**1. Problématiques et Solutions de Sécurisation**

**Problématiques :**

* Les services réseau exposés à des flux non maîtrisés (comme Internet ou les réseaux Wi-Fi publics) sont particulièrement vulnérables aux attaques.
* Une mauvaise configuration ou des vulnérabilités non corrigées peuvent être exploitées pour accéder illégitimement au système.

**Solutions Proposées :**

1. **Cloisonnement des Services Réseau**
   * **Conteneurs :** Utiliser Docker ou Kubernetes pour isoler les services.
   * **Machines Virtuelles :** Héberger les services sur des VMs distinctes.
   * **Comptes Utilisateurs Dédiés :** Attribuer des comptes spécifiques pour chaque service.
2. **Durcissement des Services Exposés**
   * **Configuration Sécurisée :** Remplacer les configurations par défaut par des configurations sécurisées.
   * **Mises à Jour Régulières :** Appliquer les patchs de sécurité et mises à jour des logiciels.
   * **Authentification Renforcée :** Utiliser des méthodes fortes comme l'authentification multi-facteurs.
   * **Validation des Entrées/Sorties :** Mettre en place des mécanismes pour valider les données.
3. **Surveillance Active des Services**
   * **Monitoring :** Utiliser des outils comme Prometheus ou Nagios pour surveiller les performances et comportements.
   * **Journalisation :** Activer la journalisation pour suivre les activités.
   * **Analyse des Logs :** Centraliser et analyser les journaux avec des outils comme ELK Stack ou Splunk.
4. **Réduction de la Surface d'Attaque**
   * **Limiter les Interfaces Réseau :** Configurer les services pour écouter uniquement sur les interfaces nécessaires.
   * **Filtrage des Ports :** Utiliser des pare-feu pour restreindre l'accès aux services nécessaires.
5. **Tests de Pénétration et Autres Mesures**
   * **Tests de Pénétration :** Réaliser des tests réguliers pour identifier les vulnérabilités.
   * **Segmentation Réseau :** Séparer les différents types de services pour réduire les impacts.
   * **Gestion des Droits d'Accès :** Auditer et gérer les droits d'accès pour minimiser les risques.

**2. Logiciels Recommandés pour la Mise en Place des Solutions**

**Cloisonnement :**

* **Conteneurs :** [Docker](https://www.docker.com/), [Kubernetes](https://kubernetes.io/)
* **Machines Virtuelles :** VMware vSphere, Proxmox VE

**Durcissement :**

* **Configuration Sécurisée :** [Chef](https://www.chef.io/), [Puppet](https://puppet.com/)
* **Mises à Jour :** [WSUS](https://www.microsoft.com/en-us/windows-server/windows-server-update-services), [Unattended Upgrades](https://help.ubuntu.com/community/AutomaticSecurityUpdates)
* **Authentification :** [OpenSSH](https://www.openssh.com/), [Vault](https://www.vaultproject.io/)
* **Validation des Entrées :** [OWASP ZAP](https://www.zaproxy.org/)

**Surveillance :**

* **Monitoring :** [Prometheus](https://prometheus.io/), [Nagios](https://www.nagios.org/)
* **Journalisation :** [ELK Stack](https://www.elastic.co/what-is/elk-stack), [Splunk](https://www.splunk.com/)

**Réduction de la Surface d'Attaque :**

* **Limiter les Interfaces Réseau :** [UFW](https://wiki.ubuntu.com/UncomplicatedFirewall), iptables
* **Filtrage des Ports :** [pfSense](https://www.pfsense.org/)

**Tests de Pénétration :**

* [**Metasploit**](https://www.metasploit.com/), **Burp Suite**
* [**Nmap**](https://nmap.org/) : Pour scanner les réseaux et tester la sécurité.

**Conclusion**

La sécurisation des services réseau passe par des mesures de cloisonnement, de durcissement, de surveillance, et de réduction de la surface d'attaque. Les logiciels recommandés permettent de mettre en place ces mesures efficacement, en automatisant et en renforçant les configurations de sécurité. La mise en place de ces solutions est essentielle pour protéger les services réseau contre les attaques et garantir l'intégrité du système.

 **Introduction**

* Objectif : Déploiement et sécurisation des services réseau avec Ansible.

 **Préparation de l'Environnement Ansible**

* Installation d'Ansible
* Configuration SSH
* Inventaire Ansible

 **Playbook Ansible pour Sécurisation**

* Mise à jour du système
* Installation des outils de sécurité
* Configuration du pare-feu (UFW)
* Configuration des mises à jour automatiques
* Installation et configuration de Docker
* Installation de Prometheus pour la surveillance
* Configuration de fail2ban
* Installation et configuration d’ELK Stack
* Configuration SSH

 **Commandes pour Déployer le Playbook**

* Commande pour exécuter le playbook

 **Résumé des Étapes et Logiciels Utilisés**

**. Introduction**

**Objectif :** Déploiement et sécurisation des services réseau avec Ansible.

Ce document décrit comment déployer une machine avec Ansible tout en intégrant des éléments de sécurité essentiels tels que le cloisonnement, le durcissement, la surveillance, et la réduction de la surface d'attaque.

**2. Préparation de l'Environnement Ansible**

**Installation d'Ansible :**

**sudo apt update**

**sudo apt install ansible**

**Configuration SSH :**

**# Générer une clé SSH (si vous n'en avez pas déjà)**

**ssh-keygen -t rsa -b 4096 -C "your\_email@example.com"**

**# Copier la clé sur la machine cible**

**ssh-copy-id user@machine\_ip**

**Inventaire Ansible :**

**# Fichier inventory.ini**

**[servers]**

**target ansible\_host=target\_ip ansible\_user=username**

**. Playbook Ansible pour Sécurisation :**

**# Fichier deploy\_security.yml**

**- name: Déploiement et Sécurisation des Services Réseau**

**hosts: servers**

**become: yes**

**tasks:**

**# 1. Mise à jour du Système**

**- name: Mise à jour de tous les paquets**

**apt:**

**update\_cache: yes**

**upgrade: dist**

**# 2. Installation des Outils de Sécurité**

**- name: Installer UFW, Fail2Ban, et autres outils**

**apt:**

**name:**

**- ufw**

**- fail2ban**

**- unattended-upgrades**

**- docker.io**

**- python3-pip**

**state: present**

**# 3. Configuration du Pare-feu (UFW)**

**- name: Configurer le pare-feu UFW**

**ufw:**

**rule: allow**

**port: '22'**

**proto: tcp**

**- name: Activer UFW**

**ufw:**

**state: enabled**

**# 4. Configuration des Mises à Jour Automatiques**

**- name: Configurer les mises à jour automatiques**

**copy:**

**dest: /etc/apt/apt.conf.d/20auto-upgrades**

**content: |**

**APT::Periodic::Update-Package-Lists "1";**

**APT::Periodic::Unattended-Upgrade "1";**

**# 5. Installation de Docker et Configuration Basique**

**- name: Démarrer Docker**

**service:**

**name: docker**

**state: started**

**enabled: yes**

**# 6. Installation et Configuration de Prometheus pour la Surveillance**

**- name: Installer Prometheus**

**shell: >**

**docker run -d --name prometheus**

**-p 9090:9090**

**-v /etc/prometheus/prometheus.yml:/etc/prometheus/prometheus.yml**

**prom/prometheus**

**# 7. Installation de fail2ban pour la Protection contre les Intrusions**

**- name: Configurer fail2ban**

**copy:**

**dest: /etc/fail2ban/jail.local**

**content: |**

**[sshd]**

**enabled = true**

**# 8. Installation et Configuration d’ELK Stack**

**- name: Installer Elasticsearch**

**shell: >**

**docker run -d --name elasticsearch**

**-p 9200:9200**

**-e "discovery.type=single-node"**

**docker.elastic.co/elasticsearch/elasticsearch:8.3.3**

**- name: Installer Kibana**

**shell: >**

**docker run -d --name kibana**

**-p 5601:5601**

**docker.elastic.co/kibana/kibana:8.3.3**

**# 9. Configuration SSH**

**- name: Désactiver SSH root login**

**lineinfile:**

**path: /etc/ssh/sshd\_config**

**regexp: '^PermitRootLogin'**

**line: 'PermitRootLogin no'**

**notify: Restart SSH**

**handlers:**

**- name: Restart SSH**

**service:**

**name: ssh**

**state: restarted**

Commandes pour Déployer le Playbook :

**ansible-playbook -i inventory.ini deploy\_security.yml**

**Résumé des Étapes et Logiciels Utilisés**

1. **Mise à Jour :** Ansible pour automatiser apt update et apt upgrade.
2. **Outils de Sécurité :** Installation d’UFW, Fail2Ban, Docker.
3. **Pare-feu UFW :** UFW configuré via Ansible.
4. **Mises à Jour Automatiques :** Utilisation d’unattended-upgrades.
5. **Docker :** Utilisé pour déployer Prometheus et ELK Stack.
6. **Surveillance :** Prometheus pour la surveillance.
7. **Protection contre les Intrusions :** Fail2Ban pour protéger SSH.
8. **Journalisation :** ELK Stack pour collecter et analyser les journaux.
9. **Sécurisation SSH :** Configuration pour désactiver le login root via SSH.