Projet Réseau (Sinkhole IP)

- **Binôme:**
  - **Valentin LOBSTEIN**
  - **Lubin MARTIN HOURIEZ**

- Projet Réseau (Sinkhole IP)
- Introduction
- Compréhension des Concepts de Base
- Mise en Place du Sinkhole
  - Schéma du scénario
  - Préparation du Système
  - Configuration du Sinkhole (Machine Debian #2)
  - Configuration du Routage (Machine Debian #1)
  - Capture du Trafic avec Tcpdump (Machine Debian #2)
  - Création d'un Sinkhole Personnalisé
    - Utilisation du Sinkhole Personnalisé
    - Features du Sinkhole Personnalisé
- Surveillance et Analyse du Trafic
  - Surveillance en temps réel
  - Analyse du trafic
  - Réaction aux attaques
- Conclusion
- Annexe
  - Annexe A : Code du Sinkhole Personnalisé

Introduction

Dans un monde où la connectivité numérique s'est imposée comme une norme plutôt que comme une exception, la sécurité des réseaux est devenue un enjeu majeur pour les organisations de toutes tailles. Face à la sophistication croissante des cyber-menaces, les professionnels de la sécurité ont recours à une gamme de plus en plus diversifiée de stratégies et d'outils pour protéger les infrastructures réseau. L'une de ces stratégies consiste à utiliser un dispositif appelé "Sinkhole" dans le contexte de la gestion du trafic réseau.

Ce rapport a pour objectif de décrire en détail le processus de mise en place et d'utilisation d'un sinkhole sur un réseau basé sur le système d'exploitation Debian. Il a pour but de fournir une compréhension claire des concepts, des techniques et des outils utilisés, tels que le routage IP, le firewall iptables et le sniffer de paquets tcpdump. En particulier, nous expliquerons comment ces éléments peuvent être configurés et utilisés pour capter, rediriger et analyser le trafic réseau dans un contexte de sécurité.

Le rapport débute par une explication détaillée des concepts de base, suivi d'un guide étape par étape sur la configuration d'un sinkhole et du routage approprié sur une machine Debian. Enfin, nous démontrerons comment capturer et analyser le trafic réseau à l'aide de tcpdump, pour ainsi pouvoir identifier les éventuelles tentatives d'intrusion ou d'exploration non autorisées du réseau.

Compréhension des Concepts de Base

Avant de se lancer dans la mise en place du sinkhole, il est essentiel de comprendre certains concepts de base.

- **Sinkhole**
    - Un sinkhole, ou trou noir, dans le domaine de la sécurité réseau, est une mesure proactive pour rediriger le trafic réseau suspect ou malveillant vers une adresse ou un serveur spécifique (la machine "sinkhole") plutôt que vers sa destination initiale. Cette technique est généralement utilisée pour isoler les comportements suspects ou malveillants et prévenir la propagation des logiciels malveillants sur le réseau.
- **Tcpdump**
    - Tcpdump est un outil de capture de paquets qui fonctionne en mode promiscuité. Il capture tout le trafic passant par une interface réseau particulière et peut enregistrer ces données pour une analyse ultérieure. C'est un outil précieux pour surveiller le trafic réseau en temps réel ou pour étudier les comportements réseau passés.
- **Iptables**
    - Iptables est un outil de configuration de pare-feu pour les systèmes basés sur Linux. Il permet aux administrateurs de définir des règles pour le trafic entrant, sortant et de transit. Ces règles peuvent être utilisées pour rediriger, autoriser ou bloquer le trafic réseau en fonction de divers critères, tels que l'adresse IP source, l'adresse IP de destination, le port, le protocole, etc.
- **Routage IP**
    - Le routage IP est le processus par lequel un réseau détermine le chemin que les paquets doivent emprunter pour atteindre leur destination. L'activation du routage IP sur une machine lui permet de transmettre des paquets entre les différentes interfaces réseau qu'elle possède. Cela peut être utilisé pour rediriger le trafic réseau à travers la machine, comme c'est le cas avec un sinkhole.

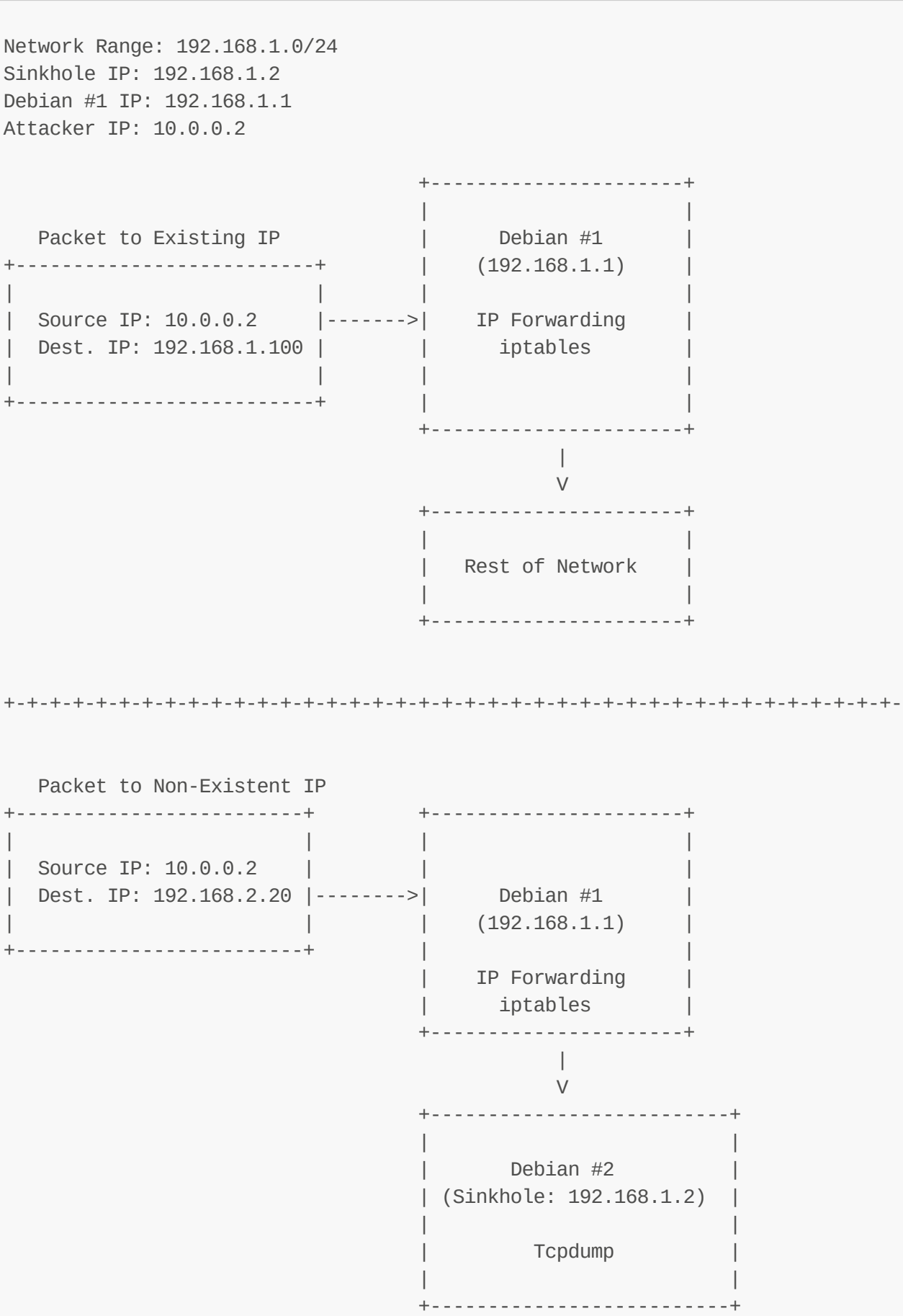
Chacun de ces concepts joue un rôle clé dans la mise en place et le fonctionnement d'un sinkhole. Dans les sections suivantes, nous examinerons comment ces outils peuvent être configurés et utilisés pour capturer et rediriger le trafic réseau dans le cadre d'une stratégie de sécurité réseau.

Mise en Place du Sinkhole

La configuration d'un sinkhole implique plusieurs étapes clés, allant de la préparation du système à la configuration de la redirection du trafic. Le but est d'intercepter tout le trafic vers des adresses IP non

locales à notre réseau. Voici comment :

Schéma du scénario



Dans ce schéma, la plage d'adresse du réseau est `192.168.1.0/24`. L'adresse IP de l'attaquant (la source du paquet) est `10.0.0.2`. Le paquet destiné à l'adresse IP existante (`192.168.1.100`) est transmis normalement à travers **Debian #1** (`192.168.1.1`) au reste du réseau. Le paquet destiné à une adresse IP non-existante dans la plage du réseau (`192.168.2.20`) est redirigé vers le sinkhole sur **Debian #2** (`192.168.1.2`).

Préparation du Système

Sur les deux machines Debian, vous devrez installer certains logiciels.

1. Sur la machine **Debian #2** (le sinkhole), installez `tcpdump` :
    - `apt update` : Cette commande met à jour l'index des paquets disponibles à partir des dépôts logiciels configurés sur votre système.
    - `apt install tcpdump` : Cette commande installe tcpdump, un outil de capture de paquets réseau, sur votre système.
2. Sur la machine **Debian #1** (le routeur), activez le routage IP et installez `iptables` :
    - Editez le fichier `/etc/sysctl.conf` et ajoutez ou décommentez la ligne suivante : `net.ipv4.ip_forward=1`. Cette ligne active le routage IP, ce qui permet à votre machine de transmettre des paquets entre ses différentes interfaces réseau.
    - Enregistrez et fermez le fichier, puis appliquez les modifications avec la commande `sysctl -p`.
    - Pour installer `iptables`, commencez par mettre à jour l'index des paquets avec `apt update`, puis utilisez la commande `apt install iptables` pour installer le logiciel.

Configuration du Sinkhole (Machine Debian #2)

Sur la machine Debian #2, vous aurez besoin de connaître l'adresse IP de la machine. Pour cela, utilisez la commande `ip addr`, qui affiche les adresses IP de toutes les interfaces réseau de votre machine.

Configuration du Routage (Machine Debian #1)

Sur la machine Debian #1, vous allez configurer `iptables` pour rediriger tout le trafic non local vers le sinkhole. Pour ce faire, utilisez la commande suivante, en remplaçant `<IP_SINKHOLE>` par l'adresse IP de la machine Debian #2 :

```
iptables -t nat -A PREROUTING -m addrtype ! --src-type LOCAL -j DNAT --to-
destination <IP_SINKHOLE>
```

Voici ce que fait cette commande :

- `iptables -t nat` : Ceci indique à iptables que nous voulons ajouter une règle à la table de Network Address Translation (NAT).
- `-A PREROUTING` : Ceci ajoute notre règle à la chaîne PREROUTING, qui traite les paquets dès qu'ils arrivent.

- `-m addrtype ! --src-type LOCAL` : Ceci spécifie que la règle doit s'appliquer à tout paquet dont l'adresse source n'est pas une adresse locale.
- `-j DNAT --to-destination <IP_SINKHOLE>` : Ceci indique que les paquets correspondants doivent être redirigés (Destination NAT) vers l'adresse IP du sinkhole.

Ensuite, pour que ces règles persistent après un redémarrage, enregistrez-les avec les commandes suivantes :

```
mkdir -p /etc/iptables
sh -c 'iptables-save > /etc/iptables/rules.v4'
```

Capture du Trafic avec Tcpdump (Machine Debian #2)

Enfin, sur la machine **Debian #2**, vous pouvez commencer à capturer le trafic avec `tcpdump`. Utilisez la commande suivante, en remplaçant `<INTERFACE>` par le nom de votre interface réseau :

```
tcpdump -i <INTERFACE> -w sinkhole_traffic.pcap
```

Cela démarrera une capture de tous les paquets arrivant sur cette interface, qui seront enregistrés dans le fichier `sinkhole_traffic.pcap`. Vous pouvez analyser ce fichier plus tard pour examiner le trafic intercepté.

Création d'un Sinkhole Personnalisé

Dans le cadre de cette mise en place, une solution personnalisée a été développée pour fournir un sinkhole plus robuste et personnalisable. Ce sinkhole a été développé en Python en utilisant la bibliothèque Scapy, qui offre une grande flexibilité pour analyser, manipuler et générer du trafic réseau.

Utilisation du Sinkhole Personnalisé

Pour utiliser le sinkhole personnalisé, vous devez d'abord exécuter le script Python qui a été développé. Ce script accepte deux arguments :

1. `-i` ou `--interface` : L'interface réseau que le sinkhole doit surveiller. Cet argument est obligatoire.
2. `-l` ou `--log` : Le chemin du fichier où les logs du sinkhole doivent être enregistrés. C'est un argument facultatif, par défaut, les logs sont enregistrés dans le fichier `sinkhole.log` à la racine du répertoire où le script est exécuté.

Voici un exemple d'exécution du script :

```
python3 sinkhole.py -i eth0 -l /path/to/logfile.log
```

Features du Sinkhole Personnalisé

Le sinkhole personnalisé a plusieurs caractéristiques notables :

1. **Capture de tout le trafic IP** : Le sinkhole capture tout le trafic IP redirigé vers lui, y compris les paquets ICMP, TCP et UDP.
2. **Enregistrement des attaques** : Le sinkhole enregistre les détails de chaque paquet qu'il capture, y compris l'adresse IP source, l'adresse IP de destination, le port de destination (si applicable) et le protocole.
3. **Affichage des résultats en temps réel** : Le sinkhole affiche en temps réel une table des attaques détectées, incluant les adresses IP source et de destination, les ports et le type de paquets. Il agrège les données pour une paire d'adresses IP source et de destination et affiche les trois derniers ports utilisés ainsi que le nombre total d'attaques.
4. **Enregistrement des logs** : Le sinkhole enregistre les détails de chaque attaque dans un fichier log pour une analyse ultérieure.

Pour un aperçu du code du sinkhole personnalisé, consultez **l'annexe A** de ce rapport.

Surveillance et Analyse du Trafic

La surveillance et l'analyse du trafic sont deux activités cruciales dans la gestion d'un réseau, et elles sont particulièrement importantes lors de l'utilisation d'un sinkhole. Elles permettent d'identifier les activités suspectes, de détecter les attaques et de comprendre le comportement du réseau. Voici quelques éléments à prendre en compte lors de la surveillance et de l'analyse du trafic capturé par votre sinkhole.

Surveillance en temps réel

Le sinkhole personnalisé développé affiche en temps réel une table des attaques détectées. Cette fonctionnalité permet aux administrateurs réseau de surveiller le trafic entrant dans le sinkhole et de réagir rapidement en cas d'activité suspecte.

Il est également possible de surveiller le fichier de logs créé par le sinkhole en utilisant une commande comme `tail -f /path/to/logfile.log`. Cela permet d'afficher les nouvelles entrées du fichier de logs au fur et à mesure qu'elles sont ajoutées.

Analyse du trafic

Le fichier de logs généré par le sinkhole peut être utilisé pour analyser le trafic après coup. Vous pouvez par exemple chercher les adresses IP les plus communes, les ports les plus utilisés, ou les périodes de temps avec le plus d'activité. Cette analyse peut aider à identifier les modèles d'attaque et à améliorer la sécurité du réseau.

Pour une analyse plus approfondie, le fichier pcap généré par tcpdump peut être ouvert avec un outil comme Wireshark. Wireshark fournit une interface graphique qui permet de filtrer et de visualiser le trafic de manière détaillée.

Réaction aux attaques

Lorsqu'une activité suspecte est détectée, il est important de réagir rapidement. La nature exacte de la réaction dépendra de la politique de sécurité du réseau et de la nature de l'activité suspecte, mais elle peut inclure des actions comme bloquer l'adresse IP source, alerter l'administrateur réseau, ou même déconnecter temporairement le réseau.

En conclusion, la surveillance et l'analyse du trafic sont des activités essentielles lors de l'utilisation d'un sinkhole. Elles permettent d'identifier et de réagir aux attaques, d'améliorer la sécurité du réseau, et de mieux comprendre le comportement du réseau.

Conclusion

L'utilisation d'un sinkhole IP dans un réseau est une stratégie de sécurité efficace pour détecter et contrer les menaces potentielles. Par l'interception du trafic à destination d'adresses IP inconnues ou suspectes, le sinkhole permet d'isoler et d'analyser les activités malveillantes.

Dans ce rapport, nous avons exploré la mise en place d'un sinkhole IP dans un réseau Debian. Nous avons également présenté une solution personnalisée développée pour améliorer la robustesse et la flexibilité de la détection des menaces. Avec sa capacité à capturer le trafic IP, à enregistrer les détails des attaques et à afficher les résultats en temps réel, cette solution personnalisée offre une surveillance et une analyse du trafic approfondies.

Cependant, comme pour toute stratégie de sécurité, l'utilisation d'un sinkhole IP doit s'inscrire dans le cadre d'une approche de sécurité en profondeur. D'autres mesures, comme l'utilisation d'un système de détection d'intrusion (IDS), la mise en œuvre de politiques de sécurité solides et la formation continue des utilisateurs à la sécurité, sont également cruciales pour garantir la sécurité d'un réseau.

Annexe

Annexe A : Code du Sinkhole Personnalisé