

Master 2 ISSD / UE 10

Examen

**Semestre 10 -2023/2024 – 1^{ère} session
avril 2024**

Durée : 1h00 / documents non autorisés

I. Recherche d'information (5 points : 2 + 1,5 + 1,5)

1. Définissez l'OSINT et ses champs d'applications
2. En quoi l'OSINT est intéressant pour attaquer une cible mais surtout aussi pour se défendre ?
3. Resituer le rôle et les impacts de l'OSINT dans un processus d'attaque cyber.

II. Accès à distance (6 points : 1,5 + 1,5 + 1,5 + 1,5)

Il y a quelques jours, le responsable de l'entreprise UPS-ISSD a découvert que son site web externe (<https://www.ups-issd.fr> utilisant le CMS (Content Management System) Wordpress) avait été « défacé » par des cyberactivistes.

1. Quelles hypothèses concernant les mécanismes d'intrusion pouvez-vous formuler ?
2. Quels sont les risques collatéraux à cette attaque que vous pouvez identifier ?
3. Pourquoi la connexion à un site web en HTTPS n'est pas forcément une garantie de sécurité ?
4. Quelles sont vos préconisations afin d'identifier et de limiter le risque ?

III. Hacking & Menaces (9 points : 2 +2 +5)

Considérons le problème des attaques de type *Rançongiciel* à un ordinateur.

1. Expliquez les mécanismes d'infiltration, de déploiement et d'exploitation de ce type d'attaque
2. Quelles sont les mécanismes utilisés par les « hackers » pour inciter les victimes à payer la rançon demandée ?
3. Le bulletin de l'Université de Toulouse (public cible : **grand public**) vous a recruté pour rédiger un article de vulgarisation sur le sujet suivant (une page maximum) !
« IA génératives face aux humains : le cocktail explosif pour la cybersécurité ? »
Vous pouvez étayer votre propos par des exemples de l'actualité récente.