Monitorando Ataques com a Ferramenta Prelude

Giani Petri[1], Tarcisio C. Junior[1], Raul Ceretta Nunes[1], Osmar M. dos Santos[1]

[1]Programa de Pós-Graduação em Informática – PPGI
Universidade Federal de Santa Maria – UFSM
Av. Roraima, 1000 – 97.105-900 – Santa Maria – RS – Brasil

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

Abstract. *The number of attacks exploiting vulnerabilities has grown exponentially in recent years. This fact has stimulated and cognized enterprises and institutions to invest in tools to gain knowledge about the network and to monitor potential attacks. This paper proposes the use of Prelude as a system manager implemented an infrastructure to monitor attacks on a network of computers. A case study carried out in the network of an educational institution allowed an effective monitoring of the institution's network, identifying security events and alerting security teams to potential attacks.*

Resumo. *O número de ataques explorando vulnerabilidades tem crescido exponencialmente nos últimos anos. Este fato tem conscientizado e estimulado as empresas e instituições a investir em ferramentas para obter um conhecimento sobre a rede e monitorar possíveis ataques. Este trabalho propõe a utilização do Prelude como um sistema gerenciador de uma infraestrutura implementada para monitorar ataques em uma rede de computadores. Um estudo de caso realizado na rede de uma instituição de ensino superior permitiu um efetivo monitoramento da rede da instituição, identificando eventos de segurança e alertando as equipes de segurança para ataques em potencial.*

1. Introdução

A Internet já é amplamente utilizada pela sociedade, auxiliando na efetivação de negócios, transações comerciais e também na realização de tarefas pessoais. A rapidez na comunicação, no acesso e compartilhamento de informações potencializou a sua popularização. Em paralelo a esse fenômeno é notório o aumento no volume de dados que trafegam pelas redes de computadores e um acréscimo substancial no número de ataques que exploram as vulnerabilidades existentes [Symantec 2011].

Diante deste cenário, os sistemas tradicionais de detecção de intrusão (IDS) estão tornando-se obsoletos. A crescente quantidade de dispositivos conectados à rede, gerando *petabytes* de dados e *gigabytes* de informações transferidas já não estão mais sendo suportadas pelos IDSs tradicionais [Golling and Stelte 2011].

Para suprir a necessidade de monitorar os ataques perante este novo cenário, a construção de *Internet Early Warning Systems* tem sido explorada [Bastke et al. 2010] [Hesse and Pohlmann 2008]. 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 [Golling and Stelte 2011].

A infraestrutura de um *Internet Early Warning System* ainda é um problema de pesquisa em aberto. Apel et al. (2009) apresentam um arquitetura de um *Early Warning System* de grande porte, que trabalha em nível nacional. A arquitetura é composta por componentes para coleta e análise de intrusões e *malwares*, além de criar de forma automática novas assinaturas de acordo com o comportamento dos dados analisados [Apel et al. 2009].

Em [Engelberth et al. 2010] é apresentada uma visão geral da estrutura do *InMas*, uma plataforma modular para monitoramento em larga escala de *malwares* na Internet. A estrutura do *InMas* integra diversas ferramentas para coleta e análise de *malwares*, com o objetivo de detectar precocemente a ocorrência de eventos causados por *softwares* maliciosos.

Em [Bsufka et al. 2006] é apresentado uma abordagem para um sistema de alertas precoce baseado em agentes para infraestruturas críticas. Na abordagem proposta, há uma combinação com mecanismos de segurança existentes (*firewalls* e IDSs) com novas abordagens para criar uma visão global e determinar o atual estado de ameaça. Em síntese, as propostas existentes na literatura, tendem a construir uma arquitetura de grande porte e que englobam uma diversidade de componentes.

Uma ferramenta livre e que permite a construção de uma infraestrutura de maneira similar a um *Internet Early Warning System* é o Prelude [Prelude 2012]. O Prelude é definido como um gerenciador de eventos de segurança da informação e permite a unificação de vários tipos de aplicações ou sensores, com código-fonte proprietário ou livre, em um sistema centralizado. O Prelude utiliza o padrão IDMEF (*Intrusion Detection Message Exchange Format*) [Debar et al. 2007] que permite que diferentes tipos de sensores criem eventos utilizando o mesmo padrão de comunicação.

Este trabalho propõe a utilização do Prelude como um sistema gerenciador de uma infraestrutura proposta de forma similar a um *Internet Early Warning System*. A infraestrutura é composta por sensores alocados em pontos estratégicos da rede para realizar o monitoramento dos ataques. Os sensores encaminham os alertas de ataques para um componente centralizado que os armazena em um banco de dados e disponibiliza, através de uma interface *web*, o estado dos sensores, as estatísticas e eventos de segurança identificados durante o monitoramento.

Um estudo de caso realizado na rede da Universidade Federal de Santa Maria (UFSM) permitiu um efetivo monitoramento da rede da instituição, identificando eventos de segurança, alertando para possíveis ataques. A infraestrutura construída com o Prelude é gerenciada através da interface *Prewikka*, que permite a visualização dos alertas disparados pelos sensores, auxiliando as equipes de segurança em tomadas de decisão de resposta a um evento.

O restante do artigo está estruturado da seguinte forma. A seção 2 apresenta os trabalhos relacionados. A seção 3 descreve a proposta da utilização do Prelude como um gerenciador da infraestrutura para monitorar ataques. Na seção 4 é apresentado um estudo de caso realizado para validar a proposta. Por fim, a seção 5 apresenta as conclusões do trabalho.

2. Trabalhos Relacionados

O crescente número de ataques ocorridos nos últimos anos vem estimulando a conscientização de empresas e instituições a investir tempo e dinheiro em mecanismos para aumentar o nível de segurança. Na medida em que o volume de dados que trafega nas redes de computadores aumenta consideravelmente a cada instante, os tradicionais sistemas de detecção de intrusão utilizados pelas empresas tornam-se obsoletos para processar e analisar grandes quantidades de dados.

Em contrapartida, pesquisadores vêm propondo soluções que exploram a construção de *Internet Early Warning Systems*. Estes sistemas trabalham no monitoramento de ambientes de rede e seu principal objetivo é detectar ameaças com antecedência, antes que elas possam causar qualquer perigo, ou antes de causar o máximo de perigo [Golling and Stelte 2011]. Além disso, estes sistemas auxiliam na construção de uma consciência situacional do ambiente, criando uma imagem de segurança dos recursos de rede, auxiliando a equipe de segurança em tomadas de decisão.

Em [Apel et al. 2009] é apresentada um arquitetura de um *Early Warning System*, que trabalha a nível nacional. A arquitetura é composta por quatro módulos básicos. O módulo *Collecting and Learning* (CL) corresponde aos componentes para coleta de *malwares* e efetiva análise para geração de padrões apropriados. O módulo *Threat Repository* é usado para centralizar e gerenciar as informações dos *malwares* e detectar critérios entregues pelo módulo CL. O repositório fornece informações para a detecção de eventos para o módulo *Detecting and Alerting* (DA), que contém os componentes funcionais para detectar violações de segurança e para gerar respectivos alertas. Os alertas gerados pelo módulo DA, bem como informações sobre *malwares* fornecidos pelo repositório de ameaças, possibilitam a construção de uma imagem da situação do ambiente monitorado e são gerenciados no módulo *Alert Repository*.

Engelberth et al. (2010) apresentam a estrutura do *InMas*, uma plataforma modular para monitoramento de eventos maliciosos na Internet. O foco dos autores é o monitoramento de *malwares* em larga escala. A estrutura do *InMas* possui o *honeypot Nepenthes* responsável por emular as vulnerabilidades para a coleta de informações sobre potenciais ataques e a ferramenta de análise de *malwares* dinâmicos *CWSandbox*. Além disso, a estrutura possui uma interface gráfica para auxiliar os administradores e analistas. A interface apresenta os resultados das análises realizadas e permite que os administradores configurem o ambiente, adicionando e removendo sensores e criando regras de classificação para a análise de algumas ferramentas [Engelberth et al. 2010].

Bsufka et al. (2006) apresentam um *Early Warning System* para infraestruturas críticas. A proposta baseia-se na utilização de ferramentas de segurança já existentes, tais como *firewalls* e sistemas de detecção de intrusão. Além disso, os autores propõem a utilização de sensores baseados em agentes para detecção de eventos em *hosts* e redes [Bsufka et al. 2006].

A literatura atual destaca diversos trabalhos que apresentam propostas para monitorar eventos de segurança nesse novo cenário da Internet. Os trabalhos exploram a construção de *Internet Early Warning Systems* para a realização de um efetivo monitoramento nos ambientes, possibilitando a detecção de ataques antes que eles causem alguma consequência.

3. Monitorando Ataques com a Ferramenta Prelude

Uma ferramenta que permite a construção de uma arquitetura similar a um *Internet Early Warning System* é o Prelude [Prelude 2012]. O Prelude destaca-se como uma ferramenta que integra vários sensores distribuídos e possui um componente principal que trabalha como gerenciador da arquitetura. Definido como um *Security Information Management* (SIM), o Prelude coleta, normaliza, classifica, agrega e reporta todos os eventos relacionados a segurança, independentemente da licença dos sensores utilizados [Prelude 2012].

A infraestrutura implementada, para realizar o monitoramento de ataques, tem como base o uso do *framework* Prelude. A utilização do Prelude permite a integração de sensores distribuídos e localizados em pontos estratégicos da rede. Estes sensores são configurados para comunicarem-se com um componente centralizado do Prelude que realiza a inserção dos dados no banco de dados. O componente gerenciador da arquitetura é o *Prelude-Manager* que trabalha como um servidor que aceita conexões de sensores distribuídos e armazena os eventos recebidos em um banco de dados.

Os sensores utilizados na infraestrutura implementada são os sistemas de detecção de intrusão Snort e Suricata. O Snort é um sistema de detecção de intrusão para rede (NIDS), um dos mais populares IDS existentes, sua popularização dá-se através da flexibilidade nas configurações de regras e constante atualização frente às novas ferramentas de invasão [Roesch and Telecommunications 1999]. O Snort é um IDS baseado em assinaturas e possui um amplo cadastro de assinaturas para a detecção de intrusos. Além disso, o Snort possui uma constante atualização em seu código-fonte e regras de assinaturas [Snort 2012].

O outro sensor integrado a arquitetura do Prelude é o Suricata [Suricata 2012]. O Suricata é um IDS *open-source*, considerado uma ferramenta da nova geração para a detecção de intrusão e prevenção. Como é um sistema *multi-thread*, oferece maior velocidade e eficiência na análise do tráfego de rede [Suricata 2012].

A Figura 1 apresenta a infraestrutura implementada através do uso do Prelude e seus componentes.

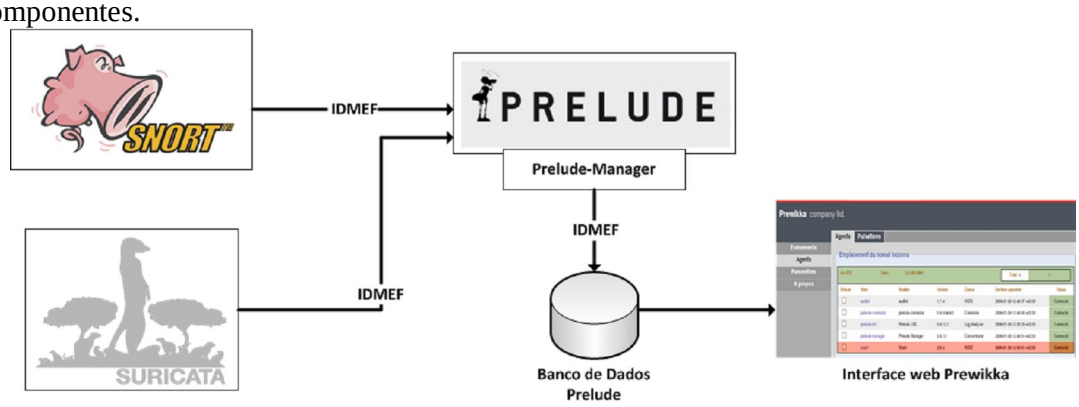

Figura 4. Infraestrutura para o Monitoramento de Ataques

Conforme apresenta a Figura 1 os IDSs (Snort e Suricata) são responsáveis pela detecção dos eventos maliciosos e encaminhá-los para o gerenciador *Prelude-Manager*. A comunicação entre os sensores e o *Prelude-Manager* é realizada através do formato IDMEF (*Intrusion Detection Message Exchange Format*).

O modelo IDMEF, criado pelo grupo IDWG (*Intrusion Detection Work Group*), é um formato de dados 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 um padrão de 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. Os dados do formato IDMEF são modelados em uma série de classes, definidas através de DTD (*Document Type Definition*) XML [Debar et al. 2007].

Em seguida, o gerenciador *Prelude-Manager* realiza o processo de inserção dos eventos no banco de dados para análise da equipe de segurança através de uma interface *web*.

A administração da infraestrutura é realizada através da interface *web Prewikka*. A interface permite visualizar alertas gerados pelos sensores, além de possibilitar o gerenciamento e identificar os estados dos sensores, assim como estatísticas de todos os alertas e atividades do IDS integrados, potencializando uma visão de toda infraestrutura implementada, auxiliando a equipe de segurança no processo de tomada de decisão.

Além disso, a coleta dos eventos de segurança realizada em pontos estratégicos da rede permite à equipe de segurança um entendimento e compreensão dos eventos que estão ocorrendo no ambiente de rede monitorado. Desta forma, proporcionando a construção de uma consciência situacional do ambiente, para a percepção do estado de segurança dos recursos da rede.

4. Validação

Para validar a integração dos componentes e a infraestrutura implementada foi realizado um estudo de caso utilizando dois pontos para a coleta de dados de eventos maliciosos na rede da Universidade Federal de Santa Maria. O estudo de caso envolveu as redes do setor responsável pelo vestibular (Coperves) e do Centro de Processamento de Dados (CPD), da referida universidade.

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* na versão 0.9.15-4, o banco de dados e a interface *Prewikka*. As outras duas VMs realizam o processo de coleta de dados, os sensores utilizados na infraestrutura implementada são os sistemas de detecção de intrusão Snort em sua versão 2.8.5.2-2 e o Suricata, na versão 1.2.1.

Após a instalação e configuração dos IDSs para se comunicarem com o *Prelude-Manager*, foi necessário registrar cada IDS para efetivamente trabalhar como um sensor do Prelude. As duas VMs estão alocadas na infraestrutura, uma para coletar dados da rede do CPD e a outra da Coperves.

Ao identificar algum evento malicioso, compatível com as regras de detecção dos IDSs, os sensores criam um alerta e enviam os dados formatados com o padrão IDMEF para o componente *Prelude-Manager*, que por sua vez, realiza o processo de armazenar os alertas no

banco de dados. O banco de dados utilizado é o PostgreSQL na versão 8.4 [PostgreSQL 2012] que está modelado de acordo com os dados do formato IDMEF.

Os sensores estão ativos realizando a coleta de dados de forma permanente. A interface *Prewikka* possibilita a visualização dos estados de cada sensor integrado. A interface que apresenta os estados de cada sensor utilizado pode ser observada na Figura 2.

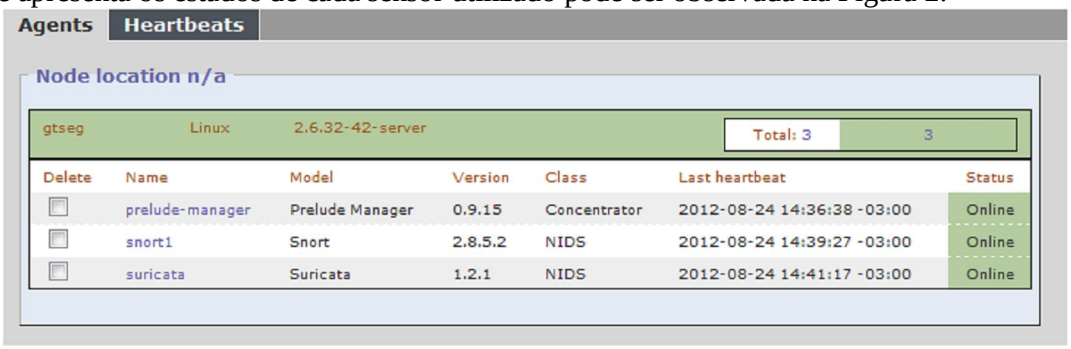

Figura 2. Estados dos sensores utilizados no estudo de caso.

Além dos estados dos sensores a interface *web Prewikka* permite identificar o montante de alertas gerados por cada sensor, os detalhes de cada alerta, destacando a hora da detecção, a origem e o alvo do evento e também uma classificação inicial da gravidade do alerta, dentre outros.

A Figura 3 apresenta uma lista dos alertas detectados na rede da UFSM e que estão classificados de acordo com seu nível de gravidade, definido pelos IDSs. Os alertas em cor vermelha representam os eventos com uma gravidade alta, os eventos em cor laranja destacam os alertas com gravidade média e os eventos em cor verde são os alertas com gravidade baixa. Além do nível de gravidade destacado pelas cores, é possível identificar a origem e o destino do ataque, representados respectivamente nas colunas *Source* e *Target*, além da data e hora de geração do evento e o sensor (*Analyzer*) que disparou o alerta.

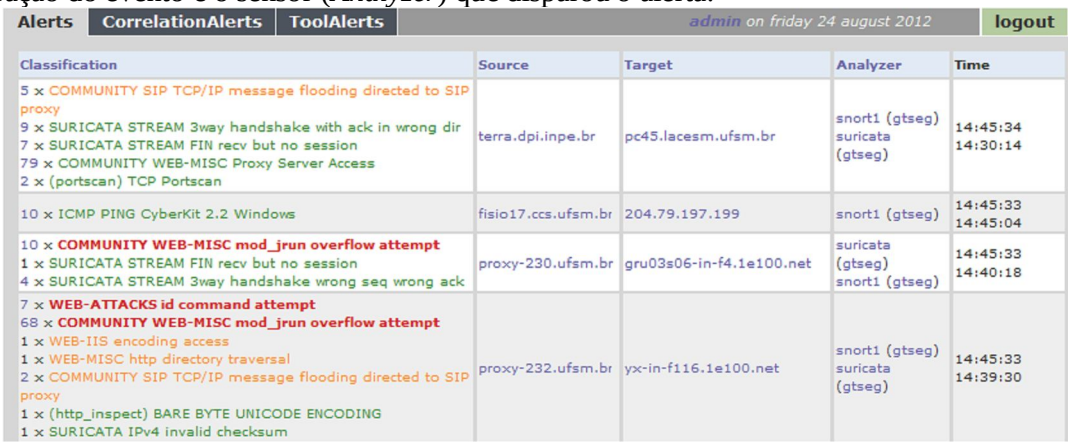

Figura 3. Lista de alertas detectados na rede da UFSM.

A interface *Prewikka* possibilita também a criação de filtros que permite a compreensão dos eventos ocorridos no ambiente monitorado e potencializa a obtenção da consciência situacional. A utilização de filtros facilita a identificação das principais origens e alvos dos eventos, além de visualizar os alertas de ataques mais ocorridos e a partir destas informações implementar medidas preventivas para aumentar o nível de segurança do ambiente de rede.

Através da interface também é possível gerenciar os sensores integrados e visualizar todas as informações capturadas no ambiente monitorado, permitindo uma ampla visão sobre o funcionamento da infraestrutura implementada, auxiliando a equipe de segurança em tomadas de decisões.

5. Conclusões

A popularização do uso da Internet juntamente com o aumento gradativo no número de ataques potencializaram a criação de novas infraestruturas para o monitoramento de ataques, cujo objetivo é aumentar o nível de segurança da informação e dos sistemas computacionais.

Ao trabalhar de forma similar a um *Internet Early Warning System* o Prelude destaca-se como uma ferramenta bastante completa para monitorar os eventos de uma rede através da integração de sensores distribuídos.

A infraestrutura proposta utilizada no estudo de caso realizado nas redes da Coperves e do CPD da Universidade Federal de Santa Maria possibilitou a realização de um efetivo monitoramento dos eventos de segurança ocorridos na rede da instituição.

O estudo de caso permitiu a identificação de um grande número de alertas de ataques em potencial. Além disso, através do uso da interface *Prewikka* foi possível realizar uma análise detalhada nos alertas de ataques, identificando a classificação do alerta, sua gravidade, além da origem e destino do evento. E ainda, permitiu a compreensão dos eventos de segurança ocorridos no ambiente monitorado, dando suporte à equipe de segurança para a tomada de decisões de medidas para minimizar as possíveis consequências ocasionadas pelos eventos.

Em um trabalho futuro, o componente *Prelude-Correlator* será integrado a infraestrutura do Prelude. Através do uso deste componente será possível correlacionar, em tempo real, os vários eventos gerados a partir de diferentes sensores.

Referências

Apel, M., Biskup, J., Flegel, U., and Meier, M. (2009). Early warning system on a national level – project amsel. In *4th International Workshop on Critical Information Infrastructure Security*.

Bastke, S., Deml, M., and Schmidt, S. (2010). Internet early warning systems – overview and architecture. In *1st European Workshop on Internet Early Warning and Network Intelligence (EWNI)*, Hamburg, Germany.

Bsufka, K., Kroll-Peters, O., and Albayrak, S. (2006). Intelligent network-based early warning systems. In *Critical Information Infrasturctures Security First International Workshop*, Samos Island, Greece.

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

Engelberth, M., Freiling, F. C., G¨obel, J., Gorecki, C., Holz, T., Hund, R., Trinius, P., and Willems, C. (2010). The inmas approach. In *1st European Workshop on Internet Early Warning and Network Intelligence (EWNI)*, Hamburg, Germany.

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

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

PostgreSQL (2012). Postgresql, inc. Disponível em: http://www.pgsql.com/. Acesso em: 05 set. 2012.

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

Roesch, M. and Telecommunications, S. (1999). Snort - lightweight intrusion detection for networks. In *13th USENIX CONFERENCE ON SYSTEM ADMINISTRATION*, pages 229 – 238, Berkeley, CA, USA. USENIX Association.

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 (2011). Symantec internet security threat report trends for 2011. Disponível em: http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_ report_2011_21239364.en-us.pdf. Acesso em: 15 jun. 2012.