

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMA DE INFORMAÇÃO**

JULIANO DIEGO DAMÁSIO DE SOUSA BRAGA PONTE

**ESTUDO DE CASO: IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO EM UMA MÉDIA EMPRESA**

JULIANO DIEGO DAMÁSIO DE SOUSA BRAGA PONTE

IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO EM UMA MÉDIA EMPRESA

ESTUDO DE CASO: IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO EM UMA MÉDIA EMPRESA

Monografia de conclusão de curso apresentada ao Centro Universitário do Rio Grande do Norte como requisito final para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Aluizio
Ferreira da Rocha Neto, M.Sc.

BIBLIOTECA UNI-RN

004 P813e - RB: 37278 (M002094)

Título: Estudo de caso : implantação de um ...

Autoria: Ponte, Juliano Diego Damásio de

2012, ex. 1

Catalogação na Publicação – Biblioteca do UNI-RN
Setor de Processos Técnicos

Ponte, Juliano Diego Damásio de Sousa Braga.

Implantação de um sistema de detecção de intrusão em uma média empresa. / Juliano Diego Damásio de Sousa Braga Ponte. – Natal, 2012. 41f.

Orientador: Msc. Prof^o. Aluizio Ferreira da Rocha

Monografia (Graduação em Sistemas de Informação) – Centro Universitário do Rio Grande do Norte.

1. SNORT - Monografia. 2. Segurança da Informação - Monografia. 3. Sistema de Detecção de Intrusão - Monografia. 4. IDS - Monografia. I. Rocha, Aluizio Ferreira da. II. Título.

RN/UNI-RN/BC

CDU 004

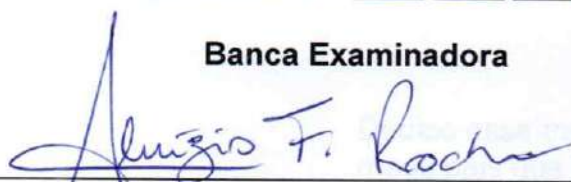
JULIANO DIEGO DAMÁSIO DE SOUSA BRAGA PONTE

ESTUDO DE CASO: IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO EM UMA MÉDIA EMPRESA

Monografia de conclusão de
curso apresentada ao Centro
Universitário do Rio Grande do
Norte como requisito final para
obtenção do título de Bacharel
em Sistemas de Informação.

Aprovado em: ____/____/____

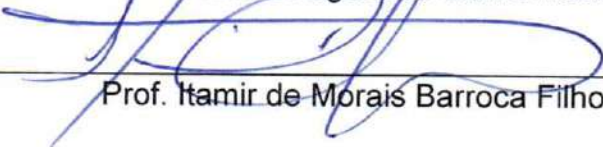
Banca Examinadora



Prof. Aluizio Ferreira da Rocha Neto
Orientador



Prof. Rômulo Fagundes Cantanhede



Prof. Itamir de Moraes Barroca Filho

Dedico esse trabalho primeiramente aos meus pais que me apoiaram em todos os momentos da minha vida, aos meus irmãos que sempre acreditaram em mim e me estimularam a seguir atrás de meus sonhos

RESUMO

Nos dias atuais, constantemente surgem novas ameaças para obtenção de dados confidenciais de uma empresa, ou até mesmo fazer com que algum serviço deixe de funcionar, gerando assim prejuízos incalculáveis para a organização. Com isso, os administradores de redes que são responsáveis pela segurança da informação em uma organização, tem que utilizar as mais atuais ferramentas para a prevenção e proteção contra esses tipos de ameaças, que podem ser tanto externamente, como também um ataque interno. Existem várias ferramentas que atuam auxiliando os administradores de rede nesse sentido, e uma dessas ferramentas é o IDS, do inglês *Intrusion Detection System* ou Sistema de Detecção de Intrusão, que faz um varredura no tráfego de dados que passa pela rede em busca de alguma possível ameaça. Nesse estudo de caso, realizado na SEMARH – Secretária de Estado de Meio Ambiente e Recursos Hídricos, foi utilizado o IDS chamado SNORT, que é um software livre, reduzindo assim os custos, e obtendo um nível de segurança alto.

Palavras Chaves: SNORT, segurança da informação, Sistema de Detecção de Intrusão, IDS.

ABSTRACT

Nowadays, new threats emerge constantly to obtain confidential data from a company, or even make a service stop working, thus generating incalculable damage to the organization. Thus, network administrators who are responsible for information security in an organization, must use the most current tools for prevention and protection against these types of threats, which can be both externally as well as an internal attack. There are several tools that work assisting network administrators in this direction, and one of these tools is the IDS, the English Intrusion Detection System or Intrusion Detection System, which makes a sweep of the data traffic passing through the network in search of some possible threat. In this case study, conducted in SEMARH - Secretaria de Estado e Meio Ambiente e dos Recursos Hídricos, was used IDS called Snort, which is free software, reducing costs, and achieving a high level of security.

Keywords: SNORT, Information Security, Intrusion Detection System, IDS

LISTA DE FIGURAS

Figura 1 – Tela inicial do BASE.....	31
Figura 2 – Tela inicial do BackTrack 5	32
Figura 3 - Tela inicial do OpenVAS	33
Figura 4 - Alertas geradas pelo Snort para o tráfego ICMP destinado ao Servidor...34	
Figura 5 - Cabeçalho da mensagem ICMP	34
Figura 6 - Criação do alvo para ataque no OpenVAS	35
Figura 7 - Criação dos testes de vulnerabilidade no OpenVAS.....	36
Figura 8 - Relatório final gerado pelo OpenVAS	37
Figura 9 - Alertas de escaneamento de portas gerado pelo Snort	37

SUMÁRIO

1	INTRODUÇÃO	10
1.1	OBJETIVOS	11
1.1.1	Objetivos Específicos	11
1.2	ORGANIZAÇÃO DO TRABALHO	11
2	REFERENCIAL TEÓRICO.....	13
2.1	SEGURANÇA DA INFORMAÇÃO.....	13
2.2	TIPOS DE ATAQUES	15
2.1	Explorando vulnerabilidades	16
2.1.1	Varredura na rede	16
2.1.2	Falsificação de E-mail (Spoofing)	17
2.1.3	Interceptação de tráfego (Sniffing)	17
2.1.4	Força Bruta (Brute Force)	17
2.1.5	Desfiguração de página (Defacement)	17
2.1.6	Negação de serviço (DoS e DDoS)	18
2.2	TIPOS DE ATACANTES.....	18
2.2.1	Newbie.....	18
2.2.2	Lamer.....	18
2.2.3	Wannabe	19
2.2.4	Hacker.....	19
2.2.5	Crackers	19
2.2.6	Phreaker.....	20
2.3	SISTEMA DE DETECÇÃO DE INTRUSÃO	21
2.3.1	NIDS (Network Intrusion Detection System).....	22
2.3.2	Formas de detecção de um IDS	23
2.4	O SOFTWARE SNORT	24
2.4.1	Arquitetura e o funcionamento do SNORT	25
2.4.2	Decodificador de Pacotes.....	25
2.4.3	Engenharia de Detecção.....	25
2.4.4	Plugins de saída	26
2.4.5	Regras no SNORT	26
2.4.5.1	Cabeçalho de Regras.....	26
2.4.5.2	Cabeçalho de Opções	28

3	ESTUDO DE CASO - SEMARH	29
3.1	CARACTERIZAÇÃO DA EMPRESA	29
3.2	PORQUÊ DA UTILIZAÇÃO DO SNORT	29
3.3	IMPLEMENTAÇÃO DO SNORT	30
3.4	REALIZAÇÃO DE TESTE	31
3.5	AVALIAÇÃO DO SNORT	33
3.5.1	ICMP	33
3.5.2	Escaneamento de Portas	35
3.5.3	<i>Denial of Service</i>	38
4	CONCLUSÕES	39
	REFERÊNCIAS BIBLIOGRÁFICAS	40

1 INTRODUÇÃO

É praticamente inviável, atualmente, manter em atividade uma empresa sem que esta se utilize, de alguma forma, das vantagens proporcionadas pela tecnologia. E se um sistema não funciona bem ou vem a apresentar falhas importantes para a sua execução, vindo a parar de funcionar, os prejuízos à empresa podem chegar a valores imensuráveis.

Tomando como exemplo, uma grande empresa de fabricação de calçados, que por algum motivo desconhecido, tem problemas com sua rede de computadores, fazendo com que seu equipamento de fabricação dos calçados venha a perder a conectividade da rede, acarretando a paralisação de toda a produção em virtude da perda da comunicação com o servidor de banco de dados (que contabiliza cada unidade confeccionada).

Todo o período de tempo passado desde o momento em que o equipamento fica impossibilitado de fabricar até o momento em que o administrador de redes finalmente soluciona o problema, a empresa terá prejuízos deixando de produzir e atender às demandas do mercado, ou seja, perderá dinheiro. A empresa que tem visão de mercado e trabalha com planejamento estratégico para se manter competitiva e continuar a crescer, entende a importância de investir constantemente na aquisição de novas tecnologias.

Por outro lado, se não for bem administrada em suas potencialidades, a tecnologia utilizada pode ter um efeito reverso, trazendo "dor de cabeça" e complicações ao bom andamento dos processos e atividades desenvolvidas. Basta que algum equipamento da rede pare de funcionar ou algum intruso tenha acesso às informações, vindo a obter dados confidenciais ou prejudicando o seu funcionamento.

Para diminuir as chances de incidentes na rede é importante que o seu administrador tenha um bom conhecimento e saiba como protegê-la desses possíveis ataques, aliado ao desempenho satisfatório dos dispositivos e ferramentas disponíveis. O Snort é um IDS open source é bastante utilizado entre as empresas por ser totalmente gratuito e, ao mesmo tempo, ser uma ferramenta completa.

1.1 OBJETIVOS

Esse trabalho de conclusão de curso de bacharelado em Sistema de Informação tem como objetivo mostrar as funcionalidades de um IDS, e ajudar um administrador de redes na implementação dessa ferramenta, e para os estudantes e amantes de informática que querem conhecer um pouco mais sobre o mundo da segurança da informação e suas ferramentas. O IDS utilizado foi o Snort que foi instalado em uma máquina física com o sistema operacional Linux Debian.

O principal objetivo para a realização desse trabalho foi adquirir o conhecimento na implementação dessa poderosa ferramenta, já que hoje em dia cada vez mais temos que nos preocupar com a segurança nas empresas. E para servir como fonte de estudos para quem deseja ter mais conhecimento, ou até mesmo realizar a implementação em sua empresa.

1.1.1 Objetivos Específicos

- Fonte de conhecimento para estudantes ou profissionais da área que queriam implementar o Snort;
- Para atender futuras necessidades na infraestrutura de rede da organização SEMARH;
- Adquirir conhecimento para utilizar em minha vida profissional;
- Descrever a configuração de uma ferramenta de pentest que nesse trabalho foi utilizada a ferramenta OpenVAS.

1.2 ORGANIZAÇÃO DO TRABALHO

O presente trabalho está organizado da seguinte forma:

- O capítulo 1 fala sobre a introdução e a importância da segurança da informação na empresa;
- O capítulo 2 aborda o conceito de segurança da informação e o quanto essa informação precisa estar protegida para fornecer disponibilidade, integridade e confidencialidade ao cliente;

- A seção 2.2 fala sobre os tipos de ameaças mais comuns que um administrador de redes enfrenta;
- A seção 2.3 fala sobre os tipos de atacantes também conhecidos como hackers, e como eles são classificados;
- A seção 2.4 fornece uma visão geral sobre o que é um Sistema de Detecção de Intrusão, os tipos e cada função dos IDS que existem no mercado, e suas formas de detecção;
- A seção 2.5 faz o estudo sobre o Sistema de Detecção de Intrusão chamado Snort, assim como sua arquitetura e funcionalidade. É dada uma explicação de como criar novas regras específicas para cada necessidade.
- O capítulo 3 fala sobre a implantação da ferramenta Snort na organização SEMARH, junto com a implementação e os testes realizados em cima dessa ferramenta.

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a proteção dos dados para que estes não sejam modificados ou acessados sem autorização. Essas informações podem ser tanto de um indivíduo como de uma empresa. Assim como acontece no mundo real em que uma casa precisa estar bem protegida, e isto se dá através de portas, janelas, grades e outros métodos que o proprietário encontra para manter o seu bem seguro, o mesmo ocorre no mundo virtual. Em "Segurança de Redes em Ambientes Cooperativos", Emilio Nakamura e Paulo de Geus demonstram a importância de manter o ambiente virtual seguro dos hackers e de outros tipos de ameaça:

"A necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios" (p.25,2012)

A segurança da informação faz parte da tecnologia da informação e seus diversos usos pelas empresas, sendo adequada à natureza e necessidade de cada organização. A globalização e disputa por novos mercados cresce a cada dia, e quem sabe manter suas estratégias e informações seguras pode torna-se mais competitivo e preparado para as oportunidades que surgem e exigem tomadas de decisões rápidas e eficientes. Portanto, a infraestrutura da tecnologia, se usada adequadamente, pode ser uma aliada para o sucesso corporativo, contribuindo para a evolução dos negócios. As parcerias e comunicação entre as empresas e suas filiais, clientes, distribuidores e outros protagonistas destas redes de negócios trazem como consequência uma maior complexidade de cuidados e medidas a serem tomadas para manter suas informações seguras. Sobre isto, dizem Nakamura e de Geus: "A segurança em ambientes cooperativos será o resultado de esforços para entende o ambiente e as tecnologias, saber como utilizá-las e implementá-las de modo correto", (2012,p.41).

São três as características da segurança da informação que visam à proteção desses dados:

- **Confidencialidade:** Somente pessoas autorizadas tem acesso aos dados determinado pelo proprietário da informação.
- **Integridade:** Protege contra alterações indevidas, mantendo assim toda sua característica original.
- **Disponibilidade:** As informações estarão disponíveis em sua maior parte do tempo e quando necessário.

•

Para Nakamura e de Geus, a confiabilidade é uma quarta propriedade ligada diretamente às demais características da segurança da informação, adequada e eficaz, como vemos a seguir:

"A confiabilidade, integridade e disponibilidade dessa estrutura de rede passam, assim, a ser essenciais para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. A proteção visa, sobre este ponto de vista, a manutenção do acesso às informações que estão sendo disponibilizadas para o usuário. Isso significa que toda a informação deve chegar aos usuários de uma forma íntegra e confiável. Para que isso aconteça, todos os elementos da rede por onde a informação flui até chegar ao destino, devem estar disponíveis, e devem preservar a integridade das informações" (2012, p.44)

A segurança na rede de computadores não está associada apenas à utilização de ferramentas computacionais, fazendo a segurança lógica das informações, mas também precisa que os dados sejam protegidos fisicamente, não permitindo acesso de pessoas não autorizadas em setores que o acesso é restrito, onde o mesmo pode ter acesso a um servidor, podendo roubar, alterar, apagar as informações contidas nele, ou até danificar o equipamento para que alguns serviços parem de funcionar.

As informações precisam ser guardadas em um lugar seguro em forma de backup, para caso aconteça algum desastre no local, os dados não sejam completamente perdidos. Outra solução para esse tipo de problema é a utilização de salas cofres, que são salas preparadas para em caso de desastres como terremoto, incêndios os dados permaneçam intactos não sendo afetado por esses fatores externos, mas esse tipo de solução custa valores muito altos, sendo somente acessível para empresas de grande porte.

A decisão da Política de Segurança a ser adotada, ou seja, o conjunto de norma, métodos e procedimentos que promovam a segurança da informação, deve ter uma visão técnica e criteriosa, além de difundida para todos os usuários e com o perfil da empresa em que ela é utilizada. Como dizem Fernando Ferreira e Márcio de Araújo em "Política de segurança da informação: guia prático para elaboração e implementação"

"A política, preferencialmente, deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evita reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade" (2008, p.37)

Por fim, há outra questão também a ser pensada quando se fala em segurança dos dados, como explica Carlos Morimoto em "Redes: guia prático":

"(...) usamos cada vez mais tecnologias diferentes de acesso e transmissão de dados, o que torna manter sua rede segura uma tarefa mais complicada. Por exemplo, sua rede pode ser bastante segura contra invasões 'diretas', via internet, graças ao *firewall* ativo no *gateway* da rede, mas ser ao mesmo tempo muito fácil de invadir através da rede wireless, caso você utilize o WEP ou simplesmente deixe a rede aberta, sem encriptação". (2009, p.389)

2.2 TIPOS DE ATAQUES

Os *hackers* possuem vários mecanismos a seu favor, atingindo diferentes alvos e com diferentes objetivos, tanto com o objetivo de obter vantagens de cunho financeiro ou não, ou apenas por diversão, ou ainda, como forma de provar seu poder e capacidade técnica para invadir um sistema. Quanto mais difícil for o acesso ao alvo, maior será a prova de sua habilidade. Sobre isto, explicam Nakamura e de Geus:

"As invasões aos sistemas podem ser executadas por meio da exploração de técnicas que podem ter como base, a engenharia social ou invasões técnicas. Essas invasões exploram deficiências na concepção, implementação, configuração ou no gerenciamento dos serviços e sistemas, e continuarão existindo na medida em que o mercado é centrado nas características dos produtos, e não na segurança" (2012, p.80)

Os ataques geralmente acontecem ou são facilitados a partir de "brechas" existentes em algum dos níveis de proteção de informação, ou seja, é

importante que em cada um destes haja uma segurança "hermética", completa. Isto porque o hacker precisa apenas de uma "janela" de vulnerabilidade para ter acesso concreto à informação que procura. O profissional de segurança precisa fechar todas estas "brechas" que naturalmente facilitam os ataques.

2.1 Explorando vulnerabilidades

Para Claudemir da Costa Queiroz, 2007:

"uma vulnerabilidade corresponde a um ponto fraco que possui características inerentes ou falhas que estão associadas a um bem material ou a seu ambiente. O que pode permitir um comprometimento ao ambiente ou a um dado bem. As vulnerabilidades são desencadeadas ou atacadas de forma intencional ou por acontecimento fortuito. Uma vulnerabilidade pode ser uma simples fraqueza ou uma série de pontos fracos que acabam permitindo uma ou várias ameaças. Uma ameaça usa uma ou mais vulnerabilidades para afetar a confidencialidade, a integridade e/ou a disponibilidade de um bem." (p.22)

Ou seja, vulnerabilidades são falhas em programas, equipamentos de redes, em serviços que quando descoberto por um atacante pode ocasionar vários tipos de ações, como deixar um serviço inacessível, acessar informações confidenciais, dentre outros. Vale relacionar, a seguir, os principais ataques às informações do ambiente virtual, conforme informações do Cert.br (renomado site do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil):

2.1.1 Varredura na rede

Tem como objetivo a varredura na rede de computadores em busca de informações dos ativos de rede, sendo informações de qual sistema operacional aquela máquina utiliza, quais programas e serviços estão rodando nela, com isso o hacker pode procurar possíveis vulnerabilidades através dessas informações coletadas. Esse tipo de técnica é utilizada pelos administradores de redes a fim de procurar possíveis falhas na sua rede, e ao descobrir essas falhas tentar corrigi-las antes que algum atacante descubra primeiro.

2.1.2 Falsificação de E-mail (Spoofing)

É uma técnica onde os *hackers* alteram o cabeçalho de um e-mail, dando a impressão que esse e-mail foi enviado de uma origem, mas na verdade foi enviado de outro lugar. Normalmente é usada essa técnica para a propagação de arquivo malicioso, envio de spam ou obtenção de dados pessoais.

2.1.3 Interceptação de tráfego (Sniffing)

Consiste em o atacante usar programas específicos como Wireshark, Microsoft Network Monitor, dentre outros, para fazer a captura e inspeção dos tráfegos em uma rede de computadores. Assim como a varredura de rede, essa técnica pode ser também utilizada pelo administrador de redes para detectar problemas, analisar o desempenho da sua rede ou procurar possíveis ameaças.

2.1.4 Força Bruta (Brute Force)

Um ataque de força bruta é a tentativa forçada para a descoberta por tentativa e erro de um usuário e senha para obter privilégios que esse mesmo usuário. Hoje em dia é uma técnica muito utilizada em casas ou empresas que tem internet sem fio, e esses atacantes usam ferramentas de *brute force* para ter acesso à internet de terceiros. Outro problema que esse tipo de ataque gera, é que muitos serviços hoje em dia bloqueia a conta do usuário caso ele erre a senha em certa quantidade de vezes, inutilizando assim aquela conta, até que o usuário verdadeiro desbloqueie.

2.1.5 Desfiguração de página (Defacement)

Consiste em modificar o conteúdo de uma página Web, normalmente a página principal onde tem maior visibilidade, como forma de protesto, ou até mesmo para vangloriar-se diante os outros hackers ou para os administradores de sistemas, provando que conseguiu acessar aquele sistema.

2.1.6 Negação de serviço (DoS e DDoS)

A negação de serviço é uma técnica onde o hacker tenta derrubar a operação de um serviço no caso DoS (*Denial of Service*) se esse ataque for provido de somente um atacante, no caso de um ataque onde vários computadores estão participando é chamado de DDoS (*Distributed Denial of Service*) ou Negação de Serviço Distribuído.

O objetivo desse tipo de ataque não é ter acesso às informações restritas, mas fazer com que um serviço pare de funcionar, gerando assim prejuízo enormes para a empresa, como recentemente grupo de hackers fizeram ataques diários a grandes bancos no Brasil, fazendo com que o serviço fosse impossibilitado de ser acessado por milhares de pessoas, gerando assim um prejuízo incalculável, já que o banco perde também com futuros clientes que deixam de utilizar esse serviço pela insegurança causada.

2.2 TIPOS DE ATACANTES

No livro "Universidade H4ck3r", 2004, Henrique Ulbrich e James Valle trazem os principais tipos de atacantes que podem agir contra a segurança da rede:

2.2.1 Newbie

O termo vem do inglês e significa alguém que é iniciante em alguma coisa, seja no ramo da informática ou em um curso de língua estrangeira, por exemplo. A tradução mais próxima do português para esse termo seria "calouro", "novato". Especificamente na área da informática, é o usuário que está iniciando seus conhecimentos em computação.

2.2.2 Lamer

É um *newbie* que aprendeu a usar alguns programas disponibilizados na internet para prejudicar outros usuários, como por exemplo, invadindo seu

computador pessoal, expulsando-o de salas de bate-papo, dentre outros. Eles não sabem como o ataque funciona, sabendo somente como operar o programa. Lamer em português literal, quer dizer manco ou aleijado.

2.2.3 Wannabe

Palavra utilizada nos anos 80 para os fãs da cantora Madonna, que tentavam se vestir e ser igual ela. Esse termo foi adaptado para a informática que seria o indivíduo que quer ser um *hacker*, mas não tem a mínima ideia de como fazê-lo.

2.2.4 Hacker

Inicialmente essa palavra era utilizada para denominar pessoas que faziam móveis usando machados. Nos anos 60, a palavra passou a ser utilizada para denominar pessoas que tinham um conhecimento avançado em programação ou especialistas em computação. Hoje, depois que a mídia popularizou o termo, de forma equivocada, passou a ser usado para identificar pessoas que detêm o conhecimento em invasão e utilizam esse conhecimento para prejudicar. Essa é uma definição errada, uma vez que esse conhecimento nem sempre é utilizado para prejudicar alguém ou algo, mas através de seu ataque, por exemplo, pode apenas querer chamar a atenção da empresa ou usuário sobre a insegurança no sistema.

2.2.5 Crackers

É a versão *hacker* voltada para fazer o mal. Utiliza seu conhecimento para tirar proveito ou prejudicar os outros. Procuram formas de burlar os serviços ou programas que são disponibilizado de forma paga, para utilizá-los de forma gratuita, técnica popularmente chamada de "pirataria". São responsáveis por atos de vandalismo e roubos de informações como conta e senha de contas de banco, e-mail, entre outros.

2.2.6 Phreaker

São os *crackers* especializados em sistemas telefônicos, tem tanto conhecimento eletrônico como de telefonia, fazendo chamadas sem pagar por elas.

2.3 SISTEMA DE DETECÇÃO DE INTRUSÃO

Com a expansão da internet cresceu também o aumento de ataques e os tipos e maneiras que eles são realizados. Um forte ataque é capaz de paralisar os serviços de uma empresa, por isso é preciso, às vezes, um grande investimento para implementar uma boa segurança, não bastando a simples prevenção para garantir a continuidade de um serviço. Essa é uma das funções do IDS- Sistema de Detecção de Intrusão. O IDS é um conjunto de meios técnicos para descobrir em uma rede de computadores, acessos não autorizados, podendo agir de duas maneiras.

A primeira delas é somente alertando as tentativas ao responsável, ou da segunda forma que é agindo ao perceber alguma tentativa de invasão, aplicando as ações necessárias contra o ataque. Para Oscar Abreu, em "Implementação de um Sistema de Detecção de Intrusão em uma Pequena Empresa Utilizando Máquinas Virtuais", 2008, os sistemas IDS's:

"(...) são essenciais em políticas de segurança, e colaboram para a resposta de incidentes através de alertas emitidos pela detecção de tentativas de invasão. As decisões dos IDS's baseados em assinaturas de ataques são tomadas a partir de informações obtidas de comportamentos dos atacantes na rede. Isso é possível, pois essas ferramentas de segurança são capazes de analisar os tráfegos de entrada e saída de uma rede, ou dados locais de uma máquina na qual é executado, procurando tentativas de ataques de diversas naturezas."

A intrusão é um conjunto de ações que tentam comprometer a integridade, confiabilidade, ou disponibilidade do sistema, podendo ser um ataque de fora ou da própria base. Segundo Pedro Soares Figueiredo, 2010 a intrusão:

"(...) diz respeito a atividades realizadas com o intuito de comprometer a integridade, disponibilidade ou confidencialidade dos dados do sistema. Integridade é um aspecto que diz que, se o sistema é seguro, a informação contida em um conjunto de dados não deve ser destruída nem corrompida, e desta forma, o sistema funciona corretamente; disponibilidade diz que, se o sistema é seguro, há garantia permanente de recursos ou de serviços sempre que estes forem requisitados por um usuário, e confidencialidade diz que as informações contidas nos dados só devem estar disponíveis para aqueles que realmente possuem autorização para acessá-los."

E o intruso é como um personagem que ingressa na rede sem permissão.

As modalidades de IDS estão divididas em três categorias: HIDS, NIDS e WIDS, cada um realizando uma função específica. O primeiro que vamos falar é o HIDS – Host Intrusion Detection System, é um tipo de IDS que é instalado em uma máquina host, monitorando individualmente as atividades de um computador ou servidor. O segundo é o NIDS – Network-based Intrusion Detection System, que é a modalidade mais utilizada hoje em dia pelas empresas, diferente do HIDS ele monitora as atividades realizadas em toda a rede de computadores, buscando padrões que possam caracterizar um ataque, e quando é detectado alguma ameaça, ele pode alertar ou tomar alguma ação programada. Por último vamos falar do WIDS – Wireless Intrusion Detection System, que não é muito utilizado nas empresas, mas cada vez mais está ganhando espaço nas empresas, onde cada dia que passa os números de redes sem fio cresce e a necessidade de manter uma rede wireless segura também. Seu mecanismo é semelhante ao NIDS, mas com a diferença de que é voltado para a segurança da rede sem fio.

As principais funcionalidades do IDS é fazer um monitoramento na rede coletando as informações, fazendo assim a identificação de suas origens. Assim que é encontrado algum pacote suspeito, ele é analisado por métodos de assinatura de ataque ou detecção de anomalias, e por último a ferramenta vai tomar alguma atitude em relação à ameaça detectada.

2.3.1 NIDS (*Network Intrusion Detection System*)

Algumas das características devem ser observadas na implantação de um IDS em uma empresa: a sua execução constante com a mínima intervenção humana para seu funcionamento; ser tolerante a falhas, tendo em redundância sua base de conhecimento, caso o primeiro venha a falhar, o outro assume; resistente às tentativas de alterações de sua base, no caso de um intruso tentar modificar as regras do IDS, para não reconhecer aquela ação como uma invasão; ter o mínimo de impacto no funcionamento da rede, para que consiga coletar as informações necessárias para que possa repassar para o Proxy ou firewall; Poder detectar mudanças no funcionamento da rede;

Os tipos de erros emitidos pelo IDS são categorizados em falsos positivos, falsos negativos e erros de subversão. O falso positivo é quando a ferramenta coloca uma determinada ação como um possível ataque, mas na verdade não passa

de um tráfego normal na rede, como exemplo um usuário que tentou acessar sua máquina, mas digitou a senha errada várias vezes. Falso negativo acontece quando IDS não consegue detectar uma ação maliciosa, como exemplo um intruso que tem acesso à senha de um funcionário, e que acessa a máquina dela realizando uma invasão. Os erros de subversão ocorrem quando o hacker modifica as configurações do IDS principalmente sua base de conhecimento, com intuito de passar despercebido pela ferramenta.

Existe a necessidade de minimizar o máximo o número de falso positivo, já que eles são bastante prejudiciais para a empresa, tendo o gasto de tempo e de pessoas para analisar falsas ameaças que não comprometem em nada o sistema. Diferente dos erros de falsos negativos que passam despercebidos pelo IDS, e quando descobertos o problema está bem maior, gerando enormes prejuízos para a empresa.

2.3.2 Formas de detecção de um IDS

As formas do IDS detectar uma ameaça em uma rede são feitas de duas maneiras: Análise baseada em assinatura de ataque e análise baseada em comportamento.

Detecção baseada em assinatura analisa os pacotes procurando padrões de ataques com os que são cadastrados em sua base de conhecimento, funcionando como acontece nos antivírus, no caso ao invés de assinaturas são utilizadas vacinas, que fazem a prevenção para cada tipo de vírus determinado. Uma de suas vantagens é que gera poucos falsos positivos, pois os ataques já são conhecidos pela ferramenta, tomando as medidas estabelecidas pelo administrador de redes. E sua desvantagem é que em casos de ataques não conhecidos, o IDS não vai detectar essas ameaças, tendo que ter sua base de conhecimento atualizado constantemente.

Detecção baseada em comportamento determina se tal ação é uma ação maliciosa de acordo com os desvios de padrões em uma rede de computadores, causando dois desafios para quem o administra, uma é determinar se certa ação é padrão ou não, e a outra é como melhor detectar esses tipos de desvios. Primeiramente quando se é utilizado dessa forma é preciso que tenha um período

de reconhecimento do ambiente que a ferramenta vai ser implementada, coletando assim informações dos usuários e aprendendo os comportamentos normais de cada um deles. Para a utilização do IDS nessa modalidade é preciso que a ferramenta seja bem configurada, pois esse tipo de detecção gera muitos falsos positivos e seus resultados são difíceis de ser interpretado.

O IDS possui dois modelos de utilização, em modo passivo ou modo reativo, no primeiro modo o IDS, ao detectar um tráfego malicioso, ele irá enviar uma mensagem de alerta para o administrador de redes, não realizando nenhum procedimento em relação ao ataque. No segundo modo, reativo, em um IDS configurado dessa maneira, ao detectar um tráfego malicioso, além de enviar uma alerta para o administrador de redes, ele tem ações pré-definidas para atuar em relação ao ataque.

2.4 O SOFTWARE SNORT

O "Snort" é um sistema de detecção de intrusão para rede (NIDS) de código aberto, desenvolvida em linguagem C, tanto para plataforma Linux como para Windows, e sua primeira versão foi disponibilizada em dezembro de 1998, desenvolvida por Martin Roesch. Esta ferramenta, segundo Oscar Abreu (2008), oferece para o profissional de segurança, informações que ajudam na tomada de decisões em uma empresa: quando há a suspeita de um ataque:

"(...) o mesmo realiza uma análise metódica do tráfego gerado pela rede. Este software é capaz de inspecionar o payload (área que contém os dados) do pacote, verificando as correspondências entre os conteúdos destes com as suas assinaturas de ataques. Esta ferramenta de detecção de intrusão é considerada bem completa, pois possui uma base com milhares de assinaturas de ataques desenvolvidas tanto pela SourceFire quanto pela comunidade de usuários do Snort"

Seu desenvolvedor, Martin Roesch, deixou disponível o código-fonte do Snort, o que ajudou a popularizá-lo, podendo ser baixado por qualquer usuário interessado para testá-lo e modificá-lo para implementar sua utilização.

2.4.1 Arquitetura e o funcionamento do SNORT

É preciso habilitar a placa de rede do computador em que foi instalado o Snort para trabalhar em modo promíscuo, permitindo que os pacotes trafegados sejam capturados e analisados para descobrir algum evento malicioso na rede. Através das regras que são assinaturas de ataque conhecida, é possível detectar desvios de comportamentos, e enviar alertas em tempo real.

A arquitetura do Snort consiste em:

- Decodificador de pacotes;
- Engenharia de detecção;
- Plugins de saída.

2.4.2 Decodificador de Pacotes

A função do decodificador de pacotes é capturar os pacotes usando a biblioteca libpcap do nível da camada de dados, subindo até a camada de transporte, e finalmente chegando à camada de aplicação. Sendo possível analisar os pacotes tanto em redes ethernet, SLIP (Serial Line Internet Protocol) e PPP (Point-to-Point Protocol)

2.4.3 Engenharia de Detecção

Os pré-processadores fazem a checagem dos pacotes podendo permitir, modificar ou descartar o mesmo, antes que passem para o mecanismo de detecção, diminuindo as quantidades de alertas, e juntamente os números de falsos positivos e falsos negativos.

O Snort possui duas listas uma com o Cabeçalho de Regras (Chain Headers) que contém as características comuns das regras e o Cabeçalho de opções (Chain Option) que contém os padrões de ataque que serão pesquisados junto aos pacotes capturados, e a ação que a ferramenta deve utilizar.

O banco de regras do Snort precisa ser atualizado constantemente, já que cada dia surge novos tipos de ameaças.

2.4.4 Plugins de saída

Agora que os pacotes já passaram pelo mecanismo de detecção, é preciso saber que ações o IDS deve tomar sobre aquela ameaça, podendo enviar uma alerta aos responsáveis ou até mesmo tomar uma decisão imediata. O Snort pode utilizar o protocolo SMNP para enviar alertas para o sistema de gerenciamento de redes, ou atualizar o firewall inserindo novas condições para aquela ameaça.

2.4.5 Regras no SNORT

A ferramenta Snort utiliza a detecção de intrusão baseada em regras, com isso o Snort deve ser alimentado com regras que vão de acordo com a política de segurança da organização.

Por questão de organização, as novas regras criadas devem ser nomeadas de forma alto explicativa e em um arquivo específico para cada tipo de situação, como por exemplo, a criação de um arquivo para escaneamento de porta, devemos então criar um arquivo com o nome port-scan.rules

Exemplo de uma regra criada para o Snort:

- **alert TCP any any -> any any (msg: "É um pacote TCP");)**

O que está antes dos parênteses é considerado o cabeçalho de regras (Chain Headers), e o que está dentro dos parênteses é considerado cabeçalho de opções (Chain Option), nesse exemplo será enviado um alerta para qualquer pacote que entre na rede que utilize o protocolo TCP.

2.4.5.1 Cabeçalho de Regras

Aqui se define de que maneira as informações do pacote capturado devem ser analisadas. Sendo dividido em cinco partes, que são elas:

- Ação da regra;
- Protocolo utilizado;

- Operadores de direção;
- Informações da origem do pacote;
- Informações do destino do pacote;

O administrador precisa classificar essas alertas de acordo com a sua importância, e gravidade, podendo somente registrar essas ameaças em logs no sistema.

As regras que podem ser tomadas pelo snort são as seguintes:

- **Activate:** ela gera um alerta e depois inicia a regra dinâmica específica;
- **Dynamic:** Essa regra fica inativa até que uma regra Activate a ative;
- **Alert:** Registra o pacote e depois alerta ao usuário;
- **Pass:** Ignora esse pacote;
- **Log:** Registra o pacote, não enviando uma alerta.

Aqui estou mostrando um exemplo de uma regra criada utilizando o log, onde o mesmo só vai registrar o pacote, não tomando nenhuma atitude:

- **log tcp 10.0.0.10 any -> 10.0.0.55/24 22 (msg:"SSH");**

Nesse exemplo a cima, estamos especificando uma regra de log, com o endereço de origem 10.0.0.10 com destino ao range de rede de 10.0.0.55 com máscara de rede 255.255.255.0, onde toda vez que o dispositivo de origem tentar acessar aquele range de rede utilizando o protocolo SSH (porta 22), ele irá gerar um log.

- **log tcp [10.0.0.10, 10.0.0.20] any -> 10.0.0.55/24 80 (msg:"tráfego Web");**

Nesse exemplo a cima, estamos especificando um range de endereços de origem separados por vírgula e entre colchetes.

- **log tcp any any -> 10.0.0.10/24 1:1024**

Nesse exemplo a cima, estamos especificando um range de portas, então ele irá criar um log para todos os pacotes TCP de qualquer origem para a rede 10.0.0.10 com máscara 255.255.255.0 em qualquer porta entre 1 até 1024.

- **log udp any any -> 10.0.0.10/24 !53**

Nesse exemplo a cima, estamos criando um log para qualquer pacote UDP de qualquer origem com destino a rede 10.0.0.10 com máscara 255.255.255.0, e que seja qualquer porta diferente da porta 53, que usada para serviços de resolução de nomes (DNS).

2.4.5.2 Cabeçalho de Opções

São definidas depois do cabeçalho de regras dentro dos parênteses, fazendo identificação de ataques mais complexos. As quatros categorias são:

- **Meta-data:** Fornecem informações personalizadas sobre as regras;
- **Non-Payload Detection:** Levam em consideração somente os dados dos cabeçalhos dos pacotes;
- **Payload Detection:** Leva em consideração os dados contidos nos pacotes e permitem fazer correlações entre eles;
- **Post-Detection:** São opções utilizadas depois que acontece um reconhecimento de um evento malicioso

3 ESTUDO DE CASO - SEMARH

3.1 CARACTERIZAÇÃO DA EMPRESA

As atividades desse órgão tiveram início em 25 de fevereiro de 1996 com a SERHID – Secretaria de Estado dos Recursos Hídricos e em 31 de janeiro de 2007 passou a funcionar como SEMARH – Secretaria de Estado e Meio Ambiente e dos Recursos Hídricos.

Essa secretaria é responsável pela gestão dos recursos hídricos e do meio ambiente no estado do Rio Grande do Norte. São órgãos vinculados à SEMARH, o IGARN – Instituto de Gestão das Águas no Rio Grande do Norte, a CAERN – Companhia de Água e Esgoto do Rio Grande do Norte, e o IDEMA – Instituto de Desenvolvimento do Meio Ambiente.

O parque tecnológico da SEMARH dispõe de mais de 100 máquinas com o sistema operacional Windows XP, um servidor Windows Server 2003 criando o domínio da rede SEMARH, trabalhando paralelo a ele, temos um servidor Linux que roda o Iptables e Squid fazendo a função de firewall e proxy da rede, entre vários outros dispositivos como impressoras, scanners, Xerox.

3.2 PORQUÊ DA UTILIZAÇÃO DO SNORT

O Snort é o IDS mais utilizados nas empresas combinando simplicidade e eficiência, foi desenvolvido por Martin Roesch e é disponibilizado de forma gratuita já que é uma ferramenta de código aberto. E uma de sua grande vantagem em relação aos outros IDS disponíveis é que ele tem uma grande variedade de assinaturas de ataques, e essas assinaturas são atualizadas rapidamente assim que é conhecida uma vulnerabilidade nova.

A sua grande comunidade que existe hoje auxiliam bastante nas buscas de informações e documentações para a melhor configuração do Snort. Existindo também uma comunidade Brasileira que me auxiliou bastante com uma grande variedade de informações e documentações de instalação.

3.3 IMPLEMENTAÇÃO DO SNORT

Atualmente na Secretaria de Estado do Meio Ambiente e dos Recursos Hídricos – SEMARH, está sendo desenvolvido em linguagem PHP um sistema que vai ser disponibilizado na internet para o setor do Programa Semi Árido – PSP que é o SmiPSP, e pensando nesse sistemas e em sistemas futuros que venham a ser desenvolvidos na SEMARH, sentir a necessidade da implantação de uma ferramenta que aumentasse a segurança da informação naquela organização.

Vários outros serviços importantes como firewall, servidor de arquivos, DNS, entre outros que estão sendo disponibilizados em nossos servidores que também precisam ser monitorados para prevenção contra ataques externos ou internos de hackers.

Para implantação do Snort foi utilizado uma máquina com a seguinte configuração:

- Processador: Pentium G620 2.6 GHz LGA 1155 - Dual Core
- Placa-mãe GIGABYTE GA-H61M-DS2H LGA1155
- Disco Rígido de 500GB SATA II
- 4GB Memória DDR3 1333MHz (1 X 4GB)

Foi utilizado o sistema operacional Debian Server, que é uma distribuição Linux com uma comunidade bastante ativa na internet, por isso a escolha desse sistema. Para a instalação do Snort é preciso usar a biblioteca Libpcap para a captura dos pacotes que chegam à interface eth0 da máquina para serem analisados pelo IDS. Foi necessário a instalação do MySQL que é uma ferramenta de gerenciamento de Banco de Dados – SGDB, e seu plugin o Snort-MySQL que faz a conexão do Snort com o MySQL, para que o tráfego analisado seja armazenado no banco de dados e com isso gere estatísticas e resumos das alertas.

O Snort não possui uma interface gráfica, isso faz com que dificulte assim as análises feitas pelo administrador de redes, e isso pode ser bastante prejudicial para a empresa, já que ataques podem passar despercebidos. O Acid BASE – Basic Analysis and Security Engine é uma ferramenta escrita em PHP que gera uma interface gráfica para o usuário, podendo se obter maiores informações sobre o ataque, mostrando as alertas em tempo real, podendo ser criados relatórios deixando a análise feita pelos profissionais de TI mais completa. Como é utilizado

scripts PHP e necessita de um servidor WEB é preciso ter instalado o PHP e o Apache. A Figura 1 mostra a tela inicial do BASE.

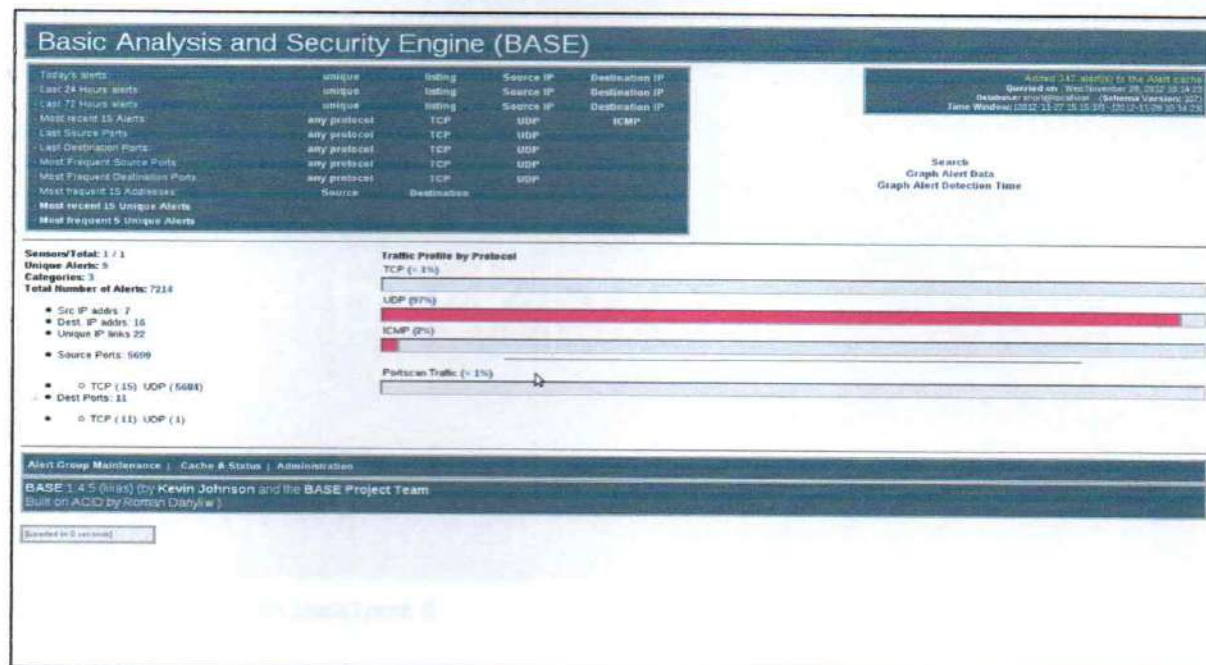


Figura 1 – Tela inicial do BASE

3.4 REALIZAÇÃO DE TESTE

Para a realização dos testes foi utilizado o VMware Workstation que é um software de virtualização desenvolvida pela VMware, para a instalação de um máquina virtual utilizando o sistema operacional BackTrack 5 que é baseado no Ubuntu, e já possuem disponível ferramentas focadas em testes de segurança e testes de penetração – Pentest.

A figura 2 mostra o BackTrack 5 e o menu com algumas das várias ferramentas das mais diversas utilidades que são usadas tanto como para fazer análises de vulnerabilidade pelos administradores de rede para conhecer as falhas de segurança, como programas usados por hackers para realização dos mais diversos ataques.



Figura 2 – Tela inicial do BackTrack 5

O BackTrack 5 tem entre suas ferramentas o Open Vulnerability Assessment System – OpenVAS que é um scanner de vulnerabilidade, possuindo mais de 28.000 tipos de teste de falhas de segurança, entre eles: Escaneamento de portas, Força bruta, falhas de configuração de bancos de dados, Denial of Services, entre outros vários.

A Figura 3 mostra a tela inicial do OpenVAS.

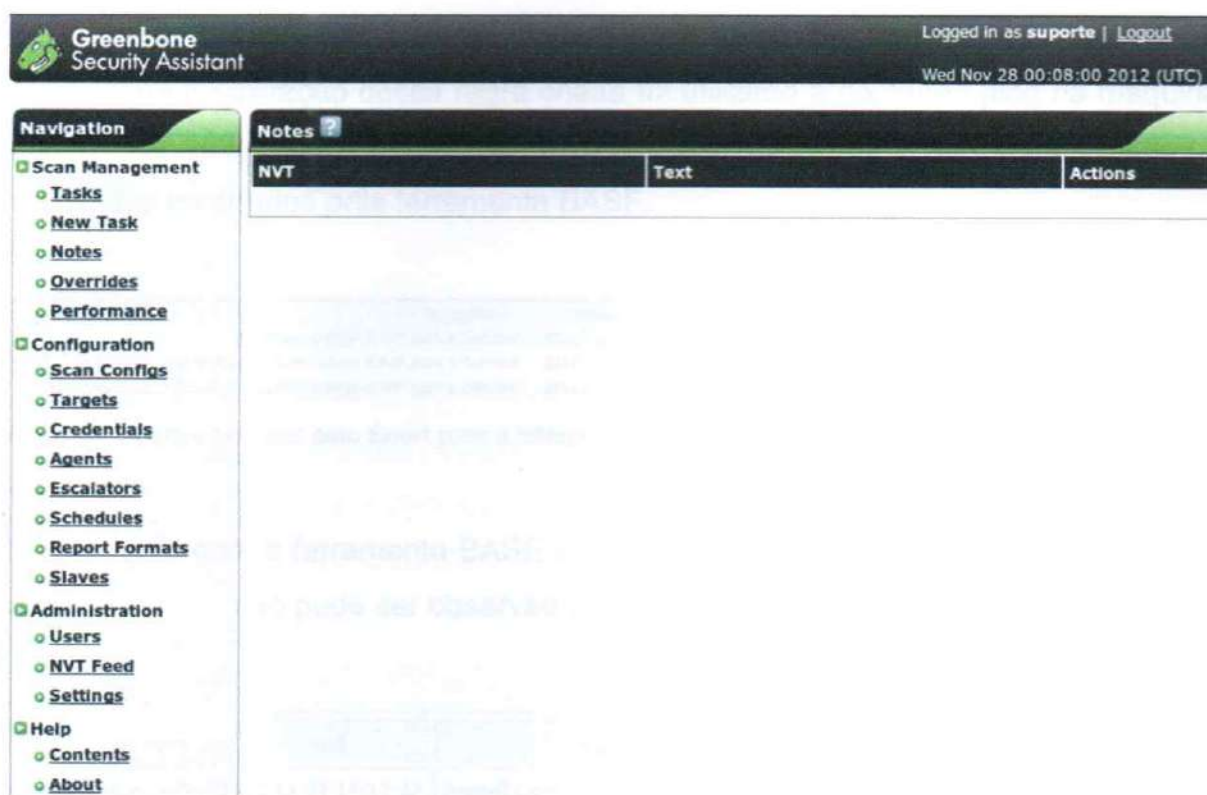


Figura 3 - Tela inicial do OpenVAS

3.5 AVALIAÇÃO DO SNORT

Nesta seção será apresentada uma avaliação do desempenho da ferramenta Snort, através da realização de diversos testes de simulação de ataque.

3.5.1 ICMP

No diretório de regras `/etc/snort/rules` da configuração do Snort foi criada uma nova regra salva com o nome de `icmp-servidor.rules`, sendo adiciona a seguinte condição:

- **Alert icmp any any -> 192.168.0.203 any (msg: "Detectado tráfego ICMP para o Servidor"; SID: 1000010;)**

Essa nova regra vai gerar uma mensagem mostrada acima, para qualquer tráfego ICMP originado de qualquer origem para o servidor de testes 192.168.0.203.

Para o Snort analisar essa nova regra é preciso incluí-la no arquivo de configuração `/etc/snort/snort.conf` na seção de regras:

- **include /etc/snort/rules/icmp-servidor.rules**

Para a validação dessa regra criada foi utilizado o comando ping na máquina com IP 192.168.0.65 para o servidor com o IP 192.168.0.203, e na Figura 4 estão os resultados mostrados pela ferramenta BASE.

☐	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
☐	#0-(4-556)	[snort] Detectado trafego ICMP para o Servidor	2012-11-27 15:17:43	192.168.0.65	192.168.0.203	ICMP
☐	#1-(4-556)	[snort] Detectado trafego ICMP para o Servidor	2012-11-27 15:17:42	192.168.0.65	192.168.0.203	ICMP
☐	#2-(4-551)	[snort] Detectado trafego ICMP para o Servidor	2012-11-27 15:17:41	192.168.0.65	192.168.0.203	ICMP

Figura 4 - Alertas gerados pelo Snort para o tráfego ICMP destinado ao Servidor

Junto com a ferramenta BASE é possível ver o cabeçalho da mensagem que foi analisada, como pode ser observado na figura 5.

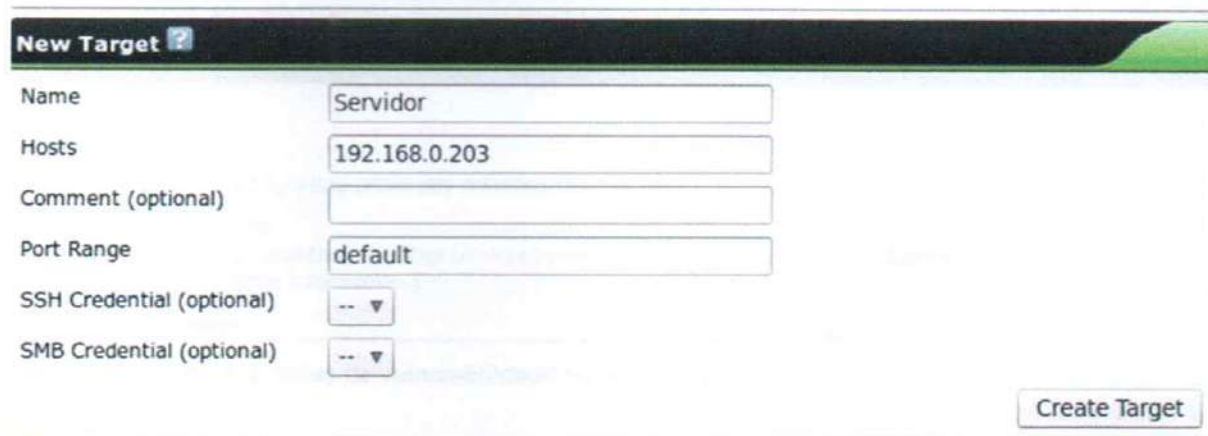
Meta	ID #	Time	Triggered Signature								
	4 - 556	2012-11-27 15:17:42	[snort] Detectado trafego ICMP para o Servidor								
	Sensor	Sensor Address	Interface	Filter							
		192.168.0.203	eth0	none							
	Alert Group	none									
IP	Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	chksum
	192.168.0.65	192.168.0.203	4	20	0	60	40838	no	0	128	6366 = 0x18de
	Options	none									
ICMP	type	code	checksum	ID	seq #						
	(8) Echo Request	(0) 0	22095 = 0x564f	1024	62220						
Payload											
Plain Display	length = 32										
Download of Payload	000 : 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghi jklmnop 010 : 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi										
Download in pcap format											

Figura 5 - Cabeçalho da mensagem ICMP

Esse teste realizado teve o intuito de certificar o funcionamento da ferramenta estudada, e os pacotes destinados ao servidor foram capturados com sucesso pelo Snort.

3.5.2 Escaneamento de Portas

Esse segundo teste realizado vai utilizar as regras padrões que já vem atribuída no momento da instalação do Snort, será utilizado a ferramenta OpenVAS para simular um invasor fazendo o escaneamento das portas em nosso Servidor.



New Target ?	
Name	Servidor
Hosts	192.168.0.203
Comment (optional)	
Port Range	default
SSH Credential (optional)	-- ▼
SMB Credential (optional)	-- ▼
Create Target	

Figura 6 - Criação do alvo para ataque no OpenVAS

Na figura 6 está sendo mostrado o momento da criação do alvo, o Servidor que tem o endereço IP 192.168.0.203. Com o alvo criado, pode-se realizar diversos tipos de testes de vulnerabilidade.

New Scan Config ?

Name

Comment (optional)

Base ☒ Empty, static and fast
☐ Full and fast

Create Scan Config

Import Scan Config ?

Import XML config Browse...

Import Scan Config

Scan Configs ?

Name	Familles		NVTs		Actions
	Total	Trend	Total	Trend	
BF - Teste	1		11		
Full and fast (Most NVT's; optimized by using previously collected information.)	50		28843		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	50		28843		
Full and very deep	50		28843		

Figura 7 - Criação dos testes de vulnerabilidade no OpenVAS

Na figura 7 está sendo mostrada o momento da criação de um Scan no OpenVAS, podendo ser escolhido os Scans padrões que já vem na ferramenta, mas até o que é denominado "fast", já é bastante completo e demorada, fazendo a análise de várias falhas de segurança. Em nosso caso foi criado o Scan com o nome de "PortScan-SEMARH" para identificar que aquele teste é para ser realizados especificamente ataques de vulnerabilidade de portas.

Foi realizado o escaneamento de portas com destino ao Servidor com o IP 192.168.0.203, e no final a ferramenta gera um relatório para o usuário com algumas informações adicionais, segue abaixo:

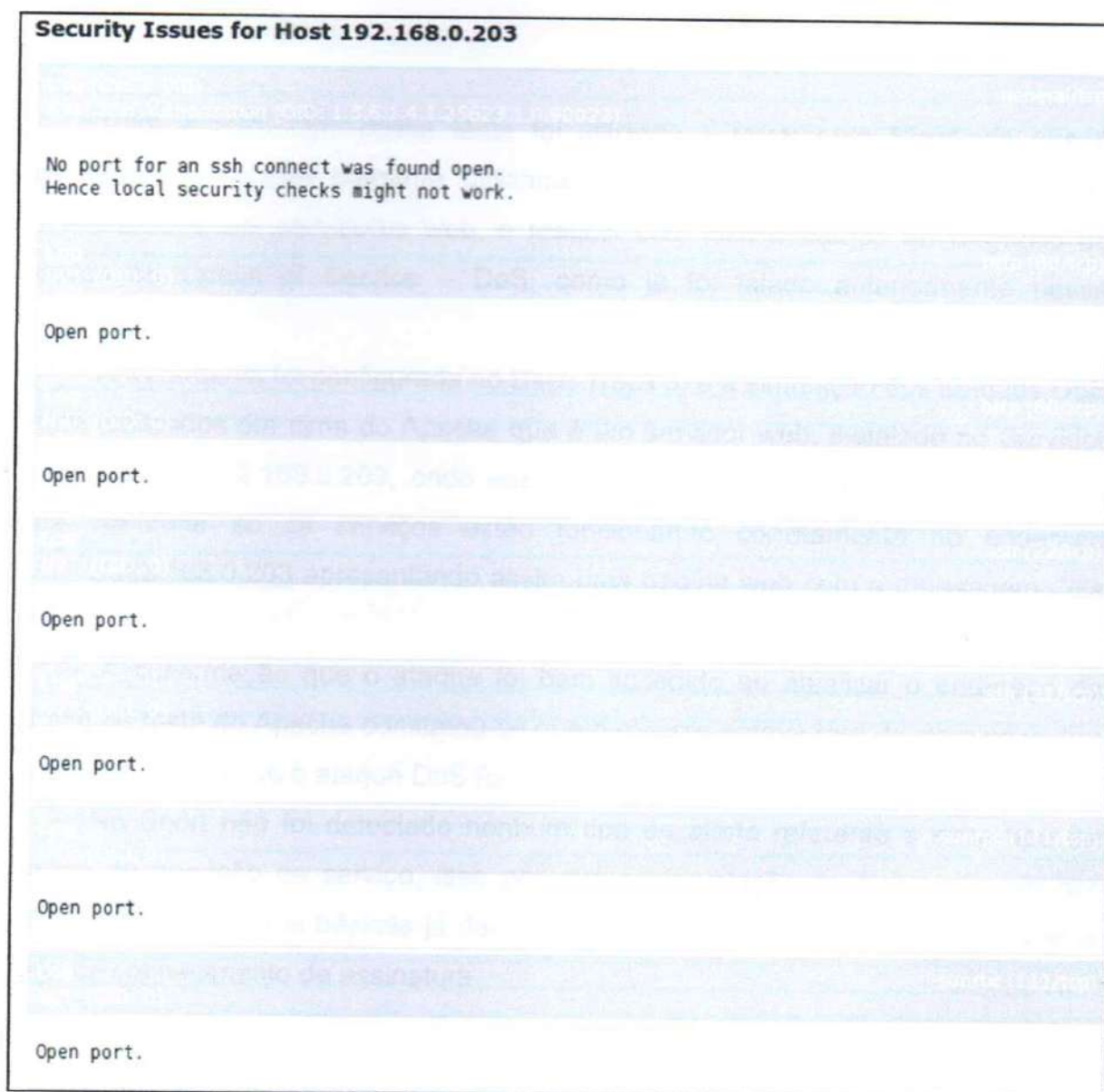


Figura 8 - Relatório final gerado pelo OpenVAS

E como mostrado na figura 9, pode-se verificar que o Snort conseguiu alertar sobre os ataques de varredura de portas destinada ao Servidor.

☐	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
☐	#0-(4-1882)	[snort] (portscan) Open Port: 80	2012-11-28 09:46:15	192.168.0.1	192.168.0.203	Raw IP
☐	#1-(4-1836)	[snort] (portscan) TCP Portscan: 8894:8954	2012-11-28 09:45:57	192.168.0.142	192.168.0.203	Raw IP
☐	#2-(4-1609)	[snort] (portscan) TCP Portscan: 2049:2092	2012-11-28 09:44:56	192.168.0.142	192.168.0.203	Raw IP
☐	#3-(4-1401)	[snort] (portscan) Open Port: 22	2012-11-28 09:43:56	192.168.0.142	192.168.0.203	Raw IP
☐	#4-(4-1402)	[snort] (portscan) Open Port: 80	2012-11-28 09:43:56	192.168.0.142	192.168.0.203	Raw IP
☐	#5-(4-1403)	[snort] (portscan) Open Port: 111	2012-11-28 09:43:56	192.168.0.142	192.168.0.203	Raw IP
☐	#6-(4-1396)	[snort] (portscan) TCP Portscan: 2:7	2012-11-28 09:43:55	192.168.0.142	192.168.0.203	Raw IP

Figura 9 - Alertas de escaneamento de portas gerado pelo Snort

3.5.3 Denial of Service

Para a realização desse teste foi utilizada a ferramenta SlowLoris que é desenvolvida em Perl bastante utilizada pelos hackers por explorar falhas de vulnerabilidade em servidores web, e realizar com isso o ataque de Negação de Serviço ou Denial of Service – DoS, como já foi falado anteriormente nessa monografia.

A ferramenta foi configurada no Back Track 5, e a simulação dos ataques DoS foram realizados em cima do Apache que é um servidor web, instalado no Servidor Linux com IP 192.168.0.203, onde esse servidor apresenta uma página de teste para confirmar se os serviços estão funcionando corretamente no endereço HTTP://192.168.0.203 apresentando assim uma página web com a mensagem: "It's Works!"

A confirmação que o ataque foi bem sucedido ao atualizar o endereço da página de teste do Apache constatou-se que o mesmo estava fora do ar, e só voltou ao normal depois que o ataque DoS foi finalizado.

No Snort não foi detectado nenhum tipo de alerta referente a esse tipo de ataque de negação de serviço, isso por que na instalação do Snort só vem por padrão algumas regras básicas já definidas, sendo necessária a atualização dessa base de conhecimento de assinatura.

4 CONCLUSÕES

Hoje em dia, cada vez mais as empresas precisam se preocupar com a segurança das suas informações, e em manter a disponibilidade e qualidade dos serviços prestados aos seus clientes. E a utilização de uma ferramenta de Sistema de Detecção de Intrusão é um item obrigatório para quem se preocupa com a segurança, facilitando e melhorando e muito a vida de um administrador de redes, tornando o seu parque tecnológico mais seguro, e dificultando assim a vida dos hackers.

Atualmente a estrutura lógica e física da SEMARH não permite a implantação do Snort, já que a utilização dessa ferramenta necessita de uma infraestrutura bem organizada, e uma equipe trabalhando diretamente para que seja configurado corretamente gerando poucas alertas de falsos positivos. A organização precisa ter suas políticas de segurança bem definidas, e que sejam cumpridas pelos funcionários da forma que foi estabelecida, e isso não é uma prática muito comum no órgão público. Por exemplo, muitos usuários não têm essa consciência, e acabam por fornecer sua senha de acesso à máquina para outros usuários.

O desenvolvimento dessa monografia agregou bastante conhecimento. Pude praticar todo o conhecimento adquirido ao longo dos anos do curso de Sistema de Informação, além de despertar um interesse maior por essa área de segurança da informação que vem cada vez mais tendo mais importância na medida em que o fluxo de informação aumenta e consequentemente os ataques praticados na internet.

REFERÊNCIAS BIBLIOGRÁFICAS

ATAQUES na Internet Disponível em: <<http://cartilha.cert.br/ataques/>>. Acesso em: 10 out. 2012.

FERREIRA, Fernando Nicolau de Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**. 2. ed. Rio de Janeiro: Ciência Moderna Ltda, 2008. 259 p.

FIGUEIREDO, Pedro Soares. **Sistemas de Detecção de Intrusão**. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2010. 6 p. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/figueiredo/index.html>. Acesso em: 21 nov. 2012.

MACÊDO, Diego. **IDS - Sistema de detecção de intrusão**. Disponível em: <<http://www.diegomacedo.com.br/ids-sistema-de-deteccao-de-intrusos/>>. Acesso em: 15 out. 2012.

MORIMOTO, Carlos E.. **Redes guia prático**. 2. ed. Porto Alegre: Meridional Ltda, 2008. 555 p.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes**. 4. ed. São Paulo: Novatec, 2012. 483 p.

QUEIROZ, Claudemir Da Costa. **SEGURANÇA DIGITAL: UM ESTUDO DE CASO**. 2007. 71 f. Monografia (Bacharel Em Curso De Ciência Da Computação) - Faculdade Lourenço Filho, Fortaleza, 2007. Disponível em: <http://www.flf.edu.br/revista-flf/monografias-computacao/seguranca_digital.pdf>. Acesso em: 21 nov. 2012.

SEGURANÇA da Informação Disponível em: <http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o>. Acesso em: 10 out. 2012.

SILVA JÚNIOR, Marcos Vinícius da. **O que é segurança da informação**. Disponível em: <<http://webinsider.uol.com.br/2009/09/23/o-que-e-seguranca-da-informacao/>>. Acesso em: 12 out. 2012.

SNORT Disponível em: <<http://www.snort.org/>>. Acesso em: 10 out. 2012.

SNORT Disponível em: <<http://www.snort.com.br/>>. Acesso em: 12 out. 2012.

ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade Hacker**. 4. ed. São Paulo: Digerati Books, 2004. 348 p.