RELATÓRIO FINAL DE BOLSISTA

PROGRAMA FAPEAM		**N. DO EDITAL**	
MODALIDADE DE BOLSA			
NÍVEL	( ) NÍVEL A ( ) NÍVEL B ( ) NÍVEL C ( ) NÍVEL ÚNICO		

É OBRIGATÓRIO PREENCHIMENTO DO PROGRAMA, BOLSA E NÍVEL.

1. DADOS DO BOLSISTA (não omita ou abrevie nomes)					
NOME:	Wallison da Costa Coutinho				
E-MAIL:	wallisoncoutinho@gmail.com				
CPF:	845190702-44	**PASSAPORTE (ESTRANGEIRO):**			
ENDEREÇO DE CORRESPONDÊNCIA:	Rua G4, 130, Conjunto Nova Republica				
BAIRRO:	Distrito Industrial	**CEP:**	69075580		
CIDADE:	Manaus	**ESTADO:**	AM		
TELEFONE:	36156909	**CELULAR:**	81514119	**FAX:**	

2. PROJETO DE PESQUISA EM QUE O BOLSISTA DESENVOLVEU SUAS ATIVIDADES					
COORDENADOR / ORIENTADOR:	Dr. Edjard de Souza Mota				
TÍTULO DO PROJETO:	Auto-proteção contra ataques de recusa de serviço em sistemas operacionais para redes.				
TÍTULO DO PLANO DE TRABALHO DO BOLSISTA:	Auto-proteção contra ataques de recusa de serviço em sistemas operacionais para redes.				
INÍCIO:	13/08/2009	**TÉRMINO:**	28/ 07/10	**PERÍODO A QUE SE REFERE ESSE RELATÓRIO:**	/ /

3. DADOS DO COORDENADOR / ORIENTADOR					
E-MAIL:	edjard@dcc.ufam.edu.br				
ENDEREÇO DE CORRESPONDÊNCIA:	Rua Constelação de Orion, 10				
BAIRRO:	Morada do Sol	**CEP:**	69060-088		
CIDADE:	Manaus	**ESTADO:**	AM		
TELEFONE:	(92) 3236-8063	**CELULAR:**	(92) 8414-4314	**FAX:**	

4. INSTITUIÇÃO ONDE O BOLSISTA DESENVOLVE ATIVIDADES			
INSTITUIÇÃO:	Universidade Federal do Amazonas		
UNIDADE E DEPARTAMENTO:	Departamento de Ciência da Computação		
ENDEREÇO:	Av. Rodrigo Octavio Jordão Ramos, 3000		
TELEFONE:	(92) 3647-4225	**FAX:**	

5. INFORMAÇÕES DA BOLSA CONCEDIDA					
INÍCIO:	13/08/2009	**TÉRMINO:**	28/07/2010	**PERÍODO CONCEDIDO (MESES):**	12
ALTERAÇÕES:	( ) BOLSA CANCELADA A PARTIR DE: / /				
	(X) SUBSTITUIÇÃO DO BOLSISTA (Williamns Tadeu de O L Belo) A PARTIR DE : 01/11/2009				
	( ) BOLSA RENOVADA A PARTIR DE: / /				
	( ) NÃO HOUVE ALTERAÇÕES				
JUSTIFIQUE A ALTERAÇÃO:					
Desistência do bolsista Williamns Tadeu de O L Belo.					

6. OBJETIVOS PROPOSTOS NO PLANO DE TRABALHO (máximo 15 linhas- não alterar formatação)

Esse trabalho visa investigar uma solução para o problema de ataques DoS em ambientes com sistemas operacionais de rede utilizando os conceitos de redes autonômicas. As redes autonômicas possuem a característica de auto-gerenciamento, ou seja, elas são auto-configuráveis, auto-otimizáveis, auto-recuperáveis e auto-protegidas. A auto-proteção oferece para essas redes a capacidade de se proteger contra erros e falhas oriundos de ataques maliciosos. Os elementos autonômicos que constituem essas redes podem cooperar na prevenção, detecção e remediação de ataques de DoS na rede. Para os sistemas operacionais de rede, a autonomia pode ser uma forma de proteger o canal de comunicação entre o servidor de gerenciamento e os dispositivos físicos da rede sendo controlados.

O principal objetivo desse trabalho é desenvolver uma solução híbrida de auto-proteção contra ataques de recusa de serviço em sistemas operacionais de rede utilizando conceitos de redes autonômicas. Outros objetivos foram: investigar o problema de ataques de recusa de serviço em ambientes com sistemas operacionais de rede; investigar e propor uma solução contra ataques de recusa de serviço baseada em elementos autonômicos; implementar os elementos autonômicos de auto-proteção contra ataques DoS na arquitetura dos sistemas operacionais de rede e realizar testes de desempenho da solução.

7. RESULTADOS OBTIDOS (máximo 30 linhas - não alterar formatação)

Descreva os resultados obtidos e analise-os em função dos objetivos propostos em seu plano de trabalho

Para coleta de resultados de ataques DDoS em uma rede baseada em NOX, foi utilizado scritps baseado em Qemu/Vde o qual permite emular uma rede com o NOX com qualquer topologia. Os testes com DDoS foram realizados utilizando a ferramenta Stacheldraht, a qual dispõe de diversos tipos de ataques. Neste trabalho foi escolhido o ataque TCP/SYN pelo fato deste ataque ser um dos mais utilizados para ataques DDoS na Internet. Foram realizados experimentos em dois cenários: rede sem ataque, todos os hosts das duas redes executam um loop com intervalos de 4 segundos, onde é gerado um fluxo de pacotes TCP/IP. Rede sob ataque, um dos hosts na rede atacante torna-se atacante real. O fluxo de pacotes de ataque é gerado com a porta de origem forjada. Para realizar a avaliação do impacto de ataques DDoS em redes baseadas em NOX, foram analisadas as flow-initiations. Para calcular o número de flow-initiations durante um intervalo de tempo, basta contabilizar o número de pacotes de controle do OpenFlow do tipo Flow Modification. Haja vista que toda ocorrência de uma flow-initiation acarreta em mensagem de controle Flow Modification. É possível perceber o aumento linear do número de flow-initiations durante o período de ataque DDoS. Enquanto que em um cenário sem ataque o número de flow-initiations se mantém estável. Este forte crescimento deve-se ao fato de o fluxo de pacotes de ataque DDoS ter a característica de forjar campos de cabeçalho de pacote, o que no caso deste trabalho foi o campo da porta de origem. Como os valores desse campo são gerados de forma aleatória dificilmente existe casamento entre um novo pacote de chegada ao switch com alguma entrada na tabela de fluxo do mesmo. Isto acaba se tornando um problema haja vista que esse aumento implica em um overhead no NOX, pois todos esses pacotes flow-initiations devem ser processados pelo NOX, impossibilitando o mesmo de responder com rapidez as flow-initiations de usuário legítimos. O crescimento linear do número de flow-initiations durante período de ataque DDoS acarretou em um aumento também linear do número de entradas na tabela de fluxos presente no switch OpenFlow da rede da vítima. Isto se deve a fato que para todo pacote de controle do tipo Modification gerado é adicionada uma entrada na tabela de fluxo. Em períodos de ataques onde a taxa do fluxo de pacotes foi aumentada ocorreram erros no switch OpenFlow da rede da vítima. Isto se deve ao incapacidade de armazenar pacotes no buffer de pacotes de chegada no mesmo. Este trabalho apresentou um estudo sobre o comportamento de uma rede baseada em NOX sob ataque DDoS, mostrando o impacto desse tipo de ataque sobre os componentes da mesma. Para isto foi experimentado de forma virtual ataque DDoS do tipo TCP/SYN em um cenário de rede usando NOX, detalhes sobre o experimento pode ser visto na seção de Experimentos. Os experimentos mostraram que redes baseadas em NOX é vulnerável em determinados aspectos como por exemplo o crescimento de flow-initiations, oque aumentando de forma linear o número de requisições ao NOX. Os resultados obtidos nesse trabalho vem para contribuir com pesquisas futuras de DDoS para este tipo de rede, além de apontar os pontos fracos contra esses ataques.

8. PRODUÇÃO BIBLIOGRÁFICA GERADA PELO PROJETO, COM A PARTICIPAÇÃO DO BOLSISTA(*)	
(*) Trabalhos individuais ou em cooperação, submetidos e/ou publicados.	
QUANTIFICAR:	_____ Trabalhos apresentados em eventos técnico-científicos.
	_____ Artigos publicados em revistas especializadas.
	_____ Relatórios/notas técnicas.
	_____ Outra (especificar).
LISTAR COM REFERÊNCIA BIBLIOGRÁFICA COMPLETA E INCLUIR CÓPIA (CAMPO ILIMITADO)	

9. PARTICIPAÇÃO EM EVENTOS			
SEQ	**NOME DO EVENTO**	**DATA**	**APRESENTOU TRABALHO?**
1		/ /	**( ) SIM ( ) NÃO**
2		/ /	**( ) SIM ( ) NÃO**
3		/ /	**( ) SIM ( ) NÃO**
4		/ /	**( ) SIM ( ) NÃO**

10. *NO GERAL, EM TERMOS DE SUA CAPACITAÇÃO, AMADURECIMENTO E CRESCIMENTO PROFISSIONAL, COMO VOCÊ AVALIA AS ATIVIDADES DESENVOLVIDAS*? (A SER RESPONDIDA PELO BOLSISTA, SE PERTINENTE À MODALIDADE DE BOLSA)

( ) ACIMA DAS EXPECTATIVAS	**(X) CORRESPONDEU ÀS EXPECTATIVAS**	**( ) ACRESCENTOU POUCO**

AVALIE, NUMA ESCALA DE 1 A 5 (SENDO 1= MUITO FRACA E 5 = EXCELENTE), OS SEGUINTES ITENS:

(5) Orientação recebida

(3) Infra-estrutura da Instituição

(5) Relacionamento com a equipe de pesquisa

(5) Quantidade e qualidade do trabalho desenvolvido

JUSTIFIQUE SUA AVALIAÇÃO, INDICANDO OS PONTOS POSITIVOS E NEGATIVOS

Em trabalhos com tecnologia da Internet do futuro, experimentação física depende bastante de equipamento de com tecnologia de ponta, o que não pode ser oferecido pela instituição. Sendo assim, decidimos utilizar ambientes virtualizados.

11. GANHOS OBTIDOS PELA INSTITUIÇÃO, ADVINDOS DO TRABALHO DO BOLSISTA (A SER RESPONDIDO PELO ORIENTADOR/TUTOR (máximo 15 linhas- não alterar formatação)

Avalie o desempenho e a contribuição do bolsista, tendo em vista o desenvolvimento do projeto específico, a linha de pesquisa, a equipe, dentre outros.

O aluno trabalhou em uma área importante para o grupo de pesquisa que é a parte de segurança. Essa área depende bastante de como o sistema se comporta diante de um ataque malicioso. Esse trabalho foi o primeiro passo para o desenvolvimento de uma solução para um problema muito corriqueiro na Internet e no ambiente de sistemas operacionais de redes e o aluno soube aproveitar a oportunidade para se envolver nas tarefas necessárias para obtenção desses objetivos.

12. GANHOS OBTIDOS PELO BOLSISTA. (A SER RESPONDIDO PELO ORIENTADOR/TUTOR) (máximo 10 linhas-não alterar formatação)

Avalie os progressos do bolsista considerando sua formação/capacitação profissional.

O bolsista se especializou em uma área nova de pesquisa que é a Internet do Futuro. Para isso ele teve que ganhar experiência através de livros, documentações, implementações e discussões dentro do nosso grupo. Isso ajudou no seu desenvolvimento intelectual, bem como uma primeira experiência no cotidiano de pesquisa com novas tecnologias.

Manaus _____ de _____ de _____.

_____

ASSINATURA DO BOLSISTA

Manaus _____ de _____ de _____.

_____

ASSINATURA DO COORDENADOR / ORIENTADOR DO BOLSISTA

É OBRIGATÓRIO O PREENCHIMENTO DE TODOS OS ITENS E DAS ASSINATURAS