MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABDELHAMID IBN BADIS – MOSTAGANEM

Faculté des Sciences Exactes et de l'Informatique
Département de Mathématiques et d'Informatique
Filière : Informatique

SUPPORT DE COURS

Pour Master en Informatique
Option : Ingénierie des Systèmes d'Information

Sécurité des Systèmes d'Information

Enseignante : Dr. BENTAOUZA Chahinez Mériem.

E-mail : chahinez.bentaouza@univ-mosta.dz

Site web: https://sites.google.com/view/cours-bentaouza/accueil

Année Universitaire 2019-2020

Table des matières

Préambule …… 4

I. Introduction SSI ……... 5
I.1. Définition de la SI ……... 5
I.2. Sous-domaines de la SI ……... 5
I.3. Objectifs de la SI …… 5
I.4.Historique de la sécurité …….. 5
I.5. Domaine d'application de la sécurité ……..…… 6
I.7. Concepts de sécurité ……... 6
I.6. Différences entre accidents et malveillances …….. 6

II. Cryptologie …… 7
II.1. Introduction ……... 7
II.2. Terminologie …… 7
II.3. Cryptographie …… 8
II.4. Cryptanalyse …….. 9

Fiche TP 1 « Cryptologie » ……... 10

III. Politique de sécurité ……... 15
III.1. Plan de sécurité …….. 15
III.2. Cybercriminalité ……. 16
III.3. Cybersécurité …… 17
III.4. Autres définitions ……... 17
III.5. Méthode de sécurité ……... 17
III.6. Norme de sécurité …….. 17

Fiche TD 1 « Charte de Sécurité » ……... 19

IV. Stockage ……... 20
IV.1. Support de stockage …….. 20

V. Partitionnement …… 22
V.1. Définition du partitionnement ……. 22
V.2. Objectif de partition …… 22
V.3. Type de partition ……. 22
V.4. Table de partitions ……... 22
V.5. Système de fichier ……... 23

Fiche TP 2 « Partitionnement » ……... 25

V.6. Système de Droits 27
V.7. Redondance (Redundancy) 28

Fiche TP 3 « Droit d'Accès » 30

VI. Sécurité TCP/IP 31
VI. 1. Rappel TCP/IP 31
VI. 2. Méthodologie d'attaque 33
VI. 3. DOS 35
VI. 4. Techniques 37

Fiche TP 4 « Commandes TCP/IP » 39

VII. Architectures et protocoles de sécurité 42
VII.1. Architecture 42
VII.2. Protocoles 43

Fiche TP 5 « WireShark » 45

VIII. Authentification 48
VIII .1. Définition 48
VIII .2. Facteurs d'authentification 48
VIII .3. Méthodes d'authentification 48

« Liste des Logiciels à Tester en project » 54

Bibliographie 57

Préambule

•Cours + TP

Objectifs

•Les entreprises et organisations produisent des documents et des données dont la pérennité doit être garantie et l'accès contrôlé.
•Ce module traite des méthodes de stockage et de transmission de ces données en sécurité.

Connaissances préalables recommandées

Systèmes d'information, réseaux

Coefficient et crédit

•Crédits : 4
•Coefficient : 2

Mode d'évaluation :

•Test personnel + (Travail de groupe (exposé) + consultation personnelle)
•Contrôle continu (40 %) et examen final (60%)

Réglementation

•Présence -> non obligatoire au cours / obligatoire en TP
•Retard -> ne pas déranger
•Portable -> éteint ou silencieux
•Discussion -> ne pas exagérer
•Question -> ne pas se vanter
•Cours en français, mais documentation et exposé en anglais

I. Introduction SSI

I.1. Définition de la SI

•La sécurité de l'information est l'ensemble des activités qui s'appliquent à tous les aspects de la sureté, de la garantie et de la protection de l'information quel que soit son support pour la conserver ou la transmettre.

« La sécurité de l'information est un processus visant à protéger des données contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisée. »

NB: la SI n'est pas confinée à la sécurité informatique ce sont des sous-domaines de la SI.

Exemple : l'information du début à la fin

I.2. Sous-domaines de la SI

•sécurité informatique
•Sécurité du réseau
•sécurité du système d'information
•Sécurité de la communication

I.3. Objectifs de la SI

•La sécurité informatique vise généralement cinq principaux objectifs :
•La confidentialité permet d'empêcher la divulgation non-autorisée de données ;
    ▫seules les personnes autorisées aient accès aux ressources échangées ;
•L'intégrité permet d'empêcher la modification non-autorisée de données ;
    ▫ c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
•L'authentification permet d'empêcher l'utilisation non-autorisée de ressources;
    ▫seules les personnes autorisées aient accès aux ressources.
•La disponibilité permet de maintenir le bon fonctionnement du système d'information ;
•La non répudiation permet de garantir qu'une transaction ne peut être niée ;

I.4.Historique de la sécurité

•La sécurité physique : les messagers était escortés par des soldats.
•La sécurité des communications : Jules César créa les messages codés.
•La sécurité des transmissions : 1950, en analysant les signaux électriques d'une ligne téléphonique.
•La sécurité de l'ordinateur : 1970, un modèle pour sécuriser les opérations des ordinateurs.
•La sécurité des réseaux : La mise en réseau des ordinateurs, à la fin des années 1980 pose un problème.
•La sécurité de l'information : Début des années 2000.

I.5. Domaine d'application de la sécurité

•Sécurité physique : la sécurité au niveau des infrastructures matérielles : salles sécurisées, postes de travail des personnels, etc.
•Sécurité logique : la sécurité au niveau des données, notamment les applications ou les systèmes d'exploitation.

•Sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
NB: mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs.

I.6. Différences entre accidents et malveillances

•Sécurité = « Safety »
C'est la protection contre des événements accidentels imprévisibles.
Ex : Pompiers
•Sécurité = « Security » (Sureté)
C'est la protection par rapport à des événements intentionnels.
Ex : Police
Exemple : le transport aérien (portable, arme)

I.7. Concepts de sécurité

•Le risque en termes de sécurité est généralement caractérisé par l'équation suivante :

Risque = (Menace x Vulnérabilité x Impact) / Contre-mesure

•la menace (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu.
•la vulnérabilité (en anglais « vulnerability »), appelée parfois faille ou brèche représente le niveau d'exposition face à la menace dans un contexte particulier.
•l'impact ou conséquence fait parti du risque aussi comme représenté dans iso 27005.
•la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

Exemples de Risque

•Compromission d'informations
•Destruction d'informations
•Vol d'informations
Qui peut engendrer :
•Perte financière
•Un désastre sans sauvegarde

La sécurité un processus et non un ensemble de produits

II. Cryptologie

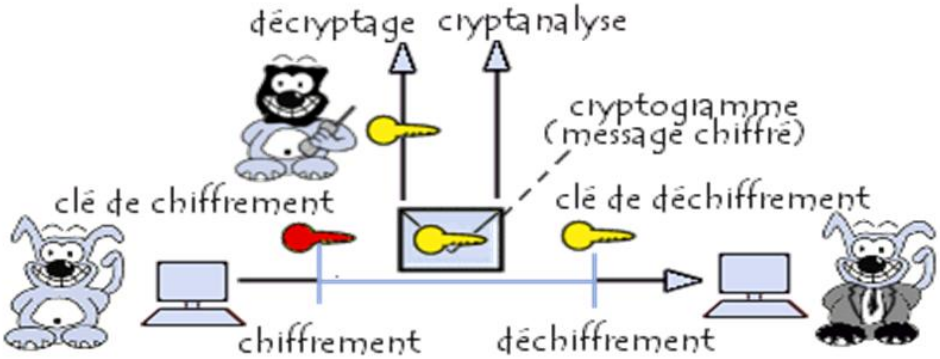
II.1. Introduction

Depuis 3000 ans environ, les êtres humains ont tenu à garder secret certaines conversations.
Pour cela, il y eût diverses techniques reposant sur des principes méconnus des "espions" adverses.

La cryptographie était le domaine réservé des services du chiffre chez les militaires, du code de César à la machine Enigma.
Elle fait aujourd'hui partie de notre vie quotidienne : cartes à puce et monétique, Internet et courrier électronique ...
Nous faisons déjà tous de la cryptographie sans le savoir.
Cette science intéresse donc tout le monde, pour garder un secret entre deux personne (ou plus) tout simplement.
L'objectif de ce module est de permettre à chacun de connaître l'histoire de cette science et se familiariser avec et d'en comprendre les mécanismes.

II.2. Terminologie

- Cryptologie = cryptographie + cryptanalyse
- Chiffrement, déchiffrement et décryptage
- Alice et Bob
- Ève vient de l'anglais «eavesdropper» c.à.d. «oreille indiscrète».



- Cryptologie: Science des écritures secrètes des documents.
  - Issu du grec cryptos(caché ou secret) et logie (science)

- Cryptographie: Ensemble des techniques de chiffrement de données.
  - Issu du grec cryptos(caché ou secret) et graphie(écriture)
- Le chiffrement ou cryptage : méthode qui rend un texte clair en texte chiffré à l'aide d'une *clef de chiffrement*,
- Le déchiffrement: méthode qui rend un texte chiffré en texte clair *clef de déchiffrement*.

- Cryptosystème: un mécanisme (algorithme) dont l'objectif est de protéger l'information.
- Cryptogramme: texte chiffré à l'aide d'un crypto-système.
- Acteurs:
  - Alice et Bob ou Bernard : ils souhaitent se transmettre des informations de façon légitime ;
  - Oscar, Eve, Robert : un opposant (ou ennemi, espion, adversaire) qui a pour but d'espionner les communications entre Alice et Bob.
  - Cryptanalyse ou décryptage ou décryptement: retrouver le texte en clair ou la clé sans connaître la clé (attaque).
    - On parle généralement de « casser » !

II.3. Cryptographie

Objectifs de la cryptographie

- La confidentialité permet d'empêcher la divulgation non-autorisée de données ;
  - seules les personnes autorisées aient accès aux ressources échangées ;
- L'intégrité permet d'empêcher la modification non autorisée de données ;
  - c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- L'authentification permet d'empêcher l'utilisation non-autorisée de ressources;
  - seules les personnes autorisées aient accès aux ressources.
- La non répudiation permet de garantir qu'une transaction ne peut être niée.

NB : Authenticité = Authentification + Intégrité

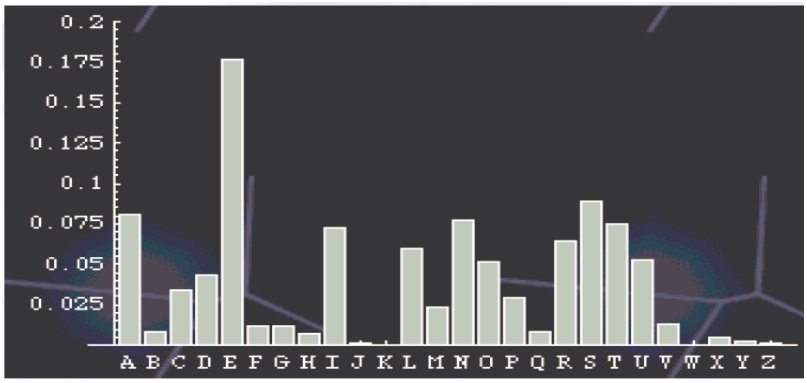
Diagramme de cryptographie

- Cryptographie classique
  - Substitution (César, Vigenère, Polybe, Hill)
  - Transposition (ADGFX)
  - Registres à décalage (LFSR)
- Cryptographie moderne
  - Symétrique: à clé secrète (DES, AES)
  - Asymétrique: à clé publique (Merkle-Hellman, RSA, El Gamal)
  - Hybride : clé publique et secrète
- Cryptographie en recherche
  - Quantique
    - par envoi d'impulsions de photons polarisés
    - pour transmettre une clé secrète: perturber le canal de transmission

II.4. Cryptanalyse

Type de cryptanalyse

- Cryptanalyse statistique
  - Le cryptogramme doit être suffisamment long pour avoir des moyennes significatives.
  - De plus, chaque langue dispose de fréquences différentes : il faut donc avoir sous les yeux les fréquences de toutes les langues si on ne connaît pas l'origine du message.



- Cryptanalyse différentielle
  - Étude sur la manière dont les différences entre les données en entrée affectent les différences de leurs sorties.
  - Exemple :
    - ✓ Choisir un grand nombre de couples (texte en clair, texte chiffré)
    - ✓ Exemple : Pour le DES : choisir 247 textes en clair

- Cryptanalyse linéaire
  - Etablir une équation linéaire entre certains bits du texte en clair et certains du texte chiffré
  - Exemple :
    - ✓ pour le DES : utiliser 243 couples, on trouve 26 bits des 56 bits de la clé par cette attaque.

Attaques sur un chiffrement

- Attaque à texte chiffré connu : l'opposant ne connait que le message chiffré y.
- Attaque à texte clair connu : l'opposant dispose d'un texte clair x et du message chiffré correspondant y.
- Attaque à texte clair choisi : l'opposant a accès à une machine chiffrante. Il peut choisir un texte clair et obtenir le texte chiffré correspondant y, mais il ne connait pas la clef de chiffrement.
- Attaque à texte chiffré choisi : l'opposant a accès à une machine Déchiffrante. Il peut choisir un texte chiffré y et obtenir le texte clair correspondant x, mais il ne connait pas la clef de déchiffrement.

Fiche TP 1 « Cryptologie »

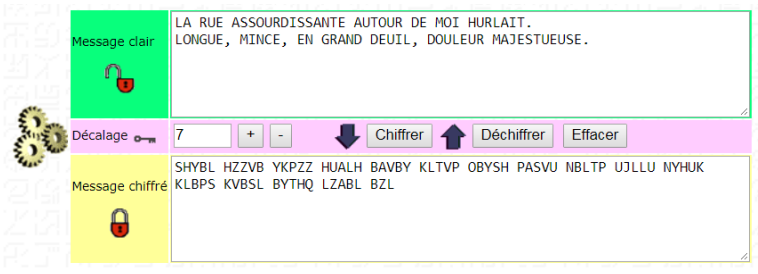
Exercice 1 : « Chiffre de César »

1. Chiffrer à la main le texte suivant en décalant les lettres de 7 rangs puis vérifier avec le programme :
« La rue assourdissante autour de moi hurlait. Longue, mince, en grand deuil, douleur majestueuse. »

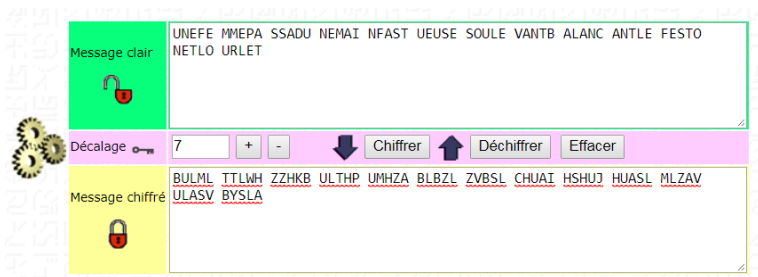
2. Déchiffrer à la main le texte ci-dessous chiffré avec le chiffre de César en décalant les lettres de 7 rangs :
« BULML TTLWH ZZHKB ULTHP UMHZA BLBZL ZVBSL CHUAI HSHUJ HUASL MLZAV ULASV BYSLA »

Corrigé :

1.



2.

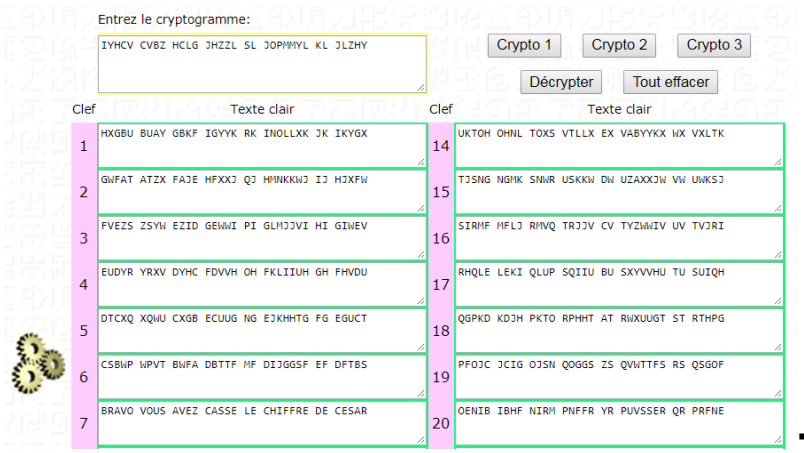


Exercice 2 : « Décryptement du chiffre de César »

1. Décrypter les trois cryptogrammes proposés (Crypto 1, Crypto 2 et Crypto 3).

Corrigé :

1.

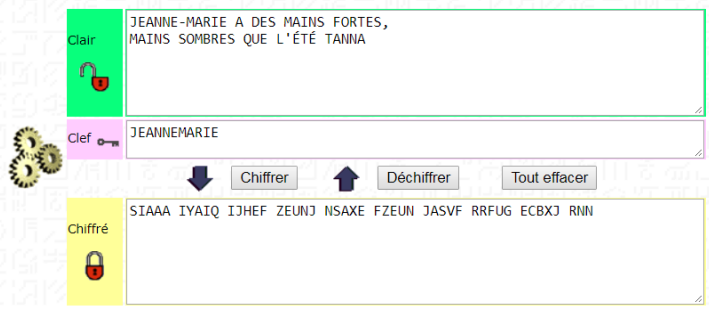


➔ 7

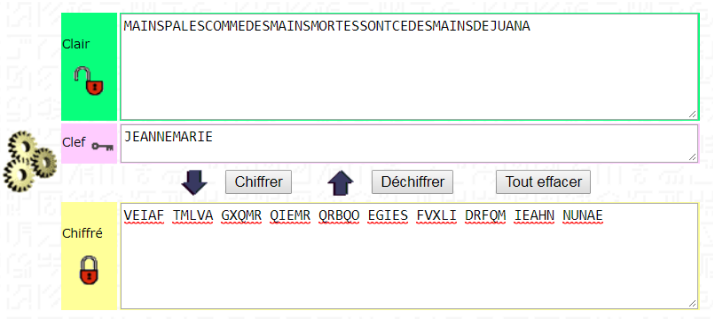
Exercice 3 : « Chiffre de Vigenère »

1. Chiffrer à la main le texte suivant en utilisant le mot-clef « Jeanne-Marie » puis vérifier avec le programme :
   « Jeanne-Marie a des mains fortes,
   Mains sombres que l'été tanna »
2. Déchiffrer à la main le texte suivant en utilisant le mot-clef « Jeanne-Marie » :
   « VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE »

Corrigé :

1. 

2.

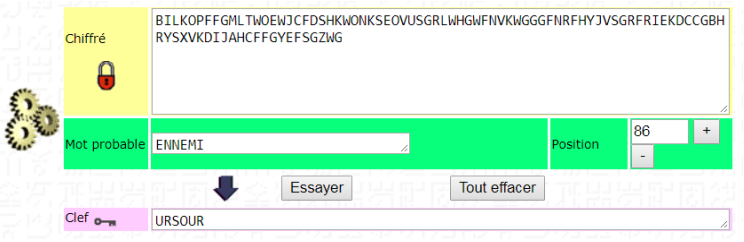


Exercice 4 : « Décryptement du chiffre de Vigenère »

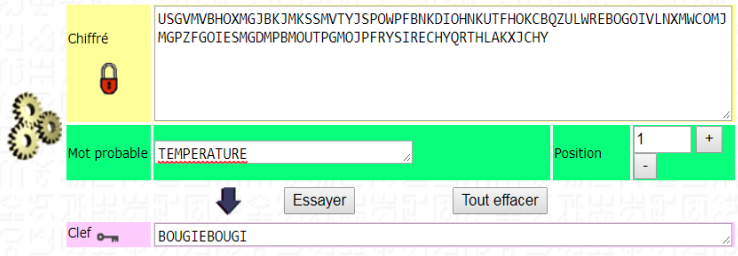
1. Faire une attaque par mot probable dans le cryptogramme de l'exemple en utilisant le mot « ENNEMI » (commencer à la position 80).
2. Décrypter le message suivant, sachant qu'il débute par un bulletin météorologique :
« USGVM VBHOX MGJBK JMKSS MVTYJ SPOWP FBNKD IOHNK UTFHO KCBQZ ULWRE BOGOI VLNXM WCOMJ MGPZF GOIES MGDMP BMOUT PGMOJ PFRYS IRECH YQRTH LAKXJ CHY »

Corrigé :

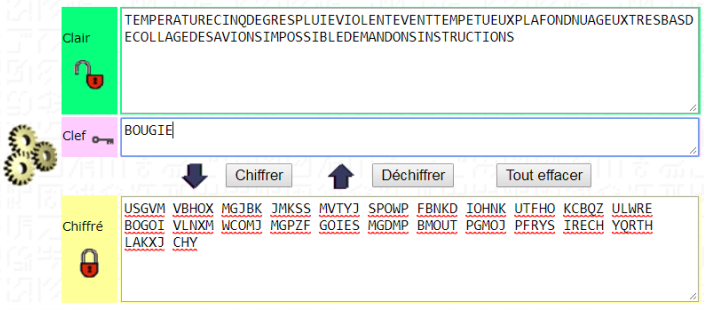
1.



➔ OURS



2. ➔ **BOUGIE**

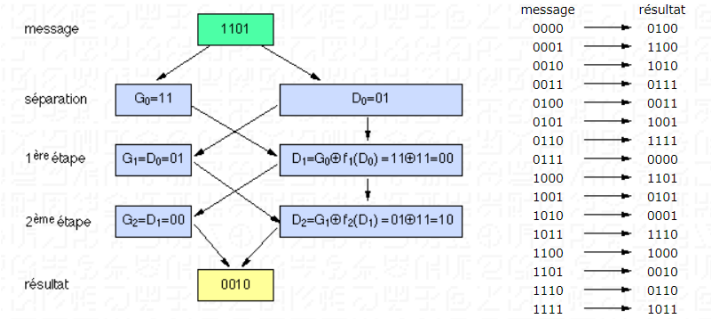


Exercice 5 : « Réseau de Feisel »

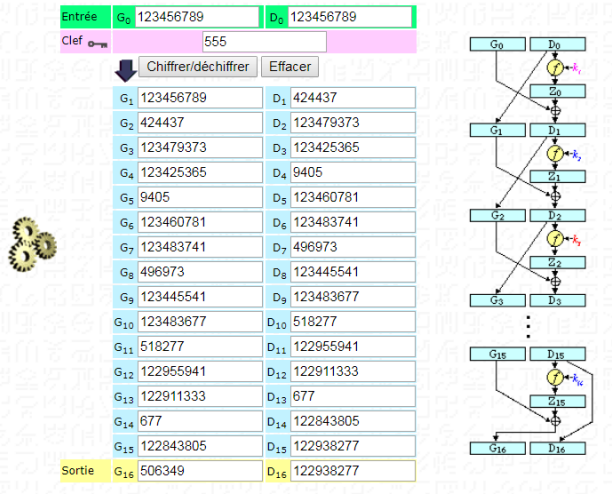
1. Vérifier les images des 16 messages possibles.
2. Trouver comment déchiffrer les messages (cela revient à utiliser le schéma de Feistel "à l'envers").

Corrigé :

1.



2.



Exercice 6 : « RSA »

Partie I

1. Chiffrer le message de l'exemple du Javascript avec les 2 tables de conversion.
2. Quelle est la différence ?

Partie II

1. Reprendre l'exemple du cours, chiffrer puis déchiffrer.
2. Varier le e. Que se passe-t-il ?
3. Varier le d. Que se passe-t-il ?
4. Varier la taille du bloc. Que se passe-t-il ?

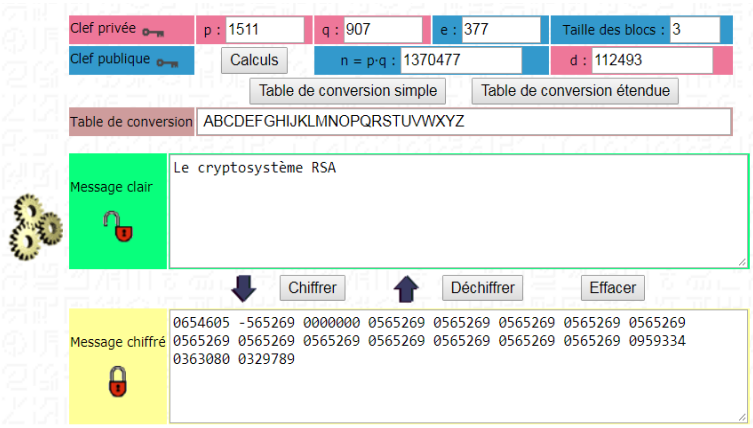
Partie III

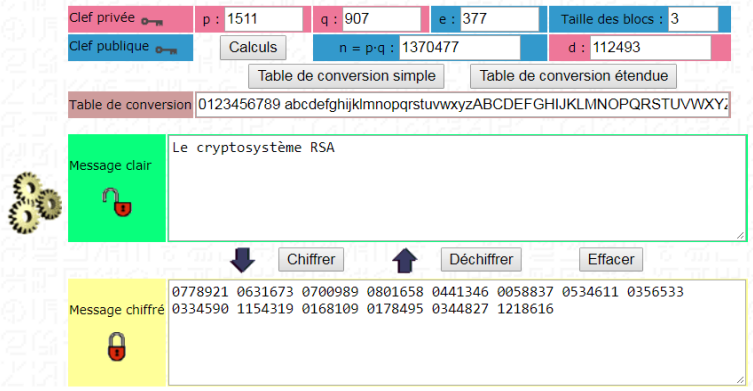
1. Reprendre l'exercice donné dans le cours.
2. Chiffrer à la main le mot "bonjour", puis déchiffrer.
3. Vérifier avec le programme.

Partie IV

1. Chiffrer le mot "bonjour" avec p=3, q=11, e=11 et bloc de 2. Que peut-on dire ?
2. Chiffrer le mot "bonjour" avec p=3, q=11, e=11 et bloc de 3. Que peut-on dire ?

Corrigé :





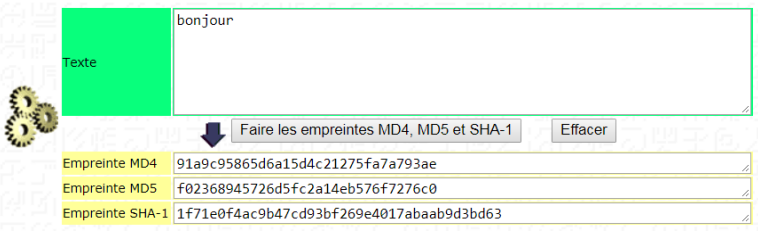
Exercice 7 : « Intégrité »

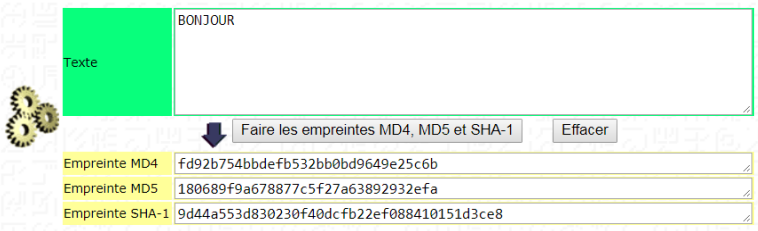
Créer les empreintes des messages suivants :

- bonjour
- BONJOUR

1. Que peut-on dire sur les différentes empreintes créées par MD4 MD5 et SHA-1 ?
2. Que peut-on dire lorsqu'on modifie un caractère du message ?

Corrigé :





➔ C'EST DIFFERENT

III. Politique de sécurité

III.1. Plan de sécurité

•les cinq phases suivantes sont importantes en matière de sécurité pour réduire les risques :
▫Inspection
▫Protection
▫Détection
▫Réaction
▫Réflexion

Inspection

•L'inspection permet de faire :
•L'identification des besoins (inventaire des ressources)
▫Personnes, fonctions, matériels, réseau, communications, données et etc.
•L'analyse des risques
▫ Evaluation de la menace (faible, moyenne, haute)
▫Analyse des pertes (analyse de l'impact commercial)
▫Identification des vulnérabilités
•La définition de la politique de sécurité
▫Organisation de la protection
▫Sauvegardes, etc.
▫**NB :**
Charte de sécurité : ensemble de lois (règlement)
Politique de sécurité : manière de diriger (stratégie)

Protection

•La protection permet de protéger l'information définies dans la politique de sécurité avec :
▫Sécurité physique
▫Contrôle d'accès
▫Chiffrement des données
▫Pare-feu, antivirus
▫Sauvegardes
▫**NB:**
Audit de sécurité: consiste à s'appuyer sur une société spécialisée en sécurité afin de valider la politique de sécurité définie.

Détection

•La détection doit permettre de détecter les :
▫Incidents
Prévoir des détecteurs de fumée
▫Intrusions
Analyse des traces
Analyse du trafic
Analyse des événements

▫**NB:**
IDS (Intrusion Detection Systems) en générant des alertes

Réaction
•La réaction consiste à la mise en place d'un plan de secours d'urgence :
•Surveiller et avertir : dès qu'un incident est détecté un responsable en est averti.
•Réparer et signaler : tenter de remédier à l'incident le plus vite possible, signaler au responsable.
•Poursuivre en justice : Rassembler les preuves et alerter le plus vite possible le service juridique de l'entreprise.
▫**Exemple :**
Extinction du disjoncteur (si c'est physique)
Obtention de l'adresse du pirate
Extinction de l'alimentation de la machine
Débranchement de la machine du réseau
Restauration

Réflexion
•La réflexion sont les procédures à suivre après un incident
▫Documentation de l'incident
▫Évaluation de l'incident
▫Relations publiques
▫Suites judiciaires
▫**NB:**
Répétition du plan de sinistre pour sensibiliser les responsables de cet acte.

III.2. Cybercriminalité
•La cybercriminalité, c'est l'ensemble des infractions pénales commises sur les réseaux de télécommunication (Larousse).
NB :
▫Infractions liés aux :
Technologies (virus, ver, …)
Contenus (racisme, …)
▫Infractions facilitées par les :
Réseaux (copies illicites de logiciels ou d'oeuvres audiovisuelles …)
•Il n'existe à l'heure actuelle aucune législation véritablement internationale concernant la criminalité informatique.

•La cybercriminalité recouvre deux types d'infractions pénales :
•les infractions spécifiques aux technologies de l'information et de la communication (TIC) dans lesquelles l'informatique est l'objet même du délit.
les infractions aux cartes bancaires.
•les infractions liée ou facilitée par les TIC et pour lesquelles l'informatique n'est qu'un moyen.

les atteintes aux personnes.
les escroqueries en ligne.
la violation de propriété intellectuelle.

•Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

III.3. Cybersécurité

•C'est un état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
•La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
•**NB:** ensemble des procédés informatiques visant à protéger les données transitant par Internet

III.4. Autres définitions

•Cyberespace :
Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.
•Cyberdéfense :
Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

III.5. Méthode de sécurité

•Méthode M.A.R.I.O.N
▫Méthode d'Analyse des Risques Informatiques optimisée par Niveau. (à partir de 1984)
▫C'est une méthode d'audit, visant à évaluer le niveau de sécurité informatique d'une entreprise.
•Méthode MEHARI
▫Méthode harmonisée d'analyse des risques
▫C'est une méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme
□ISO 27001
•Méthode EBIOS
▫Expression des besoins et identification des objectifs de sécurité
▫Elle permet de comprendre les risques Sécurité des systèmes d'information et de contribuer à leur traitement.
□Compatible avec la norme ISO 17799

III.6. Norme de sécurité

•Norme = règle

•ISO Organisation internationale de normalisation (International Organization for Standardization)
•ISO 17799
▫Sécurité de l'information 2000
•ISO 27001
▫Système de gestion de la sécurité de l'information 2005
•ISO 27005
▫Complément de 27001 2008

Mieux vaut Prévenir que Guérir

Fiche TD 1 « Charte de Sécurité »

Exercice 1 :

1. Dans le mémento, pourquoi on parle de « safety » et pas de « security » ?
2. Le mémento parle de la formation ou de la sensibilisation ? ou des deux ? Pourquoi ?
3. Donner une menace non informatique non intentionnelle.
4. Donner la contre mesure en prévention de la menace citée dans la question 3.

Exercice 2 :

1. Quelles sont les points les plus importants traités dans la charte informatique ?
2. Quelles sont les interdits cités dans la charte informatique ?
3. A quel niveau intervient la « réaction » dans la charte informatique ?

Exercice 3 :

1. Comment se fait la gestion du choix du mot de passe sécurisé ? pourquoi ?
2. Pourquoi l'utilisateur doit signer à la fin ?

IV. Stockage

IV.1. Support de stockage

•Les supports de stockage informatique on beaucoup évolués ces dernières années.
•Les unités de mesure sont :

Le kilo-octet (ko) = 1 000 octets
Le méga-octet (Mo) = 1 000 ko
Le giga-octet (Go) = 1 000 Mo
Le téra-octet (To) = 1000 Go

Disquette

•La disquette 3 ½ pouce peuvent stocker 1.44 Mo.
•Elle a été lancée par IBM en 1697 en 8 pouces.
•En 1978, une version plus petite 5 ¼ pouce.
•En 1984, Apple lance une plus petite 3 ½ pouce.

NB:

▫Ils ont disparu à cause de leur faible espace de stockage.

CD Rom

•Il a été inventé par Philips en 1979 puis en audio en 1982 pour stocker les données.
•Sa capacité est de 700 Mo pour CD R et 650 Mo pour CD RW

NB:

□R read
□RW read write

DVD Rom

•Il a été lancé en 1995 pour stocker des données.
•Sa capacité est de 4,7 Go en simple couche et 8,5 Go en double couche.

NB:

▫Blu-Ray de 25 à 128 Go pour le stockage des films en 3D
▫HVD de capacité 3,9 To

Disque dur

•Il a été inventé en 1956 pour stocker des données sous forme de fichiers et dossiers.
•Leurs capacités est de 250 Go à 3 To
•Ils tournent à une vitesse de 7200 tours/minutes.

NB:

▫Plus le disque tourne vite moins le temps d'accès sera long.

SSD

•Solid State Drive, lecteur à l'état solide
•C'est une unité de stockage constituée d'une mémoire flash.
•Sa capacité va de 32 Go à 2 To.

NB:

▫Avantage : silence de fonctionnement + vitesse à des milliers de tours par minute+ pas de mécanique + faible consommation électrique + résistant aux chocs

Inconvénient : prix

Carte mémoire

•Elle permet de transférer des données entre appareils.
•Les appellations sont : MS, SD, MMC, SM.
•Leurs capacités actuelles sont de 2 Go, 8 Go à 2 To

NB:

▫La carte SD de 512 Mo est compatible avec tous les appareils

Clé USB

•C'est un petit support de stockage qui se branche sur un port USB.
•Sa capacité est de 1 Go à 256 Go.
•Elle est pratique pour transférer des données entre ordinateurs sans installer un programme.

NB:

▫Certains intègre un mot de passe comme moyen de sécurité.

Autres supports

•Lecteur Zip avec une capacité de 750 Mo
•Lecteur REV est actuellement le plus répandu avec une capacité de stockage de 75 Go.
•Lecteur de bande magnétique utilisé par l'armé ou les grandes surfaces.

La clé USB du futur peut stocker 360 To de donnés pendant 14 milliards d'années

Disque dur de Quartz 5d de 360 To

Microsoft voit le futur du stockage des données… dans notre ADN

Capacités de stockage XXL !!!

V. Partitionnement

V.1. Définition du partitionnement

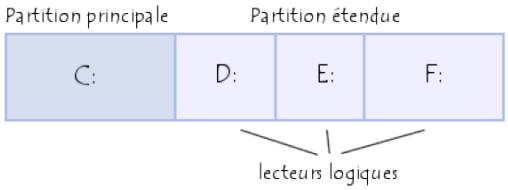
•C'est le partage d'un support de stockage en unités distinctes.
•Elle est utilisée en informatique, où cette expression fait référence à la partition d'un disque dur, c'est-à-dire à l'une de ses parties dont on diminue le volume, le plus souvent dans le but de créer une autre partition.

V.2. Objectif de partition

•Installer plusieurs systèmes d'exploitation sur le disque n'utilisant pas le même système de fichiers
•Organiser les données plus facilement en créant plusieurs lecteurs dont les données sont séparées.
•Économiser de l'espace disque
•Augmenter la sécurité de des fichiers

V.3. Type de partition

•La partition principale
▫Elle doit être formatée logiquement, puis contenir un système de fichier correspondant au système d'exploitation installé sur cette partition.
•La partition étendue
▫Elle a été mise au point pour outrepasser la limite des quatre partitions principales, en ayant la possibilité de créer autant de lecteurs logiques cette partition.
•Les lecteurs logiques
C'est l'impression qu'on ait plusieurs disques durs de taille inférieur.



NB:
•Un disque peut contenir jusqu'à :
•Quatre partitions principales
•Dont une seule peut être active et visible,
•Ou trois partitions principales et une partition étendue.
•Au moins un lecteur logique est nécessaire dans une partition étendue.

V.4. Table de partitions

•Les informations sur les partitions sont conservées sur le disque dans des zones appelées tables de partitions (partition map).
•La table de partitions principale est contenue dans le premier secteur du disque ou secteur d'amorçage (MBR ou GPT) qui contient le programme d'amorçage.

•NB:

▫Chaque ligne d'une table de partitions contient l'adresse de début de la partition et sa taille.

MBR

•Le secteur de démarrage (appelé Master Boot Record ou MBR en anglais) est le premier secteur d'un disque dur (cylindre 0, tête 0 et secteur 1).

•Il contient la table de partition principale (partition table) et le code, appelé boot loader, qui, une fois chargé en mémoire, va permettre d'amorcer (booter) le système.

•NB :

▫Ce secteur est le plus important du disque dur, il sert au setup du BIOS à reconnaître le disque dur.

▫Sans lui, le disque dur est inutilisable, c'est une cible de prédilection pour les virus.

GPT

•C'est une table de partitionnement GUID, en anglais GUID Partition Table (GPT) est un standard pour décrire la table de partitionnement d'un disque dur.

•NB :

▫Il est utilisé sur certains BIOS à cause des limitations de la table de partitionnement du MBR.

V.5. Système de fichier

•Un système de fichiers (« FS » pour File System en anglais) ou système de gestion de fichiers (SGF) est une façon de stocker les informations et de les organiser dans des fichiers sur des supports de stockage.

Fonctions d'un SGF

•Manipulation des fichiers;

•Allocation de la place sur mémoires secondaires;

•Localisation des fichiers;

•Sécurité et contrôle des fichiers :

Il permet le partage des fichiers par différents programmes d'applications tout en assurant la sécurité et la confidentialité des données.

Donc, un nom et une clé de protection sont associés à chaque fichier afin de le protéger contre tout accès non autorisé ou mal intentionné lors du partage des fichiers.

Le SGF se doit aussi de garantir la conservation des fichiers en cas de panne du matériel ou du logiciel.

Système de fichiers et système d'exploitation

•Le choix du système de fichiers se fait en premier lieu suivant le système d'exploitation.

•**NB** :
▫Plus le système d'exploitation est récent plus le nombre de systèmes de fichiers supportés sera important.

Exemples de système de fichiers
•FAT : c'est une table d'allocation de fichiers (en anglais FAT, File Allocation Table).
•NTFS : c'est un système de fichiers développé par Microsoft Corporation pour sa famille de systèmes d'exploitation (New Technology File System).
•EXT : c'est le premier système de fichiers créé en avril 1992 spécifiquement pour le système d'exploitation Linux (extended file system).

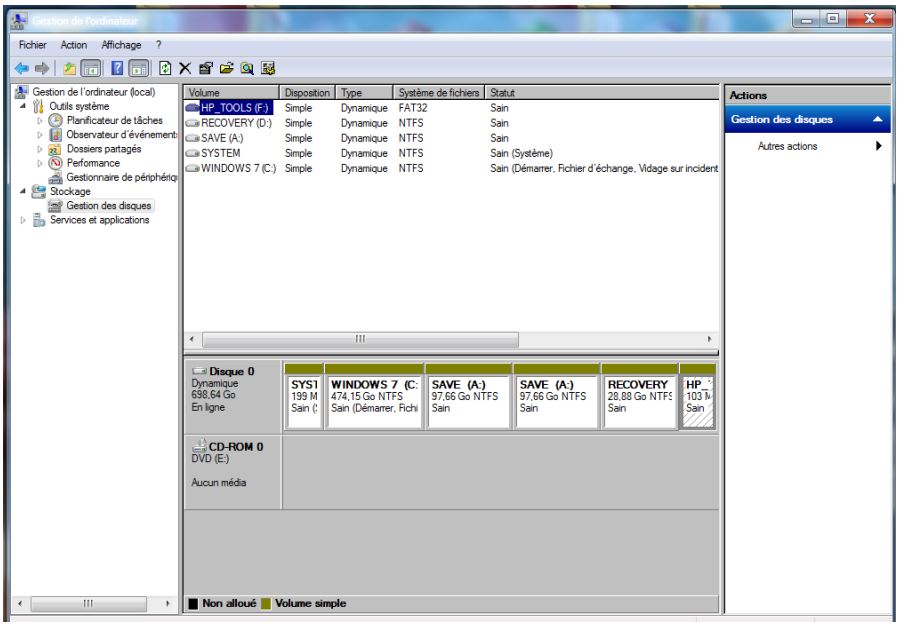
Système d'exploitation	Types de système de fichiers supportés
Dos	FAT16
Windows 95	FAT16
Windows 95 OSR2	FAT16, FAT32
Windows 98	FAT16, FAT32
Windows NT4	FAT, NTFS (version 4)
Windows 2000/XP	FAT, FAT16, FAT32, NTFS (versions 4 et 5)
Linux	Ext2, Ext3, ReiserFS, Linux Swap(, FAT16, FAT32, NTFS)
MacOS	HFS (Hierarchical File System), MFS (Macintosh File System)
OS/2	HPFS (High Performance File System)
SGI IRIX	XFS
FreeBSD, OpenBSD	UFS (Unix File System)
Sun Solaris	UFS (Unix File System)
IBM AIX	JFS (Journaled File System)

Fiche TP 2 « Partitionnement »

Exercice 1 :

1. Cliquer bouton droit sur « Ordinateur » puis « Gérer ».
2. Cliquer sur « Stockage » puis « Gestion des disques ».
3. Citer les informations obtenues.
4. Choisir un volume puis cliquer sur « Réduire le volume »
5. Créer un volume logique.

Corrigé :



Exercice 2 :

1. Tester le shareware « Disk Password Protection ».

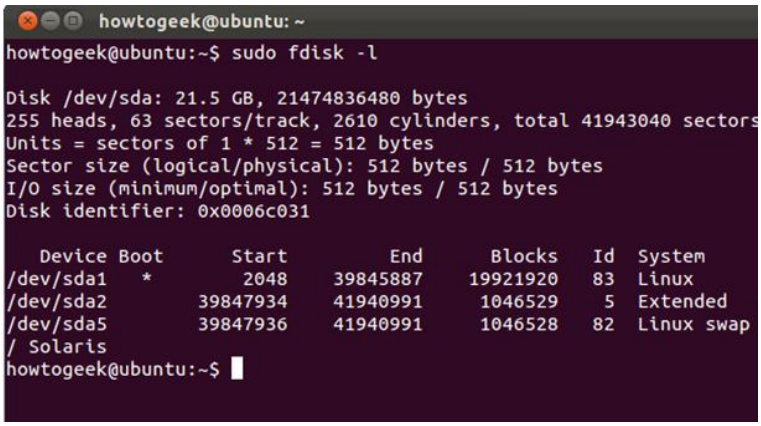
   NB: Attention le PWD sera en qwerty !
2. Tester le freeware « TrueCrypt ».

Corrigé :

Exercice 3 :

1. Tester « fdisk » sous « ubuntu ».

Corrigé :



V.6. Système de Droits

Droit d'accès

•Le droit sur un fichier permet de limiter les accès à une information dans un base de données, droit d'administration, serveur informatique ou outils de sécurité comme FW, suivant un certain nombre de paramètres.

•**NB**:

▫C'est une base de la sécurité informatique

Droits de fichier

•Les trois principaux droits sur des fichiers sont :

▫la lecture

r

▫l'écriture

w

▫l'exécution

x

•L'exécution d'un fichier correspond :

▫pour un programme : à son exécution, son lancement

▫pour un répertoire : à y entrer

Permission Unix

•Unix est un système multiutilisateurs.

▫Donc, plusieurs personnes peuvent travailler simultanément sur le même OS.

•Puisque plusieurs utilisateurs peuvent être connectés en même temps.

▫Donc, avoir une excellente organisation dès le départ.

▫Ainsi, chaque personne a son propre compte utilisateur.

▫De ce fait, il existe un ensemble de règles qui disent qui a le droit de faire quoi.

Droits d'Unix

•Les droits sont associés à trois types d'utilisateurs :

▫le propriétaire du fichier

u

▫les utilisateurs appartenant au groupe auquel appartient le fichier

g

▫tous les autres utilisateurs

o

•**NB**:

▫Seuls root et le propriétaire d'un fichier peuvent changer ses permissions d'accès.

Lorsque le droit n'est pas attribué, on écrit un tiret « - »

Représentation des droits

```
rwxr-xr--
\ /\ /\ /
 v  v  v
 |  |  droits des autres utilisateurs (o)
 |  |
 |  droits des utilisateurs appartenant au groupe (g)
 |
droits du propriétaire (u)
```

Définition privilège

•C'est un avantage exclusif, droit particulier, accordé à quelqu'unou à une certaine catégorie de population.

NB:

passe-droit

Attribution des privilèges

•Ils sont attribuer à :

▫Utilisateur spécifique

Administrateur

Modérateur

▫Groupe d'users

Membre d'un département

Gestion des privilèges

•Elle se fait selon :

▫Groupe de travail (Workgroups)

▫Groupe résidentiel

▫Domaines spécifiques aux serveurs réseaux

Exemple SQL

Classes de privilèges	Types de compte
accès au contenu de l'information	utilisateur, application
gestion du schéma de la base de données	administrateur, application (parfois)
gestion des privilèges utilisateurs	administrateur
gestion des paramètres systèmes	administrateur

V.7. Redondance (Redundancy)

Définition de la redondance

•En informatique et dans les télécommunications, duplication d'informations afin de :

▫ Garantir leur sécurité en cas d'incident (Larousse)

▫Corriger des erreurs de transmissions pour assurer la fiabilité

code correcteur

▫Détecter les erreurs

somme de contrôle

▫Assurer un fonctionnement sans interruption en cas de dysfonctionnement du premier, le second en reprend le relais

•**NB**:

La compression de données permet de réduire ou d'éliminer la redondance que l'utilisateur ne désire pas conserver

Contrôle par redondance

•Un contrôle par redondance consiste à ajouter des données à la fin d'un message pour détecter des erreurs et éventuellement les corriger.

•N'importe quelle fonction de hachage comme MD5 peut être utilisée en tant que contrôle par redondance.

•Les plus simples sont les sommes de contrôle, incluant le bit de parité. On trouve également d'autres contrôles par redondance : le CRC (Cyclic Redundancy Check) ou (Contrôle de redondance cyclique)

Code correcteur

On présente ici un exemple élémentaire de code correcteur obtenu en complétant une suite de trois nombres (constituant l'information à transmettre) par deux autres nombres (constituant le code de contrôle de l'information). L'ensemble des cinq nombres permet alors de détecter et de corriger une erreur qui se serait produite sur l'un des trois premiers nombre lors de la transmission.

Soit donc un bloc de 3 nombres que l'on souhaite transmettre : 02 09 12

Ajoutons deux nombres de contrôle de l'information.
Le premier est la somme des 3 nombres : 02 + 09 + 12 = 23
Le second est la somme pondérée des 3 nombres, chacun est multiplié par son rang : 02×1 + 09×2 + 12×3 = 56
À la sortie du codeur, le bloc à transmettre est : 02 09 12 23 56

À la suite d'une perturbation, le récepteur reçoit : 02 **13** 12 23 56

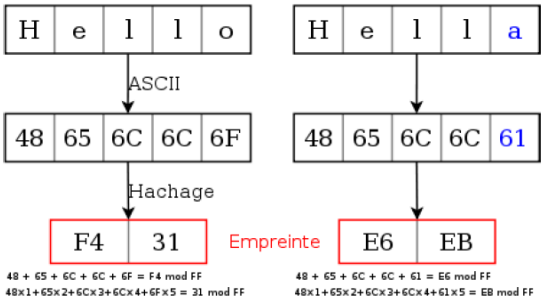
À partir des données reçues, le décodeur calcule :
Sa somme simple : 02 + **13** + 12 = **27**
Sa somme pondérée : 02x1 + **13**x2 + 12x3 = **64**

La différence entre la somme simple calculée (**27**) et celle reçue (23) indique la valeur de l'erreur : **4** (**27**-23 = **4**)
La différence entre la somme pondérée calculée (**64**) et celle reçue (**56**), elle-même divisée par la valeur de l'erreur indique la position o l'erreur se trouve : 2 ((**64**-**56**) / **4** = 2).
Il faut donc retirer 4 au nombre du rang 2.

Le bloc original est donc 02 (**13**-4=09) 12 23 56

Lors d'une transmission sans perturbation, les différences des sommes simples et des sommes pondérées sont nulles.

Somme de contrôle

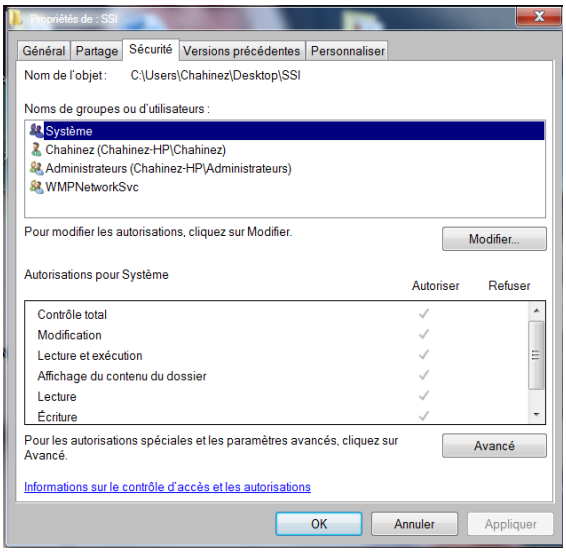


Fiche TP 3 « Droit d'Accès »

Exercice 1 : « Windows »

1. Cliquer avec le bouton droit sur le dossier ou fichier à sécuriser.
2. Cliquer sur l'onglet « Sécurité ».
3. Choisir l'autorisation.

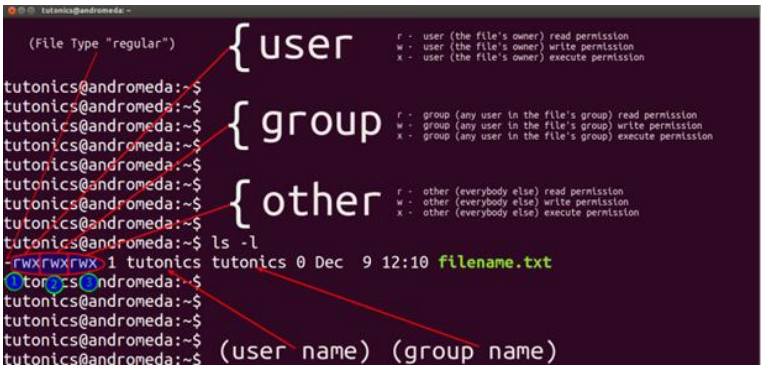
Corrigé :



Exercice 2 : « Ubuntu »

1. Lire les informations des 3 pages web données.
2. Cliquer avec le bouton droit sur le fichier à sécuriser, puis sur « Permissions ».
3. Tester la commande « Chmod ».

Corrigé :



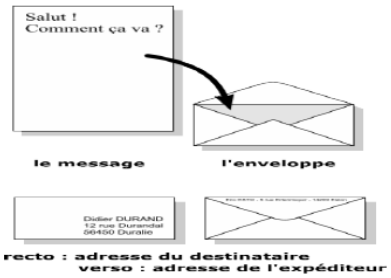
VI. Sécurité TCP/IP

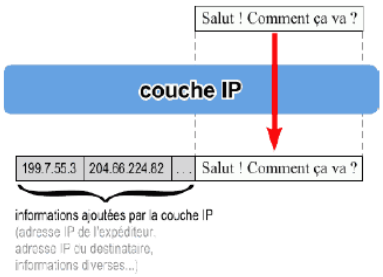
VI. 1. Rappel TCP/IP

•TCP/IP est un protocole de communication.
•IP signifie Internet Protocol : C'est le principal protocole utilisé sur Internet.
•IP permet aux ordinateurs reliés à des réseaux de dialoguer entre eux.
•Faisons un parallèle avec la poste.

IP

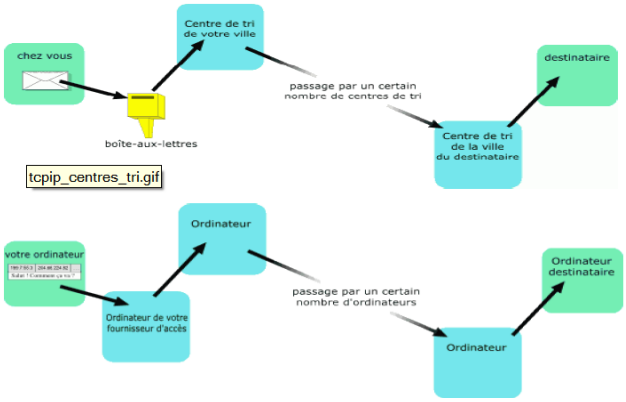
•Quand vous voulez envoyer une lettre par la poste:
•vous placez votre lettre dans une enveloppe,
•sur le recto vous inscrivez l'adresse du destinataire,
•au dos, vous écrivez l'adresse de l'expéditeur (la votre).
•l'adresse de l'expéditeur (votre adresse IP),
•l'adresse IP du destinataire,
•différentes données supplémentaires (qui permettent de bien contrôler l'acheminement du message).





Adresse IP est une adresse unique à chaque ordinateur sur Internet, de même, l'adresse postale.

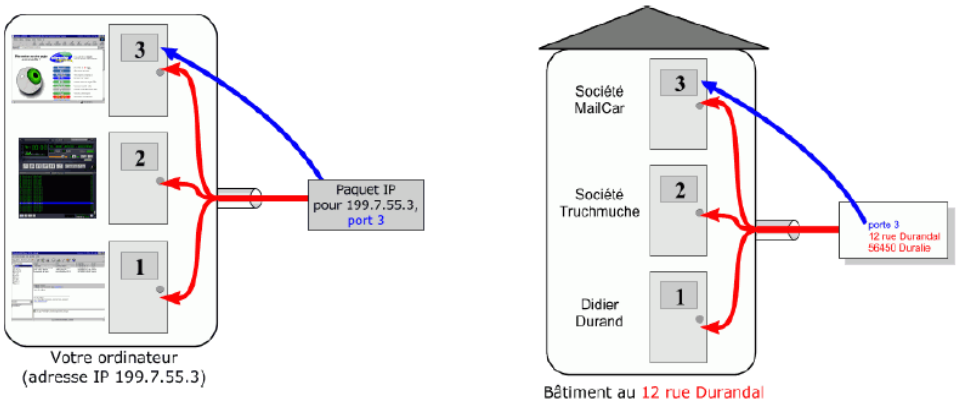
Routage IP



Ports

L'adresse IP permet de s'adresser à un ordinateur donné, et le numéro de port permet de s'adresser à un logiciel particulier sur cet ordinateur.

UDP/IP est un protocole qui permet justement d'utiliser des numéros de ports en plus des adresses IP



TCP Transmission Control Protocol

•Quand vous envoyez un paquet IP sur Internet. Et il arrive que des paquets IP se perdent ou arrivent en double exemplaire.

•La taille des paquets IP est limitée (environ 1500 octets).

•C'est pour cela qu'a été conçu TCP.

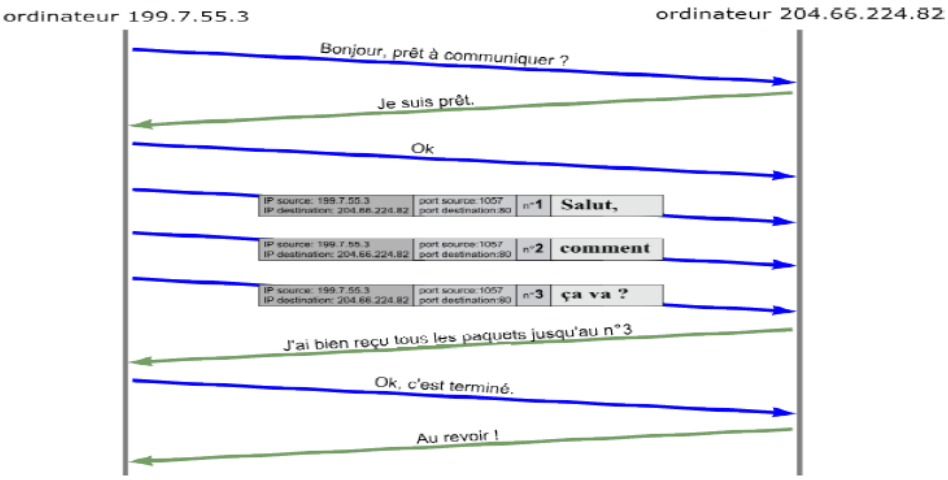
•TCP est capable:

•de faire tout ce que UDP User Datagram Protocol sait faire (ports).

•de vérifier que le destinataire est prêt à recevoir les données.

•de découper les gros paquets de données en paquets plus petits pour que IP les accepte

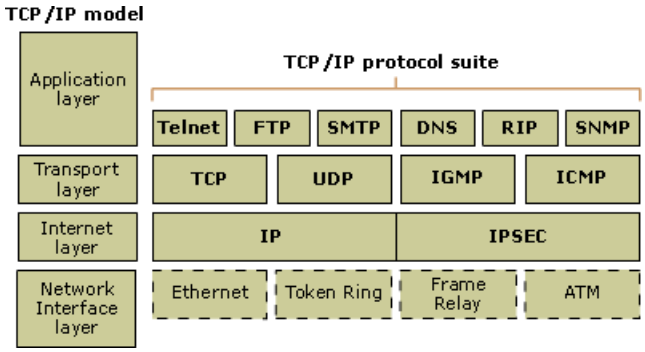
•de numéroter les paquets, et à la réception de vérifier qu'ils sont tous bien arrivés, de redemander les paquets manquants et de les réassembler avant de les donner aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées.



Par exemple, pour envoyer le message "Salut, comment ça va ?", voilà ce que fait TCP (Chaque flèche représente 1 paquet IP):

A l'arrivée, sur l'ordinateur 204.66.224.82, la couche TCP reconstitue le message "Salut, comment ça va ?" à partir des 3 paquets IP reçus et le donne au logiciel qui est sur le port 80

Modèle TCP/IP



Application

Définit les protocoles d'application TCP/IP et explique comment l'hôte programme l'interface avec les services de couches de transport pour utiliser le réseau.

HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, autres protocoles d'application

Transport

Propose la gestion des sessions de communication entre les ordinateurs hôtes. Définit le niveau de service et l'état de la connexion utilisés lors du transport des données.

TCP, UDP, RTP

Internet

Regroupe les données en datagrammes IP qui contiennent des informations sur les adresses de source et de destination utilisées pour transmettre les datagrammes entre les hôtes et à travers les réseaux. Effectue le routage des datagrammes IP.

IP, ICMP, ARP, RARP

Interface réseau

Donne des détails sur le mode d'envoi physique des données à travers le réseau, y compris sur la façon dont les bits sont électriquement signalés par les périphériques matériels jouant directement le rôle d'interface avec un support réseau, comme un câble coaxial, une fibre optique ou un fil de cuivre à paire torsadée.

Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

VI. 2. Méthodologie d'attaque

Récupération d'informations sur le système

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de prise d'empreinte, est un préalable à toute attaque. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible :

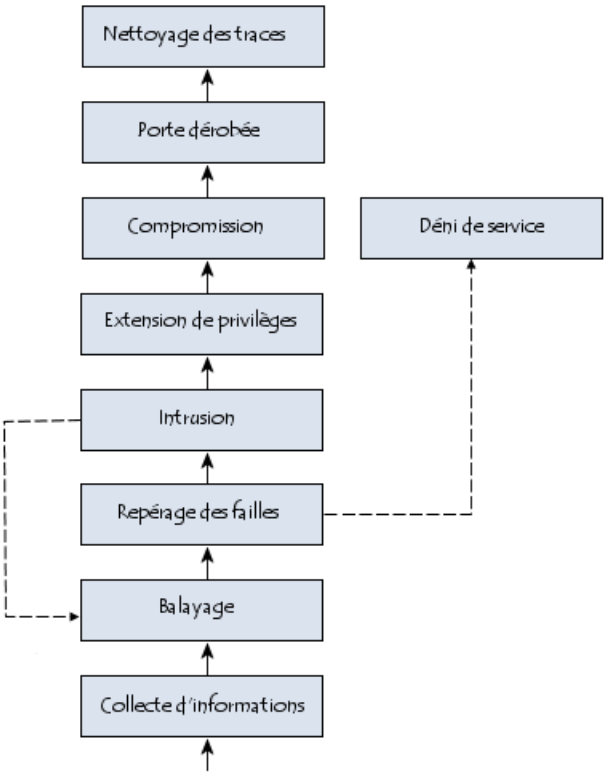
Adressage IP,

Noms de domaine,

Protocoles de réseau,

Services activés,

Architecture des serveurs, etc.



Balayage du réseau

Lorsque la topologie du réseau est connue par le pirate, il peut le scanner (le terme balayer est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé scanner ou scanneur en français) quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.
L'un des outils les plus connus pour scanner un réseau est Nmap, reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau.

Ingénierie sociale

L'ingénierie sociale (en anglais « Social Engineering ») consiste à manipuler les êtres humains, c'est-à-dire d'utiliser la naïveté et la gentillesse exagérée des utilisateurs du réseau, pour obtenir des informations sur ce dernier. Ce procédé consiste à entrer en contact avec un utilisateur du réseau, en se faisant passer en général pour quelqu'un d'autre, afin d'obtenir des renseignements sur le système d'information ou éventuellement pour obtenir directement un mot de passe. De la même façon une faille de sécurité peut être créée dans le système distant en envoyant un cheval de Troie à certains utilisateurs du réseau.

Repérage des failles

Il existe ainsi des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité. Le principal scanneur de failles est :
Nessus

L'intrusion

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :
L'ingénierie sociale, leur identifiant de connexion et leur mot de passe. se faisant passer pour l'administrateur réseau.
La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides
Les attaques par force brute (brute force cracking), consistant à essayer de façon automatique différents mots de passe sur une liste de compte

Extension de privilèges

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se logeant sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant l'accès root (en français superutilisateur ou superadministrateur), on parle ainsi d'extension de privilèges.
Il lui est ainsi possible d'installer un sniffeur (en anglais sniffer), c'est-à-dire un logiciel capable d'écouter (le terme reniffler, ou en anglais sniffing, est également employé) le trafic réseau en provenance ou à destination des machines situées sur le même brin.

Compromission

Grâce aux étapes précédentes, le pirate a pu dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès root sur au moins l'une d'entre-elles. Cette technique d'usurpation d'identité, appelée spoofing, permet au pirate de pénétrer des réseaux privilégiés auxquels la machine compromise a accès.
Porte dérobée
Lorsqu'un pirate a réussi à infiltrer un réseau d'entreprise et à compromettre une machine, il peut arriver qu'il souhaite pouvoir revenir. Pour ce faire celui-ci va installer une application afin de créer artificiellement une faille de sécurité, on parle alors de porte dérobée (en anglais backdoor, le terme trappe est parfois également employé).

Nettoyage des traces

Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant en supprimant les lignes d'activité concernant ses actions. Par ailleurs, il existe des logiciels, appelés « kits racine » (en anglais « rootkits »). L'objectif d'un rootkit est donc de tromper l'administrateur en lui masquant la réalité.

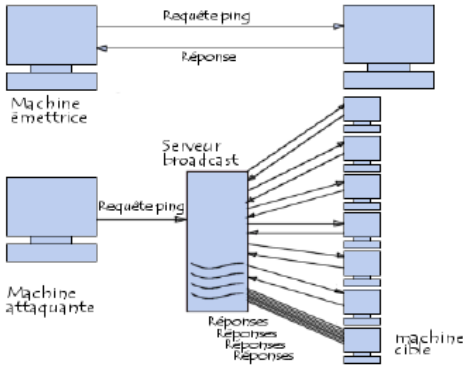
VI. 3. DOS

Attaques par déni de service (Refus)

Une « attaque par déni de service » (en anglais « Denial of Service », abrégé en DoS) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

La technique dite « par réflexion »

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



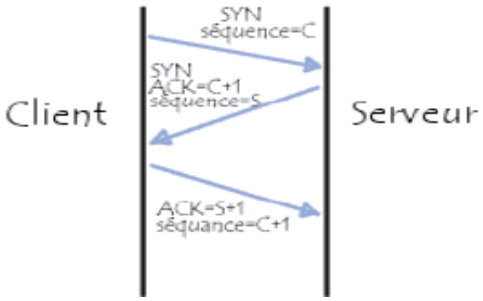
Attaque du ping de la mort

L'attaque du ping de la mort » (en anglais « ping of death ») est une des plus anciennes attaque réseau.

Le principe du ping de la mort consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage.

Plus aucun système récent n'est vulnérable à ce type d'attaque.

L'« attaque SYN » (appelée également « TCP/SYN Flooding ») est une attaque réseau par saturation (déni de service) exploitant le mécanisme de poignée de main en trois temps (en anglais Three-ways handshake) du protocole TCP.



Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet ACK.

NB

•Attaque :

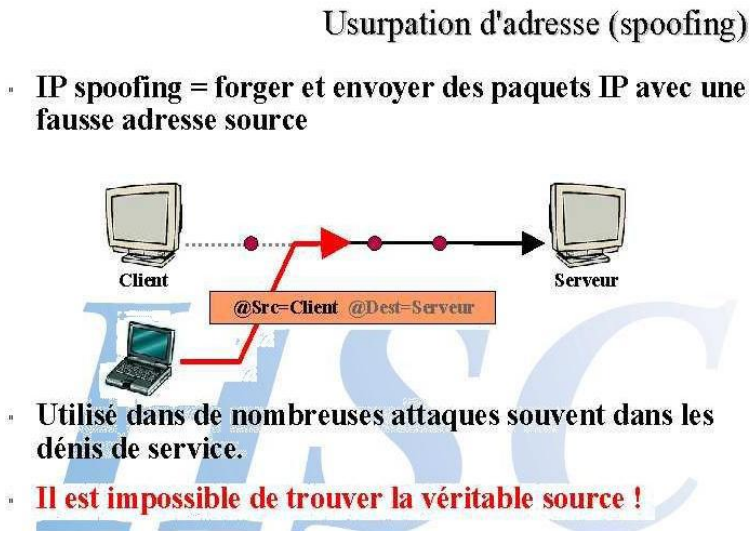
▫Découverte systématique d'information, tentative réelle d'intrusion ou déni de service.

•Intrusion :

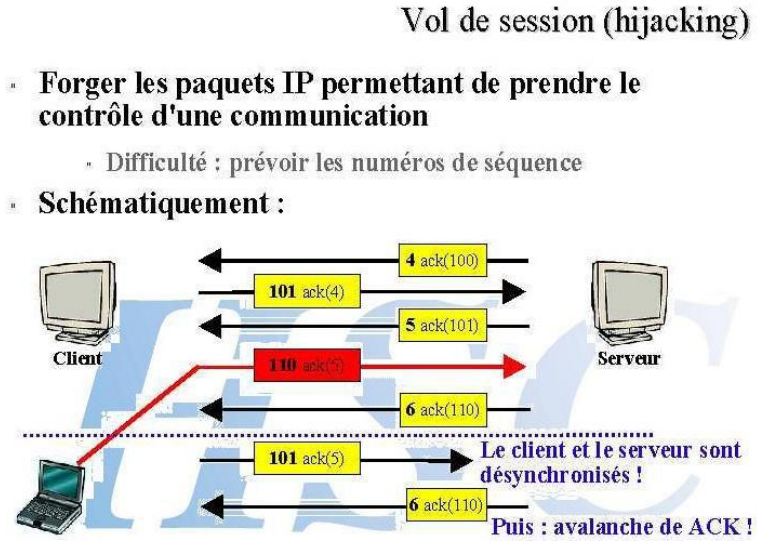
▫Prise de contrôle partielle ou totale d'un système distant.

VI. 4. Techniques

L'« usurpation d'adresse IP » (également appelé mystification ou en anglais spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.



Le « vol de session TCP » (également appelé détournement de session TCP ou en anglais TCP session hijacking) est une technique consistant à intercepter une session TCP initiée entre deux machine afin de la détourner.

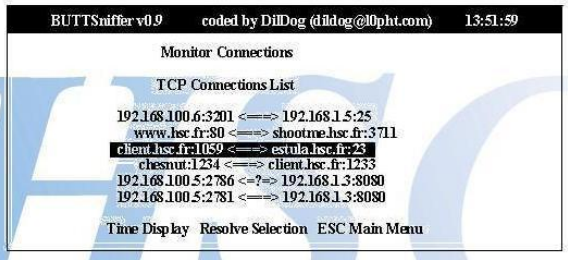


Un « analyseur réseau » (appelé également analyseur de trames ou en anglais sniffer, traduisez « renifleur ») est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.
Ethereal (WireShark)

Ecoute de réseau (sniffing)

- Exemple d'écoute réseau avec BUTTSniff
  - Attention : utilisable avec Back Orrifice

Sur chesnut : **BUTTSniff -i 0 1234**
Sur client : **telnet chesnut.hsc.fr 1234**



- SNMPsniff, WEBsniff, LINsniff, sniffit, ...

On appelle « spam » ou « pollupostage » (les termes pourriel, courrier indésirable ou junk mail sont parfois également utilisés) l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.
Les spammeurs collectent des adresses électroniques sur internet (dans les forums, sur les sites internet, dans les groupes de discussion, etc.)

Fiche TP 4 « Commandes TCP/IP »

Exercice 1 : « Adresse IP »

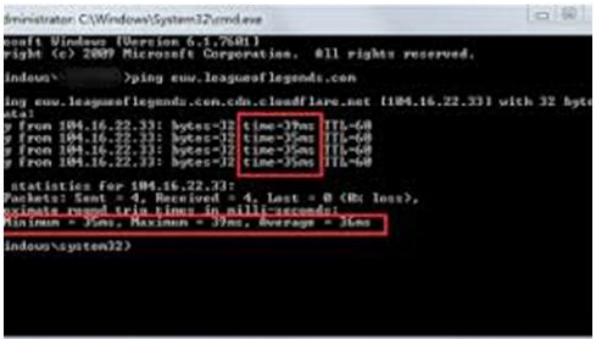
1. A partir de votre terminal, exécuter la commande « ipconfig ».
2. A partir de votre terminal, exécuter la commande « ipconfig /all ».
3. Donner l'adresse physique (MAC) et l'adresse logique (IP) de votre station.
4. Que représente l'adresse mac ?

Corrigé :

Exercice 2 : « Tester le réseau »

1. A partir de votre terminal, exécuter la commande « ping 127.0.0.1 ».
2. Que fait cette commande ?
3. A partir de votre terminal, exécuter la commande « ping nom_de_votre_machine ».
4. A partir de votre terminal, exécuter la commande « ping adresse_ip_de_votre_machine ».
5. A partir de votre terminal, pinguer toutes les stations de votre salle de TP.
6. Quelles sont les machines Inaccessibles ?

Corrigé :



Exercice 3 : « Routage »

1. A partir de votre terminal, exécuter la commande « route print ».
2. A partir de votre terminal, exécuter la commande « netstat –a ».
3. A partir de votre terminal, exécuter la commande « netstat –r ».

4. A partir de votre terminal, exécuter la commande « netstat –n ».
5. Quelle est la différence entre les deux commandes (netstat & route) ?
6. A partir de votre terminal, exécuter la commande « tracert nom_de_votre_station » (Ou @ IP).
7. A partir de votre terminal, exécuter la commande « tracert nom_de_la_station_voisine » (Ou @ IP).
8. A partir de votre terminal, exécuter la commande « tracert www.google.fr ».
9. Que pouvez-vous dire ?

Corrigé :

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.0.1        10.0.0.75     35
         10.0.0.0    255.255.255.0         On-link         10.0.0.75    291
        10.0.0.75  255.255.255.255         On-link         10.0.0.75    291
       10.0.0.255  255.255.255.255         On-link         10.0.0.75    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         10.0.0.75    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
```

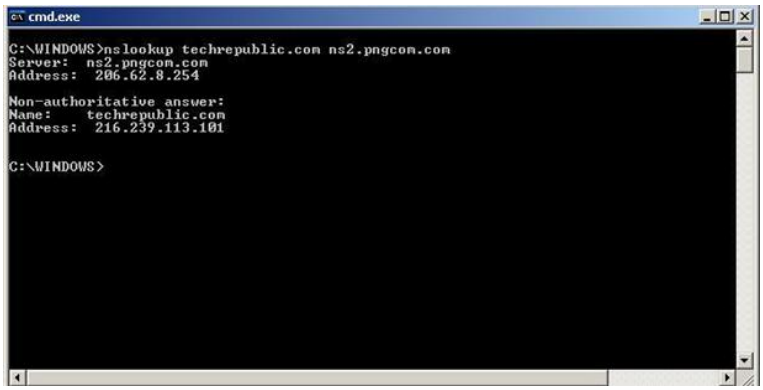
```
C:\Users\USER>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.12:50061     172.217.22.137:443     ESTABLISHED
  TCP    192.168.1.12:50083     216.239.38.120:443     TIME_WAIT
  TCP    192.168.1.12:50428     69.46.36.6:80          ESTABLISHED
  TCP    192.168.1.12:50439     69.46.36.10:4005       ESTABLISHED
  TCP    192.168.1.12:50467     216.58.201.238:443     TIME_WAIT
  TCP    192.168.1.12:50563     34.194.177.112:443     ESTABLISHED
  TCP    192.168.1.12:50671     216.58.204.98:443      TIME_WAIT
  TCP    192.168.1.12:50728     216.58.204.99:443      ESTABLISHED
  TCP    192.168.1.12:50809     216.58.213.174:443     ESTABLISHED
  TCP    192.168.1.12:50811     69.46.36.6:80          TIME_WAIT
  TCP    192.168.1.12:50812     216.58.205.3:443       ESTABLISHED
  TCP    192.168.1.12:50813     216.58.204.97:443      ESTABLISHED
  TCP    192.168.1.12:50814     216.58.207.227:443     ESTABLISHED
  TCP    192.168.1.12:50815     216.58.215.33:443      ESTABLISHED
  TCP    192.168.1.12:50819     69.46.36.6:80          TIME_WAIT
```

```
C:\Documents and Settings\Alain>tracert www.orange.fr

Détermination de l'itinéraire vers www.orange.fr.multis.x-echo.com [193.252.122
avec un maximun de 30 sauts :

  1     1 ms    <1 ms    <1 ms  192.168.0.1
  2     2 ms     1 ms     1 ms  HSIB.home [192.168.1.1]
  3    42 ms    43 ms    41 ms  86.199.179.1
  4    42 ms    42 ms    42 ms  10.125.237.82
  5    43 ms    42 ms    42 ms  193.253.150.182
  6    49 ms    49 ms    49 ms  193.252.99.158
  7    54 ms    49 ms    49 ms  193.252.99.197
  8    58 ms    57 ms    58 ms  81.253.129.222
  9    58 ms    58 ms    58 ms  81.253.129.90
 10    58 ms    57 ms    57 ms  193.252.161.129
 11    58 ms    57 ms    58 ms  193.252.227.154
 12    58 ms    58 ms    57 ms  193.252.121.149
 13    58 ms    58 ms    58 ms  193.252.122.103

Itinéraire déterminé.

C:\Documents and Settings\Alain>
```

Exercice 4 : « Serveur DNS »

1. A partir de votre terminal, exécuter la commande « nslookup ».
2. Donner l'adresse IP et le nom du serveur DNS.

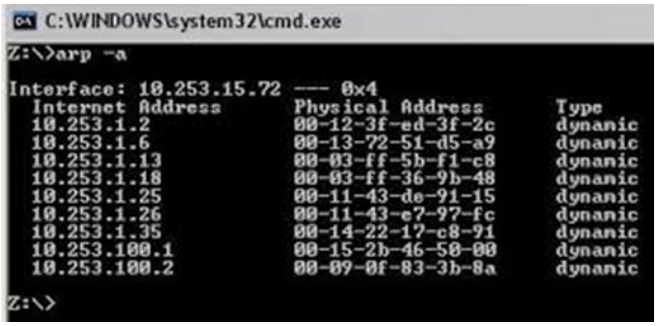
Corrigé :



Exercice 5 : « ARP »

1. A partir de votre terminal, exécuter la commande « arp –a ».
2. Que fait cette commande ?

Corrigé :

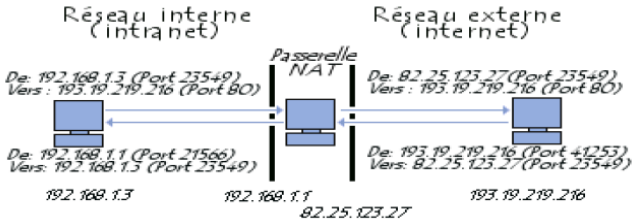


VII. Architectures et protocoles de sécurité

VII.1. Architecture

NAT

•Le mécanisme de translation d'adresses (en anglais Network Address Translation noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).
•En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées à internet.
•Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.
•Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP).
•Étant donné que la passerelle masque complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation.



Cette fonction est généralement implémentée sur un routeur ou éventuellement un firewall
Le seul avantage en termes de sécurité à utiliser un proxy par rapport à la NAT est que le proxy peut posséder des fonctionnalités de sécurité, et peut filtrer le trafic d'après le contenu, pour protéger votre machine
NAT cache l'ensemble des machines du réseau derrière la passerelle, qui apparaît comme étant le seul système connecté à Internet,

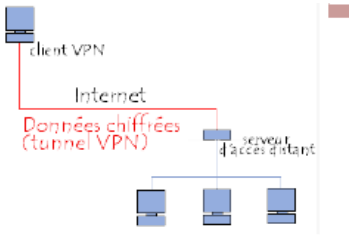
IPV6

•Doit résoudre le problème de pénurie d'adresse
•Il doit fournir une meilleure sécurité (authentification et confidentialité) que l'actuel protocole IP,
•La nouveauté majeure d'IPv6 est l'utilisation d'adresses plus longues qu'IPv4.
•Une nouvelle notation a été définie pour décrire les adresses IPv6 de 16 octets. Elle comprend 8 groupes de 4 chiffres hexadécimaux séparés avec le symbole deux-points. Par exemple :
▫8000:0000:0000:0000:0123:4567:89AB

•Après optimisation, on obtient:
▫8000::123:4567:89AB:CDEF

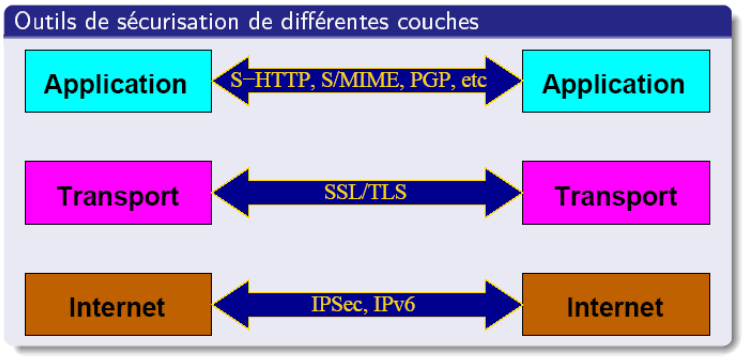
VPN (virtual private network)

•Réseau privé virtuel
•Ce réseau est dit virtuel car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et du VPN (des filiales, des clients ou même du personnel géographiquement éloignées via internet) peuvent "voir" les données.
•VPN permet donc d'obtenir une liaison sécurisée à moindre coût, car la ligne spécialisée est couteuse.



Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant de chiffrer les données par des algorithmes de cryptographie.
Les principaux protocoles de tunneling sont les suivants :
PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

VII.2. Protocoles



HTTPS

•C'est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP mise au point en 1994.

•Il permet de fournir une sécurisation des échanges lors de transactions en cryptant les messages afin de garantir aux clients la confidentialité des données, (de leur numéro de carte bancaire ou de toute autre information personnelle).
•Couche application

SSL

•SSL Secure Sockets Layers, est un procédé de sécurisation des transactions effectuées via Internet.
• Le standard SSL a été mis au point par Netscape.
•Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet.
•Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.
Un serveur web sécurisé par SSL possède une URL commençant par https://, où le "s" signifie bien évidemment secured (sécurisé).

TLS

•En 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'IETF (Internet Engineering Task Force) qui «produit la plupart des nouveaux standards d'Internet » et a été renommé pour l'occasion TLS (Transport Layer Security).

IPSEC

•IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.
•Le protocole IPSec est basé sur trois modules :
▫IP Authentification Header (AH) concernant l'intégrité, l'authentification et la protection contre le rejeu. des paquets à encapsuler.
▫Encapsulating Security Payload (ESP) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu.
▫Security Assocation (SA) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algo de sécurité utilisés par les protocoles, les clés utilisées,...). L'échange des clés se fait soit de manière manuelle soit avec le protocole d'échange IKE (la plupart du temps), qui permet aux deux parties de s'entendre sur les SA.

Fiche TP 5 « WireShark »

L'objectif de ce TP est d'analyser un réseau en utilisant l'outil « WireShark ».

Partie 1 : Téléchargement

- À l'adresse suivante : https://www.wireshark.org/download.html
- Télécharger le logiciel « Windows Installer (64-bit) » ou « Windows Installer (32-bit) » selon le système d'exploitation.
- Lire les informations sur la page.

Partie 2 : Installation

- Installer le logiciel « WireShark ».

Partie 3 : Prise en main

- Lancer le logiciel « WireShark » (à partir du menu Démarrer).

Partie 4 : Capture

- Ouvrir l'application WireShark
- Que fait cet outil ?
- Aller vers le menu capture -> Interfaces -> à coté de votre carte réseau -> cliquer sur « Start »
- Que remarquez-vous ?
- Aller vers le menu capture -> cliquer sur « Stop »
- Est ce que toutes les trames sont identiques ?

Partie 5 : Analyse de trame TCP

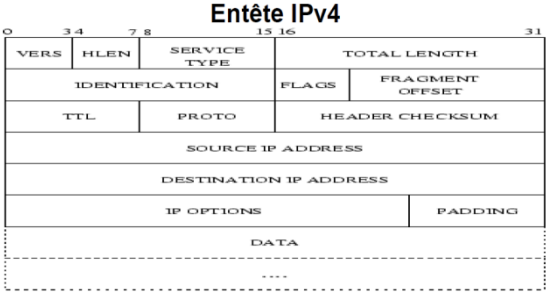
- Quelle est la taille de cette trame en octets puis en bits ?
- Quels sont les protocoles encapsulés dans cette trame ?
- Quelle est l'adresse MAC de la source et du destinataire ?
- Quelles sont les adresses IPv4 (en notation décimale pointée et en hexadécimale) de la source et du destinataire ?
- Quels sont les ports de la source et du destinataire ?
- Donner le corps du message en ASCII puis en texte.

Partie 6 : Interception de message

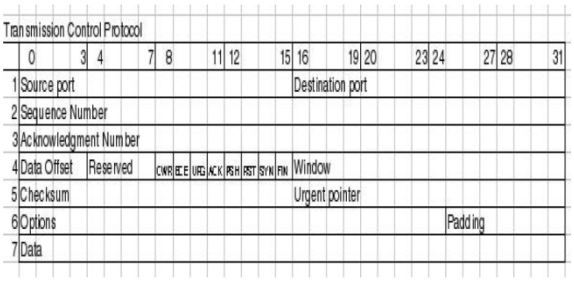
- Lancer une capture réseau
- Dialoguer avec la machine voisine
- Stopper la capture
- Trouver le message en clair échangé

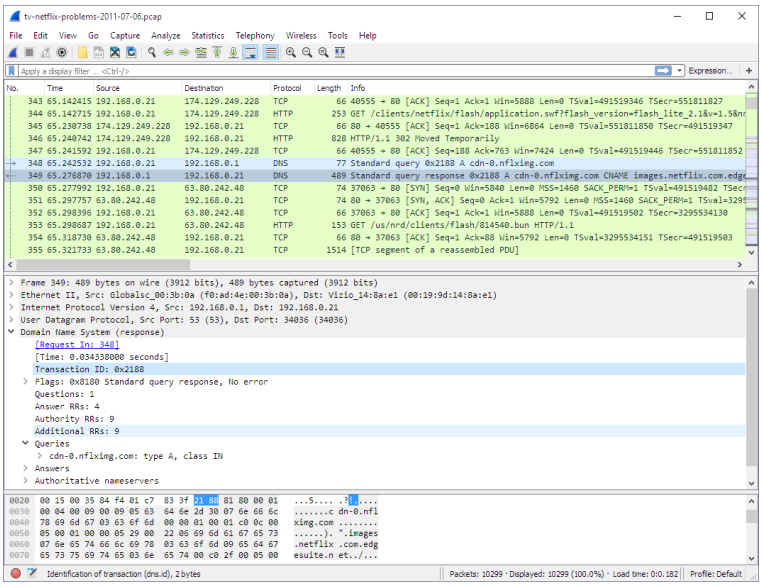
Corrigé :

Entête IPv4

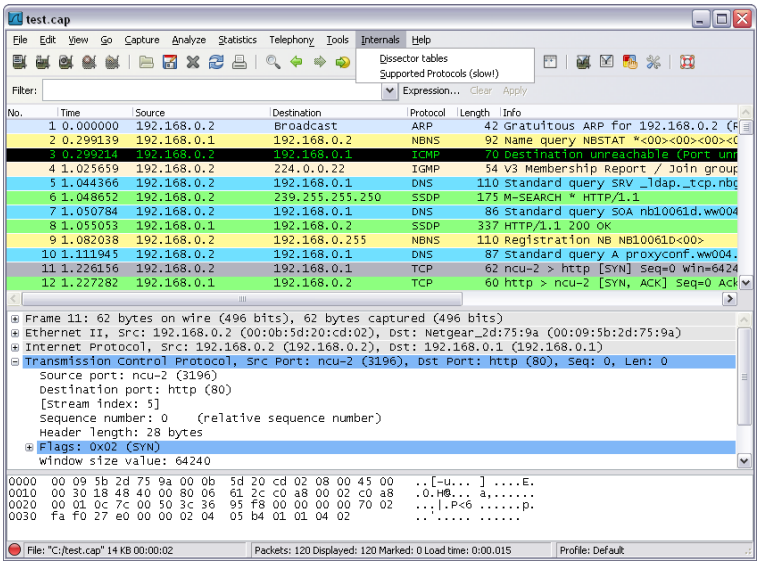


Entête TCP

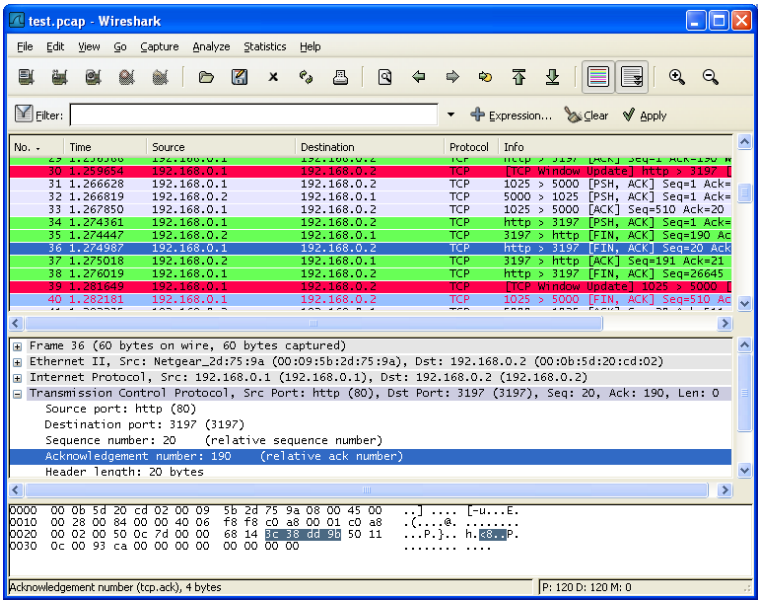




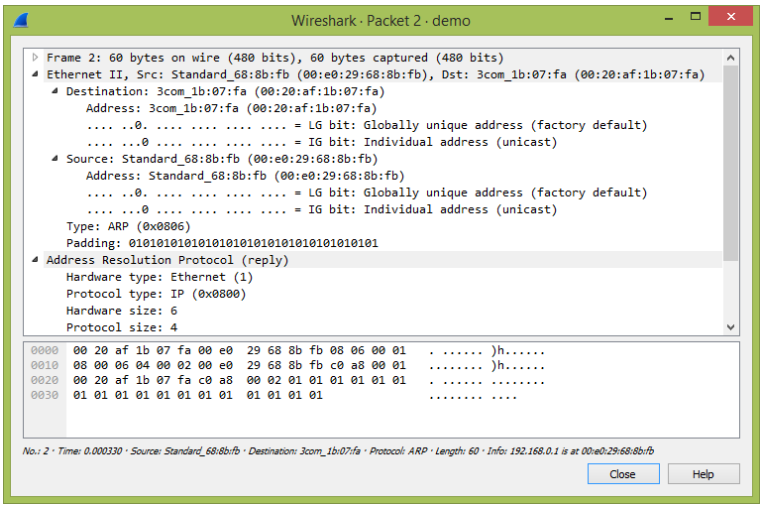
➔ **Trames différentes**



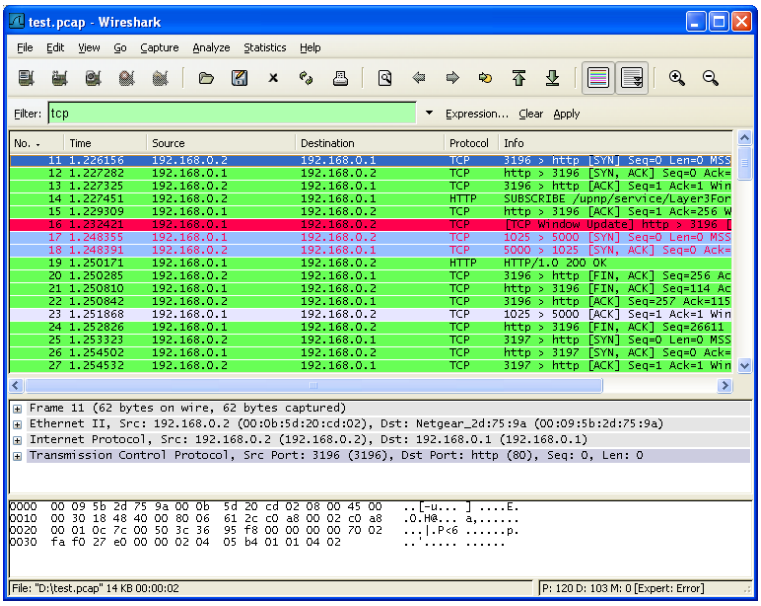
➔ **3 parties représentatives**



➔ **Recherche**



➔ **Détails de paquet**



➔ **Filtrage paquet**

VIII. Authentification

VIII .1. Définition

•Il existe une différence toute simple entre identification et authentification : c'est la preuve.
•Une identification s'appuie sur une simple déclaration comme la réception ou la lecture d'un code d'identification (identifiant, n° de série, code barre,…). Ce code d'identification n'est pas supposé secret. C'est une donnée publique.
•L'authentification s'appuie sur un élément de preuve comme un secret partagé ou un secret asymétrique. L'authentification permet de s'assurer avec un niveau de confiance raisonnable de l'identité de l'utilisateur.

VIII .2. Facteurs d'authentification

•Ce qu'il sait (mot de passe, numéro d'identification personnel).
•Ce qu'il possède (acte de naissance, carte grise, carte d'identité, carte à puce, droit de propriété, certificat électronique, diplôme, passeport, carte Vitale, Token OTP, Carte OTP, Téléphone portable, PDA, etc.).
•Ce qu'il est (photo, caractéristique physique, voire biométrie).
•Ce qu'il sait faire (geste, signature).

VIII .3. Méthodes d'authentification

*Exemples de système d'authentification à **1** facteur :*	▪ Identifiant + mot de passe (élément **que l'on sait),** ▪ Identification sans contact (élément **que l'on possède),** ▪ Biométrie ou identifiant + biométrie (élément **que l'on est).**
*Exemples de système d'authentification à **2** facteurs :*	▪ Carte à puce + code PIN (éléments **que l'on possède ET que l'on sait),** ▪ Carte à puce + biométrie (élément **que l'on possède ET que l'on est),** ▪ Biométrie + mot de passe (élément **que l'on est ET que l'on sait)).**
*Exemple de système d'authentification à **3** facteurs :*	▪ Carte à puce + code PIN + biométrie (éléments **que l'on possède ET que l'on sait ET que l'on est).**

Inconvénients du multi facteurs

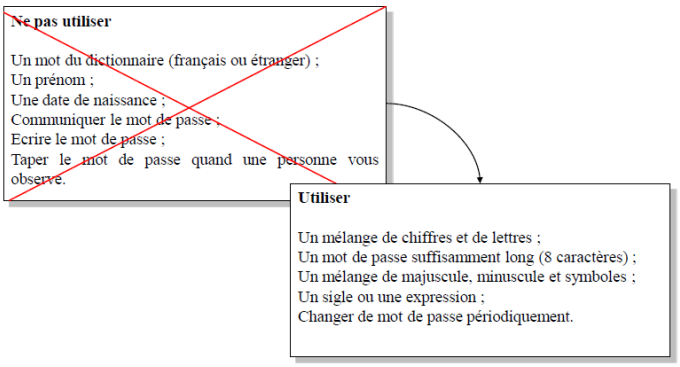
•La multiplication du nombre de facteurs d'authentification augmente le niveau de sécurité général, mais pose les problèmes suivants :
•Le cycle de vie de chaque facteur doit être géré : réinitialisation des mots de passe et codes PIN, distribution des cartes à puce, …,
•L'ergonomie d'utilisation peut devenir trop contraignante pour les utilisateurs,
•Les coûts des périphériques (cartes à puce, lecteurs, capteurs biométriques) sont additionnés.

Ce qu'il sait

Mot de passe (password)

•Le mot de passe est une clé qui protège le compte, système d'exploitation, carte bancaire, boite électronique …
•D'où l'importance de bien le choisir :
▫facile à retenir,
▫assez complexe pour ne pas être intercepté.

Recommandations



"J'ai acheté 1 CD pour cent euros cet après-midi" : ght1CD%E7am

Attaque sur mot de passe

•Attaque par dictionnaire
•Attaque par force brute
▫26N si le mot de passe ne contient que des lettres de l'alphabet totalement en minuscules ou en majuscules ;
▫52N si le mot de passe ne contient que des lettres de l'alphabet, avec un mélange de minuscules et de majuscules ;
▫62N si le mot de passe mélange les majuscules et les minuscules ainsi que les chiffres.
•Attaque indirectes
▫Keyllogers
▫Ingénierie sociale
▫Espionnage

Ce qu'il possède

PKI Public Key Infrastructure

•Chaque utilisateur dispose d'une clef publique, laquelle est librement diffusée à d'éventuels interlocuteurs à partir d'un annuaire par exemple, ainsi qu'une clef privée, qui elle, est secrète, Cette clef privée permettra de déchiffrer un message.
•Le problème qui se pose alors, est qu'un intrus pourrait intercepter un message et remplacer la clef publique de l'émetteur par la sienne.
•Cette faille oblige à valider l'identité des différents propriétaires de clefs publiques, ce par l'intermédiaire d'un certificat numérique.

Certificat numérique

•Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité.

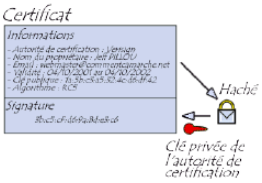
•Le tiers de confiance est une entité appelée communément autorité de certification (ou en anglais Certification authority, abrégé CA)

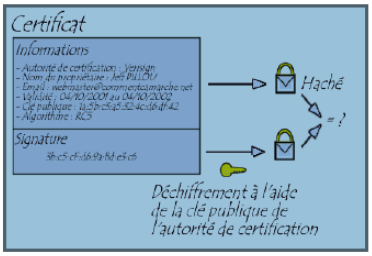
•Il est possible de faire l'analogie d'un certificat à une carte d'identité délivrée par une autorité reconnue comme sure, comme une préfecture de police ou un ministère de l'intérieur.

Certificat

•La version de X.509 à laquelle le certificat correspond ;
•Le numéro de série du certificat ;
•L'algorithme de chiffrement utilisé pour signer le certificat ;
•Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice ;
•La date de début de validité du certificat ;
•La date de fin de validité du certificat ;
•L'objet de l'utilisation de la clé publique ;
•La clé publique du propriétaire du certificat ;
•La signature de l'émetteur du certificat (thumbprint).

Exemple





Outils- options internet – contenu –certificat

Carte à puce

•La carte à puce contient un processeur et une mémoire intégrée.
•Le processeur permet d'effectuer les calculs de chiffrement, déchiffrement et hachage.
•La mémoire permet de stocker les clés privées de manières sures.
•Les avantages d'une infrastructure PKI à carte à puce sont les suivants :
▫Elles évitent de taper un mot de passe devant les regards indiscrets
▫Une souplesse d'utilisation, elles peuvent être utilisés partout, sur plusieurs machines,
▫C'est un gain de temps appréciable car pour ouvrir une session, par la peine de faire Ctrl + Alt + Suppr , puis entrer le nom d'utilisateur, d'une le mot de passe.... Il suffit tout simplement d'introduire la carte à puce dans le lecteur et la session s'ouvre instantanément, de même pour bloquer la session, il suffit de retirer la carte.
▫Elles sont aujourd'hui particulièrement répandues dans des applications comme les cartes bancaires françaises, les cartes Vitale, mais aussi les cartes SIM sur portable

Ce qu'il est

Biométrie

•On peut constater que la biométrie est une véritable alternative aux mots de passe et autres identifiants pour sécuriser les contrôles d'accès.

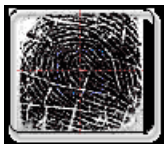
•Elle permet de vérifier que l'usager est bien la personne qu'il prétend être.

•La biométrie est en pleine croissance et tend à s'associer à d'autres technologies de sécurité comme la carte à puce.

Empreinte digitale

•Cette technologie de reconnaissance s'appuie sur les structures périodiques des empreintes digitales. Ces structures sont appelées 'minuties'.

•Les minuties sont les points permettent d'identifier l'empreinte de façon unique.



•Avantages :

- Coût faible.
- Système biométrique facile à mettre en place.
- Le niveau de sécurité est élevé.

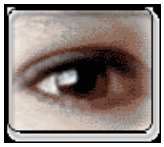
•Inconvénients :

- Est ressentie comme étant intrusif.
- Système assez vulnérables aux attaques (créer un 'faux doigt' en utilisant l'empreinte digitale d'une autre personne dont le modèle biométrique est stocké dans la base de donnée associé au lecteur d'empreintes digitale).
- Brulures …

Iris

•La méthode d'authentification biométrique par l'iris est sans doute l'une plus efficaces.

•Il y a quasiment aucune chance pour que deux personnes possèdent les mêmes caractéristiques au niveau de l'iris.



•Avantages :

- Actuellement la meilleure technique de reconnaissance biométrique (avec la reconnaissance rétinienne).

•Désavantages :

- Perçues comme intrusives par les usagers.
- L'effort demandé aux utilisateurs est grand (le lecteur d'iris utilise un faisceau lumineux de basse intensité qui éclaire l'iris).
- Malade …

Forme du visage

•elle caractérise les visages par des distances et des proportions entre des points particuliers et les éléments les moins susceptibles aux changements du visage:

▫les grands traits supérieurs des orbites,

▫les secteurs entourant les pommettes,

▫les côtés de la bouche, les yeux, le nez.

•Avantages :

Technologie biométrique peu couteuse.

S'associe très bien avec un système de télésurveillance vidéo

•Désavantages :

2 jumeaux, elle ne pourrait pas les distinguer.

Si la personne porte un déguisement, un masque,

Signe de vieillesse

Vocale

•Une fois capturée par un micro, la voix est convertie en algorithmes mathématiques.

•La reconnaissance vocale n'est pas considérée comme une des meilleures techniques de reconnaissance biométrique.

•Elle est plutôt associée à d'autres technologies de contrôle d'accès tel que la carte à puce.

•Avantages :

Technologie biométrique facile à mettre en oeuvre.

Permet de sécuriser une conversation téléphonique

• Désavantages :

Technologie biométrique vulnérable aux attaques.

Enregistrer la voix

Grippe …

Ce qu'il sait faire

Signature

•Signer un document pour s'identifier est un geste naturel. Que ce soit pour confirmer une transaction sur son compte de carte de crédit ou simplement.

•Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification.

•On distingue deux façons de capturer une signature, soit avec des capteurs qui s'assimilent à de simples scanners, soit par l'usage d'une tablette graphique et d'un stylet sensible à la pression.

•Avantages

▫Simple

▫Utiliser des plusieurs pays pour s'authentifier

•Inconvénients

▫Les difficultés liées à la capture d'une signature viennent du fait qu'une personne ne signe jamais deux fois de la même façon ,

▫En effet suivant les émotions ou la fatigue, une signature peut fortement évoluer.

Clavier

•Il s'agit d'une technique de reconnaissance des personnes basée sur le rythme de frappe qui leur est propre.

•Elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à « imiter »

•Lors de la mise en place de cette technique, il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite.

•A l'aide d'un algorithme qui exploite le temps d'appui sur chaque touche et le temps entre chaque touche,

•Les avantages

▫Pas de hardware supplémentaire, un simple logiciel suffit

▫Aucune carte ou Token à perdre par l'utilisateur

▫Réduit sensiblement la nécessité de changement de mot de passe

•Les inconvénients

▫Pour ceux qui sont susceptibles de voyager et donc d'utiliser des claviers d'un format différents AZERTY, QUERTY …, il faut un profil par format

▫Il ne faut pas être dérangé lors de la frappe ! cela peut provoquer un refus de son propre mot de passe !

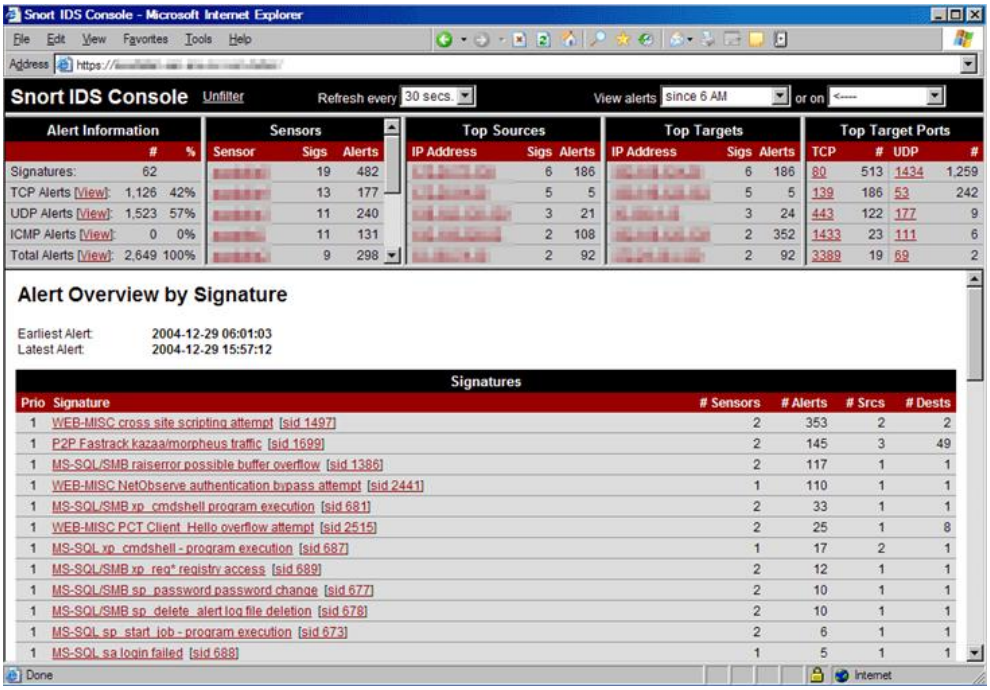
▫Malade

« Liste des Logiciels à Tester en project »

NMAP : Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

```
root@siteduzero:~# nmap 192.168.1.65

Starting Nmap 4.20 ( http://insecure.org ) at 2007-
01-26 00:18 CET
Interesting ports on 192.168.1.65:
Not shown: 1692 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
1234/tcp open  hotline
6112/tcp open  dtspc

Nmap finished: 1 IP address (1 host up) scanned in
5.622 seconds
root@siteduzero:~#
```

SNORT : Snort est un système de détection d'intrusion (ou NIDS) libre publié sous licence GNU GPL. À l'origine écrit par Marty Roesch (en), il appartient actuellement à Sourcefire. Des versions commerciales intégrant du matériel et des services de supports sont vendus par Sourcefire. Snort est un des plus actifs NIDS Open Source et possède une communauté importante contribuant à son succès.



AIRCRACK : Aircrack-ng est une suite de logiciels de surveillance des réseaux sans fil dont l'utilisation principale est de « casser » les clés WEP et WPA des réseaux WIFI. C'est en fait une « reprise » du logiciel aircrack (premier du nom) qui a été abandonné.

```
CH  0 ][ BAT 100% ][ GPS    0.000    0.000    0.000   0.00 ][ 2006-05-08 13:04

BSSID              PWR  Beacons   # Data  CH  MB  ENC   ESSID

00:0F:CC:39:8A:BC   65      780       39   7  54. WEP   Jungnetz

BSSID              STATION            PWR  Packets  Probes

(not associated)   00:12:79:40:90:65   73       23
(not associated)   00:15:00:45:0E:FF   80      148  ANIT,geziistanbul,AIRTIES
```

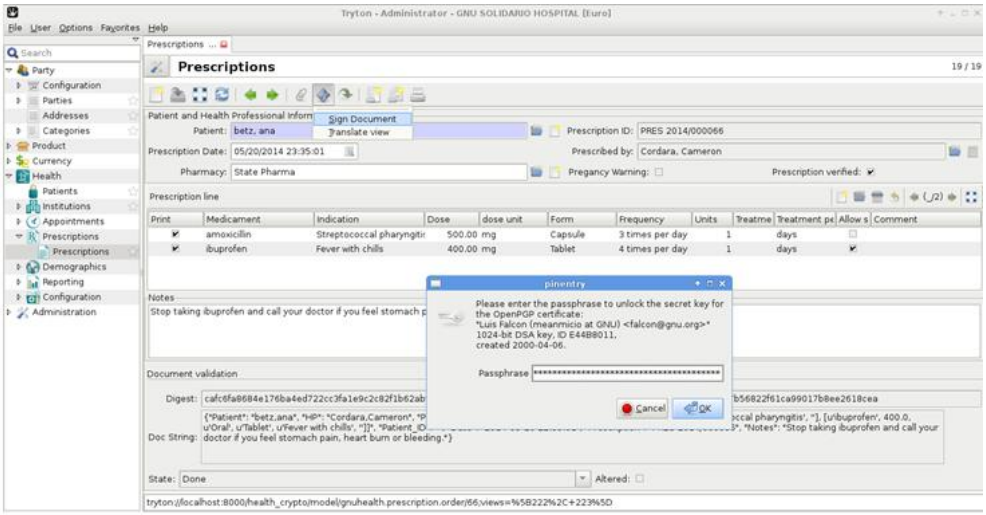
OPEN SSH : OpenSSH (OpenBSD Secure Shell) est un ensemble d'outils informatiques libres permettant des communications sécurisées sur un réseau informatique en utilisant le protocole SSH.

```
root@boris:~
File  Edit  View  Terminal  Tabs  Help
[karam@vladimir ~]$ ssh root@192.168.1.113
root@192.168.1.113's password:
Last login: Thu Jun 28 06:06:51 2007 from 192.168.1.114
[root@boris ~]# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda3              7676832    712336   6964496  10% /
none                    128028         0    128028   0% /dev/shm
/dev/sda1                38888      9150     27730  25% /boot
/dev/sda4              5251040    877336   4373704  17% /home
[root@boris ~]# free
             total       used       free     shared    buffers     cached
Mem:        256056     185880      70176          0        160     121160
-/+ buffers/cache:      64560     191496
Swap:       265064          0     265064
[root@boris ~]# cal
     June 2007
Su Mo Tu We Th Fr Sa
                1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30

[root@boris ~]# ping e-lyrics.org
PING e-lyrics.org (64.202.189.170) 56(84) bytes of data.
64 bytes from pwfwd-v01.prod.mesa1.secureserver.net (64.202.189.170): icmp_seq=1 ttl=111 time=77.4 ms
64 bytes from pwfwd-v01.prod.mesa1.secureserver.net (64.202.189.170): icmp_seq=2 ttl=111 time=73.0 ms
64 bytes from pwfwd-v01.prod.mesa1.secureserver.net (64.202.189.170): icmp_seq=3 ttl=111 time=70.3 ms
64 bytes from pwfwd-v01.prod.mesa1.secureserver.net (64.202.189.170): icmp_seq=4 ttl=111 time=71.8 ms

--- e-lyrics.org ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 70.338/73.164/77.473/2.674 ms
[root@boris ~]#
```

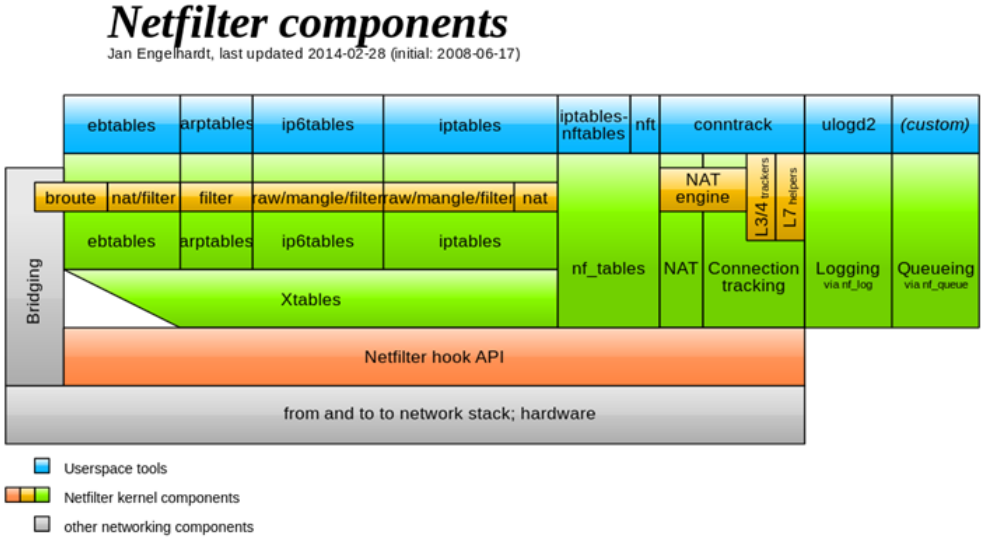
TRUE CRYPT : TrueCrypt est à la fois un format de système de fichier chiffré, notamment géré par Linux dans son module dm-crypt depuis la version 3.131,2, et un logiciel de chiffrement à la volée fonctionnant sur Microsoft Windows XP/2000/2003/Vista (32-bit et 64-bit)/7, Mac OS X et GNU/Linux, ce dernier étant à l'origine de ce système de fichier.
TrueCrypt permet de créer un disque virtuel chiffré (volume TrueCrypt) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, par exemple une disquette ou une clé USB. Le chiffrement est automatique, en temps réel et transparent.

Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré, y compris noms de fichiers et répertoires. Les volumes TrueCrypt se comportent, une fois montés, comme des disques durs physiques. Il est ainsi possible, par exemple, d'en réparer le système de fichiers avec Check Disk, ou de défragmenter les volumes créés par TrueCrypt.

GNU PG/PGP: GnuPG (ou GPG, de l'anglais GNU Privacy Guard) est l'implémentation GNU du standard OpenPGP défini dans la RFC 48803, distribuée selon les termes de la licence publique générale GNU. Ce logiciel permet la transmission de messages électroniques signés et chiffrés, garantissant ainsi leurs authenticités, intégrité et confidentialité.



NETFILTER: Netfilter est un cadriciel (framework) implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau. La version 1.4.2 a reçu un Certificat de Sécurité de Premier Niveau (CSPN) par l'Agence nationale de la sécurité des systèmes d'information1.



Bibliographie

D. Kim & M. G. Solomon : "Fundamentals of Information Systems Security". Jones & Bartlett Learning, 2014.

M. Stewart, M. Chapple & D. Gibson : « CISSP : Certified Information Systems Security Professional », Study Guide. John Wiley& sons, 2012.

Cryptographie appliquée, Schneier Bruce, International THOMSON Publishing France, 1997.
Cours de cryptographie, Gilles Zémor, Cassini, 2000.

Cryptography, Theory and Practice, 3ème édition, Douglas Stinson, Chapman and Hall, 2002.
Introduction to cryptography with coding theory, 2ème édition, Wade Trappe and Lawrence C. Washington, 2ème édition, 2006.

An Introduction to Coding Theory, 3ème édition, van Lint, Springer, 1998.

The theory of error-correcting codes, 11ème édition, MacWilliams and Sloane, North-Holland, 2003.

Information and Coding Theory, G. A. Jones and J. M. Jones, Springer, 2000.

Applied Cryptography, Second Edition, Bruce Schneier, Wiley Interscience, 1996

Les codes secrets décryptés, par Didier Müller, City Editions, 368 pages, ISBN 2-35288-041-6, février 2007

Computer Security Handbook, Seymour Bosworth, Michel E. Kabay (editors), John Wiley, 2002

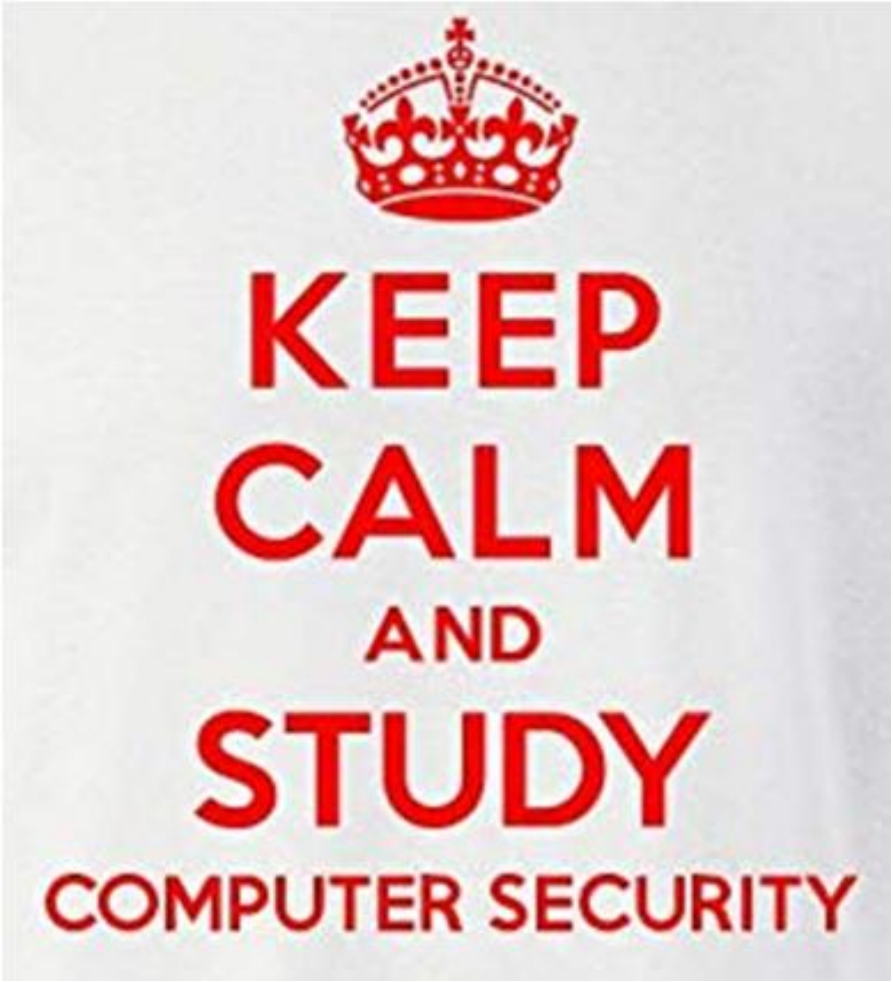
Les protocoles de sécurité de l'internet, S. Natkin, Dunod, 2002

EFS, IPSEC, SSL : Mise en oeuvre de la sécurité sous Windows Server 2003, de Benoît Lanlard, édition ENI, février 2006

Guide pratique de sécurité informatique : Mise en œuvre sous Windows et Linux, de Bruno Favre et Pierre-Alain Goupille, édition DUNOD, octobre 2005

La sécurité informatique dans la petite entreprise - Etat de l'art et Bonnes Pratiques, de Jean-François Carpentier, édition ENI, avril 2009

Sécurité des réseaux. Applications et standards (Broché), de William Stallings (Auteur), Editeur : Vuibert, mars 2002


KEEP
CALM
AND
STUDY
COMPUTER SECURITY