CRIAÇÃO DE UM PROJETO DE SOC DE PEQUENO PORTE, VIABILIZANDO MELHORAS DE MONITORAMENTO E SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO.

CREATION OF A SMALL SOC DESIGN PORTE, ENABLING IMPROVEMENTS OF MONITORING AND INFORMATION SECURITY SOLUTIONS.

Fabio Lucio Lopes de Mendonça,
Renato José da Silva Camões,
João Paulo Pimentel

RESUMO

Um SOC - Security Operations Center em português Centro de Operações de Segurança, é um termo genérico que descreve parte ou a totalidade de uma plataforma cujo objetivo é prestar serviços de detecção e reação a incidentes de segurança, hoje em dia um SOC tem uma enorme importância nas empresas de médio e grande porte, pois controla os acessos e vulnerabilidades da empresa. Entretanto empresas de pequeno porte não investia em tal tecnologia por ser uma tecnologia de “alto custo” não sendo um fator essencial para empresa.

Palavras-Chave: SOC, Segurança da Informação, Sistema Distribuídos e Redes de Computadores.

ABSTRACT

Decentralization and increased access to systems allowed new studies about A Security Operations Center (SOC) is a generic term that describes part or all of a platform aimed at providing security incident detection and response services. medium and large, because it controls the access and vulnerabilities of the company. However, small-scale companies do not have innovation in high technology because they are a “high cost” technology and are not an environmental factor for the company.

Keywords: *SOC, Information Security, Distributed System and Computer Networking.*

INTRODUÇÃO

Um centro de operações de segurança, do inglês security operation center (SOC), é um centralizador dos serviços voltados à segurança da informação, desde da parte de manual de conduta até processos e projetos adotados por empresas de variados portes. O SOC é processo de segurança associado a um serviço necessário para organizações que desejam lidar com conformidade e gerenciamento de ameaças, pois seu principal objetivo é garantir a segurança dos dados (PIERR, 2013).

No SOC é pensado para melhorar a gestão de segurança de uma empresa ou organização, abrigado uma equipe de analistas cuja responsabilidade é de identificar, investigar, priorizar, escalar e solucionar problemas de segurança de dados. Como o uso da internet, novas tecnologias e softwares estão cada vez mais dinâmicos e avançados, a preocupação com a segurança da informação e dos dados também evoluiu nos últimos 10 anos. Por este motivo, a importância do SOC vem crescendo a medida que o uso de novas tecnologias aumenta (MILOSLAVSKAYA, 2016)

Dessa forma, este artigo propõe um modelo de melhores práticas para a criação de um projeto de SOC de pequeno porte viabilizando melhores monitoramentos e soluções para problemas encontrados no decorrer do projeto. Entretanto, será necessário a configuração e monitoramento de todos os componentes da topologia proposta para de forma a garantir a integridade e segurança.

Para isso, será necessário avaliar questões sobre velocidade de resposta, recuperação de dados e informações de monitoramento preciso, além de garantir melhores análises otimizando as ações para tomadas de decisões de gestores.

Os resultados deste projeto permitirão aumentar os níveis de proteção de segurança e apresentar procedimentos, o que pode reduzir a probabilidade de eventos indesejados e métodos de diminuir suas consequências. O projeto visa desenvolver uma plataforma abrangente de monitoramento de segurança cibernética, que será o software e a solução organizacional (modelos de gerenciamento e procedimentos organizacionais). A parte do software da

plataforma constituirá vários módulos especializados em vários tipos de avaliação do nível de segurança. O artigo enfoca o módulo integrado de um SOC para empresas de pequeno porte.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação parte do princípio que um sistema é aquele no qual os componentes localizados em computadores interligados em rede se comunicam e coordenam suas ações apenas passando mensagens, porém seguindo os princípios de integridade, disponibilidade, confidencialidade e acessibilidade, entretanto, o uso cada vez mais disseminado de sistemas informatizados integrados por meio de redes é um fato determinante da Sociedade da Informação. Este universo de conteúdos e continentes digitais está sujeito a várias ameaças que comprometem seriamente a segurança do complexo usuário-sistema-informação (MARCIANO,2006).

A tecnologia da informação é capaz de apresentar parte da solução a este problema, mas não é capaz de resolvê-lo integralmente. As políticas de segurança da informação devem contemplar o adequado equilíbrio dos aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos de políticas atuais, extremamente voltados às questões tecnológicas.

Dessa forma este trabalho tem por finalidade propor medidas de segurança para empresas de pequeno porte com a utilização de um SOC de baixo custo, utilizando técnicas e ferramentas open source, propondo um modelo de arquitetura para tal cenário.

Este trabalho teve por finalidade a análise dos pressupostos necessários para o tratamento da segurança da informação, por meio da formulação de políticas de segurança da informação, baseando-se em uma estratégia de análise fenomenológica. Tal abordagem visa a dar às políticas formuladas uma abordagem social, de caráter humanista, centrada nos pontos de vista do usuário e que se contraponha aos modelos tecnicistas atuais.

Além dessas, existem muitas definições de seguranaça da informação, que deve contemplar não só os aspectos técnicos como também os sociais,

relacionados ao ambiente organizacional e às pessoas.

Historicamente, a segurança da informação começou na área técnica do processamento de dados, por isso, os aspectos sociais da organização e as pessoas foram deixados de lado. Um outro fato importante, que deve ser considerado, é que mesmo os aspectos técnicos têm uma conotação mais ampla (PIERRE,2013). Além disso, embora violações da segurança e danos aos sistemas de informação ainda se originem dentro da organização, as violações externas estão aumentando, pois as empresas que se dedicam ao comércio eletrônico estão abertas a estranhos que chegam pela Internet. É difícil para as organizações determinar quão abertas ou fechadas elas devem ser para se protegerem. Um sistema que requeira muitas senhas, autorizações ou níveis de segurança para acessar uma informação acabará caindo em desuso. Controles eficientes e que não criem obstáculos para indivíduos autorizados utilizarem o sistema são difíceis de planejar (FONTES,2015).

Torna-se importante ressaltar que todas as definições sobre segurança da informação tem aspectos importantes. Um dos aspectos é que os computadores são protagonistas desse sistema. Outro fator é que os computadores necessitam estar interligados em rede para uma comunicação. Por fim, outro fator essencial é a comunicação e a colaboração realizada entre os componentes e usuários do sistema.

Um dos principais desafios da segurança de rede é que as caixas intermediárias de segurança, como firewalls e IDSs (Intrusion Detection Systems), têm apenas uma visão local da rede. Isso diminui a eficiência da detecção de segurança e dificulta a localização das fontes das ameaças. Há uma demanda crescente por operações e dispositivos de segurança que estão cientes da distribuição e do comportamento dos fluxos em toda a rede(THIAGO,2017). A capacidade de controle logicamente centralizado da Rede Definida por Software (SDN) permite que o controlador de rede adquira a visão global da rede. Neste caso o SOC pode tratar informações baseadas em SDN.

MODELO DE ARQUITETURA

A arquitetura proposta na Figura 1 conta com um *firewall Iptables* configurado de modo a não permitir que as máquinas que estão disponibilizadas na DMZ tenha qualquer tipo de comunicação com a rede intranet, para isso o primeiro item do trabalho o firewall contou com apenas 4 regras, outras regras foram implementadas no decorrer do projeto para impossibilitar alguns ataques previamente escolhidos.

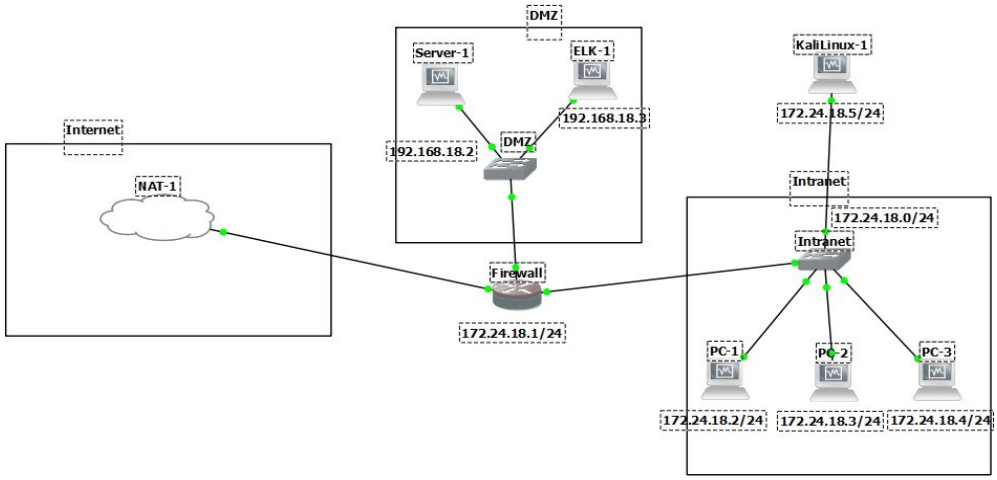

Figura 1- Arquitetura proposta para o SOC de pequeno porte

Essa arquitetura foi subdividida em três módulos:

- O primeiro bloco será o bloco de internet, que é constituído apenas de um ponto de acesso a rede externa na forma de NAT.
- Em uma Demilitarized Zone(Zona Desmilitarizada em português) - DMZ, foi instalado um switch com o IP de número 192.168.18.0.
- Um servidor de DNS com o IP 192.168.18.2.
- Um servidor com o ELK disponível no IP 192.168.18.3, esse bloco da arquitetura tem a faixa de IP 192.168.18.X, onde X pode ser variado de acordo com o a inclusão de novos dispositivos.
- Por fim, a intranet foi configurada com um switch de IP 172.24.18.0 e três computa- dores com o sistema operacional Ubuntu instalado, onde o IP variou de 172.24.18.2 a 172.24.18.4.

As configurações iniciais inseridas no firewall foram as seguintes:

```
1  iptables -P FORWARD DROP
2
3  #Forward section
4#Chain DMZ to LAN
5  iptables -A FORWARD -i enp0s9 -o enp0s8 -m state --state NEW
      ,ESTABLISHED, RELATED -j ACCEPT
6  iptables -A FORWARD -i enp0s8 -o enp0s9 -m state --state ESTABLISHED,
   RELATED
      -j ACCEPT
8#CHain DMZ to WAN
10  iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state NEW
      ,ESTABLISHED, RELATED -j ACCEPT
11  iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state NEW
      ,ESTABLISHED, RELATED -j ACCEPT
13   #Nat SECTION
15   iptables -A POSTROUTING -o enp0s3 -j MASQUERADE
```

O uso do servidor DNS (Domain Name Server) foi utilizado para facilitar as operações entre as máquinas, onde teve o domínio configurado como trabalho final, e cada máquina teve um subdomínio diferente a partir disso. Na Tabela 1 tem a associação de cada nome a seus respectivos IPs.

Tabela 1- Domínios cadastrados no servidor DNS

Domínio	IP
pc-1	172.24.18.2
pc-2	172.24.18.3
pc-3	172.24.18.4
fw	172.24.18.1
elk	192.168.18.3

O IPERF é uma ferramenta que reúne em uma única aplicação o relatório da análise de várias métricas, como a capacidade máxima fim-a-fim a nível de transporte, o jitter e a perda de pacotes. A sua utilização simplifica a análise de problemas de rede por parte dos administradores de redes. Desse modo, essa foi uma das motivações de sua escolha como ferramenta para análise nesse documento (DINIZ,2014).

Para realizar atender a tarefa número 2 foi instalado o software IPERF nas máquinas com o IP 192.168.18.3 e 172.24.18.5, onde a primeira máquina teve o comportamento de servidor e a segunda atuou como o cliente que envia o tráfego, foram simulados tráfegos TCP, UDP e FTP. Na Figura 2 temos o funcionamento da ferramenta de simulação de tráfego onde temos o output do tráfego visualizado a partir da ferramenta *Wireshark*.

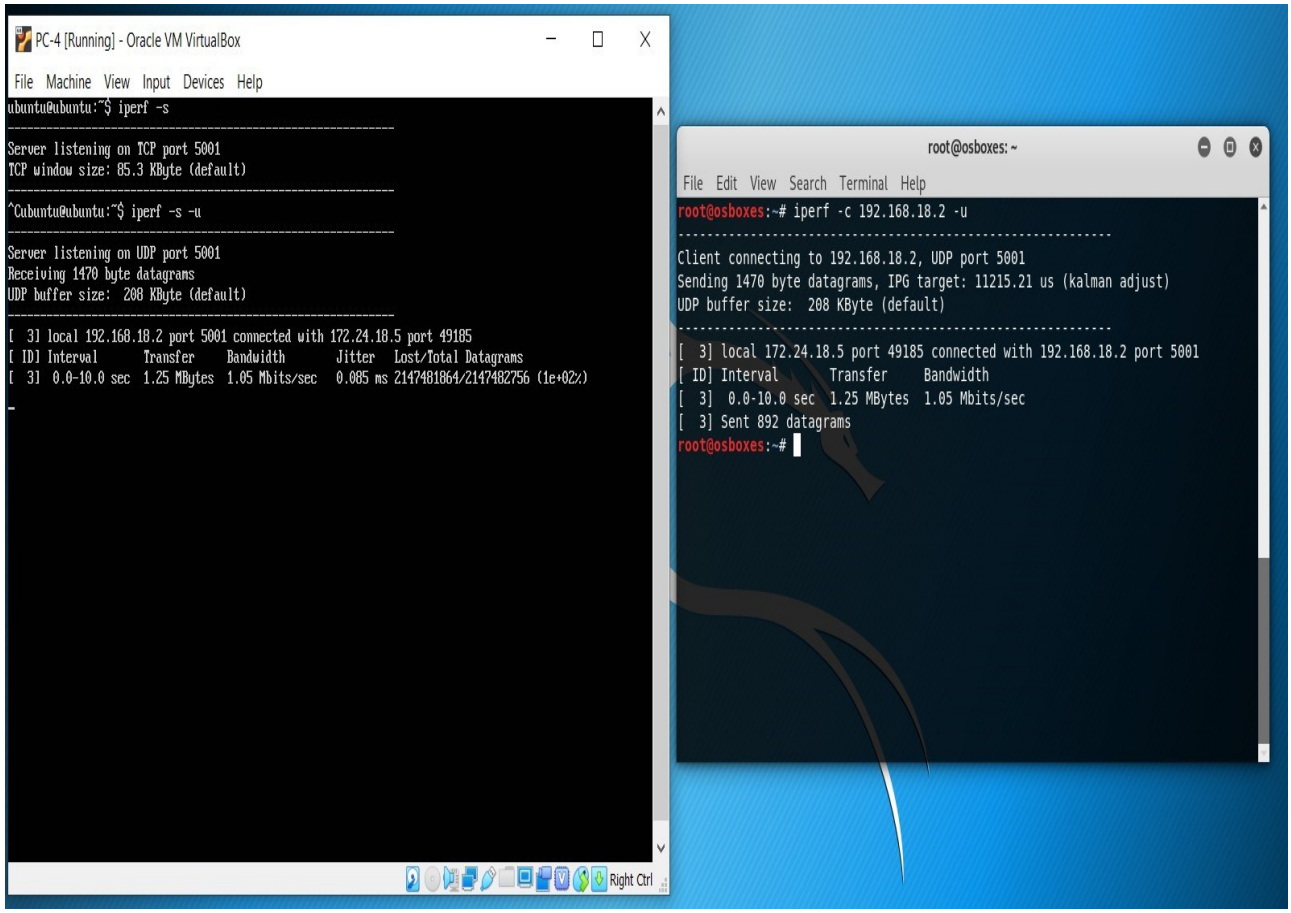

Figura 2- Simulação de tráfego UDP com IPERF

A pilha *elasticsearch*, *kibana* e *logstash* foi instalada na máquina de IP 192.168.18.3 na região da DMZ. Para isso, foi necessário mudar a porta do *kibana* que originalmente é a 5601 para a 443, conforme consta nas especificações desse trabalho. Para um perfeito funcionamento na coleta do log dos pacotes, foi necessário instalar um outro módulo nessa aplicação, chamado de *packetbeat*, esse é um sniffer que realiza a captura do tráfego gerado em uma rede, onde é possível realizar um filtro de quais protocolos irão ser monitorados, na Figura 3 temos a

arquitetura de coleta de pacotes utilizada nesse trabalho.

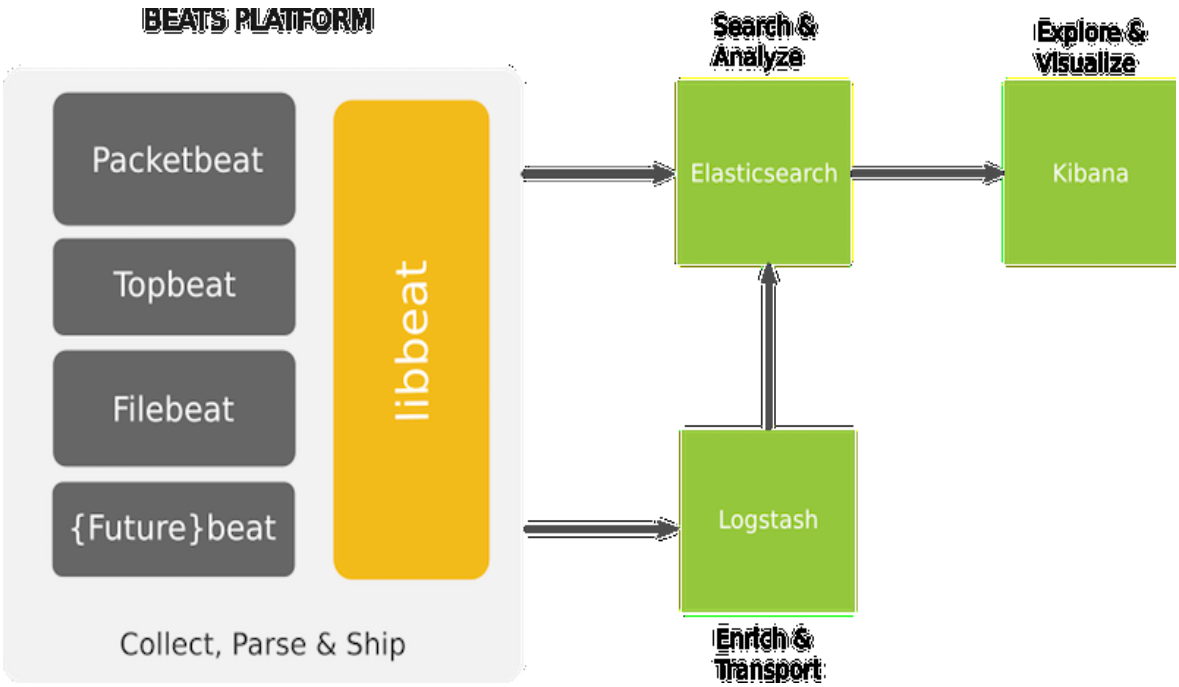

Figura 3 – Modelo de Arquitetura de coleta de pacotes e sua visualização e indexação

Para uma melhor visualização foi desenvolvido um módulo com interface gráfica desenvolvido em Python com o auxílio do biblioteca *Dialog*, onde o administrador de rede tem a possibilidade de realizar o *ping* para os dispositivos da rede, cuja é responsável pela a administração, na Figura 4.

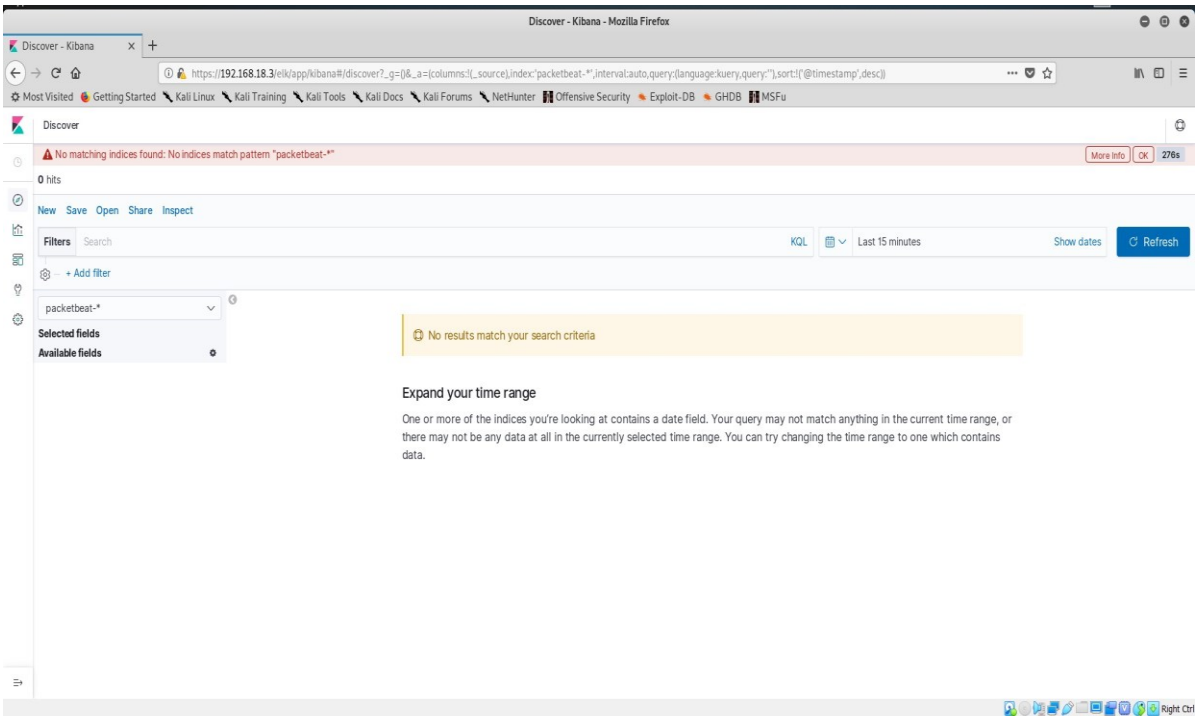

Figura 4 - Funcionamento do Kibana via browser

Foi também desenvolvido um módulo com interface gráfica desenvolvido em Python com o auxílio do biblioteca *Dialog*, onde o administrador de rede tem a possibilidade de realizar o *ping* para os dispositivos da rede, cuja é responsável pela a administração.

Como parte dos objetivos específicos, foram escolhidos 5 ataques para executá-los da intranet para a topologia do projeto. O primeiro ataque escolhido foi o *Synflood*, também conhecido como ataque SYN (sincronizado), que consiste numa forma de ataque de negação de serviço, do inglês Denial of Service (DOS) . Nele um nó de ataque envia uma série de requisições SYN via TCP com endereços alvo, a fim de sobrecarregar diretamente a camada de transporte e indiretamente a camada de aplicação do modelo OSI (AROTE,2015. Um ataque de *Syn Flood* é feito com os ips forjados (spoof), para que o atacante não receba os ACKs de suas falsas solicitações(DINIZ,2014). Para apresentação do funcionamento do script desenvolvido em *Python* e para simular o envio das requisições SYN para o servidor DNS da nossa topologia. É possível visualizar o tráfego gerado a partir desse ataque.

Para impedir esse ataque foi necessário incluir uma nova regra no firewall da

topologia, essa regra irá bloquear pacotes incompletos. A seguinte linha foi adicionada ao IPTABLES: iptables − AFORWARD − ptcp − mlimit − −limit1/s – jACCEPTllx

O segundo ataque escolhido foi o PortScan, que consiste em enviar uma mensagem para uma porta de destino específica e esperar por uma resposta dela. O dado que for recebido, então, vai indicar ao atacante se aquela porta está disponível ou não, o que vai ajudá-lo a encontrar a melhor maneira de invadir um servidor [6]. Esse é considerado um ataque inicial, onde o atacante irá explorar vulnerabilidades na topologia implementada, vale ressaltar que esse tipo de ação é considerada crime no Brasil. Nesse caso temos quais portas estão abertas no servidor DNS.Para evitar esse tipo de varredura nas portas, foi adicionada a seguinte linha no firewall, através do comando:

- iptables−AFORWARD−ptcp−−tcp−flagsSY N, ACK, FIN, RST−mlimit−−limit1/s− jACCEPT

Já o terceiro ataque escolhido foi o Ping da Morte, do inglês Ping of Death, que é um ataque que envolve o envio de um grande pacote de ping para uma máquina destino. O seu ataque é feito a partir de solicitações ping com um tamanho de pacote muito elevado e numa frequência também alta (milhares de vezes por segundo). Ele é considerado como um ataque de estouro de buffer, no qual o emissor envia um ”ping” com uma grande sobrecarga no sistema destino. Um ping tem geralmente 64 bytes, enquanto que um ping da morte é tão grande quanto o máximo permitido, que é de 65.535 bytes.(GEETHA,2014). Para evitar esse tipo de ataque é necessário colocar um limite no número de requisições do tipo icmp, a seguinte linha foi adicionada ao firewall da topologia:

- iptables − AFORWARD − picmp − −icmp − typeecho − request − mlimit − −limit1/s − jACCEPT

O quarto ataque foi o ARP Spoofing, que é uma técnica de ataque em que um atacante envia mensagens ARP (Address Resolution Protocol) com o intuito de associar seu ende- reço MAC ao endereço IP de outro host, como por exemplo, o endereço IP do gateway padrão, fazendo com que todo o tráfego seja enviado para o endereço IP do atacante ao nvés do endereço IP do gateway. Isso permite ao

atacante que intercepte, modifique e até pare os quadros da rede trafegada (KAUSHIK,2010). Para realizar a proteção a ataques de spoofing foi desenvolvido o script abaixo.

O quinto e último ataque foi o ataque Smurf, também conhecido como Fraggle, que con- siste em ser um ataque distribuído de negação de serviço (DDoS) distribuído pela rede. Ele é parecido com ataque via inundações por ping, pelo fato de ambos serem realizados pelo envio de uma série de solicitação de pacotes ICMP (Internet Control Message Proto- col) Echo para o IP de origem falsificado da vítima usando um endereço IP de broadcast. Porém, este ataque é vetor de ataque de amplificação que aumenta seu potencial de dano, explorando as características das redes de transmissão (YIHUNIE,2018).

Através de um trabalho coordenado e interdependente entre os testes foram realizados em um ambiente controlado de forma que pode se obter os devidos resultados para implementação de um SOC em um empresa de pequeno porte onde as etapas de cada fase foram planejadas, discutidas, executadas e documentadas.

CONCLUSÃO

Com os avanços em tecnologia, tem sido possível perceber o papel relevante que um projeto de SOC são capazes de exercer. O principal aspecto dessa modalidade de ser- viço é o provimento de dados e informações para disponibilizá-los aos gestores da área de segurança da informação de maneira rápida e prática através do modelo proposto.

Neste trabalho foram apresentados a concepção, o desenvolvimento e a implantação de algumas aplicações que visam contribuir com a melhoria da segurança em uma organização de pequeno porte. Entretanto se aprofundar os desenvolvimento dos modelos os resultados dos mesmos podem ser implementado em diversas organizações.

Foi possível também perceber que a implantação dessas aplicações tanto no contexto deste trabalho quanto em demais trabalhos podem ser aproveitadas para diversas situações de implementação de segurança. Além de reunir os conceitos de redes de computadores, segurança da informação e programação distribuída.

REFERÊNCIAS

PIERRE Jacobs, Alapan Arnab, “Classification of security operation centers,” IEEE 2013 Information Security for South Africa, 2013.

MILOSLAVSKAYA, “Security operations centers for information security incident manage- ment,” IEEE 4th International Conference on Future Internet of Things and Cloud (Fi- Cloud), 2016.

MARCIANO, João Luiz Pereira. Segurança da informação: uma abordagem social. 2006.

FONTES, Edison Luiz Gonçalves; BALLONI, Antonio José; LAUDON, Kenneth C. A segurança de sistemas da informação: aspectos sociotécnicos. A SEGURANÇA DE SISTEMAS DA INFORMAÇÃO: ASPECTOS SOCIOTÉCNICOS...5, 2015.

DINIZ and N. A. Junior, “Ferramenta iperf: geração e medição de tráfego tcp e udp,” Notas Técnicas, vol. 4, no. 2, 2014.

THIAGO P.B.V., Danilo F. Tenórioa, “Model order selection and eigen similarity based framework for detection and identification of network attacks,” Journal of Network and Computer Applications, 2017.

GEETHA, “Syn flooding attack — identification and analysis,” IEEE International Conference on Information Communication and Embedded Systems, 2014.

KAUSHIK, E. S. Pilli, “Network forensic system for port scanning attack,” IEEE 2nd International Advance Computing Conference (IACC), 2010.

YIHUNIE, E. Abdelfattah, “Analysis of ping of death dos and ddos attacks,” IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018.

AROTE, “Detection and prevention against arp poisoning attack using modi- fied icmp and voting,” IEEE International Conference on Computational Intelligence and Networks, 2015.