IMPLEMENTAÇÃO DE UM MINI SNIFFER DE REDE

Gabriel Angelo Freire Gonçalves[1]

[1]Universidade Estatdual do Ceará (UECE)
Av. Dr. Silas Munguba, 1700 - Campus do Itaperi, Fortaleza - CE, 60741-000

1. Informações gerais

O objetivo deste artigo é descrever alguns detalhes técnicos da implementação de um mini sniffer de rede.

2. Funcionamento

Ao escrever o comando "python sniffer <timeout> <interface> <file_pcap>" o script executa primeiramente um comando tcpdump que captura os pacotes na interface de rede durante o tempo definido (timeout) e escreve os dados em um arquivo .pcap. Após isso, uma rotina de obtenção desses pacotes é feita usando a lib pyshark que lê os pacotes do arquivo e os transforma em objetos python de alto nível para manipulações estatísticas. Após obter a coleção de pacotes, as seguintes rotinas são executadas:

- Apresentação de fluxos ;
- Ip origem que mais transmitiu;
- Ip destino mais acessado;
- Tamanho médio de pacotes;
- Montante de dados transmitidos.

3. Parâmetros

- timeout: tempo de captura de pacotes;
- interface: interface de rede ao qual deseja examinar;
- file_pcap: arquivo de captura que será usado posteriormente para obtenção dos pacotes

4. Imagens

- **Fluxos**

```
(tcp) gabriel@gabriel-Inspiron-5458:~/projects/redes/work1$ python sniffer.py 10 wlp6s0 mofi
[sudo] senha para gabriel:
tcpdump: listening on wlp6s0, link-type EN10MB (Ethernet), capture size 262144 bytes
145 packets captured
149 packets received by filter
0 packets dropped by kernel

#####FLOWS#####

+---------+--------------------+--------------------+---------+
| type    | from               | to                 | size    |
+---------+--------------------+--------------------+---------+
| UDP/DNS | 192.168.15.27:53   | 192.168.15.1:36585 | 75 kb   |
| UDP/DNS | 192.168.15.27:53   | 192.168.15.1:36585 | 75 kb   |
| UDP/DNS | 192.168.15.1:36585 | 192.168.15.27:53   | 91 kb   |
| UDP/DNS | 192.168.15.1:36585 | 192.168.15.27:53   | 103 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 74 kb   |
| TCP/TCP | 216.58.222.78:55834| 192.168.15.27:443  | 74 kb   |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 583 kb  |
| TCP/TCP | 216.58.222.78:55834| 192.168.15.27:443  | 66 kb   |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 222 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 117 kb  |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 159 kb  |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 452 kb  |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 135 kb  |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 104 kb  |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 104 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55836| 74 kb   |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/TCP | 216.58.222.78:55834| 192.168.15.27:443  | 66 kb   |
| TCP/TCP | 216.58.222.78:55834| 192.168.15.27:443  | 66 kb   |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 440 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 104 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/SSL | 216.58.222.78:55834| 192.168.15.27:443  | 112 kb  |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55834| 66 kb   |
| TCP/SSL | 192.168.15.27:443  | 216.58.222.78:55834| 112 kb  |
| TCP/TCP | 216.58.222.78:55836| 192.168.15.27:443  | 74 kb   |
| TCP/TCP | 192.168.15.27:443  | 216.58.222.78:55836| 66 kb   |
```

- **Estatísticas**

```
| TCP/SSL | 64.4.54.254:59766    | 192.168.15.27:443    | 917 kb  |
| TCP/TCP | 192.168.15.27:443    | 64.4.54.254:59766    | 66 kb   |
| TCP/SSL | 192.168.15.27:443    | 64.4.54.254:59766    | 192 kb  |
| TCP/TCP | 216.58.222.78:55834  | 192.168.15.27:443    | 66 kb   |
| TCP/SSL | 64.4.54.254:59766    | 192.168.15.27:443    | 117 kb  |
| TCP/SSL | 192.168.15.27:443    | 64.4.54.254:59766    | 1420 kb |
| TCP/TCP | 64.4.54.254:59766    | 192.168.15.27:443    | 66 kb   |
| TCP/SSL | 64.4.54.254:59766    | 192.168.15.27:443    | 380 kb  |
| TCP/SSL | 192.168.15.27:443    | 64.4.54.254:59766    | 97 kb   |
| TCP/TCP | 192.168.15.27:443    | 64.4.54.254:59766    | 66 kb   |
| TCP/TCP | 64.4.54.254:59766    | 192.168.15.27:443    | 66 kb   |
| TCP/SSL | 158.85.224.178:55062 | 192.168.15.27:443    | 173 kb  |
| TCP/TCP | 192.168.15.27:443    | 158.85.224.178:55062 | 66 kb   |
+---------+----------------------+----------------------+---------+
+----------------------+------------------+--------------------+------------+
| main ip transmitter  | main ip receptor | packet middle size | total size |
+----------------------+------------------+--------------------+------------+
| 192.168.15.27        | 192.168.15.27    | 231.94 kb          | 33400 kb   |
+----------------------+------------------+--------------------+------------+
 OK
```

5. Observações

- O projeto foi escrito em python 3;

- O script precisa ser executado em modo sudo.

- Ao final da execução, uma exception é lançada, porém deve ser ignorada.

References

J. Kurose and K. Ross, Computer Networking: A Top Down Approach Using theInternet, Addison-Wesley Computer Science, 6th Edition, 2013.