

**O que é hacker ético?**

E por que você deve ter membros na equipe preparados para se tornar um hacker ético certificado

Prof.º Denilce Veloso

Disciplina: Programação Web

BRAYAN GUILHERME BARBOSA 0030482021037

Sorocaba

Março/2022

**Índice**

1. Introdução
2. Pentester
3. Cursos

3.1. Certificado de Hacker ético

3.2. Sans GPEN

3.3. Certificado de segurança ofensiva

3.4**. Foundstone Ultimate Hacking**

3.5. **CREST**

**O que é hacker ético?**

1**. Introdução**

Se você não conseguir pensar como um hacker, será mais difícil se defender dos crakers. Essa é a premissa do hacking ético.

Uma falha de segurança pode causar prejuízos gigantescos em empresas, podendo causar roubo de informações e dinheiro, prejuízos à sua imagem, paralisação de seus serviços e diversos outros danos.

Devido a esses riscos, empresas das mais variadas áreas como bancos, telecomunicações, grandes corporações em geral, tem procurado por profissionais e empresas especializadas em Ethical Hacking.

**2.Pentester**

Um hacker ético (ou pentester, como também é comumente chamado), é um profissional de segurança especializado em Offensive Security, ou seja, na parte da cibersegurança que é mais focada em processos de identificação de vulnerabilidades e, consequentemente, no desenvolvimento de métodos de proteção. O que ele faz? Em linhas gerais, ser pago para tentar invadir sistemas, para detectar vulnerabilidades. Sua função é encontrar vulnerabilidades de segurança que um hacker malicioso poderia potencialmente explorar. Para tanto, precisa desenvolver habilidades em técnicas de penetração de sistemas.

Mas esses os testadores profissionais de penetração devem seguir um código de ética para orientar tudo o que fazem. O EC-Council, criadores do exame Certificated Ethical Hacker (CEH), possui [um dos melhores códigos de ética](https://www.eccouncil.org/code-of-ethics/) disponíveis.

Paciência, persistência e perseverança são qualidades importantes para Hackers Éticos devido ao período e nível de concentração necessária para obter sucesso na maioria dos ataques. Habilidades de programação web e banco de dados, bem como conhecimento aprofundado de redes de computadores, são bastante úteis para o hacker na realização de hacking ético e testes de vulnerabilidade.

Com base nesses conhecimentos fundamentais, o hacker ético irá utilizar técnicas específicas que irão permitir que ele invada e detecte as vulnerabilidades dos sistemas.  A maioria dos hackers éticos se torna profissional de teste de penetração aprendendo essas técnicas de duas maneiras: ou aprendendo habilidades de hackers por conta própria, ou tendo aulas formais. Muitos, como Roger Grimes, co-autor deste texto, fizeram as duas coisas.

1. **Cursos**

Embora às vezes ridicularizados por autodidatas, os cursos e certificações de hackers éticos muitas vezes são a porta de entrada para um bom trabalho como testador de penetração.

O currículo atual de educação em segurança de TI é repleto de cursos e certificações que ensinam alguém a ser um hacker ético. Para a maioria dos exames de certificação, o profissional pode estudar sozinho e levar sua própria experiência para o centro de testes ou fazer um curso de educação aprovado. Embora o profissional não precise de uma certificação para se empregar como testador profissional de penetração, ela sempre é bem-vinda.

Abaixo estão 5 cursos de hacking ético com certificações reconhecidas internacionalmente.

**3.1 Certificado de Hacker Ético**

O [Certificado de Hacker Hacker (CEH)](https://iclass.eccouncil.org/our-courses/certified-ethical-hacker-ceh/) do EC-Council é o mais antigo e mais popular curso e [certificação](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/) de intrusão. O curso oficial, que pode ser feito on-line ou com um instrutor ao vivo, contém 18 campos de assuntos diferentes, incluindo assuntos tradicionais de hackers, além de módulos sobre malware, wireless, nuvem e plataformas móveis. O curso remoto completo inclui seis meses de acesso ao [Cyber Range iLab](https://ilabs.eccouncil.org/cyber-range/) on-line, que permitirá aos alunos praticar mais de 100 habilidades de hackers.

A sessão para a certificação CEH requer um curso oficial ou, se for autodidata, uma prova de dois anos de experiência ou educação relevante. Ele contém 125 perguntas de múltipla escolha com um limite de tempo de quatro horas. Fazer o exame requer a aceitação do [Código de Ética do EC-Council](https://ilabs.eccouncil.org/cyber-range/), que foi um dos primeiros códigos de ética exigidos para os usuários de testes de segurança de computadores. O material didático e o teste são rotineiramente atualizados.

**3.2 SANS GPEN**

O SysAdmin, Networking e Security (SANS) Institute é uma organização de treinamento altamente respeitada, e tudo o que eles ensinam junto com suas certificações é muito respeitado pelos profissionais de segurança de TI. O SANS oferece vários [cursos e certificações para testes de intrusão](https://ilabs.eccouncil.org/cyber-range/), mas seu [GIAC Penetration Tester (GPEN)](https://www.giac.org/certification/penetration-tester-gpen) é um dos mais populares.

O curso oficial para o GPEN, [SEC560: Teste de intrusão em rede e Hacking ético](https://www.sans.org/course/network-penetration-testing-ethical-hacking), pode ser feito on-line ou presencialmente. O exame GPEN tem 115 perguntas, um limite de tempo de três horas e exige uma pontuação de 74% para passar. Nenhum treinamento específico é necessário para qualquer exame do GIAC. O GPEN é coberto pelo [código geral de ética do GIAC](https://www.giac.org/about/ethics), que eles levam muito a sério, como atestado por uma contagem de candidatos que foram desqualificados por violar o código.

O exame abrange tudo, desde abordagens técnicas detalhadas até testes em todo o escopo, regras de engajamento e relatórios. Ele é muito focado no cenário, portanto, apresentará um determinado cenário de teste de intrusão e perguntará qual é o melhor caminho a seguir. Ou, ele mostrará a saída de uma ferramenta e perguntará o que a ferramenta está dizendo e o que você deve fazer a seguir.

**3.3 Certificado de Segurança Ofensiva**

O curso e a certificação do [OFSC (Offensive Security Certified Professional)](https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/) conquistaram uma reputação de solidez bem merecida, com uma estrutura e um exame muito práticos. O curso oficial de treinamento individual é chamado de [Teste de Intrusão com Kali Linux](https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/) e inclui 30 dias de acesso ao laboratório. Por depender do Kali Linux (o sucessor da distro Linux favorita dos pentesters, BackTrack), os participantes precisam ter uma compreensão básica de como usar o Linux, bash shells e scripts.

O OSCP é conhecido por pressionar seus alunos e examinadores mais do que outros cursos de pentest. Por exemplo, o curso OSCP ensina e o exame exige a capacidade de obter, modificar e usar o código de exploração obtido publicamente.

Para o exame, o participante recebe instruções para se anexar remotamente a um ambiente virtual onde espera-se que ele comprometa vários sistemas operacionais e dispositivos em 24 horas e os documente completamente como ele o fez. O Offensive Security também oferece cursos e exames de pentests ainda mais avançados (por exemplo, envolvendo exploração da Web, exploração wireless e [exploração avançada do Windows](https://www.offensive-security.com/information-security-training/advanced-windows-exploitation/)). Os leitores podem querer tirar proveito de seu curso básico e gratuito de [Ferramenta Metasploit on-line](https://www.offensive-security.com/?s=metasploit+tool+course).

**3.4 Foundstone Ultimate Hacking**

A unidade de negócios Foundstone da McAfee foi um dos primeiros cursos práticos de teste de intrusão disponíveis. Sua série de livros e [cursos Ultimate Hacking](https://enosecurity.com/training-tutorials-courses/foundstone-ultimate-hacking-training/)) liderou o campo por um longo tempo. Eles cobriam Windows, Linux, Solaris, web, SQL e uma série de técnicas avançadas de hackers (como o tunelamento). Infelizmente, os cursos da Ultimate Hacking não têm exames e certificações formais.

Hoje, a Foundstone oferece uma [série de opções de treinamento](https://www.mcafee.com/us/services/education-services/security-training.aspx) que vão muito além dos testes de intrusão, incluindo análise forense e resposta a incidentes (como muitos dos outros participantes deste artigo). Além disso, a Foundstone oferece treinamento em hacking de internet das coisas (IoT), firmware, sistemas de segurança de controle industrial, Bluetooth e RFID. Os instrutores da Foundstone são frequentemente pentesters e consultores de segurança, embora muitos dos cursos de treinamento, se não a maioria, sejam feitos pelos parceiros.

**3.5 CREST**

Internacionalmente, os cursos e exames de teste de intrusão do organismo de certificação e credenciamento de garantia da informação da [CREST](http://www.crest-approved.org/), uma organização sem fins lucrativos, são comumente aceitos em muitos países, incluindo o Reino Unido, Austrália, Europa e Ásia. A missão da CREST é educar e certificar pentesters de qualidade. Todos os exames aprovados pela CREST foram revisados e aprovados pelo [Escritório Central de Comunicação do Governo do Reino Unido (GCHQ)](https://www.gchq.gov.uk/), que é análogo à NSA dos Estados Unidos.

O exame básico de pentesting da CREST é conhecido como CREST Registered Tester (ou CRT), e há exames para pentesters de Web e de infraestrutura. Os exames e os custos variam de acordo com o país. Os participantes do teste CREST devem rever e reconhecer o [Código de Conduta CREST](https://www.crest-approved.org/wp-content/uploads/2016/05/Code-of-Conduct_Individual.pdf). A certificação OSCP de Segurança Ofensiva pode ser usada para obter o CRT.

**Ferramentas de hacking ético**

Os hackers éticos geralmente têm um conjunto padrão de ferramentas de hacking que usam o tempo todo, mas podem precisar estocar ferramentas diferentes, dependendo da especificidade do trabalho. Por exemplo, se o pentester for solicitado a atacar servidores SQL e não tiver experiência relevante, ele pode começar pesquisando e testando diferentes ferramentas de ataque SQL.

A maioria dos pentesters começa com uma “distro” do SO Linux especializada em testes de intrusão. Distribuições Linux para hackers vêm e vão ao longo dos anos, mas atualmente a [distro Kali](https://www.kali.org/) é a mais profissional e a preferida dos hackers éticos. Existem milhares de ferramentas de hackers, incluindo um [conjunto de robustas](https://www.csoonline.com/article/2943524/network-security/17-pen-testing-tools-the-pros-use.html) que quase todos os pentesters usam.

O ponto mais importante de qualquer ferramenta de hacking, além de sua qualidade e adequação ao trabalho em questão, é garantir que ela não contenha [malware](https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html) ou outro código projetado para hackear. A grande maioria das ferramentas de hackers que você pode acessar na Internet, especialmente de graça, contém malware e backdoors não documentados. Geralmente, você pode confiar nas ferramentas de hacking mais comuns e populares, como o [Nmap](https://nmap.org/), mas os melhores hackers éticos escrevem e usam suas próprias ferramentas porque não confiam em nada escrito por outra pessoa.

O software de testes de invasão ou vulnerabilidade sempre fez parte do kit de ferramentas de hackers éticos. Mais do que provável, o cliente já está executando um ou ambos destes em uma base regular. Um dos desenvolvimentos mais empolgantes no pentesting são as ferramentas que essencialmente fazem todo o trabalho duro, desde a descoberta até a exploração, da mesma forma que um invasor pode fazer.

Um exemplo desse tipo de ferramenta é o código aberto [Bloodhound](https://github.com/BloodHoundAD/BloodHound). O Bloodhound permite que os invasores visualizem, graficamente, as relações entre diferentes computadores em uma rede do Active Directory. Se você inserir um objetivo de destino desejado, o Bloodhound poderá ajudar a visualizar rapidamente várias rotas hackers para seguir até chegar ao alvo, geralmente identificando as que você não sabia que existiam. Eu vi usos complexos onde os pentesters simplesmente entravam nos pontos inicial e final; o Bloodhound e alguns scripts faziam o resto, incluindo todas as etapas de hacking necessárias para ir do ponto A ao Z. É claro que o software de testes de intrusão comercial tem tido esse tipo de sofisticação por muito mais tempo.

**Uma imagem vale mais que mil palavras**

Costumava-se vender uma defesa para a gerência sênior hackeando-a ou mostrando a documentação enviada pelos pentesters. Hoje, a gerência sênior quer decks de slide, vídeos ou animações de como os hacks foram executados em seu ambiente. Eles o usam não apenas para convencer outros gerentes seniores em defesas específicas, mas também como parte da educação dos funcionários.

**Gerenciamento de riscos**

Também não é suficiente entregar uma lista de vulnerabilidades encontradas para o restante da empresa e considerar o trabalho como concluído. Não, os pentesters de hoje precisam trabalhar com o gerenciamento de TI para identificar as ameaças maiores e mais prováveis. Agora, eles fazem parte da equipe de gerenciamento de riscos, ajudando a reduzir ainda mais os riscos de maneira eficiente que apenas vulnerabilidades puras. Isso significa que hackers éticos fornecem ainda mais valor ao mostrar aos gerentes e defensores o que é mais provável que aconteça e como, e não apenas mostrar a eles um hack único, aquele improvável que ocorra de um intruso da vida real.

O teste de intrusão profissional não é para todos. É necessário tornar-se um especialista em várias tecnologias e plataformas diferentes, bem como um desejo intrínseco de ver se algo pode ser quebrado fora dos limites apresentados. Se você tem esse desejo e pode seguir algumas diretrizes legais e éticas, também pode ser um hacker profissional.

Referencias

<https://itforum.com.br/noticias/o-que-e-hacking-etico/>

<https://www.softsell.com.br/hacker-etico-tudo-o-que-voce-precisa-saber-sobre-essa-profissao/>

<https://www.udemy.com/pt/topic/ethical-hacking/>

<https://www.portalgsti.com.br/profissoes-de-ti/hacker-etico/>