Drone Elisee Mission C et D cybersecurité

Mission C

* 1. Expliquez pourquoi le formulaire de création des identifiants de connexion permet une authentification sécurisée.

Le formulaire de création des identifiants de connexion permet une authentification sécurisée car il requiert que le mot de passe ait une longueur de 8 caractères minimum, qu’il contienne au moins une minuscule, une majuscule, un chiffre, et un caractère spécial. De plus le formulaire vérifie également si le mot de passe fait partie du dictionnaire, si c’est le cas il demande à l’utilisateur de le changer. Ainsi toutes ces mesures permettent d’avoir un mot de passe fort qui n’appartiennent pas à un dictionnaire et qu’on ne peut pas facilement deviner, de plus cela permet de se prémunir d’attaque par force brute qui vise souvent des mots de passe faible et facile à deviner.

* 1. Précisez l’objectif de la procédure d’authentification décrite. Justifiez votre réponse en spécifiant le type d’authentification utilisée.

L’objectif de la procédure d’authentification décrite est de vérifier que le mot de passe soit solide et complexe. Le type d’authentification utilisée est l’authentification par mot de passe, qui doit être de 8 caractères au minimum et doit comporter au moins une minuscule, une majuscule, un chiffre et un caractère spécial et ne doit pas appartenir à un dictionnaire. Ainsi cela permet de réduire le risque d’une attaque par dictionnaire ainsi que de l’attaque par brute force qui vise souvent des mots de passes simple.

* 1. Indiquez si la procédure d’initialisation des drones chez DRONE-SECURITE permet d’éviter les failles de sécurité décrites dans l’étude.

La procédure d’initialisation des drones chez DRONE-SECURITE ne permet pas d’éviter les failles de sécurité décrites dans l’étude car Drone sécurité utilise des identifiants prés configurés et n’impose pas la modification lors du démarrage de l’appareil, ainsi si un attaquant a accès au drone et si l’exploitant n’a pas changé les identifiants par défaut, il aura alors accès aux données d’authentification. De plus on ne sait pas si drone sécurité utilise les mêmes données de connexion standards sur tout ses drones, si c’est le cas beaucoup de leur drone contiennent la même faille de sécurité. De plus on ne sait pas si le noyau linux des drones utilise une ancienne version ou si la version utilisée est à jour.

Mission 2

2.1 Montrer comment la configuration des partages permet de contrôler l’accès aux données.

La configuration des partages permet de contrôler l’accès aux données notamment avec les autorisations sur le fichier util\_Durand. Il y a des permissions qui concernent le contrôle, la modification, la lecture et l’exécution, l’affichage du dossier, la lecture et l’écriture. De plus pour le partage des dossiers il y a le partage avancé qui permet de gérer si l’on veut partager le dossier, tout en limitant le nombre d’utilisateurs ainsi que les autorisations.

2.2 Préciser l’intérêt de séparer (dans un autre VLAN) le serveur de fichiers des autres serveurs.

Séparer le serveur de fichier des autres serveurs permet de renforcer la sécurité car s’il ne se trouve pas sur les serveurs il sera isolé et le risque pour un utilisateur non autorisé à avoir accès au dossier sera moins élevé. En effet l’accès au fichier sera restreint ce qui améliore grandement la sécurité si d’autres parties du serveur présentent des failles. De plus cela permet de limiter l’accès en mettant en place un contrôle.

Dossier D

* 1. Le développement de la page d’authentification de Géomap doit faire l’objet de toutes les attentions car elle doit éviter les accès non autorisés. Si la page n’est pas suffisamment sécurisée les comptes peuvent être compromis.
  2. La première version n’est pas sécurisée car elle est vulnérable aux attaques par injection SQL.

Ligne 6

if (oneAuth.isValidInput(loginSaisi) && oneAuth.isValidInput(passwordSaisi)) { SaisieSecurise = true;

2.1 Tracer les tentatives d’authentification permet de surveiller les tentatives d’authentification qui sont suspectes avec des identifiants qui sont faux et utilisées plusieurs fois à la suite. Cela pourrait permettre de retracer l’activité également des utilisateurs.

2.2