17º WRNP Workshop RNP

30 | 31 MAIO
SALVADOR | BA

PILOTO

GT-Actions
Ambiente Computacional para Tratamento de Incidentes com Ataques de Negação de Serviço

EQUIPE

Iguatemi E. Fonseca
Moisés R. Nunes Ribeiro
Vivek Nigam
Leonardo C. Almeida
Hélio Waldman
Yuri G. Dantas
Eduardo S. Gama
Marcílio O. O. Lemos
Roberto O. S. Junior
Sabrina F. Bertuani
Rafael B. M. Carvalho
Túlio Pascoal
Lucas Aversari
Gustavo B. Sampaio
João Henrique Corrêa

Parceiros

Coordenação de Aperfeiçoamento de Pessoal do Nível Superior (Capes)
Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)
Instituto Federal da Paraíba (IFPB)
Universidade Federal do Espírito Santo (Ufes)
Universidade Federal do ABC (UFABC)
Universidade Federal da Paraíba (UFPB)
Universidade Estadual de Campinas (Unicamp)

SITE

http://lar-ufpb.net/

CONTATO

Gerência de Grupos de Trabalho da RNP
ggt@rnp.br

DESCRIÇÃO

Ataques DDoS (*Distributed Denial-of-Service*) representam um dos principais desafios de segurança na internet e têm ocorrido com frequência na rede Ipê entre 2009 e 2015, segundo relatórios do Centro de Atendimento a Incidentes de Segurança da RNP (CAIS). Sites comerciais, acadêmicos e governamentais, como por exemplo o do governo federal, são alvos frequentes. Devido à sua grande capacidade de mudança em assumir novas características, é preciso desenvolver estratégias para mitigar tais ataques (Figura 1).

O principal objetivo da Fase 1 do GT-Actions foi desenvolver um protótipo de defesa, chamado SeVen (*Selective Verification in Application Layer*), implementado com *software* livre e código desenvolvido pela equipe científica, contra ataques DDoS na camada de aplicação. Depois, a sua eficiência foi validada por meio de simulações e experimentos na rede. Nessa primeira fase, foram alcançados os seguintes resultados: a) foi desenvolvida uma estratégia inédita na literatura; b) essa defesa foi formalizada pelo uso de ferramentas do estado da arte em métodos formais; c) a mesma foi validada por simulações que exploram o protocolo HTTP; d) implementou-se um protótipo de SeVen em C++; e) a eficiência da defesa foi validada por meio de experimentos na rede. Esses experimentos mostraram que um servidor Apache de pequeno a médio porte (200 conexões simultâneas) fica indisponível na presença de um ataque Slowloris ou POST quando não rodando SeVen, mas fica disponível a 95% dos clientes na presença do mesmo ataque quando rodando SeVen.

Como principais resultados a serem alcançados ao final da Fase 2 do projeto, podem-se destacar:

1. O desenvolvimento e aprimoramento de estratégias de defesas seletivas para o tratamento de ataques DDoS;
2. A concepção de uma metodologia para criação de novas defesas contra ataques DDoS;
3. A consolidação do protótipo desenvolvido na Fase 1;
4. A implantação de pilotos em diversas instituições parceiras, como a UFPB, Ufes, UFBA, PoP-SC, a Universidade do Sul de Santa Catarina (Unisul), a Universidade Estadual de Ponta Grossa (UEPG), o fone@RNP e a Flexa Information Technology (http://www.flexait.com.br).

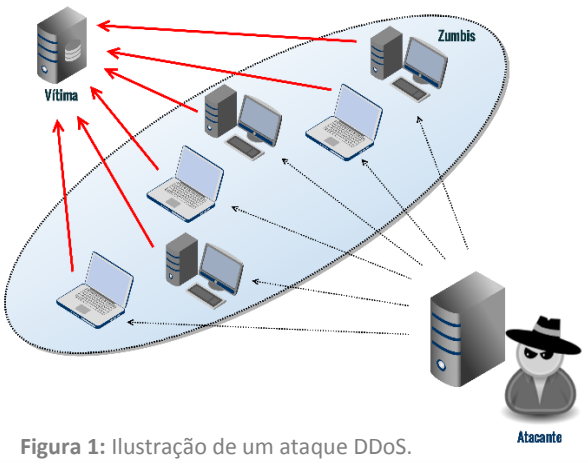

Figura 1: Ilustração de um ataque DDoS.

GT-Actions
Ambiente Computacional para Tratamento de Incidentes com Ataques de Negação de Serviço

Demonstrações

O GT-Actions programou um conjunto de demonstrações para o WRNP 2016. A ferramenta de defesa contra ataques DDoS na camada de aplicação (SeVen – *Selective Verification in Application Layer*) será demonstrada em cenários capazes de explorar pontos como: a) a nova interface gráfica de configuração do SeVen, bem como suas funcionalidades e facilidades disponíveis para o administrador da rede; b) o uso do SeVen em uma arquitetura N-para-M, em que N seria o número de instâncias do SeVen e M seria o número de servidores *web* protegidos; c) a demonstração de ataques com servidores *web* distintos, como por exemplo, Apache, Nginx, Tom Cat, IIS; d) a realização de cenários de ataques diversos, nos quais diversos tipos de ataques da camada de aplicação serão empregados; e) a demonstração do funcionamento do SeVen como proteção do serviço fone@RNP contra ataques DDoS do tipo VoIP, como TDoS (Telephony DoS).

Em outra demonstração realizada, as máquinas que realizarão o ataque estarão localizadas nas instituições parceiras da Fase 2 do GT-Actions. A Figura 2 mostra uma ilustração desse cenário, destacando as instituições parceiras. O tráfego tanto dos clientes legítimos quanto dos atacantes passará pela rede Ipê e o serviço *web* alvo estará na UFPB. Serão utilizados no experimento os ataques Slowloris, HTTP Post e Slowread DDoS.

Nas demonstrações, uma aplicação *web* usada como alvo dos ataques DDoS e abrigada no servidor *web* do Laboratório de Redes (LaR) da UFPB será uma emulação do formulário do Sistema de Seleção Unificada (Sisu). O preenchimento dos formulários do Sisu será feito por meio de robôs que simularam usuários legítimos. Durante as demonstrações, informações sobre monitoramento do tráfego serão disponibilizadas em tempo real, tanto de usuários legítimos quanto de atacantes, de disponibilidade do servidor *web*, tempo de resposta do servidor *web* a uma requisição, uso da CPU e da memória por parte do servidor *web*, além de métricas inerentes à navegação por parte dos robôs que simularão os usuários legítimos. Algumas dessas métricas serão exibidas na interface gráfica do SeVen, que está sendo desenvolvida na Fase 2 do GT-Actions, e poderão ser acessadas diretamente pelo administrador da rede e/ou usuário do SeVen. Adicionalmente, serão demonstradas as potencialidades da interface gráfica do SeVen, bem como as funcionalidades e facilidades disponíveis para o administrador da rede.

Figura 2: Experimento na rede Ipê executado pelo GT-Actions.