Modelagem de uma Base de Conhecimento para o Monitoramento de Ataques

Giani Petri, Tarcisio Ceolin Junior, Raul Ceretta Nunes, Osmar Marchi dos Santos
Programa de Pós-Graduação em Informática – PPGI
Universidade Federal de Santa Maria - UFSM
{gpetri, ceolin, ceretta, osmar}@inf.ufsm.br

***Resumo*—A crescente popularização da Internet vem acompanhada do aumento no número de ataques às vulnerabilidades. Diante disto, há uma necessidade de obter um conhecimento sobre a rede para monitorar possíveis ataques. Este trabalho propõe uma base de conhecimento chamada KBAM e apresenta a modelagem dos dados. A base KBAM representa informações de diferentes aspectos da rede. O uso da base KBAM em um estudo de caso permitiu a obtenção de uma consciência situacional do ambiente monitorado.**

I. INTRODUÇÃO

A popularização da Internet vem acompanhada do aumento no número de aplicações *web* que trabalham com informações críticas. Em paralelo a isso, é notório o acréscimo no volume de dados que trafegam pelas redes de computadores, bem como o aumento substancial no número de ataques às vulnerabilidades encontradas [1].

Neste cenário, os sistemas tradicionais de detecção de intrusão (IDS) estão tornando-se limitados. A quantidade de dispositivos conectados à rede, *petabytes* de dados, *gigabytes* de informações transferidas já não estão mais sendo suportadas pelos IDSs tradicionais [2].

Para suprir a necessidade de monitorar a Internet perante este novo cenário, a construção de *Internet Early Warning Systems* tem sido explorada [3][4]. O objetivo destes sistemas é defender e proteger as funcionalidades da Internet, detectando precocemente as ameaças. Além disso, permitem obter uma consciência situacional (percepção da situação de segurança dos recursos de rede) que possibilita uma reação precoce a um evento malicioso, um maior controle e monitoramento dos recursos envolvidos, auxiliando em tomadas de decisões [2].

Para realizar o monitoramento de ataques é preciso uma base de conhecimento que contenha diferentes aspectos sobre a rede monitorada e que dê suporte para as decisões das equipes de segurança. Estes aspectos correspondem aos dados sobre o comportamento normal da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas [3].

Porém, os trabalhos existentes na literatura não englobam todos estes aspectos de uma base de conhecimento. Em [5] é proposto uma abordagem para detecção de intrusão utilizando redes neurais artificiais como mecanismo de detecção e uma base de conhecimento contendo assinaturas de ataques conhecidos para a fase de treinamento e aprendizagem, desconsiderando informações sobre medidas de respostas. Em [6] é apresentado um sistema que captura e analisa o tráfego de rede com o objetivo de criar uma base de conhecimento com regras que permita a tomada de decisões, porém esta proposta desconsidera o armazenamento de registros de incidentes.

Em [7] é proposta uma abordagem baseada em conhecimento para a modelagem de detecção de intrusão, mas essa abordagem também não engloba medidas de respostas. Em síntese, existem diversos trabalhos que envolvem bases de conhecimento na literatura, entretanto, os mesmos não abordam todos os aspectos básicos necessários para uma base de conhecimento conforme citado em [3].

Este trabalho propõe uma base de conhecimento chamada KBAM (*Knowledge Base for Attacks Monitoring*), que engloba os diferentes aspectos de uma base de conhecimento voltada ao monitoramento de ataques. A base KBAM representa os dados de eventos de detecção de intrusão explorando o formato padrão *Intrusion Detection Message Exchange Format* (IDMEF) [8] para as mensagens de detecção de intrusão e o formato *Intrusion Detection Response Exchange Format* (IDREF) [9] para as mensagens de respostas. A representação dos dados contidos na base KBAM contempla os seguintes aspectos: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta, estatísticas do tráfego da rede realizado através da coleta dos contadores dos parâmetros destacados em [10], além das assinaturas dos ataques já conhecidos.

Um estudo de caso realizado na rede da Universidade Federal de Santa Maria, demonstra que o uso da base KBAM permite a obtenção de uma consciência situacional do ambiente monitorado, pois fornece informações que possibilitam um conhecimento da atual situação de segurança da rede.

O restante do trabalho está organizado da seguinte forma. A seção II apresenta uma breve revisão bibliográfica, incluindo os trabalhos relacionados. A seção III apresenta a modelagem dos dados e destaca as principais tabelas e atributos da base KBAM. Na seção IV é realizada uma discussão sobre o uso da base KBAM e é apresentado um estudo de caso. Por fim, a seção V apresenta as conclusões do trabalho.

II. REVISÃO BIBLIOGRÁFICA

Uma base de conhecimento é um repositório de dados que agrupa informações referentes a uma área específica [11]. Na arquitetura de um *Internet Early Warning System* 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, ou antes de causar o máximo de perigo. Logo, criar uma consciência situacional, que corresponde a uma imagem da situação atual de segurança [3], depende das informações contidas na base.

De acordo com Bastke, Deml and Schmidt [3], as informações que devem ser armazenadas em uma base de conhecimento de um *Internet Early Warning System* devem corresponder aos seguintes aspectos: dados sobre o

comportamento normal da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas.

Os trabalhos existentes na literatura não atendem a todos estes aspectos de uma base de conhecimento. Lima et al. [5] propõem uma abordagem para detecção de intrusão através do uso de redes neurais artificiais. A proposta utiliza, nas fases de treinamento e aprendizagem, uma base de conhecimento com regras de detecção previamente definidas e utiliza as redes neurais como mecanismo para detectar variantes de intrusões.

Flior et al. [6] propõem um sistema que captura e analisa o tráfego de rede. O objetivo é criar uma base de conhecimento com regras a partir da fusão dos dados do comportamento normal e malicioso, coletados por múltiplos sensores. Entretanto, a proposta apresentada em [6] não engloba todos os aspectos básicos de uma base de conhecimento, desconsiderando o armazenamento de informações sobre incidentes e suas medidas de respostas. Em [7], More et al. apresentam um *framework* para uma abordagem ontológica que utiliza diversas fontes para a coleta dos dados de detecção de intrusão e logs. Porém, esta abordagem não armazena informações referentes as respostas aos alertas de detecção.

Na área de detecção de intrusão existem alguns padrões para interoperabilidade de mensagens de detecção e de respostas. Estes padrões, baseados em XML (*eXtensible Markup Language*), definem uma formatação dos dados para serem compartilhados. Um desses padrões é o IDMEF. Criado pelo grupo IDWG (*Intrusion Detection Work Group*), o IDMEF é um formato de dados padrão que sistemas de detecção de intrusão utilizam para reportar e compartilhar alertas sobre eventos considerados suspeitos [8]. O principal objetivo do formato IDMEF é definir uma formatação de dados e procedimentos para a interoperabilidade entre sistemas de detecção de intrusão.

Umas das principais aplicações do formato IDMEF é para a comunicação de alertas entre o componente de análise e o gerenciador de um IDS. Além disso, o formato IDMEF também pode ser usado para a troca de informações e correlação de alertas, além da possibilidade de padronização de informações em um banco de dados.

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 [9]. O IDREF é compatível com o modelo de alertas IDMEF, possibilitando assim, a integração dos dois modelos. O modelo IDREF, assim como o modelo IDMEF, também é orientado a objetos e suas classes foram projetadas com base nas informações contidas nos alertas formatados pelo modelo IDMEF.

III. Modelagem de uma Base de Conhecimento para o Monitoramento de Ataques

Esta seção apresenta o levantamento e a modelagem dos dados que estão representados na base KBAM.

A. Levantamento dos Dados

Os dados contidos na base KBAM representam os aspectos básicos de uma base de conhecimento, focando em incidentes de segurança específicos da área de detecção de intrusão.

1) Informações sobre alertas de detecção de intrusão

O registro de informações históricas sobre os incidentes de segurança é importante para o auxílio na confirmação de eventos futuros. Com enfoque em eventos de detecção de intrusão a base KBAM representa os dados dos alertas disparados por IDSs em acordo com os atributos do formato IDMEF. Por ser um formato padronizado e orientado a objetos, o IDMEF permite uma flexibilidade na extensão de informações de ataques, através dos mecanismos de herança e agregação.

2) Informações sobre medidas de respostas

A representação das respostas aplicadas aos eventos detectados está em acordo com as classes e atributos contidos no modelo de dados para troca de respostas de detecção de intrusão IDREF. Por ser um formato padrão similar ao IDMEF, os modelos possuem um forte relacionamento. Além disso, o formato IDREF também permite a representação de diversos tipos de respostas através de sua arquitetura orientada a objetos.

3) Informações sobre assinaturas de ameaças

As assinaturas de eventos maliciosos já conhecidos e aceitos pela comunidade científica estão representadas em arquivos de regras padronizadas, conforme utiliza o IDS Snort [12]. A utilização de regras definidas possibilita um aumento na precisão da confirmação de atividades maliciosas já consolidadas.

Neste trabalho, assume-se que a representação das assinaturas das ameaças é integralmente realizada pela ferramenta Snort. Desta forma, o ambiente monitorado em que é utilizada a base KBAM, também deve estar equipado com a ferramenta Snort, que fica responsável pela detecção de eventos maliciosos a partir das regras previamente definidas. Assim, não há uma representação das assinaturas de ameaças na base KBAM, ficando esta tarefa com responsabilidade irrestrita da ferramenta Snort.

4) Informações sobre o comportamento normal

Monitorar o tráfego de uma rede é essencial para obter uma visão de seu comportamento. O monitoramento dá-se através da quantificação dos dados sobre o tráfego que está ocorrendo em uma determinada rede. A quantificação é realizada através de um coletor, também conhecido como *sniffer*, que é responsável pela escuta e captura do que está acontecendo na rede e também pelo armazenamento desses dados.

Para criar uma visão real do comportamento, além de coletar estatísticas do tráfego é necessária a distribuição dos coletores em locais estratégicos do ambiente monitorado, para capturar informações em diferentes pontos da rede.

A seleção dos parâmetros quantificados a partir do tráfego da rede fundamenta-se nos descritores usados pela sonda do sistema IAS (*Internet Analysis System*) apresentado em [4] e detalhados em [10]. A sonda de um IAS trabalha de forma similar a um *sniffer*, realizando a captura de dados do tráfego de uma rede. Os parâmetros utilizados neste trabalho correspondem aos contadores dos protocolos TCP, ICMP, UDP, HTTP, SMTP, dentre outros.

B. Modelagem dos Dados

As informações armazenadas na base KBAM são representadas em um modelo relacional de dados. O modelo de dados é composto por 51 entidades que representam os dados dos alertas de detecção de intrusão,

as respostas a um alerta e as estatísticas sobre o tráfego da rede.

Os alertas de detecção de intrusão são representados através dos atributos do modelo IDMEF. A Figura 1 apresenta as principais entidades da base KBAM que armazenam informações sobre os alertas.

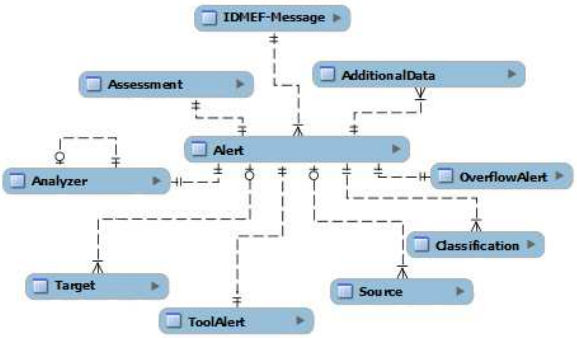

Figura 1. Principais entidades que representam os alertas de detecção.

Conforme mostra a Figura 1, a entidade que registra as informações referentes aos alertas disparados pelos detectores é a entidade *Alert*. O atributo *ident* armazena um identificador para o alerta, o instante da criação do alerta é armazenado no atributo *create-time*, o atributo *analyzer-time* armazena o momento em que o alerta foi disparado, já o instante em que o evento foi detectado está no atributo *detect-time*. A entidade *Alert* relaciona-se com as entidades *Assessment*, *Analyzer*, *Target*, *Source*, *ToolAlert*, *Classification*, *OverflowAlert* e *AdditionalData*.

A entidade *AdditionalData* armazena as informações que não se encaixam no modelo IDMEF. Já a entidade *OverflowAlert* representa informações específicas de alertas do tipo *overflow*. Por sua vez, a entidade *Assessment*, armazena as informações que permitem uma avaliação do evento causador do alerta. A entidade não possui atributos, porém relaciona-se com outras três entidades, *Impact*, *Action* e *Confidence*. Já a entidade *Analyzer* armazena informações referentes a identificação do analisador que originou o alerta. Os dados sobre o nome, a versão, classificação, modelo e fabricante do analisador ficam registrados nesta tabela, além de informações do tipo e versão do sistema operacional que o analisador atua. As entidades *Source* e *Target* correspondem, respectivamente, a possível origem e alvo do evento. Por sua vez, a entidade *Classification* registra uma possível classificação do tipo de alerta. A partir da classificação, o alerta pode ter alguma documentação externa que possua maiores informações referentes ao alerta gerado, essas informações ou *links* para os documentos ficam armazenadas na entidade *Reference*.

As principais entidades que representam os dados referentes as respostas aos alertas gerados estão modelados conforme apresenta a Figura 2.

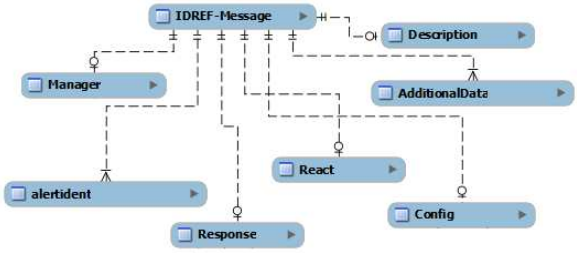

Figura 2. Entidades que representam as respostas aos alertas.

A principal entidade que representa uma resposta a um evento é a *IDREF-Message*. Esta entidade relaciona-se com *Response*, *React* e *Config*, que representam os tipos de respostas suportados pelo modelo IDREF.

O primeiro tipo de resposta é representado pela entidade *Response*, que representa o envio de informações cujo objetivo é avisar ou controlar um ataque. Uma resposta pode ser o envio de pacotes TCP e mensagem ICMP a um alerta ocorrido.

Outro tipo de resposta é através da alteração de configurações de um recurso do ambiente para conter um ataque, representada na entidade *Config*. Esta entidade relaciona-se com *Command* e *Resource*, que representam o(s) comando(s) a ser(em) executado(s) pelo recurso a ser configurado.

Além de permitir o envio de informações e a alteração de configurações, o modelo IDREF também permite a reação do ambiente contra um ataque. Este tipo de resposta é representado pela entidade *React* que possui dois relacionamentos, *Block* e *Shutdown*. As entidades *Block* e *Shutdown* representam respectivamente, o bloqueio e o fechamento de algum recurso.

A entidade *Resource* também está relacionada com as entidades *Block* e *Shutdown* e representa um recurso ao qual a resposta será aplicada. Um recurso pode ser um nó ou um serviço da rede, uma lista de usuários, uma lista de arquivos ou um processo do sistema operacional. Estes recursos são representados, respectivamente, pelas entidades: *Node*, *Service*, *UserList*, *FileList* e *Process*.

A quantificação dos dados capturados pelo *sniffer* para o captura dos contadores dos pacotes que trafegam na rede são armazenadas nas entidades apresentadas na Figura 3.

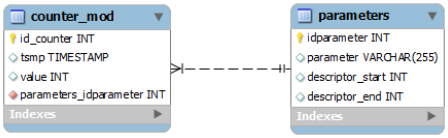

Figura 3. Entidades que representam a quantificação do tráfego da rede.

Conforme mostra a Figura 3, a entidade *parameters* contém todos os parâmetros que são 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. Por sua vez, 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 *parameters*.

IV. Discussão sobre o Uso da Base KBAM

Obter uma consciência situacional do ambiente monitorado requer um conhecimento dos dados que trafegam na rede, bem como uma ciência da atual situação de segurança dos recursos envolvidos [4]. As bases de conhecimento dos trabalhos existentes na literatura [5][6][7] não permitem a construção de uma consciência situacional, pois focam somente em aspectos específicos.

Em contrapartida, a base KBAM atende os diferentes aspectos para a construção de uma base de conhecimento. Desta forma, os dados dos aspectos armazenados na base KBAM fornecem informações para a obtenção de um

conhecimento da atual situação de segurança do ambiente monitorado, permitindo a criação de uma consciência situacional.

A construção de uma consciência situacional é realizada a partir de dados coletados em pontos estratégicos da rede monitorada. Mas há diversas maneiras de popular a base KBAM para criar uma consciência situacional. Uma das formas é apresentada no estudo de caso realizado na rede da Universidade Federal de Santa Maria, descrito a seguir.

O estudo de caso envolveu dois pontos de monitoramento para a coleta de dados na UFSM: a rede do setor responsável pelo Vestibular (Coperves) e a rede do Centro de Processamento de Dados (CPD).

A coleta dos alertas de detecção de intrusão foi realizada através do uso do *framework* Prelude. O Prelude destaca-se como uma ferramenta que integra vários sensores distribuídos e possui como principal componente em sua arquitetura o *Prelude-Manager*, que trabalha como um servidor que aceita conexões de sensores distribuídos e armazena os eventos recebidos em um banco de dados [13].

Os sensores utilizados no estudo de caso são os sistemas de detecção de intrusão baseados em assinaturas Snort, em sua versão 2.8.5.2-2 e o Suricata [14], na versão 1.2.1. Os sensores utilizam o formato IDMEF para enviar ao *Prelude-Manager* os eventos detectados. Os eventos são armazenados em um banco de dados modelado de acordo com os dados do formato IDMEF.

No estudo de caso foram utilizadas três máquinas virtuais (VMs) com o sistema operacional Ubuntu Server 10.04.4 LTS x86-32 e o VMware Workstation 8 como monitor das máquinas virtuais. Na infraestrutura implementada, uma das VMs faz o papel do gerenciador, ou seja, nela estão instalados o *Prelude-Manager* e o banco de dados. As outras duas VMs realizam o processo de coleta de dados, utilizando para isso, os sensores Snort e Suricata.

Os dados coletados através da ferramenta Prelude são exportados automaticamente por um *script* que realiza a inserção dos eventos coletados na base KBAM. Além disso, as duas VMs que hospedam os sensores, também hospedam um *sniffer* que realiza a captura do tráfego da rede e armazena nas entidades da base KBAM.

O *sniffer* utilizado no estudo de caso é uma adaptação ao coletor SniffStat2DB, apresentado em [15]. A adaptação realizada no SniffStat2DB refere-se a implementação para a captura de dados de parâmetros utilizados no escopo deste trabalho.

Para armazenar os dados referentes a respostas, foi implementado um componente que gera respostas a um alerta no formato IDREF. O componente atende aos requisitos descritos em [8], permitindo a seleção de um alerta em uma lista de alertas, gerando as respostas ao alerta selecionado e as armazena na base KBAM.

Como resultado do caso de estudo, observa-se que a base KBAM contém informações que permitem a construção de uma consciência situacional sobre a segurança não só nos setores monitorados da instituição.

V. CONCLUSÕES

O presente trabalho apresentou a modelagem dos dados da base de conhecimento KBAM. Armazenando dados sobre alertas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta e estatísticas do tráfego da rede, a base KBAM atende os diferentes aspectos necessários para a construção de uma base de conhecimento.

A realização de um estudo de caso na rede da Universidade Federal de Santa Maria permitiu coletar uma série de dados para inserir na base KBAM. Os dados coletados permitiram a obtenção de uma consciência situacional da rede da instituição.

Em um trabalho futuro, os dados coletados no estudo de caso serão minerados e utilizados para potencializar uma futura tomada de decisão das equipes de segurança.

REFERÊNCIAS

[1] Symantec Internet Security Threat Report Trends for 2011. April 2012. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_212393 64.en-us.pdf

[2] M. Golling and B. Stelte. “Requirements for a future EWS - Cyber Defence in the internet of the future,” in 3rd International Conference on Cyber Conflict (ICCC), Tallinn, Estonia, pp.1-16, June 7-10, 2011.

[3] S. Bastke, M. Deml and S. Schmidt. “Internet Early Warning Systems – overview and architecture,” European Workshop on Internet Early Warning and Network Intelligence, Hamburg, Germany, January 27, 2010.

[4] M. Hesse and N. Pohlmann. “Internet Situation Awareness,” in eCrime Researchers Summit, Atlanta, GA, pages 1-9, Oct. 2008.

[5] I. Lima, J. Degaspari and J. Sobral. “Intrusion detection through artificial neural networks,” in Network Operations and Management Symposium (NOMS), Salvador, Bahia, pages 867-870, April 7-11, 2008.

[6] E. Flior, T. Anaya, C. Moody, M. Beheshti, J. Han and K. Kowalski. “A knowledge-based system implementation of intrusion detection rules,” in Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, Las Vegas, NV, pages 738 –742, April 12-14, 2010.

[7] S. More, M. Matthews, A. Joshi, T. Finin. "A Knowledge-Based Approach to Intrusion Detection Modeling," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on* , pp.75-81, 24-25 May 2012.

[8] H. Debar, D. Curry and B. Feinstein. “The Intrusion Detection Message Exchange Format (IDMEF)”. RFC 4765. March, 2007.

[9] P. F. Silva and C. B. Westphall. “An Intrusion Answer Model Compatible with the Alerts IDWG Model,” in Network Operations and Management Symposium (NOMS), Vancouver, BC, pages 1-4, April 3-7, 2006.

[10] G. Ricci. “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, 2008.

[11] S. Russel, P. Norving. “Artificial Inteligence: A modern approach,” Prentice Hall, New York, 1st Edition, 1995.

[12] M. Roesch and S. Telecommunications. “Snort - lightweight intrusion detection for networks,” in 13TH USENIX CONFERENCE ON SYSTEM ADMINISTRATION. Proceedings, Seattle, Washington: USENIX Association, pages 229–238, 1999.

[13] PRELUDE. Disponível em: <http://www.prelude-technologies.com/en/welcome /index.html>. Acesso em: jun. 2012.

[14] SURICATA. Open Information Security Fundation. Disponível em: <http://96.43.130.5/index.php/downloads> Acesso em: jun. 2012.

[15] A. H. Schmidt. “Sniffstat2DB: Uma Ferramenta para Coleta e Armazenamento dos Contadores do Tráfego de uma Rede” Trabalho de Graduação. Universidade Federal de Santa Maria, Santa Maria, 2009.