Ministerul Educației, Culturii și Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
FACULTATEA Calculatoare, Informatică și Microelectronică
Departamentul Informatică şi Ingineria Sistemelor

Admis la susținere:
Șef DIIS: conf. univ., dr. Sudacevschi Viorica
"09" 01 2019

MANAGEMENTUL SECURITĂȚII INFORMAȚIONALE ȘI ANALIZA EVENIMENTELOR DE SECURITATE ÎN REȚELE DE CALCULATOARE

Teză de master în
Calculatoare şi Reţele Informaţionale

Masterand: Pavlov Mihail
Conducător : Victor Moraru

Chișinău – 2019

ADNOTARE

La teza de master: „Managementul securității informaționale și analiza evenimentelor de securitate în rețele de calculatoare”, elaborat de Pavlov Mihail, Chișinău, 2019.

Cuvinte cheie: securitatea rețelelor de calculatoare, riscurilor şi vulnerabilități a rețelelor, instrumentele și tehnici de securității, securitatea informației, procesul de management al securității rețelei, politica de securitate a rețelei.

Lucrarea de față are drept scop implementarea unui sistem de analiză a evenimentelor de securitate în rețele de calculatoare. La baza sistemului stă un server Ubuntu cu serviciile de tip OpenSource - Easticsearch, Logstash şi Kibana. Sistemul reprezintă un instrument pentru analist în domeniul securității rețelei și presupune colectarea, ajustarea, corelarea și vizualizarea evenimentelor de securitate.

Această lucrare poate servi drept ghid pentru implementarea și managementul securității a unei rețele existente sau planificate din punct de vedere organizatoric cît și tehnic. Totodată reprezintă un studiu ce ține de asigurarea securității informaționale în rețelele de calculatoare, fiind abordate subiectele referitoare la proiectarea și managementul securității precum și metode și tehnicile de protecție a rețelelor și serviciilor oferite de rețea.

Teza vizează implementarea unui sistem de analiză a stării securității, ceea ce de fapt este foarte actual în diversitatea rețelelor și al serviciilor de rețea. Odată cu creșterea numărului elementelor într-o rețea, crește riscul pentru securitatea informațiilor care circulă în ea, astfel este necesar de aplicat măsuri și tehnici conform cerințelor contemporane. Fiecare din elemente trebuie securizat și monitorizat în modul corespunzător, ca la apariția unor incidente să fie generate alerte și întreprinse măsuri de contracarare. Sistemul are o interfață grafică destul de intuitivă care permite vizualizarea evenimentelor de securitate de la diferite surse și prin intermediul mai multor protocoale de rețea colectate centralizat.

Memoriul explicativ conține: Introducere, 3 capitole, concluzii, bibliografie cu 16 titluri, dintre care 71 pagini text de bază, 34 figuri, 3 tabele şi o anexă pe 5pagini.

Capitolul 1 definește concepte de bază a securității rețelelor, metode de proiectare a securității în raport cu riscurile și referințe la acte necesare pentru documentarea rețelei de calculatoare.

Capitolul 2 definește rolurile de bază, responsabilitățile și descrie activitățile desfășurate în procesul de management al securității rețelei. Totodată sunt examinate măsurile tehnice aplicabile pentru asigurarea dimensiunilor securității informațiilor procesate.

Capitolul 3 descrie structura generală a sistemului de analiză a evenimentelor, inclusiv toate metodele de colectare și transmitere centralizată a evenimentelor de securitate. Este prezentat un set de recomandări și mostre pentru documentarea mediului de rețea securizat conform standardelor și cerințelor contemporane.

ANNOTATION

In the master thesis: "Information security management and analysis of security events in computer networks", elaborated by Pavlov Mihail, Chisinau, 2019.

The Explanatory Memo contains: Introduction, 3 chapters, conclusions, bibliography with 16 titles, of which 71 basic text pages, 34 figures, 3 tables and an annex on 5 pages.

Key words: computer networks security, network risks and vulnerabilities, security tools and techniques, information security, network security management, network security policy.

This paper aims to implement a system for analyzing security events in computer networks. At the core of the system is a Ubuntu server with OpenSource services - Easticsearch, Logstash and Kibana. The system is an analytical tool for network security and involves collecting, adjusting, correlating, and viewing security events.

This paper can serve as a guide of implementation and management of an existing or planned network from both approaches, technically and organizationally. At the same time, it represents a study on the provision of information security in computer networks, being addressed the topics related to security design and management as well as methods and techniques of protection of networks and services provided by the network.

The thesis aims at implementing a security status analysis system, which is very actual in our days when we have a diversity of networks and services. With the increase of the number of network elements, the risk for the security of the information flow increases, so it is necessary to apply controls and techniques according to the contemporary requirements. Each item must be secured and monitored in the proper way as alerts are generated when incident occur. The system has a fairly intuitive graphical interface that allows viewing of security events from different sources and are centrally collected through multiple network protocols.

Chapter 1 defines basic concepts of network security, security design methods in relation to risks and references for documenting process of the computer network.

Chapter 2 defines the basic roles and responsibilities, also describes the activities performed in the network security management process. At the same time, the applicable technical measures are being examined to ensure all security dimensions of the processed information.

Chapter 3 describes the general structure of the event analysis system, including all methods of collecting and centrally transmitting security events. A set of recommendations and templates are presented for documenting a network security environment according to standards and contemporary requirements.

Cuprins