UNIVERSITATEA TEHNICĂ A MOLDOVEI

ANALIZA VULNERABILITĂȚILOR ÎN CADRUL REȚELEI ȘI MODALITĂȚI DE EVITARE ALE ACESTORA

Masterand:

Ana EȘANU

Conducător:

conf. univ., dr. Victor ABABII

Chişinău 2022

ADNOTARE

la teza de master cu tema „Analiza vulnerabilităților în cadrul rețelei și modalități de evitare ale acestora" a masterandului grupa CRI-201M Ana EȘANU.

Structura tezei cuprinde: introducere, trei capitole, concluzii și bibliografie, 79 pagini de text de bază, 26 figuri, 2 tabele.

Scopul lucrării: prezentarea, analiza și studierea vulnerabilităților apărute în cadrul rețelei unei companii precum și simularea unui atac și prezentarea software-ului ce poate asigura respingerea acestuia și securitatea ulterioară a rețelei.

Câteva din **obiectivele** principale ale lucrării sunt analiza generală a rețelei unei companii, studierea celor mai frecvente tipuri de vulnerabilități în rețelele companiilor, precum și a tehnicilor utilizate pentru depistarea sau evitarea acestora, prezentarea practică a unui soft capabil să depisteze și să prevină vulnerabilitățile de rețea.

Capitolul I, **„Rețeua transort de date"** este axat pe analiza generală a unei rețele transport de date ce vizează o companie din perspectiva literaturii de specialitate dedicate temei de cercetare analizate. La fel am propus spre prezentare și modalitatea de realizare a unui transfer de date fiabil și integru, dar și importanța monitorizării acestui transport de date. Se reflectă propria înţelegere a temei şi se formulează scopul şi sarcina de cercetare.

În Capitolul II, **„Descrierea vulnerabilităților rețelei unei companii"** conține aspectele teoretice şi metodologice în domeniul vulnerabilităților inevitabile în sistemul de comunicații. În acest capitol este analizat conceptul de vunerabilitate de rețea, se prezintă principalele vulnerabilități și amenințări ale unei rețele dar și se descrie tehnicile şi metodele de evitare ale acestora prin soluții de securitate.

Capitolul III, **„Simularea unor vulnerabilități și testarea software-ului propus".** În acest capitol am prezentat practic-aplicativ soluții de securitate pentru un sistem de comunicații, astfel că am ridicat o mașină virtuală pe care am instalat, configurat și testat software-ul necesar în captarea, stocarea și indexarea pachetelor de rețea și ulterior am simulat mai multe vulnerabilități și pe final am prezentat o analiză asupra atacurilor depistate și am accentuat importanța monitorizării traficului și a fluxului de date, ceea ce duce la păstrarea securității rețelei unei companii.

Teza de masterat nu prezintă un produs finit. Lucrarea dată este doar o analiză generală asupra vulnerabilităților unui sistem de comunicații atribuit companiilor de mici și mari dimensiuni, astfel etapa următoare constă însăși din implimentarea de către aceste companii a softurilor prezentate, și intergrarea însăși a tuturor măsurilor de securitate propuse în cadrul rețelelor companiilor.

Valoarea aplicativă a cercetării: se propune spre implimentare a tuturor regulilor de securitate informațională precum și a softurilor de monitorizare a transferului de date în rețea în vederea stabilirii unei inalte performanțe a sistemului de comunicații în cadrul unei companii.

Cuvinte-cheie: rețea, vulnerabilități, securitate, firewall, software.

ANNOTATION

to the master's thesis with the topic "Analysis of vulnerabilities in the network and ways to avoid them" of the master student group CRI-201M Ana EŞANU.

The structure of the thesis includes: introduction, three chapters, conclusions and bibliography, 78 pages of basic text, 26 figures.

The aim of the paper: to present, analyze and study the vulnerabilities that have appeared within a company's network as well as to simulate an attack and to present the software that can ensure its rejection and the subsequent security of the network. Some of the main **objectives** of the paper are the general analysis of a company's network, the study of the most common types of vulnerabilities in company networks, as well as the techniques used to detect or avoid them, the practical presentation of software capable of detecting and preventing network vulnerabilities. .

Chapter I, **"Data Transmission Network"** is focused on the general analysis of a data transport network targeting a company from the perspective of the literature dedicated to the research topic analyzed. We also proposed for presentation the way to achieve a reliable and complete data transfer, but also the importance of monitoring this data transport. It reflects one's own understanding of the topic and formulates the purpose and task of the research.

In Chapter II, "**Description of the vulnerabilities of a company's network"** contains the theoretical and methodological aspects in the field of unavoidable vulnerabilities in the communications system. This chapter analyzes the concept of network vulnerability, presents the main vulnerabilities and threats of a network but also describes the techniques and methods to avoid them through security solutions.

Chapter III, **"Simulation of vulnerabilities and testing of the proposed software".** In this chapter we presented practical-application security solutions for a communications system, so we set up a virtual machine on which we installed, configured and tested the necessary software in capturing, storing and indexing network packets and then simulated more many vulnerabilities and finally presented an analysis of the detected attacks and emphasized the importance of monitoring traffic and data flow, which leads to maintaining the security of a company's network.

The master's thesis does not present a finished product. This is just a general analysis of the vulnerabilities of a communications system attributed to small and large companies, so the next step is the implementation by these companies of the software presented, and the integration of all proposed security measures within company networks.

The applicative value of the research: it is proposed for the implementation of all information security rules as well as the software for monitoring the transfer of data in the network in order to establish a high performance of the communication system within a company.

Keywords: network, vulnerabilities, security, firewall, software.

CUPRINS

INTRODUCERE

Informația și transmiterea ei a evoluat de la epocă la epocă, odată cu apariția omului, și chiar înainte de el, cu sute de mii de ani în urmă. Acestea fiind tot mai complexe pe parcursul mileniilor, întrucât societățile umane devin mai numeroase și mai ierarhiceiar dezvoltarea nu a lipsit ci dimpotrivă a avansat mult. Fiecare etapă în evoluția transmiterii informațiilor se datorează transformării societății contemporane care este marcată de o accelerare a dezvoltărilor informaționale. Fiecare instituție, organizație sau companie de astăzi are unul sau mai multe sisteme de comunicații care transmit diferite informații necesare pentru viața și dezvoltarea acestora. Aceste sisteme sunt organizate în rețele, iar aceste rețele sunt supuse zilnic la vulnerabilități de orice gen.

Vulnerabilitatea rețelei se referă la impactul atacurilor și erorilor asupra comportamentelor rețelei și ale sistemului. Odată cu creșterea defecțiunilor și a atacurilor asupra infrastructurii Internetului cresc și atacurile asupra rețelei unei companii, astfel că se simte tot mai mult nevoia de a dezvolta tehnici pentru a analiza vulnerabilitatea rețelei și a serviciilor. Protejarea împotriva vulnerabilităților rețelei este o muncă complexă. Fiecare dispozitiv, fiecare software și fiecare persoană din rețea poate contribui la securitatea cibernetică sau poate fi un factor de risc. Sunt necesare revizuiri periodice ale politicilor și practicilor de securitate.

Securitatea rețelei unei companii devine continuu o zonă de concentrare extraordinară, indiferent dacă este o companie de dimensiuni mici sau mijlocii, aceasta poate fi o țintă pentru o varietate de atacuri de rețea care pot opri în mod direct afacerea. Monitorizarea rețelei este una dintre cele mai importante sarcini necesare pentru organizarea managementului deplin al unei rețele de calculatoare într-o companie. Soluțiile de monitorizare a performanței rețelei pot ajuta companiile să prevină un dezastru chiar înainte ca acesta să se întâmple. Acestea pot furniza vizualizări privind valorile cheie ale performanței în timp ce generează automat rapoarte de performanță, care includ în mod ideal atât date recente, cât și date istorice. Deși este util pentru urmărirea performanței sistemelor personale, ajută și companiile să facă față amenințărilor la adresa securității care invadează rețelele.

Administrarea rețelelor ocupă un loc foarte important pentru activitatea ulterioară a companiei astfel că monitorizarea traficului rețelei este un segment indispensabil astfel menționăm că în această eră a informației, există multe instrumente disponibile pentru analiza traficului iar majoritatea sistemelor de captare, stocare și indexare a pachetelor de rețea, oferă instrumente pentru evaluarea vizuală a fluxurilor de trafic și căutarea de informații legate de activitatea în rețea, ce ulterior ne permite intreprinderea măsurilor de evitare a atacurilor și vulnerabilităților.

BIBLIOGRAFIE

[1]. HABRAKEN Joe, traducere de VOIN SORIN Doru, Rețele de calculatoare, București, Editura BIC ALL, pag. 270, an. 2002,. ISBN 14538008;

[2]. NEWMAN Mark, Networks, SUA, Editura EBOOK, pag 161, an. 2018. ISBN: 9780198805090;

[3]. BATTISTON Stefano, CALDARELLI Guido, and GARAS Antonios

Multiplex and Multilevel Networks, Marea Britanie, Editura Oxford, pag. 192, an 2018. ISBN: 9780198809456;

[4] DOLOCA Adrian, Rețele de calculatoare și lucru în internet , Iași, Editura U.M.F, pag 297, an. 1997;

[5] BIANCONI Ginestra, Multilayer Networks, Marea Britanie, Editura Oxford, pag. 426, an. 2018. ISBN: 9780198753919;

[6] ESTRADA Ernesto, The Structure of Complex Networks, Marea Britanie, Editura Oxford, pag. 278, an. 2011. ISBN: 9780199591756 ;

[7] http://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf [accesat la data de 19.09.2021, ora 11:32];

[8] MANZUIK Steve, PFEIL Ken, GOLD Andrew, Network Security Assessment: From Vulnerability to Patch, SUA, Ediția Elservier, pag. 402, an. 2006. ISBN: 9780080512532;

[9] SINGER Peter and FRIEDMAN Allan,Cybersecurity and Cyberwar, Editura Oxford , pag 306, an. 2014, ISBN: 978-0199918119;

[10] MACKENZIE Catriona, ROGERS Wendy, DODDS Susan, Vulnerability New Essays in Ethics and Feminist Philosophy, Ediția Oxford, an. 2013, pag. 336, ISBN: 9780199316656;

[11] KENNEDY D., GORMAN J., KEARNS D., AHARONI M., Metasploit: The Penetration Tester's Guide, an. 2011, pag. 328, ISBN-13: 978-1593272883;

[12] ORIYANO Sean-Philip, CEHv9 Computer Ethical Hacking, Editura Cybex, an. 2016, pag. 648, ISBN: 9781119252245;

[13] LUCAS George, Ethics and Cyber Warfare, Editura Oxford, an. 2017, pag.209, ISBN: 9780190276522;

[14]https://stisc.gov.md/ro/incepand-cu-14-ianuarie-2020-pc-urile-care-ruleaza-sistemul-de-operare-windows-7-nu-vor-mai-primi [accesat 21.11.2021 ora 12:45];

[15] ESTRADA Ernesto, Journal of Complex Networks, Editura Oxford, an. 2021, pag. 120;

[16] COUNCIL E., Ethical hacking and countermeasures, Editura Kindle an. 2011, pag. 696, ISBN:978-1435483644;

[17] MARTIN Paul, The Rules of Security Staying Safe in a Risky World, Editura Oxford, an. 2019, pag. 272, ISBN: 9780198823575;

[18] PARKINSON Simon,CRAMPTON Andrew, HILL Richard, Guide to Vulnerability Analysis for Computer Networks and Systems, Ediția Kindle, an. 2018, ISBN: 9783319926247;

[19] MAYNOR David, MOOKHEY K., Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research , an. 2007, ISBN: 9780080549255;

[20] FLICK Tony, MOREHOUSE Justin în Securing the Smart Grid, Editura Kindle an. 2011, ISBN: 9781597495707;

[21]https://www.linuxcapable.com/ro/cum-se-instaleaz%C4%83-metasploit-ramework-pe-ubuntu-20-04/[accesat la data de 29.11.2021 ora 14:54].