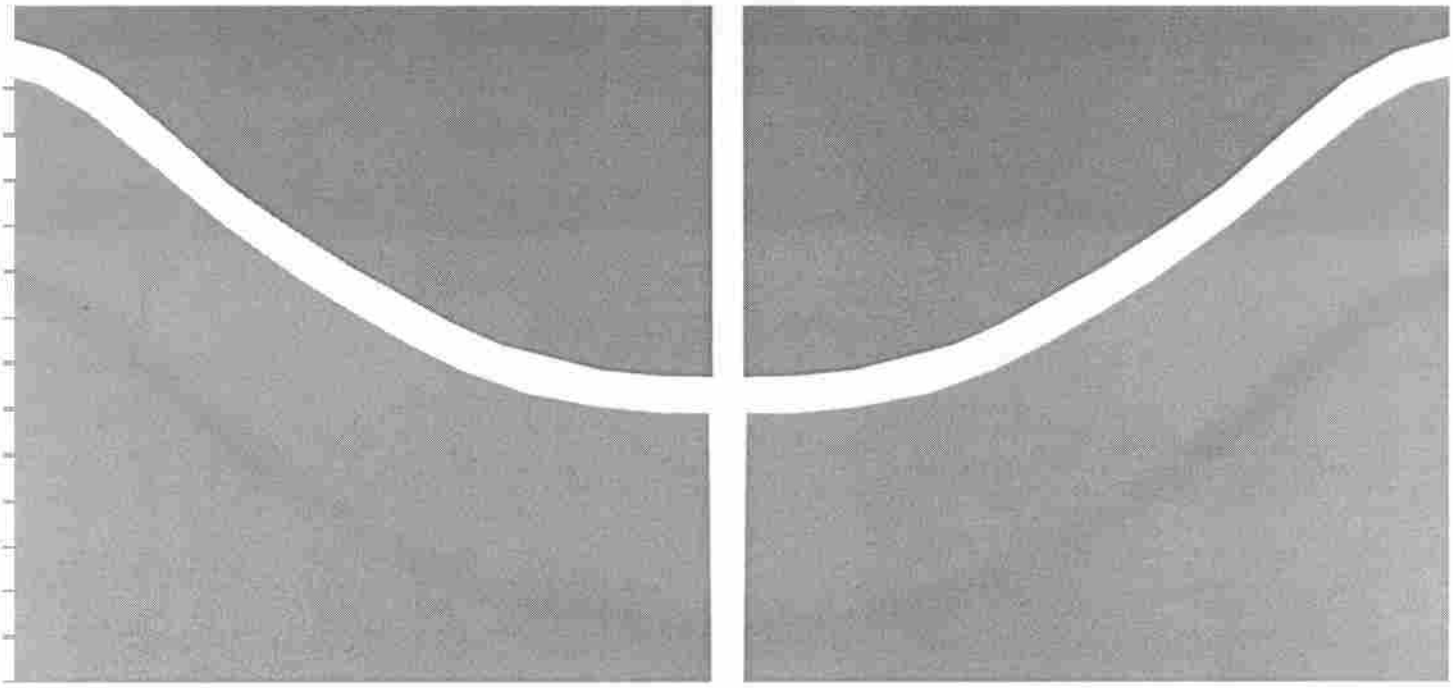


IMPLEMENTAÇÃO DE UM SISTEMA SIEM
ESTUDO DE CASO

JOÃO PAULO SOUSA DA CONCEIÇÃO

MONOGRAFIA DE ESPECIALIZAÇÃO 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

IMPLEMENTAÇÃO DE UM SISTEMA SIEM

ESTUDO DE CASO

JOÃO PAULO SOUSA DA CONCEIÇÃO

ORIENTADORA: PROFESSORA ELIANE CARNEIRO SOARES

MONOGRAFIA DE ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PUBLICAÇÃO: UnBLabRedes.MFE.047/2017

BRASÍLIA/DF: JUNHO - 2017.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

IMPLEMENTAÇÃO DE UM SISTEMA SIEM
ESTUDO DE CASO

JOÃO PAULO SOUSA DA CONCEIÇÃO

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO TÍTULO DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____

Eliane Carneiro Soares, **Mestre, SEEDF (ORIENTADORA).**

_____

Rafael Timóteo de Sousa Júnior, **Dr., UnB (EXAMINADOR INTERNO)**

_____

Robson de Oliveira Albuquerque, **Dr., ABIN (EXAMINADOR EXTERNO)**

BRASÍLIA - DF, 23 DE JUNHO DE 2017.

FICHA CATALOGRÁFICA

CONCEIÇÃO, JOÃO PAULO SOUSA DA
Implementação de um sistema SIEM – Estudo de Caso [Distrito Federal] 2017.
Xiii, 64p., 210 x 297mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.

1. Gerenciamento de Eventos
2. Correlacionamento de eventos
3. Ataques na internet
4. Segurança da Informação
5. Sistema de Detecção de Intrusão
I. ENE/FT/UnB
II. Título (série)

CESSÃO DE DIREITOS

AUTOR: João Paulo Sousa da Conceição

TÍTULO DO MONOGRAFIA: Implementação de um sistema SIEM – Estudo de Caso.

TÍTULO / ANO: Especialista / 2017

João Paulo Sousa da Conceição

João Paulo Sousa da Conceição
QSC19 Ch 26 Conjunto A-1 Lote 11B Taguatinga Sul
CEP: 72.017-287 - Brasília - DF
Tel. +55 - 61 - 9 8176-0044 / joaopauloyhwh@gmail.com

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus por ser a base da minha vida, mentor de todas as coisas.

A minha esposa, Tatiana, por todo apoio e paciência.

Ao meu filho, Paulo Elian, pela compreensão da ausência.

Aos meus pais, Eduardo e Graça, pela criação e por tudo que fizeram por mim.

Aos meus queridos irmãos, Eduardo Sousa, Ana Paula e Glaucia, e todos os demais familiares.

Ao amigo Clayton Lobato pela ajuda, dicas e críticas construtivas.

A minha Orientadora Professora Eliane, e a todos os outros amigos do peito.

Meu muito obrigado a todos.

RESUMO

IMPLEMENTAÇÃO DE UM SISTEMA SIEM – ESTUDO DE CASO

Autor: João Paulo Sousa da Conceição

Orientador: Professora Eliane Carneiro Soares

Programa de Pós-graduação em Engenharia Elétrica

Brasília, 23 de junho de 2017.

Hoje, as informações são muito valiosas para as organizações. Sem o devido cuidado, essas informações podem ser roubadas, apagadas ou modificadas. Por conta disso, são necessários mecanismos que salvaguardem as informações, e que ainda, possam gerar alertas caso aconteça alguma anomalia.

Sabendo da importância da segurança da informação, o presente estudo pretende mostrar quais são os pontos importantes na implementação de um sistema SIEM, bem como suas características e funcionamento. Para que, desta forma, os resultados de sua implementação contribuam de forma eficaz no processo de mitigação das ameaças e o gerenciamento centralizado de eventos de segurança da informação na infraestrutura de uma rede corporativa.

O estudo de caso será desenvolvido em uma arquitetura virtualizada, na qual serão utilizados diversos sistemas operacionais para testes – separando seguimentos de redes com DMZ, integrando soluções de segurança de Firewall proprietários e *opensource* ao SIEM. E também, explorando vulnerabilidades em sistemas e aplicações para gerar eventos que serão tratados pelo SIEM.

ABSTRACT

IMPLEMENTATION OF A SIEM SYSTEM - CASE STUDY

Author: João Paulo Sousa da Conceição

Supervisor: Professora Eliane Carneiro Soares

Programa de Pós-graduação em Engenharia Elétrica

Brasília, June 2017

Today, information is very valuable to organizations. Without due care,this information can be stolen, deleted or modified. Because of this,mechanisms that safeguard information, and which,should anomalies occur.

Knowing the importance of information security, the present study intends to show whichare important points in the implementation of an SIEM system, as well as itscharacteristics and operation So that, in this way, the results of its implementationcontribute effectively to the process of threat mitigation and management.centralized information security events in the infrastructure of a corporate network.The case study will be developed in a virtualized architecture, in which various operating systems for testing - separating network segments with DMZ,integrating proprietary and opensource Firewall security solutions to SIEM. And also,exploiting vulnerabilities in systems and applications to generate events that will be treatedby SIEM.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ACRÔNIMOS

IDS	Intrusion Detection System
SIEM	Security information and events management
PCI DSS	Payment Card Industry Data Security Standard
HIPAA	Health Insurance Portability and Accountability Act
SOX	Lei Sarbanes-Oxley
TI	Tecnologia da Informação
FISMA	Federal Information Security Management
ISO	International Organization for Standardization
OSSIM	Segurança da informação, Monitoramento, Redes

1 INTRODUÇÃO

A informação tornou-se o bem mais importante das organizações. Como citado por Nakamura: "como conhecimento é o principal capital das organizações, protegê-lo significa proteger o seu próprio negócio. Assim, a segurança passa a fazer parte do processo de negócios das organizações" (NAKAMURA; GEUS, 2007, p. 50). Percebe-se a informação como parte do negócio, e protegê-la tem sido um dos desafios das instituições após o surgimento das redes de computadores e, consequentemente, da internet.

A evolução dos ataques cibernéticos tem aumentando consideravelmente. Tal realidade tem por consequência a existência de ambientes de redes cada vez mais complexos em relação ao gerenciamento destes.

Preocupados em proteger suas informações, empresas, órgãos governamentais, centros de pesquisas, universidades, entre outros, dispõem de métodos, técnicas, ferramentas e profissionais para resguardar seus ativos, bem como mantê-lo o mais seguro possível e distante dos invasores.

No caso das tecnologias e ferramentas disponíveis, o mercado oferece uma imensa quantidade de proteção que vai desde firewall dedicado, passando por sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS), Proxys, servidores de antivírus, e entre outros. Com isso, as empresas e instituições vão adquirindo soluções e incorporando-as à sua infraestrutura. Porém, cada uma dessas ferramentas tem a sua própria interface de gerenciamento, apresentação de dados e relatórios. O analista de segurança e o administrador de sistemas precisam acessar essas soluções para saber o que está acontecendo em sua rede, e isto requer tempo e não oferece uma visão global da real situação.

Neste trabalho, propõe-se apresentar os conceitos que envolvem o sistema de gerenciamento de eventos e seus alertas, que vão desde uma simples verificação de um evento até um desastre de indisponibilidade na organização. Será apresentado como o processo de gerenciamento de eventos funciona e como este pode ajudar a identificar, coletar as informações necessárias, padronizar as informações, aplicar as regras de correlação, monitorar e, por fim, classificar qualquer atividade; mostrando, assim, as possíveis ocorrências de segurança.

1.1 JUSTIFICATIVA

No que se refere às questões da segurança da informação, é importante coletar e correlacionar as diferentes atividades que estão acontecendo na infraestrutura da rede. Tal informação é fundamental para se identificar, priorizar e responder à ataques cibernéticos, violações de políticas e conformidades.

Para isto, as instituições estão dispostas a investir cada vez mais para que estas informações sejam protegidas e, com isso, fazer crescer o mercado de segurança da informação. Mais à frente neste trabalho, será apresentado como a indústria de segurança da informação teve investimentos gigantescos. E, assim, a pesquisa sobre novas tecnologias ganhou força, e ganhará ainda mais, fazendo surgir diversas tecnologias.

Contudo, este trabalho está fundamentado em explicar umas das tecnologias empregadas atualmente. E com a eficácia que será comprovada ao decorrer desta dissertação, este trabalho torna-se relevante, pois não apenas serão apresentados conceitos de segurança relevantes, como também explicaremos e aplicaremos uma ferramenta Open Source: AlienVault OSSIM. Esta ferramenta serve como alternativa em relação às grandes soluções proprietárias de mercado que as grandes empresas e/ou organizações podem usar para garantirem seu isolamento de falhas de segurança, tanto em tentativas de acesso indevido de rede, como também em dados de sistemas internos da instituição.

1.2 OBJETIVO GERAL

O objetivo desse trabalho é implementar o SIEM OSSIM do acrônimo - *Open Source Security Information Manegemant* – em um laboratório de teste, com planejamento em cada etapa do processo, para que o mesmo seja analisado, visando prover as vantagens e desvantagens da solução.

1.3 OBJETIVOS ESPECÍFICOS

- Criar fluxo baseado em etapas, onde os eventos serão direcionados dentro do processo e como esses eventos serão correlacionados;
- Apresentar a arquitetura da ferramenta utilizada na implementação do sistema SIEM;
- Simular o mecanismo proposto gerando eventos de segurança por meio de um laboratório, e ao final do processo, indicar qual tipo, a prioridade, o correlacionamento e o tratamento adequado de cada evento;

1.4 METODOLOGIA DE PESQUISA

Para facilitar o entendimento do trabalho, a metodologia de pesquisa proposta foi dividida em fases. A saber: fase 1, fase 2 e fase 3. A divisão em fases busca o aprofundamento do estudo relacionado ao tema e problema proposto neste trabalho, identificando os assuntos abordados pela comunidade acadêmica atualmente e as métricas a serem identificadas para fornecer um sistema de gerenciamento de eventos de segurança.

Fase 1: f azer uma pesquisa bibliográfica, levando em conta a importância de ser um mecanismo que permite a identificação, leitura e análise de artigos relevantes ao desenvolvimento do trabalho. Tais artigos e documentos analisados e registrados nessa fase, servem para acrescentar a dinâmica no trabalho e deixá-lo mais produtivo.

Fase 2: explorar informações sobre os problemas relacionados ao gerenciamento de eventos e segurança da informação, identificando as soluções conceituais e práticas.

Fase 3: simular e implementar o sistema SIEM proposto, analisando os resultados. Nesta fase serão efetuadas as conclusões e identificação das contribuições.

1.5 CONTRIBUIÇÕES DO TRABALHO

Busca-se com este trabalho as seguintes contribuições:

- Apresentação do estado da arte do gerenciamento de eventos de segurança, levando em consideração aspectos que são importantes para definição de segurança da informação;
- Apresentação de uma proposta de um mecanismo de gerenciamento de eventos de segurança, permitindo que seja possível a validação das informações e os alertas necessários;
- Simulação da ferramenta proposta, aplicando a solução proposta gerando os alertas de detecção de intrusão em sistemas;
- Fortalecimento da confiança na tomada de decisões, correlacionando-o com os eventos de segurança.

1.6 ORGANIZAÇÃO DO TRABALHO

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

No próximo capítulo deste trabalho, serão apresentadas as conformidades adotadas por diversas instituições em torno da segurança, mostrando diversos mecanismos legais ou convenções adotadas por diversos setores para garantir níveis de segurança aceitáveis em seus setores.

Continuamos abordando uma das primeiras tentativas das organizações em se defenderem de acessos indevidos aos seus sistemas, os sistemas de detecção de intrusão (IDS). Mostrando alguns dados históricos de quando estes sistemas foram usados pela primeira vez, abordaremos também os seus conceitos e desafios enfrentados por estas tecnologias.

Finalizado o tópico, entramos no conteúdo principal deste trabalho: os gerenciadores de eventos e informações de segurança (SIEM). Neste tópico, mostraremos os conceitos em torno destes gerenciadores, e a anatomia de tais sistemas em detalhes, fazendo com que o leitor entenda o que é um SIEM e como ele funciona. E finalizamos este capítulo com uma pequena conclusão para que possamos passar ao próximo capítulo.

No capítulo seguinte, abordaremos a instalação e configuração da ferramenta escolhida na implementação do nosso SIEM, tentaremos mostrar detalhadamente as operações para que a ferramenta esteja instalada e funcione corretamente.

Finalizaremos este trabalho mostrando os resultados da implementação do SIEM configurado no capítulo acima citado, mostrando gráficos e comparativos, para demonstrar a eficiência e eficácia destas ferramentas no processo de detecção de acessos não autorizados e possíveis falhas de segurança na rede ou sistemas internos das instituições.

2 REVISÃO SOBRE ATAQUES DE REDES E ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

Este capítulo tem como foco a apresentação do histórico do surgimento das redes de computadores e, com isto, mostrar suas fragilidades de segurança devido a popularização, aumento do volume de dados trafegados nestas redes e, ainda, apresentar algumas das soluções empregadas para aumentar a segurança dos dados. Com intuito de abranger o tema de forma sucinta, dividimos este capítulo em múltiplos tópicos.

Na seção 2.1, apresentaremos alguns pontos relacionados à rede de computadores e segurança da informação. Na sessão 2.2, serão apresentados os ataques na internet. Na sessão 2.3, apresentaremos recomendações de conformidade. Na sessão 2.4, presentaremos o conceito de Sistema de Detecção de Intrusão. Na sessão 2.5, mostraremos o gerenciamento de eventos e informações de segurança (SIEM). E na sessão 2.6, os problemas relacionados ao SIEM.

2.1 REDES DE COMPUTADORES E A SEGURANÇA DA INFORMAÇÃO

Desde os tempos remotos, a informação é considera um dos bens mais preciosos da organização humana, como citado por Nakamura e Geus: "como conhecimento é o principal capital das organizações, protegê-lo significa proteger o seu próprio negócio. Assim a segurança passa a fazer parte do processo de negócios das organizações" (2007, p. 50). Após o surgimento da internet, onde a informação circula cada vez mais rápido, proteger este bem tão valioso é essencial para as empresas.

Segundo o dicionário Aurélio, a segurança é um conjunto de dados acerca de alguém ou algo. Já para a ABNT (Associação Brasileira de Normas Técnicas), associação responsável por criar normas que regem a implantação de sistemas de gerenciamento de segurança, explica que "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio". A partir desta afirmação, notamos que a proteção da informação é, na verdade, a proteção da própria empresa.

A Figura 1 mostra os investimentos em segurança desde 2012 até o ano de 2015 na América Latina, apresentado pela empresa de consultoria Frost & Sullivan, com apoio da Cisco.

Figura 1 - Mercado de Segurança da informação na América Latina.

Fonte: Frost & Sullivan (2015).

Na Figura 1 pode-se notar que até o ano de 2015 os investimentos em segurança da informação ultrapassaram um bilhão de dólares em investimentos, sendo que aproximadamente 50% deste valor foi investido em segurança, mostrando que a segurança é uma das partes fundamentas das instituições.

A Figura 2 mostra um gráfico que apresenta o valor investido nos maiores mercados da América Latina.

Figura 2 - Investimentos em TI por região na América Latina.

Fonte: Frost & Sullivan (2015).

Um dado importante apresentado no gráfico acima é que o Brasil é um dos países que mais investe em segurança da informação. Na América Latina, o Brasil foi responsável por 43,7% dos investimentos em Segurança da Informação no ano de 2012, em função da extensão territorial e da maior maturidade do mercado com empresas globais atuando diretamente no país" (FROST; SULLIVAN, 2015).

Como pode ser notado, as empresas estão investindo muito em segurança e esses investimentos têm aumentando cada vez mais, pois existe preocupação das organizações em manter as informações seguras e evitar possíveis problemas como o vazamento e a perda das informações. Embora seja preciso um melhor investimento na capacitação de profissionais em segurança da informação, como apresentado em um recente estudo do (ISC)² durante o Security Congress Latin America 2017.

2.2 ATAQUES NA INTERNET

Os ataques que ocorrem na internet têm sempre um motivo específico, seja por simples curiosidade ou para acessar os dados de uma empresa concorrente causando danos. Como demonstrado pela cartilha do CERT.BR (2017), existem diversos motivos para um ataque:

> - **Demonstração de poder:** o atacante necessita acessar determinada informação de um site para saber se é capaz de tal ataque, causando ou não dano para empresa alvo.
> - **Prestígio:** neste ponto o atacante busca reconhecimento de outros atacantes, mostrando suas habilidades através do roubo de informações de uma empresa ou ao desfigurar um site e ainda ser o primeiro a realizar um ataque a um alvo determinado.
> - **Motivações financeiras:** devido estes ataques serem vastos e causarem dano às organizações, os atacantes tentam formas de conseguir dinheiro através das falhas nos sistemas ou aplicando golpes nos usuários que não tem conhecimento básico de segurança.
> - **Motivações comerciais:** como há competitividade entre as organizações, algumas dessas tentativas tem o poder de tornar inacessível determinada aplicação ou site, causando a desconfiança dos usuários comprometendo a reputação da empresa.
>
> Por esses motivos, os ataques na internet evoluíram e existem vários tipos de ataques. Os ataques apresentados abaixo são os mais utilizados pelos hackers para obter informações de forma criminosa, indisponibilizar um serviço ou aplicação que esteja apontada para internet, danificar um sistema ou até mesmo chantagear um empresário, o qual não deseja que a informação seja repassada para concorrentes.
>
> - **Ataque de força bruta:** é a maneira mais utilizada para a quebra de senha de algum servidor. Normalmente este ataque busca tentar combinações realizadas por tentativa e erros de senhas até que seja concedido acesso ao servidor. (CERT.BR, 2017)

Existem muitas ferramentas que fazem este tipo de tentativa, apesar de poderem ser executadas manualmente. O CERT.BR mostra que há várias formas de adivinhação de senhas, buscam em dicionários, lista de palavras mais comuns, substituição de caracteres por caracteres

especiais, sequências numéricas e de teclado, informações pessoais coletadas na internet ou através de engenharia social.

- **Ataque de escaneamento de porta:** o ataque de escaneamento de porta é usado para buscar informações sobre determinado servidor sabendo as portas abertas. Normalmente o escaneamento de porta é utilizado pela equipe de segurança para mitigar os possíveis ataques a determinado sistema (SZYMANSKY, 2012).

  O escaneamento de portas detecta os serviços abertos e a quantidade de informações que podem ser extraídas utilizando as ferramentas adequadas. Os sistemas que são acessíveis via web vão utilizar as portas, sendo que estas ficam abertas. Porém, é necessário ter um controle dos usuários autorizados às portas abertas e negar o acesso para as portas fechadas (CHRISTOPHER, 2001).

- **Ataque de negação de serviço:** negação de serviço é um ataque que utiliza a rede para inviabilizar o uso de uma aplicação ou tentar deixá-la fora do ar até os serviços voltarem a serem estabelecidos. Os ataques de negação de serviços começaram a ocorrer por volta de 1989 e atualmente o grande problema é que existe uma variedade enorme de formas, as quais requerem pouco recurso, causando a indisponibilidade dos serviços e, muitas vezes, gerando danos financeiros às companhias. Existem diversas técnicas de ataques de negação de serviço, como Ataque de Inundação Volumétrica, Inundação HTTP, Renegociação SSL, Inundação no mecanismo de Pesquisa, DNS reflexivo, ampliação de pesquisa DNS (SEPE, 2015).

As organizações necessitam proteger suas informações por conta dos danos que os ataques podem causar. Há várias formas de proteger as informações e uma delas é atendendo às conformidades regulatórias que tratam sobre padrões de segurança em determinados setores, sejam eles financeiros ou hospitalares. As conformidades oferecerão o direcionamento do que uma organização precisa para se proteger.

2.3 CONFORMIDADE COM AS REGULAMENTAÇÕES.

Pensando na perda de informações, recursos e dinheiro geradas pelos ataques e vulnerabilidades dos sistemas, muitas instituições decidiram criar padrões de segurança observando políticas de auditoria de conformidade regulamentar, sendo um requisito para todas as organizações. Normas como PCI DSS, FISMA, SOX, ISO 27001 e HIPAA exigem que as organizações monitorem sua rede, garantam um alto nível de segurança para os ativos e

forneçam relatórios de conformidade para os auditores quando necessário (ZOHO, 2015). Por esses motivos, é necessário apresentar cada uma dessas conformidades regulatórias.

Payment Card Industry Data Security Standard (PCI DSS): foi criada no intuito de proteger o setor bancário baseado nos pagamentos efetuados por catões de crédito. Sendo obrigatório para todas as instituições que lidam com crédito. Empresas como Visa, Master Card e American Express utilizam esse padrão. Devido ao aumento das ameaças que surgem todos os dias, as empresas que prestam esse tipo de serviço estão mais atentas e seguem cada vez mais esses padrões, pois o que move a instituição é a credibilidade. E caso as informações de seus clientes fossem roubadas seria desastroso para a reputação (ZOHO, 2015).

Figura 3 - PCI DSS 12 áreas de atuação.

Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível

Construir e manter uma rede segura	1. Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão 2. Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do portador do cartão	3. Proteger os dados armazenados do titular do cartão 4. Criptografar a transmissão dos dados do titular do cartão em redes abertas e públicas
Manter um programa de gerenciamento de vulnerabilidades	5. Usar e atualizar regularmente o software ou programas antivírus 6. Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas de controle de acesso rigorosas	7. Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio 8. Atribuir uma identidade exclusiva para cada pessoa que tenha acesso ao computador 9. Restringir o acesso físico aos dados do titular do cartão
Monitorar e testar as redes regularmente	10. Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão 11. Testar regularmente os sistemas e processos de segurança
Manter uma política de segurança de informações	12. Manter uma política que aborde a segurança das informações para todas as equipes.

Fonte: Conselho de Padrões de Segurança LLC do PCI (2010).

O PCI DSS atua em 12 áreas diferentes para melhorar a segurança das instituições. Cada área tem tópicos específicos que mostram o que deve ser feito para atender todas as regulamentações necessárias. Estas áreas podem ser aproveitadas e implementadas em organizações que não são da área bancária.

Lei Sarbanes-Oxley (SOX): foi criada para tratar os casos de fraudes em empresas de capital aberto. Sancionada pelo presidente George W. Bush, tem o intuito de evitar escândalos como os que que aconteceram com as empresas WorldCom e Tyco. Souza (2004), declara:

> Desta forma a lei Sarbanes-Oxley, um pacote de reformas dedicado a ampliar a responsabilidade dos executivos, aumentar a transparência, assegurar mais independência ao trabalho dos auditores, introduzir novas regras para o trabalho desses profissionais e reduzir os conflitos de interesses que envolvem analistas de investimentos entra para ampliar substancialmente as penalidades associadas a fraudes e crimes do colarinho branco.

Federal Information Security Management Act (FISMA): lei criada visando a segurança da informação para as agências federais. Este visa garantir a segurança para os sistemas de informação e que suportam as operações e ativos das agências. A FISMA exige que cada agência deve desenvolver, documentar e implementar um programa para toda agência garantindo a segurança das informações, dos ativos, dos fornecedores, entre outras fontes que complementam cada agência (NIST, 2002). A *National Institute of Standards and Technology* (NIST) diz que um programa de segurança da informação efetivo baseado no FISMA:

- Categorizar a informação a ser protegida;
- Selecionar controles mínimos de referência;
- Limitar controles usando um procedimento de avaliação de risco;
- Documentar os controles no plano de segurança dos sistemas;
- Implementar controles de segurança em sistemas de informação;
- Avaliar a eficácia dos controles de segurança, uma vez que foram implementadas;
- Risco de nível da agência para a missão ou caso do negócio;
- Autorizar o sistema de informação para processamento;
- Monitorar os controles de segurança em uma base contínua.

International Organization for Standardization 27001: é um padrão internacional que visa a gestão da segurança da informação. Desenvolvida incialmente pelo governo britânico. Esta norma tem como principal objetivo aplicar as práticas relacionado à Gestão de Segurança da Informação. Esta norma é independente de fabricante, trazendo um modelo genérico, estabelecendo somente processos e procedimentos baseando na realidade de cada organização. A ideia da norma ISO 27001 é desenvolver um modelo que estabelece, implementa, operacionaliza, monitora e revisa um Sistema de Gestão de Segurança da Informação (SGSI) (INTEGRITY, 2015).

Health Insurance Portability and Accountability Act (HIPAA): a lei de privacidade HIPAA busca a proteção das informações de saúde dos pacientes, o qual têm uma série de direitos relacionados a essas informações. A lei especifica várias diretrizes para salvaguarda administrativa, física e técnica para proteger a informação de modo a assegurar a

confidencialidade, integridade e disponibilidade das informações de saúde (HHS, 2015).

Para que as conformidades regulatórias sejam colocadas em prática, é interessante tratar algumas ferramentas que podem auxiliar a cumprir, não todas, mas alguns pontos específicos de cada regulamento como o IDS e o SIEM.

2.4 SISTEMAS DE DETECÇÃO DE INTRUSÃO

Como citado no capítulo anterior, a informação é o bem mais valioso da instituição. Logo, este bem tão valioso está sempre sujeito à cobiça de outras instituições ou agentes maliciosos que queiram esta informação para fins próprios. Com o surgimento das redes de computador, as instituições começaram a perceber maior dificuldade em controlar o acesso aos dados sigilosos. E no ano de 1987, surge um novo termo para os sistemas que detectam este tipo de acesso, seu nome é *Intrusion Detection System* (IDS), em português: Sistema de Detecção de Intrusão.

A primeira menção a este tipo de sistema foi no ano acima citado, em um artigo cuja autoria é de Denning, com título "*An Intrusion-Detection Model*". Neste artigo, o autor, com base nas tecnologias da época, justifica a existência de tais sistemas, os quais em "tempo real", monitoram as vulnerabilidades do sistema e apresentavam algumas soluções que tais sistemas pretendiam resolver; com relação à ataques e abuso dos privilégios por parte de usuários (DENNING, 1987).

Segundo Barber e Mell (2001), IDS são sistemas de *hardware* ou *software* que possam automatizar o processo de monitoramento de eventos de segurança gerados pela rede de computadores e sistemas informatizados, ajudando a encontrar e analisar problemas de segurança (BARBER; MELL, 2001). Como pode-se notar, desde 1987, o conceito em torno do IDS não mudou drasticamente, apenas apontando pequenas mudanças. Pela definição em 2009 por Lu Hong, que define o IDS da mesma forma que Barber e Mell, e com a evolução das tecnologias, mostra como evitar uso indevido de usuários internos em redes de computadores e sistemas da instituição (HONG, 2009).

Nota-se que a evolução do conceito foi mínima com o passar dos anos, mas este tipo de conceito gerou uma subdivisão destes sistemas. São eles: *Host-Based* IDS (HIDS), o *Network* IDS (NIDS), sendo que este último engloba tanto as redes cabeadas como as redes *wireless*. A *Information Assurance Tecnology Analysis Center* (IATAC), em um relatório escrito por Tyler e Wu (2009), define o que cada uma destes IDS deve analisar, sendo que

os HIDS analisarão configurações específicas de sistemas, como controle de acesso a um determinado *software* ou a política de segurança, este nível estando nas máquinas locais. Já os NIDS são colocados pelos autores como responsáveis pelo nível de segurança na camada *Open System Interconnection* (OSI) verificando-se a finalidades do tráfego da rede e fazendo análise de atividades suspeitas da rede (TYLER; WU, 2009).

Mesmo com o desenvolvimento deste tipo de tecnologia, o desafio gerado com a difusão do uso dos computadores pessoais e o acesso à internet acabou por trazer um grande volume de dados; acarretando, com isso, a geração de falso-positivos como citado por Silva (2011):

> Um destes desafios de implementação é conseguir fazer a gestão dos grandes volumes de tráfego que são gerados nos dias de hoje numa organização. Este fato acaba por remeter para um outro desafio relacionado com os falso-positivos e consequentemente com aumento de trabalho do ponto de vista dos administradores (SILVA, 2011).

Como citado acima, falso-positivos podem gerar um volume desnecessário dos analistas envolvidos no processo de garantir a segurança da infraestrutura da empresa e consequentemente possibilitando acessos indevidos à informações relevantes para a instituição. Mas este volume de informação, normalizado e armazenado de maneira correta, pode ser correlacionados para gerar informações úteis, poupando esforço e diminuindo a carga de trabalho dos administradores e analistas.

A implementação de ferramentas vai dar a estrutura necessária sobre o conceito de SIEM. Contudo, é necessário conhecer a anatomia de cada ferramenta para que sejam avaliadas de acordo com seu intuito. As ferramentas apresentadas vão desde um agente instalado em um servidor como *Host Intrusion Detection System* (HIDS) até o tratamento dessas informações em tempo real utilizando um sistema via web.

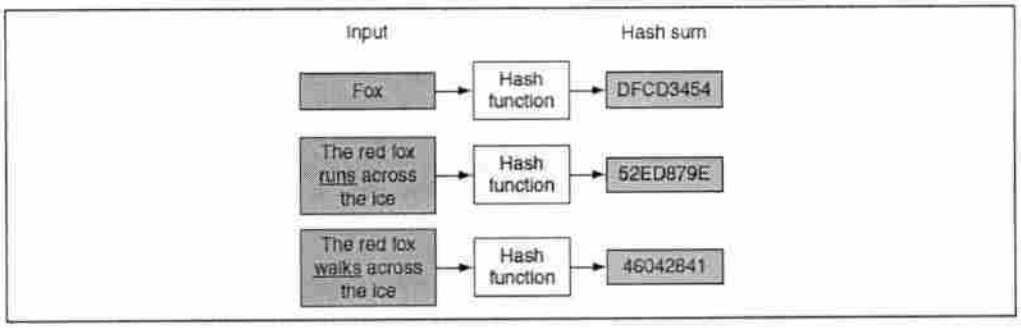
Segundo Nakamuda e Geus (2010), um sistema de detecção de intrusão baseado em hosts (HIDS) monitora os sistemas através de informações fornecidas pelos logs e agentes de auditoria. Um Sistema de Detecção de Intrusão, além disso, pode checar a integridades dos arquivos, monitorar os registros do sistema, realizar a análise de logs, detecção de rootkit, alertas em tempo real e ter respostas ativas em caso de um alarme seja disparado (MICRO, 2015).

Checagem da integridade de arquivos: com a verificação de integridade dos arquivos, o hids pode saber se os arquivos foram alterados e gerar um hash para cada modificação no sistema. Um hash é uma função criptográfica da mensagem através de algoritmos complexos,

e sempre vai gerar uma saída de tamanho fixo (PISA, 2012).

A Figura 4 mostra como toda vez que é modificado um arquivo, um novo hash é gerado comparando com o antigo hash. Caso esse hash não for igual, o hids vai gerar um alerta avisando que aquele arquivo do sistema foi alterado.

Figura 4 -Exemplo de um criptográfico hash gerado a partir de entrada diferente.



Fonte: Cid (2008).

Monitoramento do Sistema de Registro: segundo Cid (2008), normalmente em sistemas Microsoft Windows, o sistema de registro é um diretório no qual ficam todas as diretivas, como: lista de hardware e software de usuários, configuração do sistema operacional, dos usuários e grupos. Então, um HIDS pode detectar se um registro foi modificado e alterado com uma intenção maliciosa.

Detecção de Rootkits: rootkit são ferramentas com intuito de ocultar sua presença em sistemas operacionais, deixando brechas para que invasores tenham domínio sobre o sistema. Alguns desses rootkits fazem parte de worms e ferramentas. Ficando meses sem ser descoberto (MURILO; STEDING-JESSEN, 2011). Um rootkit instalado pode se esconder em serviços, processos, portas, arquivos e diretórios.

Resposta ativa: uma resposta ativa executa automaticamente um comando ou resposta específica para determinada situação. O uso de respostas ativas é interessante quando suas regras estão bem definidas, caso o contrário, um atacante pode provocar um ataque que simule uma situação gerando um falso positivo e assim, bloqueia o acesso ao serviço (CID, 2008).

No próximo capítulo, serão apresentados sistemas que integra o IDS com a geração mais precisa de informações por meio de correlacionamentos e gerenciamento de eventos baseados na estrutura SIEM.

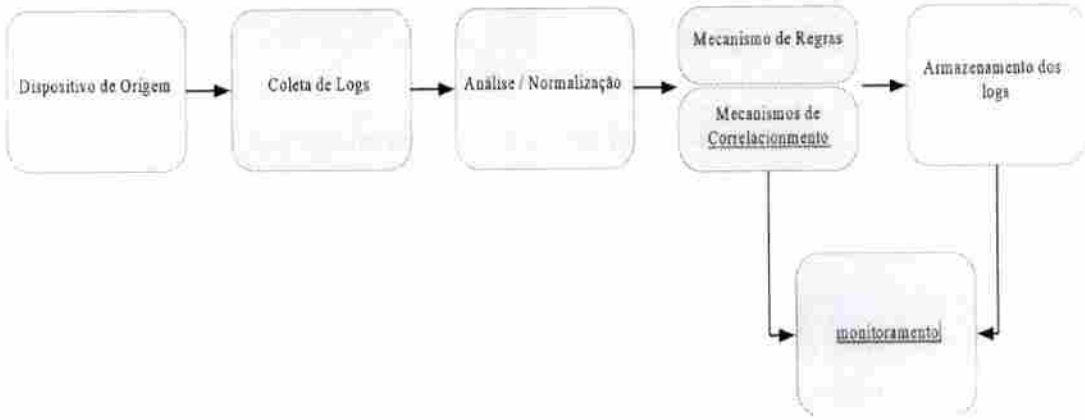
2.5 SISTEMA DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA

Nesta sessão será abordado o SIEM (*Security Information and Event Management*), mostrando os conceitos básicos sobre o que é um SIEM, as principais utilizações deste gerenciador, seus componentes básicos e seu funcionamento.

Um SIEM é uma estrutura que contém várias partes, e cada uma tem uma função específica e trabalha independentemente da outra. Porém, sem essas partes trabalhando em conjunto, o SIEM não funcionará corretamente. O SIEM pode ser divido em seis partes. Sendo elas: o dispositivo de origem; análise/normalização dos registros; mecanismos de regras e correlacionamento; armazenamento de eventos; recuperação para futuras análises.

A primeira parte de um SIEM irá descrever como os dispositivos de origem passarão as informações para os coletores de logs. Depois, essas informações coletadas passarão por um tratamento no qual serão analisados e normalizados; após essa etapa, os logs passarão pelos mecanismos de regras e correlacionamento, faltando somente serem armazenados específicos. E, por último, ocorrerá o monitoramento em tempo real ou dos logs armazenados.

Figura 5 - Funcionamento básico de um SIEM.



Fonte: Adaptado Miller, et al. (2010).

2.5.1 Dispositivo de Origem

O dispositivo de origem é onde são gerados os volumes de informações para o SIEM, as pessoas não têm noção de quanto informações são geradas por esses dispositivos. Então, todas as informações ao saírem do computador utilizado pelo usuário, vai gerarão uma

informação que passa por vários outros dispositivos, como switches, roteadores, firewalls, entre outros (MILLER, 2010).

As informações que alimentam inicialmente um SIEM vêm de um dispositivo de origem, e esse dispositivo pode ser um switch, roteador, aplicação ou qualquer outra coisa que gere informação para o SIEM. Por isso, é importante que quem administra um SIEM tem que conhecer bastante sua infraestrutura. Para um SIEM, esses registros serão armazenados e processados, se um SIEM não tem informações de um dispositivo de origem, ele não servirá para nada, pois uma de suas funções é trabalhar em cima da informação que vem de algum lugar ou chega até ele (MILLER, 2010).

Sistemas operacionais: os sistemas operacionais em sua maioria, como Linux, UNIX, AIX, Mac OS, Windows, entre outros diferentes tipos, os quais são utilizados pelas empresas hoje em dia, são muito extensos. Porém, mesmo sendo diferentes, todos esses sistemas operacionais geram logs, que são informações que mostram estatísticas do sistema, como quem acessou o sistema, quem executou determinada rotina no sistema, quem utilizou aplicativo, podendo ser registrado tudo que o que foi realizado. Porém, a maioria das pessoas desconhecem que seu sistema atua dessa forma. Todos esses logs podem ser muito úteis ao realizar uma resposta a incidentes de uma atividade de segurança, diagnóstico de problemas e erros de configuração (MILLER, 2010).

Sistemas embarcados: a maioria dos equipamentos são sistemas que tem seu acesso restrito, nos quais os administradores podem somente administrá-los sem ter acesso direto ao sistema operacional do equipamento. Normalmente, usam uma interface web ou linha de comando; porém, os acessos às modificações internas do sistema para alterar a forma com que ele trabalha, é impossível em vias normais. Exemplo deste tipo de sistemas são roteadores e switches, podendo ser sistemas operacionais com acesso restrito. Os dispositivos que atuam dessa forma armazenam seus registros em formato de logs, e estes são enviados em formato de syslog compreensível por maioria dos SIEM (MILLER, 2010).

Aplicações: as aplicações que rodam em cima de um sistema operacional podem ser variadas, desde um *Deny of Service* (DNS), *Dynamic Host Configuration Protocol* (DHCP), aplicações web, banco de dados, serviços de e-mail entre outros tipos de sistemas e aplicações. O importante é saber se esses logs são úteis ou não, e se precisam estar em conformidade com alguma lei. Um grande problema ao buscar esses logs é que algumas aplicações e sistemas podem gerar logs que não são padrões, o que dificulta o processo de trazer esses logs para um

SIEM corretamente (MILLER, 2010).

Determinar o que é necessário e o que o SIEM precisa: é necessário saber como está o ambiente e quais são as informações dos logs que administrador deseja coletar. O interessante é coletar informações importantes para melhor proteger o ambiente, ajudando a diagnosticar problemas que podem acontecer na rede. A necessidade de coletar os logs é devida as conformidades com os padrões de PCI e SOX, as quais exigem que os logs devem ficar salvaguardados por um período específico de tempo (MILLER, 2010).

Nem todos os logs são necessários serem coletados. Contrariamente o pensamento de vários profissionais de segurança, que acreditam que todos os registros são necessários. Porém, essa forma de pensar causa alguns problemas, pois o SIEM não conseguirá processar todo tipo de informação mantendo um equilíbrio do que é necessário para ser analisado. Com a capacidade do sistema, o analista de segurança tem a obrigação de saber o que será analisado pelo SIEM e quais são os registros de maior significância para o ambiente com o objetivo de maximizar a eficácia do SIEM implementado. A razão para analisar os logs no SIEM é porque, incialmente, o SIEM pode ser sobrecarregado com informações de incidentes supérfluos e tornar os incidentes difíceis de detectar problemas ou incidentes de segurança na rede ou servidor. Para que o SIEM funcione é preciso levar em considerações quais os recursos necessários como Miller (2010) descrever:

> - Qual a prioridade do dispositivo de origem, pois será é interessante porque dependendo da quantidade de logs o SIEM não conseguirá cobrir todos.
> - Qual o tamanho dos logs que serão armazenados e por quanto tempo, pois determinará quanto de espaço será necessário para armazenar por um período.
> - Qual o custo disso para rede, pois é necessário saber como está a infraestrutura entre o dispositivo de origem e o SIEM.
> - E por último qual a necessidade de manter um sistema em tempo real, talvez algumas aplicações não são necessárias para esse tipo de atuação porque podem gerar muito consumo de memória e processamento. (MILLER, 2010)

2.5.2 Coleta de Logs

Depois de definir os dispositivos de origem, agora é necessário saber como o SIEM agirá na busca desses logs no servidor. Cada aplicação ou serviço trabalham de formas diferentes, mas basicamente há dois métodos de conseguir as informações de um dispositivo de origem. A primeira forma é utilizar o método *push*, o dispositivo de origem vai enviar as informações para o servidor. A outra forma é utilizar o método *pull* que o SIEM busca a informação e recupera os logs do dispositivo de origem. Esses métodos têm suas vantagens e desvantagens, porém, são funcionais (MILLER, 2010).

Método de Push: através de um receptor, o método push se torna mais fácil de instalar e configurar no SIEM, pois é preciso apontar o dispositivo de origem para o receptor. Ao configurar, por exemplo, o syslog com o endereço IP ou o nome DNS de um servidor syslog, o dispositivo começa a enviar os logs automaticamente para o receptor de syslog que se encontra no SIEM. A vantagem é a facilidade de configuração, mas a desvantagem desse método é porque o sistema utiliza pacotes de UDP, e se caso a rede onde o dispositivo de origem estiver com o tráfego muito alto, os pacotes UDP podem se perder ou serem dropados, e assim, não são reencaminhados para o destino e o SIEM não terá como adivinhar que aquele pacote chegou ao seu destino. Outro ponto importante, é que esse tipo de configuração pode ser um problema na segurança caso os pacotes sejam interceptados e modificados, podendo, assim, inundar o SIEM com informações falsas gerando alertas falsos (MILLER, 2010).

Método de Pull: ao contrário do método de push dos logs, a configuração do dispositivo para buscar as informações a partir do SIEM se torna mais complicada. O SIEM que iniciará o processo de busca dos logs no dispositivo de origem, neste caso, é interessante notar que os logs podem não estar chegando em tempo real, diferentemente do método push, no qual ao gerar os logs, é enviado direto para o SIEM. Então, é importante observar quanto tempo o servidor irá buscar essas informações nos dispositivos de origem. Ao chegar no dispositivo fonte e puxar os logs, a coleta pode ser agrupada funcionando em determinados períodos de tempo. Por exemplo, colocar o SIEM para buscar as informações a cada dois segundos ou duas horas, dependendo da prioridade e criticidade do sistema (MILLER, 2010).

Construção pré-definida de logs e logs personalizados: quando se tem um sistema que gera logs padrões, se torna fácil configurar o SIEM, tanto para buscar informações quanto para o dispositivo de origem enviar as informações para o SIEM. Agora, quando uma aplicação personalizada gera informações, o qual o SIEM não conhece, então, é preciso tratar essas informações com mais cuidado, pois terá que construir uma forma visível de configurar essas informações no SIEM, para que este dê o devido tratamento dos logs que serão analisados. Quando o log é diferenciado e o SIEM tem que entendê-los, então, dependendo da aplicação, é necessário configurar os campos necessários que o log produz e gerar um log, que, por exemplo, pode estar formato padrão do syslog (MILLER, 2010).

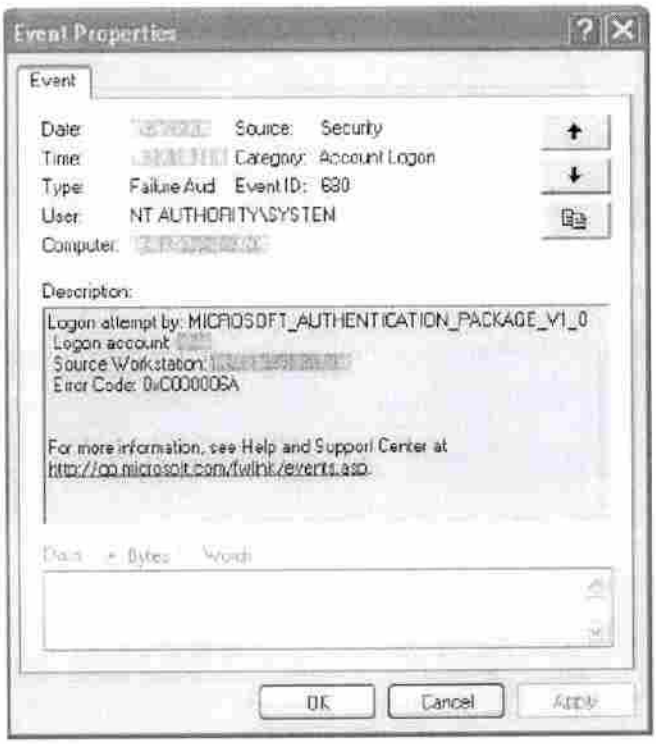
A vantagem de criar seu próprio método de logs é ter controle de toda a informação que chega no SIEM para análise, bem como dos processos de recuperação e de análise que ocorrem. A desvantagem dessa forma de tratamento dos logs é que tem de ser construídos

manualmente e saber se o SIEM é capaz de interpretar esse log que foi criado (MILLER, 2010).

2.5.3 Analisando / Normalização de Logs

Quando os logs estão sendo encaminhados para o SIEM, pode acontecer de existir uma infinidade de dispositivos e aplicações diferentes no ambiente. Quando isso acontece, os logs estão todos em seu formato original sem nenhum tratamento adequado, além que devem estar em um local apropriado como um centralizador de logs. Para que os logs fiquem compreensíveis para o administrador, é necessário que estes estejam em um formato padrão que seja utilizável pelo SIEM. Neste caso, esse processo de tratar os logs e colocá-los em um único padrão é chamado de Normalização (MILLER, 2010).

Figura 6 - Evento de Log do Windows.



Fonte: Miller, et al. (2010).

Figura 7 - Mensagem do Syslog do Cisco ASA.

Fonte: Miller, et al. (2010).

Figura 8 - Eventos Normalizados.

Time	Date	Source Device IP Address	Event Message	Event ID
22:54:53 CST	17-Jan-10	192.168.1.1	User login	ASA-sys-6-605005
22:54:53 CST	17-Jan-10	192.168.1.18	User login	Security: 680

Fonte: Miller, et al. (2010).

Para mostrar como a normalização funciona, os geram dois ambientes com logs distintos. O primeiro é um log de evento do Windows na Figura 6, e um ASA Cisco na Figura 7, com isso é gerado um acesso via *login*, o que é dependente de cada fornecedor; então, é necessário que o administrador entenda o formato e os detalhes do log. A normalização de logs no SIEM ajuda quando a apresentação de uma interface é diferente da outra. Como mostrado nas figuras, precisam ser legíveis no mesmo formato no SIEM. Assim, para todo o tipo de sistemas que o SIEM busca a informação, este processo acontece. Dessa forma, torna-se mais fácil e permite que um formato padrão se constitua no SIEM (MILLER, 2010).

2.5.4 Mecanismo de Regras

O mecanismo de regras trabalha com diferentes fontes. A ideia é disparar alertas dentro do SIEM, conforme as condições específicas nesses logs que as regras trazem. Normalmente as regras começam simples e dependendo do que se quer daquele dispositivo de origem, podem se tornar complexas. Quando cria-se as regras, algumas condições, em sua maioria booleana, determinam se as condições específicas foram alcançadas (MILLER, 2010).

2.5.5 Mecanismo de Correlação

O mecanismo de correlação é o tratamento dado as regras, o qual vai correlacionar vários eventos padrões de diferentes fontes em um único evento correlacionado. A ideia é tornar mais fácil os procedimentos de resposta a incidentes para o ambiente, mostrando em um único evento, muitos eventos que são provenientes de diversos dispositivos origem (MILLER, 2010).

Figura 9 - Padrões de eventos SIEM.

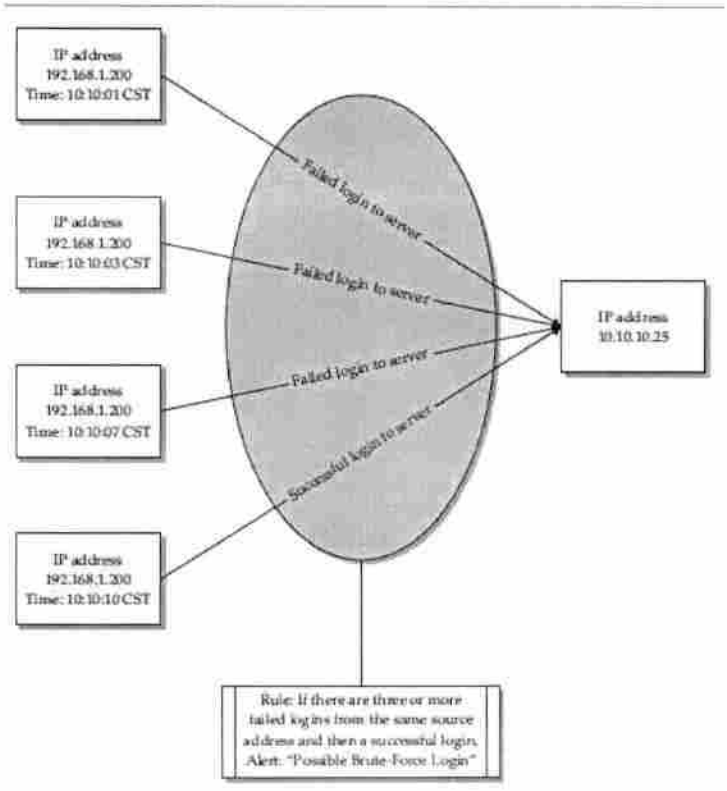
Time	Event Number	Source	Destination	Event
10:10:01 CST	1035	192.168.1.200	10.10.10.25	Failed login to server
10:10:02 CST	1036	192.168.1.90	10.10.10.21	Successful login to server
10:10:03 CST	1037	192.168.1.200	10.10.10.25	Failed login to server
10:10:04 CST	1038	192.168.1.91	10.10.10.35	Failed login to server
10:10:05 CST	1039	192.168.1.10	10.10.10.2	Successful login to server
10:10:06 CST	1040	192.168.1.10	10.10.10.3	Successful login to server
10:10:07 CST	1041	192.168.1.200	10.10.10.25	Failed login to server
10:10:08 CST	1042	10.10.10.54	192.168.1.201	Failed login to server
10:10:09 CST	1043	10.10.10.34	192.168.1.10	Failed login to server
10:10:10 CST	1045	192.168.1.200	10.10.10.25	Successful login to server

Fonte: Miller, et al. (2010).

A Figura 9 explica que vários eventos de login entraram no SIEM em um período de 10 segundos. Esses login tiveram falhas e o login de sucesso teve várias fontes e destinos diferentes. O que acontece é que um padrão vindo de um único IP tenta acessar o sistema com várias falhas de login, e logo em seguida, o login é concedido com sucesso. Este tipo poderia ser uma tentativa de força bruta. O grande problema é que essas tentativas baseada somente nas regras não vão gerar um correlacionamento e o administrador teria que ficar atento para saber que aquilo é um ataque, e assim, teria que analisar as tentativas de login e contabilizá-las. Como isso é quase que impossível, então, o correlacionamento de eventos tratará isso (MILLER, 2010).

O mecanismo de correlacionamento de eventos de um SIEM pegará de um período de tempo específico e observará os eventos de login que falharam com o mesmo endereço de origem para ao mesmo endereço de destino para o servidor de destino e, a partir daí, tomará as medidas necessárias que mitiguem o problema. Então, se tornará o agrupamento de eventos individuais que pode ser parte de um possível incidente mal-intencionado, em vez de procurar eventos separados para o mesmo fim, o SIEM vai correlacioná-lo em um único evento (MILLER, 2010).

Figura 10 - Correlação de eventos.



Fonte: Miller, et al. (2010).

A Figura 10 mostra como o correlacionamento de eventos é associado a uma regra de detecção. Neste caso, o acesso externo do IP 10.10.10.25 está realizando várias tentativas de acesso SSH e a regra diz que se caso seja negado três ou mais tentativas e logo após conseguir um acesso ao servidor, o sistema gerará um alerta, mostrando a possibilidade de login por força bruta.

2.5.6 Armazenamento dos Logs

O armazenamento dos grandes volumes de logs gerados e que vão para o SIEM precisa ser armazenado para que futuramente possa ser possível utilizar essas informações em consultas. Há três formas de armazenamento: Banco de Dados, Arquivo de texto simples ou um arquivo binário. (MILLER,2010)

Banco de Dados: o motivo e armazenar os logs no SIEM em um banco de dados é porque este método permite uma interação fácil e recuperação dos dados armazenados. Se o banco de dados for otimizado para ser utilizado com o SIEM, o SIEM ganhará em desempenho. Os problemas que podem surgir ao utilizar um banco de dados é que se o SIEM for uma

plataforma fechada, o banco de dados não terá muita interação com o SIEM, e por outro lado, se o sistema for utilizado em um ambiente aberto em que se possa ter acesso às informações, um bom administrador de banco de dados terá um grande trabalho para configurar o banco (MILLER, 2010).

Arquivo de Texto Simples: neste método, um arquivo de texto plano é utilizado como padrão, o que facilita a leitura do arquivo. Este arquivo deve ser delimitado de alguma forma, seja por vírgula, um separador específico ou qualquer tipo que demonstra que aquilo é um delimitador. Este método não é utilizado para organizações grandes, pois os tipos e volumes de informações vindas são grandes, desta forma o ato de escrever e ler em um arquivo pode ser penoso e causar queda no desempenho. Um benefício importante deste tipo de armazenamento é que se torna fácil para um analista retirar as informações que deseja, pois, o formato é legível e muitas vezes este analista foi quem utilizou uma ferramenta de pesquisa através do arquivo que ele mesmo criou (MILLER, 2010).

Arquivo Binário: o formato de arquivo em binário é um arquivo utilizando um formato personalizado para armazenar as informações binárias que são usadas somente pelo SIEM. Com isso, o SIEM é o único que sabe ler e escrever o que este arquivo faz, sendo altamente proprietário da plataforma (MILLER, 2010).

2.5.7 Monitoração

Esta é a fase final de um SIEM, ele utilizará os logs armazenados através de um modo de interação. Normalmente todo SIEM usa uma interface web como console para interagir e entender melhor o que está acontecendo com os logs. Com isso, o SIEM ficará mais fácil para ser administrado, até porque desta forma todo ambiente será visto trabalhando em conjunto em um único lugar. Isso é interessante, pois o SIEM normaliza os dados e através da interface web, o analista pode retirar as informações necessárias para gerar uma interface no SIEM, o qual pode facilitar os manipuladores de incidentes (MILLER, 2010).

Um SIEM só funciona se todas as partes estão integradas e funcionando em conjunto. Cada parte tem uma função importante que não funcionaria sem a outra. Na próxima sessão será detalhado (MILLER, 2010).

2.6 PROBLEMAS RELACIONADOS AO SIEM

Apesar do SIEM ser uma ferramenta que auxilia os administradores e analistas a

tomarem decisões para mitigar possíveis ataques e problemas na infraestrutura, um SIEM mal implementado pode gerar muitos problemas. Por isso, é importante frisar os possíveis problemas que os administradores e analistas podem passar.

Segundo Barraco (2014), no site Alien Vault, o SIEM pode se tornar muito complexo pois coleta os logs, agrega, normaliza e correlaciona diferentes tecnologias e isso torna-se uma tarefa difícil. Isso toma muito tempo, pois vai gerar várias horas gastas para absorver todas as fontes que geram logs e depois direcioná-los para o SIEM. Dependendo da escala, pode tomar meses de implementação completa do SIEM.

Outro fator importante a levar em consideração para as organizações que vão implementar o SIEM é o valor agregado ao serviço, e isso pode se tornar muito caro para empresas que desejam tornar a sua infraestrutura segura. Além disso, as empresas devem observar que o SIEM abarcará toda a organização, e que provavelmente, será necessário ainda contratar engenheiros e arquitetos de soluções para projetar e implementar a integração.

Segundo o site Securonix (2013), os analistas e profissionais de segurança percebem que o SIEM não resolverá todos os problemas de segurança, mas que este é um passo para a evolução de segurança em camadas. As tecnologias SIEM vendidas hoje prometem inúmeras soluções como: correlação, centralização, consolidação, redução de pessoas administrando vários sistemas fazendo tudo ao mesmo tempo, e por último, só faz aquilo que foi programado.

3 ESTUDO DE CASO

Para a realização do deste estudo, as atividades foram divididas em quatro etapas que serão descritas a seguir. Após a realização das pesquisas bibliográficas, verificamos que o SIEM OSSIM é uma ótima solução. Além de possuir excelente qualidade, ele é um sistema livre e gratuito; por outro lado, seus concorrentes são muito caros e de difícil acesso para testes.

Para testar a solução, montamos um laboratório. Realizamos a implantação da ferramenta e alguns testes, afim de mostrar um passo a passo da implementação e as melhores práticas.

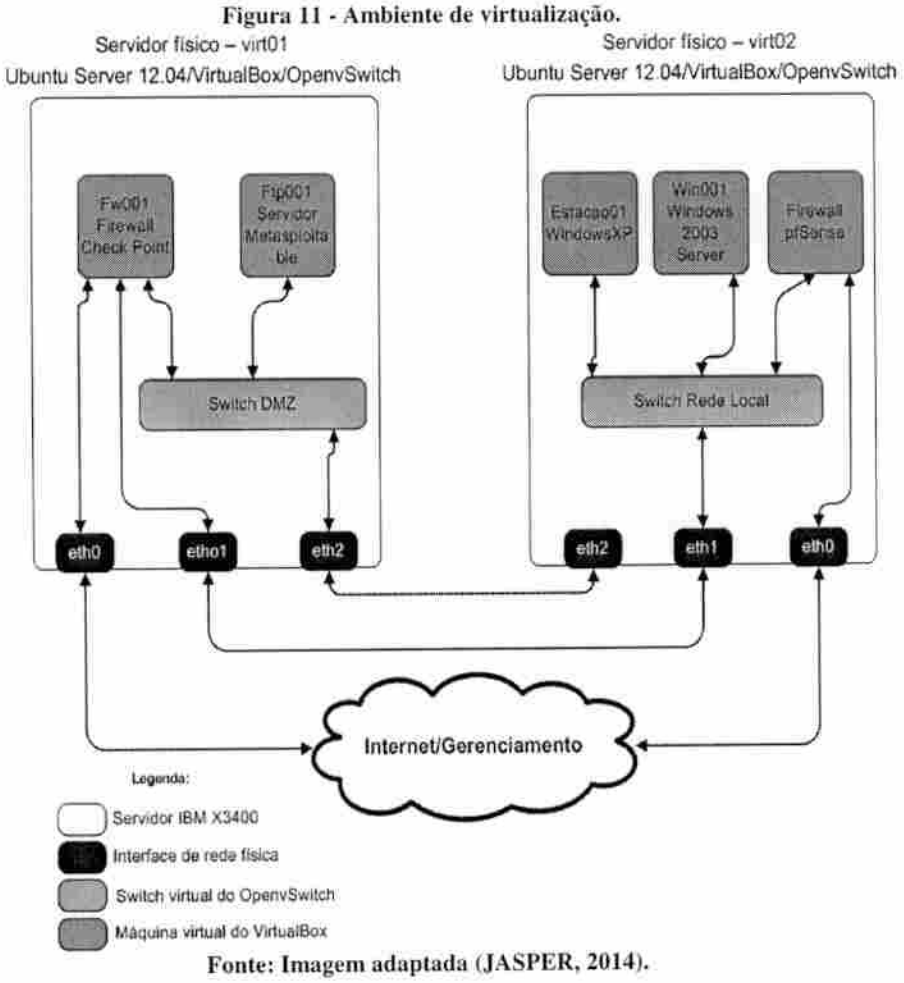
3.1 MONTAGEM DO LABORATÓRIO

A primeira atividade a ser desenvolvida neste estudo foi a montagem do laboratório de testes, o qual foi inteiramente virtualizado, garantindo uma maior flexibilidade e economia de espaço e energia.

Dispomos de dois servidores IBM X3400 com um processador Intel XEON 2GHz com quatro núcleos, 4GB de memória RAM, 500GB de espaço em disco rígido e três interfaces de rede cada.

Como solução de virtualização livre, utilizamos o Oracle VirtualBox, que apesar de não ser o melhor em desempenho e gerenciamento, atende perfeitamente ao objetivo deste trabalho. O único problema é que ele não tem a opção de espelhamento de portas de rede, configuração essencial para utilização do sistema de detecção de intrusos utilizado neste estudo. Para garantir esta opção instalamos, também, o Open vSwitch, sistema livre e de código aberto de *switch* virtual. Com ele podemos não apenas espelhar portas, mas também criar *vlans*, *netflow*, entre outras opções. A Figura 11 mostra como ficou nosso ambiente de virtualização.

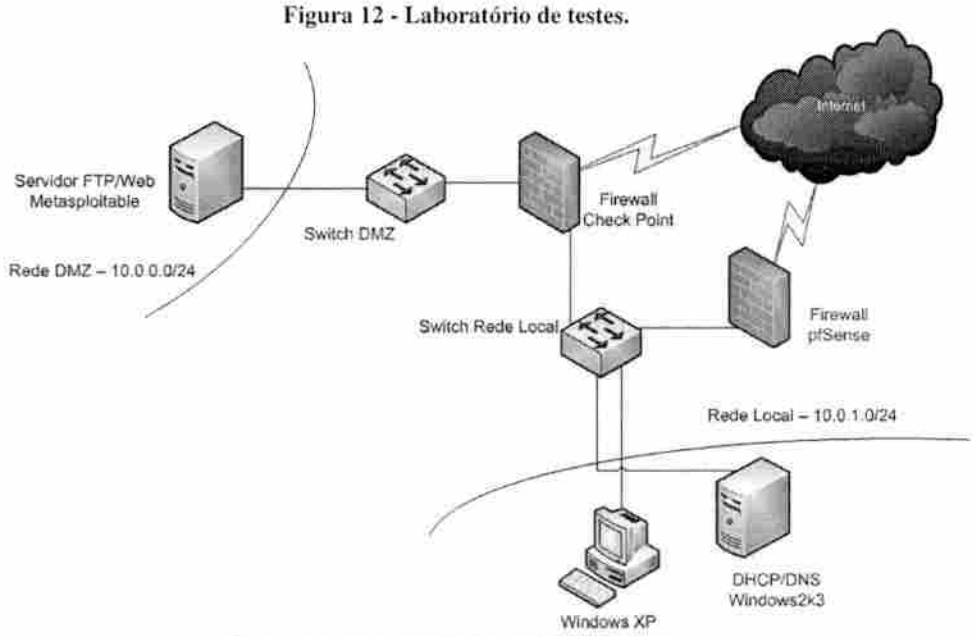
Figura 11 - Ambiente de virtualização.



Fonte: Imagem adaptada (JASPER, 2014).

Nosso objetivo nesse laboratório foi montar uma rede completa e que contasse com sistemas e equipamentos, possibilitando-nos assim testar o OSSIM. Observando a imagem 12, é possível visualizar a rede de testes antes da implantação do SIEM.

Figura 12 - Laboratório de testes.



Fonte: Imagem adaptada (JASPER, 2014).

Apesar de ser relativamente simples, podemos observar que nosso laboratório tem uma infraestrutura completa: conta com dois dispositivos de segurança do tipo *firewall*, servidores que recebem acesso externo à rede como no caso do servidor FTP/*web* e também possui serviços de rede internos como DHCP e DNS.

Na figura podemos observar que existem duas redes internas:

- 10.10.0.0/24 → É a DMZ, uma rede na qual ficam os equipamentos que serão acessados externamente. Nesse caso, apenas um servidor com sistemas *web* e FTP.
- 10.10.1.0/24 → É a rede local constituída por uma estação de trabalho e um servidor responsável pelos serviços de DHCP e DNS. É pela rede local que também é possível acessar a interface de gerenciamento do servidor IDS.

Como foge do escopo deste estudo, não entraremos em detalhes das configurações de virtualização e dos serviços configurados no laboratório, iremos apenas ressaltar alguns aspectos a fim de contextualizar os testes.

3.1.1 Firewall

O *firewall* principal utilizado no laboratório foi um *appliance* virtual da empresa Check Point. É um dos produtos mais respeitados neste tipo de solução.

De regra, existirão apenas as liberações de acessos externos na porta 80 (portal) e 21 (FTP) para a máquina www.xp.teste, 443 (HTTPS) para acesso à interface administrativa do

próprio firewall, 8080 que será redirecionada para a 443 do servidor do OSSIM e 2222 que redirecionará para a 22 (ssh) do mesmo servidor.

Além disso, haverá uma regra de *nat* para que as redes internas possam ter acesso à Internet; todo o tráfego entre as máquinas e as redes internas é liberado. A política padrão é bloquear qualquer acesso, exceto os que se encaixem nas regras já mencionadas.

Em relação ao sistema pfSense, ele possui as mesmas regras do *firewall* principal e será utilizado apenas para fins de teste de integração com o OSSIM.

3.1.2 DMZ

A rede DMZ tem um servidor com o sistema operacional Linux Metasploitable, o qual é, intencionalmente, baseado em uma versão antiga do Linux Ubuntu, com várias falhas de segurança e aplicativos vulneráveis instalados. Ele receberá conexões externas nas portas 21 com um servidor *vsftpd* e na 80 com um servidor *web* Apache, ambos com versões antigas e passíveis de serem explorados. Essa distribuição foi criada para ajudar profissionais em seus testes e é mantida pela Rapid7, empresa que criou o sistema Metasploit, o *framework* mais utilizado para testes de segurança em redes e sistemas.

3.2 IMPLANTAÇÃO DO OSSIM

Esta etapa descreverá como instalamos e configuramos o servidor OSSIM para monitorar a rede de testes.

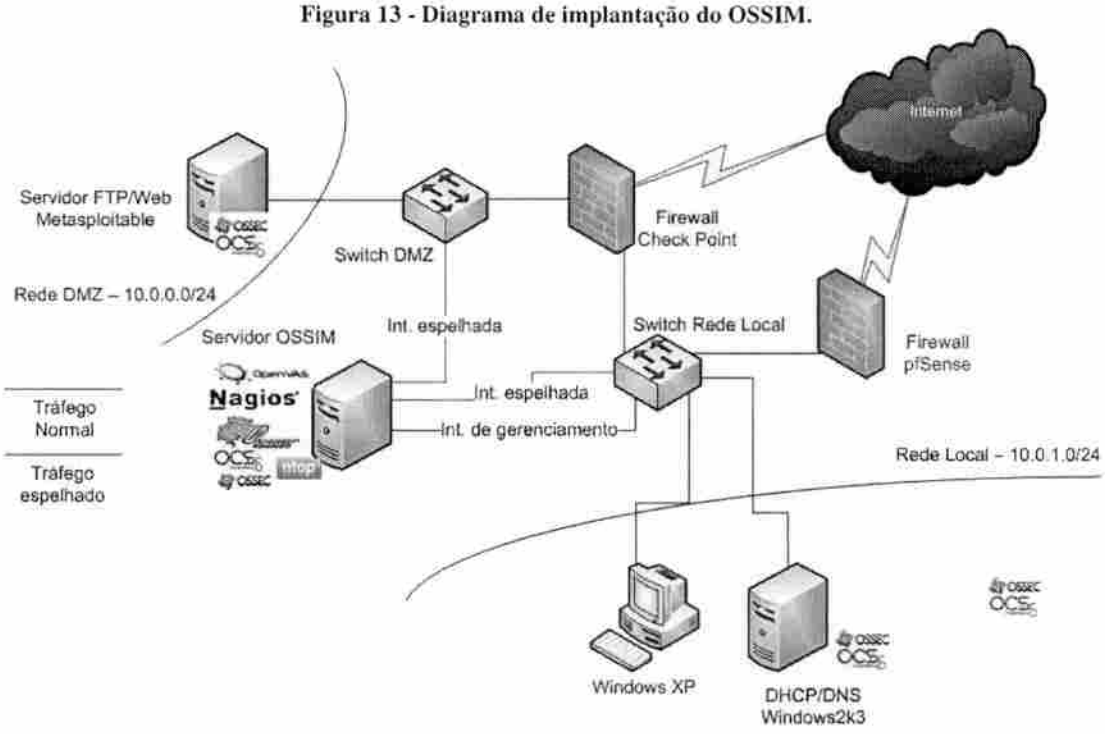
3.2.1 Planejamento

Agora, iremos falar sobre a instalação do SIEM OSSIM, que é bem fácil, mas que precisa de atenção em alguns pontos; logo, não descreveremos em detalhes toda a operação, iremos apenas apontar as questões que consideramos mais importantes.

Antes de começar, é necessário decidir qual será a estratégia para a implantação e é fundamental ter um bom conhecimento sobre toda topologia da rede. Fatores como redes e sistemas existentes, acesso remotos, criptografia, entre outros, devem ser levados em consideração antes da instalação de um SIEM.

No nosso caso, já foi explanado em tópicos anteriores, a topologia de nossa rede de testes e sua estrutura pode ser vista no diagrama apresentado na Figura 12. A partir desta figura, da análise dos equipamentos e sistemas existentes, decidimos nossa tática para implantação do OSSIM.

Figura 13 - Diagrama de implantação do OSSIM.



Fonte: Imagem adaptada (JASPER, 2014).

Como podemos observar na figura, o servidor tem sua interface de gerência conectada ao *switch* da rede local, a qual foi configurada com o endereço IP 10.10.1.252, e este será o endereço para acesso à interface administrativa do OSSIM. Além disso, foram configuradas duas portas espelhadas, uma em cada *switch*, nas quais conectamos as duas interfaces do sistema que atuam em modo promíscuo – apenas escutando a rede. Inicialmente configuramos os seguintes sensores:

- Snort – Irá analisar os dados a partir das interfaces que estão em modo promíscuo.
- OSSEC – Instalação do agente em todos os hosts.
- OCS – Instalação do agente em todos os hosts.
- Nagios – Configurado para monitorar a disponibilidade dos servidores.
- OpenVas – Realização de varreduras programadas em busca de vulnerabilidades.

Além destes, ainda estarão ativos outros que o OSSIM habilita por padrão, mas que não alteramos suas configurações.

3.2.2 Hardware

A necessidade de hardware depende mais da quantidade de eventos gerados e do

tráfego da rede, do que do sistema em si. Porém, Barraco (2014), no site Alien Vault recomenda um mínimo para o funcionamento tranquilo, como 2GB de memória *RAM*, e um bom espaço em disco rígido, visto que podem ser gerados uma grande quantidade de eventos.

É recomendado também, o uso de processadores 64 bits, pois assim haverá um melhor aproveitamento de desempenho devido ao suporte a *multithreading* que muitos de seus componentes possuem. A versão 32 bits, inclusive, já foi descontinuada a partir da versão 4.0.

É recomendada, também, a utilização de placas de rede que suportem o *driver* e1000, pois estas têm um melhor suporte nativo. Diante destas recomendações, nós utilizaremos um servidor com as seguintes configurações de *hardware*:

- 1 Processador com 4 núcleos.
- 2 GB de memória RAM.
- 55 GB de espaço no disco rígido.
- 1 Interface de rede que suporta o *driver* e1000.

É um equipamento suficiente para a instalação neste estudo, mas que dependendo do tamanho da rede e da quantidade de ativos a serem monitorados, é necessária uma máquina mais robusta.

3.2.3 Instalação

Depois de definida a estratégia e separado o servidor que receberá o sistema, o próximo passo é obter a imagem em formato *iso* do OSSIM no site da Alien Vault. Em nosso laboratório utilizamos a versão 5.4, sendo esta a mais recente. Depois de terminado o *download*, gravamos a imagem em um DVD e configuramos a BIOS do servidor para iniciar o sistema a partir deste drive.

Por ser distribuído como uma distribuição Linux, completa baseada em Debian, o OSSIM tem uma instalação padrão, semelhante às distribuições Linux mais utilizadas, com uma sequência de telas em modo gráfico, nas quais aparecem as opções a serem definidas.

Inicialmente, é necessário configurar a linguagem que será utilizada no processo de instalação, a localidade e o padrão do teclado. Após essas opções, aparecerá uma das questões mais importantes que é o perfil da instalação, pois o OSSIM pode ter alguns de seus componentes instalados em diferentes servidores. Sendo assim, podemos escolher entre quatro perfis:

- *Server* → Instalação apenas dos componentes de SIEM e Logger (este último apenas na versão paga).

- *Sensor* → Aqui são habilitados apenas os Detectores e Coletores.
- *Framework* → Este perfil instalará apenas a interface de gerenciamento web.
- *Database* → Instalação do banco de dados SQL onde ficam armazenados os eventos.

Isto é interessante, pois em redes muito complexas é possível separar esses componentes e obter uma maior flexibilidade, escalabilidade e disponibilidade. É possível, por exemplo, ter vários servidores sendo gerenciados por apenas uma interface web. No laboratório, iremos marcar todas as opções, pois utilizaremos apenas um servidor como podemos observar na Figura 14.

Figura 14 - Instalação do OSSIM - Seleção de perfil.

Fonte: Elaborado pelo autor (2017).

Continuando, o processo de instalação irá realizar a detecção do *hardware* e carregar os componentes necessários. Depois, chega a hora da configuração de rede, outra parte importante e que é necessária atenção. Como este servidor possui três interfaces de rede, é necessário escolher uma para gerenciamento. Depois serão pedidos os parâmetros para a configuração da rede, que foram definidos da seguinte maneira:

- Endereço IP → 10.10.1.252
- Máscara de rede → 255.255.255.0
- Gateway → 10.10.1.254

- DNS → 10.10.1.253
- Nome do servidor → ossim
- Nome do domínio → labsiem.teste

Figura 15 - Instalação do OSSIM - Seleção de interface.

Fonte: Elaborado pelo autor (2017).

Na próxima tela, será solicitada a senha do usuário *root*, e caso a senha seja deixada em branco, o usuário será desabilitado, ficando o usuário inicial do sistema com o poder administrativo por meio do comando *sudo*. Após a configuração da senha, é solicitada a configuração do relógio através da escolha do fuso horário.

O processo chega, então, ao outro ponto importante: o particionamento do disco. No nosso caso, devido à pouca complexidade do cenário, utilizamos uma opção mais simples que é o particionamento assistido e utilizado o disco inteiro com LVM. Ou seja, todo o sistema ficará em uma única partição. Escolhemos o uso de LVM, pois caso seja necessário, existe a flexibilidade de se aumentar o espaço em disco. Em ambientes mais complexos, é recomendado utilizar partições separadas principalmente a /var, que tende a crescer muito devido aos *logs* e banco de dados.

Finalizada a configuração do particionamento, o sistema criará e formatará as partições e, então, começa a instalação de fato, que por sinal é um pouco demorada devido à quantidade de configurações necessárias.

Durante a instalação básica do sistema são requisitadas algumas configurações iniciais, começando pela escolha das interfaces que atuarão em modo promíscuo (sem configuração de rede, apenas capturando pacotes), e que no nosso servidor ficaram a eth1 e eth2. Depois, são pedidos os endereços das redes que serão monitoradas, ou seja, as redes 10.10.0.0/24 (DMZ) e 10.10.1.0/24 (Rede Local). Outra configuração que é solicitada, é a de e-mail, pois pode-se configurar o OSSIM para enviar e-mails com alertas e relatórios.

Por fim, duas últimas configurações são necessárias e extremamente importantes: a seleção dos *plugins* de detecção e os de monitores. Para nosso caso, deixamos habilitados os que vêm por padrão, pois iremos habilitar outros à medida que necessitarmos. É importante ressaltar que toda essa configuração feita na instalação pode ser alterada e revista tanto pela interface *web* quanto pela linha de comando; podendo, inclusive, ser feita a mudança de perfil de instalação.

Figura 16 - Instalação do OSSIM - Seleção dos plugins

Fonte: Elaborado pelo autor (2017).

Após mais alguns minutos necessários para configurar os componentes com os parâmetros passados e da atualização do sistema, a instalação do SIEM OSSIM é finalizada.

3.2.4 Configuração

Após a instalação, é hora de começar a configuração da ferramenta. Para isto, basta abrir um navegador e acessar o endereço IP configurado na instalação, no nosso caso é 10.10.1.252.

Figura 17 - Tela inicial do OSSIM.

Fonte: Elaborado pelo autor (2017).

Ao acessar a interface web pela primeira vez, serão solicitadas informações para completar o perfil da conta de administrador – usuário *admin* – como a senha e e-mail. Após o envio dessas informações, é mostrada a tela de *login* para acesso ao sistema.

O OSSIM já vem praticamente pronto, e assim que acessamos a sua interface, podemos observar que ele já começou a monitorar e exibir alertas, principalmente através do IDS Snort. E assim, em um primeiro momento, é necessário apenas adequá-lo à infraestrutura existente, configurando os ativos e integrando com as ferramentas existentes.

3.2.5 Configuração dos ativos

A primeira etapa da configuração que realizamos e que consideramos mais importante foi o cadastro dos ativos que queremos monitorar. Esse passo é bastante crucial, pois este banco de informações servirá de base para muitas das funcionalidades do SIEM como a correlação dos eventos e o cálculo de riscos.

No menu à esquerda da interface, temos a opção *Asset* (Ativo), e ao clicarmos nela, esta se expande nos mostrando mais três opções.

- Assets: clicando nesta opção temos acesso ao nosso inventário de ativos, no qual podemos consultar, cadastrar, configurar ou excluir os ativos. Aqui, podemos organizar nossa infraestrutura por *hosts* individuais, grupos de *hosts*, redes, grupos de redes e portas; além de poder acessar o inventário dos equipamentos pela aba do OCS.
- *Asset Search*: o sistema nos dá a possibilidade de busca de ativos por várias

características, assim, podemos pesquisar quais deles têm determinado sistema operacional ou pesquisar quais possuem uma determinada vulnerabilidade ou evento.

- *Asset Discovery*: aqui podemos realizar vários tipos de escaneamentos na rede, afim de achar automaticamente nossos ativos. A partir dessas varreduras, podemos inserir ativos e informações de modo automatizado.

No nosso caso, primeiro instalamos o agente do OCS Inventory em todas as máquinas do laboratório, assim, todas as informações a respeito de cada host foram enviadas ao servidor, que automaticamente os incluiu na lista de ativos. O OSSIM já possui um instalador pré-configurado do agente do OCS e que fica no menu *Configuration* > submenu *Collection* > aba *Downloads*. Para instalá-lo basta apenas salvar o arquivo nas máquinas, descompactar. Caso o sistema seja Linux, executar o script setup.sh, se for Windows, executar o install.bat.

Figura 18 - Relação de Ativos.

Fonte: Elaborado pelo autor (2017).

Após a inserção dos ativos é necessário completar os dados referentes a cada um como a localização, qual sensor irá monitorá-lo e o é seu valor, este é mais importante, e seu valor pode ser de um a cinco; e, como já mencionado, fará parte do cálculo de risco. Quanto mais informações forem disponibilizadas, melhor o sistema irá trabalhar. Sendo assim, é necessário um bom conhecimento da infraestrutura existente e dos serviços disponíveis.

3.2.6 Verificação das vulnerabilidades

Após popular nosso banco de ativos, partimos, então, para uma verificação ativa das vulnerabilidades existentes em nossa infraestrutura. O qual é um passo bastante importante para manter a segurança de uma rede, pois como cita Ferreira e Araújo (2008): "uma fonte de ameaça não representa riscos quando não existe vulnerabilidade que possa ser utilizada".

Mais uma vez, o sistema se mostra bastante simples na tarefa de agendar as buscas. Ao acessar o menu *Analysis* e o submenu *Vulnerabilities*, é apresentada uma tela com quatro abas que nos dá as seguintes opções:

- *Vulnerabilities* → Mostra vários gráficos e estatísticas sobre as vulnerabilidades encontradas, como os *hosts* com mais falhas de segurança.
- *Reports* → Como o próprio nome já diz, esta aba permite acesso aos relatórios resultantes das varreduras, eles podem ser emitidos em formato pdf, html ou planilha.
- *Scan Jobs* → Opção na qual são configuradas e agendadas as buscas por vulnerabilidades.
- *Threads Database* → Repositório de vulnerabilidades usadas para os testes.

Então, agendamos uma varredora no servidor ftp.labsiem.teste, afim de descobrir quais vulnerabilidades existem naquele sistema. Como era de se esperar, devido ao uso do Linux Mestaploitable nesse servidor, foram descobertas inúmeras falhas.

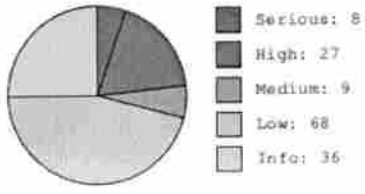
Figura 19 - Estatísticas sobre vulnerabilidades.

OSSIM

AlienVault: I.T Security Vulnerability Report

Scan time:	2017-05-15 13:02:25	Generated:	2017-05-02 12:33:44

Total number of vulnerabilities identified on 1 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Serious	High	Med	Low	Info
10.10.0.200	ftp-labsiem-teste	8	27	9	68	36

10.10.0.200	ftp-labsiem-teste

Fonte: Elaborado pelo autor (2017).

Até este ponto, se tivéssemos apenas o OpenVas instalado isoladamente, também poderíamos ter realizado a varredura e a geração de um relatório, mesmo que com um pouco mais de trabalho. Porém, no que tange ao assunto de gerenciamento de vulnerabilidades, existem duas grandes vantagens na utilização do OSSIM para tal tarefa:

- Abertura automática de chamados (tickets) → O sistema tem a capacidade de abrir

chamados automaticamente ao detectar uma vulnerabilidade. Por padrão, quando forem do tipo altas (high) e críticas (serious).

- Correlacionamento → Ao saber que existe uma falha em um sistema, o OSSIM é capaz de gerar alertas críticos caso alguma forma de exploração da mesma seja detectada. E caso exista uma ameaça contra uma vulnerabilidade inexistente, ele detecta a tentativa, mas gera alertas medianos.

Com isto, o administrador tem um controle bem maior sobre as falhas de sua infraestrutura, inclusive com capacidade para acompanhar as soluções para eliminá-las ou mitigá-las.

Figura 20 - Ticket de vulnerabilidade existente em ftp.labsiem.teste.

Fonte: Elaborado pelo autor (2017).

3.2.7 Sistemas de detecção de intrusão

Na implantação do SIEM utilizamos dois tipos de sistemas de detecção de intrusão como sensores, sendo um baseado em rede e um em *host*. É possível ainda utilizar outro tipo de IDS para rede sem fio através do *software* livre Kismet, mas que não foi abordado neste estudo.

3.2.7.1 HIDS

Como já mencionado anteriormente, o OSSIM traz o HIDS – *Host Intrusion Detection System* – OSSEC e o configuramos para ajudar na realização de nossos testes, pois ao instalar o agente deste sistema em nossas máquinas, temos a possibilidade de verificar a integridade do sistema e de arquivos, problemas com permissões, acessos indevidos, entre muitos outros.

Como no caso do OCS, o OSSIM já traz um instalador do agente. Porém, para Windows, neste caso específico, não vem pré-configurado, e não sabemos o porquê. Logo, para

a implantação dos agentes, foi necessária a realização de alguns procedimentos tanto no servidor quanto nas máquinas a serem monitoradas. Para os servidores Linux, instalamos via pacote disponível no site do projeto OSSEC.

Primeiramente, é necessário adicionar o agente que será instalado através do menu *Analysis*, submenu *Detection*, aba HIDS. Ao acessar a referida aba, fica disponível uma aba *Agents*, na qual podemos realizar o procedimento. Após adicionar um agente do OSSEC, é necessário extrair sua chave criptografada de comunicação com o servidor clicando no ícone na coluna *Actions*. Esta chave deve ser inserida juntamente com o endereço IP do servidor OSSIM ao instalar o agente nas máquinas.

Temos poucas máquinas no nosso laboratório, por isso, foi simples a tarefa de implantação dos agentes. Contudo, no caso de muitas máquinas, esse processo se torna bastante trabalhoso, mas existe outro método (o qual não foi abordado) para que este processo seja otimizado. Ainda no caso de uma infraestrutura muito grande, também será necessário mais cuidado ao planejar quais hosts serão monitorados, pois o OSSEC dispara muitos alertas e pode dificultar o processo de visualização dos mesmos.

3.2.7.2 NIDS

No que tange ao IDS baseado em rede Snort presente no próprio OSSIM, não foi necessária nenhuma configuração adicional. Na interface web, temos apenas as opções de configurar quais interfaces serão utilizadas para monitorar – estas serão colocadas em modo promíscuo – e quais redes serão monitoradas, opções estas que já foram escolhidas no momento da instalação. Estas configurações podem ser feitas ou alteradas através o menu *Configuration* e a opção *System Configuration* na aba *Sensor Configuration*.

No caso da atualização das regras do Snort, estas serão atualizadas todas as vezes que o OSSIM for atualizado; logo, não é necessária a instalação de nenhum programa adicional para realização da tarefa. Para criação de regras personalizadas, pode-se fazê-lo através do menu *Intelligence* e da opção *Policy & Actions*, inclusive para eliminação de falso-positivos e falso-negativos.

Posteriormente, configuramos o servidor IDS já existente para enviar suas informações ao servidor OSSIM, para que este possa analisá-las. Esta integração será abordada mais à frente.

3.2.8 Configurações gerais

No menu do OSSIM, podemos acessar todas as informações, configurações do servidor e do sistema através da opção *Configuration*. Esta opção é dividida em sete submenus que são descritas a seguir.

3.2.8.1 *System Configuration*

Neste submenu, temos acesso à tela de *status* do servidor, com informações a respeito do consumo de recursos, configuração de rede, atualizações do sistema e sobre o sistema de SIEM em si.

Existem ainda cinco abas que possibilitam:

- *Software Updates* – Permite acesso às atualizações disponíveis.
- *General Configuration* – Configurações gerais do servidor, como nome e servidores de e-mail e tempo.
- *Network Configuration* – Configurações de rede para gerência.
- *Sensor Configuration* – Aqui é possível habilitar e desabilitar sensores e *plugins*, bem como, configurar redes e interfaces a serem monitoradas.
- *Logs* – Visualização dos registros gerados pelo sistema operacional e dos serviços de *Server*, *Agent* e *Web* do OSSIM.

3.2.8.2 *Main*

Opções de configuração do sistema de SIEM. Pode-se modificar valores referentes às métricas como o valor padrão de um ativo, bem como configurações de *backup* do sistema e *tickets*.

Acessando a aba de configuração avançada, é possível modificar parâmetros referentes ao acesso aos bancos de dados do Snort, OSVDB e OpenVas, por exemplo. Barraco (2014), no site Alien Vault, desaconselha qualquer realização de modificações nas configurações avançadas, pois uma opção errada pode prejudicar todo o sistema.

3.2.8.3 *Users*

A gerência de usuários do OSSIM é muito flexível, permitindo a criação de usuários

com diferentes níveis de acesso. Permitindo que alguém da parte operacional de segurança da informação tenha acesso apenas aos alarmes e *tickets* para visualização e resolução dos problemas. Já um diretor de TI, só necessitaria de acesso aos gráficos de métricas e relatórios executivos.

Além disso, por padrão, todas as ações disponíveis pela interface de gerenciamento são passíveis de registros, o que permite uma série de auditorias.

3.2.8.4 *Alien Valt Components*

Nesta parte, temos acesso às informações e configurações referentes aos componentes do OSSIM espalhados pela infraestrutura. Podemos adicionar ou remover sensores e servidores, bem como mudar algumas de suas configurações e opções.

Existe ainda a aba *Locations*, na qual ficam as informações sobre os locais onde ficam os equipamentos; permitindo, assim, uma melhor organização dos destes.

3.2.8.5 *Collection*

Neste submenu existem três abas que auxiliam na configuração dos sensores e plugins:

- *Iventory* – Aba onde ficam definidas tarefas de inventário do parque de equipamentos. Configurações a respeito de agendamentos e parâmetros dos sensores *NMAP* que varre a rede em busca de novos *hosts* e serviços, OCS e WMI.
- *Data Sources* – Repositório onde é possível visualizar e modificar cada um dos plugins disponíveis no sistema.
- *Downloads* – Agentes pré-configurados para utilização na implantação do SIEM, como é o caso do OCS e do OSSEC.

3.2.8.6 Backup

Por último, e não menos importante, tem a opção de gerenciamento das cópias feitas a partir da configuração no submenu *Main*. Aqui é possível visualizar os registros a respeito das tarefas de *backup* agendadas e saber se está acontecendo algum problema.

A partir daqui pode-se também restaurar cópias de segurança armazenadas ou excluí-las caso precise de espaço em disco.

3.3 INTEGRAÇÃO

Uma das maiores vantagens que se tem na utilização de um SIEM é a centralização das informações, a qual visa resolver a problemática levantada no início deste trabalho: que o analista de segurança deve acessar várias interfaces de diferentes ferramentas para visualizar o estado de sua rede.

O OSSIM possui a capacidade de analisar eventos oriundos dos mais diversos sistemas e equipamentos utilizados em uma infraestrutura de rede de computadores. Para garantir a integração do SIEM com essas ferramentas externas simultaneamente, a Alien Vault criou um sistema de *plugins*, os quais são bastante simples e flexíveis em sua utilização, permitindo inclusive a criação de *plugins* e regras personalizados. Nesta seção descreveremos a integração com um *firewall* da empresa Check Point, com um sistema de detecção de intruso já implantado na rede de testes e como é a criação de um *plugin* personalizado.

3.3.1 Firewall Check Point

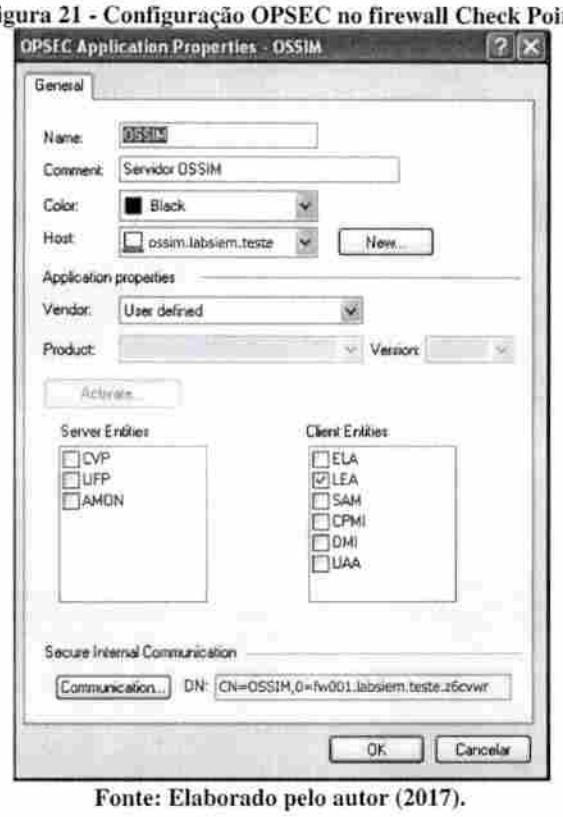
Utilizamos a solução de *firewall* da empresa israelense Check Point, uma das melhores neste segmento, afim de testar sua integração com o OSSIM.

Dentre os inúmeros *plugins* existentes no *framework*, há dois para produtos da Check Point: o *fw1-alt* e o *fw1ngr60*; sendo este último o mais recente e que deve ser utilizado com as soluções mais novas da empresa, como no nosso caso.

Inicialmente, é necessário configurar a comunicação entre o OSSIM e o *firewall*, pois o primeiro precisa acessar os registros de eventos do segundo. Para isso, existe uma ferramenta chamada *fw1-loggrabber*, a qual faz uso do *framework Open Plataform for Security* (OPSEC) que visa garantir a interoperabilidade entre ferramentas e aplicações de segurança.

O *fw1-loggrabber* é o responsável por copiar remotamente os *logs* do *firewall* e salvá-los em um arquivo no servidor do OSSIM. Para configurá-lo, primeiro acessamos a interface de gerência do Check Point e adicionamos uma nova aplicação OPSEC através do menu *Manage*, conforme podemos ver na figura a seguir.

Figura 21 - Configuração OPSEC no firewall Check Point.



Fonte: Elaborado pelo autor (2017).

Após o procedimento feito na gerência do *firewall*, partimos para a configuração do *fw1-loggrabber* no servidor do OSSIM, a qual é toda feita via linha de comando. Os arquivos de instalação da ferramenta encontram-se em /usr/share/ossim/www/downloads/ e depois de instalado seu executável e arquivos de configuração ficam localizados no diretório /usr/local/fw1-loggrabber/. É necessário a modificação de alguns valores de parâmetros presentes nos dois arquivos de configuração.

- *fw1-loggrabber.conf* – Possui configurações referentes ao arquivo de *logs*, como rotação e nível de detalhamento. Aqui foram alterados os valores das variáveis "ONLINE_MODE" para "yes" – garantindo assim acesso em tempo real dos registros – e "OUTPUT_FILE_PREFIX" que ficou com o valor /var/log/ossim/fw1-loggrabber, o qual sempre deve ser o mesmo do parâmetro "location" presente no arquivo de configuração do *plugin*, localizado no arquivo /etc/ossim/agent/plugins/fw1ngr60.cfg.
- *lea.conf* – Neste arquivo estão as opções com as quais a ferramenta irá se autenticar e comunicar com a *API* de exportação de registros do Check Point.

Inserimos o endereço IP do *firewall* na opção "lea_server ip" e modificamos o valor presente em "opsec_sic_name" para o valor presente no campo "DN" da Figura 19. Na variável

"lea_serveropsec_entity_sic_name", ajustamos o valor para que ficasse "cn=cp_mgmt,ofw001.labsiem.teste.z6cvwr".

Antes de finalizar a integração, é necessário salvar um certificado digital do *firewall* no servidor do OSSIM. Para esta etapa, foi necessário fazer o *download* de outra ferramenta, disponível no site do projeto do *fw1-loggrabber,* chamada *opsec-tools* e executar o comando: ossim:~#opsec_pull_cert–h10.10.1.254–nOSSIM–possim123–o/usr/local/*fw1-*loggrabber/etc/opsec.p12.

Com toda configuração do *fw1-loggrabber* realizada, bastou apenas acessar a interface de gerenciamento do OSSIM, acessar a opção de configuração dos sensores presente no submenu *System Configuration* e ativar o *plugin fw1ngr60* em *Collection.* A partir disto, já podemos visualizar os registros do *firewall* na interface *web* do nosso SIEM.

Figura 22 -Eventos do firewall da Check Point.

Fonte: Elaborado pelo autor (2017).

3.3.2 Firewall pfSense

Após realizar a integração com o *firewall* da Check Point, decidimos testar outra ferramenta, desta vez um *software* livre chamado pfSense. Trata-se de uma distribuição baseada no FreeBSD e customizada para servir de *firewall* e roteador; além de possuir outras funcionalidades como *proxy* e IDS. Sendo assim, decidimos testá-la.

Para sistemas operacionais baseados em Linux e BSD, o OSSIM traz a possibilidade de receber os *logs* via *rsyslog*, programa padrão nestes sistemas para enviar os registros para um servidor remoto. A interface do pfSense é bem simples e intuitiva, é possível realizar essa

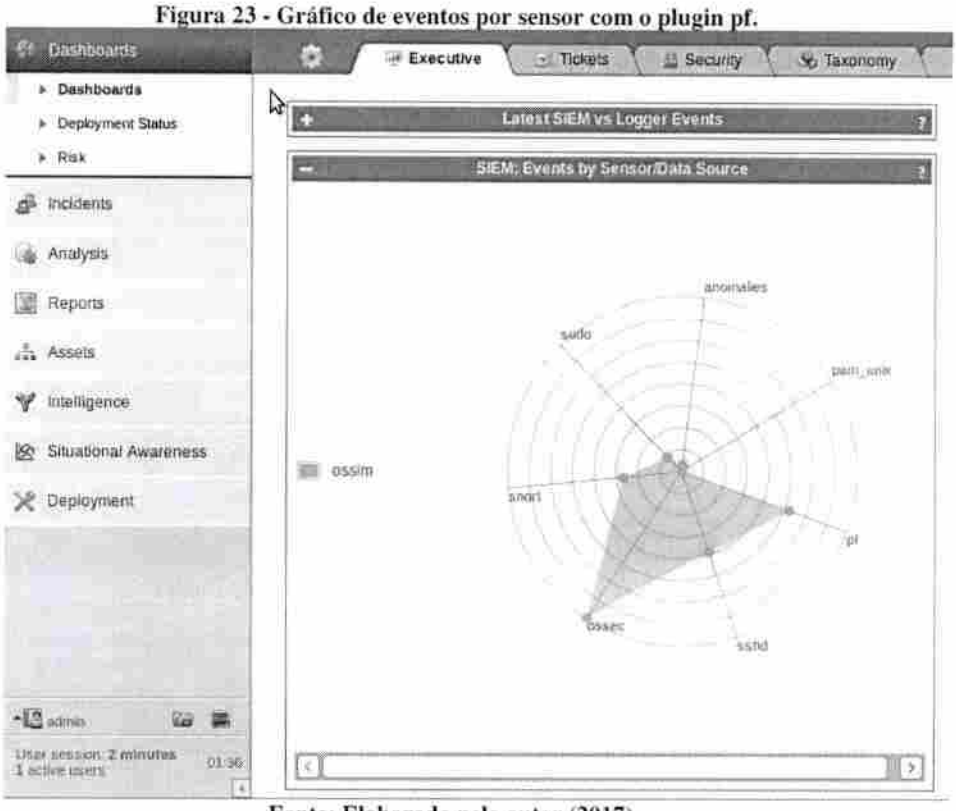
configuração acessando o menu *Status*, opção *System Logs* na gerência *web* do sistema. Na aba *Settings*, basta marcar a opção "*Enable syslog'ing to remote syslog Server*" e colocar o endereço IP do SIEM logo abaixo.

Feito isto, os registros do *firewall* já podem ser visualizados no arquivo do *syslog* do OSSIM. Então, configuramos o arquivo referente ao *pluginpf*–/etc/ossim/agent/plugins/pf.cfg–, modificamos a variável *"location"* apontando para o arquivo do *syslog* e ativamos o *plugin*.

Porém, os eventos não estavam sendo visualizados na interface do OSSIM, e pesquisando sobre essa integração, vimos que o formato dos registros do pfSense 2.x mudou em relação à versão 1.x e o *plugin* não foi atualizado em relação a isto. Pesquisando um pouco mais, descobrimos que antes, cada evento era registrado em apenas uma linha e que nesta nova versão eram duas. Ao realizar alguns testes, notamos que esse comportamento é causado por uma opção presente no arquivo /etc/inc/filter.inc presente no pfSense. Este arquivo possui o seguinte comando: /usr/sbin/tcpdump-s56-v-l-n-e-ttt-ipflog0llogger-tpf-plocal0.info. Esse é o comando que envia os eventos para o *syslog* do *firewall* e a opção -v é que está causando a mudança nos *logs*, ao retirar a mesma, os registros começaram a serem escritos em uma única linha, fazendo com que o *plugin* do OSSIM conseguisse entender o texto que estava analisando.

A partir deste momento, já podemos observar na interface de gerenciamento do OSSIM a participação do *plugin pf* no gráfico de eventos por sensor da tela inicial.

Figura 23 - Gráfico de eventos por sensor com o plugin pf.



Fonte: Elaborado pelo autor (2017).

Na Figura 24 pode-se ver um evento vindo do pfSense em detalhes, inclusive o *log* deste, agora apresentado em uma única linha, mas que originalmente é uma para o registro do tráfego e outra com o registro da ação.

Figura 24 - Detalhes do evento do pfSense.

Fonte: Elaborado pelo autor (2017).

3.4 TESTES

Já que o objetivo do SIEM OSSIM é o monitoramento de segurança de uma infraestrutura de redes. Então, decidimos realizar alguns ataques contra máquinas presentes em nosso laboratório e contra o próprio servidor do OSSIM, pois o mesmo deve garantir sua integridade para o caso de acontecer alguma violação na rede ou sistema.

3.4.1 Ataque à máquina Metasploitable

Quando fizemos a busca por vulnerabilidades em nossa rede de testes, descobrimos que o servidor FTP chamado *vsftpd* instalado na máquina ftp.teste tem uma séria vulnerabilidade, informando que essa versão contém um *backdoor*. Esta falha permite que usuários não autorizados acessem o sistema operacional do servidor e, neste caso específico, com privilégios de *root*. O OSSIM, ao encontrar essa vulnerabilidade, a classificou como de alto nível; tendo, inclusive, aberto automaticamente um *ticket*, como podemos observar na Figura 22 do tópico 3.2.6. A Figura 25 apresenta detalhes referentes a essa falha no relatório de vulnerabilidades gerado pelo sistema.

Figura 25 - Detalhes da vulnerabilidade do vsftp.

High:

vsftpd Compromised Source Packages Backdoor Vulnerability
Risk:High
Application:dm_pts
Port:6200
Protocol:tcp
ScriptID:103185
Overview:
vsftpd is prone to a backdoor vulnerability.
Attackers can exploit this issue to execute arbitrary commands in the
context of the application. Successful attacks will compromise the
affected application.
The vsftpd 2.3.4 source package is affected.
Solution:
The repaired package can be downloaded from
https://security.appspot.com/vsftpd.html. Please validate the package
with its signature.
References:
http://www.securityfocus.com/bid/48539
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://security.appspot.com/vsftpd.html
http://vsftpd.beasts.org/
CVSS Base Score : 7.5
Family name: Gain a shell remotely
Category: attack
Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH
Summary: Determine if vsftpd is installed with a backdoor
Version: $Revision: 13555 $

Fonte: Elaborado pelo autor (2017).

A exploração dessa falha é muito fácil e não tivemos problema em testá-la em nosso laboratório. Em síntese, ao enviar os caracteres ":)" como nome do usuário, o servidor fornece acesso ao *shell* do sistema com permissões de usuário *root*. Para realizar a exploração, utilizamos o *framework* Metasploit.

O ataque foi realizado com sucesso e conseguimos acesso em nível de super-usuário, tendo acesso irrestrito às pastas, arquivos e a todo o sistema. Apesar de não impedir os ataques, visto que o OSSIM não está funcionando como um IPS, ele detectou os ataques e gerou um alerta de risco máximo, como podemos observar na figura a seguir.

Figura 26 - Detecção do ataque ao servidor ftp.labsiem.teste.

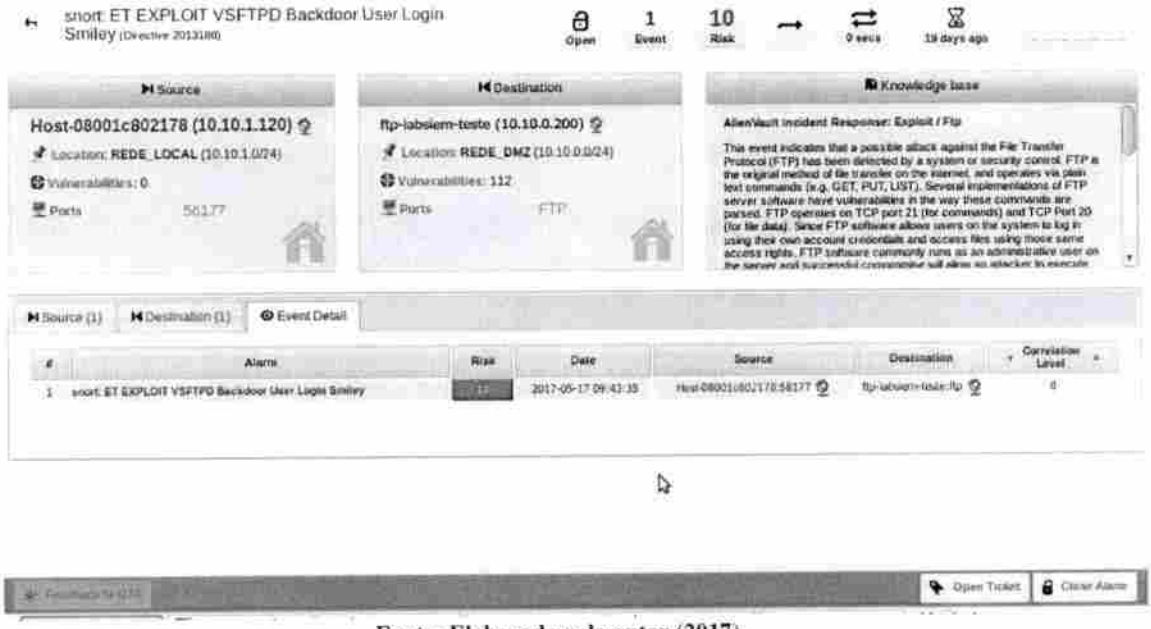
	Signature	Events	Risk	Duration	Source	Destination	Status
	Thursday 17-Jan-2017 [Delete]						
	snort: ET EXPLOIT VSFTPD Backdoor User Login Smiley	1	10	0 secs	Host-08001c802178:58177 ftp-labsiem-teste:ftp		open
	snort: ET EXPLOIT VSFTPD Backdoor User Login Smiley	1	10	0 secs	Host-08001c802178:54462 ftp-labsiem-teste:ftp		open
	SSHd: Did not receive identification string	1	1	0 secs	10.10.1.252:ANY	10.10.1.252:ssh	open
	AV FREE-FEED Policy violation, Linux package manager update detected on Unknown	15	1	3 secs	10.10.1.252:47662	10.0.1.28:squid-http	open

Fonte: Elaborado pelo autor (2017).

Ainda, o sistema nos permite visualizar mais detalhes ao clicar no alarme gerado, e desta

forma, o analista tem acesso às informações sobre as máquinas envolvidas, métricas, detalhes de como funciona a falha, podendo, inclusive, baixar o arquivo *pcap* gerado pela captura do Snort. Aqui, também, tem a opção de abertura de um *ticket* para acompanhamento do problema.

Figura 27 - Detalhes do ataque ao ftp.labsiem.teste.



Fonte: Elaborado pelo autor (2017).

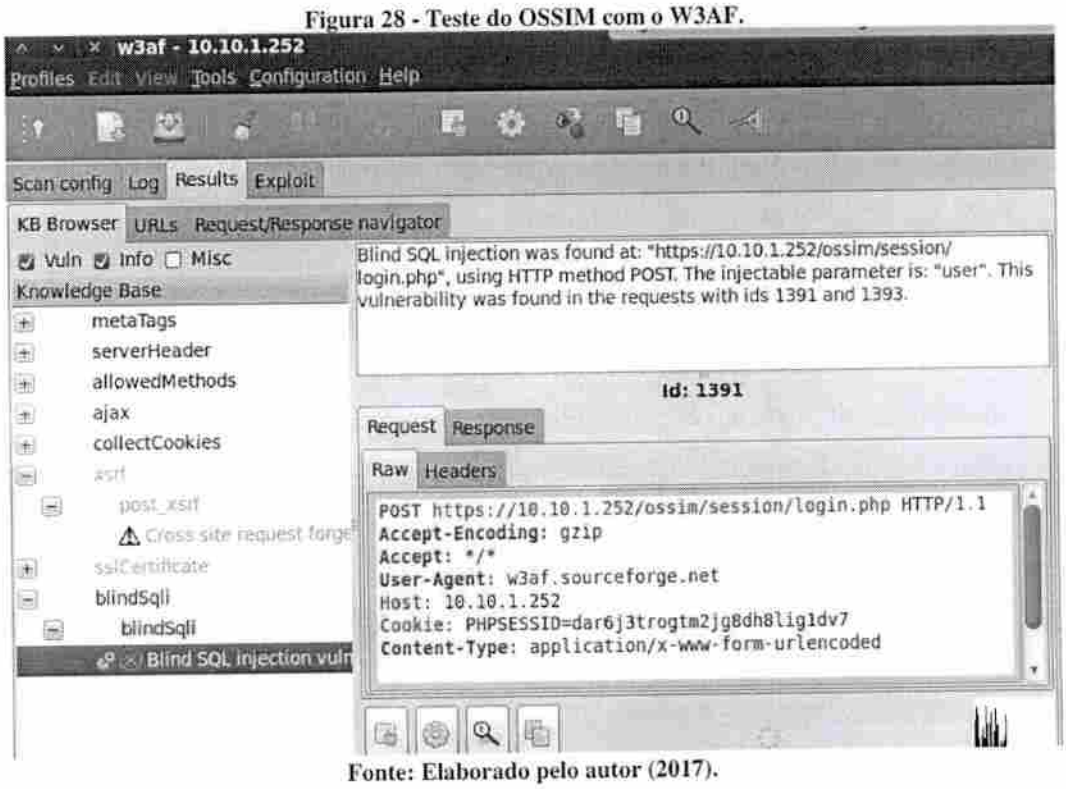
3.4.2 Teste de vulnerabilidade do OSSIM

Neste estudo realizamos alguns testes contra o servidor do OSSIM a fim de verificar a existência de falhas de segurança neste. Não foram testes muito aprofundados, pois neste primeiro momento, estudamos a ferramenta como um todo, para poder visualizar suas vantagens e desvantagens.

Inicialmente, realizamos um escaneamento com a ferramenta NMAP, o qual é um poderoso *scanner* de rede, com código aberto e livre, muito utilizado para conseguir informações a respeito do alvo, como serviços disponíveis, sistema operacional, entre outros. Nosso objetivo foi observar se apenas as portas necessárias estavam abertas. Constatamos que somente as portas referentes aos serviços essenciais estavam aceitando conexões, as quais são 22 do *ssh*, 80 e 443 da interface *web* de gerenciamento e a 514, que é na qual o *rsyslog* recebe os registros vindos de outros sistemas. Mas isto, pode variar de acordo com os *plugins* habilitados, pois alguns deles usam outras portas, como no caso do *fw1-loggrabber* que utiliza a 18184.

Após esse teste inicial, decidimos examinar a interface *web* e para tal demanda executamos um programa chamado *W3AF*, desenvolvido pela Rapid7 – mesma mantenedora do Linux BackTrack – que funciona buscando vulnerabilidades em aplicações *web*. Neste caso, foi encontrada uma vulnerabilidade do tipo SQL Injection, considerada crítica, mas infelizmente não conseguimos realizar um teste de exploração nesta. No mais, foram encontrados apenas alertas medianos e baixos. Outro ponto a destacar, foi que na etapa em que o *scanner* executou técnicas de força bruta, deixou o sistema do OSSIM fora do ar, pois foram iniciadas várias instâncias do apache, o que acabou consumindo os recursos dá máquina. Logo, ao dimensionar o servidor é necessária mais atenção nos recursos.

Figura 28 - Teste do OSSIM com o W3AF.

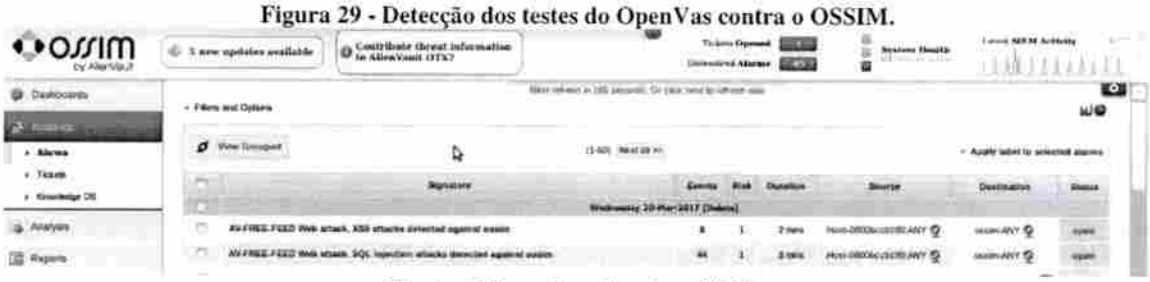


Fonte: Elaborado pelo autor (2017).

Por fim, foi realizado uma varredura em busca de vulnerabilidades utilizando o OpenVas, já descrito em tópicos anteriores. Seu relatório não apresentou nenhuma vulnerabilidade séria, apenas dois alertas medianos e algumas informações, mas nada que seja preocupante.

É importante frisar que durante as três verificações realizadas, o sistema do OSSIM detectou as tentativas e gerou vários eventos. Porém, apenas durante o último evento foram disparados alertas, como podemos observar a seguir.

Figura 29 - Detecção dos testes do OpenVas contra o OSSIM.



Fonte: Elaborado pelo autor (2017).

4 CONCLUSÕES

O objetivo geral desse trabalho foi implementar, de forma planejada, um sistema SIEM; o qual, por suas próprias características, tem uma arquitetura que nos permite, de maneira objetiva, extrair as informações dos dispositivos de origem através de um sistema de gerenciamento centralizado de eventos de segurança, e tratar esses eventos de acordo com as premissas de segurança implementadas.

Através da implementação da estrutura proposta com a ferramenta OSSIM, foi possível implementar um SIEM que coleta, analisa, normaliza os logs, trata os logs e correlaciona estes. Além disso, é possível armazenar e monitorar os logs, ajudando de forma eficaz a tomada de decisão para eventos de segurança.

O estudo relatado visou demonstrar como o SIEM OSSIM trabalha e testa alguns pontos acerca de seu funcionamento e segurança. O que vimos foi um sistema de código aberto e livre muito maduro e bem feito.

O OSSIM é uma ferramenta bastante complexa e com muitas funcionalidades para serem exploradas. No entanto, como o objetivo deste estudo não foi esgotar todas as suas funções, deixamos como sugestão, para pesquisas posteriores, uma abordagem a respeito do sistema de correlação utilizada pelo *framework*, o qual, por meio das pesquisas bibliográficas nos pareceu bem robusto e eficiente.

Por fim, podemos dizer que, em relação ao problema que foi levantado como motivação deste estudo, o sistema de gerenciamento de informações e eventos de segurança OSSIM, apesar de com alguns problemas, supriu nossas expectativas quanto ao monitoramento centralizado de segurança, e ainda, supriu também as expectativas em relação ao auxílio na gestão, atuando com um sistema de métricas, relatórios gerenciais e gráficos em tempo real.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRACO, L. Top 5 Problems with Traditional SIEM (Infographic). Disponível em: <https://www.alienvault.com/blogs/security-essentials/top-5-problems-with-traditional-siem-infographic#sthash.M4mdBhvZ.dpuf>. Acessado em: 20 de junho de 2017.

BRAINTHEE. pfSense 2.x firewall logs. Disponível em <https://alienvault.vanillaforums.com/discussion/962/pfsense-2-x-firewall-logs>. Acesso em 10 de janeiro de 2017.

SANTOS NETO, RUBENS CEDRO. Monografia Pós-graduação em Gestão de Segurança da Informação – Mecanismo de Gerenciamento de Eventos de Segurança para Auxílio na Tomada de Decisão, Distrito Federal, 2015.

CERT.BR. Cartilha de Segurança para Internet: redes. Disponível em: <http://cartilha.cert.br/redes/>. Acessado em: 20 de junho de 2017.

CERT.BR. Cartilha de Segurança para Internet: ataques. Disponível em: <https://cartilha.cert.br/ataques/>. Acessado em: 20 de junho de 2017.

CHRISTOPHER, ROGER. Port Scanning Tecniques and the Defense Against Them. <http://www.sans.org/reading-room/whitepapers/auditing/port-scanning-techniques-defense-70>. Acessado em: 07 de junho de 2017.

CID, D. B., Log Analysis Using OSSEC, Disponível em: <http://OSSEC.net/OSSEC-docs/auscert-2007-dcid.pdf>. Acessado em: 07 de junho de 2017.

DENNING, D. E., An Intrusion-Detection Model. IEEE Transactions on Software Engineering, SE-13(2), 222-232. doi:10.1109/TSE.1987.232894, (1987).

FROST & SULLIVAN. O Crescente Desafio de Manter Sua Empresa Segura. Disponível em: <http://www.cisco.com/web/BR/assets/pdfs/fs_white_paper_cisco-security_portuges.pdf >. Acessado em 02 de junho de 2017.

GEFTIC, S. Are you solving the right security problems? Disponível em: <https://blogs.rsa.com/solving-right-security-problems/>. Acessado em: 19 de Junho de 2017.

INTEGRITY, Portal Informativo ISO 27001. Disponível em: <https://www.27001.pt/iso27001_2.html>. Acessado em: 05 de junho de 2017.

JASPER, Nichols. (2014). Respostas a Incidentes de Segurança com Ferramentas SIEM. In: 16° Congresso de Tecnologia – FATEC-SP, São Paulo, Brasil. Disponível em <https://www.slideshare.net/nicholsjasper/resposta-a-incidentes-de-segurana-com-ferramentas-siem>. Acessado em: 22 de setembro de 2017.

MILLER, Daniel, R. et al. Security Information and Event Management (SIEM) Implementation. Editora Network Pro Library, 2011.

NAKAMURA, E. T.; GEUS, P.L. Segurança em Ambientes Corperativos. Novatec Editora, 2007.

NIST, Federal Information Security Management Act (FISMA) Implementation Project. Disponível em: < http://csrc.nist.gov/groups/SMA/fisma/overview.html>. Acessado em: 03 de junho de 2017.

OPSEVICES, O que é correlação de eventos? Porto Alegre, Disponível em: <http://www.opservices.com.br/correlacao-eventos>. Acessado em: 04 de Abril de 2017.

PCI SECURITY STANDARDS COUNCIL, Padrão de Segurança de Dados. Disponível em: <https://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/minisite/en/docs/pci_dss_v2-0.pdf>. Acessado em 06 de Junho de 2017.

SECURONIX, The trouble with SIEM. Disponível em: <http://www.securonix.com/the-trouble-with-siem/>. Acessado em: 20 de junho de 2017.

SEPE, R. W., Denial of Service Deterrence. Disponível em: <http://www.sans.org/reading-room/whitepapers/basics/denial-service- deterrence-35877>. Acessado em: 09 de Junho de 2017.

SILVA, Nelson Ricardo Lima da, Método de Implementação de SIEMs: Resultados de Experiências Práticas, Braga, 2011.

SOUZA, Rodrigo Garcioni. Lei Sarbanes-Oxley. 2004. 153. Monografia Graduação em Administração – Universidade Federal de Santa Catarina, Florianópolis, 2004.

STRONG SECURYTI, O que é um SIEM?, São Bernardo do Campo, Disponível em: <http://www.strongsecurity.com.br/portal/o-que-e-um-siem/>. Acessado em: 09 de Maio de 2017.

SWIFT, T. A Practical Application of SIM/SEM/SIEM: Automating Threat Identification, Disponível em: <http://www.sans.org/reading_room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification_1781>. Acesso em: 11 de Maio de 2017.

SZYMANSKY, Thiago. Os 4 ataques hackers mais comuns da web. Disponível em: <http://www.tecmundo.com.br/ataque-hacker/19600-os-4-ataques-hackers-mais-comuns-da-web.htm>. Acessado em: 25 de Junho de 2017.

U.S. Department of Health & Human Services, Health Information Privacy. Disponível em: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>. Acessado em: 08 de junho de 2017.

ZOHO CORPORATION, It Compience and Regulatory Challenges. Disponivel em: <https://www.manageengine.com/products/eventlog/eventlog-compliance.html>. Acessado em: 04 de Junho de 2017.