Aplicação de Segurança Informática

Instituto Politécnico de Beja

Escola Superior de Tecnologia e Gestão de Beja

Mestrado em Engenharia de Segurança Informática

Linguagens de Programação Dinâmicas

Docente: José Jasnau Caeiro

Aluno: Gonçalo Béjinha nº 13428

Aplicação de Segurança Informática

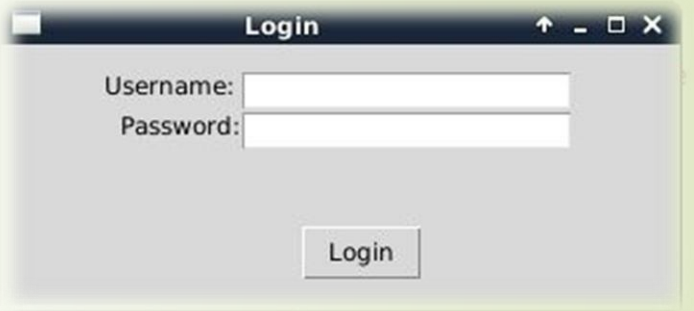
- No âmbito da Unidade Curricular de Linguagens de Programação Dinâmicas do Mestrado em Engenharia de Segurança Informática foi elaborada uma aplicação de segurança informática com as seguintes funcionalidades:
  - Deteção dos portos de várias máquinas numa rede local;
  - Deteção de ligações ativas numa determinada máquina;
  - Processamento de ficheiros *log de firewall;*
  - *Esta aplicação pode ainda exportar a informação em vários formatos, nomeadamente, PDF, CSV e SQL.*

Desenvolvimento da aplicação

- Sistema de Controlo de Versões
  - Foi utilizado o sistema de controlo de versões Git
    - Alguns comandos: git init; git add; git commit; touch ignore; git branch; git merge; git clone <link do repositório>; git push origin master;
- SO Linux
  - Debian 7.1
  - Geany
  - Emacs;
  - Python 2.7.3

Interface / Funcionamento da Aplicação

- A aplicação produzida com recurso à linguagem de programação Python, versão 2.7.
- A aplicação apresenta uma interface gráfica, construída com auxilio da biblioteca Tkinter.



  - Sistema de Login (criptografia)
    - A aplicação apresenta uma interface gráfica com sistema de autenticação, desenvolvido com Tkinter
  - Interface Principal
    - Depois de efetuar o login, fica disponível a interface principal
    - A interface principal também foi desenvolvida com Tkinter e faz a ligação a todos os módulos da aplicação

Interface / Funcionamento da Aplicação 2

- **1 – IP Scan**
  - Para fazer um scan à rede local deve pressionar no botão "1 – IP Scan" na interface gráfica e em seguida escrever o comando com a gama de IP pretendida. Ex: **python lan_scan.py –network=192.168.1.0/24**
  - Para a utilizar este módulo é preciso instalar scapy

```
LAN Scanner

Version 1.0 (LPD 2015)
_____________________________________________________

[!] Wrong argument and parameter passed. Use --help for more information.
[!] Usage: sudo ./lan_scan.py --network=<your network>
[i] Usage Example: sudo ./lan_scan.py --network=192.168.1.0/24
```

- **Scan Portos ativos**
  - Este módulo é uma pequena réplica da ferramenta NMAP, escrita em python
  - O código deste módulo é da autoria de phillipsme, disponível em https://www.phillips321.co.uk

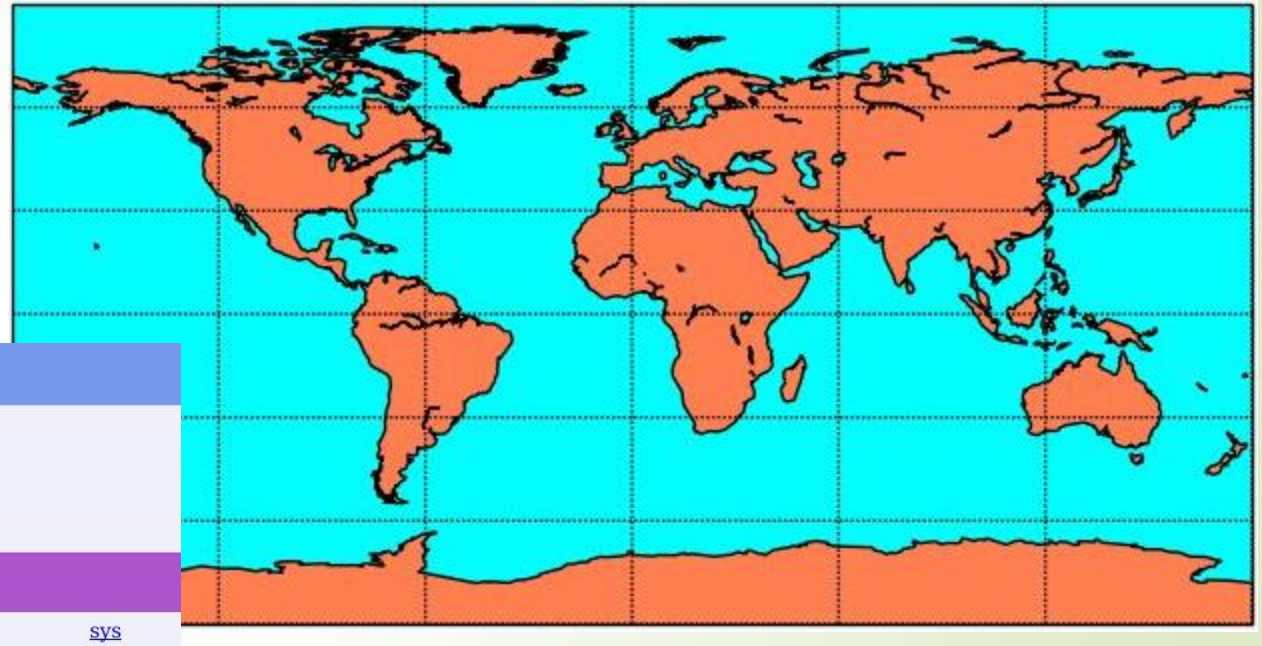
```
usage: active.py [-h] [-v] [-sS] [-sU] [-p PORTS] [-t TARGETS]

Replicates limited nmap functionality in python

optional arguments:
  -h, --help            show this help message and exit
  -v, --verbose         Enable this for full output
  -sS, --tcpscan        Enable this for TCP scans
  -sU, --udpscan        Enable this for UDP scans
  -p PORTS, --ports PORTS
                        The ports you want to scan (21,22,80,135-139,443,445)
  -t TARGETS, --targets TARGETS
                        The target(s) you want to scan (192.168.0.1)
```

Interface / Funcionamento da Aplicação 3

- Processamento de ficheiros log



- Relatórios

active

```
#-------------------------------------------------------------------------------
# Author:       phillipsme
# Copyright:    (c) phillipsme 2014
# Licence:      Free to use, free to have fun!
# Developer:    Goncalo Bejinha
#-------------------------------------------------------------------------------
```

Modules

argparse socket sys

Functions

bin2ip(b)

dec2bin(n, d=None)

errormsg(msg)

ip2bin(ip)

iprange(addressrange)

main()

portscan(target, ports, tcp, udp, verbose)

printmsg(msg)

Conclusões

- Concluída a aplicação, destaca-se a importância das matérias abordadas e aprendidas durante as aulas e investigação, nomeadamente o conjunto de bibliotecas necessárias para o desenvolvimento de aplicações desta natureza.
- Um dos aspetos positivos a realçar no desenvolvimento da aplicação são as imensas fontes de informação disponíveis para recolha e análise de conteúdos técnicos sobre segurança informática.
- Por outro lado, a falta de experiência em programação pode dificultar o tratamento e adaptação dos *scripts às necessidades proposta para aplicação*.