18º WRNP Workshop RNP

15 | 16 MAIO
Belém | PA

EXPERIMENTAL

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

EQUIPE
Iguatemi E. Fonseca
Moises R. Nunes Ribeiro
Vivek Nigam
Leonardo C. Almeida
Helio Waldman
Yuri G. Dantas
Eduardo S. Gama
Marcílio O. O. Lemos
Davyson S. Pimentel
Matheus A. Silva
Sabrina F. Bertuani
Rafael B. M. Carvalho
Túlio A. Pascoal
Gustavo B. Sampaio
João Henrique Corrêa

Parceiros:
Capes - Coordenação de Aperfeiçoamento de Pessoal do Nível Superior
CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico
IFPB – Instituto Federal da Paraíba
UFES – Universidade Federal do Espírito Santo
UFABC – Universidade Federal do ABC
UFPB – Universidade Federal da Paraíba
Unicamp - Universidade Estadual de Campinas

SITE
http://lar-ufpb.net/?page_id=40

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

DESCRIÇÃO

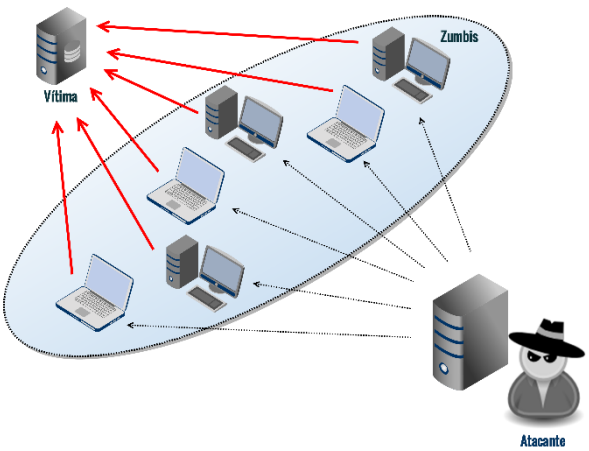
Segundo relatórios do Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP, ataques DDoS (*Distributed Denial of Service*) têm ocorrido com frequência na rede Ipê entre 2009 e 2016 e são, portanto, um dos principais desafios da segurança na internet. Sites comerciais, acadêmicos e governamentais, e.g., do governo federal, são alvos frequentes desses ataques. Como ataques DDoS têm uma grande capacidade de mudança e podem assumir novas características, é preciso desenvolver estratégias para mitigar tais ataques. A Figura 1 mostra uma ilustração de um ataque DDoS.

O principal objetivo da Fase 1 do GT-Actions foi desenvolver um protótipo de defesa, chamado de SeVen (*Selective Verification in Application Layer*), contra ataques DDoS na camada de aplicação, além de validar a sua eficiência por meio de experimentos na rede. Na Fase 1, foram alcançados, como resultados, o desenvolvimento de uma estratégia inédita na literatura, que funciona tanto como um *proxy* quanto como um módulo Apache, bem como a validação da defesa a partir de vários e diferentes tipos de experimentos na rede. Na Fase 2 (piloto), criou-se o protótipo do produto SeVen-HTTP e SeVen-VoIP, que foi aplicado em várias instituições parceiras (UFPB, Ufes, UFBA, PoP-SC, Unisul, UEPG e fone@RNP). O SeVen obteve excelentes resultados em todos os testes realizados. Nessa fase, também se iniciou pesquisas e desenvolvimento de uma defesa para mitigação de ataques em sistemas VoIP.

Atualmente, como principais resultados a serem alcançados no final da Fase 3 do projeto, podemos destacar:

1. Finalização do produto SeVen-HTTP como um ambiente para tratamento de ataques DDoS na camada de aplicação, com interface de gerenciamento e monitoramento, bem como homologação pelo CAIS/RNP e implantação em servidores *web* hospedados pela RNP e seus parceiros;
2. Desenvolvimento e aprimoramento do SeVen-VoIP, um módulo de defesa contra ataques DDoS em sistemas VoIP para as plataformas OpenSIPs e Asterisk;
3. Implantação de pilotos em parceiros para homologação do produto SeVen-HTTP e SeVen-VoIP;
4. Desenvolvimento de um modelo de negócios com o intuito de buscar meios para a sustentabilidade do projeto.

Figura 1: Ilustração de um ataque DDoS.



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 2017. A ferramenta de defesa contra ataques DDoS na camada de aplicação (SeVen) será demonstrada em cenários que sejam capazes de explorar pontos como: i) a nova interface gráfica de configuração do SeVen, bem como suas funcionalidades e facilidades disponíveis para o administrador da rede; ii) arquitetura em funcionamento no site do WRNP 2017; iii) Modelos de negócio, Canvas, Pitch para investidores, sustentabilidade do projeto e captação de clientes.

Também serão feitas demonstrações do funcionamento do SeVen como proteção do serviço fone@RNP contra ataques Telephony DoS. Essas demonstrações consistem na apresentação de alguns resultados obtidos com a condução de experimentos sobre os módulos PBX-IP (OpenSIPS) e Gateway Transparente (Asterisk) do fone@RNP, implantados na rede local do LaR-UFPB. Nesses experimentos, foi levado em consideração o comportamento das chamadas de clientes reais dos serviços (ex. características de tráfego), de modo a obter um cenário de teste mais próximo do cenário operacional do serviço. Também será apresentada a versão piloto do SeVen-VoIP, desenvolvida como um conjunto de módulos diretamente acoplados às principais aplicações de VoIP (OpenSIPS e Asterisk) usadas pelo fone@RNP. Por fim, será proposto um modelo de implantação do SeVen-VoIP nas instituições clientes do fone@RNP.

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