

**Sujet d'épreuves de la 48^e Compétition Nationale
des Métiers**

MÉTIER N°54 CYBERSÉCURITÉ

HARDENING ENTERPRISE MODULE A

EXPLICATION DU SUJET

DUREE TOTALE DE L'ÉPREUVE	8 heures
DIFFUSION DU SUJET	Découvert le jour de la compétition

INTRODUCTION

Durant cette épreuve, vous serez plongé dans la vie d'un administrateur système qui intervient après une attaque informatique ayant eu lieu dans une entreprise.

CONSEILS

Le sujet est rédigé de sorte que les recommandations soient claires à réaliser. La notation s'effectuera sur la vérification de ces différentes recommandations à la fin de l'épreuve. La réalisation de certaines documentations sera également exigée et comptera dans la notation.

Votre objectif pour la compétition est de capitaliser un maximum de points. Concentrez-vous sur votre réalisation, et non sur celle des autres. Enfin, n'oubliez pas que vous formez une équipe, alors ne vous précipitez pas. Prenez le temps de lire le sujet une première fois dans son intégralité, communiquez avec votre coéquipier et partagez-vous les tâches. Optimisez votre temps.

DESCRIPTION

L'objectif est de mettre à l'épreuve vos compétences en cybersécurité du point de vue d'un administrateur système. Pour cela, vous serez placés dans un contexte réaliste d'entreprise ayant subi une attaque. Au début de l'épreuve, vous aurez à disposition une description suffisante de l'infrastructure existante de l'entreprise, ainsi qu'un rapport post-mortem de la réponse à incident ayant eu lieu, accompagné des recommandations à mettre en œuvre. L'épreuve se déroulera sur une journée de 8h, durant laquelle vous travaillerez sur un hyperviseur de type Proxmox et devrez configurer différentes machines présentes dans l'infrastructure.

Durant l'épreuve, vous serez évalués selon les critères suivants :

- Votre aptitude à comprendre un rapport post-mortem de réponse à incident ;
- Votre maîtrise des différentes machines mises à disposition (OPNSense, Debian, Windows, Windows Server) ;
- Vos connaissances sur les différents applicatifs au sein d'une entreprise (Active Directory, Postfix).

L'entièreté de l'épreuve se déroulera sur l'hyperviseur et les différentes machines virtuelles déployées sur celui-ci. Vous devrez configurer les machines et les services de manière à suivre les recommandations du rapport post-mortem. Chaque recommandation ou demande appliquée rapportera un nombre plus ou moins élevé de points en fonction de sa difficulté.

À la fin de l'épreuve, vous devrez laisser les machines virtuelles et l'hyperviseur dans leur dernier état. Afin de déterminer votre note finale, les évaluateurs se baseront sur les configurations que vous aurez effectuées sur les services. Aucune étape liée à la rédaction d'un rapport ne sera proposée.