Cyber Security Awareness : Démo à l'attention de futurs bacheliers en informatique de gestion.

But :

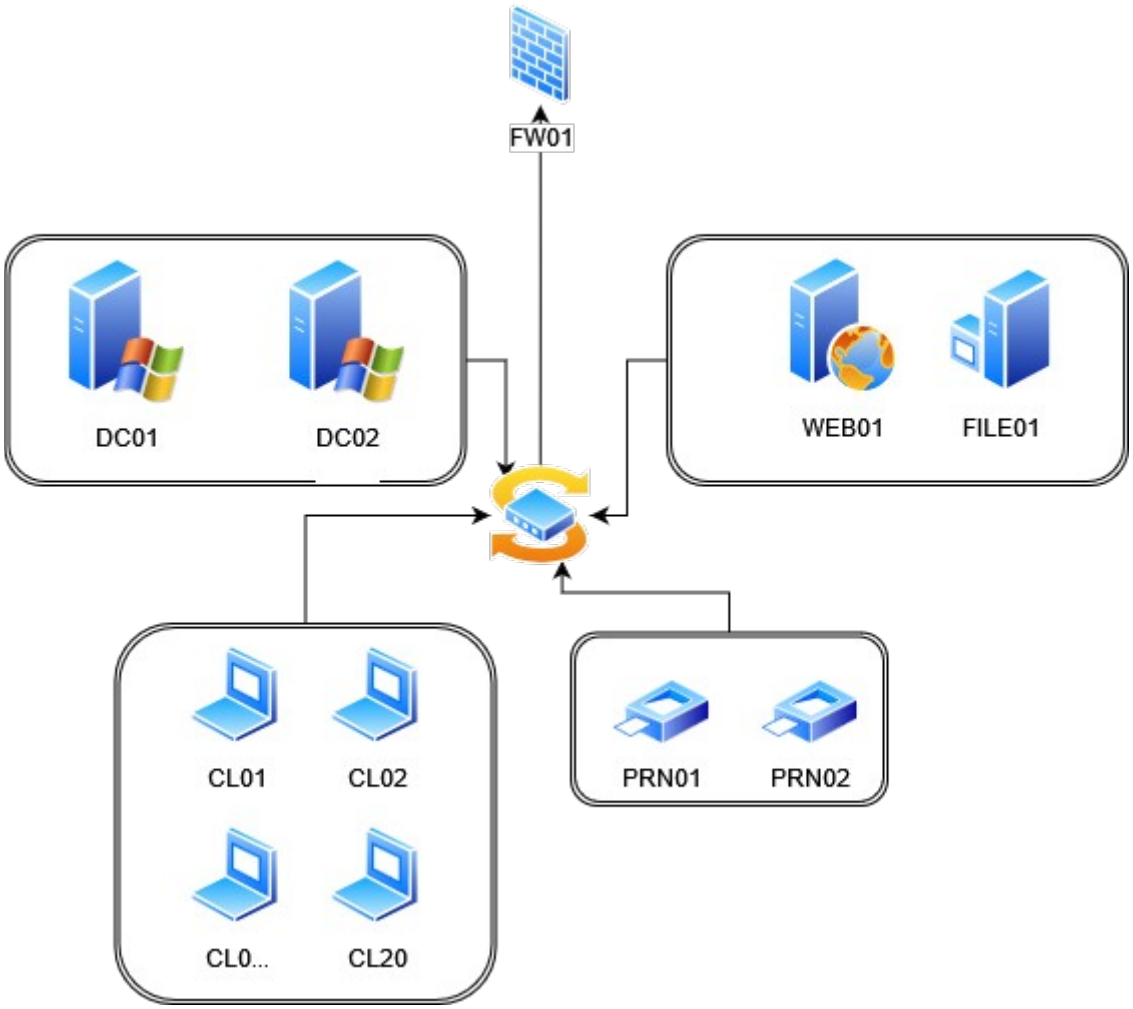
Faire prendre conscience aux étudiants que les choix qu'ils feront dans leurs développements peuvent avoir des conséquences importantes pour l'entreprise dans laquelle ils travailleront au niveau de la sécurité de l'infrastructure et des données.

Comment :

<u>Scénario de la démonstration</u> :

Le scénario est le suivant, un ancien étudiant de l'IEPS de Colfontaine a été engagé par une PME comme informaticien. Historiquement, cette PME faisait appel à une société de service mais vu que les besoins augmentaient de plus en plus, ils ont décidés d'engager quelqu'un à temps plein pour s'occuper de l'infrastructure et des développements internes.

Le schéma réseau est le suivant :



Avant la période COVID, il n'y avait pas de télétravail au sein de cette PME, le COVID a forcé l'entreprise à mettre en place du télétravail. Il a été décidé que seule l'application web se trouvant sur WEB01 serait disponible pour le télétravail étant donné qu'il s'agit de la principale application utilisée par l'entreprise.

Malheureusement régulièrement, le serveur de base de données (MySQL) qui tourne également sur ce serveur semble ne plus répondre. Afin de se faciliter la vie, le nouvel informaticien a développé une petite page web qui lui permet de vérifier et au besoin redémarrer le service MySQL à distance.

Déroulement de la démo :

Explication du scénario et à chaque étape importante :

- Présentation du schéma réseau
- Présentation du code développé pour le monitoring
- …

Des questions seront posées aux étudiants afin de voir quelles sont leurs connaissances en matière de sécurité mais également leur ouvrir les yeux sur les risques des différents choix.

En raison des erreurs, une compromission complète de l'infrastructure sera démontrée :

1. Exploitation du code « monitoring » sur le serveur web.
2. Accès à la base de données MySQL se trouvant sur le serveur web via l'utilisateur/mot de passe qui est codé en dur dans les fichiers de configuration de l'application web.
3. Récupération des utilisateurs et mot de passe se trouvant dans la base de données.
4. Scan du réseau afin de trouver d'autres ordinateurs/serveurs.
5. Connection à une machine utilisateur en Remote Desktop via un utilisateur/mot de passe trouvé dans la base de données (réutilisation de mot de passe).
6. Extraction des utilisateurs/mots de passe en mémoire sur l'ordinateur dont l'administrateur du domaine.

Dans ce scénario, les erreurs seront les suivantes :

- Aucune segmentation du réseau qui permet à un attaquant de se déplacer latéralement facilement dans le réseau.
- Accès direct à une application WEB sans protection supplémentaire par exemple un Web Application Firewall.
- Mauvais choix de solution pour résoudre un problème de type monitoring (des solutions éprouvées existent).
- Aucun monitoring permettant de se rendre compte de l'intrusion.
- Mauvaises pratiques des utilisateurs (réutilisation de mot de passe pour des services différents).