



**INSTITUTO POLITÉCNICO
DE BEJA**

**Escola Superior de Tecnologia e
Gestão**



Mestrado de Engenharia de Segurança Informática

Manual de Utilização da Aplicação de Segurança Informática

Linguagens de Programação Dinâmica
Prof. José Jasnau Caeiro

Trabalho elaborado por:
António Urbano Baião Nº 5604
Carlos Rijo Palma Nº 5608

**Beja
2012/2013**

Índice

| | | |
|-------|--|----|
| 1 | Introdução | 4 |
| 2 | Guia de utilização da aplicação de Segurança informática | 5 |
| 2.1 | Introdução | 5 |
| 2.2 | Como executar a aplicação..... | 5 |
| 2.3 | Como fazer análise de ficheiro de logs da firewall | 6 |
| 2.3.1 | Criar relatório PDF..... | 8 |
| 2.3.2 | Criar ficheiro CSV | 9 |
| 2.3.3 | Criar Gráfico | 9 |
| 2.4 | Detetar portos de rede de várias máquinas disponíveis numa rede local (PortScanning) 10 | |
| 2.4.1 | Criar relatório PDF..... | 11 |
| 2.4.2 | Criar ficheiro CSV | 11 |
| 2.5 | Determinar que conexões se encontram ativas numa determinada rede local | 11 |
| 2.5.1 | Criar relatório PDF..... | 12 |
| 2.5.2 | Criar ficheiro CSV | 13 |

Índice de Ilustrações

| | |
|---|----|
| Ilustração 1 - Executar a aplicação..... | 5 |
| Ilustração 2 - Menu Inicial | 6 |
| Ilustração 3 - Analise Ficheiro Log..... | 6 |
| Ilustração 4 - Resultado da análise Ficheiro Log | 7 |
| Ilustração 5 - Menu Extra File Log | 8 |
| Ilustração 6 - Geração de PDF | 8 |
| Ilustração 7 - Geração de CSV | 9 |
| Ilustração 8 - Gráfico estatístico..... | 10 |
| Ilustração 9 - Introdução dados para portscanning..... | 10 |
| Ilustração 10 - Introdução de dados para analisar conexões ativas | 12 |

1 Introdução

Este trabalho foi proposto no âmbito da disciplina de Linguagens de Programação Dinâmica, inserida no Mestrado de Engenharia de Segurança Informática. Tem como objetivo o desenvolvimento de um manual de utilização da aplicação de segurança informática criada também no âmbito da mesma disciplina do Mestrado. A aplicação permite aos utilizadores da mesma, que façam análises aos ficheiros de *logs* da *firewall*, detetarem portos de rede de várias máquinas que se encontrem disponíveis numa determinada rede local e permite ainda determinar que conexões se encontram ativas numa determinada máquina. Importa referir que, esta aplicação corre em modo de linha de comando e possibilita ao utilizador analisar os dados que lhe foram devolvidos pela aplicação, através de ficheiros PDF e CSV.

O manual de utilização da aplicação é composto por dois capítulos, sendo os quais os seguintes, o capítulo da introdução e o capítulo Guia de utilização da aplicação de Segurança Informática. O primeiro capítulo descreve o âmbito do documento, e a estrutura do mesmo. O segundo capítulo faz referência ao guia de utilização da aplicação.

2 Guia de utilização da aplicação de Segurança informática

2.1 Introdução

A aplicação de Segurança informática permite ao utilizador escolher uma de três opções, sendo elas as seguintes:

- Processar ficheiros de log das *firewall*;
- Detetar portos de rede de várias máquinas que se encontrem disponíveis numa determinada rede local;
- Determinar que conexões se encontram ativas numa determinada máquina.

Após o utilizador escolher a opção desejada, a aplicação permite fazer ao utilizador criar relatórios em PDF ou ficheiros CSV com a informação devolvida.

2.2 Como executar a aplicação

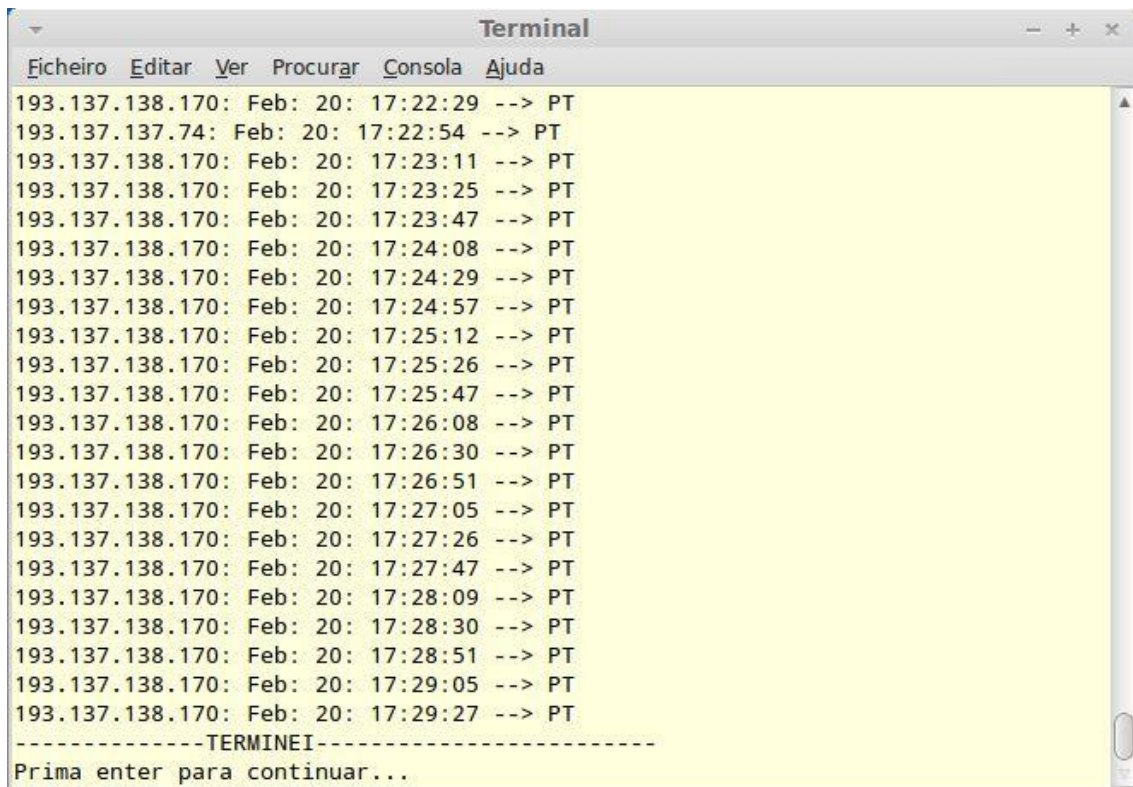
A aplicação deve ser executada em modo de administrador (“sudo su”) e para tal na diretoria onde se encontra o projeto, no terminal introduzimos:

```
$sudo python executarApp.py
```



Ilustração 1- Executar a aplicação

Se o caminho tiver correto, será iniciada a análise e posterior impressão na consola.



```
Terminal
Ficheiro Editar Ver Procurar Consola Ajuda
193.137.138.170: Feb: 20: 17:22:29 --> PT
193.137.137.74: Feb: 20: 17:22:54 --> PT
193.137.138.170: Feb: 20: 17:23:11 --> PT
193.137.138.170: Feb: 20: 17:23:25 --> PT
193.137.138.170: Feb: 20: 17:23:47 --> PT
193.137.138.170: Feb: 20: 17:24:08 --> PT
193.137.138.170: Feb: 20: 17:24:29 --> PT
193.137.138.170: Feb: 20: 17:24:57 --> PT
193.137.138.170: Feb: 20: 17:25:12 --> PT
193.137.138.170: Feb: 20: 17:25:26 --> PT
193.137.138.170: Feb: 20: 17:25:47 --> PT
193.137.138.170: Feb: 20: 17:26:08 --> PT
193.137.138.170: Feb: 20: 17:26:30 --> PT
193.137.138.170: Feb: 20: 17:26:51 --> PT
193.137.138.170: Feb: 20: 17:27:05 --> PT
193.137.138.170: Feb: 20: 17:27:26 --> PT
193.137.138.170: Feb: 20: 17:27:47 --> PT
193.137.138.170: Feb: 20: 17:28:09 --> PT
193.137.138.170: Feb: 20: 17:28:30 --> PT
193.137.138.170: Feb: 20: 17:28:51 --> PT
193.137.138.170: Feb: 20: 17:29:05 --> PT
193.137.138.170: Feb: 20: 17:29:27 --> PT
-----TERMEI-----
Prima enter para continuar...
```

Ilustração 4 - Resultado da análise Ficheiro Log

Findo isto, o utilizador terá 4 opções extra:

1. Imprimir a informação em PDF;
2. Imprimir a informação em CSV;
3. Gerar um gráfico estatístico;
4. Voltar a menu anterior.

2.3.2 Criar ficheiro CSV

No menu extra, existem varias opções de entre as quais a 2) que consiste em gerar um CSV com a informação analisada referente do ficheiro de log. Para isso o utilizador escolhe o número 2, seguido de “Enter”.

O CSV gerado ficará armazenado na diretoria do projeto com o nome “fileLog.csv”.

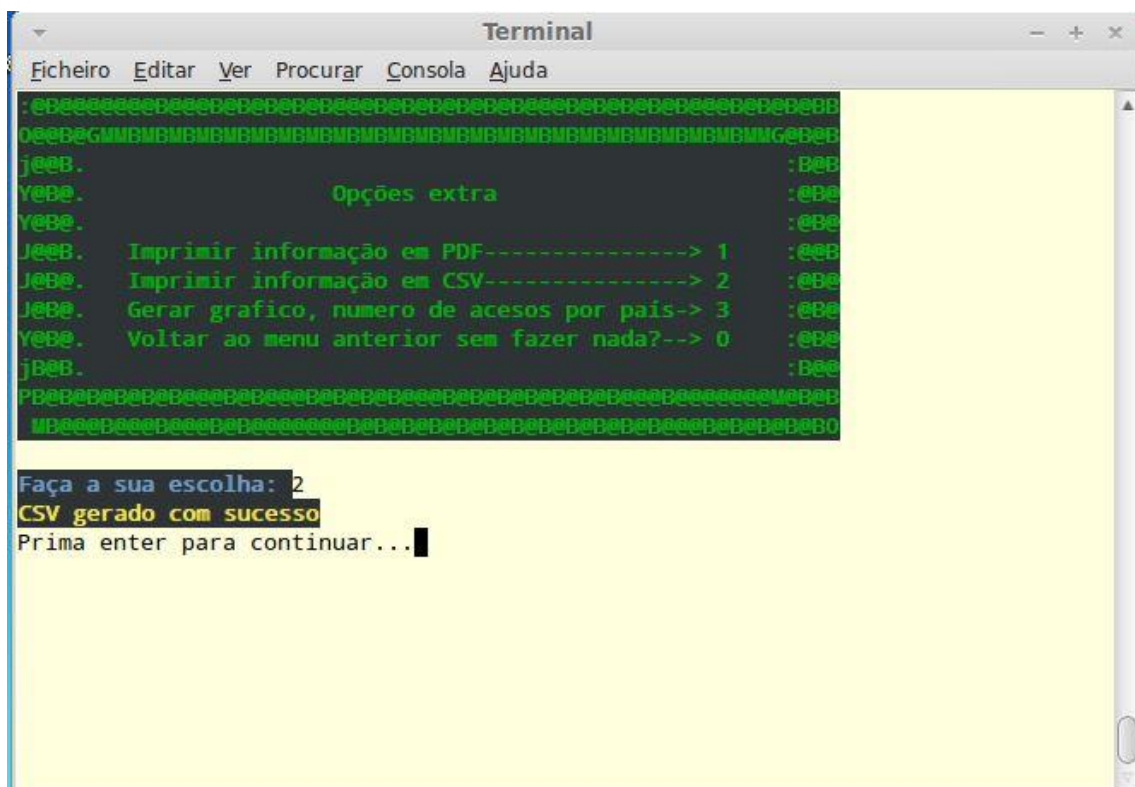


Ilustração 7 - Geração de CSV

2.3.3 Criar Gráfico

No menu extra, existem varias opções de entre as quais a 3) que consiste em gerar um gráfico de barras com a informação analisada referente do ficheiro de log. Esse gráfico mostrará o número de tentativas de acessos por país. Para isso o utilizador escolhe o número 3, seguido de “Enter”.

O gráfico estatístico é apresentado numa nova janela.

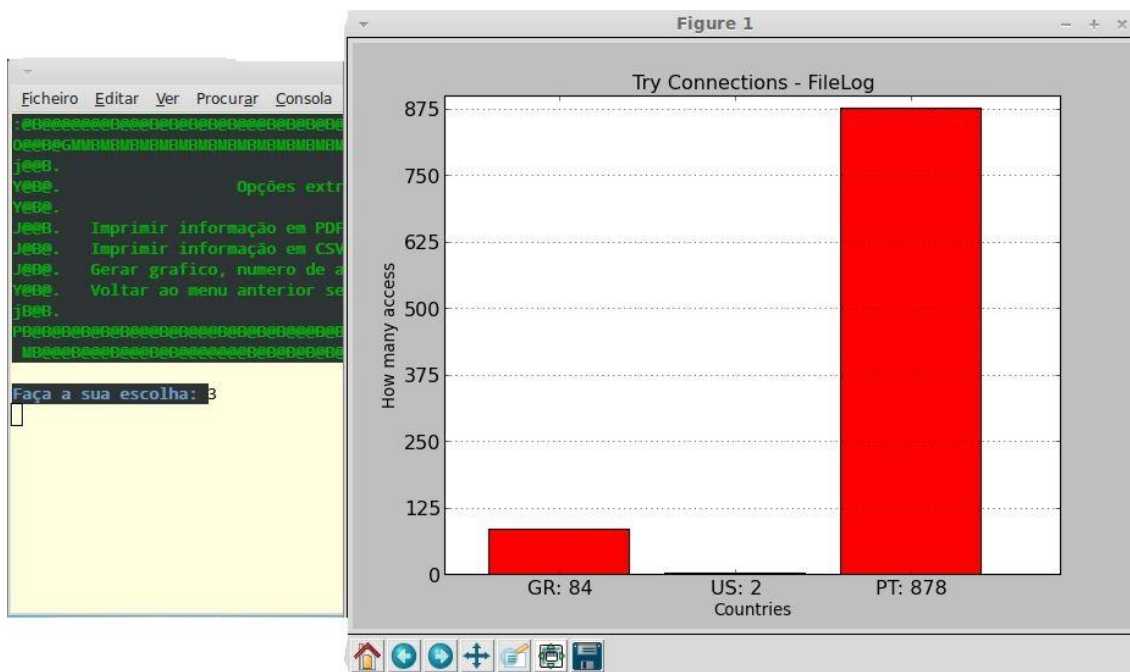


Ilustração 8 - Gráfico estatístico

2.4 Detetar portas de rede de várias máquinas disponíveis numa rede local (PortScanning)

Com a aplicação a correr, segue-se a indicação do menu principal e introduz-se o numero 2 seguido de “Enter”. De seguida aparecerá a interface de consola onde é pedido ao utilizador que introduza o endereço de IP da rede que o utilizador quer analisar, e a mascara da mesma rede seguido sempre de “Enter”.

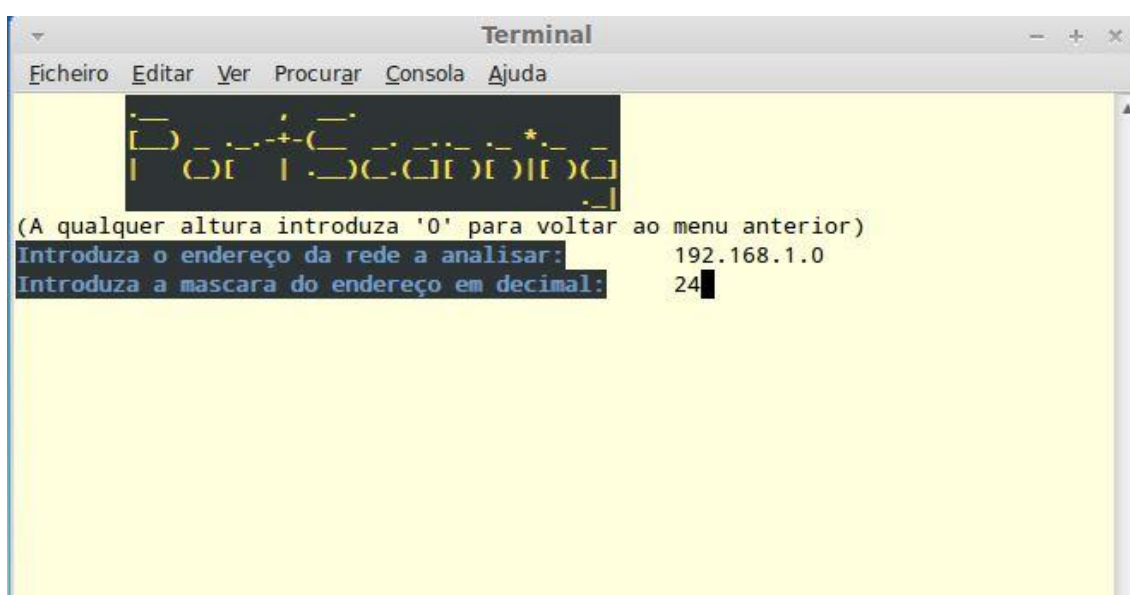


Ilustração 9 - Introdução dados para portscanning

O IP e a Mascara serão verificados e se tiverem corretos a aplicação procederá com a análise. Depois de feita a análise é apresentado na consola os resultados referentes as maquinas na rede e os portos que estiverem abertos.

Findo isto, o utilizador terá 3 opções extra:

1. Imprimir a informação em PDF;
2. Imprimir a informação em CSV;
3. Voltar a menu anterior.

2.4.1 Criar relatório PDF

No menu extra, existem varias opções de entre as quais a 1) que consiste em gerar um PDF com a informação analisada referente ao portScanning realizado. Para isso o utilizador escolhe o número 1, seguido de “Enter”.

O PDF gerado ficará armazenado na diretoria do projeto com o nome “portScanning.pdf”.

2.4.2 Criar ficheiro CSV

No menu extra, existem varias opções de entre as quais a 2) que consiste em gerar um CSV com a informação analisada referente ao portScanning realizado. Para isso o utilizador escolhe o número 2, seguido de “Enter”.

O CSV gerado ficará armazenado na diretoria do projeto com o nome “portScanning.csv”.

2.5 Determinar que conexões se encontram ativas numa determinada rede local

Com a aplicação a correr, segue-se a indicação do menu principal e introduz-se o numero 3 seguido de “Enter”. De seguida aparecerá a interface de consola onde é pedido ao utilizador que introduzo o endereço de IP da maquina que o utilizador quer analisar os serviços ativos, seguido sempre de “Enter”.

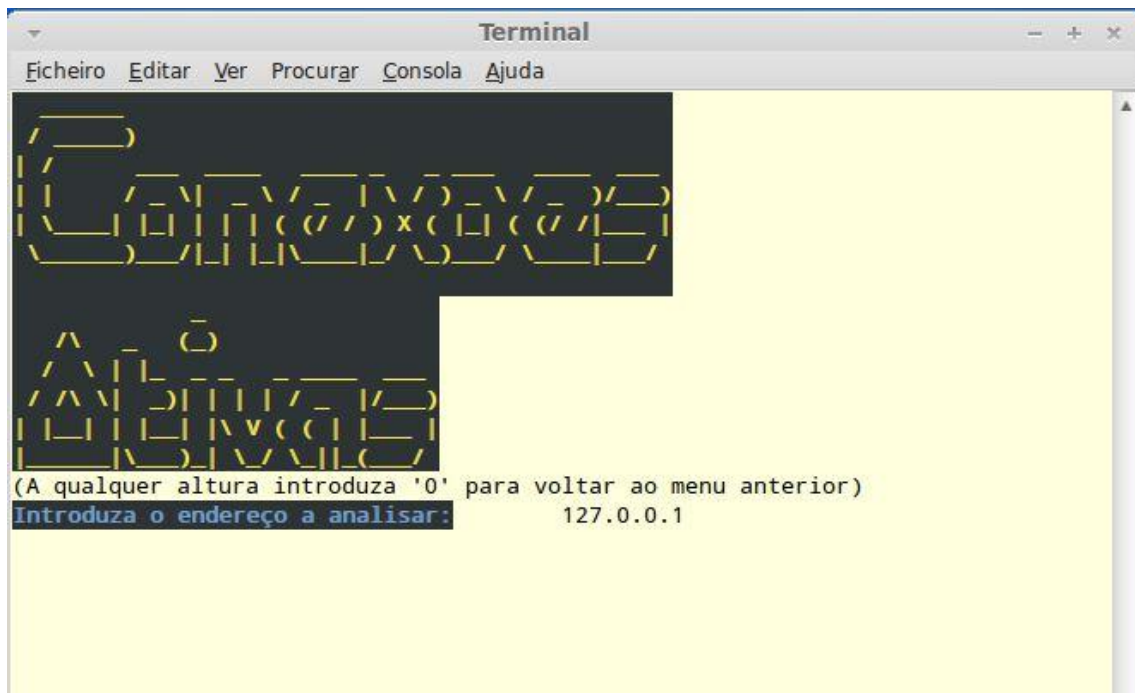


Ilustração 10 - Introdução de dados para analisar conexões ativas

O IP será verificado e se tiver correto a aplicação procederá com a análise. Depois de feita a análise dos serviços ativos, é apresentado na consola os resultados referentes aos serviços ativos na máquina.

Findo isto, o utilizador terá 3 opções extra:

1. Imprimir a informação em PDF
2. Imprimir a informação em CSV
3. Voltar a menu anterior

2.5.1 Criar relatório PDF

No menu extra, existem varias opções de entre as quais a 1) que consiste em gerar um PDF com a informação analisada referente à análise dos serviços ativos. Para isso o utilizador escolhe o número 1, seguido de “Enter”.

O PDF gerado ficará armazenado na diretoria do projeto com o nome “scanningConnections.pdf”.

2.5.2 Criar ficheiro CSV

No menu extra, existem varias opções de entre as quais a 2) que consiste em gerar um CSV com a informação analisada referente à análise dos serviços ativos. Para isso o utilizador escolhe o número 2, seguido de “Enter”.

O CSV gerado ficará armazenado na diretoria do projeto com o nome “scanningConnections.csv”.