GOHACKING ADVANCED DIGITAL FORENSICS FOR WINDOWS – (GHADFW)

DESCRIÇÃO

(Nível Intermediário/Avançado)

Carga Horária: 40 hrs

Instrutor: Rodrigo Lange

A perícia forense em sistemas Windows é essencial para a investigação de incidentes cibernéticos, análise de crimes digitais e recuperação de evidências. O **GoHacking Advanced Digital Forensics for Windows (GHADFW)** é um treinamento abrangente, que capacita profissionais a coletar, extrair, analisar e interpretar artefatos digitais presentes no sistema operacional Windows, permitindo a reconstrução de eventos e a identificação de atividades suspeitas.

Este curso oferece uma abordagem prática e aprofundada, cobrindo desde técnicas de coleta e análise de evidências até a aplicação de metodologias avançadas de investigação digital, buscando atingir os seguintes objetivos:

- Identificar e analisar artefatos críticos do Windows para fins forenses.
- Realizar coleta e preservação de evidências digitais de forma segura e estruturada.
- Utilizar ferramentas especializadas para análise de logs, registros e arquivos do sistema.
- Reconstruir a linha do tempo de eventos e correlacionar atividades de usuários e processos.
- Detectar manipulações, acessos não autorizados e tentativas de ocultação de evidências.
- Aplicar técnicas avançadas para análise de malwares e ataques em sistemas Windows.

A perícia digital de ambientes Windows é um campo essencial para a investigação de incidentes cibernéticos, análise forense e resposta a ameaças. O sistema operacional Windows armazena uma grande quantidade de evidências digitais, desde registros de execução de aplicativos até informações de rede e uso de dispositivos. A correta identificação e interpretação desses artefatos são fundamentais para reconstruir atividades suspeitas e garantir a integridade das investigações.

Durante o treinamento, os alunos serão guiados pelas melhores práticas na análise forense digital de artefatos do sistema operacional Windows, explorando técnicas avançadas para reconstrução de atividades de usuários e identificação de ações maliciosas.

Além de aprofundar o conhecimento sobre os principais artefatos do Windows, o curso aborda técnicas sofisticadas de investigação digital, incluindo a análise de logs, detecção de execução de aplicativos, identificação de conexões de rede suspeitas e rastreamento do uso de dispositivos USB. Essas são as mesmas técnicas empregadas por peritos forenses e especialistas em segurança para revelar ataques, fraudes e acessos indevidos em sistemas computacionais.

MÓDULO 1 – Perícia Digital

- Introdução à Perícia Digital
- Ordem de Volatilidade
- Cadeia de Custódia
- Perícia Digital e Resposta a Incidentes
- Desafios da Perícia Digital
- Ferramentas

MÓDULO 2 – Funcionamento do Windows

- Modos de Usuário e Kernel
- Programas, Processos, Threads e Jobs
- Identificadores de Processo (PID) e de Threads (TID)
- Principais Processos
- Serviços (Service Control Manager – SCM)
- Globally Unique Identifier (GUID)
- Security Identifier (SID)
- Privilégios
- Tarefas Agendadas
- SVCHOST
- Drivers
- Handles
- Mutex/Mutant
- Variáveis de Ambiente
- Windows Management Instrumentation (WMI)
- PowerShell
- Registro do Windows
- Volume Shadow Copies (VSC)
- Logs de Eventos
- Sistema de arquivos NTFS

MÓDULO 3 – Coleta em Ambientes Windows

- Comandos do Windows, WMI e PowerShell
- KAPE
- Velociraptor
- Criptografia
- Captura da Memória RAM
- Exame de Dumps de Memória

MÓDULO 4 – Informações sobre o Sistema e Uso de Dispositivos USB

- Conjunto de Controles Atual (*Current Control Set*)
- Versão do Sistema Operacional e Atualizações
- Nome do Computador
- Último Desligamento do Sistema
- Período com Computador Ligado
- Informações Sobre Criptografia nos Volumes
- Data e Horário de Formatação dos Volumes

- Arquivos de Paginação de Memória e Hibernação
- Configurações do Defender
- Variáveis de Ambiente
- Informações sobre Política de Grupo (*Group Policy* - GPO)
- Identificação de Dispositivos USB
- Número de Série de Dispositivos USB
- Nome dos Dispositivos USB
- Data e Hora de Conexão e Desconexão
- Nome do Volume dos Dispositivos USB
- Última Letra do Volume Montado
- Identificador (*Globally Unique Identifier* - GUID) do Volume
- Conta de Usuário que utilizou o Dispositivo USB
- Número Serial do Volume (*Volume Serial Number* - VSN)
- Consolidando as Informações de Dispositivos USB
- Memória RAM

MÓDULO 5 – Evidências Relacionadas a Contas de Usuários e Grupos

- *Security Identifier* (SID) e *Relative Identifier* (RID)
- Contas de Usuários Existentes
- Senha dos Usuários
- Detalhes da Conta Microsoft de Usuário
- Criação de Contas de Usuário
- Exclusão de Contas de Usuário
- Perfis de Usuários
- Último Logon no computador
- Logons Locais com Sucesso e com Falha
- Logons no Domínio com Sucesso e com Falha
- Identificador de Logon
- Grupos de Usuários Existentes
- Participação de Usuários em Grupos
- Associações de Aplicações
- Uso de *Remote Desktop Protocol* (RDP) - MRU
- Uso de *Remote Desktop Protocol* (RDP) - Eventos
- Uso de *Remote Desktop Protocol* (RDP) - Cache
- Serviços
- Uso do PowerShell
- Uso do WMI
- *User Account Control* (UAC)
- Memória RAM

MÓDULO 6 – Evidências Relacionadas à Rede e Localização

- Interfaces de Rede
- Endereço IP e DHCP
- Endereços MAC
- Cache ARP
- Conexões Ativas
- Rotas de Rede

- Arquivos Abertos (localmente e pela rede)
- Histórico de Redes
- Geolocalização de Endereços IP
- Redes Sem Fio
- Pastas Compartilhadas
- MRU Drives de Rede Mapeados
- *System Resource Utilization Monitor* (SRUM)
- Informações de Diagnóstico (EventTranscript.db)
- Informações sobre a Região
- Idiomas Instalados no Windows
- Fuso Horário (*Timezone*)
- Horário de Verão (*Daylight Saving*)
- *Alternate Data Streams* (ADS)
- Metadados de Arquivos
- Windows *User Access Logging* (UAL)
- Memória RAM

MÓDULO 7 – Evidências Relacionadas a Execução de Aplicações

- System Resource Usage Monitor (SRUM)
- Prefetch
- Superfetch
- Shimcache
- Amcache
- Histórico de Atividades (Windows Timeline)
- *Task Bar Feature Usage*
- *Background Activity Moderator* (BAM) e *Desktop Activity Moderator* (DAM)
- Jump Lists
- *Capability Access Manager*
- UserAssist
- Notificações do Windows (*Windows Push Notification*)
- *Program Compability Assistant* (PCA)
- Aplicativos do Windows Store
- Programas de Inicialização Automática
- Tarefas Agendadas
- Informações de Desinstalação
- MRU Últimas Visitas (Last Visited MRU)
- MRU Executar (Run Dialog MRU)
- *Multilingual User Interface Cache* (MUICache)
- *Resource Exhaustion Detection and Resolution* (RADAR)
- AppLocker
- Log de Eventos
- Memória RAM
- Aplicações Específicas

MÓDULO 6 – Evidências Relacionadas a Existência de Arquivos e Pastas

- Jump Lists
- MRU Últimas Visitas
- MRU Abrir/Salvar
- MRU Documentos Recentes
- MRU Histórico de Buscas
- MRU Arquivos Recentes do Office
- Arquivos de Atalhos – LNK
- Pasta Itens Recentes
- ShellBags
- MS *Word Reading Locations*
- Registros de Confiança do Office
- Log de Eventos do Office
- Internet Explorer (WebCacheV01.dat)
- Miniaturas
- *Windows Search Database*
- Caminhos Digitados pelo Usuário
- Lixeira (*Recycle Bin*)
- Histórico de Arquivos
- *Spooler* de Impressão
- *Volume Shadow Copies* (VSC)
- Sistema de Arquivos NTFS
- Memória RAM

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Comandos básicos do prompt (cmd.exe)
  - Uso básico do PowerShell
  - Configuração de rede
  - Gerenciamento de usuários locais
- Conhecimentos básicos do Registro do Windows
- Conhecimentos básicos de Sistemas de Arquivos do Windows
- Conhecimentos básicos de Rede de Computadores
- Conhecimentos básicos de Protocolos de Rede
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO-ALVO

- Especialistas em Segurança da Informação
- Peritos Digitais
- Peritos Criminais
- Analistas de Segurança da Informação
- Membros de CSIRT/ETIR/CTIR
- Analistas de SOC
- Membros de Blue Team
- Membros de Red Team
- Pentesters
- Profissionais de TI com interesse e afinidade na área 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 de 1 a 2 Máquinas Virtuais (VM) simultaneamente.
- Desejável 02 (dois) monitores para incremento na produtividade do curso
- Configuração mínima de 16GB de RAM, 80 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Software de Virtualização: VMWare, versão mais atualizada, de preferência *Workstation* (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS).

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do curso no formato PDF
- Máquina Virtual Windows com as ferramentas necessárias
- Gravações das sessões ao vivo
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Compreender os principais conceitos e fundamentos da perícia digital em ambientes Windows.
- Identificar e interpretar artefatos forenses essenciais para análise de execução de aplicações, histórico de arquivos e interações do usuário com o sistema.
- Analisar registros de eventos e logs do Windows para reconstrução de atividades e detecção de comportamentos suspeitos.
- Identificar e extrair evidências relacionadas ao uso de dispositivos USB, conexões de rede e execução de comandos remotos.
- Realizar a análise forense de arquivos de sistema, incluindo Volume Shadow Copies, Lixeira, Jump Lists e Shell Bags.
- Compreender e utilizar técnicas avançadas para identificação de ataques, fraudes e acessos não autorizados.
- Utilizar ferramentas especializadas para extração e análise de evidências digitais.
- Aplicar metodologias forenses para garantir a integridade das provas e elaborar relatórios técnicos detalhados.
- Avaliar e correlacionar informações extraídas do sistema para identificar indícios de comprometimento ou atividades maliciosas.

RODRIGO LANGE