



Ministério da
Ciência e Tecnologia



INPE-15340-TDI/1376

APLICAÇÃO DE TÉCNICAS DE DATA MINING PARA A ANÁLISE DE LOGS DE TRÁFEGO TCP/IP

André Ricardo Abed Grégio

Dissertação de Mestrado do Curso de Pós-Graduação em Computação Aplicada,
orientada pelos Drs. Antonio Montes Filho e Rafael Duarte Coelho dos Santos,
aprovada em 27 de fevereiro de 2007.

Registro do documento original:

<<http://urlib.net/sid.inpe.br/mtc-m17@80/2007/04.04.18.29>>

INPE
São José dos Campos
2008

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE

Gabinete do Diretor (GB)

Serviço de Informação e Documentação (SID)

Caixa Postal 515 - CEP 12.245-970

São José dos Campos - SP - Brasil

Tel.:(012) 3945-6911/6923

Fax: (012) 3945-6919

E-mail: pubtc@sid.inpe.br

CONSELHO DE EDITORAÇÃO:**Presidente:**

Dr. Gerald Jean Francis Banon - Coordenação Observação da Terra (OBT)

Membros:

Dr^a Maria do Carmo de Andrade Nono - Conselho de Pós-Graduação

Dr. Haroldo Fraga de Campos Velho - Centro de Tecnologias Especiais (CTE)

Dr^a Inez Staciarini Batista - Coordenação Ciências Espaciais e Atmosféricas (CEA)

Marciana Leite Ribeiro - Serviço de Informação e Documentação (SID)

Dr. Ralf Gielow - Centro de Previsão de Tempo e Estudos Climáticos (CPT)

Dr. Wilson Yamaguti - Coordenação Engenharia e Tecnologia Espacial (ETE)

BIBLIOTECA DIGITAL:

Dr. Gerald Jean Francis Banon - Coordenação de Observação da Terra (OBT)

Marciana Leite Ribeiro - Serviço de Informação e Documentação (SID)

Jefferson Andrade Ancelmo - Serviço de Informação e Documentação (SID)

Simone A. Del-Ducca Barbedo - Serviço de Informação e Documentação (SID)

REVISÃO E NORMALIZAÇÃO DOCUMENTÁRIA:

Marciana Leite Ribeiro - Serviço de Informação e Documentação (SID)

Marilúcia Santos Melo Cid - Serviço de Informação e Documentação (SID)

Yolanda Ribeiro da Silva e Souza - Serviço de Informação e Documentação (SID)

EDITORAÇÃO ELETRÔNICA:

Viveca Sant´Ana Lemos - Serviço de Informação e Documentação (SID)



Ministério da
Ciência e Tecnologia



GOVERNO FEDERAL

INPE-15340-TDI/1376

APLICAÇÃO DE TÉCNICAS DE DATA MINING PARA A ANÁLISE DE LOGS DE TRÁFEGO TCP/IP

André Ricardo Abed Grégio

Dissertação de Mestrado do Curso de Pós-Graduação em Computação Aplicada,
orientada pelos Drs. Antonio Montes Filho e Rafael Duarte Coelho dos Santos,
aprovada em 27 de fevereiro de 2007.

Registro do documento original:

<<http://urlib.net/sid.inpe.br/mtc-m17@80/2007/04.04.18.29>>

INPE
São José dos Campos
2008

Dados Internacionais de Catalogação na Publicação (CIP)

G861a Grégio, André Ricardo Abed.

Aplicação de técnicas de data mining para a análise de logs de tráfego TCP/IP/ André Ricardo Abed Grégio. – São José dos Campos: INPE, 2008.

134p. ; (INPE-15340-TDI/1376)

1. Redes de computadores. 2. Data mining. 3. Segurança de sistemas de informação 4. Análise de logs. 5. Detecção de intrusão. I. Título.

CDU 004.7

Copyright © 2008 do MCT/INPE. Nenhuma parte desta publicação pode ser reproduzida, armazenada em um sistema de recuperação, ou transmitida sob qualquer forma ou por qualquer meio, eletrônico, mecânico, fotográfico, microfílmico, reprográfico ou outros, sem a permissão escrita da Editora, com exceção de qualquer material fornecido especificamente no propósito de ser entrado e executado num sistema computacional, para o uso exclusivo do leitor da obra.

Copyright © 2008 by MCT/INPE. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use of the reader of the work.