



**Sujet d'épreuves des Sélections régionales
de la 47^e Compétition des Métiers**

MÉTIER N°54

CYBERSECURITE

MODULE C

Soumis par :

Samy SCANNA, Expert WorldSkills France

TABLE DES MATIERES

1.	EXPLICATION DU SUJET.....	3
2.	PLANNING JOURNALIER	5
3.	MATERIAUX ET CONSOMMABLES	6
4.	OUTILLAGE PERSONNEL	ERREUR ! SIGNET NON DEFINI.
5.	BARÈME DE CORRECTION.....	7
6.	ANNEXES	ERREUR ! SIGNET NON DEFINI.

1. EXPLICATION DU SUJET

DURÉE TOTALE DE L'ÉPREUVE :

4h30 heures

DIFFUSION DU SUJET :

Découvert le jour de la compétition

PREAMBULE

INTRODUCTION

WorldSkills France accueille la compétition mondiale en 2024 à Lyon, dans ce contexte les Administrateurs Systèmes & Réseaux de WorldSkills ont fait évoluer l'infrastructure informatique afin de permettre un travail des collaborateurs dans les meilleures conditions.

En votre qualité d'auditeur Cybersécurité, WorldSkills France vous sollicite pour réaliser un test d'intrusion sur sa nouvelle infrastructure, pour auditer certains codes applicatifs et afin d'anticiper toute future attaque informatique, vous demande d'auditer une machine qui serait à priori infectée.

CONSEILS ET CONSIGNES DANS LE CADRE DE LA REALISATION DU SUJET

En tant qu'équipe prétendante au titre de champion régional dans votre métier ainsi qu'à la représentation de votre région aux prochaines finales nationales, votre victoire passera inéluctablement par la compréhension des éléments suivants.

Le sujet est rédigé de sorte que les réponses attendues aux questions soient pour la majorité des réponses uniques et simples, c'est-à-dire que les réponses seront les mêmes pour tout le monde et aucune variation ne sera possible.

Ainsi soyez très attentif aux éléments de réponse, si le résultat attendu est « **explorer.exe** », ne donnez pas « **Explorer.exe** » comme réponse, cela sera considéré comme faux. L'objectif ici n'est pas de vous embêter dans votre épreuve mais de vous préparer au mieux à la compétition internationale, car certaines questions/configurations seront corrigées automatiquement et attendront un résultat strictement identique à ce qui est prévu.

Soyez donc attentifs aux majuscules/minuscules et aux accents.

Si vous pensez ne pas pouvoir finaliser le sujet, concentrez-vous sur ce que vous maîtrisez. **Votre objectif pour la compétition est de capitaliser un maximum de points.**

Concentrez-vous sur votre réalisation et non celle des autres.

On peut parfois être tenté de regarder l'état d'avancement des autres compétiteurs, mais sachez que dans notre métier, dû à son manque de concret visuel, les personnes qui semblent les plus avancées ne sont pas forcément celles qui capitaliseront le maximum de points.

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 co-équipier et **partagez**-vous les tâches, **optimisez** votre temps.

DESCRIPTION DU SUJET

Le Module C consiste à mener une investigation numérique sur une machine vérolée préparée spécialement pour l'épreuve et à répondre à un ensemble de questions.

Cette investigation se veut rapide et se déroule en un temps restreint de 1h que l'on peut appeler « Speed Module », ainsi l'investigation n'implique pas de techniques de reverse engineering afin d'analyser les binaires incriminés mais se contentera simplement d'une analyse de surface de la machine vérolée.

MODULE C – FORENSIC

Ce module nécessite une **connexion à Internet**, ainsi il se déroule uniquement lorsque les modules A et B sont terminés et rendus.

L'activité se déroule sur la machine virtuelle **WS-FORENSIC**, la session s'ouvre automatiquement au démarrage du système, il n'y a pas de mot de passe. La machine est connectée à Internet.

L'objectif de ce module est de mener une investigation numérique sur une machine (**WS-FORENSIC**), cette machine vous est fournie par une personne qui se dit victime d'un logiciel malveillant. D'après les dires de la victime, son ordinateur se comporte curieusement depuis qu'elle a téléchargé des fichiers sur internet, nous n'avons pas plus d'information.

Vous devez répondre à un certain nombre de question fournies ci-dessous, pour chacune des questions, vous justifierez vos réponses par une capture d'écran de l'élément/outil vous ayant permis d'obtenir l'information.

Q1 - Identifiez le fichier téléchargé qui est à l'origine de l'infection, expliquez pourquoi c'est selon-vous ce fichier ?

Q2 - Identifiez le site web ayant permis le téléchargement du fichier vérolé.

Q3 - D'après-vous, comment la victime a obtenu ce lien de téléchargement ?

Q4 - Identifiez la date et l'heure du téléchargement ainsi que le navigateur web utilisé par la victime.

Q5 - Pourquoi l'antivirus intégré à la machine n'a pas détecté le lancement du fichier vérolé ?

Q6 - Dans quel dossier le logiciel malveillant s'est installé ?

Q7 - Quel est le nom du processus en arrière-plan infecté par le logiciel malveillant ?

Q8 - Que pouvez-vous dire de ce processus ?

Q9 - Comment le processus se lance-t-il au démarrage du système ? Donnez des détails.

Q10 - Quelles actions le processus réalise-t-il en arrière-plan ?

Q11 – Quel est le type du logiciel malveillant ?

Q12 - Identifier le nom DNS, l'adresse IP et le port du serveur de Command & Control.

Q13 - Où est hébergé le serveur de Command & Control (hébergeur et localisation) ?

Q14 - Identifiez à qui appartient le nom de domaine du serveur de Command & Control

Q15 - Que pouvez-vous déduire de l'information obtenue à la question précédente ?

2. PLANNING JOURNALIER

Le sujet devra rentrer dans une durée de concours de **4 heures 30 maximum**.

	DÉBUT	FIN	TÂCHES	TOTAL
C1	7h30		Arrivée des candidats	
	8h00	9h00	Consignes du jury, étude du premier sujet, et prise en main de l'espace métier	1h00
	9h00	12h00	Module A et B – Test d'intrusion et revue de code	3h00
	12h00	13h30	Déjeuner	1h30
	13h30	15h00	Module C - Forensic	1h30
	15h00	17h00	Correction	2h00
	TOTAL ÉPREUVE (h)			4h30

3. MATÉRIAUX ET CONSOMMABLES

A) MIS A DISPOSITION PAR L'ORGANISATION

Liste des matériaux et consommables mis à disposition à chaque compétiteur pour la réalisation de l'épreuve :

INTITULÉ	DESCRIPTION / RÉFÉRENCE	QUANTITÉ	REMARQUES
Poste de travail Windows 10	Destiné à héberger les VM	1 par compétiteur	Accès à internet nécessaire Logiciels : VMWare Workstation, Putty
VM WS-FORENSIC	VM du Module C	1 par compétiteur	Accès à internet nécessaire (Vmware NAT)

4. BARÈME DE CORRECTION

Grille avec le détail des critères de notation objectifs et jugements.

CYBERSECURITE						
Critère	Sous Critère	Jour	Intitulé du critère de notation	Objectif ou Jugement	Barème	Coef.
			Poste de travail			
C			Critère C :			
			MODULE C : FORENSIC			
C	01	1	Q1	J	2	1
C	02	1	Q2	O	1	1
C	03	1	Q3	J	1	1
C	04	1	Q4	O	1	1
C	05	1	Q5	J	2	1
C	06	1	Q6	O	1	1
C	07	1	Q7	O	1	1
C	08	1	Q8	J	2	1
C	09	1	Q9	O	1	1
C	10	1	Q10	O	1	1
C	11	1	Q11	O	1	1
C	12	1	Q12	O	2	1
C	13	1	Q13	O	1	1
C	14	1	Q14	O	1	1
C	15	1	Q15	J	2	1
TOTAL :					20	
TOTAL				20		