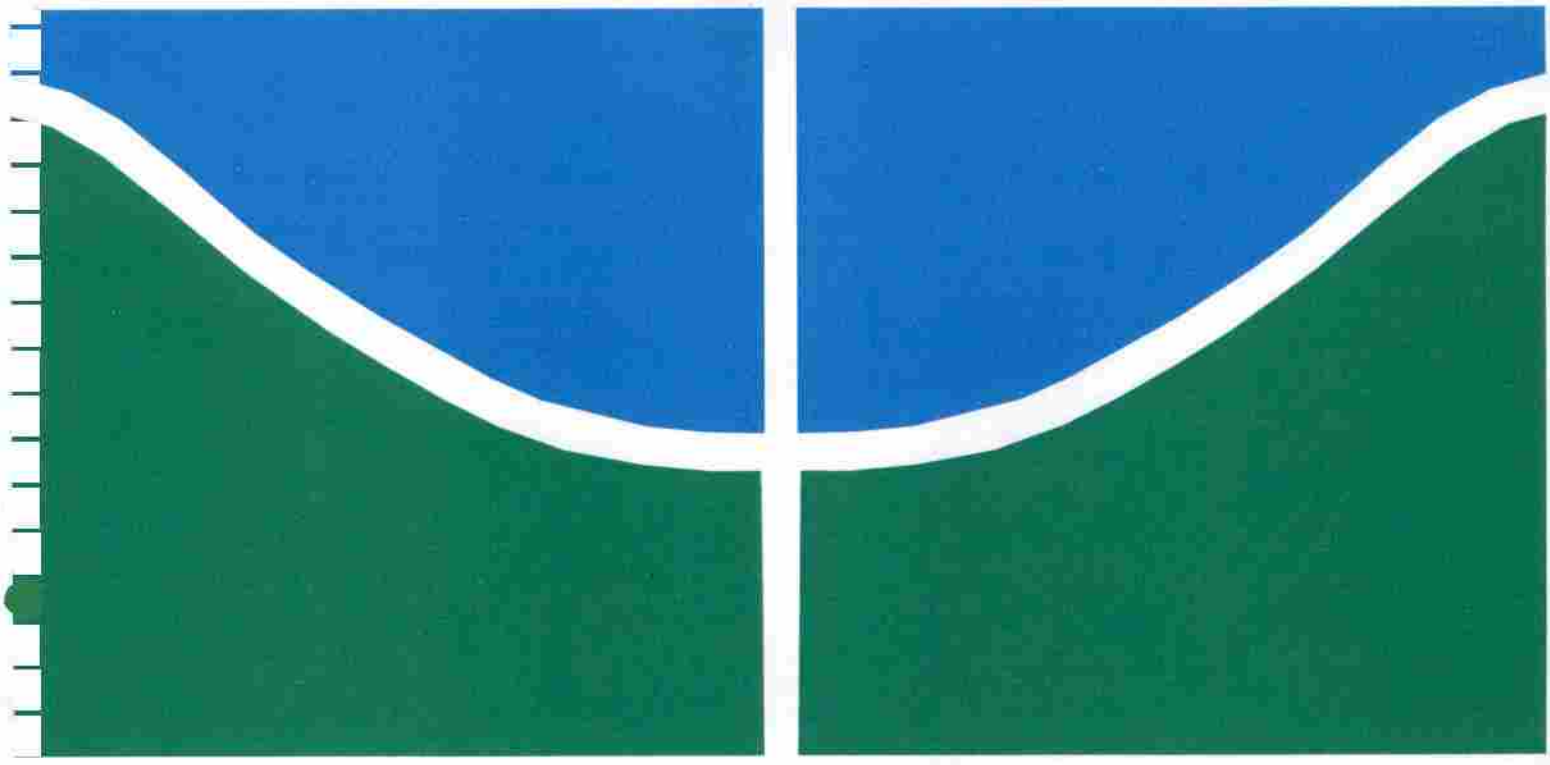


UTILIZAÇÃO DO SIEM PARA DETECÇÃO DE CIBERATAQUE

JOÃO VICTOR DE ANDRADE VERDE

TRABALHO DE CONCLUSÃO DE CURSO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UTILIZAÇÃO DO SIEM PARA DETECÇÃO DE CIBERATAQUE

JOÃO VICTOR DE ANDRADE VERDE

ORIENTADOR: PROFESSORA DRA. EDNA DIAS CANEDO
CO-ORIENTADOR: PROFESSOR MSC. ALCYON FERREIRA DE SOUZA JUNIOR

TRABALHO DE CONCLUSÃO DE CURSO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO: PPGENE.TCC – 034 /2017

BRASÍLIA, DF: 30 DE AGOSTO / 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UTILIZAÇÃO DO SIEM PARA DETECÇÃO DE CIBERATAQUE

JOÃO VICTOR DE ANDRADE VERDE

TRABALHO DE CONCLUSÃO DE CURSO DE PÓS-GRADUAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO TITULO DE PÓS-GRADUADO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

EDNA DIAS CANEDO, FGA (UNB) (ORIENTADORA)

_____

RAFAEL TIMÓTEO DE SOUSA JÚNIOR ENE (UNB) (MEMBRO INTERNO)

_____

ELIANE CARNEIRO SOARES SEEDF (GDF) (MEMBRO EXTERNO)

BRASÍLIA, DF, 30 DE AGOSTO DE 2017.

FICHA CATALOGRÁFICA

Verde, João Victor de Andrade Verde.

Utilização do SIEM para detecção de ciberataque [Distrito Federal], 2017.

Trabalho de Conclusão de Curso de Pós-Graduação – Universidade de Brasília, Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. Detecção de Ciberataque
2. SIEM
3. Visibilidade da Rede
4. Classificação de nível de ataque

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Verde, João Victor de Andrade. (2017). Utilização do SIEM para detecção de ciberataque. Trabalho de conclusão de curso de pós-graduação, Publicação UnBLabRedes.MFE.034/2017, Lab Redes, Universidade de Brasília, Brasília, DF, 33p.

CESSÃO DE DIREITOS

AUTOR: João Victor de Andrade Verde

TITULO DO TCC: Utilização do SIEM para detecção de ciberataque.

GRAU / ANO: Pós-graduado / 2017

João Victor de Andrade Verde

João Victor de Andrade Verde
SGAN 914 – Módulo H – Bloco B Apartamento 142
Condomínio Monte Carlo – Asa Norte
CEP: 70790-148 - Brasília - DF
Tel. 55 – 61 – 981022250 / jvictorverde@gmail.com

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus pela minha saúde e por me iluminar nessa caminhada sem ele nada disso seria possível, aos meus pais pelo apoio de sempre e principalmente o incentivo e amor incondicional, ao meu irmão pela motivação e parceria.

A esta universidade pela oportunidade de fazer o curso e toda equipe do LabRedes, pela dedicação e empenho.

A minha orientadora professora Edna Dias, pelo suporte, correções e incentivos.

Ao co-orientador professor Alcyon Júnior pelo os ensinamentos passados.

A todos os professores do curso que foram fundamentais para os conhecimentos que obtive ao longo do curso.

Aos meus grandes amigos pela força e incentivo ao longo do curso e apoio na conclusão deste trabalho.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

UTILIZAÇÃO DO SIEM PARA DETECÇÃO DE CIBERATAQUE

Autor: João Victor de Andrade Verde
Orientador: Dra. Edna Canedo Dias
Co-Orientador: Msc. Alcyon Ferreira de Souza Júnior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 29 de Agosto de 2017.

Com o aumento significativo nos últimos anos de ciberataques, a preocupação com o ambiente de infraestrutura de TI corporativo ser afetado, tem aumentado as preocupações das equipes de segurança, para ter a visibilidade e o controle desses ataques, há necessidade de uma solução que proporciona essas caraceteristicas. O SIEM uma solução que realiza a gestão de eventos e informações de segurança, é propicio para esse cenário, o objetivo desse trabalho foi a utilização da aplicação em open-source do SIEM denomida de OSSIM, para detecção de ciberataque. Foram simulados ataques reais em um ambiente controlado a fim de realizar a detecção desses ataques pela aplicação, os ataques foram pertinentes de vulnerabilidades já conhecidas, através de falhas encontradas no ambiente controlado. Os resultados obtidos foram satisfatórios, tendo em vista que o OSSIM foi capaz de detectar esses ataques e alertar sobre os ataques ocorridos. Conclui-se que a solução SIEM é de suma importância para o apoio na gestão de vulnerabilidades, eventos e entre outras caracteristicas e funcionalidades que o SIEM pode proporcionar para as equipes de segurança e tomada de decisão para os gestores. Entre diversas opções de vendor's no mercado para o SIEM, o OSSIM por ser open-source foi a aplicação modelo para ser estudada e implementada ao longo deste trabalho a fim de verificar a detecção de ciberataque e se comportou com uma ótima opção para ser implementado um SIEM em ambientes corporativos de pequenos e médio porte.

ABSTRACT

USE OF SIEM FOR CYBER-ATTACK DETECTION
Author: João Victor de Andrade Verde
Supervisor: Dra. Edna Canedo Dias
Co-Supervisor: Msc. Alcyon Ferreira de Souza Júnior
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 29 August 2017

With the significant increase in recent years of cyber-attacks, concern for the corporate IT infrastructure environment has been affected, security concerns have increased, visibility and control of these attacks is needed, a solution is needed that provides these Characteristics. SIEM a solution that manages events and security information, is suitable for this scenario, the objective of this work was the use of the open-source SIEM application called OSSIM, for detection of cyberattack. Real-time attacks were simulated in a controlled environment in order to detect these attacks by the application, the attacks were pertinent to known vulnerabilities, through flaws found in the controlled environment. The results obtained were satisfactory, considering that OSSIM was able to detect these attacks and to alert about the attacks that occurred. It is concluded that the SIEM solution is of paramount importance for the support in the management of vulnerabilities, events and among other characteristics and functionalities that the SIEM can provide for the security teams and decision making for the managers. Among several vendor's options on the market for SIEM, the OSSIM for being open-source was the model application to be studied and implemented throughout this work in order to verify the detection of cyberattack and behaved with a great option to be implemented a SIEM in small and medium-sized corporate environments.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

DDoS	*Distribuited Denial of Service*
RNP	*Rede Nacional de Ensino e Pesquisa*
CAIS	*Centro de Atendimento e Incidentes de Segurança*
CERT.BR	*Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*
SIEM	*Security Information and Event Management*
OSSIM	*Open Source Security Information Management*
HIDS	*Host-based Intrusion Detection System*
NIDS	*Network Intrusion Detection System*
OSSEC	*Open Source Security*
CALM	*Compromise and Attack Level Monitor*
DoS	*Deny of Service*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
SIM	*Security Information Management*
SEM	*Security Event Manager*
IBM	*International Business Machines*
SSH	*Secure Shell*
FTP	*File Transfer Protocol*
HTTP	*Hypertext Transfer Protocol*
IP	*Internet Protocol*
SLA	Acordo de Nível de Serviço
TCP	*Trusted Computing Platform*
SOC	*Security Operations Center*
VM	*Máquina Virtual*

1 - INTRODUÇÃO

Nos últimos anos, as organizações vêm enfrentando grandes desafios e ameaças de segurança na rede. Os ataques mais populares são realizados através de mensagens eletrônicas como o spam, técnicas como *phishing* e *pharming* para roubo de dados, ataques de negação de serviço (DDoS), vírus, *worms* e diversos código maliciosos, estão se tornando mais comuns no dia-dia das organizações.

Ao longo dos anos, os ataques evoluíram de acordo que a tecnologia cresce para se tornarem baseados em conteúdo. As infecções mais comuns nas organizações vêm através de engenharia social ou ataques utilizando *exploit* de um dia-zero (vulnerabilidade nova encontrada).

As diversas técnicas utilizadas para realizar ataques estão sendo realizado de forma mais intrusiva na forma de realizar uma invasão explorando a falha de uma vulnerabilidade, os ataques contra os sistemas de informação cresceram em sofisticação e em complexidade, detecção e reação é uma atividade desafiadora para a equipe de segurança. Além disso, os dispositivos de sistema são projetados para suportar ambientes heterogêneos, com características diferentes e funcionalidades que aumentam a dificuldade desta tarefa. A definição de políticas de segurança para proteger esses sistemas é um grande desafio que requer uma grande experiência e conhecimento.

Dados do relatório elaborado de estatísticas sobre incidentes de segurança do Centro de Atendimento a Incidentes de Segurança da RNP (CAIS) juntamente com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) mostra que os ataques cibernéticos estão mais comuns e causando grandes impactos de reputação e financeiro para as organizações.

A dificuldade em acompanhar esse crescente aumento de ameaças maliciosas, muitas vezes é a inoperância de soluções como forma de mitigar tais riscos e ameaças para intervir esse tráfego malicioso. Normalmente, uma resposta ao incidente de forma efetiva é comprometida por falsos negativos e positivos por falta de correlacionamento de logs gerados por outras fontes da infraestrutura corporativa. Segundo Kawakani (2014) o surgimento de novas ameaças, torna-se novos desafios para a segurança da informação na tentativa de mitigar essas ameaças, tornando um processo com ciclo, onde é realizado a descoberta de uma nova ameaça (*zero-day*), estudadas e desenvolvido uma solução para

prevenção da aquela ameaça vista como um processo cíclico, o qual começa com a descoberta de novas ameaças.

Uma proposta para solução em gerenciar e mitigar os riscos que essas ameaças trazem as organizações é a implementação de um SIEM Gerenciamento de Eventos e Informações de segurança), atuando a nível de incidentes proativo a às ameaças.

Neste trabalho, é proposto a realização de um estudo descritivo da utilização do OSSIM para promover a detecção de anomalias na rede. O objetivo é realizar um levantamento de quais técnicas são mais utilizadas e ataques de maneira de analisar o comportamento no OSSIM, abrindo um leque de opções para mais estudos inovadores com foco no SIEM.

Entretanto sabe-se que mesmo um sistema de gerenciamento de eventos e informações de segurança (SIEM) configurado corretamente e gerenciado em conformidade de acordo com as boas práticas, a rede não está segura na sua totalidade, tendo em vista que com o surgimento de novas vulnerabilidades, qualquer ameaça externa pode tornar um risco, comprometendo a infraestrutura a depender do objetivo final.

Implantar um SIEM em um ambiente corporativo necessita mais do que tecnologia para que a mesma funcione. É necessário considerar aspectos como política de segurança, gestão de risco e o planejamento do catálogo de serviços.

Para mitigar os efeitos de um determinado ataque, há necessidade de implementar medidas de segurança e contramedidas.

Contramedidas são ações de segurança necessárias para se opor a um ataque, seja eliminando ou prevenindo, minimizando o dano que pode causar, ou descobrindo e relatando de modo que a ação corretiva pode ser tomada. Uma contramedida combinada, resulta da implementação simultânea de duas ou mais contramedidas para mitigar um determinado ataque essa contramedida é analisada como uma solução única com um custo combinado e uma eficiência combinada.

1.1 - MOTIVAÇÃO

A preocupação com a segurança da informação nas redes corporativas está promovendo cada vez mais investimentos em tecnologias e pessoas, na tentativa de mitigar os possíveis riscos que ameaças podem comprometer uma organização se um dado sensível for comprometido. Diante desse fato há necessidade de que aplicações e elementos de

seguranças que participam do processo seja sempre revisados e atualizados de acordo com as boas práticas para acompanhar a rápida evolução e crescente das ameaças.

Com essa crescente evolução das ameaças pode ocasionar um problema crítico para a rede corporativa. Hoje estamos vivenciando o que é chamado de guerra cibernética, onde ataques de diversas formas e origens estão acontecendo a todo momento pelo mundo, sendo assim existe uma dificuldade para controlar e avaliar esses ataques se direcionados para a rede corporativa. Em busca de mitigar essas ameaças e controlar os riscos há diversas ferramentas que buscam uma prevenção preventiva e ativa na gestão de rede e que têm sido com uma das soluções paliativas na tentativa de mitigar os problemas que surgem ao decorrer do tempo.

1.2 - OBJETIVOS DO TRABALHO

A tecnologia SIEM (Sistema de Gerenciamento de Eventos e Informações de Segurança) utilizada no decorrer do trabalho é em open source, desenvolvido pela empresa Alien Vault que se denomina o OSSIM (Gerenciamento de Informações de Segurança de Código Aberto). O OSSIM é uma aplicação que gerencia informações, correlacionando eventos de diversas fontes que auxiliam para um resultado melhor. A aplicação vem por padrão o que se chama plug-ins que são diversas ferramentas que dentre elas podemos citar um IDS na tratativa de realizar detecção de intrusões e tem a visibilidade de toda a rede o que pode gerar milhões de eventos e pode-se gerar falsos positivos, o que pode dificultar na análise dos resultados finais eficiente:

a. Estudar como funciona a aplicação, seus sensores e plug-ins (OSSIM);
b. Análise das regras da aplicação de forma que os alarmes de falsos negativos, possam ser reduzidos;
c. Simular ataques reais em um ambiente controlado para verificar os eventos gerados na aplicação e na detecção dos ataques realizados;

Assim, o principal objetivo deste trabalho, é analisar o comportamento do OSSIM na tratativa de detecção de ciberataques.

1.3 - METODOLOGIA DE PESQUISA

A metodologia de pesquisa proposta foi dividida em fases, 1, 2 e 3, para facilitar o entendimento do trabalho, conforme apresentado a seguir. A divisão em fases busca aprofundar o estudo relacionado ao tema e problema proposto neste trabalho.

Fase 1: Realizar pesquisa bibliográfica sobre a solução SIEM, o qual é fundamental essa análise para realizar um embasamento por parte da leitura em artigos, teses que são relevantes para o desenvolvimento do trabalho.

Fase 2: Obter informações sobre os ataques mais comuns na rede, bem como a construção e proposta de um SIEM na detecção de ataques.

Fase 3: Simular ataques reais em um ambiente controlado para uma análise do OSSIM na capacidade de detectar ataques, analisando os resultados. Nesta fase serão efetuadas as conclusões e identificação das contribuições.

1.4 - CONTRIBUIÇÕES DO TRABALHO

Buscam-se com este trabalho as seguintes contribuições:

- Apresentação de uma aplicação eficaz na detecção de ataques cibernéticos.
- Visibilidade da rede.
- Simulação do modelo proposto, aplicando à solução proposta em um cenário de ambiente controlado, simulando ataques em hosts com diversas vulnerabilidades e utilizando a aplicação no auxílio da monitoração e detecção desses ataques.

1.5 - ORGANIZAÇÃO DO TRABALHO

Para um melhor entendimento deste trabalho, a sua organização é descrita a seguir.

O Capítulo 2 oferece uma revisão dos principais conceitos abordados, incluindo principalmente o conceito de SIEM e os ataques cibernéticos populares. É apresentado os trabalhos relacionados.

No Capítulo 3 o modelo proposto é apresentado a topologia de rede utilizado na simulação em um ambiente controlado e os resultados coletados para análise da aplicação OSSIM.

2 – ESTADO DA ARTE E REVISÃO BIBLIOGRÁFICA

Este capítulo tem como foco a revisão dos principais conceitos de SIEM, a aplicação *open-source* OSSIM, tipos de ataques cibernéticos populares. Com o objetivo de abranger o tema em um cenário amplo e ao mesmo tempo, ser possível a separação dos conceitos, assuntos correlatos e de assuntos similares, foi realizado uma divisão dos assuntos em tópicos específicos. Na seção 2.1 é abordado o tema de SIEM e a aplicação em *open-source* OSSIM. Na seção 2.2 a arquitetura do OSSIM. Na seção 2.3 é abordado os conceitos relacionados a tipos de ataques cibernéticos.

2.1 - SIEM

Gerenciamento de Eventos e Informações de Segurança (*Security Information and Event Management* - SIEM). É uma aplicação para gerenciamento de eventos de segurança, centralizando logs de diversas soluções de segurança como firewall, ids, ips, antivírus entre outros. Segundo Miller (2011) projetado para dar visibilidade de toda a infraestrutura de TI da corporação de forma clara para a equipe de segurança. A aplicação deve ser capaz de correlacionar eventos coletados de outras soluções existente na infraestrutura para realizar detecção de ataques e vulnerabilidade e facilitar o gerenciamento de incidentes e geração de relatórios.

Uma solução SIEM permite que soluções de segurança como (firewalls, proxies, sistemas de prevenção a intrusão (IPS) e antivírus) sejam detectados, coletados, armazenados e correlacionados; o que possibilita uma rápida identificação e resposta aos incidentes.

A arquitetura de um SIEM conforme a figura 2.1 normalmente é composta por detectores, coletores, o SIEM propriamente dito e o *front-end* para gerenciamento, onde os eventos gerados por diversos sistemas são recolhidos, normalizados e correlacionados.

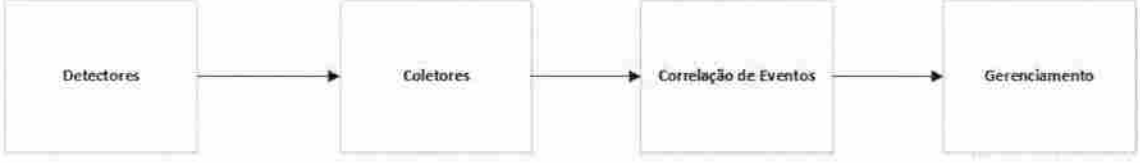


Figura 2.1 – Funcionamento básico do SIEM (o autor, 2017)

Detectores: Qualquer sistema que gera algum evento poderá ser considerado um detector.

Coletores: Agrupa as informações dos detectores, realiza a interpretação dos dados e classifica e envia para o SIEM. A coleta dos eventos de cada detector pode ocorrer através dos métodos *Push* e *Pull*. No primeiro, os eventos são enviados em formato nativo e no segundo um agente é instalado no dispositivo detector.

Correlação de Eventos: Após receber os dados tratados pelos coletores, o SIEM atribui um grau de risco numa escala de 0 a 5 para cada evento, realizando a correlação com o objetivo de detectar ataques e novos padrões e na tentativa de reduzir o número de falsos positivos e negativos.

Gerenciamento: Recebendo as informações, elas são armazenadas no banco de dados onde é possível consultar os eventos e alarmes gerados, onde será permitido a geração de relatórios, gerenciamento de vulnerabilidades e chamados e a configuração do sistema, como por exemplo o ajuste de valoração dos ativos, as definições de grau de risco, ajustes de métricas de detecção e automatização de ações.

2.2 - OSSIM

O OSSIM (Gerenciamento de informações de segurança de código aberto) é baseado no sistema operacional Linux na distribuição Debian com diversas ferramentas integradas, todas *open-source*. Segundo Miller (2011) O principal objetivo do OSSIM é estabelecer uma estrutura totalmente centralizado que permite visualizar e analisar eventos relevantes que ocorrem em uma infraestrutura de TI. O gerenciamento do OSSIM para coletar dados e filtrar milhares de eventos que acontecem na rede corporativa em conjuntos com outras soluções existentes em produção na infraestrutura, permite seja uma aplicação extremamente útil para um gerenciamento centralizado. O OSSIM é integrado com plug-ins específicos de diversas soluções de segurança o que aumenta o desempenho e a escalabilidade com outros tipos de soluções. O funcionamento da arquitetura do OSSIM é realizado em processamento de multitarefas, como os agentes de coleta de dados que tem a tarefa de realizar a coleta dos logs de cada host que tem-se visibilidade e fazer o envio para o servidor de gerenciamento do OSSIM tornando-se um evento. O processo de coleta de logs envolve um processo de filtro por agente e informações que nessa etapa é realizado a classificação de uma informação do host monitorado que determina se os dados coletados vai ser gerado evento para o OSSIM.

Segundo Bowling (2010) ao final de uma implementação consistente é tornar a gestão de riscos um processo organizado e observável para uma tomada de decisão por partes dos gestores.

2.2.1 – Arquitetura do OSSIM

A arquitetura do OSSIM dividido por Miller (2011) tem cinco componentes: agente, sensores, servidor, banco de dados e a interface.

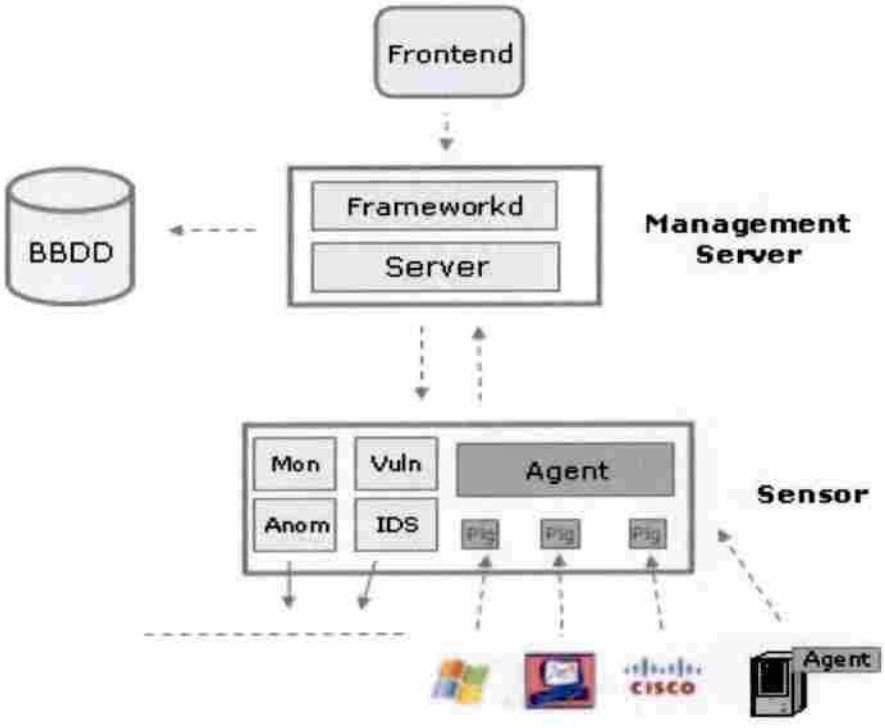


Figura 2.2: Modelo do OSSIM (Miller, 2011)

Agente: tem a função de realizar a coleta dos eventos de redes gerados nos *hosts* que ele está monitorando.

Sensores: reúnem as informações coletadas pelo agente, realizam a classificação e enviam para o tratamento do servidor.

Servidor: onde é feito todo o gerenciamento, realiza o tratamento das informações recebidas e a capacidade de fazer o correlacionamento, a avaliação de riscos, varreduras de vulnerabilidades e monitoramento de toda a rede.

Base de Dados: armazena as informações para análise e exploração dos dados.

Interface: Para acesso de todas as informações geradas como evento, gerenciamento de incidente, relatórios, detecção em tempo real, gerenciamento dos tickets, entre outras funcionalidades.

Segundo Gallardo (2014) desenvolvedores da Alienvault afirmam que para ter uma aplicação de qualidade teria de estar em conformidade com os princípios básicos da segurança da informação. Segundo a ISO 27002 define da seguinte forma:

Confidencialidade: informações restritas é acessível somente por um determinado grupo de usuários.

Integridade: dados alterados por uma pessoa não autorizada.

Autenticidade: garantir que a comunicação é autêntica, origem e destino confirmar que é realmente a identidade de quem está se comunicando do outro lado.

Disponibilidade: garantir que os recursos estejam sempre disponíveis para acesso por pessoas autorizadas.

2.2.2 – HIDS e NIDS na utilização do OSSIM

2.2.2.1 - NIDS – Detecção de Intrusão em rede

Um sistema de detecção de intrusão em rede, denominado como NIDS (*Network Intrusion Detection System*) é uma tecnologia utilizado para monitorar e analisar o tráfego de rede. A sua função é realizar um filtro de todos os pacotes de entrada na rede e procurar por algo suspeito que venha comprometer a rede corporativa.

Se alguma ameaça for descoberta, é realizado contramedidas baseado no nível da gravidade, que pode realizar um alerta de notificação para os analistas, bloquear o endereço IP de origem.

2.2.2.2 - Snort

O Snort é uma das aplicações integradas ao OSSIM, é o NIDS utilizado no OSSIM. É uma aplicação que realizar *sniffer* na rede e analisa os tráfegos na rede. Quando alguma atividade suspeita é identificada pelo Snort, é enviado um alerta para o *syslog* para ser tratado uma possível invasão.

2.2.2.3 - HIDS – Detecção de Intrusão no host.

O sistema de detecção de intrusão baseado em hosts HIDS (*Host Intrusion Detection System*) funciona de forma cliente/servidor e realiza o monitoramento no host especifico, através de um agente instalado que auxilia na detecção de uma intrusão ou alguma atividade suspeita de uso indevido do sistema, reportando a algum servidor responsável pelo agente instalado no host.

O agente monitora e analisa as atividades suspeitas seja interna ou externa que comprometeu a política de segurança do host

2.2.2.4 - Ossec

OSSEC (*Open Source Security*) é o HIDS que o OSSIM tem integração e plug-ins para o agente a ser instalado, como é denominado um HIDS é baseado no modelo cliente/servidor, onde cada agente do OSSEC é instalado no host que pretende-se monitorar e coletar os logs e envia as informações para o servidor central.

2.2.3 – Correlação no OSSIM

A Correlação é fundamental para um bom funcionamento do OSSIM, seu papel é realizar o tratamento e correlacionar eventos vindo de diversas fontes de dados (firewall, IPS, IDS, antivírus), uma das grandes vantagens de correlacionar eventos, é identificar uma causa raiz que causou instabilidade no ambiente e na identificação de novos ataques.

Existem três tipos de correlação segundo Karg (2003): correlação lógica, correlação de inventário e correlação cruzada.

Correlação lógica: utiliza como base, regras pré-definidas que realiza um processo de condição e de acordo que eventos já conhecidos for surgindo, essa condição é consultada para verificar a prioridade que o evento deve ser classificado antes de disparar um alarme e abrir um ticket.

Correlação de inventário: realiza a comparação de um host ativo/inativo com algum tipo de ameaça. Essa medida diminui alarmes de falsos positivos, já que um ataque está sendo realizado a um host que não está disponível, sendo assim, se o host não está disponível, não pode ser realizado ataques direcionados.

Correlação Cruzada: informações vindo do IDS e de outros sensores da rede, realiza o cruzamento dessas informações que descarta falsos positivos.

2.2.4 – Métodos de avaliação de riscos utilizados no OSSIM

A avaliação de riscos no OSSIM tem uma tarefa importante no processo de mensurar o risco e avaliar o grau de importância para tratativa do evento de acordo com o grau determinado que vai de 0 a 5. O OSSIM tem a visibilidade de todos os hosts ativos da rede corporativa, monitorando as ameaças e o tráfego de rede sendo assim ele atribui um valor de grau de risco para cada evento gerado na rede. A partir dessa classificação é definido se é um ataque ou um falso-positivo. O cálculo da avaliação de riscos é baseado da seguinte forma: O valor do ativo para a organização "Quanto é valioso a informação que o ativo possui? ". Prioridade, o quanto ameaça pode afetar a organização "Se comprometido, posso tirar alguma lição?". E a probabilidade que o evento ocorre.

Segundo Tavares (2015) a análise de riscos é uma das *features* integrada ao OSSIM e se faz necessária, sua função é mensurar o risco e fazer a avaliação dos eventos mais relevantes, tendo um papel fundamental no apoio ao processo da tomada de decisão dos gestores. O OSSIM realiza o cálculo de risco do evento gerado, baseado nos parâmetros: valor do ativo para organização (0 a 5); priorização, ameaça que tem relevância para o evento (0 a 5); Probabilidade que o evento ocorre (0 a 10). A fórmula para o cálculo do risco é baseado da seguinte forma:

$$\text{Risco} = (\text{Valor} * \text{Priorização} * \text{Probabilidade}) / 25$$

2.2.5 – Avaliação do nível de ataque utilizando o algoritmo CALM

Segundo Karg (2003) o CALM (Compromisso de monitorização de nível de ataque), é um algoritmo de avaliação que guarda um grande volume de eventos para recuperação com o tempo. Recebe na entrada um grande volume de eventos e como saída um único indicador que realiza a tradução de cada host ativo na rede, tudo que está sendo monitorado. A coleta dos eventos gerados é realizado através do grau de risco de cada evento. Ele exibe o nível de compromisso e ataque da seguinte forma:

- Variável nível "C" é o compromisso que mede a possibilidade de um host está comprometido;

• Variável nível "A" é o ataque, que está sujeito a um sistema, host que mede o possível risco que está sofrendo ataques.

A divisão de cada variável é que são características distintas sendo a variável "A" indica que há possibilidade de estar sofrendo ataques. Já o nível "C' é uma possibilidade indicando que o host pode ter sido comprometido.

A designação das variáveis em um host na rede, é realizado da seguinte forma: Qualquer possível ataque entre host 1 e host 2 será designado a variável "A" (Nível de ataque recebido) para o host 2 e variável "C" (nível de compromisso de ações que supostamente um invasor realizaria) para o host 1. No caso de tratamento de resposta de ataque elevaria a variável C nos dois hosts. Eventos internos a variável C é categorizada apenas no host de origem.

2.3 – TIPOS DE ATAQUES POPULARES

O CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) contabilizou no ano de 2016, 647.112 incidentes que foram reportados, deste total 60.432 foram sobre notificações que computadores participaram de ataques de negação de serviço (DoS) e que teve um aumento de 138% em relação a 2015, uma grande parcela referente a essas notificações corresponderam a ataques que tiveram origens por equipamentos de IoT (Internet das Coisas) que foram alvos e participaram de *botnets*.

Outro dado interessante realizado pela equipe do CERT.br o ataque de *phishing* aumentou 37% em relação a 2015, em contrapartida a utilização de cavalos de troia, utilizado principalmente para roubo de informações, tiveram uma queda de 46% em relação a 2015. Notificações de varreduras nas portas em busca de falhas/vulnerabilidades somaram 383.903 em 2016, as portas mais comuns para realizar ataques de força-bruta ainda são alta. Houve uma diminuição para 16% de notificações a ataques a servidores Web em relação a 2015 totalizando 55.441 notificações (CERT.br, 2016).

2.3.1 - Phishing

Segundo o *Anti-Phishing Working Group* APWG (2010) a definição de *phishing* é uma forma de fraude em que o invasor por meio de técnicas conhecidas como engenharia social tentam roubar dados confidenciais, a prática utilizada por uma pessoa mal-intencionada é enviar *e-mail's* ou páginas web com *link's* maliciosos, na tentativa de

ludibriar o usuário. O meio mais comum para essa prática, é o envio de e-mail parecendo ser autêntico enviado por uma empresa conhecida; incluem logos, telefones e endereços para que o e-mail parece ser verídico e clicar no link malicioso para inserção de dados pessoais e inúmeras coisas pode ser utilizado e baixado por exemplo software maliciosos, sendo totalmente ofuscado.

2.3.2 - Negação de serviços (DoS)

O ataque de negação de serviços – *Deny of Service* (DoS) torna-se o acesso a sistemas indisponível para o usuário, basicamente o ataque funciona através de várias requisições seguidas de acesso para o servidor que hospeda o sistema, mantendo assim a resposta do servidor sempre ocupada, tornando o acesso indisponível para o usuário, o ataque pode ser iniciado a partir de um único host. Diferente acontece em um ataque distribuído de negação de serviço (DDoS) onde são utilizados várias máquinas realizando um ataque simultâneo ao um servidor especifico e o mesmo não puder responder a todas requisições que estão na fila.

2.3.3 - Malware

O *malware* é definido como um software malicioso com o objetivo diversos como roubar informações, criptografar dados, alterar e excluir. Pode também ter o controle total do computador sem a percepção do usuário. Existem diferente tipos de malwares: Vírus, Worm, Cavalo de tróia, Spyware, Ransoware, Rootkit e até backdoor pode ser classsifcado como um malware.

- **Vírus:** é o *malware* mais comum, é um software malicioso que se auto-executa e realiza a infecção na máquina.
- **Worm:** atua diferente do vírus, já que ele pode se auto replicar, sem a necessidade de um software especifico.
- **Cavalo de tróia:** é ofuscado como um software legitimo, após ser instalado, ele executa suas funções maliciosas.
- **Spyware:** ele coleta informações e dados e monitora as atividades que o usuário realiza, sem o consentimento do mesmo.
- **Ransoware:** bastante popular nos últimos tempos, ele é projetado para criptografar os dados do usuário, é exigido em então pelo individuo mal-intencionado pagamento em criptomoedas como forma de resgate dos dados.

- **Rootkit:** tem a capacidade de camuflar outros tipos de *malwares* utilizados, instalado na máquina do usuário sem que haja detecção, fornece também o nível de administrador.
- **Backdoor:** um sistema já infectado, que permite acesso remoto a máquina.

2.4 – TRABALHOS RELACIONADOS

A seção apresenta os trabalhos relacionados que foram estudados sobre o OSSIM e sua implementação em ambiente corporativo.

2.4.1 - Gerenciamento centralizado de eventos de segurança da informação

Este trabalho apresentou como um estudo de caso a utilização do OSSIM integrado com outras ferramentas de segurança para coleta de dados consistentes como: firewall, IDS e IPS. Com o objetivo de prover uma maior segurança na infraestrutura do Tribunal de Justiça da Paraíba (TJ-PB) com foco de ter os eventos gerados de forma centralizadas para o auxílio de gerenciamento de incidentes. A preocupação com a segurança no TJ-PB, se deve ao motivo de ter sistemas de processos eletrônicos.

2.4.2 - Open-Source intelligence em sistemas SIEM

A técnica utilizada neste trabalho é a integração do algoritmo de aprendizagem de máquinas supervisionada, com o objetivo de refiná-los, na garantia que ao SIEM é repassada apenas a informação relevante. Para a validação do trabalho, foi utilizado provas empíricas da aplicabilidade da solução, em contexto prático e real, demonstrando, efetivamente, o poder de síntese, com base em feedback do utilizador, solução proposta. Os resultados do trabalho apresentaram bons indicadores de que a abordagem é viável e que o componente é capaz de reduzir e filtrar volumes significativos de informação.

2.4.3 - Análise de eventos de segurança: OSSIM

O foco dessa dissertação, é a análise do OSSIM para gestão de eventos com foco em especifico para gestores no apoio da tomada de decisão. A dificuldade encontrada se deu ao fato da geração de inúmeros eventos recorrentes e atrapalhou a forma de avaliação dos eventos e mostrar que o OSSIM é uma alternativa de solução *opensource* para o SIEM. Realizado um estudo sistemático dos logs e revisão constante de regras e configurações, para

amenizar eventos de falsos negativos e otimizar a correlação dos falsos positivos. Foram realizados testes para verificar o comportamento do OSSIM.

2.5 – APLICAÇÕES SIEM

O conceito SIEM foi definido por Mark Nicolett e Amrit Williams ambos da Gartner em 2005. A descrição para o conceito, é que uma solução para coleta, análise e apresentar de forma correlacionada os eventos coletados de diversas fontes de dados da rede como firewall, IDS, IPS, antivírus, logs de servidores, banco de dados, aplicações.

A origem para o termo SIEM, foi da integração de duas tecnologias já conhecidas no mercado, que operavam de formas distintas a SIM (Gerenciamento de Segurança da Informação) e o SEM (Gerenciamento de Eventos de Segurança). Os papéis de ambos eram distintos:

SIM (Gerenciamento de Segurança da Informação): Focado na análise forense, realizava o armazenamento de logs por maiores períodos para posteriormente ser usado na análise e geração de relatórios.

SEM (Gerenciamento de Eventos de Segurança): Realizava o monitoramento de dados em tempo real para apoio a tomada de decisão de incidentes de segurança.

Com o crescente avanço e a intensificação massiva de ataques, houve a necessidade de integrar os dois conceitos, criando o SIEM, que proporcionou uma visibilidade maior da rede, integrando o monitoramento em tempo real, armazenamento de logs para análise e a correlação de eventos de diversas fontes de informação.

Atualmente existem diversos *vendors* para soluções SIEM, como podemos ver pela imagem 2.3 do quadrante mágico, onde lista os melhores do mercado no ano de 2016, avaliados pelo Gartner.

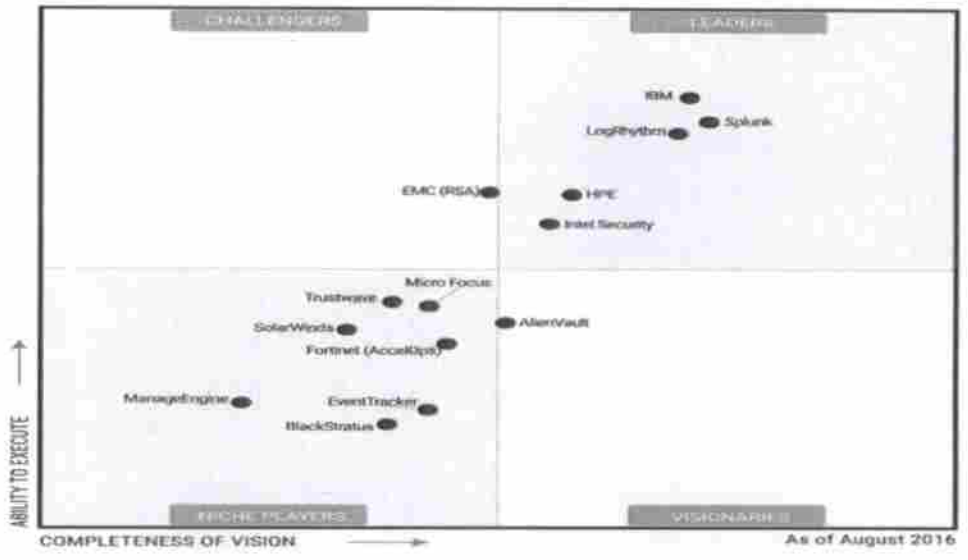


Figura 2.3: Quadrante mágico gartner dos SIEM'S (Gartner, 2016).

O quadrante mágico, produzido pelo Gartner, é dividido em quatro quadrantes: visionários, concorrentes de nicho, desafiadores e líderes.

Visionários: São empresas que focadas na pesquisa e desenvolvimento, são visionárias, mas não possuem tecnologia capaz de executar o que a aplicação promete.

Concorrentes de Nicho: Empresas focadas em uma especifica características da aplicação.

Desafiadores: São empresas que tem a capacidade execução plena da aplicação mas possuem apenas uma parte do mercado.

Líderes: Empresas que possuem tecnologias mais avançadas, tem uma melhor visão do mercado e entregam a aplicação como prometida

Dados apresentados pela Gartner no quadrante mágico dos SIEM, será apresentado os líderes de mercados que são: IBM (QRadar), Splunk, LogRhytm.

2.5.1 - IBM QRadar

A IBM possui uma plataforma especifica para SIEM, o IBM QRadar que oferece uma integração de logs, detecção de anomalias, gerenciamento de incidentes e vulnerabilidade.

QRadar utiliza um mecanismo de "*Sense Analystics*" na tentativa de realizar detecção de ameaças de alto risco e ataques.

Uma das vantagens de se utilizar o QRadar é que os alertas dos eventos gerados dos clientes são enviados para serem tratados e avaliados na SOC da IBM. Outra característica é a unificação em uma só arquitetura que agrega diversos *features* como a análise de logs, *netflows*, busca de vulnerabilidades:

- Realiza a correlação de eventos em tempo real na identificação de ameaças e ataques.
- Prioridade nos incidentes identificado como alto risco.
- Análise constante de risco existente na rede, que envolve problemas de configuração e vulnerabilidade conhecidas.
- Atua proativamente nas respostas automatizadas que envolve incidentes.

2.5.2 - Splunk

O Splunk com a aplicação SIEM titulado como Splunk Enterprise Security (ES) fornece informações sobre fontes de dados diversos de tecnologias de segurança, permite que centro de operações de segurança realizem a detecção e respondam proativamente a ataques internos e externos.

O Splunk Enterprise Security pode ser dimensionado para qualquer tamanho corporativo. Uma das vantagens é um relatório da visão de risco de negócios que uma determinada ameaça pode vir a causar.

A aplicação tem a flexibilidade para realizar a personalização de pesquisas de alertas, correlação de eventos, geração de relatórios e painéis que atende a necessidades específicas.

Outras funcionalidades importantes para o Splunk Enterprise Security são:

- Monitoramento em tempo real de forma que visualize com clareza os resultados das análises de eventos gerados.
- Uma visibilidade segura dos dados corporativos o que aumenta a eficácia na detecção de intrusões e assim a resposta de incidentes.
- Correlações visuais, dinâmicas e estáticas na tratativa de detectar anomalias e ameaças na rede.

2.5.3 - LogRhytm

LogRhythm é uma plataforma de segurança inteligente que combina SIEM, gerenciamento de logs, monitoramento de integridade de arquivos com *forensics* de rede e

hosts. Ele é desenvolvido para correlacionar o endereçar os eventos de rede e as possíveis vulnerabilidades, riscos e ameaças em uma única tecnologia com alta performance e que entrega controles e visibilidades exigidos em conformidades e regulamentações (Kavanagh et al 2014).

Características do LogRhythm:

- SIEM de próxima geração e gerenciamento de logs;
- *Forensic* de host independente e monitoramento de integridade de arquivo;
- *Forensic* de redes com identificação de aplicação e captura do pacote completo;
- Log Rhythm Machine Analytics:
- Correlação avançada e reconhecimento de padrões;
- Usuários multi dimensionais/Host/Detecção de anomalia por comportamento de rede;
- Consultas rápidas, fáceis e inteligentes;
- Análise e consultas de dados por meio visual e *drill down*;
- Resposta automática a eventos por meio do LogRhythm SmartResponse;
- Gerenciamento de casos integrado a plataforma.
- Detecta *malwares* customizados com Detecção de Anomalias pelo Comportamento do Host.
- Expõe credenciais comprometidas com Detecção de Anomalia pelo Comportamento do Usuário.
- Identifica vazamento de dados com Detecção de Anomalias pelo Comportamento da Rede.

2.6 – SÍNTESE DO CAPITULO

O objetivo na elaboração do capitulo foi realizar uma explicação do que seria o siem e as suas vertentes, como também apresentar o OSSIM e a sua arquitetura. Mostrado também como é realizado e classificado as correlações e métricas utilizadas para o funcionamento de um dos principais papéis do OSSIM que é correlacionar eventos. Além disso, mostra os principais tipos de ataques mais populares atualmente e os seus conceitos. Os trabalhos correlatos que foram permitidos citar os autores dos trabalhos que referenciaram na utilização do SIEM e implantação. As principais aplicações SIEMs foram discutidas e mostrado suas vantagens.

3 – RESULTADOS DA UTILIZAÇÃO DO SIEM PARA DETECÇÃO DE CIBERATAQUES

Este capítulo apresenta o modelo proposto do SIEM utilizando a aplicação *open-source* OSSIM na detecção de ataques cibernéticos para a proteção da rede corporativa bem como no auxílio na tomada de decisão quando detectado anomalias na rede.

3.1 - MODELO PROPOSTO

A necessidade de utilização de uma solução que visa centralizar em uma única interface, se tornando um grande apoio para a equipe de segurança da informação, pode ser obtida através de um SIEM que possibilita ter toda a visibilidade da rede corporativa em tempo real.

O SIEM tem como uma das características a correlação de eventos, onde dados são obtidos de diversas fontes com geração de logs. A aplicação usada neste trabalho o OSSIM, tem diversos plug-ins que permite a integração com essas diversas fontes que geram logs para coleta e realizar de maneira eficaz a correlação dos eventos. Na garantia de melhores resultados, existem regras na configuração do OSSIM que podem ser editadas e melhoradas.

As simulações dos ataques foram realizadas em um ambiente controlado com dois hosts já conhecidos por ter diversas vulnerabilidades, com o objetivo de verificar como o OSSIM identifica e gerencia os eventos gerados na rede.

3.2 - TOPOLOGIA DA REDE

O laboratório de rede constitui de uma estação de trabalho, um servidor com diversos serviços (ssh, ftp, http), servidor OSSIM, duas máquinas atacantes e um modem/roteador.

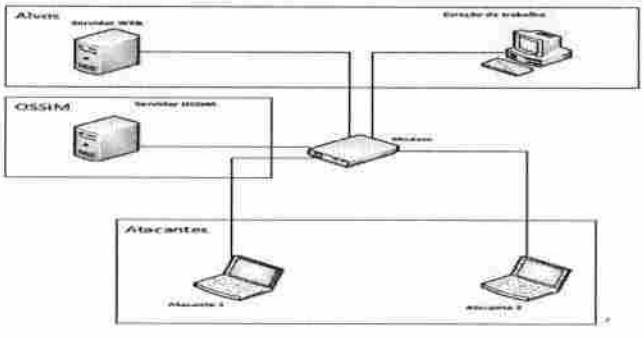


Figura 3.1: Topologia do Laboratório.

Na topologia da Figura 4.3 temos dois hosts como alvos, a estação de trabalho com o sistema operacional Windows XP com o hostname "target" e um servidor ubuntu com hostname "serverweb2" que contém diversos serviços rodando, as escolhas dos dois hosts foram pertinentes por conter diversas vulnerabilidades já conhecidas para ser explorada. Dois hosts terão a tarefa de realizar os ataques, uma forma de identificar ataques de diversas origens. No centro da topologia temos um modem/roteador, que está configurado para atribuir IP automático. O servidor OSSIM tem o endereço com o ip fixo: 192.168.0.10. O servidor ubuntu também utiliza IP fixo: 192.168.0.2 e contém diversos serviços. A estação de trabalho configurado para receber IP automático e no momento da simulação o dhcp do modem/roteador, atribuiu o IP 192.168.0.3.

Por fim temos duas máquinas atacantes com algumas ferramentas instaladas no auxílio de realizar os ataques e observar o comportamento do OSSIM quando é efetuado os ataques de diversas origens.

3.3 - SIMULAÇÕES E RESULTADOS

3.3.1 – FERRAMENTAS UTILIZADAS

Na busca de uma solução que centralizar toda a visibilidade e eventos que o ocorre na rede corporativa. A escolha de um SIEM, tem todos os pré-requisitos para esse cenário, já que o objetivo é uma aplicação que gerencia eventos de segurança, logs, relatório, abertura de tickets, entre outras funcionalidades. A aplicação escolhida como base deste trabalho, é a aplicação OSSIM, por ser *open-source* e tem um propósito definido. Um erro muito comum para quem quer realizar uma implantação de um SIEM na rede corporativa, é achar que fazer as configurações somente na primeira vez, é o suficiente para manter a aplicação de forma eficaz, mas não é, tem que está em constante revisão das regras e realizando novas configurações periodicamente. O OSSSIM apesar de ser um software livre está em crescente evolução e possui uma comunidade ativa.

3.3.2 - Cenário de Simulação

Na elaboração do cenário de simulação em um ambiente controlado, foi definido as seguintes configurações para cada host:

- Estação de trabalho (Alvo) – Sistema operacional Windows Xp, processador de um núcleo, memória ram 512MB, 50 GB de HD.

- Servidor (Alvo) – Sistema operacional Linux – Ubuntu Server 8, processador de dois núcleos, memória ram 1GB, 60GB de HD.

- Servidor OSSIM – Processador de três núcleos, memória ram de 6GB, 80GB de HD.

Todos os hosts, foram virtualizados e criado uma range de IP especifica 192.168.0.1/28 para o ambiente, durante todo o processo de simulação, os ataques tiveram origem da rede interna. Somente o OSSIM com os agentes OSSEC instalado nos alvos foram testados no ambiente sem integração com firewall, IDS e IPS externos.

3.4 – SIMULAÇÃO DOS ATAQUES

Antes de iniciar os ataques aos hosts, foi realizado uma varredura direcionada com versionamento para cada host, em busca de portas abertas e possíveis vulnerabilidades com auxílio da ferramenta nmap. É relevante ressaltar, que foram utilizados dois métodos para realizar a varredura, o primeiro partindo da máquina do atacante foi com nmap, uma ferramenta livre em *open-source* que sua principal função é o mapeamento da rede e utilizado para fazer a varredura de portas. O segundo método, foi realizado pelo próprio OSSIM com o seu gerenciamento de vulnerabilidade, utilizando uma das ferramentas integradas a ele que é o OpenVAS um scanner de vulnerabilidade.

A primeira varredura foi realizada no servidor com o *hostname* "serverweb2", utilizando os dois métodos citados anteriormente.

Quando realizamos a varredura em busca por vulnerabilidades no ambiente proposto, descoberto que o servidor "serverweb2" executa um serviço FTP com a versão 2.3.4 que possui uma vulnerabilidade crítica nessa versão como apontou o relatório de vulnerabilidade realizado pelo OpenVAS, essa versão contém um *backdoor,* que através dessa falha, temos acesso ao *shell* reverso do servidor com privilégios de root, tendo o controle completo do servidor, que a partir dele, podemos ter controle total da rede, explorando outros ativos da rede.

O OSSIM ao encontrar essa vulnerabilidade o classificou como de alto risco. Abaixo é mostrado detalhes referentes a essa falha no relatório de vulnerabilidades gerado pelo sistema e no scanner de portas utilizando a ferramenta nmap da máquina do atacante.

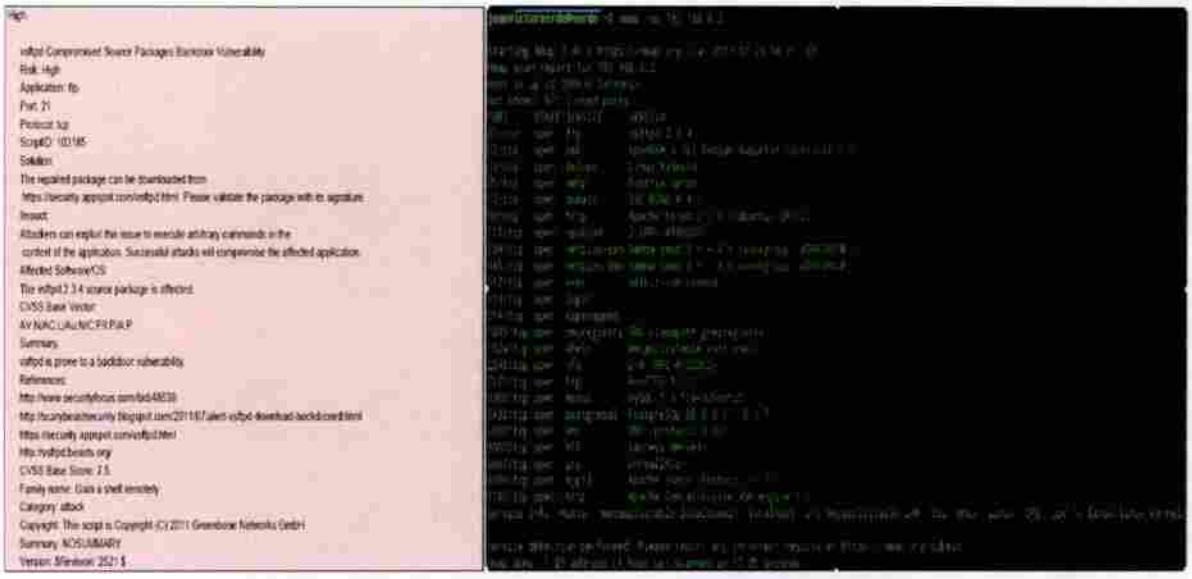


Figura 3.2: Resultado do Scanner de vulnerabilidade realizado pelo OpenVAS e varredura de portas pelo nmap (o autor, 2017).

O relatório de vulnerabilidade realizado pelo OSSIM, identificou diversas vulnerabilidades no servidor, como já era esperado, a escolha para explorar essa vulnerabilidade especifica da versão do ftp, se motivou pelo fato de obter acesso ao shell como root e sem realizar nenhum tipo de intervenção fisica na máquina alvo ou utilizar técnicas de engenharia social.

A segunda varredura realizada na estação de trabalho, também se utilizou os dois métodos e o resultado foi o esperado, com um sistema legado mas muito utilizado como estação de trabalho pelo mundo o sistema operacional Windows XP, encontrado diversas vulnerabilidades que podem ser exploradas.

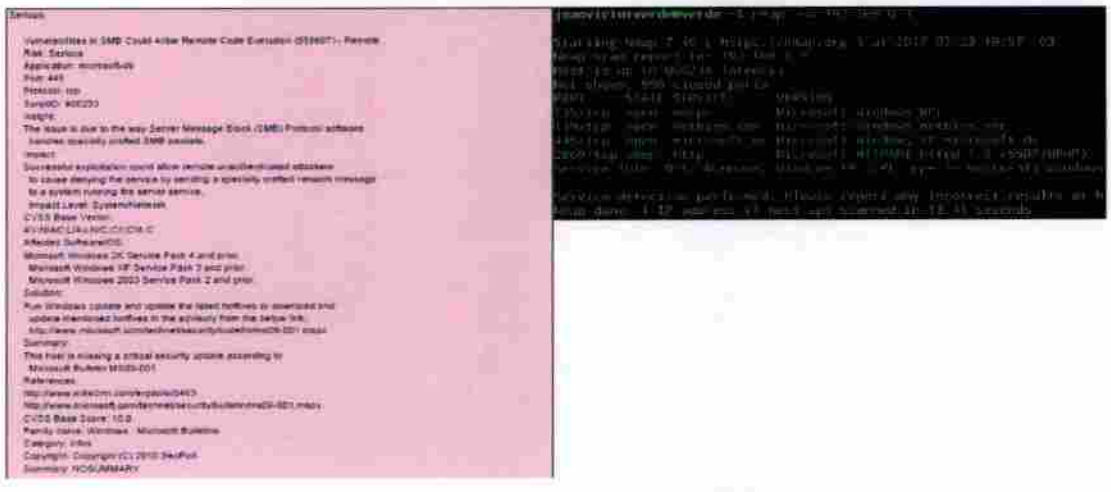


Figura 3.3: Resultado do Scanner de vulnerabilidade realizado pelo OpenVAS e varredura de portas pelo nmap na estação de trabalho (o autor, 2017).

A vulnerabilidade encontrada é explorada pela porta 445 do SMB (*Server Message Block*) no Windows esse serviço provê aceso compartilhado a arquivos e impressoras na rede, com essa falha explorada pela porta, obtivemos o controle total da estação de trabalho, sem realizar qualquer tipo de autenticação ou utilizar de técnicas de engenharia social para ter sucesso do ataque.

3.4.1 - REALIZAÇÃO DOS ATAQUES

Na realização dos ataques, foram utilizadas duas máquinas distintas para analisar o comportamento da aplicação OSSIM quando se trata de ataques de diversas origens ao mesmo tempo. O sistema operacional utilizado para realizar os ataques foi o Kali Linux, que é uma distribuição especifica para testes de penetração que já vem integrado várias ferramentas para auxilio. Após a varredura e o conhecimento das vulnerabilidades, deu-se prosseguimento com os ataques, explorando as falhas e vulnerabilidade encontradas.

3.4.2 - Ataque ao servidor

A ferramenta Metasploit foi escolhida para realizar o ataque e utilizando um *exploit* existente que explora a falha da versão do ftp 2.3.4, foi possível obter um *shell* reverso remoto do servidor e com privilégios root.

```
msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.0.2
RHOST => 192.168.0.2
msf exploit(vsftpd_234_backdoor) > ex
exit     exploit
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.2:21 - USER: 331 Please specify the password.
[+] 192.168.0.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.8:35485 -> 192.168.0.2:6200) at 2017-07-13 23:40:44 -0400
```

Figura 3.4: Ataque explorando a falha na versão do FTP (o autor, 2017).

3.4.3 - Ataque a estação de trabalho

Utilizada a mesma ferramenta ao ataque no "serverweb2", realizado uma pesquisa dos *exploits* disponíveis para obter acesso ao alvo por meio do Shell reverso.

```
msf exploit(smb_relay) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.3
RHOST => 192.168.0.3
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] 192.168.0.3:445 - Automatically detecting the target...
[*] 192.168.0.3:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Portuguese - Brazilian
[*] 192.168.0.3:445 - Selected Target: Windows XP SP3 Portuguese - Brazilian (NX)
[*] 192.168.0.3:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.3:1131) at 2017-07-23 19:06:31 -0400

meterpreter >
```

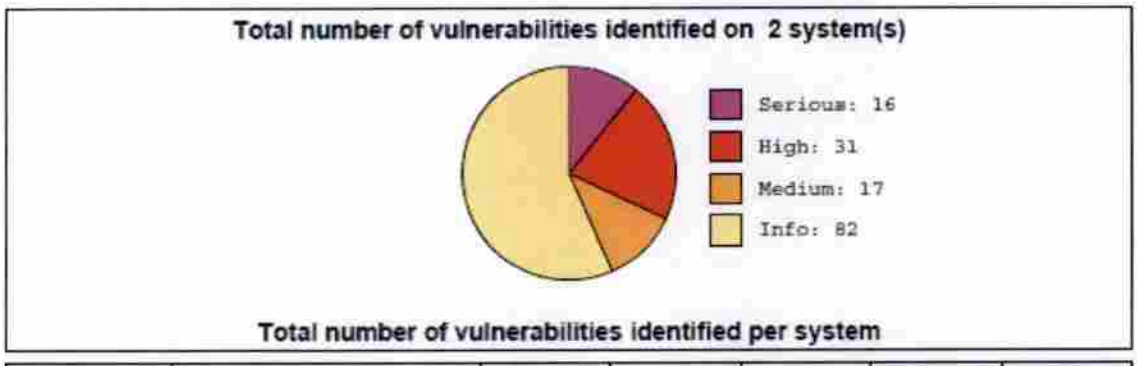
Figura 3.5: Ataque na vulnerabilidade do SMB na porta 445 (o autor, 2017).

3.5 - RESULTADOS DAS ANÁLISES DE DETECÇÃO DOS ATAQUES NO OSSIM

Após a realização dos ataques nos hosts, a coleta de eventos realizados pelo OSSIM, foi satisfatória. Como já mencionado na sessão anterior, realizado um scanner completo na rede, em busca de vulnerabilidades dos hosts que se tem visibilidade.

Após o fim da varredura, realizado pela ferramenta integrada ao OSSIM, o OpenVAS, foi gerado um relatório contendo todas as informações e graus de riscos que a vulnerabilidade representa para os hosts.

O gráfico abaixo, extraído diretamente do OSSIM, mostra em detalhes a quantidade de vulnerabilidades encontrada:



HostIP	HostName	Serious	High	Med	Low	Info
192.168.0.2	serverweb2	14	31	17	--	67
192.168.0.3	windowsxp	2	--	--	--	15

Figura 3.6: Gráfico de quantidade de vulnerabilidade na rede (o autor, 2017).

O gerenciamento de vulnerabilidade após realizar a varredura, automaticamente realiza a abertura de tickets a ser tratado para cada vulnerabilidade encontrada.

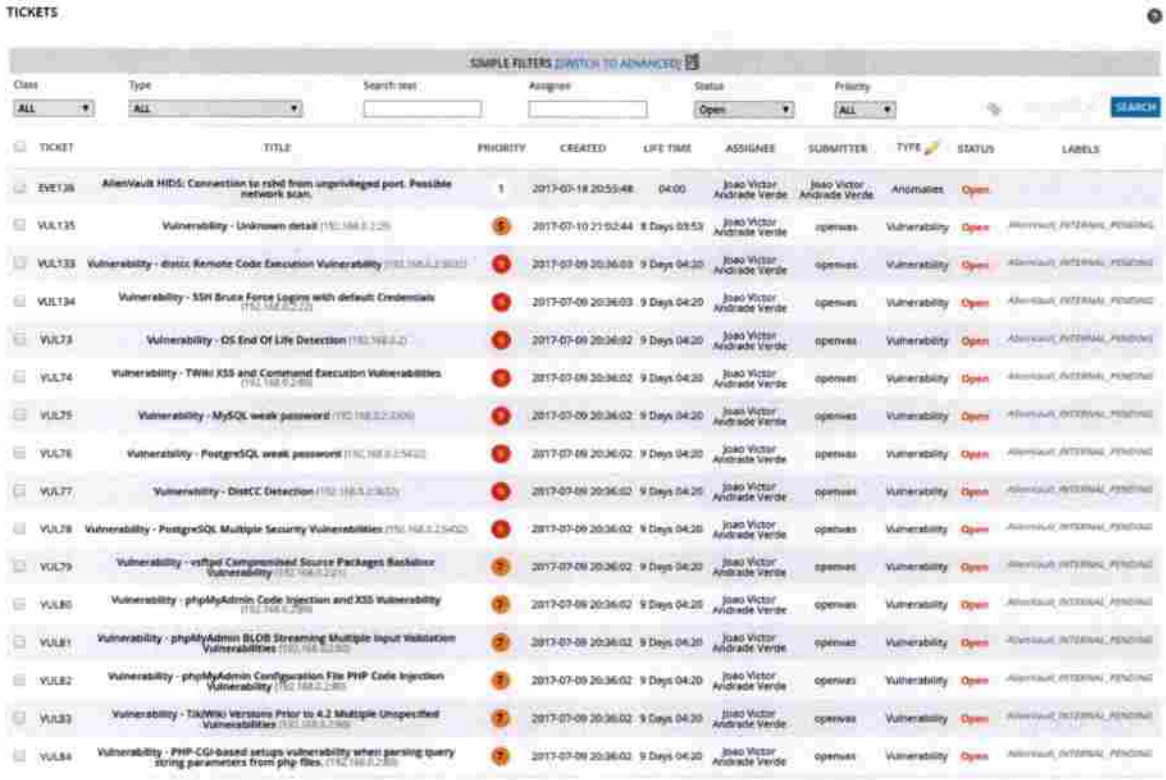


Figura 3.7: Tickets abertos após a verificação de vulnerabilidade (o autor, 2017).

Como o scanner ele é de modo intrusivo, surgiu vários alarmes no OSSIM alertando diversos eventos sendo como ataques nos hosts, sendo assim foram falsos positivos.

Figura 3.8: Eventos de Falsos Positivos (o autor, 2017).

Além dos ataques realizados citados, foi feito também um ataque de força-bruta para acesso remoto através do SSH no servidor "serverweb2" o OSSIM identificou o ataque imediatamente partindo das máquinas dos atacantes e abriu dois tickets:

Figura 3.9: Alarmes de Ataques de força-bruta (o autor, 2017).

Utilizando o nmap a partir do host do atacante, enquanto era realizado o scanner na rede, mais uma vez obtivemos êxito no resultado e o OSSIM identificou o *scan* na rede:

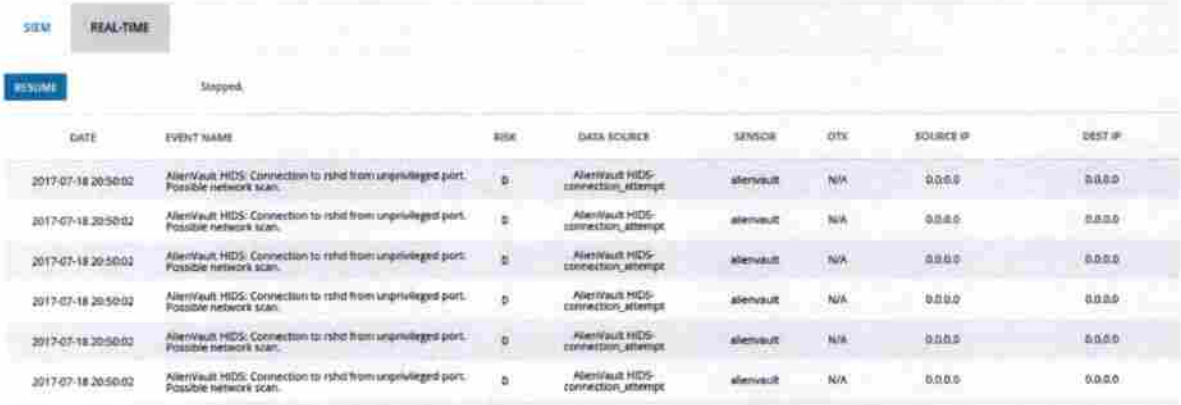


Figura 3.9.1: Evento identificado no OSSIM como *scan* na rede (o autor, 2017).

Figura 3.9.2: Detalhes do evento do scanner (o autor, 2017).

Como resultado dos ataques realizados o OSSIM identificou os eventos de ataques sendo realizado nos hosts:

No primeiro ataque no host da estação de trabalho, que foi aproveitado de uma falha na versão do SMB porta 445 que dar privilégios para executar códigos remotamente através do *shell*, o OSSIM identificou que estava tendo um ataque e gerou o evento identificando que a porta foi infectada e está tendo um tráfico não comum pela porta.

Figura 3.9.3: Detalhe do evento gerado com um tráfego não comum na porta 445 (o autor, 2017).

Já no segundo ataque, realizado no serviço FTP do servidor web identificado tráfego no serviço FTP mas não ficou claro que se tratava de um *backdoor* da falha do VSFTPD:

Figura 3.9.4: Detalhe do evento com tráfego no serviço FTP (o autor, 2017).

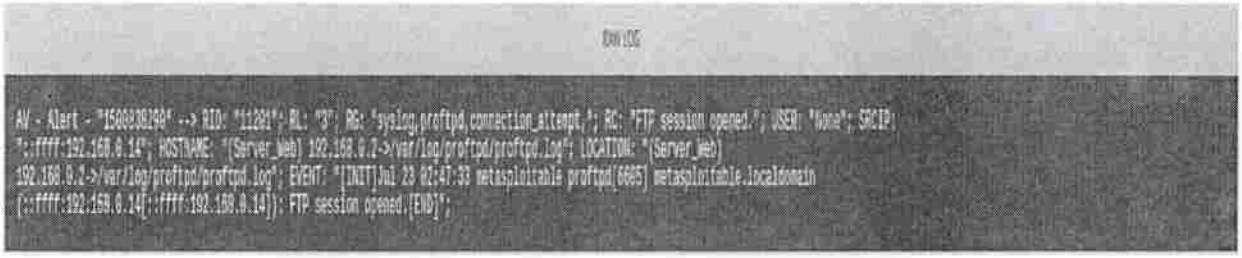


Figura 3.9.5: *Raw Log* apontando o servidor de origem do tráfego (o autor, 2017).

Apontado nos logs o ip do servidor de ataque, não foi classificado como uma invasão através do *backdoor*, o log informou que o serviço FTP teve a sessão aberta. Após o fim dos testes de laboratório obteve-se um total de 17,152 eventos registados na base de dados.

3.6 – SÍNTESE DO CAPÍTULO

O objetivo deste capítulo foi realizar a implementação e fazer uma análise da utilização do SIEM na detecção de ciberataque, utilizado no modelo proposto a aplicação OSSIM.

Na simulação de ataques realizados, foi instalado um HIDS em cada host como alvo, utilizando o OSSEC como agente que enviou as informações coletadas em cada host para o servidor central. Conforme definido no cenário de simulação do ataque na seção 3.4.2 os ataques ao servidor web, explorando uma das vulnerabilidades encontradas tiveram êxitos. Assim como na seção 3.4.3 que foi explorado uma vulnerabilidade através da porta 445 do SMB no sistema operacional Windows XP.

Na coleta dos resultados dos ataques realizados nas seções anteriormente na seção 3.5 o OSSIM realizou a detecção dos ataques com sucesso e apontou outras diversos possíveis ataques que ocorreram na rede como por exemplo: autenticação de força bruta via ssh e varredura de porta. Atingindo as perspectivas, os resultados obtidos de acordo com as simulações de ataques a aplicação OSSIM coletou os dados de forma satisfatórias. Na análise dos resultados as definições de regras na detecção de ataques, mostrou-se como uma regra bem ajustada define a forma que cada ataque será tratado.

No capítulo seguinte é realizado a conclusão do trabalho de como os objetivos foram alcançados e que se mostrou eficaz na proposta deste trabalho e uma análise da ferramenta OSSIM no geral e suas particularidades.

4 - CONCLUSÕES

A utilização de um SIEM com as funcionalidades integradas, torna-se essa aplicação uma solução de grande apoio a equipes de segurança e SOC. O OSSIM uma aplicação SIEM em *opensource* utilizado como modelo nesse trabalho, realiza o papel que é proposto a fazer, a aplicação ainda está em processo de melhoria e maturidade, mas já se mostra uma opção para implementação em diversos ambientes corporativos. Há muitas regras e configurações de ajustes a serem feitas constantemente, com o objetivo de ter correlação de eventos de forma mais clara, amenizando os problemas de falso positivo e melhorando na detecção de falso negativo.

A metodologia utilizada no trabalho, mostrou-se eficiência para a implementação em um ambiente controlado do OSSIM. Através das pesquisas bibliográficas foi possível conceituar diversos pontos relacionados ao SIEM que foram importantes para o desenvolvimento do trabalho.

Os objetivos propostos apontados neste trabalho, com o intuito de ter uma aplicação capaz de unificar em uma única interface, os diversos eventos gerados e realizando de forma concisa um correlacionamento para auxilio da tomada de decisão. O SIEM se mostra como uma proposta eficiente nesse sentido.

O papel da gestão no acompanhamento dos processos que envolve a aplicação, é fundamental na determinação de eventos gerados, tendo em vista que a classificação de prioridade, tem que está alinhado com o valor do ativo que ele representa para a organização.

Um destaque que o OSSIM possui é a possibilidade de unificar a aplicação, as conformidades de segurança como a PCIDSS e a ISO27001 como forma de especificar controles e mapear os processos de forma centralizada.

Na utilização da aplicação OSSIM os resultados foram satisfatórios, na medida que foi executado as simulações de ataques em um ambiente controlado e com falhas e vulnerabilidades conhecidas. Avaliado os principais recursos que o OSSIM oferece como gerenciamento de vulnerabilidades, eventos, incidentes, abertura automática de tickets para verificação de eventos classificados como incidentes e monitoramento em tempo real.

Verificou-se que ataques simulados foram detectados pelo OSSIM, possibilitando auxílio no apoio a tomada de decisão para definição de qual maneira o ataque pode ser mitigado.

4.1 - TRABALHOS FUTUROS

Como proposta de trabalhos futuros são indicados alguns pontos que podem ser evoluídos.

Há a necessidade de aprimorar e integrar com outros métodos para ter uma melhoria significativa e fazer frente aos SIEM proprietários, algumas dessas medidas é o foco nos dispositivos IoT (Internet das Coisas) que é um mercado emergente em plena expansão e crescimento pelo mundo. Realizar um levantamento de estudo para integrar com conformidade com uma das principais normas da área de segurança a PCI DSS e a ISSO27002, tem a necessidade de criar mapeamentos desses modelos e estudar a forma de ter a conformidade trabalhar em conjunto com a aplicação.

Um ponto relevante para um trabalho futuro, é o estudo de algoritmos de aprendizagem de máquinas, como foco em aprender o tipo de ataque, ser capaz de classificar e ao mesmo tempo fazer a prevenção do mesmo. É um recurso diferencial a ser utilizado nos SIEM, tendo em vista que é um processo cíclico por parte do time de segurança quando um ataque é realizado na rede corporativa. A criação de plug-ins para determinados fontes de dados que agregam ao SIEM com o objetivo de melhoria na correlação de eventos.

A simulação em um ambiente de produção não foi realizada. Acredita-se que os resultados e as coletas de informação seriam mais consistentes e claro, já que a partir do momento que um host está na internet, torna-se vulnerável para qualquer tipo de ataque independentemente da origem, coletando por exemplo se houve alguma varredura de porta especificando aquele host. Esta simulação validaria as regras na detecção de ataques de origem externa e o real impacto e melhoria na centralização de eventos de segurança em uma só aplicação.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2005. (2005). Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação. ISBN 978-85-07-00668-0.

Bowling J (2010) AlienVault: the Future of Security Information Management. Linux J 2010:2.

CERT.br Centro de Estudos, Resposta e Tratamento de incidentes de Segurança no Brasil. Incidentes reportados ao cais: por ano, 2016. Disponível em: https://www.cert.br/stats/incidentes/2016-jan-dec/analise.html. Acesso em 22 de junho de 2017

CAIS. Incidentes reportados ao cais: por ano, 2014. Disponível em: https://www.rnp.br/servicos/seguranca/tratamento-incidentes/estatisticas. Acesso em 22 de junho de 2017

Chen K.. et al; Chen Kang and Zen WeiMing. (2009) "Cloud computing: system instance and current research," Journal of Software, 20-25:1337-1347.

Chandola et al., 2009 Chandola, V., Banerjee, A., Kumar, V. (2009), "Anomaly Detection : A Survey", ACM Computing Survey.

Carracedo Gallardo J (2004) Seguridad en redes Telemáticas. Editor Mc Graw Hill 1:1–32 Computer Communication, Vol. 34, pp. 1328-1341.

Department of Homeland Security. Cyber security research and development, 2011

Kavanagh K, Nicolett M, Rochford O (2014) Magic Quadrant for Security Information and Event Management. In: Licens. Distrib. - Gart. Disponível em http://www.gartner.com/technology/reprints.do?id=1-1VW8N7D&ct=140625&st=sb. Acesso em 29 de Junho 2017

Kumar e Selvakumar, 2011 Kumar, P. A. R., Selvakumar, S. (2011). "Distributed Denial of Service Attack Detection Using an Ensemble of Neural Classifier", Computer Communication, Vol. 34, pp. 1328-1341.

Karg D, Muñoz JD, Gil D, et al (2003) Descripción General del Sistema. AlienVault Docs

Miller D, Harris S, Harper A, et al (2011) Security information and event management (SIEM) implementation.

SOUZA, V. M. Sistema de Gerenciamento de Eventos e Informações de Segurança (SIEM). 2016. Disponível em: <http://www.usuarioseguro.com.br/16/2016/06/24/siem-sistema-de-gerenciamento-de-eventos-e-informacoes-de-seguranca/>. Acesso em: 28 de junho de 2017.

Tavares (2015) Análise de eventos de segurança:baseado no OSSIM. 2015

Yue e Wang, 2009 Yue, C., Wang, H. (2009) "Charatering Insecure JavaScript

Zadrozny P, Kodali R (2013) Big Data Analytics Using Splunk: Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources. Apress - P.11