GOHACKING DIGITAL FORENSICS (GHFOR)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 horas

O curso GoHacking Digital Forensics (GHFOR) apresenta desde os conceitos básicos da criminalística e computação forense até os conceitos fundamentais sobre aplicação de técnicas forenses em sistemas operacionais com foco no Sistema Operacional Windows. Unindo teoria e prática na análise dos principais artefatos encontrados no ambiente Windows, proporciona ao discente a compreensão do funcionamento dos sistemas operacionais desenvolvidos pela Microsoft, bem como os elementos neles contidos podem ser utilizados para análise forense computacional, auxiliando na determinação da materialidade, autoria e dinâmica de fatos.

Apesar das frequentes versões e atualizações dos Sistemas Operacionais Windows, existe um eixo comum compartilhado por todas as versões, principalmente no tocante a artefatos utilizados para melhoria de desempenho em detrimento das ferramentas de auditoria. É justamente em cima daquelas que reside grande parte do trabalho forense digital, haja vista os elementos originalmente criados para auditoria serem, por padrão, seletivos no tocante ao registro e tipos de ocorrências perenizadas em arquivos de logs.

Nesse treinamento, serão trabalhadas desde a fundamentação em criminalística e forense computacional até a análise forense tanto dos artefatos do sistema operacional como também da memória principal (RAM), onde os alunos terão uma compreensão das principais formas de progressão na análise pericial sem prejuízo da manutenção de integridade da cadeia de custódia.

O curso GHFOR prepara o aluno para desempenhar trabalhos forenses nas diversas versões do sistema operacional Windows, detentor de um *market share* próximo dos 90%.

MÓDULOS

1. **Fundamentos da Criminalística**
    a. Conceito de Criminalística
    b. Metodologia de Ação da Criminalística
    c. Cadeia de Custódia

2. **Fundamentos de Computação Forense**
    a. Fundamentos Básicos da Computação
    b. Normativos Legais associados à Computação Forense
    c. Fluxo de Trabalho em Computação Forense
    d. Laudo Pericial – Anatomia e Composição
    e. Proteção à informação – Confidencialidade, Integridade, Disponibilidade, Autenticidade.
    f. Fluxo de Trabalho em Resposta a Incidentes
    g. Bases de representação da informação: binária, decimal e hexadecimal.
    h. Boot e Sistemas de Arquivos.
    i. Aquisição de Mídias e Duplicação Forense.
    j. Montagem de kit com Ferramentas para Forense Computacional.

3. **Sistema Operacional Windows**
    a. Histórico e versões do Sistema Operacional.
    b. Registro do Windows – Registry.
    c. Index Search – Local usado para armazenar os termos e resultados das pesquisas feitas localmente
    d. Thumbs.db. Thumbscache.- Arquivo oculto criado pelo sistema operacional Windows, contendo as imagens visualizadas no explorador de arquivos.
    e. Recycle Bin – Pasta especial oculta utilizada como ponto intermediário para a exclusão de arquivos.
    f. Prefetch. Superfetch – Recurso de aceleração de carregamento de programas utilizado no aumento de desempenho do sistema.
    g. Arquivos de Spool – Repositório temporário de arquivos submetidos ao processo de impressão.
    h. Arquivos Link/Shortcut (.LNK) – Arquivos de atalho criados tanto pelo usuário quanto pelo sistema operacional para acesso aos arquivos por eles apontados.
    i. Jump Lists – Recurso de agrupamento de arquivos e pastas baseados na recentidade e frequência de acesso a arquivos.
    j. Shellbags – Região especial do Registro encarregada de armazenar a personalização organizacional visual das pastas.
    k. User Assist - Chaves do Registro com informações sobre a execução de aplicativos e o uso de atalhos associados a tais aplicações
    l. MRU - Listas dos arquivos usados recentemente por determinado usuário do sistema operacional.
    m. Event Logs (Evtx e Evt) - Repositório de informações importantes sobre programas, segurança, eventos do sistema, usuário,

4. **Análise Live – Parte 3**
    a. Metodologia Live. Procedimentos e Ferramentas.
    b. Dump de Memória. Ferramentas.
    c. Análise de Memória Volátil.

PRÉ-REQUISITOS

- Conhecimento básico sobre sistemas operacionais (Windows e Linux)
- Familiaridade com ferramentas de Virtualização – VMWare e/ou VirtualBox

PÚBLICO ALVO

- Analistas de Segurança da Informação
- Especialistas em Segurança da Informação
- Membros de Blue Team
- Membros de CSIRT ou SOC
- Analistas de Forense Computacional
- Pesquisadores de Segurança da Informação
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Entusiastas de Segurança da Informação
- Auditores de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar 01 (uma) Máquina Virtual (VM) compatível com o formato VDI.
- Configuração mínima de 8GB de RAM, 40 GB de espaço livre em disco, placa de rede (RJ45 ou wireless) para acesso à Internet
- Desejável 02 (dois) monitores para incremento na produtividade
- Software de Virtualização: Preferencialmente VirtualBox, na versão mais atual

MATERIAL RECEBIDO

- As máquinas virtuais com as aplicações utilizadas nos exercícios
- Slides do curso no formato PDF
- Certificado de conclusão do curso no formato PDF (com a carga horária e ementa)
- Acesso ao portal do aluno, o GoHacking Academy
- Acesso às gravações do curso no GoHacking Academy

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Adquirir conceitos e técnicas necessárias para que se possa recuperar e analisar os artefatos obtidos nos sistemas operacionais Microsoft Windows de forma eficaz.
- Entender os fundamentos de uma análise forense computacional em sistema Windows.
- Identificar dos principais artefatos forenses encontrados no sistema Windows.
- Resolver casos envolvendo perícias computacionais em Sistema Windows.

Sobre o Instrutor:

Gustavo Pinto Vilar

Perito Criminal Federal do Departamento de Polícia Federal - MJ. Formado em Processamento de Dados e Ciência da Computação pela Associação Paraibana de Ensino Renovado. Especialista em Docência do Ensino Superior pela Universidade Federal do Rio de Janeiro, especialista em Locais de Crime pela Academia Nacional de Polícia e mestrando em Perícias Forenses pela Universidade de Pernambuco. Atuou no Serviço Público como Papiloscopista Policial Federal e como Policial Rodoviário Federal. É Oficial da Reserva de 2ª classe do Exército Brasileiro no posto de Primeiro Tenente da Arma de Cavalaria, trabalhou como Analista de Sistemas na multinacional Xerox do Brasil, foi coordenador de informática na TV Cabo Branco (afiliada da Rede Globo na Paraíba), atuou como docente em cursos preparatórios para concursos da Polícia Federal e na rede privada de ensino superior. Atualmente, leciona na rede ITnerante e ProvasdeTI como docente presencial e na produção de videoaulas. Coautor e revisor dos livros Tratado de Computação Forense, Ciências Forenses - Uma Introdução Às Principais Áreas Da Criminalística, Polícia científica transformando vestígios em evidências à luz da cadeia de custódia. Professor em cursos de especialização relacionados com Ciências Forenses.
CV: http://lattes.cnpq.br/7761508045557488