Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique

Mémoire de Post-graduation spécialisée

En sécurité Informatique

Thème

Un outil de collecte de paquets TCP/IP et extraction de leurs contenus pour la surveillance des réseaux

Présenté par : Mr. BARECHE Mohammed Nadji

Soutenu le 01 /12 /2015

devant le jury composé de :

Mm	BESSAI Fatma Zohra	Maître de Recherche, CERIST	Présidente
Mr	AMIRA Abdelouahab	Attaché de Recherche, CERIST	Examinateur
Mr	BOUCENNA Fateh	Attaché de Recherche, CERIST	Examinateur
Dr.	NOUALI Omar	DIRECTEUR DE RECHERCHE, CERIST	Directeur de mémoire
Mr.	KRINAH Abdelghani	CHARGE DE RECHERCHE, CERIST	Co-directeur de mémoire

2014/2015

Résumé

La sécurité informatique est de nos jours devenue un souci majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques [25]. Et tant que le réseau local est le cœur de la majeure partie de l'activité informatique de nos organismes, tous efforts de sécurisation s'y répercutent avec d'autant plus d'effet. Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux [26].

Dans ce sujet, ce mémoire a pour but de présenter notre projet « SnifferParserProject ». Ce Sniffeur permet à examiner et analyser le trafic dans le réseau. Il décode ce trafic et fait le un sens.

Mots clés : Sniffeur, trafic, réseau, IP, TCP, ISO.

Abstract

Computer security is today become a major problem in the management of corporate networks and for the growing number of individuals to connect to the Internet. The transmission of sensitive information and the desire to ensure the confidentiality of the latter has become a key point in the development of computer networks [25]. And as the local network is the heart of most computer activity of our organizations, all of them affects security efforts all the more effective. This consideration alone justifies paying special attention to securing LANs [26].

In this subject, the purpose of this thesis to present the project "SnifferParserProject". This Sniffer allows reviewing and analyzing all traffic in the network. It decodes this traffic and make's sense.

Keywords: Sniffer, traffic, network, IP, TCP, ISO.

Table de matière

Table des figures