



Aplicação de Segurança Informática

LINGUAGENS DE PROGRAMAÇÃO DINÂMICAS

Funcionalidades

Aplicação em Inglês

- ▶ Portscan
 - ▶ Connections
 - ▶ Firewall Log Processing
 - ▶ Add user to DB
 - ▶ DNS Lookup
 - ▶ WhoIS
 - ▶ Reverse Lookup
-
- ▶ Visualização geográfica de endereços ip
 - ▶ Exportação, CSV, Mapas, Gráficos

Iniciar Aplicação

- ▶ Aceder diretoria da aplicação no Terminal e introduzir o comando:
 - ▶ `python main_exe.py`
- ▶ Efetuar login

```
user@ubuntu: ~/Desktop/lpd14156043/src
Username: fonte
Password: mesi2015

Sucess.
```

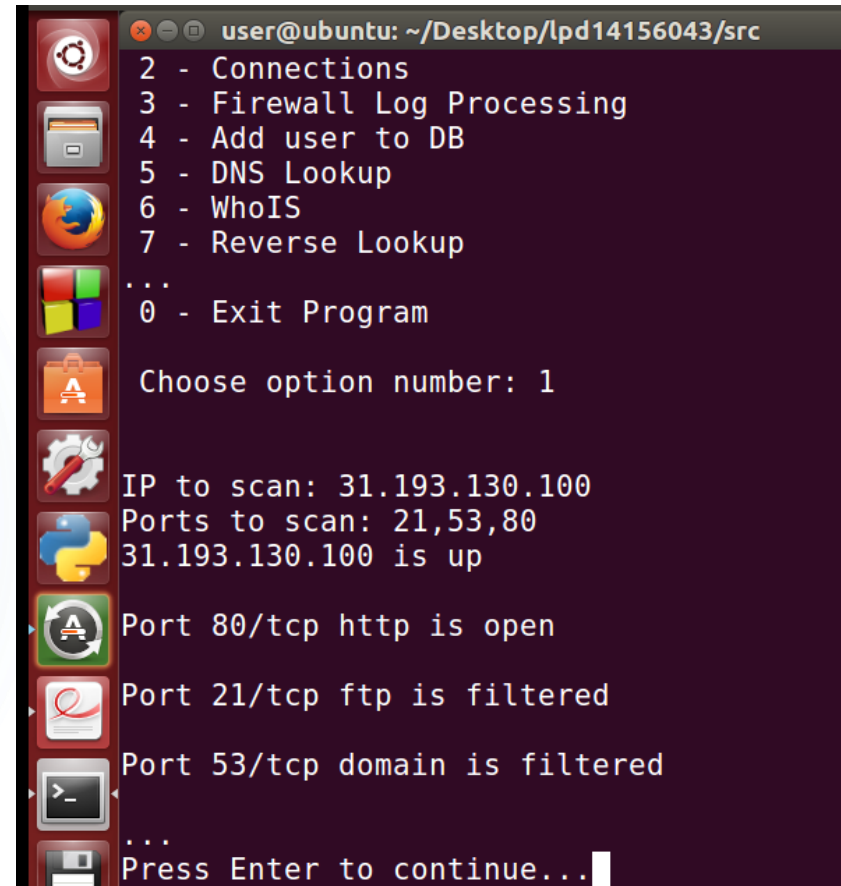
Menu Principal

- ▶ Escolher opção pretendida através do número correspondente

```
-----  
----- Network Security Application -----  
-----  
----- Author: Luis Fonte -----  
----- LPD MESI IPBEJA -----  
-----  
  
--MENU--  
1 - Portscan  
2 - Connections  
3 - Firewall Log Processing  
4 - Add user to DB  
5 - DNS Lookup  
6 - WhoIS  
7 - Reverse Lookup  
...  
0 - Exit Program  
  
Choose option number: █
```

Portscan

- ▶ Introduzir endereço IP e portos pretendidos



```
user@ubuntu: ~/Desktop/lpd14156043/src
2 - Connections
3 - Firewall Log Processing
4 - Add user to DB
5 - DNS Lookup
6 - WhoIS
7 - Reverse Lookup
...
0 - Exit Program
Choose option number: 1
IP to scan: 31.193.130.100
Ports to scan: 21,53,80
31.193.130.100 is up
Port 80/tcp http is open
Port 21/tcp ftp is filtered
Port 53/tcp domain is filtered
...
Press Enter to continue...
```

Connections

Opção 1

- ▶ Escolher opção do submenu (Active Connections)

```
--Connections--  
1 - Show Active Connections  
2 - Generate CSV  
3 - Generate Graph  
...  
0 - Back
```

Choose option number: 1

PROTOCOL	LOCALUSER	PORT	CONNECTION	PROTO	STATE	CLOSE_WAIT
tcp	192.168.139.137	51867	productsearch.ubu	https	CLOSE_WAIT	
IT						
tcp	192.168.139.137	42055	onslaught.tornode	https	ESTABLISHED	
HED						
tcp	192.168.139.137	58188	tor.kumbier.it	https	ESTABLISHED	
tcp6	ip6-localhost	38142	ip6-localhost	ipp	CLOSE_WAIT	

Press Enter to continue...

Connections

Opção 2

- ▶ Escolher opção do submenu (Generate CSV)
- ▶ O ficheiro CSV é criado na diretoria src

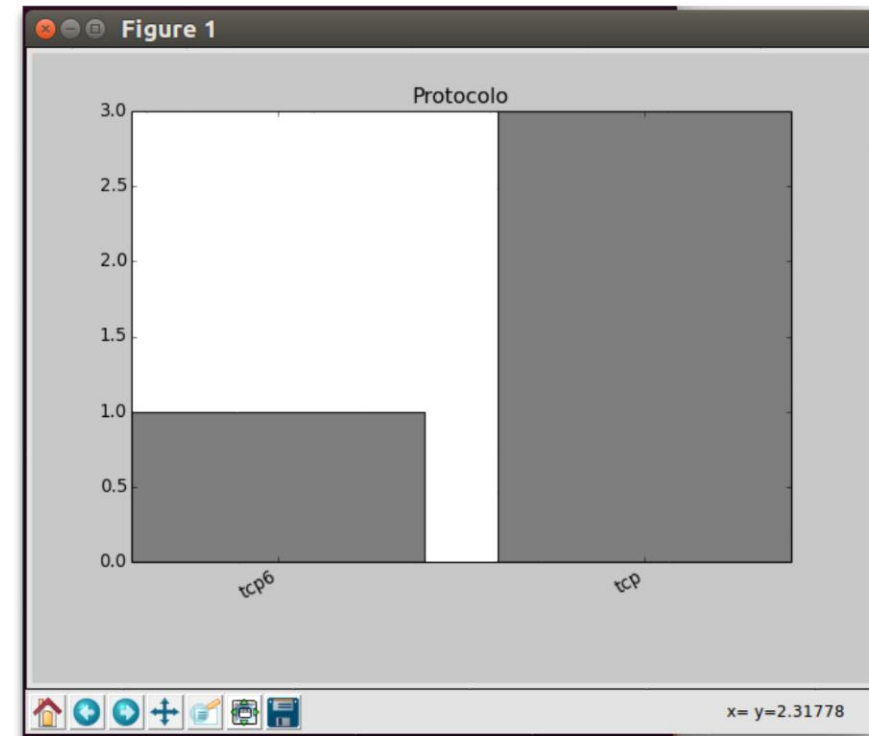
```
--Connections--  
1 - Show Active Connections  
2 - Generate CSV  
3 - Generate Graph  
...  
0 - Back  
  
Choose option number: 2  
  
||| Csv generated |||
```

Connections

Opção 3

- ▶ Escolher opção do submenu (Generate Graph)
- ▶ Escolher opções para o gráfico
- ▶ O gráfico surge de seguida no ecrã

```
--Connections--  
1 - Show Active Connections  
2 - Generate CSV  
3 - Generate Graph  
...  
0 - Back  
  
Choose option number: 3
```



Firewall Log Processing

Opção 1

- Escolher opção do submenu (Show Logs)

```
--Firewall--  
1 - Show Logs  
2 - Generate Map  
3 - Generate CSV  
4 - Generate Graph  
...  
0 - Back
```

Choose option number: 1

```
Feb2017:03:52 wlan0 193.137.138.170 224.0.0.1 UDP 50377 E  
U Portugal Beja  
Feb2017:04:06 wlan0 193.137.138.170 224.0.0.1 UDP 59240 E  
U Portugal Beja  
Feb2017:04:27 wlan0 193.137.138.170 224.0.0.1 UDP 62315 E  
U Portugal Beja  
Feb2017:04:48 wlan0 193.137.138.170 224.0.0.1 UDP 63505 E  
U Portugal Beja  
Feb2017:05:09 wlan0 193.137.138.170 224.0.0.1 UDP 50582 E  
U Portugal Beja  
Feb2017:05:31 wlan0 193.137.138.170 224.0.0.1 UDP 60176 E  
U Portugal Beja  
Feb2017:05:52 wlan0 193.137.138.170 224.0.0.1 UDP 57051 E  
U Portugal Beja  
Feb2017:06:06 wlan0 193.137.138.170 224.0.0.1 UDP 56251 E  
U Portugal Beja  
Feb2017:06:27 wlan0 193.137.138.170 224.0.0.1 UDP 63995 E  
U Portugal Beja  
Feb2017:06:49 wlan0 193.137.138.170 224.0.0.1 UDP 58959 E  
U Portugal Beja  
Feb2017:07:17 wlan0 193.137.138.170 224.0.0.1 UDP 58528 E  
U Portugal Beja
```

Firewall Log Processing

Opção 2

- ▶ Escolher opção do submenu (Generate Map)
- ▶ O mapa é criado na diretoria src
- ▶ Nome do ficheiro com o mapa _firewallLog_map.htm



```
--Firewall--  
1 - Show Logs  
2 - Generate Map  
3 - Generate CSV  
4 - Generate Graph  
...  
0 - Back  
  
Choose option number: 2  
  
||| Map generated |||
```

Firewall Log Processing

Opções 3 e 4

- ▶ Escolher opção do submenu “Generate CSV” e “Generate Graph”
- ▶ Os ficheiros são criados na diretoria src
- ▶ O gráfico surge no ecrã

The image shows a terminal window on the left and a LibreOffice Calc spreadsheet on the right. The terminal displays a menu for Firewall log processing with options 1 to 4, and option 3 (Generate CSV) has been selected. The spreadsheet, titled 'firewall_logs.csv', contains a table of log entries with columns for time, interface, source IP, destination IP, protocol, port, and location. The first row is highlighted in orange.

```
--Firewall--  
1 - Show Logs  
2 - Generate Map  
3 - Generate CSV  
4 - Generate Graph  
...  
0 - Back  
  
Choose option number: 3  
  
||| CSV with logs generated |||
```

	A
1	Feb1712:08:44,wlan0,,108.160.160.164,192.168.1.107,TCP,80,NA,United States,San Francisco,-122.417,37.77940000000001
2	Feb1814:02:28,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
3	Feb1814:02:40,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
4	Feb1814:02:41,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
5	Feb1814:02:41,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
6	Feb1814:02:58,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
7	Feb1814:02:59,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
8	Feb1814:03:00,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
9	Feb1814:03:00,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
10	Feb1814:03:02,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
11	Feb1814:03:03,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
12	Feb1814:03:07,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014
13	Feb1814:03:10,wlan0,,94.71.2.233,192.168.1.107,TCP,63556,EU,Greece,Athens,23.733300000000014,37.983300000000014

DNS Lookup

- ▶ Permite determinar o endereço IP, através do nome de domínio, introduzido pelo utilizador

```
-MENU--  
1 - Portscan  
2 - Connections  
3 - Firewall Log Processing  
4 - Add user to DB  
5 - DNS Lookup  
6 - WhoIS  
7 - Reverse Lookup  
..  
0 - Exit Program  
  
Choose option number: 5  
  
Address to check: edia.pt  
['31.193.130.100']
```


WhoIS

- Fornece informações sobre registo e range de ip na internet, dum determinado endereço IP, introduzido pelo utilizador

```
Choose option number: 6

IP address to search for: 31.193.130.100

{'asn': '29550',
 'asn_cidr': '31.193.128.0/20',
 'asn_country_code': 'GB',
 'asn_date': '2011-04-27',
 'asn_registry': 'ripenc',
 'nets': [{'abuse_emails': 'abuse@as29550.net',
            'address': 'Simply Transit\nUnit 2\nSmallmead Road\nReading\nBerkshire\nRG2 0QS',
            'cidr': '31.193.128.0/22',
            'city': None,
            'country': 'GB',
            'created': '2011-05-09T14:44:29',
            'description': 'Customer range',
            'handle': None,
            'misc_emails': None,
            'name': 'Cust-MS-VPS',
            'postal_code': None,
            'range': '31.193.128.0 - 31.193.131.255',
            'state': None,
            'tech_emails': None,
            'updated': '2011-05-09T14:44:29'}],
 'query': '31.193.130.100',
 'raw': None}

Click Enter to continue...
```

Reverse Lookup

- ▶ Permite determinar um nome de domínio, a partir do endereço IP, introduzido pelo utilizador.

```
Choose option number: 7

-Reverse Lookup-

Enter the IP address: 31.193.130.100

('alqueva.edia.pt', [], ['31.193.130.100'])

Click Enter to continue...
```

Questões?



Obrigado