UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

CARLOS ANTÓNIO KOMBO

MONITORAMENTO DE INVASÕES, SIMULAÇÃO DE ATAQUES DE UM SERVIDOR HONEYPOT EM AMBIENTE CONTROLADO

CRICIÚMA

2019

CARLOS ANTÓNIO KOMBO

MONITORAMENTO DE INVASÕES, SIMULAÇÃO DE ATAQUES DE UM SERVIDOR HONEYPOT EM AMBIENTE CONTROLADO

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Esp. Marcel Campos Inocencio

CRICIÚMA

2019

CARLOS-ANTÓNIO KOMBO

MONITORAMENTO DE INVASÕES, SIMULAÇÃO DE ATAQUES DE UM SERVIDOR HONEYPOT EM AMBIENTE CONTROLADO.

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em segurança da informação.

Criciúma, 03 de dezembro de 2019.

BANCA EXAMINADORA

Prof. Marcel Campos Inocencio - Esp. - (UNESC) - Orientador

Prof. Paulo Joãõ Martins - Me. - (UNESC)

Prof. Rogério Antonio Casagrande - Dr. - (UNESC)

Aos meus queridos pais, verdadeiros heróis. Aos meus irmãos pelo suporte de sempre e aos amigos pela energia positiva.

AGRADECIMENTOS

Primeiramente a Deus, que sempre me capacitou e me abençoou ao longo dessa jornada. Ao meu pai, meu herói que fez de mim o homem que sou hoje, a grande rainha minha mãe, pelo seu amor incondicional. Aos meus irmãos por me inspirarem a continuar lutando nos momentos difíceis, e aos amigos pelo apoio direta ou indiretamente.

Agradeço também ao meu orientador Marcel Campos Inocencio por me orientar e direcionar aos caminhos que me levaram a desenvolver o trabalho de conclusão de curso. Agradeço a academia pelos longos anos de aprendizagem, a todos os professores pelo conhecimento passado e aos colegas que fizeram parte da minha jornada.

“O modo como você reúne, administra e usa a informação determina se vencerá ou perderá.”

Bill Gates

RESUMO

A incessante busca, a distribuição e o processamento da informação, tem sido o grande combustível das organizações nessa nova era digital, assim sendo, a segurança da informação tem se tornado um fator cada vez mais indispensável, devido ao valor que ela agrega para uma organização. É essencial que as ferramentas utilizadas para auxiliar na sua proteção sejam sempre atualizadas e atendam da melhor maneira possível. O trabalho apresenta um estudo sobre monitoramento de invasões, simulação de ataques de um servidor *honeypot* em ambiente controlado. Onde o objetivo é implantar uma ferramenta de monitoração de ataques a um servidor e simular invasões, criando um ecossistema na instância do *google cloud* com a implantação do T-POT *honeypot*, a fim de analisar toda coleta de ataques e reforçar cada vez mais as políticas de segurança da informação, com as devidas recomendações de melhorias e técnicas de solução. Em testes realizados com a ferramenta, assim como todos os logs gerados durante o período que esteve monitorando a rede, o servidor online recebeu ataques que não eram simulações, e os resultados apresentados demostram que a mesma é ideal para a análise e auxilio na segurança da informação.

Palavras-chave: Segurança da informação. *Honeypots*. T-Pot. Ataques. Redes de computadores.

ABSTRACT

The relentless pursuit, distribution, and processing of information, has been a major fuel for organizations in this new digital age, so information security has become an increasingly indispensable factor because of the value it adds to an organization. It is essential that the tools used to help protect you are always up to date and in the best possible way. The paper presents a study on intrusion monitoring, simulation of attacks from a honeypot server in a controlled environment. Where the goal is to deploy an attack monitoring tool to a server and simulate intrusions by creating an ecosystem on the google cloud instance with the T-POT honeypot deployment to analyze all attack collection and increasingly enforce policies information security, with appropriate improvement recommendations and solution techniques. In tests conducted with the tool, as well as all logs generated during the period that was monitoring the network, the online server received attacks that were not simulations, and the results show that it is ideal for analysis and assistance in the security of the network information.

Keywords: Information Security. Honeypots. T-Pot. Attacks. Computer network.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DOS	Denial of Service
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Eletronics Engineers
ISO	International Organizational for Standardization
LOG	Arquivo de Registro de Informações
PCS	Personal Computers
POP3	Post Office Protocol
S.O	Sistema Operacional
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
DTAG	Deutsche Telekom
SSH	Secure Shell
NMAP	Network Mapper
IP	Internet Protocol
WIFI	Wireless Fidelity
PING	Packet Internet Network Grouper
LAN	Local Area Network
RAM	Random Access Memory
SSD	Solid State Drive
PaaS	Platform-as-a-Service
VM	Virtual Machine
VNC	Virtual Network Computing

SUMÁRIO

1 INTRODUÇÃO

O crescimento das tecnologias tem proporcionado uma manipulação mais rápida e melhor das informações, e nesse universo todo, um dos principais focos em várias organizações é a questão da segurança. Tendo em conta a proporção de sistemas computacionais e o grande fluxo de dados dentro de uma rede, não importando se é uma grande ou pequena empresa (HIDALGO; PEREIRA, 2018).

A globalização tem permitido rápidos avanços tecnológicos, as oportunidades de negócios vêm e vão com a mesma velocidade desses avanços. Todos experimentam uma época de grandes transformações tecnológicas, econômicas e mercadológicas (NAKAMURA; GEUS, 2007).

As parcerias estratégicas e a maneira de comunicação avançam, de tal modo que as infraestruturas de rede com vital importância para os negócios, passam a ser uma peça fundamental para o contexto atual, de grandes mudanças comerciais e mercadológicas. Acrescentando a importância cada vez mais da finalidade da Internet, fazendo com que um novo ambiente surja, no qual múltiplas empresas trocam informações por meio de uma rede adaptada. Informações técnicas, comerciais e financeiras, necessárias para o bom prosseguimento dos negócios, uma vez que, estes agora trafegam por essa rede, que conecta matrizes com suas filiais, assim como seus clientes, seus parceiros comerciais, seus distribuidores e todos os seus usuários móveis (NAKAMURA; GEUS, 2007).

Por ser uma rede composta, a sua complexidade atinge níveis aceitáveis, o que requer uma série de cuidados e medidas que devem ser tomadas, sobretudo em relação à proteção das informações contidas nessa rede (NAKAMURA; GEUS, 2007).

Dependendo de quão sensível for a informação para a organização e, obviamente, dependendo do seu valor diante dos concorrentes ou para o mercado, a empresa precisa implementar controles sobre o uso (mesmo correto) dessas informações (FONTES, 2006).

O fato é que com a evolução destas tecnologias, onde novas ferramentas são criadas, novos equipamentos são desenvolvidos, as organizações de pequeno, médio e grande porte, passaram a aplicar e a experimentar cada vez mais essas inovações. Considerando as limitações de armazenamentos iniciais, o avanço do uso desses novos conhecimentos, as informações e os sistemas em si,

deixam de estar no modo seguro e passam a estar susceptíveis aos mais variados tipos de ataque ou invasões, que podem ser provenientes de usuários mal-intencionados, ou até mesmo de um órgão qualquer (SÊMOLA, 2003).

Surge, então, a necessidade de auxiliar na segurança dessas informações ou dados, e esse processo exige uma boa forma e prática de proteção, por meio de ferramentas que coletam dados de invasores com intuito de entender as finalidades dos seus ataques e melhorar as proteções dos dados e servidores. Ferramentas como *Honeypot*, que significa “pote de mel” tem como finalidade registrar os ataques, permitindo medidas preventivas, bem como sua utilização para esclarecer a forma como os ataques são efetuados, para os servidores reais. A ideia do mesmo é funcionar como uma armadilha para que os atacantes possam pensar que estão realmente invadindo um ambiente, enquanto seus dados são coletados e o servidor principal fica longe do alcance dos ataques (RODRIGUES; SOUZA; DINIZ, 2015).

Além das funcionalidades citadas, o *honeypot* serve ainda para descobrir a forma como novos ataques são efetuados. Rastreando o passo a passo do invasor, é possível identificar qual vulnerabilidade foi utilizada, para obter o acesso a rede ou sistema.

As empresas de pequeno porte não investem muito na questão de segurança, e precisam tomar medidas nesse sentido, nomeadamente: exigirem a construção de senhas robustas e a sua alteração periódica, definirem e divulgarem uma prática de utilização da Internet, aplicarem mecanismo de controle e bloqueio de utilização da Internet, bloquearem a ligação de dispositivos de armazenamento externos, definirem rotinas de *backup* automático dos arquivos de trabalho para servidores específicos (PIMENTA; QUARESMA, 2016). Assim como também, devem buscar ampliar seus investimentos em mais proteções da informação (COMUNICAÇÃO, 2018).

1.1 OBJETIVO GERAL

O objetivo deste trabalho é implantar uma ferramenta de monitoração de ataques a um servidor e simular invasões em um ambiente controlado.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são:

1) Identificar principais tipos de ataques ao servidor;
2) Instalar a ferramenta *honeypot* para coletar dados de invasões;
3) Simular ataques a fim de validar a coleta de informação gerada pelo *honeypot;*
4) Analisar resultados gerados a fim de minimizar as vulnerabilidades do servidor.

1.3 JUSTIFICATIVA

A necessidade de se proteger a informação dentro de qualquer organização é muito importante, pois a informação, independentemente de seu formato, é um ativo importante da empresa. Os ambientes e os equipamentos utilizados para o seu processamento, seu armazenamento e sua transmissão devem ser protegidos. Devido à dificuldade de se garantir a segurança da informação, pois, por mais que se busque garanti-la, sempre haverá falhas. Serviços de segurança como autenticação, controle de acesso, auditoria e criptografia devem ser projetados e implementados como parte integrante das plataformas de serviços em redes (FONTES, 2006).

Quando se trabalha em organizações, é preciso lembrar que a informação é um bem, e que ela tem um grande valor para a empresa e deve ser protegida, cuidada por meios de políticas e regras, da mesma maneira que os recursos financeiros e materiais são tratados dentro da instituição (ABNT, 2005). Uma forma de prevenção é a detecção das tentativas de invasão, para que seja gerada uma notificação ao administrador de rede ou uma documentação, de modo a servir como referência a mecanismos de segurança, procurando assim evitar que as mesmas anomalias ou falhas ocorridas possam ser repetidas posteriormente (MODOLON, 2010). Por esse motivo, pode-se utilizar um Sistema de Detecção de Intrusão (IDS), cuja função principal, é de monitorar e analisar as possíveis tentativas de invasões, que possam ocorrer em um ambiente computacional de uma empresa.

A análise e o estudo dessas tentativas são importantes para que possam ser prevenidos novos ataques. Há necessidade de ferramentas mais específicas para isso, como por exemplo, os *honeypots*, ferramentas que têm como objetivo serem atacados e invadidos, gravando todas as informações do ataque efetuado. Bruce Schneier (SCHNEIER, 2004), perito em criptografia, fundador e diretor da *Counterpane Internet Security*, decompõe a segurança em três domínios distintos: prevenção, detenção e reação, sendo que, o *honeypot* demostra-se útil nas três categorias. *Honeypot* não impede um atacante de entrar na rede, mas quando o invasor cai na armadilha do honeypot as suas ações ficam registradas e podem ser analisadas, possibilitando a prevenção de novos ataques dessa natureza.

A utilização desta tecnologia permite cada vez mais trazer ao centro das discussões, técnicas e ferramentas com grande utilidade no quesito da segurança, permitindo assim monitorar todo tipo de atitude tomada por atacantes dentro de um servidor.

No curso de Ciência da Computação existe um trabalho de conclusão de curso, no qual foi utilizada a ferramenta *honeypot honeyd,* cuja ideia é imitar vários diferentes tipos de servidores, permitindo ao utilizador simular um número infinito de configurações de redes de computadores. Uma visão aplicada em um ambiente virtual de laboratório (máquinas virtuais). A mesma ferramenta também se encontra obsoleta, ela foi descontinuada pelos seus desenvolvedores. Já para este trabalho será utilizada a ferramenta *honeypot T-Pot,* que é uma ferramenta mais atualizada, baseada em Debian Server, contendo vários sensores honeypots paravirtualizados (virtualização que usa o próprio kernel da máquina hospedeira) em *docker* container, como alguns deles: *dionaea, conpot, tanner, cowrie, honeytrap* e o sistema de detecção de intrusão suricata. Será aplicado e testado em um ambiente controlado, onde o servidor ficará monitorando a rede por um período que se estende de 28 de setembro até 25 de outubro, ou seja, por um período de 27 dias.

Após, então, serão efetuadas simulações de invasão, para ao final, já com os resultados obtidos analisar os logs e recomendar as ações necessárias para melhorias no que tange a proteção, garantindo assim a integridade, confiabilidade e a disponibilidade da informação que são processadas, armazenadas e distribuídas na rede. É o que se busca com esse trabalho. Serão simulados ataques como: *brute force, denial of service e scans com nmap, sparta e nikto.*

Este trabalho busca atualizar a bibliografia, os softwares e descobrir as novas técnicas de invasões e ataques em relação ao trabalho anterior.

1.4 ESTRUTURA DO TRABALHO

O trabalho está dividido em sete capítulos. Sendo que o primeiro capítulo apresenta uma breve descrição sobre o tema do trabalho, contendo a introdução, o objetivo geral, os objetivos específicos e a justificativa do mesmo.

O segundo capítulo aborda assuntos relacionados à segurança da informação, a sua importância, o motivo de ser um fator importante para uma organização, ativos, pilares da informação, princípios de prevenção e proteção, métodos de avaliação de segurança e também sobre a política de segurança, o que é e o porquê se aplicar, assim como questões referentes a vulnerabilidades, riscos, ameaças e ataques e serviços de redes.

O terceiro capítulo trata do levantamento teórico referente a tipos de ataque, formas de ataque, motivação dos atacantes e exemplos de casos reais de ataque.

O quarto capítulo apresenta conceitos concernente aos *honeypots*, o que são, para que servem, os níveis de interação, a sua importância, os tipos, sua localização na rede, e um breve estudo de forma objetiva sobre virtualização, *docker* e containers.

No quinto capítulo são apresentados trabalhos correlatos que foram realizados na mesma linha de pesquisa ao trabalho desenvolvido.

O sexto capitulo apresenta a apresenta a estrutura referente ao trabalho desenvolvido, onde se aborda a metodologia aplicada para a implantação da ferramenta, a coleta dos ataques, assim como os análises dos resultados obtidos dentro desse cenário elaborado.

O sétimo e último capítulo apresenta a conclusão do trabalho desenvolvido.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação diz respeito a proteção existente sobre as informações de uma certa empresa ou ainda uma pessoa, ou seja, aplica-se tanto aos dados corporativos quanto aos pessoais. A segurança de uma determinada informação pode ser comprometida por fatores comportamentais e de uso de quem à utiliza, pelo ambiente ou infraestrutura que a cerca ou ainda, em alguns casos por pessoas mal-intencionadas com o objetivo de roubar, destruir ou alterá-la (DIAS, 2000).

A segurança da informação refere-se a um conjunto de procedimentos, políticas e ações onde a finalidade é a proteção das informações, permitindo assim, que o negócio da organização não tenha interrupções e que sua missão seja alcançada (FONTES, 2006).

A segurança da informação em si não deve ser tida como um estado a ser alcançado, onde uma vez alcançado não seja mais necessário se preocupar, mas sim como um processo, pois nada é completamente seguro, porém, com um nível de segurança que seja considerado como aceitável. Por esta razão, não há como afirmar que algo que se considere seguro, permanecerá seguro, sendo que a todo momento surgem novas ameaças, e com isso o risco para a segurança aumenta, ainda mais com a evolução e uso da Internet (WADLOW, 2000).

A necessidade de segurança é uma realidade que vai além do limite de produtividade e da funcionalidade. Quando se considera a eficiência e a velocidade em todos os processos de negócios como uma vantagem competitiva, a ausência de segurança nos meios que habilitam as tais eficiência e velocidade pode ocasionar em grandes prejuízos e falta de novas oportunidades de negócio (NAKAMURA; GEUS, 2007).

A ideia principal da segurança da informação é reduzir ao máximo qualquer tipo de risco concernente ao vazamento de dados, tendo em conta que na maioria dos casos o maior inimigo pode estar dentro da própria empresa. Deste modo, é necessário um conjunto de técnicas, procedimentos e ferramentas para garantir a melhor proteção possível para a informação (BARBOSA; SILVA, 2016).

Garantir que haja segurança, é uma das maneiras mais básicas e prioritárias de uma rede corporativa, e para todos os recursos utilizados através desta. Esse processo se fundamenta em tecnologias e métodos específicos, com a

ideia de preservar as três propriedades, que definem a segurança de uma rede. O crescimento das empresas, e o seu interesse em se conectar a Internet, movidas pela possibilidade de usá-las, para tornar mais conhecido os seus negócios, traz uma série de preocupações, especialmente a segurança dos dados. Nos tempos atuais, em que a informação se tornou um bem tão valorizado quão o próprio patrimônio das empresas. Os firewalls são sistemas que controlam, e permitem o acesso de fora para dentro e vice-versa, somente a aqueles usuários autorizados, evitando dessa forma, acessos indevidos, sejam eles de usuários internos da rede, tentando acessar sites não autorizados na Internet, ou ainda acesso de usuários externos, como hackers, vindos pela Internet para a sua rede interna (STARLIN; NOVO, 2000).

Toda e qualquer informação tem um valor para a empresa, de igual modo para a concorrência e para o mercado em que ela atua. Na área de serviços, o cadastro de clientes, por exemplo, tem um valor importantíssimo e deve haver uma proteção adequada (FONTES, 2006).

Ainda segundo Nakamura e Geus (2007), a questão da segurança, tanto no que concerne à violência urbana ou em hackers, é especifico. Marcado por uma evolução continua, onde novos ataques implicam em novas respostas, novas formas de proteção, que despertam o desenvolvimento de novas técnicas de ataques, de modo que é possível observar a formação de um ciclo. Tanto que não é por coincidência que é exatamente no elo mais fraco que os ataques acontecem.

No mundo da informação a segurança deve ser continua e evolutiva, tudo porque o conjunto de defesa utilizado pelas empresas pode funcionar contra determinados tipos de ataque, entretanto, pode não ter a mesma efetividade contra novas técnicas desenvolvidas para burlar esse conjunto de defesa (NAKAMURA; GEUS, 2007).

Segundo Junior e Kon (2007) atualmente os problemas em relação a proteção dos dados são mais discretos, porém, longe de serem menos importantes. Com o envolvimento e crescimento cada vez mais das tecnologias nas organizações, instituições governamentais e até mesmo em habitações de milhares de pessoas, o perigo de uma possível ameaça às informações prioritárias e de suma importância se faz presente todo o momento.

As empresas realizam os seus negócios diariamente, utilizando a Internet como meio de comunicação. Bancos têm disponibilizado as suas transações

financeiras por meio de redes públicas de dados e alterações de informações podem causar resultados desastrosos.

Um sistema é tido como seguro quando se pode depender dele e seu software apresentar comportamentos esperados (JUNIOR; KON, 2007).

Sabe-se, todavia, que criar um sistema computacional totalmente seguro é extremamente difícil (se não impossível), mas, no entanto, é preciso definir quais limites dos riscos aceitáveis. Questões como: Quais serviços serão disponibilizados externamente, quais são os controles necessários para o sistema e o nível de segurança desejado, respondem o escopo do problema a ser delineado (GARFINKEL; SPAFFORD; SCHWARTZ, 2003).

Cerca de 75% dos documentos que são arquivados em servidores das empresas contêm informações sigilosas, que poderiam causar algum estrago, caso caíssem em mãos de pessoas mal-intencionadas (FONTES, 2006).

A propriedade intelectual é uma informação frequentemente cobiçada pelos concorrentes. Dependendo do tipo de negócio, um vazamento (por um erro ou ainda por ações de má-fé) pode originar em perdas irreparáveis, comprometendo a empresa no mercado. Para escapar desse tipo de problema, o procedimento mais indicado deve ser o acesso restrito às cópias de segurança, destruição de informação que perdeu utilidade, registro de acessos à informação e comprometimento dos usuários com a proteção da informação (FONTES, 2006).

Quando não implementados os controles mínimos, pode ocorrer o vazamento de informações, sem que a empresa detecte. Algumas vezes, são evidências no mercado e nas organizações concorrentes que despertam a empresa para o fato ocorrido (FONTES, 2006).

Toda e qualquer organização está susceptível a vazamento de informação. Grande parte, o fato acontece exatamente com a participação de pessoas que atuam internamente na empresa, por intermédio de pessoas que tinham autorização para acessar a informação. Infelizmente, sucedem casos em que muitas dessas pessoas utilizam essa autorização para praticar um delito (FONTES, 2006).

2.1 ATIVOS DA EMPRESA

Ativos é o conjunto de todos os bens que a empresa possui, tais como: imóveis, móveis, veículos e um dos mais valiosos, a informação. A informação precisa ser difundida por canais seguros, com o intuito de que possam conter confiabilidade e integridade que se precisa em seus conteúdos (MOREIRA, 2001).

Todo e quaisquer bens pertencente a empresa, são seus ativos, a começar pelos ativos de informação até imóveis, e assim como todo bem valioso, precisa ser protegido. Na visão de Sêmola (2003), ativo é todo elemento que compõe os processos que manipulam e processam a informação, tais como equipamentos, aplicações, usuários, ambientes, a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

Os ativos precisam ser identificados, registrados e possuírem proprietários que zelam pela sua manutenção, segurança e controle adequado para a sua manipulação (CARDOSO, 2013).

É necessário que uma vez identificados todos os ativos, a empresa documente também a importância desses ativos, convém que o inventário do ativo abranja todas as informações indispensáveis que permitam a recuperação de um possível desastre, incluindo o tipo de ativo, formato, localização, informações concernentes a cópia de segurança, informações concernentes a licença e a importância do ativo para o negócio (ABNT, 2005).

Ainda de acordo com a norma ABNT (2005), existem diversos tipos de ativos, tais como:

1) Ativos de informação: refere-se a base de dados e arquivos, assim como todos os contratos e acordos, documentação de sistema, informações relacionadas a pesquisa, manuais de usuário, material, de treinamento, procedimentos de suporte ou operação, procedimentos de recuperação, planos de continuidade de negócio, auditoria e informações armazenadas;
2) Ativos de software: baseiam-se em sistemas, aplicativos e ferramentas de desenvolvimento e utilitários;
3) Ativos físicos: são relativos a equipamentos computacionais, mídias removíveis, equipamentos de comunicação e os demais equipamentos;

4) Serviços: refere-se a serviços de computadores e comunicação, bem como utilidades gerais, nomeadamente: aquecimento, iluminação, eletricidade e refrigeração;
5) Pessoas e suas qualificações: diz respeito à habilidades e experiências;
6) Intangíveis: concerne a reputação e a imagem da organização.

2.2 PILARES DA INFORMAÇÃO

A identificação da informação, e seus pilares dentro de uma organização, são essenciais para estabelecer as melhores práticas, e métodos para sua segurança. A informação produzida por uma empresa deve ser cautelosamente classificada e organizada, e assim, protegida para que haja prosseguimento dos negócios (LYRA, 2008).

Ainda conforme Lyra (2008), quanto aos pilares da informação tem-se:

a) Confidencialidade: diz respeito à capacidade de um sistema permitir ou não o acesso de usuários específicos;
b) Integridade: mostra a exatidão e a validade da informação, sem alterações;
c) Disponibilidade: a informação deve estar sempre disponível para ser acessada;
d) Autenticação: Significa confirmação de autoria de usuário;
e) Não repúdio: é quando o sistema é capaz de provar que um usuário realizou uma determinada tarefa;
f) Privacidade: é a capacidade de um sistema em manter o sigilo das suas informações, garantindo assim a reserva de todos os dados da empresa;
g) Auditoria: define-se como a capacidade do sistema em identificar e registrar todas ações realizadas por usuários.

Ainda de acordo com Lyra (2008), sobre os pilares da informação, na confidencialidade tem-se quatro níveis:

a) Informação pública: nesse caso são informações que não possuem um impacto direto para empresa ainda que forem divulgadas

externamente, pois a sua essência está na capacidade de ser divulgada para todos de forma geral. Um exemplo claro seria o catálogo dos produtos;

b) Informação interna: as informações possuem aspectos ligadas a organização, porém se divulgadas não haverá consequências críticas;
c) Informação confidencial: são informações categorizadas como restritas e protegidas, tendo em conta o potencial risco de perdas relacionado a nível financeiro. Exemplo: Senhas de acesso, dados de clientes e muito mais;
d) Informação secreta: refere-se às informações importantíssimas para os negócios da organização, por essa razão o seu acesso deve ser restrito a pessoas de confiança, devendo estabelecer regras e critérios para o seu uso e aplicação. Exemplos: Contratos confidencias, informações militares.

Uma pesquisa revelou que em apenas 17% das empresas, a segurança da informação atinge as finalidades ambicionadas, ou seja, é eficaz, pois a ineficácia na área de segurança atinge 83% das empresas. E nesse panorama, 93% estão mantendo ou melhorando seus investimentos em segurança para reagir contra a crescente ameaça dos ataques cibernéticos (PWC, 2018).

As empresas pretendem e almejam a privacidade e segurança, e não a privacidade ou a segurança. E elas precisarão de métodos para cumprir essa expectativa (PWC, 2018).

2.3 PRINCIPIOS DE PREVENÇÃO E PROTEÇÃO

Os princípios de prevenção e proteção da informação utilizada nos sistemas de informação requerem medidas de segurança, que em muitos casos servem também como formas de garantir a autenticidade da informação. Todas essas medidas, além do seu objetivo, precisam ser implementadas muito antes da concretização do risco, isto é, antes dos eventos inesperados ocorrerem (ARAUJO, 2008).

Conforme demostra a figura 1, a estrutura dos três princípios básicos que regem a segurança da informação.

Figura 1 – Princípios de segurança da informação

Fonte: Araújo (2008).

Para aplicarem-se as medidas de forma a garantir a segurança da informação, e saber quais devem ser adotadas para a proteção, deve-se definir alguns objetivos e identificar o que se quer proteger, de quem, a que custos, e quais os riscos.

Ferreira (2003, p.3) destaca que:

> Antes de implementar um programa de segurança de informações, é aconselhável definir nosso universo computacional, deve-se responder as seguintes perguntas:
> • O que deve proteger?
> • Contra que ou quem?
> • Quais as ameaças mais prováveis?
> • Qual a importância de cada recurso?
> • Qual o grau de proteção desejado?
> • Quanto tempo, recurso humano e financeiro pretende-se gastar para atingir os objetivos de segurança desejados?
> • Quais as expectativas dos usuários e clientes em relação à segurança das informações?
> • Quais as consequências para a organização se os sistemas e informações forem corrompidos ou roubados?

Quando se pensa na necessidade de segurança, a ideia é reduzir certos riscos: Fraude, acesso indevido, uso indevido, sabotagem, erros (ARAUJO, 2008).

Ainda segundo Fontes (2006), a ideia de a segurança da informação existir é para reduzir os riscos do negócio quanto a necessidade do uso de recursos de informação para o funcionamento da empresa. Sem a informação ou se porventura, ela estiver incorreta, as chances de haver perdas que comprometam o desempenho da organização são grandes, afetando de igual modo o retorno de investimento dos acionistas.

Os eventos inesperados estão crescendo cada vez mais não só porque existem ameaças, mas também porque certas empresas se posicionam de modo a investir em novas tecnologias para detectá-las melhor. Nessa sequência, a maior detecção de incidentes deve ser visível como sendo um acontecimento positivo (PWC, 2014).

2.3.1 Métodos de avaliação da segurança

De acordo com Hagen (2008), existem algumas metodologias que buscam medir o índice de implementação de medidas organizacionais de segurança de informação e a eficácia destas mesmas metodologias uma vez implementadas.

Ainda segundo Hagen (2008), essa eficácia pode ser observada de quatro maneiras ou perspectivas inter-relacionadas:

a) Perspectiva da gestão de riscos: medidas de segurança da informação têm a obrigação de reduzir de forma aceitável o risco de incidentes de indesejáveis;
b) Perspectiva econômica: medidas de segurança da informação que retornam positivamente nos investimentos;
c) Perspectiva legal: medidas de segurança da informação com intuito de evitar a violação de requisitos legais;
d) Perspectiva cultural: medidas de segurança da informação precisam criar uma boa cultura de segurança.

Hagen (2008) ainda afirma que, as medidas organizacionais em segurança da informação, podem ser divididas em quatro grupos, e os mesmos nos seguintes itens:

a) Política de segurança: implementação de políticas de segurança da informação - item único;

b) Procedimentos e controles: constituído por itens como - rotinas de segurança para o pessoal contratado, instruções de uso, acordos de confidencialidade e processos disciplinares;
c) Ferramentas e métodos: classificação de ativos, análise de riscos, auditoria interna, auditoria externa, indicadores de chave de desempenho, sistemas de notificação e planos de tratamento de incidentes são alguns itens que compõem esse grupo;
d) Criação de sensibilização: grupo composto por cinco itens - formação/educação, campanhas da alta gerencia, participação por parte do usuário, envolvimento da alta gerencia, envolvimento em todas as partes da organização como um todo em processos de aprendizagem a partir de eventos inesperados.

As medidas de segurança estão sujeitas a serem classificadas de acordo com a maneira como abordam as ameaças, em dois âmbitos: prevenção e proteção.

A prevenção refere-se a um conjunto de medidas que se destina a minimizar a probabilidades de efetivação de ameaças existentes. Quando uma ameaça se torna um incidente, é frequente que os efeitos dessas medidas de segurança desapareçam.

Já a proteção, por sua vez, está relacionada ao conjunto das medidas que se propõem a equipar os sistemas de informação com capacidade de monitorar, examinar, detectar, ter reações e reflexos, permitindo assim amenizar e limitar o impacto causado pelas ameaças quando estas chegam a se concretizar. Normalmente essas medidas só atuam caso ocorra um incidente (SILVA; CARVALHO; TORRES, 2003).

2.3.2 Riscos e considerações quanto à segurança

De acordo com Nakamura e Geus (2007), vários aspectos importantes que precisam ser levados em consideração quando se estabelece uma rede como parte integrante de uma empresa. Alguns dos riscos presentes, assim como algumas considerações a serem feitas são:

e) A falta de uma classificação das informações relativamente ao seu valor e a sua confiabilidade, que serve de base para estabelecer uma estratégia de segurança apropriada. Isso resulta em um fator de risco

para a empresa, para além de tentar impedir o dimensionamento das perdas originadas por ataques;

f) O controle de acesso mal definido faz com que os usuários autenticados no início da conexão, tenham acesso absoluto em todas as partes da rede interna, incluindo as partes do sistema que não são necessárias para a realização de suas tarefas;
g) A dificuldade do administrador em relação ao controle sobre todos os sistemas da rede interna, gera situações não confiáveis. Os bugs nos sistemas operacionais ou nos softwares utilizados por esses equipamentos podem ocasionar brechas na rede interna;
h) A Internet deve ser vista como um ambiente desfavorável e, logo, não confiável. Deste modo, todos os usuários devem ser considerados não confiáveis e potencias atacantes;
i) As informações que trafegam pela rede são passiveis a serem capturados;
j) As senhas que trafegam pela rede estão sujeitas a serem capturadas;
k) Os e-mails podem ser lidos, capturados, modificados e falsificados;
l) Toda conexão entre a rede interna e qualquer outro ponto pode ser devidamente utilizada para ataques a rede interna;
m) Novas tecnologias significam novas vulnerabilidades.

Ainda conforme Nakamura e Geus (2007) é preciso entender que essas considerações não só revelam o quanto a segurança é abrangente, mas também como ela é multidisciplinar. Proteger alguns pontos e descuidar de outros pode comprometer totalmente a empresa, visto que os incidentes sempre ocorrem no elo mais fraco da rede, ou seja, no ponto mais vulnerável do ambiente. Todos os níveis de segurança devem ser considerados para que a informação, que é o maior bem da organização, seja protegida. Desde o sistema operacional, é necessário avaliar e considerar também os protocolos, os serviços, as redes, as aplicações, os usuários e as instalações físicas envolvidas com a informação.

A importância da segurança cresce cada vez mais, quando se leva em conta o rápido aumento da complexidade das conexões, o que é muito característico nos ambientes corporativos. Um ponto essencial, quando se discute a questão da segurança, é que ela é inversamente proporcional às funcionalidades, ou

seja, quanto maiores as funcionalidades, como serviços, aplicativos e as demais facilidades, menor é a segurança desse ambiente (NAKAMURA; GEUS, 2007).

Nakamura e Geus (2007), ainda destacam que a segurança pode ser comprometida pelos seguintes fatores:

a) Exploração de vulnerabilidades em sistemas operacionais, aplicativos, serviços e protocolos;
b) Falha no desenvolvimento e na implementação da política de segurança;
c) Falha na configuração de serviços e sistemas de segurança;
d) Desenvolvimento de ataques mais sofisticados.

2.4 POLITICA DE SEGURANÇA

De acordo com Nakamura e Geus (2007), a política de segurança é a base por todas questões referentes a segurança da informação, exercendo um papel importantíssimo em toda e qualquer empresa. A obrigação de estabelecer uma política de segurança é um fato evidenciado coletivamente do meio empresarial, pela norma *International Standardization Organization/International Elecrical Technical* (ISO/IEC).

Ainda na visão de Nakamura e Geus (2007), a construção da política de segurança é o primeiro e o principal passo de uma estratégia de segurança dentro de uma organização. É por meio dessa política que os demais aspectos envolvidos na proteção dos recursos existentes são estabelecidos, sendo assim, grande parte do trabalho é dedicado à sua elaboração e ao seu planejamento.

A política de segurança de informações é um modo de precaver a proteção dos dados e atividades importantes dentro de uma organização que estabelece um padrão de segurança a ser posto em prática pelo corpo técnico e gerencial e pelos usuários, internos e externos. A política de segurança deve se responsabilizar em estabelecer princípios institucionais de como a empresa irá proteger, controlar e monitorar todos os seus recursos computacionais e consequentemente as informações por elas manipuladas (DIAS, 2000).

É necessário que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e distinga as principais ameaças, riscos e impactos envolvidos (DIAS, 2000).

De acordo com Guimarães, Lins e Oliveira (2006, p.12),

> É importante que a política de segurança defina os perímetros de segurança da rede. Isso impõe limite e organiza a rede da organização. Como por exemplo, define uso, responsabilidades, normas e detalhes de planos e ações destinados a responder sobre violação de sua política. Lista o que é permitido ou não na rede e nos sistemas de sua organização.

A política de segurança baseia-se em um conjunto de normas, métodos e procedimentos usados e aplicados para a manutenção da segurança da informação, com a obrigação de ser formalizada e divulgada a todos os usuários que fazem o uso dos ativos de informação (FERREIRA; ARAUJO, 2008).

> A política deve possuir a assinatura do principal executivo aprovando-a, a data da última atualização e do início de sua vigência. Estas informações são importantes, pois ajudam a controlar suas revisões e atualizações periódicas (FERREIRA; ARAÚJO, 2008, p.43).

Segundo Ferreira e Araújo (2008), para as políticas de segurança é indispensável que possuam caraterísticas gerais para a qualidade no que se refere a sua implementação, tais como:

a) Simples e compreensíveis: sem processos cansativos e irrelevantes, com facilidade de entendimento e aplicação;
b) Homologadas e assinadas pela alta administração: ter a permissão do nível hierárquico e superior é fundamental;
c) Estruturadas de forma a permitir a sua implantação por fases: os níveis de aplicabilidade precisam ser definidos para atenuar e medir o impacto no negócio;
d) Orientadas aos riscos: onde a segurança das políticas é obrigada a priorizar os riscos existentes;
e) Flexíveis e preventivas: tendo a possibilidade de ser adaptados de acordo com as novas tecnologias e processos que protejam e previnam a perda de dados.

2.5 VULNERABILIDADES

As vulnerabilidades referem-se as fragilidades presentes na organização, exploradas pelas ameaças. São debilidades existentes ou agregadas a ativos que manipulam e processam informações, que ao ser sondadas por ameaças, possibilita a ocorrência de eventos inconvenientes na segurança, atingindo de forma negativa um ou mais princípios da segurança da informação (SÊMOLA, 2003).

Uma vulnerabilidade pode ser entendida como uma falha no projeto ou na implementação de software ou até mesmo no sistema operacional, e quando explorada por um atacante ocasiona em uma violação de segurança do computador (SMITH, 2007).

Todos os sistemas são vulneráveis, partindo da ideia de que não existem sistemas totalmente seguros. Muitas vezes, as medidas de segurança adotadas pelas empresas possuem vulnerabilidades. Diante disso, a ineficiência de medidas de proteção, em função de configurações inapropriadas é uma das causas (MOREIRA, 2001).

Ainda conforme Moreira (2001), medidas de segurança são ações como procedimentos, software, configurações, hardware e técnicas aplicadas para atenuar as vulnerabilidades, com o intuito de reduzir as chances de ocorrência da ação de ameaças.

Sêmola (2003), ainda destaca que as fragilidades podem ser:

a) Físicas: concerne às instalações prediais que se encontram fora dos parâmetros, como: salas mal idealizadas e com falta de extintores, detectores de fumaça e outros tipos de recursos usados para o combate a incêndio em sala de armários e arquivos estratégicos, risco de explosões e vazamentos ou incêndios;

b) Naturais: refere-se a computadores, que por sua vez são susceptíveis a desastres naturais, como incêndio, enchentes, terremotos, tempestades, e outros, como o caso de falha de energia, acúmulo de poeira, aumento de humidade e temperatura;

c) Hardware: brecha nos recursos tecnológicos, desgaste, enfraquecimento, mau uso ou ainda erros durante a instalação;

d) Software: tem a ver com erros de instalação ou na configuração, podendo causar como consequência acessos indevidos, fuga de

informações, perdas de dados ou indisponibilidade de recursos quando necessário;

e) Mídia: os discos, fitas, assim como relatórios impressos podem ser perdidos ou sofrerem danos;
f) Comunicação: perda de comunicação ou acesso não permitido;
g) Humanas: falta de capacitação, compartilhamento de acessos a informações que são confidenciais, não realização de rotinas de segurança, erros, sabotagens, vandalismo, roubo e demolição de propriedades ou dados.

Nakamura e Geus (2007) destacam alguns fatores para que haja preocupação com a segurança contínua:

a) Entender a natureza dos ataques é fundamental: é importante entender que muitos dos ataques que acontecem são resultados da exploração de vulnerabilidades, que podem existir por conta de uma falha no projeto ou mesmo na implementação de um protocolo, aplicação, serviço ou sistema ou ainda por causa de erros de configuração e administração dos recursos computacionais. Isso quer dizer que uma falha pode ser corrigida, porém sempre existirão novos bugs.
b) Novas tecnologias trazem consigo novas vulnerabilidades: é preciso ter noção de que novas vulnerabilidades surgem diariamente. Considerando que novas tecnologias e novos sistemas são criados dia após dia, é compreensível o fato de que novas vulnerabilidades sempre existirão e, portanto, novos ataques serão sempre criados. Um exemplo claro seria as redes sem fio (wireless), elas trazem grandes vantagens para as empresas e aos usuários, mas também trazem novas vulnerabilidades que podem colocar em risco todos os negócios da organização.
c) Novas formas de ataques são criadas: a história relata e mostra a constante evolução das mais variadas técnicas usadas para ataques, que estão sendo cada vez mais sofisticados. Quando se combina diferentes técnicas e o uso de tecnologia para esconder vestígios a cooperação entre atacantes e a criatividade são as causas que tornam a defesa mais difícil do que o habitual.

d) Aumento de conectividade resulta em novas possibilidades de ataques: quanto mais o acesso se torna fácil, acarreta consigo consequências, o número de novos curiosos aumenta, assim como a possibilidade de disfarce que podem ser usados nos ataques. Além do mais, novos recursos e tecnologias, principalmente os novos protocolos de comunicação móvel, alteram o paradigma de segurança. Por exemplo, num cenário cujo os usuários de telefones celulares são alvos de ataques se usados como porta de entrada para ataques a uma rede corporativa, é completamente possível.
e) Existência tanto de ataques direcionados quanto de ataques oportuníssimos: embora na sua maioria dos ataques sejam registrados como oportuníssimos, os ataques direcionados também se encontram em grande número. Esses ataques direcionados podem ser considerados muito mais perigosos, já que, existindo a intenção de atacar, a estratégia pode ser cuidadosamente pensada e estudada, e executada de maneira a explorar o elo mais fraco da empresa. Geralmente, esses são os ataques que causam prejuízos maiores, pois, acontecem de modo aleatório, assim como ocorre com os ataques oportuníssimos. Isso pode ser constatado também pelo nível de agressividade dos ataques. Quanto mais agressivo for o ataque, maior é o nível de empenho dispensado a ataques direcionados a um alvo especifico.

2.5.1 Varreduras de redes - *scan*

A finalidade é escanear redes de computadores. É uma técnica muito utilizada na identificação de quais computadores estão ativos na rede e assim coletar toda informação sobre eles, procurando encontrar vulnerabilidades existentes, com uma única intenção, que é facilitar um possível ataque (CARDOSO, 2013).

Varreduras em redes, conhecido também como *scan*, são técnicas que têm como objetivo efetuar buscas minuciosas em redes, com a ideia de identificar computadores ativos e colher informações sobre eles, nomeadamente serviços

disponibilizados e programas instalados. Baseado nas informações coletadas é possível relacionar possíveis vulnerabilidades aos serviços cedidos e aos programas instalados nos computadores ativos detectados (CERT.Br, 2012).

2.6 AMEAÇAS

Uma ameaça baseia-se na possibilidade de violar um sistema computacional, podendo ser acidental ou intencional. Uma ameaça é tida como acidental quando ela não foi planejada. Por exemplo, uma falha no hardware ou no software. Por outro lado, a intencional, está relacionada a uma intenção premeditada (PINHEIRO, 2017).

Ameaça é tida como qualquer tipo de ação física ou lógica, que seja capaz de explorar uma vulnerabilidade e como resultado, acarretar prejuízos para a empresa (CARDOSO, 2013).

Ameaças são fatores ou condições responsáveis por causar incidentes que comprometem as informações e seus ativos, por intermédio da exploração de vulnerabilidades, originando perdas de confidencialidade, integridade, disponibilidade e, como resultado, causando algum impacto aos negócios de uma determinada organização (SÊMOLA, 2003).

De acordo com Peixoto (2006), certas vezes é notável sentir-se ameaçado em determinadas situações, porém isso não significa necessariamente, que se vive um estado de vulnerabilidade naquele dado momento. Já na situação oposta, quando se vive exatamente num momento ou estado vulnerável, certamente a pessoa vê-se ameaçada. Não se trata de uma regra, mas ela é considerada válida quando comparada ao que se diz a respeito das informações.

Ainda conforme Peixoto (2006), ameaça nada mais é do que o resultado de alguma vulnerabilidade existente, com a capacidade de provocar a perda dos elementos ou princípios básicos da segurança da informação.

Ainda de acordo com *Starlin* e Novo (2000) certos produtos, nomeadamente servidores ou até mesmo sistemas operacionais completos, vêm configurados da fábrica com pouca segurança, e é importante conhecer todos os aspectos da nova ferramenta, instalada no sistema, para que se faça um uso correto.

Programas como servidor de e-mail, *FileTransfer Protocol* (FTP), web ou configurações dos sistemas considerados como permissões de arquivos, aplicativos

desnecessários, devem ser vistoriados, todos por completo, antes de qualquer instalação, de modos a se informar sobre suas capacidades de auditoria e sobre seus recursos de segurança.

É possível ainda, caso o próprio sistema em questão seja inseguro e necessário, analisar produtos que possam implementar esta segurança à parte, dando a mesma importância a ele, instalando-os simultaneamente, e não deixar para depois, porque se alguém conseguir detectar algum problema, poderá explora-lo imediatamente. Uma vez que estas configurações padrões, ou erros mais comuns no decorrer da instalação, são tidos como grande alvo dos hackers, em pouco tempo o sistema pode sofrer ataque e ficar comprometido por completo por falta de pura atenção.

2.7 SERVIÇOS DE REDES

Na visão de *Starlin* e Novo (2000) basicamente, redes locais são um conjunto de *Personal Computers* (PCs) conectados aos servidores. Os usuários de uma *local area network* (LAN) realizam suas atividades a partir de seus PCs.

Essas atividades, normalmente, são tarefas como edição de texto, planilhas eletrônicas ou aplicações gráficas e o acesso a aplicações disponíveis nos servidores de rede.

Ainda segundo com *Starlin* e Novo (2000), a característica mais relevante, é exatamente, seu recurso de aceitar aplicativos cooperativos, nos quais um aplicativo é feito, em parte nas estações de trabalho e, outra parte, num servidor de rede local ou um host de *mainframe*.

Mainframe é um recurso computacional de grande porte, dedicado a processar um grande volume de informações (SORDI; MARINHO; NAGY, 2006).

Rede local é um sistema de comunicação de dados que permite que um número de dispositivos independentes estabeleça comunicação direita um com o outro, dentro de uma área geográfica bem delimitada, tamanho moderado, e por meio de um canal de comunicações de taxas de dados razoáveis. Os componentes constituintes de uma rede local são: servidores, PCs desktop (*Workstations*) e recursos de comunicação (STARLIN; NOVO, 2000).

Servidor é uma máquina com enorme capacidade de processamento, cuja função é disponibilizar serviços a rede. De modo geral, é um computador que

processa grandes volumes de dados (data-base), requerendo CPUs rápidos e dispositivos de armazenamento (Hard Disks) de alta capacidade e de rápido acesso (IEEE apud STARLIN; NOVO, 2000, pág. 41).

Os serviços de rede são de suma importância para fornecer uma boa funcionalidade e conectividade as redes internas como também as externas, e o trabalho destaca alguns serviços, tais como:

a) *Simple Mail Transfer Protocol* (SMTP) é o protocolo que se responsabiliza em fazer chegar à mensagem de e-mail a um destinatário. Sempre que um e-mail for enviado, existe um servidor SMTP que se encarrega de leva-los até ao destino. Geralmente se aloja na porta 25. O fato curioso do SMTP é que para se enviar um e- mail não necessita senha, ao contrário do POP3 (visto a seguir). E essa falta de segurança no envio de mensagens é apontado como ponto de partida para a facilidade de se enviar e-mails anônimos. O SMTP ainda permite anexar conteúdos binários nas mensagens de textos que são enviadas (programas por exemplo), utilizando o MIME (ASSUNÇÃO, 2002).
b) *Post Office Protocol* (POP3) é um outro protocolo de mensagem, esse por sua vez, é responsável por recebimentos das mensagens enviadas. O POP3 diferente do SMTP, precisa de senhas para poder habilitar o acesso aos usuários e suas caixas postais. Localiza-se com muita frequência na porta 110, esse protocolo é capaz de remontar os arquivos enviados em formato MIME com o SMTP. A grande desvantagem dele é que as chances de se concretizar um ataque de *bruteforce* para tentar descobrir senhas são enormes, uma vez que a maioria dos servidores possuem falhas que possibilitam softwares maliciosos ao serem rodados (ASSUNÇÃO, 2002)
c) FTP sua grande tarefa consiste em prover serviços de transferência, renomeação, e eliminação de arquivos, fora a criação, alteração e exclusão de diretórios. Para que a sua operação aconteça, duas conexões precisam ser mantidas: Uma de dados e outra de controle. Não implementa segurança, deixando para o TCP, salvo as requisições de senhas de acesso a determinados arquivos ou servidores FTP (STARLIN; NOVO, 2000).

d) TELNET (ou terminal remoto) é uma maneira de fazer acesso remoto dos sistemas como se estivesse operando localmente. Por exemplo: Usando o *telnet* (e um trojan instalado) é possível ter acesso ao MS-DOS de qualquer um. Da mesma forma que se pode digitar comandos para listar, copiar e excluir dados, também é possível faze-lo estando conectado a um outro computador. Na realidade, todos os trojans são clientes *telnet*, disfarçados com botõezinhos bonitinhos. Quando existe uma porta aberta em algum sistema, (qualquer uma que seja, trojan, SMTP, POP3, etc...), existe a possiblidade de uma conexão por *telnet* (ASSUNÇÃO, 2002).

e) *Simple* Network *Management Protocol* (SNMP) é um protocolo simples para manejar a rede, o uso dela permite obter informações detalhadas sobre contas de usuários, equipamentos de rede, portas, serviços abertos e muito mais (ASSUNÇÃO, 2002).

2.7.1 Portas

Há uma grande diversidade de serviços que são rodados em computadores de empresas, com a necessidade de estabelecer comunicação com filiais e clientes, portanto esses são apenas alguns e de fato, um sistema com esses serviços ativos, pode ganhar sérios problemas com a segurança. Toda vez que uma porta de alguma máquina se abre para estabelecer contato com um site ou uma outra máquina, ou seja, cada vez que for feita uma conexão, a porta mudará. Impedindo que algum invasor fique espionando e se conectando a portas padrões. Dificulta, porém não impede. Se der o caso de ser instalado algum cavalo de troia, sem que se saiba, então há probabilidade de se abrir uma porta qualquer e desta forma, permitir a conexão de qualquer pessoa. Para detectar quais portas estão abertas em um sistema remoto utiliza-se o *port scan*, ou seja, o *scan* de portas (ASSUNÇÃO, 2002).

Conforme o quadro 1, mostra as principais series de portas pré-definidas para determinados serviços que são aceitos universalmente.

Quadro 1 - Serie de portas

Serviços	Portas	Descrição
FTP	21	*File Transfer Protocol* (Protocolo de transferência de arquivos)
Telnet	23	Para se conectar remotamente a um servidor
SMTP	25	Para enviar um e-mail
Gopher	70	*Browser* baseado em modo texto
HTTP	80	Protocolo www – Netscape, Mosaic
POP3	110	Para receber e-mail
NNTP	119	*Newsgroups*
IRC	6667	*Internet Relay Chat* – Bate papo on-line

Fonte: Starlin e Novo (2000).

3. TIPOS DE ATAQUES

De acordo com Assunção (2002), os sistemas podem sofrer apenas dois tipos de ataque, sendo como primeiro o *Denial of Service* (DoS) ou recusa de serviço, como é muito conhecido. Esse tipo de ataque tem como única finalidade a máquina alvo, onde o atacante utiliza técnicas, enviando dezenas de pacotes de informação com o objetivo de gerar uma paralisia no processamento e um consumo gigantesco de toda memória. É um típico de ataque que causa apenas danos temporários, como tirar o servidor do ar, porém não fornece acesso aos arquivos. Já a invasão, consiste em procurar e utilizar alguma falha do sistema contra ele próprio ou ainda, instalar programas como *trojans* e *sniffers* com o objetivo de monitorar todo trafego de senhas e assim fornecer arquivos de suma importância.

3.1 FORMAS DE ATAQUE

De acordo com O´Brien e Marakas (2013), as principais formas de ataque dos hackers são:

a) DOS - negação de serviço: é uma forma que consiste em explorar na rede o equipamento de um determinado site, assim como vários pedidos de informação, podendo sobrecarregar efetivamente o sistema, reduzir a velocidade ou até mesmo derrubar o site ou servidor;
b) *Scans*: refere-se a investigações na internet, feitas de uma maneira aprofundada para determinar os tipos de computadores, serviços e conexões em uso, de modo que os hackers possam tirar o proveito da fraqueza em um determinado software, sistema ou recurso de um computador;
c) Farejadores: são programas que realizam suas buscas de pacotes de forma oculta quando trafegam pela rede, capturando assim as senhas ou ainda conteúdos inteiros;
d) *Spoofing*: remete-se a falsificação de e-mail ou página web, com o intuito de burlar usuários, para que assim forneçam informações importantes, como senha e dados do cartão de crédito;
e) Cavalo de Tróia: normalmente são softwares desconhecidos ao usuário, contendo instruções que exploram vulnerabilidades conhecidas de um software;
f) *Back doors*: uma vez que a porta de entrada é descoberta, utilizam-se

caminhos ocultos de apoio para facilitar a reentrada e torna-las difícil de detectar. Pois é por meio da porta que a comunicação de dispositivo a outro é efetuado pela rede;

g) *Applets* nocivos: refere-se a pequenos programas que abusam dos recursos do computador, modificando arquivos no disco rígido, enviam e-mails falsos e roubam senhas;
h) *Password crackers:* são programas desenvolvidos para descobrir senhas;
i) *Adware:* é um tipo de software que durante o tempo em que está em uso, também permite aos anunciantes da internet exibir seus anúncios por meio de banners, sem autorização do usuário. Ele também pode coletar dados do usuário do computador e mandar via internet para o seu desenvolvedor;
j) Engenharia social: relativo as táticas usadas para se obter acesso aos sistemas de uma empresa, conversando de maneira insuspeita com quem deseja colher informações importantes, tais como a senha. A ação pode ter como alvo um funcionário da empresa ou até mesmo um usuário comum.

3.2 MOTIVAÇÃO

De acordo com a CERT.Br (2012), a cada dia ocorrem diversos ataques na internet, com vários objetivos, tendo em vista os diferentes alvos e usando as mais variadas técnicas. Qualquer serviço, computador ou rede que seja acessível por meio da internet pode ser alvo de um ataque, do mesmo modo que qualquer computador com acesso à internet pode participar de um ataque.

Os motivos que levam os atacantes a lançar ataques na internet são bastante diversos, e variam desde a simples diversão até a realização de ações criminosas. Motivações como:

a) Demonstração de poder: mostrar a uma determinada empresa que ela pode ser invadida ou ter seus serviços suspensos e, dessa maneira, tentar vender os serviços ou chantageá-la para que o ataque não volte a acontecer;

b) Prestigio: engrandecer-se perante outros atacantes, por ter conseguido invadir computadores, tornando seus serviços inacessíveis, ou ainda desconfigurar sites considerados destacados ou difíceis de serem atacados, competir com outros atacantes ou grupos de atacantes para desvendar quem consegue realizar o maior número de ataque ou ser o primeiro a conseguir atingir um alvo especifico;

c) Motivações financeiras: com base em coleta e uso de informações confidenciais de usuários para aplicar golpes;

d) Motivações ideológicas: consiste em tornar inacessível ou invadir sites que divulguem conteúdo contrário a opinião dos atacantes; divulgar mensagens de apoio ou contrárias a uma determinada ideologia;

e) Motivações comerciais: consiste em tornar inacessível ou invadir sites e computadores de organizações concorrentes, com o objetivo de impedir o aceso dos clientes ou ainda comprometer a reputação destas empresas.

3.3 EXEMPLOS REAIS DE ATAQUE

Conforme mostra a figura 2, um caso de ataque relatado pelos funcionários da VestaCP, onde foi utilizado honeypot como estratégia de segurança para poder descobrir o que aconteceu. Para mais informações, nos anexos.

Figura 2 – Relato de ataque na VestaCP.

Fonte: Albertus *et al*. (2018)

4. HONEYPOTS

Um honeypot é uma ferramenta ou sistema criado, cujo o objetivo é enganar um atacante e faze-lo crer que invadiu realmente o sistema, quando na verdade ele está em um ambiente simulado, onde todos os seus passos são vigiados (ASSUNÇÃO, 2008).

Para além de capturar as informações sobre os ataques, o honeypot pode mostrar as intenções dos ataques, bem como fazer com que os hackers percam tempo com ataques não concretos, enquanto os especialistas extraem o máximo de informações para poder melhorar a segurança das organizações (MARCELO; PITANGA, 2003).

De acordo com Marcelo e Pitanga (2003), o termo *honeypot* é originário do inglês, que em português traduz-se em pote de mel. O mel na antiguidade era um alimento muito desejado, por ser muito consumido pela classe nobre, e também devido a sua demasiada doçura. Um honeypot em uma rede de computador deve seguir este mesmo princípio, ser muito atraente para os atacantes.

É preciso compreender que um honeypot não contém dados ou aplicações vitais para a empresa, e sua única finalidade é poder passar-se por um equipamento fidedigno da organização, que por sua vez é configurado para interagir com um hacker, um determinado invasor. Assim, todos os detalhes da técnica utilizada e do ataque realizado em si, podem ser capturados, analisados e estudados (NAKAMURA; GEUS, 2007).

Um sistema de detenção de intrusão pode ser utilizado como fonte de aprendizado sobre novos ataques, para além de exercer uma função fundamental, que é a detecção (NAKAMURA; GEUS, 2007).

Segundo Assunção (2009), existem dois tipos de honeypots:

a) Honeypots de pesquisa: o objetivo primordial deste honeypot não é ser utilizado como um sistema de detecção de intrusão ou denominado *Intrusion Detection System* (IDS), consiste em meios técnicos de revelar a uma rede quando está tendo acessos não permitidos que possam apontar a ação de um hacker ou funcionários mal- intencionados. A intenção é realmente ser atacado imensas vezes para que posteriormente se estude cada detalhe de cada ataque. Cada

arquivo que o invasor acessar, cada senha que ele digitar, cada comando, absolutamente tudo será salvo e estudado.

b) Honeypots de produção: A finalidade é detectar intrusos na rede e tomar as providencias contra os invasores o mais rápido que puder. É o que realmente se recomenda em uma empresa ou uma organização que pretende proteger a sua rede. No *honeypot* de produção é necessário o uso de um ambiente de baixa interação, já que são ambientes simulados e não oferecem risco algum ao sistema real e, caso o atacante descubra a armadilha, não há problemas.

4.1 CLASSIFICAÇÃO DE HONEYPOTS

De acordo com Franco, Barbato e Montes (2004), os honeypots podem ser classificados por baixa e alta interatividade, partindo dos serviços falsos, ou seja, baixa interatividade, até máquinas com serviços reais, isto é, alta interatividade, onde os atacantes conseguem obter total acesso ao sistema.

1) Baixa interatividade: *Back Officer Friendly, Deception Tolkit (DTK), Specter, Honeyd, Labrea, Tarpit.*

2) Alta interatividade: *User-mode linux* (UML), *VMware, Mantrap*.

Ainda de acordo com Franco, Barbato e Montes (2004), as finalidades dos honeypots são:

a) Coletar códigos maliciosos;

b) Identificar varreduras e ataques;

c) Fazer acompanhamento das vulnerabilidades;

d) Conhecer a motivação dos atacantes;

e) Correlacionar informações com outras fontes;

f) Auxiliar os sistemas de detecção de intrusão;

g) Manter atacantes afastados de sistemas importantes.

Segundo Assunção (2009), os serviços de alta interação consistem nos serviços que são adicionados ao *honeypot* no momento que ele é concebido e implantado. Esses serviços podem ser um *software* que funcione como servidor de correio ou ainda de transferência de arquivos. Então, caso se entregue ao atacante um sistema real com serviços que funcionem realmente, esses serviços são de alta interação, pois ao se dispor uma máquina com serviços reais para um invasor, existe

uma grande chance de ele ser capaz de comprometer esse computador e assim conseguir acesso a outro da rede, uma vez que ele terá um sistema operacional real completamente a sua disposição para fazer o que quiser já os serviços de baixa interação: são opostos aos serviços de alta interação, onde todos os serviços, assim como serviços de correio, são simulados. O invasor não consegue ter o acesso ao sistema real, somente às versões simuladas dos mesmos, o que acaba sendo vantajoso, no que tange a segurança, pois se o que o atacante consegue visualizar é apenas uma simulação, então ele não será capaz de comprometer a segurança do sistema e ganhar acesso a outro computador da rede.

Segundo Rodrigues, Souza e Diniz (2015), com uso do *honeypot* é possível visualizar as ações do atacante e assim o responsável pela rede da empresa pode se prevenir e averiguar as técnicas de defesas mais eficientes contra- ataques externos. É possível verificar também se os principais dispositivos de segurança como *firewall*, antivírus, entre outros, são realmente eficientes e se podem de fato, amenizar a possibilidade de invasão de estações de trabalho de uma rede de computadores.

Ainda segundo Rodrigues, Souza e Diniz (2015), um dos grandes benefícios do honeypot é o fato de que quase não acusa falsos negativos, ou seja, não aponta para uma atividade como sendo ataque quando essa atividade na verdade não é um ataque, já que é um *honeypot*, então ele não está divulgado na rede e, qualquer tipo de tentativa de acesso pode ser considerada um ataque, o risco de um sistema desse tipo, também é muito baixo, pois ele é projetado para não deixar o ataque se espalhar na rede, isto é, o administrador pode ficar tranquilo quando ocorrer um ataque, por mais que seja muito bem planejado e de força bruta, será executado dentro de um ambiente controlado.

Outro fator interessante referente ao uso de *honeypot* é que dentro das configurações corretas, o mesmo se torna uma armadilha totalmente segura, onde o atacante pensará estar invadindo um sistema real, no entanto, não existe nenhum dado de valor que seja importante para um furto, nesse caso, toda ação do atacante será monitorada pelo *honeypot* e em seguida esses dados servirão para prevenir ataques a outros sistemas, de modos que se consiga resolver as vulnerabilidades que antes existiam.

Os *honeypots* têm uma suma importância para ambientes onde técnicas inovadoras precisam ser detectadas, conhecidas e estudadas, para que se adquira

informações primordiais para o aperfeiçoamento da defesa, como a frequência de ataques, as técnicas mais utilizadas e as tendências de ataques. Além de providenciar informações sobre ataques, um *honeypot* pode apresentar as intenções do ataque e também fazer com que o atacante perca tempo com ataques não apropriados, enquanto a empresa vai colhendo informações sobre ele e sobre maneiras de melhorar a prevenção. Isso só é possível porque o honeypot faz com que o invasor tenha uma compreensão errada das medidas de segurança adotadas pela organização (NAKAMURA; GEUS, 2007).

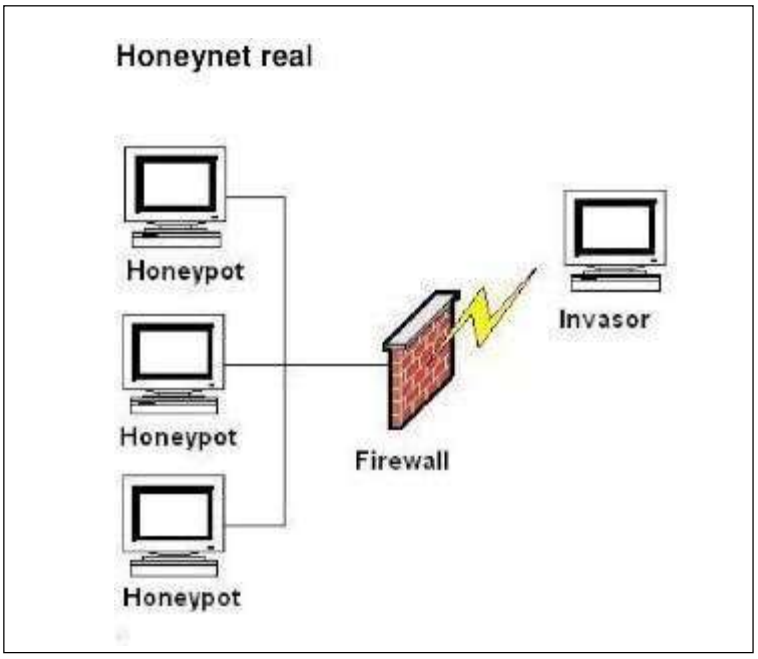
4.2 HONEYPOT E HONEYNET

Segundo Assunção (2009), *honeypot* pode ser definido em uma só palavra, que é a palavra armadilha, ao passo que uma *honeynet* é uma ferramenta de pesquisa baseada em uma rede preparada especificamente para ser comprometida, contendo mecanismos de controle para evitar que seja utilizada como base de ataques a outras redes, na verdade é um tipo de *honeypot*, entretanto intitulado como sendo um *honeypot* de pesquisa.

Existem duas maneiras possíveis de se implementar um *honeypot* ou *honeynet*: Real ou virtual. Uma *honeynet* ou *honeypot* real consiste em diversos componentes de uma rede comum como servidores, computadores, *switches* e roteadores atuando de um modo que o *honeypot* pudesse ser implementado. Esse tipo de solução requer, um custo financeiro mais elevado, tendo em conta que a ideia é montar uma rede real. A outra maneira seria uma *honeypot* virtual, desse modo seria possível criar em um único *host* várias máquinas virtuais simulando um ambiente real, com um custo inferior se comparado ao *honeypot* real (ASSUNÇÃO, 2009).

A figura 3 apresenta a arquitetura do *honeypot* real, em ambiente estruturado por três *honeypots,* um *firewall* e um invasor.

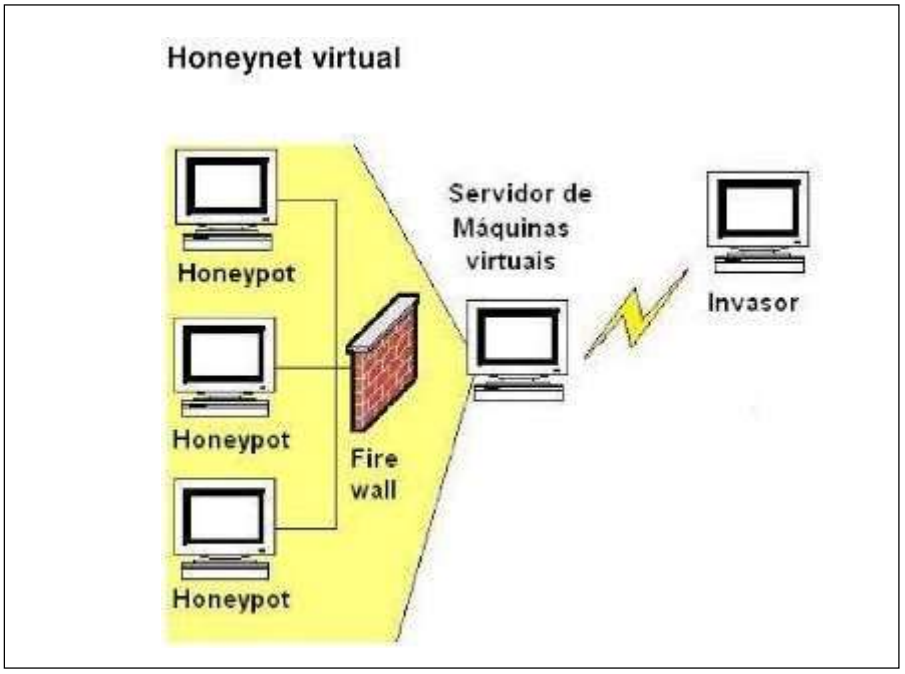
Figura 3 - *Honeypot* Real



Fonte: Assunção (2009).

Arquitetura do *honeypot* virtual, em ambiente estruturado por três *honeypots,* um *firewall*, um servidor de máquinas virtuais e um invasor (figura 4).

Figura 4 - *Honeypot* Virtual



Fonte: Assunção (2009).

4.2.1 Virtualização

A virtualização é a maneira mais simples de se montar uma *honeypot*, cada vez mais utilizado, seja em ambientes acadêmicos ou ambientes corporativos, o uso de maquinas virtuais tem crescido significativamente (ASSUNÇÃO, 2009).

A virtualização mostra-se como sendo uma boa opção para se implementar honeypots, e existem algumas razões como: caso o sistema operacional seja comprometido, adota-se como solução a remoção da máquina virtual e a instanciação de uma nova. A outra razão é a possibilidade de se instalar várias maquinas virtuais em um mesmo hardware físico, onde cada máquina pode ter um sistema operacional diferente das demais maquinas virtuais e da própria máquina host (CARISSIMI, 2008).

Na visão de Assunção (2009), uma *honeynet* real é aquela cujo todos os computadores e componentes são físicos, ou seja, cada computador *honeypot* existe fisicamente dentro da rede. É o tipo de rede que mais próximo chega de uma situação verdadeira.

No entanto, há um problema: custo, pois montar uma *honeynet* real requer verbas, logo é necessária a compra de diversos equipamentos que farão parte da rede, e só depois fazê-la funcionar.

Separar os computadores *honeypots* é uma vantagem no que se refere a segurança, porque as chances de eles não ficarem sobrecarregados são mais elevadas, dado que os ataques possivelmente serão distribuídos entre todos.

4.2.2 Docker - Containers

Containers são ambientes isolados, ou ainda, máquinas virtuais leves, podemos assim dizer. Eles são uma virtualização em nível do sistema operacional e não da máquina em si. Ou seja, compartilha um mesmo kernel do sistema operacional de um determinado host. Trazendo assim, um isolamento parcial que faz os containers serem mais ágeis e mais rápidos nas suas inicializações. E o fato deles não possuírem o sistema operacional como um todo dentro deles, permite com que eles necessitem menos recursos.

Pode-se dizer ainda, que containers são mecanismos leves de virtualização em nível de sistema operacional, sem ter a necessidade de executar

várias máquinas virtuais com a emulação de seus hardwares. Pois, são ambientes de execução que possuem CPU isolada, memória, blocos I/O e recursos de rede, mas compartilham o mesmo *kernel* do sistema operacional. Containers tem um funcionamento parecido com os de uma máquina virtual, porém, diferente em sua arquitetura, se apresentando mais leve, uma vez que não é necessário executar todo um sistema operacional na máquina. (ORACLE, 2012).

Os containers isolam aplicações de forma individuais, fazendo o uso de recursos do próprio sistema operacional que foram abstraídos pelo ecossistema *docker*. Eles permitem também o empacotamento de uma aplicação juntamente com todas as suas dependências como unidade, o que torna viável a questão de gerenciamento de dependências e também simplifica o gerenciamento de versões da aplicação (PRADA *et al*., 2017).

Já o *docker* é um gerenciador de containers. Um recurso virtual que provê processos que podem ser utilizados para instalar serviços e aplicações. É um grande orquestrador de ambientes isolados, facilitando a criação e administração desses mesmos ambientes.

O *docker* é uma plataforma aberta, criada com o objetivo de facilitar o desenvolvimento, assim como a implantação e execução de aplicações em ambientes isolados. Foi projetada principalmente para disponibilizar uma aplicação de maneira mais rápida e possível (GOMES, 2019).

Foi criado pela *dotCloud Inc*., uma empresa especialista em PaaS (Platform-as-a-Service) que em 2013 resolveu tornar open *source* o core de sua plataforma, dando assim a origem ao *docker*. No início a primeira versão do *docker* era apenas um encapsulamento do LXC integrado ao *Union Filesystem*, no entanto, seu crescimento foi bastante rápido, o que permitiu que o projeto fosse muito bem aceite pela comunidade. Com isso a *dotCloud* passou a se chamar de *docker*, e em seguida foi lançada a primeira versão oficial da plataforma (VITALINO; CASTRO, 2016).

Um diferencial do *docker* é que ele possui uma *engine* para o *deploy* (colocar o projeto em produção) de seus processos ou aplicações, sendo executadas num ambiente virtualizado de container. Ele foi criado com a visão de ser um ambiente leve e rápido, onde se podem executar aplicações e também fluxos de trabalhos para o *deploy* das mesmas (TURNBULL, 2014).

O uso do *docker* permite ainda, gerenciar com facilidade a infraestrutura de uma aplicação, agilizando assim, o processo de criação, manutenção e modificação de serviço. A grande ideia do *docker* é permitir múltiplos ambientes isolados, dentro de um mesmo host, porém, acessível no mundo externo (GOMES; SOUZA, 2015).

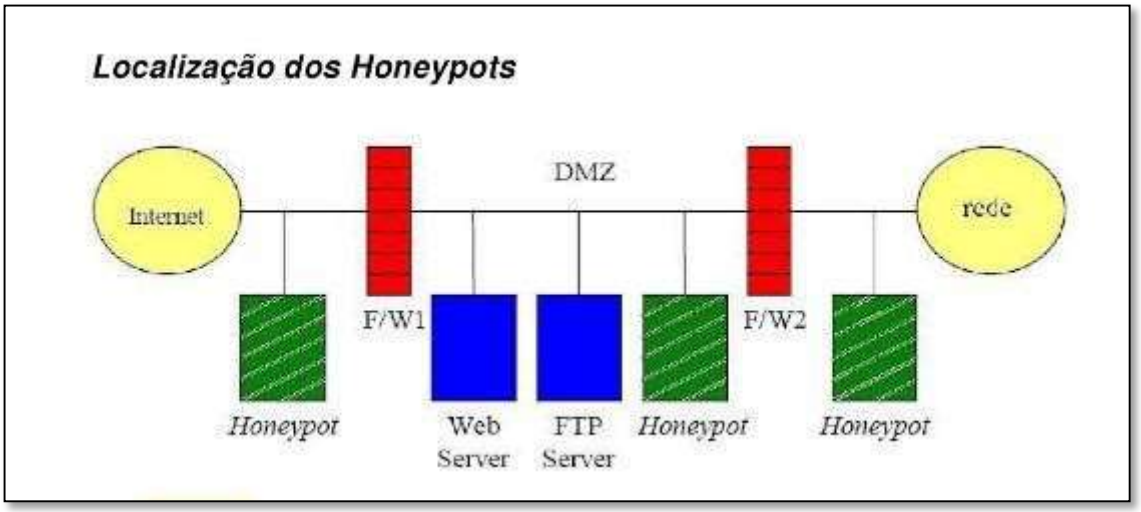
4.3 LOCALIZAÇÃO DOS HONEYPOTS

Segundo Assunção (2009), honeypot pode ser localizado em três zonas distintas, tais como:

1) Antes do primeiro *firewall* (F/W1): nessa zona o honeypot ficará propositalmente exposto ao máximo, sem qualquer proteção. É uma situação onde provavelmente o invasor consiga causar mais danos, porém, exatamente por isso é o mais interessante da perspectiva de capturar ações maliciosas, que é a finalidade do honeypot de pesquisa.
2) Na zona desmilitarizada (DMZ): nessa situação o honeypot estará no mesmo nível dos principais servidores reais da rede, não ficando tão exposto a ataques e por estarem dentro da mesma faixa, o atacante pode tentar realizar uma varredura de portas.
3) Junto à rede interna, após o segundo firewall (F/W2): é um local onde dificilmente o honeypot receberá ataques provenientes da internet. Pode correr, mas a frequência é bem menor, pois essa localização é o ideal para capturar atacantes que venham da rede interna.

Conforme a figura 5 pode-se observar as três possíveis zonas onde é encontrado o honeypot na rede de uma organização.

Figura 5 – Localização dos *honeypots*



Fonte: Assunção (2009).

5. TRABALHOS CORRELATOS

A todo o momento são realizadas várias pesquisas no mundo inteiro na área de tecnologia. Questões como segurança da informação são cada vez mais abordadas, exploradas e tratadas no meio das organizações e não só, devido ao acesso indevido, acesso não autorizado ou outros tipos de intenções contra a informação.

A seguir são abordados alguns desses trabalhos relacionados a mesma linha de pesquisa ao trabalho proposto.

5.1 ANÁLISE E IMPLEMENTAÇÃO DE HONEYPOT EM AMBIENTE LINUX

Em 2010, o acadêmico Anderson Brunel Modolon, do programa de graduação em ciência da computação na Universidade do Extremo Sul Catarinense, em Criciúma, realizou um estudo e implementação do *honeypot Honeyd* em um ambiente *Linux*, com o objetivo de analisar o comportamento do sistema honeypot, para isso foi necessário à realização de um estudo aprofundado sobre invasões, ataques e também a preparação de um ambiente onde foram simulados ataques a hosts falsos que respondem como verdadeiros e, em seguida analisado os *logs* gerados.

Foram também instalados maquinas virtuais com o programa *virtualBox,* no intuito de que fossem confundidas tanto quanto as máquinas reais como também os hosts criados pelo *Honeyd*, além de um estudo e implementação feita com um sistema de detecção de intrusão para monitorar o tráfego na rede, com a finalidade de ajudar na monitoração contra-ataques.

Assim sendo, a implantação de *honeypot* em ambiente Linux com a análise de seus resultados foi realizada, e por meio dos testes comprovada então a importância que um *honeypot* pode ter quando aplicado e configurado de maneira adequada, podendo detectar atividades onde outros tipos de ferramentas em determinada situação não seriam capazes de detectar, quer sejam pela má configuração delas ou realmente por uma determinada invasão que consiga passar por elas sem ser detectada (MODOLON, 2010).

5.2 PROJETO HONEYNET: INSTALAÇÃO E PESQUISA NA UNIVERSIDADE CATÓLICA DE BRASÍLIA

Em 2008, o acadêmico Flávio Cordeiro, do programa de pós-graduação Latu Sensu em segurança em redes de computadores da Universidade Católica de Brasília, elaborou um estudo com o objetivo de implantar uma *honeynet* na mesma universidade, onde foram configuradas duas máquinas distintas com sistemas *OpenBSD* e *FreeBSD* com vários honeypots de baixa interatividade, utilizando a ferramenta *Honeyd*. Como partes deste projeto foram tratadas também todos os aspectos da segurança da informação e seu funcionamento, detalhando o uso de *honeypots* e *honeynets*.

Fez-se também uma análise em um número considerável de outras ferramentas de código aberto, assim como a ferramenta utilizada nesse mesmo trabalho, descreveu-se o ambiente da implantação, apresentando na sequencia os resultados obtidos.

Por fim, o trabalho também propôs a utilização do Honeyd nas máquinas *OpenBSD* e *FreeBSD* que apresentou um resultado excelente, capturando mais de 2GB de ataques e, não havendo muitas ferramentas para análise desses logs da honeynet de forma simplificada, foi sugerido que a Universidade trabalhasse no desenvolvimento dessas ferramentas em parceria com o consórcio de honeynets e com a comunidade de software livre (CORDEIRO, 2008).

5.3 HONEYPOT EM AMBIENTE ADSL: UM ESTUDO DE CASO

Em 2008, o acadêmico Hamilton José Correia, do programa de pós-graduação Latu Senso em gerência de Redes de Computadores e Tecnologia Internet do núcleo de computação eletrônica da Universidade Federal do Rio de Janeiro, realizou um estudo sobre *honeypot* em ambiente ADSL, com o objetivo de analisar os ataques ocorridos utilizando *honeypots* e, aproveitar os resultados dos estudos como solução para melhorias contra vulnerabilidades e prevenção de ataques e invasões nesse tipo de rede.

Elaborou-se um ambiente forjado para iludir invasores com o uso de *honeypots* e realizar a coleta de suas ações, a fim de encontrar caminhos para novas soluções do ambiente de produção corporativa (CORREIA, 2008).

5.4 HONEYPOT: UM AMBIENTE PARA ANALISE DE INTRUSÃO

Em 2008, o acadêmico Frederico Santos de Oliveira, do programa de graduação pela Universidade Federal de Lavras, no curso de Ciências da Computação, desenvolveu uma pesquisa com o objetivo de criar um perfil dos invasores, retratando suas intenções a partir de dados capturados das instruções estabelecidas, entender as suas técnicas e também conhecer suas motivações ao realizar um ataque.

A pesquisa feita contou com ferramentas como *honeypot,* que fez a captura dos dados em relação ao tráfego e ações realizadas. Foram centralizados os dados em um *honeywall*, que permitiu uma manutenção fácil e a coleta de dados, comprovando assim, como é necessário o uso de *honeynets* como ferramentas para manutenção de segurança em uma rede.

Elaborou-se um ambiente de forma controlada, onde os invasores mostraram-se estar cientes de ter invadido um *honeypot*. E com os resultados obtidos o grande atrativo que é o uso dessa ferramenta, e ao final, compreender a importância dos *honeypots* como ferramentas adicional as políticas de segurança existentes, ao estudo da conduta tomada por atacantes, a interpretação dos seus passos e ações adotadas para burlar a segurança de uma rede ou sistema (OLIVEIRA, 2008).

5.5 WEBSERVICE HONEYPOT UTILIZANDO A BIBLIOTECA JHONEY

Em 2015, o acadêmico Ricardo de Lima, do programa de graduação pela Universidade Regional de Blumenau no curso de Ciência da Computação, realizou um trabalho de pesquisa com o objetivo de disponibilizar uma ferramenta de simulação de serviços de rede para que sejam expostos na Internet a fim de serem atacados, e deste modo, registrar todas as informações do atacante, endereço de origem do ataque, comandos e *scripts* utilizados para efetuar o ataque, e só depois estudar o comportamento desses hackers a fim de melhorar a segurança de uma rede.

No trabalho desenvolvido foi utilizada uma biblioteca em Java que simula alguns serviços que podem ser configurados atendendo o tipo de captura. E o *honeypot* foi inserido em paralelo a um servidor seguro HTTPS, utilizando HTTP em

sua porta padrão 80, tornando-se um alvo fácil para usuários mal intencionados que tentará invadir o sistema, e assim o *honeypot* vai fazendo a coleta de dados desses invasores e inserindo em uma lista de bloqueios do *firewall* da rede principal, onde se encontra o servidor HTTPS. Deste modo pode-se complementar a segurança da rede principal, pois, se porventura algum usuário mal-intencionado tentando um acesso, ele será impedido pelo firewall que já tem registrado o seu endereço na lista de bloqueios (LIMA, 2015).

6. TRABALHO DESENVOLVIDO

A partir das análises dos trabalhos correlatos, observou-se a evolução dos honeypots, quando se buscava por soluções que atendessem ao problema da pesquisa desenvolvida. Alguns softwares foram descontinuados, como é o caso do *honeyd*, *kojoney*, *kippo* e entre outros. Procurou-se então por honeypots mais atuais, e nessa fase algumas dificuldades foram encontradas: Falta de documentação dos projetos *honeypots*, dificuldades na configuração de alguns *honeypots* atuais testados, por falta de suporte ou materiais de apoio, assim como a falta de modelos de projetos *honeypots* funcionando na prática.

Neste trabalho implementou-se a ferramenta *honeypot T-Pot*, por ser uma das mais atuais, de código aberto, baseado em *docker*-compose e executado no Debian (Sid), incluindo versões *dockerizadas* de alguns sensores como: *conpot*, *cowrie*, *dionaea*, *tanner*, *rdpy* e *honeytrap*. A ferramenta escolhida permitiu a concretização da pesquisa por se mostrar ser mais atual, e não só, mais também pela praticidade e simplicidade de ser implantada e configurada. Vem sendo uma das plataformas de honeypots mais bem-sucedidas, não simplesmente pela sua baixa manutenção, e toda tecnologia que o envolve, mas também por causa dos bons painéis e sensores de investigação (DTAG, 2015).

Desenvolvida pela Deutsche Telekom (DTAG), com a finalidade de registrar tráfegos maliciosos que possam existir, estudá-los e analisá-los, permitindo assim melhorar a segurança da informação e todos ativos da organização a partir dos resultados ou logs gerados.

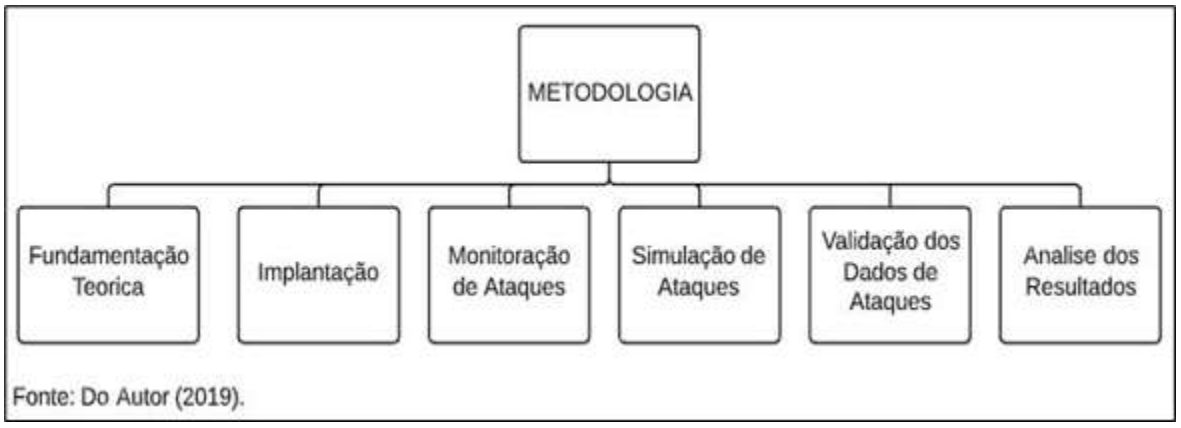
Implantar *honeypots* configurá-los e mantê-los ao longo do tempo, e na sequência, analisar os dados capturados sempre foi uma tarefa exigente e desafiadora. E isso fez com que não fossem adotados amplamente como solução, em alguns casos, devido a sua complexidade, apesar da ferramenta já ter sido madura. (ANOMALI, 2019).

O T-Pot apresenta vários sensores honeypots em execução paralela e redireciona o tráfego capturado na interface de rede para os honeypots mais adequados disponíveis. Os dados capturados são exibidos em painéis, permitindo analisar os ataques e fazer uma pesquisa sobre dos dados de um modo fácil (DTAG, 2015).

6.1 METODOLOGIA

Para a concretização deste trabalho foi elaborado um cronograma de levantamento bibliográfico relacionado a segurança da informação, políticas de segurança, vulnerabilidades, riscos, ameaças e ataques, serviços de redes, tipos de ataque, formas de ataque e motivação dos atacantes, e também foi feito uma busca sobre os honeypots mais atuais, bem como as novas formas de implementação, monitoração de ataques, simulação de ataques, validação dos dados de ataques, e a análise dos resultados gerados. A figura 6 mostra o passo a passo, da busca realizada.

Figura 6 – Metodologia utilizada



Fonte: Do Autor (2019).

Primeiramente foi criada uma instância de VM do *google cloud platform*, com *Debian buster*. E em seguida foi implantada a ferramenta, com as suas devidas configurações. Foram criadas regras de acesso à Internet para então poder monitorar a rede e todos ataques possíveis. Na sequência, foi feita a simulação de ataques, e análise dos resultados dos dados de ataque coletado pela ferramenta.

O honeypot foi implantado obedecendo alguns requisitos mínimos para que o sistema funcionasse da melhor maneira, a saber:

1) 6-8 GB de *RAM* (menos *RAM* é possível, porém não aconselhável).
2) *SSD* de 128 GB (menor é possível, mas limita a capacidade de armazenamento).
3) Uma conexão com a Internet (ele baixa as imagens do *docker*).

Na figura 7, destacada abaixo, observa-se a criação do ambiente no *google cloud platform.*

Figura 7 - Criação da instancia VM na nuvem

Fonte: Do Autor (2019).

Foram utilizados os comandos abaixo para atualizar a instancia:

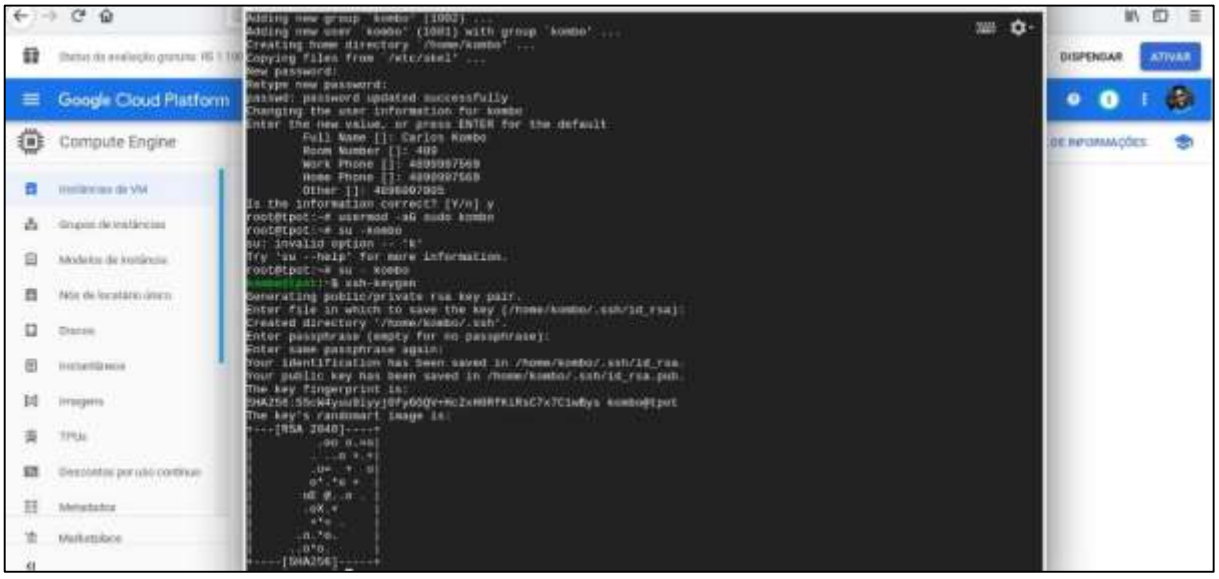
~$ sudo apt-get update

~$ sudo apt-get upgrade

~$ sudo apt-get dist-upgrade

Em seguida foi adicionado um novo usuário ao grupo sudo, a fim de validar a chave ssh, como pode ser observado na Figura 8.

Figura 8 - Inserção de usuário ao sudo e geração de chave ssh



Fonte: Do Autor (2019).

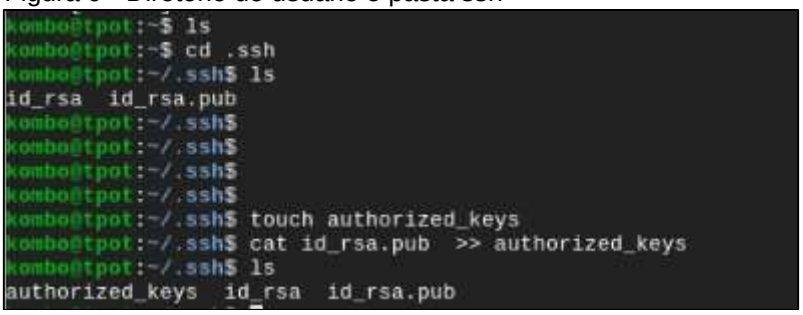
Depois de ser gerada a senha ssh para o usuário kombo, caso estiver pedindo um nome para salvar os arquivos-chave, digita-se identidade como root.

touch allowed_keys

cat identity.pub >> allowed_keys

Do contrário, salva-se os arquivos-chave no usuário sem privilégios, como é demonstrado na Figura 9.

Figura 9 - Diretório de usuário e pasta ssh

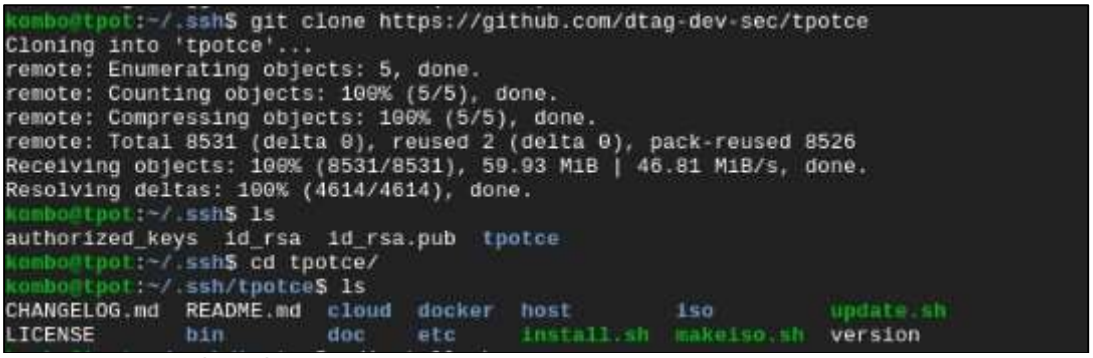


Fonte: Do Autor (2019).

Prosseguindo com a implementação, logo em seguida foi feita a instalação do T-Pot. Uma vez executada a etapa anterior com sucesso, é aconselhável permanecer na mesma pasta que é a pasta ssh para executar as etapas para instalar o honeypot T-Pot, como indicado na Figura 10.

```
# git clone https://github.com/dtag-dev-sec/tpotce
# cd tpotce/iso/installer/
# ./install.sh --type=user
```

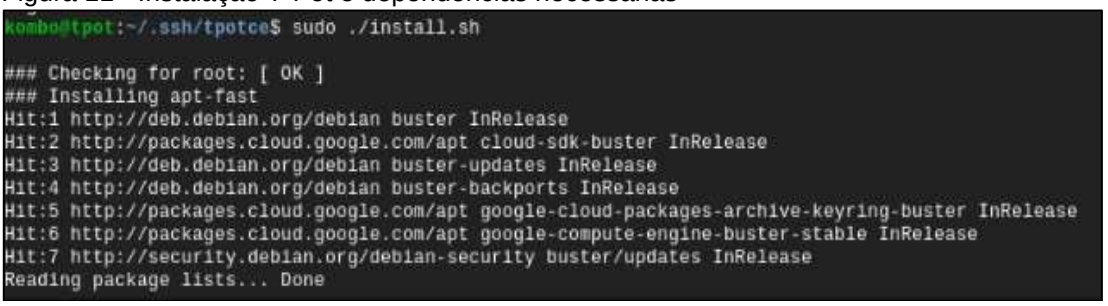
Figura 10 - Baixando T-Pot



Fonte: Do Autor (2019).

Durante o processo de instalação e configuração será solicitado duas vezes a inserção de uma senha. Uma é para o usuário kombo, e a outra é para o usuário T-Pot kombo (lembrando que o nome de usuário pode ser qualquer outro, nesse caso foi escolhido o nome de usuário kombo). Também serão instaladas todas as dependências necessárias para o funcionamento correto do T-Pot, representado na Figura 11.

Figura 11 - Instalação T-Pot e dependências necessárias



Fonte: Do Autor (2019).

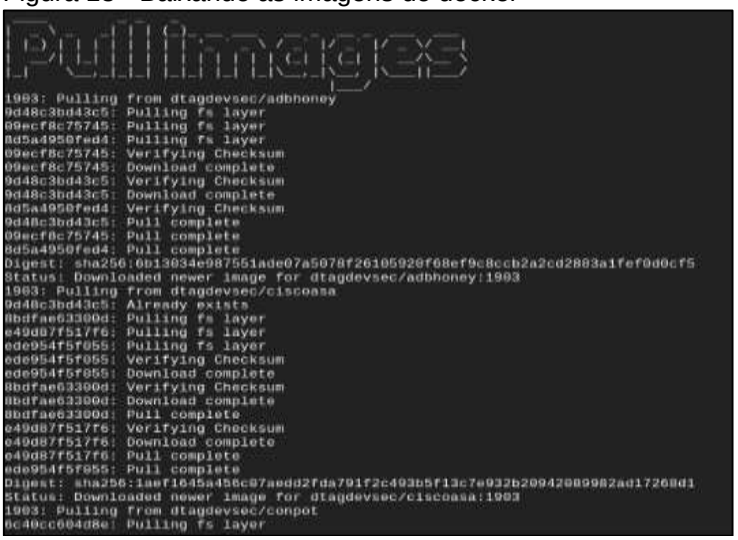
Ambos os números de portas, 64295 e 64297 são importantes, pois posteriormente é delas que será feito o *login* no sistema *honeypo*t, por padrão.
Para fazer *login* na porta ssh 64295 e no sistema com o painel *dashboard* porta 64297, esse esquema é indicado na Figura 12.

Figura 12 - Configuração automática

Fonte: Do Autor (2019).

O T-Pot *honeypot*, é fortemente baseado em *docker*, *docker-compose*.
Os sensores são totalmente dockerizadas, como pode ser visualizado na Figura 13.

Figura 13 - Baixando as imagens do docker



Fonte: Do Autor (2019).

A figura 14 ilustra uma atualização dos endereços IPs do honeypot no momento da configuração.

Figura 14 - Atualizando os IPs do servidor

Fonte: Do Autor (2019).

Na figura 15 foi feita a configuração do *firewall*. É importante criar regras de acesso à Internet, e restringir o acesso a porta ssh 64295 e ao portal de administração da web gui 64297. Pois nesse processo a porta ssh padrão (22) será usado como *honeypot*, assim como no caso das portas 80 e 443, que normalmente são usadas para exibir páginas da web, serão usadas como *honeypots* também. Portanto, será usado a porta 64297 para conectar-se ao navegador com o nome de usuário e senha definidos durante a instalação.

Figura 15 - Criando regras de acesso

Nome	Tipo	Destinos	Filtros	Protocolos/portas	Ação	Prioridade	Rede
allow-other-higher	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:64298-65535 udp icmp	Permitir	1000	default
allow-other-tcp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:0-64294 udp icmp	Permitir	1000	default
default-allow-http	Entrada	http-server	Intervalos de IP: 0.0.0.0/0	tcp:80	Permitir	1000	default
default-allow-https	Entrada	https-server	Intervalos de IP: 0.0.0.0/0	tcp:443	Permitir	1000	default
ssh-access	Entrada	Aplicar a todas	Intervalos de IP: 177.183.238.125/32	tcp:64295	Permitir	1000	default
web-access	Entrada	Aplicar a todas	Intervalos de IP: 177.183.238.125/32	tcp:64297	Permitir	1000	default
default-allow-icmp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	icmp	Permitir	65534	default
default-allow-internal	Entrada	Aplicar a todas	Intervalos de IP: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Permitir	65534	default
default-allow-rdp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:3389	Permitir	65534	default
default-allow-ssh	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:22	Permitir	65534	default

Fonte: Do Autor (2019).

Na interface Kibana, seleciona-se a opção *dashboard*, seguido de um *click* em T-Pot e logo será obtido gráficos de todos ataques efetuados. O que será abordado logo mais em resultados, como indicado na Figura 16.

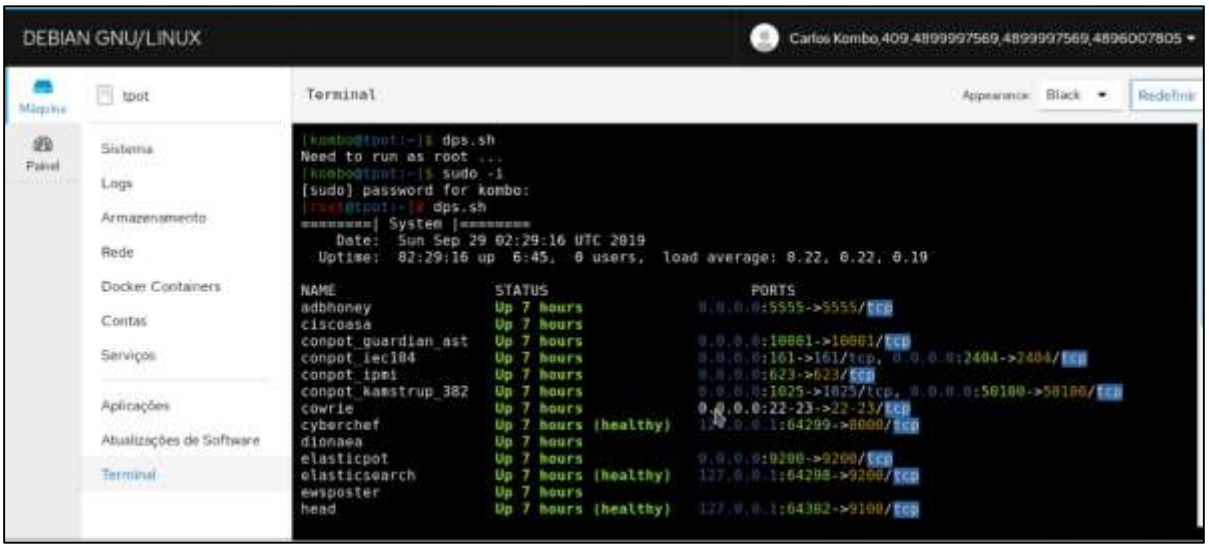
Figura 16 - Interface web

Fonte: Do Autor (2019).

Na figura 17 e 18, tem-se todos os sensores iniciados, rodando um único comando apenas:

~$ dps.sh

Figura 17 - Sensores iniciados



Fonte: Do Autor (2019).

Figura 18 - Sensores em execução

Fonte: Do Autor (2019).

Cada sensor do T-Pot simula serviços diferentes, como no caso do conpot que simula um sistema de controle industrial, o sensor *cowrie* que imita um servidor ssh, e o *mailoney*, por exemplo, que simula um servidor de e-mail.

E tem o suricata, que é um sistema de detecção de intrusão IDS/IPS que usa conjunto de regras para monitorar o tráfego de rede e disparam alertas sempre que ocorrem eventos suspeitos ou atividades mal-intencionadas.

Basicamente, o que acontece quando o sistema é iniciado é:

a) Iniciar sistema host
b) Iniciar todos os serviços necessários (por exemplo, *cockpit* e *docker*).
c) Iniciar todos os containers do *docker* por meio do *docker-compose* (honeypots, IDS, suricata).

Onde cada sensor recebe todo o tráfego TCP e UDP em portas especificas, por padrão, como ilustrado no quadro 02.

Quadro 2 - Sensores honeypots e portas

Honeypot	**Protocolos**	**Portas**
Conpot	TCP	81, 102, 502
Conpot	UDP	161
Cowrie	TCP	22
Dionaea	TCP	21, 42, 135,443, 445, 1433, 3306, 5060, 5061
Dionaea	UDP	69, 5060
Tanner	TCP	80
Honeytrap	TCP	25, 110, 139, 3389, 4444, 5900, 21000

Fonte: Adaptado

O *honeytrap* para além de observar ataques contra serviços TCP ou UDP, ele também liga dinamicamente qualquer porta que não seja coberta por outros sensores *honeypot*.

6.2 RESULTADOS E DISCUSSÃO

Com a pesquisa realizada neste trabalho e a aplicação dos fundamentos obtidos por meio dos levantamentos bibliográficos, assim como a implementação da ferramenta, foi possível monitorar a rede durante 27 dias e coletar dados de ataques, vindo de alguns países do mundo.

A ferramenta apresenta uma interface muito intuitiva, que possibilita ainda consultar o banco de dados dos ataques recebidos, e entender como os atacantes tentam comprometer cada máquina. Por exemplo, percebe-se uma nuvem de tags com os usuários e senhas mais testadas para entrar no honeypot cowrie, que simula ser um servidor ssh, representado na Figura 19.

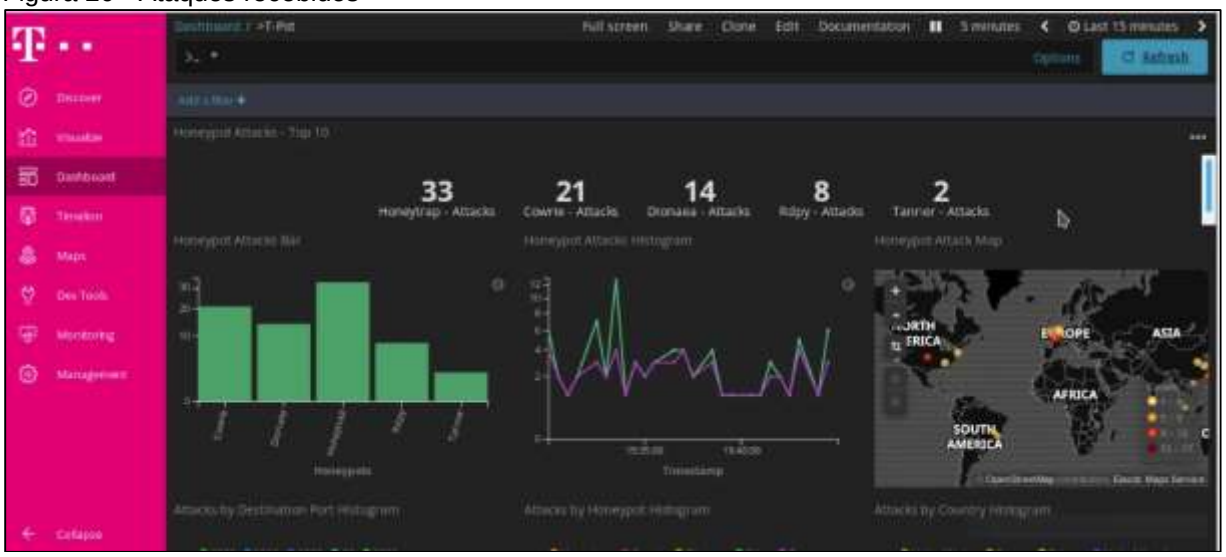
Figura 19 - Tagcloud

Fonte: Do Autor (2019).

O painel padrão mostra com eficiência todos os ataques coletados, como pode ser visualizado logo abaixo, na figura 20. Onde se verificou que o sensor *honeytrap*, seguido pelo *cowrie* são os que mais estão recebendo ataques até ao momento, pois o número de eventos é dinâmico.

Do lado, tem-se o mapa, que permite analisar os dados de ataques e conhecer de uma forma geográfica em qual parte do mundo estão vindos os ataques.

Figura 20 - Ataques recebidos



Fonte: Do Autor (2019).

Na figura 21 é possível observar a distribuição dos sistemas operacionais, utilizados pelos atacantes em várias partes do mundo, assim como suas reputações e os respetivos países que mais efetuaram os ataques.

Figura 21 - Origem dos ataques

Fonte: Do Autor (2019).

Ter o suricata IDS/IPS analisando o trafego é de extrema importância, pois é possível obter uma visão mais aprofundada de quais tipos de ataques estão atingindo o sistema, e também permite uma melhor pesquisa, caso se busque por ataques específicos, como pode ser visualizado na Figura 22.

Figura 22 - Suricata alertas

Suricata Alert Signature - Top 10

ID	Description	CNT
2100560	GPL POLICY VNC server response	4,922
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	3,890
2002920	ET POLICY VNC Authentication Failure	2,494
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)	2,494
2013031	ET POLICY Python-urllib/ Suspicious User Agent	1,506
2017515	ET INFO User-Agent (python-requests) Inbound to Webserver	1,272
2009582	ET SCAN NMAP -sS window 1024	324
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	309
2402000	ET DROP Dshield Block Listed Source group 1	213
2100384	GPL ICMP_INFO PING	133

Fonte: Do Autor (2019).

No painel, Kibana são reportados também todas as portas que estão sendo atacadas por países, como ilustrado na figura 23.

Figura 23 - As portas atacadas

Fonte: Do Autor (2019).

Os logs gerados pelos ataques podem ser visualizados em *logstash*, e explorados de forma interativa em tempo real, fazendo buscas por datas, ver os endereços IPs e seus países de origem, cidade e entre outros.

As figuras 24 e 25 são apenas algumas telas dos logs gerados durante a coleta de ataque na fase de monitoramento de 27 dias.

Figura 24 - Log dos ataques

Fonte: Do Autor (2019).

Figura 25 - Log dos ataques

Fonte: Do Autor (2019).

6.2.1 Simulação de Ataques

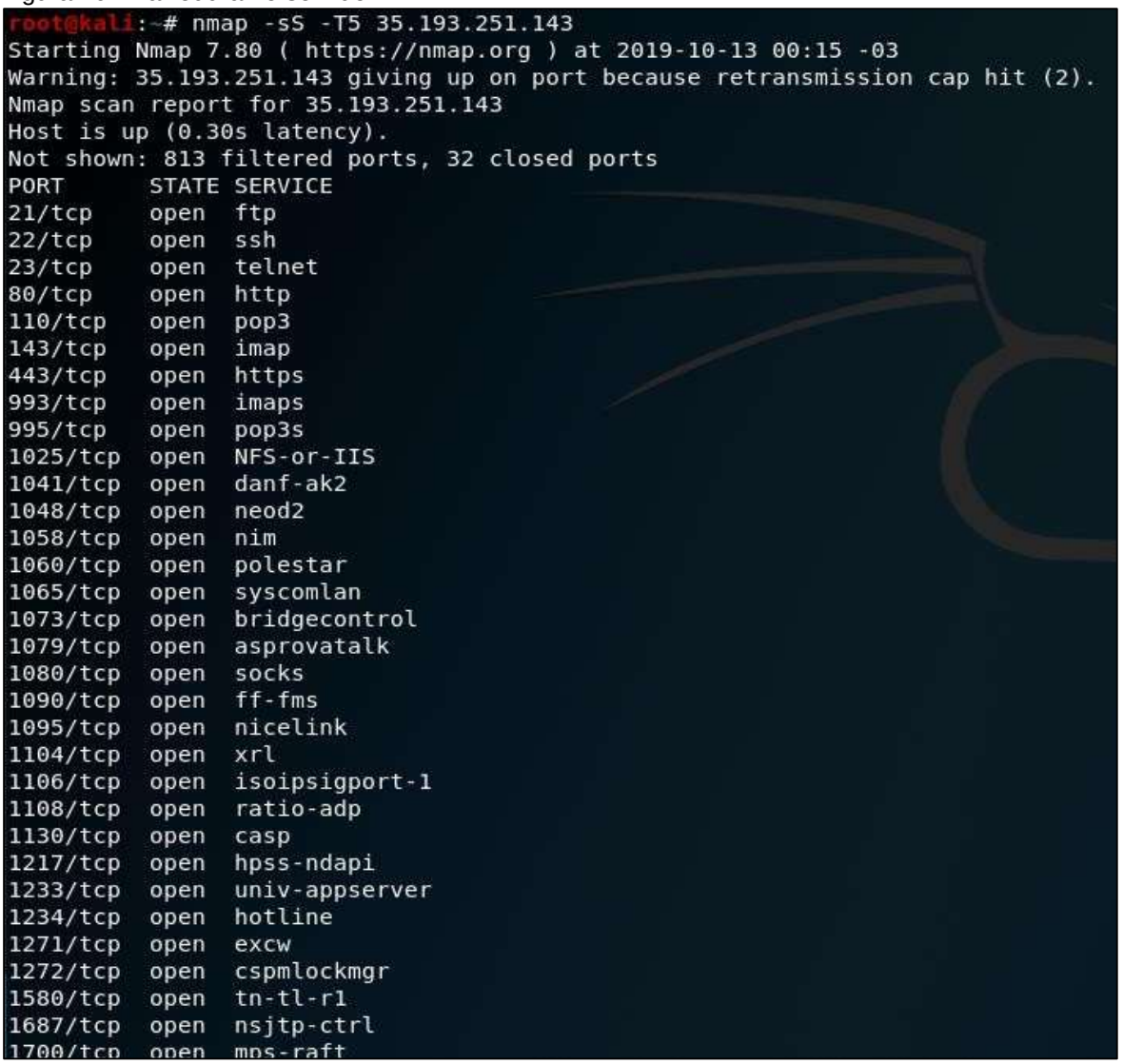
Foram feitas varreduras com o nmap e o nikto. Com o nmap buscou-se saber quais serviços e portas estavam abertas, e com o nikto, buscou-se por possíveis vulnerabilidades no servidor. A imagem 27 mostra todas as portas falsas abertas no servidor honeypot.

nmap -sS -T5 35.193.251.143

Onde: - sS está relacionado com a técnica conhecida por *half-open*, pois não abre uma conexão TCP completa. A grande vantagem desse parâmetro é que há possiblidades de o alvo não detectar esse *scanning* de portas.

O -T5 é relativo ao tempo, a rapidez que o *nmap* executa os *scans*.

Figura 26 - Varredura no servidor



Fonte: Do Autor (2019).

Como mencionado acima, realizou-se também um *scan* com o *nikto* em busca de vulnerabilidades no servidor. A filtragem x-xss, que geralmente padrão nos navegadores, não foi definido, o que poderia ocasionar um ataque de *script*.

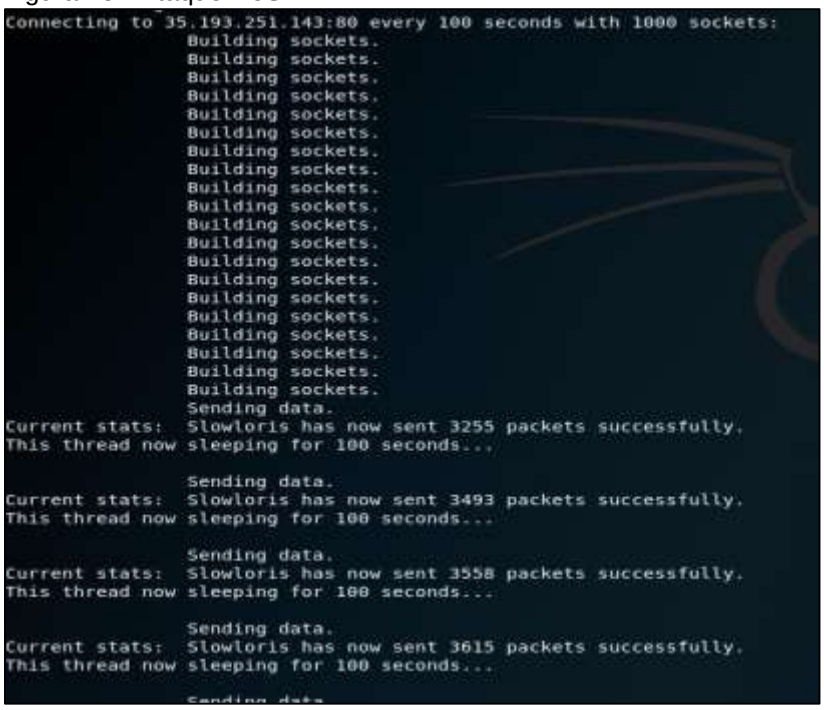
A figura 28 mostra algumas dessas vulnerabilidades.

Figura 27 - *Scan* com *nikto*

Fonte: Do Autor (2019).

Foram simulados alguns ataques como: DoS, força bruta, e os *scan*s com *nmap*, sparta e o *nikto*. Na figura 28, tem-se uma simulação de ataque DoS feita com a ferramenta *slowloris* no *kali linux*. O ataque basicamente consiste em sobrecarregar um computador ou servidor, apartir do envio de várias requisições, tornando assim, indisponíveis os recursos do sistema por um período.

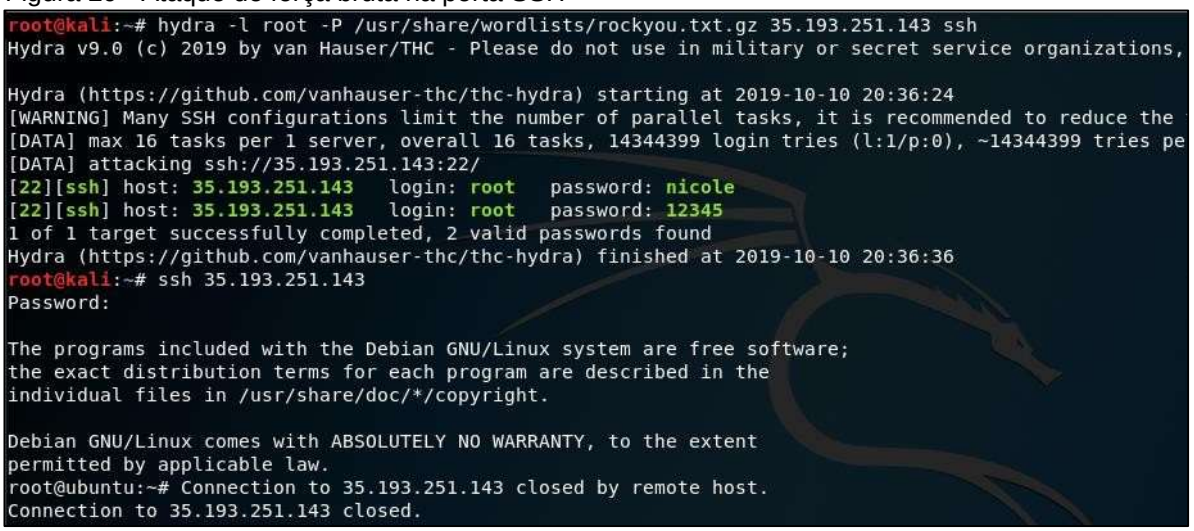
Figura 28 - Ataque DoS



Fonte: Do Autor (2019).

As figuras 29 e 30 também ilustra como foi feita a simulação de ataques de força bruta, na porta SSH e FTP, com o uso do *hydra*. O *rockyou* é uma das *wordlist* que o *hydra* usa para poder efetuar o ataque. Ele vai tentando todas as combinações de senhas disponíveis na wordlist até conseguir concretizar o ataque, ou seja, até invadir o servidor ou o sistema alvo.

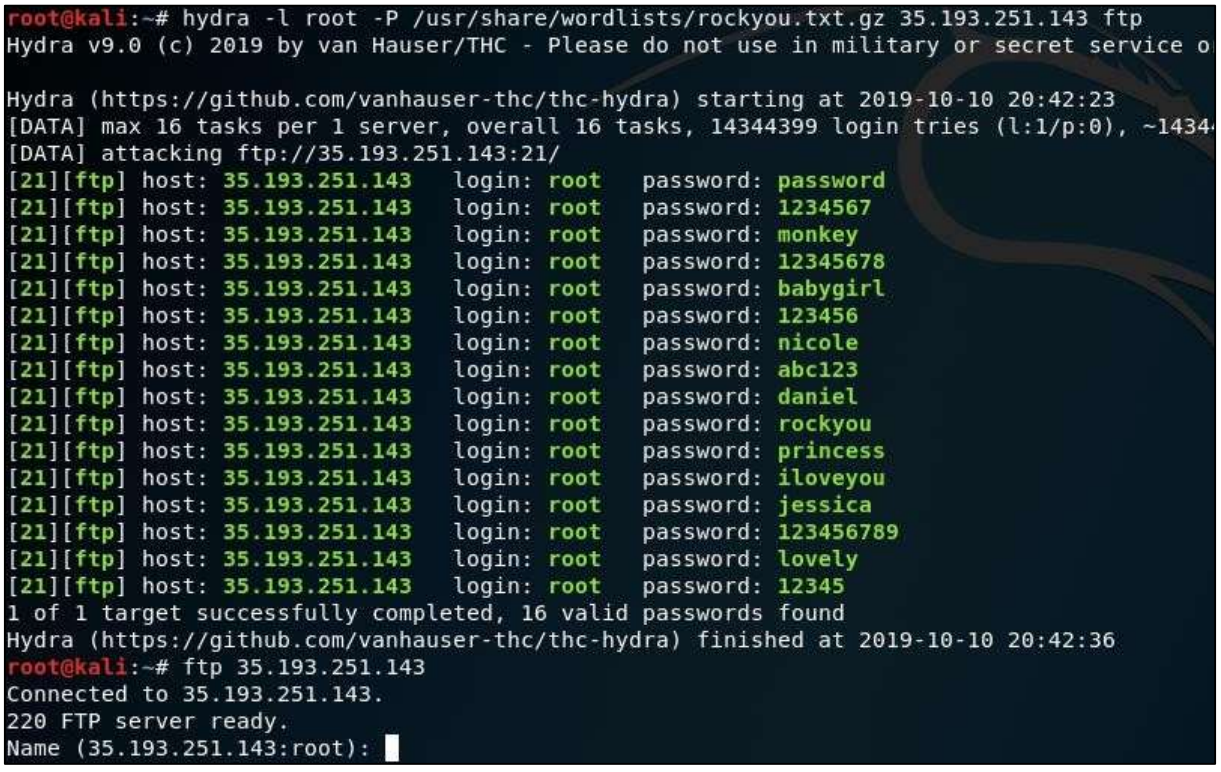
Figura 29 - Ataque de força bruta na porta SSH



Fonte: Do Autor (2019).

O comando -L, diz respeito ao usuário que se quer atacar, e o comando -P, diz respeito à porta que se pretende invadir, como mostrado na Figura 30.

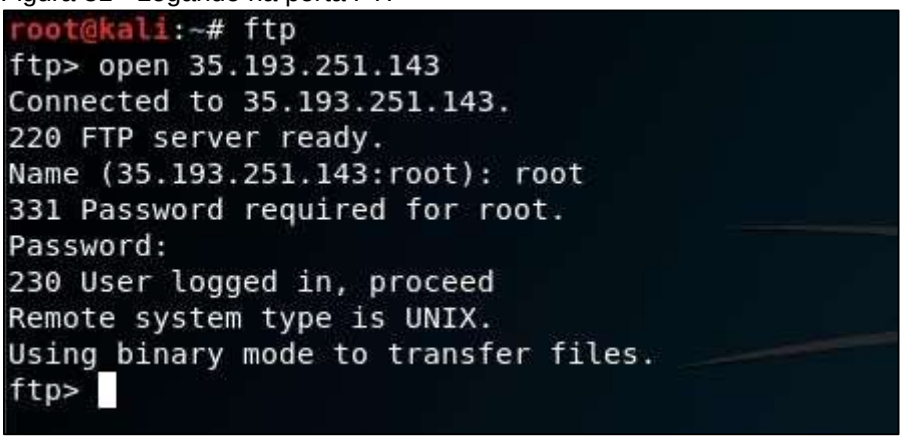
Figura 30 - Ataque de força bruta na porta FTP



Fonte: Do Autor (2019).

Na figura 31 observa-se o acesso na porta FTP do servidor, após a concretização do ataque de força bruta.

Figura 31 - Logando na porta FTP



Fonte: Do Autor (2019).

A figura 32 mostra um ataque onde foi utilizado o sparta, que é uma ferramenta gráfica do *kali linux*, ela invoca várias ferramentas para fazer ataques e varreduras na rede, de modo a poupar tempo no momento de *pentest* (testes de intrusão).

Figura 32 – Ataques com Sparta

Fonte: Do Autor (2019).

6.2.2 Análise dos resultados

Durante o monitoramento da rede, foram coletados ataques, que muitos deles são *botnets*, que por sua vez são uma rede de agentes de software ou *bots* que executam de forma autônoma, ou seja, uma grande rede de zumbis que obedecem a um computador principal. Observou-se na figura 20, que a maioria dos ataques foram coletados pelos sensores honeytrap, cowrie e dionaea. Com um total de 33 ataques

contra serviços de rede, 21 ataques de força bruta, e 14 ataques de malwares (softwares maliciosos). O sensor rdpy registrou 8 ataques de *man in the middle*, e o sensor tanner registrou 2 ataques web. Apartir dos resultados observou- se também que o sistema mais utilizado pelos atacantes na concretização desses ataques foi o sistema Linux. Na *tagcloud* da figura 19 pode-se observar cerca de 43 interações de shell e senhas mais testadas durante as tentativas de invasão e os seus nomes de usuário. Apesar do mapa não mostrar as origens dos ataques por continentes, o que acaba não ficando muito claro sobre quais países estão realizando os ataques, na outra tag da interface kibana podem ser observados esses países, e inclusive o ranking dos quais países estão realizando mais ataques até ao momento, assim como ilustrado na figura 21. Também verificou-se, que os países mais atacantes são os Estados Unidos, China, Holanda e Brasil. A figura 23 traz a ordem das portas mais atacadas: 8088, 3389, 5595, 9203, 81, 5060, 23, 42012, 47134, 60001, 80.

O suricata disparou alertas de respostas de conexões, *exploits*, *scan* com *nmap, backdoor doublepulsar* (que permite que o invasor injete qualquer carga útil bruta de código de shell), e tentativas de autenticação.

Na simulação de ataques observou-se algumas vulnerabilidades como xss, senhas fracas, e muitas delas não recomendadas, como no caso da senha 12345 do usuário root, ilustrado na figura 30. Outro dado importante e curioso, foi o ataque de força bruta realizado com o hydra. O ataque encontrou várias senhas e usuários root na mesma porta 21, como ilustrado na figura 31 e foi possível logar com várias dessas senhas descobertas. A figura 32 foi somente um dos casos.

6.2.3 Recomendações para melhorias na segurança da informação

(a) Desenvolver ferramentas para realização de testes de desempenho e disponibilidade, visando o comportamento da rede, e de sistemas em possíveis cenários de sobrecarga (CLAVIS, 2019).
(b) Identificar vulnerabilidades nos softwares e atualiza-los ou substitui-los (POSITIVO, 2017).
(c) Planejar um redimensionamento de recursos críticos a fim de melhorar a disponibilidade dos sistemas e aplicações dentro da organização (TOTVS, 2018).
(d) Definir uma agenda de correções de vulnerabilidades encontradas a partir de atualizações de softwares e novas configurações de ferramentas (INFONOVA, 2018).
(e) Realizar auditoria de testes de invasão (INOVE DADOS, 2019).

(f) Criar políticas de segurança personalizadas, de maneira a manter as soluções eficazes e atuais, substituindo assim as políticas ineficazes e depreciadas (TOTVS, 2018).

(g) Criar uma cultura de segurança, fazendo treinamentos e conscientização aos demais membros da organização (ALERTA SECURITY, 2019).

(h) Criar uma equipe de respostas a incidentes de segurança (CLAVIS, 2019)

(i) Fazer automatização de *backups*. Tendo em conta que a disponibilidade é um dos pilares da segurança da informação, automatizar *backups* se torna uma ação de suma importância quando se precisa reforçar questões ligadas a disponibilidade (POSITIVO, 2017).

(j) Utilizar ferramentas de criptografia para senhas, com o intuito de impedir com que os conteúdos das senhas possam ser acessados por softwares maliciosos, hackers ou pessoas indevidas. São recursos que impossibilitam a leitura da informação, ainda que o sistema tenha sido invadido (TOTVS, 2018).

(k) Configurar *firewalls* é de certeza uma das maneiras de se proteger informações da organização. Fazendo a filtragem do fluxo de dados e permitindo apenas acessos autorizados (ALERTA SECURITY, 2019).

(l) Estabelecer controle de acesso dentro da organização, com a ideia de restringir certa informação a grupos específicos, evitando assim a exclusão acidental ou ações inadequadas dos usuários (CLAVIS, 2019).

(m) Mudar as senhas constantemente, usando senhas fortes e únicas, misturando letras e números. Dessa maneira é possível dificultar ataques de força bruta, que acontecem a todo o momento (TOTVS, 2018).

7. CONCLUSÃO

A realização do presente trabalho de conclusão de curso, possibilitou uma análise de como a escolha de ferramentas adequadas, podem ajudar a melhorar a segurança da informação. Além disso, também permitiu uma pesquisa aprofundada sobre diversos ataques e obter dados mais consistentes de seu funcionamento.

O trabalho proporcionou ainda adquirir conhecimentos em diversas áreas, agregando a importância de se ter *honeypots* em uma organização. Foi possível perceber a evolução dos *honeypots*, assim como a sua implementação nos dias de hoje. Monitoramento e simulação de ataques foram os principais conceitos que direcionaram essa pesquisa, levando a execução das técnicas diversas abordadas nesse trabalho.

As técnicas e tecnologias utilizadas foram no intuito de buscar atender um objetivo principal: monitorar invasões, simular ataques e analisar os resultados de um servidor *honeypots* em um ambiente controlado. Vale ressaltar que pela indisponibilidade da empresa, os testes foram feitos em um ambiente controlado, porém com resultados satisfatórios. Verificou-se uma coleta de ataques considerável, conforme mostra a figura 20 nos resultados obtidos. Permitindo dessa maneira, que os objetivos propostos fossem alcançados.

Os objetivos específicos listados para a elaboração dessa pesquisa foram todos atingidos, o que por sua vez, foram os responsáveis por direcionar o desenvolvimento da pesquisa.

Os logs gerados na coleta de ataques conseguiram mostrar às informações necessárias dos atacantes de vários pontos do mundo, de igual modo à ferramenta mostrou-se muito eficaz, durante o período de monitoramento e período de testes. Pode-se então dizer, que com uso de *honeypots* em ambientes organizacionais e não só, é possível obter um mapeamento das atividades maliciosas direcionadas aos servidores, e orientando assim os administradores de redes a tomarem medidas preventivas para melhorarem cada vez mais segurança.

Dada a importância do assunto, torna-se então necessário cada vez mais pesquisas voltadas a melhorar a segurança da informação, assim como novas formas de implementar soluções com *honeypots.*

Durante o processo de implantação do *honeypots*, algumas dificuldades foram encontradas, logo após duas semanas a empresa mostrou-se indisponível para dar sequência ou permitir a continuidade da pesquisa em seu espaço. Por outro lado, certas ferramentas perderam suporte pelos mantenedores, ou seja, ficaram obsoletas, o que ocasionou em uma grande paralisia no prosseguimento do trabalho e outras ferramentas, como no caso do mhn, que é um gerenciador de honeypots, desenvolvido pela *Anomali* (antiga *ThreadStream*). Após a implantação com sucesso, alguns problemas de configurações foram surgindo, onde foi possível entrar em contato com *Anomali*, buscando por um possível suporte, porém responderam apenas um e-mail em duas ocasiões. Foi difícil gerir essa situação e achar outra solução que atendesse igual. Porém, com a ajuda do embasamento teórico adquirido durante o levantamento bibliográfico realizado, foi possível compensar e contornar a essas dificuldades.

Como sugestão para trabalhos futuros, propõe-se aplicar um estudo comparativo, implantando um dos dois honeypots mais recentes, o T-Pot no google *cloud* e o mhn na aws e analisar os seus comportamentos, a coleta de seus ataques e qual mais eficiente, e assim o mais recomendável para um ambiente empresarial ou ambiente de produção. Propõe-se também que na realização dos ataques simulados, no *shell* do sistema invadido, serviços ou portas invadidas, possam ser feitos testes, rodando algum comando que consiga comprometer o sistema operacional, como o caso do comando rm-rf /, de modos a serem analisados o desempenho, o comportamento do servidor, assim como até que ponto o *honeypot* pode auxiliar na segurança da informação de forma eficiente e ativa.

REFERÊNCIAS

ABNT. NBR 27002; **tecnologia da informação - técnicas de segurança - código de política para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005. Disponível em: < http://www.concursopedia.com>. Acesso em: 20/10/2018.

ALBERTUS *et al*. **Security fix release:** Got 10 VestaCP servers exploited. 2018. Vesta Control Panel - Forum. Disponível em: <https://forum.vestacp.com/viewtopic.php?p=68594#p68594>. Acesso em: 07 maio 2018.

ALERTA SECURITY (São Paulo). Como permanecer Seguro contra um ataque DDoS! 2019. Disponível em: <https://www.alertasecurity.com.br/como-permanecer-seguro-contra-um-ataque-ddos/>. Acesso em: 28 out. 2019.

ARAUJO, Everson Santos. **Introdução à Segurança da Informação**. 2008.

ASSUNÇÃO, Marcos Flavio Araújo. **Aprenda a detectar e enganar invasores.** Honeypots e Honeynets - Aprenda a Detectar e Enganar Invasores Ed. Florianópolis: Visual Books, 2008.

_____. **Guia do Hacker Brasileiro**. 2. ed. Florianópolis: Visual Books, 2002;

_____. **Guia do hacker brasileiro**. Marcos Flávio Araújo Assunção, 2002.

_____**. Honeypots e Honeynets**: aprenda a detectar e enganar invasores. Florianópolis, Visual Books, 2009.

AZEVEDO, Tiago Souza**. Honeypots - A segurança através do disfarce**. 2005. Disponível em: <http://www.ravel.ufrj.br/honeypots-segurança-através-disfarce>. Acesso em: 21 abr. 2018.

BARBOSA, Guilherme Augusto Ruani; SILVA, Maria Helena Barriviera e. **SEGURANÇA DA INFORMAÇÃO:** A PROTEÇÃO CONTRA O VAZAMENTO DE DADOS E SUA IMPORTÂNCIA PARA AS EMPRESAS PRIVADAS. Revista Eletrônica eF@ tec, v. 6, n. 1, p. 10-10, 2016.

BAREA, Emerson Rogério Alves, *et al*. **HonIoT: Arquitetura de Honeynet com Controle de Propagação de Malwares para Dispositivos de IoT**. In: Anais do II Workshop de Segurança Cibernética em Dispositivos Conectados. SBC, p. 23-36,2019.

CARDOSO, Diego Bento. **Política de segurança da informação para o departamento de segurança da faculdade do conhecimento.** 2013. 87 f. TCC (Graduação) - Curso de Tecnologia de Segurança da Informação das Faculdades Integrais, Faculdades Integradas Promove de Brasília, Guará, 2013.

CARVALHO, Luciano G. **Segurança de Redes.** Rio de Janeiro: Ciência Moderna, 73p, 2005.

CARISSIMI, Alexandre. **Virtualização: da teoria a solução**. In: 26ə SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 26., 2008, São Paulo. Anais. São Paulo: Instituto de Informática, p. 174 – 207, 2008.

CERT.Br. **Cartilha de segurança para internet**. São Paulo: Comitê Gestor de Segurança do Brasil, 2012., v4. Disponível em: < http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 15/10/2018.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Honeypots e honeynets**: Definições e aplicações., ver, v. 1, 2007. Disponível em:<http://www.cert.br/docs/whitepapers/honeypots-honeynets/> Acesso em 03 de novembro de 2018.

CERT.br. **Honeypots e honeynets:** Definições e aplicações. Disponível em:
DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** 3. ed. Rio de Janeiro: Gizella Narcisi, 218 p,2000.

CLAVIS (Rio de Janeiro). **Sistema de Gerenciamento de Eventos e Informações de Segurança: Tenha visibilidade plena sobre os eventos e informações de segurança de sua organização.** 2019. Disponível em: <https://clavis.com.br/solucoes/octopus-siem-analise-de-seguranca-orientada-por-dados/>. Acesso em: 28 out. 2019.

CORDEIRO, Flávio. **Projeto Honeynet: Instalação e Pesquisa na Universidade Católica de Brasília.** 2007. 157 f. Monografia (Especialização) - Curso de Segurança

em Redes de Computadores, Tecnologia de Informação, Universidade Católica de Brasília, Brasília, 2008.

CORRÊA, Hamilton José. **Honeypots em ambiente ADSL: Um estudo de caso.** 2007. 109 f. Monografia (Especialização) - Curso de Gerencia de Redes de Computadores, Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2018.

DA SILVA ALVES, Bruno; CHARÃO, Andrea S.; LIMA, João Vicente F. **Uma Experiência de Execução de Aplicação MPI em Containers com *Docker* Swarm**. In: Anais da XIX Escola Regional de Alto Desempenho da Região Sul. SBC, 2019.

DOCKER DOCS. ***Docker* documentation**. 2019. Disponível em: <https://docs.*docker*.com/>. Acesso em: 23 out. 2019.

DTAG COMMUNITY HONEYPOT PROJECT. **Release T-Pot 19.03**. 2019. Disponível em: <https://dtag-dev-sec.github.io>. Acesso em: 03 set. 2019

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Marcio Tadeu de. **Política de Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

FONTES, Edison. **Segurança da Informação: O usuário faz toda a diferença.** São Paulo: Saraiva, 2006.

FRANCO, Lucio Henrique; BARBATO, Luiz Gustavo C.; MONTES, Antônio. **Instalação e uso de honeypot de baixa interatividade**. Centro de Pesquisas Renato Archer, São Paulo, p.1-88, 01 abr. 2004.

GARFINKEL, Simson; SPAFFORD, Gene; SCHWARTZ, Alan. **Practical UNIX and Internet security.** " O'Reilly Media, Inc.", 2003.

GOMES, Rafael. ***Docker* para desenvolvedores**. Salvador: Universidade Federal da Bahia, 2019.

GOMES, Rafael; SOUZA, Rodrigo. ***Docker* - Infraestrutura como código, com autonomia e replicabilidade**. Salvador: Universidade Federal da Bahia, 2015.

GUIMARAES, Alexandre Guedes; LINS, Rafael Dueire; OLIVEIRA, Raimundo. **Segurança com Redes Privadas Virtuais** VPNS, São Paulo: Brasport Livros e Multimídia. 2006.

HAGEN, J. M. at al. **Implementation and effectiveness of organizational information security measures**. Information Management & Computer Security, v.16, n. 4, p. 377-397, 2008. Disponivel em: <https://www.emeraldinsight.com/doi/abs/10.1108/09685220810908796> Acesso em 26 nov. 2018.

HAYDEN, Matt. **Aprenda em 24 horas redes**. 2. ed. Rio de Janeiro: Campus, 461 p,1999.

HIDALGO, Alexandre Henrique Picão; PEREIRA, Júlio Cesar. **SEGURANÇA EM REDES: HONEYPOTS E HONEYNETS**. Disponível em: <http://web.unipar.br/~seinpar/2015/_include/artigos/Alexandre_Henrique_Picão_Hidalgo.pdf>. Acesso em: 19 mar. 2018.

INFONOVA (São Paulo**). Melhores Práticas Para o Controle e a Segurança da TI**. 2018. Disponível em: <https://www.infonova.com.br/artigo/melhores-praticas-do-para-o-controle-e-a-seguranca-da-ti/>. Acesso em: 28 out. 2019

INOVE DADOS (Minas Gerais). **Soluções Customizadas em Segurança da Informação**. 2019. Disponível em: <https://inovedados.com.br/seguranca-da-informacao>. Acesso em: 28 out. 2019.

JUNIOR, José de Ribamar Braga Pinheiro; KON, Fabio. **Segurança em grades computacionais**. Mini-curso de segurança em Grades. Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP), 2007.

LIMA, Ricardo de**. WEBSERVICE HONEYPOT UTILIZANDO A BIBLIOTECA JHONEY.** 2014. 41 f. TCC (Graduação) - Curso de Ciência da Computação, Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau, 2015.

OLIVEIRA, Frederico Santos de. **Honeypot: Um Ambiente Para Análise De Intrusão**. 2007. 50 f. TCC (Graduação) - Curso de Ciência da Computação, Ciência da Computação, Universidade Federal de Lavras, Minas Gerais, 2008.

ORACLE. **About Linux Containers**. Disponível em: <https://docs.oracle.com/cd/E37670_01/E37355/html/ol_about_containers.html>. Acesso em: 23 out. 2019.

KHANJI, Salam *et al*. **Evaluation of Linux SMTP Server Security Aspects- A Case Study**. 2016. Disponível em: <https://ieeexplore.ieee.org/document/7476120/>. Acesso em: 21 abr. 2018

KUROSE, James F.; ROSE, Keith W. **Redes de computadores e a internet**: Uma abordagem top-down. 5. ed. São Paulo: Gabriela Trevisan, 602 p. Opportunity Translations, 2010.

LYRA, Mauricio Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

MARCELO, Antônio; PITANGA, Marcos. **Honeypots; A arte de iludir hackers**. Rio de Janeiro: Brasport, 2003.

MELO, Laerte Peotta de; AMARAL, Dino Macedo. **Estudo de taxonomia de ataques e atacantes em um honeypot de alta interação**, 2019. Disponível em: <https://www.scilit.net/article/7d7d949c2973ab8b9eea6b767e690983>. Acesso em: 21 abr. 2018.

MODOLON, Anderson Brunel. **Análise e Implementação de Honeypot em Ambiente Linux**. 2010. 113 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, 2010.

MOREIRA, Nilton S. S**egurança Mínima Uma Visão Corporativa da Segurança de Informações**. Rio de Janeiro: Axcel Books, 2001.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** Novatec editora, 2007.

NORTHCUT, Stephen *et al*. **Desvendando segurança em redes**: O guia definitivo para fortificação de perímetros de rede usando Firewall, VPNs, Roteadores e sistemas de detenção de intrusão. 3º ed. Rio de Janeiro: Campus, 2002. 650 p. Daniel Vieira.

O'BRIEN, J. A; MARAKAS, G. M**. Administração de Sistemas de Informação**.

Tradução Rodrigo Dubal; revisão técnica: Armando Dal Colleto. – 15. ed. Porto Alegre: AMGH, 2013.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PIMENTA, Alexandre Manuel Santareno; QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. JISTEM-**Journal of Information Systems and Technology Management**, 13.3: 533-552, 2016.

PINHEIRO, José Maurício dos Santos. **Ameaças e Ataques aos Sistemas de Informação:** Prevenir e Antecipar. Cadernos UniFOA, v. 3, n. 5, p. 11-21, 2017.

POSITIVO (Curitiba). Segurança da informação: conheça as 12 melhores práticas. 2017. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/>. Acesso em: 28 out. 2019.

PRADA, Dan Lucio *et al*. ***Docker* - apresentação da ferramenta**. In: CONGRESSO CATARINENSE DE CIÊNCIA DA COMPUTAÇÃO, 4., 2017, Rio do Sul. **Anais.** Rio do Sul: Unisul, v. 4, p. 46 – 56, 2017.

PWC. Cyber Laws and Cyber Security: The Jurisprudence and Judicature. Indian Journal of Computer Science, 3.6: 20-24,2018.

RODRIGUES, Fabrício dos Santos; SOUZA, Thiago Rafael de; DINIZ, Cristiano Antônio. **Avaliação da Ferramenta de Segurança da Informação Honeypot,** 2015. Disponível em: <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a91.pdf>. Acesso em: 19 mar. 2018.

RODRIGUES, Fabrício dos Santos; SOUZA, Thiago Rafael de; DINIZ, Cristiano Antônio. **Avaliação da Ferramenta de Segurança da Informação Honeypot.** Revista Pensar Tecnologia, v. 4, n. 1, 2015.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos sistemas de informação:** Gestão estratégica da segurança empresarial. Lisboa: Centro Atlântico, 256 p, 2003.

SÊMOLA, Marcos. **Gestão da segurança da informação**: Uma visão executiva. 7. ed. Rio de Janeiro: Elsevier, 2003. 156 p.

SOARES, Luis Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores das LANS, MANS E WANS às Redes ATM**. 2. ed. Rio de Janeiro: Campus, 705 p, 1995.

SORDI, José Osvaldo de; MARINHO, Bernadete de Lourdes; NAGY, Marcio. **Benefícios da arquitetura de software orientada a serviços para as empresas:** Análise Da Experiência Do Abn Amro Brasil. Revista de Gestão da Tecnologia e Sistemas de Informação, São Paulo, v. 3, n. 1, p.19-34, 30 abr. 2006.

SMITH. **Hackers Segredos e Confissões**. E-book de distribuição na Internet, 2007.

STARLIN, Gorki; NOVO, Rafael. **Segurança contra hacker**. Rio de Janeiro: Book Express, 342 p, 2000.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro: Elsevier, 945 p. Vandenberg D. de Sousa, 2003.

TEIXEIRA JUNIOR, José Helvécio *et al*. **Redes de computadores**: Serviços, administração e segurança. 2. ed. São Paulo: Makron Books, 493 p, 1999.

TURNBULL, James. **The *Docker* Book**. Creative Commons, 2014.

THOMAS, Tom. **Segurança de redes**: Primeiros Passos. Rio de Janeiro: Ciência Moderna, 2007.

TOTVS (Brasil). Explicamos os procedimentos de segurança da informação que você deve adotar. 2018. Disponível em: <https://www.totvs.com/blog/seguranca-da-informacao/>. Acesso em: 28 out. 2019.

TROST, Jason. **Modern Honey Network**: Open source honeynet management platform. 2014. Disponível em: <https://www.anomali.com/blog/mhn-modern-honey-network>. Acesso em: 27 ago. 2019.

VITALINO, Jeferson Fernando Noronha; CASTRO, Marcus André Nunes. **Descomplicando o *Docker***. Rio de Janeiro: Brasport, 2016.

VIRTI, Emerson; BERTHOLD, Leandro Márcio; TAROUCO, Liane**. Utilizando Honeypots para medição de atividade de rede não usual na internet**. 2013. 14 f. Tese (Doutorado) - Curso de Ciência da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2017.

WADLOW, Thomas A. **Segurança de redes: projeto e gerenciamento de redes seguras.** Rio de Janeiro: Campus, 269 p, 2000.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. **Building Internet Firewalls: Internet and Web Security.** " O'Reilly Media, Inc.", 2000.

APÊNDICE(S)

APÊNDICE A – Artigo

Monitoramento de Invasões, Simulação de Ataques de um Servidor Honeypot em Ambiente Controlado

Carlos António Kombo[1], Marcel Campos Inocencio[2]

[1]Acadêmico do Curso de Ciência da Computação

Universidade do Extremo Sul Catarinense (UNESC) - Criciúma, SC - Brasil

[2]Professor do Curso de Ciência da Computação

Universidade do Extremo Sul Catarinse (UNESC) - Criciúma, SC - Brasil

carloskombo.ck@gmail.com, marcel.inocencio@gmail.com

Abstract. The relentless pursuit, distribution, and processing of information, has been a major fuel for organizations in this new digital age, so information security has become an increasingly indispensable factor because of the value it adds to an organization. The paper presents a study on intrusion monitoring, simulation of attacks from a honeypot server in a controlled environment. Where the goal is to deploy an attack monitoring tool to a server and simulate intrusions by creating an ecosystem on the google cloud instance with the T-POT honeypot.

Resumo. A incessante busca, a distribuição e o processamento da informação, tem sido o grande combustível das organizações nessa nova era digital, assim sendo, a segurança da informação tem se tornado um fator cada vez mais indispensável, devido ao valor que ela agrega para uma organização. O trabalho apresenta um estudo sobre monitoramento de invasões, simulação de ataques de um servidor *honeypot* em ambiente controlado. Onde o objetivo é implantar uma ferramenta de monitoração de ataques a um servidor e simular invasões, criando um ecossistema na instância do *google cloud* com a implantação do T-POT *honeypot*.

1. INTRODUÇÃO

O crescimento das tecnologias tem proporcionado uma manipulação mais rápida e melhor das informações, e nesse universo todo, um dos principais focos em várias organizações é a questão da segurança. Tendo em conta a proporção de sistemas computacionais e o grande fluxo de dados dentro de uma rede, não importando se é uma grande ou pequena empresa (HIDALGO; PEREIRA, 2018).

A globalização tem permitido rápidos avanços tecnológicos, as

> oportunidades de negócios vêm e vão com a mesma velocidade desses avanços. Todos experimentam uma época de grandes transformações tecnológicas, econômicas e mercadológicas (NAKAMURA; GEUS, 2007).

Dependendo de quão sensível for a informação para a organização e, obviamente, dependendo do seu valor diante dos concorrentes ou para o mercado, a empresa precisa implementar controles sobre o uso (mesmo correto) dessas informações (FONTES, 2006).

O fato é que com a evolução destas tecnologias, onde novas ferramentas são criadas, novos equipamentos são desenvolvidos, as organizações passaram a aplicar e a expermentar cada vez mais essas inovações. Porém, cada vez mais que vão aderindo e expermentando essas inovações, vão ficando também cada vez mais susceptíveis aos mais variados tipos de situações que comprometem a integridade, confiabilidade e a disponibilidade da informação. Situações como tentativas de ataque ou invasões, que podem ser provenientes de usuarios mal-intencionados, ou até mesmo de um orgão qualquer (SÊMOLA, 2003).

2. TRABALHO DESENVOLVIDO

Para este trabalho implementou-se a ferramenta *honeypot T-Pot*, por ser uma das mais atuais, de código aberto, baseado em *docker*-compose e executado no Debian (Sid), incluindo versões *dockerizadas* de alguns sensores como: *conpot*, *cowrie*, *dionaea*, *tanner*, *rdpy* e *honeytrap*. A ferramenta escolhida permitiu a concretização da pesquisa por se mostrar ser mais atual, e não só, mais também pela praticidade e simplicidade de ser implantada e configurada. Vem sendo uma das plataformas de honeypots mais bem-sucedidas, não simplesmente pela sua baixa manutenção, e toda tecnologia que o envolve, mas também por causa dos bons painéis e sensores de investigação (DTAG, 2015).

Desenvolvida pela Deutsche Telekom (DTAG), com a finalidade de registrar tráfegos maliciosos que possam existir, estudá-los e analisá-los, permitindo assim melhorar a segurança da informação e todos ativos da organização a partir dos resultados ou logs gerados.

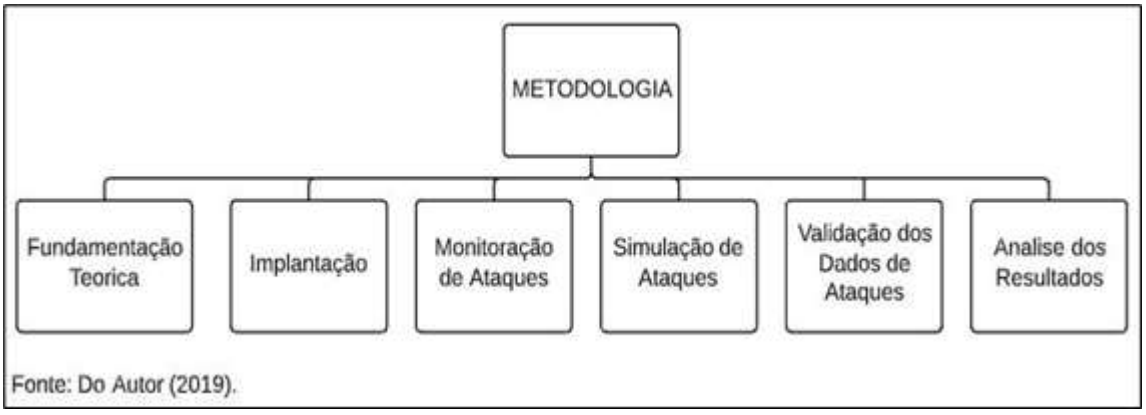
Implantar *honeypots* configurá-los e mantê-los ao longo do tempo, e na sequência, analisar os dados capturados sempre foi uma tarefa exigente e desafiadora. E isso fez com que não fossem adotados amplamente como solução, em alguns casos, devido a sua complexidade, apesar da ferramenta já ter sido madura. (ANOMALI, 2019).

O T-Pot apresenta vários sensores honeypots em execução paralela e redireciona o tráfego capturado na interface de rede para os honeypots mais adequados disponíveis. Os dados capturados são exibidos em painéis, permitindo analisar os ataques e fazer uma pesquisa sobre dos dados de um modo fácil (DTAG, 2015).

2.1 METODOLOGIA

Para a concretização deste trabalho foi elaborado um cronograma de levantamento bibliográfico relacionado a segurança da informação, políticas de segurança, vulnerabilidades, riscos, ameaças e ataques, serviços de redes, tipos de ataque, formas de ataque e motivação dos atacantes, e também foi feito uma busca sobre os honeypots mais atuais, bem como as novas formas de implementação, monitoração de ataques, simulação de ataques, validação dos dados de ataques, e a análise dos resultados gerados. A figura 6 mostra o passo a passo, da busca realizada.

Figura 33 – Metodologia utilizada



Fonte: Do Autor (2019).

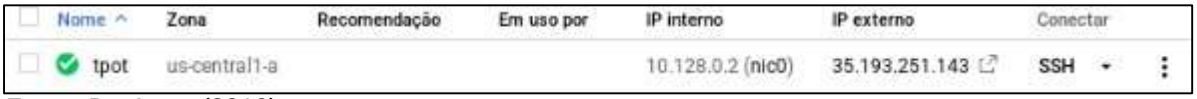
Primeiramente foi criada uma instância de VM do google cloud platform, com Debian buster. E em seguida foi implantada a ferramenta, com as suas devidas configurações. Foram criadas regras de acesso à Internet para então poder monitorar a rede e todos ataques possíveis. Na sequência, foi feita a simulação de ataques, e análise dos resultados dos dados de ataque coletado pela ferramenta.

O honeypot foi implantado obedecendo alguns requisitos mínimos para que o sistema funcionasse da melhor maneira, a saber:

1) 6-8 GB de *RAM* (menos *RAM* é possível, porém não aconselhável).
2) *SSD* de 128 GB (menor é possível, mas limita a capacidade de armazenamento).
3) Uma conexão com a Internet (ele baixa as imagens do *docker*).

Na figura 7, destacada abaixo, observa-se a criação do ambiente no *google cloud platform.*

Figura 7 - Criação da instância VM na nuvem



Fonte: Do Autor (2019).

Foram utilizados os comandos abaixo para atualizar a instancia:

~$ sudo apt-get update

~$ sudo apt-get upgrade

~$ sudo apt-get dist-upgrade

Durante o processo de instalação e configuração será solicitado duas vezes a inserção de uma senha. Uma é para o usuário kombo, e a outra é para o usuário T-Pot kombo (lembrando que o nome de usuário pode ser qualquer outro, nesse caso foi escolhido o nome de usuário kombo). Também serão instaladas todas as dependências necessárias para o funcionamento correto do T-Pot, representado na Figura 11.

Figura 34 - Instalação T-Pot e dependências necessárias

```
kombo@tpot:~/.ssh/tpotce$ sudo ./install.sh

### Checking for root: [ OK ]
### Installing apt-fast
Hit:1 http://deb.debian.org/debian buster InRelease
Hit:2 http://packages.cloud.google.com/apt cloud-sdk-buster InRelease
Hit:3 http://deb.debian.org/debian buster-updates InRelease
Hit:4 http://deb.debian.org/debian buster-backports InRelease
Hit:5 http://packages.cloud.google.com/apt google-cloud-packages-archive-keyring-buster InRelease
Hit:6 http://packages.cloud.google.com/apt google-compute-engine-buster-stable InRelease
Hit:7 http://security.debian.org/debian-security buster/updates InRelease
Reading package lists... Done
```

Fonte: Do Autor (2019).

2.2 RESULTADOS E DISCUSSÃO

Com a pesquisa realizada neste trabalho e a aplicação dos fundamentos obtidos por meio dos levantamentos bibliográficos, assim como a implementação da ferramenta, foi possível monitorar a rede durante 27 dias e coletar dados de ataques, vindo de alguns países do mundo.

A ferramenta apresenta uma interface muito intuitiva, que possibilita ainda consultar o banco de dados dos ataques recebidos, e entender como os atacantes tentam comprometer cada máquina. Por exemplo, percebe-se uma nuvem de tags com os usuários e senhas mais testadas para entrar no honeypot cowrie, que simula ser um

servidor ssh, representado na Figura 19.

Figura 35 - Tagcloud

Fonte: Do Autor (2019).

O painel padrão mostra com eficiência todos os ataques coletados, como pode ser visualizado logo abaixo, na figura 20. Onde se verificou que o sensor *honeytrap*, seguido pelo *cowrie* são os que mais estão recebendo ataques até ao momento, pois o número de eventos é dinâmico.

Do lado, tem-se o mapa, que permite analisar os dados de ataques e conhecer de uma forma geográfica em qual parte do mundo estão vindos os ataques.

Figura 36 - Ataques recebidos

Fonte: Do Autor (2019).

2.3 ANÁLISE DOS RESULTADOS

Durante o monitoramento da rede, foram coletados ataques, que muitos deles são *botnets*, que por sua vez são uma rede de agentes de software ou *bots* que executam de forma autônoma, ou seja, uma grande rede de zumbis que obedecem a um

computador principal. Observou-se na figura 20, que a maioria dos ataques foram coletados pelos sensores honeytrap, cowrie e dionaea. Com um total de 33 ataques contra serviços de rede, 21 ataques de força bruta, e 14 ataques de malwares (softwares maliciosos). O sensor rdpy registrou 8 ataques de *man in the middle*, e o sensor tanner registrou 2 ataques web. Apartir dos resultados observou- se também que o sistema mais utilizado pelos atacantes na concretização desses ataques foi o sistema Linux. Na *tagcloud* da figura 19 pode-se observar cerca de 43 interações de shell e senhas mais testadas durante as tentativas de invasão e os seus nomes de usuário. Apesar do mapa não mostrar as origens dos ataques por continentes, o que acaba não ficando muito claro sobre quais países estão realizando os ataques, na outra tag da interface kibana podem ser observados esses países, e inclusive o ranking dos quais países estão realizando mais ataques até ao momento, assim como ilustrado na figura 21. Também verificou-se, que os países mais atacantes são os Estados Unidos, China, Holanda e Brasil. A figura 23 traz a ordem das portas mais atacadas: 8088, 3389, 5595, 9203, 81, 5060, 23, 42012, 47134, 60001, 80.

O suricata disparou alertas de respostas de conexões, *exploits*, *scan* com *nmap, backdoor doublepulsar* (que permite que o invasor injete qualquer carga útil bruta de código de shell), e tentativas de autenticação.

Na simulação de ataques observou-se algumas vulnerabilidades como xss, senhas fracas, e muitas delas não recomendadas, como no caso da senha 12345 do usuário root, ilustrado na figura 30. Outro dado importante e curioso, foi o ataque de força bruta realizado com o hydra. O ataque encontrou várias senhas e usuários root na mesma porta 21, como ilustrado na figura 31 e foi possível logar com várias dessas senhas descobertas. A figura 32 foi somente um dos casos.

3. CONCLUSÃO

A realização do presente trabalho de conclusão de curso, possibilitou uma análise de como a escolha de ferramentas adequadas, podem ajudar a melhorar a segurança da informação. Além disso, também permitiu uma pesquisa aprofundada sobre diversos ataques e obter dados mais consistentes de seu funcionamento.

O trabalho proporcionou ainda adquirir conhecimentos em diversas áreas, agregando a importância de se ter *honeypots* em uma organização. Foi possível perceber a evolução dos *honeypots*, assim como a sua implementação nos dias de hoje. Monitoramento e simulação de ataques foram os principais conceitos que direcionaram essa pesquisa, levando a execução das técnicas diversas abordadas nesse trabalho.

As técnicas e tecnologias utilizadas foram no intuito de buscar atender um objetivo principal: monitorar invasões, simular ataques e analisar os resultados de um servidor *honeypots* em um ambiente controlado. Vale ressaltar que pela indisponibilidade da empresa, os testes foram feitos em um ambiente controlado, porém com resultados satisfatórios. Verificou-se uma coleta de ataques considerável, conforme mostra a figura 20 nos resultados obtidos. Permitindo dessa maneira, que os objetivos propostos fossem alcançados.

Os objetivos específicos listados para a elaboração dessa pesquisa foram todos atingidos, o que por sua vez, foram os responsáveis por direcionar o desenvolvimento da pesquisa.

Os logs gerados na coleta de ataques conseguiram mostrar às informações necessárias dos atacantes de vários pontos do mundo, de igual modo à ferramenta mostrou-se muito eficaz, durante o período de monitoramento e período de testes. Pode-se então dizer, que com uso de *honeypots* em ambientes organizacionais e não só, é possível obter um mapeamento das atividades maliciosas direcionadas aos servidores, e orientando assim os administradores de redes a tomarem medidas preventivas para melhorarem cada vez mais segurança.

REFERÊNCIAS

ABNT. NBR 27002; **tecnologia da informação - técnicas de segurança - código de política para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005. Disponível em: < http://www.concursopedia.com>. Acesso em: 20/10/2018.

ALBERTUS *et al*. **Security fix release:** Got 10 VestaCP servers exploited. 2018. Vesta Control Panel - Forum. Disponível em: <https://forum.vestacp.com/viewtopic.php?p=68594#p68594>. Acesso em: 07 maio 2018.

ALERTA SECURITY (São Paulo). Como permanecer Seguro contra um ataque DDoS! 2019. Disponível em: <https://www.alertasecurity.com.br/como-permanecer-seguro-contra-um-ataque-ddos/>. Acesso em: 28 out. 2019.

ARAUJO, Everson Santos. **Introdução à Segurança da Informação**. 2008.

ASSUNÇÃO, Marcos Flavio Araújo. **Aprenda a detectar e enganar invasores.** Honeypots e Honeynets - Aprenda a Detectar e Enganar Invasores Ed. Florianópolis: Visual Books, 2008.

_____. **Guia do Hacker Brasileiro**. 2. ed. Florianópolis: Visual Books, 2002;

_____. **Guia do hacker brasileiro**. Marcos Flávio Araújo Assunção, 2002.

_____**. Honeypots e Honeynets**: aprenda a detectar e enganar invasores. Florianópolis, Visual Books, 2009.

AZEVEDO, Tiago Souza**. Honeypots - A segurança através do disfarce**. 2005. Disponível em: <http://www.ravel.ufrj.br/honeypots-segurança-através-disfarce>. Acesso em: 21 abr. 2018.

BARBOSA, Guilherme Augusto Ruani; SILVA, Maria Helena Barriviera e. **SEGURANÇA DA INFORMAÇÃO:** A PROTEÇÃO CONTRA O VAZAMENTO DE DADOS E SUA IMPORTÂNCIA PARA AS EMPRESAS PRIVADAS. Revista Eletrônica eF@ tec, v. 6, n. 1, p. 10-10, 2016.

BAREA, Emerson Rogério Alves, *et al*. **HonIoT: Arquitetura de Honeynet com Controle de Propagação de Malwares para Dispositivos de IoT**. In: Anais do II Workshop de Segurança Cibernética em Dispositivos Conectados. SBC, p. 23- 36,2019.

CARVALHO, Luciano G. **Segurança de Redes.** Rio de Janeiro: Ciência Moderna, 73p, 2005.

CERT.Br. **Cartilha de segurança para internet**. São Paulo: Comitê Gestor de Segurança do Brasil, 2012., v4. Disponível em: < http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 15/10/2018.

DA SILVA ALVES, Bruno; CHARÃO, Andrea S.; LIMA, João Vicente F. **Uma Experiência de Execução de Aplicação MPI em Containers com *Docker* Swarm**. In: Anais da XIX Escola Regional de Alto Desempenho da Região Sul. SBC, 2019.

HIDALGO, Alexandre Henrique Picão; PEREIRA, Júlio Cesar. **SEGURANÇA EM REDES: HONEYPOTS E HONEYNETS**. Disponível em:

<http://web.unipar.br/~seinpar/2015/_include/artigos/Alexandre_Henrique_Picão_Hidalgo.pdf>. Acesso em: 19 mar. 2018.

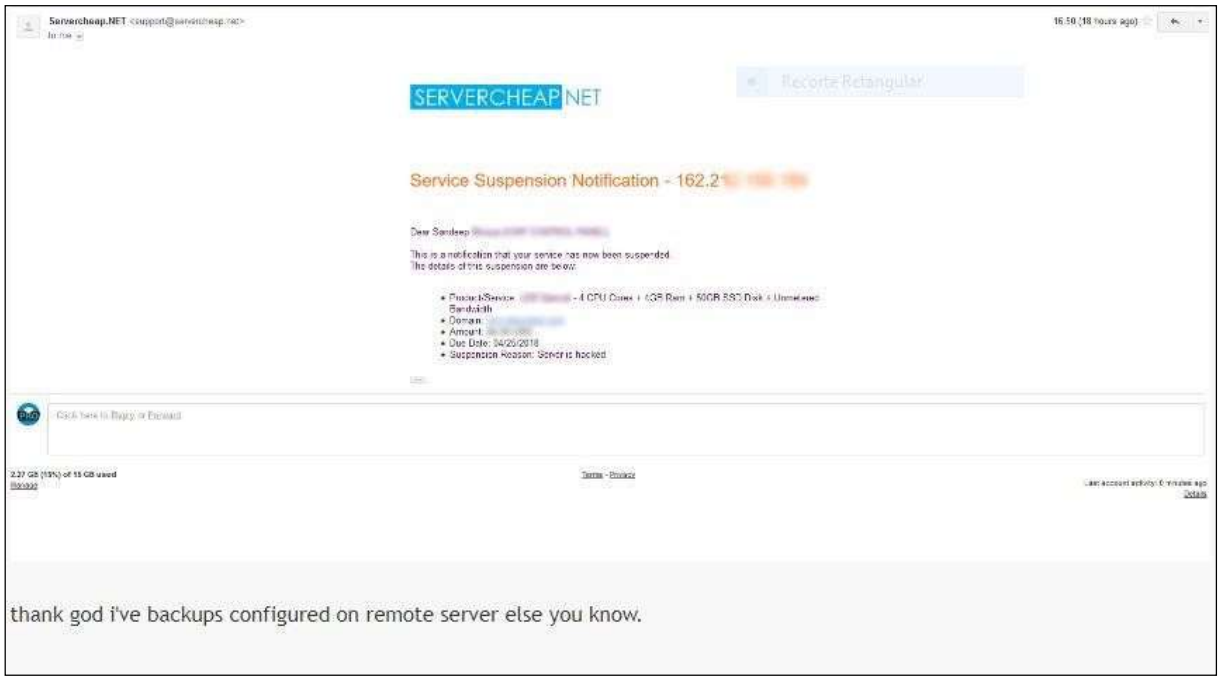
ANEXOS

ANEXO 1 – RELATO DE ATAQUES

Figura 33 - Relato de ataques na VestaCP

Fonte: Albertus *et al*. (2018)

Figura 34 - Relato de ataques na VestaCP



Fonte: Albertus *et al*. (2018)

Figura 35 - Relato de ataque na VestaCP

Re: Got 10 VestaCP servers exploited

Here is what we know so far:
1. The first wave happened on April 4. Servers were infected with /etc/cron.hourly/gcc.sh
2. It was an automated hack
3. CentOS, Debian, Ubuntu all distros are affected it's platform independent
4. We didn't find any traces in vesta and system logs yet
5. On April 7 infected servers started to DDoS remote hosts using /usr/lib/libudev.so.

What you can do:
The best way to stay safe is to temporary disable vesta web service

```
service vesta stop
```

```
systemctl disable vesta
```

or limit access to port 8083 using firewall

What we are doing:
Few users provided us with root access to their servers. We are investigating what happened. We also launched a couple honeypots in order to get full picture of the hack.

Fonte: Albertus *et al*. (2018)

Figura 36 - Relato de ataque na VestaCP

Re: Got 10 VestaCP servers exploited

Hi Everyone,

I also have one of my new server by ovh who is suspended.. I had a two factor auth for every ssh user.

I already stop vesta on my other servers. Maybe you should add a Two factor auth for vesta.

Thanks for your help :)

Fonte: Albertus *et al*. (2018)

Figura 37 - Relato de ataque na VestaCP

Re: Got 10 VestaCP servers exploited

skid wrote: ↑ Sun Apr 08, 2018 7:05 am

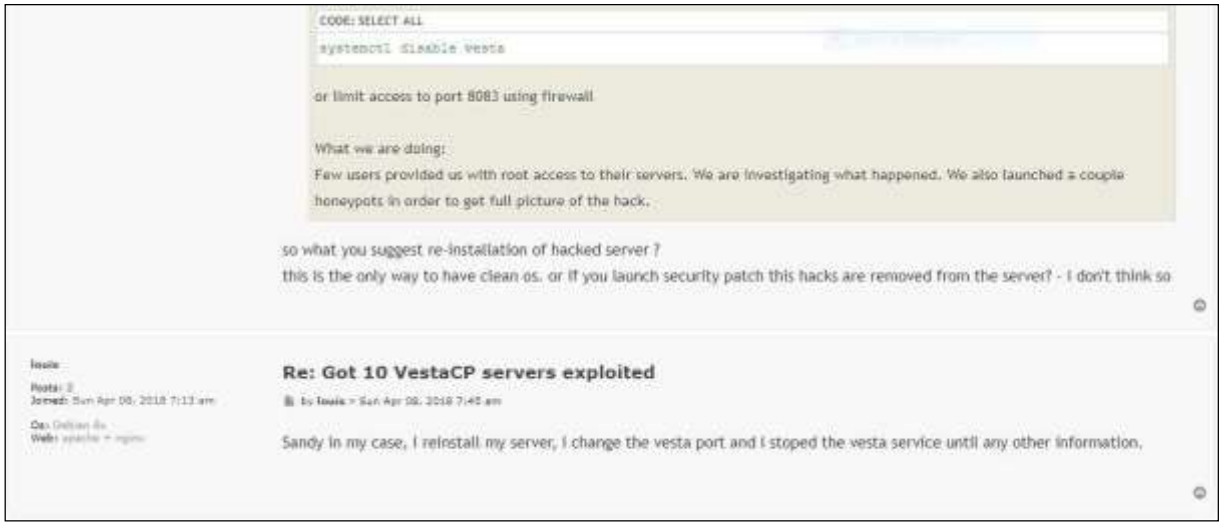
Here is what we know so far:
1. The first wave happened on April 4. Servers were infected with /etc/cron.hourly/gcc.sh
2. It was an automated hack
3. CentOS, Debian, Ubuntu all distros are affected it's platform independent
4. We didn't find any traces in vesta and system logs yet
5. On April 7 infected servers started to DDoS remote hosts using /usr/lib/libudev.so.

What you can do:
The best way to stay safe is to temporary disable vesta web service

```
service vesta stop
```

Fonte: Albertus *et al*. (2018)

Figura 38 - Relato de ataque na VestaCP



Fonte: Albertus *et al*. (2018)