Segurança da Informação com Python

Introdução aos conceitos de Segurança da Informação e Ping

Por que Python?

* Linguagem Simplista - Fácil de Programar
* Menos linhas de código
* Orientada a Objetos
* API’s e Bibliotecas Prontas para Redes, Web, etc
* Multiplataforma
* Além da facilidade de iniciação no Python e da pequena curva de aprendizagem de qualquer linguagem para Python, a mesma é amplamente utilizada na segurança da informação facilitando desde desenvolvimentos de scripts de automação até o desenvolvimento de ferramentas e projetos inteiros utilizando a linguagem e suas facilidades

O que é segurança da informação?

* Dado: pode ser uma representação simbólica, numérica ou textual qualquer
* Informação: é o conjunto ou a junção de dados que fazem um contexto ou sentido
* Segurança da Informação: área que tem como objetivo assegurar que todos os dados de uma ou mais informações estejam sempre confidenciais, íntegros e disponíveis em qualquer meio de comunicação
* Por que Segurança da Informação?
* Pirâmide de Maslow
  + Realização
  + Estima
  + Sociais
  + Segurança
  + Fisiológicas
* Princípios da Segurança da Informação
  + Integridade: visa proteger a informação de alterações indevidas
  + Confidencialidade: visa manter um informação confidencial
  + Disponibilidade: visa garantir que um recurso e/ou informação esteja disponível
  + Identificação: visa identificar uma entidade
  + Autenticação: visa verificar a entidade e suas credenciais
  + Autorização: visa autorizar a entidade dentro de um sistema
  + Não repúdio: visa evitar que uma entidade negue suas ações em um sistema

O que é Ping?

* ICMP (internet Control Message Protocol), é um protocolo integrante do protocolo IP utilizado para fornecer relatórios de erros à fonte original
* Ping: é uma ferramenta que usa protocolo ICMP para testar a conectividade entre nós. É um comando disponível praticamente em todos os sistemas operacionais que consiste no envio de pacotes para o equipamento de destino e na “escuta” das respostas.
* Biblioteca os: este módulo fornece uma maneira simples de usar funcionalidades que são dependentes de sistema operacional
* Biblioteca time: este módulo fornece várias funções relacionadas ao tempo, como por exemplo tempo de execução

Introdução a Socket e cliente TCP/UDP e Server

Biblioteca Socket

* Esta biblioteca fornece acesso de baixo nível à interface de rede
* O S.O fornece a API socket que relaciona o programa com a rede
* TCP (Transmission Control Protocol): Protocolo de Controle de Transmissão é um dos protocolos de comunicação, que dão suporte a rede global Internet, verificando se os dados são enviados na sequência correta e sem erros
* UDP (User Datagram Protocol): Protocolo simples da camada de transporte que permite que a aplicação envie um datagrama dentro de um pacote IPv4 ou IPv6 a um destino, porém sem qualquer tipo de garantia que o pacote chegue corretamente

Desenvolvimento de um cliente TCP

Desenvolvimento de um cliente UDP

Desenvolvimento de um Server

Desenvolvimento de Ferramentas - Parte 1

O que é a biblioteca Random, um hash e um Multithreading

* Biblioteca Random: implementa geradores de números pseudo aleatórios para várias distribuições. Esta biblioteca será utilizada no gerador de senhas para randomizar letras e números e a cada execução do programa gerar uma nova senha aleatória
* Hash é como se fosse um identificador único gerado através de um algoritmo que vai analisar byte a byte de determinado dados para gerar de forma única, um determinado código que só aquele arquivo terá. Se neste mesmo arquivo um único bit for alterado o hash gerado será diferente
* <https://md5decrypt.net/en/>
* Hashlib: biblioteca que implementa uma interface comum para muitos algoritmos de hash seguro como SHA1, SHA256, MD5 entre outros. Usaremos esta biblioteca em nosso comparador de hashes para comparar dois arquivos
* Multithreading: thread é o processo e no ambiente multithread, cada processo pode responder a várias solicitações concorrentemente ou mesmo simultaneamente.
* Threading: esta biblioteca constrói interfaces de alto nível para processamento usando o módulo Thread, de mais baixo nível, ou seja relação direta com o processador
* ipaddress: esta biblioteca tem a capacidade de criar e manipular endereços IP do tipo IPv4, IPv6 e até redes inteiras.

Desenvolvendo um gerador de senhas

* random: Implementa geradores de números letras e símbolos aleatórios para várias situações
* string: implementa operações comuns para strings

Desenvolvendo um comparador de Hashes

* Hashlib: implementa uma interface comum para muitos algoritmos de hash seguro como SHA1, SHA256, MD5 entre outros
* <https://docs.python.org/>
* Trabalhando com Threads e IP’s

Desenvolvimento de ferramentas - Parte 2

* Objetivos da aula
* Desenvolvimento um gerador de Hashes
  + Hashlib: implementa uma interface comum para muitos algoritmos de hash seguro como SHA1, SHA256, MD5 entre outros
* Desenvolvendo um gerador de Wordlists
  + Wordlists são arquivos contendo uma palavra por linha. São utilizados em ataques de força bruta como quebra de autenticação, pode ser usada para testar a autenticação e confidencialidade de um sistema
  + Itertools: esta biblioteca fornece condições para iterações como permutação e combinação
* Desenvolvendo um Web Scraping
  + Web scraper é uma ferramenta de coleta de dados web, uma forma de mineração que permite a extração de dados de sites da web convertendo-os em informação estruturada para posterior análise
  + BeautifulSoup: pe uma biblioteca de extração de dados de arquivos HTML e XML
  + requests: permite que você envie solicitações HTTP em Python
* Desenvolvendo um Web Crawler
  + Web Crawler é uma ferramenta usada para encontrar, ler e indexar páginas de um site. É como um robô que captura informações de cada um dos links que encontra pela frente, cadastra e compreende o que é mais relevante. (palavras-chave)
  + Muito utilizado em levantamento de informações em um processo de Pentest
  + BeautifulSoup: é uma biblioteca de extração de dados de arquivos HTML e XML.
  + operator: exporta um conjunto de funções eficientes correspondentes aos operadores intrínsecos do Python como: +=\*/ not and
  + collections: nos ajuda a preencher e manipular eficientemente as estruturas de dados como tuplas, dicionários e listas

Desenvolvimento de ferramentas - Parte 3

* Objetivos da aula
* Desenvolvendo um verificador de telefone
  + Biblioteca phone numbers: fornece vários recursos, como informações básicas de um número de telefone, validação de um número de telefone, etc.
* Desenvolvendo um ocultador de arquivos
  + biblioteca ctypes: fornece tipos de dados compatíveis com C e permite funções de chamada em DLL ou bibliotecas compartilhadas.
* Desenvolvendo um verificador de IP externo
  + Biblioteca re: permite operações com expressões regulares
  + Biblioteca json: fornece operação de codificação e decodificação JSON
  + urllib.request import urlopen: funções e classes que ajudam a abrir URLs
  + <http://ipinfo.io/json>
* Ferramenta Gráfica para abrir o navegador
  + Biblioteca webbrowser - fornece uma interface de alto nível para permitir a exibição de documentos Web aos usuários.
  + Biblioteca tkinter: fornece interface padrão do Python para o kit de ferramentas gráficas Tk