# PROJET CR350

Date limite de remise : 31 mars 2025 à 20h55

# Objectif du projet

L’objectif du projet est de mettre en place une infrastructure de journalisation sous un hyperviseur de type 2 tels qu’Oracle VirtualBox, VMware Workstation, etc.

Cette infrastructure comprendra trois ou quatre machines virtuelles interconnectées pour centraliser les journaux et tester différentes configurations de sécurité.

# Machines virtuelles :

* + Serversyslog : machine virtuelle sous un système d'exploitation Linux de votre choix, chargée de centraliser tous les logs générés dans l'infrastructure.
  + Clientsyslog : machine virtuelle sous une distribution Ubuntu 22 ou supérieur, configurée pour envoyer ses logs à Serversyslog.
  + Testeursyslog (ou Testeusesyslog) : machine virtuelle sous un système d'exploitation de votre choix, utilisée pour réaliser des tests de connexion et des balayages réseaux.

# Partie 1 : Mise en place de l’infrastructure [ /5pts ]

Chaque membre de l'équipe doit configurer une des machines virtuelles (Serversyslog, Clientsyslog, Testeursyslog ou Testeusesyslog).

Dans le cas d'une équipe de quatre personnes, la machine Testeursyslog sera divisée en Testeursyslog1 et Testeursyslog2.

1. Construisez un schéma réseau d’une telle infrastructure
2. Réalisez ce schéma réseau avec les contraintes décrites ci-dessus. Justifiez vos choix.
3. Vérifiez la connectivité entre toutes les machines à l’aide de la commande ping.
4. Sur la machine Clientsyslog, installez et démarrez un serveur SSH (openssh-server) ainsi qu’un serveur web (apache2).

# Partie 2 : Test de la journalisation [ /8pts ]

1. Supprimez toutes les règles de firewall existantes sur Serversyslog et Clientsyslog.
2. Interceptez uniquement les communications syslog entre Clientsyslog et Serversyslog durant les tentatives de connexion SSH de Testeursyslog (ou Testeusesyslog) à Clientsyslog, en incluant deux tentatives réussies et deux tentatives échouées. Quel port et quel protocole sont utilisés pour le service syslog?
3. Quelles configurations doivent être mises en place sur Serversyslog pour autoriser uniquement le flux syslog en provenance de Clientsyslog ?
4. Redirigez tous les logs du serveur web vers Serversyslog. Interceptez le trafic réseau de deux tentatives d’accès web depuis Clientsyslog vers le serveur web. L’adresse IP de la machine Clientsyslog est-elle présente dans les logs sur le serveur Serversyslog ?

# Partie 3 : Installation d’outils IDS/IPS [ /5pts ]

1. Quelle machine configurer pour respecter la politique suivante : « Toute adresse IP qui échoue à établir une connexion SSH à Clientsyslog plus de deux fois en l’espace de 5min est automatiquement bloquée pour une durée de 1h » ?
2. Expliquez brièvement le fonctionnement de Fail2ban.
3. Implémentez la politique de blocage mentionnée à l’aide de Fail2ban.
4. Effectuez trois tentatives de connexion infructueuses depuis Testeursyslog (ou Testeusesyslog) vers la machine Clientsyslog. Que se passe-t-il?
5. Affichez les règles actives du firewall sur Clientsyslog, puis désactivez-les et réitérez la tentative de connexion. Comparez et expliquez les résultats obtenus.

# Consignes

Veuillez respecter les consignes ci-après :

* + Les noms attribués aux machines doivent être conformes aux directives fournies.
  + Le travail doit être réalisé en équipe de trois ou quatre personnes.
  + Un rapport au format PDF de 12 pages maximum est attendu avec des captures d’écran pertinentes.

# Grille de notations

* Partie 1 (5 points), Partie 2 (8 points), Partie 3 (5 points)
  + Clarté et précision des réponses
  + Exactitude des configurations
  + Pertinence des preuves (commandes, captures d’écran, etc.)
* Respect des consignes : 2 points
  + Respect du nombre maximal de pages
  + Respect du format du livrable
  + Respect du nom des machines
  + Respect du nombre de membres par équipe
* Des malus sont comptés pour les remises en retard et des travaux remis seul(e)

# Ressources

* + [VirtualBox](https://www.virtualbox.org/wiki/Downloads)
  + [VMware](−%09https:/www.vmware.com/)
  + [Rsyslog](−%09https:/www.geeksforgeeks.org/getting-started-with-rsyslog-in-linux/)
  + [OpenSSH](https://www.it-connect.fr/chapitres/installation-dun-serveur-ssh-et-premiere-connexion/)
  + [Apache2](https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-fr)
  + [Fail2Ban](https://forum-debian.fr/wiki/Fail2ban)