Université Grenoble Alpes

IUT1 de Grenoble

Département RESEAUX et TELECOMMUNICATIONS

Bachelor Universitaire de Technologie

Cyber

Réseaux et Telecom

R5.cy.12-Norme Normes, standards et analyse de risque

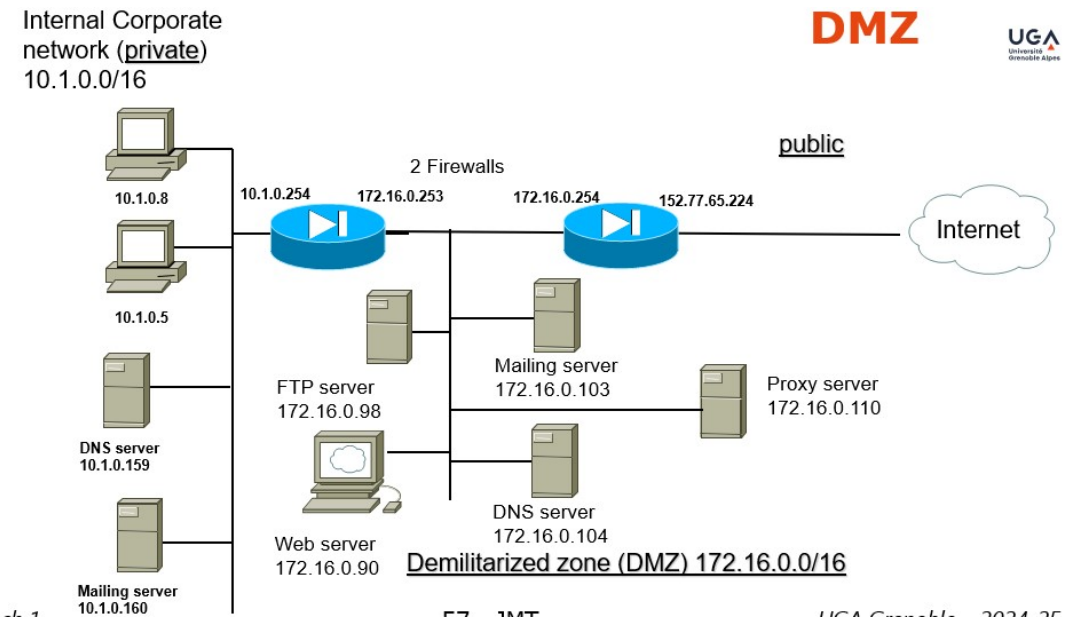
Prise de notes partielle

--

Enoncés de TD

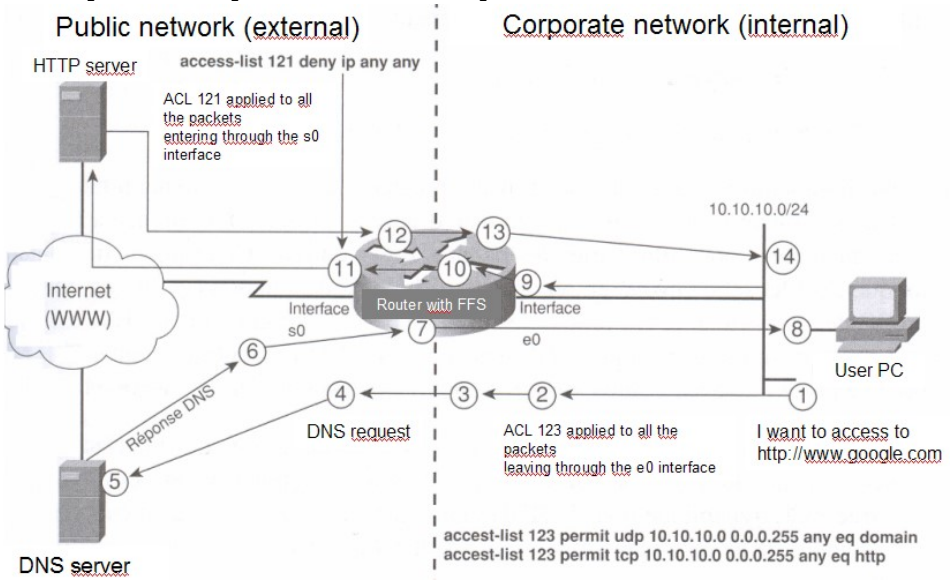
Jean-Marc THIRIET

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
```



TD 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 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 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.

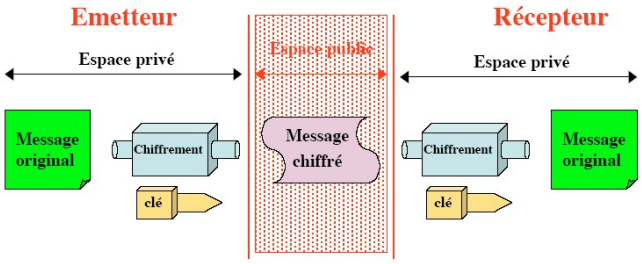
Ex 3 : Filtrage applicatif

Qu'apporte le filtrage effectué au niveau applicatif ?

Ex 4 : Masquage des adresses IP

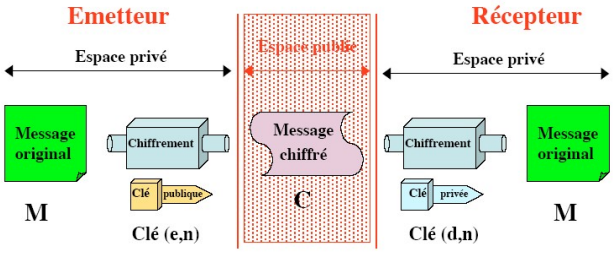
Quel est l'intérêt principal de masquer les adresses IP internes à une organisation ? Quel type de système permet de le faire ?

C. Prot. CRYPTOGRAPHIE



✓**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

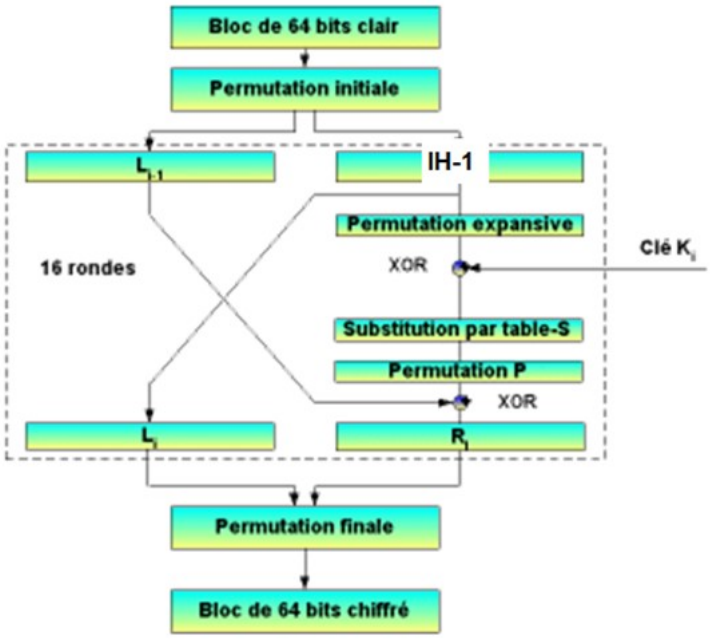
- Nécessite des clés de très grande taille pour être peu vulnérable…

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

TD : C. Prot. : cryptage

Ex 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 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 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 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 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 6 : Limitations des certificats numériques

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

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

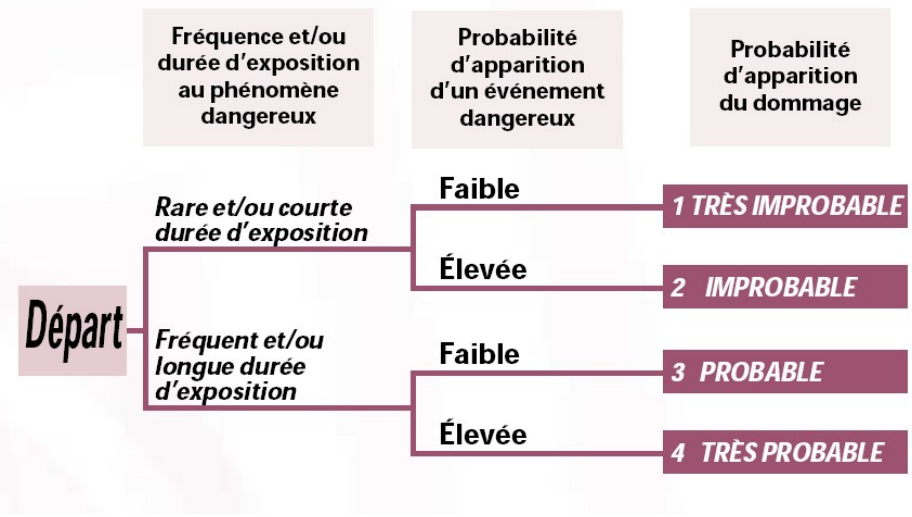
- Mécanismes de sécurité par logiciel
  - Identification
  - Authentification
  - Autorisation
- Dispositifs mis en place pour garantir la confidentialité et l'intégrité
  - Cryptographie
  - Gestion efficace des mots de passe
  - Antivirus
  - Sauvegarde des informations sensibles
- Classification des 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 Approche pour l'analyse de risques :

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

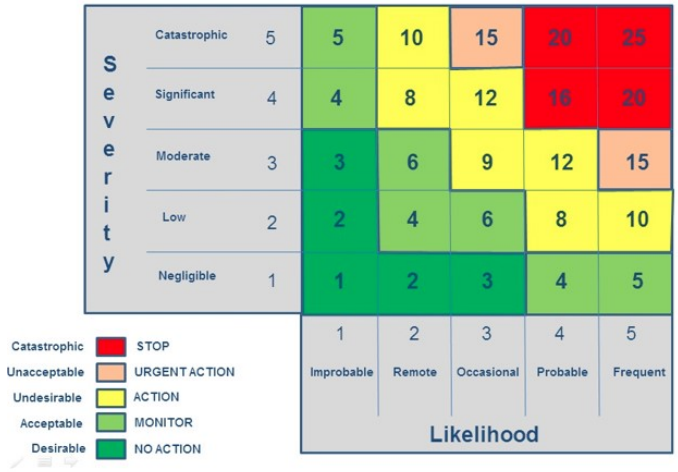


Depending on the type of company or the application, sometimes we take into account only the frequency and/or the duration of the danger:

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**

Risk Rating = Likelihood x Severity



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)	

TD Cyber-Attaques

Ex 1: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.

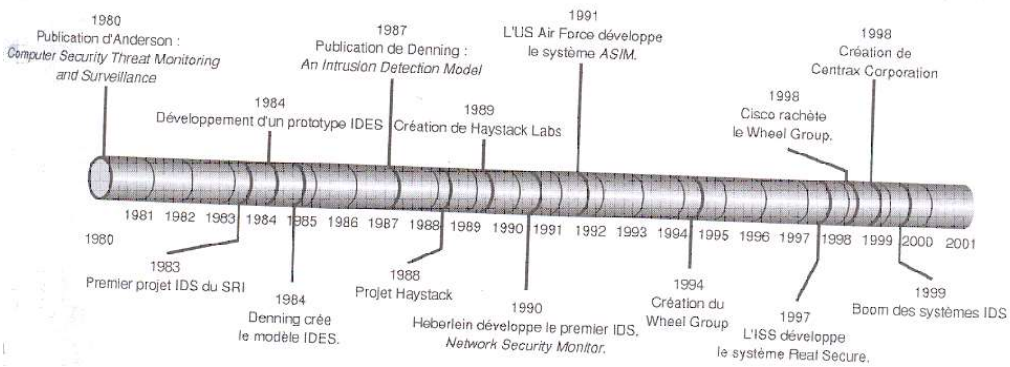
1. Comment le pirate peut-il réaliser une attaque par déni de service contre le serveur pauvre.victime.com ?
2. Si le pirate possède une bande passante de 256 kbps et qu'il est capable de l'utiliser à 100 % pour son attaque, quelle sera la bande passante appartenant à pauvre.victime.com qui sera utilisée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

C.menaces, réponses : 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

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)

TD Stratégie et Politique de sécurité

Ex 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 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 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 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 ?

Evaluation de la sécurité du « cloud »
Un cadre de sécurité pour le Cloud

D'après « Securing the Cloud, cloud computer security technologies and tactics », Vic J.R. Winkler, Elsevier.

Checklists for Evaluating Cloud Security

Checklist 9.1 Policy, Standards, and Guidelines[8–10]

Policy, Standards, and Guidelines

- Has a security policy been clearly documented, approved, and represented to all concerned parties as representing management's intent?
- Has the security policy had legal, privacy, and other governance review?
- Has the security policy been augmented by security standards and/or guidelines?
- Has the policy been augmented by a privacy policy?
- Are the security and privacy policies, as well as standards and guidelines, consistent with industry standards (such as 27001, CoBIT, and so on)?
- Are third party providers held to the same policies and standards?

Checklist 9.2 Transparency[11–13]

Transparency

- Does the CSP provide customers with a copy of the governing policies, standards, and guidelines?
- Are customers notified of changes to governing policies, standards, and guidelines?
- Does the CSP provide customers visibility into third party compliance audits?
- Does the CSP provide customers visibility into penetration tests?
- Does the CSP provide customers visibility into internal and external audits?
- Does the CSP provide customers visibility into CSP asset management and repurposing of equipment?

Checklist 9.3 Personnel Security[14–16]

Personnel Security

- Are there policies and procedures for:
- Hiring employees who will have access to or control over cloud components?
- Pre-employment checks for personnel with privileged access?

- Are personnel security policies consistent across locations?
- Do they apply to online cloud systems and data as well as to offline systems that either stored data or to offline systems that will be provisioned for online use?
- Is there a security education program, and if so, how extensive is it?
- Is personnel security frequently reviewed to determine if employees with access should continue to have access?
- Are personnel required to have and maintain security certifications?
- Does physical access to the CSP's facility require background checks?

Checklist 9.4 Third Party Providers[17–19]

Third Party Providers

- Are any services or functions provided by a third party?
- If any part of a cloud is subcontracted or otherwise outsourced, does the providing party comply with the same policy and standards that the CSP enforces?
- If used, are third party providers audited for compliance with the CSPs policies and standards?
- Does the CSP security policy (or equivalent) and governance extend to all third party providers?

Checklist 9.5 Legal[20–22]

Legal

- Where—in which jurisdiction—will data be stored?
- Where—in which jurisdiction—is the CSP incorporated?
- Does the CSP use third party providers who are not located in the same jurisdiction?
- Does the CSP subcontract any services or personnel?
- Does the CSP use a customer's data in any manner that is not part of the service?
- Does the CSP have a documented procedure for responding to legal requests (such as a subpoena) for customer data?
- In the event of a subpoena, how does the CSP produce data for a single customer only without providing non-subpoena data?
- Is the CSP insured against losses, including remuneration for customer losses due to CSP outages or data exposure?

Checklist 9.6 Business Continuity[23–25]

Business Continuity

- Does the CSP have a formal process or contingency plan that documents and guides business continuity?
- What are the service recovery point objective (RPO) and recovery time objective (RTO)?
- Is information security integral to recovery and restoration?
- How does the CSP communicate a disruption of services to customers?
- Is there a secondary site for disaster recovery?

provisioning.

Checklist 9.7 Resource Provisioning[27–29]

Resource Provisioning

- What controls and procedures are in place to manage resource exhaustion, including processing oversubscription, memory or storage exhaustion, and network congestion?
- Does the CSP limit subscriptions to the service in order to protect SLAs?
- Does the CSP provide customers with utilization and capacity planning information?

software assurance.

Checklist 9.8 Software Assurance[30–32]

Software Assurance

- What controls are in place to maintain integrity of operating systems, applications, firmware updates, configuration files, and other software?
- What industry standards, guidelines, or best practices are followed?
- What controls or guidelines are used to obtain or download software and configuration files?
- What guidelines or procedures are used to maintain software integrity?
- Is penetration or vulnerability testing used on each release?
- How are identified vulnerabilities remediated?

One very

Checklist 9.9 Network Security[33–35]

Network Security

- What controls are in place to manage externally sourced and internally sourced attacks, including distributed denial of service (DDoS)?
- For customers, how is isolation managed between VMs by the hypervisor?
- For customers, how is isolation managed between VMs by network hardware and routing?
- What standards or best practices are used to implement virtual network infrastructure?
- How are MAC spoofing, ARP poisoning, and so on protected against?
- How is isolation managed between customer accessed/routable systems and cloud management systems and infrastructure?
- Is cloud customer processing dependent on off-cloud tenant components such as LDAP?
- Does the CSP perform periodic penetration testing against the cloud?
- If so, is penetration testing done both from external to the cloud and from inside the cloud and the cloud infrastructure?
- Does the CSP perform vulnerability testing of the cloud infrastructure, cloud management, and also customer accessible components?
- How are identified vulnerabilities tracked and addressed?
- Is vulnerability information made available to customers?
- Does the CSP allow customers to perform vulnerability testing against the customer's own VMs or other containers?

Checklist 9.10 Host and VM Security[36–38]

Host and VM Security

- Are customer VMs encrypted and/or otherwise protected when stored?
- Are VM images patched before they are provisioned?
- How and how frequently are VM images patched after being provisioned?
- To which standards or guidelines are VM images hardened before being provisioned?
- What are the procedures for protecting hardened and patched VM images?
- Can a customer provide his/her own VM image?
- Does the CSP include any authentication credentials, and if so, what are they used for?
- Do hardened and patched VM images include operating firewall instances by default? (And if so, what are the allowed services/ports?)
- Do hardened and patched VM images include operating IDS or intrusion prevention systems (IPS)?
- If so, does the CSP have access to these in operation (and if so, how)?
- Do hardened and patched VM images include any form of network, performance, or security instrumentation that the CSP or tenant has access to?
- How is isolation ensured between server colocated VMs for different customers?
- How is communication implemented between VMs for the same customer?
- How is security ensured for user data in storage systems?
- How is security ensured for user data in motion between storage systems and customer VMs?
- How is security ensured for user data and user interaction between a VM and a non-cloud user system?
- Does the CSP provide information to customers to guide customer security so that it is appropriate for the virtualized environment?

Checklist 9.11 PaaS and SaaS Security[39–41]

PaaS and SaaS Security

- How does the CSP isolate multitenant applications?
- How does the CSP isolate a user's or tenant's data?
- How does the CSP identify new security vulnerabilities in applications and within the cloud infrastructure?
- Does the CSP provide security as a service features for PaaS (such as authentication, single sign on, authorization, and transport security)?

- What administrative controls does the CSP provide to a tenant/user and do these support defining/enforcing access controls by other users?
- Does the CSP provide separate test and production environments for customers?

Checklist 9.12 Identity and Access Management[42–44]

Identity and Access Management

- Do any CSP controlled accounts have cloud-wide privileges (if so, which operations)?
- How does the CSP manage accounts with administrator or higher privilege?
- Does the CSP use 2-man access controls, and if so, for which operations?
- Does the CSP enforce privilege separation (for instance, RBAC), and if so, what roles are used to limit which privileges (security, OS admin, identity, and so on)?
- Does the CSP implement break-glass access, and if so, under what circumstances are they allowed and what is the process for post-clean up?
- Does the CSP grant tenants or users administrator privileges, and if so, what are the limits to this?
- Does the CSP verify user identity at registration, and if so, are there different levels of checks depending on resources to which access is granted?
- How are credentials and accounts deprovisioned?
- Is deprovisioning of credentials and accounts done in a cloud-wide atomic-operation manner?
- How is remote access managed and implemented?

For CSP supplied customer-use identity and access management systems:

- Does this support federated identity management?
- Is the CSP's system interoperable with third party identity provider systems?
- Can a customer incorporate single sign on?
- Does this system support separation of roles and LPP?

How does a CSP verify their identity to a customer under the following scenarios:

- When the CSP communicates out-of-band to a customer or user?
- When a customer interacts with the CSP via an API?
- When a customer uses a cloud management interface?

Authentication

- How is authentication implemented for high-assurance CSP operations?
- Is multifactor authentication used?
- Is access to high-assurance operations limited to only operations cloud-networks and only from whitelisted IP addresses?
- Does intrusion detection/anomaly detection detect multiple failed logins or similarly suspicious authentication or credential compromise activities?
- What procedures are invoked if a customer's credentials or account is compromised?

Checklist 9.13 Key Management and Cryptography[45–47]

Key Management

- For keys that the CSP controls:
- How does the CSP protect keys, and what security controls are in place to effect that?
- Are hardware security modules used to protect such keys?
- Who has access to such keys?
- How are those keys protected for sign and encrypt operations?
- What procedures are in place to manage and recover from the compromise of keys?
- Is key revocation performed in a cloud-wide atomic-operation?

Cryptography

- For what operations (and where) is encryption used?
- Are all encryption mechanisms based on third party tested and evaluated products?
- Does security policy clearly define what must be encrypted?

Checklist 9.14 Data Center: Physical Security and Power and Networking[48–50]

Data Center: Physical Security

- What are the requirements for being granted physical access to the CSP's facility?
- Do non-employees require escort in the facility?
- Is entry into the facility constrained by function and entry location? (Examples: shipping and receiving, housekeeping)
- Is the facility divided into zones such that each requires access permissions?
- Is strong authentication (for example, multifactor card and pin or card and biometric) required for physical access?
- Is all access monitored and documented?
- Are all entry locations alarmed and monitored?
- Is video monitoring complete for all common areas of the facility?
- How long is video retained?
- How often is a risk assessment performed for physical security?
- Does the CSP require that all deliveries or equipment removals be performed by the CSP within the facility (that is, is there a separate shipping facility outside the physical perimeter of the cloud facility itself)?

Data Center: Power and Networking

- Is power and networking secured within the facility?
- Are environmental systems (lighting, AC, fire detection) implemented to industry standards?
- Is air conditioning sized to withstand extended periods of extreme conditions?
- Is the facility exposed to moderate or higher risk of environmental or weather damage?
- Does the facility receive power from multiple power sources?
- Does the facility provide backup power generation for a period or time that is adequate to recover from loss of a primary power source?
- Does the facility have adequate UPS for short or temporary outages?
- Does the facility have multiple Internet connections, and are these from different tier 1 providers?

Checklist 9.15 Data Center Asset Management[51–53]

Data Center Asset Management

- Does the CSP maintain a current and complete inventory of all hardware, network, software, and virtual components that comprise the cloud?
- Does the CSP automate such inventory tracking and management?
- Does the CSP maintain a record of all assets that a customer has used or on which a customer has stored data?
- Does the CSP support asset categories of different sensitivity levels, and if so, how are these isolated or separated from each other?
- Does the CSP maintain segregation or physical separation of assets at different sensitivity levels?

Checklist 9.16 Operational Practices[54–56]

Operational Practices

- Is there a formal change control process, and are the procedures clearly documented?
- Does change control include a means to guide decisions as to what changes require a reassessment of risk?
- Are operating procedures clearly documented and followed?
- Are there separate environments for development, testing, staging, and production?
- What system and network security controls are used to secure end user or tenant applications and information?
- What security controls are used to mitigate malicious code?
- What are the backup procedures (who does this, what gets backed up, how often is it done, what form does it take, and are backups periodically tested)?
- Where are back ups stored, and for how long are they kept?
- Will the CSP securely delete all copies of customer data after termination of the customer's contract?
- Under what circumstances are customer resources sanitized using industry best practices (for example, degaussing)?
- Does the CSP have documented security baselines for every component that comprises the cloud infrastructure?

Checklist 9.17 Incident Management[57–59]

Incident Management

- What information is captured in audit, system, and network logs?
- How long is it retained, and who has access to it?
- What controls are used to protect these logs from unauthorized access and to preserve the chain of custody of such materials?
- How and how often are logs reviewed?
- How and how often are logs checked for integrity and completeness?
- Are all systems and network components synchronized to a single time source (NTP)?
- Does the CSP have a formal process to detect, identify, and respond to incidents?
- Are these processes periodically tested to verify that they are effective and appropriate?
- Are log and other security data maintained to comply with legal requirements for chain-of-custody control, and do the data and controls comply with legally admissible forensic data?
- What is the escalation process for incident response?
- Does the CSP use intrusion detection, security monitoring, or SEIM to detect incidents?
- Does a CSP accept customer events and incident information into their security monitoring and incident management process?
- Does the CSP offer transparency into incident events, and if so, what kind of information is shared with customers and users?
- How are security events and security logs protected and maintained?
- How long are security logs retained?
- Who has access to such logs?
- Does the CSP allow customers to implement a host-based IDS in VMs?
- If so, can a customer send such VM IDS data to the CSP for processing and storage?
- How are incidents documented as they take place?
- How are incidents analyzed after the incident has ended?
- Can the CSP provide a forensic image of a customer VM?
- Does the CSP report statistics on incidents to customers?

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