Université Sultan Moulay Slimane

Faculté Polydisciplinaire **Khouribga**

Sciences Mathématiques et Informatique

Administration Réseaux

Chapitre 5 : Sécurité dans les réseaux

Pr. Ibtissam Bakkouri

i.bakkouri@usms.ma

Année Universitaire : **2022/2023**

Plan

Introduction

La sécurité des équipements dans les réseaux est essentielle pour garantir un fonctionnement efficace et sécurisé des infrastructures de communication modernes. Les réseaux sont constamment exposés à des menaces potentielles, telles que les cyberattaques, les malwares, les tentatives d'accès non autorisées, et d'autres activités malveillantes. La sécurité des équipements dans les réseaux vise à protéger ces équipements contre de telles menaces et à minimiser les risques pour les données, les communications et les opérations.

Introduction

Voici quelques raisons pour lesquelles la sécurité des équipements dans les réseaux est cruciale :

- **Confidentialité des données :** Les équipements dans les réseaux traitent et transportent souvent des données sensibles, telles que des informations de clients, des données financières, des secrets industriels, etc. La sécurité des équipements vise à protéger la confidentialité de ces données en empêchant tout accès non autorisé.
- **Intégrité des données :** Les équipements dans les réseaux garantissent également l'intégrité des données en s'assurant qu'elles ne sont pas altérées ou corrompues pendant leur transit. Une sécurité robuste des équipements est donc nécessaire pour empêcher toute altération ou manipulation non autorisée des données.

Introduction

- **Disponibilité du réseau :** La disponibilité du réseau est essentielle pour garantir un fonctionnement efficace des communications. Les attaques contre les équipements du réseau peuvent entraîner des interruptions de service, des pannes et des temps d'arrêt coûteux. La sécurité des équipements vise à protéger la disponibilité du réseau en minimisant les risques d'attaques et de pannes.
- **Confiance des utilisateurs :** La confiance des utilisateurs est un élément clé dans l'adoption et l'utilisation des réseaux. Les utilisateurs doivent être assurés que leurs données et leurs communications sont sécurisées pour utiliser les services de communication en toute confiance. La sécurité des équipements dans les réseaux contribue à établir cette confiance en protégeant les données et les communications des utilisateurs.

Introduction

- **Protection contre les attaques malveillantes :** Les attaques malveillantes, telles que les cyberattaques, les attaques par déni de service (DDoS) et les attaques de type "homme du milieu", sont de plus en plus sophistiquées et peuvent causer des dommages importants aux réseaux et aux services de communication. La sécurité des équipements dans les réseaux est cruciale pour protéger contre ces types d'attaques et minimiser les risques de perturbations du réseau.

La sécurité des équipements dans les réseaux est d'une importance cruciale pour garantir un fonctionnement efficace et sécurisé des infrastructures de communication modernes. Elle contribue à protéger la confidentialité, l'intégrité et la disponibilité des données, à établir la confiance des utilisateurs, et à protéger contre les attaques malveillantes.

Introduction

Il existe divers types d'équipements réseau utilisés dans les infrastructures de communication modernes, et chacun peut présenter des vulnérabilités spécifiques en fonction de sa fonction, de sa configuration, de sa gestion et de son environnement. Voici quelques exemples d'équipements réseau couramment utilisés et de leurs vulnérabilités potentielles :

- **Routeurs :** Les routeurs sont des dispositifs clés dans les réseaux qui dirigent le trafic entre différentes parties du réseau. Ils peuvent être vulnérables à des attaques telles que l'injection de paquets malveillants, les attaques d'écrasement de tampon, les attaques de déni de service (DoS) et les attaques de contournement d'authentification si les mises à jour de sécurité ne sont pas appliquées, si les configurations sont faibles, ou si les mots de passe sont facilement devinables.

Introduction

- **Commutateurs :** Les commutateurs sont utilisés pour relier les appareils sur un réseau local (LAN) et sont responsables de la gestion du trafic entre les différents ports. Les vulnérabilités potentielles des commutateurs incluent les attaques d'usurpation d'adresse MAC, les attaques d'inondation de commutation (flooding), et les attaques de redirection de trafic. La sécurité des commutateurs peut être compromise si les mises à jour de sécurité ne sont pas appliquées, si les configurations sont mal sécurisées ou si les protocoles de gestion sont faibles.

Introduction

- **Pare-feu :** Les pare-feu sont utilisés pour protéger les réseaux en contrôlant les flux de trafic entre les réseaux internes et externes. Les pare-feu peuvent être vulnérables à des attaques telles que les contournements de règles, les injections de paquets malveillants, les attaques de saturation, et les attaques de contournement d'authentification si les règles de pare-feu ne sont pas correctement configurées, si les mises à jour de sécurité ne sont pas appliquées, ou si les politiques de sécurité sont faibles.

Introduction

- **Points d'accès sans fil :** Les points d'accès sans fil (Wi-Fi) sont utilisés pour permettre la connectivité sans fil dans les réseaux. Ils peuvent être vulnérables à des attaques de type **homme du milieu**, des attaques d'usurpation d'identité, des attaques d'injection de paquets malveillants, et des attaques de déni de service si les protocoles de sécurité sans fil ne sont pas correctement configurés, ou si les mots de passe d'accès sont faibles.
- **Serveurs :** Les serveurs sont des éléments clés dans les réseaux. Les vulnérabilités potentielles des serveurs comprennent les vulnérabilités logicielles, les vulnérabilités de configuration, les faiblesses des protocoles d'authentification, et les vulnérabilités liées à la gestion des correctifs de sécurité.

Introduction

La sécurité des équipements dans les réseaux présente plusieurs enjeux et défis, notamment :

- **Protection des données sensibles :** Les équipements réseau sont souvent responsables de la gestion du trafic et de la transmission des données sensibles, telles que les informations d'identification des utilisateurs, les données de l'entreprise, les données financières, etc. La sécurité des équipements réseau est essentielle pour protéger ces données contre tout accès non autorisé, interception ou altération.

Introduction

- **Continuité de service :** Les équipements réseau sont critiques pour le fonctionnement continu des infrastructures de communication modernes. Les interruptions de service causées par des vulnérabilités ou des attaques peuvent entraîner des perturbations opérationnelles, des pertes financières et une diminution de la confiance des utilisateurs. La sécurité des équipements réseau est nécessaire pour garantir une continuité de service fiable.

Introduction

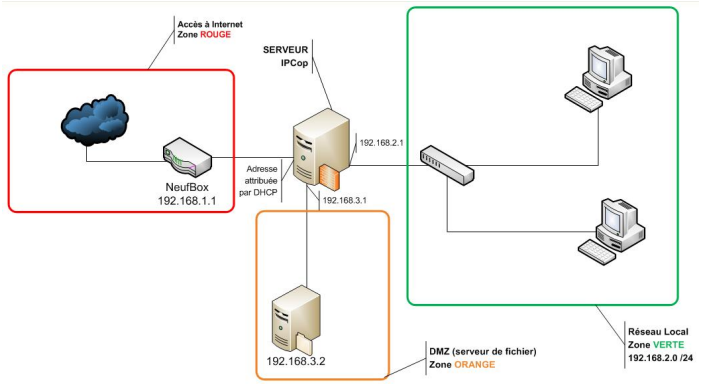
- **Protection contre les attaques malveillantes :** Les équipements réseau sont susceptibles d'être ciblés par des attaques malveillantes, telles que les attaques de déni de service, les attaques de contournement d'authentification, les attaques d'injection de paquets malveillants, etc. La sécurité des équipements réseau doit être renforcée pour détecter, prévenir et contrer ces attaques.
- **Gestion des mises à jour de sécurité :** Les équipements réseau nécessitent des mises à jour régulières pour corriger les vulnérabilités connues et les failles de sécurité. Cependant, la gestion des mises à jour de sécurité peut être complexe, notamment dans les environnements réseau étendus et hétérogènes.

Introduction

- **Complexité des configurations :** Les équipements réseau ont souvent des configurations complexes, comprenant de nombreuses options et paramètres. Une mauvaise configuration peut entraîner des vulnérabilités de sécurité. La gestion des configurations, y compris la mise en œuvre de bonnes pratiques de sécurité, est un défi important pour assurer la sécurité des équipements réseau.
- **Évolution technologique :** Les réseaux évoluent constamment avec de nouvelles technologies, telles que la virtualisation, le cloud computing, l'Internet des objets (IoT), etc. Ces nouvelles technologies peuvent introduire de nouvelles vulnérabilités et défis de sécurité. Il est nécessaire de rester à jour avec les dernières tendances technologiques et de mettre en place des mesures de sécurité appropriées.

Politiques de sécurité

Les politiques de sécurité sont un ensemble de règles, de procédures et de directives qui sont établies pour protéger les systèmes informatiques, les réseaux, les données et les informations sensibles d'une organisation contre les menaces et les risques potentiels. Les règles de filtrage sont un élément clé des politiques de sécurité et définissent les critères selon lesquels le trafic réseau est autorisé ou bloqué en fonction de divers paramètres, tels que l'adresse IP, le port, le protocole, l'application ou d'autres attributs.



Politiques de sécurité

Voici quelques étapes générales pour définir les règles de filtrage dans une politique de sécurité :

- **Utiliser les pare-feu :** Les pare-feu sont des dispositifs de sécurité qui permettent de contrôler le flux du trafic réseau entre différentes zones de sécurité. Dans Packet Tracer, vous pouvez utiliser des pare-feu pour définir des règles de filtrage en autorisant ou en bloquant certains types de trafic en fonction de critères tels que l'adresse IP, le port, le protocole, etc. Vous pouvez configurer les pare-feu en utilisant les dispositifs Cisco ASA (Adaptive Security Appliance) ou les pare-feu intégrés à certains routeurs Cisco.

Politiques de sécurité

- **Utiliser les listes de contrôle d'accès (ACL) :** Les ACL sont des listes de règles qui permettent de filtrer le trafic en fonction de critères spécifiques tels que l'adresse IP, le port, le protocole, etc. Dans Packet Tracer, vous pouvez configurer les ACL sur les interfaces des routeurs ou des commutateurs Cisco pour autoriser ou bloquer le trafic entrant ou sortant. Vous pouvez définir les règles d'ACL en utilisant les numéros de port, les adresses IP source et destination, les protocoles, etc.

Politiques de sécurité

- **Utiliser les objets de sécurité :** Les objets de sécurité sont des éléments configurables dans Packet Tracer qui vous permettent de définir des politiques de sécurité pour les dispositifs du réseau, tels que les hôtes, les routeurs, les commutateurs, etc. Vous pouvez créer des objets de sécurité pour définir des règles de filtrage en fonction de différents critères tels que les adresses IP, les ports, les protocoles, etc. Vous pouvez ensuite appliquer ces objets de sécurité aux interfaces des dispositifs pour contrôler le trafic réseau.

Politiques de sécurité

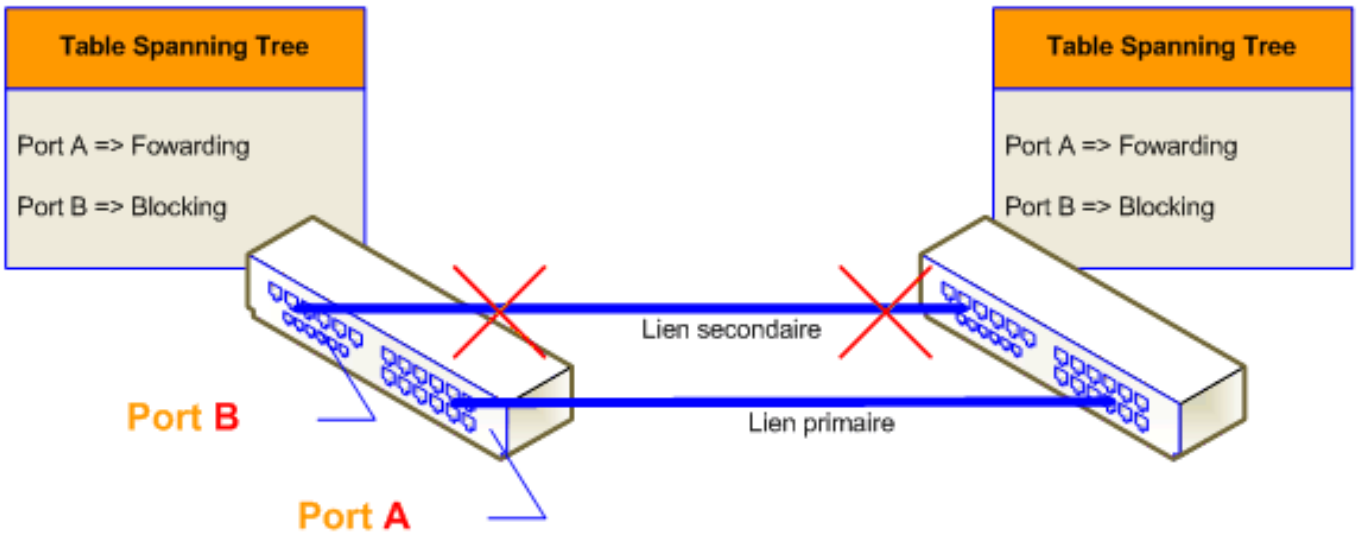
- **Configurer les règles de filtrage :** Selon le dispositif de sécurité que vous utilisez dans Packet Tracer, vous devrez configurer les règles de filtrage en utilisant les commandes appropriées, telles que celles de configuration des pare-feu, des ACL ou des objets de sécurité. Vous pouvez définir les règles en spécifiant les critères de filtrage, tels que les adresses IP source et destination, les ports, les protocoles, etc., ainsi que les actions à prendre sur le trafic, telles que l'autorisation ou le blocage.

Politiques de sécurité

- **Tester et vérifier les règles de filtrage :** Après avoir configuré les règles de filtrage, il est important de les tester et de les vérifier pour vous assurer qu'elles fonctionnent comme prévu. Vous pouvez envoyer du trafic de test à travers le réseau simulé dans Packet Tracer et vérifier si le trafic est autorisé ou bloqué en fonction des règles de filtrage que vous avez définies.

Types de filtrage

Le filtrage est un processus de contrôle qui permet de gérer ou de bloquer le trafic réseau en fonction de certains critères, tels que l'adresse IP, le port, le protocole, etc. Il existe plusieurs types de filtrage utilisés dans les réseaux informatiques pour renforcer la sécurité et garantir le bon fonctionnement du réseau.



Types de filtrage

Voici quelques-uns des types de filtrage les plus couramment utilisés :

- **Filtrage par adresse IP :** Cela implique de bloquer ou de permettre le trafic en fonction des adresses IP source ou destination. Par exemple, on peut configurer un pare-feu pour bloquer les adresses IP provenant de pays spécifiques ou pour permettre uniquement l'accès à certaines adresses IP autorisées.
- **Filtrage par port :** Cela consiste à bloquer ou à autoriser le trafic en fonction des numéros de port source ou destination. Les ports sont des numéros attribués aux différentes applications et services réseau. Par exemple, on peut configurer un pare-feu pour bloquer les ports utilisés par les protocoles de partage de fichiers peer-to-peer.

Types de filtrage

- **Filtrage par protocole :** Cela implique de bloquer ou de permettre le trafic en fonction des protocoles réseau utilisés, tels que TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), etc. Par exemple, on peut configurer un pare-feu pour bloquer les protocoles considérés comme moins sécurisés.
- **Filtrage par contenu :** Cela consiste à bloquer ou à permettre le trafic en fonction du contenu des données échangées. Par exemple, on peut configurer un filtre de contenu pour bloquer les sites web ou les fichiers contenant des virus ou du contenu inapproprié.

Types de filtrage

- **Filtrage par application :** Cela implique de bloquer ou de permettre le trafic en fonction des applications spécifiques utilisées. Par exemple, on peut configurer un pare-feu pour bloquer certaines applications de messagerie instantanée ou de réseaux sociaux.
- **Filtrage par temps :** Cela consiste à bloquer ou à permettre le trafic en fonction du moment de la journée ou du jour de la semaine. Par exemple, on peut configurer un pare-feu pour bloquer l'accès à certaines ressources pendant les heures de bureau ou les jours fériés.

Règles de filtrage IP avec Iptables

Les règles de filtrage IP avec iptables, un outil de gestion de pare-feu sous Linux, sont basées sur un ensemble de principes clés pour garantir un filtrage efficace et sécurisé du trafic réseau. Voici quelques principes de configuration des règles de filtrage iptables :

- **Principe du *Default Deny* :** Par défaut, toutes les connexions entrantes doivent être interdites, sauf celles qui sont expressément autorisées. Cela signifie que si une connexion ne correspond à aucune règle autorisée, elle sera automatiquement rejetée.
- **Principe du *Least Privilege* :** Les règles doivent être configurées pour permettre uniquement le trafic réseau nécessaire. Il est important de limiter l'accès aux ports et aux services réseau uniquement aux utilisateurs ou aux applications qui en ont besoin, et de bloquer tout le reste.

Règles de filtrage IP avec Iptables

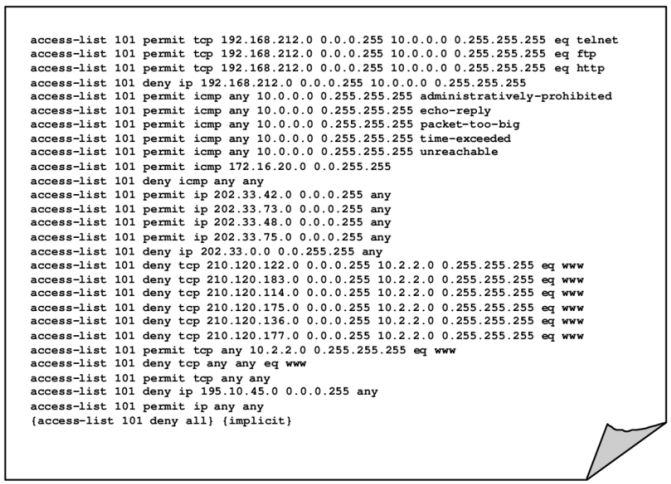
- **Principe de l'ordre des règles :** Les règles sont évaluées dans l'ordre dans lequel elles sont définies dans la chaîne de règles iptables. Il est donc important de configurer les règles dans l'ordre approprié, en commençant par les règles les plus restrictives et en finissant par les règles les plus permissives.
- **Principe de la spécificité des règles :** Les règles iptables sont évaluées de manière séquentielle, et la première règle correspondante est appliquée. Par conséquent, il est important de créer des règles spécifiques pour traiter les cas particuliers avant les règles plus générales.

Règles de filtrage IP avec Iptables

- **Principe de la gestion des connexions établies :** Il est important de permettre le trafic de retour pour les connexions établies, afin de garantir le bon fonctionnement des connexions réseau déjà établies. Cela peut être réalisé en utilisant l'état de connexion d'iptables pour suivre les connexions établies et les autoriser implicitement.
- **Principe de la surveillance et de la journalisation :** La surveillance et la journalisation des règles iptables sont importantes pour diagnostiquer les problèmes de sécurité et de réseau, ainsi que pour auditer l'activité du pare-feu. Il est donc recommandé de configurer la journalisation des règles pour un suivi ultérieur.

Gestion des listes de contrôle d'accès

La gestion des listes de contrôle d'accès (ACL) est un aspect crucial de la sécurité des équipements, tels que les routeurs, les commutateurs, les pare-feu et les serveurs. Les ACL sont utilisées pour définir les règles de filtrage qui autorisent ou refusent le trafic réseau en fonction de critères tels que les adresses IP source et destination, les ports, les protocoles et d'autres paramètres.



```
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq telnet
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq ftp
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq http
access-list 101 deny ip 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 administratively-prohibited
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 echo-reply
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 packet-too-big
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 time-exceeded
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 unreachable
access-list 101 permit icmp 172.16.20.0 0.0.255.255
access-list 101 deny icmp any any
access-list 101 permit ip 202.33.42.0 0.0.0.255 any
access-list 101 permit ip 202.33.73.0 0.0.0.255 any
access-list 101 permit ip 202.33.48.0 0.0.0.255 any
access-list 101 permit ip 202.33.75.0 0.0.0.255 any
access-list 101 deny ip 202.33.0.0 0.0.255.255 any
access-list 101 deny tcp 210.120.122.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.183.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.114.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.175.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.136.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.177.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 permit tcp any 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp any any eq www
access-list 101 permit tcp any any
access-list 101 deny ip 195.10.45.0 0.0.0.255 any
access-list 101 permit ip any any
{access-list 101 deny all} {implicit}
```

Gestion des listes de contrôle d'accès

Voici quelques exemples de règles d'ACL pour renforcer la sécurité des équipements réseau:

- **Autoriser uniquement les protocoles et les ports nécessaires :** Définir des règles d'ACL qui autorisent uniquement les protocoles et les ports nécessaires pour le fonctionnement normal des équipements réseau, et bloquer tout le reste. Par exemple, autoriser uniquement les protocoles spécifiques tels que SSH (22), HTTP (80), HTTPS (443), etc., et bloquer tous les autres protocoles non nécessaires.

Gestion des listes de contrôle d'accès

- **Limiter les adresses IP sources et destinations:** Définir des règles d'ACL qui autorisent uniquement les adresses IP sources et destinations nécessaires pour les communications autorisées. Par exemple, autoriser uniquement les adresses IP des sous-réseaux ou des réseaux de confiance, et bloquer les adresses IP inconnues ou suspectes.
- **Définir des règles de liste blanche plutôt que de liste noire:** Plutôt que de bloquer spécifiquement les adresses IP ou les protocoles indésirables, il est souvent plus sécurisé de définir des règles de liste blanche qui autorisent uniquement les adresses IP, les protocoles et les ports spécifiques autorisés, et de bloquer tout le reste.

Gestion des listes de contrôle d'accès

- **Définir des règles basées sur le rôle ou le niveau d'autorisation de l'utilisateur :** Utiliser des ACL pour définir des règles basées sur le rôle ou le niveau d'autorisation de l'utilisateur, afin de restreindre l'accès aux équipements réseau en fonction des besoins et des droits d'accès de chaque utilisateur.

(Voir l'Annexe C)

Outils de diagnostic

Il existe plusieurs outils de diagnostic de sécurité réseau qui peuvent être utilisés pour évaluer la sécurité d'un réseau informatique. Voici quelques exemples d'outils populaires:

- **Nmap :** Nmap (Network Mapper) est un outil de scanning de réseau qui permet de découvrir les hôtes actifs sur un réseau, de scanner les ports ouverts, d'identifier les services en cours d'exécution sur ces ports, et d'autres informations relatives à la sécurité du réseau.
- **Wireshark :** Wireshark est un outil d'analyse de paquets réseau qui permet de capturer, analyser et inspecter le trafic réseau en temps réel. Il peut être utilisé pour examiner les paquets de données qui circulent sur un réseau afin de détecter d'éventuelles vulnérabilités de sécurité.

Outils de diagnostic

- **Nessus :** Nessus est un outil d'analyse de vulnérabilités qui permet de scanner un réseau pour détecter les vulnérabilités connues dans les systèmes d'exploitation, les applications et les services. Il peut aider à identifier les failles de sécurité qui pourraient être exploitées par des attaquants.
- **OpenVAS :** OpenVAS (Open Vulnerability Assessment System) est une suite d'outils d'évaluation de la sécurité qui permet de scanner les réseaux pour détecter les vulnérabilités et les faiblesses de sécurité dans les systèmes d'exploitation, les applications et les services.

Outils de diagnostic

- **Snort :** Snort est un système de détection d'intrusion (IDS) basé sur les règles qui peut être utilisé pour surveiller le trafic réseau et détecter les activités suspectes ou malveillantes. Il peut être configuré pour alerter les administrateurs en cas de comportement anormal ou de tentatives d'attaques.
- **Firewall :** Un pare-feu est un dispositif de sécurité réseau qui peut être configuré pour filtrer le trafic réseau entrant et sortant, en fonction de règles de sécurité définies. Les pare-feu peuvent aider à bloquer le trafic non autorisé et à protéger le réseau contre les attaques.