Guide du participant CCENT 5

Section 9.5 Dépannage des couches 4 et supérieures

Cette section consacrée au dépannage vous permettra d'étudier les conditions nécessaires à l'obtention d'une certification CCENT. En effet, il convient de réussir l'examen ICND1 640-822. Ces guides d'étude vous proposent une méthode qui vous aidera à organiser vos révisions en fonction des objectifs de l'examen ICND1.

Protocoles et services réseaux

Objectif : décrire les applications réseau courantes, notamment les applications Web

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Services réseaux : ce chapitre décrit les applications réseau client/serveur courantes. Il indique le protocole utilisé, le port affecté à l'application, ainsi que les informations sur les fonctionnalités client de chaque application réseau. Veillez à mémoriser le port TCP ou UDP affecté par défaut à chaque application. En effet, il est important pour le dépannage et la création de listes de filtre de pare-feu.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Services des fournisseurs de services Internet : la section Services et protocoles traite des différents services de la couche application offerts par les fournisseurs de services Internet. Elle contient également des informations sur les divers protocoles utilisés pour délivrer ces services. Cette section est plus détaillée que celle traitant du fonctionnement des services FTP et de messagerie dans CCNA Discovery : Réseaux domestiques et pour petites entreprises.

Responsabilités des fournisseurs de services Internet : la rubrique ***Chiffrement des données*** décrit les méthodes de sécurisation des protocoles courants de la couche application.

Objectif : résolution des problèmes de fonctionnement du système DNS

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Services réseaux : la rubrique ***Service de noms de domaine (DNS)*** décrit le fonctionnement du système de noms de domaine. Lorsque la résolution DNS d'un nom de domaine ou d'une URL échoue, aucune communication ne peut être établie. Examinez attentivement les conditions requises permettant la résolution d'un nom : 1. Une adresse de serveur DNS correcte doit être configurée pour l'hôte, manuellement ou via le protocole DHCP. 2. Le serveur DNS doit être accessible à partir de l'hôte. 3. Le serveur DNS doit être configuré pour résoudre le nom de l'hôte de destination spécifique via une adresse IP valide. Exercez-vous à utiliser la commande nslookup pour vérifier que le système DNS fonctionne correctement sur le réseau.

Dépannage de votre réseau : la rubrique ***Dépannage à l'aide de la commande nslookup*** décrit l'interprétation du résultat de la commande nslookup sur un ordinateur Windows.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Services des fournisseurs de services Internet : la section ***Système de noms de domaine*** fournit des informations détaillées sur la structure d'un système DNS, ainsi que sur les différents composants devant fonctionner correctement pour que la résolution d'un nom réussisse. Si le système DNS échoue, toutes les applications destinées à l'utilisateur final et qui s'appuient sur la résolution du nom échouent également. Il est important de toujours vérifier la disponibilité et le bon fonctionnement du système DNS lorsque les utilisateurs signalent l'échec de plusieurs applications réseau.

Objectif : décrire l'impact des applications (voix sur IP et vidéo sur IP) sur un réseau

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Services réseaux : dans la section ***Clients, serveurs et leur interaction***, la rubrique ***Protocoles de transport TCP et UDP*** explique pourquoi il est préférable de ne pas choisir le protocole TCP pour la transmission du trafic vocal et vidéo sur le réseau. La rubrique ***Clients et serveurs vocaux*** décrit les fonctionnalités de la téléphonie IP sur Internet.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Services des fournisseurs de services Internet : à la section ***Protocoles prenant en charge les services des fournisseurs de services Internet***, la rubrique ***Protocoles de la couche transport*** décrit les différentes caractéristiques des protocoles TCP et UDP.

Exercices pratiques :

1. Créez un tableau récapitulant toutes les applications Internet et réseau courantes. Pour chaque application, identifiez le protocole, le port affecté par défaut et si l'application utilise le protocole TCP ou UDP. Dans certains cas, comme pour la voix ou la vidéo, il se peut que le port ne soit pas connu.

   Exemple :

Application	Protocole de l'application	Port	Protocole de transport
Navigateur Web	http	80	TCP
Recherche des noms de domaine	DNS	53	TCP et UDP

2. Identifiez toutes les applications clientes installées sur votre ordinateur. Déterminez le type de serveur auquel chacune d'entre elles se connecte pour recevoir les informations.
3. Utilisez la commande netstat pour afficher le nombre de connexions TCP initialisées lorsque vous affichez une page Web ou envoyez un courriel.

Pratiques et périphériques liés à la sécurité réseau

Objectif : expliquer les menaces croissantes aujourd'hui en matière de sécurité réseau et la nécessité de mettre en place une stratégie de sécurité complète

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Sécurité de base : les trois premières sections de ce chapitre décrivent les menaces, les méthodes d'attaque et les exigences en matière de stratégie de sécurité pour les réseaux des particuliers et des petites entreprises. La rubrique ***Mesures de sécurité courantes*** explique pourquoi une stratégie de sécurité complète est nécessaire et décrit son contenu. N'oubliez pas de réviser le contenu du graphique interactif associé à cette rubrique.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Responsabilités des fournisseurs de services Internet : la rubrique ***Listes de contrôle d'accès et filtrage de port*** décrit les attaques par déni de service. La rubrique ***Sécurité de l'hôte*** illustre les mesures à entreprendre pour minimiser les menaces sur les périphériques hôtes.

Objectif : expliquer les méthodes générales de minimisation des menaces de sécurité courantes dans les périphériques, les hôtes et les applications réseau

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Sécurité de base : la section ***Stratégie de sécurité*** de ce chapitre décrit les mesures de sécurité recommandées pour empêcher toute attaque indésirable ou malveillante d'atteindre les hôtes ou le réseau. Examinez attentivement le type de mesure préventive s'adressant au type d'attaque.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Responsabilités des fournisseurs de services Internet : la première section de ce chapitre, ***Considérations sur la sécurité des fournisseurs de services Internet***, met l'accent sur les meilleures pratiques et les problèmes de sécurité courants rencontrés par les fournisseurs de services Internet et leurs clients.

Objectif : décrire les fonctions des équipements et des applications de sécurité courants

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Sécurité de base : la section ***Utilisation de pare-feu*** décrit les pare-feu et le filtrage de port. Elle répertorie les différentes méthodes utilisées par les pare-feu pour autoriser ou refuser le trafic. L'animation de la rubrique ***Utilisation d'un pare-feu*** illustre le concept des différentes zones de sécurité. Cette rubrique inclut également des travaux pratiques, qui permettent de mettre en pratique la configuration des paramètres de pare-feu.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Responsabilités des fournisseurs de services Internet : la section ***Outils de sécurité*** décrit les différents types de technologies de sécurité utilisées sur les réseaux, ainsi que les types de menaces contre lesquelles elles protègent le système. Garantir la sécurité d'un réseau est l'une des tâches les plus importantes d'un technicien réseau ou d'un ingénieur. Assurez-vous de comprendre la fonction de chaque type de mesure de sécurité en détail. La rubrique ***Sécurité des réseaux sans fil*** décrit les types de mesures de sécurité nécessaires pour sécuriser des réseaux locaux sans fil.

Objectif : décrire les pratiques recommandées en matière de sécurité, y compris les étapes initiales de sécurisation des périphériques réseau

Chapitres de révision CCNA Discovery : Réseaux domestiques et pour petites entreprises :

Technologies sans fil : la section ***Considérations sur la sécurité d'un réseau local sans fil*** contient des informations sur la sécurisation d'un point d'accès sans fil.

Chapitres de révision CCNA Discovery : Travailler dans une PME ou chez un fournisseur de services Internet :

Configuration des périphériques réseau : la rubrique ***Configuration de base***, dans la section ***Configuration d'un routeur à l'aide de l'interface de ligne de commande IOS***, décrit la définition des mots de passe pour accéder aux modes utilisateur et privilégié. Elle inclut également les commandes permettant d'autoriser l'accès Telnet au périphérique et de définir le mot de passe de connexion d'accès VTY (Telnet). Il est recommandé de chiffrer tous les mots de passe sur un périphérique à l'aide de la fonction service password-encryption. Les commandes permettant de définir les mots de passe et les bannières sont les mêmes sur un commutateur Cisco et sur le routeur ISR. La rubrique ***Connexion du commutateur de réseau local au routeur*** présente les mesures de sécurité supplémentaires à mettre en œuvre sur un commutateur.

Exercices pratiques :

1. Créez une liste de contrôle à respecter pour définir la sécurité de base sur chaque périphérique réseau important : routeur, commutateur, point d'accès sans fil intégré. Mettez en pratique la configuration de la sécurité de base sur chaque périphérique.
2. Créez un graphique de chaque technologie de sécurité réseau importante : pare-feu, listes d'accès, IPS, IDS, services de connexion, méthodes d'authentification, d'autorisation et de chiffrement. Décrivez la fonction de chaque technologie, ainsi que les menaces contre lesquelles elle protège le système. Indiquez les technologies basées sur un hôte et celles implémentées sur les périphériques réseau ou sur un équipement réseau.

Exemple :

Technologie de sécurité	Fonction	Protection contre les menaces	Basée sur un hôte	Basée sur le réseau
Listes d'accès	Filtre le trafic basé sur l'adresse ou le port source ou de destination.	Bloque le trafic indésirable sur un réseau ou dans un processus hôte.	Oui	Oui
Protection antivirus	Identifie tout logiciel malveillant par modèle de trafic ou contenu de fichier.	Empêche tout logiciel malveillant d'endommager les fichiers hôtes ou de créer un trafic réseau excédentaire.	Oui	Non

3. Répertoriez les rubriques à inclure dans une stratégie de sécurité.
4. Répertoriez les meilleures pratiques de sécurisation des réseaux et des hôtes.