SIFEH - Segurança da Informação x Forense x Ethical Hacker
Os segredos oficialmente práticos

O ser humano sempre se preocupou com a sua segurança e de seus bens, isto faz parte de nossos instintos. Na sociedade moderna, o maior bem que a humanidade possui são as informações e conhecimentos gerados por ela, tanto para concretização de negócios quanto para tomada de decisões e planejamento estratégico. Atualmente as informações são consideradas recursos críticos e se encontram sob constante risco, como nunca estiveram antes. Com isso a segurança da informação tornou-se ponto crucial para sobrevivência das organizações, gerando a necessidade do desenvolvimento de métodos e técnicas que permitissem a sua proteção.

O meio cibernético é um ambiente hostil e você deve estar preparado para enfrentar ameaças reais. Com o programa SIFEH, você aprenderá na prática e com a "mão na massa" a analisar as falhas de segurança em um ambiente de infraestrutura de TI do ponto de vista de um hacker. Você aprenderá técnicas e recursos usados nos ataques dos principais grupos hackers do mundo.
Segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade em sistemas de informações.
A Segurança da Informação surge não apenas como um diferencial competitivo, mas também, como uma questão estratégica para proteger a informação de diversos tipos de ameaças, garantindo assim a continuidade dos negócios e, por conseguinte, a própria sobrevivência da organização.
Os esforços relacionados com a busca de melhores mecanismos para salvaguardar a segurança culminaram com a homologação da "Norma Internacional de Segurança da Informação" denominada "ISO/IEC 27002". Esta norma trata da segurança das informações e não somente dos dados que trafegam pela rede ou que residem dentro de um sistema computacional.
Lembre-se que o que acontece no seu ambiente de trabalho é sua responsabilidade e entender como os ataques são deflagrados ajuda a definir e por em pratica um plano de contingência rápido e eficiente.

OBJETIVO
O curso tem como objetivo transmitir aos alunos conceitos, metodologias e práticas de Gerência de Segurança da Informação, uma vez que pessoas e processos, e não somente a tecnologia, são aspectos essenciais para a segurança dos negócios das organizações, como: analisar a sua exposição a ameaças de segurança, proteger os sistemas e os dados da sua organização, reduzir a suscetibilidade de ataque adotando medidas estratégicas, sistemas de criptografia de dados e recursos de segurança em várias camadas, avaliar os mecanismos de autenticação de usuário e computadores, gerenciar os riscos internos da organização e da Internet, proteger os usuários de rede de aplicativos hostis e vírus e identificar os riscos de segurança que precisam ser abordados dentro da sua organização.

ÉTICA
As informações desse treinamento devem ser utilizadas com prudência e ética. Neste treinamento serão ensinadas táticas e truques da cultura hacker. Não passe informações adiante e use as ferramentas apresentadas somente para fins educacionais.

PONTO DE ATENÇÃO
Esse treinamento usa prática em sala de aula de ataques hackers e não deve ser reproduzido em ambientes reais salvo aqueles em que há acordo e analise e que sejam controlados.

A QUEM SE DESTINA:
Profissionais dos diversos níveis envolvidos com sistemas de Gestão, Segurança, Forense, Auditoria, Controladoria, Inovação, Estruturação Organizacional e demais interessados em desenvolver habilidades fundamentais para implementar sistemas de segurança destinados a proteção das informações de sua organização contra ameaças.

CARGA HORÁRIA: 24 Horas

METODOLOGIA:
O curso será ministrado aliando teoria e prática com aulas expositivas, estudo de textos, sessões de vídeo, simulações e debates.
Importante
O curso terá como base a bibliografia sobre segurança da informação, Cada técnica envolverá 2 ou mais ferramentas. (A ISSX & Blackdoor Security seguem o padrão de uso das melhores ferramentas de mercado ou "0 Day").a legislação e o instrumental produzidos pela International Standards Organization (ISO) e Associação Brasileira de Normas Técnicas (ABNT).

Conforme Cláusula Primeira das Condições Gerais do Contrato de Prestação de Serviço Educacional, estamos reservado no direito de alterar a data de início do Curso ou de cancelá-lo, na hipótese de não ser atingido o número mínimo de alunos necessários à cobertura dos custos envolvidos, sendo garantido ao(à) aluno(a), sem qualquer correção, a devolução das quantias pagas. Adicionalmente, nos reservamos ao direito de introduzir melhorias e/ou aperfeiçoamentos no Curso, podendo, para tanto, alterar seu conteúdo e/ou a ementa das disciplinas, desde que tais melhorias e/ou aperfeiçoamentos preservem o objetivo acadêmico do Curso e não importem em ônus adicional para o(a) aluno (a) ou na redução da carga horária total.