

EVELYN RUTH KLER
GELSON PRADO

SEGURANÇA DE REDES
SISTEMA DE DETECÇÃO DE INTRUSÃO

CURITIBA

2004

EVELYN RUTH KLER
GELSON PRADO

SEGURANÇA DE REDES
SISTEMA DE DETECÇÃO DE INTRUSÃO

Monografia apresentada como requisito parcial à conclusão do Curso de administração com ênfase em análise de sistemas da Faculdade Internacional de Curitiba.

Professor Mestre: Marcos Laureano.

CURITIBA

2004

Dedicamos este trabalho a todos os professores que vem nos acompanhando ou que nos acompanharam desde o início de nossa vida acadêmica, aos nossos familiares que nos educaram e nos incentivam a buscar as melhores oportunidades em nossas vidas e a Deus que nos dá saúde e sabedoria e nos ajuda a escolher os melhores caminhos para o sucesso.

"A maioria das redes dá acesso às informações vitais aos funcionários, parceiros e clientes remotos, fora das tradicionais dependências da empresa. Isso permite que façam seus trabalhos de forma mais eficiente, embora a vulnerabilidade seja maior. Assim, a segurança é fundamental. Ademais, não é o bastante ter redes robustas apenas nas matrizes se as filiais sofrem de má performance de rede. O mesmo nível de acesso à informação e tecnologia fora da empresa é crucial".(John Chambers - CEO da Cisco)

AGRADECIMENTOS

Ao professor mestre Marcos Laureano, pelas sugestões apresentadas e contribuições no decorrer do trabalho.

Aos professores pela oportunidade concedida de seguirmos nosso próprio caminho, mais sabendo a direção.

A todos que, direta ou indiretamente, colaboraram para a realização deste trabalho.

SUMÁRIO

DEDICATÓRIA	3
RESUMO	9
1 INTRODUÇÃO.....	10
1 INTRODUÇÃO.....	10
2 SEGURANÇA – CONCEITOS, ABORDAGENS E TECNOLOGIAS	12
2.1 INFORMAÇÃO.....	12
2.1.1 IMPORTÂNCIA DA INFORMAÇÃO	12
2.1.2 SEGURANÇA DA INFORMAÇÃO.....	13
2.2 RISCOS E AMEAÇAS	15
2.2.1 ATAQUES, ATACANTES E MOTIVAÇÕES	16
2.2.1.1 CLASSIFICAÇÃO DE ATAQUES CONFORME OBJETIVO	17
2.2.1.2 CLASSIFICAÇÃO DE ATAQUES CONFORME A ORIGEM	18
2.2.1.3 CLASSIFICAÇÃO DE ATAQUES CONFORME A SEVERIDADE.....	20
2.2.2 FORMAS DE ATAQUE	22
2.2.2.1 ATAQUES AUTOMATIZADOS	22
2.2.2.2 ATAQUES MANUAIS	25
2.2.3 FERRAMENTAS DE ATAQUE	26
2.2.3.1 CLASSIFICAÇÃO DE FERRAMENTAS DE ATAQUE POR EFEITO	26
2.3 MECANISMOS PARA CONTROLES DE SEGURANÇA	29
2.3.1 CONTROLE DE ACESSO	33
2.3.2 CRIPTOGRAFIA	34
2.3.3 VPN (VIRTUAL PRIVATE NETWORKS).....	37
2.3.4 FIREWALL.....	38
2.3.5 ANTIVÍRUS	41
2.4 SISTEMAS PARA DETECÇÃO DE INTRUSÃO	42
2.4.1 CARACTERÍSTICAS DOS IDS'S	43
2.4.1.1 CARACTERÍSTICAS DESEJÁVEIS EM IDS'S	44
2.4.1.2 CARACTERÍSTICAS INDESEJÁVEIS EM IDS'S	47
2.4.2 FORMAS DE MONITORAÇÃO	47
2.4.3 QUANTO ÀS FORMAS DE DETECÇÃO.....	51
2.4.3.1 DETECÇÃO POR ASSINATURA	51
2.4.3.2 DETECÇÃO POR ANOMALIA	52
2.4.3.3 DETECÇÃO HÍBRIDA	55
2.4.4 Modelo conceitual de uma ferramenta de IDS.....	55
2.4.5 Modelo CIDF (Common Intrusion Detection Framework - Working Group).....	57
2.4.6 LIMITAÇÕES DO IDS	58
2.4.7 FERRAMENTAS EXISTENTES	61
2.4.7.1 EMERALD.....	61

2.4.7.2 NETSTAT	63
2.4.7.3 BRO	64
2.4.7.4 SNORT	65
3 CONCLUSÃO	67
4 REFERÊNCIAS	69
5 GLOSSÁRIO	73

LISTA DE FIGURAS

Figura 1	Etapas envolvidas no processo de cifragem / decifração	32
Figura 2	Cenário do <i>Firewall</i>	36
Figura 3	Conjunto de componentes que define uma ferramenta de IDS	54

RESUMO

O estudo focaliza os diversos tipos de ataques em rede que as empresas estão suscetíveis atualmente e a importância da proteção das informações para as organizações. Verifica-se a interação dos mecanismos que auxiliam os responsáveis pela segurança da rede de computadores na prevenção desses ataques. Como metodologia optou-se por uma abordagem de informações e conhecimento. Desta forma, realizou-se a princípio uma pesquisa bibliográfica, buscando em literaturas, sites disponíveis na *internet* e artigos que esclarecessem as questões levantadas na problemática do tema em estudo. Demonstram-se alguns conceitos que descrevem ataques e vulnerabilidades mais comuns e as formas de prevenção, através de mecanismos para controles de segurança e como foco principal os sistemas de detecção de intrusão e suas ferramentas existentes. Desta forma os impactos dos ataques que ocorrem em rede serão minimizados e melhor administrados.

1 INTRODUÇÃO

O avanço da tecnologia está cada vez mais rápido, e traz algumas conseqüências para as organizações que trabalham com seus computadores ligados em rede, como por exemplo, o problema da segurança das informações, sendo como tema abordado neste estudo a segurança para o ambiente de rede, especificamente o IDS - sistemas de detecção de intrusão.

O estudo tem como problemática a identificação, classificação e prevenção de ataques que podem ocorrer em uma rede corporativa.

Devido às empresas utilizarem a *Internet* para diversificação e automatização de seu negócio, estão passíveis a vários ataques em sua rede corporativa. Um atacante pode ter vários objetivos ao realizar uma invasão como, causar prejuízos ou procurar vulnerabilidades no sistema para depois divulgar estas informações. Estas vulnerabilidades podem estar ligadas a um sistema mal configurado, falhas na especificação de um software ou falta de planejamento na política de segurança do departamento de informática.

Este trabalho tem como justificativa defender os três princípios básicos da segurança da informação, que são integridade, confidencialidade e disponibilidade através de alguns conceitos sobre sistemas de detecção de intrusão, quais os riscos que as empresas estão sujeitas atualmente e como prevenir estes tipos de ataques.

O objetivo geral deste estudo é demonstrar através de conceitos as formas mais comuns de ataques aos quais qualquer empresa está suscetível e através destas informações contidas no decorrer do estudo as empresas poderão minimizar prejuízos financeiros, operacionais e maximizar a proteção das informações corporativas, uma vez que a informação é um bem de grande valor.

O objetivo específico deste trabalho é identificar ataques e classificá-los, assim como as tecnologias existentes para segurança de redes sendo o foco principal os sistemas de detecção de intrusão.

Foi colocada como primeira hipótese a possibilidade de se ter uma rede de computadores interligados sem correr riscos de segurança e como segunda hipótese se a elaboração de uma boa política de segurança pode minimizar os danos causados por intrusões.

Este trabalho tem como metodologia a análise de informações disponíveis em fontes bibliográficas específicas, artigos e informações nos *sites* de segurança de maneira quantitativa para assim fundamentar o objetivo deste trabalho.

Primeiramente teremos uma análise sobre a informação e a importância da segurança da mesma para a organização. Logo após sobre os riscos e ameaças para os computadores interligados em rede, em seguida sobre os mecanismos para o controle de segurança, dentre estes se encontra o Sistema de Detecção de Intrusão (*Intrusion Detection System*) onde será explicado sobre suas características, formas de monitoração e detecção e ferramentas existentes.

2 SEGURANÇA – CONCEITOS, ABORDAGENS E TECNOLOGIAS

A necessidade e a facilidade do manuseio da informação faz com que as organizações se preocupem cada vez mais com a segurança da informação.

2.1 INFORMAÇÃO

Para compreendermos o conceito de informação primeiramente precisamos descrever sobre os dados, que são descrições básicas de coisas, eventos, atividades e transações que são capturados, registrados mais não organizados para transmitir qualquer significado.

A Informação é um conjunto de fatos ou dados organizados de modo a fazer sentido ao seu destinatário, ou seja, os dados com uma interpretação lógica ou natural dada a ele por seu usuário. A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias.

Vivemos em uma sociedade que se baseia em informações e que exhibe uma crescente propensão para coletar e armazenar informações e o uso efetivo da informação permite que uma organização aumente a eficiência de suas operações (CARUSO, 1999).

2.1.1 Importância da informação

Hoje é comum nas organizações trafegarem um grande volume de informações entre os computadores e redes, para isto é preciso entender que a

informação é um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor em si, este valor está diretamente ligado à maneira como ela ajuda os tomadores de decisões a atingirem as metas.

A informação é um ativo que como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. Na sociedade da informação, a mesma é o principal patrimônio da empresa e está sob constante risco, representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa. A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade.

As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital, este controle é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão, deve ser administrada em seus particulares, diferenciada e salvaguardada (LAUREANO, 2003).

2.1.2 Segurança da informação

Nos últimos anos a segurança da informação está se tornando cada vez mais necessária, isto ocorre devido ao rápido crescimento da tecnologia que torna as corporações mais dependentes das redes de computadores para realizar suas

atividades e investimentos, pelas vantagens em custos e pela facilidade de acesso.

A segurança da informação possui algumas características básicas para o seu bom funcionamento, são elas:

- **Confidencialidade** - revelar informações apenas para pessoas autorizadas. A proteção de informações confidenciais é muito importante para afastar ameaças como, por exemplo, acesso indevido a informações restritas, quebra de estratégias comerciais, perda de vantagens competitivas e proteção do negócio da empresa;

- **Integridade** - Assegurar a precisão e a integridade da informação, ou seja, manter as informações intactas de acesso de pessoas não autorizadas. A não aplicação deste pode resultar em erro no planejamento, erro na operacionalização e (o mais grave) erro na tomada de decisão, através da alteração dos dados.

- **Disponibilidade** - Assegurar que a informação e os sistemas de informações estejam acessíveis podendo ser usados a qualquer tempo e na forma requerida, caso contrário haverá clientes insatisfeitos, parcerias comerciais interrompidas e retrabalho.

Além dos aspectos citados acima existem outros que devem ser levados em consideração como:

- **Autenticidade** - Garante que a informação ou o usuário do sistema é autêntico;

- **Não repúdio** - Não é possível negar (no sentido de dizer que não foi feito) uma operação ou serviço;

- **Legalidade** - Garante a legalidade (jurídica) da informação;

- Privacidade - Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve ser vista, lida ou alterada somente por quem a criou e com a garantia de que a informação não será disponibilizada para outras pessoas;
- Auditoria - Rastreabilidade dos diversos passos que um negócio ou processo realizou, identificando os participantes, os locais e horários de cada etapa.

Com o advento da *Internet* e sua grande utilização os computadores estão expostos, disponibilizando seus dados ao alcance de praticamente todos os usuários da mesma, com o conseqüente risco de acesso não autorizado, causando assim diversas oportunidades de ataques, ou seja, qualquer tentativa de quebrar alguma propriedade de segurança (LAUREANO, 2003).

2.2 RISCOS E AMEAÇAS

O risco não é um novo problema ou uma nova terminologia, os seres humanos sempre tiveram de enfrentar (ou encarar) os riscos no seu meio ambiente, embora seu significado tenha mudado, como tem mudado a sociedade e o próprio meio onde vive. No passado, a grande preocupação estava centrada nos desastres naturais (geológicos e climatológicos) na forma de inundações, secas, terremotos e tempestades. Após a revolução e o decorrer dos tempos, os riscos naturais foram substituídos por aqueles gerados pelo próprio homem, do

qual fez necessários, ferramentas mais poderosas no gerenciamento de riscos uma delas é o conhecimento.

Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, e esta deve ser tratada como tal, sendo protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade. Neste contexto, o gerenciamento de risco indica os caminhos e as informações que devem ser protegidas.

Risco pode ser descrito como uma medida da incerteza associada aos retornos esperados de investimentos, conforme (FANTINATTI, p.34, 2002), risco não é ruim por definição, é essencial para o progresso e as falhas decorrentes são parte de um processo de aprendizado.

Os riscos devem ser avaliados ou analisados através de processos que identifiquem sistematicamente os recursos valiosos de sistemas e ameaças que os mesmos podem ter, quantificando as exposições de perda (isto é, potencialidade de ocorrer uma perda) baseadas em freqüências estimadas e custos de ocorrências, e (opcionalmente) recomendar como alocar recursos às contramedidas no para minimizar a exposição total.

Após a análise ou avaliação é necessário o gerenciamento dos riscos, através de processos para identificar e controlar os eventos incertos, eliminando ou minimizando os que podem afetar os recursos de sistema.

Se não for possível eliminar o risco, deve-se tentar reduzi-lo, limitar sua área de atuação e controlar o ambiente ameaçado.

2.2.1 Ataques, atacantes e motivações

Segundo (SHIREY, 2000) um ataque é uma ação nociva à segurança de um sistema que deriva de uma ameaça inteligente, sendo essa ameaça uma tentativa deliberada (no sentido de método ou técnica) de evitar os serviços de segurança e violar a política de segurança de um sistema, podendo ser classificado, inicialmente quanto ao seu objetivo em passivo e ativo e também quanto à sua origem em interna e externa.

Em (CAMPANA, 2004) encontramos uma forma adicional de classificação de ataques baseada no grau de severidade do dano que o ataque pode causar, variando desde vandalismo virtual até negação de serviço e destruição de equipamentos.

Para auxiliar na compreensão dos riscos de ataque aos quais os sistemas digitais estão expostos, é necessário classificar os ataques conforme objetivo, origem e severidade.

Conforme (CAMPANA, 2004) existe uma fronteira virtual erguida pelas entidades na forma de sua Política de Segurança. Uma política de segurança é um conjunto de regras que visa regulamentar a produção, acesso e tráfego de informações e recursos computacionais em uma organização e determinar formas de agir em caso de violação destas regras. Este conjunto de regras é usado como limitador e para determinar o escopo das técnicas e ferramentas de segurança de uma rede.

As políticas de segurança trazem as expressões "perímetros de segurança" e "domínios de segurança" como sinônimos, que serão usados a seguir.

2.2.1.1 Classificação de ataques conforme objetivo

- Ataque Passivo - Ataques passivos são aqueles que buscam obter informações de um sistema, evitando influenciar o funcionamento do sistema afetado. Furtos de senhas, de endereços de e-mails, espionagem digital, fraude bancária e esquemas de desvio de dinheiro são exemplos de ataques do tipo passivo. As entidades que são mais vulneráveis a este tipo de invasão são as instituições financeiras (bancos, companhias de cartão de crédito), instituições privadas (empresas, sociedades) e departamentos governamentais. Estas instituições são mais visadas devido ao tipo de informação que trafegam, pois o mesmo representa ganhos imediatos para o atacante (por exemplo: desvio de fundos, espionagem industrial, hostilidades internacionais).

- Ataque ativo - Ataques ativos são os que buscam afetar o funcionamento dos dispositivos de uma rede, seja através da desativação de serviços críticos em servidores, comprometimento de informações do alvo, desperdício de recursos, destruição de informações e até comprometimento físico dos recursos de um sistema. Ataques ativos são exemplificados pela pichação de *sites*, destruição intencional de dados, desperdício de recursos do sistema (processamento, memória, documentos de impressão), suspensão dos serviços e até desativação por completo de um alvo, e, potencialmente, danos físicos ao equipamento envolvido.

2.2.1.2 Classificação de ataques conforme a origem

- Ataque interno - Ataques internos são aqueles que são iniciados do lado de dentro do perímetro de segurança que é criado pelas políticas de segurança de uma organização. São considerados ataques internos todas as atividades que

visam abusar ou fazem mau uso dos recursos computacionais aos quais teriam direitos de acesso regularmente. Funcionários que utilizam os recursos da empresa para buscar informações sensíveis, vírus que contaminem máquinas de usuários para depois atacar servidores e ações de engenharia social, nas quais um indivíduo mal intencionado se vale da confiança a ele garantida para tentar comprometer informações são exemplos de ataques internos.

- **Ataque externo** - Ataques externos são todas as atividades nocivas ao funcionamento dos recursos computacionais que partam do perímetro externo ao domínio da política de segurança da entidade atacada. Esse perímetro diferencia os usuários internos dos externos e caracteriza os ataques externos como todos aqueles que são gerados por usuários não autorizados ou ilegítimos do sistema. Considera-se então o ambiente da *Internet* como a origem da maioria dos ataques externos a um sistema devido ao alto grau de conectividade dos sistemas a essa rede. No entanto, em uma rede corporativa é possível conceber-se diversos perímetros de segurança, e ataques vindos de outros setores, apesar de estarem partindo da mesma rede física, seriam considerados como ataques externos. Exemplificando: um administrador de sistemas constrói um domínio de segurança chamado "diretoria", e outro chamado "funcionários". Se um usuário autorizado e autenticado no domínio "funcionários" efetua uma ação de ataque contra o domínio "diretoria", esse ataque seria considerado como externo do ponto de vista dos domínios de segurança, mas interno do ponto de vista da rede corporativa (ambos os sistemas se encontram na mesma rede, porém separados por políticas e regras de segurança diferentes). Os agentes de ataque externo potenciais são os amadores que pregam peças baseadas em ferramentas automatizadas de

ataque, os criminosos virtuais organizados, terroristas internacionais e até entidades governamentais hostis.

2.2.1.3 Classificação de ataques conforme a severidade

Outra forma de classificação dos ataques é a que abrange o dano causado quando o ataque obtém sucesso. A severidade é determinada de acordo com o tempo gasto na recuperação e prejuízo que o ataque consegue causar ao sistema afetado. O grau de severidade, no entanto, não é uma informação quantitativa, mas sim qualitativa, e diretamente ligada ao objetivo principal da entidade atacada. Um ataque de baixa severidade para uma entidade pode ser de severidade crítica para outra. Durante a construção da política de segurança, o administrador de sistemas deve determinar quais são os tipos de ataques que devem se encaixar em quais categorias e durante o processo de caracterização destes incidentes, o administrador deve avaliar os itens abaixo:

- Principal objetivo em relação ao negócio da corporação;
- Quanto tempo à corporação pode continuar em funcionamento após a interrupção dos serviços;
- Entre todos os serviços disponibilizados, quais os mais importantes para a corporação;

Com estas informações é possível determinar quais são as prioridades no caso de falhas múltiplas e contabilizar os danos sofridos em caso de ataques bem sucedidos (SHIREY, 2000).

- **Baixa Severidade** - Estes ataques são todos aqueles cujo acontecimento não atrapalhem o funcionamento da empresa. Considera-se também de baixa

severidade os ataques que podem ser rapidamente reparados, com pouco ou nenhum impacto para entidade. Um ataque que causasse a deleção de arquivos importantes, mas os mesmos pudessem ser rapidamente recuperados do conjunto de *backups* do dia anterior, e a brecha que permitiu o acontecimento for fechada, seria considerado de baixa severidade.

- Alta Severidade - Ataques de alta severidade são aqueles que, em geral, dificultariam o funcionamento da empresa ou que gastariam tempo e ou recursos para o reparo. Epidemias de vírus na rede interna, quedas de servidores de arquivos e interrupções no acesso à *Internet* são considerados eventos de alta severidade. Danos que incorram em re-instalação, reconfiguração ou perdas de dados sem *backup* e danos físicos com necessidade de substituição de equipamentos envolvidos também são inseridos nessa categoria.

- Ataques Críticos ou Incapacitantes - Ataques críticos ou incapacitantes são todos aqueles ataques cujo acontecimento representaria grandes prejuízos ou causariam a finalização das atividades da entidade. Os ataques críticos são todos aqueles que afetam diretamente o negócio principal das entidades afetadas, e como tal, variam de cenário para cenário. Uma empresa financeira cujo cadastro de clientes furtado (com todas as informações pessoais desde nome completo até cartão de crédito, por exemplo), uma entidade de segurança nacional que tivesse seus servidores invadidos (posicionamento de tropas militares, por 25 exemplos) ou uma entidade formal que sofresse um ataque à sua reputação através de *e-mails* forjados (oferecendo ofertas duvidosas ou difamando outrem, por exemplo) são todos exemplos de ataques críticos (LAUREANO, 2003).

2.2.2 Formas de ataque

Uma vez conhecendo os tipos de ataque é necessário saber como os mesmos são feitos para poder finalmente proteger os sistemas. Entender as formas de ataque e as ferramentas utilizadas é uma necessidade para se conseguir gerar ferramentas e técnicas de prevenção a novas ações.

Duas formas de ataque são caracterizadas: ataques manuais e ataques automatizados.

Ataques automatizados são mais comuns e responsáveis pela maioria das invasões e brechas em sistemas, enquanto ataques manuais são considerados potencialmente mais perigosos em seu escopo, devido à maneira de sua execução e à experiência necessária por parte do atacante para a execução de cada um (CAMPANA, 2004).

2.2.2.1 Ataques automatizados

Ataques automatizados são aqueles que não demandam atenção humana para sua efetivação, podendo ocorrer apenas através da execução de *scripts* e *softwares* específicos para invasão (MEINELL, 2004)

Existem diversas formas de ataques automatizados: vírus, *worms*, cavalos de tróia e *scripts* de invasão.

- Vírus - são seções de código nocivo, que modificam programas originais através da inserção deste código no início dos arquivos afetados. Vírus podem se propagar através dos recursos computacionais pela execução de seus programas hospedeiros, afetando assim novos alvos. São considerados ataques automatizados, pois sua capacidade de replicação não depende da atividade do atacante, mas sim do atacado. Quanto mais sistemas interagirem com o alvo

infectado, maior será a ação dos vírus. Vírus são detectados através de suas assinaturas, particularidades de código conhecido, que programas específicos conseguem ler dentro dos arquivos afetados e efetuar a remoção apenas do código virótico, restaurando o arquivo afetado a sua condição normal. Vírus não podem ser executados e sua propagação está ligada à execução dos seus hospedeiros.

- *Worms* - diferem de vírus por serem programas completos, executáveis independentemente da existência de um hospedeiro eles se propagam através de mensagens de correio eletrônico, conexões de rede e camuflados em arquivos aparentemente inocentes. A existência de *worms* também é endereçada pelos mesmos aplicativos que cuidam de infecções por vírus, porém para um *worm* não há correção, sendo que a cura para a existência de *worms* em um sistema é a deleção dos mesmos. São considerados ataques automatizados pela mesma razão que os vírus: capacidade de propagação e de causa de danos independente da interação do atacante.

- Cavalos de tróia - São *softwares* aparentemente úteis e inofensivos, mas que em seu código contém seções nocivas que buscam burlar políticas e sistemas de segurança, gerando vulnerabilidades que possam ser exploradas posteriormente pelo atacante. Cavalos de tróia em geral não são detectados pela sua assinatura em arquivos contaminados (vírus) nem pela sua execução em sistemas contaminados (*worms*), mas pelos seus efeitos. Quando um sistema é contaminado por um cavalo de tróia, esta aplicação maliciosa abre uma porta que aceita conexões externas por onde o invasor irá efetuar seu ataque com sucesso, porta esta conhecida em jargão técnico como *Backdoor*. É através da monitoração destes efeitos que os programas antivírus conseguem encontrar a

presença de cavalos de tróia em um sistema. A infecção por um cavalo de tróia onde o usuário pode ser exposto a estes riscos através de *sites* aparentemente idôneos, *softwares* e ferramentas condescendentes com pirataria de software e aplicativos de origem duvidosa. *Worms* podem conter em seu código um componente de cavalo de tróia, permitindo que o atacante tenha a capacidade de infecção de um vírus com a abertura de brechas no sistema característica do cavalo de tróia.

- *Scripts* de invasão e ferramentas de exploração de falhas - são pacotes de *softwares* e instruções encadeadas para se fazer invasões a sistemas. Estes *scripts* são criados por indivíduos com alto grau de capacidade técnica, para exploração de amplas listas de fragilidades e falhas conhecidas em sistemas. Estas falhas e fragilidades em geral são expostas pelo próprio criador do *software* envolvido, e subseqüentes remendos são desenvolvidos para o *software*, com o objetivo de evitar a falha conhecida. Porém, nem todos os administradores têm tempo ou disposição para atualizar seus sistemas, fazendo com que vulnerabilidades passem despercebidas pelo administrador (CAMPANA, 2004). Os criadores de *scripts*, então, criam ferramentas e receitas que visam exatamente atacar estas falhas conhecidas, buscando tomar o controle do sistema afetado. Uma vez que as ferramentas e *scripts* estão criados, os mesmos são disponibilizados na *internet*, em geral de maneira ruidosa para chamar a atenção de diversos possíveis atacantes que vêem nos *scripts* ferramentas para efetuar os ataques que eles próprios não conseguem, por incapacidade técnica. Todos os dias equipamentos conectados à *Internet* apresentam centenas de sondagens, de diversas fontes diferentes. Esse grande número de tentativas de invasão e sondagens diárias dá-se por um motivo simples: o ciclo apresentado

acima, em um computador doméstico moderno com *internet* de alta velocidade, demora apenas alguns segundos; logo, o computador e o usuário comum podem executar sondagens a um grande número de dispositivos na *internet* a cada dia. Como o método de invasão é totalmente automático, o atacante pode apenas executar suas ferramentas de invasão em segundo plano, permitindo que as invasões aconteçam automaticamente.

2.2.2.2 Ataques manuais

São diferentes em motivação e em perfil do executante dos ataques automáticos. Um atacante manual escolhe cuidadosamente um alvo e um objetivo antes de selecionar a técnica de invasão. Os motivos por trás do ataque podem variar, desde a simples pichação ideológica até a mais sofisticada fraude eletrônica bancária.

Uma vez que o alvo tenha sido escolhido e o objetivo seja determinado, o atacante manual irá sondar a rede escolhida minuciosamente, testando todos os sistemas alcançáveis em busca de qualquer falha que não tenha sido remediada. Para o atacante manual basta uma falha não atendida para que o ataque possa ser efetuado.

Os atacantes manuais eventualmente constroem suas próprias ferramentas, para automatizar seu trabalho. Provavelmente, uma vez que a ferramenta tenha sido utilizada, esta será disponibilizada na *internet*, aumentando os recursos dos amadores automatizados nas suas invasões.

Os atacantes manuais são mais nocivos exatamente por terem ao seu lado o conhecimento técnico que falta aos invasores automáticos, permitindo a eles a construção de ferramentas para seus desígnios específicos, ferramentas estas

que por vezes podem atacar fragilidades pouco conhecidas ou ainda inéditas, minando todos os esforços em assegurar um sistema.

2.2.3 Ferramentas de ataque

Com as ferramentas de ataque devidamente classificadas, pode-se enumerar os efeitos particulares das ferramentas, e citar alguns exemplos de ferramentas capaz de atingir os objetivos dos invasores.

2.2.3.1 Classificação de ferramentas de ataque por efeito

Um ataque pode ter diversos efeitos adversos em um sistema. Negação de serviço, obtenção de acesso indevido, aumento indevido de direitos e até controle total do sistema afetado. Serão enumeradas as ferramentas mais comuns para cada tipo de ataque e técnica utilizada pelos invasores.

- Negação de serviço - é um efeito que os ataques podem causar nos sistemas afetados. Por definição, negação de serviço é "um conjunto de ações que leva à indisponibilidade temporária de um determinado recurso computacional em um sistema" (HACKING, 2004). Os ataques de negação de serviço podem ser efetuados a partir de ferramentas simples, como o *ping* dos sistemas operacionais modernos, até vírus e *worms* que obrigam os sistemas afetados a tentarem numerosas conexões com alvos pré-determinados em janelas de tempo pré-determinadas (MEINELL, 2004). O funcionamento de um ataque deste é bem simples: o atacante busca tomar tantos recursos quanto possíveis do atacado, usando desde conexões normais até redirecionamento de IP para que o atacado gaste recursos processando os pacotes IP, até que o atacado perca toda a

capacidade de atender as requisições, sendo "afogado" em um volume muito grande de informações. Porém a capacidade de um atacante solitário conseguir afetar um grande servidor de maneira definitiva é pequena, causando uma evolução nesta técnica, que passou a ser conhecida como Negação de Serviço Distribuída (DDoS - *Distributed Denial of Service*). A nova técnica consiste em aumentar a quantidade de atacantes que tentam afetar o mesmo alvo simultaneamente, fazendo com que bandas de dados e capacidade de processamento sejam sobrepajados mais rapidamente. Os DDoS's então, podem ser iniciados manualmente por um grupo organizado de atacantes, ou através de vírus e *worms* que infectam um grande número de sistemas na *Internet*, contendo em seu código instruções para efetuar ataques dentro de uma janela de tempo específica contra sistemas específicos da *Internet* (CAMPANA,2004). Ataques de negação de serviço, no entanto, também podem ser lançados internamente em um sistema, de modo que a inserção de código nocivo venha a prejudicar a capacidade de processamento do alvo, requisitando, por exemplo, serviços.

- Enumeração de portas - são softwares auxiliares para o invasor. Uma vez apontados para um sistema cujo IP seja conhecido, estes softwares tentam conexões em todas as suas portas, buscando identificar serviços e versões de software para reportar ao invasor. Uma destas ferramentas é o *Ncat*, que conta entre suas funcionalidades à capacidade de ser apontado para um bloco de endereços, automatizando o trabalho de se identificar sistemas e portas disponíveis em uma rede.

- Obtenção de acesso - a obtenção de acesso também é um objetivo do invasor. Por obtenção de acesso pode-se entender que o atacante vai ter ao seu alcance um nome de usuário e uma senha válida no sistema, sendo que esse

nome de usuário não obrigatoriamente é o nome de um usuário com privilégios de administrador do sistema, pois muitos ataques podem ser efetuados para a elevação de privilégio. Ferramentas de obtenção de acesso são quebradores de senha, farejadores de rede e softwares que buscam conexões em sistemas cuja configuração de compartilhamento de dados não esteja segura. Um quebrador de senha, por exemplo, *L0phtcrack's* vai tentar efetuar *logons* em um servidor através de uma combinação de métodos de geração de senhas, tanto por força bruta, onde o software tentará "adivinhar" a senha, quanto pela utilização de dicionários de palavras, para efetuar tentativas baseadas em comportamento humano, levando em conta a mentalidade do usuário ao cadastrar suas senhas.

- Aumento de privilégio - aumento de privilégio é um passo das ações de um ataque. O atacante busca o aumento de privilégio a partir de uma conexão que já se encontra efetuada no sistema a ser comprometido, com a conexão feita através de um usuário legítimo do sistema (o usuário e senha podem ter sido obtidos anteriormente com o uso de ferramentas de obtenção de acesso). O aumento ou elevação de privilégio ocorre por falhas em serviços ou softwares disponíveis no sistema, ou por problemas com a configuração de segurança do sistema. A ferramenta *getadmin2k* é um utilitário de linha de comando para *Windows 2000* que permite, em se executando o utilitário, acessar diretamente as informações contidas no *active directory*, permitindo alterar qualquer senha facilmente. É uma ferramenta poderosa, apesar de deixar pistas claras da invasão do sistema.

- *Backdoor* - são softwares que uma vez instalados em sistemas, os deixam vulneráveis à conexão remota e controle total da máquina, através da abertura de portas de conexão. *Backdoors* costumam ser inseridos em

ferramentas automáticas de invasão pelos invasores manuais e construtores de ferramentas de invasão que fazem isso com o intuito de tornar os sistemas utilizados pelo script *kiddies* susceptíveis às invasões dos atacantes experientes. Ferramentas como o *NETBus* permitem diversos graus de interação com o sistema afetado, desde acesso aos dispositivos físicos (por exemplo: imprimir remotamente uma mensagem ameaçadora na impressora local do atacado) até a desativação do sistema afetado.

- Apagadores de rastros - uma vez efetuado um ataque, o atacante precisa partir sem deixar rastros de que esteve ali, deixando apenas os efeitos da invasão. Existem ferramentas automatizadas, mas não 100% eficazes que podem modificar arquivos de *log*, alterar históricos de sistema operacional e até recalcular *checksum* de arquivos, evitando que os arquivos modificados pareçam modificados. *Wipe* e *zap* são utilitários de linha de comando que funcionam assim.

- Sondas (*Scanners*) - uma sonda é um software capaz de testar um *host* ou conjunto de *hosts* contra um grupo de vulnerabilidades conhecidas. Esta capacidade pode ser usada em duas maneiras antagônicas: ao passo que o administrador pode se utilizar desta ferramenta para sondar a sua rede por vulnerabilidades em seu sistema com o intuito de repará-las, o invasor efetuará a sondagem buscando um alvo em potencial. Há vários *scanners*, tanto comerciais quanto livres, mas todos funcionam sobre o mesmo princípio de sondar o IP, sondar a porta, verificar sistema em execução na porta e reportar.

2.3 MECANISMOS PARA CONTROLES DE SEGURANÇA

Um dos principais meios de controle de segurança é elaborar, divulgar e manter atualizado documento que descreva a política de segurança de informações (KATZAN JR, 2000).

A alta gerência deve estar comprometida com a política de segurança de informações, a qual deve ser implantada de acordo com o documento formal por ela aprovado. Com o crescente número de ameaças, internas e externas, torna-se imperativo que as empresas implementem controles de segurança para proteger seus principais ativos.

Primeiramente deve-se analisar as ameaças, calcular os riscos e desenvolver estratégias para controlar esse ambiente vulnerável.

Como os ambientes computacionais são complexos, a melhor estratégia de implementação de segurança é utilizar controles em camadas. Essa estratégia tem-se revelado muito mais efetiva do que a segurança por meio de uma única e rígida medida de segurança (CARUSO, 1999).

A estratégia de segurança única tem a grande desvantagem de que, se o controle de segurança for quebrado, o sistema se tornará completamente vulnerável.

A disposição de várias camadas de segurança entre a ameaça e o recurso diminui consideravelmente a vulnerabilidade desse recurso, pois mesmo se uma das camadas for quebrada, existirão ainda outras para proteger o recurso.

Uma forma de implementação de segurança em camadas pode ser feita pela divisão dos sistemas de informações em camadas:

- programas aplicativos;
- serviços;
- sistema operacional;

- hardware;

Os controles nas diversas camadas estão relacionados entre si de tal forma que se uma pessoa não autorizada conseguir acessar uma camada mais superior terá outras barreiras a transpor.

2.3.1 Políticas de segurança

Para garantir que a segurança esteja prevista nos projetos desde os primeiros momentos de especificação, torna-se necessária uma Política de Segurança Corporativa. Esta política deve conter diretrizes, normas, procedimentos, produtos, estruturas gerais de segurança, além de um programa de conscientização e mensagem executiva da alta administração demonstrando apoio à política, sem o qual não se consegue a adesão necessária.

As responsabilidades e penalidades também devem estar previstas segundo a filosofia, normas administrativas e códigos de conduta empresarial de cada empresa. O momento é crítico, pois ao mesmo tempo em que aumenta o número de negócios *on-line*, os riscos crescem a cada dia e os usuários sentem-se desprotegidos, a espera de orientação quanto aos critérios e medidas a utilizar.

Não basta proteger as informações e sistemas atuais, é preciso conhecer e entender as novas ameaças e vulnerabilidades que vão surgir no futuro. As empresas assistirão o aumento de fraudes em transações eletrônicas, quebra de privacidade em e-mails, extorsões, roubo de segredos industriais e uso indevido de seus sistemas e infra-estrutura de tecnologia da informação.

Para minimizar estas fraudes, faz necessária a elaboração de uma boa política de segurança, que atenda a vários propósitos, como por exemplo:

- Descrever o que está sendo protegido e por quê;
- Definir prioridades sobre o que precisa ser protegido em primeiro lugar com qual custo;
- Permitir e estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;
- Fornecer ao departamento de segurança um motivo válido para dizer “não” quando necessário;
- Proporcionar ao departamento de segurança a autoridade necessária para sustentar o “não”;
- Impedir que o departamento de segurança tenha um desempenho fútil.

Entretanto a maioria das empresas considera difícil a tarefa de criar uma política eficiente, por várias razões:

- **Prioridade:** A política de segurança é importante, mas se for necessário que a alta administração precise deixar o que consideram urgentes e usar o tempo para concordar com a política de segurança, será muito difícil ter sucesso. Portanto a definição da prioridade deve ser feita de forma cautelosa.

- **Política interna:** Em qualquer empresa, grande ou pequena, vários fatores internos afetam qualquer decisão ou prática.

- **Propriedade:** Em algumas empresas existe uma discordância entre vários grupos que desejam ser os responsáveis pela política e, em outras empresas, a discordância ocorre entre vários grupos que explicitamente não querem ser os responsáveis pela política.

- **Dificuldade para escrever:** Uma boa política é um documento difícil de se organizar de maneira precisa, principalmente quando é necessário que seja abrangente. Não é possível prever todos os casos e todos os detalhes, por isto a mesma deve ser revisada constantemente.

Uma vez que a política tenha sido estabelecida ela deve ser claramente comunicada aos usuários, pessoal e gerentes. Deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concordaram com a política estabelecida. Esta é uma parte importante do processo. Finalmente sua política deve ser revisada regularmente para verificar se ela está suportando com sucesso suas necessidades de segurança.

No intuito de tornar a política viável à longo prazo, é necessário bastante flexibilidade baseada no conceito de segurança arquitetural. Uma política deve ser largamente independente de hardware e softwares específicos. Os mecanismos para a atualização da política devem estar claros. Isto inclui o processo e as pessoas envolvidas. Também é importante reconhecer que há expectativas para cada regra. Sempre que possível à política deve expressar quais expectativas foram determinadas para a sua existência.

2.3.1 Controle de acesso

O controle de acessos encontra-se em dois níveis, o lógico e o físico. Alguns dos aspectos lógicos são definidos previamente no controle de segurança, mais especificamente na política de segurança da empresa.

Os aspectos de segurança apresentados a seguir podem ser utilizados como uma lista de controles, tanto pela gerência de segurança de sistemas, como pela equipe de auditoria. Para a gerência de segurança, essa lista pode servir como

um conjunto de tarefas a serem realizadas para garantir a segurança de acesso lógico em uma empresa (CARUSO, 1999).

Os danos intencionais ou acidentais provocados por funcionários, prestadores de serviço, equipe de limpeza e de vigilância podem variar desde o roubo de equipamentos e componentes internos (placas de memória, chips, mouses, discos rígidos) até alteração, cópia ou divulgação de informações confidenciais e atos de vandalismo (destruição de equipamentos, corte de cabos elétricos e linhas telefônicas), estão relacionados ao controle de acesso físico.

A falta de controle de acesso físico aos computadores pode facilitar também a atuação dos invasores em suas tentativas de burlar controles lógicos de acesso aos recursos computacionais e suas informações, comprometendo a integridade e a confidencialidade dos dados (CARUSO, 1999).

2.3.2 Criptografia

A criptografia é baseada sempre em um mecanismo de conversão (o algoritmo de criptagem) para converter as informações de texto claro para texto cifrado pelo uso de uma chave de criptagem do conhecimento somente do emissor e do receptor (em princípio). O mecanismo pode ser de conhecimento público ou até mesmo não ser conhecido por nenhuma das partes, mas as chaves usadas no processo nunca podem ser reveladas. Em virtude do risco de decifração do texto e conseqüente dedução da chave, as mesmas devem ser trocadas com freqüência, o que implica a possibilidade de interceptação do meio usado para comunicar as chaves entre as partes (CARUSO, 1999).

As técnicas criptográficas são baseadas na substituição ou na transposição de caracteres (ou *bits*). A substituição consiste na troca de determinado padrão de

caracteres ou *bits* por outro padrão estabelecido pela chave de cifragem. A transposição implica a troca de posição das seqüências dentro da mensagem, controlada pela chave. Em ambos os processos, pode haver diversas passagens pelo algoritmo de cifragem antes que a mensagem seja transmitida. Na outra ponta da linha, o processo inverso é executado e se obtém de volta o texto claro.

Quando se usa criptografia, a principal variável com que se conta é o conceito do “tempo hábil”. Somente se pode obter proveito do conhecimento de uma informação criptografada se esse conhecimento chegar a tempo de se obter algum tipo de proveito com a mesma. É o caso específico das transações financeiras, em que a interceptação somente pode resultar em proveito do atacante se este conseguir interceptá-la ainda durante o processo de transmissão, passado o melhor momento, a decodificação da mensagem deixa de ter interesse para o atacante.

Tradicionalmente, o processo de criptografia implica a existência de um algoritmo criptográfico que, por meio de uma chave de cifragem, transforma um texto claro em criptograma, conforme a figura 1.

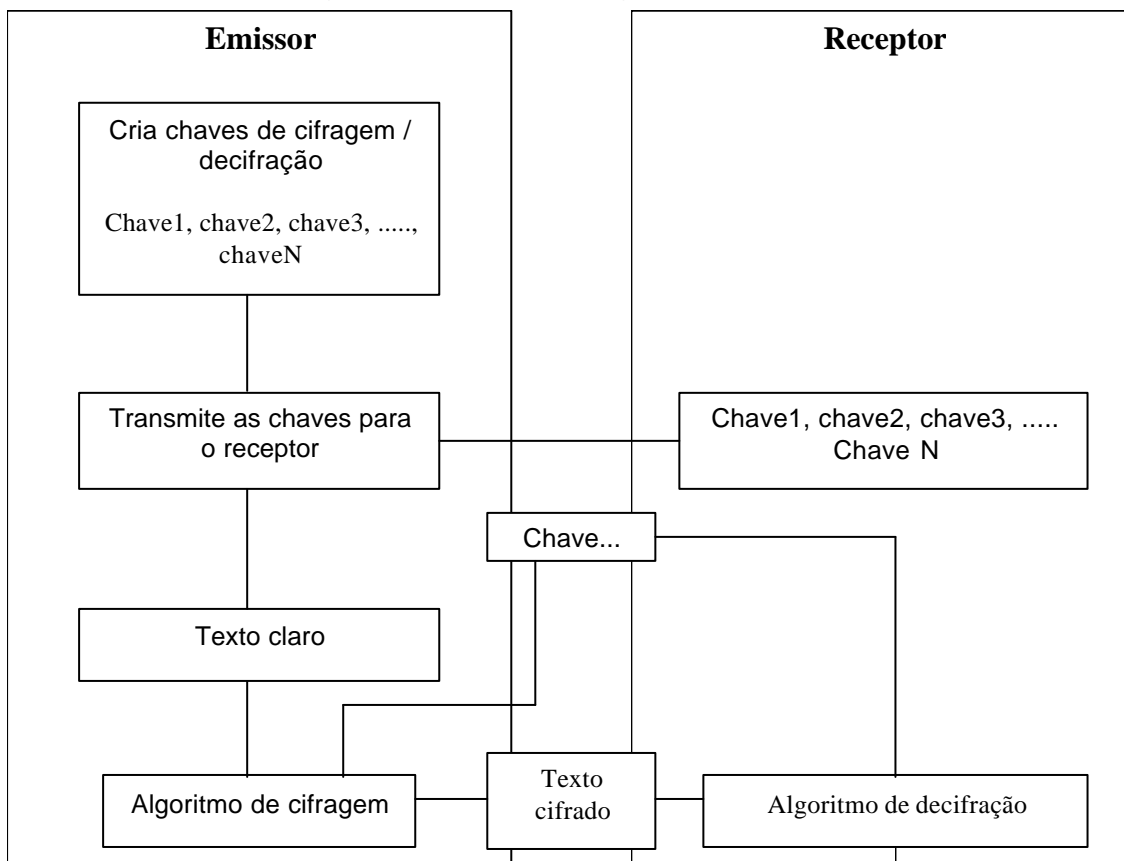


Figura 1 - Etapas envolvidas no processo de cifragem / decifração

Isso implica o conhecimento do algoritmo de cifragem ou da maneira como usá-lo, por parte de ambos os envolvidos no processo, ou mesmo o uso de um algoritmo de conhecimento público e da chave de cifragem ou decifração. As chaves usadas no processo precisam ser transmitidas pelo emissor para o receptor.

Em virtude do risco de quebra da cifragem pela análise do criptograma, existe a possibilidade de um determinado criptograma vir a ser decifrado e revelar qual o algoritmo e qual a chave usada para cifrar. Por esse motivo, as chaves de cifragem são trocadas freqüentemente, de acordo com um esquema combinado previamente. É nesse ponto que reside à vulnerabilidade do processo; a forma de comunicar as chaves usadas no processo é passível de interceptação por terceiros. Além do risco de interceptação, a lista de chaves precisa ser arquivada em algum meio de registro, e isso também é passível de revelação (KATZAN JR, 2000).

Entretanto, existe uma técnica de criptografia em que não é necessário transmitir as chaves de cifragem do emissor para o receptor, e são chamadas de chaves públicas.

Neste processo, a chave é dividida em duas partes, sendo cada uma delas o complemento da outra. Uma das partes é secreta, de conhecimento somente de

seu proprietário, e outra é pública, de conhecimento geral. O texto cifrado por uma delas somente pode ser decifrado pela outra e nunca pela mesma parte da chave que cifrou a mensagem. Dessa forma, uma mensagem cifrada com a parte de conhecimento público não pode ser decifrada por uma pessoa que conheça somente a parte pública da chave, e vice-versa. Outra vantagem reside no fato de se garantir através deste método autenticidade da mensagem, já que se pode usar a parte secreta da chave para gerar um criptograma que será decodificado com a parte pública. Como uma mensagem criptografada somente pode ser decifrada pela chave complementar à que foi usada no processo de cifragem, quando se decifra uma mensagem usando a chave complementar, sua autenticidade fica garantida, pois a chave secreta que a gerou é somente de conhecimento de quem a fez. Uma terceira vantagem é o fato de se eliminar o arquivo de armazenamento de chaves de cifragem em ambas as pontas de uma linha de comunicação e os conseqüentes riscos de ataque e revelação de chaves (KATZAN JR, 2000).

2.3.3 VPN (*Virtual Private Networks*)

A tecnologia de VPN permite que as empresas com linhas dedicadas formem um circuito fechado e seguro pela *Internet*, entre elas próprias. Dessa maneira, essas empresas asseguram que os dados passados entre elas e suas contrapartes estejam seguros (e normalmente criptografados) (SHIREY, 2000).

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela *Internet*, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados. Outro serviço oferecido pelas VPNs é a conexão

entre corporações (*Extranets*) através da *Internet*, além de possibilitar conexões *dial-up* criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador permitiria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensível.

Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita.

Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a confidencialidade das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.

2.3.4 Firewall

O conceito de *firewall* está ligado às paredes internas de uma construção que impedem que o fogo se propague de uma sala para outra da construção. Fundamentalmente, uma *firewall* tem três objetivos principais:

- Restringir o acesso de pessoas a ambientes controlados.
- Impedir que eventuais atacantes cheguem muito perto das defesas internas.
- Impedir que as pessoas passem por um ponto controlado sem que tenham autorização para tanto.

Normalmente, um *firewall* é instalado no ponto de interligação de uma rede interna com a *Internet*, conforme figura 2.

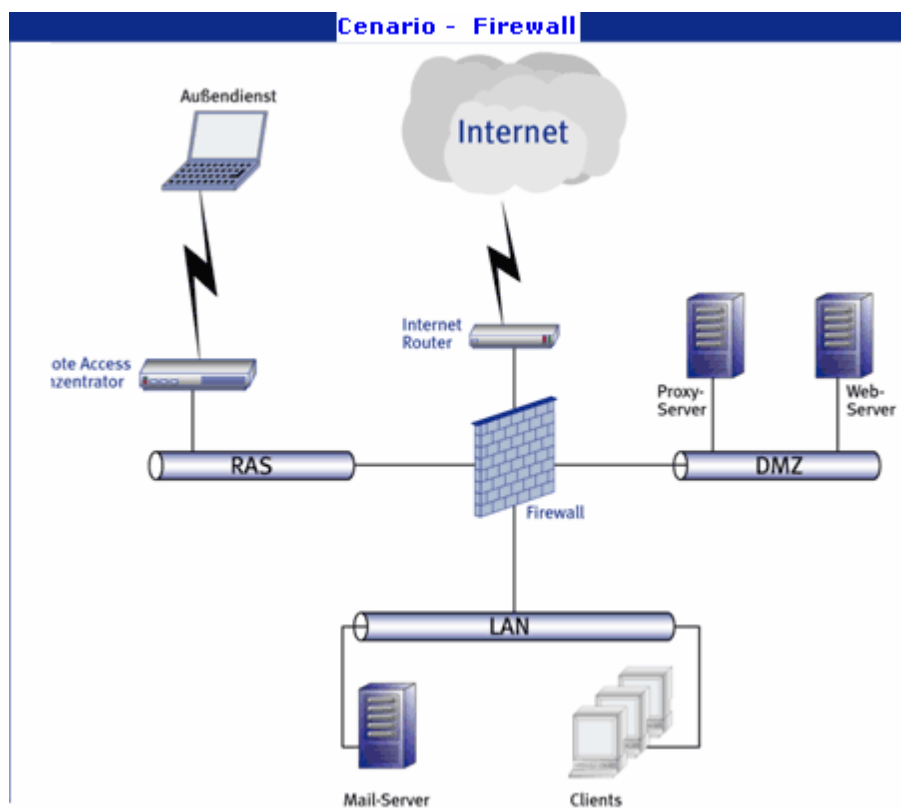


Figura 2 - Cenário do *Firewall*

Todo o tráfego, nos dois sentidos, tem de passar por esse ponto e, dessa forma, atender aos requisitos da política de segurança da instalação. Uma *firewall* funciona como separador de ambientes e, ao mesmo tempo, como controlador de acesso e analisador de tráfego (CARUSO, 1999).

Em geral, um *firewall* é composto por diversos dispositivos, variando em função de cada ambiente, e implica uma complexidade razoável. Além do custo,

um *firewall* tem outras desvantagens, entretanto, ainda é o meio mais efetivo de proteger uma instalação.

O *firewall* facilita muito o trabalho de segurança, indo além do escopo para o qual foi projetado, conforme podemos analisar os itens citados abaixo:

- Foco de decisões sobre segurança – pode-se centralizar todas as decisões sobre segurança em cima do *firewall*, pois ele passa a monitorar o ponto em que a rede se interliga com a *Internet*,

- Imposição da política de segurança – o *firewall* pode ser utilizado para forçar a política de segurança em uma organização, fazendo com que somente as atividades pré-definidas de acordo com a política de segurança sejam autorizadas pelo *firewall*.

- Registro de atividades – o mecanismo de *firewall* pode ser utilizado para registrar as atividades dentro da *Internet*. O administrador da rede pode registrar e controlar tudo o que passa através do *firewall*.

- Limitação de exposição – devido ao fato de um *firewall* permitir a separação de ambientes, o administrador da rede impede que um problema afete a um ambiente em particular sem que se propague para outro.

Apesar das vantagens mencionadas acima, o *firewall* não protege contra todos os riscos e ameaças um determinado ambiente, deve-se complementar a segurança proporcionada por um *firewall* com outras medidas de segurança.

Abaixo as principais limitações que estão associadas ao *firewall*:

- Usuários mal-intencionados – não há como um *firewall* proteger uma rede contra esse tipo de usuário. Afinal, ele pode simplesmente efetuar uma cópia das informações sensíveis em algum tipo de mídia e carregar consigo. Além disso,

assim que o atacante estiver dentro dos limites do *firewall*, este mecanismo praticamente nada pode fazer contra este usuário.

- Conexões alternativas – um *firewall* nada pode fazer pela rede se houverem outras conexões que estão fora dos limites dele. Estas conexões alternativas são chamadas de “portas dos fundos”, por exemplo, o modem.

- Ameaças novas – se o *firewall* foi configurado para enfrentar todas as ameaças que existiam em determinada época, ameaças novas, surgidas depois de sua configuração, não serão barradas.

- Vírus – devido à natureza intrínseca dos diferentes tipos de vírus, é virtualmente impossível detectar vírus que estejam sendo descarregados com informações úteis. A única maneira de se proteger contra os mesmos é utilizar os softwares de antivírus (KATZAN JR, 2000).

2.3.5 Antivírus

Há 22 anos atrás, criar um antivírus era considerado um ótimo negócio. Principalmente porque não havia muita informação sobre estas pragas eletrônicas (para se ter uma idéia, na década de 80 só havia conhecimento de duas dúzias de vírus). Atualmente, já é impossível competir com as multinacionais que se dedicam inteiramente à criação de proteção.

Os antivírus são programas utilizados para detectar vírus num computador ou disquete. A maioria usa método simples de procura por uma seqüência de *bytes* que constituem o programa vírus. Desde que alguém tenha detectado e analisado a seqüência de *bytes* de um vírus, é possível escrever um programa que procura por essa seqüência. Se existe algo parecido, o programa antivírus anuncia que encontrou um vírus. O antivírus, por sua vez, funciona como uma

vacina dotada de um banco de dados que cataloga milhares de vírus conhecidos.

Quando o computador é ligado ou quando o usuário deseja examinar algum programa suspeito, ele varre o disco rígido em busca de sinais de invasores.

Quando um possível vírus é detectado, o antivírus parte para a limpeza, alguns antivírus conseguem reparar os arquivos contaminados; entretanto nem sempre isso é possível. Muitas vezes a única saída é substituir o arquivo infectado pelo mesmo arquivo “*clean*” do software original, ou de outro computador com programas e sistema operacional idênticos ao infectado. Dependendo do vírus e das proporções dos danos ocasionados, apenas alguém que realmente entenda do assunto poderá limpar o computador e, se possível, recuperar os arquivos afetados (GARGAGLIONE, 1999).

2.4 SISTEMAS PARA DETECÇÃO DE INTRUSÃO

A tecnologia evolui gradativamente e devido a isto as ferramentas e mecanismos de segurança também estão se adaptando a estas mudanças. Conforme (ALLEN, 1999), a Internet mudou as formas como se usam sistemas de informação.

As possibilidades e oportunidades de utilização são ilimitadas, assim como, infelizmente, os riscos e chances de ataques maliciosos. Por isso, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas. Mesmo assim, com a tecnologia disponível no momento, é praticamente impossível impedir que isso aconteça. Não existe um mecanismo único que forneça uma solução para esse problema. Desta forma, foi introduzido

o conceito de segurança em profundidade, que faz uso de várias camadas de segurança, englobando os sistemas de informação e as redes que os interligam.

Um dos mecanismos que pode desempenhar a função de mais uma camada para a proteção de sistemas de informação é conhecido como Sistema de Detecção de Intrusão (IDS). O sistema de detecção de intrusão ou IDS tem como objetivo de detectar as variações de comportamento na rede, os quais podem sinalizar a existência de um ataque ocasionado por alguém que esteja tentando entrar em um sistema ou se algum usuário legítimo está fazendo mau uso do mesmo (LAUREANO, 2003).

Isso pode ser feito por meio da monitoração de sistemas (*host-based*), pela monitoração do tráfego de rede (*network-based*) ou por uma combinação das duas formas de monitoração (sistemas híbridos). Estes sistemas procuram detectar tentativas de intrusão, gerando alertas que permitam a correção de eventuais problemas posteriores ou atuando sobre o tráfego de rede de maneira a interromper o ataque.

Segundo (LAUREANO, 2003), para obter as informações se a rede sofreu algum tipo de ataque ou invasão, é necessário que a ferramenta fique funcionando constantemente de modo que não seja percebida (*background*) e somente demonstre sua existência através de uma notificação quando detectar algo que seja suspeito ou ilegal, estas notificações irão ser relatadas através *e-mail*, *pager* e telefone ao responsável da rede, possibilitando assim uma elaboração de uma estratégia rápida e eficaz na prevenção de algum dano na rede.

2.4.1 Características dos IDS's

IDS's são ferramentas de segurança automatizadas que visam proteger a rede através da monitoração do tráfego de dados, gerando alarmes e informando sobre ações que violem a política de segurança de uma organização (KOZIOL, 2003).

A tecnologia dos IDS difere em escopo e em objetivo do *firewall* e serve como complemento a essa ferramenta. Ao passo que os *firewalls* situam-se às margens das redes, nos pontos de transição entre uma rede e outra, os IDS precisam estar imersos na rede, com grande visibilidade para todos os pacotes que trafegam no meio. Onde os *Firewalls* buscam evitar ataques, IDS são criados tomando por base o fato de que, mais cedo ou mais tarde, haverá um ataque que será capaz de burlar o *firewall* e penetrar na rede interna, onde o IDS deve detectar esta intrusão e agir de acordo para emitir alarmes (SOMMER, PAXSON 2003).

Se, analogamente, um *firewall* é a porta de um cofre, o IDS é o sensor de movimento que monitora a sala do cofre. A porta do cofre protege seu interior do meio externo, mas o sensor de movimento, ao detectar uma presença na sala do cofre, dispara os alarmes apropriados.

Um IDS então pode ser resumido como "um sistema digital capaz de monitorar o tráfego de um segmento de rede e classificá-lo como seguro e inseguro, e, em caso de apontamento de tráfego inseguro, determinar a insegurança do mesmo e alertar a administração da rede" (KOZIOL, 2003).

2.4.1.1 Características desejáveis em IDS's

Para que se possa considerar a implementação de IDS's como confiável, é necessário exigir da implementação um conjunto de características desejáveis,

propriedades que o IDS, como sistema automatizado e de alarmes, deva possuir (ALLEN, 2003):

- Simplicidade de configuração - os IDS's, preferencialmente devem ser simples e rápidos de se configurar, demandando pouco tempo para sua implantação numa rede, evitando que se desperdice recursos importantes na instalação de uma ferramenta auxiliar de segurança.

- Simplicidade de administração - estas ferramentas devem gerar alarmes que sejam facilmente interpretados pelo administrador do sistema, evitando complicações para a parte humana do processo.

- Independência de operação - a ferramenta não deve demandar operação manual, e salvo atualizações e intervenções administrativas, deve ser capaz de atender ao seu ciclo de vida sem interação humana (por ciclo de vida temos o conjunto de ações "captura de dados, análise, decisão, ação apropriada").

- Tolerância a falhas - como é uma ferramenta automatizada e não assistida, espera-se que a ferramenta não tenha travamentos nem chegue em condições de parada; caso estas condições aconteçam, a ferramenta deve ignorar o erro, assumir a falha encontrada e resumir sua operação normal. Nesta característica também se inclui a capacidade de retorno das operações com uma reinicialização do sistema.

- Segurança – o sistema deve ser seguro, de modo que tentativas de subversão ao seu sistema de análise de invasões sejam infrutíferas; Também não devem estar hospedados na mesma máquina quaisquer serviços que possam vir a ser explorados por um ataque direto ao sistema de detecção de intrusão. Por estar inserido na rede, os sistemas de detecção de intrusão estão muito próximos dos *hosts* em produção e em caso de comprometimento do mesmo, o grau de

risco é muito grande para os sistemas de produção, pois o *host* que executa o IDS está diretamente conectado à rede, fazendo com que o comprometimento do mesmo exponha toda a rede ao invasor.

- Baixo impacto no funcionamento do sistema - os sistemas de detecção de intrusão devem funcionar como monitores de tráfego, e não devem gerar tráfego na rede que venha a prejudicar a operação normal dos sistemas, e nem estar instalados em máquinas de produção, pois a análise de tráfego demanda grande carga de processamento.

- Analisar padrões - seja através de bases de dados de assinaturas com informações sobre intrusões ou através da configuração meticulosa, a ferramenta de detecção de intrusões deve ser capaz de separar, entre todo o volume de tráfego de um segmento específico de rede, aquelas informações que podem constituir riscos para a segurança da organização.

- Discrição - um sistema de detecção de intrusão deve se manter em modo promíscuo em uma rede, ouvindo requisições e respondendo ao menor número possível de pacotes, de modo que um possível invasor não seja alertado da presença do sistema automatizado. Assim como as câmeras de vigilâncias são pequenas e difíceis de se distinguir, os IDS devem ser discretos e sua operação na rede não deve deixar pistas de que os há monitoração nos segmentos de rede.

- Resistente a erros de monitoração - um sistema automatizado de detecção de intrusão é suscetível a três tipos de erro: Falsos Positivos, Falsos Negativos e erros de subversão. Falsos Positivos são ocorrências de tráfego que a ferramenta classifica como ataques, mas não são; Falsos negativos são ocorrências em que o tráfego é uma ameaça, mas a ferramenta não foi capaz de captar ou interpretar corretamente e erros de subversão são ataques diretos à

ferramenta que geram falsos negativos ou que fazem com que a ferramenta perca a capacidade de interpretar tentativas de invasão corretamente.

2.4.1.2 Características indesejáveis em IDS's

Com as informações extraídas dos sistemas de computação, uma ferramenta de IDS pode identificar as tentativas de intrusão e até mesmo registrar a técnica utilizada (ROESCH, 1999 p. 229-238). Entretanto um IDS não é perfeito, podendo ocorrer:

- Falsos positivos – ocorrem quando a ferramenta classifica uma ação como uma possível intrusão, quando na verdade trata-se de uma ação legítima; Um bom exemplo de falso positivo é o ataque de *SYN FLOOD*. O simples fato de acessar um determinado tipo de página pode gerar uma detecção da ocorrência de um ataque *SYN FLOOD*.

- Falsos negativos – ocorrem quando uma intrusão real acontece, mas a ferramenta permite que ela passe como se fosse uma ação legítima;

- Subversão – ocorre quando o intruso modifica a operação da ferramenta de IDS para forçar a ocorrência de falso negativo.

Os sistemas de detecção de intrusão servem, como já foi citado, para indicar que alguma tentativa de intrusão que foi feita em um sistema. Para isto, podem ser classificados de duas maneiras com relação a sua forma de monitoração (origem dos dados) e aos mecanismos de detecção utilizada.

2.4.2 Formas de monitoração

Classificamos as ferramentas de detecção de intrusão com relação à sua posição perante a rede (NIDS e HIDS) e com relação ao seu escopo e tempo relativo de funcionamento (SIV e LFM) (ALLEN, 2000).

- HIDS

Os IDS baseados em *host*, que são computadores locais, foram os primeiros sistemas de detecção de intrusão implementados. O objetivo deles é monitorar toda a atividade existente em uma estação específica. O funcionamento desses sistemas se dá através da coleta e análise de dados originados em uma máquina que hospeda um serviço. Depois de coletados, esses dados podem ser analisados localmente ou até enviados para uma máquina remota responsável pelo exame (ANDERSON, 2001).

Resumidamente, podemos dizer que os sistemas baseados na estação monitoram dados em uma determinada máquina, sejam eles processos, sistemas de arquivos e o uso de Hardware da máquina.

Um exemplo típico de um sistema de coleta de dados seria um sistema de registros (*logs*). Esses sistemas são responsáveis pelo armazenamento de ocorrências em aplicações que rodam na estação. Ou seja, as aplicações estão configuradas para enviar seus registros para este sistema e ele é o encarregado de armazená-los em uma série de arquivos. Um eventual sistema de análise usaria essa base de registros do sistema comparando-a com padrões pré-estabelecidos com o objetivo de detectar intrusões.

Os HIDS são instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor.

A velocidade da rede e o uso de criptografia são facilmente tratados pelos sistemas HIDS. Todavia, como esse sistema é instalado na própria máquina a monitorar, pode ser desativado por um invasor bem-sucedido.

- NIDS

Os IDS baseados em *network*, ou seja, computadores em rede, monitoram todo o tráfego que passa através da rede, os dados ou informações deste tráfego são chamados de pacotes. Os pacotes que trafegam na rede são capturados e é feita uma análise em cada um deles para verificar se está dentro de padrões pré-determinados ou não, indicando respectivamente tráfego normal ou uma tentativa de ataque.

Em um meio compartilhado onde dois ou mais computadores estão interligados através da rede, os pacotes passam livremente e todas as interfaces, (mecanismos de entrada e saída de informações) conectadas aos computadores recebem estes pacotes. A princípio, todas as interfaces recebem todo o tráfego. Sendo assim, é necessário posicionar o NIDS na rede que se quer proteger para que ele possa receber os pacotes necessários para sua análise (ANDERSON, 2001).

Os NIDS são instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes de rede e seus detalhes como informações de cabeçalhos e protocolos. Podem monitorar diversos computadores simultaneamente. Todavia, sua eficácia diminui na medida em que o tamanho e a velocidade da rede aumenta, pela necessidade de analisar os pacotes mais rapidamente.

- Híbridos

Os dois tipos de detecção de intrusão apresentados se diferenciam bastante, mas se complementam. À medida que os HIDS atuam somente em estações críticas (servidores), o NIDS atua analisando todo o tráfego de rede, inclusive para estações que não contém um sistema de detecção rodando. Uma configuração bastante comum seria a de um NIDS para a rede local e HIDS rodando nos servidores principais.

Esta combinação das duas técnicas é denominada de Híbrida (ALLEN, 1999).

- SIV

Existem ferramentas que podem ser executadas em *hosts* para se verificar se, em caso de invasão, o invasor efetuou alguma modificação em comandos críticos do sistema, deixando para trás marcas da invasão. Um SIV (*System Integrity Verifier*) é uma ferramenta capaz de verificar a integridade do sistema invadido através de um banco de assinaturas e da comparação desse banco de assinaturas com os arquivos monitorados do sistema afetado.

Ferramentas SIV podem funcionar em tempo real, verificando os arquivos monitorados em tempos pré-determinados ou ainda funcionar conforme a demanda do administrador do sistema.

- LFM

Assim como os NIDS que monitoram o tráfego de rede, ferramentas automáticas de monitoração de registros históricos podem ser aplicadas para se verificar de sistemas bem conhecidos da rede, buscando informações que caracterizem mal uso dos sistemas. O LFM (Log File Monitors) ou monitor de *logs* podem incorrer no problema de apresentarem demora para analisar todo o tráfego, por vezes deixando de emitir os alarmes apropriados em tempo de se evitar danos aos sistemas de rede.

2.4.3 Quanto às formas de detecção

Muitas ferramentas de IDS realizam suas operações a partir da análise de padrões do sistema operacional e da rede, tais como: utilização de CPU, dispositivo de entrada e saída, uso de memória, atividades dos usuários, número de tentativas de *login*, número de conexões, volume de dados trafegando no segmento de rede entre outros. Estes dados formam uma base de informação sobre a utilização do sistema em vários momentos ao longo do dia, e também bases de informações com padrões de ataque previamente montados, permitindo também a configuração dos valores das bases bem como inclusão de novos parâmetros (ALLEN, 2000).

2.4.3.1 Detecção por assinatura

Os dados coletados são comparados com uma base de registros de ataques conhecidos (assinaturas). Por exemplo, o sistema pode vasculhar os pacotes de

rede procurando seqüências de *bytes* que caracterizem um ataque de *buffer overflow* contra o servidor.

A detecção por assinatura analisa a atividade do sistema, procurando por eventos ou conjunto de eventos que correspondem a um determinado padrão e caracteriza um ataque conhecido. Em geral, essa abordagem gera um número menor de falsos positivos, se comparados à detecção por anomalia. Por se basear em padrões a detecção é mais rápida e específica, possibilitando ações diferenciadas para cada caso, mas em compensação é ineficiente para novos padrões de ataques.

Uma assinatura tradicional contém uma seqüência de *bytes* que representam ou especificam um ataque. Se esta assinatura estiver no pacote de rede, é uma provável indicação de um ataque. Os sistemas NIDS utilizam esta abordagem para a detecção de intrusão, através da utilização de expressões regulares, análise de contexto ou linguagens de assinatura, os pacotes de rede são analisados e comparados com uma base de dados de assinaturas. Um exemplo de IDS baseado em assinatura é o SNORT (SOMMER; PAXSON 1998 P. 262-271).

2.4.3.2 Detecção por anomalia

Os dados coletados são comparados com registros históricos da atividade considerada normal do sistema. Desvios da normalidade são sinalizados como ameaças. Os modelos estatísticos mais utilizados em detectores de intrusão por anomalia foram propostos em (DENNING, 1987).

A detecção de anomalia caracteriza como ataque os padrões de comportamento considerados incomuns em um sistema ou

rede. Para caracterizar um comportamento como anormal, são construídos perfis com base em dados coletados durante um período de operação normal. O IDS então utiliza um conjunto de métricas para determinar quando a informação monitorada difere dos perfis estabelecidos. A detecção de anomalia, por ser baseada no comportamento normal do sistema e não nas características específicas do ataque, como na detecção por assinatura, é capaz de detectar ataques desconhecidos. Além disso, em alguns casos, as informações produzidas pela detecção de um ataque podem ser utilizadas como assinatura na detecção. Entretanto, a maior desvantagem dessa abordagem é que geralmente a análise produz um grande número de falsos positivos. Isso acontece, porque o comportamento normal de um sistema pode variar de acordo como tempo através da adição de novos usuários e da utilização de novas aplicações.

Ainda neste contexto existem quatro modelos estatísticos que podem ser utilizados em um detector de intrusão por anomalia. Cada modelo descrito na seqüência é considerado apropriado para um tipo particular de métrica.

- Modelo operacional – este modelo aplica-se a métricas como, por exemplo, contadores de eventos para o número de falhas de *login* em um determinado intervalo de tempo. O modelo compara a métrica a um limiar

definido, identificando uma anomalia quando a métrica excede o valor limite. Esse modelo pode ser aplicado tanto na detecção por anomalia quanto na detecção por assinatura.

- Modelo de média e desvio padrão – este modelo propõe uma caracterização clássica de média e desvio padrão para os dados. Uma nova observação de comportamento é identificada como anormal se ela encontra-se fora de um intervalo de confiança. Esse intervalo de confiança é definido como sendo d desvios padrões da média, para algum parâmetro d . Denning levanta a hipótese de que essa caracterização é aplicável a métrica do tipo contador de eventos, intervalos de tempo e medidas de recursos.

- Modelo multivalorado – este modelo é uma extensão ao modelo de média e desvio padrão, baseia-se na correlação entre duas ou mais métricas. Desse modo, ao invés de basear a detecção de uma anomalia estritamente em uma métrica, essa detecção é baseada na correlação dessa métrica com alguma outra medida.

- Modelo de processo de *Markov* – este modelo é mais complexo e limitado a contadores de eventos. Segundo o mesmo, o detector considera cada tipo diferente de evento de auditoria como uma variável de estado e usa uma matriz de transição de estados para caracterizar as frequências com que ocorrem as transições entre os estados. Uma nova observação de comportamento é definida como anormal se sua probabilidade, determinada pelo estado anterior e pelo valor na matriz de transição de estados, for muito baixa. Esse modelo permite que o detector identifique seqüências não usuais de comandos e eventos, introduzindo a noção de análise de fluxos de eventos com memória de estado (DENNING, 1987 p. 222-232).

2.4.3.3 Detecção híbrida

O mecanismo de análise combina as duas abordagens anteriores, buscando detectar ataques conhecidos e comportamentos anormais.

A detecção por assinatura é a técnica mais empregada nos sistemas de produção atuais. Os sistemas antivírus também adotam a detecção por assinatura. A detecção de intrusão por anomalia ainda é pouco usada em sistemas de produção (LAUREANO, 2003).

2.4.4 Modelo conceitual de uma ferramenta de IDS

Devido a grande variedade de sistemas de IDS foi proposto um modelo, CIDF – Common Intrusion Detection Framework (LAUREANO, 2003), este modelo Agrupa um conjunto de componentes que define uma ferramenta de IDS:

- Gerador de Eventos (E-boxes) - A função deste componente é obter os eventos a partir do meio externo ao CIDF, ou seja, ele “produz” os eventos mas não os processa, isso fica a cargo do componente especializado na função de processamento, que por sua vez após analisar os eventos (violação de política, anomalias, intrusão) envia os resultados para outros componentes.
- Analizador de Eventos (A-boxes) - Este componente basicamente recebe as informações de outros componentes, analisa estas informações e as envia de forma resumida para outros componentes, ou seja, recebe os dados de forma bruta, faz um refinamento e envia para outros.

- Database de Eventos (D-boxes) - A função deste componente é armazenar os eventos e/ou resultados para uma necessidade futura.
- Unidade de Resposta (R-boxes) - Este componente é responsável pelas ações, ou seja, matar o processo, resetar a conexão, alterar a permissão de arquivos, notificar as estações de gerência, etc.

O modelo pode ser demonstrado conforme figura abaixo.

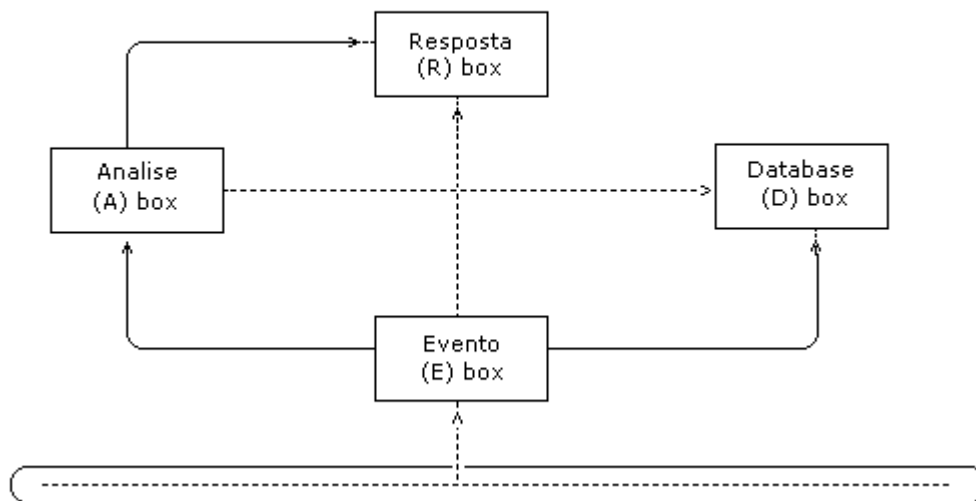


Figura 3 - Conjunto de componentes que define uma ferramenta de IDS

Algumas características desejáveis dos componentes são:

- Devem ser reutilizados em um contexto diferente do qual foram originalmente desenvolvidos, ou seja, devem ser configuráveis de forma a adaptarem-se a ambientes distintos;

- Os sistemas de IDS podem ser elaborados em módulos com funções distintas;
- Estes componentes podem compartilhar/trocar informações entre si, via API ou através da rede, para uma melhor precisão na identificação de ataques;
- Componentes novos devem automaticamente identificar os demais componentes;
- O grupo de componentes poder atuar mutuamente de forma a dar a impressão de ser um único elemento.

Segundo a padronização do CIDF, existe um modelo de linguagem para troca de informações entre os componentes, o CISL – *Common Intrusion Specification Language*, este formato é referenciado como GIDO – *generalized intrusion detection objects*.

A comunicação entre os componentes é definida por uma arquitetura de camadas:

- *Gido layer*
- *Message layer*
- *Negotiated Transport layer*

Esta arquitetura garante a comunicação entre os elementos, bem como sistemas de criptografia e autenticação, estes mecanismos estão definidos no *Comm – Communication in the Common Intrusion Detection Framework*.

2.4.5 Modelo CIDF (*Common Intrusion Detection Framework - Working Group*)

O *Common Intrusion Detection Framework Working Group* foi à primeira tentativa de padronizar os sistemas de detecção de intrusão, no final da década

de 90, como uma iniciativa da DARPA (*Defense Advanced Research Projects Agency*). A necessidade de padronização surgiu com o advento de ataques cada vez mais sofisticados, e capazes de serem distribuídos através de redes metropolitanas durante longos períodos, exigindo a utilização de Sistemas de Detecção de Intrusão Distribuídos. Neste tipo de ambiente distribuído a habilidade de IDS's, e de seus componentes, compartilharem informações "avançadas" se tornou extremamente importante (ALLEN, 2003).

O objetivo do CIDF é desenvolver protocolos e interfaces de programação, de forma que projetos de pesquisa em detecção de intrusão possam compartilhar informações e recursos, para permitir que diferentes componentes de um IDS compartilhem informações da forma mais detalhada e completa possível e que um sistema possa ser reutilizado em contextos diferentes do qual ele foi originalmente configurado.

O esforço principal do CIDF *working group* é definir uma "linguagem" de camada de aplicação para descrever informações de interesse de um sistema e um protocolo para codificar essa informação para compartilhá-la entre componentes.

A última atualização do CIDF consta de 10 de setembro de 1999, aparentando que o projeto está suspenso.

2.4.6 Limitações do IDS

Existem características limitantes nas ferramentas de detecção de intrusão. Segmentação da rede, limitação de recursos, ataques desferidos contra o próprio IDS e técnicas específicas de evasão.

O modelo CIDF possui falhas ao considerar que pacotes de dados contêm informações suficientes para se interpretar e atribuir um grau de periculosidade ao tráfego analisado e também ao considerar que o computador de destino irá interpretar os pacotes enviados da mesma maneira que o IDS irá. Estas limitações podem ser exploradas e a ferramenta pode ser fragilizada, suspendendo assim sua capacidade de interpretar o tráfego corretamente (ALLEN, 2003).

- Segmentação de rede - é uma necessidade moderna. Devido ao crescimento das redes *ethernet*, a aplicação dos *switches* em redes é cada vez mais comum. Em uma rede segmentada, um NIDS tem alcance limitado ao domínio de broadcast que é atingível. Esta fragmentação afeta os NIDS, e pode ser evitada através do planejamento da implementação do IDS, garantindo o seu posicionamento em local de alta visibilidade da rede.

- Limitação de recursos - um IDS também possui recursos de processamento, armazenamento e memória que são utilizados para se analisar o tráfego. Um atacante que possua recursos suficientes pode ser capaz de sobrepujar a capacidade de processamento da ferramenta. Um motivo adicional para a limitação de recursos ser um risco real é que comparativamente, se o atacante gasta aproximadamente 5 ciclos de processamento para gerar um pacote aleatório, a ferramenta de IDS gastará 7 ciclos de processamento para interpretar este mesmo pacote (KOZIOL, 2003).

- Ataques contra o IDS - as ferramentas IDS também são frágeis e suscetíveis a ataques. Uma ferramenta IDS que venha a ser comprometida em uma rede apresenta um grau de risco ainda maior do que um ataque a um *host* qualquer da rede, visto que as ferramentas de IDS são projetadas para possuírem

alto grau de visibilidade na rede e as ferramentas, por serem automatizadas, recebem menos esforço administrativo, facilitando os ataques.

- Evasões simples - a evolução das redes está trazendo ferramentas melhores para evasão de IDS. Cifragem de dados e o uso de VPN's são técnicas bastante exploradas para se evadir do controle de um IDS.

- Evasões complexas - existem duas formas complexas de se evadir um IDS: inserção e evasão. O método de inserção baseia-se no conceito de detecção de invasão através de base de conhecimentos; se o invasor sabe o que o IDS está buscando na rede, forja-se uma larga quantidade de pacotes com o conteúdo que o IDS busca, forçando a geração de falsos positivos que por sua vez demandarão bastante esforço do administrador de sistemas para identificar o verdadeiro pacote de invasão entre uma quantidade grande de dados. Evasão ataca diretamente uma fragilidade do modelo CDIF que presume que tanto o IDS quanto o *host* de destino irão reagir da mesma maneira perante um pacote. Por definição a pilha TCP exige que todos os *hosts* reajam da mesma forma perante um pacote, porém é sabido que implementações incorretas, versões de software e de *drivers* de rede podem influenciar nesta interpretação de dados; além disso, o tráfego é diferente em pontos diferentes da rede: se um IDS recebe um pacote em um momento, nada garante que o *host* destino irá receber o mesmo pacote pois entre o IDS e o *host* destino sempre há a rede local e o tráfego normal da rede, com isso não é possível garantir que ocorrência de atraso possa influenciar tanto na leitura do pacote pelo IDS quanto na recepção do pacote pelo *host* de destino.

2.4.7 Ferramentas existentes

A tecnologia de IDS ainda é imatura e dinâmica (está continuamente em desenvolvimento e pesquisa). Um IDS não utiliza medidas preventivas, quando um ataque é descoberto age ele como um informante. A maneira mais comum para descobrir intrusões é a utilização dos dados das auditorias gerados pelos sistemas operacionais e ordenados em ordem cronológica de acontecimento, sendo possível à inspeção manual destes registros, o que não é uma prática viável, pois estes arquivos de *logs* apresentam tamanhos consideráveis.

Existem diversos tipos de ferramentas IDS para diferentes sistemas operacionais, porém as ferramentas IDS trabalham basicamente de modo parecido, ou seja, analisando os pacotes que trafegam em uma rede e comparando-os com assinaturas já prontas de ataques, identificando-os de forma fácil e precisa qualquer tipo de anomalia ou ataque que possa vir a ocorrer em uma rede ou computador (KOZIOL, 2003).

2.4.7.1 Emerald

O EMERALD – *Event Monitoring Enabling Responses to Anomalous Live Disturbances* (Monitoração de Eventos Ativando Respostas a Perturbações Anômalas *on-line*), desenvolvida pela SRI Internacional, verifica se houve uma intrusão baseando em desvios de comportamento do usuário (anomalias) e padrões de intrusão conhecidos (assinaturas). A meta principal do projeto EMERALD é trabalhar com redes de empresas grandes (heterogêneas). Estes

ambientes são difíceis de monitorar e de analisar devido à diversificação da informação que trafega pela rede. O EMERALD estrutura os usuários em um conjunto de domínios independentemente administrados. Cada conjunto provê uma cobertura de serviços de rede (ftp, http, telnet) que podem ter relações de confiança e políticas de segurança diferentes entre si (PORRAS, 1996).

A estrutura hierárquica provê três níveis de análise: monitores de serviço, domínio e empresa. Estes monitores possuem a mesma arquitetura básica: um conjunto de mecanismos de perfil (para descobertas de anomalia), mecanismos de assinatura e um componente determinador que integra os resultados gerados pelos mecanismos. É possível configurar e personalizar cada nível.

No nível mais baixo, o monitor de serviço suporta a detecção de intrusão para os componentes individuais e serviços de rede dentro de um domínio, sondando ou verificando *logs* e eventos, verificando assinaturas e realizando análises estatísticas. Os monitores de domínio integram a informação dos monitores de serviço para prover uma visão de invasões, enquanto os monitores de empresa executam uma análise interdomínio para avaliar as ameaças sob uma perspectiva global.

O NIDS (*Network Intrusion Detection System*) demonstrou técnicas de análise estatísticas que poderiam ser efetivas com usuários ou aplicações (ANDERSON, 2001). A monitoração de aplicações (anonymous ftp, por exemplo), era efetiva se menos perfis de aplicação fossem exigidos. O EMERALD generaliza a técnica de perfil pela abstração do que é um perfil, separando gerenciamento de perfil de análise de perfil. O EMERALD está em contínuo desenvolvimento, sendo um exemplo de rumo que futuras ferramentas de IDS podem tomar.

2.4.7.2 Netstat

O NetSTAT (VIGNA, 1998) é a mais recente ferramenta de uma linha de ferramentas de investigação “STAT” produzida pela Universidade da Califórnia em Santa Bárbara. Este IDS explora o uso da análise de transição de estados para descobrir a intrusão em tempo real.

Sistemas HIDS analisam se houve uma invasão a partir da análise de trilhas de auditoria. Porém, na análise STAT (PORRAS, 1992) a informação de trilha de auditoria é transformada por um analisador que filtra e abstrai as informações que são recolhidas na trilha de auditoria. Estas abstrações, que são mais adequadas para análise, portabilidade e compreensão humana, são chamadas de assinaturas de estados. A análise da assinatura modifica a seqüência de estados, cada mudança de estado deixa o sistema mais próximo de identificar uma intrusão. Seqüências de intrusão são definidas pelos diversos estados que são capturados neste sistema baseados em regras.

A aplicação inicial do método era um sistema HIDS desenvolvido para UNIX e chamado de USTAT. Era composto de um pré-processador, uma base de conhecimento (ações e regras), um mecanismo de inferência e um mecanismo de decisão.

O NetSTAT está sob desenvolvimento e difere dos sistemas NIDS. O NetSTAT é composto de sondas que agem remotamente em cada sub-rede, caso alguma sonda identifique algum componente de intrusão, um evento é enviado as outras sondas interessadas para adquirir mais detalhes sobre a intrusão. Desta forma é possível identificar intrusões em sub-redes.

As sondas são suportadas por um analisador, que é responsável pela administração da base de dados (base de conhecimento). É o analisador que determina qual e como os eventos serão monitorados.

2.4.7.3 BRO

O BRO (PAXSON, 1998) é uma ferramenta de investigação que foi desenvolvida pelo *Lawrence Livermore National Laboratory*. Foi construído, em parte, para explorar as emissões relacionadas à robustez de ferramentas de IDS, isto é, avaliando quais características fazem um IDS resistir a ataques contra si mesmo. As metas do projeto abrangem:

- Monitoração *high-load* (capacidade de controlar altos tráfegos de rede);
- Notificação em tempo real;
- Separação de políticas de filtros, identificação e reação aos eventos.

Facilita a aplicação e manutenção do sistema;

- Um amplo banco de dados com relação a ataques conhecidos e habilidade de acrescentar novos ataques a esta base;
- Habilidade para repelir ataques contra si mesmo da rede associada aos protocolos *finger*, *ftp*, *portmapper* e *telnet* que são os protocolos.

O BRO trabalha com uma hierarquia de três níveis, na camada mais baixa é utilizado um utilitário chamado *libpcap*, este utilitário extrai pacotes sobre os quais o BRO trabalha atualmente. A camada de evento executa verificações de integridade nos cabeçalhos (*headers*) dos pacotes, que verifica se deve ser feita uma análise mais profunda no pacote ou não. Na terceira camada os pacotes passam por um *script* que verificam as políticas de segurança.

Atualmente o BRO monitora quatro aplicações (*finger*, *ftp*, *portmapper* e *telnet*), mas novas aplicações podem ser adicionadas a partir de uma derivação de uma classe em C++, somente devem ser acrescentadas algumas informações que correspondem à nova aplicação a ser monitorada (ROESCH, 1999 p. 229-238).

2.4.7.4 SNORT

O SNORT é um dos NIDS mais utilizados atualmente (KOZIOL, 2003). O SNORT mantém regras de detecção de intrusão em uma lista através do controle de uma cadeia de cabeçalhos (*headers*) e opções (*options*). Através da análise dos cabeçalhos dos pacotes de rede, chegam-se as possíveis opções de análise.

A cadeia de regras é pesquisada recursivamente para cada pacote de rede que chega ao computador. A maior vantagem do SNORT é a simplicidade para se escrever novas regras de detecção, possibilitando a tomada de ações ou simplesmente a notificação do administrador de rede (ROESCH, 1999 p. 229-238).

O SNORT é uma ferramenta *Open Source*, ou seja, é um software livre de custo e tem sido utilizada com mais frequência na implementação da segurança de um servidor ou servidores em uma rede (e da própria rede em si). Ele é classificado como ferramenta NIDS (*Network Intrusion Detection System*) que, de forma simples, é um sistema que analisa pacotes que trafegam em uma rede de pequeno ou médio porte a partir de um *host/node* dessa rede, comparando tais pacotes com um banco de dados baseados em regras pré-estabelecidas (*ruleset*), que geralmente são assinaturas de comportamento ou ação de diversos tipos de ataques conhecidos, gerando alertas a cada vez que um é detectado.

O SNORT é considerado uma ferramenta de fácil instalação e utilização até mesmo para o usuário sem muita experiência em IDS, porém ao mesmo tempo, possuindo diversas formas de configuração e adaptação às mais variadas situações e tipos de rede.

Uma característica favorável do SNORT está relacionada, é que o mesmo permite atualização automática de suas assinaturas de ataque via *internet* e com isto reduz falhas do tipo falso positivo. Outro aspecto positivo é que o próprio usuário personaliza sua regra de ataques e escolhe-os da forma que melhor se adapta.

3 CONCLUSÃO

Os negócios e novos mercados estão se direcionando cada vez mais para a *Internet* e *Intranets*. Torna-se necessário o conhecimento e análise dos riscos e vulnerabilidades a que estamos expostos, de forma que possamos definir os mecanismos adequados para a segurança.

Apesar dos problemas, podemos afirmar que o uso adequado da tecnologia de segurança e dos mecanismos de proteção e controle na *Internet* e *Intranet* permite realizar operações comerciais em condições mais seguras do que os meios de transações e comunicações convencionais.

De nada valem os conceitos e preocupações contidos neste trabalho se a organização não tem a intenção de formar ou adotar uma “cultura” voltada para a segurança. A segurança não é um ato isolado em um dado momento ou de competência de apenas algumas pessoas.

Cada vez mais, no dia-a-dia de cada funcionário, por mais simples que seja sua função, devem ser colocados periodicamente os conceitos básicos de segurança e deve ser exigida sua parcela de colaboração.

A sobrevivência da empresa não é fundamental apenas quanto ao aspecto da rentabilidade do negócio, mas também quanto ao aspecto da manutenção da operacionalidade em níveis que não possam interrompê-la.

Com base nestas informações foi apresentada uma introdução a sistemas de detecção de intrusão, de forma geral e passando pelos seus diferentes tipos de detecção e de análise.

Atualmente, segurança é um assunto que vem conseguindo cada vez mais a atenção tanto da área de pesquisa quanto nas implementações. A cada dia,

surgem novas soluções que tentam resolver problemas customizados dos clientes. Já foram desenvolvidas várias ferramentas de segurança que auxiliam os administradores de rede, dentre elas o *firewall*, ferramentas criptográficas, VPN's, controles de acesso, antivírus e os sistemas de detecção de intrusão.

Os sistemas de detecção de intrusão têm como objetivo tentar reconhecer um comportamento ou uma ação intrusiva, através da análise das informações disponíveis em um sistema de computação ou rede, para alertar um administrador responsável pela rede ou automaticamente disparar contra-medidas.

Um IDS automatiza a tarefa de analisar dados da auditoria. Estes dados são extremamente úteis, pois podem ser usados para estabelecer a culpabilidade do atacante e na maioria das vezes é o único modo de descobrir uma atividade sem autorização, detectar a extensão dos danos e prevenir tal ataque no futuro, tornando desta forma o IDS uma ferramenta extremamente valiosa para análises em tempo real e também após a ocorrência de um ataque.

Embora ainda longe de estarem perfeitos, IDS's constituem-se em mais um importante auxiliar na melhoria da segurança assim como outras ferramentas de segurança dissertadas no estudo.

4 REFERÊNCIAS

ALLEN, Julia et al. **State of the Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99-TR028.** Disponível em: <http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html>. Acesso em: Janeiro de 2003.

ALLEN, Julia et al. **State of the Practice of Intrusion Detection Technologies.** Pittsburgh: Software Engineering Institute, 2000.

ANDERSON, Debra et al. (SRI International). **Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES) (SRI-CSL-95-06).** Menlo Park, CA: Computer Science Laboratory, SRI International, 2001. Disponível em: <http://www.sdl.sri.com/nides/index5.html>.

CAMPANA, C. **Ferramentas de segurança.** Disponível em: <http://www.rnp.br/newsge/9711/seguranca.html>. Acesso em: Março de 2004.

CARUSO, Carlos A. A.; STEFFEN, Flávio D. **Segurança em Informática e de Informações.** São Paulo: Editora SENAC, 1999.

DENNING, Dorothy E. **An Intrusion-Detection Model:** IEEE Transactions on Software Engineering. Cidade: Editora, 1987. v.13.

FANTINATTI, João Marcos. **Segurança em Informática: Metodologia e Prática**. São Paulo: MC Graw - Hill, 2002, 78p.

GARGAGLIONE, Bruno D.; PAULA, Pedro C. **Vírus – Uma Ameaça Letal**. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 1999.

GEORGE, Joel. **The Hacking Exposed**. Disponível em: <<http://www.hackingexposed.com/home.html>>. Acesso em: Abril de 2004.

HACKING EXPOSED – Disponível em: <<http://www.hackingexposed.com/tools/tools.html>>. Acesso em: Março de 2004.

KATZAN JR., Harry. **Segurança de Dados em Computação**. Rio de Janeiro. Livros Técnicos e Científicos, 2000.

KOZIOL, Jack. **“Intrusion Detection with Snort”**. USA: Editora Sams. 2003.

LAUREANO, Marcos A. P. **Sistemas para identificação de invasão**. Disponível em <<http://www.modulo.com.br/index.jsp>. Modulo Security>. Acesso em: Abril de 2003.

MAGALHÃES, Luzia E. R.; ORQUIZA, Liliam M. **Metodologia do Trabalho Científico: Elaboração de Trabalhos**. Curitiba: Fesp, 2002. 130p.

MEINELL C. **The Überhacker II**: More ways to break into a computer. Disponível em: <<http://www.happyhacker.org/tuh.shtml>>. Acesso em: Março de 2004.

PAXSON, Vern. "**Bro**: A System for Detecting Network Intruders in Real-Time," Proceedings of 7th USENIX Security Symposium, 1998.

PORRAS, Phillip A.; NEUMANN, Peter G. "**EMERALD**: Conceptual Overview Statement". Disponível em: <<http://www.sdl.sri.com/papers/emerald-position1>>. 1996.

PORRAS, Phillip A.; NEUMANN, Peter G. "**EMERALD**: Event Monitoring Enabling Responses to Anomalous Live Disturbances". Disponível em: <<http://www.sdl.sri.com/papers/emerald-niss97>>. 1997.

PORRAS, Phillip A. "**STAT**: A state transition analysis tool for intrusion detection," M.S. thesis, Computer Science Dep., University of California Santa Barbara, 1992.

ROESCH, Martin. "**Snort** - Lightweight Intrusion Detection for Networks". Proceedings of the 13th Conference on Systems Administration. 1999, 238p.

SHIREY, R. **Internet Security Glossary**. Disponível em: <<http://www.ietf.org/rfc/rfc2828.txt>>. Acesso em: Maio de 2000.

SOMMER, Robin; PAXSON, Vern. "**Enhancing byte-level network intrusion detection signatures with context**". Proceedings of the 10th ACM conference on Computer and communication security. 2003, 271p.

VIGNA, Giovanni; KEMMERER, Richard A. "**NetSTAT**: A Network-Based Intrusion Detection Approach." Proceedings of the 14th Annual Computer Security Applications Conference, 1998.

5 GLOSSÁRIO

Backups – Gravação de dados ou informações em mídias, fitas DLT, disquetes, ou outro computador;

Bit - menor unidade de informação do computador.

Buffer - designa um trecho de memória para armazenamento temporário de dados.

Byte - 1 Byte é composto por 8 bits.

Chave – seqüência de símbolos destinada a permitir que o algoritmo cifre uma mensagem em texto claro ou decifre uma mensagem criptograda.

Chave de acesso – código de identificação de determinado usuário.

Cifragem – processo de transformação de uma mensagem de texto claro para texto cifrado, de forma a torná-la ininteligível.

Criptografia – técnica para converter uma mensagem de texto claro para texto cifrado ou vice-versa.

Decifração – técnica inversa a cifragem; consiste na transformação de um criptograma em texto claro pelo uso do algoritmo e da chave de cifragem.

L0phtcrack's – Programa que testa sucessivamente palavras contidas em um dicionário até encontrar a **senha** de um sistema;

Modem – equipamento eletrônico que converte o código binário usado internamente nos computadores em tons sonoros, para que sejam transmitidos por linhas de comunicação, ou que executam o processo inverso, convertendo os tons sonoros em código binário novamente;

Penetração – ato de entrar em um sistema ou acessar mensagens sem a devida autorização.

ethernet - Uma das arquiteturas possíveis em redes locais. As redes Ethernet usam normalmente cabos coaxiais que interligam vários computadores. Cada um deles acessa à rede em concorrência com os outros, existindo depois regras/convenções que permitem designar qual o computador que deve transmitir informação num determinado instante. A informação pode ser transmitida em modo "Broadcast", ou seja, para todos os outros computadores da rede e não apenas para um só.

FTP - File Transfer Protocol é um protocolo da Internet para transferência de arquivos;

HTTP - é um protocolo utilizado para acessar sites de páginas da Web;

LAN - Local Area Network. Rede Local. É uma rede com 2 ou algumas dezenas de computadores que não se estende para além dos limites físicos de um qualquer edifício. Normalmente utilizada nas empresas para interligação local dos seus computadores. Existem varias tecnologias que permitem a realização de uma rede local, sendo as mais importantes, a Ethernet e o Token-Ring;

LFM - (Log File Monitors) ou monitor de *logs*;

Logs - são registros de atividades gerados por programas de computador;

Login - é a operação através da qual o usuário é identificado e reconhecido pelo sistema;

Overflow - que significa “entornar”, “extravasar”, “verter para fora algo que excedeu a capacidade”;

SIV - (*System Integrity Verifier*) verifica a integridade do sistema invadido;

SYN FLOOD - tentativa de desabilitar um equipamento ou até mesmo a rede inteira;

TELNET - permite que se uma conexão remota com outro computador na *Internet*;