Sommaire

Introduction Générale……..……..1

Chapitre1 : Présentation du cadre du projet et généralités sur la sécurité des réseaux...3

1. Présentation de l'organisme d'accueil, POLYGONE……...3

2. Etude de l'existant ….……3

2.1 Présentation du réseau de POLYGONE…….……3

3. Approches du travail ……...……..……5

4. Les exigences de la sécurité des réseaux…….…..……... 6

5. Rappel sur le protocole TCP/IP …….…….…..……8

5.1 Présentation du modèle TCP /IP……8

5.2 Couche application ……8

5.3 Couche transport ……..11

5.4 Couche internet…… 12

5.5 Couche accès réseau ……13

6. Menaces de sécurité courantes……..…… 14

6.1 Faiblesses de sécurité des réseaux ……14

Chapitre 2 : Les routeurs Cisco ……15

1. Rappel sur un routeur…….. 15

1.1 Architecture des routeurs Cisco……. 15

2. Les routeurs et leurs rôles le réseau des PME……....16

2.1 Protéger le réseau avec le routeur ……...16

2.2 Vulnérabilité des routeurs …….……....18

3. Inter network operating System IOS……. 18

3.1 Le rôle du système d'exploitation Inter network Operating System (IOS)……. 19

3.2 Méthodes d'accès à Cisco IOS …….…….. 20

3.3 Fichiers de configuration…….…… 23

4. Configuration de base d'un routeur Cisco……. 24

4.1 Configuration de base d'un routeur……... 24

4.2 Mode Cisco IOS…….26

4.3 Configuration du nom d'hôte IOS…….…… 29

4.4 Limitation de l'accès aux périphériques avec mots de passe…….……30

4.5 Configuration d'une interface……32

4.6 Les commandes IOS de base ……33
4.7 Vérification de la connectivité …… 35
5. Etude des techniques d'attaques réseaux ……..37
5.1 Le sniffing des mots de passe et des paquets ……...37
5.2 L'usurpation d'adresse IP …… 38
5.3 Les scanners ……39
5.4 Attaque de type " Deny of Service " ……...39
Chapitre 3 : Politique de sécurité ……42
1. Environnement du Travail ……42
1.1 Environnement Matériel ……..42
1.2 Environnement Logiciel……... 42
2. Définition de la politique de sécurité du routeur ……45
2.1 Les check-lists DISA de sécurité Routeur Cisco……...……45
2.2 Les étapes d'une politique de sécurité réseau ……..……46
3. Application de la politique de sécurité……... 48
3.1 Sécurisation mots de passe et privilèges ……..48
3.2 Désactiver les services et interfaces non utilisés…….. 50
3.3 Sécuriser l'accès Telnet ……51
Conclusion Générale……..……66
Bibliographie et Nétographie ……67
ANNEXES ……..……68

Liste des figures

Figure 1 : schéma du réseau de la société POLYGONE…… 4
Figure 2 : Modèle TCP/IP ……..……..8
Figure 3: Fonctionnement du protocole SNMP……9
Figure 4 : Architecture interne d'un routeur Cisco…… 15
Figure.5: Routeur reliant les réseaux locaux ……..16
Figure 6 : Routeur externe reliant différents site ……17
Figure 7 : routeur frontal relie un réseau interne à un réseau externe ……17
Figure 8 : Cisco IOS (Inter network Operating System) ……19
Figure 9 : Vue arrière du routeur Cisco : Les ports d'accès…… 20
Figure 10 : Fichiers de configuration……... 23
Figure 11: lignes configuration routeur……... 24
Figure 12 : Propriétés de COM1 ……25
Figure 13 : enregistrement d'un fichier texte dans HyperTerminal …… 26
Figure 13 : Structure de l'invite IOS……... 27
Figure 14 : Les principaux modes IOS ……...28
Figure15 : Configuration du nom d'hôte IOS ……..29
Figure 16 : Configuration le mot de passe de console…… 30
Figure 17 : Limitation de l'accès Telnet…….. 32
Figure 18: Configuration d'une interface Ethernet …….33
Figure 19 : Commande Ping ……...36
Figure 20 : Test la pile de protocoles TCP/IP locale…….. 36
Figure 22 : Exemple de scénario d'écoute sur le réseau ……..37
Figure 23: Usurpation de l'adresse IP…… 38
Figure 24: Demande d'établissement d'une connections TCP…… 39
Figure 25 : Principe de Syn Inondation ……..40
Figure 26: attaque smurf ……..…….41
Figure 27 : Page d'accueil d'un Packet Tracer…… 43
Figure 28 : Outils de construire un réseau ……...43
Figure 29 : Schéma d'un réseau……... 44
Figure 30 : Configuration des machines…… 45
Figure 31 : schéma d'un réseau avec serveur Taccas ……..52
Figure 32: Mise en place d'un serveur log (syslog)…… 57

Introduction Générale

Les réseaux informatiques sont devenus indispensables à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont aujourd'hui de plus en plus ouverts sur Internet, est à priori bénéfique, pose néanmoins un problème majeur : il en découle un nombre croissant d'attaques qui peuvent aboutir à de graves conséquences professionnelles et financières en menaçant l'intégrité, la confidentialité et la disponibilité de l'information. Les menaces informatiques peuvent se catégoriser de la manière suivante :

- Accès physique,
- Interception de communication,
- Détournement ou altération de message,
- Déni de service(Dos),
- Intrusion.

Afin de pouvoir immuniser un système contre ces menaces, il est nécessaire de

- se tenir informé des mises à jour des OS et les correctifs des failles ,
- mettre en place des dispositifs (pare-feu, système de détection d'intrusion, antivirus) permettant de sécuriser l'infrastructure réseau,
- de corriger les erreurs de conception et d'implémentation par les constructeurs (comme CISCO, Microsoft…) dés que la vulnérabilité est découverte.

L'infrastructure réseau, qui présente le périmètre du Système d'Information, est considérée comme la première cible des pirates.

Etant donné que la plupart des entreprises déploient des équipements réseaux de marque CISCO, les routeurs de cette marque ont été la cible de plusieurs attaques basées sur l'exploitation frauduleuse des protocoles réseaux, ainsi que les failles liées à leurs configurations.

En vue de protéger son Système d'Information, et essentiellement son infrastructure réseau, constituée principalement d'équipements CISCO, la société

POLYGONE a eu le besoin de prévenir les menaces susceptibles de nuire au bon fonctionnement du réseau.

Le présent projet a pour but de définir l'ensemble des attaques ciblant les routeurs CISCO en vue de déceler leurs vulnérabilités pour les corriger en appliquant les règles de sécurité recommandées.

D'ou le travail demandé est :

- Identifier les failles des routeurs CISCO,
- Mettre en place les procédures de sécurité selon les check-lists de DISA (Defense Information Systems Agency) pour prévenir ces attaques

Ce rapport est organisé conformément au plan suivant :

Le premier chapitre inclut le cadre du projet et un ensemble de concepts théoriques liés à la sécurité des réseaux. Le deuxième chapitre, comporte la présentation des routeurs Cisco et leurs vulnérabilités. Le dernier chapitre décrit la phase de réalisation du projet qui comporte les **procédures recommandées pour la sécurisation des routeurs.**

Chapitre1 : Présentation du cadre du projet et généralités sur la sécurité des réseaux

Introduction

Dans ce chapitre, il s'agit de mettre mon travail dans son contexte général. La première section comprend alors la présentation de l'organisme d'accueil et la deuxième, une brève description de la méthodologie du travail adoptée suivie des notions théoriques jugées nécessaires pour le déroulement de notre travail.

1. Présentation de l'organisme d'accueil, POLYGONE

POLYGONE est un acteur dans le domaine de l'intégration de réseau, de la téléphonie, de la vidéosurveillance… Avec une gamme de produits variée et étendue, POLYGONE propose des services relatifs aux besoins en télécommunication, sécurité, réseau informatique intégré, réseau sans fil, câblage informatique vidéosurveillance.

Pour ce faire, il va sans dire que POLYGONE s'est dotée de toutes les ressources humaines, techniques et logistiques susceptibles de satisfaire tous les besoins et exigences de la manière la plus efficace et fiable de ses clients.

POLYGONE offre aux entreprises des solutions adaptées dans le domaine de la mise en place d'un réseau : de câblage informatique, téléphonique, domotique, système de sécurité, plancher surélevé…

2. Etude de l'existant :

2.1 Présentation du réseau de POLYGONE

Le réseau de la société POLYGONE permet de relier chaque ordinateur entre eux via un serveur qui va gérer l'accès à Internet, les mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers. Le réseau permet à la société de centraliser ses données, de travailler en équipe de manière productive.

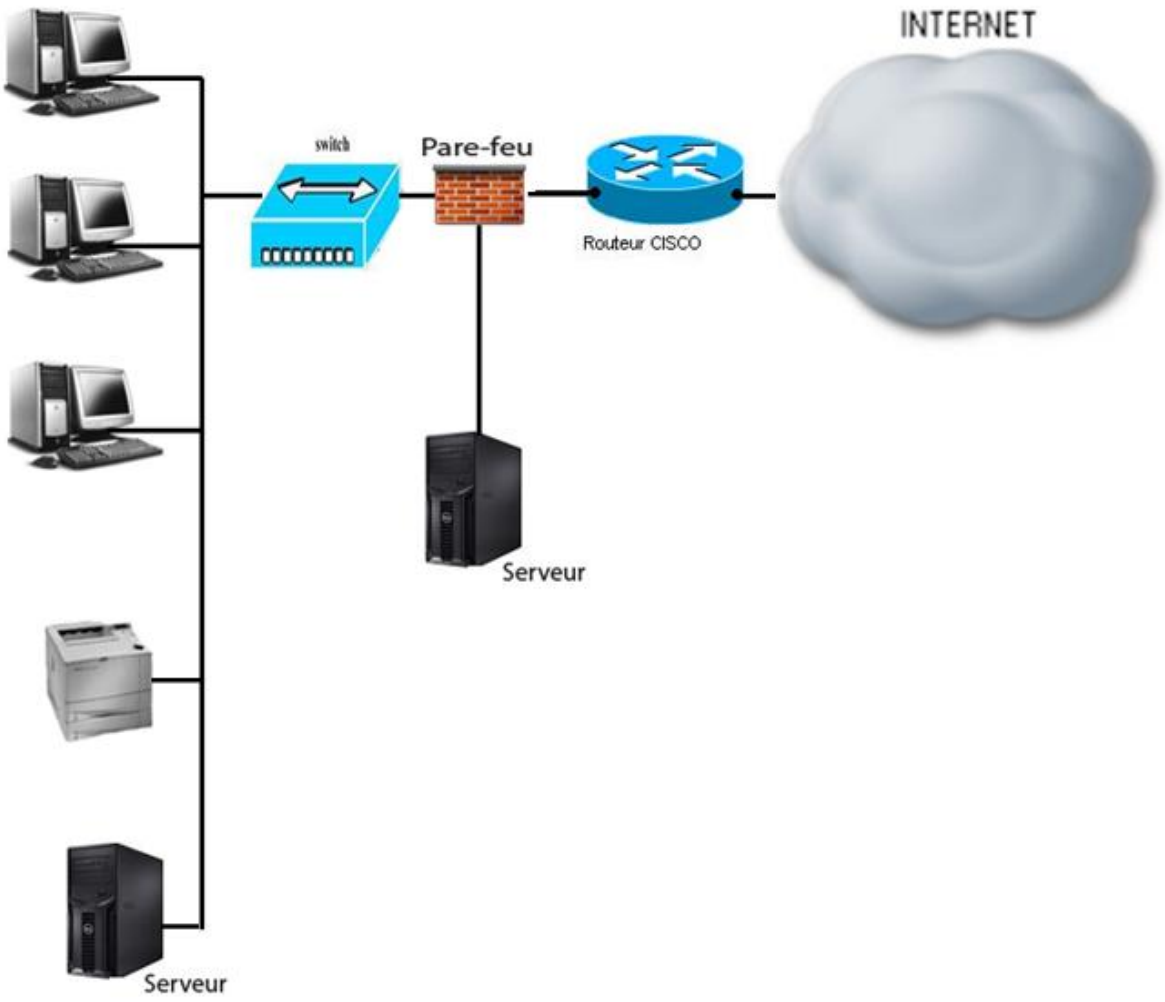


Figure 1 : schéma du réseau de la société POLYGONE

Le réseau local d'une entreprise représente le cœur de la majeure partie de l'activité informatique de cette entreprise. Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux.

Par ailleurs, il est généralement estimé que la majorité des malveillances informatiques ont une origine complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significative des pertes par rapport aux deux autres : accidents et erreurs).

Devant cette spécificité, la société POLYGONE a eu le nécessité donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local.

Il est aise d'échafauder sur le papier des configurations de systèmes d'information, sécurisés avec les techniques les plus Sophistiquées matière de « firewalls » et de contrôles

d'accès, mais il est fréquent qu'un audit sérieux révèle encore de nombreuses insuffisances, notamment sur le plan physique (accès aux équipements, continuité de fonctionnement).

Ce sont précisément des situations de ce type qu'il est nécessaire de prendre en compte dans une conception de réseau local sécurise. Les locaux techniques sont des points essentiels du reseau local, sans lesquels il ne peut fonctionner correctement. Ils presentent un point de vulnerabilite important dans la mesure ou ils abritent nombre d'appareils sensibles (hubs, routeurs, etc.) et sur lesquels pèsent des menaces importantes (ecoute, piratage, etc.).

Cette étude, a pour but de protéger leur infrastructure réseau a travers de définir l'ensemble des attaques ciblant les routeurs CISCO en vue de déceler leurs vulnérabilités, POLYGONE a eu le besoin de prévenir ces menaces susceptibles de nuire au bon fonctionnement du réseau en appliquant les règles de sécurité recommandées.

3. Approches du travail

- Etude bibliographique
  - Recherche d'informations sur les menaces informatiques, les failles de sécurité des routeurs et des protocoles réseaux et les différentes techniques et outils d'attaques afin d'avoir une meilleure idée sur les procédures à appliquer.
- Etude théorique :
  - Etudier les routeurs Cisco et leur configuration,
  - Etudier les attaques possibles ciblant cet équipement,
  - Rechercher un simulateur réseau.
- Etude d'ingénierie
  - Gestion et réalisation du projet : Maîtrise d'ouvrage et maîtrise d'œuvre,
  - Rédaction des procédures correspondantes aux choix techniques et fonctionnels,
  - Exploitation des bases scientifiques pour comprendre le mécanisme des attaques pour pouvoir appliquer les procédures de sécurité.
- Réalisation :
  - Manipulation des configurations du routeur et application des procédures de sécurité afin d'établir les règles de protection nécessaires.

4. Les exigences de la sécurité des réseaux

Les exigences de sécurité et de confidentialité, résultant de l'utilisation d'inter-réseaux pour échanger des informations confidentielles et commerciales d'importance critique, excèdent ce que l'architecture actuelle peut offrir. C'est pourquoi des efforts considérables sont consacrés à ce secteur de recherche et de développement pour combattre les failles de sécurité inhérentes à l'architecture réseau.

Les conséquences d'une violation de la sécurité d'un réseau peuvent être les suivantes :

- Pannes du réseau empêchant les communications et les transactions et entraînant donc une perte d'activité,
- Mauvaise utilisation ou perte de fonds personnels ou de l'entreprise,
- Vol d'éléments de propriété intellectuelle d'une entreprise (idées de recherche, brevets ou dessins de conception) ensuite utilisée par un concurrent,
- Communication des détails de contrats avec des clients à des concurrents ou au public entraînant une perte de confiance en l'entreprise de la part du marché ,
- Si le public n'a plus confiance dans la capacité de l'entreprise à assurer les niveaux de confidentialité et d'intégrité requis, la société risque de perdre des ventes et même de faire éventuellement faillite.

Pour éviter ces conséquences graves, il faut assurer:

- La disponibilité : demande que l'information sur le système soit disponible aux personnes autorisées,
- La confidentialité : demande que l'information sur le système ne puisse être lue que par les personnes autorisées,
- L'intégrité : demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.

Pour être en mesure de répondre à ces attentes, il est indispensable de garantir la fiabilité de ces quatre éléments essentiels constituant un réseau :

- Les protocoles : Les règles ou conventions qui déterminent la façon dont les messages sont envoyés, orientés, reçus et interprétés,
- Les messages ou unités d'information qui transitent d'un périphérique à un autre,
- Un moyen d'interconnecter ces périphériques, c'est-à-dire un support capable de transporter les messages d'un périphérique à un autre,

- Les périphériques du réseau (routeur, commutateur, hub…) qui échangent des messages entre eux,
- Protection des équipements :

Il y a un certain nombre de façons de fournir la sécurité physique aux équipements. Les pièces qui contiennent ces équipements devraient être sans interférence électrostatique ou magnétique.

Pour aider à protéger les équipements contre certaines attaques de service et permettre de soutenir la gamme la plus large de services de sécurité, les équipements devrait être configuré avec la quantité maximale de mémoire possible.

- Intégrité des messages :

Garantir l'intégrité des données consiste à veiller à ce que les informations ne soient pas modifiées lors de leur transmission de leur point d'origine à leur destination. L'intégrité des données peut être compromise quand les informations ont été corrompues (sciemment ou accidentellement) avant que leur destinataire prévu ne les reçoive.

L'utilisation de signatures numériques, d'algorithmes de hachage et de mécanismes de somme de contrôle contribuent à assurer l'intégrité de la source et des données sur un réseau afin de prévenir toute modification non autorisée des informations.

- Protection du câblage :

L'aspect de la sécurité physique du réseau le plus souvent ignoré est celui du câblage. En effet, si des pirates ont accès à des câbles exposés du réseau, ils disposent alors de plusieurs méthodes pour voler les données.

Sur la plupart des réseaux (de diffusion, tels qu'Ethernet ou à jetons), les données ne sont jamais envoyées exclusivement au PC auquel elles sont destinées. En effet, elles sont envoyées sur tous les PC connectés mais sont ignorées par tous, excepté le PC auquel elles sont destinées. Du fait de cette diffusion des données, chaque câble actif du réseau présente la capacité de transporter des données. Par conséquent, il suffit à un pirate de se raccorder clandestinement à un câble pour capturer les paquets qui transitent par la ligne.

- Fiabilité des protocoles :

Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à leurs implémentations. Il est donc indispensable d'appliquer les correctifs pour les failles découvertes en appliquant les mises à jour aux systèmes implémentant ces protocoles.

5. Rappel sur le protocole TCP/IP

Pour pouvoir comprendre les attaques qui se base sur les protocoles réseau, il est indispensable d'étudier en détaille leurs fonctionnements.

5.1 Présentation du modèle TCP /IP

Le sigle TCP/IP désigne un protocole de communication utilisé sur Internet. Ce protocole définit les règles que les ordinateurs doivent respecter pour communiquer entre eux sur le réseau Internet. Le sigle TCP/IP est formé sur les noms des deux protocoles majeurs utilisés sur Internet : le protocole TCP pour "Transmission Control Protocol" et le protocole IP pour "Internet Protocol". Ce sigle désigne aussi une suite de protocoles, c'est-à-dire de règles de communication que les ordinateurs doivent respecter pour communiquer entre eux via Internet.

La figure suivante présente les différentes couches du modèle TCP /IP ainsi que quelques protocoles utilisés par chaque couche.

Figure 2 : Modèle TCP/IP

5.2 Couche application

La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue. Outre la prise en charge du transfert de fichiers, du courrier électronique et de la connexion à distance, le modèle TCP/IP possède des protocoles prenant en charge des services comme : TELNET, http, SMTP, DNS, TFTP, SNMP …

Protocole Telnet (TErminal NETwork **ou** TELecommunication NETwork**):**

Ce protocole permet d'accéder à distance à un autre périphérique du réseau. Cela permet à un utilisateur d'ouvrir une session sur un hôte distant et d'exécuter diverses commandes. Un client TELNET est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.

- Vulnérabilité du protocole Telnet

Le côté sommaire de Telnet fait que toute communication est transmis en clair sur le réseau, mots de passe compris. Des logiciels d'écoute sur les réseaux comme tcpdump[1] ou Wireshark [2] permettent d'intercepter les communications de la commande Telnet.

Protocole SNMP (Simple Network Management Protocol)

C'est le protocole de gestion de réseaux proposé par l'IETF (*Internet Engineering Task Force : est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet)*. Il est actuellement le protocole le plus utilisé pour la gestion, supervision et diagnostique des problèmes réseaux et matériels.

- Fonctionnement du protocole SNMP

Le protocole SNMP constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager (la station de supervision) envoie des requêtes à l'agent (GetRequest : demande d'information, SetRequest : Affectation), qui retourne des réponses (GetResponse). Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager.

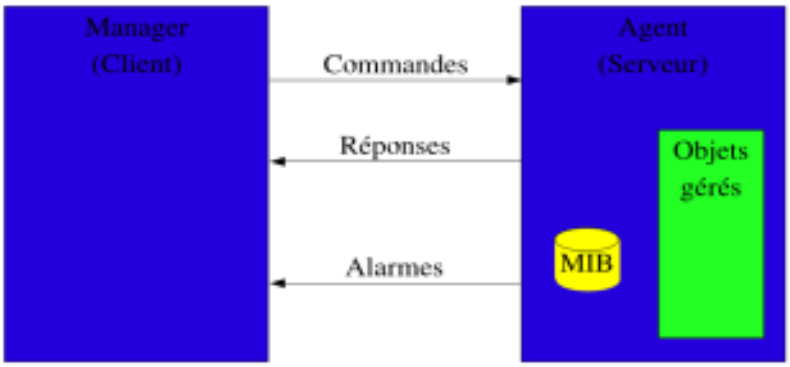


Figure 3: Fonctionnement du protocole SNMP

SNMP utilise le protocole UDP .L'agent reçoit les requêtes de la station de gestion sur le port 161. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents.

- Les MIBS

La MIB (Management Information base) est la base de données des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur, et il est aussi possible d'utiliser un explorateur de MIB tel que : MIB Browser [3].

Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. Par exemple, la variable 1.3.6.1.2.1.2.2.1.7.1 est l'élément ou l'OID(1) (Object Identifié) correspondante au nom «ifAdminStatus» qui contient le statut des interfaces de l'élément actif questionné.

- Notion de communauté dans SNMP

Une communauté SNMP est un ensemble de machines gérées par la même station de supervision. On dit qu'un équipement appartient à une (ou plusieurs) communauté SNMP. Pendant la transaction SNMP la communauté fait office de mots de passe. Ainsi les stations ne faisant pas partie de la communauté ne peuvent pas envoyer ou répondre aux requêtes SNMP.

- Vulnérabilité du protocole SNMP

Il est possible de connaître à distance l'état ou la configuration d'un routeur (fonction GET). Il est également possible d'influer sur le comportement d'une machine en écrivant des données dans la base d'information(MIB) du périphérique (fonction SET).

Les premières versions du protocole (v1 et v2) ne proposaient pas de mesures de sécurité efficaces pour éviter l'accès aux informations sensibles. Il suffisait de connaître un nom de communauté valide pour pouvoir accéder aux informations.

Un nom de communauté, actif et présent par défaut sur un routeur, peut permettre à un attaquant présent sur le réseau d'accéder en lecture seule à la configuration complète du routeur et même de la modifier.

Par exemple, des informations comme des adresses IP et Ethernet, le contenu des tables de routage, des statistiques sur le trafic, seront disponibles. Un attaquant peut donc récupérer facilement des informations qui peuvent lui faciliter une attaque ultérieure.

(1) *: OID: c'est la suite d'entiers qui désigne de manière non ambiguë un objet SNMP*

5.3 Couche transport

La couche transport fournit une connexion logique entre les hôtes source et de destination. Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure, entre les deux points d'extrémité. Le rôle principal de la couche transport est d'assurer une fiabilité et un contrôle de bout en bout lors du transfert des données. Les fenêtres glissantes, les numéros de séquençage et les accusés de réception permettent d'obtenir ce résultat. Ces paramètres sont gérer par le protocole TCP de cette couche, contrairement au protocole UDP, qui n'ouvre pas de session et n'effectue pas de control d'erreur. Officiellement, cette couche n'a que deux implémentations: le protocole TCP(Transmission Control Protocol) et le protocole UDP(User Datagram Protocol).

Protocole TCP:

TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion

- Vulnérabilité du protocole TCP

Une vulnérabilité dans sa mise en œuvre permet à un individu mal intentionné d'effectuer un déni de service sur les connexions TCP préalablement établies par l'envoi de paquets TCP judicieusement formés. Comme l'attaque Synflood qui sera décrite ultérieurement.

Protocole UDP:

Ce protocole est en revanche un protocole plus simple que TCP: il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP: la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final. De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

- Vulnérabilité du protocole UDP

Un expéditeur transmet aux entités communicantes un volume de demande pour un diagnostic des services UDP qui utilise toutes les ressources de l'unité centrale.

De nombreuses attaques utilisent ces failles car le protocole UDP ne crée pas de connexion et n'utilise pas de numéro de séquence. Il est très facile de falsifier ou simuler un échange. La plus grande prudence est demandée pour l'utilisation de ce protocole qui est capable, soit de saturer un réseau ou une machine, soit de permettre l'accès à des fichiers distants (NFS fonctionne avec UDP). De nombreuses applications, telles que DNS et SNMP, utilisent UDP. Ce protocole expose les utilisateurs au « déni de service ».

5.4 Couche internet

Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Le principal protocole de cette couche est le protocole IP. La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche. Parmi les protocoles qui s'exécutent au niveau de cette couche on trouve IP, ICMP et ARP.

Protocole IP

Le protocole IP effectue les opérations suivantes:

- Il définit un paquet et un système d'adressage,
- Il transfère des données entre la couche Internet et la couche d'accès au réseau,
- Il achemine des paquets à des hôtes distants.

Le protocole IP est parfois qualifié de protocole non fiable. Cela ne signifie pas qu'il n'envoie pas correctement les données sur le réseau, mais qu'il n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction. Ces fonctions sont disponibles uniquement dans les protocoles de couche supérieure des couches application ou transport.

Protocole ICMP (Internet Control Message Protocol)

Ce protocole permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des Datagrammes en erreurs.

Le mécanisme de requête et de réponse par écho du protocole ICMP est utilisé pour contrôler la présence d'un hôte, la commande Ping permet d'envoyer une requête ICMP

'Echo' d'une machine à une autre machine. Si la machine ne répond pas il se peut que l'on ne puisse pas communiquer avec elle (c'est le principe de la commande Ping).

- Vulnérabilité protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est souvent considéré comme un protocole innocent et sans danger. Toutefois, si un système d'exploitation ou un pare feu vient à le manipuler de manière incorrecte, des pirates peuvent alors l'utiliser à des fins malveillantes.

Protocole ARP:

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol).

5.5 Couche accès réseau

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau. Ainsi, la couche accès réseau contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local LAN (Ethernet), ou WAN (Frame Relay, RNIS, RTC, LS, ADSL..).
Elle prend en charge les notions suivantes :

- Acheminement des données sur la liaison,
- Coordination de la transmission de données (synchronisation),
- Format des données,
- Conversion des signaux (analogique/numérique),
- Contrôle des erreurs à l'arrivée.

En outre, les protocoles de la couche d'accès au réseau mappent les adresses IP avec les adresses matérielles physiques et encapsulent les paquets IP dans des trames.

6. Menaces de sécurité courantes

6.1 Faiblesses de sécurité des réseaux

▪ Vulnérabilité du protocole TCP/IP :

Les protocoles http, FTP et ICMP sont intrinsèquement non sécurisés. Les protocoles SNMP, SMTP et les inondations SYN sont liés à la structure intrinsèquement non sécurisés qui est à la base de la conception du TCP.

▪ Vulnérabilité des Systèmes d'exploitation :

Tous les systèmes d'exploitation présentent des problèmes de sécurité qui doivent être résolus.

▪ Vulnérabilité des équipements réseaux :

Les différents types d'équipements réseau tels que les routeurs, les firewalls et switchs ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent la protection des mots passe, le manque d'authentification, les protocoles de routage et les ouvertures dans para feux.

– Comptes système ou utilisateurs non sécurisés : les données des comptes utilisateurs ou système peuvent être transmises de manière non sécurisée dans le réseau ce qui expose les noms utilisateurs et leurs mots de passe aux logiciels d'espion.

– Paramètres par défaut non sécurisés : un grand nombre d'équipements ont des paramètres par défaut peuvent générer des failles de sécurité.

– Equipement mal configuré : une mauvaise configuration de l'équipement lui-même peut engendrer de sérieux problèmes de sécurité.

▪ Absence d'une politique de sécurité écrite :

Une stratégie de sécurité non écrite ne peut pas être appliquée ni respectée de manière cohérente.

▪ Manque de continuité

▪ Contrôle d'accès logiques non appliqué

Conclusion

Ce chapitre nous a donné l'occasion de présenter le cadre du stage et d'exposer les enjeux de la sécurité informatique. Cette étude a permis de mettre en évidence les différentes failles qui peuvent infecter les routeurs ainsi que les protocoles de communication.

Chapitre 2 : Les routeurs Cisco

Introduction

Dans ce chapitre, nous allons décrire les procédures à suivre pour connecter et configurer les ordinateurs, les routeurs formant un réseau local Ethernet. Nous allons présenter les procédures de configuration de base des périphériques réseau Cisco. Ces procédures requièrent l'utilisation du système d'exploitation Cisco Inter network Operating System (IOS) et des fichiers de configuration connexes pour les périphériques intermédiaires. Il est essentiel que les administrateurs et les techniciens réseau comprennent le processus de configuration avec IOS. L'organisation de ce chapitre est la suivante : dans la première partie la définition le rôle du système d'exploitation Inter network Operating System (IOS), la deuxième partie présente les Vulnérabilités de routeur Cisco, enfin étudier le techniques d'attaques réseaux.

1. Rappel sur un routeur

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Un routeur est chargé de recevoir sur une interface des données sous forme de paquets et de les renvoyer sur une autre en utilisant le meilleur chemin possible. Selon l'adresse destination et l'information contenue dans sa table de routage

1.1 Architecture des routeurs Cisco

Tous Les routeurs Cisco ont une architecture interne qui peut être représenté par :

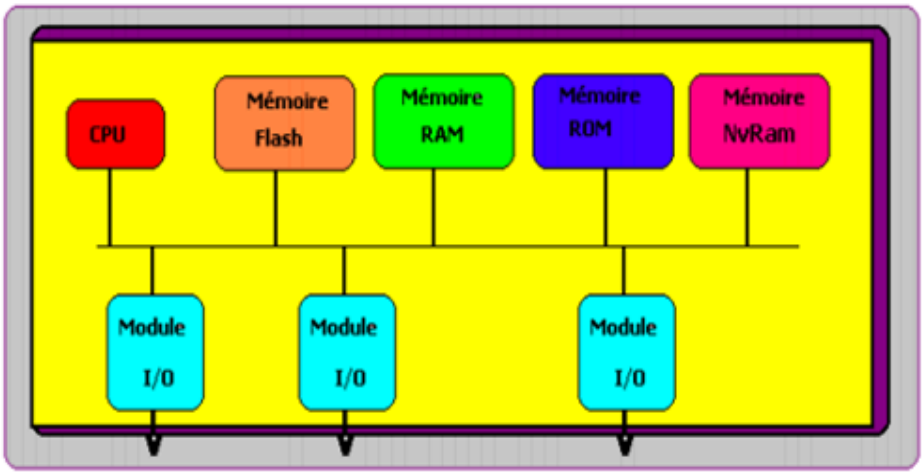


Figure 4 : Architecture interne d'un routeur Cisco

Ils contiennent tous :

- Une mémoire **NVRam** pour Ram non Volatile et sur laquelle l'administrateur va stocker la configuration qu'il aura mise dans le routeur. Elle contient également la configuration de l'IOS,
- Une carte mère qui est en général intégrée au châssis,
- Une **CPU** qui est un microprocesseur Motorola avec un BIOS spécial nommé " I.O.S. " pour Internetwork Operating System,
- Une mémoire **RAM** principale contenant le logiciel IOS, c'est dans laquelle tout sera exécuté un peu à la manière d'un simple ordinateur,
- Une mémoire **FLASH**, également une mémoire non volatile sur laquelle on stocke la version courante de l'IOS du routeur,
- Une mémoire **ROM** non volatile et qui, quant à elle, contient les instructions de démarrage (bootstrap) et est utilisée pour des opérations de maintenance difficiles de routages, ARP, etc.), mais aussi tous les buffers utilisés par les cartes d'entrée.

2. Les routeurs et leurs rôles le réseau des PME :

2.1 Protéger le réseau avec le routeur

Les routeurs peuvent jouer un rôle dans la garantie de réseaux. Les routeurs exécutent beaucoup de travaux différents dans des réseaux modernes, mais pour cette discussion nous examinerons trois voies fondamentales pour lesquels les routeurs sont employés :

- Routeurs Intérieurs

Un routeur intérieur transmet le trafic entre deux ou plusieurs réseaux locaux au sein d'une organisation ou une entreprise. Les réseaux connectés par un routeur intérieur partagent souvent la même politique de sécurité et le niveau de confiance entre eux est d'habitude haut. Des routeurs intérieurs peuvent imposer certaines restrictions sur le trafic envoyé entre les réseaux.

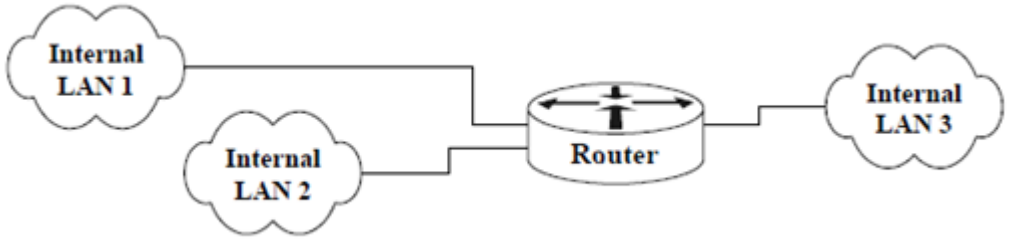


Figure.5: Routeur reliant les réseaux locaux

▪ Routeurs Backbone

Un routeur Backbone ou un routeur extérieur est celui qui transmet le trafic entre les différents sites d'une entreprise.

Le niveau de confiance entre les réseaux connectés par un routeur Backbone est d'habitude très bas. Généralement, les routeurs de backbone sont conçus et configurés pour acheminer le trafic aussi rapidement que possible, sans imposer de restrictions sur ce point.

Le principal objectif d'un routeur backbone pour assuré la sécurité est de :

– Veiller à ce que la gestion et le fonctionnement du routeur sont réalisés uniquement par les parties autorisées.

– Protéger l'intégrité des données acheminées on acheminant le trafic avec un protocole de routage, ou en se référant à une table de routage statique.

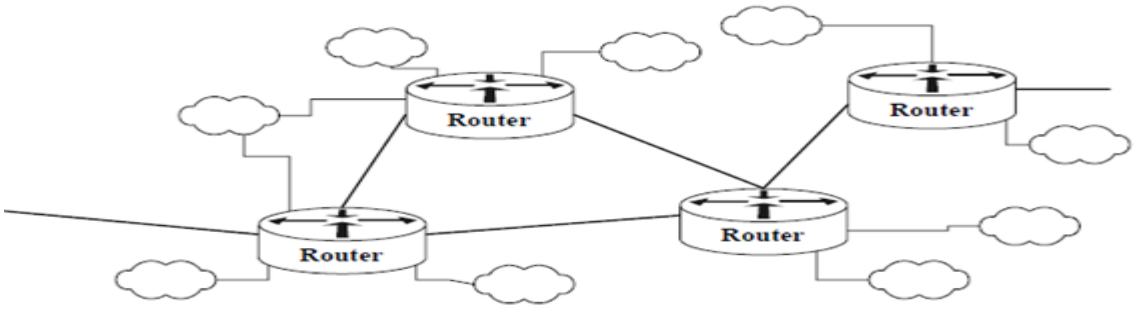


Figure 6 : Routeur externe reliant différents site

▪ Routeurs frontaux

Un routeur frontal achemine le trafic entre le réseau de l'entreprise et le réseau extérieurs. L'aspect clef d'un routeur de frontière est qu'il présente la partie intermédiaire entre les réseaux internes sécurisés d'une entreprise et des réseaux externes non sécurisés (par exemple l'Internet). Il peut aider à sécuriser le périmètre d'un réseau d'entreprise en appliquant des restrictions au trafic qu'il contrôle. Un routeur de frontière peut utiliser des protocoles d'acheminement, ou il peut dépendre des routes statiques.

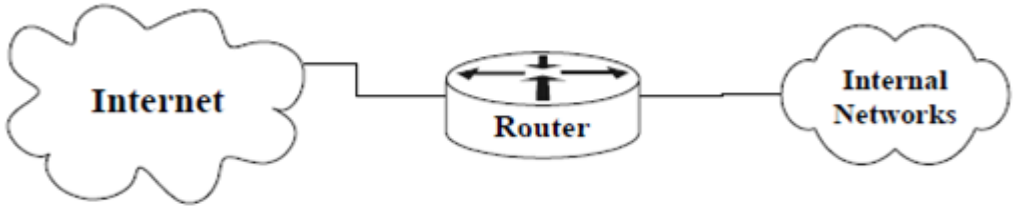


Figure 7 : routeur frontal relie un réseau interne à un réseau externe

2.2 Vulnérabilité des routeurs

Vu le rôle important qu'assure le routeur pour garantir les réseaux, il est nécessaire d'examiner de proche cet équipement pour découvrir ses vulnérabilités dans le but de limiter les menaces qui peuvent se présenter.

Les vulnérabilités d'un routeur peuvent se présenter dans :

- La configuration

Un routeur est semblable à beaucoup d'ordinateurs dans lesquels il y a beaucoup de services permis par défaut. Beaucoup de ces services sont inutiles et peuvent être utilisés par un attaquant pour la collecte d'informations ou pour l'exploitation. Comme les services SNMP .Parfois aussi les noms des utilisateurs et les mots de passe sont laissés par défaut.

- Gestion du Routeur

Le contrôle de l'accès à un routeur par des administrateurs est une tâche importante. Il y a deux types d'accès :

- L'accès local implique une connexion directe à un port de console sur le routeur avec un terminal ou un ordinateur portable,
- L'accès à distance implique généralement la permission Telnet ou des connexions SNMP au routeur à partir d'un ordinateur sur le même sous-réseau ou un sous-réseau différent.

Pendant l'accès éloigné (à distance) tous les mots de passe Telnet ou les noms de communauté SNMP sont envoyés en clair sur le réseau, donc une écoute sur le réseau suffit pour les connaître.

Ainsi ces failles peuvent être à l'origine des différentes attaques qui visent à prendre contrôle sur le routeur, ce qui veut dire prendre le contrôle sur l'acheminement des données dans le réseau. Comme elle peut avoir un autre objectif celui d'arrêter le service du routeur pour perturber le réseau.

3.InternetWork operating System IOS

IOS est l'acronyme de "Inter networks Operating System", soit, pour les anglophobes, "Système d'exploitation pour l'interconnexion de réseaux .Ce système est administrable en lignes de commandes, propres aux équipements de Cisco Systems

3.1 Le rôle du système d'exploitation Inter network Operating System (IOS)

À l'instar d'un ordinateur personnel, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation. Sans système d'exploitation, le matériel est inopérant. Cisco IOS est le logiciel système des périphériques Cisco. Il s'agit d'une technologie centrale qui s'étend à pratiquement tous les produits Cisco. Cisco IOS est exécuté par la plupart des périphériques Cisco, quels que soient leur taille et leur type. Ce logiciel est par exemple utilisé pour des routeurs, des commutateurs de réseau local, des petits points d'accès sans fil, des grands routeurs dotés de douzaines d'interfaces et bien d'autres périphériques.

Figure 8 : Cisco IOS (**Inter network Operating System)**

Cisco IOS fournit aux périphériques les services réseau suivants :

- fonctions de routage et de commutation de base,
- accès fiable et sécurisé aux ressources en réseau,
- évolutivité du réseau.

Les détails du fonctionnement de Cisco IOS varient d'un périphérique à l'autre selon le but et le jeu de fonctions de l'appareil.

Pour accéder aux services fournis par IOS, vous utilisez généralement une interface de ligne de commande (ILC). Les fonctions accessibles à travers ILC varient selon la version de Cisco IOS et le type du périphérique.

Le fichier IOS proprement dit, dont la taille atteint plusieurs méga-octets, est stocké dans une zone de mémoire semi-permanente appelée Flash. La mémoire Flash assure un stockage non volatil. En d'autres termes, cette mémoire conserve son contenu lorsque le périphérique n'est plus sous tension. À la différence d'une mémoire morte, toutefois, la mémoire Flash permet de modifier ou de recouvrir son contenu s'il y a lieu.

Grâce à la mémoire Flash, il est possible de mettre IOS à niveau en installant de nouvelles versions ou de lui ajouter de nouvelles fonctions. Dans de nombreuses architectures de routeur, IOS est copié en mémoire vive à la mise sous tension du périphérique et il s'exécute en mémoire vive. Cette fonction améliore les performances du périphérique.

3.2 Méthodes d'accès à Cisco IOS :

Il y a plusieurs moyens d'accéder à l'environnement ILC. Les méthodes les plus répandues utilisent :

- le port de console,
- le protocole Telnet ou SSH,
- le port AUX.

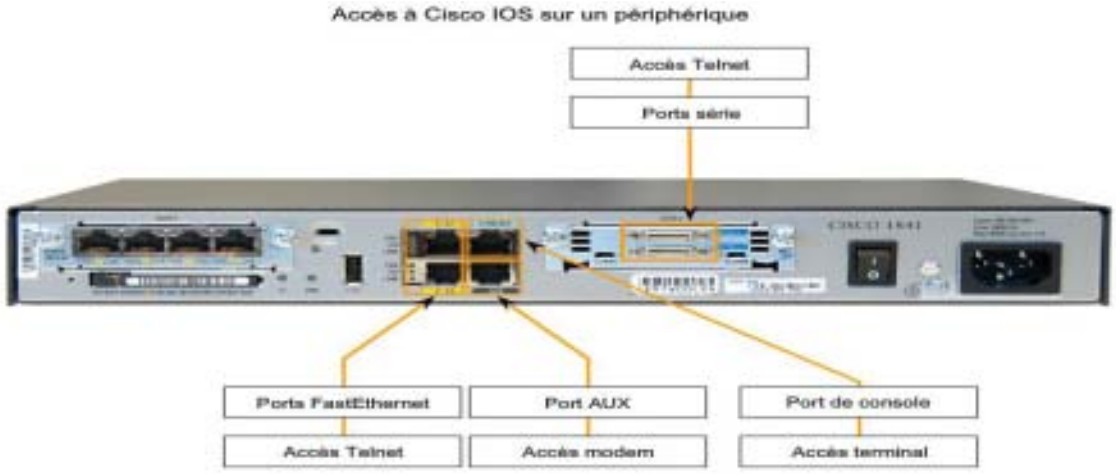


Figure 9 : Vue arrière du routeur Cisco : Les ports d'accès

- **Port de console**

Il est possible d'accéder à l'environnement ILC par une session console, également appelée ligne CTY. La console connecte directement un ordinateur ou un terminal au port de console du routeur ou du commutateur via une liaison série lente.

Le port de console est un port de gestion permettant un accès hors réseau à un routeur. Le port de console est accessible même si aucun service réseau n'a été configuré sur le

périphérique. Le port de console est souvent utilisé pour accéder à un périphérique avant que les services réseau ne soient lancés ou lorsqu'ils sont défaillants.

La console s'utilise en particulier dans les circonstances suivantes :

- configuration initiale du périphérique réseau,
- procédures de reprise après sinistre et dépannage lorsque l'accès distant est impossible,
- procédures de récupération des mots de passe.

Lorsqu'un routeur est mis en service pour la première fois, ses paramètres réseau n'ont pas été configurés. Le routeur ne peut donc pas communiquer via un réseau. Pour préparer le démarrage initial et la configuration du routeur, un ordinateur exécutant un logiciel d'émulation de terminal est connecté au port de console du périphérique. Ainsi, il est possible d'entrer au clavier de l'ordinateur connecté les commandes de configuration du routeur.

S'il est impossible d'accéder à distance à un routeur pendant qu'il fonctionne, une connexion à son port de console peut permettre à un ordinateur de déterminer l'état du périphérique. Par défaut, la console transmet les messages de démarrage, de débogage et d'erreur du périphérique.

Pour de nombreux périphériques IOS, l'accès console ne requiert par défaut aucune forme de sécurité. Il convient toutefois de configurer un mot de passe pour la console afin d'empêcher l'accès non autorisé au périphérique. En cas de perte du mot de passe, un jeu de procédures spécial permet d'accéder au périphérique sans mot de passe. Il est recommandé de placer le périphérique dans une pièce ou une armoire fermée à clé pour interdire l'accès physique.

- **Telnet et SSH**

Une autre méthode d'accès distant à une session ILC consiste à établir une connexion Telnet avec le routeur. À la différence des connexions console, les sessions Telnet requièrent des services réseau actifs sur le périphérique. Le périphérique réseau doit avoir au moins une interface active configurée avec une adresse de couche 3, par exemple une adresse IPv4. Les périphériques Cisco IOS disposent d'un processus serveur Telnet qui est lancé dès le démarrage du périphérique. IOS contient également un client Telnet.

Un hôte doté d'un client Telnet peut accéder aux sessions vty en cours d'exécution sur le périphérique Cisco. Pour des raisons de sécurité, IOS exige l'emploi d'un mot de passe dans la session Telnet en guise de méthode d'authentification minimale. Les méthodes permettant de configurer les ouvertures de session et les mots de passe seront expliquées plus loin dans ce chapitre.

Le protocole Secure Shell (SSH) permet un accès distant plus sécurisé aux périphériques. À l'instar de Telnet, ce protocole fournit la structure d'une ouverture de session à distance, mais il utilise des services réseau plus sécurisés.

SSH fournit une authentification par mot de passe plus résistante que celle de Telnet et emploie un chiffrement lors du transport des données de la session. La session SSH chiffre toutes les communications entre le client et le périphérique IOS. Ceci préserve la confidentialité de l'iD d'utilisateur, du mot de passe et des détails de la session de gestion. Il est conseillé de toujours utiliser SSH à la place de Telnet dans la mesure du possible.

La plupart des versions récentes de Cisco IOS contiennent un serveur SSH. Dans certains périphériques, ce service est activé par défaut. D'autres périphériques requièrent une activation du serveur SSH.

Les périphériques IOS incluent également un client SSH permettant d'établir des sessions SSH avec d'autres périphériques. De même, vous pouvez utiliser un ordinateur distant doté d'un client SSH pour démarrer une session ILC sécurisée. Le logiciel de client SSH n'est pas fourni par défaut sur tous les systèmes d'exploitation. Il peut donc s'avérer nécessaire d'acquérir, d'installer et de configurer un logiciel de client SSH pour votre ordinateur.

- **Port AUX**

Une autre façon d'ouvrir une session ILC à distance consiste à établir une connexion téléphonique commutée à travers un modem connecté au port AUX du routeur. À l'instar de la connexion console, cette méthode ne requiert ni la configuration, ni la disponibilité de services réseau sur le périphérique.

Le port AUX peut également s'utiliser localement, comme le port de console, avec une connexion directe à un ordinateur exécutant un programme d'émulation de terminal. Le port de console est requis pour la configuration du routeur, mais les routeurs ne possèdent pas tous un port AUX. En outre, il est préférable d'utiliser le port de console plutôt que le port AUX pour le dépannage, car il affiche par défaut les messages de démarrage, de débogage et d'erreur du routeur.

En général, le port AUX ne s'utilise localement à la place du port de console qu'en cas de problèmes liés au port de console, par exemple lorsque vous ignorez certains paramètres de la console.

3.3 Fichiers de configuration:

Les périphériques réseau ont besoin de deux types de logiciels pour fonctionner : le système d'exploitation et le logiciel de configuration. Le système d'exploitation, comme celui d'un quelconque ordinateur, facilite l'exploitation de base des composants matériels du périphérique.

Les fichiers de configuration, quant à eux, contiennent les commandes du logiciel Cisco IOS utilisées pour personnaliser les fonctionnalités d'un périphérique Cisco. Les commandes sont analysées (traduites et exécutées) par le logiciel Cisco IOS au démarrage du système (à partir d'un fichier appelé startup-config) ou lorsqu'elles sont entrées dans l'environnement ILC en mode configuration.

Un administrateur réseau crée une configuration qui définit la fonctionnalité souhaitée d'un périphérique Cisco. La taille d'un fichier de configuration va généralement de quelques centaines à quelques milliers d'octets.

- ***Types de fichiers de configuration***

Un périphérique réseau Cisco contient deux fichiers de configuration :

- le fichier de configuration en cours, que le périphérique utilise en fonctionnement normal,
- le fichier de configuration initiale, qui est chargé quand le périphérique démarre et sert de copie de sauvegarde de la configuration.

Il est également possible de stocker un fichier de configuration à distance sur un serveur en guise de copie de sauvegarde.

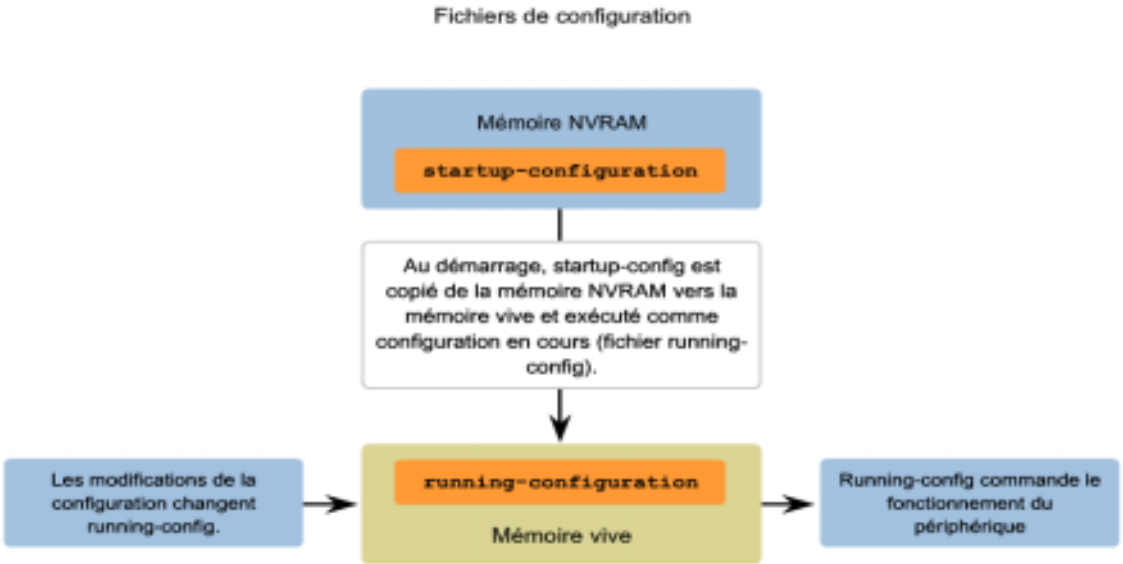


Figure 10 : Fichiers de configuration

4.Configuration de base d'un routeur Cisco :

La configuration de base d'un routeur Cisco (et des autres aussi) se fait en général via la porte console. La porte console, sur un routeur, est configurée comme une interface DTE (Data Terminal Equipment). Les lignes de configuration d'un routeur sont les suivantes

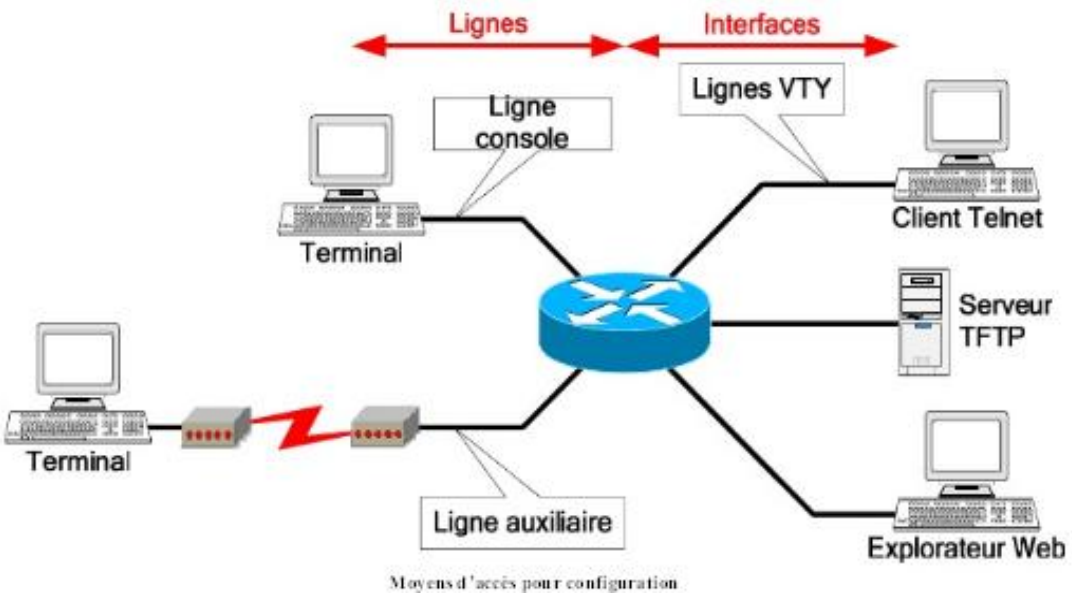


Figure 11: lignes configuration routeur

Un routeur peut être configuré à partir des sources externes suivantes :

- **Ligne console :** Accès primaire, à utiliser si aucun autre accès de configuration n'est Disponible,
- **Ligne auxiliaire :** Accès à distance via une liaison RTC et modems interposés,
- **Ligne(s) VTY :** Accès via un client Telnet (5 ou 16 lignes disponibles par routeur en fonction du modèle),
- **Explorateur Web :** Accès utilisant le serveur HTTP interne du routeur,
- **Serveur TFTP :** Import/export de fichiers de configuration,
- **Serveur FTP:** Import/export de fichiers de configuration

4.1 Configuration de base d'un routeur :

Connectez un câble console sur le port console du routeur et branchez l'autre extrémité au port COM 1 du PC en utilisant un adaptateur DB-9 ou DB-25. Cela doit être effectué avant de mettre une quelconque unité sous tension.

- **HyperTerminal**
  - Mettez sous tension l'ordinateur et le routeur.
  - À partir de la barre des tâches de Windows, accédez au programme HyperTerminal Démarrer > Programmes > Accessoires > Communications > Hyper Terminal.
- **Nommez la session HyperTerminal**

Dans la boîte de dialogue « Description de la connexion », entrez un nom dans le champ Nom (exemple CISCO). Et cliquez sur **OK.**

- **Spécifiez l'interface de connexion de l'ordinateur**

Dans la boîte de dialogue « Connexions », utilisez la flèche de déroulement dans le champ Se connecter en utilisant : pour sélectionner COM1, puis cliquez sur **OK.**

- **Spécifiez les propriétés de connexion de l'interface**

Dans la boîte de dialogue « COM1 Propriétés », utilisez les flèches de déroulement pour sélectionner : Bits par seconde : 9600 Bits de données : 8 Parité : Aucune Bits d'arrêt : 1 Contrôle de flux : Aucun

Puis cliquez sur OK.

Figure 12 : Propriétés de COM1

Lorsque la fenêtre de la session HyperTerminal apparaît, mettez le routeur sous tension, si ce n'est déjà fait. Appuyez ensuite sur la touche Entrée. Le routeur doit répondre. La connexion s'est alors déroulée avec succès. Consignez dans le journal technique la procédure correcte pour établir une session en mode console avec le routeur.

- **Sauvegarde des configurations par capture de texte (HyperTerminal)**

Vous pouvez enregistrer/archiver les fichiers de configuration dans un document texte. Cette procédure permet de s'assurer qu'une copie de travail des fichiers de configuration est disponible en vue d'une modification ou une réutilisation ultérieure.

Dans HyperTerminal, effectuez les étapes suivantes :

1. Dans le menu Transfert, cliquez sur Capture de texte.
2. Choisissez l'emplacement.
3. Cliquez sur Démarrer pour commencer à capturer le texte.

Enregistrement d'un fichier texte dans HyperTerminal

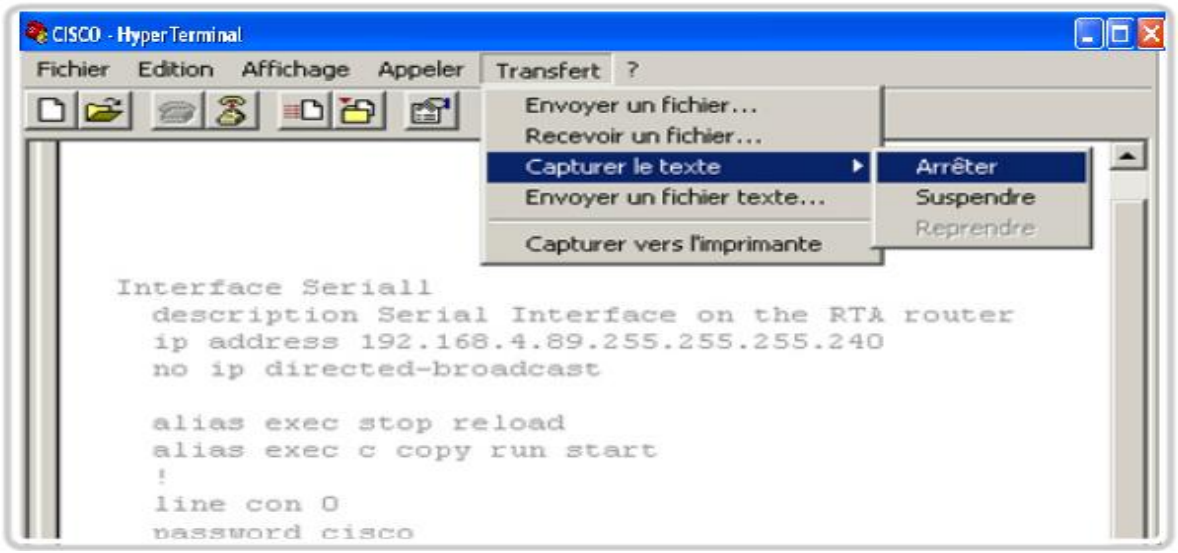


Figure 13 : enregistrement d'un fichier texte dans HyperTerminal

Par défaut tous les interfaces d'un routeur :

- Désactivés,
- Hors fonction,
- Administratively down.

4.2 Mode Cisco IOS:

Cisco IOS a été conçu comme un système d'exploitation modal. L'adjectif modal qualifie un système offrant différents modes d'exploitation ayant chacun son propre domaine de fonctionnement. Les modes de l'environnement ILC sont organisés selon une structure hiérarchique.

Dans l'ordre de haut en bas, les principaux modes sont les suivants :

- mode d'exécution utilisateur,
- mode d'exécution privilégié,
- mode de configuration globale,
- autres modes de configuration spécifiques.

- **Invites de commandes**

Dans l'environnement ILC, le mode dans lequel vous travaillez est reconnaissable à son invite de commandes unique. Cette invite est composée des mots et des symboles qui apparaissent au début de la ligne de commande. Comme l'indique le mot invite, le système vous invite à effectuer une entrée.

Par défaut, toute invite commence par le nom du périphérique. Après le nom du périphérique, le reste de l'invite précise le mode. Par exemple, l'invite par défaut pour le mode de configuration globale sur un routeur est :

Router(config)#

Comme le montre la figure, lorsque vous entrez des commandes et passez d'un mode à l'autre, l'invite change pour refléter le contexte en cours.

Structure de l'invite IOS

```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

Figure 13 : Structure de l'invite IOS

- **Modes principaux**

Les deux principaux modes d'exécution sont :

- le mode utilisateur,
- le mode privilégié.

Par mesure de sécurité, Cisco IOS prévoit deux modes d'accès distincts pour les sessions d'exécution. Ces deux modes d'accès principaux sont utilisés dans le cadre de la structure hiérarchique de l'environnement Cisco ILC.

Ces deux modes offrent des commandes semblables. Toutefois, le mode d'exécution privilégié bénéficie de pouvoirs plus étendus dans les actions qu'il permet d'exécuter.

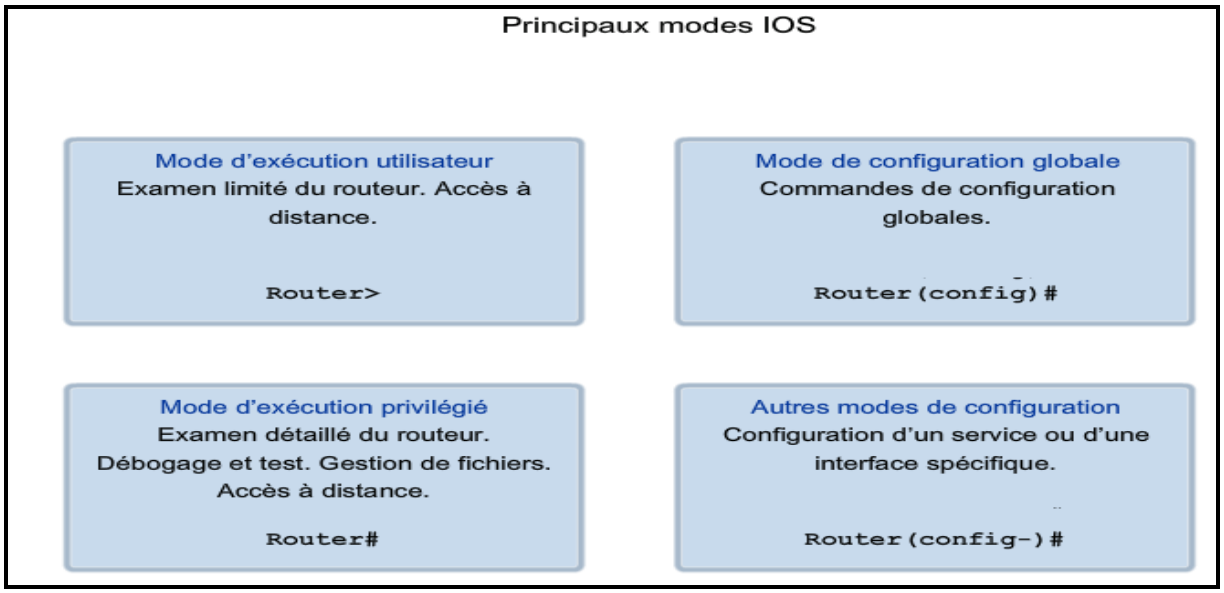


Figure 14 : Les principaux modes IOS

Les principaux modes sont les suivants :

- Mode d'exécution utilisateur : Permet de consulter toutes les informations liées au routeur sans pouvoir les modifier. Le shell est le suivant:

  Router >

- Mode d'exécution privilégié : Permet de visualiser l'état du routeur et d'importer/exporter des images d'IOS. Le shell est le suivant:

  Router #

- Mode de configuration globale : Permet d'utiliser les commandes de configuration générales du routeur. Le shell est le suivant:

  Router (config) #

- Mode de configuration d'interfaces: Permet d'utiliser des commandes de configuration des interfaces (Adresses IP, masque, etc.). Le shell est le suivant:

  Router (config-if) #

- Mode de configuration de ligne: Permet de configurer une ligne (exemple: accès au routeur par Telnet). Le shell est le suivant:

  Router (config-line) #

- Mode spécial: RXBoot Mode de maintenance qui peut servir, notamment, à réinitialiser les mots de passe du routeur. Le shell est le suivant:

  rommon >

4.3 Configuration du nom d'hôte IOS

En mode d'exécution privilégié, accédez au mode de configuration globale en entrant la commande configure terminal :

Router# configure terminal

Après exécution de cette commande, l'invite devient :

Router(config)#

En mode de configuration globale, entrez le nom d'hôte :

Router(config)#hostname r1

Après exécution de cette commande, l'invite devient :

r1(config)#

Observez que le nom d'hôte apparaît dans l'invite. Pour quitter le mode de configuration globale, utilisez la commande exit.

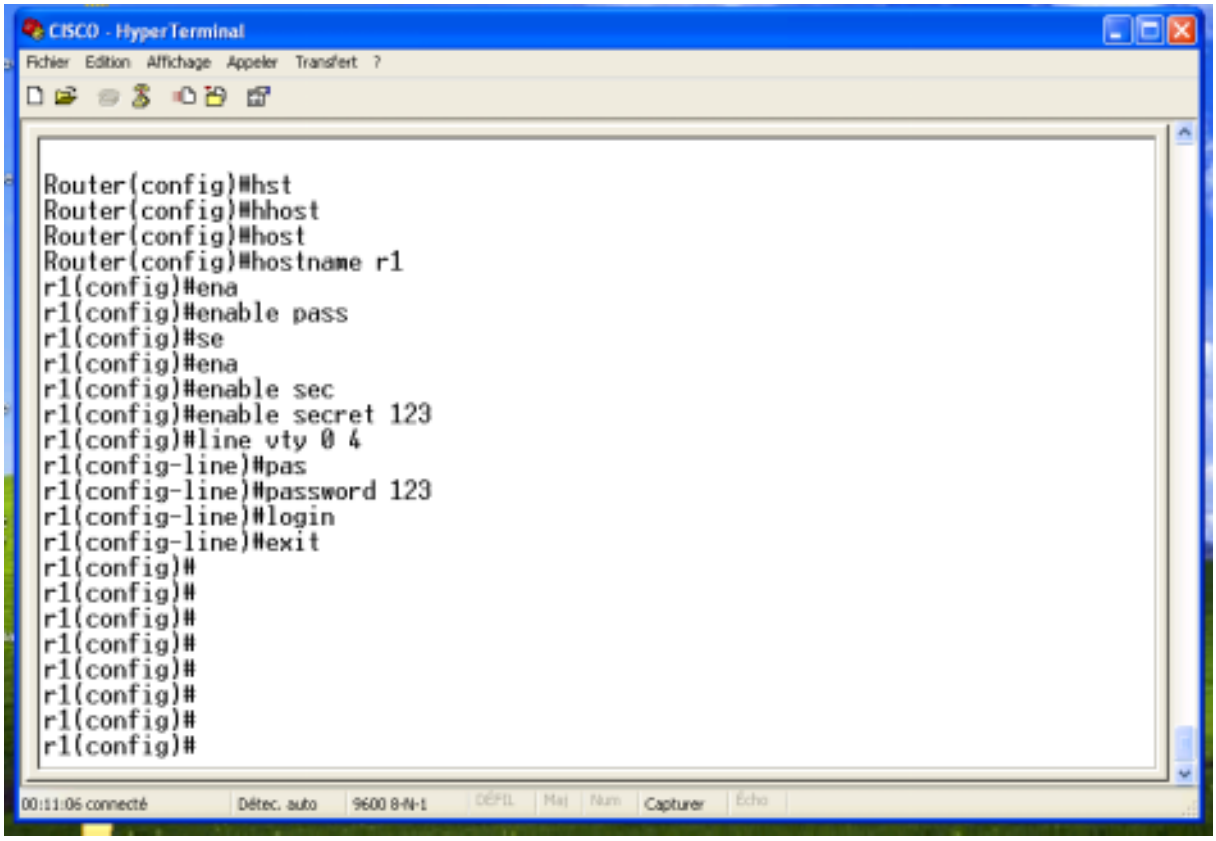


Figure15 : Configuration du nom d'hôte IOS

4.4 Limitation de l'accès aux périphériques avec mots de passe

Les mots de passe présentés ici sont les suivants :

- Mot de passe de console - limite l'accès au périphérique par une connexion console

r1 (config)#line console 0

r1 (config-line)#password 123

r1 (config-line)#login

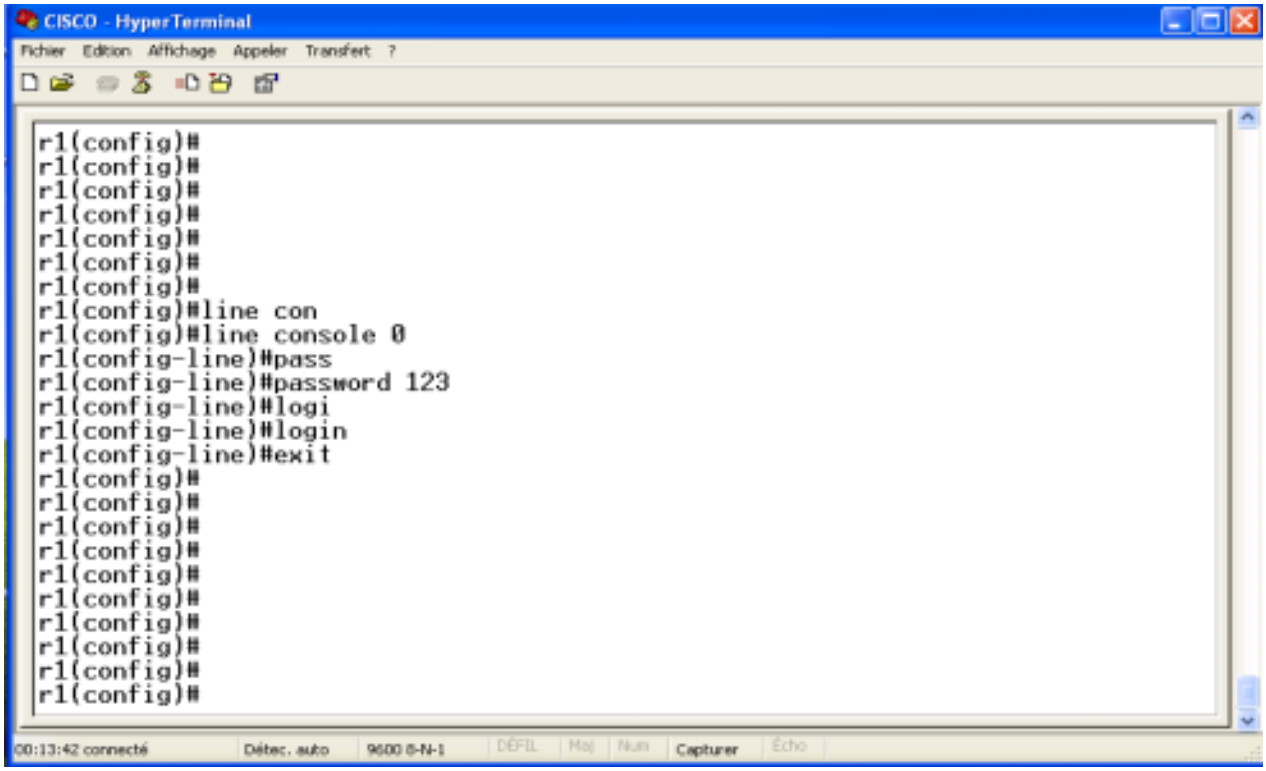


Figure 16 : Configuration le mot de passe de console

- Application d'un mot de passe à l'accès Privilégié

Cette partie explique comment appliquer un mot de passe à l'utilisateur privilégié.

Il faut tout d'abord, se connecter en mode privilégié, puis en mode de configuration globale pour effectuer cette manipulation:

r1 > enable

r1 # configure terminal

r1(config) #

Une fois en mode de configuration globale, Il suffit de taper une seule commande pour appliquer un mot de passe:

r1 (config) # enable password mot_de_passe

A présent, la prochaine fois qu'un utilisateur tentera de se connecter en mode utilisateur privilégié, un mot de passe vous sera demandé.

A ce stade, il est recommandé d'enregistrer régulièrement la configuration à l'aide de la commande suivante (à effectuer en mode privilégié):

copy running-config startup-config

- Mot de passe **« enable secret »** - chiffré, limite l'accès au mode d'exécution privilégié

  r1(config)#enable secret 123

- Configuration de l'accès Telnet au routeur

La configuration avec le câble console et HyperTerminal n'étant pas très pratique, il est possible d'autoriser les administrateurs à se connecter au routeur via une session Telnet à partir de n'importe quel poste des deux réseaux.

Passez d'abord en mode de configuration globale, puis en mode de configuration de ligne VTY:

r1 > enable

Password:

r1 # configure terminal

r1 (config) # line vty 0 4

Va configurer la possibilité de 5 sessions telnet simultanées sur ce routeur. Nous arrivons maintenant sur le prompt de configuration de ligne. Pour activer le Telnet, il vous suffit juste d'appliquer un mot de passe à la ligne:

r1 (config-line) # password mot_de_passe

r1 (config-line) # login

r1 (config-line) # exit

Il est recommandé d'utiliser des mots de passe différents pour chacun de ces niveaux d'accès. En effet, bien que l'utilisation de plusieurs mots de passe différents ne facilite pas l'ouverture d'une session, cette précaution est nécessaire pour protéger convenablement l'infrastructure réseau contre l'accès non autorisé

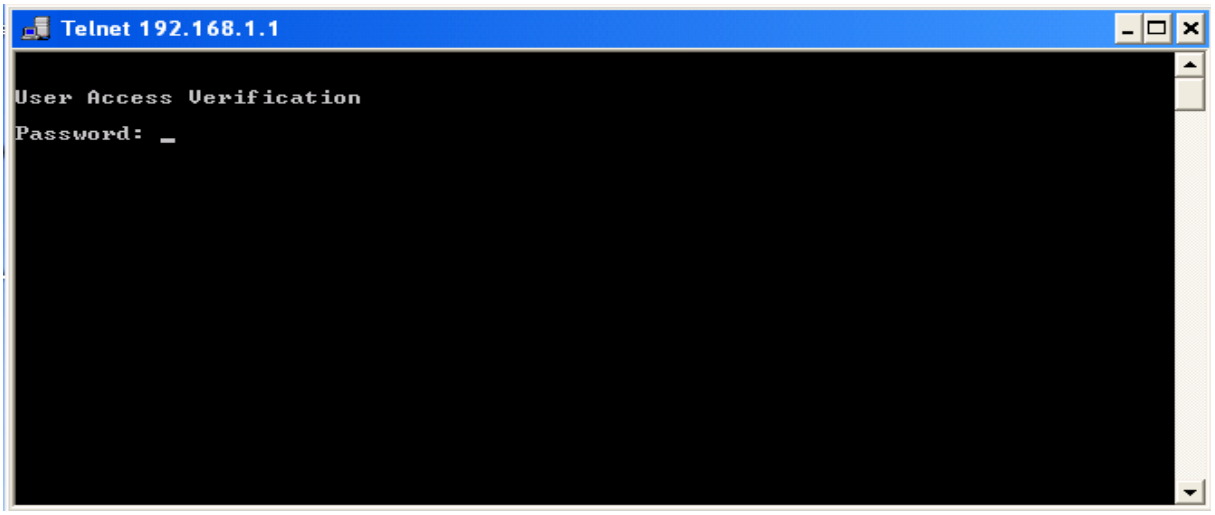


Figure 17 : Limitation de l'accès Telnet

4.5 Configuration d'une interface

Nous devons faire communiquer les deux réseaux connectés au routeur. Admettons que le nom de l'interface reliée au PC1 est fa0/0 et celle reliée au PC2, fa0/1 et que nous sommes en mode de configuration globale.

Les étapes de configuration d'une interface sont les suivantes :

- Étape 1. Spécification du type d'interface et du numéro de port de l'interface,
- Étape 2. Spécification d'une description de l'interface,
- Étape 3. Configuration de l'adresse IP et du masque de sous-réseau de l'interface,
- Étape 4. Définition de la fréquence d'horloge si vous configurez une interface série en tant que DCE,
- Étape 5. Activation de l'interface.

Voici les commandes à saisir:

Interface fa0/0:

r1 (config) # interface fa0/0

r1 (config-if) # ip address 192.168.1.1 255.255.255.0

r1 (config-if) # no shutdown

r1 (config-if) # exit

Interface fa0/1:

r1 (config) # interface serial 0/0/0

r1 (config-if) # ip address 10.0.0.1 255.0.0.0

r1 (config-if) no shutdown

r1 (config-if) exit

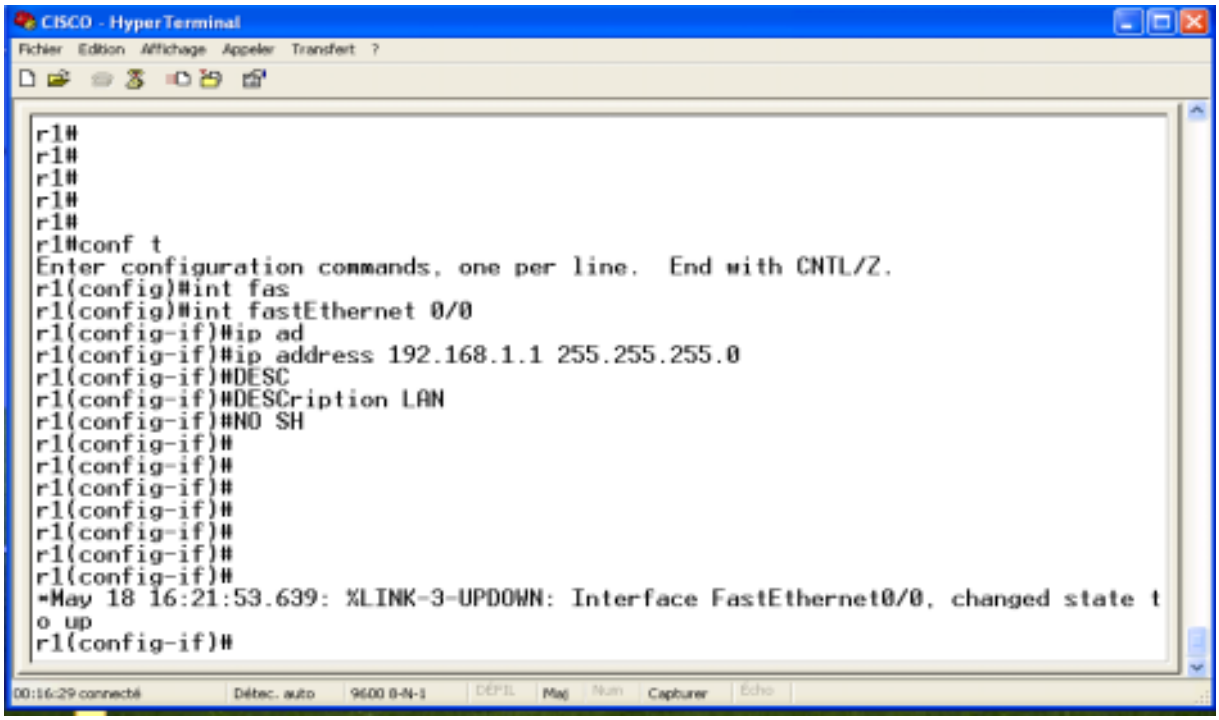


Figure 18: Configuration d'une interface Ethernet

4.6 Les commandes IOS de base

4.6.1 Passage entre les différentes modes d'utilisateurs

- Utilisateur normal: Aucune commande à effectuer, c'est dans ce mode que commence une session.
- Utilisateur privilégié (à effectuer à partir du mode normal):

  r1 > enable

  r1 > en
- Mode de configuration globale (à effectuer à partir du mode Privilégié):

  r1 # configure terminal

  r1 # conf t
- Mode de configuration d'interface (à effectuer à partir du mode de configuration globale):

  r1 (config) # interface nom_interface

  r1 (config) # int nom_interface
- Mode de configuration de ligne (à effectuer à partir du mode de configuration globale):

r1 (config) # line nom_de_la_ligne

4.6.2 Commandes d'information

Les commandes d'information permettent d'afficher les informations relatives au routeur. Elles commencent toutes avec le préfixe show ou sh. Elles sont, pour la plupart, à effectuer à partir du mode privilégié.

- Afficher le fichier de configuration courante du routeur:

  show running-config

  show run

  sh run

- . Afficher les informations sur la configuration matérielle du système et sur l'IOS:

  show version

  sh version

- Afficher les processus actifs:

  show processes

- Afficher les protocoles configurés de couche 3 du modèle OSI:

  show protocols

- Afficher les statistiques de mémoire du routeur:

  show memory

- Afficher des information et statistiques sur une interface:

  show interfaces nom_interface

  sh interfaces nom_interface

  sh int nom_interface

- Afficher la table de routage IP:

  sh ip route

4.6.3 Commandes d'interface

Ces commandes sont liées à la configuration des interfaces du routeur. Elles sont, pour la plupart, à effectuer à partir du mode de configuration d'interface.

- Attribution d'un adresse IP à une interface:

  ip address @IP masque

- Activation de l'interface:

  no shutdown

4.6.4 Commandes d'enregistrement de la configuration courante

Ces commandes permettent de sauvegarder la configuration actuelle pour la réappliquer automatiquement en cas de redémarrage du routeur. Elles s'exécutent en mode Privilégié

- Sauvegarde avec demande de confirmation:

  copy running-config startup-config

  copy run start

- Sauvegarde sans demande de confirmation:

  write

4.6.5 Commandes d'annulation

Cette commande permet de revenir à la dernière configuration enregistrée, annulant toutes les modifications ayant été faites à la configuration depuis. Elle s'exécute en mode Privilégié.

copy startup-config running-config

copy start run

4.6.6 Annulation d'une commande particulière

Pour annuler une commande particulière, on utilisera le préfixe no devant la commande précédemment exécutée.

Exemple: annuler la configuration d'une interface:

no ip address

4.7 Vérification de la connectivité

4.7.1 Test de la pile de protocoles:

- Commande Ping

L'utilisation de la commande Ping constitue un moyen efficace de tester la connectivité. Cette vérification est souvent appelée test de la pile de protocoles parce que la commande Ping passe de la couche 3 du modèle OSI à la couche 2, puis à la couche 1. La commande Ping emploie le protocole ICMP pour vérifier la connectivité.

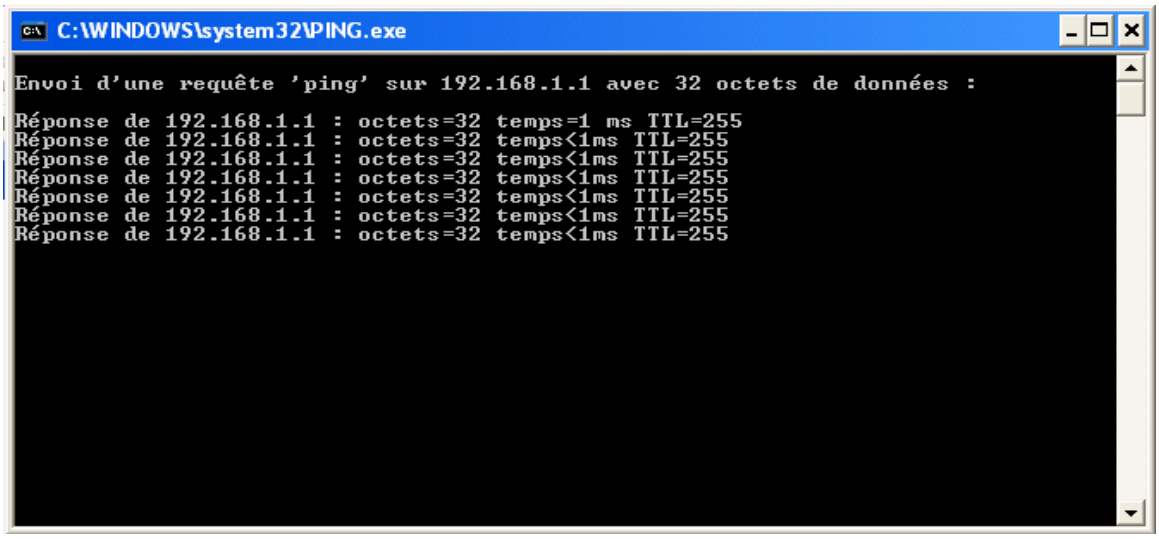


Figure 19 : Commande Ping

- Test la pile de protocoles TCP/IP locale

En guise de première étape dans la série de tests, vous utilisez la commande ping pour vérifier la configuration IP interne sur l'hôte local. Comme vous le savez, ce test s'effectue en exécutant la commande Ping sur une adresse réservée appelée adresse de bouclage (192.168.1.2). Ceci permet de vérifier le bon fonctionnement de la pile de protocoles de la couche réseau à la couche physique (et en sens inverse) sans pour autant envoyer de signal sur les supports.

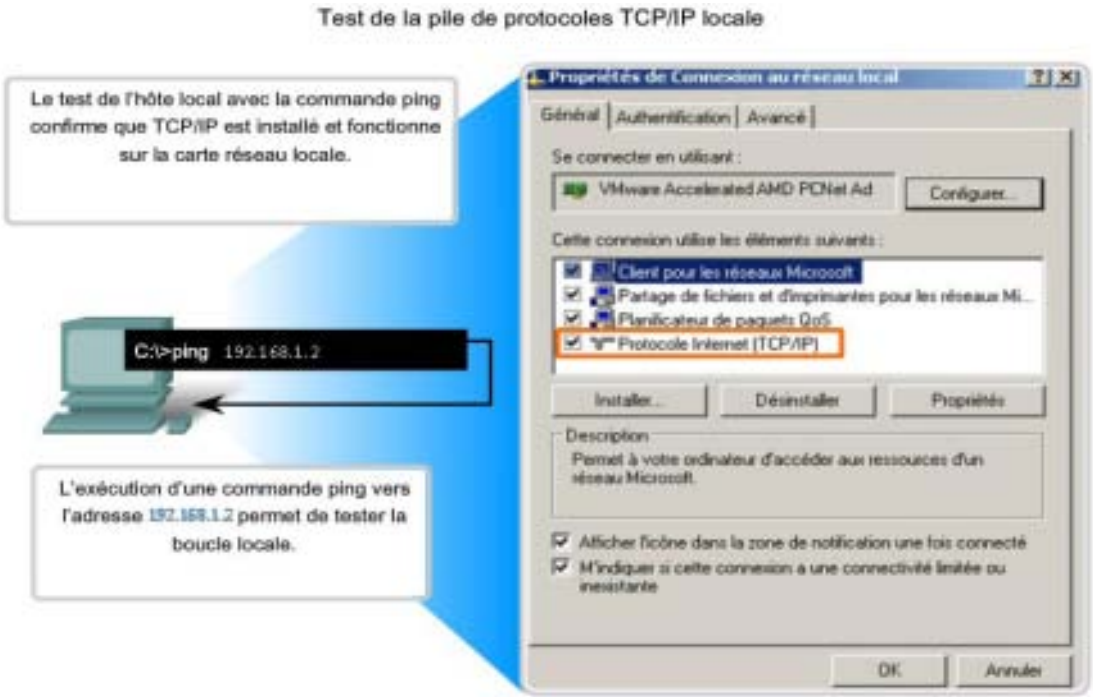


Figure 20 : Test la pile de protocoles TCP/IP locale

- Test l'affectation des interfaces

Après avoir appris à utiliser des commandes et des utilitaires pour vérifier la configuration d'un hôte, vous allez maintenant aborder des commandes permettant de vérifier les interfaces des périphériques intermédiaires. IOS fournit plusieurs commandes pour vérifier le fonctionnement des interfaces de routeur et de commutateur

```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.2.254   YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/1/0            172.16.1.2      YES manual up                    up
Vlan1                  unassigned      YES manual administratively down down
```

Figure 21 : vérification du fonctionnement des interfaces de routeur

5.Etude des techniques d'attaques réseaux

L'objet de cette étude est de comprendre les mécanismes d'attaques, autrement dit, comprendre l'esprit d'un pirate et savoir manipuler ses outils pour pouvoir cerner les menaces et trouver des contre-attaques.

5.1 Le sniffing des mots de passe et des paquets

Si un hacker ne peut pas deviner un mot de passe, il a d'autres outils pour l'obtenir. Une façon qui est devenue assez populaire est le sniffing.

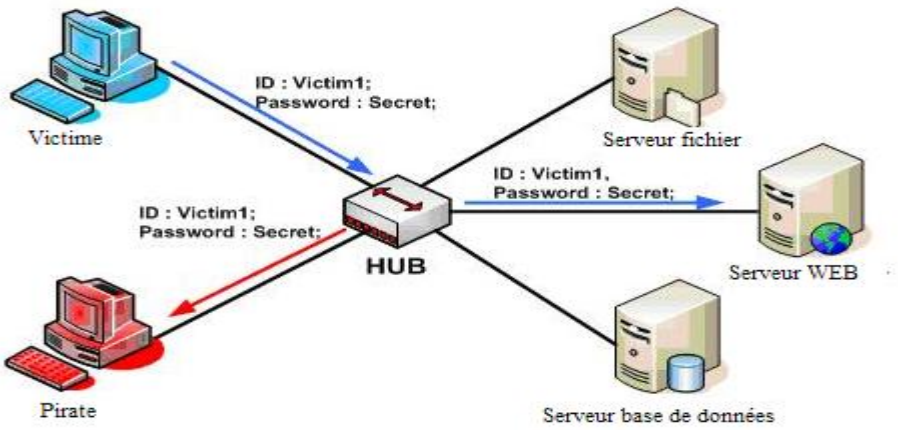


Figure 22 : Exemple de scénario d'écoute sur le réseau

La plupart des réseaux utilisent la technologie de broadcast (comme Ethernet). En pratique, tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message

ne leur est pas destiné et vont donc l'ignorer. Mais par contre, beaucoup d'ordinateurs peuvent être programmés pour regarder chaque message qui traverse le réseau c'est le mode promiscuité.

Il existe des programmes qui utilisent ce procédé et qui capturent tous les messages qui circulent sur le réseau en repérant les mots de passe. Si quelqu'un se connecte à un ordinateur à travers un réseau (à travers Telnet, par exemple), alors cette personne risque de donner son mot de passe.

C'est pourquoi il existe une menace sérieuse pour les personnes qui se connectent sur des ordinateurs distants, où les mots de passe apparaissent en clair dans la trame. Comme par exemple accéder à un périphérique réseau (routeur, Switch..) pour mettre à jour sa configuration à distance.

Parmi les programmes de sniffing les plus connus l'outil dsniff [4] : est un renifleur de trafic réseau, comme tcpdump et ethereal/wireshark, mais il se contente de rechercher les mots de passe qui transitent en clair, exploitant ainsi les faiblesses de certains protocoles. Il supporte les protocoles FTP, Telnet, SMTP, http, POP, SNMP, RIP, OSPF.

5.2 L'usurpation d'adresse IP

En anglais IP spoofing, cette technique est basée sur le trucage de l'adresse source. Pour pénétrer un système, le pirate substitue son adresse IP par une adresse autorisée et émet avec cette adresse. Il peut ainsi passer toutes les barrières qui ne font pas de l'anti-spoofing.

Le principe de base de cette attaque consiste à forger ses propres paquets IP dans lesquels le pirate modifiera, entre autres, l'adresse IP source. Effectivement, les réponses éventuelles des paquets envoyés ne peuvent pas arriver à la machine du pirate puisque la source est falsifiée. Ils se dirigent donc vers la machine spoofée.

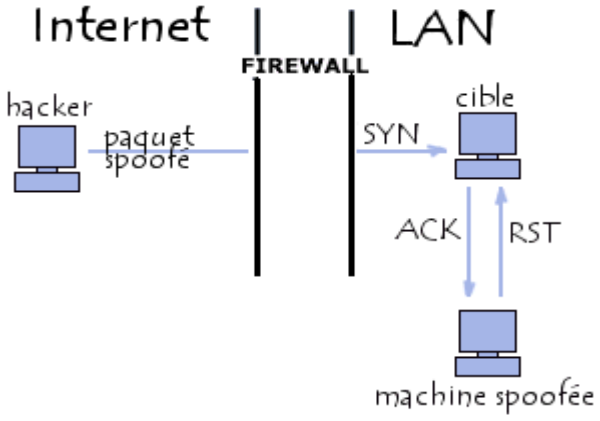


Figure 23: Usurpation de l'adresse IP

L'outil [5] est un outil Open source en ligne de commande permettant de manipuler des paquets IP. Outre le fait que cet outil soit une excellente alternative à la commande ping,

celui-ci rajoute son lot de fonctionnalité. Il est ainsi possible d'effectuer des requêtes TCP ou UDP personnalisées sur un port de destination quelconque.

5.3 Les scanners

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les Hackers utilisent les scanners pour savoir comment ils vont procéder pour attaquer une machine. Leur utilisation n'est heureusement pas seulement malsaine, car les scanners peuvent aussi permettre de prévenir une attaque.

Nmap[6] est parmi les scanners les plus utilisés. Nmap utilise diverses techniques d'analyse basées sur des protocoles tels que TCP, IP, UDP ou ICMP

5.4 Attaque de type " Deny of Service "

Les attaques par déni de service sont destinées à refuser des services à des hôtes légitimes qui tentent d'établir des connexions. Les attaques par déni de service sont utilisées par les pirates pour bloquer les réponses système.

5.4.1 TCP Flooding ou SYN Flooding

Elle exploite le processus normal d'échange en trois étapes et oblige les unités cibles à envoyer un accusé de réception à des adresses source, qui ne complètent pas l'échange en trois étapes.

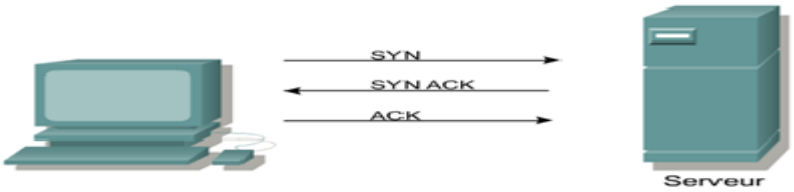


Figure 24: Demande d'établissement d'une connection TCP

L'échange en trois étapes débute lorsque le premier hôte envoie un paquet de synchronisation (SYN). Le paquet SYN inclut l'adresse IP source et l'adresse IP de destination. Ces informations d'adresse sont utilisées par le récepteur pour renvoyer le paquet d'accusé de réception à l'unité émettrice.

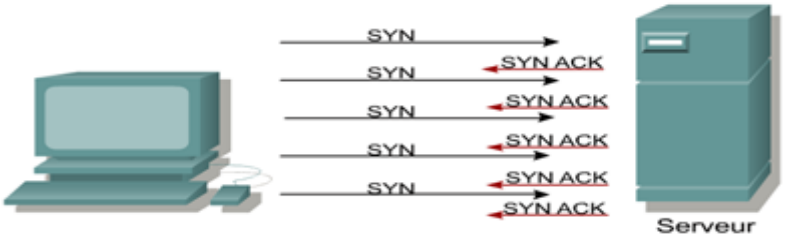


Figure 25 : Principe de Syn Inondation

Dans une attaque par déni de service, le pirate lance une synchronisation mais « usurpe » l'adresse IP source. On parle de « spoofing » lorsque l'unité réceptrice répond à une adresse IP inexistante et inaccessible, puis est placée dans un état d'attente jusqu'à recevoir l'accusé de réception final de l'unité émettrice. La requête d'attente est placée dans une file d'attente de connexion ou dans une zone d'attente en mémoire. Cet état d'attente oblige l'unité attaquée à consommer des ressources système, telles que la mémoire, jusqu'à ce que le délai de connexion expire.

Les pirates inondent l'hôte attaqué de fausses requêtes SYN, l'obligeant à utiliser toutes ses ressources de connexion, ce qui l'empêche de répondre aux requêtes de connexion légitimes. TCP déclare une connexion "ouverte" après un double acquittement. Le *SYN flood* consiste à faire la moitié du travail chaque connexion qui reste à demie ouverte consomme de la mémoire dans la pile TCP/IP. Au bout d'un moment, le noyau les détruit. La solution consiste donc à "ouvrir" ces connexions suffisamment vite. Quand la table du noyau est pleine, le serveur refuse les nouvelles connexions et devient inaccessible.

5.4.2 Utilisation frauduleuse des commandes ICMP

- ICMP Flooding :

L'ICMP Flooding est à l'origine identique à un Ping mais qu'on renouvelle un nombre de fois suffisant pour bloquer la machine attaquée et saturer sa bande passante. Cette opération nécessite d'avoir une connexion Internet plus rapide que la victime.

- ICMP redirect

Un pirate envoie à une machine un paquet ICMP-redirect en lui indiquant un autre chemin à suivre. La machine ne peut alors plus communiquer.

- ICMP-destination unreachable

Un hackeur peut envoyer un message « Destination unreachable » vers une machine, la machine ne peut donc plus communiquer avec d'autres postes sur le réseau.

- Attaque Smurf

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Le scénario d'une telle attaque est le suivant :

– la machine attaquante envoie une requête Ping à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre) et en fournissant l'adresse IP d'une machine cible,

– le serveur de diffusion répercute la requête sur l'ensemble du réseau,

– toutes les machines du réseau envoient une réponse au serveur de diffusion,

– le serveur broadcast redirige les réponses vers la machine cible.

Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routées sur la machine cible.

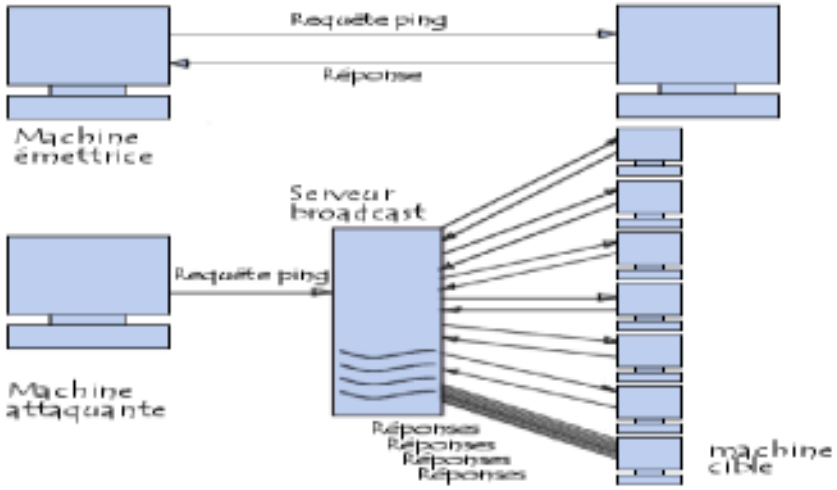


Figure 26: attaque smurf

Conclusion

Dans ce chapitre, nous avons appris comment accéder aux modes et aux procédures de configuration de base d'un routeur Cisco.

L'étude du routeur ainsi que sa configuration nous a permis de mettre en évidence les différentes failles qui peuvent infecter les routeurs ainsi que les protocoles de communication.

Chapitre 3 : Politique de sécurité

Introduction

Dans ce chapitre, nous allons présenter les procédures de configuration de base des routeurs Cisco et prévenir les techniques d'attaques qui menacent l'intégrité du routeur. Nous allons exposer aussi notre environnement de travail tout en définissant les exigences de sécurité à prendre en compte.

L'IOS offre diverses commandes permettant de répondre à ce besoin, principalement les ACL (Access Control List) qui permettent de filtrer des paquets suivant des critères définis ainsi que les différentes méthodes peuvent empêcher ces menaces.

1. Environnement du Travail

1.1 Environnement Matériel

L'environnement matériel sur lequel nous avons travaillé est constitué :

- PC portable DELL INSPIRAN 5010,
- Un Processeur Core I3-350 (2,13GHz) 3Mo CACHE,
- Memoire 4G ,
- DISQUE DUR 320 Go.

1.2 Environnement Logiciel

Pour la configuration des routeurs in a fait recours au logiciel de simulation **Packet tracer**

- **Présentation de Packet Tracer**

Packet Tracer est un logiciel permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc .

- **Description générale**

La figure ci-dessous montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipements peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils comme select

pour déplacer des équipements,– Move Layout pour déplacer le plan de travail,plcae note, delete…….

La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de passer du mode temps réel au mode simulation.

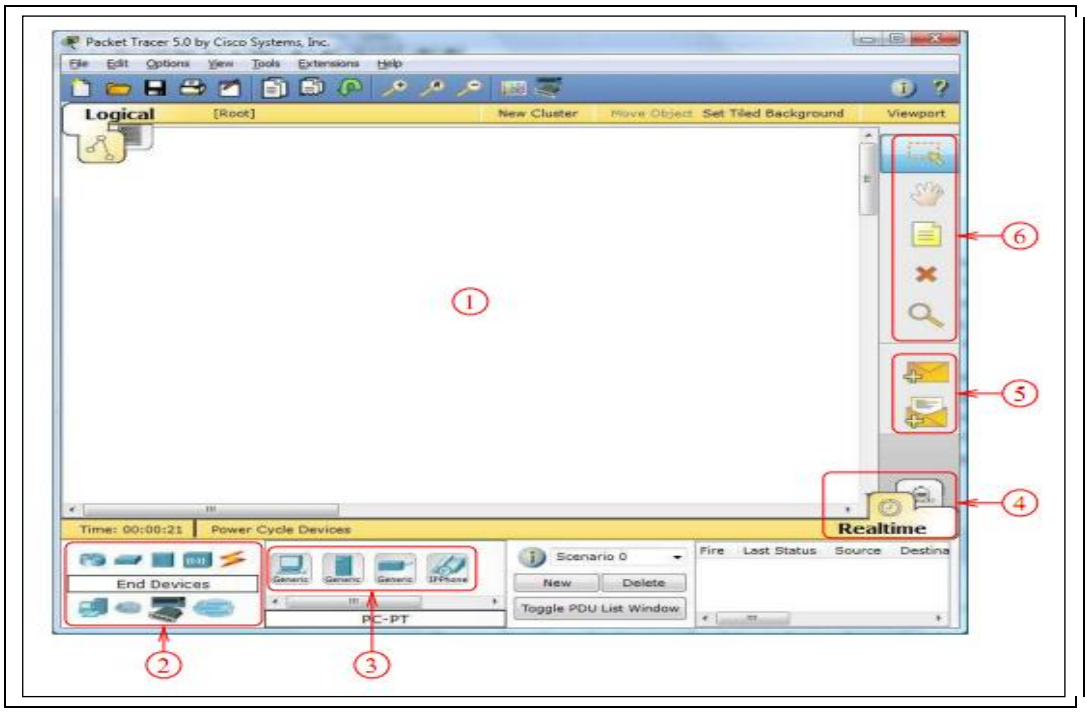


Figure 27 : Page d'accueil d'un Packet Tracer

- **Construire un réseau**

  Pour construire un réseau, on doit choisir l'équipement à configurer « routeur »

Figure 28 : Outils de construire un réseau

Puis pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée.

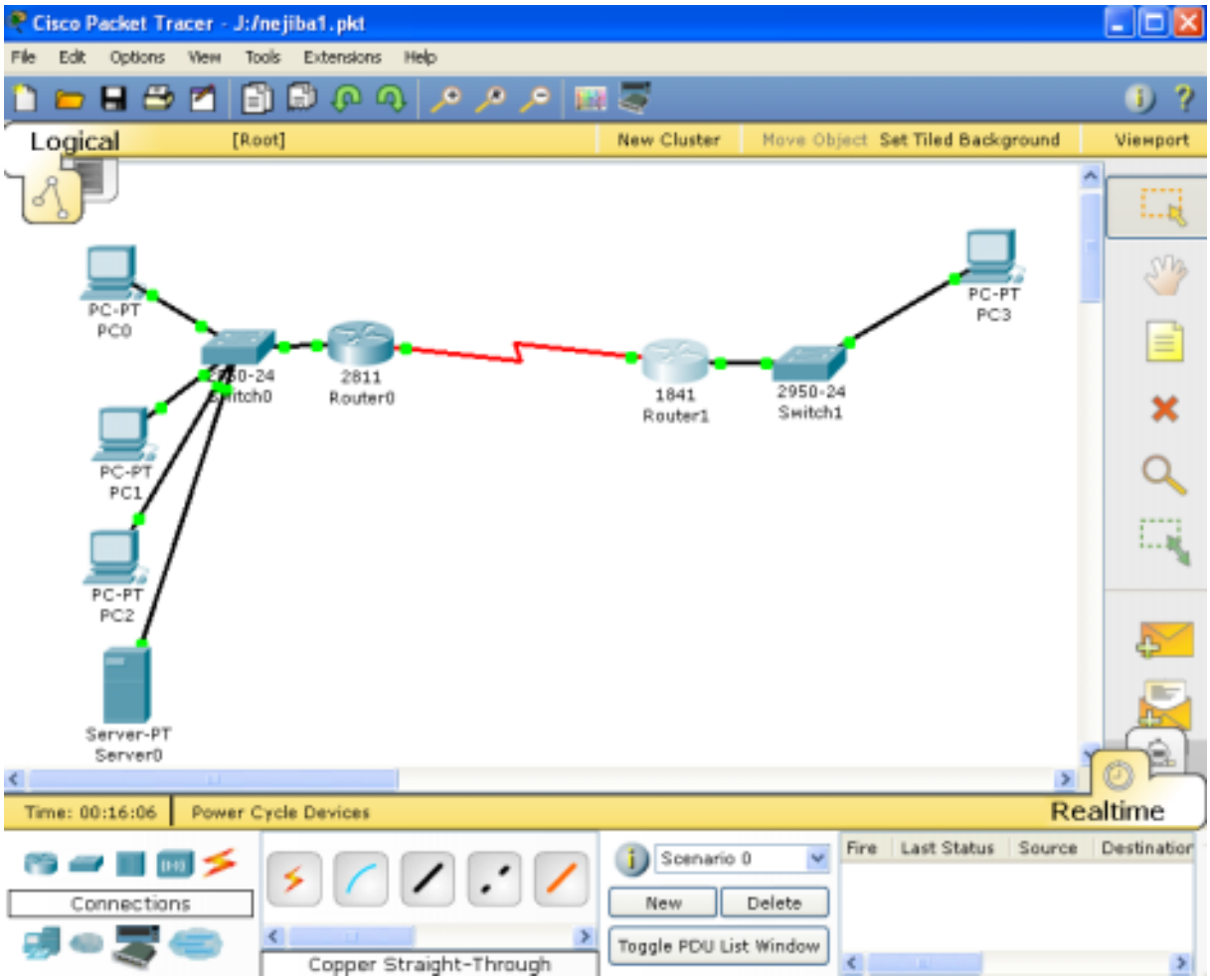


Figure 29 : Schéma d'un réseau

- **Configuration d'un équipement**

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet Tracer), il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant 3 onglets : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur Web).

Dans l'onglet Config, il est possible de configurer la passerelle par d´efaut, ainsi que l'adresse du serveur DNS (cliquez pour cela sur le bouton Settings en-dessous du bouton Global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquez pour cela sur le bouton FastEthernet en-dessous du bouton INTERFACE)

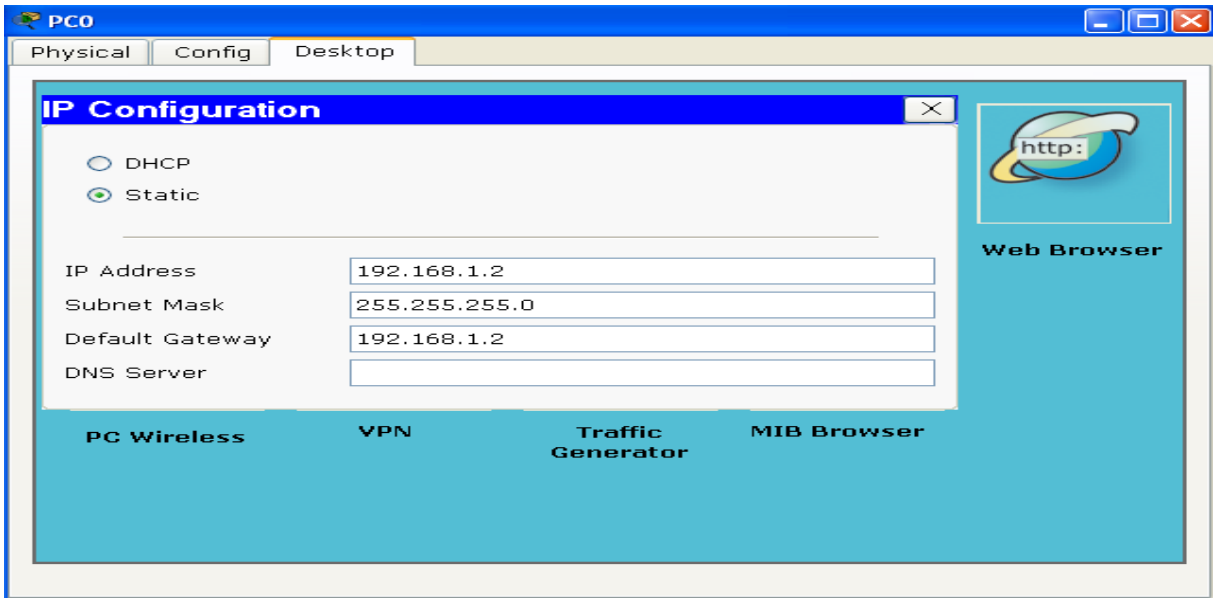


Figure 30 : Configuration des machines

2. Définition de la politique de sécurité du routeur

La politique de sécurité d'un routeur dans une entreprise est une exigence qui découle de la politique appliquée sur le Système d'information.

La politique ne donne fruit que lorsqu' on a une stratégie de sécurité dans l'entreprise.

La stratégie de sécurité, qui est une déclaration formelle des règles qui doivent être respectées par les personnes ayant accès aux ressources technologiques et données vitales de l'entreprise, définit un ensemble de fonctions qui participe à réussite et la mise en place d'une telle politique de sécurité.

2.1 Les check-lists DISA de sécurité Routeur Cisco

La politique de sécurité pour un routeur la plus recommandée est celle de DISA (Defense Information Systems Agency) qui définit une ensemble de exigences et des procédures pour la sécurité d'un routeur Cisco.

Cette liste doit être utilisée pour l'audit d'un environnement qui comporte des routeurs Cisco. La liste de contrôle fournit les considérations de sécurité lors d'un audit technique et exclut les considérations d'emploi, comme des considérations de sécurité physique. Avant d'utiliser cette considération liste de contrôle devrait être donnée à ce qui suit:

- Emplacement du routeur:

Il est important de vérifier l'emplacement du routeur sur le réseau car cela a un impact sur certains éléments de sécurité, par exemple désactivation du service SSL n'est pas appropriée lorsque le routeur est de routage du trafic vers un serveur web externe.

- Aspect pratique des recommandations de sécurité:

La liste des listes des considérations de sécurité de nombreux, qui ne peut être pratique, car elle pourrait nuire aux performances du réseau. Il est important de déterminer le risque de ne pas avoir attribué à certains éléments de sécurité et si la direction a décidé d'accepter le risque de ne pas avoir ces éléments.

- Atténuer les contrôles:

Le contrôle des routeurs Cisco ne peut pas être effectuée dans le vide. L'auditeur doit prendre en compte l'impact de la sécurité dans d'autres éléments, par exemple pare-feu, système d'exploitation hôte, etc Une faiblesse en matière de sécurité au niveau du routeur peut être atténué par un contrôle rigoureux au niveau du firewall par exemple filtrage des ports qui ne sont pas 80,23, etc

- Interopérabilité:

Dans des circonstances où le routeur utilise la fonctionnalité d'autres éléments dans l'environnement par exemple un serveur syslog pour enregistrer les événements de routeurs Cisco ou une station de gestion SNMP, l'auditeur doit examiner la sécurité sur les autres éléments. Cette liste ne fournit pas les considérations de sécurité pour ces autres éléments.

- Applicabilité des considérations de sécurité:

Cette liste de contrôle pour les tentatives de fournir une liste complète de tous les éléments de sécurité à considérer lors d'une vérification du routeur Cisco, cependant, dans certains environnements certains éléments peuvent ne pas être applicable, par exemple dans un environnement Windows, il n'est pas nécessaire de se préoccuper de filtrer les services rlogin ou ssh.

- Serveurs de réseau:

Cette liste ne comprend pas les considérations de sécurité pour le système d'exploitation exécutant TACACS ou RADIUS.

2.2 Les étapes d’une politique de sécurité réseau

Une politique de sécurité d’un routeur doit passer par les étapes suivantes :

1. Gestion de la sécurité routeur (mesures de sécurité de bases)
2. Sécurisation des accès administratifs à distances des routeurs

3. Journalisation de l'activité du routeur
4. Sécurisation des services et des interfaces vulnérables du routeur
5. Sécurisation des protocoles de routage
6. Contrôle et filtrage du trafic

La politique de sécurité peut commencer avant même l'acquisition et le déploiement du routeur.

2.2.1 Politique d'acquisition

Avant d'acquérir un routeur, il convient de définir une politique d'acquisition.

- Quelles sont les fonctionnalités auxquelles nous souhaitons que le routeur assure?
- Quel constructeur choisir?
- Quel est la garantie?
- Le support est- il assuré ?
- Faut-il un contrat de maintenance ?

Ce sont quelques questions dont les réponses doivent figurer dans la politique d'acquisition.

2.2.2 Politique de déploiement ou de mise en œuvre

Une fois le routeur acquis, il convient de définir une politique de mise en œuvre. Cette politique devra tenir compte de son installation, de sa configuration et de sa mise en service. Par exemple, il doit être placé dans un endroit sécurisé (accès protégé), derrière un dispositif de protection comme un pare-feu par exemple.

2.3.3 Gestion de sécurité du routeur ou mesures de base de sécurité :

- Politique de mot de passe

Les routeurs présentent plusieurs types et niveaux d'accès (telnet, ligne virtuelle (vty), http, ligne auxiliaire, mode enable, etc.). Chacun de ces accès est protégé par un mot de passe. Une politique de mots de passe doit être définie et appliquée pour éviter leur compromission. Par exemple, les mots de passe doivent être changés suivant une périodicité (tous les trois mois par exemple). Ils doivent être forts, c'est à dire composé des chiffres, caractères spéciaux (@§!&#), majuscules et minuscules. Ceci permet d'éviter les attaques par dictionnaire ou par force brute.

2.3.4 Politique de durcissement

Il convient de définir une politique de durcissement du routeur. Par exemple, en définissant les rôles et responsabilités des différents intervenants (administrateur réseaux, fournisseurs, etc.), les services et comptes inutiles à désactiver, les types d'accès autorisés, la politique de sauvegarde de la configuration, etc... .

2.3.5 Politique de journalisation

Un routeur étant un équipement sensible, il est important de le surveiller afin d'avoir une idée sur ses différentes activités (trafic, connexion, etc.). Cette surveillance passe par les fichiers journaux générés par celui ci. Il convient donc de définir une politique de journalisation. Par exemple, comment doivent être utilisé les fichiers journaux, où doivent-ils être stockés ? L'envoi des fichiers journaux (log) vers un serveur centralisé (syslog par exemple) doit être sécurisé, une sauvegarde d'une copie des logs doit être réalisée.

3.Application de la politique de sécurité

3.1 Sécurisation mots de passe et privilèges

- **Configuration des mots de passe de routeur**

Cette commande permet d'attribuer un mot de passe pour le mode configuration

```
pfe(config)#enable pass
pfe(config)#enable password uvt@2011
pfe(config)#end
pfe#
%SYS-5-CONFIG_I: Configured from console by console
```

Vérification

```
pfe#show run
Building configuration...

Current configuration : 595 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname pfe
!
!
!
enable password uvt@2011
```

- **Chiffrement de mot de passe**

Cette commande permet de secret le mot de passe

```
pfe(config)#enable secret uvt@2011
pfe(config)#end
pfe#
%SYS-5-CONFIG_I: Configured from console by console
pfe#sh
pfe#show run
Building configuration...

Current configuration : 642 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname pfe
!
!
!
enable secret 5 $1$mERr$yKOp76DC95hMW.TXwzLNml
```

- **Activer le service de cryptage**

```
pfe(config)#service password-encryption
pfe(config)#end
```

Vérification

```
pfe#show run
Building configuration...

Current configuration : 651 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname pfe
!
!
!
enable secret 5 $1$mERr$yKOp76DC95hMW.TXwzLNml
enable password 7 08345A5A294B554643
```

- **Application d'une longueur de mot de passe minimale**

```
pfe(config)#security passwords min-length 10
```

- **Utilisateurs et niveaux de privilèges**

Les configurations d'accès vues précédemment se limitent à empêcher n'importe qui d'accéder à des services statiques. L'lOS Cisco permet toutefois de définir des tables d'utilisateurs et de leur accorder jusqu'à 16 niveaux (de 0 à 15) de privilèges (définir, par exemple, les commandes accessibles par privilège). Lorsque les services sont restreints par défaut, c'est le plus haut niveau qui est défini (15)

- Niveau de privilège 1 = le niveau par défaut pour la connexion,
- Niveau de privilège 15 = privilégiés (invite routeur #), le niveau après la mise en activer le mode,
- Niveau de privilège 0 = niveau de privilège rarement utilisé, mais comprend 5 commandes: désactiver, activer, la sortie, Aide et Déconnexion.

3.2 Désactiver les services et interfaces non utilisés

Un certain nombre de services peuvent être activés sur le matériel Cisco. Selon les versions de l'IOS ces services sont activés par défaut, mais sont bien souvent inutiles

- **Finger**

Ce service peut révéler à une personne mal intentionnée et non autorisée des informations sur les utilisateurs connectés. :

```
pfe(config)#no service finger
```

- **UDP small server et tcp small server**

Ces deux services représentent les services echo, chargen, discrad et daytime avec les protocoles UDP et TCP. Ces services peuvent être exploités pour obtenir indirectement des informations sur le système cible ou effectuer des Dénis de services.

```
pfe(config)#no service tcp-small-server
pfe(config)#no service udp-small-server
```

- **Bootp**

Bootp est un protocole permettant à une machine de booter sur le réseau. Ce service permet à un routeur d'être utilisé comme serveur Bootp pour les autres routeurs.

```
pfe#no ip bootp server
```

- **Requêtes TFTP**

Les routeurs Cisco émettent des requêtes TFTP à intervalles réguliers pour vérifier l'intégrité de leur configuration. Cela peut présenter un risque de sécurité, il est conseillé de le désactiver.

```
pfe(config)#no service config
```

- **Cisco Discovery Protocol**

CDP est un protocole activé par défaut sur le matériel Cisco fournissant de nombreuses informations sur les équipements voisins comme les interfaces du routeur auxquelles ils sont connectés, leur numéro de modèle, etc. Une personne mal intentionnée pourrait utiliser les informations fournies par CDP pour parvenir à ses fins.

```
pfe(config)#no cdp run
```

- **Proxy arp(En mode de configuration d'interface)**

Le proxy arp est utilisé sur les routeurs lorsqu'un PC du réseau ne dispose pas de passerelle pour joindre un autre réseau. Si celui-ci ne dispose pas d'une adresse de passerelle et possède un masque lui faisant croire être dans le même réseau que l'hôte du réseau distant, alors il enverra une simple requête ARP pour le joindre et c'est le routeur qui y répondra grâce au proxy arp. Le routeur se fera donc passer pour la machine distante en répondant à sa place, d'où le nom proxy arp.

```
pfe(config-if)#no ip proxy arp
```

- **Désactivé le port auxiliaire**

Assurer que le port auxiliaire est désactivé avec une configuration similaire à la suivante

```
pfe(config)#line aux 0
pfe(config-line)#no exec
pfe(config-line)#transport input none
```

3.3 Sécuriser l'accès Telnet

- **1er solution : Limiter l'accès au routeur :**

Modifier le port d'écoute Telnet

Router(config)#line vty 0 4

Router (config)# rotary

La commande rotary met Telnet sur le port 3000. Pour spécifier le numéro de port, il est possible d'ajouter un nombre à 30000.Par exemple rotary 50 changera le port d'écoute à 3050.

Limiter l'accès par Telnet

Pour limiter les accès on utilise une Access Liste

```
pfe(config)#access-list 10 permit 10.0.0.0 0.0.0.255
pfe(config)#line vty 0 4
pfe(config-line)#password uvt@2011000000
pfe(config-line)#access-class 10 in
pfe(config-line)#login
pfe(config-line)#exec-timeout 1 30
pfe(config-line)#exit
```

La commande Access-List simplifiée n'autorise que le réseau d'adresse10.0.0.0/24.

La commande Access-Class 10 active l'Access-List 10 sur les vty 0 à 4.

Enfin, il est recommandé de mettre une temporisation pour déconnecter la session en cas d'inactivité, à l'aide de la commande Exec-Timeout mm ss où mm est le temps en minute et ss le complément en secondes.

- **2eme solution: T.A.C.A.C.S**

Les authentifications de type TACACS permettent de gérer des comptes individuels d'accès associés à des types de profils définis, dans lesquels les commandes autorisées sont clairement spécifiées et limitées. On filtre ainsi les classes d'adresses IP autorisées à accéder au routeur, tout en limitant les temps de connexion au routeur sans activité.

Il existe 3 versions, 1 ancienne (époque ARPANET) en UDP, 1 version moins ancienne, en TCP, et une dernière, avec une bonne prise en compte de la sécurité (TACACS+).

La dernière version fait bien la séparation entre les trois A : on peut les mettre sur 3 services différents.

- Protocole d'authentification :

  Start

  Reply : début de transaction entre client (routeur) et serveur

  Renvoi d'AVP (Attribute Value Pair) par le serveur

  Request Response, envoi d'autres AVP.

- Protocole d'accounting :

  Start

  Stop

  Watchdog

  More

On ajoute un serveur Taccas

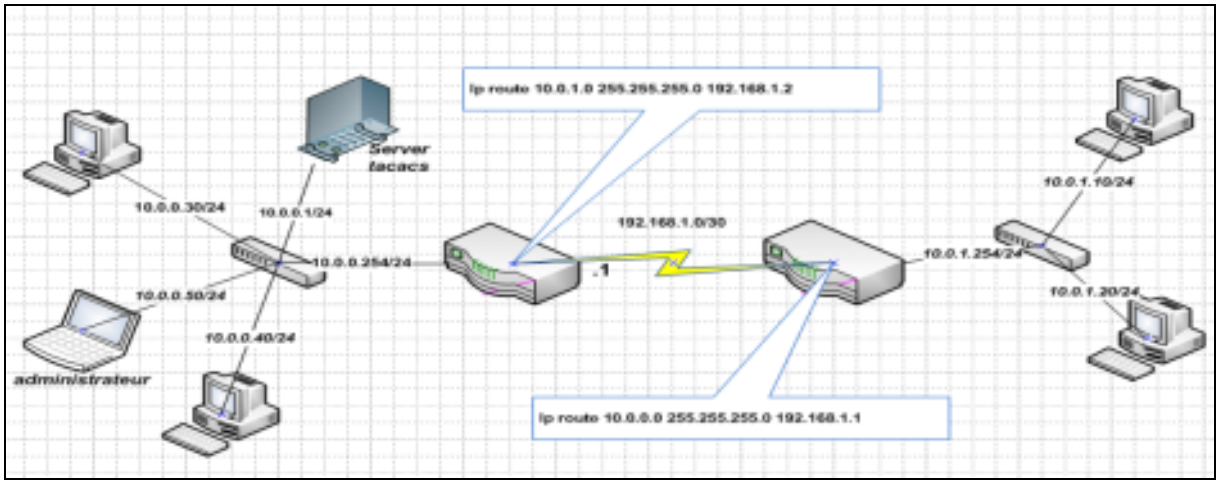


Figure 31 : schéma d'un réseau avec serveur Taccas

–Configuration du routeur :

Les commandes suivant est pour configurer un client Tacacs (le routeur)

```
pfe(config)#aaa new-model
pfe(config)#aaa authentication login tel
pfe(config)#aaa authentication login telnet group tacacs+ local
pfe(config)#tacacs-server host 10.0.0.1
pfe(config)#tacacs-server key uyt-mnt
pfe(config)#line vty 0 4
pfe(config-line)#login authentication telnet
pfe(config-line)#exec
pfe(config-line)#exec-timeout 1 30
```

Pour fonctionner, le service AAA doit être activé sur le routeur avec la commande suivante: « **aaa new-model**. »

La commande « aaa authentication login »permet de **référer à un ensemble de défini précédemment** TACACS + serveurs

Définition des adresses IP des serveurs TACACS ainsi que une clé utilisée pour l'authentification des serveurs.

TACACS-server host {IP}

TACACS-server key {clé}

La commande « login authentification » permet d'active le model Tacacs+ à la ligne Telnet

Un accès administratif au routeur, un seul compte est défini localement sur le routeur pour une utilisation dans un cas d'urgence (serveur d'authentification tombe en panne)

```
pfe(config)#username administrateur password admin-iYUh
```

- **3eme solution L'utilisation du protocole SSH**

SSH ('**S**ecure **SH**ell') est un protocole hautement sécurisé, de conception récente. L'utilisation du protocole SSH au lieu de Telnet pour se connecter à distance au routeur permet de faire diminuer sensiblement les menaces car :

La signature numérique d'un serveur fournit la vérification pour son identité.

La communication complète entre un système client et un système serveur (routeur) ne peut être utilisé si elle est interceptée car tous les paquets sont chiffrés.

Il n'est pas possible d'usurper l'identité d'un des deux systèmes, parce que les paquets sont chiffrés et leurs clés ne sont connues que par les systèmes locaux et distants.

```
pfe(config)#line vty 0 4
pfe(config-line)#no transport input
pfe(config-line)#end
```

La commande « Line vty 0 4 » permet de entrer en mode de configuration de ligne telnet

La commande « no transport input » désactiver les lignes virtuelle

La commande « transport input SSH » permet d'activer le SSH

– Configuration de SSh :

Etape1 : Réglage des parmètres du routeur

```
Router(config)#hostname R2
R2(config)#
```

Etape2 : Définition du nom de domaine

```
R2(config)#ip domain-name cisco.com
```

Etape 3 :Génération de clés asymétriques

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 400
% Generating 400 bit RSA keys, keys will be non-exportable...[OK]
```

Etape 4 :Configuration de l'authentification locale et VTY

```
R2(config)#username student secret cisco
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#
```

Etape 5 :Configuration des détails d'attente SSH

```
R2(config)#ip ssh time-out 15
R2(config)#ip ssh authentication-retries 2
```

3.3.1 Sécurisé le protocole de gestion SNMP :

Il faut :

- Modifier le nom de communauté par défaut (comme public et private).
- Utiliser la version 3 du protocole qui ajoute la sécurité : authentification, intégrité et confidentialité des données.
- Configurer le routeur de telle façon qu'il filtre le trafic SNMP provenant seulement des machines légitimes. (on n'autorise que l'administrateur)

```
pfe(config)#access-list 10 permit host 10.0.0.40
pfe(config)#snmp-server community ro 10
```

- **Access-list contre le spoofing**

L'Access-List suivante interdit l'accès au réseau pour tous les datagrammes en provenance de l'extérieur, dont :

L'adresse source est locale (127.0.0.0, 0.0.0.0)

L'adresse source est privée (10.0.0.0, 172.16.0.0 et 192.168.0.0),

L'adresse source est une adresse multicast (224.0.0.0) ou broadcast (255.255.255.255)

L'adresse source est sur le réseau interne

```
access-list 100 deny IP 127.0.0.0 0.255.255.255 any
access-list 100 deny IP 10.0.0.0 0.255.255.255 any
access-list 100 deny IP 224.0.0.0 31.255.255.255 any
access-list 100 deny IP host 0.0.0.0 any
access-list 100 deny IP host 255.255.255.255 any
access-list 100 deny IP 192.168.0.0 0.0.255.255 any
access-list 100 deny IP 172.16.0.0 0.0.255.255 any
access-list 100 deny IP numéro-sous-réseau masque-sous-réseau  any
access-list 100 permit IP any any
```

Cette Access-List doit être appliquée sur toutes les interfaces externes à l'aide de lacommande suivante:

IP Access-Group 100 in

Il est possible aussi de limiter le spoofing sur le réseau interne. L'Access-List suivante ne peut pas empêcher un utilisateur d'usurper une autre adresse IP du réseau, mais elle l'empêche d'usurper une adresse externe.

Access-List 101 permit IP 10.0.10.0 10.0.10.254 any

Access-List 101 deny IP any any

Elle est appliquée sur l'interface du réseau interne:

IP Access-Group 101 in

3.3.2 Contre attaque Synflood

L'administrateur doit utiliser la commande TCP intercept pour protéger contre les attaques SYN Flood. Grâce à cette commande le routeur intercepte l'établissement d'une connexion TCP, et détermine si l'adresse source est joignable .Si la machine est joignable le routeur permet la connexion, sinon il empêche la connexion. La configuration doit être au :

IP TCP intercept list 107
Access-List 107 permit TCP any 10.0.0.0 255.255.255.0
Access-List 107 deny IP any any
Interface eth0
IP Access-Group 107 in
Exit

3.3.3 Contre l'utilisation Frauduleuse du protocole ICMP

- Rejet des broadcasts dirigés

Un broadcast dirigé permet d'envoyer un datagramme vers toutes les stations d'un réseau, même distants. Cette technique est utilisée dans les attaques de type Smurf.

- No IP directed-broadcast

Cette commande appliquée sur chaque interface du routeur a pour effet de ne pas propager les broadcasts dirigés. C'est la configuration par défaut à partir de la version IOS 12.0.

- Désactivation du routage des redirections ICMP

Les messages ICMP redirect permettent de modifier les tables de routage des équipements.

L'utilisation de messages ICMP redirect peut aussi altérer la politique de routage définie par l'administrateur du réseau. Il est donc prudent de rejeter ces messages.

- No IP redirect

Cette commande appliquée sur chaque interface indique que le routeur ne doit ni générer, ni accepter de paquets ICMP Redirect.

3.3.4 Mise en place d'un serveur log (syslog)

Le Syslog se compose d'une partie cliente et d'une partie serveur. La partie cliente émet les informations sur le réseau, via le port UDP 514. Les serveurs collectent l'information et se chargent de créer les journaux.

L'intérêt de Syslog est donc de centraliser les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau.

Il existe aussi un logiciel appelé Syslog, qui est responsable de la prise en charge des fichiers de journalisation du système.

```
pfe(config)#logging 10.0.0.1
pfe(config)#%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.0.0.1 port 514 star
ted - CLI initiated
pfe(config)#logging trap debugging
pfe(config)#SERvice timestamps debug datetime msec
pfe(config)#SERvice timestamps log datetime msec
pfe(config)#
```

La commande « logging Ip » Active la journalisation des messages système à un hôte distant

La commande « logging trap » Afin de limiter les messages enregistrés sur les serveurs syslog fonction de la gravité, utilisez la commande trap enregistrement en mode de configuration globale. Pour revenir les hôtes exploitation à distance au niveau par défaut

La commande “service timestamps [debug | log] [uptime | datetime [msec] [localtime] [show-timezone] [year]] ” utilisé pour configurer le système pour appliquer un horodatage des messages de débogage ou de messages de journalisation système, utilisez la commande service timestamps en mode de configuration globale. Pour désactiver ce service, utilisez la forme no de cette commande.

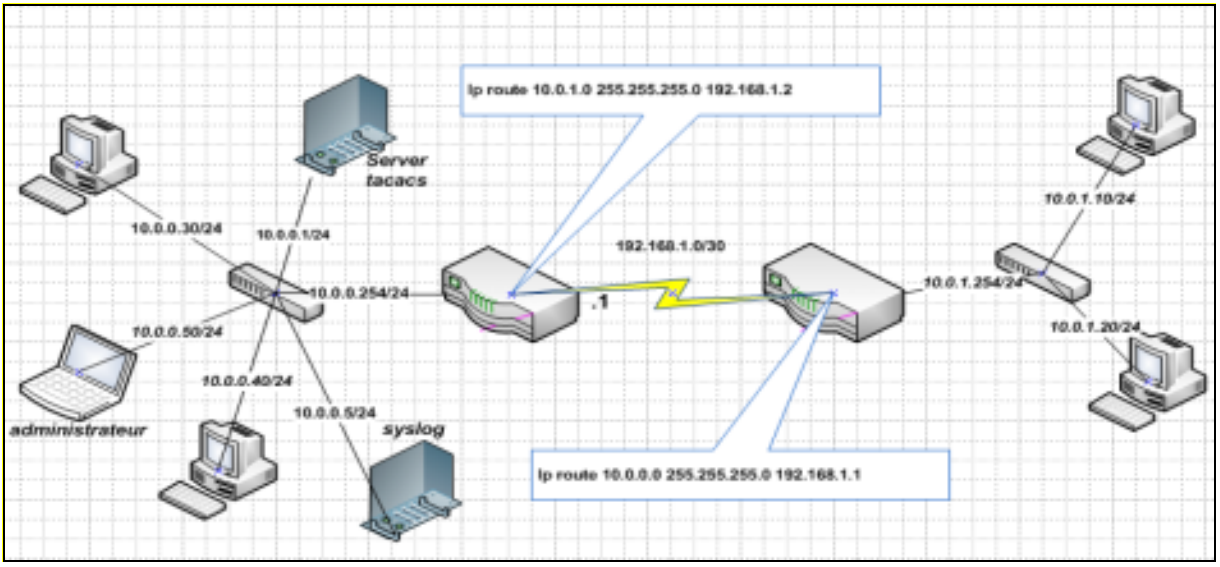


Figure 32: Mise en place d’un serveur log (syslog)

- **Détection des sniffer**

En principe, les sniffers sont indétectables puisque ne générant aucun trafic, se contentant d'être passif, en écoute active. Il existe des outils pour essayer de les piéger. Voici quelques méthodes utilisées pour tenter d'opérer cette détection.

- **Le contrôle des temps de latence**

La méthode consiste à produire une surcharge de travail pour l'hôte suspect. On teste le délai des réponses à diverses requêtes, avant la surcharge. Puis on surcharge le réseau avec du trafic suspecté d'être sniffé. Ceci devrait générer une suractivité pour l'hôte sniffeur et donc 50 accroître ses temps de réponses. Les résultats permettent de renforcer la suspicion ou de disculper l'hôte en question.

- **La méthode Ping**

Cette méthode permet d'identifier les interfaces réseau en mode **promiscuous**, autrement dit celles sur lesquelles écoute un sniffer. Une interface Ethernet ne répond en principe qu'aux trames qui lui sont destinées.

1. On construit un paquet **ICMP Echo Request** à destination de l'adresse IP de l'hôte surveillé dans lequel l'adresse MAC destination a été modifiée (i-e différente de celle de l'hôte surveillé).

2. Si l'hôte est en mode normal, le filtre MAC joue son rôle, le démultiplexage des couches supérieures ne se fait pas, l'adresse IP destination n'est pas reconnue et il n'y a donc pas de réponse à cette requête.

3. Si maintenant il est en mode **promiscuous**, le filtre n'opère plus, le démultiplexage a lieu, l'adresse IP est reconnue et une réponse est renvoyée.

Si le sniffer prévoit la mise en place d'un filtre d'adresse MAC, la méthode devient inefficace.

On peut affiner cette approche par l'utilisation de paquets corrompus, devant produire une réponse **ICMP error**.

3.3.5 Sécurisation des protocoles de routage

- Exigence:

Authentification MD5 voisin doit être mis en œuvre pour tous les protocoles de routage avec tous les routeurs par les pairs au sein même ou entre systèmes autonomes (AS).

- Procédure:

Déterminer quels sont les protocoles de routage ont été mis en œuvre sur le bord externe avec leurs pairs ainsi que l'intérieur. À l'exception de l'extérieur ou NIPRN et pairs SIPRN et l'authentification du prochain doit être implémentée en utilisant MD5. Les

protocoles de routage suivant le support MD5: BGP, OSPF, IS-IS, EIGRP et RIP V2. Voici quelques exemples de configuration pour le protocole BGP, OSPF, EIGRP et l'authentification voisine.

BGP

router bgp 100

neighbor external-peers peer-group

neighbor 171.69.232.90 remote-as 200

neighbor 171.69.232.90 peer-group external-peers

neighbor 171.69.232.100 remote-as 300

neighbor 171.69.232.100 peer-group external-peers

neighbor 171.69.232.90 ***password*** *xxxxxxxxxx*

neighbor 171.69.232.100 password xxxxxxxxxx

Note: La déclaration mot de passe voisin peut être appliquée à des groupes de pairs ou de la définition voisine.

OSPF

interface Ethernet0

ip address 10.10.10.10 255.255.255.0

ip ospf message-digest-key 10 md5 mypassword

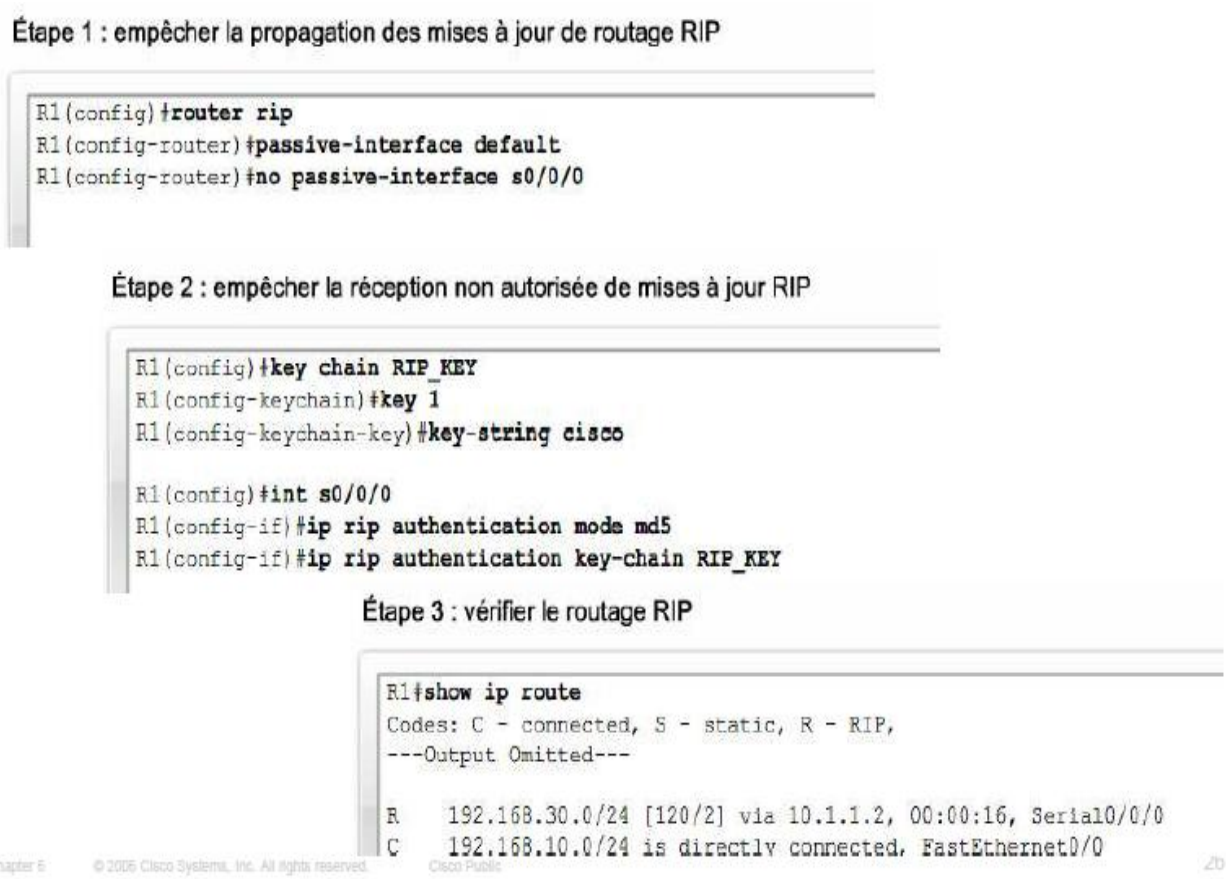
router ospf 10

network 10.10.0.0 0.0.255.255 area 0

area 0 authentication message-digest

Note: D'authentification doit être activée pour chaque zone. Dans OSPF, une interface appartient à un seul domaine; donc, il y aurait toujours une déclaration de réseau sous l'ID de processus OSPF pour chaque interface qui a un trafic OSPF. La déclaration de réseau définit la zone dans laquelle le réseau appartient. Le key_id MD5 et mot de passe est défini pour chaque interface connectée à un voisin OSPF.

Configuration de RIPv2 avec authentification



EIGRP

interface Ethernet0

ip address 10.10.10.10 255.255.255.0

ip authentication mode eigrp 1 md5

ip authentication key-chain eigrp 1 mypassword

.

.

.

key chain mypassword

key 12345

key-string abcdefg

accept-lifetime infinite

.

.

.

router eigrp 1

network 10.0.0.0

no auto-summary

3.3.6 Contrôle et filtrage du trafic

Listes d'accès sont utilisés pour contrôler et gérer l'accès d'intéressant et non de trafic intéressant.

Listes d'accès sont des outils puissants pour contrôler l'accès vers et à partir de deux segments de réseau. Ils peuvent filtrer les paquets inintéressants et être utilisées pour mettre en œuvre les politiques de sécurité. En utilisant la bonne combinaison de listes d'accès, gestionnaires de réseau sera armé avec le pouvoir de faire appliquer une politique d'accès près qu'ils peuvent inventer. Après les listes sont construites, elles peuvent être appliquées soit à l'arrivée ou le trafic sortant sur une interface. En appliquant des listes d'accès du routeur peut effectuer pour analyser chaque paquet en passant par l'interface spécifique à la direction et également prendre des mesures.

Les ACL, ou Access Control List permettent de filtrer ce qui entre ou sort par les interfaces d'un routeur, en fonction :

- De l'IP Source.
- De l'IP de destination
- Du port source
- Du port de destination
- Du protocole (IP, TCP, UDP, ICMP)

Il est possible d'autoriser ou d'interdire les paquets IP. Une ACL contient plusieurs règles qui sont lues séquentiellement jusqu'à ce que l'une d'elles corresponde au paquet traité. La lecture de la liste s'arrête alors.

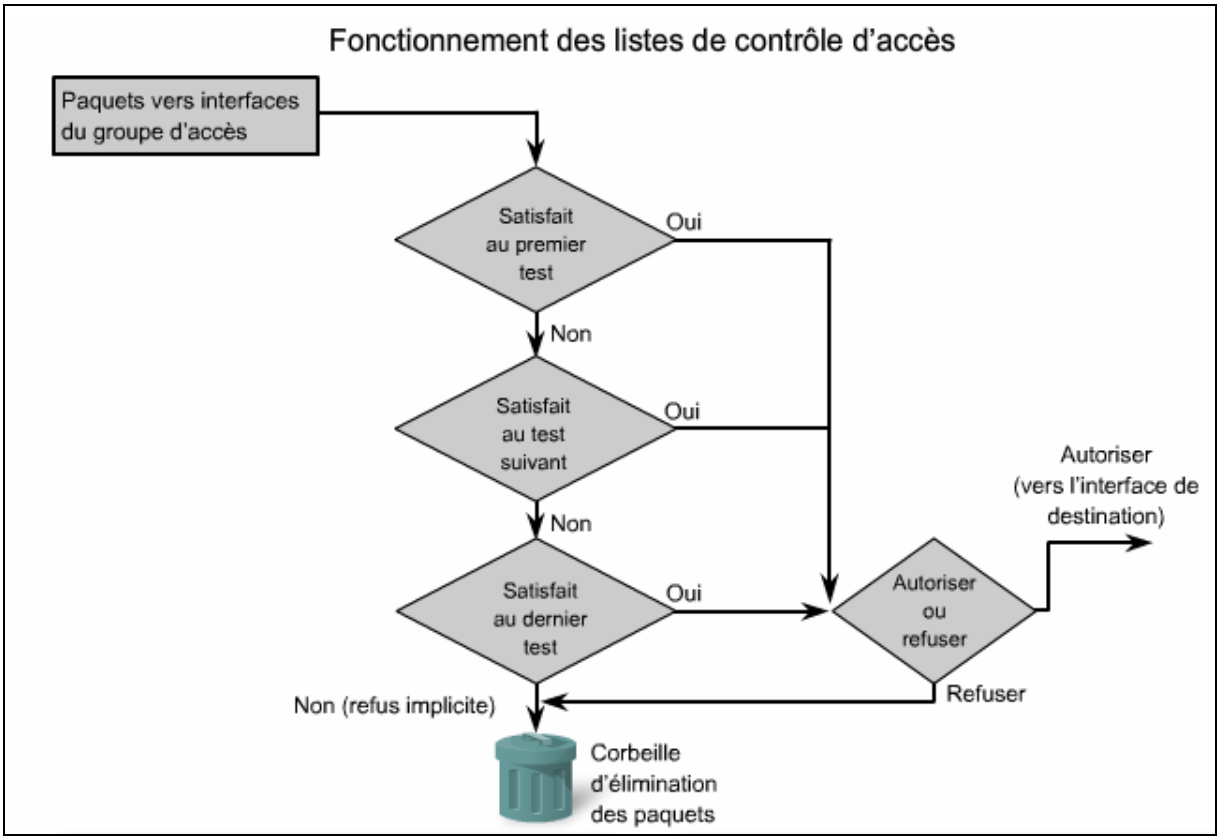


Figure 33:Fonctionnement des listes de contrôle d'accès

- **Types d'ACL**

On distingue les types d'ACL selon le type de protocole de niveau 3 concerné. Ainsi, sur les routeurs CISCO on peut voir grâce à l'instruction access-list ? cette liste (Il faut être en mode de configuration)

```
<1-99> IP standard access list
<100-199> IP extended access list
<200-299> Protocol type-code access list
<300-399> DECnet access list
<600-699> Appletalk access list
<700-799> 48-bit MAC address access list
<800-899> IPX standard access list
<900-999> IPX extended access list
<1000-1099> IPX SAP access list
<1100-1199> Extended 48-bit MAC address access list
<1200-1299> IPX summary address access list
<1300-1999> IP standard access list (expanded range)
<2000-2699> IP extended access list (expanded range)
```

Figure 34: les types d'ACL

Les plus utilisées sont les **<100-199> IP Extended Access List**, car ce sont souvent des paquets IP qui transitent, notamment sur l'internet

- **Masque générique**

Les ACL permettent de désigner des groupes d'adresses grâce à l'utilisation d'un masque générique. Dans un masque générique, les 0 signifient qu'il faut vérifier la valeur du bit correspondant, et les 1 signifient qu'il faut l'ignorer.

Une ACL s'applique en deux temps :

–Identification du ou des flux (définition de l'ACL) : *access-list*

–Application des règles à une interface (application de l'ACL) : *access-group*

Il faut de plus définir le sens sur lequel l'ACL agit, c'est à dire si c'est en entré ou en sortie (In ou Out).Il existe 2 types ACL :

- **Liste d'accès standard :**

access-list number { deny | permit } source masque générique

- **Liste d'accès étendu :**

access-list 100-199 {permit|deny} {ip|tcp|udp|icmp} source source-mask [lt|gt|eq|neq]

[source-port] destination dest-mask [lt|gt|eq|neq] [dest-port] [log]

- **Méthode souhaité**

La création, la mise à jour, le débogage nécessitent beaucoup de temps et de rigueur dans la syntaxe Il est donc conseillé

De créer les ACL à l'aide d'un éditeur de texte et de faire un copier/coller dans la configuration du routeur

Placer les extended ACL au plus près de la source du paquet que possible pour le détruire le plus vite possible

Placer les ACL standard au plus près de la destination sinon, vous risquez de détruire un paquet trop top

Rappel : les ACL standard ne regardent que l'IP source

Placer la règle la plus spécifique en premier

Avant de faire le moindre changement sur une ACL, désactiver sur l'interface concerné celle-ci (no ip access-group)

- **Exemples des Access-List**

– Exigence :

Les administrateurs routeur restreindre le routeur principe d'accepter tous les paquets entrants qui contiennent une adresse IP du réseau interne, une boucle d'accueil locales de retour d'adresse (127.0.0.0 / 8), la gamme lien-local adresse IP(169.254.0.0/ 16), ou toute autre adresse réservés privé dans le domaine source

– Procédure :

Examen du principe configuration des routeurs Cisco pour assurer ACL sont en place pour restreindre les adresses IP entrantes.

interface *FastEthernet 0/0*

description to NIPRNet core router

ip address 199.36.92.1 255.255.255.252

ip access-group ***100 in***

.

.

access-list 100 deny ip <internal network range> <wildcard mask> any log

access-list 100 deny ip 0.0.0.0 0.255.255.255 any log

access-list 100 deny ip 10.0.0.0 0.255.255.255 any log

access-list 100 deny ip 127.0.0.0 0.255.255.255 any log

access-list 100 deny ip 169.254.0.0 0.0.255.255 any log

access-list 100 deny ip 172.16.0.0 0.15.255.255 any log

access-list 100 deny ip 192.0.2.0 0.0.0.255 any log

access-list 100 deny ip 192.168.0.0 0.0.255.255 any log

access-list 100 deny ip 224.0.0.0 15.255.255.255 any log

access-list 100 deny ip 240.0.0.0 7.255.255.255 any log

- Exigence :

Le filtre d'entrée n'est pas appliquée aux interfaces externes ou l'évacuation filtre n'est pas appliqué aux interfaces internes; à la fois sur une direction d'arrivée.

Note: Tous les filtres doivent être appliqués aux interfaces appropriées sur une direction d'arrivée

- Procédure :

Examen de la configuration courante du routeur hypothèse et de vérifier que toutes les interfaces, à l'exception des interfaces de bouclage, ont l'entrée appropriée ou ACL sortie appliquée à un sens entrant.

interface *FastEthernet 0/0*

description NIPRNet link

ip address 199.36.92.1 255.255.255.252

ip access-group 101 ***in***

Remarque: Le sens par défaut pour le "ip access-group" commande est "out ".

Conclusion

Dans ce chapitre nous avons présenté la différente étape de configuration de base des routeurs Cisco qui a sollicité une bonne compréhension les procédures recommandées pour leur sécurisation ainsi prévenir les techniques d'attaques qui menacent l'intégrité du routeur.

Conclusion Générale

Le présent projet, était une opportunité pour aborder de près le domaine le plus important de nos jours, celui de la sécurité des Systèmes d'Information(SI). Nous avons examiné de prés la sécurité des routeurs CISCO qui présentent la colonne vertébrale de l'infrastructure réseaux de POLYGONE ou tout autre entreprise déployant ce type de routeur, en vu de satisfaire le besoin de la société en matière de sécurité des équipements réseaux.

La méthodologie adoptée dans ce travail consistait à cerner les vulnérabilités qui peuvent se présenter, en étudiant les techniques des attaques sur le routeur. Ces dernières exploitent les vulnérabilités dans les protocoles réseau. Ensuite, établir les procédures de sécurité pour se protéger contre ces menaces au niveau du routeur.

Nous avons également beaucoup appris les notions de la sécurité réseau, ce qui m'a permis de comprendre les techniques utilisées par les pirates et la façon de s'en protégés.

Ce travail fut aussi un apport considérable, en effet il m'a permis de m'intégrer au sein de la société POLYGONE, de s'initier à la vie professionnelle, de collaborer avec les membres de l'équipe réseau et de développer des qualités relationnelles avec l'ensemble du personnel.

Puisque tout projet n'atteint jamais le parfait, la correction des failles de sécurité n'empêche pas l'apparition de nouvelles menaces d'où la politique de sécurité doit être périodiquement auditée.

Bibliographie et Nétographie

Bibliographie

Jean François Pillou. « Tout sur la sécurité informatique», Canada, Dunod, 2005,123 pages ;

Michal Zalewski « Menaces sur le réseau », France , CampusPress, 322 pages 2004

Laurent Bloch « Sécurité informatique - Principes et méthodes », Eyrolles,2006 261 pages

Cisco IOS Router Checklist Procedure Guide (Supplement to the Network Infrastructure Checklist V6R1 DISA FIELD SECURITY OPERATIONS)

Nétographie

[1] www.tcpdump.org

[2] www.wireshark.fr

[3] www.softcities.com/telecharger-mib-browser/60214.htm

[4] www.*wiki.backtrack-fr.net*

[5] www.hping.org

http://www.ietf.org/rfc.htm

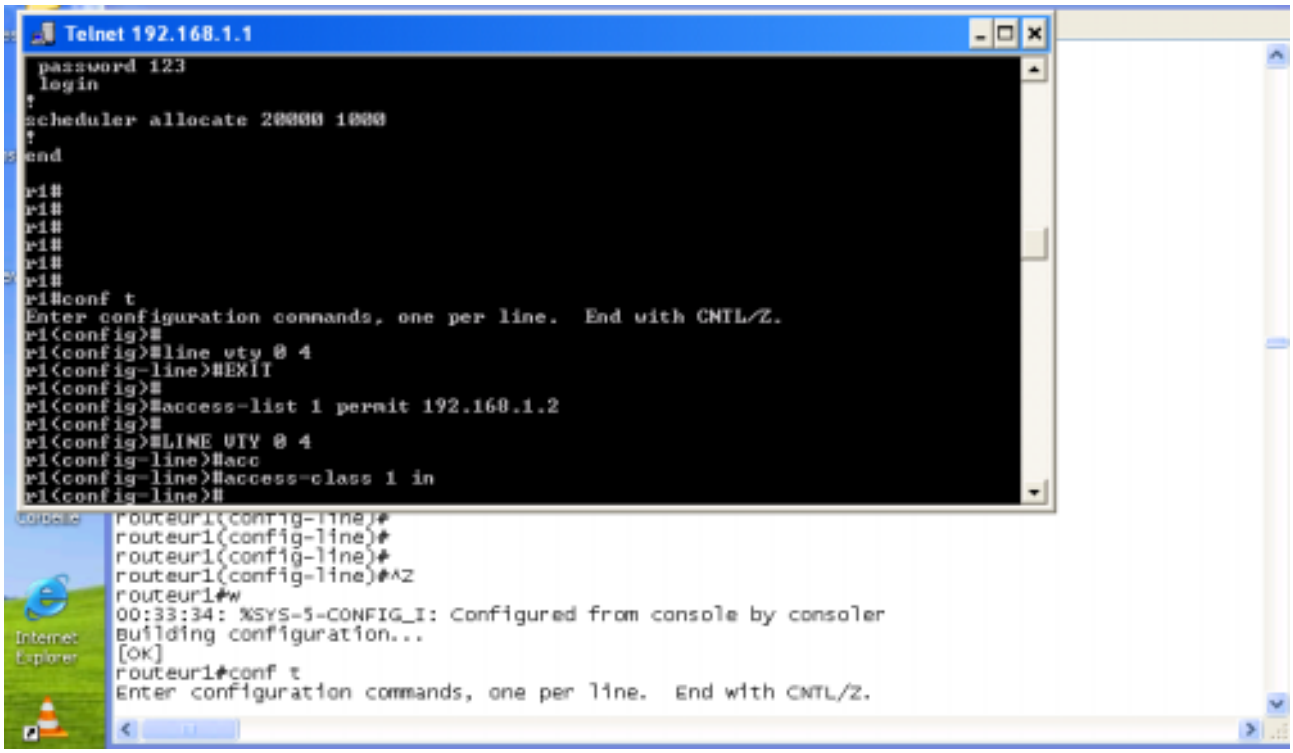
www.cisco.com

www.ansi.tn

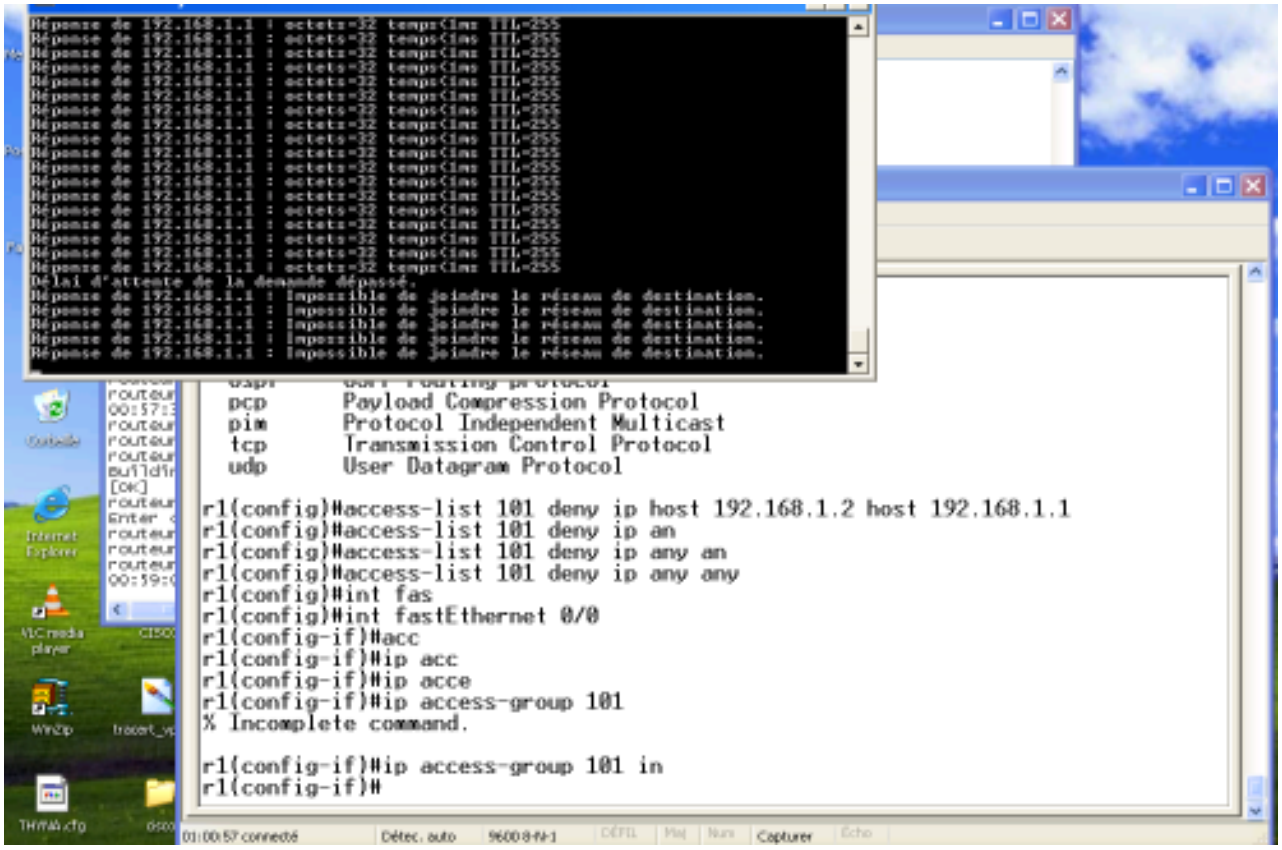
http://www2.cegep-rdl.qc.ca/prive/pr-cisco/ccna4e/doc/Exploration_Accessing_WAN_Chapter4-fr.pdf

ANNEXES

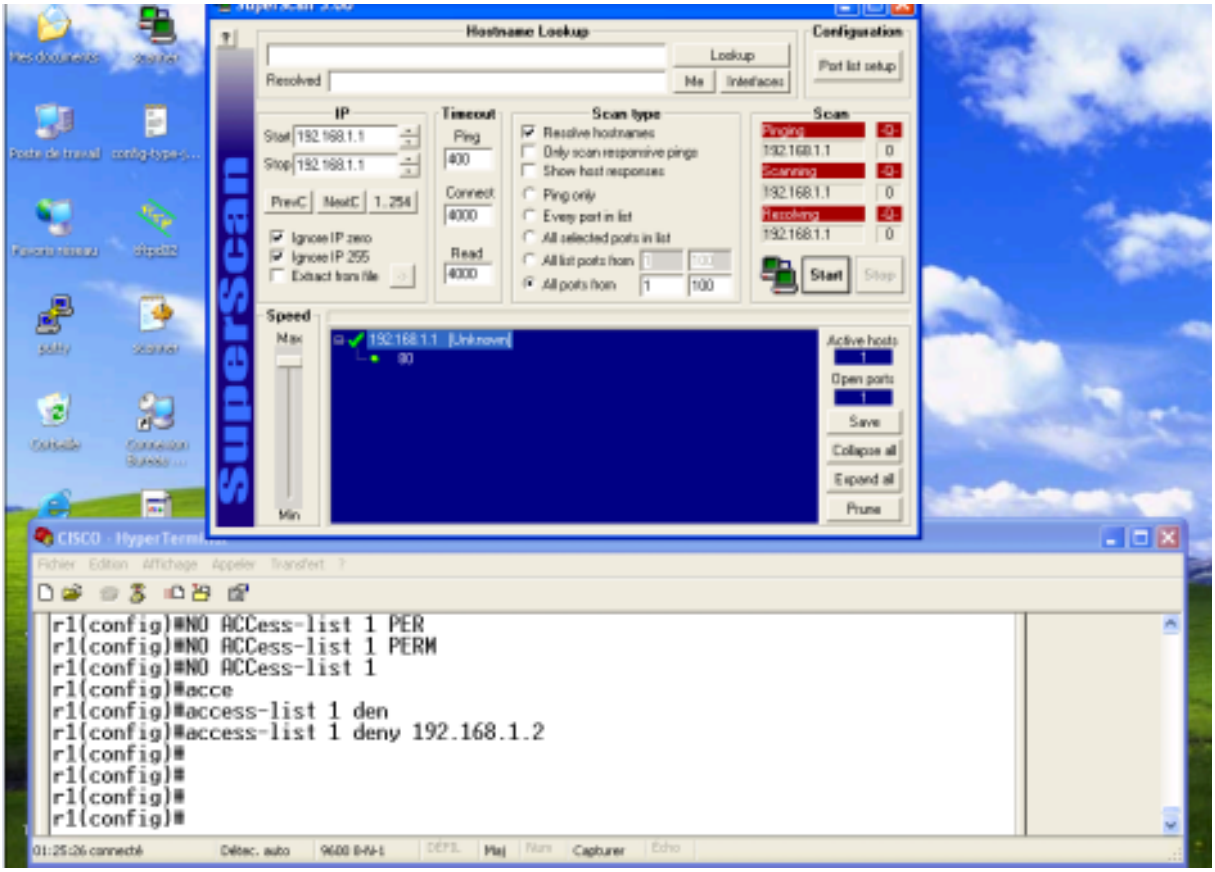
- **Limitation de l'Accès avec Telnet à l'aide Access List**



- **Exemple d'Access- List étendu permettent filtrer des paquets en fonction de l'adresse de destination IP**



- **Super scan : Logiciel catégorie scanner de ports**



▪ Scénario des attaques

Les scénarios représentent séquentiellement le déroulement des traitements et des interactions entre les éléments du système et/ou les acteurs.

1. Attaque synflood avec NetFlood

Cette attaque consiste à envoyer un paquet TCP SYN (qui débute les connexions) très rapidement, de sorte que le routeur attaqué s'attend à compléter un grand nombre de connexion sur le port spécifié, ce qui épuise ses ressources et affecte les connexions légitimes.

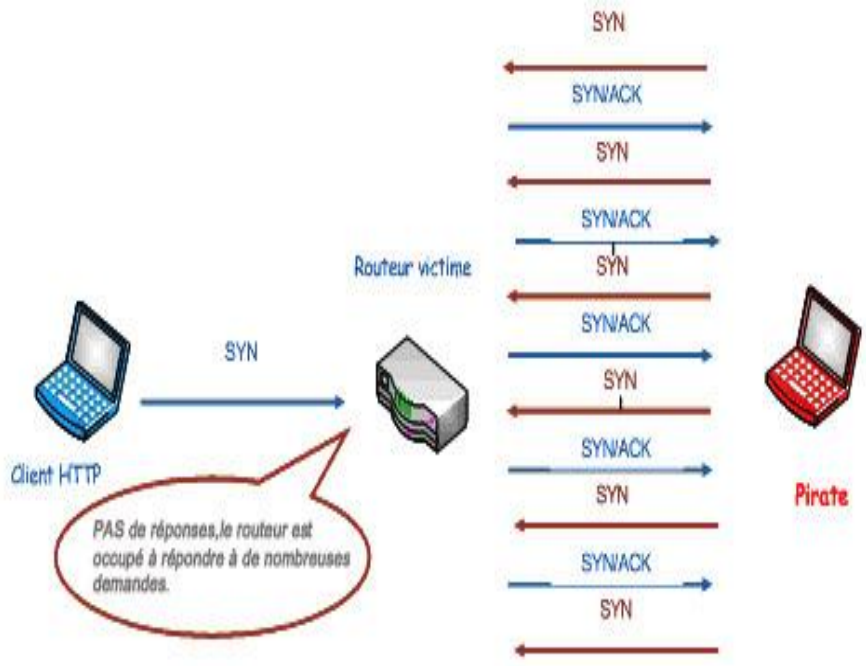


Figure : Scénario d'attaque SynFlood

2. Attaque avec SnmpDos

Cette attaque consiste à envoyer une requête Snmp « SET » qui comporte L'OID de l'état de l'interface du routeur le but de cette requête est de désactiver l'interface, donc rendre le routeur inaccessible à partir de cette interface.

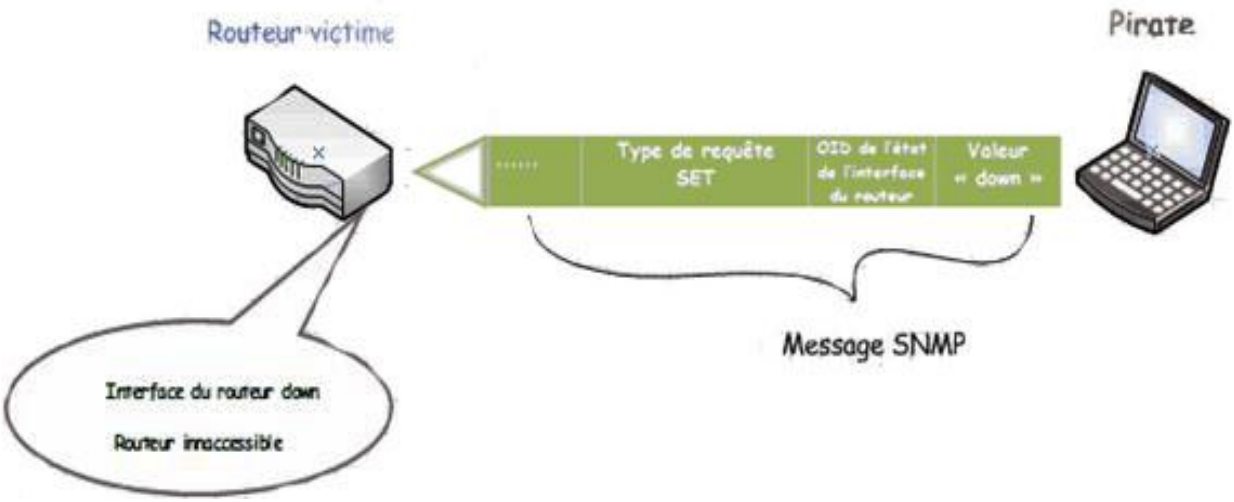


Figure: Scénario de l'attaque avec SnmpDos

3. Attaque par ICMP flood

Cette attaque vise à inonder le routeur avec un nombre important de paquet ICMP, pour alourdir sont fonctionnement. D'ailleurs, que les cibles répondent ou pas à l'ICMP, l'objectif premier étant de saturer sa bande passante d'accès réseau, processeurs, mémoire ...

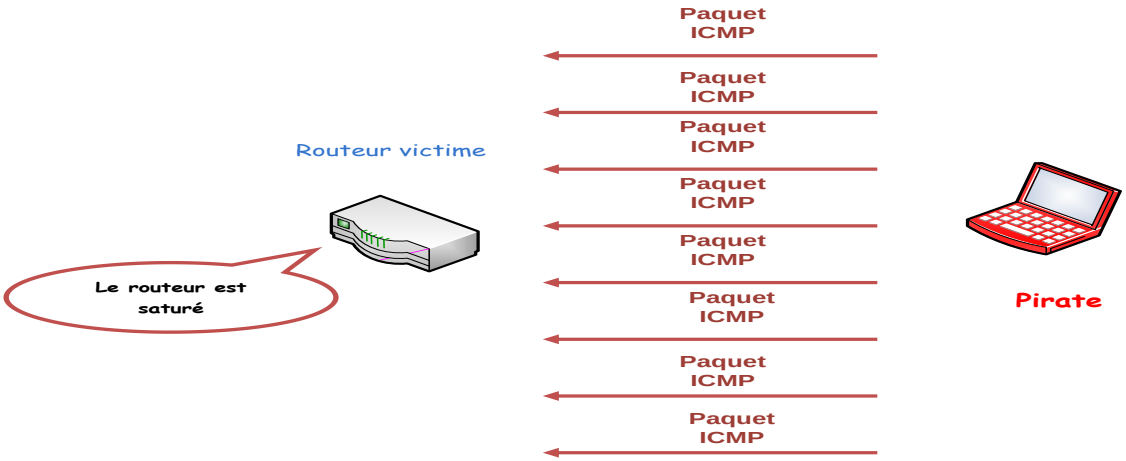


Figure : Scénario de l'attaque ICMP Flood

4. Attaque par UDP flood

NetFlood va se mettre à envoyer un maximum de paquets UDP sur le port spécifié de la machine cible.

Cette masse de paquets va submerger le routeur qui ne pourra plus répondre à aucune autre requête (d'où le terme de déni de service).

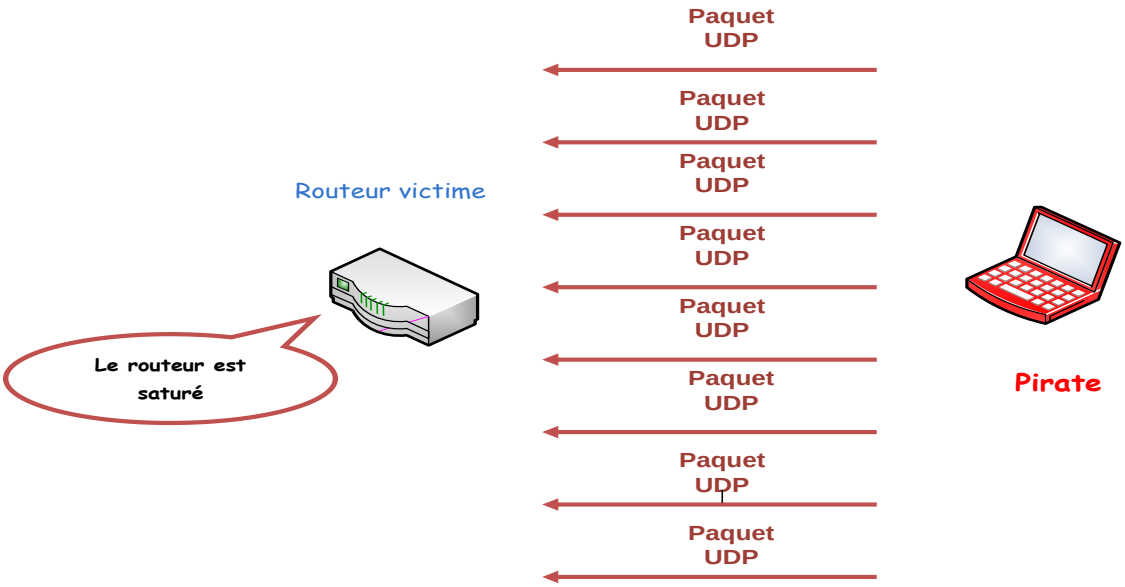


Figure: Scénario d'UDP Flood

5. Ecoute avec SnifferTelnet

SnifferTelnet met l'interface en mode transparent (promiscuous) pour capturer toutes les trames circulantes dans le réseau. SnifferTelnet applique un filtre à 'interface d'écoute selon :

- Le port destination : Il n'accepte que les paquets ayant le port destination 23 celui du service TELNET ,
- L'adresse destination : il n'intercepte que les paquets ayant l'adresse destination du routeur pour garantir que le trafic susceptible de contenir le mot de passe est destiné au routeur.

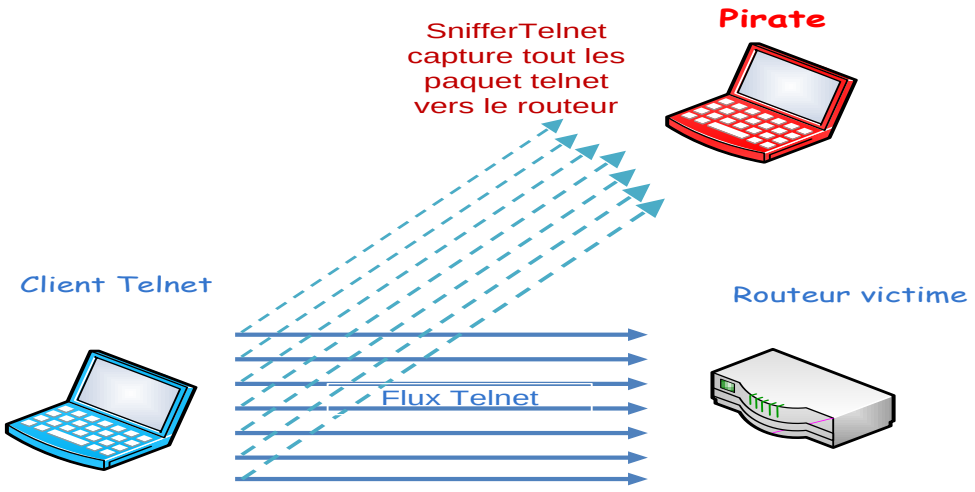


Figure : Scénario de capture du mot de passe Telnet

Type de sécurité des routeurs Cisco selon la check-list DISA

1. Sécurisation accès

1ère exemple :

- **Exigences**

L'ONS assuré que si un serveur d'authentification est utilisé pour l'accès administratif au routeur, un seul compte local peut être pour une utilisation en cas d'urgence

- **Procédures**

Examen de la configuration en cours d'exécution et de vérifier qu'un seul compte local a été défini. Un exemple d'un compte local est illustré dans l'exemple ci-dessous

username xxxxxxx password 7 xxxxxxxxxxx

2ème exemple :

- **Exigences**

L'ONS veillera à ce que tous les hors-la gestion des connexions à bande au routeur nécessitent des mots de passe

- **Procédures**

Etude de la configuration de chaque routeur de veiller à ce que le port de la console et les ports vty utilisé par le réseau OOBM besoin d'une invite de connexion

line con 0
***login** authentication admin_only*
exec-timeout 15 0
line vty 0 4
***login** authentication admin_only*
exec-timeout 15 0
transport input ssh

2. Sécurisation d'accès : privilège

1ère exemple :

- **Exigences**

Les administrateurs routeur feront en sorte que tous les comptes utilisateurs se voient attribuer le niveau le plus bas privilège qui leur permet d'exercer leurs fonctions.

- **Procédures**

Il ya 16 niveaux de privilèges possibles qui peuvent être spécifiées pour les utilisateurs dans la configuration du routeur. Les niveaux peuvent carte aux commandes, qui ont mis en niveaux de privilège - ou vous pouvez réaffecter les niveaux des commandes. Les noms d'utilisateurs avec mot de passe correspondant peuvent être réglés à un niveau spécifique. Il y aurait plusieurs noms d'utilisateur

"*name* password *password"*

Suivi par nom d'utilisateur

"*name"* privilège "*level"*.

L'utilisateur sera automatiquement acquis que le niveau de privilège lors de la connexion en dessous est un exemple d'attribution d'un niveau de privilège à un compte d'utilisateur local et de modifier le niveau de privilèges par défaut de la commande terminal configurer

username junior-engineer1 privilege 7 password xxxxxx

username senior-engineer1 privilege 15 password xxxxxx

privilege exec level 7 configure terminal

Remarque : L'exemple ci dessus ne couvre que

Les comptes locaux, vous aurez toujours besoin de vérifier les comptes et leurs niveaux de privilèges associés configuré dans le serveur d'authentification. Vous pouvez également utiliser TACACS pour granularité encore plus au niveau du commandement. Voici un exemple de Cisco Secure serveur TACACS

```
user = junior-engineer1 {
    password = clear "xxxxx"
    service = shell  {
        set priv-lvl = 7
    }
}
```

3. Désactivation port console

- **Exigences**

Les administrateurs routeur feront en sorte que les ports auxiliaires du routeur sont désactivés.

- **Procédures**

Voir la configuration de chaque routeur Cisco afin de s'assurer que le port auxiliaire est désactivé avec une configuration similaire

line aux 0

no exec

transport input none

4. sécurisation console

- **Exigences**

Les administrateurs routeur que le port console du routeur sont configurés pour expirer après 15 minutes d'inactivité.

- **Procédures**

Examen de chaque configuration des routeurs Cisco pour assurer que la console est désactivée après 15 minutes d'inactivité

line con 0

login authentication admin_only

exec-timeout 15 0

Note: la valeur par défaut est de 10 min, ce qui est plus restrictif

5. Sécurisation interfaces inactives

- **Exigences**

Les administrateurs routeur permettent de désactiver les interfaces du routeur qui ne sont pas en cours d'utilisation

- **Procédures**

En collaboration avec le diagramme de topologie réseau, utilisez l'interface « *show interface »* ou « *show ip interface brief »* commande de concilier toutes les interfaces qui ont un statut de protocole et de la place.

Interfaces avec le statut de administrativement vers le bas et vers le bas du protocole sont configurés avec un "*shutdown"* commande alors que les interfaces avec un statut de haut et de bas protocole indique que l'interface n'est pas désactivée via "shutdown" de commande et il n'est pas un lien actif. Cela pourrait aussi être un lien qui oscille.

Interfaces handicapées pour un routeur Cisco auront le "shutdown" commande en vertu de la déclaration d'interface

interface Ethernet1

no ip address

no ip directed-broadcast

shutdown

6. Fixation d'adresse d'administrateur

- **Exigences**

Les administrateurs routeur feront en sorte que le routeur ne permet que des séances de gestion dans la bande provenant d'adresses IP autorisées à partir du réseau interne.

- **Procédures**

Examen toutes les configurations de routeur Cisco et de vérifier que seules les connexions internes autorisés sont admis sur les ports VTY.

access-list 3 permit 192.168.1.10 log

access-list 3 permit 192.168.1.11 log

access-list 3 deny any

line vty 0 4

access-class 3 in

7. Recommandation d'utilisation de SSH au lieu de Telnet

- **Exigences**

Les administrateurs routeur assurer l'accès de gestion in-band pour le routeur est limitée à SSH

- **Procédures**

Examiner toute les configurations des routeurs Cisco et vérifier que ssh est autorisé seulement sur les ports VTY.

line vty 0 4

transport input ***ssh***

8. Log

- **Exigences**

L'administrateur routeur fera en sorte que le routeur enregistre toutes les tentatives d'accès dans la bande de gestion.

- **Procédures**

Examen de chaque configuration des routeurs Cisco pour s'assurer que toutes les tentatives de connexion aux ports VTY sont enregistrées.

access-list 3 permit 192.168.1.10 **log**

access-list 3 permit 192.168.1.11 **log**

access-list 3 deny any **log**

.

line vty 0 4

access-class 3 in

9. Deactivation de HTTP, FTP

- **Exigences**

HTTP, FTP, et tous les r-commandes BSD serveurs doit être désactivé.

- **Procédures**

Examen toutes les configurations de routeur Cisco afin de vérifier que la commande IOS pas de serveur http ip est présent

Note: Le serveur HTTP n'est pas disponible avec IOS versions antérieures à 11.0. En outre, http-server est désactivée par défaut dans la version IOS 12.0, d'où le no-ip-serveur http commande n'apparaît pas dans la configuration courante. FTP, RCP et RSH sont désactivés par défaut.

ftp-server enable

ip rcmd rcp-enable

ip rcmd rsh-enable

.

.

line vty 0 4

transport input rlogin telnet

10.Sécurisation ICMP: Ping

1ère exemple :

- **Exigences**

Notifications ICMP inaccessible, les réponses masquent, et les redirections ne sont pas handicapées sur toutes les interfaces externes du routeur prémisse.

- **Procédures**

Pour la version IOS 12.0 et d'examiner ultérieurement la configuration courante du routeur principe et d'assurer les commandes suivantes ne sont pas présents sur toutes les interfaces externes: "*ip unreachable", "ip redirects"*, et *"ip mask-reply"*. Pour les versions antérieures à 12,0,

d'assurer les commandes suivantes sont presents: "“*no ip unreachable, no ip redirects,”* et “*no ip mask-repy”.*

interface F*astEthernet 0/0*

description NIPRNet link

ip address 199.36.92.1 255.255.255.252

ip access-group 101 in

no ip redirects

no ip unreachables

no ip mask-reply

2ème exemple

- **Exigences**

Deux Network Time Protocol (NTP) des serveurs doivent être utilisés pour synchroniser toutes les horloges routeur.

- **Procédures**

Examen des configurations de routeur et de vérifier que les serveurs NTP ont été définis comme dans l'exemple suivant:

ntp update-calendar

ntp server 129.237.32.2

ntp server 142.181.31.6

11. Access Control List

1ère exemple :

- **Exigences**

L'administrateur routeur fera en sorte que toutes les tentatives de n'importe quel port, protocole ou service qui est refusée sera connecté

- **Procédures**

Examen de la configuration courante du routeur hypothèse et de vérifier que la pénétration à la fois le routeur et ACL évacuation ont un mot-clef log après chaque infirmer la déclaration.

access-list 101 permit tcp

access-list 101 permit tcp

access-list 101 permit tcp

.

access-list 101 deny any ***log***

2ème exemple :

- **Exigences**

L'administrateur routeur mettra en œuvre entrée et la sortie de filtrage sur tous les routeurs principe repose sur une politique de rejet par défaut.

- **Procédures**

Examen de la configuration courante du routeur hypothèse et de vérifier que les deux du routeur d'entrée et de sortie ACL sont basés sur une nier par la politique par défaut. Lorsque la vérification du respect par Deny exigence par défaut, vérifiez que l'ACL se termine avec le nier toute règle (implicite ou explicite) que la dernière ligne de l'ACL.

access-list 101 permit tcp . . . . . .

access-list 101 permit tcp . . . . . .

access-list 101 permit tcp . . . . . .

.

.

.

access-list 101 ***deny any*** *log*

3ème exemple:

- **Exigences**

L'administrateur routeur restreindre le routeur d'accepter tous les paquets IP sortants qui contient une adresse illégitime dans le champ d'adresse source par l'intermédiaire d'évacuation ou ACL en permettant Unicast Reverse Path Forwarding (RPF).

- **Procédures**

Examen de la configuration des routeurs pour assurer principe ACL évacuation sont en place sur toutes les interfaces internes pour restreindre le routeur d'accepter les paquets sortants IP qui contiennent une adresse IP externe dans le domaine source.

Afin de se conformer à la nier par la politique par défaut, permis des déclarations pour ces ports, qui sont autorisés devront être définies par le suivi nier toute déclaration. Les états de permis doit bénéficier de l'adresse source avec la plage d'adresses réseau interne.

Procédure d'Unicast Reverse

Path Forwarding: Examen de la configuration des routeurs pour assurer principe FPR a été configuré sur toutes les interfaces internes. Voici un exemple de configuration:

interface FastEthernet 0/0

description **downstream link to our network**

ip address 199.36.90.1 255.255.255.0

ip verify unicast reverse-path 197

!

access-list 197 deny ip any any log

*****

interface FastEthernet 0/0

description **downstream link to our network**

ip address 199.36.90.1 255.255.255.0

ip access-group 102 **in**

.

.

access-list 102 permit tcp any any established

access-list 102 permit udp host [external DNS] any eq domain

access-list 102 permit udp host [external DNS] any gt 1023

access-list 102 permit tcp [**internal network**] [wildcard mask] any eq ftp-data

access-list 102 permit tcp [**internal network**] [wildcard mask] any eq ftp

access-list 102 permit tcp [**internal network**] [wildcard mask] any eq http

access-list 102 permit . . . . . .

access-list 102 deny any

12. Simple Network Management Protocol (**SMNP)**

- **Exigences**

Les administrateurs routeur assurer SNMP est activé dans le mode lecture seule; en lecture / écriture ne sera pas permis que s'il est approuvé par l'ONS.

- **Procédures**

Examen toutes les configurations de routeur Cisco pour assurer l'accès SNMP à partir des stations de gestion de réseau est en lecture seule.

access-list 10 permit host 7.7.7.5

*snmp-server **community** xxxxxxxxx **ro** 10*

SYNC

- **Exigences**

Les administrateurs routeur utilise le protocole TCP Intercepte commande pour protéger les serveurs contre les attaques TCP SYN flood de tout un réseau extérieur.

- **Procédures**

Examen du principe ou de routeur de bordure de configuration pour assurer la commande d'intercepter TCP est en place pour intercepter les demandes déconnexion TCP SYN.

ip tcp intercept list 107

access-list 107 permit tcp any <internal network> < wildcard mask>

13.Ping

1ère exemple :

- **Exigences**

À l'exception d'Echo Reply (type 0), Temps dépassé (type 11), et Destination unreachable (type 3), le filtre d'entrée permet de bloquer tous les messages ICMP.

- **Procédures**

Examen du principe configuration des routeurs Cisco pour assurer que les blocs ACL pénétration tous les types de trafic entrant message ICMP à l'exception de Echo Reply (type 0),Temps dépassé(type 11), et Destination unreachable (type 3).

***interface** FastEthernet 0/0*

description to NIPRNet core router

ip address 199.36.92.1 255.255.255.252

*ip access-group **100 in***

.

access-list 100 permit icmp any any echo-reply

access-list 100 permit icmp any any time-exceeded

access-list 100 permit icmp any any unreachable

access-list 100 ***deny icmp any any*** *log*

Note: The above ACL could also look similar to the following using the icmp type codes instead of the icmp message type:

access-list 100 permit icmp any any 0

access-list 100 permit icmp any any 11

access-list 100 permit icmp any any 3

access-list 100 deny icmp any any log

2ème exemple

- **Exigences**

L'administrateur routeur bloque sortant types message ICMP Echo Request trafic à l'exception (type 8), de problème de paramètre (type 12) et Source Quench (type 4).

- **Procédures**

Examen du principe configuration des routeurs Cisco pour assurer l'évacuation ACL sont liés aux interfaces appropriées pour bloquer tous les types de message ICMP sortant de la circulation, sauf Echo, de problème de paramètre et Source Quench.

interface FastEthernet 0/0

description link to our network

ip address 199.36.90.1 255.255.255.0

ip access-group 107 in

.

.

access-list 107 permit icmp 199.36.90.0 0.0.255.255 any echo

access-list 107 permit icmp 199.36.90.0 0.0.255.255 any parameter-problem

access-list 107 permit icmp 199.36.90.0 0.0.255.255 any source-quench

access-list 107 **deny icmp any any** log