ETHICAL HACKING REVERSE ENGINEERING MALWARE – EHREM

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 50hrs

Versão: 2.3 (2023)

Um analista de malware examina softwares mal-intencionados, com o objetivo principal de entender a natureza de sua ameaça e como mitigá-lo. Esta tarefa geralmente envolve a engenharia reversa do código malicioso e análise de como o programa interage com seu ambiente. Além disso o analista pode ser solicitado a documentar as capacidades de ataque do artefato, compreender suas características de propagação e criar regras ou definir assinaturas para detectar sua presença.

Empresas com produtos de segurança, indústria de antivírus ou prevenção de intrusão de rede estão contratando massivamente os profissionais e analistas de malware para desenvolver formas de conter atividades destrutivas de códigos maliciosos.

As grandes organizações e indústrias cujo foco não é a segurança também podem contratar analistas de malware em tempo integral para contribuir na proteção do seu ambiente contra ataques ou como colaborador no time de resposta a incidentes. As habilidades de análise de malware também são valorizadas por empresas que não podem justificar a contratação de pessoas em tempo integral para realizar esse trabalho, mas que desejam que seus administradores de segurança ou de TI possam ser capazes de examinar softwares mal-intencionados quando houver necessidade.

Esse tipo de conhecimento é útil para profissionais que trabalham com resposta a incidentes, investigação forense, segurança da informação e administração de sistemas.

O treinamento tem caráter prático onde aborda inicialmente a análise de malware em um nível introdutório, progredindo gradativamente para utilização de ferramentas e técnicas de maior complexidade. Durante as aulas o conteúdo será apresentado de forma prática e serão utilizados casos reais de análises de malware encontrados no cenário brasileiro e mundial.

MÓDULO 0x00

1. Introdução
    - Apresentação do instrutor
    - Evolução dos malwares
    - Definições e conceitos
    - Configuração do Laboratório e familiarização com as máquinas virtuais
    - Tipos de análise e metodologia
    - Fundamentos da análise de malware

MÓDULO 0x01

1. Interação com sites maliciosos
    - Anonimato para proteção do analista
    - Reputação de sites e domínios
2. Análise de tráfego malicioso
    - Identificação de ataques
    - Extração de artefatos
3. Análise de scripts maliciosos
    - Apresentação de ferramentas
    - Manipulação do código fonte para desofuscação dos scripts
    - Técnicas de análise para scripts do padrão VBS, JS, PS1
    - Debuggers
    - Interpretadores

MÓDULO 0x02

1. Análise de documentos maliciosos
    - Metodologia e objetivos específicos da análise de documentos
    - Análise de artefatos OLE (Object Linking Embedding)
    - Análise de artefatos baseados em Macros do pacote Office
    - Análise de artefatos do padrão PDF (Portable Document Format)

MÓDULO 0x03

1. Análise de artefatos do padrão PE (Portable Executable)
    - Análise preliminar
        a. Técnicas de OSINT aplicadas à análise de malware
        b. Emprego de Inteligência Artificial em Análise de Malware (ChatGPT)
    - Análise automatizada
        a. Sandboxes e ferramentas automatizadas. Vantagens, desvantagens e limitações.
    - Análise de propriedades estáticas
        a. Metadados, strings e estruturas de arquivos

    b. Subsídios para análises posteriores
- Análise de comportamento
    a. Apresentação de ferramentas
    b. Instrumentação da máquina virtual para identificação de comportamentos e interações do malware com o sistema operacional
- Análise de código
    a. Introdução ao assembly e arquitetura de computadores para análise de malware (x86 e x64)
    b. Calling conventions, registradores, sintaxe, endianess, controle de fluxo, estutura e interação com a pilha, ponteiros, labels, loops, chamadas API, chamadas a funções...
    c. Técnicas de decriptação de código fonte protegido
    d. Técnicas de injeção e execução de código malicioso em binários
    e. Apresentação de ferramentas utilizadas na análise de código (Debugger: x64dbg e Disassembler: IDA Pro)

2. Técnicas de injeção de código
    - DLL injection
    - DLL Side Loading
    - PE injection
    - Process Hollowing
3. Rootkits
    - Ring 3
        a. API Hook
        b. Técnicas de ocultação de arquivos
        c. Técnicas de ocultação de tráfego
        d. Técnicas de ocultação de informações do registro

MÓDULO 0x04

1. Análise de memória
    - Apresentação de técnicas e para análise e coleta de evidências em artefatos maliciosos que não tocam dispositivos de *storage* (*fileless*), só existem na memória RAM
    - Extração de processos, módulos e artefatos maliciosos da memória
    - Laboratório

MÓDULO 0x05

1. Relatórios e produtos da análise
    - Identificação de IOCs relevantes e adequados
    - Informações úteis que relatórios de análise de malware devem conter
    - Criação de regras para detecção de artefatos maliciosos em disco e em memória (Vacina)
    - Laboratório

MÓDULO 0x06

1. Técnicas anti-reverse
    - Detecção de ferramentas de análise
    - Detecção de ambiente virtualizado
    - Ofuscação de strings
    - Técnicas anti-debug
    - Técnicas anti-dump
    - Técnicas anti-disassembly

MÓDULO 0x07

1. Unpacking
    - Oligomorfismo, Polimorfismo e Metamorfismo
    - Packers e Crypters
    - Técnicas de EPO (Entry Point Obscuring)
    - Identificação do OEP (Original Entry Point)
    - Técnicas de decriptação manual de packers

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt, configuração de rede
- Conhecimentos básicos em Sistema Operacional Linux
  - Estrutura de diretórios, comandos básicos do shell, configuração de rede, verificação de serviços e processos
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, FTP, HTTP, HTTPS, SMB, SSH, DNS, ICMP
- Conhecimentos básicos de linguagem de programação de alto nível
- Controle de fluxo (while, for, repeat), variáveis, constantes e funções
- Familiaridade com ferramentas de Virtualização – VMWare, Virtual Box
- Experiência em programação e conhecimentos sobre linguagem de baixo nível são desejáveis, mas não são necessários para o acompanhamento do curso

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team / Blue Team
- Membros de CSIRT
- Analista de SOC
- Gestor de Segurança da Informação
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos precisam de um computador (Windows, Linux ou Mac OS), com a capacidade de executar de 02 Máquinas Virtuais (VM) simultaneamente
- Desejável 02 monitores para incremento na produtividade
- Configuração mínima de 8GB de RAM, 80 GB de espaço livre em disco
- Conexão rápida com a internet
- Software de Virtualização: VMWare, versão mais atualizada, de preferência Workstation (para hosts Windows ou Linux) ou Fusion (para host Mac OS), pode ser a versão trial. O VMWare Player também é capaz de executar as VMs do curso

MATERIAL RECEBIDO

- As Máquinas Virtuais com as aplicações utilizadas nos exercícios
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo, disponibilizadas no GoHacking Academy
- 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:

- Diferenciar as atividades de Engenharia reversa e Análise de malware
- Entender aspectos de criptografia e desofuscação aplicados à análise de malware
- Compreender modelos e frameworks como MAEC e MITRE ATT&CK
- Compreender e aplicar a fases da metodologia de análise de malware
- Interpretar mnemônicos assembly básicos de forma a identificar estruturas de controle de fluxo do programa analisado
- Utilizar ferramentas de anonimato para fins de proteção do analista
- Interagir de forma segura com sites maliciosos e manipular scripts de forma a desofuscar o código fonte
- Manipular e identificar documentos maliciosos
- Utilizar de ferramentas e *sandboxes* consagradas para executar a análise de malware
- Utilizar debugadores e descompiladores aplicados à análise de malware
- Entender a estrutura de um arquivo binário do windows *Portable executable* (PE)
- Utilizar ferramentas de extração de memória e analisar o resultado obtido
- Identificar mecanismos de persistência utilizados por malwares
- Identificar funcionalidades e técnicas utilizadas pelos autores de malwares
- Entender princípios de arquitetura e características de Sistemas de Comando e Controle (C2)
- Realizar a engenharia reversa do protocolo de comunicação do malware
- Identificar e sobrepujar técnicas de *anti-reverse* e utilizada por malwares
- Identificar malwares protegidos com *packers* e *crypters*
- Identificar e criar *Indicators of compromise* (IoC)
- Identificar informações importantes para compor um relatório de análise de malware
- Criar regras específicas para a de detecção de malwares com base na ferramenta YARA

RAFAEL SALEMA MARQUES