Ementa CP.M.2: Técnicas e ferramentas para descriptografia de dados

Instrutor: Matheus Bichara de Assumpção — Perito Criminal Federal, Polícia Federal*Data/Horário:* 27 de outubro de 2026, das 13h às 17h- *Carga horária:* 4 horas

1. Objetivo

Proporcionar aos participantes conhecimentos teóricos e práticos sobre técnicas e ferramentas utilizadas na identificação, extração e tentativa de acesso a dados protegidos por criptografia e senhas, com foco na atuação pericial.

O minicurso abordará fundamentos técnicos, boas práticas, limitações operacionais e exemplos práticos relacionados à análise de mídias, arquivos, contêineres criptografados, senhas protegidas por mecanismos do sistema operacional e outros artefatos digitais protegidos. Também serão discutidas metodologias para levantamento, análise e priorização de senhas, com ênfase em estratégias aplicáveis à rotina da perícia digital.

2. Pré-requisitos e infraestrutura necessária

Por parte da organização do evento:

* Sala com mesas e cadeiras;

* Computadores ou notebooks com Windows e acesso estável à internet;

* Pontos de energia suficientes para todos os alunos;

* Disponibilização de pendrives para distribuição de ferramentas e materiais de apoio.

Por parte dos alunos:

* Notebook pessoal, se não fornecido pela organização;

* Conhecimentos básicos de informática, sistemas operacionais e perícia digital.

3. Conteúdo programático

Módulo 1 — Fundamentos de criptografia aplicada à perícia digital

* Conceitos básicos;

* Diferenças entre codificação, hash, senha e criptografia;

* Principais cenários encontrados em exames periciais envolvendo dados protegidos;

* Noções sobre arquivos, volumes, bancos de dados, credenciais e contêineres criptografados;

* Limitações técnicas na tentativa de acesso a dados protegidos;

* Importância da preservação da evidência digital.

Módulo 2 — Identificação, triagem e extração de artefatos protegidos

* Reconhecimento de arquivos, volumes, bancos de dados e contêineres criptografados;

* Triagem de mídias e sistemas em busca de senhas e artefatos potencialmente relevantes;

* Introdução ao DPAPI e aos mecanismos de proteção de credenciais em sistemas Windows;

* Noções sobre hashes NTLM e sua relevância na análise de credenciais em ambientes Windows;

* Análise de senhas protegidas, credenciais armazenadas por aplicações e artefatos vinculados ao sistema operacional;

* Uso de ferramenta para análise, triagem e extração de artefatos em imagens, sistemas de arquivos e ambientes Windows;

* Organização dos dados extraídos para subsidiar etapas posteriores de análise e tentativa de quebra.

Módulo 3 — Metodologia para priorização e quebra de senhas com Hashcat e John the Ripper

* Levantamento e organização de possíveis senhas a partir do caso;

* Análise de padrões de formação de senhas;

* Priorização de senhas e estratégias de ataque conforme o contexto investigativo;

* Construção, tratamento e validação de listas;

* Uso de informações contextuais da investigação para geração de candidatos;

* Ataques de dicionário, força bruta, máscaras, regras customizadas e ataques híbridos;

* Preparação de hashes e artefatos para tentativa de quebra;

* Demonstrações práticas com as ferramentas Hashcat e John the Ripper;

* Discussão sobre desempenho, limitações, tempo estimado, hardware disponível e estratégias de otimização.

4. Minicurrículo do instrutor

Matheus Bichara de Assumpção possui graduação em Engenharia Eletrônica pela Universidade de Brasília (UnB) e em Engenharia de Computação pelo Centro Universitário de Brasília (CEUB), além de mestrado em Electrical and Computer Engineering pela University of Florida, nos Estados Unidos. Tornou-se Perito Criminal Federal em 2020 e atua no campo de criptografia e quebra de senhas, sendo um dos desenvolvedores de técnica inovadora de desbloqueio de dispositivos protegidos com BitLocker. Atua também como pesquisador, tendo publicado trabalho no periódico Forensic Science International: Digital Investigation, premiado como melhor artigo na DFRWS EU 2023, realizada na Alemanha.Conquistou o primeiro lugar, com a equipe da Polícia Federal, na competição de cibersegurança National Cyberleague, em Madri, Espanha, que contou com a participação de agências como FBI, Serviço Secreto dos Estados Unidos e Europol. Também foi finalista na competição internacional SCAN 2024, voltada ao rastreamento de criptomoedas e ativos digitais, realizada em Seul, Coreia do Sul.Atualmente, atua no Instituto Nacional de Criminalística da Polícia Federal, em perícias de informática e projetos