Sécurité des SI
Généralités

Jean-Marc Muller

Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Les origines

- Novembre 1988. Ver Morris
  - ➡ Robert Morris a exploité des vulnérabilités connues de sendmail et de la commande finger sur des systèmes UNIX
  - ➡ 10% des machines des machines de l'époque contaminées (≈ 6000)
  - ➡ Interruption de services. Préjudice estimé de 10 à 100 millions de $
- Travail collectif pour résoudre le problème
  - ➡ Robert Morris a été condamné (400 heures, 10000$)
  - ➡ Prise de conscience des problèmes de sécurité
  - ➡ Création du CERT (Computer Emergency Response Team)

L'artisanat

- Années 1990
  - ➡ Démocratisation d'Internet
  - ➡ Kevin Mitnick premier hacker recherché par le FBI (l'art de la supercherie)
  - ➡ Premières exploitations de vulnérabilités par dépassement de tampon, injection SQL, XSS (« cross-site stripping »)
- Début 2000
  - ➡ Apparition de DDOS (« distributeur dénial of service ») et des premiers Botnets (quelques centaines d'ordinateurs)
  - ➡ Apparition des premiers vers informatiques (I Love You, Code Red,…)

L'industrialisation

- La cybercriminalité
  - ➡ Apparition de gangs de hackers notamment dans les « pays de l'Est »
  - ➡ Organisations criminelles sévissent sur Internet
    - Ex : Silk Road fermé en 2013 par le FBI (drogue et vente d'arme)
    - Ex: rançon logiciels (ransomware)
  - ➡ Pertes estimées à plusieurs centaines de millions d'euros par an
    - Agissent à partir de paradis numériques
  - ➡ Commerce d'armes d'intrusion ou de destruction numérique
    - Ex : location de botnets, achat de 0-day

La mondialisation

- La guerre de l'information
  - ➡ Influence grandissante des gouvernements
  - ➡ Affecter l'information de l'adversaire, ses processus basés sur l'information, ses systèmes d'information, tout en se protégeant simultanément
  - ➡ Prise en compte du numérique en Chine par l'Armée de Libération du Peuple
  - ➡ Chine, Russie, Inde, Etats-Unis sont réputés pour leur attitude agressive dans ce domaine et pour l'importance des moyens investis
  - ➡ L'espace numérique devient un territoire de guerre et de diplomatie
    - Estonie en 2007, Stuxnet en 2010, Snowden en 2013
      - « Les nouveaux maîtres du monde » documentaire de la chaîne ARTE
      - « On nous écoutes - L'histoire secrète de la NSA »

Actuellement

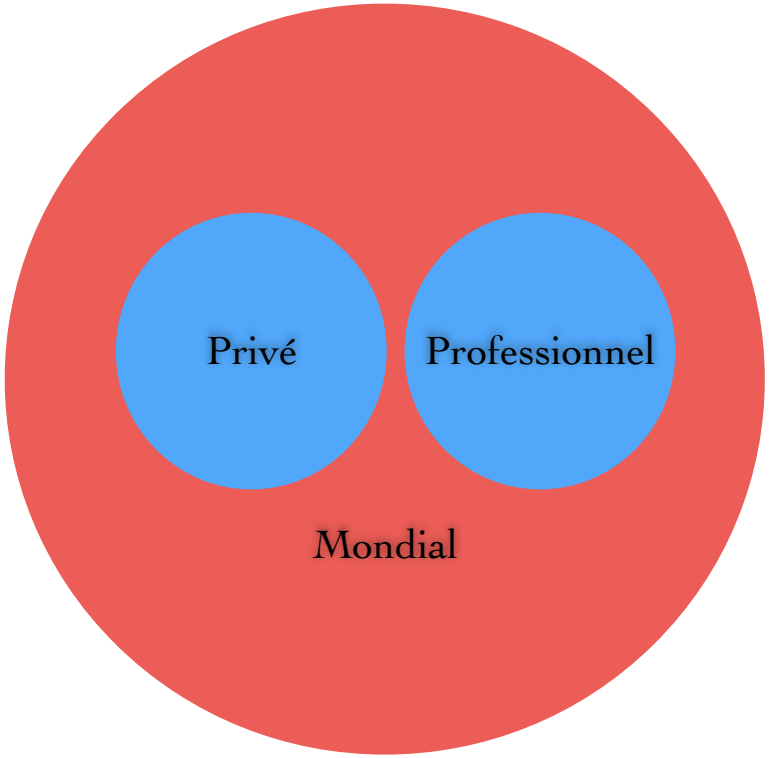
- Les objets connectés
  - ➡ (Septembre 2016) DDoS à partir de botnet (Mirai) de 100000 caméras IP (OVH, Dyndns,..)
  - ➡ Compromission de véhicules, de drones, de jouets, de télévision, de dispositifs médicaux, de vibromasseurs…
- La politique et le vote en ligne
  - ➡ Élections américaines, défiance de la France,..
- Malwares pour smartphones (Exo Android Bot, Mazar 3, …)
- Ransomwares (cryptolocker, cryptowall, torrentlocker, teslacrypt,…)
- Développement de l'usage du Darknet (Tor, Alphanet,…)

Contexte

- Difficultés de poursuite
- Manque de moyens (coût de l'enquête souvent supérieur au préjudice)
- Facilité d'action (rebond, anonymisation)
- Attaques nombreuses de tous niveaux, outils disponibles
- Ca vient de toutes parts…

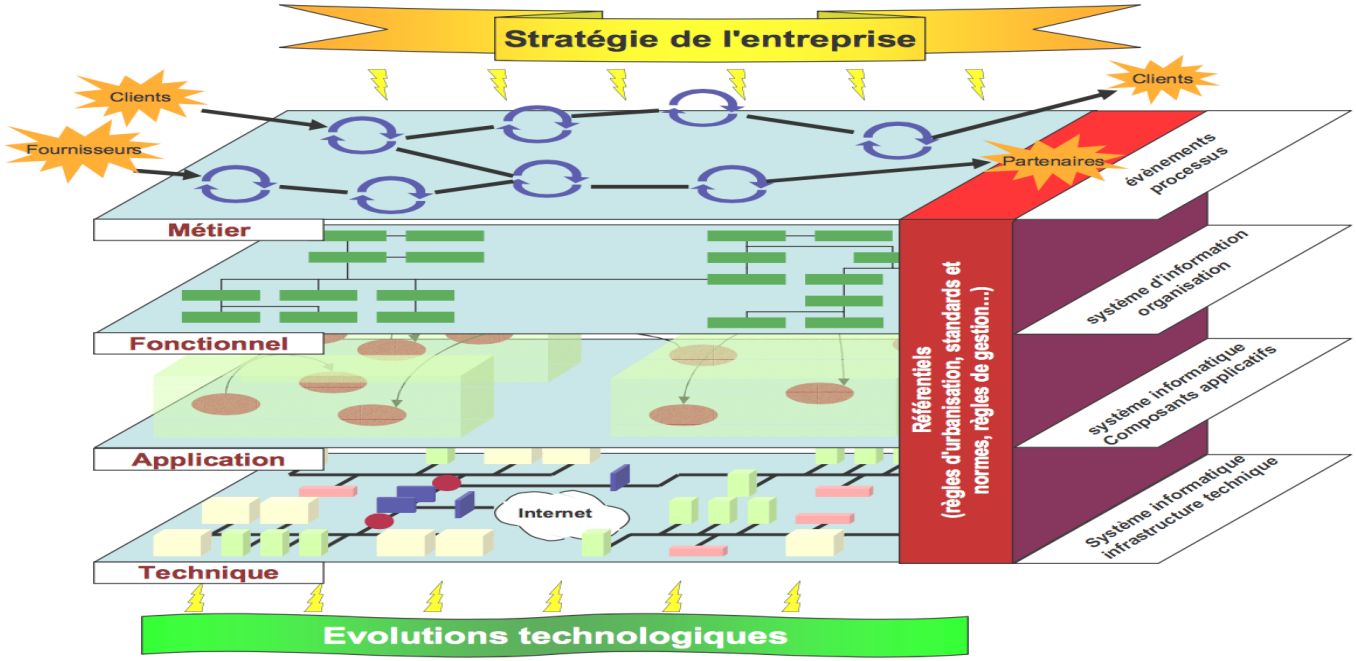
Contexte

- Trois domaines



Sécurité des systèmes d'information

- SI : éléments participant à la gestion, le stockage, le traitement, le transport, la diffusion de l'information au sein d'une organisation



Source : Cigref

Sécurité des systèmes d'information

- Challenge technique
  - Domaine vaste (système, réseau, chiffrement, BD, Web, …)
  - Évolutions rapides (portables, smartphones, objets connectés, …)
- Challenge humain
  - Contrainte vs service, centre de coût, sensibilisation
- Amplification des problèmes
  - Connectivité réseau globale, de partout et à tout moment
  - Changement des pratiques (BYOD, externalisation)

De nombreuses problématiques

- Quelle est la sécurité adaptée à mon entreprise ? Comment l'organiser ?
- Peut-on utiliser le Cloud ? Comment ?
- Comment gérer le nomadisme ? Comment gérer le BYOD ?
- Comment gérer les utilisateurs du SI (authentification, chiffrement des données,..) ?
- Concurrence avec les services gratuits ?
- Comment respecter le droit des usagers …
- Les entreprises sont très mal protégées
  - Pas ou peu de PRA, peu de RSSI, peu de formations…

Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

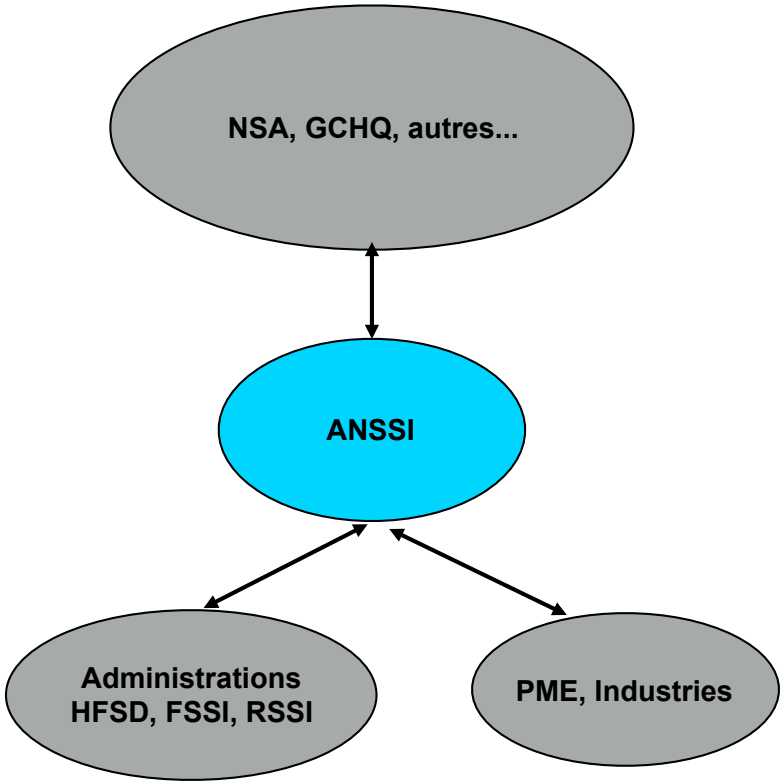
ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

Directement sous l'autorité du premier ministre

Missions

- Assurer la sécurité des SI de l'Etat
- Contribuer l'expression de la politique gouvernementale en matière de SSI
- Evaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir
- Développer l'expertise scientifique et technique dans le domaine de la SSI au bénéfice de l'administration et des services publics
- Assurer la sensibilisation et la formation des français à la SSI



DGSI et autres

- Direction Générale de la Sécurité Intérieure
  - ➡ Ex DCRI, elle-même ex DST + RG
  - ➡ Protection du patrimoine économique
- Dépend du ministère de l'intérieur
- Missions
  - ➡ Contrespionnage
  - ➡ Protection du potentiel économique, industriel et scientifique du pays
  - ➡ Intervient dans les cas de piratage «sensibles»

CERT

- Computer Emergency Response Team
- Plusieurs au niveau international et national
- En France : CERT-FR, CERT-Renater, CERT-IST, CERT-LEXSI, CERT-XMCO, CERT-Osiris,..
- Missions
  - ➡ Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations
  - ➡ Traitement des alertes et réaction aux attaques informatiques
  - ➡ Etablissement et maintenance d'une base de donnée des vulnérabilités
  - ➡ Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquence

CNIL

- Commission Nationale de l'Informatique et des Libertés
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Autorité administrative indépendante
- Missions
  - ➡ Protéger la vie privée et les libertés individuelles ou publiques.
  - ➡ Veiller au respect de la loi "Informatique et Libertés" qui lui confie 6 missions principales
    - Informer, garantir le droit d'accès, recenser les fichiers
    - Contrôler, réglementer, sanctionner
- Nomination de CIL (Conseiller Informatique et Liberté)
  - http://www.cil.cnrs.fr/

Les organismes de normalisation

- L'ISO
  - Organisme international de normalisation
  - Ex : ISO 17799, ISO 2700x
- Les normes du British Standard Institute
  - Organisme de normalisation de Royaumes Unis
  - Ex : BS7999-2
- Les lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux d'information
  - Organisation de coopération et de développement économique
- Les critères communs pour l'évaluation de la sécurité des systèmes d'information
  - Standards dans les domaines de la SSI
  - Version américaine : livre orange du DoD

Les acteurs privés

- CLUSIF
  - Club de la Sécurité de l'Information Français
  - Club professionnel, ouvert aux entreprises ou collectivité.
  - Agir pour la sécurité de l'information, facteur de pérennité des entreprises
  - Sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique …
- Les cabinets d'expertise
  - Ex : HSC Herve Schauer Consultants. Anime le club 27001
- Les cabinets en droit
  - Ex : Alain Bensoussan Avocats

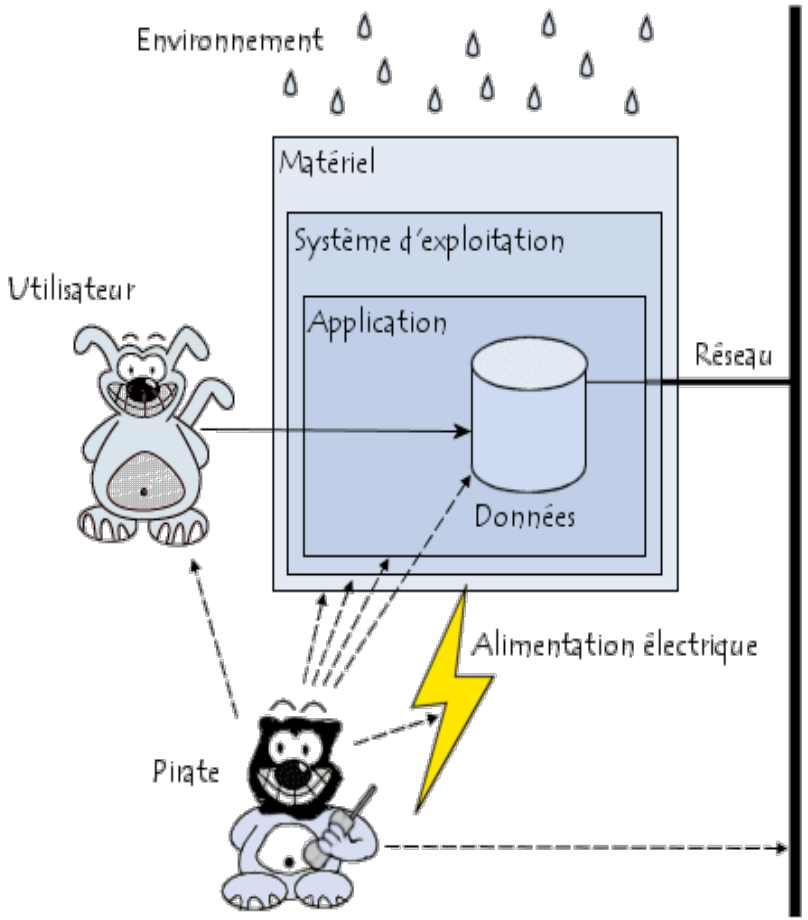
Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Risque

- **RISQUE = Menace * Vulnérabilité * Impact**

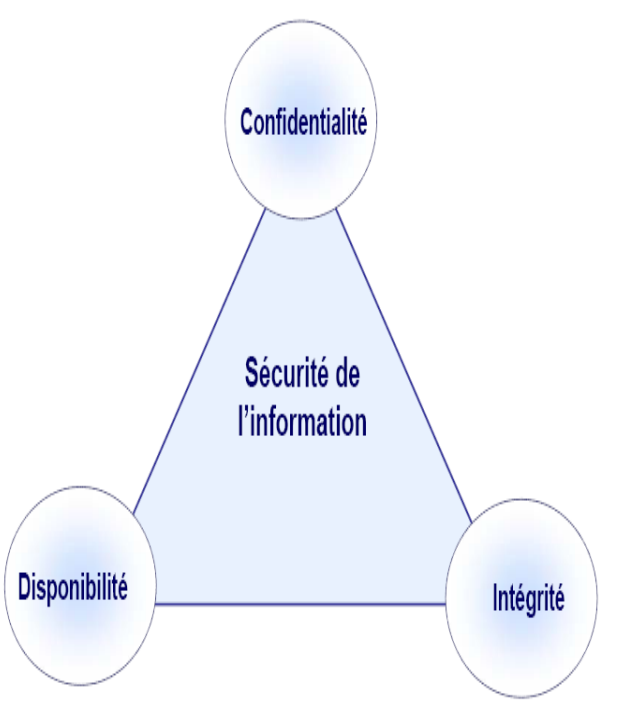
- Menace
  - ➡ Attaquant possible d'un élément du système d'information
- Vulnérabilité
  - ➡ Faiblesse, faille au regard de la sécurité d'un élément du système d'information
- Impact
  - ➡ Conséquence de l'occurrence du risque
  - ➡ Peut être quantifié par un niveau de sévérité



- **RISQUE = Probabilité occurrence * Préjudice**

Les objectifs

- Disponibilité
  - ➡ Accessibilité et utilisation de la ressource
- Intégrité
  - ➡ Assurer que l'information est exacte, pas altérée, modifiée
- Confidentialité
  - ➡ Information accessible aux seuls ayant droits
- Authenticité, autorisation, traçabilité
  - ➡ Prouver identité
  - ➡ Gérer les droits d'accès aux ressources
  - ➡ Historique des actions effectuées sur les données



Les impacts

- Financier
  - ➡ Perte d'argent
- Image
  - ➡ Dégradation de la réputation
- Organisationnels
  - ➡ Soucis de continuité d'activité
- Réglementaires
  - ➡ Poursuites juridiques

Les menaces

e-Crime organisé

Services d'Etats

Script kiddies

Hacktivistes

Les menaces

- Venant de l'intérieur
  - ➡ Utilisateur novice (maladresse, curiosité)
  - ➡ Utilisateur averti, surtout quand c'est l'administrateur (fraude, revanche)

Les vulnérabilités

- Peuvent être de plusieurs types
  - ➡ Humaines
  - ➡ Réseaux
  - ➡ Systèmes et logicielles

Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Vulnérabilités humaines

- Incompréhension des enjeux
  - ➡ La sécurité est perçue comme une contrainte, car les enjeux sont souvent mal expliqués
- Manque de pédagogie
  - ➡ Adapter la sécurité aux utilisateurs : niveau de compréhension
- Contournement de la politique de sécurité
  - ➡ Mot de passe sur un post-it, logiciels à la mode, peer to peer...
- Nature humaine
  - ➡ Site pornographiques, ..

L'histoire de Jacky

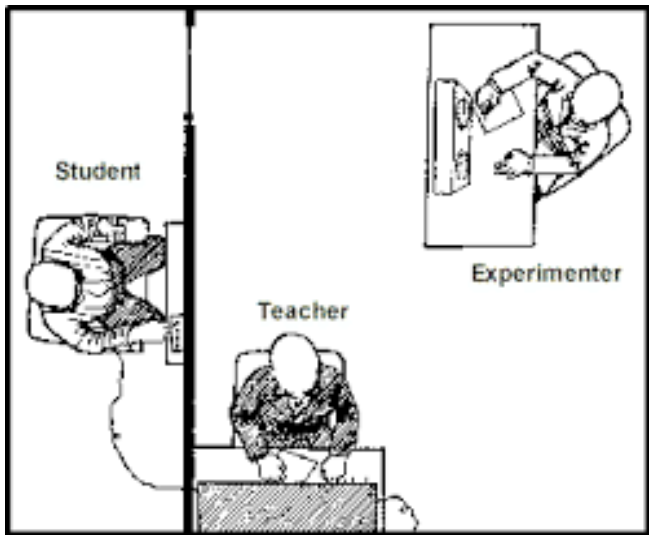
- Jacky découvre la puissance et la magie de l'informatique
  - ➡ Usage de sites pornographiques
  - ➡ Réinstallation encore et encore de son système d'exploitation
- Jacky prend peur
  - ➡ Message d'avertissement et de menace
  - ➡ Destruction du disque dur de son PC
- Jacky se fait arnaquer
  - ➡ Fausse alerte virale
  - ➡ Recours à un prestataire en ligne pour régler ses soucis
- A suivre …

Vulnérabilités humaines

- Les humains sont influençables et corruptibles
  - ➡ 37% des personnes ont donné leur mot de passe spontanément
  - ➡ 71% (y compris les 37%) contre une barre chocolatée
- L'attaquant doit donner l'impression qu'il est de la maison
  - ➡ Kevin Mitnick : "l'art de la supercherie"
- S'appuie sur des ressorts psychologiques
  - ➡ Rien d'obligatoire, guider vers la solution, pas de conflit, approche physique, dilution de responsabilité, déresponsabilisation, devoir moral
  - ➡ Attaques ciblées - Etat de l'art et méthodologies (2012)
  - ➡ Expérience de Milgram (soumission à l'autorité contraire à la morale)

Expérience de Milgram

- Effectuée entre 1960 et 1963 par le psychologue Stanley Milgram
- Inspirée par les camps d'extermination de la seconde guerre mondiale
- Évaluer le degré d'obéissance d'un individu devant une autorité qu'il juge légitime
- Analyser le processus de soumission à l'autorité quand elle pose des problèmes de conscience



Expérience de Milgram

- Apprenant
  - 75v : grognements
  - 120v : cris de douleur
  - 150v : demande d'arrêt de l'expérience
  - 200v : hurlements
  - 300v : refus de répondre, marmonnements au sujet de la douleur
  - 330v à 450v : silence

- Réponses de l'expérimentateur
  - "Il va bien. Continuez"
  - "Le bon déroulement de l'expérience nécessite que vous poursuiviez"
  - "Il est absolument essentiel que vous poursuiviez"
  - "Vous n'avez pas le choix. Vous devez continuer"

Expérience de Milgram

- Résultats
  - ➡ Plus de 20% des participants sont allés au bout de l'expérience ...

- Analyse
  - ➡ Pas de sadisme
  - ➡ Désir de tenir la promesse faite
  - ➡ Souhait de se montrer digne de l'autorité légitime
  - ➡ Incapacité à bouleverser une situation sociale bien définie
  - ➡ Abandon de responsabilité personnelle en se laissant instrumentaliser
  - ➡ ...

Vulnérabilités humaines

- Exemple de phishing

Chèr(e),

Vous avez saisi une autre adresse email comme adresse électronique de contact pour votre identifiant Université de Strasbourg . Pour terminer le processus, nous devons vérifier qu'il s'agit bien de votre adresse électronique. Cliquez simplement sur le lien ci-dessous et ouvrez une session à l'aide de votre identifiant Université de Strasbourg et de votre mot de passe.

Vérifiez maintenant >

http://ec2-52-10-20-140.us-west-2.compute.amazonaws.com/agenda.unistra.fr

Pourquoi ce courrier électronique vous a-t-il été envoyé ?
L'envoi de ce courrier électronique s'applique lorsqu'une personne ajoute ou modifie une adresse électronique de contact pour un compte identifiant Université de Strasbourg. Si cela ne vous concerne pas, ne vous inquiétez pas. Personne ne peut utiliser votre adresse électronique comme adresse de contact pour un identifiant Université de Strasbourg sans votre vérification.

Pour plus d'informations, consultez la rubrique Questions et réponses.

Merci,
L'assistance à la Université de Strasbourg

Collecte d'informations passive

- Informations personnelles
  - ➡ Les sites Web institutionnels
  - ➡ Réseaux sociaux
    - ➡ Les adresses de messagerie (TheHarvester - script python)
    - ➡ Les traces laissées sur les réseaux sociaux
      - ➡ https://inteltechniques.com/menu.html
    - ➡ Les comptes compromis
      - ➡ https://haveibeenpwned.com
      - ➡ http://pastebin.com

Collecte d'informations passive

- Informations personnelles
  - ➡ Les services gratuits en ligne
  - ➡ https://donottrack-doc.com/

- *"La vie privée est devenue une sorte de monnaie d'échange. Elle nous sert à payer les services en ligne. Google ne fait rien payer pour Gmail. En lieu et place, il lit vos emails et vous envoie des publicités en fonction des mots-clés trouvés dans votre correspondance privée*". Dan Lyons, éditorialiste à *Newsweek*

Collecte d'informations passive

- Les moteurs de recherche
  - ➡ Google dorking

    www.googleguide.com/advanced_operators_reference.html

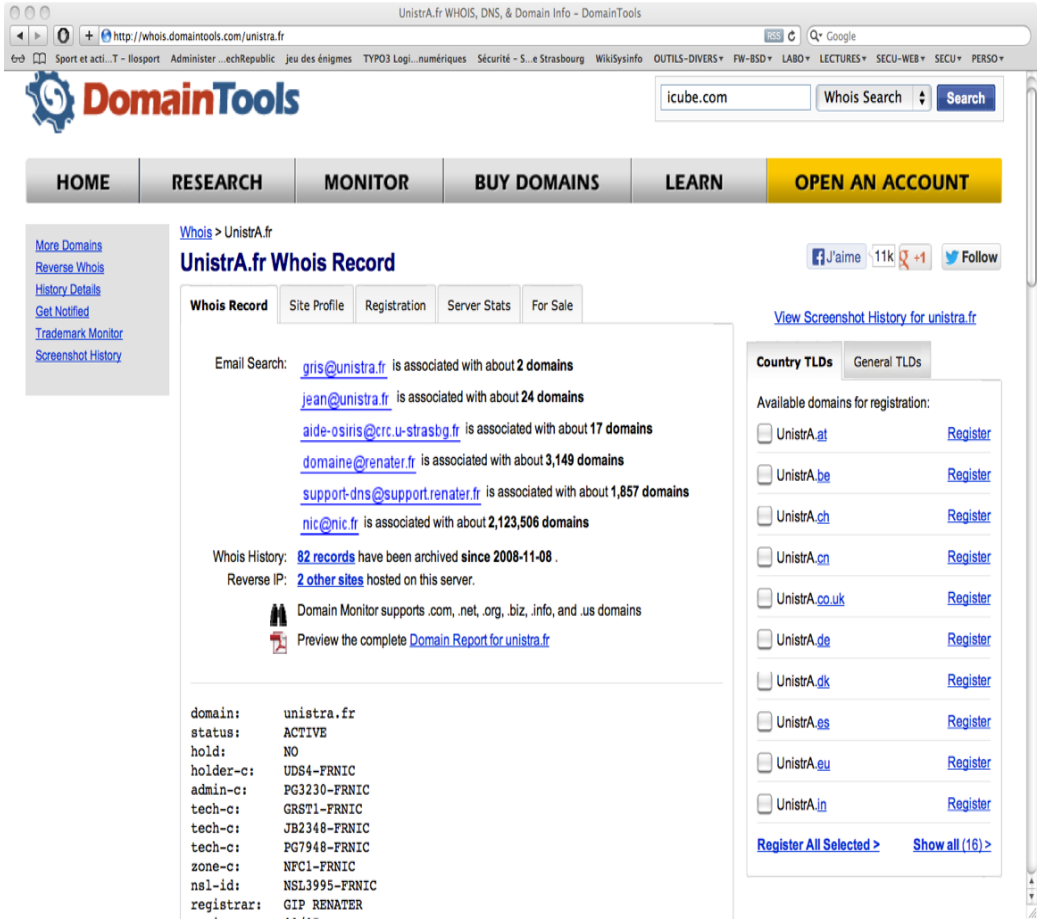
    https://www.exploit-db.com/google-hacking-database/

  - ➡ NerdyData Hacking

    Recherche de morceaux de codes intégrés à un site web

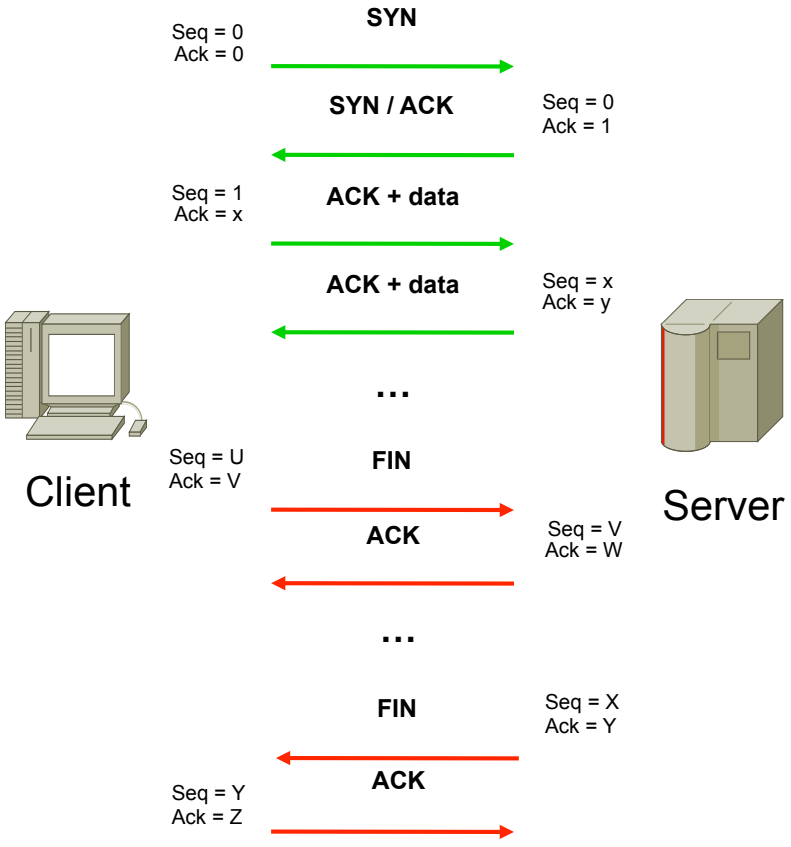
Collecte d'informations passive

- Informations techniques
  - ➡ DNS (dig, nslookup)
  - ➡ Whois
    - http://whois.domaintools.com/
  - ➡ Robtex
    - www.robtex.com

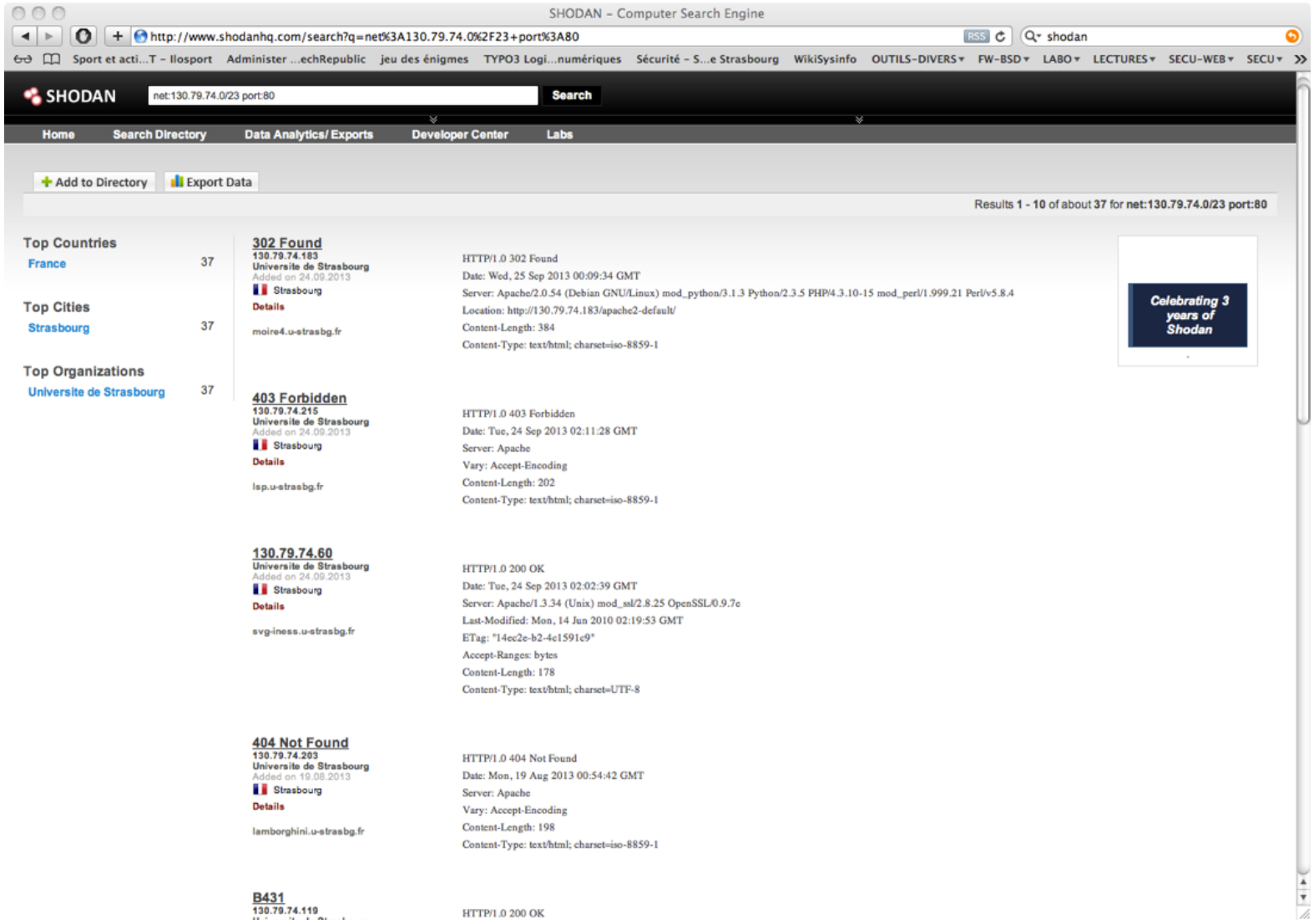


Collecte d'informations (nmap)

- Cartographie du réseau
  - ➡ Traceroute (UDP, TTL variable)
  - ➡ Balayage ICMP (ping),
  - ➡ Balayage TCP
- Identification des systèmes
  - ➡ Prise d'empreinte système (TCP, ICMP)
  - ➡ Identification/traversée des équipements filtrants

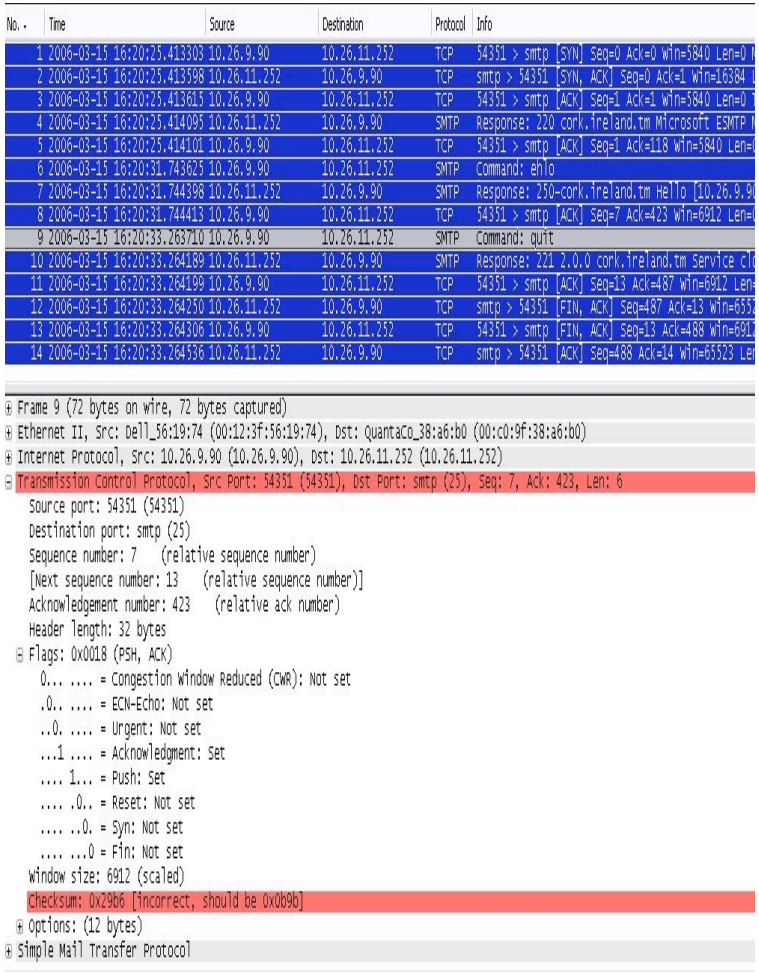


Collecte d'informations (shodan)



Collecte d'informations (sniffing)

- Accès aux réseaux
  - ➡ Accès au réseau filaire/sans-fil
  - ➡ Absence/faiblesse des mécanismes de chiffrement
- Écoute du trafic (Sniffing)
  - ➡ Cartographie
  - ➡ Récupération de mots de passe



Vulnérabilités systèmes & logicielles

- Faiblesses d'authentification
  - ➡ Recherche de mots de passes triviaux
    - Tentatives itératives de pénétration
    - Attaque par dictionnaire, attaque par brute force
  - ➡ Comptes classiques (oracle, admin, root, …)
  - ➡ Mot de passe constructeurs
    - Recherche google "default admin password"
  - ➡ Protocoles bavards (pop, smtp, telnet,…)

Vulnérabilités systèmes & logicielles

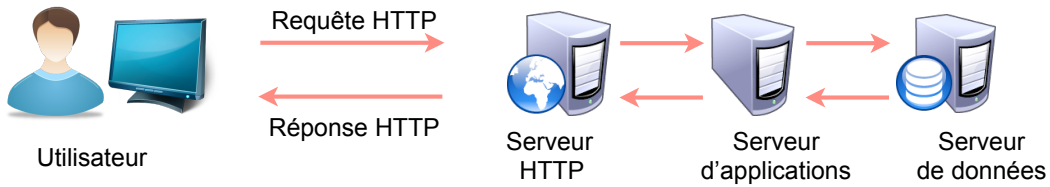
- Faiblesses de conception (implémentation)
  - ➡ Failles systèmes
    - Difficultés de mise à jour
  - ➡ Failles protocolaires
    - Faille openssl debian (2008), Heartbleed, Shellshock (2014)
- Publication des vulnérabilités
  - ➡ SecurityFocus, Exploit Database, Intelligent Exploit, Full Disclosure, Openwall …
  - ➡ Zero day attack

Vulnérabilités systèmes & logicielles

- Faiblesses des langages
  - ➡ Attaque par débordement de tampon (buffer overflow)
    - Modification de l'adresse de prochaine exécution pour exécuter un code malicieux
  - ➡ Injection SQL
- Trop de programmeurs sont de mauvais programmeurs
  - ➡ Écrire un programme c'est faisable, bien écrire c'est plus difficile (ex : openSSL - faille HeartBleed)
  - ➡ Pas/mauvais contrôle des paramètres passés

Vulnérabilités web

- Multiples vulnérabilités
  - Client
  - Serveur web
  - Serveur d'applications
  - Serveur de données
  - Communications



- WASC (Web Application Security Consortium)

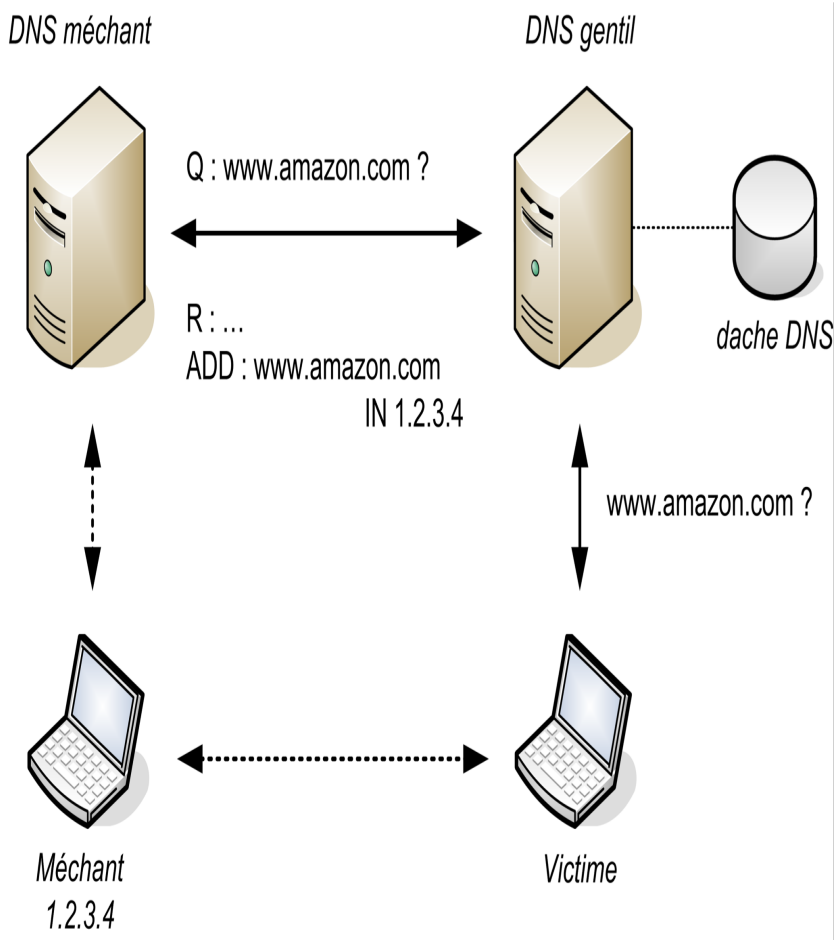
- Owasp (Open Web Application Security Project)
  - Top 10
  - Injection
  - Violation d'authentification

Les attaques réseaux

- Usurpation d'identité / de session
  - ARP spoofing
  - IP spoofing
  - Man in the middle
    - Relais applicatif (nécessaire pour SSL)
    - Hijacking (vol de session TCP)

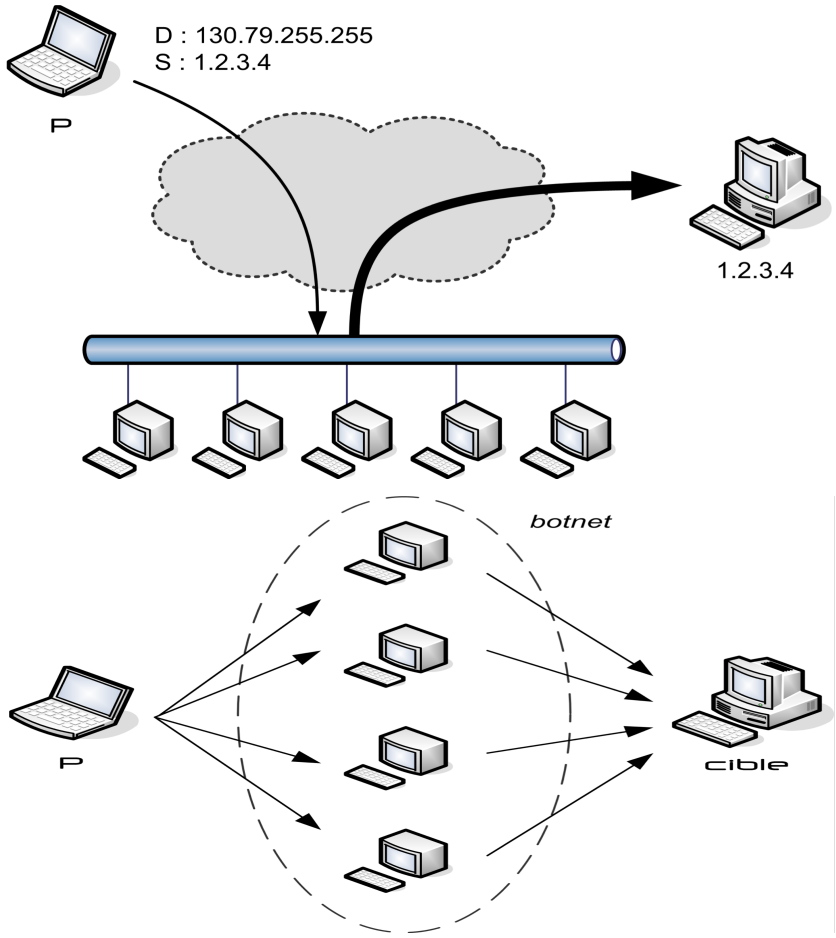
Les attaques réseaux

- Falsification du routage
  - ➡ Par OSPF
  - ➡ DNS Poisoning
  - ➡ Par BGP
    - 2008 Pakistan Telecom contre youtube
    - 2010 China Telecom détournement d'une partie du trafic d'internet



Les attaques réseaux

- Déni de service
  - ➡ Smurf attack
  - ➡ SYN flooding
  - ➡ DDoS (Botnets)
  - ➡ Spam (90% messages)



Botnets

- Flashback (avril 2012)
  - ➡ 600000 Mac OSX infectés
  - ➡ Faille logiciel JAVA
  - ➡ Vecteur d'infection : pages web compromises (dont dlink.com)
  - ➡ Une visite d'un site infecté suffit à contaminer le système
- Simda (démantelé en avril 2015)
  - ➡ 770000 machines avec une dizaine de serveur de commandes et de contrôle

Botnets


Arctic Ocean
GREENLAND (DEN.)
North America
CANADA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
ALGERIA
LIBYA
EGYPT
MALI
NIGER
NIGERIA
SUDAN
ETHIOPIA
C.A.R.
BRAZIL
ANGOLA
ZAMBIA
NAMIBIA
INDONESIA
PALAU
MARSHALL ISLANDS
FEDERATED STATES OF MICRONESIA
PAPUA NEW GUINEA
KIRIBATI
VANUATU
AUSTRALIA
Pacific Ocean
Atlantic Ocean
Indian Ocean

Les attaques ciblées

- Kali Linux
  - ➡ Distribution de pentest
- Scanner de vulnérabilités système
  - ➡ Nessus
  - ➡ OpenVas
- Metasploit
  - ➡ Framework d'intrusion

Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Authentification

- AAA (Authentication, Authorization, Accounting)
- Vérification de l'identité d'une entité pour autoriser l'accès à des ressources
  - ➡ Identification : action de nous distinguer parmi d'autres (login)
  - ➡ Authentification : action d'apporter la preuve que l'identifiant nous appartient (mot de passe)
  - ➡ Autorisation : ce à quoi l'authentification nous donne accès (droits)
- Mécanismes plus ou moins élaborés
  - ➡ Single Sign-On
  - ➡ Ex : CAS, Shibboleth

VPN

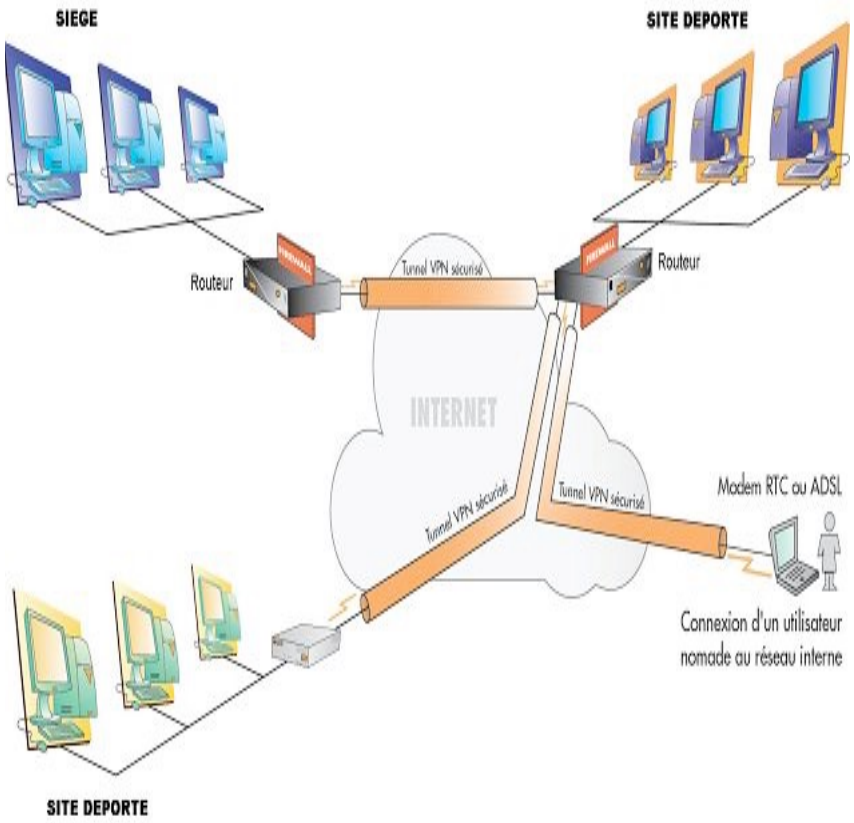
- Utilisation d'une infrastructure publique pour raccorder deux sites distants

  ➡ Avec IPSEC (IETF), avec PPTP (Microsoft et 3COM), ..

- Pas de coûts d'infrastructures supplémentaires

- Coûts ne dépendent pas de la distance

- Difficultés à garantir la bande passante (Internet)

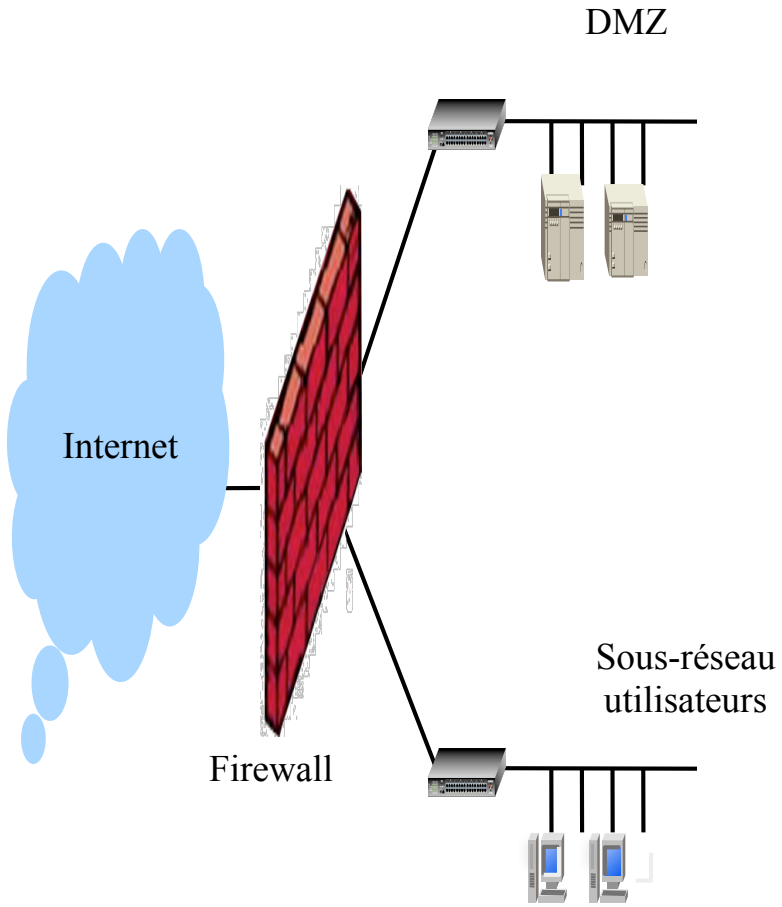


Pare-feu

- Contrôler l'ensemble des paquets
- Permet d'appliquer une politique de sécurité
  - ➡ Acceptation
  - ➡ Rejet
  - ➡ Destruction
- Permet une journalisation des actions
  - ➡ Possibilité d'accounting

DMZ

- Zone démilitarisée
- Sert à isoler les réseaux sensibles des machines vulnérables
- Protège mieux les machines faibles (postes)
- Permet d'exposer des services sur internet



Serveur mandataire

- Proxy
- Pare-feu de niveau applicatif
- Relaie l'information selon divers critères
  - ➡ Authentification
  - ➡ Contrôle de contenu
  - ➡ Contrôle de la source et destination
- Filtre en fonction du contenu et/ou protocole
  - ➡ Mots interdits dans les URL

IDS & IPS

- Système de détection d'intrusion
  - ➡ Capture de trafic ou analyse des logs
- Analyse
  - ➡ Pattern matching (séquence d'octets), protocol decode (contenu des champs), heuristic analysis (comportemental)
- Bases de données de signatures
- Risque de « faux positifs »
- Qualifié selon trois critères
  - ➡ Taille de la base de connaissance, validité de la base, ratio alarmes justifiées / non justifiées
- IPS = IDS + Parefeu

Pot de miel (Honeypot)

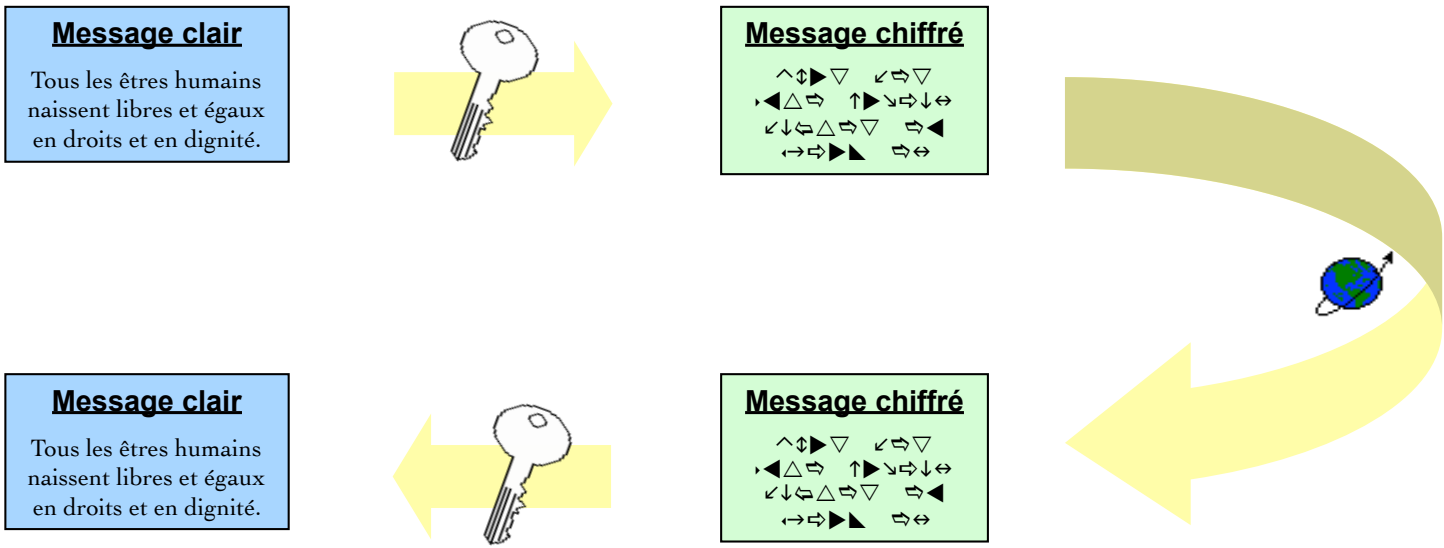
- Machine qui simule un serveur ou réseau
- Elle attire toutes les attaques
- Couplée à un IDS ou un IPS
- Système cloisonné pour éviter les rebonds
- Permet d'anticiper et comprendre les stratégies d'attaque

Chiffrement

- L'identification
  - ➡ Garantir l'identité de l'utilisateur
- L'authentification
  - ➡ Garantir l'origine de l'information
- La confidentialité
  - ➡ Garantir le secret de l'information transmise
- L'intégrité
  - ➡ Garantir la validité des informations
- La non répudiation
  - ➡ Impossibilité d'un auteur de nier avoir transmis/écrit une information

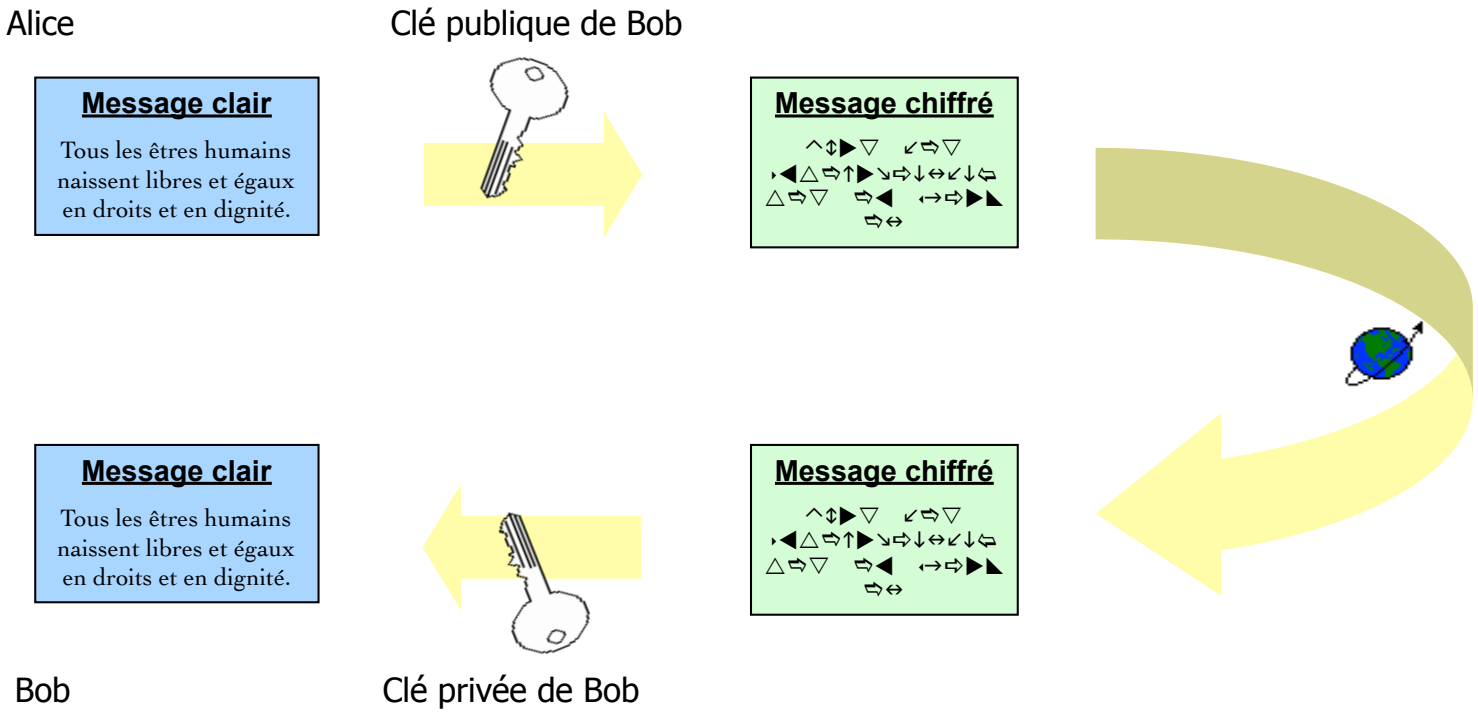
Chiffrement symétrique

- Utilisation d'une clé secrète partagée entre l'expéditeur et le destinataire



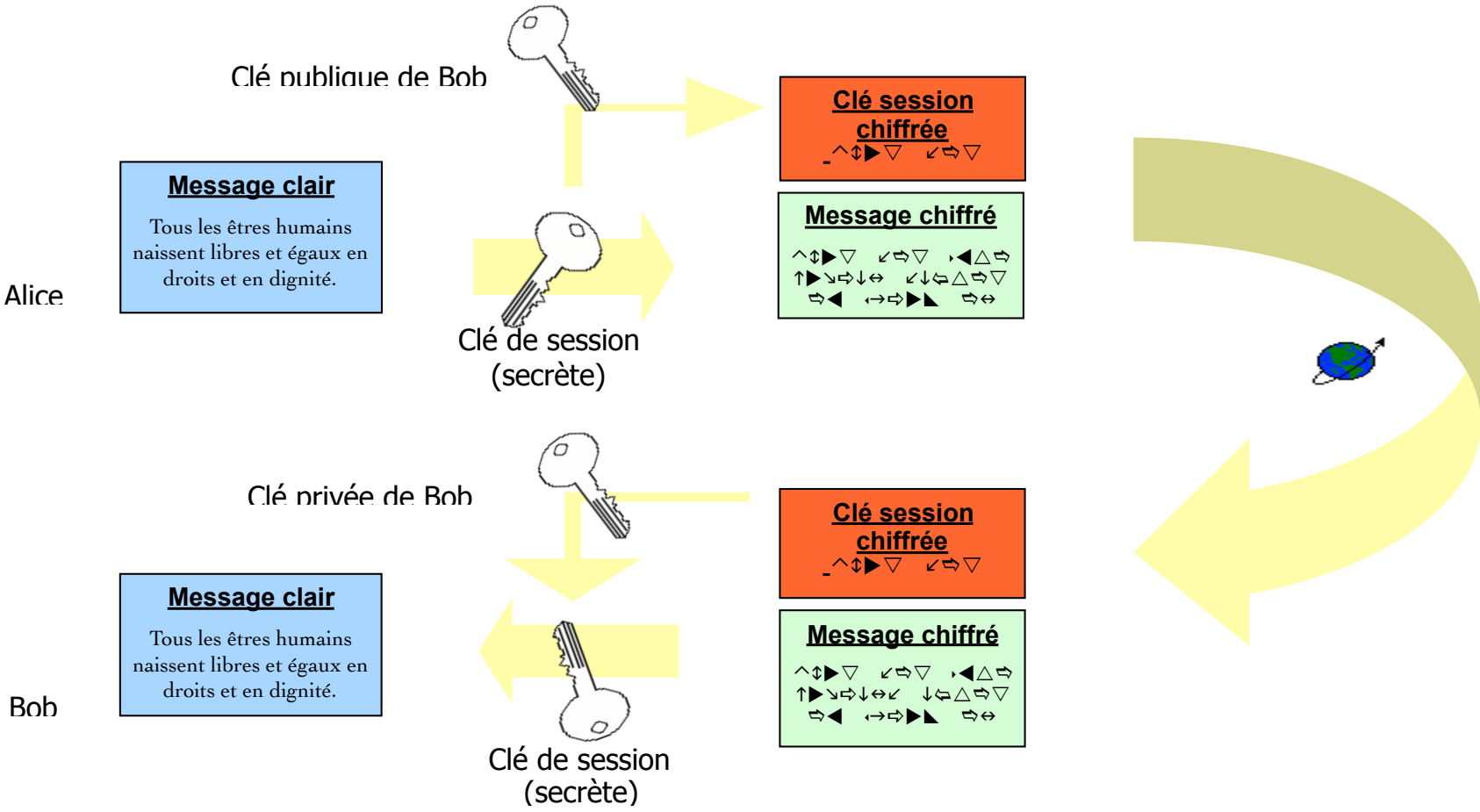
- DES, IDEA, Blowfish, SAFER, RC5, AES

Chiffrement asymétrique



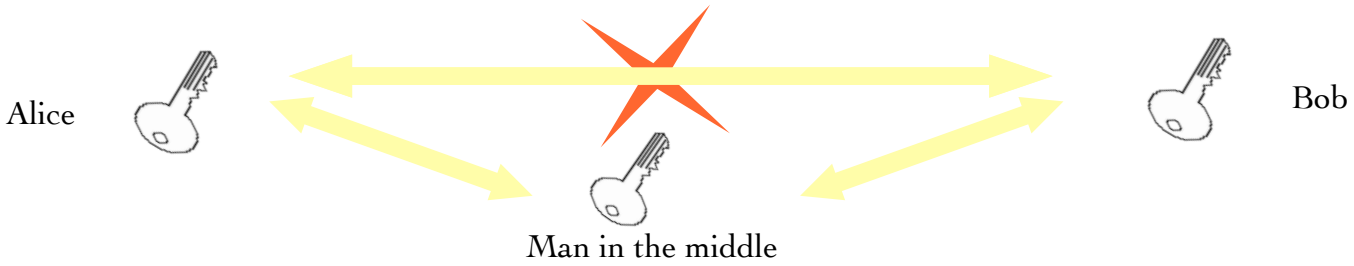
- RSA, Rabin, ElGamal, courbes elliptiques

Clé de session



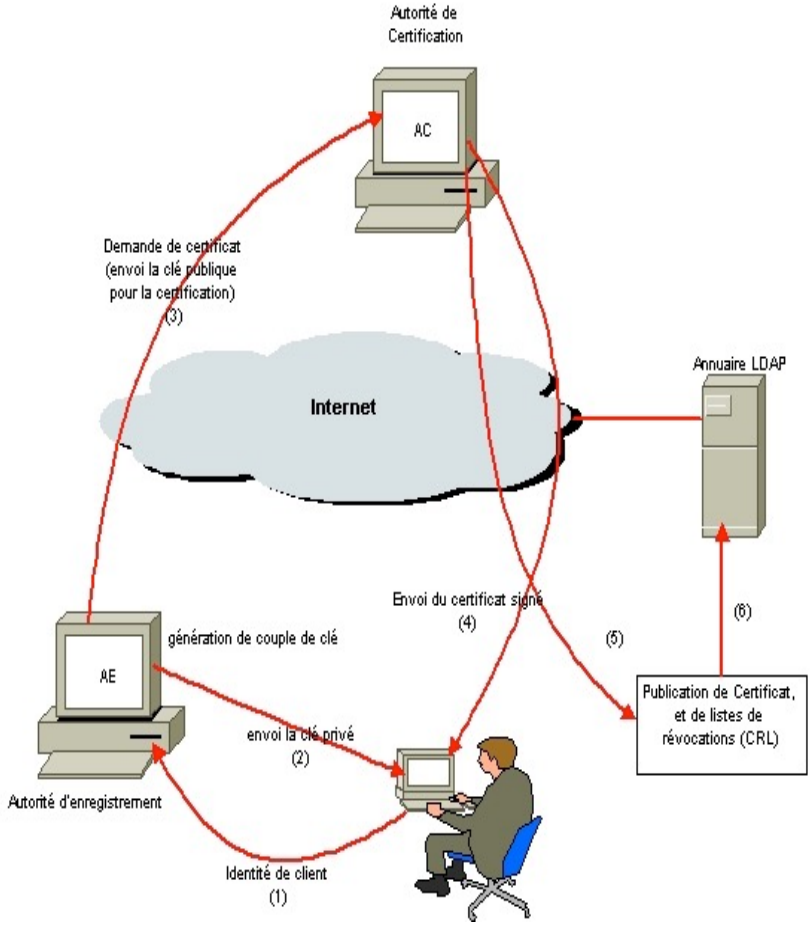
Certificats

- Problème du chiffrement asymétrique :
  - ➡ Comment s'assurer de la provenance d'une clé publique ?
  - ➡ Communiquer sa clé publique à ses correspondants
    - La transmettre par un canal (poste, Internet…) a priori non sécurisé.
  - ➡ Une personne mal intentionnée peut
    - Intercepter cette clé publique
    - La remplacer par sa propre clé publique
    - Attaque "man in the middle"



PKI

- Public Key Infrastructure
- Infrastructure de gestion de certificats
- Permet de mettre à disposition les clefs publiques
- Chaque demande de certificats fait l'objet d'une demande de validation auprès d'une autorité



Plan

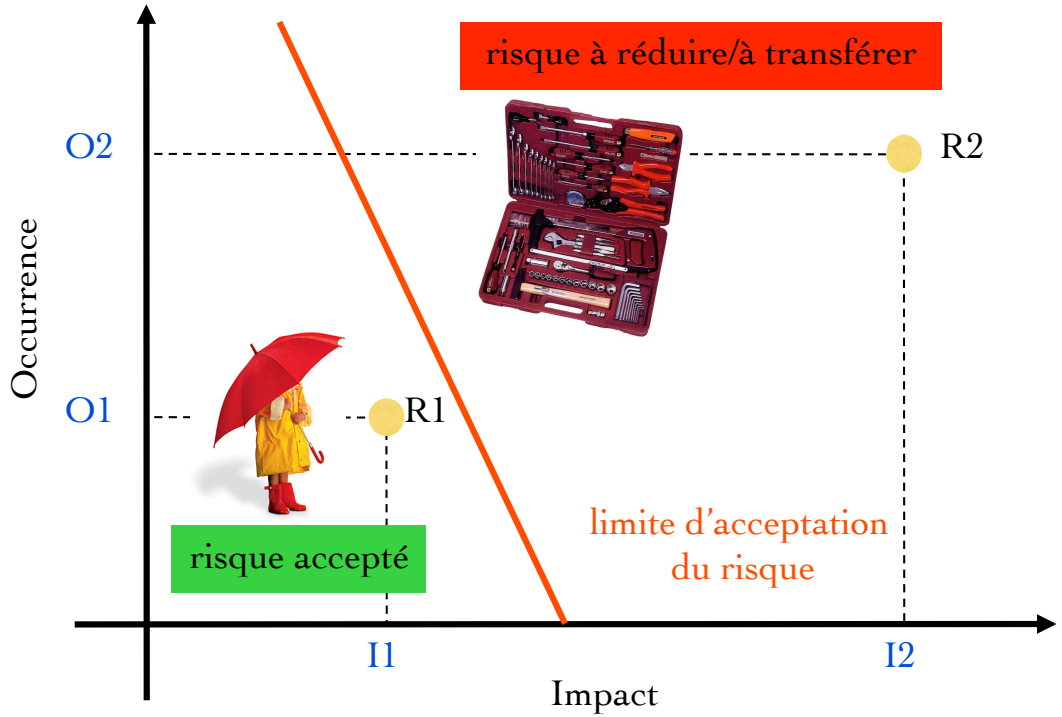
1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Organisation de la sécurité

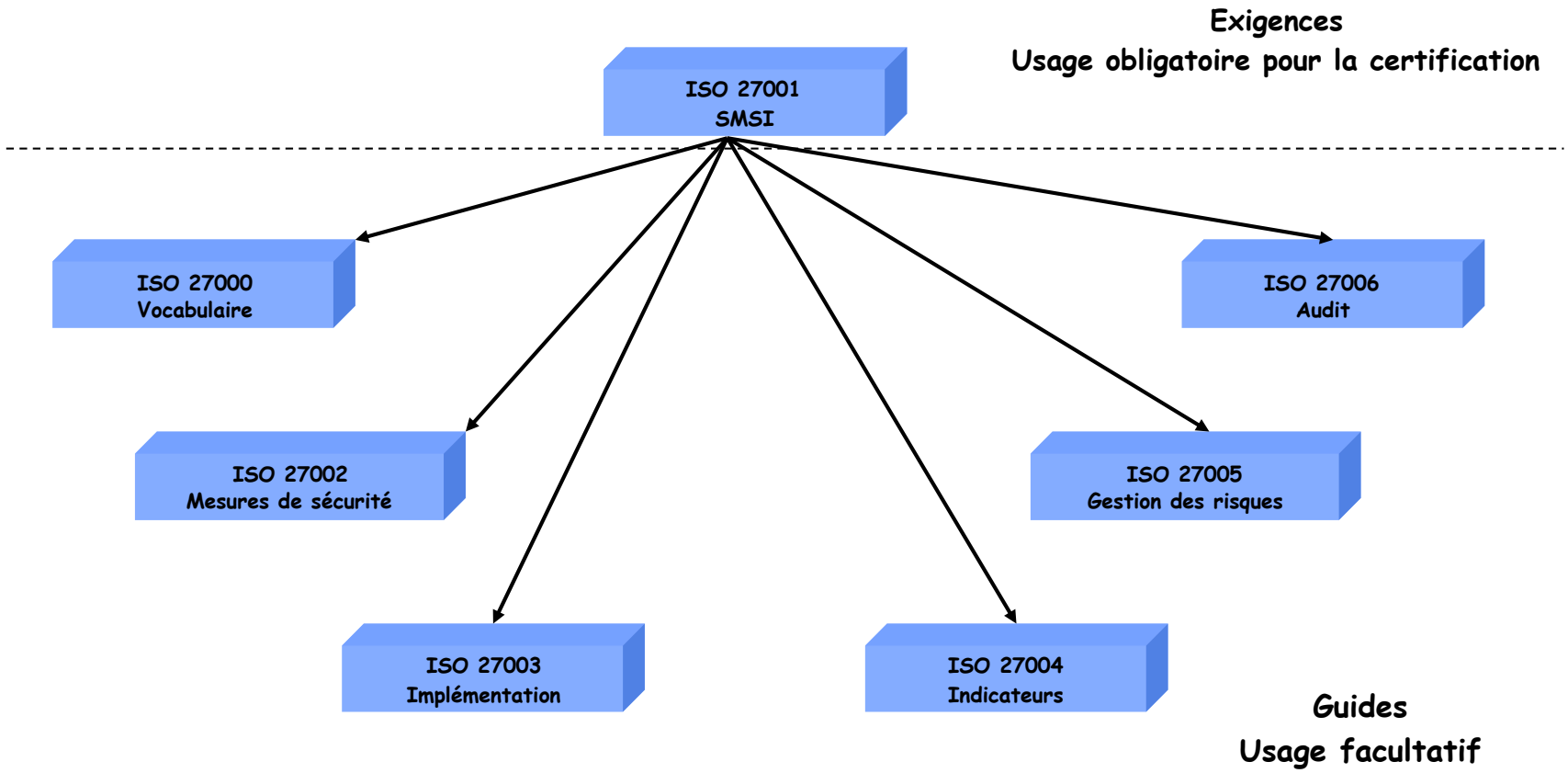
- Plusieurs référentiels selon le domaine d'activité
  - ISO27001 pour les systèmes d'information, Critères communs, catalogues de sécurité
- Approche organisationnelle
  - ➡ SMSI (Système de management de la Sécurité de l'Information)
  - ➡ Permet de mettre en place, faire évoluer et maintenir dans le temps
    - des mesures de sécurité techniques et organisationnelles
    - permettant d'atteindre les objectifs de sécurité fixés

Appréciation des risques

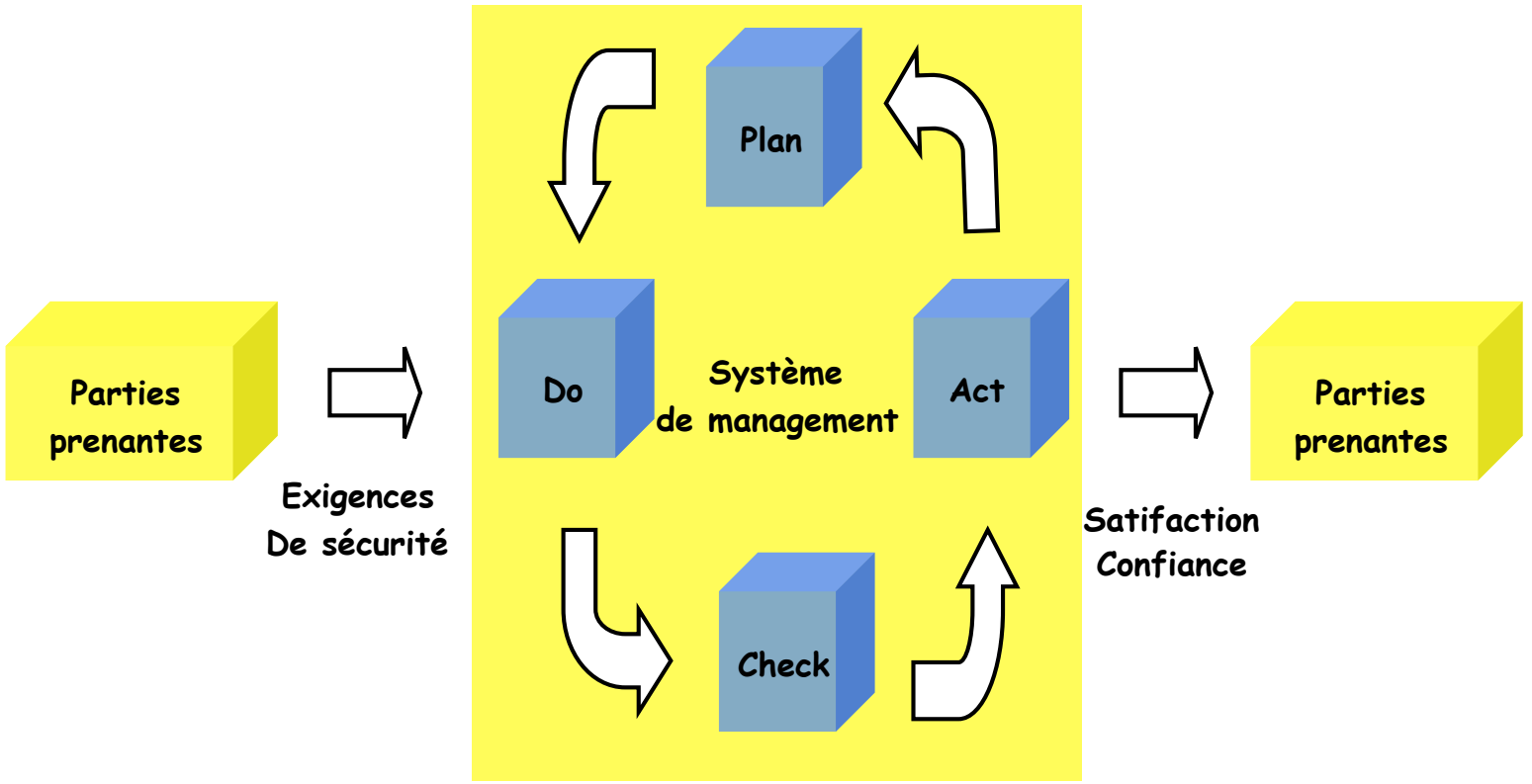
- Constituer une liste pondérée de risques
- Faire un choix



La norme ISO 27001

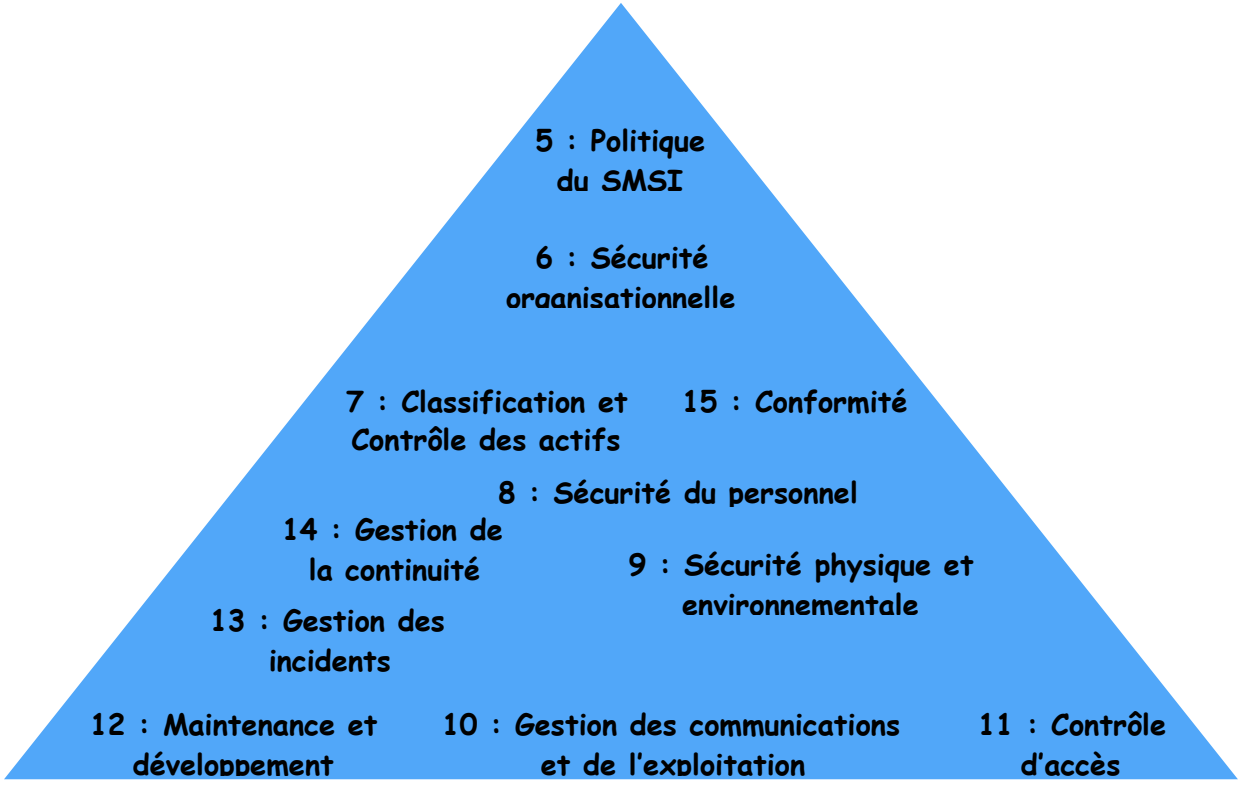


La norme ISO 27001



La norme ISO 27002

- Environ 130 mesures de sécurité détaillées



Plan

1. Introduction
2. Les acteurs
3. Concepts de base
4. Attaques et vulnérabilités
5. Les outils et techniques de protection
6. Organisation de la sécurité
7. Sécurité au quotidien

Les concepts de base

- Moindre privilège
- Défense en profondeur
- Simplicité
- Placer l'utilisateur au centre de la démarche
- Points d'accès uniques
- Interdiction par défaut
- Maillon faible
- Pas d'obscurité

Sécurité physique

- Serveurs sous clés et sous alarme
- Postes
  - ➡ Boîtiers fermés
  - ➡ Mot de passe BIOS
  - ➡ Boot sur média amovible dans BIOS désactivé
- Sécurité climatique
- Sécurité électrique

Sensibilisation des utilisateurs

- Des conseils à dispenser
  - ➡ Ne pas donner son mot de passe
  - ➡ Ne pas tenter de contourner les barrières
  - ➡ Connaître les applications douteuses
  - ➡ Mettre en place des solutions sûres

- En résumé

  Ne pas prendre d'initiatives en cas de doute !

Choix des applications

- Eviter les logiciels connus pour leurs défauts
  - ➡ telnet
  - ➡ ftp
  - ➡ RPC
- Souvent il y a un équivalent sécurisé
  - ➡ Grâce à SSL

Mises à jour

- Indispensable
- Différentes façons :
  - ➡ Patches
  - ➡ Apt-get update / upgrade
  - ➡ Compilation
- Sans mise à jour pas de sécurité valable

Gestion des comptes utilisateurs

- Éviter comptes sans mot de passe
- Changer mot de passe par défaut
- Gestion des droits
- Authentification
  - ➡ Ex : PAM, Kerberos, LDAP
- Single Sign-On (propagation d'identité)
  - ➡ Ex : CAS, Shibboleth

Les sauvegardes

- Permet la récupération des données détruites
- Assure la continuité de l'activité
- Différents types
  - ➡ Complète
  - ➡ Incrémentale
- Distinguer stockage, sauvegarde et archivage

Sécurisation des communications

- Au niveau système
  - ➡ Chiffrement des communications
    - SSH
    - VPN
  - ➡ Chiffrement des données
- Au niveau réseau
  - ➡ Pare-feu
  - ➡ IDS

Traitement des logs

- Détecter les tentatives d'intrusion
- Bien les configurer
  - ➡ Ni trop : saturation
  - ➡ Ni trop peu : peu de valeur
- Stockage des logs sur serveur dédié
- Durée de stockage limitée (CNIL)

Veille

- Se documenter
  - ➡ Magazines (MISC, HAKIN9)
  - ➡ CERT, SecurityFocus
  - ➡ Sites Web (ssi.gouv.fr, Slashdot, Hoaxbuster, donottrack…)
- Connaître parfaitement les composants du SI
  - ➡ Environnement physique, matériel, logiciel
  - ➡ et humain !

Vous êtes piraté !

- Avertir votre responsable sécurité
- Supprimer les accès externes
- Faites une sauvegarde du système
- Informer les usagers
- Examiner les traces du système
- Examiner les autres machines du réseau
- Réinstaller la machine en évitant la faille

ABC de la sécurité dans notre milieu enseignement/recherche

- Sauvegarde sur un support externe
- Antivirus / Parefeu /Mise à jour
- Limitation des droits administrateurs
- Chiffrement des supports de stockage
- Protection contre le vol
- Robustesse des mots de passe
- Prudence à l'égard des supports externes
- Utilisation prudente d'Internet
- Attitude prudente vis à vis des messages reçus
- Prévenir les responsables techniques et sécurité en cas de compromission

Conclusion

- Compromis entre sécurité et service à fournir
- Mettre l'utilisateur au centre
  - ➡ Menace principale vs client principal
  - ➡ Sensibiliser, communiquer
- Chaîne de la sécurité
  - ➡ Le pirate n'ira pas contre l'obstacle, il le contournera
  - ➡ Maillon le plus faible

Logiciels utiles

- Environnement système
  - ➡ Tails, John the ripper, sudo
- Surveillance réseau
  - ➡ Alerte ARP : arpwatch + Scan : nmap, Shodan + Scan amélioré : Nessus, Nikto (Web)
  - ➡ Accounting : MRTG + Cartographie : Nagios & Centreron
- Proxy : Squid + IDS : Snort, Bro, Suricata
- Audit : Kali Linux (ex Backtrack)
- Intrusion : Metasploit

Liens utiles

- Les CERTs
  - CERT-FR : http://www.cert.ssi.gouv.fr/
  - CERT-IST : http://www.cert-ist.com/
  - CERT XMCO : http://www.xmco.fr/
- Portail de la sécurité informatique : http://www.ssi.gouv.fr/
- La CNIL
  - http://www.cnil.fr/
  - http://www.cil.cnrs.fr/
- L'OSSIR : http://www.ossir.org/