16º WRNP Workshop RNP

18 | 19 MAIO
VITÓRIA | ES

PROTÓTIPO

GT-Actions

Ambiente computacional para tratamento de incidentes com ataques de negação de serviço

Equipe

Iguatemi E. Fonseca
Vivek Nigam
Leandro C. Almeida
Helio Waldman
Moises R. N. Ribeiro
Yuri G. Dantas
Eduardo S. Gama
Breno Frizera
Pedro Cleis
Sabrina Felix
Joanacelle Caldas
Aellison Cassimiro
Lucas Aversari
Fabrício L. Soares
João Henrique Corrêa

Site
http://www.lar-ufpb.net/gt.html

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

Descrição

Segundo relatórios do Centro de Atendimento a Incidentes de Segurança da RNP (CAIS/RNP), ataques DDoS (*Distributed Denial-of-Service*) na rede Ipê têm ocorrido com frequência entre 2009 e 2013, sendo, portanto, um dos principais desafios da segurança na internet. Sites comerciais, acadêmicos e governamentais, como o do governo federal, são alvos frequentes desses incidentes. Ataques DDoS têm uma grande capacidade de mudança e assumem novas características. Portanto, em vez de construir defesas específicas para ataques DDoS específicos, é mais importante desenvolver uma metodologia para adequar rapidamente os algoritmos para o tratamento de novas versões de ataques. A Figura 1 mostra uma ilustração de um ataque DDoS.

Ao partir de dois protótipos em desenvolvimento pelos proponentes, esse projeto trata da concepção de uma plataforma computacional para tratamento em tempo real de ataques DDoS e a proposta de uma metodologia para invenção de novos algoritmos.

O objetivo principal do GT-Actions é desenvolver uma plataforma computacional, metodologias e técnicas para tratamento de ataques de negação de serviço (DDoS). Para isso, com base na modelagem matemática e análise do perfil do tráfego dos ataques, será implementada uma ferramenta computacional, chamada Actions (Ambiente computacional para tratamento de incidentes com negação de serviço), que seja capaz de tomar medidas preventivas contra ataques DDoS em tempo real.

O Actions será implementado por meio de *software* livre e código desenvolvido pela equipe científica e poderá ser instalado nas instituições que fazem uso da rede Ipê.

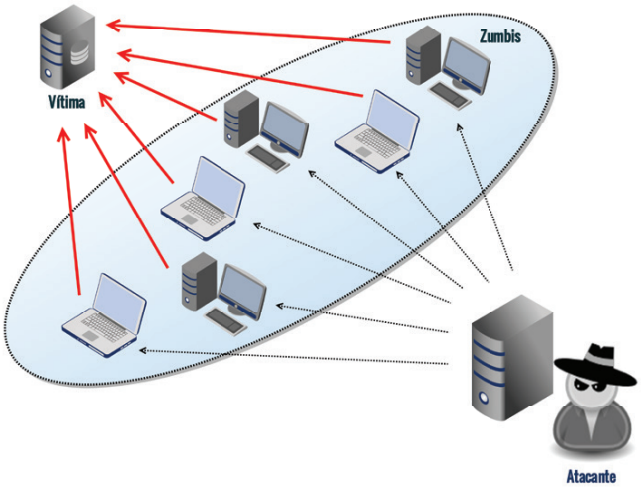

Figura 1: Ilustração de um ataque DDoS.

Demonstrações

O GT-Actions programou três demonstrações para o WRNP. Na primeira, a ferramenta de defesa contra ataques DDoS na camada de aplicação (chamada de SeVen – *Selective Verification in Application Layer*) será testada em um cenário em que o tráfego do ataque será gerado em máquinas localizadas no próprio estande, ou seja, de forma local ou em rede local (LAN), como mostrado na Figura 2.

Na segunda demonstração, as máquinas que realizarão o ataque estarão localizadas nos campi da Universidade Federal da Paraíba (UFPB) e Instituto Federal da Paraíba (IFPB), em João Pessoa, ou seja, o ataque será realizado no contexto de uma rede de longa distância (WAN) e terá como alvo um servidor web localizado na Universidade Federal do Espírito Santo (Ufes), em Vitória, como visto na Figura 3. Em ambos os casos, o alvo será um servidor web, que provê acesso aos serviços do protocolo HTTP.

A terceira demonstração será feita em conjunto com o GT-EWS (Mecanismos para um sistema de alerta antecipado), e a ideia é utilizar um mecanismo de alerta para identificar que o ataque DDoS está sendo orquestrado.

Durante as demonstrações, serão disponibilizadas, em tempo real, informações sobre monitoramento do tráfego tanto de usuários legítimos quanto de atacantes, disponibilidade e, tempo de resposta do servidor *web* a uma requisição entre outras.

Figura 3: Experimento em rede WAN, em recorte da rede Ipê.

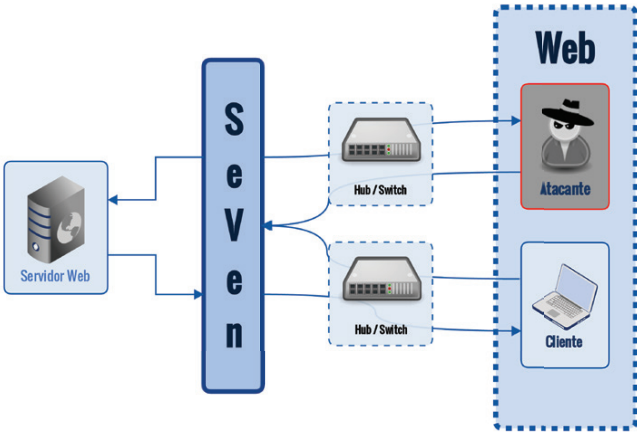

Figura 2: Experimento em rede LAN.