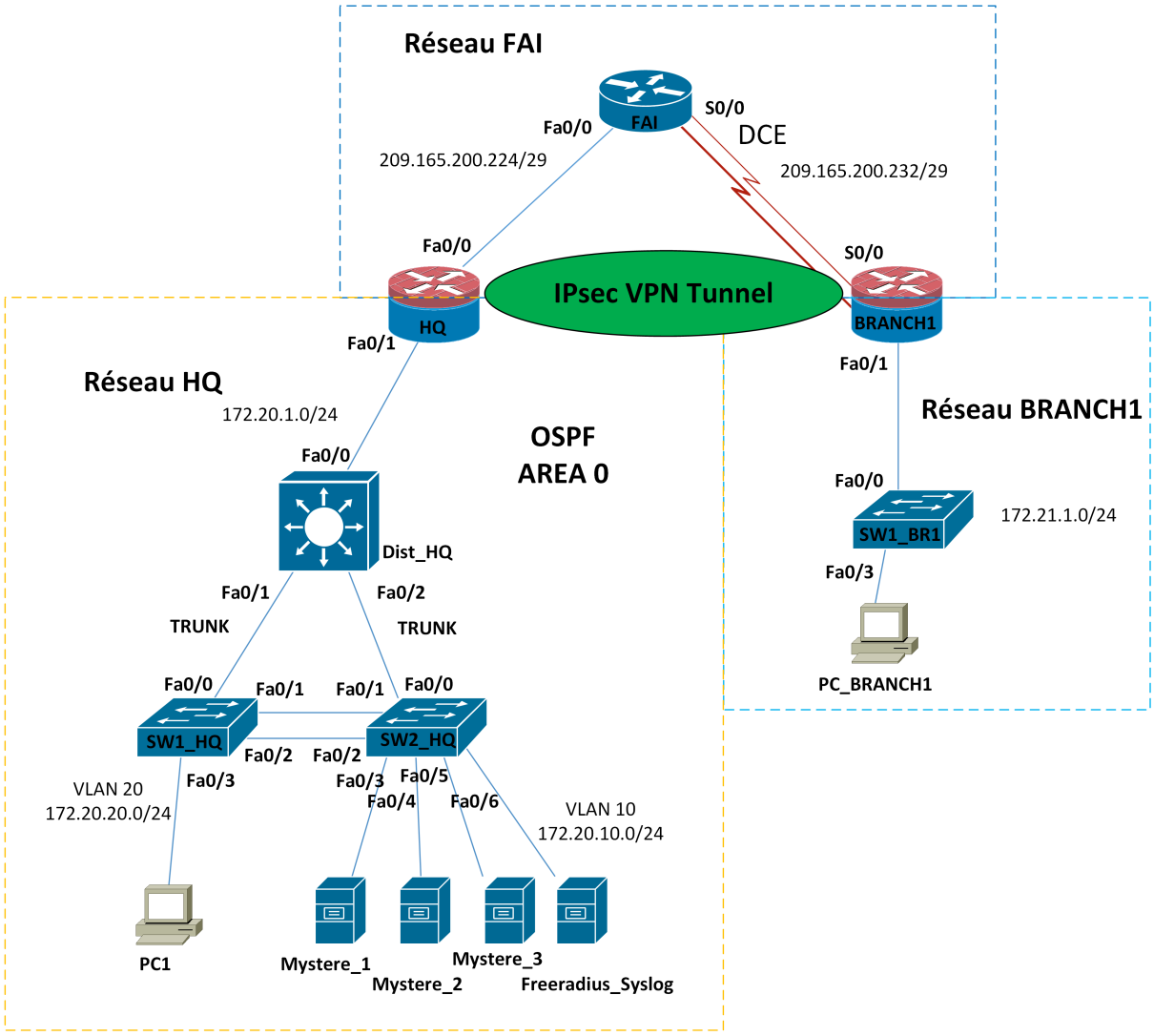
Étude de cas – 420-F52-SF

Topologie



- L'étude de cas se fait en équipe de 2 à 3 membres.

Table d'adressage IP

Noeud	Interface/ VLAN	Adresse IP	Passerelle	Nom VLAN
FAI	Fa0/0	209.165.200.225/29	N/A	N/A
	s0/0	209.165.200.233/29	N/A	N/A
HQ	Fa0/0	209.165.200.226/29	N/A	N/A
	Fa0/1	172.20.1.1/24	N/A	N/A
BRANCH1	s0/0	209.165.200.234/29	N/A	N/A
	Fa0/1	172.21.1.1/24	N/A	N/A
Dist_HQ	Fa0/0	172.20.1.2/24	N/A	N/A
	VLAN 10	172.20.10.1/24	N/A	SERVERS
	VLAN 20	172.20.20.1/24	N/A	USERS
	VLAN 200	172.20.200.1/24	N/A	MGMT
	VLAN 666			NATIF
	VLAN 999			BLACK_HOLE
SW1_HQ	VLAN 200	172.20.200.6/24	172.20.200.1	N/A
SW2_HQ	VLAN 200	172.20.200.7/24	172.20.200.1	N/A
SW1_BR1	VLAN 21	172.21.1.6/24	172.21.1.1	BRANCH1
PC1	NIC	?.?.?.?	172.20.20.1	N/A
Mystere_1	NIC	?.?.?.?	172.20.10.1	N/A
Mystere_2	NIC	?.?.?.?	172.20.10.1	N/A
Mystere_3	NIC	?.?.?.?	172.20.10.1	N/A
Freeradius_Syslog	NIC	172.20.10.205/24	172.20.10.1	N/A
PC_BRANCH1	NIC	DHCP	172.21.1.1	N/A

Objectifs

Partie 1 : Monter le réseau et faire une configuration de base (15 points)

Partie 2 : Sécuriser les appareils réseau (25 points)

- Configuration des mots de passe sécurisés et d'une bannière de login.
- Configuration de la sécurité pour les connexions de console et VTY : timeout, login infructueux, SSH, authentification AAA locale.
- Configuration d'ACLs et d'un mur par feu par zone (ZPF).

Partie 3 : Configurer un VPN Site-À-Site (15 points)

Partie 4 : Sécuriser les commutateurs (20 points)

- Configuration des mots de passe sécurisés et d'une bannière de login.
- Configurer un VLAN de gestion, ainsi que sa sécurité.

- Sécuriser les ports trunk et les ports d'accès.
- Appliquer une protection pour les attaques au STP.
- Configurer la sécurité des ports et désactiver les ports inutilisés.
- Configurer le DHCP Snooping.

Partie 5 : Pentesting (15 points)

- Intégration des VM mystères et PC1.
- Découverte du réseau.
- Vérification de vulnérabilités et tentatives d'exploiter des vulnérabilités découvertes.
- Extraction de mots de passe.

Partie 6 (défi) : Configuration de syslog et AAA centralisé (+10 points)

- Configuration d'un serveur syslog
- Configuration de AAA avec freeradius.

Partie 7 : Rapport final (10 points)

Note : Assurez-vous que tous les appareils réseau ont été réinitialisés avant de débuter.

Besoin matériel

- 2 routeurs possédant l'IOS Advanced IP Service ou comparable
- 1 routeur possédant Cisco IOS Release 15.4.3M5
- 3 commutateurs
- 3 VMs Serveurs mystères fournis par l'enseignant
- 1 VM PC1 fournit par l'enseignant
- 1 VM serveur freeradius / syslog
- 1 (ou plus) VM Kali Linux

Scénario

Cette étude de cas va vous permettre de compléter l'évaluation de la compétence FZ08 "Assurer la sécurité du réseau". Les compétences FZ03 "Analyser l'architecture d'un réseau" et FZ05, "Réaliser une étude d'implantation d'un réseau informatique" seront également partiellement évaluées. L'étude de cas est divisée en 7 parties dont une partie est un défi à réaliser. Même si cette étude de cas est réalisée en équipe, chaque étudiant doit se mettre responsable de certains éléments : routeurs, commutateurs, serveur, au moins une VM à hacker.

Partie 1 : Monter le réseau et faire une configuration de base

Dans cette partie, vous allez monter la topologie et faire une configuration de base sur les routeurs et les commutateurs. Suivre les étapes indiquées ci-dessous.

Étape 1 : Câblez le réseau comme dans la topologie. (1 point)

a. Câblez le réseau en respectant les ports entre les appareils réseau. L'ajout des postes se fera plus loin. Ajustez le type de ports selon vos appareils : Ehternet, FastEthernet ou GigaEthernet.

Routeurs

Étape 2 : Configuration de base sur tous les routeurs. (1 point)

a. Configurez le nom d'hôte tel que démontré dans la topologie.

b. Configurez les adresses IP des interfaces selon la table d'adressage IP (ne pas oublier les descriptions).

c. Désactivez le DNS lookup.

d. Configurez un mot de passe **`enable`**. Utilisez le mot de passe **ciscoenapa55.**

Étape 3 : Sauvegardez la configuration de chacun des routeurs.

Commutateurs

Étape 4 : Configuration de base sur les commutateurs. (1 point)

a. Configurez le nom d'hôte comme démontré dans la topologie.

b. Désactivez le DNS lookup.

c. Configurez un mot de passe **`enable`**. Utilisez le mot de passe **ciscoenapa55.**

Étape 5 : Configuration des VLANs et des adresses IP des commutateurs. (2 points)

a. Configurer le VLAN 999 sur tous les commutateurs.

b. Configurez les VLANs 10, 20, 200 et 666 sur chacun les commutateurs du réseau HQ.

c. Configurer le VLAN 21 sur le commutateur SW1_BR1.

d. Configurez les adresses IP des interfaces VLANs et Fa0/0 de Dist_HQ selon la table d'adressage IP (ne pas oublier les descriptions).

e. Sur le commutateur d'accès SW1_HQ, configurez au moins 4 ports de votre choix pour le VLANs 20 et au moins 4 ports de votre choix pour le VLANs 200.

f. Sur le commutateur d'accès SW2_HQ, configurez au moins 4 ports de votre choix pour le VLANs 10 et au moins 1 port de votre choix pour le VLANs 200.

g. Mettre le port Fa0/0 du commutateur SW1_BR1 dans le VLAN 21.

h. Sur le commutateur d'accès SW1_BR1, configurez au moins 4 ports de votre choix pour le VLAN 21.

Étape 6 : Configuration des Trunks et des Etherchannels dans le réseau HQ. (2 points)

a. Dans le réseau HQ, configurez des Trunks entre les commutateurs d'accès et le commutateur de distribution selon le schéma de la topologie.

b. Configurez un Trunk - Etherchannel entre les commutateurs d'accès selon le schéma de la topologie.

Routage

Étape 7 : Configuration du routage. (2 points)

a. Configurez des routes statiques résumées du FAI vers HQ et BRANCH1.

b. Configurez une route statique par défaut de HQ et BRANCH1 vers le FAI.

c. Configurez OSPFv2 sur le réseau HQ **seulement** tel que démontré dans la topologie. Propagez la route par défaut dans OSPFv2.

Étape 8 : Sauvegardez la configuration de chacun des appareils réseau et vérification. (2 points)

a. Assurez-vous de sauvegarder la configuration de vos appareils réseau : localement et de secours.

b. Vérifiez le routage, la configuration des VLANs, les Trunks et les EtherChannels.

c. Vérifiez la connectivité entre les appareils réseau, entre des postes à l'intérieur du même réseau, vers le FAI et entre HQ et BRANCH1.

DHCP

Étape 9 : Configuration du DHCP pour HQ. (2 points)

a. Configurez un serveur DHCP sur le commutateur Dist_HQ pour les VLANs MGMT et USERS.

b. Allouez les adresses 50 à 99 pour chacun des réseaux.

c. Configurez le nom de domaine **acme.hq**.

d. Configurez le serveur DNS à l'adresse 172.20.10.221.

e. Vérifiez qu'un poste reçoit une adresse IP.

f. Configurez un relais DHCP pour l'adresse 172.20.10.221

Étape 10 : Configuration du DHCP pour BRANCH1. (2 points)

a. Configurez un serveur DHCP sur le routeur BRANCH1 pour le VLAN BRANCH1.

b. Exclure les 25 premières adresses.

c. Configurez le nom de domaine **acme.hq**.

d. Configurez le serveur DNS à l'adresse 172.20.10.221.

e. Vérifiez qu'un poste reçoit une adresse IP.

Vérification 1 par l'enseignant

Partie 2 : Sécuriser les appareils réseau

Dans cette partie, vous allez vous assurer que les appareils possèdent la version la plus récente d'IOS, vous allez configurer l'accès sécuritaire aux routeurs et commutateurs, sécuriser les mots de passe, sécurisé le protocole routage, activer le mur par feu… Suivre les étapes indiquées ci-dessous.

Tâche 1 : S'assurer d'avoir la version la plus récente d'IOS.

Étape 1 : installer la version d'IOS la plus récente. (1 point)

a. Vérifiez sur chacun des appareils réseau que vous avez la version d'IOS la plus récente.

b. Si vous n'avez pas la version d'IOS la plus récente, demandez-la à votre enseignant.

Tâche 2 : Configuration des mots de passe et de la bannière d'accueil.

Étape 1 : Sur tous les appareils réseau le permettant, configurez la longueur minimum des mots de passe à 10 caractères. (1 point)

Étape 2 : Configurez un mot de passe enable secret plus sécuritaire. (0,5 point)

a. À partir de l'IOS 15.3(3)M il est possible de modifier l'algorithme de hashage du mot de passe **`enable secret`** à un algorithme plus sécuritaire.

Pour les appareils ayant cette fonctionnalité, modifiez l'algorithme de hashage du mot de passe **`enable secret`** à **scrypt**.

Étape 3 : Chiffrez les mots de passe en texte clair. (0,5 point)

Étape 4 : Configurez les lignes console et les lignes VTY. (1 point)

a. Configurez le mot de passe console **ciscoconpa55** et activez le login.

b. Ajustez le exec-timeout pour débrancher après 5 minutes d'inactivées.

c. S'assurer que les messages de console ne nuisent pas aux entrées de commandes en lien console.

d. Configurez le mot de passe vty **ciscovtypa55** et activez le login. Ajustez le exec-timeout pour débrancher après 5 minutes d'inactivées.

Étape 5 : Configurez une bannière d'accueil sur les appareils réseau. (1 point)

a. Configurez la bannière « message-of-the-day (MOTD) » avec la phrase suivante : "Unauthorized access strictly prohibited and prosecuted to the full extent of the law!".

Étape 6 : Désactivez les accès HTTP. (1 point)

a. Sur un commutateur l'accès HTTP est actif par défaut. Désactivez le serveur HTTP et le serveur HTTP sécurisé.

b. Si le service est actif sur les routeurs, le désactiver également.

Étape 7 : Authentification du protocole de routage. (1 point)

a. Configurez l'authentification du protocole de routage OSPFv2 dans le réseau HQ en utilisant l'algorithme le plus sécuritaire disponible.

Tâche 3 : Sécurisation des lignes d'accès virtuel.

Étape 1 : Configurez les lignes d'accès virtuel vty. (2 points)

a. Configurez une liste d'accès pour que seulement les PCs du VLAN MGMT puissent accéder aux appareils réseau de HQ et BRANCH1 en ligne VTY.

b. Configurez une liste d'accès sur le routeur FAI pour que seulement les PCs du VLAN MGMT puisse y accéder en ligne VTY.

Tâche 4 : Configuration d'une authentification locale à l'aide d'AAA.

Étape 1 : Configurez des utilisateurs locaux sur les appareils réseau de HQ et BRANCH1. (1 point)

a. Créez un compte d'utilisateur **Admin01** avec le mot de passe secret de **Admin01pa55** et ayant un niveau de privilège 15.

b. Vous pouvez vous configurer d'autres comptes si vous le désirez.

Étape 2 : Activez le service AAA. (1 point)

Étape 3 : Implantez le service AAA en utilisant la base de données locale. (2 points)

a. Le login d'authentification par défaut doit utiliser l'authentification locale (en prenant compte de la casse) en premier et le mot de passe enable en redondance.

b. Les autorisations pour le CLI utilisent la base de données locale et seulement si l'utilisateur est authentifié.

c. Lorsqu'un utilisateur ayant un privilège 15 établit une connexion console, il doit arriver en mode privilégié.

d. Pour tester, quittez la session console jusqu'à l'affichage : **RX con0 is now available, Press RETURN to get started**.

e. Établir une connexion console au routeur avec l'utilisateur **Admin01** et le mot de passe **Admin01pa55.** Ceci va permettre de vérifier que l'authentification locale fonctionne.

f. Quitter une autre fois la session console jusqu'à l'affichage : **RX con0 is now available, Press RETURN to get started**.

g. Essayer une connexion console avec l'utilisateur **baduser** et un mot de passe quelconque.

Tâche 5 : Configuration du service SSH sur les appareils réseau de HQ et BRANCH1.

Étape 1 : Configurez le nom de domaine acme.hq sur les appareils réseau. (1 point)

Étape 2 : Configurez les lignes VTY. (1 point)

a. Spécifiez que les lignes VTY n'acceptent que les connexions SSH.

b. Assurez-vous que les lignes VTY permettent qu'un utilisateur ayant un niveau de privilège 15 entre immédiatement en mode EXEC privilégié. Tous les autres utilisateurs entrent en mode utilisateur.

Étape 3 : Générez la clé de chiffrement RSA. (1 point)

a. Configurez la clé RSA avec un modulo de 1024 bites.

b. Assurez-vous d'avoir la version 2 de SSH

Étape 4 : À partir de PC dans le VLAN MGMT, vérifiez la connexion SSH. (1 point)

a. Utilisez le compte **Admin01** avec le mot de passe **Admin01pa55**.

Tâche 6 : Sécuriser les appareils réseau de HQ et BRANCH1 contre les attaques de login.

Étape 1 : Configurez les paramètres suivants. (1 point)

- Période de blocage quand une attaque de login est détectée : 60
- Le manque maximum d'essai de login infructueux : 2
- Le temps entre le nombre de login infructueux : 30
- Gardez une trace (log) des essais de login infructueux

Étape 2 : Configurez NTP. (2 points)

a. Configurez l'heure et la date sur le routeur HQ. Ne pas oublier l'ajustement aux changements d'heure.

b. Configurez le routeur HQ comme serveur NTP maître avec un startum de 5.

c. Le routeur BRANCH1 et le commutateur Dist_HQ se connectent sur HQ :
- Clé d'authentification : **NTPpassword**.
- Chiffrement : **MD5**.
- Clé : **1**.
- Ne pas oublier l'ajustement aux changements d'heure.

d. Les commutateurs d'accès de HQ reçoivent l'heure en diffusion (broadcast) de Dist_HQ.

e. Le commutateur d'accès de BRANCH1 reçoit l'heure de BRANCH1

Étape 3 : Configurez la journalisation Syslog. (1 point)

a. Configurez le service syslog sur les appareils réseau de HQ et BRANCH1.

b. Activez le timestamp de date et d'heure en millisecondes.

c. Envoyez les log au serveur Freeradius_Syslog.

d. Ajustez la sévérité de journalisation à **Warning**.

Étape 4 : Sauvegardez la configuration dynamique dans la configuration de démarrage.

Tâche 7 : Configuration d'un mur par feu par zone (ZPF) sur les routeurs HQ et BRANCH1.

Étape 1 : Vérification de la connectivité.

a. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du routeur HQ.
Résultat : _____

b. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du commutateur Dist_HQ.
Résultat : _____

c. À partir d'un PC de HQ, **pigner** l'interface s0/0 du routeur BRANCH1.
Résultat : _____

d. À partir d'un PC de HQ, **pigner** un PC dans le réseau de BRANCH1.
Résultat : _____

e. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur HQ. La session devrait aboutir.

f. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur BRANCH1. La session devrait aboutir.

g. À partir d'un PC du VLAN MGMT, établir une session **Telnet** à FAI. La session devrait aboutir.

Étape 2 : Configurez le ZPF sur le routeur HQ. (2 points)

a. Configurez un ZPF sur HQ avec les informations suivantes :

Configuration	Spécification
Créer le nom des zones.	Nom de la zone inside : **INSIDE** Nom de la zone outside : **FAI**

Créer une inspect class map.	Nom Class map : **INSIDE_PROTOCOLS** Type d'inspection : **match-any** Protocoles permits : **tcp, udp, icmp**
Créer une inspect policy map.	Nom Policy map : **INSIDE_TO_FAI** Lier la class map à la policy map.
Créer une zone pair.	Nom Zone pair : **IN_TO_OUT_ZONE** Zone source : **INSIDE** Zone destination : **FAI**
Appliquer la policy map à la zone pair.	Nom Zone pair : **IN_TO_OUT_ZONE** Nom Policy map : **INSIDE_TO_FAI**
Assigner les interfaces aux zones de sécurités.	Interface Fa0/1 : **INSIDE** Interface Fa0/0 : **FAI**

Étape 3 : Vérification la fonctionnalité du ZPF.

a. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du routeur HQ.
Résultat : _____

b. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du commutateur Dist_HQ.
Résultat : _____

c. À partir d'un PC de HQ, **pigner** l'interface s0/0 du routeur BRANCH1.
Résultat : _____

d. À partir d'un PC de HQ, **pigner** un PC dans le réseau de BRANCH1.
Résultat : _____

e. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur HQ. La session devrait aboutir.

f. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur BRANCH1. La session devrait aboutir.

g. À partir d'un PC du VLAN MGMT, établir une session **Telnet** à FAI. La session devrait aboutir**.**

Étape 4 : Configurez le ZPF sur le routeur BRANCH1. (1 point)

a. Configurez un ZPF sur BRANCH1 avec la même configuration que HQ. N'oubliez pas d'ajuster l'interface outside (FAI) à s0/0.

Étape 5 : Vérification la fonctionnalité du ZPF. (1 point)

a. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du routeur HQ.
Résultat : _____

b. À partir d'un PC de BRANCH1, **pigner** l'interface Fa0/0 du commutateur Dist_HQ.
Résultat : _____

c. À partir d'un PC de HQ, **pigner** l'interface s0/0 du routeur BRANCH1.
Résultat : _____

d. À partir d'un PC de HQ, **pigner** un PC dans le réseau de BRANCH1.
Résultat : _____

e. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur HQ. La session devrait aboutir.

f. À partir d'un PC du VLAN MGMT, établir une session **SSH** au routeur BRANCH1. La session devrait aboutir.

g. À partir d'un PC du VLAN MGMT, établir une session **Telnet** à FAI. La session devrait aboutir.

Étape 6 : Sur votre routeur, sauvegardez la configuration dynamique dans la configuration de démarrage.

Vérification 2 par l'enseignant

Partie 3 : Configuration d'un VPN Site-à-Site entre HQ et BRANCH1

Dans cette partie, vous allez configurer un tunnel IPsec entre les routeurs HQ et BRANCH1. Je vous recommande de désactiver votre mur par feu (enlever vos interfaces dans les zones) le temps de faire fonctionner votre VPN. Quand le VPN fonctionnera, faites les modifications à votre ZPF et le réappliquer après. Vous devez savoir que pour le ZPF de HQ, le réseau BRANCH est un réseau extérieur et vice versa.

Tâche 1 : Configuration d'un VPN Site-à-Site entre HQ et BRANCH1.

Étape 1 : Configurez la connexion VPN sur BRANCH1. (5 points)

a. Configurez la connexion VPN sur BRANCH1 avec les informations suivantes :

Configuration	Spécification
Activez l'IKE.	Note: ISAKMP est actif par défaut.
Créez une politique ISAKMP.	Politique de la priorité ISAKMP : **1** Type d'authentification : **pre-share** Chiffrement : **aes 256** Algorithme Hash : **sha** Diffie-Hellman Group Key Exchange : **2**
Configurez la clé pre-shared.	Preshare key : **ciscopreshare** Adresse : **209.165.200.226**
Configurez l'IPsec transform set.	Tag: **TRNSFRM-SET** ESP transform: **ESP_AES 256** Hash function: **ESP_SHA_HMAC**
Définir le trafic intéressant.	ACL: **101** Réseau source : **172.21.0.0 0.0.255.255** Réseau destination : **172.20.0.0 0.0.255.255**
Créez une crypto map.	Nom Crypto map : **CMAP** Numéro de séquence : **1** Type: **ipsec-isakmp** ACL: **101** Peer: **209.165.200.226** Transform-set: **TRNSFRM-SET**
Appliquez la crypto map à l'interface.	Interface: **s0/0** Crypto map name: **CMAP**

Étape 2 : Configurez la connexion VPN sur HQ. (5 points)

a. Configurez la connexion VPN sur HQ avec les informations suivantes :

Configuration	Spécification
Activez l'IKE.	Note: ISAKMP est actif par défaut.
Créez une politique ISAKMP.	Politique de la priorité ISAKMP : **1** Type d'authentification : **pre-share** Chiffrement : **aes 256** Algorithme Hash : **sha** Diffie-Hellman Group Key Exchange : **2**
Configurez la clé pre-shared.	Preshare key : **ciscopreshare** Adresse : **209.165.200.234**
Configurez l'IPsec transform set.	Tag: **TRNSFRM-SET** ESP transform: **ESP_AES 256** Hash function: **ESP_SHA_HMAC**
Définir le trafic intéressant.	ACL: **101** Réseau source : **172.20.0.0 0.0.255.255** Réseau destination : **172.21.0.0 0.0.255.255**
Créez une crypto map.	Nom Crypto map : **CMAP** Numéro de séquence : **1** Type: **ipsec-isakmp** ACL: **101** Peer: **209.165.200.234** Transform-set: **TRNSFRM-SET**
Appliquez la crypto map à l'interface.	Interface: **Fa0/0** Crypto map name: **CMAP**

Étape 3 : Sauvegardez la configuration dynamique dans la configuration de démarrage.

Tâche 2 : Vérification du VPN entre HQ et BRANCH1. (5 points)

a. À partir d'un PC de BRANCH1, pigner l'interface Fa0/0 de Dist_HQ.

Note : Pour remettre à zéro (reset) le tunnel VPN et recommencer une vérification, vous pouvez utiliser la commande CLI **`clear crypto session`**. Cette commande remet également les compteurs à zéro.

b. À partir de BRANCH1, vérifier la fonctionnalité du tunnel VPN à l'aide des commandes **`show crypto isakmp sa`** et **`show crypto ipsec sa.`**

c. Démontrez que votre ZPF est actif à l'aide de la commande **`show zone security.`**

Vérification 3 par l'enseignant

Partie 4 : Sécuriser les commutateurs

Tâche 1 : Sécurisez les ports Trunk

Étape 1 : Mettre tous les commutateurs en mode VTP transparent. (1 point)

Étape 2 : Gestion des VLAN sur les ports Trunks du réseau HQ. (1 point)

a. Laissez passer seulement les VLANs nécessaires sur les Trunks.

b. Changez le VLAN natif au VLAN 666.

Étape 3 : Gestion du STP. (2 points)

a. Assurez-vous que le commutateur Dist_HQ soit le pont racine du STP.

b. Activez le root guard sur le commutateur Dist_HQ.

Étape 4 : Empêchez l'utilisation de DTP sur les ports trunk. (1 point)

Étape 5 : Vérifiez la configuration des ports trunk sur les commutateurs de HQ.

Tâche 2 : Sécurisez les ports d'accès

Étape 1 : Désactivez le trunking sur les ports d'accès. (2 points)

a. Configurez tous les ports non trunk en port d'accès seulement (access mode).

b. Empêchez l'utilisation de DTP sur les ports d'accès.

Tâche 3 : Protégez les commutateurs contre les attaques STP

Étape 1 : Activez le PortFast sur les ports d'accès des commutateurs. (2 points)

Étape 2 : Activez la prévention de BPDU (BPDU guard) sur les ports d'accès des commutateurs. (2 points)

Tâche 4 : Configurez la sécurité des ports (Port Security) et désactivez les ports non utilisés.

Étape 1 : Configurez une sécurité de base sur les ports d'accès. (3 points)

a. Désactivez tous les ports non trunk.

b. Sur les ports du VLAN SERVERS, configurez la sécurité (port security) sur ces ports pour qu'une seule adresse MAC soit permise et que le port se désactive s'il y a une violation. Configurez ces ports pour qu'ils apprennent de manière dynamique les adresses MAC et que ces adresses soient placées dans la configuration dynamique (running-config).

c. Sur les autres ports d'accès, configurez la sécurité (port security) sur ces ports pour que quatre adresses MAC soient permises et que le port se désactive s'il y a une violation.

d. Réactivez seulement les ports d'accès utilisés où la sécurité est appliquée.

Étape 2 : Gestion des ports non utilisés sur les commutateurs. (2 points)

a. Assurez-vous que les ports non utilisés soient désactivés.

b. Mettre les ports non utilisés dans le VLAN BLACK_HOLE.

Tâche 5 : Configurez du DHCP snooping.

Étape 1 : Activez le DHCP snooping. (2 points)

a. Activez le DHCP snooping globalement sur les commutateurs d'accès SW1_HQ, SW2_HQ et SW1_BR1.

b. Activez le DHCP snooping sur les VLANs USERS et BRANCH1.

Étape 2 : Configurez les ports de confiance. (2 points)

a. Mettre le port Fa0/0 des commutateurs SW1_HQ, SW2_HQ et SW1_BR1 comme des ports de confiance de DHCP snooping.

b. Mettre les ports Fa0/1 et Fa0/2 des commutateurs SW1_HQ et SW2_HQ comme des ports de confiance de DHCP snooping.

Étape 3 : Sauvegardez la configuration dynamique dans la configuration de démarrage.

Vérification 4 par l'enseignant

Partie 5 : Pentesting

Tâche 1 : Intégration des VMs mystères et Windows

Étape 1 : Copiez les VMs. (2 points)

a. Copiez les VMs Mystere_1 et Mystere_2 sur un poste de travail dans le VLAN 10.

b. Copiez la VM Mystere_3 sur un autre poste de travail dans le VLAN 10.

c. Copiez la VM PC1 sur un troisième poste de travail dans le VLAN 20.

d. Démarrez les VMs.

Étape 2 : Découverte du réseau. (3 points)

a. Trouvez les adresses IPs de tous les appareils du réseau HQ.

b. Trouvez les systèmes d'exploitation s'exécutant sur les VMs Mysteres et PC1. Déterminez le plus d'information possible : OS, version, Service Packs…

c. Découvrez le nom des nœuds : vous pouvez essayer nslookup et dig.

d. Trouvez les ports ouverts sur les VMs.

Étape 3 : Découverte des nœuds ayant les services SMB et SNMP en fonction. (2 points)

a. Balayez chacun de vos nœuds pour vérifier si les services SMB et SNMP sont en fonction.

b. Utilisez le logiciel enum4linux (https://labs.portcullis.co.uk/tools/enum4linux/) pour trouver des informations à travers le service SMB.

c. Utilisez le logiciel **snmpwalk** pour découvrir des informations sur vos nœuds (voir l'annexe 1).

d. Vous pouvez également utiliser le script perl **snmpenum.pl** disponible à l'adresse https://github.com/pwnieexpress/pwn_plug_sources/tree/master/src/snmpenum.

Étape 4 : Extraction de mots de passe. (3 points)

a. Gagnez l'accès à la VM PC1.

b. Extraire les mots de passe de cette machine (je vous conseille d'utiliser la liste de mots rockyou.txt).

Étape 5 : Vérification de vulnérabilités. (3 points)

a. Utilisez les scripts nmap pour découvrir des vulnérabilités.

b. Vous pouvez également utiliser les logiciels OpenVAS ou Nessus.

c. Vous pouvez également essayer les modules auxiliaires de Metasploit.

Étape 6 : Exploitez des vulnérabilités. (2 points)

a. Essayez d'exploiter quelques-unes des vulnérabilités découvertes pour gagner l'accès à un système.

b. Vous pouvez consulter l'annexe 2 pour vous aider avec certains nœuds vulnérables. Plusieurs machines sont vulnérables du côté applicatif, donc vous devrez lire sur les XSS, CSRF, les injections SQL, l'injection de commande… Comme, ce ne sont pas des sujets traités dans votre formation, vous ne serez pas évalué sur vos capacités à découvrir et exploiter ces vulnérabilités, mais sur votre cheminement. Surtout, essayer de vous amuser ☺.

c. Si vous modifiez les appareils (ajout d'un utilisateur, installation de logiciel, modification de fichier de configuration), n'oubliez pas de faire le ménage après et de tout remettre dans le même état qu'avant l'exploitation.

Vérification 5 par l'enseignant

Partie 6 (défi) : Configuration de syslog et AAA centralisé

Dans cette partie, vous allez configurer un serveur centralisé pour gérer l'authentification AAA et la journalisation syslog. Cette partie est en bonus, il n'est pas possible d'avoir plus de 100 % pour l'étude de cas, mais il vous est possible de récupérer des points perdus ailleurs dans l'étude de cas.

Tâche 1 : Installation d'un serveur syslog

Étape 1 : Création d'une VM serveur Linux Ubuntu. (+1 point)

a. Créez une VM serveur Linux Ubuntu.

b. Pour la mise à jour, vous devez mettre votre VM directement sur le réseau du cégep.

Étape 2 : Activez le service syslog. (+2 points)

a. Configurez le serveur syslog pour qu'il puisse recevoir les logs des appareils réseau.

b. Vérifiez que vous recevez des logs.

Tâche 2 : Installation d'un serveur AAA

Étape 1 : Installez Freeradius. (+2 points)

a. Installez Freeradius sur votre serveur Ubuntu.

Étape 2 : Ajoutez des utilisateurs locaux à Freeradius. (+1 point)

Étape 3 : Testez localement Freeradius. (+1 point)

a. Testez localement Freeradius avec un des utilisateurs créés.

Étape 4 : Testez SW2_HQ pour l'authentification avec Freeradius. (+2 points)

a. Modifiez la configuration de SW2_HQ pour l'utilisation de Freeradius pour l'authentification centralisée.

b. Testez avec un utilisateur créé sur Freeradius.

c. Si ça ne fonctionne pas, utiliser des commandes debug tel **`debug aaa authentication`**.

Étape 5 : Modifiez les autres appareils réseau de HQ pour l'authentification centralisée. (+1 point)

Vérification 6 par l'enseignant

Partie 7 : Rapport final (10 points)

Le rapport se fait en équipe, mais le nom de la personne responsable de l'élément doit être indiqué tout au long du rapport. Dans votre rapport final, vous devez inclure :

- Configurations de tous les appareils réseau : routeurs et commutateurs.
- Rapport du Pentesting :
  - Découverte des systèmes en ligne (adresses IP de tous les nœuds, s'ils sont visibles ou non).
  - Découverte des systèmes d'exploitation
  - Énumération des nœuds ayant les services SMB et SNMP en fonction
  - Énumérations des services sur chacun des nœuds
  - Liste, description et niveau de sévérité des vulnérabilités découvertes, ainsi que la méthode pour corriger la vulnérabilité.
  - Description du nettoyage fait.

Annexe 1

Utilisation de snmpwalk

#Énumère la MIB complet
snmpwalk -c public -v1 192.168.11.219

#Énumère les utilisateurs Windows
snmpwalk -c public -v1 192.168.17.203 1.3.6.1.4.1.77.1.2.25

#Énumère les processus Windows qui s'exécutent
snmpwalk -c public -v1 192.168.17.203 1.3.6.1.2.1.25.4.2.1.2

#Énumère Ports TCP ouverts
snmpwalk -c public -v1 192.168.17.203 1.3.6.1.2.1.6.13.1.3

#Énumère les logiciels installes
snmpwalk -c public -v1 192.168.17.203 1.3.6.1.2.1.25.6.3.1.2

Numéro d'entrée dans la MIB avec leur signification

#Windows

System Process	1.3.6.1.2.1.25.1.6.0
Running Programs	1.3.6.1.2.1.25.4.2.1.2
Process Path	1.3.6.1.2.1.25.4.2.1.4
Storage Units	1.3.6.1.2.1.25.2.3.1.4
Software Name	1.3.6.1.2.1.25.6.3.1.2
User Accounts	1.3.6.1.4.1.77.1.2.25
TCP Local Ports	1.3.6.1.2.1.6.13.1.3

#Linux

Linux	RUNNING PROCESSES	1.3.6.1.2.1.25.4.2.1.2
Linux	SYSTEM INFO	1.3.6.1.2.1.1.1
Linux	HOSTNAME	1.3.6.1.2.1.1.5
Linux	UPTIME	1.3.6.1.2.1.1.3
Linux	MOUNTPOINTS	1.3.6.1.2.1.25.2.3.1.3
Linux	RUNNING SOFTWARE PATHS	1.3.6.1.2.1.25.4.2.1.4
Linux	LISTENING UDP PORTS	1.3.6.1.2.1.7.5.1.2.0.0.0.0
Linux	LISTENING TCP PORTS	1.3.6.1.2.1.6.13.1.3.0.0.0.0

Utilisation de snmpenum.pl

#Énumère les informations des numéros d'entrée de la MIB contenue dans le fichier linux.txt
perl snmpenum.pl 192.168.17.215 public linux.txt

Annexe 2

Hackxor

You play a professional blackhat hacker hired to track down another hacker by any means possible. Start by checking your email on wraithmail, and see how far down the rabbit hole you can get. The key websites in this game are http://wraithmail:8080 http://cloaknet:8080 http://gghb:8080 and http://hub71:8080 so if you don't feel like tracking down your target you may hack them in any order. Each website will be properly introduced through the plot.

Vous pouvez trouver des indices à http://hackxor.sourceforge.net/cgi-bin/hints.pl.