INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Linguagens de Programação Dinâmica

Aplicação de Segurança Informática

Gonçalo Béjinha nº 13428

Beja

2015

Índice

Índice de Figuras

Introdução

No decorrer da unidade curricular de Linguagens de Programa Dinâmica do Mestrado em Engenharia de Segurança Informática foi elaborado o presente manual sobre aplicação de Segurança Informática.
Este manual tem como objetivo explicar o modo de funcionamento de uma aplicação de segurança informática, apresentando todas as janelas (Interface), botões e comandos para executar cada módulo.
A aplicação foi desenvolvida com auxílio da Linguagem de programação Python, no Sistema Operativo Debian 7.1, a aplicação tem como objetivos:

- Deteção do IP de várias máquinas numa rede local;
- Deteção de ligações ativas numa determinada máquina;
- Processamento de ficheiros log da *firewall*;
- Esta aplicação pode ainda exportar a informação em vários formatos, nomeadamente, PDF, CSV e SQL.

A aplicação apresenta uma interface gráfica com um sistema de autenticação, mas todos os módulos podem ser executados individualmente através da linha de comandos.

Interface Gráfica

Para iniciar a aplicação o utilizador deve entrar na pasta ***src*** e executar o ficheiro **login.py** (ex: python login.py) para abrir a janela de login da aplicação, em seguida deve introduzir o *Username* e *Password* e finalmente deve carregar no botão Login.

Se errar o *Username* e/ou *Password* mais de duas vezes a janela irá fechar, sendo mostrado o número de tentativas restantes.

Username: abelha

Password: maia

Figura 1 - Sistema de Autenticação

Janela Principal

Depois de efetuar o login corretamente no passo anterior, será apresentada a janela principal, onde se destaca os botões Figura 2:

Figura 2 - Interface

- Sobre a aplicação

Quando clicado este botão será apresentado um pequeno texto introdutório sobre a Aplicação.

"No âmbito da disciplina de Linguagens de Programação Dinâmica do Mestrado em Engenharia de Segurança Informática foi desenvolvida a presente aplicação, que permite detetar os portos ativos nas máquinas de uma rede local, analisar ficheiros log e salvar relatórios dos dados."

- 1 – IP Scan

O Botão "1 – IP Scan" quando clicado irá executar o módulo **lan_scan.py,** que permite fazer o scan a uma rede local e detetar o IP das máquinas.

- 2 – Portos Ativos

O Botão "2 – Portos Ativos" quando clicado irá executar o módulo **active.py,** que permite fazer o scan das ligações ativas de uma determinada máquina.

- 3 – *Firewall*

O Botão "3 – Firewall" quando clicado irá executar o módulo **FirewallData.py,** que permite analisar os ficheiros log, apresentando no mapa-mundo os locais dos ataques detetados na *firewall*, este botão apresenta também um gráfico de barras com o número de ataques de cada país.

Lan Scanner

Lan Scanner pode ser executado em separado ou a partir da janela principal clicando no botão "1 – IP Scan", este *script* corresponde ao módulo **lan_scan.py** do projeto.
Para executar corretamente este código o utilizador precisa de indicar a gama de IP´S que quer analisar, por exemplo: **python lan_scan.py –network=192.168.1.0/24**

Figura 3 - Lan Scanner

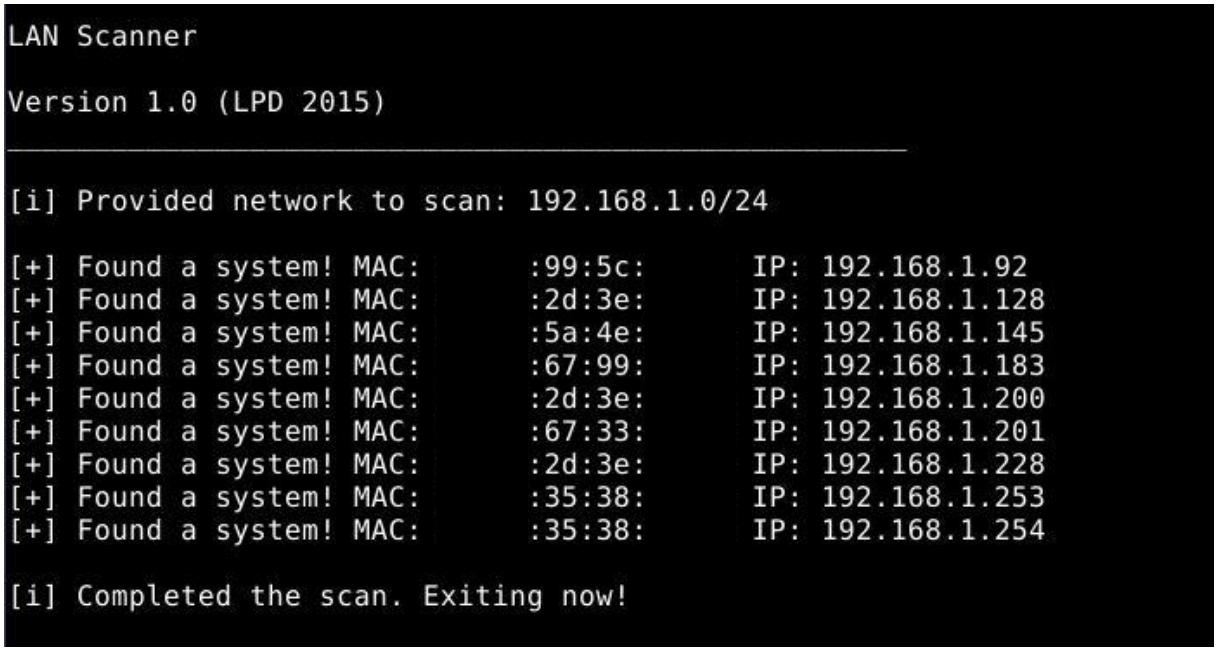

Figura 4 - Lan Scanner em execução

Por razões de segurança foram ocultados os endereços MAC das máquinas.

Scan de portos ativos

active.py é um dos módulos mais importantes do projeto, pois irá analisar as ligações ativas de uma determinada máquina, este código apresenta funcionalidades idênticas à ferramenta NMAP, executando TCP e UDP scan Figura 5.

Para executar corretamente este código o utilizador precisa de indicar o IP da máquina vitima que quer analisar e os argumentos opcionais, por exemplo: **python active.py -v -sS -sU -p 21,22,80,135-139,443,445 -t 192.168.1.128**

```
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)
```

Figura 5 - Portos ativos

```
21/tcp  closed
22/tcp  closed
80/tcp  closed
135/tcp         closed
136/tcp         closed
137/tcp         closed
138/tcp         closed
139/tcp         closed
443/tcp         closed
445/tcp         closed
21/udp  open
22/udp  open
80/udp  open
135/udp         open
136/udp         open
137/udp         open
138/udp         open
139/udp         open
443/udp         open
445/udp         open
```

Figura 6 - Scan Ligações ativas

Análise Firewall Log

A análise de ficheiros log é apoiada com a representação gráfica, através do módulo **FirewallData.py,** este ficheiro também não foge à exceção, ou seja, pode ser executado pela linha de comandos ou pela interface gráfica, clicando no botão *Firewall*.

A informação dos ficheiros log é tratada de modo a ser recolhida a informação essencial para se saber a localização dos ataques e o respetivo número de ataques que cada país apresenta.

Para executar o script deve entrar na pasta src e escrever o seguinte comando*:* **python FirewallData.py**

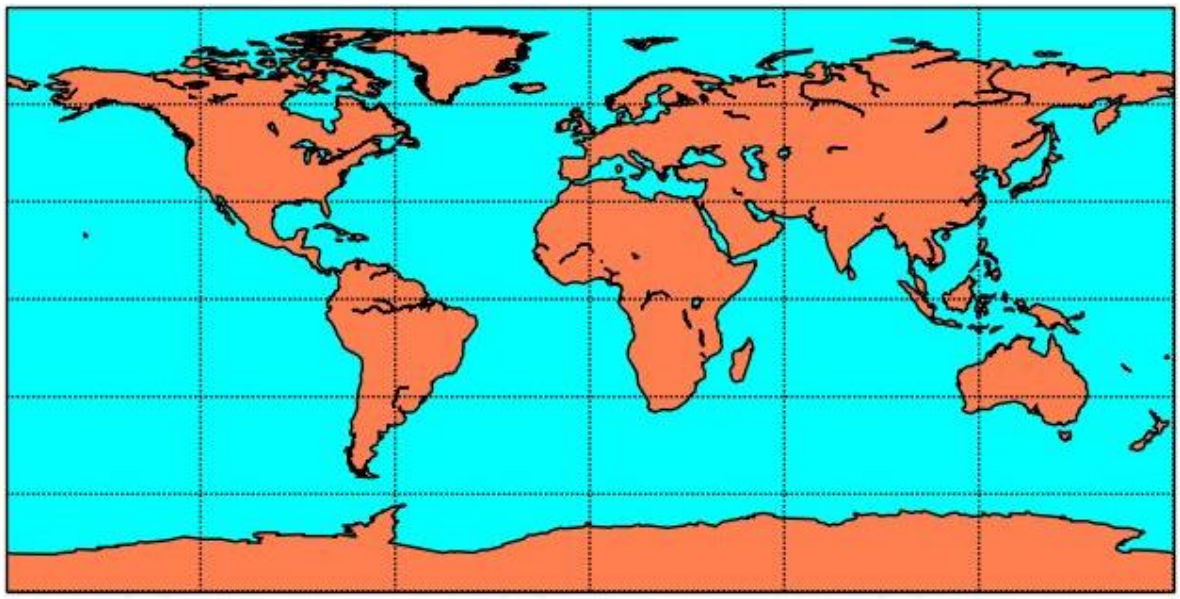

Figura 7 - Análise de ficheiros Log

Exportar resultados

A aplicação permite gravar em vários formatos, para visualizar os resultados obtidos dos módulos.

No final de cada módulo foi adicionada uma porção de código, de modo a facultar ao utilizador as opções de exportar os resultados em formato PDF, CSV ou SQL.

Referências

[1] Vivek, “Html to Pdf,” 3 Outubro 2012. [Online]. Available: http://www.cyberciti.biz/open-source/html-to-pdf-freeware-linux-osx-windows-software/.

[2] Python, “Pydoc,” [Online]. Available: http://pydoc.org/2.4.1/pydoc.html. [Acedido em 25 Junho 2015].

[3] Python, “Cryptographic modules for Python,” Python Software Foundation, 20 junho 2014. [Online]. Available: https://pypi.python.org/pypi/pycrypto.

[4] Python, “Tkinter - Python interface to Tcl/Tk,” Python Software Foundation, [Online]. Available: https://docs.python.org/2/library/tkinter.html.

[5] J. Hunter, “matplotlib,” [Online]. Available: http://matplotlib.org/.

[6] P. Biondi, “Scapy - Download and Installation,” Python, [Online]. Available: http://www.secdev.org/projects/scapy/doc/installation.html.

[7] “Numerical Python,” [Online]. Available: http://sourceforge.net/projects/numpy/files/OldFiles/1.4.0rc2/.

[8] Maxmind´s, “Pure Python GeoIP API,” [Online]. Available: https://pypi.python.org/pypi/pygeoip/.

[9] “Python-nmap : nmap from python,” [Online]. Available: http://xael.org/norman/python/python-nmap/.

[10] Maxmind, “GeoLite Legacy Downloadable Databases,” MaxMind Dev, [Online]. Available: http://dev.maxmind.com/geoip/legacy/geolite/.

[11] webnull, “scan-network,” 14 Agosto 2011. [Online]. Available: https://github.com/webnull/scan-network. [Acedido em 22 junho 2015].

[12] gambit240809, “PortScanner,” 19 novembro 2013. [Online]. Available: https://github.com/OpenFireTechnologies/PortScanner. [Acedido em 22 junho 2015].

[13] R. rosario, “Quick and Dirty GeoIP Lookup Function in Python,” [Online]. Available: http://rickyrosario.com/blog/quick-and-dirty-geoip-lookup-function-in-python/. [Acedido em 23 junho 2015].

[14] Python, “Modules,” Python Software Foundation, [Online]. Available: https://docs.python.org/2/tutorial/modules.html. [Acedido em 23 junho 2015].

[15] “The Reportlab Toolkit,” Python Software Foundation , [Online]. Available: https://pypi.python.org/pypi/reportlab. [Acedido em 23 junho 2015].

[16] “How to detect the country and city of a user accessing your site?,” stackoverflow, [Online]. Available: http://stackoverflow.com/questions/1163136/how-to-detect-the-country-and-city-of-a-user-accessing-your-site. [Acedido em 24 junho 2015].

[17] B. Matplotlib, “Equidistant Cylindrical Projection,” [Online]. Available: ttp://matplotlib.org/basemap/users/cyl.html. [Acedido em 21 junho 2015].

[18] “Python for PDF Generation,” Devshed Network, [Online]. Available: http://www.devshed.com/c/a/Python/Python-for-PDF-Generation/#whoCFCPh3TAks368.99. [Acedido em 25 junho 2015].