UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Cássia Maria Carneiro Kahwage

ATAQUES A REDES DE COMPUTADORES E RECOMENDAÇÕES PARA SISTEMA DE DETECÇÃO DE INTRUSOS -IDS

Florianópolis
Santa Catarina - Brasil
Março 2002

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Cássia Maria Carneiro Kahwage

ATAQUES A REDES DE COMPUTADORES E RECOMENDAÇÕES PARA SISTEMA DE DETECÇÃO DE INTRUSOS -IDS

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Orientadora: Prof.“ Dr.“ Elizabeth Sueli Specialski

Florianópolis
Santa Catarina - Brasil
Março 2002

ATAQUES A REDES DE COMPUTADORES E RECOMENDAÇÕES PARA SISTEMA DE DETECÇÃO DE INTRUSOS -IDS

Cássia Maria Carneiro Kahwage

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração Sistema de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Edíríano'A. Ostini Gauthier, Dr.
Coordenador do Curso.

Banca Examinadora

Elizabeth Speciálski, Dr.
Professora Orientadora

Luiz Fernando Jacintho Maia, Dr.

Orlando Fonseca Silva, Dr.

Florianópolis,_____de _____de 2002.

Tfedico a memória de minha avó
T,te[vina TerciCiana LoSão Carneiro

Agradecimentos

A Deus pgí tocto pocleh-oso.
A meus pgis Mg Ha e jo͡go, pelo apoio e compf-essão.
A mínhg prafessoh-g oríentgdof-g, Betb que me gpoío e motivou pgi-g o tei'mino cjotf-gbglho, e g gmízgde e gtenção cjispensgcla a mím.
Ao ph-ofessoi' Bosco, pelg compreensão e gpoíou de sempfe.
Ao CESWPA ngs pessogs cjo pf-ofessoh- Séf-gío Mendes e prafesso^g Conceição cie Mello pelo gpoío e incentivos pgi-g o cjesenvolvímento 4este tf-abglho.
Ao coorden^doi' locgl *c|o* mesth-a4o Gustavo Qmpos pelg sug gf-^nde pgcíêncíg, e confi'^nç^.
Ao ^mígo If-^níMo/ sócio e colega de ti^gbglho, pelo gpoío e incentivos.
Ao amigo e colega de trabalho Cipf-iano, que não mediu esforços pa^a meaiudaf".
E um especial agi^adecimento ao pf-ofessor Nelson Veiga pelo incentivo, apoio e caHnbo.
E a todos os colegas e amigos do mesth-ado pelas horas maravilhosas que passamos [untos, Marcelo, Lourenço, Marcos, Jacqueline, Andréia, Almeida, Otávio, afinal todos.

RESUMO

Com o aumento do número de ataques às redes de computadores, uma das maiores preocupações dos administradores de redes é utilizar ferramentas de auxílio no processo de defesa e monitoração de suas redes coorporativas.

Com o crescimento em larga escala da utilização de computadores de pequeno porte, a distribuição das aplicações que facilitam a confecção de ataques e o uso das facilidades da Internet, tomaram a segurança da rede e o funcionamento correto da rede um desafio.

Um dos problemas encontrados para monitorações em redes de computadores reside em detectar tentativas de intmsão. Os Sistemas de Detecção de Intmsos são ferramentas que analisam o tráfego da rede com objetivo de identificar ataques ou tráfego suspeito, enviando alertas ao administrador, e em alguns casos, realizando ações de defesa com a inclusão de filtro no firewall automaticamente.

Este trabalho apresenta métodos de ataques mais comuns e técnicas de defesas, e recomendações sobre a utilização de ferramentas automatizadas para a detecção de intmsão, como forma de garantir a segurança de redes com arquitetura TCP/IP. Propõe um modelo IDS distribuído para amenizar problemas das atuais ferramentas.

ABSTRACT

Considering the increase of the number computers networks attacks, one of mean networks administrators warning is to use aided tools in the defense process of corporative networks.

After widely use of small computer sets, the distribution of the applications that leads to attacks and hitemet environment use, made the network security and their right use a on challenge.

One of the problems found to survey of the computer networks security, is to detect the intrusion trying. The hitruders Detection System as a tools, analyze network traffic in order to identify attacks or suspect traffics, sending dangerous messages to the administrator, and in some cases, moving defense actions with the filter inclusion in the firewall automatically.

This presents work introduces some methods of most common attacks, defense techniques, and recommendations of use automated tools for the intrusion detection, as some manners to assure the security of TCP/IP architecture network. Also an IDS model distributed solution is proposed, in order to reduce the current IDS tolls problems.

SUMÁRIO

Lista de Figuras

Lista de Abreviaturas

ACK - Acknowledgement.

ARP - Address Resolution Protocol.

BIND - Berkeley Internet Name Daemon.

BO - Back Orifici.

CA - Autoridade de Certificação.

CERT - Computer Emergency Response Team.

CIAG - Global Incident Analsys Center.

CIDF - Common Intrusion Detection Framework.

CIRT - Computer Incident Response Team.

CMDS- Computer Misuse Detection System.

DDOS- Distribuited Denial Of Service.

DES - Data Encrytion Standart.

DF - Don't Fragment.

DHCP - Dynamic computador Configuration Protocol.

DMZ - DeMilitarized Zone.

DNS - Domain Name Service.

DNSec- DNS Security Extensions.

DOS - Denial Of Service.

EOI - Events of Interest.

FTP - File Transfer Protocol.

GOTS - Government Off-the-Shelf

HIDS - Host Intrusion Detection System.

HLEN - Internet Header Length.

HTTP - Hypertext Transfer Protocol.

lANA - Internet Address Numbers Authority.

ICMP - Internet Control Message Protocol.

ICSA - International Computer Security Association.

IDEA - International Data Encryption Algorithm.

IDES - Intrusion Detection Expert System.

IDS - Intrusion Detection System.

IETF - Intemet Engineering Task Force.

IKE - Intemet Key Exchange.

IP - Intemet Protocol.

IPsec - IP Security Protocol.

ISS - Intemet Security Systems.

LAN - Local Area Network.

MAC - Media Access Controler.

MD5 - Message Digest 5.

MF - More Fragments.

MIDAS- Multics Intmsion Detection and Alerting System.

MMS - Maximum Segment Size.

MTU - Maximun Tranfer Unit.

NADIR - Network Audit Director and Intmsion Reporter.

NAT - Network Address Translation.

NFN - Network Flight Recorder.

NFS - Network File System.

NIC - Network Intreface Card.

NIDS - Network Intmsion Detection System.

OOB - Out of Band.

PWS - Personal Web Server.

RFC - Request For Comments.

RIP - Routing Information Protocol.

RSA - Rivest- Shamir-Adleman.

SDSI - Stateful Dymamic Signature Inpection.

SHA - Secure Hash Algorith.

SNMP- Simple Network Management Protocol.

SPI - Stateful Packet Inspection.

SSL - Secure Socket Layer.

TCP - Transmission Control Protocol.

TFTP - Trivial File Transfer Protocol.

TLS - Transporte Layer Security.

TTL - Time To Live.

UDP - User Datagram Protocol.

VPN - Virtual Private Network.

EMERALD - Event Monitoring Enabling Responses to Anomalous Live Disturbances.

1. Introdução

"A segurança é um processo e não um estado ou uma meta" (WADLOW, 2000).

Desde o tempo das pinturas nas paredes das cavernas, passando pelos escritos em papel, até a atualidade, em sua forma digital, a informação vem mudando seu suporte. Atualmente, os diversos tipos de informação são armazenados em meios digitais como discos magnéticos, DVD, CD-ROM, etc.

Uma vez que o mercado é cada dia mais competitivo, as organizações necessitam possuir informações para sobreviver, o que implica em uma crescente informatização das organizações e um suporte tecnológico cada vez mais complexo.

As organizações utilizam cada vez mais os computadores, e o intercâmbio de informações, no âmbito de pequenas e grandes distâncias, é suportado pelas redes de computadores.

Além do compartilhamento de informações, as organizações utilizam a infra-estrutura das redes de computadores para o compartilhamento de alguns recursos tais como, impressoras, bancos de dados centralizados e linhas de acesso a redes de longa distância.

O crescimento das redes de computadores fez o mundo ficar menor, encurtar distâncias perder fronteiras.

A rede mundial de computadores, conhecida como Internet, pode ser considerada uma revolução, pois milhões de computadores são conectados entre si, permitindo que usuários domésticos, grandes e pequenas empresas, e órgãos governamentais, troquem mensagens, publiquem páginas e visitem sites em busca de informações e serviços. Com alguns cliques no mouse, pode-se visitar museus, ou fazer compras em grandes magazines.

Todo este avanço faz com que as informações e o controle sobre elas sejam estratégicos para as organizações.

Com o aumento do tráfego de informações nas redes de telecomunicações, observa-se a tendência de aumento na quantidade de informações estratégicas e sigilosas armazenadas nos meios computacionais.

Por outro lado, a interligação das redes locais das organizações à Internet trouxe a grande ameaça de invasão a estas redes, com a conseqüente possibilidade de alteração de informação ou roubo de informações secretas e, também, a paralisação de seus sistemas.

O risco de ataque às redes locais é cada vez maior, pelo aumento dos números de computadores na Internet, pela proliferação de ferramentas e scripts de auxílio para hackers e crackers, e, também, pela própria fragilidade da arquitetura da rede Internet.

Não é incomum ler-se nos noticiários que o site de empresa "X" foi invadido, e que ao invés da página da empresa aparece uma página pornográfica, com dizeres de repúdio ou sátira à empresa.

A CERT (Computer Emergency Response Team) uma organização criada para responder aos incidentes de segurança na Internet, deve centralizar os incidentes e providenciar as correções e punições necessárias. O número de incidentes recebidos vem aumentando no decorrer dos anos; em 1998 foram 3.734 incidentes, em 1999, 9.859 incidentes, em 2000, 21.756 incidentes, e em 2001, 34.754 incidentes (CERT, **2002**).

Observa-se, portanto a grande escalada dos números de incidentes e, provavelmente existem muito mais incidentes do que os reportados à CERT, pois, nem todas as organizações divulgam que sofreram ataques. Esta prática muitas vezes é adotada por falta conhecimento, ou mesmo por que é interessante para a vítima esconder que foi atacada por algum intruso.

A arquitetura da Internet foi inicialmente planejada para compartilhamento de dados. O objetivo militar do projeto inicial era o da robustez, isto é, caso ocorresse um ataque em algum ponto físico da rede, ela deveria continuar em `funcionamento; não houve, portanto, preocupação com a segurança de dados.

O número de incidentes de segurança nas redes tem acompanhado o crescimento da Internet nos últimos anos. Os sistemas, serviços e protocolos estão vulneráveis aos ataques. Os intrusos podem realizar uma simples sondagem, executar ações que causem o comprometimento de contas, escuta de pacotes, negação de serviços, exploração de relações de confiança, ou ainda, inserir programas que ficam

ocultos no sistema e possuem os mais diversos objetivos, tais como os chamados cavalos de tróia. (ALEN, et ali 2000).

Não somente o número dos ataques vem aumentado, mas prejuízos causados por estes ataques somam milhões de dólares. A tabela 1.1 classifica os ataques e quanto em valores foram os prejuízos causados pelos intrusos.

Tabela 1-1 Perdas Financeiras

Perdas financeiras registradas nos EUA

Fonte : 5^ Pesquisa Nacional sobre Segurança da Informação, 2001 apud FBI

	Incidentes Reportados	Prejuízo Total
Roubo de informações proprietárias	23	$ 42.496.000
Sabotagem de dados na rede	27	$4.421.000
Grampo em telecomunicações	10	$ 765.000
Invasões externas dos sistemas	28	$ 2.885.000
Abuso de funcionários Autorizados	81	$ 7.576.000
Fraude financeira	27	$ 39.706.000
Denial of Service	28	$ 3.255.000
Vírus	116	$ 5.276.000
Acesso não autorizado de funcionários	25	$ 3.576.000
Fraude em telecomunicações	29	$ 773.000
Grampo na rede	1	$ 20.000
Roubo de Notebooks	150	$ 13.038.000

Obs: Apenas 31 das empresas americanas conseguiram quantificar as perdas.

Os ataques exploram várias características dos protocolos da arquitetura TCP/IP, as falhas de implementação dos sistemas operacionais e os sistemas de serviços Internet como DNS (Domain Name Service), servidores de e-mail e servidores web. Os ataques são inúmeros e cada vez mais sofisticados.

É comum a utilização de ferramentas e scripts que auxiliem na identificação e exploração de sistemas operacionais, serviços disponíveis e sua configuração ou má configuração. Um exemplo seria a utilização do NMap, um software que identifica, através de sondagem, o sistema operacional da máquina vítima e quais os serviços estão rodando em determinadas portas deste computador.

O desafio que se apresenta para os atuais administradores de redes consiste em bloquear os ataques e garantir a segurança das redes internas das organizações

conectadas à Internet. Este desafio não é de simples solução, pois a segurança de uma rede depende da combinação de diversas técnicas e estratégias de defesa.

Uma única técnica isolada pode não oferecer a segurança, necessária ou suficiente para a rede da organização.

Segurança pode ser definida como uma corrente composta por diversos elos, onde esses elos são estruturas identificadas como pontos vulneráveis, merecedores de maior atenção. Nessa corrente, existe a preocupação em manter-se cada elo em um nível de segurança adequado para que se possa alcançar um nível de segurança que seja satisfatório para a corrente como um todo; um único elo fi^aco pode comprometer toda a estrutura.

A simples adoção de um firewall, já não é mais considerada suficiente para a proteção das redes. Conforme mencionado anteriormente, existem outras técnicas que são necessárias para melhorar o nível de segurança de uma rede. As técnicas mais utilizadas atualmente além do firewall são: a criptografia e os protocolos criptografados, a autenticação, as redes privadas virtuais - VPN (Virtual Private Network), o monitoramento e os Sistemas de Detecção de Intrusos - IDS (Intrusion Detection System).

Este trabalho tem como objetivo descrever os tipos de ataque mais comuns e suas respectivas de técnicas de defesas, gerando recomendações sobre a utilização de ferramentas automatizadas para a detecção de intrusão, como forma de garantir a segurança de redes com arquitetura TCP/IP.

A justificativa e a motivação para a execução deste trabalho repousam no fato do crescimento dos números de sites e publicações sobre tipos e receitas de ataque e muitas ferramentas que facilitam os ataques, aumentado em quantidade, variedade e complexidade destes, tomando a tarefa de atualização dos filtros de firewalls, para filtrar o tráfego perigoso, extremamente difícil. Além disso, os passos de como os hackers e crackers iniciam seus ataques, seguem geralmente um padrão: primeiro é necessário a obtenção de dados dos computadores vítimas, tais como número IP da máquina, serviços e portas instaladas para, em seguida, realizar o ataque; na maioria das vezes explorando alguma falha do sistema operacional ou de algum serviço.

É muito difícil que os administradores da rede ou de segurança conheçam todos os ataques com detalhes; e é muito mais difícil monitorar todo o tráfego da rede sem a utilização de uma ferramenta para automatização do processo.

Para auxiliar os administradores, as ferramentas de IDS podem detectar tentativas de intrusão e auxiliar na confecção de melhores filtros para os firewalls.

Parte essencial de um sistema de segurança, as ferramentas IDS, ou Intrusion Detection System, são merecedores de destaque na mídia atualmente, devido a inúmeros casos de ataques que ocorreram durantes os últimos meses a grandes sites, entre eles os de bancos e de governos, e que nos fez notar a necessidade e a importância de uma ferramenta IDS para o sucesso da segurança de um site.(CARFFARO, 2001)

As ferramentas IDS trabalham basicamente com a análise do tráfego da rede, comparando o tráfego com as assinaturas de ataques anteriores, e identificando o tráfego anormal na rede, estas ferramentas não possuem cem por cento de acertos, pois podem gerar alarmes falsos ou mesmo não gerar alarmes quando existe um ataque real. Estas situações são denominadas falsas positivas e falsas negativas respectivamente.

Neste trabalho, além das características dos IDS, serão discutidos também os prós e contras destas ferramentas. Mesmo que estas ferramentas não possuam grande grau de certeza sobre os alarmes gerados, acredita-se que elas apresentam um dos caminhos que podem auxiliar a segurança de redes de computadores.

O trabalho foi organizado em sete capítulos. Nesta introdução, apresenta-se o contexto do trabalho e o problema a ser resolvido. O segundo capítulo descreve as principais características da arquitetura Internet e de seus protocolos. O terceiro capítulo descreve as estratégias e tipos mais comuns de ataques. O quarto capítulo discorre sobre os principais mecanismos e técnicas de segurança. O quinto capítulo apresenta os componentes e ferramentas IDS. No sexto capítulo, descreve-se as recomendações de como utilizar as ferramentas IDS para detecção de tentativas de intrusão, e o modelo de IDS distribuído. No sétimo as conclusões. A bibliografia empregada no apoio a este trabalho é apresentada no oitavo capítulo.

A metodologia utilizada consiste em levantamento bibliográfico, teste e configuração de software de monitoramento e detecção de intrusos.

2. Características da arquitetura e protocolos TCP/IP

2.1 O modelo TCP/IP Internet

Atualmente é comum um usuário de computador fazer acesso a uma página Web ou enviar um e-mail. Freqüentemente é visto em comerciais e programas na tevê o incentivo à participação dos telespectadores em sites na Internet. Estas tarefas aparentemente banais têm, em sua infraestrutura, muitos processos realizados. Para um simples acesso ao servidor de página Web remota, podem ser realizados centenas de processos.

Os processos envolvem comunicações computador a computador. Na figura 2.1 é mostrado um exemplo de comunicação computador a computador. A transferência, como por exemplo, de um pedido de envio de documento para um servidor Web, inicia na caixa escrita *aplicação.* Esta requisição é empacotada e enviada através dos vários processos e camadas, representados pelas caixas inferiores na figura 2.1. Cada caixa da figura 2.1 representa uma camada da arquitetura de rede da Internet e consiste em um segmento lógico, por onde passa a mensagem, originada na camada de aplicação, na viagem do computador emissor para o computador receptor.

Em cada camada, no sentido vertical de cima para baixo, a mensagem é adicionada com os controles necessários para a comunicação, isto é, cada camada recebe a mensagem da camada superior, adiciona os seus dados de controle e repassa a mensagem para a sua camada inferior. Esta técnica é conhecida como "empacotamento", mostrado na figura 2.2. Depois de serem empacotados nas diferentes camadas, os dados seguem do emissor para o receptor através da rede física, representada pela linha horizontal, na parte inferior da figura 2.1. No computador receptor, o processo é executado ao inverso, isto é, cada camada "desembrulha" o pacote, retira os dados de controle inseridos pela camada par remota e repassa a mensagem para a sua camada superior, no sentido de baixo para cima, até que a mensagem chegue na camada de aplicação do receptor.

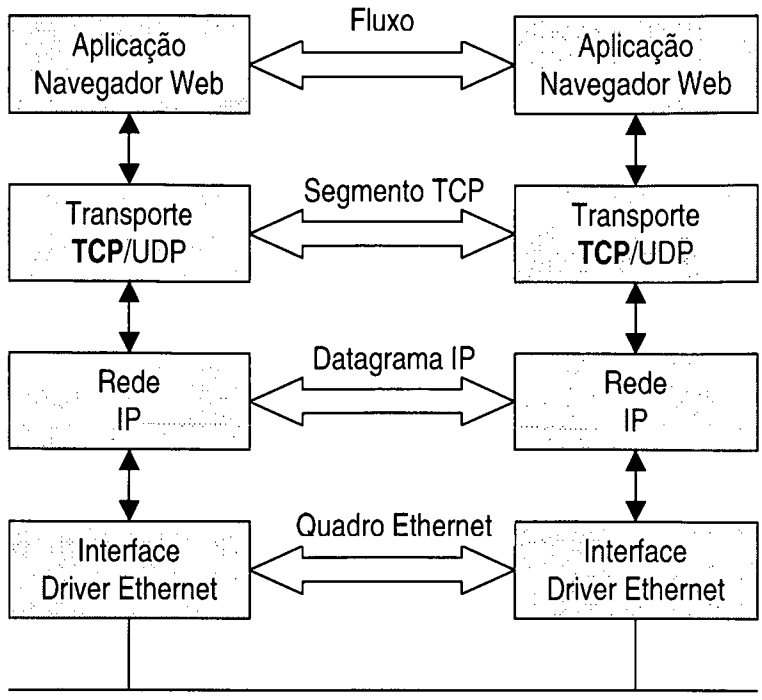

Figura 2.1- Exemplo de utilização da arquitetura de rede

No exemplo da figura 2.1, pode-se identificar as camadas que compõem a arquitetura de rede Internet: Aplicação, Transporte, Rede e Interface.

A camada de Aplicação fornece serviços e processos de aplicativos; é a interface através da qual o usuário tem acesso aos serviços, tais como, terminal virtual TELNET, transferência de arquivos FTP (File Transfer Protocol), navegação Web, correio eletrônico e outros.

A camada de Transporte fica abaixo da camada aplicação. Esta camada abrange vários aspectos de comunicação entre o computador emissor e receptor. A camada de transporte está freqüentemente envolvida em fornecer segurança para as outras camadas inerentemente falíveis. Esta camada possui dois protocolos: o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol). O TCP é um protocolo orientado à conexão e confirmado, e é considerado seguro pelo mecanismo de distribuição de dados; já o UDP, não é orientado à conexão e nem confirmado, não garantindo, portanto, uma transferência de dados segura.

A camada de Rede, situada abaixo da camada de transporte, é responsável pelo roteamento dos pacotes (nesta camada, chamados de datagramas). O roteamento

consiste na identificação de um caminho, através da rede, para que o pacote possa chegar ao computador destino.

A camada de interface é a camada mais inferior na arquitetura TCP/IP, é responsável pela comunicação entre o computador e o meio físico que ele está. Muitas das vezes o componente físico que implementa esta camada é uma placa Ethemet, mas existem outras interfaces. Esta camada se preocupa com o recebimento e envio de dados por meio de uma interface específica de rede.

2.2 O Processo de Empacotamento dos dados

o fluxo de dados trocados entre os computadores emissor e o receptor necessita ser "empacotado", isto é, a camada adiciona os seus dados de controle e repassa a mensagem para a sua camada inferior, e assim sucessivamente até a camada mais inferior, como mostrado na figura 2.2. Os controles são interpretados pela camada par do computador receptor.

As camadas são empilhadas umas sobre as outras, advindo o termo "pilha TCP/IP", e cada pacote consiste em um conjunto de cabeçalhos e dados. Toda a encapsulação é realizada para enviar algum tipo de dado ou conteúdo, mas requer diferentes informações de cabeçalho em diferentes níveis em sua viagem da origem ao destino.

Suponha-se uma comunicação Telnet, a aplicação Telnet utiliza o protocolo TCP, enviando o fluxo de dados para a camada imediatamente abaixo, nesta camada está implementado o protocolo TCP.

O TCP transforma o fluxo de dados em segmento TCP e inclui o seu cabeçalho aos segmentos, que são enviados para a camada inferior, que é a camada de rede que implementa o protocolo IP (Internet Protocol).

O protocolo IP pré-anexa (anexa na parte da frente) as informações de seu cabeçalho no segmento TCP, tomado-se um datagrama IP.

O datagrama IP é enviado para a camada de interface da pilha TCP/IP, esta camada pré-anexa seu cabeçalho transformado o datagrama em quadro (frame), a camada de interface transporta o quadro pelo meio físico.

o processo descrito se repete na ordem inversa, quando o quadro chega no host destino, todos os cabeçalhos são retirados e passados aos protocolos de camadas superiores.

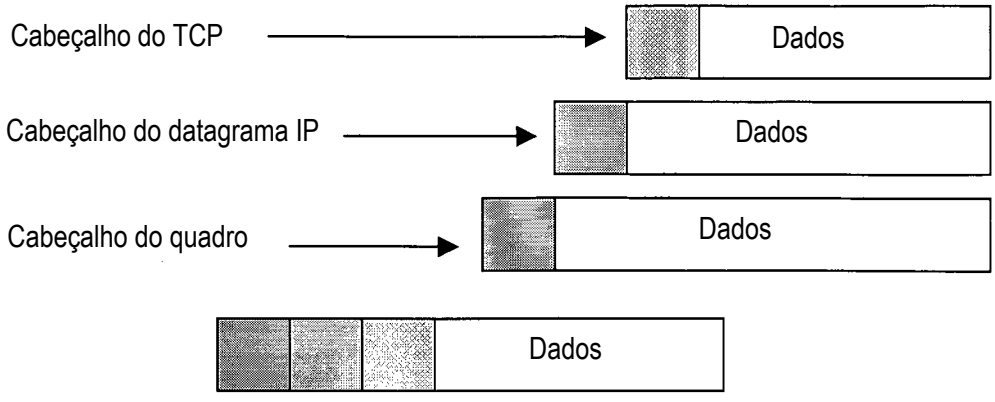

Figura 2.2 - Os cabeçalhos pré-anexados conforme empacotamento da pilha TCP/IP

2.3 Endereçamento

Endereços físicos são os números das interfaces de redes de cada computador. As interfaces possuem um número de 48 bits chamado de endereço MAC (Media Access Controler). Os endereços MAC são os números das placas de rede inseridas pelos fabricantes. Os endereços lógicos são os números IP, números de 32 bits que endereçam um computador da Intemet, na versão 4 deste protocolo.

Atualmente, os números IPv4 válidos são escassos; por esse motivo, existem subterfúgios para amenizar esta problemática. Um deles é a alocação de imi número IP por sessão ou por tempo de conexão, através de uma aplicação do DHCP (Dynamic Computer Configuration Protocol).

O DHCP atribui um número IP v4 temporariamente, pela duração de uso ou tempo determinado, significando que nem todos os hosts estarão ativos simultaneamente. Assim, um grupo menor de números pode ser utilizado. Uma outra opção seria a utilização de endereços reservados. O lANA (Internet Address Numbers Authority) reservou blocos de endereços IPv4 para serem utilizados apenas como endereços de redes internas, por exemplo, 192.168 e 172.16. O tráfego com os endereços reservados não devem ultrapassar o gateway da rede intema para a rede

extema. A utilização de endereços de redes de classes B, que endereçam em tomo de 65.000 hosts, na rede intema, permite economizar endereços válidos. Vale ressaltar que os pacotes que saem da rede intema devem ter seus endereços não válidos trocados para endereços válidos antes de serem enviados para o tráfego na Intemet.

A utilização dos endereços reservados pode dificultar a invasão dos hackers externos, pois pacotes com estes endereços não são roteados na rede extema.

O mapeamento dos endereços MAC físicos para endereços IP lógicos é efetivado através do protocolo ARP (Address Resolution Protocol). O protocolo ARP mapeia os endereços lógicos e físicos, isto é, endereços IP em endereços MAC. O tráfego ARP se restringe a hosts conectados na mesma rede IP, não podendo ser realizado entre hosts de redes diferentes.

O endereço MAC é um número de 48 bits, onde os fabricantes de NIC (Network Intreface Card) possuem cada qual um prefixo que os identifica.

O hacker pode utilizar uma placa com edição MAC editáveis, isto é, pode colocar qualquer número MAC em sua máquina. Esta estratégia é bastante incomum, pelo auto custo da confecção da placa.

O endereço IPv4 é um número de 32 bits expressos em quatro números decimais de 0 a 255, separados por pontos como, 190.0.0.2. Os números IP são divididos em gmpos chamados de rede que possuem o mesmo prefixo binário. O restante do número binário identifica o host. Os gmpos foram distintos por cinco classes; as classes dizem quantos hosts existem em determina rede ou quantos bits no endereço IP são endereços atribuídos para hosts exclusivos em uma rede. As classes A, B e C foram determinadas como classes de endereçamento. Na tabela 1 estão os números de bits utilizados para endereçar rede e host.

Tabela 2-1 - Classes de Endereçamento IP

Classe	*Bits da Rede*	*Bits do host*	*Número de hosts*
A	8	24	16 milhões +
B	16	16	65.000 +
C	24	8	254

Cada uma das classes possui número de redes (netid) e prefixo de identificação. A identificação de host (hostid) é mostrada na figura 2.3, abaixo:

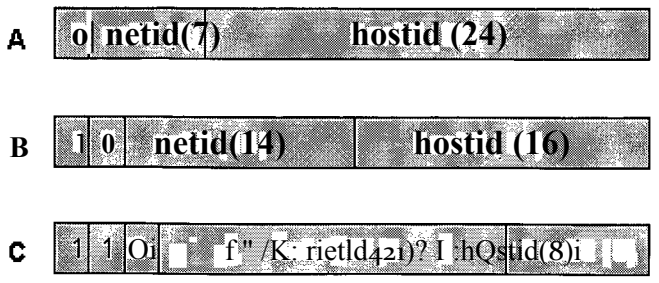

Figura 2.3 - Classes de endereçamento IP

A máscara de sub-rede determina ao sistema quantos bits de seu endereço IPv4 foram reservados para endereçamento da rede e quantos bits para endereçamento de host. Cada bit de rede é mascarado pelo bit ‘ 1 ’ na máscara. Um endereço de classe C 192.0.0.1 possui 24 bits para endereçamento da rede, portanto a máscara padrão de um endereço de classe “C” seria 255.255.255.0. Pode-se modificar o número de bits para endereçar a rede de 24, por exemplo, para 25, dividindo a rede de classe C em duas com número menor de endereçamento de host, isto é, duas redes de 126 endereços de host, sendo a primeira do host ‘1’ até o ‘126’ e a segunda de ‘129’ até ‘254’. A máscara de sub-rede então seria 255.255.255.128.

O mecanismo de máscara de sub-rede permitiu que os endereços IP fossem melhor aproveitados.

2.4 Protocolo IPv4

A figura 2.4 mostra o cabeçalho do datagrama IPv4. Os grupamentos lógicos de bits são chamados de campos. Cada campo identifica uma característica do protocolo. Cada linha possui 32 bits (0 a 31).

Segundo (SOARES, 1996) as características principais do IPv4 são:

Serviço de datagrama não confiável;

Endereçamento hierárquico;

Facilidade de fragmentação e remontagem de datagramas;

Identificação da importância do datagrama e do nível de confiabilidade exigido;

Identificação de urgência de entrega e da ocorrência, futura ou não, de pacotes na mesma direção (pré-alocação, controle de congestionamento).

Campo especial indicando qual protocolo a ser utilizado no nível superior;

Roteamento adaptativo distribuído nos gateways;

Descarte e controle de tempo de vida dos pacotes inter-rede no gateway.

A identificação do nível confiabilidade exigido, muitas vezes não lido pelos roteadores. Esta característica é mais bem implementada na versão 6 do IP.

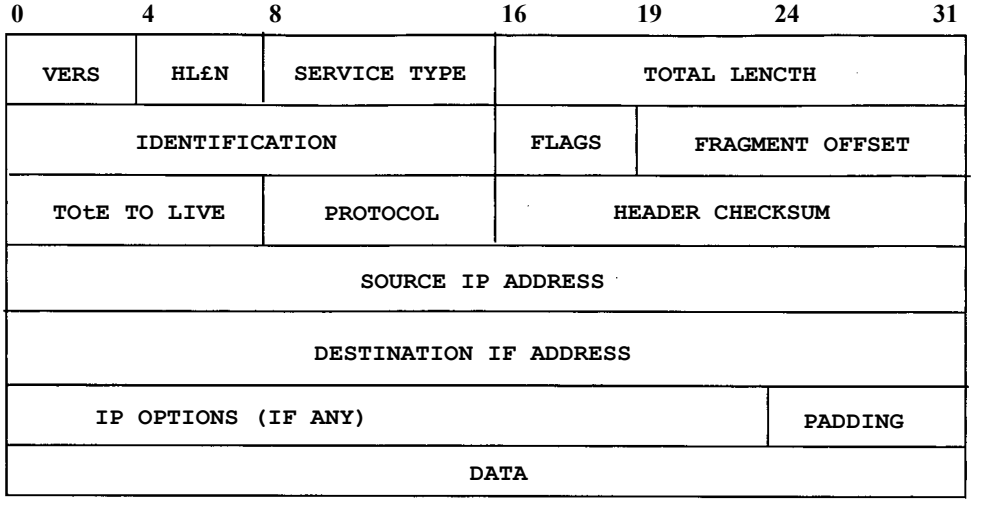

Figura 2.4 - Datagrama IP

A figura 2.4 mostra o os campos que constituem o datagrama IP.Os campos do protocolo IP são os seguintes, com respectivas utilizações: (CHIOZZOTO, 1999).

VERS (4 bits): Indica a versão do protocolo utilizado no datagrama se IPv4 ou IPv6-

HLEN - Internet Header Length (4 bits) Anota o tamanho do cabeçalho em números de 32 bits, isto é, em quantos conjuntos de 32 bits ou palavras compõe o cabeçalho.

Service Type (8 bits): é especificado em outros sub-campos;

Precedence: (3 bits) indica prioridade dos datagramas com valores desde 0 (precedência normal) até 7 (controle da rede). Com estes bits permite-se ao transmissor indicar a importância de cada datagrama que ele está enviando.

Bits D,T,R: indicam o tipo de transporte que o datagrama deseja. Baixo Retardo(D), Alta Capacidade de Processamento(T) e Alta Confiabilidade(R). Não é possível que estes tipos de serviços sempre sejam oferecidos, já que dependem das condições físicas da rede.

Total Lenght (16 bits): quantidade total de bytes do datagrama IP, somados à área do cabeçalho mais os dados.

Identification (16 bits): Número que identifica o datagrama.

Flags (3 bits): bit 0 DF-Don't Fragment, este bit indica a não fragmentação do datagrama. Bits 2 e 3 MF-More Fragment, indica se existem mais fragmentos.

Fragment Offset: especifica o início do datagrama original dos dados que estão sendo transportados no fragmento. É medido em unidades de 8 bytes.

TTL (Time To Live): especifica o tempo em segundos que o datagrama está permitido a permanecer na rede.

Protocol: especifica qual protocolo está no nível superior, e que foi encapsulado pelo protocolo IP.

Header-Checksum: assegura integridade dos valores do cabeçalho.

Source And Destination Ip Address: especifica o endereço IP de 32 bits do host de origem e destino.

Options: é um campo opcional. Este campo varia em comprimento dependendo de quais opções estão sendo usadas. Algumas opções são de um byte.

COPY-. (1 bit) controla a forma em que o gateway trata as opções durante a fragmentação:

1: a opção deve ser copiada em todos os fragmentos

0: a opção deve ser copiada somente no primeiro fragmento.

CLASS (2 bits): especifica a classe geral da opção.

OPTION NUMBER(): especifica uma opção na classe determinada no campo CLASS.

Padding: Completa o conjunto de 32 bits de options. A somatória de options mais padding deve ser múltiplo de 32.

Os datagramas IPv4 são encaminhados através da camada de interface à camada física como um conjunto de bits, que trafegam nos cabos físicos da rede com destino a rede intema ou extema. Se o destino for a rede extema, os datagramas são direcionados através do gateway (roteadores nas redes TCP/IP) da rede intema para o próximo gateway extemo. Este processo de envio de pacotes através dos gateway é chamado de roteamento

2.4.1 Roteamento

O roteamento consiste no direcionamento dos datagramas IP de uma rede IP para outra rede IP, através de um host que realiza o processo. Os roteadores possuem uma tabela de roteamento interno que determina o destino dos datagramas de cada rede IP, possibilitando a transferência dos datagramas de uma rede para outra.

A figura 2.5 mostra o esquema simplificado de duas redes, LAN A (Local Area Network) e LAN B.

O host A quer enviar uma solicitação de conexão HTTP (Hypertext Transfer Protocol) para o host B: verifica que o host B está em outra rede IP e empacota o fluxo de dados e envia datagrama para a camada de interface.

A camada interface envia o frame ao gateway padrão, que, no caso, é o roteador de endereço IP 10.0.0.1/24.

Como o host A não conhece o endereço MAC do roteador, então envia uma requisição ARP para a rede, então, o roteador responde à requisição com o seu número MAC. Só então o host A envia o frame para o roteador.

O roteador, ao receber o frame, envia os dados para camada de rede, que através das informações contidas no cabeçalho IP, verifica para qual destino enviará o datagrama, com base em sua tabela de roteamento. No exemplo, o datagrama será enviado para a interface **ethl.**

O datagrama enviado para a interface ligada à rede com hots B, ao enviar o datagrama para a camada imediatamente inferior a de interface o roteador verifica o endereço MAC do destinatário; se não o possuir será enviando uma requisição ARP à rede de endereço IP 10.0.1.0 para obtenção do endereço. O host B responderá qual seu endereço MAC. Quando o roteador receber a resposta da requisição ARP, envia o frame para o meio físico. Assim o pacote chegará até seu destino.

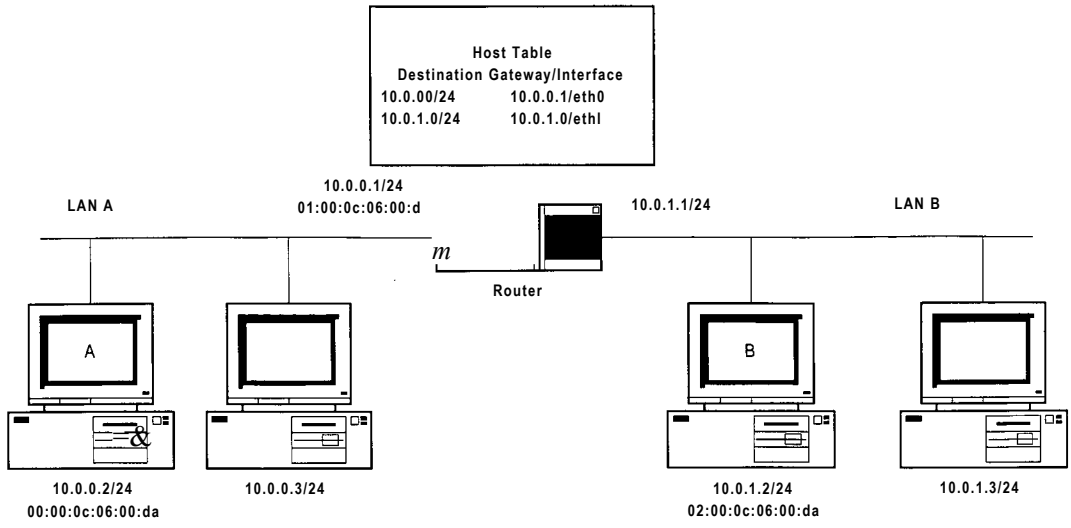

Figura 2.5 - Roteamento IP

2.4.2 Fragmentação IP

A fragmentação IP é o processo que divide um datagrama IP em vários fragmentos, com objetivo de enviar os datagramas de maior tamanho, em redes de tamanho máximo de pacote (MTU- Maximun Tranfer Unit) menor que o datagrama a ser enviado. A fragmentação ocorre na origem, em um roteador de fronteira, por exemplo, e é remontado no destino.

Quando há fragmentação, os dados da mesma são anotados nos cabeçalhos dos fragmentos para que a remontagem seja realizada.

Os fragmentos necessitam estar associados ao datagrama original. Esta associação é feita através do número de identificação repetido nos fi'agmentos, isto é, os fragmentos originados do datagrama original possuirão todos o mesmo número de identificação.

O campo flag do cabeçalho define algumas das características da fragmentação; o primeiro bit deste campo não é utilizado, o bit seguinte marca 0 bit DF Don't Fragment, marcará os fragmentos que não podem ser fragmentados.

MF signiflca more fragments, isto é, quando este bit está ativado significa que este não é o último fragmento; o fragmento que não possuir este bit ativado é o último fragmento, avisando que a remontagem pode iniciar.

Muitos administradores de rede desabilitam a fragmentação de pacotes em seus computadores servidores para evitar ataques que utilizem a fragmentação IP.

2.4.3 Protocolo ICMP

O ICMP (Internet Control Message Protocol) foi criado para detectar problemas na rede e reportar considerações de erro. Este protocolo é encapsulado pelo protocolo IP, mas mesmo assim, é considerado ser um protocolo da camada de rede. A aplicação mais conhecida é a requisição/resposta eco, utilizada através do chamado ping. O protocolo ICMP foi criado com boas intenções, mas também é utilizado para ataques a redes. A figura 2.6 mostra o formato de um pacote ICMP.

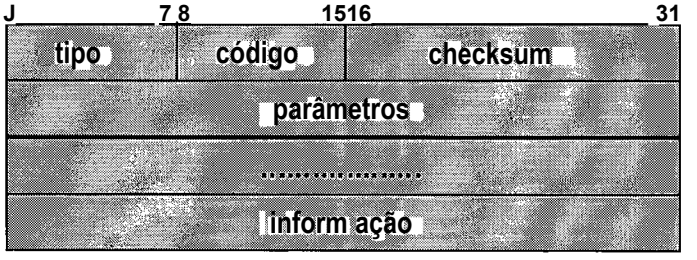

Figura 2.6 - Formato do cabeçalho ICMP

2.5 IPv6

O IPv4 é um protocolo que nos últimos 20 anos sofreu poucas alterações. Seu maior problema era o endereçamento de 32 bits, pois o número de endereços disponíveis é cada vez mais escasso. O IPv6 é uma evolução do IPv4, onde o objetivo principal é eliminar o problema de endereçamento. Ele é o resultado direto da insuficiência de espaço de endereço do IPv4- O IPvó aumenta o tamanho de 32 para 128 bits de modo a fornecer suporte a mais níveis da hierarquia de endereçamento, a um número bem maior de nós endereçáveis e uma autoconfiguração mais simples de endereços.(Naugle, 2001).

O protocolo IPv6 também implementa outros recursos além da expansão do endereçamento.

Possui um cabeçalho mais simplificado, para tomar o protocolo mais eficiente; alguns campos do cabeçalho foram eliminados e o cabeçalho possui tamanho estático de 40 bytes. Além disso, implementa o conceito de extensão de cabeçalho, flexibilizando a introdução de opções fiituras.

O protocolo IPv6 permite a rotulagem de pacotes pertencentes a "fluxo" de tráfego específicos, para os quais o remetente solicita tratamento especial, como qualidade de serviço acima dos padrões ou serviços em "tempo real".

O roteamento I?v6 é semelhante ao roteamento IPv4, mas os protocolos de roteamento precisam ser modificados para os endereços de 128 bits. Os protocolos OSPF, RIP, IDRP e IS-S podem ser utilizados com modificações mínimas.

O IPv6 implementa recursos de autenticação e privacidade para melhor segurança, através de extensões do cabeçalho.

A segurança do protocolo IPv6 é implementada através das extensões de cabeçalho, que são a extensão de segurança com a autenticação e carga de segurança de encapsulamento (RFC' 1826, RFC 1827), que são opcionais. A não ufilização dos cabeçalhos pode deixar o protocolo vulnerável.

Este protocolo não altera os protocolos da camada superior, portanto as vulnerabilidades dos protocolos TCP e UDP ainda podem ser exploradas.

A ampla implementação do protocolo IPv6 se dará por etapas, nos próximos anos. Por enquanto está em utilização em apenas em uma parte pequena da rede, utilizando parte da Internet IPv4 atual. (Naugle, 2001).

Como o protocolo ainda não tem a sua utilização na Internet como um todo, ainda não sofreu o teste final, que é o ataque dos hackers. As implementações do IPv6 só poderão ser realmente testadas quando a chave for virada e toda a Internet utilizar a nova implementação IP.

2.6 Protocolo da camada de transporte

Dois modelos de transporte diferentes são descritos nesta camada: um *modelo baseado em conexão e com um serviço confirmado* (TCP) e outro *sem conexão e sem confirmação* (UDP). *Baseado em conexão* significa que o software realiza conexão antes da entrega dos dados e *serviço confirmado* significa que, quando o receptor reconhece a mensagem como válida, envia uma confirmação para o emissor.

' Request For Comments: Documento para proposição de padrões para Internet.

O TCP inicia uma tarefa de transferência de dados estabelecendo uma conexão, conhecida como handshake (aperto de mão). O UDP simplesmente envia os dados esperando que eles cheguem, sem maiores preocupações e sem nenhuma garantia de segurança. A tabela 2 mostra um resumo das características dos protocolos TCP e UDP.

Tabela 2-2 - Características TCP e UDP

TCP	UDP
Confiável	Não Confiável
Baseado em conexão	Sem conexão
Mais lento	Mais rápido
Otimizado para Internet	Otimizado para Internet

2.6.1 As portas de Serviços

Os protocolos possuem campos de 16 bits em seus cabeçalhos e são chamados de portas. Isto significa que o valor máximo para as portas é de 2^^, isto é, 65.536 portas de serviços. Cada um dos serviços será identificado por uma porta que espera por algum tipo de solicitação. Os serviços da Internet estão associados a portas padrões, como, por exemplo, o Telnet (Terminal Virtual) que está associado à porta TCP 23. As portas podem ser mudadas pelo administrador do sistema, e esta também pode ser uma maneira de um invasor esconder um serviço em um host.

Qualquer serviço pode ser executado em qualquer porta, mas quando se deseja estabelecer conexão com outros hosts na Internet, é recomendado se utilizar as portas padrões. Além disso, esta prática também facilita instalações de atualizações e path de correção.

As portas abaixo de 1.024 são portas especiais de serviços padrões da Internet, antes chamadas de portas "seguras", porque somente a raiz poderia utilizá-las. Isto não é mais válido e as portas acima de 1.024 são agora conhecidas como *portas efêmeras* ou *portas de usuário,* o que significa que elas podem ser utilizadas por qualquer serviço, por qualquer razão.

Em aplicações que não toleram perda de pacotes deve-se usar o TCP, pois ele possui um mecanismo de verificação das seqüências dos dados, conhecido como mecanismo de *acknowledgement.*

O acknowledgement (ACK) é gerado pelo receptor, para cada pacote recebido. Se o receptor não gera um ACK para um determinado pacote é por que não foi recebido. Neste caso, o emissor envia o pacote novamente. O TCP é mais seguro, mas pode gerar overhead.

O protocolo UDP é mais simplificado, havendo somente a montagem e o envio dos pacotes. É um protocolo mais rápido, mas não confiável: as aplicações que o utilizam são as que requerem alta velocidade e que suportam perda de dados, isto é, se um ou outro datagrama se perder, não fará falta à aplicação. Um exemplo poderia ser a transmissão de áudio.

2.6.2 O protocolo TCP

Alguns mecanismos que asseguram confiabilidade ao protocolo TCP são;

- Conexão exclusiva e única entre os dois hosts;
- Números de seqüência que determinam uma cronologia aos dados TCP. Cada segmento possui um número de seqüência ao ser enviado do emissor para o receptor. O número de seqüência é incrementado a cada segmento enviado e é utilizado para a remontagem dos dados no destino.
- Acknowledgment; são os avisos de recebimentos, que possuem o número de seqüência do segmento confirmado.

A figura 2.7 mostra o formato do cabeçalho TCP. A descrição dos campos e sua utilização são relacionadas abaixo; (CHIOZZOTO, 1999).

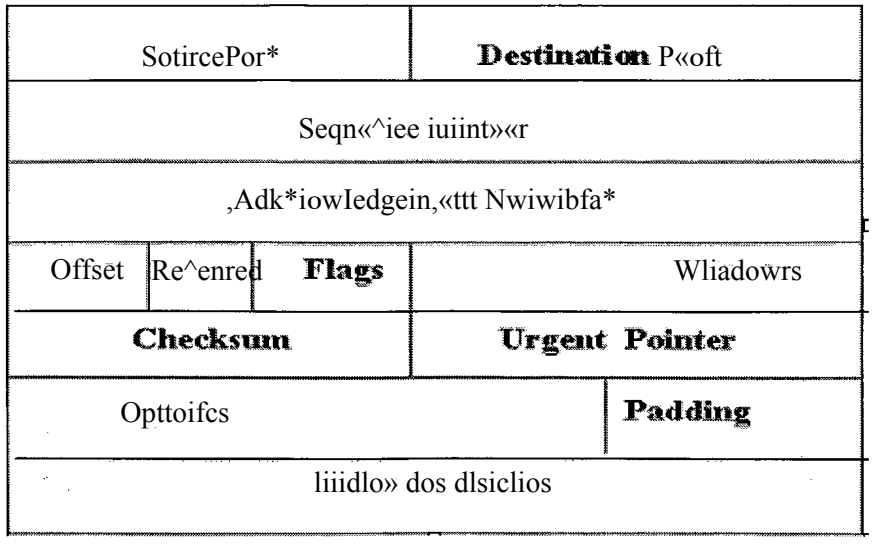

Figura 2.7 - Segmento TCP

Source e Destination Port (16 bits): O ponto de acesso ao serviço (SAP) do protocolo TCP, identifica o canal virtual entre a aplicação de origem e aplicação destino.

Sequence Number (32 bits): número de idenfificação da seqüência do segmento TCP.

Acknowledgement Number: este número identifica o próximo segmento a ser recebido.

Offset (4 bits): indica o tamanho do cabeçalho TCP em número de 32 bits.

Reserved (6 bits): Reservados para uso futuro.

Flags (6 bits): assumem valores para estabelecimento de conexão, finalização de conexão, transferência de dados urgentes e outros. Os valores para estes campos estão descritos na tabela 3:

Tabela 2-3 - Flags TCP

Flag TCP	Representação do Flag	Descrição
URGENT	Urg	Campo indica dados urgentes de urgência;
ACK	Ack	Envio de confirmação de recebimento de dados do emissor;
PSH	P	Entrega de dados urgentes a aplicação, sem bufferização;
RST	R	Intenção do host em abortar imediatamente a conexão;
SYS	S	Uma requisição de estabelecimento de sessão, primeira parte da conexão TCP;
FIN	F	Finaliza a conexão elegantemente.

Windows (16 bits): indica o tamanho da janela que o indicador pode operar.

Checlísum (16 bits): utilizado para detecção de erros em todo o segmento inclusive os dados.

Urgent Point (16 bits): indica a presença de dados urgentes no segmento, o valor aponta a localização dos dados;

Options: sinaliza dados extras não definidos no cabeçalho padrão, como por exemplo, o MMS (Maximum Segment Size);

Padding: completa o conjunto de 32 bits já que campo options possui tamanho variável.

O Handshake

O estabelecimento de conexão obedece a um ritual chamado de handshake. A figura 2.8 esquematiza o estabelecimento de conexão. O cliente é o computador que envia uma solicitação de serviços para Servidor, o computador de destino, que envia resposta ao cliente, que recebe e envia a mensagem para confirmação da conexão.

O servidor executa os serviços em uma porta que está na escuta de prováveis solicitações. O TCP exige que uma porta de destino seja especificada para realizar a solicitação de conexão.

1° passo: O cliente envia um pacote com o flag SYS para sinalizar uma requisição de conexão.

2° passo: Se o servidor estiver ligado e oferecer os serviços na porta determinada, o servidor envia ao cliente a requisição do cliente com um novo SYS e acusa o recebimento de conexão do cliente com o flag ACK, em um único pacote.

3° passo: Se o cliente recebendo os Flags SYS+ACK, ainda quiser continuar a conexão, ele envia um último ACK para o servidor. Neste ponto a conexão está estabelecida os dados podem ser agora transferidos.

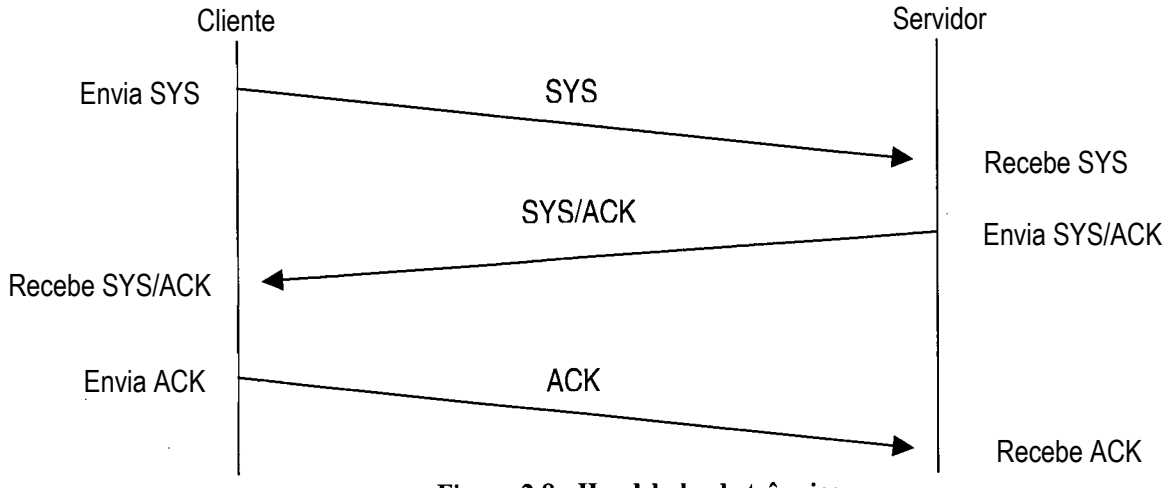

Figura 2.8 - Handshake de três vias

Duas conexões são estabelecidas, uma entre o cliente e o servidor, e outra entre o servidor e o cliente, pois o protocolo é full duplex.

Uma conexão de três vias é um conjunto de mensagens trocadas entre dois computadores. As mensagens são conjuntos de bits, que se exibidos como bits dificultariam a leitura das mensagens, então usam o formato TCPdump. Esta notação é um formato resumido do pacote em formato de string, facilitando assim a leitura dos pacotes. (NORTHCUTT, 2001)

A seqüência de string abaixo exibe a conexão do computador host.com.br com o computador telnet.com.br em três passos.

1° passo:
```
host.com.br.38804 > telnet.com.br.23 S 7333 8182 9:7333 8182 9(0) win <mss 1460>
(DF)
```
2° passo:
```
telnet.com.br.23 > host.com.br.3 8804 S 1192930639: 119293063 9(0) ack 733381830
win 1024 <mss 1460> (DF)
```
3o passo:
```
host.com.br.38804 > telnet.com.br.23 :. ack win 8760 (DF)
```

O computador *host.com.br* é o cliente e *telnet.com.br é o* servidor. O cliente seleciona a porta efêmera 38804, e se comunica com a porta 23 do servidor. A conexão pode ser finalizada com o envio de um pacote com o flag FIN, que solicita o final da conexão.

Existem duas maneiras de se terminar uma conexão, a primeira conforme já descrito anteriormente, consiste em enviar um FIN; a solicitação pode ser feita tanto

pelo cliente como pelo servidor. O destinatário da solicitação deve responder um ACK, aceitando a finalização de conexão. A outra maneira definida em uma conexão consiste em se enviar um flag de RESET, finalizando abruptamente a conexão, sem nenhuma resposta do destinatário.

2.6.3 O protocolo UDP

O UDP aceita dados de várias aplicações e os envia num único fluxo de informação, para a camada inferior. As aplicações negociam com o sistema operacional obtendo um protocol port, especificando um UDP source port. Quando da recepção dos datagramas, faz a desmultiplexação para porta de destino.

Aplicações que necessitam de velocidade e que os dados não críticos utilizam este protocolo, podem ser, por exemplo: RIP (Routing Information Protocol), DNS (Domain Name Service) TFTP (Trivial File Transfer Protocol), NFS (Network File System), SNMP (Simple Network Management Protocol) e outros.

A figura 2.9 mostra o esquema do protocolo UDP:

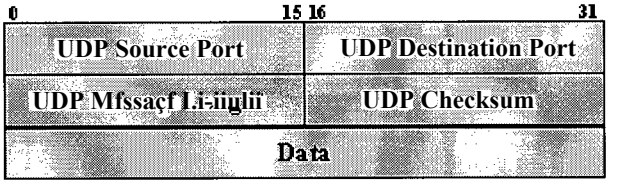

Figura 2.9- Segmento UDP

UDP Source Port: identifica a porta de origem do processo que envio a mensagem

UDP Destination Port: porta de destino do processo ou serviço do host de destino.

UDP Message Length: número de octetos total do pacote UDP (cabeçalho + dados).

UDP checksum: checagem da mensagem UDP. O preenchimento do campo é opcional.

2.7 *Domain Name System*

Gerenciar uma grande quantidade de nomes que são constantemente modificados, não é uma tarefa fácil. Conceitualmente a Internet é divida em diversos domínios (domains) de primeiro nível, onde cada domínio cobre muitos hosts. Os domínios são particionados em subdomínos, que também são particionados, e assim por diante, podendo ser representados como uma árvore. (TANENBAUM, 1997)

Todos os domínios, independentes de serem host simples ou domínio de primeiro nível, podem ter um conjunto de registros associados a eles. A atribuição de nomes na Internet utiliza um sistema de banco de dados distribuído, o Domain Name System (DNS) que realiza o controle dos registros de domínio e endereços IP, além das trocas de correspondência e outras informações. Na consulta em um servidor DNS, um processo pode mapear um nome de domínio na Internet para o endereço IP usado para a comunicação com os domínios.

Os servidores contêm freqüentemente os arquivos relativos a um ou mais domínios. Os servidores de domínio globais tais como: *.com, .edu, .br,* etc, possuem arquivos contendo o IP dos servidores de domínios comuns, tais como, *ufsc.br* ou *altavista.com.* Nos servidores de domínios comuns estão os endereços dos hosts ou subdomínios daquele domínio existente.

Este serviço da Intemet possibilita que o usuário consulte páginas web, e não necessite decorar o número IP dos servidores web; basta que ele saiba o nome do domínio como, por exemplo, como www.altavista.com.

Os comandos principais dos serviços DNS são *gethostbyaddress* e *gethostbyname* que consultam a base de dados do servidor DNS solicitando um endereço IP ou um nome de um host de determinado IP, como definem os comandos no próprio nome.

O servidor DNS recebe as consultas através do protocolo UDP na porta 53, o resultado da consulta é enviado para o cliente.

O serviço de DNS é alvo para os atacantes, pelo fato que o não funcionamento deste faz que vários serviços não possam ser utilizados. Outros serviços com WWW, WEB, servidores de e-mail e servidores FTP, também são alvo dos invasores.

O próximo capítulo descreve as estratégias de ataque utilizadas pelos intrusos.

3. Estratégias e tipos mais comuns de ataques

Os ataques aos sistemas são cometidos por invasores, idolatrados por uns e odiados por outros. Os tipos de invasores podem ser enquadrados na classificação abaixo relacionada:

Hacker: são grandes conhecedores da arquitetura Internet; possuem grande astúcia na operação de sistemas operacionais e linguagem de programação e procuram falhas, ou brechas em sistemas e programas. A convenção hacker define que um hacker não rouba informações, ele apenas alerta administradores sobre as falhas dos sistemas e dizem serem bem intencionados; (TANENBAUM, 1997).

Cracker: possui grande conhecimento e astúcia, assim como um hacker, só que estes roubam e destroem informações, são furtivos, e usam seu conhecimento em benefício próprio. Os próprios hackers definem os cracker como "os caras do mal"; (INFORMÁTICA passo a passo, 2001)

Phreaker: especializado em sistemas telefônicos, usam a rede telefônica para obter ligações gratuitas tentando não ser identificado; (ROMANO, 2001).

Arakers: são os hackers de araque; não possuem grande conhecimento, mas atualmente podem fazer uso de scripts causando danos; (TANENBAUM, 1997).

Lamer: são os interessados no comportamento dos hackers, são os estudiosos dos ataques; (TANENBAUM, 1997).

Wannabe: São os iniciantes, possuem algum conhecimento, mas fazem uso de scripts e ferramentas escritas por hacker, freqüentemente causam danos. (TANENBAUM, 1997).

A intenção deste trabalho é a identificação dos ataques; se ele é ou não bem intencionado, não interessa ao contexto deste trabalho. Interessa sim o fato de que está se cometendo um delito quando se invade áreas privadas de empresas, e que se está roubando algo, mesmo que sejam alguns bits no disco rígido ou lançando alguns pacotes na rede. Qualquer tipo de ataque é sempre prejudicial ao sistema, por mais bem intencionado que ele seja. Se o atacante é mesmo bem intencionado, ele pode pedir ao administrador para fazer testes em sua rede, explicando quais as ferramentas serão utilizadas. O ideal seria direcionar este esforço para a área de segurança.

Existe uma remota possibilidade de um hacker ser contratado para trabalhar na área de segurança, pois as técnicas de ataques são diferentes das técnicas de defesa, mas existem exceções: hackers que trabalham em *tiger team* ou até fazem palestras, mas não são a maioria.

Existem milhares de incidentes de segurança sendo executados por ano, e muitos hacker são conhecidos por passarem de atacantes a defensores, mas não tanto quanto o número de atacantes. Muitas empresas não contratam ex-invasores com receio de serem roubados ou extorquidos.

A escalada dos ataques é surpreendente e vem quase dobrando a cada ano. O gráfico apresentado na figura 3.1, mostra a escalada dos ataques em sua sofisticação e a falta de conhecimento dos atacantes na utilização de ferramentas.

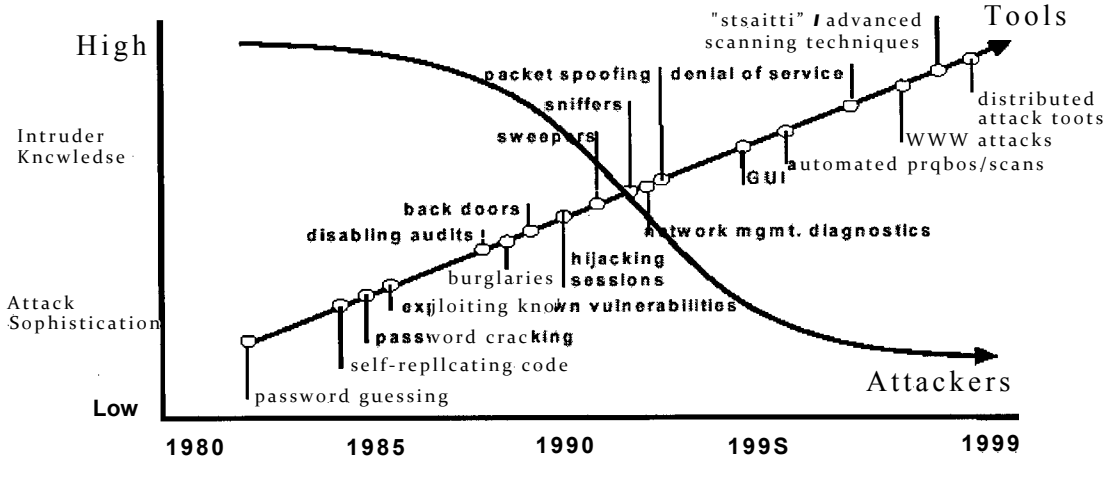

Figura 3.1 - Escalada da sofisticação dos ataques

Fonte: (ALEN, 2001 aprud DONN PARKER, 2000)

Segundo a figura 3.1, a facilidade de se obter ferramentas e scripts que orientam ataques possibilita que pessoas com pouco conhecimento realizem ataques altamente sofisticados.

As motivações dos hackers são: coleção de troféus; acesso gratuito aos meios de comunicação, acesso a recursos computacionais, ponte para outras máquinas, realizar danos (mais ou menos sofisticados) e obter informações.

3.1 Passos da Invasão

Os passos realizados pelos atacantes seguem um padrão e podem ser organizados nos seguintes:

Footprintíng: consiste na criação do perfil de segurança de uma organização, utilizando ferramentas para obtenção de informações como: o nome do domínio, blocos de endereços IP e quais sistemas então conectados à Internet.

Varredura: consiste em procurar informações como: qual o número IP do servidor DNS, qual o sistema operacional atual, qual o correio eletrônico. Neste tipo de atividade o hacker pode fazer uso da engenharia social para obtenção de algumas informações. As varreduras possuem este nome devido ao método de como são obtidas as informações, como as varreduras baseadas na exploração do handshake TCP ou varredura ping, entre outras.

Enumeração: após a identificação, aquisição do alvo e a sondagem, realizada com sucesso, o atacante poderá identificar usuários com recursos de compartilhamento mal protegidos. Existem muitas maneiras de extrair contas e compartilhamentos, inclusive ferramentas poderosas para vários sistemas operacionais que facilitam muito a enumeração para o intruso.

Penetração: é a entrada no sistema. Esta entrada muitas vezes explora bugs do sistema operacional ou dos serviços. Neste momento o hacker pode utilizar ferramentas de quebra de senhas de contas para penetrar no sistema.

Escalada de privilégios: assim que o atacante penetra no sistema ele tenta a escalada para obtenção de privilégio de root. A obtenção de privilégios de root é geralmente obtida através de exploração de bugs de programas instalados, tais como, send mail, http, tfltp e outros.

Furto: o intruso com privilégio de administrador pode obter quaisquer informações da máquina invadida, podendo ver, editar, apagar, copiar ou executar qualquer arquivo do sistema. Muitos atacantes quando têm interesse roubam as informações neste momento.

Instalação de portas dos fundos: após da invasão realizada há a preocupação da manutenção do acesso; nesta hora o hacker instala um cavalo de tróia no computador, que fica com seu sistema comprometido.

Cobertura dos rastros: com acesso total o atacante trata de apagar os vestígios de sua atividade no sistema, alterando o log do sistema e a data de acesso a alguns arquivos.

Exploração de um novo "salto": Não tendo mais o que fazer na máquina atacada, o hacker pode utilizar esta máquina como base para a realização de ataques a outras máquinas, dificultando a localização da origem do ataque.

As máquinas invadidas são chamadas de *sistemas comprometidos.* Geralmente a recomendação é a instalação de todos os sistemas novamente, pois não se tem conhecimento do que foi alterado, uma vez que o hacker pode alterar os rastro das ações realizadas.

3.2 *Tipos de Incidentes de Segurança*

Os incidentes de Segurança foram classificados como: (DEKKER , 1997)

Probe *{sondagem, investigação)* - É caracterizado pela tentativa de se obter acesso em sistemas ou descobrir sobre o sistema. Um exemplo é a tentativa de logar com contas não usadas. Sondar eletronicamente é equivalente a tentar girar as maçanetas da porta de carros em um estacionamento, para achar alguma porta aberta para entrada fácil;

Scan *{varredura)* - É simplesmente um número grande de tentativas feitas utilizando ferramentas automatizadas. A varredura pode ser resultado de perda de configuração ou outro erro, mas podem ser prelúdio para um ataque direcionado no sistema que o intruso achou vulnerável.

Account Comprimise *{contas comprometidas)* - Uma conta comprometida, é um usuário não autorizado com uma conta de usuário legítimo, sem envolver o nível de sistema ou direitos do root (privilégios de administrador de sistema ou gerente de rede). Uma conta comprometida pode expor a vítima a sérios problemas como, perda de dados, roubo de dados ou serviços roubados. A falta do privilégio de root toma o dano menor, mas o privilégio da conta pode ofertar um ponto de entrada para um grande acesso ao sistema.

Root Comprimise *{root comprometido)* - É o comprometimento da conta root, ou similar. O termo "root" é derivado da conta do sistema UNIX que, tipicamente, tem acesso ilimitado ao sistema, ou de privilégios de superusuário. Intrusos que

possuírem direitos de root podem fazer qualquer coisa no sistema da vítima, inclusive rodar seus próprios programas, mudar o funcionamento do sistema e esconder seus rastros.

Packet Sniffer *(farejador de pacotes)*- É um programa que captura informações dos pacotes que trafegam na rede. Os dados podem incluir nomes, senhas, e informação proprietária que trafegam na rede sem criptografia. Além do conteúdo dos pacotes o sniffer pode ver quais tipos de pacotes estão sendo utilizados na rede. Assim fazem com que intrusos possam lançar freqüentes ataques no sistema.

Denial Of Service DOS *{negação de serviços)* - O objetivo do ataque de negação de serviço não é ganhar acesso não autorizado às máquinas ou aos dados, mas é impedir que usuários legítimos façam uso do serviço da rede. O ataque de negação de serviços pode chegar de várias maneiras. Ataques podem ser de inundação (flood), onde um grande volume de dados pode deliberadamente consumir o pouco ou limitado recurso disponível. Pode também interromper componentes físicos da rede que manipulam dados em trânsito, incluindo dados criptografados.

Exploitation of Trust *{exploração de confiança)* - Computadores em uma rede freqüentemente possuem relacionamento de confiança uns com os outros. Por exemplo, antes de executar alguns comandos remotamente, o computador verifica uma série de arquivos que especificamente executam o comando e quais os outros computadores na rede que possuem permissão para usar aquele comando. Se um ataque pode forjar a identidade de um computador, pode se beneficiar da relação de confiança que um computador possui em outro, assim podendo ganhar acesso não autorizado ao outro computador.

Malicious Code - Código malicioso é geralmente o nome de um programa, que, ao ser executado, pode causar resultados indesejados no sistema. Usuários do sistema usualmente não são conscientes do programa de código malicioso, até que se descubram os danos causados ao sistema. São considerados programas de códigos maliciosos os Cavalos de Tróia (Trojan horses), os vírus, e vermes (worms).

Cavalos de Tróia e vírus são usualmente escondidos em programas ou arquivos legítimos que o invasor tenha alterado, e que, ao executarem, realizam atos maliciosos, como apagar arquivos, enviar informações, etc.

Vermes são programas auto-replicantes que se alastram sem a intervenção humana. Vírus também são programas auto-replicantes, mas freqüentemente requerem alguma ação pela parte de um usuário para disseminar-se de forma não intencional em outros programas ou sistemas. Estes pequenos programas podem comandar uma séria perda de dados, queda de performance, negação de serviços, e outros tipos de incidentes de segurança.

Internet Infrastructure Attacks - Estes raros, mas sérios ataques, envolvem componentes chaves da infraestrutura da Internet, especialmente em sistemas específicos na Internet. Exemplos são servidores de nomes da rede, provedores de acesso, e grande sites de arquivos que muitos usuários dependem. Ataques na infraestrutura afetam grande parte da Internet e podem impedir seriamente o dia a dia das operações de vários sites na Internet.

3.3 Uso malicioso das características da arquitetura TCP/IP

Muitos dos ataques conhecidos exploram as características dos protocolos, como por exemplo, do TCP em sua característica de handshake, para realizar sondagem em redes ou ataques DOS.

As redes locais em sua maioria utilizam o padrão ethemet, o qual trabalha com difusão de pacotes, facilitando a escuta dos pacotes por outros hosts. A escuta do segmento de rede pode ser utilizada de forma maliciosa para descobrir dados importantes para os invasores.

Existem inúmeros softwares de escuta de segmentos e muitos são conhecidos como sniffer (farejadores). A placa ethemet é executada em modo promíscuo para captura dos pacotes da rede. O TCPdump é uma ferramenta de análise de tráfego da plataforma Unix que coleta dados da rede, decifra os bits e exibe a saída de maneira semi coerente, isto é, de maneira mnemónica, para que possam ser lidos os dados que são dados binários. O TCPdump também possui uma versão Windows chamada Windump. A saída deste software é bastante coerente e conhecida e quase padrão. No descrever dos pacotes usará a notação deste software.

Os invasores exploram o handshake do protocolo TCP para realizar sondagem em uma determinada rede para saber quais serviços estão disponíveis, ou até mesmo qual o sistema operacional está sendo utilizado em um host determinado.

A exploração do handshake pode ser feita de várias maneiras, a automatização de varredura, que foi inicialmente implementada Floyde, na ferramenta chamada Nmap. O Nmap envia uma série de pacotes forjados e através dos pacotes resposta do host alvo, concluir informações como, qual sistema operacional, que serviços está em execução no alvo e compartilhamentos disponíveis, para aquisição de alvos mais específicos. (MCCLUDE, SCAMBRAY e KURTZ aprud FLOYDE, 2000).

As varreduras podem ser classificadas nos seguintes tipos:

Varredura de conexão TCP: esta varredura se conecta a porta do host alvo, realizando todas as três etapas do handshake. (SYS, SYS/ACK, ACK);

Varredura TCP SYS: nesta varredura a conexão não é completada, o intruso emissor forja um pacote com fiag SYS e o envia para uma porta TCP do computador alvo;

Se o computador destino responder um pacote com fiag RST/ACK significa que não é uma porta que esteja na escuta, isto é, não possui nenhum serviço anexado a porta; se responder um pacote com fiag SYS/ACK pode-se deduzir que esta porta está escutando e existe um serviço na porta correspondente;

Varredura TCP FIN: Consiste em enviar um pacote FIN para a porta alvo. O host alvo deve responder um RST para uma porta fechada, baseada na RFC 793 Normalmente funciona em pilhas TCP/IP baseadas em UNIX;

Varredura TCP de árvore de Natal: Esta técnica consiste em enviar um pacote FIN, URG e PUSH para a porta alvo. O sistema que possuir a determinada porta fechada deve responder um RST, conforme a RFC 793;

Varredura TCP nula: Esta técnica desHga todos os fiags, com base na RFC 793; o sistema deve responder um RST nas portas fechadas;

Varredura ACK: consiste em enviar um pacote de flag ACK para o host alvo que responderá um RST para as portas fechadas ou abertas;

Varredura UDP: Envia o pacote a uma porta UDP alvo. Se o alvo responder com uma mensagem ICMP "ICMP port unreachable", a porta destino está fechada; se não responder, a porta está na escuta.

Os ataques podem se beneficiar de conexões TCP realizando escuta, e através da escuta coletar informações para tentar clonar a conexão. As informações de interesse são;

Número IP - Estes números são fixos do início ao final da conexão;

Números de Portas - O TCP estabelece portas para conexão de origem e destino; as portas não mudam durante a conexão;

Número de seqüência - Este número identifica a seqüência TCP, e é variável em relação ao ISN (número de seqüência inicial) e ao número agregado de bytes enviados de um computador para outro.

Número de acknowledgement - Este número muda em relação aos números de seqüências do segmento enviado a estação destino. A estação destino envia uma confirmação para a estação emissora confirmando o recebimento de um segmento.

Com posse destas informações, o invasor pode se passar por um computador autorizado e invadir uma sessão, que pode ser uma de alta autoridade, com acesso à raiz do sistema.

A característica de fragmentação do datagrama IP também pode ser utilizada de maneira maliciosa.

Dois ataques muitos famosos utilizam-se da fragmentação, são elas: o Ping of Death e o Teardrop.

O ping of Death é um dos ataques mais notificados que se conhece; com um único pacote, que se transforma em aproximadamente 30 datagramas, o invasor pode congelar o sistema. Se o comando, Ping -l *65510 target. ip. address* for executado no Windows NT, tem-se a possibilidade do congelamento do sistema alvo.

O objetivo deste comando é exceder o tamanho máximo de um pacote ICMP, que é de 65535 bytes, travando o sistema que não tratar esta exceção.

O código a seguir mostra o rastro dos pacotes fragmentados deste ataque, no formato TCP dump: (NORTHCUTT, 2001)

```
12:43:58.431 pinger> target:        icmp:echo request (frag
4321:380@0+)
12:43:58.431 pinger> target: (frag 4321:380@2656+)
12:43:58.431 pinger> target: (frag 4321:38003040+)
12:43:58.431 pinger> target: (frag 4321:38003416+)
12:43:58.431 pinger> target: (frag 4321:3800376+)
12:43:58.431 pinger> target: (frag 4321:38003800+)
12:43:58.431 pinger> target: (frag 4321:38004176+)
12:43:58.431 pinger> target: (frag 4321:3800+)
```

```
...
12:43:58.491 pinger> target: (frag 4321 :380063080+)
12:43:58.491 pinger> target: (frag 4321 :380063456+)
12:43:58.491 pinger> target: (frag 4321 :380063840+)
12:43:58.491 pinger> target: (frag 4321 :380064216+)
12:43:58.491 pinger> target; (frag 4321 :380064600+)
12:43:58.491 pinger> target: (frag 4321 :380064976+)
12:43:58.491 pinger> target: (frag 4321 :380065360+)
```

Este ataque é antigo, os sistemas operacionais atualizados não são mais vulneráveis a ele.

O pacote IP pode ter 65535 bytes de extensão (RFC 791), incluindo o cabeçalho IP de aproximadamente de 20 bytes e ICMP de 8 bytes. Como já dito anteriormente, na maioria das vezes, a camada de interface implementa a tecnologia Ethemet que possui uma unidade de transferência máxima (MTU) de 1500 bytes. Os pacotes que excedem o tamanho máximo de transferência da camada inferior são fragmentados na origem, e remontados no destino.

> *"Note que é possível enviar um pacote de eco ilegal com mais de 65507 (65535-20 (IP) -8 (ICMP)= 65507) octetos de dados devido ao modo como a fragmentação é realizada. A fragmentação é baseada em um valor de deslocamento em cada fragmento para determinar o lugar que o fragmento individual deve ocupar na hora da remontagem. Assim no último fragmento, é possível combinar um deslocamento válido comum ao tamanho do fragmento, adequando tal que, o deslocamento mais o tamanho seja maior que 65.535. Como as máquinas típicas não processam o pacote até que tenham recebido todos os fragmentos e tenham tentado remontá-lo, há a possibilidade do estouro das variáveis internas de 16 bits, o que pode causar congelamento do sistema, reinicializações, drumps de kernel e coisas semelhantes. "*
>
> *(NORTHCUTT, 2001 apud http://sophist.demon. com. uk/vine/)*

Os invasores podem disfarçar suas varreduras, utilizando a fragmentação, ou simplesmente forjando fragmentos inconsistentes, como criando fragmentos de deslocamento o ou ainda enviando vários fragmentos de datagramas diferentes na tentativa de inundação, pois o computador alvo ficará aguardando os outros fragmentos.

O ICMP também é utilizado para varreduras e outros tipos de ataque. Uma das maneiras mais básicas de varredura é a utilização do PING, que é um pacote ICMP *echo* (resposta). Essas varreduras têm como objetivo a obtenção de alvos, e são feitas em blocos de endereços IP. Existem muitas ferramentas para automatizar as varreduras.

A varredura ping é apenas uma amostra do que o ICMP pode oferecer de informações para ataques. Obter a hora do sistema, através de uma consulta de TIMESTAMP, ou ainda, obter a máscara da rede com a mensagem ICMP ADDRESS MASCK REQUEST, assim o intruso envia pacotes com consultas ICMP para obter estas informações.

O redirecionamento do tráfego pode ser realizado através de um aviso ICMP malicioso, utilizando-se a mensagem ICMP REDIRECT, que permite que um roteador diga a um host emissor, que ele não é o melhor roteador para envio daquele tráfego ao destino. Se o computador que recebe esta mensagem possui algum sistema automatizado de adequação de tabelas de rotas, pode-se ter um host enviando o tráfego para algum lugar indesejado como, por exemplo, um outro roteador.

Os roteadores da CISCO não escutam a mensagem ICMP REDIRECT, pois este foi um ataque muito comum para estes roteadores, que ficavam com suas tabelas de rotas incorretas, muitas das vezes parando de funcionar. O fabricante optou pela medida de não mais interpretar este tipo de mensagem ICMP.

O serviço de DNS é alvo muito desejado pelos invasores, pois além fornecer dados sobre a rede, também pode interferir no serviço de nomes que outros serviços utilizam.

A transferência de zona não autorizada pode facilitar a obtenção de várias informações para os invasores.

A transferência de zona é o processo de sincronização dos dados de uma zona do servidor primário para o secundário, o servidor de backup. O servidor secundário atualiza seu banco de dados da zona a partir do primário. Esta transferência só deve ser realizada por servidores secundários verdadeiros e não para qualquer outro computador.

As versões mais atuais do BIND (Berkeley Internet Name Daemon), a partir da versão 8, permitem a restrição dos computadores na realização da transferência de zona, sendo possível à configuração de quais computadores podem realizar este processo.

MCCLUDE e SCAMBRAY (MCCLUDE & SCAMBRAY, 2000) apresentam as contra-medidas para que a transferência de zona não seja realizada, citando a inibição do tráfego TCP na porta 53. Já NORTHCUTT fala que a restrição

nesta porta pode inviabilizar consultas DNS legítimas, uma vez que as consultas longas ao DNS (com resposta com mais de 512 bytes) são realizadas via porta 53 usando o protocolo TCP.

Os registros HINFO do DNS podem fornecer até a identificação do sistema operacional do computador alvo. Os computadores que consultam o DNS confiam nas informações enviadas por ele, mas se o servidor DNS for comprometido ele pode informar um IP diferente do servidor de e-mail ou web. Em alguns casos, o endereço indicado pelo DNS comprometido pode conter um clone do site ou do servidor de correio eletrônico, possibilitando a captura de diversas informações que o usuário disponibiliza, acreditando estar no endereço correto. Pode-se prevenir este problema utilizando-se o DNSSEC (DNS Security Extensions), que fornece um mecanismo de autenticação baseada nas assinaturas criptográficas, para validar a integridade da origem dos dados DNS.

3.4 Os Ataques

Existem mais de 2000 ataques diferentes registrados pela CERT. O trabalho não irá descrever todos, apenas os mais conhecidos e mais graves.

3.4.1 Smurf

Este ataque explora a capacidade do ICMP de enviar tráfego ao endereço de difusão. O objetivo é um ataque de negação de serviço no host alvo. Baseando-se em muitos hosts responderem uma única requisição de ICMP eco enviada a um endereço de difusão, pelo atacante. Este envia a requisição ICMP ao endereço de difusão com o endereço de origem forjado, para que todos os hosts membros do endereço de difusão respondam ao endereço que solicitou a resposta através do pacote ICMP.

O ataque é realizado em várias etapas;

Primeiro um usuário malicioso envia várias solicitações ICMP eco ao endereço de difusão, com um endereço de origem forjado, o endereço do computador vítima;

A segunda etapa seria o site intermediário permitir a difusão, Se o site intermediário possui muitos hosts, todos irão responder ao computador vítima;

Se o site alvo possui uma conexão lenta, a vítima será inundada, como mostra a figura 3.2

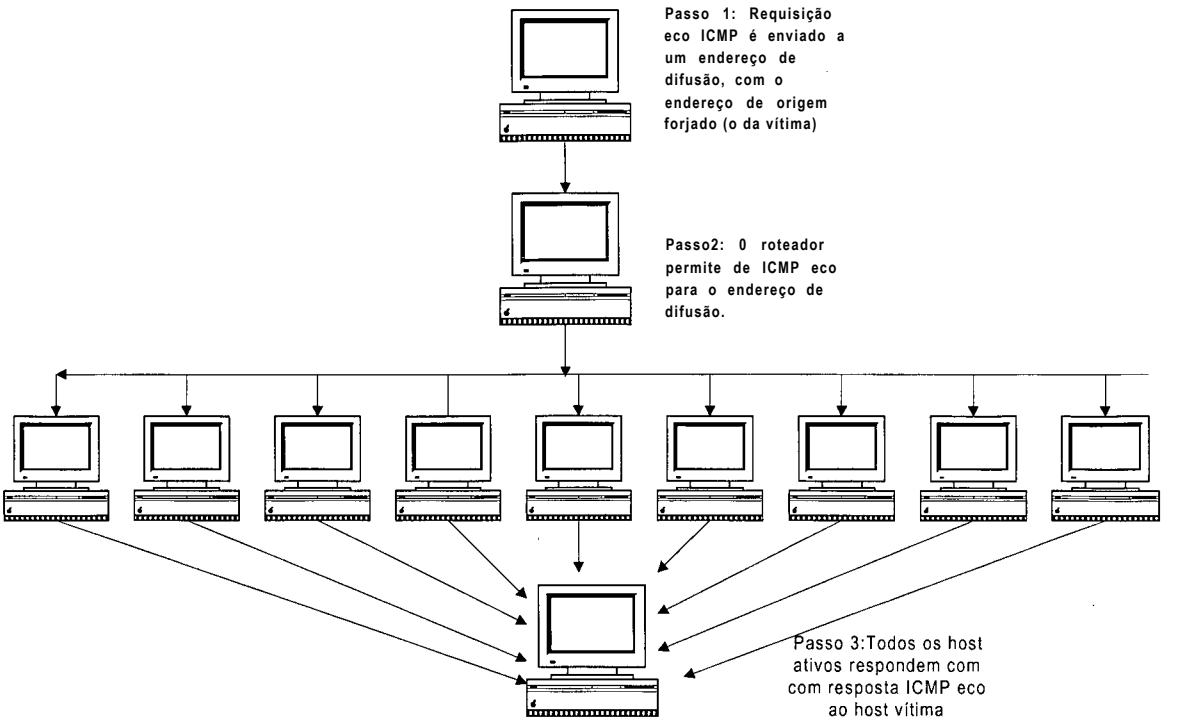

Figura 3.2 - Ataque Smurf

3.4.2 DDOS

Ataque de negação de serviço distribuída é um dos ataques mais temidos. Consiste no envio indiscriminado de tráfego em um computador alvo, visando causar indisponibilidade dos serviços oferecidos por ele. Este ataque utiliza um conjunto de computadores comprometidos, que são utilizados para lançar o ataque.

No ataque smurf um computador utiliza um IP forjado para enviar mensagem para rede intermediária. No ataque DDOS vários computadores coordenam os host comprometidos, tentando dificultar a identificação da origem do ataque. Os programas Trinno, TFN, TFN2K, Stacheldraht, Mstream e Shaf são utilizados para a realização deste ataque.

Os ataques Distributed Denial of Service são o resultado da conjugação de dois conceitos a negação de serviços e intrusão distribuída. Os ataques DDOS podem ser definidos como ataques DOS diferentes partindo de várias origens, disparadas

simultaneamente, e coordenados sobre um ou mais alvos, é vim ataque DOS em larga escala. (HARKCER n° 1, 2001)

Os primeiros ataques DDOS ocorreram em 1999. Mas foi no período de 7 a 11 de fevereiro de 2000, que se tomaram mais conhecidos. O ataque deixou inoperantes por algumas horas sites como Yahoo, Ebay, Amazon e CNN, também foram atacados sites brasileiros como UOL, Globo e IG.

3.4.3 RingZero

O RingZero é um cavalo de tróia que realiza sondagens em hosts aleatórios nas portas 80, 8080 ou 3128, procurando servidores proxy da Web. Quando encontrados eram enviados a um site FTP. A intenção do coletor provavelmente era de atacar a lista de servidores proxy da sua coleta.

3.4.4 Ataque Tribe Flood Network

Como descrito anteriormente este ataque é um DDOS, que se inicia na rede intermediária para ampliação como mostrado na figura 3.3. Os host daemmon são host comprometidos, que se comunicam com o host master através de resposta ICMP eco. A inundação é feita pelos hosts daemon (da rede intermediária), desta maneira viabilizando uma inundação UDP ou SYS TCP. Os computadores da rede intermediária são comprometidos através de um cavalo de tróia, que executa nestas estações um serviço que recebe comandos do computador master e os executa.

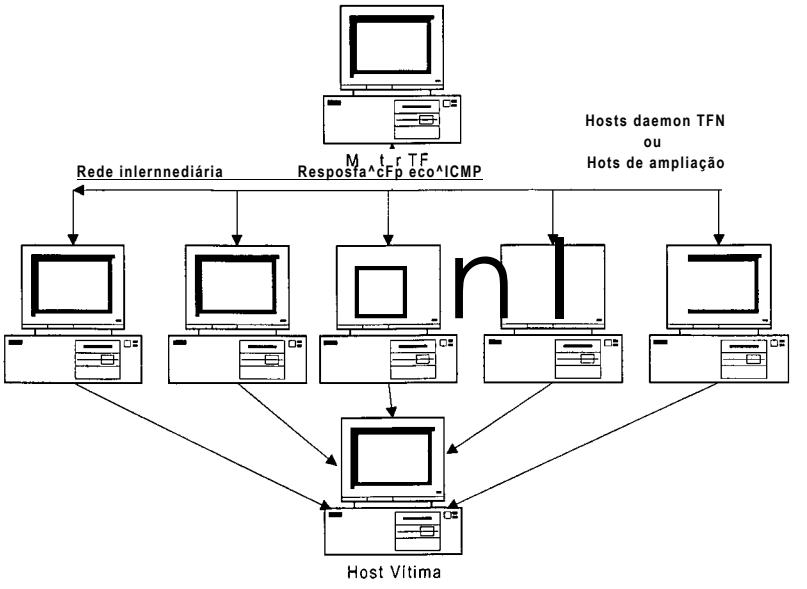

Figura 3.3 - Ataque Tribe Flood Networking

3.4.5 WinFreezze

Este ataque funciona apenas em computadores suscetíveis Windows. O atacante geralmente responde aos pacotes enviados pelo computador alvo, com pacotes forjados com mensagem ICMP redirect, que informa a um host emissor que ele tentou usar um roteador inadequado. O computador emissor ao receber a mensagem forjada inclui um "melhor" roteador em sua tabela de roteamento. O ataque pode levar hosts Windows NT vulneráveis a sofrer uma negação de serviço ou a diminuição da performance deste computador.

3.4.6 LOKI

É um cavalo de tróia que utiliza o protocolo ICMP para trocar mensagens entre a aplicação cliente e a servidora. Para que este ataque funcione é necessário que a aplicação do cavalo de tróia servidor esteja instalado no host vítima, para que um cliente LOKI solicite e receba dados do servidor, as solicitações geralmente requerem o envio dos arquivos de senhas, para acesso irrestrito do invasor a esta máquina. Desta maneira, utilizando o ICMP, a aplicação LOKI tenta camuflar o tráfego destas informações.

3.4.7 Spoofing ou Spoof

Esta técnica consiste que o atacante se faça passar por um computador autorizado, para se beneficiar de uma relação de confiança existente entre dois computadores. O primeiro passo consiste que o invasor escute o tráfego entre os dois computadores vítimas "A" e "B". Em seguida derrubar o computador vítima "B", através de um ataque de inundação tipo SYS. Como este computador fica impossibilitando de responder, o invasor prevê, com base na escuta anterior, o número das seqüências do tráfego TCP, se fazendo passar pelo computador B. A figura 3.4 demonstra a esquema do ataque.

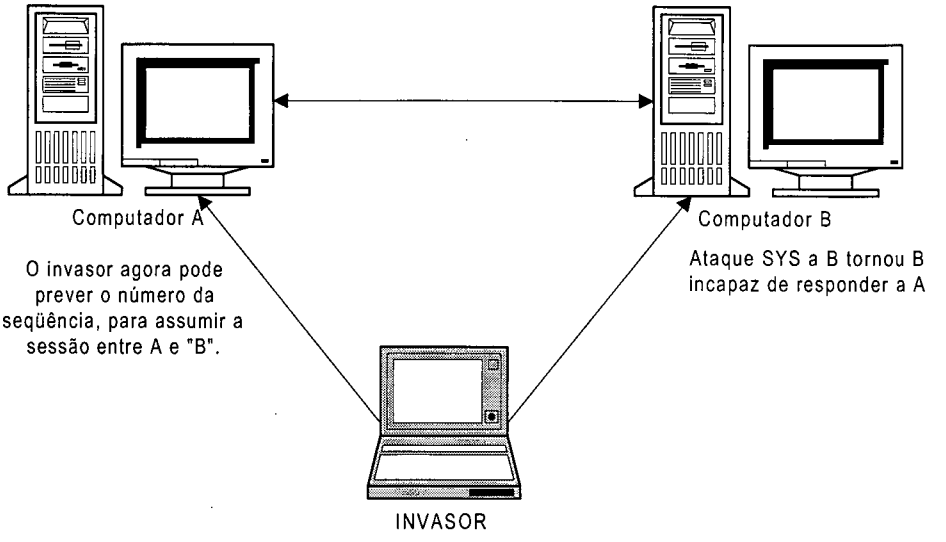

Figura 3.4 - Spoofing

Algumas variações desta técnica são o DNS Spoof, e o IP Spoof O DNS Spoof realiza este ataque ao servidor de nomes para modificar os registros do servidor. O IP Spoof muda seu IP para o IP do servidor para explorar a relação de confiança entre A e B.

Nem todos os sistemas operacionais são suscetíveis a este ataque; comumente aqueles que implementam a pilha TCP/IP completa podem ser vulneráveis.

3.4.8 Nuke, WinNuke ou OOBNuke

O objetivo deste ataque é a "tela azul da morte", e é e bastante comum de ocorrer em máquinas Windows. O ataque consiste no envio de um pacote forjado para a porta TCP 139 com flag definido *Out of Band (OOB).* Como o sistema não tem como

tratar esta exceção, então exibe mensagem de erro, na conhecida tela azul da Microsoft, paralisando o sistema.

3.4.9 Land

A característica principal do ataque é enviar um pacote forjado ao computador vítima com IP de origem e destino iguais. Alguns sistemas operacionais não implementam fùnções para tratamento deste erro e em conseqüência, há o travamento do sistema.

3.4.10 XmasTree

O ataque define o envio de pacote forjado com todos os flag com bits 1, e pode fazer o sistema parar ou ficar mais lento.

3.4.11 BackOrifici

O BO é um cavalo de tróia que consiste em uma aplicação cliente servidor para o Windows e que permite que o cliente (invasor) monitore e administre a máquina servidora. O cliente fica com total controle da máquina, vendo, inclusive o que o usuário digita no teclado, podendo até intervir nas ações. A instalação do servidor no host vítima é silenciosa e o usuário não percebe. Este aplicativo roda na porta TCP 31337. Esta porta é bastante conhecida e, lida em um espelho, mostra as letras da palavra ELEET, a “elite dos hackers”.

3.4.12 Ataque de falhas de segurança em aplicativos de serviços.

Muitos aplicativos possuem falhas de segurança que podem ser exploradas por invasores. Descreve-se, a seguir, algumas destas falhas de aplicativos, para ilustração.

O **Wu-FTPD** é um software FTP para Linux e variantes. O programa recebe sinais após o caractere“-”isto é, o comando passado a FTPD pode ser interpretado após o hífen, no caso de envio de um arquivo com “ə“ no inicio, o comando será interpretado. Usando este mecanismo é possível explorar executando qualquer comando no alvo. (MONTANARO, 2001).

SendMail é um software servidor de e-mail muito conhecido, possuindo vulnerabiUdade em suas versões 8.2.x. Na opção de linha de comando (commandline), o parâmetro -d que seta o nível de debug a ser utilizado, a opção é passada internamente ao programa para uma variável que foi declarada do tipo inteiro com sinal positivo, sem verificação posterior para aplicação. Caso seja remetido um valor negativo, o valor é passado para o server como um índice de vetor. Quando negativo irá escrever em áreas de memória não permitidas, possibilitando ao atacante o privilégio de root em comandos arbitrários no sistema, tomando assim o host vulnerável a ataques. (MONTANARO, 2001)

Redes Windows 9x. A senha de compartilhamento é fraca e avisa quando o usuário acerta o primeiro caracter, facilitando a utilização de programas que quebram senha na força brata. A Microsoft disponibilizou em seu site a correção, mas mesmo após a instalação do path de correção, se forrem utilizadas senhas pequenas o cracker facilmente quebra a senha. Não citando aqui a vulnerabilidade para o viras Ninda. (MONTANARO, 2001)

PWS Personal Web Server. Este aplicativo, bastante conhecido do Windows 9x, como o nome diz é um servidor http pessoal para disponibilizar arquivos e documentos. Se for adicionado "..." pontos, passa para o diretório anterior. Se o host possui habilitado busca em pastas e execução de scripts, o atacante pode executar programas mahciosos. (MONTANARO, 2001)

Muitos dos ataques são explorações de bugs das aplicações que os hackers identificam, ou usam maliciosamente características dos protocolos. Outros tipos de ataques comuns são decorrentes da má instalação e configurações de softwares por parte dos administradores, que utilizam instalações padrões com configurações inseguras, ou até mesmo deixam configuradas senhas padrões dos aplicativos. Deixam assim margens para ataque.

O questionamento de como defender tantos ataques é inevitável, e as técnicas utilizadas atualmente são descritas no próximo capítulo.

4. Técnicas e Mecanismos de Segurança.

Não existe um sistema totalmente seguro, como não existe casa, cofre ou banco invioláveis, mas pode-se dificultar bastante a jornada dos atacantes, fazendo com que eles desistam, ou simplesmente não consigam as informações que procuram.

> *"A segurança deverá ser proporcional ao valor do que se está protegendo. Parte desse valor é realmente um valor; outra parte é o trabalho necessário para restabelecê-lo; uma outra parte mais sutil é o trabalho que permitirá confiar em sua rede novamente (WADLOW, 2000).*

Muitos autores falam de proteger o que se tem de valor, mas existem atos que não possuem valor, como por exemplo, uma empresa ser acusada de participar de um ataque a um banco onde foram roubados alguns milhões. O preço de um processo deste é arriscado afirmar.

É importante notar que, mesmo que não exista nenhum arquivo de valor a defender, os atacantes podem utilizar os computadores como pontes para outros ataques. Um pensamento comum em alguns administradores de rede é que, se não tem nada de valor, não é necessário se preocupar com a segurança. Esta linha pensamento é errada, pois existem ataques apenas para indisponibilizar os recursos da rede, que o hackers podem fazer por simples maldade ou curiosidade, além da possibilidade dos recursos das redes vulneráveis serem utilizados em outros ataques.

As propriedades da segurança são:

Confidencialidade: Medida que serviços e/ou informações estão protegidos contra o acesso de estranhos. Tem como o objetivo de manter a confidencialidade e proteger informações privadas, evitando escuta ou cifrando as informações, e somente disponibilizando as informações para usuários autorizados.

Autenticidade: Medida que serviços e/ou informações estão protegidos contra a personificação por intrusos, com objetivo de reconhecer assinaturas, evitando que intrusos façam uso da engenharia social, ou que exista abuso de confiança;

Integridade: Medida que serviços e/ou informações estão protegidos contra a modificação ou deterioração causadas por intrusos. Como objetivo evitar que arquivos logs sejam alterados e forjados;

Disponílibilidade; Medida que serviços e/ou informações estão protegidos contra a recusa de provisão ou acesso provocada por intrusos, devem ser evitadas ações de bloqueio à rede.

Em vista das vulnerabilidades e ameaças às redes, sendo pela vulnerabilidade dos sistemas ou características de difusão das redes locais, não se deve esquecer que o elemento humano também falha, isto é, nem todas as vezes a causa é incompetência, mas sim falta de treinamento, falta de tempo ou falta de ferramentas para auxílio de suas atividades.

A segurança é um processo que deve ser aplicado repetidamente para a manutenção de segurança confortável. Se não houver avaliação do processo ao longo do tempo, o nível de segurança pode diminuir, pois à medida que o tempo passa, os atacantes organizam outras técnicas para burlar a segurança.

(WADLOW, 2000) compara este processo com a tríade grega, que consiste na análise, síntese e avaliação, como ilustrado na figura 4.1.

Análise: levantamentos de dados para identificação dos problemas;

Síntese; solução do problema levando em consideração as ferramentas disponíveis;

Avaliação: verificar se a solução proposta soluciona o problema.

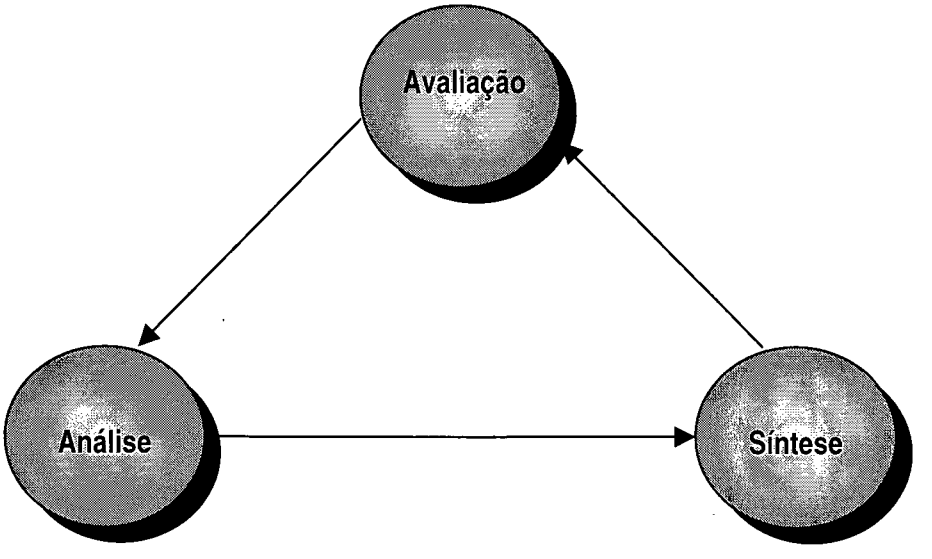

Figura 4.1 - Tríade Grega

4.1 Firewall

Um firewall é um sistema que impõe uma política de controle de acesso entre duas redes - como uma LAN privada e a Internet, e determina quais serviços internos podem ser utilizados e vice-versa. Como o nome diz, é um muro de fogo contra os invasores da rede externa.

Apesar de aparentemente o firewall significar um "muro de fogo" este possui mecanismo para bloqueio e permissão do tráfego, isto é, não bloqueia todo o tráfego, permite permeabilidade do fluxo autorizado. Oferece um ponto único de restrição entre a rede pública e a rede privada.

Os firewalls possuem regras para o controle de tráfego, que são definidas de maneira que ataques e sondagens não trafeguem na rede interna.

4.1.1 Finalidades básicas de um Firewall

A instalação de um firewall em uma rede tem como objetivos:

- Restringir o tráfego de pacotes da rede externa para a rede interna, dificultando a ação de intrusos;
- Ocultar informações sobre a rede interna e métodos de defesa, isto é, dificultar que o invasor sonde a rede interna, analise a topologia, e outros elementos da rede. O firewall é o ponto de acesso da rede interna à rede externa e o ponto de acesso da rede externa à rede interna, como mostra a figura 4.2;
- Restringir o tráfego de saída, controlando a saída do tráfego interno.

O tráfego direcionado pelo firewall à rede interna e externa pode ser configurado, isto é, a política de segurança pode controlar o tráfego como, e-mail, arquivo transferido, login remotos e outros tipos de troca de informações de aplicativos.

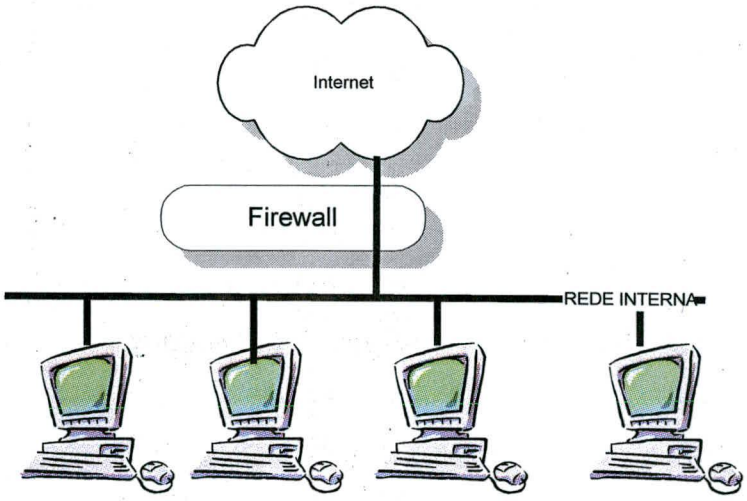

Figura 4.2 - O firewall geralmente separa a rede Interna da Internet

Um firewall muito raramente é um simples objeto, embora alguns produtos comerciais tentem colocar tudo em uma mesma caixa. (ZWICKY, 2000)

Firewalls baseados em roteadores/firmware

Alguns fabricantes colocam as funções de um firewall em um único equipamento, ou adicionam a roteadores a função de firewall através de opções de software ou firmware, para a realização da tarefa. É necessário cuidado para que roteador não fique sobrecarregado.

Alguns destes equipamentos, além das características de firewall podem também possuir funcionalidades de VPN (Virtual Private Networkig), filtragem de conteúdo e proteção contra vírus. Geralmente este tipo de solução é cara, possuindo a desvantagem da difícil atualização e up-grade conforme o crescimento da rede interna e números de acessos da rede externa.

Firewall baseados em software.

Estes firewalls são aplicativos executados em sistemas operacionais de rede como Unix, Linux e Windows NT. Pode-se considerar o valor do sistema operacional como custo, mas alguns são freeware. Neste aspecto existem muitos aplicativos, desde simples filtros a aplicativos sofisticados e complexos. É claro que estes aplicativos estão suscetíveis à falhas do sistema operacional, mas a atualização contínua do sistema operacional e paths de segurança diminuem a vulnerabilidade. Por outro lado, existe a facilidade de atualizações de filtros e up-grades conforme o crescimento de números dos acessos à rede.

É fundamental a atualização do sistema operacional, para correção de falhas de segurança, como também dos filtros ativos, para cobrir falhas recém descobertas na segurança.

4.1.2 Políticas de Filtragem

A política de filtragem de um firewall é governada por duas antíteses: negar tudo ou permitir tudo.

Prudente ou Negar tudo: A política do firewall é negar tudo o que não for especificamente permitido. Significa que as regras devem ser escritas para tudo que é permitido, se o tráfego http é permitido, a porta TCP 80 é aberta para o tráfego. Neste tipo de política a chance de ser atacado por um tipo de ataque não conhecido é menor. Este é o método mais indicado para filtro de pacotes. A desvantagem é que qualquer novo serviço ou aplicativo que se queira utilizar na rede interna para externa deve ter regras específicas no firewall para permissão. Às vezes alguns usuários não ficam satisfeitos porque querem utilizar algum software novo, e ele não funciona, até que se comunique com a equipe de segurança para análise da ferramenta, para posterior liberação do tráfego.

Permissiva ou Permitir tudo: A política do firewall é permitir tudo o que não é especificamente negado, as regras de filtragem devem ser escritas para tudo que é proibido, como por exemplo, o site não permite conexões telnet da rede externa então deve existir uma regra proibindo conexão TCP porta 23. Esta é uma política arriscada, mas algumas instituições podem achar que a liberdade e fiexibilidade são mais importantes que a segurança, como é o caso em laboratórios ou instituições de ensino. Esta política possui maior dificuldade para a defesa da rede que a anterior.

É aconselhável, quando está política for adotada, agrupar os computadores administrativos ou aqueles que possuem informações relevantes em um segmento mais protegido.

Veríssimo descreve outras duas políticas a de Paranóica e Promíscua:

Paranóica: Algumas instituições ficam receosas em conectar suas redes na Internet, possuem uma política paranóica de que ao se ligarem à rede irão ser invadidos,

Promiscua: quando tudo é permitido, não existe preocupação com a segurança, a rede não possui um firewall. (VERÍSSIMO, 1999)

4.1.3 Níveis de filtragem

O firewall pode filtrar o tráfego nos dois sentidos, tanto o da rede interna para a externa, quanto da rede externa para interna. O tráfego de entrada, como pode representar ataques, geralmente é tratado mais cuidadosamente. Existem três tipos de filtragem:

Filtragem por bloqueio, quando qualquer dado não solicitado deve ser bloqueado.

Filtragem pelo endereço do remetente e destino

Filtragem pelo conteúdo da comunicação

O nível de filtragem, que pode ser realizado como um processo de eliminação, pode ser verificado da seguinte maneira:

Primeiro: verifica se aquela transmissão foi solicitada pelo usuário; se não, rejeita.

Segundo: se a transmissão foi solicitada o site de envio é um endereço confiável: se sim, aceite; se não, rejeite;

Terceiro: o conteúdo é permitido: se sim, envie; se não, rejeite.

4.1.4 Os tipos de Firewall

A ICSA (International Computer Security Association) classifica os firewall em três grandes grupos: Firewall de filtragem de pacotes, servidores proxy de aplicativos e firewall SPI (Stateful Packet Inspection).

O Firewall de Filtragem de Pacotes

Este firewall tem como base regras de filtragem permissivas ou restritivas, conforme a política de segurança adotada. Cada pacote é analisado e verificado as informações nos cabeçalhos dos protocolos, endereço IP de origem e destino; portas UDP e TCP, e mensagem ICMP fragmentadas. As restrições podem ser tão rigorosas ou flexíveis quanto o administrador indicar.

Um roteador de rede pode ter condições de filtrar o tráfego por endereço, que pode ser burlado pelo IP spoofing.

Há necessidade de grande cuidado nas regras de filtragem, pois a inclusão de uma regra má definida, pode anular várias outras, deixando brechas na segurança. Os administradores necessitam conhecer os novos ataques para criarem os filtros mais adequados, além de testarem continuamente os que tiverem em uso.

Servidores Proxy

Os servidores proxy de aplicativos autorizam conexões e examinam o fluxo de dados, forçando todo o tráfego de rede a passar por um aplicativo inteligente que é executado no sistema de firewall específico para esse serviço (FTP,HTTP, SMTP, etc). Este tipo de proxy controla funções no nível de aplicativo, fornecendo proteção contra ataques. Os servidores proxy podem fazer autenticação por usuário, possibilitando o controle de quais usuários tem acesso a que serviços, quando, e a que velocidade. Esta característica pode ser interessante para muitas organizações. Outra característica destes servidores é a de cache de tráfego http, aumentando a velocidade de resposta aos usuários e economizando largura de banda.

Firewall SPI

Este firewall é mais recente, a inspeção de pacotes é considerada mais avançada e segura; examina todas as partes de um pacote IP para decidir a negação ou não do pacote. Acompanha as solicitações de informações originadas da rede interna, para somente deixar os pacotes solicitados entrarem na rede interna, descartando os pacotes que não foram solicitados.

Os dados prosseguem para um nível superior de filtragem, determinando assim um estado para cada pacote, por isso o nome SPI - Statefiil Packet Inspection (inspeção de dados de pacotes).

Funções e recursos adicionais de um Firewall

Filtro de conteúdo: firewall que filtra o tráfego pelo conteúdo dos dados do pacote, através de strings, como palavras chaves, sendo possível evitar que usuários da rede intema vejam conteúdo pornográfico, pornografia infantil, violência e outros, existem produtos especializados com filtros somente com essa finalidade.

Muitos firewalls usam funções de VPN (Virtual Private Network) possibilitando que usuários na rede externa vejam o conteúdo da rede intema, fazendo que o tráfego passe pela rede pública criptografado.

Os firewalls podem ter a habilidade de procurar vírus no tráfego da rede, rejeitando os pacotes suspeitos.

Interface de rede: a grande maioria dos firewalls é multi-residente, possibilitando a separação física da rede interna da externa. O host onde está instalado o software do firewall possuindo duas interfaces de rede. Os endereços IP na rede externa ficam na interface externa, e os endereços IP da rede interna na interface interna.

Assim, as solicitações de comunicação dos endereços internos da rede para a rede externa necessitariam dos endereços de rede da interface externa, então os endereços internos são transformados através do NAT (Network Address Translation) em endereços válidos externos.

A translação de endereço além de esconder os endereços da rede interna, ajuda a preservar endereços IP válidos.

É necessário que o firewall possua desempenho para o processamento das regras e pacotes; quanto maior o tráfego, maior deve ser o poder de processamento do firewall.

Alguns softwares de firewall registram em um log as tentativas de conexão bem e mal sucedidas.

Estes logs possuem informações como, quem utilizou, a que horários, quais os endereços IP externos conectaram a rede interna e outras informações. Alguns firewalls possuem ainda capacidade de alertar os administradores.

4.2 Conexões discadas

Alguns administradores de rede podem ser sentir seguros com a instalação de firewall em sua rede, mas existem outros pontos de entrada na rede como as conexões discadas, que podem servir como entrada para os invasores. É como trancar as porta e deixar as janelas abertas.

É um engano usuários se sentirem seguros ao utilizarem linhas telefônicas, pois podem ser alvo de escuta ilícita e meio para que outros usuários não autorizados possam conectar a rede. As conexões discadas devem possuir mecanismo de autenticação de usuários para certificar a autenticidade do usuário.

O call back é uma técnica bastante utilizada e consiste em interromper a ligação no momento que o usuário se identifica e o servidor ligar de volta para o número armazenado no banco de dados. Assim diminui-se a possibilidade de usuários não autorizados se conectarem.

4.3 *Criptografia* e *Comunicação Segura.*

A criptografia é bastante antiga, e consiste na técnica de "embaralhar" ou "substituir" os dados de maneira que o texto cifrado perca o sentido para quem não possui os métodos ou chaves para desfazer o processo.

Os militares foram os grandes incentivadores da criptografia. Uma técnica bem simples é a cifragem de mensagens com o deslocamento das letras do alfabeto. Por exemplo, considerando-se que um texto ser cifrado é "caba" e o deslocamento no alfabeto seja 2, a letra A será substituída pela letra C, a B por D, a C por E, e assim por diante. Então o texto cifrado será "ECDC", dificultando o entendimento do significado da palavra. Se o espião conseguir o conteúdo da mensagem, não conseguirá ler facilmente e, mesmo sabendo o método, também precisará saber que a chave é 2. (TANENBAUM, 1997).

É claro que a técnica apresentada é bastante simplificada, mas com advento dos computadores, as técnicas criptográficas ficaram muito mais complexas e seguras.

Não é comum o sigilo da técnica criptográfica, pois o segredo da criptografia não está na maneira como texto foi cifrado, mas na variável da técnica que cifra o texto, chamada de chave.

> *"Não é possível enfatizar o caráter não sigiloso do algoritmo. Ao tornar o algoritmo público, o especialista em criptografia se livra de consultar inúmeros criptólogos ansiosos por decodificar o sistema para que possam publicar artigos demonstrando sua esperteza e inteligência. Caso muitos especialistas tenham tentado decodificar o algoritmo durante cinco anos significa que o algoritmo é muito bom ''.(TANENBAUM, 1997).*

O tamanho da chave é fator de grande importância, chaves maiores aumentam número de possibilidades de chaves, chaves de 256 bits possuem milhões de possibilidades a mais do que as chaves de 64 bits.

Existem dois tipos de cifragem: de substituição e transposição. A primeira substitui um caractere ou grupo de caracteres por outro, a outra troca a ordem dos símbolos no texto, como se embaralhasse as letras.

Os tipos de algoritmos de criptografia são os de Chave Secreta ou simétrica, e Chave Pública ou assimétrica

Criptografia simétrica

Este sistema utiliza uma única chave para criptografar e descriptografar a mensagem, que deve ser compartilhada entre a origem e o destino.

Uma mensagem deve trafegar de maneira segura entre a origem e o destino. Na origem, o texto simples é cifrado por um algoritmo através de uma chave; desta maneira, a mensagem é transmitida ao destino, onde será decifrada por um algoritmo com a mesma chave anterior, como mostra a figura 4.3:

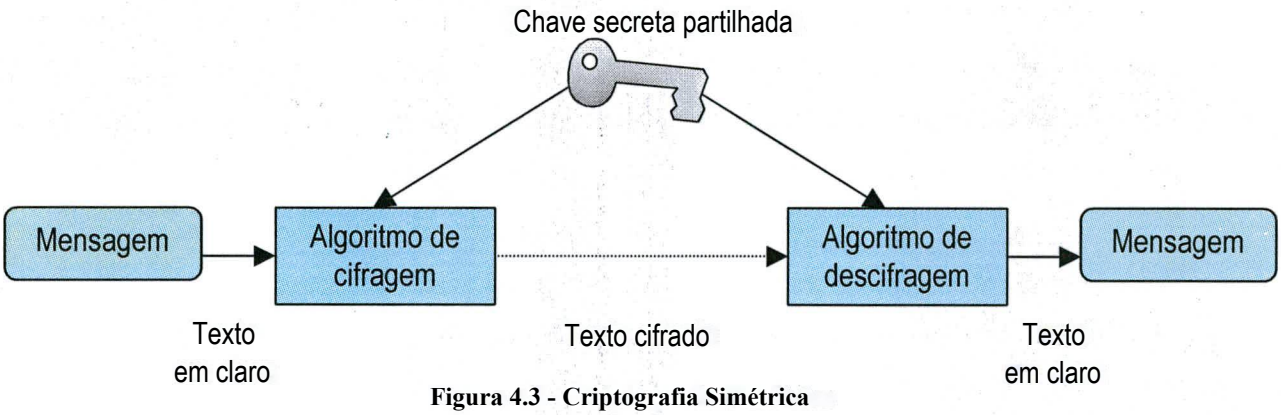

Figura 4.3 - Criptografia Simétrica

O DES - Data Encrytion Standart foi adotado pelo governo dos Estados unidos em 1977 como padrão para comunicação de informações. É a implementação de uma técnica de criptografia de chave simétrica que segundo Wayner não é atualmente seguro a não ser com modificações, como por exemplo, o Tri-DES. (TANENBAUM, 1997 apud Wayner, 1995).

Outra técnica de chave simétrica é o IDEA (International Data Encryption Algorithm) projetado por pesquisadores suíços que utiUza chave de 128 bits.

A desvantagem desta técnica de chave simétrica é que a chave deve ser compartilhada ou transferida, pois é necessário que o receptor e transmissor combinem a chave.

Uma vantagem desta técnica é o menor tempo de processamento em comparação ao método assimétrico, isto é, o tempo para cifrar uma mensagem com os algoritmos de chave simétrica é menor de que se a crifagem da mesma mensagem fosse utilizando algoritmos de chaves assimétricas.

Criptografia Assimétrica

A vulnerabilidade da técnica de chave simétrica é a chave, pois a mesma deve ser compartilhada entre o emissor e o receptor. A distribuição de chave é um ponto fraco do sistema criptográfico. Mesmo tendo um método robusto, o intruso poderia roubar a chave. A distribuição das chaves era um problema, pois ao mesmo tempo em que a manutenção das chaves protegidas era importante, a distribuição desta era necessária.

Em 1976 Diffie e Hellmam da Universidade de Stanford apresentaram um sistema diferente, onde as chaves de criptografia de descriptografia eram diferentes entre si, não podendo ser derivadas entre si.

A dificuldade de deduzir uma das chaves de posse de outra é enorme, então não existe necessidade de proteção das duas chaves, sendo possível a divulgação de uma delas, sem a perda de segurança. Uma seria chave pública e outra privada. A pública é disponível a todos e a secreta é mantida em segredo com o usuário.

Com duas chaves, não é mais necessária a troca de senhas entre o emissor e o receptor; cada um possui uma chave pública e uma secreta. Pode-se criptografar a mensagem com a chave pública e somente descriptografar com a chave secreta ou ainda, criptografar com a chave secreta e descriptografar com a chave pública, conforme mostrado na figura 4.4.

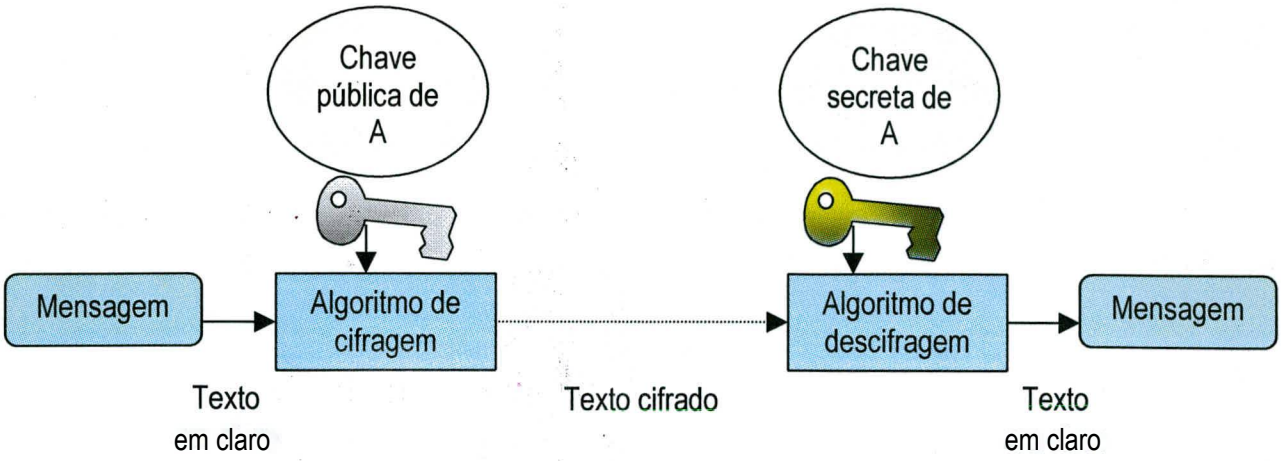

Figura 4.4 - Criptografia Assimétricas

Este método necessita de maior poder de processamento que o anterior, mas além da vantagem do não tráfego da chave, existe também a validação do emissor, através da assinatura digital; e a garantia de não alteração da mensagem, pois um caractere trocado comprometerá toda mensagem.

Além de oferecer sigilo, a técnica de chave assimétrica possui a característica de autenticação, de modo que o emissor, ao receber uma mensagem do receptor e tenha certeza que esta realmente se comunicando com o verdadeiro receptor, e não outro tentando se passar como receptor. Assim a criptografia também pode ser usada para permitir que as mensagens sejam assinadas, de forma que o transmissor não possa negar a identidade da mensagem após o envio.

O algoritmo conhecido é o RSA Rivest-Shamir-Adleman.

Nesta técnica pode-se assegurar a autenticidade do emissor e do receptor, além da confidencialidade da mensagem, isto é, se a mensagem for alterada no envio, do emissor para o receptor ela perderá a leitura da informação, quando do processo da descriptografia, o processo de envio da mensagem criptografada, de chave assimétrica é realizado da seguinte maneira:

O remetente 'A' cifra a mensagem com a sua chave secreta e cifra novamente com a chave pública do receptor, e envia a mensagem pela rede. O receptor 'B' recebe a mensagem que somente ele pode decifrar com sua chave secreta, e decifra novamente com a chave pública do emissor 'A'.

A gestão das chaves é fator de importância, pois de posse das chaves o sigilo é perdido. A distribuição das chaves é realizada por uma entidade chamada de *autoridade de certificação* (CA) ou cartórios digitais. A credibilidade de um sistema de chaves depende na medida direta da credibilidade da CA.

Os ataques à mensagens criptografadas podem ser realizados através da dedução de um erro do algoritmo de criptografia. Segundo Tanenbaum existe a necessidade da publicação e teste dos algoritmos, para que eventuais erros sejam descobertos e testes sejam feitos por diversos pesquisadores da comunidade.

As chaves têm em geral 40, 64, 80 ou 128 dígitos. E quanto maior a chave mais rígida a criptografia, isto é, maior é o esforço computacional necessário para viola-lá. (BENETT, 1997).

Atualmente as chaves utilizadas são maiores que 64 bits, e os ataques às senhas são ataques que testam sucessivamente combinação de caracteres e palavras. Este método é conhecido como método de *força bruta. A* utilização de senhas curtas e de palavras comuns facilita o trabalho de aplicativos de quebra de senha através da força bruta. O uso de senhas grandes e robustas, isto é senhas com mais de 8 caracteres e com caracteres especiais, pode-se tomar o trabalho de quebra de senha por força bmta bastante difícil, ou com que tempo de processamento aumente exponencialmente.

A criptografia não é somente utilizada no envio simples de mensagens; muitos protocolos de comunicação foram criados baseados em métodos de criptografia.

4.3.1 Os protocolos que utilizam a criptografia

IPsec (IP Security Protocol)

O IPsec é o protocolo projetado pelo lETF (Intemet Engineering Task Force) para trafegar dados seguros fim a fim através de Intemet ou de uma rede Privada. Muitos sistemas operacionais mais populares como Linux e Windows 2000 já possuem implementação para o IPsec. Alguns equipamentos, como roteadores implementam também o protocolo.

O tráfego de datagramas IP utiliza funções de segurança com autenticação e integridade através da criptografia, encapsulando o datagrama criptografado para transmissão.

O protocolo permite a um sistema selecionar protocolos e algoritmos de segurança, além de estabelecer chaves de criptografia, utilizando o IKE (Internet Key Exchange) que autentica os pares da comunicação, podendo utilizar diversas tecnologias, como, DES, MD5 (Message Digest 5), SHA (Secure Hash Algorith) e outros. Existe uma negociação do nível de segurança para escolha dos métodos ou protocolos criptográficos.

SSL (Secure Socket Layer)

O SSL foi desenhado em 1993 pela Netscape para prover encriptação de dados fim a fim, proteger a integridade, e autenticar servidores na web. Este protocolo fica acima do protocolo TCP na camada transporte. Possui várias versões como 1, 2 e 3. A versão 2 possui problema de vulnerabilidade, e é a versão conhecida como TLS (Transporte Layer Security), mas é o mesmo SSL.

HTTPS

É a utilização do protocolo HTTP em conjunto com o protocolo SSL que foi desenvolvido para fornecer uma camada de segurança entre a camada de transporte e os protocolos de aplicação como http.

S-HTTP

Extensão do http, fornece transações seguras incorporando criptografia e autenticação no protocolo http, dando um nível de segurança em transações fim a fim entre o cliente e o servidor web.

Existem outros protocolos menos conhecidos não citados aqui.

4.4 Virtual Private Netwok - VPN

As VPN são redes de dados privadas, similares às linhas privadas de comunicação de dados, que utilizam a infra-estrutura da Internet ou de outras redes públicas, oferecendo maior segurança às empresas. Utilizam técnicas de criptografia para assegurar que somente usuários autorizados possam utilizar os serviços da rede privada, dificultando a escuta dos pacotes e ataques.

É uma alternativa de baixo custo para interligar uma matriz com as filiais, com a vantagem que usuários remotos podem se conectar com a rede para utilizar os serviços.

Na implementação deve haver a preocupação de todos os dispositivos suportarem o mesmo nível de criptografia. O Data Encrypton Standart de 168 bitts (3DES) é uma boa alternativa, considerado atualmente inviolável, pelo menos até o momento.

A VPN é um túnel de dados encriptados origem destino. O tunelamento encapsula os dados em pacotes IP. (STARLIN, 2000)

Existem dois tipos de VPN, os realizados de rede privada para rede privada (LAN to LAN) e os de usuários conectados através de conexões discadas para a rede privada (Client to LAN)

LAN to LAN: é quando um roteador ou um Firewall, ao até mesmo um host, combinam ponto a ponto manter uma conexão com tráfego criptografado. A constituição desse fluxo criptografado, evita escuta do tráfego de informações sigilosas, como por exemplo: o firewall da matriz transfere dados para o Firewall da filial servindo como um gateway seguro em cada ponto. Cada equipamento toma-se uma das extremidades do túnel virtual de fluxo criptografado, desta forma, os usuários de ambas as LANs poderão utilizar o túnel de maneira transparente para se comunicarem entre si.

Client-to-LAN: consiste que um usuário remoto, ao acessar a rede coorporativa, criptografe o fluxo de informações trocado entre ele a conexão à rede privada.

4.5 Verificação da segurança

Após a instalação de alguns elementos que podem prover segurança, como o firewall, a certeza se a rede está ou não segura pode ser verificada através de teste automatizados no firewall e nos computadores da rede.

Os testes de verificação de segurança não devem ser realizados uma única uma vez. A realização de reavaliações rotineiramente é bastante importante.

Uma solução para os teste de confiança na segurança seria a contratação de um "tiger team" para testes de penetração, contudo, nem todos possuem orçamento para a contratação do "tiger team" rotineiramente.

Outra solução seria utilizar ferramentas de sondagem (probe), que consiste em uma escolha eficiente e econômica.

Algumas ferramentas de sondagem realizam a verificação automática de vulnerabilidades tanto da rede intema quando da externa, avaliando os riscos, e realizando aconselhamentos de como reparar as falhas encontradas.

A seguir, algumas das ferramentas de sondagem serão descritas:

> *"O Nmap é uma ferramenta para realização de auditoria e exploração de segurança de redes. Suporta ping scanner (para determinação de quais hosts estão "vivos " numa determinada rede), várias técnicas de port scanning (que determinam quais serviços determinados hosts oferecem) e TCP/IP fmgerprinter (para "adivinhação" de computadores remotos). Também oferece diversas outras opções como sunRPC scanning, decoy scanning e muito mais, sendo considerado como um dos mais rápidos e eficientes Security Scanner (verificadores de segurança) disponíveis. " (Revista do Linux, 2001).*

Nessus

É uma ferramenta de verificação de segurança remota para Linux, BSB, Solaris e outros UNIX, e utiliza plugins atualizados freqüentemente. Mais de 500 verificações de vulnerabilidades diferentes são realizadas. Este aplicativo emite relatórios em HTML, XML e outros e sugere soluções para as vulnerabilidades encontradas.

Fwlogwatch

Ferramenta utilizada para análise de filtro de pacotes IPChains. O IPChains é software de criação de filtro de pacotes, isto é,um software firewall para LINUX onde os filtros de pacotes são criados para que somente o tráfego autorizado penetre na rede intema. O Fwlogwatch analisa as regras de filtragem e logs do IPChains analisando anormalidades de configuração e vulnerabilidades da rede, possibilita a geração de relatórios em HTML ou TXT para simples impressão o publicação dos relatórios na web.

Apsend

Utilizado para testes em firewalls e outras aplicações de rede. Possui opção para SYS flood, ataque DOS LAND, DOS e outros.

Enterprise Security Manager - Symantec

È uma solução de gerenciamento de segurança. Verifica ativamente vulnerabilidades de segurança, avalia o risco para mais de 55 plataformas.

NetRecon Symantec

Analisa vulnerabilidades de rede e explora buracos de segurança.

System Scanner 4.2 da ISS

A ISS em 1994 desenvolveu o primeiro programa de identificação e reparos de falhas de segurança e atualmente possui inúmeros produtos na área de segurança. A ferramenta é de fácil instalação, está disponível para Windows NT e Windows 2000, e possui três módulos: Start Session, View report, e Administration Interface. Gera relatório no formato HTML, falhas de segurança, com possibilidade de agendar verificações, mas não realiza os reparos automaticamente. (SUGUIMOTO, 2001)

Outras ferramentas bastante conhecidas são, o SATAN, ISS scanner, e CyberCop Scanner.

Sentinelas

A verificação de logs e o controle do tráfego é uma batalha para os administradores de redes. A instalação de um software que automatize estas tarefas para auxílio da verificação de logs e análise do tráfego da rede e detecção de invasão da rede é de fundamental importância para a segurança das redes. O próximo capítulo falará sobre estas ferramentas conhecidas como IDS (Intrusion Detection System).

5. IDS - Intrusion Detection System: Componentes e Ferramentas

> *"Em tempos remotos, o administrador de rede carregava uma cruz nas costas. Não bastava apenas aplicar correções para os bugs que encontrava em listas de discussões ou mesmo adicionar regras em seus filtros de pacotes. Existia a real necessidade de algo mais. Algo que pudesse alertar em tempo real não só as tentativas de ataque, como também qual o método utilizado nas mesmas, tanto para fins de investigação ou a caráter de curiosidade" (NETO, 2001).*

Existem milhares de ataques atualmente, é bastante trabalhoso para um administrador de rede ou para uma analista de segurança saber todos de cor. Mesmo que ele se debruce para estudar todos os tipos existentes, não adianta, pois enquanto ele estuda, novos ataques estão sendo construídos. Também é muito difícil analisar todo o tráfego da rede através de logs e muito mais difícil verificar todos os pacotes da rede um a um.

É necessário automatizar este processo, disponibilizando ferramentas para os administradores, que o auxiliem na detecção de ataques nas redes.

Existem softwares de análise de tráfego para determinar os gargalos, erros, enfim o comportamento da rede, que emitem alertas aos administradores. Além da captura do tráfego, fazem gráficos para análise, mas são diferentes dos IDS, pois não são especificamente desenhados para detectar ataques.

Os Sistemas de Detecção de Intrusos são ferramentas para defesa da rede. De grande importância para os administradores da rede, pois nenhum administrador gosta de saber que foi vítima de um ataque pelos sintomas, tais como, serviços não funcionando ou arquivos apagados. No entanto, ataques não são fáceis de identificar sem uma ferramenta de monitoração ou de IDS.

As ferramentas IDS isoladamente não tomam a rede mais segura, mas é uma ferramenta considerável para os administradores incluírem no planejamento das políticas de segurança de suas redes.

"É uma rígida e ativa tentativa em descobrir ou detectar a presença de atividade intmsa". (BRUNEAU, 2001)

A detecção de intrusos tem como objetivos: detectar e identificar as ameaças diretamente direcionadas a uma organização, garantindo assim que os sistemas possam ser robustecidos contra as ameaças.

É necessário que os administradores tenham um controle sobre os aplicativos, host, e tráfego da rede, para diagnosticar os ataques.

Os IDS podem ser úteis tanto para a detecção de intrusos, quanto para testar os firewalls e identificar erros de configuração.

As organizações colocam a utilização de ferramentas IDS em terceiro lugar no investimento nos próximos 12 meses. A figura 5.1 mostra o gráfico de investimento de organizações americanas coletado por uma pesquisa de Network Computing em novembro de 2001.

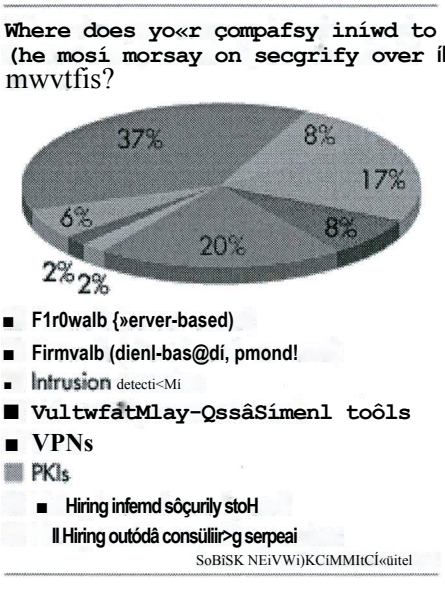

Figura 5.1 - Investimentos em Segurança

5.1 Um pequeno histórico

Em 1972 James P. Anderson publicou um artigo pela USAF sobre os problemas de segurança. Em 1980, James publica um estudo de linhas gerais de como melhorar a auditoria de segurança e inspeção nas redes de clientes: "How to use accounting audit files to detect unauthorizes access", tendo grande influência para o início da área de IDS. (BRUNEAU, 2001)

De 1984 a 1986 Doroty e Peter Neuman desenvolveram o primeiro modelo de detecção de intrusos em tempo real. O primeiro protótipo foi lançado e chamado de IDES (Intrusion Detection Expert System). No início IDES era baseado em regras.

No período de 1980 a 1990 o governo dos Estudos Unidos investiu em projetos na área de segurança. Projetos como, Discovery, Haystack, Multics Intrusion Detection and Alerting System - MIDAS, Network Audit Director and Intrusion Reporter -NADIR.

Com o passar dos anos, houve grande crescimento na detecção de intrusos, e muitas ferramentas foram desenvolvidas. Em 1990 duas das mais populares empresas da detecção de intrusão a Wheelgroup do Netranger e Internet Security Systems do RealSecure, desenvolvem os primeiros IDS baseados em rede.

A empresa Whellgroup comercializa um produto chamado de NetRanger; este produto procura no tráfego assinaturas de abuso, enviando alertas em tempo real e detalhes dos ataques furtivos que poderiam comprometer a rede. Em fevereiro de 1998 a Whellgroup foi incorporada pela Cisco, e nos tempos atuais, a Cisco comercializa o NetRanger.

A Internet Security Systems, Inc (ISS) iniciou suas atividades em 1994. Em 1996 a ISS lançou uma ferramenta para incrementar a segurança nas redes, baseada no reconhecimento de ataques em tempo real chamado RealSecure. Em agosto de 1997 lançou a primeira versão comercial chamada RealSecure 1.0 para Windows NT 4.0.

Atualmente estas ferramentas ainda estão sendo aperfeiçoadas e suas dificuldades são discutidas anualmente em uma convenção, em busca de soluções para problemas relativos a novos tipos de ataque.

Um ataque pode ser identificado por sua característica, por exemplo, se houver tentativas de conexão TCP em um host na porta 31337, provavelmente é um intruso tentando conectar, de algum modo num cavalo de tróia. Geralmente os cavalos de tróia são executados nesta porta.

O sistema de detecção de intrusos busca identificar, no tráfego, pacotes que tentam conexão TCP porta 31337. Ao detectar o pacote, a ferramenta gera um alerta sobre o provável ataque.

5.2 *Terminologias*

Como a detecção de intrusos é uma área muito nova, existem inconsistências nos termos, bem como discussões até mesmo sobre o termo, se o correto é "detecção de intrusos" ou se "detecção de ataques". Este trabalho usará o termo detecção de intrusos. (ALEN, et ali 2001).

Os termos utilizados na detecção de intrusos possuem origem na língua inglesa, muitas das vezes sendo de difícil tradução para um equivalente na língua portuguesa. Traduções de termos em inglês não são iguais em algumas publicações. A definição da terminologia de alguns termos tem como objetivo a diminuição da imprecisão na utilização de alguns. A segui alguns termos utilizados e suas definições:

Analysis approaches (Análise de aproximação) - é o mecanismo ou método pelo qual o IDS realiza a detecção ou não de ataques. As técnicas principais são a de assinatura e tráfego anormal.

Assinaturas: consiste na identificação do ataque através de um padrão como o TCP porta 31337, citado anteriormente. Estes padrões são procurados no tráfego, através de uma espécie de sniffer, que reconhece os protocolos e realiza busca das assinaturas.

Tráfego anormal: é todo o tráfego diferente do tráfego esperado, ou seja, é diferente do tráfego normal, ou do comportamento esperado. A maior parte do tráfego em uma rede é o tráfego normal, por exemplo, um host interno copiando arquivos de um servidor de arquivos ou uma consulta a servidores Web, etc. O tráfego anormal geralmente é produzido pelo invasor de maneira artificial através de scripts de software ou geradores de pacotes. Pode-se definir o padrão do tráfego normal, ou o comportamento esperado da rede, de duas maneiras: manual e automática.

O Tráfego Normal Manual: é gerado pelo administrador levando em conta: a rede IP utilizada, protocolos utilizados e quais serviços da Internet existem, e em que portas eles estão sendo executados. Desta maneira, se o administrador não possuir domínio sobre o comportamento padrão e conhecimentos de redes, a definição do padrão poderá ficar bastante prejudicada.

O Tráfego Normal Automático: existe quando a geração automática do padrão da rede é realizada pela captura do tráfego durante o comportamento normal da rede, de maneira estatística ou outros algoritmos.

Nem todo tráfego anormal é necessariamente um ataque, ele poderá ser ocasionado por um serviço mal configurado ou fora do padrão.

Ataque: é uma ação conduzida por um adversário, o intruso, contra outro adversário, a vítima. O intruso realiza um ataque com um objetivo específico em mente.

Para o administrador responsável por manter um sistema, um ataque é um conjunto de um ou mais eventos que podem possuir uma ou mais conseqüências de segurança; para o intruso, um ataque é um mecanismo para alcançar um objetivo. Muitos podem não achar perigoso ter seu servidor usado por um "scan" de portas, mas é uma atitude suspeita e poderá ser seguido por uma série de ataques mais perigosos.

Exploração: é o ato de explorar alguma vulnerabilidade do sistema.

Falsas positivas: é a identificação de um ataque que verdadeiramente não ocorreu, isto é, é a identificação de um ou mais pacotes como ataques, quando estes pacotes são legítimos e não representam nenhum ataque.

Falsas negativas: é quando um ataque ocorre, e o sistema não o identifica.

Regras: As regras são como o mecanismo de busca por assinatura, identificam os prováveis ataques como, por exemplo, gerar um alarme em todo o pacote TCP 31337.

5.3 Componentes Principais do IDS

Os três componentes principais do IDS são os sensores, o analisador e a interface com usuário. (NORTHCUTT, 2001)

Sensores: São componentes responsáveis em coletar dados. Os dados podem ser coletados em qualquer segmento da rede e, portando, é possível possuir vários sensores em uma só rede. O sensor coleciona e transmite os dados para os analisadores;

Analisadores: Recebem os dados de sensores e realizam uma análise para determinação da ocorrência de ataques. O resultado da análise dos dados serão os ataques identificados. Os diagnósticos devem ser acompanhados dos pacotes que levaram à conclusão da ocorrência de ataque. Este componente pode ou não tomar providências de contra-ataque.

Interface do Usuário. Esta interface é utilizada para a visualização dos resultados do modulo analisador.

Alguns autores (ALEN, 2001) e (NED, 1999) citam outros componentes como:

Honeypot: (Pote de mel ou isca) utilizado para atrair intrusos, fornecendo dados de vulnerabilidades incorretas, mas que na verdade funcionam, como um sensor.

Unidade de Resposta: As respostas a ataques e sistemas de detecção de intrusos vêm tradicionalmente sido pensadas como dois processos separados; entretanto, a linha entre eles está começando a obscurecer. Com o desenvolvimento e melhorias dos IDS, estes estão começando incorporar características para responder aos ataques. Nem todos os aplicativos possuem o módulo de resposta.

As respostas podem ser feitas de diversas maneiras. A mais freqüente é o envio de notificação ao firewall para suspensão do tráfego suspeito, ou ainda envio de alerta administrativo.

Banco de dados: Módulo de armazenamento de detecções anteriores.

Devido à grande variedade de modelos existentes foi criado o CIDF *(Common Intrusion Detection Framework)* (CID, 1999). Este modelo agrupa um conjunto de componentes que são: o Gerador de Eventos (E-box) ou sensores, os Analisador de Eventos (A-box), a Base de Dados de Eventos (D-box), e a Unidade de Resposta (R-box), como mostra a figura 5.2

Fonte: (Oliveira, 2001).

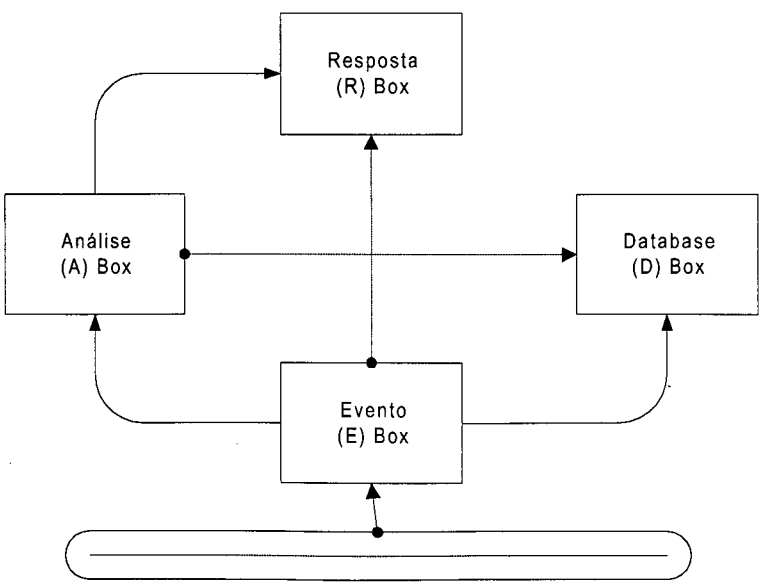

Figura 5.2- Componentes IDS

5.4 Tipos e Hierarquia de IDS

A maioria dos autores (NORTHCUTT, 2001) define o IDS somente como host e rede, mas Alen (ALEN, 2001) classifica os IDS conforme o tipo de dados que este analisa. Como a abordagem de ALEN é mais abrangente será mais interessante abordá-la:

Aplicação: Sistema que examina o comportamento das aplicações, geralmente analisando o log de aplicações do sistema operacional ou outros aplicativos como servidor web, de correio, etc.

Host: Este sistema examina a data dos arquivos, alterações de tamanho, quantidade e log do sistema; processa as informações de contas, ações de usuários e saídas do sistema para identifica possíveis alterações ilegais. Como exemplo, detectar um arquivo que misteriosamente apareceu em um diretório, sem nenhum registro dos usuários de inserção deste.

Networking: Sistema de detecção de intrusos de redes, examina o tráfego da rede. É o tipo mais comum atualmente.

Multi-networkig: geralmente tem a forma de "in team" de resposta a incidentes (IRT- an incident response team), quando a entrada de um sistema vem de sites dentro de seu domínio. Dados comunicados por este tipo de IDS são geralmente de aplicações, host, network ou outros multi-networkig.

O nível hierárquico dos tipos de IDS é o apresentado, isto é, o menor nível hierárquico é o de aplicações, o de host, de rede é o nível intermediário e do de maior nível hierárquico é multi-networking.

5.5 Limites de Observação inerentes a redes

O IDS tem como objetivo analisar todo o tráfego da rede, da infraestrutura da rede e host. Existem fatores que dificultam a observação de todos os eventos ocorridos na rede:

Segmentação das redes: atualmente existe uma tendência na segmentação de redes utilizando a instalação de *switches,* que fazem com que a característica de difusão redes diminua e não exista, pois estes equipamentos direcionam o tráfego ethemet das redes locais do emissor diretamente para o receptor analisando o endereço

MAC da máquina destino. Se todos os computadores de uma rede local forem conectados a um switch, a difusão do tráfego unicast de uma rede ethemet não existiria.

O tráfego segmentado faz com que nem todos os pacotes da rede trafeguem em todos os segmentos da rede, isto é, um pacote onde o emissor e o receptor estão no mesmo segmento não trafega em outro segmento. Se um sensor IDS esta em um dos segmentos de uma rede de múltiplos segmentos, o sensor irá capturar somente o tráfego destinado ou emitido aquele segmento. Desta maneira o switch dificultam a instalação do IDS em pontos estratégicos, sendo necessário uma análise cuidadosa da localização dos sensores do IDS.

Existem soluções propostas para estes problemas, como a adotada pela Cisco com o seu NetRanger que avisa aos equipamentos switches da existência de um sensor automaticamente, ou ainda, colocar sensores em todos os segmentos, mas não existe nenhum consenso sobre eles. A solução da Cisco é uma saída bastante razoável, apenas tem problemas de padronização entre os fabricantes de hardware e dos fabricantes de software IDS. Alguns outros switches aceitam a configuração de que uma porta receba todo o tráfego.

A segunda solução possui um problema e este ocorre quando em um segmento um host se comunica com outro. Como o switch direciona o tráfego diretamente para o destinatário, o IDS não verá este tráfego.

Outras soluções são a introdução de trap, nos switch, para que o sensor receba todo o tráfego da rede. Os trap são elementos que repetem o tráfego.

Aumento da largura de banda: O aumento da largura de banda tanto das redes intema como da externa, dificulta a coleta e análise do tráfego, pelo aumento do volume do tráfego e da velocidade de passagem dos dados. Os produtos comerciais publicam que seus produtos são compatíveis com redes FDDI e GigabitEthemet de alta velocidade, mas é claro que não divulgam a estratégia de coleta e nem qual a percentagem de perda de pacotes na captura nas redes de alta velocidade. Um fator que ameniza a perda de pacotes com a ampliação da taxa de transmissão das redes de alta velocidade é o aumento do poder de processamentos nos computadores que analisam o tráfego. É comum em redes de alta velocidade e alta taxa de transferência de tráfego que o IDS sejam instalados e máquinas RISC com grande poder de processamento.

Diante da dificuldade da coleta de todos os eventos ocorridos, Northcutt alerta sobre a impossibilidade da coletar todos os eventos de uma rede, e como analisar todos os eventos é difícil, sugere que sejam coletados os eventos nos segmentos importantes, desta maneira seriam coletados somente os eventos interessantes (EOI - Events of Interest).

Os Eventos de Interesse possuem três principais aspectos na detecção de intrusão e são eles:

Equilíbrio entre falsas positivas e falsas negativas;

A focalização do sensor para garantir a detecção de EOI;

Os efeitos dos limites na capacidade de detecção

A ocorrência de falsas positivas está relacionada às assinaturas que muitas das vezes identificam padrões que tanto podem ser tráfego normal, como um ataque (como exemplo, em um serviço configurado na porta 31337, o IDS irá soar o alarme, embora seja um tráfego legítimo), mas, se esta assinatura for desabilitada, perde-se a possibilidade de identificar as tentativas de conexões em cavalos de tróia, como o do Back Orifici. Outra maneira da geração de falsa positiva é a má definição do tráfego normal, não abrangendo algumas exceções.

As falsas negativas podem ser provocadas por um novo ataque que ainda não possua uma assinatura, ou que esteja criptografado; portanto, muitos IDS atualizam mensalmente os arquivos de assinaturas.

Sistemas perfeitos não existem, mas as falsas positivas podem ser analisadas por analistas de tráfegos especializados.

O posicionamento do sensor é fato de grande importância discutido nos próximos itens, já que se tem o problema da segmentação e de aumento do tráfego.

5.6 Comparação dos métodos de análise

Existem duas maneiras de detectar ataques conhecidos e não conhecidos: os baseados em assinaturas e os baseados em anomalias.

5.6.1 Baseado em Assinatura

Este método é baseado em padrões de ataque. É necessário o conhecimento de todos os tipos ataques existentes em detalhes para a identificação do padrão e criação da assinatura. A assinatura deve somente identificar o tráfego do ataque, sem detectar

tráfego legítimo. O conhecimento dos detalhes de fiincionamentos dos protocolos e serviços da Internet é necessário para que as assinaturas sejam escritas corretamente.

Além da dificuldade técnica na criação das assinaturas, existem dificuldades como: a falta de conhecimento de detalhes da arquitetura TCP/IP, a falta de comunicação entre a equipe de firewall e a equipe de detecção de intrusos, a falta de tempo dos analistas para documentação dos ataques e para desenvolvimento de ferramentas.

Em comparação com as assinaturas de vírus, que passam de 60 mil, as de ataques são muito menores; a maior é a do aplicativo snort que possui não mais que 2 mil assinaturas.

A configuração das assinaturas também não é muito fácil, pois a linguagem de criação das assinaturas é complexa. Além disso, cada software IDS possui sua própria linguagem, dificultando para o administrador saber se a assinatura ou filtro criado é eficiente e não anula outros existentes.

Muitos softwares permitem a atualização de assinaturas. Para a criação de um filtro é necessário que o analista tenha os seguintes conhecimentos: (NORTHCUTT, 2001)

Linguagem na qual o filtro deve ser escrito;

O procedimento de instalação do filtro;

A assinatura do ataque para a qual o analista está criando o filtro;

Os fundamentos de rede TCP/IP;

Existe uma grande problemática quanto ao método de assinaturas, pois não existe um centro popular para notificação de ataque. A CERT é, em princípio, o órgão mais indicado para exercer este papel, mas muitos não o conhecem e nem sabem como reportar os ataques, além do que, há de existir a centralização, padronização e divulgação de resultados para comunidade. Existem esforços neste sentido, mas ainda não surtiram os resultados esperados.

5.6.2 Baseado em anomalias

Os sistemas de detecção de intrusos baseados em anomalias consistem na definição do que é o tráfego normal para a detecção de tráfego anormal. Para definição do tráfego normal da rede é necessário conhecer o comportamento do sistema.

identificar os serviços instalados, coletar dados e efetuar a análise estatística destes dados.

Alguns sistemas permitem a configuração do tráfego normal, mas é uma tarefa difícil, pois a linguagem de configuração é complexa e não possui padronização.

Atualmente existem muitas pesquisas de metodologias para determinar o tráfego normal do sistema, e regra de assinatura como: Métodos estatísticos, Redes Neurais, Algoritmos genéticos. Mineração de dados, Fusão de Dados e Redes de Petri.

Os IDS baseados em assinaturas e anormalidades ainda produzem falsas positivas e falsas negativas, mas as duas técnicas utilizadas conjuntamente podem identificar um grande número de ataques nas redes.

5.7 *Posicionamento do Sensor*

o local da colocação do sensor é muito importante, pois pela localização do sensor pode-se selecionar os eventos que forem mais interessantes de serem observados. O sistema pode não funcionar satisfatoriamente se a posição não fora adequada.

5.7.1 Sensor fora do firewall

Os sensores normalmente são instalados fora do firewall, para que possa ver todos os ataques provenientes da Internet. Geralmente são instalado na DMZ^ (DeMilitarized Zone), possibilitando aos administradores verificarem todos os ataques, inclusive os que os firewall estão suscetíveis. Desta maneira o administrador poderá monitorar o tráfego que vem da Internet como também o que sai para Internet, podendo identificar ataques da rede extema.

Os IDS podem também identificar falhas na configuração do firewall e outro serviço como servidor web, e DNS. Algumas versões do IDS identificam que as versões usadas possuem vulnerabilidades.

---

^ Segmento de rede onde o acesso para usuários da Internet é permitido sem autenticação, é nesta zona onde ficam os Servidores Web e outros serviços direcionados ao público da Internet, esta zona possuem um nível de segurança menor que a rede corporativa.

5.7.2 O sensor dentro do firewall

O sensor dentro firewall não será exposto a todo o tráfego vindo da rede externa, pois o firewall filtrará alguns ataques, mas em compensação o sensor ficará mais protegido, livre de ataques específicos, dificultando o comprometimento deste sensor.

Como o sensor ficará livre de alguns ataques, irá enviar menor número de falsas positivas, além de facilitar bem mais a configuração dos firewall.

5.7.3 Dentro e fora do firewall

Com dois sensores monitorando os ataques, um fica na parte mais externa da rede, antes do firewall e outro na parte intema da rede. Desta maneira existirá maior facilidade para configuração do firewall, pois os administradores poderão comparar os alertas dos dois sensores, o intemo e o extemo.

O sensor intemo poderá detectar ataques internos da rede, do segmento escutado. É claro que existe a problemática do custo, não só do hardware duplicado mais também da licença de utilização de dois sensores, no caso da utilização de produto comercial. É um ponto a ser avaliado vendo o custo/benefício da implantação de dois sensores.

5.7.4 Outros Locais para sensores.

O local mais freqüente de instalação do sensor é fora firewall, mas outros locais da estmtura física da rede podem trazer benefícios:

Sub redes, tanto de filiais como redes associadas;

Segmentos de alto valor, como financeiro, setor de contabilidade ou pesquisa.

5.8 *Ferramentas*

Existem muitos softwares de IDS atualmente: os comerciais, os de domínio público e de órgãos governamentais. Algumas características dos IDS baseados em rede e host estão relacionadas abaixo:

Estas ferramentas necessitam de poder de processamento, memória e espaço em disco. Nada adiantará colocar um velho Pentium com 32 MB de memória e 2 GB de

disco; provavelmente agravaria a problemática da perda na captura dos pacotes, e tempos de sincronização excessiva.

Ferramentas Comerciais;

5.8.1 ISS RealSecure

A ISS - Internet Security System possui o RealSecure que é uma das ferramentas comerciais mais conhecidas. É dividido em gerenciadores que são usados em tarefas administrativas, operacionais e sensores e geradores de eventos. Possui duas versões de sensores de host e de rede em versões UNIX e Windows NT. A interface de uso possui somente versão Windows NT.

No ISS pode-se configurar as políticas de segurança máxima cobertura, cobertura mínima e média, podendo, além da escolha da política, desabilitar filtros que imitam grande número de falsas negativas ou criar novas assinaturas. Assim que a política seja definida o sensor inicia o mecanismo de coleta de dados e detecção de eventos enviando-os para o console em tempo real.

O console visualiza os eventos em vários níveis marcando-os com cores verde, amarela e vermelha, sendo a vermelha as de prioridade mais elevada. O sistema possui, junto ao módulo de detecção baseado em rede, o módulo de resposta, que quando da existência de detecção de atividade não autorizada, pode; terminar a conexão, enviar uma alerta por e-mail, enviando mensagem da reconfiguração do firewall, ou outra ação configurada pelo usuário. O mecanismo de IDS de rede necessita de uma estação dedicada para execução.

O módulo baseado em host analisa logs, arquivos, examinando se o ataque teve ou não sucesso, possuindo capacidade de reposta aos ataques, interrompendo processos e suspendendo as contas do sistema.

O produto possui um banco de dados, que possibilita e extração de relatório para análise posterior. Para que os dados sejam incluídos na base de dados é necessário realizar a sincronização do banco de dados e transferir os eventos do sensor para o console.

É considerado um dos melhores IDS comerciais, principalmente pela sua interface gráfica. É claro que possui defeitos, como o número de assinaturas (em tomo

de 170). Alguns usuários reclamam da dificuldade do envio das intrusões ao CIRT (Computer Incident Response Team). (NORTHCUTT, 2001).

5.8.2 NetProwler

O Netprowler oferece detecção dinâmica de invasão à rede, isto é, analisa em tempo real o tráfego da rede enviando alertas em tempo real, quando existe indícios de uso não autorizado, mau uso ou abuso de sistemas de computadores por sabotadores internos ou hackers internos. Possui um "processador virtual" SDSI (Stateful Dymamic Signature Inpection), ainda de patente pendente. Este processador virtual possibilita o desenvolvimento imediato de assinaturas de ataque personalizadas, para determinar até mesmo as mais sofisticadas violações de segurança. (SYMANTEC do Brasil, 2001)

Este produto foi adquirido pela Network Associates, possui uma idéia interessante de compilação de filtros, permitindo que as assinaturas sejam executadas como um conjunto de instruções, isto é cada assinatura é um conjunto de instruções que o processador virtual SDSI executa usando uma entrada de cache.

Para cada sistema operacional existe um conjunto diferente de assinaturas, baseadas nas vulnerabilidades do sistema operacional específico.

Possui também capacidade de resposta a ataques e troca de dados com outros produtos do fabricante como o firewall. Este sistema é baseado Windows NT.

5.8.3 CMOS

Computer Misuse Detection System é uma ferramenta atualmente mantida por ODS Networks Inc, que trabalha com dois métodos de busca, o baseado em assinaturas e o baseado em anormalidades.

O método de busca baseado em anormalidades obtém o modelo de comportamento da rede através de estudos estatísticos em: tempo de login e logout dos usuários; aplicações utilizadas com freqüência; número de arquivos abertos, modificados e apagados; usos de direitos administrativos e diretórios mais utilizados.

Esse método possibilita geração de vários relatórios, inclusive gráficos.

5.8.4 NetRanger

Como dito anteriormente esta ferramenta foi incorporada pela Cisco, que com o passar do tempo a está aperfeiçoando. Os componentes do Netranger são:

sensores e uma estação de análise, chamada de Director. A comunicação entre os sensores e o módulo de administração é realizado através de um protocolo proprietário da Cisco.

A ferramenta possui módulo de resposta para ataques, tem várias opções que incluem geração de alarmes sonoros, envio de e-mail, término abrupto de sessões, reinicializações de conexões, negação de acesso e acesso à rede. As ações da caixa de resposta são realizadas por meio do envio de mensagens para serem executadas pelos roteadores Cisco.

A característica de integração do NetRanger com os equipamentos da Cisco favorece esta ferramenta. É uma ferramenta apreciável para as redes de grandes organizações que já possuem hardware Cisco.

O Director fornece administração centralizada, permite instalação remota de novas assinaturas dentro dos sensores, coleciona e analisa dados de segurança.

Os eventos monitorados pelos sensores são classificados por nível de importância associando um código de cores. De acordo com o evento ocorrido será dado um estado que é representado por uma cor diferente. O estado normal é mostrado em verde; estados marginais ou de atenção são mostrados em amarelo, enquanto estados críticos são mostrados em vermelho.

Os sensores monitoram os logs dos roteadores cisco, como os pacotes das redes, o cabeçalho e o corpo do pacote.

Este produto realiza a montagem dos fragmentos IP com objetivo de analisar os pacotes anteriormente fragmentados, pois muito invasores realizam tentativas de ataques com pacotes fragmentados para burlar filtros dos firewall ou assinaturas dos IDS.

Como muitos dos produtos Cisco, possuem a desvantagem do altocusto.

5.8.5 Tripwire

É um IDS de host, que cria e armazena uma soma para verificação dos arquivos. Se não houve alteração nos arquivos que não deveriam ser alterados, esta soma é a soma binária dos arquivos, que possui grande confiabilidade. Também verifica logs e o comprometimento do sistema.

A geração de alarmes indica o provável comprometimento do sistema. O comprometimento do sistema obriga ao administrador realizar ações de restauração de backup ou a reinstalação do sistema como um todo. O tripwire auxilia na identificação do um backup não comprometido.

A ferramenta foi originalmente desenvolvida pela Pardue University, e possui atualmente versões comerciais e de domínio público. A versão comercial atual é a versão 2.X para UNIX e similares e também disponível para Windows NT 4.0.

A versão acadêmica é a 1.3 do ano de 1992. Existem também versões para as plataformas HP/UX e IBM/AIX.

Ferramentas de domínio público;

Existem muitas ferramentas de domínio público e, ao contrário que alguns possam imaginar, estas ferramentas possuem grande suporte, treinamento e atualização tão bons ou melhores que as ferramentas comerciais.

5.8.6 Snort

Foi desenvolvido por Maty Roesch e atualmente possui grande popularidade entre as ferramentas IDS, não só pelo fato de ser uma ferramenta free, mas também por possuir grande suporte, atualização e treinamento. A SANS Institute a adota como ferramenta padrão para seus treinamentos.

A SANS Institute treina e certifica muitos analistas de tráfego, como também é responsável pela publicação de vários livros sobre o assunto de detecção de intrusos.

O Snort possui versões Windows e UNIX em suas várias plataformas. Possui um grande número de assinaturas desenvolvidas pela comunidade. É bastante leve, pode-se atualizar as regras, possui ferramenta para leitura dos logs e eventos de maneira a facilitar e leitura de dados.

É considerado por muitos o melhor sistema de detecção de intrusos atualmente. (NORTHCUTT, 2001)

5.8.7 Shadow

O Shadow era utilizado anteriormente nos treinamentos do SANS Institute. É uma ferramenta para ambiente Unix. Foi lançado para domínio público pela Naval Surface Warfare Center Dahlgren Division.

O Shadow foi desenvolvido para ser um IDS para ser instalado na DMZ. É uma ferramenta rápida e leve, que permite que o analista avalie os eventos, analisa o *pay load* e o conteúdo dos pacotes, podendo possuir assinaturas de string.

A CERT, utilizando várias ferramentas de IDS em sua DMZ, relata que o Shadow foi o único a ajudar na detecção de uma vulnerabilidade de um software instalado; também foi utilizado em casos judiciais onde os eventos armazenados por este sistema serviram de provas, mas infelizmente o Shadow não trabalha em tempo real. (ALEN, et ali 2001).

Grava as informações em formato TCP Dump, e possui interface baseada em aplicação e relatórios vistos na web.

5.8.8 NFN - Network Flight Recorder

Está disponível na versão de domínio público e versão comercial. É uma ferramenta de monitoramento de rede de finalidade geral, oriunda de um aperfeiçoamento do libpcap, com implementação de aplicação em modo promíscuo; tem boa performance de velocidade, e as fiinções de alert e record são utilizadas para extração de informações após o filtro nos dados.

O NFN possui capacidade de permitir a construção de novas assinaturas. A versão comercial possui seus próprios filtros atualizados, na versão de domínio público possui poucos filtros, e para fiincionamento com eficiência é necessária a confecção de outros filtros.

Desenvolvimento governamental

5.8.9 GOTS -Government Off-the-Shelf

Existe muita controvérsia sobre esta ferramenta, afinal as informações são "sigilosas". O governo desenvolve as sua própria ferramenta, pois o objetivo é detectar além dos ataques prováveis, também ataques de espionagem e terrorismo.

> *" (...) um eufemismo para o software de qualidade "quase de papel de embrulho ", que pode realmente nunca ver a luz do dia. O governo dos Estados Unidos financiou a maioria das pesquisas de detecção de intrusão. Quando considero a capacidade do NID e Shadow, tenho dificuldade de entender por que os órgãos do governo são tão ansiosos para utilizar sistemas comerciais. Os sistemas GOTS são usados para os maiores arrays de sensor de detecção de intrusão que foram construídos atualmente. Se você estiver considerando construir uma capacidade de detecção de intrusão que foram construídos atualmente. Se você estiver considerando construir uma capacidade de detecção de intrusão de larga escala, eu recomendo firmemente que leia o máximo possível de notas sobre os sistemas GOTS atuais. Não há necessidade de repetir todos os erros daqueles que foram, antes de você. "* (NORTHCUTT, 2001)

A comunidade vem discutindo os principais ataques e maneiras de defesa, e nos debates são discutidos as idéias para chegar a conclusões e teste das melhores técnicas de defesa. Os sites governamentais têm sido atacado constantemente por hackers, de maneiras como também organizações, muitas das vezes estes ataques são muitos similares ou iguais.

5.9 Envio de dados do sensor para o módulo analisador.

Quando um sensor detecta um evento, deve enviar estas informações para o módulo de análise. A maneira como estes dados são enviado deve ser rápida e segura.

A rapidez nunca será instantânea para que o envio seja em tempo real, mas pode ser rápido com pouco retardo. Alguns fabricantes aconselham a instalação de duas interfaces de rede para melhoria de desempenho e segurança.

A utilização de duas interfaces seria de tal maneira que uma interface ficaria em modo promíscuo, onde estaria instalado o sensor, e a outra seria exclusiva para a comunicação do sensor diretamente com a estação de análise. A primeira seria uma interface insegura que receberia os prováveis ataques, enquanto a outra, como é exclusiva, seria a interface segura. Por outro lado, esta seria uma abordagem que garantiria uma certa segurança e uma boa performance em termos de velocidade, pois o barramento entre o sensor e a estação de análise estaria sempre livre para o tráfego de dados entre elas, mas outro autor (ALEN, et ali 2000) chama a atenção que a interface

promíscua não deve ficar completamente insegura e exposta. Mesmo assim seria uma boa solução e possuiria um custo razoável.

Existe a necessidade de utilização de um protocolo seguro entre o sensor e a estação de análise e, portanto, muitos dos fabricantes de IDS utilizam protocolos proprietários; outra solução similar é a utilização de conexões seguras SSH.

Outra abordagem na comunicação entre o sensor e a interface é arquitetura utilizada; Essa comunicação pode ser *Push* ou *Pull.*

A utilização do *Push* produz pacotes em resposta a uma detecção, sendo fácil na monitoração do sensor para descoberta de sua configuração, possibilitando que intrusos determinem o funcionamento do sensor. Outra maneira seria enviar mensagens regularmente, independentes de eventos ocorridos, para disfarçar o funcionamento do sensor.

A arquitetura *Pull* produz mensagens quando solicitada e é vulnerável na hora em que são enviadas as solicitações, pois elas podem ser monitoradas pelos intrusos de palavra ou termos chaves.

A arquitetura push é a mais aconselhada para a detecção em tempo real. Muitos dos sistemas de detecção em tempo-real possuem sistemas de alarmes como bipes, envio de e-mail, mensagem em Pager e até celulares.

No início da utilização de uma ferramenta que gera muitas falsas positivas os alarmes devem aborrecer o administrador, mas quando a ferramenta estiver bastante adequada a uma rede particular, este alarmes podem ser úteis inclusive se enviarem o tipo de ataque para o administrador. É claro que, se o alarme soar às três da manhã para o administrador, e ele estiver dormindo, não será agradável, mas se ele estiver conectado e receber o alarme, não custará nada verificar o ocorrido remotamente.

5.10 A interface do usuário

Após a determinação do local dos sensores, instalação da ferramenta, a atividade de detecção deve ser iniciada, e o analista irá interagir com a interface do sistema. Os recursos da interface determinam a boa utilização da ferramenta e as melhores interfaces geralmente conquistam mais adeptos.

Console rápido: se o console for lento e demorar a exibir dados, pode afastar o usuário ou requerer maior custo e uma máquina mais veloz. É claro que nem

todos gostariam de arcar com despesas extras pelo mau desenho e implementação de uma ferramenta.

Melhor gerenciamento de falsas positivas: É bom que o analista tenha como gerenciar as falsas positivas, modificando assinaturas, acrescentado ou desabilitando filtros. Alguns produtos documentam as mais freqüentes falsas positivas para auxílio do analista iniciante. 0 esquema de código de cores, por exemplo, pode ser suscetível a configuração do usuário, permitindo que o usuário promova um evento para alerta máximo ou rebaixe.

Filtros de exibição: Os filtros de exibição ajudam o analista na visualização do tráfego para melhor análise. Os filtros podem ser por IP origem ou destino, por tipo de pacote TCP ou UDP. Quanto mais opções de filtro, melhor.

Marca de analisado: Marca eventos já analisados e pode ser de grande vantagem impedindo que um analista perca tempo analisando o que já foi analisado.

Drill Down: É a característica de poder ver os detalhes dos eventos como o pacote, a estrutura dos cabeçalhos, com somente alguns cliques de mouse. Assim que seja relatado um evento de ataque, o analista deve observar os detalhes do pacote ou grupo de pacotes para confirmação do ataque, para que não reporte uma falsa positiva. O recurso de drill drown é a possibilidade do analista verificar os detalhes do evento analisado.

Correlação: É a possibilidade de cruzamento de dados, isto é, de relacionar dados coletados anteriormente com os atuais, tais como números IP, horário de tráfego mais acentuado. A ferramenta pode manter uma tabela de endereços IP, de atividades suspeitas de análises anteriores, associando-os a cores possíveis de edição pelo analista, pois o controle manual ou através da memorização do analista são métodos bastante falhos.

Capacidade de relatórios: É a capacidade de gerar relatório dos ataques em quantidades e tipos diversos, com detalhes do ataque. A possibilidade de configurar novos tipos de relatórios é conveniente. O formato do relatório emitido (se TXT, HTML ou outro formato), possibilita a publicação na web ou busca de padrões. Os relatórios podem ser enviados por e-mail diariamente para o administrador da rede.

Capacidade de edição das regras do tráfego normal: As ferramentas que utilizam este método de análise geralmente não deixam claro qual o padrão de

comportamento do tráfego normal da rede, mas a edição destes parâmetros pode caracterizar a identificação de novos ataques.

Banco de dados: É a capacidade de armazenamento, em banco de dados, do tráfego capturado de maneira compacta, e de gerência de capturas antigas. Muitas ferramentas consomem grande espaço em disco, ficando a cargo dos analistas a tarefa de gerenciar os arquivos. Se estes dados forem armazenados e catalogados, a consulta posterior fica facilitada.

5.10.1 Aspectos humanos

Os IDS são ferramentas de auxílio aos administradores da rede e analistas de tráfego, porém, esta ferramenta sozinha não faz nenhum milagre. O aumento do número de ataques é fato, mas o aumento da segurança não cresce na mesma proporção.

Atualmente nem todos se preocupam com a segurança de suas redes, sabem que se conectar a Internet é importante, mas não existe uma preocupação concreta de planejamento e realização de uma política de segurança, que acaba ficando em segundo plano.

Muitos que trabalham como responsáveis pela segurança, não possuem treinamento para análise de tráfego, não possuem conhecimento profundo sobre os protocolos e serviços TCP/IP. Geralmente são pessoas inteligentes, trabalhadoras e antes de tudo, autodidatas; aprendem a utilizar as ferramentas IDS através de documentos publicados na Internet.

Os analistas possuem uma rotina de teste de ferramentas. Quando adotam uma ferramenta, passam um período para aprender a utilização esta ferramenta, que não é perfeita, e como o número de falsas positivas é bastante elevado, isto leva os analistas a não relatarem os eventos ao time de resposta, ou desacreditarem nos alertas. Geralmente como não passaram por treinamento, não conhecem os padrões de um possível ataque e acabam utilizando pouco a ferramenta, por não possuírem grande confiança nos alarmes gerados pelos IDS.

Muitas das vezes o analista reporta os eventos, como os de varreduras, para o time de resposta. Estes por sua vez armazenam os dados e não tomam nenhuma providência. Mesmo quando o analista relata um evento desconhecido, que paralisa os

sistemas, o time de resposta também engaveta, e o analista não relata novamente. Assim, as assinaturas demoram mais para serem anexadas às ferramentas.

O Global Incident Analsys Center (GIAC), é uma organização de CERT, formada por voluntários, disposta a publicar padrões de modo centralizados, de ataque para debate e análise dos ataques pela comunidade.

Os IDS nos Estados Unidos começam a ser utilizados; existe treinamento sobre como deve ser feita a análise do tráfego, para minimizar o número de falsas positivas e falsas positivas. A SANS treina e certifica estes profissionais. O treinamento é caro; cada módulo do curso custa em tomo de US$ 2,300.00 (dois mil e trezentos dólares). No Brasil, as ferramentas começam a ser conhecidas não existe nenhum treinamento específico sobre ferramentas de monitoração e detecção de intmsos.

5.11 Limitações dos sistemas IDS

Os fabricantes anunciam seus produtos prometendo máxima segurança contra os ataques, realizam teste em ambientes fabricados para impressionar, mostrando como seus produtos são bons e modemos, mas quando os usuários compram e instalam o produto, a realidade é outra.

A detecção de intmsos é uma área nova e em desenvolvimento e possui limites que devem ser esclarecidos aos usuários. Não seria bom que o administrador confiasse cegamente em seu IDS, pois as falhas existem. Nada pior que pensar que sua rede está totalmente imune aos ataques.

As ferramentas estão em processo de amadurecimento e possuem limitações, e ainda não identificam os ataques com precisão. Os limites mais importantes atualmente da ferramenta são:

O uso de mensagem criptografada no tráfego de informações maliciosas: como os dados estão cifrados os filtros podem não funcionar corretamente;

O tráfego crescente na rede: a largura de banda das redes é cada vez maior, variando de 10 Mbits/s a um IGbits/s e, portanto existe, a possibilidade do sensor não capturar todo o tráfego da rede Alguns fabricantes garantem o fiincionamento do sensor em redes de alta velocidade;

Falta da padronização na linguagem de assinaturas: muitas ferramentas estão no mercado e cada uma possui sua linguagem e suas assinaturas. Nenhuma padronização existe e o investimento em treinamento em uma ferramenta que não se desenvolve, é um dinheiro jogado fora, não há aproveitamento do conhecimento anterior na utilização de ferramentas similares;

Problema na distribuição da atualização das assinaturas dos sistemas: As atualizações das assinaturas não são regulares, nem automatizadas;

Dificuldade de detecção dos ataques de scripts e applets hostis, em arquivos anexados a e-mail, Java e Active-X;

Ataques a sistemas de detecção: Os ataques são cada vez mais astutos e já existem ataques que foram criados especificamente para o comprometimento do sensor ou do IDS;

Risco de respostas automatizadas impróprias: os módulos automatizados de resposta podem tomar decisões de defesas, mas isto não seria muito apropriado no caso em que o evento ser uma falsa positiva, ocasionando que um serviço seja interrompido, ou até mesmo a paralisação de um roteador;

Grande índice de falsas positivas e falsas negativas, dificultando determinar as verdadeiras positivas;

Os switches limitam a visibilidade do tráfego da rede, pela segmentação realizada por este tipo de equipamento;

Redes mais rápidas impedem análise de tempo-real efetivo de todo o tráfico em larguras de banda grandes;

Não reconhecimento de protocolos antigos, isto é, não reconhece todos os protocolos.

Mesmo com as limitações dos IDS acredita-se que ele possa ser de grande utilidade para a detecção de ataques.

No próximo capítulo serão discutidas as recomendações de pesquisa e de utilização de ferramentas.

6. Recomendações.

As ferramentas de IDS são úteis na monitoração de redes e host, podendo detectar ataques e responder com ações para que os ataques não ocorram, mas a principal questão reside no fato de que quando estas ferramentas são propícias para uso e onde devem ser localizados seus componentes, em relação à topologia da rede. Este capítulo descreve as recomendações para a melhor aquisição e instalação destas ferramentas.

6.1 Quando utilizar

As ferramentas de IDS baseadas em rede devem ser utilizadas para:

Detectar ataques conhecidos e acionar processos automatizados de respostas, mas nem todas as ferramentas possuem módulo de resposta;

Monitorar a política do firewall colocando o IDS próximo ao firewall, antes ou depois do firewall ou de ambos os lados;

Detectar ataques DOS, supervisionar servidores ou hosts específicos, serviços, ou protocolos;

Monitorar portas TCP e UDP.

As ferramentas de IDS baseados em host devem ser utilizadas para:

Monitorar arquivos críticos em busca de cavalos de tróia, e modificações não autorizadas;

Monitorar arquivos de log;

Monitorar aplicações e processos em servidores e hosts;

Operar em um ambiente no qual tráfego de cadeia é criptogafado;

A utilização dos dois tipos de ferramentas, host e rede, se completam.

6.2 Como escolher a ferramenta

É necessário verificar o orçamento para a instalação da ferramenta, pois a quantia disponível terá um impacto na seleção da ferramenta. Além das ferramentas comerciais, existem muitas ferramentas que são de domínio público e estão disponíveis para várias plataformas. As ferramentas de domínio público têm boa quantidade de

assinaturas e a comunidade tem realizado esforços para a centralização da documentação de ataques e assinaturas. Em contrapartida, muitas ferramentas comerciais anunciam características de resposta e integração com outros produtos, tais como firewall.

Outro fator importante para a escolha é qual o sistema operacional que está sendo utilizado pela empresa atualmente. Se a empresa possui um sistema baseado em Unix, a escolha deve recair em sistemas desta plataforma; se for Windows, a escolha deve recair em sistemas Windows e, se possuir os dois, deve ser escolhido um sistema que tenha implementação nas duas plataformas ou, ao menos, que existam sensores para ambas. Deve-se levar em conta que, além da cultura necessária para manejar estas ferramentas, os protocolos e ataques são diferentes entre os sistemas operacionais.

Muitos fabricantes de sistemas de IDS comerciais disponibilizam cópias do produto gratuitas para teste, que geralmente funcionam somente por 30 dias; as cópias gratuitas disponibilizam tudo, inclusive o código fonte.

A avaliação de sistemas de IDS pode consumir muito tempo, mas é um fator muito importante no processo de decisão. Primeiro deve-se verificar o que cada produto oferece e comparar com as necessidades. Os questionamentos abaixo podem ajudar na escolha da ferramenta.

Para quais sistemas operacionais o produto é disponibilizado?

Com que fi-eqüência o banco de dados de assinatura é atualizado?

Quantas assinaturas a ferramenta possui?

Quais são os apoios para redes segmentadas ou comutadas?

Quanto é fácil ou difícil a instalação?

Quanto é fácil ou difícil a manutenção e ajuste das assinaturas?

A ferramenta analisa os eventos em tempo real?

Possui caixa de resposta automatizada?

Interage com outros sistemas?

E se interagem, o faz com quais sistemas?

Possui interface fiincional?

Emite bons relatórios?

Infelizmente não existe uma comparação dos produtos entre si; existem apenas comparações entre os produtos gratuitos e avaliações independentes dos comerciais.

6.3 Onde colocar os sensores

Existem muitos locais onde se pode colocar um sensor, mas, dependendo do objetivo do IDS, ele pode ser colocado na frente ou atrás de um firewall.

Por primeiro deve-se verificar como é a topologia da rede onde irá ser instalado o IDS baseado em rede.

Conhecendo a rede será bem mais fácil escolher o local mais adequado para instalar os componentes da ferramenta IDS. Devem ser identificados os pontos de entrada de usuários externos tais como conexões com a Internet e conexões discadas. Se a rede possui um ou mais firewalls, ou se existem switches, é muito importante identificar o posicionamento destes, pois são variáveis que influenciam o local de instalação do sensor da rede.

A zona desmilitarizada é uma área de acesso de usuários exteínos na rede intema, onde geralmente ficam as máquinas com os serviços de Internet prestados pela rede aos usuários extemos. Na zona desmilitarizada os filtros de pacotes permitem tráfego para consulta de DNS e conexão com servidor web, por exemplo. Por esse motivo esta zona tem menor defesa e é conhecida como zona desmilitarizada. A instalação do sensor IDS na DMZ (DeMilitarized Zone), seria adequado, pois esta zona possui máquinas freqüentemente atacadas, pois chamam a atenção de invasores.

Freqüentemente a DMZ fica entre dois firewall, um após o roteador e um outro antes da rede privada, onde geralmente se localiza nos servidores DNS, FTP e WWW. Se o planejamento é a instalação de somente um sensor, o melhor local seria na DMZ.

Se o segmento onde estão as máquinas da DMZ for segmentado por um switch, uma das portas deste switch deverá ser configurada para receber todo o tráfego desde segmento. A figura 6.1 mostra o exemplo deste cenário.

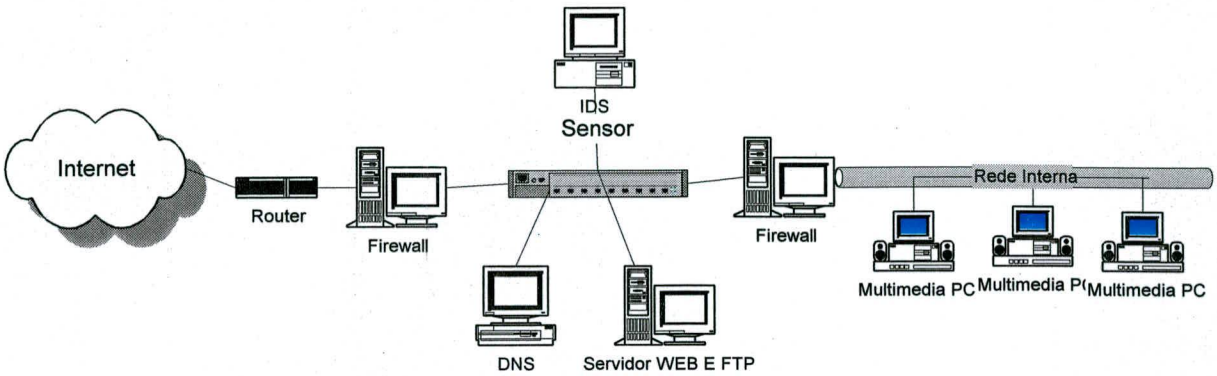

Figura 6.1 - Sensor entre Firewall

No exemplo do cenário da figura 6.1 os eventos monitorados pelo sensor seriam os direcionados para as máquinas da DMZ.

O cenário anterior somente monitora os eventos da DMZ. Para monitoração da rede intema seria necessário a instalação de um sensor no segmento da rede intema.

A instalação de mais sensores possibilita a monitoração de mais eventos. A instalação de um sensor, na rede intema possibilita a supervisão dos eventos ocorridos no segmento da rede privada e também auxilia o ftincionamento do firewall. A figura 6.2 mostra um exemplo de cenário de uma rede com dois sensores; um, localizado na DMZ e outro, na rede intema.

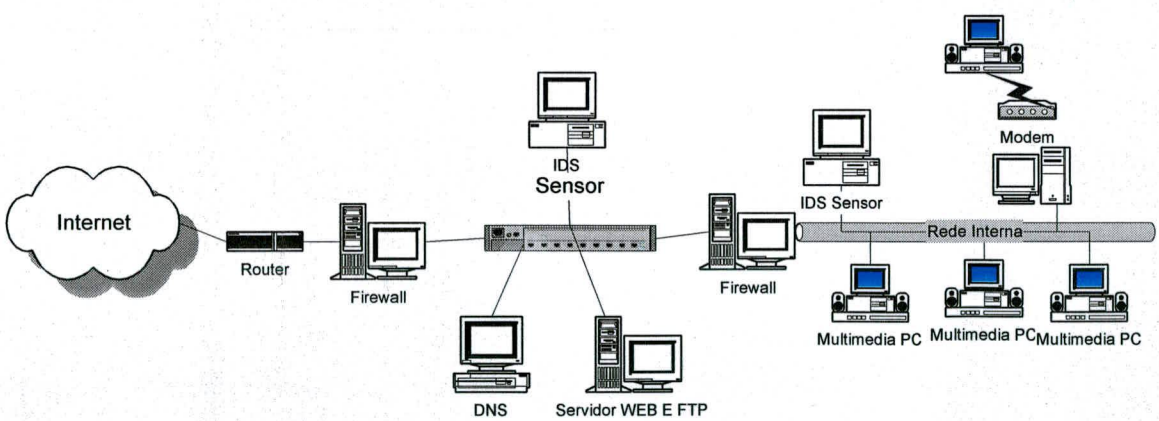

Figura 6.2 - Dois sensores, um na DMZ outro na Rede Interna

Como dito anteriormente, o orçamento disponível influencia de maneira direta na aquisição da ferramenta e planejamento da instalação do IDS e o plano de segurança como um todo.

Cenários com configurações mais simples também podem se beneficiar dos IDS.

A colocação de um sensor IDS em uma rede com um único firewall, pode ser instalado entre o roteador e o firewall. Desta maneira haveria o monitoramento de todos os ataques sem nenhum filtro do firewall, mas o sensor ficaria exposto a ataques com poucas ou nenhuma defesa. O roteador poderia possuir algum filtro para diminuir a exposição do sensor, pois muitos ataques atualmente são direcionados ao comprometimento dos sensores. A figura 6.3 mostra a um exemplo deste cenário.

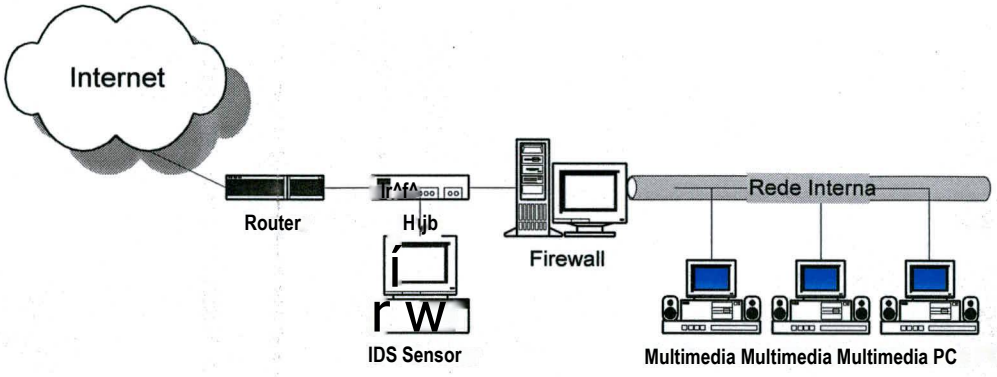

Figura 6.3 - Sensor entre o roteador e firewall

Para prevenção dos ataques direcionados ao comprometimento dos sensores configuração mais adequada é a colocação do sensor após o firewall. Neste caso, o sensor, além de um pouco mais protegido, monitoraria ataques que o firewall não foi capaz de filtrar. Esta configuração é mostrada na figura 6.4

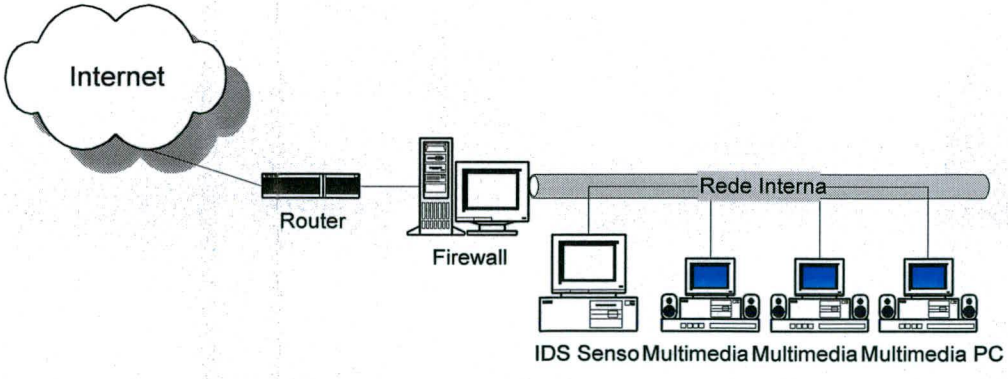

Figura 6.4 - Sensor na rede Interna

O melhor local para a instalação dos componentes da ferramenta IDS é aquele que se adapte melhor à topologia da rede e aos recursos disponíveis. Se for possível, a configuração com dois firewall e dois sensores é a mais aconselhada, mas também é a de maior custo. A regra básica de custo/benefício deve ser obedecida.

6.4 Ferramentas e recursos humanos

A alta taxa de falsos alarmes (falsas positivas) dos Sistemas de Detecção de Intrusos requer a alocação de recursos humanos significativos para avaliar a veracidades dos resultados da análise dos eventos.

Como as ferramentas ainda não estão totalmente automatizadas para detecção de intrusos com grau de acerto de 100%, é necessário que os analistas de tráfego avaliem a saída do sistema.

Não adiantaria muito colocar profissionais que não tenham o mínimo de conhecimento na área de análise de tráfego, pois a maioria das ferramentas exibe linhas de alerta e mensagem com os resumos do pacote na identificação de um tipo de ataque. Existe a necessidade que os profissionais que utilizarão estas ferramentas possuam conhecimento na área, treinamento e constante atualização.

A inexistência de pessoal capacitado para identificar a veracidade dos ataques e equilibrar o índice de falsas positivas e negativas dificultará a correta identificação de um ataque., mesmo que haja escolha da ferramenta adequada e o local adequado para a instalação do sensor.

Segundo Alen, alguns analistas reportaram várias falsas negativas à CERT, e ficaram tão desacreditados que, quando relataram ataques verdadeiros, foram totalmente ignorados. (ALEN, 2001).

Se for impossível realizar o treinamento formal do analista de tráfego, existe ainda a possibilidade de fazer com que adquiram conhecimento sobre o assunto, através de outros meios. Atualmente já existem cursos a distância e muito material de ajuda em sites especializados.

6.5 Reporte os ataques

Os fabricantes de ferramentas anti-vírus constituíram um processo para a criação de assinaturas de vírus, que tem funcionado e dado muitos bons resultados.

Considerando-se que muitos administradores sabem por experiência que, quando a máquina não está funcionando "adequadamente" é sinal de que pode haver um vírus em ação, adotou-se a regra de entrar em contato com os fabricantes e enviar os arquivos para análise. Isto faz com que, e em algumas horas, as assinaturas estejam disponíveis para a comunidade. Seria necessária a elaboração de uma estrutura similar para a criação de assinaturas de ataque.

É necessário para reportar os ataque, em primeiro lugar, colecionar e analisar dados, elaborando relatórios que reportem as intrusões definidas e bem documentadas. Estes relatórios devem ser reportados para o CERT ou outro órgão, que organize estas informações e que mantenha uma equipe de resposta para criação de assinaturas.

Os IDS analisam o tráfego e detectam os ataques que analistas de tráfego identificam e devem reportar. Seria de grande ajuda que as ferramentas emitissem relatórios automáticos que permitissem reportar um ataque, principalmente os desconhecidos, pois os ataques desconhecidos são de grande interesse de todos, principalmente para serem discutidos pela comunidade para que a assinatura seja confeccionada.

6.6 O futuro do IDS

Como relatado anteriormente, os testes nestas ferramentas não apresentaram resultados satisfatórios. Padrões para a realização dos testes devem ser traçados e utilizados em testes de várias ferramentas, inclusive nas ferramentas em fase de projeto.

As atuais ferramentas IDS baseadas em rede ainda apresentam um aho índice de falsas positivas e isto tem sido imia das principais dificuldades para a disseminação da utilização das ferramentas. As assinaturas, se utilizadas conjuntamente com a comparação do tráfego anormal, poderiam reduzir, em muito, o índice de falsas positivas.

Uma simples conexão de browser da Microsoft Internet Explorer em servidor web, pode disparar um alarme de inundação de SYN (fiood sysn), pois cria uma conexão para cada transferência de elementos HTML, JPEG, GIF. (NORTHCUTT, 2001).

Se um comportamento tão normal e comum como este pode gerar um alarme, a combinação da técnica de assinaturas com a técnica de comportamento normal do tráfego da rede poderia reduzir o número de falsas positivas.

Ainda não existe uma classificação padronizada dos tipos de ataques dificultando a análise da documentação enviada pelos analistas. Existem propostas, mas não um padrão. Enfim, falta da padronização no que tange aos nomes de ataques e quais aa suas principais características.

Inexistência de classificação e padronização dos tipos de ataques dificulta a análise da documentação enviada pelos analistas. Existem propostas, mas ainda nenhum foi adotado como padrão. Enfim, falta da padronização no que tange aos nomes de ataques e quais aa suas principais características.

Divulgação dos relatórios de ataque aos times de resposta: falta de uma definição de uma equipe de segurança, resposta, observação e investigação fazem com que as pequenas e médias redes fiquem perdidas não sabendo a quem reportar os relatórios.

Troca de dados entre os HIDS e NIDS: os IDS baseados em host (HIDS) avaliam o funcionamento dos hosts e os baseados em redes (NIDS) monitoram o tráfego entre os host extemos e internos. Existem dois aspectos que importantes na detecção de intmsos: os eventos que ocorrem nos hosts que seriam capturados pelos HIDS, os eventos que ocorrem no meio de difusão onde trafegam os pacotes que são trocados entre host da mesma rede e outras redes. Este tráfego é monitorado pelos NIDS.

A análise conjunta dos sensores de host e de rede pode facilitar a detecção e atividade suspeita na rede.

6.7 Firewall pessoal

o crescimento da utilização e comercialização de firewall pessoais tais como o Blackice da ISS, o Load-and-forget da Symantec e o Firewall security da Norton é cada vez maior. Os usuários adquirem e instalam em suas máquinas, geralmente com plataforma Windows, para se defenderem de invasões.

Em uma pesquisa com 400 leitores americanos a revista Networking Computing perguntou sobre a utilização de firewall pessoal nas empresas. De acordo

com os resultados 38% das organizações já adotaram firewall pessoais para proteger as informações nos equipamentos de usuários remotos. Outros 18% pensam em implementar esta tecnologia em, no máximo, um ano.(NETWORXING COMPUTING, 2001).

Dentre os que utilizam os firewalls pessoais, quase metade dos entrevistados (47%) relata que o fator mais importante para investir na aquisição da ferramenta é a proteção de dados estratégicos das empresas. Muitos utilizam esta tecnologia para proteção de laptops e acessos de usuários remotos (63%) e 15% fazem uso em estações de trabalho ligadas à rede e 22% que possuem firewall pessoais o utilizam em notebooks e workstation.

A utilização crescente dos firewall pessoais, que coletam e identificam os ataques em máquinas individualmente. Toma as informações coletadas por esta ferramenta interessante.

Os firewalls pessoais analisam todo o tráfego que chega à estação que o executa, analisando somente os pacotes direcionados àquela estação. Funcionam como um mini IDS, analisando o tráfego e reportando as tentativas de invasão para o usuário da estação.

6.8 O modelo IDS distribuído

Os firewalls pessoais são utilizados em empresas para defender seus computadores. É recomendável o aproveitamento desta nova "camada" de software na detecção de intmsos, pois os eventos que podem ser perdidos pelos sensores NIDS, e provavelmente serão detectados no destino. E se o fnewall pessoal estiver comprometido, o evento do intmso poderá se detectados pelo IDS de rede e vice versa.

Os firewall pessoais analisam o tráfego e geram alertas para os usuários da estação (que geralmente são pessoas leigas ou não fazem parte da equipe de segurança da rede intema), fazendo com que os alertas se tomem somente mais uma mensagem do Windows, a qual os usuários simplesmente apertam o botão de "OK", mesmo sem entender o que diz a caixa de mensagem.

Mesmo que alguns usuários mais avançados entendam o conteúdo da mensagem de alerta, provavelmente não saberão como proceder para defesa da sua

estação ou da rede, e nem como reportar o evento, ou ainda identificar a veracidade e gravidade do evento.

Se a verificação e análise dos eventos coletados pelos firewall pessoais fossem administradas de maneira centralizada, possibilitaria que os administradores da rede visualizassem os eventos ocorridos no tráfego das estações que possuem a ferramenta, sem possibilidade de perda de pacotes e análise do tráfego sem o problema da segmentação da rede. Sendo os administradores mais aptos a verificarem a veracidades dos ataques e responsáveis por reportar os ataques.

Os eventos recolhidos pelos firewalls pessoais seriam enviados para um analisador central de eventos, que combinaria os resultados da análise do sendor do firewall pessoal, com resultado dos analisadores NIDS e HIDS, e todos os eventos fossem re-analisados e exibidos de forma centralizada, permitindo ao analista de tráfego observar todos os eventos coletados, com menor possibilidade de possuir eventos não detectados. A figura 6.5. mostra modelo de junção dos dados coletados.

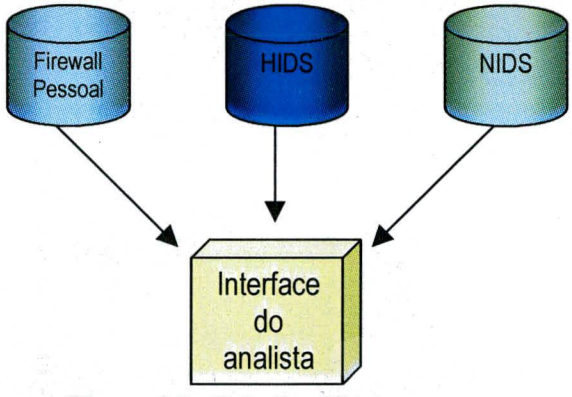

Figura 6.5 - Três tipos de sensores

Os firewall pessoais coletam seus eventos gerando alertas e armazenando estas informações em forma de arquivos. O envio das informações coletadas da ferramenta para o analisador central poderá ser realizado de duas maneiras. A primeira seria o envio dos arquivos periodicamente para o analisador e a segunda, o envio em tempo real da ocorrência do evento para o analisador central. Para maior segurança estas informações devem ser enviadas criptografadas.

Os firewalls atuais possuem mecanismo de gravar os eventos, assim seria mais fácil na implementação apenas o envio do arquivo para o analisador. Por outro lado, seria importante a implementação de mecanismo em tempo real, para que haja a

possibilidade da ação de uma caixa de resposta. A figura 6.6 mostra o esquema de envio de eventos para o analisador central.

De posse dos eventos ocorridos, o analisador central analisará cada ocorrência, e também o conjunto, pois alguns ataques são direcionados para um hots alvo e outros se caracterizam por enviar pacotes para vários computadores simultaneamente.

Os dados coletados pelos firewalls pessoais são previamente analisados reportando o tipo de ataque e de comportamento suspeito, de modo que estes dados possam ser classificados e enviados para interface para verificação do analista de tráfego. Os outros eventos reportados seriam o do resultado da análise de todos os eventos simultaneamente, como por exemplo, uma varredura UDP em várias máquinas.

Os eventos de-mesma origem que ocorrem com diferença no intervalo de tempo podem identificar um ataque. E devem ser observados pelo analista de tráfego.

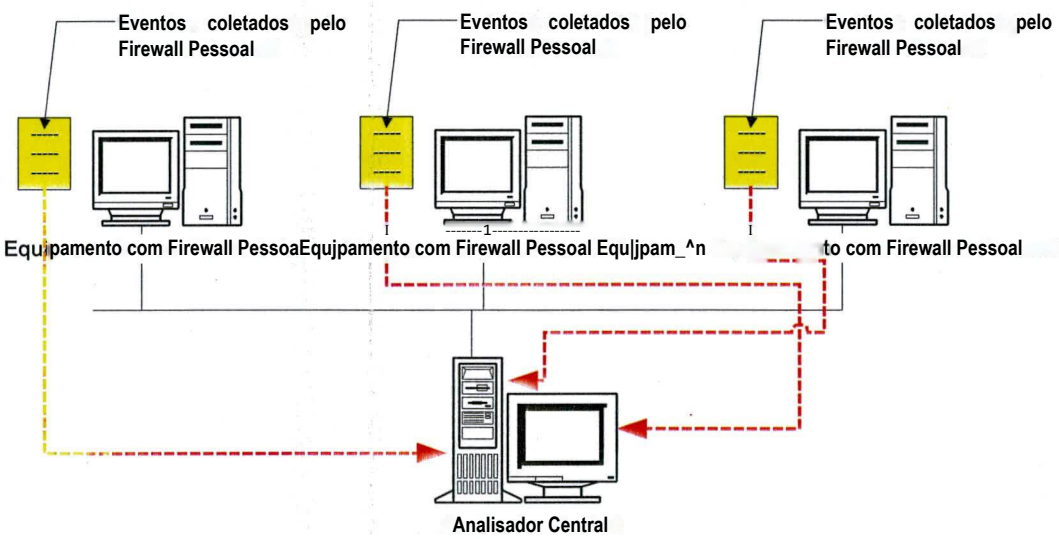

Figura 6.6 - Analisador central de eventos coletados pelos firewalls pessoais

A análise dos eventos enviados para o analisador central deve ser feita através da construção de uma tabela com os eventos de mesma origem, com tempo aproximado, menor que segundo. Se existirem eventos desta natureza estes devem ser analisados por assinaturas de ataques com características do fipo de ataque.

A figura 6.7 mostra eventos coletados pelo firewall pessoal BlacklCE. A figura mostra a denominação do ataque. É necessário que além das informações que são

exibidas no desktop da ferramenta, o tráfego correspondente também seja enviado para o analisador central.

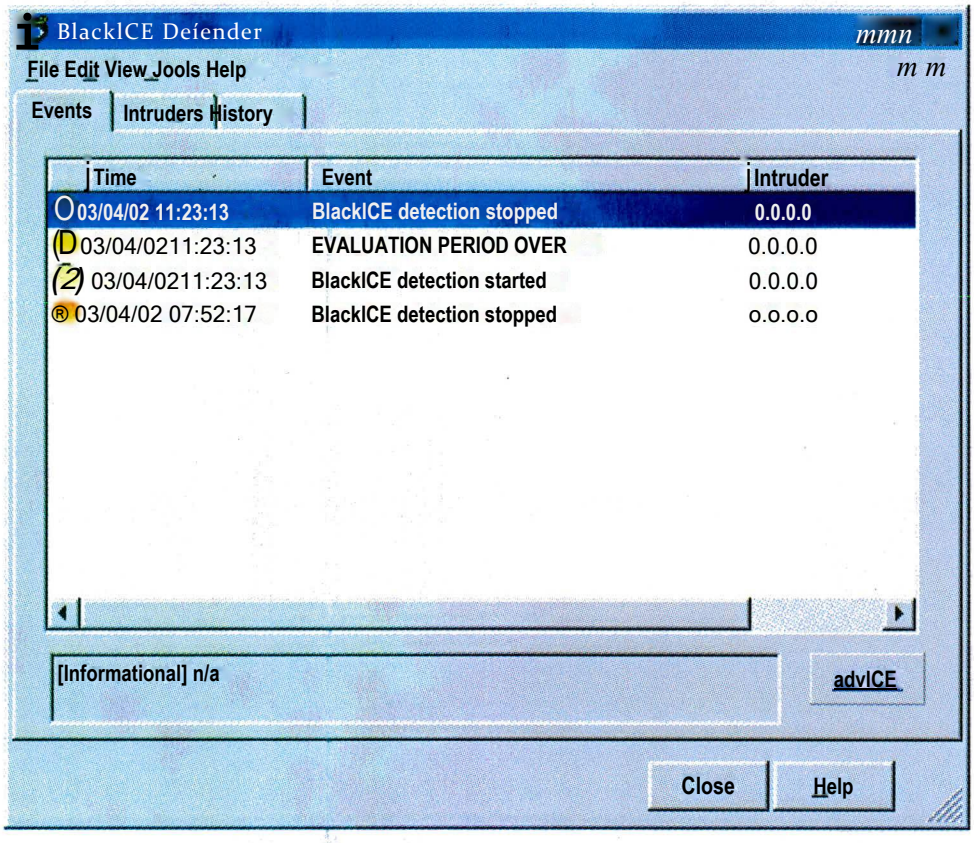

Figura 6.7 - Visualizador de eventos do firewall pessoal BlackICE

Os firewall pessoais funcionam com IDS de análise de tráfego individual, isto é, com um sensor*na máquina.

Quando uma empresa de segurança de prédios realiza seus projetos, procura colocar sensores de movimento e câmeras em lugares estratégicos, e quanto mais sensores e câmeras maior a segurança do local.

Se os firewalls pessoais fossem instalados em todos os host da rede teríamos capturado todos os eventos da rede enviados a estes hosts, isto é, existiriam vários sensores distribuídos em toda a rede.

O uso simultâneo de NIDS, HIDS e firewall pessoal possibilitará a captura de todos os eventos da rede. Os hosts mais suscetíveis a ataques, como os servidores, devem possuir um sensor de HIDS para relato dos eventos que possam ocorrer com as aplicações e arquivos deste computador.

A figura 6.8 mostra um cenário com dois firewall de rede delimitando a rede intema e extema, formado entre eles a DMZ. Na DMZ localizam-se um sensor de rede

(NIDS), para captura de eventos deste segmento, ainda na DMS os servidores possuem IDS baseados em host (HIDS) Na rede intema outro IDS de rede (NIDS) para capturar todos os eventos ocorridos na rede intema.(HIDS) o servidor da rede intema possui instalado um IDS de host (HIDS) e nas estações da rede intema um aplicativo similar aos firewall pessoais atuais, um mini IDS pessoal, que envie os eventos capturados para o analisador central. Todos os IDS os de host rede e pessoal enviariam os eventos ao analisador central.

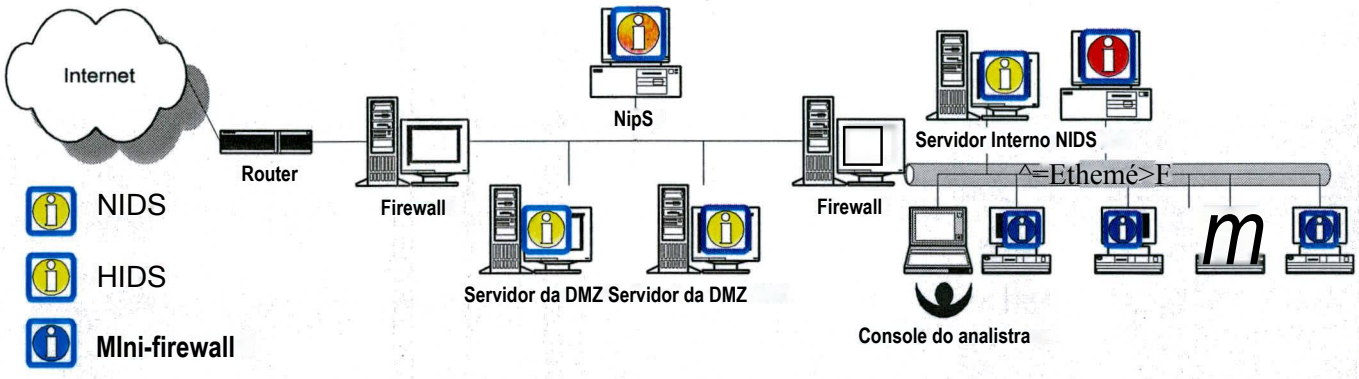

Figura 6.8 - Localização dos sensores HIDS, NIDS, e Firewall pessoais

O custo ficará da seria mais elevado, pois teremos sensores em todos os computadores, e o custo de desenvolvimento do mecanismo para análise dos dados dos firewalls pessoais.

Desta maneira o problema da não coleta de todos os eventos das redes estaria sendo diminuído, além de poder disparar o módulo de resposta, que geralmente não é implementado nos firewalls pessoais atuais.

Os firewalls pessoais atualmente são implementados para os dois principais sistemas operacionais para desktop, o Windows e o Linux.

A implementação de um software com características similares aos firewall pessoais, que fossem capazes de enviar os eventos suspeitos ocorridos em cada estação possibilitaria a distribuição da coleta e processamento de todo o tráfego da rede.

Os IDS pessoais somente analisariam os eventos direcionados à aquela determinada estação e eventos de broadcast. Se todas as estações da rede realizassem a mesma atividade teríamos todos os eventos da rede capturados, com algumas vantagens,

como: captura dos eventos independente da segmentação da rede, a remontagem dos fragmentos de rede somente no destino e possibilidade de análise dos pacotes criptografados.

Como descrito anteriorrnente, as estações onde estariam os IDS pessoais enviariam os eventos a uma estação central para visualização e análise dos eventos. Além da análise dos eventos conjuntamente dos NIDS e HIDS, o visualizador geral poderá realizar o gerenciamento de quais estações estão enviando periodicamente os eventos e detectando quais estações não estão funcionando adequadamente, desta maneira alertando o administrador. Como mostra a figura 6.9.

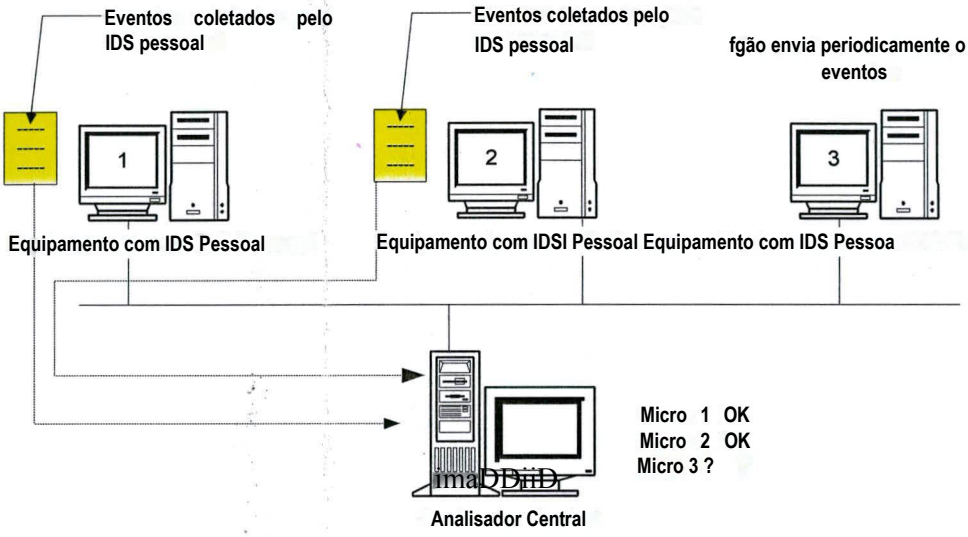

Figura 6.9 - Controle de funcionamento dos IDS pessoais

A implementação desta ferramenta poderia diminuir as limitações dos sistemas IDS, que são elas:

Mensagens criptografadas: Como o IDS pessoal está em uma das extremidades de comunicação (origem ou destino), seria possível a leitura de pacotes criptografados, sendo que esta possibilidade dependeria da implementação da ferramenta que teria de se comunicar com as aplicações que estariam criptografando esta mensagem;

Tráfego crescente; Como o tráfego é coletado em seu destino o processamento da coleta e análise é distribuído entre todas as estações da rede e o aumento do número de estações e de tráfego não teria grande influência;

Segmentação: A segmentação das redes, isto é, a utilização de switches, não limitaria a coleta de tráfego.

Caixa de resposta: Possibilidade de implementação de respostas automatizadas em tempo real como o IDS esta em cada estação. Ao ocorrer algum evento que seja considerado um ataque o software pode fechar a porta de conexão imediatamente ou simplesmente descartar o pacote.

Ataques aos IDS: Os ataques a IDS pessoais poderiam existir, mas como os IDS estariam localizados em todas as estações, existiria uma maior dificuldade de ataque a todos ao mesmo tempo, e se ataque fosse direcionado ao analisador central, os IDS nas estações ainda estariam em funcionamento.

Funções extras de distribuições de novas assinaturas para os IDS pessoais teriam de ser implementadas.

Outras limitações ainda persistiriam como: dificuldade de análise de scripts e applets hostis, além da possibilidade de ocorrência de falsas positivas.

7. Conclusões

o crescente número de ataques às redes de computadores faz com que sejam investidos milhões de dólares no desenvolvimento de técnicas para prevenir e impedir os ataques de invasores. Uma das técnicas que vem se desenvolvendo são os Sistemas de Detecção de Intrusos.

Os Sistemas de Detecção de Intrusos estão se desenvolvendo, ao longo do tempo, mas ainda não atingiram a perfeição ou um grau de acertos elevado, dado o alto número de falsas positivas e falsas negativas.

Somente os IDS utilizados isoladamente não dão seguranças para as redes. Um método de monitoração do tráfego com identificação de ataques é de grande valia para auxílio na defesa das redes, não só pela detecção de intrusos, mas também pelos testes de filtro de firewall e testes de penetração.

Muitas ferramentas estão no mercado, a maioria baseada em sistemas de assinaturas, mas o projeto de pesquisa EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) desenvolve uma ferramenta de IDS que analisa eventos baseados em assinaturas e anomalias na rede.

Algumas ferramentas falam que interagem os dados dos dois tipos de sensores (NIDS e HIDS), mas não divulgam como; simplesmente exibem os eventos isoladamente no mesmo console.

Os fabricantes de anti-vírus começam lançar produtos na área de segurança como firewalls pessoais, sniffer e IDS de host, através de desenvolvimento ou incorporação. Existe a probabilidade de que os fabricantes de antivírus desenvolvam ferramentas para a segurança de plataformas desktop, principalmente as baseadas em Windows.

Quanto à falta de padronização como, por exemplo, linguagens de assinaturas, protocolos de comunicação do sensor e mecanismo de análise, são próprios de áreas em desenvolvimento. Com o amadurecimento das ferramentas IDS algum nível de padronização será uma necessidade.

A implementação de IDS pessoais diminuiria algumas das limitações dos IDS atuais, além da escalabilidade do IDS Distribuídos, pois seriam úteis em pequenas e grandes redes.

A principais vantagens dos IDS pessoais distribuídos seriam a possibilidade de análise do tráfego criptografado, independência da segmentação da rede, caixa de resposta em tempo real, e maior dificuldade no ataques aos sensores.

A implementação e teste de uma ferramenta com as características, aqui apresentadas, ficam como sugestão para trabalhos futuros. E como possibilidade de desenvolvimento de tese de doutorado pela autora.

Mesmo com todos os seus problemas, os Sistemas de Detecção de Intrusos são de grande utilidade na segurança de rede, pois podem identificar muitos ataques, que seriam muito difíceis ou impossíveis de detecção sem estas ferramentas.

Referências bibliográficas

.....*5°Pesquisa Nacional sobre Segurança da Informação.* Julho 1999 [on-line] Disponível: http://www.modulo.com.br [capturado em dez..2001].

ALEN, Julian et al. *State of the Practice of Intrusion Detection Technologies,* [on-line] Disponível: http://www.cert.org [capturado dez. 2001]

BENNET, Gordon. *Intranets: como implantar com sucesso na sua empresa.* Rio de Janeiro: Campus, 1997.

BRLTNEAU, Guy. *The History and Evolution of Intrusion Detection.* October 13, 2001 [on-line] Disponível: http://rr.sans.org/intrusion/evolution.php [capturado dez. 2001].

CARFFARO, Marcelo L. *Sistemas de Detecção de Intrusos.{on-\\no* Disponível: http://www.securenet.com.br/artigo.php?artigo=95 [capturado dez. 2001].

CHIOZZOTO, Mauro, SILVA, Luis Antonio P. *TCP/IP Tecnologia e Implementação.* São Paulo: Erica, 1999.

COMMON INTRUSION DETECTION FRAMEWORK - CIDF. [on-line] Disponível: http://www.isi.edu/gost/cidf/ [capturado nov. 2001].

COMPUTER EMERGENCY RESPONSE TEAM - CERT. [on-line] Disponível: http://www.cert.org/archive/index.html. [capturado dez. 2001].

DEKKER, Marcel. *Encyclopedia of Telecommunications* vol. 15. New York, 1997. [on-line] Disponível: http://www.cert.org/encyc_article/tocencyc.html [capturado dez. 2001].

HARKCER, São Paulo, n°l, 2001.

LANTIMES. São Paulo: CMP Media, mar. 1998 - Mensal.

MCCLUDE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hackers Expostos: Segredos e Soluções para a Segurança de Redes.* , São Paulo: Makron Books, **2000**.

MONTANARO, Domingo M. Falhas de Segurança. *PC* Master São Paulo.edição 54, p.50-52. 2001

NAUGLE, Matthew G. *Anatomia Completa das Redes TCP/IP.* São Paulo: Berkeley Brasil, 2001.

NED, Frank. *Sistemas de Detecção de Intrusão e Aspectos Legais.* Jullho, 1999. [on-line] Disponível: http://www.securenet.com.br/artigo.php?artigo=8 [capturado dez. 2001].

NETO, Pedro Ortale. *Snort IDS.* [on-line] Disponível: http://www.linuxsecurity.com.br/sections.php?op=viewarticle&artid=10 [capturado dez. 2001].

NORTHCUTT, Stephen, NOVAK, Judy, MACHLAN, Donald. *Segurança e Prevenção em Redes.* São Paulo: Berkeley Brasil, 2001.

REVISTA DO LINUX. São Paulo. 2001 ano II n° 24 12/DEZ - Mensal.

ROMANO, Marcelo.O que é um hacker? *Informática Passo a Passo.* São Paulo: Escala, Ano 1 n° 3, p. 26-33, 2001.

SOARES, Luiz Fernando. *Redes de Computadores: das Lan, Man e Wan às redes ATM.* 2® Edição revisada e ampliada. Rio de Janeiro. Editora Campus, 1996.

STARLIN, Gorki, NOVO, Rafael. *Segurança Completa Contra Hackers.* Rio de Janeiro: Book Express, 2000.

SUGUIMOTO, Fernando. Os auditores da rede. *Network Computing.* N°28, p.56-64. São Paulo: IT Mídia. 2001.

SYMAMTEC DO BRASIL. *Introdução à Segurança,* [on-line] Disponível: http://www.symantec.com.br [capturado em dez. 2001].

TANENBAUM, Andrew S. *Redes de Computadores.* 3° ed. Rio de Janeiro: Campus, 1997.

WADLOW, Thomas *A. Segurança de Redes: projeto e gerenciamento de redes seguras.* Rio de Janeiro: Campus, 2000.

ZWICKY, Elizabeth D. COOPER, Simon, CHAPMAN, D. Brent. Building *Internet Firewall. 2°* ed. Sebastopol, CA-USA: O'Reilly. 2000.