Modelo de Dados de uma Base de Conhecimento para Monitorar Ataques em Redes de Computadores

Giani Petri[1,2], Raul Ceretta Nunes[1], Tarcisio Ceolin Junior[1], Osmar Marchi dos Santos[1]

[1] Curso de Sistemas de Informação – Universidade Luterana do Brasil (Ulbra)
Rod. BR 285 KM 335 – 99.500-000 – Carazinho – RS – Brasil

[2]Programa de Pós-Graduação em Informática - PPGI
Centro de Tecnologia – Universidade Federal de Santa Maria (UFSM)
Av. Roraima 1000 – 97.105-900 – Santa Maria – RS – Brasil

{gpetri,ceretta,ceolin,osmar}@inf.ufsm.br

Abstract. *The popularization of the Internet has provided an increase number of web applications that work with critical information, increasing the number of attacks that exploit the vulnerabilities of these applications. This scenario has encouraged companies to invest in tools to monitor its computer networks infrastructures. This paper proposes a data model of a knowledge base that represents information of different aspects of computer networks with a focus on intrusion detection events, such as data alerts generated by intrusion detection systems, information about countermeasures, and traffic statistics. A case study conducted in a real network infrastructure demonstrates the applicability of the data model and allows us to identify the advantages of its use, demonstrating its potential use on building situational awareness.*

Resumo. *A popularização da Internet tem proporcionado um aumento no número de aplicações web que trabalham com informações críticas, aumentando os ataques que exploram as vulnerabilidades dessas aplicações. Este cenário tem estimulado as empresas a investir em ferramentas para monitorar sua infraestrutura de redes de computadores. Esse trabalho propõe um modelo de dados de uma base de conhecimento que representa informações de diferentes aspectos de redes de computadores com foco em eventos relacionados a detecção de intrusão, tais como: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre medidas de respostas e estatísticas do tráfego. Um estudo de caso realizado em uma infraestrutura de redes real demonstra a aplicabilidade do modelo de dados e permite identificar as vantagens de sua utilização, demonstrando seu potencial de uso na construção de consciência situacional.*

1. Introdução

A expansão do uso da Internet tem proporcionado um acréscimo no número de aplicações *web* que trabalham com informações críticas que, normalmente, são estratégicas para as organizações. Muitas vezes, os projetos de *software* das aplicações *web* não consideram o uso de boas práticas de segurança, deixando inúmeras vulnerabilidades nos sistemas. Em consequência, o número de ataques que exploram as vulnerabilidades existentes tem aumentado consideravelmente [Symantec 2012], causando também um aumento no número

de notificações de ataques registradas nos últimos anos [CERT.br 2012]. Este cenário tem estimulado as empresas a investir em ferramentas para o monitoramento de sua infraestrutura de redes de computadores, a fim de proporcionar melhora no nível de segurança de suas informações.

Uma das principais ferramentas utilizadas no monitoramento e identificação de atividades mal-intencionadas são os Sistemas de Detecção de Intrusão (IDS), responsáveis pela detecção de atividades maliciosas em redes de computadores ou em um computador em específico. Porém, os IDSs tradicionais estão tornando-se limitados devido ao acréscimo significativo de dispositivos, dados e informações transferidas [Golling and Stelte 2011]. Neste cenário, a construção de *Internet Early Warning Systems* (IEWS) tem sido explorada [Hesse and Pohlmann 2008] [Bastke et al. 2010].

Na arquitetura de um IEWS a base de conhecimento é um dos componentes técnicos mais importantes, por manter informações que possibilitam ações mais efetivas, pois o objetivo é detectar ameaças precocemente, antes que elas possam causar qualquer perigo. Conforme Bastke (2010), para realizar o monitoramento de ataques é preciso uma base de conhecimento que contenha diferentes aspectos (dados sobre o comportamento normal da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas) sobre a rede monitorada e que dê suporte para as decisões das equipes de segurança.

Na literatura existem trabalhos que envolvem bases de conhecimento, mas que relaxam na manutenção dos aspectos necessários. Em [Flior et al. 2010] é apresentado um sistema que captura e analisa o tráfego de rede com o objetivo de criar uma base de conhecimento com regras que permitam a tomada de decisões. Porém, na proposta de [Flior et al. 2010] não há representação de informações sobre as mensagens de alertas de detecção e medidas de respostas. Em [More et al. 2012] é proposta uma abordagem baseada em conhecimento para a modelagem de detecção de intrusão, mas essa abordagem também não engloba medidas de respostas. Undercoffer et al. (2004) apresentam uma ontologia para modelar informações de ataques em categorias agrupadas a partir do alvo do ataque, da localização e de suas consequências. Em [Chetan and Ashoka 2012] é proposta uma arquitetura para detecção de intrusão centrada em um banco de dados que armazena informações coletadas por diversos sensores. Aos dados armazenados no banco de dados são aplicadas técnicas de mineração de dados objetivando a criação de regras de detecção. No entanto, os trabalhos de [Undercoffer et al. 2004] e [Chetan and Ashoka 2012] também não representam os dados de medidas de respostas a alertas, não atendendo a todos aspectos destacados em [Bastke et al. 2010].

Este trabalho propõe um modelo de dados de uma base de conhecimento chamada KBAM (*Knowledge Base Attack Monitoring*), que engloba os diferentes aspectos de uma base de conhecimento para *Internet Early Warning Systems*. A base KBAM representa os dados de eventos de detecção de intrusão explorando o padrão de formatação de dados *Intrusion Detection Message Exchange Format* (IDMEF) [Debar et al. 2007] para mensagens de detecção de intrusão e o formato *Intrusion Detection Response Exchange Format* (IDREF) [Silva and Westphall 2006] para mensagens de respostas. A representação dos dados contidos na base contempla os aspectos necessários indicados por [Bastke et al. 2010]: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta, além dos parâmetros

para captura do tráfego da rede destacados em [Ricci 2008]. O trabalho estende o apresentado em [Petri et al. 2012] e [Petri et al. 2013b], tendo como principal contribuição a apresentação de detalhes sobre a representação dos dados/conhecimento, bem como sobre o uso da base para construção de uma consciência situacional em ambiente de rede monitorado. Como prova de conceito foi realizado um estudo de caso numa instituição real que demonstra a aplicabilidade do modelo de dados e a possibilidade da construção de consciência situacional. Na prática, a base provê informações que possibilitam reconhecimento da atual situação de segurança da rede e direcionam as atividades da equipe de segurança, auxiliando no processo de decisão de respostas a ataques em potencial.

O trabalho está organizado da seguinte forma. A seção 2 apresenta um breve referencial teórico sobre os padrões de formatação de dados. A seção 3 apresenta o modelo de dados da base de conhecimento KBAM, destacando as principais entidades e atributos. Na seção 4 é descrito o estudo de caso com a inserção da KBAM em um arquitetura de redes. A seção 5 relaciona a proposta aos trabalhos existentes na literatura. Por fim, a seção 6 apresenta as conclusões do trabalho.

2. Padrões de formatação de dados

Um Sistema de Detecção de Intrusão é uma das principais ferramentas para a identificação de ataques em redes de computadores. No entanto, essas ferramentas utilizam alguns padrões para interoperabilidade de mensagens de detecção e de respostas a intrusões. Estes padrões definem uma formatação dos dados a serem compartilhados entre as ferramentas utilizadas no monitoramento de redes de computadores. Os principais padrões utilizados são o formato IDMEF (Seção 2.1) para as mensagens de intrusão e o formato IDREF (Seção 2.2) para as mensagens de respostas a intrusões.

2.1. O Formato IDMEF

Criado pelo grupo IDWG (*Intrusion Detection Working Group*) do IETF (*Internet Engineering Task Force*), o formato IDMEF (*Intrusion Detection Message Exchange Format*) [Debar et al. 2007] é um padrão que sistemas de detecção de intrusão utilizam para reportar e compartilhar alertas sobre eventos considerados suspeitos. O principal objetivo do formato IDMEF é definir uma formatação de dados e procedimentos para a interoperabilidade entre sistemas de detecção de intrusão.

O formato IDMEF é utilizado para a troca de informações e correlação de alertas, e também para padronização de informações em um banco de dados. O IDMEF possui uma classe que é base para todo o modelo (*IDMEF-Message*) e todas as outras classes derivam desta classe base. A classe *IDMEF-Message* possui duas classes especializadas que agregam uma série de classes, são elas: *Alert* e *Heartbeat*. Uma mensagem de *Heartbeat* é utilizada pelos analisadores para indicar seu estado de funcionamento atual para os gerenciadores. A mensagem *Alert* representa um evento de segurança disparado por um IDS. A mensagem deve conter a descrição do analisador, representado pela classe *Analyzer*, o instante de criação da mensagem pelo analisador, classe *CreateTime* e uma possível classificação para o evento, determinada na classe *Classification*. A classe *Alert* ainda possui outras classes agregadas. Desta forma, possibilita uma flexibilidade do modelo para a inserção de novas especificações conforme a necessidade da mensagem de alerta.

2.2. O Formato IDREF

Outro formato de dados que objetiva dar continuidade nos modelos desenvolvidos pelo grupo IDWG, criando mecanismos de envio de respostas aos alertas identificados, é o formato IDREF (*Intrusion Detection Response Exchange Format*) [Silva and Westphall 2006]. O IDREF é compatível com o modelo de alertas IDMEF, possibilitando assim, a integração dos dois modelos.

De forma similar ao modelo IDMEF, o modelo IDREF também é representado em classes. A classe base do modelo IDREF é nomeada *IDREF-Message*, ela possui três classes derivadas (*Response*, *React* e *Config*), representando os tipos de respostas que o modelo IDREF suporta. Além disso, possui algumas classes agregadas, *AdditionalData*, *Description* e *Manager*.

A classe *Response* representa o envio de informações cujo objetivo é avisar ou controlar um ataque. A classe *Config* possibilita representar uma alteração de configuração de um recurso do ambiente para conter um ataque. A classe *React* representa uma reação contra um ataque. As classes agregadas permitem representar informações sobre o originador da resposta (*Manager*), uma descrição da resposta que está sendo aplicada (*Description*) e informações adicionais relevantes (*AdditionalData*).

3. Modelo de Dados da Base de Conhecimento KBAM

Esta seção apresenta o modelo de dados da base de conhecimento KBAM, composto por 50 entidades de representação. O modelo está voltado ao monitoramento de ataques em redes de computadores e contém entidades para representar os seguintes aspectos: dados dos alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta e parâmetros para a quantificação dos pacotes que trafegam na rede.

3.1. Representação de Alertas

Os alertas de detecção de intrusão são representados através dos atributos do modelo IDMEF [Debar et al. 2007]. As principais entidades da base KBAM que armazenam informações sobre os alertas estão ilustradas no diagrama entidade-relacionamento da Figura 1.

Note que a entidade que registra as informações referentes aos alertas disparados pelos detectores é a entidade *Alert*. Nela, o atributo *ident* armazena um identificador para o alerta, o *create-time* armazena o instante da criação do alerta, o *analyzer-time* armazena o momento em que o alerta foi disparado e o *detect-time* o instante em que o evento foi detectado. Esta entidade relaciona-se com outras entidades nomeadas *AdditionalData*, *OverflowAlert*, *ToolAlert*, *Classification* e *Assessment*, descritas a seguir.

A entidade *AdditionalData* armazena as informações adicionais das mensagens de alertas, que não se encaixam no formato IDMEF. Já a entidade *OverflowAlert* representa informações específicas de mensagens de alertas do tipo *overflow*, a *ToolAlert* contém informações referentes a alertas de ataques gerados por programas ou ferramentas. A entidade *Classification* registra uma classificação do tipo de alerta. A classificação dos eventos é determinada conforme a configuração de cada regra de detecção dos IDSs. A partir da classificação, o alerta pode ter alguma documentação externa que possua maiores

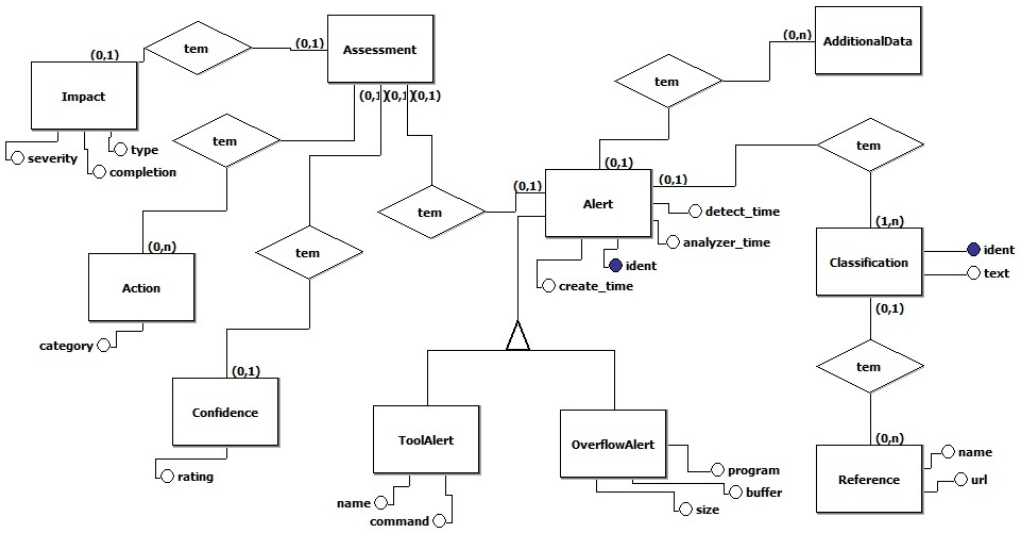

Figura 1. Entidades que representam os alertas de detecção.

informações referentes ao alerta gerado. Essas informações ou *links* para os documentos ficam armazenadas na entidade *Reference*.

As informações que permitem uma avaliação do evento causador do alerta são armazenadas na entidade *Assessment*, por isto esta entidade relaciona-se a outras três: *Impact*, *Action* e *Confidence*.

A entidade *Impact* provê informações referentes ao nível do impacto do evento sobre o sistema, registradas em três atributos. O atributo *severity* armazena uma *string* com o identificador do nível do impacto (0-Alerta representa uma atividade informativa; 1-Impacto Baixo; 2-Médio; 3-Alto). O atributo *completion* armazena a informação se o evento foi completado com sucesso ou não (*failed*=0 e *succeeded*=1). O *type* registra o tipo de tentativa do evento, aceitando os seguintes valores: 0-*admin*, tentativa ou obtenção de privilégios administrativos; 1-*dos*, tentativa ou realização de ataque de negação de serviço; 2-*file*, tentativa ou realização de ações em um arquivo; 3-*recon*, tentativa ou realização de ações de reconhecimento do sistema; 4-*user*, tentativa ou obtenção de privilégios de usuários; e 5-*other*, o evento não se enquadra em nenhuma das categorias anteriores.

As ações tomadas pelos administradores em resposta ao evento de alerta são armazenadas na entidade *Action*, que possui somente o atributo (*category*). Neste atributo podem estar armazenadas as seguintes categorias: 0-*block-installed*, indicando que algum tipo de bloqueio (endereço, porta, desabilitar conta de usuário, etc) foi realizado para prevenir que um ataque atinja seu destino; 1-*notification-send*, indicando que uma mensagem de notificação foi enviada através de e-mail, pager, etc; 2-*taken-offline*, indicando que um sistema, computador ou usuário envolvido com o ataque foi tirado de funcionamento; 3-*other*, indicando uma ação que não se enquadra nas categorias acima.

Já a *Confidence* determina o nível de confiança das informações prestadas pelo componente de análise. O atributo *rating* desta entidade armazena o nível de confiança, podendo ter os seguintes valores: 0-*low*, baixo nível de confiança; 1-*medium*, média; 2-*high*, alta; e 3-*numeric*, valor numérico que especifica o percentual de confiança.

Representado o alerta, o modelo também contém entidades que permitem armazenar informações sobre as mensagens de alerta. Para tal a entidade *Alert* também se relaciona com outras entidades, conforme ilustrado na Figura 2.

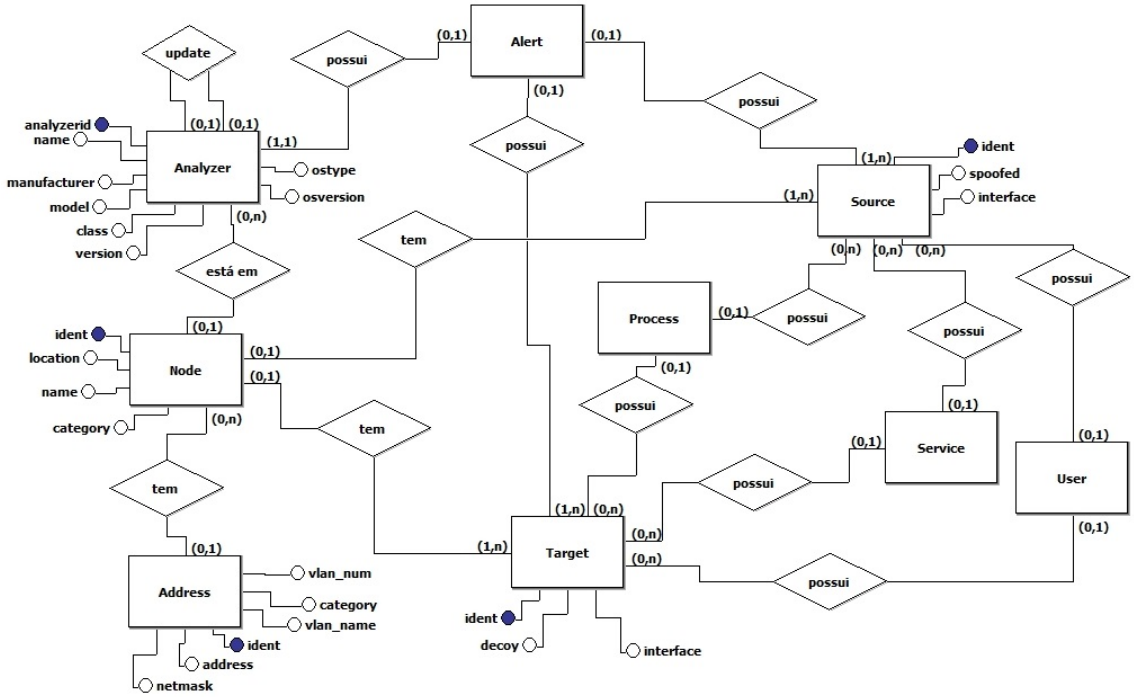

Figura 2. Entidades que representam informações sobre mensagens de alertas.

A entidade *Analyzer* armazena informações referentes a identificação do analisador que originou a mensagem de alerta. Apenas um analisador pode ser identificado para cada alerta originado. Os dados sobre o nome, a versão, a classificação, o modelo e o fabricante do analisador ficam registrados nesta entidade, além de informações do tipo e a versão do sistema operacional que o analisador atua. A entidade *Analyzer* possui um auto relacionamento, pois quando o alerta é enviado para outro analisador é necessário atualizar a informação do analisador original. O local do analisador (*host* ou dispositivo de rede) é armazenado na entidade *Node*, que tem como atributos: a localização do dispositivo (*location*), o ambiente onde o dispositivo atua (*category*) e o nome do equipamento (*name*), além de seu identificador (*ident*). A entidade associada *Address* detalha o endereçamento de rede do *host* ou dispositivo. A entidade possui um identificador único (*ident*) e o atributo *category* armazena informações referentes ao tipo de endereço de rede que está sendo utilizado (IPv4, IPv6, ATM, MAC, etc). Os atributos *vlan-name* e *vlan-num* representam, respectivamente, o nome e o número que identifica a rede que o endereço pertence. O campo *address* especifica o endereço e o atributo *netmask* armazena a máscara de rede, quando apropriada para o endereço utilizado.

As informações sobre os nodos fonte e destino do evento de alerta são armazenadas nas entidades *Source* e *Target*, respectivamente. Conforme a Figura 2, a entidade *Source* possui um identificador (*ident*) e dois atributos. O atributo *spoofed* contém um indicador se o componente de análise conseguiu identificar se as informações de origem do ataque são verdadeiras. Os valores aceitos neste campo são: 0-*unknow*, 1-*yes* e 2-*no*.

O valor *yes* (1) determina que as informações de origem são falsas e o valor *no* (2) determina que as informações prestadas pelo analisador são verdadeiras. O atributo *interface* explicita a interface de rede que gerou o alerta. De maneira similar a entidade *Target* representa informações sobre os possíveis alvos dos eventos que geraram um alerta. Tanto a entidade *Source* como a entidade *Target* se relacionam com outras entidades para permitir o mapeamento do processo (*Process*), serviço (*Service*) e/ou usuário (*User*) que podem ter iniciado o evento.

3.2. Representação de Respostas

Para modelar as respostas aos alertas gerados pelos IDSs, foi utilizado o padrão de formatação de dados IDREF. De acordo com o diagrama entidade-relacionamento da Figura 3, na base KBAM a principal entidade que representa uma resposta a um alerta é a *IDREF-Message*. Esta entidade contém os atributos *ident* e *version* que representam, respectivamente, uma identificação única para as respostas geradas e a versão do modelo de dados utilizado.

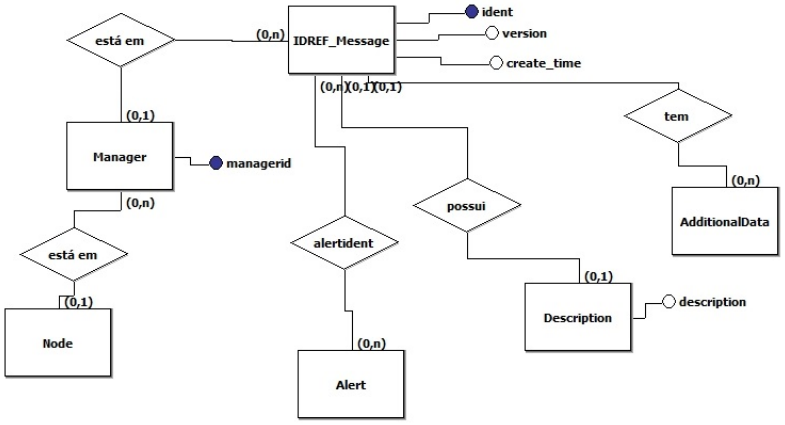

Figura 3. Entidades que representam as respostas aos alertas.

Assim como no formato IDMEF, na modelagem das respostas a entidade *AdditionalData* se relaciona com *IDREF-Message* para armazenar informações que não são suportadas pelo formato IDREF, habilitando a inserção de informações adicionais sobre a resposta a um evento. No modelo a relação *alertident* representa o relacionamento entre as mensagens de alertas e as medidas aplicadas em resposta a estes alertas.

Outra entidade que se relaciona a *IDREF-Message* é a entidade *Description*, que armazena uma descrição da resposta que está sendo executada. Nesta descrição podem ser inseridas informações específicas sobre a resposta ou informações extras que sejam úteis para análises posteriores. Por sua vez, a entidade *Manager* contém informações referentes ao gerenciador que enviou a resposta ao alerta e relaciona-se com a entidade *Node* que representa o nodo em que está hospedado.

A entidade *IDREF-Message* também se relaciona com *Response*, *React* e *Config*, que representam os tipos de respostas suportados pelo formato IDREF, conforme apresenta a Figura 4.

A entidade *Response* armazena as informações sobre o aviso de um ataque e se relaciona com as entidades *TCP*, *ICMP*, *Notify* e *Address*. A entidade *TCP* contém

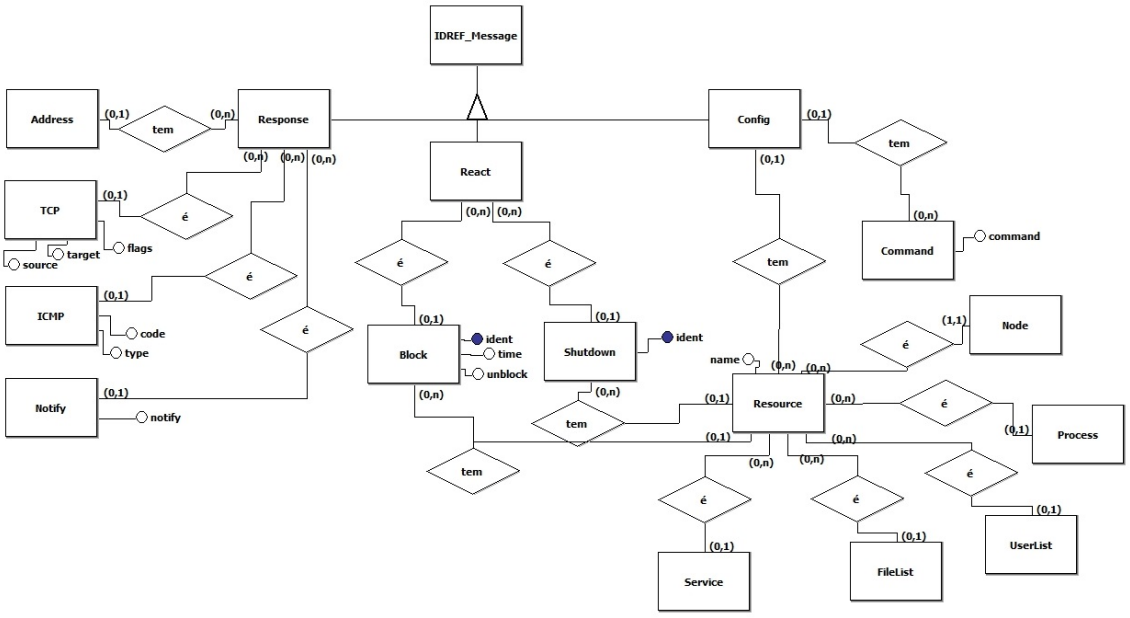

Figura 4. Entidades que representam os tipos de respostas.

informações referentes ao envio de pacotes TCP pela rede para responder a um alerta. Seus atributos *source*, *target* e *flags* armazenam os dados que devem ser colocados no pacote TCP para ser enviado. Já a entidade *ICMP* armazena informações sobre as mensagens ICMP enviadas em resposta a uma mensagem de alerta. Os atributos *type* e *code* contêm informações que devem ser inseridas na mensagem ICMP a ser enviada. Logo, a entidade *Notify* armazena informações sobre o ataque, podendo representar até mesmo o alerta no formato IDMEF. Por sua vez, a entidade *Address* registra o endereço de destino da resposta, conforme o tipo identificado no atributo *type*.

Outro tipo de resposta a um alerta é representado através da entidade *React*. Esta entidade representa as reações do ambiente para conter um ataque. Uma reação pode ser realizada através do bloqueio (*Block*) ou fechamento (*Shutdown*) de algum recurso. A entidade *Block* representa o bloqueio de um recurso, contendo um identificador único do bloqueio representado pelo campo *ident*, o atributo *unblock* indica o momento que o recurso deve ser desbloqueado. Este atributo pode conter dois valores: *reset*, quando o recurso deve ser reinicializado para ser desbloqueado ou *time*, que indica que o recurso deve permanecer bloqueado por um tempo determinado no atributo *time*, que contém em minutos o tempo que o recurso deve permanecer bloqueado. A entidade *Shutdown* representa o desligamento de algum recurso e possui um atributo que representa o identificador da reação executada. Um bloqueio ou um desligamento é realizado sobre um único recurso. O recurso envolvido na reação é representado na entidade *Resource*.

Além do envio de mensagem pela rede e do bloqueio de algum recurso, outro tipo de resposta pode ser realizado através da reconfiguração dos dispositivos de rede. A alteração nas configurações de algum recurso é representada pela entidade *Config*, conforme apresenta a Figura 4. Os dados sobre os recursos configurados estão armazenados na entidade *Resource*. Um recurso pode ser um nó ou um serviço da rede, uma lista de usuário, uma lista de arquivos ou um processo do sistema operacional. Estes recursos são

representados pelas entidades: *Node*, *Service*, *UserList*, *FileList* e *Process*. Os comandos executados na reconfiguração dos recursos ficam armazenados na entidade *Command*, podendo ter vários comandos para uma única resposta a ser executada em um recurso específico.

3.3. Representação sobre Tráfego de Rede

Os dados sobre o tráfego da rede podem ser armazenados nas entidades *Parameters* e *Counter_mod*, conforme ilustra a Figura 5.

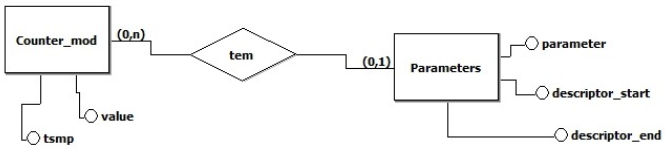

Figura 5. Entidades que representam a quantificação do tráfego da rede.

A entidade *Parameters* permite armazenar todos os parâmetros de interesse capturados do tráfego da rede monitorada. O atributo *parameter* armazena a descrição do parâmetro utilizado e os atributos *descriptor_start* e *descriptor_end* contêm o intervalo dos descritores de cada parâmetro, caso o mesmo tenha um descritor. Já a entidade *Counter_mod* é responsável por armazenar todos os contadores dos pacotes capturados na rede. O momento da captura dos dados é armazenado no atributo *tsmp*, a quantificação dos pacotes está no campo *value* e a identificação do parâmetro é realizada através do relacionamento com a entidade *Parameter*.

Os parâmetros representados na base de conhecimento KBAM para quantificar o tráfego da rede foram alinhados aos descritores de rede usados pela sonda do sistema IAS (*Internet Analysis System*) apresentados em [Hesse and Pohlmann 2008] e detalhados em [Ricci 2008]. A sonda de um IAS trabalha de forma similar a um *sniffer*, realizando a captura de dados do tráfego de uma rede. Deste modo os parâmetros considerados são: IP, UDP, TCP, TCP Flag SYN, TCP Flag SYN-ACK, TCP Flag ACK, HTTP, HTTPS, HTTP Post, HTTP Get, HTTP Head, SMTP, SMTPS, IMAP/POP, SIP, ICMP, ICMP(Type 0), ICMP(Type 3), ICMP(Type 4), ICMP(Type 5), ICMP(Type 6), ICMP(Type 8), ICMP(Type 11), entre outros. A seleção destes parâmetros está baseada no trabalho de Ricci (2008), que destaca os parâmetros considerados essenciais para a criação de uma visão global que permita a construção de uma consciência situacional para detectar possíveis eventos maliciosos.

4. Estudo de caso: inserindo a Base de Conhecimento KBAM em uma Arquitetura de Redes

Como prova de conceito da modelagem apresentada, foi desenvolvido um estudo de caso na rede da Universidade Federal de Santa Maria (UFSM), o qual envolveu o monitoramento de duas sub-redes para a coleta de dados. As sub-redes correspondem a pontos estratégicos na infraestrutura de rede da instituição (CPD e Coperves) e que estão frequentemente sob ataques.

Nos ambientes monitorados foram instalados os sistemas de detecção de intrusão baseados em assinaturas Snort [SNORT 2012], em sua versão 2.8.5.2-2, e o Suricata

[SURICATA 2012], na versão 1.2.1. A integração destes IDSs é realizada através do uso do *framework* Prelude [PRELUDE 2012].

No estudo de caso, os IDSs trabalham como sensores e estão configurados para se comunicarem diretamente com o Prelude. A configuração permite que os sensores, ao identificar algum evento malicioso, compatível com as regras de detecção, gerem os alertas e automaticamente encaminhem para Prelude armazenar os eventos no banco de dados próprio da ferramenta, que também está modelado com os dados do formato IDMEF. A Figura 6 apresenta graficamente este processo de integração.

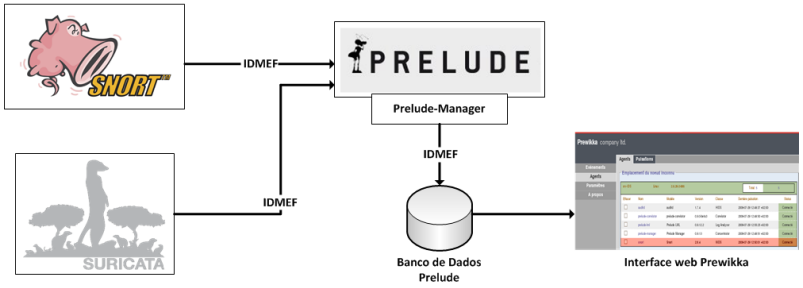

Figura 6. Arquitetura implementada para a integração dos IDSs.

A interface *web Prewikka* permite à equipe de segurança monitorar os eventos através da visualização de todas as informações contidas nas mensagens de alertas, potencializando a identificação do montante de alertas gerados, bem como dos detalhes de cada alerta, tais como: hora da detecção, gravidade, origem, alvo, dentre outras informações de interesse.

Os IDSs e o *Prelude* foram instalados em três máquinas virtuais (VMs). Uma VM é o gerenciador, onde estão instalados o Prelude, o banco de dados e a interface *Prewikka*. As outras duas VMs são os sensores que possuem os IDSs Snort e Suricata. A Figura 7 apresenta a arquitetura de rede implementada no estudo de caso.

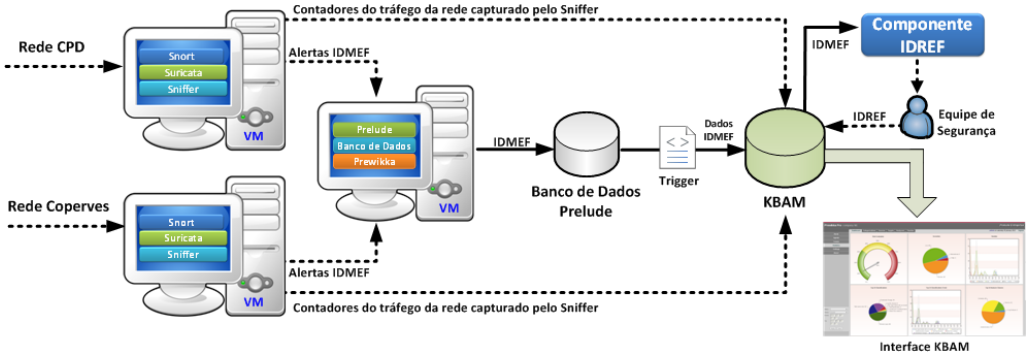

Figura 7. Infraestrutura do estudo de caso.

Conforme pode ser observado na Figura 7, as mensagens de alerta são geradas pelos sensores e encaminhadas para a VM gerenciadora que direciona as mensagens de alertas ao banco de dados do Prelude. No banco de dados da ferramenta Prelude está inserida uma *trigger* que realiza o processo de inserção dos dados dos alertas na KBAM. Esta inserção seguiu as representações especificadas na seção 3.1.

Nas VMs que trabalham como sensores também está instalado o Wireshark [WIRESHARK 2012] que trabalha como um *sniffer* capturando e quantificando os pacotes que trafegam na rede da instituição. Após a captura dos dados através do Wireshark, os contadores de cada um dos parâmetros coletados são armazenados na KBAM. Com a quantificação do tráfego da rede disponível na KBAM as equipes de segurança utilizam diferentes técnicas para detecção de comportamentos anômalos. Há diversas técnicas para detecção de anomalias dentre elas se destacam: [Azevedo et al. 2012] e [Pereira and Jamhour 2011]. A representação na KBAM seguiu o especificado na seção 3.3.

O Componente IDREF está conectado a KBAM e disponibiliza em sua interface inicial as mensagens de alertas para a equipe de segurança selecionar a mensagem que uma resposta será aplicada. Ao selecionar a mensagem de alerta o Componente IDREF busca na KBAM as contramedidas efetuadas em resposta a alertas similares (que foram gerados pela mesma regra de detecção de intrusão), disponibilizando-as e dando suporte à equipe de segurança na criação da contramedida atual. Após a configuração da cotrametida ela é adicionada na KBAM para apoiar a equipe de segurança na criação de futuras contramedidas.

Como pode ser observado na Figura 7, o processo de criação de uma contramedida através do Componente IDREF é cíclico e com interação humana da equipe de segurança. Deste modo, a medida de resposta é refinada a cada ciclo em que é utilizada para responder a um alerta.

O resultado do estudo de caso foi a demonstração de que o uso da KBAM além de armazenar os dados das mensagens de alertas gerados pelos IDSs e da quantificação do tráfego da rede, armazena também um conhecimento sobre as contramedidas que são refinadas continuamente pela equipe de segurança a cada iteração. Na prática a KBAM potencializa uma detecção mais precisa de ataques, dado que as informações correspondentes aos diferentes aspectos citados por [Bastke et al. 2010] estão armazenadas na KBAM e disponíveis para a equipe de segurança construir a consciência situacional do ambiente monitorado. Ao construir a consciência situacional a equipe adquire uma compreensão das atividades maliciosas que estão ocorrendo e suportam a sua tomada de decisão na criação de contramedidas em respostas a ataques em potencial. Mais detalhes sobre a construção da consciência situacional com base nos dados armazenados na KBAM é resumidamente apresentada em [Petri et al. 2013a].

5. Trabalhos Relacionados

Monitorar ataques em infraestruturas de redes de computadores é uma atividade complexa que exige experiência e profissionais especialistas. Logo, para a equipe de segurança fundamentar suas decisões no processo de resposta à atividades maliciosas é necessário uma base de conhecimento de contenha informações que suportam essas decisões e que permita a construção da consciência situacional do ambiente em que se está monitorando. De acordo com Bastke, Deml and Schmidt (2010), as informações que devem ser armazenadas em uma base de conhecimento devem corresponder aos seguintes aspectos: dados sobre o comportamento normal da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas.

No entanto, os trabalhos existentes na literatura não atendem integralmente a es-

tes aspectos necessários para uma base de conhecimento, dificultando o trabalho das equipes de segurança em buscar as informações em repositórios de dados diferentes e não integrados. Todavia, alguns trabalhos propõem soluções relacionadas. Dentre eles, [Undercoffer et al. 2004] propõe uma ontologia que objetiva modelar os ataques categorizados em acordo com o alvo do sistema, os significados do ataque, suas consequências e a localização do atacante. No entanto, a ontologia proposta por [Undercoffer et al. 2004] não representa os dados do tráfego da rede e também não aborda informações sobre as medidas de respostas para conter os ataques.

Flior et al. (2010) propõem um sistema especialista que utiliza a classificação como técnica de mineração de dados aplicada em um conjunto de informações capturadas do tráfego da rede, objetivando criar uma base de conhecimento com regras a partir da fusão dos dados do comportamento normal e malicioso, coletados por múltiplos sensores, e que permita fazer decisões em tempo real e responder apropriadamente aos eventos. Entretanto, a proposta apresentada em [Flior et al. 2010] não engloba todos os aspectos de uma base de conhecimento, desconsiderando o armazenamento de informações sobre incidentes e suas medidas de respostas.

Em More et al. (2012) é apresentado um *framework* que trabalha com a integração de dados de sensores heterogêneos utilizados para a captura de dados de detecção de intrusão e logs. Os dados capturados são armazenados em uma base de conhecimento que é estruturada por uma abordagem ontológica para modelar os dados das ameaças identificadas. Porém, esta abordagem não representa informações referentes as respostas aos alertas de detecção.

Chetan e Ashoka (2012) apresentam um sistema de detecção de intrusão em rede baseado em mineração de dados. A proposta possui uma arquitetura centrada em um banco de dados para auxiliar na detecção de intrusão, utilizando componentes que trabalham como sensores para a coleta dos eventos e um repositório centralizado responsável por armazenar os dados coletados. Em seguida, diversas técnicas de mineração de dados são aplicadas aos dados armazenados no repositório para a geração de regras de detecção. No entanto, a proposta apresentada em [Chetan and Ashoka 2012] também não trabalha com informações de respostas a alertas de detecção.

Observa-se assim, que os trabalhos que utilizam bases de conhecimento, não costumam abordar todos os aspectos necessários para a criação de uma base de conhecimento voltada ao monitoramento de ataques. Além disso, também não exploram os padrões de interoperabilidade voltados a detecção de intrusão, o que pode ser um limitador na integração a sistemas de monitoramento. O modelo de dados apresentado neste trabalho possibilita tanto o alinhamento aos padrões de interoperabilidade como a representação dos aspectos de rede essenciais para a realização de um monitoramento de ataques, integrando informações de diversos aspectos da rede em um repositório de dados integrado.

6. Conclusões

Este trabalho apresentou o modelo de dados da base de conhecimento KBAM, que armazena dados de mensagens de alertas gerados por IDSs, a quantificação do tráfego da rede e as medidas aplicadas em resposta a um alerta, ou seja, conhecimento. A base KBAM atende os diferentes aspectos necessários para a construção de uma base de conhecimento voltada ao monitoramento de ataques, podendo ser utilizada em *Internet Early Warning*

Systems. Focada numa modelagem baseada em formatos padrões (IDREF e IDMEF) a base pode ser inserida em qualquer infraestrutura de rede que possui IDSs que utilizam esses padrões.

A realização de um estudo de caso numa arquitetura de redes real permitiu destacar a aplicabilidade da KBAM em um ambiente de rede em produção e realçar as vantagens de sua utilização: o armazenamento de dados coletados através de sistemas de detecção de intrusão integrados; a representação de dados através de formatos padrões existentes na literatura; a quantificação do tráfego da rede e o armazenamento de conhecimento agregado no processo cíclico de criação de contramedidas aplicadas aos eventos maliciosos. Adicionalmente, os dados armazenados na KBAM ficam disponíveis para a equipe de segurança criar consciência situacional do ambiente de rede, agregando conhecimento e expertise no processo de tomada de decisão na aplicação de contramedidas em respostas a ataques em potencial.

Como trabalho futuro pretende-se agregar técnicas de mineração de dados e técnicas de recomendação para auxiliar as equipes de segurança na identificação de padrões nos dados das mensagens de alertas, potencializando a criação automática de contramedidas a serem aplicadas em resposta a eventos maliciosos.

Referências

Azevedo, R. P., Mozzaquatro, B. A., Nunes, R. C., Cappo, C., Schaerer, C., and Kozakevicius, A. (2012). Detecção de ataques dos utilizando a transformada wavelet 2d. In *Conferência Latinoamericana en Informática - CLEI*, Medelin, Colômbia.

Bastke, S., Deml, M., and Schmidt, S. (2010). Internet early warning systems - overview and architecture. In *European Workshop on Internet Early Warning and Network Intelligence*, Hamburg, Germany.

CERT.br (2012). Centro de estudos, resposta e tratamento de incidentes no brasil. Disponível em: ¡http://www.cert.br/¿. Acesso em: 25 out. 2012.

Chetan, R. and Ashoka, D. (2012). Data mining based network intrusion detection system: A database centric approach. In *Computer Communication and Informatics (ICCCI), 2012 International Conference on*, pages 1–6, Coimbatore, India.

Debar, H., Curry, D., and Feinstein, B. (2007). The intrusion detection message exchange format (idmef). RFC 4765. March 2007.

Flior, E., Anaya, T., Moody, C., Beheshti, M., Han, J., and Kowalski, K. (2010). A knowledge-based system implementation of intrusion detection rules. *Information Technology: New Generations (ITNG)*, pages 738–742.

Golling, M. and Stelte, B. (2011). Requirements for a future ews - cyber defence in the internet of the future. In *3rd International Conference on Cyber Conflict (ICCC)*, pages 1–16, Tallinn, Estonia.

Hesse, M. and Pohlmann, N. (2008). Internet situation awareness. In *eCrime Researchers Summit*, pages 1–9, Atlanta, GA.

More, S., Matthews, M., and A. Joshi, T. F. (2012). A knowledge-based approach to intrusion detection modeling. *Security and Privacy Workshops (SPW)*, pages 75–81.

Pereira, H. and Jamhour, E. (2011). Método heurístico para rotular grupos em sistema de detecção de intrusão baseado em anomalia. *XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Brasília - DF, Brasil.

Petri, G., Nunes, R. C., Junior, T. C., and Santos, O. M. (2012). Modelagem de uma base de conhecimento para o monitoramento de ataques. In *Escola Regional de Redes de Computadores*, pages 75–78, Pelotas, RS, Brasil. ERRC 2012.

Petri, G., Nunes, R. C., Orozco, V., Junior, T. C., and dos Santos, O. M. (2013a). Building situation awareness to monitor critical infrastructures. In *LADC 2013 - Fast Abstract*, Rio de Janeiro, Brazil.

Petri, G., Nunes, R. C., Orozco, V., Junior, T. C., and dos Santos, O. M. (2013b). Kbam: Data model of a knowledge base for monitoring attacks. In *LADC 2013 - Fast Abstract*, Rio de Janeiro, Brazil.

PRELUDE (2012). Prelude siem web site. Disponível em: ¡http://www.prelude-technologies.com/en/welcome/index.html¿. Acesso em: 29 jun. 2012.

Ricci, G. (2008). Betrachtung der vom ias gesammelten kommunikationsparameter auf relevanz zur anomalie und angriffserkennung (evaluation of the relevance for the detection of abnormalities and attacks of the communication parameters collected by the internet analysis system). Master's thesis, University of Applied Sciences, Gelsenkirchen, Germany.

Silva, P. F. and Westphall, C. B. (2006). An intrusion answer model compatible with the alerts idwg model. *Network Operations and Management Symposium (NOMS)*, pages 1–4.

SNORT (2012). Snort home page. Disponível em: ¡http://www.snort.org/¿. Acesso em: 11 jul. 2012.

SURICATA (2012). Open information security fundation. Disponível em: ¡http://96.43.130.5/index.php/downloads¿. Acesso em: 29 jun. 2012.

Symantec (2012). Symantec internet security threat report trends for 2011. Disponível em: ¡http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf¿. Acesso em: 15 jun. 2012.

Undercoffer, J., Joshi, A., Finin, T., and Pinkston, J. (2004). Using daml+oil to classify intrusive behaviours. *The Knowledge Engineering Review*, 18:221–241.

WIRESHARK (2012). Wireshark. Disponível em: ¡ http://www.wireshark.org/¿. Acesso em: 30 dez. 2012.

