FACULDADES INTEGRADAS DE CARATINGA

FACULDADE DE CIÊNCIA DA COMPUTAÇÃO

DETERMINAÇÃO DO PERFIL DE ATAQUES EM HONEYPOTS DE ALTA INTERAÇÃO

LUIZ FILIPE DE FREITAS

CARATINGA

2012

Luiz Filipe de Freitas

DETERMINAÇÃO DO PERFIL DE ATAQUES EM HONEYPOTS DE ALTA INTERAÇÃO

Monografia apresentada à Faculdade de Ciência da Computação das Faculdades Integradas de Caratinga como exigência parcial da disciplina de Trabalho de Conclusão de Curso, sob orientação do professor Msc. Jacson Rodrigues Correia da Silva.

CARATINGA

2012

Luiz Filipe de Freitas

DETERMINAÇÃO DO PERFIL DE ATAQUES EM HONEYPOTS DE ALTA INTERAÇÃO

Monografia submetida à Comissão examinadora designada pelo Curso de Graduação em Ciência da Computação das Faculdades Integradas de Caratinga como requisito para obtenção do grau de Bacharel.

_____

Prof. Msc. Fabrícia Pires Souza Tiola

Faculdades Integradas de Caratinga

_____

Prof. Msc. Jacson Rodrigues Correia da Silva

Faculdades Integradas de Caratinga

_____

Prof. Glauber Luís da Silva Costa

Faculdades Integradas de Caratinga

Caratinga, 12/12/2012

DEDICATÓRIA

Dedico este trabalho em especial a minha namorada por ter ficado ao meu lado nestes quatro anos, me apoiando nos piores momentos. Ao seu lado eu conseguia forças para querer prosseguir.

Te amo Winnie Kelly.

AGRADECIMENTOS

A Deus por ter me sustentado durante estes quatro anos, me dando coragem e força para seguir em frente.

Agradeço aos meus avós, minha mãe, minhas tias, em especial a minha tia Ana Paula por ter contribuído para que este sonho se tornasse realidade.

A minha namorada que tanto me apoiou ao longo destes anos, trazendo-me calma em momentos difíceis.

Aos professores que compartilharam seus conhecimentos nestes anos, em especial ao professor Jacson, pela orientação e paciência neste trabalho de conclusão.

Aos meus patrões Milton Alves e Milton Alves Junior pelos dias de folga concebidos os quais foram de extrema importante para a conclusão deste projeto.

Agradecimento especial a estes oito guerreiros que assim como eu nunca desistiram de seus sonhos. No final dessa jornada vejo que não cultivei amigos, mais sim irmãos, aos quais sempre levarei no coração, lembrando-me dos momentos de sufoco, de descontração e de risos. Desejo sucesso a todos e que em alguns anos passamos nos encontrar de novamente, todos profissionalmente realizados.

“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece ao inimigo, para cada vitória também ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas”. (Sun Tzu – “A Arte da Guerra”).

RESUMO

A Internet trouxe consigo diversas vantagens, sendo atualmente o principal meio de comunicação e pesquisa. Mas em meio a tantas vantagens surgem os problemas relacionados à segurança. Desde seu surgimento, a principal preocupação é proteger os dados que trafegam por ela, tornando-se uma tarefa difícil já que nos dias atuais há alta incidência de ataques à grandes empresas e órgãos governamentais, mostrando que os invasores estão à um passo á frente dos Administradores de redes e profissionais de segurança. Com a expansão rápida destes ataques, o estudo sobre *Honeypots* pode ser um grande aliado para descobrir a origem e como estes ataques são realizados.

Honeypots são recursos de rede que tem o objetivo de serem atacados e comprometidos, ludibriando um atacante e fazendo-o pensar que está invadindo um serviço real. Com isso, podem-se levantar diversas informações sobre o ataque, como por exemplo, qual seu perfil e quais as motivações do invasor, que ferramentas e métodos foram utilizados e quais serviços são mais desejados por eles. O estudo de *Honeypots* pode ajudar no desenvolvimento de novas tecnologias para identificar, impedir e detectar possíveis invasões.

Para que este estudo fosse possível, utilizou-se neste trabalho um ambiente *Honeypot* de alta interação, com serviços e sistemas operacionais reais, instalados em máquina virtual, conectados à Internet e totalmente sem qualquer tipo de método de segurança, com intuíto de facilitar o registro de possíveis ações maliciosas.

Após a coleta de informações dos alertas gerados pelo sistema de detecção de intrusão e da coleta de pacotes da rede obtidos pelo programa Wireshark, foram obtidas e analisadas informações, como: IP de origem do invasor, usuários e senhas utilizados em conexões sem criptografias, arquivos e registros do sistema modificados, identificação do perfil de ataque e país de origem do ataque.

Palavras chave: *Honeypots*, *Honeynets,* Sistemas de detecção de intrusão, virtualização.

ABSTRACT

The Internet has brought many advantages, and is currently the primary means of communication and research. More amidst so many advantages arise security issues. Since its inception the primary concern is to protect the data that passes through it, protect them has become a difficult task since nowadays the high incidence of attacks on large companies and government agencies showed that the invaders are one step ahead of network administrators and security professionals with the rapid expansion of these attacks on the study Honeypots can be a great ally to discover the origin and how these attacks are performed.

Honeypots are network that aims to be attacked and compromised, an attacker deceiving and making him think that is invading a real service. With it, you can get various information about the attack, such as what is the profile of the attack and the motivations of the attacker, what tools and methods were used, which services are most desired by them. The study of Honeypots and Honeynets can help in the development of new technologies to identify, prevent and detect possible intrusions.

For this study it was possible, was used in this work a high-interaction honeypot environment, with real operating systems and services, installed on virtual machine connected to the Internet and completely without any security method, with intuited to facilitate the registration of possible malicious actions.

After collecting information from the system alerts generated by intrusion detection and collection of network packets obtained by Wireshark program were obtained and analyzed information, such as source IP of the attacker, usernames and passwords used in connection with no encryption, file and modified records system, identification of attack profile and country of origin of the attack.

Keywords: *Honeypots, honeynets, intrusion detection systems, Virtualization.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

FTP	File Transfer Protocol
SSH	Shell Shell
IP	Internet Protocol
IDS	Sistema de detecção de intrusão
PDI	Política de detecção de intrusão
TCP	Transmission Control Protocol
HOST	Computador conectado a rede
DARPA	Defense Advanced Research Projects Agency
SMTP	Simple Mail Transfer Protocol
HTTP	HyperText Transfer Protocol
SDI	Sistema de Detecção de Intrusão
SDIH	Sistema de Detecção Baseados em Host
SDIR	Sistema de Detecção Baseados em Rede
SDIH	Sistema de Detecção Híbridos
LBL	Lawrence Berkely Laboratory
TELNET	Protocolo cliente servidor que permite comunicação entre computadores
CERT.BR	Centro de Estudos, respostas e tratamento de incidentes de segurança no Brasil

SUMÁRIO

1. INTRODUÇÃO

Em 07 de dezembro 1942, os Estados Unidos da América foram vítimas de um bombardeio surpresa de aviões japoneses na sua base de Pearl Habor, muitas pessoas morreram. Em 11 de setembro de 2001, os Estados Unidos foram vítimas de um ataque terrorista em Nova York quando dois aviões colidiram com as famosas torres gêmeas, ambas desabaram matando milhares de pessoas (BARBATO, 2005).

O que há em comum sobre estes dois acontecimentos é que mesmo com grande investimento em segurança para identificar e interceptar o inimigo. As estratégias adotadas pelos invasores foram mais bem planejadas e eficazes do que as estratégias utilizadas pelo órgão de defesa. No ambiente digital essa prática também é aplicada a fim de se defender de ataques, o que motivou os administradores de redes e profissionais de segurança a criarem formas para obter informações dos invasores através da utilização de *Honeypots* (BARBATO, 2005).

Segundo SPITZNER (2002), “um *Honeypot* é um recurso de rede projetado especificamente para ser sondado, atacado e comprometido (invadido)”. A sua implantação pode fornecer a capacidade de tomar medidas ofensivas contra os invasores. Os *Honeypots* podem ser utilizados como simples “alarmes”, sistemas de reposta a incidentes ou ferramentas que recolham informações sobre as táticas utilizadas pelos invasores. Quando existe um conjunto *Honeypots* agrupados em uma mesma rede, existe uma evolução no termo, chamado de *Honeynets.*

A legalidade da utilização de *Honeypots* é bastante discutida. Por se tratar de uma tecnologia nova, muitas pessoas ainda desconhecem o seu funcionamento. Algumas pessoas dizem que os *Honeypots* induzem alguém a fazer algo que normalmente não faria, o que é considerado crime, porém a utilização dos *Honeypots* não induz ninguém, já que os ataques são por iniciativa do invasor, sendo como qualquer outro computador conectado à Internet (SPITZNER, 2002).

Muitos ataques na Internet a empresas ocorrem devido ao descaso que muitas delas têm em relação a falhas de segurança em seus sistemas, falhas que poderiam ser facilmente corrigidas. Uma pesquisa divulgada pela Módulo Security Solutions aponta que 43% das empresas admitem que já sofreram algum tipo de ataque na Internet nos últimos 12 meses, sendo que 24% destes foram registrados

apenas nos últimos 6 meses. Outro dado importante apontado na pesquisa é que apenas metade das empresas brasileiras possui algum tipo de plano de ação formalizado em caso de ataques (ULBRICH e VALLE, 2009).

Ainda segundo ULBRICH e VALLE (2009), existem diversos fatores que contribuíram para o aumento dos números de ataques, um deles é a existência de sites inseguros. É ainda citado um estudo do Gartner Group a estimativa de que quase 2/3 dos servidores Web podem ser invadidos de alguma forma. Outro fator importante que contribui para este aumento é a facilidade de se encontrar ferramentas de ataques na Internet, sendo que qualquer pessoa com tempo livre e conhecimentos medianos podem utilizá-las para direcionar ataques.

O objetivo deste trabalho foi identificar os métodos utilizados, a origem e o perfil dos ataques, além de levantar informações sobre o comportamento dos invasores após o comprometimento do sistema. Para isso, foram criados três *Honeypots* de alta interação instalados em máquina virtual, além de um servidor que foi responsável por receber todos os *logs* gerados pelo sistema de detecção de intrusos, formando-se assim uma *Honeynet* virtual. Para o teste foram utilizados sistemas operacionais diferentes baseados nas plataformas Windows e GNU/LINUX e os serviços utilizados nos testes foram: SSH, TELNET e FTP, ficando disponíveis na Internet por aproximadamente 12 dias. Através da realização deste trabalho foi possível identificar a origem e métodos utilizados pelos invasores, determinar o perfil dos ataques sofridos, realizar uma análise quantitativa dos ataques e determinar qual país mais originou ataques.

No capítulo 2 deste trabalho, foram abordadas as principais definições à respeito dos temas mais relevantes utilizados atualmente. No capítulo 3 foi abordada a metodologia utilizada no presente trabalho, mostrando a estrutura criada e seus requisitos. No capítulo 4 foram apresentados os resultados obtidos na utilização de *Honeypots* de alta interação, além de incluir um resumo dos ataques sofridos. No capítulo 5 foi realizada a conclusão do presente trabalho e uma abordagem dos trabalhos futuros.

2. REFERENCIAL TEÓRICO

Nas próximas seções serão apresentadas as definições encontradas na literatura à respeito dos temas mais relevantes abordados no presente trabalho.

2.1 O MODELO DE REFERÊNCIA TCP/IP

O modelo de referência TCP/IP (Transmission Control Protocol/ Internet Protocol) surgiu através de trabalhos do DARPA (Defense Advanced Research Projects Agency) dos Estados Unidos, por volta da década de 70. Inicialmente a arquitetura TCP/IP foi concebida em um contexto de guerra, onde uma das principais preocupações era interligar os diversos computadores de forma simples e não centralizada, ou seja, caso ocorresse algum ataque que eventualmente pudesse destruir os computadores, a rede continuaria funcionando independente daqueles que foram destruídos (BRANDINO, 1998).

Segundo TANENBAUM (1997) quando foram criadas as redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes da época, o que forçou a criação de uma nova arquitetura de referência, que se responsabilizaria de conectar várias redes ao mesmo tempo, vindo a ser conhecida como Modelo de Referência TCP/IP.

Segundo ULBRICH e VALLE (2009) o protocolo TCP/IP está dividido em diversas camadas, conforme abaixo:

- Camada de aplicação: A camada de aplicação (Figura 1) é responsável pela comunicação entre protocolo destinado ao transporte e os aplicativos em execução, como por exemplo, FTP, SSH, TELNET, HTTP e SMTP, entre outros.

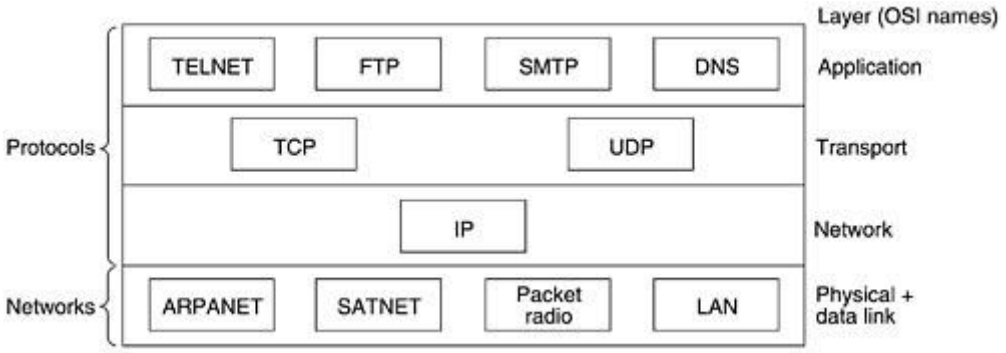

Figura 1: Protocolos e redes no modelo TCP/IP inicial (TANENBAUM, 1997)

- Camada de transporte: está camada é responsável por criar a conexão virtual entre dois computadores.
- Camada de Internet: é responsável pela organização e o roteamento dos pacotes definindo seus endereços.
- Camada de interface com a rede: está camada é responsável pelo envio dos datagramas provenientes da camada de Internet. Ela não faz parte do protocolo TCP/IP, mais é considera um componente obrigatório.

Na próxima seção serão abordados os principais conceitos de sistemas de detecção de intrusão, também utilizados neste trabalho, fornecendo informações sobre os ataques.

2.2 SISTEMAS DE DETECÇÃO DE INTRUSÃO (SDI)

Neste trabalho foram utilizados sistemas de detecção de intrusão com intuito de levantar informações sobre os ataques sofridos, com intuito de identificar o perfil do ataque, métodos utilizados pelos invasores, IP de origem de ataque, modificações feitas no sistema.

Existem hoje em dia diversas tecnologias de segurança para combater ataques ao perímetro da rede. Porém, isso não impede um invasor de obter acesso autenticado aos computadores e ter privilégios como se fosse um usuário legítimo, pois os invasores podem obter tais privilégios por meio de softwares maliciosos

como, por exemplo, cavalos de Tróia. Por este motivo é necessário monitorar todos os pacotes que passam através do *firewall,* fazendo uma analise de como cada usuário utiliza os computadores sejam ele um usuário legítimo ou um invasor, com isso ser capaz de diferenciá-los através de suas ações (WANG, 2009).

Segundo WANG (2009) a utilização dos sistemas de detecção de intrusão foi iniciada por Denning e Peter Neumann, por volta de 1980. Naquela época eles observaram que os invasores muita das vezes tinham um comportamento diferente de um usuário legítimo, essa diferença podia ser medida, sendo possível fazer uma analise quantitativa da invasão. O objetivo da detecção de intrusão é identificar as atividades da invasão que já ocorreram ou podem ocorrer em uma rede, quanto mais rápido se tomar conhecimento de um ataque maior são as chances de minimizar os danos que podem ser causados pelo invasor (WANG, 2009).

A metodologia básica para detectar invasores é através de auditoria do sistema, possuindo dois tipos: a auditoria que trabalha com informações estatísticas das configurações, conhecidas como perfis de segurança; e a auditoria que trabalha com eventos do sistema. No primeiro tipo se definem os valores dos parâmetros de segurança, por exemplo, qual é a quantidade de *logins* sem sucesso tolerado, qual é o tamanho mínimo permitido e o tempo de vida de uma senha. No segundo tipo tratam da análise e gravação de eventos que ocorreram no sistema, estes eventos devem conter no mínimo os campos (WANG, 2009):

- sujeito: fornece informações do autor do evento;
- ação: fornece informações das operações realizadas pelo sujeito, por exemplo, abrir um arquivo do sistema;
- objeto: fornece o receptor do evento;
- condições de exceção: fornece uma condição de exceção, por exemplo, uma falha ao abrir o arquivo do sistema;
- uso de recursos: a utilização dos recursos computacionais usados pelo evento, por exemplo, o uso de memória e processamento utilizado;
- marcação de tempo: quanto tempo o evento durou;

Por meio das informações coletadas do sistema é possível fazer a análise dos eventos e comportamentos a fim de detectar a invasão e emitir alarmes. As etapas mais comuns que os sistemas de detecção possuem são (WANG, 2009):

- avaliação: analisa as necessidades de segurança necessárias de um sistema a fim de produzir um perfil de segurança;
- detecção: o sistema de detecção faz a coleta de eventos do uso do sistema e analisa-os a fim de detectar atividades de invasão. Além de coletar informações sobre o comportamento dos usuários o SDI também é capaz de analisar o comportamento de programas, verificando se suas atividades são comuns;
- alarme: faz a emissão de alertas quando um invasor consegue acesso ao sistema.

Um SDI também pode fazer o uso de uma Política de Detecção de Intrusão (PDI) que são usadas para identificar as atividades da invasão, fazendo a especificação de quais dados devem ser protegidos e como eles devem ser protegidos. Na PDI também se pode especificar que tipos de atividades são consideradas de fato uma invasão, e como reagir quando atividades suspeitas são identificadas (WANG, 2009).

Um SDI ideal deve ser simples, eficaz e de fácil implementação, gerando o mínimo de alarmes falsos. Isto é, não deve permitir que o SDI detecte algo normal como anormal (Falso Positivo) ou detecte algo anormal como normal (Falso Negativo). A detecção de falsos positivos e falsos negativos é comum nos SDI, podendo ocorrer de uma competir com a outra. Por exemplo, para reduzir a detecção de Falsos Positivos, pode aceitar atividades como normais, dessa forma a diminuiria os Falsos Positivos, porém aumentaria os Falsos negativos (WANG, 2009).

Segundo SILVA (2003) os sistemas de detecção de intrusão podem ser classificados quanto ao tipo da informação analisada e também em relação ao modo como essas informações coletadas são analisadas. Quanto às informações analisadas, os sistemas podem ser classificados da seguinte forma:

- Sistema de detecção baseado em Rede (SDIR): Os sistemas de detecção baseados em rede (Figura 2) monitoram os pacotes que trafegam na rede, estes sistemas costumam trabalhar com informações de endereçamento, protocolo e portas de aplicação para identificar uma tentativa de invasão. Essas informações são obtidas do cabeçalho dos protocolos que estão contidos nos pacotes, sendo mais rápidas de

analisar. No entanto, alguns sistemas SDI também podem executar a verificação do conteúdo do *payload* do pacote para detectar outros tipos de ataque, SILVA (2003).

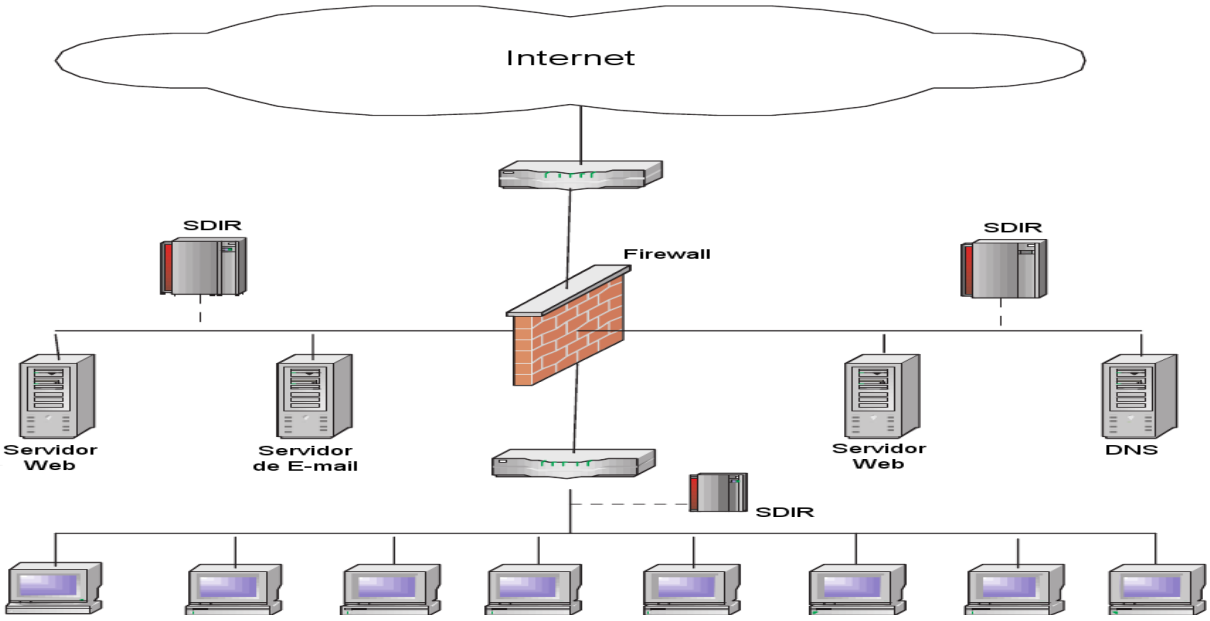

Figura 2: Sistemas de Detecção de Baseados em Rede. (SILVA, J. 2011)

- Sistema de detecção baseado em *Host (SDIH)*: Os sistemas de detecção baseados em *host* (Figura 3) são responsáveis por monitor o comportamento dos sistemas, analisando dados como, por exemplo, arquivos de *log,* chamadas de sistema, dados de equipamentos como firewalls e roteadores, entre outros. Neste tipo de SDI são estudados os eventos internos ao *host,* analisando as informações geradas pela execução de operações no sistema, SILVA (2003).

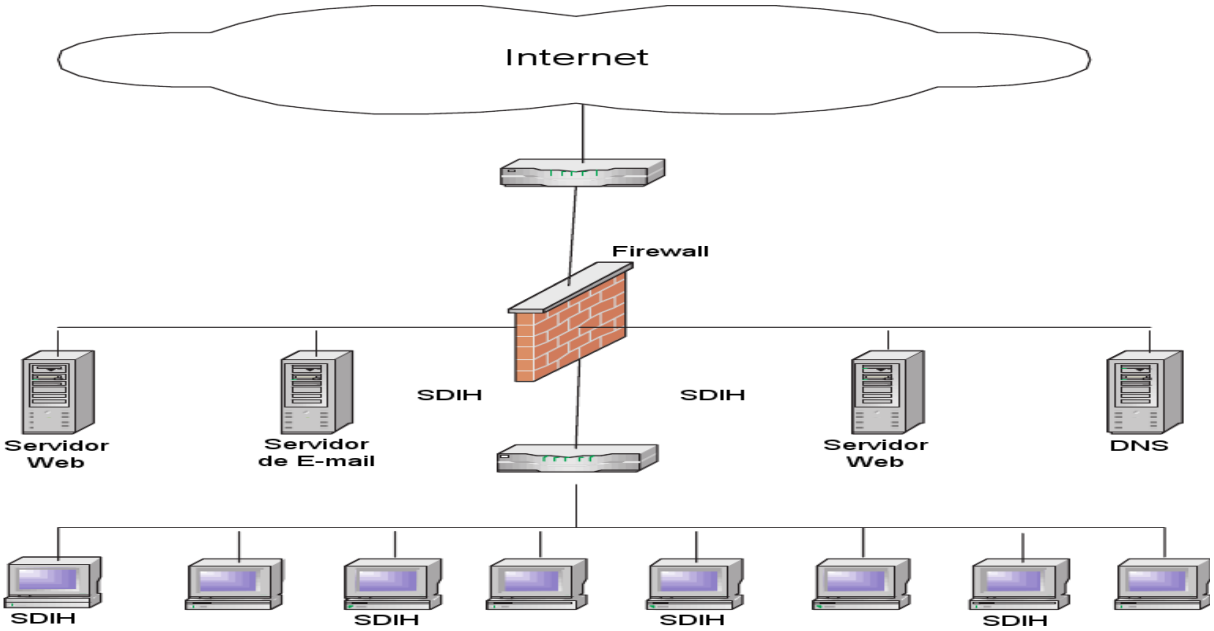

Figura 3: Sistemas de Detecção de Baseados em Host. (SILVA, J, 2011).

- Sistema de detecção Híbrido (SDIH): Os sistemas de detecção híbridos (Figura 4) são sistemas que monitoram tanto os pacotes da rede, quanto as informações dos sistemas, possuindo funcionalidades de ambos SDI citadas anteriormente.

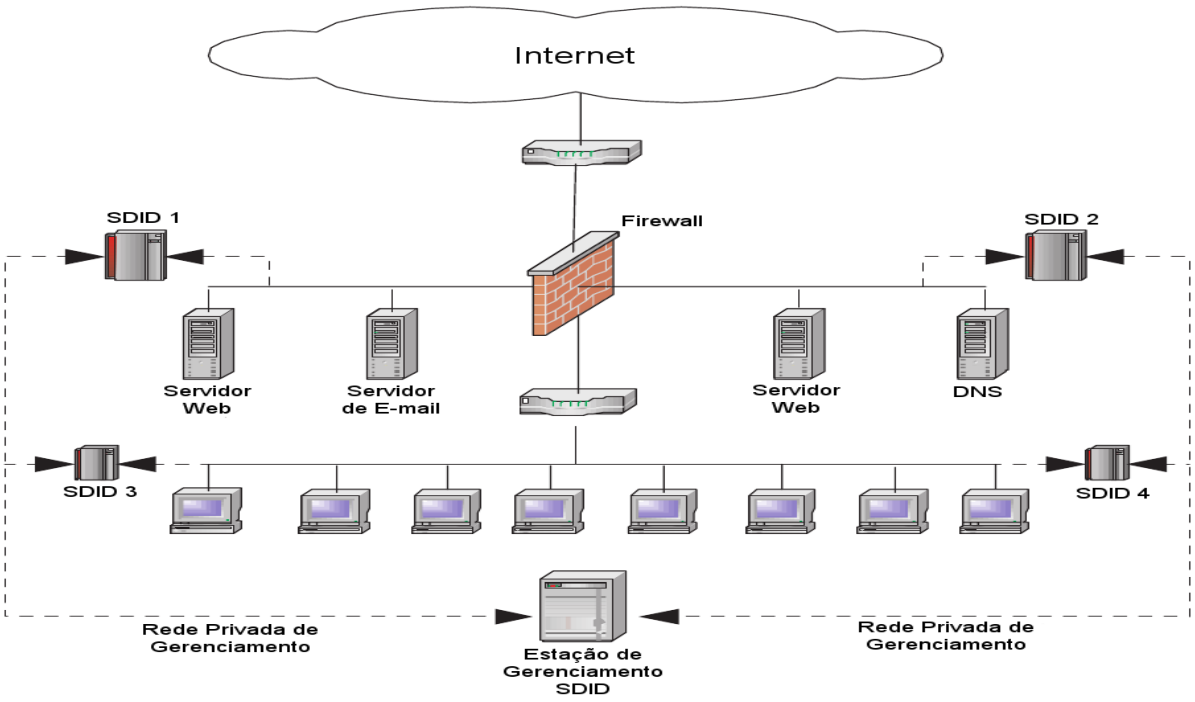

Figura 4: Sistemas de Detecção Híbridos. (SILVA, J, 2011)

Neste trabalho foi utilizado um sistema de detecção de intrusão baseado em *host,* esse tipo de SDI foi escolhido, pois é possível, por exemplo, monitorar qualquer modificação nos arquivos do sistema, ficando mais fácil de determinar o perfil do ataque do invasor.

A ferramenta SDI utilizada foi o Ossec, sendo escolhida por ter suporte à vários sistemas operacionais como Microsoft Windows e UNIX/LINUX utilizados nos testes, além de ser *opensource*. O Ossec possui varias funcionalidades, as principais são (OSSEC, 2012):

- Analise de *logs;*
- Verificação de integridade de arquivos;
- Detecção de *rootkit*;
- Alertas em tempo real e configurável;
- Monitoração dos registros do Windows;
- Interface Web, onde se pode verificar todos os alertas e eventos registrados por ele.

Na próxima seção serão abordados alguns conceitos de virtualização, para melhor entendimento de como foram fornecidos os sistemas operacionais utilizados como *Honeypots*.

2.3 VIRTUALIZAÇÃO

Segundo LAUREANO (2006) o conceito de virtualização ou simplesmente máquinas virtuais (Virtual Machine – VM) é antigo, sendo orginalmente desenvolvidas para centralizar os sistemas de computador utilizados no ambiente VM/370 da IBM. Neste sistema, cada máquina virtual simula uma réplica física da máquina real, fazendo com que os usuários tenham a ilusão de que o sistema está disponível para seu uso exclusivo. A utilização de máquinas virtuais está se

tornando uma vantajosa alternativa para vários sistemas de computação, devido ao custo baixo e portabilidade.

> “De uma perspectiva empresarial, existem muitas razões para utilizar a virtualização, principalmente na camada “Consolidação de Servidores”. Ao virtualizar determinado número de sistemas sub-utilizados em um único servidor físico, você economizará espaço em estrutura física, espaço em disco, refrigeração, energia e centralizará o gerenciamento” (SILVA, C. et al, 2008).

Existem várias vantagens em se utilizar virtualização em sistemas de computação, algumas delas são (SILVA, C. et al(2008):

- Facilita o aperfeiçoamento e testes de novos sistemas operacionais;
- Auxilia no ensino prático de sistemas operacionais, pois permite a execução de vários sistemas para comparação no mesmo equipamento;
- A possibilidade de se executar vários sistemas operacionais no mesmo hardware, simultaneamente;
- Pode simular falhas e alterações no hardware para testes ou reconfiguração de um sistema operacional, provendo confiabilidade e escalabilidade para aplicações;
- Pode se desenvolver novas aplicações para diversas plataformas, garantindo a portabilidade dessas aplicações;
- Diminuições de custos com aquisição de hardware;
- Gerenciamento centralizado e facilitado, migração e replicação de computadores, aplicações ou sistemas operacionais.

Segundo ainda LAUREANO (2006) as técnicas mais utilizadas para virtualização são:

- Virtualização total: Na virtualização total (Figura 5), uma estrutura completa de hardware é virtualizada, com isso o sistema a ser virtualizado (sistema convidado) não sofre nenhum tipo de alteração.

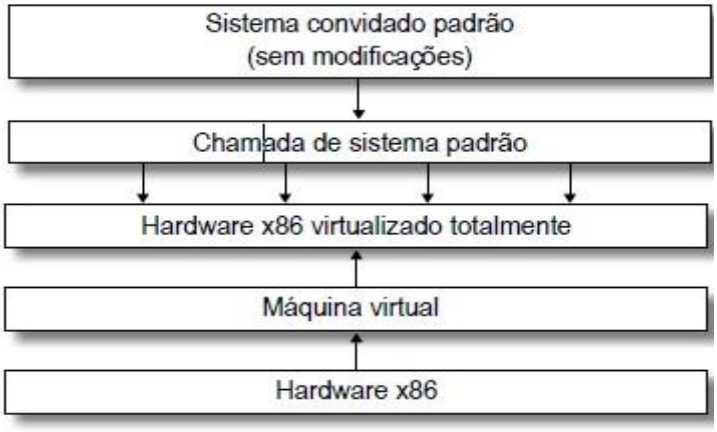

Figura 5: Virtualização total (LAUREANO, 2006)

A principal vantagem de se usar virtualização total é justamente o fato de que o sistema que será virtualização não sofre qualquer tipo de alteração, em compensação, seu funcionamento é mais lento e o monitor de máquinas virtuais precisa implementar alternativas para que as operações privilegiadas possam ser executadas em processadores que não suportem este tipo de virtualização nativamente.

- Paravirtualização: Na paravirtualização (Figura 6), o sistema que será virtualizado (sistema convidado) sofre modificações para que a integração com o monitor de máquinas virtuais seja de fato mais eficiente.

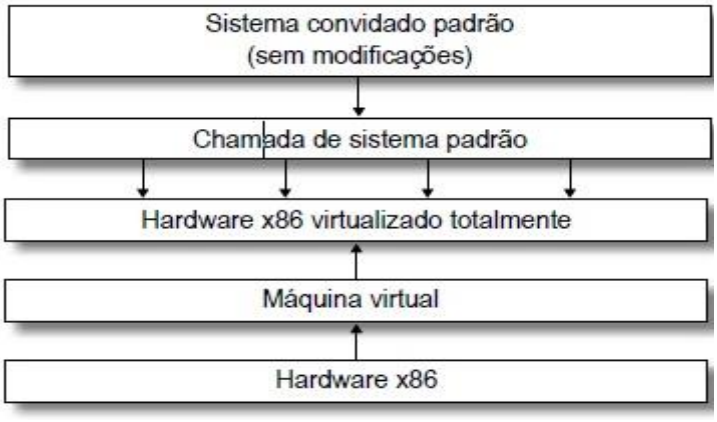

Figura 6: Paravirtualização (LAUREANO, 2006)

Embora a paravirtualização exija que o sistema a ser virtualizado seja de fato modificado, o que consequentemente diminui a portabilidade do sistema, também permite que o sistema convidado acesse diretamente os recursos de hardware. O acesso direto ao hardware é monitorado pelo monitor de máquinas virtuais, que fornece ao sistema convidado todos os “limites” do sistema, por exemplo, endereços de memória que podem ser utilizados e endereçamento em disco.

Com a paravirtualização é possível reduzir a complexidade do desenvolvido das máquinas virtuais, pois, historicamente, os processadores não suportam a virtualização nativa. Uma das vantagens de se utilizar paravirtualização é o ganho com performance, compensando as modificações que serão implementadas nos sistemas convidados LAUREANO (2006).

No presente trabalho foram testadas três softwares de virtualização, sendo elas:

- WMware Workstation: Primeira solução comercial de virtualização para *desktops,* lançada em 1999, ganhadora de mais de 50 prêmios do setor. Possuindo um amplo suporte aos sistemas operacionais atuais. Este software utiliza a técnica de virtualização total (VMWARE, 2012).

- Citrix XenServer: Este software é voltado para virtualização de servidores, atualmente gratuito, para sua utilização basta se cadastrar no site oficial, a licença é valida por 1 ano e deve ser renovada anualmente. (CITRIX, 2012).

- VirtualBox: Software de virtualização gratuito, desenvolvido atualmente pela Oracle (ORACLE, 2012).

O WMware Workstation 9 foi escolhido por apresentar um desempenho superior se comparado ao VirtualBox (MARTINS, 2012). Não foi possível efetuar testes concretos no XenServer devido a incompatibilidade no *hardware* disponível.

Na próxima seção serão abordados os principais conceitos sobre ataques na Internet e suas classificações.

2.4 ATAQUES NA INTERNET

Segundo SHIRLEY (2000), um ataque é uma ação nociva à segurança de um sistema computacional que deriva de uma ameaça inteligente, ou seja, um ato inteligente, sendo essa ameaça uma tentativa delibera de se enganar os serviços de segurança e as políticas de segurança de um sistema.

Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes tipos de alvos e usando técnicas variadas. Qualquer dispositivo conectado à Internet pode ser alvo de um ataque. Existe diversos motivos que levam a um invasor desferir ataques na Internet, Alguns exemplos são (CERT.BR):

- Demonstração de poder: o invasor quer demonstrar suas habilidades para determinada empresa, mostrando que ela pode ser invadida e ter seus serviços suspensos por ele;
- Prestígio: o invasor quer se vangloriar perante outros invasores, por ter conseguido invadir determinado sistema;
- Motivações financeiras: o invasor pode coletar informações confidenciais do usuário com objetivo de aplicar golpes;
- Motivações ideológicas: tornar inacessível ou invadir sites que divulgue conteúdo contraria à sua opinião.
- Motivações comerciais: tornar inacessível um serviço disponibilizado por empresas concorrentes, com intuído de comprometer sua reputação.

Segundo ainda o CERT.BR(2012) os invasores utilizam diversas técnicas para obter sucesso em um ataque, como: exploração de vulnerabilidades, falsificação de e-mail, varreduras de redes, interceptação de tráfego de rede, força bruta, entre outras.

2.4.1 Exploração de vulnerabilidades

Uma vulnerabilidade pode ser definida como uma condição que, quando explorada por um invasor, pode resultar na violação da segurança de um sistema computacional. Este tipo de ataque ocorre quando o invasor utiliza uma vulnerabilidade, com intuito de executar ações maliciosas, invadir sistemas, acessar informações confidenciais, utilizar o computador invadido para disparar ataques a outros computadores ou paralisar os serviços fornecidos. Exemplos de vulnerabilidade são falhas no desenvolvimento de software, a má configuração de algum equipamento da rede (CERT.BR, 2012).

No presente trabalho foram utilizados sistemas operacionais defasados nos *Honeypots*, com diversas vulnerabilidades conhecidas, além de fornecer serviços com senhas fáceis, com intuito de facilitar ao máximo para o invasor.

2.4.2 Varreduras em redes

As varreduras em redes é uma técnica que consiste em efetuar uma busca minuciosa em uma rede, identificando os computadores ativos a fim de coletar informações sobre ele como, por exemplo, quais serviços estão sendo disponibilizados e quais programas instalados. A partir dessas informações coletadas é possível fazer uma associação entre possíveis vulnerabilidades dos serviços disponibilizados e dos programas instalados nos computadores ativos. A varredura e a exploração das vulnerabilidades podem ser usadas da seguinte forma (CERT.BR, 2012):

- Legítima: são executadas por pessoas autorizadas, com intuito de verificar a segurança dos computadores e das redes, assim, podendo tomar medidas corretivas e preventivas ao se detectar uma vulnerabilidade.
- Maliciosa: são executadas por invasores, estes utilizam as vulnerabilidades encontradas para a execução de atividades maliciosas

nos serviços e programas instalados. O invasor também pode fazer o uso de um computador ativo para propagar códigos maliciosos e deferir ataques de força bruta.

Está técnica é amplamente utilizada pelos invasores, onde é possível obter diversas informações que podem facilitar no comprometimento de um sistema.

2.4.3 Falsificação de *e-mail (E-mail spoofing)*

A falsificação de *e-mail* é uma técnica que permite alterar campos do cabeçalho de um *e-mail,* com intuito de aparentar que este foi enviado por uma determinada origem quando, na verdade, foi enviado de outra. Estes ataques são bastante utilizados para propagação de códigos maliciosos, envio de *spam* e fraudes eletrônicas*.* Os invasores utilizam os endereços de *e-mail* coletados de computadores infectados para enviar mensagens e fazer com que seus destinatários acreditem que elas vieram de pessoas conhecidas por elas (CERT.BR, 2012).

2.4.4 Interceptação de tráfego de rede (*Sniffing*)

A interceptação de tráfego de rede é uma técnica que consiste em capturar todos os pacotes que trafegam em uma rede, utilizando programas específicos conhecidos como *sniffers.* Esta técnica pode ser usada de duas formas (CERT.BR, 2012):

- Legítima: são executadas por administradores de rede, a fim de detectar problemas, analisar desempenho e monitorar atividades maliciosas referentes aos computadores ou a rede.
- Maliciosa: são executadas por invasores, com intuito de capturar informações privilegiadas, como, por exemplo, senhas, números de

cartão de credito, ou qualquer outro tipo de informações que esteja trafegando na rede sem criptografia.

Alguns exemplos de programas *sniffers* são: *Wireshark*, *Microsoft Network Monitor*, *Capsa Packet Sniffer, NetworkMiner, SniffPass*. Dentre estas opções o que mais se destaca é o Wireshark (WIRESHARK, 2012), devido a sua popularidade, suporte a diferentes sistemas operacionais e por possuir uma grande variedade de filtros podendo, por exemplo, filtrar os pacotes de apenas de um computador ou de um determinado protocolo.

2.4.5 Força bruta (*Brute force*)

Um ataque de força bruta consiste em adivinhar, por tentativa e erro, o *login* e a senha de um determinado usuário, com isso poder utilizar sites, computadores e serviços. Qualquer equipamento conectado a Internet que utiliza um *login* e uma senha pode ser vítima de um ataque de força bruta, caso o invasor consiga ambos ele pode efetuar ações maliciosas como, por exemplo (CERT.BR, 2012):

- trocar a senha, dificultando que a vítima tenha acesso a determinado site ou computador invadido;
- ter acesso ao serviço de *e-mail* utilizado pela vítima, obtendo acesso ao conteúdo das mensagens e à lista de contato, além disso, o invasor pode enviar mensagens se passando pela vítima;

Mesmo que o invasor não consiga a senha, a vítima pode ter problemas para acessar sua conta novamente, pois geralmente muitos sistemas bloqueiam as contas após múltiplas tentativas de acesso sem sucesso. Os ataques de força podem ser realizados manualmente ou por meio de ferramentas automatizada, que podem ser facilmente encontradas na Internet (CERT.BR, 2012).

2.4.6 Negação de serviço (DoS ou DDoS)

Um ataque de negação de serviço ou DoS (Denial of Service), é uma técnica que permite ao invasor tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando este ataque é realizado de forma distribuída, ou seja, quando vários computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service). Esse tipo de ataque não tem objetivo de invadir ou coletar informações, mais sim exaurir os recursos computacionais e causar indisponibilidade ao alvo (CERT.BR, 2012).

2.4.7 Vírus e *Worm*

Vírus é um programa ou parte de um programa de computador, geralmente com objetivos maliciosos. O vírus se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para que um vírus se torne ativo dando continuidade ao processo de infecção, é necessário que seja executado um computador hospedeiro. A propagação desse tipo de praga virtual, geralmente acontecia através da utilização de disquetes, com o tempo estes tipos de mídias caíram em desuso, forçando aos invasores a criar novas maneiras de propagação, por exemplo, o envio de *e-mail.* Os vírus podem executar diversas atividades sem o conhecimento do usuário (CERT.BR, 2012).

O *worm é* um programa que tem a capacidade de se propagar automaticamente pelas redes, enviando cópias de se para outros computadores. Diferente do vírus, a propagação de o *worm* não é feita inserindo cópias de si mesmo em outros programas ou arquivos, mais sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidade existente em algum programa instalado, essa propagação pode afetar o desempenho de redes e a utilização dos computadores (CERT.BR, 2012).

2.4.8 *Bot* e *botnets*

Um programa *bot* dispõe de mecanismos de comunicação com o invasor, permitindo que ele consiga controlar um computador remotamente. A sua propagação é similar ao do *worm,* ou seja, tem a capacidade de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados. Um computador infectado por um *bot* é chamado de zumbi (*zumbie computer),* pois pode ser controlado pelo invasor remotamente, sem o conhecimento do usuário. Uma rede formada por centenas ou milhares de *bots* é denominada de *Botnet,* essa rede potencializa os possíveis danos causados pelos *bots.*

Algumas ações maliciosas que costumam ser executadas através de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos, coletar informações de uma grande quantidade de computadores, enviar *spam* e camuflar a real identidade do invasor (CERT.BR, 2012).

2.4.9 *Backdoor &* Cavalo de Tróia

O cavalo de Tróia é um programa é um programa *backdoor* (porta dos fundos) que permite ao invasor retornar a um computador após o tê-lo comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído a partir das ações de outros códigos maliciosos, que tenham previamente infectado o computador, ou por invasores que exploram vulnerabilidades existentes nos programas instalados. Após ser inserido, o *backdoor* garante o acesso futuro ao computador comprometido, permitindo assim controla-lo remotamente. Há casos em que fabricantes de programas, incluíram *backdoors* propositalmente, sob alegação de necessidades administrativas (CERT.BR, 2012).

2.4.10 Rootkit

Rootkit é um conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de um código maliciosos em um computador comprometido. Os *rootkits* podem ser usados para (CERT.BR, 2012):

- apagar rastros do invasor;
- instalar códigos maliciosos
- ocultar informações e atividades, como arquivos, diretórios, processos, chaves de registro, conexões de rede, entre outras;
- fazer o mapeamento de vulnerabilidades em outros computadores;
- capturar informações da rede, interceptando o tráfego.

Os *rootkis* não são utilizados para obter acesso privilegiado a um computador, mais para mantê-los. Os invasores utilizam desta técnica, pois assim, não precisariam recorrer novamente aos métodos utilizados na invasão.

2.5 CLASSIFICAÇÕES DE ATAQUES

Para auxiliar na compreensão dos riscos de ataque que os sistemas digitais estão expostos, é necessário classificar estes ataques conforme seu objetivo, origem e severidade, (RAVANELLO; HIJAZI; MAZZORANA, 2004).

2.5.1 Classificação de ataques conforme objetivo

Nessa classificação o invasor pode ter dois objetivos, por exemplo, roubar informações (ataque passivo) ou causar algum dano ao sistema (ataque ativo).

No ataque passivo o invasor está interessado em obter informações de um sistema, o invasor passivo não tem interesse em danifica-lo. Furtos de senhas de endereços de e-mails, fraude bancária e esquemas de desvio de dinheiro, espionável digital, todas estas práticas são características de um invasor passivo. (RAVANELLO; HIJAZI; MAZZORANA, 2004).

No ataque ativo o invasor tem o proposito afetar o funcionamento do sistema, seja através de paralização ou desativação dos serviços críticos em servidores, comprometimentos das informações armazenadas, consumo elevado de recursos computacionais, destruição de informações e ate mesmo o comprometimento físico dos recursos de um sistema (RAVANELLO; HIJAZI; MAZZORANA, 2004).

2.5.2 Classificação de ataques conforme a origem

Nessa classificação o invasor pode vir de duas direções, por exemplo, ataque vindo externamente pela Internet (ataque externo) ou vindos de rede local (ataque interno).

O ataque interno refere-se aos ataques nas quais o invasor está dentro do perímetro da rede de uma organização. Qualquer tipo de abuso ou mau uso dos recursos computacionais pode ser considerado ataque interno. Geralmente são realizados por funcionários que buscam informações privilegiadas (RAVANELLO; HIJAZI; MAZZORANA, 2004).

Já os ataques externos são qualquer tipo de atividade nociva ao funcionamento dos recursos computacionais que partam do perímetro externo da rede. Podemos considerar a Internet como a principal origem dos ataques externos a um sistema computacional. No entanto, em uma rede corporativa, por exemplo, á existência de diversos perímetros de rede, um ataque vindo de outros setores também pode ser considerado como um ataque externo, mesmo estando na mesma rede física (RAVANELLO; HIJAZI; MAZZORANA, 2004).

2.5.3 Classificação de ataques conforme a severidade

Segundo RAVANELLO; HIJAZI; MAZZORANA (2004), outra forma de se classificar um ataque é medindo o dano causado pelo invasor ao sistema. A severidade é determinada conforme o tempo gasto na recuperação e prejuízo que o

ataque conseguiu causar ao sistema. O grau de severidade não é uma informação quantitativa e sim qualitativa, diretamente ligada ao objetivo principal da entidade atacada, esse grau pode variar de acordo com a entidade, por exemplo, um ataque pode ser classificado de baixa severidade em uma entendida e ser de severidade critica para outra. O administrador de sistemas durante a construção da política de segurança deve determinar quais tipos de ataques devem se encaixar em qual grau de severidade. Durante este processo de criação o administrador deve responder as seguintes perguntas:

- Qual o objetivo do sistema em relação ao negócio da entidade?
- Quanto tempo á entidade pode funcionar caso ocorra a paralização dos serviços?
- De todos os serviços disponíveis, quais são os mais importantes perante os objetivos da entidade?

Com essas informações é possível determinar quais são as prioridades no caso de ocorrer falhas múltiplas, a fim de contabilizar os dados sofridos com o ataque. Severidade pode ser medida conforme abaixo, (RAVANELLO; HIJAZI; MAZZORANA, 2004):

- Baixa severidade: Ataques de baixa severidade são aqueles não atrapalham o funcionamento de uma empresa. Também pode ser considerado de baixa severidade ataques cujos danos causados podem ser rapidamente reparados, causando pouco ou nenhum impacto para empresa.
- Alta severidade: Ataques de alta severidade são aqueles que no geral, dificultam o funcionamento de uma empresa fazendo-a gastar tempo e recursos para seu reparo. Uma empresa vítima de uma epidemia de vírus em sua rede, causando a interrupção de alguns serviços são considerados eventos de alta severidade.

2.6 *FIREWALL*

Segundo KUROSE (2010) um firewall é a combinação de hardware e software responsável pelo isolamento de uma rede interna da Internet em geral, permitindo ou bloqueando pacotes. Um firewall permite que um administrador de rede controle o acesso entre a rede interna com a rede externa e vice versa e os recursos da que da rede que administra gerenciando todo o fluxo de tráfego de e para esses recursos.

O primeiro firewall do mundo foi desenvolvido pela empresa Bell Labs em meados dos anos 80, encomendado pela gigante das telecomunicações AT&T, com intuito de “filtrar” todos os pacotes que entrasse ou saísse de sua rede, de modo a manipulá-los conforme as regras definidas pelos cientistas da Bell, mesmo com a evolução dos meios tecnológicos, o firewall ainda possui os mesmos conceitos desenvolvidos pela Bell. O que antes era classificado como apenas sendo um “filtro de pacotes” ganhou algumas classes, passando a ser exposto da seguinte forma, (NETO, 2004):

- Firewall filtro de pacote: Está classe de firewall é responsável por filtrar todo o trafego direcionado ao próprio firewall ou a rede que ele isola. Este filtro ocorre mediante a análise das regras definidas pelo administrador. O filtro de pacotes realiza a análise dos cabeçalhos dos pacotes chamados de Headers, enquanto trafegam na rede. Através dessa análise é possível decidir o destino de cada pacote, a filtragem pode deixa-lo trafegar normalmente na rede ou parar a sua trajetória ignorando-o por completo, (NETO, 2004).
- Firewall NAT: Está classe de firewall, tem como objetivo manipular a rota padrão dos pacotes que atravessam o firewall, aplicando o conceito de “tradução de endereço”. Dentre suas funcionalidades o firewall NAT tem a capacidade de manipular o endereço de origem e o destino dos pacotes, (NETO, 2004).

- Firewall híbrido: Está classe de firewall agrega para si as funções de filtragem de pacotes e NAT. Tratando-se, da união de ambas as classes e não somente uma classe isolada com propriedades próprias. Com o

> passar dos anos na prática pode-se observar que foram agregadas novas funções aos firewalls, destoando do projeto original da Bell Labs, (NETO, 2004).

Segundo ainda NETO (2004) o *firewall* de filtro de pacotes é o mais utilizado "não aplicar seus conceitos é deixar as portas abertas e permitir a livre circulação de pacotes não confiáveis por sua rede".

2.7 *HONEYPOTS* E *HONEYNETS*

O primeiro relato do uso de um sistema de acompanhamento de invasão ocorreu em 1988, naquela época Clifford Stoll relatou um ataque sofrido a LBL (Lawrence Berkely Laboratory). Nesta invasão a LBL, ao invés de bloquear o intruso, Stoll juntamente com sua equipe decidiram permitir o acesso ao sistema enquanto monitoravam todas as atividades do invasor até que sua origem fosse descoberta, o acompanhamento dessa invasão durou cerca de um ano, com o resultado das informações coletadas foi possível identificar quais objetivos e motivações, e quais redes tinham sido comprometidas e quais redes o invasor estava interessado em atacar (BARBATO, 2005).

Em 1992, Bill Cheswick fez a publicação de um artigo descrevendo o acompanhamento de uma invasão que ocorreu no Laboratório Bell da AT&T em 1991. O objetivo dessa monitoração era descobrir quem era o invasor; qual origem e frequência do ataque e que tipo de vulnerabilidade era explorada, este acompanhamento durou alguns meses (BARBATO, 2005).

O uso dos termos *Honeypots* e *Honeynets* são novos, com pouco mais de 15 anos, antes disso não se tinha uma definição correta, geralmente cada autor propunha uma abordagem diferente.

Segundo BARBATO(2005) em 17 de maio de 2002, Lance Spitzner definiu claramente o conceito de *Honeypot* como sendo "Um recurso de segurança preparado para ser sondado, atacado e comprometido".

> “os honeypots e honeynets podem ser considerados ambientes de monitoramento de ataques. Diferentes estruturas podem ser construídas na captura de ataques, as quais dependem de diversos fatores tais como o que se deseja monitorar e quis os tipos de informações que se espera obter” (ANDRUCIOLI, 2005).

Segundo BELCHIOR et al (2004) uma *Honeynet* é uma rede projetada para ser comprometida, a fim de obter informações sobre o comportamento, táticas e ferramentas utilizadas pelo invasor.

2.8 REPRESENTATIVIDADE DE *HONEYPOTS* E *HONEYNEYS*

Na Figura 7 é representado o uso de *Honeypots* em uma rede mista, composta por rede wireless, conexão com a Internet e um servidor VMware responsável pelo emulação dos serviços.

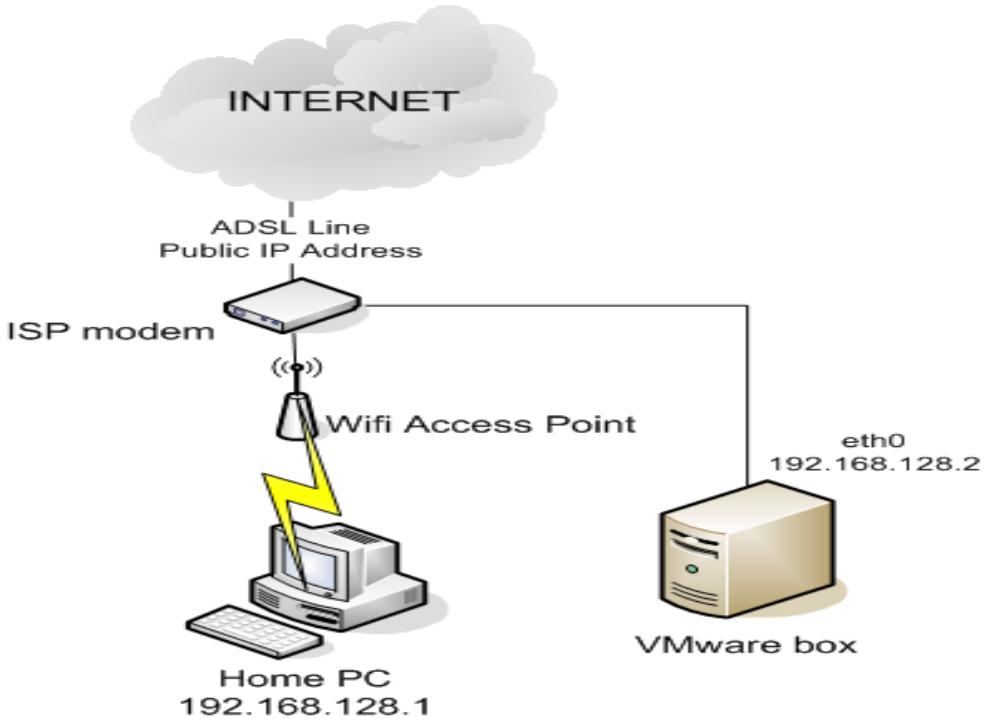

Figura 7: Representatividade de um Honeypot. Obtido em (The Honeynet Project 2012)

Na Figura 8 é representada uma *Honeynet,* onde todos os *logs* gerados pelos *Honeypots* são encaminhados para o servidor, que é responsável de armazenar as informações coletadas e posteriormente realizar a auditoria destas.

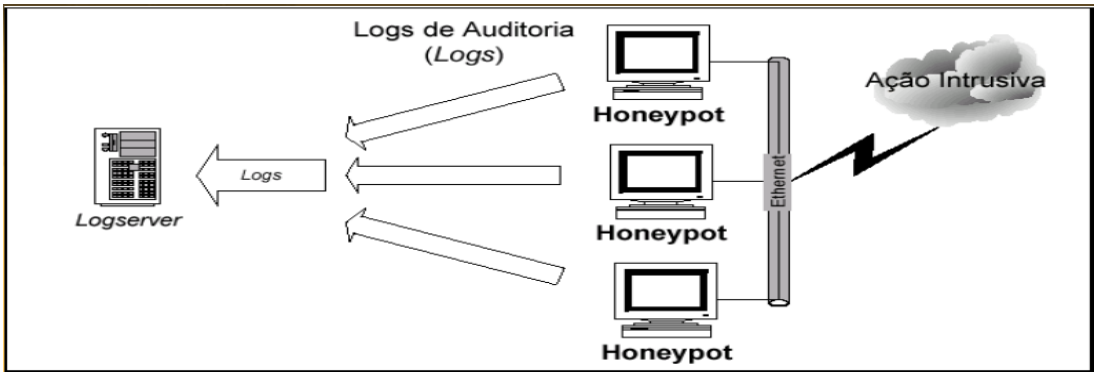

Figura 8: Representatividade de uma *Honeynet.* Obtido em (The *Honeynet* Project, 2012)

As *Honeynets* são dividas em dois tipos (CERT.BR 2012):

- *Honeynet* real: neste tipo de *Honeynet* (Figura 9) todos os componentes, incluindo os *Honeypots*, mecanismos de contenção, sistemas de alertas, são físicos, ou seja, é formada por diversos computadores. As principais vantagens de se utilizar este tipo são: baixo custo por dispositivo; como se trata de um sistema distribuído é tolerante a falhas; em contrapartida, a sua manutenção é difícil e trabalhosa, necessitando de muito espaço físico para os equipamentos.

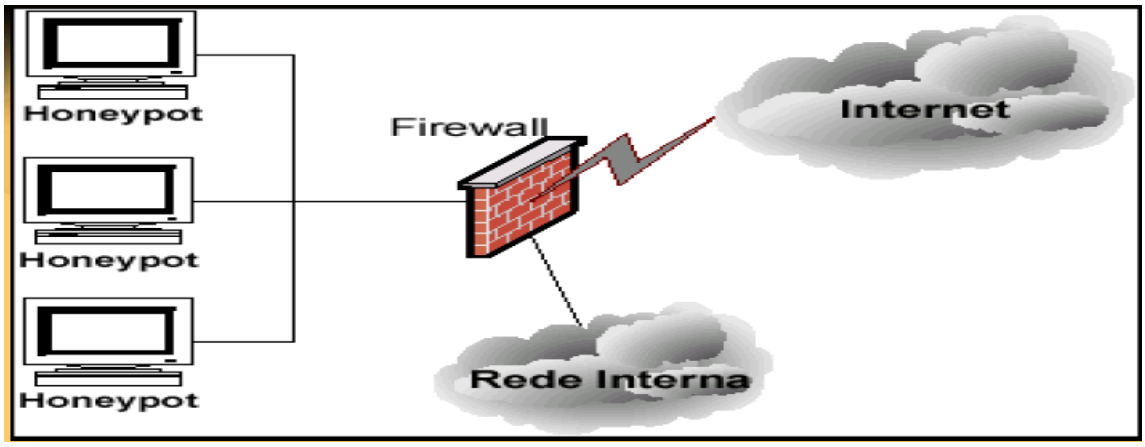

Figura 9: *Honeynet* Real. Obtido em (The Honeypot Project, 2012)

A Figura 9 faz a representatividade de um Honeynet real, onde cada componente é de fato físico, ou seja, os Honeypots e o firewall são computadores individuais.

- *Honeynet* virtual: na *Honeynet* virtual (Figura 10) todos os serviços são virtualizados, reduzindo o número de dispositivos físicos. Geralmente sua instalação é feita em um único computador com um sistema operacional instalado, servindo de base para a execução do *software* responsável pela virtualização. As principais vantagens de se utilizar este tipo de *Honeynet* são: manutenção simples e centralizada, custo baixo, diminuição de dispositivos físicos, em contrapartida, o *software* de virtualização pode limitar o uso do *hardware*, podendo causar uma diminuição de desempenho.

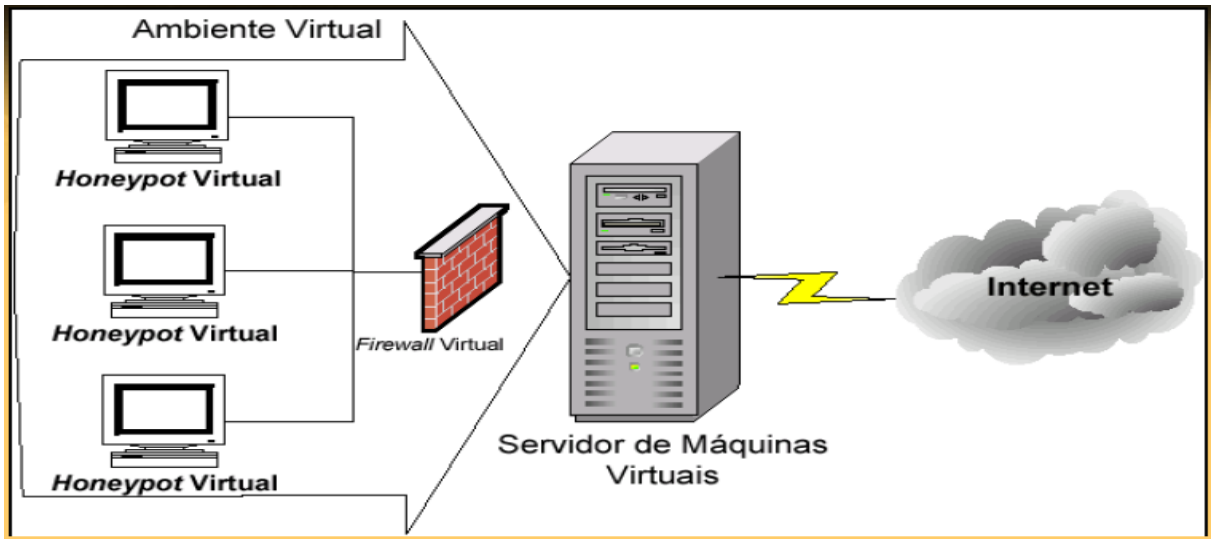

Figura 10: Honeynet virtual. Obtido em (The Honeynet Project, 2012)

A Figura 10 faz a representação de uma *Honeynet* virtual sendo composta por um servidor que fará o gerenciamento das máquinas virtuais, e os *Honeypots* que são responsáveis por capturar as ações dos invasores, nesta representação utilizou-se de um *firewall*.

2.9 NÍVEIS DE INTERAÇÃO

Os *Honeypots* podem ser classificados por níveis de interação, segundo ANDRUCIOLI (2005) este nível é equivalente ao grau de interação do invasor com o sistema comprometido, sendo dividido em três níveis: baixa, média e alta interação.

Os *Honeypots* de baixa interação são normalmente fáceis de instalar, configurar, implantar e manter, devido a sua simplicidade, além de gerar mínimo de risco a rede. Os *Honeypots* de baixa interação fazem a emulação de serviços reais, limitando o atacante apenas nos serviços predeterminados. Geralmente eles envolvem a instalação de softwares, que serão responsáveis pela emulação dos serviços e sistemas operacionais. A principal desvantagem desse tipo é que as informações coletadas são limitadas além de ser facilmente detectado pelo invasor (SPITZNER 2002).

Nos *Honeypots* de média interação, a interação com o invasor se torna maior, mesmo assim não é equivalente a um sistema real, quando se aumenta o nível de interação os riscos também são aumentados, exigindo um maior cuidado em relação as ferramentas de *scripts* que fazem a interação com invasor. Ele possui similaridade com o de baixa interação, a principal diferença entre os dois é que no de média interação há mais detalhes, simulando assim melhor o ambiente falso (MARCELO e ALVES, 2003).

Os *Honeypots* de alta interação são extremamente difíceis de construir e manter, havendo um alto risco em utilizá-los. Seu objetivo é dar ao atacante acesso total aos serviços e ao sistema operacional real, sendo um sistema real nenhum dos serviços disponibilizados são emulados. Uma vez que invasor tem acesso ao *Honeypot*, ele tem um sistema operacional para interagir, dando-lhes a capacidade de fazer o que quiser (SPITZNER 2002).

No presente trabalho foi utilizado *Honeypots* de alta interação, devido ao fato de neste tipo de Honeypot o invasor tem total acesso ao sistema, podendo assim determinar mais facilmente o perfil do ataque do invasor.

2.10 CLASSIFICAÇÃO

2.10.1 Honeypots de pesquisa

Honeypots de pesquisa oferecem uma plataforma voltada ao estudo, nas quais o objetivo é compreender a comunidade hacker, não apenas estudar ferramentas utilizadas na invasão, mais sim obter informações importantes como: qual ferramenta utilizada para testar o sistema, qual exploit utilizado para comprometê-lo e cada tecla utilizada após a invasão (SOUZA, 2005).

2.10.2 Honeypots de Produção

Segundo SPTIZNER (2002), este tipo de *Honeypot* tem sido utilizado mais do que o de pesquisa, devido à facilidade de implementação, apesar de possuir funcionalidades limitadas e não armazenarem as informações sobre as ações do atacante. O principal objetivo desse tipo de *Honeypot* é diminuir ao máximo a incidência de riscos a uma rede.

Uma clássica definição sobre *Honeypots* de produção segundo SOUZA (2005):

> "são sistemas que aumentam a segurança de uma organização em especifico e ajuda a mitigar riscos. São fáceis de construir porque requerem menos funcionalidades. Usualmente possuem as mesmas configurações que a rede de produção e transportam para ela todo o aprendizado obtido com os ataques sofridos" (Souza, 2005).

Após identificar o ataque, é necessário coletar evidencias de como o invasor obteve acesso ao sistema, qual a origem do ataque, e com isso fazer o encaminhamento das evidencias as autoridades responsáveis, SOUSA (2005).

2.11 LEGALIDADE DOS HONEYPOTS

Segundo SPITZNER (2002) *Honeypots* são tecnologias novas e ainda emergentes para comunidade de segurança. Muitos profissionais de segurança ainda desconhecem ou estão apenas agora começando a entender o que são *Honeypots*, seus tipos, como funcionam, e o seu valor. Como acontece com muitas tecnologias novas, não é apenas os profissionais tentando aprender sobre elas, mais também a comunidade jurídica. À medida que *Honeypots* se tornaram populares, as pessoas começaram a se perguntar o que questões jurídicas poderiam aplicar.

Os *Honeypots* possuem três principais questões que são comumente discutidas: armadinha, privacidade, responsabilidade (SPITZNER, 2002):

- armadilha: coagir ou induzir uma pessoa a fazer algo que normalmente não faria, ou seja, instigar a prática de um delito é crime o que pode ocasionar processo judicial. A utilização de *Honeypots* não induz ninguém, os ataques são por iniciativa do invasor.
- privacidade: o sistema invadido não pertence ao invasor, portanto a monitoração do mesmo não pode ser caracterizada como quebra de privacidade.
- responsabilidade: após o seu comprometimento o *Honeypot* deve ser desativado suspendendo todos os seus serviços e bloqueando o invasor, pois ele não pode de hipótese alguma ser usado para prejudicar outras redes, podendo ocasionar processo civil.

A vantagem na legalidade do uso de *Honeypots* é que após uma invasão, as informações coletadas podem ser utilizadas como prova confiável de um crime digital.

3. METODOLOGIA

O presente trabalho efetuou a análise de um conjunto de três *Honeypots* de alta interação e um servidor responsável por coletar os *logs* gerados pelo SDIH Ossec (OSSEC, 2012), ambos instalados em máquinas virtuais, formando assim uma *Honeynet* virtual. Em cada *Honeypot* foram instalados sistemas operacionais diferentes e com versões já defasadas. Segundo ASSUNÇÃO (2009), a instalação de diferentes sistemas operacionais e serviços torna a *Honeynet* mais atrativa aos invasores.

Os sistemas operacionais escolhidos para utilização na *Honeynet* foram: GNU/Linux Debian 5 Lenny, Microsoft Windows XP SP2 e Microsoft Windows Server 2003 Enterprise Edition. A escolha destes sistemas operacionais já defasados foi intencional, pois possuem diversas vulnerabilidades conhecidas que podem ser exploradas, o que aumenta ainda mais o poder de atração dos *Honeypots* perante aos invasores. No servidor de *logs* foi utilizada a versão atual da distribuição Linux Debian 6.0.6 Squeeze. Segundo MORIMOTO (2009), a distribuição Debian é madura e segura, sendo líder em ambientes de produção e servidores.

Para o experimento foi utilizado um microcomputador com as seguintes características: Processador Intel Pentium Dual Core 2.6GHZ, com 4 GB de memória RAM DDR2, com 1 interface de rede 10/100 Mbps, com Disco Rígido de 500 GB e como sistema operacional padrão o Microsoft Windows XP SP3.

Atualmente existem diversas opções de virtualização, tanto para o uso em *desktops* quanto voltados a servidores. O software de virtualização utilizado foi o VMware Workstation 9 (VMWARE, 2012) por causa de suas características citadas no referencial teórico. O VMware é um software proprietário, porém é possível utilizar todas as suas funcionalidades por um período de 30 dias, após cadastro no *site* (VMWARE, 2012).

Na próxima seção será apresentada toda a estrutura criada para a utilização da *Honeynet.*

3.1 CONFIGURAÇÃO E INSTALAÇÃO DA HONEYNET

Após a instalação do software de virtualização, foram instalados os sistemas operacionais, configurando os serviços conforme exibido na Figura 11.

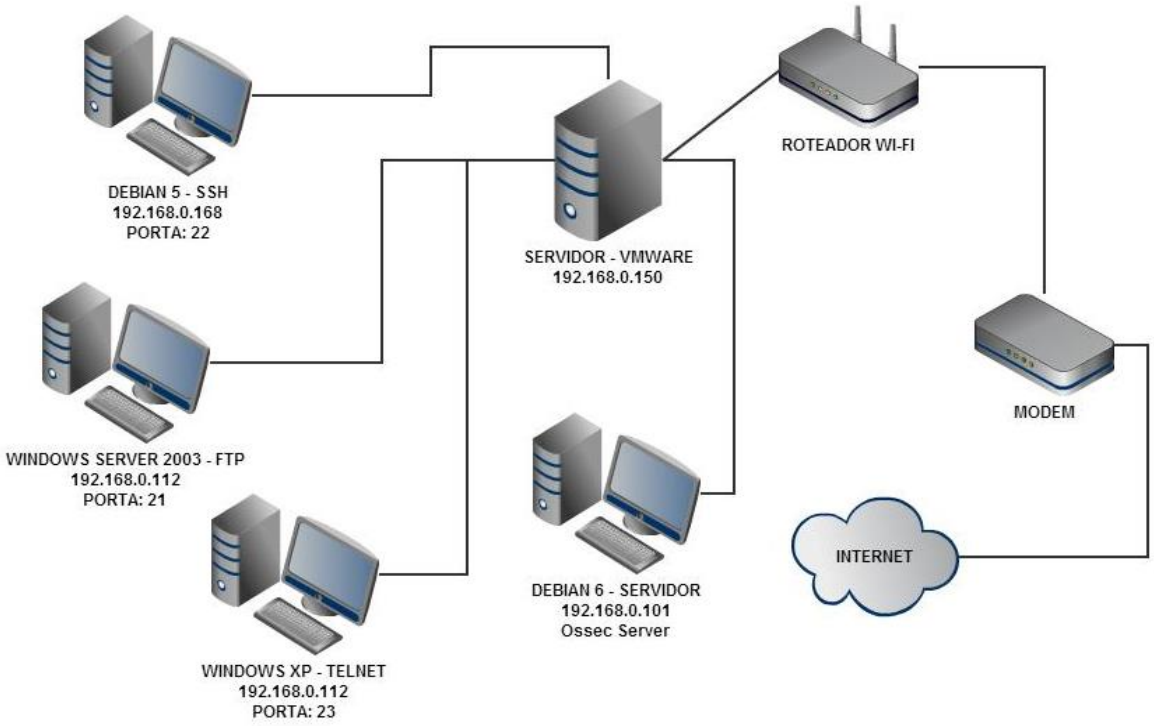

Figura 11: Representatividade da Honeynet (Elaborada pelo autor)

Como exibido na Figura 11, foram virtualizados quatro sistemas operacionais, sendo três *Honeypots* e um servidor que será responsável pela coleta de *logs* gerados pelo sistema de detecção de intrusão (Ossec). Em cada *Honeypot* foi disponibilizado um serviço diferente, ficando da seguinte forma:

- Microsoft Windows XP: TELNET, serviço de acesso remoto, utilizando a porta 23, usuário: admim e senha: 1234.
- Debian 5 Lenny: SSH, possui a mesma função que o TELNET porém é seguro pois utiliza criptografia, utilizando porta 22, usuário: root e senha 1234.

- Microsoft Windows Server 2003: FTP, protocolo utilizado para transferência de arquivos, usando porta 21, usuário: admin e senha: 1234.

A utilização de usuários padrões e senhas fracas foi com o propósito de facilitar sua descoberta pelos invasores, tanto na forma de testes manuais ou de programas com força bruta. Para que os *Honepots* ficassem acessíveis na Internet, foi necessário liberar e redirecionar as portas no roteador (21, 22 e 23) aos respectivos IPs dos *Honeypots* conforme exibido na figura 12.

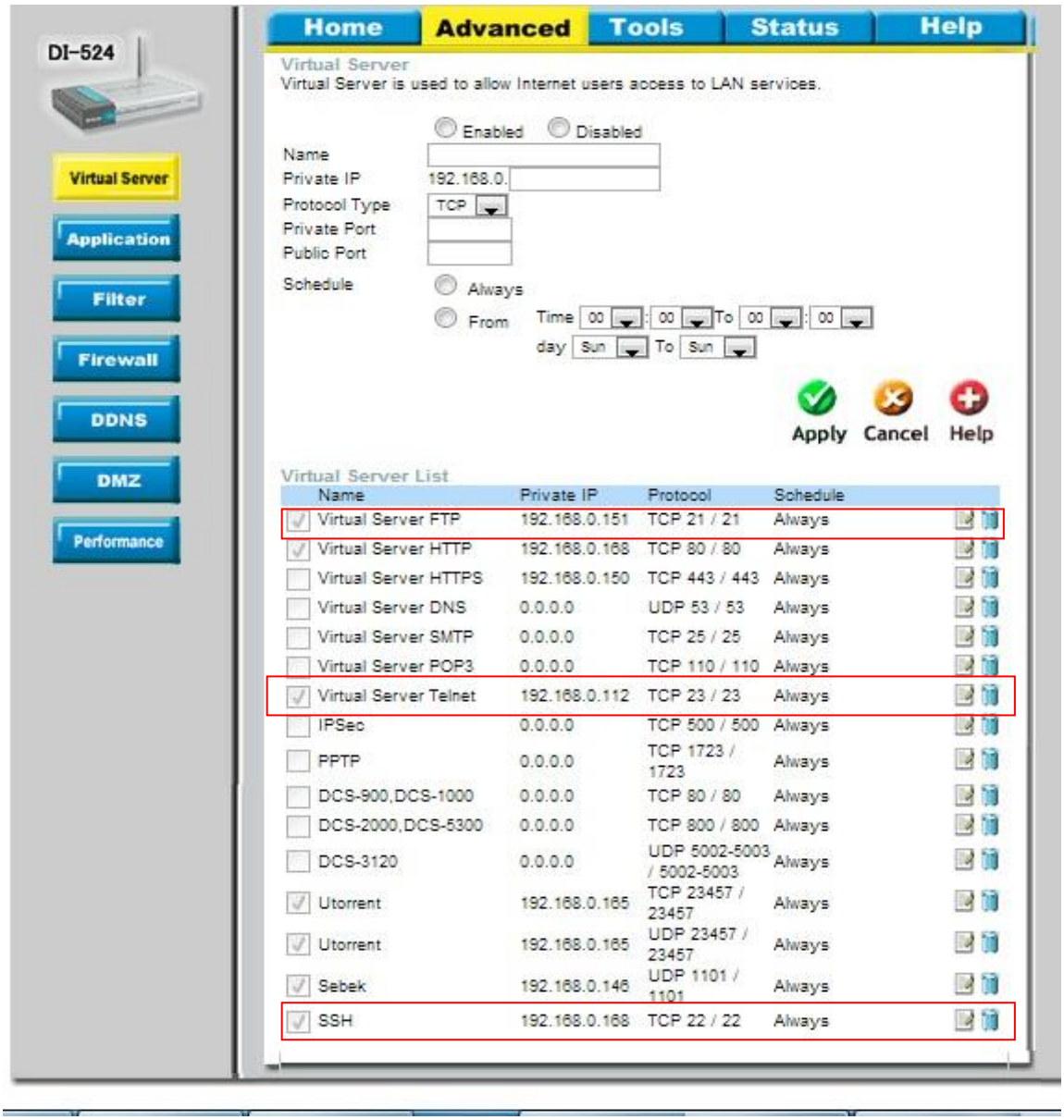

Figura 12: Liberação de portas no roteador D'Link 524

Nos sistemas operacionais Microsoft a escolha dos serviços FTP e TELNET se deram, pois ambos os serviços são nativos do sistema operacional, não sendo necessária a instalação de outro software para fornecê-los, fornecendo assim um ambiente similar ao de uma instalação padrão de um usuário da Internet. Já no sistema operacional Debian a escolha do serviço SSH se deu, pois, além de se um dos serviços mais comuns em ambientes GNU/Linux, também fornece possibilidades de ter acesso total ao sistema, podendo o invasor: acessar diretórios, instalar programas, adicionar ou excluir usuários, apagar arquivos, entre outros.

A distribuição de recursos computacionais nas máquinas virtuais, como memória e disco rígido ficou da seguinte forma:

- Microsoft Windows XP: 512 MB memória RAM, 20 GB de disco rígido;
- Microsoft Windows Server 2003: 512 MB de memória RAM, 20 GB de disco rígido;
- Debian 5 Lenny: 512 MB de memória RAM, 20 GB de disco rígido;
- Debian 6 (servidor): 512 MB de memória RAM, 20 GB de disco rígido.

Não foi utilizado nenhum tipo de *firewall* ou sistema de contenção, com intuito de não impor nenhum tipo de restrição ou dificuldade ao invasor. Porém foi necessária a utilização de um programa de analise de tráfego de rede (*sniffer*), para que fosse possível registrar todas as conexões estabelecidas nos *Honeypots*. Para essa tarefa foi utilizado o software Wireshark (WIRESHARK, 2012), este software foi escolhido devido as suas características citadas no referencial teórico.

3.2 CONFIGURAÇÃO E INSTALAÇÃO DO OSSEC

Após a instalação dos sistemas operacionais e seus respectivos serviços, foi instalado o sistema de detecção de intrusão baseado em *host,* que foi responsável de gerar alertas de possíveis invasões. Dentre as opções disponíveis no mercado citadas no referencial, optou por utilizar o SDIH o Ossec (OSSEC, 2012), por ser um

software gratuito e de código aberto, sendo considerado em 2007 como uma das 5 melhores ferramentas de análise de segurança pela Linuxworld (VIEIRA, 2011).

A instalação do Ossec é dividida em três categorias, local, agente e servidor. A seguir as principais características de cada instalação (OSSEC, 2012):

- Local: toda a monitoração é feita no próprio *host*, a principal desvantagem desse tipo de instalações é que, caso o invasor obtenha acesso ao sistema, os *logs* e alertas gerados podem ser comprometidos, gerando uma ineficiência do IDS;
- Agente: o agente pode ser considerado um cliente que envia as informações para o servidor processar e analisar, gerando ou não um alerta;
- Servidor: responsável pelo armazenamento dos *logs* gerados pelos agentes e pela geração de alertas, os alertas podem ser enviados por *e-mail* ou por mensagem de texto.

Para a realização desse trabalho optou-se pela instalação agente/servidor, isso garante que mesmo que um *Honeypot* seja comprometido, os *logs* e alertas gerados pelo o agente estarão seguros. A Figura 13 mostra o funcionamento do Ossec, onde o servidor é responsável de receber todos os eventos gerados pelos agentes e após encaminhá-los aos administradores.

Figura 13: Arquitetura Ossec (OSSEC, 2012)

Neste trabalho não será apresentado os passos para instalação do Ossec tanto nos *Honeypots* quanto no servidor. Os requisitos do sistema e o guia de instalação pode ser encontrado no *site* oficial (OSSEC, 2012).

Na próxima seção serão apresentados os resultados obtidos pelo sistema de detecção de intrusão Ossec e pelo analisador de tráfego Wireshark.

Os *Honeypots* foram disponibilizados na Internet dia 05/11/2012 às 00:25 e teve o seu funcionamento interrompido dia 19/11/2012, neste período houve apenas 2 dias de indisponibilidade devido a interrupção de energia e acesso a Internet. Os serviços ficaram disponíveis por aproximadamente 12 dias, o suficiente para sofrer diversos ataques.

4. RESULTADOS

Nas próximas seções serão apresentados os resumos dos resultados obtidos, contendo gráficos, tabelas e figuras.

4.1 ANÁLISE

Nesta seção será feita a análise de alguns alertas gerados pelo Ossec a fim de identificar o perfil de ataque, a origem e métodos utilizados pelos os invasores.

4.1.1 Análise do *Honeypot* Debian SSH

Após poucas mais de 7 horas disponível na Internet o *Honeypot* Debian sofreu a primeira tentativa de invasão, a Figura 14 mostra um alerta enviado pelo *e-mail*.

OSSEC HIDS Notification.
2012 Nov 05 18:59:39

Received From: (potDebian5) 192.168.0.168->/var/log/auth.log
Rule: 5712 fired (level 10) -> "SSHD brute force trying to get access to the system."
Portion of the log(s):

Nov 5 18:59:44 server sshd[11224]: Failed password for invalid user guest from 195.88.130.76 port 58630 ssh2
Nov 5 18:59:42 server sshd[11224]: Invalid user guest from 195.88.130.76
Nov 5 18:59:31 server sshd[11218]: Failed password for invalid user ghost from 195.88.130.76 port 42428 ssh2
Nov 5 18:59:29 server sshd[11218]: Invalid user ghost from 195.88.130.76
Nov 5 18:59:23 server sshd[11214]: Failed password for invalid user test from 195.88.130.76 port 41975 ssh2
Nov 5 18:59:21 server sshd[11214]: Invalid user test from 195.88.130.76
Nov 5 18:59:19 server sshd[11212]: Failed password for invalid user admin from 195.88.130.76 port 41765 ssh2
Nov 5 18:59:17 server sshd[11212]: Invalid user admin from 195.88.130.76

Figura 14: Alerta Força Bruta SSH

A partir deste alerta (Figura 14) é possível constatar que o invasor está utilizando ferramentas de força bruta para tentar obter acesso ao sistema, pode-se observar que o invasor tentou por diversas vezes se autenticar no serviço SSH

usando diferentes usuários e senhas além de utilizar portas aleatórias para na tentativa de conexão, é possível ainda identificar alguns usuários utilizados por ele.

Na Figura 15 é mostrado algumas conexões SSH capturadas pelo Wireshark, pode-se observar que diversos IPs foram capturados conforme marcação, alguns deles aparecem repetidas vezes.

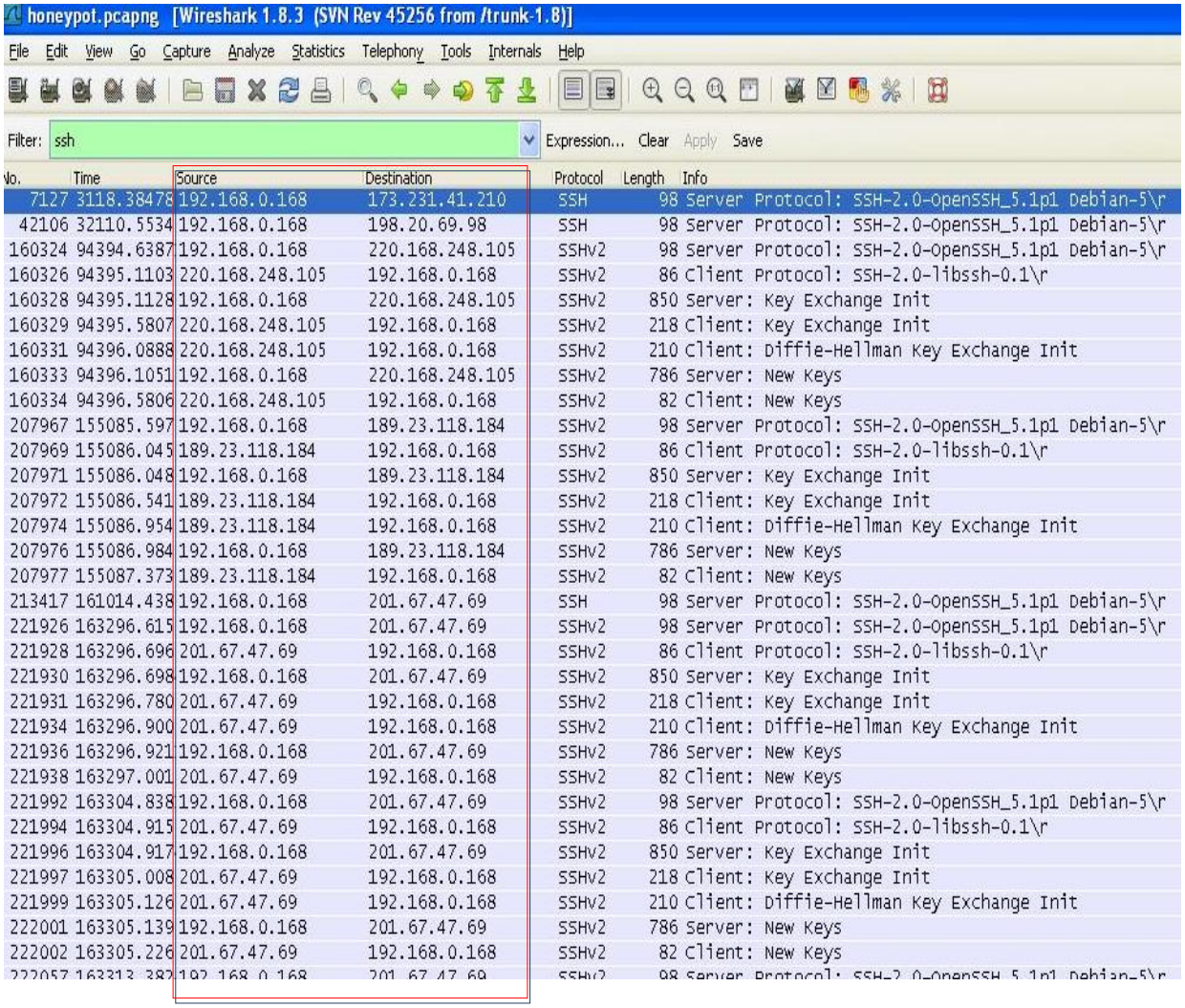

Figura 15: Filtragem Wireshark SSH

Ainda no dia 5/11, o Ossec gerou o alerta mostrado na Figura 16, onde é possível identificar a alteração nos arquivos /etc/passwd (lista de usuários cadastrados no sistema) e /etc/shadow (senha dos usuários cadastrados no sistema), este tipo de arquivo e responsável por armazenar informações de do usuário.

O invasor somente adicionou no sistema um novo usuário e senha com poderes de superusuário, com intuito de garantir o acesso posterioriormente ao sistema. Sendo que não foi identificada nenhuma alteração dos arquivos do sistema ou programas.

Através dessas informações pode-se identificar o perfil de ataque do invasor como sendo um ataque passivo, pode-se chegar a esta conclusão, pois o invasor não danificou o funcionamento do sistema seu objetivo foi apenas garantir acesso ao mesmo futuramente, o invasor passivo como mencionado no referencial teórico tem como objetivo roubar informações e não causar danos ao funcionamento do sistema.

Essas características puderam ser levantadas devido ao sistema se tratar de um *Honeypot* de alta interação, pois em um *Honeypot* de baixa interação, somente é possível recuperar as tentativas de acesso do mesmo, já que o invasor fica limitado aos programas que simulam o sistema e o serviço real.

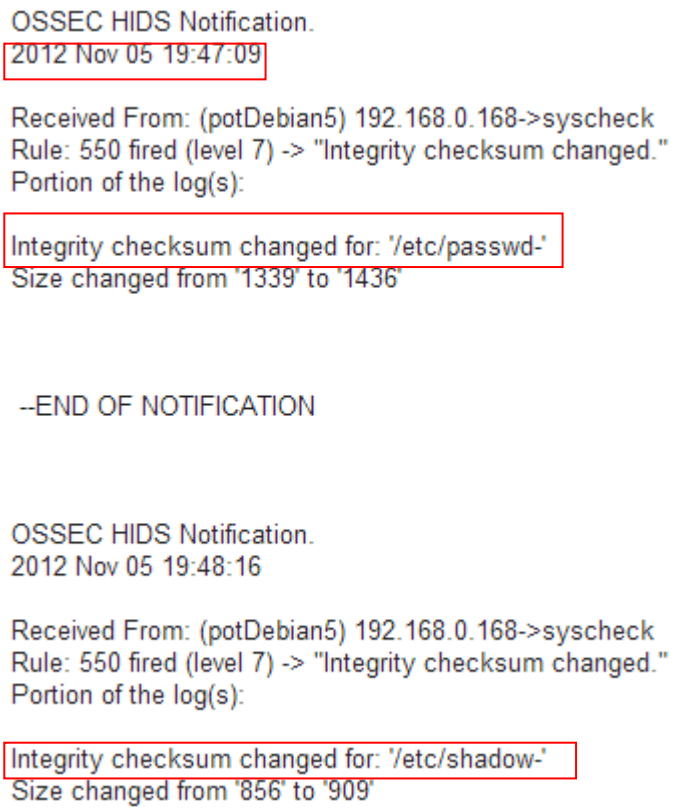

Figura 16: Criação de usuário e senha Debian 5

Além de alertas enviados por *e-mail* o Ossec ainda conta com uma interface *web* responsável por exibir os *logs* gerados com uma maior clareza, sendo possível ainda realizar filtrar dos alertas gerados por dia ou por *host*. A Figura 17 exibe um alerta na interface *web* do Ossec nas quais depois de diversas tentativas para descobrir a senha do SSH finalmente o invasor conseguiu acesso ao sistema.

Figura 17: Conexão estabelecida SSH

Na próxima seção será apresentada a analise dos *Honeypots* com sistema operacional Microsoft Windows.

4.1.2 Análise nos *Honeypots* Microsoft Windows

Os *Honeypots* com sistemas operacionais Microsoft também registram invasões, na Figura 18 é mostrado algumas tentativas de conexões FTP no *Honeypot* Microsoft Windows Server 2003 capturadas pelo Wireshark. Pode-se notar que o invasor também utilizou métodos de força bruta para tentar obter acesso ao serviço.

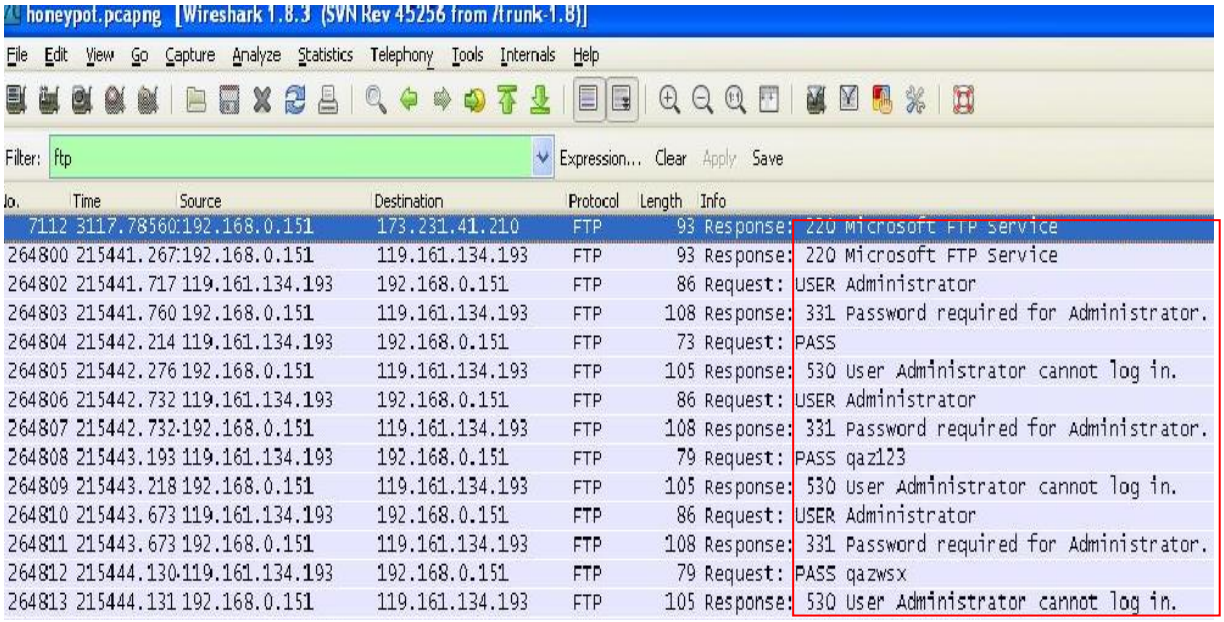

Figura 18: Filtragem Wireshark FTP**:**

Como se pode observar ainda na Figura 18, nas múltiplas tentativas de acesso o *login* utilizado foi o mesmo, isso porque o *login* “Administrador” é padrão no Windows. Também foram registradas tentativas de conexão no serviço TELNET exibido na Figura 19.

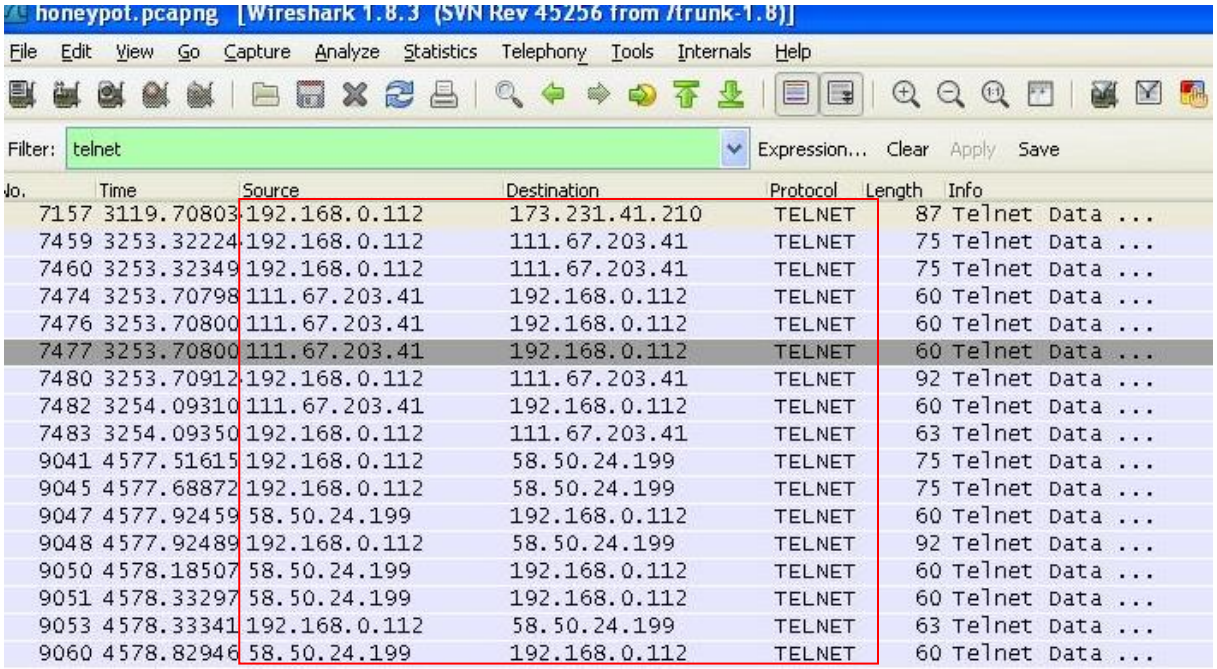

Figura 19: Filtragem Wireshark TELNET

O Ossec identificou algumas alterações no registro do Windows (Figura 20). Infelizmente, foi possível determinar somente onde ocorreu a alteração, mais não foi possível determinar o intuito das mesmas.

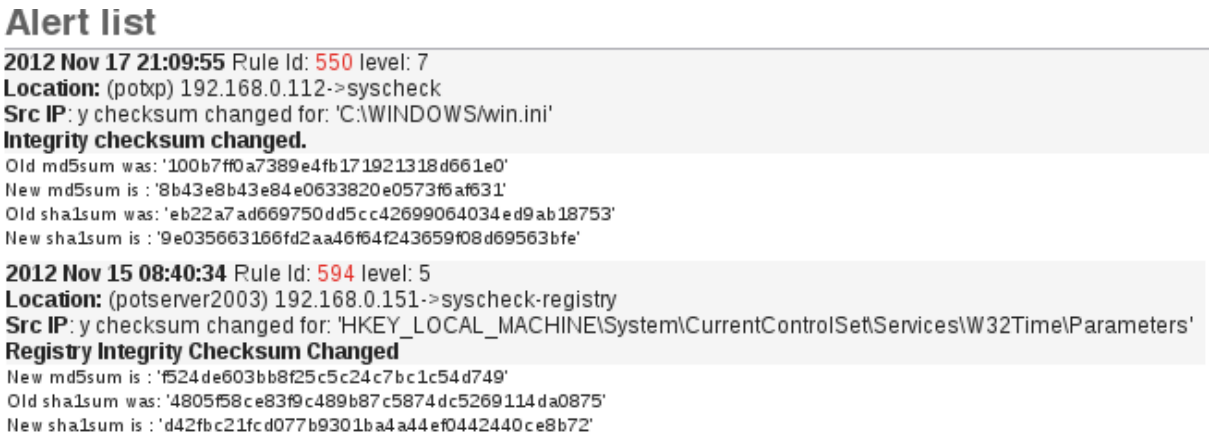

Figura 20: Alerta do registro Microsoft Windows

A Figura 21 exibe um alerta gerado pelo Ossec é detectada a ação de um *malware* no *Honeypot* Microsoft Windows Server 2003.

Figura 21: Alerta *malware* Windows

Através destas análises pode-se concluir que com a utilização de *Honeypots* de alta interação é possível levantar diversas informações sobre os ataques sofridos,

informações que vão muito além das que um *Honeypot* de baixa interação conseguiria fornecer.

Na próxima seção serão apresentados os resumos dos ataques sofridos nos dias em que os *Honeypots* ficaram disponíveis na Internet.

4.2 RESUMO QUANTITATIVO DE ATAQUES

Nos dias em que os *Honeypots* foram monitorados, foi registrado um grande número de ataques a diferentes serviços, com poucas horas de monitoração já puderam ser identificadas algumas tentativas de invasão. Destes ataques, vários destes ocorreram apenas uma única vez relacionados a um mesmo IP, como da mesma forma ocorreram reincidência.

É possível observar na tabela 1 informações sobre os ataques como: IP, país de origem, números de ataques e data. Através de sua análise é possível concluir que a China se mantém como o país que mais gerou ataques.

Resumo quantitativo de ataques (Elaborado pelo autor)

DATA	IP	Nº ATAQUES	PAIS
06/11/2012	198.20.69.98	12	Estados Unidos
06/11/2012	220.168.248.105	4	China
06/11/2012	189.23.118.184	3	Brasil
09/11/2012	201.67.47.69	16	Brasil
12/11/2012	189.83.222.29	21	Brasil
14/11/2012	95.132.213.230	1	Ucrânia
15/11/2012	221.13.34.3	4	China
15/11/2012	58.22.107.20	245	China
18/11/2012	59.53.94.9	4	China
18/11/2012	125.76.230.107	4	China
11/11/2012	119.161.134.193	267	China
18/11/2012	187.87.255.145	1	Brasil
08/11/2012	111.67.203.41	4	China
08/11/2012	58.50.24.199	4	China
09/11/2012	67.60.75.38	2	Estados Unidos
09/11/2012	58.40.19.200	2	China
09/11/2012	186.233.114.121	2	Brasil
09/11/2012	186.233.118.52	3	Brasil
09/11/2012	186.233.118.55	2	Brasil

09/11/2012	190.42.35.192	2	Peru
09/11/2012	95.13.56.105	2	Turquia
09/11/2012	190.232.184.253	2	Peru
09/11/2012	196.205.182.18	4	Egito
09/11/2012	90.150.37.123	2	Rússia
09/11/2012	190.9.120.54	2	Colômbia
09/11/2012	78.181.85.29	2	Turquia
09/11/2012	190.69.208.192	2	Colômbia
09/11/2012	186.115.236.250	2	Colômbia
09/11/2012	60.52.19.123	2	Malásia
09/11/2012	78.177.206.92	2	Turquia
09/11/2012	88.238.111.220	2	Turquia
09/11/2012	41.130.85.89	2	Egito
09/11/2012	41.130.219.114	3	Egito
09/11/2012	186.112.8.212	1	Colômbia
09/11/2012	95.175.90.183	2	Kuwait
09/11/2012	78.189.210.12	2	Turquia
09/11/2012	175.107.34.175	4	Paquistão
09/11/2012	219.90.147.127	5	Austrália
09/11/2012	83.6.154.216	2	Polônia
12/11/2012	178.137.239.211	3	Ucrânia
12/11/2012	115.108.108.106	2	Índia
12/11/2012	59.1.59.241	1	Coreia do Sul
13/11/2012	211.20.51.167	1	Taiwan
14/11/2012	95.6.3.209	2	Turquia
14/11/2012	87.16.175.11	2	Itália
15/11/2012	107.2.133.171	2	Estados Unidos
15/11/2012	68.198.211.125	4	Estados Unidos
15/11/2012	41.241.114.212	2	África do Sul
15/11/2012	189.41.117.133	2	Brasil
16/11/2012	201.58.183.63	2	Brasil
16/11/2012	111.67.203.41	8	China
16/11/2012	58.50.24.199	4	China
16/11/2012	121.245.239.213	2	Índia
16/11/2012	58.50.24.199	4	China
16/11/2012	220.188.102.196	2	China
18/11/2012	222.95.56.162	4	China
18/11/2012	111.67.203.41	5	China
18/11/2012	58.50.24.199	4	China

Tabela 1: Resumo quantitativo de ataques

A Figura 22 a seguir mostra o ranking dos países onde mais se originaram ataques com base na coleta de informações sob *Honepots* de alta interação

utilizando o sistema de detecção de intrusão Ossec e a ferramenta de análise de tráfego Wireshark.

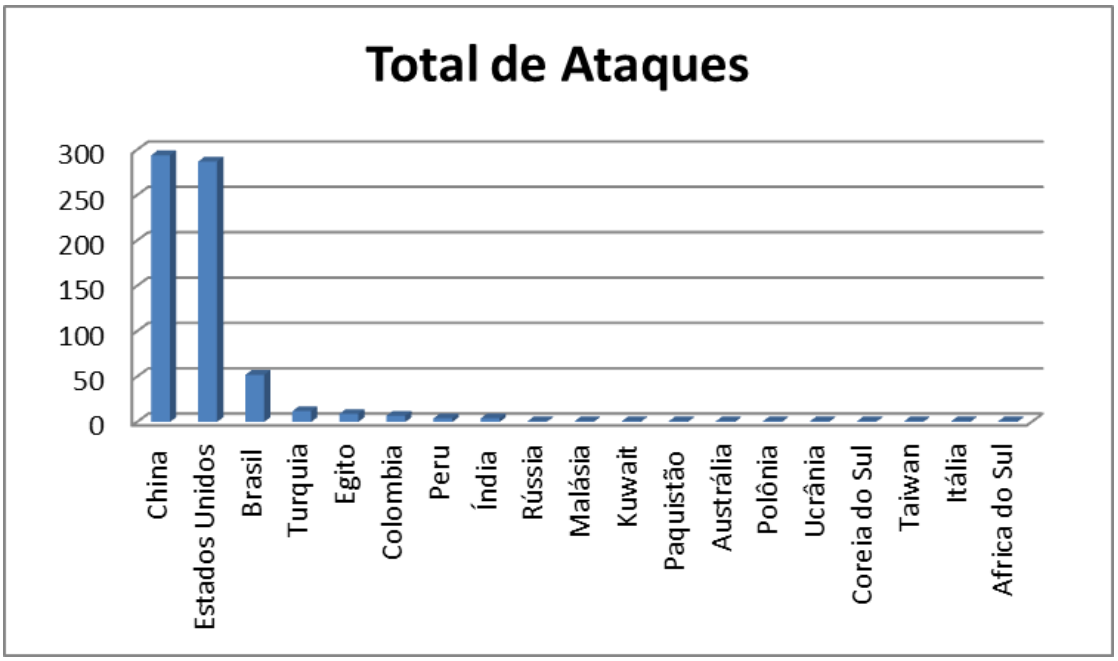

Figura 22: Ranking dos países onde mais se originaram ataques.

A Figura 22 mostra que de fato a China foi o país que mais originou ataques acompanhados dos Estados Unidos. O Brasil ficou logo após na terceira colocação, seguido de vários outros países. Isso nos mostra o quanto sistemas conectados a Internet podem estar vulneráveis a ataques, e que se deve cada vez mais investir na segurança destes sistemas.

4.3 SERVIÇOS COM MAIS OCORRÊNCIAS DE ATAQUES

Como é mostrado na Figura 23 o serviço mais procurado pelos invasores foi o SSH, isso ocorreu devido a este serviço está executando dentro de uma distribuição Debian, segundo MORIMOTO (2009) por ser líder no mercado de servidores como sistema operacional padrão, esse serviço acaba sendo o principal alvo de ataques.

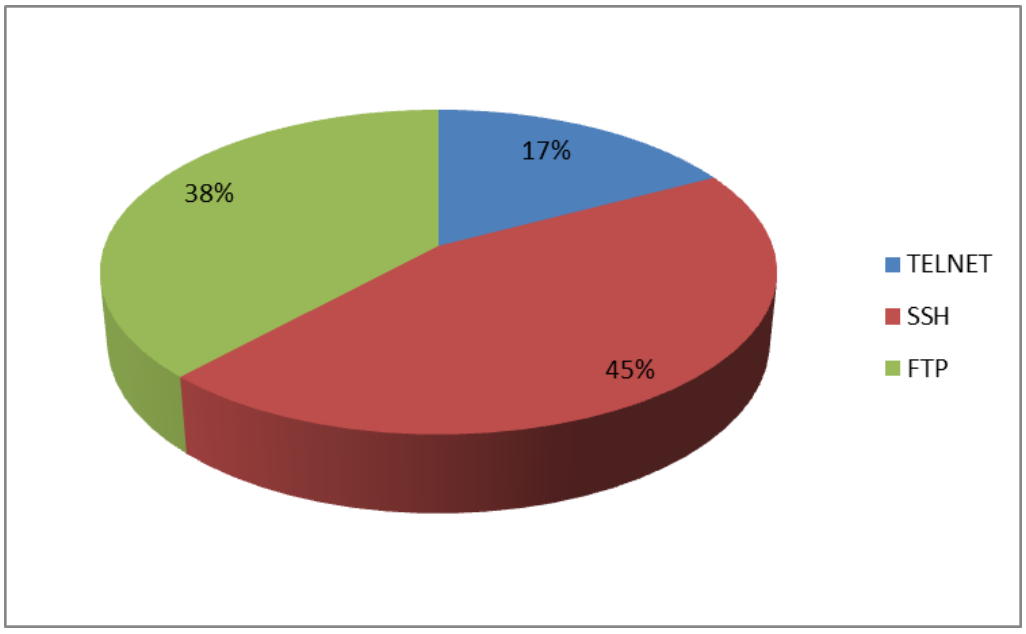

Figura 23: Serviços mais desejados pelos invasores.

O serviço SSH permite que o invasor tenha acesso total ao sistema comprometido remotamente, ou seja, o invasor pode fazer o que quiser dentro do sistema. Sendo este o principal fator que levou a ser o serviço mais procurado pelos invasores.

5. CONCLUSÃO

Atualmente grandes empresas e órgãos governamentais têm sofrido enormes prejuízos causados por invasões em seus servidores, mesmo com o grande investimento em segurança é notável que as medidas adotadas para prevenir, proteger e identificar estes ataques não são totalmente eficientes.

Durante o desenvolvimento deste trabalho, foi possível constatar a importância no desenvolvimento de novas tecnologias de prevenção e detecção de ataques. O estudo de *Honeypots* tem sido um grande aliado para o desenvolvimento destas tecnologias, podendo coletar informações valiosas sobre a origem do ataque, técnicas utilizadas, perfil do ataque, motivações, entre outras.

Apesar da sua grande eficiência os *Honeypots* não substituem as técnicas de seguranças aplicadas em uma rede de computadores, por isso deve ser usado como um complemento agregando suas funcionalidades a fim de aperfeiçoas as técnicas usadas atualmente.

A implantação de *Honeypots* de alta interação mostrou-se complexa devido à falta de artigos e descrições de trabalhos utilizando este nível de interação. A visualização e a coleta de todas as informações dos invasores provenientes de suas ações aos serviços disponibilizados ainda devem ser tralhadas, pois mostraram-se, após testes de diversas ferramentas, ainda ser uma abordagem pouco trabalhada. Mesmo assim os *Honeypots* podem fornecer um aspecto mais real para a análise de segurança por fornecer as ações do invasor e não somente as tentativas de acesso.

Os resultados obtidos no presente trabalho, como: países de origem com seus respectivos IPs, a identificação de ataques utilizando de força bruta, a identificação de ataques passivos, os usuários e senhas utilizados em conexões FTP, a modificação dos registros do Windows e a detecção de *rootkits*, confirmam a importância de se utilizar *Honeypots* de alta interação, devido à quantidade de informações que podem ser podem coletadas.

Como trabalhos futuros fica a sugestão de manter os *Honeypots* de alta interação por um período superior ao realizado no presente trabalho, podendo assim coletar maiores informações sobre os ataques sofridos. Fica também a sugestão de criar ferramentas que consigam fazer o acompanhamento de uma invasão desde a

sondagem até o comprometimento do *Honeypot,* fazendo uma analise detalhada de tudo que foi feito pelo invasor.

Outra opção é a implantação de *Honeypots* de alta interação na Infraestrutura de TI dessa instituição, a fim de estudar as vulnerabilidades exploradas, identificar os possíveis invasores e desviar as ações maliciosas para os *Honeypots*, dando tempo de agir aos administradores de rede.

REFERÊNCIAS

ANDRUCIOLI, Alexandre Pinaffi. **Proposta e Avaliação de um Modelo Alternativo Baseado em Honeynets para Identificação de Ataques e Classificação de Atacantes na Internet**. COPPE/UFRJ [Rio de Janeiro] 2005.

ASSUNÇÃO, Flávio Marcos Araújo. **Honeypots e Honeynets: Aprenda a detectar e enganar os invasores**. Florianópolis: Visual Books, 2009.

BARBATO, Luiz Gustavo Cunha. **Monitoração de atividades e máquinas preparadas para serem comprometidas (Honeypots)**. 2004. 147 f. Dissertação (Mestrado em Computação Aplicada) - São José dos Campos: 2004. (INPE-12904-TDI/1010).

BEALE, Jay et al. **Snort 2.1 Intrusion Detection**, Second Editions. Syngress Publishing, 2004.

BELCHIOR, Francisco de Oliveira; SOUSA, Iara Moura; ARAÚJO, Lêda Brito. **Projeto: Utilizando Honeynets como ferramenta auxiliar na verificação de vulnerabilidades em sistemas operacionais.** Faculdade AD1, Brasília, novembro 2004.

BRANDINO, Wandreson Luiz. **Apostila TCP/IP** – Disponível em: <http://www.wandreson.com/download/training-networking-tcpip.pdf>, 1998 Acesso em: 25/11/2012.

CERT.BR. **Cartilha de segurança para Internet**. Disponível em: <http://cartilha.cert.br/download> 2012. Acesso em: 16 de Julho de 2012.

CITRIX, **XenServer** –Disponível em: <http://www.citrix.com/products/xenserver/overview.html> Acesso em 09/10/2012.

COSTA, Nilson Santos. **Proteção de Sistemas Elétricos Considerando Aspectos de Segurança da Rede de Comunicação**. 2007. 209 f. Tese (Doutorado em Engenharia Elétrica) - Curso de Engenharia Elétrica, Escola de Engenharia de São Carlos, São Carlos, Abril, 2007.

JONES, M. Tim. **Virtual Linux**. 2006. Disponível em: <http://www.ibm.com/developerworks/linux/library/l-linuxvirt/?ca=dgr-lnxw01Virtual-Linux> Acesso em: 12/11/2012.

KUROSE, James F.; ROSS, Keith W. **REDES DE COMPUTADORES E A INTERNET**, Uma abordagem Top-Down 5º Edição. São Paulo: Pearson 2010.

LAUREANO, Marcos. **Máquinas Virtuais e Emuladores Conceitos, Técnicas e Aplicações**. Editora Novatec, 2006.

MARCELO, Antônio, ALVES, Marcos José Pitanga. **Honeypots: A arte de iludir hackers.** Rio de Janeiro: Brasport, 2003.

MARINHO, Renato Rodrigues. **Honeypots: Acompanhando os passos de uma invasão em tempo real**. UNIFOR [Fortaleza] 2005.

MARTINS, Elaine. **VM Ware, Virtual Box ou Virtual PC: qual é o melhor programa para virtualização? –** Disponível em: < http://www.tecmundo.com.br/comparacao-/28433-vm-ware-virtual-box-ou-virtual-pc-qual-e-o-melhor-programa-para-virtualizacao-.htm#ixzz2DOPeQfZz> Acesso em : 25/11/2012.

MORIMOTO, Carlos Eduardo. **Servidores Linux, Guia prático**. Porto Alegre: Sul Editores, 2006.

NETO, Urubatan. **Dominando Linux Firewalls Iptables**. 1ªed. Ciência Moderna Ltda, Rio de Janeiro – Brasil, 2004.

ORACLE, **Virtual Box** – Disponível em: <www.virtualbox.org> Acesso em: 21/11/2012.

OSSEC. **Ossec** – Disponível em: <http://www.ossec.net/> Acesso em: 28/10/2012.

RAVANELLO, Anderson Luiz; HIJAZI, Houssam Ali; MAZZORANA, Sidney Miguel. **Honeypots e Aspectos Legais.** Universidade Católica do Paraná, Curitiba, 2004.

SHIRLEY, R. **Internet Security Glossary RFC 2828.** Disponível em: <http://www.ietf.org/rfc/rfc2828.txt>, 2000. Acesso em: 12 de Novembro de 2012

SILVA, Ana Cristina Benso. **Sistema de Detecção de Intrusão baseado em Métodos Estatísticos para Análise de Comportamento.** Tese (Doutorado). Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, julho de 2003.

SILVA, Diogo Ezídio; OLIVEIRA, Gilberto Lima; RANGEL, Leandro de Souza; FLORÃO, Lucas Timm. **Virtualização como Alternativa para Ambiente de Servidores.**

SILVA, Jacson Rodrigues Correia. **Sistemas de Detecção de Intrusão com Técnicas de Inteligência Artificial**. 2011. 157 f. Dissertação (Mestrado em Ciência da Computação) – Universsidade Federal de Viçosa, 2011.

SOUZA, Tiago. **Honeypots – A segurança através do disfarce.** Ravel – COPPE/UFRJ, GRIS – DCC/UFRJ 9 de Agosto de 2005.

SPITZNER, Lance. **Honeypots: Tracking-Hackers.** 1ªed Addison-Wesley Professional 2002.

TANENBAUM, Andrew S. **Redes de Computadores**, 3º Edição. Rio de Janeiro: Campus, 1997.

ULBRICH, Henrique César, VALLE, James Della. **Universidade H4CK3R**. 6º Ed. São Paulo: Digerati Books 2009.

VIEIRA, Vinícius**. Saiba tudo que acontece em seu *host* com OSSEC** – Disponível em: <www.sejalivre.org/saiba-tudo-que-acontece-em-seu-host-com-ossec> Acesso em: 21/11/2012.

VMWARE, **Workstation** – Disponível em: <http://www.vmware.com/products/workstation/overview.html> Acesso em: 09/10/2012.

WANG, Jie. **Computer Network Security:** Theory and Practice. Higher Education Press, Beijing and Springer-Verlag GmbH Berlin Heidelberg, 2009

WIRESHARK. **Wireshark** – Disponível em: <http://www.wireshark.org/> Acesso em: 28/10/2012.