UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

PRISCILA LONDERO ARCARO

ANÁLISE DE SEGURANÇA EM REDES UTILIZANDO O SISTEMA DE DETECÇÃO DE INTRUSÃO SNORT

CRICIUMA, JULHO DE 2011

PRISCILA LONDERO ARCARO

ANÁLISE DE SEGURANÇA EM REDES UTILIZANDO O SISTEMA DE DETECÇÃO DE INTRUSÃO SNORT

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. M.Sc. Rogério Antônio Casagrande

CRICIUMA, JULHO DE 2011

PRISCILA LONDERO ARCARO

Análise de Segurança em Redes Utilizando o Sistema de Detecção de Intrusão Snort

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Rogério Antônio Casagrande (UNESC)
Orientador

Prof. MSc. Fábricio Giordani. Nome (UNESC)

Prof. MSc. Paulo João Martins (UNESC)

Aos meus pais Venicio e Zeni!

AGRADECIMENTOS

Este espaço é dedicado a elogiar e destacar todos aqueles que tiveram uma participação no desenvolvimento deste trabalho.

Começo, agradecendo a Deus por ter me dado, a inspiração, paciência e a perseverança para que eu pudesse concluir este trabalho da melhor forma possível.

Em seguida, agradeço aos meus pais, pois sem eles, francamente, eu não teria chegado aqui. Ambos são responsáveis por cada sucesso obtido na minha vida. Durante todos esses anos vocês foram para mim um grande exemplo de força, de coragem, e energia infinita, me ensinaram a nunca desistir diante dos obstáculos. Vocês são e sempre serão meu maior porto seguro, meu maior exemplo de vitória, meus heróis e simplesmente aqueles que MAIS AMO. Obrigada por estarem sempre comigo. Obrigada simplesmente por participarem dessa caminhada, me ajudando a construir os alicerces de um futuro que começa agora.

Agradeço carinhosamente ao meu orientador, professor Rogério Antônio Casagrande pelos ensinamentos e lições recebidas. Obrigada pelas dicas, conselhos, gargalhadas e toda a ajuda.

Não posso deixar de lembrar: Marlise, Diego, Gélio, Thaffaréu, Lucas, Guilherme e Anderson, amigos das horas difíceis e das inúmeras horas boas também.

Como todo bom trabalho tem sempre uma consequência, acabei perturbando muito um grande amigo, para o esclarecimento das minhas dúvidas, relativas à parte prática do trabalho. Muito obrigada Marcos por ter perdido horas me ajudando em instalações e configurações.

A todos aqueles que me ouviram e, por conseguinte, aturaram os meus delírios, principalmente você, Margarete, nesses últimos meses, gostaria de expressar o meu mais sincero obrigado!

Assim, não corro o risco de esquecer ninguém!

Ama sempre, fazendo pelos outros o melhor que possas realizar. Age auxiliando... Serve sem apego... E assim vencerás!

Chico Xavier

RESUMO

O crescimento da Internet facilitou o compartilhamento de recursos e informações, estas informações passaram a agregar um valor muito grande, e para protegê-las, estratégias de segurança começaram a surgir. A partir daí, a comunicação segura se tornou um requisito importante, visto que uma tentativa de ataque pode causar prejuízos a uma empresa ou usuário comum. As ameaças existentes trazem grandes problemas, já que muitas empresas e usuários deixam de utilizar a Internet para realizar tarefas que envolvam o uso de dados pessoais e principalmente financeiros. Existem atualmente várias técnicas utilizadas para a proteção de redes e computadores, dentre elas, pode-se destacar os Sistemas de Detecção de Intrusão. Os IDSs representam meios de se descobrir se uma rede ou host está sendo alvo de acessos não autorizados. Este trabalho apresenta o conceito de segurança da informação, os principais tipos de ameaças e ataques às redes, e também realiza testes de eficiência no Sistema Operacional Windows utilizando as ferramentas Nmap e Brutus, estes sendo detectados por meio da ferramenta Snort que em conjunto com a ferramenta EventSentry possibilita a configuração de filtros com as assinaturas dos ataques, gerando assim, respostas passivas.

Palavras chave: Snort; Sistema de Detecção de Intrusão; Ataques, Ameaças.

ABSTRACT

The growth of the Internet has facilitated the sharing of resources and information, these information are passed to aggregate a very large value, and to protect them, security strategies began to emerge. By the way, the secure communication has became an important requirement, since an attempted attack can damage a company or user. Existing threats bring big problems, since many companies and users fail to use the Internet to perform tasks involving the use of personal data and mainly financial. There are currently several techniques used to protect networks and computers, among which we can outstanding the Intrusion Detection Systems. The IDSs represent means of discovering whether a network or host is the target of unauthorizeds access. This paper present the concept of information security, the main types of threats and network attacks, and also performs tests of efficiency in the Windows OS tools using Nmap and Brutus, these being detected by the tool Snort which together with the tool EventSentry enables the configuration of filters with the signatures of attacks, thus generating passive responses.

Keywords: Snort, Intrusion Detection System; Attacks, Threats.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ACID	*Analysis Console for Intrusion Databases*
ARPANET	*Advanced Research Projects Agency Network*
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CPU	*Central Processing Unit*
DNS	*Domain Name System*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
MAC	*Media Acess Control*
NIC	*Network Interface Card*
NTP	*Network Time Protocol*
PHP	*Hypertext Preprocessor*
POP3	*Post Office Protocol*
SGBD	Sistema de Gerenciamento de Banco de Dados
SMB	*Server Message Block*
SNMP	*Simpe Network Management Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*

SUMÁRIO

1 INTRODUÇÃO

Conforme Monteiro (2003) em meados da década de 60, o Departamento de Defesa Americano criou o *Advanced Research Projects Agency Network* (ARPANET) que interligava todas as agências de defesa dos Estados Unidos e, posteriormente, empresas públicas do governo e universidades. O governo americano utilizou como meio de transmissão a infra-estrutura pública das companhias telefônicas. Mais tarde, surgiu a necessidade de um protocolo que pudesse conectar diferentes redes, o Protocolo de Controle de Transmissão (*Transmission Control Protocol* - TCP) e ainda assim manter essa rede sem um ponto central, pois essa rede deveria suportar um ataque nuclear, já que o departamento de defesa tinha que manter um sistema de comunicação ativo. Com o crescimento da rede ARPANET, ocorreu à adoção oficial deste protocolo de comunicação.

Com a conexão de diversas redes e a abertura para fins comerciais, à Internet obteve um crescimento enorme na década de 90, e então se tornou uma rede gigante a nível mundial. Só no Brasil existem aproximadamente 27,7 milhões de internautas (BRASIL..., 2010).

As redes de computadores surgiram da necessidade de compartilhamento de dados e dispositivos. Este novo panorama traz consigo muitos benefícios às organizações e serviços cada vez mais atraentes aos clientes, além de promover interessantes oportunidades de negócios.

Contudo, surgiram também os problemas com segurança, sendo esta um requisito essencial para todo tipo de rede sujeita à presença de intrusos. Paralelamente a essa nova tecnologia surge a necessidade de implantação de mecanismos de segurança não somente corretivos, mas também preventivos.

A segurança da informação tem a finalidade de garantir disponibilidade, sigilo, integridade, autenticidade, controle de acesso e o não-repúdio da informação (OLIVEIRA, 2001).

A presença de um intruso na rede num caminho onde trafegam dados pode interferir em toda produtividade da rede, prejudicando o alcance dos objetivos. Comumente, as redes de computadores e hosts são invadidas e infectadas com níveis mais sofisticados de invasão, ficando, portanto difícil de implementar técnicas de detecção de intrusão eficazes. Por consequência desses acontecimentos muitas técnicas de proteção são utilizadas para tentar bloquear definitivamente ou parcialmente as tentativas de invasões.

Os vírus e variantes tornam-se tão comuns, que segundo Melis Neto e Gonçalvez (2005) até convencionou-se um nome para esses códigos: são os *Malwares*, essa categoria engloba toda espécie de pragas digitais, incluindo os *vírus*, *cavalos de tróia*, *sniffers*, *spywares*, *adwares*, entre outros. Além de conhecer estes agentes nocivos, o usuário tem que ter em mãos ferramentas e técnicas que permitam identificar e eliminar estas pragas.

Para identificar se um computador ou uma rede está comprometida, utilizam-se ferramentas que auxiliam na monitoração das redes, como por exemplo, os *sniffers*. Estes são largamente utilizados por *hackers* para monitorar o tráfego do segmento da rede onde foi instalado, e representam sérias ameaças à segurança, pois "podem comprometer a confidencialidade dos dados em tráfego, além de capturarem qualquer informação em modo texto", como: senhas, dados do usuário, entre outros (CASAGRANDE, 2003, p. 11).

Detectar essas atividades é de suma importância e os Sistemas de Detecção de Intrusão (*Intrusion Detection System* - IDS) constituem mais uma oportunidade disponível para emissão de alertas à administração da rede na detecção de intrusão. Os IDSs apresentam vantagens, quando bem posicionados podem monitorar grandes redes, além de não interferirem no funcionamento destas, são difíceis de serem percebidos por atacantes e

possuem grande segurança contra ataques. Porém, podem falhar em reconhecer um ataque em um momento de tráfego intenso, e não analisam informações criptografadas, sendo este um grande problema, pois a maioria dos atacantes utiliza criptografia em suas invasões. Alguns destes *softwares* não identificam se um ataque foi bem ou mal sucedido, apenas alertam quando o ataque foi iniciado (PUPO, 2009).

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) mantido pelo Comitê Gestor da Internet no Brasil (NIC) o número de incidentes em 1999 era de 3.107 por ano. Comparado com a análise realizada até dezembro de 2009, este número cresceu para 358.343 incidentes reportados ao CERT (CERT, 2010). Um aumento considerável de 11.533,41%.

Sendo assim, este trabalho propõe a simulação de alguns tipos comuns de ataques e a verificação do comportamento do *software* para detecção de intrusão, juntamente com a elaboração da documentação analisada possibilitando descobrir se um computador ou rede foi comprometido.

1.1 OBJETIVO GERAL

Avaliar o comportamento e eficiência do Sistema de Detecção de Intrusão na iminência de tipos de ataques mais conhecidos.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são listados abaixo:

a) entender os aspectos de funcionamento das redes;

b) verificar e analisar as vulnerabilidades de redes;

c) compreender o funcionamento das arquiteturas IDS;

d) analisar as técnicas de detecção de intrusão;

e) analisar e comparar as funcionalidades dos *softwares* responsáveis pela detecção de intrusão nos sistemas e redes;

f) estudar sobre o funcionamento do Sistema de Detecção de Intrusão Snort;

g) simular ataques e avaliar o comportamento dos IDSs em relação a sua eficiência;

1.3 JUSTIFICATIVA

As redes de computadores foram criadas para facilitar a transmissão e o compartilhamento de dados (CHOLEWA, 2001).

Considerando o volume de usuários conectados a Internet, tanto em organizações, comércios, empresas e até usuários domésticos, a segurança vem se tornando um requisito de grande valor. Conforme Oliveira (2001) a segurança da informação é um componente complexo e pode envolver certas situações como: erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, entre outros.

A segurança deve ser tratada como sendo a restrição dos recursos de um microcomputador em uma rede, ou de porções desta rede para outros usuários ou computadores. Esta restrição não é nada além do que a gestão da segurança, o que estabelece regras, consequentemente, a política de segurança (OLIVEIRA, 2001).

A utilização de ferramentas IDSs livres serve para mostrar que estas apresentam baixo custo e muitas funcionalidades, sendo que este tipo de análise vai contribuir incentivando empresas e entidades a implementar em suas redes o uso de um sistema de

detecção de intrusão devido ao baixo custo e diminuição de riscos relacionados à segurança (SANTOS, M., 2004).

Este trabalho tem o objetivo de mostrar a eficiência que ferramentas IDSs têm em monitorar eventos que incidem em um sistema computacional, diminuindo o risco de fraudes, ocasionando maior controle das informações e assegurando a identidade dos sistemas participantes de uma transação, a integridade dos dados, a confidencialidade, a autoria da transação, a defesa contra indisponibilização forçada, a unicidade da transação, impedindo sua replicação indevida, e muitos outros motivos que conforme Oliveira (2001) acarretam na preocupação com a segurança.

1.4 ESTRUTURA DO TRABALHO

Este trabalho está organizado em seis capítulos. No Capítulo 1 é apresentada uma introdução ao tema proposto, os objetivos gerais e específicos e a justificativa deste trabalho.

O tema segurança da informação e sua importância, bem como normas, políticas de segurança e criptografia está descrito no Capítulo 2.

É apresentado no Capítulo 3 as ameaças e ataques e algumas ferramentas utilizadas para obter sucesso em um ataque. Aborda também os sniffers e seu funcionamento.

No Capítulo 4 será estudado os Sistemas de Detecção de Intrusão, as suas características desejáveis e toda sua classificação segundo fonte de informação, análise e resposta, apresenta exemplos de IDSs como Snort e Bro, explicando seu funcionamento.

Alguns dos trabalhos correlatos que mais auxiliaram na realização deste trabalho de pesquisa estão descritos no Capítulo 5.

Por fim, o Capítulo 6 apresenta o trabalho desenvolvido, a descrição das metodologias e o ambiente de rede utilizado.

2 SEGURANÇA DA INFORMAÇÃO

Este capítulo apresenta uma introdução à segurança da informação. Primeiramente é abordada a importância da segurança nas redes de computadores, políticas de segurança e a norma que regulamenta a gestão da segurança da informação. Apresenta-se a comunicação de dados e meios de como manter uma comunicação mais segura por meio da utilização de criptografia.

Segundo Deschamps, Peres e Zipf (2005) o termo Comunicação de Dados caracteriza os Sistemas de Telecomunicações, cuja informação tanto na origem como no destino aparecem de forma digital. Estas informações aparecem na forma de voz, áudio, imagem, vídeo ou texto. Na maioria das vezes o sinal analógico é convertido para digital por meio de sistemas computacionais ou sistemas que possuam as características para efetuar a conversão, e assim atender a necessidade de cada usuário em diversas localidades.

Para efetuar a transferência destas informações podem ser usados meios próprios, tal como uma rede de computadores de uma organização, ou provedores de serviços, que interligam pontos distantes.

Uma rede de computadores, conforme cita Thomé (2000) tem como objetivo disponibilizar meios de acesso, para que usuários em diferentes localidades possam se comunicar. A questão está no compartilhamento de recursos, tais como programas, banco de dados, recursos de transmissão, entre outros.

Devido a esta possibilidade de compartilhamento de informações, a segurança das redes e informações tornou-se crítica, surgindo à necessidade de segurança no compartilhando de informações. Malta (2006) diz que é ampla a possibilidade de que pessoas não autorizadas consigam acesso a informações confidenciais por meio de métodos ilícitos.

2.1 IMPORTÂNCIA DA SEGURANÇA NAS REDES DE COMPUTADORES

Uma grande parte dos problemas com segurança em redes é causada por pessoas maliciosas que tentam usufruir de algum benefício, chamar atenção ou prejudicar alguém (TANENBAUM, 2003).

Wadlow (2000) ao abordar sobre segurança destaca que o processo de segurança abrange três características básicas: **Análise**, **Síntese** e **Avaliação**.

No processo de análise, deve-se considerar o problema e tudo que se conhece sobre ele. No processo de síntese, busca-se uma solução para o problema a partir da análise concluída. E, a avaliação tem como objetivo instruir quais aspectos não corresponderam a suas expectativas.

Para tornar uma rede segura é preciso ter a consciência de que muitas vezes os invasores são inteligentes, dedicados e bem subsidiados, este processo envolve muito mais do que mantê-la livre de erros de programação, as medidas utilizadas para interromper a atividade de eventuais invasores, terá menor impacto em invasores mais experientes. Com o aumento no uso das redes, a questão da segurança tornou-se indispensável. A segurança que as organizações buscam está na garantia de que nenhuma pessoa mal-intencionada possa ler, tenha acesso ou até mesmo modifique mensagens ou dados por meio da rede, tornando assim, a rede menos vulnerável a possíveis invasões, e a comunicação mais segura.

Para garantir a segurança de uma rede ou um sistema de computadores, é preciso considerá-la como um processo e não, uma meta, daí surgiu à idéia de criação das Políticas de Segurança e para regulamentar este processo em junho de 2007 foi atualizada a antiga NBR ISO/IEC 17799 para numeração NBR ISO/IEC 27002 esta norma é um conjunto de recomendações para práticas na gestão de Segurança da Informação.

2.1.1 Normas e Políticas de Segurança

É fundamental para que muitos dos requisitos de segurança sejam cumpridos e auxiliem a manutenção desta, que normas e políticas sejam adotadas, principalmente pelas organizações.

Uma política de segurança consiste em inúmeras decisões que em conjunto irão determinar como uma organização ou até mesmo uma pessoa, irá se comportar em relação à esta. De acordo com Lemos (2001) as políticas determinam os limites de tolerância e os níveis de respostas às violações que possam incidir. Estas diferem de uma organização para outra, mas o importante é que toda organização, independente do seu tipo ou tamanho, deve apresentar uma política de segurança bem definida. Segundo Lemos (2001), estas políticas devem ser utilizadas para a manutenção da segurança da informação, e por isso devem ser documentadas e de conhecimento de todos.

A norma ABNT NBR/ISO IEC 27002, é a versão nacional da norma internacional ISO 27002, esta última versão passou a vigorar em 30/09/2005. Ela estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (BRASIL, 2009).

Aborda também regras de termos e definições, política de segurança da informação, classificação e controle dos ativos de informação, segurança física e do ambiente, gerenciamento das operações e comunicações, conformidades da lei, controle de acesso entre outros. Os objetivos definidos nesta norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação (NIEHUES, 2007).

Para diminuir as ocorrências de incidentes de segurança, pode-se adotar normas e políticas de segurança, pois estas permitem criar formas padronizadas e eficazes no

gerenciamento da informação, e podem ser utilizadas por organizações, bem como por usuários domésticos que buscam maior proteção de seus dados.

2.2 COMUNICAÇÃO SEGURA

A transferência de dados, as transações comerciais, a comunicação via rede, ou quando se utiliza o meio compartilhado (Internet), são fatores importantes quando se fala de comunicação segura.

Quando dois ou mais usuários optam por trocar informações ou trabalhar em conjunto, eles precisarão de meios de comunicação seguros ("seguros" refere-se à transmissão da comunicação protegida compartilhada entre as partes).

De acordo com Belo (2003) a comunicação segura tem como objetivos: a **Confidencialidade, Autenticação, Integridade, Disponibilidade e Acesso.**

Na confidencialidade existe um sigilo entre as informações trocadas entre o expedidor e o destinatário, de modo que só ambos conhecem o conteúdo de cada mensagem trocada.

Na autenticação o expedidor e o destinatário são reais e verdadeiros.

Na integridade a mensagem enviada é recebida sem alterações e somente o expedidor e o destinatário podem modificar as mensagens trocadas por eles.

Na Disponibilidade e Acesso existe a possibilidade de comunicação e sua legitimidade.

De acordo com Laufer (2003) existem muitas ferramentas que em conjunto colaboram significativamente para a melhoria da segurança de uma rede. Como por exemplo, a criptografia, pois esta estabelece um nível de proteção aos dados.

Com a necessidade do envio de informações sensíveis por um meio de comunicação não-seguro, ou seja, em um meio onde não é possível garantir que um intruso não irá interceptar o fluxo de dados para leitura (intruso passivo) ou para modificá-los (intruso ativo) surgiu a criptografia. Esta tem por objetivo, criptografar uma mensagem utilizando um método de cifragem, que recebe como entrada a própria mensagem e uma chave, produzindo como resultado uma mensagem cifrada. A mensagem é transmitida ao receptor, que para decriptografá-la utiliza um método de decifragem que recebe como entrada a mensagem e uma chave de decifragem e fornece como saída à mensagem original.

A Figura 1 apresenta este processo:

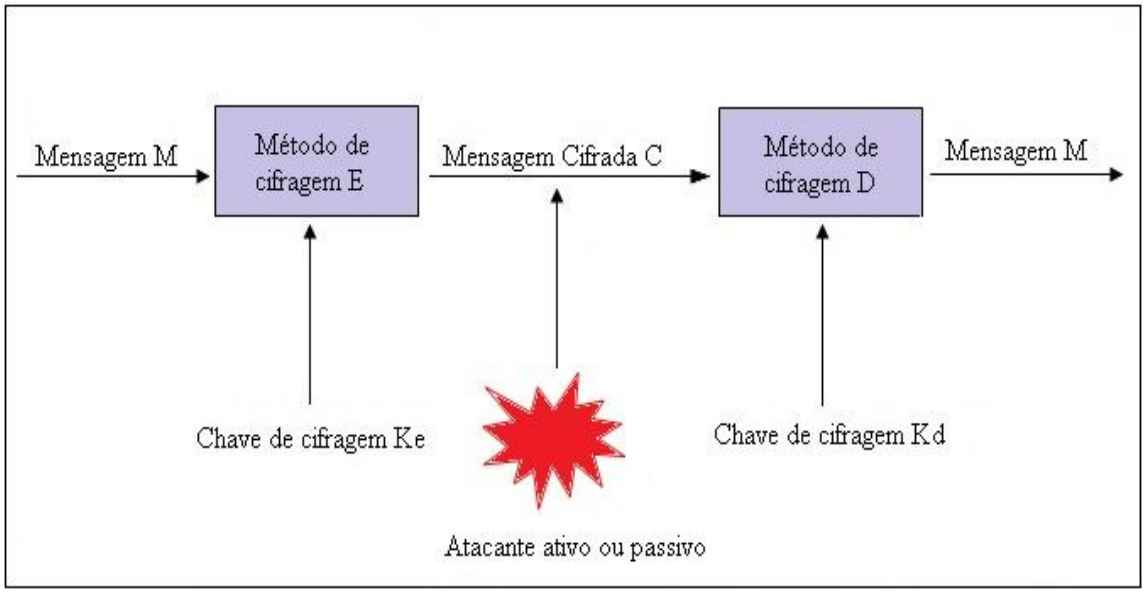


Figura 1. Sistema de Criptografia
Fonte: Adaptado de FRANCESCHINELLI, D. (2003, p. 14)

Os sistemas de Criptografia envolvem um valor secreto, chamado de chave e um algoritmo. Existem três tipos de funções criptográficas, criptografia de chave secreta ou simétrica, criptografia de chave pública ou assimétrica e função Hash (NORTHCUTT et al., 2002).

2.2.1 Criptografia de Chave Secreta ou Simétrica

De acordo com Northcutt et al (2002) este método criptográfico emprega o mesmo valor de chave para codificar e decodificar mensagens trocadas entre emissor e receptor, levando em consideração que tiveram um tempo antecipado para compartilhar a chave. Este método de criptografia pode ser rápido, pois a matemática usada para criar o texto cifrado desta chave não é tão complexa.

Uma grande desvantagem do algoritmo simétrico é que muitas vezes é difícil trocar remotamente ou começar uma troca simétrica com um parceiro desconhecido, pois é complexo autenticar se essa pessoa é realmente quem diz ser. Como vantagem, este algoritmo de chave secreta apresenta rapidez de execução e forte autenticação ativa se comparado aos algoritmos de chave pública. Como a criptografia simétrica funciona compartilhando-se uma chave entre o emissor e o receptor da mensagem, o principal problema encontrado é o gerenciamento da chave, pois, se por algum descuido ou de forma proposital, está chave for descoberta, o sigilo da informação estará prejudicado. Conforme ilustra a Figura 2:

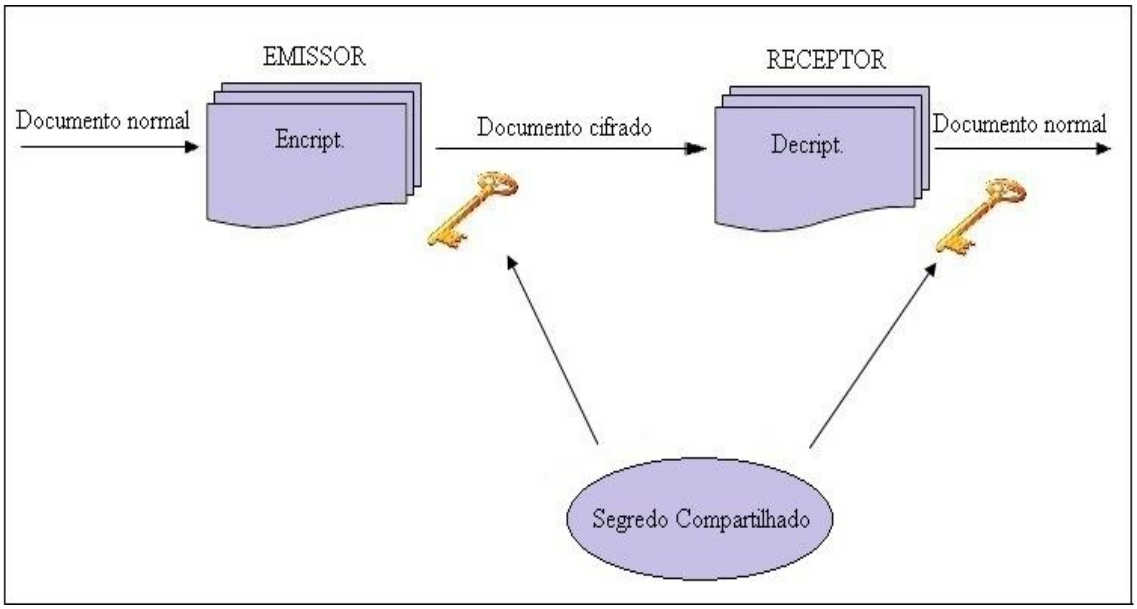


Figura 2. Criptografia de Chave Secreta ou Simétrica
Fonte: Adaptado de FRANCESCHINELLI, D. (2003, p. 15)

2.2.2 Criptografia de Chave Pública ou Assimétrica

Algoritmos de chave assimétrica, segundo Northcutt et al (2002), utilizam um meio de criptografia distinto. São usadas duas chaves diferentes: uma chave pública e uma chave privada. Neste algoritmo a chave pública é utilizada para codificar o texto cifrado e a chave privada para decodificar este texto e retorná-lo novamente no texto original.

A matemática usada pelos algoritmos assimétricos é muito mais complexa, pois, apesar do texto cifrado poder ser gerado por qualquer pessoa que tenha uma cópia da chave pública, somente a pessoa que tiver a chave privada pode decodificá-lo. A desvantagem é que este algoritmo exige muito mais processamento e, portanto, é mais lento.

No método assimétrico o sigilo está garantido porque, neste caso, a única chave capaz de decriptografar o documento é a chave privada do receptor, mas não a autenticidade, já que a chave pública não pode comprometer o texto cifrado, esta pode ser amplamente distribuída. Isso faz com que não haja garantia de que o documento esteja vindo da pessoa que o emissor diz ser. Conforme apresentado na Figura 3:

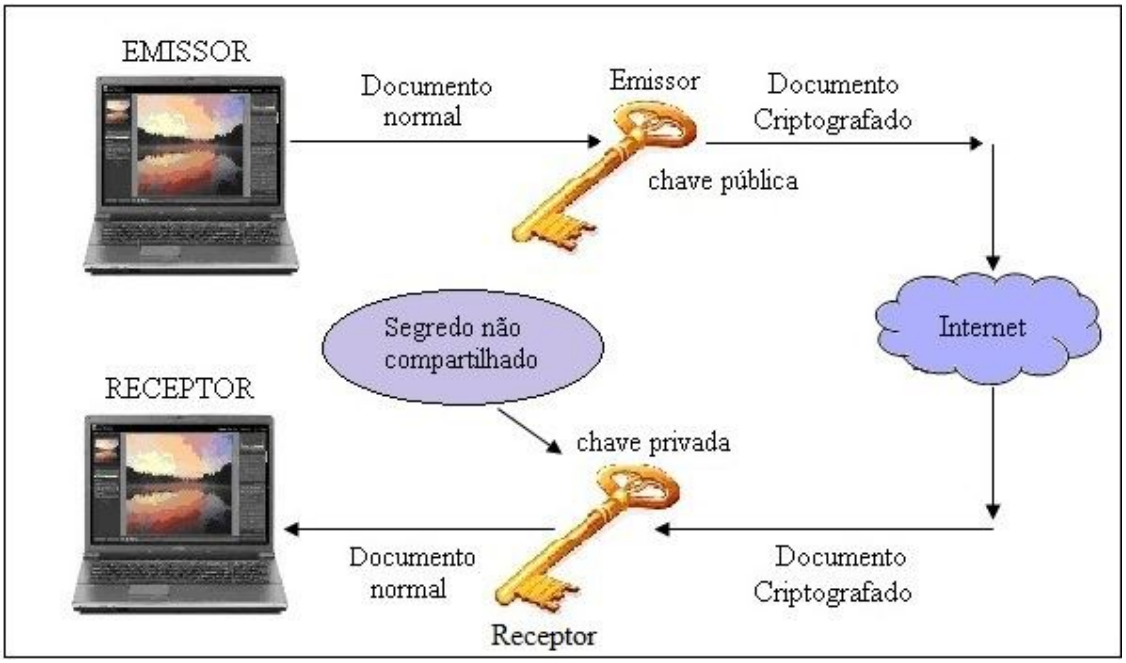


Figura 3. Criptografia de Chave Pública ou Assimétrica
Fonte: Adaptado de FRANCESCHINELLI, D. (2003, p. 16)

2.2.3 Função Hash

"A idéia básica de uma função *hash* é truncar a informação de tal maneira que o processo não possa ser revertido" (FRANCESCHINELLI, 2003, p. 16).

O valor de entrada da mensagem tem comprimento variável, porém o valor de saída da função possui tamanho fixo (geralmente 128 a 256 bits). Qualquer mínima alteração na mensagem produz alteração significativa na mensagem final. Contudo, a probabilidade de se encontrar duas mensagens que produzam o mesmo valor *hash* de saída é praticamente nula. De acordo com Franceschinelli (2003) a função *hash* tem como objetivo garantir a integridade do documento recebido e apresentar agilidade na decifragem do mesmo.

Conforme o que foi mencionado até então, o uso adequado da Segurança da Informação, e dos mecanismos de proteção auxiliam nas condições mais seguras da transmissão e compartilhamento de dados, contudo, é necessário conhecer e analisar os riscos existentes.

3 AMEAÇAS E ATAQUES

Este capítulo fala sobre os tipos de ameaças e ataques que todo usuário conectado na Internet pode sofrer, descreve também sobre algumas ferramentas que são utilizadas para concretizar estes ataques.

Segundo Machado e Freire (2006, p. 32) “a maioria dos problemas de segurança que acontecem nos computadores domésticos, é causada pela falta de informação do usuário sobre os códigos maliciosos que se proliferam e sobre o próprio sistema operacional que ele usa”.

3.1 TIPOS DE AMEAÇAS

Conforme Franceschinelli (2003) os atacantes podem apresentar comportamentos diferentes em relação às posições de origem e destino das mensagens. O objetivo de um atacante é: **Interromper**, **Interceptar**, **Modificar** ou **Fabricar** mensagens.

Na interrupção o objetivo do atacante é interromper o fluxo de dados que parte da origem, para deixar o destinatário sem receber os pacotes de informações.

Na interceptação o atacante quer ter acesso ao fluxo de dados que está trafegando. Este acesso influencia na confiabilidade das informações.

Na modificação além do atacante ter acesso aos dados, ele também modificá-os para consequentemente enviá-los ao destino. Neste caso, há uma perda na integridade dos dados que foram desrespeitados.

E na fabricação o atacante produz dados para enviar a um destinatário, que não tem como saber quem os enviou. Não há autenticidade na informação enviada.

A Figura 4 apresenta este processo:

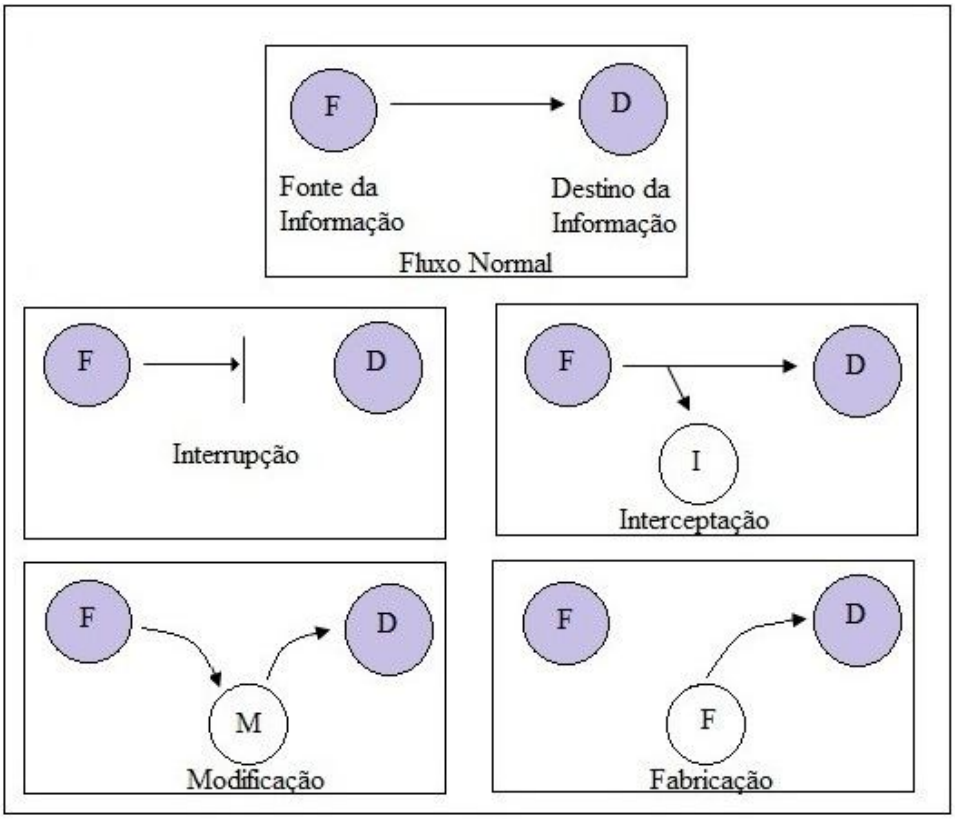


Figura 4. Posição do atacante em relação à origem e ao destino
Fonte: Adaptado de FRANCESCHINELLI, D. (2003, p. 7)

Segundo Machado e Freire (2006, p.33) “há muito despreparo por parte dos usuários com relação a melhores práticas e procedimentos no uso do computador e da Internet”.

De acordo com as estatísticas do CERT, de janeiro até setembro de 2010 foram registradas 101.156 notificações de tentativas de fraudes digitais. Porém a grande maioria poderia ter sido evitada se houvesse maior conhecimento por parte dos usuários da Internet (CERT, 2010).

Conforme ISOC (2000) existem três tipos de ameaças:

a) **ameaça inteligente:** o invasor tem a capacidade técnica e operacional para encontrar e explorar as vulnerabilidades do sistema;

b) **ameaça potencial:** esta ameaça existe quando há uma causa, ação ou evento que poderia interromper a segurança e causar dano;

c) **ameaça de análise:** é realizada uma análise da probabilidade da ocorrência de um ataque e dos resultados de ações prejudiciais ao sistema.

Além da classificação por tipo, as ameaças podem ser divididas quanto ao seu grau de intencionalidade (SÊMOLA, 2003):

a) **naturais**: estas ameaças são causadas por fenômenos da natureza, como incêndios, terremotos, furacões, inundações, entre outros;

b) **involuntárias**: ameaça inconsciente, quase sempre causada pela falta de conhecimento, podem também serem causadas por erros no sistema, acidentes, falta de energia, entre outros;

c) **voluntárias**: ameaças intencionais causadas por uma pessoa ou um grupo de pessoas, como por exemplo, invasores, *hackers*, ladrões, espiões, criadores e disseminadores de vírus de computador. Ameaças voluntárias se dividem em dois grupos: ameaças intencionais internas e externas:

- **ameaças intencionais internas:** são realizadas por um intruso ou grupo de intrusos que fazem parte do cotidiano do local e que possuem autorização limitada para acessar máquinas e seus recursos,
- **ameaças intencionais externas:** são realizadas por um intruso ou grupo de intrusos que não fazem parte do cotidiano do local e que não tem acesso autorizado às informações, porém os invasores conhecem o local e estudaram o sistema de segurança para posteriormente atacá-lo.

As ameaças anteriormente citadas aparecem de diversas formas, Niehues (2007) destaca que na Internet existem diversos aplicativos, como vírus, ou ferramentas de ataque muito perigosas, que monitoram o uso do computador. A seguir serão citados tipos de ataques e seu funcionamento.

3.2 PRINCIPAIS TIPOS DE ATAQUES

A RFC 2828 cita que ataque é uma ação que ameaça a segurança de um sistema, o ataque explora as vulnerabilidades no sistema alvo e muitas vezes, pode não ser bem sucedido. Um ataque é a concretização de uma ameaça, este ataque pode ser *ativo*, quando o resultado obtido é a alteração dos dados; *passivo*, quando o objetivo é a liberação dos dados, e *destrutivo* quando visa negar acesso a serviços ou dados. O sucesso de um ataque depende da vulnerabilidade do sistema e da eficácia de contra medidas existentes (ISOC, 2000, tradução nossa).

Dos vários tipos de ataques existentes pode-se destacar: **Engenharia Social, Vírus, Cavalos de Tróia, Worms, Phishings, Sniffing, Ataques de Força Bruta, Bots e Botnets, Rootkits, Phaming, Exploits, Ataques de Buffer Overflow, Spyware, Adware, Backdoors, Keyloggers e Screenlogger, Denial of Service.**

3.2.1 Engenharia Social

Engenharia Social é um ataque onde a principal estratégia utilizada é a capacidade de convencer pessoas a fornecerem informações, executar programas e muitas vezes fornecer senhas de acesso (SANTOS, L., 2004).

Os acessos indevidos à informação em formato eletrônico, em papel ou em outros formatos são feito por meio do levantamento de dados preliminares que tornam a tentativa de invasão mais eficiente. O levantamento de dados pode ser feito por meio de e-mail, telefone, chat, fax e até mesmo pessoalmente.

Segundo Mitnick e Simon (2005) uma das táticas da engenharia social é obter informações que são consideradas inofensivas por usuários e utilizá-las para conseguir a confiança de outros usuários e assim alcançar as informações que ele deseja.

Este tipo de ataque é quase sempre fácil de identificar com um pouco de atenção e conhecimento, uma decisão errada pode ser evitada não comprometendo a segurança do computador ou de uma rede.

3.2.2 Vírus

Os vírus são pequenos códigos executáveis e maliciosos de programas que infectam sistemas computacionais. O que os torna diferente dos outros tipos de códigos maliciosos é que este se replica tornando possível infectar outros computadores, sempre com o intermédio do usuário, o vírus permanece indetectável até que seja ativado e se propaga rapidamente pela Internet, podendo infectar muitos computadores em pouco tempo (CRONKHITE; MCCULLOUGH, 2001).

Para Melis Neto e Gonçalvez (2005) existe um conceito que define o que é cada código mediante análise de suas instruções, comportamento, infecção, propagação e consequências. Existe um número enorme de nomenclaturas. O número de pragas conhecidas pode variar de acordo com o fabricante do antivírus, pois alguns consideram as famílias de vírus e outros consideram que cada variação seja um tipo diferente de vírus.

Conforme Niehues (2007) existem diferentes tarefas que podem ser executadas por vírus em um sistema computacional, dentre elas:

a) excluir arquivos pessoais ou do sistema;

b) diminuir o desempenho do computador;

c) alterar o conteúdo de arquivos;

d) conceder acesso às informações confidenciais;

e) monitorar a utilização do computador;

f) diminuir o desempenho da rede (local e Internet);

g) impossibilitar o uso de periféricos.

3.2.3 Cavalos de Tróia

Os Cavalos de Tróia ou *Trojan Horse* foram criados por programadores com a intenção de prejudicar outros usuários. Possuem várias funções, mas com relação à segurança na Internet, eles podem realizar algumas funções que mostram ao programador informações privilegiadas sobre um determinado sistema, podendo comprometê-lo.

De acordo com Gomes (2000) Cavalos de Tróia são programas maliciosos e não autorizados que estão contidos dentro de outro programa autêntico. Contém funções desconhecidas e que não são utilizadas por um usuário comum. As funções de um programa autêntico que foi alterado por um cavalo de tróia são inutilizáveis.

Os *trojans* representam um alto risco, pois, por serem encontrados em formas binárias, são difíceis de detectar. Este tipo de ataque pode ser fatal para um administrador de sistemas que possua um conhecimento a nível médio de segurança, porque ele pode comprometer totalmente um sistema, "um *cracker*[1] com privilégios *root* pode alterar um sistema inteiro e conseguir o que quiser" (GOMES, 2000, p. 129).

Para Machado e Freire (2006) atualmente os *trojans* são a principal ameaça digital, uma vez que permitem a captura de informações do disco rígido, de e-mail, de textos, sendo que os dados mais procurados são os financeiros.

[1] Pessoa que utiliza sua sabedoria para comprometer a segurança da rede (GOMES, 2000).

3.2.4 Worms

Apesar de não serem vírus, estes *worms* ou vermes têm a capacidade de se disseminar por meio de redes e enviar cópias de si mesmo de uma máquina para outra. Os vermes se replicam, porém não precisam de outro programa para se propagar, por isso não se encaixam na definição tradicional de vírus (CERT, 2006).

Worms consomem recursos, comprometem o desempenho de redes e lotam o disco rígido do computador, pois costumam fazer muitas cópias de si mesmo, se propagam por meio de vulnerabilidades ou falhas na configuração dos *softwares* instalados nos computadores e são difíceis de remover (EGOSHI; ROMANO, 2003).

De acordo com Niehues (2007) os vermes possuem algoritmos inteligentes e exploram desde sistemas operacionais falhos até sistemas disponíveis em outras máquinas.

3.2.5 Phishing

Uma das fraudes mais utilizadas no exterior, criada em 2003 é o *phishing*. Esta fraude foi desenvolvida para roubar informações de usuários da Internet (CERT, 2006).

Mensagens são enviadas para os usuários por meio de e-mail ou técnicas de Engenharia Social, quando o destinatário digita suas informações pessoais ou sigilosas, como, por exemplo, números de cartões de crédito ou senhas, as informações são capturadas para serem utilizadas em roubos entre outros.

Conforme Niehues (2007) uma tentativa de *phishing* solicita que o usuário efetue ou atualize um cadastro, e então as informações digitadas são levadas diretamente para o invasor.

Por causa da falta de atenção dos usuários, muitos acabam sendo enganados, pois não se atentam aos detalhes e muitas vezes, acreditam que estes e-mails são autênticos.

3.2.6 Sniffing

De acordo com Gomes (2000) o *sniffing* é uma técnica que intercepta e monitora o tráfego da rede, possibilitando a captura de informações, como senhas, usuários ou qualquer dado confidencial.

Em um ambiente de rede normal, os nomes de usuário e as senhas passam por meio da rede por um texto não criptografado, um intruso utilizando uma máquina com interface de rede em modo promíscuo pode obter com facilidade qualquer informação.

Conforme citado por Niehues (2007) esta técnica é direcionada para ataques em redes locais, porém “pode ser utilizada em *links* de Internet via cabo e outros que utilizam uma pequena rede local, como condomínios, prédios, onde a Internet é compartilhada”.

3.2.7 Ataques de Força Bruta

O ataque de força bruta é uma das técnicas mais antigas de invasão, consiste em descobrir o nome de usuário e a senha de um sistema. Para conseguir a senha geram-se todas as combinações possíveis de letras, números e símbolos, geralmente estes ataques são iniciados a partir de logins padrão, como por exemplo, admin, administrador, root. (MACHADO; FREIRE, 2006).

Ainda de acordo com Machado e Freire (2006) para obter uma maior segurança o usuário deve criar senhas mais seguras com pelo menos sete caracteres, utilizar letras maiúsculas e minúsculas e incluir números em sua senha. Com o avanço no poder de cálculos

dos computadores, o tempo necessário para adivinhar uma senha mais longa tem reduzido bastante, porém, esta técnica de ataque vem sendo pouco utilizada, devido à facilidade de ser combatida. A grande maioria dos servidores bloqueia tentativas sucessivas de acesso em virtude dos dados estarem incorretos.

3.2.8 Bots e Botnets

Segundo o CERT (2006) *Bots* são semelhantes à *worm*, pois, se propagam automaticamente e exploram vulnerabilidades ou falhas na configuração de *softwares* instalados no computador. A diferença consiste em que o *Bot* pode ser controlado remotamente.

Ao se comunicar com um *bot*, o invasor pode enviar instruções para que ele realize atividades como: desferir ataques na Internet, executar um ataque de negação de serviço, furtar dados de computadores, enviar e-mails de *phising* ou *spam.*

Quando se tem muitos computadores infectados com *bots*, estes formam uma rede que é chamada de *botnet*. Estas redes são formadas por centenas ou milhares de computadores, o invasor que tem controle sobre uma *botnet* pode utilizá-la para aumentar a força de seus ataques (CERT, 2006).

3.2.9 Rootkits

De acordo com Hatch, Lee e Kurtz (2002) os *rootkits* são conjuntos de programas binários com cavalos de tróia, pré-empacotados, que são instalados rapidamente assim que um invasor conseguir acesso à máquina. A maioria dos *rootkits* possui um farejador que procura senhas na rede local.

Depois de instalado no computador, podem executar tarefas sem que o usuário perceba, todas estas administradas remotamente pelo invasor, como abrir portas, criar contas de usuário, ativar ou desativar serviços, entre outras tarefas (NIEHUES, 2007).

3.2.10 Pharming

Pharming é uma atividade realizada com a intenção de redirecionar o tráfego da rede de um *site* para outro idêntico. O usuário é enganado e sem perceber fornece suas informações, como usuário e senha a um site desonesto (MICROSOFT, 2009).

O *pharming* é semelhante ao *phishing*, pois pode ser executado por correio eletrônico, porém é muito mais perigoso, uma vez que redireciona o usuário para um site falso, sem qualquer participação ou conhecimento.

Segundo Morais (2008) no *pharming* o atacante altera a correspondência entre uma *Uniform Resource Locator* (URL) legítimo e um endereço IP, de forma que a URL de um site autêntico passa a estar associada ao endereço IP de um site malicioso. Quando o usuário toma a iniciativa de utilizar a URL do site autêntico os dados são redirecionados para o site malicioso.

Os sites que mais são alvos deste ataque são os bancários, pois os criminosos tentam obter informações pessoais para ter acesso a contas bancárias, para furtarem identidades ou cometerem outros tipos de fraudes.

3.2.11 Exploits

Exploits são pequenos códigos de programas desenvolvidos com a intenção de explorarem falhas em aplicativos por erros involuntários de programação. Estes podem atacar um sistema local ou remotamente.

De acordo com Almeida (2005) como são pequenos códigos preparados para explorar vulnerabilidades muito específicas, na maioria das vezes há um *exploit* para cada tipo de aplicativo, falha ou sistema operacional. Os *exploits* podem existir como programas executáveis ou, quando usados remotamente, podem estar ocultos, como por exemplo, dentro de uma mensagem de correio eletrônico ou dentro de determinado comando de um protocolo de rede.

3.2.12 Ataques de Buffer Overflow

"As vulnerabilidades do *buffer overflow* (estouro de pilha) são criadas quando técnicas impróprias de codificação são utilizadas para executar alguma operação em um programa" (HATCH; LEE; KURTZ, 2002, p. 176).

De acordo com Niehues (2007) estes ataques são utilizados para danificar o espaço de endereçamento da memória do computador, deste modo quando o endereçamento de memória chega ao limite, o sistema consenti que os dados sejam executados como código pelo processador.

Quando a memória é excedida, o invasor pode interagir com o sistema operacional possibilitando que o sistema execute as tarefas que o invasor desejar.

3.2.13 Spyware

Spyware é uma tecnologia que reúne informações sobre uma pessoa ou computador e transmite estas informações para anunciantes, *hackers*[2] entre outros. Ele envia informações de usuários e máquinas de volta para seus servidores, dentre estas informações

[2] Pessoa interessada em testar e recondicionar qualquer tipo de sistema operacional (MCAFEE INC., 2007).

estão endereços de IP, endereços de e-mail, configurações do sistema e, em alguns casos, informações pessoais.

O *spyware* é uma classe de programa difícil de localizar, utilizada para diversos fins, tanto benignos, quando malignos. Estes programas são capazes de gravar o pressionamento de teclas, registrarem sessões de bate-papo e até mesmo registrar o conteúdo de e-mails, conforme estão sendo escritos (MCAFEE INC., 2007).

3.2.14 Adware

Adware ou *Advertising Software* (*software* de propaganda) é um tipo de *software* projetado para apresentar propagandas, por meio de um *browser* ou por meio de algum outro programa instalado em uma máquina (CERT, 2006).

Existe uma categoria de *adware* que é considerado um tipo de *spyware*, pois são projetados para monitorar os hábitos dos usuários durante o uso da Internet, direcionando assim para este usuário, as propagandas que são apresentadas.

Os *adwares* são programas que não prejudicam o sistema operacional, apenas exibem anúncios não desejados. Conforme citado em Wikipedia (2010) existem *adwares* sofisticados que são difíceis de remover, estes podem modificar registros do sistema operacional, para garantir que estas modificações não sejam desfeitas, eles somem, fazendo-se necessário reparar o registro do sistema.

3.2.15 Backdoors

Backdoors são pequenos pedaços de códigos que provocam falhas de segurança e permitem acesso ao sistema operacional. Estes códigos abrem portas de acesso ao invasor, para que este consiga executar diversas tarefas (CERT, 2006).

Os *backdoors* são abertos devido à falha no projeto dos programas ou por defeito de fabricação, podem ocorrer acidentalmente ou podem ser introduzidos propositalmente ao programa. O *backdoor* é uma forma de garantir que um invasor consiga retornar a um computador comprometido sem ser notado e sem precisar invadi-lo novamente.

Devido aos programas antivírus não serem capazes de descobrir *backdoors*, para se prevenir é preciso sempre atualizar as versões dos programas instalados no computador, este é o único meio de eliminar o problema.

3.2.16 Keyloggers e Screenlogger

Keyloggers são *softwares* capazes de capturar e armazenar as teclas digitadas pelo usuário, posteriormente criam um arquivo com estas informações que é enviado por meio da Internet. Dentre as informações capturadas podem estar textos de e-mail, logins, senhas, números de conta corrente e cartão de crédito e até mesmo dados digitados na declaração do imposto de renda (CERT, 2006).

Normalmente o *keylogger* aparece como parte de um programa *spyware* ou cavalo de tróia, fazendo-se necessário que este programa seja executado para que o keylogger se instale no computador, geralmente *keyloggers* aparecem anexados a *e-mails* ou estão disponíveis em sites da Internet.

Para evitar fraudes devido à captura de teclas digitadas, os sites passaram a exigir um grau de segurança maior, as instituições financeiras, por exemplo, desenvolveram os teclados virtuais, para que seus clientes não digitassem a senha e sim selecionassem as teclas com o mouse. Então, foram desenvolvidas técnicas mais avançadas de *keyloggers* conhecida como *screenloggers*, capazes de armazenar a posição do cursor no momento em que o mouse

é clicado e capturar a tela apresentada no monitor, isto reduz consideravelmente a segurança imposta pelos teclados virtuais (CERT, 2006).

3.2.17 Denial of Service e Distributed Denial of Service

Nos ataques de negação de serviço (*Denial of Service* - DoS) o invasor utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

Este ataque pode gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo, pode também gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível ou até mesmo tirar do ar serviços importantes, impossibilitando o acesso dos usuários (CERT, 2006).

Os ataques de negação de serviço distribuídos (*Distributed Denial of Service* - DDoS) utilizam um conjunto de computadores para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Este tipo de ataque busca ocupar toda a banda disponível para acesso a um computador ou rede, ocasionando lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede (CERT, 2006).

Muitos invasores se aproveitam da falta de conhecimento dos usuários para realizarem ataques, como por exemplo, os listados acima, explorando as vulnerabilidades de um computador ou rede e consequentemente obtendo informações confidenciais para algum fim ilícito, para garantir que seus ataques sejam bem sucedidos os invasores utilizam ferramentas que facilitam o sucesso do ataque.

A próxima seção descreve algumas das ferramentas de ataques mais comuns utilizadas para explorar falhas e invadir sistemas, todas elas estão disponíveis para download na Internet.

3.3 FERRAMENTAS DE ATAQUE

Atualmente existem diversas ferramentas de ataques[3] criadas para centenas de finalidades e sistemas operacionais. Algumas dessas ferramentas estão relacionadas a seguir:

a) **Nessus[4]:** esta ferramenta faz a inventariação remota das vulnerabilidades para sistemas *Unix*. Gera relatórios em HTML, XML, LaTeX e textos simples que mostram as vulnerabilidades detectadas;

b) **Ethereal[5]:** ferramenta de análise de protocolo para sistemas operacionais *Unix* e *Windows*. Permite observar dados capturados na rede em tempo real ou previamente capturados e guardados num arquivo ou disco;

c) **Netcat[6]:** ferramenta que analisa problemas e explora as redes utilizando os protocolos TCP e UDP. Para *Linux, Windows* e sistemas *Unix* proprietários (Solaris, IRIX, entre outros);

d) **TCPDump[7]:** ferramenta muito conhecida para análise do tráfego da rede, pode ser usada para detectar problemas, para monitorar atividades ou capturar dados na rede. Para *Linux* e sistemas *Unix* proprietários (Solaris, IRIX, entre outros);

e) **Hping2[8]:** cria e envia pacotes ICMP/UDP/TCP específicos. Possui um modo *Traceroute* e permite fragmentação de IP. Esta ferramenta é útil para descobrir o

[3] Uma lista bastante extensa pode ser obtida em *http://insecure.org/tools/tools-pt.html*.
[4] Pode ser obtida em *http://www.nessus.org*.
[5] Pode ser obtida em *http://www.ethereal.com.*
[6] Pode ser obtida em *http://www.symantec.com/business/index.jsp.*
[7] Pode ser obtida em *http://www.tcpdump.org.*

caminho de máquinas por detrás de um *firewall* e verificar se este caminho está funcionando. Disponível para *Linux* e *Unix* proprietários;

f) **Trin00[9]:** ferramenta utilizada para iniciar ataques de negação de serviço distribuídos. A vitima é infectada por uma grande quantidade de pacotes, o que ocasionará congestionamento e indisponibilidade dos serviços oferecidos a ela. Para *windows*, *Linux* e *Unix*;

g) **Brutus[10]:** ferramenta utilizada para ataques de força bruta, para *Windows*. Este programa realiza tentativas de descoberta de senhas e logins. Possui suporte a HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP e outros.

Com todas as ferramentas de ataques disponíveis hoje, é importante que os administradores de redes e até mesmo usuários da Internet, consigam diagnosticar problemas em sua rede, além de conhecer o tráfego que existe nela, para isso é possível usar Sistemas de Detecção de Intrusão, pois são baseados em sniffers.

Os sniffers utilizam uma base de dados de regras para detectar redes suspeitas. A seção seguinte descreve os tipos de sniffers existentes e seu funcionamento.

3.4 SNIFFER

O termo *sniffer* tem origem de um produto chamado *Sniffer* da Network General Corporation. Devido ao fato desta marca ter dominado o mercado, este termo popularizou-se e a partir de então, todos os analisadores de protocolo passaram a ser chamados de *sniffers* (FURMANKIEWICZ, 2000).

---

[8] Pode ser obtida em *http://www.hping.org.*
[9] Pode ser obtida em *http://software.informer.com/getfree-download-trin00.*
[10] Pode ser obtida em *http://www.hoobie.net/brutus/brutus-download.html.*

Conforme afirma Trombim (2006) *sniffer* é uma ferramenta muitas vezes vista como uma forma de “bisbilhotar” a rede, porém foi criada para auxiliar na administração destas. São utilizados para diagnosticar problemas nas redes, que apesar de imperceptíveis ao usuário, comprometem o seu desempenho.

Deste modo, *sniffer* é um programa capaz de capturar e analisar todos os pacotes que estão trafegando em uma rede.

A Figura 5 apresenta a arquitetura de um *sniffer*:

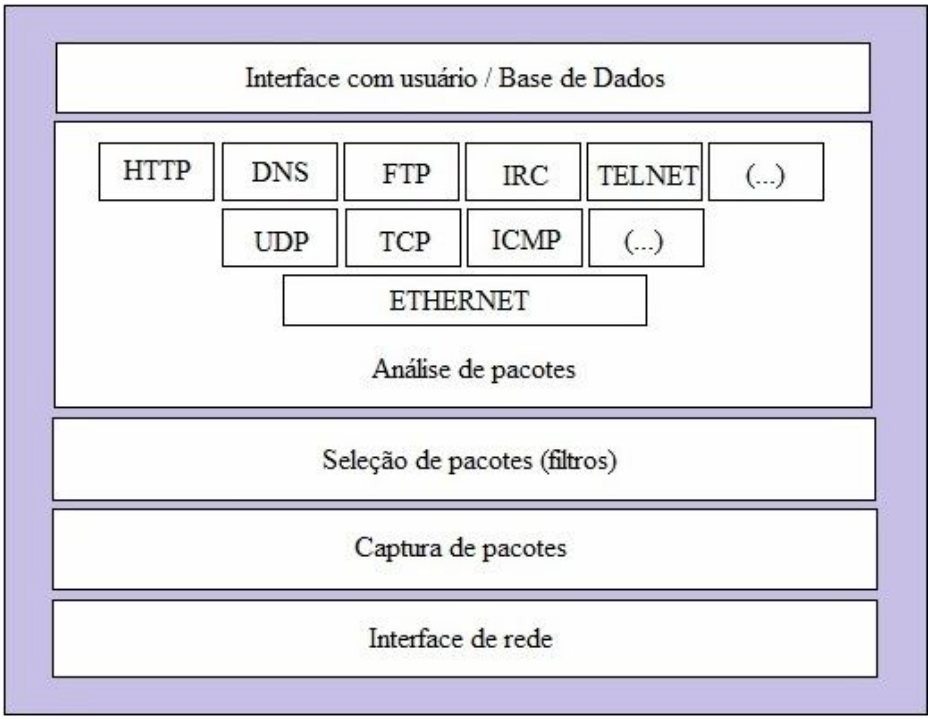


Figura 5. Arquitetura de um sniffer
Fonte: Adaptado de TROMBIM, D. (2006, p. 58)

Embora existam diversas maneiras e propósitos para a utilização de *sniffers*, o princípio de funcionamento destes continua sendo o mesmo: “capturar e analisar o tráfego da rede sem interferir no seu funcionamento” (REIS JÚNIOR; SOARES FILHO, 2002).

Para que todos os pacotes que estão trafegando em rede sejam capturados, é preciso que a placa de rede esteja em modo promíscuo, ou seja, os *hosts* “ouvem” e respondem somente a pacotes endereçados a elas, ignorando os pacotes cujo endereço físico

Media Acess Control (MAC) não seja correspondente. Uma vez que a placa de rede esteja em modo promíscuo, o *sniffer* poderá capturar e analisar qualquer tráfego que passe no segmento em que se encontra instalado (TROMBIM, 2006).

A seguir, será detalhado o funcionamento dos *sniffers*.

3.4.1 Principio de Funcionamento dos Sniffers

Toda estação pertencente a uma rede *Ethernet* possui uma interface chamada de *Network Interface Card* (NIC) e cada interface possui um endereço físico MAC de 6 bytes que a identifica na rede e é fornecido pelo fabricante. Toda comunicação na *Ethernet* é baseada neste endereço de *hardware*. A interface de rede pode ser configurada com diferentes filtros para receber ou rejeitar determinados tipos de pacotes, como por exemplo, *unicast*, *broadcast* e *multicast* (CASAGRANDE, 2003).

Ainda de acordo com Casagrande (2003) os *hosts* da rede “ouvem” e estão aptos a responder apenas a pacotes endereçados a eles, pois uma interface *Ethernet* em funcionamento normal ignora todo o tráfego da rede que não seja destinado a ele. Portanto, o *host* descarta todo pacote que contenha endereço MAC não direcionado a este. Como na rede Ethernet todos os *hosts* compartilham o mesmo meio é possível configurar uma interface para que capture todos os pacotes, independente do direcionamento do mesmo. Consequentemente todo *host* apresenta condições de monitorar e capturar o tráfego da rede, ignorando o endereço de destino. Conforme ilustra a Figura 6.

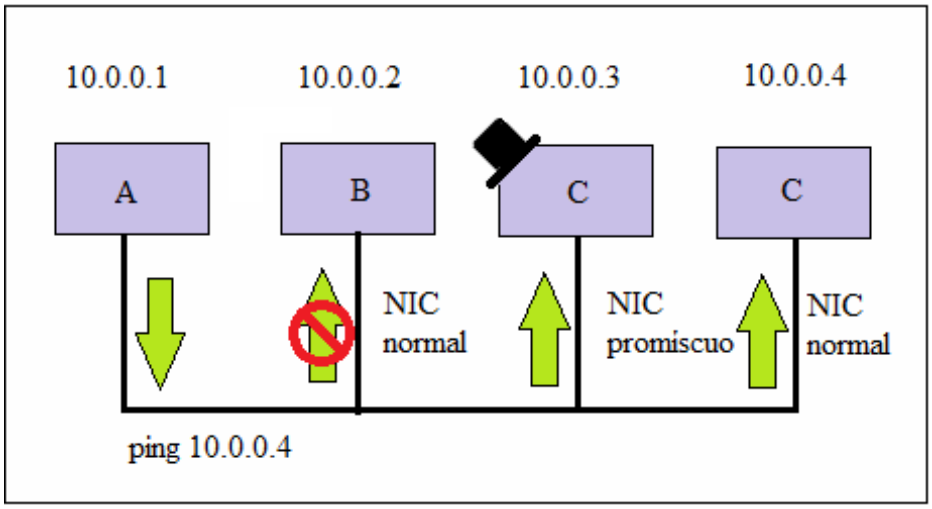


Figura 6. Filtro de hardware
Fonte: Adaptado de CASAGRANDE, R. (2003, p. 26)

Existem muitos tipos de *sniffers*[11], alguns dos tipos mais comuns são listados na próxima seção.

3.4.2 Tipos de Sniffers

Atualmente existem diversos *softwares sniffers* desenvolvidos com diversas finalidades e para muitos sistemas operacionais. Casagrande (2003) cita que os mais utilizados em sistemas operacionais *Windows*, *Linux* e alguns para *Unix* são:

a) **Ethereal**[12]**:** esta ferramenta possibilita identificar rapidamente qualquer tipo de *trojan*, *spyware* ou acesso não autorizado, possibilitando o controle de tudo que entra e sai de uma máquina. Para ambientes *Windows* e *Unix*;

b) **Snort**[13]**:** é um sistema de detecção de intrusão gratuito, portado para mais de 10 plataformas diferentes, possui funções *sniffer*;

[11] Uma lista bastante extensa pode ser obtida em *http://packetstormsecurity.nl/sniffers.*
[12] Pode ser obtido em *http://www.ethereal.com.*
[13] Pode ser obtido gratuitamente em *http://www.snort.org/start/download.*

c) **Sniffit**[14]**:** este *sniffer* permite capturar sessões de serviços completas, ou seja, qualquer dado que trafegue entre cliente e servidor em tempo real. Para ambientes *Windows* e *Unix*;

d) **Hunt**[15]**:** este *software* pode receber pacotes da rede, modificá-los e recolocá-los novamente na rede. Permite o *sniffing* em redes com *switches*. Para ambientes *Linux* e *Unix*;

e) **BlackICE Pro**[16]**:** um *sniffer* local e não promíscuo. Para ambiente *Windows*;

f) **Kismet**[17]**:** este sniffer permite monitoramento de todo o tráfego recebido de rede *Wireless*. Captura pacotes de redes dos tipos: 802.11a, 802.11b e 802.11g. Funciona com sistemas operacionais *Linux*, *Unix* e existe um cliente para *Windows*, porem é necessário usar um servidor externo;

g) **Trinux**[18]**:** esta ferramenta possui o *tcpdump* e o *sniffit* entre outros utilitários e cabe em um disquete inicializável. Disponível para sistemas operacionais *Linux* e *Unix*.

Sniffers são *softwares* muito úteis. A sua utilidade é tão grande que até mesmo os Sistemas de Detecção de Intrusão, como por exemplo, o Snort, são feitos com base em *sniffers, pois* capturam informações para verificar possíveis anomalias. A próxima seção descreve sobre os IDSs, suas características, classificação, métodos de detecção entre outras informações.

[14] Pode ser obtido em *http://sniffit.sourceforge.net*.
[15] Pode ser obtido em *http://www.cri.cz/kra/index.html.*
[16] Pode ser obtido em *http://www.networkice.com.*
[17] Pode ser obtido em *http://kismetwireless.net.*
[18] Pode ser obtido em *http://www.trinux.org.*

4 SISTEMAS DE DETECÇÃO DE INTRUSÃO

Sistemas de Detecção de Intrusão (*Intrusion Detection System* - IDS) são sistemas de *software* ou *hardware* que monitoram eventos ocorridos em um sistema computacional, auxiliando na procura de indícios de problemas de segurança em redes de computadores (SANTOS, 2005).

A ferramenta IDS de *hardware* é um dispositivo independente instalado e configurado, normalmente é de uso proprietário ou comercial, podendo ser um *firewall*[19] ou *proxy*[20], dependendo do fabricante. A ferramenta IDS de *software* é executada em conjunto em *firewalls* ou *proxies*, podendo ser de uso proprietário ou gratuito. Ambas as ferramentas podem trabalhar independente de *firewall* ou *proxies* (VIEIRA JUNIOR, 2002).

De acordo com Bace 2001, Intrusão é uma tentativa de comprometer a confidencialidade, integridade e disponibilidade ou burlar mecanismos de segurança de um sistema computacional.

A utilização de uma ferramenta IDS permite analisar tentativas de ataques e auxilia na segurança de redes de computadores. Por meio desta análise é possível descobrir de onde está partindo a invasão, podendo-se assim, bloquear a comunicação com a origem, evitando uma possível invasão.

Conforme Vieira Junior (2002) o IDS detecta e notifica tentativas de invasão, por meio da captura e análise dos pacotes que estão trafegando na rede, procurando identificar evidências do andamento de um ataque, para posteriormente emitir alarmes ou executar uma ação automática.

---

[19] Firewall é um dispositivo que aplica uma política de segurança a um determinado ponto de controle da rede (VIEIRA JUNIOR, 2002).

[20] Proxy é um serviço que oferece o acesso à Internet para uma rede local, gerenciando o tráfego de informações, e armazenando páginas da Internet tornando o acesso mais rápido e confiável (VIEIRA JUNIOR, 2002).

Os IDSs possuem muitas características, a próxima seção apresenta as características mais importantes e desejáveis.

4.1 CARACTERÍSTICAS DESEJÁVEIS

Segundo Casagrande (2003) e Militelli (2006) os IDSs possuem algumas características desejáveis dentre as quais se podem destacar:

a) executar continuamente com o mínimo de supervisão humana;
b) ser tolerante a falhas, sendo apto a se recuperar de panes acidentais ou causadas por atividades maliciosas. Depois de reiniciado um IDS deve ser apto a recuperar seu estado imediatamente anterior à falha;
c) ser apto a monitorar a si mesmo e detectar se ele foi alterado por um atacante;
d) impor uma mínima sobrecarga no sistema onde está sendo executado, não interferindo na operação normal do sistema;
e) ser configurável para permitir implementar políticas de segurança do sistema que está sendo monitorado;
f) ser adaptável a mudanças no sistema e características de usuário. Por exemplo, novas aplicações sendo instaladas, usuários mudando de atividade ou novos recursos disponíveis podem causar mudanças nos padrões;
g) ser escalável para monitorar um grande número de estações, provendo resultados de maneira rápida e eficaz;
h) causar leve degradação do serviço. Se algum componente do IDS pára de executar por qualquer razão, o restante do sistema deve ser afetado minimamente;

i) permitir reconfiguração dinâmica, permitindo que o administrador faça mudanças na configuração sem a necessidade de reiniciar o sistema;

j) ser difícil de enganar.

4.2 PRINCIPAIS TIPOS DE IDS

Existem muitos tipos de IDSs, caracterizados por análise e monitoramentos distintos, cada um com suas vantagens e desvantagens. Contudo eles podem ser descritos em função de três componentes funcionais essenciais (BACE, 2001):

a) **Fontes de Informação:** são usadas para definir se um ataque ocorreu ou não. Podem ocorrer em diferentes níveis do sistema, rede, host e aplicação.

b) **Análise:** organiza e classifica os eventos provenientes da fonte de informação, decidindo quais eventos mostram que uma intrusão ocorreu. Os tipos são detecções por mau uso e anomalia.

c) **Resposta:** são as ações que o sistema executa quando detecta uma intrusão. São agrupadas em medidas ativas e passivas.

4.2.1 Classificação Quanto à Fonte de Informação

IDSs podem ser agrupados segundo sua fonte de informação. Eles analisam estas fontes de informação geradas pelo sistema operacional ou pela aplicação a procura de sinais de intrusão.

Alguns IDSs têm a sua arquitetura baseada segundo a localização, podendo ser Centralizados e Distribuídos. “Um IDS Centralizado é aquele onde a análise dos dados é feita em um número fixo de locais, independente de quantas estações estão sendo monitoradas”

(CASAGRANDE, 2003, p. 21). E um IDS Distribuído é aquele onde a análise dos dados é efetuada em um número de locais igual ao número de estações que está sendo monitorada.

4.2.1.1 IDS Baseado em Host

Os sistemas de Detecção de Intrusão de Host (HIDS) atuam sobre informações coletadas em estações individuais (CERT, 2009).

De acordo com Malta (2006) HIDS analisam com grande precisão atividades, determinando exatamente que usuários e processos estão envolvidos em um determinado ataque, pois podem acessar e monitorar diretamente os dados e processos do sistema que são alvos de ataques.

Laufer (2003) cita que o funcionamento destes sistemas acontece por meio da procura de atividades incomuns em acessos a arquivos, tentativas de login, alterações em privilégios do sistema entre outros. Após, os dados originados em uma máquina que hospeda um serviço são coletados e analisados. Os dados podem ser analisados localmente, ou enviados para uma máquina remota.

IDSs baseados em host podem atuar em muitas áreas dentro de uma mesma máquina. Tendo sua atuação baseada em detecção por anomalia, ou seja, executam operações para detectar se o comportamento é normal ou não (MALTA, 2006).

Conforme Barbosa (2000) e Malta (2006) HIDS possuem as seguintes vantagens:

a) em muitas circunstâncias podem dizer com precisão o que o intruso fez;
b) podem detectar ataques que não são detectados por um IDS baseado em rede, pois monitoram eventos locais;
c) não são afetados por redes com *switches*;
d) menor risco de uma configuração errada ser realizada;

e) menor número de falsos positivos do que o IDS baseado em rede;

f) mais difícil de ser enganado.

Ainda de acordo com Barbosa (2000) e Malta (2006) os HIDS apresentam como desvantagens:

a) para cada host monitorado deve ser instalado e configurado um IDS, tornando difícil seu gerenciamento;

b) podem ser desativados com alguns tipos de ataques DoS;

c) apenas monitoram uma máquina, pois possuem visão extremamente localizada;

d) utilizam recursos computacionais da própria estação que está sendo monitorada, afetando no desempenho do sistema;

e) não são próprios para monitorar varreduras de rede, pois somente analisam pacotes recebidos pela própria estação.

4.2.1.2 IDS Baseado em Rede

Os Sistemas de Detecção de Intrusão de Rede (NIDS) detectam ataques por meio da captura e análise de pacotes da rede. Monitoram todo o tráfego afetando múltiplas estações que estão conectadas ao segmento de rede, protegendo estas estações (CERT, 2009).

Um IDS baseado em rede consiste em um conjunto de sensores ou estações colocados em vários pontos de uma rede. Estes sensores monitoram o tráfego da rede, executando uma análise local e respondendo a indícios de ataques para uma central de gerenciamento (NORTHCUTT et al, 2003).

NIDS possuem dois componentes:

a) **sensores:** colocados em distintos seguimentos de rede, nos quais se deseja monitorar;

b) **estação de gerenciamento:** recebe os alarmes dos sensores, informando ao administrador, possui uma interface gráfica.

Conforme Barbosa (2000) e Malta (2006) NIDS possuem as seguintes vantagens:

a) poucos IDSs instalados, mas bem posicionados podem monitorar grandes redes;
b) pode ser bastante eficiente contra ataques a ainda ser invisível para muitos atacantes;
c) detectam acessos sem autoridade e com excesso desta;
d) não afeta diretamente o sistema computacional onde está instalado;
e) não há necessidade de alterações em servidores ou em quaisquer outras máquinas.

Ainda de acordo com Barbosa (2000) e Malta (2006) os NIDS apresentam como desvantagens:

a) em períodos com alto tráfego, um NIDS pode ter dificuldade de processar todos os pacotes de uma grande rede, podendo falhar em reconhecer um ataque iniciado;
b) não consegue monitorar tráfego em sessões encriptadas;
c) inadequado para tratar ataques mais complexos;
d) grandes quantidades de dados podem trafegar entre os agentes e estações de gerência.

4.2.1.3 IDS Baseado na Aplicação

De acordo com Casagrande (2003) este tipo de IDS baseado na aplicação é um subconjunto especial dos IDSs baseado em host, estes analisam eventos tendo como base o

software de aplicação. Suas fontes de informações são os arquivos de *logs* de transações. IDSs baseados na estação detectam comportamento suspeito e também usuários que excederam seus limites devido a habilidade de interagir diretamente com o *software*, com domínio ou conhecimento específico da aplicação incluídos no processo de análise. Ainda segundo Casagrande (2003) IDSs baseado na aplicação apresentam as seguintes vantagens:

a) monitora a interação entre o usuário e a aplicação, o que permite detectar atividades não permitidas para cada usuário;
b) executam em ambientes cifrados, pois sua interface com a aplicação é feita por troca de informações não cifradas.

E Casagrande (2003) cita as seguintes desvantagens para IDSs baseados na aplicação:

a) devido ao fato de monitorarem eventos em nível de usuário, não detectam alguns ataques com ferramentas, como por exemplo, cavalos de tróia;
b) podem ser mais vulneráveis a ataques que os IDSs baseados em host.

4.2.2 Classificação Quanto a Análise

As técnicas ou métodos de detecção de intrusão que analisam os dados que são coletados pelo IDS podem ser classificados em dois grupos: Análise da detecção de intrusão baseada em assinaturas e Análise da detecção de intrusão baseada em anomalias.

4.2.2.1 Análise da Detecção de Intrusão Baseada em Assinatura

A detecção baseada em assinatura tem como objetivo identificar ações ou assinaturas suspeitas. Não existe nenhuma forma de identificar assinaturas de mau uso, a detecção é feita por meio de intrusões e vulnerabilidades conhecidas.

Malta (2006) cita que esta análise se baseia na forma de padrões, ou seja, esta técnica busca sequências de ações que são claramente caracterizadas como inválidas registradas em uma base de dados que contém um conhecimento acumulado sobre ataques específicos e vulnerabilidades do sistema.

Ainda de acordo com Malta (2006) esta técnica de detecção é muita utilizada, pois não possui um custo computacional elevado, não interferindo no desempenho do sistema, apresentando as seguintes vantagens:

a) geram um número pequeno de alarmes falsos;
b) diagnosticam de forma rápida e eficiente, uma ferramenta ou técnica de ataque;
c) permitem rastrear problemas de segurança no sistema, iniciando procedimentos de tratamento de incidentes;
d) mesmo com grandes bases de assinaturas, possui melhor desempenho.

A detecção baseada em assinatura apresenta as seguintes desvantagens de acordo com Malta (2006):

a) detectam somente ataques conhecidos e devem ser atualizados constantemente;
b) detectores deste tipo analisam poucas variações de assinaturas para detectar as variantes de ataques comuns;
c) dificuldade em detectar abusos de privilégios.

4.2.2.2 Análise da Detecção de Intrusão Baseada em Anomalia

Esta técnica também é conhecida como técnica de detecção por observação do comportamento, pois consiste na observação de como o sistema se comporta, auxilia na identificação de desvios estatísticos, comparando às métricas de comportamento consideradas padrão (MALTA, 2006).

Os detectores de anomalias identificam um procedimento anormal em uma estação ou rede. Eles assumem que os ataques são diferentes das atividades normais e são detectados pelo sistema que identifica essas diferenças (CERT, 2009).

Detectores de anomalias coletam históricos em um período de operação normal para posteriormente construírem modelos de usuários, estações e conexões de rede com comportamentos considerados normais.

Segundo Tavares (2002) para detectar anomalias os detectores coletam dados de eventos e usam diversas medidas para determinar que alguma atividade desviou-se do modelo de comportamento padrão.

Devido a grande variação nos padrões do usuário e comportamento do sistema, um grande número de alarmes falsos pode ser gerado.

A detecção baseada em anomalia apresenta as seguintes vantagens CERT (2009):

a) detectam comportamentos anormais;
b) produzem informações que podem ser usadas para definir assinaturas para um detector por mau uso.

Ainda conforme o Cert (2009) a detecção baseada em anomalia apresenta as seguintes desvantagens:

a) produzem um número grande de alarmes falsos;
b) para formarem um padrão de comportamento normal precisam de um extenso conjunto de registros de eventos do sistema.

4.2.3 Classificação Quanto a Resposta

A partir do momento que os IDSs conseguiram as informações sobre os eventos e os analisaram procurando sintomas de ataques, se alguma tentativa de intrusão for detectada, alertas são enviados, podem haver dois tipos de respostas: Ativas e Passivas.

4.2.3.1 Respostas Ativas

Conforme Casagrande (2003) respostas ativas são ações geradas pelo próprio sistema quando uma intrusão é detectada. Existem três categorias de respostas ativas:

a) **coletar informação adicional:** nos IDSs a forma de coletar informações adicionais seria aumentar o número de eventos de *logs*, capturando todos os pacotes, ao invés de determinada porta ou sistema. Coletar estas informações auxilia na detecção do ataque, na investigação sobre a origem do ataque e posteriormente dá suporte às medidas legais, civis e criminais;

b) **mudança do ambiente:** interromper um ataque em progresso e bloquear novos acessos pelo atacante também é uma resposta ativa. Bloquear um acesso específico de um usuário não é uma característica típica dos IDSs, mas é possível bloquear o endereço IP utilizado pelo atacante;

c) **atitudes contra o atacante:** alguns pesquisadores acreditam que uma forma de resposta ativa é tomar uma iniciativa contra o atacante, ou seja, disparar ataques contra o invasor ou tentar obter informações relevantes sobre a estação ou localização do invasor. Contudo, além de ilegal, os atacantes costumam usar endereços falsos para realizarem seus ataques.

4.2.3.2 Respostas Passivas

Nas respostas passivas são gerados relatórios para que o administrador do sistema, baseado nestas informações, possa tomar as medidas que julgar necessárias. Respostas passivas podem ser divididas em:

a) **alarmes e notificações:** IDSs geram alarmes e notificações para informar aos responsáveis pelo sistema quando um ataque é detectado. As notificações podem variar de mensagens simples até mensagem bem detalhadas contendo IP fonte e destino, ferramenta utilizada para o ataque e caminho percorrido. IDSs também podem enviar notificações remotas, para telefones celulares, *pagers* e e-mail;

b) **interrupções SNMP e plugins:** alguns IDSs são projetados para, a partir da utilização de interrupções SNMP gerar alarmes e alertas e postar estes alertas em uma central de gerenciamento de rede, onde poderão ser vistos pelo administrador da rede;

c) **relatórios e arquivos:** muitos dos IDSs, principalmente os comerciais, geram relatórios com informações detalhadas sobre o tráfego da rede, os relatórios podem ser semanais, mensais, outros em formato próprio para inclusão em sistemas de banco de dados.

4.3 FALSOS POSITIVOS E FALSOS NEGATIVOS

De acordo com Malta (2006) os maiores problemas enfrentados hoje com relação à detecção de intrusão, não levando em consideração as Vulnerabilidades, são os Falsos Positivos e Falsos Negativos.

Os Falsos Positivos ocorrem quando o sensor do IDS gera um alerta que não existe, ou seja, pacotes são identificados pela ferramenta de segurança como uma tentativa de ataque, quando na verdade se trata de uma ação legítima. Um número grande de falsos positivos pode ser causado pela má configuração do IDS, ao examinar o arquivo de registros de eventos o administrador percebe a quantidade de alertas gerados, e pode chegar à conclusão que o sistema está sendo atacado, quando na verdade estes alertas são falsos (MALTA, 2006).

Os Falsos Negativos ocorrem quando tentativas autênticas de ataques não são alertadas, ou seja, o sensor do IDS não gera nenhum alerta. Algumas das causas que podem gerar falsos negativos são: ataques desconhecidos, sobrecarga ou configuração errada do sensor. Falsos Negativos não devem ocorrer, pois pode ser um ataque que passa despercebido pelo IDS e pode comprometer a segurança da rede ou das informações contidas nos sistemas computacionais (CERT, 2009).

4.4 FREQUÊNCIA DE USO

Um sistema baseado na forma de frequência de uso, caracteriza-se por estar em contínuo monitoramento ou *online* (em tempo real), ou seja, procura uma invasão no momento do ataque (MALTA, 2006).

A análise periódica realizada com os dados armazenados durante um período de tempo de uso do sistema é caracterizada por ser *offline*, ou seja, a análise procura uma invasão depois de já ter ocorrido o ataque.

4.5 NECESSIDADE DE IDS SEGURO

"Um sistema de computação deverá prover confidencialidade, integridade e garantia contra negação de serviço" (MALTA, 2006), porém, com o aumento da conectividade e a grande quantidade de aplicações financeiras realizadas na Internet, cria-se um cenário mais propenso a intrusões.

Um intruso que tem interesse em uma rede e suspeita da existência de um IDS, sua primeira ação será realizar um ataque à máquina no qual o IDS está sendo executado, desabilitando ou reconfigurando-o para que este não identifique suas ações maliciosas, "se isto não fosse possível, ele poderia utilizar técnicas de construção de pacotes para que o IDS não consiga identificar corretamente suas ações" (BARBOSA, 2000, p.42).

As empresas mantêm o código fonte fechado na comercialização de *softwares*, ou seja, há uma confiança por parte do usuário, pois este não sabe se o *software* desempenha com eficiência o seu papel. Com o *software* livre, além de o código ser aberto, existe a possibilidade de revisão ou até mesmo alteração por outras pessoas. A desvantagem é que a descoberta de uma falha torna-se mais simples.

"A escolha, instalação e configuração de um IDS devem ser feitas com o máximo de cuidado, estudando diversas possibilidades que propiciem flexibilidade e segurança associadas" (BARBOSA, 2000, p. 43).

Para que a escolha seja feita da melhor forma possível é necessário conhecer alguns dos *softwares* de detecção de intrusão, a próxima seção apresenta alguns exemplos destes *softwares*.

4.6 EXEMPLOS DE IDS

Esta seção fala sobre alguns dos IDSs, identificado em cada ferramenta as suas principais características.

4.6.1 Snort

O Snort é uma ferramenta baseada em rede, desenvolvida por Martin Roesch, seu código é open-source. Esta ferramenta é bastante conhecida devido a fácil configuração de regras e constante atualização no banco de dados de assinaturas. O Snort é leve, pequeno, realiza escaneamentos e verifica anomalias dentro de toda a rede ao qual um computador está inserido (SNORT, 2009).

São recomendados para escanear redes TCP/IP pequenas, pode detectar uma grande variedade de tráfegos suspeitos, bem como ameaças externas, fornecendo informações que auxiliam na tomada de decisão de administradores.

O Snort habilita a placa de rede do computador, onde está configurado, para o modo *promíscuo*, capturando todos os pacotes que trafegam naquele segmento de rede. Utiliza assinaturas de ataques conhecidos como regras para descobrir uma variedade de ataques e sondagens, como por exemplo, Portscan.

De acordo com Malta (2006) a estrutura básica do Snort é baseada na captura de pacotes na rede por meio da biblioteca *Winpcap*[21] e em um analisador eficiente e simples que trata informações do cabeçalho e da área de dados dos pacotes coletados.

Conforme Santos (2005) existem quatro elementos básicos que compõem o Snort: o farejador, o pré-processador, o mecanismo de detecção e os *plugins* de saída. Basicamente,

[21] Biblioteca necessária para funcionamento do Snort na plataforma Microsoft Windows (MALTA, 2006).

o Snort é um farejador de pacotes, projetado para pré-processar os pacotes capturados e posteriormente comparar esses pacotes com uma série de regras.

a) **farejador:** o tráfego da rede é obtido por meio da biblioteca *Winpcap.* Ao passar pelos mecanismos de detecção, a estrutura dos pacotes é montada para os protocolos de enlace, “os quais são ainda mais decodificados para os protocolos de nível mais alto, como as portas TCP e UDP” (SANTOS, 2005, p. 33);

b) **pré-processador:** após, os pacotes passam por um conjunto de pré-processadores onde são examinados e encaminhados ao mecanismo de detecção. Cada pré-processador analisa se o pacote deve ser examinado, modificado ou alertar a seu respeito;

c) **mecanismo de detecção:** No mecanismo de detecção os pacotes são verificados em relação às regras listadas no arquivo do Snort;

d) **plugins de saída:** A saída dos alertas do mecanismo de detecção, dos pré-processadores ou do farejador é produzida pelo Snort.

A Figura 7 apresenta a arquitetura do Snort:

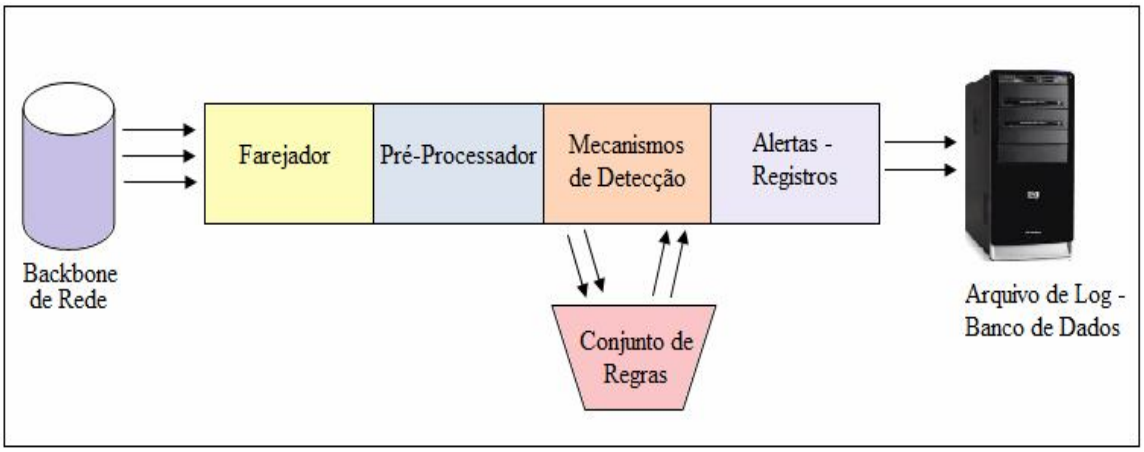


Figura 7. Arquitetura do Snort
Fonte: Adaptado de VIEIRA JUNIOR, F. (2002, p. 4)

4.6.1.1 Requisitos para Instalação do Snort

O Snort pode ser instalado em mais de dez plataformas diferentes, porém para ser instalado no Windows ele precisa de uma biblioteca chamada *Winpcap*. Para trabalhar com o *Basic Analysis and Security Engine* (BASE), ferramenta para navegação e análise de dados do Snort armazenados em um banco de dados, é necessário o uso de um Sistema de Gerenciamento de Bando de Dados (SGBD), podendo ser *MySQL* ou *PostgreSQL*. É necessário também um servidor Web, como por exemplo, o *Apache*, pois possui suporte a *PHP*[22], devido aos *scripts* da BASE serem escritos em *PHP* (MALTA, 2006).

4.6.2 Bro

Esta ferramenta IDS foi desenvolvida pelo Laboratório Nacional de Lawrence Livermore, nos Estados Unidos. É semelhante ao Snort, sendo de rede e baseado em assinatura. Este IDS possui uma linguagem própria para especificar ataques, parecida com a linguagem C. O Bro mantém uma lista com o número de acessos de cada máquina em cada porta no servidor, se esse número de acessos for bastante alto, um alerta é disparado (KONRATH, 2001).

De acordo com Malta (2006) o Bro possui implementações em FreeBSD, Solaris, SunOS e Linux. Pode ser dividido em dois componentes: uma máquina de eventos e um interpretador de *scripts*. A máquina de eventos é responsável por reduzir um fluxo de dados anteriormente filtrado e o interpretador de *scripts* processa a linguagem que descreve as políticas de segurança.

[22] Linguagem de programação de computadores MALTA (2006).

5 TRABALHOS CORRELATOS

Esta seção relaciona alguns dos trabalhos científicos com teor semelhante a esta fundamentação teórica utilizados no desenvolvimento deste trabalho de pesquisa.

5.1 DETECÇÃO DE INTRUSÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso de Marcelo Alvim Malta, para obtenção do grau de bacharel em Ciência da Computação, em 2006, pela Universidade Estadual de Londrina – UEL, no estado do Paraná.

O trabalho apresenta os principais conceitos sobre a detecção de intrusão em rede de computadores e realiza um estudo sobre as tecnologias usadas na detecção de intrusão apresentando alguns dos IDSs disponíveis para realização desta detecção.

5.2 AMEAÇAS DIGITAIS: UM ESTUDO DOS RISCOS ENVOLVIDOS NO USO DA INTERNET, SEUS IMPACTOS E FORMAS DE PROTEÇÃO

Trabalho de Conclusão de Curso de Lucas Urgioni Niehues, para obtenção do grau de bacharel em Ciência da Computação, em 2007, pela Universidade do Extremo Sul Catarinense – UNESC, no estado de Santa Catarina.

O trabalho apresenta um estudo das principais ameaças digitais existentes e as formas de proteção, para demonstrar as formas de proteção foi realizada uma simulação de ataque utilizando técnicas de captura de informações, além de uma pesquisa de campo demonstrando o grau de instrução e conhecimento dos usuários com relação ao uso da Internet.

5.3 TÉCNICAS DE DETECÇÃO DE SNIFFERS

Dissertação de Mestrado apresentada em 2003 por Rogério Antônio Casagrande, pela Universidade Federal do Rio Grande do Sul – UFRGS, para obtenção do grau de Mestre em Ciência da Computação, no estado do Rio Grande do Sul.

O trabalho apresenta uma visão geral sobre os Sistemas de Detecção de Intrusão, com suas vantagens e desvantagens para cada tipo de IDS. A seguir, é apresentado o IDS *Asgaard*, desenvolvido pelo grupo de segurança da UFRGS. Também são discutidos os *sniffers*, técnicas de detecção de *sniffers* de forma local e remota e os cenários que se aplicam cada técnica. São apresentadas as ferramentas para realizar a detecção de *sniffers* e a avaliação de cada técnica adotada para este fim.

5.4 DETECÇÃO DE INTRUSOS UTILIZANDO O SNORT

Monografia de Bruno Ribeiro dos Santos apresentada como requisito das exigências do curso de Pós-Graduação, para obtenção do título de especialista em Administração de redes Linux apresentada em 2005 pela Universidade Federal de Lavras - UFLA em Minas Gerais.

Este trabalho apresenta conceitos relacionados à segurança da informação, abordando os tipos de ataques mais comuns. Apresenta a ferramenta de detecção de intrusão Snort e descreve o seu funcionamento, componentes, entre outros. O autor realiza um teste de eficiência com o Snort utilizando as ferramentas de invasão *Nmap* e *Nessus*.

6 UTILIZAÇÃO DA FERRAMENTA SNORT NA DETECÇÃO DE IMINÊNCIAS DE ATAQUES MAIS CONHECIDOS

Este trabalho tem como objetivo analisar e descrever os resultados obtidos por meio de um estudo realizado com alguns tipos de ataques conhecidos e com o auxílio da ferramenta de detecção de intrusão baseada em rede, o Snort, visando detectar se o uso desta ferramenta é eficiente e auxilia na detecção de intrusos nas redes de computadores, para isto algumas etapas metodológicas foram seguidas.

As etapas realizadas da metodologia para a elaboração do trabalho constituíram-se de levantamento bibliográfico, onde foi utilizada a busca em livros, revistas online, sites e trabalhos científicos com conteúdos referentes à fundamentação teórica.

A segunda etapa constituiu-se de um estudo sobre o funcionamento das redes e alguns requisitos de como obter uma comunicação um pouco mais segura, para isso foi necessário leituras em livros, pesquisas na Internet. Foram estudados temas como criptografia, norma ABNT NBR/ISO IEC 27002 e políticas de segurança dentro das empresas.

A terceira etapa foi realizada buscando conteúdo em sites, fóruns, livros, trabalhos científicos, que fornecessem algum conhecimento sobre a atuação de sistemas de detecção de intrusão nas redes de computadores, foi estudado sobre seu funcionamento, forma de captura de pacotes e detecção de ameaças e tipos de IDSs disponíveis.

6.1 CENÁRIO UTILIZADO PARA REALIZAÇÃO DOS TESTES DE EFICIÊNCIA COM O SNORT

Para que este trabalho fosse realizado, foram utilizados os seguintes softwares:

a) Sistema Operacional XP Professional (Service Pack 3);

b) WinPcap 4.1.2;

c) IDS Snort 2.9.0.4;

d) MySQL 5.5.9;

e) AdoDB 5.1.1;

f) PHP 5.2.17;

g) Apache 2.2.17;

h) Basic Analysis and Security Engine (BASE) 1.4.5;

i) EventSentry 2.91.0.110.

Para realização dos testes foi utilizado um *hub*, conforme ilustra a Figura 8:

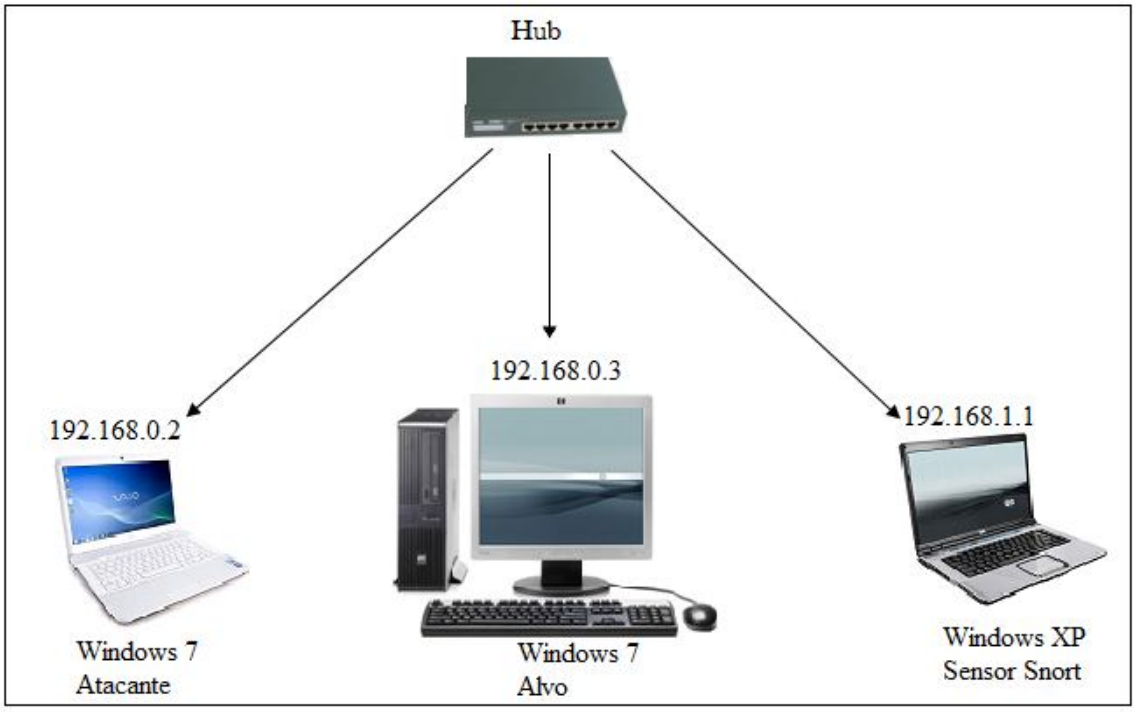


Figura 8. Ambiente Montado para Realização dos Testes

Montada a arquitetura, é necessário instalar a WinPcap, biblioteca padrão do Snort para Windows, que habilita a placa de rede em modo promíscuo para realizar a captura de pacotes da rede.

Para que o IDS funcione corretamente é necessário um Sistema de Gerenciamento de Bando de Dados (SGBD) para armazenar os dados capturados e assim, monitorar os *logs*.

Em seguida o Snort foi instalado e configurado para que capture todos os pacotes cuja origem ou destino seja os *hosts* da rede que será analisada. Para que isso seja possível é necessário realizar alterações no arquivo “snort.conf”. A seguir parte da configuração utilizada para definir qual rede o Snort ira analisar (mais detalhes no apêndice A):

```
#var HOME_NET any
var HOME_NET 192.168.0.0/24
```

E para que o Snort analise somente a própria rede, é necessário inserir a linha abaixo:

```
#var EXTERNAL_NET any
var EXTERNAL_NET $HOME_NET
```

O AdoDB foi instalado, pois é uma biblioteca orientada a objetos escrita em PHP, que constitui uma camada de abstração para interação do PHP com o MySQL. O PHP também instalado é uma linguagem de *scripts* amplamente utilizada para fins gerais que o BASE utiliza.

A seguir, o Apache foi instalado, pois a ferramenta BASE necessita de um servidor *Web* para funcionar.

O BASE é um conjunto de *scripts* PHP que fornece uma interface entre um navegador Web e o banco de dados MySQL, trabalhando com alertas armazenados no banco de dados. Através do BASE é possível obter informações estatísticas de alertas, possibilitando a descoberta de números de acessos dividido por protocolo, por porta de origem e destino, entre outras informações. A Figura 9 exibi a tela principal, apresentando dados como, o número de alertas, porta de origem e destino, protocolos e outras informações do BASE.

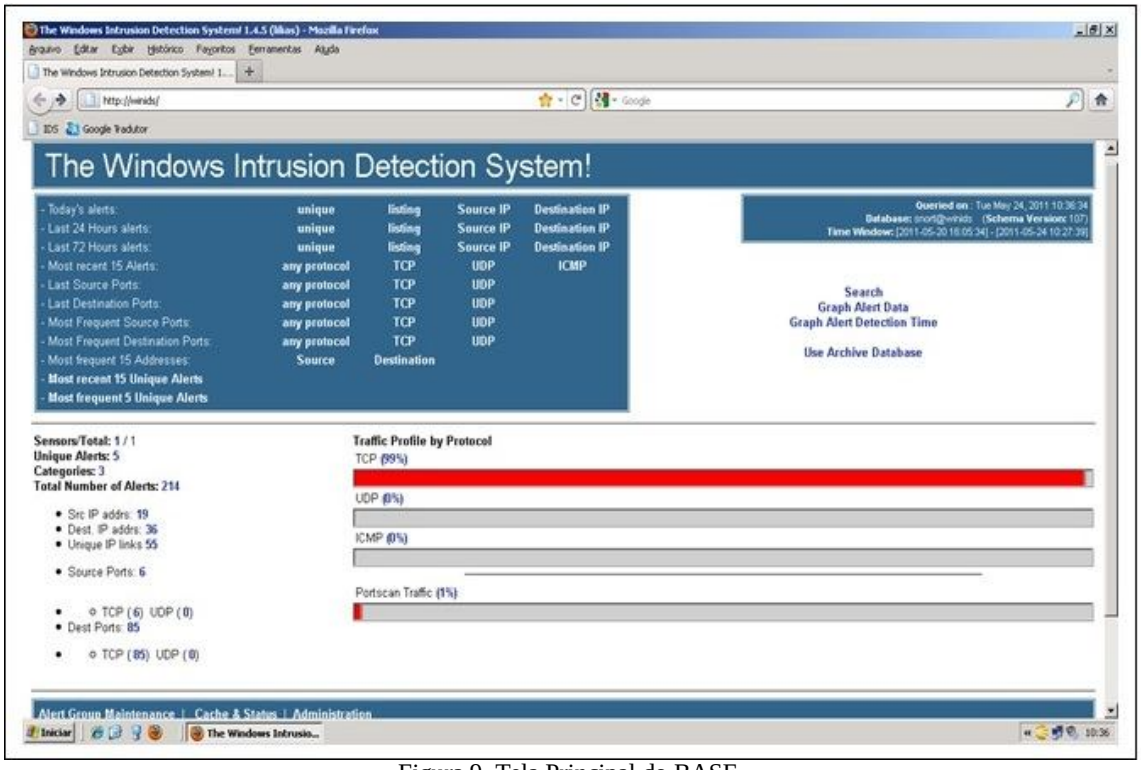


Figura 9. Tela Principal do BASE

E por fim, o EventSentry foi instalado para que os eventos gerados pelo Snort que ficam armazenados no Windows sejam apresentados no formato sonoro, pop-up, e enviados para uma conta de e-mail.

Para um melhor entendimento a Figura 10 apresenta a ordem de instalação e dependência dos softwares utilizados:

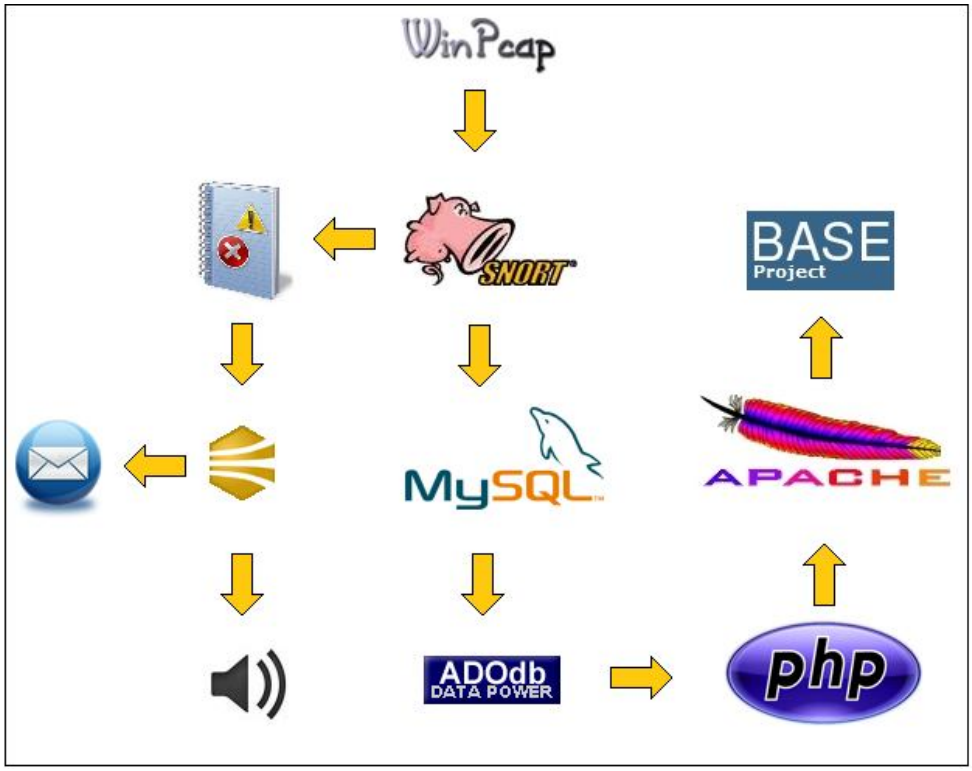


Figura 10. Ordem de Instalação dos Softwares Requeridos

Para realização dos testes foram utilizadas as ferramentas Nmap e Brutus. O Nmap é um *software* livre que realiza Portscan, ou seja, desempenha uma varredura de portas e serviços. Sendo muito utilizado para analisar a segurança de um computador, detectando quais serviços estão rodando no mesmo. O Brutus é um *software* que realiza ataques de força bruta, ou seja, este software realiza varreduras para obter login e senha de usuários. O Brutus possui suporte para os protocolos: HTTP, FTP, POP3, TELNET, SMB.

6.2 TESTE DE EFICIÊNCIA DO SNORT UTILIZANDO A FERRAMENTA NMAP

A etapa de teste se inicia instalando a ferramenta Nmap para realizar a tentativa de Portscan. Em seguida para que o IDS apresente um bom funcionamento deve-se configurar o Snort para que fique executando como um serviço, pois uma vez desativado, uma tentativa de

invasão pode ocorrer na rede e esta não ser percebida. Para executar o Snort como um serviço, é necessário executar as seguintes linhas no *prompt* de comando (detalhes no apêndice A):

‘snort/SERVIÇO/install-cd:\winids\snort\etc\snort.conf-ld:\winids\snort\log-K ascii-i1’

‘start sc config snortsvc = auto’

A Figura 11 apresenta a tela inicial do Snort:

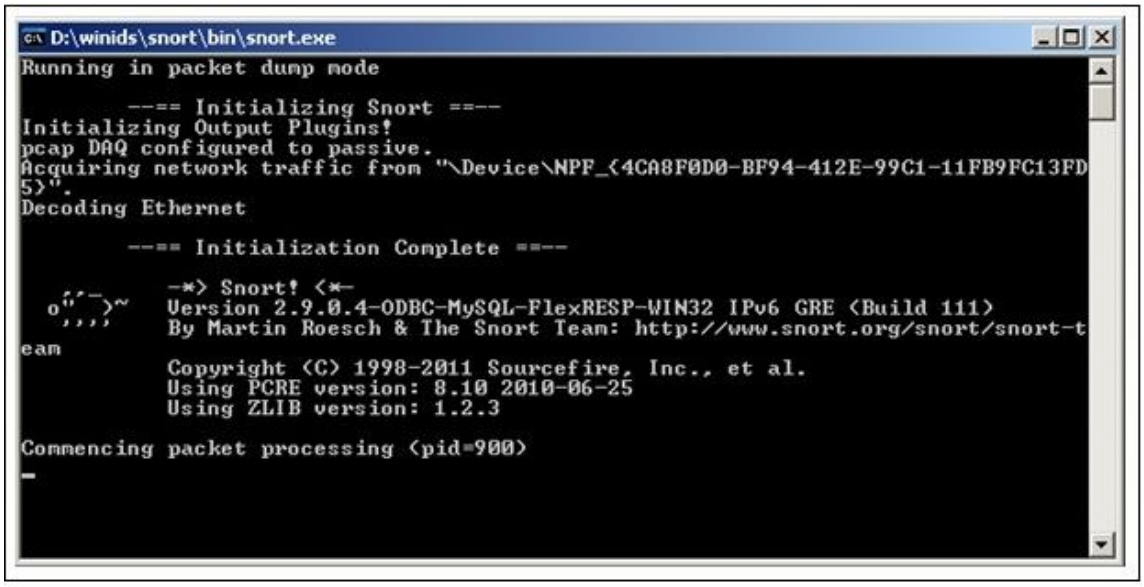


Figura 11. Tela Inicial do Snort

No primeiro teste, nenhum filtro de assinatura do EventSentry está configurado, isso faz com que o Snort gere um grande número de falsos positivos, ou seja o Snort marca como uma possível tentativa de invasão pacotes que não apresentam risco nenhum aos computadores da rede. A Figura 12 apresenta o comando *ping* feito da máquina atacante para a máquina alvo:

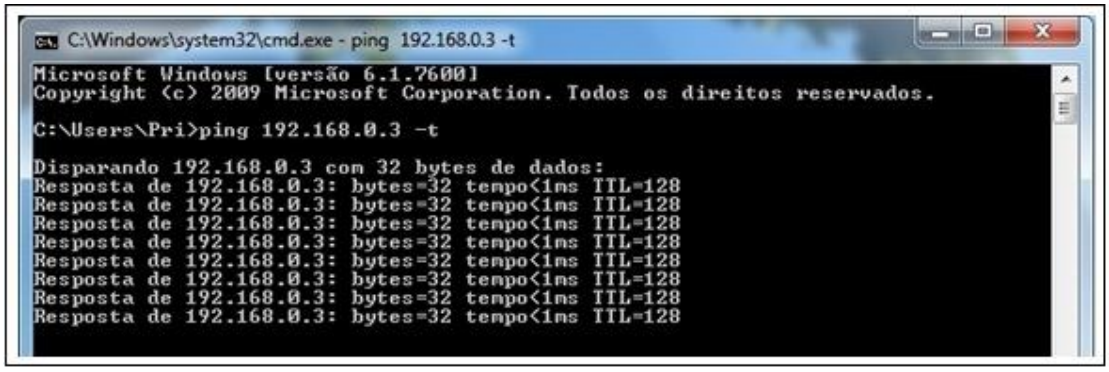


Figura 12. Pingando para a Máquina Alvo

E a Figura 13 mostra a tela do EventSentry sem nenhuma assinatura configurada, porém com o alerta sendo gerado.

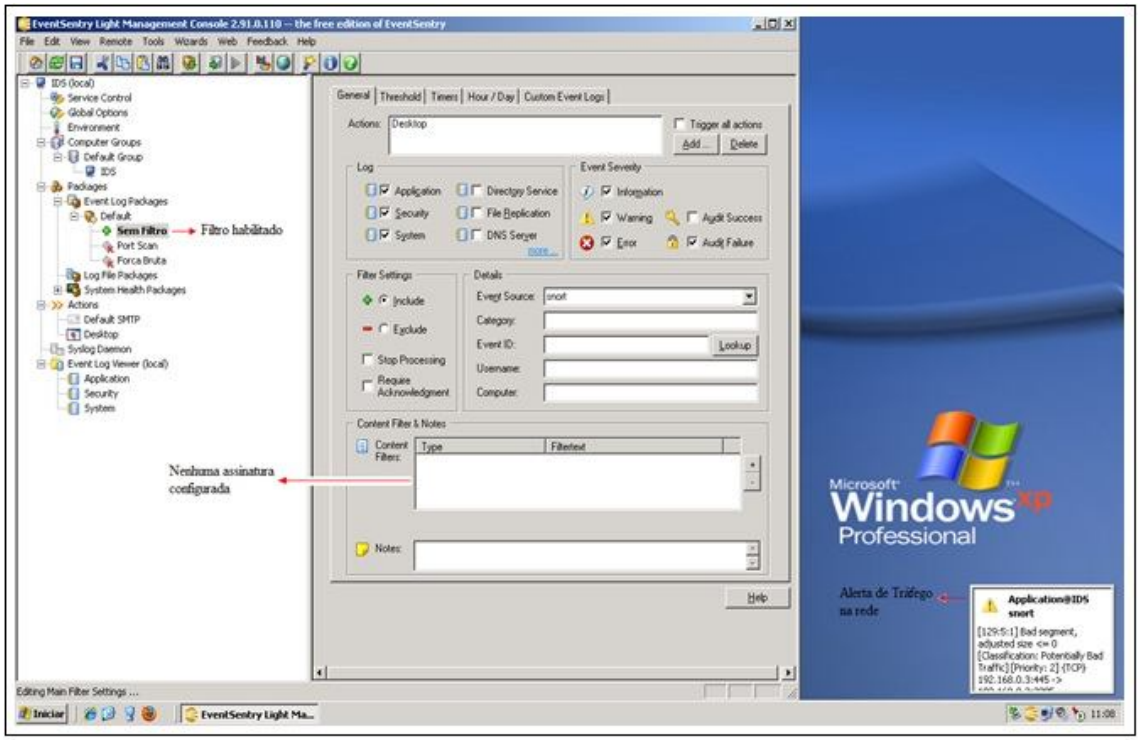


Figura 13. Falso Positivo

Para minimizar o número de falsos positivos deve-se configurar o filtro do EventSentry com a assinatura do ataque em questão, assim quando o Snort compara a assinatura do EventSentry com a assinatura contida nas suas regras, detecta apenas ataques reais.

Utilizando a ferramenta Nmap, realizou-se a tentativa de execução de um Portscan, a máquina atacante contendo o IP 192.168.0.2, tentou encontrar quais portas e serviços estavam em execução na máquina alvo que continha o IP 192.168.0.3. A Figura 14 apresenta a tentativa de Portscan:

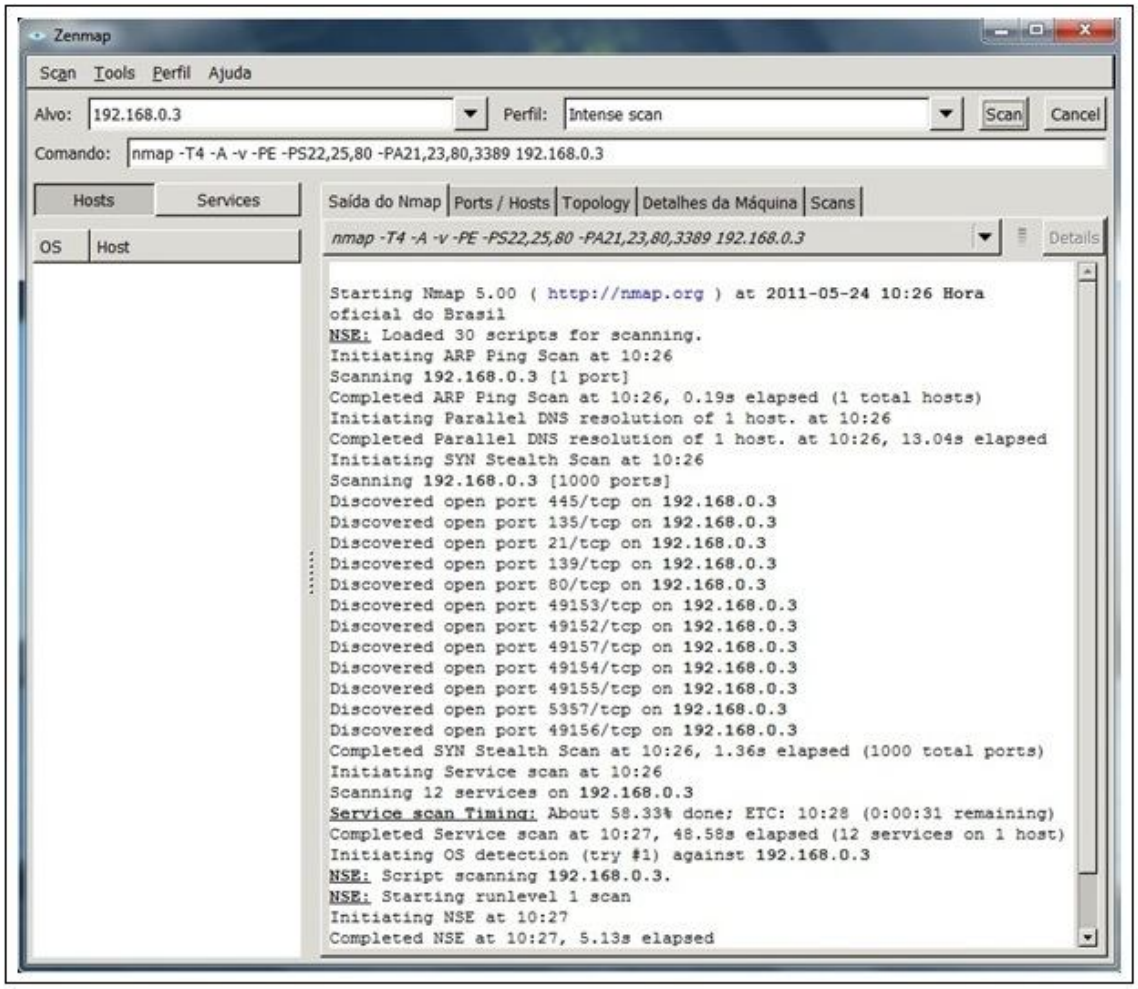


Figura 14. Tentativa de Portscan

O resultado obtido proveniente deste Portscan é apresentado na Figura 15:

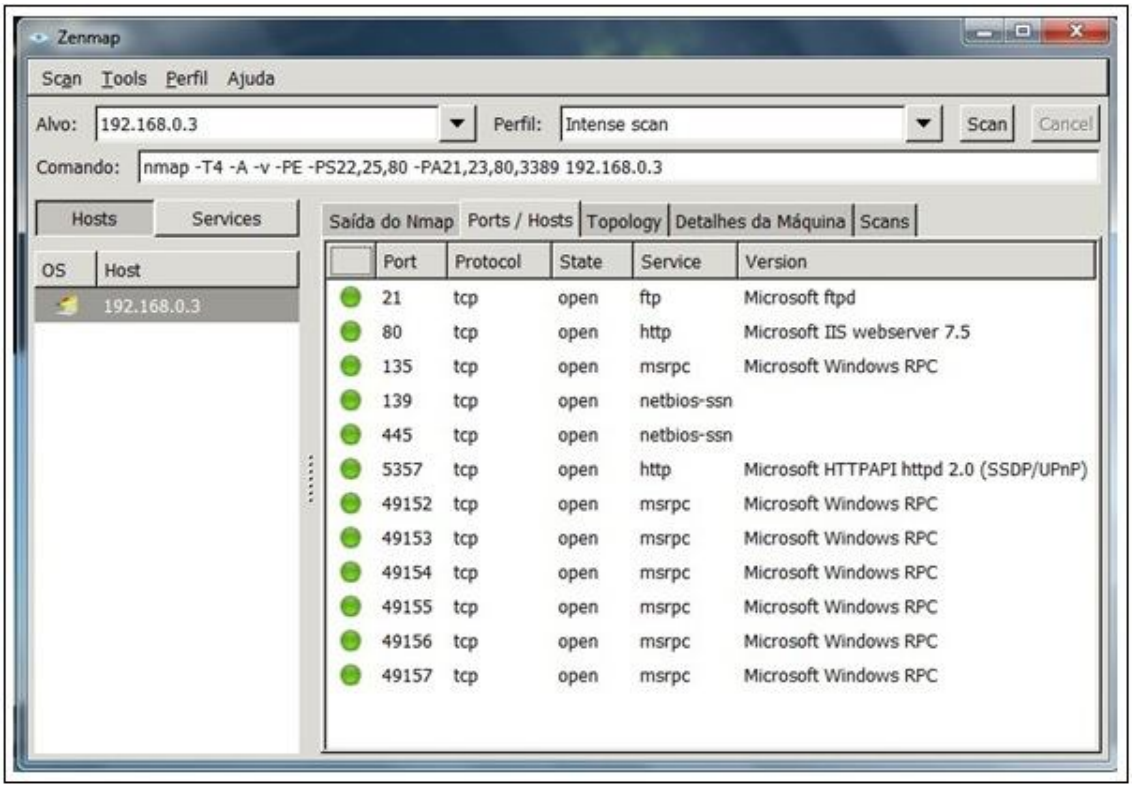


Figura 15. Resultado do Portscan na Máquina Alvo

Apesar da tentativa de scaneamento de portas apresentar resultado positivo, no momento da sua realização o Snort estava em execução na rede e o EventSentry gerou o seguinte alerta apresentado na Figura 16:

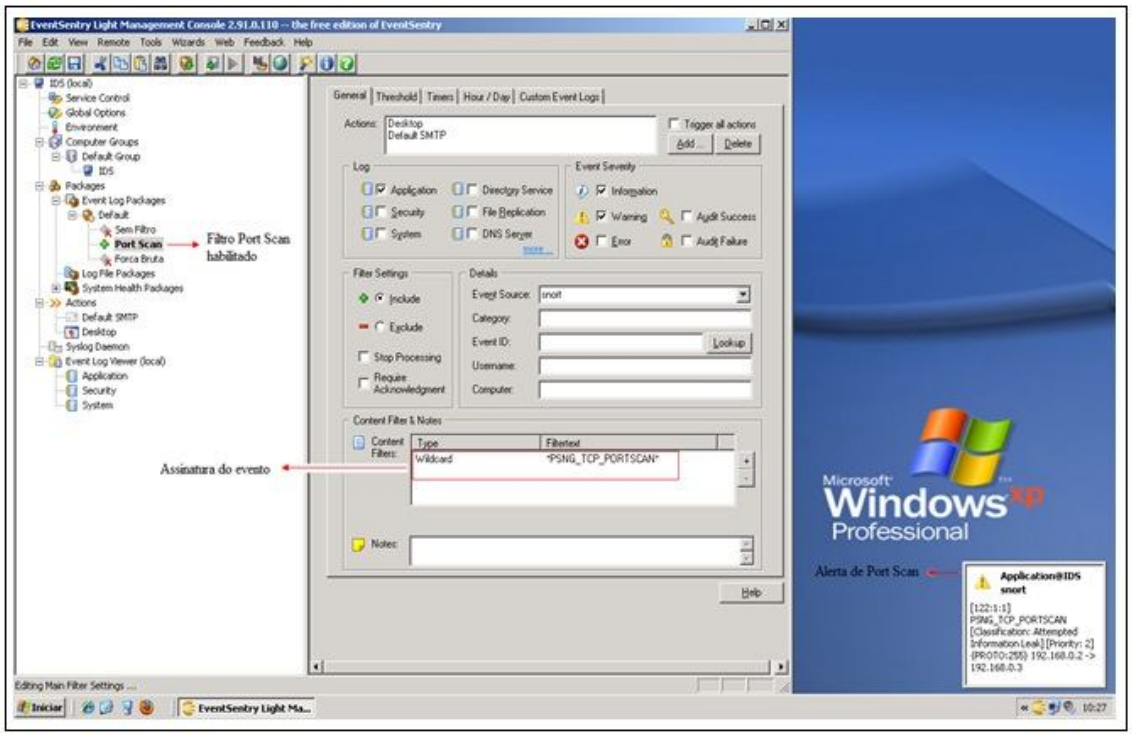


Figura 16. Detecção do Portscan

Além do alerta gerado em forma de pop-up na tela o EventSentry permite que seja configurado uma conta de e-mail para que os alertas também sejam enviados para este e-mail. A Figura 17 apresenta a tela de configuração do e-mail:

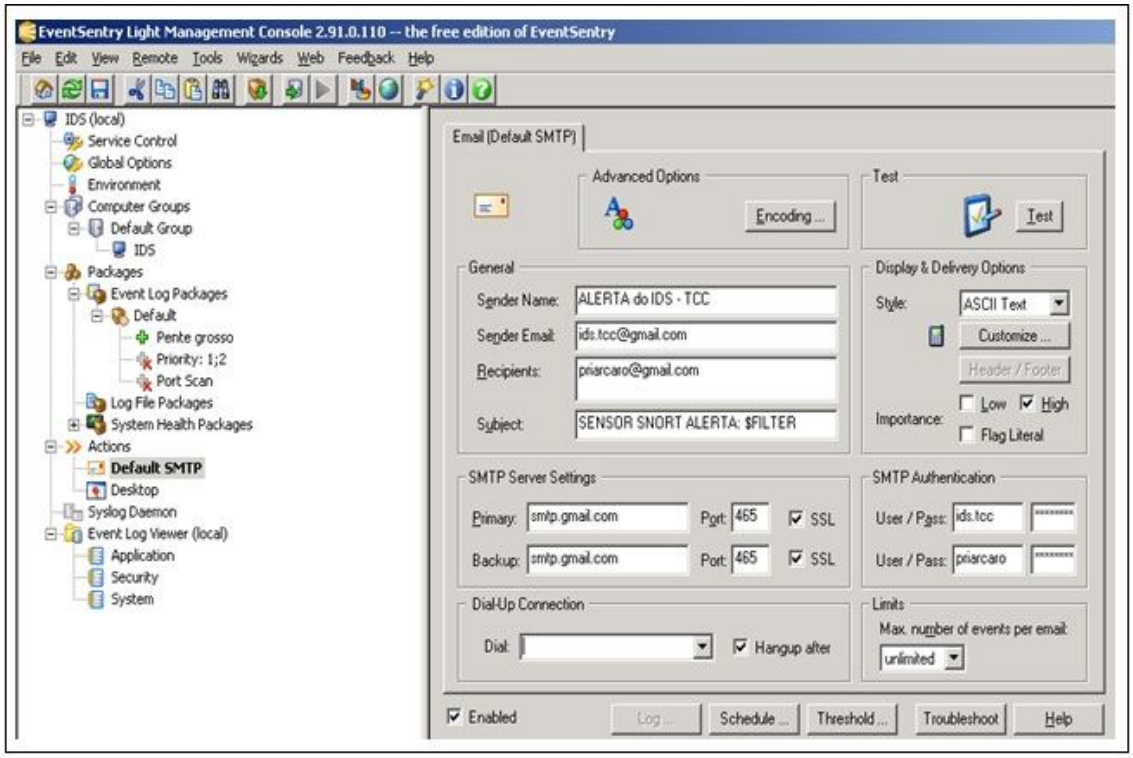
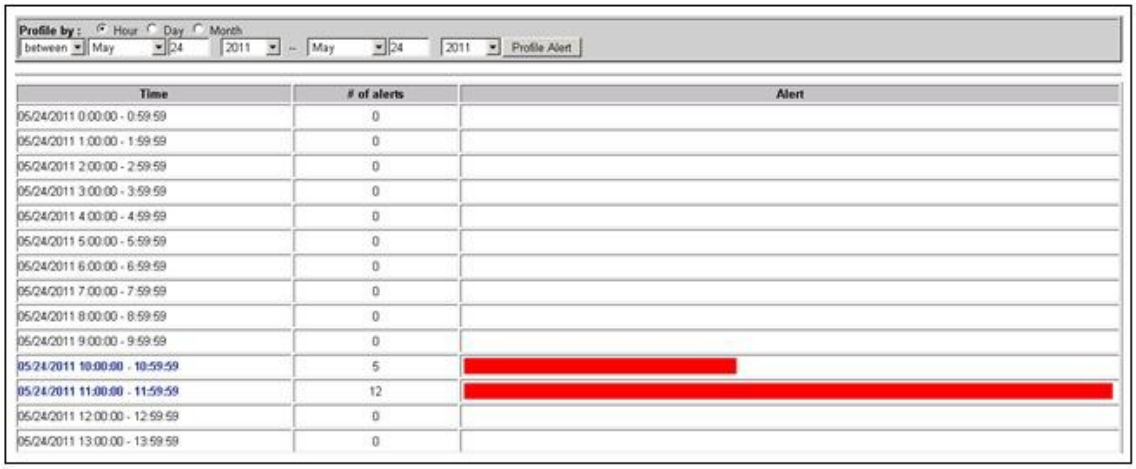


Figura 17. Configuração de Envio do Alerta para E-mail

O e-mail recebido descreve qual tipo de ataque está acontecendo e apresenta a origem e destino deste ataque, conforme ilustra a Figura 18:

Figura 18. E-mail Alertando sobre Portscan
Fonte: Gmail – Google, (2011)

Utilizando a ferramenta BASE se pode obter maiores informações sobre os eventos armazenados no MySQL como por exemplo o número de alertas por hora, conforme Figura 19:

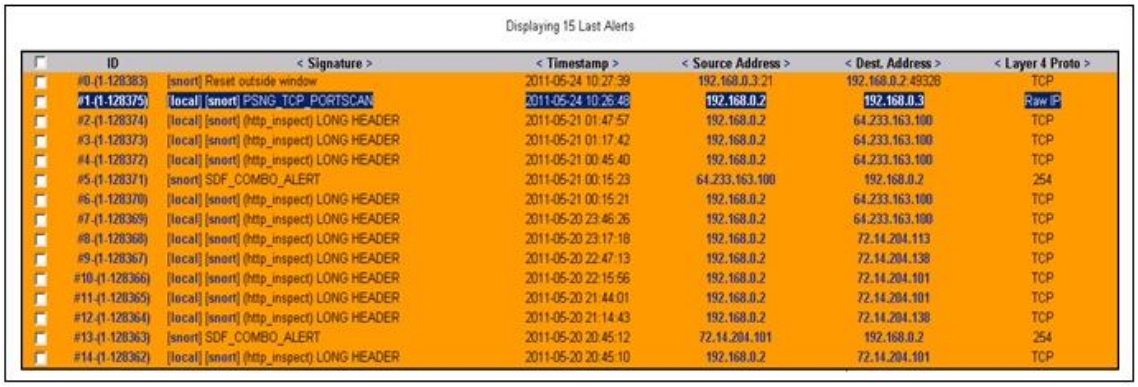


Profile by : Hour Day Month
between May 24 2011 -- May 24 2011 Profile Alert

Time	# of alerts	Alert
05/24/2011 0:00:00 - 0:59:59	0	
05/24/2011 1:00:00 - 1:59:59	0	
05/24/2011 2:00:00 - 2:59:59	0	
05/24/2011 3:00:00 - 3:59:59	0	
05/24/2011 4:00:00 - 4:59:59	0	
05/24/2011 5:00:00 - 5:59:59	0	
05/24/2011 6:00:00 - 6:59:59	0	
05/24/2011 7:00:00 - 7:59:59	0	
05/24/2011 8:00:00 - 8:59:59	0	
05/24/2011 9:00:00 - 9:59:59	0	
05/24/2011 10:00:00 - 10:59:59	5	
05/24/2011 11:00:00 - 11:59:59	12	
05/24/2011 12:00:00 - 12:59:59	0	
05/24/2011 13:00:00 - 13:59:59	0	

Figura 19. Número de Alertas por Hora
Fonte: BASE, (2011)

Também é possível visualizar eventos por data, por protocolo, os 24 últimos alertas ou os 15 últimos alertas. A Figura 20 mostra os últimos quinze alertas gerados pelo Snort:

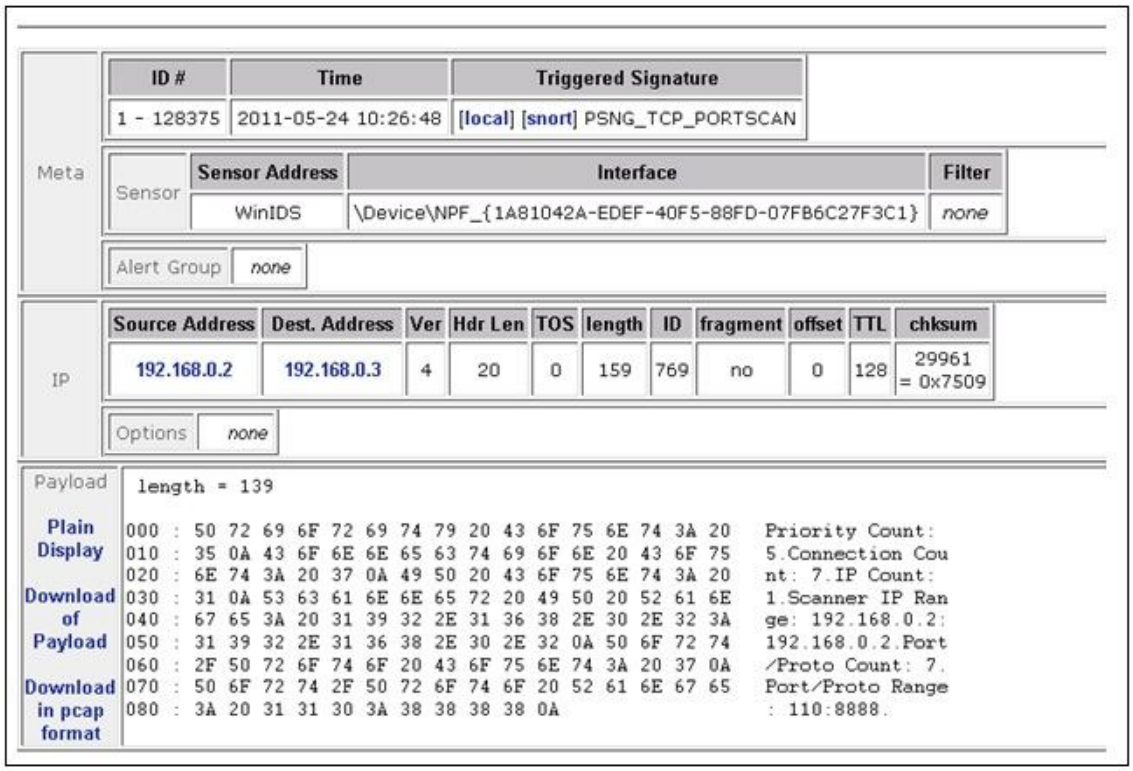


Displaying 15 Last Alerts

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-128383)	[snort] Reset outside window	2011-05-24 10:27:39	192.168.0.3:21	192.168.0.2:49328	TCP
#1-(1-128375)	[local] [snort] PSNG_TCP_PORTSCAN	2011-05-24 10:26:48	192.168.0.2	192.168.0.3	Raw IP
#2-(1-128374)	[local] [snort] (http_inspect) LONG HEADER	2011-05-21 01:47:57	192.168.0.2	64.233.163.100	TCP
#3-(1-128373)	[local] [snort] (http_inspect) LONG HEADER	2011-05-21 01:17:42	192.168.0.2	64.233.163.100	TCP
#4-(1-128372)	[local] [snort] (http_inspect) LONG HEADER	2011-05-21 00:45:40	192.168.0.2	64.233.163.100	TCP
#5-(1-128371)	[snort] SDF_COMBO_ALERT	2011-05-21 00:15:23	64.233.163.100	192.168.0.2	254
#6-(1-128370)	[local] [snort] (http_inspect) LONG HEADER	2011-05-21 00:15:21	192.168.0.2	64.233.163.100	TCP
#7-(1-128369)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 23:46:26	192.168.0.2	64.233.163.100	TCP
#8-(1-128368)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 23:17:18	192.168.0.2	72.14.204.113	TCP
#9-(1-128367)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 22:47:13	192.168.0.2	72.14.204.138	TCP
#10-(1-128366)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 22:15:56	192.168.0.2	72.14.204.101	TCP
#11-(1-128365)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 21:44:01	192.168.0.2	72.14.204.101	TCP
#12-(1-128364)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 21:14:43	192.168.0.2	72.14.204.138	TCP
#13-(1-128363)	[snort] SDF_COMBO_ALERT	2011-05-20 20:45:12	72.14.204.101	192.168.0.2	254
#14-(1-128362)	[local] [snort] (http_inspect) LONG HEADER	2011-05-20 20:45:10	192.168.0.2	72.14.204.101	TCP

Figura 20. Últimos 15 Alertas
Fonte: BASE, (2011)

Clicando sobre cada ID da Figura 20, é possível visualizar detalhadamente cada alerta, conforme indica a Figura 21:



Meta

ID #	Time	Triggered Signature
1 - 128375	2011-05-24 10:26:48	[local] [snort] PSNG_TCP_PORTSCAN

Sensor

Sensor Address	Interface	Filter
WinIDS	\Device\NPF_{1A81042A-EDEF-40F5-88FD-07FB6C27F3C1}	*none*

Alert Group: *none*

IP

Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	chksum
192.168.0.2	192.168.0.3	4	20	0	159	769	no	0	128	29961 = 0x7509

Options: *none*

Payload

Plain Display

Download of Payload

Download in pcap format

```
length = 139

000 : 50 72 69 6F 72 69 74 79 20 43 6F 75 6E 74 3A 20   Priority Count:
010 : 35 0A 43 6F 6E 6E 65 63 74 69 6F 6E 20 43 6F 75   5.Connection Cou
020 : 6E 74 3A 20 37 0A 49 50 20 43 6F 75 6E 74 3A 20   nt: 7.IP Count:
030 : 31 0A 53 63 61 6E 6E 65 72 20 49 50 20 52 61 6E   1.Scanner IP Ran
040 : 67 65 3A 20 31 39 32 2E 31 36 38 2E 30 2E 32 3A   ge: 192.168.0.2:
050 : 31 39 32 2E 31 36 38 2E 30 2E 32 0A 50 6F 72 74   192.168.0.2.Port
060 : 2F 50 72 6F 74 6F 20 43 6F 75 6E 74 3A 20 37 0A   /Proto Count: 7.
070 : 50 6F 72 74 2F 50 72 6F 74 6F 20 52 61 6E 67 65   Port/Proto Range
080 : 3A 20 31 31 30 3A 38 38 38 38 0A                  : 110:8888.
```

Figura 21. Detalhes do Alerta com ID 1
Fonte: BASE, (2011)

O BASE também gera gráficos com os dados dos alertas armazenados no MySQL no formato de barra, linha ou pizza, pode-se gerar gráficos de diferentes tipos, como por exemplo, de hora versus número de alertas, dia, mês, Endereço de IP Origem, Endereço de IP Destino, TCP de origem e destino, UDP de origem e destino, país de origem e destino, sensor, assinatura, versus número de alertas.

Um exemplo de gráfico de barra do tipo Endereço IP de Destino versus Número de Alertas por ser observado na Figura 22:

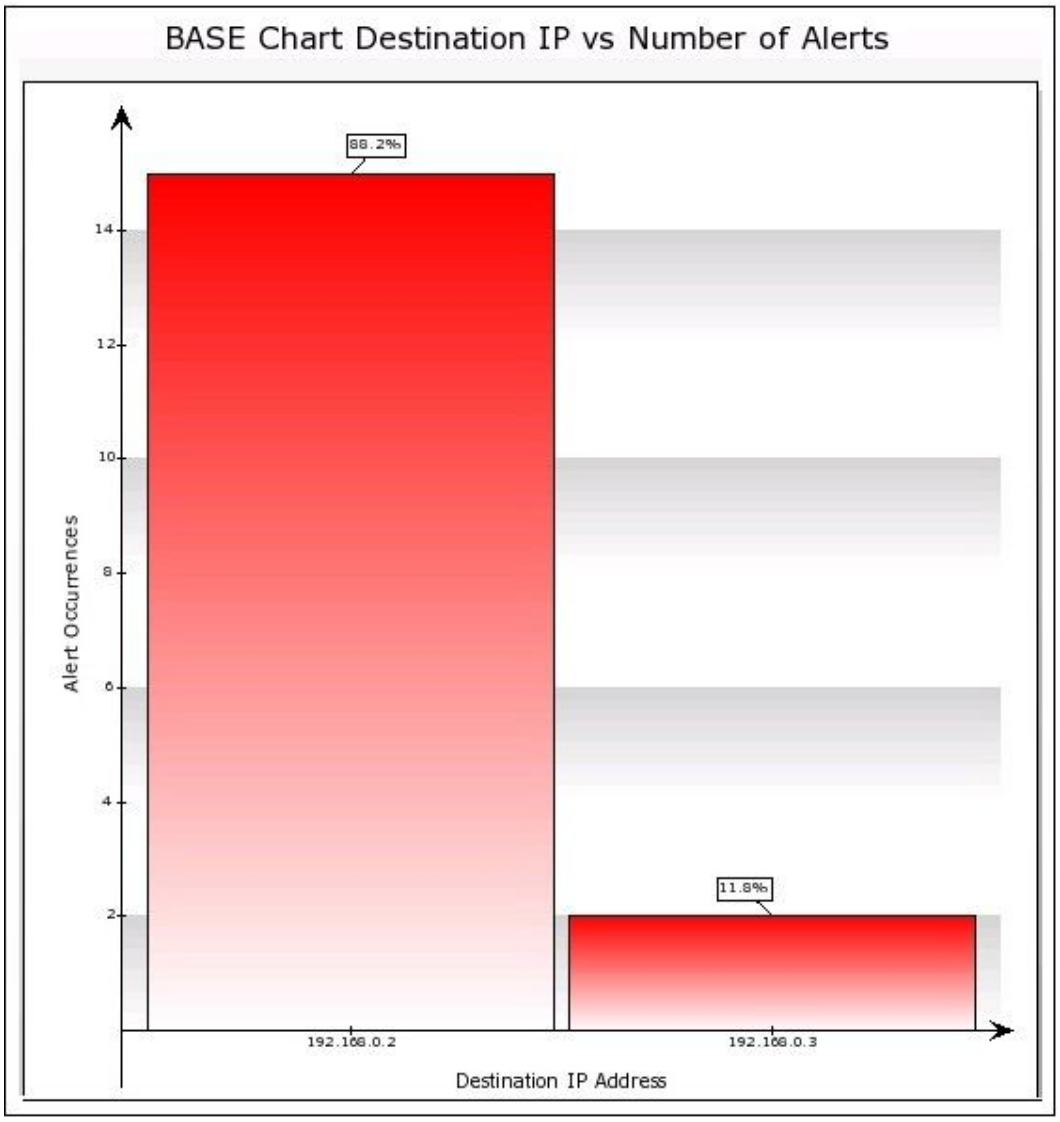


Figura 22. Gráfico Endereço IP de Destino vs Número de Alertas
Fonte: BASE, (2011)

6.3 TESTE DE EFICIÊNCIA DO SNORT UTILIZANDO A FERRAMENTA BRUTUS

Utilizando a ferramenta Brutus, realizou-se uma segunda tentativa de invasão, desta vez realizando um ataque de Força Bruta, a máquina atacante contendo o IP 192.168.0.2, tentou descobrir a senha de um Cliente FTP instalado na máquina alvo que continha o IP 192.168.0.3. A Figura 23 apresenta a tentativa de Força Bruta:

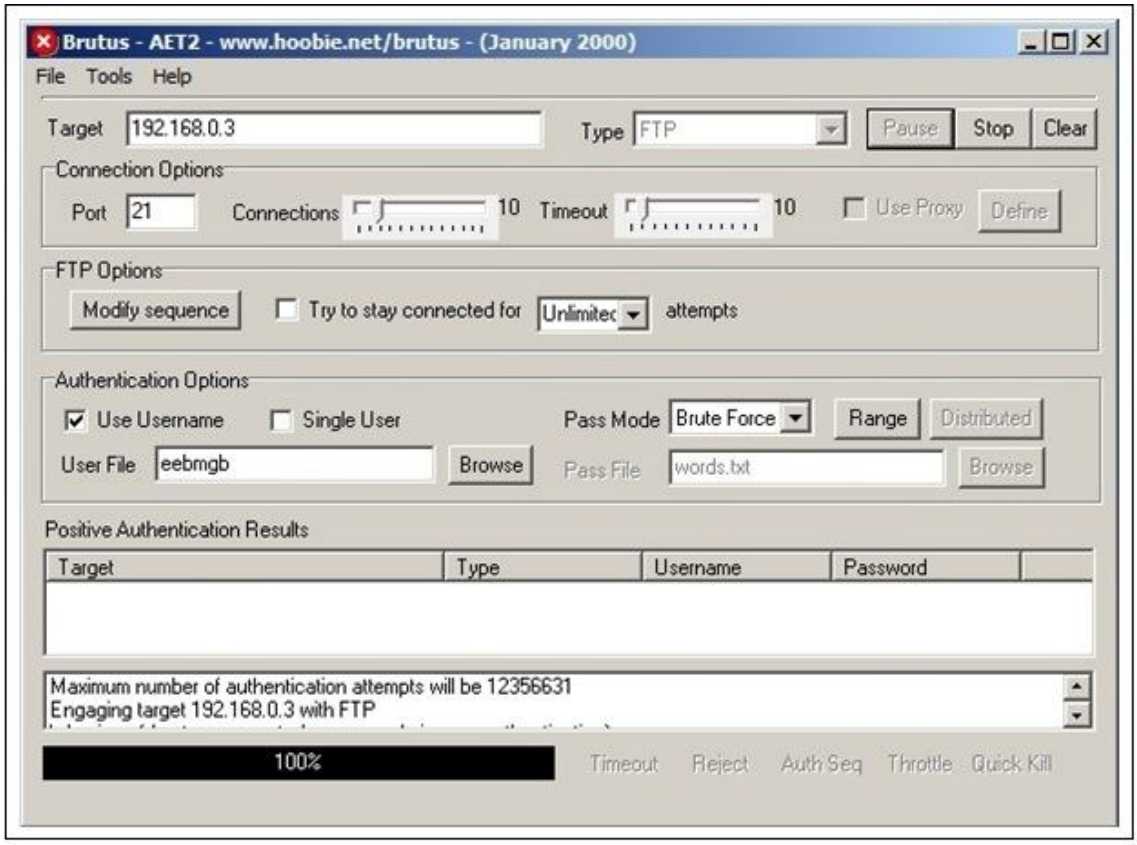


Figura 23. Tentativa de Força Bruta

Apesar da tentativa de descobrir a senha FTP, no momento da sua realização o Snort estava em execução na rede e o EventSentry gerou o seguinte alerta apresentado na Figura 24:

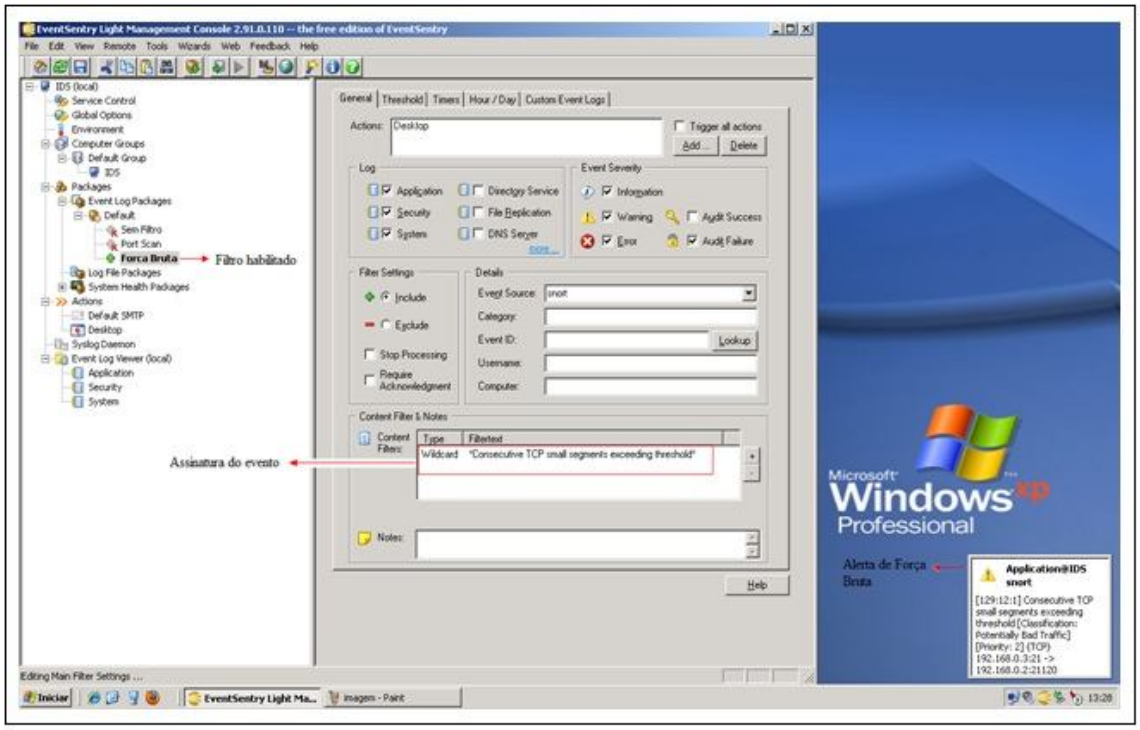


Figura 24. Detecção de Força Bruta

Todos os ataques de Portscan e Força Bruta foram replicados cinquenta vezes cada, e em todas as tentativas o Snort reconheceu a assinatura e gerou o alerta. A Figura 25 apresenta o gráfico de Porcentagem de Alertas x Ataques:

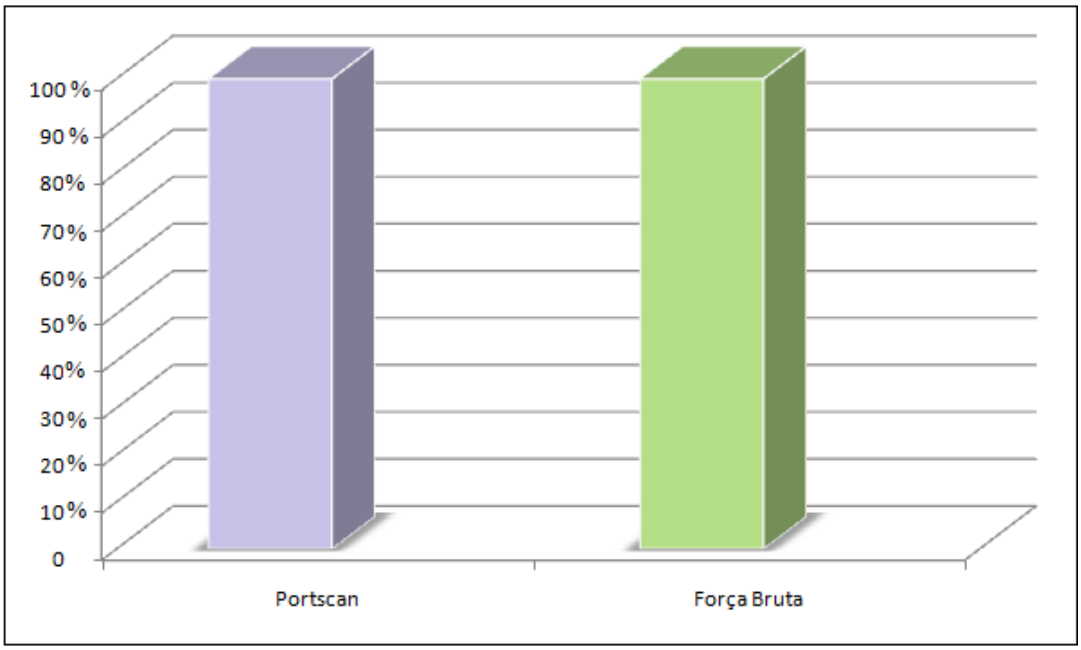


Figura 25. Porcentagem de Alertas Gerados x Ataques

CONCLUSÃO

Neste trabalho, foram apresentados conceitos e definidos procedimentos para a instalação e configuração do IDS Snort e de todos os aplicativos auxiliares que compõem a implantação de um IDS na rede. É importante destacar que a proteção de uma rede não é uma tarefa singular e muito menos simples. Não basta apenas implantar um IDS para que todos os problemas de segurança se resolveram. Problemas complexos requerem soluções complexas.

Não se pode pensar em segurança, sem um trabalho contínuo de atualizações dos aplicativos e das ferramentas utilizadas. É um grande erro pensar que com a implementação de uma solução de segurança a rede estará protegida, não existindo mais problemas e preocupações com assuntos ligados à segurança da informação.

Como abordado anteriormente, neste trabalho optou-se pela implantação de um sensor IDS através da utilização do Snort. Apesar de o Snort ser uma ferramenta destinada à segurança de rede, ele é um *software* e como todo *software* está sujeito a falhas. Deve-se ficar atento aos seus boletins de segurança, atualizações e as novas vulnerabilidades descobertas.

O Snort mostrou ser uma ferramenta bastante poderosa para fornecer segurança a uma rede, constituindo uma ótima alternativa para administradores de rede, porém por ser uma ferramenta da comunidade *open source* baseada em regras, estas regras atualmente tem um preço de 1.400,00€ anuais, contudo depois de cinco dias do lançamento da nova atualização do pacote de regras, é disponibilizado gratuitamente pela comunidade um pacote *default.*

No desenvolvimento deste projeto algumas dificuldades foram encontradas, uma delas foi a falta de documentação em relação à instalação e configuração do IDS Snort no Sistema Operacional *Windows,* a segunda dificuldade foi encontrar quais softwares seriam necessários para que Snort conseguisse gerar os alertas, estas dificuldades foram sanadas

através da troca de e-mails com aos mantenedores da comunidade Snort no Brasil, onde estes disponibilizaram um tutorial em inglês que apresentava um exemplo de configuração do Snort e este mesmo tutorial citava o uso de uma ferramenta que em conjunto com o Snort realizada os alertas, o EventSentry.

A partir do EventSentry, o filtro de cada ataque realizado era configurado e continha a assinatura do evento e a medida que se realizava a tentativa de ataque com as ferramentas Nmap e Brutus, habilitava-se o filtro desejado para que o alerta fosse gerado.

Nestes testes realizados o Snort detectou todas as tentativas de invasão de Portscan e Força Bruta a ele submetidas, gerando um baixo número de falsos positivos, já que os alertas gerados eram feitos por meio da comparação da assinatura. Os falsos positivos ocorriam apenas quando nenhum filtro do EventSentry estava habilitado, isto porque qualquer ação que ocorria na rede era classificada como uma possível ameaça.

Estes alertas são classificados como respostas passivas geradas pelo IDS, ou seja por meio destes alertas são gerados relatórios para que o administrador da rede, baseado nas informações armazenadas, possa tomar as medidas que julgar necessárias, o Snort também pode enviar estas notificações para telefones celulares e e-mail.

Com a implantação do Snort as empresas têm a oportunidade de gerarem uma ação pró-ativa na rede, onde é possível analisar quais são os acessos não autorizados que estão ocorrendo e adotar uma iniciativa para bloquear estes acessos.

O Snort apresenta muitas vantagens, além de possibilitar maior segurança às redes, ligado a ferramenta BASE possibilitou inspecionar com detalhes todos os *logs* capturados e armazenados no MySQL.

Este trabalho possibilitou um grande aprendizado sobre segurança da informação e os tipos de ameaças e ataques a que os usuários das redes estão expostos. Gerou um amplo conhecimento também sobre a instalação, configuração e funcionamento de um Sistema de

Detecção de Intrusão em rede, especificadamente sobre o Snort, visto que esta foi a ferramenta escolhida para a detecção dos testes de Portscan e Força Bruta. Por fim para que este desafio fosse vencido houve a necessidade da leitura de muitos trabalhos acadêmicos que em sua maioria foram realizados no Sistema Operacional Linux, mas que foram significantes para o começo do entendimento de como os testes seriam realizados neste trabalho.

Segundo Santos (2005) atualmente o Snort é o IDS mais utilizado, existindo muitas ferramentas que podem trabalhar junto a ele. Em virtude disso, sugere-se os seguintes trabalhos futuros:

a) realizar outros tipos de ataques;
b) avaliar métricas de eficiência para IDSs;
c) implementação do Snort no modo *inline*. O modo *inline* permite ao Snort prevenir as invasões, em vez de somente detectá-las. No modo *inline* o Snort obtém os pacotes do *Iptables* ao invés da biblioteca *WinPcap*. Desde modo o Snort trabalha em conjunto com o *firewall*, bloqueando e permitindo pacotes baseados nas regras do Snort;
d) utilização do *SnortSam*, que é um *plugin* para o Snort de código aberto. Este *plugin* permite o bloqueio automático de ataques em diversos *firewalls*.

REFERÊNCIAS

ALMEIDA, Aléxis Rodrigues de. **Como funcionam os exploits.** Minas Gerais. 2005. 9 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro, 2002.

BACE, R.; MELL, P. **Intrusion Detection System**. Scotts Valley: NIST, 2001. (NIST Special Publication SP 800-31).

BARBOSA, André S. **Sistemas de Detecção de Intrusão.** Rio de Janeiro. 2000. 47 p.

BELO; Carlos. **Segurança em redes.** Lisboa, 2003. Disponível em: http://mega.ist.utl.pt/~ic-rc2/aula325.pdf. Acesso em: 15 de Mar. 2009.

BRASIL. ABNT. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação.** 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=1532>. Acesso em: 15 set. 2010.

BRASIL ganhou 12 milhões de internautas em 2009, mostra IBGE. 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/09/brasil-ganhou-12-milhoes-de-internautas-em-2009-mostra-ibge.html>. Acesso em: 09 set. 2010.

CASAGRANDE, Rogério Antônio. **Técnicas de Detecção de Sniffers.** 2003. 59 f. Dissertação (Mestrado) - Curso de Ciências da Computação, UFRGS, Porto Alegre, 2003.

CERT.br. **Cartilha de Segurança para Internet**. 2006. Disponível em: http://cartilha.cert.br. Acesso em: 14 set. 2009.

CERT.br – **Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil**. 2010. Disponível em: http://www.cert.br/stats/incidentes. Acesso em: 15 out. 2010.

CERT.br. **O que é e como funciona uma ferramenta IDS?**. 2009. Disponível em: <http://www.clm.com.br/snort/comofuncionaids.asp>. Acesso em 17. out. 2010.

CHOLEWA, Rômulo Moacir. **Segurança em Redes**: Conceitos Básicos. 2001. Disponível em: <http://www.rmc.eti.br>. Acesso em: 06 set. 2009.

CRONKHITE, Cathy; MCCULLOUGH, Jack. **Hackers Acesso Negado:** O Guia Completo para a proteção dos seus negócios on-line. Rio de Janeiro: Campus, 2001. 253 p.

DESCHAMPS, Eduardo; PEREZ, Fábio Luis; ZIPF, José Gil Fausto. **Sistema Digital de Comunicações Móveis**. 2005. Disponível em: <http://www.estudostecnologicos.unisinos.br/index.php?e=1&s=9&a=33>. Acesso em: 15 mar. 2009.

EGOSHI, Koiti; ROMANO, Marcelo. **Como Atacam: Worms**. Aprenda Fácil. São Paulo, 2003.

FRANCESCHINELLI, Daniella Arruda. **Estudo Comparativo dos Aspectos de Segurança em Redes WWAN, WLAN e WPAN.** 113 f. Dissertação (Mestrado em Computação) - Universidade Estadual de Campinas, São Paulo, 2003.

FURMANKIEWICZ, Edson. **Segurança Máxima:** O guia de um hacker para proteger seu site na Internet e sua rede. Rio de Janeiro: Campus, 2000. 826 p.

GOMES, Olavo José Anchieschi. **Segurança total.** São Paulo: Makron Books, 2000. 276 p.

HATCH, Brian; LEE, James; KURTZ, George. **Hackers Expostos:** Segredos e Soluções para a Segurança do Linux. São Paulo: Makron Books, 2002. 493 p.

ISOC. Internet Society. Internet Engineering Task Force (IETF). **Request for Comments (RFC 2828).** 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 22 set. 2010.

JUNIOR, Ademar de Souza Reis; FILHO, Milton Soares. **Um Sistema de Testes para a Detecção Remota de Sniffers em Redes TCP/IP.** 2002. 68f. Monografia (Graduação em Ciência da Computação) – Curso de Ciência da Computação, Universidade Federal do Paraná, Paraná, 2002.

KONRATH, Marlom Alves. **Estudo da Vulnerabilidade da Arquitetura TCP/IP e Desenvolvimento de uma Ferramenta para Detecção de Intrusão.** 55 f. Curso de Informática, Unisinos, São Leopoldo, 2001.

LAUFER; Rafael P. **Introdução a Sistemas de Detecção de Intrusão**. Rio de Janeiro, 2003. Disponível em: <http://www.gta.ufrj.br/grad/03_1/sdi/index.htm>. Acesso em 01 Set. 2010.

LEMOS, Aline Morais de. **Política de Segurança da Informação.** Rio de Janeiro, 2001. Disponível em: www.estacio.br/campus/millorfernandes/monografias/aline_morais.pdf. Acesso em: 15 set. 2010.

MACHADO, André; FREIRE, Alexandre. **Como Blindar seu PC:** aprenda transformar seu computador numa fortaleza digital. Rio de Janeiro: Elsevier, 2006.

MALTA, Marcelo Alvim. **Detecção de Intrusão em Redes de Computadores.** 2006. 55 f. Trabalho Acadêmico (Bacharel em Ciência da Computação) - Departamento de Computação, Universidade Estadual de Londrina, Londrina/PR, 2006.

MCAFEE INC. (Estados Unidos). **Spyware:** uma campanha mutante. 2007. Disponível em: <http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_spyware_morphing_campaign_br_pt.pdf>. Acesso em: 30 set. 2010.

Microsoft Corporation. **Segurança em Casa.** 2010**.** Disponível em: <http://www.microsoft.com/portugal/athome/security/privacy/pharming.mspx>. Acesso em: 28 Set. 2010.

MILITELLI, Leonardo Cavalarri. **Proposta de um agente de aplicação para detecção, prevenção e contenção de ataques em ambientes computacionais.** 2006. 73 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Escola Politécnica da Universidade de São Paulo, São Paulo, 2006.

MITNICK, Kevin D; SIMON, William L. **A Arte de Invadir**. São Paulo: Prentice-Hall, 2005. 256 p.

MONTEIRO, Emiliano Soares. **Segurança em Ambientes Corporativos**. Florianópolis: Visual books, 2003.

MORAIS, Luis. Cuidados a ter com o Pharming. **CERT.PT**, Portugal. 2008. Disponível em: <http://www.cert.pt/index.php/pt/recomendacoes/1224-pharming>. Acesso em: 28 set. 2010.

NBR/ISO/IEC 17799. **Tecnologia da Informação - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2001.

_____. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro, 2002.

NETO, Fernando Melis; GONÇALVEZ, Robério. **Entenda Melhor a Segurança Virtual**: Guia Fácil Informática: Segurança. São Paulo, 2005. v. 4, p. 12-19.

NORTHCUTT, Stephen et al. **Desvendando Segurança em Redes:** O Guia Definitivo para Fortificação de Perímetros de Rede usando Firewalls, VPN's, Roteadores e Sistemas de Detecção de Intrusão. Rio de Janeiro: Campus, 2002. 650 p.

NIEHUES, Lucas Urgioni. **Ameaças Digitais:** Um estudo dos riscos envolvidos no uso da Internet, seus impactos e formas de proteção. Criciúma. 2007. 86 p.

OLIVEIRA, Wilson José. **Segurança da Informação**. Florianópolis: Visual Books, 2001. 181 p.

PUPO, Alexandre Silveira. **O que é e como funciona uma ferramenta IDS?:** Privacidade, Segurança e Direito. 2009. Disponível em: <www.snort.org.br>. Acesso em: 30 jun. 2009.

SANTOS, Bruno Ribeiro dos. **Detecção de Intrusos utilizando o Snort.** 2005. 91 f. Curso de Administração de Redes Linux, UFLA, Minas Gerais, 2005.

SANTOS, Luciano Alves Lunguinho. **O Impacto da Engenharia Social na Segurança da Informação.** Aracaju. 2004. 83 p.

SANTOS, Marcos Antonio de Oliveira. **Sistema de Detecção de Intrusos - IDS**. 2004. 45 f. Trabalho de Conclusão de Curso, Faculdade de Ciências Aplicadas de Minas - Uniminas, Uberlandia, 2004.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma visão executiva. 7. ed. Rio de Janeiro: Elsevier, 2003. 156 p.

SNORT BR. Disponível em: < http://www.snort.com.br/snort.asp>. Acesso em 12 out. 2009.

TANENBAUM, Andrew S. **Redes de computadores.** Rio de Janeiro: Campus, 2003. 945 p.

TAVARES, Dalton Matsuo. **Avaliação de Técnicas de Captura para Sistemas Detectores de Intrusão.** 2002. 110 f. Dissertação (Mestrado) - Usp, São Paulo, 2002.

THOMÉ, Antonio G. **Comunicação de Dados.** 2000. Disponível em: <http://equipe.nce.ufrj.br/thome/comdados/apostila.pdf>. Acesso em: 01 set. 2010.

TROMBIM, Diordgenes. **Diagnóstico do Tráfego de Rede de Laboratórios de Informática**. Estudo de Caso: Universidade do Extremo Sul Catarinense. Criciúma. 2006. 115 p.

VIEIRA JUNIOR, Francisco. **Estudo de Caso em Segurança de Redes usando como Ferramenta de IDS (Intrusion Detection System) o Snort.** São Paulo. 2002.

WADLOW, Thomas A. **Segurança de Redes:** Projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2000. 269 p.

WIKIPEDIA. **Spyware**. 2010. Disponível em: <http://pt.wikipedia.org/wiki/Spyware>. Acesso em: out. 2010.

BIBLIOGRAFIA COMPLEMENTAR

BERNARDES, M. **Avaliação do Uso de Agentes Móveis em Segurança Computacional**. 1999. 105 f. Dissertação (Mestrado) - Curso de Engenharia de Eletricidade, UFMA, São Carlos, 2003.

BERNSTEIN, Terry et al. **Segurança na Internet**. Rio de Janeiro: Campus, 1997. 461 p.

BONIFACIO, J. **Sistemas de Segurança Distribuídos**: integração de firewall com sistemas de detecção de intrusão. 1998. Dissertação (Mestrado) - Icmc/usp, São Paulo, 1998.

CANSIAN, A. **Desenvolvimento de um Sistema Adaptativo de Detecção de Intrusos em Redes de Computadores**. 1997. Tese (Doutorado) - USP, São Carlos, 1997.

COMBS, G. **Ethereal**, 2004. Disponível em: <http://www.ethereal.com/distribution/ win32>. Acesso em 31 out 2009.

COMER, D. E. **Interligação em Rede Com TCP/IP**. Rio de Janeiro: Campus, 1998. v. 1.

LAUDON, Kanneth C; LAUDON, Jane P. **Gerenciamento de Sistemas de Informação**. Rio de Janeiro: LTC, 1999.

MARTINS, José Carlos Cordeiro. **Gestão de projetos de segurança da informação**. Rio de Janeiro: Editora Brasport: 2003.

NORTHCUTT, Stephen; NOVAK, Juddy; MCLACHLAN, Donald. **Segurança e Prevenção em Redes.** São Paulo: Berkeley, 2001. 478 p.

PERES, A.; WEBBER R. Considerações sobre segurança em redes. In: III Workshop em Segurança de Sistemas Computacionais, 2003, Natal. **Anais**... Natal: UFRN, 2003.

REIS, A.S., Soares M. **Um sistema de testes para detecção remota de sniffers**. UFPR, 2002. Disponível em: <http://www.sniffdet.sourceforge.net>. Acesso em 14 set. 2009.

RIZZO, Alexandre Marcos; CARONE, Guilherme; FREITAS, Ladislau Tenório de. **Proteção Total:** Segurança. Guia Completo. São Paulo, 2004. v. 1, p. 19-24.

TEIXEIRA JÚNIOR, José Helvécio et al. **Redes de Computadores:** Serviço, Administração e Segurança. São Paulo: Makron Books, 1999. 493 p.

THOMAS, Tom. **Segurança de Redes:** Primeiros Passos. Rio de Janeiro: Ciência Moderna, 2007. 395 p.

APÊNDICE A

TUTORIAL DE INSTALAÇÃO DO SISTEMA DE DETECÇÃO DE INTRUSÃO

(Windows 2000, XP e 2003)

1. TOPOLOGIA CONCEITUAL

Existem vários pacotes de software que produzem essa topologia. Abaixo está uma breve descrição de cada um dos pacotes:

a) **Snort:** Ferramenta de detecção de intrusão que inspeciona e orienta os pacotes de entrada de dados;

b) **WinPcap:** Esta é a arquitetura utilizada para a captura de pacotes, biblioteca padrão para Windows do snort;

c) **Apache Web Server:** Este é o servidor web para a maioria dos sites de Internet;

d) **MySQL:** Esse é uma plataforma Free SQL baseada em servidor de banco de dados para armazenar os alertas WinIDS;

e) **ADODB:** Esta é uma biblioteca orientada a objetos escrita em PHP, que torna abstratas as operações do banco de dados para obter a portabilidade;

f) **PHP:** Esta é uma linguagem de scripts amplamente utilizada para fins gerais que a BASE utiliza;

g) **Análise e Basic Security Engine (BASE):** Esta é uma aplicação PHP baseada na Web para exibir alertas do Snort no browser.

2. INSTALAÇÃO DOS PRÉ-REQUISITOS

a) instalar o Microsoft Windows XP;

b) instalar o Winrar 4.0;

c) instalar o NotePad++ (para trabalhar com arquivos de configuração);

d) desativar atualizações automáticas;

e) desativar Firewall (o sensor do snort fica transparente ao firewall);

f) desativar Central de Segurança;

g) baixar o pacote WinIDS disponível em:

http://www.winsnort.com/index.php?module=Downloads

h) criar uma partição nova no HD, com a letra de unidade D: e uma pasta winids;

i) Adicionar uma entrada de resolução de host ’127.0.0.1 winids’ no arquivo C:\windows\system32\drivers\etc\hosts (abre a base com o nome winids);

j) descompactar o pacote winids em D:\temp;

k) adicionar entrada no registro em D:\temp\win7-RegTweaks (mostra as extensões de arquivos e arquivos ocultos).

3. INSTALAÇÃO DO SNORT

a) instalar o WinPcap 4.1.2;

b) instalar o snort 2.9.0.4 com suporte para IPv6 no diretório D:\winids\snort;

c) extrair as rules (regras) para o diretório D:\winids\snort\etc;

d) abrir o snort.conf com notepad++ e alterar as seguintes linhas:

Original: var HOME_NET any
mudar para: var HOME_NET 192.168.1.0/24

Original: var RULE_PATH ../rules
mudar para: var RULE_PATH d:\winids\snort\rules

Original: var SO_RULE_PATH ../so_rules
mudar para: var SO_RULE_PATH d:\winids\snort\so_rules

Original: var PREPROC_RULE_PATH ../preproc_rules
mudar para: var PREPROC_RULE_PATH d:\winids\snort\preproc_rules

Original: dynamicpreprocessor directory
/usr/local/lib/snort_dynamicpreprocessor/
mudar para: dynamicpreprocessor directory
d:\winids\snort\lib\snort_dynamicpreprocessor

Original: dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
mudar para: dynamicengine
d:\winids\snort\lib\snort_dynamicengine\sf_engine.dll

Original: dynamicdetection directory /usr/local/lib/snort_dynamicrules
mudar para: # dynamicdetection directory /usr/local/lib/snort_dynamicrules

Original:
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6

Mudar para:
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6

Original: # preprocessor sfportscan: proto { all } memcap { 10000000 }
sense_level { low }
mudar para: preprocessor sfportscan: proto { all } memcap { 10000000 }
sense_level { low } logfile { portscan.log }

e) logo abaixo da saida do 'log_tcpdump: tcpdump.log' inserir essa linha a seguir:

Original: # output database: log, <db_type>, user=<username>
password=<password> test dbname=<name> host=<hostname>

mudar para: output database: log, mysql, user=snort password=l0gg3r
dbname=snort host=winids sensor_name=WinIDS

Original: include classification.config
mudar para: include d:\winids\snort\etc\classification.config

Original: include reference.config
mudar para: include d:\winids\snort\etc\reference.config

Original:
include $PREPROC_RULE_PATH/preprocessor.rules

include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules

mudar para:
include $PREPROC_RULE_PATH/preprocessor.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules

Original: include threshold.conf
mudar para: include d:\winids\snort\etc\threshold.conf

f) salvar e copiar o snort.conf para D:\winids\snort\etc.

4. INSTALAÇÃO DO APACHE

a) criar a pasta em D:\winids\apache;

b) instalar Apache 2.2.17 (httpd);

c) domínio da rede: winids;

d) nome do servidor: winids;

e) endereço de e-mail do admin: admin@fake.com;

f) parar o serviço do apache, clicar com botão direito no ícone **open apache monitor**, Stop, OK (interrompo a execução para efetuar configurações necessárias);

g) abrir o httpd.conf com notepad++ no caminho D:winids\apache\conf e no final do arquivo acrescentar as seguintes linhas:

LoadModule php5_module d:\winids\php\php5apache2_2.dll
AddType application/x-httpd-php .php
PHPIniDir d:\winids\php

5. INSTALAÇÃO DO PHP

a) instalar o PHP 5.2.17 em D:\winids\php;

b) copiar o php.ini-dist ali mesmo para php.ini (renomear);

c) abrir o php.ini com notepad++ e alterar as seguintes linhas:

Original: max_execution_time = 30
mudar para: max_execution_time = 60

Original: ;include_path = ".;c:\php\includes"
mudar para: include_path = "d:\winids\php;d:\winids\php\pear"

Original: ; extension_dir = "ext"
mudar para: extension_dir = "d:\winids\php\ext"

Original: ; extension=php_gd2.dll
mudar para extension=php_gd2.dll

Original: ; extension=php_mysql.dll
mudar para: extension=php_mysql.dll

Original: ;date.timezone =
mudar para: date.timezone = America/Sao_Paulo

Original: ;session.save_path = "/tmp"
mudar para: session.save_path = "c:\windows\temp"

6. CONFIGURAÇÃO DO IDS EM MODO DE SERVIÇO

a) no Prompt digitar ‘cd d:\winids\snor\bin’ e executar o comando (sem as aspas):

'snort /SERVICE /INSTALL -c d:\winids\snort\etc\snort.conf -l

d:\winids\snort\log -K ascii -i1’ (1) Interface de rede que está sendo usada;

b) no prompt digito o comando ‘sc config snortsvc start= auto’ para que o snort

permaneça sempre executando.

7. INSTALAÇÃO DO MYSQL

a) Instalar o mysql 5.5.9 em D:\winids\mysql;

b) observar se todos ao pacotes estão na mesma pasta com exceção do **Server**

data files que deve ficar em D:\winids\mysql\datafiles.

7.1 CRIANDO O BANDO DE DADOS WINIDS:

a) inserir os comandos a seguir no prompt (sem as aspas):

'drop database test;' enter
'create database snort;' enter
'create database archive;' enter
'show databases;' enter

7.2 CRIANDO AS TABELAS DO BANDO DE DADOS WINIDS:

a) inserir os comandos a seguir no prompt (sem as aspas):

'connect snort;' enter
'source d:\winids\snort\schemas\create_mysql' enter
'show tables;' enter
'connect archive;' enter
'source d:\winids\snort\schemas\create_mysql' enter
'show tables;' enter

7.3 CRIANDO O BANDO DE DADOS WINIDS COM ACESSO A USUÁRIO:

a) inserir os comandos a seguir no prompt (sem as aspas):

'set password for root@localhost = password('d1ngd0ng');'

'quit;'
'mysql -u root -p'

'd1ngd0ng'

'grant INSERT,SELECT,UPDATE on snort.* to snort identified by 'l0gg3r';'

'grant INSERT,SELECT,UPDATE on snort.* to snort@localhost identified by 'l0gg3r';'

'grant INSERT,SELECT,UPDATE,DELETE,CREATE on snort.* to base identified by 'an@l1st';'

'grant INSERT,SELECT,UPDATE,DELETE,CREATE on snort.* to base@localhost identified by 'an@l1st';'

'grant INSERT,SELECT,UPDATE,DELETE,CREATE on archive.* to base identified by 'an@l1st';'

'grant INSERT,SELECT,UPDATE,DELETE,CREATE on archive.* to base@localhost identified by 'an@l1st';'

'use mysql;'
'select * from user;'

'quit;'

8. INSTALAÇÃO DO ADODB

a) instalar o AdoDB em D:\winids\adodb;

b) extrair o pacote base em D:\winids\apache\htdocs\base;

c) abrir o arquivo base.conf com notepad++ e realizar as configurações a seguir

no prompt (sem as aspas):

'copy d:\winids\apache\htdocs\base\base_conf.php.dist d:\winids\apache\htdocs\base\base_conf.php'
'mkdir d:\winids\apache\htdocs\base\signatures'
'xcopy d:\winids\snort\doc\signatures d:\winids\apache\htdocs\base\signatures\ /Q /Y'

d) Vá até a pasta D:\winids\apache\htdocs\base abra o arquivo base_conf.php com

notepad++ e faça substituas as linhas abaixo:

Original: $BASE_urlpath = '';
mudar para: $BASE_urlpath = 'http://winids';

Original: $DBlib_path = '';
mudar para: $DBlib_path = 'd:\winids\adodb';

Original: $DBtype = '?????';
mudar para: $DBtype = 'mysql';

Original:
$alert_dbname = '?????';
$alert_host = '?????';
$alert_port = '?????';
$alert_user = '?????';
$alert_password = '?????';

mudar para:
$alert_dbname = 'snort';
$alert_host = 'winids';

$alert_port = '';
$alert_user = 'base';
$alert_password = 'an@l1st';

Original:
$archive_exists = 0; # Set this to 1 if you want access to the archive DB from BASE
$archive_dbname = '?????';
$archive_host = '?????';
$archive_port = '?????';
$archive_user = '?????';
$archive_password = '?????';

mudar para:
$archive_exists = 1; # Set this to 1 if you want access to the archive DB from BASE
$archive_dbname = 'archive';
$archive_host = 'winids';
$archive_port = '';
$archive_user = 'base';
$archive_password = 'an@l1st';

Original: $show_rows = 48;
mudar para: $show_rows = 90;

Original: $show_expanded_query = 0;
mudar para: $show_expanded_query = 1;

Original: $portscan_file = '';
mudar para: $portscan_file = 'd:\winids\snort\log\portscan.log';

Original: $colored_alerts = 0;
mudar para: $colored_alerts = 1;

Original: $priority_colors = array
('FF0000','FFFF00','FF9900','999999','FFFFFF','006600');
mudar para: $priority_colors =
array('000000','FF0000','FF9900','FFFF00','999999');

Original: $graph_font_name = "DejaVuSans";
mudar para: $graph_font_name = "Verdana";

Original: //$Geo_IPfree_file_ascii = "/var/www/html/ips-ascii.txt";
mudar para: $Geo_IPfree_file_ascii = "d:\winids\apache\htdocs\base\ips-ascii.txt";

8.1 CRIANDO AS TABELAS DE CONSOLE DE SEGURANÇA DO WINIDS

a) inserir os comandos a seguir no prompt (sem as aspas):

'mysql -u root -p'

'd1ngd0ng'

'connect snort;'

'source d:\winids\apache\htdocs\base\sql\create_base_tbls_mysql.sql'

'show tables;'

'connect archive;'

'source d:\winids\apache\htdocs\base\sql\create_base_tbls_mysql.sql'

'show tables;'

'quit;'

8.2 CONFIGURANDO GRÁFICOS DO CONSOLE DE SEGURANÇA DO WINIDS

a) inserir os comandos a seguir no prompt (sem as aspas):

'cd d:\winids\php'

'go-pear'

b) tecle Enter para instalar ‘System-Wide’;

c) tecle Enter;

d) no "Pressione qualquer tecla para continuar. . . ', pressione qualquer tecla para voltar para o prompt;

e) continue inserindo os comandos a seguir no prompt (sem as aspas):

'pear upgrade-all'
'pear install Image_Color-alpha'

'install ok: channel://pear.php.net/Image_Color-...'

'pear install Image_Canvas-alpha'

'install ok: channel://pear.php.net/Image_Canvas-...'

'install Image_Graph-alpha'

'install ok: channel://pear.php.net/Image_Graph-...'

'pear install Log-alpha'

'install ok: channel://pear.php.net/Log-...'

'pear install Numbers_Roman-alpha'

'install ok: channel://pear.php.net/Numbers_Roman-...'

'pear install Numbers_Words-alpha'

'install ok: channel://pear.php.net/Numbers_Words-...'

'pear install Mail-alpha'

'install ok: channel://pear.php.net/Mail-...'

'pear install Mail_Mime-alpha'

'install ok: channel://pear.php.net/Mail_Mime-...'

'pear upgrade-all'

'copy d:\winids\apache\htdocs\base\world_map6.*
d:\winids\php\pear\image\graph\images\maps'

8.3 CONFIGURANDO O CONSOLE DE SEGURANÇA DO WINIDS

a) inserir os comandos a seguir no prompt (sem as aspas):

'mkdir d:\winids\apache\passwords'

'cd d:\winids\apache\bin'

'htpasswd -c d:\winids\apache\passwords\passwords Console'

b) nas duas próximas perguntas você deve digitar e confirmar a senha ‘pass’,

feche o prompt;

c) abrir com notepad++, o arquivo httpd.conf que está em D:\winids\apache\conf

e efetuar as seguintes mudanças:

Original: DocumentRoot "D:/winids/apache/htdocs"
mudar para: DocumentRoot "D:/winids/apache/htdocs/base"

d) logo abaixo do trecho:

<Directory />
Options FollowSymLinks
AllowOverride None
Order deny,allow
Deny from all
</Directory>

e) Acrescentar as seis linhas:

<Directory "d:\winids\apache\htdocs\base">
AuthType Basic
AuthName "WinIDS"
AuthUserFile d:\winids\apache\passwords\passwords
Require user Console
</Directory>

f) Alterar as próximas linhas:

Original: Options Indexes FollowSymLinks
mudar para: Options -Indexes FollowSymLinks

Original: DirectoryIndex index.html
mudar para: DirectoryIndex base_main.php

g) Reinicie o seu Sistema de Detecção de Intrusão.

APÊNDICE B

ANÁLISE DE SEGURANÇA EM REDES UTILIZANDO O SISTEMA DE DETECÇÃO DE INTRUSÃO SNORT

Priscila Londero Arcaro[1], Rogério Antônio Casagrande[2]

[1]Acadêmica do curso de Ciência da Computação – Unidade Acadêmica de Ciências Engenharias e Tecnologias – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma- SC – Brasil

[2]Professor do curso de Ciência da Computação – Unidade Acadêmica de Ciências Engenharias e Tecnologias – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma- SC – Brasil

priarcaro@gmail.com, roc@unesc.net

Abstract. *The growth of the Internet has facilitated the sharing of resources and information, these information are passed to aggregate a very large value, and to protect them, security strategies began to emerge. Existing threats bring big problems, since many companies and users fail to use the Internet to perform tasks involving the use of personal data and mainly financial. There are currently several techniques used to protect networks and computers, among which we can outstanding the Intrusion Detection Systems The IDSs, for example the Snort, represent means of discovering whether a network or host is the target of unauthorizeds access and enables the generation of security alerts.*

Keywords: *Snort, Intrusion Detection System; Attacks, Threats.*

Resumo. *O crescimento da Internet facilitou o compartilhamento de recursos e informações, estas informações passaram a agregar um valor muito grande, e para protegê-las, estratégias de segurança começaram a surgir. As ameaças existentes trazem grandes problemas, já que muitas empresas e usuários deixam de utilizar a Internet para realizar tarefas que envolvam o uso de dados pessoais e principalmente financeiros. Existem atualmente várias técnicas utilizadas para a proteção de redes e computadores, dentre elas, pode-se destacar os Sistemas de Detecção de Intrusão. Os IDSs, como por exemplo o Snort, representam meios de se descobrir se uma rede ou host está sendo alvo de acessos não autorizados e possibilita a geração de alertas de segurança.*

Palavras chave*: Snort; Sistema de Detecção de Intrusão; Ataques, Ameaças.*

1. INTRODUÇÃO

As redes de computadores surgiram da necessidade de compartilhamento de dados e dispositivos. Este novo panorama traz consigo muitos benefícios às organizações e serviços cada vez mais atraentes aos clientes, além de promover interessantes oportunidades de negócios. Contudo, surgiram também os problemas com segurança, sendo esta um requisito essencial para todo tipo de rede sujeita à presença de intrusos. Paralelamente a essa nova tecnologia surge a necessidade de implantação de mecanismos de segurança não somente corretivos, mas também preventivos.

Para identificar se um computador ou uma rede está comprometida, utilizam-se ferramentas que auxiliam na monitoração das redes, como por exemplo, os *sniffers*. Estes são largamente utilizados por *hackers* para monitorar o tráfego do segmento da rede onde foi instalado, e representam sérias ameaças à segurança, pois "podem comprometer a confidencialidade dos dados em tráfego, além de capturarem qualquer informação em modo texto", como: senhas, dados do usuário, entre outros (CASAGRANDE, 2003, p. 11).

Detectar essas atividades é de suma importância e os Sistemas de Detecção de Intrusão (Intrusion Detection System - IDS) constituem mais uma oportunidade disponível para emissão de alertas à administração da rede na detecção de intrusão. Os IDSs apresentam vantagens, quando bem posicionados podem monitorar grandes redes, além de não interferirem no funcionamento destas, são difíceis de serem percebidos por atacantes e possuem grande segurança contra ataques. Porém, podem falhar em reconhecer um ataque em um momento de tráfego intenso, e não analisam informações criptografadas, sendo este um grande problema, pois a maioria dos atacantes utiliza criptografia em suas invasões. Alguns destes softwares não identificam se um ataque foi bem ou mal sucedido, apenas alertam quando o ataque foi iniciado (PUPO, 2009).

2. SEGURANÇA DA INFORMAÇÃO

Uma rede de computadores, conforme cita Thomé (2000) tem como objetivo disponibilizar meios de acesso, para que usuários em diferentes localidades possam se comunicar. A questão está no compartilhamento de recursos, tais como programas, banco de dados, recursos de transmissão, entre outros.

Devido a esta possibilidade de compartilhamento de informações, a segurança das redes e informações tornou-se crítica, surgindo à necessidade de segurança no compartilhando de informações. Malta (2006) diz que é ampla a possibilidade de que pessoas não autorizadas consigam acesso a informações confidenciais por meio de métodos ilícitos.

3. NORMAS E POLÍTICAS DE SEGURANÇA

Uma política de segurança consiste em inúmeras decisões que em conjunto irão determinar como uma organização ou até mesmo uma pessoa, irá se comportar em relação à esta. De acordo com Lemos (2001) as políticas determinam os limites de tolerância e os níveis de respostas às violações que possam incidir. Estas diferem de uma organização para outra, mas o importante é que toda organização, independente do seu tipo ou tamanho, deve apresentar uma política de segurança bem definida. Segundo Lemos (2001), estas políticas devem ser utilizadas para a manutenção da segurança da informação, e por isso devem ser documentadas e de conhecimento de todos.

A norma ABNT NBR/ISO IEC 27002, é a versão nacional da norma internacional ISO 27002, esta última versão passou a vigorar em 30/09/2005. Ela estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (BRASIL, 2009).

4. TIPOS DE AMEAÇAS

Conforme Franceschinelli (2003) os atacantes podem apresentar comportamentos diferentes em relação às posições de origem e destino das mensagens. O objetivo de um atacante é: **Interromper**, **Interceptar**, **Modificar** ou **Fabricar** mensagens.

Na interrupção o objetivo do atacante é interromper o fluxo de dados que parte da origem, para deixar o destinatário sem receber os pacotes de informações.

Na interceptação o atacante quer ter acesso ao fluxo de dados que está trafegando. Este acesso influencia na confiabilidade das informações.

Na modificação além do atacante ter acesso aos dados, ele também modificá-os para consequentemente enviá-los ao destino. Neste caso, há uma perda na integridade dos dados que foram desrespeitados.

E na fabricação o atacante produz dados para enviar a um destinatário, que não tem como saber quem os enviou. Não há autenticidade na informação enviada.

5. TIPOS DE ATAQUES

A RFC 2828 cita que ataque é uma ação que ameaça a segurança de um sistema, o ataque explora as vulnerabilidades no sistema alvo e muitas vezes, pode não ser bem sucedido.

5.1 Força Bruta

O ataque de força bruta é uma das técnicas mais antigas de invasão, consiste em descobrir o nome de usuário e a senha de um sistema. Para conseguir a senha geram-se todas as combinações possíveis de letras, números e símbolos, geralmente estes ataques são iniciados a partir de logins padrão, como por exemplo, admin, administrador, root. (MACHADO; FREIRE, 2006).

5.2 Portscan

O Portscan consiste em uma varredura de portas e serviços, usado para verificar quais destes estão em execução, geralmente é empregado como primeiro passo para planejar invasões.

6. SISTEMAS DE DETECÇÃO DE INTRUSÃO

Sistemas de Detecção de Intrusão (Intrusion Detection System - IDS) são sistemas de software ou hardware que monitoram eventos ocorridos em um sistema computacional, auxiliando na procura de indícios de problemas de segurança em redes de computadores (SANTOS, 2005).

Conforme Vieira Junior (2002) o IDS detecta e notifica tentativas de invasão, por meio da captura e análise dos pacotes que estão trafegando na rede, procurando identificar evidências

do andamento de um ataque, para posteriormente emitir alarmes ou executar uma ação automática.

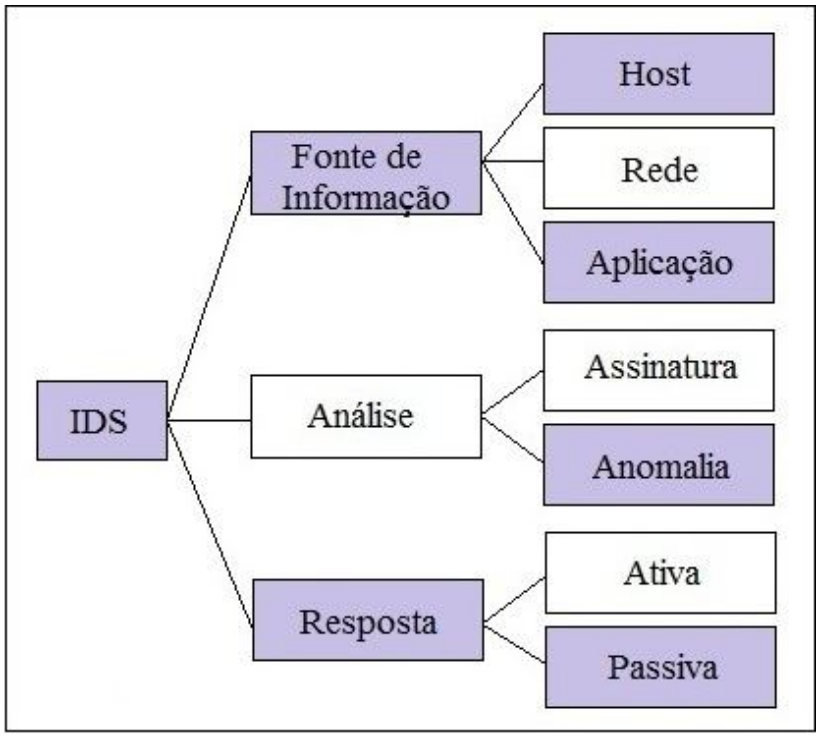


Figura 1. Classificação de um IDS

Os principais tipos de IDSs podem ser descritos em função de 3 componentes essenciais: **Fonte de Informação, Análise e Resposta**.

A Fonte de Informação é quem define se um ataque ocorreu ou não. Esse ataque pode ocorrer em 3 níveis do sistema: **Host, Rede e Aplicação**.

- No Host o IDS atua sobre as informações coletadas sobre estações individuais.
- Na Rede o IDS captura e analisa os pacotes da rede.
- A Aplicação é subconjunto dos IDS baseados em Host, onde o IDS atua sobre os arquivos de logs das transações.

No componente de Análise os eventos provenientes da Fonte de Informação são organizados e classificados, definindo quais mostram que uma intrusão ocorreu. A analise é dividida em 2 níveis: **Assinatura e Anomalia.**

- A detecção baseada em Assinatura é feita por meio de intrusões e vulnerabilidades conhecidas.
- Na detecção baseada em Anomalia, o IDS observa o comportamento do sistema.

O componente de Resposta são as ações que o sistema executa quando detecta uma intrusão.

- A Resposta pode ser Ativa: quando é gerada pelo próprio sistema.
- Ou Passiva: quando são gerados relatórios para que o administrador do sistema tome as medidas que julgar necessárias.

7. SNORT

O Snort é uma ferramenta baseada em rede, desenvolvida por Martin Roesch, seu código é open-source. Esta ferramenta é bastante conhecida devido a fácil configuração de regras e constante atualização no banco de dados de assinaturas. O Snort é leve, pequeno, realiza escaneamentos e verifica anomalias dentro de toda a rede ao qual um computador está inserido (SNORT, 2009).

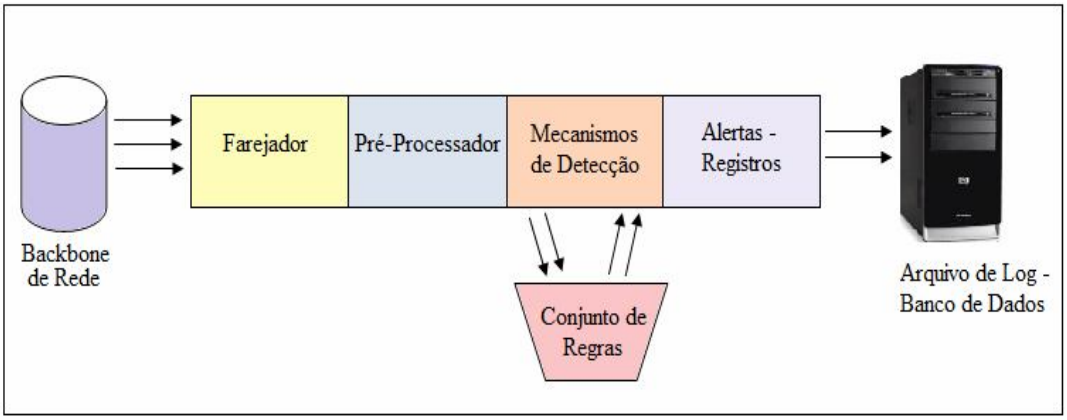


Figura 2. Figura 7. Arquitetura do Snort

Conforme Santos (2005) existem quatro elementos básicos que compõem o Snort: o farejador, o pré-processador, o mecanismo de detecção e os *plugins* de saída. Basicamente, o Snort é um farejador de pacotes, projetado para pré-processar os pacotes capturados e posteriormente comparar esses pacotes com uma série de regras.

No Farejador: o tráfego da rede é obtido por meio da biblioteca Winpcap;

No Pré-Processador: os pacotes são examinados e encaminhados ao mecanismo de detecção.

Mecanismo de Detecção: os pacotes são verificados em relação às regras listadas no arquivo do Snort;

Plugins de Saída: são as respostas geradas pelo Snort.

8. CENÁRIO UTILIZADO PARA REALIZAÇÃO DOS TESTES COM O SNORT

Foram utilizados os seguintes softwares:

j) Sistema Operacional XP Professional (Service Pack 3);
k) WinPcap 4.1.2;
l) IDS Snort 2.9.0.4;
m) MySQL 5.5.9;
n) AdoDB 5.1.1;
o) PHP 5.2.17;
p) Apache 2.2.17;
q) Basic Analysis and Security Engine (BASE) 1.4.5;
r) EventSentry 2.91.0.110.

Para realização dos testes foi utilizado um *hub*, conforme ilustra a Figura 3:

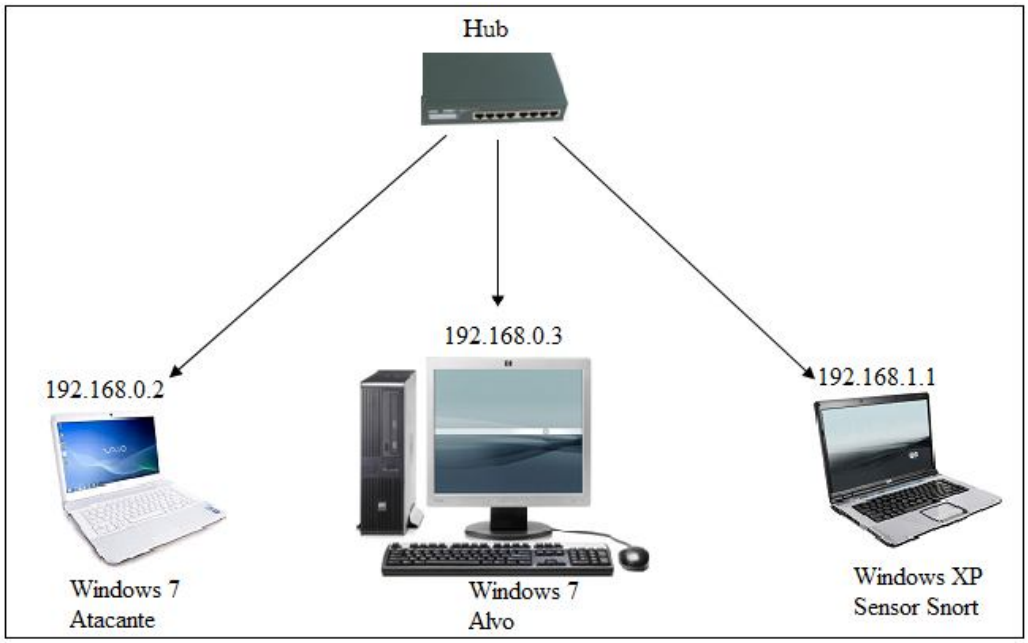


Figura 3. Ambiente Montado para Realização dos Testes

9. TESTE DE EFICIÊNCIA DO SNORT UTILIZANDO A FERRAMENTA NMAP

No primeiro teste, nenhum filtro de assinatura do EventSentry está configurado, isso faz com que o Snort gere um grande número de falsos positivos, ou seja o Snort marca como uma possível tentativa de invasão pacotes que não apresentam risco nenhum aos computadores da rede.

Para minimizar o número de falsos positivos deve-se configurar o filtro do EventSentry com a assinatura do ataque em questão, assim quando o Snort compara a assinatura do EventSentry com a assinatura contida nas suas regras, detecta apenas ataques reais.

Utilizando a ferramenta Nmap, realizou-se a tentativa de execução de um Portscan, a máquina atacante contendo o IP 192.168.0.2, tentou encontrar quais portas e serviços estavam em execução na máquina alvo que continha o IP 192.168.0.3.

A Figura 4 apresenta o Filtro de Portscan habilitado com a devida assinatura configurada e apresenta o alerta gerado na hora da detecção do portscan:

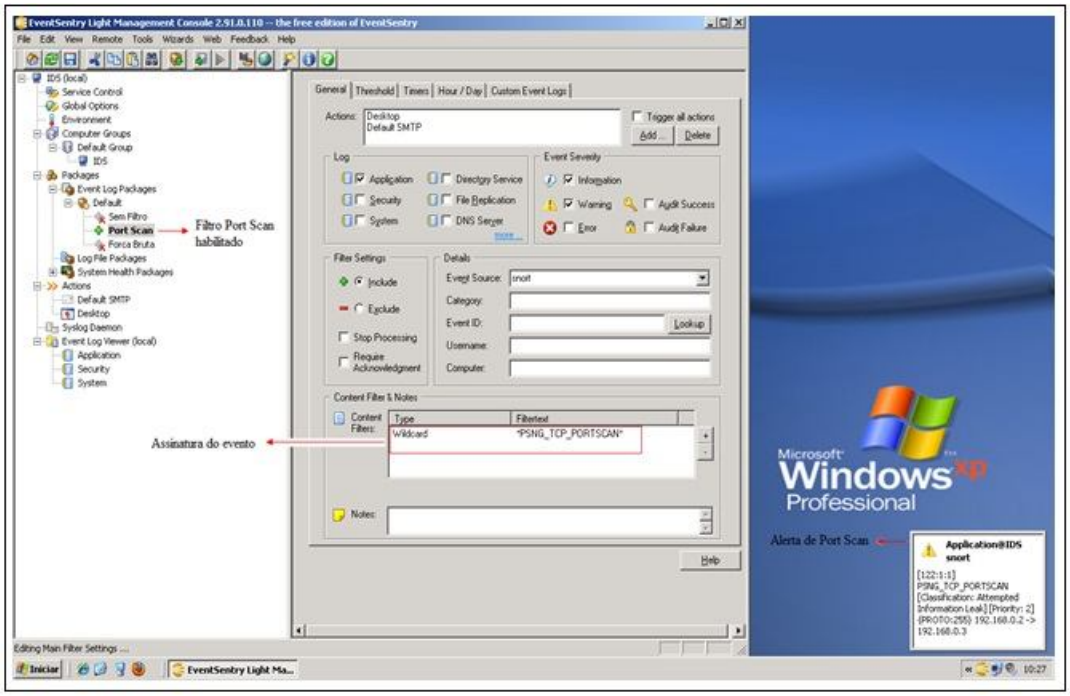


Figura 4. Assinatura do filtro configurada e detecção do Portscan

Além do alerta gerado em forma de pop-up na tela o EventSentry permite que seja configurado uma conta de e-mail para que os alertas também sejam enviados para este e-mail, conforme ilustra a Figura 5:

Figura 5. E-mail Alertando sobre Portscan

Utilizando a ferramenta BASE se pode obter maiores informações sobre os eventos armazenados no MySQL como por exemplo o número de alertas por hora. Também é possível visualizar eventos por data, por protocolo, os 24 últimos alertas ou os 15 últimos alertas.

O BASE também gera gráficos com os dados dos alertas armazenados no MySQL no formato de barra, linha ou pizza, pode-se gerar gráficos de diferentes tipos, como por exemplo, de hora versus número de alertas, dia, mês, Endereço de IP Origem, Endereço de IP Destino, TCP de origem e destino, UDP de origem e destino, país de origem e destino, sensor, assinatura, versus número de alertas.

Todos os ataques de Portscan e Força Bruta foram replicados cinquenta vezes cada, e em todas as tentativas o Snort reconheceu a assinatura e gerou o alerta. A Figura 6 apresenta o gráfico de Porcentagem de Alertas x Ataques:

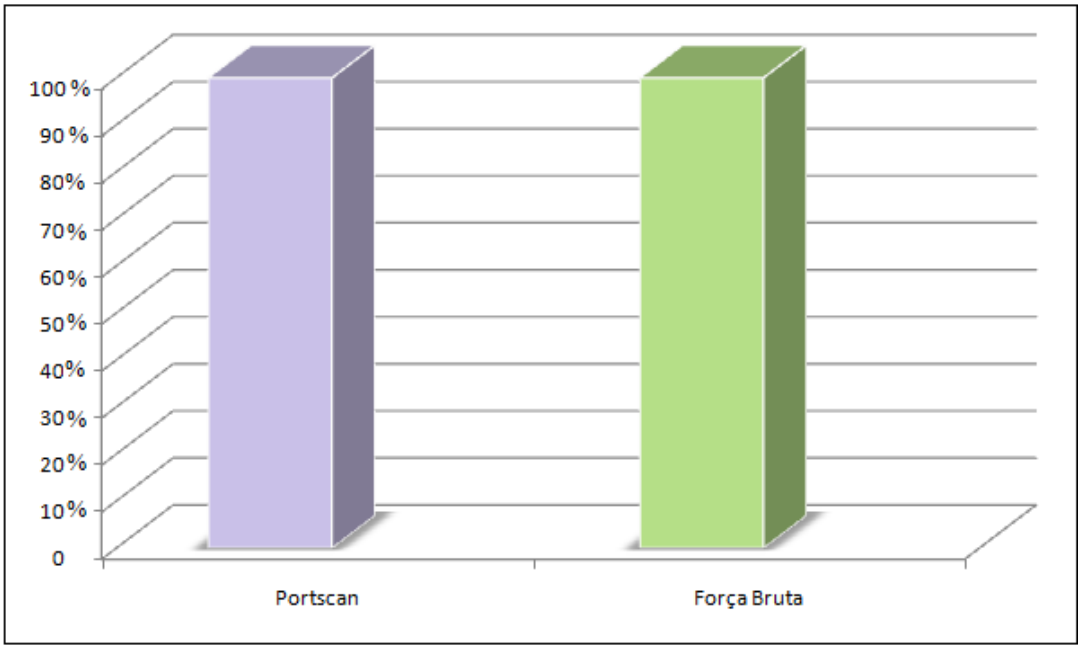


Figura 6. Porcentagem de Alertas Gerados x Ataques

10. CONCLUSÃO

Neste trabalho, foram apresentados conceitos e definidos procedimentos para a instalação e configuração do IDS Snort e de todos os aplicativos auxiliares que compõem a implantação de um IDS na rede, porém não se pode pensar em segurança, sem um trabalho contínuo de atualizações dos aplicativos e das ferramentas utilizadas.

O Snort mostrou ser uma ferramenta bastante poderosa para fornecer segurança a uma rede, constituindo uma ótima alternativa para administradores de rede.

No desenvolvimento deste projeto algumas dificuldades foram encontradas, uma delas foi a falta de documentação em relação à instalação e configuração do IDS Snort no Sistema Operacional *Windows*, a segunda dificuldade foi encontrar quais softwares seriam necessários para que Snort conseguisse gerar os alertas, estas dificuldades foram sanadas através da troca de e-mails com aos mantenedores da comunidade Snort no Brasil, onde estes disponibilizaram um tutorial em inglês que apresentava um exemplo de configuração do Snort e este mesmo tutorial citava o uso de uma ferramenta que em conjunto com o Snort realizada os alertas, o EventSentry.

A partir do EventSentry, o filtro de cada ataque realizado era configurado e continha a assinatura do evento e a medida que se realizava a tentativa de ataque com as ferramentas Nmap e Brutus, habilitava-se o filtro desejado para que o alerta fosse gerado.

Estes alertas são classificados como respostas passivas geradas pelo IDS, ou seja por meio destes alertas são gerados relatórios para que o administrador da rede, baseado nas informações armazenadas, possa tomar as medidas que julgar necessárias, o Snort também pode enviar estas notificações para telefones celulares e e-mail.

Com a implantação do Snort as empresas têm a oportunidade de gerarem uma ação pró-ativa na rede, onde é possível analisar quais são os acessos não autorizados que estão ocorrendo e adotar uma iniciativa para bloquear estes acessos.

REFERÊNCIAS

BRASIL. ABNT. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação.** 2009. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=1532>. Acesso em: 15 set. 2010.

LEMOS, Aline Morais de. **Política de Segurança da Informação.** Rio de Janeiro, 2001. Disponível em: www.estacio.br/campus/millorfernandes/monografias/aline_morais.pdf. Acesso em: 15 set. 2010.

MACHADO, André; FREIRE, Alexandre. **Como Blindar seu PC:** aprenda transformar seu computador numa fortaleza digital. Rio de Janeiro: Elsevier, 2006.

MALTA, Marcelo Alvim. **Detecção de Intrusão em Redes de Computadores.** 2006. 55 f. Trabalho Acadêmico (Bacharel em Ciência da Computação) - Departamento de Computação, Universidade Estadual de Londrina, Londrina/PR, 2006.

SANTOS, Bruno Ribeiro dos. **Detecção de Intrusos utilizando o Snort.** 2005. 91 f. Curso de Administração de Redes Linux, UFLA, Minas Gerais, 2005.

SNORT BR. Disponível em: < http://www.snort.com.br/snort.asp>. Acesso em 12 out. 2009.

TANENBAUM, Andrew S. **Redes de computadores.** Rio de Janeiro: Campus, 2003. 945 p.

THOMÉ, Antonio G. **Comunicação de Dados.** 2000. Disponível em: <http://equipe.nce.ufrj.br/thome/comdados/apostila.pdf>. Acesso em: 01 set. 2010.

VIEIRA JUNIOR, Francisco. **Estudo de Caso em Segurança de Redes usando como Ferramenta de IDS (Intrusion Detection System) o Snort.** São Paulo. 2002.