Détection des intrusions

Assurer la sécurité d'un système, c'est d'abord mettre en œuvre des outils de protection : confidentialité des échanges par des techniques de chiffrement (SSL, SSH), intégrité des données (CRC, Hachage, salage), authentification (compte, MFA : multiple factor authentication, Radius, OTP : one time password, etc).

Mais une surveillance active des échanges sur le réseau ou vers un service est un complément nécessaire pour détecter des intrusions ou des comportements anormaux qui risquent de permettre des accès indus, des tentatives d'attaque ou de brute force.

Divers outils permettent ces détections : on parle d'IDS ou Intrusion Detection System.

- Fail2ban pour la protection des services
- Snort pour les comportements anormaux sur le réseau