Proposta de Piloto

Grupo de Trabalho – Segunda Fase

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

Coordenador: Iguatemi E. Fonseca, UFPB

Coordenador Adjunto: Moisés R. N. Ribeiro, UFES

3/setembro/2015

1. Concepção

1.1. Resumo

Devido a sua efetividade e a falta de mecanismos de defesas, os Ataques de Negação de Serviços Distribuídos (DDoS) tem explorado cada vez mais protocolos na camada de aplicação. O principal objetivo da Fase 1 do GT-ACTIONS foi desenvolver um protótipo da defesa, chamada de **SeVen (*Selective Verification Defense*)**, contra ataques DDoS na camada de aplicação e validar a sua eficiência por meio de simulações e experimentos na rede. Nestes 10 meses da Fase 1 conseguimos resultados promissores, a saber: 1) Desenvolvemos uma estratégia inédita na literatura; 2) Formalizamos essa defesa usando ferramentas do estado-da-arte em métodos formais; 3) Validamos usando simulações a nossa estratégia de defesa contra dois ataques DDoS que exploram o protocolo HTTP, i.e., os ataques Slowloris e POST; 4) Implementamos um protótipo de SeVen em C++ que pode ser usado em uma configuração *Proxy*; 5) Validamos a eficiência da nossa defesa por meio de experimentos na rede: mostramos 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; finalmente, 6) implementamos um módulo Apache contendo a defesa SeVen. O objetivo da Fase 2 do GT-ACTIONS é consolidar o protótipo desenvolvido focando em IEEE pontos: i) Interface/Interação com o usuário (I); ii) Estabilidade (E); iii) Escalabilidade (E) e iv) Extensibilidade (E) do SeVen. Na Seção 2 desta proposta estes IEEE pontos serão detalhados.

1.2. Abstract

Due to the effectiveness and the lack of defense mechanisms, Denial of Service Attacks (DDoS) have exploited more often application layer protocols. The main objective of GT-ACTIONS Phase 1 was to develop a prototype of the defense called SeVen (Selective Verification Defense) for mitigating DDoS attack on the Application Layer and validate its efficiency through simulation and by carrying out experiments on the network. In the first 10 months of the project, we have had very promising results, namely: 1) Developed a novel defense strategy; 2) Formalized this defense using state-of-the-art formal methods tools; 3) Validated our defense through simulation against two DDoS attacks exploiting the HTTP protocol, namely, Slowloris and POST attacks; 4) Implemented a prototype of SeVen in C++ which may be used as a proxy; 5) Validated the efficiency of our defense by carrying out experiments on the network: we showed that a small to mid-size Apache server (200 simultaneous connections) becomes unavailable in the presence of a Slowloris or POST attack when SeVen is not running, but is available to 95% of the legitimate clients under the same attack when SeVen is running. The objective of Phase 2 of GT-ACTIONS is to consolidate the prototype focusing in following points: i) Interface/Interaction with the user; ii) Stability; iii) Scalability; and iv) Extensibility of SeVen. Section 2 of this proposal details these points.

1.3. Descrição do produto/serviço

Garantir que serviços estejam disponíveis e sejam resistentes contra ataques DDoS é uma necessidade para qualquer provedor de serviços. O nosso produto, SeVen, implementa um mecanismo inovador e eficiente de defesa contra ataques do tipo Low-Rate, onde atacantes simulam uma quantidade grande de usuários, sem gerar tráfego suficiente para que as defesas existentes possam mitigá-las. Uma grande vantagem de SeVen é que pode ser configurado e/ou adaptado para mitigar diferentes tipos de ataques e pode ser facilmente incorporada para trabalhar em conjunto com mecanismos de defesa existentes, como lista negras. Como SeVen é uma estratégia genérica, i.e., sem assumir um perfil de ataque, SeVen pode também ser usado para mitigar combinações de ataques, por exemplo, ataques simultâneos na camada de aplicação como, por exemplo, ataques POST e Slowloris. Também é possível utilizar SeVen para defender servidores Web de ataques que exploram o protocolo HTTP e defender sistemas de telefonia VoIP de ataques TDoS (*Telephony Denial of Service*).

Através dos nossos testes e estudos construímos o *know-how* para configurar SeVen em diferentes cenários, arquiteturas e aplicações. A RNP pode prover o serviço aos seus clientes ajudando-os com a configuração do SeVen e mantê-lo atualizado para tratar novos tipos de ataques. Por exemplo, estamos investigando como configurar SeVen para trabalhar com o modelo de classes de serviços em que clientes são classificados nas classes de clientes Ouro, Prata e Bronze dependendo do produto/serviço contratado. Assim durante uma sobrecarga do serviço, SeVen pode privilegiar clientes Ouro acima de clientes Prata e estes acima dos clientes Bronze.

A comunidade de usuários pode também identificar novas estratégias e configurações e integrar as suas defesas com o SeVen. Manter essa comunidade ativa será de grande valor para o rápido entendimento de ataques e do desenvolvimento de novas defesa para novas configurações. Apesar de criar essa comunidade de usuários ainda não ser o objetivo desta fase, podemos imaginar a RNP como um moderador de tal fórum. De fato, o GT-EWS está propondo algo na mesma direção com o uso do Twitter.

1.4. Identificação do público alvo

A priori qualquer usuário que tenha um servidor Web baseado em processos, como o servidor Apache, pode sofre ataques POST e Slowloris e, portanto, seria um potencial usuário do SeVen. Identificamos alguns usuários específicos da RNP e do Governo Federal que podem usufruir dos frutos deste projeto:

i) o SeVen pode ser instalado e configurado para proteger serviços e/ou servidores Web`s em qualquer cliente/usuário da RNP, como por exemplo, as Universidades e Institutos Federais, contra ataques DDoS da camada de aplicação. De acordo com informações da equipe da RNP que participou do Workshop de transferência de tecnologia do GT-ACTIONS realizado na UFPB em 28/julho/2015, atualmente a RNP não possui uma ferramenta que seja capaz de mitigar ataques DDoS da camada de

aplicação. Dessa forma, o SeVen pode preencher essa lacuna passando a ser ofertado a instituições clientes da RNP; ii) sistema de matrículas das universidades: Em particular, este é um serviço que tem sofrido muita sobrecarga (e possivelmente ataques DDoS) durante períodos de matrícula fazendo com o que o sistema esteja indisponível a usuários legítimos. Ter este serviço indisponível por longos períodos gera muita atenção na mídia causando um grande prejuízo na imagem da instituição na sociedade para a qual ela atende. Estes sistemas podem, portanto, capitalizar no desenvolvimento deste GT, integrando SeVen para mitigar esses problemas;

iii) a RNP pode ainda disponibilizar o SeVen para proteger sites e servidores Web do Governo Federal, como por exemplo, site do SISU/MEC, Gabinete da Presidência da República, Portal Brasil, Exército Brasileiro, dentre outros, os quais constantemente são alvo de ataques DDoS da camada de aplicação. Tal ação pode também refletir positivamente na imagem da RNP perante o Governo Brasileiro e incentivar a injeção de mais recursos/investimentos nos programas de P&D da RNP; iv) serviço Fone@RNP: o SeVen pode ser adaptado para mitigar outros ataques da camada de aplicação. Na Fase 2 do GT pretende-se estender o SeVen para mitigar outros tipos de ataques, como por exemplo, ataques aos serviços VoIP do Fone@RNP. Nós já contactamos os responsáveis pelo Fone@RNP e eles se mostraram interessados em mitigar ataques TDoS (Telephony DoS) usando SeVen. Tendo uma rede segura de ataques TDoS será de grande valor para o serviço de telefonia usando VoIP demonstrando que o sistema é seguro com relação a ataques de negação de serviço.

2. Definição do piloto 2.1

Arquitetura do piloto

a) Arquitetura

A seguir é apresentada a versão da defesa SeVen que funciona como proxy. Além disso, está em fase final de desenvolvimento e testes um módulo para o servidor Web Apache contendo a ferramenta de defesa. A versão do SeVen que funciona como proxy foi desenvolvida na linguagem C++ e, como pode ser visto na Figura 1, funciona e pode ser instalada entre o servidor e os usuários da Internet. O SeVen controla o acesso ao servidor por meio de uma lista que contém todas conexões ativas no servidor Web. Vale a pena mencionar que também é possível instalar o SeVen na mesma máquina que roda o servidor Web.

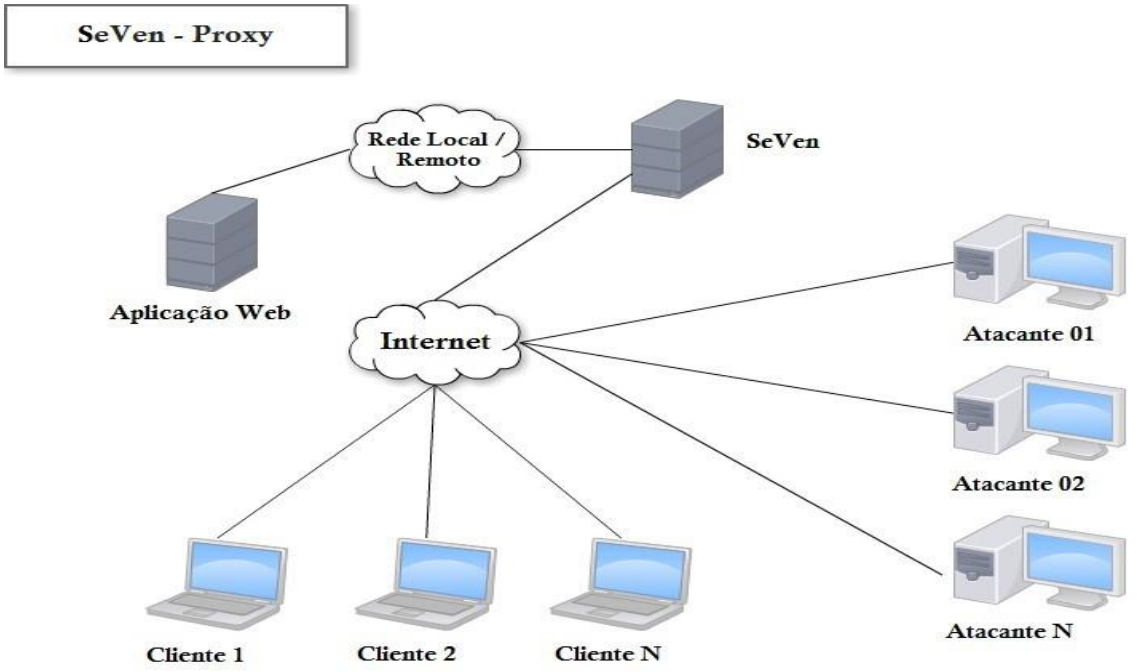

Figura 1 – SeVen-Proxy.

A Figura 2 apresenta a sequência de passos da comunicação entre o usuário e servidor Web com a ferramenta SeVen ativa. Primeiro, o cliente inicia o processo realizando uma requisição HTTP por meio de alguma aplicação que permita o envio dessas requisições, i.e. cURL, Siege, browser e etc. No momento em que o pedido de conexão chega ao SeVen, é verificado se há espaço na memória para abrir o socket. Se houver, a conexão é aceita pelo SeVen e encaminhada para o módulo seguinte, caso contrário, a conexão é rejeitada pelo SeVen.

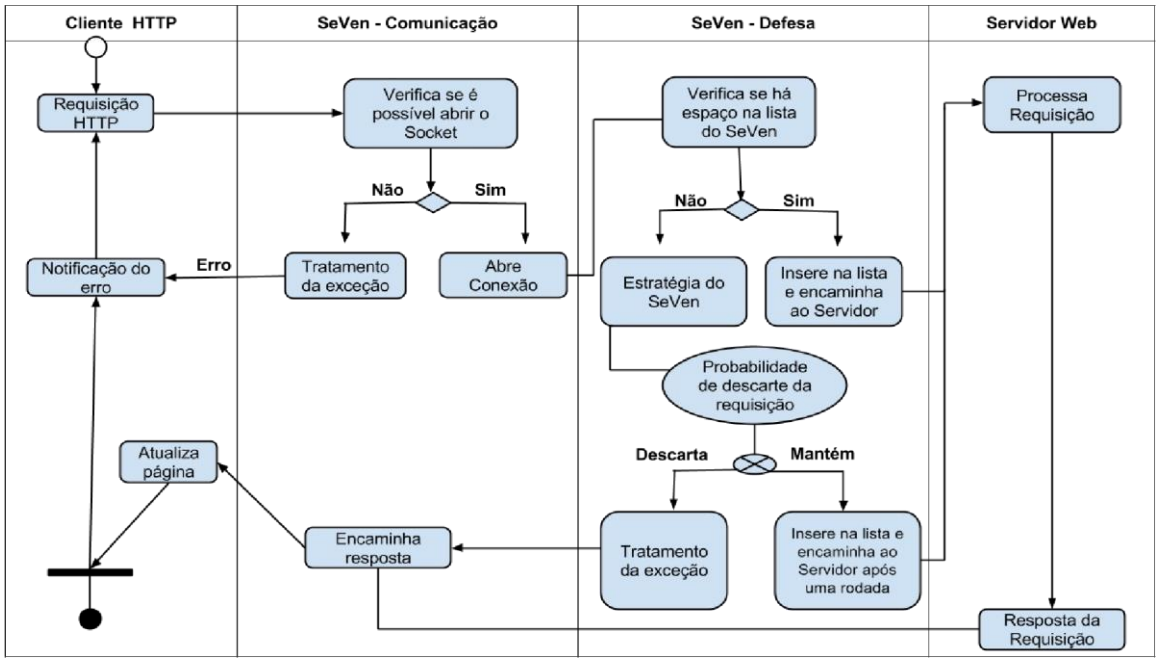

Figura 2 – Estrutura dos processos do SeVen.

Posteriormente à abertura do socket, é verificado se há espaço disponível na lista das conexões ativas do SeVen, caso exista, o SeVen funciona como um *proxy* básico, ou seja, apenas encaminha a mensagem para o Servidor Web. Caso contrário, é iniciada a estratégia do SeVen para verificar se a requisição HTTP deve ser aceita ou descartada pela defesa. Para checar essa condição é gerado um número aleatório de acordo com uma distribuição uniforme de probabilidade (U). Caso o SeVen decida descartar o pacote, uma mensagem de erro é enviada para cliente informando que não foi possível responder a solicitação, i.e, servidor indisponível (503). Caso opte por ficar com a requisição, baseado na mesma distribuição de probabilidade (U), é escolhido um usuário que deve ser removido da lista. Por fim, ao final da rodada, a requisição é encaminhada para o servidor Web, que por sua vez, processa a informação e envia sua resposta, a qual é encaminhada pelo SeVen ao cliente.

Perceba que, como é utilizada uma distribuição uniforme de probabilidade, todas as conexões presentes na lista, independente de ser de um cliente legítimo ou de um atacante, terão a mesma probabilidade de descarte. Por exemplo, se a lista de conexões tiver 200 posições, a probabilidade de remover qualquer uma das conexões é igual a 1/200. Como em uma situação de ataque DDoS é esperado que o número de conexões de atacantes seja bem maior que a de clientes, a probabilidade de remover uma conexão de um atacante é maior.

b) Equipamentos e softwares complementares

Como a defesa SeVen pode ser instalada na mesma máquina em que roda o servidor Web, em princípio, não é preciso instalar/utilizar novas máquinas nas instituições que iram participar da Fase Piloto do GT-ACTIONS. Além disso, o SeVen também não requer a instalação de qualquer outro *software* para o seu funcionamento.

Vale a pena mencionar que todo o desenvolvimento do SeVen foi feito em C++ e usando software livre e, na Fase 2, o GT-ACTIONS continuará com a mesma filosofia.

2.2 Instituições participantes

As instituições parceiras para a Fase 2 do GT-ACTIONS são:

a) PoP-ES: Magnus Martinello (magnos@inf.ufes.br);Rafael Emerick (rezo@popes.rnp.br);

b) NTI-UFES (Núcleo de Tecnologia da Informação da UFES): Hans Jorg Andreas Schneebelli (diretor.geral@npd.ufes.br); Leandro M. Lima (leandro.m.lima@ufes.br);

c) STI-UFPB (Superintendência de Tecnologia da Informação da UFPB): Jânio CarlosM. Vieira (janio@sti.ufpb.br), Pedro Jácome de Moura Junior (diretor@sti.ufpb.br);

d) Serviço Fone@RNP: Alex Galhano Robertson (alex.galhano@rnp.br);

e) Flexa *Information Technology* (http://www.flexait.com.br): Deivid Bitti Padilha (deivid.bitti@flexait.com.br).

A participação do NTI-UFES e STI-UFPB se dará principalmente para viabilizar o teste do SeVen no sistema de matrículas da UFES e UFPB, respectivamente. Como mencionado no Item 1.4 desta proposta, o sistema de matrículas de universidades experimentam um volume razoável de tráfego e por vezes sofrem ataques DDoS, portanto representam um ótimo cenário para testes da ferramenta de defesa. A nossa ideia é testar os aspectos de **Estabilidade e Escalabilidade** previstos nos IEEE pontos a serem focados na Fase 2 do GT-ACTIONS.

O aspecto de **Extensibilidade** leva a ferramenta a outros ambientes e aplicações. Para este fim, agregamos diferentes parceiros que operam no dia a dia serviços que, embora fora de eixo de desenvolvimento inicial do SeVen, podem trazer importantes contribuições à ferramenta na Fase 2 do GT-ACTIONS. Além de avaliarem a nossa ferramenta segundo critérios operacionais mais severos, podem estender o conjunto de requerimentos do SeVen para a generalização da solução de mitigação de ataques DDoS em camada de aplicação. Como exemplos, sistemas de telefonia Fone@RNP e servidores baseados em eventos, como Nginx por baixo de aplicações como o viaipe.rnp.br. É importante destacar que o parceiro comercial (*Flexa Information Technology*) não terá acesso ao código fonte e assinará NDA (*NonDisclosure Agreement*) relativo à ferramenta. A sua participação é muito importante para avaliação ampla, com critérios usados fora do ambiente acadêmico, do potencial e na realimentação para a evolução do SeVen para uma fase futura de serviço experimental da RNP.

2.3 Refinamento do protótipo

O objetivo da Fase 2 do GT-ACTIONS é consolidar o protótipo desenvolvido focando em IEEE pontos: i) Interface/Interação com o usuário (I); ii) Estabilidade (E); iii) Escalabilidade (E) e iv) Extensibilidade (E) do SeVen.

O **ponto I (Interface/Interação com o usuário)** vislumbra desenvolver um conjunto de Logs para que possam ser registrados eventos importantes durante a execução da defesa SeVen. Tais registros podem ser utilizados pelo administrador da rede para averiguar situações atípicas e comportamento de tráfego, bem como para auditoria e diagnósticos de problemas/falhas tanto da ferramenta de defesa quanto do servidor Web sob proteção. Em uma outra vertente, o **ponto I** visa também criar uma interface para o SeVen de forma a torná-lo amigável para usuários e administradores de rede.

O **ponto 1E (Estabilidade)** objetiva a realização de testes longos e com cargas e cenários de ataques diversos. Neste ponto estamos interessados em estabilidade do ponto de vista da resposta do SeVen a um ataque de longa duração, ou seja, buscamos respostas para perguntas como: i) o SeVen suporta um ataque DDoS da camada de aplicação que tem duração de 1, 2 ou 4 dias ou uma semana? E se esse ataque for composto por dois ou mais tipos de ataques DDoS da camada de aplicação? Quanto de recursos computacionais são usados/necessários em ataques desta natureza?

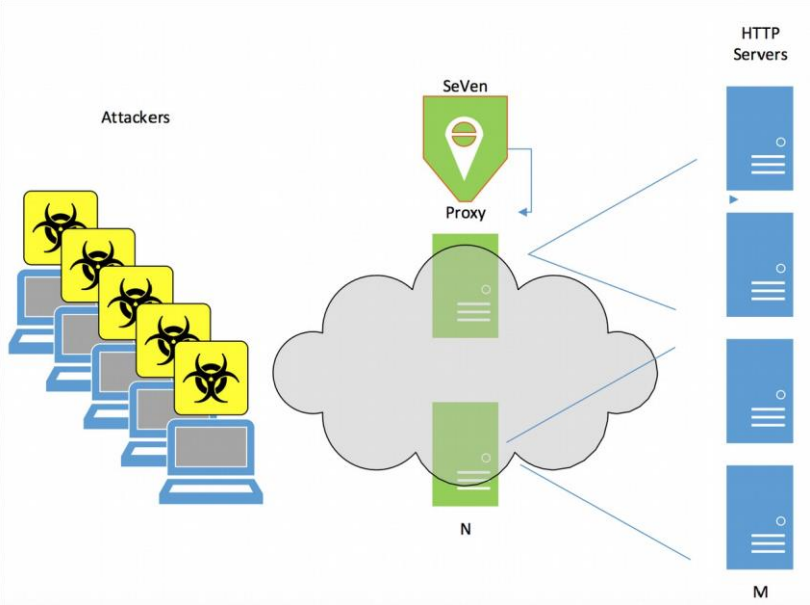

Figura 3: Ilustração de uma combinação número de proxy versus número de servidores Web no estudo da Escalabilidade.

O **ponto 2E (Escalabilidade)** visa estudar e testar combinações e arquiteturas de número de proxy (N) versus número de servidores Web (M). A ideia é encontra relações/configurações entre N e M que são necessários para manter o serviço Web disponível em diversos cenários de ataques. A Figura 3 ilustra um exemplo de combinação N, M.

Finalmente, o **ponto 3E (Extensibilidade)** vislumbra a extensão do SeVen em três eixos, a saber: i) novos ataques da camada de aplicação; ii) operar em servidores baseados em eventos, como o servidor Nginx, além dos baseados em processos, como Apache; iii) adaptação para o Fone@RNP. Assim, o SeVen será extendido para operar em outros domínios, como, por exemplo, gateways/servidores VoIP, em que além de mitigar ataques TDoS, existe a necessidade de estender o SeVen para incorporação de identificação de uso legítimo por usuários não autorizados do serviço Fone@RNP. Adicionalmente, além do TDoS, pretende-se estudar e testar a eficácia do SeVen contra o ataque *Slow Read DDoS,* o qual é um ataque da camada de aplicação, e similarmente ao Slowloris e POST, explora vulnerabilidades do protocolo HTTP. Um ponto interessante deste ataque é que além de servidores baseados em processos como o Apache, o ataque *Slow Read DDoS* também pode ser nocivo contra servidores baseados em eventos, como o Nginx. Dessa maneira, o SeVen será extendido para operar em servidores baseados em eventos, portanto poderá também ser instalado em clientes da RNP que usam servidores Nginx.

2.4 Ferramentas de suporte à operação (para propostas de serviço)

Apesar de não ser o foco deste projeto, existe o potencial da RNP prover o serviço de manutenção do SeVen em seus clientes. Por exemplo, com o surgimento de novos ataques com diferentes perfis assim como novas configurações de serviços,

SeVen necessitará de novas configurações, em particular, novas distribuições de probabilidades de descarte. Através do estudo mais rigoroso do SeVen, em especial, o ponto Extensibilidade, iremos entender como a mudança da probabilidade de descarte do SeVen afeta a sua eficiência no tratamento de diferentes ataques. Esse estudo dará à RNP o *know-how* para prover este serviço de configuração do SeVen.

3. Cronograma

A ideia das etapas da Fase 2 do GT-ACTIONS é atacar os IEEE pontos descritos na Seção 2.3. Para tanto, como na Fase 1, continua-se-á utilizando tanto modelos analíticos e métodos formais em computação quanto simulação numérica em computador e experimentos em uma rede real para o teste e validação dos algoritmos. Especificamente, na parte de experimentação, pretende-se, além de experimentos em cenários controlados em laboratório, realizar testes em ambiente mais realistas e de produção por meio da colaboração com a empresa *Flexa Information Technology.*

A seguir estão descritos os passos a serem seguidos na Fase 2. Os testes experimentais serão realizados tanto em cenários de rede LAN, como também em cenários de WAN por meio da participação dos parceiros listados no Item 2.2.

- **1:** Desenvolvimento de um conjunto de Logs para registro de eventos importantes durantes dos testes com o SeVen. Pretende-se coletar informações como:
  i) total de requisições que chegaram para serem atendidas; ii) requisições que foram bloqueadas pelo SeVen no primeiro sorteio da moeda; iii) requisições retiradas do buffer do servidor Web pelo SeVen no segundo sorteio da moeda;
- **2:** Desenvolvimento de interfaces (por exemplo, Web) para interação/configuração do SeVen;
- **3:** Incorporação de novos ataques da camada de aplicação no SeVen, como os ataques TDoS e S*low Read DDoS*;
- **4:** Estudo e desenvolvimento de arquiteturas de número de proxy versus número de servidores Web. Nesta etapa, os servidores Apache e Nginx poderão ser testados ao mesmo tempo em um experimento;
- **5:** Realização de testes experimentais com as arquiteturas propostas na Etapa 4;
- **6:** Realização de testes experimentais diversos de longa duração com o SeVen. Pretende-se, além da questão temporal, investigar o que acontece quando o ataque DDoS é composto por dois ou mais tipos de ataques DDoS da camada de aplicação;
- **7:** Implantação e testes experimentais com o serviço Fone@RNP; • **8:** Implantação e testes com o sistema de matrículas da UFES e UFPB;
- **9:** Testes com o parceiro *Flexa Information Technology.*

A Tabela 1 mostra a distribuição das etapas ao longo dos 14 meses da Fase 2 do GT-ACTIONS. Cada coluna representa um período de um bimestre, totalizando portanto 14 meses de duração.

Tabela 1: Sugestão de cronograma de execução para a Fase 2.

Etapa	**Tempo (bimestres)**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1	x						
2	x	x					
3	x	x	x				
4		x	x				
5			x	x			
6			x	x	x		
7				x	x	x	x
8			x	x	x	x	x
9			x	x	x	x	x

4. Recursos financeiros

4.1 Equipamentos e softwares

A Tabela 2 mostra a lista de equipamentos sugeridos para a Fase 2 do GTACTIONS. Esses equipamentos complementarão e darão suporte aos equipamentos já adquiridos na Fase 1, bem como a outros equipamentos existes no Laboratório de Redes (LaR) da UFPB e no Laboratório de Telecomunicações (LabTel) da UFES.

Como o total geral de equipamentos foi inferior a R$ 25.200,00, solicita-se que R$ 10.150,00 sejam alocados para a rubrica Pessoal para pagamento a um Assistente 3 que trabalhará na UFPB ou UFES.

Tabela 2: Sugestão de equipamentos para a Fase 2.

Descrição	**Quantidade**	**Valor Unitário (R$)**	**Total do item (R$)**
RouterBoard 2011 UiAS-IN	4	800,00	3.200,00
RouterBoard 2011 UiAS-RM	4	800,00	3.200,00
No-Break 3200 VA UPS 220 V	1	3.200,00	3.200,00
Hack 36 U`s equipamento com badejas, guia cabos e unidade de ventilação	1	2.500,00	2.500,00
Monitor LED 24`	1	1.400,00	1.400,00
		Total Geral	R$ 13.500,00

[Além do custeio de pessoal, equipamentos e softwares, o programa de GTs da RNP poderá custear também viagens nacionais para membros dos Grupos de Trabalho, sujeitas às seguintes condições:

- As viagens deverão ter necessariamente como objetivo a **realização de reuniões do projeto** e **atividades de implantação do piloto**.
- Será custeado um número máximo de de 5 passagens e 10 diárias.
- Ao longo do desenvolvimento do GT, a RNP poderá solicitar, a seu critério e arcando com todos os custos, a participação do coordenador e de membros do GT nas seguintes situações: em reuniões de acompanhamento do projeto, na representação da RNP em eventos externos, na participação nos eventos internos da RNP (WRNP e SCI), como palestrantes ou instrutores, e na realização de eventos (treinamentos ou workshops) na fase de disseminação do serviço]