

**Sujet d'épreuves des Finales
Nationales de la 47^e Compétition des
Métiers**

**MÉTIER N°54
CYBERSECURITE**

**Module A – Hardening
d'infrastructure Equipe 1**

Soumis par :

Samy SCANNA, Expert WorldSkills France

TABLE DES MATIERES

1.	MODULE A – HARDENING D’INFRASTRUCTURE	3
2.	PLANNING JOURNALIER	3
3.	DONNEES TECHNIQUES	4
4.	TRAVAIL A REALISER	5
5.	BARÈME DE CORRECTION	8

1. MODULE A – HARDENING D'INFRASTRUCTURE

DURÉE TOTALE DE L'ÉPREUVE :

3h30 heures

L'objectif de ce module est d'évaluer les capacités à renforcer la sécurité dans une infrastructure préexistante.

Il s'appuie sur des notions systèmes Windows et GNU Linux.

L'accès à internet n'est pas autorisé durant toute la durée du module.

2. PLANNING JOURNALIER

C1	DÉBUT	FIN	TÂCHES	TOTAL
	7h30	8h00	Arrivée des candidats	30mn
	8h00	9h00	Consignes du jury, étude du sujet, et prise en main espace métier	1h00
	9h00	12h30	Épreuve Module A + pause	3h30
	12h30	13h30	Service du déjeuner	1h
	13h30	17h00	Épreuve Module B + pause	3h30
	17h00	19h00	Correction	2h00
TOTAL ÉPREUVE (h)				7h00

3.DONNEES TECHNIQUES

EQUIPE 1			
Nom VLAN	ID Vlan	Adressage IP	Passerelle
DATACENTER	10	172.16.120.0/26	172.16.120.1
FRONTOFFICE	11	172.16.130.0/27	172.16.130.1
DMZ	12	172.16.140.0/28	172.16.140.1
REMOTE	13	192.168.100.0/24	192.168.100.1

EQUIPE 1				
Machines	ID Vlan	IP	Masque	Passerelle
SRV-AD01	10	172.16.120.5	255.255.255.192	172.16.120.1
SRV-AD02	10	172.16.120.10	255.255.255.192	172.16.120.1
SRV-CENT01	10	172.16.120.15	255.255.255.192	172.16.120.1
CLT-WIN01	11	172.16.130.2	255.255.255.224	172.16.130.1
SRV-CENT02	12	172.16.140.2	255.255.255.240	172.16.140.1
SRV-CENT03	12	172.16.140.3	255.255.255.240	172.16.140.1
CLT-WIN02	13	192.168.100.2	255.255.255.0	192.168.100.1

Voici les informations d'authentification vous permettant de vous connecter au serveur VPN (le compte permet deux connexions), le profil OpenVPN est déjà présent sur la machine candidat, vous devez simplement l'importer puis vous connecter :

EQUIPE 1 - Accès VPN	
Identifiant VPN	Mot de passe VPN
equipe1	Ap84jf1z0

4. TRAVAIL A REALISER

WINDOWS SERVER SRV-AD01 & SRV-AD02 – LAN DATACENTER

Précision : Aucune modification de la GPO « Default Domain Controllers Policy » ne doit être faite, toute action liée aux GPOs devra se faire dans une nouvelle GPO créé pour l'occasion et nommée de manière explicite afin de faciliter la correction.

- Domaine: **ws2023.org**
- Faire de AD02 un contrôleur de domaine secondaire du domaine.
- Implémenter les utilisateurs et groupes suivants, le compte utilisateur étant formé selon la règle suivante : première lettre prénom+nom de famille.

Nom Groupe	Utilisateurs	Remarque
GRP-USR-ADMINS	Rob HALFORD Dave MUSTAINE John GALLAGHER Klas RYDBERG	Groupe des administrateurs informatiques
GRP-USR-FRONTOFFICE et GRP-USR-REMOTE	Led ZEPPELIN Rose PETIT Roger WATERS	Groupe des utilisateurs en contact avec les clients et qui disposent d'un accès VPN.
GRP-USR-RECHERCHE	Syd BARRET Andrew LATIMER David GILMOUR	Groupe de R&D

- Tous les utilisateurs ont pour des raisons de commodité (candidats/Jury) le mot de passe **W@rldskills01**
- Lorsqu'un utilisateur essaie de se connecter, afficher le message "**Accès restreint aux seules personnes autorisées**".
- Seuls les utilisateurs membres du groupe **GRP-USR-ADMINS** ont le droit de se connecter en RDP ou en local aux serveurs **AD01** et **AD02**.
- Les utilisateurs du groupe **GRP-USR-FRONTOFFICE** ne peuvent se connecter sur leur PC qu'entre **8:30** et **19:00**.
- Profils des utilisateurs : les utilisateurs disposent d'un profil itinérant, ces profils seront stockés dans **\\AD1\profiles\<nom de l'utilisateur>**
- Le quota par utilisateur sera de **100 Mo**
- Interdire le stockage de tout fichier exécutable, de dll, de fichier vidéo ou musical dans le profil de l'utilisateur
- Chaque groupe d'utilisateur doit disposer d'un lecteur partagé qui s'installera automatiquement lors de la connexion de l'utilisateur, via le lecteur "**X**", et qui s'intitulera "**PARTAGE**"
- A l'intérieur de ce dossier, seuls les membres du groupe d'utilisateur auquel appartient l'utilisateur pourront lire et écrire
- Chaque utilisateur disposera d'un lecteur "**Y**" intitulé, "**COMMUN**", tout le monde pourra lire et écrire dans ce dossier, sauf les utilisateurs du groupe "**GRP-USR-REMOTE**" qui n'ont qu'un accès en lecture.
- Configurer les politiques d'audit pour que toute demande de **suppression** ou **modification** de fichier non autorisée sur le lecteur **Y** génère une alerte dans le journal d'évènement.

- Configurer le suivi des tentatives d'authentification utilisateur infructueuses
- Configurer le suivi des modifications des stratégies de sécurité
- Configurer le suivi des blocages automatiques des comptes
- Sur le serveur **AD01**, placer un fichier "c:\nepastoucher.txt", générer dans les logs AD une alerte en cas de tentative d'accès à ce fichier.
- Activer le verrouillage automatique de session au bout de **10** minutes d'inactivité
- Activer la réplication **DFS** des dossiers de partage (**COMMUN** et **PARTAGE**) sur le serveur **AD02**
- Interdisez l'accès au réseau des postes Windows si les postes:
 - N'ont pas le pare-feu activé,
 - Aucun antivirus n'est installé (nous ne cochons pas si les mises à jour sont faites, pour raison d'accès internet interdit),
- Le pare-feu des clients sera automatiquement paramétré de sorte que les services suivants soient autorisés :
 - Remote Desktop
 - Remote Assistance
 - Network Discovery
 - Tout service nécessaire au bon fonctionnement de l'infrastructure, et tout accès aux services de la DMZ.
- La taille minimale des mots de passe des utilisateurs sera de **12** caractères, composés de chiffres lettres, majuscules, minuscules et au moins un caractère spécial.
- Chaque mot de passe expire au bout de **30** jours
- Désactiver tout compte pour **1** heure en cas de saisie de **4** mauvais mots de passe
- Configurer les clients et serveurs Microsoft pour qu'ils utilisent **SMB signé**.
- Configurer l'authentification en **NTLMv2**, interdire **LM** et **NTLM**
- Activer le mode de chiffrement élevé pour le bureau à distance
- Transférer les logs/journaux d'événements **des serveurs AD** vers **Splunk** sur **CENT01**
- Chaque machine de l'infrastructure doit disposer de son enregistrement DNS au format « **hostname.ws2023.org** ».

CLI-WIN-01 – LAN FRONTOFFICE

- Nom: **CLT-WIN01**
- Joint au domaine

CLI-WIN-02 – LAN REMOTE

- Nom: **CLT-WIN02**
- Client **OpenVPN**, servira à tester l'authentification sur le serveur VPN.

SRV-CENT01 – LAN DATACENTER

- Créer les 4 utilisateurs suivants en respectant le nommage utilisé pour les serveurs AD.
 - Rob HALFORD
 - Dave MUSTAINE
 - John GALLAGHER
 - Klas RYDBERG
- Ils auront tous comme mot de passe **W@rldskills01**
- Les mots de passe expirent au bout de **30 jours**, il est impossible de réutiliser les **10 derniers mots de passe**
- La taille minimale pour les mots de passe est de **12 caractères**, comprenant au moins **un chiffre, une minuscule, 4 majuscules, un caractère spécial**
- Les comptes sont désactivés au bout de **4 essais infructueux**, et se réactivent au bout d'**une heure**
- Vous installerez un serveur **Splunk** qui recevra les logs des serveurs **AD**, assurez-vous d'utiliser « admin » et « W@rldskills01 » pour l'interface Splunk.
- Vous installerez un serveur **DNS** secondaire qui se synchronisera de façon sécurisée avec le serveur **DNS** de **AD1**.

SRV-CENT02 – LAN DMZ

- Ce serveur héberge un service **OpenVPN**, à destination des travailleurs à distance (**GRP-USR-REMOTE**).
- Ces utilisateurs disposent, afin de se connecter d'un certificat qui leur est personnel et du client OpenVPN, assurez-vous de configurer le serveur OpenVPN pour l'ensemble des utilisateurs membres de **GRP-USR-REMOTE** et sur la machine **CLT-WIN02** à minima de la présence de la bonne configuration pour l'utilisateur **Led ZEPPELIN** (1^{er} de la liste).
- Il doit y avoir une double authentification: via certificat ET utilisateur/mot de passe, **openvpn-auth-ldap** (sur ce même serveur) gèrera l'authentification des utilisateurs membres de **GRP-USR-REMOTE**.
- Le trafic sera chiffré entre les télétravailleurs et l'entreprise via les standards de sécurité les plus modernes disponibles dans OpenVPN.
- Lorsqu'un utilisateur est connecté en VPN à partir de **CLT-WIN02**, il doit pouvoir **joindre le serveur web** disponible sur **SRV-CENT03**, ce qui n'est pas le cas par défaut.

SRV-CENT03 – LAN DMZ

- Ce serveur est équipé du service **Apache (httpd)**
- Le serveur Apache est accessible sur le port **80** et **443**.
- Tout trafic **HTTP** est directement redirigé vers **HTTPS**
- Vous générerez un certificat depuis une **autorité interne** installée sur ce serveur, et on partira du principe que cette autorité est une autorité de confiance pour le monde entier.
- Le service HTTPS devra être disponible depuis l'adresse www.worldskills.fr, depuis n'importe quel poste, cette adresse doit être résolue par le DNS interne, depuis le VPN, vous pouvez ajouter manuellement la correspondance nom Hôte/IP manuellement.

5. BARÈME DE CORRECTION

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

CYBERSECURITE – N°54						
Critère	Sous Critère	Jour	Intitulé du critère de notation	Objectif ou Jugement	Barème	Coef.
A			Module A : Infrastructure Hardening		25	
A	01	1	SRV-AD1 et SRV-AD2	O	8	1
A	02	1	CLI-WIN-01	O	1	1
A	03	1	CLI-WIN-02	O	1	1
A	04	1	SRV-CENT01	O	5	1
A	05	1	SRV-CENT02	O	5	1
A	06	1	SRV-CENT03	O	5	1
TOTAL					25	