



Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER -
SECURITY IMPLEMENTATION



C|EH[®]v12
Certified Ethical Hacker

Não ensinamos apenas Hacking Ético
WE DON'T JUST TEACH

**ETHICAL
HACKING**

WE BUILD CYBER CAREERS
Construímos carreiras cibernéticas

Attain the World's No.1 Credential in Ethical Hacking
Obtenha a credencial número 1 do mundo em Hacking Ético

Sobre o Certified Ethical Hacker

O certificado “Certified Ethical Hacker” (CEH) da EC-Council é uma das certificações de segurança ofensiva mais bem estabelecidas e amplamente reconhecidas. É credenciado pela ANSI e aprovado pelo DoDD 8140, o que a torna excepcionalmente valiosa para profissionais de segurança que trabalham nos setores público e privado.

No entanto, a certificação CEH não é barata. O exame CEH custa US\$ 1.199 e o retake custa US\$ 450. A inscrição para fazer o exame custa US\$ 100 (sem treinamento oficial). Não é barato para começar e isso antes mesmo de estar apto.

No entanto, o CEH é o padrão de ouro para validar as habilidades de segurança ofensivas, em parte devido a esses rigorosos padrões de aplicação. Abordaremos as várias etapas necessárias para obter uma certificação CEH.

Certificação Certified Ethical Hacker

O exame C|EH é um exame de 4 horas com 125 questões de múltipla escolha. Este exame baseado em conhecimento testará suas habilidades em ameaças de segurança da informação e vetores de ataque, detecção de ataques, prevenção de ataques, procedimentos, metodologias e muito mais!

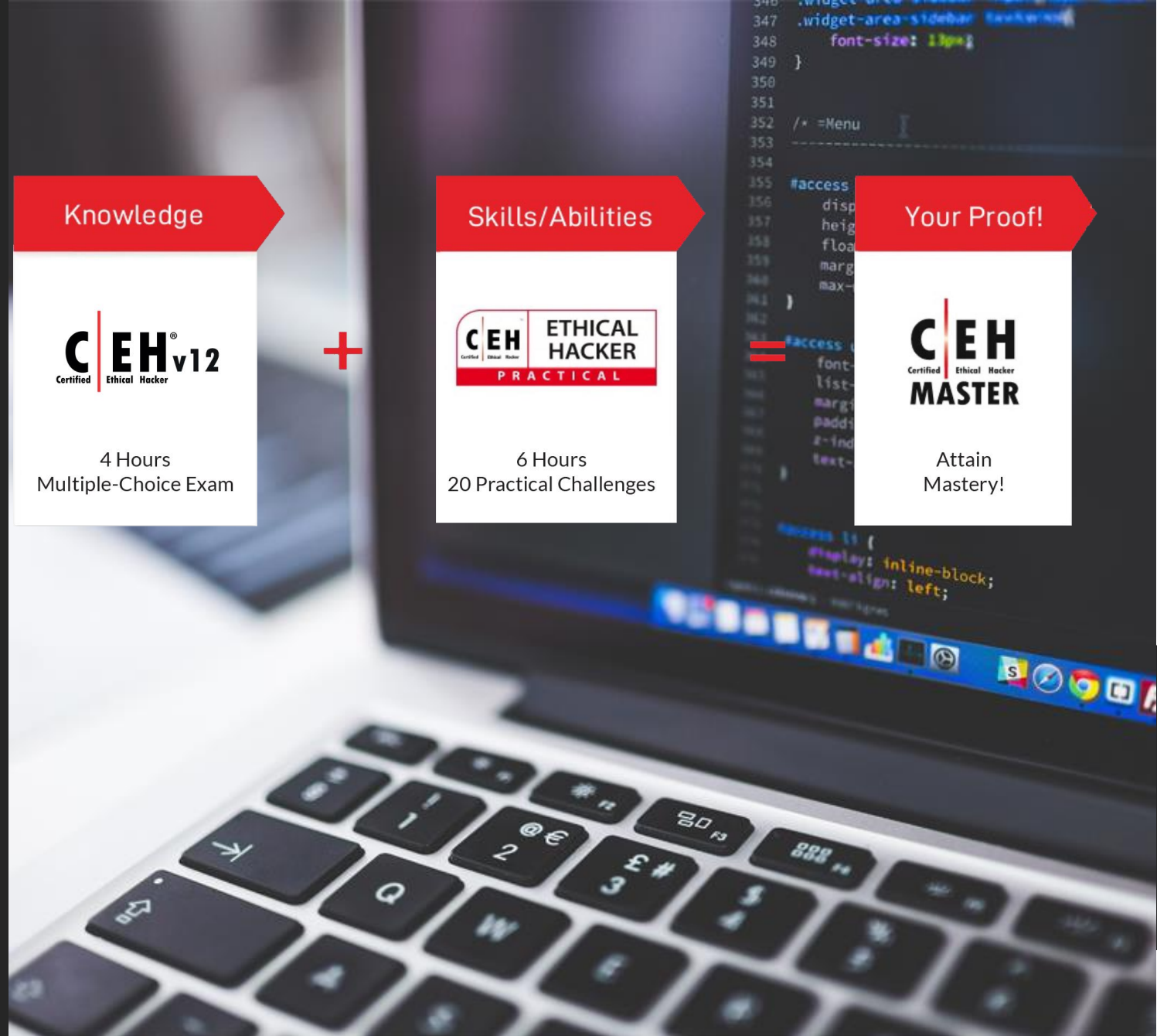
Certificação Prática C|EH

Este é o próximo passo para se tornar um C|EH Master depois de obter sua certificação C|EH. No C|EH Practical, você tem um tempo limitado para concluir 20 desafios que testam suas habilidades e proficiência em uma faixa cibernética baseada em desempenho.

Certificação C|EH Master

Após a conclusão do programa C|EH (Master), que consiste em C|EH e C|EH (Prático), a designação C|EH (Master) é concedida.

C|EH Masters demonstram proficiência em nível teórico e prático.



Tópicos da Prova



Módulo 1. Introdução ao Hacking Ético



Módulo 2. Foot Printing e Reconhecimento



Módulo 3. Scanning de Redes



Módulo 4. Enumeração



Tópicos da Prova



Módulo 5. Análise de Vulnerabilidade



Módulo 6. Hacking de Sistemas



Módulo 7. Ameaças de Malware



Módulo 8. Sniffing



Tópicos da Prova



Módulo 9. Engenharia Social



Módulo 10. Negação de serviço



Módulo 11. Sequestro de Sessão



Módulo 12. Fugindo de IDS, Firewalls
e Honeypots



Tópicos da Prova



Módulo 13. Hackeando Servidores da Web



Módulo 14. Hackeando aplicativos da Web



Módulo 15. Injeção de SQL



Módulo 16. Hackeando redes sem fio



Tópicos da Prova



Módulo 17. Hackeando plataformas móveis



Módulo 18. IoT e OT Hacking



Módulo 19. Computação em Nuvem

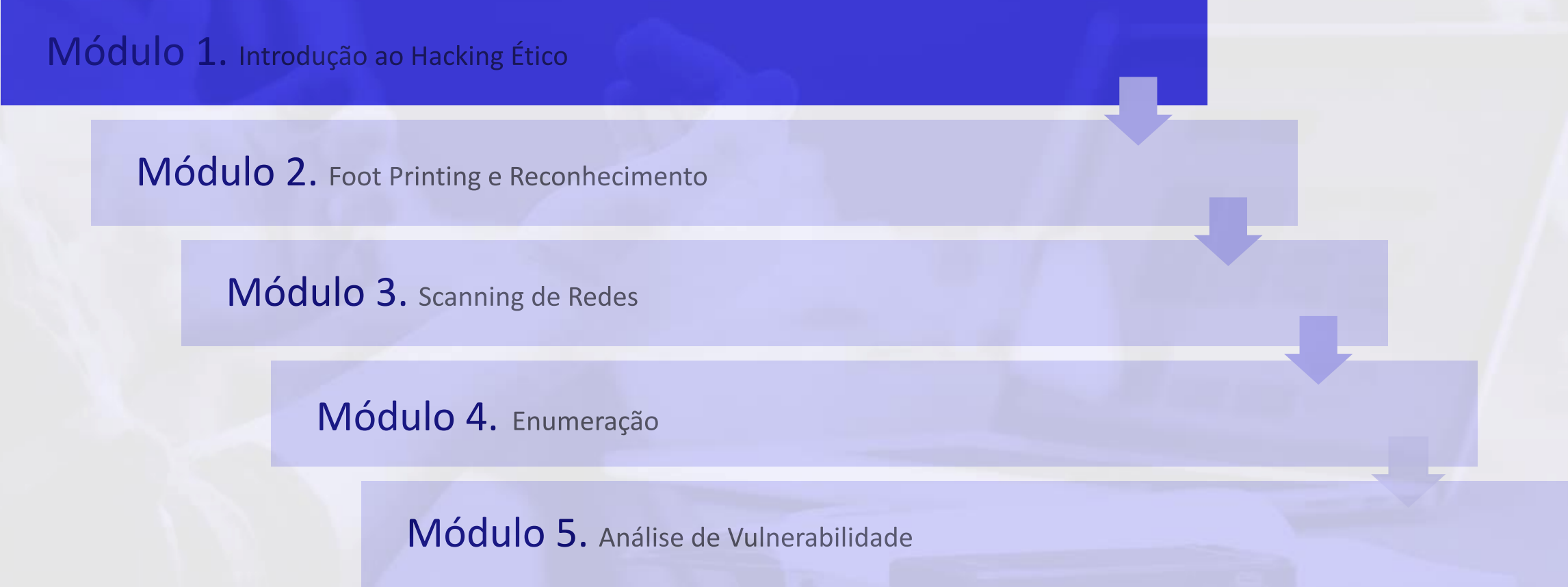


Módulo 20. Criptografia



Progresso do curso

Módulo 1. Introdução ao Hacking Ético



```
graph TD; M1[Módulo 1. Introdução ao Hacking Ético] --> M2[Módulo 2. Foot Printing e Reconhecimento]; M2 --> M3[Módulo 3. Scanning de Redes]; M3 --> M4[Módulo 4. Enumeração]; M4 --> M5[Módulo 5. Análise de Vulnerabilidade];
```

Módulo 2. Foot Printing e Reconhecimento

Módulo 3. Scanning de Redes

Módulo 4. Enumeração

Módulo 5. Análise de Vulnerabilidade

Descrição:

O programa CEH (ANSI) exige que o candidato tenha dois anos de experiência profissional no domínio da Segurança da Informação e deve ser capaz de fornecer uma prova do mesmo conforme validado através do processo de candidatura, a menos que o candidato frequente um treinamento oficial.

<https://cert.eccouncil.org/application-process-eligibility.html>

Exame sem treinamento:

Para serem considerados para o exame EC-Council sem participar de treinamento oficial, os candidatos devem primeiro ser aprovados por meio do processo de inscrição de elegibilidade.

Certification Title	CEH
Experience Required in Information Security	2 years
Experience Required in Domains	<ol style="list-style-type: none">1. Information Security and Ethical Hacking Overview2. Reconnaissance Techniques3. System Hacking Phases and Attack Techniques4. Network and Perimeter Hacking5. Web Application Hacking6. Wireless Network Hacking7. Mobile Platform, IoT, and OT Hacking8. Cloud Computing9. Cryptography <p>Please refer to the exam blueprint here</p>
Remit a Non-Refundable Eligibility Application Fee	\$100
Submit an Eligibility Application Form	Yes
Approval Required from EC-Council's Cert. Dept.	Yes
Exam Voucher Price	<ol style="list-style-type: none">1. Pearson Vue voucher (\$1199)2. ECC exam voucher (\$950)3. The voucher purchase link will be sent upon application approval
More Information is Available at:	https://www.eccouncil.org/Certification/certified-ethical-hacker

CEHv12 (ANSI)

Exame sem treinamento oficial

Descrição:

O programa CEH (ANSI) exige que o candidato tenha dois anos de experiência profissional no domínio da Segurança da Informação e deve ser capaz de fornecer uma prova do mesmo conforme validado através do processo de candidatura, a menos que o candidato frequente um treinamento oficial.

<https://cert.eccouncil.org/application-process-eligibility.html>

Exame com treinamento oficial:

Se um candidato concluiu um treinamento oficial da EC-Council em um Centro de Treinamento Credenciado, por meio da plataforma iClass ou em uma instituição acadêmica aprovada, o candidato é elegível para tentar o exame EC-Council.

O curso eletrônico oficial consiste apenas em material de estudo. Os alunos devem se inscrever para elegibilidade antes de comprar um comprovante de exame.

A compra de um e-courseware oficial não garante que o aluno possa passar no exame. Um aluno pode consultar qualquer outro material de estudo para se preparar para o exame. Os candidatos são incentivados a consultar o plano de exame antes de se inscrever para um exame.

Como várias leis do consumidor em todo o mundo proíbem qualquer tipo de "fixação de preços", o departamento de Certificação do EC-Council não pode prescrever preços mínimos para seus exames. Isso permite uma abordagem de mercado livre que beneficia nossa comunidade de certificação.

Como o preço de um voucher de exame é muitas vezes associado ao treinamento oficial de nossos parceiros credenciados, o preço pode variar dependendo da região, instalações de treinamento, parceiro de treinamento, experiência do instrutor, custo de supervisão do exame e até mesmo o modo de treinamento do o parceiro.

É imperativo que deixemos claro que nenhum aluno deve ser considerado como tendo qualquer vantagem adicional de um modo de treinamento para outro, a fim de contestar o exame CEH ANSI, pois o exame é um exame padrão para todos, independentemente do método de Treinamento.

CEHv12 (ANSI)

Exame com treinamento oficial

Descrição:

O programa Certified Ethical Hacker é o auge do programa de treinamento em segurança da informação mais desejado em que qualquer profissional de segurança da informação jamais desejará estar. Para dominar as tecnologias de hacking, você precisará se tornar um, mas ético! O curso credenciado fornece as ferramentas e técnicas avançadas de hacking usadas por hackers e profissionais de segurança da informação para invadir uma organização. Como dizemos, “para derrotar um hacker, você precisa pensar como um hacker”. Para mais detalhes, visite <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

Este produto é composto por:

- Curso CEHv12 (Curso Digital e Manual de Laboratório digital) com validade de 2 anos.
- Ferramentas (para download on-line e instruções fornecidas no e-Courseware)

Observação:

- O voucher do exame não está incluído.



CEHv12 e-Courseware

\$850.00

1

 Pay

— OR —

Add to cart

CEHv12 e-Courseware

Curso Oficial

Descrição:

Taxa de comprovante de exame de retomada de RPS para CEH.

Modo de entrega do exame:

Online, o exame é supervisionado remotamente pela equipe RPS.

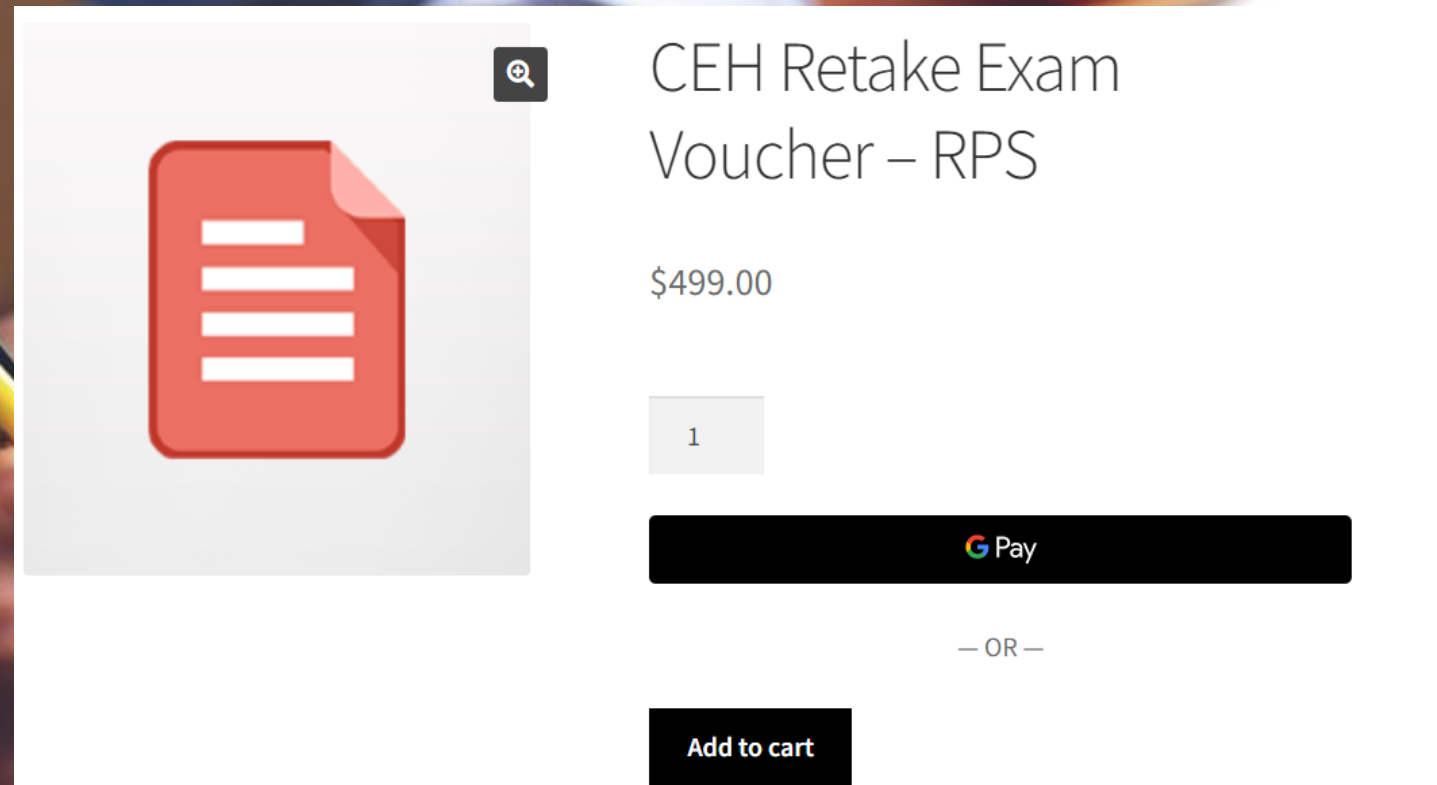
Observação:

Este produto é limitado para candidatos que desejam refazer o exame e foram aprovados pelo EC-Council por meio do formulário de inscrição listado em

<https://cert.eccouncil.org/retake-exam-promo.html>

O voucher do exame é intransferível e válido por um ano a partir da data de liberação.

Sujeito à política de retomada do exame (<https://cert.eccouncil.org/ec-council-exam-retake-policy.html>)



The screenshot shows a product listing for a 'CEH Retake Exam Voucher – RPS'. On the left is a red document icon with white horizontal lines. To the right of the icon, the product name 'CEH Retake Exam Voucher – RPS' is displayed in a large, dark font. Below the name, the price '\$499.00' is shown. A small grey box with the number '1' indicates the quantity. Below the quantity is a black button with the Google Pay logo and the text 'Pay'. Below this button is the text '— OR —'. At the bottom right is a black button with the text 'Add to cart'.



RPS Retake Exam Voucher

Candidatos que desejam refazer o exame

Descrição:

Este produto inclui um único voucher CEH (Practical) Aspen Dashboard que lhe dará acesso a:

- Após a ativação, o acesso ao painel da Aspen dura 365 dias, o que significa que você pode agendar seu exame a qualquer momento dentro deste período.
- O código do painel é válido por 1 ano a partir da data de recebimento, o que significa que você deve ativar o código dentro de 1 ano ou ele expira.
- Acomodação de serviços de supervisão remota (reserva de vagas precisa ser feita 3 dias antes da data do exame).
- CEH cyber range challenge exam (6 hours)



CEH (Practical) Exam

\$550.00

1

— OR —

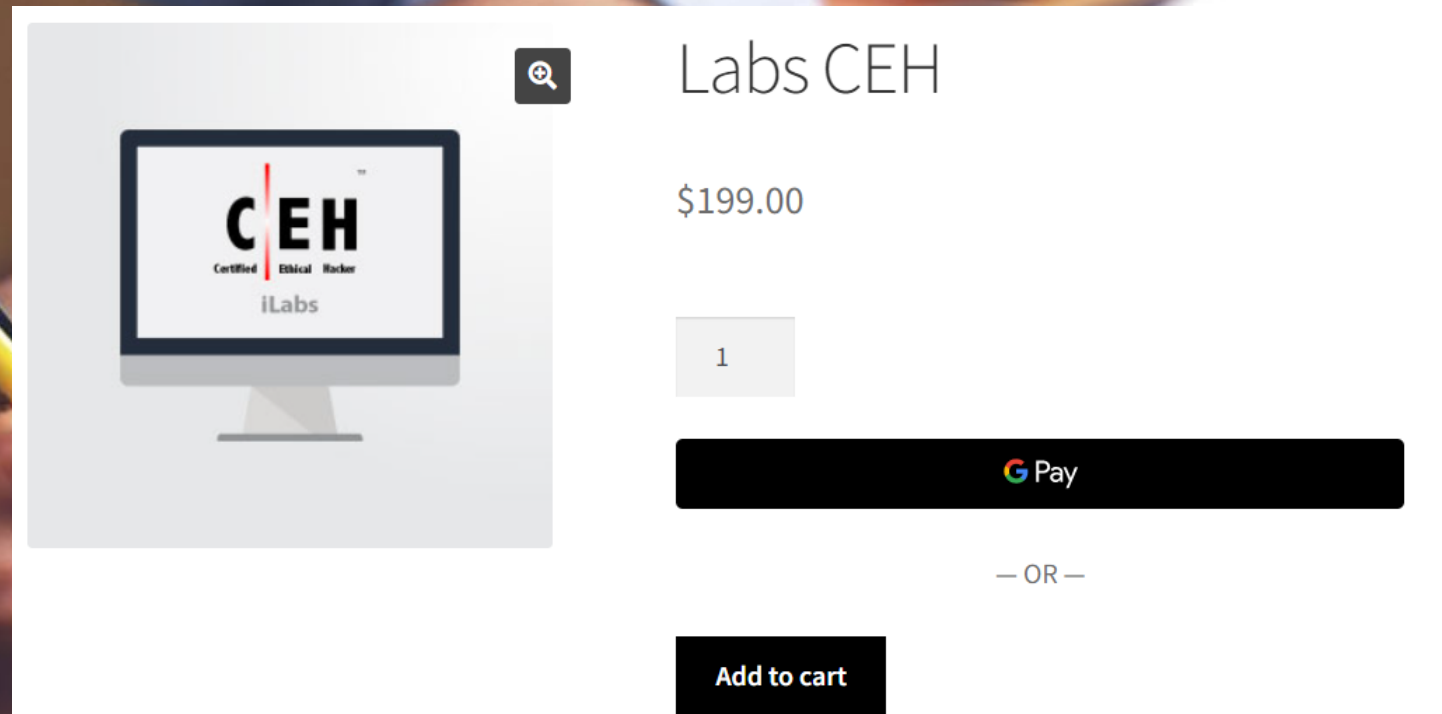
Add to cart

CEH (Practical) Exam

CEH (Practical) Aspen Dashboard

Descrição:

Os alunos agora podem acessar dinamicamente uma série de máquinas virtuais pré-configuradas com vulnerabilidades, exploits, ferramentas e scripts de qualquer lugar com conexão à Internet. Este é um serviço de assinatura baseado em nuvem do EC-Council, projetado para oferecer práticas práticas sérias para o profissional de segurança da informação. O portal na nuvem permite que um participante do curso inicie uma ampla gama de máquinas-alvo e acesse-as remotamente com apenas alguns cliques. É a solução de laboratório ao vivo mais econômica e fácil de usar disponível globalmente hoje. Este produto consiste em 6 meses de acesso ao ambiente de laboratório virtual EC-Council para CEH.



The screenshot shows a product listing for 'Labs CEH'. On the left is an image of a computer monitor displaying the 'CEH iLabs' logo. To the right of the image is a magnifying glass icon. The product name 'Labs CEH' is displayed in a large font. Below it, the price '\$199.00' is shown. A quantity selector shows the number '1'. Below the quantity is a black button with the 'G Pay' logo. Underneath this is the text '— OR —'. At the bottom right is a black button labeled 'Add to cart'.

Labs CEH

Acesso por 6 meses em laboratório da EC-Council

Como obter a credencial C|EH (Master)?

- C|EH Master, é a próxima evolução para a credencial Certified Ethical Hacker de renome mundial e um 'próximo passo' lógico para aqueles que possuem a prestigiosa certificação. Ganhar a designação C|EH Master é a sua maneira de dizer: “Aprendi, entendi e provei”.



- Para provar que você é proficiente em Ethical Hacking , não oferecemos simulações de exames. Muitos outros provedores de certificação falam sobre avaliações baseadas em desempenho, mas a realidade está longe de testar suas habilidades em um ambiente da vida real. A maioria desses 'testes baseados em desempenho' é limitada a simulações ou formas interativas de testar teoricamente seu conhecimento.

Sobre o Exame

Exame #1

Exame C|EH

- ✔ Número de perguntas: 125
- ✔ Duração do teste: 4 horas
- ✔ Formato do teste: Múltipla Escolha
- ✔ Entrega de teste: EXAME ECC, VUE
- ✔ Prefixo do exame: 312-50 (ECC EXAM), 312-50 (VUE)

Exame #2

C|EH (Prático)

- ✔ Título do exame: Certified Ethical Hacker (Prático)
- ✔ Quantidade de Desafios Práticos: 20
- ✔ Duração: 6 horas
- ✔ Disponibilidade: Aspen – iLabs
- ✔ Formato de teste: iLabs Cyber Range
- ✔ Pontuação de aprovação: 70%
- ✔ Livro aberto: como no mundo real!

- Testamos suas habilidades com desafios do mundo real em um ambiente do mundo real, usando laboratórios e ferramentas que exigem que você conclua desafios específicos de hacking ético dentro de um limite de tempo, assim como você enfrentaria no mundo real! No exame EC-Council C|EH (Prático), uma rede complexa de uma grande organização, composta por vários sistemas de rede (incluindo DMZ, Firewalls etc.) vulnerabilidades de tempo enquanto também audita os sistemas.

Visão geral do exame C|EH

Validade da Certificação e renovação:

- A partir de 1º de janeiro de 2009, todas as certificações do EC-Council são válidas por três anos a partir da data da certificação.
- Durante o período de três anos, a certificação deve ser renovada participando do Programa de Educação Continuada (ECE) do EC-Council.
- Após a conclusão do programa ECE de 3 anos e o cumprimento dos requisitos, a validade da certificação do membro será estendida por mais três anos a partir do mês de vencimento.

The C|EH Exam at a Glance

Exam Details	CEH (MCQ Exam)	CEH (Practical)
Number of Questions / Practical Challenges	125	20
Test Duration	4 Hours	6 Hours
Test Format	Multiple Choice Questions	iLabs Cyber Range
Test Delivery	ECC EXAM, VUE	-
Availability	-	Aspen - iLabs
Exam Prefix	312-50 (ECC EXAM), 312-50 (VUE)	-
Passing Score	Please refer to https://cert.eccouncil.org/faq.html	70%

C|EH e o mercado de Trabalho

- A C|EH foi classificada entre as 5 certificações de segurança cibernética mais bem pagas nos últimos 10 anos e continua a crescer em todo o mundo.
- Não confie apenas em nós - aqui estão alguns exemplos para que você possa ver o que outras pesquisas concluíram.

<https://www.zdnet.com/education/computers-tech/best-ethical-hacking-certification>

<https://www.roberthalf.com/blog/salaries-and-skills/which-it-certifications-are-most-valuable>

<https://www.enterprisestorageforum.com/management/cybersecurity-certifications/>

<https://www.infosec-careers.com/the-best-cyber-security-certifications-in-2022/>

<https://www.cio.com/article/193586/top-15-it-certifications-in-demand-for-2021.html>

Atualmente em sua 12ª versão, o C|EH é uma certificação muito conhecida no espaço de segurança cibernética. Uma simples pesquisa por anúncios de emprego globais no LinkedIn (a partir de agosto de 2022) mostra mais de 32.000 empregos disponíveis solicitando candidatos com certificação C|EH, representando mais de 72% do mercado em anúncios de emprego colocados por empregadores combinados em Career Builder, LinkedIn, Dice, Indeed, Monster e Naukri, enquanto são comparados a outras certificações como SANS GPEN, OSCP e Pentest+.

Objetivos do Curso

- Ambientar o aluno ao mundo da segurança da informação.
- Preparar o aluno para a certificação CEHv12.
- Fazer com que ele seja capaz de entender o que acontece no mundo hacking.
- Fazer com que o aluno seja autossuficiente para adquirir novos conhecimentos e buscar a informação sozinho.
- Incentivar o aluno a praticar constantemente.
- Trazer um ambiente prático, mas não se esquecendo dos fundamentos e conceitos necessários.

Sobre mim!

José Leandro Sant'Anna

- Consultor de segurança da Informação na Petrobras (Techbiz Forense Digital);
- Mais de 18 anos de experiência no mercado de TIC/SI;
- Pós Graduação - MIT em Engenharia de Redes (INFNET);
- Pós Graduação - MBA em Gestão de Segurança da Informação (INFNET);
- Pós Graduação - Computação Forense e Segurança Da Informação (IPOG)
- Certificações: MCSA, LPIC-3-303 Security, ISO 27002, Security+, CEH ANSI, CEH Practical, CEH Master, L260 LogRhythm Network Monitor Certified Professional, dentre outras...
- Ex trompetista, agora metido a guitarrista roqueiro 😊. 🎸

O que é o Certified Ethical Hacker (CEH)

Oferecido por meio do EC-Council, o profissional Certified Ethical Hacker (CEH) demonstra a capacidade de encontrar vulnerabilidades em sistemas de computador. Como um hacker ético, é alguém que usa as mesmas habilidades, técnicas e conhecimentos de um hacker mal-intencionado para ajudar a estabelecer melhores medidas de segurança para evitar ataques futuros. Os hackers éticos são responsáveis por encontrar pontos fracos nas redes e sistemas da organização e, em seguida, usar esse conhecimento para proteger a empresa contra possíveis ameaças.

A certificação CEHv12 é um programa de treinamento 100% ofensivo. Ela não é um programa de treinamento de segurança de redes, não é um programa de treinamento de análise de segurança ou testes de segurança de redes.

Para essas áreas a EC-council oferece outros programas de treinamentos como o ENSA, ECSA e LPT. Lembre-se que o programa de treinamento da CEH é focado 100% em rede ofensiva e NÃO defensiva.

Sobre o Treinamento

O treinamento para a prova de CEH é extremamente intensivo, e deve ser encarado como um desafio à parte da prova.

É necessário muita dedicação e esforço para completar o treinamento. A quantidade de ferramentas abordadas durante o curso é bastante extensa e por isso **o instrutor NÃO será capaz de demonstrar todas as ferramentas durante as aulas**. Ele irá selecionar as ferramentas mais apropriadas e utilizadas no mercado atualmente.

É extremamente importante que o aluno pratique as ferramentas citadas durante o treinamento fora da escola. Essa prática irá reforçar o conteúdo visto em aula e gerar dúvidas para serem discutidas junto ao instrutor.

Elementos da SI

- **CONFIDENCIALIDADE** - É a garantia de que uma informação é acessível apenas para pessoas autorizadas.
- **INTEGRIDADE** - É a confiabilidade dos dados no sentido de prevenir mudanças não autorizadas.
- **DISPONIBILIDADE** - É a garantia de que o sistema responsável por entregar, armazenar e processar informação está acessível quando solicitado.
- **AUTENTICIDADE** - Se refere a características de uma comunicação, documento ou qualquer dado que garanta a qualidade de ser genuíno ou não corrompido do original. Ex. Checksum, certificados digitais, smart cards, etc.
- **NÃO REPÚDIO** - É a garantia de que alguém não pode negar alguma coisa. Normalmente, não-repúdio refere-se à capacidade de garantir que uma parte de uma comunicação não pode negar a autenticidade da sua assinatura em um documento ou o envio de uma mensagem de que eles se originaram.

Segurança da informação

Segurança da informação significa proteger e defender qualquer tipo de informação sensível e sistema de informação de acessos não autorizados, divulgação não autorizada, alteração ou manipulação indevida, rompimento ou corrupção e perda de dados.

A segurança da informação não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma.

O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a segurança da informação também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

.

Mecanismos de segurança

CONTROLES FÍSICOS:

São barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controles físicos:

- Portas
- Trancas
- Paredes
- Blindagem
- Guardas
- Etc ...

Mecanismos de segurança

CONTROLES LÓGICOS:

São barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apoiam os controles lógicos:

- Mecanismos de cifração ou encriptação
- Assinatura digital
- Mecanismos de garantia da integridade da informação
- Mecanismos de controle de acesso
- Mecanismos de certificação
- Integridade
- Honeypot
- Protocolos seguros

Ameaças da segurança da informação

As ameaças aproveitam das falhas de segurança da organização, que é considerado como ponto fraco, provocando possíveis danos, perdas e prejuízos aos negócios da empresa. Elas são constantes podendo acontecer a qualquer momento.

1. **Ameaças Naturais** – Desastres naturais, enchentes, terremotos, tsunamis e vulcões.
2. **Ameaças Físicas** – Perda ou dano de recursos computacionais, invasão física, sabotagem, espionagem e erros em geral.
3. **Ameaças Humanas** - Hackers, intrusos, engenharia social e falta de conhecimento.

Ameaças humanas

1. **Ameaças de Rede** – Coleta de informação, sniffing, spoofing, session hijacking, man-in-the-middle, sql injection, arp poisoning, negação de serviço.
2. **Ameaças de Host** – Ataques de malware, Footprinting do alvo, ataques de senhas, DoS, execução de código arbitrário, acesso não autorizado, escalção de privilégio, back door.
3. **Ameaças de aplicação** – Validação de data/input, autenticação e autorização, gerenciamento de configuração, divulgação de informação, gerenciamento de questões de sessão, buffer over flow, criptografia, manipulação de parâmetro, manipulação de erros.

Tipos de Ataques

- **OPERATING SYSTEM ATTACKS** - Os atacantes procuram por vulnerabilidades no sistema operacional.
- **APPLICATIONS-LEVEL ATTACKS** - Softwares de aplicação vêm com milhares de funcionalidades e essas funcionalidades podem conter vulnerabilidades que podem se tornar a origem de um ataque.
- **MISCONFIGURATIONS ATTACKS** - Muitos administradores não tem o conhecimento necessário para controlar ou resolver os problemas de uma rede, o que pode levar a erros de configuração. Tais erros podem gerar vulnerabilidades que podem comprometer o sistema.
- **SHRINK WRAP CODE ATTACKS** - Aplicações de sistemas operacionais vêm com vários exemplos de configurações, mas esses mesmos exemplos podem conter vulnerabilidades que podem levar a ataques shrink wrap code.
- Veja: <http://cktech.blogspot.com.br/2010/05/shrink-wrap-code-attack.html>

Fases de um ataque

- **Reconnaissance** - Essa é fase preparatória onde um atacante ganha o máximo de informações que puder obter antes de iniciar o ataque. Essa fase envolve a busca de informações públicas mas também pode envolver escâneres de rede (passive and active reconnaissance), engenharia social e dumpster diving (vasculhar o lixo).
- **Scanning** - Essa é a fase de pré-ataque, nessa fase o atacante utiliza os dados obtidos na fase de reconhecimento para identificar vulnerabilidades específicas. O escâner pode ser considerado uma extensão da fase de reconhecimento.
- **Gaining Access** - Essa é a fase mais importante de um ataque. O atacante pode ganhar acesso no nível do sistema operacional, nível de aplicação, ou nível de rede. Uma vez que o atacante ganha o acesso ele pode tentar escalar o privilégio para ter controle total do sistema alvo.
- **Maintaining Access** - Uma vez que o atacante ganha acesso ao sistema alvo, ele deve manter o acesso para ações futuras, para isso ele pode utilizar backdoors, rootkities e trojans.
- **Clearing Tracks** - Nessa fase o atacante apaga todos os rastros de suas ações dentro do sistema.

Terminologia

- **Hack Value** - É a noção entre hackers que alguma coisa é interessante ou vale a pena ser feita.
- **Exploit** - Um exploit é uma definição para violar a segurança de um sistema através de uma vulnerabilidade. O termo exploit é utilizado quando qualquer tipo de ataque foi feito em um sistema ou rede. Um exploit pode também ser definido como código malicioso ou comando malicioso.
- **Vulnerabilidade** - Uma vulnerabilidade é uma fraqueza no design de um sistema ou um erro de implementação que pode levar a um evento inesperado e indesejável dentro do sistema, o que pode comprometer a segurança do sistema.
- **Target of Evaluation** - Um alvo de avaliação é um sistema de TI, produto ou componente que é submetido para uma avaliação de segurança.
- **Zero-day Attack** - No ataque 0day o atacante explora as vulnerabilidades dentro de um sistema antes que o fornecedor lance uma correção.
- **Daisy Chaining** - Ganhar acesso privilegiado a base de dados SQL e depois apagar os rastros do ataque.

Conceitos sobre Hacking

Hacking significa explorar vulnerabilidades de sistemas e comprometer controles de segurança para ganhar acesso não autorizado ou acesso inapropriado aos recursos computacionais do sistema.

Isso envolve modificar sistemas ou funcionalidades da aplicação para alcançar um objetivo fora do propósito original do criador ou arquiteto responsável pelo sistema.

Ethical Hacking envolve o uso de ferramentas Hacking, truques e técnicas para identificar vulnerabilidades, assim como garantir a segurança do sistema. O foco dessa atividade é simular técnicas utilizadas por atacantes reais para identificar a existência de vulnerabilidades exploráveis nos sistemas.

Quem é um Hacker?

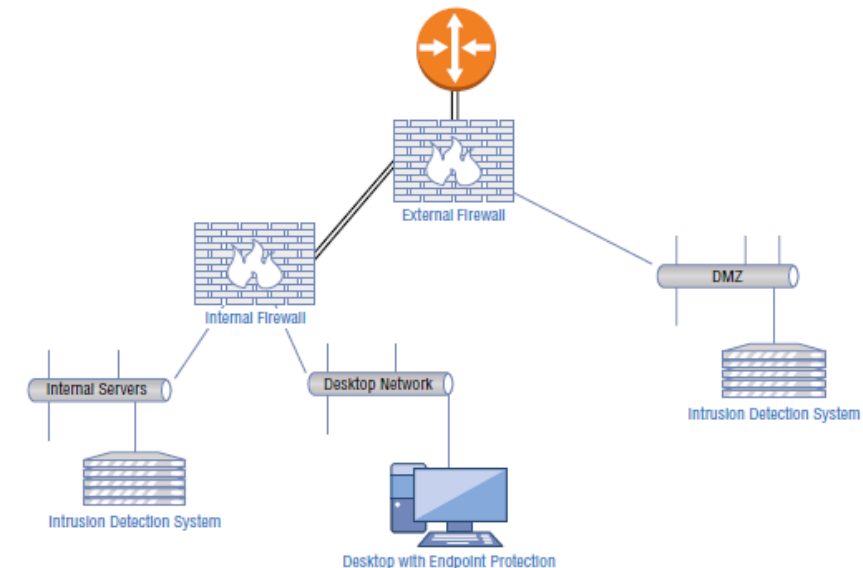
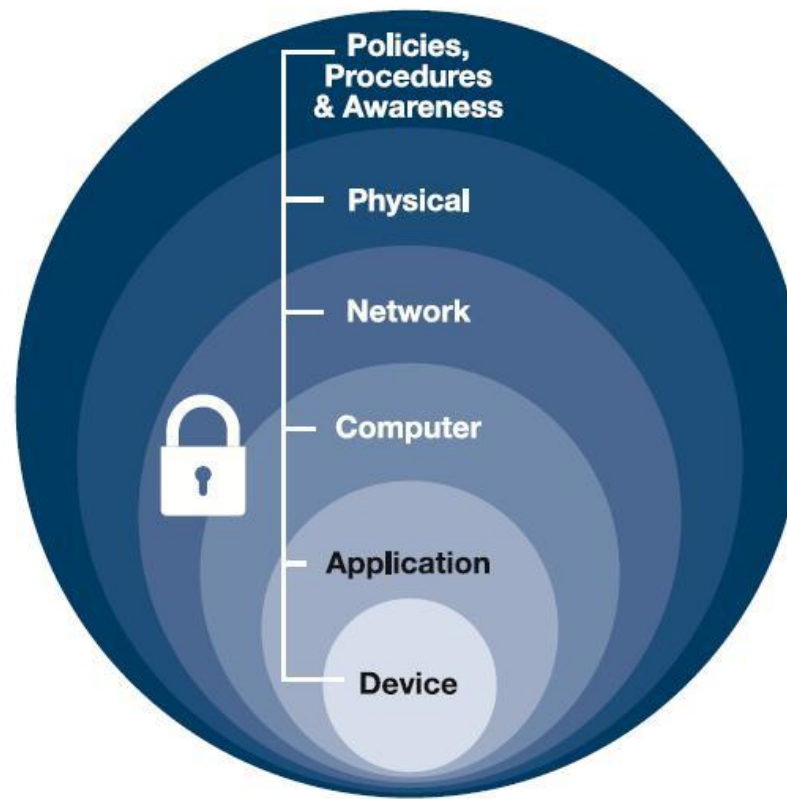
- Indivíduos inteligentes com excelentes conhecimentos computacionais, com a habilidade de criar e explorar o software e hardware do computador.
- Para alguns hackers, Hacking é um hobby, uma forma de ver quantos computadores ou redes eles podem comprometer.
- As intenções deles podem ser simplesmente ganhar conhecimento ou fazer coisas ilegais.
- Alguns hackers tem intenções maliciosas, tais como roubar dados de negócio, informações de cartões de crédito, senhas de e-mails e etc.

Conhecimentos de um Ethical Hacker

- **PLATAFORMA** – Ter conhecimento profundo dos principais sistemas operacionais de mercado, tais como Linux, Unix, Mac OS e Windows.
- **REDES** – Ter conhecimento profundo sobre redes de computadores (protocolos, topologias, modelo OSI, switch TCP/IP, fluxo de dados, etc..), tecnologias e hardware/software relacionados.
- **COMPUTER EXPERT** – Deve ser um usuário de computador extremamente avançado em domínios técnicos
- **SEGURANÇA** – Ter profundo conhecimento na área de segurança e problemas relacionados.
- **CONHECIMENTO TÉCNICO** – Ter um alto conhecimento técnico para realizar um ataque sofisticado.

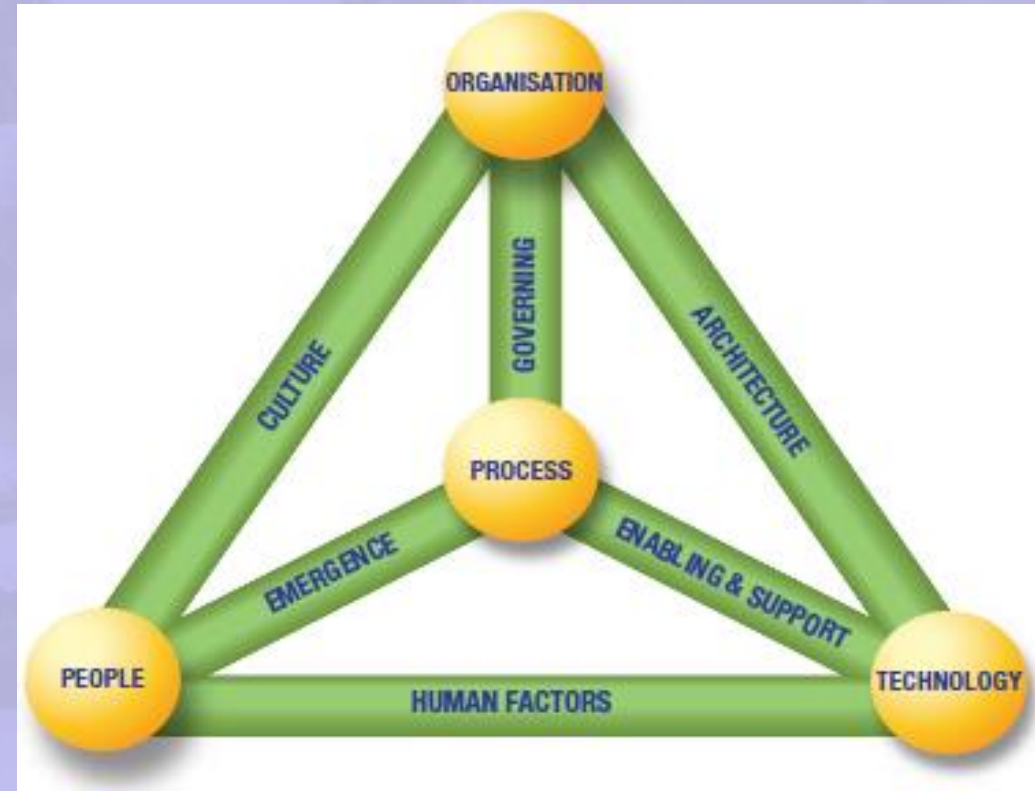
Defense-in-Depth/Defesa em profundidade

- Defense in depth é um conceito de segurança da informação em que várias camadas de controles de segurança são colocadas ao longo de um sistema de tecnologia da informação.
- Sua intenção é fornecer redundância no caso de um controle de segurança falhar ou uma vulnerabilidade explorada. Pode cobrir aspectos de pessoal, procedimentos, técnicas e físicas para a duração do ciclo de vida do sistema.



Políticas de Segurança da Informação

- Uma política de segurança é um documento ou conjunto de documentos que descrevem os controles de segurança que devem ser implementados na empresa em alto nível para proteger a rede organizacional de ataques de dentro e de fora.
- Este documento define a arquitetura completa de segurança de uma organização e o documento inclui objetivos claros, metas, regras e regulamentos, procedimentos formais, e assim por diante.



Tipos de políticas de segurança

- **Promíscua** - Com uma política promíscua, não há nenhuma restrição no acesso à Internet. Um usuário pode acessar qualquer site, fazer download de qualquer aplicativo e acessar um computador ou uma rede de um local remoto.
- **Permissiva** - Em uma política permissiva, a maioria do tráfego da Internet é aceito, mas vários serviços e ataques perigosos conhecidos são bloqueados.
- **Prudente** - A política prudente começa com todos os serviços bloqueados. O administrador permite os serviços seguros e necessários individualmente.
- **Paranoica** - Em uma política paranoica, tudo é proibido. Não há conexão com a Internet ou uso severamente limitada a Internet.

Avaliações de segurança

As avaliações de segurança envolvem o processo de validação do nível de segurança dos recursos de rede utilizando auditorias de segurança, avaliações de vulnerabilidades e testes de invasão.

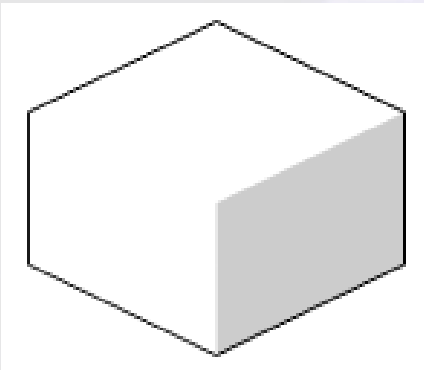
- **Auditorias de Segurança:** as auditorias de segurança concentram-se nas pessoas e nos processos utilizados para projetar, implementar e gerenciar a segurança em uma rede. O National Institute of Standards and Technology (NIST) tem várias publicações especiais que podem ser utilizadas como guias—SP 800-53 para a especificação de controles de segurança e SP 800-53A para a avaliação da eficácia do controle de segurança. Para obter mais informações, visite o Instituto Nacional de Padrões e Tecnologia (www.nist.gov/).
- **Avaliações de Vulnerabilidade:** as avaliações de vulnerabilidade examinam a rede em busca de vulnerabilidades de segurança conhecidas. As ferramentas de verificação de vulnerabilidades comparam o computador com o Índice de Vulnerabilidade e Exposição Comum (CVE) e boletins de segurança fornecidos por fornecedores de software. O CVE é uma lista independente de fornecedor de vulnerabilidades de segurança relatadas e é mantida. Para obter informações, visite o site da CVE (<http://cve.mitre.org/>). O software de verificação de vulnerabilidade executado no contexto de segurança de um administrador de domínio retornará resultados diferentes daqueles executados no contexto de um usuário autenticado.
- **Teste de Invasão:** Um teste de penetração vai um passo além da varredura de vulnerabilidades porque não apenas apontará vulnerabilidades, mas também documentará como as fraquezas podem ser exploradas e como vulnerabilidades menores podem ser escaladas por um invasor.

Hackers Vs Ethical Hackers

- **BLACK HATS** - Indivíduos com extraordinário conhecimento em computação voltado para praticas maliciosas.
- **WHITE HATS** - Indivíduos com conhecimentos hackers que atuam para a segurança defensiva, também conhecidos como analistas de segurança.
- **GRAY HATS** - Indivíduos que trabalham para ambos os lados, black e white hats.
- **SUICIDE HACKERS** - Indivíduos que visam comprometer sistemas críticos por uma causa não se preocupam de serem pegos ou pagarem pelos seus crimes.
- **SCRIPT KIDDIES** - Indivíduo sem conhecimento que comprometem sistema executando scripts, ferramentas e softwares feitos por hackers reais.
- **SPY HACKERS** - Indivíduos empregados por organizações para descobrir segredos do concorrente.
- **CYBER TERRORISTS** - Indivíduos com largo conhecimento, motivados por uma religião ou intuições políticos.
- **STATE SPONSORED HACKERS** - Indivíduos empregados pelo governo para obter segredos e outras informações de outros governos.

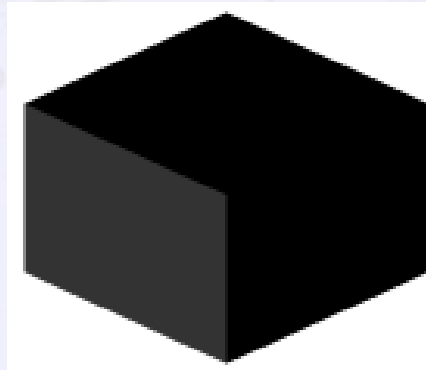
Tipos de Penteste

White-box



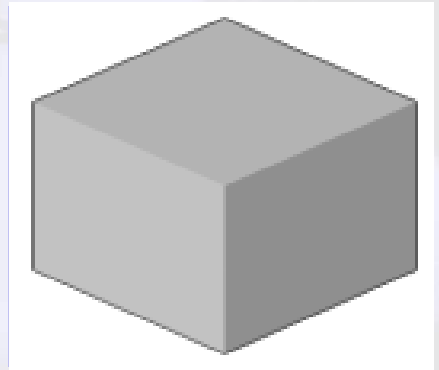
Teste de invasão no qual o analista possui conhecimento detalhado do sistema alvo.

Black-box



Teste de invasão no qual o analista sabe apenas o endereço IP de destino ou nome de domínio

Grey-box



Teste de invasão no qual o analista possui conhecimento parcial do sistema alvo.

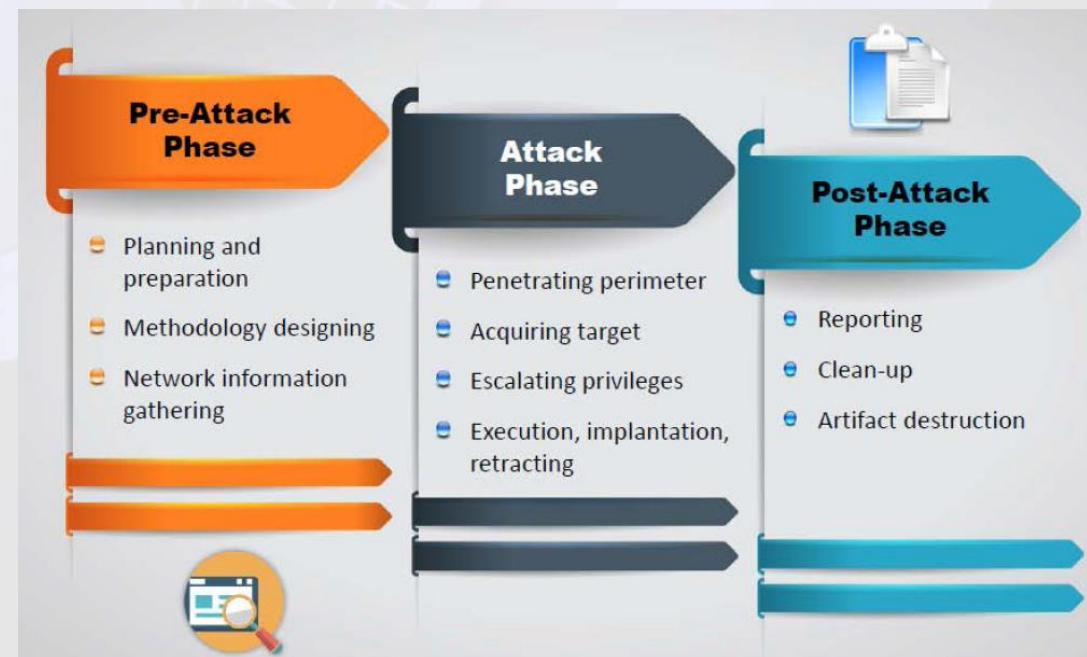
Fases do Penteste

1. Fase de planejamento: Na fase de planejamento, as regras são identificadas e as metas de teste são definidas. As informações sobre o alvo são coletadas na fase pré-ataque. As informações coletadas formarão a base da estratégia de ataque.

2. Fase pré-ataque: A fase pré-ataque inclui identificação de ameaças para ajudar a conduzir uma avaliação de risco e calcular a criticidade relativa da ameaça. O impacto comercial das ameaças pode ser designado como alta, média ou baixa. Métricas internas usam dados disponível dentro de uma organização para avaliar o risco de ataque, enquanto as métricas externas são derivadas de dados coletados fora da organização.

3. Fase de ataque: A fase de ataque envolve o próprio comprometimento do alvo, talvez explorando uma vulnerabilidade encontrada durante a fase pré-ataque ou utilizando brechas de segurança, como uma segurança fraca de política de acesso.

4. Fase pós-ataque: é de responsabilidade do analista para restaurar quaisquer sistemas para o estado pré-teste. Lembrar o objetivo do penteste é mostrar onde existem falhas de segurança, não para corrigir os problemas.



Metodologias PenTeste

Metodologia:

Um sistema de métodos utilizados em uma determinada área de estudo ou atividade

Metodologia (PenTest)

A abordagem sistemática que um Pentester utiliza antes, durante e depois de um teste de invasão, avaliação ou prestação de um serviço

Os testes de invasão utilizam as mesmas etapas tomadas por agentes de ameaças ou hackers

Metodologias PenTeste

Emulação Adversária

Imita as táticas, técnicas e procedimentos de um agente de ameaças do mundo real em um teste de invasão

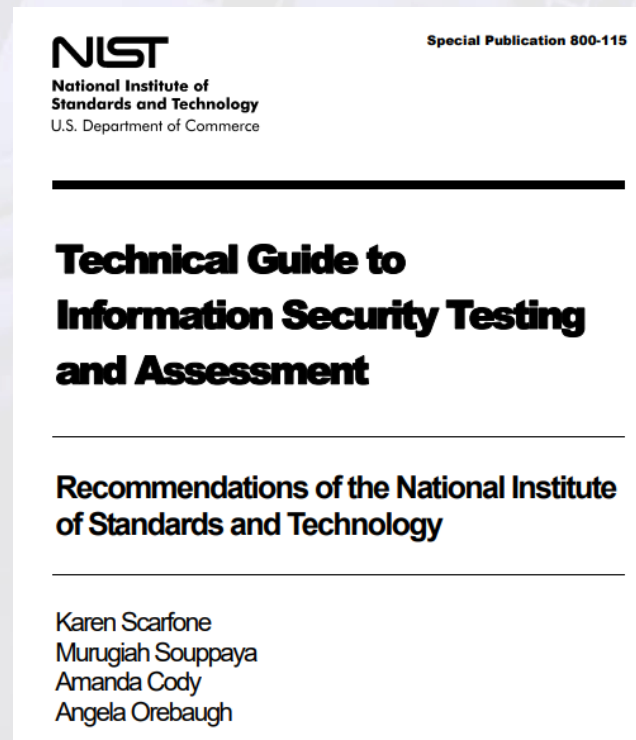
EC Council CEH	CompTIA PenTest+	NIST SP 800-115
Permission	Planning and Scoping	Plan
Reconnaissance	Information Gathering and Vulnerability Scanning	Discover
Scanning and Enumeration		
Gaining Access		
Escalation of Privileges	Attacks and Exploits	Attack
Maintaining Access		
Covering Your Tracks and Installing Backdoors		
Reporting	Reporting and Communication	Report

Metodologias PenTeste

Publicação Especial NIST 800-115 (Technical Guide to Information Security Testing and Assessment)

Guia Técnico para Testes e Avaliação de Segurança da Informação

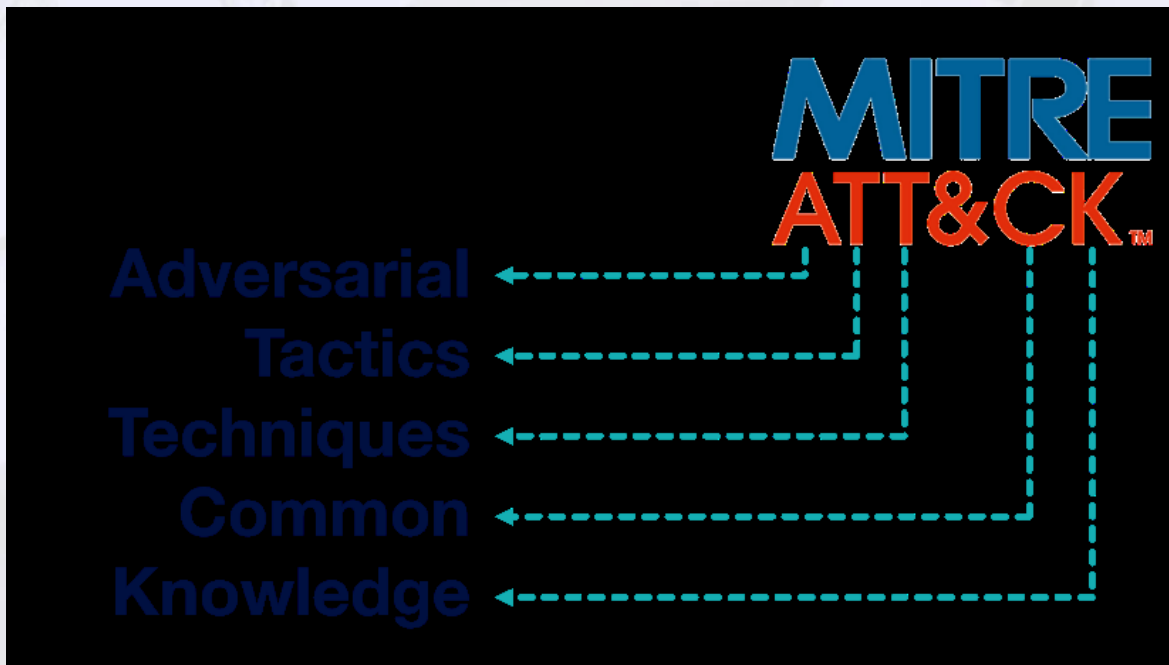
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>



Metodologias PenTeste

Estrutura MITRE ATT&CK (<https://attack.mitre.org/>)

Uma base de conhecimento mantida pela MITRE Corporation para listar e explicar táticas e técnicas comuns de adversários observadas no mundo real (attack.mitre.org)



Mapeia a metodologia de cada ator de ameaça durante diferentes tipos de ataques

É uma ótima maneira de visualizar as técnicas, táticas, conhecimentos e capacidades de um adversário

Obs: Excelente fonte para criação de relatórios.

Metodologias PenTeste

Padrões para Testes de Invasão

Open Web Application Security Project (OWASP) (<https://owasp.org/>)

Fornecer projetos de software liderados pelas comunidades de educação e treinamento, e se tornou a fonte para proteger aplicações/páginas web (owasp.org)

Guia de teste de segurança da Web OWASP

Um guia abrangente para testar a segurança de aplicativos e serviços da web

OWASP Top 10 (<https://owasp.org/Top10/>)

Um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web

Metodologias PenTeste

Padrões para Testes de Invasão

Open-Source Security Testing Methodology Manual (OSSTMM)

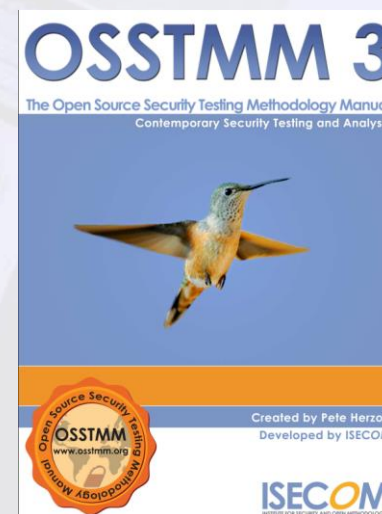
Manual de metodologia de teste de segurança de código aberto

Fornece uma metodologia para um teste de segurança completo

De código aberto e livre para divulgar e utilizar

A última versão (Ver.3) foi lançada em 2010

Auditoria OSSTMM



Utilizado para criar uma medição precisa de segurança em um nível operacional em uma organização, sem suposições e evidências anedóticas

Anedóticas : Ocorre quando há falsa relação de causa e efeito, que muitas vezes vai contra as informações científicas do assunto em questão.

Material: <https://www.isecom.org/OSSTMM.3.pdf>

Metodologias PenTeste

Padrões para Testes de Invasão

Information Systems Security Assessment Framework (ISSAF)

Estrutura de Avaliação de Segurança de Sistemas de Informação

Um guia abrangente ao realizar um teste de invasão que vincula etapas individuais de teste de invasão com as ferramentas de teste de invasão relevantes

Criado pelo Open Information Systems Security Group (OISSG)

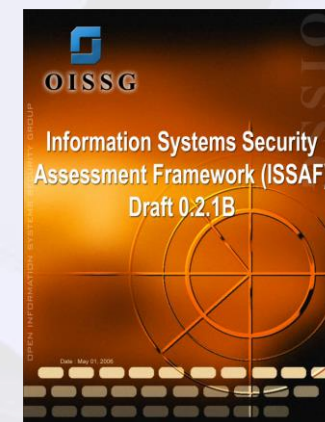
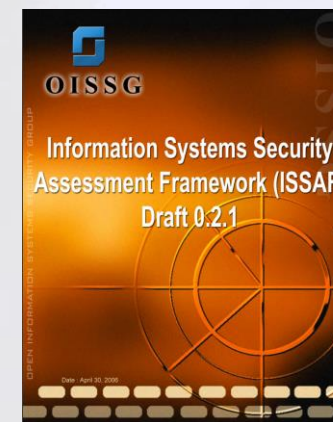
Última atualização em 2015

Material: Information Systems Security Assessment Framework (ISSAF) draft 0.2:

<https://untrustednetwork.net/files/issaf0.2.1.pdf>

Material: Penetration Testing Framework (PTF)

http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf



Metodologias PenTeste

Padrões para Testes de Invasão

Padrão de Execução de Teste de Penetração (PTES)

Desenvolvido para cobrir tudo relacionado à um teste de invasão

Visa fornecer uma linguagem comum e escopo para realizar testes de invasão

Material: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Diretrizes Técnicas PTES

Esta seção foi projetada para ser as diretrizes técnicas do PTES que ajudam a definir certos procedimentos a serem seguidos durante um teste de penetração. Algo a ter em conta é que estes são apenas métodos de linha de base que foram usados na indústria. Eles precisarão ser continuamente atualizados e alterados pela comunidade, bem como dentro de seu próprio padrão. Diretrizes são apenas isso, algo para guiá-lo em uma direção e ajudar durante certos cenários, mas não um conjunto abrangente de instruções sobre como realizar um teste de penetração. Pense fora da caixa.



Metodologias PenTeste

Planejamento dos Testes de Invasão



Metodologias PenTeste

Planejamento dos Testes de Invasão

Considerações de Planejamento			
Público-alvo	Objetivo	Compliances/ Conformidades	Recursos
Plano de comunicação	Produto/ Relatório	Restrições Técnicas	Abrangência

Padrões

PCI-DSS

O Payment Card Industry Security Standards Council (PCI-SSC) foi fundado pela American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc., como um fórum global para a disseminação de padrões de segurança na proteção de dados de pagamento, e define o PCI Data Security Standard (PCI-DSS).

O PCI Data Security Standard (PCI-DSS) especifica recomendações mínimas de segurança obrigatórias para todas as empresas que participam da rede de captura de pagamento com cartões, o comércio, e prestadores de serviços que processam, armazenam e/ou transmitem eletronicamente dados do portador do cartão de crédito.



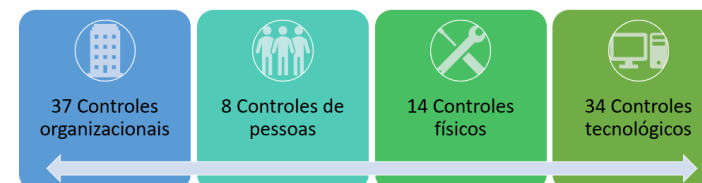
ISO/IEC 27001:2022

É publicado pela Organização Internacional de Normalização (ISO) e da Comissão Eletrotécnica Internacional (IEC).

É uma especificação para um sistema de gestão de segurança da informação (ISMS). Organizações que cumpram a norma pode ser certificado em conformidade por um organismo de certificação independente e credenciada na conclusão bem sucedida de uma auditoria de conformidade formal.

Ela especifica os requerimentos para determinar, implementar, manter e melhorar constantemente um sistema de gerenciamento de segurança da informação dentro do contexto da organização.

93 Controles da nova ISO 27002



Padrões

HIPAA

HIPAA (Health Insurance Portability and Accountability Act) é um conjunto de normas que organizações de saúde norte-americanas devem cumprir para proteger as informações. Em português, seria Lei de Portabilidade e Responsabilidade de Seguro Saúde.

A norma HIPAA é uma lei norte-americana que, embora não se aplique no Brasil, vem servindo de inspiração para hospitais do nosso país, pois, estar em conformidade com a HIPAA demonstra uma maior maturidade da segurança das informações das instituições.

A norma HIPAA ganhou visibilidade quando houve uma série de crimes cibernéticos nos Estados Unidos. O sequestro de dados dos sistemas de hospitais provocaram prejuízos inestimáveis à imagem dessas instituições.



SOX

A Lei Sarbanes-Oxley é uma lei estadunidense, assinada em 30 de julho de 2002 pelo senador Paul Sarbanes e pelo deputado Michael Oxley. Motivada por escândalos financeiros corporativos, essa lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas.

A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas.



Padrões

DMCA

Digital Millennium Copyright Act, conhecido como DMCA é uma lei dos Estados Unidos da América sobre direito autoral, que criminaliza não só a infração em si, mas também a produção e a distribuição de tecnologia que permita evitar as medidas de proteção aos direitos de autor. Além disso, ela aumenta as penas por infrações de direitos autorais cometidas via Internet.

Aprovada em 12 de outubro de 1998 por unanimidade no Senado dos Estados Unidos e sancionada pelo presidente Bill Clinton em 28 de outubro de 1998, a DMCA alterou a legislação dos EUA para ampliar o alcance dos direitos de autor, ao mesmo tempo em que limitou a responsabilidade dos prestadores de serviços on-line sobre violações de direitos autorais cometidas por seus usuários.



FISMA

Define um framework para a gestão da segurança da informação que deve ser seguido por todos os sistemas de informação utilizados ou acionados por uma agência do governo federal dos EUA sobre os poderes executivos ou legislativos, ou por um contratante ou outra organização em nome de uma agência federal nesses ramos. Este framework é ainda definido pelas normas e diretrizes desenvolvidas pelo NIST. Isso inclui:

- Padrão para categorização da informação e sistema de informação por impacto.
- Padrão para requerimento mínimo de segurança para informação e sistemas de informação.
- Guia para selecionar controles de segurança apropriados para sistemas de informação.
- Guia para avaliar controles de segurança em sistemas de informação e determinar controles de segurança efetivos.
- Guia para autorização de segurança do sistema de informação





Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.