MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Microelectronică şi Inginerie Biomedicală

Admis la susţinere
Şef interimar departament MIB:
conf.univ., dr. Serghei RAILEAN

_____
„ ____ ” _____ 2022
)

Abordări metodologice în securitatea serverelor virtuale și fizice bazate pe SO Linux

Teză de master

Student: **Matei Nicolae gr. MN-211M**

Conducător: **Monaico Eduard, dr. conf.**

Chişinău, 2022

ADNOTARE

Acesta lucrare de master a fost elaborată de studentul Matei Nicolae, grupa MN-211M cu tema "Abordari metodologice în securitatea serverelor virtuale si fizice bazate pe SO Linux" Structura lucrarii este formata din Introducere, Capitolul 1. STRUCTURA ȘI DIRECTIILE DE APLICABILITATE ALE SISTETMULUI DE OPERARE LINUX, unde este descris la general despre sistemul de operare Linux. Capitolul 2. PRACTICI DE SECURITATE UTILIZATE PE SCARA LARGĂ ÎN LINUX, în capitolul dat am descris metodele de securitate a SO Linux. Capitolul 3. APLCAREA UNOR MĂSURI DE SECURITATE ÎNTRU-UN SISTEM DE OPERARE EXISTENT, în acest capitol am pus în practica toate masurile de securitate care ne va permite să avem un server sigur și securizat.

Obiectivele acestei lucrari de master este de a planifica asigurarea confidențialității, integrității, autentificării si disponibilitatea datelor de pe server. Prezentarea metodelor de protecție cum ar fi: autentificarea utilizatorilor si controlul accesului, autentificarea cu cheia privata, setarea unui firewall, disponibilitatea datelor si a serviciilor. Instalarea si configurarea unui webserver in linux.

În concluzie, implementarea acestui proiect s-a bazat pe etapele stabilite de principalele obiective ale acestei lucrări. În primul rând, au fost planificate regulile de bază ale firewall-ului, după care au urmat metode de înregistrare mai complexe. A fost dezvoltată o parolă unică de 50 de caractere, greu sau aproape imposibil de ghicit.

După aceea, au fost generate 2 chei RSA, dintre care una este o cheie publică, iar a doua este una privată. Astfel, prin conectarea prin cheia privată, vom fi mai în siguranță și veți ști exact cine are voie să se conecteze la server.

De asemenea, au fost implementate sisteme de jurnal, în care conexiunea la server este fixată pentru câteva zile, deci dacă pe server este comisă o infracțiune, este posibil să se detecteze când și de la ce adresă IP a fost comisă. Pe parcurs, regulile au fost dezvoltate în firewall pentru a se potrivi diferitelor nevoi.

Astfel, securitatea serverelor Linux este la un nivel mai ridicat decât restul, dar mai este loc de îmbunătățire. Evoluția securității avansează în funcție de complexitatea infracțiunilor și atacurilor, așa că știind câte metode de atac există, putem lua măsuri de protecție a datelor.

ANNOTATION

This master's thesis was developed by the student Matei Nicolae, group MN-211M with the theme "Methodological approaches in the security of virtual and physical servers based on Linux OS" The structure of the work consists of Introduction, Chapter 1. STRUCTURE AND APPLICABILITY DIRECTIONS OF THE SYSTEM LINUX OPERATING, where the Linux operating system is described in general. Chapter 2. SECURITY PRACTICES USED ON A LARGE SCALE IN LINUX, in the given chapter I described the security methods of the Linux OS. Chapter 3. APPLICATION OF SOME SECURITY MEASURES WITHIN AN EXISTING OPERATING SYSTEM, in this chapter we put into practice all the security measures that will allow us to have a safe and secure server.

The objectives of this thesis is to plan to ensure the confidentiality, integrity, authentication and availability of the data on the server. Presentation of protection methods such as: user authentication and access control, private key authentication, setting a firewall, availability of data and services. Installation and configuration of a webserver in linux.

The purpose of this license agreement is to ensure the confidentiality, integrity, authentication and confidentiality of server data. The representation of these methods of testing would be: user authentication and access control, private key authentication, setting a firewall, data and service fragmentation. Installing and configuring a web server in linux.

In conclusion, the implementation of this project was based on the stages established by the main objectives of this work. First, basic firewall rules were planned, followed by more complex logging methods. A unique password of 50 characters, difficult or almost impossible to guess, has been developed.

After that, 2 RSA keys were generated, one of which is a public key and the second is a private key. Thus, by connecting via the private key, we will be more secure and you will know exactly who is allowed to connect to the server.

Log systems have also been implemented, where the connection to the server is fixed for several days, so if a crime is committed on the server, it is possible to detect when and from which IP address it was committed. Over time, rules have been developed in the firewall to suit different needs.

Thus, the security of Linux servers is at a higher level than the rest, but there is still room for improvement. The evolution of security advances according to the complexity of crimes and attacks, so knowing how many attack methods there are, we can take measures to protect data.

Cuprins

INTRODUCERE

Securitatea informației a devenit un subiect de interes destul de popular nu numai în comunitatea Linux, ci și în toate domeniile tehnologiei informației. Performanța acestui sistem de operare va fi prezentată pas cu pas cu un exemplu de server configurat conform celor mai recente bune practici pentru securitatea serverului, iar datele stocate pe server vor fi dezvoltate în produsul final.

Pe măsură ce Internetul crește, la fel crește și numărul de servere Linux și venerabilul Linux disponibile publicului.Utilizatorii Linux au la dispoziție o gamă largă de instrumente și metode pentru a se proteja împotriva majorității tipurilor de intruziune, dar nici un sistem de securitate. Cu toate acestea, cu măsuri de securitate îmbunătățite în rețea și implementare corectă, acele sisteme vor deveni o țintă mai dificilă.

Câteva caracteristici ale Linux:

● Flexibilitate. Linux este flexibil deoarece acceptă aplicații de server de înaltă performanță, aplicații desктop și sisteme încorporate.

● Fiabilitate: sistemele Linux nu necesită reporniri periodice atunci când sunt instalate programe sau software noi. Astfel, nivelul de performanță al sistemului este menținut.

● Performanță: gestionarea mai multor utilizatori în același timp nu degradează performanța sistemului.

● Compatibilitate cu rețeaua: Linux este un sistem de operare familiar în ceea ce privește caracteristicile rețelei, cum ar fi: Ușor personalizabil.

Pe măsură ce costul securității eficiente continuă să crească, administratorii de server au decis să-și migreze infrastructura personală la sistemul de operare Linux. Pentru a asigura o securitate eficientă, nicio pretenție nu poate fi făcută prin niciun mijloc că informațiile se află în limitele de securitate ale unui sistem de securitate perfect. Prin urmare, funcționalitatea oricărei configurații de securitate trebuie să includă adaptabilitatea infrastructurii la noile cerințe. Testarea performanței de atac și încărcare pentru a atenua vulnerabilitățile descoperite.

Cerințele de securitate ale serverului se încadrează în una dintre următoarele categorii:

● Confidențialitatea datelor

● Integritatea datelor

● Autentificarea utilizatorului și controlul accesului

● Disponibilitatea datelor și a serviciilor

Scopul lucrării Masterului este de a implementa diferitele măsuri de securitate oferite de serverele Linux pentru a aborda potențialele riscuri și vulnerabilități care sunt deja cunoscute și bine cunoscute, precum și riscurile și vulnerabilitățile care pot apărea în timpul funcționării.

Toate valorile introduse pe parcurs vor fi incluse în serverele create în mediul de virtualizare OpenStacк.

Scopul acestei lucrări

Planificați pentru a asigura confidențialitatea, integritatea, autentificarea și disponibilitatea datelor de pe serverele dvs.

Prezentați metode de securitate, cum ar fi autentificarea utilizatorului și controlul accesului, autentificarea cu chei private, implementarea firewall-ului, disponibilitatea datelor și a serviciilor etc.

Instalarea și configurarea unui server web pe Linux.

Conform planului tehnic:

Este selectat un set de distribuție în care cele mai recente practici de securitate a serverului sunt implementate pas cu pas. Primul pas este să gestionați ce utilizatori și grupuri se pot conecta prin SSH. Se fac apoi modificările necesare pentru a limita riscul unui atac care compromite contul de administrator (rădăcină) prin conectarea utilizatorului cu o cheie privată și dezactivarea conexiunii la server cu o parolă. Schimbat implicit prin portul SSH. Un sistem firewall complex este apoi configurat pentru a filtra traficul prin restricționarea accesului la server în funcție de diferite criterii care vor fi întâlnite în partea actuală a tezei.

În acest fel, serverele web reduc riscul următoarelor tipuri de atacuri.

❑ Compromisarea contului root

❑ Atacurile DDoS:

➢ Teardrop

➢ Synflood

❑ Furtul de sesiune

Rezultatul final este un mediu sigur pentru găzduirea serviciilor web cu risc limitat.

BIBLIOGRAFIE

1. Introduction to Linux. A Hands on Guide

   Disponibil: https://losst.ru/wp-content/uploads/2016/08/younglinux.info-Introduction-to-Linux-A-Hands-on-Guide-Vvedenie-v-Linux-Rukovodstvo-po-rabote.pdf

2. Structura directoarelor Linux
   Disponibil:https://www.linuxando.com/tutorial.php?t=A%20estrutura%20de%20diret%C3%B3rios%20Linux_6

3. Distributii Linux

   Disponibil: https://it.wikipedia.org/wiki/Distribuzione_Linux

4. Tipuri de distributii Linux

   Disponibil: https://it.linux-console.net/?p=1388#gsc.tab=0

5. Managmentul pachetelor RPM

   Dispoonibil: https://web.mit.edu/rhel-doc/3/rhel-sag-pt_br-3/ch-rpm.html

6. Diferenta dintre terminal, consola, shell

   Disponibil: https://www.geeksforgeeks.org/difference-between-terminal-console-shell-and-command-line/

7. Instrumente pentru a proteja confidentialitate

   Disponibil: https://www.dltec.com.br/blog/linux/ferramentas-para-proteger-sua-privacidade-na-internet/

8. Web server

   Disponibi: https://www.techtarget.com/whatis/definition/Web-server

9. What is Apache Web Server

   Disponibil: https://www.sumologic.com/blog/apache-web-server-introduction/

10. Ce este Nginx

    Disponibil: https://www.nginx.com/resources/glossary/nginx/

11. LiteSpeed web server
    Disponibil: https://www.hivelocity.net/kb/what-is-litespeed/

12. Ce este Kernel

    Disponibil: https://it.tipsandtrics.com/how-easily-upgrade-ubuntu-s-linux-kernel-with-ukuu-763488

13. Ghid SSH server

    Disponibil: https://linuxhub.ro/ghid-esential-ssh-servere-clienti-si-chei-criptografice/

14. Generalitati IPTables

    Disponibil: https://interface31.ru/tech_it/2020/02/osnovy-iptables-dlya-nachinayushhih-chast-1.html