Instituto Politécnico de Beja

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Linguagem de Programação Dinâmica

Projeto Individual de Python

Manual do utilizador

Elaborado por:

Horlando Marciano Correia

Nº 22272

Beja

2024

Índice

Introdução

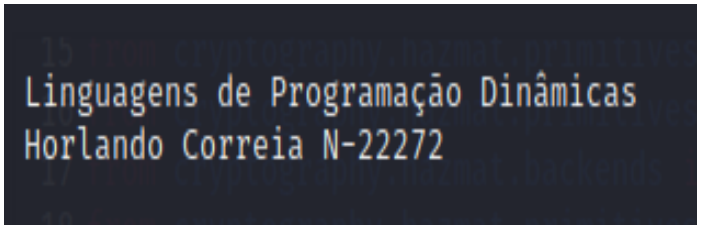
O presente documento faz parte de uma das componentes de avaliação do projeto de Python da disciplina de Linguagens de Programação Dinâmica.
O projeto em si tem por objetivo a aplicação na perspetiva do utilizador, ou seja, pretende se que o utilizador tenha conhecimento de como funciona a aplicação no seu todo, sem ter de se preocupar com questões técnicas desconhecida porque esta especificado passo a passo neste documento.

Inicial a aplicação

Para iniciar a aplicação é necessário executar o ficheiro **python3 projecto_LPD.py** no terminal através do comando **python3 projecto_LPD.py**

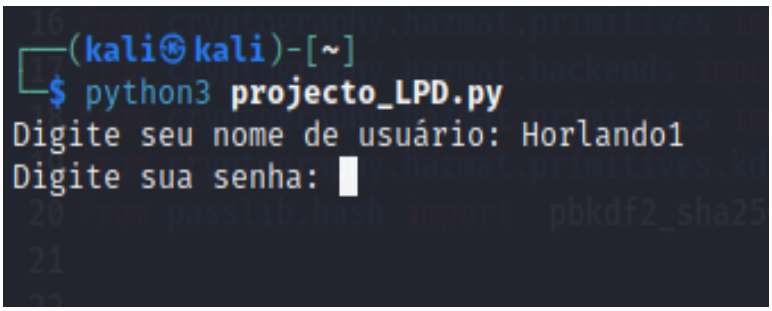
Banner da aplicação

Ao executar o comando para iniciara o programa aparece um banner com a informação do aluno da disciplina



Login

Para poder utilizar a aplicação o utilizador deverá estar registado. Se não possui conta criada deverá proceder ao registo da mesma.

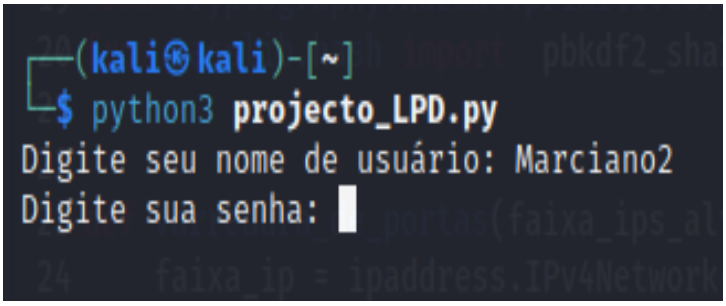


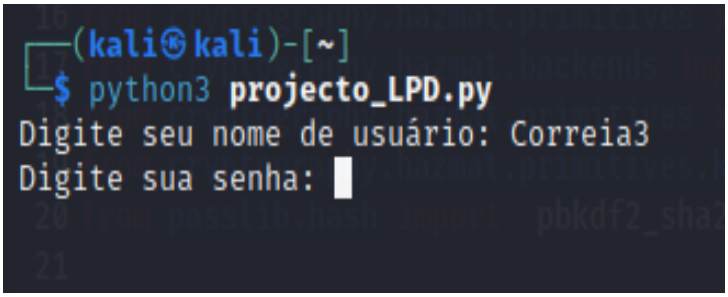
Para entrar na aplicação é necessário introduzir as credenciais de acesso:

- Nome Utilizador
- Password

Registar

Esta tela permite o registo os utilizadores existentes que possui uma conta para que possa aceder a aplicação.



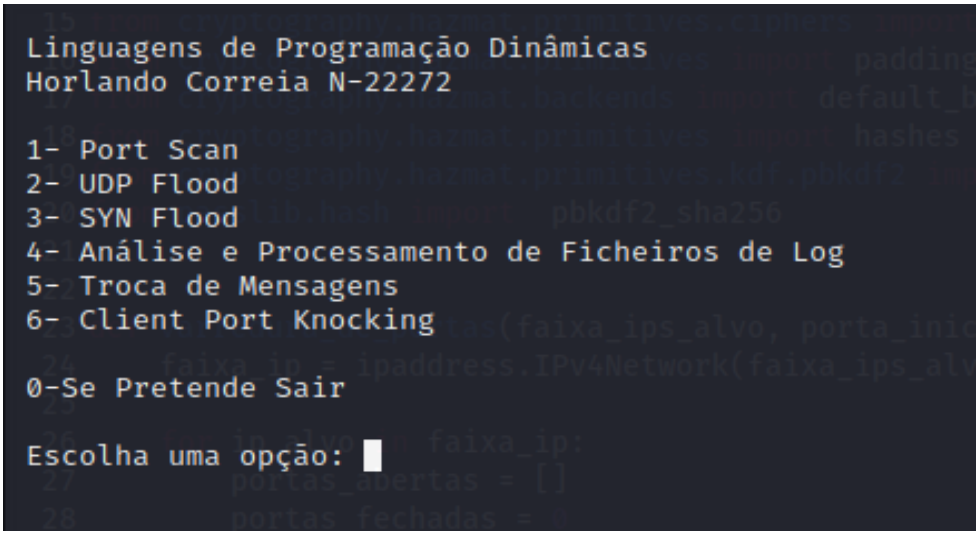


Os campos que devem constar no registo de um utilizador são:

- Nome utilizador
- Password

Menu Principal – perfil administrador

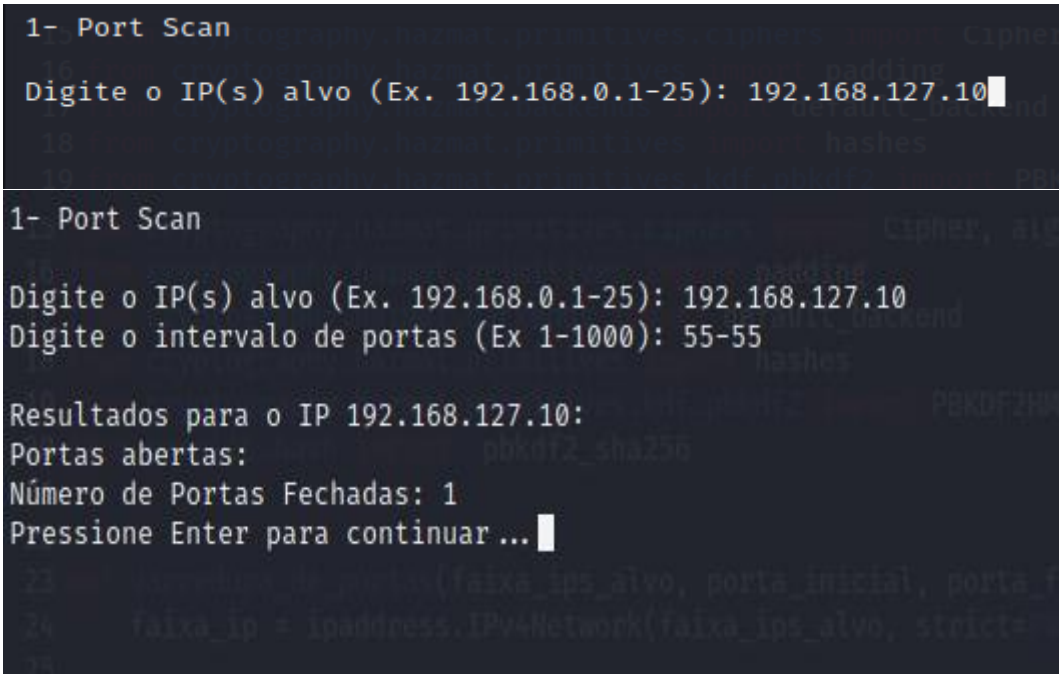
A aplicação de menus principais, e perfis de utilizadores:



O utilizador (Horlando1) escolhe uma opção de cada vez do menu conforme a indicação. Os itens do menu estão enumerados de 1 a 6 com exceção do sair que é número (0).

Port Scanner

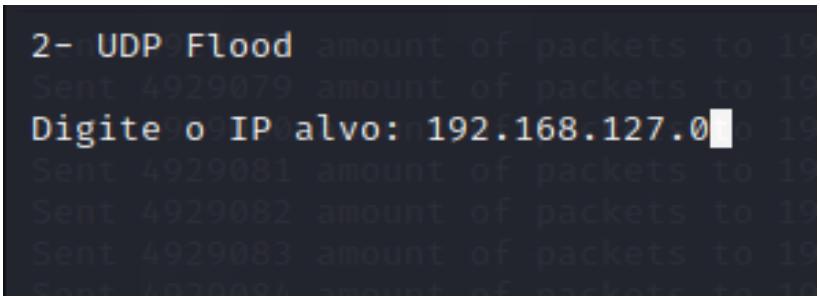
Esta opção permite ao utilizador fazer uma varredura de todos os portos e IP indicados pelo ele.

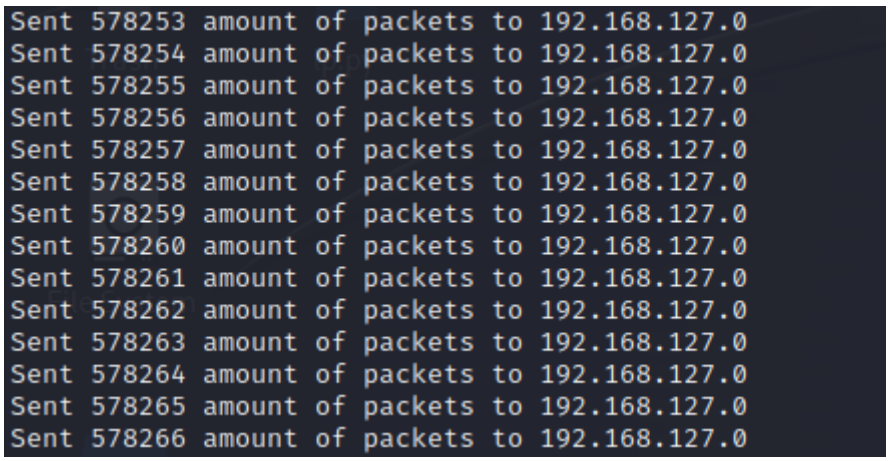


Para executar está funcionalidade o utilizador devera indicar:

- IP do alvo
- Porto inicial
- Porto final

UDP Flood

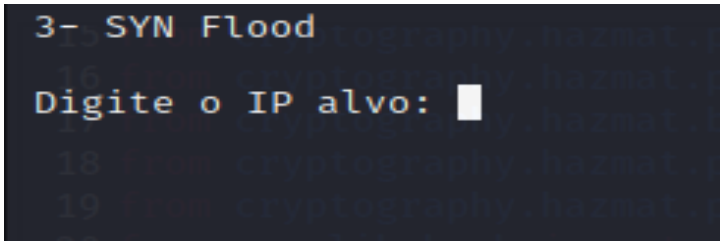




UDP ao IP alvo especificado (`ip_alvo`). O método `sendto` é usado para enviar dados por meio de um socket UDP. A variável `bytes_to_send` contém os dados que estão sendo enviados para determinado IP alvo.

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



Análise e Processamento de Ficheiros de Log

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.

Cliente 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

```
6- Port Knocking
Para configurar um servidor, primeiro utilize seguinte script:

* filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:TRAFFIC - [0:0]
:SSH-INPUT - [0:0]
:SSH-INPUTTWO - [0:0]
# TRAFFIC chain for Port Knocking. The correct port sequence in this example is 8881 → 7777 → 9991; any other sequence will drop the traffic
-A INPUT -j TRAFFIC
-A TRAFFIC -p icmp --icmp-type any -j ACCEPT
-A TRAFFIC -m state --state ESTABLISHED, RELATED -j ACCEPT
-A TRAFFIC -m state --state NEW -m tcp -p tcp --dport 22 -m recent --rcheck --seconds 30 --name SSH2 -j ACCEPT
-A TRAFFIC -m state --state NEW -m tcp -p tcp -m recent --name SSH2 --remove -j DROP
-A TRAFFIC -m state --state NEW -m tcp -p tcp --dport 9991 -m recent --rcheck --name SSH1 -j SSH-INPUTTWO
-A TRAFFIC -m state --state NEW -m tcp -p tcp -m recent --name SSH1 --remove -j DROP
-A TRAFFIC -m state --state NEW -m tcp -p tcp --dport 7777 -m recent --rcheck --name SSHO -j SSH-INPUT
-A TRAFFIC -m state --state NEW -m tcp -p tcp -m recent --name SSHO --remove -j DROP
-A TRAFFIC -m state --state NEW -m tcp -p tcp --dport 8881 -m recent --name SSHO --set -j DROP
-A SSH-INPUT -m recent --name SSH1 --set -j DROP
-A SSH-INPUTTWO -m recent --name SSH2 --set -j DROP
-A TRAFFIC -j DROP
COMMIT
# END or further rules
Pressione Enter para continuar ...
```

Navegação na aplicação menu

- 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.

Conclusão:

I. Este manual serve de apoio para qualquer usuário que quer utilizar esta aplicação, para poder orientar de acordo com instrução e funcionamento passo-a-passo desta aplicação sem ter conhecimento técnico do criador, porque tem tudo explicado de forma simples e clara.