Instituto Politécnico de Beja

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Linguagem de Programação Dinâmica

Projeto Individual de Python

Relatório

Elaborado por:

Horlando Marciano Correia

Nº 22272

Beja

2024

Índice

Introdução

O presente relatório faz parte de uma das componentes de avaliação do projeto de Python da disciplina de Linguagens de Programação Dinâmicas.

Este relatório é um manual técnico laboratorial que visa apresentar as técnicas e tecnologias utilizada para desenvolver está aplicação e serve também para orientar os usuários. Será abordada ao longo dos passos deste documento a linguagem de programação utilizada, as livrarias da linguagem, e diversos tipos de implementação de cifra as funcionalidades essências e suas formas de implementação. E serviço de troca de mensagem entre o cliente e servidor nas suas respetivas e as varreduras das portas do IP

Python 3

Existe duas grandes versões do Python (versão 3.12 e versão 3.11). A duas versões continuam até hoje a ser utilizadas por empresas e organizações. Que foi lançado em 2 de outubro de 2023.

A linguagem de programação dinâmica que foi utilizado para desenvolver desta aplicação foi o Python na sua versão 3, em específico.

Python 3.12 é uma versão mais recente da linguagem de programação Python, que foi lançada em 2 de Outubro de 2023. Esta versão foi lançada principalmente para corrigir problemas que existem em Python 2 e 3. A natureza destas alterações é tal que Python 3 era incompatível com Python 2.

Python 3.12 é a versão estável mais recente da linguagem de programação Python, com uma combinação de alterações na linguagem e na biblioteca padrão. As alterações da biblioteca se concentram na limpeza de APIs descontinuadas, usabilidade e correção. É importante notar que o pacote distutils foi removido da biblioteca padrão. O suporte ao sistema de arquivos em os e pathlib teve uma série de melhorias e vários módulos têm melhor desempenho

Algumas características de Python 3 foram retro portadas para as versões Python 2.x para facilitar o processo de migração em Python 3. Como resultado, para qualquer organização que estava a utilizar a versão Python 2.x, a migração do seu projeto para a versão 3.x necessitava de muitas alterações. Estas mudanças não só estão relacionadas com projetos e aplicações, mas também com todas as bibliotecas que fazem parte do ecossistema Python.

Diferencias essenciais entre Python 3 e Python 2

A sintaxe Python 3 é mais simples e de fácil compreensão enquanto a sintaxe Python 2 é comparativamente difícil de compreender.

Python 3 valor de variáveis nunca muda enquanto em Python 2 valor da variável global será alterado enquanto a utiliza dentro do *for-loop*.

As exceções em Python 3 devem ser incluídas entre parênteses enquanto as exceções em Python 2 devem ser incluídas em anotações.

As regras de comparação de ordenação de Python 3 são simplificadas enquanto as regras de comparação de ordenação de Python 2 são complexas.

Python 3 oferece a função *Range()* para realizar iterações enquanto, em Python 2, o *xrange()* é utilizado para iterações.

Porque utilizar Python 3?

Python 3 apoia técnicas modernas como a IA, *machine learning*[1], e a ciência dos dados

Python 3 é apoiado por uma grande comunidade de desenvolvedores Python. Obter apoio é fácil.

É mais fácil de aprender a linguagem Python em comparação com as versões anteriores.

- Oferece um poderoso conjunto de ferramentas e bibliotecas
- Misturável com outras línguas

Biblioteca Python 3 Utilizadas

Uma biblioteca Python é uma coleção de módulos relacionados. Contém pacotes de código que podem ser usados repetidamente em diferentes programas. Torna a Programação Python mais simples e conveniente para o programador. Como não precisamos de escrever o mesmo código uma e outra vez para programas diferentes, (Manchanda, 2021)

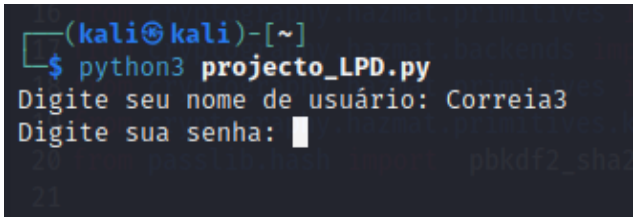
Funcionalidade da aplicação

Login

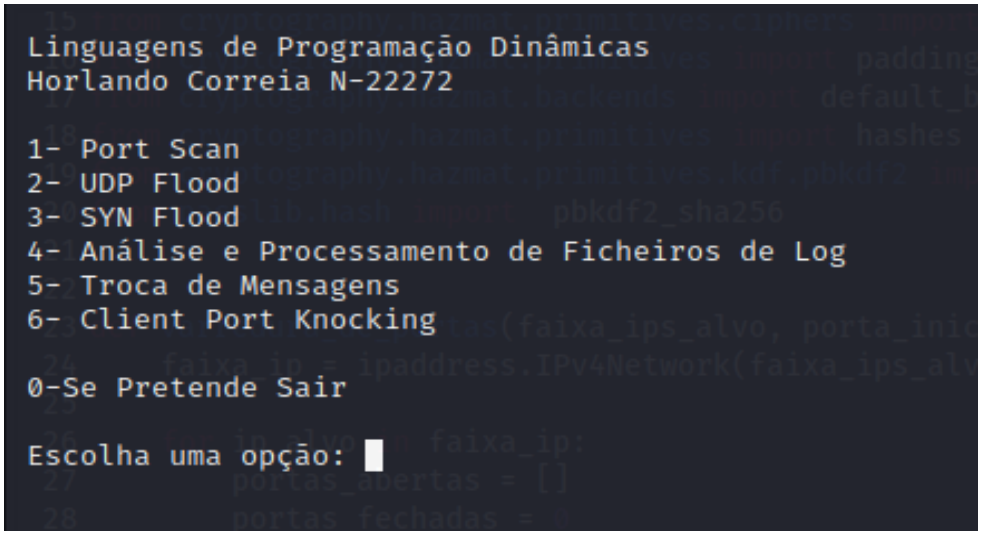
Para aceder a aplicação o utilizador deve efetuar primeiro o login.

O utilizador entra com o username e a password.

Para efetuar a autenticação do utilizador, ou seja, verificar se as credencias utilizadas são validas par ter acesso a opções da aplicação:



Ao entrar no programa o menu abrirá automaticamente toda as opções disponíveis.



Escolha as opções correspondentes a funcionalidade desejada e pressione o ENTER e siga toda a instrução especifica de cada funcionalidade.

Para sair o programa exibira uma opção última opção indicada por (0) é sair, ao ser acionada o utilizador sai da aplicação, ou seja, termina a sessão.

- O utilizador introduz a credencias
- Um *digest* da password é gerado da password utilizando a função hash.
- É feito uma consulta na base de dados, procurando um utilizador com tem o *username* introduzido e o mesmo *digest* da password gerado no momento. A implementação da autenticação é feito no Python através de

um método criado de nome autenticacao(), ela recebe por parâmetro o *username* e a password e returna 1 ou 0.

Password Hash
A password é gerada um *digest* através da função hash e armazenada no passe de dados.

Geração de par de chaves
No ato do registo é gerada um par de chaves (publica e privada). Foi utilizada uma cifra assimétrica em que o nome é RSA.
Chave publica
A chave publica é guarda no servidor na diretoria aplicacao/chavespublicas

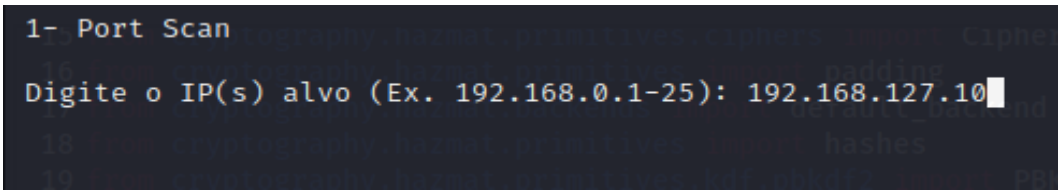
Chave privada

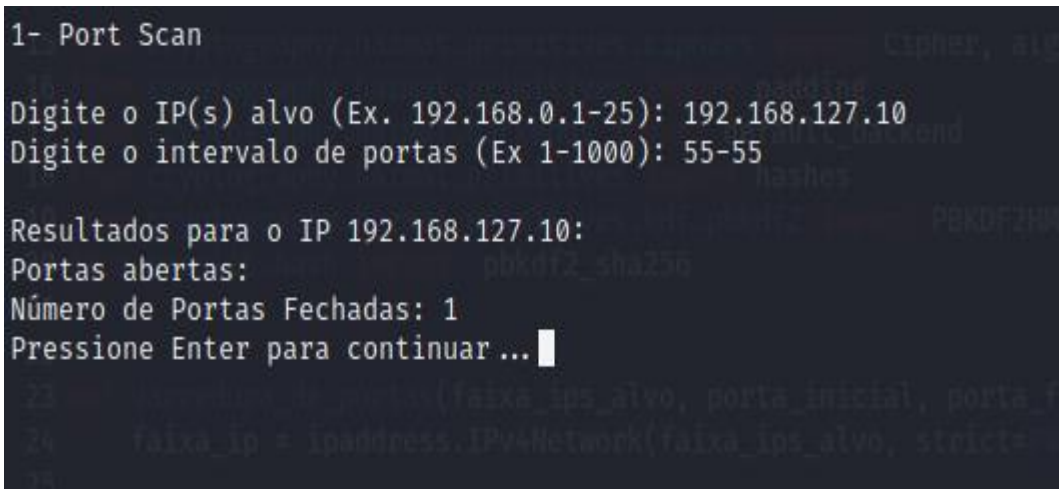
A chave privada é guarda numa localização definida pelo utilizador.

PortScanner

Esta funcionalidade permite varrer um IP e seus portos.

Para sua implementação foi utilizado *socket* e colocado os portos num ciclo em que o intervalo é definido pelo utilizador.



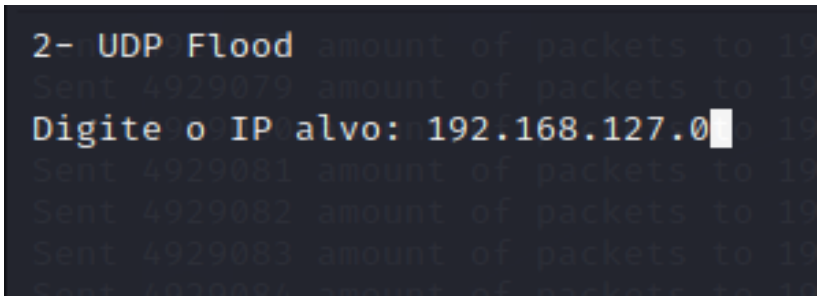


Cifragem das mensagens trocadas
Todas as mensagens trocadas são cifradas e armazenadas na BD. Por ser uma cifra assimétrica cada mensagem é cifrada com a chave publica do utilizador e decifrada com a chave privada.

A ilustração seguinte ilustra as mensagens cifradas na base de dados.

UDP Flood

UDP ao IP alvo especificado (`ip_alvo`). O método `sendto` é usado para enviar dados por meio de um socket UDP. A variável `bytes_to_send` contém os dados que estão sendo enviados para determinado IP alvo.



```
Sent 578253 amount of packets to 192.168.127.0
Sent 578254 amount of packets to 192.168.127.0
Sent 578255 amount of packets to 192.168.127.0
Sent 578256 amount of packets to 192.168.127.0
Sent 578257 amount of packets to 192.168.127.0
Sent 578258 amount of packets to 192.168.127.0
Sent 578259 amount of packets to 192.168.127.0
Sent 578260 amount of packets to 192.168.127.0
Sent 578261 amount of packets to 192.168.127.0
Sent 578262 amount of packets to 192.168.127.0
Sent 578263 amount of packets to 192.168.127.0
Sent 578264 amount of packets to 192.168.127.0
Sent 578265 amount of packets to 192.168.127.0
Sent 578266 amount of packets to 192.168.127.0
```

SYN Flood

Tem como por objetivo realizar um ataque de inundação SYN Flood para testar a resiliência de um servidor
Instrução: Selecionar a opção 3 e digite o IP alvo conforme indicação

```
3- SYN Flood

Digite o IP alvo:
```

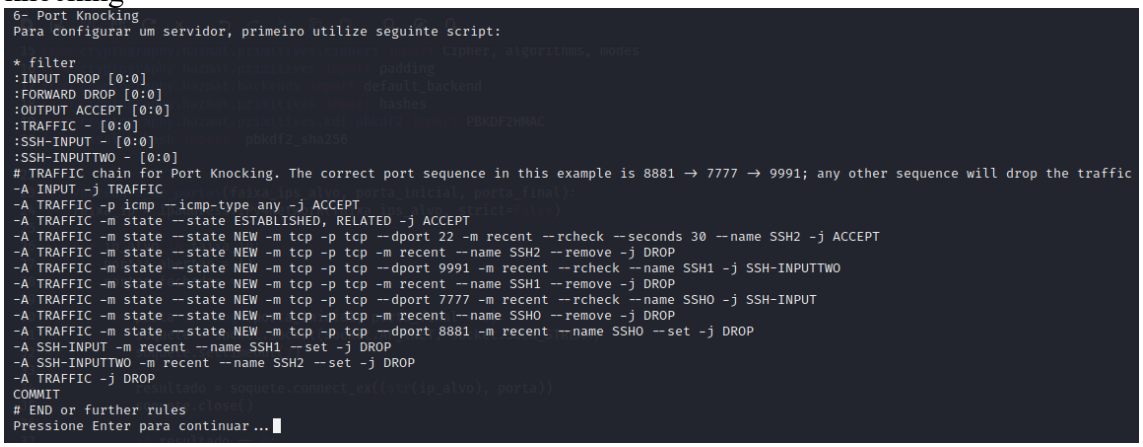
Troca de Mensagens

A troca de mensagem é gerida através de cliente e servidor onde a mensagem é criptografada ponto a ponto
Instrução: é selecionar a opção 5 e siga as indicações para configurar o servidor ou o cliente.

```
Digite 1 para Servidor e 2 para Cliente:
```

Client Port Knocking

É cessar os serviços ocultos por meio de um sequencia especifica de portas
Instrução: é escolher opção 6 e digite endereço de IP do servidor alvo e as portas de port knocking



Controle de versões

O controle de versões utilizado no desenvolvimento deste projeto foi o GitHub com o repositório.

Bibliografia

Learning Python [Livro] / autor Romano Fabrizio. - 2018.
Python 3 [Online] / autor Campbell Steve // guru99. - 2024. - 27 de 02 de 2024. - https://www.guru99.com/python-2-vs-python-3.html.

Python Penetration Testing [Livro] / autor Mohit. - 2015.
Libraries in Python [Online] / autor Manchanda Parth // geeksforgeek. - 2024. - 27 de 02 de 2024. - https://www.geeksforgeeks.org/libraries-in-python/. matplotlib [Online] // matplotlib. - 2024. - https://matplotlib.org/.