ETHICAL HACKING MODERN WEB EXPLOITATION (EHMWX)

DESCRIÇÃO

(Nível Avançado)

Carga Horária: 40hrs

O curso Ethical Hacking Modern Web Exploitation (**EHMWX**) apresenta técnicas ofensivas de exploração de sistemas Web com foco em casos de sucesso recentes, ou seja, as classes de vulnerabilidades que estão sendo exploradas atualmente.

A relevância dos sistemas web é cada vez mais crescente, o que implica em uma preocupação maior com a segurança desses sistemas. Pois, além de armazenarem e processarem dados vitais às empresas, eles também são comumente usados como porta de entrada de ataques cibernéticos para um comprometimento total da infraestrutura de uma organização. Desta forma, o curso se concentra no aspecto da exploração no lado servidor dos sistemas, o que, no geral, resulta em uma atividade de elevado impacto.

O curso pretende abordar diversas tecnologias e linguagens de desenvolvimento de sistemas web, tais como: Java, NodeJS, PHP e Python. Dentre os diversos tipos de vulnerabilidades, serão trabalhados: Desserialização em PHP e Java, *Prototype Pollution* (NodeJS), *Server Side Request Forgery, Template Injection* (Python, PHP e Java), HTTP *Request Smuggling*, GraphQL e outros tópicos que, apesar de não serem tão recentes, ainda são atuais e relevantes devido a novas descobertas.

Vale ressaltar que o curso não trata de temas básicos sobre exploração de sistemas web e, por esse motivo, ter um conhecimento sólido das vulnerabilidades básicas e as respectivas técnicas de exploração é altamente recomendável.

Por fim, a metodologia adotada compreenderá a explicação teórica das vulnerabilidades, com debate sobre casos de explorações reais e práticas em ambientes simulados. Ainda, sempre que adequado, será mostrado como é possível descobrir as referidas vulnerabilidades, sob a ótica de um pesquisador.

MÓDULO 1

1. Apresentação do Curso
   - Ambiente de aprendizado
   - Desafios

2. Server Side Request Forgery (SSRF)
   - Impactos da falha
   - Relevâncias em ambiente de Cloud
   - Protocol Smuggling
   - Caso real de exploração de SSRF e Bypass
   - Falhas recentes de SSRF. Microsoft Exchange.
   - DNS Rebinding

3. XML eXternal Entity (XXE)
   - Método por DTD externo
   - Método baseado em erro
   - Método por DTD interno
   - Falhas recentes de XXE

MÓDULO 2

1. Visão geral sobre Template e Expression Language Injection
   - Histórico de vulnerabilidades em OGNL
   - Confluence
   - Vulnerabilidades no SpEL
   - Primefaces
   - Velocity
   - Jira
   - Casos reais de exploração em Template Injection
   - Novas vulnerabilidades (vCenter)

2. Exploração de Templates em Outras Linguagens
   - PHP - Twig

MÓDULO 3

1. Visão Geral sobre Desserialização

2. Desserialização em Java
   - Entendendo o processo de desserialização nativo do Java
   - Estrutura do objeto serializado - SerializationDumper
   - Como funcionam os gadgets
   - Principais gadgets
   - YSoSerial

- Falhas recentes de desserialização em Java
- Caso real de exploração

3. Desserialização em PHP
   - Entendendo o processo de desserialização em PHP
   - Estrutura do objeto serializado
   - Gadgets em PHP
   - Reproduzindo a análise para busca de um gadget
   - Desserialização com PHAR
   - Falhas recentes de desserialização em PHP

4. Desserialização em outras linguagens
   - Python Pickle
   - NodeJS

MÓDULO 4

1. Prototype Pollution
   - Entendendo a ideia de classes e objetos em JavaScript
   - Noção de Prototype
   - Poluição do Prototype
   - Casos reais de exploração
   - Falhas e pesquisas recentes

MÓDULO 5

1. HTTP Request Smuggling
   - Entendendo a vulnerabilidade
   - Casos reais de exploração
   - Novo vetor com HTTP/2

2. GraphQL
   - Conhecendo GraphQL
   - Introspection
   - Formas de exploração de GraphQL
   - Casos reais de exploração

3. Tópicos Gerais
   - Path Traversal ainda é atual?
   - Ferramentas que auxiliam
   - Fontes de estudo para tópicos atuais

PRÉ-REQUISITOS

- Familiaridade com protocolos tradicionais de rede (HTTP, HTTPS, DNS, SSL/TLS)
- Conhecimento básico de linguagens de programação comumente utilizadas em aplicação web (PHP, Java, JavaScript, Python)
- Familiaridade com o Sistema Operacional Linux e comandos do shell
- Habilidade para escrever scripts simples em Python, Perl, PHP e Bash
- Familiaridade com web proxies, tais como Burp Suite e ferramentas similares
- Conhecimentos básicos em exploração de Sistemas Web
- Familiaridade com conceitos e metodologias de Pentest em Aplicações Web
- Entendimento e familiaridade com as falhas descritas no OWASP Top 10 mais recente
- Familiaridade com softwares de Virtualização, tais como VMWare
- Capacidade de manipular e configurar Máquinas Virtuais
- Interesse em entender as vulnerabilidades de impacto crítico que afetam o backend de aplicações web

PÚBLICO ALVO

- Analista de Segurança da Informação
- Especialista em Segurança da Informação
- *Pentesters*
- *Bug Hunters*
- Membros de *Red Team*
- Membros de *Blue Team*
- Membros de CSIRT
- Analista de SOC
- Pesquisadores da área de Segurança da Informação
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Entusiastas de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho/laptops (Windows, Linux ou Mac OS), com a capacidade de executar até 02 (duas) Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco
- Caso possível, dispor de 02 (dois) monitores para incremento na produtividade.
- Software de Virtualização: recomendável a utilização do VMWare, versão mais atualizada, de preferência *Workstation* (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS). É possível utilizar a versão de avaliação (*trial*). O VMWare *Player* também é capaz de executar VMs apesar de não possuir a capacidade de realizar *snapshots*, que é importante, mas não imprescindível para o curso.

MATERIAL RECEBIDO

- Slides do Treinamento no formato PDF
- Gravações das sessões ao vivo, disponibilizadas no GoHacking Academy
- Certificado de Conclusão do Curso (com a carga horária e ementa)
- Acesso aos laboratórios online, no GoHacking Academy, pelo período mínimo de 04 (quatro) meses.

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Entender técnicas atuais de exploração de sistemas web
- Realizar análise avançada de códigos de aplicações web para encontrar falhas
- Utilizar formas criativas e inovadores para encontrar e explorar falhas em aplicações web
- Descobrir e explorar vulnerabilidades do tipo SSRF
- Descobrir e explorar vulnerabilidades do tipo XXE
- Descobrir e explorar vulnerabilidades de desserialização em sistemas Java
- Descobrir e explorar vulnerabilidades de desserialização em sistemas PHP
- Descobrir e explorar vulnerabilidades do tipo *Prototype Pollution* para alcançar RCE em sistemas NodeJS
- Descobrir e explorar vulnerabilidades de *Expression Language Injection*
- Entender e explorar HTTP *Request Smuggling*
- Entender e explorar as principais falhas em APIs Web
- Entender e explorar GraphQL API

MANOEL TEIXEIRA DE ABREU NETTO