

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	Examineur
Mr	BOUCENNA Fateh	Attaché de Recherche, CERIST	Examineur
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

Résumé	3
INTRODUCTION GENERALE	8
CHAPITRE I INTRODUCTION AUX RESEAUX INFORMATIQUE	11
Introduction :	11
1. Notion de base des réseaux :	11
1.1. Définition :	11
1.2. Topologie des réseaux :	12
1.3. Catégorie des réseaux :	13
2. Le modèle OSI « OpenSystems Interconnections » :	14
2.1. Description du modèle OSI :	14
2.2. Transmission de données à travers le modèle OSI :	15
3. Le modèle TCP/IP :	16
3.1. Couche Application :	16
3.2. Couche Transport :	16
3.2.1. TCP « Transport Control Protocol » :	17
3.2.2. UDP « User Datagram Protocol » :	19
3.3. Couche Internet :	20
3.3.1. IP « Internet Protocol » :	20
3.3.2. ICMP :	26
3.3.3. ARP/RARP :	27
3.4. Couche interface réseau :	27
Conclusion :	28
CHAPITRE II ETUDES DES SNIFFEURS EXISTANTS	30
Introduction :	30
1. L'utilité des Sniffeurs:	30
2. Quelques sniffeurs existants:	31
2.1. Wireshark :	31
2.2. Carnivore :	32
2.3. Dsniff :	34
2.4. Snort :	36
2.4.1. Que permet-il de faire exactement ?	36
2.4.2. Modes d'utilisation de Snort	36
2.5. Tcpdump :	37

2.5.1. Description de fonctionnement de Tcpdump :	38
2.5.2. Exemples d'utilisation de Tcpdump :	39
3. Conclusion	40
CHAPITRE III PRESENTATION DU PROJET	42
Introduction	42
1. Aperçu de la solution proposée :	42
2. Importance de Sniffer de paquets :	42
3. L'architecture de l'application	42
3.1. Les fonctionnalités de SNPAPR :	42
3.2. Conception de système :	43
4. Diagrammes de fonctions :	43
4.1. Diagrammes de flux de données DFD :	43
4.2. Diagramme de déploiement :	45
4.3. Diagramme de composants :	46
4.4. Diagrammes de structure :	47
4.5. Diagramme de cas d'utilisation :	51
5. Conclusion	52
CHAPITRE IV L'APPLICATION « SnifferParserProject »	54
Introduction	54
2. Outils et bibliotheques utilisés :	54
2.1. Jpcap :	54
2.2. PCAP :	55
2.3. LibPCAP :	55
2.4. WinPCAP	55
2.5. Le Parseur :	55
3. Environnement de développement :	55
4. L'installation et l'exécution de l'application	57
5. Avantages de SNPAPR	57
6. Algorithmes et codes de source de SNPAPR :	57
6.1. Analyzer code :	58
6.2. Parser code :	58
6.3. Stat code :	60
6.4. Les interfaces graphiques et leurs codes source :	61
7. CONCLUSION	69

Conclusion générale et Futurs perfectionnements.....	70
Références	71

Table des figures

Figure 01 Topologies des réseaux	12
Figure 02 Catégorie des réseaux	13
Figure 03 Modèle OSI	14
Figure 04 Transmission de données dans le modèle OSI	15
Figure 05 Modèle OSI versus modèle TCP/IP	16
Figure 06 Suite de protocoles du modèle TCP/IP	16
Figure 07 Structure de l'en-tête TCP	17
Figure 08 Etablissement d'une connexion TCP	19
Figure 09 Structure de l'en-tête UDP	19
Figure 10 Structure de l'en-tête du datagramme IP	21
Figure 11 Représentation d'adresse IPv4 des différentes classes	25
Figure 12 Plages d'adresse IPv4 des différents classes	25
Figure 13 Encapsulation d'un message ICMP	27
Figure 14 Interface principale de Wireshark.....	31
Figure 15 Wireshark en cour d'exécution.....	32
Figure 16 Le programme de configuration de Carnivore.....	34
Figure 17 dsniff en cour d'execution.....	35
Figure 18 Snort initialisation.....	37
Figure 19 Diagramme de flux de données d'un sniffeur standard.....	44
Figure 20 DFD pour le contexte d'un sniffeur standard.....	44
Figure 21 DFD de SNPAPR	44
Figure 22 DFD pour le processus d'analyseur des protocoles avec SNPAPR	44

Figure 23 DFD pour le processus de parseur des paquets avec SNPAPR.....	45
Figure 24 Diagramme de déploiement	46
Figure 25 Diagramme de composants	47
Figure 26 Diagramme de structure	48
Figure 27 Module d'entrée pour la reconnaissance de type des paquets	48
Figure 28 Module d'analyse des protocoles	49
Figure 29 Module de sortie	51
Figure 30 Diagrammes de cas d'utilisation	52
Figure 31 le déroulement de processus de parseur	59
Figure 32 Fenêtre des statistiques	61
Figure 33 Choix de L'interface réseau et les options	63
Figure 34 L'interface de l'application en cour d'exécution	64
Figure 35 Message de confirmation 'sauvegarder le fichier de capture'.....	65
Figure 36 Message d'erreur 'besoin d'accès root pour l'exécution'.....	66
Figure 37 Message d'erreur 'parser un fichier de capture non compatible' ...	67
Figure 38 erreur bibliothèques Jpcap introuvable	68
Figure 39 erreur bibliothèques Jpcap et/ou Libpcap/Winpcap introuvable	69