Date :04/06/2018

I/Superviseur

Définition

Personne qui aspire au rôle de chef d’équipe, contremaître, gérant, superviseurs, coordonnateur et gestionnaire, ou encore pour celle qui occupe de telles fonctions et qui pourrait bénéficier d’un perfectionnement dans un contexte en perpétuel changement où la gestion du capital humain est un enjeu stratégique pour laquelle des habiletés plus pointues sont de plus en plus sollicitées et requises.

CONTENU

En tant qu'administrateur, superviseur ou utilisateur disposant de droits d'administrateur ou de superviseur, du serveur NetWare, vous pouvez conserver des versions de sauvegarde des fichiers de votre serveur NetWare et les restaurer rapidement et aisément en cas de perte ou de détérioration des fichiers originaux. Le niveau de privilège administrateur est obtenu par l'affectation du droit superviseur.

II/firewall

Définition

Un *firewall* (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

III/Routeur & Switch

1)routeur

Rôle

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles.

Fonctionnement

Configuration

https://www.linksys.com/ca/fr/support-article?articleNum=142912

Installation

2)Switch

Rôle

Un switch, également appelé commutateur réseau, est un boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier plusieurs câbles ou fibres dans un réseau informatique.

Fonctionnement

Il permet de créer des circuits virtuels, de recevoir des informations et dès les envoyer vers un destinataire précis sur le réseau en les aiguillant sur le port adéquat. Les switches ont plusieurs avantages : ils sécurisent les données transmises sur le réseau et peuvent être utilisés pour augmenter le nombre d'ordinateurs connectés sur un réseau Ethernet.

Configuration

II.I. Le setup

Pour configurer un switch (première configuration ou reconfiguration complète), il vous faut d'abord entrer en mode privilégié :.

>enable

#

Au tout début, le mode privilégié n'aura pas de mot de passe, à vous d'en configurer un nouveau pour la suite.

Entrez ensuite la commande :

configure terminal

Le système passe en mode de configuration global.

Pour changer le nom du switch, tapez "hostname" en mode configure.

hostname NOM_SWITCH

Installation

II.II Configurer l'accès telnet

Pour que l'accès telnet soit autorisé il faut positionner un mot de passe :

conf t

line vty 0 4

password MOTDEPASSE

end

II.IV. La sécurité

- Mot de passe privilégié

Le mot de passe est par défaut positionné en mode non encrypté, et apparaîtra donc à

Chaque exécution de la commande "show run". Pour y remédier, encrypter le password du mode privilégié :

conf t

enable secret MOTDEPASSE

Kali Linux

Définition

Kali Linux est une distribution GNU/Linux sortie le 13 mars 2013, basée sur Debian. La distribution a pris la succession de BackTrack. L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion.

Hyper-V

Hyper-V, également connu sous le nom de Windows Server Virtualisation, est un système de virtualisation basé sur un hyperviseur 64 bits de la version de Windows Server 2008.

Machine Virtuel

Définition

Une machine virtuelle, ou VM (Virtual Machine), est un environnement d'application ou de système d'exploitation (OS, Operating System) installé sur un logiciel qui imite un matériel dédié. Côté utilisateur final, l'interaction avec une machine virtuelle est la même qu'avec un matériel dédié.

Fonctionnement

Elle s'exécute dans une fenêtre, comme tout autre programme, en offrant à l'utilisateur final une expérience identique à celle qu'il aurait sur le système d'exploitation hôte. La machine virtuelle est placée dans un « bac à sable » qui l'isole du reste du système, de sorte que les logiciels installés sur la machine virtuelle ne peuvent ni s'échapper, ni modifier l'ordinateur hôte. Cela produit un environnement idéal pour tester d'autres systèmes d'exploitation, dont des versions bêta, l'accès à des données infectées par des virus, la création de sauvegardes de système d'exploitation et l'exécution de logiciels ou d'applications sur des systèmes d'exploitation auxquels ils ne sont pas destinés à l'origine. Il est possible d'exécuter plusieurs machines virtuelles simultanément sur un même ordinateur physique. Chaque machine virtuelle fournit son propre matériel virtuel, à savoir les processeurs, la mémoire, les disques durs, les interfaces réseau et les autres périphériques nécessaires. Le matériel virtuel est ensuite mappé au matériel réel sur la machine physique, ce qui permet de réaliser des économies en réduisant le besoin de disposer de systèmes matériels physiques, ainsi que les coûts de maintenance associés, tout en réduisant la demande en alimentation et refroidissement.

Attaque informatique

Fonctionnement

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Protection

La sécurisation d'un système informatique est généralement dite « asymétrique », dans la mesure où le pirate n'a qu'à trouver une seule vulnérabilité pour compromette le système, tandis que l'administrateur se doit de corriger toutes les failles.

Mais aussi on peut voir que l’on peut protéger son système avec :

- Installer des antivirus
- Mettre a jour les system et les programme

- Utiliser un Pare-feu physique
- Utiliser un navigateur protéger
- Utiliser une Wifi sécuriser