TryHackMe Windows PrivEsc

Sites extras :

- HackXpert
- VulnHub
- PicoCTF