PROPOSTA E IMPLEMENTAÇÃO DE UMA FERRAMENTA PARA GERÊNCIA DE SEGURANÇA EM REDES BASEADA NUMA NOVA METODOLOGIA USANDO ANÁLISE DE TRÁFEGO EM BACKBONES IP

Cláudia de Abreu Silva

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por:

Prof. Luís Felipe Magalhães de Moraes, Ph. D.

Prof. Luís Alfredo Vidal de Carvalho, D. Sc.

Prof. Márcio Portes de Albuquerque, D. Sc.

RIO DE JANEIRO, RJ - BRASIL

SETEMBRO DE 2006

SILVA, CLÁUDIA DE ABREU

Proposta e Implementação de Uma Ferramenta Para Gerência de Segurança em Redes Baseada Numa Nova Metodologia Usando Análise de Tráfego em Backbones IP [Rio de Janeiro] 2006

XV, 141 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. Segurança de redes

2. Visualização da segurança

3. Consciência do estado da segurança de rede

4. Netflow

I. COPPE/UFRJ II. Título (série)

Dedicatória

A meu marido, Valfran.
A meu filho, Vinícius.

Perdoem-me pela ausência.

Agradecimentos

Agradeço a Deus pela vida, saúde e pela ajuda na superação dos obstáculos apresentados na luta pelos meus ideais.

A meu marido, Valfran Nunes Pereira, pelo amor, apoio e compreensão durante um dos períodos mais difíceis de minha vida.

A meu filho, Vinícius Silva Pereira, que, mesmo com minha ausência, me proporcionou muito carinho, renovando minhas energias sempre que precisei.

A meus pais, Alberto Ferreira da Silva e Edyr de Abreu Silva, e toda a minha família que sempre me apoiaram e amaram incondicionalmente.

A meu orientador, Professor Luís Felipe Magalhães de Moraes, pela confiança, orientação e suporte em torno deste trabalho. Aos professores, Luís Alfredo Vidal de Carvalho e Márcio Portes de Albuquerque, que aceitaram prontamente participar da minha Banca Examinadora.

À Marinha do Brasil pela oportunidade e, especialmente, ao Exmo Sr. Almirante-de-Esquadra Aurélio Ribeiro da Silva Filho, que me apoiou incansavelmente na conquista da indicação para a realização do curso. Aos amigos da Marinha, pelo apoio e incentivo prestado.

Aos amigos do Laboratório Ravel, especialmente ao Bruno, ao Carlos Alberto e ao Paulo, pela ajuda na revisão deste texto, ao Diogo e ao Airon, pela ajuda na programação, à Michelini, pelo apoio prestado e a todos os meus irmãos Ravelianos, por todo companheirismo e experiências compartilhadas, pelos bons momentos e pelos momentos difíceis.

A todos aqueles que, de alguma forma, contribuíram para o fim desta jornada.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

PROPOSTA E IMPLEMENTAÇÃO DE UMA FERRAMENTA PARA GERÊNCIA DE SEGURANÇA EM REDES BASEADA NUMA NOVA METODOLOGIA USANDO ANÁLISE DE TRÁFEGO EM BACKBONES IP

Cláudia de Abreu Silva

Setembro/2006

Orientador: Luís Felipe Magalhães de Moraes
Programa: Engenharia de Sistemas e Computação

A análise de tráfego constitui um importante instrumento para a identificação de atividades maliciosas que vêm assolando as redes de computadores. Pragas digitais, também denominadas *worms*, têm sido ameaça constante na rede, provocando ataques avassaladores e coordenados com o intuito de sobrecarregar o tráfego nas redes locais e congestionar os enlaces da *Internet*. Trabalhos relacionados à aplicação do monitoramento voltado para a análise de segurança das redes foram realizados, adotando algoritmos e critérios de classificação baseados na variação do volume de tráfego, na variação do número de conexões abertas, na periodicidade de ocorrência de fluxos ou no conteúdo dos dados dos pacotes trafegados. Entretanto, nenhum deles consegue classificar, com eficácia e de forma imediata, as características das atividades de propagação dos worms.

O presente trabalho propõe uma nova metodologia para a identificação de atividades maliciosas, características da propagação de *worms* em redes de dados. Propõe-se o uso de um algoritmo que classifica e filtra o tráfego, com base nas informações contidas nos cabeçalhos dos fluxos trafegados e no conhecimento prévio das portas comumente exploradas por aplicativos maliciosos. A fim de validar a metodologia proposta, é feita a implementação do protótipo de uma ferramenta composta por módulos que efetuam a classificação, filtragem, registro do histórico das ocorrências e a apresentação visual dos eventos anômalos resultantes deste trabalho, em tempo próximo do real. Os resultados obtidos comprovaram o diferencial qualitativo positivo e inovador em relação aos demais trabalhos da literatura, possibilitando a adoção imediata das medidas necessárias para conter uma epidemia de *worms* em andamento. Destaca-se, ainda, a capacidade de mensurar o volume médio de tráfego oriundo de atividades de propagação de *worms* em uma rede *gigabit ethernet* acadêmica e de pesquisa e os benefícios obtidos com a visualização permanente dos eventos anômalos da rede, provenientes da propagação de *worms* e com o acesso imeditato aos registros de ocorrências.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

PROPOSAL AND IMPLEMENTATION OF A TOOL FOR MANAGEMENT OF SECURITY IN NETWORKS BASED IN A NEW METHODOLOGY USING ANALYSIS OF TRAFFIC IN BACKBONES IP

Cláudia de Abreu Silva

September/2006

Advisor: Luís Felipe Magalhães de Moraes
Department: Computer and System Engineering

Traffic analysis define an important instrument for identification of malicious activities that threaten computer network users all over the world. Worms have been a constant threat to networks causing coordinated, devastating attacks with the objective of overloading local area networks and Internet links. Works related to the application of traffic monitoring in network security analysis have been done, adopting algorithms and classification criteria based on traffic volume variations, variations in the number of opened connections, periodicity of flows occurrences or based on the data content in the packets composing network traffic. However, none of those could classify, fast and efficiently, the characteristics of worms propagation activities.

The present work proposes a new methodology to identify the characteristics of malicious worm propagation activities in a data network. It is proposed the use of an algorithm that classifies and filters network traffic, based on information contained in heading of the flow traffic and on previews knowledge of common exploited ports. In order to evaluate the work done, a tool was built implementing the proposed methodology. This tool is composed by modules that perform tasks like classification, filtering, registering and visual presentation of detected network anomalies in real time. The obtained results had proven the positive and innovative qualitative differential in relation to others works of literature, having made possible the immediate adoption of the measures necessary to contain a in progress epidemic of worms. It is distinguished, still, the capacity of measuring of traffic anomalies caused by worms propagation in a gigabit ethernet academic research network and the benefits gotten with the permanent visualization of the anomalous events of the net, proceeding from the propagation of worms and with the immediate access to the registers of occurrences.

Glossário

IP :	*Internet Protocol*;
TCP/IP :	*Transmission Control Protocol / Internet Protocol*;
API :	*Application Programming Interface*;
TAP :	*Test Access Port*;
SPAN :	*Switched Port ANalyser*;
BPF :	*BSD Packet Filtering*;
BSD :	*Borland* ;
PPP :	*Point-to-Point Protocol*;
SLIP :	*Serial Line Protocol*;
IPX :	*Internetwork Packet Exchange*;
SPX :	*Sequenced Packet Exchange*;
IETF :	*Internet Engineering Task Force*;
IPFIX :	*IP Flow Information Export* ;
RFC :	*Request-for-Comments*;

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Considerações Iniciais

A obtenção, o processamento e a distribuição da informação constituem o foco da evolução tecnológica ocorrida durante o século XX. Um marco significante nesta evolução foram as redes de computadores, que surgiram, inicialmente, em decorrência das necessidades de compartilhamento de recursos materiais, tais como impressoras, dispositivos de armazenamento de dados, entre outros.

Como evolução natural, utilizou-se a infra-estrutura das redes de computadores para o fornecimento de diversos serviços. A necessidade de acesso aos diversos serviços, mundialmente distribuídos, fomentou estudos para a interligação das redes de computadores e, na década de 70, deu-se o início da rede global de informações, a *Internet*.

Ao longo dos últimos anos, a *Internet* vem incorporando diversos serviços de suma importância para a sociedade. As empresas com o comércio eletrônico, os estudos acadêmicos e as pesquisas de âmbito mundial, a comunicação reduzindo fronteiras com as vídeo-conferências, a telefonia de voz sobre IP (*Internet Protocol*), os recursos de mensagens instantâneas e compartilhamento de arquivos, entre outros, representam serviços que fazem parte do cotidiano da atualidade. Ou seja, a evolução tecnológica, progressivamente, transformou as redes de dados em compo-

nentes heterogêneos, complexos e, infelizmente, vulneráveis a falhas.

Com o aumento da abrangência das redes de computadores, bem como o aumento da velocidade de transmissão e da capacidade de processamento das informações, a exposição das vulnerabilidades inerentes aos seus aplicativos aumenta em igual proporção a possibilidade de exploração dessas vulnerabilidades. Indivíduos mal intencionados, com uso de técnicas e aplicativos adequados, conseguem burlar a suposta segurança existente.

O número de vulnerabilidades relatadas na *Internet* cresce a cada ano, totalizando 26.713 de 1995 até o segundo trimestre de 2006, e estatísticas indicam que este crescimento tende a continuar. Em paralelo, o número de incidentes de segurança reportados cresce exponencialmente de 6 em 1988 para 137.529 em 2003 [11].

O grau de sofisticação das ameaças à segurança também está evoluindo. Pragas digitais, também denominadas *worms* (vermes), assumem o controle dos computadores pessoais, transformando inocentes usuários em propagadores inconscientes e ingênuos destes. As infecções de *worms* causam sobrecarga de tráfego nas redes locais e congestionamentos nos enlaces da *Internet*, gerando sérios prejuízos financeiros para as empresas. Estes ataques - avassaladores, coordenados, com o propósito de causar um efeito multiplicador em cascata - mudaram o cenário das questões relativas à segurança, gerando a necessidade do estudo de técnicas automáticas para a detecção destes eventos, a fim de minimizar o seu impacto nos serviços de rede.

1.2 Segurança em Redes

Uma rede idealmente projetada seria extremamente difícil de ser atacada tanto externa quanto internamente. Mas os projetos ideais não são práticos. Suas limitações criam muitas inconveniências para os usuários de uma maneira em geral, pois uma rede ideal nunca interagiria com sistemas não confiáveis. A realidade apresenta um cenário onde é necessário, freqüentemente, o acesso a recursos não confiáveis na própria rede ou remotamente, além do acesso externo, não confiável, aos recursos

internos da rede. As necessidades práticas freqüentemente geram um desequilíbrio entre funcionalidade e segurança. Conseqüentemente, a maioria das redes reais contém fraquezas. Sistemas com falhas em suas configurações e serviços executados desnecessariamente são os principais geradores de vulnerabilidades.

São utilizadas diversas tecnologias de fortalecimento da segurança das redes para minimizar os riscos apresentados. Busca-se utilizar um ponto onde os acessos externos e internos possam ser controlados, mediante a adoção de dispositivo que age como parede corta-fogo(*firewall*). Utiliza-se a restrição do acesso às redes baseadas na autenticação por usuário com o uso de equipamentos que agem como procuradores (*proxies*), recebendo as solicitações, autenticando o solicitante, realizando a consulta, e retornando o resultado da consulta ao solicitante. Utiliza-se endereçamento reservado nas redes locais e a tradução do endereço de rede (*Network Address Translator - NAT*) para a comunicação externa. Efetua-se a priorização do tráfego e a gerência da largura de banda disponível, mediante adoção de técnicas de qualidade de serviço (*Quality of Service - QoS*). Sempre que possível, busca-se, também, manter os dados seguros enquanto percorrem redes inseguras, através do uso de redes privadas virtuais (*Virtual Private Network - VPN*).

Diversos tipos de ataques em rede de computadores podem ser realizados explorando vulnerabilidades ou brechas nos sistemas computacionais e nas tecnologias de fortalecimento das redes, variando de simples tentativa de obtenção de informações, a sofisticados ataques visando obtenção do acesso privilegiado ao sistema. Somente o monitoramento adequado do tráfego pode determinar certos tipos de ataques em rede, pois desta forma é possível analisar o que realmente está acontecendo e não o que foi bloqueado por dispositivos de segurança. Fazendo-se uma analogia com o corpo humano, os dados que efetivamente trafegam na rede são equivalentes à corrente sangüínea. Como um exame laboratorial do sangue pode reportar doenças aparentemente inexistentes, a análise do tráfego pode fornecer a consciência do estado da segurança da rede.

Há uma variedade de tipos de ataques maliciosos contra ou através da rede.

Os ataques de negação de serviço (*Deny of Service - DoS*) e as epidemias de *worms* foram os mais notórios recentemente. O tipo mais popular de DoS ou DoS distribuído (DDoS) é o *flooding*, que simplesmente bombardeia uma vítima com pacotes além da largura de faixa ou da capacidade de processamento da vítima. Durante os meses de dezembro de 2005 e janeiro de 2006, foram reportados 1500 casos de ataques utilizando um novo método de negação de serviço distribuído onde são enviadas inúmeras requisições de consultas a servidores de domínio de nomes (*domain name system - DNS*) com endereço de origem forjado, apontando para o endereço da vítima [12].

Quanto à epidemia de *worm*, em termos de tráfego da rede, esta manifesta-se na forma de varredura de equipamentos (*hostscan*). Ao tentar infectar outros equipamentos, são realizadas varreduras em larga escala de endereços IP. Esta técnica também é utilizada por atacantes que buscam vítimas em potencial, geralmente para uma vulnerabilidade específica. Ataques recentes mostram que as técnicas utilizadas pelas primeiras epidemias como Code-Red [13], *Nimda* [14] e *SQL Slammer* [15], estão sendo aprimoradas. Na epidemia do worm *Witty* em março de 2004, apresentou-se o mais curto intervalo de tempo, de 24 horas, entre a divulgação da vulnerabilidade dos produtos de segurança do *Internet Security Systems* (*ISS*) e o inicio de sua proliferação, tendo atingido em torno de 12.000 equipamentos, após 45 minutos [16].

1.3 Motivação e Escopo

Nas tentativas de identificação de anomalias no tráfego da rede, os administradores de segurança contam com registros de ocorrências de ferramentas de segurança de rede, tais como *firewall* e listas de acesso. Porém, estes recursos não são eficazes na identificação do que está efetivamente acontecendo, uma vez que é feito o registro do que foi bloqueado, ou seja, do que "não aconteceu".

Em ambientes abertos, como redes acadêmicas e de pesquisa ou em uma infra-

estrutura de *backbone*, a restrição de acesso do usuário a aplicações nem sempre é uma opção. Conseqüentemente, a manutenção da segurança e o controle do uso dos recursos deste ambiente é não somente imprescindível, como também é uma tarefa extremamente difícil, uma vez que o volume de dados, observados e coletados durante o monitoramento da rede, tem aumentado substancialmente.

Neste contexto, a captura e a sumarização de todo o tráfego da rede compõem elementos essenciais para a análise e classificação de eventos anômalos na rede. Ferramentas de captura de tráfego tradicionais como o "Ethereal", "LANExplorer", "Trafshow" e outras, já não conseguem manipular, satisfatoriamente, grandes quantidades de informações a um custo viável e sem perda de pacotes. Elas também são ineficientes na identificação de comportamentos maliciosos devido a não interpretação das diversas informações inerentes a cada protocolo utilizado, muitas vezes limitando-se à análise do volume de dados trafegados.

Com o aumento de vulnerabilidades e demanda no uso dos recursos em rede, a administração da segurança da rede mostrou-se carente de ferramentas de apoio de tomada de decisão para ações de controle de incidentes em redes.

Diversas ferramentas populares de monitoração, baseadas em fluxos de dados de redes, tais como FlowScan [17], Netflow FlowAnalyzer [18] e AutoFocus [19], são utilizadas, basicamente, como analisadores de tráfego a fim de suprir a necessidade de gerência do desempenho da rede. Fornecem somente informações quanto ao número de pacotes trafegados e estados dos enlaces monitorados. Do ponto de vista da gerência da segurança das redes, estes recursos são muito limitados.

Atualmente, para que um gerente de segurança possa identificar uma anormalidade no tráfego de sua rede, é necessária a execução de diversos procedimentos, geralmente manuais, a fim de isolar as características dos problemas apresentados. Por exemplo, sendo um gerente de uma infra-estrutura de backbone, este deverá inicialmente identificar o tráfego de cada bloco de endereços IP no *backbone*, em seguida deverá identificar o protocolo e o sentido do tráfego anormal, identificar o serviço afetado para então tomar uma providência a fim de sanar o problema.

Algumas ferramentas de monitoramento de tráfego utilizam relatórios para a apresentação dos dados coletados, o que acarreta uma dificuldade maior na análise dos mesmos. Estudos realizados [20, 21] mostram que é possível apresentar inúmeros registros de dados em uma única cena visual sendo, assim, a percepção visual humana um eficiente meio de interpretação de um grande volume de dados.

Desta forma, torna-se necessário o estudo de novas metodologias para diagnóstico de alterações comportamentais do tráfego da rede, além de recursos para a interpretação de dados volumosos de tráfego de redes com a apresentação concisa de seus resultados com foco em segurança.

1.4 Objetivos

Com base nesta discussão, este trabalho objetiva a apresentação de uma nova metodologia de classificação e filtragem de tráfego, com foco na gerência da segurança de redes e baseada nas informações contidas nos cabeçalhos dos fluxos trafegados, identificando fluxos com atividades maliciosas, características das atividades de propagação dos *worms*.

Busca-se atingir os seguintes objetivos:

1 - Prover subsídios para a manutenção da segurança de redes em ambiente livre de restrições de acesso, tal como um ambiente acadêmico ou um *backbone*;

2 - Identificar atividades de pragas digitais (*worms*) em grandes volumes de dados trafegados;

3 - Não interferir no tráfego benigno;

4 - Apresentar visualmente o resultado das análises do tráfego classificado.

5 - Prover um histórico das anormalidades identificadas.

6 - Automatizar o processo de atualização de base de dados das portas de comunicação comumente utilizadas pelos *worms*.

7 - Automatizar os procedimentos adotados para a identificação dos autores do tráfego oriundo de atividades de propagação de *worms*.

Para tal, é proposto o uso de um algoritmo de classificação e filtragem do tráfego, fundamentado na interpretação das características das conexões e estados dos sinalizadores (*flags*) dos protocolos dos fluxos que trafegam na rede e nas portas de comunicação comumente utilizadas pelos *worms*.

1.5 Contribuições e Inovações

Um dos métodos mais utilizados para a caracterização do tráfego malicioso é o uso do modelo baseado no padrão de normalidade da rede. O tráfego, que for classificado fora deste escopo, será considerado como anômalo. Esta classificação se dá tanto quanto ao numero de sessões estabelecidas quanto ao volume dos dados trafegados.

Trabalhos, relacionados à aplicação do monitoramento voltado para a análise de segurança das redes, foram realizados [22, 4, 5, 23] adotando algoritmos e critérios de classificação de atividades maliciosas. Basicamente os estudos estão focados na análise da variação do volume de tráfego, na variação do número de conexões abertas, na periodicidade de ocorrência dos fluxos ou no conteúdo dos dados dos pacotes trafegados. Porém, estas metodologias não fornecem subsídios para uma reação imediata, necessitando de procedimentos manuais do gerente de segurança para a identificação do autor da anomalia. Nenhuma das metodologias tradicionais consegue classificar, com eficácia e de forma imediata, as características das atividades de propagação de *worms*, que consomem recursos preciosos da rede durante sua proliferação.

Diferentemente das propostas anteriores, esta dissertação propõe uma nova metodologia que permite a identificação de atividades maliciosas dos *worms* em redes de dados, em tempo próximo do real, com base nas informações contidas nos cabeçalhos dos fluxos trafegados, automatizando processos comumente praticados pelos

gerentes de segurança na tentativa de controle de incidente de atividades de *worms*, reduzindo, desta forma, o tempo de reação. O trabalho mostra como as informações inerentes da comunicação entre os equipamentos podem agregar valores às atuais técnicas de identificação de anomalias em rede. Utiliza-se o conhecimento prévio de portas comumente exploradas por aplicativos maliciosos e as informações contidas nos sinalizadores dos fluxos de dados que são acumulados e sumarizados por um mecanismo de captura de tráfego.

A fim de validar a metodologia proposta, é feita a implementação do protótipo de uma ferramenta composta por módulos que efetuam a classificação, a filtragem e a apresentação visual dos eventos anômalos resultantes desta classificação, em tempo próximo do real.

É feita a monitoração passiva dos dados capturados, oriundos do *backbone* da Rede Rio [24], que é uma rede *gigabit ethernet*, integrada por universidades e centros de pesquisa localizados no Estado do Rio de Janeiro.

Os resultados obtidos nos permite mensurar, em tempo próximo do real, o volume médio de tráfego oriundo de atividades de propagação de *worms* em um ambiente acadêmico e de pesquisa. Destaca-se, ainda, o benefício obtido com a visualização permanente dos eventos anômalos da rede, provenientes da propagação de worms e o acesso imeditato aos registros de ocorrências, proporcionados neste trabalho, que possibilita a adoção imediata de medidas necessária para conter uma epidemia de *worms* em andamento.

Em resumo, as contribuções deste trabalho podem ser traduzidas pelos cinco tópicos abaixo.

1. Proposta de nova metodologia que permite a identificação de atividades maliciosas dos worms em redes de dados, em tempo próximo do real;

2. Implementação de protótipo de uma ferramenta que classifica, filtra e apresenta visualmente os eventos anômalos resultantes da classificação, em tempo próximo do real.

3. Automação dos processos comumente praticados pelos gerentes de segurança na tentativa de controle de incidente de atividades de worms;

4. Fornecimento de informações estatísticas sobre o número de propagações detectadas, em tempo próximo do real, a fim de prover uma visão mais realística dos eventos de propagação de *worms* que diariamente ocorrem no *backbone*.

5. Alimentação automática da base de portas suspeitas, utilizada na assinatura do evento anômalo proveniente de propagação de *worms*.

1.6 Estrutura da Dissertação

O restante desse trabalho encontra-se organizado da seguinte forma. O Capítulo 2 apresenta a fundamentação teórica necessária para o entendimento deste trabalho. O Capítulo 3 apresenta o algoritmo proposto para classificação de tráfego malicioso. O Capítulo 4 apresenta a aplicação da metodologia ao monitoramento da segurança de redes. O Capítulo 5 apresenta os resultados obtidos na execução da ferramenta e, finalmente, no Capítulo 6 apresentamos as conclusões e os trabalhos futuros.

Capítulo 2

Fundamentação Teórica

Neste capítulo, é apresentada a fundamentação teórica necessária para a compreensão deste trabalho, o qual baseia-se na aplicação da análise de tráfego das redes de computadores para a classificação de fluxos, visando a detecção e visualização de atividades anômalas em andamento na rede. Os tópicos a serem abordados, ao longo do capítulo, abrangem os principais protocolos de rede utilizados, as técnicas de captura e análise de tráfego de dados e alguns padrões de anomalias afetos à segurança de rede de dados, comumente encontradas na *Internet*.

Os fundamentos das comunicações das redes de computadores sobre a *Internet* com base no modelo *Internet* TCP/IP, seus principais elementos e funcionalidades são mostrados na primeira parte da discussão deste capítulo. Posteriormente, são abordadas as principais técnicas utilizadas para o acesso e captura dos dados que trafegam na rede. Em seqüência, são apresentadas as vantagens e desvantagens dos métodos de análise, baseados em pacotes, em relação à análise baseada em fluxos. Por fim, são apresentados aspectos do comportamento dos padrões de anomalias dos *worms* e suas principais técnicas de varreduras.

2.1 Modelo *Internet* TCP/IP

Fruto da necessidade de compartilhamento de recursos, a rede de computadores surgiu como um conjunto de computadores autônomos capazes de trocar informações por meio de uma única tecnologia [25]. Inicialmente, restrições de ordem tecnológica e econômica e necessidades diversas resultaram em tipos de redes de computadores com topologias e soluções proprietárias. A solução encontrada para resolver os problemas de conexão entre redes diferentes foi a adoção de padrões. A partir de então, os sistemas que respeitassem um determinado padrão poderiam interagir cooperativamente, compartilhando dados e funções entre si.

Na *Internet*, que é uma rede de computadores mundial, a comunicação entre os seus diversos elementos, tais como a solicitação de uma página *Web* e a respectiva resposta, é apresentada de forma transparente para o usuário final. Esta comunicação só é possível porque estes equipamentos cumprem determinadas regras pré-estabelecidas. Os "protocolos" fornecem estas regras por meio de um método padrão para a troca de mensagens, definindo os formatos das mensagens e as condições de manipulação de erros.

O *Internet Engineering Task Force* (*IETF*) [26] é uma comunidade aberta internacional de especialistas da área de rede de dados (projetistas , operadores, fabricantes e pesquisadores) preocupados com a evolução da arquitetura e a operação da *Internet*. Esta comunidade é responsável por manter a especificação oficial do *Internet Protocol* (IP) e do *Transmission Control Protocol* (TCP), por intermédio de recomendações RFC (Request for Comments).

Uma das pilhas de protocolos mais utilizada para interconexão em redes de computadores na atualidade é conhecida como pilha TCP/IP (*Transmission Control Protocol/Internet Protocol*).

O modelo *Internet* TCP/IP recebe esta denominação devido aos seus dois principais protocolos: o *IP* mantido sobre o RFC 791 [27] e o protocolo *TCP* mantido sobre o RFC 793 [28].

O entendimento do funcionamento do modelo TCP/IP é necessário neste trabalho para a compreensão de algumas técnicas utilizadas por ferramentas maliciosas no ambiente da rede de dados, que exploram o princípio de funcionamento dos protocolos para obtenção de informações de suas vítimas e para sua proliferação. As principais características da pilha de protocolos TCP/IP serão apresentadas a seguir.

Para reduzir a complexidade de projeto, as redes de computadores, em sua maioria, são estruturadas em camadas ou níveis, onde cada camada desempenha uma função específica dentro do objetivo maior que é a tarefa de comunicação. As camadas são construídas umas sobre as outras e cada camada oferece seus serviços para as camadas superiores, protegendo estas dos detalhes de como os serviços oferecidos são de fato implementados.

Existem dois modelos dominantes sobre a divisão dos protocolos em camadas. O primeiro foi proposto pela *International Organization for Standardization* (ISO), é conhecido como modelo *Open Systems Interconnection* (OSI) composto por sete camadas. O segundo modelo, mais adequado à realidade e utilizado pela *Internet*, designa a pilha de protocolos TCP/IP, que é a combinação de diferentes protocolos e normalmente representado por um sistema de quatro camadas: aplicação, transporte, rede e enlace/física [1]. Um esquema comparativo desses dois modelos é apresentado na Figura 2.1.

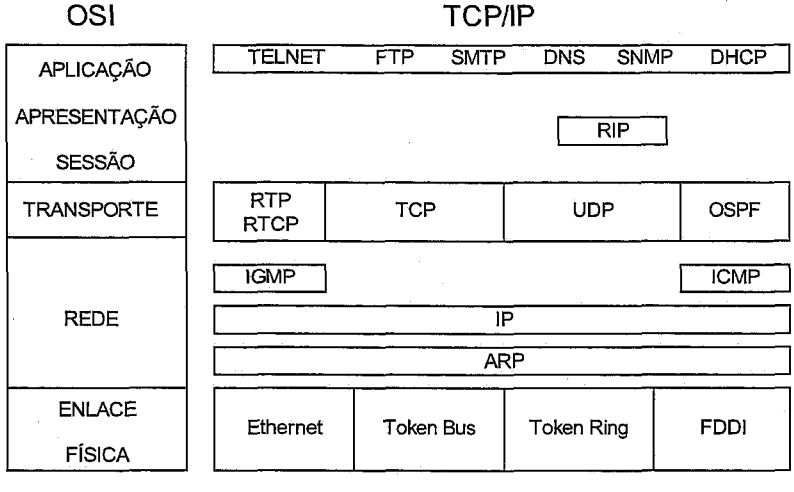

Figura 2.1: Os modelos OSI e TCP/IP.

A Figura 2.2 fornece um diagrama conceitual modelo *Internet* TCP/IP, representando ainda uma comunicação *Web* cliente/servidor.

O fluxo de dados, enviado por um computador, desce na sua pilha de camadas, trafega pela rede, chega ao computador de destino e ascende na pilha de camadas TCP/IP daquele. As linhas horizontais entre os computadores significam que cada camada interage com sua respectiva camada no outro computador, porém os dois computadores não interagem diretamente.

Quando um pacote com uma solicitação (requerimento de uma página Web por exemplo) é enviado, este percorre o caminho descendente na sua pilha e em cada camada é feito o "encapsulamento", ou seja, é acrescentado um cabeçalho contendo uma mensagem para cada camada no computador de destino, até chegar à respectiva camada da solicitante (servidor Web por exemplo), dando a impressão de que as camadas interagem diretamente.

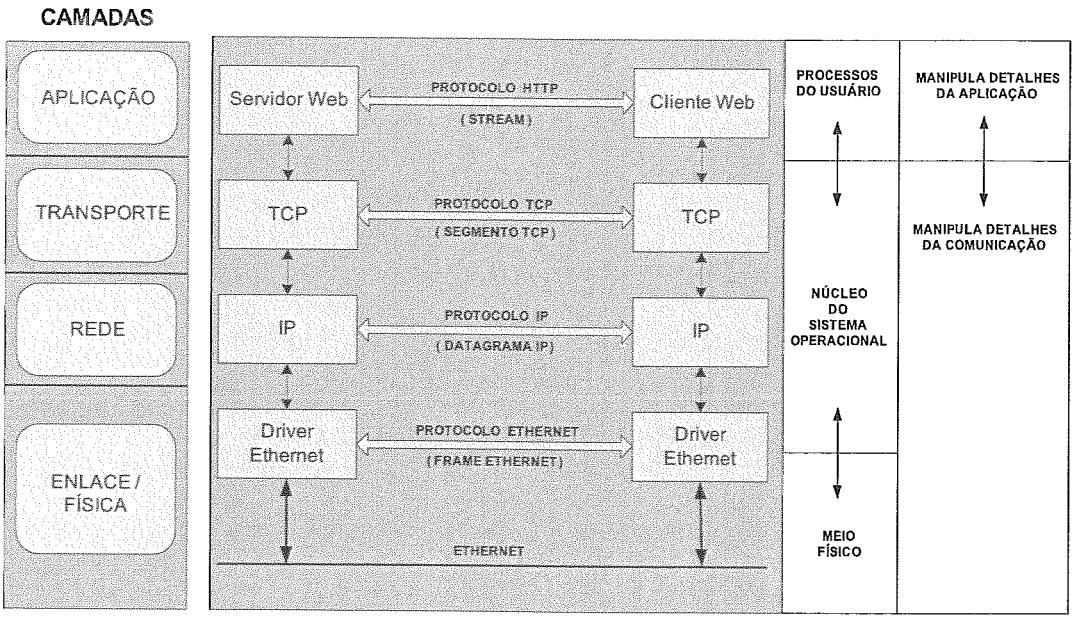

Figura 2.2: Modelo TCP/IP.

2.1.1 Endereçamentos Reservados

Devido à limitação de endereços IP válidos, e visando o aumento da segurança da rede interna, utiliza-se uma rede privativa, com blocos de endereços reservados descritos na RFC 1918. Para que os equipamentos das redes privadas possam interagir com uma rede pública, como a *Internet*, utiliza-se o recurso de tradução de endereço de rede (*Network Address Translation - NAT*) descrito na RFC 1631. Tipicamente, uma rede privada será configurada com endereços IP de um ou mais dos seguintes blocos de endereçamento:

10.0.0.0/8 (10.0.0.0 a 10.255.255.255)

172.16.0.0/12 (172.16.0.0 a 172.31.255.255)

192.168.0.0/16 (192.168.0.0 a 192.168.255.255)

Além dos endereços reservados para utilização em redes privativas, designou-se pela RFC1700, que o bloco de endereços 127.0.0.0/8 é limitado para uso interno do equipamento, na comunicação com as suas camadas superiores. Este endereçamento não é utilizado para o roteamento.

Os endereços reservados e de uso interno não podem ser utilizados para o roteamento global. A presença de tráfego com estes endereçamentos, em um ambiente de roteamento global, é um indício de comprometimento da segurança da rede, visto que pode ser oriundo da falha de configuração de equipamentos no que diz respeito à filtragem de pacotes, da falha do recurso de tradução de endereços (NAT) ou fruto de um ataque com endereçamento forjado.

2.1.2 Comunicação dos Processos em uma Rede

Nas aplicações em rede, os processos em diferentes hospedeiros se comunicam enviando e recebendo suas mensagens por intermédio de suas "portas", que podem ser vistas como uma via de acesso ao processo, agindo como interface entre a camada de aplicação e a camada de transporte.

Quando um processo quer enviar uma mensagem a outro processo em um outro hospedeiro, ele o faz enviando a mensagem através desta porta, entendendo que há uma infra-estrutura do outro lado da porta capaz de transportar a mensagem até a porta do processo de destino.

A fim de fornecer serviços para clientes desconhecidos, um número de porta de contato é definido.

Os números das portas são divididos em três faixas a saber:

- Portas de conhecimento geral - Estas portas são gerenciadas pelo *Internet Assigned Numbers Authority* (IANA)[29] e correspondem ao intervalo de 0 e 1023. Somente podem ser usadas por processos do sistema ou por programas executados por usuários privilegiados.
- Registradas - São as correspondentes ao intervalo de 1024 a 49151 e representam os serviços conhecidos. São utilizadas por processos ou programas executados por usuários não privilegiados.
- Dinâmicas (ou Privadas) - Correspondem ao intervalo entre 49152 até 65535. Estão disponíveis para o uso por qualquer aplicação na comunicação com qualquer outra aplicação.

Um *Socket* é a concatenação entre o endereço IP e uma porta de comunicação. Um par de *Sockets* identifica unicamente cada conexão numa rede. O *Socket* de envio é o endereço IP de origem mais número de porta de origem, enquanto o *Socket* de recebimento corresponde ao endereço IP de destino mais número de porta de destino.

Na maioria das implementações TCP/IP, um equipamento cliente aloca um número de porta entre 1024 e 5000, denominada efêmera (de vida curta). É dada esta denominação, pois, tipicamente, um cliente existe somente durante o tempo em que o equipamento necessitar do serviço do equipamento servidor. Em contrapartida, o servidor tem uma porta alocada por todo o período em que o servidor

estiver ativo e pronto para atender às solicitações.

2.1.3 Encapsulamento dos Dados

A idéia de encapsulamento é um dos conceitos mais importantes em TCP/IP. Cada camada acrescenta um cabeçalho que é usado para passar à respectiva camada da aplicação de destino, informações referentes aos dados transmitidos. Um esquema de encapsulamento é apresentado na Figura 2.3.

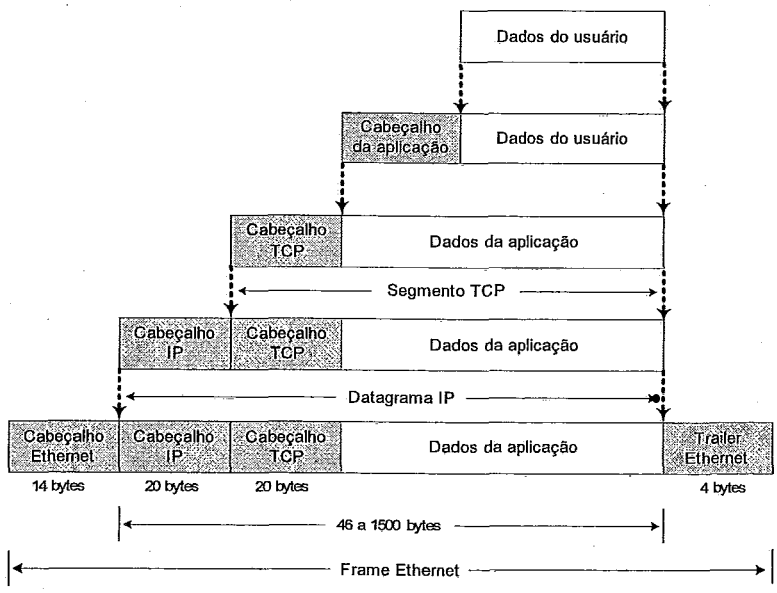

Figura 2.3: Encapsulamento de dados.

Do ponto de vista de segurança de redes, as informações disponíveis nos cabeçalhos são muito importantes. Os cabeçalhos fornecem informações sobre a origem e o destino, qual o protocolo utilizado, a qual serviço se destina o pacote, o sinalizador (*flag*) utilizado na comunicação, entre outros.

O campo de dados contém os dados transmitidos, de onde pode-se obter informações tais como senhas, endereços de correio eletrônico, arquivos transferidos, entre outros.

No Capítulo 3 é apresentado como o presente trabalho utiliza as informações contidas nos cabeçalhos dos pacotes, sumarizadas nos fluxos de dados, para efetuar

a classificação do tráfego capturado.

2.1.4 Camadas do Modelo TCP/IP

Como dito anteriormente, cada uma das camadas desempenha um conjunto de funções cruciais para que a comunicação ocorra.

Cada camada do modelo TCP/IP é responsável por:

`Aplicação`: Prover a interface com o usuário e o suporte a vários tipos de serviços como correio eletrônico, acesso remoto a arquivos, entre outros. São as aplicações que encaminham os dados a serem enviados ao outro equipamento, à camada de transporte, que por sua vez se encarrega de tratar adequadamente o envio até o destinatário. O envio dos dados realizado nesta camada é feito mediante o uso de protocolos específicos tais como o HTTP (*Hyper Text Transfer Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*) entre outros.

`Transporte`: Esta camada desempenha a importante tarefa de fornecer serviços de comunicação diretamente aos processos de aplicação, rodando em hospedeiros diferentes, ou seja, tem a responsabilidade da entrega de toda mensagem de um equipamento de origem ao destino, recebendo os dados da camada de aplicação e os encapsulando em segmentos, incluindo os cabeçalhos dos protocolos TCP ou UDP (*User Datagram Protocol*). Também faz parte desta camada o estabelecimento, gerenciamento e sincronismo das conexões entre o equipamento de origem e o de destino.

`Rede`: Responsável pela entrega de datagramas através de vários enlaces da rede. A camada de rede garante que cada datagrama saia de seu equipamento de origem para o de destino de maneira eficiente. Nesta camada destaca-se o protocolo IP que é utilizado para encapsular os protocolos da camada anterior e também os outros protocolos da camada de rede, tais como o ICMP, IGMP e RIP.

`Enlace/Física`: Coordenar as funções requeridas para transmitir um conjunto de

bits através do meio físico. Esta camada também é responsável pelas especificações mecânicas e elétricas, como conectores, cabos, sinalização que fisicamente ligam dois nós em uma rede, etc.

2.1.5 Informações dos Cabeçalhos

O presente trabalho baseia-se na premissa de que, a análise das informações contidas nos cabeçalhos dos protocolos das diversas camadas do TCP/IP, nos fornece subsídios suficientes para as tarefas de classificação e filtragem dos dados coletados no monitoramento de uma rede de dados, visando à identificação de tráfego malicioso.

Os cabeçalhos das camadas de aplicação e enlace/física são específicos para o tipo de aplicação utilizada (HTTP, TELNET, SMTP, FTP, TFTP, entre outros) e o *hardware* de rede utilizado no qual a máquina esteja conectada (Ethernet, Token Ring, FDDI, entre outros). Desta forma, serão detalhados, a seguir, somente os cabeçalhos e o princípio de funcionamento dos protocolos IP, TCP e UDP, que são os protocolos que fundamentam este trabalho.

Internet Protocol - IP

Essencialmente, os pacotes enviados sobre a *Internet* são pacotes IP. Desta forma, o IP é o protocolo fundamental da *Internet*, sendo utilizado para encapsular todos os outros protocolos das camadas superiores. O resultado deste encapsulamento é o que chamamos de datagrama IP.

O formato do datagrama IP está ilustrado na Figura 2.4.

TCP

O TCP provê uma comunicação entre aplicações, como se houvesse um circuito físico para tal; por este motivo, é chamado de protocolo **orientado à conexão.**

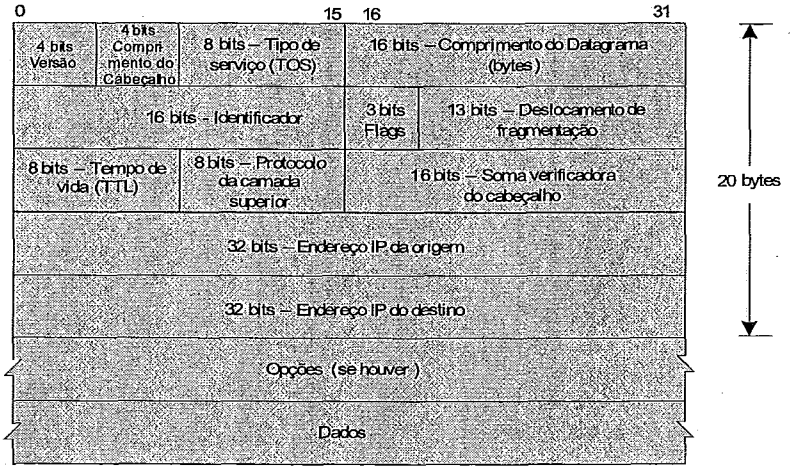

Figura 2.4: Datagrama IP, com destaque para o cabeçalho IP [1].

Ele realiza um procedimento de apresentação que faz com que o cliente e o servidor troquem informações de controle da camada de transporte, antes que as mensagens da camada de aplicação comecem a fluir. Após a realização da fase de apresentação, pode-se dizer que existe uma conexão TCP entre a porta do processo de origem e a porta do processo de destino. Esta conexão TCP é mantida até expirar o seu tempo ou até que um dos equipamentos (cliente ou servidor) termine a conexão.

Ao projetar-se uma aplicação, caso esta não tolere a incerteza do recebimento dos pacotes ou a possibilidade da entrega de pacotes em ordem diferente da enviada, deve-se optar pelo uso do TCP, pois este garante a confiabilidade da entrega dos pacotes na ordem correta através do uso dos seguintes mecanismos:

- Conexão exclusiva - Também chamada de conexão "*unicast*", onde a negociação de uma sessão única permite a ambos os lados rastrear o tráfego trocado entre os dois equipamentos.

- Seqüência numérica - Provê o senso cronológico dos dados enviados e recebidos, permitindo que os dados possam ser reordenados de forma correta.

- Confirmações de recebimento (Acknowledgements) - São utilizadas para acusar ao emissor o recebimento dos pacotes. Caso o emissor não receba a confirmação

de recebimento de determinado pacote em certo intervalo de tempo, ele assume que o pacote perdeu-se e o retransmitirá.

Para facilitar a comunicação, a mensagem a ser enviada é quebrada em pedaços gerenciáveis denominados *pacotes*. O cabeçalho do pacote é um pequeno segmento de informação localizado no início do pacote com a finalidade de prover sua identificação.

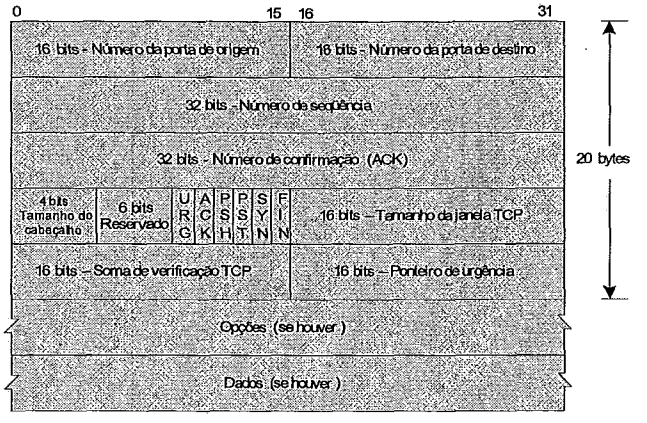

Figura 2.5: Segmentop TCP, com destaque para o cabeçalho [1].

A Figura 2.5 representa o cabeçalho TCP. Os campos do cabeçalho TCP mais importantes dentro do escopo deste trabalho são:

- *Porta de origem e porta de destino*: estes campos contêm os números de portas TCP que identificam os programas de aplicação dos extremos de uma conexão.
- *Número de seqüência*: identifica a posição no fluxo de *bytes* do segmento enviado pelo transmissor. O número de seqüência refere-se ao fluxo de dados que vai na mesma direção do segmento.
- *Número de Reconhecimento*: este campo identifica a posição do *byte* mais alto (ou último *byte*) que a origem recebeu. O número de reconhecimento refere-se ao fluxo de dados na direção contrária ao segmento. Os reconhecimentos sempre especificam o número do próximo *byte* que o receptor espera receber.

- *Sinalizadores (Flags)*: seis *bits* que determinam o propósito e conteúdo do segmento, codificado conforme a Tabela 2.1. Um ou mais deles podem estar ativos ao mesmo tempo.

A Tabela 2.1 enumera e apresenta a utilização dos sinalizadores do cabeçalho do TCP.

As informações contidas neste campo são primordiais para o estabelecimento, controle e encerramento da comunicação TCP

Sinalizador	**Utilização**
URG	Indicação de urgência de dados.
ACK	Confirmação de recebimento da dados
PSH	Indica que o dado deverá ser levado para a aplicação o mais breve possível.
RST	Indica que algo de errado aconteceu e a conexão será desfeita.
SYN	Usado para iniciar e sincronizar uma conexão. Os números de seqüência são sincronizados para que se saiba a ordem dos pacotes subseqüentes.
FIN	Usado para finalizar a conexão.

Tabela 2.1: Sinalizadores do protocolo TCP

O TCP utiliza uma técnica denominada "aperto de mão em três vias" ("three-way handshake") para o estabelecimento de uma conexão, que pode ser descrita da seguinte maneira:

Passo 1: A máquina, que deseja iniciar a conexão (denominado cliente e representado na Figura 2.6 pelo equipamento A), envia um pacote com o sinalizador SYN ativo e um número de seqüência aleatório "x", a fim de checar se a máquina de destino (denominado servidor e representado na Figura 2.6 pelo equipamento B) está pronta para o estabelecimento da conexão TCP.

Passo 2: B responde para o A, enviando um pacote com os sinalizadores SYN e ACK ativos, um número de seqüência aleatório "y" e número de confirmação "x+1".

Passo 3: Após o recebimento do pacote SYN/ACK, A envia para B um pacote com o sinalizador ACK ativo, número de seqüência "x+1" e número de confirmação "y+1" e estão concluídas as três etapas do procedimento e estabelecida a conexão entre as máquinas cliente e servidor.

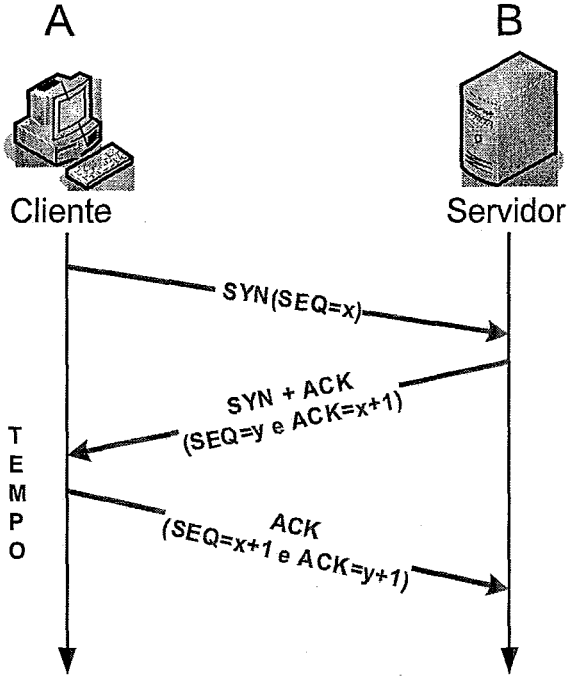

Figura 2.6: Estabelecimento de conexão TCP.

É possível que uma máquina servidora receba várias requisições de conexão na mesma porta, fazendo com que o TCP use sua funcionalidade de multiplexação de conexões para organizar as diversas conexões na mesma porta. O TCP/IP usa o conjunto de endereço IP e porta (*socket*) para identificar diferentes conexões com portas de destino e origem iguais, porém com endereços IP diferentes.

UDP

Este protocolo oferece um serviço de transferência de dados não confiável e sem controle de fluxo. Ele não depende do estabelecimento prévio de uma conexão para o envio das mensagens; conseqüentemente, quando um processo envia uma

mensagem para dentro de uma porta UDP de um processo em outro hospedeiro, não há nenhuma garantia de que a mensagem alcance a porta receptora.

Os campos contidos no cabeçalho UDP, apresentados na Figura 2.7, ajudam o sistema operacional dos equipamentos a identificar os processos comunicantes; os números de porta de origem e de destino são utilizados com esta finalidade.

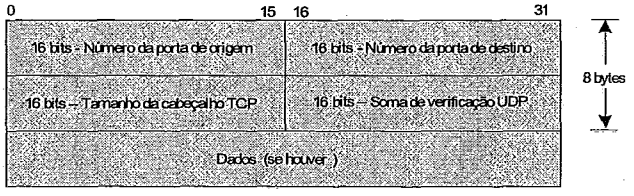

Figura 2.7: Cabeçalho do protocolo UDP.

2.2 Mecanismos de Captura do Tráfego

2.2.1 Acessando o Tráfego

Para a análise do tráfego de rede é necessário, de alguma forma, ter acesso a esse tráfego. Em redes sem fio, devido à sua característica de transmissão por meio compartilhado, basta configurar a placa de rede do equipamento sensor em "modo promíscuo" [1] para visualizar todo o tráfego dentro do seu raio de alcance [30].

No caso de redes infra-estruturadas, serão apresentados a seguir alguns recursos utilizados para esta tarefa:

Hub

É inserido um *hub* Ethernet entre os dispositivos de rede. Como um *hub* repete o pacote recebido em cada porta, exceto na que transmitiu o mesmo, todas as

[1] É um modo de operação no qual cada pacote transmitido pode ser recebido e lido por um adaptador de rede, independentemente do destino do pacote.

máquinas conectadas ao *hub* terão condições de visualizar o tráfego daquele segmento de rede.

Vantagens: Barato, simples, não requer modificação de configurações no sensor.

Desvantagens: Opera em modo *half-duplex* (permite que somente um equipamento possa transmitir por vez), gera muitas colisões no enlace, quando submetido a alto volume de tráfego, além de introduzir ponto de falha na rede.

Porta *SPAN*

Conhecida também como "espelhamento de porta" ("*port mirroring*"). É um recurso, encontrado em alguns *switches*; permite que todo o tráfego passante por determinada porta seja "espelhado" em outra, onde o sensor está conectado.

Vantagens: Fácil acesso ao tráfego de rede, sendo necessária apenas a conexão da placa de rede do sensor à porta *SPAN*. Pode ser configurada para receber o tráfego de várias portas do *switch*. Não interfere no tráfego.

Desvantagens: Se for mal configurada, pode introduzir erros na rede. Se submetida a alto volume de tráfego, pode não visualizá-lo por completo. O uso da porta SPAN implica em que o tráfego passe através de um único *switch*, introduzindo um ponto de falha na rede.

TAP

É um dispositivo de rede especialmente criado para capturar/espelhar tráfego. Sua utilização é similar à do *hub*, ou seja, deve ser colocado entre dois dispositivos de rede. Os modelos tradicionais (de duas saídas) possuem quatro portas, uma para cada dispositivo a ser interligado, uma para monitoramento do tráfego entrante e outra para o monitoramento do tráfego sainte. Atualmente já são utilizados *TAPs* de três portas, onde a terceira porta atua como agregadora dos fluxos entrantes e saintes.

Vantagens: Preserva a natureza "*full-duplex*" do enlace entre os dois dispositivos vizinhos. Pode ser configurado para agir de forma totalmente passiva, não alterando os pacotes observados. Não exige configuração especial. Não interfere no tráfego, mesmo em caso de falha.

Desvantagens: Relativamente caro (se comparado com os *hubs*). Para os *TAPs* de duas saídas, é necessário o uso de sensor com duas placas de rede com aplicativo para "recombinar" o tráfego em um único fluxo.

Equipamento especializado

Realiza atividades de maior flexibilidade e complexidade que um equipamento de infra-estrutura de rede utilizado na visualização do tráfego (*hub*, porta *SPAN* ou *TAP*). Geralmente é construído usando o sistema UNIX e pode ser configurado como um roteador, ou como uma *bridge*, para captura/analise do tráfego que passa por ele.

Vantagens: Possibilidade de combinação com *firewalls* para oferecer controle de acesso ("*filtering bridges*") .

Desvantagens: Introduz um novo ponto de falha na rede. Adiciona latência ao enlace.

2.2.2 Capturando o Tráfego

A captura do tráfego é feita por um sensor, que pode ser um aplicativo em um equipamento conectado à rede ou um equipamento (combinação de "*software / hardware*") desenvolvido especificamente para este propósito. Estes equipamentos geralmente possuem dispositivos de alta performance que podem capturar um volume muito grande de pacotes minimizando as perdas.

O aplicativo de captura de tráfego trabalha colocando o dispositivo de rede em "modo promíscuo", permitindo a captura de todos os pacotes que trafegam no seg-

mento de rede ao qual está conectado.

Serão apresentadas, a seguir, algumas ferramentas utilizadas pelos sensores na realização da captura do tráfego:

BPF

O *BPF - BSD Packet Filtering* [2] é uma arquitetura encontrada em diversas versões do *Unix*, composta de dois elementos principais: o interceptador de rede e o filtro de pacotes. O primeiro coleta cópias dos pacotes da interface de rede e as entrega às aplicações que monitoram a rede. O segundo decide se o pacote será aceito e, caso afirmativo, o quanto do mesmo será copiado para a aplicação.

A captura do pacote é feita no nível de usuário, permitindo o uso de estações de trabalho para monitoramento da rede de forma eficiente. Como sensores são executados no espaço de processos no nível de usuário, os pacotes devem ser copiados para uma área cujo acesso seja permitido, de forma que possam ser manipulados pelos sensores. Esta cópia é feita por um agente do núcleo do sistema operacional (*kernel*) chamado filtro de pacote. O *BPF* permite que essa cópia seja feita de forma muito eficiente, já que é baseado em registradores e possui um sistema de armazenamento temporário de dados ("*straighforward buffering*") que permite que seja muito rápido.

Na chegada do pacote na interface de rede, o "*driver*" da camada de enlace o envia para a pilha de protocolo do sistema, mas, se o *BPF* estiver "escutando" esta interface, o pacote será enviado para o *BPF*. O *BPF* envia o pacote para cada filtro associado a cada processo que se encontra monitorando a rede. Cada filtro decide se o pacote será aceito e quantos *bytes* serão lidos. Após a aceitação do pacote pelo filtro, o *BPF* copia a quantidade de *bytes* solicitados para o respectivo *buffer*. O esquema de funcionamento do *BPF* pode ser melhor visualizado na Figura 2.8.

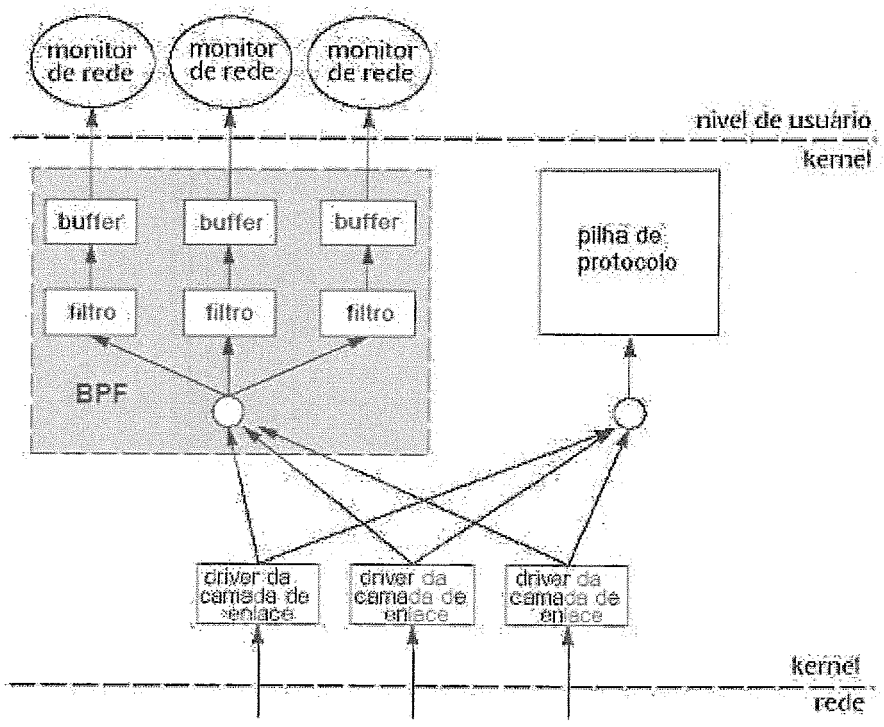

Figura 2.8: Esquema de funcionamento do BPF [2].

Biblioteca libpcap

A biblioteca *libpcap* [31] provê uma interface de alto nível (*API*)para os sistemas de captura de pacotes. Esta biblioteca é responsável pela captura de pacotes provenientes da rede e pela entrega destes ao programa, mediante critérios de filtragem baseados na arquitetura BPF. Em resumo, a *libpcap* é um conjunto de rotinas para implementação do BPF.

É uma biblioteca que possui características de grande rapidez, alta eficiência e de simples utilização. Também é bastante versátil, pois permite a captura não apenas de pacotes Ethernet, mas também de pacotes PPP, SLIP, IPX, SPX entre outros, bastando para isso que o programador defina corretamente o tipo de *frame* a ser capturado.

A biblioteca *libpcap* está presente como interface de captura em diversos projetos de monitoramento, tais como o Tcpdump [32], Ethereal [33], Snort [34] e muitos

outros.

Arquitetura Netflow

Desenvolvida em 1996 por Darren Kerr e Barry Bruins, na *Cisco Systems*, a tecnologia *NetFlow* permite o acúmululo de estatísticas dos pacotes trafegados na rede.

A arquitetura *Netflow* funciona seguindo o modelo proposto pelo *Real-Time Flow Measurement* (RTFM) [35], onde existem três elementos: o sensor, o coletor e o gerente, conforme pode ser observado na Figura 2.9.

Os roteadores funcionam como sensores, realizando a captura dos pacotes e totalizando os mesmos em tabelas de fluxos (armazenados localmente em área denominada *cache*) que depois são enviados para os coletores encapsulados em pacotes UDP.

Existem algumas ferramentas de código aberto desenvolvidas para o sistema operacional *GNU/Linux*, que geram os *probes*, ou seja, capturam, condensam e exportam os dados, como se fossem um roteador Cisco com suporte ao *NetFlow* habilitado. Algumas dessas ferramentas são: nProbe [36], fprobe [37] e argus [38].

Os coletores são máquinas com programa permanentemente ativo que fica "ouvindo" uma determinada porta UDP, pronto para receber os pacotes enviados pelo sensor. Ao receber o pacote contendo as informações dos fluxos, estes são armazenados em um sistema de arquivos para posterior análise.

Diferentes coletores armazenam seus dados em diferentes formatos. Existem várias ferramentas de código aberto desenvolvidas para o sistema operacional GNU/Linux para coletar, processar e gerenciar os registros do *Netflow*. Podem ser citados: flow-tools [4], cflowd [39] e ntop [40].

Os gerentes (ou analisadores) realizam a análise dos dados coletados, baseados em critérios pré-definidos, aplicados à tarefas tais como engenharia de tráfego,

planejamento de rede, tarifação, segurança e outros. São responsáveis, também, pela divulgação do resultado da análise realizada.

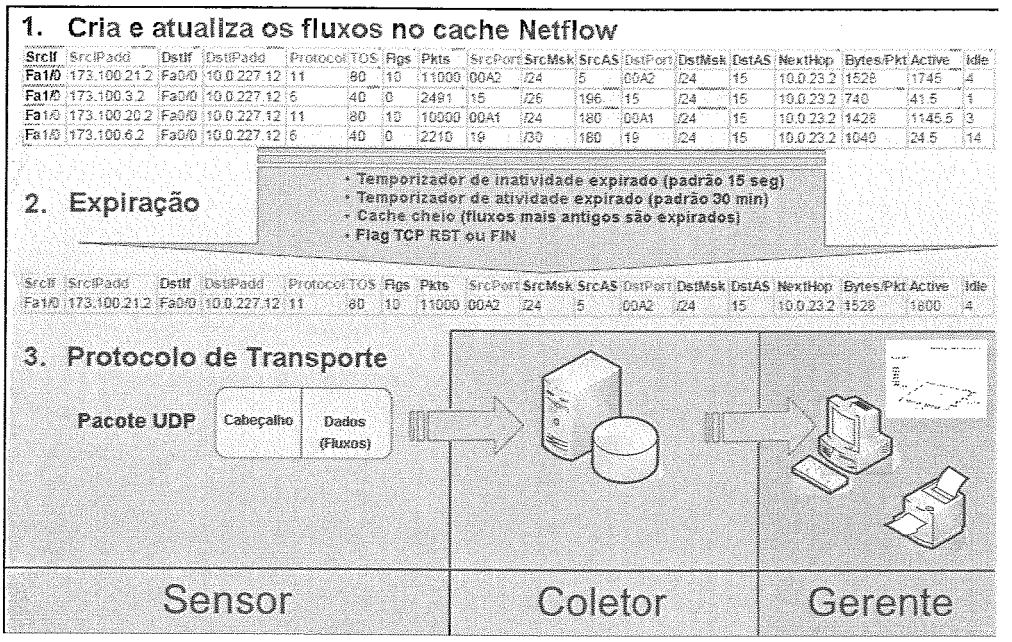

Figura 2.9: Arquitetura Netflow.

A fim de aprimorar o monitoramento do tráfego de dados diretamente em equipamentos de rede, tais como roteadores e *switches*, o *Internet Engineering Task Force* (IETF) criou o grupo de trabalho responsável pelo desenvolvimento do protocolo base para a especificação do formato de exportação de fluxos de dados IPFIX (*IP Flow Information eXport*). Após diversas análises, em 2004, o grupo de trabalho IPFIX publicou na RFC 3955 [41] a escolha do *Cisco Netflow System* [42] como base para o protocolo a ser implementado.

No conceito do *Netflow*, um fluxo é definido como uma seqüência unidirecional de pacotes entre um par de endereços IP (origem e destino).

Exemplificando o conceito acima, é possível imaginar uma situação onde se deseja estabelecer uma sessão de acesso remoto a partir do equipamento A na porta 1234, para a porta 23 do equipamento B. O pacote inicial de A para B provoca no roteador a criação, em sua área de armazenamento temporário, de um fluxo {TCP,A,1234,B,23}. O fluxo relacionado {TCP,B,23,A,1234} é criado no roteador,

pela resposta de B para A. Os dados do tráfego subseqüente se agregarão dentro destes dois registros de fluxo até que a sessão TCP termine ou até que os registros de fluxo sejam removidos do *cache* (por ultrapassar determinado período de tempo ou por falta de espaço de armazenamento na tabela de fluxos). Os registros de fluxos armazenam o protocolo IP (TCP, UDP, ICMP), as interfaces pelas quais o tráfego foi recebido e enviado, além do número de pacotes e octetos observados naquele fluxo até então. Quanto ao tráfego TCP, os registros de fluxos também vão armazenar o valor da operação lógica OR, cumulativa de todos os sinalizadores contidos no cabeçalho dos pacotes observados naquele fluxo até então.

Como pode ser avaliado, a maioria das interações resultarão em pelo menos dois fluxos, um para cada direção do tráfego. É importante destacar o fato de que uma sessão TCP pode consistir de muito mais do que dois fluxos. Pode-se dizer que os fluxos pertencem ao mesmo "aglomerado" correspondente aos endereços IP e número de portas.

Verifica-se se o fluxo contém pacotes do início, meio ou fim da conexão analizando-se os sinalizadores da comunicação TCP. Por exemplo, um fluxo cujo sinalizador inclua o *bit* FIN mas não inclua o *bit* SYN significa que ele agregou pacotes do meio e da extremidade de uma conexão do TCP. Já os fluxos dos protocolos UDP e ICMP são somente coleções de pacotes "semelhantes", uma vez que nenhum destes protocolos é orientado à conexão.

A unicidade da identificação de um fluxo é obtida pela combinação dos sete campos chaves a saber:

1. Endereço IP de origem
2. Endereço IP de destino
3. Número da porta de origem
4. Número da porta de destino
5. Tipo de protocolo

6. Tipo do serviço (ToS)[2]

7. Interface lógica de entrada

Se um pacote possuir um campo chave diferente de outro pacote, considera-se que este pertença a outro fluxo. Como dito anteriormente, os fluxos são armazenados em uma tabela de fluxos também chamada de *cache Netflow.*

Os registros NetFlow são enviados para um equipamento coletor nas seguintes circunstâncias:

- Em conexões TCP, quando a conexão for encerrada (depois de um RST ou FIN);
- Quando não ocorrer tráfego durante 15 segundos;
- Quando o tempo exceder os 30 minutos a partir do início do fluxo;
- Quando a tabela de fluxos estiver cheia.

Cada registro NetFlow contém dados sobre os pacotes que são representados nesse fluxo, além dos identificadores únicos listados anteriormente.

O *Netflow* possui a vantagem de, quando implementado em roteador, não exigir modificações na topologia da rede, porém tem as desvantagens de não ser suportado em qualquer tipo de roteador, necessitar de uma máquina para fazer a coleta e análise dos fluxos, além de não analisar o conteúdo (dados) dos pacotes.

[2]O Tipo de Serviço é utilizado para a seleção da qualidade do serviço desejado, ou seja, é um resumo ou conjunto generalizado de parâmetros (precedência, atraso, vazão e confiabilidade) que são mapeados nos parâmetros reais do serviço das redes por onde o datagrama passa. [27]

2.3 Análise de Tráfego Baseada em Pacotes X Baseada em Fluxos

Os sistemas de captura e análise de tráfego baseados em pacotes possuem a vantagem da visibilidade de todo o conteúdo dos dados que estão sendo trafegados, proporcionando uma maior granularidade para critérios de filtragens e análise do tráfego. Em contrapartida, a manipulação de um volume de tráfego elevado, tal como o encontrado em um *backbone*, gera um custo computacional muito grande para processamento e armazenamento, podendo provocar perda de pacotes [43], o que prejudica a qualidade da análise feita.

Diferentemente, um registro de fluxo não apresenta nenhuma informação das camadas mais altas, contendo apenas o perfil do tráfego. Desta forma, os sistemas de análise de tráfego, baseados em fluxos, perdem na análise de conteúdo, mas, por outro lado, as informações obtidas são suficientes para se tirar muitas conclusões sobre o tráfego, baseadas nas informações contidas nos cabeçalhos dos pacotes. A vantagem desta abordagem é a velocidade, pois, não coletando as informações de dados dos pacotes, causa uma grande redução de recursos computacionais, sendo adequado para o uso em ambientes com tráfego pesado, como os apresentados em *backbones*.

2.4 Padrões de Anomalias de *Malwares* em Rede

Alguns atacantes introduzem, nas máquinas de suas vítimas, conjuntos de códigos de instruções capazes de fazer com que os sistemas operacionais dessas máquinas realizem ações planejadas pelos atacantes, sem o conhecimento das vítimas. Este conjunto de instruções são denominados *malwares* [3].

Os mecanismos utilizados na implementação e distribuição dos códigos maliciosos são muito diferentes entre si e requerem conhecimentos específicos. As maiores categorias de *malwares* e suas características são apresentadas na Tabela 2.2.

Tipo de código malicioso	***Características***
Vírus	Infecta um arquivo para posterior exploração. Geralmente requer interação humana para sua replicação (para abrir um arquivo, ler uma mensagem eletrônica, executar um programa, etc.).
Worm	Se propaga através da rede de dados, explorando sistemas vulneráveis e mal configurados. É auto-replicável e geralmente não requer interação humana para sua replicação.
Código malicioso móvel	São programas leves, baixados de um sistema remoto e executados localmente, com mínima ou nenhuma intervenção do usuário. Escrito tipicamente em *Javascript*, *VBScript*, *Java* ou *ActiveX*.
Porta dos fundos (*Backdoor*)	Burla os controles de segurança da máquina para fornecer acesso ao atacante.
Cavalo de tróia	Disfarça-se como um programa útil, mascarando sua finalidade maliciosa escondida.
Rootkit (nível de usuário)	Modifica programas executáveis utilizados por administradores de sistemas e usuários.
Rootkit (nível de núcleo)	Modifica o núcleo do sistema operacional para criar e esconder portas dos fundos.

Tabela 2.2: Principais categorias de códigos maliciosos.

A maioria dos desenvolvedores de ferramentas maliciosas não se limita a criar ferramentas em uma única categoria. Algumas ferramentas são vírus e *worms*. Da mesma forma, *worms* podem carregar *Rootkits* ou *Backdoors* e assim por diante.

Limitando o foco do trabalho à segurança de rede de dados, apresentaremos a seguir,um resumo do princípio de funcionamento dos *worms*, a fim de identificarmos seus padrões de atividades nas redes de dados. Os *worms* dependem da infra-estrutura de redes para sua propagação, podendo sobrecarregar o tráfego nas redes locais e congestionar os enlaces da *Internet*.

Os *worms* oferecem aos atacantes uma escala que não é facilmente conseguida com outros tipos de ataques. Os *worms* utilizam o poder das grandes redes distribuídas (principalmente a *Internet*) para efetuar a sua propagação e disseminação,

minando as redes, imitando o movimento dos vermes.

Os atacantes empregam estas potencialidades dos *worms* para alcançar vários objetivos, tais como a tomada de controle de diversos sistemas, a possibilidade de tornar mais difícil o rastreamento para identificação da autoria do ataque e, conseqüentemente, ampliar os danos.

Se um atacante necessitar de muito processamento para quebrar uma chave criptografada, por exemplo, com o uso de *worm*, conquistando mil máquinas, ele conseguirá executar o trabalho mil vezes mais rápido do que com uma única máquina.

O *worm* pode ser utilizado para realizar varredura distribuída e lenta, dificultando a localização do atacante e evitando a identificação pelos sistemas de detecção, que são baseados unicamente em volume de tráfego que chega na vítima.

Os *worms* típicos são compostos por cinco elementos, ilustrados na Figura 2.10.

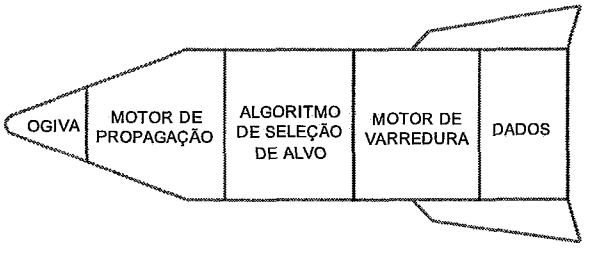

Figura 2.10: Os elementos componentes de um *worm* [3].

Para entendermos o princípio de funcionamento dos *worms*, apresentaremos, a seguir os passos dados pelo *worm* para efetuar a sua proliferação, identificando os propósitos dos componentes do *worm* em cada estágio do ciclo de infecção. Os *worms* geralmente exploram falhas nas vítimas, para conquistá-las automaticamente, sem que o usuário ou administrador tenha que fazer nada para tal. Eles usam o elemento ogiva para esta finalidade.

As técnicas mais populares para a obtenção do acesso às vítimas são:

Exploração de "*Buffer overflow*" - Falhas no desenvolvimento de aplicativos podem fazer com que o programa permita o acesso a determinadas posições da

memória, tornando-o vulnerável ao "buffer overflow". Explorando estas falhas, os atacantes enviam mais dados do que o programa é capaz de manipular, corrompendo várias estruturas de memória da máquina vítima. Usando instruções específicas, um *worm* pode abrir um acesso na vítima e efetuar sua propagação.

Ataque de compartilhamento de arquivos - Os usuários podem ler ou gravar arquivos através da rede, transparentemente, por meio de compartilhamentos de arquivos do Windows ou do Network File System (NFS) do UNIX. O *worm Ninda*, por exemplo, sobrescreve um arquivo compartilhado na máquina da vítima, para que posteriormente seja executado pelo usuário da máquina.

Correio eletrônico - Atualmente, a maioria de máquinas pode enviar ou receber correio eletrônico. Adicionalmente, os leitores e os servidores de correio provaram ser alvos altamente vulneráveis. Usuários podem ser facilmente ludibriados, para que executem os arquivos com códigos maliciosos anexados às mensagens. Quanto aos servidores de correio eletrônico, há um número elevado de falhas nos aplicativos que permitem ao atacante comprometer o sistema completamente, sem qualquer intervenção de usuários. Além disso, as listas de distribuição de correio eletrônico podem conter milhares de usuários. Um *worm* pode se proliferar utilizando estas listas para aumentar o número de vítimas. Com este acesso difundido e vulnerabilidades, o correio eletrônico torna-se um veículo ideal para a penetração dos *worms* em sistemas. Esta técnica foi utilizada pelo vírus/*worm Melissa*, o *Love Bug* e ainda o *Nimda*.

Após conseguirem o acesso às vítimas, o *worm* deverá transferir o restante do seu "corpo" para a vítima. Em alguns casos, o elemento ogiva pode ser usado para carregar todo o código do *worm*, os chamados "auto-carregados". Por exemplo, no compartilhamento de arquivos, um *worm* inteiro pode ser gravado no sistema de arquivos da vítima. Da mesma forma, *worms* completos podem ser enviados como arquivos anexos ao correio eletrônico. Nestes casos, a ogiva e o motor de propagação formam um único elemento.

Em outros *worms*, que exploram as falhas de "*buffer overflows*" ou outras falhas de configuração, o elemento ogiva somente abre uma porta para que o *worm* possa executar instruções na máquina da vítima: são os *worms* que necessitam de um segundo canal para sua propagação.

Emprega-se, então, o motor de propagação para mover-se na rede e rastejar para dentro da vítima. Por meio do elemento ogiva, o *worm* executa instruções na vítima para transferir o código restante. Os métodos de propagação mais comuns são mostrados na tabela 2.3.

Programa de transferência de arquivo	***Descrição***
FTP	O *File Transfer Protocol* é utilizado para mover arquivo através das redes, com identificação de usuário e senha em texto-claro ou anônimo.
TFTP	O *Trivial File Transfer Protocol* suporta acesso não autenticado para gravar ou ler arquivos através da rede.
HTTP	O *HyperText Transfer Protocol* é comumente usado para acessar páginas Web, mas pode ser usado também para transferir arquivos.
SMB	O protocolo *Server Message Block* da Microsoft é usado pelo *Windows* para compartilhar arquivos, e também é suportado por servidores *UNIX* que executem o *SAMBA* [3].

Tabela 2.3: Principais métodos de propagação dos *worms*.

Os *worms* buscam específicas portas funcionais em suas vítimas. Por exemplo, o *worm* "*SQL Slammer*" trabalha acessando a porta 1434, o "*Netbus Trojan*" acessa a porta 12345, entre outros. Após efetuar a propagação, o *worm* se auto-instala na vítima, carregando seus processos na memória e alterando as configurações do sistema para que sejam capazes de executar continuamente, escondidos no sistema.

O *worm*, em execução na máquina vítima, inicia o algoritmo de seleção de vítimas, buscando por novas vítimas para atacar. Cada endereço selecionado por este elemento sofrerá uma varredura para levantamento de vulnerabilidades. A Seção 2.5

apresenta as técnicas de varredura mais utilizadas pelos *worms* e que também serão utilizadas como parâmetros para o algoritmo de classificação proposto.

Na máquina vítima, os programadores dos *worms* podem utilizar diferentes técnicas de seleção de novas vítimas, tais como:

Endereços eletrônicos - Um *worm* pode copiar endereços eletrônicos dos aplicativos de correio eletrônico da vítima, tornando todo o remetente ou destinatário de correio eletrônico da máquina da vítima um alvo em potencial.

Listas de equipamentos - Alguns *worms* colhem endereços de várias listas de máquinas no equipamento local (/etc/hosts no *UNIX* e LMHOSTS no *Windows*).

Sistemas confiáveis - No ambiente UNIX, o *worm* pode procurar por relacionamentos confiáveis entre a vítima atual e outras, mediante a análise do arquivo /etc/hosts.equiv. Estes relacionamentos, que às vezes estão configurados para que os usuários possam acessar uma máquina a partir de outra sem o fornecimento de senha, são uma grande ajuda para os *worms* conquistarem outras vítimas.

Lista de recursos disponíveis numa rede local - Em redes *Windows*, alguns *worms* exploram a lista de recursos disponíveis numa rede local para encontrar novas vítimas em potencial. Os *worms* buscam por servidores de arquivos próximos, enviando requisições por meio dos protocolos *SMB* e *Netbios*.

Pesquisa DNS - O *worm* se conecta ao servidor de nomes local (Domain Name Service - DNS) associado à máquina vítima e pesquisa por endereços de outras vítimas. O DNS, desta forma, torna-se um grande repositório de vítimas em potencial.

Selecionando aleatoriamente um endereço de rede : Um *worm* pode simplesmente selecionar aleatoriamente um endereço de sua vítima, utilizando um algoritmo para calcular um valor razoável para tentar infectar.

Usando endereços gerados pelo motor de seleção de alvo, o *worm* varre ativamente através da rede para determinar as vítimas apropriadas. Usando o motor de varredura, o *worm* envia um ou mais pacotes contra um alvo em potencial para avaliar se o seu elemento ogiva obterá sucesso naquela vítima. Quando um alvo satisfatório é encontrado, o *worm* então infecta aquela nova vítima e todo o processo de propagação é repetido. A ogiva abre a porta, o *worm* se propaga, os dados são executados, novas vítimas são selecionadas e então varre-se novamente. Uma única interação de todo o processo é geralmente completado em segundos ou menos. Num instante, o *worm* infecta a vítima e usa isto para espalhar o contágio.

Os dados do *worm* são um pedaço do código definido para implementar alguma ação específica na vítima em nome do atacante. Ou seja, os dados são o que os *worms* fazem quando assumem o controle da vítima.

Muitos *worms* realmente não fazem muita coisa quando alcançam um alvo, exceto a propagação para outras máquinas. Neste caso, os dados do *worm* não existem. Estes *worms* são apenas "reprodutores" e não "guerreiros", causando dano somente à largura de faixa disponível na rede.

Para os *worms* "guerreiros", o desenvolvedor tem muitas opções para incluir na área de dados, tais como:

- Abrir uma porta dos fundos;
- Plantar um agente de ataque de negação de serviço distribuído;
- Executar uma operação matemática complexa.

A análise das peculiaridades descritas até então nos permite identificar padrões de tráfego indicadores de atividades de *worms*. O Capítulo 3 apresentará o algoritmo utilizado para a classificação e filtragem deste tipo de tráfego.

2.5 Técnicas de Varreduras em Rede

A idéia principal das varreduras (*scans*) em rede é procurar pelo maior número de canais de comunicação abertos que possam ser potenciais alvos de ataque. As varreduras variam conforme o protocolo de comunicação utilizado na troca de informações entre os equipamentos.

Existem várias técnicas para a realização de varredura em um equipamento, uma rede de computadores ou mesmo uma grande faixa de números IP. Abaixo, serão evidenciadas algumas delas:

- TCP connect()
- TCP SYN (half-open)
- TCP FIN (stealth)
- SYN/FIN usando fragmentação de IP
- UDP recvfrom()

TCP connect()

Essa é a forma mais básica de varredura baseada no protocolo TCP . A chamada de sistema *connect()*, fornecida pelo sistema operacional, é utilizada para abrir uma conexão para cada porta desejada em uma máquina. Se a porta está apta a receber conexões, a primitiva *connect()* terá sucesso, caso contrário, a porta estará inalcançável [25].

TCP SYN (half-open)

Essa técnica é denominada *half open*, pois a conexão TCP não é totalmente aberta. Um pacote, contendo apenas o sinalizador SYN, é enviado para o equipamento de destino, como se os procedimentos para uma conexão real se iniciassem. De acordo com a resposta enviada pela máquina destino, pode-se chegar às seguintes conclusões [28]:

· Se um pacote, contendo os sinalizadores SYN/ACK, for enviado pela máquina destino, conclui-se que a porta está disponível (aberta). O próximo passo do procedimento de varredura é enviar um pacote com o sinalizador RST para finalizar a conexão.

· Se um pacote, contendo os sinalizadores RST/ACK, for enviado pela máquina destino, conclui-se que a porta não está apta a receber conexões para a troca de dados, ou seja, é inacessível. A vantagem dessa técnica é que poucas máquinas armazenam registros de auditoria do sistema sobre esse tipo de anomalia nas conexões.

TCP FIN

As varreduras TCP FIN, ao contrário da técnica TCP SYN, em sua maioria não são detectadas pelos sistemas de auditoria. Esses tipo de varredura é baseada no fato de que as portas que não aceitam conexões, estando de acordo com a RFC793 [28], enviam um pacote com sinalizador RST, em resposta ao pacote recebido apenas com o sinalizador FIN ativo. Já as portas abertas tendem a ignorar esse pacote (FIN), não processando o seu pedido de finalizar uma conexão inexistente. Dessa forma, dependendo do comportamento do equipamento de destino ao lidar com o pacote com sinalizador TCP FIN ativo, o atacante fica sabendo quais portas estão abertas e quais não.

TCP Null

Similar às varreduras TCP FIN, a varredura TCP Null baseia-se no fato de que as portas que não aceitam conexões, estando de acordo com a RFC793 [28], enviam um pacote com sinalizador RST em resposta ao pacote recebido sem sinalizador nenhum ativo. O receptor interpreta que o pacote não deveria ter chegado até ele e descarta o pacote e retorna um pacote para o atacante com o sinalizador RST. Dessa forma, este fica sabendo quais portas estão abertas e quais não.

TCP SYN/FIN com fragmentação de IP

Essa técnica consiste na modificação de outras técnicas de varredura pré-existentes. Ao invés de apenas enviar um pacote de dados, esse método divide o pacote em pe-

quenos fragmentos. A idéia é dividir o cabeçalho TCP em muitos pedaços, com o objetivo de dificultar o trabalho de detecção, mantendo, dessa forma, oculto o processo de varredura para o sistema alvo.

UDP recvfrom()

Essa técnica é utilizada para determinar portas abertas através do tratamento adequado de uma resposta ICMP, dada ao requisitante da conexão caso a porta requisitada não esteja aberta. Quando recebe um pacote para uma porta fechada, a maioria dos equipamentos envia um erro de ICMP_PORT_UNREACH. Sendo assim, descobre-se quais portas estão abertas, pois, neste caso, não se recebe nada de volta.

2.6 Trabalhos Relacionados

2.6.1 Análise de Tráfego na Segurança de Redes

Diversas ferramentas populares de monitoração de tráfego de redes, tais como FlowScan [17], Netflow FlowAnalyzer [18] e AutoFocus [19], são utilizadas a fim de suprir a necessidade de gerência do desempenho da rede.

Quando a questão é a obtenção de informações, que agreguem valores à gerência da segurança de redes, são utilizadas metodologias visando a identificação de ocorrências de eventos anômalos, fundamentadas nos seguintes fatores:

1. - Alteração de volume de tráfego;
2. - Elevação do número de sessões estabelecidas;
3. - Conteúdo da área de dados dos pacotes;
4. - Periodicidade de ocorrências de fluxos.

Estas metodologias apresentam características comuns na execução das tarefas

necessárias, desde a ocorrência do evento até a tomada de providência para sanar o problema. Estas tarefas podem ser agregadas em etapas, representadas pela Figura 3.1 e sumarizadas a seguir:

1. Monitoramento da rede - A partir do monitoramento da rede, observa-se a ocorrência de um evento de anomalia no tráfego (alteração de volume de tráfego, número elevado de sessões estabelecidas , conteúdo da área de dados dos pacotes ou periodicidade de ocorrências de fluxos)

2. Identificação do serviço causador da anomalia - Com base nos arquivos de fluxos, são executados programas para efetuar as filtragens necessárias para identificação do serviço causador da anomalia.

3. Identificação dos usuários do serviço causador da anomalia - Ainda com base nos arquivos de fluxos, são executados programas para efetuar novas filtragens a fim de identificar os usuários do serviço causador da anomalia.

4. Providência - Com base nas informações colhidas nas etapas anteriores, o gerente de segurança pode adotar as providências cabíveis para a solução do problema.

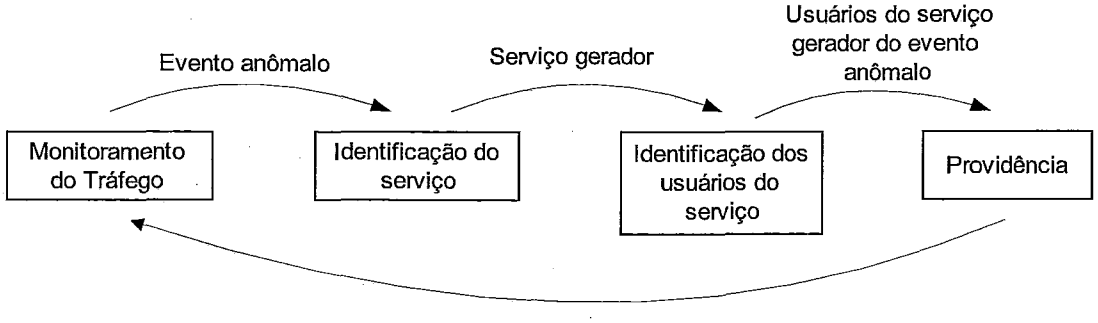

Figura 2.11: Diagrama esquemático das metodologias comumente utilizadas.

Veremos, a seguir, algumas abordagens propostas para detectar, impedir e minimizar as atividades maliciosas em redes de dados que utilizam as metodologias tradicionais.

Soluções baseadas em assinaturas, tais como sistemas de detecção de intrusão em rede (*Network Intrusion Detection System - NIDS*), tentam combinar regras pré-estabelecidas ao tráfego, a fim de identificar anomalias conhecidas, tais como ataques de negação de serviço (*Deny of Service - DoS*) a partir do tráfego próximo das vitimas. Os métodos baseados em assinaturas são rápidos e confiáveis para identificação de padrões conhecidos. Eles são muito populares entre os sistemas de segurança, pois apresentam uma taxa de detecção muito alta e geram muito menos falsos alarmes do que outros métodos. Porém, devido ao fato das técnicas utilizadas para exploração de falhas estarem em constante desenvolvimento, a manutenção da base de assinaturas é uma tarefa onerosa em termos de trabalho humano e de tempo.

Várias formas de assinaturas têm sido propostas para representar perfis de anomalias de tráfego. A desproporção do tráfego de fluxos bi-direcionais, por exemplo, pode ser usada como assinatura de tráfego anômalo [22], que visa a sobrecarga do canal de transmissão de dados da rede e a falha de funcionamento dos roteadores próximos da vítima. Contudo, as informações analisadas constituem somente um indício de anomalia, não fornecendo subsídios suficientes para a identificação do autor do evento anômalo.

Em [4] é apresentado um conjunto de ferramentas utilizadas para manipular arquivos de registros gerados pela arquitetura *Netflow*. Uma destas ferramentas, o *Flow-dscan*, realiza a detecção e gera relatórios (Figura 2.12) de eventos anômalos na rede, tais como o número excessivo de octetos ou pacotes por fluxo, varredura de equipamentos e varredura de portas, sendo que esta última limitada ao intervalo de portas entre 0 e 1023. A limitação apresentada influi diretamente na restrição do estudo de comportamentos anômalos dos *worms* como, por exemplo, o perfil de atividade do *SQL slammer*, que varre a porta de destino 1434, buscando por vulnerabilidades dos servidores Microsoft SQL, a fim de infectá-los.

A abordagem de análise do conteúdo dos dados do tráfego, proposta em [45], visa identificar atividades de propagação de worms que utilizam o correio eletrônico para sua propagação, mediante técnicas de transmissão de código malicioso na área

```
> flow-cat cf05.199-05-01.* | flow-filter -r6 -il | flow-dscan -b -W

flow-dscan: info(6):  load_suppress 0
flow-dscan: info(6):  load_suppress 1
flow-dscan: info(6):  host scan: ip=164.107.94.233 start=922930706
flow-dscan: info(6):  port scan: src=140.254.224.212
                                 dst=128.146.125.26 start=922930706
flow-dscan: info(6):  host scan: ip=164.107.100.128 start=922930706
flow-dscan: info(6):  host scan: ip=140.254.230.153 start=922930706
```

Figura 2.12: Resultado da execução do Flow-dscan [4].

de dados dos pacotes trafegados. A aplicação desta abordagem acarreta a captura de uma grande parte do pacote e, ao ser utilizada em redes de alto volume de tráfego, além de gerar um custo computacional muito grande para processamento e armazenamento, torna esta solução sujeita à perda de pacotes analisados [43], o que prejudica a qualidade do resultado obtido.

Em [5], foi proposta uma abordagem que utiliza um algoritmo de classificação de dados denominado RADAR (*Real-time Attack Detection And Report*). A partir do tráfego capturado, este algoritmo classifica e identifica eventos de ataques de negação de serviço (*Deny of Service - DoS*), varreduras de equipamentos (*hostscan*) e varreduras de portas (*portscan*). Neste algoritmo, utiliza-se uma tabela *hash* para cada variável monitorada (endereço IP de origem, endereço IP de destino e porta de destino). Para cada fluxo analisado, registra-se na tabela *hash* da respectiva variável a ocorrência e a marca de tempo (*timestamp*) do mesmo. De acordo com a periodicidade de registros de ocorrências nas tabelas, ou seja, se a diferença do tempo de registro de duas ocorrências na tabela *hash* da variável analisada for inferior a determinado intervalo de tempo, caracteriza-se um valor significante para uma assinatura a ser gerada.

Exemplificando esta classificação, utilizaremos uma simulação de fluxos <IP de origem, IP de destino, porta de destino> discriminados na Tabela 2.4 .

Nesta simulação, assume-se um intervalo de tempo de observação L igual a 2. Quando o fluxo (3) chegar no instante t+2, receberá a assinatura <IP de origem, IP de destino, porta de destino> igual a <1, 0, 1>. Pois o IP de origem 1.2.3.4

Tempo de chegada	*Fluxo*	*Identificação do fluxo*
t	<3.4.5.6, 5.6.7.8, 90>	(1)
t+1	<1.2.3.4, 5.6.7.8, 80>	(2)
t+2	<1.2.3.4, 3.4.5.6, 90>	(3)

Tabela 2.4: Exemplo de classificação de fluxos segundo [5].

apareceu no fluxo (2) e a porta de destino 90 apareceu no fluxo (1). O IP de destino não apareceu nem no fluxo (1) nem no fluxo (2), recebendo "0" para a coordenada IP de destino. Mas, se o intervalo de tempo de observação L fosse igual a 1, o fluxo (1) já teria sido apagado da memória quando o fluxo (3) chegasse, e o fluxo (3) receberia a assinatura <1, 0, 0>. Ou seja, o "0" na assinatura significa que o valor da coordenada não foi visto recentemente em fluxos anteriores.

Nesta abordagem, utilizou-se, ainda, a visualização intuitiva de manifestações gráficas obtidas na plotagem do resultado da classificação do algoritmo RADAR. Foram consideradas apenas as assinaturas cujos fluxos, quando plotados, representavam formas geométricas de linhas retas e retângulos.

A Tabela 2.5 sumariza as seguintes classificações baseadas na ocorrência de fluxos durante um intervalo de tempo pré-estabelecido e nas manifestações gráficas do resultado:

- Fluxos, com valores de IP de origem e IP de destino repetitivos e porta de destino variável, são caracterizados como a ação de varredura de portas (*portscan*), sendo atribuída a estes fluxos a assinatura <1, 1, 0>.
- Fluxos, com valores de IP de origem e porta de destino repetitivos e o IP de destino variável, são caracterizados como ação de varredura de equipamentos (*hostscan*), sendo atribuída a estes fluxos a assinatura <1, 0, 1>.
- Fluxos, com valores de IP de origem variável e IP de destino e porta de destino repetitivos, são caracterizados como ação de ataque de negação de serviço (DoS) com ip de origem forjado e porta de destino fixa, sendo atribuída a estes fluxos a assinatura <0, 1, 1>.

- Fluxos, com valores de IP de origem repetitivo e IP de destino e porta de destino variáveis, não são caracterizados como um ataque, mas sim como uma ação suicida, pois é ilógico alguém emitir altas taxas de pacotes para destinos aleatórios em portas aleatórias. Estes fluxos recebem a assinatura <1, 0, 0> e a denominação de "*kamikaze*".

- Fluxos, com valores de IP de origem e porta de destino variáveis e IP de destino repetitivo, são caracterizados como ação de ataque de negação de serviço (DoS) com ip de origem forjado e porta de destino variável, sendo atribuída a estes fluxos a assinatura <0, 1, 0>.

Assinatura	*Tipo de ataque*	*Manifestação gráfica*
<1, 1, 0>	Varredura de portas	linha reta
<1, 0, 1>	Varredura de equipamentos	linha reta
<0, 1, 1>	DoS com origem forjada (porta de destino fixa)	linha reta
<1, 0, 0>	Kamikaze	retângulo
<0, 1, 0>	DoS com origem forjada (porta de destino variada)	retângulo

Tabela 2.5: Assinaturas de ataques [5].

Nesta metodologia, a classificação do tráfego capturado restringe-se somente à periodicidade dos dados analisados. As informações dos flags que sinalizam a comunicação representada no fluxo não são consideradas. Conforme [46], aplicações ponto a ponto (*Peer to peer - P2P*) [4], tais como o Gnutella, Skpye, Kazaa, EMule, Shareaza, entre outros, apresentam padrões de conexão similares. Resumidamente, este padrão pode ser descrito da seguinte forma: em um período de tempo determinado, a partir de um único IP com porta UDP fixa, ocorre o envio de pacotes para muitos destinos IP, com portas fixas ou aleatórias. Este padrão de comportamento é apresentado na proposta [5], como sendo dois tipos de ataques de negação

[4]Modelo de conexão no qual cada um dos equipamentos conectados tem os mesmos recursos e cada parte pode dar início a uma sessão. Na *Internet*, refere-se a uma rede transitória que garante a um grupo de usuários com o mesmo programa acessar arquivos instalados no disco rígido de outros.

de serviço. Desta forma, aplicativos da *Internet*, que utilizam servidores muito populares, tais como os serviços de mensagem instantânea (MSN Messenger, ICQ e outros), serviços de voz sobre IP - VoIP (Skype, Gizmo e outros), sítios Web populares e outros, no contexto da proposta [5], contribuem para ocorrências de falsos positivos. A fim de melhor avaliar a metodologia utilizada em [5], foi implementado o algoritmo RADAR, utilizando-se o mesmo cenário da implementação proposta neste trabalho, que será apresentado na Seção 4.4. A Figura 2.13 exemplifica a classificação de tráfego legítimo como ataque de DoS, apresentando alguns segmentos de registros de ocorrências obtidos na execução da implementação do algoritmo RADAR. São apresentados registros com respostas de consultas ao sítio do Google e o processamento de fluxos de conexões oriundos do aplicativo Gnutella (P2P), como sendo frutos de atividades maliciosas. Esta abordagem também não considera a possibilidade de uso de técnicas de varreduras lentas, onde as pesquisas por vulnerabilidades são realizadas em um intervalo de tempo superior ao período de análise das coordenadas.

2.6.2 Visualização na Segurança de Redes

Historicamente, a visualização tem sido aplicada extensivamente para o monitoramento da saúde e desempenho da rede [47, 48, 49, 50, 51]. Com a necessidade de melhores mecanismos para análise dos dados referentes à segurança da rede, técnicas de visualização tem sido exploradas nos últimos anos a fim de suprir esta demanda.

Ao aplicar a visualização ao estudo da segurança da *Internet*, os pesquisadores exploram a habilidade humana inata e altamente eficiente de processar a informação visual, permitindo que complexas tarefas de monitoramento da rede e a detecção de alterações comportamentais do tráfego sejam executadas com maior eficácia.

Em [7], explora-se a técnica para a visualização de dados hierárquicos mediante mapas em árvore (*Tree-Maps*), apresentada em [6] e sumarizada na Figura 2.14, para a identificação das anomalias que ocorrem na rede. Com esta técnica, busca-se utilizar 100% do espaço disponível para visualização das informações, mapeando a

IP de origem	IP de destino	Porta de destino
-- corta --		
64.233.179.96	200.156.37.7	1110
64.233.179.99	152.92.198.41	1173
64.233.179.99	157.86.156.1	59002
64.233.179.99	157.86.156.1	59525
64.233.179.99	200.11.0.34	45033
64.233.179.99	200.11.0.34	45265
64.233.179.99	200.11.0.34	45283
64.233.179.99	200.11.0.56	40532
64.233.179.99	200.11.0.56	40535
64.233.179.99	200.11.0.56	40631
64.233.179.99	200.156.24.131	44568
64.233.179.99	200.156.24.99	1614
64.233.179.99	200.156.51.2	32770
64.233.179.99	200.156.51.2	32817
64.233.179.99	200.156.51.2	32820
64.233.179.99	200.156.51.2	32834
64.233.179.99	200.20.110.1	53628
64.233.179.99	200.20.164.2	16647
64.233.179.99	200.20.180.5	56264
64.233.179.99	200.20.180.5	56867
64.233.179.99	200.20.228.62	2512
64.233.179.99	200.20.33.40	62574
64.233.185.104	200.20.168.70	57576
64.233.185.189	161.79.252.2	58614
64.233.185.189	200.156.17.1	18895
64.233.187.104	157.86.170.217	2000
64.233.187.104	157.86.24.1	29690
64.233.187.104	200.20.164.2	17335
64.233.187.104	200.20.164.2	17507
64.233.187.104	200.20.164.2	17586
64.233.187.104	200.20.168.70	57515
64.233.187.104	200.20.227.40	43828
64.233.187.104	200.20.24.250	11729
64.233.187.104	200.20.24.250	11939
64.233.187.99	157.86.24.1	30135
64.233.187.99	200.156.7.40	52352
64.233.187.99	200.156.72.1	59509
-- corta --		

(a) Respostas de consultas ao Google

IP de origem	IP de destino	Porta de destino
-- corta --		
146.164.76.209	136.179.87.217	6346
146.164.76.209	158.75.211.100	6346
146.164.76.209	195.218.21.180	6346
146.164.76.209	196.217.236.56	6346
146.164.76.209	200.102.67.123	6346
146.164.76.209	200.113.62.148	6346
146.164.76.209	200.206.225.66	6346
146.164.76.209	200.223.251.66	6346
146.164.76.209	200.233.105.236	6346
146.164.76.209	200.3.249.146	6346
146.164.76.209	201.1.216.29	6346
146.164.76.209	201.11.222.180	6346
146.164.76.209	201.2.226.72	6346
146.164.76.209	201.21.70.193	6346
146.164.76.209	201.23.64.2	6346
146.164.76.209	201.26.123.138	6346
146.164.76.209	201.40.14.70	6346
146.164.76.209	201.65.171.143	6346
146.164.76.209	203.177.201.158	6346
146.164.76.209	212.127.152.74	6346
146.164.76.209	212.194.202.224	6346
146.164.76.209	212.76.248.32	6346
146.164.76.209	213.103.220.130	6346
146.164.76.209	213.103.59.74	6346
146.164.76.209	217.122.55.199	6346
146.164.76.209	217.129.9.108	6346
146.164.76.209	219.90.245.125	6346
146.164.76.209	220.188.130.163	6346
146.164.76.209	24.188.246.195	6346
146.164.76.209	24.215.17.50	6346
146.164.76.209	58.169.193.145	6346
146.164.76.209	65.13.107.217	6346
146.164.76.209	66.36.149.62	6346
146.164.76.209	66.36.155.53	6346
146.164.76.209	68.110.193.223	6346
146.164.76.209	68.15.23.126	6346
146.164.76.209	68.220.239.56	6346
-- corta --		

(b) Atividades do aplicativo *P2P Gnutella*

Figura 2.13: Resultados do processamento do algoritmo RADAR [5] apresentando fluxos legítimos, classificados como *DoS*.

hierarquia dos dados em regiões retangulares. O principal ponto forte desta técnica é conseguir mostrar de forma eficiente grandes hierarquias, que podem chegar a centenas de milhares de itens. Em [7], assumiu-se a premissa de que o protocolo utilizado pelo correio eletrônico é um dos mais procurados pelos invasores de rede e, por este motivo, foi feito um direcionamento da aplicabilidade da ferramenta através da seleção de registros de fluxos destinados à porta 25 (*Simple Mail Transfer - SMTP* [29]) de qualquer máquina da rede. A Figura 2.15 representa o resultado de um experimento em [7], que selecionou somente os fluxos destinados a porta 25, totalizando 12.360 registros. Percebe-se que houve cinco IPs de origem, representados pelos retângulos maiores, que realizaram num número excessivo de conexões para diversos

IPs de destino da rede estudada, representados pelos sub-grupos de cada grupo. As cores em tonalidade mais escura mostram que foram enviados muitos pacotes com as mesmas características dos pacotes gerados pelas ferramentas de varreduras de portas. O quadro branco representa a parte da rede em que teve um comportamento normal. O direcionamento da análise para um único serviço restringe muito as características de anormalidade da rede, mascarando muitos eventos importantes de anomalias que utilizam outras portas de acesso.

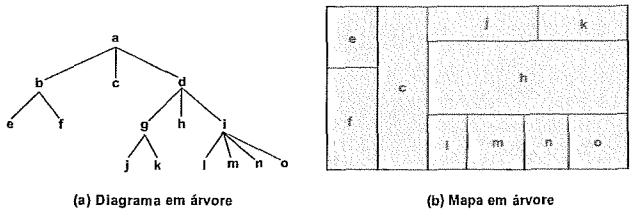

Figura 2.14: Mapa em árvore (*Tree-Map*) [6].

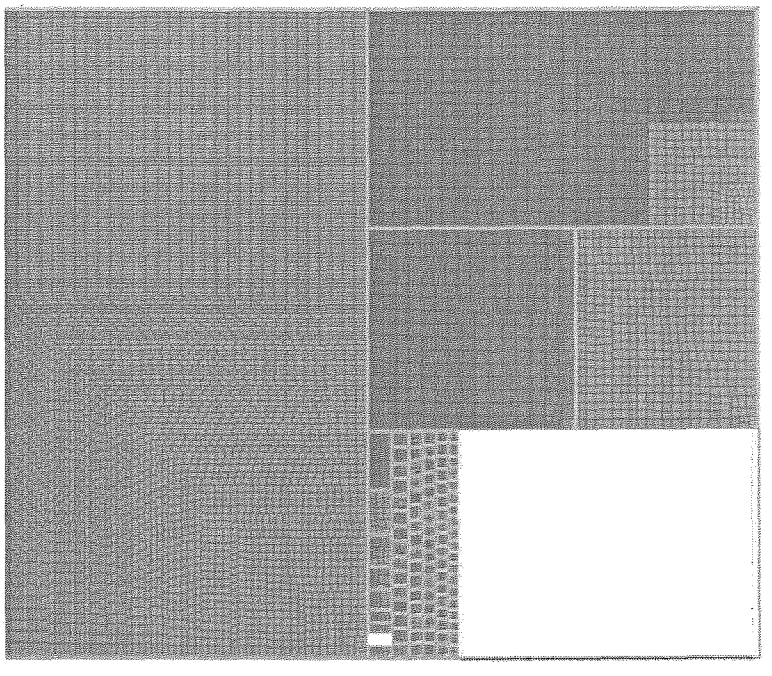

Figura 2.15: Visualização dos fluxos com porta de destino 25 [7].

Alguns trabalhos [8, 9] foram realizados, utilizando-se a apresentação visual multi-dimensional com coordenadas paralelas, técnica proposta por Inselberg [52] em 1980. Em coordenadas paralelas, todos os eixos são paralelos entre si e espaça-

dos igualmente, diferentemente das coordenadas cartesianas tradicionais, onde todos os eixos são mutuamente perpendiculares. Utiliza-se esta técnica na segurança de redes a fim de representar o relacionamento entre os diversos equipamentos, tentando, desta forma, mostrar o estado atual da rede, indicando as atividades relacionadas aos seus equipamentos. A Figura 2.16 representa uma visão global, obtida em [8], mostrando um padrão de tráfego suspeito na rede. Neste caso, um domínio estranho está gerando uma quantidade de tráfego significante para diversos equipamentos da rede local. Na Figura 2.17 são retratadas as impressões digitais obtidas no trabalho [9], que simulou e gerou imagens dos ataques obtidos mediante ferramentas comumente utilizadas por invasores. Utilizou-se o recurso de coordenadas paralelas para representar o relacionamento de portas externas com as portas internas do equipamento monitorado. O recurso de coordenadas paralelas tem boa aplicabilidade em redes pequenas, pois identifica melhor os elementos relacionados. Em uma rede com grande volume de tráfego e muitos componentes, como um *backbone por* exemplo, a apresentação visual com o uso desta técnica fica prejudicada pelo excesso de informação visual, o que dificulta sua análise.

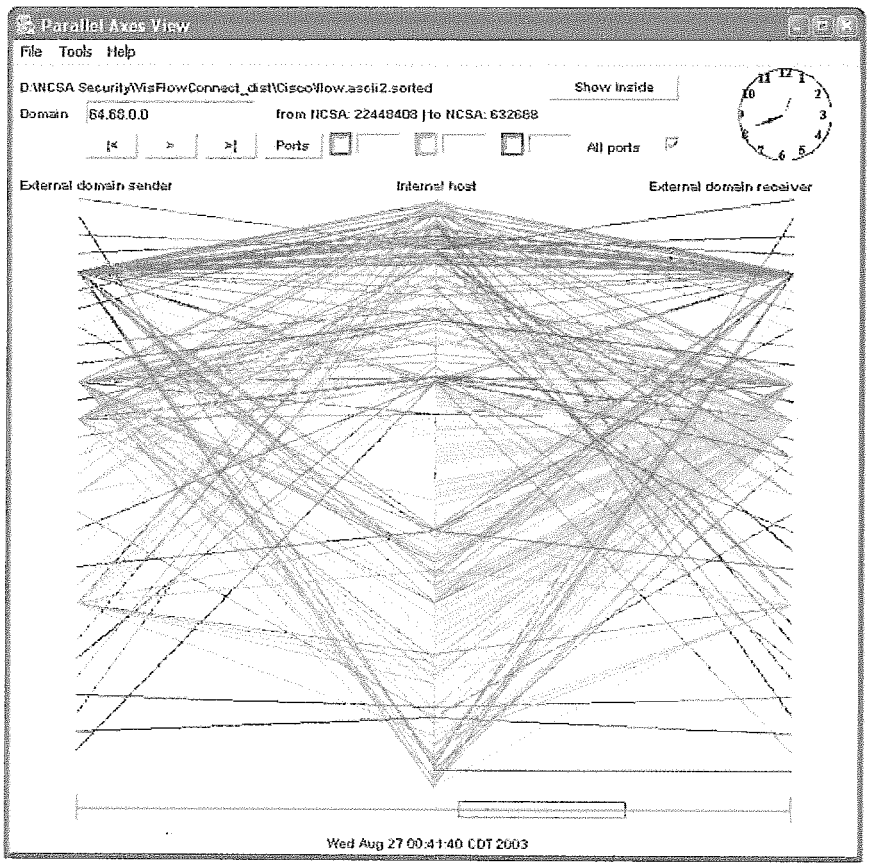

Figura 2.16: VisFlowConnect e sua visão de tráfego suspeito [8].

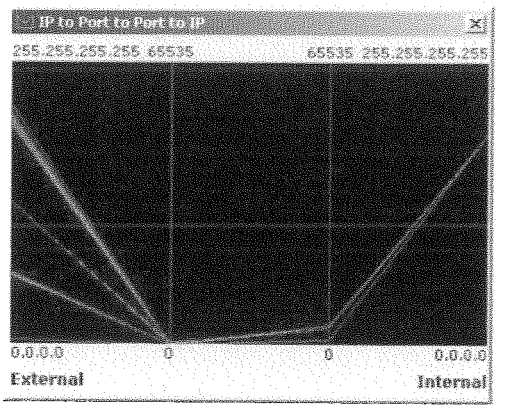

Figura 2.17: Impressão digital visual passiva [9].

Em [10], desenvolve-se um sistema que gera as visualizações baseadas na representação de um grafema ("*glyph*"), onde todos os sistemas monitorados são representados como nós. Os nós são conectados pelos raios que são feitos de acordo com as características do tráfego entre os nós. A sua aplicação à segurança de redes se dá como indício de uma possível atividade indesejável, sendo necessária análise adicional para sua identificação. A Figura 2.18 representa o mecanismo de detecção de intrusão desta abordagem, que mostra o sistema monitorado no centro da janela e os sistemas conectados em círculos concêntricos ao redor. Neste sistema, cada raio representa uma dezena de usuários e a espessura do círculo interno representa a carga do sistema. Um nó com duas linhas paralelas é indicativo de uma conexão não autenticada. Se as linhas paralelas forem vermelhas, significa que houve falha de autenticação. As linhas contínuas são conexões de *telnet* ou *rlogin*, as linhas tracejadas longas são conexões privilegiadas de *FTP* e as linhas tracejadas curtas são conexões *FTP* anônimas. As linhas com setas múltiplas, geralmente quatro, são indicativas de conexões *NFS*. Uma conexão NFS perdida é representada destacando-se o nó em amarelo. As linhas vermelhas grossas representam ataques identificados. O uso da representação de grafemas, da mesma forma que o estudo apresentado em coordenadas paralelas, quando aplicado em uma rede com grande volume de tráfego e muitos elementos, fica prejudicado pelo excesso de informação visual, dificultando a análise como um todo.

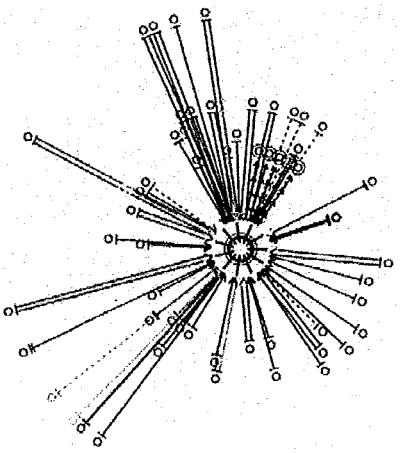

Figura 2.18: Visualização de detecção de intrusão [10].

Em [5], explora-se o recurso visual, a fim de apresentar o resultado da classificação e filtragem do tráfego capturado, realizado pelo algoritmo RADAR (descrito na Seção ??). Nesta abordagem, utiliza-se um gigantesco espaço tridimensional (2^{32} X 2^{32} X 2^{16}), onde são plotados somente os fluxos com assinaturas de ataques, apresentando formas geométricas regulares e distintas e explorando a capacidade visual para a identificação dos eventos de negação de serviço (*DoS - Deny of Service*), varreduras de equipamentos (*hostscan*) e varreduras de portas (*portscan*). A Figura 2.19 mostra um ataque de negação de serviço (DoS1), que utiliza somente a metade do espaço de endereços IP de origem possíveis e todas as portas de destino possíveis. O ataque de negação de serviço (DoS2) utiliza todo o espaço de endereços IP de origem e somente as portas de destino inferiores a 1024. São mostradas também as varreduras de equipamentos e varreduras de portas, representadas graficamente. A idéia da visualização, em uma única imagem, de todo o espaço de endereçamento IP possível, associado às todas as portas de destino possíveis, é utilizada neste trabalho no Capítulo 4, para a implementação da metodologia proposta.

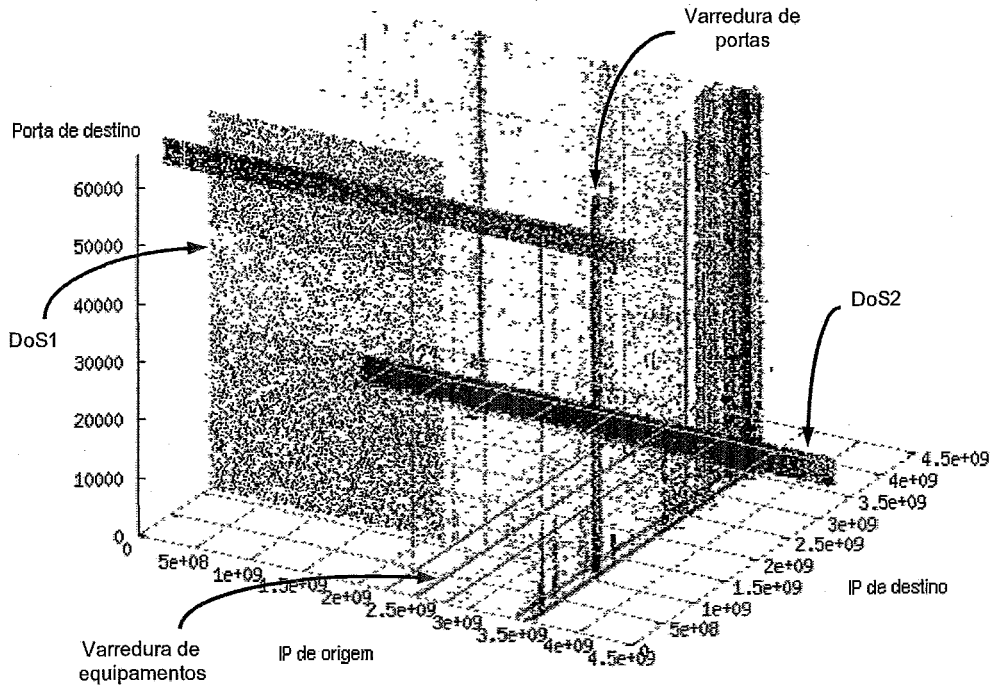

Figura 2.19: Plotagem tridimensional de um tráfego trans-pacifico [5].

2.7 Considerações Finais

Este capítulo ateve-se a descrever a fundamentação teórica necessária para a compreensão deste trabalho. Foram apresentados os fundamentos das comunicações das redes de computadores sobre a *Internet* com base no modelo *Internet* TCP/IP. Posteriormente, foram apresentadas as principais técnicas utilizadas para o acesso e captura dos dados que trafegam na rede, suas vantagens e desvantagens. Em seguida, foram apresentadas as vantagens e desvantagens dos métodos de análise, baseados em pacotes, em relação à análise baseada em fluxos. Por fim, foram apresentados os aspectos do comportamento dos padrões de anomalias dos *worms* e suas principais técnicas de varreduras. O próximo capítulo mostrará, como a análise das peculiaridades descritas até então, nos permite identificar padrões de tráfego indicadores de atividades de *worms*.

Capítulo 3

Metodologia Proposta para Classificação de Tráfego de Propagação dos *Worms*

No Capítulo 1 pudemos observar o princípio de funcionamento das metodologias comumente utilizadas na identificação de atividades maliciosas em rede e como as abordagens relacionadas se enquadram nestas metodologias. Neste capítulo será apresentada uma nova metodologia para a identificação de comportamentos de atividades de propagação de *worms* em redes de dados, com base nas informações contidas nos cabeçalhos dos fluxos trafegados.

Propõe-se a automatização dos processos comumente praticados pelos gerentes de segurança, na tentativa de controle de incidente de atividades de *worms*, reduzindo, desta forma, o tempo de resposta para reação. Mostraremos como informações inerentes à comunicação entre equipamentos podem agregar valores às atuais técnicas de identificação de anomalias em rede. Isto é feito, tanto através das informações contidas nos sinalizadores dos fluxos de dados, que são acumulados e sumarizados por um mecanismo de captura de tráfego, quanto através do conhecimento prévio das portas comumente exploradas por aplicativos maliciosos. Antes de iniciar a especificação da metodologia para a classificação, os requisitos que a proposta deverá

atender serão relacionados. Posteriormente, serão apresentadas as premissas adotadas pela proposta e, finalmente, explanaremos a técnica de visualização de fluxos adotada.

3.1 Requisitos

Esta seção descreve as necessidades de funcionalidade da metodologia proposta. A seguinte lista define os requisitos ordenados por importância:

Prover subsídios para a manutenção da segurança de redes

Como mencionado anteriormente, a solução deverá prover informações relevantes para a manutenção da segurança de um ambiente de rede, baseadas no que efetivamente está ocorrendo e não com base em arquivos de registros de ações banidas por dispositivos de segurança tradicionais (*firewall*, listas de acesso, etc).

Identificar atividades de pragas digitais (worms)

A metodologia proposta deverá reconhecer tráfego oriundo de atividade de *worms*, baseado nos princípio de funcionamento dos *worms*, descrito na Seção 2.4 e dos protocolos de transporte utilizados em rede.

Apresentar visualmente o resultado das análises do tráfego

Deverá ser adotada uma apresentação dos resultados da classificação de maneira visual e concisa, de forma a facilitar a tomada de decisão, por parte dos administradores de segurança, nos casos de controle de incidentes na rede.

Não interferir no tráfego benigno

O tráfego benigno não poderá sofrer perda de pacotes ou retardo, ou seja, não deverá sofrer interferências.

3.2 Definições de Premissas

Analisando-se o princípio de funcionamento dos protocolos da camada de rede e as peculiaridades apresentadas pelas características das atividades dos *worms*, podemos identificar os padrões de tráfego indicadores dessas atividades.

As características dos *worms* foram apresentadas na Seção 2.4. Também foram classificados de acordo com o mecanismo de escolha das vítimas e pelo tráfego gerado em suas varreduras. A metodologia, para detecção dos *worms* apresentada neste trabalho, está focada no tráfego das varreduras que ocorrem na rede.

Todos os equipamentos infectados com um código de *worm*, durante a sua fase de proliferação, apresentam a característica de envio de pacotes para as vítimas em potencial. Muitos *worms* buscam explorar certas vulnerabilidades encontradas em aplicações em portas determinadas. Os *worms* podem usar diversos métodos de varreduras, desta forma, cada varredura tem sua característica própria.

Diversos sítios da *Internet* [53, 54, 55, 56] divulgam listas correlacionando as mais variadas portas com os respectivos *malwares* associados. Desta forma, é possível montar uma base inicial de informações contendo as portas comumente exploradas por estes elementos.

Com base nas informações acima especificadas, as seguintes premissas são assumidas pelo algoritmo de classificação como indicadores de tráfego malicioso:

1) Como visto na Seção 2.1.2, na maioria das implementações TCP/IP, um equipamento cliente aloca um número de porta entre 1024 e 5000 para efetuar a comunicação com um servidor. A fim de alcançar todas as implementações, assume-se que um equipamento cliente inicia uma conexão por meio de uma porta superior a 1023.

2) Para o caso do uso do protocolo TCP, durante a fase de propagação do *worm*, assume-se que o primeiro pacote transmitido será um pacote TCP SYN. Como o UDP não é orientado à conexão, assume-se que o primeiro pacote UDP entre dois equipamentos será interpretado como o pacote de início da comunicação entre os dois equipamentos.

3) Respostas TCP RST indicam que houve uma falha na tentativa de conexão TCP a um equipamento protegido por dispositivos de segurança, conseqüentemente, assume-se que um tráfego com este perfil é um indicador de atividade maliciosa.

4) Devido ao fato de as portas de destino, comumente exploradas pelos *worms*, serem de conhecimento prévio, assume-se a existência de uma base de portas suspeitas que será utilizada como parâmetro de análise do tráfego malicioso.

5) Assume-se que, se uma porta de destino não pertencente à base de portas previamente conhecidas como exploradas por *worms* apresentar um volume de tráfego superior a 1% do volume total do tráfego analisado, esta nova porta será incorporada à base de portas suspeitas. A estimativa deste valor está baseada em [57], que registra a distribuição do percentual de fluxos utilizados por serviço, observados em um período de sete semanas. Os dados foram coletados do *backbone* da Rede Rio [24], que é uma rede acadêmica e de pesquisa, de onde também serão coletados os dados utilizados neste trabalho. Analisando-se a Tabela 3.1, que apresenta a sumarização da distribuição dos fluxos por serviço conforme [57], podemos confirmar o aumento da tendência do uso de ferramentas de compartilhamento *P2P*, visto que o serviço E-Donkey ocupa a segunda colocação em fluxos trafegados, superando em muito os serviços de transferência de arquivos (FTP), correio eletrônico (SMTP) e outros. Como visto na Subseção 2.6.1, em [5], a presença do tráfego de aplicativos *P2P* contribui para ocorrências de falsos positivos.

Serviço	**Percentagem de Fluxos**
Web	43,02
E-Donkey	11,94
DNS	4,35
HTTPS	3,81
SMTP	3,20
SSH	0,94
FTP	0,04
Outros	31,63

Tabela 3.1: Serviços utilizados na Rede Rio em um período de sete semanas

3.3 Definição da Metodologia

O monitoramento do tráfego e a identificação de problemas de segurança em tempo real, em ambientes sem restrições de acessos é uma tarefa difícil, devido à manipulação de grande volume de informações e das dificuldades encontradas para identificar atividades anômalas de uma maneira geral.

Neste trabalho, buscamos utilizar os recursos que melhor atendam às necessidades da análise do tráfego e da identificação de anomalias. Desta forma, adotamos o monitoramento do tráfego da rede, baseado em fluxos de dados, a fim de não interferir no tráfego benigno e minimizar as probabilidades de perdas de pacotes. Utilizamos o diferencial de rapidez e eficiência das classificações baseadas em assinaturas, em conjunto com a automação da atualização da base de dados de portas suspeitas, utilizada na geração das assinaturas, a fim de identificar novos tipos de varreduras dos *worms*. Na Subseção 2.6.1, vimos que a manutenção da base de assinaturas é uma tarefa onerosa em termos de trabalho humano e tempo. A automação da atualização da base de dados de portas suspeitas visa a minimizar este problema.

Como visto na Subseção 2.6.1, trabalhos relacionados à aplicação do monitoramento, voltado para a análise de segurança das redes, foram realizados adotando algoritmos e critérios de classificação de atividades maliciosas. Basicamente os estudos estão focados na análise da variação do volume de tráfego, na variação do número de conexões abertas, na periodicidade de ocorrência dos fluxos ou no conteúdo dos dados dos pacotes trafegados. As metodologias tradicionais não fornecem subsídios para uma reação imediata, necessitando de procedimentos manuais do gerente de segurança para a identificação do autor da anomalia. Além de não classificarem, com eficácia e de forma imediata, as características das atividades de propagação de *worms*, que consomem recursos preciosos da rede durante sua proliferação. A Figura 3.1 retrata as tarefas executadas nas metodologias tradicionais já explanadas.

A metodologia proposta, diferentemente das metodologias tradicionais, simplifica o trabalho realizado pelos gerentes de segurança, proporcionando uma visão, em

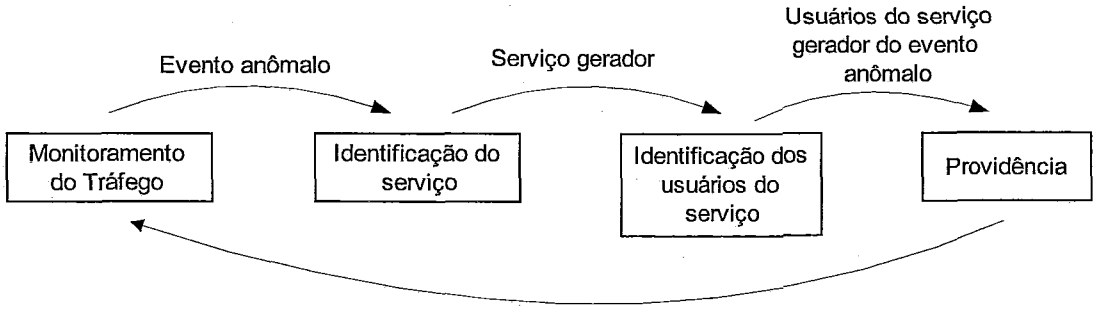

Figura 3.1: Diagrama esquemático das metodologias comumente utilizadas.

tempo próximo do real, das ocorrências de eventos, frutos da propagação de *worms* e um acesso imediato às informações necessárias para a adoção das providências para sanar o problema, além de prover uma base de histórico de ocorrências destes eventos, fornecendo subsídios para futuras análises forenses caso sejam necessárias.

A Figura 3.2 apresenta um diagrama esquemático da metodologia proposta, que consiste em:

1. Monitoramento da rede - A partir do monitoramento da rede, visualiza-se a ocorrência de eventos oriundos de atividades de propagação de *worms*

2. Providência - Com base nas informações fornecidas imediatamente, o gerente de segurança pode adotar as providências cabíveis para a solução do problema.

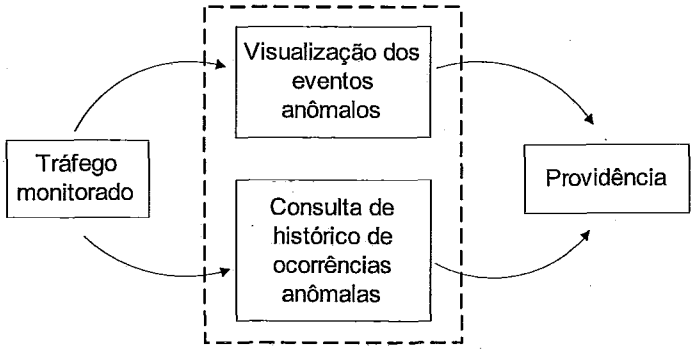

Figura 3.2: Diagrama esquemático da metodologia proposta.

Para a execução da metodologia proposta, utiliza-se uma base de fluxos coletados que serão classificados através de um algoritmo baseado em assinaturas propostas.

Em seqüência, os dados filtrados são armazenados em uma base de histórico de registros de ocorrências, nos formatos de texto e de imagem, e então são apresentados visualmente. Na Seção 3.5 esta visualização será abordada em mais detalhes.

3.4 Definição do Algoritmo de Classificação Proposto

O algoritmo de classificação proposto está fundamentado na análise de tráfego baseada em fluxos, discutida na Subseção 2.6.1, a fim de atender ao requisito de não interferência do tráfego benigno, além de minimizar a probabilidade de perda dos pacotes analisados.

Desta forma, o algoritmo proposto para a classificação e filtragem de tráfego com características de atividades de *worms* é definido da seguinte forma:

Algoritmo 1 Algoritmo de classificação de tráfego com propagação de *worms*.

1: **se** porta de origem > 1023 e porta destino = porta *worm* e protocolo = TCP e flag = SYN **então**
2: indicador *worm* = SYN_TCP;
3: **senão se** porta de origem > 1023 e porta destino = porta *worm* **então**
4: indicador *worm* = SYN_UDP;
5: **senão se** porta de origem > 1023 e protocolo = TCP e flag = RST/ACK **então**
6: indicador *worm* = SYN_half_open;
7: **senão se** protocolo = TCP e flag = RST **então**
8: indicador *worm* = FIN_Null_TCP;
9: **senão se** flag = RST/ACK **então**
10: indicador *worm* = SYN_TCP_porta_baixa;
11: **fim se**

- Se a porta de origem for maior que 1023, significa que se trata de uma porta efêmera, não sendo, desta forma, fruto de um processo do sistema ou programa

executado por usuário privilegiado, como visto na Subseção 2.1.2. Neste caso, cabe analisar se a porta de destino é uma das portas previamente conhecidas como portas utilizadas pelos *worms*. Se as sentenças anteriores forem verdadeiras, analisa-se se o protocolo de origem é o TCP. Tal análise visa verificar se o fluxo se refere a uma resposta de um servidor para uma porta efêmera.

- Se o protocolo for TCP e o sinalizador do fluxo indicar que é uma tentativa de inicio de conexão (SYN), este comportamento é caracterizado como sendo oriundo de um processo utilizado na propagação de *worm*, denominado neste trabalho como SYN_TCP. Se o protocolo não for TCP, conseqüentemente, ele não será orientado à conexão. Desta forma, não é necessário analisar o sinalizador, sendo este fluxo caracterizado como oriundo de um processo utilizado na propagação de *worm* denominado neste trabalho como SYN_UDP.

- O próximo passo do algoritmo é a análise das técnicas de varreduras utilizadas pelos *worms* para exploração de serviços em portas registradas no IANA [29]. Quando o fluxo é de um protocolo TCP, possui porta de origem superior a 1023 e apresenta os sinalizadores RST e ACK ativos, conclui-se que este fluxo é uma resposta de uma tentativa de conexão em uma porta que não está apta a receber conexões para a troca de dados; para este tipo de comportamento é atribuída a assinatura SYN_half_open.

- Caso o fluxo seja de um protocolo TCP e, se este apresentar o sinalizador RST ativo, conclui-se que este fluxo é uma resposta ao pacote recebido sem sinalizador nenhum ativo, onde o receptor interpreta que o pacote, em início de conexão com todos os sinalizadores desativados, não deveria chegar até ele e cancela a conexão enviando um fluxo com o sinalizador RST ativo. Este tipo de comportamento recebe a assinatura FIN_Null_TCP.

- Finalizando, os fluxos, que não possuem porta de origem maior que 1023 e apresentam os sinalizadores RST e ACK ativos, são caracterizados como tentativas de conexões oriundas de aplicativos privilegiados destinados a serviços

protegidos por mecanismos de segurança. Para este tipo de comportamento é atribuída a assinatura SYN_TCP_porta_baixa.

3.5 Visualização de Fluxos

A técnica de visualização dos fluxos permite que um operador, invocando o poder do sistema visual humano, identifique instantaneamente o estado da rede monitorada, provendo a imediata avaliação de ocorrência de problemas. Isto permite ao gerente de segurança identificar e implementar uma solução antes que a rede monitorada possa sofrer maiores danos.

A alta dimensionalidade e a sumarização dos resultados faz da utilização do espaço tridimensional de (2^{32} X 2^{32} X 2^{16}), abrangendo todo o endereçamento IP de origem, todo o endereçamento IP de destino e todas as portas de destino possíveis, um recurso visual adequado para a apresentação dos resultados da classificação utilizada na metodologia deste trabalho.

Na Seção 5.1 será mostrada a praticidade do uso desta técnica na obtenção dos resultados desejados.

3.6 Considerações Finais

Este capítulo apresentou a metodologia proposta para a classificação de tráfego de propagação de worms. Mostrou como informações inerentes à comunicação entre equipamentos podem agregar valores às atuais técnicas de identificação de anomalias em rede. As necessidades de funcionalidade desta metodologia e as premissas assumidas pelo algoritmo de classificação proposto foram apresentadas. Também foi reportado o recurso visual utilizado para a apresentação dos resultados da classificação.

Capítulo 4

Aplicação da Metodologia ao Monitoramento da Segurança de Redes

Este capítulo tem por finalidade apresentar a implementação da metodologia proposta no Capítulo 3. A arquitetura do sistema e os seus diversos módulos são apresentados e comentados. O cenário da implementação é descrito em seguida, juntamente com um resumo das tecnologias empregadas e a descrição do funcionamento do sistema.

4.1 Objetivo

O objetivo do sistema é efetuar a classificação e filtragem do tráfego coletado, visando à identificação e apresentação visual do tráfego com atividades oriundas de propagação de *worms*, em tempo próximo do real. A sua idéia, por analogia, pode ser comparada à de uma câmera de segurança, que registra e apresenta somente as imagens dos atos suspeitos. , além de prover um histórico desses registros para posteriores análises, caso necessário.

4.2 Arquitetura do Sistema

A arquitetura do sistema, representada na Figura 4.1, segue o modelo proposto pelo *Real-Time Flow Measurement* (RTFM) [35] utilizado pela arquitetura *Netflow*, apresentado na Seção 2.2.2, que é composta por três elementos: o sensor, o coletor e o analisador (ou gerente).

- Sensor - Captura, sumariza e exporta os fluxos trafegados. Função realizada, na implementação, por um roteador CISCO, exportando fluxos com formato *Netflow* Versão 5.

- Coletor - Recebe os registros de fluxos exportados pelo sensor e os armazena em arquivos. Função realizada, na implementação, por uma das ferramentas do conjunto *flow-tools*, o *flow-capture*. Esta ferramenta recebe os registros de fluxos e os armazena em arquivos gerados e organizados em intervalos de um minuto.

- Analisador - A partir dos arquivos de fluxos gerados, efetua as análises necessárias. Na implementação efetuada, esta função é executada por uma ferramenta desenvolvida neste trabalho, composta por módulos, responsáveis pelo processamento dos fluxos coletados, para a extração das informações necessárias ao monitoramento das atividades de propagação dos *worms* na rede.

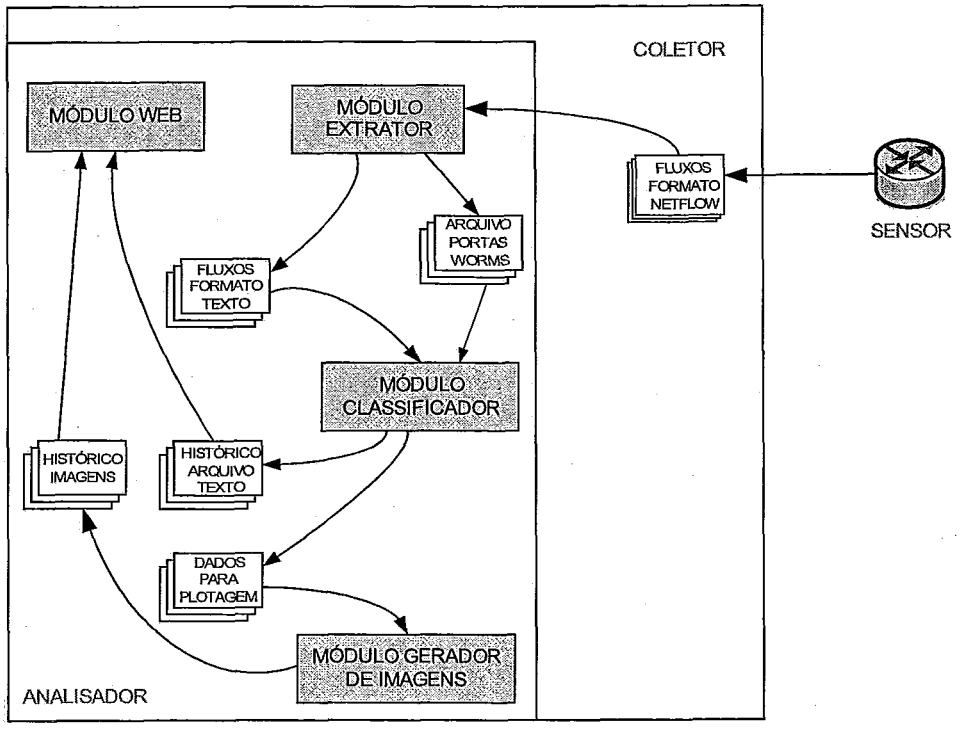

Figura 4.1: Arquitetura do sistema.

4.3 Ferramenta de Análise do Tráfego

A automação necessária para classificação, filtragem e apresentação das atividades oriundas da propagação dos *worms* na rede, depende de um conjunto de ferramentas, agregadas em módulos, que apresentaremos a seguir.

O "Módulo Extrator" é o responsável pela adaptação dos dados armazenados no formato *Netflow* para o formato texto, extraindo as informações necessárias para a entrada do "Módulo Classificador". Este módulo também efetua a verificação da existência de alguma porta não cadastrada no arquivo de portas comumente utilizadas pelos *worms*. Caso seja observado um volume de fluxos superior a 1% do volume total trafegado no último minuto, este módulo também será responsável pelo cadastramento desta porta no referido arquivo de portas, que será utilizado pelo "Módulo Classificador".

O "Módulo Classificador" analisa os fluxos convertidos pelo "Módulo Extrator"

e efetua a classificação e filtragem dos fluxos, de acordo com o algoritmo de classificação de tráfego com atividades de *worms*, proposto na Seção 3.4. Para cada tipo de assinatura gerada, este módulo cria um arquivo com as informações necessárias para a montagem do histórico das ocorrências e um arquivo com as informações necessárias para o "Módulo Gerador de Imagem".

O "Módulo Gerador de Imagem" é responsável pela plotagem dos arquivos de fluxos classificados, gerados pelo "Módulo Classificador". É explorada a técnica utilizada em [5] e discutida aqui na Seção 3.5. Este módulo também é responsável pelo mecanismo de alimentação do histórico dos dados analisados.

O "Módulo Web" é responsável pela apresentação dos resultados gerados pela ferramenta. A fim de proporcionar flexibilidade para seu acesso, as imagens do estado da segurança da rede e as respectivas estatísticas de processamento são apresentadas via ambiente Web, através deste módulo. Este módulo fornece, ainda, os controles para solicitação de informações analisadas no passado, proporcionando o acesso ao histórico gerado pela ferramenta.

4.4 Cenário da Implementação

O protótipo foi implementado, utilizando a monitoração passiva dos dados capturados, oriundos do *backbone* da Rede Rio [24], que é uma rede *gigabit ethernet*, integrada por universidades e centros de pesquisa localizados no Estado do Rio de Janeiro.

Os fluxos classificados são obtidos a partir do roteador de borda da Rede Rio [24], oriundos das interfaces ligadas à Embratel [58] e à Rede Nacional de Ensino e Pesquisa [59], sendo constituídos de todo o tráfego com destino à Rede Rio e todo o tráfego com origem na Rede Rio.

O coletor e o analisador dos fluxos encontram-se instalados em um equipamento do Laboratório de Redes de Alta Velocidade/COPPE [60], localizado na Universi-

dade Federal do Rio de Janeiro [61].

A Figura 4.2 reporta o cenário onde a implementação está executando.

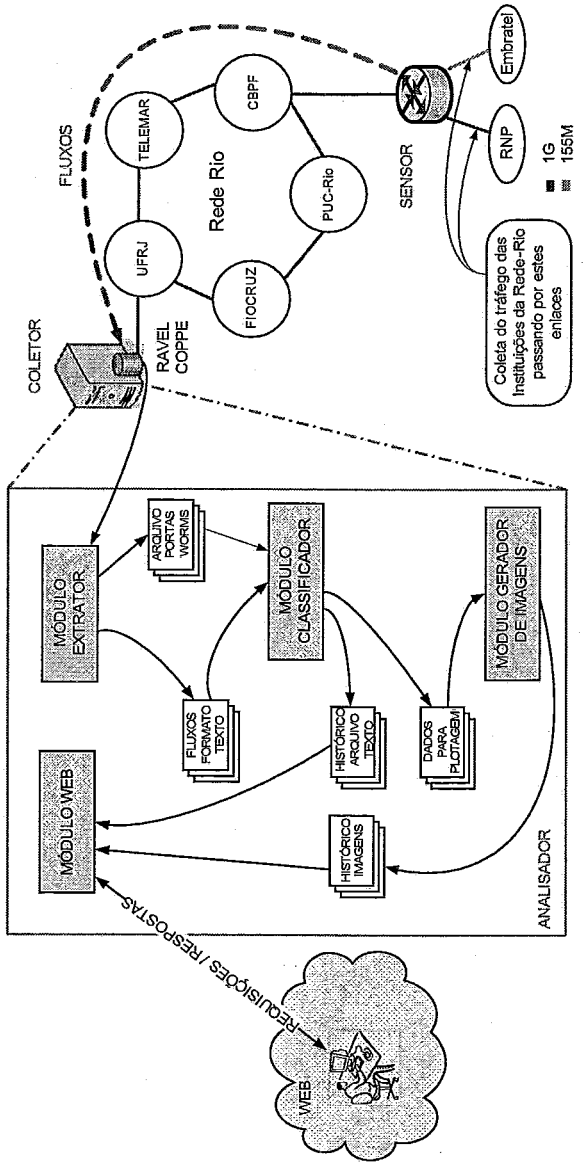

Figura 4.2: Cenário da implementação.

4.5 Tecnologias Envolvidas na Implementação

Na implementação do protótipo, buscou-se o uso de aplicativos de código aberto, com elevado grau de portabilidade entre as plataformas de *hardware* e *software* existente atualmente.

A Figura 4.3 ilustra as tecnologias envolvidas na implementação:

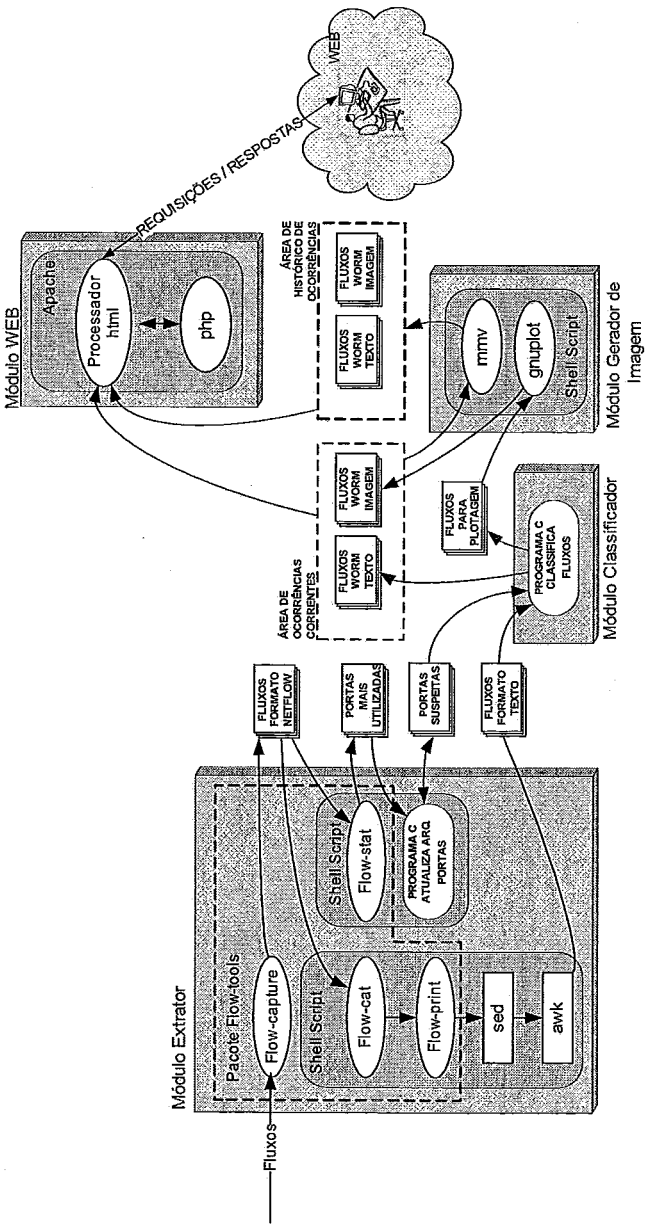

Figura 4.3: Tecnologias envolvidas na implementação.

Fonte de captura de fluxos

A implementação utiliza os fluxos de dados gerados pela ferramenta *Netflow*. A escolha do uso do *Netflow*, como fonte de captura de dados do tráfego da rede, ocorre pelo fato deste não interferir no tráfego benigno, além de ser a base para a especificação do protocolo de exportação de dados conforme definido pelo Internet Engineering Task Force (IETF) [41]. Como visto na Subseção 2.2.2, existem várias ferramentas de código aberto desenvolvidas para o sistema operacional *GNU/Linux*, que capturam, condensam e exportam os dados como se fossem um roteador Cisco com suporte ao *NetFlow*, não sendo esta, portanto, uma solução proprietária.

Coleta e manipulação dos registros de fluxos

Para a coleta e manipulação dos registros de fluxos, é utilizado um conjunto de ferramentas de código aberto denominado flow-tools [50]. Das diversas ferramentas que compõem o flow-tools, são utilizadas as ferramentas flow-capture (para a coleta, e armazenamento e gerência de espaço em disco), o flow-cat (para concatenação de arquivos de fluxos), o flow-print (para converter e apresentar os fluxos em caracteres ASCII) e o flow-stat (para apresentar resumos de utilização dos fluxos). Optou-se por esta solução por sua flexibilidade de configuração de filtros e sua rapidez de processamento. São utilizados, ainda, os recursos de *scripts* do ambiente *shell* (*Shell Script*) e a linguagem de interpretação de texto *AWK*. Graças ao ambiente *shell*, foi possível o desenvolvimento dos *scripts* de extração de dados utilizando-se os comandos básicos de uma distribuição Linux, evitando a necessidade do desenvolvimento de novos aplicativos.

Classificação dos fluxos

Por sua rapidez de processamento, o algoritmo de classificação proposto foi implementado utilizando-se a linguagem de programação C.

Visualização dos resultados

Para a visualização dos resultados classificados, são utilizadas as seguintes ferramentas:

- gnuplot - solução de código aberto para plotagem de gráficos tridimensionais;
- Apache Web Server - software de código aberto, multiplataforma, que possui suporte a várias linguagens CGIs (Common Gateway Interface), dentre as quais: o *Perl* e o *PHP*, é um dos servidores de *http* mais populares e estáveis já desenvolvidos. Este servidor tem por finalidade suportar a execução dos scripts *PHP* que formam o *front-end* do protótipo com o usuário.
- PHP - linguagem de **script** executada no servidor (*server-side*), que desde seu surgimento tem chamado atenção devido sua flexibilidade e portabilidade. Atualmente esta linguagem é suportada pela grande maioria dos servidores web incluindo: *Apache*, *Microsoft Internet Information Server*, *Personal Web Server* e etc.

4.6 Funcionalidades

A partir da tela de apresentação do protótipo, representada pela Figura 4.4, pode ser observado, no lado direito, a visualização das ocorrências de propagação de *worms* em andamento, classificadas por tipo de varredura (em destaque na Figura 4.5). No lado esquerdo da tela, são apresentados os resumos estatísticos referentes ao último minuto processado (em destaque na Figura 4.6), proporcionando acesso ao histórico de ocorrências e às imagens das propagações por assinatura, além das informações de ocorrências de tráfego de fluxos com endereçamento reservado.

As funcionalidades apresentadas pelo aplicativo, tais como o benefício obtido com a visualização permanente dos eventos anômalos da rede, provenientes da propagação de *worms* e o acesso imediato aos registros de ocorrências, possibilitam a adoção imediata de medidas necessária para conter uma epidemia de *worms* em andamento.

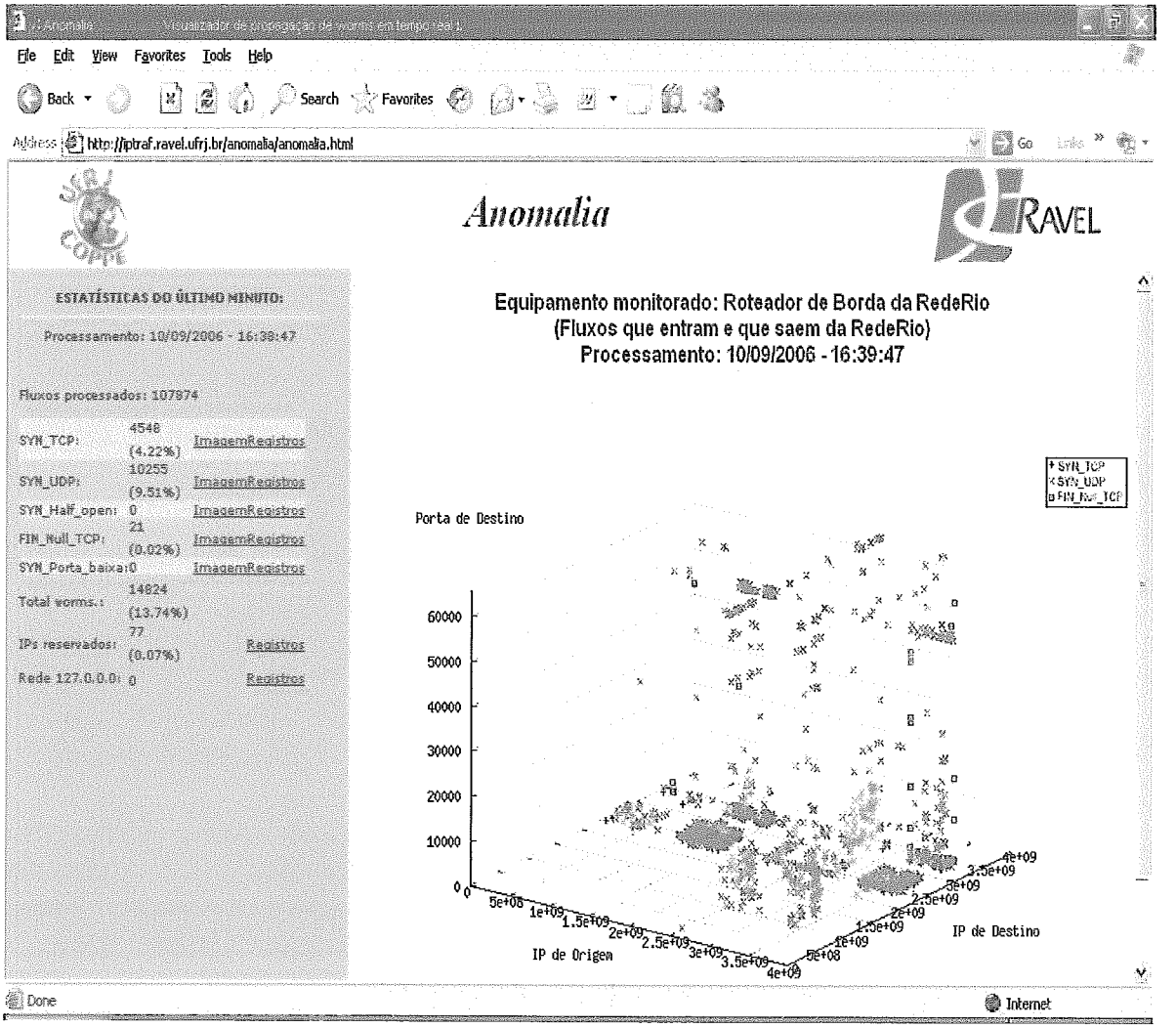

Figura 4.4: Front-end do aplicativo.

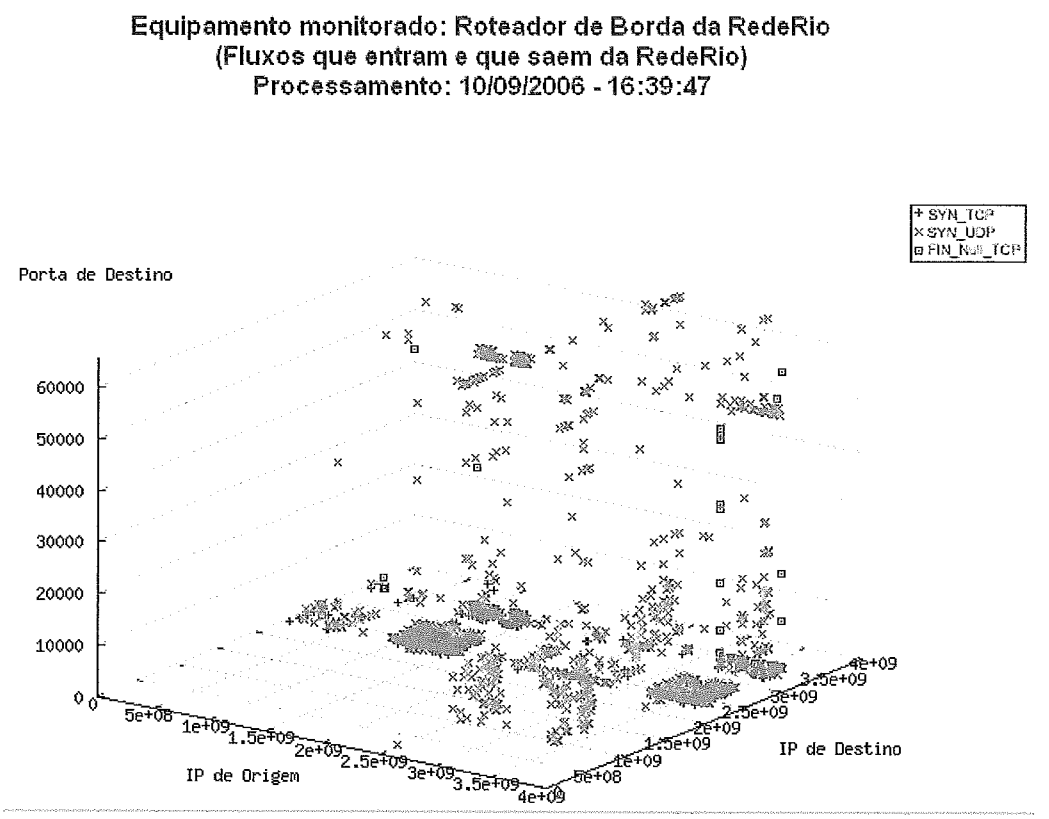

Figura 4.5: Visualisação de propagações em andamento.

ESTATÍSTICAS DO ÚLTIMO MINUTO:

Processamento: 10/09/2006 - 16:38:47

Fluxos processados: 107874

SYN_TCP:	4548 (4.22%)	ImagemRegistros
SYN_UDP:	10255 (9.51%)	ImagemRegistros
SYN_Half_open:	0	ImagemRegistros
FIN_Null_TCP:	21 (0.02%)	ImagemRegistros
SYN_Porta_baixa:	0	ImagemRegistros
Total worms.:	14824 (13.74%)	
IPs reservados:	77 (0.07%)	Registros
Rede 127.0.0.0:	0	Registros

Figura 4.6: Resumo estatístico do último minuto de processamento.

4.7 Considerações Finais

Neste capítulo, apresentamos a implementação da metodologia proposta para classificação de tráfego de propagação dos *worms*. A arquitetura do sistema e os seus diversos módulos foram discriminados e comentados. O cenário da implementação e as tecnologias adotadas foram descritos e, finalizando, foram expostas as funcionalidades obtidas pelo aplicativo. Mostramos como podemos, a partir de tecnologias de domínio público, aplicar a metodologia proposta a fim de proporcionar, ao gerente de segurança da rede, base para a adoção imediata de medidas necessárias para conter uma epidemia de *worms* em andamento.

Capítulo 5

Resultados Obtidos

Neste capítulo, apresentamos alguns resultados obtidos na aplicação da metodologia proposta, materializada no protótipo desenvolvido. Mostraremos, inicialmente, como as técnicas de propagação são identificadas, apresentadas visualmente e registradas em histórico, fornecendo os subsídios necessários para auxílio na tomada de decisão em incidentes de epidemias de *worms*. Posteriormente, serão apresentados os resultados referentes ao volume médio de fluxos, classificados como propagação de *worms* e, finalmente, mostraremos o resultado do estudo do volume médio de tráfego, oriundo de endereçamento IP reservado encontrado no ambiente monitorado.

5.1 Visualização de Propagações de Worms

Apresentaremos, a seguir, as informações extraídas durante um minuto de análise da ferramenta implementada. Cabe ressaltar que os dados analisados foram extraídos de uma rede *gigabit ethernet*, conforme descrito na Seção 4.4. Desta forma, a partir de um grande volume de tráfego, podemos obter os seguintes resultados em um tempo próximo do real:

5.1.1 Visão global da rede monitorada

A Figura 5.1 apresenta uma visão global de todas as ocorrências de propagação ocorridas durante o intervalo de observação de um minuto. Além da informação visual da situação da segurança da rede, é informado o resumo estatístico do último minuto de processamento, onde, neste caso, foram analisados 387.835 fluxos, dos quais 30.575 (7,88%) foram classificados como oriundos de propagação de *worms*.

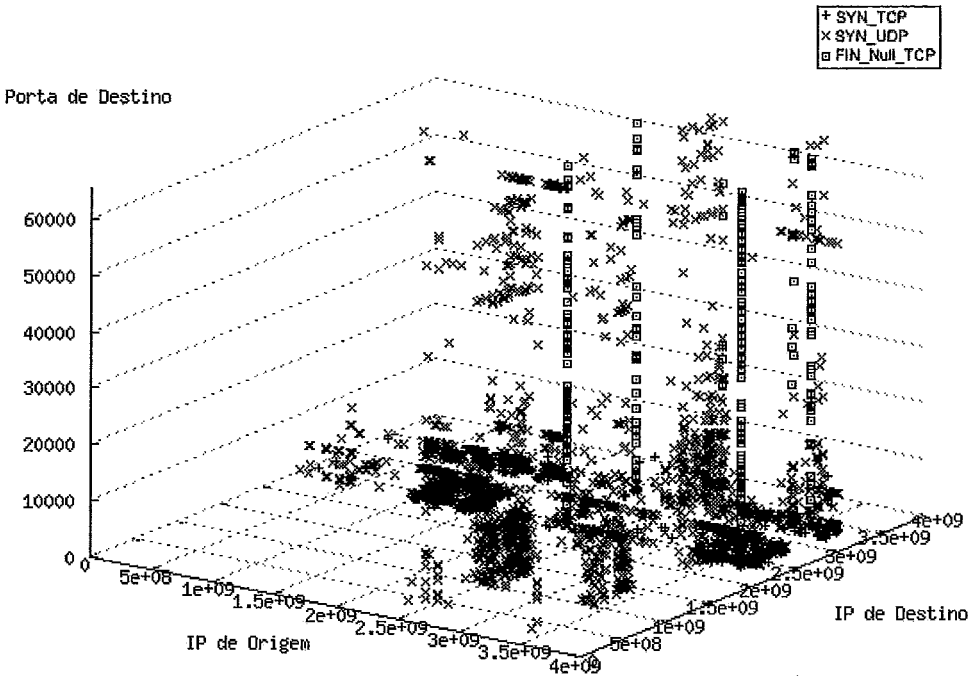

Figura 5.1: Visão global da rede monitorada em um minuto de análise. Cada ponto plotado representa uma anomalia encontrada e registrada no histórico de ocorrência. A apresentação gráfica das anomalias encontradas pode, ainda, formar linhas horizontais, representando ataques de negação de serviço e varreduras de equipamentos, e linhas verticais, representando varreduras de portas.

5.1.2 Visualização de propagação SYN_TCP

A Figura 5.2 destaca os fluxos classificados como provenientes de propagação do tipo SYN_TCP. Neste caso, são compostos, basicamente, de acessos às portas 135, 139 e 445 (como pode ser verificado no extrato do histórico correspondente, representado na Figura 5.3). Estes acessos visam a explorar a vulnerabilidade do serviço RPC[1] (Remote Procedure Call) do *Windows*, que permite ao atacante a execução de qualquer código desejável.

Para minimizar estas ocorrências, recomenda-se que as instituições, interligadas

[1] O RPC fornece um mecanismo de comunicação entre processos que permite que um programa de um computador execute, sem diferenças, códigos em um sistema remoto.

ao *backbone* monitorado, efetuem a filtragem das portas TCP do intervalo entre as portas 135 e 139 e das portas 445 e 593. Caso os IPs de origem dos referidos fluxos pertençam a equipamentos de uma instituição componente do *backbone*, esta instituição deverá ser notificada para que efetue as devidas correções nos respectivos equipamentos de origem.

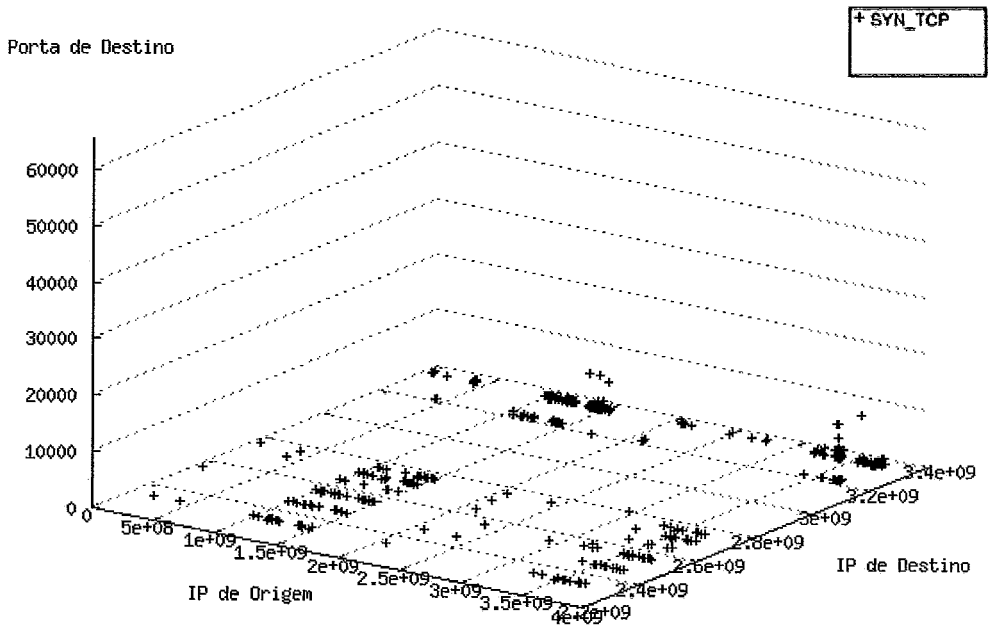

Figura 5.2: Visualização de propagação SYN_TCP. Cada ponto plotado representa um fluxo TCP com porta de origem superior 1023 e porta de destino comumente utilizada na propagação de *Worms*.

Seqüência	IP de origem	IP de destino	Prot.	P. Orig.	P. Dest.	Timestamp	Flag
1	24.109.180.253	200.156.186.139	6	2198	135	824.12:49:56	2
2	24.109.180.253	200.156.190.235	6	2224	135	824.12:49:57	2
...							
3864	89.236.74.250	200.156.82.90	6	2681	135	824.12:49:7	2
3865	89.236.74.250	200.20.151.249	6	2551	135	824.12:49:5	2
3866	89.236.74.250	200.20.26.46	6	3025	135	824.12:49:10	2
3867	24.173.101.217	192.80.209.198	6	1972	139	824.12:49:58	2
...							
3868	69.221.123.255	200.156.13.233	6	4049	139	824.12:50:0	2
3869	69.221.123.255	200.156.140.30	6	3665	139	824.12:49:14	2
...							
6576	86.197.27.82	139.82.54.8	6	2775	139	824.12:49:48	2
6577	86.197.27.82	139.82.54.9	6	2776	139	824.12:49:48	2
6578	4.154.111.133	200.156.77.7	6	2985	445	824.12:49:45	2
6579	4.226.111.108	152.92.88.87	6	2815	445	824.12:49:27	2
...							
6580	4.233.143.149	152.92.118.236	6	3212	445	824.12:49:16	2
6581	4.235.206.103	200.20.106.26	6	4529	445	824.12:49:23	2
...							
9680	89.50.118.205	200.156.41.157	6	3831	445	824.12:49:50	2
9681	89.51.127.200	164.85.124.221	6	4045	445	824.12:49:30	2

Figura 5.3: Extrato do histórico de propagação SYN_TCP. Apresenta as informações necessárias (IP de origem, IP de destino, porta de origem, porta de destino, protocolo, sinalizador e registro do dia/horário da ocorrência) para a adoção de medidas cabíveis para a solução da anomalia.

5.1.3 Visualização de propagação SYN_UDP

A Figura 5.4 destaca os fluxos classificados como provenientes de propagação do tipo SYN_UDP. Foram encontrados diversos fluxos com porta de destino 127. Estes acessos buscam por serviços *Netbios SMB*, que podem ser indícios de buscas por informações sobre as vítimas, através do aplicativo *NBSTAT*, ou indícios de propagação do *worm* conhecido como *network.vbs*. O processo de infecção se inicia com uma solicitação do aplicativo NBSTAT, caso a solicitação seja atendida, o *worm* tentará uma sessão na porta TCP 139 e irá tentar montar a partição "C" para compartilhamento sem senha. Caso o *worm* tenha sucesso, ele irá se instalar em vários diretórios da vítima. Na maioria dos casos, o objetivo deste *worm* é somente a sua proliferação, porém, nada impede que ele execute tarefas mais prejudiciais. Foram encontradas, ainda, muitas ocorrências de fluxos destinados à porta 1434. Estes fluxos, provavelmente, são oriundos de sistemas infectados com o *worm SQL Slammer*, buscando por vulnerabilidades em servidores SQL, a fim de infectá-los. A

Figura 5.5 representa um extrato do histórico correspondente a estas propagações.

Para minimizar estas ocorrências, recomenda-se que as instituições interligadas ao *backbone* monitorado efetuem a filtragem das portas acima relacionadas. Caso os IPs de origem dos referidos fluxos pertençam a equipamentos de uma instituição componente do *backbone*, esta instituição deverá ser notificada para que efetue as devidas correções nos respectivos equipamentos de origem.

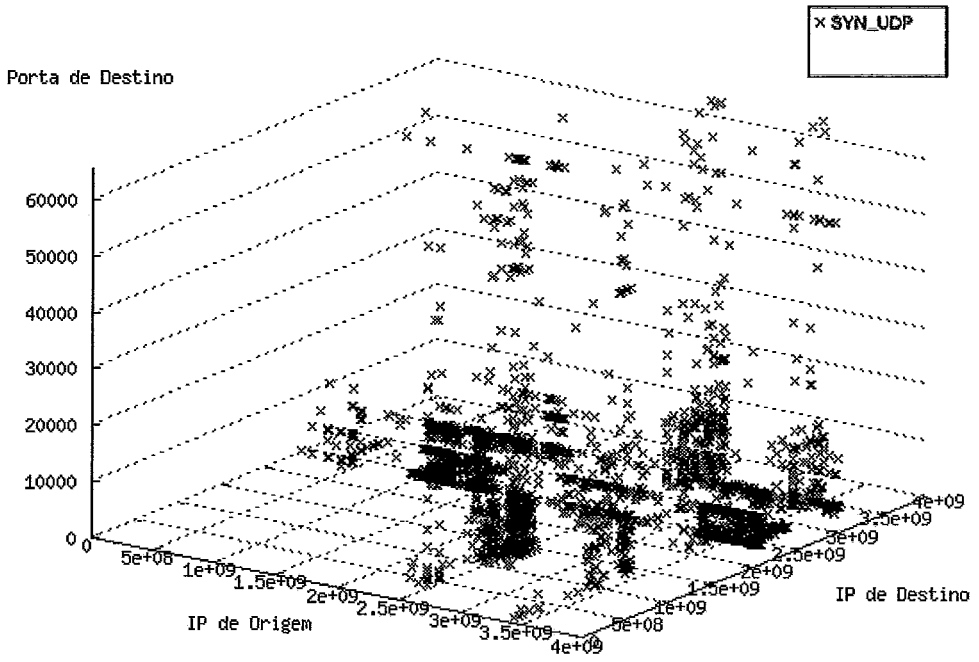

Figura 5.4: Visualização de propagação SYN_UDP. Cada ponto plotado representa um fluxo UDP com porta de origem superior 1023 e porta de destino comumente utilizada na propagação de *Worms*.

Seqüência	IP de origem	IP de destino	Prot.	P.orig.	P.dest.	Timestamp	Flag
1	70.104.130.122	200.156.205.100	17	1030	137	824.12:50:04	0
2	70.104.130.122	200.156.205.102	17	1030	137	824.12:50:05	0
...					...		
3266	85.97.108.174	152.92.81.98	17	1030	137	824.12:49:08	0
3267	200.20.217.63	199.146.22.106	17	1027	137	824.12:49:26	0
3268	200.20.217.63	199.146.22.107	17	1027	137	824.12:49:26	0
3269	200.20.217.63	199.146.22.108	17	1027	137	824.12:49:26	0
3270	200.20.217.63	199.146.22.109	17	1027	137	824.12:49:27	0
3271	200.20.217.63	199.146.22.110	17	1027	137	824.12:49:27	0
3272	200.20.217.63	199.146.22.111	17	1027	137	824.12:49:27	0
3273	200.20.217.63	199.146.22.112	17	1027	137	824.12:49:27	0
3274	200.20.217.63	199.146.22.113	17	1027	137	824.12:49:27	0
3275	200.20.217.63	199.146.22.114	17	1027	137	824.12:49:28	0
...							
6076	4.154.214.121	200.20.89.35	17	2145	1434	824.12:49:19	0
6077	24.165.194.156	161.79.118.135	17	2503	1434	824.12:49:27	0
6078	61.175.163.195	139.82.153.30	17	1048	1434	824.12:49:17	0
6079	61.175.163.195	139.82.160.85	17	1048	1434	824.12:49:24	0
6080	61.175.163.195	139.82.167.140	17	1048	1434	824.12:49:30	0
6081	61.175.163.195	139.82.174.195	17	1048	1434	824.12:49:37	0
6082	61.175.163.195	139.82.22.1	17	1048	1434	824.12:49:54	0
6083	61.175.163.195	139.82.236.182	17	1048	1434	824.12:49:15	0
6084	61.175.163.195	139.82.243.237	17	1048	1434	824.12:49:21	0
6085	61.175.163.195	139.82.36.111	17	1048	1434	824.12:50:07	0
6086	61.175.163.195	139.82.63.79	17	1048	1434	824.12:49:13	0
6087	61.175.163.195	139.82.77.189	17	1048	1434	824.12:49:26	0
6088	61.175.163.195	139.82.84.244	17	1048	1434	824.12:49:32	0
6089	61.175.163.195	139.82.91.43	17	1048	1434	824.12:49:39	0
6090	61.175.163.195	139.82.98.98	17	1048	1434	824.12:49:45	0
6091	61.175.163.195	146.164.10.170	17	1048	1434	824.12:49:52	0
6092	61.175.163.195	146.164.100.38	17	1048	1434	824.12:49:04	0
6093	61.175.163.195	146.164.22.27	17	1048	1434	824.12:49:09	0
...							

Figura 5.5: Extrato do histórico de propagação SYN_UDP. Apresenta as informações necessárias (IP de origem, IP de destino, porta de origem, porta de destino, protocolo, sinalizador e registro do dia/horário da ocorrência) para a adoção de medidas cabíveis para a solução da anomalia.

5.1.4 Visualização de propagação FIN_Null_TCP

A Figura 5.6 destaca os fluxos classificados como provenientes de propagação do tipo FIN_Null_TCP. Este tipo de assinatura de propagação foi definido para atender os casos de respostas aos fluxos de tentativa de conexão TCP sem nenhum sinalizador ativo. O comportamento do equipamento receptor seria o de desfazer a conexão enviando um fluxo com o sinalizador RST ativo. Porém, foram encontrados diversos fluxos classificados como FIN_Null_TCP que, a princípio, aparentavam ser um ataque de negação de serviço distribuído (*DDoS*), pois o padrão era um IP de origem emitindo diversos fluxos com porta de origem 80, para diversos IPs de

destino em diversas portas de destino. Desta forma, poderia ser interpretado que vários equipamentos estariam enviando pacotes sem sinalizadores para uma única vítima, na porta 80 e esta estaria emitindo diversos fluxos cancelando as tentativas de conexões.

Analisando-se um pouco melhor, foi observado que vários dos IPs de destino dos referidos fluxos não existem. Na verdade, são de classes IPs alocadas a instituições integrantes do *backbone*, mas que, efetivamente, não foram atribuídos a seus equipamentos. Devido a estas particularidade nestes fluxos classificados como provenientes de propagação do tipo FIN_Null_TCP, podemos considerar a possibilidade de serem originados de um ataque de força bruta TCP Reset.

A Figura 5.7 representa um extrato do histórico correspondente a estas propagações.

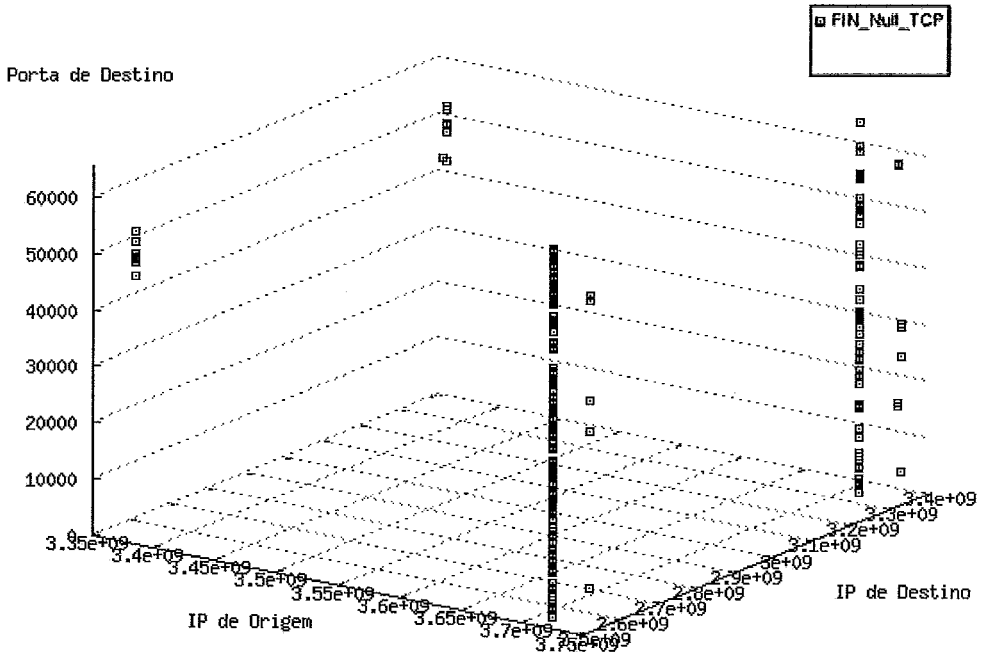

Figura 5.6: Visualização de propagação FIN_Null_TCP. Cada ponto plotado representa um fluxo de resposta a um fluxo TCP sem sinalizadores ativos. O conjunto destes fluxos representam, graficamente, uma varredura de portas.

Seqüência	IP de origem	IP de destino	Prot.	P.orig.	P.dest.	Timestamp	Flag
1	221.5.2.72	152.84.10.37	6	80	48685	824.12:49:36	4
2	221.5.2.72	152.84.10.94	6	80	27661	824.12:49:54	4
3	221.5.2.72	152.84.103.126	6	80	14436	824.12:49:34	4
...							
130	221.5.2.72	152.84.96.111	6	80	59933	824.12:49:30	4
131	221.5.2.72	152.84.98.20	6	80	30746	824.12:49:55	4
132	221.5.2.72	200.20.100.90	6	80	29030	824.12:49:52	4
133	221.5.2.72	200.20.106.123	6	80	40207	824.12:49:31	4
134	221.5.2.72	200.20.124.87	6	80	43868	824.12:49:47	4
135	221.5.2.72	200.20.125.43	6	80	4193	824.12:50:8	4
136	221.5.2.72	200.20.127.35	6	80	39734	824.12:49:23	4
137	221.5.2.72	200.20.127.88	6	80	4478	824.12:49:46	4
184	221.5.2.72	200.20.88.16	6	80	33852	824.12:49:43	4
185	221.5.2.72	200.20.89.77	6	80	55123	824.12:50:10	4
186	221.5.2.72	200.20.97.92	6	80	89	824.12:50:10	4
187	222.216.109.73	200.156.113.102	6	80	30260	824.12:49:36	4
188	222.216.109.73	152.84.121.88	6	80	34169	824.12:49:44	4
189	222.216.109.73	152.84.152.120	6	80	6472	824.12:49:33	4
...							
198	222.216.109.73	200.20.148.50	6	80	17031	824.12:49:44	4
199	222.216.109.73	200.20.220.25	6	80	16573	824.12:49:35	4
200	200.203.183.25	200.156.169.126	6	443	49649	824.12:49:49	4
201	200.203.183.25	200.156.218.201	6	443	52767	824.12:50:11	4
202	200.203.183.25	152.84.129.128	6	443	48325	824.12:49:27	4
203	200.203.183.25	152.84.137.113	6	443	49275	824.12:50:0	4
204	200.203.183.25	152.84.175.122	6	443	47705	824.12:49:21	4
205	200.203.183.25	152.84.18.145	6	443	48814	824.12:49:40	4
206	200.203.183.25	152.84.228.171	6	443	45427	824.12:50:18	4
207	200.203.183.25	152.84.31.12	6	443	51546	824.12:50:8	4
208	200.203.183.25	152.84.83.155	6	443	53304	824.12:50:17	4
209	200.203.183.25	200.156.143.32	6	443	48433	824.12:49:28	4
210	200.203.183.25	200.156.212.60	6	443	52371	824.12:50:16	4
211	200.203.183.25	200.156.89.61	6	443	43342	824.12:49:30	4
212	200.203.183.25	200.156.91.188	6	443	49736	824.12:49:49	4
213	200.203.183.25	200.20.48.147	6	443	44171	824.12:49:47	4

Figura 5.7: Extrato do histórico de propagação FIN_Null_TCP. Apresenta as informações necessárias (IP de origem, IP de destino, porta de origem, porta de destino, protocolo, sinalizador e registro do dia/horário da ocorrência) para a adoção de medidas cabíveis para a solução da anomalia.

5.2 Monitoramento de Fluxos Oriundos de Endereçamento Reservado

Como visto na Subseção 2.1.1, os endereços reservados e de uso interno não podem ser utilizados para o roteamento global. A presença de tráfego com estes endereçamentos, em um ambiente de roteamento global, é um indício de comprometimento da segurança da rede. A fim de mensurar este tipo comportamento do tráfego e proporcionar subsídios para a gerência da segurança da rede, foi introduzido, no algoritmo de classificação da ferramenta implementada, uma rotina para contabilizar e apresentar, em tempo próximo do real, mantendo o histórico de ocorrências, todos os fluxos trafegados que apresentem IPs originados ou destinados a endereçamento reservado e de uso interno. A Figura 5.8 apresenta um extrato do resultado da classificação de fluxos com estas características, em um período de observação de um minuto.

IP de origem	IP de destino	Prot.	P.orig.	P. Dest.	Timestamp	Flag
-- corta --						
10.10.100.39	82.129.35.231	17	137	137	825.21:39:40	0
10.10.100.39	82.129.35.235	17	137	137	825.21:39:41	0
10.10.100.39	82.129.35.237	17	137	137	825.21:39:41	0
10.10.100.39	85.17.34.14	17	137	137	825.21:39:10	0
10.10.100.39	88.213.35.5	17	137	137	825.21:39:25	0
10.10.100.39	96.121.34.0	17	137	137	825.21:39:05	0
10.10.100.39	96.67.34.0	17	137	137	825.21:39:05	0
10.10.13.3	200.20.186.75	17	1024	123	825.21:38:48	0
10.24.24.50	86.61.36.127	6	25	1300	825.21:39:20	0
139.82.74.4	172.16.129.109	6	51749	25	825.21:39:34	2
139.82.74.4	172.16.129.109	6	51749	25	825.21:40:20	2
146.164.34.145	172.28.1.10	6	1507	9876	825.21:39:37	2
146.164.34.145	172.28.1.10	6	1508	9876	825.21:39:47	2
200.156.51.12	10.1.5.33	1	8	0	825.21:39:40	0
200.156.51.12	10.1.5.37	1	8	0	825.21:39:38	0
200.156.51.12	10.1.5.41	1	8	0	825.21:39:41	0
200.156.51.12	10.1.5.46	1	8	0	825.21:39:41	0
200.156.51.12	10.1.5.49	1	8	0	825.21:39:40	0
200.156.51.12	10.1.5.5	1	8	0	825.21:39:41	0
200.156.51.12	10.17.0.1	1	8	0	825.21:39:38	0
200.20.114.67	192.168.0.255	17	520	520	825.21:39:49	0
200.20.114.67	192.168.0.255	17	520	520	825.21:40:19	0
200.20.189.231	192.168.0.1	6	3692	26760	825.21:39:45	2
200.20.189.244	192.168.0.1	6	1542	1393	825.21:40:01	2
200.20.92.177	192.168.0.10	1	0	781	825.21:39:31	0
200.20.92.177	192.168.0.27	1	0	781	825.21:40:09	0
200.20.94.1	172.16.10.8	1	0	781	825.21:40:04	0
-- corta --						

Figura 5.8: Extrato de ocorrências de fluxos oriundos de endereçamento reservado. Apresenta as informações necessárias (IP de origem, IP de destino, porta de origem, porta de destino, protocolo, sinalizador e registro do dia/horário da ocorrência) para a adoção de medidas cabíveis para a resolução do problema.

5.3 Volume Médio de Fluxos Classificados como Propagação de Worms

Em uma análise realizada entre 23 a 31 de agosto de 2006, foram observados em torno de 2 bilhões e 200 milhões de fluxos, dos quais, aproximadamente, 212 milhões (9,59%) foram classificados como tráfego oriundo de propagação de worms. A Tabela 5.1 apresenta o resumo estatístico por assinatura apresentado na análise.

Podemos observar a predominância de ocorrências de propagações classificadas como SYN_UDP, que caracteriza a preferência pela utilização de técnicas de propagação que não dependem de conexão e, conseqüentemente, são mais rápidas na proliferação.

Observa-se, ainda, a inexistência de propagações utilizando as técnicas de propagação SYN_Half_open e SYN_Porta_baixa. Tal fato é devido à falta de ocorrência de fluxos com somente os sinalizadores RST e ACK ativos, pois, provavelmente, os elementos de destino dos fluxos estão protegidos por dispositivos de segurança ou estão configurados para não fornecerem informações, caso a porta de destino não esteja apta a receber conexões para a troca de dados.

Descrição	**Número de fluxos**	**Percentual**
Total analisado	2.212.189.939	
SYN_TCP	71.623.813	3,24%
SYN_UDP	139.748.823	6,31%
SYN_Half_open	0	0
FIN_Null_TCP	932.873	0,04%
SYN_Porta_baixa	0	0
Total de tráfego de propagação de *worms*	212.305.509	9,59%

Tabela 5.1: Resumo estatístico por assinatura apresentado na análise, realizada entre 23 a 31 de agosto de 2006. Foram observados em torno de 2 bilhões e 200 milhões de fluxos, dos quais, aproximadamente, 212 milhões (9,59%) foram classificados como tráfego oriundo de propagação de worms.

5.4 Volume Médio de Fluxos Oriundos de Endereçamento Reservado

Em análise realizada entre 25 a 31 de agosto de 2006, foram observados aproximadamente 1 bilhão e meio de fluxos dos quais, em torno de 1 milhão e quatrocentos mil (0,096%), apresentaram endereços reservados como origem ou destino dos fluxos. Uma vez que o ambiente analisado é um *backbone Internet*, estes fluxos caracterizam possíveis falhas em configurações oriundas de algumas instituições interligadas ao backbone analisado, que, desnecessariamente, utilizam recursos da rede. E, como visto na Seção 2.1.1, estes fluxos são indícios de comprometimento da segurança da rede, podendo até mesmo serem oriundos de ataques que utilizam endereços forjados. Comparando-se com o volume médio de tráfego observado em [57], para o mesmo ambiente analisado, o volume destinado à propagação de fluxos com endereçamento reservado é superior ao volume de fluxos utilizados no serviço transferência de arquivos (File Transfer Protocol - FTP) que é de 0,040%.

5.5 Análise Comportamental de Um Elemento Monitorado

Com base nos dados armazenados nos históricos, podem ser extraídas várias informações estatísticas e visuais referentes a valores de variáveis específicas. Por exemplo, durante o período de uma hora, foram analisados em torno de 7 milhões de fluxos. Destes, 643 (0,009%) foram classificados como fluxos suspeitos oriundos de um determinado IP de origem (146.164.X.X) monitorado. Tendo como foco um endereço IP específico (146.164.X.X), podemos extrair a informação visual de seu comportamento durante o período observado. A Figura 5.9 representa graficamente a plotagem bi-dimensional dos pontos de IP de origem e porta de destino de cada fluxo classificado como suspeito, tendo como origem o IP monitorado.

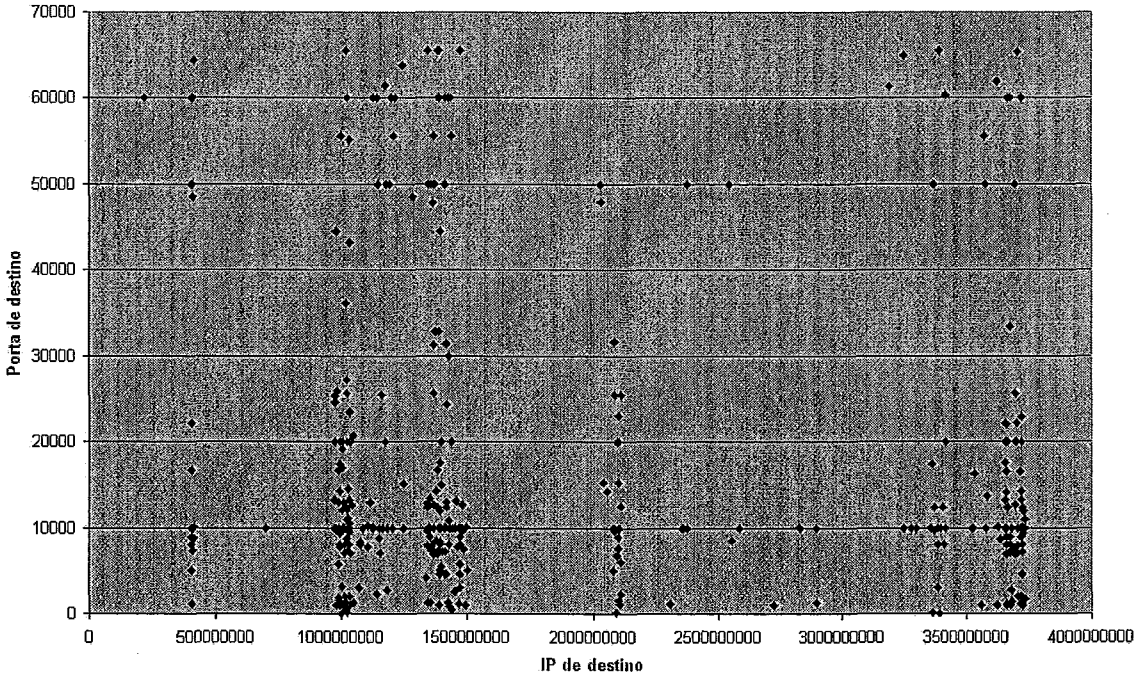

Figura 5.9: Exemplo de visualização comportamental de um elemento específico, mostrando a plotagem bi-dimensional dos pontos de IP de origem e porta de destino de cada fluxo classificado como suspeito, tendo como origem o IP 146.164.X.X, durante o intervalo de uma hora de observação.

Capítulo 6

Conclusões e Trabalhos futuros

A necessidade de conhecimento das atividades maliciosas que efetivamente ocorrem na rede dados, transformou a análise de tráfego em uma grande aliada da gerência da segurança de redes. Metodologias encontradas na literatura fundamentam-se em propriedades que, isoladamente, não fornecem informações suficientes para a tomada de decisão no controle de incidentes de segurança na rede.

O presente trabalho buscou utilizar os dados provenientes do tráfego da rede para fornecer subsídios necessários à manutenção da segurança das mesmas. Para tal, apresentou uma nova metodologia para a identificação de atividades provenientes da propagação de *worms* em rede. Com esta metodologia é possível, em tempo próximo do real, identificar o tipo de anomalia encontrada, além do autor, da vítima e do serviço utilizado no evento anômalo.

Por tratar-se de uma nova metodologia com base em métricas específicas, baseada na análise do cabeçalho do fluxo, não foi possível realizar o estudo comparativo da eficiência do algoritmo de classificação com outras soluções da literatura. Desta forma, foi realizada a comparação qualitativa e não quantitativa do trabalho. A redução dos procedimentos utilizados pelo gerente de segurança na identificação dos autores da anomalia, mostrou-se um diferencial qualitativo positivo e inovador em relação aos demais trabalhos da literatura.

Através da ferramenta implementada para validar a metodologia proposta, informações estatísticas e de utilidade imediata puderam ser obtidas. A partir destas informações, mostrou-se que é possível rapidamente localizar equipamentos contaminados com *worms*, fornecendo subsídios para o isolamento, através de listas de acessos nos equipamentos de segurança da infra-estrutura analisada, até realizar o contato com os responsáveis pelas redes das instituições interligadas ao *backbone*.

Explorou-se o recurso visual, como meio de divulgação do resultado da análise em tempo próximo do real, sem interferência no tráfego benigno.

Os resultados obtidos mostram que, em média, aproximadamente 10% de todos os fluxos trafegados são oriundos de propagação de *worms* e de utilização indevida de endereçamento IP reservado .

O fornecimento de informações estatísticas sobre o número de propagações detectadas, em tempo próximo do real e preservando seu histórico, garante uma visão mais realística dos eventos de propagação de *worms* que diariamente trafegam no *backbone*, constituindo um importante elemento para a manutenção da segurança.

Desta forma, o trabalho realizado cumpriu os requisitos necessários, contribuindo para o aperfeiçoamento da gerência da segurança de redes.

Como trabalhos futuros, são sugeridos os seguintes tópicos:

- Análise de novos parâmetros, a fim de gerar novas assinaturas e a renovação automática dessas assinaturas, para cobrir uma área maior das vulnerabilidades encontradas no ambiente de redes de computadores.
- Considerar a exploração visual da rede monitorada em "N" variáveis, visando buscar novos padrões gráficos para as anomalias encontradas.
- Considerar a exploração visual automática do comportamento de uma variável específica (IP de origem, IP de destino ou porta de destino) ou alguma outra variável de interesse.
- Considerar dispositivo para, a partir de determinados parâmetros definidos,

emitir sinal de alarme para o gerente informando o grau de periculosidade encontrado.

- Efetuar estudo da eficência do algoritmo de classificação, utilizando ambiente de avaliação controlado, com tráfego especificamente projetado com os diversos tipos de ataques.

- Efetuar estudo comparativo da eficiência do algoritmo de classificação com outros da literatura que venham a explorar a mesma metodologia, utilizando ambiente de avaliação controlado, com tráfego especificamente projetado com os diversos tipos de ataques.

- Efetuar a integração do sistema atual com sistemas de rastreamento de atacantes, denominados *IP Traceback Systems*. Desta forma, mesmo com o uso de endereços IP de origem forjados, seria possível localizar o real atacante.

Bibliografia

[1] STEVENS, W. R. *TCP/IP illustrated (vol. 1): the protocols.* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1993. ISBN 0-201-63346-9.

[2] MCCANNE, S.; JACOBSON, V. The BSD packet filter: A new architecture for user-level packet capture. In: *USENIX Winter.* [S.l.: s.n.], 1993. p. 259–270.

[3] SKOUDIS, E.; ZELTSER, L. *Malware: Fighting Malicious Code.* Upper Saddle River, NJ, USA: Prentice Hall PTR, 2003. ISBN 0131014056.

[4] ROMIG, S. The osu flow-tools package and cisco netflow logs. In: *LISA '00: Proceedings of the 14th USENIX conference on System administration.* Berkeley, CA, USA: USENIX Association, 2000. p. 291–304.

[5] KIM, I. K. H.; BAHK, S. Real-time visualization of network attacks on high-speed links. *IEEE Network*, v. 18, p. 30–19, 2004.

[6] JOHNSON, B.; SHNEIDERMAN, B. Tree-maps: a space-filling approach to the visualization of hierarchical information structures. In: *VIS '91: Proceedings of the 2nd conference on Visualization '91.* Los Alamitos, CA, USA: IEEE Computer Society Press, 1991. p. 284–291. ISBN 0-8186-2245-8 (PAPER).

[7] SAMPAIO, L. et al. Um ambiente de gerenciamento de medições por fluxo de tráfego baseado na utilização de mapas em Árvore. *II WPerformance*, Campinas, SP, Brasil, p. 115–128, 2003.

[8] YIN, X. et al. Visflowconnect: netflow visualizations of link relationships for security situational awareness. In: *VizSEC/DMSEC '04: Proceedings of the 2004*

ACM workshop on Visualization and data mining for computer security. Washington DC, USA: ACM Press, 2004. p. 26–34. ISBN 1-58113-974-8.

[9] CONTI, G.; ABDULLAH, K. Passive visual fingerprinting of network attack tools. In: *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security.* New York, NY, USA: ACM Press, 2004. p. 45–54. ISBN 1-58113-974-8.

[10] ERBACHER, R. F. Glyph-based generic network visualization. In: *Proceedings of the SPIE '2002 Conference on Visualization and Data Analysis.* [S.l.: s.n.], 2002. p. 228–237.

[11] CERT Statistics, último acesso em 15/08/06. Disponível em: <http://www.cert.org/stats/cert_stats.html>.

[12] FARRELL, N. *New DoS attack a real killer, último acesso em 15/08/06.* Disponível em: <http://www.theinquirer.net/default.aspx?article=30361>.

[13] CODE-RED: a case study on the spread and victims of an Internet worm, último acesso em 15/08/06. In: PROCEEDINGS of the Internet Measurement Workshop (IMW). [s.n.], 2002. Disponível em: <http://www.caida.org/outreach/papers/2002/codered/codered.pdf>.

[14] CERT/C, C. *CERT Advisory CA-2001-26 Nimda Worm, último acesso em 15/08/06.* CERT/CC, September 2001. Disponível em: <http://www.cert.org/advisories/CA-2001-26.html>.

[15] MOORE, D. et al. Inside the slammer worm. *IEEE Security and Privacy*, IEEE Computer Society, Los Alamitos, CA, USA, v. 01, n. 4, p. 33–39, 2003. ISSN 1540-7993.

[16] SHANNON, C.; MOORE, D. The spread of the witty worm. *IEEE Security and Privacy*, IEEE Educational Activities Department, Piscataway, NJ, USA, v. 2, n. 4, p. 46–50, 2004. ISSN 1540-7993.

[17] PLONKA, D. Flowscan: A network traffic flow reporting and visualization tool. In: *LISA '00: Proceedings of the 14th USENIX conference on System administration.* Berkeley, CA, USA: USENIX Association, 2000. p. 305–318.

[18] OVERVIEW of the NetFlow FlowAnalyzer, último acesso em 15/08/06. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfa/>.

[19] ESTAN, C.; SAVAGE, S.; VARGHESE, G. *Automatically inferring patterns of resource consumption in network traffic.*

[20] TUFTE, E. R. *Visual Explanations: Images and Quantities, Evidence and Narrative.* [S.l.]: Graphics Press, 1997. ISBN 0961392126.

[21] MARCHETTE, D. J. *Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint.* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2001. ISBN 0387952810.

[22] GIL, T. M.; POLETTO, M. Multops: a data-structure for bandwidth attack detection. In: *In the Proceedings of the 10th USENIX Security Symposium.* Berkeley, CA, USA: USENIX Association, 2001. p. 23–38.

[23] ROESCH, M. Snort - lightweight intrusion detection for networks, último acesso em 15/08/06. In: *LISA'99: 13th Systems Administration Conference.* [S.l.: s.n.], 1999. p. 229–238.

[24] REDE Rio, último acesso em 15/08/06. Disponível em: <http://www.rederio.br/>.

[25] TANENBAUM, A. S. Computer networks, fourth edition. Prentice Hall PTR, August 2002.

[26] IETF - The Internet Engineering Task Force, último acesso em 15/08/06. Disponível em: <http://www.ietf.org>.

[27] RFC791. Internet protocol, último acesso em 15/08/06. September 1981. DARPA Internet Program Protocol Specification. Disponível em: <http://www.ietf.org/rfc/rfc791.txt>.

[28] RFC793. Transmission control protocol, último acesso em 15/08/06. September 1981. DARPA Internet Program Protocol Specification. Disponível em: <http://www.ietf.org/rfc/rfc793.txt>.

[29] IANA - Internet Assigned Numbers Authority, último acesso em 15/08/06. Disponível em: <http://www.iana.org/assignments/port-numbers.>.

[30] BEJTLICH, R. *The Tao of Network Security Monitoring Beyond Intrusion Detection.* [S.l.]: Addison Wesley, 2004.

[31] LIBPCAP - Lawrence Berkeley National Labs - Network Research Group, último acesso em 15/08/06. Disponível em: <http://www.tcpdump.org/>.

[32] THE Tcpdump Group, último acesso em 15/08/06. Disponível em: <http://www.tcpdump.org/>.

[33] ETHEREAL, último acesso em 15/08/06. Disponível em: <http://www.ethereal.com/>.

[34] ROESCH, M. Snort - lightweight intrusion detection for networks. In: *LISA '99: Proceedings of the 13th USENIX conference on System administration.* Berkeley, CA, USA: USENIX Association, 1999. p. 229–238.

[35] RFC2722. Traffic flow measurement: Architecture, último acesso em 15/08/06. October 1999. Network Working Group. Disponível em: <http://www.ietf.org/rfc/rfc2722.txt>.

[36] NPROBE: Network protocol analysis, último acesso em 15/08/06. Disponível em: <http://www.cl.cam.ac.uk/Research/SRG/netos/nprobe/>.

[37] FPROBE, último acesso em 15/08/06. Disponível em: <http://sourceforge.net/projects/fprobe>.

[38] ARGUS, último acesso em 15/08/06. Disponível em: <http://www.qosient.com/argus/>.

[39] CFLOWD design, último acesso em 15/08/06. Disponível em: <http://www.caida.org/tools/measurement/ cflowd/design/design.html>.

[40] DERI, L.; SUIN, S. *Effective Traffic Measurement using ntop, IEEE Communications Magazine, 38(5), pp 138-145, May 2000.*

[41] RFC 3955, último acesso em 15/08/06. Disponível em: <http://www.ietf.org/rfc/rfc3955.txt>.

[42] NETFLOW Services Solutions Guide, último acesso em 21/06/05. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm>.

[43] LI HUI ZHANG, Y. Y. T. H. Z. Linuxflow: A high speed backbone measurement facility. In: *Passive and Active Measurement Workshop (PAM 2003).* [S.l.: s.n.], 2003.

[44] TEAM, T. S. *SAMBA - Opening Windows to a Wider World, último acesso em 15/08/06.* Disponível em: <http://us4.samba.org/samba/>.

[45] AKRITIDIS P. ANAGNOSTAKIS, K. M. E. Efficient content-based detection of zero-day worms. *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, Vol. 2, p. 837 – 843, May 2005.

[46] GONG, Y. Identifying p2p users using traffic analysis, último acesso em 15/08/06. Http://www.securityfocus.com/infocus/1843. July 2005.

[47] BROWN, J.; MCGREGOR, A. *Network Performance Visualization: Insight Through Animation.* 2000.

[48] MA, K.-L.; CAMP, D. M. High performance visualization of time-varying volume data over a wide-area network. *sc*, IEEE Computer Society, Los Alamitos, CA, USA, v. 00, p. 29, 2000. ISSN 1063-9535.

[49] ESTRIN, D. et al. Network visualization with nam, the vint network animator. *Computer*, IEEE Computer Society Press, Los Alamitos, CA, USA, v. 33, n. 11, p. 63–68, 2000. ISSN 0018-9162.

[50] ROMIG, S.; FULLMER, M.; LUMAN, R. The osu flow-tools package and cisco netflow logs. In: *LISA*. [S.l.: s.n.], 2000. p. 291–303.

[51] OETIKER, T. Mrtg: The multi router traffic grapher. In: *LISA '98: Proceedings of the 12th Conference on Systems Administration*. Berkeley, CA, USA: USENIX Association, 1998. p. 141–148. ISBN 1-880446-40-5.

[52] ALFRED Inselberg - Home of Parallel Coordinates, último acesso em 15/08/06. Disponível em: <http://www.math.tau.ac.il/ aiisreal/>.

[53] AKERMAN, R. *Trojan Port Lists, último acesso em 15/08/06*. Disponível em: <http://www.chebucto.ns.ca/ rakerman/trojan-port-table.html>.

[54] CONSULTING, S. *Trojan Port Lists, último acesso em 15/08/06*. Disponível em: <http://www.simovits.com/trojans/trojans.html>.

[55] DOSHELP.COM. *Trojan Port Lists, último acesso em 15/08/06*. Disponível em: <http://www.doshelp.com/Ports/Trojan_Ports.htm>.

[56] ONCTEK. *Trojan Port Lists, último acesso em 15/08/06*. Disponível em: <http://www.onctek.com/trojanports.html>.

[57] VILELA, G. S. *Caracterização de Tráfego Utilizando Fluxos de Comunicação*. Dissertação (Mestrado) — Universidade Federal do Rio de Janeiro/COPPE, March 2006.

[58] EMBRATEL, último acesso em 15/08/06. Disponível em: <http://www.embratel.com.br/>.

[59] RNP, último acesso em 15/08/06. Disponível em: <http://www.rnp.br/>.

[60] RAVEL, último acesso em 15/08/06. Disponível em: <http://www.ravel.ufrj.br>.

[61] UFRJ, último acesso em 15/08/06. Disponível em: <http://www.ufrj.br>.

Apêndice A

Recomendações Para Melhoria da Segurança das Redes

A.1 Prevenção de Ações de Códigos Maliciosos (Malwares) em Rede - Worms

1. Manter o sistema operacional e os demais aplicativos atualizados, com as devidas correções (*patches*) aplicadas;
2. Instalar e manter atualizado um aplicativo de antivírus;
3. Instalar *firewall* pessoal, a fim de evitar que uma possível vulnerabilidade venha a ser explorada ou evitar a propagação de Worm já instalado na máquina;
4. Analisar tráfego buscando por comunicações em portas de destino constantes na lista de portas suspeitas relacionada no Apêndice B.

A.2 Proteção do Tráfego de Entrada de Uma Instituição Interligada a Um Backbone IP

O equipamento responsável pela interligação da rede institucional com o *Backbone* IP deverá fornecer a proteção desta contra ataques do tipo "Spoofing"[1] e de negação de serviço. Esta proteção é proporcionada em forma de listas de acesso (*access-list*) que são criadas para permitir ou negar o fluxo de informações através de uma ou mais interfaces do equipamento. A Tabela A.1 exemplifica a aplicação de lista de acesso em um roteador de borda para proteção do tráfego de entrada:

Regra	Lista	Ação	Protocolo	Endereço Origem	Máscara Endereço Origem	Endereço Destino	Máscara Endereço Destino	Opção
1	111	deny	IP	10.0.0.0	0.255.255.255	any		log
2	111	deny	IP	172.16.0.0	0.255.255.255	any		log
3	111	deny	IP	192.168.0.0	0.255.255.255	any		log
4	111	deny	IP	127.0.0.0	0.255.255.255	any		log
5	111	deny	IP	224.0.0.0	31.255.255.255	any		log
6	111	deny	IP	interface interlig.c/ *Backbone*	0.0.0.0	interface interlig.c/ *Backbone*	0.0.0.0	log
7	111	deny	IP	0.0.0.0	0.255.255.255	any		log
8	111	permit	ICMP echo replay	0.0.0.0	0.255.255.255	any		log
9	111	deny	ICMP	any		any		log
10	111	permit	IP	any		any		

Tabela A.1: Exemplo de lista de acesso a ser aplicada em um roteador de borda para proteção do tráfego de entrada de uma instituição interligada a um Backbone IP.

Analisando-se cada regra implementada, temos:

Regra #1 - Bloqueio de pacotes originários de endereçamento privado.

Regra #2 - Bloqueio de pacotes originários de endereçamento privado.

[1]IP spoofing é uma técnica de subversão de sistemas informáticos que consiste em mascarar (*spoof*) pacotes IP com endereços remetentes falsificados

Regra #3 - Bloqueio de pacotes originários de endereçamento privado.

Regra #4 - Bloqueio de pacotes que tenham como origem o endereço de *loop-back.*

Regra #5 - Bloqueio de pacotes que tenham como origem endereço de *multicast.*

Regra #6 - Bloqueio de pacotes que tenham como endereço de origem e destino origem o endereço da interface do roteador que o conecta com o *Backbone* IP.

Regra #7 - Bloqueio de pacotes que não tenham endereçamento IP.

Regra #8 - Permissão da passagem de tráfego ICMP (retorno de "ping" quando o mesmo é solicitado a partir da rede interna).

Regra #9 - Bloqueio de qualquer pacote do tipo ICMP com destino a qualquer equipamento no perímetro ou rede interna.

Regra #10 - Permite a passagem de qualquer tipo de tráfego.

A regra #6 restringe o envio de pacotes ao roteador que tenham como origem e destino o próprio endereço do roteador. O ataque *LAND* consiste em gerar um pacote tendo como origem e destino o endereço da interface do roteador que o conecta com o *Backbone* IP. Isto faz com que o equipamento entre em "*looping*" eterno, causando seu reinício automático.

Deve-se atentar também para a última regra (#10), que deve sempre liberar o protocolo IP. A última regra será sempre, de forma implícita, DENY ALL. A inexistência da regra #10 fará com que o roteador descarte todos os pacotes recebidos.

A lista de acesso criada (111) deverá ser aplicada como INBOUND na interface que conecta o roteador de borda ao *Backbone* IP. Ela é responsável pela filtragem de todo o tráfego de entrada a partir da Internet.

A.3 Proteção do Tráfego de Saída de Uma Instituição Interligada a Um Backbone IP

Para aumentar o nível de segurança do perímetro, é recomendada a criação de outra lista de acesso, responsável pela filtragem do tráfego de saída. O objetivo desta lista de acesso é permitir somente a saída de pacotes que pertençam ao intervalo de endereçamento IP válido utilizado pela instituição. Em outras palavras, deve ser analisado quais os elementos do perímetro interno de uma instituição que necessitam abrir conexão com o mundo externo. Deve-se focar nos endereços reservados que deverão ser traduzidos para endereços públicos.

Normalmente, identifica-se a subrede com endereçamento válido atribuída a uma instituição para que o filtro de pacotes realizado pelo roteador permita somente a saída de máquinas que estejam dentro desta subrede. Entretanto, um nível maior de segurança pode ser obtido especificando-se individualmente a permissão de saída a cada endereço IP. Este método é mais trabalhoso, porém traz maior segurança e confiabilidade, assegurando que somente os endereçamentos previamente autorizados trafegem para a Internet. Isso evita, por exemplo, a prática de burlar servidores de "*proxy*" ou *firewalls* adicionando-se o IP válido a máquinas da rede interna da instituição. A Tabela A.2 exemplifica a aplicação de uma lista de acesso em um roteador de borda para proteção do tráfego de saída:

Regra	Lista	Ação	Protocolo	Endereço Origem	Máscara Endereço Origem	Endereço Destino	Máscara Endereço Destino	Opção
1	112	permit	IP	X.X.X.X	0.255.255.255	any		
2	112	permit	ICMP	any	5	any		log
3	112	deny	IP	any		any		log

Tabela A.2: Exemplo de lista de acesso a ser aplicada em um roteador de borda para proteção do tráfego de saída de uma instituição interligada a um Backbone IP.

Analisando-se cada regra implementada, temos:

Regra #1 - Permissão de saída de endereços pertencentes a classe de endereça-

mento válido da instituição (X.X.X.X).

Regra #2 - Permissão de saída de pacotes do tipo ICMP.

Regra #3 - Bloqueio de todos os pacotes que não satisfazem as condições estabelecidas pelas regras #1 e #2, executando o registro de ocorrências.

A lista de acesso criada (112) deverá ser aplicada como INBOUND na interface que conecta o roteador de borda à rede interna. Ela é responsável por filtrar todo o tráfego de saída a partir da rede interna com destino a Internet.

É importante verificar que, ao contrário da lista de acesso 111 da Tabela A.1, que baseia-se em critérios de negações específicas liberando no último critério todo tipo de tráfego IP desde que o pacote não tenha satisfeito as condições estabelecidas, a lista de acesso 112 baseia-se primeiramente em critérios de permissões específicas negando e registrando os pacotes que, por sua vez, não tenham satisfeito as condições de permissão estabelecidas.

Apêndice B

Lista de Portas Suspeitas

Porta	Interpretação Possível do Ataque
1	Possível ataque (UDP) - Sockets des Troie, Bonk Attack, Breach, Ping of Death, Sockets de Troie, SocketsDeTroie, Socks Des Troie
2	Possível ataque Death, Death Trojan, Land Attack
3	Possível ataque SynDrop
5	Possível ataque yoyo, Incoming Routing Redirect Bomb
7	Possível ataque fraggle attack attempt
8	Possível ataque Ping Attack
9	Possível ataque Chargen Attack
11	Possível ataque Skun
15	Possível ataque B2
16	Possível ataque Skun
17	Possível ataque Skun
18	Possível ataque Skun
19	Possível ataque Skun, Chargen
23	Possível ataque ADM worm, Aphex's Remote Packet Sniffer , AutoSpY, ButtMan, Fire HacKer, My Very Own trojan, Pest, RTB, 666, Tiny Telnet Server - TTS, Truva Atl, Fire HacKer, My Very Own trojan, RTB 666, Telnet Pro, Tiny Telnet Server - TTS
24	Possível ataque Back Orifice 2000 (BO2K) Control Port, BO2K
27	Possível ataque Assasin

28	Possível ataque Amanda
30	Possível ataque Agent 40421, Agent 40422
31	Possível ataque Agent 40421, Masters Paradise, Skun, Agent 31, Hackers Paradise, Masters Paradise, Hacker's Paradise, Skun
37	Possível ataque ADM worm, W32.Sober
39	Possível ataque SubSARI
41	Possível ataque Deep Throat , Foreplay , Reduced Foreplay
44	Possível ataque Arctic
48	Possível ataque DRAT
50	Possível ataque DRAT
51	Possível ataque Fuck Lamers Backdoor
52	Possível ataque MuSka52, Skun
53	Possível ataque ADM worm, li0n, MscanWorm, MuSka52, Lion, DNS Spoof, li0n, MscanWorm, MuSka52, Trojan.Esteems.c
54	Possível ataque MuSka52
58	Possível ataque DMSetup
59	Possível ataque DMSetup
66	Possível ataque AL-Bareki
68	Possível ataque Sub-7, SubSeven
69	Possível ataque BackGate, BackGate Kit, Nimda, Pasana, Storm, Storm worm, Theef, Pasana, Listening port for MS Blaster, Nimda, Storm, Storm worm, Theef, w32.cycle W32.Mockbot.A.Worm
70	Possível ataque ADM worm, W32.Evala.Worm
79	Possível ataque ADM worm, Back Orifice 2000 (BO2K) Data Port, CDK, Firehotcker or improper Finger port use attack.
81	Possível ataque Asylum, RemoConChubo, Beagle.S, RemoConChubo Trojan
85	Possível ataque Common Port for phishing scam sites
87	Possível ataque Common Port for phishing scam sites
88	Possível ataque pwsteal.likmet.a
90	Possível ataque Hidden Port 2.o
99	Possível ataque Hidden, Hidden Port, Mandragore, NCX, Common Port for phishing scam sites, Hidden Port v2.0
101	Possível ataque Skun
102	Possível ataque Delf, Skun

103	Possível ataque Skun
104	Possível ataque Comm. 300, Comm.300
105	Possível ataque NerTe
107	Possível ataque Skun
109	Possível ataque ADM worm
110	Possível ataque ADM worm, ProMail trojan
111	Possível ataque ADM worm, MscanWorm, Looking for Sun RPC PortMapper/RPCBIND.
113	Possível ataque ADM worm, Alicia, Cyn, DataSpy Network X, Dosh, Gibbon, Taskman , Invisible Identd Daemon, Kazimas, Invisible Identd Deamon
119	Possível ataque Happy99, Happy99 Trojan
120	Possível ataque Skun
121	Possível ataque Attack Bot, God Message, JammerKillah, AttackBot, BO JammerkillahV
123	Possível ataque Net Controller Trojan
129	Possível ataque Generator Protocol attack, Password Generator Protocol
133	Possível ataque Farnaz, 146, Faranz, Farnaz Trojan, Infector
135	Possível ataque DCOM/MSBlast exploitation attack, Netbios Remote Procedure Call, Netbios RPC, W32.Blaster, W32/Lovsan.worm
137	Possível ataque Chode, Nimda, Msinit, Qaz, Bugbear, Netbios name (DoS), Netbios name (DoS)., Nimda, Opaserv, OpaSoft
138	Possível ataque Chode, Netbios datagram, Nimda
139	Possível ataque Chode, Fire HacKer, Msinit, Nimda, Opaserv, Qaz, God Message worm, Msinit, Netlog, Network, Qaz, Sadmind, SMB Relay, Fire HacKer, God Message, Netbios session, Opaserv
142	Possível ataque NetTaxi, NetTaxi Trojan
143	Possível ataque ADM worm
146	Possível ataque Infector, Infector 1.3, Infector v1.3
166	Possível ataque NokNok
170	Possível ataque A-trojan
171	Possível ataque A-trojan
173	Possível ataque Nestea
200	Possível ataque CyberSpy

201	Possível ataque One Windows Trojan
202	Possível ataque One Windows Trojan, Skun
211	Possível ataque One Windows Trojan
212	Possível ataque One Windows Trojan
221	Possível ataque Snape
222	Possível ataque NeuroticKat, Snape
230	Possível ataque Skun
231	Possível ataque Skun
232	Possível ataque Skun
285	Possível ataque Delf, WCTrojan
286	Possível ataque WCTrojan
299	Possível ataque One Windows Trojan
334	Possível ataque Backage, Backage Trojan
335	Possível ataque Nautical
370	Possível ataque NeuroticKat
382	Possível ataque W32.Rotor
400	Possível ataque Argentino
401	Possível ataque One Windows Trojan
402	Possível ataque One Windows Trojan
411	Possível ataque Backage
420	Possível ataque Breach, Breach Trojan, Incognito, W32.kibuv.b
421	Possível ataque TCP Wrappers trojan
445	Possível ataque Backdoor.rtkit.b, Lioten, Randon, Sasser, Nimda, Trojan.Netdepix.b, W32.HLLW.Deloder, W32.ifbo.a, W32.korgo.a, W32.mytob.e, W32.mytob@mm, W32.Scane, W32.spybot.khc, W32.spybot.nps, W32.spybot.ofn, W32/Deloder.A, WORM_DELODER.A, W32.hllw.lioten
455	Possível ataque Fatal Connections
456	Possível ataque Hackers Paradise
510	Possível ataque t0rnkit sshd backdoor
511	Possível ataque T0rn Rootkit
513	Possível ataque ADM worm, Grlogin, Grlgon Trojan
514	Possível ataque ADM worm, RPC Backdoor, RPC Backdoor Trojan
515	Possível ataque MscanWorm, lpdw0rm, Ramen
520	Possível ataque (UDP) - A UDP backdoor

530	Possível ataque W32.kibuv.worm
531	Possível ataque Net666, Net 666, Rasmin
555	Possível ataque 711 trojan (Seven Eleven), PhaseZero, Phase-0, Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy, PhaseZero, Phaze
559	Possível ataque Backdoor.domwis, Backdoor.solufina
564	Possível ataque Oracle
589	Possível ataque Assasin
600	Possível ataque SweetHeart, Sadmind
605	Possível ataque Secret Service, Secret Service Trojan
606	Possível ataque Secret Service Trojan
623	Possível ataque RTB 666
635	Possível ataque ADM worm, Looking for Linux System
650	Possível ataque Assasin
660	Possível ataque Zaratustra
661	Possível ataque NokNok
665	Possível ataque Attack FTP, lpdw0rm, Shadow Phyre, ServU, Satans Back Door - SBD, NokNok, Cain & Abel, Back Construction, BLA trojan, th3r1pp3rz (= Therippers), BackConstruction, Attack FTP, Back Construction, BLA trojan, NokNok, Reverse Trojan, Shadow Phyre, Unicorn, Back Construction, BLA trojan, Cain & Abel, lpdw0rm, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers), BackConstruction, Bla, Ipdw0rm, N0kN0k Trojan, Reverse Trojan, Satans Back Door (SBD), Satanz Backdoor, ServeU, Unicorn, yoyo
667	Possível ataque NokNok, SniperNet, SniperNet Trojan
668	Possível ataque Unicorn, th3r1pp3rz (= Therippers)
669	Possível ataque DP trojan , SniperNet
680	Possível ataque RTB 666, RTB666
692	Possível ataque GayOL, GayOL Trojan
700	Possível ataque REx
777	Possível ataque Undetected, AimSpy, (the) Undetected Trojan, BackDoor.Netcrack.B, Tiny
778	Possível ataque BackDoor.Netcrack.B
785	Possível ataque NetworkTerrorist

798	Possível ataque Oracle
800	Possível ataque NeuroticKitten
808	Possível ataque WinHole, WinHole Trojan
831	Possível ataque NeuroticKat, NeuriticKat
880	Possível ataque Common Port for phishing scam sites
901	Possível ataque Net-Devil, Pest, Backdoor.Devil, NetDevil, Pest
902	Possível ataque Net-Devil, Pest, Backdoor.Devil
903	Possível ataque Net-Devil
911	Possível ataque Dark Shadow, Dark Shadow
956	Possível ataque Crat Pro
991	Possível ataque Snape
992	Possível ataque Snape
999	Possível ataque Deep Throat , Foreplay , Chat power, Foreplay, WinSatan, Reduced Foreplay
1000	Possível ataque Der Späher / Der Spaeher, Direct Connection, GOTHIC Intruder , Theef, Connecter, Direct Connection, Insane Network, Der Spacher 3, Der Spaeher, Der Spaher, DerSpaeher, GOTHIC Intruder
1001	Possível ataque Der Späher / Der Spaeher, GOTHIC Intruder , Lula, One Windows Trojan, Theef, Le Guardien, Silencer, Theef, WebEx, Backdoor.Wortbot, Der Spacher 3, Der Spaeher, Der Spaher, DerSpaeher, GOTHIC Intruder, Lula, One Windows Trojan
1005	Possível ataque Pest, Theef
1008	Possível ataque AutoSpY, li0n, Lion
1010	Possível ataque Doly Trojan, Der Spaeher, Der Spaher, DerSpaeher
1011	Possível ataque Doly Trojan
1012	Possível ataque Doly Trojan
1015	Possível ataque Doly Trojan
1016	Possível ataque Doly Trojan
1020	Possível ataque Vampire, Vampyre
1023	Possível ataque Sasser.e FTP
1024	Possível ataque attack on Voice Streaming Audio, Jade, Latinus, Lithium, NetSpy, Ptakks, RAT[no.2], Backdoor.lingosky
1025	Possível ataque AcidkoR, BDDT, DataSpy Network X, Fraggle Rock , KiLo, MuSka52, NetSpy, Optix, Optix Pro , Paltalk, Ptakks,

	2000, Remote Anything, Remote Explorer Y2K, Remote Storm, RemoteNC, 5 Backdoor, DataSpy, Mavericks Matrix 1.2 - 2.0, Yajing
1026	Possível ataque BDDT, Dark IRC, DataSpy Network Delta Remote Access , Dosh, Duddie, IRC Contact, Remote Explorer 2000, RUX The TIc.K
1027	Possível ataque Clandestine, DataSpy Network X, ICKiller, ICQ Trojan, KiLo, UandMe
1028	Possível ataque DataSpy Network X, Dosh, Gibbon, KiLo, KWM, Litmus, Paltalk, SubSARI
1029	Possível ataque Clandestine, ICQ Nuke 98, ICQ Trojan, InCommand Access, KWM, Litmus, SubSARI
1030	Possível ataque Gibbon, KWM
1031	Possível ataque KWM, Little Witch, Xanadu, Xot
1032	Possível ataque Akosch4, Dosh, ICQ Trojan, KWM
1033	Possível ataque Dosh, ICQ Trojan, KWM, Little Witch, Net Advance, NetSpy
1034	Possível ataque KWM, Backdoor.Zincite.a
1035	Possível ataque Dosh, KWM, Multidropper, RemoteNC, Truva Atl
1036	Possível ataque KWM
1037	Possível ataque Arctic , Dosh, KWM, MoSucker
1039	Possível ataque Dosh
1041	Possível ataque Dosh, RemoteNC
1042	Possível ataque Bla, BLA, Rasmin
1043	Possível ataque Dosh
1044	Possível ataque Ptakks
1045	Possível ataque Rasmin
1047	Possível ataque RemoteNC
1049	Possível ataque Linux: /sbin/initd, Seeking Linux system with /sbin/initd Trojan, Delf, The Hobbit Daemon
1050	Possível ataque MiniCommand
1052	Possível ataque Fire HacKer, Slapper, The Hobbit Daemon
1053	Possível ataque The Thief
1054	Possível ataque AckCmd, RemoteNC
1080	Possível ataque MyDoom.F, Seeking Win32:BugBear-B, SubSeven 2.2, WinHole
1081	Possível ataque WinHole Trojan
1090	Possível ataque Xtreme

1092	Possível ataque Hvl RAT
1095	Possível ataque Blood Fest Evolution, Hvl RAT, Remote Administration Tool
1099	Possível ataque Bfevolution, Blood Fest Evolution, Hvl RAT, Remote Administration Tool (RAT)
1104	Possível ataque (UDP) - RexxRave
1111	Possível ataque Backdoor.Aimvision, Daodan, Tport, Ultors Trojan
1115	Possível ataque Lurker, Protoss
1116	Possível ataque Lurker
1122	Possível ataque Last 2000, Singularity
1130	Possível ataque Noknok
1133	Possível ataque SweetHeart
1150	Possível ataque Orion
1151	Possível ataque Orion
1160	Possível ataque BlackRat
1166	Possível ataque CrazzyNet
1167	Possível ataque CrazzyNet
1170	Possível ataque Psyber Stream Server - PSS, Streaming Audio Server, Voice
1174	Possível ataque DaCryptic
1180	Possível ataque Unin68
1183	Possível ataque Cyn, SweetHeart
1200	Possível ataque (UDP) - NoBackO
1201	possível ataque (UDP) - NoBackO
1207	Possível ataque SoftWAR
1208	Possível ataque Infector
1212	Possível ataque Kaos Trojan
1215	Possível ataque Force
1218	Possível ataque Backdoor.Sazo, Force
1219	Possível ataque Force
1221	Possível ataque Fuck Lamers Backdoor
1222	Possível ataque D Network, Fuck Lamers Backdoor
1225	Possível ataque Scarab
1234	Possível ataque Java client, KiLo, SubSeven Sub-7, W32.Beagle.Y Ultor's Trojan
1243	possível ataque BackDoor-G, Sub7, SubSeven, SubSeven Apocalypse, Tiles
1245	Possível ataque GabanBus, NetBus, Vodoo, VoodooDoll
1255	Possível ataque Scarab

1256	Possível ataque Project nEXT, RexxRave
1257	Possível ataque Sub Seven v2.1
1269	Possível ataque Mavericks Matrix, Maverick's Matrix
1272	Possível ataque The Matrix
1313	Possível ataque NETrojan
1314	Possível ataque Daodan
1337	Possível ataque Shadyshell
1338	Possível ataque Millenium Worm, Millennium Worm
1349	Possível ataque BO dll, BackOrifice, BackOrifice DLL, BackOrifice DLL Comm
1369	Possível ataque SubSeven 2.2
1386	Possível ataque Dagger
1394	Possível ataque BackDoor, Backdoor G-1, GroFriller
1415	Possível ataque Last 2000, Singularity
1433	Possível ataque SQL Snake, SQLsnake attempt to find unprotected MS SQL Server, w32.spybot.ofn, Voyager Alpha Force
1434	Possível ataque SQL Slammer
1441	Possível ataque Remote Storm
1480	Possível ataque RemoteHack
1492	Possível ataque FTP99CMP Trojan
1505	Possível ataque FunkProxy
1509	Possível ataque Psyber Streaming, Psyber Streaming server
1524	Possível ataque Attempting attack at Sun system (Trinoo trojan)
1525	Possível ataque Archie, Prospero
1533	Possível ataque Backdoor.Miffice
1534	Possível ataque Bizex.Worm
1560	Possível ataque Big Gluck, Duddie
1561	Possível ataque (UDP) - MuSka52
1568	Possível ataque Remote Hack, RemoteHack
1600	Possível ataque DirectConnection, Shivka Burka, Shivka-Burka
1601	Possível ataque DirectConnection, Direct Connection
1604	Possível ataque ICA Browser
1634	Possível ataque Net Crack, NetCrack
1703	Possível ataque Exploiter
1711	Possível ataque yoyo
1772	Possível ataque Backdoor.NetControle

1777	Possível ataque Scarab
1784	Possível ataque Snid
1807	Possível ataque SpySender, Spy Sender
1826	Possível ataque Glacier
1833	Possível ataque TCC
1834	Possível ataque TCC
1835	Possível ataque TCC
1836	Possível ataque TCC
1837	Possível ataque TCC
1863	Possível ataque Backdoor.Kaitex.e
1905	Possível ataque Delta Remote Access
1911	Possível ataque Arctic
1966	Possível ataque Fake FTP
1967	Possível ataque For Your Eyes Only - FYEO, WM FTP Server
1969	Possível ataque OpC BackOrifice, OpC BO
1978	Possível ataque (UDP) - Slapper
1981	Possível ataque Bowl trojan, Shockrave trojan
1983	Possível ataque Q-taz
1984	Possível ataque Intruzzo , Q-taz
1985	Possível ataque Black Diver, Q-taz
1986	Possível ataque Akosch4
1991	Possível ataque PitFall, Pit Fall
1999	Possível ataque BackDoor Trojan, BackDoor.BiFrose, Trans Scout, Transmission Scout, TransmissionScout, TransScout trojan
2000	Possível ataque A-trojan, Atrojan, Der Späher Der Spaeher, Fear, Force, GOTHIC Intruder , Insane Network, Last 2000, Real 2000, Remote Explorer 2000, Remote Explorer Y2K, Senna Spy Trojan Generator, Singularity
2001	Possível ataque Scalper, Der Spaeher, Der Spaeher3, Der Spaher, DIRT, Duddie, Glacier, Insane Network, Protoss, Senna Spy Trojan Generator, Singularity, Trans Scout, TransScout, TrojanCow
2002	Possível ataque Duddie, Peer-toPeer UDP DDos (PUD), Senna Spy Trojan Generator,Sensive, Slapper, TransScout, Transmission Scount
2003	Possível ataque Trans Scout, TransScout, TransmissionScout
2004	Possível ataque Duddie, Trans Scout, TransmissionScout

2005	Possível ataque Duddie, (the) Unspecified Trojan, Transmission Scout, TransmissionScout, TransScout trojan
2020	Possível ataque Backdoor Rockse, Backdoor.Rockse
2023	Possível ataque Dialup Ripper, Pass Ripper, PassRipper, Ripper, RipperPro
2040	Possível ataque InfernoUploader
2041	Possível ataque W32.korgo.a
2060	Possível ataque Protoss
2080	Possível ataque Backdoor.TJServ, WinHole Trojan
2086	Possível ataque Corba exploit, Netscape exploit
2090	Possível ataque Backdoor.Expjan
2101	Possível ataque SweetHeart
2115	Possível ataque Bugs
2130	Possível ataque (UDP) - Mini BackLash
2140	Possível ataque Deep Throat, Deepthroat, The Invasor, Foreplay, Foreplay or Reduced Foreplay
2149	Possível ataque Deep Throat
2150	Possível ataque R0xr4t
2155	Possível ataque Illusion Mailer
2156	Possível ataque Oracle
2222	Possível ataque BackDoor.Botex, SweetHeart, Rootshell, Way
2255	Possível ataque Nirvana Trojan
2281	Possível ataque Nautical
2283	Possível ataque (the) Unknown Trojan, Dumaru.Y, HvL RAT, HVL Rat 5
2300	Possível ataque Storm, Xplorer trojan
2311	Possível ataque Studio 54
2322	Possível ataque backdoor.shellbot
2330	Possível ataque IRC Contact
2331	Possível ataque IRC Contact
2332	Possível ataque IRC CONTACT, Silent Spy, SilentSpy
2333	Possível ataque IRC Contact, backdoor.shellbot
2334	Possível ataque IRC Contact, Eyeveg.worm.c, Power
2335	Possível ataque IRC Contact, backdoor.shellbot
2336	Possível ataque IRC Contact
2337	Possível ataque IRC Contact, The Hobbit Daemon
2338	Possível ataque IRC Contact

2339	Possível ataque IRC Contact, Voice Spy
2343	Possível ataque Asylum
2345	Possível ataque Doly Trojan
2400	Possível ataque Portd
2407	Possível ataque yoyo
2414	Possível ataque vbs.shania
2418	Possível ataque Intruzzo
2525	Possível ataque Backdoor Rockse, Backdoor.Rockse
2535	Possível ataque Bagle.aa, Bagle.z
2555	Possível ataque li0n, Lion, T0rn Rootkit
2556	Possível ataque Beagle.N
2565	Possível ataque Striker trojan
2583	Possível ataque (the) Unknown Trojan, WinCrash, WinCrash 2, WinCrash2
2589	Possível ataque Dagger
2600	Possível ataque Digital Root Beer, DigitalRootBeer
2702	Possível ataque Black Diver
2716	Possível ataque The Prayer 1.2 -1.3, The Prayer 2, The Prayer v1.2 or v1.3
2719	Possível ataque Change
2721	Possível ataque Phase Zero
2745	Possível ataque Bagel W32/Bagel.c@mm, Bagle, Beagle, Tanx
2766	Possível ataque W32.hllw.deadhat.b
2772	Possível ataque Sub7, SubSeven, Sub Seven Screen Capture Port
2773	Possível ataque Sub7, SubSeven 2.1, Sub Seven Key Logger Port
2774	Possível ataque Sub7, SubSeven 2.1, Sub Seven Key Logger Port
2776	Possível ataque Software
2777	Possível ataque Software
2800	Possível ataque Theef
2801	Possível ataque Phineas Phucker
2929	Possível ataque Konik
2983	Possível ataque Breach
2989	Possível ataque Backdoor.Brador.A, RAT, Remote Administration Tool - RAT
3000	Possível ataque InetSpy, Remote Shut, Remote Shutdown, Theef
3006	Possível ataque Clandestine
3024	Possível ataque WinCrash
3028	Possível ataque Backdoor.Wortbot

3030	Possível ataque W32.Mytob.cz@mm
3031	Possível ataque MicroSpy
3067	Possível ataque W32.korgo.a
3119	Possível ataque Delta Remote Access
3127	Possível ataque Moody.Worm, MyDoom, MyDoom.A, MyDoom.B@mm, W32.HLLW.Deadhat, W32.HLLW.DoomJuice, W32.MockBot.A, W32.SoLame.A, W32.Welchia.D Worm, W32.DoomHunter
3128	Possível ataque Reverse WWW Tunnel Backdoor , RingZero, Masters Paradise, MyDoom, MyDoom.B@mm, squid HTTP Proxy server scan
3129	Possível ataque Master's Paradise, MyDoom, MyDoom.B@mm
3130	Possível ataque MyDoom, MyDoom.B@mm
3131	Possível ataque MyDoom, SubSARI
3132	Possível ataque MyDoom, MyDoom.B@mm
3133 a 3149	Possível ataque MyDoom, MyDoom.B@mm
3150	Possível ataque Deep Throat, Deepthroat, Foreplay, Foreplay, Mini Backlash, The Invasor
3151 a 3198	Possível ataque MyDoom, MyDoom.B@mm
3215	Possível ataque BlackStar, Ghose, XHX
3217	Possível ataque Telecomm Env
3256	Possível ataque W32.HLLW.Dax
3291	Possível ataque Associates - LM
3292	Possível ataque Xposure
3295	Possível ataque Xposure
3306	Possível ataque Backdoor.Nemog.D
3332	Possível ataque Q0 W32.cycle
3333	Possível ataque Daodan
3410	Possível ataque OptixPro, W32.mockbot.a.worm
3417	Possível ataque Xposure
3418	Possível ataque Xposure
3456	Possível ataque Backdoor.Fearic, Fear, Force, Teror Trojan, TerrorTrojan
3459	Possível ataque Eclipse 2000, Sanctuary
3505	Possível ataque AutoSpY
3547	Possível ataque Backdoor.Amitis.B

3586	Possível ataque Snid
3587	Possível ataque ****Head trojan, S**tHead trojan, ShitHead trojan
3630	Possível ataque S Remote Database Port
3631	Possível ataque S Web Services Port
3700	Possível ataque POD, Portal of Doom (POD), PortalOfDoom
3721	Possível ataque Whirlpool
3723	Possível ataque Mantis
3737	Possível ataque Backdoor.helios
3742	Possível ataque Service Tracker
3777	Possível ataque PsychWard
3791	Possível ataque Total Solar Eclypse trojan
3800	Possível ataque Total Solar Eclypse trojan
3801	Possível ataque Total Solar Eclypse trojan
3945	Possível ataque Delta Remote Access
3996	Possível ataque Remote Anything, RemoteAnything
3997	Possível ataque Remote Anything, RemoteAnything
3999	Possível ataque Remote Anything, RemoteAnything
4000	Possível ataque Attack on Voice Streaming Audio, Connect-Back Backdoor, Psyber Streaming Server, Psyber StreamingServer, RemoteAnything, Skydance trojan, WityWorm (BlackICE/ISS)
4001	Possível ataque Backdoor.OptixPro.13.C
4092	Possível ataque WinCrash
4128	Possível ataque Backdoor.rcserv, RedShad
4156	Possível ataque (UDP) - Slapper
4201	Possível ataque War trojan, Wartrojan
4210	Possível ataque Netkey
4211	Possível ataque Netkey
4225	Possível ataque Silent Spy, SilentSpy
4242	Possível ataque Backdoor.Nemog.D, Virtual Hacking Machine (VHM) trojan
4300	Possível ataque Backdoor.smokodoor
4315	Possível ataque Power
4321	Possível ataque BoBo, SchoolBus
4387	Possível ataque Phatbot
4414	Possível ataque AL-Bareki
4442	Possível ataque Oracle

4444	Possível ataque Alex Trojan, AlexTrojan, CrackDown, Oracle, Prosiak, SwiftRemote, MS Blaster listening port, Swift Remote trojan, W32.Blaster Worm, W32.Hllw.Donk.M, W32.mockbot.a.worm, W32.reidana.a
4445	Possível ataque Oracle
4447	Possível ataque Oracle
4449	Possível ataque Oracle
4451	Possível ataque Oracle
4488	Possível ataque Event Horizon, EventHorizon
4512	Possível ataque W32.mytob.db
4523	Possível ataque Celine
4545	Possível ataque InternalRevise, Internal Revise, Remote Revise
4567	Possível ataque BackDoor-IW, FileNail
4590	Possível ataque ICQ Trojan, ICQTrojan
4646	Possível ataque Backdoor.Nemog.D
4653	Possível ataque Cero
4661	Possível ataque Backdoor.Nemog.D
4666	Possível ataque Mneah
4700	Possível ataque Theef
4751	Possível ataque Beagle.U
4820	Possível ataque Backdoor.tuxder
4836	Possível ataque Buttman, Power
4837	Possível ataque Buttman
4888	Possível ataque W32.Opanki
4899	Possível ataque W32.RaHack
4903	Possível ataque Common Port for phishing scam sites
4950	Possível ataque (the) Unknown Trojan, ICQ trojan, ICQTrojan, IcqTrojen
4983	Possível ataque T Intercom
5000	Possível ataque Back Door Setup, BioNet Lite, Blazer5, Bubbel, Kibuv, ICKiller, Ra1d, Sockets des Troie, W32.Bobax.A, W32.Bobax.D
5001	Possível ataque Back Door Setup, Bubble, Sockets des Troie
5002	Possível ataque cd00r, Linux Rootkit IV (4), Shaft
5005	Possível ataque Aladino
5010	Possível ataque Solo attack, Team Asylum (DOS attack)
5011	Possível ataque modified, One of the Last Trojans (OOTLT), Peanut Brittle
5025	Possível ataque WM Remote KeyLogger

5031	Possível ataque Net Metropolitan, Net Metropolitan 1.0, NetMetro
5032	Possível ataque Net Metropolitan, Net Metropolitan 1.0, NetMetro
5033	Possível ataque Net Metropolitan, Net Metropolitan 1.0, NetMetro
5050	Possível ataque R0xr4t, RoxRat
5135	Possível ataque Bmail
5150	Possível ataque Pizza
5151	Possível ataque Optix Lite, OptixLite
5152	Possível ataque Backdoor.laphex.client
5155	Possível ataque Oracle
5190	Possível ataque MBomber, W32.hllw.anig
5221	Possível ataque NOSecure
5250	Possível ataque Pizza
5277	Possível ataque WinShell
5313	Possível ataque Reliable Data
5321	Possível ataque Firehotcker
5333	Possível ataque Backage, NetDemon
5343	Possível ataque WC Remote Administration Tool, wCrat
5350	Possível ataque Pizza
5377	Possível ataque Iani
5400	Possível ataque Back Construction, Blade Runner, Digital Spy
5401	Possível ataque BackConstruction, Black Construction, BladeRunner, Deep Throat, DeepThroat, Digital Spy, Mneah
5402	Possível ataque BackConstruction, Black Construction, BladeRunner, Deep Throat, DeepThroat, Digital Spy, Mneah
5418	Possível ataque Backdoor.DarkSky.B, DarkSky, Dark Sky
5419	Possível ataque Backdoor.DarkSky.B, DarkSky, Dark Sky
5430	Possível ataque Net Advance
5450	Possível ataque Pizza
5501	Possível ataque (the) Unanalyzed trojan
5503	Possível ataque Remote Shell Trojan
5512	Possível ataque Illusion Mailer, Xtcp
5521	Possível ataque Illusion Mailer
5534	Possível ataque The Flu, TheFlu
5550	Possível ataque Pizza, Xtcp, X-TCP, Xtcp2
5553	Possível ataque Backdoor.Xlog

5554	Possível ataque W32.Sasser.Worm
5555	Possível ataque Daodan, Backdoor.OptixPro, Backdoor.Sysbug, Noxcape, ServeMe, W32.MiMail.P
5556	Possível ataque BackOrifice, BO Facil
5557	Possível ataque BackOrifice, BO Facil
5558	Possível ataque Backdoor.Easyserv
5569	Possível ataque RoboHack, Robo-Hack
5588	Possível ataque Backdoor.EasyServ
5631	Possível ataque de exploração do PCanywhere
5632	Possível ataque de exploração do PCanywhere
5636	Possível ataque PC Crasher
5637	Possível ataque PC Crasher
5638	Possível ataque PC Crasher
5650	Possível ataque Pizza
5666	Possível ataque PC Crasher
5669	Possível ataque SpArTa
5679	Possível ataque Nautical
5695	Possível ataque Assasin
5696	Possível ataque Assasin
5697	Possível ataque Assasin
5714	Possível ataque WinCrash
5741	Possível ataque WinCrash
5742	Possível ataque WinCrash
5760	Possível ataque Portmap Remote Root Linux Exploit
5800	Possível ataque Backdoor.Evivinc
5802	Possível ataque Y3K RAT, Y3KRat
5810	Possível ataque Y3K RAT, Y3KRat
5858	Possível ataque Y3K RAT, Y3KRat
5873	Possível ataque SubSeven 2.2
5880 a 5890	Possível ataque Y3K RAT, Y3KRat
5900	Possível ataque Backdoor.Evivinc
5933	Possível ataque NOSecure
6000	Possível ataque Aladino, LovGate.ak, NetBus , The Thing
6006	Possível ataque Bad Blood, BadBlood, The Thing trojan

6129	Possível ataque Dameware Worm, W32.mockbot.a.worm
6180	Possível ataque Common Port for phishing scam sites
6187	Possível ataque Trojan.Tilser
6267	Possível ataque DarkSky
6272	Possível ataque Secret Service Trojan
6400	Possível ataque The Thing trojan
6521	Possível ataque Oracle
6526	Possível ataque Glacier
6556	Possível ataque AutoSpY
6565	Possível ataque Backdoor.Nemog.D
6631	Possível ataque backdoor.sdbot.ag
6655	Possível ataque Aqua
6660	Possível ataque LameSpy
6661	Possível ataque TEMan, Weia-Meia
6666	Possível ataque AL-Bareki, Dark Connection, Dark Connection Inside, KiLo, LameRemote, NetBus, ProjectMayhem, SpArTa
6667	Possível ataque Acropolis, BlackRat, Dark FTP, Dark IRC, DataSpy Network X, EGO, Gunsan, InCommand, Kaitex, KiLo, Laocoon, Maniac rootkit, Moses, Net-Devil, Reverse Trojan, ScheduleAgent, SlackBot, SubSeven , Subseven 2.1.4 DefCon 8, The Thing Trinity, WinSatan, Y3K RAT, yoyo
6669	Possível ataque Host Control, ScheduleAgent, Trinity, Vampire, Vampyre, Voyager Alpha Force, WinSatan
6670	Possível ataque BackWeb Server, Deep Throat , DeepThroat, Foreplay, Reduced Foreplay, WinNuke eXtreame
6671	Possível ataque Deep Throat, Deepthroat, DeepThroat v3.1
6697	Possível ataque Force
6699	Possível ataque Host Control, HostControl
6711	Possível ataque BackDoor-G, Duddie, KiLo, Little Witch, Netkey, NokNok, Spadeace, SubSARI, Sub7, SubSeven , SweetHeart, UandMe
6712	Possível ataque Funny trojan, KiLo, Spadeace, Sub7, SubSeven
6713	Possível ataque KiLo, SubSeven
6714	Possível ataque KiLo
6715	Possível ataque KiLo
6718	Possível ataque KiLo

6723	Possível ataque Mstream (attacker to handler), Mstream attack-handler
6766	Possível ataque KiLo
6767	Possível ataque KiLo, NTRC, Pasana, UandMe
6771	Possível ataque Deep Throat , DeepThroat, Foreplay, Reduced Foreplay
6776	Possível ataque 2000 Cracks, BackDoor-G, SubSeven , VP Killer
6777	Possível ataque W32/Bagle@MM
6789	Possível ataque Doly Trojan, NetSky.U
6796	Possível ataque Sub-7, SubSeven
6838	Possível ataque Mstream (attacker to handler), Mstream Agent-handler
6883	Possível ataque Delta Source DarkStar, Delta Source DarkStar (??)
6891	Possível ataque Force
6912	Possível ataque Sh*t Heap, Shit Heep trojan, ShitHeep, Shit-Heep
6913	Possível ataque Danny, Shit Heep, ShitHeep, Shit-Heep
6939	Possível ataque Indoctrination
6953	Possível ataque Lithium
6969	Possível ataque 2000 Cracks, BlitzNet, Danton, Dark IRC, GateCrasher, IRC3, Kid Terror, Laphex, Net Controller, Priority, SpArTa, Vagr Nocker
6970	Possível ataque Danton, Gate Crasher
7000	Possível ataque Aladino, Exploit Translation Server, Gunsan, Kazimas, Remote Grab, SubSeven , SubSeven 2.1 Gold, Theef
7001	Possível ataque Freak88, Freak2k, NetSnooper Gold
7002	Possível ataque groups database
7007	Possível ataque Silent Spy
7020	Possível ataque Basic Hell
7028	Possível ataque (the) Unknown Trojan, Unknown Trojan
7030	Possível ataque Basic Hell
7119	Possível ataque Massaker
7158	Possível ataque Lohoboyshik
7200	Possível ataque Massaker
7215	Possível ataque SubSeven , SubSeven 2.1 Gold
7227	Possível ataque M Protocol
7274	Possível ataque AutoSpY
7290	Possível ataque NOSecure
7291	Possível ataque NOSecure
7300	Possível ataque Coced, NetMonitor, NetSpy

7301	Possível ataque Coced, NetMonitor, NetSpy
7302	Possível ataque Net Monitor, NetMonitor, Net Spy, NetSpy
a 7307	Possível ataque Net Monitor, NetMonitor, Net Spy, NetSpy
7308	Possível ataque NetMonitor, NetSpy, X Spy
7309	Possível ataque Net Monitor, NetMonitor
7312	Possível ataque Yajing
7323	Possível ataque Sygate Backdoor
7329	Possível ataque Backdoor.netshadow
7410	Possível ataque Backdoor.phoenix, Phoenix, Phoenix II
7424	Possível ataque HostControl, Host Control trojan
7511	Possível ataque Genue
7597	Possível ataque QaZ (Remote Access Trojan), QaZ Trojan
7609	Possível ataque Snid
7614	Possível ataque Backdoor.GRM, Wollf
7626	Possível ataque Binghe, Glacier, Hyne
7648	Possível ataque BlackStar, Ghost, XHX
7673	Possível ataque Neoturk
7676	Possível ataque Neoturk
7677	Possível ataque Neoturk
7718	Possível ataque Glacier
7722	Possível ataque KiLo
7777	Possível ataque God Message, The Thing, Tini trojan
7788	Possível ataque Last, Last2000, Last 2000, Matrix, Singularity
7789	Possível ataque Back Door SetupICKiller, Mozilla
7800	Possível ataque Paltalk
7823	Possível ataque Backdoor.Amitis.B
7826	Possível ataque MiniOblivion, Oblivion
7850	Possível ataque Paltalk
7878	Possível ataque Paltalk
7879	Possível ataque Paltalk
7887	Possível ataque SmallFun
7891	Possível ataque The ReVeNgEr
7955	Possível ataque W32.kibuv.b
7979	Possível ataque VagrNocker, Vagr Nocker
7983	Possível ataque Mstream (handler to agent), MStream handler-agent

7997	Possível ataque VagrNocker
8000	Possível ataque squid HTTP Proxy server scan, XConsole
8001	Possível ataque squid HTTP Proxy server scan
8011	Possível ataque Way
8012	Possível ataque Backdoor.Ptakks.b
8033	Possível ataque Brown Orifice, Generic backdoor, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero
8076	Possível ataque W32.Spybot.pen
8081	Possível ataque W32.Bufei
8090	Possível ataque Aphex's Remote Packet Sniffer, Backdoor.Asniffer
8097	Possível ataque Kryptonic Ghost Command Pro
8100	Possível ataque Back streets
8110	Possível ataque DLP, LoseLove
8111	Possível ataque DLP, LoseLove
8126	Possível ataque W32.PejayBot
8127	Possível ataque 9_119, Chonker
8130	Possível ataque 9_119, Chonker, DLP
8131	Possível ataque DLP
8301	Possível ataque DLP, LoseLove
8302	Possível ataque DLP, LoseLove
8311	Possível ataque SweetHeart
8322	Possível ataque DLP
8329	Possível ataque DLP
8372	Possível ataque NetBoy
8488	Possível ataque (UDP) - KiLo
8489	Possível ataque (UDP) - KiLo
8685	Possível ataque Unin68
8720	Possível ataque Connection
8732	Possível ataque Kryptonic Ghost Command Pro
8734	Possível ataque AutoSpY
8783	Possível ataque Suspected but unanalyzed trojan used port
8787	Possível ataque Back Orifice 2000
8811	Possível ataque Backdoor.Monator, Fear, Force
8812	Possível ataque FraggleRock Lite
8821	Possível ataque Alicia

8848	Possível ataque Whirlpool
8864	Possível ataque Whirlpool
8866	Possível ataque Beagle.B@mm, W32.Beagle.B@mm worm
8879	Possível ataque BackOrifice 2000, Hack Office Armageddon
8888	Possível ataque Dark IRC, squid HTTP Proxy server scan, W32.Axatak
8889	Possível ataque W32.Axatak
8897	Possível ataque HackOffice
8899	Possível ataque Last
8988	Possível ataque BacHack, BackHack
8989	Possível ataque Rcon, Recon, Xcon
9000	Possível ataque Aristotles, Netministrator trojan, W32.randex.ccf
9090	Possível ataque Aphex's Remote Packet Sniffer
9117	Possível ataque Massaker
9125	Possível ataque Backdoor.nibu.k
9148	Possível ataque Nautical
9301	Possível ataque DLP, LoseLove
9325	Possível ataque Mstream (handler to agent), MStream Agent-handler
9329	Possível ataque DLP
9400 a 9402	Possível ataque InCommand, In Command
9536	Possível ataque Lula
9561	Possível ataque CRatPro, Crat Pro
9563	Possível ataque CRatPro, Crat Pro
9580	Possível ataque TheefLE
9604	Possível ataque W32.kibuv.worm
9612	Possível ataque Danton, Ghost
9696	Possível ataque Backdoor.gholame, Danton, Ghost
9697	Possível ataque Backdoor.gholame
9870	Possível ataque BackDoor.RC3.B, Remote Computer Control Center (R3C)
9872 a 9875	Possível ataque Portal of Doom (POD), Portal of Doom 1.x
9876	Possível ataque Cyber Attacker, Rux trojan
9877	Possível ataque Small Big Brother, SmallBigBrother
9878	Possível ataque SmallBigBrother, Trans Scout, Transmission Scout
9879	Possível ataque Small Big Brother, SmallBigBrother

9898	Possível ataque Dabber, W32.dabber.a
9899	Possível ataque Ini-Killer, Ini-Killer trojan, W32.dabber.a
9900 a 9988	Possível ataque W32.dabber.a
9989	Possível ataque Ini-Killer trojan, W32.dabber.a
9990 a 9994	Possível ataque W32.dabber.a
9995	Possível ataque W.32.Sasser Worm, W32.dabber.a
9996 a 9998	Possível ataque W32.dabber.a
9999	Possível ataque BlitzNet, ForcedEntry, Infra, Oracle, Spadeace, The Prayer 1, The prayer 1.2 -1.3, The Prayer trojan, W32.dabber.a
10000	Possível ataque Oracle, OpwinTRojan, TCP Door, W32.dumaru.ad, XHX
10001	Possível ataque Backdoor.Zdemon.126, DTr, Lula
10002	Possível ataque Backdoor.Zdemon.126, Lula
10003	Possível ataque Lula
10005	Possível ataque OpwinTRojan
10008	Possível ataque Cheese worm, li0n, Lion, Lion Worm
10012	Possível ataque Amanda
10013	Possível ataque Amanda
10067	Possível ataque Portal of Doom (POD), Portal of Doom 4.x
10080	Possível ataque Mydoom.B
10084 a 10086	Possível ataque Syphillis trojan
10100	Possível ataque backdoor.ranky.o, Control Total, GiFt trojan, Scalper
10101	Possível ataque BrainSpy, NewSilencer, Silencer
10102	Possível ataque backdoor.staprew
10103	Possível ataque backdoor.tuimer
10167	Possível ataque Portal of Doom (POD), Portal of Doom 5.x, PortalOfDoom
10498	Possível ataque Mstream, Mstream (handler to agent), Mstream handler-agent
10520	Possível ataque Acid Shivers trojan
10528	Possível ataque Host Control trojan, HostControl
10607	Possível ataque Coma

10666	Possível ataque (UDP) - Ambush
10752	Possível ataque LINUX mounts Backdoor
10887	Possível ataque BDDT
10889	Possível ataque BDDT
11000	Possível ataque DataRape, Senna Spy, Senna Spy Trojan Generator
11011	Possível ataque Amanda
11050	Possível ataque Host Control trojan, HostControl
11051	Possível ataque Host Control trojan, HostControl
11111	Possível ataque Breach
11223	Possível ataque AntiNuke, Progenic trojan, Secret Agent
11225	Possível ataque Cyn
11306	Possível ataque Noknok
11660	Possível ataque Back streets
11718	Possível ataque Kryptonic Ghost Command Pro
11831	Possível ataque DarkFace, DataRape, Katux, Latinus Server, Pest
11977	Possível ataque Cool Remote Control
11978	Possível ataque Cool Remote Control
11980	Possível ataque Cool Remote Control
11991	Possível ataque PitfallSurprise
12000	Possível ataque Backdoor.Satancrew, Reverse Trojan
12043	Possível ataque Frenzy
12065	Possível ataque Backdoor.Berbew.j
12076	Possível ataque Gjamer
12223	Possível ataque Hack 99 KeyLogger
12310	Possível ataque PreCursor
12321	Possível ataque Protoss
12345	Possível ataque Adore sshd, cron / crontab, Ashley, Backdoor.Amitis.B, Bluelce 2000, Fade, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, trojan, NetBus Toy, NetBus worm, Pie Bill Gates, Q-Taz, Sensive, Vagr Nocker, ValvNet, ValvaNet, Whack Job, X-bill, Snape
12346	Possível ataque Fat Bitch trojan, GabanBus, NetBus trojan, X-bill
12348	Possível ataque BioNet
12349	Possível ataque BioNet, The Saint, Webhead
12361	Possível ataque TCP Whack-a-mole

12362	Possível ataque TCP Whack-a-mole, Whack-a-mole 1.x
12363	Possível ataque Whack-a-mole
12389	Possível ataque KheSanh
12456	Possível ataque NetBus
12478	Possível ataque Bionet
12623	Possível ataque ButtMan, DUN Control
12624	Possível ataque ButtMan trojan, Power
12625	Possível ataque Buttman
12631	Possível ataque Whack Job, WhackJob
12684	Possível ataque Power
12701	Possível ataque Eclipse 2000, Eclypse 2000
12754	Possível ataque Mstream (attacker to handler), Mstream attack-handler
12904	Possível ataque Acropolis, Akropolis, Rocks
12973	Possível ataque QR keylogger/remote access
12975	Possível ataque QR keylogger/remote access
13000	Possível ataque Senna Spy Trojan Generator
13010	Possível ataque BitchController, Hacker Brasil - HBR, Hacker Brazil
13013	Possível ataque PsychWard
13014	Possível ataque PsychWard
13028	Possível ataque Back streets
13079	Possível ataque Kryptonic Ghost Command Pro
13173	Possível ataque Backdoor.Amitis.B
13223	Possível ataque Hack´99 KeyLogger
13370	Possível ataque SpArTa
13371	Possível ataque Optix Pro
13468	Possível ataque W32.Sober.D
13473	Possível ataque Chupacabra
13500	Possível ataque Theef
13700	Possível ataque (the) Unknown Trojan, Kuang 2 The Virus
13753	Possível ataque Anal FTP, AFTP
14100	Possível ataque Eurosol
14194	Possível ataque CyberSpy
14247	Possível ataque Trojan.Mitglieder.h
14285	Possível ataque Laocoon
14286	Possível ataque HellDriver, Laocoon

14287	Possível ataque Laocoon
14500 a 14504	Possível ataque PC Invader, PCInvader
15000	Possível ataque NetDemon, R0xr4t, Route to the Hell
15092	Possível ataque Host Control trojan, HostControl
15104	Possível ataque Mstream (attacker to handler), Mstream attack-handler
15206 e 15207	Possível ataque KiLo
15210	Possível ataque (UDP) - UDP remote shell backdoor server
15382	Possível ataque SubZero
15432	Possível ataque Cyn, Backdoor.Cyn
15485 e 15486	Possível ataque KiLo
15500	Possível ataque In Route to the Hell
15512	Possível ataque Iani
15551	Possível ataque In Route to the Hell
15555	Possível ataque ICMIBC
15695	Possível ataque Kryptonic Ghost Command Pro
15845	Possível ataque (UDP) - KiLo
15852	Possível ataque Kryptonic Ghost Command Pro
15858	Possível ataque CDK trojan
16057	Possível ataque MoonPie
16322	Possível ataque Backdoor.Lastdoor, LastDoor
16484	Possível ataque Mosucker trojan
16514	Possível ataque KiLo
16515	Possível ataque KiLo
16523	Possível ataque Back streets
16660	Possível ataque Stacheldracht, Stracheldracht, Stracheldraht
16661	Possível ataque Backdoor.Haxdoor.D, Dfch
16712	Possível ataque KiLo
16761	Possível ataque Kryptonic Ghost Command Pro
16772	Possível ataque ICQ Revenge trojan
16959	Possível ataque SubSeven , Subseven 2.1.4 DefCon 8
16969	Possível ataque Portal of Doom (POD), Priority trojan, Progenic
16982	Possível ataque AcidShiver

17166	Possível ataque Mosaic trojan
17300	Possível ataque Kuang 2, Kuang 2 the Virus, Kuang2, Kuang2.B Trojan
17449	Possível ataque Kid Terror trojan
17499	Possível ataque CrazzyNet, CrazyNet
17500	Possível ataque CrazzyNet
17569	Possível ataque Infector
17593	Possível ataque AudioDoor
17777	Possível ataque Nephron trojan
18667	Possível ataque Knark
18753	Possível ataque Shaft (handler to agent), Shaft handler to Agent
19191	Possível ataque BlueFire
19216	Possível ataque BackGate Kit
19604	Possível ataque Metal
19605	Possível ataque Metal
19864	Possível ataque ICQ Revenge trojan
19937	Possível ataque Backdoor.Gaster
19991	Possível ataque Dfch
20000	Possível ataque Millenium (Lm), Millenium Worm, PSYcho Files, XHX
20001	Possível ataque Insect, Millenium Worm, Millennium, PSYcho Files
20002	Possível ataque AcidkoR trojan, PSYcho Files
20005	Possível ataque MoSucker
20023	Possível ataque VP Killer
20034	Possível ataque NetBus 2 Pro, NetRex, Whack Job
20139	Possível ataque skanbotz IRC-SubSeven Trojan
20168	Possível ataque W32.HLLW.Lovgate.C@mm
20203	Possível ataque Chupacabra trojan, Logged!, Logged! Attack
20331	Possível ataque BLA trojan, (the) Unknown Trojan
20432	Possível ataque Shaft (client to handler), Shaft Client to handlers
20433	Possível ataque Shaft (agent to handler), Shaft Agent to handlers
20480	Possível ataque Trojan.Adnap
20742	Possível ataque Trojan.Mitglieder.E
21212	Possível ataque Schwindler, Sensive
21544	Possível ataque (the) Unknown Trojan, Exploiter, Girl Friend, Kid Terror, Matrix, Schwindler, Winsp00fer
21554	Possível ataque Exploiter, FreddyK, GirlFriend, Kid Terror,

	Schwindler, Sensive, Winsp00fer
21579	Possível ataque Breach
21584	Possível ataque Breach
21684	Possível ataque Intruse
21957	Possível ataque Latinus
22068	Possível ataque AcidShiver
22115	Possível ataque Cyn
22222	Possível ataque Donald Dick, G.R.O.B., Prosiak, Prosiak 0.47, Ruler, RUX The TIc.K
22223	Possível ataque RUX The TIc.K
22311	Possível ataque Backdoor.Simali
22456	Possível ataque BLA, Clandestine
22457	Possível ataque AcidShiver, BLA
22554	Possível ataque Schwindler
22783	Possível ataque Intruzzo
22784	Possível ataque Backdoor-ADM, Intruzzo
22785	Possível ataque Intruzzo
22845	Possível ataque Breach
22847	Possível ataque Breach
23000	Possível ataque Storm worm
23001	Possível ataque Storm worm
23005	Possível ataque NetTrash, Infinaeon, Olive, W32.hllw.nettrash
23006	Possível ataque Infinaeon, NetTrash, Oxon, W32.hllw.nettrash
23023	Possível ataque Logged trojan
23032	Possível ataque Amanda
23232	Possível ataque backdoor.berbew.j
23321	Possível ataque Konik
23432	Possível ataque Asylum
23435	Possível ataque Trojan.Framar
23456	Possível ataque Clandestine, Evil FTP, Ugly FTP, Vagr Nocker, BagrNocker, Whack Job, WhackJob
23476	Possível ataque DonaldDick, Donald Dick
23477	Possível ataque Donald Dick, DonaldDick, InetSpy, Inet Spy
24000	Possível ataque Infector
24289	Possível ataque Latinus
24307	Possível ataque Wildek

24680	Possível ataque Suspected but unanalyzed trojan used port
25002	Possível ataque MOTD
25123	Possível ataque Goy'Z TroJan
25386	Possível ataque MoonPie
25486	Possível ataque MoonPie
25555	Possível ataque FreddyK
25556	Possível ataque FreddyK
25685	Possível ataque MoonPie
25686	Possível ataque DarkFace, MoonPie
25799	Possível ataque FreddyK
25885	Possível ataque MOTD
25982	Possível ataque DarkFace, MoonPie
26274	Possível ataque (UDP) - Delta Source
26681	Possível ataque Spy Voice
27160	Possível ataque MoonPie
27184	Possível ataque Alvgus trojan 2000
27373	Possível ataque Charge
27374	Possível ataque Bad Blood, EGO, Fake SubSeven, 0n, Lion, Muerte, Ramen, Seeker, SubSeven , SubSeven 2.1 Gold, bseven 2.1.4 DefCon 8, SubSeven 2.2, SubSeven Muie, The Saint, loader, Webhead
27379	Possível ataque Backdoor.optix.04, Optix Lite
27444	Possível ataque Denial of Service , Trin00/TFN2K
27573	Possível ataque Sub-7 2.1, Sub-7 v2.0
27665	Possível ataque Denial of Service , Trin00 DoS Attack
28218	Possível ataque Oracle
28429 a 28436	Possível ataque Hack'a'Tack, Hack-a-Tack
28678	Possível ataque Exploiter
29104	Possível ataque Host Control, HostControl, NETrojan
29147	Possível ataque Backdoor.Sdbot.ai
29292	Possível ataque BackGate Kit, Backdoor.NTHack
29369	Possível ataque ovasOn
29559	Possível ataque AntiLamer BackDoor , DarkFace, DataRape, Katux, Latinus, :atomis Server. Pest, Vagr Nocker

29589	Possível ataque KiLo
29891	Possível ataque The Unexplained
29976	Possível ataque Trojan Spirit 2001a
29980	Possível ataque Trojan Spirit 2001a
29984	Possível ataque Trojan Spirit 2001a
29999	Possível ataque AntiLamer BackDoor, Backdoor.Antilam.20
30000	Possível ataque DataRape, Infector
30001	Possível ataque Err0r32, ErrOr32, Terr0r32, TerrOr32
30003	Possível ataque Lamers Death trojan, LamersDeath
30005	Possível ataque Backdoor JZ, Litmus
30029	Possível ataque AOL Admin trojan, AOLTrojan
30100 a 30103	Possível ataque NetSphere
30129	Possível ataque Masters Paradise
30133	Possível ataque NetSphere, NetSphere Final, Trojan Spirit 2001a
30303	Possível ataque Socket 23, Socket 25, Socket23, Sockets de Troie 1.x, Sokets de Trois v1
30331	Possível ataque MuSka52
30464	Possível ataque Slapper
30700	Possível ataque Mantis
30947	Possível ataque Intruse trojan
30974	Possível ataque Intruse
30999	Possível ataque Kaung 2, Kaung2
31221	Possível ataque Knark
31320	Possível ataque LittleWitch, Little Witch
31335	Possível ataque attempted Denial of Service (Trin00/TFN2k), Trin00 DoS Attack
31336	Possível ataque BO-Whack, ButtFunnel
31337	Possível ataque ADM worm, Back Fire, Back Orifice, Back Orifice (Lm), Back Orifice 1.20 patches, Back Orifice russian, Baron Night, Beeone, bindshell, BlitzNet, BO client, BO Facil, BO spy, BO2, cron / crontab, Deep BO, Freak2k, Freak88, Gummo, Khaled, Linux Rootkit IV, Netpatch, OPC, NoBackO, Sm4ck, Sockdmini
31338	Possível ataque Back Orifice (BO), ButtFunnel, Deep BackOrifice, Netspy, NetSpy (DK), NetSpy DK, DeepBO

31339	Possível ataque Little Witch, LittleWitch, Net Spy, NetSpy (DK)
31340	Possível ataque Little Witch
31382	Possível ataque Lithium
31399	Possível ataque NetSpy (DK)
31415	Possível ataque Lithium
31416	Possível ataque Lithium
31554	Possível ataque Schwindler
31557	Possível ataque NetBus, Xanadu
31631	Possível ataque CleptoManicos
31666	Possível ataque BOWhack
31745	Possível ataque BuschTrommel
31785 a 31792	Possível ataque Hack'a'Tack, Hack'a'Tack, Hack-A-Tack Attack
31887	Possível ataque BDDT
31889	Possível ataque BDDT
32000	Possível ataque BDDT
32001	Possível ataque Donald Dick, DonaldDick
32100	Possível ataque Peanut Brittle, Project nEXT
32121	Possível ataque backdoor.berbew.j
32418	Possível ataque Peanut Brittle, AcidBattery, Project nEXT
32440	Possível ataque Backdoor.Alets.B
32768	Possível ataque Hacker's Paradise
32791	Possível ataque Acropolis, Akropolis, Rocks
33270	Possível ataque Trinity trojan
33291	Possível ataque RemoteHak
33333	Possível ataque Blackharaz, Blakharaz trojan, Prosiak
33390	Possível ataque (the) Unknown Trojan
33545	Possível ataque G.R.O.B.
33567	Possível ataque li0n, Lion, T0rn Rootkit
33568	Possível ataque li0n, Lion, T0rn Rootkit
33577	Possível ataque PsychWard, Son of PsychWard
33911	Possível ataque Spirit 2000, Spirit 2001, Spirit 2001 a, Spirit 2001a
34312	Possível ataque Delf
34313	Possível ataque Delf
34324	Possível ataque BigGluck, TelnetServer, TN

34343	Possível ataque Osiris
34444	Possível ataque Donald Dick, DonaldDick
34555	Possível ataque Trin00 ping/pong response attack, Trinoo (Windows)
34763	Possível ataque Infector
35000	Possível ataque Infector
35555	Possível ataque Trin00 ping/pong response attack, Trinoo (Windows)
35600	Possível ataque SubSARI
36183	Possível ataque Backdoor.Lifefournow
36794	Possível ataque Bugbear
37237	Possível ataque Mantis
37266	Possível ataque The Killer Trojan
37651	Possível ataque Charge, Yet Another Trojan, Yet Another Trojan - YAT
37653	Possível ataque Yet Another Trojan - YAT
38741	Possível ataque CyberSpy, Cyber Spy
38742	Possível ataque CyberSpy, Cyber Spy
39507	Possível ataque Busters
39999	Possível ataque TrojanProxy.Win32.Mitglieder
40071	Possível ataque Ducktoy
40308	Possível ataque SubSARI
40412	Possível ataque TheSpy, The Spy
40421 a 40426	Possível ataque Agent, Agent 40421, Master's of Paradise, MastersParadise
40999	Possível ataque DiemsMutter
41337	Possível ataque Storm
41626	Possível ataque Shah
41666	Possível ataque RBT, Remote Boot Tool , Remote Boot Tool
43210	Possível ataque Master's Paradise
43720	Possível ataque (UDP) - KiLo
44014	Possível ataque Iani
44280	Possível ataque Backdoor.Amitis.B
44390	Possível ataque Backdoor.Amitis.B
44444	Possível ataque Prosiak
44575	Possível ataque Exploiter
44767	Possível ataque School Bus
45092	Possível ataque BackGate Kit

45454	Possível ataque Osiris
45559	Possível ataque Maniac rootkit
45632	Possível ataque Little Witch
45673	Possível ataque Acropolis, Akropolis, Rocks
46626	Possível ataque Psychward
46666	Possível ataque Taskman
46882	Possível ataque Psychward
47017	Possível ataque T0rn Rootkit
47252	Possível ataque Delta Source
47262	Possível ataque (UDP) - Delta Source
47387	Possível ataque Backdoor.Amitis.B
47698	Possível ataque KiLo
47785	Possível ataque KiLo
47891	Possível ataque AntiLamer BackDoor, Backdoor.antilam.20
48004	Possível ataque Fraggle Rock, FraggleRock
48006	Possível ataque Fraggle Rock, FraggleRock
48512	Possível ataque Arctic
49000	Possível ataque Fraggle Rock, FraggleRock
49301	Possível ataque OnLine KeyLogger
49683	Possível ataque Fenster
49698	Possível ataque (UDP) - KiLo
50000	Possível ataque Infector, SubSARI
50005	Possível ataque Trojan.Fulamer.25
50021	Possível ataque Optix Pro
50130	Possível ataque Enterprise
50505	Possível ataque Sokets de Trois v1, Sokets de Trois v2, Sockets des Troie
50551	Possível ataque R0xr4t
50552	Possível ataque R0xr4t
50766	Possível ataque Fore 1.0 trojan, Schwindler
50776	Possível ataque Fore, Fore 1.0 trojan, Remote Windows Shutdown
50829	Possível ataque KiLo
51234	Possível ataque Cyn, Backdoor.Cyn
51435	Possível ataque W32.kalel.a@mm
51966	Possível ataque Cafeini trojan

51996	Possível ataque Cafeini trojan
52317	Possível ataque Acid Battery 2000
52365	Possível ataque Way
52901	Possível ataque (UDP) - Omega
53001	Possível ataque Remote Windows Shutdown - RWS
54283	Possível ataque SpyPort, Spy Port, SubSeven , SubSeven 2.1 Gold
54320	Possível ataque Back Orifice, Back Orifice 2000
54321	Possível ataque Back Orifice 2000, Delta Source, PCInvader
55165	Possível ataque File Manager trojan, WMTrojan Generator
55166	Possível ataque WM Trojan Generator
55555	Possível ataque Shadow Phyre
55665	Possível ataque Latinus, Pinochet
55666	Possível ataque Latinus, Pinochet
56565	Possível ataque Backdoor.Osirdoor, Osiris
57163	Possível ataque BlackRat
57341	Possível ataque NetRaider
57785	Possível ataque G.R.O.B.
58008	Possível ataque BackDoor.Tron
58009	Possível ataque BackDoor.Tron
58134	Possível ataque Charge
58339	Possível ataque Butt Funnel, ButtFunnel
58666	Possível ataque BackDoor.Redkod
59211	Possível ataque BackDoor.DuckToy, Duck Toy
60000	Possível ataque Foreplay, Sockets des Troie, Deep Throat , Deepthroat, MiniBacklash, Reduced Foreplay
60001	Possível ataque Trinity
60006	Possível ataque Trojan.Fulamer.25
60008	Possível ataque li0n, Lion, T0rn Rootkit
60068	Possível ataque Xzip 6000068 trojan, The Thing
60411	Possível ataque Connection
60551	Possível ataque R0xr4t
60552	Possível ataque R0xr4t
60666	Possível ataque Basic Hell
61000	Possível ataque Backdoor.mite
61115	Possível ataque Protoss

61337	Possível ataque Nota
61348	Possível ataque Bunker-Hill
61440	Possível ataque Orion
61466	Possível ataque TeleCommando
61603	Possível ataque Bunker-Hill
61746	Possível ataque KiLo
61747	Possível ataque KiLo
61748	Possível ataque (UDP) - KiLo
61979	Possível ataque Cool Remote Control
62011	Possível ataque Ducktoy
63485	Possível ataque Bunker-Hill trojan
63808	Possível ataque Phatbot
63809	Possível ataque Phatbot, W32.hllw.gaobot.dk
64101	Possível ataque Task Manager trojan, Taskman
64429	Possível ataque Backdoor.Amitis.B
65000	Possível ataque Devil, Sockets des Troie, Stacheldraht
65289	Possível ataque yoyo
65390	Possível ataque Eclypse
65421	Possível ataque Alicia, Jade
65422	Possível ataque Alicia
65432	Possível ataque The Traitor (= th3tr41t0r)
65506	Possível ataque Agobot, Gaobot, PhatBot infection
65530	Possível ataque Windows Mite
65534	Possível ataque /sbin/initd
65535	Possível ataque Adore Worm/Linux, RC trojan, Adore worm, Sins