**1) Hyperviseur**

La virtualisation est un outil qui permet de virtualiser un OS sur un système hôte. La virtualisation s’appelle « l’hyperviseur ». On peut utiliser « vitualbox » pour virtualiser un ordi niveau personnelle.

Pour la version pour les entreprises, on peut utiliser VMware qui est payant.

Dans le système hyperviseur on peut mettre système invité.

**2) Système invité (Machine virtuel)**

Pour Windows 7 🡺 2GO

Pour linux (sans environnement graphique) 🡺 512 Mo

Pour le réseau, il y a :

* Le mode bridge : aucune restriction
* Le mode interne : ne communique avec qu’avance les autres machines virtuelles
* Le mode hôte : ne peux communiquer qu’avec les autres machines virtuelles et la machine hôte

Système de fichiers :

**1e) partitionnement**

Partition :

* Primaires : nombre limité de partition (linux : 4 ; Windows : plus de 4) par défaut
* Etendue : pour ajouter découpe du disque que l’on veut
* Logiques

**2e) Amorce**

* MBR
* GPT

**3e)Formatage**

Windows :

* FAT32
* NTFS
* exFAT

Linux :

* ext2
* ext3
* ext4

Mac :

* HFS

**Protections**

**Matériels**

* Onduleur
* Refroidissement
* RAID

**Données/Communication**

* Firewall / Le pare-feu
* Antivirus/Antimalware
* VPN
* Mot de passe
* Sandbox
* Chiffrement
* Certificat
* sauvegarde

**Utilisateurs**

* Norme de sécurité

**Logiciels**

* Licence
* DRM

**1) matériels**

L’onduleur est une grosse batterie pour garder les appareils allumés. Il prend le rôle de filtre suite à des surintensités.

Le refroidissement, inclus un système de sonde qui permet d’éteindre l’ordinateur pour éviter la destruction de la machine.

Le RAID est le fait de faire de la mise en parallèle plusieurs de disque dure. Il existe plusieurs RAID :

* RAID 0 : c’est des questions de performance
* RAID 1 : Mirroring : c’est pour mettre 2 disques en parallèle et ils ont les mêmes données\*
* RAID 5 : minimum 3 DD

NAS : c’est un boitier que l’on branche en Ethernet pour faire une baie de stockage

SAN : c’est un boitier que l’on branche en ESATA pour être plus rapide que l’Ethernet.

**2) Données/Communication**

Firewall : filtrage des communications réseaux entrantes et/ou sortante

Antivirus : pour enlever les virus

* Vers
* Cheval de Troie
* Keylogger

Antimalwares : le plus connue 🡺 spyware

* Malwarebytes
* Adwcleaner (1ere couche)
* Roguekiller

VPN/chiffrement : SSL/TLS ou IPSec

Certificat : HTTPS

Mot de passe : 8 caractère minimum : Majuscules, Minuscules, symboles, chiffres

Sauvegarde :

Logiciels :

* Légal
* Libre (gratuit)
* Propriétaire
* Payant
* Shareware
* Freeware
* Protection copie
* Numéro de série
* Protection CD/DVD (Securom, safedisk)

Utilisateurs :

* Aménagement du plan de travail
* Repose poignet
* Siege spécialisé
* Périphérique ergonomique
* Données privées
* Cookies
* Identité numérique

**Chapitre 2 : Gestion de projet**

* Liste des besoins
* Le cahier des charges
* Formaliser des demandes
* Estimation
* Cout d’investissement
* Cout de fonctionnement
* Gérer le temps et les ressources
* Diagramme de Gantt
* Estimation de temps par tache avant et pendant
* Ressources
* Réalisation
* Tests
* Documentations
* Manuel technique
* Manuel utilisateur

Diagramme de Gantt :

* Liste des taches
* Evaluer la durée des taches (jours/heures/semaines)
* Définir les extériorités

|  |  |  |
| --- | --- | --- |
| Taches | antériorités | Durée J |
| A | - | 10 |
| B | A | 5 |
| C | - | 4 |
| D | C | 12 |
| E | - | 10 |
| F | C | 5 |
| G | E, F | 6 |

**//Diagramme de Gantt**

**XML :** extemeible Markup Language

\\[exemple xml](exemple%20xml.xml)

CSV : Comma Separated Values :

Ex : valeur, valeur, « valeur » (pour éviter le conflit avec les chiffres a virgules)

Services (protocoles)

HTTP web

FTP : transfère de fichier (port 20/21)

SSH chiffrer information

Bittorent transfère de ficher

SMTP (l’envoi), POP, IMAP (le réception)

DHCP IP dynamique

DNS

TCP/IP, UDP

SMB, SAMBA, CIFS partage de fichier

ICMP Ping

Webdav partage de fichier

Telnet

NAT

Schéma de processus :

1) acteurs

2) évènements

Tout ce qui peut se produire dans l’entreprise (recevoir un mail et envoyer un colis)

3) activités/actions

Inscription à Godefroy

|  |  |  |  |
| --- | --- | --- | --- |
| M. Gagneur  Responsable filière  111 Acceptation de la  Demande    Tri des demandes   * Examiner dossiers * Faire un entretien   Accepté Refusé | Chef de travaux | Secrétaire  ou  Inscription   * Saisir info * Vérification   Du dossier    Ok pas ok  Dossier refusé  Dossier validé | Elève  Demande d’inscription  Demande de  Correction  Dossier complété  Demande rejeté  Demande Validé |

xDsl

1. Principe

Puissance

Téléchargement

Flux descendant

Téléversement

Montant

RTC

Bas débit

1. Famille

Bas débit => 56 kb/s => 7 ko/s

ADSL => 13380 kb/s => 1672.5 ko/s

SDSL

Envoi 1024 kb/s

13 Mb/s => 1.5 Mo/s

ADSL2+ => 25 Mb/s => 3 Mo/s

3Mb/s =>

IDSL (RSIS, Numéro) => 2x64 Kbits/s

|  |  |  |  |
| --- | --- | --- | --- |
|  | Image  2 Mo | Musique  Album MP3  110 Mo | Vidéo  700MO |
| Bas débit | 292 s = 5 min | 16091 s = 268 min = 4h | 102400 s = 1706 min = 28h |
| ADSL | 1,33 s | 73 s = 1min13 | 467 s = 8min13 |
| ADSL2+ | 0,66 | 37 s | 230 s = 4min25 |

1. Modulation

T

5V

t

1. Les limites

Distance limite entre le box et le boitier maximum pour un débit de 2Mbits/s a 5755 m (ADSL) et pour l’adsl2+ 3MB/s

Télé basse qualité : 4-5 Mb/s

Télé HD : 8-10 Mb/s

1. Fonctionnement

Ligne non dégrouper :

PBAX

DSLAM

Filtre

Filtre

Téléphone

BOX

Ligne dégroupage total :

// mettre schéma comme avant !!

Liaison filaire et WIFI

1. Liaison filaire (réseau local)

Ethernet 🡺 10 Mb/s

Fast Ethernet 🡺 100 Mb/s

Gigabit 🡺 1 Gb/s

1. WIFI

Normes :

802.11 a : Wifi 5 : 27-54 Mb/s : envion 10m

802.11 b : 6-11 Mb/s : 300 m

802.11 g : 25-54 Mb/s : 300 m

802.11 n : 100-300 mb/s : 100 m

802.11 ac : 433-1300 Mb/s : >300 m

|  |  |  |  |
| --- | --- | --- | --- |
|  | Image (2Mo) | Album (115 Mo) | Film (700 Mo) |
| Ethernet 10Mb/s | 1,6 s | 92 s = 1,5 min | 560 s = 9,33 min |
| FastEthernet 100Mb/S | 0,16 s | 9,6 s | 56 s |
| Gigabit 1 Gb/s | 0.016 s | 0,92 s | 5,6 s |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 2 Mo | 115 Mo | 700 Mo |
| 802.11 a 54 Mb/s | 0.29 s | 17.03 s | 103,70 s =1,24 min |
| 802.11 b 11 Mb/s | 8 s | 83.6 s | 509.09 = 8,48 min |
| 802.11 g 54 Mb/s | 0.29 s | 17.03 s | 103.70 s = 1,24 min |
| 802.11 n 300 mb/s | 0.05 s | 3.06 s | 18,6 s |
| 802.11 ac 1300 Mb/s | 0.012 s | 0.70 s | 4,30 s |

Mode de fonctionnement

* Infacstucture : connexion à un point d’accès (antenne)
* Ad Hoc :
* Mode Pont (bridge)
* Répéteur

Chiffrement :

WEP 🡺 64 a 128 bits (en realité 40-104 bits)

WPA et WPA – PSK 🡺 >128 bits

WPA2

Principe de l’authentification

* Authentification
* Communication

Supervision et infogérance

3 types d’infogérance :

* TMA : Tierce Maintenance Applicative, Support aux utilisateurs et maintenance
* Gestion des infrastructures : externalisation ou non de l’hébergement
* BPO : externalisation de certain processus de l’entreprise : compatibilité, RH, paye

1. Supervision (monitoring)

Niveau 1 :

Service disponible ou non

Niveau 2 :

Intervention ponctuelle des techniciens

Niveau 3 :

Infogérance

MAJ, analyse des logs, sauvegarde, sudit

1. Infogérance et protection

Basculement ou fail-over

Basculement automatiquement sur un élément alternatif

2 modes :

* Equipement secondaire en vieille
* Equilibrage de charge

Retour à la normal, fail-back

Equilibrage de charge ou load balancing

* Fermes de serveurs (servers cluster)
* Serveur maitre distribue les taches aux machines esclaves
* NAS 🡺 Ethernet
* SAN 🡺 eSCSI

eSATA

DNS dynamique

Disponibilité :

Pour un temps de disponibilité de 99%, cela correspond à 3,65 jours hors services/an

Pour un temps de disponibilité de 99,9%, cela correspond 8.75 H

Pour un temps de disponibilité de 99,999%, cela correspond cela 5,2 min

Sécurité informatique :

1. Types d’attaques

5 P :

* Probe (sonde) 🡪 Ping, traceroute, nslookup

Scanneur de ports

* Penetrate (intrusion)

Brute Force, dictionnaire

Failles des logiciels

* Persist (persistant)

Créer des acces admin

Outil de control à distance (cheval de Troie)

* Propagate (propager)

Sonder les failles du réseau local

Propager l’intrusion

* Paralyze (paralyser)

Endommager des systèmes ou des données

Utiliser les machines pour attaquer les systèmes$

1. Attaques réseaux

* Simple => tentative de connexion aux services

Fouillent détectable

* Furtif
  + Tentative d’échange de fichier des données sans connexion
* Détournement des normes RFC
* Aveugle

Utiliser des machines intermédiaires

Spoofing : usurpation d’identité d’une machine ou d’un équipement

* Passif
  + snifing
  1. IP spoofing

Usurper une IP

* 1. ARP Spoofing

Usurper une adresse MAC d’une machine

* 1. DNS Spoofing
  2. attaque par fragment
* Fragment overlaping : changement de fragment dans une trame
* Tiny fragments : changement d’un fragment officiel par 2 fragments : 1 petit contenant de vrai information puis un 1 fragment plus grand qui contient les informations modifiées.
  1. Détournement de sessions TCP

Écouter le réseau et attendre l’identification ai eu lieu

Désynchroniser le client et le serveur en créant une latence

Usurpation du client

1. Attaques sur les logiciels

* Configuration par défaut : augmentation du risque
* Bugs
* Dépassement de pile : Permet de dépasser le mémoire exprès pour voir le contenue de la mémoire.
* Script
* Injection SQL :

SELECT \* From ‘Users’ WHERE Nom = … AND Mdp = … ;

« P@ssw0rd » ; Drop TABLE Users

SELECT \* From Users

* Homme de milieu (Middle Man)

Serveur

Homme du milieu

Client

1. Dos / D-DOS

Attaques par déni de services

* Inonder le service de demande d’échange de donnée
* Demande de connexion sans suite
* Surcharger le service en demande UDP

UDP prioritaire au TCP

* Smurfling : inonder de requête ICMP (Ping) en broadcast en usurpant l’identité de certaine machine
* DDOS : dos avec de nombreuses machines

1. Type de détection

IDS : Système de détection d’intrusions

* Surveiller la mémoire et les processus
* Trier les connexions
* Filtrer les communications sur la passerelle/routeur

1. Méthodes de détection

* Recherche de motifs (pattern matching)
* Analyse des protocoles a la recherche d’abus connus
* Analyse heuristique a la recherche de comportement inconnue
* Approche probabiliste/statistique =

Qualité de services (QoS)

1. Objectif

Optimisation des ressources réseaux pour garantir les performances

QoS selon les applications ou les utilisateurs

Mutualisation des ressources

1. Le principe

Filtrer les données sur le réseau (couche 3 : IP)

Critère de filtrage :

* Protocole/port
* La bande passante
* La source et destination
* Date et heure
* Etat du trafic réseau
* Itinéraire
* Latence

1. Limitation du trafic

Au moyen d’un algorithme

Sceau percé

1. Ordonnancement

Gestion de l’ordre de passage

* FIFO (First IN First Out)
* Priorité
* RR (Round Robin)

Arborescence de fichiers et batch

C : Racine

Windows

Programs Files

Utilisateurs

1. Chemin absolu et relatif

Chemin absolu :

C:\ProgramsFiles\Chrome\Chrome.exe

Chemin relative

.\Chrome.exe

.\Chrome\Chrome.exe

.\Program Files\Chrome\Chrome.exe

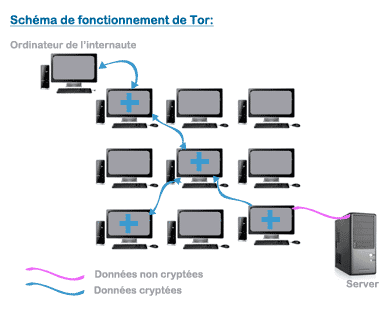
. => represente le dossier courant

1. Batch

* C : ou d : => accéder à une racine
* Cd « Programs Files »
* DIR : affiche le texte des dossiers
* MKDIR [NomDuDossiers]
* RMDIR [NomDuDossiers] : supprime un dossier
* DEL [NomDuFichier] : supprime un fichier
* REN [AncienNom.ext] [NouveauNom.ext] : renomme un fichier ou un dossier

TOR : The onion Router (le routeur oignon)

1. Principe



1. Limites

TCP seulement

Requetes DNS en claire (UDP)

Protocole des couches 5,6, et 7 ont des IP en claire (JavaScript)