SECURITY FEATURES IDENTIFICATION FOR CISCO ROUTERS

BEHNAZ FOROOZESH

A dissertation submitted in partial fulfillment of the

Requirements for the award of the degree of

Master of Science (Information Technology - Management)

Faculty of Computer Science and Information Systems

Universiti Teknologi Malaysia

JULY 2012

This dissertation is dedicate to my beloved Father, mother and husband

For their endless sacrifices, supports and encouragement.

ACKNOWLEDGEMENT

First and Foremost thanks to the almighty GOD for giving me chance of study and helping me all the time, Then I would like to express my appreciation and deepest thanks to the following people for their support.

Especially thanks To my respected supervisor Dr. Norafida bin Ithnin, I have appreciated having her as a supervisor thanks for her ideas and advice given through this research.

Besides To my dearly loved Father and Mother, who have not only lovingly raised me, but who have also helped me greatly in each step of my study and my appreciation and Many thanks to my beloved Husband for his support, patience and helping me not only in the way of improvement but also for to be happy and energetic all the time.

ABSTRACT

Todays, with complicated networks spread around the world, each action that happens or does not happen to a network can affect its state of compliance. Therefore, network compliance is of great significance to any organization and in this area the important point is that, each network infrastructure device namely; Router, Switch, Access point, Firewall etc. has a unique configuration file, containing hundreds of settings, rules and various other options. If the configuration changes are done manually the opportunity for errors is enormous. To make secure network and in that connection organizational data security and integrity, there is a need to have a tool to monitor changes to the network. Configuration audit tool is management solution for network infrastructure devices for security vulnerabilities. As a consequence of the research objectives which are to determine (a) study about the different security risks that network devices are exposed to and sequentially study about the available defense mechanisms especially related to CISCO devices.(b) study about automation auditing configurations and existing settings and solutions (c) propose and discussed about a more completed and secure categorized settings for audit configurations based on finding of researches and coding some of them as a demo the samples by Perl script to automate the auditing of the configuration file to make sure about security settings, at the end of this research suggested tool provides the usefulness of examining the device configurations for compliance to a defined set of internal policies, standards and templates by the way, greatly decrease the time for secure configurations and this tool can also be customized for each an organization. It will help to administrators to at once check each device in an Organization for a new vulnerability with only a few mouse clicks.

ABSTRAK

Hari ini,Dengan rangkaian rumit yang merebak di seluruh dunia, setiap tindakan yang berlaku atau tidak berlaku kepada rangkaian boleh menjejaskan keadaan pematuhan.Oleh itu,pematuhan rangkaian adalah amat penting kepada mana-mana organisasi dan di kawasan ini yang penting adalah bahawa, setiap peranti rangkaian infrastruktur iaitu Router,Suis,Pusatakses,dan sebagainya.Firewall mempunyai fail konfigurasi yang unik, yang mengandungi beratus-ratus tetapan, peraturan dan pelbagai pilihan lain. Jika perubahan konfigurasi telah dilakukan secara manual peluang untuk kesilapan besar.Untuk membuat rangkaian selamat dan bahawa sambungan data keselamatan dan integriti organisasi, terdapat keperluan untuk mempunyai alat untuk memantau perubahan kepada rangkaian.Konfigurasi alat audit adalah penyelesaian pengurusan untuk peranti infrastruktur rangkaian bagi kelemahan keselamatan.Sebagai akibat objektif kajian adalah untuk menentukan ,kajian mengenai risiko keselamatan berbeza peranti rangkaian terdedah kepada dan berturutan belajar mengenai mekanisme pertahanan yang terutama yang berkaitan dengan peranti,kajian mengenai konfigurasi pengauditan automasi dan sedia ada tetapan dan penyelesaian,mencadangkan dan dibincangkan kira-kira lebih siap dan selamat dikategorikan tetapan untuk konfigurasi audit berdasarkan dapatan penyelidikan dan pengekodan sebahagian daripada mereka sebagai demo sampel dengan skrip Perl untuk mengautomasikan pengauditan fail konfigurasi untuk membuat pasti tentang tetapan keselamatan, pada akhir alat kajian ini mencadangkan menyediakan kegunaan pemeriksaan konfigurasi peranti untuk pematuhan kepada satu set ditakrifkan dasar,piawaian dalaman dan template dengan cara, banyak masa untuk konfigurasi selamat dan alat ini juga boleh disesuaikan bagi setiap organisasi.IA Akan membantu kepada pentadbir sekaligus memeriksa setiap peranti dalam Pertubuhan bagi kelemahan yang baru dengan hanya beberapa Klik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CM	Configuration Management
CA	Configuration Audit
Cisco	American Multinational Network Corporation Systems
CAM	Content Addressable Memory
RAT	Router Audit Tool
MAC	Media Access Control Address
ARP	Address Resolution Protocol
DTP	Dynamic Trunk Protocol
STP	Spanning Tree Protocol
BPDU	Bridge Protocol Data Units
VTP	VLAN Trunking Protocol
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
PERL	Practical extraction and report language
CCSAT	Cisco Configuration Security Auditing Tool
ACL	Access Control List
AS	Autonomous System
PCIDSS	Payment Card Industry Data Security Standard
FDCC	Federal Desktop Core Configuration
DNS	Domain Name System
CRC	Cisco Router Configuration
SDM	Cisco Security Device Manager
GNU	General Public License
DOS	Denial of service
AAA	Network Authentication, Authorization, Accounting

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The backbone of any organization in today's world is the network and it is the availability of the network that keeps the business alive as well as how the information is treated on its way in the terms of confidentiality and integrity. Security has become a major concern for many network equipment manufacturers and software developers in the recent years so they are actively working on recognizing security vulnerabilities and trends to add built-in and add-on security protection into their products. All vendors are laying security in all their customer-training plans to increase the level of security awareness and better use of their products, which of course brings them market reputation. Hence, organizations and business owners are making huge investments on appropriate network infrastructure because they are aware that security is critical to their network infrastructure.

1.2 Research Problem Background

Although there are rich security features built into network devices but these Settings are not active by default. Network equipment vendors deliver their products with a default configuration that makes it very easy to setup and bring into operation for network administrators.

Activating security features means bringing some limitation and restrictions into the system and if not planned and implemented with consideration it might bring partial or complete service disruption into the network and since many network administrators have a limited scope of security, knowledge and skill they are very conservative to touch any of the security configurations.

Securing a network is not about turning on a single button. There are a variety of areas that a network administrator must look into and make the right decision. There are hundreds of security configuration options available in network devices but that does not mean an administrator needs to activate them all to make sure the network is secure. An administrator should know the current network, organization security policies, technical constraints, have a thorough understanding of different kind of network attacks and vulnerabilities, and know about all the security features that have been built into the network equipment by the vendor (Brand, 1990).

One common problem after an administrator implements security features in the network is that over time and during troubleshooting daily network problems administrators tend to disable security features to isolate their problems which no problem if they come back and activate the security features again but unfortunately this is not the case in most circumstances.

To overcome this, an auditing policy should be in place to check the entire configuration on network devices on regular intervals and make sure configurations Are in compliance with the recommended security settings (Yusuf, 2008).So the problems can be summed up as:

Devices “default configuration” are not secure. Security features on network devices are not enabled by default. Enable security features requires strong security knowledge on both the threats and the defense mechanisms so requires administrator with strong security knowledge. Enabling security features means changing different configuration sections in a single device configuration file which means auditing is required regular and rapidly changes, to make sure the right security settings are in place. Manual Security configurations of network devices are time-consuming ,prone to human-error with high cost besides more downtimes can reduce the network customers.No specific tool or solution is available to help the network companies in assessing auditing configurations for more security and None of the existing tools designed specifically for Cisco devices auditing (Devargas,1995).

1.3 Research Problem statements

To overcome the complexity of implementing and maintaining security, automated software is required to provide security guidelines and perform security auditing on regular basis to make sure the configuration are conforming with the security policies.

Some problems are specified in current security auditing that are used in organizations, they are common between them such as misconfigurations by admins,

high cost of implementation of auditing, untimely response, time and cost consuming and etc.Although, some tools are produced but they can not cover all the problems and even all versions of routers and switches, in the other hand in the real network marketing only SDM is available for Cisco devices which is only for monitoring and showing some limited range of configurations as an auditing reports .CIS is the security agency which published list of security configurations which should be applied in the network devices based on many best practices, so in this research is studied based on CIS recommendations for suggestions and improving auditing Cisco devices, which all this matters will be discussed in details in literature review.

Research Questions that are tried to answer in this research:

Main research question that this project is going to answer:

"How to improve controllers of Auditing tools that can be used to automating network devices auditing and assist in the security configurations?"

Some sub questions: during this research should be find answer for some sub questions to find the answer of the project question, as such as:

"What are different network attacks and vulnerabilities and the control mechanisms and what are the impacts of them on networks?"

How these control mechanisms configured on cisco devices and what are the recommended security configurations.

1.4 Research Objectives

The objectives of this project are proposes as bellow:

- To investigate the different security risks and attacks that network devices are exposed to
- To study the solutions mechanisms available to protect network devices against security risks.
- To study and conduct a survey of exciting auditing devices.
- To explain which defense mechanisms are available and are not on cisco devices and provide the auditing report.
- To propose the extraction rules that can be used to which defense mechanisms are available and are not on cisco auditor SDM and for improving security auditing, provide the recommendation based on CIS lists and network security admins requirements (gathering from questioners) and finding of other researchers.

1.5 Research Scopes

Security is a vast topic, and it can be applied to many scopes so what this project is focused on is limited to the following areas:

- Focuses on security areas which are related to securing Network Management on Layer-2 and Layer-3 attacks.
- Focus on 5 Network Organizations and IT entrepreneurs (who) of Iran
- Searching threats and solution mechanisms and rules related to cisco routers configuration.

1.6 Significant of the research

This project will help in the following:

- System administrators with little or no security knowledge can find out how secure is their cisco switches and routers and how can they secure the devices.
- It can use as part of an automated and periodic security auditing procedure.
- Preventing time and cost consuming and downtimes in network cause of Miss-configurations.
- Network devices auditing is necessary for Implementing ITIL in network companies because change management is based on auditing network.

1.7 Summary

Configuring a secure cisco switch or router requires high knowledge and understanding for the network administrator. Network administrators are more involved and concerned with the day to day operation tasks and this keeps them away from learning about the in-depth of the security and implementing security. Besides, security often makes the operation more difficult for the network administrators so they are reluctant to utilize security features. So having an automated security auditing tool that someone can run against the network devices without having much security knowledge is crucial.

REFRENCES

Akin, Thomas.,2002.*Hardening Cisco Routers*, O'reilly& Associates.

Al-Shaer, E.; Marrero, W.; El-Atawy, A.;ElBadawi, K.,2009.*Network configuration in a box*: towards end-to-end verification of network reachability and security, 17th IEEE InternationalConference on Network Protocols (ICNP), pp 123-132.

Alcatel-Lucent.,2007.*IOS Basic System Configuration Guide*.availableat: http://www.alcatel-lucent.com.

Andrew Mason., 2004 .*Sample Chapter is provided courtesy of Cisco Press* . Available at:http://www.ciscopress.com/articles/article.asp?p=341484 and http://kb.juniper.net/InfoCenter/index?page=content&id=KB7205

ArcSight tool page Available at: http://www.arcsight.com/solutions/solutions compliance/

Ballew, S.M.,1997. *Managing IP Networks with Cisco Routers, O'Reilly Associates.*

Brand, Russell.,1990.*Copingwith the Threat of Computer Security Incidents*: A Primer from Prevention through Recovery.Version CERT 0.6. Pittsburgh, Pa.

Buckley, A.ed.,1999.*Cisco IOS 12.0 Configuration Fundamentals, Cisco Press*.

Catalyst 4500 Series Switch Cisco IOS Command Reference and the publications,available at:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/indx

Caldwell, D.; Seungjoon Lee; Mandelbaum, Y.2008*;"Adaptive parsing of router configuration languages"*, Internet Network Management Workshop (INM). IEEE, pp. 1 – 6.

Chappell, L.,1998.*Introduction to Cisco Router Configuration, Cisco Press.*

Chappell, L.,1999 (ed.) *Advanced Cisco Router Configuration, Cisco Press.*

CERT Coordination Center.,1996."*CERT/CC Product Vulnerability Reporting Form Version 1.0."*, SoftwareEngineering Institute, Carnegie Mellon University.

CCSAT tool page available at: http://www.securityfocus.com/tools/3236.

Cisco System, Inc. *Network Security Policy*: Best Practices White Paper. Available http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml .

Cisco Works Network Compliance Manager Introduction, available at: http://www.cisco.com/en/US/products/ps6923/index.html

Cisco Device Hardening (Mitigating Network Attack) chapter3.Reconnaissance Attack and Mitigation.

Crocodile tool page Available at: http: //www. iese.fraunhofer .de/ en/products /crocodile.html

D. A. Maltz, J. Zhan, G. Xie, H. Zhang, G. Hja´lmty´sson, A. Greenberg, and J. Rexford.,2004.*Structure preserving anonymization of router configuration data*.In Proceedings of IMC.ACM.

Damon Reed.,2003." *SANS GIAC GSEC Practical Assignment*", version 1.4b , Option One.

David Dittrich.,1999."*The stacheldraht distributed denial of service attack tool*"31,

Devargas, Mario.,1995.*The Total Quality Management Approach to IT Security*. Oxford:NCCBlackwell.

Device Expert tool page, available at: http://demo.deviceexpert.com/NCMContainer.cc

Eldridge, B., 1999.*Building Bastion Routers Using Cisco IOS*, Phrack Magazine, Vol. 9 Issue55,.Availableat: http://www.phrack.org/show.php?p=55&a=10.

Gaithersburg, Md., 2009.National Institute of Standards and Technology.

Gill, Heasley, and Meyer, 2004The Generalized TTL Security Mechanism (GTSM), RFC3682.

Greene, B. and Smith, P.,2002.*Cisco ISP Essentials*, 1st Edition, Cisco Press.

IBM E-book; IBM Tivoli Directory Server, Version 6.3,Chapter: AdministrationGuidePart:Setting password policy , available at: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBhdjdMDS.doc/admin_gd201.htm

Icove,David;Seger,Karl;VonStorch,William.,1995.Computer Crime: *A Crimefighter's Handbook*. Sebastopol, CA: O'Reilly& Associates.

Joel Scambray, Stuart McClure, George Kurtz, and Hacking Exposed: *Network Security Secrets and Solutions*, 3rd Edition, Found stone Inc.

Kaufman,Charlie; Perlman, Radia; & Spencer, Mike.,1995.*Network Security: Private Communication in a Public World*. Englewood Cliffs, N.J.: Prentice Hall.

L. Vanbever, G. Pardoen, and O.,2010.Bonaventure. *Towards validated network configuration with NCGuard*.InProc.of INM Workshop.

Microsoft E-book; Chapter*: Security and Protection*, Part: Password Policy; available at: http://technet.microsoft.com/en-us/library/ms161959.aspx

Madalina Baltatu.,2000"*Security Issues in Control, Management and Routing Protocols"*. 22-25.

National Security Agency., 2001.Router *Security Configuration Guide*, Available at: http://nsa2.www.conxion.com

National Institute of Standards and Technology.*An Introduction to Computer Security:* The NIST Handbook (NIST Special Publication 800-12).

Nagios tool page, Available at: http://www.nagios.org/

NIPPER tool page, available at: http://www.techrepublic.com/blog/security/audit-your-cisco-routers-security-with-nipper/276

Northcutt, Stephen.,1999.Network Intrusion Detection: An Analysts Handbook, New, Riders Publishing.

Olnes, Jon.,1994."*Development of Security Policies*."Computers& Security 13, 8628-636.

Pethia, Richard D.,1990."*Developing the Response Team Network."*Workshopon Computer Security Incident Handling. Pleasanton, CA.

Radia Perlman.,2000.Interconnections:*Bridges,Routers,SwitchesInternetworking Protocols.*Massachuttes, second edition.

Rybaczyk, Peter,2000.*Cisco Router Troubleshooting Handbook*, M&T Books.

Stewart, J. and Wright, J., 2000.*Securing Cisco Routers:* Step-by-Step, SANS Institute.

Sihyung Lee; Tina Wong; Kim, H.S.,2008. "*To Automate or Not to Automate: On the Complexity of Network Configuration*", IEEE International Conference on Communications (ICC), pp. 5726 – 573.

Simon Hansman.,2003.“*Taxonomy of Network and Computer Attack Methodologies”.* Available at :http://www.passcape.com/bruteforce_attack.

V. Gill, Michael Shields.,2008. “*Automatic configuration generation and auditing of network,*”North American Network Operators’ Group (NANOG) presentation.

“What’s Behind Network Downtime?” Whitepaper by Juniper Networks May 2008.Available at: http://www-05.ibm.com/uk/juniper/pdf/200249.pdf.

West-brown,MoriaJ.,D.Stikvoort,K.P.Kossakowski, et al.Carnegie Mellon.,2008.Software Engineering Institute.*Handbook for Computer Security Incident Response Teams*(CSIRTs).

Weise, J. And C.R.Martin.,2008.Sun Microsystems, Ins. *Developing a Security Policy.* http://www.sun.com/blueprints/1201/secpolicy.pdf

William Enck,ThomasMcDaniel,SubhabrataSen,PanagiotisSpoerel,Albert Greenberg, Yu-Wei Eric Rao,William Aiello.,2009.”*Configuration management at massive scale:*System design and experience”;IEEE Journal on Selected Areas in Communication archive, vol. 27 , Issue 3 ,Special issue on network infrastructure configuration, pp:323-335.

Wood, Charles Cresson. Information Security Policies Made Easy, 6th ed. Sausalito,Calif.: Baseline Software Inc., 1998.ISBN# 1-881585-04-2.

Yusuf Bhaiji.,2008.CCIEProfessional Development Series Network Security Technologies and Solutions, Cisco Press.