Seja um investigador capaz de coletar evidências digitais e conduzir uma análise em sistemas comprometidos.

Análise Forense

O curso apresenta as técnicas e ferramentas utilizadas em análise forense computacional. Algumas das competências desenvolvidas no curso: procedimentos a serem seguidos pelo investigador durante a análise do incidente; preparação de ferramentas que serão utilizadas durante a investigação; coleta de evidências em uma imagem de disco de uma máquina comprometida; elaboração de uma cronologia do ataque, descrevendo o que aconteceu e quando ocorreu cada evento do computador investigado; compreensão das particularidades do processo de análise forense em Linux e Windows e das informações que devem ser coletadas em cada situação enfrentada; identificação das informações dos programas executados e bibliotecas associadas.

Características

- O curso está dividido em dez sessões, totalizando 40 horas.
- O curso oferece atividades práticas em laboratório. Cada aluno tem sua própria estação de trabalho.
- A Escola Superior de Redes oferece material teórico impresso.

Competências desenvolvidas

- Conhecimento sobre ferramentas forenses e sua utilização em uma investigação;
- Capacidade de elaborar uma cronologia, descrevendo cada evento do comprometimento investigado;
- Coletar informações relacionadas aos programas executados, às bibliotecas do sistema e portas relacionadas;
- Capacidade de identificar o tipo de auditoria mais adequado para cada caso.

Conhecimentos prévios

Funcionamento de sistemas Linux e Windows, conhecimento básico sobre investigação de incidentes de segurança ou o curso Segurança de Redes e Sistemas.

Investimento

- R$ 2.560,00

Programa do curso

- Princípios de análise forense: conceito e motivação;
- Como agem os atacantes;

Escola Superior de Redes RNP

esr.rnp.br

RNP

- Tipos de sistemas comprometidos;
- Procedimentos de análise forense;
- Cadeia de custódia de evidências;
- Ambiente e ferramentas de análise forense;
- Ambiente de análise forense: o hardware, o sistema operacional e o software básico;
- Pacotes forenses: ferramentas dos níveis de sistemas de arquivo e de nomes de arquivos, de metadados e de blocos de dados;
- Coleta de evidências: arquivos de logs, de inicialização do sistema e de histórico de comandos;
- Recuperação e análise de evidências;
- Sistema de arquivos Linux;
- Ferramentas de recuperação de evidências: como reaver arquivos apagados e parcialmente sobrescritos;
- Evidências avançadas: análise de executáveis e evidências avançadas;
- Cronologia dos acontecimentos e reconstrução do ataque;
- Análise forense em sistemas Windows;
- O sistema de arquivos do Windows;
- Descrição do pacote de ferramentas e primeiras ações;
- Informações sobre o sistema: identificação de ações, de usuários e do nome do sistema (hostname);
- Identificação de processos em execução no sistema;
- Identificação de portas disponíveis;
- Identificação de bibliotecas em uso;
- Registro do Windows;
- Informações adicionais do Windows;
- Métodos de ocultação de dados e informações.

Escola Superior de Redes RNP

esr.rnp.br

RNP