DEVELOPING NETWORKING TRACKING TOOLS FOR ELIMINATING SPOOFING IN LOCAL AREA NETWORK

Muatamed .A .Hajer

Universiti Utara Malaysia

2009

DEVELOPING NETWORKING TRACKING TOOLS FOR ELIMINATING SPOOFING IN LOCAL AREA NETWORK

A Thesis submitted to college Arts & Sciences in partial

Fulfillment of the requirement for the degree master

(Information Technology)

University Utara Malaysia

By

Muatamed A .Hajer (800127)

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

MUATAMED -A. HAJER
(800127)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

DEVELOPING NETWORKING TRACKING TOOLS FOR ELIMINATING SPOOFING IN LOCAL AREA NETWORK

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **MR. AMRAN AHMAD**

Tandatangan
(Signature) : _____

Tarikh
(Date) : 28 APRIL 2009

Permission to Use

In presenting this thesis of the requirements for a Master of Science in Information Technology (MSc. IT) from Universiti Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in his absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Request for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School

Universiti Utara Malaysia

06010 Sintok

Kedah Darul Aman

ABSTRACT

A network tracking tool, is a programme that helps a network administrator to keep track of moves, additions, and changes (known as MACs) to the hardware infrastructure of a network. Some network tracking tools keep track of cabling MACs only. It has become necessary to enhance the current tracking for eliminating spoofing for local area network. However, this study has come up with appropriate tracking for eliminating spoofing by using Java language for developing networking tracking. Others can keep track of all the devices connected to the network, and provide visual diagrams of the network configuration showing all the configurations, the network has had since it was first put into use. This study used MYSQL and JCreator for developing the tracking tools for spoofing over local area network. Furthermore, the proposed system has been tested by using use case test for the system pages.

Acknowledgement

My gratitude to my supportive and helpful supervisor, **Mr. Amran Ahmed** for assisting and guiding me in the completion of this research. With all truthfulness, without him, the project would not have been a complete one. **Mr. Amran Ahmed** has always been my source of motivation and guidance. I am truly grateful for his continual support and cooperation in assisting me all the way through the semester. I am grateful to **Dawood Sallem** for his help in making my project successful.

I would like to present my thanks to my father and all my family members who have always been there for me. Finally, I would like to express my appreciations to all my friends, colleagues, other staff, and everyone who have helped me in this journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

This chapter briefly elaborates the main idea of this work, providing answers to the question as to why the study was conducted and what is the main element involved in the study. The first sub-topic describes the overall idea in this study as well as the scenario and motivation that led to the implementation of the whole project. This is followed by the problem statement, objectives of the study, significance of the study and scope of the study. The last sub-topic elaborates the way this project is organised.

1. Introduction

According to Sanjay G. (2006), spoofing means the computer on a network pretends to have identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network. Furthermore the spoofing computer often does not have access to user-level commands; so attempts to use automation-level services, such as email or message handlers, are employed. Automation services designed for network interoperability are especially vulnerable, especially those adhering to open standards. The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The main types of spoofing are:

(a) IP Spoofing: this type allows the user to send packets with spoofed IP addresses to machines to fool the machine into processing the packets, that is generated by the trackers (Sanjay G., 2006). In other words, in IP spoofing, an

The contents of the thesis is for internal user only

REFERENCE

ARP Receive (2008). ARP packet structures. Retrieved on 20 May 2009. From (www.cs.clemson.edu/~westall/853/notes/**arp**recv.pdf).

Atanas, V., and Miriam, R.(2006). Static control-flow analysis for reverse engineering of UML sequence diagrams. 31(1): 96 – 102.

Atle, S. (2008). Extending UML Sequence Diagrams to Model Trust- dependent Behavior with the Aim to Support Risk Analysis. 197(2): 15-29.

Bahl, P. and Padmanabhan, V. (2000). Radar: An in-building rfbased user location and tracking system, in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), pp. 775–784.

Berson, T., and Beth, T. (1989). LAN Security Workshop LANSEC '89 Proceedings, Springer-Verlag, Berlin.

Bahrami, A. (1999). Object Oriented System Development, McGraw-Hill, United States of America.

Batten, K. Saraf, A., and Treptin, S. (2001). A secure peer-to-peer backup system, December.

Bellardo J. and Savage S. (2003). 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions, in Proceedings of the Twelfth USENIX Security Symposium. Washington, DC, USA: USENIX Association, pp. 15–28.

Bellovin S. (1989). Security Problems in the TCP/IP Protocol Suite. Computer Communications Review, vol. 19, no. 2, pp. 32-48.

Cox and Noble (2002). Pastiche: Making backup cheap and easy. In In Proceedings of Fifth Usenix Symposium on Operating Systems Design and Implementation.

Computer Incident Advisory Committee (CIAC) (1995). Advisory Notice F-08 Internet Spoofing and Hijacked Session Attacks.

Chen Y. (2006). A Novel Marking-based Detection and Filtering Scheme Against Distributed Denial of Service Attack, Masters Paper, University of Ottawa, 2006.

Daemon (1996). IP Spoofing Demystified. Phrack Magazine Review, Vol 7, No. 48, 48-14.

Davies, D. W. & W. L. (1989). Price, *Security for Computer Networks*, John Wiley, NY.

Department of Defense Password Management Guideline (1985). National Computer Security Center.

Denning, D. E. & D. K. Branstad (1996), A Taxonomy for Key Escrow Encryption Systems, *Communications of the ACM*, Vol. 39, No. 3, 34-49.

Desai, A. (2000). *The security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search*, Advances in cryptology,CRYPTO 2000 : 20th annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24,proceedings, pp359-375.

Diffie, W., & Hellman, K. (1976). New directions in Cryptography. IEEE Trans. On Information Theory IT-22, 6 644-654.

Demirbas M. and Song, Y. (2006). An rssi-based scheme for sybil attack detection in wireless sensor networks, in Proceedings of the International Workshop on Advanced Experimental Activities on Wireless Networks and Systems.

Dennis D. (1985). Security of Personal Computer Systems: A Management Guide, NBS Special Publication 500-120.

Eriksson, H., & Penker, M. (1998). UML Toolkit. USA, John Wiley & Sons, Inc.

Elnahrawy, E., Li, X. and Martin, R. (2004). The limits of localization using signal strength: A comparative study," in Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON 2004), pp. 406–414.

Federal Information Processing Standard (FIPS PUB) (1974). Guidelines for Automatic Data Processing Physical Security and Risk Management.

Gopal B., Ashish K.,& Dhanna R. (2008). Detecting and Preventing IP Spoofed Attack by Cryptography, National Conference on Challenges & Opportunities in Information Technology.

Goncalves, M. (1998). *Firewalls Complete*, McGraw Hill, New York, NY, 1998.

George, J. & Valacich, J. (1999). Modern Systems Analysis and Design (2nd Edition). United Kingdom : Addison Wesley Longman.

George, J. & Valacich, J. (2002). Modern Systems Analysis and Design (3rd Edition). Upper Saddle River, New Jersey: Prentice Hall.

Gilbert, I. (1989). Guide for Selecting Automated Risk Analysis Tools, NIST Special Publication 500-174.

Gahan, C. (1990). LAN Security, the Business Threat from Within, BICC Data Networks Limited.

Gopal B., Ashish K.. and Chakraverti, D. (2008). Detecting and Preventing IP Spoofed Attack by Cryptography.

Johnson, J. Z. (1998). Network Security Programs: Process and Metrics for the Real-World, White paper, Internet Security Systems, Inc.

Johnsson, P. & Overgaars, G. (2004). Object-oriented Software Engineering: A Use Case Driven Approach (revised). Harlow, England: Addison-Wesley.

Koo, J. (2005). Evaluation of network blocking algorithm based on ARP spoofing and its application", Lecture Notes in Computer Science 3480, pp.848-855.

Kwon, K. and Ahn, S. (2004). Network security management using ARP spoofing", Lecture Notes in Computer Science 3043, pp. 142-149. International journal of communications issue.

Katzke, W. (1992). A Framework for Computer Security Risk Management, NIST.

Ladd, A. Bekris, K., and Rudys, A. (2002). Robotics-based location sensing using wireless ethernet," in MobiCom '02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, pp. 227–238.

Mohd D., Nurhayati A. (2006). Performance Evaluation Of TCP/IP Protocol for Mobile Ad Hoc Network. WSEAS Transactions on Computers, Vol.5, No.7, pp. 1481-1486.

Mohamed G., Chin T. (2003).A secure address resolution protocol , Computer Networks, Vol.1, No.41, pp. 57-71.

McRobb, S., & farmer, R. (2002). Object-oriented System Analysis and Design 2 en Edition. UK, McGraw Hill.

Power, R.(2001). Computer Security: Issues and Trends, 2001 CSI/FBI Computer Crime and Security Survey vol. VII, No. 1,.http://www.gocsi.com/prelea/000321.html.

Redner A. and Walker, H. (1984). Mixture densities, maximum likelihood and the EM algorithm, SIAM Review, vol. 26, no. 2, pp. 195–239.

Roback, E. (1991). NIST Coordinator, Glossary of Computer Security Terminology, NISTIR 4659.

Ramachandran, V., and Nandi, S. (2005). Detecting ARP spoofing: An active technique, Lecture Notes in COMPUTER SCIENCE 3803, pp.239-250.

Schmuller, J. (2002). SAMS Teach Yourself UML in Hours . SAMS Publishing, Indiana.

Steven, J., and Vaughan, N. (2003). Hard drive technology reaches a turning point. IEEE Computer, 36(12):21– 23.

Sheng, Y., and Chen, G. (2002). Securing 802.11 wireless networks through fine-grained measurements, Submitted to IEEE Wireless Communications Magazine.

Silva, P. & Paton, N. (2003). UML: The Unified Modeling Language for Interactive Applications.

Savage S., Wetherall D., Karlin A., & Anderson T. (2000). Practical network support for IP traceback. Proc. of the 2000 ACM SIGCOMM Conference.

Steven J.& Templeton, Karl E. (2008). Detecting Spoofed Packets, retrieved on 3 Feb 2009, U.C. Davis.

U.S House of Representative (1999). Systems Development Life Cycle, pp. 1-12.

Wixom, B., & Tegarden, D. (2005). System analysis and design with UML version 2.0: an object-oriented approach with UML, 2 edition. Hoboken, NJ: John Wiley and Sons, Inc.

Whalen S. (2009). An Introduction to ARP Spoofing. Retrieved on 20 Feb 2009, from http://packetstorm.securify.co.

Xiao, B. and Gao, C. (2006). Detection and localization of sybil nodes in vanets, in Proceedings of the Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS).

Yao C., Shantanu D., Pulak D., Abdulmotaleb S., & Amiya N. (2006). An effective defense mechanism against massively distributed denial of service attacks International Journal of Network Security, Vol.7, No.1, PP.70–81.

Youssef, M., and Agrawal, A. (2003). Wlan location determination via clustering and probability distributions, in Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 143–150.