

Durcissement des systèmes

Améliorer la sécurité des systèmes

 Présentiel ou en classe à distance



3 jours (21 h)

Prix inter : 2.650,00 € HT
Forfait intra : 6.150,00 € HT

Réf.: SE011

Avec des environnements de plus en plus connectés, le risque d'attaques s'accroît... Comment dès lors minimiser ces risques sur les équipements informatiques de l'organisation ? L'application de diverses techniques de durcissement de systèmes (ou Hardening en anglais), plus ou moins complexes à mettre en œuvre, comme par exemple restreindre l'accès aux réseaux Wifi ou encore cloisonner les machines, permet de répondre à ce besoin. À l'issue de cette formation de 3 jours, les participants auront acquis les connaissances et compétences nécessaires au durcissement des systèmes Linux et Windows.

A qui s'adresse cette formation ?



Pour qui

- Administrateurs systèmes et réseaux



Prérequis

- Disposer de connaissances en administration système Windows et Linux
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

Programme

1 - Introduction générale sur la sécurité informatique

- Mise en place d'un atelier de machines Linux/Windows vulnérables et à durcir
- Cartographie d'un système d'information : identification de la topologie réseau
- Cartographie d'un système d'information : identifier les machines accessibles avec NMap
- Cartographie d'un système d'information : identifier les machines affectées par des vulnérabilités connues
- Faire une veille sur les vulnérabilités connues
- Durcissement réseau : restreindre l'accès à un réseau filaire ou sans-fil
- Durcissement réseau : cloisonner les machines
- Durcissement réseau : masquer une machine et ses services avec un pare-feu

2 - Durcissement de machines Windows

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles sur Windows
- Définir une politique de mises à jour sur les produits Microsoft
- Surveiller les mises à jour de sécurité des produits non-Microsoft
- Restreindre l'accès distant au parc Windows
- Mise en place d'alertes de sécurité sur le parc Windows
- Utilisation du pare-feu Windows
- Utilisation d'un anti-virus sur Windows
- Restreindre l'exécution des applications
- Utiliser les politiques de groupes (GPO)
- Auditer les politiques de groupes (GPO) avec Microsoft Security Compliance Manager

- Protection physique (clés USB, BIOS...)

3 - Durcissement de machines Linux

- Définition des besoins de durcissement
- Panorama des outils de durcissement disponibles sur Linux
- Définir une politique de mises du noyau Linux
- Définir une politique de mises à jour des applicatifs tiers sur Linux
- Restreindre l'accès distant au parc Linux
- Mise en place d'alertes de sécurité sur le parc Linux avec OSSEC
- Utilisation du pare-feu Linux
- Utilisation d'un anti-virus sur Linux
- Restreindre l'exécution des applications et des commandes sur Linux
- Auditer les configurations avec Lynis



Les objectifs de la formation

- Comprendre l'intérêt des techniques de durcissement systèmes et réseau
- Maîtriser les différentes techniques de durcissement des systèmes Linux et Windows
- Être capable de protéger les systèmes de l'entité contre des vulnérabilités non publiées



Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiques.
- Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).
- Les retours d'expériences de professionnels de la sécurité.
- 93% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.



Dates et villes 2026 - Référence SE011



Dernières places disponibles



Session garantie

Rennes

du 12 janv. au 14 janv.

du 28 sept. au 30 sept.

du 7 déc. au 9 déc.

A distance

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

du 7 avr. au 9 avr.

du 28 sept. au 30 sept.

Paris

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

du 7 avr. au 9 avr.

du 28 sept. au 30 sept.

Aix-en-Provence

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 28 sept. au 30 sept.

Toulouse

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 28 sept. au 30 sept.

Nantes

du 12 janv. au 14 janv.

du 28 sept. au 30 sept.

du 7 déc. au 9 déc.

Marseille

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 28 sept. au 30 sept.

Lille

du 12 janv. au 14 janv.

du 27 juil. au 29 juil.

du 28 sept. au 30 sept.

Lyon

du 7 avr. au 9 avr.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

Rouen

du 7 avr. au 9 avr.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

Sophia Antipolis

du 7 avr. au 9 avr.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

Strasbourg

du 7 avr. au 9 avr.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.

Bordeaux

du 7 avr. au 9 avr.

du 27 juil. au 29 juil.

du 7 déc. au 9 déc.