Detecção Remota de Vírus:

Implementação de Modulo para Software IPBrick

Pedro Miguel Pereira Serra

Faculdade de Engenharia da Universidade do Porto
Departamento de Engenharia Electrotécnica e de Computadores
Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

Dezembro de 2006

Ciência.Inovação 2010 Programa Operacional Ciência e Inovação 2010

Detecção Remota de Vírus:

Implementação de Modulo para Software IPBrick

Pedro Miguel Pereira Serra

Faculdade de Engenharia da Universidade do Porto
Departamento de Engenharia Electrotécnica e de Computadores
Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

Dezembro de 2006

Ciência.Inovação 2010 Programa Operacional Ciência e Inovação 2010

Detecção Remota de Vírus:

Implementação de Modulo para Software IPBrick

Pedro Miguel Pereira Serra

Trabalho realizado no âmbito da disciplina de:
Projecto Seminário e Trabalho de Fim de Curso
2º semestre de 2005/2006
Licenciatura em Engenharia. Electrotécnica e de Computadores

Orientação:
Prof. Dr. Raul Oliveira
Eng Hélder Rocha

Faculdade de Engenharia da Universidade do Porto
Departamento de Engenharia Electrotécnica e de Computadores
Rua Roberto Frias, s/n, 4200-465 Porto, Portugal

Dezembro de 2006

Ciência.Inovação 2010 Programa Operacional Ciência e Inovação 2010

Resumo

O presente trabalho tem como objectivo desenvolver uma aplicação de detecção de vírus numa rede, através de um servidor de serviços de redes desenvolvido pela iPortalMais: a IPBrick.

Pretende-se fazer uma análise viral a uma rede de forma rápida, de modo a conseguir uma ferramenta importante para avaliar o nível de segurança e uma mais valia para a protecção de dados de uma empresa.

Esta aplicação pretende criar uma maior abrangência na abordagem de segurança deste produto da iPortalMais, permitindo facilmente a entrada na rede como servidor ou cliente e, através de uma única máquina fazer uma análise a todos as máquinas que correm o sistema operativo Microsoft Windows.

O motor de análise viral utilizado é um dos mais conceituados antivírus internacionais, desenvolvido pela Kaspersky Lab e introduzido em Portugal através da iPortalMais. Este antivírus têm as melhores taxas de detecção de todos os softwares antivírus, e pode servir-se desta ferramenta para ganhar mercado no nosso país.

Abstract

The present report intends to develop a tool for virus detection on a network, through a intranet server developed by iPortalMais.

It is intended to obtain the capacity of making a fast viral analysis to a network, to evaluate the level of security. That, as a protection analysis or for an extra value confirmation for the network security.

This application intends to create an improved and including way of looking at this iPortalMais product, allowing IPBrick to register into a network and macking a vírus scan to all the machines in it.

The main vírus engine of this project is the highly appraised international antivírus developped by Kaspersky Lab and introduced in Portugal by iPortalMais. This antivírus usually gets the best detection rates on the comparative tests, and can find on this new tool a way of getting into new markets, especially the portuguese one, in which he is relatively unknown.

Prefácio

Este projecto foi desenvolvido nas instalações da iPortalMais, na cidade do Porto, desde o inicio de Março de 2006.

O trabalho foi realizado em colaboração com os engenheiros da empresa, ligando a parte de desenvolvimento do software à área de segurança e antivírus Kaspersky. Existiu portanto uma forte colaboração e partilha de conhecimentos entre estes sectores, convergindo para um empenho global na segurança da solução IPBrick. Este companheirismo é, aliás, um espelho do bom ambiente que se vive nesta jovem empresa.

Durante a realização do trabalho houve partilha de informações com os técnicos centrais da Kaspersky Lab, com importância no desenvolvimento da aplicação, como também para futuros melhoramentos do Kaspersky antivírus para Unix.

Á minha bicicleta,

que me acompanhou para o trabalho todos os dias

e me tem acompanhado sempre nas minhas deslocações.

Agradecimentos

A primeira palavra de agradecimento vai para a iPortalMais, por me ter recebido neste estágio e me ter dado a oportunidade e apoio para me desenvolver na minha área de estudos, especialmente por lidar com software livre. Claro que falo na empresa como todas as pessoas que para ela contribuem, sem excepção.

Destaco o apoio e disponibilidade dos mais próximos do meu trabalho como foram o Eng. Eduardo Maia e Eng. Miguel Ramalhão.

Foi um prazer reencontrar e conhecer melhor o Sérgio Mota e o André Dias, que acrescentaram energia positiva a este estágio. Um abraço!

Um agradecimento também à Kaspersky Lab por ter atendido com disponibilidade e empenho às minhas duvidas.

Por ultimo uma forte palavra de agradecimento aos meus orientadores Professor Raul Oliveira e Eng Hélder Rocha pela exigência e apoio que motivaram o meu empenho e o sucesso do projecto.

Índice

Resumo iii

Abstract iv

Prefácio v

Agradecimentos vii

Índice viii

Lista de Figuras x

Lista de Tabelas xi

1. Introdução 1

1.1 Motivação e Enquadramento 1

1.2 A Empresa 2

1.3 Objectivos 2

1.4 Estrutura do Relatório 3

2. Tecnologias e Ferramentas 5

2.1 Segurança 5

2.2 IPBrick 6

2.3 Kaspersky 8

2.4 Outras Ferramentas 9

3. Detecção de vírus Remotamente pela IPBrick 11

3.1 Kaspersky para Unix 11

3.2 Olhar a Rede 12

3.3 Base de Dados 14

3.4 Processo de Scan 15

3.5 Questões de Segurança 15

4. Implementação 17

4.1 Configuração do Kaspersky 17

4.2 Desenvolvimento 18

4.3 Interface Web 19

5. Testes e Resultados 23

6. Conclusões e Perspectivas de Desenvolvimento 25

Referências Bibliográficas 26

Anexos 27

Lista de Figuras

Figura 1: Evolução de numero de vírus desde 1990..... 6

Figura 2: Modelo da base de dados..... 14

Figura 3: Diagrama de funcionamento da aplicação..... 18

Figura 4: Arquitectura do processo principal..... 19

Figura 5: Interface inicial do análise viral..... 20

Figura 6: Mostra das opções escolhidas para confirmação..... 20

Figura 7: Estatistica do scan total..... 21

Lista de Tabelas

Tabela 1: Taxas de detecção de software Antivírus..... 8

Tabela 2: Comparativo detelhado..... 9

Tabela 3: Retalho do ficheiro de configuração do Kaspersky kavscanner..... 11

Tabela 4: Ficheiro log do kavscanner..... 12

Tabela 5: Comando e resultado do smbclient..... 13

Tabela 6: Output do nmap..... 13

Tabela 7: Ficheiro de configuração modificado..... 17

Tabela 8: Teste à variação de velocidade com variação de hardware..... 24

Tabela 9: Resultado do scan total a três máquinas..... 24

Capítulo 1

1.Introdução

1.1 Motivação e Enquadramento

Com o crescente desenvolvimento da tecnologia em plena era de um mundo mais globalizado, a dependência dos sistemas informáticos torna-se cada vez maior. Com esta dependência surgem também maiores riscos de ataques e, consequentemente, maior necessidade de soluções que dêem garantias às organizações.

Crescem as preocupações a nível internacional relacionadas com a segurança informática, motivando a criação de grupos dedicados à investigação nesta área. O crime é um elemento indissociável principalmente da internet, assim como a internet é, cada vez mais, uma ferramenta indispensável a qualquer empresa. Exemplo dessa preocupação é o recente protocolo realizado entre a Microsoft e o Governo português, tendo em vista um maior apoio desta empresa em termos de soluções de segurança.

Os custos associados à interrupção de funcionamento de uma empresa são habitualmente muito altos, tornando a questão da segurança uma das questões mais importantes no quotidiano organizacional.

A iPortalMais desenvolve soluções seguras e vocacionadas para o utilizador, com forte componente de protecção e recuperação. A solução IPBrick para intranet, sendo famosa pela sua capacidade de recuperação de acidentes, procura com este projecto criar uma mais valia na prevenção, acrescentando um modo de análise viral rápido a toda a rede na qual existir ou se inserir uma IPBrick.

Esta aplicação que se pretende desenvolver, acaba por ser uma mais valia não só em termos de segurança preventiva, mas também como difusora da alta taxa de detecção que o Kaspersky Antivírus tem demonstrado, que ainda é pouco conhecido em Portugal.

1.2 A Empresa

Festejou durante o periodo de estágio o seu 6º aniversário, a iPortalMais está de parabéns pelo seu desenvolvimento e inovação em termos tecnológicos.

É uma empresa que opera nas diferentes vertentes das redes de comunicações. Projecta e implementa redes estruturadas (parte passiva e parte activa); instala e configura os serviços fundamentais de uma Intranet (correio electrónico, Áreas de trabalho com sistemas de Backup, Impressão, Web interno e externo, etc); concebe e desenvolve aplicações Web para a Intranet e Internet.

As soluções de engenharia desenvolvidas pela iPortalMais são sempre que possível suportadas em ferramentas de software livre (Linux, Apache, Samba, Qmail, PHP, PostgreSQL, etc), permitindo-nos satisfazer os requisitos de operação de clientes, ao mesmo tempo que se conseguem preços extremamente competitivos, quando comparados com as soluções standard do mercado.

Recentemente mais activa a nível de exposições e feiras de tecnologia, a iPortalMais tem crescido não só em Portugal mas também em países desde a Noruega até Cabo Verde. Por isso tem merecido destaque em diversos jornais e revistas da imprensa nacional.

Destaque para a recente participação na maior feira de tecnologia do mundo, a CeBIT, na Alemanha.

A iPortalMais é uma das empresas portuguesas promissoras e um exemplo de dinamismo e inovação.

1.3 Objectivos

Neste projecto pretende-se desenvolver uma aplicação que permita a detecção de vírus remota, de toda uma rede.

Esta aplicação visa integrar o software IPBrick, sendo uma ferramenta importante na protecção , permitindo efectuar uma análise rápida a qualquer rede que conte com uma IPBrick, através do conceituado antivírus da Kaspersky Lab.

Esta ferramenta pretende ser uma mais valia não só a nível da protecção mas sambem a nível de divulgação das altas taxas de detecção do Kaspersky antivírus, que pretende ganhar mercado em Portugal.

No projecto está também inserida uma componente de investigação virada, não só para o antivírus, mas também para as ferramentas de protecção de redes de uma forma geral. Esta preocupação é devida à procura constante de melhoramento da IPBrick e do desenvolvimento desta a nível de segurança e prevenção.

1.4 Estrutura do Relatório

Este relatório encontra-se dividido em seis capítulos, estruturando o trabalho da seguinte forma:

O primeiro capitulo é uma introdução ao projecto na sua globalidade. No segundo capítulo é apresentada um descrição às tecnologias e ferramentas utilizadas, os motivos dessa escolha e uma análise as suas funcionalidades. O terceiro capitulo é uma abordagem à problemática de diversos aspectos do projecto, assim como análise das soluções passiveis e justificação das opções tomadas. O quarto e quinto capítulos descrevem o modo de implementação da aplicação e os testes e resultados obtidos. Finalmente um capitulo onde se analisam os resultados de forma conclusiva e se aborda o significado do trabalho no seu futuro desenvolvimento.

Capítulo 2

2.Tecnologias e Ferramentas

Este segundo capitulo é o resultado de uma fase inicial do estágio dedicada à pesquisa e investigação para tentar solucionar da melhor forma o problema proposto.

Abordam-se as tecnologias e ferramentas escolhidas dessa pesquisa, assim como a justificação, mais valias e problemas.

2.1 Segurança

Como já introduzido neste relatório, a segurança é o objectivo fundamental deste trabalho, mais concretamente a parte de prevenção e protecção. Tendo em conta a probabilidade de acontecer algum ataque ou acidente, pesado com os custos da corrupção ou perda de dados da empresa, esta área de trabalho é sem duvida crucial.

A abordagem do trabalho passou obrigatoriamente por uma análise do estado actual de segurança informática, dos vírus e ataques dos quais nos queremos proteger. Não foi surpresa que os ataques e infecções informáticas tivessem um crescimento enorme nos últimos anos, pois acompanharam o desenvolvimento e informatização das empresas com destaque para as novas tecnologias de redes e internet. Com este desenvolvimento cresceram também as soluções de antivírus e software de protecção contra ataques.

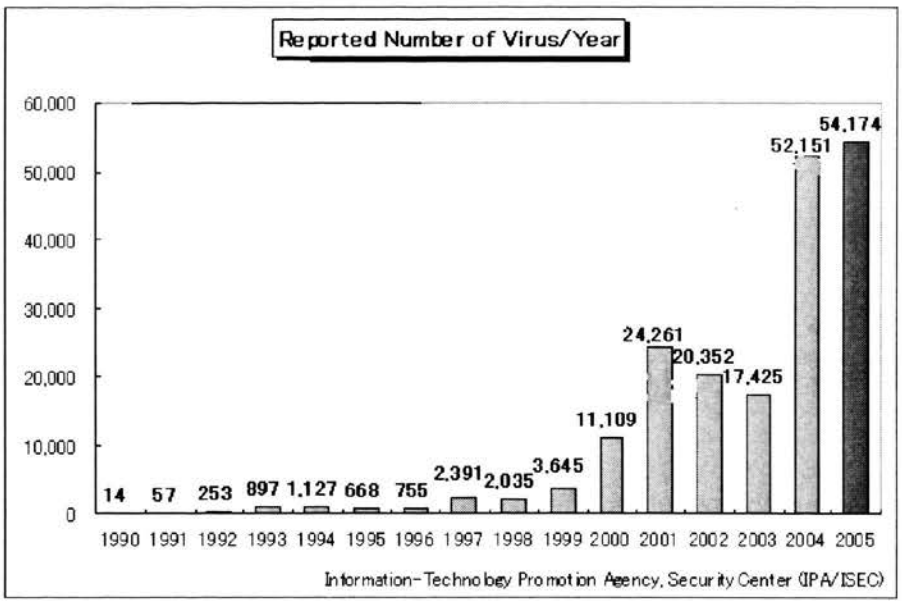

Figura 1: Evolução de numero de vírus desde 1990

Outra análise feita foi a das diferentes infecções nos diversos sistemas operativo. Da análise feita às principais empresas de antivírus, verificámos os vírus reportados por mês e os seus efeitos. De um estudo do mês de Dezembro de 2005, efectuado pela Sophos, podemos tirar a conclusão que raramente são reportados vírus para sistemas operativos de software livre e Mac.

O Microsoft Windows é o grande alvo dos ataques, não só por ser o sistema mais utilizado, mas também porque a sua politica de desenvolvimento de código fechado é um atraso à resolução de erros e falhas de segurança.

O Linux, em contrapartida, é um sistema muito mais seguro e preparado de base para funcionamento multi utilizador, além de ter um desenvolvimento de código livre que lhe permite corrigir erros de segurança de uma forma muito mais rápida.

Por este motivo, este trabalho é virado para a análise das máquinas com sistema operativo Microsoft Windows.

2.2 IPBrick

O projecto IPBrick é um desenvolvimento da iPortalMais.

O objectivo principal deste projecto é conceber servidores para Intranet e de Comunicações, simples de instalar e configurar. Para isso a IPBrick é gerida através de uma interface Web de utilização simples. Esta simplicidade deriva de

uma concepção da interface orientada para a função e não para os serviços de rede. Com isto consegue-se que empresas sem o mínimo conhecimento de redes possam configurar os seus servidores. O procedimento de instalação e recuperação seguem o mesmo princípio de simplicidade, bastando colocar o CD e uma Pen Drive na porta USB sendo quer a instalação inicial quer a recuperação da ultima configuração totalmente automáticas.

O modulo IPBrick.I é a especialização da IPBrick para Intranet. Este servidor está preparado para fornecer os serviços mais comuns de Intranet:

- Servidor de correio electrónico
- Agenda / Calendário (com partilha de informação)
- Servidor de áreas de trabalho individuais e de grupo (ficheiros) e Backup
- Servidor de domínio (compatível com Active Directory)
- Servidor de impressoras/fax
- Servidor de base de dados (PostgreSQL, MySQL)
- Gestor de projectos (dotProject)
- Servidor de imagens de estações de trabalho

O modulo IPBrick.C é uma especialização da IPBrick para Comunicações. Este servidor está preparado para fornecer os serviços mais comuns de Comunicações:

- Firewall e IDS (Intrusion Detection System)
- Controlo de conteúdos
- VPN com IPSec
- Servidor Web e FTP
- Relay de Correio Electrónico e Webmail
- Proxy HTTP/FTP com Estatísticas por utilizador
- Servidor de VoIP (usando protocolo SIP)

Além destes módulos de software, a iPortalMais apresenta diversos produtos IPBrick que incluem hardware e software, com especial destaque para o mais recente vertente, a IPBrick.GT, que complementa a solução de software IPBrick.IC com hardware seleccionado para permitir uma integração optimizada de voz e dados. A IPBrick.GT responde às exigências da integração necessária entre a telefonia tradicional, os novos telefones VoIP SIP e fornecedores de SIP. Implementa também um Gateway completo PSTN/VoIP, permitindo a ligação

directa ao PBX (RDIS E1/Bri e linhas analógicas), a operadores PSTN, à LAN da empresa e à Internet.

A IPBrick integra por defeito as mais actuais ferramentas de protecção de redes e antivírus da Kaspersky, ferramenta principal deste projecto.

2.3 Kaspersky

Fundada em 1997, a Kaspersy Lab é das mais conceituadas empresas de software de segurança informática. Tem sede em Moscovo, na Rússia, mas tem escritórios espalhados pelo mundo.

Os produtos Kaspersky recebem frequentemente prémios de publicações de tecnologia informática, entre os quais o estatuto de Gold Certified Partner status for Security Solutions. São também parceiros da SUSE e da RedHat Linux.

Muitas das funcionalidades de praticamente todos os programas de antivírus foram inventados pela Kaspersky Lab. Um grande número de fabricantes de software usam o "kernel" do Antivírus Kaspersky para soluções de segurança.

A Kaspersky Lab tem uma base de dados que é actualizada de três em três horas, o que torna possível neutralizar rapidamente os vírus mais recentes. No caso de um vírus novo ser detectado, a Kaspersky Lab garante o desenvolvimento de uma cura especial em 24 horas e entrega imediata para todos os utilizadores registados.

Em Portugal a iPortalMais é distribuidora e parceira da Kaspersky Lab, ganhando prémio de melhor lançamento de mercado em 2005 com o Kaspersky Antivírus.

As taxas de detecção do Kaspersky antivírus são desde há muito das melhores em diversos testes de detecção efectuados como se pode constatar:

6. Summary results

(a) Results over Windows viruses, Macros, Worms, Scripts and OtherOS detection:

1.	F-Secure*, Kaspersky, AVK*	99.9%
2.	McAfee	99.8%
3.	Symantec	99.7%
4.	NOD32	99.6%
5.	TrustPort*	99.1%
6.	F-Prot	98.1%
7.	AVIRA	97.9%
8.	BitDefender	97.7%
9.	Avast	97.3%
10.	Panda, Dr.Web	95.1%
11.	Norman	92.4%
12.	AVG	90.3%
13.	VBA32	80.5%

Tabela 1: Taxas de detecção de software Antivírus

Company		Kaspersky Labs		McAfee		ESET	
Product		**KAV Personal Pro**		**McAfee VirusScan**		**NOD32 Anti-Virus**	
Program version		5.0.391		10.0.21		2.51.20	
Engine / signature version		*N/A*		5.0.00 / 4690		1.1395	
Number of virus records		175.260		175.087		*unknown*	
On-demand detection of dialers (*)		*excellent*		*excellent*		*excellent*	
Certification level reached in this test		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**	
On-demand detection of virus/malware							
DOS viruses/malware	*231.088*	*231.029*	*99,97%*	*231.073*	*99,99%*	*230.399*	*99,70%*
Windows viruses	20.546	20.513	99,84%	20.501	99,78%	20.468	99,62%
Macro viruses	37.181	37.181	100%	37.180	100%	37.164	99,95%
Script viruses/malware	7.449	7.386	99,15%	7.201	96,67%	7.269	97,58%
Worms	23.398	23.294	99,56%	23.335	99,73%	23.288	99,53%
Backdoors	78.092	77.906	99,76%	75.786	97,05%	76.946	98,53%
Trojans	69.008	68.494	99,26%	63.569	92,12%	66.445	96,29%
other malware	5.912	5.788	97,90%	5.468	92,49%	5.100	86,27%
Other OS viruses/malware	2.085	2.065	99,04%	1.894	90,84%	1.843	88,39%
TOTAL	**243.671**	242.627	**99.57%**	234.934	**96.41%**	238.523	**97.89%**
Total with DOS viruses/malware	474.759	473.656	99,77%	466.007	98,16%	468.922	98,77%
On-demand detection of polymorphic viruses (**)			*99,4%*		*84,0%*		*94,3%*

Tabela 2: Comparativo detelhado

Na tabela 2 pode-se verificar um exemplo do brilharete dado pelo Kaspersky antivírus nos mais diversificados testes de detecção. Confirma-se ser um produto que pode e deve ganhar terreno no mercado português.

2.4 Outras Ferramentas

Além das principais bases de trabalho e ferramentas apresentadas, utilizam-se outras ferramentas que, ou por serem já sobejamente conhecidas ou por serem comandos mais básicos do sistema operativo, não serão abordadas ao pormenor. No entanto são mencionadas neste ponto para que fique o seu registo no relatório:

Como o trabalho tem a sua base em Unix/Linux, frequentemente se utilizaram comandos da shell, incluindo a ferramenta de escuta de rede "nmap" que nos permitiu detectar maquinas e o seu sistema operativo.

Outra ferramenta muito importante foi o Samba. Totalmente integrado na IPBrick, este software de comunicação entre sistemas operativos distintos, permitiu que se pudesse efectuar uma análise viral a máquinas com sistema operativo Microsoft Windows, a partir de uma aplicação em Linux.

Finalmente, para o desenvolvimento, utilizou-se o popular software livre php4 e PostgresSQL, que dispensam qualquer apresentação. Estas duas ferramenta s estão também completamente integradas na IPBrick, sendo também grandes participantes no desenvolvimento da própria IPBrick.

Capítulo 3

3.Detecção de vírus Remotamente pela IPBrick

Com os objectivos bem definidos e situados na tecnologia existente e adequadamente escolhida, abordam-se agora especificidades das questões e pontos críticos que se colocam para o desenvolvimento da aplicação de detecção remota

3.1 Kaspersky para Unix

A Kaspersky Lab disponibiliza inúmeras ferramentas de protecção para o sistema operativo Unix/Linux que já estão incluídas por defeito na IPBrick.

Na procura da ferramenta de analise viral mais adequada a esta questão, fizeram-se algumas análises a diversas ferramentas Kaspersky que possuíssem o modulo "*kavscanner*" - ferramenta de scan antivírus. A lógica seria utilizar o Kaspersky para Servidores Samba, mas, como o Kaspersky para Servidores de Email estava numa versão mais avançada, optou-se pelo mais recente, pois os motores de pesquisa são equivalentes.

Para configurar o *kavscanner* editamos o ficheiro de configuração deste, com uma estrutura idêntica à seguinte amostra:

```
[path]
BasesPath=/var/db/kav/5.5/kav4mailservers/bases
LicensePath=/var/db/kav/5.5/kav4mailservers/licenses
TempPath=/tmp
IcheckerDbFile=/var/db/kav/5.5/ichecker.db
[scanner.options]
Archives=yes
ExcludeDirs=
ExcludeMask=
Heuristic=yes
```

Tabela 3: Retalho do ficheiro de configuração do Kaspersky kavscanner

Este ficheiro de configuração é o que vai definir todas as opções de scan que vão ser usadas pelo *kavscanner* quando for iniciada a pesquisa. É necessário criar vários ficheiros de configuração para actuarem conforme a opção de scan que for escolhida (descrito mais à frente).

Depois de efectuada a pesquisa, o resultado do processo kavscanner é um ficheiro log que apresenta a estrutura seguinte:

```
[03/04/06 16:10:31 I] Kaspersky Anti-Virus On-Demand Scanner for Linux. Version 5.5.3/RELEASE build #100, compiled Jul 27 2005, 15:36:21
[03/04/06 16:10:31 I] Copyright (C) Kaspersky Lab, 1997-2005.
[03/04/06 16:10:31 I] Portions Copyright (C) Lan Crypto
[03/04/06 16:10:31 I] There are 1 Kaspersky license keys found:
[03/04/06 16:10:31 I] License file 000ffb3a.key, serial 0244-000400-000FFB3A, "Kaspersky Anti-Virus BO Suite European Edition. 15-19 Workstation / FileServer / MailServer 1 year Base Licence (Suite for Mail Gates)", expires 31-03-2007 in 362 days
[03/04/06 16:10:40 I] There are 174569 records loaded, the latest update 03-04-2006
[03/04/06 16:10:40 I] Config file: /etc/kav/5.5/kav4mailservers/kav4mailservers.conf
[03/04/06 16:10:40 I] The scan path: /homelocal/vírus_testes/
[03/04/06 16:10:41 A] /homelocal/vírus_testes/_____/VIRUS/Virus-corrupt/eicar.com CORRUPTED
[03/04/06 16:10:41 A] /homelocal/vírus_testes/Virus-curado/eicar.com INFECTED EICAR-Test-File
[03/04/06 16:10:41 A] /homelocal/VIRUS/Virus-deleted/eicar.com INFECTED EICAR-Test-File
[03/04/06 16:10:41 A] /homelocal/vírus_testes/_____/VIRUS/Virus-erro/eicar.com ERROR
[03/04/06 16:10:41 A] /homelocal/vírus_testes/VIRUS/Virus-suspeito/eicar.com SUSPICION EICAR-Test-File
[03/04/06 16:10:41 A] /homelocal/vírus_testes/VIRUS/Virus-warning/eicar.com WARNING EICAR-Test-File
[03/04/06 16:10:41 A] /homelocal/vírus_testes/sig ++`__^~^@_n@VIRUS/Virus-corrupt/eicar.com CORRUPTED
[03/04/06 16:10:41 A] /homelocal/vírus_testes/@@sig ----++`__^~^@_n@VIRUS/Virus-curado/eicar.com INFECTED
[03/04/06 16:10:43 I] Scan summary: Files=81 Folders=56 Archives=0 Packed=0 Infected=12 Warnings=6 Suspicios=6 Cured=0 CureFailed=0 Corrupted=12 Protected=0 Error=6 ScanTime=00:00:03 ScanSpeed=1.087 Kb/s
```

Tabela 4: Ficheiro log do kavscanner

Há que fazer um "parsing" a este ficheiro de forma adequada para poder colocar os dados estruturados numa base de dado, permitindo assim uma análise posterior mais específica.

3.2 Olhar a Rede

A primeira tarefa a ser feita na aplicação é definir as máquinas que vão ser pesquisadas. Para isso é necessário criar uma lista de máquinas disponíveis na rede, que pode ser obtida de diversas formas distintas: directamente das maquinas já registadas na IPBrick, através de uma escuta à rede com a ferramenta *nmap ou através da insereção manual das maquinas pretendidas.*

Através da IPBrick, obtemos directamente fazendo uma pesquisa à base de dados principal e copiando as máquinas para a nova base de dados dedicada ao

Kaspersky. Utilizando o nmap vamos fazer uma pesquisa na rede, a uma determinada gama de ip's definida para detectar as máquinas que estão ligadas.

Em qualquer dos casos é ainda necessária a identificação do sistema operativo das máquinas encontradas. Para isso utilizam-se duas ferramentas:

Se as máquinas são obtidas directamente da IPBrick, são sujeitas a um comando de samba que, devidamente interpretado, vai permitir identificar o sistema operativo dos terminais. Um exemplo do comando e do seu resultado estão na figura seguinte:

```
ipbrick:/homelocal/operador# smbclient -L //192.168.69.36 -U administrator
Password:
Domain=[IPORTALMAIS] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

    Sharename       Type     Comment
    ---------       ----     -------
    OFFICE11        Disk
    P$              Disk          IPC$          IPC      IPC remoto
    kav_isos        Disk
    d$              Disk
    c               Disk     nenhum de jeito \\\\_A
    updates         Disk
    C$$             Disk     hahahahahahahah :6
    KASPERSKY       Disk
    F$              Disk     Partilha predefinida
    ADMIN$          Disk     Admin remoto
    C$              Disk     Partilha predefinida
    vms             Disk
session request to 192.168.69.36 failed (Called name not present)
session request to 192 failed (Called name not present)
Domain=[IPORTALMAIS] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

    Server               Comment
    ---------            -------

    Workgroup            Master
    ---------            -------
```

Tabela 5: Comando e resultado do smbclient

Se, por outro lado, optarmos por uma detecção automática das máquinas através da escuta pelo *nmap*, interferiremos com determinadas portas (para nao tornar o processo lento) de forma a que quando se pesquisam as maquinas, se detecte logo o sistema operativo. O comando utilizado, assim como um retalho do resultado encontram-se de seguida:

```
#nmap -sT -O -p 22-25,53,110,137-139,143,4564
Interesting ports on 192.168.69.133:
Running: Microsoft Windows 2003/.NET|NT/2K/XP
Interesting ports on 192.168.69.176:
Running: Linux 2.4.X|2.5.X|2.6.X
Interesting ports on 192.168.69.180:
Running: Linux 2.4.X|2.5.X
...
Interesting ports on 192.168.69.192:
Running: IBM AIX 4.X, Microsoft Windows 2003/.NET|NT/2K/XP
```

Tabela 6: Output do nmap

Depois de detectadas as maquinas com sistema operativo pretendido, falta-nos identificar as partilhas de cada máquina. São essas partilhas que vão ser objecto de análise pelo *kavscanner*. Para isso, utilizaremos o resultado do comando *smbclient* já apresentado onde serão filtradas as partilhas administrativas. É então criada uma lista de partilhas que será tratada uma a uma pelo kavscanner do Kaspersky.

3.3 Base de Dados

Apesar deste projecto ser de utilização apenas indicativa e não necessitar guardar dados para futuras análises, é importante estruturar toda a informação quer de máquinas quer de detecções, para podermos fazer posteriores análises específicas

Por este motivo, para além do acesso à base de dados principal da IPBrick, criaram-se novas tabelas relativas a esta aplicação na base de dados já existente relativa a estatisticas de vírus do Kaspersky.

O modelo utilizado foi o seguinte:

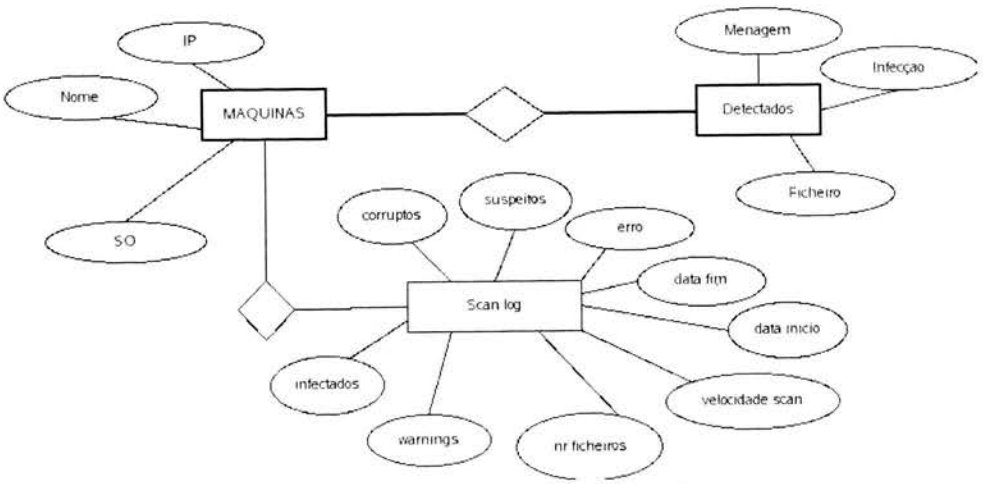

Figura 2: Modelo da base de dados

Baseado neste modelo, foram construídas as seguintes tabelas:

Máquinas (id, ip, nome, so)

Detectados (infecção, mensagem, localização)

Scan_log (n_ficheiros, n_infectados, n_corruptos, n_warnings, n_erro, n_suspeitos, n_pastas, velocidade_scan, data_start, data_fim)

3.4 Processo de Scan

A abordagem do processo de scan é possivelmente a questão mais crítica do projecto. Por um lado estamos interessados em obter o máximo de detecções possível, por outro quanto mais informação pretendermos mais demorado é o processo. Há que optimizar a análise para que seja o mais rápida possível. No entanto não podemos fugir a esta situação de ponderação entre a quantidade de informação a analisar e o tempo de scan necessário.

Para se contornar este problema é importante fazermos uma analise ao estado actual das infecções virais, assim como tipos de ficheiros e directórios com maior probabilidade de infecção. Com este conhecimento podemos definir características para o scan, de forma a que este esteja adequado ao tipo de rede a analisar.

A aplicação conta com três opções de scan distintas: rápida, geral e total. A primeira, definida como recomendada, faz uma análise muito especifica apenas aos directórios e tipos de ficheiros que são mais frequentemente infectados. O modo médio faz uma análise geral, mas exclui os ficheiros compactados, as imagens de cd e alguns tipos de ficheiros que não são tão facilmente infectados ou têm um tempo de scan demasiado grande. Finalmente a opção total proporciona uma análise global sem excepção, definida como não recomendada pois o tempo de scan pode tornar-se impraticável consoante a rede a ser analisada. No entanto pode ser útil para algumas situações especificas em que a pesquisa intensiva é necessária.

3.5 Questões de Segurança

Fugindo um pouco da análise viral mas com extrema importância para a realização do projecto temos as questões de autenticação e segurança da aplicação em si.

Ao longo do programa utilizam-se serviços que requerem autenticação de domínio ou de administrador de máquina, assim como há necessidade de correr serviços de sistema operativo com permissões de super utilizador.

Para resolver a questão de correr os serviços remotos como administrador, a aplicação oferece a possibilidade de inserir quer autenticação de domínio quer autenticação de administrador individual para cada máquina a analisar.

Outra questão surge devido à interface gráfica da aplicação ser uma interface web. Como utilizadores web temos por defeito permissões muito limitadas, quando é necessário correr serviços como super utilizador.

Para contornar esta questão utilizam-se as ferramentas da IPBrick já preparadas para correr serviços do sistema operativo com permissões ,de forma segura.

Capítulo 4

4.Implementação

Abordadas as questões de forma específica e separadamente por módulos, assim foi também construído o código abordando cada questão, para posteriormente ser tudo integrado na sua globalidade, na interface web estilo IPBrick.

Para além da programação inerente, têm relevância as modificações feitas aos ficheiros de configuração do Kaspersky, assim como as técnicas de fazer o scan escolhidas para os diversos modos de análise.

4.1 Configuração do Kaspersky

Apresentam-se de seguida as modificações feitas no ficheiro de configuração do Kaspersky para os diversos tipos de scan:

Para o scan total não ouve alterações. Todas as opções estava activadas.

Para o scan médio:

```
[scanner.options]
Archives=no
ExcludeDirs=
ExcludeMask=*.avi:*.AVI:*.mp3:*.MP3:*.txt:*.TXT:*.ISO:*.iso
Heuristic=yes
MailBases=yes
MailPlain=no
Packed=no
SelfExtArchives=yes
Ichecker=no
UseAVbasesSet=standard
[scanner.report]
Append=no
ReportFileName=/var/log/kav/5.5/kav4mailservers/onetimescan/kavscanner.log
ReportLevel=4
ShowOk=no
```

Tabela 7: Ficheiro de configuração modificado

De notar que na mascara de exclusão, temos que incluir a extensão em duplicado. Isto deve-se a estarmos num sistema operativo "case sensitive", enquanto o Windows não é.

Para o scan rápido utilizou-se também uma técnica diferente da do habitual scan. Técnica esta que permite concretizar o scan com uma funcionalidade que não é possível definir directamente no ficheiro de configuração. Utiliza-se um ficheiro de texto auxiliar onde se definem os directórios e os tipos de ficheiros a ser pesquisados, em vez da mascara de exclusão da pesquisa como existe no ficheiro de configuração. Assim, contorna-se a falta dessa funcionalidade do Kaspersky para Unix, executando várias vezes o kavscanner com argumentos diferentes. Este "truque" permite uma abordagem ao scan totalmente diferente, permitindo uma análise muito rápida. Apesar disto perde-se probabilidade de encontrar ficheiros infectados, como já foi discutido.

4.2 Desenvolvimento

Passando à arquitectura do código propriamente dita, a base do programa foi feita em php, utilizando a base de dados PostgresSQL.

Numa análise mais geral do programa, podemos dividi-lo em: detecção de máquinas, definição de opções, processo de scan, apresentação de resultados; como mostra o seguinte diagrama:

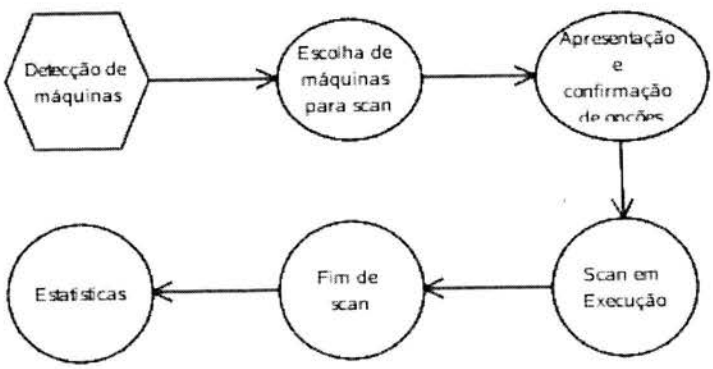

Figura 3: Diagrama de funcionamento da aplicação

O processo de scan é o "motor" do projecto e merece uma análise ao seu funcionamento. Apresenta-se de seguida a arquitectura deste processo.

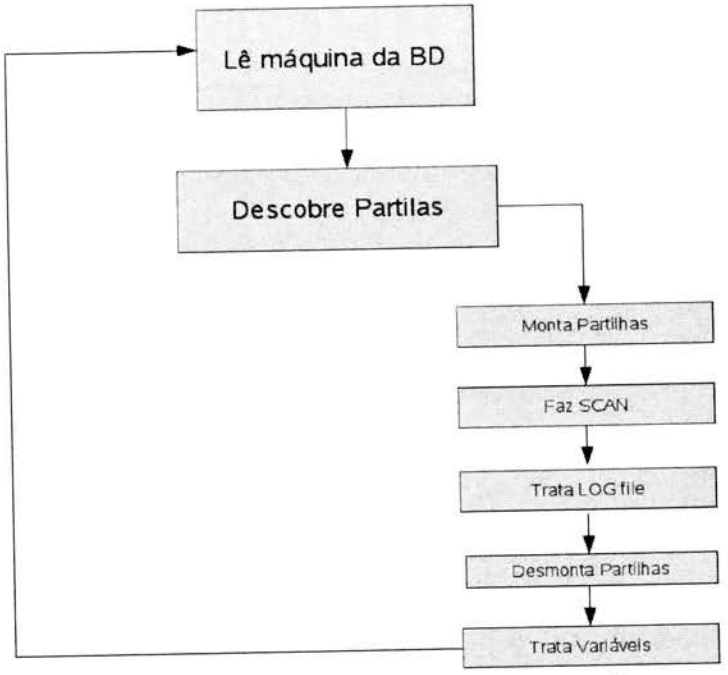

Figura 4: Arquitectura do processo principal

O código está organizado segundo a estrutura bem definida e estruturada da IPBrick, quer ao nível da abordagem do código em si, como da interface.

Finalmente é criado um log de todo o processo, que permite avaliar a evolução das tarefas e detecção de possíveis erros ou conflitos.

4.3 Interface Web

Além de estar assente num design já definido, o objectivo principal no desenvolvimento da interface gráfica web foi manter a intuitividade da utilização que a IPBrick proporciona ao utilizador, para que qualquer não técnico possa administrar a sua rede mas que permita todas as funcionalidades necessárias a um utilizador experiente.

As funcionalidades disponíveis são todas as necessárias à pesquisa viral de uma rede: pesquisa de máquinas, selecção de máquinas, opções de autenticação, começo ou paragem de scan, estatísticas globais e estatísticas por máquina.

De seguida uma visita guiada pelas funcionalidades e apresentação da interface criada:

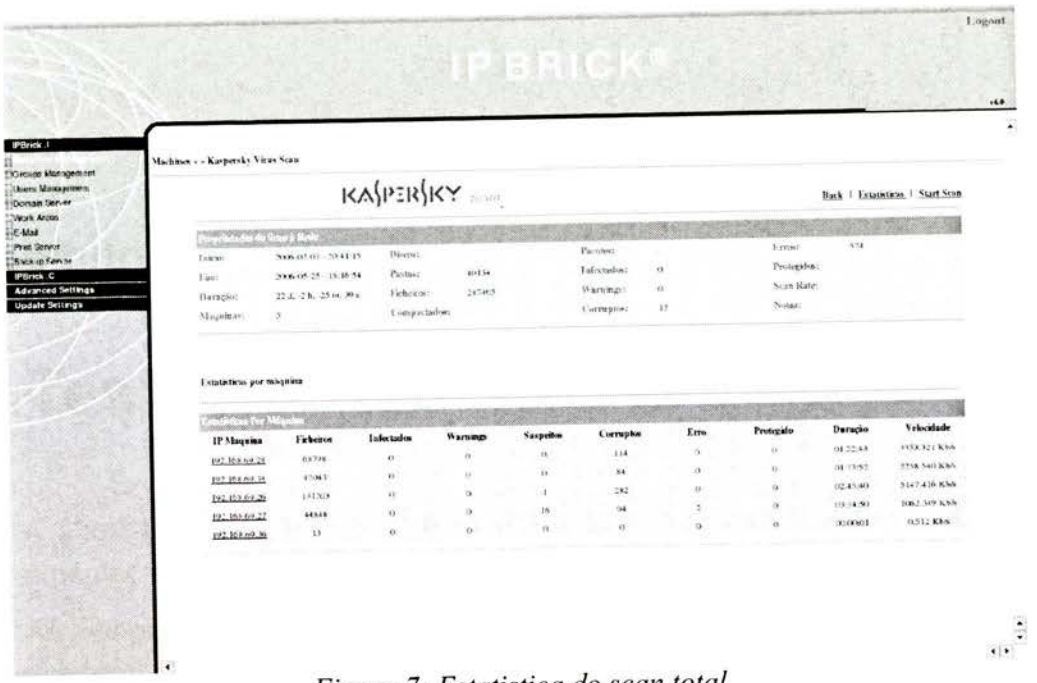

Figura 7: Estatistica do scan total

Na página de estatísticas temos uma tabela que faz um resumo geral das características do scan a toda a rede, onde averiguar número de ficheiros e pastas, numero de infecções, tempos, etc.

O IP das máquinas que sofreram análise são hiperligação para uma página idêntica a esta, mas relativa às infecções encontradas na máquina.

São apresentados detalhadamente cada ficheiro detectado com alguma infecção, erro, corrupção, aviso ou ficheiro suspeito.

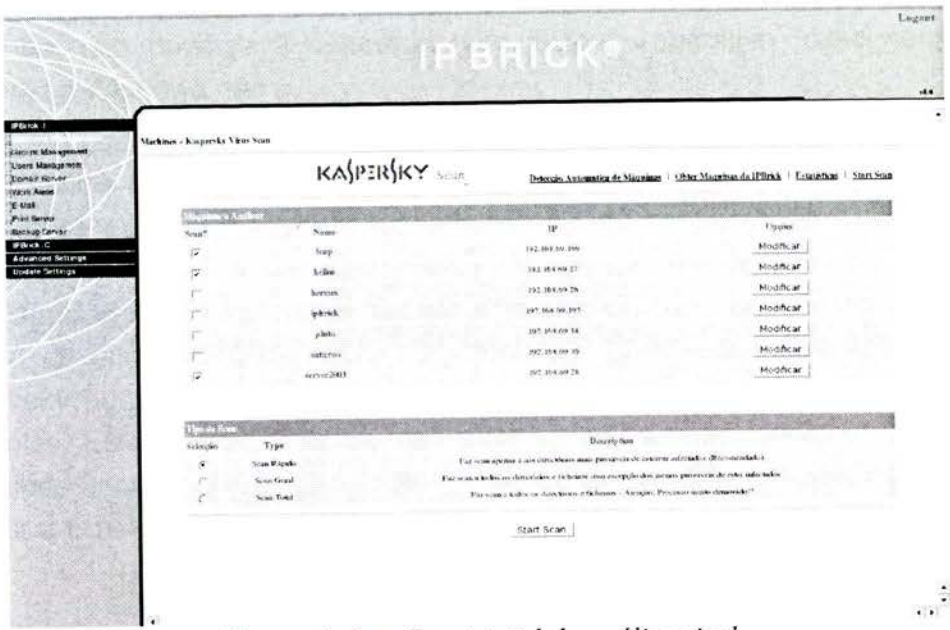

Figura 5: Interface inicial do análise viral

Inicialmente temos a listagem de máquinas, das quais podemos seleccionar as pretendidas e definir opções para cada uma delas. Podemos também escolher o tipo de scan que pretendemos.

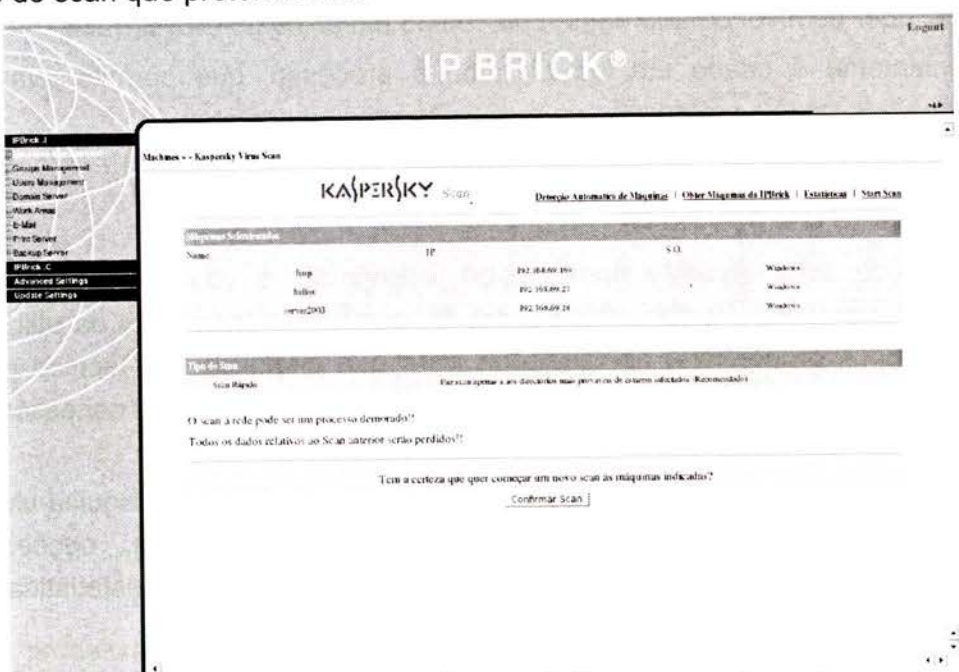

Figura 6: Mostra das opções escolhidas para confirmação

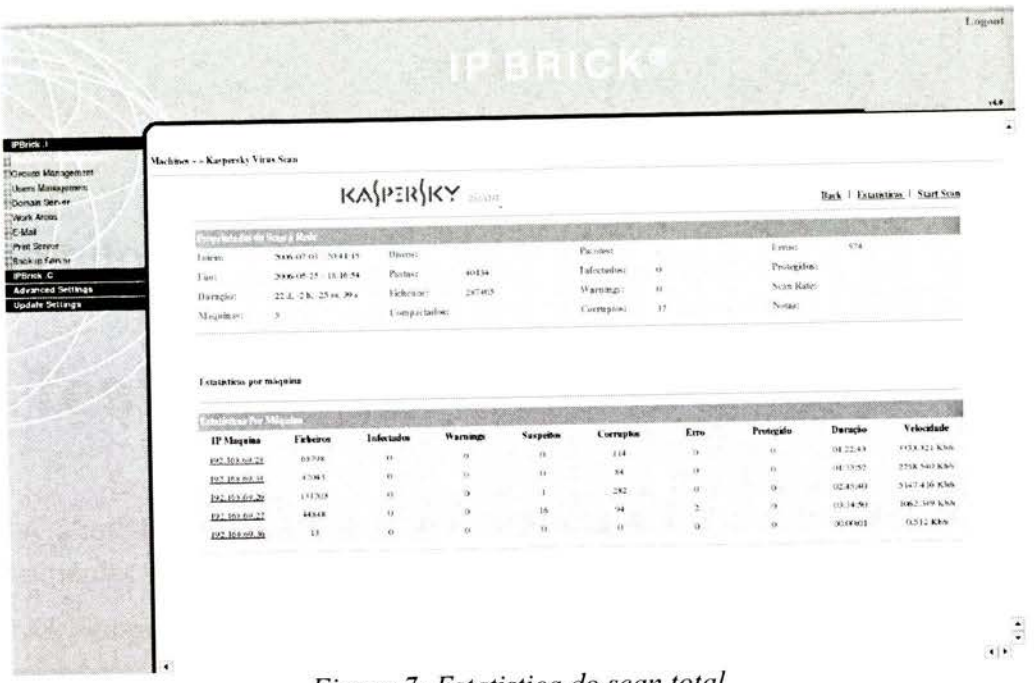

Figura 7: Estatistica do scan total

Na página de estatísticas temos uma tabela que faz um resumo geral das características do scan a toda a rede, onde averiguar número de ficheiros e pastas, numero de infecções, tempos, etc.

O IP das máquinas que sofreram análise são hiperligação para uma página idêntica a esta, mas relativa às infecções encontradas na máquina.

São apresentados detalhadamente cada ficheiro detectado com alguma infecção, erro, corrupção, aviso ou ficheiro suspeito.

Capítulo 5

5.Testes e Resultados

A abordagem dos testes foi feita em duas fases: testes parciais durante a implementação e testes específicos de análise viral.

Ao longo da implementação foi necessário efectuar diversos testes relacionados com as questões levantadas já no capitulo 3, de forma a construir uma aplicação final o mais compatível e imune possível a variações nos diversos tipos de redes.

Como exemplo, um dos conflitos encontrados foi relativo à utilização de caracteres portugueses no nome das partilhas, que altera a formatação do resultado do *smbclient* e "engana" a detecção de partilhas. A realização de testes a cada parte do programa tentando prever e criando situações diversas de análise permitiu construir a aplicação já preparada para uma diversidade de situações, como pretendido.

Mas os teste relativos ao tempo de scan é que se revelaram os mais críticos para o projecto. Em primeiro lugar porque os testes eram realizados durante a noite para não sobrecarregar a rede interferindo com o trabalho da iPortalMais. Em segundo lugar, porque os resultados se revelaram bastante fracos inicialmente.

Os primeiro testes de scan à rede de forma não condicionada não conseguiram tratar sequer um terminal passado 10 horas de scan. O problema identificou-se com algumas experiências de testes selectivos a pastas, nos quais se verificou que as imagens de CD contidas nessa máquina tinham um tempo de análise excessivo pois continham compactações dentro de compactações o que tornava uma tarefa ainda mais "pesada" para o processador.

Outra das situações que era de interesse testar era a dependencia do hardware, no processo de scan.

Os resultados da tabela que se segue sugerem também que a velocidade do processo não depende directamente da capacidade da máquina na qual esta a ser efectuado. Resultado importante e confirmado com mais alguns testes!

PENTIUM 3 550MHz 128RAM
720KB/s 5:27h para scan de 16GB (scan ao disco C e E do helios)
AMD ATHLON XP 1500+ 200RAM
482KB/s 8h para 16GB (scan ao disco C e E do helios)

Tabela 8: Teste à variação de velocidade com variação de hardware

Na segunda vaga de testes já se conseguiram obter resultados mais significativos. Os seguintes resultados foram obtidos, excluindo imagens e arquivos compactados da análise:

IP Maquina	Ficheiros	Infectados	Warnings	Suspeitos	Corruptos	Erro	Protegido	Duração	Velocidade
192.168.69.28	68798	0	0	0	114	0	0	01:22:43	3353.321 Kb/s
192.168.69.34	42043	0	0	0	84	0	0	01:33:52	2258.540 Kb/s
192.168.69.26	131703	0	0	1	282	0	0	02:45:40	5147.416 Kb/s

Tabela 9: Resultado do scan total a três máquinas

Estes resultados já foram mais satisfatórios, ainda assim, não eram viáveis para redes de maior dimensão. Foi então que se definiram outras hipóteses de scan menos exaustivas (mais rápidas) excluindo-se a análise a alguns tipos de ficheiros que não são habitualmente infectados. Assim já se conseguiu reduzir o tempo para valores a rondar a meia hora, para uma análise a 40GB. Claro que estes valores têm uma flutuação bastante grande conforme o conteúdo dos discos. Por isso definiu-se um novo mode de scan.

Este terceiro modo de análise que, em vez de colocar mascaras de exclusão, define os ficheiros e pastas a ser analisados (com a técnica explicada anteriormente), permitindo estabilizar o tempo para cada maquina como também diminuir muito o tempo de scan. O problema deste modo de análise é que tem uma capacidade de detecção duvidosa, sendo os testes pouco conclusivos relativamente a esse aspecto pois apenas se utilizou a "EICAR test file" e alguns virus copiados propositadamente para a rede interna.

Notaram-se também outras questões que influenciavam a velocidade de scan, como o pormenor do ficheiro de log do scan, que poderia atingir valores enormes se fosse demasiado pormenorizado, atrasando o acesso e consequentemente o scan.

Esta análise pemitiu optimizar o processo e ajustar os três modos de scan que o utilizador pode escolher, conforme a situação específica da sua rede.

Para além disso, caso seja desejável fazer uma análise mais intensiva, é sempre possível fazer um scan por partes, seleccionando algumas máquinas de cada vez, em vez de tentar fazer o scan da rede na sua totalidade de uma só vez. Esta opção permite uma grande flexibilidade e uma garantia que a aplicação pode funcionar em qualquer tipo de rede.

Capítulo 6

6.Conclusões e Perspectivas de Desenvolvimento

Neste trabalho foram estudadas formas de criar uma aplicação de análise de vírus numa rede, através da IPBrick.

Apesar das várias questões abordadas e das diversas dificuldades de um processo desta natureza, conseguiu-se criar uma ferramenta de segurança importante, sobre um sistema completo de serviços de redes que é a IPBrick.

Foi possível obter uma grande flexibilidade na aplicação final que permite, independentemente do tipo e tamanho da rede, optar por varias estratégias de scan. Além das três hipóteses para cada tipo de scan diferente, ainda há a possibilidade de seleccionar as máquinas a serem analisadas. Assim, no caso de ser uma rede muito grande, pode-se dividir a análise por fases.

Os principais entraves em gerir os vírus de uma rede através de uma maquina central são a enorme quantidade de recurso que os antivírus necessitam e o tempo necessário para a análise ser feita, estando de certa forma relacionadas.

A aplicação tem a particularidade de ser inserido na IPBrick que é um software português vocacionado para a segurança e facilidade de utilização, com qualidade de serviços. Este desenvolvimento da iPortalMais, além de ser uma ferramenta baseada em Linux, é um sistema operativo completo com todos os serviços necessários a uma rede empresarial.

Esta aplicação que se pretende desenvolver, acaba por ser uma mais valia não só em termos de segurança preventiva, mas também como difusora da alta taxa de detecção que o Kaspersky Antivírus tem demonstrado, que ainda é pouco conhecido em Portugal.

Este projecto tem a vantagem de lidar com um tema cada vez mais importante como é a segurança na informática empresarial.

Referências Bibliográficas

[EICAR, 2006] – *Instituto Europeu para Pesquisa de Antivírus de Computador*, 2006 [Em Linha]. Disponível em http://www.eicar.com . [Consultado em 07/04/2006]

[IPA/ISEC, 2006] – *Information-technology SEcurity Center*, 2006 [Em Linha]. Disponível em http://www.ipa.go.jp . [Consultado em 10/05/2006]

[Gilmore et al. 2006] Gilmore, W. Jason; Treat, Robert H. *Beginning PHP and PostgreSQL 8, From Novice to Professional.*

[Hughes et al. 2004] Hughes, Sterling; Zmievski, Andrei.*PHP Developer's Cookbook (2nd Edition)*

[SAMBA, 2005] Terpstra, John H. *Samba 3 by example.* Disponivel a partir de www.samba.org.

Anexos

Código do script principal da aplicação:

```
<?
include ("/opt/ipbox/serra/IfDBVirusScan.phpclass");

////////////////////////////////////////////// Variaveis Globais//////////////////////////////////////////////
//PREPARA FICHEIROS E DIRECTORIOS
if (!file_exists("/tmp/onetimescan")) exec("mkdir /tmp/onetimescan");  //cria directorio onde fica o scan do onetimescanner
exec("rm /tmp/onetimescan/*", $out, $erro); //remove os ficheiros do scan anterior
if (!file_exists("/mnt/onetimescan")) exec("mkdir /mnt/onetimescan");
$_kav_log_file = "/tmp/onetimescan/kavscanner.log"; //log por defeito do kavscanner
$_maqscan_log_file = "/tmp/onetimescan.log";

$_scan_pid_file = "/tmp/scan_pid_file.log";

////////////GET PROCESS ID FILE
$pid_scan = posix_getpid();
$ppid_scan = posix_getppid();
exec("rm $_scan_pid_file");
error_log ("$pid_scan\n$ppid_scan\n", 3, $_scan_pid_file);

function remove_duplicados ($array_inicial) {
array_change_key_case($array_inicial, CASE_LOWER);
$array_final = array_unique($array_inicial);
return $array_final;
}

                        $date=getdate();
                        $data_start = "$date[mday]-$date[mon]-$date[year]";
                        $hora_start="$date[hours]:$date[minutes]:$date[seconds]";

$estatisticas = new IfDBVirusScan (0);
if (!$estatisticas->ConnectDB1 ())
{
```

```
 die ("Error Connecting database!\n");
        error_log("erro ligando base de dados!!!!", 3, $_maqscan_log_file);
} else {
error_log (date("d-m-y/H:i:s",time())." -- NOVO SCAN --\ligaco BD efectuada, ...\n", 3,
$_maqscan_log_file);
}

$maquinas = $estatisticas->get_from_db ("SELECT * FROM maq_scan");
if isset($dom_password = $_REQUEST["dom_password"]);
if isset($dom_login = $_REQUEST["dom_login"]);

        foreach($maquinas as $maq){
                error_log ("TRATAR MAQUINA: '".$maq->ip_maq."' \n", 3, $_maqscan_log_file);

        if (isset($maq->login) && isset($maq->password )){
                $password = $maq->password;
                $login = $maq->login;
                }
        else {
                $password = $dom_password;
                $login = $dom_login;
                }

     exec("smbclient -L '".$maq->ip_maq."' -U $login%$password |grep  -Eo \"(\b[a-zA-Z]{1}[$]?)[ ]
*Disk\" |cut -b0-2", $discos);
                if (empty($discos)){
                        error_log (date("d-m-y/H:i:s",time())." - Nao foram encontrados discos na
maquina '".$maq->ip_maq."'\n", 3, $_maqscan_log_file);
                        continue;
                                } else   {

                $discos = remove_duplicados ($discos);
                $n_discos=count($discos);
                foreach($discos as $k => $disco){
                        echo "\$disco[$k] = $disco\n";
```

```
                if (!file_exists("/mnt/onetimescan/".$maq->ip_maq."")) exec("mkdir
/mnt/onetimescan/".$maq->ip_maq."");//crias dir, caso noa exista!
                if (!file_exists("/mnt/onetimescan/".$maq->ip_maq."/$disco")) exec("mkdir /mnt/one-
timescan/".$maq->ip_maq."/$disco");//crias dir, caso noa exista!
                        exec("mount -t cifs -o r,username=$login,password=$password //".$maq-
>ip_maq."/$disco /mnt/onetimescan/".$maq->ip_maq."/$disco 2>&1", $out, $erro);


                        if ($erro==0) {
                                echo "montado com sucesso: $erro\n";
                                $montado=1;  //cria a flag $montado q indica q hove sucesso
em pelo menos 1 disco!
                                error_log (date("d-m-y/H:i:s",time())." - Disco $disco montado
com sucesso! Codigo $erro  \n", 3, $_maqscan_log_file);
                        } else {
                        echo "erro na montagem: $erro\n";
                        error_log (date("d-m-y/H:i:s",time())." - Disco $disco deu erro de montagem!
erro= $erro  \n", 3, $_maqscan_log_file);
                                }
                                        }
                if (!isset($montado))
                        {
                                error_log (date("d-m-y/H:i:s",time())." - Nao foi possivel montar nen-
hum disco nesta maquina  \n", 3, $_maqscan_log_file);
                                unset($discos);
                                continue;
                        }
////////////////////////// FAZ O KAVSCANNER!!!!) //////////////////////////
                                error_log (date("d-m-y/H:i:s",time())." - SCAN EM
EXECUcaO..... \n", 3, $_maqscan_log_file);
                                echo "\n";
passthru("/opt/kav/5.5/kav4mailservers/bin/kavscanner -o /tmp/onetimescan/kavscanner.log -c
/etc/kav/5.5/kav4mailservers/onetimescan.conf /mnt/onetimescan/".$maq->ip_maq."");
                                error_log (date("d-m-y/H:i:s",time())." - SCAN FINALIZADO com
sucesso ◆maquina '".$maq->ip_maq."'\n", 3, $_maqscan_log_file);


                                if(!is_file("/tmp/onetimescan/kavscanner.log")) echo "aconteceu algum
problema!! o Scan nao gerou ficheiro!!";
                                error_log (date("d-m-y/H:i:s",time())." - A tratar log file '".$maq-
>ip_maq."'\n", 3, $_maqscan_log_file);
```

```
                                //TRATA FICHEIROS de LOG
                                if (file_exists($_kav_log_file)){
                                echo "ficheiro de log existe; $_kav_log_file\n";
                                $teste=trata_ficheiro_log($estatisticas);
                                } else {
                                echo "o ficheiro de log nao existe. kaspersky noa deve ter licensa!!!";
                                error_log (date("d-m-y/H:i:s",time())." - Ficheiro de log do kaspersky
nao existe!\n", 3, $_maqscan_log_file);
                                }
                                unset ($discos);
                                unset ($montado);
                                exec("mv /tmp/onetimescan/kavscanner.log /tmp/onetimescan/kavs-
canner".$maq->id_maq.".log");


                                exec("umount -f /mnt/onetimescan/'".$maq->ip_maq."'/*", $out, $erro);
                                error_log (date("d-m-y/H:i:s",time())." - Todos os discos desmontados
e variaveis reiniciadas para a proxima maquina - ou deviam estar :)  -  \n", 3, $_maqscan_log_file);
}
if (!$estatisticas->CloseDB ())
{
  die ("Error Closing database!\n");
  error_log (date("d-m-y/H:i:s",time())." ...Erro ao Fechar a BD...\n", 3, $_maqscan_log_file);
} else {
error_log (date("d-m-y/H:i:s",time())." ...Fechada a BD...\n", 3, $_maqscan_log_file);
}
exec("rm $_scan_pid_file", $out, $erro);
error_log (date("d-m-y/H:i:s",time())." - SCAN TOTAL FINALIZADO  \n", 3, $_maqscan_log_file);
?>
```

Função que trata o ficheiro log do Kaspersky:

```
<?
function trata_ficheiro_log($estatisticas) {
$fn = "/tmp/onetimescan/kavscanner.log";
$fp = @fopen ($fn, "r") or
die ("Nao consegue abrir a mer** do Ficheiro\n");


While ($line = @fgets ($fp, 1024)) {
$log_line = $line;
if (preg_match('/^\\[([0-9\/]{8}) ([0-9:]{8}) A]
(\/mnt\/onetimescan\/\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\/)([^\\t\\n].*?)\\t([^ ][A-Z]{4,9})\\t([^\\t\\n]+)?$/m',
$log_line, $match))
 {
$data = $match[1];
$hora = $match[2];
$localizacao = $match[4];
$infeccao = $match[5];
$virus = $match[6];
}
$insere=$estatisticas->insert_in_db("insert into detectados_scan(id_maq,ficheiro,infeccao,virus) val-
ues('".$maq->id_maq."','".$localizacao."','".$infeccao."','".$virus."')");
if ($insere == -1) {
        error_log (date("d-m-y/H:i:s",time())." Houve um erro na insere◆o na base de dados!! - \n",
3, $_maqscan_log_file);
 }
 } else if (preg_match('/\\[([0-9\/]{8}) ([0-9:]{8}) I]\\s+Scan
summary:\\s+Files=(\\d+)\\s+Folders=(\\d+)\\s+Archives=(\\d+)\\s+Packed=(\\d+)\\s+Infected=(\\d+)\\s+
Warnings=(\\d+)\\s+Suspicios=(\\d+)\\s+Cured=(\\d+)\\s+CureFailed=(\\d+)\\s+Corrupted=(\\d+)\\s+Prot
ected=(\\d+)\\s+Error=(\\d+)\\s+ScanTime=([0-9:]{8,9})\\s+ScanSpeed=(\\d+\\.\\d+\\s+\\w+\/s)/',
$log_line, $match)) {


 $data_end = $match[1];
 $hora_end = $match[2];
 $ficheiros=$match[3];
 $pastas = $match[4];
 $arquivos = $match[5];
 $compactados = $match[6];
 $infectados = $match[7];
```

```
$avisos = $match[8];
$suspeitos = $match[9];
$curados = $match[10];
$curafalha = $match[11];
$corruptos = $match[12];
$protegidos = $match[13];
$erros = $match[14];
$scantime = $match[15];
$scanspeed = $match[16];


        $infected = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='INFECTED'");
        $warning = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='WARNING'");
        $corrupted = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='CORRUPTED'");
        $error = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='ERROR'");
        $suspicion = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='SUSPICION'");


        $protected = $estatisticas->get_from_db("select count(*) from detectados_scan where
id_maq='".$maq->id_maq."' and infeccao='PROTECTED'");
        $insere=$estatisticas->insert_in_db("insert into
scan_log(id_maq,discos,n_ficheiros,n_pastas,n_infectados,n_warnings,n_corruptos,n_erros,n_sus-
peitos,n_protegidos,tempo_scan,scan_rate,data_end,hora_end,hora_start,data_start) values('".$maq-
>id_maq."','".$n_discos."','".$ficheiros."','".$pastas."','".$infected[0]->count."','".$warning[0]-
>count."','".$corrupted[0]->count."','".$error[0]->count."','".$suspicion[0]->count."','".$protected[0]-
>count."','".$scantime."','".$scanspeed."','".$data_end."','".$hora_end."','".$hora_start."','".$data_start."')
");
        if ($insere == -1) echo "erro na BD tabela scan_log \n";
}}
        @fclose($fp) or die("Nao consegue Fechar o Ficheiro de LOG!!");
return 1;
}


?>
```