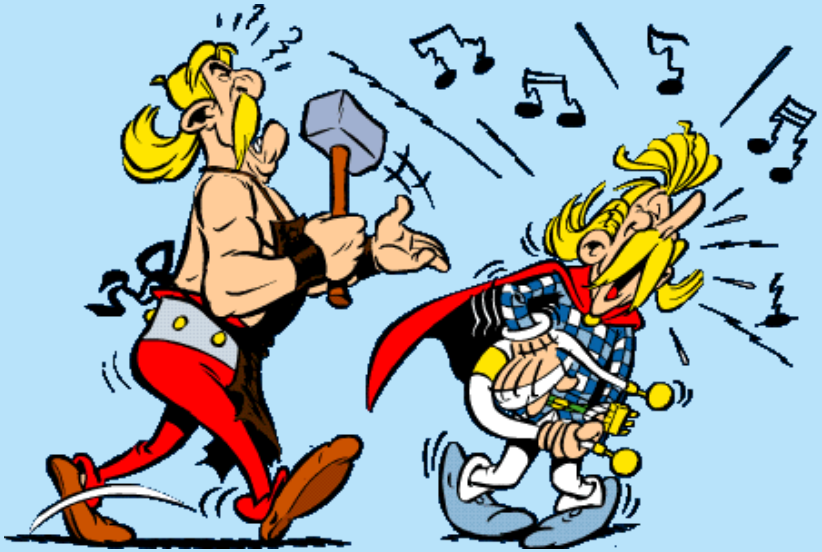
STRI
| Télécoms & Réseaux |

Projet de Sécurité

Groupe Audit

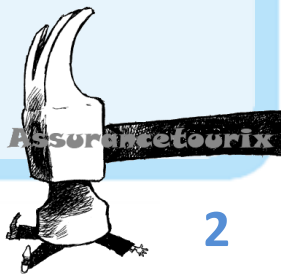
:: Assurancetourix



Réalisé par *:*

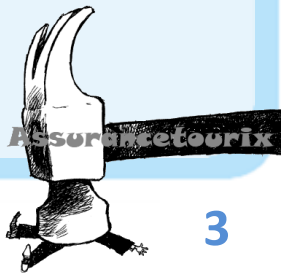
Lise BANQUET, Kenza BENGELLOUN, Goulven BUREL
Alexandre CLAMART, Tristan DELGRANGE, Christophe DUBOS
Romain LAVERNHE, Alexandre LACOURTE, Pierre-Michel LEBOULC'H
Nyaka LELO, Gwendal RAISON, Bastien TEIL,Maxime VIAUD
Médéric VIGROUX

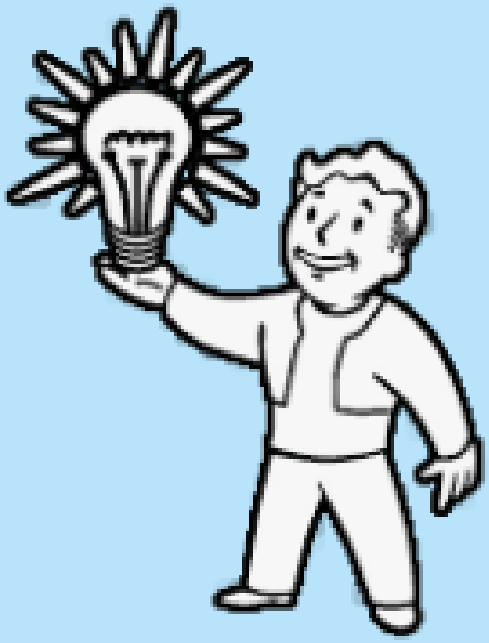
Sommaire



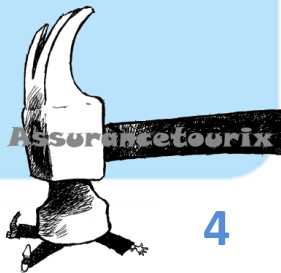
Introduction

- Projet sécurité lors MASTER 2 STRI :
  - ➔ Période attendue et source de tensions
- Promotion divisée en 3 groupes ➔ 14 personnes
  - ➔ Permet une organisation /hiérarchisation
  - ➔ Nécessite mise en place d'un moyen de communications
- Contractualisation avec l'équipe Défense
  - ➔ Définir objectifs et directives de chacun
  - ➔ Nécessite une collaboration



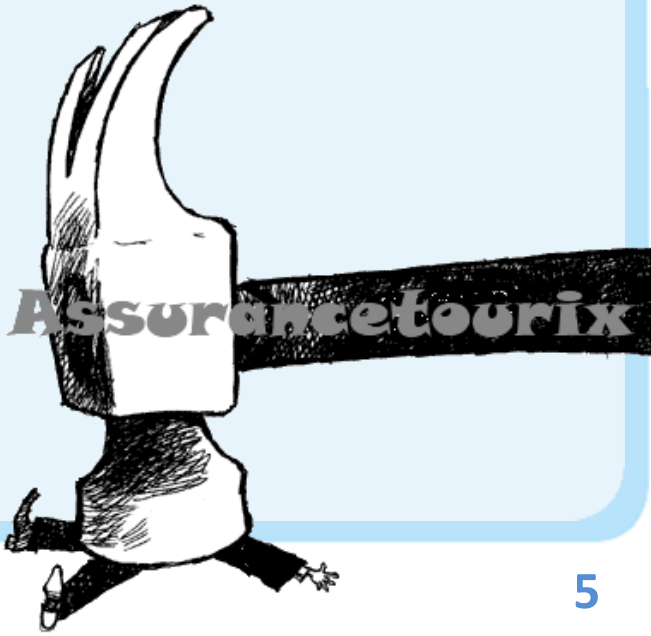


Présentation d'AssuranceTourix



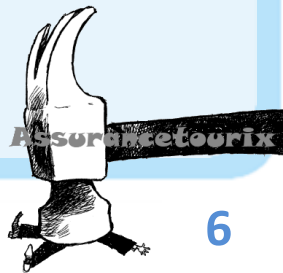
L'entreprise AssuranceTourix (1/2)

RAISON SOCIALE	AssuranceTourix France
STATUT	SAS au capital de 1 €
SIEGE SOCIAL	Université Paul Sabatier, Bât U3, IUP STRI, 118 Route de Narbonne 31062 Toulouse Cedex 9
EFFECTIF	14 personnes
HISTORIQUE	Septembre 2010 : création d'AssuranceTourix en France



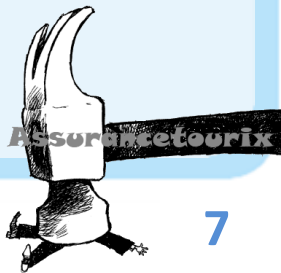
L'entreprise AssuranceTourix (2/2)

- Société d'expertise et prestataire de services :
  - Test de l'infrastructure et sécurisation ➔ Audit actif
  - Mise en œuvre téléphonie IP ➔ VoIP/ToIP
  - Suivi et pilotage de procédés ➔ Supervision
  - Surveillance, contrôle, détection ➔ IDS/IPS
- Certifications ISO 27001
  - Pour prestations d'audits de sécurité des SI
  - Management et sécurité organisationnelle et technique



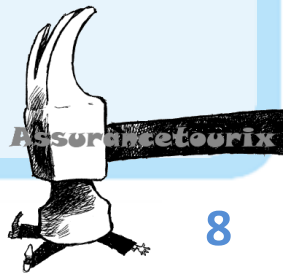
Rôle de l'audit

- Rôle Audit :
  - Avant la première confrontation :
    - Pré-étude du SI,
    - Identification des failles.
    - Déploiement de services de sécurité.
  - Pendant les confrontations :
    - Détection de tentatives d'intrusions.
    - Recommandations de sécurité.
- Problématique :
  - *Comment détecter et solutionner les failles du SI ?*

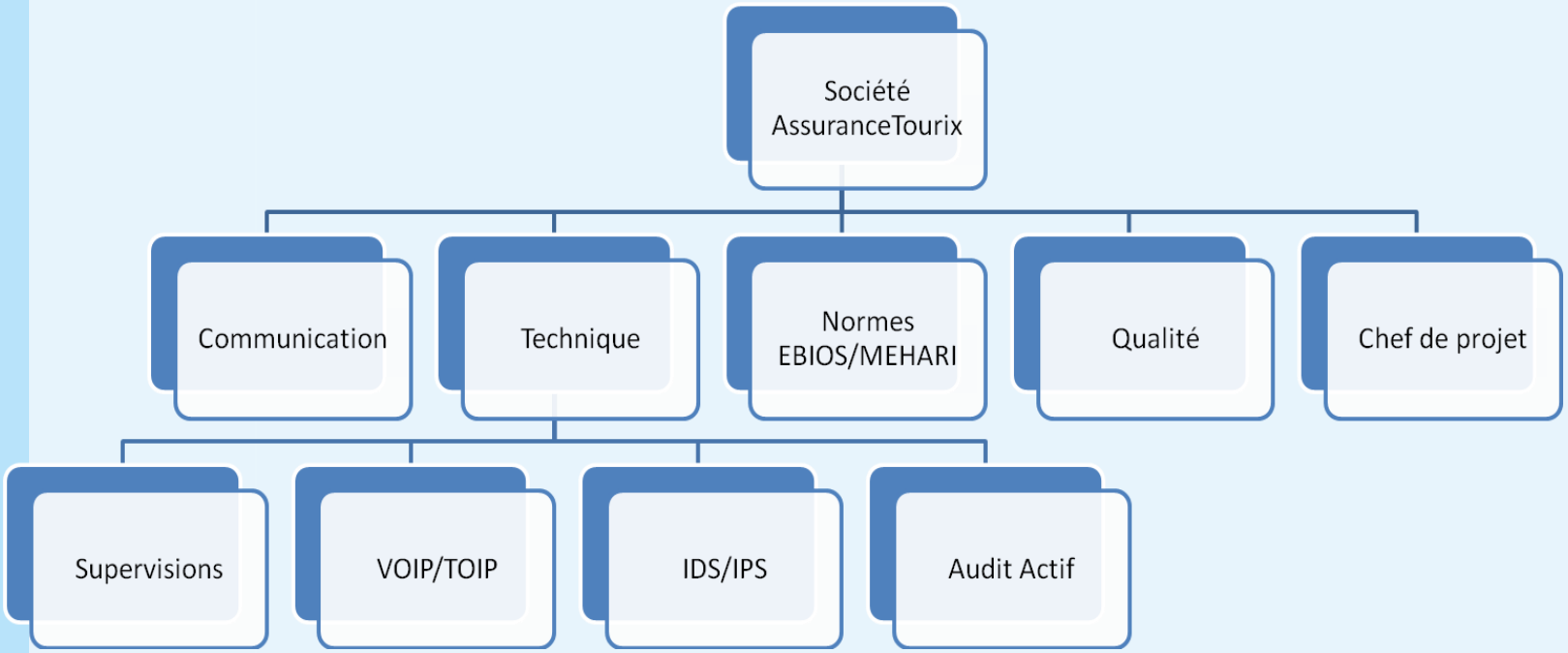


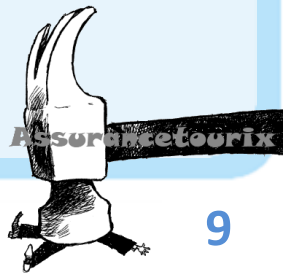
Organisation (1/2)

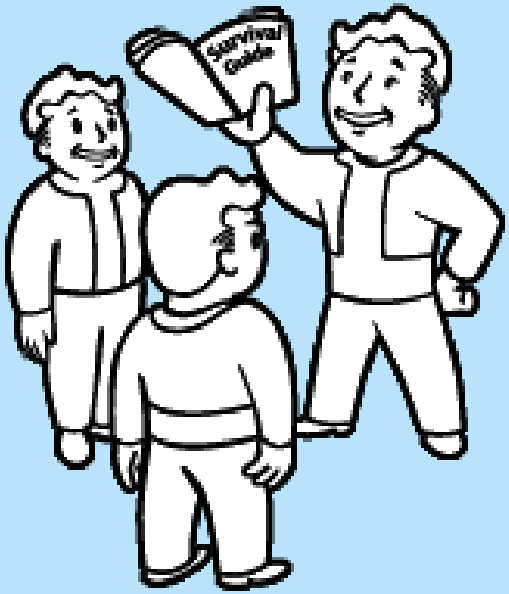
- 4 groupes majeurs :
  - Supervision : TEIL.B
  - IDS/IPS : DUBOS C.
  - Audit Actif : LACOURTE A.
  - VoIP/ToIP : VIGROUX M.
- 3 groupes supplémentaires :
  - Communication
  - Qualité
  - MEHARI



Organisation (2/2)



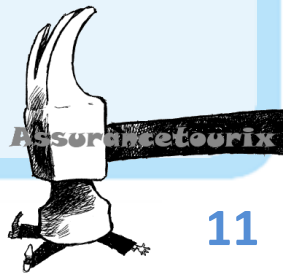




Communication

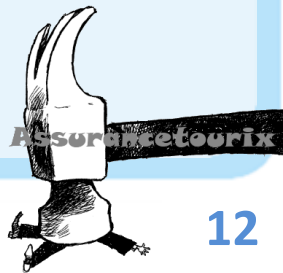
La communication interne

- Charte utilisateur du SI :
  - Limiter pertes et vols d'informations.
  - Comportements, règles et recommandations élémentaires.
    - Utilisation des ordinateurs personnels.
    - Verrouiller sa session.
    - Politique de mot de passe.
- Les échanges par mails :
  - Création d'@ mail Gmail.
  - Avantages :
    - Chiffrés et signés.
    - Rapatriement des mails (Thunderbird) et aucune redirection.
  - Inconvénients :
    - Echanger les clefs publiques.



La communication interne

- GoogleDocs
  - Avantages :
    - Accessible uniquement aux membres du groupe.
    - Partage permanent des documents.
    - Gestion plus aisée en comparaison aux mails.
  - Inconvénients:
    - Problème de sécurité : lié à Gmail.



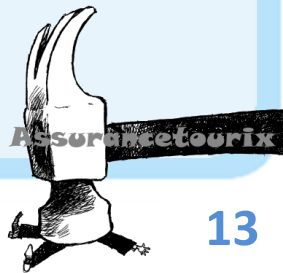
La communication externe

- Les réunions
  - Contenu des contrats
  - Moyens de communication
  - Compte rendu de réunion

- La communication formelle
  - Avant l'établissement des contrats
    - Entre services communication
    - Mails chiffrés
  - Après signature des contrats
    - Liste de contacts techniques
    - Mails non chiffrés (volonté d'Aérodef)

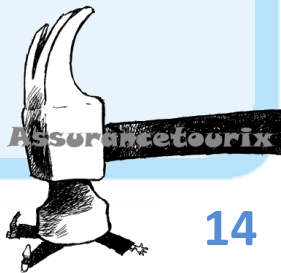
      ➔ Trop contraignant : client messagerie lourd

      ➔ Trop difficile à mettre en place
    - AéroDef d'accord de porter la responsabilité des conséquences



La communication externe

- La communication informelle
  - Processus officieux dit de « conversation de machine à café »
- Utilisation des deux types de communications
  - Formelle
    - ➔ Difficulté d'avoir des réponses au requêtes
  - Informelle
    - ➔ Résultats beaucoup plus convaincants
    - ➔ Plus rapides (quelques minutes VS quelques jours)

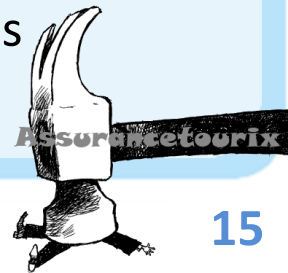


Les problèmes rencontrés

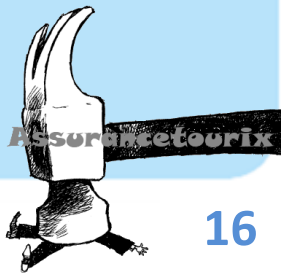
- Notamment avec le groupe de communication de la Défense.

- Une vision des choses différente entre les 2 groupes
  - Une équipe de défense très sécuritaire
    - Difficulté pour accéder aux informations
    - Mise en place de circuits de communications complexes
  - Une équipe audit dépendante de la Défense
    - Nécessité des infos pour proposer des solutions
    - Qui veut des échanges directs avec les responsables de l'architecture

➢ Prises de positions logiques mais qui ne vont pas dans le sens d'une bonne communication.



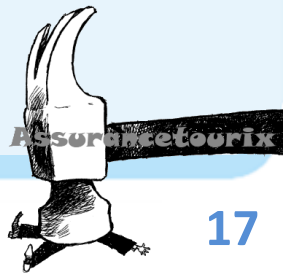
MEHARI



Définitions

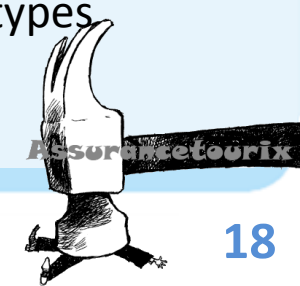
:: MEHARI

- Méthode Harmonisée d'Analyse des Risques
  - CLUSIF (Club de la Sécurité de l'Information Français)
- Evaluation et management des risques liés à l'information, ses traitements et les ressources mise en œuvre
- Open Source
  - Dernière version : Janvier 2010



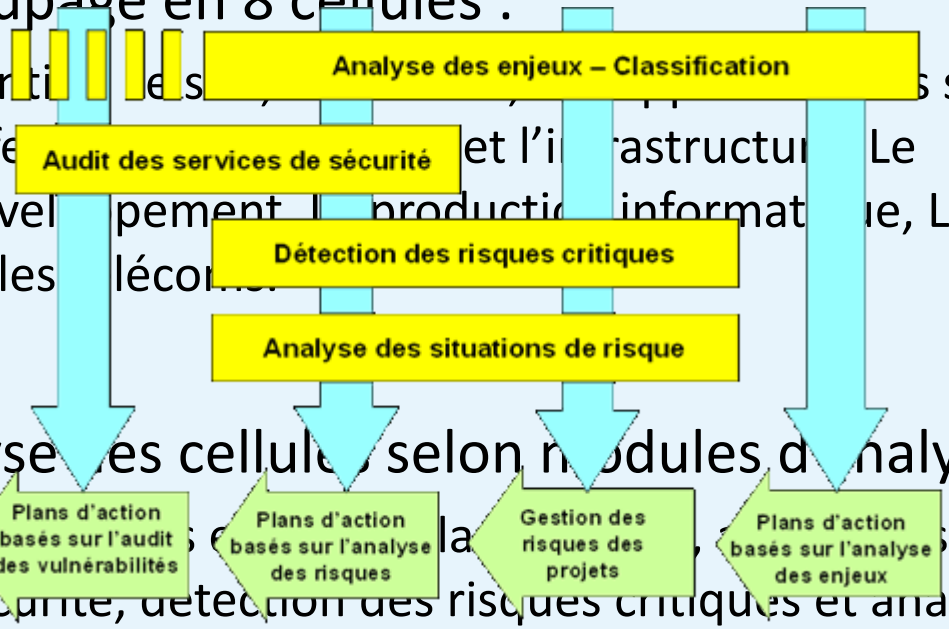
Objectifs

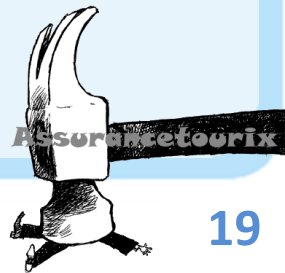
- Fournir une méthode d'analyse et de gestion des risques et plus particulièrement pour **le domaine de la sécurité de l'information**
- Une méthode **conforme aux exigences de la norme ISO/IEC 27005 :2008**, avec l'ensemble des outils et moyens requis pour sa mise en œuvre.
- Permettre une **analyse directe et individualisée** de situations de risques décrites par des scénarios de risques
- Fournir une gamme complète d'outils adaptée à la **gestion à court, moyen et long terme, de la sécurité**, quelle que soit la maturité de l'organisme en matière de sécurité et quelques soient les types d'actions envisagés.



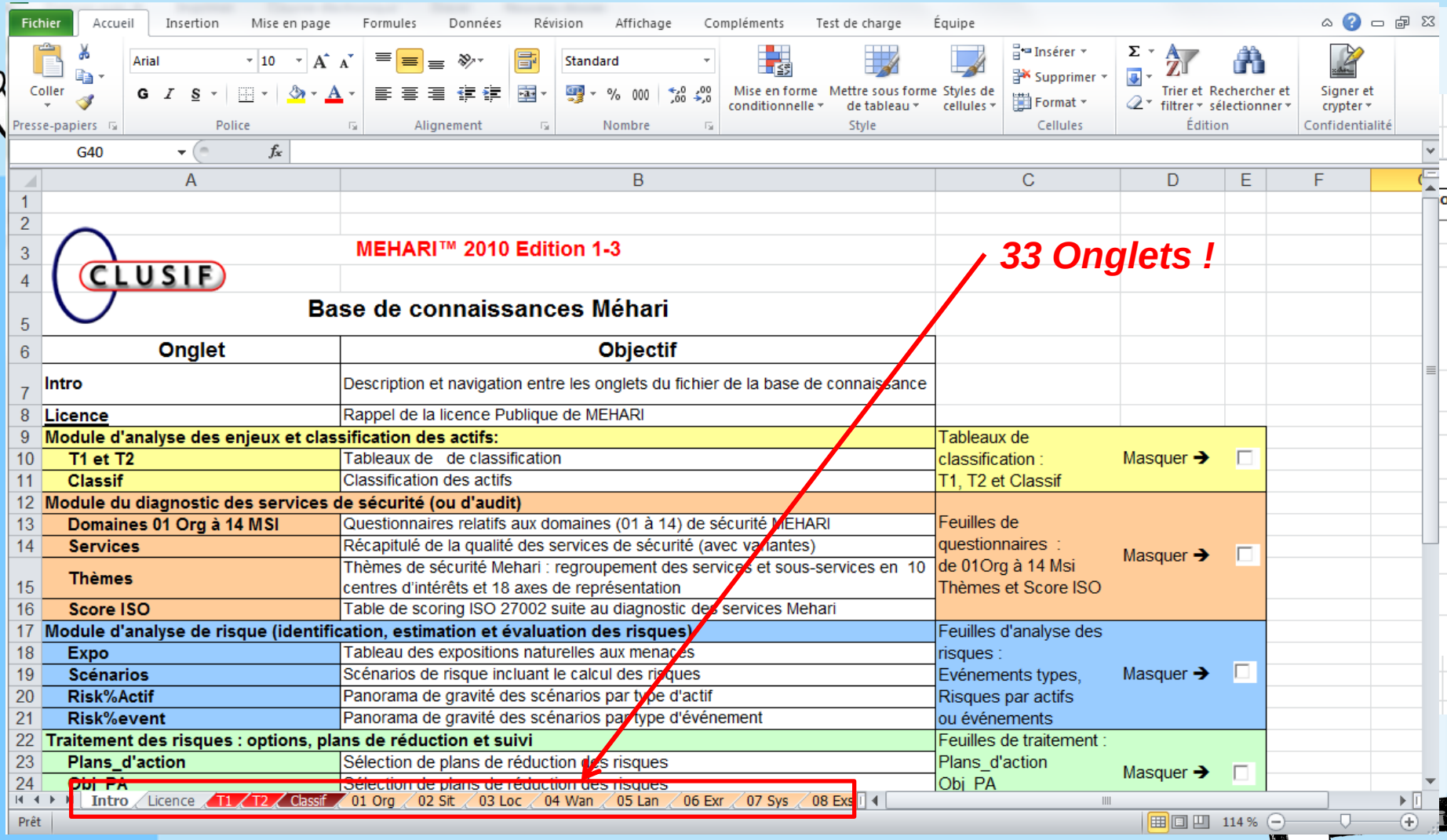
Concepts

- Concepts :
  - Découpage en 8 cellules :
    - L'entité [illegible] services offe[illegible] et l'i[illegible]rastructur[illegible] Le dével[illegible]pement [illegible]productio[illegible] informat[illegible]ue, Les réseaux et les [illegible]léco[illegible]
  - Analyse [illegible]es cellule[illegible] selon [illegible]odules d[illegible]nalyse :
    - A[illegible] la[illegible], [illegible]services de sécurité, détection des risques critiques et analyse des situations de risques





Les réalisations du groupe



MEHARI™ 2010 Edition 1-3

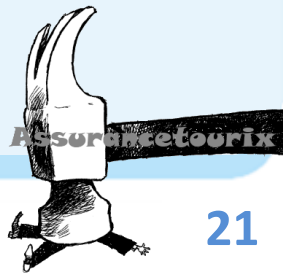
Base de connaissances Méhari

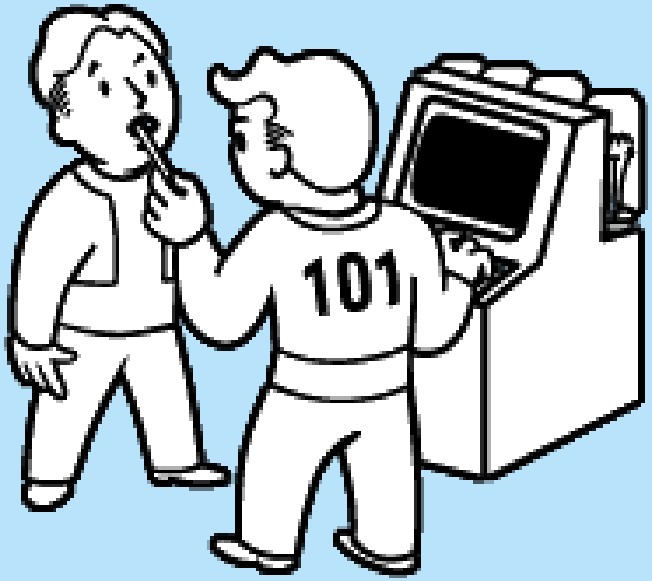
Onglet	Objectif	
Intro	Description et navigation entre les onglets du fichier de la base de connaissance	
Licence	Rappel de la licence Publique de MEHARI	
Module d'analyse des enjeux et classification des actifs:		Tableaux de classification : T1, T2 et Classif — Masquer →
T1 et T2	Tableaux de de classification	
Classif	Classification des actifs	
Module du diagnostic des services de sécurité (ou d'audit)		Feuilles de questionnaires : de 01Org à 14 Msi Thèmes et Score ISO — Masquer →
Domaines 01 Org à 14 MSI	Questionnaires relatifs aux domaines (01 à 14) de sécurité MEHARI	
Services	Récapitulé de la qualité des services de sécurité (avec variantes)	
Thèmes	Thèmes de sécurité Mehari : regroupement des services et sous-services en 10 centres d'intérêts et 18 axes de représentation	
Score ISO	Table de scoring ISO 27002 suite au diagnostic des services Mehari	
Module d'analyse de risque (identification, estimation et évaluation des risques)		Feuilles d'analyse des risques : Evénements types, Risques par actifs ou événements — Masquer →
Expo	Tableau des expositions naturelles aux menaces	
Scénarios	Scénarios de risque incluant le calcul des risques	
Risk%Actif	Panorama de gravité des scénarios par type d'actif	
Risk%event	Panorama de gravité des scénarios par type d'événement	
Traitement des risques : options, plans de réduction et suivi		Feuilles de traitement : Plans_d'action Obj_PA — Masquer →
Plans_d'action	Sélection de plans de réduction des risques	
Obj_PA	Sélection de plans de réduction des risques	

Est-ce applicable ?

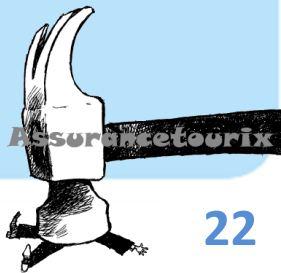
:: MEHARI

- Les +
  - Très complet
  - Très précis
  - Découpage en cellules et modules d'analyse
- Les –
  - Très complet -> « Trop »
  - « Usine à gaz »





Audit Actif



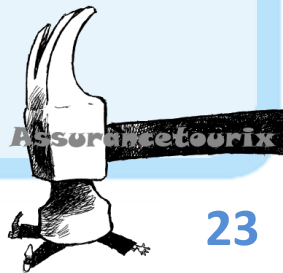
Nos objectifs

- Nos objectifs théoriques :
  - Déploiement de Nessus
  - Simulation des flux malveillants pour détection
  - Utilisation de TOOL KIT
  - Audit de machines et d'équipements réseaux
  - Migration et centralisation vers OSIM long terme

- Nos objectifs réels:

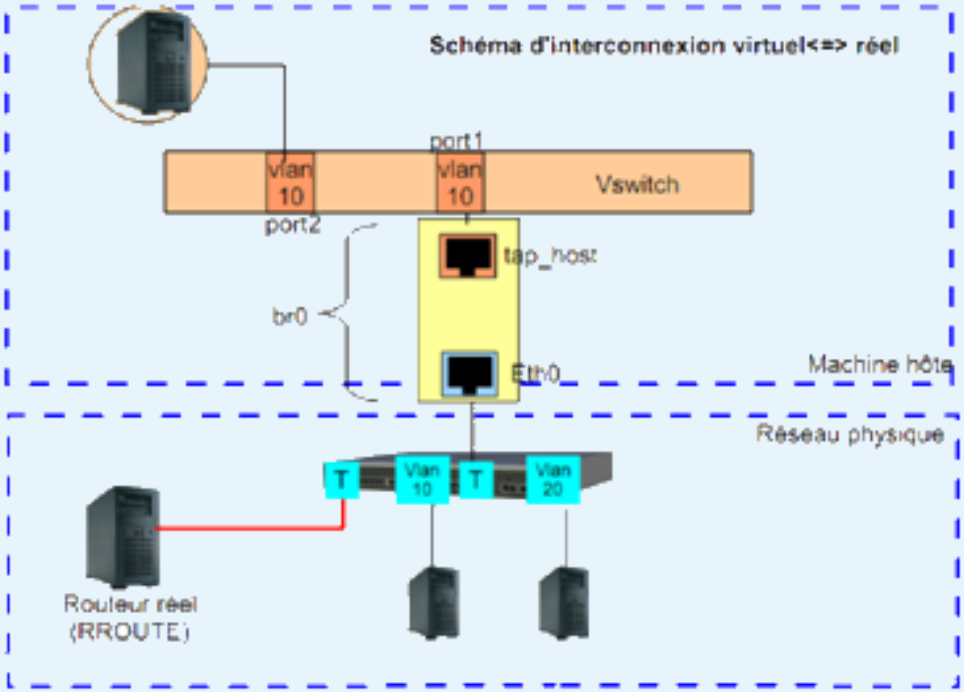
➔ Evolution suite au contrat

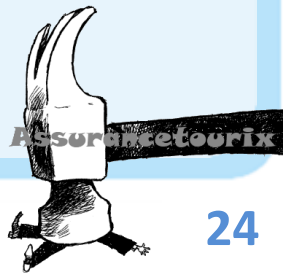
- Déployer des outils de gestion de log
- Administration du serveur
- Analyse de flux



Serveur Auditorium (1/2)

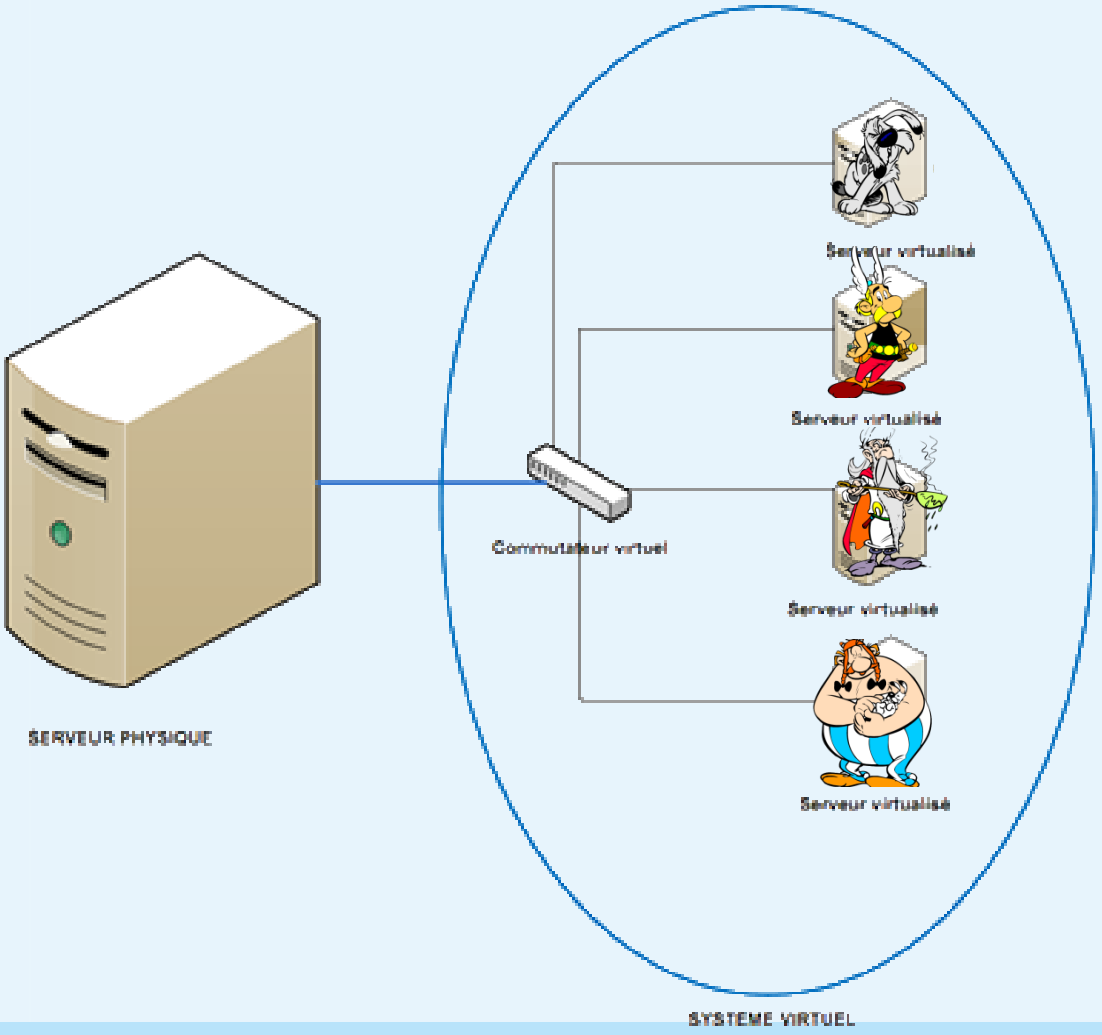
- Notre Serveur physique virtualisant :
  - Des équipements réseaux
  - Des serveurs virtuels

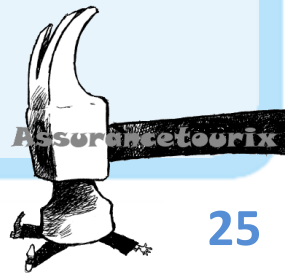




Serveur Auditorium (2/2)

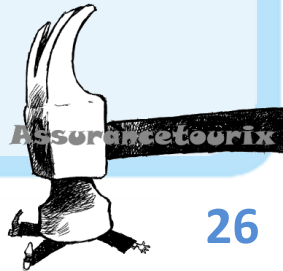
:: Audit Actif





Nessus

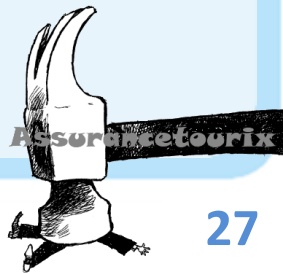
- Scanner de vulnérabilités
  - Machines clientes
  - Serveurs
- Rapports :
  - Ports ouverts
  - Failles de sécurité plus ou moins critiques
- N'a jamais été utiliser
  - ➔ Une certaine appréhension
  - ➔ Trop agressif



Gestion des logs – Syslog (1/2)

- Syslog-ng
  - Concentration des logs
  - Systèmes client/serveur
  - Infrastructure hétérogène
  - Filtrage et classification

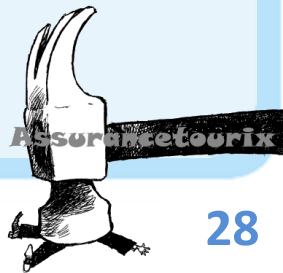
- Log-rotate
  - Rotation des logs
  - Archivages
    - ➔ Études à posteriori



Gestion des logs – Splunk (2/2)

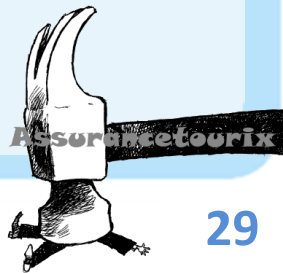
- Centralisation des logs
  - Distant
  - Local
  - Fichiers importés

- **<u>La révélation !!!</u>**
  - ✔ Analyse simplifiée
  - ✖ Gourmand en ressources
  - ✖ Usine à gaz



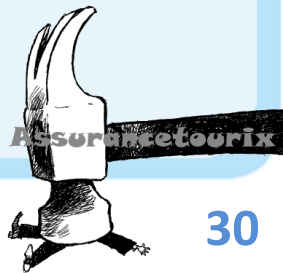
Netflow

- Propriétaire CISCO
- Analyse des compteurs de flux
- Composé de :
  - Nfsend ➔ interface graphique
  - Nfdump ➔ enregistrement
- Remonté de compteurs du routeur gateway

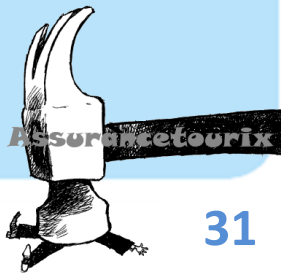


Bilan

- Les objectifs théoriques ⇔ des réels
- Mise en places de logiciels élémentaires
- Découverte aggréable de l'outils Splunk
- Difficulté d'avoir des informations

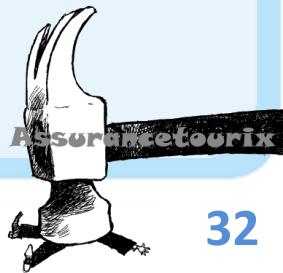


IDS / IPS



Groupe IDS/IPS

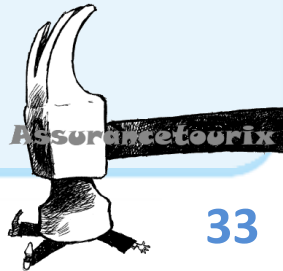
- Définition:
  - Détection d'intrusion
  - Déclenchement d'alertes de sécurité.
- 2 types d'IDS :
  - NIDS (Network Intrusion Detection System)
  - HIDS (Host based IDS)
- SIEM (Security Event Information Management)



SNORT (1/3)

- Définition:
  - NIDS,
  - Journalisation des alertes.
  - Plusieurs modes d'utilisation :

- mode sniffer:	Snort va lire le trafic réseau et le montrer à l'écran.
- mode packet logger:	Snort va enregistrer le trafic réseau sur un fichier.
- mode IDS:	Le trafic réseau correspondant aux règles de sécurité sera enregistré. (mode utilisé dans notre tutorial)
- mode IPS:	Aussi connu sous le nom de snort-inline (IPS= Intrusion Prevention System)



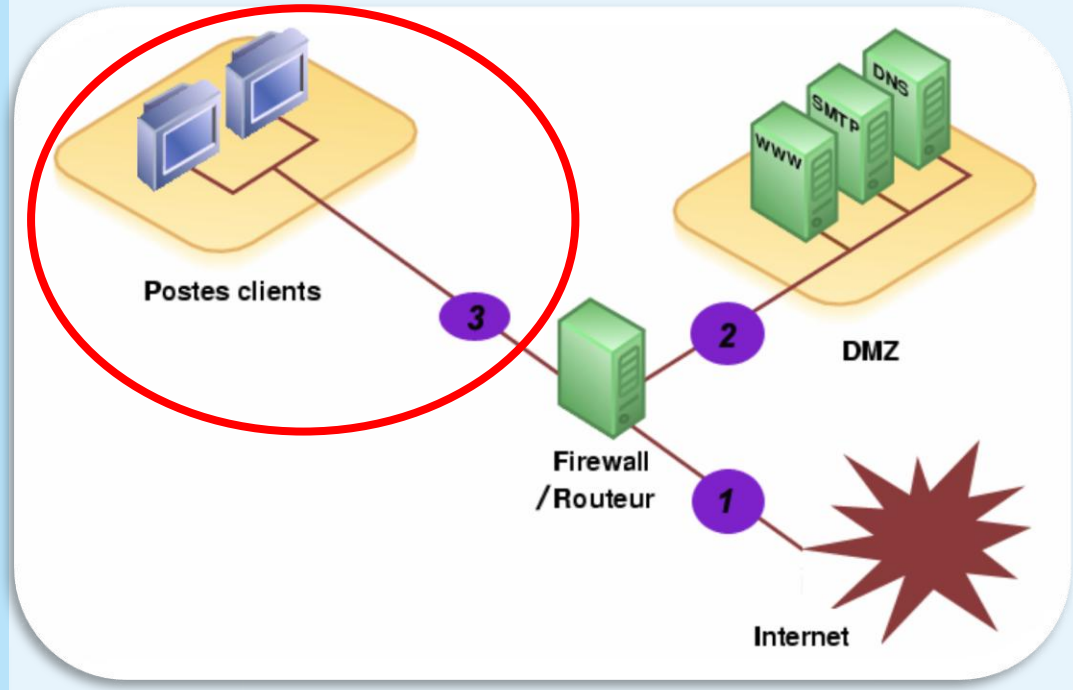
SNORT (2/3)

- Avantages et inconvénients de SNORT :

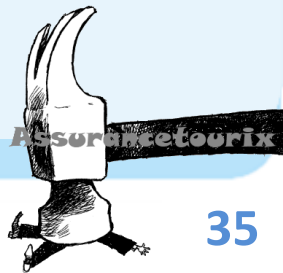
SNORT	
Avantages	**Inconvénients**
• Large communauté d'utilisateurs • Bonne base de signatures • Mise en œuvre basique rapide • Beaucoup de documentations • Fichiers d'alertes très complets (header des paquets, lien vers description de l'attaque...)	• Technologie complexe • Nécessite un degré d'expertise élevé • Long à optimiser • Réputer pour générer de fausses alertes • Encore immature • De nombreuses fonctionnalités payantes

SNORT (3/3)

- Où positionner son IDS ?
  - Architecture



Positionnement IDS dans notre cas



Problèmes rencontrés

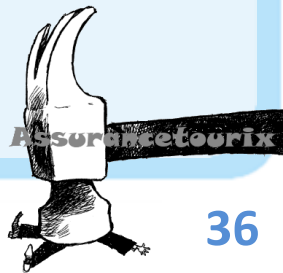
- Prélude

  ⇒ **Utilisation de SNORT.**

- Port SPAN

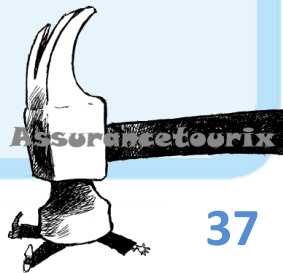
  ⇒ **Transfert de la sonde SNORT sur la machine physique.**

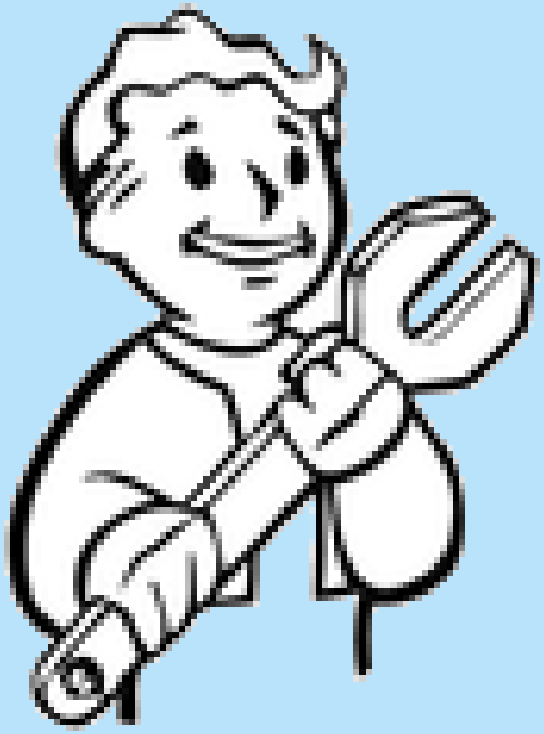
- Interruptions de service



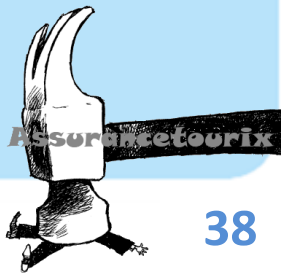
Bilan

- Détection d'intrusions
  - ⇒ **Stade expérimental.**
- Non-fiables
  - ⇒ **Faux-négatifs beaucoup trop nombreux.**
- Intrusions Prevention System
  - ⇒ **Faux-positifs beaucoup trop dangereux.**
- SIEM
  - ⇒ **Configuration et maintenance extrêmement imposantes.**





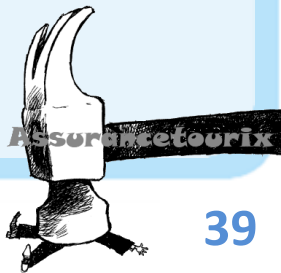
Supervision



Sommaire (SUPERVISION)

:: Supervision

- **Présentation des outils**
- **Méthodologie de déploiement**
- **Surveillance de l'architecture de la société « AéroDef »**
- **Résultats obtenus**
- **Problèmes rencontrés**



Présentation des outils

- Distribution **F A N** : (**F**ully **A**utomated **N**agios)
  - Linux (CentOS)
  - Solution globale dédiée à la supervision
  - Clé en main (installation des outils réalisée)

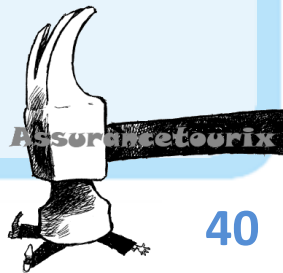
Fan
Fully Automated Nagios

- **NAGIOS** : cœur de la supervision

Nagios®

- **CENTREON** : offre une interface web intuitive

Centreon



Présentation des outils (suite)

- **NAGVIS** : cartographie du réseau

NagVis

- **NARETO**: organisation des éléments à superviser (inutilisé)

NaReTo
Nagios Reporting Tool

- **APACHE** : serveur web (https)

Apache

- **MY SQL** : BDD des informations récoltées

MySQL

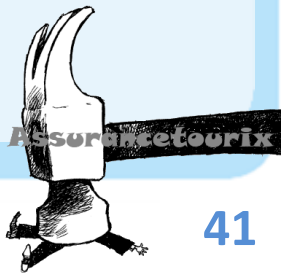
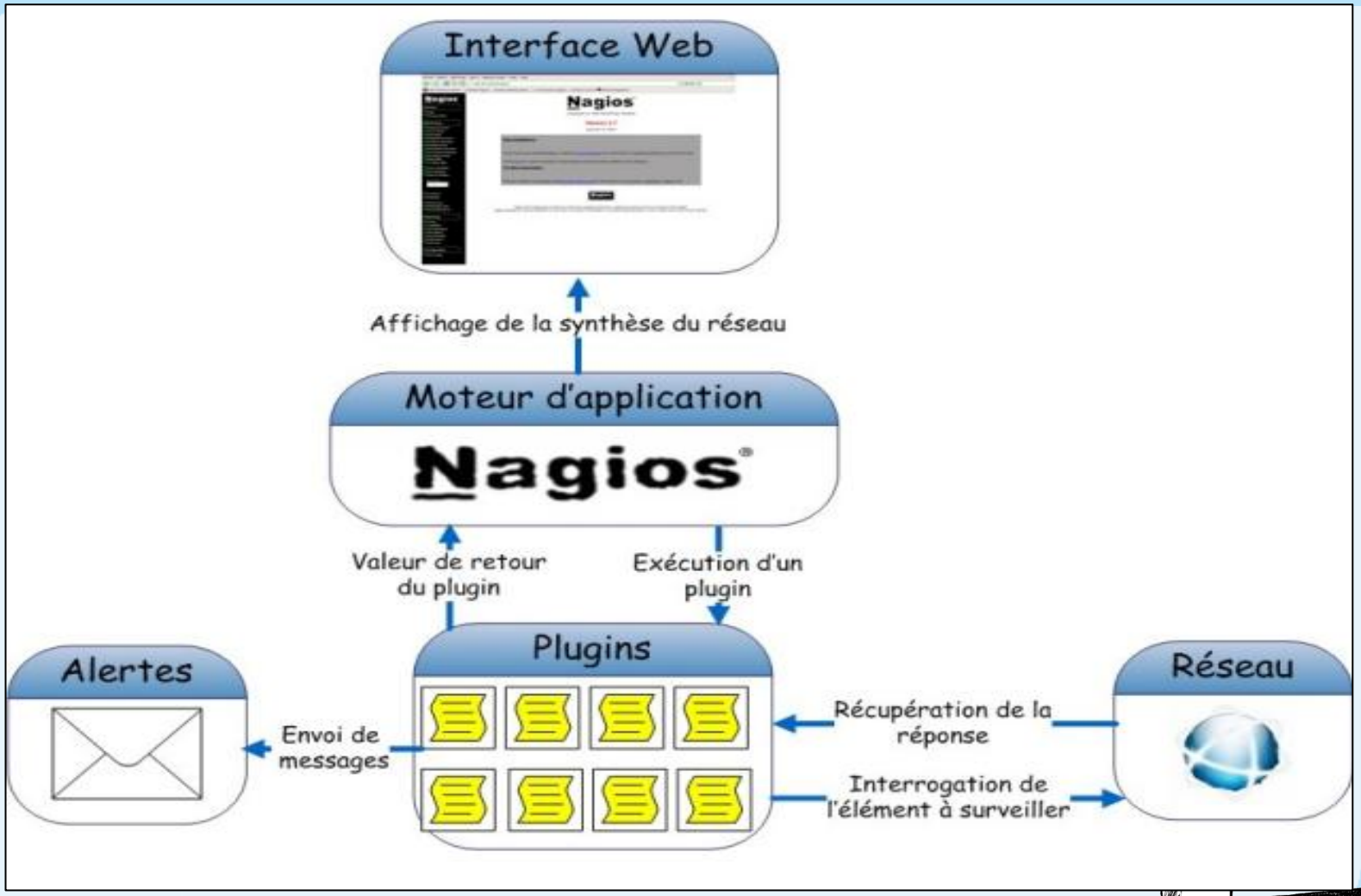


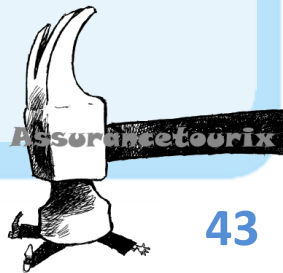
Schéma général de la supervision



La méthodologie de déploiement (1/4)

:: Supervision

- Récupération des informations :
  - Connaître l'architecture du client
  - Connaître ses besoins
  - Avoir une liste exhaustive des différents types de machines
    - Définir des niveaux de criticité
    - De manière plus générale lister les spécificités
  - Avoir la liste des services
    - Définir des niveaux de criticités



La méthodologie de déploiement (2/4)

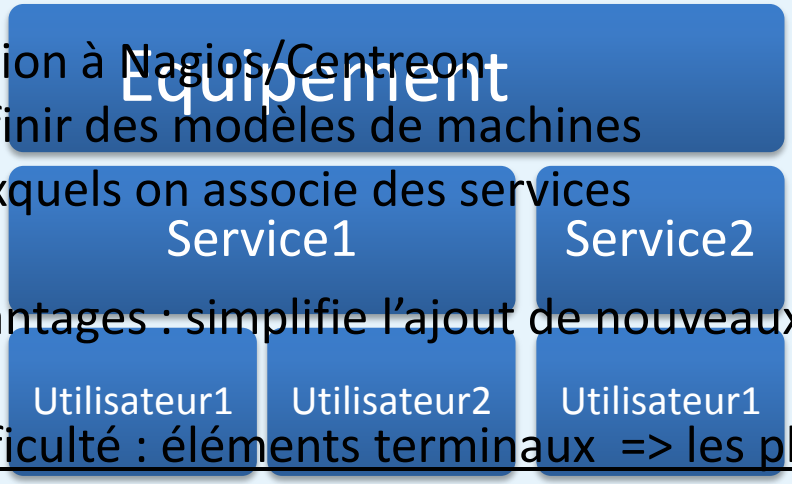
:: Supervision

Après installation de l'agent sur l'équipement à superviser

Intégration à Nagios/Centreon

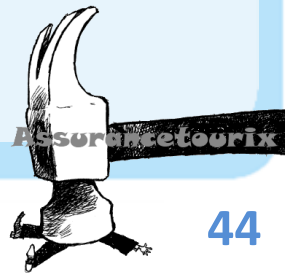
Définir des modèles de machines

Auxquels on associe des services



Avantages : simplifie l'ajout de nouveaux équipements

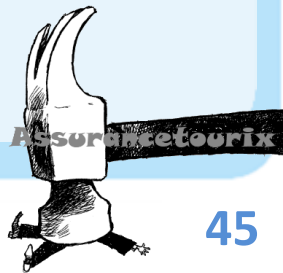
Difficulté : éléments terminaux => les plugins



La méthodologie de déploiement (3/4)

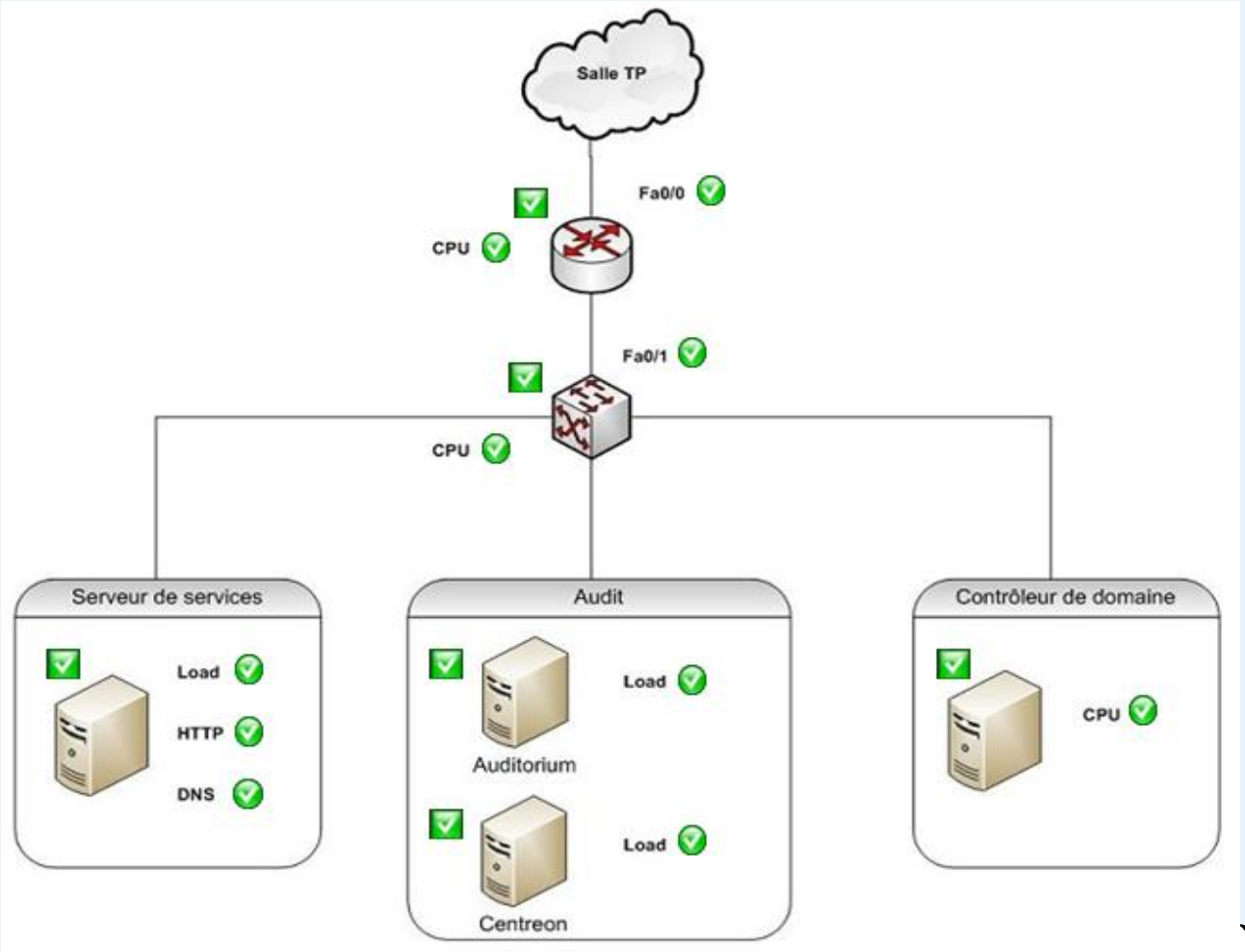
:: Supervision

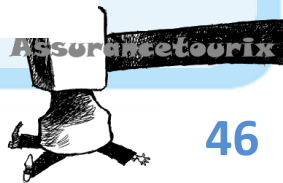
- Les utilisateurs
  - Leurs pouvoirs sont restreints
  - Grâce à des ACL
  - Alertes mail ??
- Le passage de relai :
  - Initier le client à l'outil de supervision
  - Par transmission orale



Méthodologie de déploiement (4/4)

:: Supervision





Surveillance de l'architecture AéroDef (1/2)

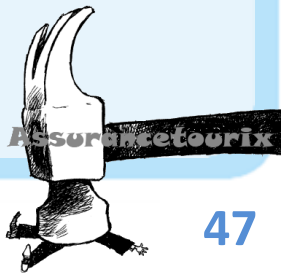
- Eléments réseau

Routeur Cisco

- Etat (UP/DOWN)
- Ping

Switch Cisco

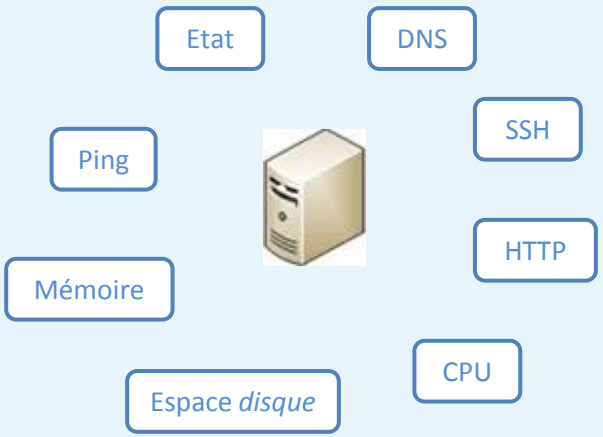
- Etat des interfaces
- CPU
- Mémoire



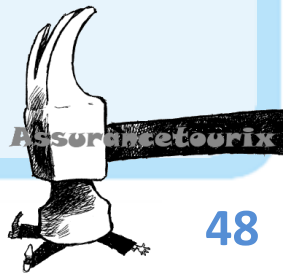
Surveillance de l'architecture AéroDef (2/2)

- Eléments système

Serveur de services (Linux)



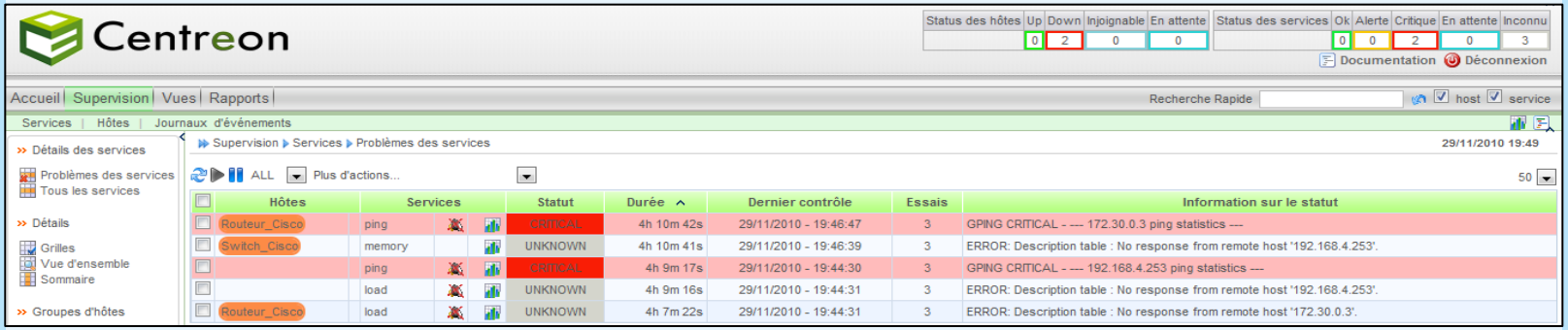
Contrôleur de domaine (Windows)



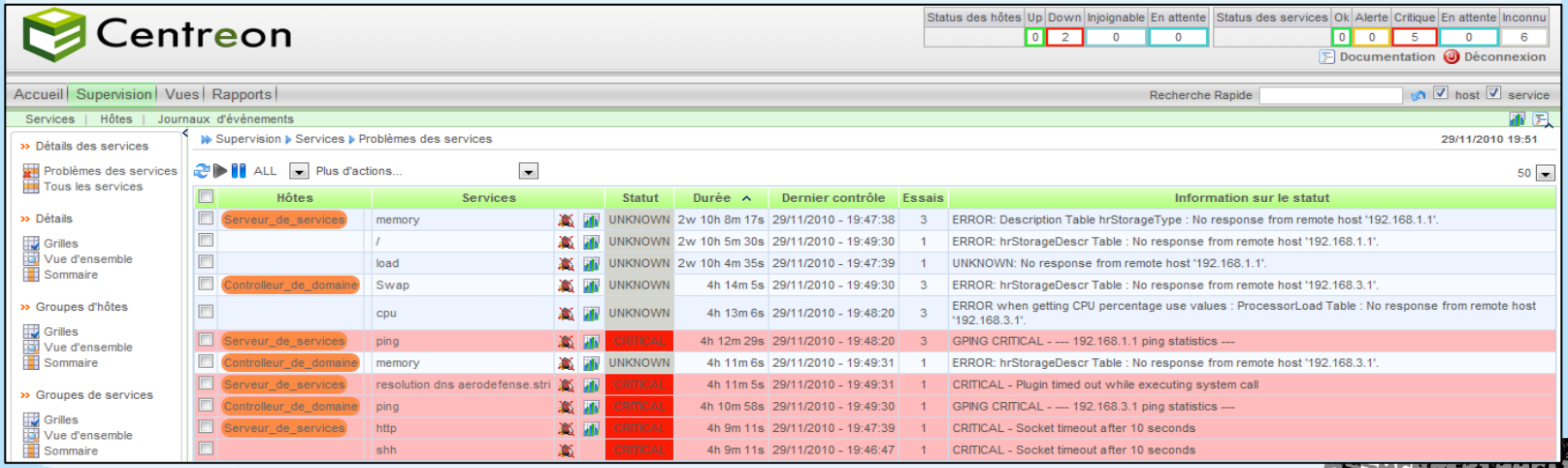
Résultats obtenus

:: Supervision

- **Interface « supervision réseau » :**



- **Interface « supervision serveur » :**

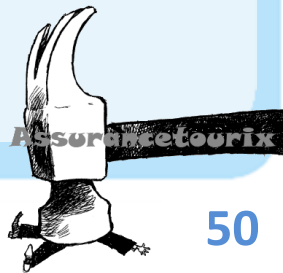


Résultats obtenus (suite)

:: Supervision

- **Détection « mauvais serveur DNS »:**

Services resolution dns aerodefense.stri sur l'hôte Serveur_de_services [Debian]	
Services	
Etat des services	CRITICAL
Information sur l'état	Domain aerodefense.stri was not found by the server
Données de performence	
Tentative actuelle	3 / 3
Type d'état	Hard
Dernier contrôle du type	Active
Dernier contrôle	15/11/2010 - 08:34:41
Prochaine planification de contrôle actif	15/11/2010 - 08:39:41
Latence	0.897 seconds
Durée de la vérification	0.05447 seconds
Changement du dernier état	07/11/2010 - 22:01:25
Durée de l'état actuel	1w 10h 34m 55s
Dernière notification du service	
Numéro de notification actuel	0
Est ce que ce service est oscillant ?	Non
Pourcentage de changement d'état	0 %
Dans la planification d'arrêt ?	Non
Dernière mise à jour	15/11/2010 - 08:36:20

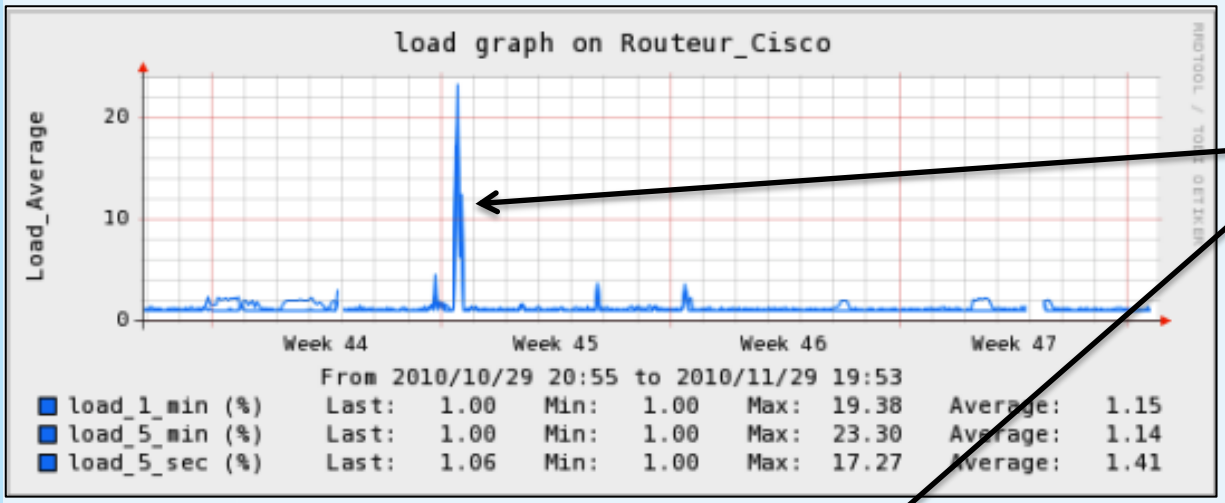


Résultats obtenus (suite)

:: Supervision

- **Détection « Surcharge du routeur »:**

Groupe Attaque

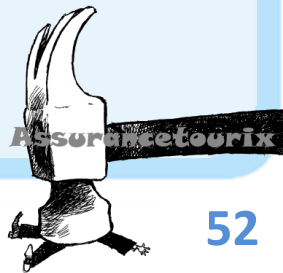


- **Détection « Serveur de services hors ligne »:**

Hôtes	Statut	Adresse IP	Dernier contrôle	Durée	Information sur le statut
Auditorium	UP	192.168.2.1	15/11/2010 - 09:50:54	5h 47m 4s	PING OK - Packet loss = 0%, RTA = 166.74 ms
Centreon	UP	127.0.0.1	15/11/2010 - 09:49:59	1w 18h 33m 19s	PING OK - Packet loss = 0%, RTA = 0.23 ms
Controlleur_de_domaine	UP	192.168.3.1	15/11/2010 - 09:50:25	5h 47m 1s	PING OK - Packet loss = 0%, RTA = 4.98 ms
Nessus	DOWN	192.168.2.102	15/11/2010 - 09:50:54	26m 24s	CRITICAL - Host Unreachable (192.168.2.102)
Routeur_Cisco	UP	172.30.0.3	15/11/2010 - 09:46:46	1w 32m 27s	PING OK - Packet loss = 0%, RTA = 1.66 ms
Serveur_de_services	DOWN	192.168.1.1	15/11/2010 - 09:49:58	6m 46s	(Host Check Timed Out)
Switch_Cisco	UP	192.168.4.253	15/11/2010 - 09:48:22	1w 32m 32s	PING OK - Packet loss = 0%, RTA = 1.29 ms

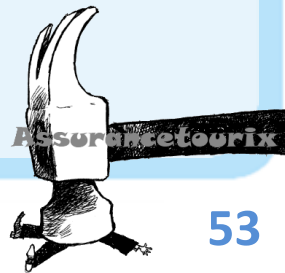
Problèmes rencontrés (1/2)

- Connaissance de l'architecture d'AéroDef
  - Non exhaustive : architecture évoluait au fur et à mesure
  - Demande d'informations nouveaux équipements
  - Plusieurs réunions avec les responsables
    - Equipements
    - Services
- Installation des agents
  - Assurancetourix aucun accès aux équipements AéroDef
  - Premiers tests sur nos équipements
  - Création de tutoriaux pour AéroDef
  - Modifs et MAJ : échanges avec les différents responsables

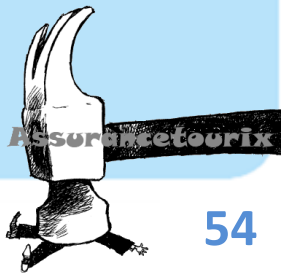


Problèmes rencontrés (2/2)

- Autorisations Firewall
  - Communication entre « manager » et « agents »
  - Contacter la personne responsable
  - Ouvrir les ports
    - SNMP
    - NRPE
- Surcharge du réseau et des logs
  - A cause des protocoles gourmands en ressources
    - ➔ Ralentissement réseau
    - ➔ Pollution des logs
  - Solution : intervalles d'interrogation des équipements plus longs
- Différence d'utilisation entre SNMP et NRPE
  - Différences installation, configuration et utilisation
  - Equipements réseau : SNMP (natif)
  - Serveurs (Linux et Windows) : utilisation des 2 pour plus de choix



VOIP - TOIP



Choix de l'architecture VOIP

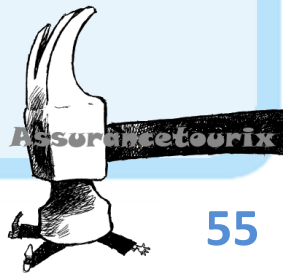
:: Téléphonie sur IP

- Utilisation de l'IPBX Asterisk

  Pourquoi ?

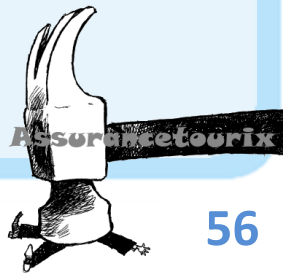
  - Gratuit & OpenSource
  - Nécessite uniquement un PC
  - Deux membres du groupe l'ont déjà utilisé
  - Forte communauté

- Utilisation du protocole SIP
  - Le plus utilisé dans le domaine
  - Plus simple d'utilisation que H323
  - Beaucoup de softphones l'utilisent



Softphone

- Comptes :
  - 6 comptes crées :
    - 4 pour AssuranceTourix
    - 2 pour Aerodef
- VLAN VoIP :
  - Tout paquet identifié dans un VLAN
  - ➔ X-lite permet marquage de ses paquets au niveau 3 mais pas au niveau 2
  - Or le switch CISCO 3560 PoE ➔ Taggage VLAN voix
- Cependant :
  - Marquage par le switch des VLAN effectif

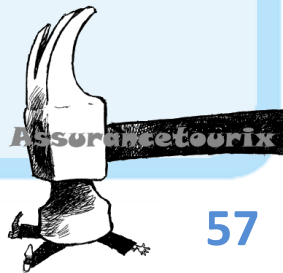


Attaques réalisables

:: Téléphonie sur IP

- Déni de Service (DOS) :
  - « flooding SIP », « TCP syn » ou « UDP ».
  - IPBX , Téléphones IP ou Softphones.
  - Saturation et mise en hors-service des services VOIP.

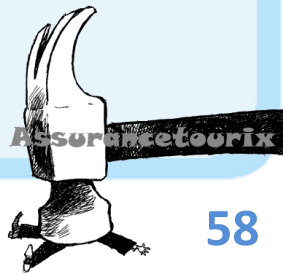
- Usurpation d'identité en interne:
  - Afficher un numéro de téléphone différent du sien.
  - Prétendre être le centre de sécurité ou le directeur.
  - Demander des informations.



Attaques réalisées

- Ecoute des flux RTP :
  - Outils : Arp-sk et Wireshark.
  - Man in the middle : entre appelant/appelé
  - Ecouter et enregistrer les conversations.

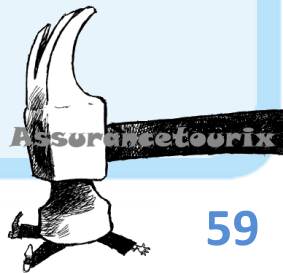
- Récupération et cassage des comptes:
  - Outils : Arp-sk, Wireshark et Sipcrack .
  - Man in the middle : entre client/serveur.
  - Intercepter les requêtes REGISTER (numéro et un hash MD5)
  - Numéro et nom du client : facilement récupérable.
  - Attaque par dictionnaire (ou bruteforce) sur le hash : Plus difficile.
  - Politique de mot de passe complexe.



Les parades

- Usurpation de numéro:
  - Détection d'attaque (IDS/IPS) : Snort ou ArpWatch.
  - Limiter nombre d'@ MAC par port : « port security ».

- Ecoutes RTP et Récupération des comptes
  - Sécurisé SIP et RTP : Clef publiques/privées
  - SIPS et SRTP



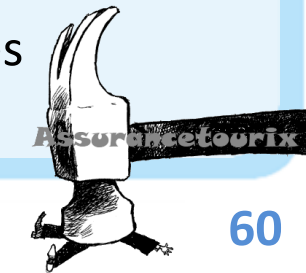
Les problèmes rencontrés

- Configuration des téléphones CISCO
  - Modèle 7945G
  - Protocole Propriétaire SKINNY de base

- Utilisation du protocole Skinny ?
  - Possible avec l'Asterisk
  - MAIS complexe

- Utilisation du protocole SIP ?
  - Mise à jour du Firmware en SIP possible
  - MAIS Call Manager obligatoire

➔ Beaucoup de problèmes avec les protocoles propriétaires



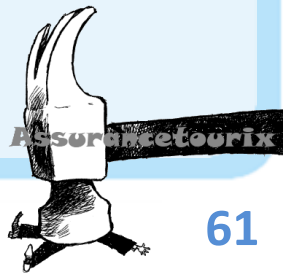
Les problèmes rencontrés

:: Téléphonie sur IP

- Filtrage des flux de la TOIP
  - Problème ?
    - ✓ Le RTP n'a pas de ports fixes !
  - Solution ?
    - ✓ Fixer les ports RTP sous Asterisk

Ou

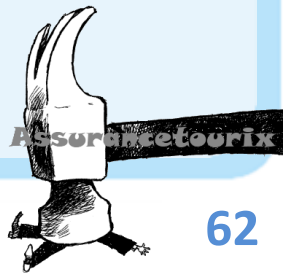
    - ✓ Utilisation d'une passerelle de niveau applicatif
      - ➢ Lecture du champ SDP des trames SIP



Les problèmes rencontrés

:: Téléphonie sur IP

- Aerodef :
  - Signature du contrat Toip: 11 jours avant la fin du projet.
  - Architecture : Connaissances partielles. (Nat/Pat, Vlans ..).
  - Administration des switchs : aucune réponse.



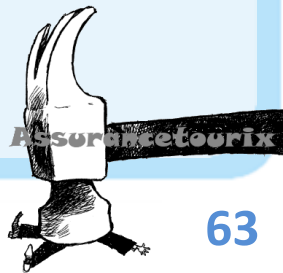
Etude

- Demande AeroDef d'une étude pour 40 postes

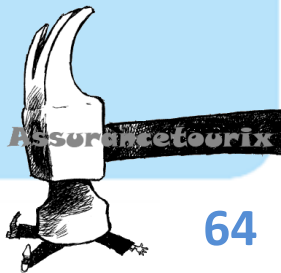
  - Les équipements :
    - ✓ Serveur Asterisk avec 512 RAM
    - ✓ Utilisation de 40 Softphones Xlite gratuit

  - Le réseau
    - ✓ Codec *G711* (64Kbit/s) pour LAN
    - ✓ Codec *G729* (8 Kbit/s) pour WAN

Dans un cas réel : Réaliser un étude complète avec calcul *Erlang*



Analyses confrontations



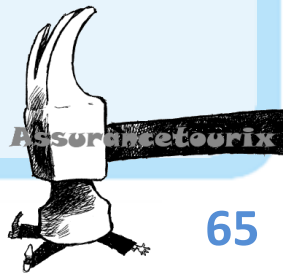
Analyse des confrontations

- Contexte :

➔ 3 confrontations

➔Les Rôles :

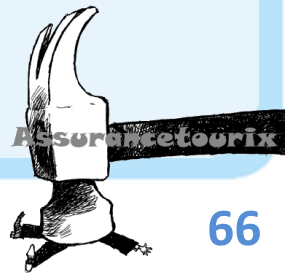
Attaque	Défense	Audit
• Intention de nuire	• Maintien de l'intégrité de leur SI	• Surveillance du SI



Analyse des confrontations

- Première Confrontation :

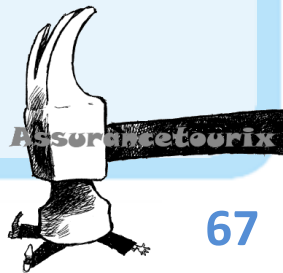
Services resolution dns aerodefense.stri sur l'hôte Serveur_de_services [Debian]	
Services	
Etat des services	CRITICAL
Information sur l'état	Domain aerodefense.stri was not found by the server
Données de performence	
Tentative actuelle	3 / 3
Type d'état	Hard
Dernier contrôle du type	Active
Dernier contrôle	15/11/2010 - 08:34:41
Prochaine planification de contrôle actif	15/11/2010 - 08:39:41
Latence	0.897 seconds
Durée de la vérification	0.05447 seconds
Changement du dernier état	07/11/2010 - 22:01:25
Durée de l'état actuel	1w 10h 34m 55s
Dernière notification du service	
Numéro de notification actuel	0
Est ce que ce service est oscillant ?	Non
Pourcentage de changement d'état	0 %
Dans la planification d'arrêt ?	Non
Dernière mise à jour	15/11/2010 - 08:36:20



Analyse des confrontations

- Deuxième Confrontation « La Revanche »:
  - Attaques réalisées :
    - DNS Spoofing
    - Site Web DEFACED

      ⇒ **Non-application des recommandations de l'audit (installation de « mod Apache Secure »).**



Analyse des confrontations

- Troisième Confrontation « Ultimate Fighting»:

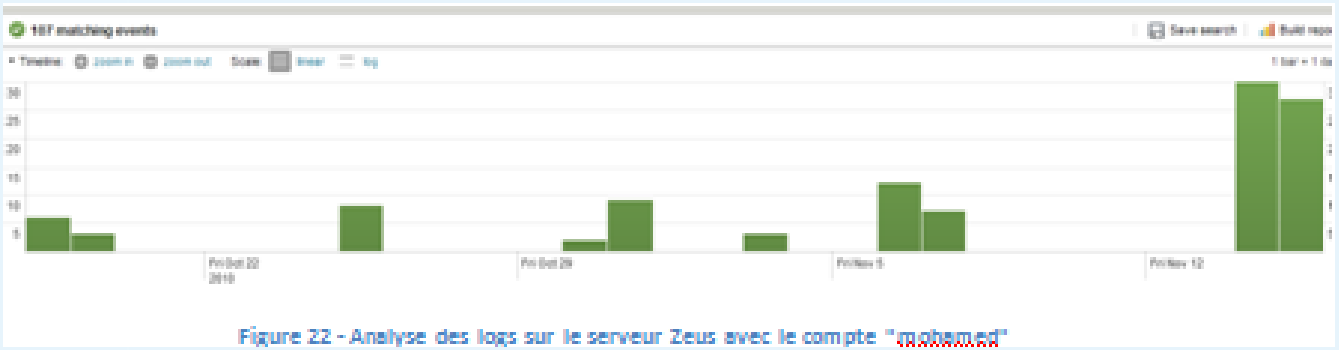
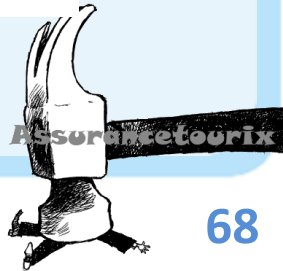


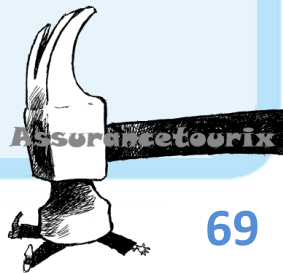
Figure 22 - Analyse des logs sur le serveur Zeus avec le compte "mohamed"

Figure 23 - Authentifications échouées (plus de 40000 en 1 seule journée)

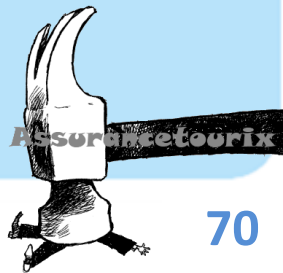


Recommandations émises

- Complexité des mots de passe
- Installation du Apache mod_security
- Surveillance des ports ouverts du routeur
- Chiffrement des emails



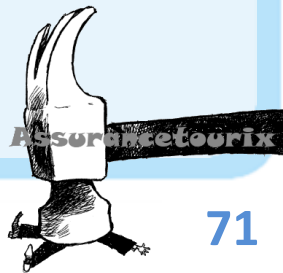
Bilan du projet



Bilan du projet

- En interne ➔ bilan positif
  - Connaissances de la sécurité accrues
  - Équipe responsable et réactive dans l'ensemble
    - Communication,
    - Organisation,
    - Répartition des taches,
  - Respect des délais imposés

- Sur le projet ➔ mitigé
  - Quelques objectifs fixés non atteints
  - Notre but était d'auditer afin de limiter les attaques/intrusions,…
  - Nouvelle approche de la sécurité grâce à la téléphonie



Avez-vous des questions ?

:: Merci pour votre attention