**CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA**
**FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"**
**BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**LUIS HENRIQUE SOUSA COSTA**

# PROTEGENDO PLATAFORMA DE COMÉRCIO ELETRÔNICO CONTRA ATAQUES DOS UTILIZANDO HONEYPOT

**MARÍLIA**
**2013**

**CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA**
**FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"**
**BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

# PROTEGENDO PLATAFORMA DE COMÉRCIO ELETRÔNICO CONTRA ATAQUES DOS UTILIZANDO HONEYPOT

Trabalho de Curso apresentado ao Curso de Graduação em Sistemas de Informação da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador:
profª. Ms. Giulianna Marega Marques

**MARÍLIA**
**2013**

HENRIQUE SOUSA COSTA, Luis

Protegendo Plataforma De Comércio Eletrônico Contra Ataques Dos Utilizando Honeypot / Luis; orientador: Profª. MS. Giulianna Marega Marques. Marília, SP: [s.n.], 2013.
73 f.

Trabalho de Conclusão de Curso (TCC) - Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha.

1. Segurança da Informação 2. Honeypot 3. E-Commerce

CDD: 658.472

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
*BACHARELADO EM SISTEMAS DE INFORMAÇÂO*

**TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL**

Luís Henrique Sousa Costa

Protegendo plataforma de comércio eletrônico contra ataques dos utilizando honeypot.

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Sistemas de Informação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Sistemas de Informação.

Nota: 9,5 ( nove e meio )

Orientador: Giulianna Marega Marques

1°. Examinador: Fábio Dacêncio Pereira

2°. Examinador: Jussara Mallia Zachi

Marília, 06 de dezembro de 2013.

# AGRADECIMENTOS

É difícil agradecer todos que estão apoiando esse trabalho e todos àqueles que estão apoiando essa fase, primeiramente, agradeço a todos de coração.

Dedico esse trabalho primeiramente aos meus pais, Pedro Marcelo Costa e Irma Aparecida de Sousa Costa e meu irmão André de Sousa Costa, pois foi com eles que aprendi tudo em minha vida, dando base para realização do curso e desse novo projeto, por mais difícil que fossem as circunstâncias, sempre estiveram do meu lado.

Agradeço a minha namorada, Shaiener de Souza Santos, pelos momentos que esteve ao meu lado e entendendo minha ausência para que esse trabalho fosse possível.

Agradeço a minha orientadora, Giulianna Marega Marques por toda paciência e dar todo apoio possível.

Agradeço aos professores que desempenharam com dedicação as aulas ministradas.

Agradeço a empresa Tray, por oferecer sua infraestrutura para implantação desse projeto.

Agradeço ao time de infraestrutura da empresa Tray, por todo apoio e compartilhamento de seus conhecimentos para auxilio implantação desse projeto.

Henrique Sousa Costa, Luis. Protegendo Plataforma De Comércio Eletrônico Contra Ataques Dos Utilizando Honeypot (Bacharelado em Sistemas de Informação) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2013.

# RESUMO

Devido ao crescente aumento do uso de computadores e em especial da internet, novas aplicações têm sido criadas com a finalidade de atingir algumas necessecidades dos novos usuários. Os aplicativos de e-business e e-commerce estão entre elas, e têm se tornado muito populares nos últimos anos. Estrategicamente utilizadas para obtenção de vantagens competitivas no mercado, as aplicações de comércio eletrônico necessitam de garantia em sua segurança. A evolução dos interesses por parte dos atacantes acarretaram o desenvolvimento de ferramentas para combate-los e estuda-los. Uma dessas ferramentas é o Honeypot, cujo objetivo é ser sondado, atacado ou comprometido simulando um ambiente real de produção, porém possui mecanismos de contenção, de alerta e de coleta de informações dos atacantes e auxilia a aliviação da carga dos ataques direcionados ao ambiente de produção real, assim não o comprometendo. Neste trabalho será apresentada a solução para proteção de uma plataforma de comércio eletrônico com várias lojas virtuais contra ataques DOS.

Palavras-Chave: honeypot, segurança da informação, e-commerce, e-businnes

Henrique Sousa Costa, Luis. Protegendo Plataforma De Comércio Eletrônico Contra Ataques Dos Utilizando Honeypot (Bacharelado em Sistemas de Informação) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2013.

# ABSTRACT

Due to the growth of the computer use and specially the internet, new applications have been made to fulfill some new users' needs. The e-business and e-commerce apps are among them and have became very popular in recent years. As they are strategically used to obtain competitive business advances, they need security guarantees. The evolution in the interests of the attackers has resulted in the development of tools to combat and study them. One of these tools is the Honeypot, which objective is to be probed, attacked or compromised, simulating a real production environment, but having contention mechanisms to alert and collect attackers' information to help evaluate the attack. In this work a solution will be presented to protect an e-commerce platform with many virtual stores against DOS attacks.

Palavras-Chave: honeypot, Information security, e-commerce, e-businnes

# SUMÁRIO

# LISTA DE ILUSTRAÇÕES

# LISTA DE GRÁFICOS

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| DARPA | *Defense Advanced Research Projects Agency* |
| MIT | *Massachusetts Institute of Technology* |
| UCLA | *University of California, Los Angeles* |
| ARPANET | *The Advanced Research Projects Agency Network* |
| CERN | *European Organization for Nuclear Research* |
| HTTP | *HyperText Transfer Protocol* |
| HTTPS | *HyperText Transfer Protocol Secure* |
| WWW | *World Wide Web* |
| HTML | *HyperText Markup Language* |
| IBOPE | *Instituto Brasileiro de Opinião Pública e Estatística* |
| B2C | *Business to Consumer* |
| B2B | *Business to Business* |
| C2C | *Consumer to Consumer* |
| G2C | *Government to Citizen* |
| G2B | *Government to Business* |
| Intranet | Rede Privada |
| Extranet | Rede Pública |
| SaaS | *Software as a service* |
| ERP | *Enterprise Resource Planning* |
| PHP | *Hypertext Preprocessor* |
| DOS | *Denial of Service* |
| DDOS | *Distributed Denial of Service* |
| DRDOS | *Distributed Reflection Denial of Service* |
| TCP | *Transmission Control Protocol* |
| IP | *Internet Protocol* |
| ICMP | *Internet Control Message Protocol* |
| UDP | *User Datagram Protocol* |
| SQL | *Structured Query Language* |
| NAT | *Network Adress Translation* |
| PAT | *Port Adress Translation* |
| VPN | *Virtual Private Network* |
| DMZ | *Demilitarized Zone* |
| IDS | *Intrusion detection system* |
| FTP | *File Transfer Protocol* |

# INTRODUÇÃO

Seguindo a evolução da tecnologia no mundo, o uso da Internet se popularizou em todo o planeta, tornando-se algo indispensável para negócios e tarefas do dia a dia. Segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br) no Brasil 38% dos domicílios possuem computador com internet em casa, um crescimento de 20% se comparado ao o ano de 2008 (CETIC, 2013). O crescimento da Internet trouxe novas aplicações e empresas para atender às necessidades de um novo tipo de mercado.

Em um ambiente em constante crescimento, cada vez mais informações valiosas como cartões de créditos, dados bancários e documentos são trafegados e por muitas vezes de forma não segura. No desenvolvimento e na hospedagem de uma aplicação são necessários cuidados com a segurança de suas informações, para que elas não fiquem a disposição de um usuário mal intencionado.

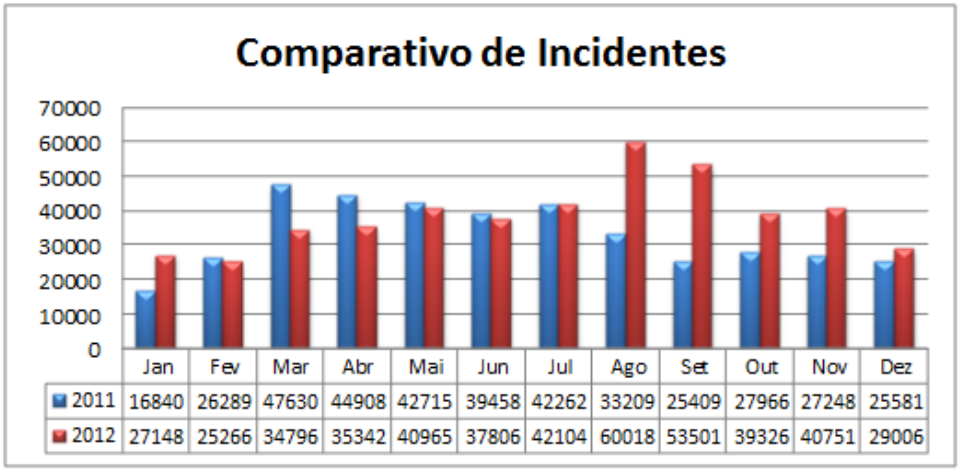
O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), do Comitê Gestor da Internet no Brasil (CGI.br), é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. O CERT.br atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio ao processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

No ano de 2012 foram notificados ao CERT.br 466.029 incidentes de segurança em computadores conectados à Internet brasileira, um número quase 16% maior que a estatística de 2011. Em detalhes, em 2012 houve um crescimento de 65% nas notificações de ataques aos servidores *web* e 94% em varreduras e propagação de códigos maliciosos.

Nos ataques são exploradas vulnerabilidades em aplicações *web* para, então, hospedar nesses sites páginas falsas de instituições financeiras, cavalos de troia, ferramentas utilizadas em ataques a outros servidores *web*, *scripts* para envio de spam ou scam e ataques de força bruta, colocando em risco todo o conteúdo das organizações que mantém hoje valiosos aplicativos de *e-business* e *e-commerce*, trazendo perdas em relação à satisfação de seus clientes, funcionamento de seus serviços e lucros (CERT, 2013).

No Gráfico 1 é possível observar o comparativo de incidentes reportados ao CERT.br no ano de 2011 e 2012.

Gráfico 1 - Comparativo de Incidentes




Fonte: CERT.br - Janeiro a Dezembro de 2011 e 2012

Segundo a Revista E-Commerce Brasil (2011), o Brasil possui mais de dez milhões de e-consumidores, e o mercado de comércio eletrônico não para de expandir, novas lojas virtuais são criadas, novos conceitos e modalidades de negócios são desenvolvidos. Com o aumento significativo de consumidores online, os *e-commerces* que não empregarem práticas de segurança, estão fadados a estagnar seu crescimento. A segurança é um dos fatores primordiais para conquistar a confiança e fidelizar o cliente.

No ponto de vista de um provedor de serviço de e-commerce, cliente é o lojista, aquele que contratou a loja virtual, mas se o provedor não garantir estabilidade e confiabilidade da loja virtual (sistema *e-commerce*), o consumidor final é afetado e como consequência, o lojista e o consumidor se tornam insatisfeitos.

## Objetivos

A idealização do objetivo é feita por meio de um conjunto de medidas chamada de tríade CIA (Confidencialidade, Integridade e Disponibilidade), presente na ABNT NBR ISO/IEC 17799, que devem ser respeitadas para proteger e preservar a informação. Os conceitos base da tríade pode ser explicado:

- Confidencialidade: propriedade que garante o resguardo da informação, onde somente quem tiver autorizado pelo proprietário poderá acessá-la.
- Integridade: propriedade que a informação não foi alterada e mantém todas suas característica originais, estabelecidas pelo proprietário.

- Disponibilidade: propriedade que garante que a informação sempre estará disponível para uso legítimo, onde não poderá ser negada para os usuários que tiverem permissão do proprietário à acessá-la.

O objetivo geral do presente trabalho é prover o aumento da segurança da informação e a disponibilidade da rede e dos servidores de sistemas e-commerce, de modo que possibilite ao provedor destes sistemas a obter ainda mais confiabilidade e fidelidade dos seus lojistas e respectivamente de seus consumidores.

Como objetivo especifico deverá ser implantado um Honeypot para prover disponibilidade em uma plataforma de comércio eletrônico, contra ataques do tipo DOS que comprometem a disponibilidade do serviço.

# CAPÍTULO 1 - A INTERNET E O COMÉRCIO ELETRÔNICO

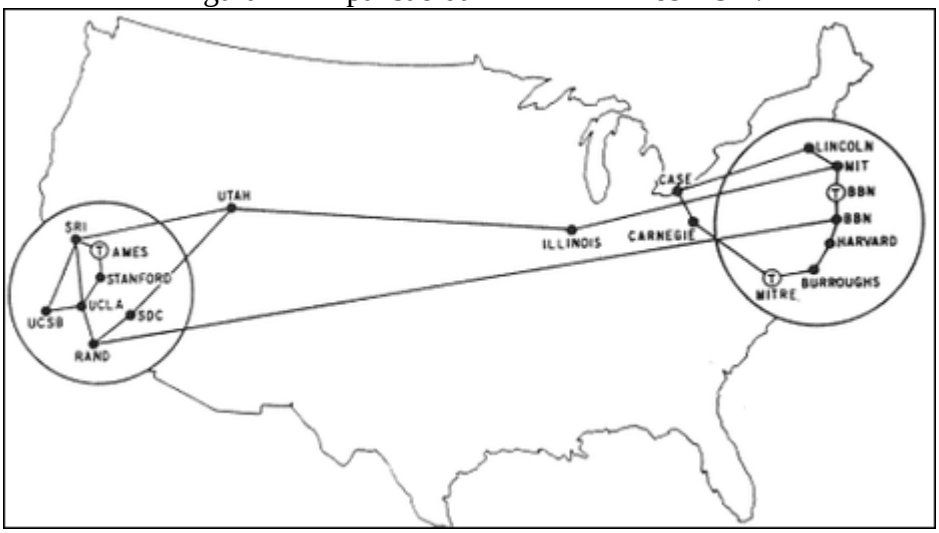
Com a criação e globalização da Internet diversos sistemas e novos conceitos surgiram com o passar dos anos, dentre eles, o de comércio eletrônico e todo seu ecossistema, que vem impulsionando a economia em todo o planeta. Para atender ao crescimento de todo o mercado eletrônico, novas empresas e grupos surgiram para suprir as necessidades de cada cliente, o qual tem se tornado cada vez mais exigente.

## 1.1 Aspectos Gerais

Criada durante os tempos da Guerra Fria, na década de 1960, a Internet surgiu com o propósito de descentralização de informações onde havia o temor da perda em possíveis ataques. Em 1962 no Instituto Tecnológico de Massachusetts (MIT) nos EUA, Joseph Carl Robnett Licklider introduziu o conceito de "Rede Galatica", para o qual imaginou um conjunto de computadores interligados globalmente que pudessem acessar dados e programas remotamente (LEINER, 2003).

Com o conceito muito parecido com a internet de hoje, por meio da DARPA (Defense Advanced Research Projects Agency) após diversas discussões e refinamento da ideia, em 1969 foi desenvolvida a ARPANET que teve seu primeiro nó instalado junto a UCLA (Network Measurement Center). Após esse momento meses e anos depois mais nós foram adicionados a ARPANET, para que pesquisas para o desenvolvimento do modelo da Internet fossem concretizadas.

Figura 1 - Expansão da ARPANET nos EUA.




Fonte: WARD, 2009

Com a expansão da ARPANET para outras cidades, e para outros continentes, em 1989 um cientista do CERN (Organização Europeia para a Investigação Nuclear) chamado Tim Berners-Lee criou o sistema *Word Wide Web* (WWW) para interligar as universidades de maneira, que trabalhos e pesquisas fossem compartilhadas mutuamente entre si.

Junto ao o sistema WWW, Tim Berners-Lee foi responsável também pela criação do código HTML e o protocolo HTTP. Com essas criações Berners-Lee permitiu que evoluções e melhorias fossem realizadas em suas criações, sendo possível ter o modelo de Internet que é encontrado hoje. Uma dessas evoluções é a do protocolo HTTP, que passou a receber um certificado junto a ele, tornando a conexão segura e chamado de HTTPS.

Com toda a evolução para modelar a Internet de hoje, não só protocolos e códigos foram criados, mas toda uma gama de sistemas para Internet foram desenvolvidos atendendo diversas àreas. Contribuindo para os 2,4 bilhões de internautas em todo o mundo (PINGDOM, 2013) que estão distribuidos por todos os tipos de sistemas, desde as redes sociais até grandes sistemas de gerenciamento empresarial.

Dentre um dos sistemas desenvolvidos ao decorrer dos anos, ganha destaque os de comércio eletrônico, que é o termo geralmente utilizado para comercialização de bens por meio de meios eletrônicos. O modelo de comércio eletrônico que é visto hoje, começou a ser construído na década de 80, quando empresas começaram a utilizar sistemas para emirtir ordem de compras.

Em 1994 a rede de restaurantes Pizza Hut começou a aceitar pedidos online, o que foi uma grande evolução pois somente 5% da população americana tinha acesso à Internet. No ano seguinte, em 1995, foi anuncionado o primeiro produto a ser vendido online pelo site eBay, tudo para testar uma idéia de uma espécie de mercado virtual.

Novas empresas de comércio eletrônico foram surgindo com o decorrer dos anos, dentre elas uma das maiores no mercado no dia de hoje, a Amazon.com. Nascida também em 1995, assim como a eBay, somente obteve grandes lucros oito anos depois, fechando o ano de 2003 com 5 milhões em caixa (UOL HOST, 2013).

Junto às evoluções do comércio eletrônico, como sistemas de leilões e compras coletivas, um grande ecossistema surgiu à sua volta. Um deles proporcionou comodidade para os clientes do comércio eletrônico, junto à popularização do cartão de crédito também nasceu em 1995, as ferramentas de pagamento online.

As ferramentas de pagamento online fazem todo o intermédio entre instituições financeiras, comércio eletrônico e cliente. Sem esta ferramenta não seria possível realizar qualquer transação financeira automatizada com o universo do comércio eletrônico, levando

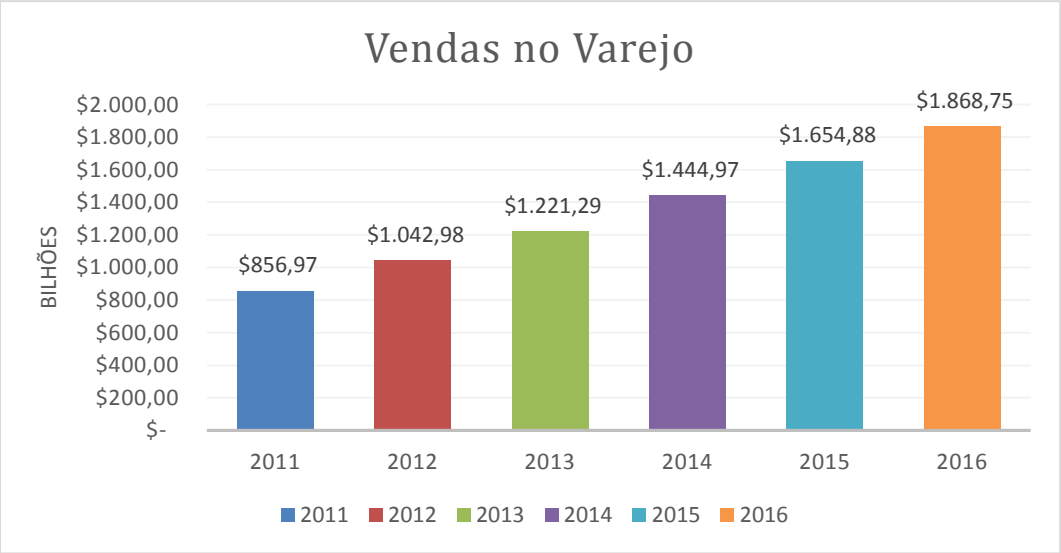
desconforto para o cliente que necessita cada vez mais, de rapidez no processo de finalização da compra. A agilidade nos processos se torna uma grande vantagem para as empresas de comércio eletrônico.

O comércio eletrônico com todas as evoluções em seu ecossistema, se tornou no mundo todo, responsável por movimentar a economia do mercado online, principalmente o varejista. Os clientes que iam em lojas físicas à procura de produtos com bons preços, passaram a procurar melhores condições e a comprarem online, com toda comodidade que o comércio eltrônico traz.

Hoje o comércio eletrônico se tornou um imenso meio de se vender produtos, mesmo com pouco investimento, é obtido um grande retorno. No ano de 2012 o mercado varejista de comércio eletrônico movimentou cerca de $1 trilhão de dólares e ainda há previsão que esse valor cresça quase 20% no ano de 2013, podende chegar a $1.221 trilhões de dólares e quase dobrar em 2016 (EMARKETER, 2013).

.

Gráfico 2 - Crescimento das vendas no varejo




Fonte: EMARKETER, 2013.

O que pode-se visualizar, é que o ainda há muito espaço para o crescimento do comércio eletrônico, que continua aquecido, tudo isso devido a mudança do hábito das pessoas ao fácil acesso à banda larga, que é impulsionada pelo aumento no acesso móvel (B2W, 2013). Todo o ecossistema do comércio eletrônico também se encontra em constante evolução e novidades ainda deverão surgir, principalmente voltada aos dispositivos de acesso móvel, que estão cada vez mais em uso no dia a dia das pessoas.

O comércio eletrônico que passou a ser globalizado ao decorrer do anos, também foi introduzido nos países emergentes, como o Brasil. Resultando no mesmo sucesso mundial, têm atraído empresas de outros países que são referências no ramo, para se consolidar no mercado local.

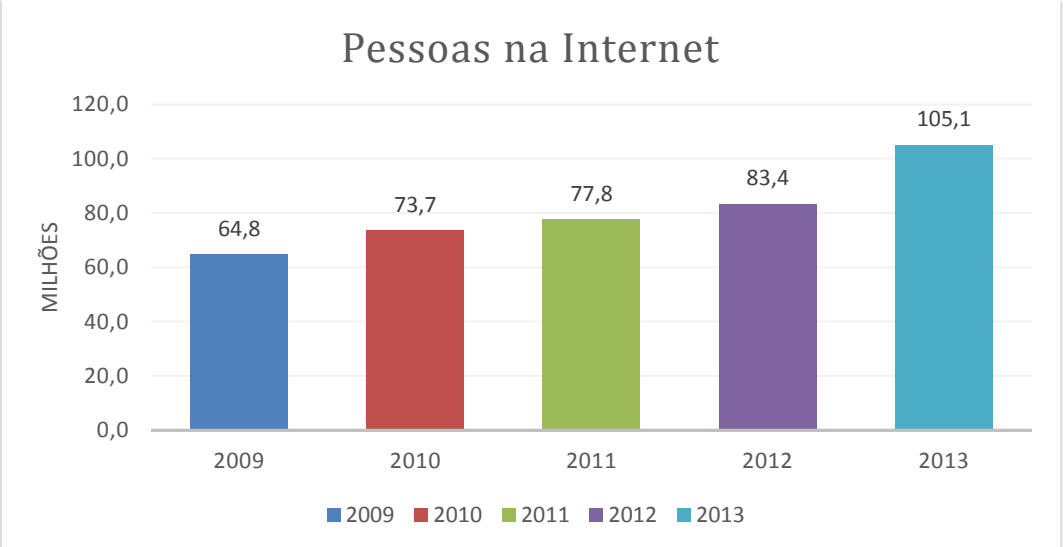
## 1.2 Estado da Arte no Brasil

Assim como no mundo, a expansão do comércio eletrônico no Brasil não deixou de ser diferente. Com a popularização da Internet na década de 90 em todo o Brasil, o comércio eletrônico começou a se firmar no mercado e não parou mais de crescer. Hoje o comércio eletrônico se tornou uma ferramenta de grande sucesso para o público brasileiro, e movimenta bilhões de reais.

Nas últimas décadas a econômia brasileira passou por mudanças estruturais que geraram estabilidade e crescimento econômico, permitindo assim, grande disponibilidade de crédito e a facilidade no acesso à Internet, fazendo com que se tornasse um país emergente ao se falar de comércio eletrônico no mundo (B2W, 2013).

Por conta de incentivos favorecidos pelo governo e devido ao momento de economia estável pelo qual passa o país, segundo pesquisa realizada pelo IBOPE, o Brasil hoje conta com 105 milhões de pessoas conectadas à Internet, uma ascensão de quase 14% se comparado ao ano de 2012, que contava com 83,4 milhões de internautas.

Gráfico 3 - Pessoas que possuem acesso a internet.




Fonte: IBOPE, 2013.

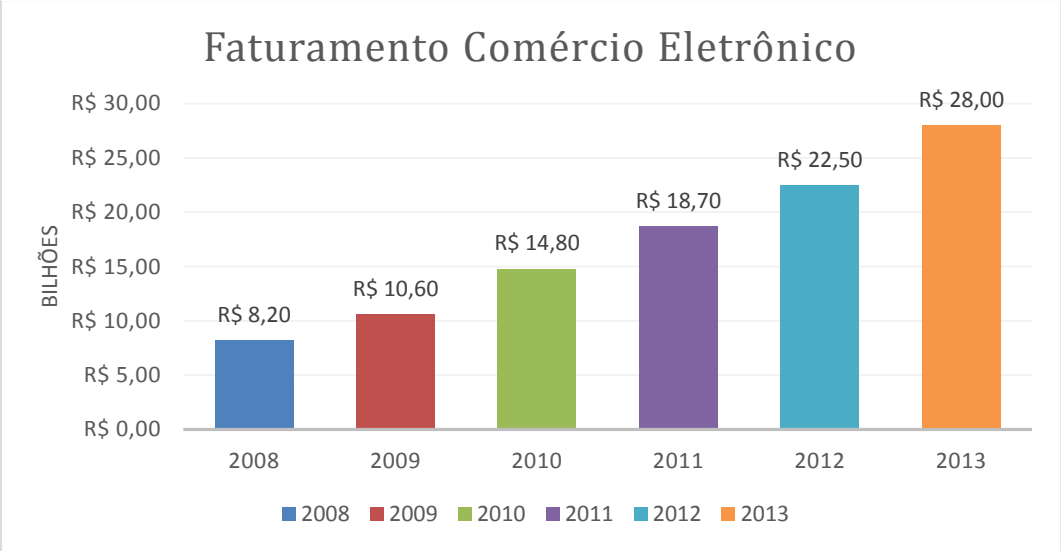
O aumento na utilização da internet impactou diretamente no percentual de acesso ao comércio eletrônico no país, o qual atrai hoje 61% dos internautas brasileiros (E-COMMERCE NEWS, 2013). Com o mercado aquecido, novas lojas virtuais são criadas a cada dia. Segundo o E-Commerce Brasil (2012) há cerca 23 mil lojas e esse número será mais que dobrado no ano de 2014, chegando a 45 mil lojas.

Apesar da grande quantidade de lojas na Internet, segundo o E-Commerce Brasil (2012) somente 30% dessas lojas investem em divulgação e realizam mais de dez vendas ao mês e, mesmo com o aumento em 2014, a proporção se mantêm em 30%. O motivo da estagnação está na facilidade de entrar no mercado com pouco investimento, na falta de conhecimento e planejamento

Como consequência do crescimento de todo o comércio eletrônico voltado para o mercado varejista, o faturamento fechou no ano de 2012 com R$ 22,5 bilhões, segundo pesquisa do e-Bit (2012). Há a expectativa de que em 2013 cresça em média 25% a mais, chegando ao faturamento de R$ 28 bilhões, um aumento de 97% se comparado com ano de 2008.

Ainda segundo a pesquisa da e-Bit, o comércio eletrônico obteve esse resultado devido ao maior número de datas comemorativas e ao natal que contribuiu sozinho com R$ 3,06 bilhões em 2012. Há ainda apontamento para o *Black Friday*, que se consolidou no mercado brasileiro como uma nova data comemorativa, chegando em um número de R$ 243,8 milhões, aumento impressionante de 143,8% que em 2011, um recorde para apenas 24 horas de vendas.

Gráfico 4 - Faturamento do comércio eletrônico por ano.




Fonte: e-Bit, 2012

Com grande visibilidade mundial no comércio eletrônico, o Brasil corresponde a 3,1%

do mercado mundial, segundo pesquisa realizada pela consultoria italiana Translated (2012), ficando em sétimo lugar no ranking. De acordo com a projeção realizada pela pesquisa, o Brasil deve estabelecer em 2016 a posição de quarto lugar, assumindo 4,3% do mercado mundial

Todos os fatos de crescimento do comércio eletrônico fez com que grandes empresas consolidadas internacionalmente e especializadas no ramo, também aderissem ao mercado brasileiro, fazendo do Brasil um ponto estratégico. Esse é o caso de duas gigantes norte-americanas a Amazon e eBay, que iniciaram suas atividades no Brasil entre os anos de 2012 e 2013 (DRSKA, 2013).

Pode se concluir que o Brasil se encontra em uma constante ascensão quando se fala em comércio eletrônico, e ainda há muito espaço para crescer. Com o crescimento do setor, novidades devem ser desenvolvidas para atender certas áreas que o comércio eletrônico ainda não conseguiu alcançar, dando destaque para as compras feitas por meio de dispositivos móveis, que tem crescido muito no Brasil.

## 1.3 Grandes Redes do Mercado Tradicional e o Comércio Eletrônico

A popularização do comércio eletrônico trouxe novas empresas que surgiram em meio à Internet, lojas físicas do varejo perceberam que poderiam aumentar suas vendas por meio da Internet. Utilizando a Internet, essas lojas puderam alcançar novas regiões onde antes não poderiam alcançar sem que realizassem grandes investimentos.

Auxiliando também nas vendas das lojas físicas, o comércio eletrônico emite maior visibilidade para a empresa, tendo em vista que a Internet permite que as lojas sejam facilmente localizadas, também fisicamente. Mesmo com toda informação disponível no comércio eletrônico, certos perfis de pessoas preferem ter contato com o vendedor e o produto antes de comprá-lo, assim é dado o aumentando também às vendas em lojas físicas.

A globalização da Internet e a ascensão social do brasileiro, fizeram com que consumidores das classes menos privilegiadas, como a C e D, também utilizassem a Internet. Acompanhando essa ascensão, grandes empresas do mercado varejistas popular também acompanharam esses consumidores, como a Casas Bahia que hoje tem sua loja virtual consolidada no mercado de comércio eletrônico.

Várias empresas hoje trabalham mantendo os dois tipos de mercado e tem maior parte de seu faturamento derivado do comércio eletrônico. Segundo Pedro Guasti (2008), grandes redes como Extra, Pão de Açúcar ou Magazine Luiza; suas lojas virtuais tem representação

assídua no faturamento, podendo chegar a representação de 10 lojas físicas, sem que tenha o investimento físico.

Apesar do comércio eletrônico complementar o faturamento das lojas físicas, segundo Fernando Di Giorgi (2013) não deve ser tratado como “mais uma loja da rede”, pois a operação de uma loja virtual se difere de uma loja física. Com característica operacionais diferenciadas onde funções como compra, venda, logística interna, transporte e reversa, devem ser autônomas em relação as lojas físicas, pois o mercado do comércio eletrônico requer ritmos diferentes.

Devido ao fato de não diferenciar a operação entre lojas da rede física e a loja virtual, o Carrefour, uma das maiores redes de varejo do mundo, encerrou suas atividades no comércio eletrônico brasileiro em 2012 (LIMA, 2012). Entre outros fatores está em não integrar seus dois tipos de lojas para realizar vendas multi-canais.

Em contramão aos fatores que retiraram o Carrefour do mercado do comércio eletrônico brasileiro, a rede de lojas Americanas detém boa parte do mercado com o entrosamento entre sua loja virtual e rede de lojas físicas, ocupando o quarto lugar entre os maiores varejistas do Brasil (IBEVAR, 2012). Uma de suas estratégias está na integração entre a loja virtual e suas lojas físicas, onde totens são disponibilizados para possibilitar a compra online.

As Lojas Americanas fazem parte de um grupo que detém o controle de 25% do mercado do comércio eletrônico no Brasil e está apoiado por mais de cinco lojas virtuais. Nascido da fusão de duas grandes lojas virtuais, o grupo B2W é especializado em comércio eletrônico que detém as maiores lojas virtuais do Brasil, que no segundo trimestre de 2013 teve um faturamento de R$ 2,9 bilhões (E-COMMERCE NEWS, 2013).

A B2W faz constates investimentos em todo seu ecossistema de comércio eletrônico e além de lojas virtuais, recentemente em um plano estratégico, será investido R$ 1 bilhão em 3 anos em logística, tecnologia e inovação (B2W, 2013). Fruto desse plano foram a aquisição de uma transportadora que possui serviço especializado para comércio eletrônico e uma empresa especializada em desenvolvimento de sistemas voltada para o varejo online (E-COMMERCE NEWS, 2013).

Sem que haja investimentos em todo o ecossistema do comércio eletrônico desde o marketing até a entrega final do produto, não há possibilidade de que uma loja virtual sobreviva por mais de um ano no mercado, entrando para os 70% de lojas que não realizam mais de dez vendas por mês. No âmbito das lojas que ainda mantêm seu mercado tradicional, seguindo como exemplo o Carrefour, deve-se tratar um operacional diferenciado para cada modelo, visando a integração das vendas entre loja física e loja virtual.

## 1.4 Modelos de Comércio Eletrônico

O comércio eletrônico atinge as demais áreas de negócios, possibilitando que desde o governo até o consumidor final, realizem troca de informações ou transações financeiras. O que fica em evidência é que a necessidade de informatização de todo de âmbito do negócio, vem atingindo não somente empresas privadas, mas também e principalmente o governo.

### 1.4.1 Business to Consumer (B2C)

O B2C é o comércio efetuado diretamente entre empresas e o consumidor final. Realizado geralmente com venda de produtos e serviços, o B2C é o mais comum hoje no meio do comércio eletrônico, devido a facilidade de se montar uma loja virtual e começar a vender minutos após. Esse fator acaba sendo uma armadilha para as empresas, pois o risco de não consolidação do negócio é alto.

O mercado B2C está em constante evolução e toda sua cadeia abrange desde o pequena até a grandes empresas. Isso favorece diretamente o consumidor que tem várias formas de comprar um mesmo produto, fazendo com que as empresas inovem e foquem em melhoria do serviço oferecido ao cliente, que está cada vez mais exigente com esse tipo de mercado.

Com o cliente mais exigentes, alguns desafios são impostos às empresas que estão contidas no modelo B2C, principalmente no serviço de logística e na fidelização do clientes, fatores decisivos na hora da compra. Os clientes exigem qualidade em todos os serviços da empresa, desde a tecnologia até a entrega do produto. Sem o foco necessário, a insatisfação do cliente é eminente e torna fácil e rápida a mudança quanto ao local de compra.

O B2C pode ser divido basicamente em três tipos:

- **Leilões Online:** Assim como o leilão tradicional, no Leilão Online, produtos são disponibilizados em uma página *web* para que o consumidor final ofereça lances, sendo assim, quem oferecer o maior lance comprará o produto.
- **Lojas Virtuais:** Uma página da Internet onde empresas anunciam e vendem produtos, que são disponibilizados em forma de catálogo, destinado ao consumidor final.
- **Serviços Online:** Onde as empresas oferecem serviços por meio da Internet para que seja contratado pelo consumidor final, tais como serviços de e-mail, hospedagem, lojas virtuais, etc.

O modelo B2C está em constante crescimento e é o mais comum dentre os demais modelos. Porém para que mais empresas se consolidem é necessário que estratégias com foco no cliente sejam traçadas. As empresas do grupo B2W teve seu faturamento de R$ 2,9 bilhões no segundo trimestre de 2013, e é um caso de sucesso do modelo B2C, onde a previsão de ascensão é de quase 25% no ano de 2013 para todo modelo, segundo pesquisa do e-Bit (2012).

### 1.4.2 Business to Business (B2B)

O B2B é o comércio efetuado diretamente entre empresas, onde empresas vendem para outras empresas. No modelo de B2B há a substituição dos processos físicos, onde empresas negociam entre si operações de compra e venda de produtos, informações e serviços que podem ser obtidas por meio da *web* e outros meios de comunicação.

Assim como todo comércio eletrônico, o B2B, substitui o meio tradicional de se negociar com fornecedores de maneira rápida, sem que haja custos adicionais com deslocamento e alocação de pessoas para realizar uma compra. Para que tudo seja possível, é importante que todo seu ecossistema possua segurança dos dados ali trafegados.

Segundo Carvalho (2006), pode-se identificar três grupos principais de portais para o B2B:

- **Portais para colaboradores (*intranet*):** Utiliza o meio de comunicação interno da empresa, onde o acesso é restrito aos colaboradores ou um grupo da empresas que tem acesso permitido na rede interna. Esse tipo de portal une a comunicação entre os colaboradores, mesmo que não estejam fisicamente próximo.
- **Portais para parceiros (*extranet*):** Relaciona diretamente uma empresa com uma outra empresa ou grupo de empresas com quem se necessita de fazer negócios. Unindo assim seus parceiros esse tipo de portal ajuda a promover a colaboração e compartilhamento de informações.
- **Portais de terceiros ou *e-markeplaces:*** Facilita por meio de intermediadores online a negociação de produtos e serviços entre organizações compradoras e vendedoras. Esse tipo de portal utiliza a Internet, o que facilita a negociação onde se tem muitos compradores ou vendedores.

O B2B vem crescendo muito nos últimos anos e se tornando popular entre as empresas,

segundo a E-Consulting Corp. (2013), transações B2B representaram R$ 947,9 bi no comércio eletrônico. Com o auxílio do comércio eletrônico e a adesão as empresas, esse número tende a crescer, fazendo com que empresas realizem seus negócios de maneira rápida, cômoda e sem custos adicionais para fechamento de negócios.

### 1.4.3 Consumer to Consumer (C2C)

Voltado para a interação entre pessoas físicas por meio do comércio eletrônico, o C2C permite que todo negociação possa ser realizada somente entre consumidores finais. Geralmente as transações realizados pelos consumidores são intermediada com o auxílio de uma empresa, como Mercado Live, OLX e Bom Negócio, que são especializadas nesse modelo de comércio.

Com uma empresa realizando o intermédio de cada transação, não é preciso que os consumidores tenham preocupações com divulgação, infraestrutura e tecnologia para realizar suas vendas, assim o retorno das empresas que intermediam vem por meio de comissões sobre as vendas. Com a vantagem de contato direto com o vendedor, possibilita que a negociação seja melhor consolidada até seu fechamento.

Uma grande barreira para o modelo C2C é a confiabilidade em quem está vendendo os produtos, pois não há garantias sobre a qualidade do produto ou sobre o próprio vendedor, sendo um mercado baseado na confiança. Para enfrentar essa barreira, os intermediadores C2C contam com sistemas onde os próprios consumidores avaliam, com comentários e notas, os produtos e os vendedoras para toda a comunidade.

O modelo C2C vem movimentando muito o mercado informal entre os consumidores e as empresas intermediadoras estão em constante crescimento. O Mercado Livre, especializado no ramo, obteve o crescimento de 30,9% no quarto trimestre de 2012 (EUGENIO, 2013). Grande fator para esse crescimento, foram os preços praticados pelos consumidores, que estão abaixo do mercado.

### 1.4.4 Government to Citizen (G2C)

O modelo G2C é o relacionamento comercial entre o governo ou algum órgão público e o consumidor, que pode ser realizado por meio de pagamentos por meio da internet de

impostos, infrações de trânsitos, tarifas públicas, dentre outros. Para que isso seja possível, pode ser considerado como meio de acesso ao G2C sites oficiais que disponibilizam estes serviços.

### 1.4.5 Government to Business (G2B)

É o relacionamento comercial entre o governo ou outro órgão público com uma empresa do setor privado, por meio de troca de informações e transações eletrônicas. O modelo G2B pode ser utilizado para divulgação de editais de compras, cotação eletrônica de preços e a geração de nota fiscal eletrônica, buscando reduzir barreiras para a formalização dos negócios.

Tecnologias são criadas para atenderem aos diversos modelos de comércio eletrônico, aquecendo a forma que o comércio é realizado desde entre consumidores até os governos.

## 1.5 Plataformas de Comércio Eletrônico

A disseminação do comércio eletrônico em todo o mundo fez com que novas tecnologias surgissem ao longo dos anos. Sistemas voltado para o comércio eletrônico se popularizaram com o objetivo de que os lojistas se preocupassem apenas com o gerenciamento. Dentre as tecnologias criadas, uma das mais importante, são as plataformas, que possibilita a criação de uma loja virtual com pouco ou nenhum conhecimento em tecnologia.

No âmbito do comércio eletrônico, plataformas são os sistemas utilizados para gerenciamento e visualização de uma loja na *web* (VALLE, 2013). Uma plataforma possibilita que produtos sejam cadastrado e disponibilizado aos consumidores, assim, permitindo que as vendas realizadas por meio da loja seja gerenciada pelo lojista sem complicações.

As plataformas de comércio eletrônico permitem que com pouco ou nenhum investimento, inicie uma loja virtual. Porém, diversos fatores podem diferenciar o que cada plataforma, como integrações com ferramentas de marketing e algumas opções essenciais para que a loja exerça suas atividades. Sendo assim, uma boa plataforma, contribui diretamente para a consolidação de uma loja virtual no mercado.

Ao decorrer dos anos diversas plataformas surgiram, cada um com seu diferencial, sendo possível a opção de escolha por parte do lojista. A tecnologia empregada pelas plataformas podem variar de plataformas totalmente proprietárias, que são vendidas como serviço, denominado *SaaS*, até as de código totalmente aberto, que podem ser customizadas de

acordo com cada necessidade.

Ambos os tipos de plataformas têm suas vantagens e devem ser selecionadas de acordo com cada necessidade, para evitar os custos adicionais.

As plataformas comercializadas que utilizam o modelo *SaaS*, tem como principal vantagem o baixo valor de investimento para abrir e manter a loja online, já que não há custo com infraestrutura ou desenvolvimento de novas tecnologias. Porém pode ser limitado no quesito de adaptação às necessidade, já que não há controle do lojista sobre a tecnologia da plataforma.

Já as plataformas de código aberto têm como sua principal vantagem a total customização do sistema, porém para que seja possível seu funcionamento poderá haver custos muito maiores que o modelo *SaaS*. Utilizando esse tipo de plataforma, fica inevitável não realizar investimentos em infraestrutura e talentos para customização do sistema.

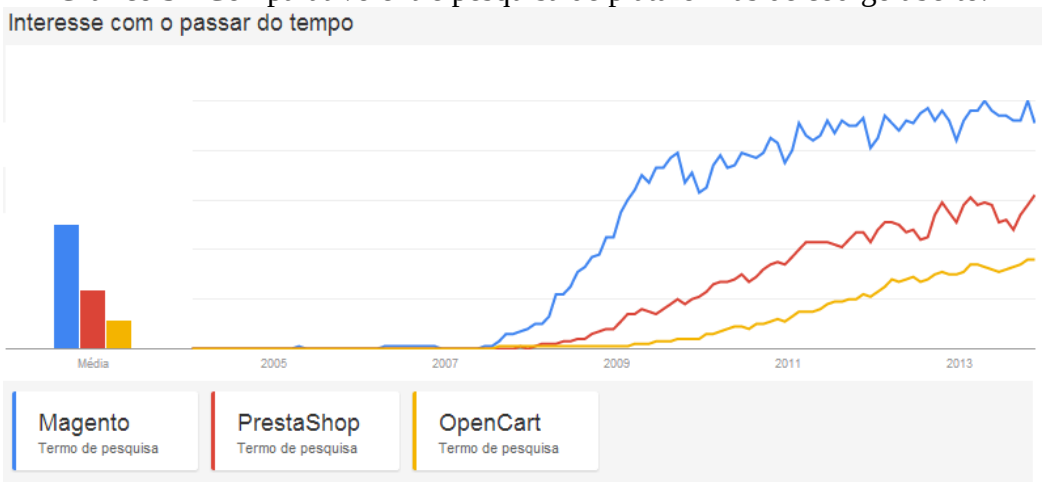
É possível encontrar diversas plataformas contidas nos dois modelos, que abrangem desde o pequeno até o grande lojista. Dentre as soluções, destacam-se o sistema gratuito Magento e a solução *SaaS* TrayCommerce.

### 1.5.1 Magento

A plataforma Magento é uma solução de comércio eletrônico de código totalmente aberto. Isso significa que quem a escolhe, pode modificar desde a visualização de produtos até o seu núcleo de funcionalidades, podendo ser moldada para pequenas e grandes empresas. A vantagem da flexibilidade e escalabilidade da plataforma, fez seu sucesso ao longo dos anos.

Controlada desde 2011 pela eBay Inc., líder no seguimento de comércio eletrônico, Magento lidera o seguimento entre plataformas grátis com mais de 200 mil lojas (MAGENTO, 2013). Em constante crescimento, Magento oferece uma gama de recursos e visa o lucro somente em consultoria e treinamento especializado, além de oferecer certificação para desenvolvedores.

Gráfico 5 - Comparativo entre pesquisa de plataformas de código aberto.




Fonte: GOOGLE, 2013.

A comunidade Magento, oferece mais de 7500 extensões de terceiros para que a plataforma seja customizado com novos recursos, sem que seja necessário conhecimento em desenvolvimento avançado. Esses fatores tornaram Magento a plataforma de código aberto mais utilizada no mundo, o seu sucesso, fez com que alguns fornecedores de plataforma utilizassem a plataforma para serem comercializadas no modelo *SaaS*.

### 1.5.2 Tray Commerce

A plataforma de comércio eletrônico Tray Commerce está a dez anos no mercado brasileiro e mantém 4500 lojas virtuais ativas (TRAY, 2013). Utilizando o modelo de software como serviço (*SaaS*), a plataforma oferece uma grande quantidade de recursos para gerenciamento de uma loja virtual e atende pequenas, médias e grandes operações.

A empresa Tray, responsável pela plataforma oferece todo um ecossistema para o mercado de comércio eletrônico contendo a plataforma, meio de pagamento, shopping virtual. Esse fator em conjunto com os mais variados tipos de integrações que é oferecido pela plataforma, faz a plataforma ser totalmente diferenciada das demais encontradas no mercado brasileiro.

Desde 2012 a empresa Tray é controlada pelo grupo Locaweb, líder no segmento de infraestrutura e hospedagem no Brasil, completando ainda mais seu ecossistema. A parceria reforça seu valor no mercado brasileiro e completa toda a plataforma com investimentos em novas tecnologias, o que permite a expansão de todo o ecossistema.

Visando à facilidade e rapidez na criação de uma loja virtual a Tray Commerce permite que em minutos, uma loja seja configurada e publicada para a Internet. Seus planos de adesão partem de R$ 79,00 (TRAY, 2013), um investimento inicial baixo, para o benefício de se possuir uma loja virtual sem que seja necessário custos adicionais com infraestrutura e desenvolvimento de tecnologia.

A ascensão da Internet e do comércio eletrônico no mercado mundial, facilitou a vida de diversos usuários e empresas. Mas assim como na vida real, pessoas má intencionadas também estão no mundo virtual, levando prejuízos a usuários e empresas. Devido a esse fato, é preciso assegurar que toda a informação trafegada seja protegida contra ataques e fraudes.

# CAPÍTULO 2 - SEGURANÇA DA INFORMAÇÃO

A informação gerada pelo avanço do uso da Internet é extremamente valiosa para todos que nela estão, e sua segurança deve ser um fator primordial para empresas e usuários. Há ferramentas no mercado que auxiliam na proteção da informação, tanto para empresas como para usuários convencionais, e devem ser constantemente atualizadas juntamente a evolução dos ataques.

## 2.1 Aspectos Gerais

A informação é algo essencial para os negócios de uma organização sendo utilizada principalmente na tomada de decisão e definições de estratégias, para assim, auxiliar no seu crescimento. O fluxo de informações importantes circulando no ambiente dos negócios vem crescendo, tendo como principais motivos às interconexões de empresas e órgãos governamentais.

Toda a informação que circula em uma organização está exposta a um crescente número de ameaças e vulnerabilidades, podendo a qualquer momento ser capturada e levando prejuízos inestimáveis. Porém, o valor real de cada informação só é reconhecido quando a mesma destruída, perdida ou roubada. Sendo assim, torna-se essencial a preocupação com a segurança da informação.

Com a chegada da internet e grandes sistemas de informações online a preocupação com a segurança da informação se tornou um desafio, pois estes hoje são alvos preferidos de usuários mal intencionados que realizam diversos tipos de ataques procurando or brechas nas redes de organizações em busca de informações valiosas.

Ao longo dos anos a segurança da informação evoluiu muito com a criação de normas e procedimentos para assegurar que nada será perdido, destruído e roubado. Uma delas é a ABNT NBR ISO/IEC 17799, segundo ela a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A segurança da informação é obtida por meio da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os

objetivos do negócio e de segurança da organização sejam atendidos (ABNT NBR ISO/IEC 17799).

Os benefícios de se proteger uma rede coorporativa e monitorá-la são imensos podendo evitar vazamentos, fraudes, espionagem e diversos outros problemas que possam trazer prejuízos para a organização. A segurança também visa reduzir as despesas, devido a não necessitar de investigações de possíveis incidentes e ter toda sua rede devidamente monitorada.

## 2.2 Atacantes, Alvos e Motivação

Com a informação cada vez mais valiosa tanto no meio da Internet ou mesmo na intranet das empresas, os atacantes cada vez mais vem evoluindo suas técnicas e disseminando métodos de ataques. Os ataques acontecem com alvos variados que são escolhidos de acordo com cada motivação dos atacantes. Os ataques podem levar a sérios prejuízos e até à estagnação de um negócio,

### 2.2.1 Atacantes

Os atacantes são usuários mal ou bem intencionados que utilizam seu alto grau de conhecimento para realizar ataques a uma rede de computadores, visando comprometer a segurança da informação. Esses usuários, em sua maioria, são munidos de grande conhecimento de técnicas de programação, análise de sistemas e especialistas em segurança de redes.

As habilidades dos atacantes mudam à medida que as brechas de segurança são corrigidas, tornando assim os ataques cada vez mais modernos. Uma grande problemática são as ferramentas desenvolvidas pelos atacantes com grandes conhecimentos, automatizando procedimentos de ataques e exploradores de brechas por meio de ferramentas utilizadas por atacantes com nenhum ou pouco conhecimento.

O grupo de atacantes pode ser dividido em dois principais tipos, sendo que alguns realizam os ataques somente para descobrir e reportarem brechas de segurança em redes ou softwares, outros para comprometer a rede computacional, causando estragos inestimáveis.

**Tipos de Atacantes:**

- *Script Kiddies*: Com o intuito de afetar o maior número de sistemas computacionais possíveis, esse tipo de atacantes não se importa se o que ele está afetando é uma rede coorporativa ou um simples computador pessoal. Muitas vezes com pouco conhecimento, utilizam *scripts* e ferramentas prontas para realizar ataques em massa. Esse tipo de atacantes, também conhecido como *lammer*, é o mais comum na rede hoje, sendo a maioria dos ataques, *scans* e sondagens realizadas por eles.
- *Advanced Blackhats:* Mesmo em menor número são considerados os mais perigosos do grupo de atacantes. Procuram realizar ataques em sistemas de alto valor causando perda financeira ou de informações valiosas, como o terrorismo patrocinado por estados. Possuem uma habilidade computacional avançada, podendo atacar sistemas sem que o administrador saiba que está comprometido.
- *Advanced Whitehats:* Conhecidos como atacantes do bem, realizando ataques em prol do conhecimento. Os *Whitehats* são responsáveis por reportarem vulnerabilidades no sistema para grandes empresas desenvolvedoras de softwares. Em prol do conhecimento a todos, não realizam ataques para prejudicar corporações ou governos.

### 2.2.2 Alvos

Muitas pessoas têm uma ideia errada de que está fora dos alvos de qualquer possível atacante, devido achar que as informações contidas em seu computador não são importantes. Porém os atacantes não buscam somente informações, seu computador pessoal poderá ser invadido e o atacante utilizar seus recursos como conexão com a internet, disco rígido, memória e processamento para realizar ataques a terceiros.

Todo e qualquer dispositivo como smartphones, notebooks, tables e computadores pessoais que estejam conectados em uma rede, podem receber um ataque.

### 2.2.3 Motivação

A motivação de se realizar um ataque ou se tornar um atacante possui diversos fatores como dinheiro, ego, diversão, ideologia, status e/ou inclusão em um grupo social. A obtenção desses fatores pode vir de várias maneiras como a invasão de uma rede coorporativa, roubo de números de cartões de créditos ou possuir controle de milhares de computadores.

Tendo seu alvo e motivação escolhido, os atacantes gozam de diversos métodos e ferramentas para realizarem os ataques. Os métodos utilizados variam de acordo com a escolha feita anteriormente ao ataque, onde o atacante irá relacionar o melhor método e/ou ferramenta irá utilizar para atingir seu objetivo.

## 2.3 Ferramentas e Tipos de Ataques

Ao longo dos anos vários ferramentas e métodos de ataques têm sidos desenvolvidos. Segue abaixo, uma lista das principais ferramentas e métodos. Desde o ano 1999, o CERT.br vem analisando as atividades na internet brasileira. Na Tabela 1 são exibidos os ataques mais reportados durante o ano de 2012.

Tabela 1 - Estatísticas de incidentes reportados

**Tabela:** Totais Mensais e Trimestral Classificados por Tipo de Ataque.

| Mês | Total | worm (%) | | dos (%) | | invasão (%) | | web (%) | | **scan** (%) | | **fraude** (%) | | outros (%) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| jan | **27148** | 6830 | 25 | 7 | 0 | 603 | 2 | 2137 | 7 | 8478 | 31 | 4096 | 15 | 4997 | 18 |
| fev | **25266** | 4404 | 17 | 34 | 0 | 452 | 1 | 2211 | 8 | 8523 | 33 | 4183 | 16 | 5459 | 21 |
| mar | **34796** | 2380 | 6 | 22 | 0 | 559 | 1 | 3508 | 10 | 10616 | 30 | 5126 | 14 | 12585 | 36 |
| abr | **35342** | 3171 | 8 | 9 | 0 | 100 | 0 | 2111 | 5 | 9557 | 27 | 7923 | 22 | 12471 | 35 |
| mai | **40965** | 3242 | 7 | 11 | 0 | 413 | 1 | 3532 | 8 | 13339 | 32 | 8557 | 20 | 11871 | 28 |
| jun | **37806** | 2702 | 7 | 9 | 0 | 619 | 1 | 3124 | 8 | 16646 | 44 | 5653 | 14 | 9053 | 23 |
| jul | **42104** | 2922 | 6 | 17 | 0 | 1320 | 3 | 2899 | 6 | 20638 | 49 | 6580 | 15 | 7728 | 18 |
| ago | **60018** | 2867 | 4 | 40 | 0 | 659 | 1 | 1717 | 2 | 41741 | 69 | 5582 | 9 | 7412 | 12 |
| set | **53501** | 3157 | 5 | 9 | 0 | 1043 | 1 | 1359 | 2 | 35571 | 66 | 5730 | 10 | 6632 | 12 |
| out | **39326** | 3380 | 8 | 9 | 0 | 754 | 1 | 1186 | 3 | 23229 | 59 | 6442 | 16 | 4326 | 11 |
| nov | **40751** | 1858 | 4 | 125 | 0 | 716 | 1 | 1116 | 2 | 28065 | 68 | 5268 | 12 | 3603 | 8 |
| dez | **29006** | 1553 | 5 | 17 | 0 | 577 | 1 | 657 | 2 | 16095 | 55 | 4421 | 15 | 5686 | 19 |
| Total | **466029** | 38466 | 8 | 309 | 0 | 7815 | 1 | 25557 | 5 | 232498 | 49 | 69561 | 14 | 91823 | 19 |

Fonte: CERT.br, 2012.

Legenda:

- **Worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **DoS** (*Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **WEB**: um caso particular de ataque visando especificamente o comprometimento de servidores *web* ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

### 2.3.1 DOS (Denial of Service)

Criado em meados da década de 90, o ataque DOS (*Denial Of Service*) têm se popularizado nos últimos anos, chamando atenção da mídia e dos profissionais de segurança. Ultimamente empregado como forma de protesto virtual a várias corporações e órgãos governamentais, o ataque DOS vem ganhando força, já que ferramentas podem ser facilmente encontradas em diversos fóruns ou sites especializados.

Grandes corporações, como eBay, Yahoo, Amazon e CNN, amargam perdas devido aos ataques DOS, cujo no ano de 2000, receberam grandes ataques do tipo DOS que resultou na perca de milhares de dólares. Em março de 2013, um ataque DOS direcionado a uma empresa especializada em AntiSpam foi noticiado pela mídia como o

maior ataque realizado na história, esse ataque chegou a causar lentidão em toda a Internet mundial [JUNQUEIRA, 2013].

O ataque DOS tem por objetivo indisponibilizar ou causar lentidão a um serviço *web* enviando várias requisições ilegítimas. A realização é feita sem que uma invasão ou infecção ao servidor seja necessária, apenas utilizando algumas características de alguns protocolos, como o TCP/IP *(Transmission Control Protocol / Internet Protocol)*.

O efeito é obtido por meio de várias requisições realizadas pelo atacante a um servidor conectado à internet com requisições inúteis, fazendo com que acarrete em uma sobrecarga do servidor que por sua vez não consegue responder a todos, negando a disponibilidade do serviço ou aproveitando-se de falhas ou vulnerabilidades presentes na máquina vítima do ataque.

Para que seja possível realizar um ataque DOS é necessário ter um computador com alto poder de processamento e uma boa banda de Internet disponível ou diversos computadores com recursos variados que se concentram para enviar a uma mesma vítima. O ataque utilizando diversos computadores é muito mais perigoso, pelo ataque partir de diversas origem e ser potencializado, podendo ser controlado por um único atacante.

#### 2.3.1.1 Formas de ataques DOS

As formas de ataques DOS são variadas e podem causar desde consumo total da banda da Internet até consumo de processamento do servidor da vítima, chegando sempre ao mesmo objetivo, são elas:

- ***SYN Flooding:***

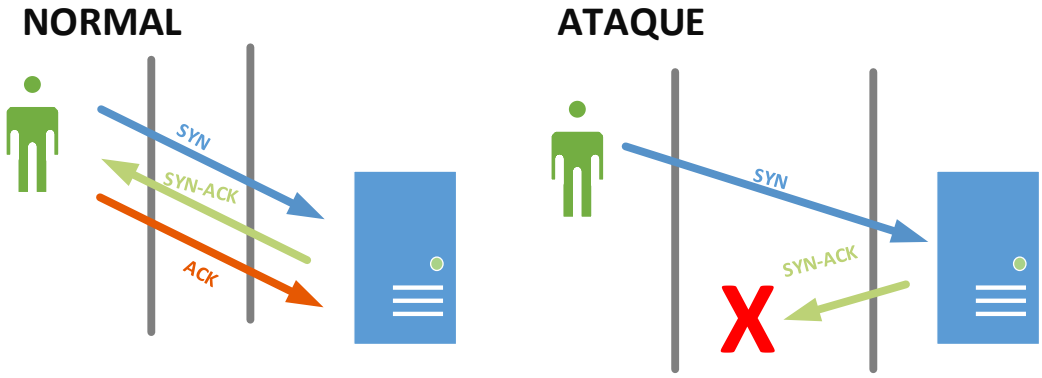
Uma forma bem comum de ataque DOS é com a utilização de pacotes TCP/SYN explorando a abertura de conexões TCP assim inundando o serviço.

O ataque funciona de forma que o cliente envia um pacote SYN contendo parâmetros para que o servidor entenda como uma sequência de acesso e retorne um pacote TCP SYN/ACK, informando ao cliente que o pacote foi aceito. Por sua vez, o cliente envia um pacote ACK para completar a abertura de conexão (DUARTE, 2013).

Utilizando a técnica de IP *Spoofing*, o IP do atacante é mascarado por um outro qualquer, dessa maneira, a vítima ao responder pelo ataque é direcionada para um endereço falso e fica aguardando a uma resposta de uma requisição que não existe. Com essa forma de ataque, os recursos do servidor passa a ser utilizados, como memória e processamento, negando

a novas requisições realizadas para o servidor.

Figura 2 - Ataque SYN Flooding




- ***Fraggle Attack:***

Outra forma comum de ataque, que utiliza pacotes UDP para entupir o servidor de requisições invalida.

Ao contrário do ataque *SYN Flooding*, o *Fraggle Attack* não aguarda resposta do servidor, pois utiliza pacotes UDP. O ataque consiste em enviar diversos pacotes UDP ao endereço de *broadcast* da rede, com cabeçalho alterado levando o IP da vítima como a origem do pacote, para todas as portas do servidor.

- ***Smurf Attack:***

O método de ataque *Smurf Attack* utiliza pacotes ICMP para saturar uma conexão da Internet de baixa ou alta velocidade.

Assim como o *Fraggle Attack*, são enviadas diversas requisições ICMP *Echo Request (ping)*, com o cabeçalho alterado, destinado ao *broadcast* da rede fazendo com que sejam gastos todos seus recursos para responder com ICMP *Echo Reply (ping)*, indisponibilizando os serviços contidos naquela rede.

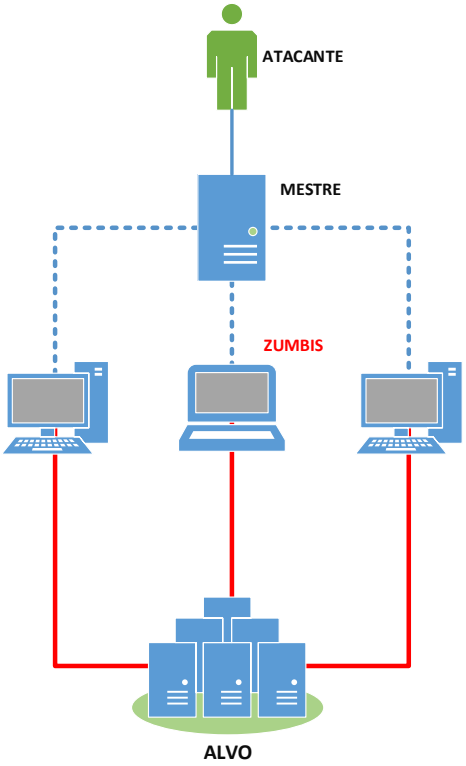
### 2.3.1.2 Tipos de ataques DOS

As variantes de ataques DOS, se diferenciam de acordo com a quantidade de computadores utilizados para realizarem os ataques. Geralmente os computadores utilizados para o ataque são infectados por ferramentas maliciosas sem que o proprietário perceba, deniminadas de zumbis, onde o controle passa a ser do atacante, que pode direcionar o ataque

com um grande poder para qualquer vítima.

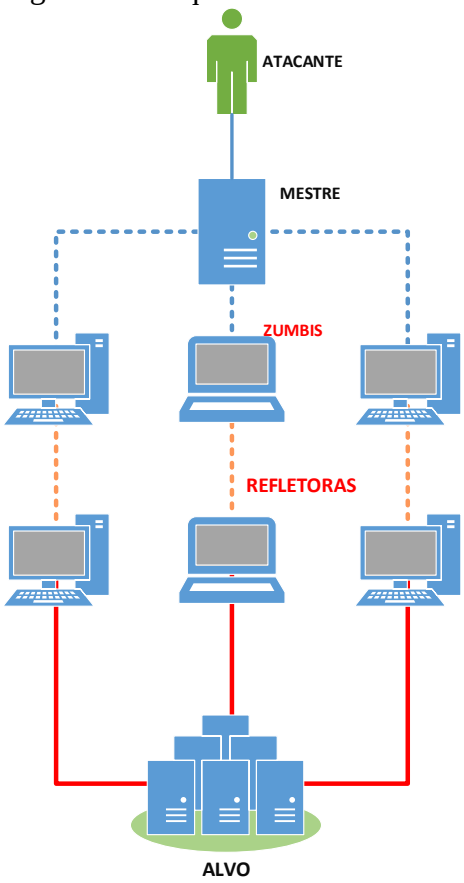
O ataque DDOS é uma evolução do ataque DOS e tem o mesmo objetivo, só que em grandes dimensões. Para realizar o ataque, o atacante utiliza várias máquinas clientes infectadas com malware (*bots*) para fazer ataques DOS simultâneos. Por muitas vezes os *bots* são computadores pessoais, alvo preferido dos atacantes, devido à melhoria da velocidade da conexão com a internet residencial.

Figura 3 - Ataque DDOS




O ataque DRDOS, é uma evolução do ataque DDOS, que além de utilizar máquinas infectadas para realizar ataques, alteram o cabeçalho do pacote para forjá-lo com o endereço IP de resposta da vítima. Assim o atacante direciona o ataque para máquinas refletora, sem que saibam, respondem o ataque ao endereço de IP vítima, inundando sua conexão com requisições inválidas.

Figura 4 - Ataque DRDOS




Os ataques DOS desafiam diretamente a disponibilidade dos servidores, à medida que novas técnicas para bloqueais para o ataque DOS e suas variantes são descoberta, novas formas de ataques vão surgindo, desafiando a segurança da informação e requerendo constantes pesquisa e aprendizado com os ataques.

### 2.3.2 Engenharia Social

É um dos mais utilizados para se conseguir informações sigilosas e importantes, explorando as falhas de segurança dos humanos. Sem que necessite necessariamente de internet, uma rede ou se quer de um computador, o ataque utiliza a confiança da pessoa para conseguir seu objetivo. O ataque pode originar-se de um simples bate-papo na internet até um encontro em um café.

### 2.3.3 Exploit

O termo *Exploit* é utilizado para se referir a pequenos códigos de programas desenvolvidos especialmente para explorar falhas introduzidas em aplicativos por erros involuntários de programação (ALMEIDA, 2013). Criado somente para explorar falhas específicas em softwares ou sistemas operacionais, geralmente há um *Exploit* diferente para cada tipo de falha que pode ser preparado para atacar local ou remotamente.

Um exemplo de *Exploit* bem comum é o SQL *Injection*, que se beneficia de um erro de programação onde os campos que recebem dados inseridos pelos usuários não são validados. O atacante por sua vez, insere códigos SQL nesses campos e executa a ação para ter acesso ao banco de dados utilizado pelo software.

### 2.3.4 Phishing

O método de *Phishing*, é uma fraude que utiliza a engenharia social para realizar roubos online. Este tipo de atividade tem se tornado muito comum na internet. O mesmo consiste em e-mail falsos, contendo códigos ou software maliciosos, enviados em nomes de grandes corporações ou instituições governamentais com o objetivo de capturar dados de documentos pessoais, conta de banco, senhas, cartão de crédito entre outras informações importante.

### 2.3.5 Backdoor

O método de ataque *backdoor* contamina o computador por meio de um cavalo de tróia que deixa propositalmente uma porta de rede aberta, assim sendo possível o acesso remoto. Esse tipo de vírus é comumente usado por ataques DDoS, onde o atacante infecta a máquina com a possibilidade de utilizar remotamente para um ataque. A infecção de vírus pode vir de várias formas, porém a mais utilizada é por meio de e-mail e utilizando páginas *web* falsas.

### 2.3.6 Sniffer

Método utilizado para interceptar e registrar todo o tráfego de dados em uma redes

ethernet ou wireless. Assim que um *sniffer* é executado em uma rede, é realizada a captura do pacote e eventualmente seu conteúdo é decodificado e analisado de acordo com a *request for coment* (RCF) ou alguma outra especificação.

### 2.3.7 Spoofing

- *Arp Spoofing*

O ataque de *Arp Spoofing* consiste em o atacante se passar pela vítima redirecionando o tráfego de rede para sua máquina. Para que isso ocorra é enviada uma mensagem ao roteador da vítima informando que o endereço de IP da vitima está atrelado ao seu endereço físico (MAC).

- *IP Spoofing*

O ataque IP Spoofing trabalha no nível de pacotes onde seu cabeçalho é alterado para que o remetente não seja descoberto. O método consiste em realizar na troca do IP de origem do pacote para um falso remetente, como os roteadores não verificam esse endereço o método se torna eficaz quando utilizado. Esse método é muito utilizado por ataques DoS.

### 2.3.8 Brute Force

Um dos métodos mais antigos para se realizar um ataque, consiste em realizar o maior número de combinações possíveis para se obter o resultado esperado, como a descoberta de um usuário e senha. Ainda muito utilizado por atacantes o resultado é obtido por meio de *scripts* ou softwares que realizam a varredura de acordo com os parâmetros passados.

### 2.3.9 BOT

Realizando tarefas automáticas, como manter controle de canais de IRC e em sua maioria para realizar ataques DDOS, o BOT é um computador infectado com uma praga que permite ser acessado remotamente para execução de qualquer tarefa requerida pelo atacante, se tornando uma máquina “zumbi”.

### 2.3.10 Malware

Segundo o CERT.BR, Códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador. Vírus, *Worm*, Trojan ou *Spyware* podem ser considerados *malwares.*

Muitos ataques realacionados a rede de computadores podem ser bloqueados de forma simples e rápida, com a utilização de tecnologias específicas. Uma delas presente tanto no meio corporativo quanto no do usuário doméstico, é chamado de *firewall*, que protege a rede de acordo com as configurações especificas realizadas pelo seu administrador.

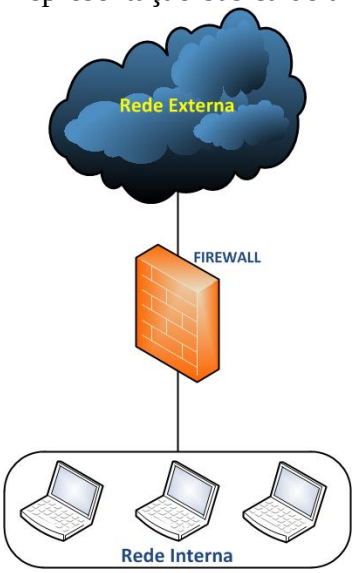
## 2.4 Firewall

O *firewall* é uma solução para segurança de rede que pode ser implementado em hardware ou software e que controla e restringe o fluxo de dados trafegados entre diferentes redes. O seu uso mais comum consiste em bloquear acessos indesejados e liberar acessos aceitos em uma rede, sendo hoje uma das soluções de segurança mais comum.

Possuindo diversos recursos, o *firewall* se tornou uma ferramenta essencial para uma rede em geral. Não só defendendo, mas criando certas políticas de segurança e controle de conteúdo como *Network Adress Translation* (NAT) / *Port Adress Translation* (PAT), estabelecimento de *Virtual Private Network* (VPN), entre outros.

Segundo Chris Roeckl (ROECKL, 2004), o f*irewall* filtra o tráfego trocado entre as redes, reforçando a política de controle de acesso de cada rede. Assegura que apenas o tráfego autorizado passa para dentro e para fora de cada rede ligada. Para evitar o comprometimento, o próprio *firewall* deve ser endurecido contra ataque. Para permitir a formulação de políticas de segurança e verificação, um *firewall* também deve fornecer monitoramento e registros.

Figura 5 - Representação básica de um firewall.




### 2.4.1 Tipos de Firewall

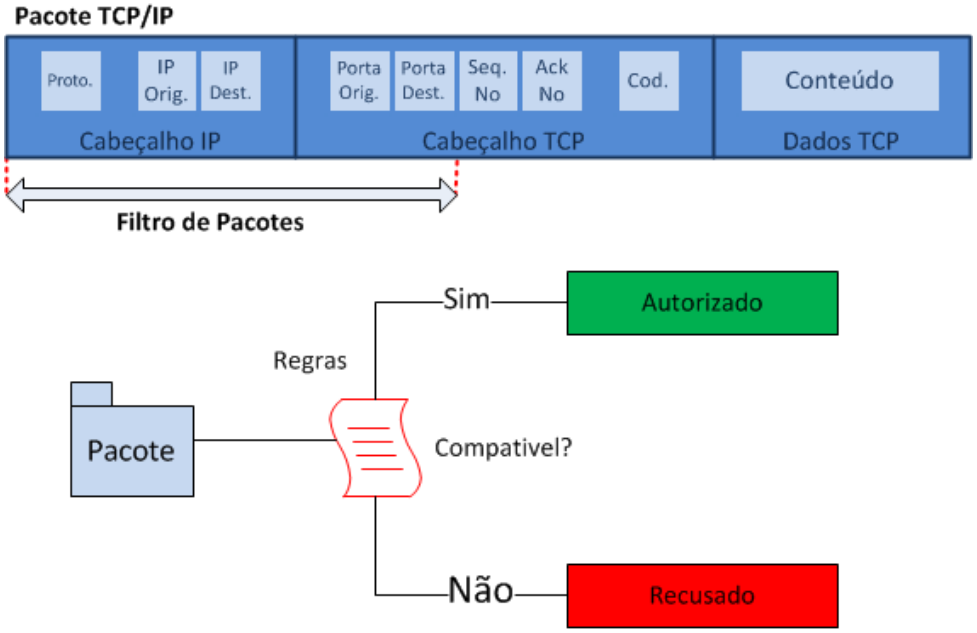
Um *firewall* pode ser utilizado de várias formas para diversos fatores. Segundo Emerson Alecrim (2013), o que deve definir a metodologia a ser utilizada são as necessidades específicas do que está sendo protegido, dentre outras características.

#### 2.4.1.1 Filtro de Pacotes

Sendo um dos tipos mais comuns o filtro de pacotes também está contido nos softwares de roteadores. Trabalhando com pacotes TCP/IP, utiliza informações do cabeçalho do pacote como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros para definir se o pacote será liberado ou rejeitado na entrada ou saída da rede.

O filtro de pacote é realizado por meio de regras de controle de acesso configuradas diretamente no *firewall* e limitadas normalmente para trabalhar nas camadas de transporte (onde ocorre o endereçamento de IP e portas) e rede (onde define o protocolo). O processamento de suas regras é relativamente rápido, porém à medida que politicas de seguranças mais complexas são adicionadas torna seu processamento mais lento e suas regras mais difícil de gerir.

Figura 6 - Esquema de filtragem de pacote.

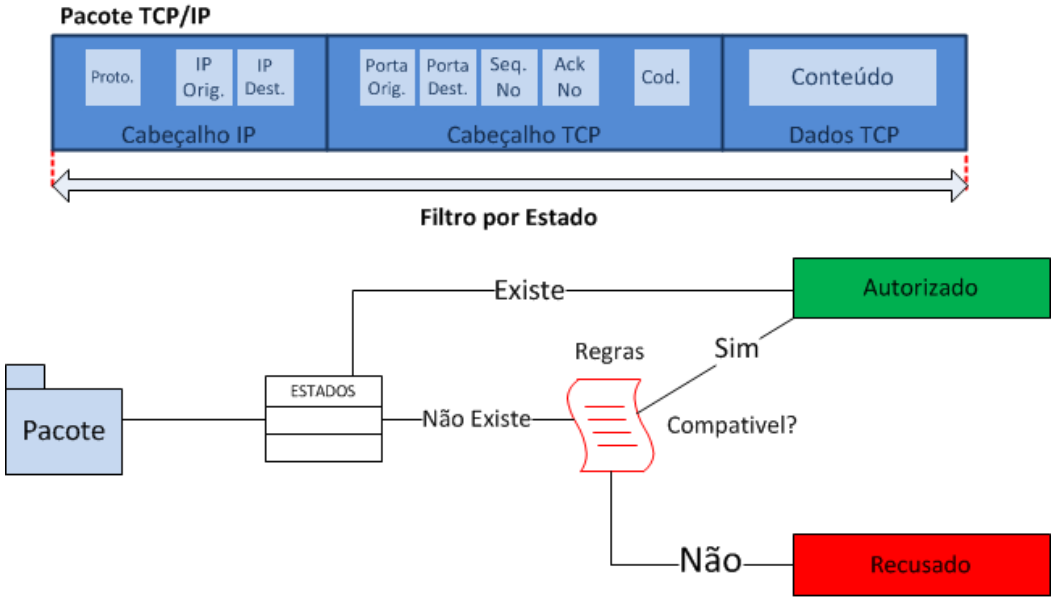



### 2.4.1.2 Filtro Baseado em Estados

Considerado uma evolução do filtro de pacotes, o filtro baseado em estados possui sua própria tabela que por sua vez é associada à tabela de regras para auxiliar na tomada de decisões. Ao iniciar a verificação o *firewall* baseado em estado realiza a inspeção completa dos pacotes ao invés de somente filtrá-los, deixando passar somente pacotes que estão com o estado pertencente à tabela.

O método de filtro baseado em estados é mais seguro e veloz, pois assegura que pacotes ilegítimos não entrem na rede e ganha desempenho, pois somente os pacotes que iniciam conexão serão comparados com a tabela de regras e os demais com a tabela de estados. Na figura 7 uma representação de um *firewall* baseado em estado.

Figura 7 - Esquema de filtragem de pacote baseado em estados.

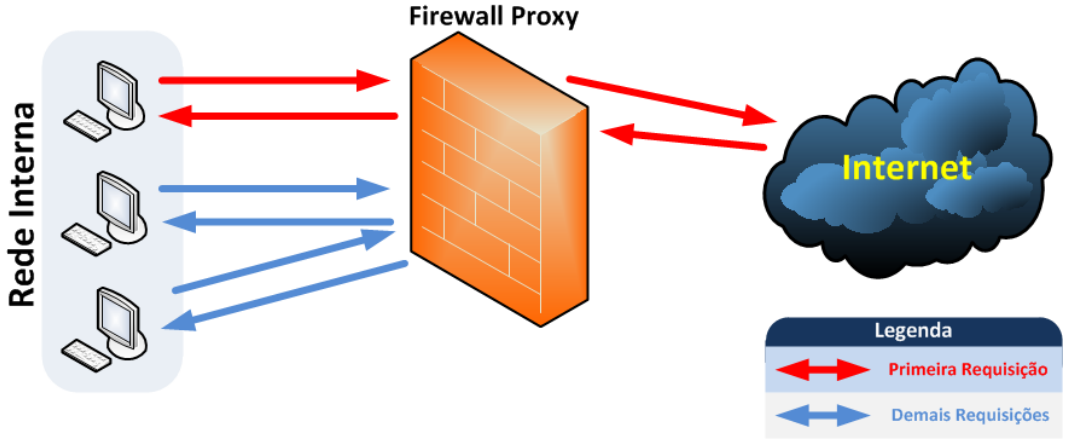



### 2.4.1.3 Firewall Proxy

Também conhecido por *firewall* de aplicação, é uma solução que faz intermediações entre uma rede interna e uma rede externa, por muitas vezes a internet, interceptando todas as mensagens que entram e saem da rede. O método possibilita que as máquinas na rede interna não tenha conexão direta com a internet para navegação, sendo responsabilidade exclusiva do *firewall* de buscar e entregar o conteúdo.

Um *firewall proxy* trabalha principalmente com requisições HTTP (*HyperText Transfer Protocol*), com características de filtragem de pacotes. A requisição realizada a uma página, são armazenadas em um *cache* em seu primeiro acesso e caso haja outra solicitação a requisição é feita ao *firewall proxy*, assim economizando banda de internet. Além da principal funcionalidade é possível disponibilizar aos administradores da rede registro do tráfego de dados e controle de acesso à página de internet por meio de autenticação de usuários.

Figura 8 - Requisições com firewall Proxy.




### 2.4.1.4 Firewall Hibrido

Sendo o mais comum encontrado no mercado, o *firewall* hibrido oferece o que há de melhor do filtro base em estado e métodos do proxy. Esse tipo de *firewall* é considerado o mais rápido e flexível em comparação com os dois modos que ele herda. São utilizados para obter maior performance e segurança em redes de muitas organizações.

## 2.4.2 Arquiteturas de Firewall

Com vários tipos de *firewall*, a implementação pode ser feita de várias formas. Uma arquitetura de *firewall* é definida de acordo com a necessidade da organização. Abaixo será descrito três arquiteturas de *firewall* que são *Dual-homed Host*, a *Screened Host* e *Screened Subnet*.

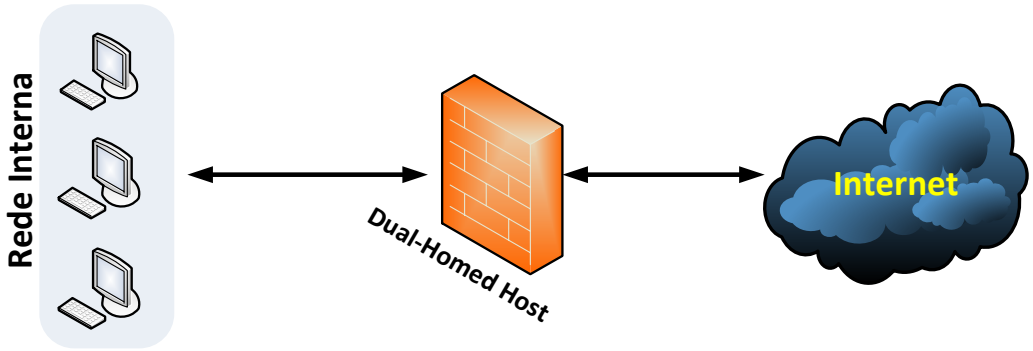
### 2.4.2.1 Dual-Homed Host

Nesta arquitetura há uma máquina que leva duas ou mais interfaces de rede, sendo uma exclusiva para rede interna e outra para rede externa. Requisição direta da rede interna a Internet não são permitidas sendo necessário o uso de um proxy para realizar a comunicação, pois ele não realiza todo tipo de roteamento.

A arquitetura não permite que seja seguro suficiente, por ter somente uma máquina responsável por realizar todo controle. Sua vantagem por ser encontrada quando utilizado quando o trafego de Internet na rede é pequeno e não critico para os negócios, não é oferecido

nenhum serviço a usuários baseado na Internet e a rede que está sendo protegida não guarda dados valiosos.

Figura 9 - Arquitetura *Dual-Homed Host.*

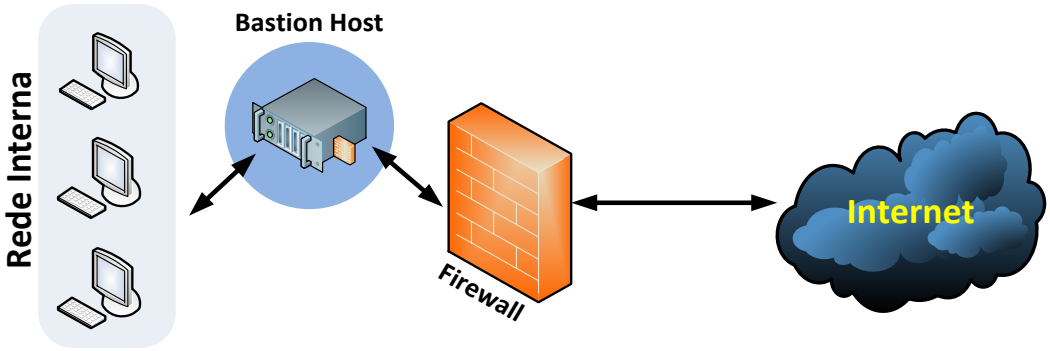



### 2.4.2.2 Screened Host

A arquitetura *Screened Host* não depende de somente uma maquina para fazer a comunicação e sim duas, sendo uma para servir como roteador e outra chamada *bastion host.* O *bastion host*, por muitas vezes um *proxy server*, irá trabalhar entre o roteador e a rede interna para que não permita comunicação direta em ambos os lados da rede, criando uma camada extra de segurança.

O roteador da rede trabalhará para filtrar os pacotes e deverá permitir acesso a Internet somente ao *bastion host*, que por sua vez deverá decidir o que deverá ter acesso à internet. Sua segurança deve ser aprimorada para caso o roteador seja atacado, a rede interna não seja comprometida. Essa arquitetura é recomendada para rede de pouco acesso a Internet, onde a rede interna for segura, e não é recomendado caso seja para uso com um servidor *web*.

Figura 10 - Arquitetura *Screened Host*

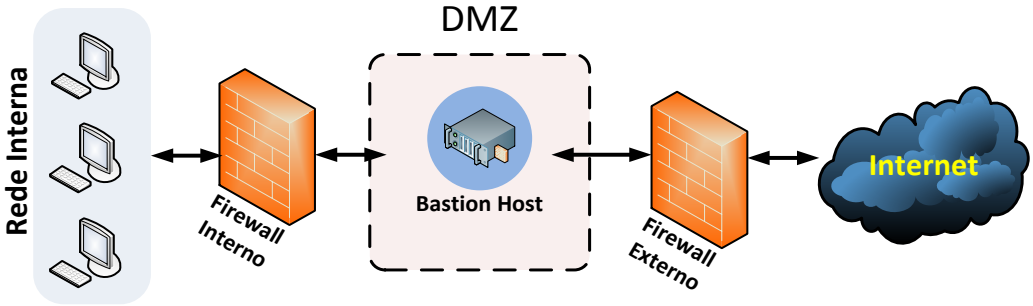


### 2.4.2.3 Screened Subnet

Utilizando uma rede DMZ (Zona Desmilitarizada) com *bastion host*, a arquitetura *Screened Subnet* proporciona maior segurança do que seu modelo anterior, a *Screened Host*. Este modelo há dois roteadores que realizam o filtro de pacotes, sendo um entre a DMZ e a rede interna e outro entre a DMZ e rede externa.

O filtro externo deve permitir que somente acessos destinado a rede DMZ sejam liberados, sendo assim os serviços localizados na DMZ não podem ter acesso a rede interna. Caso o filtro externo seja comprometido o filtro interno deverá proteger a rede interna.

Figura 11 - Arquitetura *Screened Subnet*




Além do *firewall*, outras tecnologias mais específicas são utilizadas para a detecção de uma violação na rede, porém não tanto comum. Essas tecnologias trabalham em conjunto com outras para aprimorar a seguranção da rede.

## 2.5 Sistema de Detecção de Intrusão (IDS)

Como seu próprio nome diz, o IDS é um sistema de segurança que trabalha com a coleta e análise de dados em busca de acessos não autorizados, não barrado pelo *firewall* em uma rede. Um IDS não expulsa o invasor da rede, porém em constante monitoramento com agentes que não são visíveis ao atacante funciona como um eficaz alarme contra invasores, alertando os administradores para que as medidas necessárias sejam tomadas para bloquear aquele acesso indesejado.

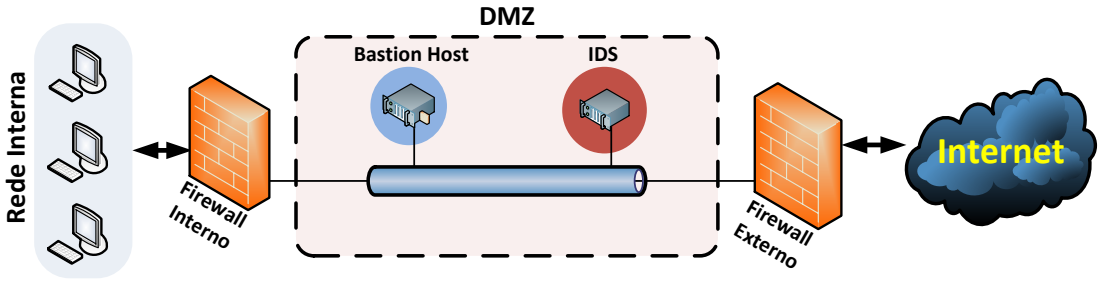
O sistema de detecção de intrusão é definido por Karen Scarfone e Peter Mell (2007) um software que automatiza o processo de monitoramento e análise de eventos ocorridos em um computador ou uma rede, para encontrar sinais de intrusão, cujo o objetivo é comprometer a confidencialidade, integridade ou disponibilidade.

Apesar de ser limitado, por apenas detectar uma invasão, é uma enorme ferramenta em uma rede. A análise dos dados para o alarme é programada de acordo com técnicas e ferramentas de ataques já conhecidas, e também podendo trabalhar em conjunto com outras ferramentas para dar uma visão mais ampla do nível de segurança da rede.

Uma boa configuração do IDS deve ser essencial para que ele detecte somente ameaça, o caso de uma má configuração pode acarretar em falsos positivos ou falsos negativos.

- **Falso Positivo:** Ocorre quando um tráfego legítimo da rede é tratado como um ataque pelo IDS, negando serviços fundamentais para a empresa.
- **Falso Negativo:** Ocorre quando um tráfego ilegítimo da rede é tradado como legitimo pelo IDS, deixando comprometer a rede.

Figura 12 - Representação de arquitetura para um IDS




## 2.5.1 Métodos de detecção e modo de reação

Para realizar a detecção de intrusos alguns métodos são utilizados são eles detecção por assinatura e anomalia.

- **Detecção por Anomalia:** Esse método utiliza uma base com padrões de atividades normais de usuários, hosts e conexões de rede, sendo o que se desviar do padrão é detectado como uma possível invasão, gerando alertas. Suas grandes desvantagens estão na várias sessões para coletar dados para prever todos os padrões de funcionamento normais e o grande número de alarmes falsos de ações não previstas.
- **Detecção por Assinatura:** Método simples e rápido de ser implantado, configurado e testado. Utiliza-se de padrões pré-definidos de ataques e outras atividades maliciosas conhecidas, com base na análise das atividades do sistema para procurar intrusões. Sua principal vantagem, em contra partida do

método anterior, é gerar um número menor de alarmes. A desvantagem do método está em somente reconhecer ataques conhecidos, assim variantes de ataques não são detectados.

O IDS há dois modos para reação de uma intrusão, sendo eles passivo e reativo.

- **Modo Passivo:** Geralmente utilizado pela maioria dos IDS. O modo passivo quando é detectado um tráfego suspeito ou malicioso, somente observa e gera uma alerta e envia ao responsável pelo sistema.

- **Modo Reativo:** Esse modo ao detectar um tráfego suspeito ou malicioso também envia um alerta ao responsável pelo sistema e reage a esse tráfego geralmente bloqueando o acesso em conjunto ao *firewall* ou até mesmo bloqueando uma conta de um usuário. Para que isso seja possível, ações pré-definidas devem ser configuradas junto a eles.

### 2.5.2 Tipos de IDS

HIDS (*Host-Based* IDS): Trabalha somente com um host (máquina), monitorando e analisando todas as informações coletadas, emitindo alertas quando necessário. Neste tipo, não há analise de nenhum tráfego na rede, o foco é sempre mantido no servidor onde é implementado, analisando os logs, portas e sistema de arquivos.

O HIDS é o tipo mais fácil de implementar e gerenciar, porém consumindo muito recurso computacional. São aplicados geralmente em servidores em que a segurança é feita em cima das informações contidas e onde a velocidade de transmissão da rede é muito grande, como redes *"Gigabit Ethernet"*.

NIDS (*Network-Based IDS*): Sendo o tipo mais comum a ser utilizado o NIDS trabalha normalmente a zona desmilitarizada, monitorando e analisando todo o segmento da rede. Os seus sensores realizam tarefas que detectam atividades maliciosas na rede, como ataques baseados em serviço, portscans, entre outros.

Sua principal vantagem está em sua implantação, pois não afeta o funcionamento normal da rede, atuando passivamente para monitoramento do tráfego. Sua grande desvantagem está em processar todos os pacotes da rede, congestionando o sistema quando o tráfego de dados for muito grande e não possibilitando que alertas sejam emitidos.

*PIDS (Protocol-Based IDS):* Um sistema de detecção de intrusão que é normalmente instalado em um servidor *web* e utilizado para monitoramento e analise do protocolo em uso no sistema, no caso de um servidor *web* o protocolo HTTP/HTTPS. O PIDS irá monitorar o comportamento e o estado dinâmico do protocolo, normalmente o ficará localizado na extremidade frontal (*front-end*) entre a comunicação entre um dispositivo e o sistema a ser protegido.

*APIDS (Aplication Protocol-Based IDS):* Assim como o PIDS, o APIDS monitora o estado dinâmico do protocolo, porém, seu agente é localizado entre dois processos ou um grupo de servidores para monitorar e analisar o protocolo de aplicação entre os dois dispositivos monitorados. Por exemplo, a comunicação de um servidor *web* e um banco dados, monitorando um protocolo SQL especifico.

*Hybrid IDS:* Utiliza dois o mais tipos de IDS para complementar a segurança da rede.

A segurança de uma rede deve ser realizada por seus adiministradores de forma primordial, para que bloqueie, detecte e identifique o usuário mal intencionado. Para que isso seja possível tecnologias especificas que provém a identificação de invasores foram criadas, que em conjuntos com as demais tecnologias tornam peça importante para a segurança.

## 2.6 Honeypots

O recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido é chamado de Honeypot (HOEPERS *et al*., 2012), pois simulam um ambiente real de produção, mas possuem mecanismos de contenção, de alerta e de coleta de informações dos atacantes que alivia a carga dos ataques direcionados ao ambiente real de produção, não o comprometendo.

Utilizando recursos para simular diversos serviços como, FTP, servidor de e-mail, SSH, dentre portas utilizadas por alguns programas, um Honeypot tem por objetivo receber todo o tráfego malicioso direcionado a um ambiente de produção e impedir que esse tráfego chegue à Internet, devolvendo somente respostas inofensivas.

O Honeypot pode ser utilizado para pesquisa ou para produção. Quando utilizado para o propósito de pesquisa, o Honeypot tem por objetivo coletar informações como novas ferramentas, malwares e táticas utilizadas pelos atacantes. Quando utilizado para o propósito de produção, o Honeypot é usado para a segurança de outros ambientes reais e assim protegendo a organização do real poder de um ataque. Esse tipo de Honeypot pode proteger a organização

de três modos, sendo eles: prevenção, detecção e resposta (SPITZNER, 2003).

- **Prevenção:** Voltado para prevenção de ataques. O Honeypot trabalha dificultando o acesso do atacante, fornecendo respostas mais lentas ou resposta pré-determinadas pelo administrador do Honeypot, confundindo o atacante e fazendo com que perca interesse ao alvo.
- **Detecção:** Importante para a detecção de atividade maliciosa, para que os administradores do Honeypot possam rapidamente tomar uma decisão sobre a ação a ser tomada, interrompendo ou minimizando possíveis danos ao ambiente de produção.
- **Resposta:** Para coletar informações necessárias, como ferramentas utilizadas pelo atacante, endereço IP e como ele agiu no sistema, com a finalidade de responder ao ataque.

Apesar do conceito ter sido criado há mais de uma década, só recentemente aplicações comerciais e artigos publicados sobre o conceito vem surgindo. Segundo Spitzner (SPITZNER, 2003), a história do Honeypot pode ser resumida na seguinte lista:

- 1990/1991 – Surgem as primeiras publicações sobre o conceito de Honeypot. Em especial os artigos publicados por Bill Cheswick (1990) e Clifford Stoll (1990) se destacam, onde em ambos os casos foi descrita o acompanhamento de uma invasão em um sistema de produção até que a identidade do invasor fosse obtida.
- 1997 – Criação da primeira solução de Honeypot para a comunidade de segurança, a *Deception Toolkit* (DTK) desenvolvida por Fred Cohen.
- 1998 – É criado o primeiro Honeypot comercial vendido ao público, chamado de *CyberCop Sting*, foi a primeira a introduzir o conceito de múltiplos sistemas virtuais em um único Honeypot. Nesse momento também surgem ferramentas mais amigáveis que tornou o Honeypot mais popular, como o *BackOfficer Friendly*, que é uma ferramenta grátis, de uso simples e roda em Windows.
- 1999 – Formação do Honeynet Project, onde um grupo se dedicaria para estudar toda a comunidade de atacantes maliciosos para aprender sobre novas técnicas e métodos de invasão. Nesse momento é de grande evolução para a tecnologia Honeypot.

- 2000/2001 – Empresas passam a usar Honeypot para estudar toda a atividade de *worm* e detecção de novas ameaças.

Com o crescimento da *web*, o desenvolvimento do Honeypot voltado para esse meio é intenso, possibilitando que uma aplicação completa para *web* seja simulada e dados com informações de ataques sejam capturados e analisados. Dessa maneira torna-se uma ferramenta importante, pois cada vez mais as aplicações locais, passam a se tornar públicas na *web*, como sites de compras, sistemas de busca e grandes sistemas ERP.

### 2.6.1 Abrangência, Vantagens e Desvantagens

Contendo em seu próprio conceito o real valor, um Honeypot permite na implementação que todo o tráfego direcionado a ele, serem decorrências de ataques ou anomalias identificadas na rede, dessa maneira há uma diminuição de falsos positivos. Essa abrangência do Honeypot confronta diretamente outras ferramentas de segurança, como o IDS e *firewall*, que trata o trafego como um todo.

Outras de suas principais vantagens, estão na implementação e na captura dos dados. A implementação do Honeypot é relativamente simples e econômica, pois não há necessidade de desenvolver algoritmos complexos, nem mesmo para trabalhar com dados criptografados e com IPV6, e não há necessidade de que o servidor tenha um hardware robusto, podendo ser virtualizado.

Quanto à captura dos dados, em teoria, os falsos negativos, não são capturados obtendo assim uma diminuição nos dados que são armazenados. Em um servidor que receberia todos os dados teriam 5.000 alertas em um arquivo de 10GB no Honeypot teriam 30 alertas em um arquivo de 10MB, simplificando a análise e dando uma reposta mais rápida ao ataque.

Uma das desvantagens de um Honeypot está na sua visão limitada dos dados que podem ser analisados, já que somente atividades que são direcionadas a ele podem ser analisadas, não identificando, por exemplo, ataques com foco a um ponto especifico da rede. É possível também que um atacante identifique o padrão de respostas de um Honeypot e direcione o ataque para outro ponto da rede.

O risco é outro ponto de desvantagem para um Honeypot, pois a partir do momento que se temo Honeypot comprometido por um atacante, pode ser utilizado para afetar outros pontos da rede da organização. Toda vez que ao adicionar novos recursos ao Honeypot utilizando um endereço IP, um risco é assumido e certas medidas de contenção devem ser

tomadas para que eles sejam minimizados. O risco pode variar de acordo com cada nível de interatividade de Honeypot.

### 2.6.2 Classificação por meio de níveis de interatividade

O Honeypot, pode ser dividido em três tipos, sendo eles, de baixa, média e alta interatividade. O nível de interação irá definir o controle que um atacante poderá ter sobre servidor. Dentre suas principais diferenças estão a complexidade na instalação e manuseio, e no propósito de utilização para pesquisa ou produção.

Tabela 2 - Comparação de Honeypot de Baixa, Média e Alta Interatividade

| Característica | Baixa Interatividade | Média Interatividade | Alta Interatividade |
|---|---|---|---|
| Instalação | Fácil | Envolvido | Difícil |
| Configuração | Fácil | Envolvido | Difícil |
| Manutenção | Fácil | Envolvido | Difícil |
| Coleta de Informações | Limitada | Variável | Extensa |
| Risco | Baixo | Médio | Alta |

Fonte: HOEPERS *et al*., 2007

No Honeypot de baixa interatividade são instaladas ferramentas que simulam um ambiente real, como um FTP ou serviços HTTP, onde não é permitido que o atacante interaja com o servidor, sendo que, para isso, é necessário que o sistema operacional seja instalado e configurado de modo seguro. Como o atacante não consegue, em teoria, controle do sistema operacional e seu nível de complexidade de implantação é menor, esse tipo se torna o mais recomendado para a utilização nas organizações, pois consegue somente detectar tipos já conhecidos de ataques.

Já um Honeypot de alta interatividade permite que o atacante tenha controle total sobre o sistema operacional e os serviços nele contido, onde os mesmos não são apenas simulados, como em um Honeypot de baixa interatividade. Este tipo é o mais arriscado e de maior complexidade de implantação, porém oferece uma gama maior na coleta dos dados. Este método de interatividade é mais utilizado para o propósito de pesquisa.

O Honeypot de média de interatividade, assume características dos Honeypots de baixa e alta, podendo ter mais interação que os de baixa mas menor que os de alta. Mesmo tendo um nível de interatividade maior, os serviços não se equivalem a um sistema real, sendo que possam ser simulados porém não somente respondendo a testes de conexão, mas acrescentando informações fazendo com que o atacante interaja mais com o ambiente. Com esse nível de interação é possível que o Honeypot seja utilizado para o propósito de produção quanto o de pesquisa, pois reúne mais informações.

### 2.6.3 Ferramentas e Soluções

Com a necessidade de otimizar a segurança, diversas ferramentas e soluções para Honeypot surgiram ao decorrer dos anos. Essas ferramentas auxiliam principalmente na defesa da rede e no aprendizado de ataques direcionados a ela. As ferramentas a seguir podem ser encontradas nas mais variadas plataformas como Unix, Linux e Windows, podendo simular diversos tipos de aplicações.

#### 2.6.3.1 BackOfficer Friendlly

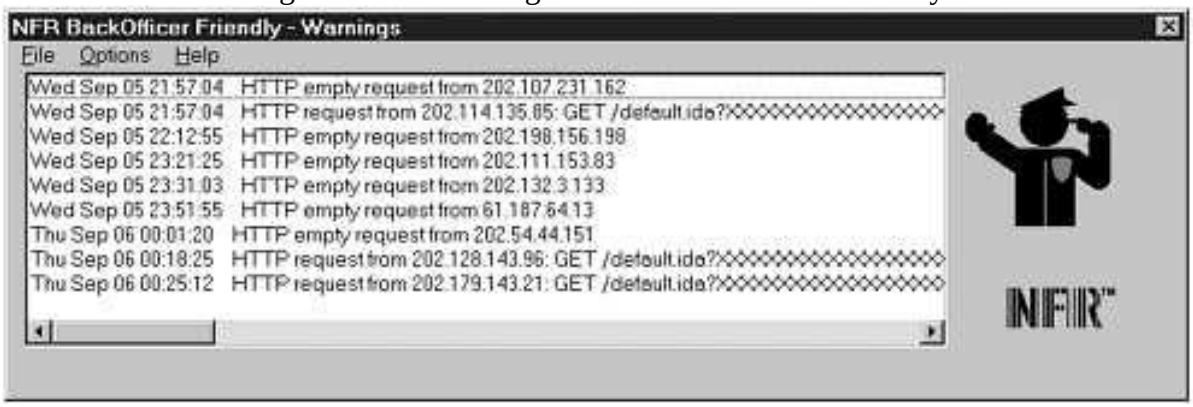
O BackOfficer Friendlly é uma ferramenta grátis de Honeypot de baixa interatividade que pode ser rodada em plataformas Unix ou Unix. Conhecida também como BOF, primeiramente foi criada para a plataforma Windows em suas versões 95 e 98 tornando uma grande solução para usuários comuns. Diferente de alguns tipos de Honeypots, o BOF pode somente emular sete portas.

Originalmente o BOF não foi desenhada para ser um Honeypot, e sim para uma ferramenta de resposta a uma ameaça bem especifica. Podendo trazer um valor a mais na detecção de ataques, porem a segurança é limitada pela falta de possibilidades na customização de serviços a serem monitorados. Por ser limitada a prevenção de ataques com o BOF é difícil por oferecer pouca interação com o atacante.

Voltado para produção o BOF não tem quase nenhum valor para se tornar um Honeypot de pesquisa por necessitar de outras tecnologias para realizar respostas a ataques, podendo somente fornecer informações para análise de tendências. Sempre enfrentando suas a barreira de suas sete portas monitoradas.

- Back Orifice: Trojan baseado em Windows que libera a porta UDP 31337 para realizar invasão.
- FTP: Protocolo utilizado para transferência de arquivos que utiliza a porta TCP 21.
- Telnet: Protocolo utilizado para acesso remoto para administradores de sistemas que utiliza a porta TCP 23.
- SMTP: Protocolo responsável por receber e enviar e-mails, utilizando a porta TCP 25.
- HTTP: Protocolo para acesso a páginas *web* que utiliza a porta TCP 80.
- POP3: Protocolo utilizado para receber e-mail utilizando a porta TCP 110.
- IMAP: Protocolo utilizado para receber e-mail utilizando a porta TCP 143.

Figura 13 - Interface gráfica do BackOfficer Firendlly




### 2.6.3.2 Honeyd

Desenvolvido e mantido desde abril 2002 por Niels Provos na Universidade de Michigan (PROVOS, 2002). O Honeyd é uma ferramenta para Honeypots de baixa interatividade que como as demais ferramentas, simulam serviços virtuais como FTP, HTTP e SSH em uma rede, utilizando *scripts* com respostas pré-programadas. Inicialmente pode ser utilizado para produção, porém possui aplicações especificas para pesquisa podendo simular todas as portas disponíveis em uma rede.

O Honeyd foi desenvolvido seguindo as práticas de Software Livre, por esse motivo, é um ferramenta grátis e de código totalmente aberto, onde pode ser customizado de acordo com a necessidade. O que é muito importante para que seja adequado a cada realidade, diferentes de outros tipos de Honeypots.

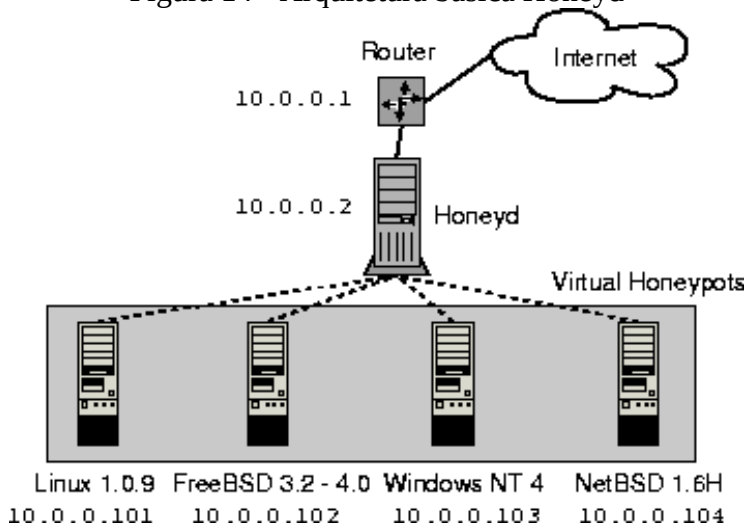
Em seu desenvolvimento o Honeyd, introduziu vários novos conceitos para Honeypots. Um desses conceitos está na resposta de ataques, já que o Honeyd não responde

somente a ataques direcionados a o IP dele, podendo assumir IPS da rede que não estão sendo utilizados para outros serviços. Isso diferencia das demais ferramentas de Honeypots disponíveis no mercado.

Outro conceito do Honeyd é que sua arquitetura também permite, além de emular diversos serviços, emular vários sistemas operacionais ao mesmo tempo. Além disso é possível emular sistemas operacionais a nível de pilha IP, podendo assim responder a scans a assinatura exata do sistema operacional emulado, se comportando com um sistema operacional legitimo.

Possuindo grande capacidade de processamento, o Honeyd pode assumir simultaneamente milhares endereços de IP e interagir ativamente com o atacante. O mais provável é que sua rede se torne um grande gargalo com a grande quantidade de IPS e não o Honeypot, que tem capacidade de trabalhar com redes extremamente grandes.

Figura 14 - Arquitetura básica Honeyd




Fonte: PROVOS, 2002.

### 2.6.3.3 HoneyView

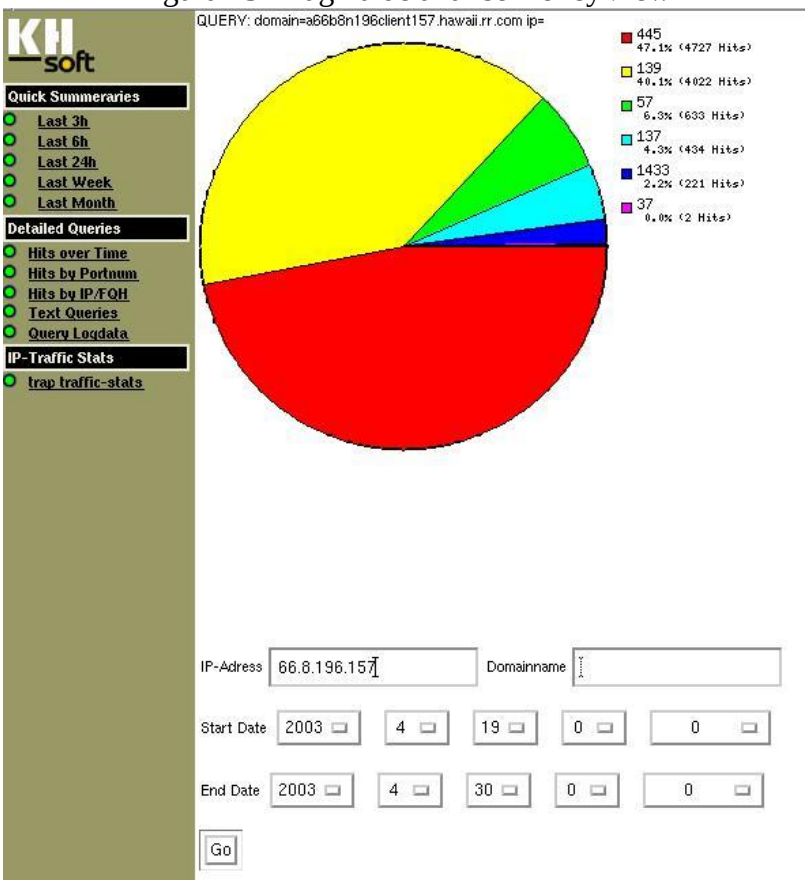
Voltado para análise de log, o HoneyView foi desenvolvido para apoiar o Honeyd e quem o implementa, facilitando a análise dos logs gerados pelo Honeyd. Com a ferramenta é possível gerar gráficos e filtrar dados para melhor visualização, sem a necessidade de abrir arquivos de textos e visualizar todo o acesso linha a linha. Auxiliando também na centralização de logs distribuídos.

Para que isso ocorra, o HoneyView utiliza *scripts* que capturam de tempo em tempo informações geradas pelo Honeyd e armazena em sua base de dados, onde posteriormente sua

parte visual pode ser consultada para visualizar os gráficos gerados com diversas informações. Nele é possível gerar filtros e visualizar informações como portas que estão sendo mais acessadas por período, IPS que estão realizando acessos, dentre outras informações.

Assim como o Honeyd o HoneyView também foi projetado seguindo padrões de Software Livre, e todo seu código se encontra disponível para customização de acordo com cada necessidade.

Figura 15 - Página de analise HoneyView




Fonte: HABLE, 2003

Com a grande gama de ataques disponíveis para os usuários mal intencionadas e a evolução dos mesmos, fica eminente a preocupação com a segurança de um ambiente corporativo, onde a informação é extremamente valiosa. A força das tecnologias que asseguram uma rede, devem ser combinadas para garantir a confidencialidade, integridade e a disponibilidade de um ambiente que abriga aplicações lucrativas.

# CAPÍTULO 3 - PROTEGENDO PLATAFORMA DE COMÉRCIO ELETRÔNICO CONTRA ATAQUES DOS UTILIZANDO HONEYPOT

O presente capítulo aborda a proposta de solução para a implantação do Honeypot. Sendo assim, serão realizadas análises dos resultados obtidos após a implantação, por meio de testes de ataques direcionados ao Honeypot.

## 3.1 Problemática e Solução

Seguindo o aumento do acesso à rede de Internet, novas ferramentas e técnicas que desafiam a segurança da informação surgiram nos últimos tempos, colocando em risco organizações que utilizam a informação para tomada de decisão e definições de estratégias.

Até pouco tempo, os ataques realizados contra a rede de organizações eram realizados por pessoas com grande conhecimento técnico de invasões, porém, ultimamente, pessoas com pouco conhecimento, conseguem realizar grandes ataques devido às ferramentas e publicações que auxiliam os atacantes a comprometer uma rede.

A rede em uma organização tem significado muito nos últimos anos, oferecendo grande suporte ao negócio e tornando-se o essencial para seu crescimento. O comprometimento de uma rede pode gerar graves problemas, podendo acarretar o fim da organização.

As aplicações de comércio eletrônico, naturalmente, dependem da rede de Internet para seu funcionamento e como toda aplicação, estão fadadas a receberem ataques. O comércio eletrônico teve grande aumento em sua visibilidade nos últimos anos, o que resultou na atração de usuários mal intencionados, procurando lesar lojistas e consumidores.

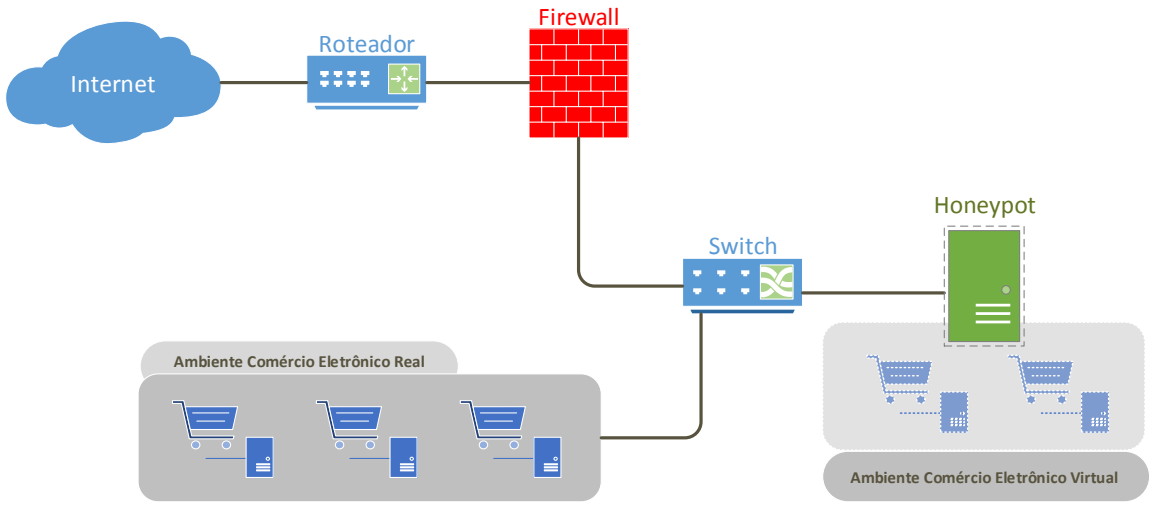
Para que lojas virtuais e plataformas se consolidem no mercado, um fator essencial, é a disponibilidade do acesso, mantendo online a aplicação para que vendas possam ser realizadas. Com a disponibilidade comprometida, a credibilidade depositada pelos clientes da empresa, pode ser perdida e a chance de estagnação do negócio é alta.

A perda causada por um ataque pode ser muito grande em uma loja virtual. Por exemplo, uma loja que fatura em média R$ 1.000.000,00 no mês amarga um perda de R$ 1388,00 por hora parada. No caso de uma plataforma, esse valor deve ser multiplicado pela quantidade de lojas que são hospedadas por ela.

Um dos ataques comuns a uma aplicação da Internet são conhecidos como DOS e DDOS, cujo principal objetivo é comprometer diretamente a disponibilidade do serviço oferecido. Utilizando técnicas e ferramentas especificas para esse tipo de ataque, os atacantes conseguem atingir seu objetivo e manter indisponível uma aplicação conectada à Internet.

Com essas informações, no modelo do projeto será implantado um Honeypot defendendo uma rede que contém uma plataforma de comércio eletrônico. Esse modelo tem por objetivo defender de ataques DOS e DDOS, que comprometem a disponibilidade.

Figura 16 - Modelo de proposta da estrutura de implantação



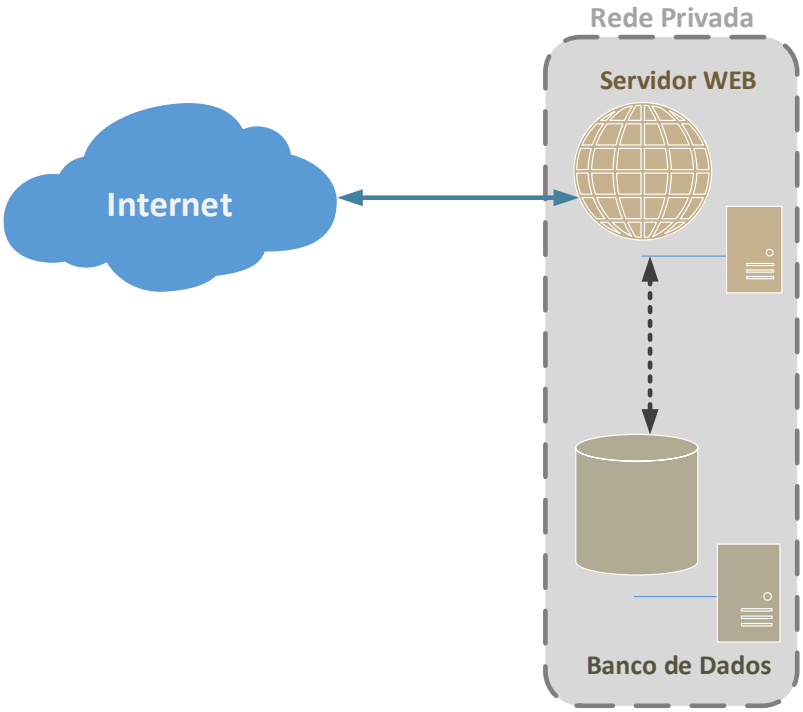

### 3.1.1 Ambiente de Comércio Eletrônico

Neste projeto é considerado Ambiente de Comércio Eletrônico, todo o conjunto de servidores que são responsáveis por manter a aplicação de comércio eletrônico na Internet. Nestes servidores, softwares específicos são utilizados para processar uma requisição realizada por um usuário por meio de um navegador, e devolver a página com as informações necessárias para visualização.

O ambiente estudado é utilizado para rodar uma plataforma de comércio eletrônico, o qual é composto por diversos servidores. Os servidores trabalham de forma separada para que cada um fique responsável por uma tarefa específica.

Podemos dividir o ambiente basicamente em dois principais servidores, sendo eles, um para processar requisições da Internet e outro para processamento de banco de dados. O processamento geralmente não necessita de conexão com a Internet, utilizando uma rede privada. Os servidores que recebem conexões diretamente da Internet, ficam expostos para receber qualquer tipo de tráfego em portas específicas.

Figura 17 - Representação do ambiente de comércio eletrônico.




De acordo com o modelo apresentado na Figura 17, o servidor *web* é responsável , utilizando aplicações especificas, a responder requisições feitas por meio da Internet. A aplicação responsável pelas requisições no ambiente de comércio eletrônico, é nomeada de Apache HTTP Server em sua versão 2.2.15, a configuração da aplicação permite que sejam aceitas requisições na porta 80.

### 3.1.2 Sistema Operacional

Segundo Tanenbaum (2002) um sistema operacional tem duas funções distintas: abstração do hardware e gerenciamento de recursos.

Basicamente, o sistema operacional é o responsável por fazer o intermédio entre o usuário e o hardware, assim não há necessidade de um desenvolvedor de software ter conhecimentos para gerenciamento de hardware. Além desse fator, o sistema operacional é responsável pelo controle de processos, indicando quais podem ser executados e qual recurso de hardware utilizar.

Neste projeto, será utilizado o sistema operacional OpenBSD que se mostrou mais estável nos testes preliminares. O OpenBSD é um sistema operacional grátis e de código aberto que obtém o título do sistema operacional mais seguro do mundo, fazendo disso sua principal

vantagem (OPENBSD, 2013). O sistema operacional já é utilizado em projetos importantes voltado para a segurança com Honeypot.

### 3.1.3 Tecnologias Utilizadas

Cada tecnologia apresentada, tem papel importante no projeto e em conjunto contribuirá para que o objetivo do seja atingido. Os softwares selecionados para serem agregados ao projeto foram previamente estudados e testados.

#### 3.1.3.1 Honeyd

O papel do Honeyd é essencial para o projeto, pois será o software responsável por rodar o Honeypot. Assim como o OpenBSD, é utilizado em grandes projetos que envolvem a criação de Honeypot e tem sua principal vantagem a flexibilidade, por ser totalmente configurável. O software será configurado a partir de seu arquivo principal *honeyd.conf*, utilizando configurações pré-definidas e adequadas para o ambiente de comércio eletrônico estudado.

#### 3.1.3.2 Arpd

O Arpd terá um papel importante nesse projeto, pois será por meio dele que IPS que não estão atribuídos na rede, serão adicionados no servidor de Honeypot. Isso faz com que se possa adicionar o bloco total da rede e o Arpd verifica quais IPS não estão sendo utilizados e por sua vez comece a responder por esses IPS.

#### 3.1.3.3 Mikrotik RouterOS

Embarcado em um hardware específico, o Mikrotik RouterOS, é um sistema operacional baseado no *kernel* Linux 2.6 que possuí ferramentas voltadas para redes de computadores como roteador, *firewall*, *proxy*, monitoramento de tráfego. Atendendo de forma flexível diversos tipos de ambientes, será utilizada a funcionalidade de *firewall* para redirecionamento do tráfego malicioso para o Honeypot.

## 3.2 Implantação do Honeypot

Nesta seção serão implantadas as soluções definidas no modelo proposto, utilizando as tecnologias em conjunto para chegar ao objetivo do trabalho.

### 3.2.1 Cenário de Implatação

Para a implantação do Honeypot é utilizada uma máquina virtualizada por meio do VMware Workstation 10. Nesse servidor será implantado um Honeypot de produção com a características de um ambiente de comércio eletrônico, tal servidor é responsável por receber ataques DOS e DDOS que serão redirecionados por meio de um *firewall*, conforme o modelo proposto.

Configurações da máquina:

- 1 GB de Ram
- 2 Processadores
- 50 GB de disco

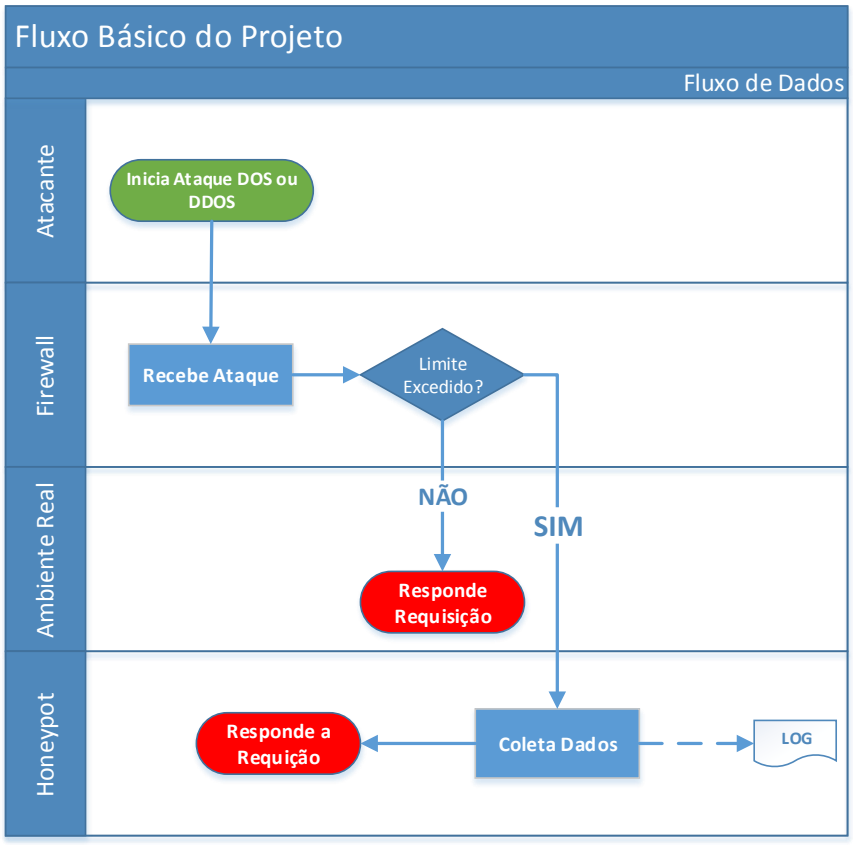
O servidor conta com o Sistema Operacional OpenBSD 5.3 e suas configurações seguem instruções da documentação de instalação oficial (OpenBSD, 2013), e as ferramentas necessárias para o funcionamento eficiente do Honeypot utilizando configurações especificas, para que o objetivo seja alcançado. Sendo assim, serão utilizados no servidor as seguintes aplicações em suas versões:

- Honeyd v1.5c
- Arpd v0.2p3

A configuração de cada aplicação segue suas respectivas documentações oficiais. Em particular, o Honeyd será configurado utilizando códigos pré-programados e adequados para a realidade do modelo proposto, para que trabalhe de maneira que a aplicação responda com semelhança a um ambiente real, não sendo identificado pelo atacante.

Considerando que os ataques serão realizados diretamente ao servidor real, o tráfego deverá ser redirecionado para o Honeypot. Para que seja possível o desvio do tráfego dos ataques, o *firewall* da rede trabalha configurado com um limite de conexões permitida por IP. Após esse limite, o tráfego será considerado como malicioso e assim redirecionado para o Honeypot, que por sua vez irá receber e armazenar as informações sobre o ataque.

Figura 18 - Fluxo de dados




O Honeypot será implantado em uma rede que contém dois servidores voltado para a disponibilização da plataforma de comércio eletrônico, sendo um para processamento de acessos *web* e outra para processamento de dados. Por se tratar de um ambiente de produção e com grande tráfego de informações, serão utilizados endereços de IPs e nomes fictícios para representar os servidores.

Os dados do *firewall* são de propriedade de uma empresa terceira, responsável pelo ambiente de produção, por esse motivo, as regras para o projeto serão solicitadas por meio de chamados. Sendo assim, os códigos de regras não foram disponibilizadas pela empresa responsável e será representados de forma ilustrativa.

Serão utilizados dois IPs no servidor sendo um para utilização própria, para manutenção e outro voltado somente ao servidor emulado pelo Honeypot. Sendo eles:

- 192.168.10.150
- 192.168.10.155

### 3.2.2 Instalação das Tecnologia Utilizadas

A instalação das tecnologias utilizas no projeto, é realizada de forma simples e rápida utilizando repositório, chamado de Ports, do próprio sistema operacional. As tecnologias pertencentes a esse repositório são homologadas para execução no sistema operacional OpenBSD, trazendo maior confiabilidade para todo o projeto.

As configurações serão baseadas em suas documentações originais, porém serão adequadas ao cenário de implantação do Honeypot. Dessa maneira, poderão ser atingidos os objetivos do modelo proposto.

Como premissa deverá ser instalado e atualizado o sistema de repositório Ports, para isso foram utilizados os passos da Figura 16.

Figura 19 - Instalação do Ports

```
# Acesso ao diretório onde deverá ser instalado o repositório:
        cd /usr
# Download do repositório completo:
        ftp ftp://ftp.openbsd.org/pub/OpenBSD/5.3/ports.tar.gz
# Descompactando o repositório:
        tar -xvzf ports.tar.gz
# Acesso ao diretório para atualização:
        cd /usr/ports
# Exportação para o sistema operacional o caminho padrão de acesso ao repositório para atualização:
export CVSROOT=anoncvs@anoncvs.ca.openbsd.org:/cvs
# Execução do comando para iniciar a atualização do repositório:
        cvs -q up -rOPENBSD_5_3 –Pd
```

Após os passos completados, todas as aplicações podem ser instaladas e configuradas normalmente, de maneira que estejam totalmente atualizadas.

#### 3.2.2.1 Arpd

O Arpd dispensa configurações para seu funcionamento, sendo somente necessário, no memento em que é executado, indicar a rede em que deve ser trabalhada.

**Instalação Arpd**

Figura 20 - Comandos para instalação do Arpd

```
# Acesso ao diretório no repositório Ports
cd /usr/ports/net/arpd
# Compilação da ferramenta:
make install clean
```

### 3.2.2.2 Honeyd

A instalação do Honeyd é simples e rápida, porém necessita de algumas bibliotecas que são utilizadas em sua compilação e para seu funcionamento.

**Instalação das Bibliotecas libevent2 e libdnet**

Figura 21 - Instalação das bibliotecas.

```
# Acesso ao diretório da ferramenta libevent2 do repositório:
cd /usr/ports/devel/libevent2/
# Compilação da ferramenta libevent2:
make install clean
# Acesso ao diretório da ferramenta libdnet do repositório:
cd /usr/ports/net/libdnet
# Compilação da ferramenta libdnet:
make install clean
```

**Instalação do Honeyd**

Figura 22 - Instalação do Honeyd.

```
# Antes e prosseguir com a instalação do Honeyd, uma variável do sistema operacional deverá ser retirada:
unset TERMCAP
# Acesso ao diretório no repositório:
cd /usr/ports/net/honeyd
# Compilação da ferramenta:
make install clean
```

### 3.2.3 Configuração do Honeypot

Para que o Honeypot seja eficiente, será trabalhada a configuração da ferramenta Honeyd para que fique semelhante ao ambiente real. A configuração do ambiente será realizada seguindo o modelo proposto e terá as características de um ambiente de comércio eletrônico:

- Sistema Operacional CentOS 6.4
- Servidor *web* Apache 2.2.15

Sua configuração geral é dada por meio do arquivo *honeyd.conf*, que contém as características do servidor emulado como serviços e versão do Linux. Sendo assim, o arquivo foi configurando da seguinte maneira:

Figura 23 - Configuração *honeyd.conf*

```
create centos64
# Primeira seção
set centos64 personality "Linux 2.6.32 (X86_X64)"
# Segunda seção
set centos64 default tcp action reset
set centos64 default udp action block
set centos64 default icmp action open
# Terceira seção
set centos64 uptime 79239
set centos64 droprate in 4
# Quarta Seção
add centos64 tcp port 80 "sh /usr/local/share/honeyd/scripts/suse8.0/apache.sh $ipsrc $sport $ipdst $dport"
# Quinta Seção
bind 192.168.10.155 centos64
```

Na configuração acima, é possível observar que:

- Na primeira seção foi criado um servidor onde a personalidade do kernel do Linux foi assumida na versão 2.6.32, o que representa o CentOS na versão 6.4.

- Na segunda seção foram configuradas respostas padrões para chamadas do tipo UDP, TCP e ICMP, sendo elas respectivamente de para reiniciar, bloquear e abrir a conexão com o Honeyd.
- Na terceira seção foram configurados o tempo de funcionamento do servidor e a porcentagem de pacotes recusados pelo servidor.
- Na quarta seção foi configurado o serviço e porta que será emulada pelo Honeypot.
- Na quinta seção foi configurado o IP no qual o Honeypot irá responder.

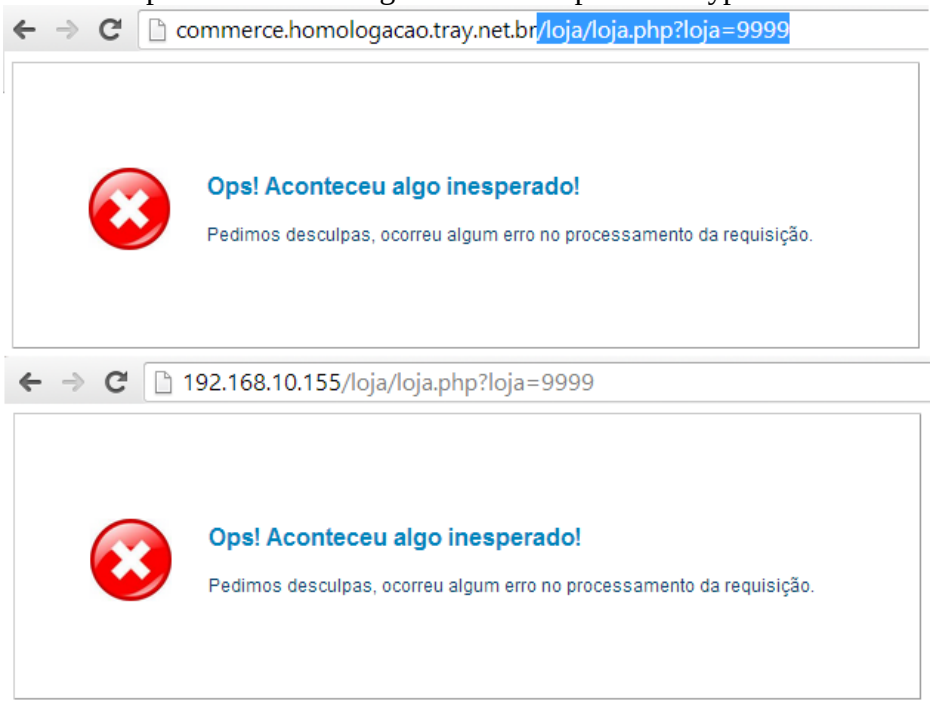
A configuração dos serviços emulados, contido na quarta seção, foi realizada por meio de modelos pré codificados e adequados para a realidade do projeto. Os códigos podem ser encontrados por meio de pacotes, no site do projeto do Honeyd e facilmente instalados junto a ferramenta.

Figura 24 - Instalação dos códigos

```
# Download da Configuração
wget http://www.honeyd.org/contrib/fabian.bieker/honeyd.tgz
# Descompactando configurações
tar -xvzf honeyd.tgz -C /usr/local/share/honeyd/
```

O código de emulação do servidor *web* apache foi editado para se adequar a realidade apresentada no projeto. As respostas dada pelo código, foram configuradas para se assemelhar com o ambiente real da plataforma de comércio eletrônico, para isso foi adicionado no código a mensagem de erro padrão do sistema. O comparativo pode ser visualizado na Figura 25.

Figura 25 - Comparativo de mensagens retornada pelo Honeypot e o ambiente real.




Para que isso fosse possível, foram retiradas as validações para cada método e criado um método de resposta padrão para qualquer chamada realizada. No cabeçalho da resposta dada a quem recebê-la é indicado que o serviço está disponível, dando a falsa impressão de que o ataque DOS ou DDOS foi bem sucedido.

Figura 26 - Código de resposta.

```
(...)
# Regra padrão
NEWREQUEST=`echo "$req1"`
if [ -n "$NEWREQUEST" ] ; then
    REQUEST="HEAD"
Fi
(...)
case $REQUEST in
  HEAD)
    cat << _eof_
# Cabeçalho de resposta
HTTP/1.1 503 Service Unavailable
(...)
```

Com todas as configurações realizadas, a inicialização do Honeypot é simples e realizada por meio de comandos. Para que atenda aos requisitos, primeiro será iniciada a ferramenta Honeyd e posteriormente o Arpd com a atribuição do IP.

O Honeyd é a primeira ferramenta a ser incializada, utilizando a linha de comando apresentada na Figura 27.

Figura 27 - Comandos para inicialização do Honeyd.

```
/usr/local/bin/honeyd \
-l /var/log/honeyd/log/honeyd.log \
-f /etc/honeyd.conf \
-p /usr/local/share/honeyd/nmap.prints 192.168.10.155
```

Com o comando acima é possível inicializar o Honeyd em segundo plano no servidor, alguns parâmetros devem ser passados para sua inicialização:

- -l: é utilizado para indicar o local de salvamento do log gerado pelo Honeyd.
- -f: opção utilizada para indicar local do arquivo de configuração do Honeyd.
- -p: indica o arquivo onde contém a assinatura do sistema operacional emulado
- 192.168.10.155: IP por qual o Honeyd irá responder.

Como o IP utilizado para esse Honeypot não está atribuído no servidor, é utilizado o Arpd para essa finalidade. Sua inicialização é realiza da maneira demonstrada na Figura 28.

Figura 28 - Inicialização Honeyd

```
/usr/local/sbin/arpd 192.168.10.155
```

Com as instruções obtidas nessa seção, o Honeypot atende ao cenário e o modelo proposto. Sendo assim, os testes e análises dos resultados podem ser feitas normalmente por meio de ataques direcionados ao ambiente real e redirecionados com o auxílio do *firewall*.

## 3.3 Análise de Resultados

A análise dos resultados consistes em provar a eficiencia do honeypot protegendo uma plataforma de comércio eletrônico. Para que a prova seja possível, testes serão realizados

direcionado ao ambiente real e redirecionados ao Honeypot com base em regras de limite de conexão criadas no *firewall*.

Foi utilizado como ferramenta de teste o *script* Slowloris (RSNAKE, 2013), desenvolvido para efetuar ataques DOS. O *script* nasceu a partir do conceito onde uma única maquina possa derrubar um servidor web, cujo o servidor web é afetado com o ataque e os demais serviços continuam funcionando, causando efeitos mínios na largura da banda de Internet e obtendo a negação de serviços web.

As requisições enviadas para o servidor web nunca são completadas, eviando cada vez mais requisições em intervalos regulares e pode assumir diversas caracteristicas, trabalhando de forma furtiva. O Slowloris não é considerado um ataque DOS do tipo TCP, pois não aguarda o retorno de uma requisição para encaminhar outra e pode trabalhar com pacotes do tipo UDP, porém necessita de codificação (RSNAKE, 2013).

O *script* se mostrou flexível para que os testes fossem realizados. Sua instalação pode ser feita em qualquer servidor Linux ou Unix de maneira simples e rápida, como demonstrada na Figura 29.

Figura 29 - Exemplo de instalação e execução.

**# Download do Script**

wget http://ha.ckers.org/slowloris/slowloris.pl

**# Exemplo de execução**

./slowloris.pl -dns “HOSTNAME” -port 80 -timeout 2000 -num 500 -tcpto 5

**# Opções**

## **-dns:** Nome do host, ou IP a ser atacado.

## **-timeout:** Tempo limite de envio de cada janela de requisições.

## **-num:** Número de requisições enviadas de acordo com o tempo limite.

## **-tcpto:** Timeout de cada requisições TCP.

Tendo essas informações como base, os testes serão divididos em três etapas:

- Carga dos servidores: Indicará se está suportando o ataques.
- Redirecionamento Falsos: Somente ataques poderão ser redirecionados ao Honeypot.
- Coleta de informações com o Honeypot: O Honeypot deve salvar informações sobre o ataque realizado.

### 3.3.1 Primeira Etapa

**Ambiente Real**

A primeira etapa de ataques foram realizadas para testar a carga do servidor do ambiente real com o objetivo de obter o número máximo de requisições que o servidor consegue suportar. Para isso foi executado o script *slowloris* de forma crescente até obter o resultado. A partir de 151 requisições ilegítimas, o *webserver* Apache passou negar repostas de requisições legitimas.

Figura 30 - Comando executado no ambiente real

```
./slowloris.pl -dns commerce.homologacao.tray.net.br -port 80 -timeout 1 -num 151
-tcpto 5
```

A performance do servidor do ambiente real se manteve estável, porém os processos abertos pelo *webserver* Apache passaram de 60 para 440.

**Ambiente Honeypot**

Na primeira etapa a carga do servidor de Honeypot também foi testada, utilizando o mesmo tip de teste no servidor do ambiente do Honeypot. Foi utilizado o valor maximo de requisições ilegítimas encontrado no ambiente real, para provar a eficiência, que em teoria deve ser maior que do ambiente real.

Figura 31 - Comando executado no ambiente Honeypot

```
./slowloris.pl -dns honeypot.tray.net.br -port 80 -timeout 1 -num 151 -tcpto 5
```

Devido à abertuda de diversos processos do simulador do *webserver* editado para maior semelhança com o ambiente real, a performance do servidor de Honeypot foi afetada. Com os testes, a carga do servidor foi de 0.26% para 260% e o número de processos aberto pelo honeypot passou de 30 para 625. Apesar desse fator, a coleta de dados não foi afetada, gerando assim 900 registros de acesso a porta 80.

Sendo assim, foi realizada uma alteração no Honeypot, no qual foi configurado para dar nenhuma resposta ao ataque. A mensagem retornada ao atacante é a mesma dada quando o

*webserver* Apache do ambiente real não responde.

Figura 32 - Código criado para respostas vazias

```
#!/bin/sh
SRCIP=$1
SRCPORT=$2
DSTIP=$3
DSTPORT=$4
```

Houve melhoria na performance do script simulador do *webserver* Apache, que foram comprovadas pelo segundo teste. A carga máxima do servidor não ultrapassou 2% e o número de processos abertos se mantiveram em 27 mantendo a média de registros salvos pelo honeypot em 900.

### 3.3.2 Segunda Etapa

A segunda etapa consiste em provar a eficiência do redirecionamento de dados realizado pelo *firewall*, para que somente requisições ilegítimas sejam redirecionadas ao Honeypot.

Com base nos testes realizados na primeira etapa, cada requisição ilegítima vem acompanhada por várias requisições com sua origem e destino sempre marcada com o mesmo endereço. Foi atribuído um limite máximo no *firewall* de 50 conexões por segundo para serem consideradas legítimas, e a partir de 51 conexões vindas da mesma origem e partindo para o mesmo destino são consideradas ilegítimas e assim redirecionadas para o Honeypot.

Este modelo evita que conexões legítimas sejam redirecionadas para o Honeypot.

### 3.3.3 Terceira Etapa

Na terceira etapa, foram testadas a eficiência em redirecionar e a capacidade de coleta de dados do Honeypot. O método do teste realizado na primeira etapa utilizando o script *slowloris* foi repetido, porém neste teste foram enviadas 500 requisições a cada segundo de uma unica vez.

Figura 33 - Comando de teste da terceira etapa.

```
./slowloris.pl -dns commerce.homologacao.tray.net.br -port 80 -timeout 1 -num 500 -tcpto 5
```

Após a execução do comando, foi recolhido o arquivo de registro do Honeyd para análise. O mesmo indicou que haviam sido redirecionadas 409 requisições ao Honeypot, o que indica que houve perda de requisições. Para prova desse valor, foi verificado o arquivo de registros do ambiente real e nele foi constatado que somente 50 requisições foram recebidas, assim como o esperado.

A consolidação das informações apresentadas podem ser observadas na Tabelas 3.

Tabela 3 - Consolidação das Informações

| ETAPA | REQUISIÇÕES | LIMITE | CARGA DOS SERVIDORES | REGISTROS |
|---|---|---|---|---|
| **1 - 1** | 151 por segundo | -- | Estável | -- |
| **1 - 2** | 151 por segundo | -- | Travamento do Honeypot | 900 |
| **1 - 3** | 151 por segundo | -- | Estável | 900 |
| **2** | 151 por segundo | 50 | Estável | -- |
| **3** | 500 por segundo | 50 | Estável | 409 Honeypot |
| **3** | 500 por segundo | 50 | Estável | 50 Real |

# CONCLUSÃO

A impotância no meio da Internet ficou eminente na realização do trablhoa, e que sua segurança deve ser algo que esteja em primeiro lugar em qualquer empresa e que há soluções disponíveis no mercado que auxiliam nessa segurança sem muitos investimos.

O objetivo desse trabalho foi atingido com a implantação de um Honeypot para proteger uma plataforma de comércio eletrônico que trabalha no modelo *SaaS* e mantém cerca de 4500 lojas virtuais onlinel, contra ataques que desafiam a disponibilidade, com o foco em ataques DOS.

O desenvolvimento do Honeypot foi composto por um servidor virtualizado por meio do VMWare Workstation, utilizando o sistema operacional seguro OpenBSD. Foram utilizadas também, ferramentas especificas como o Honeyd e o Arpd que foram responsáveis pelo funcionamento do Honeypot.

Com o estudo efetuado nesse trabalho, além do conhecimento sobre toda a história da Internet, foi possível perceber o seu crescimento e de todo o seguimento, como os usuários, aplicações e ataques. Asism a previsão é que em todos os seguimentos haja grande crescimento para os próximos anos.

Em relação ao seguimento de comércio eletrônico, constatou-se que seu crescimento para os próximos anos é exponêncial, isso indica também que a visibilidade das aplicações aumentam deixando a mercê de usuários mal intecionados da Internet. Isso torna essêncial a preocupação e a implantação de soluções de segurança da informação para essas empresas.

Com a implatação do Honeypot foi percebida a falta de documentações para as ferramentas utilizadas e fontes confiáveis para o desenvolvimento. Assim algumas das soluções foram realizadas pelo método de tentativa e erro. Foi difícil também a localização documentações em português.

Em particular a ferramenta Honeyd se demonstrou eficiente e totalmente flexível, podendo abranger diversas áreas e ter utilização diversa. A flexibilidade da ferramenta faz com que seja adequada para qualquer utilização e para qualquer propósito.

## Trabalhos Futuros

A implantação realizada nesse trabalho protege uma plataforma de comércio eletrônico contra ataques DOS, porém em sua implantação foram notados alguns incrementos para

aumentar sua abrangência.

Sendo assim foram identificadas as seguintes funcionalidades futuras:

- Atribuição de mais serviços: Com a atribuição de mais serviços no Honeypot será possível aumentar sua abrangência para mais tipos de ataques. As funcionalidades permitem que o Honeypot fique mais atraente a atacantes que sondam a procura de portas abertas.

- Abertura do Honeypot a Internet: Com a abertura do Honeypot para Internet será possível deixá-lo visível à rede pública de computadores, com isso mais ataques poderão der direcionados diretamente a ele, potencializando seu uso.

- Ingressar em uma Honeynet: Em uma Honeynet, é possível trabalhar com o Honeypot capturando dados de ataques e sendo reportados para órgãos gestores da Internet, como o CERT.br.

- Adicionar mais critérios de filtragem no *firewall*: Através de um número maior de regras de filtragem no *firewall* irá melhorar a eficiência do Honeypot.

- Trabalha em conjunto com um IDS: Com o auxílio do IDS é possível otimizar a detecção de um intruso e redirecionar ao Honeypot.

- Realizar testes de mais técnicas de ataques DOS: Para efetivar a configuração, realizar um número maior de técnicas de ataques DOS.

- Programar respostas do Honeypot: Implementar respostas no Honeypot para obter maior número de informações sobre o atacante.

# REFERÊNCIA BIBLIOGRÁFICA


ALMEIDA, A. R. **COMO FUNCIONAM OS EXPLOITS**. 2013. Disponível em: < http://www.linuxsecurity.com.br/info/general/artigo_seguranca_alexis.pdf>.

ABNT NBR ISO/IEC 17799. **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**, Segunda Edição, 2005.

B2W. **Estratégia & Investimento**. 2013. Disponível em: <http://www.b2winc.com/hotsites/relatorioanual2012/estrategia-investimento.shtml>.

BARRY, M., LEINER, *e. al*. **Brief History of the Internet**. 2013. Disponível em: < http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins> .

CETIC. **CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO**. 2013. Disponível em: < http://www.cetic.br/> .

CERT.BR. **Incidentes Reportados ao CERT.br**. 2013. Disponível em: <http://www.cert.br/stats/incidentes>.

CHESWICK, B. **An Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied**. AT&T Bell Laboratories. 1991.

CRESPO DE CARVALHO, J., ENCANTADO, L. **Logística e Negócio Electrónico**. PORTO: SPI – Sociedade Portuguesa de Inovação. 2006.

DI GIORGI, F. **Lojas virtuais de rede de lojas física: uma relação conflituosa**. 13 de feveireiro de 2013. Disponível em: < http://ecommercenews.com.br/artigos/cases/lojas-virtuais-de-rede-de-lojas-fisica-uma-relacao-conflituosa>.

DRSKA, M.. **Brasil entra na lista de desejos do eBay**. 18 de setembro de 2013. Disponível em: < http://brasileconomico.ig.com.br/noticias/brasil-entra-na-lista-de-desejos-do-ebay_135909.html?utm_source=twitterfeed&utm_medium=twitter>

E-Bit. **Shoppers Brasil**. Março de 2013. Disponível em: <http://img.ebit.com.br/webshoppers/pdf/WebShoppersBrasil_TodasEdicoes.pdf>

E-COMMERCE NEWS. **Mais de 60% dos internautas visitaram lojas on-line em agosto**. 16 de outubro de 2013. Disponível em: < http://ecommercenews.com.br/noticias/pesquisas-noticias/penetracao-do-e-commerce-atinge-61-dos-internautas-brasileiros>.

E-CONSULTING. **Business 2 Business e o Caminho da Inclusão Empresarial**. 4 de janeiro de 2013. Disponível em: <http://www.e-consultingcorp.com.br/business-2-business-e-o-caminho-da-inclusao-empresarial/>

EMARKETER. **Ecommerce Sales Topped $1 Trillion for First Time in 2012**. 05 de feveireiro de 2013. Disponível em < http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649>

EUGENIO, M. **Mercado Livre fecha quarto trimestre com faturamento de US$ 103,8 milhões**. 11 de Março de 2013. Disponível em: <http://www.dlojavirtual.com/noticias/mercado-livre-fecha-quarto-trimestre-com-faturamento-de-us-1038-milhoes/>

FLYNN, I. M. **Introdução aos sistemas operacionais. São Paulo: Pioneira Thomson Learning**. Pioneira Thomson Learning. 2002.

GOOGLE TRENDS. **Interesse com o passar do tempo**. 2013. Disponível em: <http://www.google.com/trends/explore#q=Magento%2C%20PrestaShop%2C%20OpenCart&cmpt=q>

GUASTI, P. **Dossiê: E-commerce X Varejo tradicional**. 10 de Outubro de 2008 Disponível em: <http://www.e-commercebrasil.org/numeros/dossie-e-commerce-x-varejo-tradicional/>

HABLE, K. **Honeyview**. Disponível em: <http://honeyview.sourceforge.net/>

HOEPERS, C. S.-J. **Honeypots e Honeynets: Definições e Aplicações**. 10 de agosto de 2007. Disponível em: <http://www.cert.br/docs/whitepapers/honeypots-honeynets/>

HONEYD. **Developments of the Honeyd Virtual Honeypot**. 2013. Disponível em <http://www.honeyd.org/>

IBEVAR. **Ranking 2012 100 Maiores Empresas do Varejo**. 2012.

IBOPE. **Número de pessoas com acesso à internet no Brasil chega a 105 milhões.** 03 de outubro 2013. Disponível em: <http://www.ibope.com.br/pt-br/noticias/paginas/numero-de-pessoas-com-acesso-a-internet-no-brasil-chega-a-105-milhoes.aspx>

JUNQUEIRA, D. **A história por trás do maior ataque DDoS da história que atingiu o coração da internet**. 2013. Disponível em: <http://gizmodo.uol.com.br/um-dos-maiores-ataques-ddos-da-historia-atingiu-o-coracao-da-internet/>

MAGENTO. **About US**. Disponível em: < http://www.magentocommerce.com/company/>

MIRANDA, M. **Segurança virtual não é mais diferencial, é obrigação. Revista E-Commerce Brasil. 6 Ed**. 2011.

DUARTE, O. C. M. B **Denial of Service - Negação de Serviço.** 2013**.** Disponível em: < http://www.gta.ufrj.br/grad/06_1/dos/index.html>

OPENBSD. 2013. Disponível em: < http://www.openbsd.org>

PINGDOM. **Internet 2012 in numbers**. 16 de janeiro de 2013. Disponível em: < http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/>

PROVOS, N. **Developments of the Honeyd Virtual Honeypot**. Disponível em: < http://www.honeyd.org>

ROECKL, C. **Stateful Inspection Firewalls: An overview of firewall technology and how Juniper Networks implements it.** Juniper Networks, Inc., 2004.

RSNAKE. **Slowloris HTTP DoS**. Disponível em: <http://ckers.org/slowloris/>

Scarfone, K.; Mel, P. **Guide to Intrusion Detection and Prevention Systems (IDPS).** National Institute of Standards and Technology. 2007.

SPITZNER, L. **Honeypots: Tracking Hackers**. Addison Wesley. 2002.

SPITZNER, L. **Honeypots: Definitions and Value of Honeypots**. 29 de maio de 2003. Disponível em: < http://www.tracking-hackers.com/papers/honeypots.html>.

STOLL, C. **The Cuckoo's Egg** . 1990.

TRANSLATED. **T-Index 2012, the markets that matter on the web**. 2012

TANENBAUM, A. S. **Sistemas Operacionais Modernos**. 3 ed. São Paulo: Person Prentice Hall, 2009. 638 p.

TRAY. **Tray E-Commerce Completo**. Disponível em: <www.tray.com.br>

UOL HOST. 10 curiosidades que te farão viajar na história do e-commerce. 06 de agosto de 2013. Disponível em: < http://www.uolhost.com.br/blog/10-curiosidades-que-te-farao-viajar-na-historia-do-e-commerce#rmcl>

VALLE, A. **O que é Plataforma de E-commerce?**. 24 de abril de 2013 Disponível em: < http://www.cursodeecommerce.com.br/blog/o-que-e-plataforma-de-ecommerce/>

WARD, M. **Celebrating 40 years of the net**. 29 de outubro de 2009 Disponível em: <http://news.bbc.co.uk/2/hi/technology/8331253.stm>