République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderahmane Mira de Béjaïa

Faculté des Sciences et Sciences de l'Ingénieur

Département d'Informatique

École Doctorale Réseaux et Systèmes Distribués

Mémoire de Magister en informatique

***

Option

Réseaux et Systèmes Distribués

Thème

Détection de l'attaque Eclipse dans le réseau eDonkey

Présenté par : Asma DAOUDI

Directeur du mémoire : Pr. BOUABDALLAH Abdelmadjid

Devant le jury composé de :

Président	DAHMANI Adbennasser	Professeur	Université de Bejaia,Algérie
Rapporteur	BOUABDALLAH Abdelmadjid	Professeur	UTC, Compiègne,France
Examinateur	AHMED-NACER Mohamed	Professeur	USTHB, Alger,Algérie
Examinateur	BADACHE Nadjib	Professeur	USTHB, Alger,Algérie
Invité	TARI Abdelkamel	Chargé de cours	Université de Bejaia,Algérie

Promotion 2006 – 2007

Résumé

Dans ce présent travail, nous avons analysé l'attaque Eclipse dans le cadre du réseau eDonkey. Dans cette attaque, un serveur attaquant a pour but de cacher la partie surveillée du reste du réseau en prenant comme cible la liste des serveurs du réseau eDonkey. Nous avons identifié deux scénarios différents de l'attaque Eclipse : Le premier scénario traite le cas où l'attaque est menée par un seul attaquant et le deuxième scénario traite le cas de plusieurs attaquants. Pour faire face à cette attaque nous avons proposé une solution basée sur la taille des listes des serveurs d'un client détecteur. Les résultats obtenus montrent l'efficacité de la solution proposée à détecter les deux scénarios d'attaques et à isoler les serveurs attaquants du reste des serveurs du réseau. Cependant, des fausses (accusations) alertes peuvent avoir lieu. Pour cela, nous avons proposé d'utiliser le profilage des utilisateurs, des ports TCP, UDP pour minimiser l'impact de ces fausses accusations.

Mots clés : réseax pair-à-pair, eDonkey, l'attaque Eclipse, détection d'attaques dans les réseaux P2P.

Abstract

In this work, we analyzed the Eclipse attack in an eDonkey network. In an Eclipse attack, attacker goal is to keep the supervised part hidden from the rest of the network using the list of servers in eDonkey network as a target. Two different scenarios of Eclipse attack are identified. The first one treats the case where there is only one attacker mount an Eclipse attack on an eDonkey network. The second scenario treats the case of several attackers. To prevent from this attack, we propose solution based on lists of servers size of detector's client. The obtained result shows the efficiency of our solution to detect the two scenarios of Eclipse attack and avoid (isolate) those attackers from the rest of the network. However, false positive can happened. We proposed to use a profiling of the users, TCP and UDP ports to mitigate false positive affect.

Keywords : Peer To Peer Networks, eDonkey Network , Eclipse attaks, attaks detection in P2P networks .

Dédicaces

Je dédie ce travail à ma très chère mère ,
A mon adorable père,
A mes très chères sœurs et frères ,
A toute ma famille,
A tous ceux que je ne cite pas mais aux quels je pense très fort,
vous mes amis(es)

Remerciements

Je remercie Dieu le tout Puissant qui m'a donné la force et la volonté pour réaliser ce modeste travail.

Mes remerciements iront à mes encadreurs Abdelmadjid BOUABDALLAH, Professeur à l'UTC (Compiègne, France) et Hani Ragab Hassen, Docteur à l'UTC (Compiègne, France) pour m'avoir soutenu durant cette année de Magister. Ce travail n'aurait jamais pu aboutir sans eux, qui sont toujours su me consacrer des moments de leurs temps, me guider et me conseiller. Je souhaite leur transmettre l'expression de ma reconnaissance et ma plus profonde gratitude.

Je remercie tout particulièrement les membres de jury, qui ont accepté de juger mon travail.

Je tiens aussi à remercier chaleureusement Kamel TARI, le Chef de département d'informatique et responsable de l'école doctorale, qui nous a toujours encouragé et soutenu, et je tiens aussi à remercier Monsieur Djoudi TOUAZI responsable du centre de calcul pour son aide et sa gentillesse avec tous le monde.

Mes sincères remerciements à tous nos enseignants et tous ceux qui ont contribué à la création et la réussite de l'école doctorale ReSyD de Bejaia.

Je remercie également mes amis et collègues de l'école doctorale de Béjaïa pour avoir créé un environnement d'études convivial durant toute cette formation.

Je ne pourrais clôturer ces remerciements sans me retourner vers ma raison d'être qui ont toujours été à mes cotés et qui m'ont entourée d'affection, de soutien et d'amour, ma très chère mère et mon adorable père. Qu'ils trouvent dans ce modeste travail le fruit de leur soutien.
Je voudrais aussi remercier profondément mes frères et sœurs,ainsi que toute ma famille.

Enfin je remercie tous ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail.

Table des matières