REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENNE
INSTITUT DE L'INFORMATIQUE

MEMOIRE DU PROJET DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME D'INGENIEUR D'ETAT EN INFORMATIQUE

Option
SYSTEME D'INFORMATION

Thème

APPORT DE XML POUR LES SYSTEMES D'AIDE A L'INVESTIGATION POUR LES FIREWALLS

Organisme d'accueil : CERIST
Encadré par : M^me^ H.Mellah

Réalisé par : M^elle^ Afrit Siham
M^elle^ Rahim Samia

Devant le jury composé de:

M^me^ Akli	Présidente
M^me^ Gharbi	Examinatrice
M^r^ Aklouf	Examinateur

N°79 - Promotion 2003

Résumé:

Un Firewall est un système permettant de protéger un réseau local des attaques provenant d'Internet, en contrôlant l'accès au réseau et en limitant le trafic entrant et sortant. Les Firewalls installés sur les machines sont de type divers, ce qui engendre une différence de format au niveau des journaux de bord des connexions qui sont générés par les Firewalls. Ces journaux (plus communément appelés fichiers log) sont dans la majorité des cas difficilement interprétés par l'administrateur réseau.

L'objectif de notre travail est dans un premier temps d'homogénéiser les formats des fichiers log en utilisant la norme XML pour générer un format standard directement exploitable par un interpréteur automatique, en proposant certaines solutions aux points de défaillances des Firewalls, et dans un second temps essayer d'étudier ce que le langage de définition des interfaces (IDL) de CORBA peut faire dans ce genre de situation.

Mots clés : Firewalls, Log, XML, DTD, XSL, IDL, CORBA, Filtrage.

Abstract:

Firewall is a system permitting to protect a local network of the attacks coming from Internet, while controlling the access to the network and while limiting the incoming and retiring traffic. The Firewall installed on the machines is of various types, what generates a difference of format of the connections' newspapers that is generated by the Firewalls. The administrator network in the majority of the cases difficulty interprets these newspapers (more commonly named files log).

The objective of our work is in a first time to homogenize the format of log file while using the XML norm to generate a standard format directly exploitable by an automatic interpreter, while proposing some solutions to the points of failings of the Firewalls, and in a second time to try to study what the language of definition of the interfaces (IDL) CORBA can make in this kind of situation.

Key words: Firewalls, Log, XML, DTD, XSL, IDL, CORBA, Filtering,.

Table des matières

CHAPITRE II: LA NORME XML

Partie I: Concepts Généraux Sur Les Documents

Partie II: XML(eXtensible Markup Language)

CHAPITRE II: L'IDL DE CORBA

CHAPITRE IV: CONCEPTION