ETHICAL HACKING MALWARE DEVELOPMENT ESSENTIALS – EHMDE

DESCRIÇÃO

(Nível Intermediário/Avançado)

Carga Horária: 16hrs

Instrutor: Rafael Salema Marques

O treinamento tem o objetivo de proporcionar aos participantes um entendimento aprofundado sobre desenvolvimento de *malwares* customizados multiestágio e suas aplicações práticas, tendo como alvo, sistemas operacionais Windows modernos.

O instrutor guiará os alunos por meio de exemplos práticos com foco em estratégias eficazes e furtivas para proteger suas operações e infraestrutura ofensiva. Serão fornecidos códigos fonte que serão estudados e utilizados como exemplo, de forma que o aluno seja capaz de criar seus próprios servidores de Comando e Controle (C2), bem como implantes e artefatos necessários para suportar as atividades profissionais de Pentest e Red Team.

MÓDULO 0x00 – Preparação

1. Introdução
2. Ambiente de desenvolvimento
3. Malware multiestágio

MÓDULO 0x01 – Arquitetura do C2

1. Comunicação servidor x implante
2. Estrutura do servidor
3. Estrutura do implante
4. Estratégias de proteção da infraestrutura
    - Controle de frequência de requisições
    - Controle de origem e infecção
    - Redirecionador de tráfego (implante ⇔ C2)
5. Position Independent Code (PIC)
    - Offset x RVA x VA
    - Achando o endereço do ImageBase do kernel32.dll
    - Achando o endereço do GetProcAddress
    - Delta Trick
    - Chamadas de API no contexto do PIC
6. Ofuscação do Shellcode
7. Primeiro estágio
    - Beacon
    - Reconhecimento do alvo
    - Execução de Shellcode Remoto
8. Segundo Estágio
    - Download/Upload de arquivos
    - Execução de Comandos
9. Terceiro Estágio
    - AMSI Patch
    - Keylogger
    - Servidor Socks Reverso
    - Auto Remoção (Melt)
10. Técnicas de Persistência
    - DLL Side Loading

- COM Hijack
- Schedule Tasks
- Chaves de Registro AutoRun

11. Rootkit Ring3
    - Ocultação de arquivo e pastas
    - Ocultação de Processos

MÓDULO 0x02 – Proteção do Implante

1. (In)direct syscall
2. Decrypt condicional
3. Tipos de detecção e análises
4. Técnicas de ofuscação de código
5. Técnicas de anti-reverse
    - Anti-debugger
    - Anti-VM
    - Anti-disassembler
    - Anti-sandbox
    - Anti-ferramentas de análise

PRÉ-REQUISITOS

- Conhecimentos sólidos em Sistema Operacional Windows
- Conhecimentos sólidos em Sistema Operacional Linux
- Conhecimentos sólidos de Rede de Computadores e Serviços de Rede
- Experiência de programação em linguagens de alto nível (Python, Java, Go, correlatos)
- Noções de programação em linguagens de baixo nível (Assembly, C, C++)
- Familiaridade com Debuggers (IDA Pro, x64dbg, WinDBG)
- Conhecimentos básicos de chamadas de API no Windows
- Conhecimentos básicos do formato de arquivo PE (Portable Executable)
- Familiaridade com ferramentas de Virtualização – VMWare
-

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Analistas de Malwares
- Desenvolvedores de Exploits
- Pentesters
- Membros de Red Team
- 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 acesso de administrador e capacidade de executar de 02 Máquinas Virtuais (VM) simultaneamente
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco
- 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
- ATENÇÃO: NÃO TRABALHAR COM COMPUTADORES DA APPLE (MACBOOK) COM PROCESSADORES ARM M1/M2

MATERIAL RECEBIDO

- Acesso ao portal do aluno, o GoHacking Academy
- As Máquinas Virtuais com as aplicações utilizadas nos exercícios
- Apostila do Curso no formato PDF
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)
- Códigos-fonte funcionais compatíveis com a versão mais moderna do Windows que serão usados no treinamento

CAPACIDADES ALCANÇADAS

No final do curso, espera-se que o aluno estará apto a:

- Entender o processo de desenvolvimento de código malicioso (*malware*) para o Sistema Operacional Windows
- Entender o funcionamento das APIs do Sistema Operacional Windows
- Compreender as etapas de construção de *malware* para atividades profissionais de Segurança Ofensiva
- Construir *malwares* em apoio a Operações de Red Team
- Desenvolver *malwares* customizados multiestágios
- Ofuscar código malicioso
- Entender as principais técnicas de *bypass* de controles de segurança utilizadas por *malwares*
- Criar mecanismos de Comando e Controle (C2)

RAFAEL SALEMA MARQUES