Proposta Comercial

Curso:

Técnicas de Computação Forense

Código do Curso: 509

Carga Horária:
40 horas

Oferecido nas modalidades:

- Presencial (Sob Demnada)
- Online: Live Class ou Agile Class
- In Company

4·Linux Open Software Specialists™

Empresa líder na formação de profissionais Linux e open software.

Mais de 70.00 alunos treinados.

Mais de 4800 empresas atendidas.

Muito Prazer, somos a 4Linux.

Fundada em 2001, a 4Linux é líder de mercado em cursos de Linux e open source com números que impressionam: mais de 70.000 alunos treinados, mais de 4.800 empresas atendidas e mais de 40 diferentes cursos altamente especializados. Somos uma das poucas escolas de TI que também atua em consultoria e isso traz inúmeros benefícios aos nossos alunos, com uma metodologia de ensino única.
Localizada em São Paulo, ministramos cursos para turmas fechadas na modalidade presencial e também oferecemos nossos cursos nas modalidades online e in company.

Veja abaixo por que nossos cursos transformam carreiras e nossos alunos são disputados pelas empresas:

CURSOS INOVADORES COM FOCO NA EMPREGABILIDADE

Preparatório para as principais certificações.

AULAS DO TIPO 'MÃO NA MASSA'

Metodologia IT Experience. Vivenciando o mercado de trabalho dentro da sala de aula.

BLENDED LEARNING

Mix de aulas presencial e online, com uso intenso de tecnologias.

OLHAR NO FUTURO

Ensinamos novas tecnologias que o mercado de trabalho irá contratar.

IMPLEMENTAR PROJETOS E ENSINAR

Nos torna únicos no mercado. Sabemos o que é relevante e precisa ser ensinado.

NEM CONSULTORES, NEM INSTRUTORES

CONSTRUTORES = CONSultores + insTRUTORES

Quem deve fazer este curso:

Este curso demonstra na prática as técnicas utilizadas por investigadores e peritos forenses para resolver seus incidentes.

Com assuntos das certificação

CHFI

Alguns números deste curso:

+200.000

Alunos foram treinados pela 4Linux

+984

Alunos assistiram este curso

R$7.895,00

Média salarial de quem concluiu o curso *

+56

Empresas contrataram este curso

* Valor médio aproximado com base nas pesquisas dos maiores portais de empregos: Catho, Indeed, TrabalhaBrasil, Glassdoor e Apinfo.

Após fazer este curso, o aluno estará apto a:

- Se preparar para prova de certificação CHFI;
- Realizar uma investigação;
- Conhecer a fundo o sistema operacional que trabalha;
- Compreender as técnicas utilizadas por investigadores e peritos para resolver casos envolvendo incidentes;
- Efetuar uma investigação digital em ambientes GNU/Linux e Windows;
- Desenvolver técnicas próprias de investigação forense;
- Assegurar que um ambiente possa ser analisado futuramente em caso de suspeita de comprometimento;
- Identificar os principais tipos de ataques em sistemas com suspeita de terem sido alvos;

Veja os diferenciais do curso:

01 Curso fundamentado, totalmente prático, o aluno pode aplicar os conhecimentos aprendidos no próximo dia de trabalho

02 O curso utiliza como guia as melhores normas da área de segurança

03 O curso não se foca somente em ferramentas, apresentando ao aluno uma base sólida de conceitos para que ele possa trabalhar com qualquer ferramenta

04 O curso foi elaborado levando em conta as mais conhecidas certificações da área

05 A 4Linux coloca em sala de aula instrutores que vivem o conteúdo do curso no dia a dia

06 O aluno poderá copiar a máquina virtual em um pen-drive e levar para casa, bastando ter o VirtualBox instalado (em Windows, Mac ou Linux) para utilizar

Ementa do curso

Computação Forense

- Introdução e terminologia
- Estratégias para investigação forense

Aquisição de dados

- Memória mapeada por processos
- Memória no espaço do usuário
- Memória no espaço do kernel
- Outras memórias
- Mídias USB e ópticas
- Partições
- Discos rígidos

Investigação de ambientes GNU/Linux

- Características de segurança entre versões de kernel 2.6 e 3.x
- Aquisição e análise de dados da memória com dd e /dev/fmem
- Aquisição de dados de filesystems Ext4 e XFS com dcfldd
- Análise de dumps com foremost
- Identificação de binários ELF maliciosos com objdump e gdb

Investigação de ambientes Windows

- Características de segurança entre versões do Windows 7 e 8
- Aquisição e análise de dados da memória RAM com dd e mdd
- Aquisição de dados de filesystems FAT-32 e NTFS
- Análise de dumps com volatility
- Identificação de binários PE maliciosos

Ementa do curso

Identificação e análise de outros tipos de arquivos

- Documentos PDF com pdfid.py e pdf-parser.py
- Imagens com jhead e esteganografia em multimídia com steghide e outguess

Análise de tráfego de TCP/IP

- Sniffing: conceito, funcionamento e filtros com tcpdump
- Entendendo o modelo OSI com o Wireshark
- Análise de protocolos de alto nível (HTTP, FTP etc)

Anti-forense

- Objetivo e técnicas
- Precauções e ações
- Anti-anti-forense

Pré-requisitos

Para o aluno

- Para acompanhar o curso, o aluno deve saber utilizar computadores, inicializar uma máquina virtual com VirtualBox e ter conhecimentos em administração de sistemas GNU/Linux
- Ter participado dos cursos 701, 702, 703 e 704 da Formação Linux da 4Linux ou conhecimento equivalente

Computacionais presencial/EAD/EAD AO VIVO

- É necessário que o aluno tenha um computador (Notebook ou Desktop) com no mínimo 6GB de memória RAM, com processador com suporte à 64bits pois será necessário emular máquinas virtuais para realizar os laboratórios práticos
- Ter instalado o VirtualBox com o Extension Pack em seu sistema operacional (Linux, MacOS X, Windows) pois será necessário emular máquinas virtuais para realizar os laboratórios práticos
- Caixas de Áudio ou Fones de ouvido
- Monitor configurado com resolução mínima de 1024x768
- Navegador de Internet Google Chrome/Chromium
- Sistema Operacional Linux, Windows ou MacOS X
- Recomendado 5MB de velocidade de conexão internet banda larga
- Alunos com computadores da Apple de arquitetura ARM não conseguirão realizar nossos cursos que necessitam de virtualização (VirtualBox, KVM, VMWare, Parallels), pois até o momento não há suporte oficial e/ou estável nestas plataformas para a virtualização de máquinas com arquitetura x86_64

Pré-requisitos

Acesso à plataforma de ensino

> Os materiais e video-aulas dos cursos da 4Linux estão disponíveis no seguinte endereço: https://aia.4linux.com.br . Os alunos receberão o acesso próximo do dia do treinamento , é importante que eles validem o acesso na plataforma.
> A ferramenta de conferência que utilizamos para as aulas ao vivo é o Google Meet.
  > Para fins técnicos: O Google Meet utiliza por padrão as seguintes portas: TCP/443 e UDP/19302-19309
  > IPv4: 74.125.250.0/24 IPv6: 2001:4860:4864:5::0/64

https://.google.com/
https://.googleapis.com/
https://.gstatic.com/
https://.googleusercontent.com/

In Company

> Sala equipada com projetor, Quadro Branco ou FlipChart
> Acesso à internet por Banda larga, utilizando Rede Ethernet
> Caso exista algum proxy ou bloqueio na rede, a 4Linux deverá ser informada para providenciar com antecedência o download dos arquivos necessários

FICOU COM ALGUMA DÚVIDA?

Converse agora com nossos consultores para informações de datas e valores

FALE COM A GENTE

SP

T: +55 11. 2125-4747

T: +55 11. 2125-4748

W: +55 11. 96429-0501