TP Thème 4 - Apache Logs – Analyse d’erreurs 404

Abilash SELLATHURAI – P37 M2IRS

Une image contenant texte, capture d’écran, Rectangle, nombre

Le contenu généré par l’IA peut être incorrect.

Discussion finale

**Quelles conclusions peut-on tirer ?**

L’analyse des logs Apache a permis d’identifier les adresses IP responsables d’un grand nombre d’erreurs 404. Ces erreurs proviennent en majorité de robots automatisés, souvent reconnaissables à leur user-agent. Cela indique que le site est régulièrement exploré par des bots, certains étant légitimes (comme les moteurs de recherche), d'autres potentiellement malveillants. Les erreurs 404 sont donc un indicateur pertinent pour repérer une activité inhabituelle ou suspecte sur un serveur web.

**Ces IPs doivent-elles être bannies ?**

Toutes les adresses IP identifiées comme fautives ne doivent pas forcément être bannies. Certaines appartiennent à des robots de moteurs de recherche connus, ce qui est un comportement normal. En revanche, les IPs qui génèrent un volume excessif d’erreurs 404, avec un comportement agressif ou répétitif, peuvent être considérées comme suspectes. Il est alors pertinent de les bloquer temporairement ou de les limiter via un pare-feu applicatif ou des outils comme fail2ban. La décision de bannir doit se baser sur des critères clairs, comme la fréquence des erreurs, la nature du user-agent, et le contexte du réseau.

**Peut-on automatiser ce type de détection ?**

Oui, ce type de détection peut être entièrement automatisé. Il est possible de créer un script Python qui analyse régulièrement les fichiers de logs, identifie les adresses IP fautives, et génère des alertes ou des rapports. Des outils comme fail2ban permettent également de bannir automatiquement les IPs générant trop d’erreurs 404 selon des règles définies. Enfin, des solutions plus avancées comme des systèmes de gestion des logs (SIEM) peuvent surveiller en temps réel les activités suspectes sur un réseau et déclencher des actions automatiques. Automatiser ce processus permet de renforcer la sécurité et de réagir plus rapidement face aux tentatives d'intrusion.