



Présentation

Code interne : ERI9-PROJ3

Objectifs

A l'issue de ce CTF, les participants seront capables d'identifier, analyser et exploiter des vulnérabilités dans un environnement virtuel, en mobilisant des méthodes d'investigation, de raisonnement technique et de résolution de challenges cyber.

Heures d'enseignement

TDM

Travaux Dirigés sur Machine

8h

Modalités de contrôle des connaissances

Évaluation initiale / Session principale

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Contrôle Continu	Contrôle Continu					Évaluation par score CTF : La validation du module est conditionnée à l'obtention d'un score minimal attendu correspondant à un seuil défini par l'équipe pédagogique, calculé à partir des points obtenus sur les challenges réussis. Chaque challenge attribue un nombre de points variable selon son niveau de difficulté.