



Introdução à Forense Computacional em Sistemas Unix

Rafael Soares Ferreira



Descrição e objetivos do tutorial:

A Análise Forense Computacional pode ser definida como um conjunto de técnicas utilizadas para coletar, reunir, identificar, examinar, correlacionar, analisar e documentar evidências digitais. Este curso visa familiarizar o aluno com os conceitos básicos de análise forense, e apresentar os principais procedimentos e ferramentas utilizadas no processo de coleta e análise de evidências em sistemas Unix.

Público-Alvo:

Analistas de Segurança e de Sistemas, administradores de redes, membros de CSIRTs, consultores, técnicos em informática, entusiastas e profissionais atuantes na área de investigação Computacional.

Mini-currículo do instrutor:

Rafael Soares Ferreira é analista de segurança da empresa Clavis Segurança da Informação e diretor da equipe de Resposta a Incidentes e Auditorias do Grupo de Resposta a Incidentes de Segurança do Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro - GRIS/DCC/IM/UFRJ. Desenvolvedor do projeto TamoioBSD que consiste em uma remasterização do sistema OpenBSD funcionando na forma de livecd e contendo as principais ferramentas de segurança computacional. Já ministrou cursos relacionados a segurança em diversos eventos da área. Possui experiência como membro de CSIRTs com foco nas seguintes áreas: forense computacional, resposta a incidentes e auditoria de redes e sistemas.



Ementa:

1. Definições
 - 1.1. Forense Digital x Resposta a Incidentes
 - 1.2. Evidências
2. Sistemas de arquivos
 - 2.1. Definições
 - 2.2. Particionamento lógico
 - 2.3. Abstrações do sistema de arquivos
3. Metodologia Básica
 - 2.1. Modelos internacionais vigentes
 - 2.2. Análise Viva x Morta
 - 2.3. Graus de volatilidade
 - 2.4. Coleta de evidências
 - 2.5. Linha do Tempo
 - 2.6. Recuperação de dados
 - 2.7. Relatório
4. Extração e recuperação de evidências
 - 4.1. Imagens, cópias e princípios de verificação
 - 4.2. Reconstruindo particionamento lógico
5. Linha do Tempo
 - 5.1. Modificações de timestamps: análise de MAC Times
 - 5.2. Correlacionando evidências
 - 5.3. Reconstituindo o incidente
6. Recuperando arquivos apagados
7. Estudo de Caso - Hands On

Pré-requisitos:

Conhecimentos Básicos em Unix.