Amélioration du système SNORT : Réduction du taux de faux positif

Université Kasdi Merbah de Ouargla
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et des Technologie de l'Information
Nom et prénom : Menaa Khaoula; Mennai Nabila.
Email: khauokha8@gmail.com ; nabilamennai390@gmail.com.
Encadreur : Boukhamla Akram.
Co encadreur: Salah Euschi.

Résumé

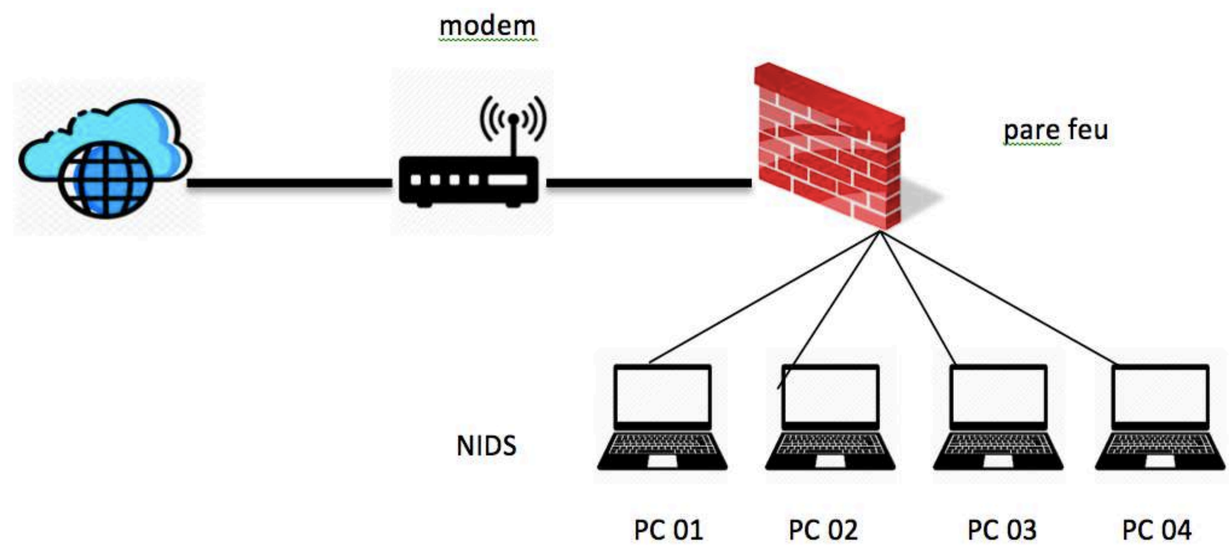
L'étude de la sécurité des réseaux LAN , nous a permis de constater qu'il n'est pas facile de protéger les systèmes informatiques et les réseaux contre le risques des attaques qui progressent chaque jour , surtout avec le développement des outils sophistiqués permettant de trouver les failles, et par la suite, les exploiter d'une façon malveillantes. Par conséquent, il est nécessaire de détecter les intrusions tant que cela est possible, grâce aux mécanismes de détection d'intrusion, qui détectent l'intrusion et découvrent l'utilisation du système informatique à des fins illégales en émettant une alerte.
Nous avons réalisé une installation de Snort qui est un système de détection d'intrusion en quatre PC, puis, nous avons mis en place un petit réseau LAN et lancé des attaques de type DoS (Denial of Service) pour les détecter via Snort.
Mots clés : attaques informatiques, Snort, IDS, Dos.

Introduction

L'expansion des systèmes informatiques ont rendu les réseaux indispensables pour les entreprises.
Mais si toutes ces innovations ont apportés de très nombreux avantages aux entreprises, elles sont accompagnées de nouveaux risques inhérents à ces nouvelles technologies, le piratage informatique. En effet, ces attaques sont de plus en plus nombreuses, efficaces et simple à mettre en œuvre.
Elles sont utilisés pour voler des informations ou simplement détruire des données numériques ou arrêter le service.
Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelés IDS (Intrusion Détection System), les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche.
Dans le cadre de notre projet, nous nous concentrerons sur l'amélioration de détection des attaques de types dénis de service (DoS).
Alors que nous allons détecter l'entrée des attaques du type de dénis de service grâce à l'utilisation de Snort IDS (intrusion détection système).

Matériels et Méthodes

Notre idée initiale est d'améliorer certaines des lacunes de Snort et nous l'avons trouvé faible contre les attaques DoS. Nous avons identifié une attaque de ce type et l'avons lancée dans notre réseau.
Avant cela, nous avions mis 4 ordinateurs avec ubuntu 16.04 comme système.
Puis nous avons installé Snort sur tous les appareils (des règles ont été ajoutées pour répondre à l'attaque DoS et attaque de Backdoor/ Subseven Un réseau local a été créé.



L'architecture de réseau LAN

```
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@lenovo-Lenovo-ideapad-100-15IBY:~# hping3 --flood -p 80 -S 192.168.1.40
HPING 192.168.1.40 (wlp4s0 192.168.1.40): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Lancement d'une attaque DoS

```
root@lenovo-Lenovo-ideapad-100-15IBY:~# sudo snort  -A console -q -c /etc/snort
/snort.conf  -i wlp4s0
04/16-09:39:23.191944  [**] [1:1000001:1] Possible TCP Dos!! BE CARFUL !! [**]
[Priority: 0] {TCP} 192.168.1.40:57180 -> 192.168.1.36:80
04/16-09:39:33.028814  [**] [1:1000001:1] Possible TCP Dos!! BE CARFUL !! [**]
[Priority: 0] {TCP} 192.168.1.40:190 -> 192.168.1.36:80
```

Détection des attaques par Snort

Résultat

Dans ce travail , nous avons illustré l'importance de la présence du système de détection d'intrusion et le mécanisme de fonctionnement de Snort . Nous avons vu à la fin, comment Snort a pu détecter une attaque DoS.
Nous avons pu créer une règles qui génère une alerte lors d'un lancement d'une attaque DoS .

Conclusion

Grâce à notre étude de cas du système de détection d'intrusion Snort qui a été présenté en open source, nous avons pu voir jusqu'où Snort était capable de détecter les attaques. Nous avons appris que les grandes menaces proviennent généralement de l'intérieur de réseau et non de l'extérieur.
Nous avons pu apporter quelques améliorations en ajoutant des règles qui servent notre réseau.
Nous aspirons à détecter d'autres types d'attaques en plus du DoS parmi eux attaque DDoS.

References

M. ABBAS Massinissa, M. AOUADI Djamel: Détection d'intrusions dans les réseaux LAN : IDS Snort sous LINUX, Promotion 2016/2017 .
M.TOUATI Azeddine: Détection d'intrusion dans les réseaux LAN/ Installation et configuration de l'IDS-SNORT, Promotion 2016/2017 .