16º WRNP Workshop RNP

18 | 19 MAIO
VITÓRIA | ES

PROTÓTIPO

GT-EWS
Mecanismos para um sistema de alerta antecipado

Equipe
Daniel Macêdo Batista
Luiz Arthur Feitosa dos Santos
Rodrigo Campiolo
Higor Luiz Farinha Celante
Italo Valcy da Silva Brito
Rafael Brito Gomes
Rafael Silverio Amaral
Rogério de Carvalho Bastos
Wagner Aparecido Monteverde

Parcerias
USP
UTFPR
UFBA
PoP-BA

Site
https://www.pop-ba.rnp.br/GTEWS/

Contato
Gerência do Programa de GT-RNP: **ggt@rnp.br**

Descrição

Os sistemas de alerta antecipado, em inglês, *Early Warning Systems* (EWS), visam detectar e prever possíveis ameaças de ataques baseados no comportamento dos sistemas, gerando alertas de situações que apresentam padrões de risco. O intuito é desencadear mecanismos reativos antecipadamente, a fim de evitar ou diminuir os danos causados por um ataque. Em síntese, os sistemas de alerta antecipado permitem estabelecer hipóteses e predições correlacionando informações incertas e incompletas providas por sensores em uma rede.

O GT-EWS tem por objetivo desenvolver uma ferramenta para monitorar atividade maliciosa e detectar antecipadamente eventos e incidentes de segurança. Esse objetivo será alcançado por meio da correlação e análise de dados providos por sensores de redes tradicionais e outras fontes, como redes sociais, fóruns e registros de redes virtuais. A ferramenta poderá ser utilizada também para monitorar o uso de nomes de instituições em fóruns e redes sociais, alertando possíveis orquestrações de atividades maliciosas.

A Figura 1 exibe uma visão em alto nível da execução da ferramenta, no momento em que ela correlaciona dados de várias fontes e antecipa para o usuário sobre uma falha causada por um *bug* no servidor *web* Apache.

Como contribuição para a RNP, espera-se que essa ferramenta auxilie os processos de segurança da informação, em especial a detecção e resposta a incidentes de segurança. A ferramenta também poderá ser oferecida como um serviço de detecção de atividade maliciosa e monitoramento de padrões para as suas instituições usuárias. É importante destacar ainda a contribuição científica do GT-EWS, que é a avaliação de novos sensores e o fornecimento de evidências empíricas do uso de técnicas de recuperação de informação para suportar novas arquiteturas de EWS.

O protótipo da ferramenta pode ser acessado em http://gtews.cm.utfpr.edu.br/ews/.

Demonstração

Há duas simulações que serão demonstradas:

Simulação 1

Detecção de tentativas de ataque por meio da orquestração desse ataque no Twitter: um grupo de atacantes realizará a orquestração de um ataque de DDoS via Twitter contra uma universidade. As mensagens postadas por esses atacantes serão simuladas e identificadas pela ferramenta, que alertará o administrador de rede sobre o ataque antes dele acontecer. Essa primeira simulação será realizada em conjunto com o GT-Actions (Ambiente computacional para tratamento de incidentes com ataques de negação de serviço) para mostrar o passo seguinte que um administrador executaria, que seria ativar a ferramenta do GT-Actions para tomar medidas preventivas contra o ataque de DDoS.

Simulação 2

Detecção de anúncios de vulnerabilidades em sistemas antes do seu anúncio em mídias tradicionais: vulnerabilidades recentes relacionadas a *softwares* encontrados em diversos clientes da RNP serão exibidas e será mostrado que elas foram detectadas pela ferramenta antes de serem informadas por fontes tradicionais que divulgam informações sobre vulnerabilidades.

A Figura 2 resume o procedimento a ser simulado nas demonstrações.

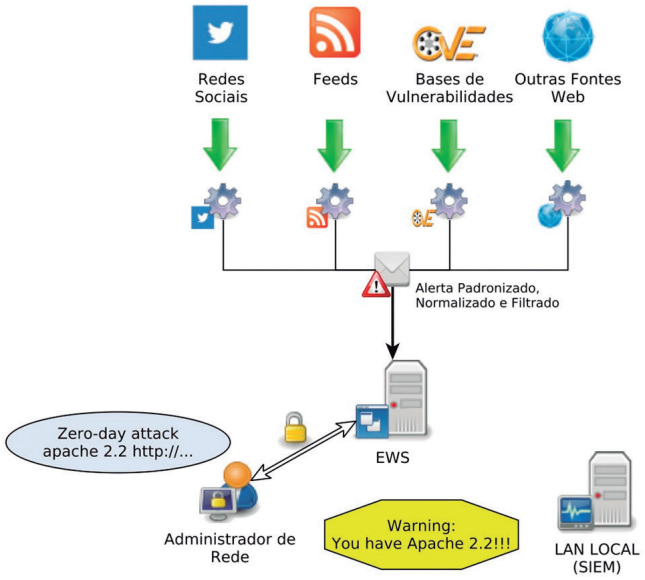

Figura 1: Visão alto nível da ferramenta do EWS.

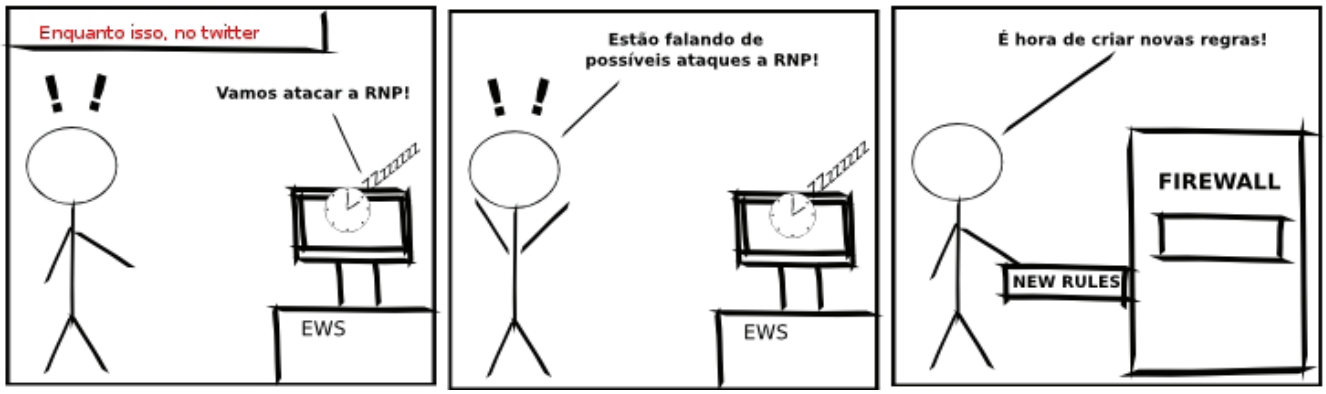

Figura 2: Procedimento de um administrador que usará a ferramenta do GT-EWS.