

Integrantes:

Arthur Galassi | RA: 82422433

Kauê Soares | RA: 824117267

Leonardo Macedo | RA: 82422817

Luiz Washington | RA: 824148694

Lucas Felipe | RA: 824138683

George Geronimo | RA: 824148488

Certified Ethical Hacker (CEH)

Requisitos:

- Não é necessário ter um diploma, mas é recomendado ter pelo menos dois anos de experiência em segurança da informação.
- Participação em um curso oficial da EC-Council é uma alternativa para quem não possui a experiência necessária.

Indústrias e Empresas:

- Usada em setores que demandam proteção contra ataques cibernéticos, como:
- Tecnologia da informação
- Finanças
- Saúde
- Governo
- Consultorias de segurança

Benefícios:

- Reconhecimento global como especialista em hacking ético.
- Melhoria nas habilidades de detecção e prevenção de vulnerabilidades.
- Aumento de oportunidades de carreira e potencial salarial.
- Relevância em cenários de resposta a incidentes e segurança proativa.

Abordagem de Gestão de Risco:

- Foca na identificação e exploração de vulnerabilidades para entender como um atacante poderia comprometer a segurança de um sistema.
- A ênfase está na aplicação prática de técnicas de ataque para reforçar a segurança.

EC-Council Certified Security Analyst (ECSA)

Requisitos:

- Recomenda-se que os candidatos tenham a certificação CEH ou experiência equivalente.
- É aconselhável ter pelo menos dois anos de experiência em segurança da informação.

Indústrias e Empresas:

- Usada em ambientes onde a segurança da informação e auditoria de segurança são críticas, como:
- Empresas de segurança cibernética
- Consultorias de TI
- Setores financeiros e bancários
- Infraestrutura crítica

Benefícios:

- Abordagem mais analítica e estratégica em segurança, focando em avaliações de segurança detalhadas.
- Melhor entendimento de como documentar e comunicar resultados de testes de penetração.
- Aumento do valor profissional e acesso a posições de análise de segurança.

Abordagem de Gestão de Risco:

- Foca em análises e relatórios após testes de penetração, enfatizando a identificação de riscos e vulnerabilidades com base em evidências.
- Proporciona uma abordagem mais detalhada e formal para entender e mitigar riscos em sistemas e redes.

Resumo das Diferenças

A CEH tem como principal objetivo capacitar os profissionais a pensar como hackers. Ela ensina técnicas de hacking ético, permitindo que os candidatos identifiquem, explorem e relatem vulnerabilidades em sistemas e redes. A certificação é voltada para quem deseja entender a mentalidade do invasor, essencial para melhorar a defesa das organizações.

Por outro lado, a ECSA se concentra em uma abordagem analítica e estruturada da segurança da informação. O objetivo é capacitar os profissionais a conduzir testes de penetração e a documentar de maneira eficaz as descobertas. A ECSA é ideal para aqueles que buscam uma compreensão mais profunda de como avaliar e relatar riscos e vulnerabilidades em um ambiente organizacional.

INFOGRÁFICO COMPARATIVO



RELATÓRIO

Aqui estão as diferenças e similaridades entre as certificações **Certified Ethical Hacker (CEH)** e **EC-Council Certified Security Analyst (ECSA)**:

Similaridades:

- Certificação de Cibersegurança:** Ambas as certificações são voltadas para profissionais de cibersegurança e focam em habilidades e conhecimentos para proteger redes e sistemas contra ataques.
- Emitidas pelo EC-Council:** Ambas as certificações são oferecidas pela mesma organização, o **EC-Council**, que é reconhecido internacionalmente por suas credenciais em cibersegurança.
- Foco em Hacking Ético:** Tanto o CEH quanto o ECSA têm um enfoque importante em técnicas de hacking ético (pentesting), embora com abordagens diferentes.
- Atenção a Ferramentas e Técnicas de Segurança:** Ambas as certificações envolvem o aprendizado de ferramentas e métodos para identificar vulnerabilidades e fortalecer a segurança.

5. **Pré-requisitos:** Para obter ambas as certificações, é necessário ter experiência ou treinamento prévio na área de cibersegurança (embora o ECSA seja mais avançado, portanto exige mais experiência).
-

Diferenças:

1. **Objetivo da Certificação:**
 - **CEH:** Foca em habilidades práticas de **hacking ético**, especificamente em técnicas para identificar e corrigir vulnerabilidades. É mais voltado para o processo de **penetração (pentesting)** e **avaliar segurança de sistemas**.
 - **ECSA:** A certificação é mais voltada para **análise de segurança e avaliação mais profunda de redes e sistemas**, com uma abordagem mais estratégica e detalhada, incluindo a análise de riscos e a realização de testes de penetração avançados.
2. **Nível de Profundidade:**
 - **CEH:** É uma certificação de **nível iniciante a intermediário**. Foca em fornecer uma visão ampla das ferramentas e técnicas usadas por hackers éticos.
 - **ECSA:** Considerado um **nível mais avançado**. Ele assume que o candidato já tem uma base sólida e busca desenvolver habilidades mais técnicas e analíticas.
3. **Conteúdo do Currículo:**
 - **CEH:** Inclui tópicos como **exploração de vulnerabilidades, malware, segurança em redes, exploits, phishing, engenharia social e testes de penetração**. Também foca em abordagens mais práticas e hands-on.
 - **ECSA:** Possui um conteúdo mais **detalhado sobre análise e avaliação de segurança**, com tópicos como **relatórios de segurança, métodos avançados de penetração, análise de risco e redes e sistemas** em uma perspectiva mais holística.
4. **Exame e Avaliação:**
 - **CEH:** O exame é mais focado em uma **avaliação prática e técnica** sobre ataques, exploits e segurança em sistemas. É um teste de múltiplas escolhas.
 - **ECSA:** O exame é mais focado em **relatórios de avaliação de segurança**, com um foco mais intenso em técnicas e análise profunda de riscos e falhas. Envolve testes práticos e um projeto final (que pode ser um relatório de pentesting detalhado).
5. **Público-alvo:**
 - **CEH:** Ideal para **novos profissionais de cibersegurança** ou aqueles que querem uma visão geral das técnicas de hacking ético. Focado em quem deseja se tornar um **pentester**.
 - **ECSA:** Focado para **profissionais de cibersegurança mais experientes**, como analistas de segurança ou gerentes de risco, que buscam uma compreensão mais profunda da segurança e das melhores práticas para análise e mitigação de riscos.
6. **Enfoque em Testes de Penetração:**

- **CEH:** Embora também cubra penetração, o foco principal é **exploração de vulnerabilidades e formas de invadir sistemas**.
- **ECSA:** Aborda penetração de forma mais **estratégica e avançada**, com ênfase em **testes de penetração completos** e análise após a exploração.