HUGO HENRIQUE FURLAN DAMACENO

DETECÇÃO DE INTRUSOS EM REDES DE COMPUTADORES

Assis
2008

DETECÇÃO DE INTRUSOS EM REDES DE COMPUTADORES

HUGO HENRIQUE FURLAN DAMACENO

Trabalho de Conclusão de Curso Apresentado ao
Instituto Municipal de Ensino Superior de Assis,
como requisito do Curso de Graduação, analisado
pela seguinte comissão examinadora:

Orientador: Alexandre L`Erário

Analisador (1): _____

Analisador (2): _____

Assis
2008

HUGO HENRIQUE FURLAN DAMACENO

DETECTAÇÃO DE INTRUSOS EM REDES DE COMPUTADORES

apresentado ao
Instituto Municipal de Ensino Superior de Assis,
como requisito do Curso de Graduação, analisado
pela seguinte comissão examinadora:

Orientador: Alexandre L`Erário

Área de Concentração: _____

_____

Assis
2008

DEDICATORIA.

Dedico este trabalho primeiramente aos meus familiares e minha noiva que me apoiaram todo tempo nesses anos cursados neste curso, também aos meus amigos que me ajudaram e meu orientador.

AGRADECIMENTOS.

Agradeço primeiramente a Deus, por ter me dado todas as condições para chegar até aqui e de me dar saúde para estar hoje realizando este trabalho;

Aos meus colegas de classe da faculdade, e também aos meus colegas de serviço, meus amigos, que sempre me apoiaram, também agradeço a Engemap, pois me deu total condição para eu poder finalizar este trabalho;

Ao meu orientador Alexandre L`Erário por suas idéias e opiniões ao meu trabalho;

Agradeço especialmente a minha noiva Natalia Carriel de Camargo por estar comigo em todos os momentos, sempre me dando forças para realizar este trabalho, me dando animo e coragem.

RESUMO.

Mesmo com o avanço da tecnologia, existe vários problemas com invasões em computadores. No que diz respeito às empresas que utilizam redes, as invasões tornam mais comuns. Da mesma forma que por um lado estes recursos facilitam o trabalho de seus funcionários, quando são mal utilizados podem expor a empresa a grandes riscos que vão desde infecção de arquivos por vírus até invasão do sistema e roubo de informações sigilosas causando prejuízos incalculáveis. Para evitar estes tipos de transtornos nas empresas os seus funcionários além de ter a consciência do que é perigoso ou seguro, também devem usar as ferramentas de proteções como antivírus, *firewall* e IDS. Ferramentas IDS (*Intrusion Detection Systems* – Sistema de Detecção de Intrusão) têm como objetivo detectar ataques à rede e comunicar ao administrador por meio de alertas antes que possam consumar-se e causar maiores prejuízos à empresa ou instituição que a utiliza, pois a utilização de antivírus, firewall não completamente eficientes e eficazes. Existe no mercado uma grande variedade de ferramentas IDS disponíveis. Algumas são soluções *open source* e outras ferramentas comerciais. Para este trabalho foi pesquisado e testado a ferramenta *Snort* onde pode-se trabalhar com versões gratuitas e também comercial, entretanto a usada neste trabalho foi a gratuita pois tem uma distribuição mais acessível.

Palavras – chave: IDS - Sistema de Detecção de Intrusão, SNORT.

ABSTRACT.

Even with the advance of the technology there is several problems due to computers invasions. Regarding companies that uses networks, the invasions becomes more common, where is used, e-mail, FTP, access sites, transfer files, VPNs. Just as the one hand these resources facilitate the job of their employees, when they are misused may expose the company to major risks ranging from files infection by viruses or invasion of the system and theft of confidential information causing incalculable damage. To avoid these types of disorders in companies beyond their employees to be aware of what is dangerous or safe should also use the tools of protections such as anti-virus, firewall and IDS. IDS tools (Intrusion Detection Systems), are designed to detect network attacks and to notify the administrator via alerts before they can consummate up and cause greater damage to the company or institution that uses it, because the use of antivirus, firewall, not completely efficient and effective. There are in the market a variety of tools available IDS. Some are open source solutions and other commercial tools. For this work was searched and tested the tool *Snort* where we can work with free versions and commercials too, therefore the one used in this work was the free one because it has a more accessible distribution.

Keywords: IDS - *Intrusion Detection Systems*, SNORT.

LISTA DE ILUSTRACOES

SUMÁRIO

1. INTRODUÇÃO

O uso de métodos de detecção de intrusos começou a crescer nos últimos anos. Usando métodos de detecção de intrusos, pode - se coletar e usar informações de tipos de ataques conhecidos e descobrir se alguém está tentando atacar a rede. A informação coletada desse modo pode ser usada para melhorar a segurança da rede como também para usos legais. Produtos comercias, bem como de código aberto, estão disponíveis para esses objetivos. Muitas ferramentas de avaliação de vulnerabilidades também estão disponíveis hoje no mercado, e podem ser usadas para avaliar diferentes tipos de falhas de segurança presentes na rede. Ferramentas como sistemas de antivírus e *firewalls* não são totalmente confiáveis quando falamos em empresas, pois não combatem totalmente alguns perigos como invasão dos seus sistemas, roubo, alteração e destruição de informações. Muitas vezes tais incidentes só são percebidos quando o sistema operacional pára de funcionar, o que pode ser tarde de mais e já ter causado grandes prejuízos.

Para minimizar tais riscos, uma opção para reforçar a segurança é através do uso de ferramentas IDS (Sistemas de Detecção de Intrusos), que possuem a função varrer constantemente o conteúdo que trafega pela rede, possuindo meios de detectar se algo de anormal está acontecendo, ou seja, Sistemas de detecção de intrusos são usados para descobrir se alguém entrou ou esta tentando entrar na rede; se achar algo ou detectar algo esta ferramenta indica ao administrador da rede através do envio de mensagens por e-mail ou para uma máquina específica relatando o fato.

1.1. OBJETIVO

Este trabalho tem por objetivo mostrar uma das ferramentas IDS, o SNORT que hoje é uma das mais utilizadas no mercado, segundo alguns fóruns relacionados sobre redes.

Mostrar as empresas ou instituições o perigo das lacunas deixadas pelos antivírus, firewalls, e que a ferramenta IDS pode ser a solução para evitar danos incalculáveis.

1.2. JUSTIFICATIVA

Atualmente a invasão de hackers no mundo da informática se tornou constante, e com isso as empresas procuram uma solução para proteger seus dados, arquivos, e este trabalho tem por finalidade apresentar uma IDS, que como já dito acima, é uma das melhores open source hoje neste mercado.

1.3. MOTIVAÇÃO

Aprofundar no conhecimento em redes, neste mundo da informática que é vasto de informações, conhecer mais das ferramentas que podem ser útil contra invasores.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

Com a realização deste trabalho pretende-se contribuir com as empresas que nos dias de hoje não tem muito conhecimento em ferramentas IDS.

1.5. ESTRUTURA DO TRABALHO

Este trabalho esta organizado em 8 capítulos, sendo o primeiro a introdução;

O capitulo 2 apresenta alguns conceitos teóricos sobre redes;

O capitulo 3 descreve sobre a ferramenta IDS (SISTEMAS DE DETECÇÃO DE INTRUSÃO);

O capitulo 4 é responsável pela descrição de outros aplicativos de segurança;

O capitulo 5 apresenta a metodologia Snort, com seus conceitos, regras, arquitetura;

O capitulo 6 se descreve passo á passo as devidas instalações e configurações para trabalhar com o Snort.

O capitulo 7 é responsável pela conclusão deste trabalho, se descrevendo as considerações finais;

O capitulo 8 traz dois anexos com um questionário sobre segurança de redes.

2. CONCEITO SOBRE REDES

Segundo Torres (2001), as redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante, como no exemplo do caixa eletrônico, onde pode-se estar tendo acesso aos dados de uma conta corrente que estão armazenados em um computador a centenas ou milhares de quilômetros de distância. Na internet, então, essa troca de informações armazenadas remotamente é levada ao extremo: acessa-se dados armazenados nos locais mais remotos e, na maioria das vezes, o local onde os dados estão fisicamente armazenados não tem a menor importância.

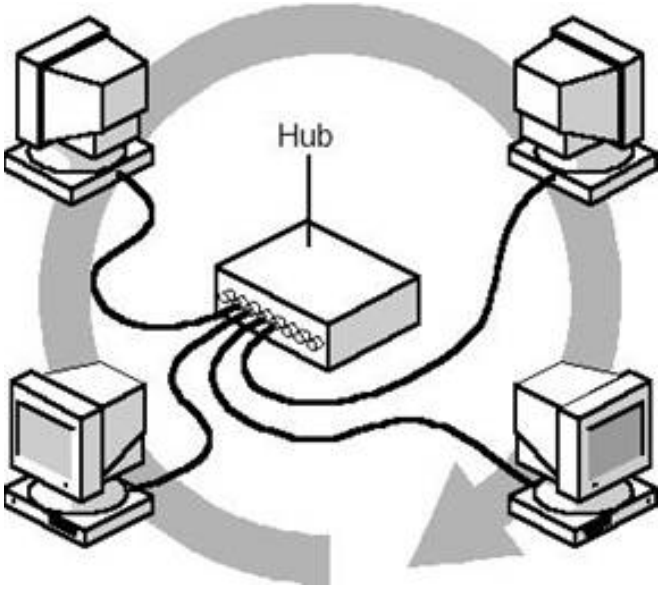

Figura 1. Exemplo ilustrativo de uma rede.

2.1. USOS DE REDES DE COMPUTADORES

Segundo Torres (2001), Com a queda do custo de implementação de redes, é praticamente impossível pensar em um ambiente de trabalho em que os micros existentes não estejam interligados, por menor que seja esse ambiente de trabalho. Mesmo em pequenos escritórios com apenas dois micros a necessidade de uma rede torna-se evidente quando é necessário ficar levando pen drives para lá e para

cá contendo arquivos de trabalho, ainda mais se esses arquivos forem grandes e não couber em um só pen drive, o que é cada vez mais comum.

2.1.1. Aplicações Comerciais

Segundo Tanembaum (1994), Uma empresa pode normalmente possuir vários computadores sendo usados para o mesmo tipo de projeto ou serviço, momentaneamente estes computadores trabalham individualmente, mas em algum momento precisará trocar informações ou dados do mesmo projeto entre um computador e outro, para isso precisaria conectá-los para que a troca de informações seja possível.

2.1.2. Aplicações Domésticas

Segundo Tanembaum (1994), Algum tempo atrás o uso de computadores em casa seria mais precisamente para processamento de textos, jogos, músicas, hoje o computador doméstico se tornou uma grande ferramenta, pois com ele se pode acessar a internet mantendo comunicação entre indivíduos, pesquisas, algum tipo de entretenimento, uma grande parte é responsável por este crescimento é devido os sites de relacionamentos.

2.1.3. Usuários Móveis

Segundo Tanembaum (1994), Por exemplo, alguns usuários que possuem Notebooks, celulares, por algum motivo específico gostariam de acessar fora da empresa ou casa, a internet, ou trocar informações via FTP com outro usuário, ou querem se manter conectados a alguns dispositivos mesmos longe dos mesmos, como usando fios ou cabos isto fica muito difícil, existe um grande interesse em redes sem fio, que pode ser usado se disponível em qualquer lugar.

3. SISTEMAS DE DETECÇÃO DE INTRUSÃO

Segundo Melo (1998), o termo intrusão pode ser caracterizado como uma violação da política de segurança de um sistema. A detecção de intrusão monitora e analisa os eventos de uma rede de computadores, visando a encontrar qualquer atividade que comprometa a confidencialidade, integridade e disponibilidade de recursos computacionais ou de rede. Seguindo o princípio de funcionalidade, verifica-se que o IDS tem como objetivo detectar ações, impróprias e incorretas, sendo um componente de defesa fundamental em uma organização. Além disso, estes sistemas também podem detectar ataques provenientes de portas legítimas que passam pelo firewall, abalando a segurança interna.

O IDS funciona como uma espécie de alarme contra invasões, tendo como base em suas detecções, assinaturas conhecidas ou desvios de comportamento. Ao identificar os primeiros sinais de um possível ataque, o IDS reconhece o problema e notifica o responsável.

Segundo Proctor (2001), Um IDS não pode ser usado com a única fonte de segurança de uma rede, nem em substituição a um *firewall,* mas sim em conjunto com outros métodos para aumentar a segurança da rede. Um IDS é composto basicamente por dois dispositivos principais, o Console de Comando e o Sensor. O console de comando, ou simplesmente console, tem como função permitir o controle do IDS, monitorar o estado do sensor e processar os alertas enviados pelo sensor.

Segundo Crothers (2003), “O sensor é o dispositivo responsável pela coleta de informação para análise de descoberta de uma invasão”.

3.1. TIPOS DE SISTEMAS DE DETECÇÃO DE INTRUSÃO

Segundo Chiavaro (2003), de acordo com os esquemas de classificação de IDS, as técnicas utilizadas na detecção de intrusão são separadas em dois modelos diferentes: modelos de detecção de mau uso e modelos de detecção baseados em anomalia, logo segue a descrição de cada modelo:

- Detecção de mau uso;

Também conhecida como detecção baseada em assinaturas, consiste em identificar e utilizar padrões de ataques conhecidos para descobrir possíveis tentativas de intrusões.

- Detecção baseados em anomalia;

O objetivo principal em estudar os processos de usuários e o tráfego de rede, para que, posteriormente, possam estabelecer padrões e encontrar a suas variações quando necessário.

3.1.1. Detecção de intrusão híbrido

Segundo Chiavaro (2003), além dos modelos de IDS baseados em rede e aqueles baseados em *host*, existem os sistemas de detecção de intrusão híbridos. Eles reúnem as características de NIDSs (Network Intrusion Detection Systems), e HIDSs (Host Intrusion Detection Systems), correlacionando arquivos de registro de eventos e informações de sistema com tráfego de rede. O IDS híbrido consiste em combinar os aspectos positivos do HIDS e do NIDS, para que a detecção de intrusão se torne mais eficaz.

Esses sistemas operam como se fossem NIDS, capturando e processando pacotes do tráfego da rede e detectando e reagindo a ataques. Porém, efetuam esse processo como HIDS, ou seja, processando os pacotes endereçados ao próprio sistema. Dessa maneira, é possível resolver o problema de desempenho dos IDSs baseados em rede. Entretanto, o problema da escalabilidade em sistemas baseados em *host* continua, sendo que um IDS híbrido deve ser instalado em cada equipamento monitorado.

Para a proteção dos recursos de uma organização, acredita-se que a melhor estratégia ao se tratar de sistemas de detecção de intrusão, é usar os dois tipos de modelos de IDS. No cenário onde uma organização possui servidores de Internet

importantes, podem acontecer diversos ataques, e o NIDS poderá detectar alguns e o HIDS outros.

3.1.2. Detecção de intrusão baseado em host

Monitora o tráfego de máquinas individuais, permitindo uma melhor precisão na análise e gerando menos falso positivo.

Detecção de intrusão baseado em host pode - se trabalhar de três ou mais formas (NORTHCUTT, 2002):

- Verificando a integridade do sistema de arquivos: procuram por mudanças não autorizadas no sistema de arquivo, a partir de uma base criada do sistema quando considerado confiável. É configurável, sendo possível indicar quais arquivos ou diretórios podem sofrer alterações, diminuindo assim os alertas;
- Verificando a conexão da rede: verifica as conexões do host a procura de ataques ou atividades maliciosas. Tem menos problemas com a sobrecarga de tráfego, pois monitora somente o tráfego destinado a um determinado host;
- Verificando os arquivos de log: observam o conteúdo dos logs e avisam quando algo suspeito é detectado. Possui uma vantagem, se vários hosts salvarem seus logs em um único ponto este sistema pode monitorar mais que um host;

Como vantagens encontram-se (BACE, 2002):

- O IDS baseado em host consegue monitorar eventos locais: pode verificar alterações em arquivos do sistema, por exemplo, enquanto que o IDS baseado em rede não consegue;
- Pode trabalhar em redes com criptografia: como analisa o host, verifica os dados antes de serem criptografados ou depois de serem descriptografados;
- Não tem problemas em redes com switches: como o IDS baseado em host analisa o conteúdo que entra ou sai do host onde está instalado, ele não é afetado pelo modo que o switch trabalha, ou seja, não importa se os pacotes são

enviados para toda a rede ou só para os dois hosts que estabeleceram uma conexão;

- Detecta cavalos de tróia e outros ataques que envolvem brechas na integridade dos softwares.

Como desvantagens (BACE, 2002):

- São mais difíceis de gerenciar;
- Pode ser atacado e desabilitado: o *host* pode sofrer um ataque e o IDS não detectar e ser comprometido ou desabilitado;
- O *host* pode sofrer ataques DoS que podem parar o IDS;
- Não pode detectar *scan* de portas ou outra ferramenta de varredura que tenha como alvo toda a rede, porque só analisa os pacotes direcionados ao *host* em que está instalado;
- Se a quantidade de informação for muita, pode ser necessário adicionar mais área para o armazenamento dos *logs*;;
- O IDS baseado em *host* influencia no desempenho do *host* que está instalado porque consome recursos para o processamento das informações.

3.1.1. Detecção de intrusão baseados em rede

Segundo Chiavaro (2003), os NIDS são considerados *sniffers* de alto nível, capturando e analisando os pacotes que passam pela rede de forma passiva, sem que os outros sistemas percebam isso. Cada pacote capturado é comparado com um conjunto de padrões de assinaturas conhecidas. São muito eficientes contra ataques de varredura de portas (*Nmap*), falsificação de IP ou *SYN flood*, prevendo ataques a um servidor de Internet.

Embora os IDSs baseados em rede apresentem boa eficiência em relação a detecção de ataques, eles trazem algumas questões que devem ser consideradas.

Segundo Nakamura e Geus (2002), os NIDSs têm como pontos positivos:

- um único IDS pode fornecer monitoramento para múltiplas plataformas;

- analisam pacotes;
- monitoram atividades suspeitas em portas conhecidas, como a porta TCP 80, que é utilizada pelo HTTP;
- os ataques podem ser detectados em tempo real e o administrador pode determinar rapidamente o tipo de resposta apropriada;
- possuem capacidade de detectar não só ataques, mas também, tentativas de ataque que não tiveram sucesso;
- apresentam cuidados para que um *hacker* não possa apagar seus rastros, caso consiga invadir um equipamento;
- um *hacker* terá dificuldades em saber que existe um NIDS monitorando suas atividades;
- não causam impacto no desempenho da rede.

Os pontos negativos que podem ser encontrados em NIDS são:

- incapacidade de monitorar grandes redes com alto tráfego;
- dificuldade de compreensão de protocolos de aplicação específicos;
- não são capazes de monitorar tráfego cifrado;

3.2. COMO UMA FERRAMENTA IDS PODE ATUAR

Em Tim Crothers (CROTHERS, 2003) encontram-se quatro finalidades primárias que podem ser alcançadas com um IDS e a empresa deveria priorizá-las na escolha do IDS:

Oferecer recursos de contabilização (*Providing accountability*): é uma capacidade que o IDS possui e pode ser usado quando a empresa procura uma forma de monitorar as atividades realizadas pelos funcionários. Muitas empresas acham que o simples fato de monitorar as atividades da rede aumenta o uso responsável da *internet*. O IDS baseado em *host* efetua melhor esta função, pois permite obter

dados mais detalhados. Na maioria dos casos, é melhor utilizar ferramentas próprias para essa tarefa, pois são mais baratas e fáceis de usar, apesar de alguns IDSs também poderem realizar esta tarefa;

Sinalizar recursos que merecem atenção (*Focusing resources*): a maioria das empresas já possui outros recursos que auxiliam na proteção da rede e dos sistemas, o IDS pode ajudar a focar o uso destas ferramentas. O IDS pode identificar quais são os pontos mais atacados e explorados, ficando assim, mais fácil identificar quais desses pontos devem obter mais atenção da equipe de segurança, quais deles devem possuir uma melhor proteção, terem suas atualizações aplicadas com mais freqüência e até terem seu acesso restringido;

Impedir danos (*Preventing damage*): embora seja possível realizá-la com a tecnologia atual, até que ponto o IDS pode realmente impedir danos é algo discutível. Falsos alertas podem gerar bloqueios ou outras ações na rede que podem ter os mesmo resultados que uma atividade maliciosa real;

Minimizar danos (*Mitigating damage*): no momento de uma intrusão, o IDS pode bloquear um ataque e auxiliar na recuperação do sistema após a tentativa. O IDS pode ajudar a minimizar os danos de três maneiras:

- Antecipar a detecção da intrusão: o ataque é descoberto mais rápido com a ajuda de um IDS. Quanto mais cedo o ataque for descoberto, menor será a chance de o hacker ter sucesso;
- Oferecer evidências do ataque: permite ter um registro detalhado do que aconteceu no sistema durante o ataque. Quanto mais detalhado for esse registro, mais rápido e fácil de reconstruir o ataque para poder identificar o *hacker* e processá-lo, como também fechar a falha de segurança utilizada pelo *hacker* para atacar o sistema;
- Permitir restauração do sistema: informações detalhadas permitem uma restauração mais fácil do sistema. Sabendo-se quais foram os arquivos que foram comprometidos, pode-se simplesmente recuperá-los de um *backup*.

3.2.1. Alguns aplicativos IDS

Existem diversos aplicativos IDS no mercado, alguns com *open source* e outros comerciais, abaixo segue alguns exemplos:

RealSecure:

Desenvolvedor: *Internet Security Systems*. www.iss.net;

Um dos primeiros aplicativos IDS comerciais baseados em rede do mercado;

Permite ao administrador criar suas próprias regras de assinaturas e alertas;
Possui atualizações automáticas para as assinaturas e atualizações do produto;

Assistência *on-line* para resposta de incidentes;

eTrust:

Desenvolvedor: *Computer Associates.* www.ca.com;

Fácil integração com outros produtos da *Computer Associates*;
Permite reconfigurar o *firewall* ;
Permite criar regras específicas a partir de endereços IP, usuários, mas contidos em um domínio NT;

Permite bloquear acessos a páginas de Internet;

Snort:

Desenvolvedor: www.snort.org;

Roda em diversos sistemas operacionais;

Estrutura de *plugins*;
Faz análise de protocolo;
Várias formas de registro: *syslog, SQL*;
Detecta *portscan*, ataque *UNICODE*, *Buffer overflows*, entre outros;
Remonta fragmentos IP e TCP;

Normaliza requisições HTTP, RPC;

Permite ao administrador criar suas próprias regras de assinaturas;

PortSentry:

Desenvolvedor: www.psionic.com/download;

Baseado em *host;*
Escuta os arquivos de registro e detecta análise de portas;
Fácil configuração;
Quando detecta um *scan*, executa uma função que esconde o sistema do ataque;

Reporta todas as violações ao *syslog*;

NFR Network Intrusion Detection:

Desenvolvedor: www.isp-planet.com;

Permite configurar o *firewall,* encerrar a conexão TCP;
Interface configurável;
Permite gerenciamento centralizado;
Atualização automática das assinaturas;

Suporte 24x7 do suporte;

***Prelude*:**

Desenvolvedor: www.prelude-ids.org;

IDS híbrido;
Possui *interface* gráfica;
Permite gerenciamento centralizado;
Permite usar as regras do SNORT;
Baseado em módulos;
Armazena os alertas em modo texto ou em banco de dados *My*SQL ou

*Postgre*SQL;

A figura 02 mostra um exemplo de um Sistema de Detecção de Intrusão.

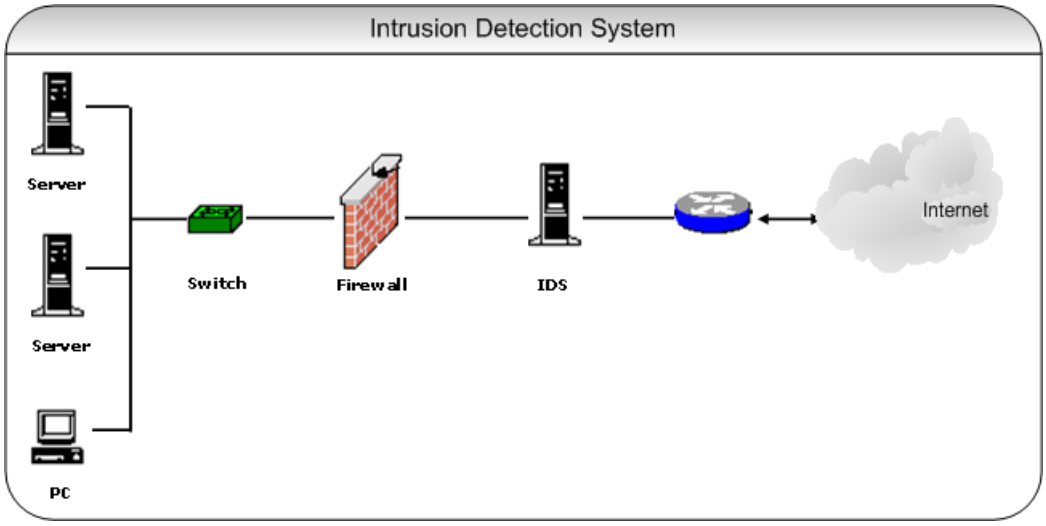

Figura 2. Exemplo de um sistema IDS

4. OUTROS APLICATIVOS DE SEGURANÇA

Quando se comenta sobre segurança computacional, hackers, invasões logo se lembra sobre os agentes combatentes destes perigos citados acima, que se dá ao nome de Antivírus e Firewalls, pois normalmente todo computador que se preze por segurança, proteção, tem em suas máquinas como proteção um Antivírus ou um Firewall ou se não os dois. Outro aplicativo que trabalha com segurança.

4.1. CONCEITOS

Firewall

É um dispositivo que atua em redes de computadores onde suas funções é regular o tráfego de rede entre redes distintas e impedir a transmissão e/ou receptação de dados nocivos ou não autorizados de uma rede a outra. Neste conceito pode-se incluir geralmente, os filtros de pacotes e os proxy de protocolos;

Sua utilização é para evitar que o tráfego não autorizado possa fluir de um domínio de rede para o outro;

O nome FIREWALL se refere ao um termo inglês corta-fogo, pois a função de um Firewall é desempenhada para evitar o crescimento de dados nocivos dentro de uma rede de computadores;

Ele existe em duas formas, tanto na forma de software e hardware;

Antivírus

Desenvolvido especialmente para detectar e eliminar vírus do computador, conforme o seu nome já diz;

Hoje no mercado existe várias opções de Antivírus tanto open source quanto comercial, e também variam de funcionalidades, ou seja, o que fazem;

A primeira contaminação por um vírus de computador ocorreu em 1988, utilizando uma BBS (*Bulletin Board Service*, primeiros serviços online, bem antes da Internet) como meio. Sendo assim, John McAfee, programador da Lockheed Air Corporation, empresa de aviação americana, desenvolveu o VirusScan, primeira vacina conhecida;

Um detalhe importante sobre os Antivírus é mante-los atualizados, alguns já se atualizam automaticamente, basta estar conectado á internet;

Os vírus informáticos apareceram e propagaram-se em larga escala devido à má gestão e programação de certos produtos que foram lançados para o mercado antes de serem devidamente testados.

Antispyware

Um anti-spyware é um software de segurança que tem o objetivo de detectar e remover adwares e spywares.
A principal diferença de um anti-spyware de um antivírus é a classe de programas que eles removem. Adwares e spywares são consideradas áreas “cinza”: nem sempre é fácil determinar o que é um adware e um spyware. Adwares são desenvolvidos por empresas de publicidade que geram milhões de lucro e que já processaram empresas que fabricam anti-spyware por removerem seus softwares das máquinas dos usuários.

5. SNORT

Segundo CASWELL (2003), o Snort é um sistema de detecção de invasão baseado em rede, de código fonte aberto. É um IDS baseado em assinaturas que usa regras para verificar a existência de pacotes com informações que podem indicar a ocorrência do ataque. Regras é um conjunto de requisitos que gerariam um alerta. O *Snort* possui muitos recursos entre os quais pode - se citar um farejador de pacotes para a captura dos dados, um mecanismo de registro de pacotes e de detecção de invasão. Ele também pode ser configurado para enviar alertas em tempo real evitando assim a necessidade de monitorar o sistema continuamente. O *Snort* é considerado um IDS leve, por possuir uma estrutura pequena e ser um software multiplataforma disponível para sistema Solaris, Linux, sistemas BSD, HP-UX, IRIX e Windows.

Segundo Snort (2002) o SNORT é um sistema de detecção de intrusão baseado em rede amplamente utilizado. Foi desenvolvido por Marty Roesch em 1998. Possui versões para vários sistemas operacionais, entre os quais se pode citar *Linux, OpenBSD, FreeBSD, NetBSD, Solaris SunOS* 4.1.x, *Windows*, entre outros.

O sistema operacional utilizado neste trabalho será o LINUX SLACKWARE, pois o motivo para esta escolha se baseia em um sistema operacional totalmente open source, mais leve e ele não tem versão comercial.

Segundo Campello (2002) o SNORT possui uma arquitetura simples baseada em *plug-ins*, executando basicamente as funções de captura de pacotes na rede, análise dos pacotes e geração de alertas. É um sistema leve, capaz de trabalhar em grandes redes e detectar uma grande variedade de ataques em tempo real, sendo o seu sistema de detecção baseado em assinaturas.

Segundo Nss Group (2002) o SNORT pode ser configurado para trabalhar de três modos:

Sniffer é simplesmente lê os pacotes da rede e mostra o resultado na console do programa gerenciador;

Gerador de log. de pacotes trabalha de maneira semelhante ao modo *sniffer*, porém armazena todos os pacotes em arquivo para uma análise futura;

Detector de intrusão é o método mais flexível e completo para analisar o tráfego da rede. Podem-se definir novas regras de detecção além das já disponíveis. Neste modo, somente são gerados alertas ou armazenados no *log* os pacotes definidos nas regras;

O modo de configuração a ser desenvolvido neste trabalho é o modo por Detector de intrusão, pois sua funcionabilidade trabalha com definições de regras definidas pelo administrador, e seu modo para análise de tráfego é mais completo;

As ferramentas a serem instaladas para o desenvolvimento desta IDS será:

Mysql como banco de dados;

Guardian como bloqueador;

ACID gerenciador de alertas;

SNORT versão 2.8.1 – Ferramenta IDS;

PHP para visualizar logs on-line;

Os motivos para esta escolha foi o uso da base Mysql principalmente, para poder usar o ACID, que é uma ferramenta que usa qualquer navegador disponível no mercado, e assim, torna a leitura dos logs do ACID, muito mais interessante, ou seja, elimina a leitura dos logs em um sistema e que normalmente, acaba deixando com que nós deixemos alguma coisa passar;

5.1. CARACTERÍSTICAS GERAIS DO SNORT

Segundo Hasenak (2001) segue abaixo algumas características do SNORT:

- Baseado em assinatura;
- Roda em diversos sistemas operacionais;
- Estrutura de *plug-ins;*
- Faz análise de protocolo;
- Várias formas de registro: *syslog, SQL;*
- Detecta *portscan*, ataque *UNICODE*, *Buffer overflows*;

Segundo Gomes (2001):

- Remonta fragmentos IP e TCP;
- Normaliza requisições HTTP, RPC;
- Ativa regras dinamicamente (regras podem ser ativadas por outras regras);

5.2. ARQUITETURA DO SNORT

Segundo Nss Group (2002) a arquitetura do SNORT se preocupa com o desempenho, simplicidade e flexibilidade. Utiliza a biblioteca *libpcap* para a captura dos pacotes. É formado basicamente pelos:

Packet decoder é responsável basicamente pela organização dos pacotes para o

detection engine;

Detection engine é responsável por comparar o pacote com a regra. O SNORT mantém as regras de detecção em duas listas chamadas *Chain Headers*, que contém os atributos comuns (endereço IP, portas) e *Chain Options* que contém as opções (*flags* do TCP, códigos ICMP)

Logging and alerting subsystem é responsável por armazenar os pacotes no arquivo de *log* ou gera o alerta. É acionado pelo *packet decoder* ou *detection engine*, depende da configuração das regras.

5.2.1. Regras SNORT

Segundo Ferreira (2004), Uma regra do Snort é composta geralmente por uma simples linha em um arquivo. Por questões de organização as regras enviadas pela comunidade Snort são gravadas em arquivo com regras em comum.

Segundo BORGES (2007) O Snort usa uma simples e clara linguagem de escrita de regras, oferecendo poderosas opções para a escrita de avançados recursos de detecção de pacotes suspeitos, além de permitir respostas no caso de alertas de alta gravidade.

Segundo Nss Group (2002) uma regra é dividida logicamente um duas partes: o cabeçalho e as opções. O cabeçalho de uma regra determina o protocolo, a direção

do tráfego, o endereço IP de origem e de destino e as portas. As ações tomadas quando uma regra coincidir com o pacote podem ser:

- *Log*: armazena o pacote em arquivo. Estes arquivos podem ser base de dados SQL, binário, arquivos XML, entre outros;
- *Alert*: gera um alerta e também armazena em *log*;
- *Pass*: ignora o pacote, usado para que o SNORT não verifique determinado tipo de tráfego;
- *Activate/Dynamic*: funciona como um gatilho e permite que uma regra dispare outra regra.

Segundo Roesch (2002) um exemplo de uma regra seria:

Alert TCP !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:``|00 01 86 a5|``;msg:``mouted access``;)

Segundo Roesch (2002) o exemplo acima a regra analisa qualquer pacote TCP com o endereço IP de origem diferente que o da rede interna e tendo como endereço de destino a rede interna na porta 111. A mensagem de alerta é gerada quando o pacote contiver a *string* 00 01 86 a5.

6. MODELO PARA DESENVOLVIMENTO

Esta seção aborda os procedimentos de instalação e configuração do aplicativo IDS – Snort.

6.1. COMPILAÇÃO DO MYSQL

Uma ferramenta IDS por sua vez deve possuir algumas características, como um baixo nível e consumo de processamento, exige também uma capacidade muito enorme de manipulação de logs. Com isso a instalação é uma implantação baseada em logs armazenados em um banco de dados que será o MySql.

Em princípio necessita-se do banco de dados MySql instalado e rodando, assim como as suas bibliotecas, para isso segue um exemplo abaixo:

```
# cd /usr/src/
# tar -xvzf mysql-x-x-x.tar.gz
# cd mysql-x-x-x
# addgroup mysql
# adduser mysql -g mysql -s /dev/nologin
# ./configure --prefix=/usr/local/mysql && make && make install
# cd /usr/local/mysql
# chown -R mysql.mysql /usr/local/mysql/var
# bin/mysqld_safe &
# cd mysql-test
# ./install-test-db
```

Figura 3. Instalação do MySql.

Precisa - se criar um login chamado snort_ids e um banco de dados chamado snort_ids, a configuração das permissões será somente para que o usuário criado tenha acesso as tabelas.

```
# mysql -u root -p mysql
  mysql> INSERT INTO user VALUES
  ('localhost','snort_user',PASSWORD('senha'),'Y')
  mysql> FLUSH PRIVILEGES;
  mysql> create database snort_ids;
  mysql> use snort_ids
  mysql> GRANT ALL PRIVILEGES ON
  *.* TO snort_ids@localhost IDENTI
  FIED BY 'senha' WITH GRANT OPTION;
  mysql> FLUSH PRIVILEGES;
```

Figura 4. Criando login e senha no MySql.

Após a instalação do MySql deverá ser digitado alguns comandos para garantir que o MySql funcionará toda vez que o Linux for reiniciado, abra um editor e digite os seguintes comandos no seu arquivo (/etc/rc.d/rc.local):

if [-x /usr/local/mysql/bin/mysqld_safe];then

echo \"Iniciando o Mysql \" /usr/local/mysql/bin/mysqld_safe &

fi

Depois de seguir as instruções acima, pode-se passar para a preparação do MySql para trabalhar junto ao Snort.

```
# /usr/local/mysql/bin/mysql -p

        Já no shell do mysql digite

> create database snort;

> grant insert, select on snort.* to snort@localhost identified by \'senha_do_snort\';

> grant insert, select, delete, update, create on snort.* to acid@localhost
identified by \'senha_do_acid\';

> quit
```

Figura 5. Configuração do MySql junto ao Snort.

6.2. CRIAÇÃO DA BASE DE DADOS DO SNORT COM O MYSQL

Agora, deve-se criar o a base de dados do Snort dentro do MySql, como ilustra a figura 06.

```
# cd /usr/src

# tar -xvzf snort-x-x-x.tar.gz

# cd snort-x-x-x/contrib

# mysql -p snort < create_mysql

> quit
```

Figura 6. Criando a base de dados do Snort no MySql.

Realizado os processos citados anteriormente, terá de ser realizada agora a compilação do Snort. Primeiramente foi compilado o MySql pois o Snort vai precisar de alguns cabeçalhos do MySql que estarão presentes no sistema após o mesmo ser instalado.

O próximo passo a ser realizado antes da compilação do Snort é a instalação do Libcap que funciona como um captor de dados que chegam à camada de enlace dos dados. Antes se deve realizar o download do mesmo (http://www.tcpdump.org).

```
# cp libcap-x-x-x.tar.gz /usr/src

# tar -xvzf libcap-x-x-x.tar.gz

# cd libcap-x-x-x

# ./configure && make && make install

# ldconfig
```

Figura 7. Instalação do Libcap.

6.3. COMPILAÇÃO DO SNORT

Depois Da instalação do Libcap, será realizada a compilação do Snort.

```
# cd /usr/src/snort-x-x-x

# ./configure --with-mysql=/usr/local/mysql

# make && make install

# mkdir /etc/snort

# mkdir /var/log/snort

# cd /usr/src

# tar -xvzf snortrules-current.tar.gz

# cd rules

# cp * /etc/snort

# cd /etc/snort

# wget http://cerebro.freeshell.org/sections/aplicationpatches/vision18.conf.gz

# gzip -d vision18.conf.gz
```

Figura 8. Compilação do Snort.

6.4. CONFIGURAÇÃO DO SNORT

Finalizado o processo acima o Snort já esta instalado no sistema operacional, a partir de agora será realizado a configuração do Snort.

Primeiramente terá de editar no arquivo de configuração as seguintes linhas no seu snort.conf:

var HOME_NET any

Esta linha acima deverá ficar ser modificada substituindo o *any* para o Ip da placa de rede do computador, caso tenha mais placas de redes configura-se da seguinte forma:

HOME_NET [10.1.1.0/24,192.168.1.0/24]

Como o diretório de regras está em /etc/snort, deverá também modificar o caminho das regras para *var RULE_PATH/etc.../snort;*

include $RULE_PATH/bad-traffic.rules é a parte final do arquivo de configuração do Snort, estás linhas são os arquivos de regras do Snort, que serão usadas para gerar os logs, pode-se optar por descomentar todas ou deixar apenas as que forem preferíveis.

Agora terá de adicionar as regras vision18.conf, e também preparar o arquivo de configuração para trabalhar com o MySql (banco de dados).

Para isso deve-se procurar a seguinte linha:

output database: log, mysql, user=snort password=suasenha dbname=snort host=localhost

Agora terá de mudar esta linha para os dados definidos no início da instalação, depois deverá ir até ao final do arquivo e adicionar a seguinte linha:

include $RULE_PATH/vision18.conf

O Próximo passo agora é realizar o funcionamento do Snort com o seguinte comando:

 # snort -D -c /etc/snort/snort.conf -l /var/log/snort/

Para conferir se o Snort está sendo executado deve-se digitar o seguinte commando:

tail -f /var/log/messages

Caso aparecer uma linha com a seguinte mensagem Snort initialization completed successfully, Snort running, o Snort está sendo executado sem nenhum problema.

6.5. INSTALAÇÃO DO GUARDIAN

Como o Snort não faz todo o trabalho sozinho, como isso ela trabalha com outra ferramenta que irá aproveitar as suas regras, para fazer a leitura das regras em tempo real agindo contra um possível invasor no momento da tentativa.

Deve - se instalar o Guardian terá de efetuar o download do mesmo no site do Snort (WWW.snort.org.br) ele se encontrará na parte de contrib, após a efetuação do download será realizado o processo de configuração e preparo do Guardian para trabalhar paralelo com o Snort.

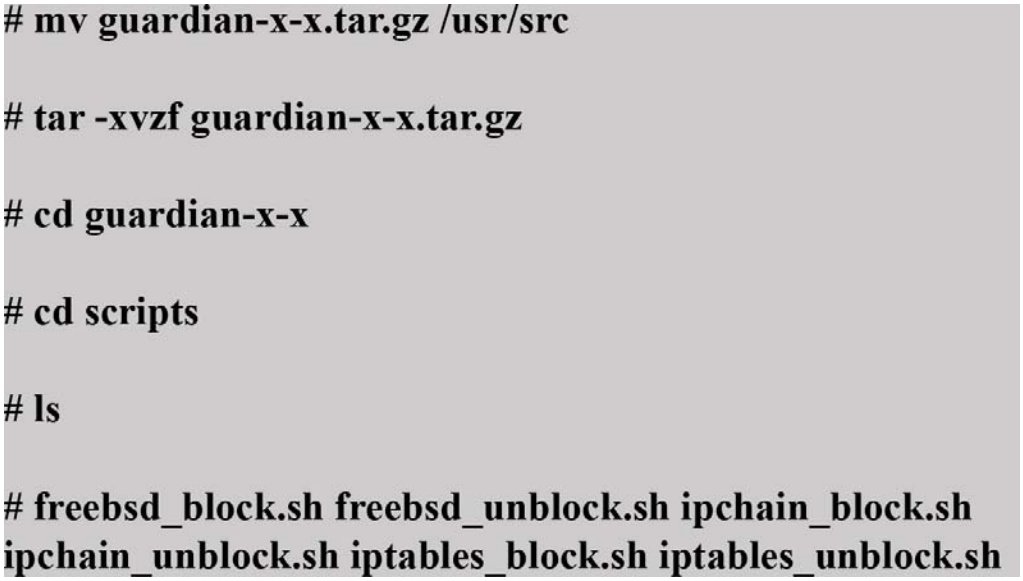

Figura 9. Configuração do Guardian.

Como pode ser notado, há diversos scripts neste diretório o Guardian, trabalha com os seguintes scripts, guardian_block.sh e guardian_unblock.sh, precisa-se escolher

oi filtro de pacotes e instalar os scripts necessários. Neste trabalho foram escolhidos os scripts referentes ao iptables.

```
# cp iptables_block.sh /usr/bin/guardian_block.sh

# cp iptables_unblock.sh /usr/bin/guardian_unblock.sh

# chmod 755 /usr/bin/guardian_block.sh /usr/bin/guardian_unblock.sh
# cd ..

# cp guardian.pl /usr/bin

# chmod 755 /usr/bin/guardian.pl

# cp guardian.conf /etc/
```

Figura 10. Instalação dos Scripts.

Deve - se mudar os valores para os valores referentes à estrutura de rede usada no computador a ser instalado.

Interface eth0 é a que vai ter os hosts hostis barrados;

AlertFile /var/adm/secure será alterado para AlertFile /var/log/snort/alert;

TimeLimit 86400 pode ser mudado para o tempo em segundos que o host fique barrado pelo firewall, 99999999 desabilita esta opção.

Agora se pode criar o arquivo de log do Guardian como segue abaixo:

touch /var/log/guardian.log

Cria-se agora o arquivo guardian.ignore com os IP’s que ele vai ignorar, como mostra o exemplo abaixo:

cat /etc/guardian.ignore

192.168.1.47

Este comando acima ignora o IP 192.168.1.47, após este comando pode-se iniciar o Guardian, para iniciá-lo é preciso digitar o seguinte comando:

guardian.pl -c /etc/guardian.conf

A partir deste comando aparecerão as seguintes mensagens:

OS shows Linux

Warning! HostIpAddr is undefined! Attempting to guess..

Got it.. your HostIpAddr is 192.168.1.1

My ip address and interface are: 192.168.1.1 eth0

Loaded 3 addresses from /etc/guardian.ignore

Becoming a daemon..

Isto significa que o Guardian foi iniciado.

6.6. INSTALAÇÃO DO APACHE E PHP

Deve - se ser preparado o sistema para possuir o Apache, PHP, MySql, Acid, todos rodando para que possa ser lido os logs do Snort on line, sem que tenha que acessar arquivos de textos enormes dentro do sistema operacional.

Para a instalação destes parâmetros citados acima, precisa-se de algumas bibliotecas como:

ADODB - http://php.weblogs.com/adodb

PHPLOT - http://www.phplot.com

GD - http://www.boutell.com/gd

Primeiramente será compiladado o PHP para ter suporte junto ao MySql e ao Apache, como ilustra a figura 11.

```
# cd /usr/src

# tar -xvzf apache-x-x-x.tar.gz

# tar -xvzf php-x-x-x.tar.gz

# cd apache-x-x-x

# ./configure

# cd ..

# cd php-x-x-x

# ./configure --with-apache=../apache-x-x-x --with-mysql=/usr/local
/mysql -with-gd --prefix=/usr/local/apache --enable-track-vars

# make && make install

# cd .. # cd apache-x-x-x # ./configure -activate-module=src
/modules/php4/libphp4.a

# make && make install
```

Figura 11. Compilação do PHP.

Depois da compilação do PHP, deve-se descompactar cada uma das bibliotecas no diretório onde se encontra os documentos HTML em que o Apache estiver instalado como ilustra a figura 12.

```
# tar -xvzf adodb.tgz

# mv adodb-x-x /usr/local/apache/htdocs

# tar -xvzf phplot-x-x-x.tar.gz

# mv phplot-x-x /usr/local/apache/htdocs
```

Figura 12. Descompactação das bibliotecas.

Pode - se preparar o Apache para executar o PHP, para isso deverá ser adicionado no arquivo httpd.conf que se encontra no diretório (/usr/local/apache/conf/httpd.conf) as seguintes linhas:

<IfModule mod_dir.c>

DirectoryIndex index.html index.php3 index.php index.phps default.htm

</IfModule>

Depois adicione também no arquivo de configuração as seguintes linhas:

AddType application/x-httpd-php .php .php3 .phtml

AddType application/x-httpd-php-source .phps

Agora o Apache já esta pronto para funcionar, como o sistema vai ficar on line em um servidor http, isto é muito perigoso pois pode ser acessado por qualquer usuário, por isso precisará de protege-lo como também o diretório do Acid precisa-se ser protegido, por isso deve-se digitar o seguinte comando:

/usr/local/apache/bin/htpasswd -c /usr/local/etc/passwd usuário

Após este procedimento também precisará adicionar as seguintes linhas no arquivo httpd.conf:

```
<Directory /user/etc/apache/htdocs/acid>
    AuthType Basic
    AuthName “Acid for Snort”
    AuthUserFile /usr/etc/apache/passwd
    Require user hugo
    Order allow,deny
    Satisfy any
</Directory>
```

Figura 13. Proteção para o Apache e o Acid.

6.7. INSTALAÇÃO E CONFIGURAÇÃO DO ACID

A partir de agora será instalado o Acid, para que gerencie os logs.

```
# tar -xvzf acid-x-x-x.tar.gz

# mv acid /usr/local/apache/htdocs/acid

# cd /usr/local/apache/htdocs/acid
```

Figura 14. Instalação do Acid.

Para editar o arquivo de configuração do PHP deve-se digitar:

vim acid_conf.php

Agora a figura 15 ilustra a configuração do Acid

```
/* Path to the DB abstraction libary
 * Note : DO NOT include a trailing backslash after the directory
 * e.q . $foo = "/tmp/" [OK]
 * e.q . $foo = "c:\tmp" [OK]
 * e.q . $foo = "c:\tmp" [WRONG]
*/

$DBlib_path = "../adodb";
/* The type of underlying alert database
 *
 * Mysql : "mysql"
 * Portgressql = "postgres"
 * MS SQL SERVER : "mysql"
 */
 $DBtype = "mysql";
 $alert_dbname = "snort";
 $alert_host = "localhost";
 $alert_port = " ";
 $alert_user = "acid";
 $alert_password = "senhadoacid";
 /* Archive DB connection parameters */
 $archive_dbname = "snort";
 $archive_host = "localhost";
 $archive_port = " ";
 $archive_user = "snort";
 $archive_password = "senhadosnort";

 * Path to the graphing library
  * Note : DO NOT include a trainling after the directory
  */
 $ChartLib_path = "../phplot";
 /* File format of charts ( 'png' , 'jpeg' , 'gif' ) */

 $Chart_file_format = "png";
```

Figura 15. Configuração do Acid.

Para acessar o Acid digitando http://seuhost/acid/ e para finalizar deve-se adicionar no */etc/rc.d/rc.local* os seguintes comandos:

```
# echo \"/usr/local/apache/bin/apachectl start\" >> /etc/rc.d/rc.local

# echo \"snort -D -c /etc/snort/snort.conf -l /var/log/snort/\" >> /etc/rc.d/rc.local

# echo \"guardian.pl -c /etc/guardian.conf\" >> /etc/rc.d/rc.local
```

Figura 16. Adicionando algumas variáveis

6.8. TESTES REALIZADOS

Para realização dos testes com a ferramenta Snort, foi realizado um "Ping" (comando que varre as portas abertas no computador) na máquina onde se encontrava o Snort de outra máquina com o sistema operacional Linux também, para que o mesmo pudesse gerar os logs de detecção, mas para realizar esta detecção precisa - se que a regra ICMP responsável pela detecção de "Ping" a imagem abaixo mostra um exemplo das regras escritas no arquivo snort.conf, pois este arquivo é responsável pela leitura de todas as regras do Snort, como ilustra a figura 17.

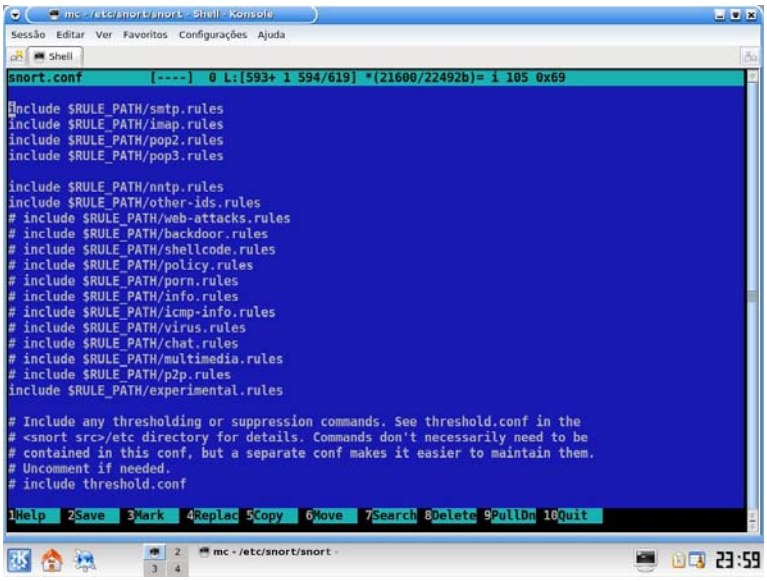

Figura 17. Arquivo Snort.conf

A linha ***#include $RULE_PATH/icmp-info.rules*** é a regra responsável pela detecção do teste realizado.

A figura 18 ilustra o comando digitado para realização do "Ping" para que o Snort pudesse detectar o mesmo.

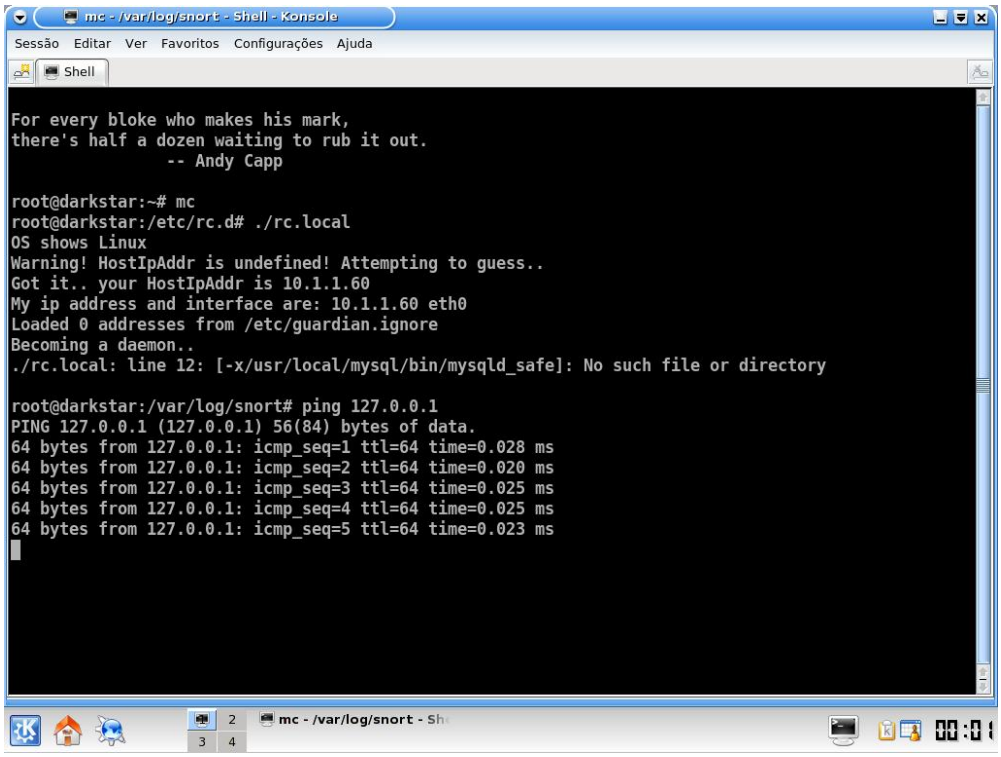

Figura 18. Comando Ping

Depois de realizado este processo o Snort automaticamente gera os Logs de detecção em um arquivo de texto, mas como este arquivo é de difícil interpretação o Acid junto ao PHP e o Apache gera um arquivo em HTML para que visualize com mais facilidade e entendimento como ilustra a figura 19.

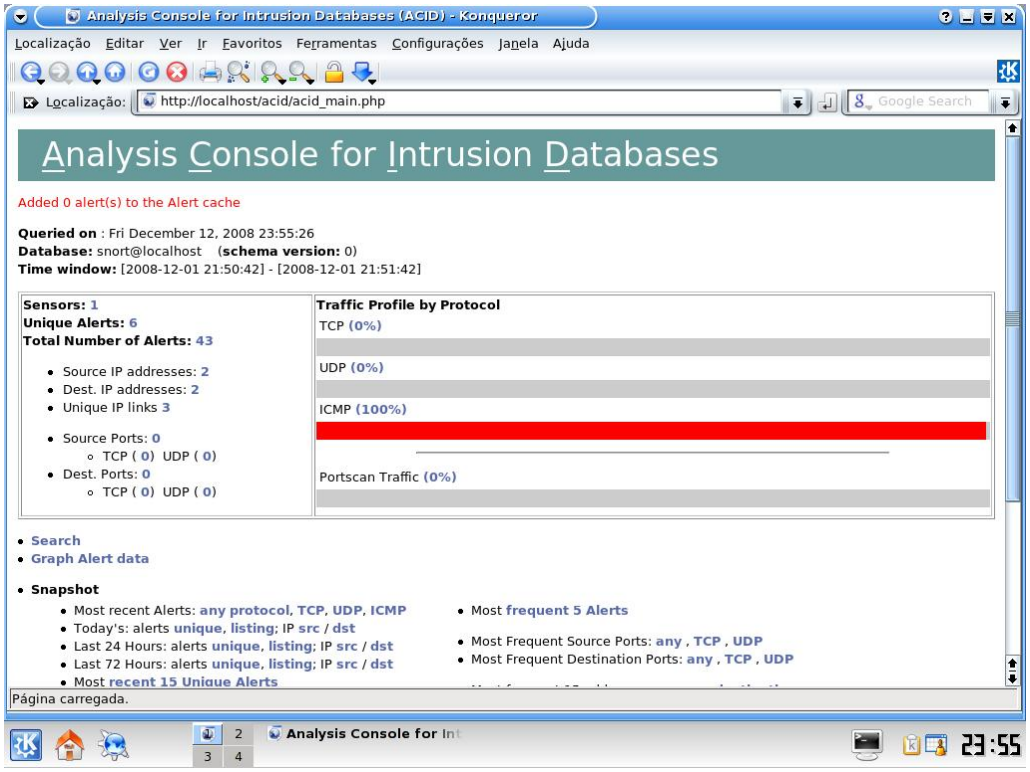

Figura 19. Página em HTML com os Logs

Esta página em HTML mostra também o IP (Protocolo de Internet) da máquina que realizou o Ping na máquina que se encontrava o Snort.

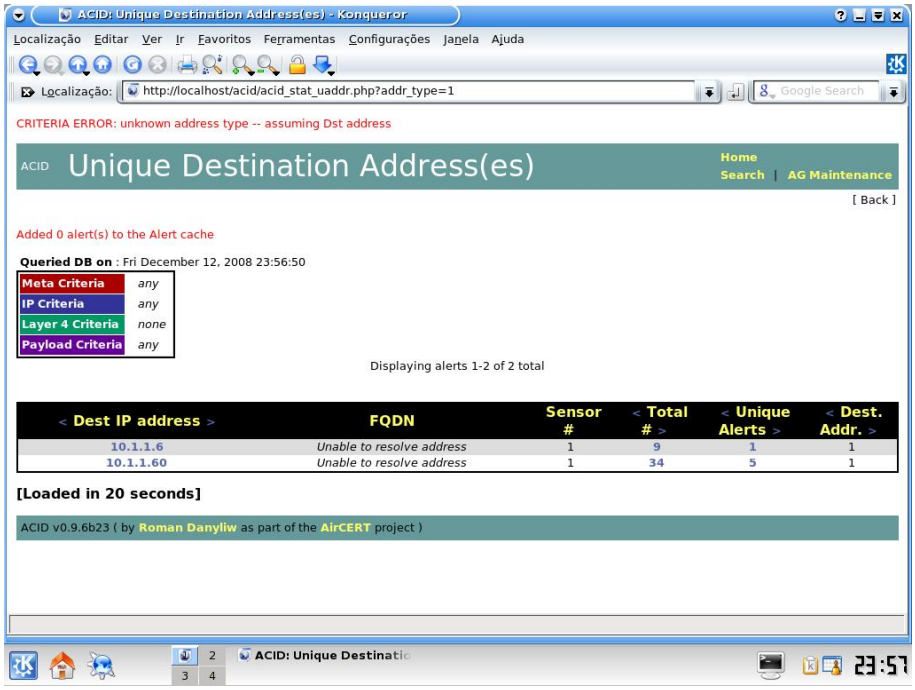

Figura 20. Página em HTML mostrando o IP detectado

Como o teste apenas testou o comando Ping, que apenas é uma varredura na máquina das portas abertas no computador o Guardian não agiu pois o mesmo só agirá quando o computador estiver recebendo ou realizando um download de arquivos maliciosos, o Guardian atuará deletando - os ou barrando - os para a segurança do computador.

Todos os arquivos HTML gerados com os logs de detecção são gravados no MySQL para armazenamento, pois a varredura de logs do Snort é constante, com isso gera - se milhares de arquivos HTML.

7. CONCLUSÃO

Este trabalho apresentou como funciona a ferramenta Snort que pode ser empregada por administradores de redes na detecção de intrusos.

A ferramenta Snort é poderosa neste sentido, pois detecta efetivamente possíveis falhas de segurança em ambientes de rede.

O fato desta ferramenta apresentar detecções contra intrusos, a mesma informa os logs, tanto pelo formato de texto do Linux quanto por HTTP on line. O Snort também apresentou o quanto é possível para qualquer pessoa trabalhar com ele, pois o mesmo possui alguns comandos referidos á área de programação, pois a regras dele não deixa de ser uma implementação.

Apenas uma ferramenta IDS não é o suficiente para a proteção de empresas e computadores em geral, pois cada aplicativo de segurança possui os seus méritos para combater aos ataques, por exemplo, se uma ferramenta IDS não conseguir barrar algum intruso, o Firewall poderá impedi-lo ou até mesmo o Antivírus poderá dependendo de cada intrusão e ação do aplicativo, ou seja, para uma segurança mais completa precisa-se desses três aplicativos de segurança, pois quando um não alcançar a intrusão o outro poderá conseguir e assim sucessivamente.

Os resultados dos testes realizados mostrou que o Snort é eficiente, e que também trabalha muito bem com os outros aplicativos instalados para a geração dos logs em HTML, pois o Snort detectou com eficiência o comando Ping realizado por outra máquina no computador onde estava instalado o Snort, com isso conclui - se que o Snort pode sim, ser usado em empresas que gostariam de adquirir uma ferramenta IDS,

REFERÊNCIAS BIBLIOGRÁFICAS

BORGES, Pedro Célio; COUTINHO, Rodrigo Trinck. *Análise de Sistemas de Detecção de Intrusão em Redes de Computadores.* 2007. 133f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação)- Universidade de Franca, Franca. Disponível em: http://www.snort.org.br Acessado em: 14/04/2008.

CAMPELLO, Rafael Saldanha; WEBER, Raul Fernando. **Sistemas de detecção de intrusão.** Disponível em: <http://www.inf.ufrgs.br/~gseg/producao/minicurso-ids-sbrc- 2001.pdf>. Acesso em: 01 novembro 2008.

CHIAVARO Ferreira, Bárbara – Sistemas de detecção de intrusão – Gravataí 2003.

CASWELL, Brian. **Snort 2: Sistema de Detecção de Intruso Open Source**. Rio de Janeiro:Alta Books, 2003. 373p.

CROTHERS, Tim. **Implementing Intrusion Detection Systems:** A Hands-on Guide for Securing the Network. Indianapolis: Wiley Publishing, 2003. 297p.

FERREIRA, André Luiz Rodrigues. **Projeto de trabalho: Escrevendo regras para o SNORT IDS**. Porto Alegre, 2004. Disponível em: http://www.freecode.linuxsecurity.com.br Acessado em: 20/04/2008.

HASENACK, Andréas. **Detecção de intrusão via rede – Snort**. Disponível em: <http://www.seguranca.conectiva.com.br>. Acesso em: 29 agosto 2008.

MELO, Daniel Araújo. 1998 **IDMEF, IDXP e CIDF – Em busca de uma padronização para Sistemas de Detecção de Intrusão.** [s.l.]: [s.s.], [s.d.] Disponível em:

http://www.modulo.com.br/index.jsp Acessado em 22 agosto 2008.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo: Berkeley Brasil, 2002. 320 p.

NORTHCUTT, Stephen; ZELTSER, Lenny et al. **Desvendando segurança em redes.** Rio de Janeiro: Editora Campus, 2002. 650p.

NSS GROUP. **Intrusion detection systems, Group test (edition 3)** 2002,

Disponível em: <http://www.nss.co.uk/ids/edition3/index.htm>. Acesso em 11 outubro 2008.

PROCTOR, Paul E. **The practical intrusion detection handbook.** New Jersey:

Prentice-Hall PTR, 2001. 359p.

ROESCH, Martin. **SNORT Users Manual:** SNORT realease 1.9.x, 2002.

Disponível em: <http://www.snort.org>. Acesso em: 17 novembro 2008.

SNORT – The open source network intrusion detection system. Disponível em:

<http://www.snort.org>. Acesso em: 14 setembro 2008.

TANENBAUM, Andrew S., 1994 – Redes de computadores / Andrew S. Tanenbaum tradução Vandenberg D. de Souza. – Rio de Janeiro: Elsevier, 2003 – 9ª reimpressão. P. 3-6-10.

TORRES, Gabriel. Rede de computadores curso completo. Rio de Janeiro, (Axcel, 2001) 5p.

YAHOO (Yahoo Respostas). Fórum de discução Disponível em: < http://br.answers.yahoo.com/question/index?qid=20070711195605AATEngZ >

Acessado em: 06 novembro 2008.

8. ANEXOS

QUESTIONÁRIO TECNICO SOBRE REDES

INFORMAÇÕES DE CONTATO COMERCIAL

Cargo: ADM DE REDES

Nome da empresa: JOÃO PAULO BERTONCINI

Telefone: | Fax: | Email:

Endereço registrado da empresa:

Cidade: ASSIS | Estado: SP | CEP:

Data de abertura da empresa: 2006

Firma individual: | Sociedade: | Corporação: | Outros:

ÁREA DE ATUAÇÃO

Descrição dos serviços : PROJETOS, INSTALAÇÕES, CONSULTORIA E GERENCIAMENTO DE REDES DE COMPUTADORES

Da suporte em alguma Empresa? Qual?

SIM

Há quanto tempo atua na área?

7 anos

QUESTÕES SOBRE REDES

Trabalha com ferramentas IDS? Qual?

SIM, SNORT

Qual Ferramenta IDS você recomdaria? Por quê?

SNORT, POR SER OPEN SOURCE, E DE FÁCIL GERENCIAMENTO, ALEM DAS REGRAS SEREM FLEXÍVEIS

Você acredita que só ferramentas como *FIREWALL* e *ANTIVÍRUS*, é seguro para uma empresa? Por que?

NÃO, A MELHOR OPÇÃO SERIA UM CONJUNTO DE FERRAMENTAS COMO IDS, FIREWALL, ANTI-VÍRUS E REGRAS PARA AUMENTAR A SEGURANÇA.

Qual segurança e quais tipos de proteção você recomendaria para uma empresa?

PARA UMA EMPRESA ESTAR SEGURA ELA PRECISA SEGUIR REGRAS E NORMAS QUE JUNTO COM AS FERRAMENTAS DE PROTEÇÃO FARIAM A MESMA TER MENOS POSSIBILIDADE DE SER ATACADA. FERRAMENTAS COMO IDS, FIREWALL, LOGS, ANTI-VÍRUS E ATUALIZAÇÕES SO AJUDAM NESSE PROCESSO DE PROTEÇÃO.

PREENCHA ABAIXO COM SUA OPNIÃO ASSUNTOS RELACIONADOS A REDES QUE NÃO FORAM QUESTIONADOS ACIMA

Luis Fernando de Oliveira - Suporte de informática

QUESTIONÁRIO TECNICO SOBRE REDES

INFORMAÇÕES DE CONTATO COMERCIAL

Cargo: Suporte de informatica

Nome da empresa: Engemap Gerenciamento

Telefone: 3421-2525 Fax: Email: luisfernando@engemap.com.br

Endereço registrado da empresa: R. Santos Dumont Nº 160

Cidade: Assis Estado: SP CEP: 1800-000

Data de abertura da empresa: — // —

Firma individual: não Sociedade: não Corporação: não Outros: não

ÁREA DE ATUAÇÃO

Descrição dos serviços :

Manutenção de micros e configuração de equipamentos em geral

Da suporte em alguma Empresa? Qual?

Não

Há quanto tempo atua na área?

6 anos

QUESTÕES SOBRE REDES

Trabalha com ferramentas IDS? Qual?

Não

Qual Ferramenta IDS você recomdaria? Por quê?

Recomendo todas as ferramentas IDS feitas em codigo aberto para uma distribuição sem custos

Você acredita que só ferramentas como *FIREWALL* e *ANTIVÍRUS*, é seguro para uma empresa? Por que?

Não pois com o desenvolvimento das tecnologias diversas ações podem ser imperceptíveis pelo sistema

Qual segurança e quais tipos de proteção você recomendaria para uma empresa?

Sistemas de monitoramento livre e com iptables com muita segurança

PREENCHA ABAIXO COM SUA OPNIÃO ASSUNTOS RELACIONADOS A REDES QUE NÃO FORAM QUESTIONADOS ACIMA

Hoje em dia a segurança na internet é o maior perigo para uma rede de uma empresa pois com a falta de atualizações constantes pode ocorrer uma expansão em massa de trojans ou vírus destruindo softwares em geral.
Procurar um sistema de segurança bom é difícil, por isso o desenvolvimento de sistemas livres é mais segura em relação à segurança de rede