Skills Compétences Canada Ontario

Practical Review: IT Network Systems Administration (Post-Secondary)

Objective: *Develop hands-on skills in* ***Windows and Linux server administration, networking, security, and troubleshooting*** *in preparation for the* ***Skills Ontario competition****.*

Task 1: Windows Server Configuration (20 points)

Goal: Install and configure Windows Server 2016 (or newer) with Active Directory and network services.

Instructions:

1. Install **Windows Server 2016 (or newer)** on a virtual machine (VM) using **VMware**.
2. Set up **Active Directory**:
    - Create a **new domain** (e.g., mydomain.local).
    - Add **three user accounts** and assign them to different **groups**.
3. Configure **DNS and DHCP**:
    - Set up **DNS zones** and create **A and PTR records**.
    - Configure **DHCP** to assign IP addresses dynamically.
4. Implement **Remote Desktop Services (RDP)** and verify remote access.
5. Document your setup with **screenshots and configuration notes**.

Evaluation Criteria:

- Correct **user and group management** (5 points)
- Functioning **Apache web server** (5 points)
- Configured **Samba or FTP for file sharing** (5 points)
- Security configuration (SSH & firewall) (5 points)

Task 2: Linux Server Administration (20 points)

Goal: Set up and manage a **Linux server** with user accounts, web services, and file-sharing.

Instructions:

1. Install **Ubuntu Server 22.04 (or newer)** on a VM.
2. Create **three users** and assign them to groups.
3. Install and configure **Apache Web Server** to host a basic webpage.
4. Set up **Samba or FTP** for file sharing between Windows and Linux.
5. Secure the server by configuring **SSH access** and **firewall rules**.
6. Document your setup with **screenshots and commands used**.

Evaluation Criteria:

- Correct **user and group management** (5 points)
- Functioning **Apache web server** (5 points)

- Configured **Samba or FTP for file sharing** (5 points)
- Security configuration (SSH & firewall) (5 points)

Task 3: Network Configuration & Troubleshooting (30 points)

Goal: Design, configure, and troubleshoot a network using **Cisco Packet Tracer**.

Instructions:

1. Use **Cisco Packet Tracer** to create a **LAN network** with:
    - **2 routers**
    - **2 switches**
    - **4 client PCs (2 wired, 2 wireless)**
2. Implement **Variable Length Subnet Masking (VLSM)** for subnetting.
3. Configure **Static & Dynamic IP addressing (DHCP)**.
4. Enable **Wi-Fi security (WPA2)** for wireless clients.
5. Troubleshoot **one networking issue** (e.g., incorrect IP, no internet access).
6. Create a **network diagram** and explain your configuration.

Evaluation Criteria:

- Proper **network topology & VLSM subnetting** (5 points)
- Working **IP addressing (Static & DHCP)** (5 points)
- Configured **Wi-Fi security** (5 points)
- Correct **network troubleshooting** (5 points)
- Clear **network diagram & documentation** (10 points)

Task 4: Cybersecurity & System Hardening (20 points)

Goal: Apply cybersecurity best practices and detect vulnerabilities.

Instructions:

1. On **Windows Server**, configure **Group Policy** to:
    - Set **password policies** (minimum length, expiration, complexity).
    - Restrict **USB access** for security.
2. On **Linux Server**, configure:
    - **SSH key-based authentication** for remote login.
    - **SUDO rules** for admin access.
3. Identify **two common cyber threats** and suggest mitigation strategies.
4. Run a **security scan** (Windows Defender or Linux ClamAV) and report findings.

Evaluation Criteria:

- Correct **Group Policy configuration** (5 points)

- Secure **SSH & SUDO access on Linux** (5 points)
- Explanation of **cyber threats & solutions** (5 points)
- Security scan results & analysis (5 points)

Task 5: Final Report & Reflection (10 points)

Goal: Summarize all tasks with screenshots, configuration details, and lessons learned.

Instructions:

1. Compile a report summarizing:
    - **Steps taken** in each task.
    - **Challenges faced** and how they were solved.
    - **Best practices** for IT network administration.
2. Include **screenshots and configuration commands**.
3. Explain **key takeaways** from the exercise.

Evaluation Criteria:

- Well-structured **documentation** (5 points)
- Thoughtful **reflection & best practices** (5 points)

Recommended self-paced courses for review:

1. Introduction to Cybersecurity
Why? Provides foundational knowledge of cybersecurity, essential for securing network systems. **Topics to Focus On:**
- Understanding cyber threats like malware and phishing
- Implementing security measures and best practices
- Exploring career opportunities in cybersecurity

Link: Introduction to Cybersecurity

2. Networking Basics
Why? Covers fundamental networking concepts, crucial for designing and managing networks. **Topics to Focus On:**
- Understanding how networks operate
- Learning about network topologies and devices
- Basic IP addressing and subnetting

Link: Networking Basics

3. Introduction to IoT and Digital Transformation
Why? Introduces the Internet of Things (IoT) and its impact on networking and digital transformation. **Topics to Focus On:**
- Understanding IoT concepts and applications
- Exploring how IoT drives digital transformation
- Learning about IoT security considerations

Link: Introduction to IoT and Digital Transformation

4. Computer Hardware Basics
Why? Provides essential knowledge of computer hardware, important for system setup and troubleshooting. **Topics to Focus On:**
- Identifying computer components and their functions
- Understanding hardware installation and maintenance
- Troubleshooting common hardware issues

Link: Computer Hardware Basics

5. Operating Systems Basics
Why? Covers fundamental concepts of operating systems, necessary for managing and configuring systems. **Topics to Focus On:**

- Understanding different operating systems
- Learning about OS installation and configuration
- Managing system resources and security

Link: Operating Systems Basics

Préparation pratique : TI - Administration de systèmes de réseau (Postsecondaire)

Objectif : *Développer des compétences pratiques en* ***administration, réseautage, sécurité, et dépannage des serveurs Windows et Linux,*** *en préparation aux* ***Olympiades de Compétences Ontario***.

Tâche 1 : Configuration d'un serveur Windows (20 points)

But : Installer et configurer un serveur de Windows 2016 (ou version plus récente), en mettant en place les services Active Directory et de gestion de réseau.

Consignes :

1. Installer la version **serveur de Windows 2016 (ou une version plus récente)** sur une machine virtuelle (VM) en utilisant **VMware**.
2. Configurer **Active Directory** :
    - Créer un **nouveau domaine** (p. ex., mydomain.local)
    - Ajouter **trois comptes utilisateurs** et les affecter à des **groupes** différents
3. Configurer des services **DNS** et **DHCP** :
    - Configurer les **zones DNS** et créer des **enregistrements** de type **A et PTR**
    - Configurer le protocole **DHCP** pour l'attribution automatique d'adresses IP
4. Configurer un environnement **Remote Desktop Services (RDP)** et vérifier l'accès à distance
5. Documenter l'ensemble de la configuration réalisée en incluant des **captures d'écran et des notes de configuration**

Critères d'évaluation :

- **Gestion adéquate des utilisateurs et groupes** (5 points)
- **Serveur Web Apache** fonctionnel (5 points)
- **Samba** ou **FTP** correctement configuré **pour le partage de fichiers** (5 points)
- Configuration de la sécurité, incluant le protocole d'accès SSH et des règles de pare-feu (5 points)

Tâche 2 : Administration du serveur Linux (20 points)

But : Configurer et administrer un **serveur Linux** en mettant en place des comptes utilisateurs, des services Web, et le partage de fichiers.

Consignes :

1. Installer **Ubuntu Server 22.04 (ou une version plus récente)** sur une machine virtuelle
2. Créer **trois utilisateurs** et les assigner à des groupes
3. Installer et configurer le **serveur Web Apache** pour héberger une page Web de base
4. Configurer **Samba** ou **FTP** pour permettre le partage de fichiers entre Windows et Linux
5. Configurer l'accès sécurisé au serveur via un protocole d'**accès SSH** et la mise en place de **règles de pare-feu**

6. Documenter l'ensemble de la configuration réalisée en incluant des **captures d'écran** et les **commandes utilisées**

Critères d'évaluation :

- **Gestion adéquate des utilisateurs et groupes** (5 points)
- **Serveur Web Apache** fonctionnel (5 points)
- **Samba** ou **FTP pour le partage de fichiers** correctement configuré (5 points)
- Configuration de la sécurité , incluant le protocole d'accès SSH et des règles de pare-feu (5 points)

Tâche 3 : Configuration et dépannage réseau (30 points)

But : Concevoir, configurer, et diagnostiquer une panne réseau en utilisant le logiciel **Cisco Packet Tracer**.

Consignes :

1. Utiliser le logiciel **Cisco Packet Tracer** pour créer un **réseau local (LAN)** composé des éléments suivants :
    - **Deux (2) routeurs**
    - **Deux (2) commutateurs**
    - **Quatre (4) ordinateurs personnels (deux (2) câblés, deux (2) sans fil)**
2. Utiliser la méthode VLSM (**Variable Length Subnet Masking**) pour effectuer le sous-réseautage
3. Configurer l'**attribution d'adresses IP à la fois statiques et DHCP**
4. Activer la **sécurité du réseau sans fil (WPA2)** pour les clients sans fil
5. Diagnostiquer la cause **d'un problème réseau** (p. ex., IP incorrecte ou un manque d'accès à Internet)
6. Créer un **diagramme de votre réseau** et expliquer chaque étape de la configuration

Critères d'évaluation :

- **Topologie réseau et sous-réseautage VLSM** adéquats (5 points)
- **Attribution d'adresses IP (statiques et DHCP)** (5 points)
- Configuration adéquate de la **sécurité du réseau sans fil** (5 points)
- **Dépannage réseau** efficace (5 points)
- **Diagramme réseau** et **documentation** clairs (10 points)

Tâche 4 : Cybersécurité et renforcement du système (20 points)

But : Appliquer des pratiques exemplaires en matière de cybersécurité et identifier les vulnérabilités.

Consignes :

1. Sur un **serveur Windows**, configurer la **Politique de groupe** pour :
    - établir des **politiques d'authentification** (longueur minimale, expiration, complexité des mots de passe)
    - restreindre **l'accès aux clés USB** pour renforcer la sécurité
2. Sur un **serveur Linux**, configurer :
    - **l'authentification par clé selon le protocole SSH** pour la connexion à distance
    - les **règles SUDO** pour l'accès Administrateur
3. Identifier **deux cybermenaces courantes** et suggérer des stratégies d'atténuation
4. Effectuer un **contrôle de sécurité** (Windows Defender ou Linux ClamAV) et signaler les résultats obtenus

Critères d'évaluation :

- **Configuration** adéquate **de la Politique de groupe** (5 points)
- **Accès** sécurisé **SSH et SUDO sur Linux** (5 points)
- Explication des **cybermenaces identifiées et des solutions proposées** (5 points)
- Résultats et analyse du contrôle de sécurité (5 points)

Tâche 5 : Rapport final et réflexion (10 points)

But : Résumer l'ensemble des tâches, fournir des captures d'écran et des détails de configuration, et présenter les leçons apprises.

Consignes :

1. Compiler un rapport résumant les :
    - **mesures prises** pour chaque tâche réalisée
    - **défis rencontrés** et les solutions mises en œuvre pour les résoudre
    - **pratiques exemplaires** pour les TI - administration de réseau
2. Inclure des **captures d'écran et des commandes de configuration**
3. Expliquer les **principaux points à retenir** de l'exercice

Critères d'évaluation :

- **Documentation** bien structurée (5 points)
- **Réflexion approfondie et pratiques exemplaires** bien expliquées (5 points)

Cours recommandés pour la préparation (auto-apprentissage) :

1. **Introduction à la cybersécurité**
   Pourquoi? Connaissances fondamentales de la cybersécurité, essentielles pour sécuriser les systèmes réseau.
   Thèmes importants à explorer :
   - *Comprendre les cybermenaces, notamment les logiciels malveillants et l'hameçonnage*
   - *Mettre en place des mesures de sécurité et des pratiques exemplaires*
   - *Explorer les perspectives de carrière en cybersécurité*

   Lien : Introduction à la cybersécurité

2. **Principes de base du réseautage**
   Pourquoi? Couvre les notions de base du réseautage, essentiels pour la conception et l'administration réseau.
   Thèmes importants à explorer :
   - *Comprendre le fonctionnement des réseaux*
   - *Explorer les différentes topologies et les périphériques réseau*
   - *Maîtriser les bases de l'adressage IP et du sous-réseautage*

   Lien : Notions de base sur les réseaux

3. **Introduction à l'IdO et la transformation numérique**
   Pourquoi? Présente l'Internet des objets (IdO) et son impact sur le réseautage et la transformation numérique.
   Thèmes importants à explorer :
   - *Comprendre les concepts et les applications de l'IdO*
   - *Explorer le rôle de l'IdO dans la transformation numérique*
   - *Découvrir les enjeux et bonnes pratiques de sécurité liés à l'IdO*

   Lien : Introduction à l'IoT (IdO) et à la transformation digitale

4. **Principes de base du matériel informatique**
   Pourquoi? Fournit des connaissances essentielles sur le matériel informatique, important pour la configuration du système et la recherche de la cause d'une panne.
   Thèmes importants à explorer :
   - Identifier les composants informatiques et leurs fonctions
   - Comprendre l'installation et l'entretien du matériel informatique
   - Développer des compétences en dépannage des problèmes informatiques courants

   Lien : Les bases du matériel informatique

5. **Principes de base des systèmes d'exploitation**
   Pourquoi? Couvre les concepts fondamentaux des systèmes d'exploitation, nécessaires pour l'administration et la configuration des systèmes.
   Thèmes importants à explorer :
   - *Comprendre les différents systèmes d'exploitation*
   - *Apprendre l'installation et la configuration d'un système d'exploitation*
   - *Gérer les ressources du système et renforcer sa sécurité*

   Lien : Operating Systems Basics (disponible en anglais seulement)