ETHICAL HACKING PYTHON
(EHPY)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

Instrutor: Ulisses Alves

O curso Ethical Hacking Python (EHPY) aborda a utilização da linguagem Python 3 em Segurança Ofensiva (Pentest, Red Team), trabalhando informações essenciais para que o aluno desenvolva suas próprias ferramentas de segurança.

O curso é voltado a profissionais da área de Segurança da Informação, da área de TI em geral, pessoas que tenham interesse em aprender Python aplicado a Segurança Cibernética, bem como aqueles que desejam aprimorar seus conhecimentos na linguagem com fins a terem a base necessária para construir seus próprios programas.

Com caráter prático, o curso oferece desafios relacionados às necessidades de um profissional de Segurança da Informação, com foco em atividades ofensivas. O aluno poderá exercitar o pensamento lógico e criativo ao ser estimulado a solucionar problemas de automação durante várias das fases de um Pentest, ou de uma operação de Red Team, além de solidificar importantes fundamentos de programação e de redes, que são sempre exigidos na área de segurança.

Este curso abordará conceitos de programação, redes, os principais módulos de Python aplicados em Segurança da Informação, automatização de tarefas e técnicas de construção de ferramentas que podem se tornar essenciais no trabalho do profissional de segurança. Os conhecimentos passados têm nível básico a intermediário, podendo variar de acordo com a experiência profissional de cada aluno.

Por fim, o curso contará com uma plataforma especial chamada PyLab, que testará os conhecimentos de todos os alunos, não importando o nível de habilidade em programação que possuam. São mais de 50 desafios, com dificuldades gradativas e com um sistema de pontuação, que servirão como uma forma prática de o aluno aplicar os conhecimentos adquiridos no curso, elevando o nível de compreensão da área. O objetivo principal do PyLab, além de incentivar o aluno a crescer, será de solidificar fundamentos. Portanto, mesmo que alguns dos desafios possam parecer fáceis, eles têm uma base que fornecem mais bagagem para o entendimento do assunto principal do curso: aplicar a linguagem Python 3 ao ambiente de Segurança Ofensiva.

MÓDULO 1 – Python 101

1. Introdução à linguagem
2. Principais diferenças entre Python 2 e Python 3
3. Principais características do Python
    - Quase tudo é objeto
    - Indentação
    - Tipagem fraca/forte
4. Python scripting
    - Python interactive shell
    - Scripts in Python
    - Uso de módulos e pacotes
    - if __name__ == '__main__':
5. Tipos de dados: caraterísticas e operações
    - String
    - Integer
    - Float
    - List
    - Tuple
    - Dictionary - Set
    - Byte
    - Boolean
6. Controles de fluxo: características e cenários de uso – for
    - while
    - if
    - break
    - continue
7. Funções
    - Definição de função
    - Parâmetro
    - Funções como parâmetro
    - Saídas de funções
    - Funções lambda
    - Organização básica de código utilizando funções

8. Tratamento de exceções
    - try: except
9. Utilização e gerenciamento de argumentos de linha de comando
    - Módulo argparse
10. Módulos importantes
    - socket
    - os
    - random
    - json
    - base64
    - requests
    - threading
    - beautifulsoup4
    - subprocess
    - pyperclip
    - time
    - Pillow

MÓDULO 2 – Information Gathering

1. DNS
    - Transferências de zonas
    - Resolução de nomes
2. Web
    - Criação de wordlists a partir de um website: introdução ao beautifullsoup
3. Introdução a expressões regulares
4. Extraindo informações importantes de arquivos de log

MÓDULO 3 – Networking

1. Revisão do conceito cliente/servidor
2. Bind and reverse Shells
3. Reverse Shell via HTTP(S)
4. Captura de pacotes de rede com o módulo Scapy
5. Exfiltração de dados via ICMP com o módulo Scapy
    - Introdução à aritmética modular
    - Operação XOR
6. Scanner de portas com o módulo socket

MÓDULO 4 – GIT

1. Introdução ao git
2. Buscador de segredos em repositórios git

MÓDULO 5 – GPT: Assistentes e Agents

1. O que são GPTs?
2. OpenAI
    - Introdução à API de assistentes
    - Introdução a Agentes (OpenAI function calls)
        - Assistente de terminal
        - Detector de e-mails spam/maliciosos com alerta via Slack e *blocklist* do remetente

PRÉ-REQUISITOS

- Conhecimentos básicos de Sistemas Operacionais Windows e Linux
  - Estrutura de diretórios, linha de comando, configuração de rede
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, HTTP, HTTPS, FTP, SMB, SSH, DNS, ICMP
- Conhecimentos básicos de programação (não é necessário ser programador, apenas ter conhecimentos mínimos sobre algoritmos e lógica de programação)
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO-ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team / Blue Team
- Analista de SOC
- 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 02 (duas) Máquinas Virtuais (VM) simultaneamente.
- Desejável 02 (dois) monitores para incremento na produtividade do curso.
- Configuração mínima de 8GB de RAM, 60 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 Pro *Workstation* (para hosts Windows ou Linux) ou Pro *Fusion* (para host Mac OS).
- Python versão 3.11 ou superior (é altamente recomendável que seja a versão mais atualizada)
- Um editor de texto/código de sua preferência (Sublime Text, VS Code, vim, nano, notepad, micro, outros).

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do curso no formato PDF.
- Todos os códigos produzidos.
- Uma máquina virtual Linux, que poderá servir como o ambiente do aluno
- A máquina virtual Linux será um ambiente completo montado para o aluno não se preocupar em preparar seu ambiente próprio. Todos os pré-requisitos já estarão devidamente instalados e configurados e ela também possuirá diversas opções de editores de código para serem utilizadas. Apesar de não ser uma obrigatoriedade, é altamente recomendado que ela seja utilizada, pois seu uso vai agilizar o início das atividades práticas do curso.
- 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:

- Reconhecer as características principais da linguagem Python 3
- Utilizar a linguagem, suas estruturas de dados e sintaxe na implementação de ferramentas de segurança ofensiva
- Utilizar Python para criar wordlists a partir de palavras de sites
- Utilizar Python para automatizar tentativas de transferência de zona
- Utilizar Python para automatizar a resolução de nomes
- Aplicar expressões regulares em ferramentas feitas em Python 3
- Implementar um shell reverso via protocolo HTTP e HTTPS
- Capturar pacotes de rede usando Python 3
- Exfiltrar dados dentro de pacotes ICMP utilizando Python 3
- Implementar scanner de portas simples
- Implementar um buscador de segredos em repositórios git
- Implementar assistentes GPT da OpenAI
- Implementar agentes GPT autônomos da OpenAI

INSTRUTOR: ULISSES ALVES