INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado de Engenharia de Segurança Informática

Implementação de uma aplicação de Segurança Informática

(Linguagem de programação Python)

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

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 uma Aplicação de Segurança Informática, aplicação essa que permite aos seus utilizadores fazer análises ao ficheiro de *logs* da *firewall*, permitem 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. A aplicação foi criada para correr em modo linha de comando e possibilita ao utilizador analisar os dados que foram devolvidos pela aplicação, através da própria linha de comando ou através de ficheiros PDF e CSV. Importa referir que, esta aplicação foi desenvolvida na linguagem de programação *Python*, uma linguagem de alto nível, orientada a objetos, moderna, com um grande padrão de bibliotecas e um conjunto de ferramentas de desenvolvimento muito sofisticadas.

De forma a tornar a leitura do relatório a mais simplificada possível, o mesmo encontra-se dividido em seis de capítulos, nomeadamente o capítulo da introdução, o capítulo intitulado de "o que é a linguagem de programação Python", o capítulo intitulado de "aplicação de Segurança Informática", o capítulo intitulado de "Estatísticas", o capítulo intitulado de "Conclusão" e por fim o capítulo intitulado de "Bibliografia". O primeiro capítulo descreve o âmbito em que se integra o relatório, o objetivo do mesmo, e a estrutura do mesmo. Por sua vez o segundo capítulo faz a caracterização da linguagem de programação Python. O terceiro capítulo faz referência a implementação da aplicação de segurança informática, o quarto capítulo é referente às estatísticas que aplicação pode efetuar. O quinto capítulo é referente às conclusões. Por fim o último capítulo refere as referências bibliográficas.

2 O que é a linguagem de programação Python

Python[4] é uma linguagem de programação de alto nível, interpretada, imperativa, orientada a objetos e de tipagem forte que permite trabalhar mais rapidamente e integrar o nosso sistema mais eficazmente. Ao aprender *python* consegue ver quase imediatamente um ganho significativo na produtividade e na diminuição dos custos de manutenção.

O *Python* corre no Windows, Linux/Unix, Mac OS X, e também é suportado pelas maquinas virtuais de Java e .NET

O *Python* é de uso gratuito, mesmo para produtos comerciais, por causa da sua licença de código aberto aprovada pela OSI.

O *Python* atualmente vai na sua versão 3.

3 Aplicação de Segurança Informática

3.1 Sinopse

A aplicação de Segurança Informática implementada, trata-se de um *software* criado com o objetivo de fazer o processamento dos ficheiros de log das firewall, com o intuito de obter informações sobre tentativas de acesso, nomeadamente, listas de origem por pais, datas e horas das tentativas. A aplicação também foi desenvolvida com o objetivo de permitir detetar que portos de rede de várias máquinas se encontram disponíveis numa determinada rede local, e ainda que permita determinar que conexões se encontram ativas numa determinada máquina.

Esta aplicação foi desenvolvida para o uso em modo de linha de comando, contudo a mesma permite ao utilizador a produção de relatórios no formato PDF, ficheiros CSV com a informação de feedback devolvida pela aplicação e a criação de gráfico com a estatísticas do processamento do ficheiros de *log* da *firewall*.

Importa referir que para a implementação desta aplicação foi utilizada uma ferramenta que permite fazer a conexão de programas criados na linguagem de programação em C com uma grande variedade de linguagens de programação de alto nível, sendo a qual, nomeada de *Swig*.

3.2 Requisitos de utilização

Os requisitos de utilização para utilizar esta aplicação de segurança informática são os seguintes:

- O utilizador da aplicação deve ter o instalado no sistema operativo onde se prepara para fazer uso aplicação, a biblioteca PYFPDF[1] , trata-se de uma biblioteca que permite criar ficheiros PDF, logo permitiu criar os ficheiros PDF que a aplicação de Segurança informática disponibiliza ao utilizador.
- O utilizador deve ainda ter instalado no seu sistema operativo, a biblioteca *matplotlib[3]* , uma biblioteca que permitiu fazer a criação dos gráficos.
- Nmap é umaplicação que realiza portscanning. É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores numa rede de computadores. Existe uma versão para trabalhar com o python[6] , e realizar programas com esta característica.

3.3 Ligação entre o C e o Python (SWIG)

No desenvolvimento da aplicação de segurança informática, foi elaborado um método que faz a verificação de IP, ou seja, vai provar que a *String* que recebe pode ou não ser um IP,

devolvendo verdadeiro ou falso consoante a verificação elaborada. O Método vai ser usado na programação em *Python*, para a utilização desse método foi utilizada uma ferramenta nomeada de *Swig*. O *Swig* é uma ferramenta que permite fazer a conexão de programas criados na linguagem de programação em C com uma grande variedade de linguagens de programação de alto nível.

3.3.1 Processo de utilização do Swig

Após criar o código na linguagem de programação em C, que posteriormente vai ser utilizado na linguagem de programação em *Python*, existe um processo que tem ser elaborado sendo as principais fases as seguintes:

- Criar um ficheiro de interface;
- Compilar com o seguinte comandos:
  - #swig -python "Ficheiro interface";
  - #gcc "Ficheiro criado em C" -c -fPIC
  - #gcc "Ficheiro wrap.c" -c -fPIC -I/usr/include/python2.7
  - #gcc -shared "Ficheiro .o" "Ficheiro wrap.o" -ld -o "Ficheiro _nome.so"´
- Posteriormente já pode ser utilizada a função criada em C num módulo de Python.

Importa referir que, no desenvolvimento desta aplicação as compilações descritas anteriormente foram feitas através de um ficheiro nomeado "makefile", para tornar a compilação a mais simplificada possível.

3.4 Análise de ficheiros de Log da Firewall

Normalmente as firewall tem configurado um ficheiro de Log, que regista todas as tentativas de acesso anormais ao sistema. Nesse ficheiro consta o IP da máquina que tentou aceder, a hora e data da tentativa.

Tendo essa informação é possível utilizando a biblioteca “pygeoip”, interpretar o conteúdo do ficheiro, como por exemplo, devolvendo informação referente ao país de origem da tentativa de acesso.

Essa informação é armazenada para posterior criação de gráfico estatístico.

3.5 PortScanning

Um portscanning consiste na verificação de portos abertos numa ou mais máquinas presentes numa rede. Esse processo de verificação de existência de portos abertos, tenta ligar-se a um

determinado porto fazendo um “Syn” e esperando receber ou um “Akc” ou “Reset”. Todos os portos que não responderem, quer com uma afirmação ou com uma quebra de ligação ficam inconclusivos sendo impossível saber o seu estado.

Para realização desta tarefa é utilizada a biblioteca “nmap” para python. Esta biblioteca permite de forma automática, realizar tentativas de ligação fazendo a interpretação da informação dai recolhida. De entre a informação recolhida está disponível:

- Porto
- Estado
- Rasão do estado
- Protocolo utilizado pelo porto

3.6 Determinar conexões ativas numa determinada máquina

A determinação de conexões ativas numa máquina, consiste em verificar que serviços a mesma têm a correr e que estão visíveis do exterior. Esta técnica consiste à semelhança do portscanning, em verificar quais os portos ativos e quais os serviços que estão a correr nesses mesmos portos.

Para realização desta tarefa é utilizada a biblioteca “nmap” para python. Esta biblioteca permite de forma automática, realizar tentativas de ligação fazendo a interpretação da informação dai recolhida. De entre a informação recolhida está disponível:

- Porto
- Estado
- Rasão do estado
- Protocolo utilizado pelo porto
- Nome do serviço ativo

4 Estatísticas

4.1 Introdução

Nesta secção são apresentadas as estatísticas que aplicação de segurança informática permite apresentar ao utilizador consoante a opção que o mesmo escolher, opções já referidas anteriormente, como a análise de ficheiros de Log da Firewall, a deteção de portos de rede de várias máquinas se encontram disponíveis numa determinada rede local e determinar as conexões ativas numa determinada máquina. As estatísticas apresentadas podem ser as seguintes, a criação de ficheiro PDF, a criação de ficheiro CSV e a criação de gráfico.

4.2 Criar ficheiro PDF

A aplicação permita ao utilizador criar os ficheiros PDF, consoante o feedback que a mesma devolve ao utilizador, em qualquer uma das três opções que o utilizador tenha escolhido realizar, permitindo assim o mesmo verificar os resultados através do ficheiro PDF criado.

Para a criação do ficheiro PDF é utilizada a biblioteca PYFPDF. Os dados devolvidos pela aplicação são guardados numa lista, e através dessa lista são enviados os dados para o ficheiro.

Importa referir que foi criada uma classe PDF, de forma a facilitar a criação do ficheiro PDF.

4.3 Criar Ficheiro CSV

Após o utilizador escolher uma das três opções que a aplicação lhe permite fazer, a aplicação devolve um feedback, o mesmo pode ser enviado para um ficheiro CSV, de forma a facilitar o utilizador na análise dos dados recebidos.

O envio para o ficheiro CSV é feito da seguinte forma:

- São guardados os dados numa lista;
- É criado o ficheiro CSV;
- São enviados os dados da lista para o ficheiro.
- O ficheiro é guardado.

4.4 Gerar Gráfico

A aplicação permite ao utilizador gerar um gráfico, após o mesmo escolher a opção de analisar os ficheiros de *log* da *firewall*, o gráfico vai apresentar ao utilizador o número de

tentativas de acesso por país. Para a criação do gráfico foi utilizada a biblioteca *matplotlib*, como já referido anteriormente.

5 Conclusão

A versatilidade e facilidade de programação tornam a linguagem *Python*, uma das melhores escolhas quando se fala em realização de ferramentas de segurança ofensiva. A verificação dos portos e serviços que existem numa maquina, pode ser o ponto de partida para que se possa incrementar a segurança do sistema e impedir possíveis intrusões. A análise dos ficheiros log de uma *firewall*, são uma mais-valia para os utilizadores tentarem incrementar a segurança e mesmo mudar as políticas da firewall para evitar o acesso de pessoas estranhas no sistema.

6 Bibliografia

[1] **PYFPDF**, http://code.google.com/p/pyfpdf/, Abril de 2013

[2] **Swig**, http://www.swig.org/, Abril de 2013

[3] **Matplotlib**, http://matplotlib.org/, Abril de 2013

[4] **Python**, http://www.python.org/, Abril de 2013

[5] **Python-doc**, http://docs.python.org/2/tutorial/, Abril de 2013

[6] **Nmap,** http://xael.org/norman/python/python-nmap/