FICHE DE COMPÉTITION : CONFRONTATION BLUE TEAM VS RED TEAM

---

1. Description des Services et Vulnérabilités

1.1. Service Samba

- **Vulnérabilité** : Version vulnérable de Samba permettant une intrusion.
- **Objectif Red Team** : Exploiter la faille pour obtenir un accès à la machine cible.
- **Objectif Blue Team** :
    - Corriger la configuration vulnérable.
    - Si la correction est impossible, détecter l'intrusion avec Wazuh et stopper l'attaque avant 5 alertes.

1.2. Service Tomcat

- **Vulnérabilité** : Mauvaise configuration de Tomcat permettant une intrusion.
- **Objectif Red Team** : Exploiter la vulnérabilité pour compromettre le service.
- **Objectif Blue Team** :
    - Corriger la configuration vulnérable.
    - Détecter l'attaque avec Wazuh et spécifier à Wazuh agent le fichier de log concerné.

1.3. Service Apache

- **Vulnérabilités** :
    - Une vulnérabilité permettant une intrusion.
    - Une mauvaise configuration permettant l'élévation de privilèges à root.
- **Objectif Red Team** :
    - Exploiter la faille pour accéder au serveur.
    - Devenir root en exploitant la mauvaise configuration.
- **Objectif Blue Team** :
    - Corriger la configuration vulnérable avant l'attaque.
    - Détecter l'attaque avec Wazuh et stopper l'attaquant avant qu'il ne devienne root.

1.4. Service SSH

- **Vulnérabilités** :
    - Une faille permettant de déterminer les utilisateurs valides.
    - Un utilisateur avec un mot de passe faible.
    - Une vulnérabilité permettant d'obtenir root.

- **Objectif Red Team** :
    - Découvrir les utilisateurs valides.
    - Accéder à la machine avec l'utilisateur faible.
    - Devenir root via l'exploit.
- **Objectif Blue Team** :
    - Détecter l'attaque avec Wazuh.
    - Stopper l'attaquant avant qu'il ne devienne root.
    - Identifier la faille, expliquer le problème lié à la version de SSH et proposer une solution.

1.5. Service Jenkins

- **Vulnérabilités** :
    - Un mot de passe administrateur faible.
    - Un fichier contenant des credentials laissé dans /home/vulnerable_user/password.txt.
- **Objectif Red Team** :
    - Exploiter ces failles pour obtenir un accès administrateur.
- **Objectif Blue Team** :
    - Empêcher l'attaque en renforçant la sécurité de Jenkins.

---

2. Système de Notation

Service	Action Red Team	Points Red Team	Action Blue Team	Points Blue Team
Samba	Accès à la machine	+1	Correction de la configuration avec explication	+1
			Détection de l'attaque et suppression du processus avant 5 alertes	+0.5
Tomcat	Accès à la machine	+1	Correction de la configuration	+0.5
			Détection de l'attaque et déclaration du fichier de log dans Wazuh	+0.5
Apache	Accès à la machine	+1	Correction de la configuration avant l'attaque	+1

	Exploitation de la faille pour devenir root	+0.5	Détection et éjection de l'attaquant avant qu'il ne devienne root	+0.5
SSH	Accès à la machine	+1	Détection de l'attaque	+1
	Exploitation pour devenir root	+0.5	Éjection de l'attaquant et analyse complète avec explication sur SSH	+0.5
Jenkins	Accès administrateur	+1.5	Empêcher l'attaque	+1

Total maximum par équipe :

- **Red Team :** 6 .5 points
- **Blue Team :** 6.5 points

Outils utiles : metasploit, nmap, hydra, python2