Grille de notation

1- Introduction [/0 pt]

[/0 pt] 1.1 Objectif du projet
[/0 pt] 1.2 Description de l'infrastructure
[/0 pt] 1.3 Etapes préliminaires

2- Mise en place de l'infrastructure [/10 pts]

2.1
[/0.25 pt] Rôle de rsyslog
[/0.25 pt] Fonctionnement de rsyslog
[/0.25 pt] Rôle de fail2ban
[/0.25 pt] Fonctionnement de fail2ban

2.2
[/0.5 pt] Principe de l'IaaC

2.3
[/0.25 pt] Raisons d'être de Docker
[/0.25 pt] Raisons d'être de Docker-compose

2.4
[/1 pt] Installation + Configuration de OpenSSH
[/1 pt] Installation + Configgguration de Fail2Ban
[/2 pts] Installation + Configgguration de Apache2
[/4 pts] Installation + Configgguration de Rsyslog

3- Tests de journalisation et IDS/IPS [/6 pts]

3.1
[/1 pt] 2 tentatives succès + 2 tentatives échecs. [/0.25 pt] / tentative

3.2
[/1 pt] Récuperer les pages /Oracle.html et /Trinity.html
[/1 pt] Constats dans les logs sur le serveur Neo
[/0.5 pt] Récuperation des fichiers + Lecture du contenu de la page /Oracle.html

3.3

[/0.5 pt] Capture réseau + Récuperation de la capture réseau

[/1 pt] Identifier le port et le protocole de la couche de transport rsyslog

3.4

[/1 pt] Constats des règles de firewall

4- Sécurité des journaux d'activités (logs) [/2 pts]

4.1

[/0.5 pt] Prise en charge de IPv6 sur rsyslog

4.2

[/0.5 pt] Avantages de la centralisation de logs

[/0.5 pt] Explications du type de centralisation privilégié (local vs distant)

4.3

4.3.a [/0.25 pt] Explication du principe de log injection

4.3.b [/0.25 pt] Justification de la conséquence de la suppression de fichiers log

4.3.c [/0.25 pt] Commentaire sur la politique de rotation des logs

5- Consignes et livrables [/2 pts]

[/1 pt] Travail remis en équipe

[/1 pt] Respect des noms de machine, réseaux et IPs