Universitatea Tehnică a Moldovei

DETECTAREA VULNERABILITĂȚILOR ÎN CADRUL UNEI REȚELE LOCALE

DETECTION OF VULNERABILITIES IN A LOCAL NETWORK

Masterand:

Deonis Robu, gr. SI-181M

Conducător:

conf. univ., dr.

Victor Moraru

Chişinău 2020

Ministerul Educației Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

FACULTATEA Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef de departament: dr. conf.univ.

Fiodorov Ion

„26" decembrie 2020

DETECTAREA VULNERABILITĂȚILOR ÎN CADRUL UNEI REȚELE LOCALE

Teză de master
Securitate informațională

Masterand: (Deonis Robu)

Conducător

conf. univ. dr.: (Victor Moraru)

Chișinău 2020

Rezumat

Securitatea informatică este o problemă vitală pentru toţi utilizatorii de internet, fie că sunt furnizori de servicii fie că sunt utilizatori. Nevoia tot mai mare de comunicare, pe de o parte şi nevoia de protecţie şi securitate a informaţiilor pe de altă parte sunt două cerinţe diferite şi chiar opuse care trebuie asigurate în reţelele şi sistemele informatice. În condiţiile în care milioane de ceăţeni folosesc în mod curent reţelele de comunicaţii şi calculatoare pentru operaţiuni bancare, cumpărături, plata taxelor şi serviciilor etc. problema securităţii este de maximă importanţă. Au apărut multe organizaţii şi organisme internaţionale care se ocupă de cele mai diverse aspecte ale securităţii informaţionale, de la aspectele legislative, la cele organizatorice, procedurale şi funcţionale.

Problemele cu care se confruntă administratorii, într-o reţea mare, variază de la întreţinerea numeroaselor servere până la rezolvarea problemelor de orice tip ale calculatoarelor clienţilor. Multe firme au un serviciu de asistenţă dedicat exclusiv rezolvării problemelor utilizatorilor. Indiferent de natura problemei, rezolvarea fiecăreia implică un anumit timp de lucru, ceea ce poate conduce la creşterea costurilor generale de utilizare.

În teza de master este descrisă o aplicaţie ce va permite controlul şi monitorizarea porturilor calculatoarelor la distanţă. Transferul de date se va face prin intermediul protocolului TCP.

Aplicaţia elaborată poate fi utilizată pentru administratea calculatoarelor în reţeua locală.

Abstract

Computer security is a vital issue for all Internet users, whether they are service providers or users. The growing need for communication, on the one hand, and the need for the protection and security of information on the other, are two different and even opposite requirements that must be ensured in computer networks and systems. Given that millions of citizens are currently using communications and computer networks for banking, shopping, paying taxes and services, etc. the issue of security is of utmost importance. Many international organizations and bodies have appeared that deal with the most diverse aspects of information security, from the legislative, to the organizational, procedural and functional aspects.

The problems that the administrators face, in a large network, vary from the maintenance of the numerous servers to the solving of the problems of any type of the clients' computers. Many companies have a support service dedicated exclusively to solving user problems. Regardless of the nature of the problem, solving each one involves a certain amount of working time, which can lead to increased overall costs of use.

The master thesis describes an application that will allow the control and monitoring of remote computer ports. The data transfer will be done through the TCP protocol.

The elaborated application can be used for the administration of computers in the local network.

Cuprins

Lista abrevierilor

OS – Operating System

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

SI – Sistem Informațional

ISPO – Internal Security and Public Order

DES – Data Encryption Standard

AES – Advanced Encryption Standard

FAT – File Allocation Table

NTFS – New Technology File System

FTP – File Transfer Protocol

SMTP – Simple Mail Transfer Protocol

TELNET – networking protocol and software program

HTTP – Hypertext Transfer Protocol

DNS – Domain Name System

WWW – World Wide Web

DDS – Digital Signature Standard

IP – Internet Protocol

TCP - Transmission Control Protocol

UDP – User Datagram Protocol

RAM – Random-access memory

SQL – Structured Query Language

XSS – Cross site scripting

XSRF – Cross-site request forgery

WAN – Wide Area Network

LAN – Local Area Network

MAC - Media Access Control

IRC – Internet Relay Chat

NAT – Network Address Translation

PAT – Port Address Translation

ARP – Address Resolution Protocol

Introducere

În prezent reţelele de calculatoare s-au răspîndit în toate domeniile: economic, administrativ, financiar, etc., din această cauză schimbul de date între calculatoare prin reţea trebuie securizat la cel mai înalt nivel. Aşadar, securitatea unui calculator sau a unei întregi reţele este foarte importantă, întrucît nimeni nu este total securizat de atacurile din reţea, orice calculator este vulnerabil într-o oarecare măsură şi într-o reţea cu securitate ridicată, un calculator fără aceste măsuri de securitate poate fi veriga slabă ce poate duce la pierderea datelor sau chiar la defecte în reţea.

Nu putem vorbi în zilele noastre despre transmisia datelor prin intermediul reţelelor de telecomunicaţii fără să vorbim şi de aspectele legate de securitate. Odată cu creşterea vitezelor de transfer şi creşterii numărului de oameni care au acces la o conexiuni de date partajate cu alţi utilizatori se pune problema dacă metodele de criptare folosite pentru asigurarea spaţiului privat sunt cu adevărat eficiente.

Securitatea informatică este o problemă vitală pentru toţi utilizatorii de internet, fie că sunt furnizori de servicii fie că sunt utilizatori. Nevoia tot mai mare de comunicare, pe de o parte şi nevoia de protecţie şi securitate a informaţiilor pe de altă parte sunt două cerinţe diferite şi chiar opuse care trebuie asigurate în reţelele şi sistemele informatice. În condiţiile în care milioane de ceăţeni folosesc în mod curent reţelele de comunicaţii şi calculatoare pentru operaţiuni bancare, cumpărături, plata taxelor şi serviciilor etc. problema securităţii este de maximă importanţă. Au apărut multe organizaţii şi organisme internaţionale care se ocupă de cele mai diverse aspecte ale securităţii informaţionale, de la aspectele legislative, la cele organizatorice, procedurale şi funcţionale.

Securitatea unei reţele depinde nu numai de software-ul instalat în interiorul reţelei (antivirus, firewall, OS, etc.), ci, în egală măsură, de componentele hardware, cunoştinţele în domeniul securităţii a personalului, etc.

Cheia succesului unei lupte reprezintă cunoaşterea atacurilor folosite de duşman, deci dacă considerăm acţiunile hackerilor ca o luptă, este crucială cunoaşterea atacurilor pe care le va utiliza.

Securitatea este un subiect vast şi ocupă o multitudine de imperfecţiuni. Majoritatea problemelor de securitate sunt cauzate intenţionat de persoane răuvoitoare care încearcă să obţină beneficii, să culeagă informaţii dar şi să provoace rău.

Concluzii

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control.

După cercetarea dată, am demonstrat importanţa securităţii în domeniul tehnologiilor informaţionale, precum şi multitudinea de daune ce poate provoca un atacator unei singure persoane sau chiar şi unei întregi organizaţii. Sistemele informaţionale niciodată nu pot fi în siguranţă totală, şi uneori preţul informaţiei este mult mai mare decît preţul acelor sisteme pe care se află, dacă se iau în consideraţie datele confidenţiale, secrete. De aceea, securitatea datelor poate fi un factor critic în economia unei companii. Lupta pentru informaţii nu poate fi stopată, de aceea hackerii vor găsi noi metode complexe de atacuri, pentru a dobîndi informaţiile secrete.

Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată. Asigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Securitatea unei reţele depinde de foarte mulţi factori, precum am spus, de aceea înainte de a securiza o reţea, este nevoie de a calcula nivelul de protecţie în raport cu datele păstrate în acele sisteme. Un utilizator simplu nu va avea nevoie de securitate foarte ridicată, preţul securizării nu trebuie să depăşească preţul informaţiei.

În urma cercetării, am demonstrat că doar dacă un calculator are antivirus şi firewall, el nu este securizat, există numeroase metode de a evita detectarea de către aceste programe, totodată experienţa utilizatorului fiind cel mai important factor ce determină securitatea. Efectuînd teza, ne-am obţinut scopul propus, demonstrînd procesele care au loc pentru principalele tipuri de atacuri, precum şi metodele de protecţie împotriva lor.

Măsurile de protecţie ar fi trebuit de implicat, indiferent de valoarea informaţiei, ci chiar şi din cauza că unele atacuri pot distruge componentele hardware. În dependenţă de nivelul de securitate necesar, protecţia poate fi asigurată printr-o singură parolă, pînă la tehnologii biometrice, smartcard-uri, parole cu tehnici deosebite de criptare, etc.

Bibliografie

1. Cezar A. Securitatea în mediul internet. – Bucureşti: Tehnica, 2008
2. Constantin Popescu. Introducere în criptografie. – Oradea, Universitatea Tehnică Oradea, 2009
3. Mircea F. Tehnologii de securitate alternative pentru aplicaţii în reţea. Universitatea Tehnică din Cluj Napoca, 2009
4. Reţele de calculatoare. Introducere în securitate. Bucureşti, 2012
5. Corneliu Buraga. Securitatea informaţională. – Iaşi: Universitatea A.I.Cuza, 2007
6. Lydia Parziale, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews, Nicolas Rosselot; TCP/IP Tutorial and Technical Overview; Business Machines Corporation, 2006
7. Tom Karygiannis, Les Owens, Wireless Network Security 802.11, Bluetooth and Handheld Devices; Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 2002
8. John E. Canavan; Fundamentals of Network Security; ARTECH HOUSE, 2001
9. Florent Parent, Managing Cisco Network Security: Building Rock-Solid Networks, Syngress Publishing, 2000
10. Christopher Leidigh; Fundamental Principles of Network Security; American Power Conversion; 2005
11. METASPLOIT UNLEASHED – FREE ETHICAL HACKING COURSE. [Resursă electronică]. - Mod de acces: http://offensive-security.com/metasploit-unleashed
12. Software and Tools [Resursă electronică]. - Mod de acces: http://www.cert.org/encyc_article/tocencyc.html
13. Introduction to Network Security [Resursă electronică]. - Mod de acces: http://www.interhack.net/pubs/network-security/
14. Code of practice for information security controls [Resursă electronică]. - Mod de acces: http://iso27001security.com/html/27002.html