INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO – CAMPUS FLORESTA

CURSO DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

SÉRGIO ALVES MENEZES

SEGURANÇA DA INFORMAÇÃO: UM GUIA DE INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA DE DETECÇÃO DE INTRUSÃO *SNORT*

Floresta – PE

2018

SÉRGIO ALVES MENEZES

SEGURANÇA DA INFORMAÇÃO: UM GUIA DE INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA DE DETECÇÃO DE INTRUSÃO *SNORT*

Monografia apresentada como requisito para obtenção da graduação no curso de Gestão da Tecnologia da Informação, do Instituto Federal de Educação, Ciência e tecnologia do Sertão Pernambucano - Campus Floresta.

Orientador (a): Prof. Severino do Ramo de Paiva

Floresta – PE

2018

Dados Internacionais de Catalogação na Publicação (CIP)

M541s Menezes, Sergio Alves

Segurança da informação: um guia de instalação e configuração do sistema de detecção de intrusão snort. / Sergio Alves Menezes - Floresta, 2018.

58 f. il.

Orientador: Severino do Ramo de Paiva .
Trabalho de Conclusão de Curso – Tecnólogo em Gestão da Tecnologia da Informação Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta.

1. Redes de computadores. 2. Ferramenta open source. 3. Crimes virtuais. 4. IDS. 5. Snort.

I. Paiva, Severino do Ramo de . II. Título.

CDD: 004.056

Elaborada pela bibliotecária Ednaene de Menezes CRB4/2133

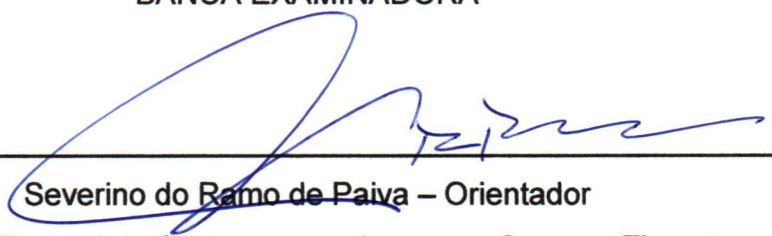
SÉRGIO ALVES MENEZES

SEGURANÇA DA INFORMAÇÃO:
UM GUIA DE INSTALAÇÃO E CONFIGURAÇÃO DO SISTEMA DE DETECÇÃO DE INTRUSÃO *SNORT*

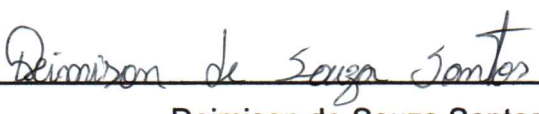
Aprovado em: __ / __ / ____

Nota: _____

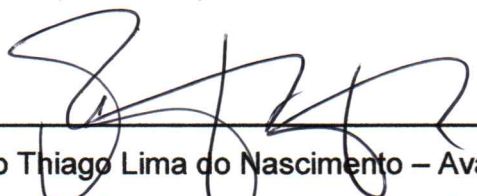
BANCA EXAMINADORA



Severino do Ramo de Paiva – Orientador
Instituto Federal do Sertão pernambucano – Campus Floresta



Deimison de Souza Santos – Avaliador
Instituto Federal do Sertão pernambucano – Campus Floresta



Paulo Thiago Lima do Nascimento – Avaliador
Instituto Federal do Sertão pernambucano – Campus Floresta

DEDICATÓRIA

Dedico este trabalho a todos que me apoiaram na caminhada até a conclusão do mesmo, a minha mãe Sônia, meu pai Sérgio, meus irmãos Stênio e Styven, a minha namorada Ana Célia, ao meu orientador Severino de Paiva, aos demais familiares e amigos que sempre me incentivaram.

AGRADECIMENTOS

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitário, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

A meus amigos e minha família, que sempre me incentivaram nessa jornada que não foi fácil, mas sempre me deram força para seguir.

Aos meus professores do IF SERTÃO, que abriram uma fonte de conhecimento na minha vida, com ensinamentos construtivos para minha formação e carreira no mercado de trabalho.

"[...] O rio atinge seus objetivos porque aprendeu a contornar obstáculos."

Lao Tsé

Resumo

Ao longo das últimas décadas, a humanidade alcançou avanços tecnológicos inimagináveis, notadamente no âmbito das TICs (Tecnologias da Informação e Comunicação). Pessoas estão usando cada vez mais esses meios de comunicação para transações, compras, vendas e outros serviços através da internet. A indústria eletrônica vem desenvolvendo novos dispositivos capazes de interligar indivíduos e empresas através da internet. Com isso, os crimes virtuais sofreram uma evolução conjunta com esses avanços tecnológicos. O presente trabalho visa discutir as melhores formas de proteção contra ataques ou intrusos, apresentando, de forma didática, um guia de instalação e configuração da ferramenta IDS (*Intrusion Detection System*) *open source Snort*. Do ponto de vista metodológico, foi utilizada uma abordagem descritiva do presente trabalho. O tratamento dos dados levantados foi eminentemente qualitativo.

Palavra-chave: rede de computadores, ferramenta *open source*, crimes virtuais, IDS, *Snort*.

Abstract

Throughout the last decades, the humanity has reached technological advances unimaginable, notably in the scope of the (TICs) Information and Communication Technologies. People are increasingly using these media for transactions, purchases, sales and other services over the internet. The electronics industry has been developing new devices capable of connecting individuals and businesses over the internet. With this, the virtual crimes have undergone a joint evolution with these technological advances. The present work aims to discuss the best forms of protection against attacks or intruders, presenting, in a didactic way, a guide for the installation and configuration of the (IDS) Intrusion Detection System open source Snort tool. From the methodological point of view, a descriptive approach of the present work was used. The treatment of the data collected was eminently qualitative.

Keyword: computer network, open source tool, virtual crimes, IDS, Snort.

LISTA DE ABREVIATURAS E SIGLAS

AC	CERTIFYING AUTHORITY
ARPA	ADVANCED RESEARCH PROJECTS AGENCY
DDOS	DISTRIBUTED DENIAL OF SERVICE
DMZ	DEMILITARIZED ZONE
GNU	GENERAL PUBLIC LICENSE
GRSI	GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO
HD	HARD DISK
HIDS	HOST-BASED INTRUSION DETECTION SYSTEM
IDS	INTRUSION DETECTION SYSTEM
IP	INTERNET PROTOCOL
IPS	INTRUSION PREVENTION SYSTEM
NFC	NEAR FIELD COMMUNICATION
NIDS	NETWORK INTRUSION DETECTION SYSTEM
OISF	OPEN INFORMATION SECURITY FOUNDATION
PDCA	PLAN DO CHECK ACT
RAID	REDUNDANT ARRAY OF INEXPENSIVE DRIVES
SGSI	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
SI	SISTEMA DE INFORMAÇÃO
SSD	SOLID STATE DRIVE
TCP	TRANSMISSION CONTROL PROTOCOL
VPN	VIRTUAL PRIVATE NETWORK

LISTA DE FIGURAS

LISTA DE TABELAS

Sumário

CAPÍTULO 1

1. INTRODUÇÃO

As redes apareceram na década de 60, como um mecanismo de troca de informações através da rede telefônica, sendo capaz de transmitir dados por circuitos eletrônicos. A primeira rede de computadores foi criada a partir de 1965, desenvolvida pela agência americana ARPA (*Advanced Research Projects Agency*) um departamento militar dos Estados Unidos da América, o projeto foi liderado por J.C.R. Licklide que tinha uma visão de interligar os computadores das bases militares aos centros de pesquisas do governo americano, mais tarde dentro do pentágono o projeto foi batizado de ARPANET. Segundo Paiva (2017), os estudos em relação aos fenômenos da informação estão sendo cada vez mais explorados, consequentemente pelo surgimento de novas tecnologias e informações, principalmente nas atividades produtivas entre o homem e os negócios de uma organização.

Segurança de redes é um dos assuntos que está em maior discursão quando se fala em serviços de tecnologia da informação, atualmente houve um crescimento da aplicação da internet nos aparelhos do nosso cotidiano (smartphones, computadores, aparelhos domésticos). E podemos dizer que a internet é o meio de comunicação e informação mais utilizado por indivíduos ou organizações.

Antigamente a internet era apenas para fazer pequenas pesquisas. Hoje em dia a realidade é outra, qualquer pessoa pode utilizá-la para diversas finalidades. Devemos tratá-la com muito cuidado mesmo tendo conceitos, regras e lições como qualquer outro tipo de segurança, a segurança da internet tem suas técnicas e particularidade diferentes a serem priorizadas. Cheswick (et al. 2005).

Seguindo esse pensamento, surge a internet das coisas (*Internet of Things*) que pode ser uma revolução tecnológica com base em conjuntos de dispositivos, redes (*wi-fi, bluetooth e* NFC) e sistemas de controle para gerenciar todos os dados. Apresenta um objetivo de interligar todos os aparelhos eletrônicos do cotidiano na internet. Com essa ideologia surge questionamentos: Como proteger os dados com segurança?; haverá algum tipo de sistema contra intrusão?; já imaginou a rede

privada de sua residência sendo atacada e seus aparelhos domésticos a mercê de pessoas mal-intencionadas?

A proposta do presente trabalho visa discutir as melhores formas de como se proteger contra ataques ou intrusos, utilizando ferramenta *open source* IDS (*Intrusion Detection System*) *Snort,* a fim de analisar essa alternativa de proteção como forma de prevenir problemas recorrentes de redes. Este trabalho está estruturado em 3 capítulos, sendo eles: Capítulo 1 – Introdução, Capítulo 2 – Fundamentação Teórica, Capítulo 3 – Guia de Instalação e Configuração da Ferramenta *Snort*. Em cada capítulo são abordados os conceitos mais importantes ao tema em questão.

1.1 Justificativa

A Tecnologia da Informação está em constante crescimento, arquivos físicos estão sendo substituídos por armazenamento digital. Pessoas estão usando mais os meios de comunicação para transações, compras, vendas e outros serviços na internet. O mercado eletrônico fabricando novos dispositivos capazes de interligar a outros dispositivos através da internet. Com isso, os crimes virtuais sofreram uma evolução conjunta com a rede de computadores.

De acordo com site Olhar Digital (2016), uma recente pesquisa realizada pela Symantec divulgou um relatório afirmando que o cibercrime ainda é um problema muito grande no Brasil e que precisa ser hostilizado se quiser minimizar esses ataques em relação ano de 2016. A pesquisa revela que a cada cinco usuários de smartphone, tablets, notebooks e outros dispositivos conectados à internet não se preocupam com outras formas de garantir a segurança de suas informações, uma parcela desses usuários confia na proteção de fábrica de seus dispositivos.

Analisando esse fato a escolha do tema visa ajudar usuários domésticos e empresas a identificar as melhores formas de como se proteger contra ataques ou intrusos, utilizando ferramenta *open source* IDS (*Intrusion Detection System*) *Snort,* a fim de analisar essa alternativa de proteção como forma de prevenir problemas recorrentes de redes, tais como invasão na intranet; roubo de informações sigilosas; perdas e paralisação nos serviços. Serão abordados conceitos básicos, procedimentos de segurança, descrição de IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*), tipos de ameaças e ataques a redes, implementação de ferramenta IDS, simulações de ataques e análises dos resultados.

1.2 Problemática

Com o avanço tecnológico na área de redes de computadores, houve também um aumento significativo de ataques de intrusões nas redes das organizações, sabendo disso muitas organizações estão procurando melhores maneiras de preservar suas informações contra esse tipo de ameaça.

Como facilitar a instalação e uso do sistema IDS (*Intrusion Detection System*) *SNORT?*

1.3 Objetivos

Nesta seção serão abordados o objetivo geral e os objetivos específicos para a realização da pesquisa.

1.3.1 Objetivo geral

Descrever um guia de instalação e configuração do *software* de detecção de intrusão *Snort*.

1.3.2 Objetivos específicos

1º elencar os principais conceitos de segurança da informação referentes a ataques e invasões;

2º apresentar os principais *softwares* de detecção e prevenção de intrusão IDS e IPS, como funcionam e suas aplicações;

3º pesquisar sobre os principais ataques a redes de computadores;

4º descrever um guia de instalação e configuração de *software* IDS.

1.4 Metodologia

O conceito de pesquisa, tendo em vista o pensamento de muitos estudiosos, é amplo, tendo consensos e divergências. Pode-se definir pesquisa como o procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. Gil (2002). Quanto ao objetivo, esta pesquisa caracteriza-se como descritiva por buscar relatar as melhores formas de como se proteger contra ataques ou intrusos, utilizando ferramenta *open source* IDS (*Intrusion Detection System*) *Snort,* a fim de analisar essa alternativa de proteção como forma de prevenir problemas recorrentes de segurança de redes.

Silva (2016) afirma que, a metodologia faz parte do projeto na qual o autor deve indicar os procedimentos para serem executados na pesquisa. Toda pesquisa é formada por um conjunto de ações, etapas e técnicas para se concretizar.

Para Lakatos e Marcone (2010) a pesquisa, é um procedimento formal, com método de pensamento reflexivo, que requer um tratamento cientifico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais.

Um projeto de pesquisa é composto de seis passos, são eles:

1. Seleção do tópico ou problema para a investigação.
2. Definição e diferenciação do problema.
3. Levantamento de hipóteses de trabalho.
4. Coleta, sistematização e classificação dos dados.
5. Análise e interpretação dos dados.
6. Relatório do resultado da pesquisa.

De acordo com Severino (2007), quando se fala de pesquisa qualitativa refere-se a conjuntos de metodologias, que envolve diversas referencias epistemológicas. A pesquisa bibliográfica é realizada a partir de registros de pesquisas anteriores, em documentos, como livros, artigos e outros.

Para atingir o objetivo proposto neste trabalho, a leitura sobre o tema foi a principal ferramenta utilizada. Em busca de meios para fazer uma abordagem com fundamentos científicos, algumas bases de dados foram utilizadas como o Portal de Periódicos da CAPES, no site do centro de estudos, resposta e tratamento de incidentes de segurança no brasil (CERT.br) e Google Acadêmico. Além dos livros disponíveis na biblioteca do IF Sertão-PE Campus Floresta, e os TCCs anteriormente produzidos pelos alunos do Curso Superior em Gestão da Tecnologia da Informação.

Quanto ao tratamento dos dados levantados, a pesquisa pode ser enquadrada como qualitativa, pois foi elaborada com dados bibliográficos na literatura existente, tendo em vista que através desse levantamento prévio, pode-se estabelecer os conceitos básicos sobre o tema segurança de redes.

Posteriormente ao levantamento das informações, foi feita a preparação do guia de instalação e configuração da ferramenta *Snort*, toda a informação sobre o guia da

ferramenta *Snort* foi retirar com base em manuais disponibilizados no site: https://www.snort.org/#documents.

Com os diferentes mecanismos de segurança de redes, o presente trabalho optou por detalhar o *Snort*, sendo a mais popular entre as ferramentas de sistema de detecção de intrusão. Segundo *Snort* (s.d.) com mais de 5 milhões de *downloads* e mais de 600.000 usuários cadastrados, é o sistema de prevenção de intrusão mais utilizado no mundo.

CAPÍTULO 2

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será exposto a fundamentação teórica utilizada no desenvolvimento deste trabalho.

2.1 Segurança da Informação

Conforme definido por Stallings (2008), a segurança da informação passou por mudanças nas últimas décadas, antes do uso de equipamentos para o processamento de informações (dados). Com o uso crescente dos computadores a segurança da informação passou a ser considerada de extremo valor para uma organização e consequentemente a necessidade do uso de ferramentas para a proteção de informações sigilosas, que são transmitidas através de redes de computadores.

Segundo Torres (2014), a segurança em redes vai além de uso de ferramentas, não adianta ter um *firewall* instalado na rede sem ele estar devidamente configurado ou usuários que não tiverem um conhecimento básico em procedimentos de segurança, tem tudo a ver com procedimentos e padrões que a tecnologia disponibiliza.

De acordo com Paiva (2017), na segurança da informação existem quatro princípios básicos:

- **Confidencialidade** – a informação deve ser protegida e somente acessada por usuário que a pertencer.
- **Integridade** – baseia-se que toda a informação deverá ser protegida contra possíveis alterações sem permissão do proprietário

- **Disponibilidade** – a informação deve estar sempre disponível para seu usuário, logo que surgir a necessidade de usá-la.
- **Autenticidade** – visa garantir a identidade da pessoa ou entidade que prestou, alterou ou descartou uma determinada informação.

Com base nesses princípios, ao longo do tempo surgiram mecanismos de segurança como IDS *Snort*, que quando configurados, podem aumentar ainda mais a segurança da sua rede contra intrusões. Os capítulos adiantes detalham de forma mais clara como esta ferramenta funciona.

2.2 Principais Tipos de Ameaças às Redes

Como lembra Stallings (2005), os ataques ativos e passivos são classificados em termos para facilitar sua identificação. Um ataque passivo tem por objetivo monitorar as transmissões de dados entre o emissor e o receptor sem afetar os recursos dos mesmos. Já o ataque ativo é mais hostil, altera o fluxo de dados ou a criação de um fluxo falso para obter as informações do sistema, podem ser divididos em quatro categorias: repetição, modificação de mensagens, negação de serviços e falsificação.

2.2.1 Ataques de Falsificação

Esse tipo de ataque geralmente inclui outro tipo de ataque ativo e tem como finalidade se passar por uma entidade do sistema, a fim de obter informações privilegiadas do sistema.

Conforme Nakamura (2007), o ataque Mitnick utiliza diferentes técnicas para obter informações, como: *IP Spoofing*, sequestro de conexão TCP (*Transmission Control Protocol*) e negação de serviço. Assim, descobrindo a relação de confiança entre o servidor e a máquina (x-terminal), em seguida tentar sobrecarregar a porta de login do servidor com uma imensa lista de pedidos de conexão para deixar o serviço indisponível.

2.2.2 Ataques de Repetição

Nakamura (2007) afirma, esse tipo de ataque é reproduzido diversas vezes, onde o invasor copia um fluxo de mensagens entre duas partes e repete as informações para um ou mais partes, ou seja, os computadores processam o fluxo de informações legítimas e consequentemente a redundância no sistema.

2.2.3 Ataques de Modificação de Mensagens

Ataque que modifica uma parte da mensagem autentica para produzir um efeito não autorizado. Nakamura (2007), os *hackers* utilizam os navegadores de internet onde é mais simples e mais fácil de capturar as informações necessárias para realizar as modificações no conteúdo das páginas dos servidores Web, consequentemente prejudicando as organizações.

Um exemplo é quando um agente malicioso intercepta uma informação de um serviço, reproduzindo esta mesma mensagem algum tempo depois com alterações.

2.2.4 Ataques de Negação de Serviço

Ataque que bloqueia o funcionamento ou gerenciamento da comunicação deixando inacessível para entidade legitima, podem ter um alvo específico que impeça o envio de mensagens para determinado destino ou desativando uma rede ou servidor com uma sobrecarga de dados.

Ataques coordenados chamados de negação de serviços, os DDoS (*Distributed Denial of Service*) faz ataques simultâneos aos alvos utilizando diversos *host* distribuídos, praticamente deixando a vítima indefesa sem ao menos saber a origem do ataque, pois os *hosts* são controlados pelo *Hacker*. Nakamura (2007).

2.2.5 Códigos Maliciosos (*Malwares*)

Desenvolvidos especificadamente para causar danos a computadores, os códigos maliciosos (*malware*) quando são bem-sucedidos passam a ter acesso aos dados do usuário, onde executam tarefas de acordo com permissões do mesmo. Segundo a Cartilha de Segurança para Internet CERT.br (2017), os motivos que leva o atacante a praticar esse tipo de atividade são os benefícios que se tem em troca, como exemplo:

- Vantagens financeiras;
- Coleta de informações confidenciais;
- Desejo de autopromoção;
- Vandalismo.

O CERT.br no ano de 2017, pesquisas apontaram que *Scan* foi o tipo de ataque mais utilizado por invasores, onde visa identificar computadores vulneráveis na redes, a figura abaixo mostra a porcentagem de cada tipo de ataque.

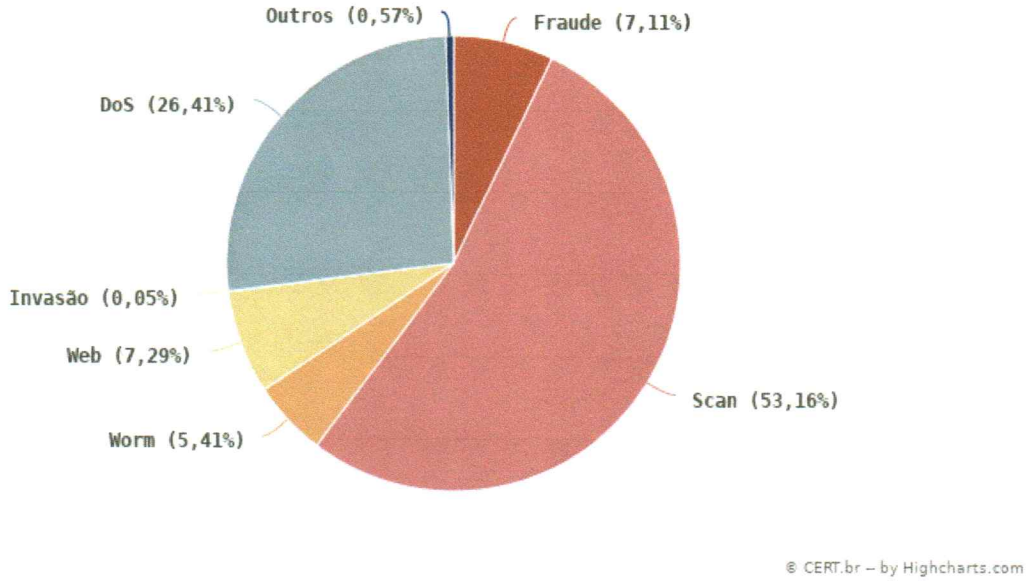
Como mostra o CERT.br 2017, os principais tipos de *malware são:* vírus, *worms, bots e botnets, spywares, backdoors, rootkits e* cavalos de tróia *(trojans).*

- Vírus é um *software* malicioso, ele se propaga através de programas já infectados, posteriormente fazendo cópias de si mesmo nos programas do computador e executando atividades sem o conhecimento do usuário.
- *Worm* executa de forma diferente do vírus, o mesmo é capaz de realizar copias de se mesmo automaticamente sem o uso de programas.
- *Bot* é um programa que utiliza a rede para se comunicar com o invasor, permitindo que seja manipulado remotamente o computador zumbi (*zombir computer). Botnets* é uma rede formada por centenas ou milhares de computadores zumbis.
- *Spyware* sendo programa capaz de monitorar as atividades do sistema infectado com o objetivo de enviar dados coletados para terceiros. Usado de duas maneiras como forma legítima ou maliciosa.
- *Backdoors* assegura ao atacante usar futuramente o computador infectado, por meio de inclusões de serviços criados ou modificados que permite o retorno do invasor.
- *Rootkits* uma biblioteca de programas e técnicas, sua especialidade é esconder e assegurar que o invasor não seja notado. Exemplo de sua utilidade: removendo evidencias em arquivos de logs, instalar outros códigos maliciosos e mapear vulnerabilidade do computador por meio da rede.
- Cavalos de tróia *(trojans)* são programas que precisam ser executados para que funcionem, normalmente é malicioso e possui diferentes tipos: *trojan downloader, trojan dropper, trojan backdoor, trojan DoS, trojan* destrutivo, *trojan clicker, trojan proxy, trojan spy, trojan banker* ou bancos.

Como mostra o CERT.br 2017, os principais tipos de *malware são:* vírus, *worms, bots e botnets, spywares, backdoors, rootkits e* cavalos de tróia *(trojans).*

- Vírus é um *software* malicioso, ele se propaga através de programas já infectados, posteriormente fazendo cópias de si mesmo nos programas do computador e executando atividades sem o conhecimento do usuário.
- *Worm* executa de forma diferente do vírus, o mesmo é capaz de realizar copias de se mesmo automaticamente sem o uso de programas.
- *Bot* é um programa que utiliza a rede para se comunicar com o invasor, permitindo que seja manipulado remotamente o computador zumbi (*zombir computer*). *Botnets* é uma rede formada por centenas ou milhares de computadores zumbis.
- *Spyware* sendo programa capaz de monitorar as atividades do sistema infectado com o objetivo de enviar dados coletados para terceiros. Usado de duas maneiras como forma legítima ou maliciosa.
- *Backdoors* assegura ao atacante usar futuramente o computador infectado, por meio de inclusões de serviços criados ou modificados que permite o retorno do invasor.
- *Rootkits* uma biblioteca de programas e técnicas, sua especialidade é esconder e assegurar que o invasor não seja notado. Exemplo de sua utilidade: removendo evidencias em arquivos de logs, instalar outros códigos maliciosos e mapear vulnerabilidade do computador por meio da rede.
- Cavalos de tróia *(trojans)* são programas que precisam ser executados para que funcionem, normalmente é malicioso e possui diferentes tipos: *trojan downloader*, *trojan dropper*, *trojan backdoor*, *trojan DoS*, *trojan* destrutivo, *trojan clicker*, *trojan proxy*, *trojan spy*, *trojan banker* ou bancos.

Figura 1 - Tipos de Incidentes Reportados ao CERT.br 2017



Fonte: CERT.br

Tabela 1 - Resumo comparativo das características de cada tipo

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por *e-mail*	✓	✓	✓	✓	✓		
Baixado de *sites* na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓			✓	✓
Como se propaga:							

Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por *e-mail*		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consome grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos		✓	✓	✓			✓
Possibilita o retorno do invasor						✓	✓
Envia *spam* e *phishing*			✓				
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Fonte: CERT.br

2.3 Mecanismos de Segurança

Atualmente existe diversos mecanismos de segurança de redes, todos com o mesmo objetivo de resguardar os dados, destacamos os principais:

2.3.1 Criptografia

Criptografia é um conjunto de técnicas que disfarça os dados originais. Segundo Nakamura (2007), "Os processos de cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são inteligíveis".

De acordo com o CERT.br no ano de 2017, a criptografia é um dos principais mecanismos de segurança que pode ser usado para se proteger de ataques por meio da internet. Com uso da criptografia você pode:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

2.3.2 *Firewall*

Firewall conhecida como parede de fogo, ela é a primeira barreira de contra ataques de pessoas externa da rede. De acordo Tanenbaum & Wetherall (2011, p. 513),

> O *firewall* atua como um filtro de pacotes. Ele inspeciona todo e qualquer pacote que entra e que sai. Os pacotes que atenderem a algum critério descrito nas regras formuladas pelo administrador da rede serão remetidos normalmente, mas os que falharem no teste serão descartados sem cerimônia.

2.3.3 Autenticação

Autenticação é um processo que busca identificar o usuário no momento que o mesmo tenta acesso ao sistema. Segundo Cheswick (et al. 2005), a autenticação consiste em três fatores que são: primeiro o que você conhece, por exemplo: *Personal Identification Number* (PIN). Segundo o que você tem, exemplo: *Token*, *smart card*. O terceiro são atributos biológicos, exemplo: biometria.

2.3.4 Controle de Acesso Físico

A principal função é gerar um ambiente seguro livre de acessos não autorizados. Com o objetivo de proteger as pessoas, os bens e os recursos da organização. Segue algumas sugestões de controle de acesso físico:

- Delimitar e identificar uma área onde o acesso é restrito;
- Impedir acesso não autorizado;
- Identificar e checar permissão de acesso;
- Liberar acesso autorizado;
- Identificar, alarmar e registrar as tentativas de acessos não autorizados.

2.3.5 Política de *Backup*

De acordo com o CERT.br (2017) ter uma boa política de *backup* é de grande relevância para uma organização, é engano pensar que não é de extrema importância. Existe uma metodologia de ciclo de vida (início, meio e fim), ou seja, sua concepção, duração, expiração e descarte. *Backups* são muito importantes, pois permitem:

- **Proteger os dados:** preservar seus dados para que sejam recuperados em situações de falha no disco rígido (HD), atualização sem sucesso do

sistema operacional, exclusão ou substituição acidental de arquivos ou ataques maliciosos.

- **Recuperação de versões:** recuperar versão anterior do arquivo alterado, parte excluída do texto, etc.

2.3.6 Certificação Digital

O certificado digital é um registro eletrônico que contém informações referentes que distingue uma entidade e associa a ela uma chave pública, ou seja, sua funcionalidade consiste em identificar uma organização, pessoa física, equipamentos ou serviços em *site web*. Podendo ser homologado para diferentes finalidades, como confidencialidade e assinatura digital, CERT.br (2017).

Um certificado digital é emitido por entidades credenciadas conhecidas como Autoridade Certificadora (AC), ela também é responsável por tornar público os certificados que não são mais confiáveis, todos são incluídos periodicamente em uma lista negra, chamada de Lista de Certificados Revogados (LCR). A seguir os dados que compõem um certificado digital:

- Versão e número de série do certificado;
- Dados que identificam a AC que emitiu o certificado;
- Dados que identificam o dono do certificado (para quem ele foi emitido);
- Chave pública do dono do certificado;
- Validade do certificado (quando foi emitido e até quando é válido);
- Assinatura digital da AC emissora e dados para verificação da assinatura.

Tipos de certificado digital:

- e-CNPJ – funciona virtualmente e serve para emissão de nota fiscal eletrônica, transmissão de escrituração fiscal digital, etc.
- e-CPF – também funciona de forma virtual, realiza entrega de declarações de renda e demais documentos eletrônicos com assinatura digital.

2.3.7 RAID (*Redundant Array of Independent Disks*)

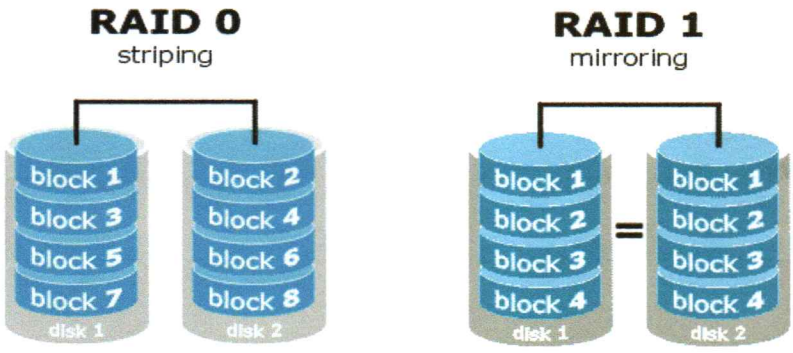
De acordo com site Techtudo (*s.d*) RAID (*Redundant Array of Independent Disks*) é uma tecnologia que é baseada em montar arranjos de dois ou mais HDs (*Hard Disk*) ou memorias SSDs (*Solid-State drive*) e funcionaram em conjunto, com o objetivo de aprimorar a segurança e *performance* de computadores, servidores e *storages.* Dois

exemplos de funcionamento RAID, ambas podem ser utilizadas em conjunto ou separadas:

RAID 0 - deixa o sistema mais rápido dividindo os dados.

RAID 1 – usando a técnica de espelhamento torna o sistema de disco mais seguro.

Figura 2 - Funcionalidade RAID



Fonte: http://www.techtudo.com.br/artigos/noticia/2012/10/entenda-o-que-e-raid-tecnica-que-torna-o-sistema-mais-rapido-e-seguro.html

Essa tecnologia foi criada no ano de 1988 por três pesquisadores da Universidade de Berkeley nos Estados Unidos da América, ela ainda continua sendo utilizada devido ao seu foco em segurança e velocidade.

2.3.8 Sistema de Detecção de Intrusão (IDS)

Segundo Nakamura (2007), o sistema de detecção de intrusão, tem um papel fundamental no ambiente corporativo. Com o objetivo de detectar atividades suspeitas, impróprias e intrusões, dá o suporte ao *firewall* que podemos dizer ser a primeira linha de defesa, um sistema de detecção de intrusão (IDS) é um elemento importante para assegurar a defesa da organização.

Conforme Cheswick (et al. 2005), um sistema de detecção de intrusão (*intrusion detection sytem - IDS*) são ferramentas que funcionam como sentinelas que atuam na proteção da rede, eles trabalham no tráfego da rede como farejadores reunindo os pacotes de dados. Ainda afirma que existe vários tipos como o IDSs de rede (NIDSs), que monitoram o tráfego de rede em busca de indícios que leve uma invasão. Outros

são baseados em *host* que analisam arquivos em busca de vírus e também de dados alterados dentro da organização.

A intrusão em redes por usuário ou *software* maliciosos são uma enorme dor de cabeça, o usuário quando faz a intrusão pelo *logon* não autorizado em um computador para obter dados privilegiados ou através de *software* que pode ter aspecto de vírus, *worms* ou cavalo de troia. Stallings (2008).

Segundo Stallings (2008, apud Anderson 1980), identificou três classes de intrusos:

- Intruso mascarado – usuário sem autorização de usar o computador, invade o sistema para ter total controle sobre a conta do usuário legitimo.
- Intruso infrator – como um legitimo usuário que tem acesso aos dados, *software* ou recursos, mas que faz mau uso dos dados.
- Intruso clandestino – Indivíduo com poderes de administrador do sistema, utiliza de tal função para escapar de auditorias.

2.3.8.1 Características de um IDS

Segundo Nakamura (2007), funcionando como um vigilante ou um alarme de intrusão, as detecções são realizadas com algum tipo de conhecimento prévio, como assinaturas ou comportamentos estranhos. O IDS também oferece segurança interna na organização, onde usuários internos atacam o ambiente corporativo. A figura apresenta as funções de um sistema de detecção de intrusão.

Figura 3 - Funções de um IDS

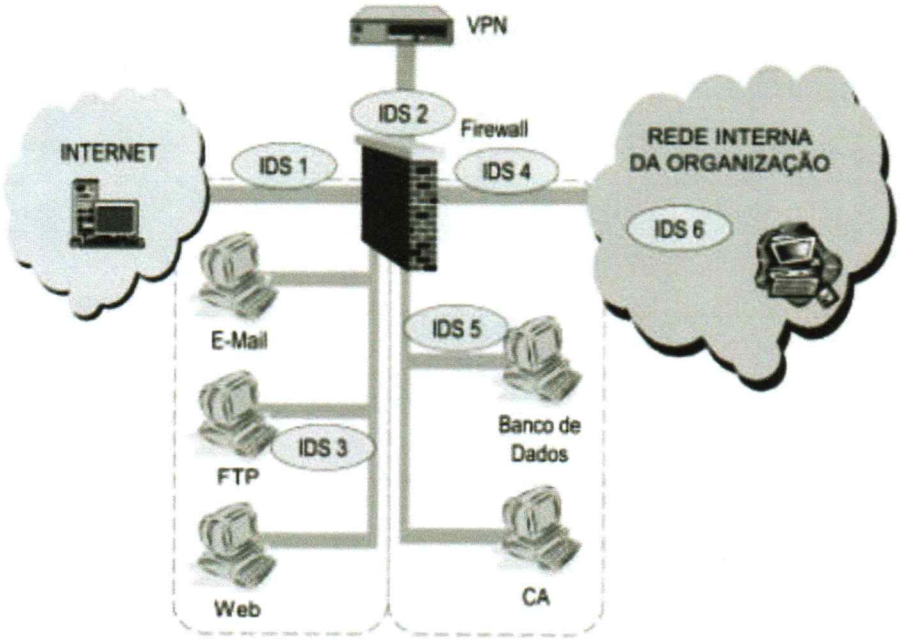
Fonte: Nakamura (2007)

2.3.8.2 Onde monitorar

De acordo com Cheswick (et al. 2005), quando instalados em locais corretos ou que sejam mais vulneráveis a ataques, o IDS se torna mais eficaz, protegendo os ativos da empresa. São como um dispositivo de vigilância que monitora os dados constantemente, onde os detectores devem ter uma maior sensibilidade nas regras para que farejem as ameaças que rondam a organização.

Segundo Nakamura (2007), a varias localizações que podemos utilizar o IDS, onde cada um terá um objetivo de segurança específico. Vejamos como funciona na figura.

Figura 4 - Posicionamento do IDS na rede



Fonte: Nakamura (2007)

- IDS 1 – detectando qualquer tipo de ataque contra a rede da empresa, como exemplo ataques a servidores web inválidos.
- IDS 2 – operando com o *firewall,* será capaz de detectar ataques ao *firewall.*
- IDS 3 – detectando ataques que passaram pelo *firewall*, tendo como alvo os servidores que ficam localizados na DMZ.
- IDS 4 – com o objetivo de atacar a rede interna, através da VPN.

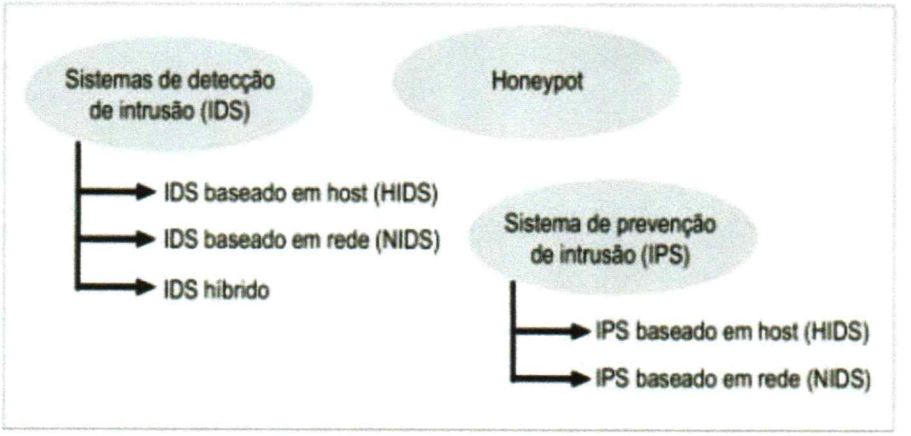
• IDS 5 – detectando tentativas contra os servidores na DMZ 2, que passaram pela segurança no *firewall*, na VPN e DMZ 1, somente é possível acesso via VPN ou algum servidor localizado na DMZ 1.

• IDS 6 – essa posição é a mais importante na área interna da organização. Com o acesso mais intenso faz com que a vigilância interna tenha um resultado satisfatório para o ambiente cooperativo.

2.3.8.3 Tipos de IDS

Conforme Nakamura (2007), existem dois tipos primários, *Host-Based Intrusion Detection System* – HIDS e *Network-Based Intrusion Detection System* – NIDS. Foi desenvolvido outro a partir das características do HIDS e NIDS, chamado de *Hybrid* IDS. O *Honeypot* tem a funcionalidade de um IDS, com a capacidade de detectar e armazenar todo tipo de ataque. Com o passar do tempo surgiu o *Intrusion Prevention System* – IPS, com a finalidade de prevenir os ataques a rede da organização.

Figura 5 - Tipos de IDS e IPS

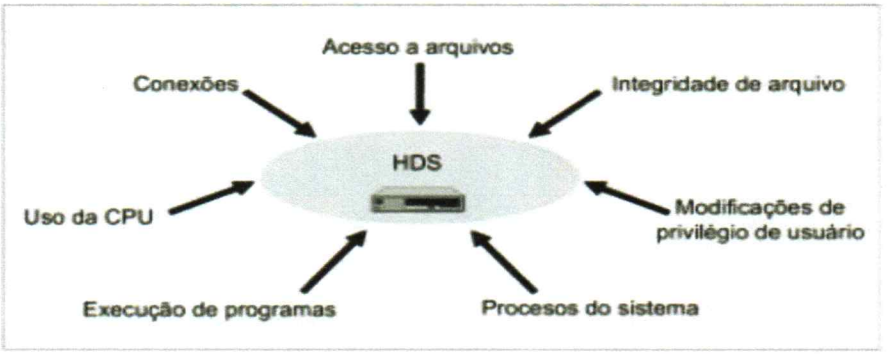


Fonte: Nakamura (2007)

- ***Host-Based Intrusion Detection System* – HIDS**

O sistema de detecção de intrusão baseado em *host,* faz a vigilância constante com base em *logs* ou agentes de auditoria. Segundo Nakamura (2007), os HIDS monitoram direto na máquina onde as alterações e acessos em arquivos do sistema, processos e execuções de programas, e *port scanning.* A figura mostra algumas detecções feitas pelo HIDS.

Figura 6 - Tipos de detecção do HIDS



Autor: Nakamura (2007)

Segundo Cheswick (et al. 2005), os sistemas de detecção de intrusão baseados em *host*, quando configurados tendem a conhecer todo o funcionamento da máquina, porém se o HIDS tiver algum tipo de problema com o *host,* seu objetivo estará comprometido.

- ***Network-Based Intrusion Detection System* – NIDS**

De acordo com Nakamura (2007), o NIDS possui sensores de monitoramento em tempo real, que faz a captura de dados no tráfego de rede, assim analisando os pacotes e comparando seu conteúdo com os padrões de regras configuradas ou assinaturas conhecidas pelo *software.* Eficaz contra ataques de *port scanning*, *IP spoofing* ou *SYN flooding.*

2.3.9 Sistema de Prevenção de Intrusão (IPS)

Cheswick (et al. 2005), sistemas baseados em prevenção de ataque de rede atuam de forma independentes, consequentemente mais seguro a ataques e detecção.

Sistemas que operam em modo ativo ou chamado de *inline,* com características como a de um *firewall*, onde todos os dados da rede da organização passa pelo sistema. Além da função detecção, pode prevenir os ataques fazendo com que os mesmos não cheguem aos servidores, causando danos a organização. Nakamura (2007), como funcionam as premissas de um IPS.

- Todos os comandos antes de serem executados, devem passar pelo *kernel.*

- Todos os privilégios de um administrador, modificação de registros ou de arquivos de sistema, execução *buffer overflow,* devem possuir o mesmo teor de objetivos.

De acordo com Ferreira (2015), existem formas diferentes de classificar os sistemas de detecção e prevenção de intrusão.

- IPS de *host* atua diretamente na máquina junto com outras aplicações já instaladas, compartilhando do mesmo *hardware,* monitorando todas as requisições permitindo que somente as confiáveis cheguem ao destino.
- IPS de rede executa entre o *firewall* e a rede externa ou *firewall* e a rede interna, tem a capacidade de analisar, detectar e bloquear tráfego malicioso de acordo com as regras definidas.
- IPS de conteúdo, atua analisando o conteúdo dos pacotes, procurando por padrões de assinaturas para garantir a prevenção de ataques conhecidos. Exemplo: *worms.*
- IPS *Rate Based,* com o objetivo de reduzir os ataques de DDos, monitora em tempo real os comportamentos anormais no tráfego de rede, armazena-nos para quando ultrapassar os limites o IPS reconhecer de imediato uma tentativa de ataque a rede.

2.3.10 Ferramentas IDS / IPS (*Open Source*)

Atualmente estão disponíveis diversas ferramentas *open source* para detecção de intrusões, cada uma com sua particularidade, exemplo são as que possuem a capacidade de prevenir de uma intrusão. O administrador escolhe de acordo com a necessidade de sua rede. A seguir serão destacadas algumas ferramentas de detecção de intrusão: OSSEC, Suricata, Samhain, HLBR e *Snort.*

2.3.10.1 OSSEC

Projetado por Daniel B. Cid, OSSEC é um sistema de detecção de intrusão baseado em *host* (HIDS), *software* livre de multi-plataforma executado na maioria dos sistemas operacionais, incluindo Linux, OpenBSD, FreeBSD, MacOS, Solaris e Windows. Pode ser modificado e redistribuído de acordo com os termos da GNU (*General Public License* v.2) conforme publicado pela FSF (*Free Software Foundation*).

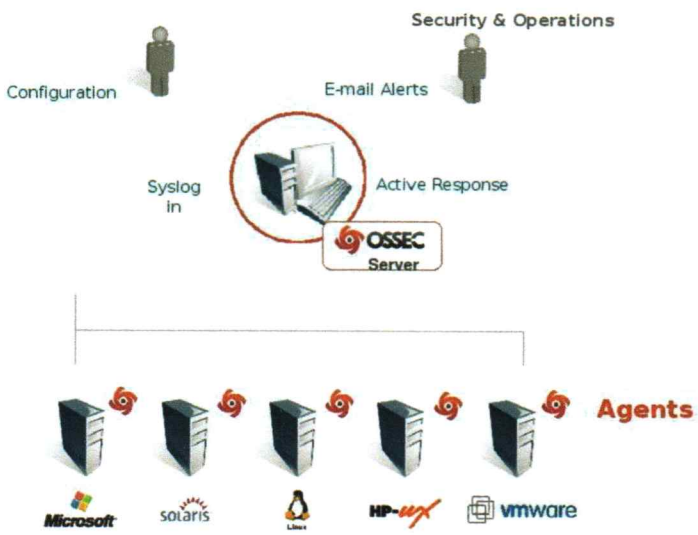
Com uma média de mais de 5.000 *donwloads* por mês. Usado por universidades e grandes corporações o OSSEC oferece análise de log, monitorando o *firewall*, ferramentas de IDS, servidores web. Possui comunidade OSSEC Github com apoio de voluntários, onde são identificados, processados e corrigidos os problemas, basta obedecer às regras de boa convivência (OSSEC, s.d.). No presente momento se encontra na versão 2.8.3, acesse o site para obter o manual, informações sobre o desenvolvimento do sistema e referências da ferramenta.

Arquitetura do OSSEC baseia-se em:

- Gerente ou servidor – armazena todos os bancos de dados, de verificação, os registros, eventos de auditoria do sistema e todas as regras para facilitar a administração.
- Agentes – são sistemas de pequeno porte, que irá coletar informações e redirecionar para o gerente.
- *Agentless* – quando um sistema de agente não tem permissão para ser instalado, utiliza o suporte de verificação de integridade que permite monitorar *firewalls,* roteadores através de eventos de *syslog*.

A seguir, diagrama apresentando o funcionamento do sistema, onde o gerente recebi as informações dos agentes e logs do sistema. Se a detecção de um ataque o administrador é informado.

Figura 7 - Diagrama de funcionalidade do sistema OSSEC



Autor: OSSEC (s.d.).

2.3.10.2 Suricata

O Suricata é um sistema de IDS e IPS de código aberto que faz um monitoramento de alto desempenho na rede. Desenvolvido por OISF (*Open Information Security Foundation*) uma fundação sem fins lucrativos com um grupo de desenvolvedores de *softwares* de setor de segurança multinacional. (Suricata, s.d.).

O sistema oferece uma lista de recursos:

- Sistema de Detecção de Intrusão de Rede (NIDS);
- Sistema de Prevenção de Intrusão de Rede (NIPS);
- Monitoramento de Segurança de Rede (NSM);
- Análise fora da linha de arquivos PCAP;
- Registro de tráfego usando pcap *logger;*
- Modo de soquete Unix para processamento automático de arquivos PCAP;
- Integração avançada com o *firewall* Linux Netfilter.

Um sistema de multi-plataforma (Linux, FreeBSD, OpenBSD, MacOS / Mac OS X e janelas) altamente escalável, possui um mecanismo multi *thread* que permite inspecionar uma grande quantidade de tráfego na rede. O Suricata 4.0 recentemente lançado, funciona com maior velocidade e eficiência na análise dos pacotes, detecta automaticamente protocolos como HTTP aplicando as regras e assinaturas poderosas armazenadas.

2.3.10.3 Samhain

Sistema baseado em *host* (HIDS) criado por Rainer Wichmann, serviço monitoramento portas e verificação de integridade de arquivos, analisando os logs de arquivos, detecção de *rootkit,* processo ocultos e fraudulentos. Utilizando licença GNU, o *software* oferece seus serviços em diferentes plataformas operacionais (Linux, * BSD, Solaris 2.x, AIX 5.x, HP-UX 11, Mac OS X e Windows).

Pode ser usado em um único *host* de modo autônomo ou em vários *hosts,* sua particularidade é o monitoramento e gerenciamento centralizado. Um sistema cliente / servidor completo é constituídos dos seguintes componentes (SAMHAIN, s.d.):

- O verificador de integridade do arquivo samhain / host - é o cliente / agente no host monitorado. É executado como um *daemon*, evitando avisos repetitivos.
- Servidor de *log* Yule – Coleta, registra relatórios, acompanha o status dos clientes em hosts remotos.

- Uma base de dados relacional – compatível com *Oracle, MySQL, PostgreSQL,* armazena os relatórios dos clientes.
- Console baseado em web – Beltane é um aplicativo PHP separado do pacote disponível, permite extrair relatórios e apresentá-los.

Sistema de implantação – opcional facilita a implantação de clientes de Samhain.

2.3.10.4 HLBR

Uma ferramenta brasileira, Hogwash Light (HLBR) foi criada no ano de 2005 e desenvolvida por Jason Larsen em 1996, mantida pelos líderes do projeto André Berelli Araújo e João Eriberto Mota Filho.

HLBR é um *software* de IPS (*Intrusion Prevention System*) filtrando pacotes de dados diretamente na camada 2 do modelo OSI, não necessitando do IP da máquina que está instalado. A detecção é feita com regras simples, permitindo o próprio usuário adicionar novas assinaturas ao banco de dados do sistema.

Ferramenta bastante eficiente, pode ser utilizada em *bridge* para *honeypots* e *honeynets.* Como não necessita de TCP/IP é impossível de ser identificada na rede. Devido a *bugs* o projeto foi interrompido desde a agosto de 2013 (HLBR, s.d.).

2.3.10.5 Snort

Ferramenta desenvolvida por Martin Roesch e fundador da empresa Sourcefire que foi adquirida pela Cisco Systems no ano de 2013.

Snort é uma ferramenta *open source* para prevenção de intrusão de rede, capaz de fazer análises do tráfego em tempo real e log de pacotes na rede. Pode ser usada para detectar diversos ataques e monitorar, como varredura de porta, vazamento de *buffer,* tentativas de impressão digital e outros (*Snort*, s.d.).

Um sistema de multi-plataforma que encontrasse na versão estável 2.9.9.0, também distribui versões pagas da ferramenta.

O sistema opera em três modos:

- Modo *sniffer* – faz a leitura de pacotes no tráfego da rede e apresenta o resultado no console (tela);
- Modo *packet logger* – registra os pacotes capturados no disco;

- Modo detecção de intrusão (NIDS) – sendo o mais completo, detecta e compara os pacotes da rede com as regras e assinaturas predefinidas pelo usuário. Muitas dessas regras são compartilhadas por outros usuários que estão disponíveis na internet.

A arquitetura do *Snort* é composta de 4 componentes básicos:

- *Sniffer* – sendo um mecanismo de captura (farejador), o sensor do sistema faz a captura dos pacotes que passam pelo mecanismo de detecção e que por sua vez realizar a decodificação para os protocolos da camada enlace.
- O pré-processador – ele verifica se esse pacote é algo que ele deve examinar, alertar a respeito ou modificar.
- O mecanismo de detecção – com o papel de verificar os pacotes com uma lista de opções de regras do *Snort.* As opções de palavra-chave são vinculadas a um *plugin* que realiza testes adicionais.
- Plugins de saída – apresenta os resultados dos alertas.

O *Snort* e uma boa ferramenta, mas como todo sistema deve ser bem implementado. Aplicando somente as assinaturas de ataques relevantes a realidade da rede, ou seja, as que realmente encontrasse em uso.

2.3.10.6 Comparativo entre ferramentas

Tabela 2 - Comparativo entre ferramentas

ASPECTO	OSSEC	Suricata	Samhain	HLBR	Snort
Tipo de sistema	HIDS	NIDS	HIDS	NIPS	NIDS
Multi-plataforma	SIM	SIM	SIM	NÃO	SIM
Open source	SIM	SIM	SIM	SIM	SIM
Suporte IPS	SIM	SIM	NÃO	SIM	SIM
Gera logs	SIM	SIM	SIM	SIM	SIM
Dispara alertas	SIM	SIM	SIM	SIM	SIM
Análise em tempo real	SIM	SIM	SIM	SIM	SIM
Boa documentação	SIM	SIM	SIM	NÃO	SIM
Suporte à interface gráfica	SIM	SIM	SIM	NÃO	SIM

Fonte: Autor

Podemos notar na Tabela 2 que as cinco ferramentas apresentadas possuem o código fonte aberto, onde a ferramenta brasileira HLBR é a única ferramenta exclusiva com IPS nativo, mas o projeto foi interrompido. Os sistemas Samhain e

OSSEC são baseados em *host*. Todas as ferramentas possuem características em comum, dispara alertas, análise em tempo real e gera *logs*. Os sistemas *Snort* e Suricata são baseados em sistemas de detecção de intrusão de rede, ambos são capazes de operar como IPS, basta habilitar a função.

Diante das várias ferramentas analisadas, o presente trabalho optou para detalhar o *Snort* que se encontra na versão estável 2.9.9.0, sendo a mais popular entre as ferramentas. Segundo *Snort* (s.d.) com mais de 5 milhões de *downloads* e mais de 600.000 usuários cadastrados, é o sistema de prevenção de intrusão mais utilizado no mundo.

2.3.11 Política de Segurança

De acordo com Paiva (2017), a Política de Segurança da Informação (PSI) é um documento que contém um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os colaboradores da organização, através de cartilhas, *workshops,* campanhas de conscientização.

> A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. A necessidade de estabelecer uma política de segurança é um fato realçado unanimemente em recomendações provenientes tanto do meio militar (como o *Orange Book* do Departamento de Defesa dos Estados Unidos) como do meio técnico (como o *Site Security Handbook* [*Request for Commennts* – RFC] 2196 do *Institute Engineering Task Force*, IETF) e, mais recentemente, do meio empresarial (norma *International Standardization Organization/International Electricaltecnical Commission* (ISO/IEC 17799), Nakamura (2007, p.188).

Segundo Comer (2007), nenhuma rede é totalmente segura, mas obter uma boa política de segurança irá mostrar onde estão os itens a serem protegidos. As políticas são bem complexas por que são um conjunto de comportamento humano tanto quanto computador e redes. Por isso é importante que cada organização identifique os aspectos de proteção que são mais importantes.

A Política de Segurança da Informação, não é uma receita de bolo, pois os ingredientes utilizados nela variam de organização para organização, o que torna impossível alcançar o mesmo resultado, ou seja, cada organização deve elaborar sua própria PSI com base na sua cultura organizacional. A PSI possui cinco características para não cair no descrédito:

- Política verdadeira
- Ter patrocínio da direção
- Não ser um manual
- Não ser um documento técnico
- Ser simples

Para uma boa PSI leva-se em consideração as normas NBR ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, essas normas possuem códigos de práticas para gerenciamento da segurança da informação, como iniciar, implementar, manter, avaliar riscos, controles que auxiliam na aplicação do Sistema de Gestão da Segurança da Informação (SGSI).

2.3.12 Normas de Segurança da Informação

Com a expansão da Tecnologia da Informação (TI) aliada a constante preocupação em garantir a integridade da informação, fez surgir normas capazes de garantir a segurança da informação dentro da organização.

De acordo com Paiva (2017, pag.122),

> As normas de Segurança da Informação (SI) são padrões e regras internacionais, cujo objetivo é manter as melhores práticas e qualidades no desenvolvimento de ações para a proteção das informações nas organizações, tais como: desenvolvimento de uma política de segurança da informação, implantação de um sistema de gerenciamento de segurança da informação, implantação de controles físicos e lógicos a fim de manter a SI, e etc.

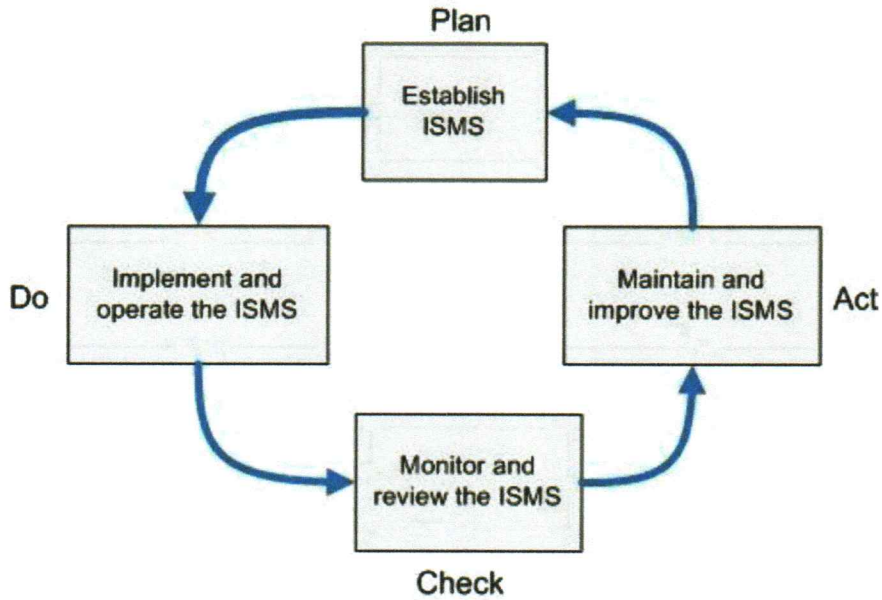
- **ISO 27001**

A Norma ISO/IEC 27001, é um padrão internacional que define requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Seu objetivo principal é aplicar um conjunto de requisitos, processos e controles para que possam reduzir e gerenciar os riscos que envolvi as suas informações.

A partir da adoção desta norma as organizações podem optar por um modelo e padrão internacional de estabelecimento, operação, monitorização, revisão e gestão de um SGSI. A norma é estruturada no ciclo PDCA (*Plan-Do-Check-Act*):

- ***Plan*** (estabelecer): o entendimento dos requisitos e a necessidade de se ter uma política da segurança da informação.
- ***Do*** (implementar): implementar e operar controles para gerenciamento dos riscos.
- ***Check*** (monitorar): monitora o desemprenho e a eficácia da política de segurança da informação.
- ***Act*** (melhoria): promover a melhoria continua.

Figura 8 - Estrutura PDCA (*Plan-Do-Check-Act*)



Fonte: http://www.governancadeti.com/2011/01/governanca-de-ti-seguranca-da-informacao-%E2%80%93-normas-iso-27000/

- **ISO 27002**

A ISO/IEC 27002, a norma fornece um guia completo de implementação e continuidade na gestão de SI (Sistema de Informação), expondo métodos para determinar os controles que são necessários para o SGSI baseados nas avaliações de níveis de riscos realizados pela organização.

É a norma internacional que está estruturada em seções. Cada seção tem uma serie de controles que podem ser implementados de acordo com a necessidade da organização. São 130 controles que podem ser implementados, dividido entre as seções a seguir:

- Política da segurança da informação

- Organizando a segurança da informação
- Gestão de ativos
- Segurança em recursos humanos
- Segurança física do ambiente
- Gestão das operações e comunicações
- Controle de acesso
- Aquisição, desenvolvimento e manutenção de sistemas de informação
- Gestão de incidentes da segurança da informação
- Gestão da continuidade do negócio
- Conformidade

- **ISO 27005**

A norma ISO/IEC 27005, fornece as diretrizes para análise, avaliação e o gerenciamento dos riscos de SI e apoiando os conceitos especificados na ISO 27001. Destacando como conceito principal:

- Risco – onde a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos, posteriormente prejudicando a organização.
- Medida de risco – é a combinação da probabilidade de um evento indesejável e a sua consequência.

A norma recomenda que seja aplicada da seguinte maneira:

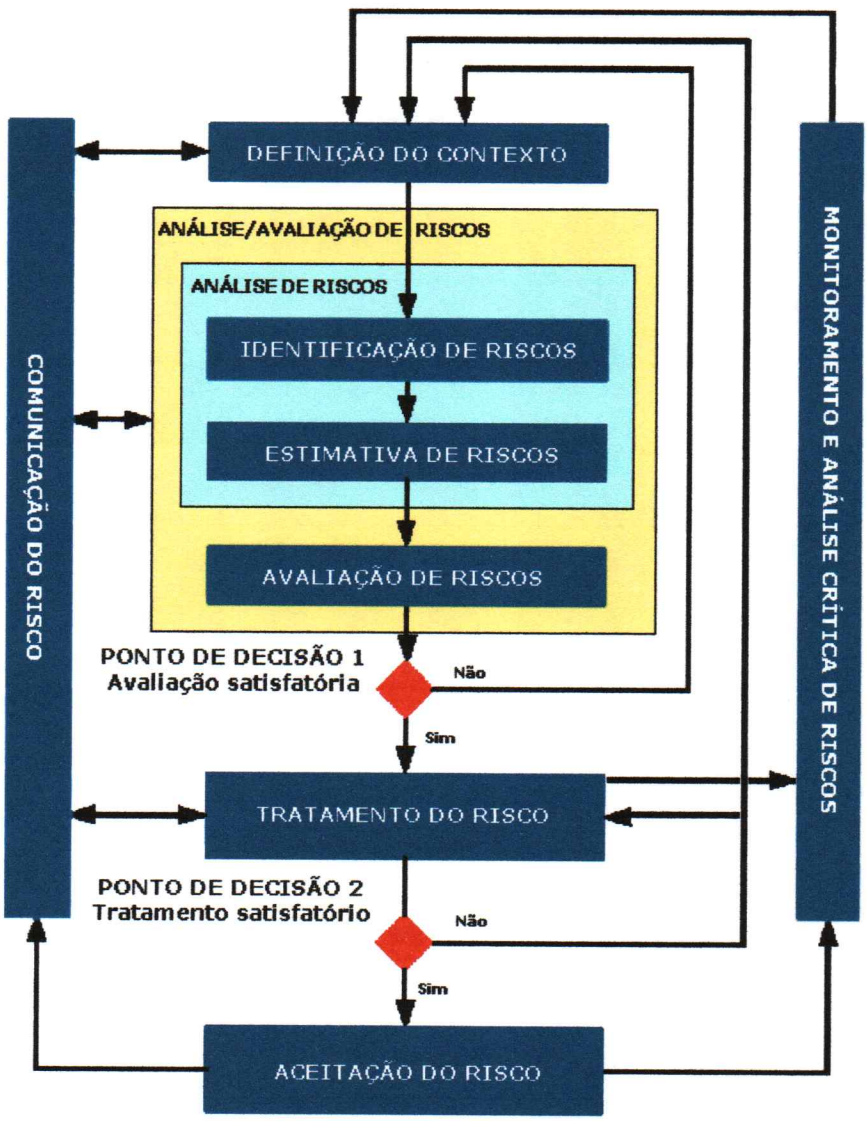
1 – Contextualização, definindo os conjuntos de elementos: o escopo, o objetivo, os métodos, os critérios básicos e a área organizacional responsável pelo processo de GRSI.

2 – Analisando o risco, aqui são identificados os eventos que possam causar perdas, ou seja, identificadas as ameaças. Também devemos identificar os controles existentes e a eficácia destes controles para que evite que uma ameaça explore as vulnerabilidades na organização. Com isso podemos identificar o nível do risco.

3 – Avaliando o risco, nesta etapa é elaborada uma lista de risco de entrada com níveis de valores designados e outra lista de saída de risco ordenadas por prioridades. Exemplo: risco de nível alto, com baixo impacto financeiro, não necessariamente deva ser priorizado antes de um nível médio, mas com grande impacto financeiro.

A Gestão de Riscos de Segurança da Informação (GRSI) considerado como uma das dimensões de processo de segurança da informação, compõe o conjunto que possibilita que o processo de SI aconteça de maneira eficiente, eficaz e continuo ao longo do tempo.

Figura 9 - Processo de gestão de riscos de SI



Fonte: https://www.qsp.org.br/artigo_27005.shtml

CAPÍTULO 3

3. GUIA DE INSTALAÇÃO E CONFIGURAÇÃO DA FERRAMENTA *SNORT*

Neste capítulo é descrito o processo de instalação e configuração da ferramenta utilizada para alcançar os objetivos propostos.

3.1 Aspectos metodológicos

Com o intuito de atingir os objetivos de gerar um guia de instalação e configuração da ferramenta, de forma atualizada, um sistema de detecção de intrusão, foi escolhido um ambiente de sistema operacional Ubuntu Server 16, para integração da ferramenta *Snort*. Todas as informações a seguir foram obtidas no site do snort.org/documents.

Uma observação a se fazer é que o usuário que pretende usar a ferramenta *Snort* tenha um conhecimento básico de utilização do sistema operacional Linux.

3.2 Pré-requisitos de instalação *Snort*

Primeiramente devemos instalar todos os pacotes necessários para o uso da ferramenta:

- pcap (libpcap-dev) disponível no repositório do Ubuntu;
- PCRE (libpcre3-dev) disponível no repositório do Ubuntu;
- Libdnet (libdumbnet-dev) disponível no repositório do Ubuntu;
- DAQ disponível (http://www.snort.org/downloads/).

Entre com o comando a seguir para instalar as ferramentas necessárias:

```
sudo apt-get install -y build-essential
```

Após as ferramentas de compilação instaladas, em seguida instalamos todos os pré-requisitos *Snort* disponíveis no repositório do Ubuntu:

```
sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev
```

Instale os pré-requisitos disponíveis na biblioteca do Snort.org:

```
sudo apt-get install -y bison flex
```

Vamos criar uma pasta para organizar uma série de pacotes de arquivos que serão baixados em seguida:

```
mkdir ~/snort_src
cd ~/snort_src
```

Baixe e instale a versão mais recente do DAQ que está disponível no site Snort.org, no momento a versão disponível é 2.0.6:

```
cd ~/snort_src
wget https://snort.org/downloads/snort/daq-2.0.6.tar.gz
tar -xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
make
sudo make install
```

Quando você executa ./configure, observe a saída que mostra quais os módulos estão sendo configurados e que estarão disponíveis quando compilar o DAQ:

```
Build AFPacket DAQ module.. : yes
Build Dump DAQ module..... : yes
Build IPFW DAQ module..... : yes
Build IPQ DAQ module..... : no
Build NFQ DAQ module..... : no
Build PCAP DAQ module..... : yes
Build netmap DAQ module..... : no
```

3.3 Instalando *Snort*

Para instalar o *Snort* no Ubuntu, existe um pré-requisito necessário adicional que precisa ser instalado, que não é mencionado na documentação: zlibg (biblioteca de compressão):

```
sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev
```

Precisamos das bibliotecas de desenvolvimento para Nghttp2: uma biblioteca HTTP / 2 C que implementa o HPAC algoritmo de compressão de cabeçalho:

```
sudo apt-get install -y libnghttp2-dev
```

Após todos os pré-requisitos estão instalados, estamos prontos para fazer o download da ferramenta *Snort*, para compilar e em seguida instalar:

```
cd ~/snort_src
wget https://snort.org/downloads/snort/snort-2.9.9.0.tar.gz
tar -xvzf snort-2.9.9.0.tar.gz
cd snort-2.9.9.0
./configure --enable-sourcefire
make
sudo make install
```

Executando esse comando atualizará as bibliotecas compartilhadas:

```
sudo ldconfig
```

Coloque um link simbólico na pasta binário *Snort*:

```
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Vamos fazer um teste como um usuário comum usando o comando –V, onde informa ao *Snort* para verificar todos os arquivos passados para ele. Em seguida observe uma tela com as informações semelhante a essa:

```
user@snortserver:~$ snort -V
        ,,_     -*> Snort! <*-
       o"  )~   Version 2.9.9.0 GRE (Build 56)
         ""     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
                Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
                Copyright (C) 1998-2013 Sourcefire, Inc., et al.
                Using libpcap version 1.7.4
                Using PCRE version: 8.38 2015-11-23
                Using ZLIB version: 1.2.8
user@snortserver:~$Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
user@snortserver:~$
```

3.4 Configurando para executar em modo NIDS

Não queremos que o *Snort* seja executado como root, então vamos criar uma conta e um grupo não privilegiados para que seja executado em snort:snort, além

disso criaremos vários arquivos e diretórios exigidos pela ferramenta e definiremos permissões nesses arquivos:

```
# Create the snort user and group:
sudo groupadd snort
sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
# Create the Snort directories:
sudo mkdir /etc/snort
sudo mkdir /etc/snort/rules
sudo mkdir /etc/snort/rules/iplists
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo mkdir /etc/snort/so_rules
# Create some files that stores rules and ip lists
sudo touch /etc/snort/rules/iplists/black_list.rules
sudo touch /etc/snort/rules/iplists/white_list.rules
sudo touch /etc/snort/rules/local.rules
sudo touch /etc/snort/sid-msg.map
# Create our logging directories:
sudo mkdir /var/log/snort
sudo mkdir /var/log/snort/archived_logs
# Adjust permissions:
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /var/log/snort/archived_logs
sudo chmod -R 5775 /etc/snort/so_rules
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

Agora vamos garantir que o *Snort* tenha total acesso aos arquivos criados acima:

```
# Change Ownership on folders:
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

O *Snort* precisa de alguns arquivos de configuração e os pré-processadores dinâmicos copiados do código fonte *Snort* para a pasta /etc/snort. Os arquivos de configuração são:

- classication.cong
- le magic.conf
- reference.cong
- snort.conf
- threshold.conf
- attribute table.dtd
- gen-msg.map
- unicode.map

Execute os seguintes comandos para copiar os arquivos de configuração e os pré-processadores dinâmicos:

```
cd ~/snort_src/snort-2.9.9.0/etc/
sudo cp *.conf* /etc/snort
sudo cp *.map /etc/snort
sudo cp *.dtd /etc/snort
cd~/snort_src/snort-2.9.9.0/src/dynamic-
preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

Agora teremos os seguintes layout de diretório e os locais:

Snort binary le:	/usr/local/bin/snort
Snort conguration le:	/etc/snort/snort.conf
Snort log data directory:	/var/log/snort
Snort rules directories:	/etc/snort/rules
	/etc/snort/so rules
	/etc/snort/preproc rules
	/usr/local/lib/snort dynamicrules
Snort IP list directories:	/etc/snort/rules/iplists
Snort dynamic preprocessors:	/usr/local/lib/snort dynamicpreprocessor/

A listagem de diretórios *Snort* serão apresentadas dessa maneira:

```
user@snortserver:~$ tree /etc/snort
/etc/snort
|-- attribute_table.dtd
|-- classification.config
|-- file_magic.conf
|-- gen-msg.map
|-- preproc_rules
|-- reference.config
|-- rules
| |-- iplists
| | |-- black_list.rules
| | |-- white_list.rules
| |-- local.rules
|-- sid-msg.map
|-- snort.conf
|-- so_rules
|-- threshold.conf
|-- unicode.map
```

A seguir vamos editar o principal arquivo de configuração do *Snort*, onde precisaremos editar as regras individualmente para serem executadas no modo NIDS.

```
sudo sed -i "s/include \$RULE\_PATH/#include \$RULE\_PATH/"
/etc/snort/snort.conf
```

Alterando manualmente algumas configurações no snort.conf:

```
sudo vi /etc/snort/snort.conf
```

Para atender ao seu ambiente altere as seguintes linhas, onde o HOME NET deve ser correspondente à sua rede interna, exemplo 10.0.0.0/24:

```
ipvar HOME_NET 10.0.0.0/24
```

Vamos definir os seguintes caminhos no snort.conf:

```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Agora, vamos habilitar o arquivo local.rules removendo a hashtag, onde podemos adicionar regras que o *Snort* possa usá-las:

```
include $RULE_PATH/local.rules
```

A seguir executamos o seguinte comando para testar o arquivo de configuração e especificar a interface que a ferramenta irá ouvir:

```
user@snortserver:~$ sudo snort -T -i eth0 -c /etc/snort/snort.conf
(...)
Snort successfully validated the configuration!
Snort exiting
user@snortserver:~$
```

3.5 Escrevendo uma regra simples para testar a detecção do *Snort*

Vamos testar as habilidades de detecção do *Snort*, criamos uma regra simples que fará com que a ferramenta gere um alerta sempre que veja uma solicitação de ICMP pedido ou resposta, utilizando o ping será fácil detectar. Para colar as regras locais utilize a linha (/etc/snort/rules/local.rules):

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1;
sid:10000001; rev:001; classtype:icmp-event;)
```

Uma coisa importante é toda vez que inserimos uma nova regra no *Snort*, devemos testar novamente o arquivo de configuração:

```
sudo snort -T -c /etc/snort/snort.conf -i eth0
```

Observe na tela a regra que criamos identificou uma solicitação de ICMP:

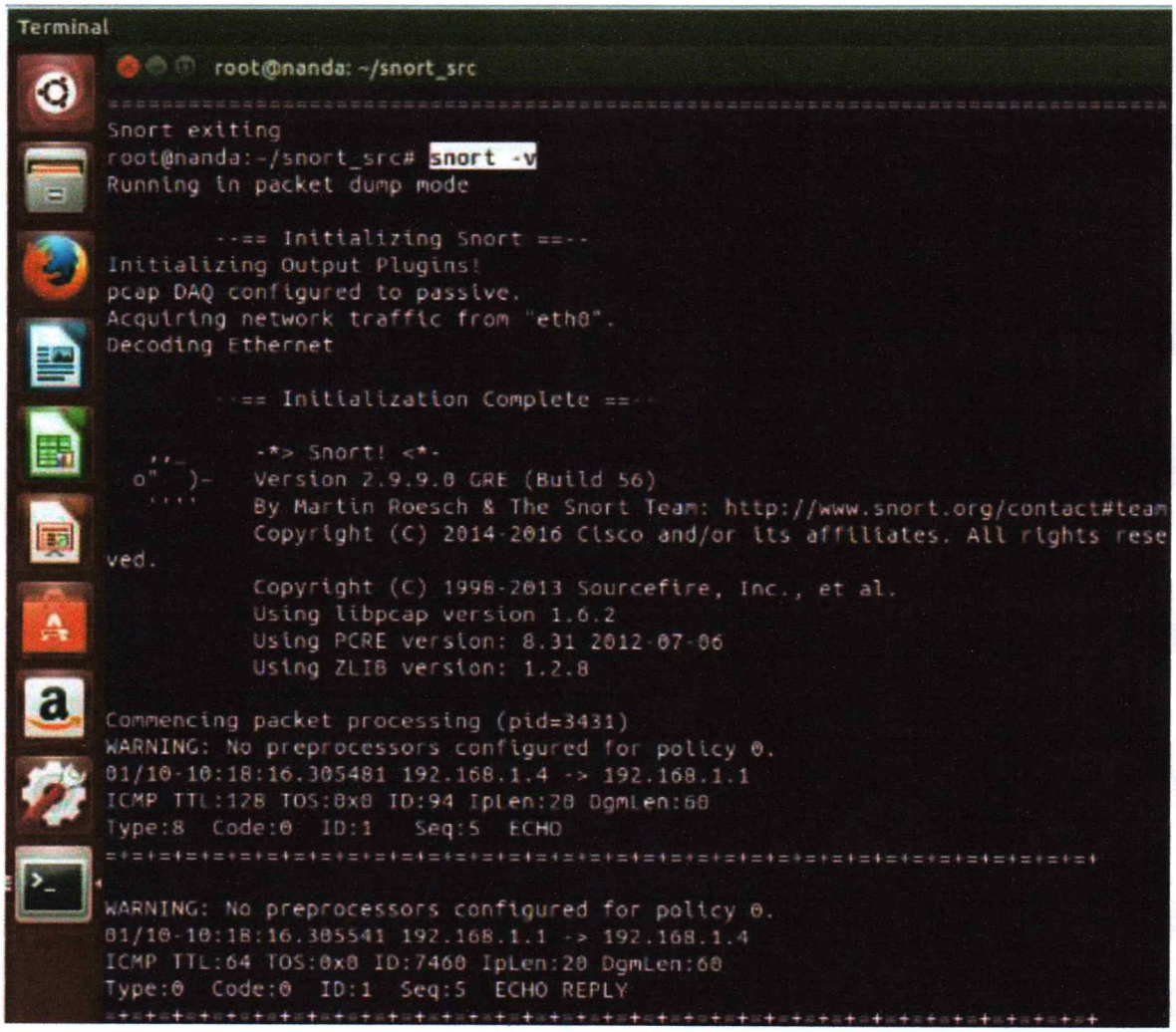
```
(...)
++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
1 detection rules
0 decoder rules
0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
0 Dynamic rules
++++++++++++++++++++++++++++++++++++++++++++++++++++
+----------------[Rule Port Counts]-----------------------------------
| tcp udp icmp ip
| src 0 0 0 0
| dst 0 0 0 0
| any 0 0 1 0
| nc 0 0 1 0
| s+d 0 0 0 0
+--------------------------------------------------------------------
```

Agora que sabemos que o *Snort* carrega as regras e os arquivos de configuração, segue alguns dos principais comandos do *Snort*:

-A console	apresenta de modo mais rápido os alertas.
-q.	modo silencioso.
-u snort	execute o Snort como o seguinte usuário após a inicialização.
-g snort	execute o Snort como o seguinte grupo após a inicialização.
-c /etc/snort/snort.conf	o caminho para configurar o Snort.
-i eth0	ouvir a interface que você utiliza.

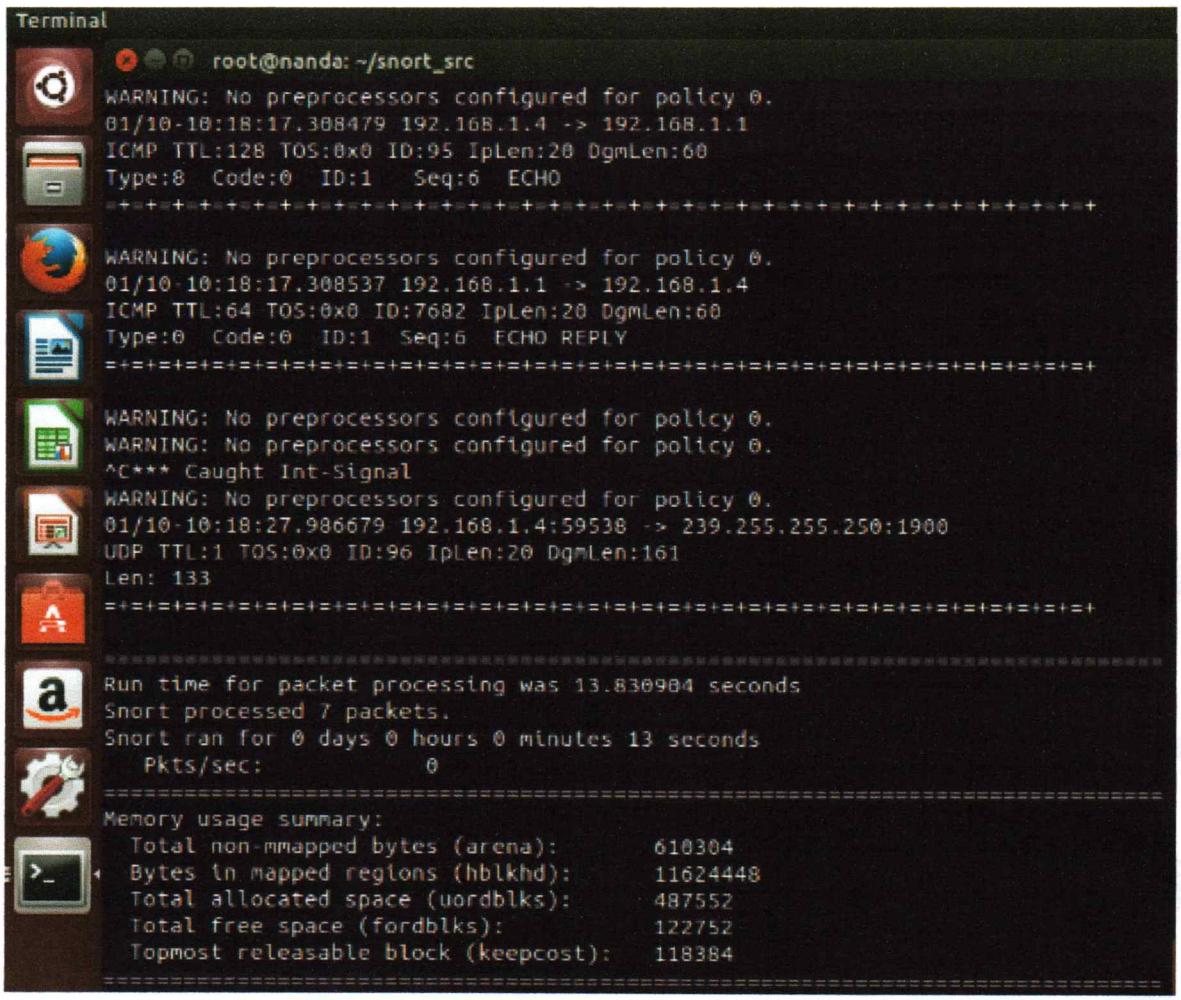
3.6 Telas do *Snort*

Figura 10 - Inicialização do *Snort*



Fonte: https://steemkr.com/utopian-io/@woking/implementation-sistem-intruder-detection-system-ids-in-ubuntu-14-04-part-1

Figura 11 - Rodando o *Snort* -v

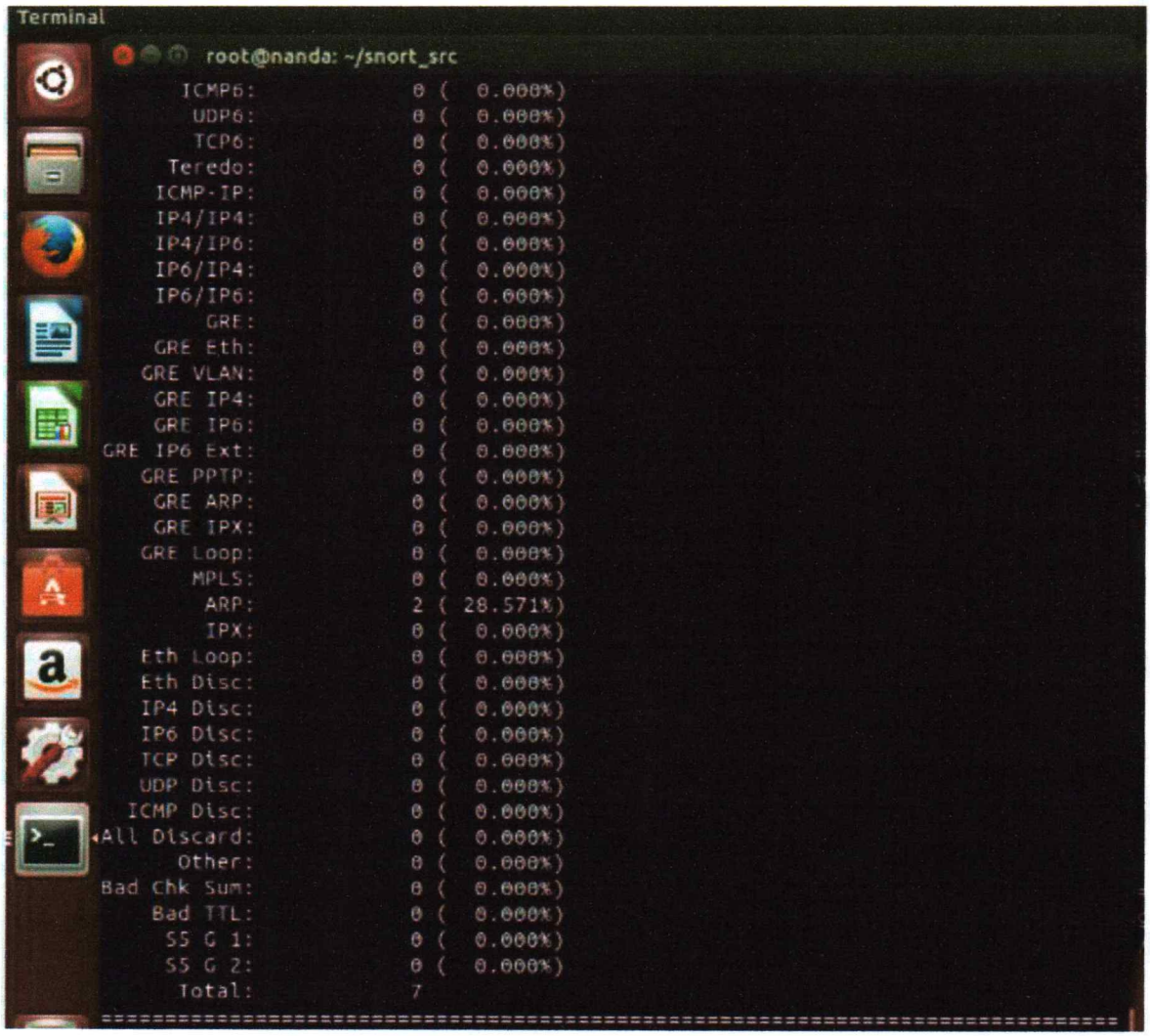


Fonte: https://steemkr.com/utopian-io/@woking/implementation-sistem-intruder-detection-system-ids-in-ubuntu-14-04-part-1

Figura 12 - Alerta de detecção

Fonte: https://steemkr.com/utopian-io/@woking/implementation-sistem-intruder-detection-system-ids-in-ubuntu-14-04-part-1

Figura 13 - Resultado da detecção



Fonte: https://steemkr.com/utopian-io/@woking/implementation-sistem-intruder-detection-system-ids-in-ubuntu-14-04-part-1

4. CONCLUSÃO

4.1 Considerações finais

A elaboração deste trabalho apresentou as melhores formas de como se proteger contra ataques ou intrusos, utilizando ferramenta *open source* IDS (*Intrusion Detection System*) *Snort,* a fim de analisar essa alternativa de proteção como forma de prevenir problemas recorrentes de redes, tais como invasão na intranet; roubo de informações sigilosas; perdas e paralisação nos serviços. Foram abordados conceitos básicos, procedimentos de segurança, descrição de IDS e IPS, tipos de ameaças e ataques a redes, comparações das melhores ferramentas IDS, guia de instalação e configuração da ferramenta *Snort.*

A realização deste estudo contribui de forma significativa para aqueles que buscam conhecimentos na área de segurança de redes. Dessa forma, é possível concluir que, o guia de instalação e configuração da ferramenta *Snort* estará somando na dura batalha pela obtenção de segurança de redes.

4.2 Trabalhos futuros

Com o tema abordado por este trabalho, é pertinente a continuação deste estudo, na busca por maior eficiência em termos de segurança em redes. Segue temas para as futuras pesquisas:

- Implementação da ferramenta *Snort* em servidores corporativos, através do uso do guia configuração e instalação deste estudo;
- Estudo de ferramentas de Sistemas de Prevenção de Intrusão IPS;
- Análise de ferramentas que são baseadas em assinaturas trazendo sua eficiência;
- Utilização e teste de eficácia do *Snort* juntamente com o *firewall.*
- Organizar um manual de instalação do *Snort.*

5. REFERÊNCIAS

ARPANET. **O QUE É ARPANET**. Disponível em <https://sites.google.com/site/sitesrecord/o-que-e-arpanet>. Acesso em: 19 de ago. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em: < https://cartilha.cert.br/criptografia/>. Acesso em: 21 mar. 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em: < https://cartilha.cert.br/mecanismos/>. Acesso em: 20 mar. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 30 mar. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 06 mai. 2017.

CHESWICK, WILLIAM R. ET AL. **Firewalls e Segurança na Internet: Repelindo o hacker ardiloso**. Bookman. Porto Alegre. 2005.

CICCO, FRANCESCO. **A NOVA NORMA INTERNACIONAL ISO 27005 DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO**. Disponível em: < https://www.qsp.org.br/artigo_27005.shtml>. Acesso em: 13 fev. 2018.

COMER, DOUGLAS E. **Rede de Computadores e Internet**. Boockman. 4. ed. Porto Alegre. 2007.

CONTROLE NET. **RAID, arranjos de discos para trabalho em conjunto. O que é RAID?**. Disponível em: <https://www.controle.net/faq/qual-o-melhor-raid-a-ser-usado>. Acesso em: 3 fev. 2018.

DOROW, EMERSON. **Governança de TI: Segurança da Informação – normas ISO 2700**. Disponível em: <http://www.governancadeti.com/2011/01/governanca-de-ti-seguranca-da-informacao-%E2%80%93-normas-iso-27000/>. Acesso em: 03 mar. 2017.

EZEQUIEL, JULIANO. **Normas de Segurança da Informação**. Disponível em: < http://www.ezequieljuliano.com.br/?p=59>. Acesso em: 19 mar. 2018.

Ferreira, Carlos. **Segurança de redes com IPS, sua relação com IDS e sua importância no trabalho conjunto com o Firewall**. 2015. Disponível em: <http://webartigos.com/artigos/seguranca-de-redes-com-ips-sua-relacao-com-ids-e-sua-importancia-no-trabalho-conjunto-com-o-firewall/128465>. Acesso em: 13 mai. 2017.

FONTES, EDSION. **Gestão de Riscos de SI – Norma 27005:2008**. Disponível em: < http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/889>. Acesso em: 11 fev. 2018.

GESTÃO DE SEGURANA PRIVADA, **CONTROLE DE ACESSO FÍSICO, COMO MEDIDA DE SEGURANÇA FÍSICA INSTALAÕES**. Disponível em: < https://www.gestaodesegurancaprivada.com.br/controle-de-acesso-fisico/>. Acesso em: 25 mar. 2017.

GIL, ANTONIO CARLOS. **Como Elaborar Projetos de Pesquisa**. 4. ed. Atlas. São Paulo. 2010.

HLBR. **Documentação HLBR**. Disponível em: <http://hlbr.sourceforge.net/>. Acesso em: 23 jul. 2017

LAKATOS, EVA MARIA; MARCONI, MARIANA DE ANDRADE. **Fundamentos de Metodologia Científica**. 7. ed. Atlas. São Paulo. 2010.

NAKAMURA, EMILIO TISSATO. **Segurança de redes em ambientes cooperativos**. Novatec. São Paulo. 2007.

OLHAR DIGITAL, **Crimes virtuais geram prejuízo bilionário ao Brasil**. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/mais-de-42-milhoes-de-brasileiros-foram-vitimas-de-crimes-virtuais-em-2016/64008>. Acesso em: 15 de jul. 2017.

OSSEC. **Documentação OSSEC**. Disponível em: < https://ossec.github.io/docs/>. Acesso em: 11 jun. 2017.

PAIVA, SEVERINO. **SEGURANÇA DA INFORMAÇÃO E AUDITORIA DE SISTEMAS**. Imprell. João Pessoa. 2017.

PESQUISA DESCRITIVA. **O QUE É ARPANET**. Disponível em < https://www.significados.com.br/pesquisa-descritiva/>. Acesso em: 02 de abri. 2018.

SAMHAIN. **Ficha técnica**. Disponível em: <http://www.la-samhna.de/samhain/s_documentation.html>. Acesso em: 18 jul. 2017.

SÊMOLA, MARCOS. **Gestão da Segurança da Informação: Visão Executiva**. Elsevier. Rio de Janeiro. 2003.

SEVERINO, ANTÔNIO JOAQUIM. **Metodologia do Trabalho Cientifico**. Cortez. 23. ed. São Paulo. 2007.

SILVA, CLÁUDIO NEI NASCIMENTO DA. **Metodologia cientifica descomplicada: prática científica para iniciantes**. Editora IFB. Brasília. 2016.

SNORT. **Documentos *Snort***. Disponível em: <https://www.snort.org/documents>. Acesso em: 14 out.2017.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes: Princípios e Práticas. Pearson**. 4. ed. São Paulo. 2008.

STALLINGS, WILLIAM. **Redes e Sistemas de Comunicação de Dados: Teoria e Aplicações Corporativas**. Rio de Janeiro. 2005.

STEEMKR. **SISTEMA DE IMPLEMENTAÇÃO DE SISTEMA DE DETECÇÃO DE INTRUSOS (IDS) EM UBUNTU 14.04 # PARTE 1**. Disponível em: <https://steemkr.com/utopian-io/@woking/implementation-sistem-intruder-detection-system-ids-in-ubuntu-14-04-part-1>. Acesso em: 26 mar. 2018.

SURICATA. **Todos os recursos**. Disponível em: <https://suricata-ids.org/features/all-features/>. Acesso em: 03 jul. 2017.

TANENBAUM, ANDREW S.; David Wethereall. **Redes de computadores**. Pearson Prenttice Hall. São Paulo. 2011.

TECHTUDO. **Entenda o que é RAID, técnica que torna o sistema mais rápido e seguro**. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2012/10/entenda-o-que-e-raid-tecnica-que-torna-o-sistema-mais-rapido-e-seguro.html>. Acesso em: 24 mar. 2018.

TECMUNDO. **Futuro da internet é visto com "otimismo e desilusão"**. Disponível em <https://www.tecmundo.com.br/internet/122148-futuro-internet-visto-otimismo-desilusao-diz-organizacao.htm>. Acesso em: 20 de set. 2017.

TORRES, GABRIEL. **Redes de Computadores: Versão Revisada e Atualizada**. Novaterra. 2. ed. Rio de Janeiro. 2014.