EduGroupe
Accompagner pour réussir

Durcissement des systèmes : Renforcer la sécurité des environnements Windows et Linux

Durée : 2 jours (14 heures)

CONNAISSANCES PREALABLES

- Connaissances de base en administration Windows et/ou Linux.
- Compréhension des concepts réseaux et systèmes.
- Une expérience en exploitation ou administration d'infrastructures informatiques est recommandée.

PROFIL DES STAGIAIRES

- Administrateurs systèmes
- Administrateurs réseaux
- Administrateurs sécurité
- Ingénieurs systèmes et infrastructures
- Analystes SOC
- Consultants cybersécurité
- Responsables techniques
- Toute personne chargée de l'exploitation et de la sécurisation des systèmes d'information.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les principes du durcissement des systèmes.
- Identifier les vulnérabilités liées aux mauvaises configurations.
- Réduire la surface d'attaque des systèmes Windows et Linux.
- Mettre en œuvre les bonnes pratiques de sécurisation des postes et serveurs.
- Renforcer la gestion des identités et des privilèges.
- Sécuriser les services, applications et protocoles réseau.
- Mettre en place des mécanismes de journalisation et de supervision.
- Évaluer le niveau de sécurité d'un système et définir un plan de remédiation.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de démonstrations techniques.
- Travaux pratiques de sécurisation de systèmes Windows et Linux.
- Études de cas inspirées de scénarios réels d'attaques.
- Exercices d'analyse de configurations et d'identification des vulnérabilités.
- Ateliers collaboratifs de remédiation.

- Cas fil rouge permettant de réaliser un audit et un durcissement progressif d'un système..

FORMATEUR

- Consultant expert en cybersécurité et administration des systèmes disposant d'une expérience significative dans la sécurisation d'infrastructures Windows et Linux, la gestion des vulnérabilités, les audits techniques et le maintien en condition de sécurité.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation continue des acquis lors des ateliers pratiques.
- Quiz de validation des connaissances.
- Évaluation des compétences lors des exercices de durcissement.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis..

CONTENU DU COURS

Jour 1 : Comprendre et mettre en œuvre le durcissement des systèmes (7h)

Module 1 : Principes du durcissement et réduction de la surface d'attaque (2h)

Objectifs

- Comprendre les enjeux du hardening.
- Identifier les principales faiblesses de configuration.

Contenu

- Définition du durcissement des systèmes.
- Menaces ciblant les serveurs et postes de travail.
- Surface d'attaque et exposition des systèmes.
- Référentiels de sécurité (ANSSI, CIS Benchmarks, ISO 27001).
- Approche "Secure by Default".
- Méthodologie de durcissement.

Mise en pratique

Brainstorming collectif :

- Identification des points faibles d'un système standard avant sécurisation.

Module 2 : Sécurisation des comptes, privilèges et accès (2h)

Objectifs

- Renforcer le contrôle des accès aux systèmes.
- Réduire les risques liés aux comptes privilégiés.

Contenu

- Gestion des comptes utilisateurs.
- Gestion des comptes administrateurs.
- Principe du moindre privilège.
- Authentification forte (MFA).
- Politique de mots de passe.
- Gestion des accès distants.

Mise en pratique

Atelier :

- Analyse d'une politique de gestion des accès et définition des améliorations à apporter.

Module 3 : Durcissement des systèmes Windows et Linux (2h)

Objectifs

- Appliquer les bonnes pratiques de sécurisation des systèmes.

Contenu

- Désactivation des services inutiles.
- Gestion des mises à jour et correctifs.
- Configuration sécurisée des systèmes.
- Protection des fichiers sensibles.
- Gestion des permissions.
- Renforcement des paramètres de sécurité.

Mise en pratique

Travaux pratiques :

- Audit simplifié de configurations Windows et Linux.
- Identification des écarts de sécurité.

Module 4 : Atelier de durcissement système (1h)

Objectifs

- Appliquer les notions étudiées durant la journée.

Mise en pratique

Cas pratique :

- Construction d'une checklist de durcissement pour un serveur d'entreprise.

Jour 2 : Sécuriser les services et renforcer la supervision (7h)

Module 5 : Sécurisation des services et protocoles réseau (2h)

Objectifs

- Réduire les risques liés aux services exposés.

Contenu

- Inventaire des services actifs.
- Sécurisation des protocoles d'administration.
- SSH, RDP et accès distants.
- Sécurisation des services Web.
- Chiffrement des communications.
- Gestion des certificats.

Mise en pratique

Atelier :

- Analyse d'un serveur exposé et identification des actions de sécurisation.

Module 6 : Journalisation, supervision et détection (2h)

Objectifs

- Améliorer la visibilité sur les événements de sécurité.
- Détecter les comportements anormaux.

Contenu

- Journaux systèmes.
- Journalisation avancée.
- Surveillance des accès.
- Collecte des événements.
- Introduction à la supervision de sécurité.
- Bonnes pratiques de conservation des traces.

Mise en pratique

Travaux pratiques :

- Analyse de journaux d'événements et identification d'activités suspectes.

Module 7 : Évaluation de la sécurité et remédiation (2h)

Objectifs

- Mesurer le niveau de sécurité d'un système.
- Définir les actions correctives prioritaires.

Contenu

- Analyse des vulnérabilités.
- Audits de configuration.
- CIS Benchmarks.
- Gestion des écarts.
- Priorisation des remédiations.
- Maintien en condition de sécurité.

Mise en pratique

Atelier :

- Élaboration d'un plan de remédiation à partir d'un audit de sécurité.

Module 8 : Cas pratique de synthèse – Durcir un système d'information (1h)

Objectifs

- Mobiliser l'ensemble des compétences acquises.

Mise en pratique

Exercice fil rouge :

À partir d'une infrastructure fictive :

- Analyse des vulnérabilités.
- Évaluation de la surface d'attaque.
- Sécurisation des comptes et des accès.
- Durcissement des systèmes et services.
- Mise en place de la journalisation.
- Élaboration d'un plan d'amélioration continue.
- Présentation des recommandations au groupe.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.