UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA

2008.2

UMA FERRAMENTA PARA A DETECÇÃO DE ANOMALIAS NO PROTOCOLO DNS

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno	Rodrigo Diego Melo Amorim	{rdma@cin.ufpe.br}
Orientador	Djamel Fawzi Hadj Sadok	{jamel@cin.ufpe.br}
Co-Orientador	Eduardo Luzeiro Feitosa	{elf@cin.ufpe.br}

22 de Agosto de 2008

Índice

1. Contexto

A área de segurança em redes de computadores apresenta-se como uma das maiores preocupações das empresas atualmente. Os ataques estão cada vez mais complexos e é necessário encontrar novas estratégias que ajudem a distinguir as anomalias do tráfego normal de uma rede.

As vulnerabilidades nos protocolos e infra-estruturas de redes não cansam de ser exploradas e, cada vez mais, técnicas de ataque vão se tornando mais complexas e críticas para o bom andamento de servidores na rede. Nesse cenário os pontos vitais da internet viram alvo fácil dos ataques, principalmente os de negação de serviço.

O serviço fornecido pelo Domain Name Service (DNS) é de fundamental importância para o correto funcionamento de quase todos os outros serviços na internet. Em estado normal, um servidor DNS trabalha resolvendo os nomes dos domínios da internet para endereços IP e vice-versa. Sem o DNS os usuários teriam que “decorar” uma grande quantidade de números para acessar um site desejado. Já em casos de ataques ou anomalias, a freqüência de requisições é demasiadamente grande, o que prejudica o funcionamento do serviço e/ou paralisa suas atividades.

Entre as principais anomalias contra o DNS estão os ataques diretos provenientes de botnet, vírus, spams e ataques de negação de serviço (DoS ou DDoS). Outro ataque com conseqüências piores é o envenenamento de cache (DNS cache poisoning). Neste tipo de ataque busca-se corromper um determinado servidor DNS com o intuito de direcionar o endereço da requisição feita a um site para um servidor DNS malicioso.

No que diz respeito a soluções e mecanismos de detecção de anomalias ao DNS, as principais são técnicas baseadas em assinaturas e através de entropia.

2. Objetivos

Este trabalho propõe a implementação de um novo algoritmo e heurística para detecção de anomalias ao DNS através da captura passiva do tráfego de rede.

Especificamente, pretende-se:

a) Levantar problemas e deficiências encontrados hoje no DNS;
b) Propor e avaliar uma ou mais técnicas de identificação de tráfego anômalo do protocolo DNS;
c) Sugerir melhorias ao DNS na Internet;

3. Cronograma

O cronograma abaixo demonstra algumas datas para as atividades principais do processo de desenvolvimento do trabalho de graduação. Os prazos podem ser alterados conforme o estudo e aprofundamento do trabalho ou o acontecimento de imprevistos.

ATIVIDADES	AGOSTO				SETEMBRO				OUTUBRO				NOVEMBRO			
Levantamento do material bibliográfico																
Definição de Escopo																
Testes de Captura																
Implementação de Protótipo																
Análise dos Resultados																
Elaboração do relatório																
Preparação da apresentação																

4. Referências

BIND 9 DNS Cache Poisoning. Disponível em: <http://www.trusteer.com/bind9dns> Data de acesso: 20 de agosto de 2008.

Caida. Passive Monitoring of DNS Anomalies. Disponível em: <http://www.caida.org/publications/papers/2007/dns_anomalies/dns_anomalies.pdf> Data de acesso: 17 de agosto de 2008.

Xu, K., Zhang, Z-L., e Bhattacharrya, S. (2005) Profiling internet backbone traffic: Behavior models and applications. ACM SIGCOMM Computer Communication Review, 35(4), páginas 169-180. ACM Press.

5. Possíveis Avaliadores

Nelson Souto Rosa
Ruy Barreto de Queiroz

6. Assinaturas

Djamel Fawzi Hadj Sadok
Orientador

Eduardo Luzeiro Feitosa
Co-Orientador

Rodrigo Diego Melo Amorim
Aluno