Computação Forense e Investigação Cibernética – 360 h

O curso trará a legislação aplicada para crimes na rede, como o usuário pode se proteger de ataques na WEB, analisar crimes cibernéticos em sistemas Windows, Linux e móveis. Análise de dispositivos eletrônicos com o intuito de alterar seu funcionamento original.

Disciplinas:

- Estratégias de Segurança Cibernéticas
    - Introdução à Segurança Computacional
    - Introdução à Privacidade e Proteção dos Dados
    - Governança
    - Ataques e suas características
    - Ferramentas e Processos

- Gestão de Segurança da Informação
    - Pilares da Segurança da Informação
    - Nomes e Padrões em Segurança da Informação (ISO / NIST / PCI)
    - Ameaças, vulnerabilidades, Riscos e tipos de ataques em segurança
    - Política e Conscientização em Segurança da Informação
    - Segurança em Internet das Coisas, Ciberataques e Ransomware
    - Segurança em Cloud Computing e segurança em dispositivos móveis

- Criptografia e Criptoanálise, privacidade e comunicações digitais
    - Esteganografia
    - Criptografia clássica
    - Criptografia Moderna Simétrica
    - Criptografia Assimétrica
    - Criptografia assimétrica com PGP
    - Hash
    - Brute Force em senhas Hash
    - Criptografia Quântica

- Análise Forense Aplicada a Sistemas Linux
    - Introdução à Forense
    - Fases de Investigação
    - Análise de um incidente
    - Documentação
    - Análise Forense
    - Análise de arquivos de log
    - Coletando hashes
    - Dump de memória RAM
    - Criando e montando imagens
    - Sistema de Arquivos, Análise de Memória e Volatility
    - Criando um perfil no Volatility
    - Malware e Além
    - Comandos úteis

- Introdução à Segurança da Informação
    - Como me proteger?
    - Entendendo Ataques
    - Incidentes de Segurança
    - Monitoramento de Segurança de Camadas
    - Ameaças Mobile
    - Ameaças Avançadas (APTs)
    - Segurança em Dispositivos Móveis
    - Telefonia Móvel

- Malware Hunting
    - O que é uma Threat (Ameaça)?
    - Malwares, Vulnerabilidades e Exploits
    - Cenário Atual
    - Entendendo alguns ataques
    - Ameaças Avançadas Persistentes (APTs)
    - DNA de uma APT
    - Etapas de uma APT
    - Sandbox
    - Threat Hunting
    - Qual time eu deveria ter
    - Empoderando meu SOC
    - Incidentes de Segurança
    - Monitoramento de Segurança em Camadas
    - Gerenciamento de Incidentes
    - Encodings

- Engenharia Social e Phishing
    - Introdução ao No-Tech Hacking
    - Ciência do comportamento
    - Linguagem corporal
    - Introdução à Engenharia Social
    - Análise de Caos
    - Phishing

- Análise Forense Computacional
    - O Perito Forense
    - Análise
    - Coleta
    - Análise Forense em Windows

- Análise Forense Aplicada a sistemas Windows
    - Histórico do Sistema Windows
    - Processo de Boot
    - Dado x Metadado
    - Caso Concreto
    - Comandos Básicos do CMD
    - Coleta e Análise FTK Imager

    - Registry – Forense Windows
    - Quesitação do Requerente
    - Princípio da localidade de Referência
    - Windows Shell Bags
    - Windows Indexing Service
    - Tudo sobre a Lixeira do Windows
    - Evento dos Logs
    - Prática Forense HD Criptografado

- Tecnologias e Frameworks para forense computacional
    - Funcionalidades do FTK IMAGER
    - Análise com VOLATILITY
    - Configuração, Execução e utilização do IPED
    - Processamento de evidências com AUTOPSY
    - Análise de registros com RegRipper