Todos nossos cursos são preparados por mestres e profissionais reconhecidos no mercado de Segurança da Informação no Brasil e exterior.

Os cursos são ministrados em português, espanhol ou inglês, atendendo suas necessidades locais de formação.

Os cursos são oferecidos em turmas abertas compostas no máximo por 9 alunos, podendo também ser oferecido na modalidade In Company.

A formação em segurança da informação destina-se ao seguinte público:

- Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação , Auditoria , Sistemas e Compliance.

- Profissionais em geral com interesse em conhecer e aprimorar as boas práticas em segurança da informação.

A nossa formação apresenta um diferencial no mercado, onde você pode se especializar na área de seu interesse, possibilitando forte reconhecimento no mercado de trabalho.

Ethical Hacking

Objetivo

Este curso permite compreender as vulnerabilidades de equipamentos e demais ativos de empresas através de uma análise, também conhecida como Penetration Testing. O aluno ao fim do curso estará apto a desenvolver análises e testes de vulnerabilidade, visando tanto a proteção de seus ativos, quando a realização de análises em demais empresas, sendo este um segmento de grande rentabilidade em segurança da informação.

Público alvo

Gestores, consultores e técnicos nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e Compliance.

Profissionais em geral com interesse em conhecer boas práticas em segurança da informação.

Benefícios

Conhecer mais profundamente as vulnerabilidades em ativos tangíveis e processos no que tange a segurança da informação.

Saber como aplicar os principais testes e analisar os resultados.

Metodologia de ensino

Exposição interativa com apresentação de estudo de casos e exercícios práticos. O curso tem como proposta preparar o participante para estar apto desenvolver análises e testes de vulnerabilidade. Através de abordagem teórica e prática, com a aplicação de exemplos e simulados, abrangendo a estrutura de controle e os processos que envolvem segurança da informação com foco em vulnerabiliade, propiciando um suporte para elucidação de dúvidas durante e após o término imediato do curso.

Pré requisitos

Não existem pré requisitos mandatórios para este treinamento; no entanto, experiência de trabalho em segurança de TI, melhoria de processos ou Serviços de TI é recomendada, bem como conhecimentos básicos da língua inglesa, na parte de leitura especificamente, dado que muitos materiais e referencias ainda se encontram neste idioma.

Carga Horária:

32 horas (08:30h às 17:30h) – 4 dias

Conteúdo Programático

1. **Introdução e Conceitos:**

   - Hacking na Ficção e Vida Real;
   - Psicologia Hacker;
   - Elementos da Segurança;
   - Requisitos e Habilidades de um Ethical Hacker;
   - Mandamentos de Um Ethical Hacker.

2. **Reconhecimento e Coleta de Informações:**

   - Tipos de Reconhecimento;
   - Fases do Reconhecimento;
   - Alcance e Relevância;
   - Metodologia para Reconhecimento;
   - Coleta de Inteligência.

3. **Enumeração e Varreduras em diversas frentes:**

   - Limitação dos Testes;
   - Processo de Varedura;
   - Tipos de Enumeração;
   - Identificação de Alvos;
   - Varredura de Portas;
   - Fingerprinting sobre sistema operacional e aplicativos;
   - Testes em Banco de Dados;
   - Análises e vulnerabilidades em aplicações, serviços e redes sem fio;
   - Ferramentas de Exploração;
   - Evasão de IDS;

- Senhas Padrão e Quebras de Senhas em Dispositivos e Sistemas.

4. **Noções de programação de Ferramentas de Segurança:**

   - Necessidades de uma boa codificação;
   - Passos para uma programação eficiente;
   - Linguagens de Programação;

5. **Backdoors e Trojans:**

   - Tipos de Trojans;
   - Funções Principais dos Trojans;
   - Backdoors.

6. **Certificações e Metodologias:**

   - Certificações do mercado nacional e internacional;
   - Metodologia OSSTMM;
   - Metodologia ISSAF.

7. **Análise e Relatório de Vulnerabilidade:**

   - Estudo de Caso;
   - Relatório de Vulnerabilidade.

Facilitador:

Tem mais de 12 anos de atuação em bancos brasileiros em Segurança da Informação e Prevenção à Fraude. É professor do curso de formação em Compliance pela FEBRABAN no Brasil, professor no MBA de Segurança da Informação da FATEC/SP e coordena o curso de Gestão em Segurança da Informação e Gerenciamento de Projetos no SENAC/SP. É Engenheiro eletrônico da EEM com pós graduação em administração pela FGV e mestre em ciência forense pela POLI/USP. É reconhecido pela imprensa Brasileira e Argentina com trabalhos realizados em vários países do mundo.