ESCOLA POLITÉCNICA
DE PERNAMBUCO

d.s.c. UPE
Departamento de Sistemas e Computação

GERENCIAMENTO E CONTROLE DE RESPOSTA A INCIDENTES EM REDES DE COMPUTADORES UTILIZANDO SOFTWARE LIVRE: UM ESTUDO DE CASO COM O SISTEMA DE CONTROLE RTIR

Trabalho de Conclusão de Curso

Engenharia da Computação

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

Francisco Hamilton de Freitas Junior
Orientador: Prof. Renato Mariz de Moraes

UNIVERSIDADE
DE PERNAMBUCO

Francisco Hamilton de Freitas Junior

GERENCIAMENTO E CONTROLE DE RESPOSTA A INCIDENTES EM REDES DE COMPUTADORES UTILIZANDO SOFTWARE LIVRE: UM ESTUDO DE CASO COM O SISTEMA DE CONTROLE RTIR

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia da Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, dezembro de 2008

Resumo

A necessidade de segurança é um fato que vem crescendo constantemente em quase todas as empresas. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios tecnológicos que dispõe de tal velocidade e eficiência pode resultar em grandes prejuízos. Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus, exploração em larga escala de ferramentas para ataques coordenados e distribuídos, que afetam e causam grandes prejuízos, notadamente, com o roubo de informações sobre clientes. Juntando isso também com a complexidade das infra-estruturas das redes de computadores e o desafio da administração destas redes interconectadas, fica difícil gerenciar corretamente a segurança deste ambiente. Os administradores de redes e de sistemas não têm práticas suficientes de segurança para se defender de ataques e minimizar os danos causados. Uma boa maneira de estabelecer uma resposta rápida e assim impedir os futuros incidentes é estabelecer um grupo de respostas a incidente de segurança em redes de computadores. Com isso esse trabalho tem como objetivo integrar um sistema de acompanhamento de requisições com ênfase em incidentes de segurança utilizando as principais ferramentas de segurança para *Linux* em *software* livre existentes atualmente nas áreas de detecção de intrusos (*Snort*), filtro de pacotes (*Iptables*), monitoramento de servidores e serviços (*Nagios*) e varredura de vulnerabilidades (*Nessus*).

Abstract

The need for security is a fact that is constantly growing in almost all companies. While the speed and efficiency in all business processes mean a competitive advantage, the lack of security in the technological means that have such speed and efficiency can result in large losses. Among the facts that demonstrate the increased importance of security, we can highlight the rapid spread of the virus, large-scale exploitation of tools for distributed and coordinated attacks, which affect and cause great damage, especially with the theft of information on customers. In addition to this, with the complexity of the infrastructure of computer networks and the challenge of the administration of these interconnected networks, it is difficult to properly manage the security of this environment. Administrators of networks and systems do not have sufficient security practices to defend themselves against attacks and minimize damage. A good way to establish a rapid response and thus prevent future incidents is to establish a group of responses to security incidents in computer networks. Therefore, this work aims to integrate a system for tracking requests with emphasis to security incidents using the main security tools for Linux on free software currently existing in the areas of intrusion detection (Snort), packet filter (Iptables), monitoring of servers and services (Nagios) and scanning of vulnerabilities (Nessus).

Sumário

RESUMO ..... **I**

ABSTRACT ..... **II**

SUMÁRIO ..... **III**

ÍNDICE DE FIGURAS ..... **VI**

ÍNDICE DE TABELAS ..... **VII**

TABELA DE SÍMBOLOS E SIGLAS ..... **VIII**

CAPÍTULO 1 INTRODUÇÃO **9**

1.1 OBJETIVOS 10

CAPITULO 2 SEGURANÇA DE REDES EM AMBIENTES CORPORATIVOS **12**

2.1 AMBIENTES CORPORATIVOS 12

2.2 SEGURANÇA DE REDES NAS CORPORAÇÕES 13

2.3 PROBLEMAS NOS AMBIENTES CORPORATIVOS 14

2.4 COMO A SEGURANÇA É VISTA HOJE 16

CAPITULO 3 RESPOSTA A INCIDENTES DE SEGURANÇA EM REDES DE COMPUTADORES **18**

3.1 POLÍTICAS DE SEGURANÇA 18

3.2 POLÍTICA DE USO ACEITÁVEL 19

3.3 USO ABUSIVO DA REDE 19

3.4 *FIREWALL* 19

3.5 SISTEMA DE DETECÇÃO DE INTRUSOS 21

3.5.1 Sistema de Detecção de Intrusão de Rede *21*

3.5.2 Sistema de Detecção de Intrusão de Host *22*

3.6 SISTEMA DE MONITORAMENTO DE REDE 22

3.7 FALSOS POSITIVOS 23

3.8 REGISTRO DE ATIVIDADES OU EVENTOS 23

3.9 NOTIFICAÇÃO DE INCIDENTES E ABUSOS 24

CAPITULO 4 GRUPOS DE RESPOSTAS A INCIDENTES EM REDES DE COMPUTADORES 26

4.1 TAMANHO DE UM GRUPO DE RESPOSTA A INCIDENTES 26
4.2 MODELO DE UTILIZAÇÃO PARA ORGANIZAÇÕES 27
4.3 RAZÕES PARA SE UTILIZAR UM GRUPO DE RESPOSTA A INCIDENTES 28
4.3 1 Habilidade para Coordenar 28
4.3 2 Especialização 28
4.3 3 Eficiência 28
4.3.4 Habilidade para Trabalhar de Forma Pró-ativa 29
4.3.5 Atingir os Requisitos Desejados pelas Agências ou corporações 29
4.3.6 Servir como elo 29

CAPITULO 5 DESCRIÇÃO DO SISTEMA 30

5.1 IPTABLES 30
5.2 NESSUS 32
5.3 SNORT 33
5.4 NAGIOS 35
5.4 1 Características 35
5.5 RTIR (SISTEMA DE CONTROLE DE REQUISIÇÃO PARA RESPOSTAS INCIDENTES) 37
5.6 INTEGRAÇÃO DAS FERRAMENTAS 38
5.6.1 Análise de Vulnerabilidade 41
5.6.2 Análise dos Registros de Eventos do Firewall 41
5.6 3 Análise dos Registros de Eventos do IDS 41
5.6.4 Alertas do sistema de Monitoramento 42
5.6.4 Registro dos Casos no Sistema de Controle de Requisições 43
5.6.6 Classificação dos Tíquetes no Sistema de Requisições 43
5.6.7 Utilização do sistema de Requisição pelos Membros do Grupo de Respostas a Incidentes 43

CAPITULO 6 CENÁRIOS DE USO 46

6.1 DESCRIÇÃO DOS AMBIENTES DE TESTE 46
6.1.1 Programas 46
6.1.2 Equipamentos 47

6.1.3 Topologias 48

6.2 CENÁRIOS 49

6.2.1 Cenário 1 – Incidentes reportados por usuários 49

6.2.2 Cenário 2 - Notificação de Parada de Servidor ou Serviço pelo Nagios 51

6.2.3 Cenário 3 – Análise de um relatório de registro do Nessus com Vulnerabilidades 53

6.2.4 Cenário 4 – Construindo uma Base de Conhecimento com Artigos 55

CAPITULO 7 CONCLUSÕES E CONTRIBUIÇÕES 57

7.1 CONTRIBUIÇÕES 57

7.2 DIFICULDADES 57

7.3 TRABALHOS FUTUROS 58

BIBLIOGRAFIA 59

ANEXO A MODELO DE POLÍTICA DE SEGURANÇA 61

ANEXO B MODELO DE POLÍTICA DE USO ACEITÁVEL 64

ANEXO C SCRIPT DE REGRAS DE FIREWALL (IPTABLES) 66

ANEXO D ANÁLISE DE VULNERABILIDADE COM NESSUS 68

ANEXO E ANÁLISE DE TRÁFEGO DO FIREWALL COM FWLOGWATCH 70

Índice de Figuras

Figura 1 Ambiente Corporativo.....13
Figura 2 Perigo das Triangulações.....15
Figura 3 Os Diferentes Níveis de Acesso.....16
Figura 4 Filtro de Pacotes.....20
Figura 5 Filtragem em Nível de aplicação.....20
Figura 6 Filtragem em Nível de Circuito.....21
Figura 7 Fluxo de Dados da Tabela *Filter* do *Iptables*.....32
Figura 8 Arquitetura do *Snort*.....34
Figura 9 Diagrama de Rede Emprel.....36
Figura 10 Troca de Mensagens e Processos Realizados para a integração.....38
Figura 11 Situação Pró-ativa de Utilização do Sistema.....39
Figura 12 Situação Reativa de Utilização do Sistema.....40
Figura 13 Topologia Utilizada nos Testes.....48
Figura 14 Topologia Sugerida para Utilização nas Corporações.....49
Figura 15 Criação Manual de Tíquete na Fila *Incidents Report* pelo Usuário.....50
Figura 16 Criação do Tíquete na Fila Incidents e Criando o Vinculo..52
Figura 17 Resolução do Tíquete para o problema do Servidor DNS..53
Figura 18 Abertura de Investigação sobre a vulnerabilidade.....54
Figura 19 Criação de um Artigo.....56

Índice de Tabelas

Tabela 1. Estrutura de Tabela do *Iptables*.....31

Tabela de Símbolos e Siglas

TCP	*Transmission control Protocol*
IP	*Internet Protocol*
FTP	*File Transfer Protocol*
TI	Tecnologia da Informação
CERT	Centro de Estudos, Respostas e Tratamentos de Incidentes
CSIRTs	*Computer Security Incident Response Teams*
IDS	*Intrusion Detection System*
NIDS	*Network Intrusion Detection System*
HIDS	*Host Intrusion Detection System*
DNS	*Domain Name System*
NAT	*Network Address Translator*
DNAT	*Destination Network Address Translator*
SNAT	*Source Network Address Translator*
RT	*Request Tracker*
RTIR	*Request Tracker for Incident Response*

Capítulo 1

Introdução

A disseminação das redes e, particularmente da Internet é o fenômeno tecnológico de maior impacto social atualmente. A capacidade de estar em todos os lugares ao mesmo tempo da Internet e a popularização do microcomputador trouxeram um novo ambiente global, no qual uma infinidade de possibilidades convive, algo de forma descontrolada, porém com crescente vitalidade. Todos reconhecem que a Internet nasceu e se desenvolveu com pouquíssimo controle central. Isso eliminou muitas barreiras de entrada e foi, certamente, um dos principais fatores de sua rápida adoção e sucesso.

Porém, à medida que vem a maturidade e que a velha economia passa a lançar olhares ambiciosos à nova economia, torna-se mais e mais necessários munir a internet dos recursos que garantam a segurança, não só dos internautas, mas também das empresas que realizam negócios pela rede. Há muitas empresas que querem abrir as corporações à rede, mas expor suas bases de informação e seus sistemas aos ataques dos malfeitores reais e virtuais que infestam a internet torna-se um grande perigo[1].

O mundo virtual tem as mesmas características do mundo real e, há tempos, os eventos de segurança, ataques e invasões em computadores deixaram de ser atividades solitárias e não destrutivas. Há muito mais envolvimento nestas ações. Pensando nisso, é primordial a preocupação em manter a segurança dos computadores e das redes que os conectam.

Conseqüentemente, a forma pela qual os criminosos cometem seus delitos também está mudando. O fácil acesso ao mundo digital possibilita novas oportunidades para estas pessoas. Muito dinheiro é gasto para investigar os crimes cometidos através dos computadores. Na pior das hipóteses um computador pode ser utilizado para prejudicar vítimas ou para violentos ataques, inclusive para gerenciar e executar atividades terroristas que ameaçam a vida de milhares de pessoas. Infelizmente em muitos casos a justiça tem ficado para trás destes criminosos, pois não possui a tecnologia e o pessoal apropriados para tratar estas recentes e crescentes ameaças, que podem ser denominadas de crimes digitais ou *cybercrimes*.

A capacidade de responder a um incidente de segurança de computador está se tornando cada vez mais importante no mundo de hoje. A eficiência da reposta de uma empresa a um incidente é que faz a diferença entre um ataque frustrado e a manchete nos jornais. O problema é que geralmente as empresas não têm conhecimento do fato até que seja tarde demais. Então essa falta pode ser prevenida com um modelo pró-ativo de resposta a incidentes. Fazer diretivas e procedimentos de resposta a incidentes de segurança previamente pode evitar muitos problemas e também economizar tempo e dinheiro.

A necessidade do mundo real de resposta a incidentes em redes computadores é anterior aos computadores em mais de um século. No caso de um cofre, por exemplo, ele deve ser testado para que as pessoas possam saber quanto tempo um criminoso pode levar para arrombar o mesmo. Este tempo é importante para ter uma expectativa de quanto tempo uma empresa tem para responder a um ataque levando em conta que este cofre esteja sendo monitorado por câmeras. Se alguém estiver observando as imagens obtidas pelas câmeras fica óbvio identificar quando o cofre esta sendo atacado e o criminoso também sabe que tem um tempo limite para completar sua tarefa[1].

No meio digital esta situação é mais complexa, pois os criminosos que fazem seus ataques pela rede têm tempo ilimitado para invadir um sistema. Uma vez que o sistema tenha sido invadido, no caso do cofre itens são removidos, mas nos casos de crimes digitais os itens podem ser copiados, deixando os originais intactos, a menos quando o motivo do crime é político e não financeiro.

Para que possam ser eficazes na reposta a incidente de segurança, as empresas necessitam combinar tecnologia com disciplina. No estado atual o cenário da segurança avança rapidamente e não espera por ninguém. Sem dominar os princípios básicos e formar um modelo de segurança preventivo, as empresas ficaram num eterno jogo de correr atrás dos avanços desta área e sempre acabar perdendo a corrida.

1.1 Objetivos

Este trabalho apresenta um sistema que é uma integração de uma ferramenta de controle de requisições para respostas a incidente com as principais ferramentas de segurança de redes em *Linux* existentes atualmente. Este sistema recebe periodicamente a análise dos registros e as notificações destas ferramentas, buscando prevenir ataques, reduzindo tempo de conhecimento de um incidente, orientar e desenvolver as ações que deverão ser tomadas, baseadas nas ações registradas para cada caso. Por isto os primeiros incidentes que a ferramenta reconhecer e que forem respondidos pelos membros poderão servir como referência para os futuros casos.

O sistema de requisições estará integrado com uma ferramenta de varredura de vulnerabilidades, que irá fazer a analise dos servidores indicados e gerar um relatório com as vulnerabilidades encontradas. Este relatório será enviado ao sistema para que os membros do grupo de respostas façam uma analise das devidas correções, caso sejam necessárias, e o registro destas ações dentro da requisição.

Na forma pró-ativa, um sistema de detecção de intrusos fará o reconhecimento dos ataques e notificará o sistema de requisições sobre estes ataques, para que os membros do grupo tenham fácil conhecimento destes ataques e possam tomar as devidas ações.

Na forma reativa, um sistema de monitoramento de rede irá notificar o sistema de requisições que um problema ocorreu em um host ou serviço e uma requisição será criada no sistema para que um membro do grupo possa tomar as ações necessárias com relação ao problema.

Ainda na forma reativa, poderão ser abertas requisições manualmente ou através do envio de mensagem eletrônica pelos usuários do sistema para que incidentes de segurança, que não podem ser identificados pelo sistema de monitoramento de rede e o sistema detector de intrusão, possam ser respondidos.

Também serão enviados periodicamente ao sistema de requisições, relatórios com informações encontradas nos registros do sistema de detecção de intrusos e nos registros do sistema de filtro de pacotes, para que os membros do grupo de resposta a incidentes tenham informações mais detalhadas dos eventos que ocorrem periodicamente na rede. Isso facilitará a análise dos registros destas ferramentas para a criação de incidentes de segurança baseados nestas análises.

Este sistema pode beneficiar as empresas em geral que estão interligadas à grande rede mundial de computadores e possuem informações confidenciais ou prestam serviços de missão crítica, pois poderá prevenir ou no mínimo reduzir o tempo de conhecimento de um incidente. Nos casos em que os incidentes forem respondidos, será armazenada uma base de conhecimento com todo o histórico dos incidentes e as ações que foram tomadas o que pode ajudar muito no desenvolvimento da resolução de futuros incidentes.

No capítulo 2 é descrito quais são os problemas que o ambiente corporativo enfrenta nos dias de hoje, no capítulo 3 é descrito o conceito de resposta a incidente de segurança em redes de computadores. No capítulo 4 é descrito o que são grupos de resposta a incidentes de segurança em redes de computadores, pra que eles servem e como podem atuar. No capítulo 5 é falado como é feita a integração do sistema de requisição de resposta a incidente com as ferramentas de varredura de vulnerabilidade, filtro de pacotes, detecção de intrusos e monitoramento de serviços e servidores de rede. Também é especificado como funciona todo sistema de requisição de resposta a incidente. No capítulo 6 são descrito os equipamentos e programas utilizados na simulação do ambiente de teste e alguns cenários para realização destes. No Capítulo 7 é apresentada a conclusão de todo conteúdo proposto.

Capitulo 2

Segurança de Redes em Ambientes Corporativos

2.1 Ambientes corporativos

No mundo globalizado e de rápidos avanços tecnológicos, as oportunidades de negócios vêm e vão com a mesma rapidez desses avanços. Todos vivenciam uma época de grandes transformações tecnológicas, econômicas e mercadológicas. Grandes fusões estão acontecendo, implicando também na fusão de infra-estrutura de redes de telecomunicações, o que pode resultar em sérios problemas relacionados à segurança. Além das fusões entre as organizações, as parcerias comerciais e as formas de comunicação avançam de tal modo que a infra-estrutura de rede, de vital importância para os negócios, passa a ser uma peça fundamental para todos, nesse novo modelo de negócios[1].

Esse contexto atual, de grandes transformações comerciais e mercadológicas, somando à importância cada vez maior do papel da Internet, faz com que surja um novo ambiente, no qual múltiplas organizações trocam informações por meio de uma rede integrada. Informações técnicas, comerciais e financeiras, necessárias para o bom andamento dos negócios, agora trafegam por essa rede que conectar matrizes de empresas com suas filiais, seus clientes, parceiros comerciais e distribuidores. A complexidade dessa rede atinge níveis consideráveis, o que implica em cuidados e medidas que devem ser tomados, principalmente com relação à proteção das informações que fazem parte dessa rede [1].

O ambiente corporativo é caracterizado pela integração dos mais diversos sistemas de diferentes organizações, nos quais as partes envolvidas cooperam entre si, na busca de um objetivo comum: velocidade e eficiência nos processos e nas realizações de negócios, que representa os elementos-chave para o sucesso de qualquer tipo de organização. A formação de um ambiente corporativo na Figura 1 pode ser visto com muitas conexões e evoluções.

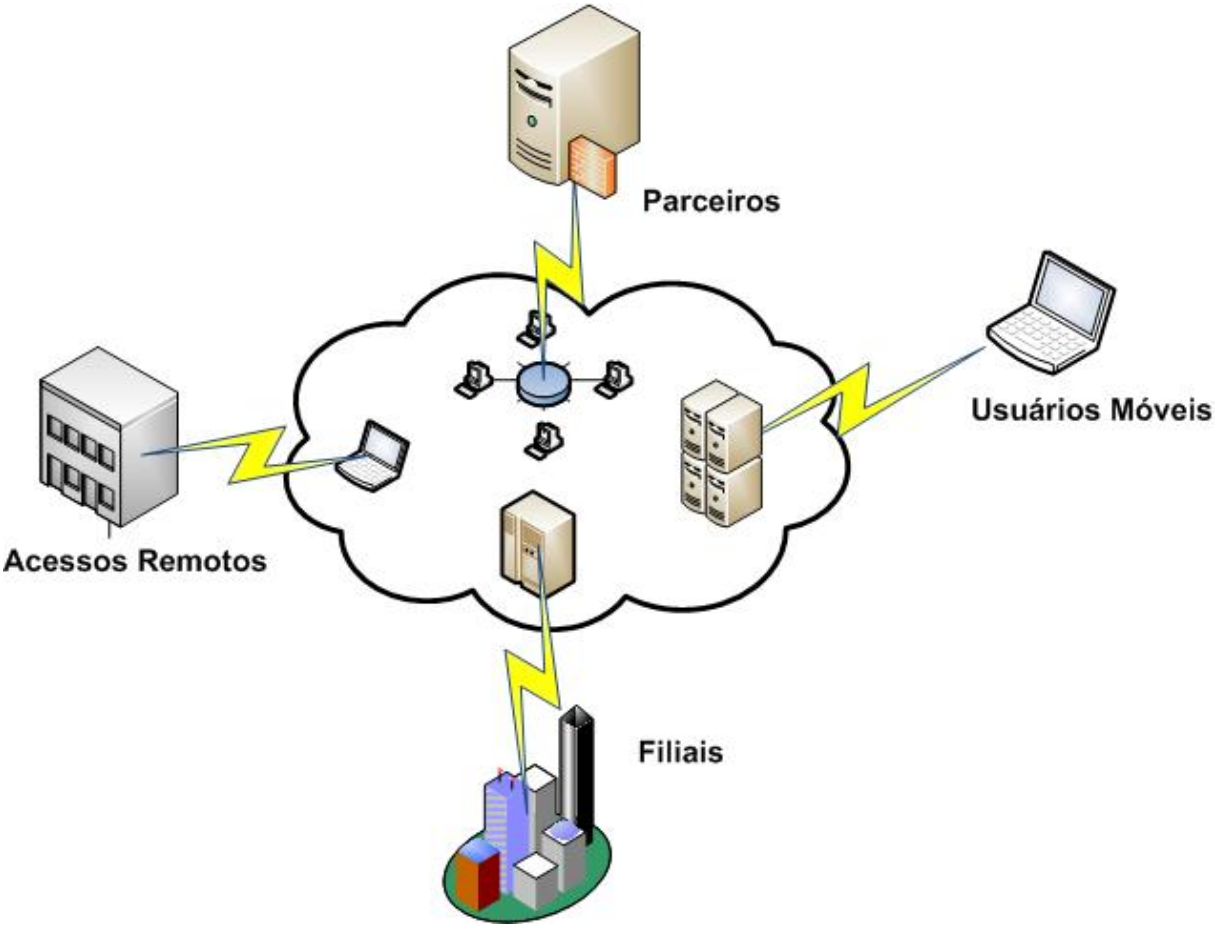

Figura 1. Ambiente Corporativo.

2.2 Segurança de Redes nas Corporações

A informática é um instrumento cada vez mais utilizado pelo homem para que ele possa realizar seus trabalhos de modo rápido, eficiente e competitivo, produzindo assim os melhores resultados. A rede é um dos elementos principais, permitindo as conexões entre os computadores. A flexibilidade, a facilidade e a disponibilidade dos recursos que são acessíveis por meio da rede resultam em uma maior produtividade e, conseqüentemente, em maiores lucros dentro de uma organização [1].

A confiabilidade e a disponibilidade dessa estrutura de redes passam, assim, a ser essenciais para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. A segurança de rede, que pode prover essa proteção, significa, na realidade, muito mais do que proteção contra hackers, maus funcionários ou vírus. A segurança significa considerar não

apenas uma proteção, mas o elemento habilitador para que os negócios da organização sejam realizados.

Dentre os fatos que demonstram o aumento da importância da segurança, pode-se destacar a rápida disseminação de vírus e de worm[1], cada vez mais sofisticados, roubos de informações privativas e invasões são um fato corriqueiro, demonstrando a rápida popularização dos ataques a sistemas de computadores.

Segundo Nakamura [1], os ataques que vêm causando os maiores problemas para as organizações são aqueles que acontecem a partir da sua própria rede, ou seja, os ataques internos. Somando a isso, está o fato de as conexões entre as redes das organizações alcançarem níveis de integração cada vez maiores. Os ambientes corporativos, formados a partir de conexões entre organizações e filiais, fornecedores, parceiros comerciais, distribuidores ou vendedores, resultam na necessidade de um novo tipo de abordagem quanto à segurança. Antes se utilizava a idéia de proteger a rede da organização isolando-a das redes publicas. O objetivo hoje é justamente o contrario: disponibilizar cada vez mais serviços e permitir a comunicação entre sistemas de diferentes organizações, de forma segura. A complexidade aumenta, pois, agora, a proteção deve ocorrer não somente contra os ataques vindos da rede publica, mas também contra aqueles que podem ser considerados internos, originados a partir de qualquer ponto do ambiente corporativo.

2.3 Problemas nos Ambientes Corporativos

A propriedade determinante dos ambientes corporativos é a complexidade que envolve a comunicação entre diferentes tecnologias, diferentes usuários, diferentes culturas e diferentes políticas internas. O conjunto de protocolos TCP/IP e a Internet possibilitam o avanço em direção aos ambientes corporativos, ao tornar possíveis as conexões entre as diferentes organizações, de modo mais simples e mais barato do que as conexões dedicadas. Porém, essa interligação teve como conseqüência uma enorme implicação quanto à proteção dos valores de cada organização [1].

Algumas situações refletindo o grau de complexidade existente nos ambientes corporativos podem ser vistas quando são analisadas, por exemplo, as conexões entre três organizações (Figura 2). Como proteger os valores da organização A, evitando que um usuário da organização B acesse informações que pertencem somente à organização A? Pode-se supor uma situação em que os usuários da organização B não podem acessar informações da organização A, porém os usuários da organização C podem fazê-lo. Como evitar que usuários da organização B acessem informações da organização A, por meio da organização C? Como pode ser visto na Figura 2, isso constitui um caso típico de triangulação, em que uma rede é utilizada como ponte para outra rede. Neste exemplo, usuários da organização B

[1] Worm é um programa similar a um vírus, porém, capaz de realizar cópias de si mesmo e de algumas de suas partes de computador para computador.

podem acessar as informações de A, o que é proibido, utilizando a estrutura da organização C como ponte.

Os problemas que aparecem quando isso ocorre são grandes, pois a organização B pode ter acesso a informações confidenciais da organização A, sem que ela sequer tome conhecimento desse fato, pois o acesso aconteceu por intermédio da organização C.

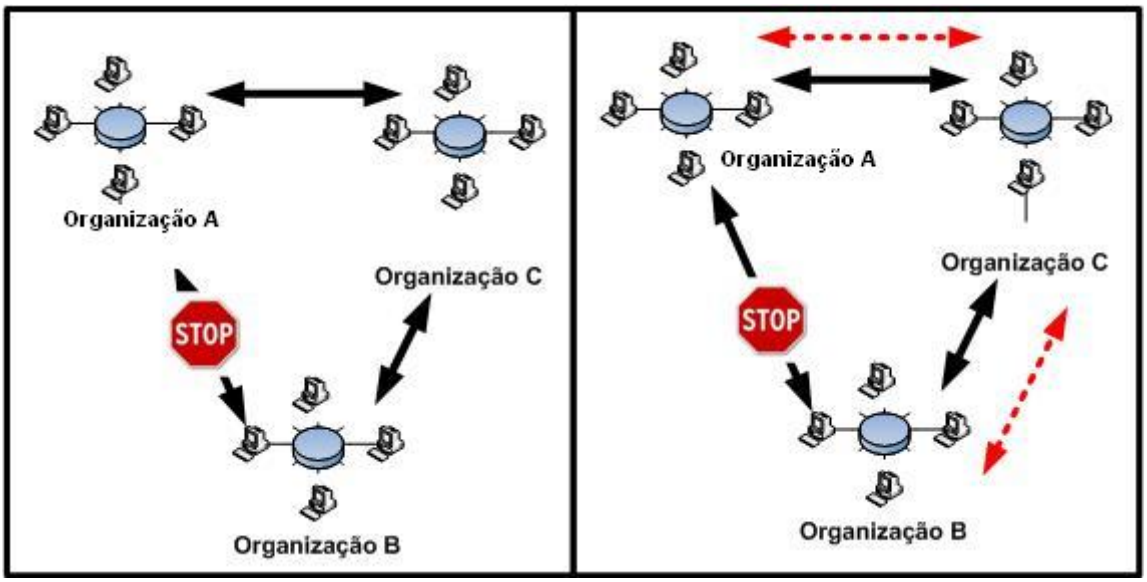

Figura 2. Perigo das Triangulações.

Além das triangulações, outro problema que pode ocorrer em um ambiente corporativo é o aumento da complexidade dos níveis de acesso. Isso pode ser visto num exemplo em que usuários da organização A podem acessarem todos os recursos da organização, enquanto os usuários da organização B podem acessar somente determinados recursos, como por exemplo, um servidor FTP que contém os arquivos de relatórios diários de uma determinada empresa ou filial. Somando isso, há fato de que os usuários da Internet não podem acessar nenhum recurso da organização A, enquanto a organização C tem acesso irrestrito aos recursos da organização A. Essa situação demonstra o grande desafio de controlar os acessos em diferentes níveis, o que pode se tornar mais complexo ainda se diferentes usuários da organização B necessitam acessar recursos da organização A. Ainda nesse exemplo, pode-se ver novamente o problema da triangulação, de modo ainda mais crítico: os usuários da Internet podem chegar à organização A, caso a organização B ou C tenha acesso à Internet. Na Figura 3 podemos ver um exemplo dessa situação.

A divisão entre os diferentes tipos de usuários, os desafios a serem enfrentados no ambiente corporativo e a complexidade que envolve a segurança desses ambientes são barreiras a ser vencidas [1].

2.4 Como a Segurança é Vista Hoje

Apesar de a segurança ser, atualmente, essencial para os negócios das organizações, a dificuldade em entender a sua importância ainda é muito grande. E isso constitui um risco muito grande para organização, pois, mais cedo ou mais tarde, alguém poderá descobrir que um grande tesouro está à sua completa disposição. De fato, é apenas uma questão de tempo para que isso aconteça, causando grandes prejuízos, sejam financeiros, morais ou relacionados à reputação. E todos sabem que uma boa reputação pode demorar anos para ser construída, mas pode ser destruída em questão de instantes. Por exemplo, para um banco, um incidente de segurança, por menor que seja, fará com que seus clientes percam a confiança nos serviços prestados, e eles procurarão outros meios para movimentarem seus recursos financeiros.

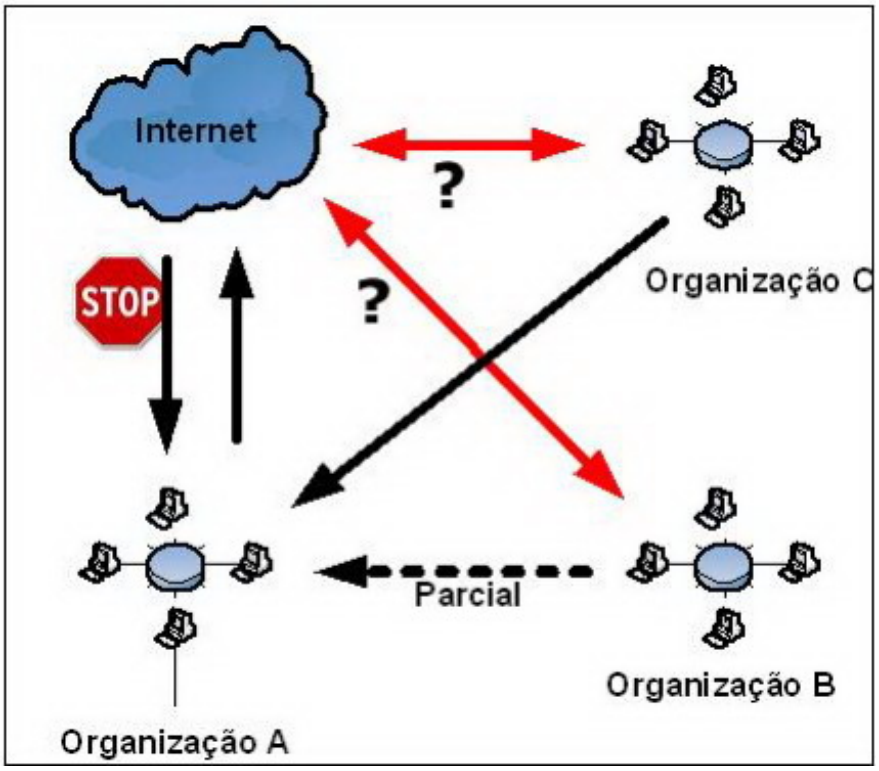

Figura 3. Os diferentes níveis e Acesso.

A organização que faz parte de um ambiente corporativo deve entender que a segurança, agora, é essencial para o sucesso de seus negócios. Se nos bancos a relação de confiança existia entre a instituição e seus clientes, hoje, essa relação ocupa dimensões ainda maiores em que a confiança não deve existir apenas entre a organização e seus clientes, mas também entre a organização e seus fornecedores, parceiros, distribuidores e funcionários.

Isso porque um incidente de segurança em um único ponto desse ambiente pode comprometer todo o ambiente corporativo [1].

O que é realmente necessário é que o ambiente corporativo seja analisado de acordo com a sua importância e com os grandes benefícios que ele pode trazer à organização. É impossível que um ambiente corporativo seja considerado sem que as questões relacionadas à segurança sejam discutidas. Esse é o maior desafio da segurança: a solução de segurança é imensurável e não resulta em soluções nos quais todos podem notar que alguma coisa foi feita. Pelo contrário, a segurança tem justamente o papel de evitar que alguém perceba que alguma coisa está errada na infra-estrutura tecnológica da organização. Sobre a segurança, ainda hoje se tem esse conceito de que ela é um artigo caro e indispensável, necessário somente quando algum ataque acontece e traz prejuízos à organização. Apesar disso, algumas organizações já vêem a segurança com outros olhos, passando a considerá-la como parte essencial do negócio. A formação de equipes de segurança é um indicativo desse fato.

A segurança ainda é um campo novo, e muitos não conseguem enxergar sua importância, imaginando apenas que as soluções são caras e não trazem nenhum retorno financeiro. Apesar de que essa visão está melhorando com o decorrer dos anos, e faz com que os executivos prefiram aplicar seus recursos em novas soluções que possam trazer vantagens visíveis aos olhos de todos [1].

Capitulo 3

Resposta a Incidentes de Segurança em Redes de Computadores

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Um incidente de segurança pode ser ocasionado por tentativas de ganhar acesso não autorizado a sistemas ou dados; ataques de negação de serviço; uso não autorizado de um sistema; modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema; desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso [2]. Neste capítulo são abordadas algumas respostas aos incidentes que ocorrem em redes de computadores

3.1 Políticas de Segurança

Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribuem direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem [2].

Um modelo de uma política de segurança foi colocado no anexo A e pode ser utilizado como modelo de uma política de segurança de uma organização.

3.2 Política de Uso Aceitável

A política de uso aceitável é um documento que define como podem ser utilizados os recursos computacionais de uma instituição, também define os direitos e responsabilidades dos usuários.

No caso dos provedores de acesso à Internet, a política de uso aceitável normalmente fica disponível em suas páginas. As empresas costumam dar conhecimento da política de uso aceitável no momento da contratação ou quando o funcionário começa a utilizar os recursos computacionais da empresa [2]. Foi incluído neste trabalho um exemplo de política de uso aceitável no anexo B.

3.3 Uso Abusivo da Rede

Existem algumas situações que ocorrem internamente nas empresas ou instituições que caracterizam o uso abusivo da rede e geralmente estão definidas na política de uso aceitável. Na Internet, comportamento como envio de *spam*, envio de correntes de felicidade e de correntes para ganhar dinheiro fácil e rápido, cópia e distribuição não autorizada de material protegido por direitos autorais, utilização da Internet para fazer calúnias, ameaças e difamações, tentativas de ataques a outros computadores, comprometimento de computadores ou redes, são geralmente considerados como uso abusivo [2].

3.4 *Firewall*

A necessidade de utilização cada vez maior da Internet pelas empresas e a constituição de ambientes corporativos levam a uma crescente preocupação quanto à segurança. Como conseqüência disso, pode-se ver uma rápida evolução na área de segurança, principalmente com relação ao *firewall*, que é uma dos principais, mais conhecidos e antigos componentes de um sistema de segurança.

O *firewall* é um sistema ou um grupo de sistemas que reforça a política de controle de acesso entre duas redes e, portanto, pode ser visto como uma aplicação da política de segurança. O *firewall* é tão seguro quanto a política de segurança com que ele trabalha e não se deve esquecer que um *firewall* muito restritivo, e, portanto mais seguro, não é sempre transparente ao usuário. Caso isso aconteça, alguns usuários podem tentar driblar a política

de segurança da organização para poder realizar algumas tarefas a que estavam acostumados antes de sofrerem restrição.

Segundo Willian [3], um *firewall* forma uma barreira através da qual o tráfego indo a cada direção precisa passar. Uma política de segurança de *firewall* dita qual tráfego tem autorização para passar em cada direção.

Antigamente os *firewalls* tinham poucas funcionalidades como, por exemplo, apenas fazia filtro de pacotes. De lá para cá, diante da obvia evolução dos meios tecnológicos, o *firewall* começou seu desenvolvimento com outras funcionalidades como: controle de serviço que determina os tipos de serviços de Internet que podem ser acessados, de entrada ou saída. O *firewall* pode filtrar o trafego com base no endereço IP e número da porta TCP; controle de direção que determina a direção em que determinadas solicitações de serviços podem ser iniciadas e permitidas para fluir através do *firewall*; controle de usuário que controla o acesso a um serviço de acordo com qual usuário está tentando acessa - lá, essa característica normalmente é aplicada aos usuários dentro do perímetro do *firewall* (usuários locais); controle de comportamento que controla como determinados serviços são usados, por exemplo, o *firewall* pode filtrar e-mail para eliminar *spam* ou pode permitir o acesso externo a apenas a informação em um servidor *web* local, na Figura 4,5 e 6 mostra alguns exemplos de tipos diferentes de estruturas e funcionalidades do *firewall* [3].

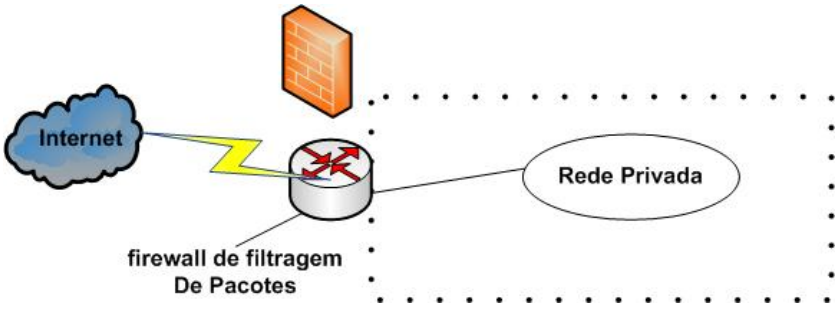

Figura 4. Filtragem de Pacotes.

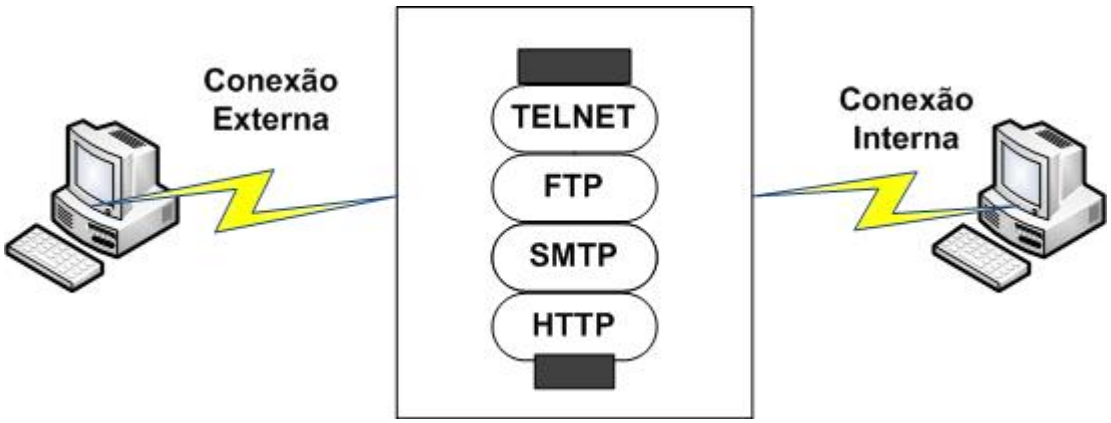

Figura 5. Filtragem em nível de aplicação.

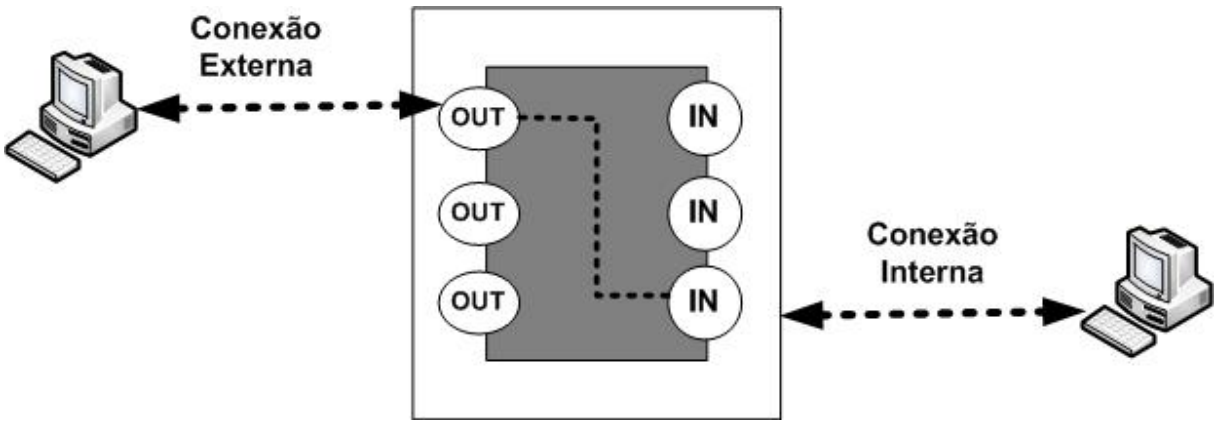

Figura 6. Filtragem em nível de circuito.

No Linux, as funções de *firewall* são agregadas à própria arquitetura do *kernel*, isso o torna, sem duvida, muito superior em relação a seus concorrentes. Enquanto a maioria dos "produtos" *firewall* pode ser definida como subsistema, o Linux possui capacidade de transformar o *firewall* no próprio [5].

Neste trabalho é utilizado o *Netfilter* (*Iptables)* para fazer a filtragem de pacotes e o *firewall admin* para fazer o gerenciamento pela web das regras do *firewall*.

3.5 Sistema de Detecção de Intrusos

O sistema de detecção de intrusos *(Intrusion Detections System - IDS)* é um componente essencial em um ambiente corporativo. Podendo detectar diversos ataques e intrusões, a localização do *IDS* é um dos pontos a serem definidos com cuidado. O IDS é capaz de detectar e alertar os administradores quanto a possíveis ataques ou comportamentos anormais na organização. Informações importantes sobre tentativas de ataques, que não se pode obter normalmente, podem ser conseguidas por meio desses sistemas. Elas podem oferecer subsídios suficientes para que a organização melhore sua proteção contra quaisquer tipos de ataques, principalmente os considerados internos [1].

3.5.1 Sistema de Detecção de Intrusão de Rede

O *Network-Based Intrusion Detection system (NIDS)* monitora o trafego de segmento de rede, geralmente com interface de rede atuando em modo

'promíscuo', ou seja, redirecionando todo trafego da rede para sua interface. A detecção é realizada com a captura e análise dos cabeçalhos e conteúdos dos pacotes, que são comparados com padrões ou assinaturas conhecidos em um banco de dados.

3.5.2 Sistema de Detecção de Intrusão de Host

O *Host Based Intrusion Detection System (HIDS)* faz o monitoramento do sistema, com base em informações de arquivos de *logs* ou de agentes de auditoria instalados como agentes em uma maquina. O HIDS pode ser capaz de monitorar acessos e alterações em importantes arquivos do sistema, modificações nos privilégios dos usuários, processos de sistemas, programas que estão sendo executados, entre outros aspectos.

O HIDS pode também realizar a checagem da integridade dos arquivos do sistema, por meio de *checksums*. Essa é uma característica importante, porque arquivos corrompidos e estranhos são detectados antes que causem problemas mais sérios. Alguns *HIDS* são pró-ativos. Eles podem capturar o tráfego de rede vindo para um *host* em particular no qual o *HIDS* está instalado e fazer um alerta em tempo real.

3.6 Sistema de Monitoramento de Rede

Sistemas deste tipo são projetados para informar aos administradores sobre problemas de rede em servidores ou serviços. Geralmente existe um processo que é central que executa checagens intermitentes nos servidores e serviços que foram especificados na configuração. Quando problemas com estes servidores ou serviços ocorrem o processo de monitoramento envia notificações para os contatos administrativos.

A identificação de ataques em uma rede pode ser feita de diversas maneiras. Quando um sistema está publicado na Internet, o *firewall* pode registrar em arquivo todas as tentativas de acesso que foram negadas e permitidas, porém quando um *firewall* permite que o acesso a um serviço que esteja publicado na Internet seja feito de qualquer lugar, fica quase impossível diferenciar um ataque que esteja sendo feito neste serviço de um acesso realmente legítimo, portanto se um ataque for realmente feito neste recurso, isto não vai ser percebido pelo *firewall*. Caso ainda não exista uma assinatura para este ataque no NIDS ou por algum motivo não foi feita a atualização das assinaturas a tempo, o NIDS também não vai perceber o ataque. Se este ataque prejudicar de alguma forma este serviço, deixando-o indisponível, então um sistema de monitoramento de rede que esteja configurado para monitorar este recurso pode fazer o alerta do problema. Este tipo de situação pode ser chamado de reativa, pois o ataque só vai ser identificado se o servidor ou serviço ficarem indisponíveis. Além disso, também podem ser monitorados alguns indicadores do servidor como utilização do processador, memória e espaço em disco.

3.7 Falsos Positivos

O termo "falso positivo" é utilizado para designar uma situação em que um *firewall* ou IDS aponta uma atividade como sendo um ataque, quando na verdade esta atividade não é um ataque. Um exemplo clássico de falso positivo ocorre quando uma ferramenta *antispam* marca uma mensagem como *spam* quando, na verdade, ela não é. Um caso comum de falso positivo ocorre quando o *firewall* não está devidamente configurado e indicam como ataques as respostas às solicitações feitas pelo próprio usuário.

3.8 Registro de Atividades ou Eventos

Logs são registros de atividades gerados por programas de computador. No caso de *logs* relativos à incidente de segurança, eles normalmente são gerados por *firewalls* ou por sistemas de detecção de intrusão.

Os *firewalls*, dependendo de como foram configurados, podem gerar *logs* quando alguém tenta acessar um computador e este acesso é barrado pelo *firewall*. Sempre que um *firewall* gera um *log* informando que um determinado acesso foi barrado, isto pode ser considerado uma tentativa de ataque, mas também pode ser um falso positivo.

Já os sistemas de detecção de intrusão podem gerar *logs* tanto para casos de tentativa de ataques, quanto para casos em que um ataque teve sucesso. Apenas uma análise detalhada pode dizer se uma atividade detectada por um IDS foi um ataque com sucesso. Assim como os *firewalls*, os sistemas de detecção de intrusão também podem gerar falsos positivos [2]. Segundo o CERT [2], *os logs* relativos a ataques recebidos pela rede, em geral, possuem as seguintes informações:

- Data e horário em que ocorreu uma determinada atividade;
- Endereço IP de origem e destino da atividade;
- Portas envolvidas.

Dependendo do grau de refinamento da ferramenta que gerou o *log* ele também pode conter informações como:

- O *timezone* do horário do *log*;
- Protocolo utilizado (TCP, UDP, ICMP);
- Os dados completos que foram enviados para o computador ou rede.

3.9 Notificação de Incidentes e Abusos

Um ataque lançado contra uma máquina ou uma rede normalmente tem uma destas duas origens:

- Um programa malicioso que está fazendo um ataque de modo automático, como por exemplo, um *worm*;
- Uma pessoa que pode estar ou não utilizando ferramentas que automatizam ataque.

Quando o ataque parte de uma máquina que foi vítima de um *worm*, reportar este incidente para os responsáveis pela máquina que originou o ataque vai ajudá-los a identificar o problema e resolvê-lo.

Se este não for o caso, a pessoa que está atacando o seu computador pode estar violando a política de uso aceitável da rede que utiliza ou, pior ainda, pode ter invadido uma máquina e a estar utilizando para atacar outros computadores. Neste caso, avisar os responsáveis pela máquina de onde parte o ataque pode alertá-los para o mau comportamento de um usuário ou para uma invasão que ainda não havia sido detectada [2].

Os incidentes ocorridos devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui:

- Os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede;
- O grupo de segurança e abusos da rede em que se está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição).

Caso algum dos sítios envolvidos seja brasileiro mantenha informado o CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), mantido pelo Comitê Gestor da Internet no Brasil (CGI. BR). O CGI é responsável pelo tratamento de incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil [2].

Dentre as atribuições do CERT estão:

- Ser um ponto central para notificações de incidentes de segurança no Brasil, de modo a prover a coordenação e o apoio no processo de resposta a incidentes, colocando as partes envolvidas em contato quando necessário;
- Manter estatísticas sobre os incidentes a ele reportados;
- Desenvolver documentação de apoio para usuários e administradores de redes Internet.

Manter o CERT com cópias das notificações de incidentes de segurança é importante para permitir que:

- As estatísticas geradas reflitam os incidentes ocorridos na Internet brasileira;
- O CERT escreva documentos direcionados para as necessidades dos usuários da Internet no Brasil;
- O CERT possa correlacionar dados relativos a vários incidentes, identificar ataques coordenados, novos tipos de ataques, etc.

Para saber como encontrar os responsáveis pela máquina de onde partiu um ataque na Internet são mantidas diversas bases de dados com as informações a respeito dos responsáveis por cada bloco de números IPs existente. Estas bases de dados estão nos chamados "Servidores de *Whois*".

O servidor de *Whois* para os IPs alocados ao Brasil pode ser consultado em http://registro.br/. Para os demais países e continentes existem diversos outros servidores. O site http://www.geektools.com/whois.php aceita consultas referentes a qualquer número IP e redireciona estas consultas para os servidores de *Whois* apropriados.

Os passos para encontrar os dados dos responsáveis incluem:

- Acessar o site http://registro.br/ e fazer uma pesquisa pelo número IP ou pelo nome de domínio da máquina de onde partiu a atividade;
- Se o IP da máquina estiver alocado para o Brasil, os dados dos responsáveis serão exibidos;
- Se aparecer a mensagem: "Não alocado para o Brasil", significa que o IP está alocado para algum outro país. Uma consulta no site http://www.geektools.com/whois.php pode retornar os e-mails dos responsáveis.

Vale lembrar que os e-mails que são encontrados a partir destas consultas não são necessariamente os e-mails da pessoa que praticou o ataque. Estes e-mails são dos responsáveis pela rede onde a máquina está conectada, ou seja, podem ser os administradores da rede, sócios da empresa, ou qualquer outra pessoa que foi designada para cuidar da conexão da instituição com a Internet [2].

Capitulo 4

Grupos de Respostas a Incidentes em Redes de computadores

Segundo Shultz e Shumway [7], muitas vezes podem ser encontrados o termo “reposta à incidente” equacionado ao termo “grupo de respostas a incidentes”. Isto pode parecer superficialmente lógico, mas quando estes conceitos são trazidos para a realidade as coisas podem ser diferentes. Pessoas que não conhecem o processo de reposta a incidentes podem estar envolvidas em lidar com incidentes relacionados a segurança. Os usuários são um exemplo clássico.

Supondo que um vírus tenha infectado diversos sistemas em uma organização. Os usuários podem colaborar com informações do que está ocorrendo e até mesmo no combate ao vírus, mas dificilmente poderiam ser chamados de um grupo de resposta, pois não têm a capacidade técnica de dar uma conclusão a um possível ou real incidente de segurança. Um grupo de resposta a incidentes possui uma série de obrigações relacionadas a levar cada incidente de segurança a uma conclusão, de acordo com os objetivos da organização que ele serve. A grande diferença entre indivíduos que lidam com um incidente e um grupo de respostas a incidentes é a missão designada a cada um, em termos de responsabilidades de sua função de trabalho. Os indivíduos podem, algumas vezes, vir a se envolver no tratamento de um incidente, mas para um grupo de resposta a incidentes é designada a responsabilidade de lidar com incidentes em uma grande parte ou de todas as descrições das tarefas dos indivíduos envolvidos.

4.1 Tamanho de um Grupo de Resposta a Incidentes

Segundo Shultz e Shumway [7], o número de componentes de um grupo de resposta a incidentes está relacionado com o tamanho da organização para a qual trabalham, podendo ser formado por apenas uma pessoa. Em alguns casos, independentemente do tamanho da organização, o grupo de respostas a incidentes é formando por uma pessoa que tem a

responsabilidade de efetivamente coordenar os esforços de um número de pessoas. Quando os esforços para tratar um incidente estão encerrados, os outros indivíduos envolvidos no incidente são dispensados de qualquer responsabilidade que eles possam ter recebido no tratamento de um incidente. Mas o membro do grupo tem a responsabilidade diária de acompanhar o tratamento dos incidentes e deverá coordenar os esforços para lidar com os próximos incidentes que ocorrerem.

Alguns grupos de resposta a incidentes possuem muitos membros, cada um com uma função específica, por exemplo, o CERT possui membros em sua equipe engajados nas operações diárias, como receber os relatórios de incidentes e tentar identificar o tipo, origem, impacto, e outras observações de um incidente de segurança que foi relatado. Outros tentam negociar com fabricantes para que vulnerabilidades conhecidas sejam fechadas em sistemas operacionais, aplicações e assim por diante. Ainda existem outros que examinam dados para identificar e projetar as tendências dos incidentes, algo mais relacionado à pesquisa.

4.2 Modelo de Utilização para Organizações

Uma organização pode ter o seu próprio grupo de resposta a incidente ou contratar uma empresa especializada para providenciar o suporte à resposta de incidentes, para ambos os modelos existem vantagens e desvantagens. A principal vantagem de contratar uma empresa especializada em resposta a incidentes é que o custo total no tratamento de incidentes relacionados à segurança seja provavelmente menor, pois o pessoal de resposta a incidentes precisa lidar apenas com incidentes que ocorrem. A menos que haja um grande número de incidentes, não existe a necessidade de manter um pessoal fixo para ficar esperando que um incidente aconteça. Adicionalmente algumas empresas de segurança de informações usualmente oferecem tipos diferentes de especialidades que muitas vezes podem não estar presente nas organizações.

A principal vantagem de manter um grupo de respostas a incidentes internamente à organização é que todos os esforços para o tratamento dos incidentes são feitos baseados na política e na cultura da organização. Os incidentes de segurança são potencialmente muito sensíveis e políticos; um grupo interno seria provavelmente a maneira mais vantajosa para a organização na condição, óbvia, de que os indivíduos dentro deste grupo entendam a cultura e a política da organização.

4.3 Razões Para se Utilizar um Grupo de Resposta a Incidentes

Existem várias questões que justificam a formação de um grupo de resposta a incidentes e segundo Shultz e Shumway [7], as principais são a habilidade de coordenar, a especialização dos indivíduos, eficiência, a habilidade para trabalhar de forma pró-ativa, atingir os requisitos desejados por agências ou corporações e ter um meio de ligação de credibilidade com outras organizações. Estas questões serão explicadas a seguir:

4.3 1 Habilidade para Coordenar

É mais fácil coordenar os esforços de indivíduos que fazem parte de um grupo de resposta a incidentes porque geralmente os indivíduos se reportam a um líder, que irá designar para cada membro do grupo uma atividade em particular para ser executada.

4.3 2 Especialização

Os incidentes de segurança da informação estão cada vez mais complexos e por isto especialista no tratamento de incidentes são cada vez mais necessários nas organizações. Técnicos muitos especializados são úteis quando um incidente ocorrer, mas somente especialidade técnica não é suficiente para muitos incidentes. É importante ter experiência em muitos incidentes anteriores e ter o conhecimento de quais políticas devem ser consideradas e quais procedimentos devem ser seguidos.

4.3 3 Eficiência

Geralmente um grupo constrói uma base de conhecimento, o que implica no aumento da eficiência. Um indivíduo sozinho pode facilmente desviar do caminho correto quando estiver lidando com um incidente, porém a inteligência coletiva acumulada dentro de um grupo pode ajudar nos esforços de fazer com que o alvo de um incidente retorne ao caminho correto. Com um time, ao contrário de um indivíduo ou poucos indivíduos independentes, é mais provável o desenvolvimento e o cumprimento de procedimentos para responder incidentes.

4.3.4 Habilidade para Trabalhar de Forma Pró-ativa

Ser pró-ativo é uma das chaves para ter sucesso no esforço de responder incidentes. Treinar usuários e administradores de sistemas para reconhecer sintomas de incidentes e o que se deve fazer, bem como o que não se deve fazer é um bom exemplo de esforço pró-ativo.

4.3.5 Atingir os Requisitos Desejados pelas Agências ou corporações

A principal razão é que um time tem indivíduos que são direcionados a uma mesma missão. É importante lembrar que algumas agências governamentais e corporações vão um passo a frente em suas exigências na qual, através de uma decisão gerencial ou política estabelecida, exigem que um grupo de respostas a incidentes seja formado.

4.3.6 Servir como elo

Grupos de resposta a incidentes são melhores para servir como elo, do que indivíduos, porque para entidades externas não estão motivadas a tratar com indivíduos. Tendo a identidade de um grupo, provavelmente uma visibilidade externa é fornecida, bem como credibilidade, ambos os quais satisfazem mais a função de ligação. Além do mais, em muitos aspectos, um grupo controla certo grau de legitimidade dentro de organizações internas e externas.

Capitulo 5

Descrição do Sistema

Este trabalho apresenta uma integração das principais ferramentas de segurança de sistemas em software de código fonte aberto nas áreas de filtro de pacotes, detecção de intrusos, varredura de vulnerabilidades e monitoramento de servidores e serviços de rede que é representado pelos seguintes softwares respectivamente: *IPTABLES*, *NESSUS*, *NAGIOS* e o *SNORT*. Os softwares se integrarão a um sistema também em código fonte aberto focado no controle de requisições para reposta a incidente de segurança em computadores chamado RTIR.

5.1 IPTABLES

O *firewall* manipula os pacotes que passam entre as redes locais e a Internet. A partir desse princípio podemos aceitar, rejeitar ou descartar pacotes. Devidamente implementado, é capaz de prover segurança e aperfeiçoar o uso dos canais de comunicação, através de um método de controle de acesso baseado em regras registradas na tabela de filtro do *Kernel*.

No Linux, a filtragem de pacotes é implementada no *Kernel* pelos módulos do *Netfilter*, que são manipulados pelo *Iptables*.

O I*ptables* é o modulo responsável pela interface de configuração das regras do *netfilter*. Com ele pode-se editar as tabelas de filtragem de pacotes nativas do *kernel*. Essa filtragem ocorre na comparação entre os dados do cabeçalho (*header*) do pacote e as regras predefinidas. O I*ptables* trata os pacotes seguindo parâmetros das regras configuradas e pode executar três diferentes tipos de ação: Aceitar (*ACCEPT*), Descartar (*DROP*) ou Rejeitar (*REJECT*). Quando em uma regra se especifica que a ação será *ACCEPT*, o *netfilter* aceitará os pacotes que estiverem em conveniência a ela. Caso a ação especificada for *DROP,* o *netfilter* irá descartar todos os pacotes de dados que se encaixarem nessa regra. Caso seja especificada a ação *REJECT*, o *netfilter* rejeita todos os pacotes pertinentes à regra e enviará uma mensagem explicando o motivo da não aceitação dos mesmos. Existem outras ações como *REDIRECT*, *MIRROR* (experimental), *LOG*. As ações *DNAT*, *SNAT* e *MASQUERADE* são especificas da tabela Nat e seus significados serão relacionados mais adiante [9].

Existem várias características que definem o *Iptables*. São elas:

- Dar suporte aos protocolos TCP/UDP/ICMP;

- Podem ser especificadas portas de endereços de origem e destino;
- Rápido, estável e seguro;
- Dar suporte a módulo externos para aumentar suas funcionalidades;
- Possui mecanismos internos que bloqueiam pacotes do tipo fragmentados;
- Permite que se adicione um numero ilimitado de regras por cadeias;
- Suporte completo a roteamento de pacotes;
- Suporte à priorização de tráfego por tipos determinados de pacotes;
- Permite redirecionamento de portas.

A estrutura lógica do *Iptables* é formada basicamente por tabelas, *chains*, e regras. As regras devem ser definidas juntamente com as tabelas e *chains,* pois elas consistem em uma forma de organizar as informações que serão processadas pelo *netfilter. As características de cada tabela do Iptables* podem ser vistas na Tabela 1. Abaixo, será descrito o que cada uma delas representa:

- As tabelas servem para representar a descrição da área de atuação das regras. As tabelas existentes por padrão são: *filter*, Nat, e *mangle*. Entretanto, outras tabelas podem ser criadas.
- As *chains* representam as "cadeias" relacionadas ao tipo de roteamento do pacote dentro da máquina *firewall*. No I*ptables* existem *chains* especificas para cada tabela. A Tabela 1 mostra uma tabela de como as *chains* são organizadas.
- As regras são diretrizes que servem de base para que o netfilter possa determinar, considerando as informações do cabeçalho do pacote, a ação que deve ser tomada por ele. Tais regras se apresentam na forma: Tabela – Opção – Chain – Parâmetros – Ação.
  Exemplo: $iptables -A INPUT -p ALL -s 127.0.0.1 -i lo -j ACCEPT

Tabela 1 Estrutura de Tabelas no Iptables [9].

TABLE	CHAIN
Filter	INPUT
	FORWARD
	OUTPUT
nat	PREROUTING
	POSTROUTING
	OUTPUT

Na Figura 7 é ilustrado o esquema lógico do fluxo de pacotes dentro do *kernel* relacionadas à tabela *filter* no *Iptables*. Nela é possível se ter uma boa noção de como os pacotes são classificados pelo *netfilter*, para que ele possa efetuar corretamente o seu processamento. Os pacotes que chegam ao *kernel* são analisados para que se constate o tipo de roteamento a ser feito.

Caso sejam destinados ao próprio *firewall*, o *netfilter* analisa as regras de *chain INPUT* e depois os encaminha para serem processados pelo processo local. Caso destinem-se a outro *host*, o *netfilter* os compara às da *chain FORWARD* e após isso, os destinam ao *host* especificado. Caso os pacotes sejam originados pelo próprio *firewall*, o *netfilter* os submete às regras da *chain OUTPUT* e só assim, os libera para saírem da máquina. Um modelo de regra de firewall está disponível no anexo C.

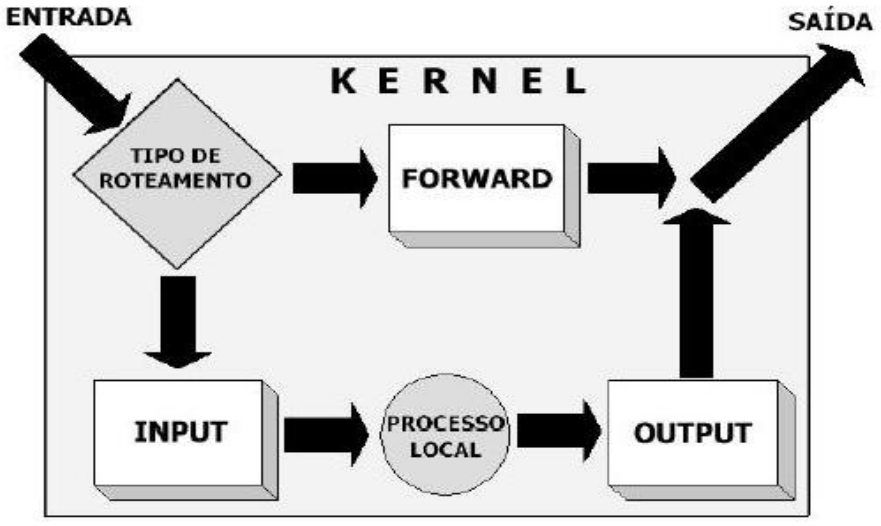

Figura 7. Fluxo de dados da tabela *filter* do *Iptables [9].*

5.2 Nessus

O *Nessus* é uma ferramenta de auditoria muito usada para detectar e indicar uma maneira de solucionar as possíveis vulnerabilidades encontradas nos computadores. Essa ferramenta era código aberto até a versão 2.2.8, e passou a ser código fechado, porém continua sendo uma ferramenta de uso gratuito e é distribuída através do site: <http://www.nessus.org>. Sua versão atual é a 3.2.

Seus recursos são muito avançados, e uma grande vantagem que possui em relação às outras ferramentas desse gênero, é que o *Nessus* varre todas as portas TCP´s detectando servidores ativos e simula invasões para identificar vulnerabilidades. Para executar as varreduras de portas, o *Nessus* utiliza o *Nmap*, um poderoso identificador de portas. Esta ferramenta possui uma facilidade que se refere ao usuário não precisa ter o servidor do *Nessus* instalado no seu computador, ou seja, precisa apenas do cliente instalado, pois ele permite a estrutura cliente-servidor para que vários pontos da rede possam ser analisados [10].

Nessa arquitetura, vários clientes podem controlar os servidores. Nesse sentido, a parte servidora executa os testes e a parte cliente configura e emite os relatórios. Ao término de uma varredura, são apontadas as

possíveis vulnerabilidades, e de uma maneira sucinta, é explicado de que forma o *host* pode ser atacado e como se proteger para corrigir essa vulnerabilidade. Além disso, nos relatórios de verificação são criados *links* para uma página específica de acordo com o *plugin* encontrado na vulnerabilidade, onde podemos encontrar mais detalhes sobre os riscos envolvidos, como o tipo de acesso (como exemplo: remoto), complexidade de ataque (indefinido, baixo ou alto), modo de autenticação (indefinido, requerido e não requerido), o impacto sobre a confidencialidade (indefinido, nenhum, parcial, completo), disponibilidade (indefinido, nenhum, parcial ou completo) e a integridade (nenhum, parcial e completo).

Esta ferramenta é eficiente na identificação dos serviços e sistemas rodando nos micros da rede. Características importantes da ferramenta: a facilidade de utilização, interface amigável, relatórios bem detalhados dos serviços rodando no computador, assim como procedimentos a serem realizados no caso de alguma vulnerabilidade ser detectada.

Como pontos negativos, um problema encontrado é que não é possível trocar endereço IP da máquina do atacante, possibilitando a identificação da origem da varredura. È uma restrição encontrada na ferramenta, foi a de que não é possível estipular um tempo de alternância entre as portas do computador alvo, podendo dessa forma a ferramenta ser detectada por *anti-portscanners*.

5.3 Snort

O *Snort* é um sistema de detecção de invasão baseado em rede (SDIR) de código fonte aberto, possuindo muitos recursos. Ele é *sniffer (*farejador de trafego de rede) que tem como diferencial a capacidade de inspecionar o *payload* do pacote, área que contém os dados do mesmo, fazendo os registros dos pacotes, além de detectar as invasões [11].

Fornecer funções de *sniffer* e registros de pacotes é a parte fundamental do *Snort*, sendo sua grande vantagem os recursos de detecção de invasão, que fazem a correspondência do conteúdo de cada pacote com as regra de invasão.

O *Snort* é um sistema avançado capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades e até avisar ao administrador do ambiente sobre o ataque [11]. Considera-se o *Snort* um SDI *ligthweight*, ou seja, ele pode ser colocado em funcionamento com muito pouco esforço tanto no sentido computacional quanto no sentido configuração e suporte. Uma característica marcante do *Snort* é a facilidade de criação de assinaturas de ataques. Profissionais da área de segurança da informação sabem da velocidade em que os eventos ocorrem no mundo virtual. A prontidão, exatidão e rapidez são assuntos essenciais em se tratando de segurança. Como o *Snort* é um sistema de código aberto e apresenta

linguagem fácil de criação de assinaturas, permite a pronta criação e adição de uma nova assinatura de ataque por parte do administrador [12].

A arquitetura do *Snort* é composta de 4 componentes básicos: o farejador, o pré-processador, o mecanismo de detecção e os *plugins* de saída. Em sua forma mais básica o *Snort* é um farejador de pacotes. Entretanto, ele é projetado para pegar pacotes e processá-los através do pré-processador e depois verificar esses pacotes com relação a uma série de regras. A Figura 8 oferece uma visão de alto nível da arquitetura do *Snort* [11].

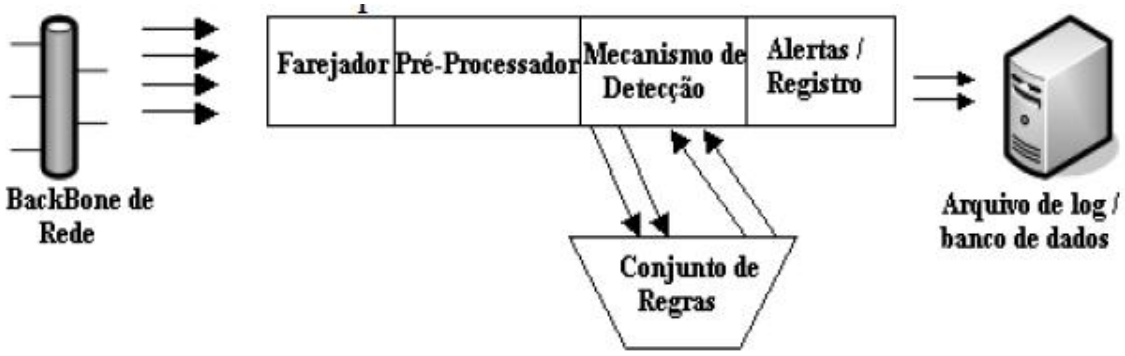

Figura 8. Arquitetura do *Snort* [11].

O *Snort* é uma ótima ferramenta, mas como todo aplicativo deve ser bem implementado. Devem ser aplicadas somente as assinaturas de ataques relevantes a realidade da rede. Por exemplo, não é necessário monitorar ataque a banco de dados *MySQL* se ele não se encontra em uso, o que ocasionaria apenas alertas irrelevantes. Além disso, o banco de assinaturas deve estar constantemente atualizado evitando assim que ataques passem despercebidos. O administrador tendo esses cuidados evita ou minimiza os falsos positivos e falsos negativos. O profissional responsável pela rede deve certificar-se que o sistema onde o *Snort* esta operando é o mais seguro possível, ou seja, deve-se esta atendo a segurança do sistema operacional onde o *Snort* esta rodando.

O *Snort* é um sistema que não requer recursos de hardware avançados. Os recursos de hardware necessário para o sistema operacional em uso atender ao *Snort*, recomenda-se duas interfaces de redes, uma para trabalhar em modo promíscuo, sendo o sensor do *Snort* e outra para conectividade de rede típica (SSH, serviços da Web etc.). As interfaces devem ser da velocidade máxima da rede, se a rede é 10/100 Mbps a interface deve ser de 100 Mbps. O *Snort* foi projetado para ser executado em uma grande gama de sistemas entre eles Linux, *FreeBSD*, *NetBSD*, *OpenBSD*, *Solaris*, *MacOS*, *Windows*, entre outros. Existe alguns programas

opcionais que podem ser instalados para melhorar/facilitar a administração do sistema. Citam-se os aplicativos para o mundo Linux. Os softwares são [11]:

- *MySQL*, para armazenamento dos alertas em banco de dados;
- *Guardian*, para leitura em tempo real dos *log* do *Snort*, e bloqueio via *firewall*;
- *Iptables*, para bloqueio de ataques;
- *Apache*, para disponibilização de informações via Web;
- *OpenSSH*, para acesso remoto;
- ACID (*Analysis Console for Intrusion Detection*), para apresentar de forma mais inteligível os *logs* do *Snort* armazenados em banco de dados.

5.4 Nagios

O *Nagios* é considerado uma das ferramentas mais poderosas para gerenciar uma rede de computadores. Através dele se consegue tirar relatórios de acesso, status das máquinas, problemas que podem estar ocorrendo na sua máquina antes que eles afetem gravemente o sistema, etc [13].

Através da configuração do *Nagios* para telefone celular se pode receber mensagens quando houver erros na rede como por exemplo, uma mensagem dizendo que o seu servidor de e-mails está com problemas.O *Nagios* é um aplicativo de monitoramento de sistemas e de redes. Ele verifica clientes e serviços, especificados pelo administrador, alertando quando as coisas estão indo mal ou se restabelecendo [14].

O *Nagios* foi originalmente desenhado para rodar no *Linux*, apesar dele poder funcionar na maioria dos sistemas operacionais *unix*.

5.4 1 Características

Algumas das várias ferramentas que o Nagios inclui:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING, etc.);
- Monitoramento dos recursos de clientes (carga de processador, uso de disco, etc.);
- Organização simples de *plugins* que permite aos usuários facilmente desenvolver seus próprios serviços de verificação;
- Verificação paralela de serviços;
- Habilidade para definir hierarquia de redes de clientes usando clientes pais (*parent hosts*), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis;
- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via *e-mail*, *pager*, ou métodos definidos pelo usuário);

- Habilidade para definir tratadores de eventos (*event handlers*) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas;
- Rotatividade automática de arquivos de *logs*;
- Interface web opcional para visualização do status atual da rede, histórico de notificações e problemas, arquivos de *log,* etc.

Na Figura 9 ilustra a interface do Nagios mostrando o diagrama da rede da EMPREL (Empresa Municipal de Informática).

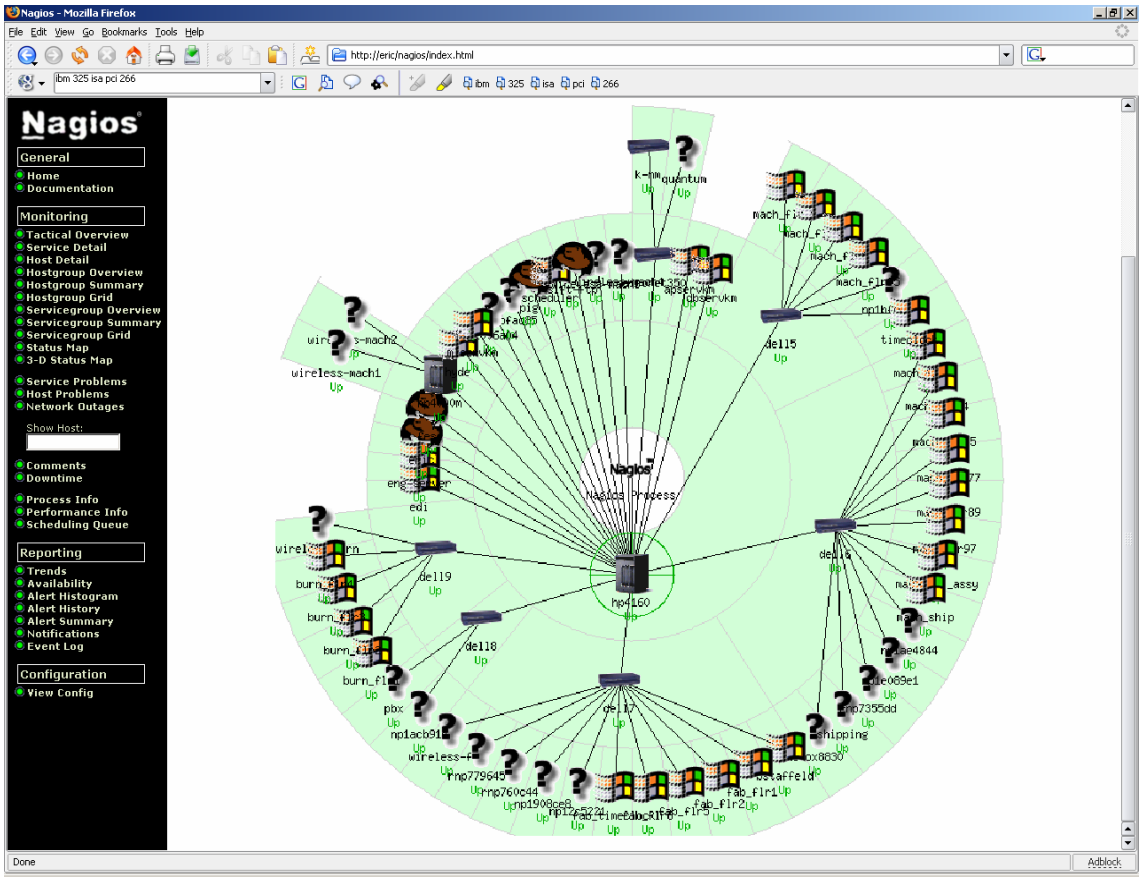

Figura 9. Diagrama de Rede EMPREL.

5.5 RTIR (Sistema de Controle de Requisição para Respostas Incidentes)

O sistema RT, do inglês *Request Tracker*, foi adotado neste trabalho porque é um sistema que possibilita o gerenciamento de tarefas, problemas e requisições por um grupo de pessoas, de forma inteligente e eficiente, submetidas por uma comunidade de usuários. Este sistema já está em desenvolvimento desde 1996, e é utilizado por administradores de sistemas, equipes de suporte a clientes, gerentes de TI e desenvolvedores em muitos lugares do mundo [6].

Escrito na linguagem orientada a objetos *Perl*, o RT é um sistema independente de plataforma que facilita a colaboração dentro de organizações, pois gerencia tarefas-chave como identificação, priorização, designação, resolução e notificação, que são fatores requeridos por aplicações de missão crítica dentro das organizações.

O RT foi criado pela empresa *Best Practical*. Esta empresa foi fundada para agregar valor à base instalada de usuários do RT, provendo desenvolvimentos específicos e suporte aos usuários do RT. Esta empresa está comprometida em fornecer suporte ao RT como uma tecnologia de código aberto, e ao mesmo tempo fornecendo qualidade no desenvolvimento e o suporte necessário para operações em organizações comerciais e corporações.

Como complemento do RT, para atender as necessidades dos grupos de resposta a incidentes, foi desenvolvido o RTIR, do inglês *Request Tracker for Incident Response*. O RTIR foi desenvolvido em cooperação com o grupo de resposta a incidente JANET (JANET é uma rede de educação e pesquisa no Reino Unido). Este grupo estava interessado no RT, mas precisava de mais algumas características especificas para resposta a incidentes [6].

A principal característica adicionada pelo RTIR após sua instalação é a criação de quatro filas(local onde se encontra os eventos específicos), dentro do RT, para o controle de incidentes. Estas filas são: *Incident Reports, Incidents, Investigations and Blocks*. Estas filas formam um pequeno fluxo que deve ser seguido durante a utilização do RTIR.

- **Incidents Reports** é a fila onde novos incidentes reportados devem aparecer. Quando um usuário envia uma mensagem de correio eletrônico, para o endereço configurado no sistema, reportando um incidente, um tíquete é criado nesta fila. A prioridade e o prazo deste tíquete podem ser ajustados automaticamente conforme as regras de nível de serviço da organização.

- Assim que um novo incidente reportado é considerado válido por algum membro do grupo, um tíquete pode ser criado na fila *Incidents* referenciado o incidente reportado. Ou o incidente reportado pode ser ligado a um tíquete já existente na fila *Incidents*. Se vários incidentes reportados são sobre o

mesmo problema ou assunto, todos estes incidentes reportados podem ser ligados a um incidente (tíquete na fila *Incidents*).

- Na fila ***Blocks*** são criados tíquetes para controlar os bloqueios feitos no *firewall* de uma rede. Estes tíquetes também podem ser criados a partir de tíquetes da fila *Incidents.*

- De um incidente existente, podem ser iniciadas investigações para entidades externas, com a criação de tíquetes na fila *Investigations*, pedindo a estas entidades que observem ou resolvam um determinado assunto ou problema.

5.6 Integração Das Ferramentas

O principal mecanismo utilizado para a integração das ferramentas de segurança com o sistema de controle de requisições são os envios de mensagens de correio eletrônico para o sistema RTIR. Na maioria dos casos são agendados roteiros no sistema operacional para que executem pequenos programas que fazem a análise dos registros destas ferramentas e quando concluída a análise, os relatórios gerados são enviados para o sistema de controle requisições através de mensagens de correio eletrônico para uma fila específica dentro deste sistema. No caso do sistema de monitoramento, toda vez que este detecta alguma falha em um servidor ou serviço monitorado, uma mensagem de correio eletrônico também é enviada para o sistema de controle de requisições para uma fila específica como pode ser observado na Figura 10.

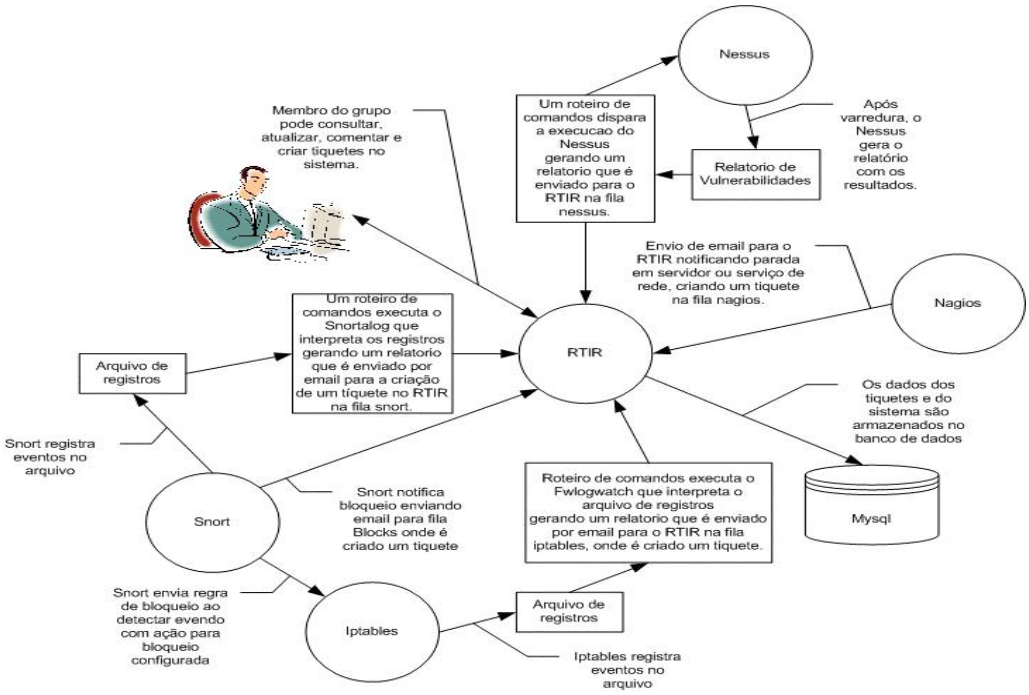

Figura 10. Troca de Mensagens e Processos Realizados para a integração [16].

O sistema atua de forma pró-ativa e reativa em relação ao tratamento dos eventos. Na forma pró-ativa, mostrada na Figura 11, atuam as ferramentas *Iptables*, *Nessus* e *Snort*, que ficam coletando informações importantes para o grupo de respostas e estas informações são inseridas no RTIR para tratamento pelos membros do grupo de respostas.

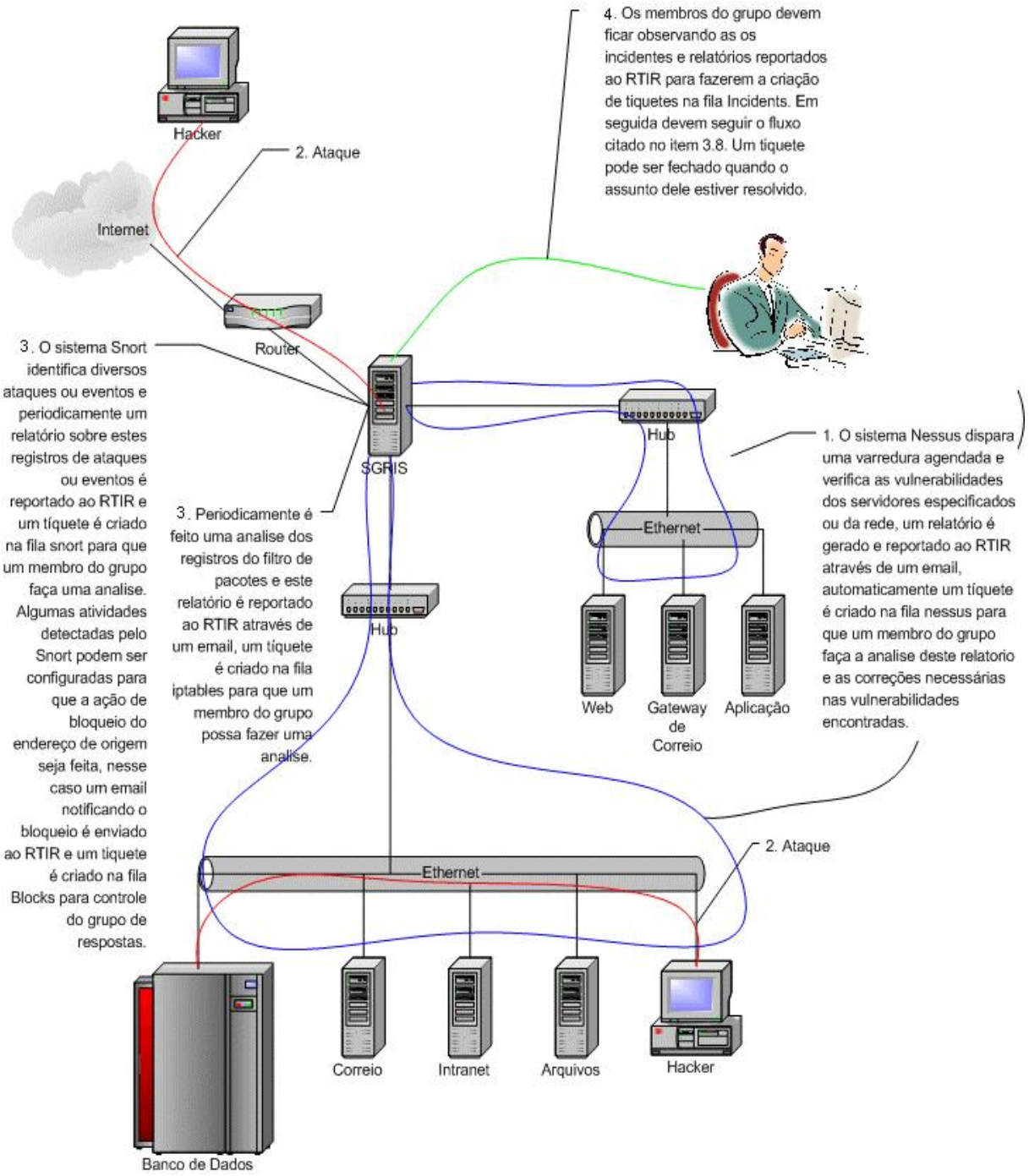

Figura 11. Situação Pró-Ativa de Utilização do sistema [16].

Na forma reativa apresentada na Figura 12, a ferramenta *Nagios*, quando detecta a parada de algum servidor ou serviço de rede, envia uma notificação através de uma mensagem de correio eletrônico para o sistema de controle de requisições. Nesta forma também se enquadram os problemas reportados por usuários através da criação de tíquetes na fila *Incindent Reports.* Estes tíquetes podem ser criados pelos usuários através do envio de mensagens de correio eletrônico para o RTIR ou através de sua interface utilizando um navegador Internet.

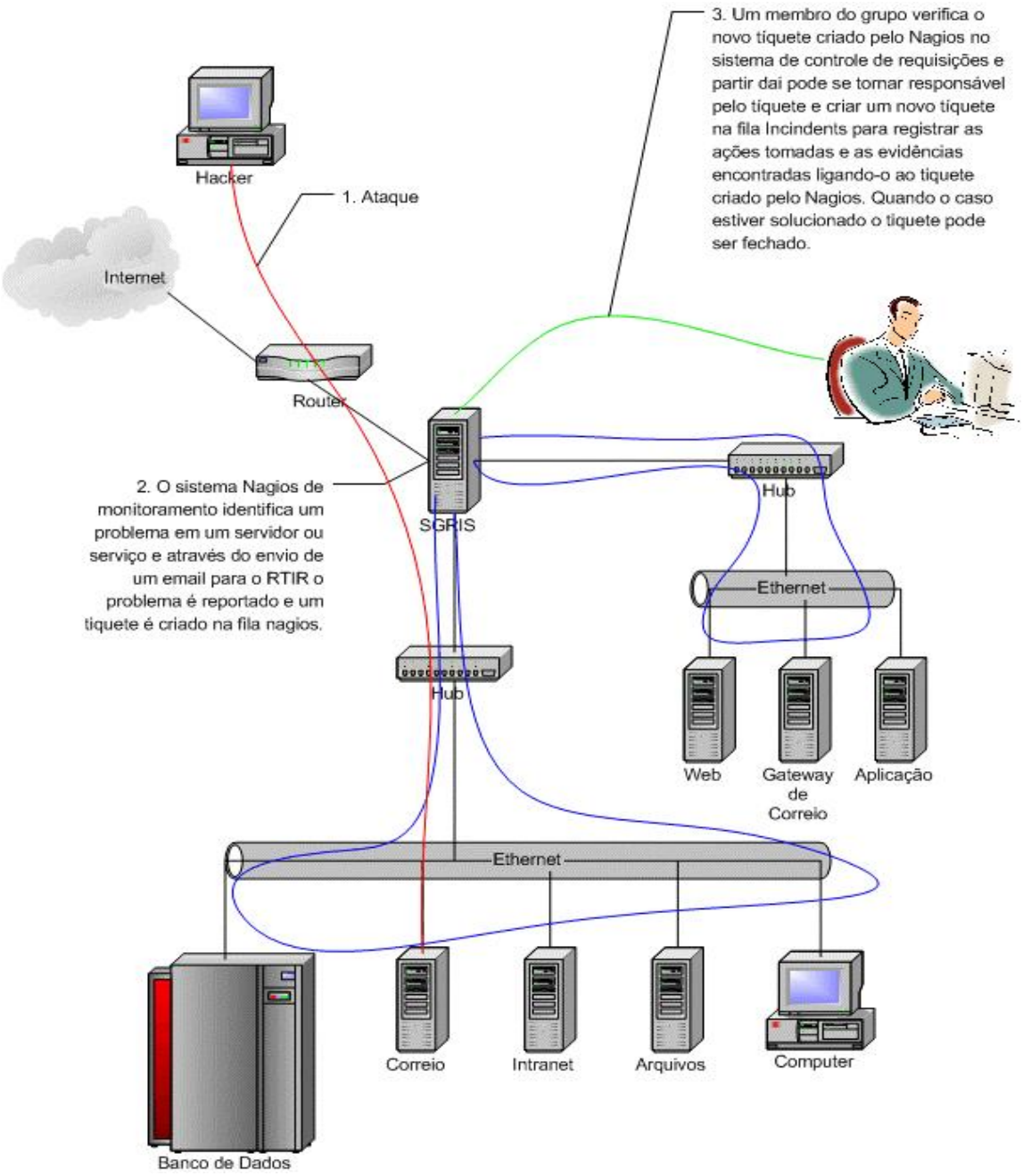

Figura 12. Situação Reativa de Utilização do Sistema [16].

5.6.1 Análise de Vulnerabilidade

Os relatórios de análises das vulnerabilidades são gerados pela ferramenta chamada de *Nessus*. Um roteiro no *Linux* fica agendado no sistema operacional para iniciar os testes e gerar um relatório que é enviado por correio eletrônico para o sistema de controle de requisições na fila *Nessus* onde é criado um tíquete. Sendo que os tíquetes criados nesta fila são classificados inicialmente de forma automática com uma prioridade média. Neste relatório são apresentadas informações como:

.

- Falhas, alertas e informações de segurança de rede para um ou mais endereços de Internet testados;
- O fator de risco das vulnerabilidades encontradas;
- Listagem das portas abertas em um endereço IP;
- Possível solução para correção da vulnerabilidade.

Nem sempre são encontradas falhas de segurança em um endereço *IP*, assim como nem sempre é dada uma solução pela ferramenta, nesses casos o responsável pelo sistema ou software deve procurar obter estas informações com especialistas de segurança do sistema ou software em questão ou com o fabricante do mesmo. Um modelo do relatório criado pela ferramenta *Nessus* pode ser consultado no anexo D.

5.6.2 Análise dos Registros de Eventos do Firewall

Através de um roteiro agendado no sistema operacional para executar o analisador de registros do *Iptables*, chamado de *Fwlogwatch*, determinadas vezes por dia ou por hora, conforme a necessidade do ambiente, um relatório é gerado e enviado por correio eletrônico ao sistema de controle de requisições para a fila *Iptables*, onde é criado um tíquete que é automaticamente classificado inicialmente com uma prioridade média, sendo que este relatório também pode ser disponibilizado em um endereço na rede que é informado no tíquete. Cada registro possui o número da regra do *firewall* que a registrou e qual ação foi tomada pelo *firewall*, o número de vezes que o registro ocorreu (número de pacotes), o endereço IP e porta de origem da conexão e o endereço IP e porta de destino da conexão.

Com estas informações podem ser realizadas pesquisas para determinar comportamentos de endereços específicos, também excluir falsos positivos e cruzar dados com outros relatórios. Um modelo do relatório criado pela ferramenta *Fwlogwatch* pode ser consultado no anexo E.

5.6 3 Análise dos Registros de Eventos do IDS

O detector de intrusos *Snort* está integrado ao sistema de controle de requisições através de um analisador de seus registros. Este analisador é um roteiro em linguagem *Perl* chamado de *Snortalog.* Ele fica agendado no sistema operacional para ser executada determinadas vezes por dia e depois de feita a análise, um relatório é gerado e enviado por correio eletrônico ao

sistema de controle de requisições para a fila *Snort*, nesta fila os tíquetes são classificados automaticamente com uma prioridade média. Nos relatórios do *Snortalog* podem ser observados dados estatísticos gerais e específicos dos eventos registrados, listados a seguir[15]:

- Dados estatísticos gerais

- Distribuição de eventos por hora;
- Distribuição de eventos por dia;
- Popularidade dos endereços de origem;
- Popularidade dos endereços de destino;
- Distribuição de eventos por porta de destino;
- Distribuição de eventos por protocolo;
- Distribuição de eventos por tipo de registro.

- Dados estatísticos específicos

- Eventos de um endereço IP para qualquer endereço utilizando o mesmo método;
- Eventos para um endereço IP de qualquer endereço utilizando o mesmo método;
- Eventos de um endereço para um endereço;
- Eventos para uma porta agrupados por ataque;
- Distribuição por modos de ataque;
- Distribuição por modos de classificação;
- Distribuição por de eventos por severidade;
- Eventos por hora.

5.6.4 Alertas do sistema de Monitoramento

O sistema de monitoramento *Nagios* está integrado ao sistema de controle de requisições de problemas através de notificações de problemas encontrados por ele em algum serviço de rede ou servidor, durante o monitoramento. Essas notificações são enviadas por mensagens de correio eletrônico para uma fila específica no sistema de controle de requisições, chamada de *Nagios*. Nesta fila os tíquetes são criados com uma prioridade alta, pois na maioria dos casos as notificações do *Nagios* são para problemas críticos como um serviço de rede que parou de funcionar ou um servidor que parou de responder a testes de envio e recebimento de pacotes de dados pela rede.

Além de serviços de rede, o *Nagios* pode monitorar também recursos de um servidor como espaço em disco, utilização de memória, utilização do processador e utilização da interface de rede. Porém neste trabalho a ferramenta está configurada para monitorar serviços TCP e a comunicação com servidores em rede.

5.6.4 Registro dos Casos no Sistema de Controle de Requisições

A criação e classificação de tíquetes no sistema podem ser feitas de forma manual por um membro do grupo de respostas, dessa maneira podem ser registrados incidentes do tipo: utilização imprópria de direitos garantidos a um usuário, uso indevido de recursos computacionais da empresa, cópias ilegais de programas ou informações por usuários e outros incidentes que possam violar as políticas de segurança ou uso aceitável.

Os acompanhamentos nos tíquetes abertos de forma automática, pelas ferramentas de segurança, devem ser registrados manualmente pelos membros do grupo de respostas. Nestes registros podem ser alterados dados como prioridade do tíquete, dono, fila e outras informações que o membro responsável por ele achar pertinente.

5.6.6 Classificação dos Tíquetes no Sistema de Requisições

O sistema de tíquetes adotado neste trabalho, conhecido como RT, utiliza o conceito de filas. A classificação dos tíquetes é inicialmente atribuída de forma automática conforme a fila em que é criado. Quando uma fila é criada dentro do sistema de tíquete é possível configurar a prioridade inicial dos tíquetes criados dentro dela.

A classificação da prioridade de um tíquete é dada por um valor inteiro, quanto mais alto este valor, maior a prioridade do tíquete. Neste trabalho foi adotada uma escala de valores para definição das classificações. Se um tíquete possuir um valor de prioridade entre zero e trinta a classificação é baixa, se o valor estiver entre o intervalo de 31 a 60, então a classificação é média. Se estiver entre 61 e 90 a classificação é alta e de 91 a 100 é muito alta a classificação. Os membros do grupo devem dar mais atenção e tentar responder mais rapidamente aos incidentes com maior prioridade, sempre buscando a resolução dos tíquetes mais antigos.

Um membro do grupo pode alterar a prioridade de um tíquete se achar necessário. Essa alteração fica registrada no tíquete indicando qual foi o usuário que a realizou, assim como a data e o horário.

5.6.7 Utilização do sistema de Requisição pelos Membros do Grupo de Respostas a Incidentes

O sistema de tíquetes ou controle de requisições pode ser acessado através de um navegador em uma estação da rede privada da organização ou da rede pública se este acesso for liberado no *firewall*. Os tíquetes podem ser criados através do envio de mensagens de correio eletrônico pelos usuários do sistema para um endereço definido previamente. Assim como o acesso ao sistema os tíquetes podem ser feito da rede pública, também podem ser criados tíquetes a partir desta rede desde que o sistema de correio eletrônico esteja configurado para aceitar estas mensagens. Neste caso é importante que o sistema de correio eletrônico verifique a veracidade destas mensagens de alguma forma, podendo ser através de configurações específicas do

sistema de correio utilizado ou da utilização de algum sistema anti-spam. Neste trabalho esta sendo utilizado o sistema de correio eletrônico *Postfix*.

Em uma corporação que esteja utilizando o sistema descrito neste trabalho, os membros do grupo podem estar observando o sistema regularmente com o objetivo de estarem sempre dando o tratamento adequado aos tíquetes abertos no RT.

Além das filas criadas pelo RTIR, foram criadas mais quatro filas, uma para cada ferramenta, onde são reportados os relatórios de analises de seus respectivos registros de eventos e notificações.

A fila *Nagios* recebe as notificações da ferramenta de monitoramento *Nagios*, nesta fila os tíquetes são criados com uma prioridade alta devido ao fato de que as notificações enviadas por esta ferramenta informam problemas de paradas em servidores ou serviços que estão sendo monitorados. Dentro do tíquete criado está às informações do problema detectado como nome do servidor ou serviço, endereço de rede, comando utilizado para realizar o teste, tipo da notificação, date e horário da notificação. Os membros do grupo devem estar atentos a esta fila, pois geralmente os tíquetes criados nesta fila são incidentes.

Para a ferramenta *Nessus* foi criada a fila *Nessus*, nesta fila são criados tíquetes com prioridade média, os tíquetes criados nesta fila apresentam o relatório de vulnerabilidades encontradas nos servidores testados pelo *Nessus*. Os membros do grupo devem observar estes tíquetes e corrigir as vulnerabilidades apresentadas nos relatórios de vulnerabilidades contidos neles. Um tíquete criado na fila *Incidents* para um servidor ou serviço pode estar ligado a um tíquete criado na fila *Nessus*, se o servidor ou serviço apresentar alguma vulnerabilidade no relatório.

O *Iptables* tem a análise de seus registros de eventos enviados para a fila *Iptables*, conseqüentemente os tíquetes abertos nestas filas possuem informações dos eventos mais freqüentes registrados pelo *Iptables*. Os tíquetes desta fila têm uma prioridade média e devem ser freqüentemente observados pelos membros do grupo, pois se estes tíquetes apresentarem informações que um membro do grupo observar como um incidente, então um tíquete pode ser criado na fila *Incindents* e ligado ao tíquete da fila *Iptables* no qual foi observado o incidente.

O detector de intrusões *Snort* também tem uma análise de seus registros que é enviada para fila que foi criada com o nome de *Snort*. Os membros do grupo devem analisar freqüentemente os tíquetes criados nesta fila, que possuem uma prioridade média. Com base nas informações do relatório contido no tíquete, pode ser criado um tíquete de incidente na fila *Incindents*.

Qualquer membro do grupo de reposta a incidentes de segurança pode criar um tíquete de incidente na fila *Incidents* quando achar necessário, este tíquete pode estar ligado a outro tíquete das filas *Nagios, Nessus, Snort, Iptables e Incident Reports*. O membro que estiver abrindo já pode dar continuação ou designar o tíquete para que outro membro do grupo dê continuidade ao fluxo de resposta a incidente para o tíquete. Os usuários de uma rede em uma organização também podem ter permissão no sistema

RTIR para criar tíquetes na fila *Incident Reports*, bem como podem ter permissão para acompanhar os registros feitos no tíquete e também registrar comentários nele. Quando um registro é feito em um tíquete, os dados contidos nele podem ser enviados para o requisitante logo após que o registro foi concluído.

As principais vantagens encontradas na utilização deste sistema são o registro constante das informações de segurança em um sistema centralizado que disponibiliza fácil consulta a estas informações contidas nos tíquetes como o histórico dos eventos e assuntos registrados. O fluxo proposto também agiliza e organiza o processo de reposta a incidentes, mas é de extrema importância que os membros do grupo tenham a responsabilidade de seguir o mesmo.

Capitulo 6

Cenários de Uso

6.1 Descrição dos ambientes de Teste

No ambiente de teste foi usado o *software Vmware* para emular a rede de teste. Ele permite a emulação de vários sistemas operacionais ao mesmo tempo sobre um sistema *host*, utilizando para isto o conceito de máquinas virtuais. Cada máquina virtual funciona como um micro inteiro, contendo processador, memória, disco, vídeo, som, porém tudo sendo emulado pelo *VMware*. Uma máquina virtual pode ainda usar, de forma simultânea com o sistema *host*, as unidades de disquete e CD-ROM. Quando falamos de "sistema *host*", queremos nos referenciar ao micro físico que possui seu próprio sistema operacional e que serve de base para a instalação do *VMware*. Outro ponto muito interessante é a possibilidade de ligação entre o sistema *host* e todas as máquinas virtuais como se estivessem numa rede tradicional sendo cada qual com seu endereço IP.

Nesse ambiente virtual foram utilizadas 3 maquinas virtuais, uma para servir como *gateway* da rede contendo *firewall, Nagios e Snort*, outra será onde o RTIR será instalado justamente com *Nessus* e por fim outra simulando um micro atacante, ou seja, um micro com intenção de invadir a rede simulada.

Porém esta não é a prática mais indicada e só foi utilizada com fins de testes de funcionalidade e análises de funcionamento para definição de uma forma de utilização dos recursos disponibilizados, pois o recomendado é que no *gateway* da rede esteja configurado apenas o *firewall* e em alguns casos um sensor de IDS também. As demais ferramentas podem ser distribuídas em pelo menos mais duas máquinas que estariam localizadas na rede interna ou privada. Outra recomendação seria a utilização de criptografia na troca das mensagens, mas não foi empregada nesta pesquisa pela limitação de tempo e pela complexidade das outras tarefas executadas e desta também, o que poderia inviabilizar a conclusão deste trabalho.

A seguir serão apresentados os programas e os equipamentos utilizados no desenvolvimento deste trabalho.

6.1.1 Programas

Os seguintes programas foram utilizados no servidor *gateway* e no servidor de aplicação com RTIR para a elaboração dos testes:

- Sistema operacional: *Debian Etch* 4.0 r4

- Sistema de detecção de intrusos: *Snort* 2.3.3
- Sistema de varredura de vulnerabilidades: *Nessus* 2.2.8
- Sistema de monitoramento: *Nagios* 3.0.2
- Sistema de controle de requisições: RT 3.8.1 com RTIR 2.4.0
- Sistema de banco de dados: *MySQL* 5.0
- Servidor HTTP: *Apache* 2.0.47
- Interpretador de comando *Perl* 5.8.3 e linguagem PHP 5.0
- Analisador de registros para *Snort*: *Snortalog* 2.4.2
- Analisador de registros para *Iptables*: *Fwlogwatch* 1.0
- Virtualização dos Servidores: *VMware Workstation* 6.0.0 *build* 47731
- Servidor de *E-mail*: *Postfix* 2.3.8

Na estação de trabalho foram utilizados o sistema operacional *Windows* 2000 *professional* com *Service Pack* 4 e os serviços de acesso remoto SSH e o *portscan nmap*. É importante observar que por motivos de facilidade de instalação, facilidade de integração com os sistemas utilizados e limitação de tempo foi utilizado o banco de dados *MySQL* 5.0, mas outros bancos mais robustos e mais seguros como *Postgresql* e *Oracle* também poderiam ser utilizados para a mesma finalidade.

6.1.2 Equipamentos

O ambiente formado para os testes e a execução da integração das ferramentas ao sistema de controle de requisições não é o ambiente ideal, pois quase todas as ferramentas estão sendo executadas no mesmo servidor, o que em certos momentos causa sobrecarga de processamento e muita utilização de memória.

Ao todo o ambiente ficou simples, devido à pequena quantidade de serviços e servidores monitorados, apesar desta característica do ambiente, mesmo assim foi possível verificar as funcionalidades das ferramentas utilizadas e os resultados da integração.

- Servidor *Gateway* Com *Firewall*, *Snort* e *Nagios* (Virtualizado)

Processador: *Celeron* M 1.6Ghz
Memória RAM: 128 MB
Disco Rigido: 8GB SCSI
(2) Interface de Rede *FastEthernet* 10/100 Mbps/s
Sistema Operacional: *Linux Debian* 4 r4

- Servidor de Aplicação Com RTIR e *Nessus* (Virtualizado)

Processador: *Celeron* M 1.6Ghz
Memória RAM: 256 MB
Disco Rigido: 8GB SCSI
1 Interface de Rede *FastEthernet* 10/100 Mbps/s
Sistema Operacional: *Linux* Debian 4 r4

- Maquina para Simular ataques (Virtualizada)

Processador: *Celeron* M 1.6Ghz
Memória RAM: 256 MB
Disco Rigido : 8Gb SCSI
1 Interface de Rede *FastEthernet* 10/100 Mbps/s
Sistema Operacional: *Windows* 2000 Professional SP4

O ideal para que esta solução seja implantada em um ambiente corporativo seria a utilização de pelo menos três servidores como o descrito acima para distribuir os serviços. Podendo ser um deles *firewall* e IDS; outro seria utilizado para fazer a varredura de vulnerabilidades, hospedarem o sistema de requisições e o banco de dados; e o terceiro seria utilizado para fazer o monitoramento dos servidores e serviços de rede.

6.1.3 Topologias

Abaixo na Figura 13 pode ser observada a topologia utilizada para o ambiente de desenvolvimento e testes.

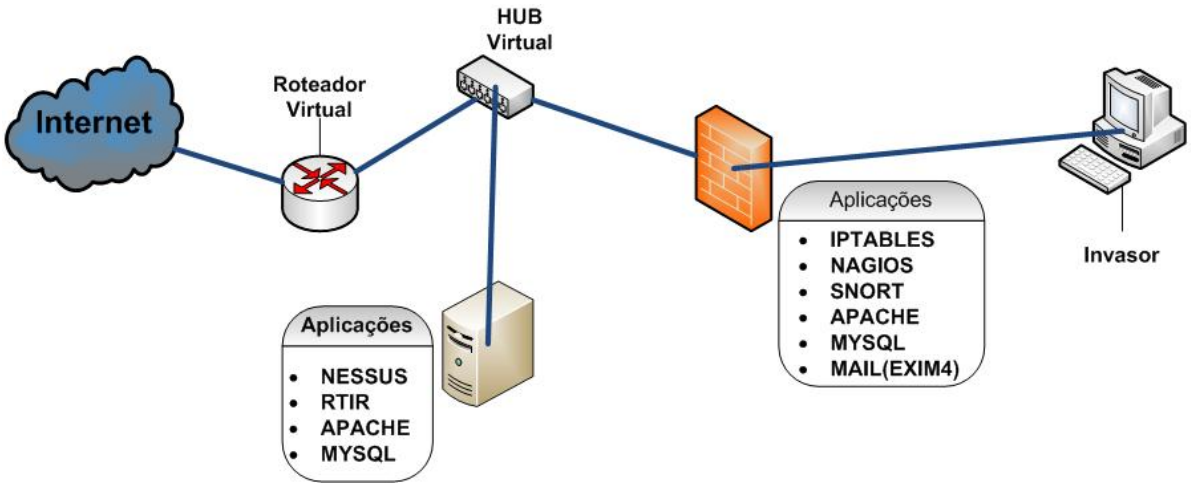

Figura 13. Topologia Utilizada nos Testes.

Abaixo na Figura 14, mostra a topologia ideal para o ambiente corporativo, visualizando a forma ideal de colocar os IDS na rede corporativa, um observando as conexões de acesso externo e o outro vasculhando a rede interna. O ideal é que numa rede corporativa tenha uma máquina fazendo cada função, ou seja, vasculhando, detectando e bloqueando situações indevidas que ocorre no ambiente, isso porque cada ferramenta ao ser ativada requer um considerável recurso de hardware para fazer sua função.

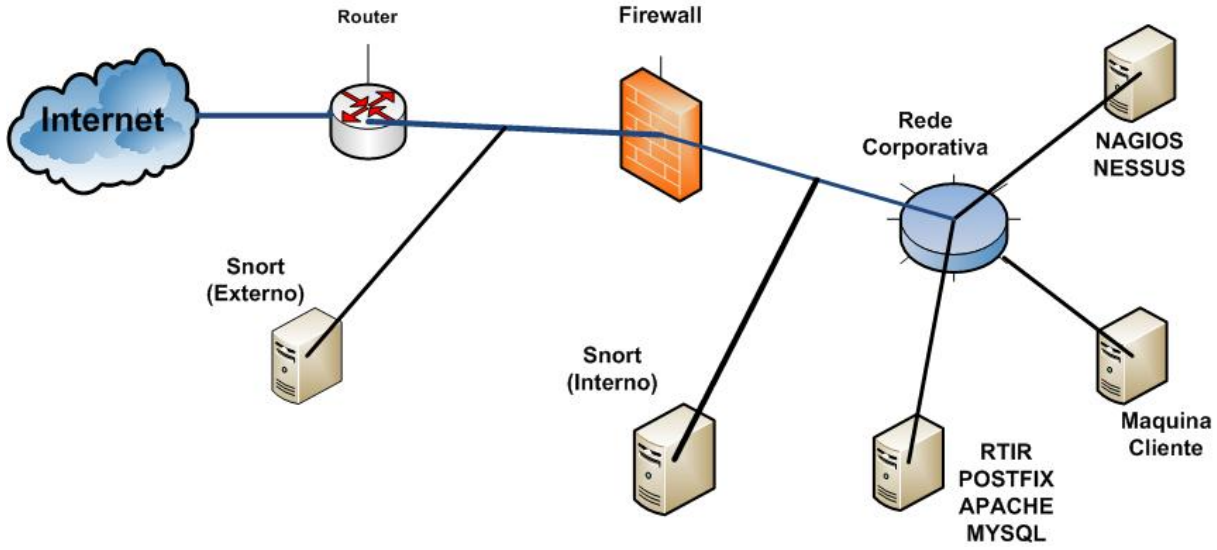

Figura 14. Topologia sugerida para utilização nas Corporações.

6.2 Cenários

Nessa seção serão descritos 5 cenários para demonstrar o funcionamento da ferramenta de detecção de intrusos, filtro de pacotes, varredura de vulnerabilidades e monitoramento de serviços e servidores integrado ao sistema de requisições.

6.2.1 Cenário 1 – Incidentes reportados por usuários

Neste cenário é simulada a criação de um tíquete por um usuário na fila *Incident Report*, onde o mesmo reporta um incidente ocorrido em sua estação de trabalho. Este incidente consiste na contaminação da estação do usuário por um vírus, onde o usuário ficou sabendo desta informação porque foi alertado pelo sistema antivírus instalado em sua estação.

1. Usuário envia uma mensagem de correio eletrônico para o endereço que aponta para a fila *Incident Report ou entra na pagina do RTIR via web,* nesta mensagem ele informa que recebeu uma notificação do sistema antivírus instalado em sua maquina, informando que a estação esta infectada por um determinado vírus.

2. Um membro do grupo se apropria do tíquete criado pelo usuário na fila *Incident Reports* e cria um novo tíquete ligado a este na fila *Incident*.

3. É passado para o usuário através de registro no tíquete, feito pelo membro do grupo, o procedimento que deve ser seguido para a remoção deste vírus utilizando a ferramenta antivírus que está instalada na estação do usuário.

4. O usuário pode comentar o tíquete do incidente através da interface do RTIR ou informar o membro do grupo que a remoção do vírus foi feita com sucesso.

5. O membro do grupo poderia abrir um tíquete na fila *Investigations*, caso fosse necessário investigar o motivo pela qual a máquina foi infectada e registrar neste tíquete os resultados da investigação.

6. O membro do grupo então muda o estado dos dois tíquetes criados neste caso para resolvido.

Na Figura 15 é mostrada uma tela de abertura de chamado do usuário na fila de *Incident Report,* com isso o usuário fica aguardando a resposta do tíquete que ele criou.

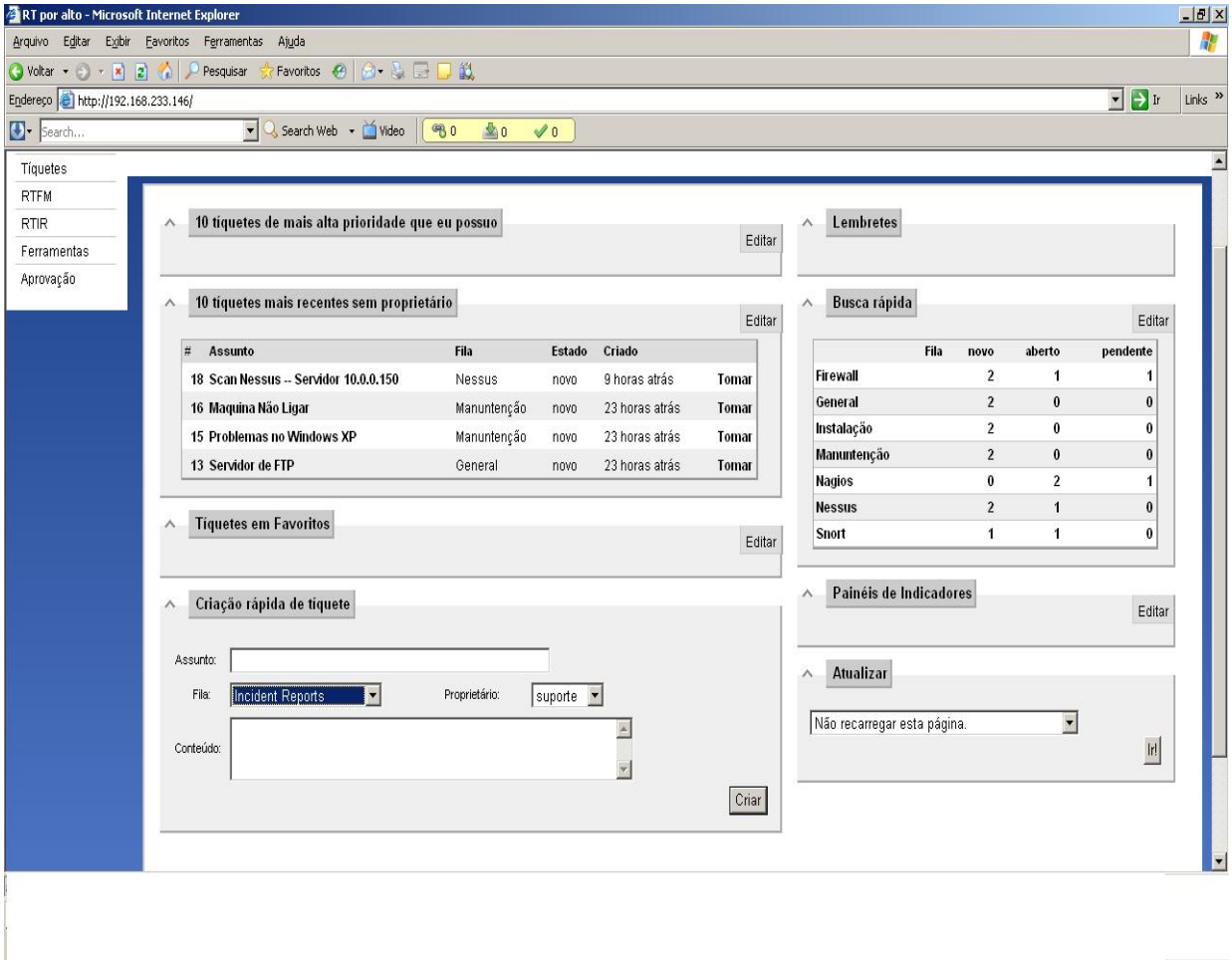

Figura 15. Criação Manual de tíquete na fila *Incidents Report* pelo Usuário.

6.2.2 Cenário 2 - Notificação de Parada de Servidor ou Serviço pelo Nagios

Este cenário apresenta a simulação de uma parada no Servidor de DNS para que o *Nagios* identifique o problema e envie uma mensagem de correio eletrônico para um endereço que aponta para a fila *Nagios* dentro do RTIR.

1. O serviço DNS é desligado propositalmente, simulando a sua falha.

2. O *Nagios* identifica o problema da falha do servidor e após três verificações indicando que a conexão foi recusada. Depois ele inicia o processo de notificação enviando uma mensagem de correio eletrônico para o responsável pela administração do servidor e outro para o endereço que aponta para a fila *Nagios* dentro do RTIR e nesta fila é criado um tíquete.

3. Um membro do grupo que está observando o sistema RTIR, verifica que um novo tíquete foi criado na fila *Nagios* e se apropria do tíquete.

4. O membro do grupo então entra em contato com o administrador do servidor e o mesmo informa que já está ciente do problema, pois já foi notificada pelo *Nagios*, e já esta solucionando o problema que ocorreu devido a uma falha na rede elétrica da sala dos servidores.

5. O membro do grupo abre um tíquete na fila *Incindent* ligado ao tíquete criado na fila *Nagios* e registra neste tíquete as informações passadas pelo administrador, como mostra a Figuras 16.

6. A equipe da elétrica troca a régua que estava em curto e liga o servidor que volta a funcionar normalmente.

7. O *Nagios* identifica a recuperação do servidor e envia uma notificação para o administrador e para o RTIR na fila *Nagios*, informando que o servidor voltou a funcionar.

8. O membro do grupo que está aguardando a criação do tíquete de *Recovery* que deve ser enviado pelo Nagios percebe que o mesmo foi criado e então ele se apropria deste tíquete, faz a ligação dele com o tíquete da fila *Incident* que referencia o problema e muda o estado destes três tíquetes para resolvido. Um exemplo de um destes tíquetes é mostrado na Figura 17.

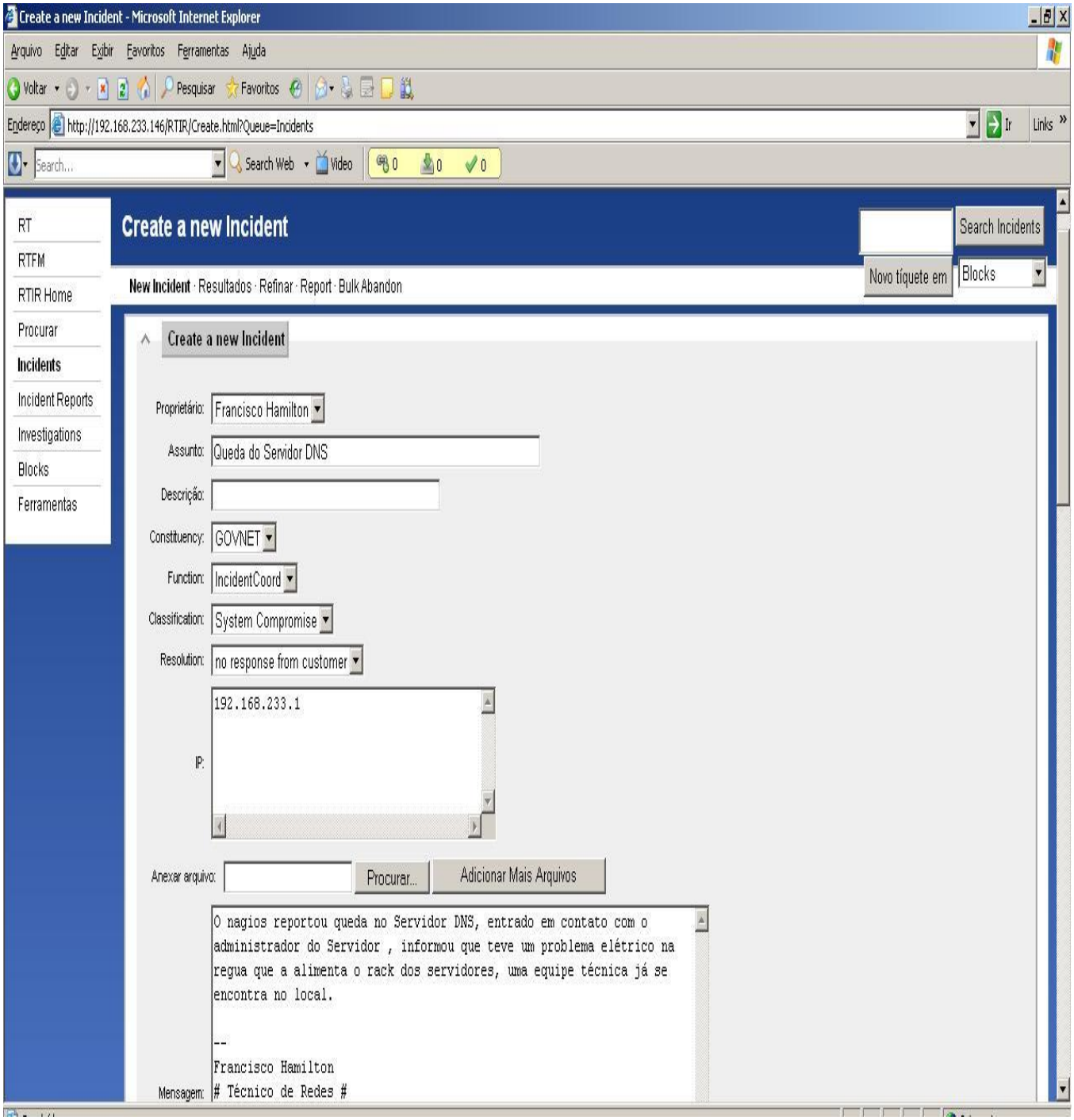

Figura 16. Criação do Tíquete na Fila *Incidents* e Criando o Vinculo.

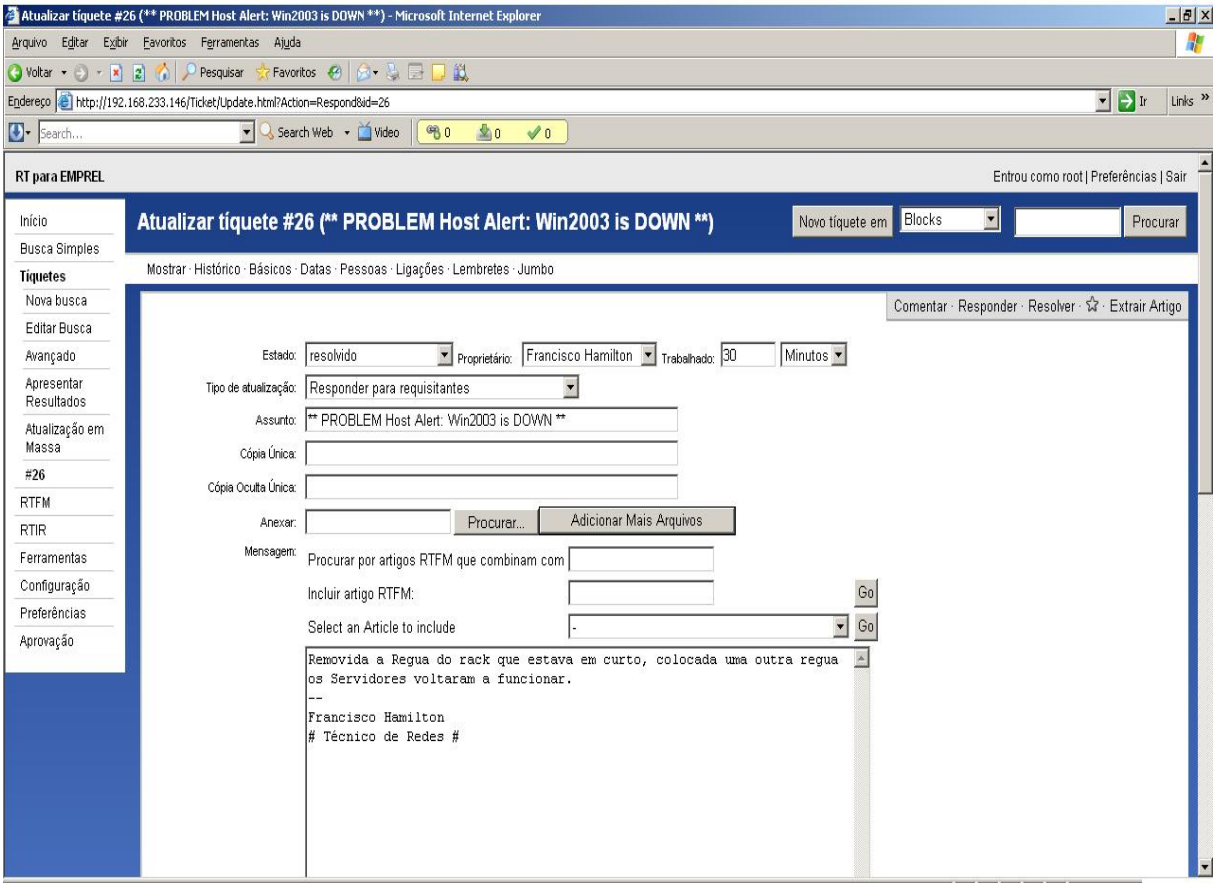

Figura 17. Resolução do tíquete para problema do Servidor DNS

O resultado deste teste foi satisfatório uma vez que o sistema cumpriu com as tarefas propostas, fazendo as notificações e criando o tíquete para o problema dentro do sistema. Os passos descritos acima ocorreram sem problemas.

6.2.3 Cenário 3 – Análise de um relatório de registro do Nessus com Vulnerabilidades

Neste cenário é demonstrada uma atividade diária de um membro do grupo de respostas onde o mesmo tem que se apropriar de um tíquete criado na fila *Nessus* e verificar se alguma vulnerabilidade critica foi apresentada no relatório. Caso alguma vulnerabilidade critica foi realmente encontrada, o membro do grupo deve seguir o fluxo de abrir um tíquete na fila *incidents*. Caso não exista vulnerabilidade crítica no relatório o tíquete deve ter seu estado alterado para resolvido e o membro do grupo deve registrar no tíquete que nenhuma atividade anormal foi encontrada.

1. Um membro do grupo de resposta a incidentes se apropria de um tíquete mais antigo da fila *Nessus*.
2. O membro identifica uma vulnerabilidade crítica no relatório e cria um novo tíquete na fila *Incidents* ligado ao tíquete criado na fila *Nessus*.
3. O próximo passo do membro do grupo pode ser iniciar uma busca para resolver o problema da vulnerabilidade encontrada, abrir uma investigação para ter mais informações sobre essa brecha de segurança, para isso ele deve criar um tíquete na fila *Investigations* ligado ao tíquete criado no passo anterior na fila *Incidents*. Neste tíquete devem ser registradas as informações obtidas sobre a vulnerabilidade encontrada na Figura 18 mostra um exemplo de uma abertura de investigação sobre a vulnerabilidade.
4. Uma vez concluída a investigação o membro do grupo deve registrar as ações tomadas, que podem ser, por exemplo: atualização de uma determinada aplicação instalada no servidor para uma versão mais nova, aplicar um *patch* de segurança do fabricante da aplicação ou mesmo a reconfiguração do aplicativo.
5. Então depois de tomadas as devidas ações, estes tíquetes devem ter seus estados alterados para resolvido.

Durante a realização deste cenário, foram realmente encontrados tíquetes criados na fila *Nessus*, que foram enviados pelo roteiro encarregado desta tarefa, com registros das vulnerabilidades críticas como por exemplo, servidor web instalado na versão antiga com várias brechas propícias ao ataque. Os passos descritos acima foram seguidos sem problemas. Este cenário é muito semelhante à atividade de análise de um relatório de registros do *Iptables* e do *Snort*.

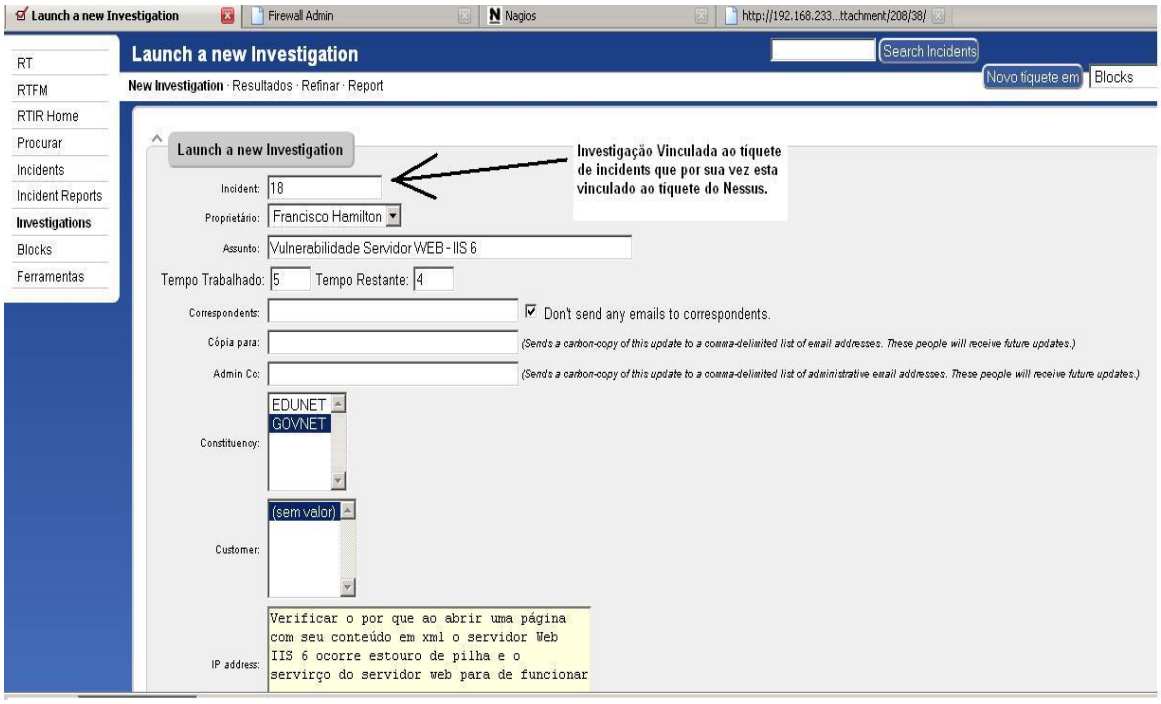

Figura 18. Abertura de Investigação sobre a vulnerabilidade

6.2.4 Cenário 4 – Construindo uma Base de Conhecimento com Artigos

Toda empresa precisa de uma base de dados, ou seja, ter uma base de conhecimentos aprofundada sobre determinado assunto. Essas informações podem ser utilizadas na solução de problemas que venha ocorrer, com isso temos aumento da velocidade de acesso ás informações, diminuição do tempo de resposta para usuários da rede em questão e facilidade de gerenciamento de conteúdo devido á estrutura simples e padronizada de arquivamento. Neste cenário é mostrado como inserir um artigo no RTIR e depois vincular esse artigo a uma determinada vulnerabilidade encontrada, tipo de ataque desconhecido ou um incidente que foi resolvido através de uma solução de outro administrador.

1. Um membro do grupo de resposta a incidentes detectou na fila do *Nessus* um tíquete que informava que o servidor de arquivos possui uma falha de segurança

2. Verificou-se que o servidor de arquivos possui uma vulnerabilidade que permitia acesso não autorizado a pastas de outros usuários.

3. O próximo passo do membro do grupo pode ser iniciar uma busca para resolver o problema da vulnerabilidade encontrada, e criar um tíquete na fila *Incidents* vinculado ao tíquete que informa a falha de segurança. Neste tíquete devem ser registradas as informações obtidas sobre a vulnerabilidade encontrada

4. Mediante pesquisa o membro conseguiu resolver o problema da vulnerabilidade, depois resolveu compartilhar a solução encontrada com o restante do grupo criando um artigo no RTIR e vincular esse artigo ao incidente reportado e solucionado. Na Figura 19 mostra como criar um artigo e vinculá-lo.

Durante a realização deste cenário, foi encontrado um tíquete na fila *Nessus* que informava essa vulnerabilidade. Ao encontrar a solução o membro pode criar artigos e vincular a esse incidente ou mesmo criar artigos aleatórios sem vínculos, apenas para ajudar na solução de futuros problemas

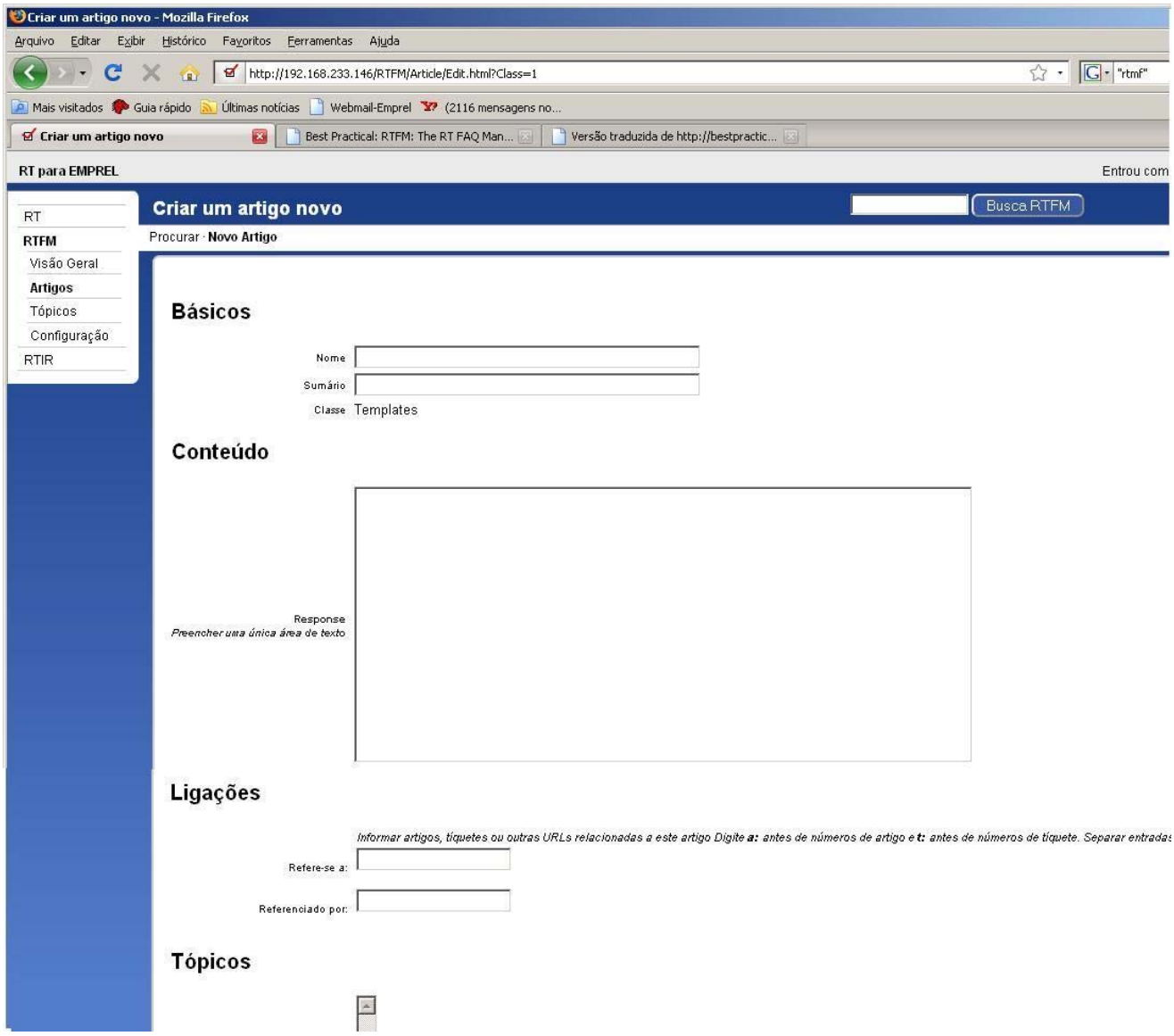

Figura 19. Criação de um Artigo

Capitulo 7

Conclusões e Contribuições

Este trabalho teve como intuito mostrar a eficiência e uma forma pratica de automatizar o processo de respostas a incidente de segurança em redes de computadores utilizando ferramentas de código aberto que rodam em sistema operacional *open souce* (*Linux*). Foi feita um estudo aprofundado na ferramenta RTIR (*Request Tracker for Incident Responce*) com a montagem de uma estrutura e configuração de rede em cima dessa ferramenta de código aberto.

7.1 Contribuições

O estudo de caso realizado sobre a ferramenta RTIR mostrou ser possível identificar uma forma de automatizar o processo de respostas a incidente de redes de computadores de uma maneira rápida e eficiente. Porém para se ter uma eficiência de uma resposta a um incidente de segurança vai depender do grupo de resposta a incidente de segurança em computadores. Com o sistema em pleno funcionamento será mais fácil de gerenciar a resposta a incidente e com o armazenamento destas informações uma base de conhecimento é construída, que pode servir como referência para futuros incidentes.

Com as informações armazenadas também poderão ser elaborados relatórios com dados estatísticos que podem ser utilizados como fonte de pesquisa para o planejamento de atividades pró-ativas pelo grupo de respostas a incidentes de segurança em computadores. À medida que elementos novos e desconhecidos forem surgindo no ambiente das redes de computadores, o RTIR possui um modulo onde poderemos vincular um artigo sobre um determinado ataque, falha de segurança ou o surgimento de um novo vírus, a um tíquete criado em uma determinada fila. Com isso quando um membro do grupo de resposta a incidente for verificar como foi resolvido um problema, ele pode ter uma base teórica e técnica do problema ocorrido.

7.2 Dificuldades

Nesse trabalho uma das dificuldades encontradas foi à instalação do software RTIR. Por ser escrito na linguagem orientada a objetos *Perl* o

sistema operacional em que ele estiver instalado tem que ter todos os módulos *Perl* necessários para o correto funcionamento do sistema. Apos resolvidos todas as pendências do sistema surgiu um dos principais problemas que é a correta classificação das filas que recebe os relatórios de incidentes de segurança uma vez que um ataque pode ser feito de diversas maneiras utilizando diversas de técnicas de invasão o que dificulta sua classificação. A princípio foi dada uma classificação inicial as filas que podem ser alteradas a qualquer momento, esse classificação pode ter uma importância grande ou pequena que quando for montada o ambiente de resposta a incidente se faz necessário a presença e análise de um especialista de segurança de rede para correta classificação.

7.3 Trabalhos Futuros

Em trabalhos futuros seria interessante a presença de criptografia no acesso a pagina de gerenciamento do RTIR e no envio de relatório das ferramentas de segurança. Outro ponto importante seria a implementação do módulo *SnortSam* acoplado ao *Snort* esse módulo tem como principal função de ao detectar uma invasão ou mesmo um acesso indevido de uma rede estranha ele adicionar uma regra de bloqueio no *firewall* impedindo o acesso do invasor ao ambiente de rede e se o *Snort* estiver devidamente configurado ele pode gera um relatório e enviar para fila de *Blocks* do RTIR com isso um membro do grupo de resposta a incidente de redes se apropria desse tíquete e observa se o bloqueio foi coerente com as regras de acesso, caso positivo ele troca o status do tíquete para resolvido.

Bibliografia

[1] NAKAMURA, Emilio; GEUS, Paulo**. Segurança de Redes: Em Ambientes Corporativos**: Berkeley, 2002.

[2] **CERT (Centro de Estudos, Respostas e Tratamento de incidentes de Segurança no Brasil)**. Disponível em: <http://www.cert.br/> Acesso em: 30 de outubro de 2008.

[3] STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas:** Pearson, 2007.

[4] SCHWEITZER, Douglas. **Incident Response: Computer Forensics Toolkit:** Wiley, 2003.

[5] NETO, Urubatan**. Dominando Linux Firewall IPTABLES**, Ciência Moderna, 2004.

[6] **Best Practical (RT-Request Tracker)**. Disponível em: <http://bestpractical.com/> Acesso em: 30 de outubro de 2008.

[7] SCHULTZ, Dr. Eugene; SHUMWAY, Russell. **Incident Response: A Strategic Guide to Handling System and Network Security,** New Riders Publishing, 2001.

[8] **ERIBERTO, 2005; Fluxo de dados na tabela filter**. Disponível em: <http://www.eriberto.pro.br/iptables/filter.jpg> Acesso em: 31de outubro de 2008.

[9] RONCARATTI FONSECA CAIO; Segurança de Redes Com Uso de um aplicativo Firewall Nativo do sistema Linux. 2006. Trabalho de Conclusão de Curso de Ciências da Computação, Centro Universitário Barão de Mauá, São Paulo.

[10] **Tenable Network Security (NESSUS)**. Disponível em: <http://www.nessus.org/>. Acesso em: 31 de outubro de 2008.

[11] **Snort Plataform Security (SNORT)**. Disponível em: <http://www.snort.org>. Acesso em: 31 de outubro de 2008.

[12] **Comunidade Snort Brasil (SNORT).** Disponível em: <http://www.snort.org.br/>. Acesso em: 31 de outubro de 2008**.**

[13] **Nagios Network Monitoring Program (Nagios)**. Disponível em**:** <http://www.nagios.org/>. Acesso em: 31 de outubro de 2008.

[14] BURTAMANN DA SILVA, VERÔNICA; Análise de Infra-Estrutura de Rede para Suporte à Videoconferência: Um Estudo de Caso.2005. Trabalho de Conclusão de Curso de Ciências da Computação, Instituto de Física e Matemática da Universidade Federal de Pelotas, Pelotas.

[15] **IDS/IPS and Firewall Logs Analyzer (Snortalog).** Disponível em: <http://jeremy.chartier.free.fr/snortalog/>. Acesso em: 13 de novembro de 2008.

[16] CESAR, Mário. **Criando um CSIRT*: Computer Security Incident Response Team****: Brasport, 2008.*

OUTROS TRABALHOS EM:
www.projetoderedes.com.br

Anexo A

Modelo de Política de Segurança

O objetivo é prestar aos funcionários serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional. Assim, para assegurar os altos padrões de qualidade na prestação desses serviços, faz-se necessária a especificação de uma política de utilização da rede.

O objetivo dessa Política de Utilização da Rede é descrever as normas de utilização e atividades que entendemos como violação ao uso dos serviços e recursos, os quais são considerados proibidos.

Podemos definir como serviços e recursos os equipamentos utilizados pelos funcionários tais como: computadores, e-mails do domínio suaempresa.com.br, link de Internet e afins. As normas descritas no decorrer não constituem uma relação exaustiva e podem ser atualizadas com o tempo, sendo que qualquer modificação será avisada em tempo hábil para remodelação (se necessário) do ambiente.

Tais normas são fornecidas a título de orientação do funcionário. Em caso de dúvida sobre o que é considerado, de alguma forma, violação, o usuário deverá enviar previamente um e-mail para abuse@suaempresa.com.br visando esclarecimentos e segurança.

Nos termos da Política de Utilização da Rede, a empresa procederá o bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com o aqui estabelecido ou de forma prejudicial à Rede.

Caso seja necessário advertir o funcionário, será informado o departamento de Recursos Humanos para interagir e manter-se informado da situação.

Atitudes que são consideradas violação à Política de Utilização da Rede foram divididas em quatro tópicos, que são:

I. Utilização da Rede
III. Utilização de acesso a Internet

Abaixo descreveremos as normas mencionadas e informamos que tudo o que não for permitido e/ou liberado é considerado violação à Política da Utilização da Rede.

I. Utilização da Rede

Esse tópico visa definir as normas de utilização da rede que engloba desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

a) Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
b) Não é permitido tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;
c) Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;

d) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/logoff da rede ou bloqueio do desktop através de senha;
e) Falta de manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis;
f) Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;
g) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designados conforme abaixo:

Tabela 1. Armazenamento de Arquivos

Compartilhamento	Utilização
Diretório XX: (usuário)	Arquivos Pessoais inerentes a empresa
Diretório ZZ: (departamento)	Arquivos do departamento em que trabalha
Diretório PP: (público)	Arquivos temporários ou de compartilhamento geral

Em alguns casos podem haver mais de um compartilhamento referente aos arquivos do departamento em qual faz parte.
h) A pasta PÚBLICO ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível;
i) É obrigatório armazenar os arquivos inerentes a empresa no servidor de arquivos para garantir o backup dos mesmos;
j) Haverá limpeza semanal dos arquivos armazenados na pasta PÚBLICO ou similar, para que não haja acúmulo desnecessário de arquivos;
k) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento técnico, através de solicitação escrita que será disponibilizada;
l) É vedado a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento técnico;
m) Não será permitido a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

II. Utilização de acesso a Internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

a) É proibido utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados não legalizados;
b) É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
c) Poderá ser utilizada a Internet para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
d) Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;

e) Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados;
f) Caso a empresa julgue necessário haverá bloqueios de acesso à:

1. Arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
2. Domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

g) Haverá geração de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório;
h) Obrigatoriedade da utilização do programa Mozilla, ou outro software homologado pelo departamento técnico, para ser o cliente de navegação;
i) Não será permitido softwares de comunicação instantânea, tais como ICQ, Microsoft Messenger e afins;
j) Não será permitido a utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus e afins;
k) Não será permitida a utilização de serviços de streaming, tais como Rádios On-Line, Usina do Som e afins.

Das Punições

O não cumprimento pelo funcionário das normas ora estabelecidas neste Documento ("Políticas de Utilização da Rede"), seja isolada ou acumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

(A) COMUNICAÇÃO DE DESCUMPRIMENTO;
– Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada.
– Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta funcional do infrator.

(B) ADVERTÊNCIA OU SUSPENSÃO;
– A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

(C) DEMISSÃO POR JUSTA CAUSA;
– Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, alienas "a" à "f".

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

Anexo B

Modelo de Política de Uso Aceitável

Política de uso aceitável

A <nome da organização> não autoriza o uso de suas redes de computadores para os seguintes fins:

• transmitir ou divulgar ameaças, pornografia infantil, material racista, discriminatório ou qualquer outro que viole a legislação em vigor no Brasil;

• propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros;

• transmitir tipos ou quantidades de dados que possam causar falhas em serviços ou equipamentos na rede da <nome da organização> ou de terceiros;

• utilizar computadores ou a rede de computadores da <nome da organização> para efetuar levantamento de informações não autorizado (SCAN) na rede de computadores da <nome da organização> ou de terceiros;

• uso da rede de computadores da <nome da organização> para o trânsito de mensagens de e-mail com cabeçalhos inválidos ou alterados, de forma a dificultar ou impedir a identificação da sua origem, ou mensagens enviadas através de servidores de e-mail de terceiros, sem a autorização dos respectivos responsáveis (relaying);

• usar a rede para tentar e/ou realizar acesso não autorizado a dispositivos de comunicação, informação ou computação;

• utilização dos computadores e redes de computadores da <nome da organização> para a coleta de endereços de e-mail dos seus clientes.

• forjar endereços Internet de máquinas, de rede ou de correio eletrônico, na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria;

• destruir ou corromper dados e informações de terceiros;

• violar a privacidade de terceiros;

• distribuir via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo 'corrente' e mensagens em massa, comerciais ou não;

• enviar grande quantidade de mensagens idênticas ao mesmo destinatário por correio eletrônico (mail bombing);

• transmitir, distribuir ou armazenar materiais protegidos por direito autoral ou quaisquer outros direitos de propriedade intelectual;

• quaisquer outros usos que violem a legislação vigente no Brasil.

A violação destas normas poderá resultar em suspensão temporária ou cancelamento dos serviços prestados, além das demais medidas necessárias, incluindo, mas não se limitando à remoção de dados, desativação de servidores e implementação de filtros.

Obedecendo as práticas definidas para a Internet, serão mantidos os endereços abuse@dominio.com.br e abuse@outrodominio.com.br para servirem de canais de reclamação de práticas abusivas vindas da rede de computadores da <nome da organização>. As pessoas que se sentirem prejudicadas por pacotes de dados vindos de

nossa rede devem denunciar a prática enviando um e-mail para esses endereços com informações detalhadas, inclusive registros de computadores (logs), sobre a prática abusiva.

Anexo C

Script de Regras de Firewall (Iptables)

```
#!/bin/sh
# Variaveis

iptables=/sbin/iptables

IF_EXTERNA=eth1
IF_INTERNA=eth0


# Ativa modulos

# ------------------------------------------------------
/sbin/modprobe iptable_nat
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_REJECT
/sbin/modprobe ipt_MASQUERADE


# Ativa roteamento no kernel

# ------------------------------------------------------
echo "1" > /proc/sys/net/ipv4/ip_forward

# Zera regras
# ------------------------------------------------------
$iptables -F
$iptables -X
$iptables -F -t nat
$iptables -X -t nat
$iptables -F -t mangle
$iptables -X -t mangle

# Determina a política padrão
# ------------------------------------------------------
$iptables -P INPUT   ACCEPT
$iptables -P FORWARD DROP
$iptables -P OUTPUT ACCEPT
```

```
#######################
# Regra de INPUT
#######################

$iptables -A INPUT -p tcp --dport 22 -i $IF_EXTERNA -j ACCEPT
$iptables -A INPUT -p tcp --dport 22 -i $IF_INTERNA -j ACCEPT
$iptables -A INPUT -p tcp --dport 5901 -i $IF_INTERNA -j LOG   --log-prefix "VNC"
$iptables -A INPUT -p tcp --dport 6001 -i $IF_INTERNA -j LOG   --log-prefix "VNC"
$iptables -A INPUT -p tcp --dport 5901 -i $IF_INTERNA -j ACCEPT
$iptables -A INPUT -p tcp --dport 6001 -i $IF_INTERNA -j ACCEPT
$iptables -A INPUT -i -lo -j ACCEPT
$iptables -A INPUT -p ALL -s 127.0.0.1 -i lo -j ACCEPT
$iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
$iptables -A INPUT -p icmp -i eth1 -j LOG --log-prefix "PING NA INTERFACE ETH1" --log-level 4
$iptables -A INPUT -p icmp -i eth1 -j ACCEPT

########################
# Regra de Forward
########################

$iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
$iptables -A FORWARD -p tcp -s 0/0 -d 200.200.200.3 --dport 3389 -j LOG  --log-prefix "Acesso Remoto" --log-level 4
$iptables -A FORWARD -p udp -s 0/0 -d 200.200.200.3 --dport 3389 -j LOG  --log-prefix "Acesso Remoto" --log-level 4
$iptables -A FORWARD -p tcp -s 0/0 -d 200.200.200.3 --dport 3389 -j ACCEPT
$iptables -A FORWARD -p udp -s 0/0 -d 200.200.200.3 --dport 3389 -j ACCEPT

#FTP
#$iptables -A FORWARD -p tcp -s 0/0 -d 10.0.0.2 --dport 21 -j ACCEPT
#$iptables -A FORWARD -p tcp -s 0/0 -d 10.0.0.2 --dport 20 -j ACCEPT
#iptables -A FORWARD -p tcp --dport 20 -j ACCEPT
#iptables -A FORWARD -p tcp --dport 21 -j ACCEPT

##################
# Regra de NAT
##################

$iptables -t nat -A PREROUTING -p tcp -d 10.4.207.248 --dport 3389 -j DNAT --to 200.200.200.3:3389
$iptables -t nat -A PREROUTING -p udp -d 10.4.207.248 --dport 3389 -j DNAT --to 200.200.200.3:3389

#Redirecionamento FTP

#$iptables -t nat -A PREROUTING -p tcp -d 192.168.0.1 --dport 21 -j DNAT --to 10.0.0.2:21
#$iptables -t nat -A PREROUTING -p tcp -d 192.168.0.1 --dport 20 -j DNAT --to 10.0.0.2:20
$iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

########################
# Regra de Output
########################

echo "Firewall Iniciado ...."
```

Anexo D

Análise de Vulnerabilidade com Nessus

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 1
- Number of security notes found : 3

TESTED HOSTS

10.0.0.50 (Security holes found)

DETAILS

+ 10.0.0.50 :
. List of open ports :
  o netbios-ssn (139/tcp) (Security notes found)
  o microsoft-ds (445/tcp) (Security notes found)
  o techra-server (1862/tcp)
  o ms-wbt-server (3389/tcp)
  o netbios-ns (137/udp) (Security warnings found)
  o general/tcp (Security hole found)

. Information found on port netbios-ssn (139/tcp)

An SMB server is running on this port

. Information found on port microsoft-ds (445/tcp)

A CIFS server is running on this port

. Warning found on port netbios-ns (137/udp)

The following 4 NetBIOS names have been gathered :
EMP_GSMR_06194
DEMPREL = Workgroup / Domain name
EMP_GSMR_06194 = This is the computer name
DEMPREL = Workgroup / Domain name (part of the Browser elections)
The remote host has the following MAC address on its adapter :
00:10:c6:a1:56:d6

If you do not want to allow everyone to find the NetBios name
of your computer, you should filter incoming traffic to this port.

Risk factor : Medium
CVE : CAN-1999-0621

. Vulnerability found on port general/tcp :

You are running a version of Nessus which is not configured to receive
a full plugin feed. As a result, the security audit of the remote host
produced
incomplete results.

To obtain a complete plugin feed, you need to register your Nessus scanner
at http://www.nessus.org/register/ then run nessus-update-plugins to get
the full list of Nessus plugins.

. Information found on port general/tcp

Information about this scan :

Nessus version : 2.2.8
Plugin feed version : 200605221015
Type of plugin feed : GPL only
Scanner IP : 10.4.233.192
Port scanner(s) : nessus_tcp_scanner
Port range : 1-15000
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : no
Max hosts : 20
Max checks : 4
Scan duration : unknown (ping_host.nasl not launched?)

Anexo E

Análise de Tráfego do Firewall com Fwlogwatch

Log do Firewall do Projeto RTIR

Generated segunda setembro 22 22:35:36 BRT 2008 by root.
289 of 301 entries in the file "/var/log/iptables.log" are packet logs, 8 have unique characteristics.
First packet log entry: Set 22 21:21:10, last: Set 22 22:35:04.
All entries were logged by the same host: "rtir".
All entries have the same target: "-".

Set 22 21:21:59 to Set 22 22:35:04 00:01:13:05 VNC eth0 269 packets (14484 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 21:21:10 to Set 22 21:21:22 00:00:00:12 PING NA INTERFACE ETH1 eth1 13 packets (780 bytes) from 200.200.200.3 (kacker) to 200.200.200.1 (servidor_rtir)

Set 22 21:22:05 to Set 22 21:22:06 00:00:00:01 VNCIN=eth0 OUT= MAC=00:60:97:<4>VNC eth0 2 packets (92 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 21:22:05 to - - VNCIN=eth0 OUT= MAC=00:60:LEN=50 TOS=0x00 PREC=0x00 TTL=128 ID=17915 DF PROTO=TCP <4>VNC eth0 1 packet (46 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 21:22:05 to - - VNCIN=eth0 OUT= MAC=00:60:97:c9:9e:c2:00:1b:78:08:69:08:08:00 SRC=10.1.253.163 DST=10.4.207.248 LEN=50 TOS=0x00 PREC=0x00 TTL=1 eth0 1 packet (50 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 21:22:05 to - - VNCIN=eth0 OUT= MAC=00:60:97:c9:9e:c2:00:1b:78:08:69:08:0<4>VNC eth0 1 packet (46 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 22:35:03 to - - VNCIN=eth0 OUT= MAC=00:60:97:c9:<4>VNC eth0 1 packet (50 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)

Set 22 22:35:03 to - - VNCIN=eth0 OUT= MAC=00:60:<4>VNC eth0 1 packet (46 bytes) from 10.1.253.163 (emp_gsmr_14124) to 10.4.207.248 (rtir)