CENTRO UNIVERSITÁRIO FILADÉLFIA

CIÊNCIA DA COMPUTAÇÃO

FERNANDO ORTIZ BORGES

A APLICAÇÃO DE HONEYPOTS DE BAIXA INTERATIVIDADE, JUNTAMENTE COM SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS) EM AMBIENTES CORPORATIVOS. UM ESTUDO DE CASO NA EMPRESA BIG INFORMÁTICA.

Londrina

2016

FERNANDO ORTIZ BORGES

A APLICAÇÃO DE HONEYPOTS DE BAIXA INTERATIVIDADE, JUNTAMENTE COM SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS) EM AMBIENTES CORPORATIVOS. UM ESTUDO DE CASO NA EMPRESA BIG INFORMÁTICA.

Trabalho de Dissertação apresentado ao Centro Universitário Filadélfia como parte dos requisitos para obtenção de graduação em Ciência da Computação. Orientador: Me Mario Henrique Akihiko da Costa Adaniya .

Londrina
2016

FERNANDO ORTIZ BORGES

A APLICAÇÃO DE HONEYPOTS DE BAIXA INTERATIVIDADE, JUNTAMENTE COM SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS) EM AMBIENTES CORPORATIVOS. UM ESTUDO DE CASO NA EMPRESA BIG INFORMÁTICA.

Trabalho de Conclusão de Curso apresentado à Banca Examinadora do curso de Ciência da Computaçãodo Centro Universitário Filadélfia de Londrina em cumprimento a requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

APROVADO PELA **COMISSÃO EXAMINADORA**
EM LONDRINA , 2016.

_____

Me Mario Henrique Akihiko da Costa Adaniya - Orientador

_____

Professor 1 - Examinador

_____

Professor 2 - Examinador

AGRADECIMENTOS

Agradeço primeiramente a meu amado Deus, eu sou grato por este presente maravilhoso que é a vida!

Ao meu professor e orientador Mario Henrique Akihiko da Costa Adaniya pelo auxilio, pela paciência, pelo tempo onde esteve sempre animado e com imensa simpatia. Obrigado por ser um excelente professor.

Dedico esse trabalho "in memorian"ao meu avô (José Aliano) e aproveito para agradece-lo, esteja onde estiver.

A minha mãe, Josiani e ao meu segundo pai Jefferson, sem os esforços de vocês, eu não poderia estar aqui agradecendo, a determinação de vocês é grande, e não existem palavras o suficiente para agradecer tudo que fazem por mim, e pelos meus irmãos.

Ao meu pai Giovane, que apesar da distância e das circustâncias que as vezes nos afastam, me ensinou à crescer em virtude.

A minha namoradinha, Marcela, por toda a paciência que tem comigo, pelo carinho, pelo amor e compreensão. Compartilho com você os melhores momentos da minha vida. Além desse trabalho, dedico todo meu amor a você.

Aos grandes amigos que fiz durante o curso, Bruno Prece, Guilherme Bexiga, Fortran, Marco Souza e Jonathan Albertoni pessoas responsáveis por me ajudarem nos momentos mais difíceis do curso.

Agradeço ao meu grande amigo Demetrius Germani, que foi meu patrão, obrigado pela ajuda com certas fórmulas matemáticas (risos), e por todo conhecimento adquirido enquanto estive ao seu lado.

"Tudo foi calculado, exceto como viver."
(Jean-Paul Sartre)

BORGES; FERNANDO, O. **A aplicação de Honeypots de baixa interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) em ambientes corporativos. Um estudo de caso na empresa Big Informática.** . Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Filadélfia . Londrina , 2016.

RESUMO

ESCREVER Resumo em português AQUI.

Palavras-chaves: Honeypots, Segurança da Informação, Honeynets.

BORGES; FERNANDO, O. **A aplicação de Honeypots de baixa interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) em ambientes corporativos. Um estudo de caso na empresa Big Informática.** . Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Filadélfia . Londrina , 2016.

ABSTRACT

Write your abstract in foreign language here *Extended abstract in English or another foreign language. 30 lines, simple spacing.* ***Keywords****: Honeypots, Information Security, Honeynets.*

SUMÁRIO

1 INTRODUÇÃO

Honeypots são recursos computacionais implantados em uma rede de computadores para serem comprometidos, atacados ou sondados. Com isso é possível obter o levantamento das técnicas que indivíduos mal-intecionados utilizam para se apossarem da rede ou do sistema operacional comprometido. Eles podem ser classificados de acordo com seu nível de interação: baixa, média ou alta interatividade.

Desta forma, é possível implantar esses sistemas juntamente com Sistemas de Detecção de Intrusão, que são técnicas utilizadas com um conjunto de ferramentas que visam descobrir se uma rede possui ou não tentativas de acessos não autorizados, sejam eles de invasores ou até mesmo de funcionários mal-intencionados.

Diante da alta tecnologia que o mercado dispõe, um fator que permanece em evidência é a importância do administrador de rede em um ambiente corporativo. Frequentemente é observado que em alguns ambientes ainda faltam segurança durante o tráfego de dados, essa segurança às vezes é deixada de lado por parte desse profissional, alguns dos fatores que implicam à isso são a falta de tempo, falta de orçamento ou falta de conhecimento.

Portanto, buscou-se reunir informações com o propósito de responder ao seguinte problema de pesquisa: De que maneira a aplicação de Honeypots de baixa Interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) auxilia na implantação de sistemas de segurança em ambientes corporativos?

O objetivo da implantação de Honeypots juntamente com Sistemas de Detecção de Intrusão visa auxiliar profissionais de rede implantar esses sistemas para a melhoria da segurança do ambiente. Isso porque medidas poderão ser tomadas antecipadamente quando um indivíduo mal-intencionado estiver atacando a rede. Um novo cenário poderá ser implantado a partir de configurações de Honeypots de baixa ou alta interatividade, para que o mesmo possa minimizar problemas relacionados a área de segurança, e também um Sistema Detector de Intrusões, para detectar tentativas de intrusões onde o ambiente se encontra. Essa combinação de técnicas será possível obter informações provenientes de uma tentativa de ataque.

A confiabilidade na segurança das informações de uma empresa nos dias de hoje tem um valor significativo dentro da organização. O surgimento de novas tecnologias no mercado, trás consigo novas vulnerabilidades e brechas que podem ser exploradas para novos tipos de ataques. Esses ataques são criados com o intuito de adquirir por meios não legais informações das instituições, quebrando o paradigma de confiabilidade na segurança dos dados. Esses ataques são criados de maneira organizada e sofisticada, onde a defesa do administrador da rede ficará ainda mais complicada caso não use meios para prevenir esses ataques.

Para tanto, as organizações precisam se posicionar de alguma maneira, procurando ter ciência de quando sua manutenção e investimento será viável e necessária. Nesse contexto citado, a proposta desse trabalho visa apresentar conceitos, definições e ferramentas necessárias para esse tipo de tomada de decisão.

Para o desenvolvimento do trabalho foram utilizadas pesquisas bibliográficas, além do estudo de caso. A pesquisa bibliográfica baseou-se em publicações científicas da área de segurança da informação. O estudo de caso foi desenvolvido na empresa Big Informática. É um estudo exploratório, pois a organização possui grau de informalidade, sendo assim, necessário investigar toda a realidade que a infra-estrutura de rede se encontra, afim de obter dados e informações para o planejamento do estudo.

O trabalho de conclusão de curso esta estruturando em seis capítulos. No primeiro a introdução acerca de Honeypots. No segundo capítulo é apresentado a metodologia aplicada no trabalho. No terceiro capítulo é o referêncial teórico, onde será apresentado os aspectos de segurança da informação, detalhando os principais tipos de ameaças e a classificação dos tipos de ataques, será apresentado também quais as motivações que levam um invasor a invadir uma rede, suas motivações e seus verdadeiros alvos. Também é apresentado detalhadamente o uso de sistemas de detecção de intrusão, mostrando estratégias utilizadas para criação de Firewalls. Por fim ele apresenta os Honeypots, introduzindo um breve histórico e demais itens que compõem a sua classificação. É apresentado as vantagens e desvantagens ao utlizá-lo. O quarto capítulo caracteriza o estudo de caso, com a análise da organização de estudo, envolvendo os demais itens que compõem a empresa Big Informática, e também as técnicas que foram realizadas na mesma, afim de criar um sistema que auxilie os administradores de rede a implantar sistemas de segurança utilizando Honeypots de baixa (ou alta) interatividade juntamente com Sistemas de Detecção de Intrusão. No sétimo capítulo é mostrado os dados obtidos com o presente estudo realizado. E por fim no oitavo capítulo é apresentado a conclusão do trabalho.

1.1 JUSTIFICATIVA

O surgimento de tecnologias novas no mercado, junto a elas surgem novas vulnerabilidades e brechas para diversos tipos de ataques e fraudes realizados por indivíduos mal-intencionados. Esses ataques podem ser realizados com o uso de ferramentas mais sofisticadas, no qual a prevenção para um administrador de rede, ou profissional da área de segurança ficará um pouco mais complicado e díficil de ser realizado.

Devido às dificuldade na implantação de sistemas de segurança, realizados por profissionais da área de segurança, essa pesquisa se justifica-se através da aplicação de Honeypots de baixa interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) em ambientes corporativos.

1.2 DELIMITAÇÃO DO TEMA

Este projeto de pesquisa delimitou-se em colher informações sobre de que maneira a aplicação de Honeypots de baixa interatividade, juntamente com Sistemas de detecção de Intrusão (IDS) auxilia na implantação de sistemas de segurança em ambientes corporativos, tendo como referência a empresa Big Informática, situada na cidade de Ibiporã-PR.

1.2.1 Formulação do Problema

Portanto, buscou-se reunir informações com o propósito de responder ao seguinte problema de pesquisa: De que maneira a aplicação de Honeypots de baixa Interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) auxilia na implantação de sistemas de segurança em ambientes corporativos?

1.2.2 Hipótese

A teoria é que a dificuldade na implantação de sistemas com mais segurança, podem ser revolvidos com a aplicação em conjunto de Honeypots de baixa interatividade, e Sistemas de Detecção de Intrusão (IDS).

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O presente trabalho tem como objetivo geral verificar de que maneira a aplicação de Honeypots de baixa Interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS) auxilia na implantação de sistemas de segurança, realizados por profissionais da área de segurança em ambientes corporativos.

A finalidade de apresentar a vantagem quando utiliza-se desses sistemas, é a melhoria da segurança no ambiente, e o conhecimento de técnicas e métodos que são utilizadas por indivíduos mal-intencionados, afim de mostrar para os profissionais dessa área o perfil desses indivíduos, para que os mesmos possam tomar as devidas medidas de segurança na empresa Big Informática.

1.3.2 Objetivos Específicos

- Apresentar o cenário atual do estudo de caso, relacionado a infraestrutura de rede em que a empresa se encontra.

- Esquematizar um novo cenário de rede, baseado e de acordo com as configurações de uso de honeypots de baixa interatividade, e um Sistemas de Detecção de Intrusão (IDS).

- Avaliar como minimizar os problemas relacionados a área de segurança.

- Desenvolver a implementação de um Honeypot de baixa Interatividade, e um Sistema de Detecção de Intrusão (IDS), afim de detectar a intrusão de usuários mal-intencionados.

- Apresentar as informações obtidas mostrando como o uso dessas técnicas ajudam na melhoria da segurança.

2 METODOLOGIA

A finalidade do estudo presente nesse trabalho é utilizar-se de uma pesquisa aplicada, visto que a mesma utilizará de uma pesquisa básica para a resolução dos problemas.

Para tratar dos objetivos, observou essa pesquisa como sendo exploratória, visto que ainda a familiaridade entre o pesquisador e o tema pesquisado são poucos conhecidos. Para isso detectou-se a necessidade de uma pesquisa bibliográfica no momento em que se faz o uso de materiais já elaborados: livros, artigos científicos, revistas, documentos eletrônicos na busca de conhecimento sobre Honeypots de baixa Interatividade, correlacionando tal conhecimento com abordagens já trabalhadas por outros autores.

A pesquisa assume como estudo de caso, sendo exploratória, que por sua vez, proporciona maior familiaridade com o problema, tornando-o explícito ou construindo hipóteses sobre ela através de principalmente do levantamento bibliográfico. Por ser um tipo de pesquisa muito específica, quase sempre ela assume a forma de um estudo de caso (Gil, 2008)

Para o tratamento dos procedimentos, será necessário a pesquisa bibliográfica, pois será utilizado materiais já publicados. Entende-se como um procedimento importante nessa pesquisa o estudo de caso como um procedimento de nível técnico.

A abordagem do tratamento da coleta de dados obtidos com o estudo de caso será????????

(VERIFICAR COM MÁRIO) ESTOU EM DÚVIDAS. Bibliográfica, Qualitativa ou Quantitativa??

O problema foi direcionando a pesquisa para as áreas de implantação de sistemas de segurança, realizados por profissionais dessa área, e ainda foi realizada uma pesquisa como estudo de caso, sendo este: A aplicação de Honeypots de baixa interatividade, juntamente com Sistemas de Detecção de Intrusão (IDS). É realizada uma análise em ambientes corporativos, que visa a empresa Big Informática como o coletivo, apresentando o cenário atual de infraestrutura de rede que a empresa se encontra.

3 REFERÊNCIAL TEÓRICO

3.1 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO

3.1.1 Descrição Geral

3.1.2 Invasores, Alvos e Motivações

3.1.2.1 Invasores

3.1.2.2 Alvos

3.1.2.3 Motivações

3.2 PRINCIPAIS TIPOS DE ATAQUES E AMEAÇAS

3.2.1 Classificação dos ataques

3.3 FERRAMENTAS E COMPONENTES DE SEGURANÇA

3.3.1 IDS - Sistema de Detecção de Intrusão

3.3.1.1 Tipos de Detecção e Reação

3.3.1.2 Tipos de IDS

3.3.2 Sistemas de Firewall

3.3.2.1 Arquiteturas de Firewall

3.3.2.2 Tipos de Firewall

3.4 HONEYPOTS

3.4.1 Conhecendo os Honeypots

Utilizados como "armadilhas", os *Honeypots* servem para atrair indivíduos mal-intencionados que desejam buscar o acesso não autorizado em computadores de determinadas redes que se encontram vulneráveis. São utilizados para serem comprometidos, para que administradores de rede possam fazer uma análise nas informações deixadas por esses indivíduos, para que os mesmos possam traçar medidas de prevenção de segurança.

Como bem nos assegura Wrightson (2014), os *Honeypots* são propositalmente configurados com vulnerabilidades específicas para que o atacante, ou seja,

o indivíduo mal-intencionado, seja atraído. Afinal, esse ambiente agora possui vulnerabilidades que são de interesse para o atacante. Esse ambiente preparado, é capaz de fornecer provas de tentativas de ataques, pois foram configurados como armadilhas, e com esse propósito.

É notável que a citação acima demonstra que o uso de *Honeypots* devem ser utilizadas de maneira propositalmente, pois é uma ferramenta utilizada para o estudo, e com esse estudo conseguir adotar medidas de prevenção. Obviamente denota-se que se for configurado de maneira errada, ou cair em mãos de indivíduos despreparados, resultará em um caminho mais fácil para o atacante, no qual poderá comprometer toda a rede.

Um *Honeypot* é um recurso de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um *Honeypot* poderá ser testado, atacado e invadido. Os Honeypots não fazem nenhum tipo de prevenção, os mesmo fornecem informações adicionais de valor inestimável. (Spitzner, 2003).

Os bens mais valiosos dentro de ambientes corporativos, são suas informações. As definições de (Wrightson, 2014) e (Spitzner, 2003) nos levam a entender que se forem utilizados de maneira correta, as armadilhas criadas com o uso de *Honeypots* podem servir para os administradores de rede tomarem atitudes e medidas de prevenção para segurança e sigilo dessas informações.

Em ambientes corporativos o termo *hacker* significa prejuízo. Mesmo que o seu real significado, empregado pela mídia, não seja esse. A falta de implantação de sistemas e medidas de segurança utilizadas por administradores de rede é que implicam o termo *hacker* tomar esse caminho. As invasões, os vírus e o roubo de informações sigilosas são um pesadelo para qualquer tipo de ambiente, e isso trás um potencial devastador para as organizações despreparadas de políticas de segurança adequadas.

É necessário implementar e manter atualizadas medidas de segurança técnicas e de procedimentos com boa relação custo-benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso. (Fontes, Edison, 2012, p.61)

O autor deixa claro na citação acima que medidas de segurança e procedimentos devem e precisam ser implementados. Esse é o motivo pelo qual é importante frisar esse ponto, uma vez que, uma falha no sistema pode comprometer toda a segurança da organização, trazendo prejuízos imensuráveis.

Com essa visão pode-se ter um conhecimento mais amplo do que são *Honeypots*, e quais os fundamentos de fazer suas implementações como medida de prevenção. Obviamente que uma série de outras medidas devem ser adotadas para impedir que esses usuários se apoderem do sistema, porém a implementação de Honeypots visa ajudar os administradores a entender como funciona o comportamento desses indivíduos, e auxiliar em medidas de prevenção.

3.4.2 Classificação de Honeypots por níveis de interatividade

Honeypots possuem níveis de interatividade que podem ser definidos por características próprias de cada nível. A facilidade na manutenção, o nível de segurança e o custo de implementação são alguns dos exemplos de características que cada nível de interatividade pode apresentar. Nas seções abaixo serão mostrados características de cada um dos três níveis de interação: baixa, média e alta.

3.4.2.1 Honeypots de baixa interatividade

Honeypots de baixa interatividade, são aqueles que emulam serviços ou até mesmo Sistemas Operacionais dentro de uma determinada rede. O nível de interatividade entre o sistema emulado e o atacante é baixo. A implementação desse nível, exige um risco pequeno e também um baixo custo de implementação.

Como bem nos assegura Vinícius Batistela e Marco Antônio Sandini Trentin (2009), *Honeypots* de baixa interatividade trás uma visão limitada de interação com o atacante, além disso, é considerado o tipo que trás menor manutenibilidade em aspectos de configuração, segurança e baixo custo. Exemplos de serviços básicos que podem ser emulados, são o *FTP - File Transfer Protocol* e o *Telnet*.

Apesar do nível de interação ser considerado baixo com o atacante, se o objetivo do administrador de rede for apenas visar na facilidade de configuração e no baixo custo de implementação, *Honeypots* de baixa interatividade são os mais ideais para o ambiente. Sua implementação a maioria das vezes é por meio de aplicativos instalados e pré-configurados, tornando o ambiente restrito a interações com atacante.

Ao executar tarefas simples, como por exemplo, monitorar as portas de um determinada rede, afim de encontrar portas abertas, esse tipo de Honeypot ficará restrito a pilha *TCP/IP*. Alguns tipos de *Honeypots* com esse nível de interatividade pode-se citar S*pecter, Honeyd e KFSensor* (MARTIM; PAULO *apud* PROVOS).

Dentre as vantagens como a baixa manutenibilidade, citada pelos autores, desvantagens existem, como a limitação de análises através de logs gerados, o que dificultará uma formulação mais precisa do perfil do atacante. Esse tipo de Honeypot é projetado para capturar atividades maliciosas conhecidas, sendo assim, com alguns comandos o atacante pode perceber a armadilha, e com pequenos comandos descobrir que está sendo alvo de investigação.

Honeypots de baixa interação explora a grande vantagem em não permitir a interação do atacante diretamente com a rede, não trazendo nenhum risco e nem servindo de ponte para outros tipos ataques realizados pelo indidíduo mal-intencionado.

Pelo fato de não permitirem a entrada do atacante, *Honeypots* de baixa interatividade apresentam a vantagem de não correrem o risco de serem utilizados como base para outros ataques, sendo os mais indicados para pessoas ou organizações

que querem começar a trabalhar com este tipo de recurso de segurança. (Batistela; Trentin, 2009).

O autor deixa claro ao citar a vantagem em utilizar esse mecanismo de baixa interação, principalmente para quem esta iniciando, visto que o mesmo não comprometerá a rede e nem servirá de base para outros ataques. Apesar de possuir a desvantagem em relação a análise de logs, para quem deseja implementar um recurso de segurança adicional na organização, afim de detectar atividades maliciosas, e com custo de implementação baixo, esse tipo de Honeypot é o mais indicado.

Diante das informações expostas, pode-se verificar a finalidade de uso desse tipo de interação. É mostrado que esse nível quando utilizado, permite ainda menos risco a rede, facilidade na configuração e na manutenção, como vantagens. É apresentado as desvantagens no uso desse tipo de interação, como a falta de informações suficientes gerados pelo serviços de *logs*.

3.4.2.2 Honeypots de média interatividade

Assim como *Honeypots* de baixa interatividade, esse tipo de *Honeypot* irá emular serviços com vulnerabilidades, porém com uma gama maior em detalhes, mas ainda assim não deixa de ser um sistema real. Esse tipo de interatividade consegue obter mais dados e informações do atacante, pois o mesmo possui interação maior com o sistema, os serviços que são emulados durante essa interação conseguem responder a requisições dos atacantes, como se fossem serviços reais disponibilizados. Graças a esse tipo de interação o atacante fica em um ambiente falso, e em momento algum terá contato com o sistema operacional real.

Antonio Marcelo e Marcos Pitanga (2003) (Verificar como citar dois autores) diz que esse tipo de interação pode nos trazer mais informações acerca do invasor, pois aqui é emulado com mais precisão os serviços. Esses serviços respondem de maneira falsa, fazendo assim o invasor achar que está em um sistema operacional real. Esse tipo de Honeypot consegue nos trazer mais informações das técnicas utilizadas pelo invasor. Apesar desse tipo oferecer mais detalhes, ele também nos trás um risco maior, pois se o invasor consegue descobrir qualquer má-configuração, ele é capaz de invadir o sistema operacional onde o serviço está sendo emulado.

Sabendo ainda que esse tipo de Honeypot podem trazer riscos a infra-estrutura da rede,é necessário então ter cautela para esse tipo de implementação, ainda mais se forem operados por usuários e administradores iniciantes e inexperientes, pois um descuido podem comprometer a rede. Nesta perspectiva entendemos que o nível de interação desse Honeypot podem nos trazer mais benefícios de estudo e comportamento do que os Honeypots de baixa interatividade, pois aqui as técnicas utilizadas pelos invasores serão trazidas com mais detalhes.

Esse tipo, pode ainda fornecer maior interatividade com o atacante, pois é pos-

sível utilizá-lo através de ferramentas que o próprio Sistema Operacional Unix oferece, o chroot. Ele é uma operação no qual será mudado o diretório de root do processo corrente e de seus processos filhos, ou seja, ele permite transformar um diretório no seu diretório raiz atual. Assim é possível criar um sistema virtual aninhado com o real. (Vinícius Batistela, Marco Antônio, 2009).

FALTA TERMINAR.

3.4.2.3 Honeypots de alta interatividade

Segundo Marcelo; Alves (2003) os *Honeypots* de alta interatividade são Sistemas Operacionais implementados e configurados com falhas reais, e não com falhas emuladas, como os *Honeypots* de baixa e média interatividade. Essas falhas são serviços instalados e configurados em um ambiente real para servir de isca para o invasor.

Como bem nos assegura Marcos Flávio Araújo Assunção (2009), os *Honeypots* de alta interatividade, se forem configurados de maneira correta, além de conseguir capturar todo o comportamento do indivíduo mal-intencionado, também consegue ficar imperceptível para o invasor, pois é semelhante ao sistema real onde o mesmo se encontra.

Para SPITZNER (2002, p. 96) os *Honeypots* de alta interatividade facilita na captura de informações mais precisas de um invasor, pois através de mecanismos implantados podemos estudar o comportamento do indivíduo para traçar medidas de prevenção de segurança. Porém esse tipo de interatividade é considerado o mais difícil de ser implementado, e além da dificuldade, apresenta riscos maiores ao ambiente, e um custo mais elevado.

Para esse autor, Honeypots de alta interatividade permite, "They give us a vast amount of information about attackers, but they are extremely time consuming to build and maintain, and they come with the highest level of risk. The goal of a high-interaction honeypot is to give the attacker access to a real operating system where nothing is emulated or restricted."(VERIFICAR ISSO)

Como se pode verificar nessa citação, os *Honeypots* de alta interatividade podem ser demorados para serem implementados, mas é evidente que se forem aplicados de maneira correta podem ser utilizados para coletarem com mais precisão as informações deixadas por invasores.

Eles funcionam na maioria das vezes em um ambiente controlado, é estruturado em uma arquitetura de rede controlada, ou seja, onde possa ser monitorada pelo administrador de rede. Cita-se, como exemplo, a criação de um *Firewall* que aceite o tráfego de entrada, e controle o tráfego de saída, juntamento com um Sistema de Detecção de Intrusão (IDS).

Ainda para SPITZNER (2002, p. 96), The firewall allows the attacker to compromise one of the honeypots sitting behind the firewall, but it does not let the attacker use the honeypot to launch attacks back out.

Nesse sentido, os *Honeypots* de alta interatividade permitem que serviços reais sejam comprometidos. Essa ferramenta configurada corretamente pode ficar imperceptível ao invasor, nos trazendo com precisão o comportamento de indivíduos mal-intencionados.

Logo, é importante compreender que apesar da complexidade, do tempo, e do custo de implementação, esse ambiente consegue nos trazer com mais detalhes o comportamento de invasores. Porém se for mal configurado, ou cair em mãos de indivíduos sem o conhecimento necessário, o risco de comprometimento da rede aumenta, servindo por exemplo, de base para novos ataques. Nesse sentido, vamos exemplificar os *Honeypots* de alta interatividade como um serviço real que pode ser configurado e comprometido para servir de isca para capturar informações com precisão de indivíduos mal-intencionados.

3.5 VANTAGENS E DESVANTAGENS NO USO DE HONEYPOTS

3.6 FERRAMENTAS UTILIZADAS

AQUI AINDA NÃO SEI AS FERRAMENTAS QUE SERÃO UTILIZADAS

4 ESTUDO DE CASO

AQUI NÃO SEI O QUE FAZER KKK

5 RESULTADOS OBTIDOS

6 CONCLUSÃO

6.1 TRABALHOS FUTUROS

REFERÊNCIAS

MARCELO, Antonio; ALVES, Marcos José Pitanga. **Honeypots A arte de iludir hackers**. Rio de Janeiro: Brasport, 2003. 98 p.

BIAZIN, D. T. **Normas da ABNT e padronização de trabalhos acadêmicos**. Londrina: Instituto Filadélfia de Londrina; 2008.

BUNEMAN, P.; CHENEY, J.; LINDLEY, S. et al. **DBWiki**: A Structured Wiki for Curated Data and Collaborative Data Management. Athens: SIGMOD'11; 2011.

WIKIBOOKS. **LaTeX**: The Free Textbook Project. Disponível em: <http://en.wikibooks.org/wiki/LaTeX>. Acesso em: 09 abr. 2014.