OSSIM alat za nadzor mreže

Tunuković, Tomislav

Undergraduate thesis / Završni rad

2014

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:779315

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

zir.nsk.hr

Image not found or type unknown

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

OSSIM ALAT ZA NADZOR MREŽA

Završni rad

Tomislav Tunuković

Osijek, 2014.

SADRŽAJ

1. UVOD 1
1.1 Zadatak završenog rada 1
2. SIGURNOST I NADZOR U MREŽAMA 2
2.1. Općenito o OSSIM alatu za nadzor mreža 3
2.2. Objedinjeni alati otvorenog koda 6
2.3. Arhitektura OSSIM alata 7
2.4. Funkcijske komponente OSSIM alata 9
3. INSTALACIJA I KONFIGURIRANJE OSSIM ALATA ZA NADZOR MREŽA 11
3.1 Instalacija 11
3.2. Konfiguriranje i implementacija USM – a 12
4. ANALIZA FUNKCIONALNOSTI SIGURNOSNIH ALATA 15
4.1. Otkrivanje upada u sustav na temelju prepoznavanja uzoraka 15
4.2. Testiranje metode otkrivanje upada u sustav na temelju prepoznavanja uzoraka 20
4.3. Otkrivanje anomalija u radu sustava 22
4.4. Nadzor rada i performansi sustava 24
5. ZAKLJUČAK 25
LITERATURA 26
SAŽETAK 27
ABSTRACT 27
ŽIVOTOPIS 28

SAŽETAK

U radu su opisani i testirani alati otvorenog koda besplatne Linux distribucije namijenjeni administraciji mrežnih i računalnih sustava, njihovoj zaštiti te uočavanju i sprečavanju zlonamjernih napada. Nakon instalacije, implementacije OSSIM – a (Open Source Security Information Management) i njegovog konfiguriranja testirani su sljedeći alati : otkrivanje upada u sustav na temelju prepoznavanja uzoraka, otkrivanje anomalija u radu sustava te nadzor rada i performansi sustava. Svaki od alata je analiziran, opisan i testiran u računalnoj internetskoj mreži. Tijekom testiranja utvrđeno je da je OSSIM alat uspješno prepoznao lažne napade na testiranu mrežu, zabilježio ih u dnevnik zapisa te alarmirao administratora o pokušaju upada u mrežu i samim time pokazao svoju učinkovitost.

KLJUČNE RIJEČI: OSSIM, mreža, napad, alat, sustav, zaštita.

ABSTRACT

In this text is the description and result of tests of open source free Linux distribution tool which it's primary objective is to administrate, to protect and to detect intrusion of both the computer and network system. After software installation, implementation and finally the configuration of Open Source Security Information Management (OSSIM) next tools have been tested : intrusion detection based on pattern recognition, system anomalies detection and system performance supervision. Each tool has been analysed, described and tested in the computer network. During the test it was confirmed that OSSIM tool has successfully recognized false attacks on the tested network, noted them in the log diary and succesfully alarmed network administrator and thus demonstrated its effectiveness.

KEY WORDS : OSSIM, network, tool, protection, system, intrusion